О. Д. Афонин, В. Ю. Каталов, А. С. Штоль

Методическое руководство

по восстановлению паролей и расшифровке данных

ЭЛКОМСОФТ
КОМПЬЮТЕРНАЯ, МОБИЛЬНАЯ
И ОБЛАЧНАЯ КРИМИНАЛИСТИКА

АПРЕЛЬ 2025

Москва

Содержание

1. Введение: для кого и о чём это пособие?

«Методическое руководство по восстановлению паролей и расшифровке данных» предназначено для экспертов правоохранительных органов и специалистов по информационной безопасности. В нём мы расскажем о том, как получить доступ к защищённым и зашифрованным данным, о различных методах снятия защиты и расшифровки данных. Одним из многих рассмотренных методов является подбор установленных пользователем паролей. Рассматриваются способы обхода и взлома шифрования как с использованием методов восстановления паролей, так и без них.

В методическом пособии также рассмотрены действия, предшествующие действиям по снятию защиты – от первичных действий при изъятии цифровой техники до снятия образов оперативной памяти и образов дисков.

В пособии не рассматриваются действия по исследованию содержимого незашифрованных дисков, а также по анализу уже расшифрованных данных.

2. Подготовка: первичные действия при изъятии цифровой техники и носителей информации

Успешное решение проблемы доступа к зашифрованной информации часто зависит от действий, произведённых на этапе изъятия цифровой техники и носителей информации. Те или иные шаги, предпринятые на этом этапе, могут оказаться критически важными, если для защиты доступа к данным используется стойкое шифрование. В худшем случае для расшифровки данных потребуется восстановить оригинальный пароль – процесс, который может оказаться чрезвычайно длительным, а результат – не гарантирован. В то же время исследование включённого компьютера с авторизованной пользовательской сессии может позволить получить доступ к зашифрованным данным или ключам шифрования на месте, для чего при изъятии цифровой техники должен присутствовать квалифицированный эксперт.

В следующих разделах мы расскажем о том, какие действия требуются в различных сценариях (см. раздел «Типичные сценарии»).

3. С чего начать?

В идеальных, тепличных условиях у эксперта будет доступ к мощному оборудованию. В его распоряжение будет передано вся изъятая у подозреваемого аппаратура, использующаяся для хранения и доступа к данным, причём оборудование будет изъято максимально корректным способом, сохранив все авторизованные сессии, смонтированные зашифрованные диски и открытые соединения. У квалифицированного эксперта при этом будет достаточно времени на исследование переданной аппаратуры и не будет никаких других дел, отвлекающих от тщательного анализа улик. В таких условиях часто вскрываются даже самые стойкие пароли – как за счёт обнаруженных в найденных паролях пользователя шаблонов, так и с использованием средств, позволяющих мгновенно получить доступ к уже смонтированным зашифрованным дискам.

К сожалению, идеальные условия встречаются редко. Откровенно говоря, они не встречаются практически никогда – за исключением единичных случаев особой важности. В

этом руководстве мы расскажем о вариантах действий исходя из того, что реально доступно и в рамках заданных ограничений по срокам работы и длительности атак.
В идеальном случае все цифровые улики должны быть доставлена эксперту в том виде, в котором они были изъяты. Для портативных компьютеров, мобильных устройств, смартфонов это обозначает транспортировку во включённом состоянии, изолированными от беспроводных сетей и подключёнными к внешнему источнику питания. Для настольных компьютеров такая транспортировка затруднена технически, поэтому при расследовании особо важных преступлений на место вместе с оперативной группой выезжает эксперт, который сможет принять решение о транспортировке или дальнейшем исследовании устройств с авторизованной пользовательской сессией на месте.

- Если устройство включено – **не выключать!**
- Если устройство выключено – **не включать!**

3.1. Возможные проблемы при неправильном изъятии цифровой техники

Какие трудности может создать безоглядное отключение настольных компьютеров от сети электропитания и их дальнейшая транспортировка? Перечислим основные из них.

1. **Улики хранятся на зашифрованных дисках**. Так, использование встроенной в Windows системы шифрования BitLocker (а также подобных систем, использующихся на компьютерах с macOS и Linux) не позволит получить доступ к данным, если не известен пароль от учётной записи пользователя. При этом в случае с BitLocker даже пароля от учётной записи может оказаться недостаточно: если в шифровании участвует модуль TPM или его эмуляция, то при изменении аппаратной конфигурации системы (например, физический накопитель извлечён из компьютера пользователя) для разблокировки раздела и расшифровки данных потребуется уже специальный ключ восстановления доступа. Найти такой ключ может оказаться нетривиальной (но всё же возможной) задачей; подробности – в разделе «Депонированные ключи в облаке и Active Directory».
2. **Улики хранятся в зашифрованной виртуальной машине**. Это – достаточно распространённый способ сокрытия улик. Шифрование современных виртуальных машин может быть достаточно стойким, а восстановление пароля к ним – исключительно длительным процессом. Зашифрованные виртуальные машины могут быть как обычными, так и «волатильными» — такими, изменения в которых не сохраняются в файле с образом виртуальной машины.
3. **Используются волатильные виртуальные машины**. Один из способов сокрытия улик – использование так называемых «волатильных» виртуальных машин. В этом случае содержимое файла, в котором содержится образ виртуальной машины, остаётся неизменным; все изменения (чаты, переписка, авторизованные онлайновые сессии, прочие виды активности) производятся только в оперативной памяти компьютера. Выключение компьютера (или закрытие виртуальной машины) не сохраняет изменения в образ, как это происходит при использовании обычных виртуальных машин, а просто сбрасывает их. Таким образом, выключение компьютера, на котором запущена волатильная виртуальная машина, приведёт к мгновенному и полному уничтожению улик, восстановить которые не поможет даже пароль от виртуальной машины. Анализ авторизованной пользовательской сессии либо снятие образа оперативной памяти компьютера – единственные способы получить доступ к таким данным.

4. **Переписка ведётся в «приватной» сессии без сохранения истории**. Распространённой является ситуация, в которой преступник ведёт переписку через веб-интерфейс браузера, работающего в режиме сокрытия следов («приватные» сессии, специализированные браузеры, Tor). Выключение компьютера уничтожит как историю переписки, так и следы её существования.

5. **Для сокрытия улик используются скрытые контейнеры**. Современные криптоконтейнеры позволяют создавать скрытые разделы, обнаружить существование которых невозможно, не зная в точности пароля и корректных параметров шифрования. В случае, если такой контейнер был смонтирован во время обыска, анализ авторизованной пользовательской сессии позволит задокументировать его наличие, не позволит преступнику отрицать факт его существования, в то же время предоставляя шанс эксперту извлечь зашифрованные улики на месте без длительных атак.

6. **Используется активная защита**. В расследовании киберпреступлений необходимо учитывать возможность наличия так называемой активной защиты. Так, попытка загрузить или разблокировать компьютер подозреваемого без знания корректной процедуры аутентификации может привести к необратимым последствиям, в то время как извлечение накопителя покажет лишь то, что он зашифрован. Анализ авторизованной пользовательской сессии на месте может оказаться единственным способом получить доступ к уликам.

Каким образом сохранить доступ к этим и другим уликам? В особо важных расследованиях в составе группы выезжает эксперт, который на месте принимает решение о проведении анализа авторизованной пользовательской сессии, гибернации или обесточивании компьютеров для их последующей транспортировки в лабораторию. В менее важных случаях, к сожалению, доступ к уликам будет безвозвратно утрачен, и эксперту в лаборатории придётся работать с тем, что имеется.

3.2. Возможная последовательность действий

В зависимости от обстоятельств, возможны различные последовательности действий. Рекомендуемая нами стратегия в англоязычной литературе описана под названием “low hanging fruit”. Смысл этой стратегии в том, чтобы в первую очередь предпринять действия, требующие минимума усилий и затрат времени при максимальной потенциальной отдаче. К таковым относятся:

- **работа в полевых условиях:** анализ авторизованной пользовательской сессии, снятие образа оперативной памяти, снятие образа смонтированных дисков; снятие образа файловой системы;
- **снятие образов встроенных накопителей:** загрузка с внешнего накопителя в Elcomsoft System Recovery; снятие образа всех обнаруженных накопителей; извлечение метаданных шифрования для зашифрованных дисков;
- **для компьютеров в состоянии гибернации или гибридного сна:** анализ файлов гибернации и подкачки (поиск ключей шифрования);
- **для извлечённых из компьютеров накопителей:** снятие образа диска; извлечение метаданных шифрования; анализ на предмет возможности парольной атаки.

В то же время действия по анализу контекста, настройке и проведению атак на пароли потребуют серьёзных затрат времени и усилий; при этом реальный процент дел, в которых

присутствовала парольная защита, которая была впоследствии вскрыта методом прямой атаки, не превышает 10–15%. По указанным причинам в рекомендуемой нами стратегии эти шаги проделываются в последнюю очередь.

4. Методы получения доступа к данным

Существуют различные методы, которыми можно получить доступ к зашифрованным данным, и восстановление установленного пользователем пароля – лишь один из них. Более того, атака на пароль, особенно с использованием метода полного перебора, является крайней мерой, к которой имеет смысл прибегать лишь после того, как были исчерпаны все остальные возможности.

В рамках данного методического пособия подразумевается, что цель эксперта – получить доступ к данным. Восстановление пароля здесь является средством, всего лишь одним из возможных способов получения доступа к информации. В то же время в некоторых ситуациях необходимо восстановить именно оригинальный пароль. Подробнее об этом рассказано в следующей главе.

Меры по восстановлению доступа к защищённым данным разительно отличаются по уровню затраченных ресурсов – в первую очередь времени работы эксперта, во вторую – машинного времени, которое потребуется на проведение атак. Ниже приводятся известные нам способы получения доступа к зашифрованным данным, отсортированные в порядке увеличения их ресурсоёмкости. По возможности рекомендуем использовать наименее ресурсоёмкие методы в первую очередь, прибегая к «тяжёлой артиллерии» в виде перебора паролей в самую последнюю очередь.

1. Для зашифрованных дисков и виртуальных машин: анализ авторизованной пользовательской сессии. Этот способ позволяет добраться до зашифрованных данных с минимальными усилиями, но требует высокой квалификации эксперта; зачастую требуется выездная экспертиза. Рекомендуем обратить особое внимание на этот метод: все прочие способы восстановления доступа к зашифрованным дискам и виртуальным машинам заметно более сложны, потребуют значительных усилий квалифицированного эксперта, не гарантируя результат.

2. Авторизованная пользовательская сессия: если доступен компьютер с активной пользовательской сессией, рекомендуем провести прямое извлечение паролей пользователя из браузеров, связки ключей (macOS), почтовых клиентов и программ мгновенного обмена сообщениями. Обратите внимание: пароли из браузерных хранилищ невозможно извлечь за рамками авторизованной пользовательской сессии в силу их шифрования посредством механизма DPAPI (Windows); для доступа к паролям потребуется пароль от системной учётной записи Windows либо учётной записи Microsoft Account пользователя. Более того, для свежих сборок Windows 10 и Windows 11 этого может оказаться недостаточным, и потребуется прохождение аутентификации через механизм Windows Hello, безопасность которого обеспечивается на аппаратном уровне (что означает невозможность подобрать пароль от учётной записи атакой при извлечении диска).

3. Авторизованная пользовательская сессия либо компьютер в состоянии сна: снять образ оперативной памяти, в котором могут найтись ключи шифрования дисков и/или зашифрованных виртуальных машин. Кроме того, в образе оперативной памяти могут найтись и данные

волатильных виртуальных машин (таких, которые сбрасываются к исходному состоянию после закрытия).

4. Рассмотреть возможность использования загрузочного накопителя с целью извлечения метаданных шифрования и снятия образов дисков.

5. Для дисков BitLocker: рассмотреть возможность использования уязвимости в модулях TPM (до того, как диск будет извлечён из компьютера).

6. Для зашифрованных дисков: провести анализ файлов гибернации и подкачки с целью поиска ключей к зашифрованным дискам и контейнерам. В данном случае наличие авторизованной пользовательской сессии не обязательно.

7. Для ряда форматов (документы, архивы и некоторые другие): использование уязвимостей для снятия защиты. Подробнее об этом рассказывается в соответствующих главах руководства. Рекомендуем ознакомиться с ними перед тем, как будет создана очередь задач на восстановление паролей. Обратите внимание:

8. Стратегия «низко висящего фрукта»: при создании очереди задач на восстановление паролей рекомендуем располагать файлы в порядке стойкости (наименее стойкие форматы – в первую очередь). Это связано как с экономией ресурсов, так и с тем, что успешно подобранный пароль может быть повторно использован пользователем для защиты более стойких форматов.

9. Атака на пароль: если других способов не осталось, проведите атаку на пароль. Атака также различаются по эффективности и ресурсоёмкости. Приблизительная последовательность: предварительная атака; атака по словарю, составленному из паролей пользователя, извлечённых из других источников; анализ шаблонов, по которым составлены пароли пользователя, и проведение атаки по тому же словарю с использованием мутаций на основе шаблонов; атака по словарю, составленному из утечек паролей; словарная атака с мутациями; атака по маскам, составленным на основе шаблонов (см. выше); атака методом полного перебора.

5. Стратегия низко висящего фрукта

В предыдущей главе упоминалась так называемая «стратегия низко висящего фрукта». Расскажем о ней подробнее.

При использовании данной стратегии приоритеты и акценты смещены с ценности самой информации в файле или документе к той его ценности, которую можно использовать для восстановления пароля. Ценность документа как цифровой улики с точки зрения сбора данных о паролях неважна.

К примеру, в рамках данной стратегии наибольшую ценность представляют хранилища паролей в веб-браузерах, для доступа к которым требуется обойти защиту Windows DPAPI. Защита DPAPI, в свою очередь, обходится путём взлома пароля от учётной записи пользователя системы из NTLM. Таким образом, атака на пароли из NTLM получает наивысший приоритет – даже если в системе нет зашифрованных дисков и зашифрованные файлы (документы, архивы и прочие) доступны в файловой системе.

В рамках стратегии низко висящего фрукта процесс сбора и анализа данных имеет итеративный характер. В качестве примера можно привести следующую стратегию:

– анализ незашифрованного диска (есть ли пароли, которые можно извлечь, минуя DPAPI)?

– обновление словаря: полученные данные используются для словаря для атаки на пароль NTLM;

– атака на пароль NTLM;

– получение доступа к данным, зашифрованным DPAPI (пароли браузера; история браузера; данные веб-форм; пароли от сетевых папок).

Необходимо собрать все пользовательские пароли, которые могут быть, извлечены моментально, или в допустимо короткое время, независимо от важности анализируемых документов.

1. Сбор базы данных для анализа.
2. Анализируются полученные данные, включая извлечённые пароли. Составляются шаблоны, маски, подключаются мутации.
3. Обновление словаря: пароли, извлечённые из браузеров пользователя, используются в качестве целевого словаря. Составляются атаки.
4. Файлы и документы, найденные на диске, располагаются в очереди атак в порядке возрастания сложности атаки. В первую очередь атакуются документы с самой слабой защитой. (Кстати, пароли NTLM относятся к паролям с относительно слабой защитой).

Стратегия низко висящего фрукта идёт вразрез с другими стратегиями, в которых приоритет отдаётся атаке на файлы и документы, представляющие наибольший интерес в качестве цифровых улик. К сожалению, документы, которые представляют такую ценность, как правило, хорошо защищены, и шанс получить доступ к данным за минимальное время есть в случае, если хорошо защищённый документ отложить, занявшись в первую очередь сбором данных для последующей атаки.

6. Методы восстановления паролей

В этом разделе описаны основные способы восстановления паролей от метода полного перебора до комплексных способов анализа.

Каким типом атак стоит воспользоваться в том или ином случае? Скорее всего, вы начнёте исследование с того, что извлечёте пароли, сохранённые в браузерах и почтовых клиентах пользователя, в связке ключей iOS или в облаке. Посмотрев на список, возможно, вы сможете вычленить повторяющиеся корни, уловить принципы, которым руководствуется конкретный пользователь при создании паролей, и, наконец, составить шаблон или шаблоны. Если это удалось — в вашем распоряжении маски и гибридные атаки. Если нет — словари и мутации.

Есть ли разница, с чего начинать атаку? Какие файлы имеет смысл атаковать в первую очередь? Порядок имеет значение. Если начать с файлов с самой слабой защитой, вы, скорее всего, сумеете их взломать быстрее прочих. Получив пароли от этих слабо защищённых файлов, вы можете использовать их для атаки на файлы с более надёжной защитой.

6.1. Метод полного перебора

Полный перебор всего пространства возможных паролей — самый простой и оттого популярный метод криптографического анализа. Посредством полного перебора можно взломать

принципиально любой пароль. Единственное ограничение – время, в течение которого должен быть восстановлен доступ к данным.

Основная идея метода полного перебора проста: в качестве потенциальных паролей опробуются все возможные комбинации указанных символов. В качестве указанных символов могут использоваться буквы (в том числе из национальных алфавитов), цифры и специальные символы. Весьма часто ограничения на использованные символы накладывается на стороне приложения или сервиса — к примеру, позволяется использовать исключительно буквы латиницы, цифры и ограниченный набор специальных символов. В то же время политики безопасности могут диктовать минимальную длину пароля и обязательное использование тех или иных элементов (например, как минимум одной заглавной буквы, цифры или специального символа).

Простейшие математические вычисления позволяют точно узнать максимальную продолжительность атаки: время, за которое можно перебрать всё пространство паролей заданной длины. Формула включает число возможных символов, из которых состоит пароль, которое возводится в степень количества знаков в пароле. Так, если в качестве возможных символов используются только буквы английского алфавита (их 26), причём как строчные, так и прописные (это ещё 26), а длина пароля — 5 знаков, то возможное число комбинаций будет таким:

$$(26 + 26)^5 = 380\,204\,032$$

Цифры экспоненциально увеличиваются с увеличением длины пароля. Например, для 7-значных паролей одного типа общее количество составляет:

$$(26 + 26)^7 = 1\,028\,071\,702\,528$$

При добавлении чисел и специальных символов из расширенного диапазона число возможных комбинаций превышает возможности метода прямого перебора:

$$(26 + 26 + 10 + 33)^7 = 69\,833\,729\,609\,375$$

Чтобы узнать максимальное время, в течение которого будет гарантированно найден пароль заданной длины, достаточно разделить число комбинаций на скорость перебора для заданного типа файлов средствами доступного аппаратного обеспечения. Например, если скорость перебора на компьютере для файла составит 10 миллионов комбинаций в секунду, на восстановление пароля из первого примера (5 букв, оба регистра) уйдёт не более пяти минут. Если скорость составляет 100 паролей в секунду (например, вы пытаетесь взломать зашифрованный последней версией Microsoft Office документ без использования GPU), а пароль содержит не менее 7 символов из расширенного диапазона, то максимальное время атаки увеличивается примерно до 700 миллиардов секунд или ~ 22 тысяч лет.

Основная сложность в переборе паролей состоит в том, что в ряде случаев ни длина пароля, ни наборы использованных символов заранее неизвестны, поэтому приходится либо пробовать все возможные комбинации, либо использовать альтернативный подход.

Важно: все способы, за исключением метода полного перебора, ограничивают исследуемое пространство пароля и могут не обнаружить те или иные пароли, если они не укладываются в заданные условия. Такие методы атаки используются для того, чтобы в ускоренном режиме опробовать наиболее вероятные с точки зрения эксперта пароли.

6.1.1. Всегда ли можно найти пароль полным перебором?

Предположим, что в нашем распоряжении достаточно времени и условно бесконечные вычислительные ресурсы. Означает ли это, что методом полного перебора рано или поздно мы точно найдём любой пароль? Казалось бы, ответ положительный, но вспомним, что "все альтернативные способы **ограничивают исследуемое пространство пароля** и могут не обнаружить те или иные пароли, если они не укладываются в заданные условия". А метод полного перебора — не ограничивает?

Оказывается, ограничивает, а в реальных приложениях для восстановления паролей "полный" перебор — не такой уж и полный. К примеру, в большинстве программ, работающих с алфавитами на основе латиницы, в качестве набора символов, по которому осуществляется перебор, используются прописные и заглавные буквы латинского алфавита (реже — с дополнительными буквами из различных европейских языков), цифры и очень ограниченный набор специальных символов. А если пользователь, к примеру, носитель языка панджаби, на котором говорит 125 миллионов человек? А если он из Китая, и в пароле может встретиться любой из доступных иероглифов, у которых даже точное число неизвестно, но уже превышает 100 000? А если он просто ввёл комбинацию из набора символов Unicode, удерживая клавишу Alt и воспользовавшись цифровой клавиатурой — например, ☼ (0x263C)?

В актуальной 15-й версии стандарт Unicode определяет 149 186 возможных символов, и доступный набор постоянно расширяется.

В любом из этих случаев атака «полным перебором» не приведёт к положительному результату: нужных символов просто не окажется в том наборе, на основе которого запускается перебор.

А если запустить атаку по всем 149 186 символам Unicode? Боюсь, в этом случае не помогут даже условно бесконечные вычислительные ресурсы: пароль даже из 6 символов, хотя бы один из которых выбивается из стандартного ряда, потребует $149\,186^6$ операций, что приблизительно составляет 11e30, или 11 нониллионов (плюс-минус несколько сотен тысяч октиллионов). Такое количество паролей обработать в разумные сроки не представляется возможным.

А действительно ли в пароле может оказаться любой из 149 186 символов стандарта Unicode? Здесь тоже ответ — отрицательный. Ряд специальных символов (например, перевод строки) не может использоваться в составе паролей в принципе, а ряд приложений и вовсе ограничивает пароли символами ASCII. В то же время многие приложения позволяют использовать большую часть из набора символов Unicode, причём для одного и того же формата файла, сохранённого в разных приложениях (а иногда и в разных версиях одного приложения) могут действовать разные ограничения. Как правило, из документации к соответствующему продукту можно заранее узнать возможные наборы символов, из которых может быть составлен пароль для различных форматов файлов. Приведём выдержку из документации[1] к операционной системе Windows 10, пароль к учётным записям которой может быть составлен из символов следующих множеств:

[1]https://learn.microsoft.com/ru-ru/previous-versions/windows/it-pro/windows-10/security/threat-protection/security-policy-settings/password-must-meet-complexity-requirements

– буквы верхнего регистра европейских языков (от A до Z, буквы с диакритическими знаками, греческие и кириллические знаки);

– буквы нижнего регистра европейских языков (от a до z, эсцет, буквы с диакритическими знаками, греческие и кириллические знаки);

– базовые 10 цифр (от 0 до 9);

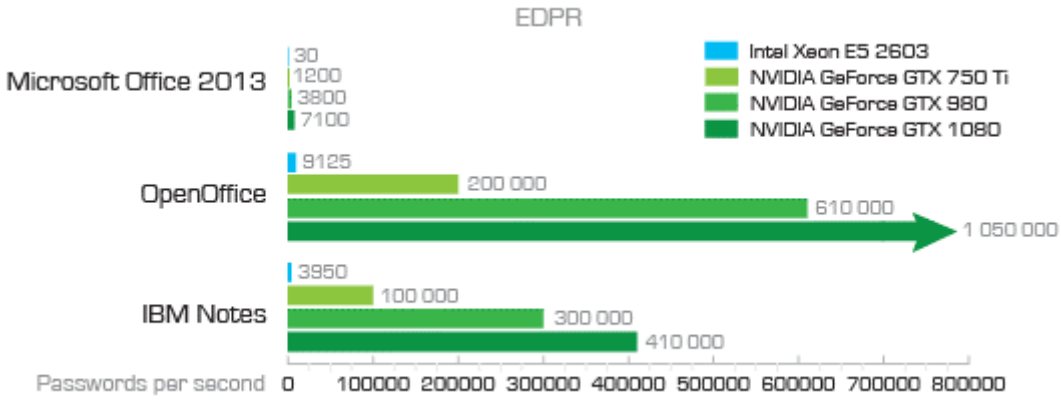
– не буквы и не цифры (специальные символы): (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/) Символы валют, такие как евро или фунт стерлингов, не считаются специальными символами для этого параметра политики;

– любой символ Юникода, классифицируемый как цифра или буква, но не в верхнем или нижнем регистре. Эта группа включает символы Юникода из азиатских языков.

Задание: каков размер множества символов, из которых может состоять пароль к учётной записи Windows 10?

6.1.2. От чего зависит скорость восстановления пароля

Посмотрим на графики:



Как видим, скорость перебора (а, следовательно, и скорость атаки) в основном зависит от двух факторов: криптографической стойкости конкретного формата (в первом приближении — число операций, необходимое для проверки пароля) и скорости аппаратного обеспечения. Однако есть и ещё один фактор, определяющий скорость атаки. Это — используемое для перебора программное обеспечение. В разных продуктах скорость атаки на тот или иной формат может отличаться в разы, а в некоторых случаях (возможность или невозможность

использования аппаратного ускорения) — на порядке. В наших тестах мы пользуемся продуктом Elcomsoft Distributed Password Recovery собственной разработки.

6.1.3. Влияние формата данных на скорость перебора

Что же касается формата данных, то значение имеет не только формат файла, но даже версия приложения, в которой этот файл был сохранён. Сравним, к примеру, стойкость шифрования резервных копий устройств под управлением iOS.

- iOS 9 (CPU): 2,400 паролей в секунду (Intel i5);
- iOS 9 (GPU): 150,000 паролей в секунду (NVIDIA GTX 1080);
- iOS 10.0 (CPU): 6,000,000 паролей в секунду (Intel i5);
- iOS 10.2+ (CPU): 0.05 паролей в секунду (или 5-6 в минуту) (Intel i5).

В 2016 году мы обнаружили ошибку в алгоритме шифрования резервных копий, созданных устройствами под управлением iOS 10. Допущенная разработчиками Apple позволила перебирать пароли со скоростью порядка шести миллионов паролей в секунду силами только центрального процессора, без помощи со стороны аппаратного ускорителя. После того, как мы опубликовали информацию об ошибке, Apple быстро исправили уязвимость, а в iOS 10.2 настолько ужесточили требования к безопасности, что скорость перебора паролей снизилась до 5-6 паролей в минуту (на CPU) или единиц паролей в секунду с использованием GPU. Таким образом, метод полного перебора полностью потерял актуальность, если речь идёт о паролях длиннее 2-3 символов.

Другой пример. Разработчики Microsoft постепенно усиливают стойкость защиты файлов, сохраняемых новыми версиями Microsoft Office: если файлы, сохраняемые Office 97-2000, можно было вскрыть практически моментально, то для уже в версии Office 2010 защита стала куда более стойкой, а документы Office 2013 и вовсе требуют кропотливой работы. В то же время пароли к документам OpenOffice можно перебирать со скоростью порядка миллиона паролей в секунду (на GPU).

	6 знаков, нижний регистр	**6 букв+цифр, оба регистра**	**7 знаков, нижний регистр**	**7 букв+цифр, оба регистра**	**8 знаков, нижний регистр**	**8 букв+цифр, оба регистра**
MS Office 2013, CPU	119 дней	60 лет	8,5 лет	3 700 лет	220 лет	вечность
MS Office 2013, GPU	0,5 дня	3 месяца	2 недели	16 лет	1 год	975 лет
RAR5, CPU	56 дней	28 лет	4 года	1 744 лет	103 года	вечность
RAR5, GPU	2 часа	26 дней	4 дня	4.4 лет	3 месяца	273 года
BitLocker, CPU	5 лет	900 лет	127 лет	вечность	3 300 лет	вечность
BitLocker, GPU	4 дня	2 года	3,6 месяца	130 лет	7,7 лет	вечность

Такая скорость означает, что если пароль, состоящий из 6 букв одного регистра, можно восстановить методом полного перебора за полдня, то пароль из 6 букв (в обоих регистрах) и цифр уже потребует 3 месяцев работы. Для более сложных паролей «умные» атаки и использование графических ускорителей являются обязательными условиями. Для взлома длинных и сложных паролей рекомендуются распределённые атаки.

Если же в пароле попадаются специальные символы или символы Unicode, то время подбора пароля превысит любые разумные сроки. Вы можете убедиться в этом, попробовав пароли разной длины и сложности:

Password Meter — A visual assessment of password strengths and weaknesses (uic.edu)[2]

И последняя небольшая иллюстрация — пароль, состоящий из одного-единственного символа.

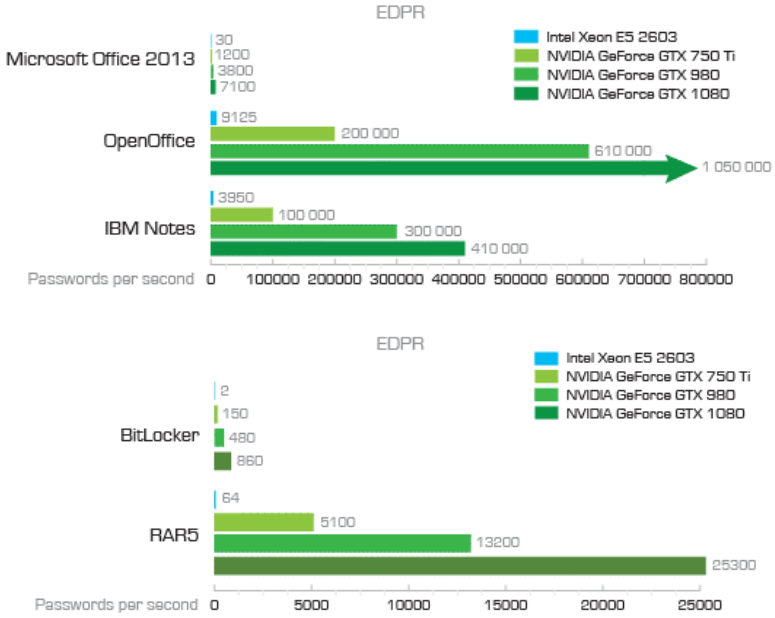
- только цифры: 10 возможных вариантов;
- буквы латиницы в одном регистре: 26 вариантов;
- буквы латиницы в одном регистре + цифры: 36 вариантов;
- буквы латиницы в обоих регистрах + цифры: 62 варианта;
- плюс специальные символы: 95 вариантов.

Для того, чтобы вычислить число вариантов, возможных для пароля заданной длины и сложности, число возможных для использования символов возводится в степень длины пароля. К примеру, для цифрового пароля, состоящего из двух знаков, значение будет $10^2 = 100$ вариантов. Пароль, состоящий из 6 символов латинского алфавита в единственном регистре, будет иметь $26^6 = 308\ 915\ 776$ возможных комбинаций.

6.2. «Умные» атаки

Общее число паролей, которое необходимо проверить в процессе атаки, зависит как от длины и сложности самого пароля, так и от криптографической стойкости конкретного формата данных, определяющей скорость перебора на заданном оборудовании. Криптографическая стойкость в современных приложениях может отличаться на несколько порядков:

[2]https://www.uic.edu/apps/strong-password/



Как видно из графиков, при использовании одинаковой аппаратной конфигурации скорость перебора самого стойкого формата на графике на три порядка (в тысячу раз!) ниже, чем скорость перебора паролей менее стойких. К примеру, скорость перебора паролей к зашифрованным документам Microsoft Office 2013 порядка 7 000 паролей в секунду при условии использования аппаратного ускорителя. 7 000 паролей в секунду — это много или мало? Попробуем разобраться.

Воспользовавшись услугами одного из калькуляторов стойкости паролей[3], рассчитаем число возможных комбинаций у паролей различной длины и сложности. Простейший пароль, составленный из 6 букв нижнего регистра (только латиница), потребует перебора 309 миллионов комбинаций. На видеокарте NVIDIA GTX 1080 можно перебирать такие пароли со скоростью 7 100 паролей в секунду для формата Microsoft Office 2013; соответственно, восстановление такого пароля займёт максимум 12 часов. Однако даже такой простой пароль, если в нём будет 8 символов, состоит из 2,8 триллионов возможных комбинаций, перебор которых займёт 12,5 лет.

Таким образом, получаем следующие реальные скорости атак:

	В секунду	**В час**	**За сутки**
MS Office 2013	7 100	25 560 000	613 440 000
Какой пароль можно восстановить	2-3 символа	4 символа (буквы и цифры)	5 символов (буквы и цифры) (с трудом)

[3]https://www.uic.edu/apps/strong-password/

Время, потребное на восстановление того или иного пароля, зависит не только от длины и сложности пароля и мощности аппаратного обеспечения, но и от того, насколько криптографически стойким является тот или иной формат.

Разумеется, никто не станет тратить месяцы и годы на полный перебор всего пространства паролей. Вместо этого возможное пространство паролей ограничивают тем или иным образом — например, используя список уже известных паролей пользователя или список из 10 000 самых распространённых паролей. В ряде случаем используются обычные словари.

6.2.1. Шаблоны и маски

Использование масок (шаблонов с подстановками символов) позволяет значительно сократить размер множества паролей, на которые будет проводиться атака. Однако маски можно применять лишь тогда, когда известна хотя бы минимальная информация о пароле. Например, предположим, что некий пароль начинается с набора символов «MoiParol», за которым следуют три цифры. При использовании метода полного перебора программе придётся проверить огромное количество комбинаций:

$$(26 + 26 + 10)^{10} = 839\ 299\ 365\ 868\ 340\ 224$$

Использование же шаблона «MoiParol???», где на место вопросительных знаков будут подставлены символы из набора «1234567890», сократит число возможных комбинаций до тысячи, что позволит восстановить пароль за несколько секунд.

6.2.2. Атака по словарю

Атака по словарю считается одной из наиболее эффективных в силу их лучшей запоминаемости. Часто используются имена и породы домашних животных, даты рождения; часто в качестве дополнения к паролю добавляются телефонные номера или две-четыре цифры, обозначающие год. Какой бы низкой ни была скорость перебора, проверка всех английских или русских слов из словаря не займёт много времени. В то же время пароли, состоящие из единственного слова, встречаются редко. Чаще всего используются комбинации слов с одним или несколькими дополнениями, которые призваны сделать пароль более безопасным.

Существует разница между понятиями «словарь» и «список слов». Даже простые пароли не всегда являются словами из орфографического словаря; например, часто используются такие комбинации, как «qwerty», сокращения (в качестве примера приведём получившую скандальную известность аббревиатуру «maga» из пароля Дональда Трампа). В программы для взлома паролей обычно входит несколько словарей и списков слов. В процессе атаки допустимо использовать собственный словарь или список слов, в том числе публично доступных.

Обратите внимание: словари, использующиеся в Elcomsoft Distributed Password Recovery, должны быть сохранены в виде текстовых файлов в формате Unicode LE (little-endian). В каждой строке файла должно содержаться ровно одно слово; пробелы до и после слов не допускаются. Все слова будут проверяться программой в точности в том виде, в котором они присутствуют в словаре, включая заглавные буквы и встречающиеся знаки препинания. Подробнее о том, в каком формате сохраняются и по каким принципам составляются словари – в разделе «Словари».

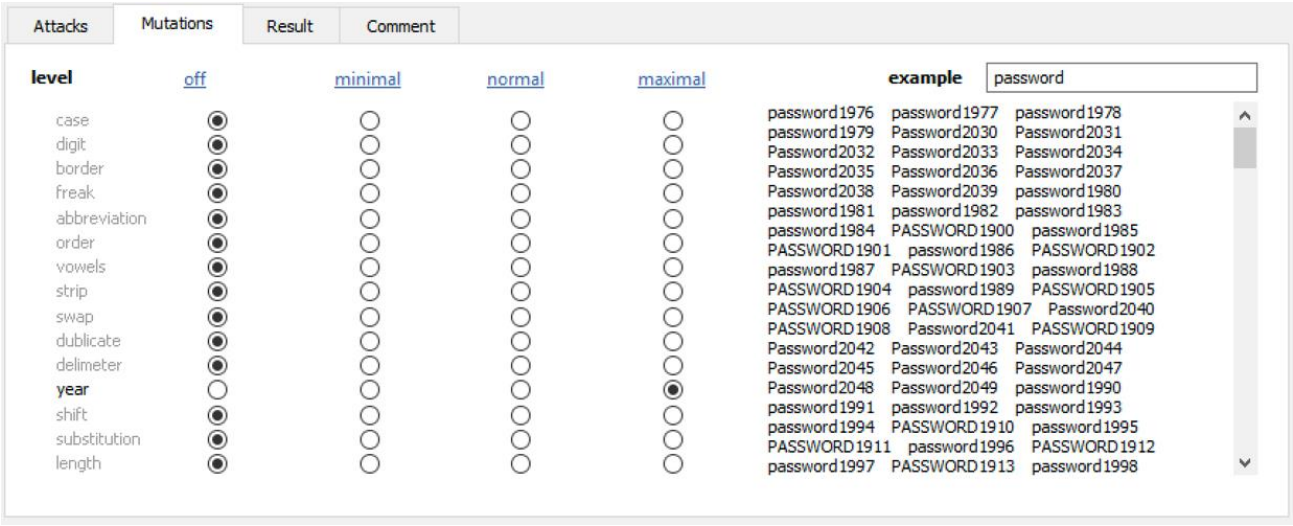
6.2.3. Мутации

Слово «password» — нестойкий, хотя и достаточно популярный, пароль. Слово «Password» — незначительно более стойкий пароль. Ещё более стойким будет вариация «Password1», и ещё более стойкими – варианты «pa$$w0rd» или «Password2020».

Многие пользователи используют эти и аналогичные комбинации, изменяя некое корневое слово определённым образом, заменяя часть символов по определённым правилам, добавляя число или дату в конце, вставляя разделители в середине, модифицируя регистр символов и используя другие несложные и лёгкие для запоминания модификации. В результате довольно эффективным решением будет использование небольшого списка слов в разных вариантах, применяя различные мутации ко всем перечисленным в нём паролям. В Elcomsoft Distributed Password Recovery собраны мутации, которые чаще всего используются в различных группах пользователей.

Как подключить мутации и когда их имеет смысл использовать? Мутации – один из наиболее эффективных механизмов расширения словарных атак, позволяющий использовать различные вариации слов из словаря в автоматическом режиме. В процессе настройки атаки по словарю можно настроить самые разные трансформации (мутации) слов из словаря. Например, из слова "password" в автоматическом режиме получаются такие варианты Password, password1, Password1, password1967 или pa$$w0rd. Какие именно варианты будут опробованы, зависит от настроек мутаций.

Вот так, например, выглядят возможные варианты паролей при включении всего одной мутации "year", которая добавляет четырёхзначное число (год) в конец слова:



Разумеется, единственной мутацией ограничиваться необязательно: мы рекомендуем использовать словарные атаки с мутациями **case**, **digit** и **year** одновременно. Для стандартных словарей мы рекомендуем использовать эти мутации в минимальной настройке ("minimal" на скриншоте). При этом силу и количество мутаций можно варьировать в зависимости как от размера словаря (среднего размера словарь имеет порядка 10 000 вхождений), так и от стойкости конкретного файла или формата, выраженной в скорости перебора на имеющемся оборудовании. Так, для небольшого словаря, состоящего из нескольких десятков повторяющихся элементов, вычлененных из известных паролей пользователя, можно включить более сильные мутации или

использовать большее их количество. Для крупных словарей рекомендуем ограничиться минимальными настройками.

6.2.4. Гибридные атаки

‘maga2020!’ — пароль Дональда Трампа, получивший всемирную известность. Этот и подобные ему пароли довольно легко подобрать, используя гибридную атаку.

Важно: данный тип «умных» атак используется для того, чтобы подобрать пароль, составленный по сложному шаблону. Сам шаблон составляется на основе известных паролей пользователя; таким образом, гибридные атаки слабо применимы для «холодных» атак.

Помимо обычных мутаций, пользователи могут использовать и более сложные модификации слов. Если в процессе атаки выявляется закономерность, по которой составлены пароли пользователя, то эту закономерность можно закодировать при помощи особого языка (синтаксис John the Ripper). В EDPR этот процесс достаточно прост благодаря визуальному редактору правил в окне настроек атаки. Вот краткая и неполная выжимка того, какие правила можно использовать:

{ – Ротация: password → asswordp

c – Заглавные буквы: password → Password

d – Дублирование слова: password → passwordpassword

q – Дублирование символов: password → ppaasssswwoorrdd

r – Обратный порядок: password → drowssap

V – Большие согласные: password → PaSSWoRD

yN – Дублировать первые N знаков

$X – Добавить символ X в конец слова

^X – Вставить символ X в начало слова

@X – Удалить все символы X из слова

!X – Не пробовать пароль, если в нём содержится символ X

/X – Не пробовать пароль, если в нём НЕ содержится символа X

Данный инструмент позволяет создавать исключительно гибкие атаки, но работает лишь в том случае, если обнаружена корректная закономерность, по которой пользователь создаёт свои пароли.

7. Человеческий фактор

В современных условиях подавляющее большинство пользователей для защиты разных файлов и типов данных использует одни и те же или очень похожие пароли. Это связано с необходимостью запоминать пароли к нескольким десяткам учётных записей, что для многих пользователей является непосильной задачей. В то же время использование разных паролей, как правило, означает лишь то, что эти пароли хранятся во внешнем хранилище – базе данных программы для управления паролями, веб-браузере или в облаке.

В результате в процессе расследования имеет смысл сместить вектор атаки на зашифрованные данные и защищённые паролем ресурсы, потратив время на поиск и извлечение существующих паролей пользователя вместо попыток увеличить вычислительную мощь атак методом перебора.

В качестве тезиса примем следующие утверждения:

1. Обычный пользовать может использовать несколько десятков учётных записей.
2. Пароли от множества разных учётных записей либо совпадают, либо в том или ином виде сохраняются на компьютере или в облаке.
3. Число уникальных паролей всегда меньше количества защищаемых паролями данных.

Вооружившись вышеуказанными тезисами, сделаем следующие предположения:

1. Существует возможность узнать (извлечь и расшифровать) сохранённые пользователем пароли.
2. Один из извлечённых таким образом паролей (или его простая модификация) подойдёт для расшифровки файлов, лобовая атака на защиту которых будет чрезвычайно ресурсоёмкой.

Согласно нашим исследованиям, порядка 60% пользователей использует набор из одних и тех же паролей для защиты разных ресурсов и типов данных. Если же считать и тех пользователей, которые варьируют свои пароли в минимальных пределах (например, используя вариации разряда password <> Password <> Password1 <> password1967), то их число достигает 70%.

Используя знания о существующих паролях пользователя, эксперт получает возможность вскрыть до 70% паролей, защищающих файлы и документы, защищённые стойким шифрованием. Если вспомнить о том, что скорость перебора паролей к документам в формате Microsoft Office 2013 – всего 7 000 паролей в секунду даже с использованием графического ускорителя, то важность такого подхода станет очевидной.

7.1. Использование утечек паролей

Многие пользователи используют одни и те же небезопасные пароли в силу их простоты и лёгкости в запоминании. Эти пароли используются многократно совершенно разными пользователями. Классический пример – пароль “Password1”, в точности отвечающий политике безопасности «минимум 8 символов, как минимум одна заглавная буква и как минимум одна цифра». Подобных паролей – множество; имеет смысл использовать такие пароли в качестве словаря.

Как узнать, какие пароли пользуются популярностью среди пользователей? На этот вопрос существует точный ответ: достаточно проанализировать массовые утечки паролей из таких известных сервисов, как LinkedIn, eBay, Twitter, Dropbox и некоторых других. В результате взлома этих сервисов становились известными сотни миллионов паролей. Исследователь безопасности Mark Burnett (https://xa.to/[4]) собрал все известные утечки воедино и обработал данные, отсортировав все утёкшие пароли по популярности и отфильтровав дубликаты. В

[4]https://xa.to/

результате получился список из 10,000 наиболее распространённых паролей. Первоисточник доступен по ссылке: https://xa.to/top10k [5]

Анализ паролей из утечек позволил обнаружить закономерности в поведении англоязычных пользователей.

- 0,5% пользователей используют слово password в качестве пароля;
- 0,4% пользователей в качестве пароля используют последовательности password или 123456;
- 0,9% используют password, 123456 или 12345678;
- 1,6% используют пароль из десятки самых распространённых (top-10);
- 4,4% используют пароль из первой сотни (top-100);
- 9,7% используют пароль из top-500;
- 13,2% используют из top-1 000;
- 30% используют из top-10 000.

Ещё одна закономерность заключается в том, что увеличение размера словаря с 10,000 до 10 миллионов паролей (https://xa.to/10m[6]) не даёт заметного прироста эффективности атак и не имеет смысла ввиду тысячекратно увеличивающегося времени перебора. Соответственно, использование компактного словаря из 10,000 «утёкших» паролей с 30% вероятностью успеха является более эффективным использованием вычислительных ресурсов.

Используя список из 10 000 утёкших паролей, сместим вектор атаки на зашифрованные данные и защищённые паролем ресурсы. Вместо бесконечного увеличения вычислительной мощности системы, на которой производится перебор паролей, можно подключить словарь из 10,000 самых популярных паролей и провести быструю атаку по словарю. Даже на самых стойких форматах на системе, оборудованной графическим ускорителем, время, потраченное на такую атаку, составит считанные секунды.

7.2. Практическая реализация атаки

Для проведения атаки используйте словарь, составленный из 10 000 самых популярных паролей.

По следующей ссылке доступно множество разнообразных словарей, включая словари, составленные из паролей, популярных в странах, в которых не говорят на английском языке:

https://github.com/danielmiessler/SecLists/tree/master/Passwords [7]

Прямая ссылка на скачивание словаря top-10 000:

https://github.com/danielmiessler/SecLists/blob/master/Passwords/darkweb2017-top10000.txt[8]

[5]https://xa.to/top10k
[6]https://xa.to/10m

[7]https://github.com/danielmiessler/SecLists/tree/master/Passwords
[8]https://github.com/danielmiessler/SecLists/blob/master/Passwords/darkweb2017-top10000.txt

Скачать файл, в котором содержатся 10 миллионов паролей, можно по ссылке из оригинальной статьи Марка Бёрнетта:

https://xa.to/10m

Обратите внимание: в файле с 10 миллионами паролей также содержатся другие данные. Вам потребуется применить фильтр для того, чтобы создать на его основе пригодный к использованию словарь.

Атака по словарю, составленному из самых распространённых паролей, показана на примере Elcomsoft Distributed Password Recovery. Последовательность атак состоит из единственного шага, который необходимо настроить следующим образом.

– используйте список top-10 000 (в нашем примере — файл “password-list.txt”) в качестве словаря. Обратите внимание, все мутации выключены. Словарь должен быть сохранён в формате Unicode (Little Endian).

Для большинства форматов, за исключением самых стойких, этот этап будет отработан практически мгновенно – за считанные секунды. У среднестатистического англоязычного пользователя с помощью, приведённой выше последовательности, раскрывается до 30% паролей.

8. Типичные сценарии

В этом разделе описываются возможные последовательности действий в различных сценариях.

8.1. Компьютер разблокирован, есть доступ к пользовательской сессии

В этом случае имеет смысл провести анализ авторизованной пользовательской сессии на месте. Для этого рекомендуем использовать следующий набор инструментов:

– Elcomsoft Encrypted Disk Hunter[9]: утилита командной строки для обнаружения зашифрованных дисков.

– Elcomsoft Forensic Disk Decryptor[10]:инструмент для снятия образа оперативной памяти и поиска ключей шифрования к смонтированным на компьютере зашифрованным дискам.

– Elcomsoft Quick Triage[11]: инструмент для извлечения паролей пользователя из веб-браузеров и почтовых клиентов.

В первую очередь рекомендуем запустить утилиту для поиска зашифрованных дисков. Если таковые обнаружены, воспользуйтесь утилитой Elcomsoft Forensic Disk Decryptor, посредством которой сохраните образ оперативной памяти компьютера (рекомендуем сохранять файл с содержимым оперативной памяти на внешний накопитель).

Независимо от того, были ли обнаружены зашифрованные диски, воспользуйтесь утилитой Elcomsoft Quick Triage для того, чтобы извлечь из компьютера список учётных записей и паролей пользователя, сохранённых в веб-браузере. В дальнейшем вы сможете использовать полученные пароли как для прямого доступа к защищённым ими ресурсам, так и для того, чтобы создать словарь для атаки на зашифрованные данные того же пользователя.

---

[9] https://blog.elcomsoft.com/2020/07/live-system-analysis-discovering-encrypted-disk-volumes/
[10] https://www.elcomsoft.ru/efdd.html
[11] https://www.elcomsoft.ru/eqt.html

8.2. Компьютер заблокирован. Диск зашифрован

Если компьютер оборудован портом FireWire, вы можете воспользоваться соответствующей уязвимостью для того, чтобы снять образ оперативной памяти с использованием сторонних инструментов. Из этого образа можно извлечь ключи шифрования дисков утилитой Elcomsoft Forensic Disk Decryptor.

Если это невозможно, вы можете использовать для восстановления доступа к системе учётную запись Active Directory. Для дисков BitLocker в Active Directory может сохраняться ключ восстановления доступа, который возможно извлечь непосредственно из базы AD (ntds.dit).

8.3. Компьютер выключен. Диск зашифрован

В этом сценарии рекомендуем воспользоваться утилитой Elcomsoft System Recovery (инструкции[12]). Обратите внимание: для того, чтобы воспользоваться утилитой, необходимо предварительно создать (на лабораторном компьютере) загрузочный накопитель, с которого затем загружается исследуемый компьютер.

После загрузки компьютера в среду Elcomsoft System Recovery воспользуйтесь функцией поиска зашифрованных дисков. Если таковые будут найдены, извлеките метаданные шифрования для последующей атаки в Elcomsoft Distributed Password Recovery.

Обратите внимание: для загрузочных дисков, зашифрованных BitLocker, парольная атака, как правило, невозможна: такие диски зашифрованы ключом, который хранится в модуле безопасности TPM 2.0. Возможным действиях в отношении TPM посвящён отдельный раздел руководства.

8.4. Файл с паролем. Владелец неизвестен

Одна из самых сложных ситуаций – та, в которой есть один или несколько зашифрованных файлов, о владельце которых неизвестно ничего. В этом случае не удастся использовать какие-либо данные о подозреваемом для сокращения множества паролей для перебора. В то же время именно для этого случая написано множество руководств, позволяющих как оценить сложность задачи, так и использовать корректный набор атак в правильном порядке.

«Холодной» атакой назовём попытку восстановить доступ к зашифрованным данным и/или подобрать пароль к зашифрованным данным в условиях, когда доступны только сами файлы с данными (либо только метаданные шифрования из заголовков файлов). В рассматриваемой ситуации недоступна никакая информация о владельце файлов, об используемых им паролях или учётных записях. Более того, в ряде случаев неизвестно даже, принадлежит ли предоставленный эксперту набор файлов одному и тому же человеку. Такая ситуация — одна из наиболее тяжёлых в работе эксперта, и в то же время — одна из самых типичных.

В общем виде действия эксперта в этом случае выглядят следующим образом:

[12] https://blog.elcomsoft.ru/2020/11/elcomsoft-system-recovery-zagruzochnyj-nakopitel-dlya-issledovaniya-kompyuterov/

1. Определить файлы, для которых могут существовать уязвимости (см. раздел «**Когда перебор не нужен»**). Такие файлы могут быть расшифрованы мгновенно или очень быстро, однако далеко не всегда при этом восстанавливается оригинальный пароль.

2. Провести оценку скорости атаки для каждого файла.

3. В первую очередь атаковать наименее стойкие файлы. Если файлов несколько, выстроить очередь атаки таким образом, чтобы наименее стойкие файлы располагались вверху очереди.

4. В зависимости от скорости атаки на имеющемся оборудовании и доступного для проведения атаки времени выстроить цепочку атак.

В цепочку атак могут входить следующие действия:

1. Атака по словарю, составленному из глобальных утечек паролей (словарь top-10000 в Elcomsoft Distributed Password Recovery).

2. Перебор цифровых паролей длиной от 1 до 8 цифр; максимальная длина цифровых паролей напрямую зависит от стойкости формата. Так, для нестойких форматов можно запустить перебор паролей длиной в 1-8 цифр, а для самых стойких – от 1 до 4 цифр.

3. Словарная атака с использованием словаря английского языка с мутациями*.

4. Словарная атака с использованием словаря русского языка (как в варианте с кириллицей, так и в различных вариантах транслитерации) с мутациями*.

5. Если после предыдущих атак пароль не найден, то в оставшееся время запускается атака методом полного перебора.

*В список мутаций, которые имеет смысл включать при атаке по умолчанию, входят следующие (активировать одновременно):

1. Мутация «год» в среднем режиме.
2. Мутация «заглавные буквы» в среднем режиме.

Рассмотрим каждый шаг подробно.

Оценка скорости атаки

Первый и необходимый шаг – оценка скорости атаки. Если файлов – несколько, то в первую очередь имеет смысл настроить атаку на файлы в наименее стойких форматах. Скорость атаки зависит от нескольких параметров:

1. Формат файла.
2. Используемое для атаки программное обеспечение.
3. Используемой для атаки аппаратное обеспечение.

Формат файла оказывает сильное влияние на скорость перебора. Так, на одном и том же оборудовании документ с расширением .doc может показать скорость атаки в 100,000 паролей в секунду, а документ с расширением .docx – уже только 150 паролей в секунду. Несмотря на то, что цифры в данном примере условные, они отражают реальное соотношение скоростей между этими двумя форматами.

В качестве программного обеспечения принимаем Elcomsoft Distributed Password Recovery – за исключением, однако, тех случаев, когда пароль с файла или документа можно снять мгновенно или очень быстро другими способами (см. раздел «**Когда перебор не нужен»**).

Наконец, в качестве аппаратного обеспечения могут выступать как отдельные компьютеры, так и компьютеры, объединённые через локальную или глобальную сеть, а также виртуальные инстансы в облачных сервисах Amazon или Microsoft Azure. В компьютерах, в свою очередь, большую важность имеет установленный графический ускоритель или ускорители; производительность центрального процессора отходит на второй план.

Скорость атаки для различных форматов в разных аппаратных конфигурациях публикуется на странице Elcomsoft Distributed Password Recovery (раздел «**Графики производительности»**). Кроме того, сравнительную скорость перебора паролей для ряда распространённых форматов файлов можно узнать из следующей таблицы:

Название формата	**Паролей в секунду / NVIDIA GTX 1080**
MD5 (single hash)	9 800 000 000
NTLM (MD4)	9 100 000 000
Domain Cached Credentials Windows 2000-2003 (2xMD4)	7 310 000 000
SHA-1 (single hash)	5 450 000 000
MD5 (many hashes)	2 820 000 000
SHA-1 (many hashes)	2 503 203 112
SHA-256	2 211 000 000
Adobe Acrobat9 PDF (SHA256+AES256)	2 050 000 000
LM (DES-56)	1 070 000 000
SHA-512	851 500 000
IKE PSK (HMAC(sha1))	200 587 000
MS SQL Server 2000	18 300 000
MS SQL Server 2005	17 650 000
SQL CE (sdf) v4.0 platform default (SHA256+AES128)	17 300 000
SQL CE (sdf) v3.0 (MD5+RC4)	17 200 000
SQL CE (sdf) v3.5 (SHA1+AES128)	17 100 000
MS SQL Server 2014	17 047 000
SQL CE (sdf) v4.0 engine default (SHA512+AES256)	16 700 000
PFX/P12 certificates (without strong enc-tion)(pbkdf2_sha1(1))	7 340 000
PGP secret key (MD5) (simple1)	3 280 000
PFX/P12 certificates (with strong encryption)(pbkdf2_sha1(?))	1 570 000
OpenOffice (pbkdf2_sha1(1024) + AES-256)	1 150 210
Keychain	1 130 000
IBM Notes (pbkdf2_sha1(5000) + AES128)	567 000
PGPDisk 10.3.0 (.pgd) (CAST5)	457 000
WPA/WPA2 PSK (pbkdf2_sha1(8192) + HMAC(sha1))	334 000
IBM Notes (pbkdf2_sha1(5000) + AES256)	289 000
PGP secret key (MD5) (simple2)	284 000
Domain Cached Credentials Vista+ (2xMD4 + pbkdf2_sha1(10240))	282 000
PGPDisk 10.3.0 (.pgd) (AES256)	273 000
PGPDisk 10.3.0 (.pgd) (EME2-AES)	273 000
LastPass	215 000
IBM Notes (pbkdf2_sha256(5000) + AES128)	205 000

ZIP (AES)	203 000
Apple iWork 09	150 000
Dashlane	139 000
iOS 4.x-9.x, 10.1 iTunes Backup	139 000
PGP WDE	134 000
PGPDisk 10.3.0 (.pgd) (Twofish)	120 000
Keepass	119 000
1Password	108 000
Hancell 2010/2014	108 000
OpenOffice (pbkdf2_sha1(1024) + Blowfish)	95 300
Microsoft Office 2007	84 400
IBM Notes (pbkdf2_sha512(5000) + AES256)	72 300
BlackBerry backup	50 700
Microsoft Office 2010	48 500
GnuPG 2.0 (secring.gpg)	30 800
PGP secret key (SHA1) (IteratedSalted1)	30 800
RAR 5	25 300
PGP zip archive (.pgp)	24 300
Apple iWork 2014	22 900
PGP secret key (SHA1) (IteratedSalted2)	18 600
RAR 3-4	17 100
OpenDocument (pbkdf2_sha1(100000) + AES256)	13 400
FileVault	9 800
OS X Password	9 650
FileVault_APFS	8 500
Encypted DMG (AES-128)	7 390
Microsoft Office 2013/2016	7 300
Bitcoin	5 920
TrueCrypt: SystemDisk AES_RIPEMD160	4 960
7Zip	4 490
TrueCrypt: SimpleDisk AES_RIPEMD160	3 010
TrueCrypt: Container AES_RIPEMD160	2 630
BitLocker	875
TrueCrypt: SystemDisk Unkn_Unkn	756
TrueCrypt: Container Unkn_Unkn	668
TrueCrypt: SimpleDisk Unkn_Unkn	667
iOS 10.2+ iTunes Backup	95

Очередь задач и последовательность атак

В понятие «очереди задач» входит список файлов, на которые будет производиться атака. «Очередь атак» включает настроенные пользователем атаки, которые будут последовательно использоваться программой, чтобы восстановить пароль для конкретного файла. Эти термины можно изобразить следующим образом:

```
Сценарий 1:
Файл 1
------ Атака 1
------ Атака 2
------ Атака 3
Файл 2
------ Атака 1
------ Атака 2
------ Атака 3
Файл 3
------ Атака 1
------ Атака 2
------ Атака 3
```

В то же время вы можете выстроить очередь задач и таким образом:

```
Сценарий 2:
Файл 1
------ Атака 1
Файл 2
------ Атака 1
Файл 3
------ Атака 1
Файл 1
------ Атака 2
Файл 2
------ Атака 2
Файл 3
------ Атака 2
Файл 1
------ Атака 3
Файл 2
------ Атака 3
Файл 3
------ Атака 3
```

Программа позволяет как настроить атаки для каждого файла, так и настроить последовательность атак для всех добавленных в очередь файлов. Пример очереди задач может выглядеть следующим образом:

```
Newdocument.docx
------ Атака по словарю top-10000
------ Атака на цифровые пароли (1-6 знаков)
------ Словарная атака с мутациями по словарю English.udic
------ Словарная атака с мутациями по словарю Translit.udic
------ Словарная атака с мутациями по словарю Russian.udic
------ Полный перебор (полный набор символов; 1-8 знаков)
Expenses.xlsx
------ Атака по словарю top-10000
------ Атака на цифровые пароли (1-6 знаков)
------ Словарная атака с мутациями по словарю English.udic
------ Словарная атака с мутациями по словарю Translit.udic
------ Словарная атака с мутациями по словарю Russian.udic
------ Полный перебор (полный набор символов; 1-8 знаков)
```

В то же время вы можете выстроить очередь и по второму сценарию.

В Elcomsoft Distributed Password Recovery добавленные в очередь задач файлы обрабатываются последовательно. Это означает, что переход на следующий файл произойдёт в одном из двух случаев: если пароль был найден в процессе какой-либо атаки, либо продукт завершил все атаки из очереди для данного файла. Именно поэтому так важно заранее оценить скорость перебора паролей для каждого из обрабатываемых файлов, расположив их в порядке возрастания стойкости (самые «быстрые» форматы – в начале очереди).

Внимание: в Elcomsoft Distributed Password Recovery отсутствует возможность задать ограничение по длительности атак. Соответственно, рекомендуем настраивать атаки таким образом, чтобы перебор заданного множества паролей завершался в течение прогнозируемого времени.

В случае, когда пароль был обнаружен для одного из файлов, этот пароль добавляется в кэш, пароли из которого автоматически проверяются перед началом атаки на все последующие файлы из очереди задач. Если для защиты всех файлов использовался один и тот же пароль, то время на восстановление пароля будет затрачено только для первого в очереди файла.

8.5. Системный диск доступен для анализа. Что искать и как искать?

Если системный диск доступен для анализа (проводится анализ пользовательской сессии), рекомендуем в первую очередь снять образ оперативной памяти компьютера, после чего – извлечь пароли пользователя.

Проведите следующие действия:

1. Запустить **Elcomsoft Forensic Disk Decryptor** и снять образ оперативной памяти (в лаборатории просканировать образ на предмет ключей к зашифрованным дискам и виртуальным машинам). Требуется административный доступ.

2. Запустить **Elcomsoft Quick Triage** и извлечь сохранённые пароли пользователя. Административные привилегии не требуются.

3. Просканировать компьютер на предмет наличия зашифрованных дисков (см. раздел «**Поиск зашифрованных дисков»**). Требуется административный доступ.

После этого рекомендуем использовать сторонние инструменты для автоматизированного поиска улик.

8.6. Если есть время и возможности: комплексный анализ

При наличии времени и возможности на комплексный анализ цифровых улик рекомендуем провести именно его. Критически важно собрать всю доступную информацию о пользователе – имя, дату рождения, адрес, имена членов семьи и домашних животных, важные даты, девичью фамилию матери. Все эти данные могут быть использованы (и часто используются в реальной практике) в качестве составных частей паролей. На практике это означает составление короткого словаря, состоящего из фамилий, дат и названий, и запуск атак, в которых вхождения из словаря использовались бы как самостоятельно (с максимумом мутаций), так и в атаке, которая комбинирует два слова из словаря (возможно, с разделителем).

При комплексном анализе исследуются все носители информации и все устройства пользователя, которые могут собирать и хранить информацию. Перечислим типы устройств и те возможные данные, которые они могут содержать.

Компьютеры

Рекомендуется исследование как портативных, так и настольных компьютеров. Если загрузочный диск хотя бы одного компьютера не будет зашифрован, то появится возможность подобрать или извлечь из него пароль к учётной записи Windows, который, в свою очередь, может подойти и к другим устройствам. Войдя же в учётную запись, можно извлечь как сохранённые пароли пользователя, так и провести полноценный анализ содержимого диска.

Смартфоны

В современных смартфонах может содержаться огромное количество информации, включая пароли (связка ключей, сторонние утилиты хранения паролей). Доступ к разблокированному iPhone может помочь сбросить пароль от компьютера под управлением macOS или узнать пароль от учётной записи Microsoft, который, в свою очередь, может использоваться для входа в систему (если для этого используется учётная запись Microsoft, а не локальная учётная запись). Подробнее о том, какие данные содержатся в смартфонах и других устройствах экосистемы Apple и как их извлечь, рассказывается в нашем методическом пособии по извлечению данных из устройств Apple.

Приставки

В телеприставках (Android TV, Apple TV) также могут содержаться релевантные данные. Анализ приставок с одной стороны упрощён (на них нельзя установить пароль); с другой стороны, количество и ценность доступных в них данных несравненно ниже в сравнении с тем, что доступно в смартфонах. Подробнее о том, какие данные содержатся в приставках Apple TV и способах их извлечения, рассказывается в нашем методическом пособии по извлечению данных из устройств Apple.

Умные часы

На рынке представлены тысячи моделей умных часов от сотен производителей. Невозможно предсказать, какие именно данные могут содержаться в той или иной модели. Хорошо изучены часы Apple Watch, в которых может содержаться исключительно важная для расследования информация об активности пользователя в интересующий период. Для часов Apple Watch разработаны как способы извлечения данных, так и методы их анализа. Подробнее о том, какие данные содержатся в часах Apple Watch и способах их извлечения, рассказывается в нашем методическом пособии по извлечению данных из устройств Apple.

IoT и устройства умного дома

Голосовые помощники от Apple, Google и Amazon присутствуют во многих домах. Физический анализ таких устройств практического смысла не имеет: практически никакие данные на таких устройствах не хранятся. В то же время большой смысл имеет облачный анализ данных, которые поставляются этими устройствами. В зависимости от производителя из облака можно получить как историю расшифрованных команд пользователя, так и аудиозаписи голосовых команд, включая ложные срабатывания слова-активатора. Обратите внимание: указанные данные будут собираться и храниться и в случае, когда голосовой помощник активируется на смартфоне или умных часах.

Пользователь может самостоятельно настроить политику приватности для голосовых помощников. По умолчанию используются следующие настройки:

Apple Siri, в устройствах HomePod и HomePod mini: аудиозаписи не сохраняются. Пользователь может самостоятельно включить сохранение данных. В iOS 15 появился режим, позволяющий iPhone обрабатывать некоторые запросы к Siri в режиме офлайн. В этом случае данные на сервер не передаются и, соответственно, не сохраняются. Данная возможность доступна для ограниченного набора команд, и поддерживает не все языки, на которых может общаться голосовой помощник.

Google Assistant, в устройствах линейки Nest Hub, а также ряда сторонних производителей: аудиозаписи сохраняются и хранятся в течение неопределённого времени. Пользователь может отключить сохранение данных в настройках. Извлечь можно все команды, включая аудиозаписи.

Amazon Alexa, в устройствах линейки Echo, а также ряда сторонних производителей: аудиозаписи сохраняются и хранятся в течение неопределённого времени. Пользователь может отключить сохранение данных в настройках Alexa. Для скачивания доступны транскрипты команд.

9. Инструментарий: когда и какие инструменты использовать

В состав Elcomsoft Desktop Forensic Bundle входит порядка полутора десятков инструментов, каждый из которых служит своей определённой цели. Для чего нужен Advanced Office Password Recovery, если есть Elcomsoft Distributed Password Recovery? Для чего нужен Advanced Archive Password Recovery, если Distributed Password Recovery способен перебрать пароли в сотни раз быстрее? В каких случаях нужно использовать Forensic Disk Decryptor, а в каких – Elcomsoft System Recovery? В последующих главах об использовании каждого продукта будет подробно рассказано в соответствующем контексте; здесь же мы расскажем о типовых сценариях использования для каждого из входящих в набор продуктов.

9.1. Инструменты для запуска на исследуемом компьютере

Многих проблем с восстановлением доступа к данным можно избежать, если есть возможность запустить программу на компьютере пользователя. В эту группу входят те утилиты, которые необходимо запускать на исследуемом компьютере – как с авторизованной пользовательской сессии, так и без неё.

9.1.1. Elcomsoft System Recovery: загрузочный накопитель

Elcomsoft System Recovery (ESR) состоит из загрузочного накопителя с предварительно настроенной средой Windows PE и самого инструмента System Recovery. В состав дистрибутива входит всё необходимое для создания такого накопителя.

С помощью Elcomsoft System Recovery можно загрузить компьютер пользователя в чистой среде, в которой можно выполнить следующие действия:

– если загрузочный диск не зашифрован: сбросить пароль учётной записи пользователя Windows или попытаться восстановить этот пароль с помощью предварительно настроенных атак, либо извлечь метаданные учётной записи, чтобы запустить перебор на другом ПК в Elcomsoft Distributed Password Recovery;

– если загрузочный диск зашифрован: быстро извлечь заголовок контейнера с метаданными шифрования, после чего запустить перебор на другом ПК в Elcomsoft Distributed Password Recovery;

– если диск зашифрован TPM или USB-ключом, ESR сэкономит время на бесполезную атаку, сразу сообщив об этом.

Другими словами, Elcomsoft System Recovery предназначен для тех ситуаций, когда в наличии – целый компьютер (а не жёсткий диск или его образ). Подробнее о продукте можно прочесть в статье Elcomsoft System Recovery: загрузочный накопитель для исследования компьютеров[13]

9.1.2. Elcomsoft Quick Triage: извлечение сохранённых паролей

Извлечение паролей пользователей из веб-браузеров и почтовых клиентов на компьютерах под управлением Windows. Запускается из-под авторизованной пользовательской сессии на компьютере пользователя либо на компьютере эксперта, если есть образ диска исследуемого компьютера или смонтированный накопитель.

9.1.3. Elcomsoft Forensic Disk Decryptor: работа с зашифрованными дисками или образами дисков

В состав продукта входят компоненты, которые запускается на компьютере пользователя. Требуется авторизованная пользовательская сессия с административными привилегиями. Эти компоненты:

– утилита для снятия образа оперативной памяти с целью последующего поиска ключей шифрования;

– инструмент для извлечения метаданных шифрования с целью последующей организации атаки на пароль шифрования.

Функции анализа образов оперативной памяти и поиска ключей шифрования проводятся в лаборатории.

9.2. Инструменты для запуска на исследуемом компьютере и использования в лаборатории

В эту группу входят инструменты, которые можно запускать как на исследуемом компьютере, так и в лаборатории.

9.2.1. Elcomsoft Forensic Disk Decryptor: работа с зашифрованными дисками или образами дисков

В отличие от ESR, Elcomsoft Forensic Disk Decryptor работает с жёсткими дисками и их образами, если таковые зашифрованы или имеют зашифрованные разделы. Сюда входят такие типы защиты, как VeraCrypt, BitLocker, TrueCrypt и другие зашифрованные контейнеры.

[13] https://blog.elcomsoft.ru/2020/11/elcomsoft-system-recovery-zagruzochnyj-nakopitel-dlya-issledovaniya-kompyuterov/

EFDD может использоваться как на компьютере пользователя, так и эксперта. В состав продукта входит инструмент для снятия образа оперативной памяти, который как раз и предназначен для запуска на компьютере пользователя с авторизованной пользовательской сессией (и административными привилегиями).

Elcomsoft Forensic Disk Decryptor поможет выполнить следующие задачи:

– расшифровать или мгновенно подключить зашифрованные тома с помощью ключей шифрования, извлечённых из файлов подкачки и файлов гибернации;

– то же с известным текстовым паролем;

– то же посредством депонированных ключей (ключей восстановления доступа), извлечённых из Active Directory или облачных учётных записей;

– анализ дампов памяти с целью поиска ключей шифрования с последующим использованием этих ключей для расшифровки или мгновенного монтирования зашифрованных томов;

– извлечение заголовка зашифрованного диска с метаданными шифрования (хэш пароля, количество итераций, алгоритм шифрования, режим шифрования и т. д.) Файл с метаданными можно использовать для запуска перебора паролей на другом ПК в Elcomsoft Distributed Password Recovery.

Входящий в состав продукта инструмент для снятия образа оперативной памяти:

– выгрузка образа ОЗУ исследуемого компьютера. Этот образ можно открыть в Elcomsoft Forensic Disk Decryptor с целью поиска ключей шифрования к зашифрованным дискам, которые были смонтированы на компьютере во время захвата.

Обратите внимание: для максимально успешного поиска ключей необходимо использовать версию инструмента для снятия образа оперативной памяти, совпадающую с версией EFDD. При использовании более старых версий инструмента с новыми версиями EFDD часть функций будет недоступна.

9.3. Инструменты для использования в лаборатории

В эту группу включены инструменты, использующиеся исключительно в лабораторных условиях.

9.3.1. Advanced Archive Password Recovery Professional Edition

Продукт ограниченного применения. Используйте в случаях, когда архив ZIP создан в очень старой версии WinZIP либо зашифрован старой версией алгоритма шифрования (до AES). В этих условиях продукт может расшифровать содержимое архива без перебора.

Не используйте данный продукт для перебора паролей, а также для восстановления паролей или расшифровки любых архивов, за исключением архивов ZIP, зашифрованных старым (до AES) методом шифрования.

9.3.2. Advanced EFS Data Recovery Professional Edition

Расшифровка данных EFS (зашифрованных папок в NTFS).

9.3.3. Advanced IM Password Recovery

Моментальное извлечение паролей из нескольких десятков программ мгновенного обмена сообщениями. Для некоторых программ (например, Skype) вместо извлечения пароля доступен перенос авторизованной пользовательской сессии на компьютер эксперта.

9.3.4. Advanced Mailbox Password Recovery

Продукт ограниченного применения. Используется для моментального извлечения паролей из почтовых приложений (POP3/IMAP/SMTP), а также для перехвата паролей при помощи MITM-атаки (с установкой посредника-прокси).

9.3.5. Advanced Office Password Recovery

Продукт ограниченного применения для расшифровки и разблокировки документов Microsoft Office, сохранённых в старых версиях приложений или современными приложениями в режиме совместимости. Используйте для того, чтобы снять пароли ограничений с документов (например, ограничения на распечатку).

Также используйте в случаях, когда документ или таблица создана в формате приложений Microsoft Office 97/2000 и зашифрованы старой версией алгоритма шифрования с коротким 40-битным ключом. В состав продукта входят таблицы Thunder Tables, позволяющие расшифровать такие документы в течение нескольких секунд (в худшем случае – минут).

Кроме того, используйте продукт для моментального восстановления паролей и снятия защиты с документов в формате приложений Intuit Quicken и QuickBooks, а также Lotus SmartSuite (Lotus Organizer, Lotus WordPro, Lotus 1-2-3, Lotus Approach и Freelance Graphics).

Во всех остальных случаях используйте Distributed Password Recovery.

9.3.6. Advanced PDF Password Recovery

Продукт ограниченного применения. Используйте в случаях, когда файл PDF создан в очень старой версии Adobe Acrobat и зашифрован старой версией алгоритма шифрования с коротким ключом. Также используйте для сброса паролей ограничений (например, ограничения на распечатку), если файл PDF не защищён дополнительно паролем на открытие. Во всех остальных случаях используйте Distributed Password Recovery.

9.3.7. Advanced SQL Password Recovery

Моментальный сброс или смена паролей от баз данных Microsoft SQL.

9.3.8. Elcomsoft Password Digger

Извлечение и расшифровка связки ключей (в них хранятся пароли пользователей) на компьютерах под управлением macOS. Запускается на компьютере эксперта. В справке продукта доступна инструкция, описывающая, каким образом скопировать нужные для работы файлы.

9.3.9. Elcomsoft Wireless Security Auditor

Предназначен для аудита корпоративной политики безопасности. Позволяет выяснить степень защищённости беспроводной сети организации путём запуска атак на пароли к беспроводным точкам доступа. Не предназначен для восстановления паролей и расшифровки данных.

9.3.10. Proactive System Password Recovery

Извлечение ключей Wi-Fi (WEP и WPA-PSK), VPN, RAS, паролей для dial-up, паролей к сетевым ресурсам, соединениям и RDP. Запускается на компьютере эксперта.

9.3.11. Elcomsoft Distributed Password Recovery: универсальный инструмент для перебора паролей

Elcomsoft Distributed Password Recovery предназначен для проведения масштабируемых атак с аппаратным ускорением с поддержкой нескольких сотен форматов данных.

В состав Elcomsoft Distributed Password Recovery входит инструмент под названием Elcomsoft Hash Extractor. Этот инструмент используется для извлечения метаданных шифрования из нескольких форматов файлов, включая офисные документы, базы данных утилит для хранения паролей и, в будущих версиях, архивов. Далее метаданные шифрования используются для перебора паролей в основной программе вместо исходного файла или документа. Смысл такого использования в обеспечении конфиденциальности атак. Атака на анонимный заголовок, в котором содержатся только метаданные шифрования, но не сам документ, выполняется в соответствии с законами о защите данных, что особенно важно при работе с субподрядчиками или использовании удалённых и облачных серверов.

Elcomsoft Hash Extractor используется для:

– извлечения метаданных шифрования из нескольких форматов файлов, включая многочисленные форматы офисных документов, баз данных утилит для хранения паролей, архивов и баз данных для восстановления паролей к учётным записям Windows. Эти значения могут использоваться в EDPR для настройки атак вместо исходного файла или документа. Для криптоконтейнеров и менеджеров паролей использование Hash Extractor обязательно, для документов – опционально;

– актуальный список поддерживаемых форматов – на странице Elcomsoft Distributed Password Recovery[14].

В состав продукта также входит облегчённая версия *Elcomsoft Forensic Disk Decryptor*, которая используется для:

– расшифровки или мгновенного подключения зашифрованных томов с помощью депонированных ключей и восстановленных паролей;

– извлечения метаданных шифрования (хэш пароля, количество итераций, алгоритм шифрования, режим шифрования и т.д.) для запуска атаки в Elcomsoft Distributed Password Recovery.

Elcomsoft Distributed Password Recovery **используется** для:

– проведения атак для восстановления пароля на файл или документ (поддерживается несколько сотен форматов);

[14] https://www.elcomsoft.ru/edpr.html#tab_2

– проведения атак для восстановления пароля на метаданные шифрования, извлечённые с помощью Elcomsoft Hash Extractor, Elcomsoft System Recovery или Elcomsoft Forensic Disk Decryptor.

Elcomsoft Distributed Password Recovery **не используется** для:

– атаки для восстановления пароля непосредственно на зашифрованном томе (BitLocker), образе диска или контейнере (TrueCrypt, VeraCrypt и подобных): необходимо предварительно извлечь метаданные шифрования;

– атаки восстановления пароля непосредственно на базы данных менеджеров паролей. Так же, как и в предыдущем случае, из базы данных необходимо предварительно извлечь метаданные шифрования.

Обратите внимание:

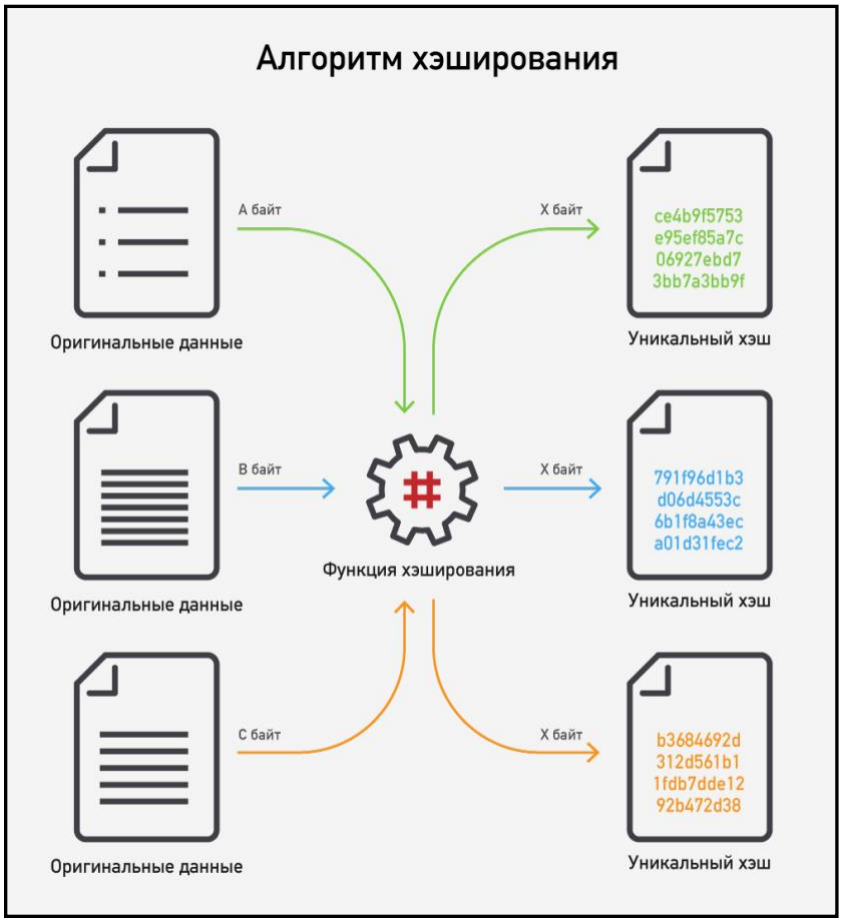
Elcomsoft Distributed Password Recovery может использоваться для восстановления паролей документов (например, документов Word, электронных таблиц Excel и подобных). В качестве исходных данных вы можете использовать либо сами документы, либо только их заголовки, в которых содержатся метаданные шифрования. Для извлечения метаданных шифрования используется утилита Elcomsoft Hash Extractor, входящая в состав продукта.

10. Основные принципы шифрования и хэширования

Пароли используются для защиты документов, баз данных, сжатых архивов, отдельных файлов и дисков целиком, а также учётных записей. За редкими исключениями (например, пароли в веб-браузерах, связке ключей или учётных записях IMAP / POP3), пароли практически никогда не сохраняются — ни в открытом виде, ни в зашифрованном. Вместо этого пароли «хэшируются», а точнее — преобразуются с помощью односторонней математической функции. Результат преобразования, если он выполнен правильно, невозможно обратить, а исходный пароль, соответственно, невозможно «расшифровать».

Шифрование — обратимая двусторонняя операция.

Суть хэширования — в детерминированном одностороннем (необратимом) преобразовании набора данных произвольного размера в массив фиксированной длины.



Хэширование — одностороннее необратимое преобразование данных.

Помимо необратимости преобразования, криптографические алгоритмы хеширования обладают несколькими интересными свойствами, основное из которых — недопустимость так называемых коллизий. Изменение единственного бита в исходном наборе данных выдаст хэш, который не будет даже минимально похож на исходный.

Рассмотрим два хэша:

```
Оригинальный текст: 000000000000
SHA-1: C2311E92660DE47B456E721B0DABC9F857AB48F0

Оригинальный текст: 000000000001
SHA-1: F6A8135A89118200A9CC55D456C4D9A2D319FA29
```

Как легко заметить, изменение единственного бита привело к радикальному изменению всего хэша. Вы можете самостоятельно проверить различные комбинации в онлайновом калькуляторе SHA-1 hash generator.[15]

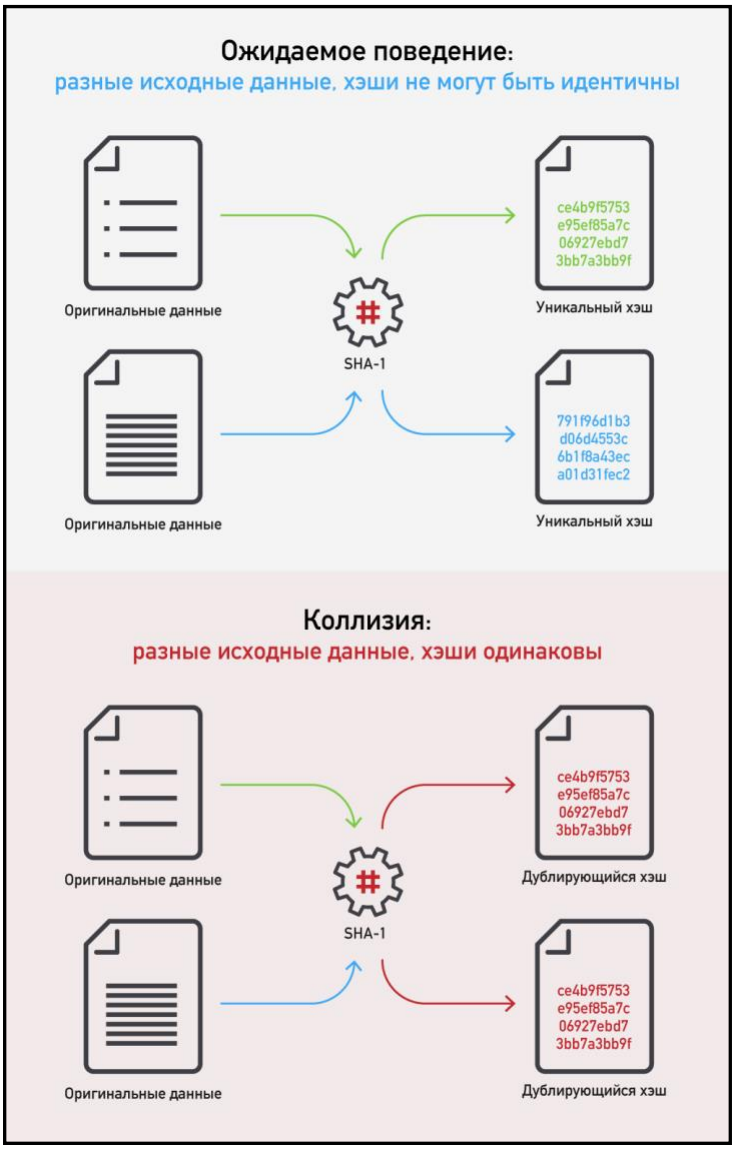
Подводя итог, хэширование — это одностороннее преобразование, которое не может быть обращено (по крайней мере, тогда, когда применяется качественный алгоритм хеширования).

[15] https://passwordsgenerator.net/sha1-hash-generator/

Максимум, который доступен в процессе атаки — сгенерировать так называемую «коллизию», то есть найти другой текст, преобразование которого посредством заданной хеш-функции выдаст совпадение (то есть, такой же хэш, как при использовании оригинального пароля). Современные алгоритмы хеширования спроектированы таким образом, чтобы свести вероятность возникновения коллизий к статистической погрешности.

Современные хэш-функции

На сегодняшний день самыми распространёнными (и считающимися в достаточной степени безопасными) являются хеш-функции SHA-256 и SHA-512, пришедшие на замену алгоритму SHA-1, в котором была обнаружена возможность коллизий.[16]



Источник: Google security blog[17]

[16] https://www.zdnet.com/article/sha-1-collision-attacks-are-now-actually-practical-and-a-looming-danger/
[17] https://security.googleblog.com/2017/02/announcing-first-sha1-collision.html

Существуют и другие функции хэширования — к примеру, алгоритм Whirlpool. Все современные хеш-функции должны отвечать ряду требований как к безопасности (те самые коллизии), так и к скорости как вычисления, так и проверки хэша. Разумеется, результат работы хеш-функции должен быть абсолютно односторонним и абсолютно необратимым.

Каким образом "абсолютная необратимость" хэш-функций соотносится с существованием многочисленных программ для взлома паролей, включая наши собственные разработки? Дело в том, что пароли обычно состоят из ограниченного числа символов. Ограниченная длина большинства паролей позволяет проверить на совпадение результаты хеширования, произведённые от всех возможных комбинаций букв, цифр и специальных символов вплоть до заданной максимальной длины. Так работает атака методом полного перебора.

Криптографическая соль

Что произойдёт, если группа злоумышленников вычислит хэш-функции для десятков миллионов популярных паролей? В таком случае для взлома пароля будет достаточно подсчитать хэш, который будет достаточно просто найти в таблице. Существует и более продвинутая версия атаки с использованием таблиц Rainbow Tables.

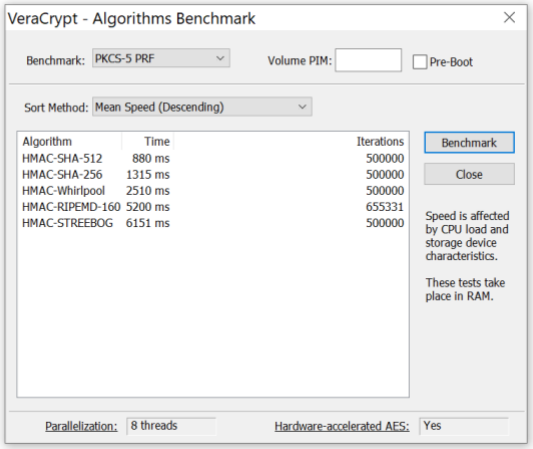
Rainbow Tables – это реализация метода time-memory trade-off, при котором нет необходимости хранить все возможные хэши. Вместо этого они разбиваются на взаимосвязанные цепочки, от которых сохраняются только начало и конец. «Радужные таблицы» требуют усилий по перебору, но перебирать нужно гораздо меньше полного диапазона, причём параметры атаки можно подобрать или вычислить заранее. Вычисление подобных таблиц занимает у хакеров длительное время, после чего сами атаки осуществляются крайне быстро.

Для противодействия подобным атакам был разработан метод, применяющий к хэшу так называемую криптографическую соль. Теперь хэш вычисляется не от самого пароля, а от комбинации пароля и добавленной к нему случайной строки («соли»). Значение соли (повторимся — это строка, состоящая из случайных данных) сохраняется рядом с хэшем; без неё восстановить правильный пароль не получится. В редких случаях в дополнение к соли используется ещё одна строка — Pepper («перец»), значение которой хранится на отдельном физическом сервере для обеспечения дополнительного уровня безопасности.

Итерации (раунды) хэширования

Итак, для преобразования пароля в ключ шифрования, как правило, используется хэширование, а число алгоритмов хэширования фактически ограничено "большой тройкой" — SHA-1, SHA-256 и SHA-512. В то же время скорость работы атак методом полного перебора может отличаться на многие порядки в зависимости от того, какой именно набор данных подвергается атаке. Почему так происходит?

Разумеется, нельзя сбрасывать со счетов разницу в алгоритмах хеширования. Так, преобразование SHA-1 работает быстрее, чем SHA-512, которое, в свою очередь, быстрее, чем SHA-256. Самым медленным из популярных алгоритмов является Whirlpool. В зависимости от того, какой именно алгоритм хеширования используют разработчики конкретного приложения или формата данных, атака может происходить с большей или меньшей скоростью.



Впрочем, скорость алгоритмов хэширования различается в считанные разы, а скорость перебора паролей в разных форматах может отличаться на многие порядки. Значит, дело не только и даже не столько в том, какой алгоритм хеширования используется. Основное влияние на скорость перебора оказывает количество итераций, или раундов хэширования.

Количество раундов (итераций хеширования) оказывает сильнейшее влияние на скорость проверки пароля. На современном оборудовании вычисление одного значения хеш-функции от короткой строки, которой является пароль, занимает доли миллисекунды. Если бы файлы были защищены с помощью единственной итерации хеширования, мы бы получили атаки, работающие со скоростью в диапазоне десятков, а то и сотен миллионов паролей в секунду. Подобные атаки были возможны в iOS 10.0 (порядка 6 миллионов паролей в секунду на процессоре Intel шестилетней давности).

В современных приложениях используются сотни тысяч и даже миллионы итераций хеш-функции. Так, документы Microsoft Office используют 100 000 итераций, что позволяет проверить порядка десятка паролей в секунду. После фиаско с iOS 10.0 разработчики Apple увеличили число раундов хеширования до миллиона (!), в результате чего скорость проверки паролей к резервным копиям iTunes составляет единицы паролей в минуту. Крипто-контейнеры VeraCrypt защищены 500 000 раундами хеширования, причём у пользователя есть возможность изменить это значение в большую сторону.

Разумеется, под "итерацией" хэширования не имеется в виду бесконечный цикл вычислений значения хэш-функции от предыдущего хэша. В такой прямолинейной реализации алгоритм хеширования вырождается, существенно увеличивается риск коллизий. Борются с этим путём добавления промежуточных значений соли на каждом этапе. Промежуточная соль вычисляется алгоритмически для каждой итерации; случайным образом генерируется только оригинальная соль, которая хранится вместе с паролем. Таким образом в результате получается стойкий детерминированный хэш, вычисление которого на заданном оборудовании занимает заранее заданное время.

Как проверяется пароль

Для проверки пароля (например, в онлайновых сервисах или при входе в локальную учётную запись Windows, Linux или macOS) по заданному алгоритму подсчитывается его хэш, который система сравнивает с контрольной строкой. Рассмотрим для примера файл /etc/shadow, в котором хранятся пароли к ОС Linux.

В описаниях формата /etc/shadow часто можно встретить упоминание, что в файле хранятся «зашифрованные пароли». Как вы уже знаете, это не так: на самом деле в файле /etc/shadow хранятся хэши паролей, соль и некоторая дополнительная информация, включая информацию о том, каким образом должен вычисляться хэш. Хэши паролей хранятся хранятся в виде $type$salt$hashed, где значение переменной type указывает на тип хэш-функции из следующего списка:

1. **1** — MD5
2. **$2a$** — Blowfish
3. **$2y$** — Blowfish
4. **5** — SHA-256
5. **6** — SHA-512

В примере ниже приводится начало строки из файла /etc/shadow (у неё есть продолжение, в котором содержится сервисная информация — такая, как время последней смены пароля, оставшийся срок действия пароля и т.п.):

```
root:$6$Zwg4GkPw$5ggbsXCbCzjT3i8O7DGUqXH8vQiPqCySGLWSPDVR4ionV3AIkG
0rqjeosDZGwpCQmsH6oP.6jqz6Zr.oA2DbA/
```

Здесь *"root"* — имя пользователя, *6* указывает на то, что используется алгоритм хэширования SHA-512, *"Zwg4GkPw"* — соль, а строка, начинающаяся с *"$5ggbs"* — соответственно, хэш от пароля. В качестве эксперимента вы можете попробовать восстановить этот пароль или самостоятельно сгенерировать его командой mkpasswd -m sha-512 PASSWORD [SALT].

Обратите внимание: если отредактировать файл /etc/shadow (для этого нужен доступ root), то пароль любого пользователя можно сменить, зайдя от его имени. А можно ли сделать так же, например, для зашифрованного архива или документа?

Когда хэш не хранится

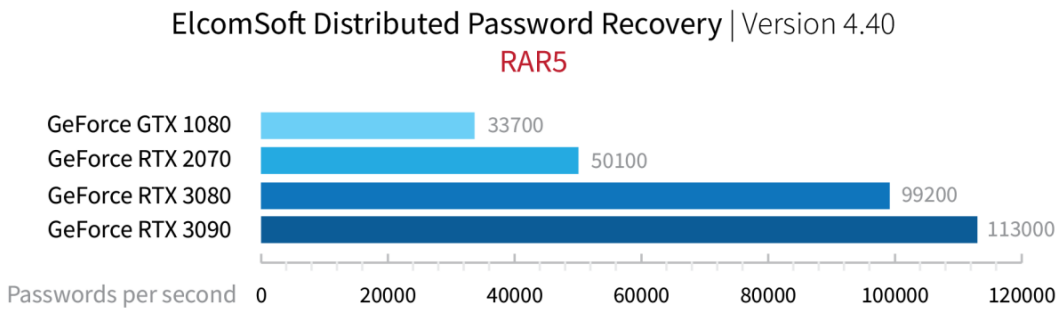
В ряде случаев при шифровании файла или документа хэш от оригинального пароля не сохраняется и, соответственно, не проверяется. Так работает, например, шифрование в формате RAR4 (а вот в пришедшем ему на смену формате RAR5 хэш от пароля вычисляется и сохраняется в заголовке архива). Вариантов два:

– ключом, сгенерированным из пароля, шифруется фиксированная строка, которая используется для шифрования файла или документа (так, например, работает BitLocker);

– ключом, сгенерированным из пароля, шифруется весь документ (так работает формат RAR4).

В обоих случаях хэширование используется для генерации ключа из пароля, однако во втором случае, если был указан неправильный пароль, файл или документ будет расшифрован, но "расшифрованные" данные не пройдут валидации. В таком случае скорость проверки пароля (и, соответственно, скорость атаки) не будет детерминированной. Вот скорость перебора паролей

в Elcomsoft Distributed Password Recovery[18] для формата RAR5, в котором хэш от пароля сохраняется в заголовке архива:



Логично было бы сравнить скорость атаки на этот формат с предшествующим форматом RAR4, но сделать это невозможно: из-за того, что в RAR4 не сохраняется хэш от пароля, для проверки пароля необходимо расшифровать хотя бы один файл, вычислить его контрольную сумму и проверить её совпадение с той, которая хранится в архиве. Если контрольная сумма расшифрованного файла совпадёт с эталоном, пароль считается правильным. Если же пароль неправильный, то файл до конца распаковать не удастся. Ошибка распаковки — тоже индикатор неправильного пароля, и этот момент учтён в процессе оптимизации перебора в Elcomsoft Distributed Password Recovery.

11. Когда включён компьютер

Стандартная процедура изъятия цифровых улик подразумевает отключение компьютеров от сети электропитания, извлечение носителей информации, создания образов дисков и их последующий анализ. В то же время своевременный анализ авторизованной пользовательской сессии может помочь получить доступ к некоторым типам данных, расшифровка которых при анализе образа диска займёт длительное время или будет невозможной. К таким данным относятся смонтированные на момент анализа зашифрованные диски и виртуальные машины; файлы, зашифрованные средствами файловой системы NTFS; пароли из веб-браузеров и некоторых программ для хранения паролей.

Ещё один способ анализа компьютера в сборе подразумевает старт со специально подготовленного загрузочного накопителя (Elcomsoft System Recovery). В этом случае зашифрованные диски останутся зашифрованными, но можно будет как просканировать систему на предмет наличия зашифрованных дисков и виртуальных машин, так и извлечь метаданные шифрования для последующей атаки в лаборатории. Использование загрузочного накопителя – не панацея, но средство значительно ускорить расследование путём распараллеливания процессов расшифровки и анализа данных.

Подытоживая вышесказанное, перечислим действия, доступные при анализе компьютера в сборе.

[18] https://www.elcomsoft.ru/edpr.html

Анализ авторизованной пользовательской сессии:

– при наличии административных привилегий: снятие образа оперативной памяти (Elcomsoft Forensic Disk Decryptor);

– поиск подключённых зашифрованных дисков (Elcomsoft Encrypted Disk Hunter);

– снятие образа подключённых зашифрованных дисков либо извлечение метаданных шифрования для последующей атаки (Elcomsoft Forensic Disk Decryptor);

– извлечение сохранённых паролей (Elcomsoft Quick Triage).

Анализ с использованием загрузочного накопителя.

Этот вид анализа производится посредством единственного продукта – Elcomsoft System Recovery. В число доступных действий входит:

– поиск зашифрованных дисков и виртуальных машин;

– анализ возможности парольной атаки на зашифрованные диски (при использовании TPM в качестве протектора атака на пароль невозможна);

– извлечение метаданных шифрования зашифрованных дисков и виртуальных машин;

– (После оценки рисков) смена или сброс паролей от учётных записей пользователей или администратора.

11.1. Поиск зашифрованных дисков

Повсеместное распространение шифрования способно не просто затруднить анализ данных, но и сделать его невозможным при малейших отклонениях от установленных процедур. В то же время точное следование процедурам изъятия компьютерной техники далеко не всегда возможно в практических условиях. Своевременное обнаружение зашифрованных дисков позволит предпринять необходимые меры для защиты доступа к зашифрованным уликам, прежде чем компьютер подозреваемого будет обесточен. Какие шаги необходимы и как узнать, используется ли в системе шифрование диска? Сделать это достаточно просто, запустив соответствующую утилиту с флэш-накопителя.

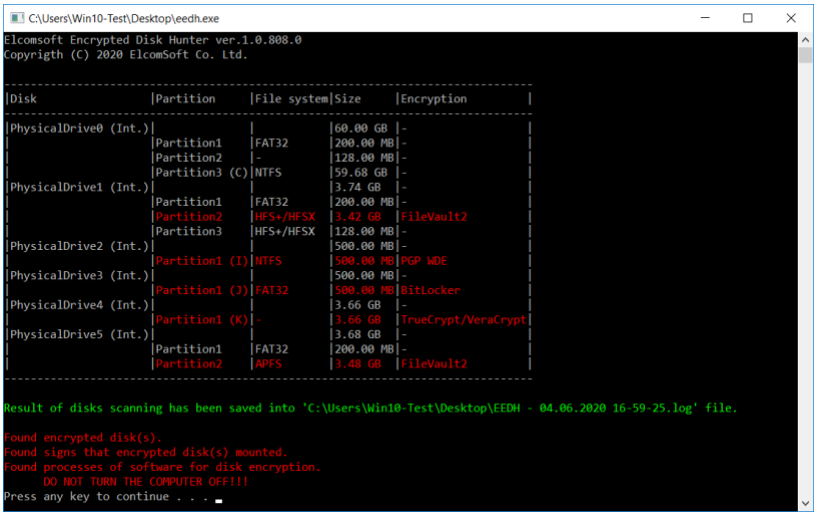
Зашифрованные диски — постоянная головная боль для экспертов-криминалистов. Доступ к уликам, хранящимся на зашифрованных томах, может оказаться невозможен без проведения достаточно длительных атак на пароль. При этом в некоторых условиях доступ к зашифрованным данным будет невозможен в принципе. Классический рабочий процесс состоит из отключения компьютера, извлечения дисков, создания образа диска через устройство с блокировкой записи и последующий анализ данных уже из виртуального образа диска.

В этом процессе есть тонкий момент: если в системе были смонтированы зашифрованные тома, то доступ к записанным на них данным пропадает при отключении питания. Разумеется, этого не произойдёт, если эксперт будет знать о наличии смонтированных зашифрованных томов и предпримет несложные шаги по консервации имеющихся данных (забегая вперёд — обычно достаточно снять образ оперативной памяти компьютера). Предлагаем воспользоваться более простым и быстрым способом узнать, присутствуют ли в системе зашифрованные диски.

С точки зрения пользователя смонтированный зашифрованный диск ничем не отличается от обычного диска. Тем не менее, при выключении компьютера зашифрованный диск, как правило, размонтируется, и при следующем включении пользователю придётся или ввести пароль, или авторизоваться в системе.

Отличить зашифрованный диск от незашифрованного «на глазок» достаточно сложно. С одной стороны, можно проанализировать настройки системы — например, приложение BitLocker в Панели управления Windows. С другой — продвинутые преступники часто используют более серьёзное шифрование, например — вложенный контейнер TrueCrypt (использование вложенного контейнера позволит подозреваемому отрицать сам факт наличия улик, выдав вместо пароля от вложенного контейнера пароль от "обёртки", в которой не будет содержаться ничего инкриминирующего).

Определить наличие зашифрованных дисков поможет бесплатная утилита командной строки Elcomsoft Encrypted Disk Hunter.



Elcomsoft Encrypted Disk Hunter — это бесплатный портативный инструмент, который поможет быстро обнаружить наличие зашифрованных дисков. Для анализа системы достаточно запустить утилиту с USB накопителя; список подключённых устройств и зашифрованных дисков выводится автоматически. Инструмент может обнаруживать зашифрованные диски TrueCrypt/VeraCrypt (эвристический анализ), а также тома BitLocker, PGP WDE, FileVault2 и LUKS (только первой версии). Необходимо отметить, что вероятность встретить диски с шифрованием FIleVault2 и LUKS, подключённые к компьютеру с Windows невелика (наша утилита работает только в этой ОС). Их поддержку мы включили для тех редких случаев, когда они могут вам понадобиться.

Что делать, если на компьютере пользователя запущена macOS или Linux? В этом случае вам поможет другой, загрузочный инструмент — Elcomsoft System Recovery.

11.1.1. Практические шаги

Прежде всего, для использования утилиты нужны права администратора в анализируемой системе. Без административных привилегий не будет низкоуровневого доступа ни к дискам, ни к оперативной памяти компьютера и списку драйверов.

После запуска Elcomsoft Encrypted Disk Hunter инструмент сканирует подключённые к системе устройства хранения информации на предмет шифрования, осуществляя поиск характерных сигнатур и заголовков в таблицах разделов. При обнаружении зашифрованных томов выводится список зашифрованных дисков.

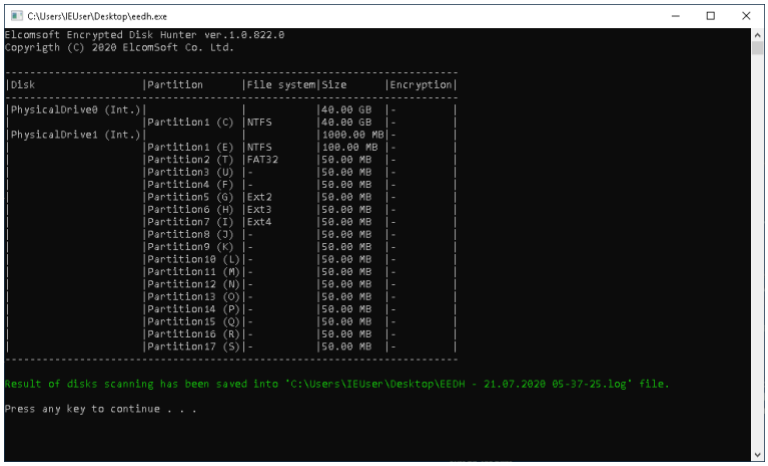
После этого проверяется, смонтирован ли какой-либо из зашифрованных томов. Если никаких явных признаков шифрования диска не обнаружено, Encrypted Disk Hunter проверяет

цепочку системных драйверов на предмет наличия в ней драйверов TrueCrypt, VeraCrypt и PGP WDE. Если распознан драйвер шифрования диска (например, truecrypt.sys, veracrypt.sys, PGPdisk.SYS, Pgpwdefs.sys или PGPwded.sys), утилита сообщит, что в системе могло использоваться шифрование, даже если в данный момент времени ни одного зашифрованного тома не обнаружено. Кстати, такая эвристика — единственный способ обнаружить диск, зашифрованный PGP WDE, т.к. последний блокирует доступ к размонтированным зашифрованным томам.

11.1.2. Дальнейшие действия

Ваши дальнейшие действия будут зависеть от выданного программой результата и проведённой вами оценки рисков.

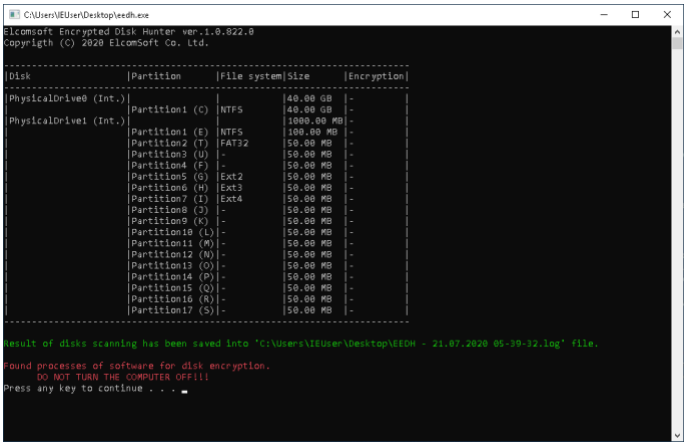
1. Если никаких признаков полного шифрования диска не обнаружено: образ оперативной памяти создать желательно, но не обязательно; отключите питание и следуйте обычной схеме. Образ оперативной памяти может быть использован для анализа в сторонних программах. Его исследование может помочь понять, какие приложения были запущены, возможно – обнаружить некоторые пароли, обрывки документов, сохранившиеся в памяти веб-страницы (в том числе для приватных сессий браузера) и т.д. Также активно используется для поиска зловредного ПО.



Признаков шифрования не обнаружено

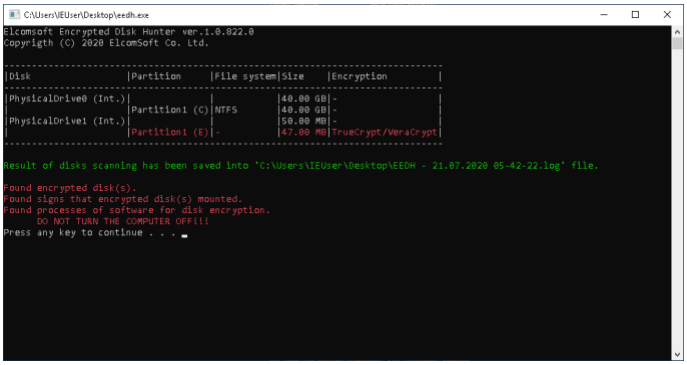
2. При обнаружении признаков шифрования: обязательно создайте образ оперативной памяти (например, посредством Elcomsoft Forensic Disk Decryptor)[19]; возможно, вам придётся потратить дополнительное время на исследование системы перед тем, как обесточить компьютер.

[19] https://www.elcomsoft.ru/efdd.html

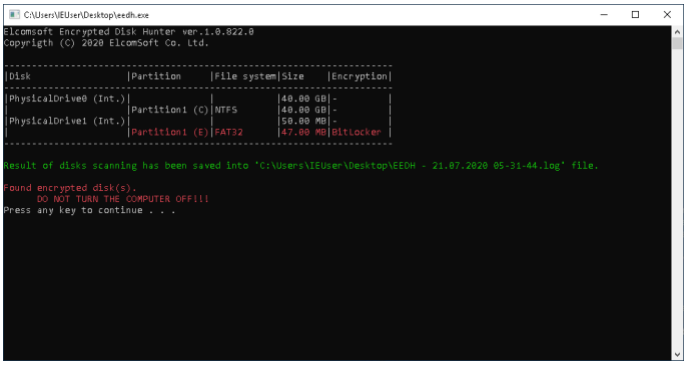


Зашифрованные тома не обнаружены, но обнаружен активный процесс шифрования диска. Требуется дальнейшее исследование.

3. Если найдены смонтированные зашифрованные диски: создайте образ оперативной памяти; попытайтесь извлечь из него ключи восстановления / депонированные ключи. Если позволяет время, попытайтесь извлечь улики из смонтированных зашифрованных томов.



Найден том TrueCrypt/VeraCrypt. Further analysis mandatory. Требуется дальнейшее исследование.



Найден том BitLocker. Требуется дальнейшее исследование.

Если смонтирован хотя бы один зашифрованный диск, обратите внимание на тип шифрования. Также рекомендуем воспользоваться утилитой Elcomsoft Forensic Disk Decryptor для создания образа оперативной памяти и поиска ключей шифрования, что позволит обойтись без попыток подобрать оригинальный пароль. Извлечение ключей шифрования из образа памяти может и вовсе оказаться единственным доступным методом для разблокировки томов BitLocker, защищённых некоторыми типами протекторов (например, TPM).

Если этот вариант не сработал, используйте Elcomsoft Distributed Password Recovery для взлома пароля. EDPR реализует все возможные оптимизации с учётом человеческого фактора,

но атака может оказаться достаточно длительной, так как перебор паролей к зашифрованным дискам может быть очень и очень медленным.

11.1.3. Elcomsoft Encrypted Disk Hunter

Elcomsoft Encrypted Disk Hunter можно скачать по ссылке с нашего сайта:

https://www.elcomsoft.com/download/eedh.zip[20]

Утилита доступна в виде ZIP-архива без установщика. В архиве содержится портативный исполняемый файл, подписанный цифровой подписью. Распакуйте архив, сохраните утилиту на USB-накопителе и используйте в системе с правами администратора. Настоятельно рекомендуем запускать инструмент непосредственно с USB-накопителя.

11.2. Образ оперативной памяти – ключ к зашифрованным контейнерам

Практически все производители инструментов для шифрования дисков реализовали стойкое шифрование, обеспечивающее защиту от несанкционированного доступа в ряде сценариев. Максимально стойкая защита (а, следовательно, трудная для атаки цель) направлена против анализа дисков, извлечённых из компьютеров, а также анализа образов дисков.

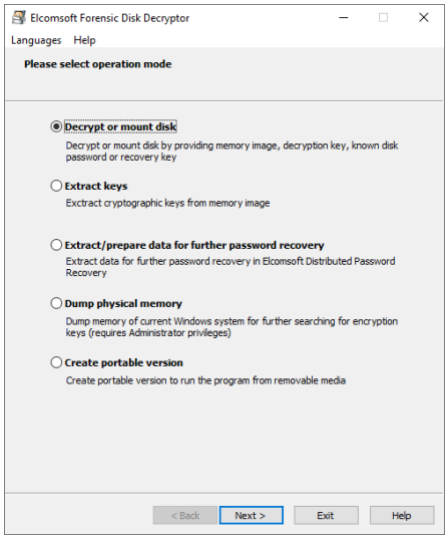
В то же время в большинстве инструментов шифрования дисков для Windows есть слабое звено. Поскольку за редкими исключениями (например, Opal) шифрование обеспечивается средствами центрального процессора, а не выделенного аппаратного сопроцессора с собственной недоступной снаружи памятью, ключ шифрования-дешифрования данных хранится в оперативной памяти компьютера в течение всего времени, пока зашифрованный диск смонтирован. Соответственно, снятие образа оперативной памяти (из авторизованной пользовательской сессии или с использованием уязвимости) и его последующий анализ с целью поиска ключей шифрования позволит избежать длительных и не всегда успешных «лобовых» атак.

Для снятия образа оперативной памяти из авторизованной пользовательской сессии с административными привилегиями рекомендуем воспользоваться утилитой Elcomsoft Forensic Disk Decryptor, доступной как в виде самостоятельного приложения, так и в составе пакета Elcomsoft Desktop Forensic Bundle.

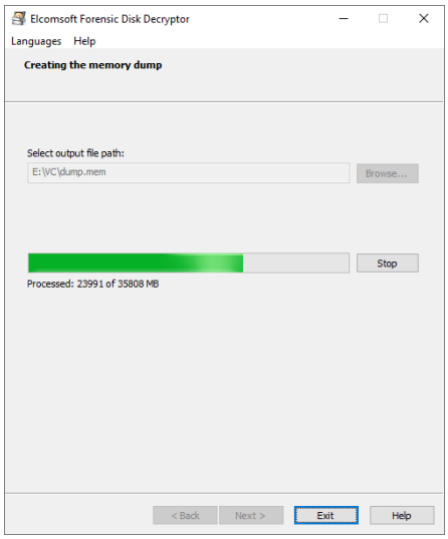
Чтобы снять образ оперативной памяти, запустите Elcomsoft Forensic Disk Decryptor на исследуемом компьютере. Для запуска рекомендуем использовать внешний диск или USB накопитель, свободный объём которого превышает объём оперативной памяти исследуемого компьютера. Накопитель должен быть отформатирован NTFS или exFAT; использование файловой системы FAT32 недопустимо, т.к. эта файловая система ограничивает максимальный размер файла 4 гигабайтами.

[20] https://www.elcomsoft.com/download/eedh.zip

Далее в главном окне EFDD выберите команду *«Dump physical memory»*. Нажмите «Next».



Укажите путь к файлу, в который будет сохранён образ оперативной памяти, и нажмите «Next».



По окончании процесса извлеките USB накопитель. Поиск ключей шифрования рекомендуем проделывать в лаборатории. Для поиска ключей шифрования также используется Elcomsoft Forensic Disk Decryptor. Подробнее об этом – в разделе «**Альтернативные способы расшифровки VeraCrypt**».

11.3. Извлечение паролей из браузера

Наименее эффективный способ восстановления оригинального пароля – атака методом полного перебора. Наиболее эффективной считается атака по словарю, составленному из существующих паролей пользователя. Повторное использование паролей большинством пользователей позволяет успешно восстанавливать доступ к зашифрованным данным, основываясь на списке паролей, составленном по данным из разных источников. Один из таких источников – база данных веб-браузеров, в которой содержатся сохранённые пользователем пароли к веб-сайтам.

Извлечение сохранённых паролей возможно при анализе авторизованной пользовательской сессии. Административный доступ не требуется. Для работы потребуется Elcomsoft Quick Triage.

Для извлечения сохранённых паролей из браузера пользователя вам потребуются:

– авторизованная пользовательская сессия (административный доступ не обязателен);
– утилита Elcomsoft Quick Triage.

Для извлечения паролей достаточно запустить Elcomsoft Quick Triage *с внешнего диска* или *USB-накопителя* на исследуемом компьютере.

– запустите Elcomsoft Quick Triage;
– выберите пункт меню Web Browsers, после чего выберите из списка используемый веб-браузер (например, Edge Chromium);
– через несколько секунд будет выведен список паролей;
– для создания словаря, в который войдут пароли из всех установленных в системе браузеров и почтовых приложений, воспользуйтесь кнопкой для экспорта паролей в файл (кнопка Export). По этой команде будет создан отфильтрованный список всех паролей пользователя. Список паролей можно использовать в качестве словаря для создания интеллектуальных атак в Elcomsoft Distributed Password Recovery.

11.4. Поиск зашифрованных виртуальных машин

Виртуальные машины, защищённые стойким шифрованием, получили широкое распространение в криминальной среде. Использование не оставляющих цифрового следа зашифрованных виртуальных машин позволяет злоумышленникам минимизировать утечку инкриминирующих данных.

Внимание: функционал поиска зашифрованных виртуальных машин реализован в Elcomsoft System Recovery, который требует загрузки компьютера с созданного программой загрузочного накопителя.

Для поиска зашифрованных виртуальных машин рекомендуем воспользоваться загрузочным устройством, созданным программой Elcomsoft System Recovery, которая автоматизирует процесс поиска. Для начала сканирования загрузите целевой компьютер в Elcomsoft System Recovery выберите пункт Encrypted Virtual Machines. При обнаружении зашифрованных виртуальных машин ESR сохраняет метаданные шифрования, необходимые для восстановления пароля посредством Elcomsoft Distributed Password Recovery. Подробные инструкции по созданию и использованию загрузочного накопителя приводятся в разделе «**Анализ компьютера с использованием внешнего загрузочного накопителя**».

12. Когда компьютер выключен

Если настольный компьютер доставлен в лабораторию в обесточенном состоянии, стандартная процедура исследования подразумевает извлечение накопителей и снятие их образов с использованием устройства, блокирующего возможность записи на аппаратном уровне. Необходимо понимать ограничения подобных устройств в случаях, когда к ним подключаются не традиционные магнитные жёсткие диски, а накопители на основе твердотельной памяти (SSD в версиях как SATA, так и NVME).

12.1. Можно ли извлечь накопитель?

Первый вопрос, на который должен ответить эксперт – это можно ли извлечь из компьютера накопитель. Для настольных компьютеров, как правило, этот процесс не вызывает трудностей (разумеется, нужно помнить о существовании как SATA, так и NVME накопителей, причём первые могут быть доступны в обычном форм-факторе или в виде устройств M.2, которые внешне похожи на накопители NVME, но физически отличаются вырезом-ключом, не позволяющим установить накопитель в не предназначенное для его типа устройство).

В то же время для многих типов устройств извлечение накопителя невозможно физически: для этого потребуется выпаивать микросхемы (например, модули eMMC).

Если накопитель извлечь можно: подключение к аппаратному устройству для блокирования записи; снятие и анализ образа диска.

Если накопитель извлечь нельзя: для снятия образа диска используйте загрузочный накопитель Elcomsoft System Recovery в режиме «только для чтения».

12.2. Повлечёт извлечение диска нежелательные последствия?

В ряде случаев извлечение накопителя окажется бесполезным (как в случае с компьютерами Mac, в которых шифрование диска реализовано на отдельном контроллере T2, без которого диск нельзя не только расшифровать, но и получить доступ извне даже к зашифрованному образу) или даже опасным. Если в системе с Windows диск зашифрован механизмом BitLocker или BitLocker Device Protection с использованием модуля TPM или его эмулятора, то любое изменение в аппаратной конфигурации устройства приведёт к «панике» модуля TPM и удалению из него ключей шифрования. В результате диск не удастся разблокировать вводом пароля от учётной записи пользователя, вместо которого придётся использовать специальный ключ восстановления доступа.

Возможны и другие варианты – например, случаи, когда несколько дисков объединены в RAID-массив или используется комбинация из обычного диска (или SSD) и кэширующего диска, выполненного по технологии Intel Optane. В последнем случае необходимо работать с обоими устройствами, что проще всего сделать в рамках оригинального компьютера пользователя.

Если извлечение накопителя не повлечёт негативных последствий: подключение к аппаратному устройству для блокирования записи; снятие и анализ образа диска.

Если есть сомнения: для снятия образа диска используйте загрузочный накопитель Elcomsoft System Recovery в режиме «только для чтения».

12.3. Работа с твердотельными накопителями и восстановление данных с SSD

Механизмы хранения, удаления и восстановления данных в твердотельных накопителях отличаются от таковых для традиционных медиа с магнитной записью. В отличие от традиционных жёстких дисков, данные на которых остаются на месте даже после удаления файла*, твердотельные накопители способны самостоятельно запустить и поддерживать процесс безвозвратного уничтожения информации, стоит лишь подать на них питание. Таким образом, стандартная в процессе экспертизы процедура снятия образа диска с использованием устройства для аппаратной блокировки записи приводит к тому, что к моменту окончания процесса на SSD не остаётся никаких следов удалённых пользователем данных.

*До недавнего времени это было именно так, однако внедрение накопителей с «черепичной» записью SMR внесло свои коррективы.

Одна из возможностей получить доступ к удалённым доступна путём извлечения чипов NAND и прямого считывания информации (с последующей реконструкцией таблиц адресации). Существует и альтернативный способ, использующий специализированное программно-аппаратное обеспечение. В этом разделе рассказывается о том, как работают механизмы хранения и удаления информации на современных SSD и о том, как восстановить данные в удалённых блоках.

Обратите внимание: в данном разделе не описан, но представляет отдельный интерес уязвимость популярного алгоритма шифрования дисков BitLocker, являющегося составной частью Windows. Как обнаружили исследователи[21], вместо программного шифрования с использованием центрального процессора BitLocker может использовать контроллер SSD для шифрования данных. Соответственно, низкоуровневый доступ к SSD позволяет найти ключ шифрования данных и расшифровать содержимое такого накопителя.

12.4. Процедурные вопросы

Рекомендуем внимательно ознакомиться с содержимым данного раздела до того, как твердотельный накопитель будет подключён к устройству для снятия образа либо на накопитель будет подано питание. **Обратите внимание:** встроенный в накопитель контроллер может начать удаление данных в момент подачи питания.

В то же время вероятность восстановления удалённых данных с твердотельных накопителей минимальна даже с использованием перечисленных ниже инструкций. В реальности описанным способом можно восстановить лишь данные, которые были удалены совсем недавно – за считанные секунды (при полном форматировании диска – минуты) после их удаления. Соответственно, в ряде случаев имеет смысл следовать стандартной процедуре снятия образа.

12.5. SSD способны самостоятельно уничтожать улики

Если на твердотельный накопитель будет подана команда *Trim*, то данные будут удаляться в фоновом режиме – в том числе непосредственно в то время, когда эксперт снимает образ диска. Для того, чтобы запустился процесс «сборки мусора», на диск будет достаточно подать питание – не обязательно даже подключать его к шине SATA или NVME. Таким образом, SSD действительно «заметают следы» и «уничтожают улики» совершенно самостоятельно и независимо от действий или бездействия специалиста по извлечению данных.

А что будет, если всё же попробовать считать данные из «удалённых» ячеек, до которых сборщик мусора ещё не успел добраться? В конце концов, нам известно, что сброс данных из ячеек – процесс далеко не мгновенный, а наоборот – достаточно длительный. Быстрое форматирование всего раздела запустит процесс сборки мусора, но процесс этот будет отрабатывать в течение достаточно длительного времени – до получаса на достаточно ёмких накопителях.

[21] https://borncity.com/win/2018/11/06/ssd-vulnerability-breaks-bitlocker-encryption/

Применение в SSD накопителях механизма сборки мусора и команды Trim сильно осложняет или делает невозможным доступ к удалённой информации. Если в процессе попытаться считать данные из ячеек, на которые уже поступила команда Trim, но которые ещё не были физически очищены, то результат будет зависеть от реализации механизма «данные после Trim» в конкретной модели накопителя. Современный SSD **может работать только в одном** из **трёх** режимов:

– *Non-deterministic Trim:* неопределённое состояние. Контроллер может вернуть фактические данные, нули или что-то ещё, причём результат может различаться между попытками (SATA Word 169 bit 0). В настоящее время почти не встречается, хотя безымянные китайские накопители могут удивить.

– *Deterministic Trim (DRAT)*: контроллер гарантированно возвращает одно и то же значение (чаще всего, но не обязательно нули) для всех ячеек после команды Trim (SATA Word 69 bit 14). Самый распространённый вариант.

– *Deterministic Read Zero after Trim (DZAT)*: гарантированное возвращение нулей после Trim (SATA Word 69 bit 5). Часто встречается в дисках, предназначенных для работы в составе RAID массивов.

Определить, к какому типу относится конкретная модель SSD, можно при помощи команды **hdparm –I**.

Пример использования:

```
$ sudo hdparm -I /dev/sda | grep -i trim
*    Data Set Management TRIM supported (limit 1 block)
*    Deterministic read data after TRIM
```

С практической точки зрения это означает только одно: сразу после удаления данных (хоть отдельно по одному файлу, хоть путём форматирования, даже быстрого, хоть разбивкой разделов) информация станет недоступной для чтения как с компьютера, так и на специальном стенде. Обычными способами, даже посредством низкоуровневых команд, получить доступ к реальному содержимому ячеек после Trim невозможно.

12.6. Жизнь после Trim: технологический режим SSD

Долгое время считалось, что извлечь данные из блоков SSD, к которым была применена команда TRIM, но данные, из которых фактически ещё не были очищены, можно только путём скорейшего обесточивания устройства и физического извлечения микросхем памяти. Этот путь долог и труден; он требует наличия высокой квалификации и специального оборудования. Извлечение данных из накопителя всего с четырьмя микросхемами NAND памяти может занять до двух недель, а работать с накопителями с десятью микросхемами согласится далеко не каждая лаборатория.

До недавнего времени альтернативы этому способу не существовало. Включение SSD неизбежно приводило к удалению данных, даже если диск подключался через специальный

адаптер, блокирующий операции записи на уровне SATA. И тем не менее, выход есть, и название ему – технический режим.

Все накопители, не важно, какие именно, будь то HDD, SSD, или даже простая USB «флешка», имеют несколько режимов работы. К примеру, «стандартный» режим активен у накопителя по умолчанию. В нём мы получаем доступ к данным, можем записать и считать информацию, стирать и перезаписывать данные. При этом во всех накопителях есть ещё и так называемый «заводской режим», или, как правильнее его назвать, «технологический режим».

Находясь в технологическом режиме, накопитель может принимать и выполнять низкоуровневые команды, поступающие извне по ATA интерфейсу (разумеется, и по любому другому – например, USB или PCI-E, в зависимости от используемого типа внешнего интерфейса). Работая в обычном режиме, накопитель не может выполнять низкоуровневые команды, а в технологическом режиме — может.

Технологический режим придуман и используется производителями накопителей на заводе-изготовителе. В традиционных жёстких дисках он использовался для нужд начальной диагностики накопителя и выявлении неисправных головок HDD в момент тестирования. В твердотельных накопителях производители используют технологический режим для выявления битовых ошибок в блоках NAND памяти. Кроме того, технологический режим может быть использован производителем и для доступа к хранящимся данным, когда накопитель вернули по гарантии или с запросом о восстановлении данных. Специалистам нужно разобраться в причинах, по которым накопитель вышел из строя, а для этого нужно получить доступ к хранящейся в устройстве микропрограмме. Сделать это можно с помощью технологического режима, когда в стандартном режиме накопитель не может работать из-за повреждения основной микропрограммы.

12.6.1. Какие производители используют технологический режим?

Технологический режим используют все без исключения производители устройств для хранения информации, оборудованных контроллером. Даже маленькая флешка прямиком из подвалов Гуанчжоу будет обладать технологическим режимом, описанным в спецификациях производителя контроллера (например, популярного Phison PS2251-07). Технологический режим доступен как в SATA накопителях, так и в устройствах с интерфейсами NVME, USB и другими.

12.6.2. Возможности технологического режима

Возможности, которые открывает эксперту технологический режим, поистине безграничны. Вот лишь несколько вещей, которые может проделать эксперт посредством специализированных команд:

– *чтение «сырых» данных из физического блока без преобразований* (аналог чтения микросхем, но без выпаивания чипов; потребуется декодирование данных, т.к. блок содержит информацию, закодированную для коррекции ошибок);

– *считывание определённого логического блока с преобразованиями* (устранение MIX между страницами и блоками, выполнение преобразования страницы с отделением данных и служебных байтов с ECC друг от друга, расшифровка данных силами контроллера);

– *для зашифрованных накопителей — поиск модуля с ключом-паролем.* Этот момент представляет особый интерес для правоохранительных органов и экспертов-криминалистов; он заслуживает отдельного рассмотрения в отдельной статье. Здесь мы лишь отметим, что

популярный алгоритм шифрования дисков BitLocker, работающий в качестве встроенной защиты в Windows 10, на SSD часто использует контроллер SSD для шифрования данных. Соответственно, использование технологического режима позволяет найти ключ шифрования данных и расшифровать содержимое накопителя, защищённого, казалось бы, надёжным методом BitLocker;

– *чтение блоков, выходящих за пределы трансляции* (блоки из категорий remapped, relocated и reserved);

– *чтение атрибутов SMART*;

– *поиск и чтение служебных блоков, содержащих микропрограмму управления SSD*;

– *сохранение служебных структур в файл для последующего анализа*.

Отдельно отметим **две** важнейших **особенности доступа к данным из технологического режима**. **Первая** особенность – это временное отключение фоновых процессов контроллера, включая процесс «сборки мусора», который в фоновом режиме очищает блоки после команды Trim. **Вторая** – полноценный доступ к неадресуемым блокам из резервного пула (overprovisioned area). Что это означает на практике? По сути, эти две особенности переворачивают сложившуюся картину мира, в которой эксперт не может остановить уничтожение улик без выпаивания микросхем памяти.

Как мы помним, команда Trim подаётся контроллеру со стороны операционной системы. Посредством этой команды операционная система даёт накопителю знать, что те или иные блоки больше не нужны системе и не содержат полезных данных. Остальное – дело уже самого контроллера. В первую очередь блоки помечаются как неиспользуемые. Дальнейшее зависит от множества факторов: нагрузки на накопитель (производятся ли операции ввода-вывода, если да – насколько интенсивные), мощности контроллера и управляющей им микропрограммы. Нам попадались накопители, которые приостанавливали операции ввода-вывода (фактически, пользователь наблюдал временный «фриз» накопителя) до завершения очистки блоков после Trim. Попадались и такие модели, которые запускали процесс очистки лишь спустя несколько секунд после падения загруженности накопителя. Наконец, мы встречали модели, которые отрабатывали команду Trim, что называется, «спустя рукава»: блоки подвергались очистке только тогда, когда подходил к концу запас свободных блоков как в адресной зоне накопителя, так и в неадресуемом резервном пространстве overprovisioned area.

Неадресуемое резервное пространство в SSD – это дополнительные блоки памяти, которые не входят в официально заявленную ёмкость накопителя. Как правило, ёмкость SSD больше заявленной. Каждый производитель может зарезервировать ту или иную ёмкость под те или иные нужды. Дополнительная область памяти идёт на резервную область под переназначение секторов, SLC кэш и на область хранения микропрограммы. У каждого производителя свои приоритеты, поэтому на одном и том же наборе микросхем NAND суммарной ёмкостью 530 ГБ (мы помним, что физический объём современных микросхем не всегда кратен двойке) можно создать накопители с официально доступным пользователю объёмом в 480 500 512 и даже 525 ГБ.

В неадресуемое пространство могут попадать и пользовательские данные после того, как блок был помечен как неиспользуемый командой Trim. Традиционными способами, через обычный режим работы накопителя, получить доступ к таким данным невозможно (если не выпаивать микросхемы). В технологическом режиме можно получить доступ ко всему пространству LBA, даже с учётом неадресуемого пространства.

12.6.3. Использование технологического режима для извлечения информации

В этой короткой главе мы подошли к самому главному: использованию возможностей технологического режима SSD накопителей для извлечения информации. К сожалению, в силу огромного разнообразия накопителей, количества производителей контроллеров и самих дисков, которые в стандартных контроллерах часто используют микропрограммы собственного производства, мы не смогли в короткой статье описать все подробности процесса. В этой главе мы опишем общий подход к процедуре. Пользователям, желающим ознакомиться с деталями процесса, рекомендуем следующие статьи:

– Особенности технологического режима SSD и использование PC-3000 Suite для доступа к данным[22]

– Пример восстановления SM2246EN (актуален для SM2246XT, SM2256K, SM2258G, SM2258H)[23]

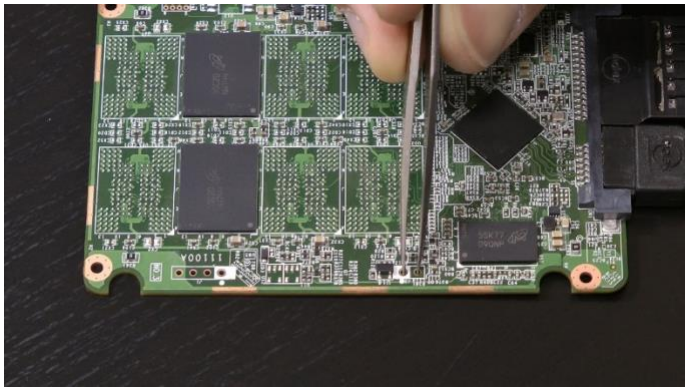
– Пример восстановления PS3109 (актуален для PS3105, PS3108, PS3109, PS3110, PS3111, TC58NC1000, TC58NC10100)[24]

В общем виде процедура извлечения данных с SSD с использованием технологического режима выглядит так.

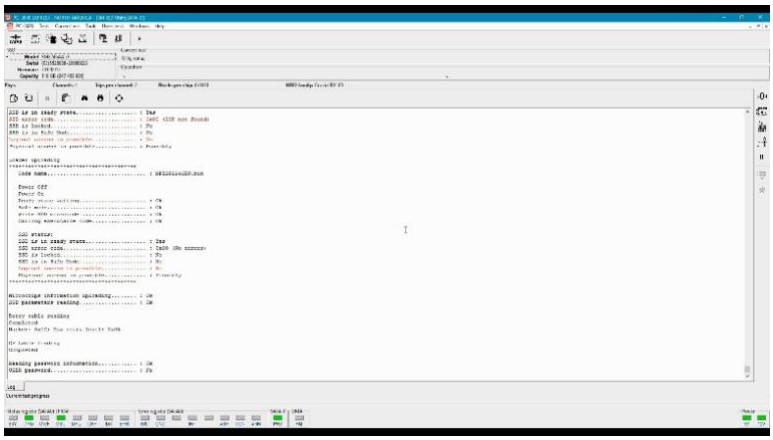
Первое и самое главное: перед тем, как подать напряжение, SSD необходимо перевести в технологический режим или его аналог (Factory Mode, Safe Mode и так далее). Для каждой модели контроллера и каждой модели SSD, не говоря уже о разных производителях, способ перевода устройства в технологический режим будет отличаться. Но прежде всего необходимо заблокировать контроллеру доступ к микросхемам памяти. Такая блокировка осуществляется замыканием служебных контактов на плате PCB. Она предотвращает считывание и инициализацию микропрограммы с микросхем памяти; соответственно, контроллер не может считать таблицу переадресаций и не запустит процесс "сборки мусора". Блокировка доступа к микросхемам памяти поможет инициализировать и повреждённый накопитель, который уходит в круговой цикл "загрузка микрокода — ошибка — сброс — загрузка микрокода", так как в этом случае контроллеру невозможно отправить команду на активацию технологического режима ввиду его загруженности (это выражается постоянно активной ATA-командой BSY-state).

[22] https://blog.acelaboratory.com/pc-3000-ssd-active-utilities-main-concept-description.html
[23] https://blog.acelab.eu.com/pc-3000-ssd-silicon-motion-sm-utility.html
[24] https://blog.acelab.eu.com/pc-3000-ssd-phison-utility.html

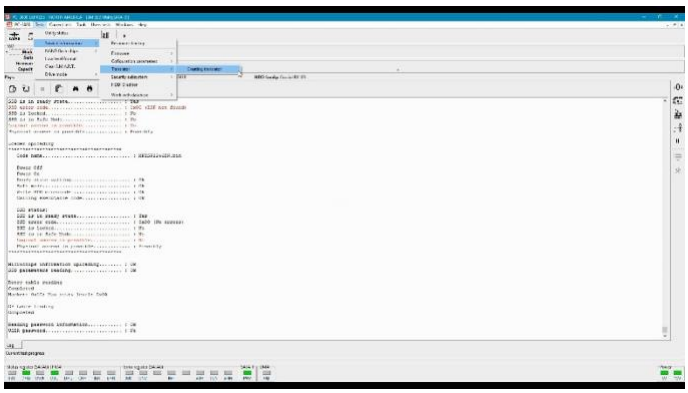
Вот так выглядит блокировка доступа к микросхемам памяти популярного, хоть и устаревшего накопителя Crucial BX100:



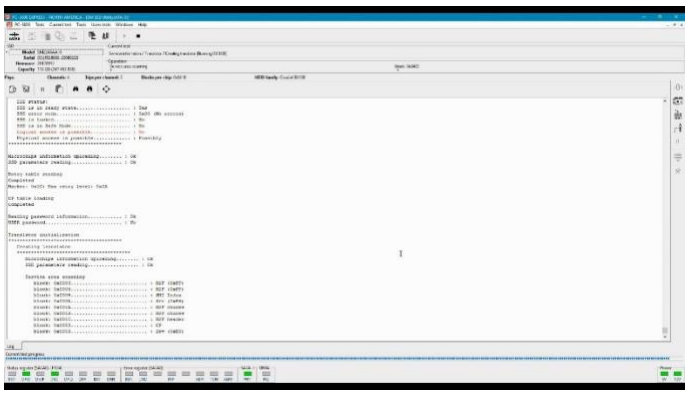
Далее мы используем комплекс PC-3000 (разработка AceLab) для перевода накопителя в технологический режим, который производится путем отправки специальной команды в контроллер SSD. Наконец, в ОЗУ контроллера загружается код микропрограммы LDR, которой впоследствии будет передано управление.



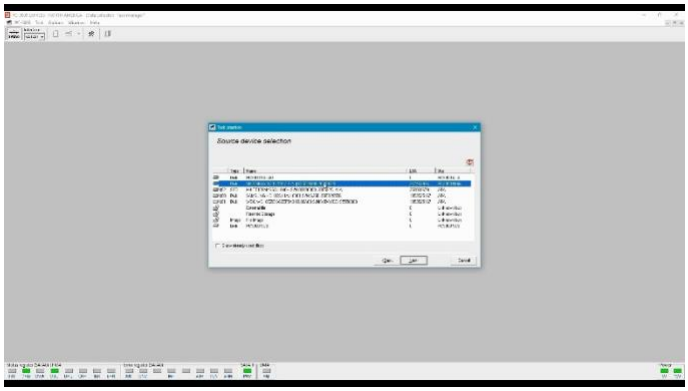
Если микропрограмма загружена успешно, следующим шагом будет восстановление таблицы трансляций, при помощи которой физические адреса переадресуются в логические. Таблица трансляций будет считана с микросхем памяти SSD. Повреждённые таблицы трансляций будут при необходимости пересобраны.



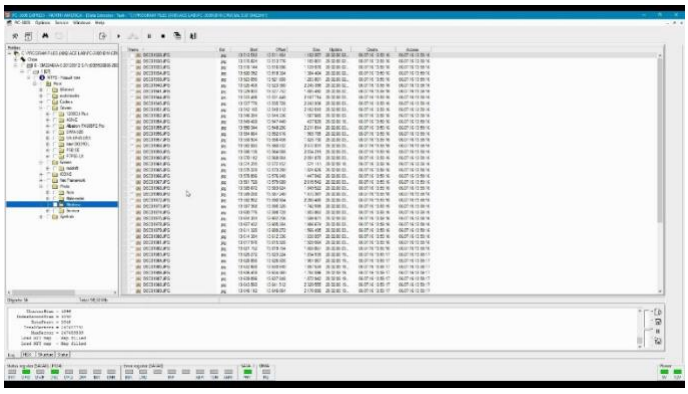
Таблицу трансляций необходимо загрузить в оперативную память (ОЗУ) контроллера:



Далее используется приложение Data Extractor, посредством которого осуществляется извлечение данных из накопителя. Данные сохраняются в виде образа. Обращаем внимание, что в этом режиме можно получить доступ и к тем блокам, для которых контроллером уже получена команда Trim, но содержимое которых ещё не было стёрто.



Данные можно извлечь и в виде файловой системы.



13. Сохранённые пароли: где хранятся, как извлечь и для чего использовать

Подбор пароля к некоторым форматам данных может быть чрезвычайно ресурсоёмким. Даже использование последних поколений графических ускорителей помогает весьма условно: скорость атак на тома BitLocker с аппаратным ускорением – всего несколько сотен паролей в секунду, документов в формате Microsoft Office 2017 – порядка нескольких тысяч паролей в секунду.

Использование словарных атак заметно повышает вероятность успешного взлома. В то же время атака по орфографическому словарю помогает не всегда: с одной стороны, количество возможных вариаций очень велико, с другой – именно ту вариацию, которую использует конкретный пользователь, автоматическая атака может пропустить.

Проблему решает использование сверхкомпактного словаря, составленного из найденных паролей самого пользователя. Согласно нашим исследованиям, такой словарь способен восстановить доступ к значительному числу защищённых ресурсов без использования вариаций. Использование вариаций, например, добавляющих до 4 цифр в конец каждого пароля (даже такая простая вариация увеличивает число вариантов для перебора в 10,000 раз) заметно увеличивает вероятность успеха. Ещё одна популярная вариация — использование заглавных букв.

13.1. Как извлечь пароли из компьютера пользователя

Для извлечения паролей пользователя с компьютера под управлением Windows используйте приложение Elcomsoft Internet Password Recovery, в котором имеется режим автоматического сканирования компьютера с сохранением найденных паролей в файл, который можно подключать в качестве словаря для атак (формат Unicode, убраны дубликаты). Для того, чтобы создать словарь, составленный из паролей пользователя, достаточно воспользоваться кнопкой “Export Passwords” и указать имя файла, в который будут сохранены пароли.

В качестве источников паролей Elcomsoft Quick Triage использует защищённые хранилища веб-браузеров и почтовых клиентов, включая Chrome, Internet Explorer, Microsoft Edge (современную и Legacy версии), Outlook, Windows Mail и некоторых других. Из браузеров извлекаются данные сохранённых паролей и форм автозаполнения, из почтовых клиентов – пароли к учётным записям POP3/IMAP/SMTP. Подробно об извлечении паролей рассказывается в разделе «**Извлечение паролей из браузера»**.

Для извлечения паролей из других источников (облачные сервисы, связка ключей iOS и macOS, базы данных программ управления паролями) используйте соответствующие инструменты.

13.2. Реализация атаки

Атака по словарю, составленному из паролей пользователя, показана на примере Elcomsoft Distributed Password Recovery. Последовательность атак необходимо настроить следующим образом.

1. На первом шаге используйте оригинальный список паролей пользователя (в нашем примере — файл “password-list.txt”) в качестве словаря без мутаций.

2. На втором этапе для того же словаря задаётся мутация, добавляющая цифры от 0 до 9999 в конец каждого пароля.

3. На последнем этапе включаются мутации Case/Digit/Year (предыдущую мутацию необходимо отключить).

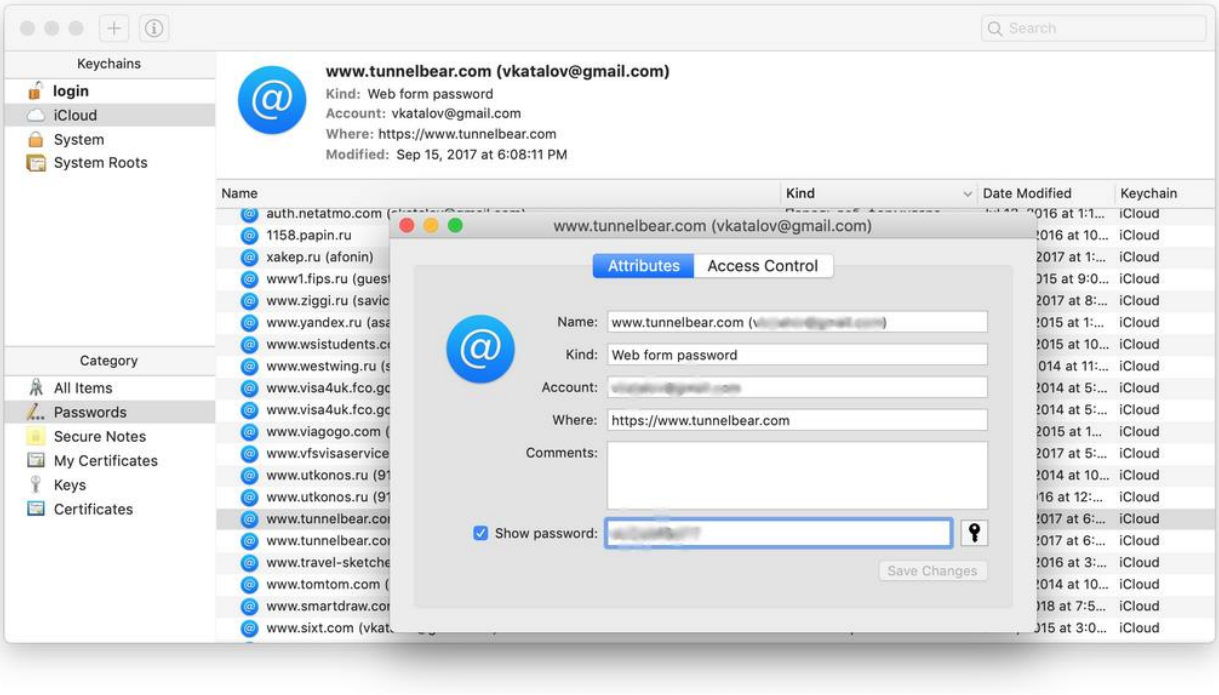
Первый этап будет отработан практически мгновенно. Второй этап проверяет в 10,000 раз больше паролей, чем содержится в самом словаре, поэтому может занять несколько секунд или минут. Последний этап заметно расширяет количество вариантов для проверки, и может занять от нескольких минут до нескольких часов в зависимости от количества паролей в словаре и скорости перебора. У среднестатистического пользователя с помощью данной последовательности раскрывается до 70% паролей.

13.3. Пароли из связки ключей macOS

На компьютерах под управлением macOS пароли пользователя хранятся в так называемой связке ключей. Содержимое связки ключей зашифровано, для доступа к ней необходима авторизованная пользовательская сессия либо пароль от учётной записи пользователя. Получить доступ к связке ключей macOS можно несколькими способами: штатным (через macOS Keychain Access) либо с использованием программы Elcomsoft Password Digger. Рассмотрим оба способа и различия между ними.

Метод 1: доступ через macOS Keychain Access

Если у пользователя есть компьютер Mac, то для доступа к паролям можно воспользоваться системной утилитой Keychain Access. Системная утилита открывает пароли по одному; более того, вам придётся вводить системный пароль от учётной записи либо пароль от связки ключей каждый раз (на новых Macbook с Touch ID достаточно приложить палец пользователя, но делать это придётся для открытия каждой записи).

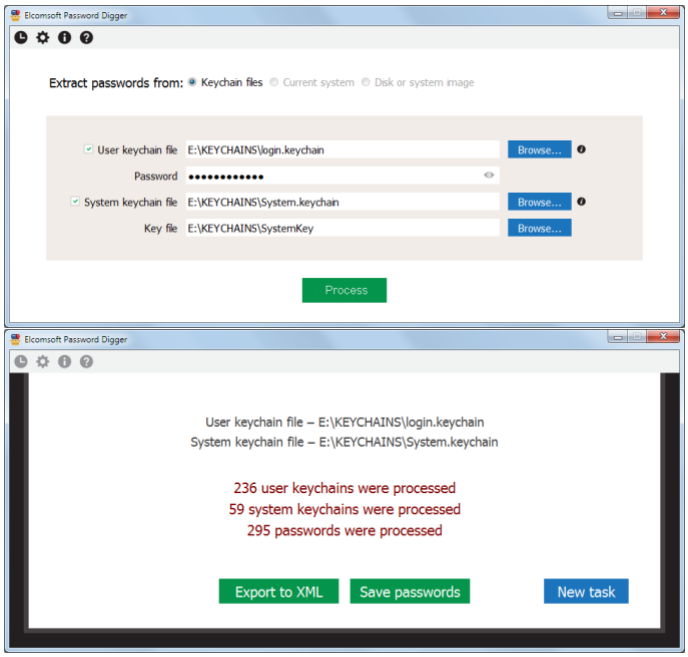


Плюсы этого метода в том, что для доступа не потребуется дополнительное программное обеспечение; доступны будут все записи. Минусов больше: доступ к паролям неудобный и последовательный; для доступа к каждой записи потребуется или вводить системный пароль (или пароль от связки ключей), или прикладывать палец пользователя. Обратите внимание: пароль от связки ключей может не совпадать с системным паролем. В таком случае вам придётся узнать и этот пароль.

Метод 2: доступ с использованием Elcomsoft Password Digger

Альтернативой последовательному просмотру записей является полное извлечение и расшифровка всей связки ключей целиком. Из компьютера с macOS (или образа диска) необходимо скопировать несколько файлов (login.keychain, System.keychain и SystemKey),

которые затем нужно будет открыть в приложении Elcomsoft Password Digger.[25] Для расшифровки записей потребуется указать системный пароль (пароль пользователя, из учётной записи которого была извлечена связка ключей). В некоторых случаях связка ключей может быть защищена отдельным паролем, не совпадающим с системным. В этом случае вместо пароля от учётной записи потребуется указать пароль от связки ключей.



Плюсы описанного метода в том, что извлекаются все данные как из пользовательской, так и системной связок ключей; все пароли извлекаются в один заход, доступны функции экспорта и сохранения паролей в файл; можно сразу создать словарь для подключения к Elcomsoft Distributed Password Recovery. В отличие от первого способа, данный метод доступен в том числе при анализе образов дисков. Для доступа нужен системный пароль или пароль от связки ключей.

При выборе между двумя способами рекомендуем остановиться на втором методе, использующем Elcomsoft Password Digger.

14. Когда перебор не нужен

В ряде случаев оригинальный пароль для доступа к защищаемой информации не нужен, а доступ к данным можно получить мгновенно или очень быстро. Такими случаями являются:

– пароли ограничений, не ограничивающие открытие документа для ряда форматов (все пароли Microsoft Office, кроме пароля на открытие).

– пароли на открытие документов в ряде форматов, включая:
  - QuickBooks;
  - Lotus SmartSuite, WordPerfect Office;

[25] https://www.elcomsoft.com/epd.html

- Sage (несколько продуктов);

– некоторые пароли PDF, включая пароль на изменения, печать, копирование и т.п. (Master password).

Кроме того, к данным некоторых типов можно получить доступ, используя уязвимости в алгоритмах шифрования. Данные не будут расшифрованы мгновенно, но атака с использованием уязвимости гарантирует результат (при соблюдении входящих условий) за гарантированный промежуток времени.

– некоторые архивы в формате ZIP, созданные архиваторами или встроенными в приложения библиотеками, использующими «классическую» схему шифрования, при выполнении ряда условия;

– документы, созданные в пакете «МойОфис»;

– документы, созданные в старых версиях Microsoft Office (атака по таблицам Thunder Tables) для форматов Office 97, Office 2000, а также Office XP и Office 2003 при сохранении в «совместимом» формате (по умолчанию).

15. Словари

Словарные атаки – одни из наиболее эффективных в случае, когда перебор паролей необходим. Одним из ключевых элементов словарных атак являются словари, под которыми подразумеваются списки слов, из которых по заданным правилам будут формироваться возможные пароли. Как выбор, так и качество исходного словаря – важнейшие факторы, влияющие на эффективность атаки.

В большинстве изученных нами руководств темы словарей поднимаются вскользь; упоминается необходимость использования качественных словарей. Но что из себя представляет «качественный» словарь, чем он отличается от «некачественного» и можно ли увеличить эффективность работы словаря? В этом разделе в форме вопросов и ответов мы даём конкретные рекомендации по использованию и составлению словарей для максимально эффективных словарных атак.

15.1. Чем коммерческие словари отличаются от тех, что можно найти в интернете?

Производитель ПО, как правило, поставляет словари, оптимизированные для его программного обеспечения. Такие словари, как правило, отсортированы в порядке, максимально эффективном для данного словаря с точки зрения производителя. Так, поставляемые нашей компанией словари общего назначения оптимизированы с точки зрения производительности перебора: вхождения упорядочены по длине слова (одна буква, две и т.п.). Такой способ сортировки связан с нашей реализацией механизма мутаций, и обеспечивает максимальную производительность именно с Elcomsoft Distributed Password Recovery. В то же время словари, в которых используются утечки, отсортированы по частоте встречаемости перечисленных в них паролей.

15.1.1. Выгодно ли сортировать словари по частоте?

Да, но не все. Сортировка по частоте имеет смысл в словарях “Top-100”, “Top-10 000” и им подобных, в которых используются реальные пароли пользователей (из утечек, извлечённыеиз компьютера пользователя и т.п.) В словарях естественных слов (например, общий словарь английского языка) такая сортировка большого смысла не имеет в силу использования механизма мутаций, и более эффективной является сортировка по длине слова (более короткие – сверху).

15.2. Какие бывают словари?

Существует несколько типов словарей, которые можно разбить на следующие группы.

Словари часто используемых паролей: глобальные и словари, разбитые по языковым группам. Сюда входят словари “Top-100”, “Top-10000” и им подобные, в которых используются реальные пароли пользователей (из утечек, извлечённые из компьютера пользователя и т.п.) Эти словари имеет смысл использовать для всех видов атак, включая «холодные».

Словари, разбитые по группам применения (узко сегментированные, например – словари «хакерских» терминов, список названия географических пунктов или словари имён из какого-либо языка). Такие словари нельзя использовать для «холодных» атак, если нет исходных данных о пользователе. Используются в атаках, если анализ паролей пользователя показывает, что он опирается на словарь соответствующего сегмента.

Общеупотребимые словари для различных языков. Например, сюда входят списки слов английского и русского языков, причём последний представлен как в написании символами кириллицы, так и в транслитерации на латиницу. Имеет смысл и использование национальных словарей. Общеупотребимые словари имеет смысл использовать для всех видов атак.

15.3. Всегда ли нужны мутации?

Мутации с разными словарями нужны не всегда. В частности, мутации несут весьма небольшую дополнительную пользу, если их использовать при атаке по часто используемым паролям из top-100, top-10000 и так далее. В то же время мутации более чем полезны при использовании тематических (специализированных) словарей и словарей общеупотребимых слов (например, словарь английского языка).

Мы различаем **два типа мутаций.**

Первый тип мутаций: **основные**. Их используют практически все пользователи. Например, регистр, добавить цифру в конец пароля, и так далее. Именно этот тип мутаций рекомендуется для «холодных» атак, когда о пользователе ничего не известно.

Второй тип мутаций: **специализированные**. Используются специфическими группами пользователей. Специализированные мутации не имеет смысла использовать, если нет исходных данных о пользователе. Используются в атаках, если анализ паролей пользователя показывает, что он опирается на словарь соответствующего сегмента.

15.4. Так всё-таки, можно ли использовать с EDPR словари из интернета?

Конечно же, можно! Однако перед подключением словаря к EDPR необходимо убедиться, что файл сохранён в поддерживаемом формате, вхождения отсортированы в корректном

порядке, приведены к нижнему регистру и очищены от дубликатов. Рекомендуем следующие варианты.

Для словарей общего назначения (словари естественных языков), а также для специализированных словарей (например, словари со списком имён, названий географических пунктов и т.п.):

– сохранить файл словаря в текстовом формате с расширением «.udic»; формат – Unicode LE (little-endian);

– все вхождения привести к нижнему регистру;

– отсортировать словарь по длине слов: вверху — самые короткие слова (из одного символа, двух и т.д.), ниже — более длинные;

– удалить дубликаты.

Для словарей, составленных из утечек реальных паролей (особенно это касается паролей пользователя, на данные которого проводится атака), действуют другие правила.

– сохранить файл словаря в текстовом формате с расширением «.udic»; формат – Unicode LE (little-endian);

– регистр слов оставляется оригинальным (допустимо создать копию словаря, в котором все вхождения приведены к нижнему регистру);

– отсортировать словарь по частоте: чем чаще встречается тот или иной пароль (повторимся, это относится к словарям, составленным из утечек реальных паролей), тем выше он должен быть в словаре;

– удалить дубликаты.

15.5. Как сформировать собственный словарь?

Что должно быть в собственном словаре? Имена собственные, фамилии (относящиеся к пользователю); даты в различных видах отображения; номера телефонов; номера документов (паспорта, водительское удостоверение и т.п.); пин-коды от любых карт, устройств; любые другие персональные данные; корневые (осмысленные или повторяющиеся, приведённые к нижнему регистру) фрагменты найденных паролей; клички домашних животных.

Сортировать такие словари следует по длине слова (короткие слова – сверху).

Все слова, которые заносятся в словарь, нормализуются (переводятся в нижний регистр). Это делается для более эффективной работы мутаций.

Оптимальный размер собственного словаря – порядка 10,000 вхождений, однако размер словаря имеет смысл коррелировать с объёмом мутаций: чрезмерно большой словарь и сильные мутации нерационально увеличат время атаки.

В EDPR предусмотрена возможность комбинирования слова из двух словарей: пароли будут составляться из комбинации двух слов, каждое из которых берётся из собственного словаря. В качестве двух словарей можно использовать разные словари или один и тот же словарь; в этом случае слова будут комбинироваться из него. Общее количество комбинаций растёт в геометрической прогрессии, и вычисляется как произведение количества слов в первом словаре на количество слов во втором.

15.6. Технические особенности

Словари для Elcomsoft Distributed Password Recovery должны сохраняться в текстовом формате с расширением «.udic»; формат – Unicode LE (little-endian). Сортировать словари следует по длине слова (короткие слова – сверху); это делается для более эффективной работы механизма мутаций. Дубликаты следует удалить, а слова привести к нижнему регистру.

Для словарей, составленных из паролей самого пользователя, делается исключение: в них предлагается сохранять пароли пользователя в оригинальном виде, не приведённом к нижнему регистру. Можно создать дополнительный словарь, в котором будет список паролей в нижнем регистре — для атаки с мутациями; однако лучше потратить время на вычленение корней — осмысленных или повторяющихся фрагментов паролей.

Кодировки UTF-8 и ANSI не поддерживаются.

16. Как ускорить перебор

Выше мы рассмотрели первый из двух способов ускорить восстановление пароля, который заключается в том, чтобы различными способами сократить множество паролей, внутри которого будет осуществляться перебор. Однако в ряде случаев (например, в случае с «холодной» атакой, см. раздел «**Файл с паролем. Владелец неизвестен»**) приходится проводить атаки по словарям с мутациями, а в случае их неуспеха – переходить к полному перебору. Скорость, с которой компьютер сможет перебирать пароли, в таких случаях критична.

Существует **несколько основных способов ускорить перебор**. В их число входят:

– *использование аппаратного ускорения.* В последние годы в качестве аппаратных ускорителей всё чаще используют бытовые видеокарты. В случае с Elcomsoft Distributed Password Recovery число поддерживаемых в рамках одного компьютера видеокарт ограничено в основном количеством доступных слотов расширения PCIe;

– *сбалансированная аппаратная платформа.* Для некоторых форматов файлов аппаратное ускорение может оказаться недоступным (например, в случаях, когда разработчики формата использовали специфический алгоритм хеширования, призванный предотвратить перебор на видеокарте). Для решения таких задач имеет смысл использовать компьютер с достаточно мощным центральным процессором и большим объёмом оперативной памяти;

– *параллельное использование нескольких компьютеров, объединённых в локальную сеть или связанных через интернет.* В случае с Elcomsoft Distributed Password Recovery увеличение числа компьютеров обеспечивает линейный рост производительности. Не забывайте, однако, об аппаратном ускорении каждого подключённого к распределённой вычислительной сети компьютера: единственный компьютер с видеокартой среднего класса в большинстве задач превосходит по производительности десятки, а иногда и сотни компьютеров, перебор пароля на которых выполняется силами только центрального процессора;

– *использование облачных вычислений.* Elcomsoft Distributed Password Recovery позволяет подключать виртуальные инстансы из облачных сервисов Amazon и Microsoft, которые работают наравне с физическими компьютерами. Не забывайте выбирать виртуальные машины, оборудованные графическими ускорителями!

Рассмотрим перечисленные способы подробнее.

16.1. Аппаратное ускорение – видеокарты и специализированные акселераторы

Современные видеокарты производства AMD и NVIDIA, а также встроенные в процессоры Intel и AMD графические ядра способны выполнять ряд специфических вычислений, разгрузив, таким образом, ресурсы центрального процессора.

Вычислительные возможности видеокарт в десятки раз превышают возможности центральных процессоров – но лишь для некоторых специфических видов вычислений, которые можно разбить на простейшие операции и выполнять в сотнях параллельных потоков. Большое количество вычислительных ядер (CU, Compute Unit), число которых может доходить до нескольких сотен, позволяет эффективно распараллелить нагрузку на видеокарту, достигнув таким образом преимущества в скорости перебора в сравнении с использованием ресурсов только центрального процессора в 50–250 раз для каждой установленной карты. Для большинства форматов, для которых доступно аппаратное ускорение, атаки на компьютере без видеокарты лишены практического смысла.

В качестве «эталонного» графического ускорителя для тестирования производительности мы используем модель NVIDIA GTX 1080. Несмотря на возраст этого ускорителя, он до сих пор обладает достаточным, а главное – хорошо известным уровнем производительности, который можно напрямую сравнивать с более современными моделями.

Технология асинхронных гетерогенных вычислений

В последние годы сама возможность выполнять вычисления на видеокартах привела к изменению рыночной ситуации, выразившейся в росте цен на мощные видеокарты в связи с ажиотажным спросом со стороны пользователей криптовалют, для добычи которых используются именно графические ускорители. Приобрести новую мощную видеокарту, цена которой вписывалась бы в установленный бюджет, стало проблемой: спровоцированный пользователями криптовалют спрос привёл к дефициту видеокарт, а дефицит – к росту цен.

Мы постарались скомпенсировать рост цен на видеокарты, разработав технологию асинхронных гетерогенных вычислений. Эта технология позволяет Elcomsoft Distributed Password Recovery одновременно использовать до 32 установленных в систему графических сопроцессоров разных моделей и производителей, от современных до достаточно старых. Поддержка гетерогенных вычислений позволяет добиться максимальной производительности при обновлении аппаратного обеспечения путём добавления, а не замены видеокарт. Таким образом, увеличить производительность системы становится возможным путём установки дополнительной бюджетной видеокарты, а не заменой старой модели на недоступную по цене более новую.

Подключив одну или несколько бюджетных видеокарт NVIDIA или AMD в любой комбинации, можно создать систему с отличным соотношением "цена/производительность", недоступным ни на каком другом аппаратном обеспечении.

16.1.1. Использование бюджетных видеокарт для ускорения перебора

В предыдущие годы для ускорения перебора использовались обычные игровые видеокарты — NVIDIA GeForce, AMD Radeon и другие. К сожалению, в 2020–2021 годах мощные видеокарты практически исчезли с полок магазинов в результате спроса со стороны добытчиков криптовалют. Мы провели замеры производительности на видеокартах, которые

остались доступны – в том числе по цене, и составили небольшой список рекомендованных моделей.

Модель безопасности современных средств защиты информации должна учитывать возможность подбора паролей злоумышленниками. Для замедления атак используются разные способы; самый простой и популярный из них — многочисленные (десятки и сотни тысяч, иногда — миллионы) итерации функции преобразования пароля в ключ. Чтобы взломать пароль, защищённый таким образом, нужны скорости, заметно превышающие возможности центрального процессора, даже если этот процессор — 16-ядерный Intel Core i9-12900K (его мы также протестировали)[26]. Требуемых скоростей можно достичь, запустив перебор не на центральном процессоре, а на мощных, а главное — многочисленных ядрах современных обычных игровых видеокарт.

Почему вычислительные возможности видеокарт настолько сильно превышают возможности центральных процессоров при сравнимом уровне энергопотребления и числе транзисторов? Дело здесь как в узкой специализации вычислений, так и в распараллеливании простейших операций на сотни потоков. Видеокарты способны выполнять некоторые простейшие целочисленные операции в десятках и сотнях потоков одновременно – но лишь для некоторых специфических видов вычислений, в число которых входит вычисление многих видов хэш-функций, которые, в свою очередь, применяются для преобразования текстового пароля в двоичный ключ шифрования. Большое количество вычислительных ядер (CU, Compute Unit) в видеокарте позволяет эффективно распараллелить нагрузку, достигнув подавляющего превосходства над обычным центральным процессором.

Таким образом, очевидно, что более мощные видеокарты, оборудованные большим количеством ядер CU (Compute Unit), смогут выполнять задачу по перебору паролей кратно быстрее. Также очевиден и следующий вывод:

Любая видеокарта лучше, чем CPU

Любая относительно современная дискретная видеокарта (а также очень и очень многие встроенные графические ядра) могут перебирать пароли значительно быстрее, чем центральный процессор. Использование даже очень старых видеокарт даёт зримое преимущество, чем и воспользовались наши разработчики, представив технологию асинхронных гетерогенных вычислений. Эта технология позволяет Elcomsoft Distributed Password Recovery одновременно использовать несколько установленных в систему графических сопроцессоров разных моделей и производителей, от современных до очень старых. С практической точки зрения поддержка гетерогенных вычислений позволяет добавлять, а не заменять видеокарты.

Сегодня мы протестируем современные видеокарты нижнего и среднего ценового сегмента.

---

[26] https://blog.elcomsoft.ru/2022/05/perebor-parolej-na-proczessorah-intel-alder-lake-12-go-pokoleniya/

Сюда вошли следующие модели:

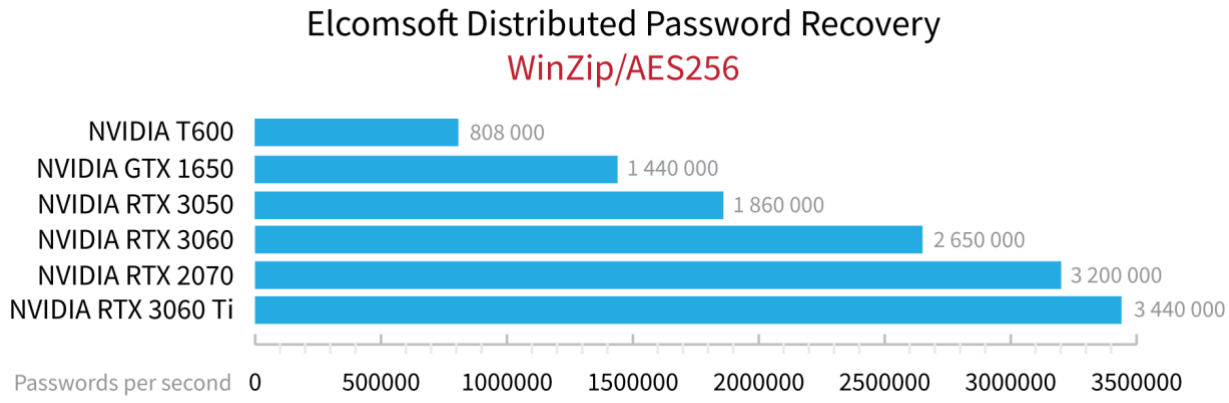
- NVIDIA GTX 1650;
- NVIDIA RTX 3050;
- NVIDIA RTX 3060;
- NVIDIA RTX 2070;
- NVIDIA RTX 3060 Ti.

Все видеокарты, за исключением RTX 2070, были протестированы в системе на основе процессора Intel Core i9-12900K. Модель RTX 2070 установлена в рабочей станции с процессором Intel Core i5-8500. На результаты тестирования видеокарт центральный процессор влияет в минимальной степени, поэтому мы сочли результаты теста корректными.

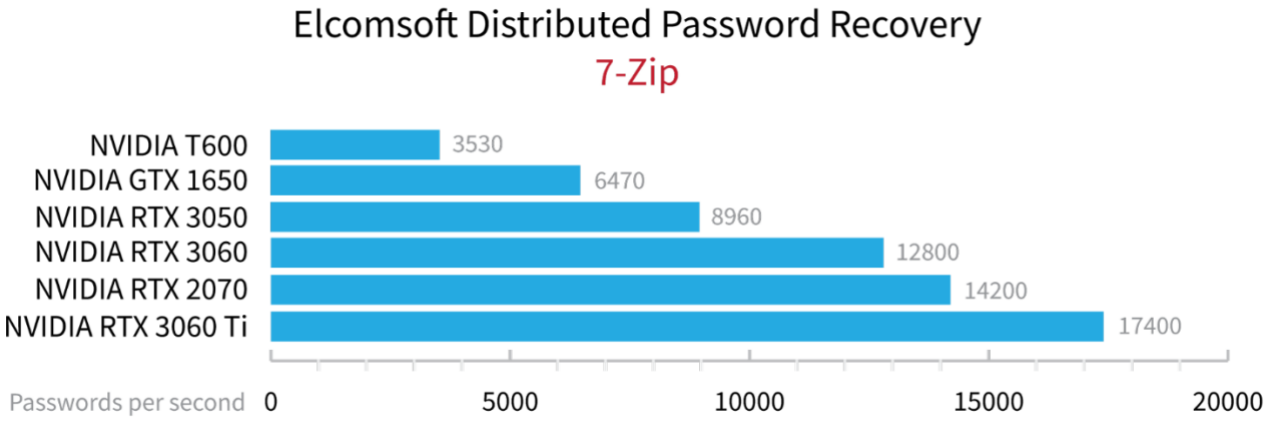
Результаты тестирования

Использовав в качестве тестовой нагрузки Elcomsoft Distributed Password Recovery, мы получили следующие результаты (цифры — число паролей в секунду, которые программа может перебрать на указанной аппаратной конфигурации).

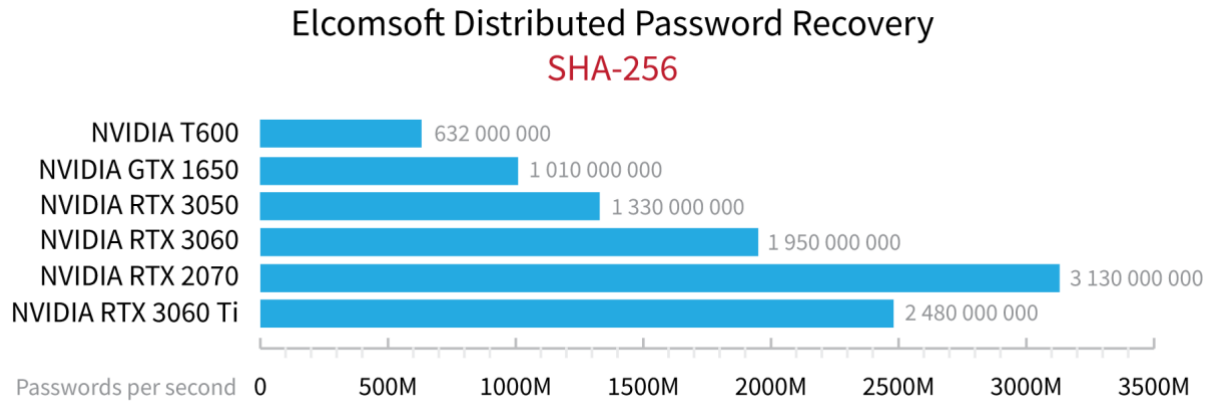
Перебор паролей к архивам ZIP вопросов не вызывает; скорость атаки напрямую зависит от мощности видеокарты, рост производительности — практически линейный.



Архивы 7Zip демонстрируют аналогичный тренд — с поправкой на большее число итераций хэш-функции, использующихся для конвертации пароля в ключ шифрования:



А вот на хэш-функции SHA-256 цифры для карты RTX 2070 выбиваются из общего ряда. Точного объяснения этому факту у нас нет; возможны варианты как в различиях в архитектуре тестируемых видеокарт, так и в том, что тестирование проводилось на разных компьютерах.



Соотношение цены и производительности

С учётом того, что в разных бенчмарках относительная производительность протестированных устройств различается (иногда — в несколько раз), а форматов файлов, которые не вошли в состав тестирования, и вовсе несколько сотен, дать однозначные рекомендации в отношении цены к производительности не удастся. По этой причине в качестве отправной точки мы выбрали тест WinZip/AES256 как один из наиболее прозрачных и оптимизированных для каждой платформы. В качестве цены использовались цены с немецких агрегаторов, деноминированные в евро.

Модель видеокарты	Скорость (паролей/сек)	Цена в евро	Соотношение цены/производительности
GTX 1650	1440000	186	1,00
RTX 3050	1860000	297	0,81
RTX 3060	2650000	377	0,91
RTX 2070	3200000	478	0,86
RTX 3060 Ti	3440000	549	0,81

Из таблицы можно сделать следующие выводы. Во-первых, рост производительности с повышением ценовой категории видеокарт — практически линейный, за исключением необъяснимого поведения карты RTX 2070 в тесте SHA-256. Во-вторых, среди протестированных бюджетных графических ускорителей в категории «цена/производительность» побеждает NVIDIA 1650, однако, лишь за счёт того, что эта устаревшая модель доступна по очень низкой цене. Наконец, последнее: в рамках линейки NVIDIA RTX 30 мы рекомендуем покупать видеокарту той модели, которая доступна в рамках выделенного бюджета — за возможным исключением моделей на основе RTX 3090,

использование которых сопряжено с повышенными требованиями к источнику питания и системам охлаждения и теплоотвода.

Существуют и другие бюджетные модели, в частности – новая линейка AMD Radeon. Производительность этой линейки ещё предстоит протестировать.

16.1.2. Энергоэффективность и теплоотвод

От чего зависит энергопотребление видеокарты, и почему при прочих равных более «горячая» карта выдаёт более высокую производительность? На производительность влияет несколько факторов. В их число входит архитектура и технологический процесс, по которому выполнен конкретный GPU (карты разных поколений при схожем потреблении могут различаться по производительности); тип кристалла (на этом подробно останавливаться не будем, но, к примеру, видеокарты NVIDIA RTX 3 060 Ti, 3070 и 3070 Ti основаны на одном и том же кристалле, а 3 080 — на другом); частоте работы графического процессора; наконец, в количестве вычислительных блоков.

Видеокарты способны выполнять некоторые простейшие целочисленные операции в десятках и сотнях потоков одновременно – но лишь для некоторых специфических видов вычислений, в число которых входит вычисление многих видов хэш-функций, которые, в свою очередь, применяются для преобразования текстового пароля в двоичный ключ шифрования. Большое количество вычислительных блоков (CU, Compute Unit) в видеокарте позволяет эффективно распараллелить нагрузку, достигнув подавляющего превосходства над обычным центральным процессором.

В то же время большее количество задействованных вычислительных блоков в рамках одного и того же типа кристалла приводит к линейному росту производительности — но и к линейному росту энергопотребления. А вот зависимость частоты графического процессора и его энергопотребления нелинейна: в тестировании видеокарты NVIDIA RTX 3090 Ti снижение максимального энергопотребления с 480 до 300 Вт (то есть, в 1.6 раза) привело к падению скорости всего на 13%. С тестированием можно ознакомиться перейдя на источник: Cool flagship instead of fusion reactor: the GeForce RTX 3090 Ti turns the efficiency list upside down with a 300-watt throttle and beats the Radeons | igor'sLAB.[27]

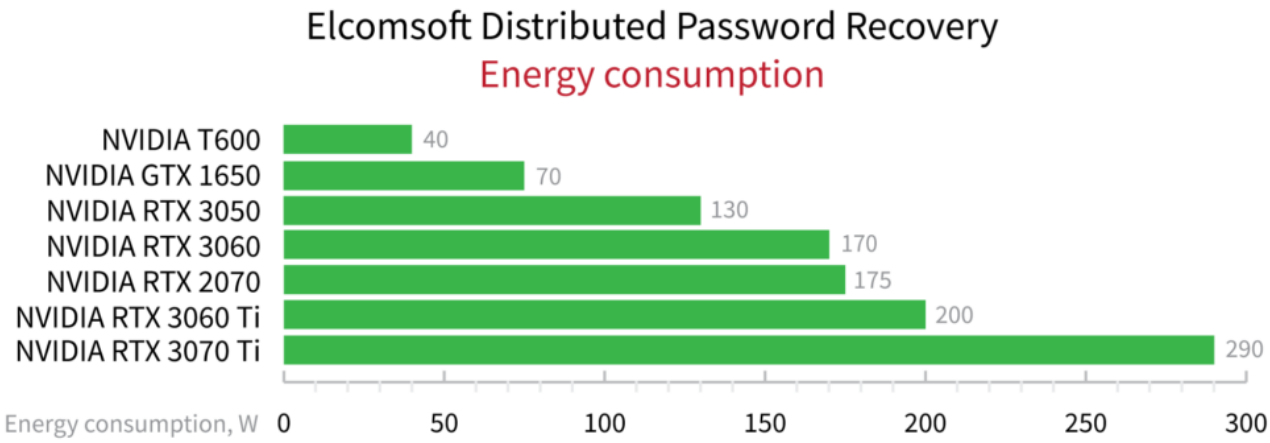
16.1.2.1. Тестирование энергоэффективности видеокарт

С одной стороны, в сети достаточно тестов видеокарт. С другой — практически никто не использует перебор паролей в качестве одного из бенчмарков. Мы протестировали ряд видеокарт актуального и предыдущего поколений. Помимо ранее изученных видеокарт, одним из участников тестирования стала мощная видеокарта NVIDIA RTX 3070 Ti в редакции Founders Edition. Максимальная потребляемая мощность этой видеокарты — впечатляющие 290 Вт; в большинстве обзоров её называют «неэффективным аутсайдером с высоким энергопотреблением». Проверим, насколько такая оценка соответствует действительности в сравнении с другими моделями.

---

[27] https://www.igorslab.de/en/cooler-breaker-station-fusion-reactor-when-the-geforce-rtx-3090-ti-with-300-watt-choke-sets-the-efficiency-list-on-its-head-and-beats-the-radeons/12/

Участники тестирования и их паспортное максимальное энергопотребление:

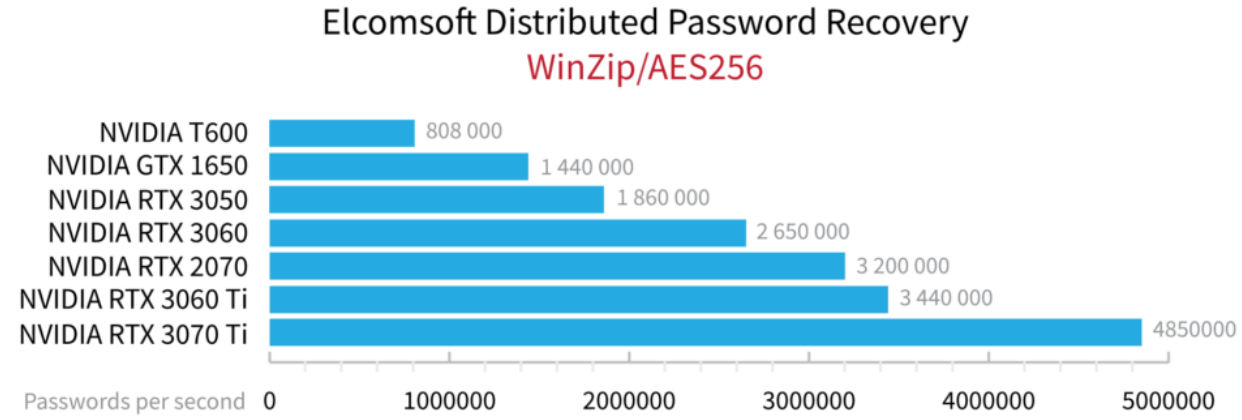


Все видеокарты, за исключением RTX 2070, были протестированы в системе на основе процессора Intel Core i9-12900K. Модель RTX 2070 установлена в рабочей станции с процессором Intel Core i5-8500. На результаты тестирования видеокарт центральный процессор влияет в минимальной степени, поэтому мы сочли результаты теста корректными.

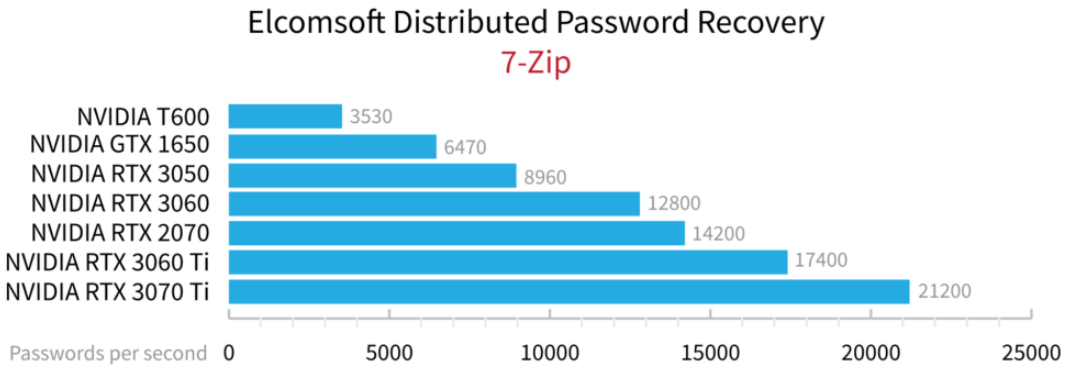
16.1.2.2. Результаты тестирования

Использовав в качестве тестовой нагрузки Elcomsoft Distributed Password Recovery, мы получили следующие результаты (цифры — число паролей в секунду, которые программа может перебрать на указанной аппаратной конфигурации).

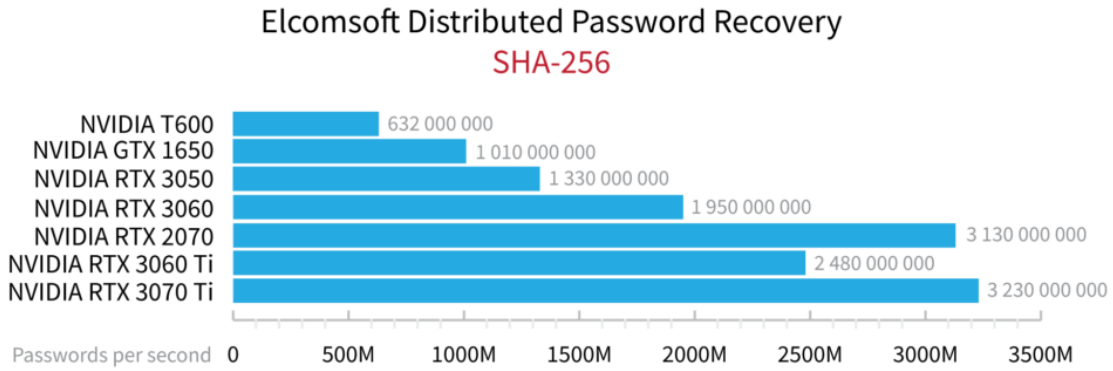
Перебор паролей к архивам ZIP вопросов не вызывает; скорость атаки напрямую зависит от мощности видеокарты, рост производительности — практически линейный.



Архивы 7Zip демонстрируют аналогичный тренд — с поправкой на большее число итераций хэш-функции, использующихся для конвертации пароля в ключ шифрования:

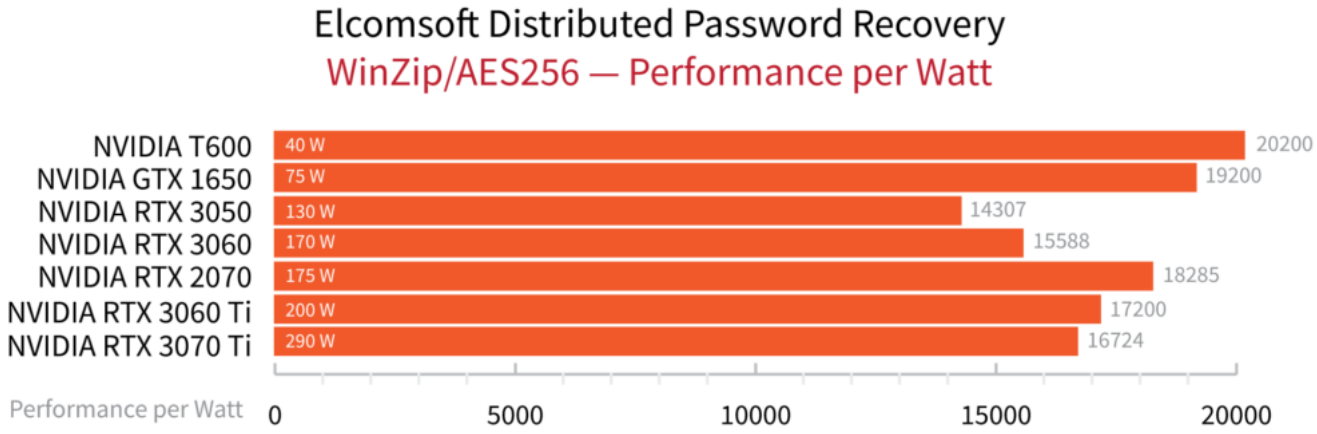


На хэш-функции SHA-256 цифры для карты RTX 2070 выбиваются из общего ряда. Точного объяснения этому факту у нас нет; дело, может быть, как в различиях в архитектуре тестируемых видеокарт, так и в том, что тестирование проводилось на разных компьютерах.

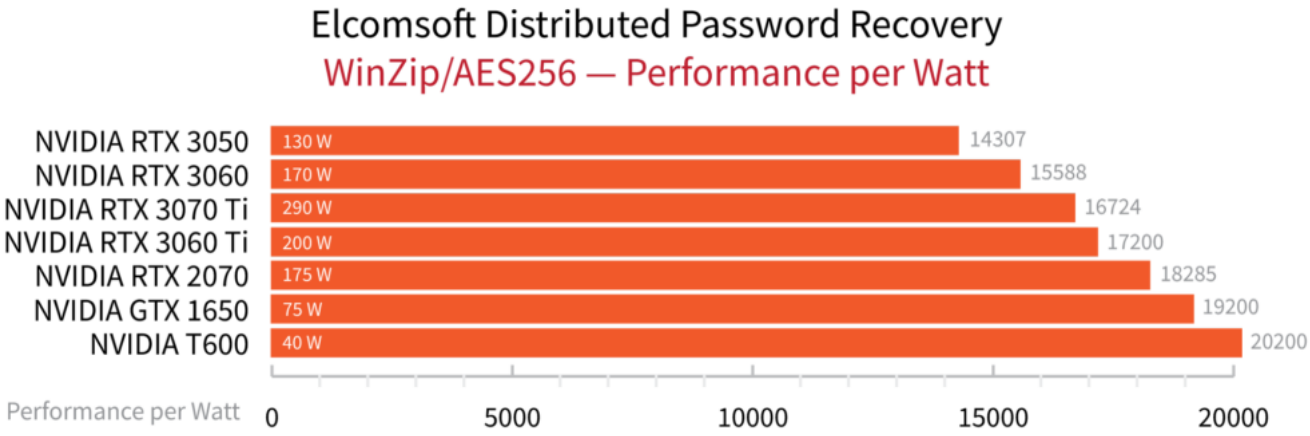


16.1.2.3. Таблица энергоэффективности

С учётом того, что в разных бенчмарках относительная производительность протестированных устройств различается (иногда — в несколько раз), а форматов файлов, которые не вошли в состав тестирования, и вовсе несколько сотен, дать универсальную оценку энергоэффективности видеокарт не удастся. По этой причине в качестве отправной точки мы выбрали тест WinZip/AES256 как один из наиболее прозрачных и оптимизированных для каждой платформы. Для оценки потребляемой мощности использовались паспортные данные соответствующих видеокарт.



Отсортируем чипы по энергоэффективности (производительность на ватт):



Признаться, результаты стали довольно неожиданными. Самая медленная видеокарта, модель NVIDIA Quadro T600 из «профессиональной» линейки, стала и самой энергоэффективной. Связано ли это с «удушением» установленного процессора или профессиональные карты обладают повышенной энергоэффективностью в принципе? Точно сказать не можем за отсутствием данных, но обзор серверной видеокарты NVIDIA A5000[28] говорит о высокой эффективности подобных решений.

Удивила и самая быстрая из протестированных видеокарт, NVIDIA RTX 3 070 Ti, являющаяся, по мнению многих обозревателей, «неэффективным аутсайдером с высоким энергопотреблением». Высокое энергопотребление? Да. Аутсайдер? Нет: на наших задачах карта обходит по энергоэффективности модели NVIDIA RTX 3 060 и 3 050, к эффективности которых претензий у сетевых обозревателей не возникает.

16.1.3. Когда аппаратное ускорение недоступно

Итак, запуск перебора на обычной бытовой видеокарте способен ускорить процесс в 50–250 раз, что кратно снижает безопасность зашифрованных данных и требует использования всё более длинных и сложных паролей. Очередным этапом противостояния щита и меча стала разработка специальных средств, призванных исключить возможность аппаратного ускорения.

Один из способов сделать перебор на видеокартах бесполезным – использование специальных функций преобразования пароля, использующих новый алгоритм хеширования Scrypt. Этот алгоритм сравним по скорости вычисления на центральном процессоре с традиционным SHA-256, однако был спроектирован таким образом, чтобы для него невозможно (или очень сложно и дорого) было бы реализовать атаку с аппаратным ускорением. **Суть аппаратного ускорения** состоит в распараллеливании потоков, а для вычисления хэша Scrypt требуется заметное количество оперативной памяти. Объём оперативной памяти в современных видеокартах позволяет одновременно запускать очень небольшое количество потоков, вычисляющих значение хэш-функции Scrypt; возникающие накладные расходы при этом заметно превышают выгоду от использования видеокарты.

---

[28] https://www.igorslab.de/en/nvidia-rtx-a5000-review-how-good-is-the-successor-of-the-quadro-rtx-5000/13/

Использование специфической хэш-функции – далеко не единственный способ, используемый разработчиками средств защиты данных для замедления перебора. Мы делаем всё возможное для того, чтобы переложить максимум доступных вычислений на аппаратный ускоритель; если это невозможно, то атака будет проводиться средствами центрального процессора. В таких случаях для ускорения перебора можно использовать как более быстрые процессоры, так и дополнительные компьютеры и/или виртуальные «облачные» серверы.

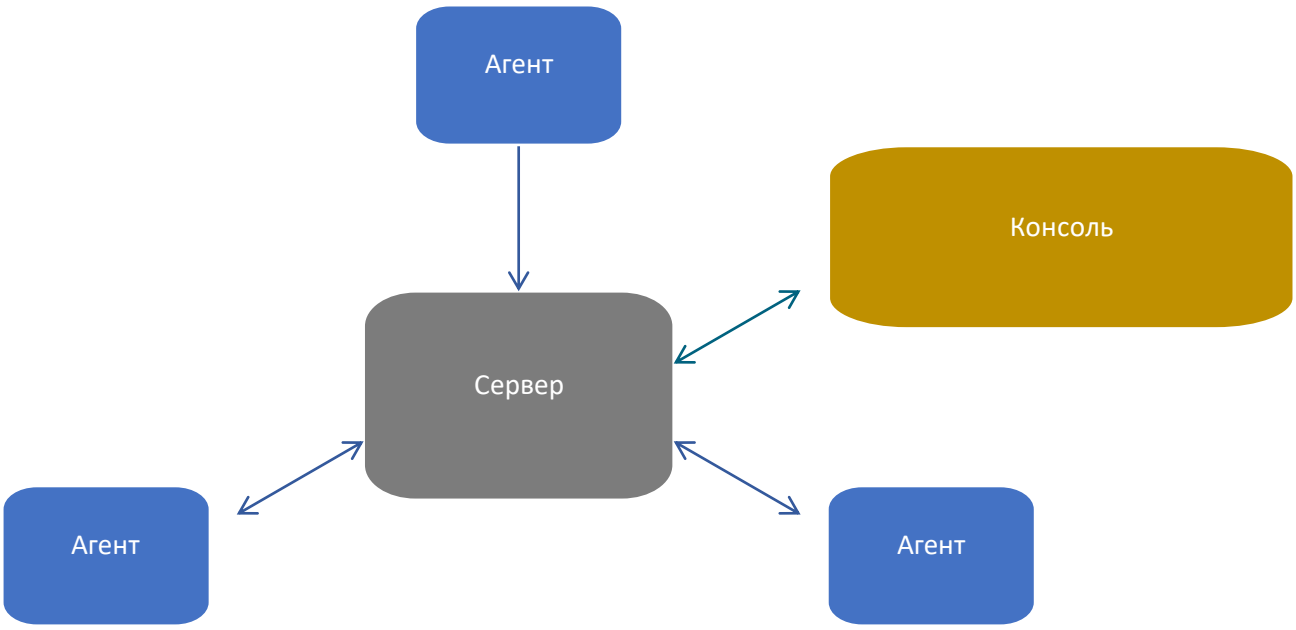
16.2. Распределённые атаки – это несложно

Ресурсов одного компьютера, даже оборудованного максимально возможным числом видеокарт для аппаратного ускорения перебора, может не хватить для завершения атаки за разумный срок. В таких случаях рекомендуется использовать распределённую атаку, использующую вычислительные ресурсы множества компьютеров, подключённых к одной локальной сети или связанных через интернет.

Elcomsoft Distributed Password Recovery позволяет достаточно легко настраивать атаки, использующие практически любое количество компьютеров. Благодаря линейному масштабированию продукт позволяет одновременно использовать до 10 000 рабочих станций, объединённых в локальную сеть или связанных через Интернет. Каждый компьютер будет работать над собственным подмножеством паролей; накладные расходы в этом случае незначительны, поэтому тысяча рабочих станций расшифрует документ ровно в тысячу раз быстрее, чем единственный компьютер. Сетевой трафик, создаваемый программой, минимален.

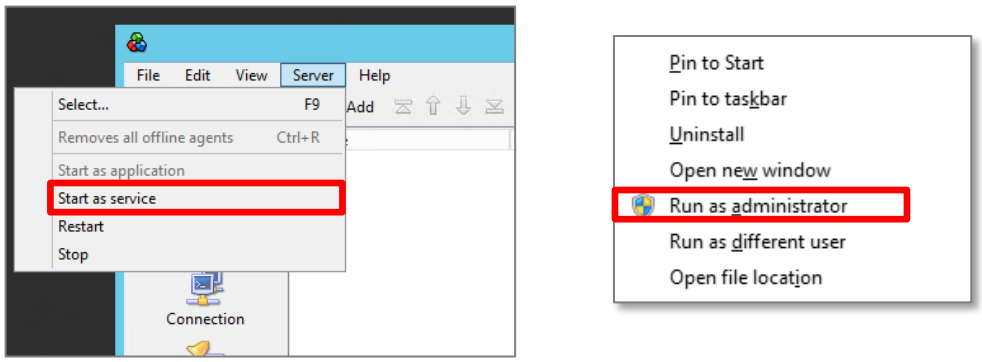
Управление процессом и настройка перебора осуществляется посредством рабочей консоли с любой рабочей станции, а автоматическая дистрибуция словарей позволяет удалённым агентам получать исходные данные для словарных атак в полностью автоматическом режиме.

Архитектуру EDPR можно изобразить в виде следующей схемы:



Сервер – часть программы, отвечающая за распределение задач, управление и коммуникацию с агентами. Если число агентов невелико (порядка нескольких десятков), то сервер можно запускать на одном компьютере с агентом: создаваемая им нагрузка на центральный процессор невелика. Если же число агентов превышает сотню, то для сервера имеет смысл использовать выделенный компьютер (в этом случае графический ускоритель в данном компьютере не понадобится: сервер не участвует в операциях перебора и не создаёт нагрузки на GPU).

Сервер не имеет отдельного пользовательского интерфейса; он может запускаться как пользовательское приложение или в виде системного сервиса (в этом случае его можно использовать даже тогда, когда на компьютере нет авторизованной пользовательской сессии).



Настройки сервера осуществляются через **консоль**.

Консоль – это пользовательский интерфейс программы; та её часть, с которой взаимодействует эксперт. Именно через консоль осуществляются настройки очереди задач и атак, настраивается работа агентов и выполняются все прочие операции, требующие вмешательства пользователя. Чаще всего консоль запускается на одном компьютере с сервером, однако её можно запускать и с любого другого компьютера, имеющего сетевой доступ к серверу.

Агент – это приложение, которое выполняет задачу собственно перебора. Агент получает задачи от сервера, выполняет свою часть работы и отчитывается серверу о результате. Агент – наиболее ресурсоёмкая часть Distributed Password Recovery; именно для работы агента используются вычислительные ресурсы процессора и видеокарт. Количество агентов, подключённых к одному серверу, может составлять до 10,000.

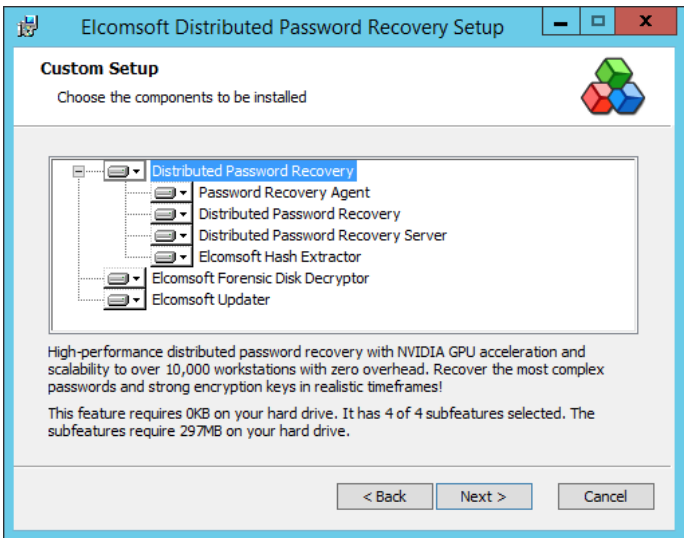
Таким образом, настройка распределённых атак распадается на следующие шаги:

1. Установка Elcomsoft Distributed Password Recovery на компьютер, который назначен на роль сервера. Автоматически будут установлены и управляющая консоль, и агент.

2. Установка агентов на остальные компьютеры в сети. Развёртывание можно осуществить как централизованно, с удалённой установкой агентов, так и интерактивно на каждом отдельном компьютере.

3. Запуск консоли и настройка атаки.

Для интерактивной установки достаточно запустить программу-установщик EDPR, в которой можно выбрать набор устанавливаемых на компьютер компонентов. При установке агентов достаточно отметить только “Password Recovery Agent” и “Elcomsoft Updater”, отключив остальные опции.



Обратите внимание: в состав продукта входит два дополнительных компонента, Elcomsoft Hash Extractor и Elcomsoft Forensic Disk Decryptor. О них рассказывается в соответствующих разделах руководства.

16.2.1.1. Удалённое развёртывание

Удалённое развёртывание Elcomsoft Distributed Password Recovery – удобный и быстрый способ установить агентов на множество компьютеров в локальной сети. При наличии административного доступа к удалённым компьютерам программа установки работает в автономном режиме и не будет выводить никаких запросов или диалогов.

В процессе удалённого развёртывание адрес сервера указывается в качестве параметра командной строки. Соответственно, в первую очередь обязательно установите, настройте и запустите сервер; устанавливаемые агенты будут автоматически подключаться к нему по мере их установки на удалённых компьютерах.

*Чтобы выполнить удалённое развёртывание, выполните **следующую команду**:*

msiexec /i "epr_agent_setup_ru.msi" /quiet STARTMENU="<0 | 1>" INSTALLDIR="<путь>" RUNASSERVICE="<0 | 1>" SERVERHOST ="<имя >" SERVERPORT = "<tcp-порт>" HIDEINDICATOR = "<0 | 1>"

В командной строке используются следующие параметры:

STARTMENU="<0 | 1>" — 0 — не создавать папку в меню «Программы», **= 1** создавать папку в меню «Программы».

INSTALLDIR="путь", папка на диске, куда будет установлена программа.

RUNASSERVICE="<0 | 1>" в значении «0» — запуск программы при входе пользователя в систему, «1» — запуск при старте Windows.

SERVERHOST ="<имя>" — имя или ip-адрес сервера, к которому будет подключаться агент.

SERVERPORT = "<tcp-порт>" — порт сервера, к которому будет подключаться агент.

HIDEINDICATOR = "<0 | 1>" — отвечает за то, будет ли у агента отображаться иконка рядом с часами (0 – не будет, 1 – будет).

Удалить установленные копии программы сразу с большого числа компьютеров в сети можно, ***выполнив следующую команду***:

msiexec /uninstall epr_agent_setup_ru.msi /quiet

Имея администраторские права, далее можно проделать следующие действия:

– запустить службу «Server», если она не запущена;
– обеспечить общий доступ к папке, где лежит файл «epr_agent_setup_ru.msi»;
– создать скрипт, который будет запускать установку клиентов. Пример скрипта agent_setup.cmd:

```
==========================================================

if not exist "%ProgramFiles%\Elcomsoft\Distributed Password Recovery\epr_agent_setup_en.msi" (

pushd \\server\share\directory

epr_agent_setup_ru.msi

)

==========================================================
```

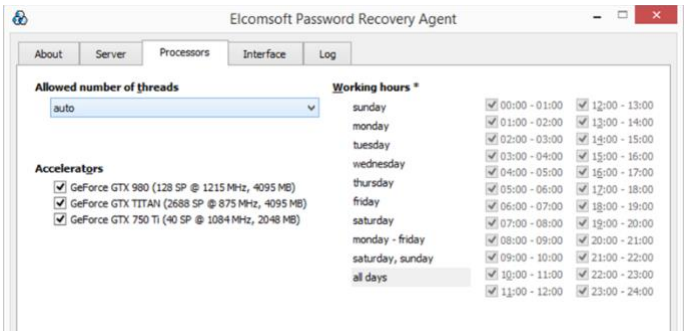
(\\server\share\directory — соответственно полный UNC путь к директории, где лежит дистрибутив);

– создать Group Policy для нужной группы пользователей и ней в качестве Logon Script прописать файл agent_setup.cmd.

Таким способом вы можете удалённо установить агентов на компьютеры в сети и удалённо запустить их. Запущенные агенты будут автоматически подключены к серверу.

16.2.1.2. Управление и настройка агентов

Управление удалёнными агентами ведётся посредством консоли, в которой можно настраивать работу агентов, управляя доступными для агента вычислительными ресурсами, в том числе по расписанию.



16.2.1.3. Настройки атаки

Подключённые удалённые агенты будут использованы в процессе атаки автоматически. Во время настройки очереди задач и атак вам не потребуется вручную выбирать агентов, которые будут заниматься перебором.

16.3. Используем облачные сервисы Amazon и Microsoft

Стойкая защита зависит не только от пароля, но и от формата данных, а точнее — используемых в нём алгоритмов шифрования и, в большей степени, функции преобразования пароля в двоичный ключ. Некоторые форматы способны гораздо дольше противостоять атакам. Например, в Microsoft Office начиная с версии 2013 используется защита, весьма устойчивая к перебору. Даже самые быстрые графические процессоры, установленные в современных видеокартах AMD и NVIDIA, позволяют достичь скоростей лишь в несколько тысяч паролей в секунду.

Если вам требуется высокая скорость восстановления, но использовать вычислительную сеть планируется лишь время от времени, собственный вычислительный центр может оказаться не лучшим решением. В качестве альтернативы рекомендуем освоить облачные вычисления с использованием виртуальных машин из сервиса Amazon EC2.

Сильная сторона облачных виртуальных машины — их моментальная доступность по требованию. С их помощью вы сможете быстро расширить вычислительные возможности вашей сети; в то же время, для них не нужно помещение, их не нужно покупать, амортизировать и обслуживать. Наконец, в любой момент времени можно заказать столько виртуальных машин, сколько необходимо для выполнения конкретной задачи, и свернуть их использование, как только необходимость в них отпадает.

Elcomsoft Distributed Password Recovery позволяет быстро наращивать мощность атак развёртыванием распределённой вычислительной сети в облаках Amazon EC2 и Microsoft Azure. Использование облачных вычислительных мощностей позволяет максимально быстро получить дополнительные мощности без необходимости капитальных инвестиций в собственный вычислительный центр. Работа в облаке позволяет быстро масштабировать вычислительные мощности, доступные Elcomsoft Distributed Password Recovery, под конкретные задачи, и так же быстро сворачивать сеть, когда в ней нет необходимости.

Облако Amazon – один из сервисов, доступных для расширения вычислительной мощности по требованию. Появившийся не так давно уровень сервиса EC2 сделал использование облачных инстансов ещё более интересным: каждая виртуальная машина Amazon P2 может быть оснащена до 16 вычислительными блоками GPU что делает их использование чрезвычайно привлекательным. Облачные инстансы можно добавлять по необходимости.

16.3.1.1. В каких случаях имеет смысл использовать облачные вычисления

Облачные вычисления широко распространены в ряде областей, а мощность доступных виртуальных машин вплотную подбираются к возможностям рабочих станций, а с недавнего времени — и превышают их. Новые экземпляры облачных виртуальных машин в сервисе Amazon EC2 не уступают в производительности современному компьютеру, оборудованному новейшим (и чрезвычайно дорогим) ускорителем NVIDIA RTX 3 080.

Возможность выполнять многие виды вычислений на мощных видеокартах привела к изменению текущей рыночной ситуации, выразившейся в росте цен и практическом исчезновении современных видеокарт из свободной продажи. Ажиотажный спрос со стороны добытчиков криптовалют сделал покупку новой видеокарты возможной лишь тогда, когда покупатель согласен с практически двойной переплатой. Собрать компьютер, оборудованный

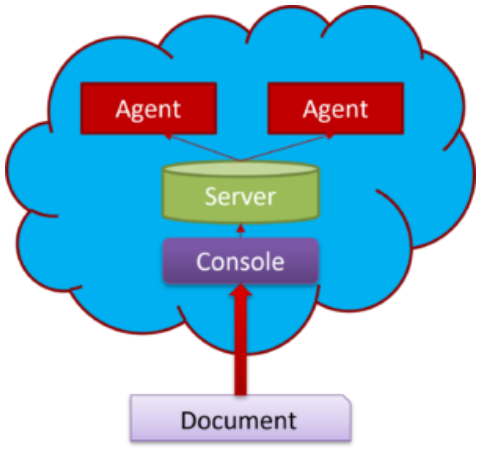
даже одной видеокартой, требует заметных затрат; полноценный вычислительный центр — серьёзных инвестиций.

В то же время специализированные ускорители (такие, как NVIDIA Tesla V100, A100, M60, T4 и A10G) остаются доступными крупным корпоративным заказчикам — таким, как Amazon. Если взлом паролей требуется не постоянно, а лишь время от времени, аренда облачных виртуальных машин, оборудованными одним или несколькими (в зависимости от бюджета) видеоускорителями становится безусловно выгодной в сравнении с построением стационарной инфраструктуры.

16.3.1.2. Варианты установки EDPR в облако

При подключении облачной архитектуры существует **три возможных способа установки EDPR**, и у каждого из них есть свои достоинства и недостатки.

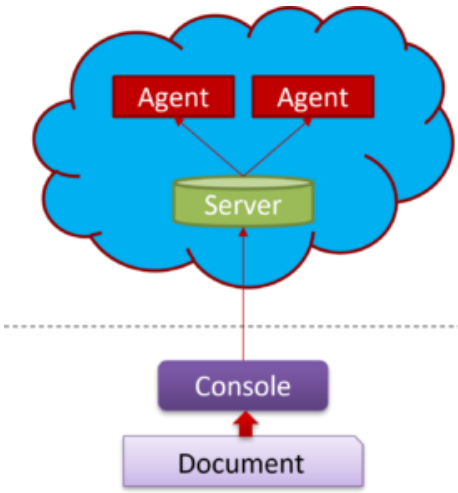
Первый способ — установка всего приложения целиком (включая агентов, сервер и консоль) в рамках облачной инфраструктуры. Обратите внимание, что в этом случае в облако попадёт весь файл или документ целиком. Для некоторых форматов эту проблему решает использование утилиты Elcomsoft Hash Extractor,[29] позволяющей передавать на сервер лишь необходимые для атаки метаданные шифрования (но не сам файл или документ), однако эта возможность доступна не для всех форматов данных.



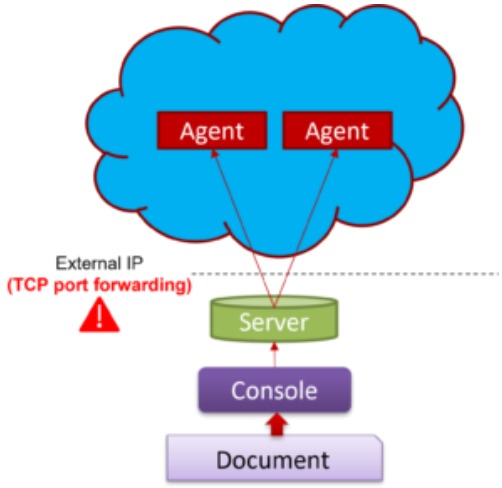
При этом варианте установки все части программы работают в облаке Amazon; доступ к консоли осуществляется удалённо.

Второй вариант установки также размещает всех агентов и сервер в облаке, однако консоль выносится за пределы облака и работает на локальном компьютере.

[29] https://blog.elcomsoft.com/2020/05/tighter-control-over-personal-information-with-attacks-on-encryption-metadata/



Наконец, **третий** вариант — установка в облако только агентов; и сервер, и консоль при этом установлены и работают в локальной сети.



Третий вариант установки *несколько сложнее* в сравнении с первыми двумя: для коммуникации между сервером и агентами необходимо, чтобы сервер был доступен извне по внешнему IP адресу, а порт 12121 был открыт и доступен. *В то же время именно этот способ обладает рядом весомых преимуществ в сравнении с остальными*, в число которых входят безопасность и масштабируемость решения.

– *защита персональных данных:* в облако не передаётся оригинальный файл или документ. Соответственно, его невозможно извлечь из облака, даже если удалённый сервер будет скомпрометирован;

– *безопасность:* найденный в облаке пароль сразу передаётся на сервер в зашифрованном виде, после чего удаляется из оперативной памяти облачной виртуальной машины. Перехватить пароль в процессе его передачи невозможно;

– *расширяемость:* сервер, работающий в локальной сети, может использовать не только облачные инстансы, но и ресурсы компьютеров в локальной сети.

В каких случаях имеет смысл использовать первый или второй варианты установки? Они подходят в случаях, когда Elcomsoft Distributed Password Recovery используется время от времени, а собственная стационарная инфраструктура для взлома паролей не используется. В

этом случае преимущества облачной установки проявляются в максимальной степени: приложение развёртывается и используется полностью в облаке в пределах чётко заданных временных рамок.

Подводя итог, мы рекомендуем следующие варианты установки EDPR:

– при наличии стационарной инфраструктуры (облачные инстансы подключаются в дополнение к существующим компьютерам): **третий вариант** установки.

– в случаях, когда безопасность и защита персональной информации критичны: **третий вариант** установки.

– при установке "с нуля" и эпизодическом использовании: **первый** или **второй** варианты.

Своеобразным водоразделом будет критичность защиты персональных данных и возможность использования Elcomsoft Hash Extractor [30]для извлечения метаданных шифрования.

16.3.1.3. Выбор типа виртуальной машины

Единственный компьютер, оснащённый видеокартой, превосходит распределённую вычислительную сеть, состоящую из десятков, и иногда и сотен компьютеров, ограниченных ресурсами центрального процессора. Это правило распространяется и на облачные вычисления. Для взлома паролей рекомендуем настроить вычислительные блоки одного из типов виртуальных машин, оборудованных графическими ядрами. В их число входят следующие варианты:

– Amazon EC2 P3 — до 8 NVIDIA Tesla V100 GPUs;
– Amazon EC2 P4 — до 8 NVIDIA Tesla A100 GPUs;
– Amazon EC2 G3 — до 4 NVIDIA Tesla M60 GPUs;
– Amazon EC2 G4 — до 4 NVIDIA T4 GPUs;
– Amazon EC2 G5 — до 8 NVIDIA A10G GPUs.

Наибольший интерес представляют самые современные вычислительные блоки Amazon G5, оборудованные последним поколением чипов NVIDIA. Каждый инстанс G5 может нести до 8 ускорителей NVIDIA A10G (в варианте **g5.48xlarge**), производительность которых на уровне видеокарт NVIDIA RTX 3 080. К сожалению, доступность самых мощных вычислительных блоков ограничена; если вам не удастся забронировать самые мощные инстансы, обратите внимание на менее производительные виртуальные машины.

Elcomsoft Distributed Password Recovery поддерживает виртуальные машины Amazon EC2 типов P2.x и P3.x.

16.3.1.4. Использование Amazon EC2 для перебора паролей

Elcomsoft Distributed Password Recovery поддерживает развёртывание агентов в учётную запись Amazon EC2. В зависимости от желаемого уровня производительности и ограничений по бюджету, вы можете выбрать те или иные конфигурации. В Elcomsoft Distributed Password Recovery доступно одновременное использование до 10 000 компьютеров, как локальных, так и облачных. Количество параллельно работающих машин ограничено типом лицензии.

[30] https://blog.elcomsoft.com/2020/05/tighter-control-over-personal-information-with-attacks-on-encryption-metadata/

Для настройки инстанса Amazon EC2 в Elcomsoft Distributed Password Recovery выполните следующие шаги.

Шаг 1. Сервер EDPR

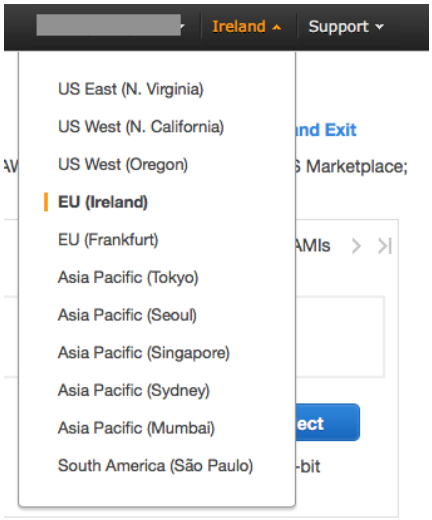
Настройте и запустите сервер EDPR. Проще всего установить сервер на локальный компьютер, но вы можете развернуть его и в облаке EC2.

Важный момент: сервер должен быть доступен извне по внешнему IP адресу, а порт 12121 должен быть открыт и доступен.

Шаг 2. Панель управления Amazon EC2

Авторизуйтесь в панель управления EC2 Management Console и нажмите “Instances”.

Шаг 3. Выбор региона

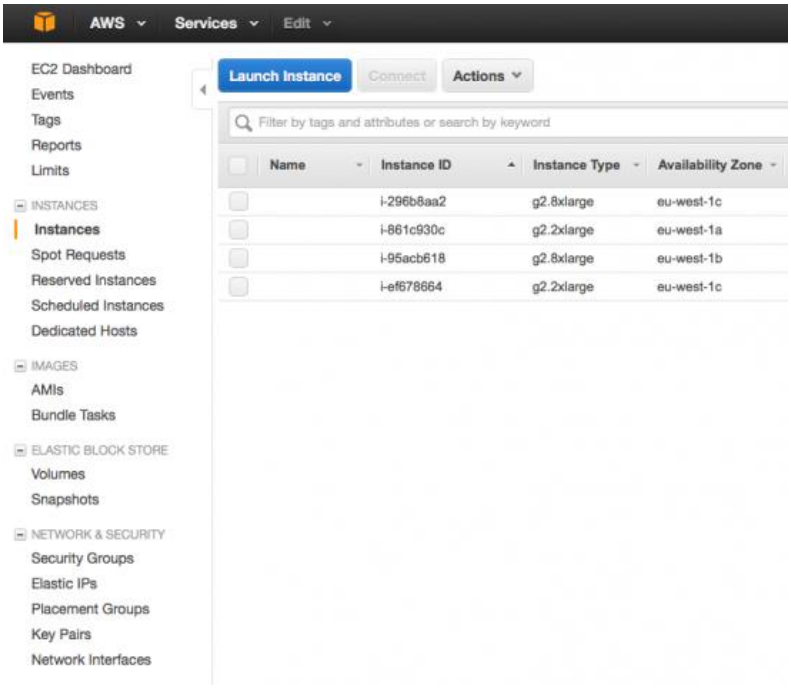


Выберите соответствующий регион. Инстансы, оснащённые графическими ускорителями, доступны в следующих центрах:

- US East (N.Virginia);
- US East (Ohio);
- US West (Oregon);
- Asia Pacific (Seoul);
- Asia Pacific (Sydney);
- Asia Pacific (Tokyo);
- EU (Ireland).

Шаг 4. Запуск инстанса

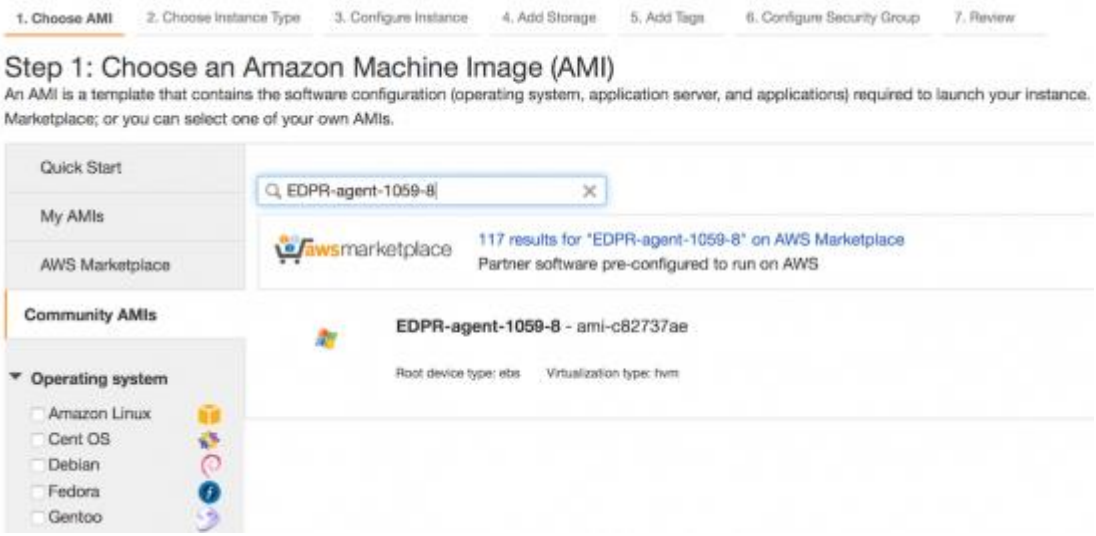
Кликните “Launch instance”.



Шаг 5. Выбор виртуальной машины

Выберите виртуальную машину “AMI” (Amazon Machine Image) в “Community AMIs”. Выберите “Community AMIs” и запустите поиск Elcomsoft AMI. Для этого в поисковой строке введите следующие строки.

- при использовании инстансов xlarge и 8xlarge: “EDPR-agent-1059-8”;
- при использовании инстансов 16xlarge: “EDPR-agent-1059-16”.



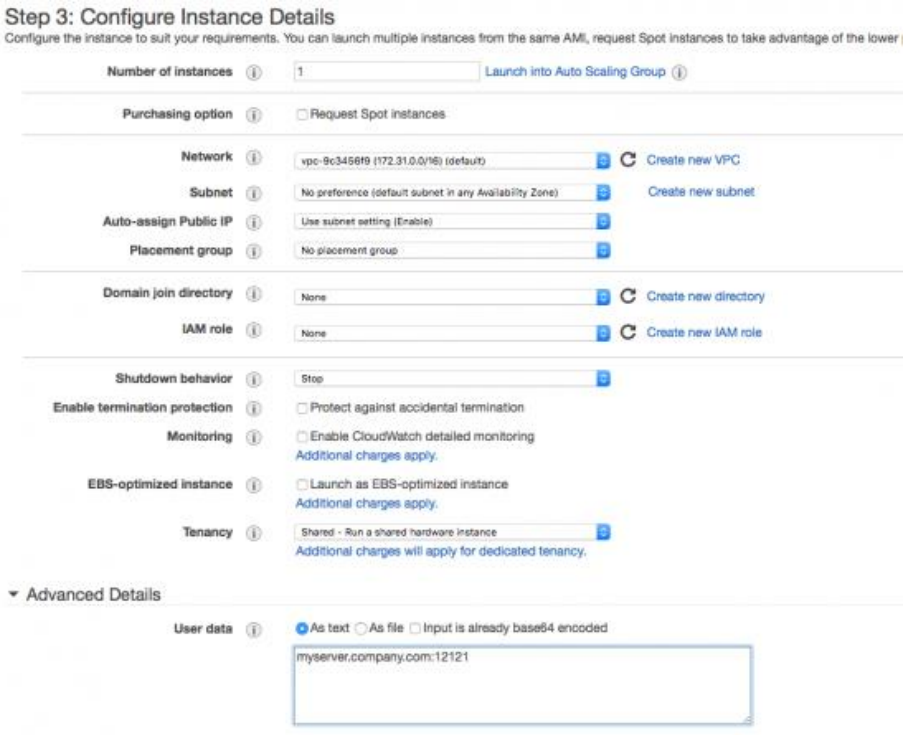
Шаг 6. Выбор конфигурации

Выберите конфигурацию виртуальной машины (тип инстанса P2). Типы инстансов отличаются числом доступных вычислительных ядер. Инстансы xlarge оснащены единственным видео-ядром (1 GPU), 8xlarge – восемью (8 GPUs), 16xlarge – шестнадцатью (16 GPUs).

В рамках бюджета имеет смысл выбирать конфигурации с максимальным числом вычислительных ядер, отдавая предпочтение меньшему числу виртуальных машин, оборудованных максимальным количеством графических ядер (GPU). В то же время реальная доступность инстансов, оборудованных более, чем одним ядром GPU, бывает ограничена. В таких случаях имеет смысл выбирать самые мощные из доступных инстансов.

Шаг 7: Настройка инстанса

Далее кликните “Next: Configure instance details” и укажите число инстансов, которые будут настроены. Разверните “Advanced details” и введите IP адрес и номер порта сервера в поле “User data”.



Шаг 8: запуск инстанса

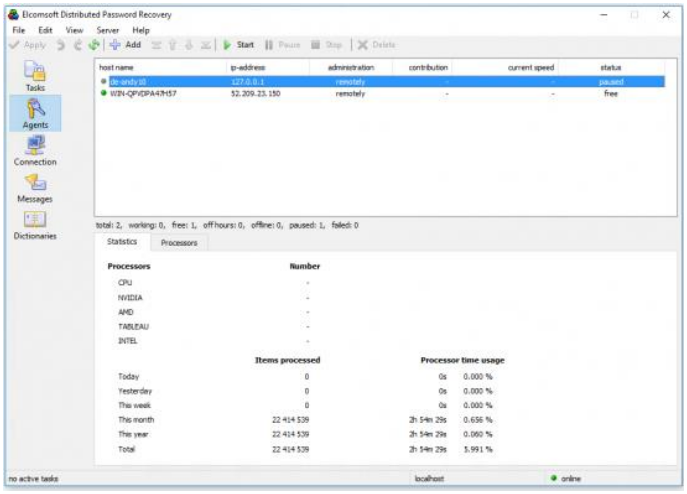
Кликните “Review and launch”. Убедитесь, что правильно заполнили формуляр, и кликните “Launch”.

Шаг 9: выбор пары ключей

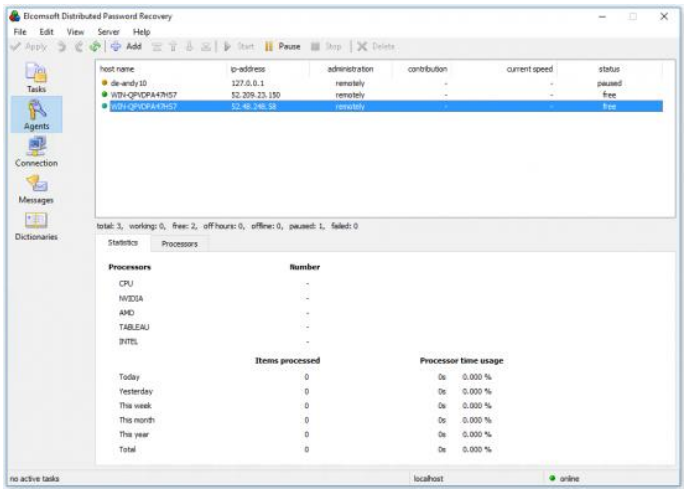
Выберите пару ключей или создайте новую.

Шаг 10: консоль EDPR

Созданные инстансы будут запущены. Через несколько минут информация о них появится в консоли EDPR:



Для запуска дополнительных агентов повторите шаги 1–7. Дополнительные агенты будут отображены в консоли EDPR, как только они будут запущены.



Обратите внимание: запуск агентов, использующих инстансы p2.16xlarge, занимает существенное время из-за инициализации значительного числа ядер CPU и GPU.

Не забывайте: инстансы Amazon EC2 оплачиваются по часам. Не забудьте своевременно освободить инстансы, когда нужда в их использовании отпадёт.

16.4. Мгновенное восстановление пароля

Помимо сохранённых пользователем паролей, мгновенному восстановлению поддаются и некоторые другие пароли. Яркие примеры – пароли от файлов QuickBooks (программой Advanced Intuit Password Recovery), ряд приложений для мгновенного обмена сообщениями (программой Advanced IM Password Recovery) и некоторые другие.

Кроме того, некоторые пароли необязательно восстанавливать – их достаточно сбросить для того, чтобы получить доступ к ограниченным функциям (таким, как распечатка или редактирование документа, копирование из него текста и т.п.) К подобным паролям относятся пароли (за исключением пароля на открытие) к файлам Adobe PDF (приложение Advanced PDF Password Recovery), ряд приложений Intuit (Advanced Intuit Password Recovery), и даже документы Microsoft Office (Advanced Office Password Recovery; мгновенно удаляются пароли ограничений, но не пароли на открытие документов).

17. Программы мгновенного обмена сообщениями

iMessage, Hangouts, Skype, Telegram, Signal, WhatsApp — эти приложения для мгновенного обмена сообщения постоянно на слуху. Проблема с безопасностью в любом из этих приложений немедленно попадает в новостные ленты, а возможность мгновенно извлечь оригинальный пароль – потенциальная проблема из разряда серьёзнейших. Неудивительно, что пароль от учётной записи из этих приложений извлечь нельзя — по крайней мере, не из самого приложения и не из сохраняемых им на компьютере данных. Но есть и другие, менее распространённые программы. alTalk, Pigin, Psi Jabber client, Gadu-Gadu, Gajim, Trillian, BigAnt и Brosix и множество подобных объединяет модель безопасности, позволяющая извлечь и расшифровать оригинальный пароль от соответствующей учётной записи.

В большинстве современных программ для мгновенного обмена сообщениями пароль для входа в учётную запись либо не используется вовсе, либо используется в качестве опционального второго фактора аутентификации. Даже в тех редких случаях, когда для входа в мессенджер используется связка логина и пароля, в системе, как правило, не сохраняется ни оригинальный пароль, ни его хэш.

Тем не менее, в ряде случаев пароль извлечь всё-таки можно, а для некоторых других приложений возможен перенос активной пользовательской сессии на другой компьютер без участия пароля. Ниже мы рассмотрим некоторые популярные приложения мгновенного обмена сообщениями и доступные для них варианты.

WhatsApp

WhatsApp не использует пароль для входа в учётную запись. В процессе входа в учётную запись осуществляется привязка устройства по номеру телефона. Авторизация нового устройства отменяет авторизацию предыдущего: WhatsApp может работать на единственном смартфоне, а приложение для компьютера требует привязки к устройству с SIM-картой. При этом первая перепривязка возможна в любой момент, а для перепривязки во второй и последующие разы предусмотрена увеличивающаяся задержка. В качестве второго фактора[31] аутентификации пользователь может выбрать PIN-код, который используется только для подтверждения входа в учётную запись и не сохраняется на устройстве.

Telegram

Похожая схема авторизации используется в Telegram, однако для привязки устройства достаточно ввести 6-значный цифровой код, который доставляется через приложение Telegram на все ранее зарегистрированные устройства. В отличие от WhatsApp, Telegram может работать на множестве устройств одновременно, не ограничивая пользователя и не заставляя перепривязывать устройства.

Извлечь или восстановить любой атакой пароли от WhatsApp или Telegram невозможно. Пароль, защищающий вход в учётную запись, не имеет отношения к защите самого мобильного приложения PIN-кодом. В Telegram для Android обе настройки находятся в разделе Settings – Privacy & Security; Passcode Lock относится к защите приложения, а Two-Factor Authentication настраивает пароль в качестве второго фактора на вход в учётную запись Telegram.

[31] https://faq.whatsapp.com/general/verification/how-to-reset-your-two-step-verification-pin/?lang=en

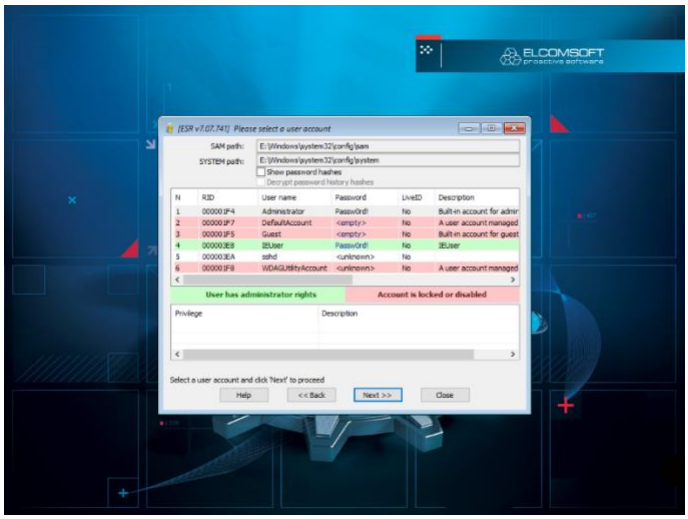
Skype

Совершенно иначе работает аутентификация у **Skype**. Выпущенный в своё время независимой компанией, Skype не использовал привязку к телефонному номеру, полагаясь на стандартный способ аутентификации по логину и паролю. После покупки компанией Microsoft пользователи смогли входить в учётные записи Skype, авторизуясь в учётной записи Microsoft Account. На компьютерах с Windows 8 и Windows 10 вход в Skype с данными Microsoft Account и вовсе происходит автоматически: мессенджер просто использует уже имеющиеся в системе реквизиты для входа.

Такой подход, с одной стороны, всё ещё не позволяет извлечь пароль (он не хранится ни в открытом, ни в зашифрованном виде), но позволяет провести ряд действий для получения доступа к истории переписки.

Во-первых, можно провести атаку на пароль к Microsoft Account, который пользователь использует для входа в Windows. Это не сработает, если для входа в систему используется локальная учётная запись, не привязанная к Microsoft Account. В то же время в случае, когда такая привязка есть (т.е. для входа в систему используются учётные данные Microsoft Account), атака происходит с высокой скоростью, а восстановленный в результате пароль позволяет авторизоваться в Skype, получить доступ к файлам OneDrive, включая содержимое "персонального сейфа", и проделать ряд других следственных действий, описанных в статье: Анализ данных из учётных записей Microsoft: Timeline, OneDrive и Personal Vault | Блог Элкомсофт (elcomsoft.ru)[32].

Как именно восстановить пароль от учётной записи Windows? Способов множество. Самый быстрый из них — загрузить систему с использованием Elcomsoft System Recovery, извлечь базы данных с хэшами паролей и запустить атаку в Distributed Password Recovery. Возможные подводные камни – шифрование диска BitLocker и использование двухфакторной аутентификации для защиты учётной записи: Microsoft может затребовать дополнительную верификацию даже в случаях, когда двухфакторная аутентификация не включена.



[32]https://blog.elcomsoft.ru/2021/08/analiz-dannyh-iz-uchyotnyh-zapisej-microsoft-timeline-onedrive-i-personal-vault/

Ещё один способ узнать пароль от Skype – извлечь пароли из связки ключей iOS при помощи Elcomsoft Phone Breaker,[33] если есть доступ к соответствующему устройству пользователя. Для этого понадобится пароль от учётной записи Microsoft, который можно найти по входам на сайты hotmail.com, live.com, outlook.com, microsoft.com, office.com и некоторым другим.

Пароли можно извлечь и из учётной записи Google программой Elcomsoft Cloud Explorer. Этот вариант доступен только в том случае, если известен пароль пользователя от учётной записи Google Account.

Если есть доступ к авторизованной сессии, то можно извлечь пароли, которые хранятся в веб-браузере пользователя программой Elcomsoft Quick Triage. Обратите внимание на пароли к учётным записям Microsoft.com, Hotmail.com, outlook.com, live.com.

Ещё одна возможность, доступная, если у вас есть доступ к авторизованной сессии, а пароля к учётной записи не обнаружено, — перенос сохранённых реквизитов для входа в Skype с компьютера пользователя на другой, с которого будет осуществляться анализ. Для этого используется приложение Advanced IM Password Recovery — функция "копирование/восстановление данных авторизованной сессии (Skype)".

17.1. Извлечение паролей из программ мгновенного обмена сообщениями

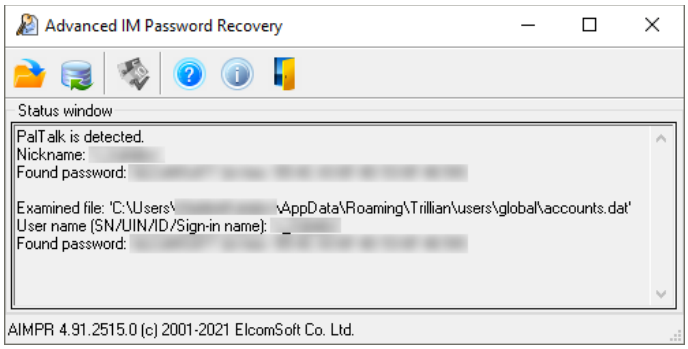
Выше мы рассмотрели способы аутентификации и привязки к устройствам популярных программ мгновенного обмена сообщениями. Существует немалый пласт мессенджеров, которые в том или ином виде сохраняют на компьютере пароли. К таким приложениям относятся мессенджеры из следующего списка: ICQ и ICQLite, AOL Instant Messenger, AIM Triton, AIM Pro, Yahoo! Messenger, MSN Messenger, Windows Live Messenger, Google Talk, Trillian и Trillian Astra, Odigo, Jabber IM, популярный альтернативный клиент ICQ — Miranda, Tencent QQ, Ipswitch Instant Messenger, Psi Jabber client, QIP Infium, Gizmo Project, MySpace IM, Exodus, Gadu-Gadu, Mail.Ru Agent, Just Another Jabber Client, Pidgin и многие другие, перечисленные на странице продукта.[34] Также поддерживаются мессенджеры PalTalk, Pigin, Psi Jabber client, Gadu-Gadu, Gajim, Trillian, BigAnt, Brosix.

Для некоторых мессенджеров приложение Advanced IM Password Recovery предоставляет возможность извлечения логинов и паролей, во многих случаях – мгновенно. Общее число поддерживаемых программ мгновенного обмена сообщениями – более 70. Не все из них дожили до наших дней, многие программы до сих пор пользуются популярностью.

Нужно отметить, что обновлённые версии некоторых из перечисленных приложений не хранят оригинальные пароли на компьютере пользователя. Для таких программ поддерживается извлечение данных, необходимых для последующей аутентификации с целью переноса авторизованной сессии на другой компьютер. Эта функция используется для таких приложений, как Skype, которые не хранят пароль на компьютере. Для этих приложений поддерживается функция копирования и восстановления данных аутентификации, что позволяет перенести

[33] https://www.elcomsoft.ru/eppb.html
[34] https://www.elcomsoft.ru/aimpr.html

авторизованную сессию с компьютера пользователя на компьютер эксперта, позволяя проводить экспертизу на собственном компьютере эксперта, а не на компьютере пользователя.



18. Зашифрованные диски и крипто-контейнеры

Шифрование диска, раздела или использование зашифрованного виртуального диска – чрезвычайно распространённые способы сокрытия улик. В отличие от шифрования файловой системы, которое часто используется в сетевых хранилищах, шифрование диска позволяет скрыть не только содержимое файлов, но и структуру файловой системы, число и размер файлов и каталогов, а также все прочие метаданные, включающие даты создания и модификации файлов. В ряде случаев шифрование диска способно скрыть даже общий объём данных, а в предельном случае благодаря использованию вложенных контейнеров – и сделать недоказуемым сам факт наличия зашифрованной информации.

Получить доступ к содержимому зашифрованных дисков можно несколькими способами. Анализ авторизованной пользовательской сессии в момент, когда зашифрованный диск смонтирован в системе – самый простой способ. Во время анализа авторизованной пользовательской сессии можно извлечь содержимое оперативной памяти компьютера (инструментом Elcomsoft Forensic Disk Decryptor[35]), после чего снятый образ сканируется на предмет поиска ключей шифрования. Образ оперативной памяти включённого компьютера с разблокированными зашифрованными дисками можно извлечь и другими способами – например, используя уязвимость в протоколе FireWire или методом заморозки модулей памяти. Об этих методах мы расскажем отдельно.

Для компьютеров, которые на момент извлечения находились в состоянии «гибридного» сна или гибернации, ключи шифрования от некоторых зашифрованных дисков можно обнаружить анализом файлов подкачки и гибернации. Для этого также используется Elcomsoft Forensic Disk Decryptor.

В случае, когда для хранения ключа шифрования используется модуль TPM2.0 (с выходом Windows 11 их популярность будет только расти), можно попробовать использовать одну из нескольких уязвимостей TPM, о которых также будет рассказано ниже. Отметим, однако, что в качестве замены аппаратному модулю TPM в подавляющем большинстве современных платформ используются технологии виртуализации Intel PTT (Platform Trust Technology) и её аналог от AMD – firmware Trusted Platform Module (fTPM). В отличие от аппаратных

[35] https://www.elcomsoft.ru/efdd.html

сопроцессоров TPM, эти технологии не нуждаются в специальном оформлении ввоза на территорию Таможенного Союза. В то же время эти технологии успешно справляются с ролью сопроцессоров безопасности, не имея характерных для отдельных чипов TPM уязвимостей.

Даже тогда, когда для хранения ключа шифрования используется аппаратный модуль безопасности (такой, как TPM2.0 или чип Apple T2), ключ восстановления доступа в ряде случаев попадает в облачную учётную запись пользователя, откуда его можно извлечь. Для шифрования BitLocker Device Protection ключи по умолчанию сохраняются в Active Directory (для корпоративных компьютеров) либо в личную учётную запись Microsoft Account того пользователя, который первым вошёл в систему с административными привилегиями и с логином от Microsoft Account (а не локальной учётной записью Windows). Такие ключи доступны по адресу: http://windows.microsoft.com/recoverykey[36] или https://onedrive.live.com/recoverykey[37]. У пользователей macOS ключи от FileVault 2 также попадают в облако; извлечь их оттуда можно при помощи нашей утилиты Elcomsoft Phone Breaker, если у эксперта есть возможность авторизоваться в Apple ID пользователя.

В ряде случаев доступ к зашифрованному диску защищается паролем. Это относится к большинству дисков, созданных VeraCrypt; внешним дискам, зашифрованным BitLocker to Go, а также к дискам, защищённым BitLocker, за исключением загрузочного. Пароль от зашифрованного диска или контейнера можно подобрать, используя специализированные атаки. Метод полного перебора малоэффективен для взлома зашифрованных дисков в силу того, что их защита в первую очередь ориентирована на противостояние именно таким атакам.

18.1. Типы зашифрованных дисков

Все зашифрованные диски объединяет то, что для пользователя системы они мало отличаются от обычных дисков. Зашифрованному тому можно назначить отдельную букву накопителя или смонтировать его по определённому пути – точно так же, как и обычный раздел. Детали реализации, однако, сильно отличаются в зависимости от типа зашифрованного диска.

Так называемое ***«полнодисковое шифрование»*** защищает блочное устройство целиком; разбивка на разделы ведётся уже внутри зашифрованного диска. На практике этот подход используется сравнительно нечасто; пример реализации – технология LUKS.

Гораздо чаще под «шифрованием диска» понимается шифрование одного из разделов, созданных на блочном (физическом) накопителе. Таким образом функционирует распространённая система шифрования BitLocker; в этом режиме могут работать LUKS, VeraCrypt и подобные системы. Обратите внимание: тома BitLocker, созданные на твердотельных накопителях, передают накопителю данные о неиспользуемых страницах для их очистки командой Trim. Эта особенность заметно увеличивает скорость записи данных и срок службы SSD накопителя, при этом позволяя узнать объём зашифрованной информации.

В системах шифрования диска выделяются так называемые «крипто-контейнеры». Крипто-контейнер – это один или несколько файлов-контейнеров, которые могут храниться в файловой системе как на обычном, так и на зашифрованном диске. Эти контейнеры содержат образ зашифрованного диска, при монтировании которого в системе появляется новый

[36] http://windows.microsoft.com/recoverykey
[37] https://onedrive.live.com/recoverykey

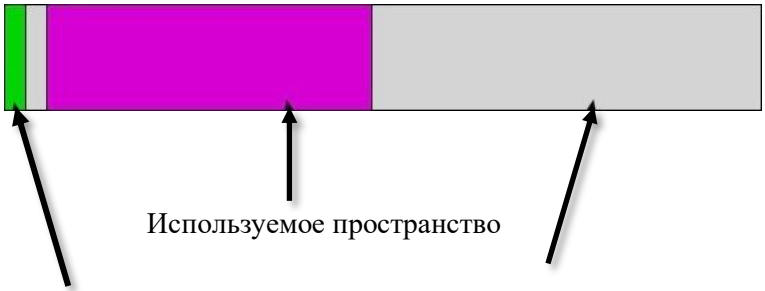
виртуальный накопитель. Для конечного пользователя работа с таким накопителем практически не отличается от работы с обычным, незашифрованным диском.

Для настройки атаки на пароль к зашифрованному диску или контейнеру из него необходимо извлечь метаданные шифрования, которые могут храниться как в заголовке раздела, так и в виде отдельного файла. Объём метаданных шифрования, как правило, не превышает нескольких килобайт; такой файл можно переслать в контрактную лабораторию, не передавая при этом сами зашифрованные данные. Для извлечения метаданных шифрования используется утилита Elcomsoft Forensic Disk Decryptor, а для последующей парольной атаки – Elcomsoft Distributed Password Recovery.

18.2. Скрытые тома и вложенные контейнеры

В начале раздела упоминались зашифрованные диски, которые делают недоказуемым сам факт наличия зашифрованной информации. Такие диски называют вложенными крипто-контейнерами. Создание вложенных контейнеров поддерживается далеко не всеми средствами шифрования диска; самый известный инструмент для создания вложенных контейнеров – VeraCrypt.

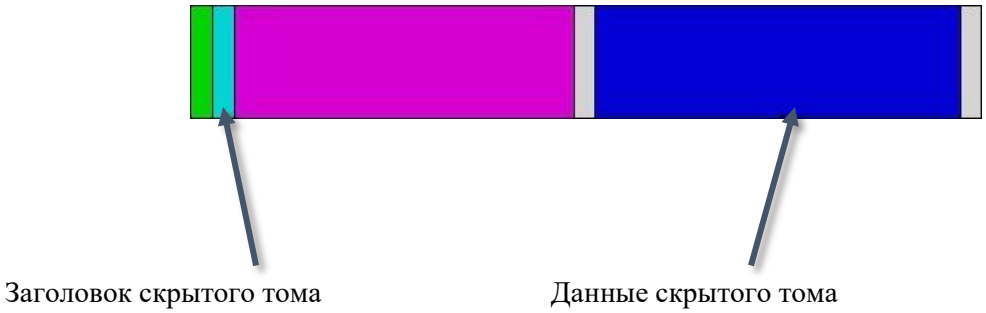
Каким именно образом использование вложенного контейнера делает недоказуемым наличие зашифрованной информации? Чтобы в этом разобраться, рассмотрим структуру зашифрованного диска на примере контейнера VeraCrypt. Стандартный крипто-контейнер можно схематично изобразить следующим образом:



На схеме изображён стандартный заголовок контейнера, в котором содержатся метаданные шифрования, а также используемое и неиспользуемое дисковое пространство. В зависимости от настроек контейнера, а также от того, на каком именно накопителе он хранится (различаются несколько случаев), незанятое пространство может содержать как набор случайных данных, внешне неотличимый от зашифрованной информации, так и пустые страницы (если контейнер создаётся на твердотельном накопителе SSD с включённой функцией Trim pass-through).

Стандартная схема подразумевает шифрование данных, но не сокрытие самого факта шифрования. Если владелец контейнера будет вынужден разгласить пароль шифрования, то всё содержимое крипто-контейнера будет расшифровано.

Ситуация в корне меняется, если в составе основного контейнера пользователь создаст дополнительный вложенный контейнер. На схеме вложенный (скрытый) том выглядит следующим образом:



В таком крипто-контейнере по-прежнему присутствует стандартный заголовок (обозначенный на схеме зелёным цветом), при этом добавляется второй заголовок – заголовок скрытого тома, в котором содержатся метаданные шифрования и адрес, с которого внутри стандартного контейнера начинаются данные скрытого тома.

Процесс монтирования скрытого тома совершенно прозрачен для пользователя. Основной и скрытый тома защищены разными паролями. При вводе пароля от основного тома монтируется основной контейнер, в котором будет присутствовать файловая система, отображающая полный размер тома без учёта размера скрытого контейнера. В основном томе могут храниться файлы, на него можно записывать данные (при неосторожном использовании содержимое скрытого тома может быть перезаписано с уничтожением хранящихся в нём данных).

Если же пользователь вводит пароль от скрытого тома, то смонтирован будет именно он. Файловая система скрытого тома будет отображать его корректный размер; на скрытом томе будут видны совершенно другие данные.

Если пароль от скрытого тома неизвестен, то его наличие или отсутствие невозможно доказать: структура заголовка скрытого тома ничем не отличается от прочих зашифрованных данных или случайной информации. Подозрения на наличие скрытого тома могут возникнуть в случаях, когда объём хранящихся в обычном контейнере данных явно не соответствует общему размеру контейнера.

В процессе атаки на пароль Elcomsoft Distributed Password Recovery может подбирать пароли ко всем вероятным контейнерам, включая скрытые. Для того, чтобы программа атаковала не только пароль от основного контейнера, но и пыталась обнаружить скрытые, нужно отметить соответствующую опцию в момент извлечения метаданных шифрования программой Elcomsoft Forensic Disk Decryptor. Если будет обнаружен пароль от скрытого контейнера, то последний может быть корректно смонтирован или расшифрован в этой же программе.

18.3. Поиск зашифрованных дисков

Повсеместное распространение шифрования часто приводит к невозможности извлечения и анализа данных, особенно при отступлении от установленных процедур изъятия цифровых устройств. В то же время точное следование процедурам изъятия компьютерной техники далеко не всегда возможно в практических условиях. Своевременное обнаружение зашифрованных дисков позволит предпринять необходимые меры для защиты доступа к зашифрованным уликам, прежде чем компьютер подозреваемого будет обесточен. Какие шаги необходимы и как узнать,

используется ли в системе шифрование диска? Сделать это достаточно просто, запустив соответствующую утилиту с внешнего накопителя.

18.3.1. Зашифрованные диски

Зашифрованные диски – один из часто используемых преступниками способов сокрытия улик, доступ к которым может оказаться невозможен без проведения достаточно длительных атак на пароль. В ряде случаев доступ к зашифрованным данным будет невозможен в принципе — например, при использовании некоторых типов защиты BitLocker. Стандартный рабочий процесс состоит из отключения компьютера, извлечения дисков, создания образа диска через устройство с блокировкой записи и последующий анализ данных из виртуального образа диска.

В этом процессе есть тонкий момент: если в системе были смонтированы зашифрованные тома, то доступ к хранящимся на них данным пропадает при отключении питания.

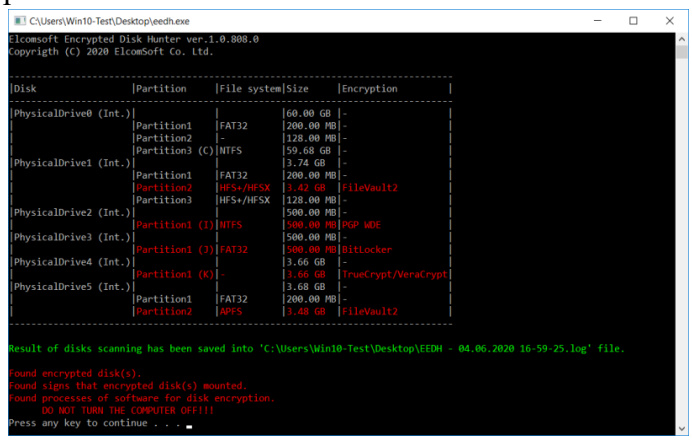
Разумеется, этого не произойдёт, если эксперт будет знать о наличии смонтированных зашифрованных томов и предпримет несложные шаги по консервации имеющихся данных (для чего бывает достаточно снять образ оперативной памяти компьютера). Мы предлагаем простой и быстрый способ узнать, присутствуют ли в системе зашифрованные диски.

18.3.2. Как обнаружить зашифрованные диски

С точки зрения обычного пользователя смонтированный зашифрованный диск ничем не отличается от обычного диска. Тем не менее, при выключении компьютера зашифрованный диск, как правило, размонтируется, и при следующем включении пользователю придётся или ввести пароль, или авторизоваться в системе. Так работает, в частности, шифрование BitLocker с ключом, который защищается посредством аппаратного модуля TPM или Intel PTT; пароля в классическом смысле слова у таких дисков нет, поэтому и любые атаки на данные из образа диска будут бесполезны.

Отличить зашифрованный диск от незашифрованного «на глазок» достаточно сложно. С одной стороны, можно проанализировать настройки системы — например, приложение BitLocker в Панели управления Windows. С другой – технически грамотные преступники часто используют более серьёзное шифрование, например — вложенный контейнер TrueCrypt, использование которого позволит подозреваемому отрицать сам факт наличия улик, выдав вместо пароля от вложенного контейнера пароль от «обёртки», в которой не будет содержаться ничего инкриминирующего.

Определить наличие зашифрованных дисков поможет бесплатная утилита командной строки Elcomsoft Encrypted Disk Hunter.



Elcomsoft Encrypted Disk Hunter — это бесплатный портативный инструмент, который поможет быстро обнаружить наличие зашифрованных дисков. Для анализа системы достаточно запустить утилиту с USB накопителя; список подключённых устройств и зашифрованных дисков выводится автоматически. Инструмент может обнаруживать зашифрованные диски TrueCrypt/VeraCrypt, BitLocker, PGP WDE, FileVault2, BestCrypt и LUKS (только первой версии). Справедливости рады, вам вряд ли встретятся диски с шифрованием FIleVault2 и LUKS, подключённые к компьютеру с Windows (наша утилита работает только в этой ОС). Их поддержку мы включили для тех редких случаев, когда они могут вам понадобиться.

Что делать, если на компьютере пользователя запущена macOS или Linux? В этом случае вам поможет другой, загрузочный инструмент — Elcomsoft System Recovery.[38]

Как это работает?

Прежде всего, для использования утилиты нужны права администратора в анализируемой системе. Без административных привилегий не будет низкоуровневого доступа ни к дискам, ни к оперативной памяти компьютера и списку драйверов.

После запуска Elcomsoft Encrypted Disk Hunter инструмент сканирует подключённые к системе устройства хранения информации на предмет шифрования, осуществляя поиск характерных сигнатур и заголовков в таблицах разделов. При обнаружении зашифрованных томов выводится список зашифрованных дисков.

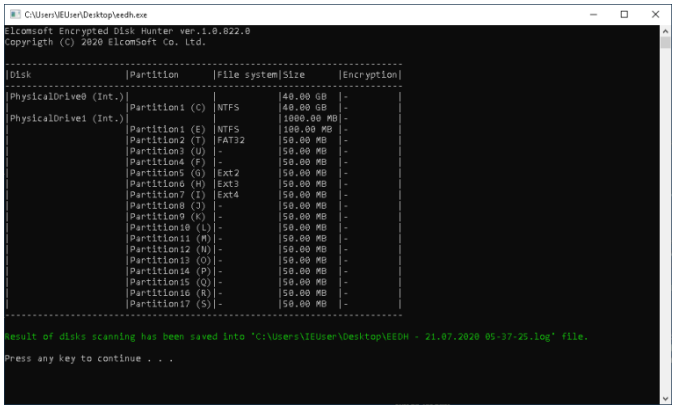
После этого проверяется, смонтирован ли какой-либо из зашифрованных томов. Если никаких явных признаков шифрования диска не обнаружено, Encrypted Disk Hunter проверяет цепочку системных драйверов на предмет наличия в ней драйверов зашифрованных дисков. Если распознан драйвер шифрования диска (например, truecrypt.sys, veracrypt.sys, PGPdisk.SYS, Pgpwdefs.sys или PGPwded.sys), утилита сообщит, что в системе могло использоваться шифрование, даже если в данный момент времени ни одного зашифрованного тома не обнаружено. Кстати, такая эвристика — единственный способ обнаружить диск, зашифрованный PGP WDE, так как последний блокирует доступ к размонтированным зашифрованным томам.

18.3.3. Дальнейшие действия

Ваши дальнейшие действия будут зависеть от выданного программой результата и проведённой вами оценки рисков.

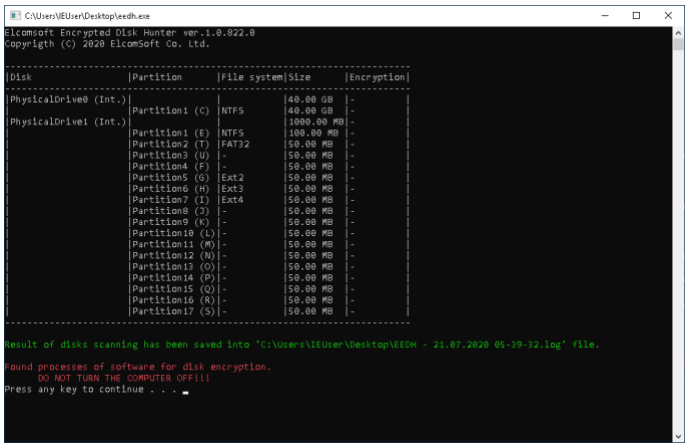
Если никаких признаков шифрования диска не обнаружено: образ оперативной памяти создать желательно, но не обязательно; отключите питание и следуйте обычной схеме.

[38] https://www.elcomsoft.ru/esr.html



Признаков шифрования не обнаружено

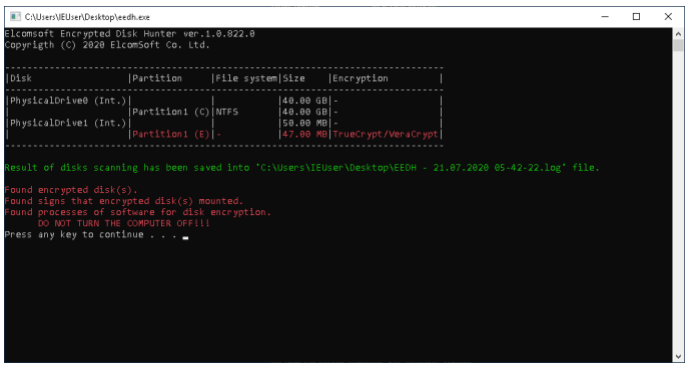
При обнаружении признаков шифрования: обязательно создайте образ оперативной памяти (например, посредством Elcomsoft Forensic Disk Decryptor[39]); возможно, вам придётся потратить дополнительное время на исследование системы перед тем, как обесточить компьютер.



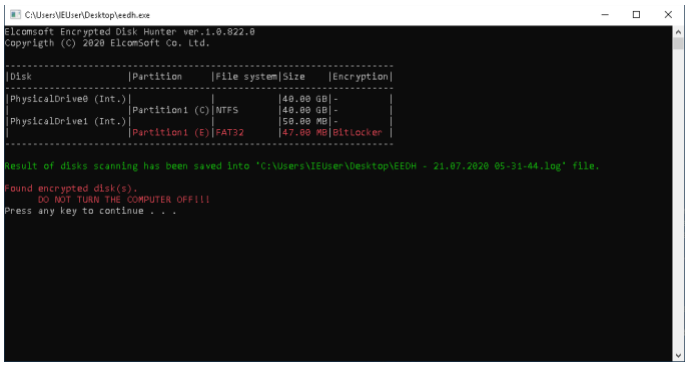
Зашифрованные тома не обнаружены, но обнаружен активный процесс шифрования диска. Требуется дальнейшее исследование.

Если найдены смонтированные зашифрованные диски: создайте образ оперативной памяти; попытайтесь извлечь из него ключи восстановления / депонированные ключи. Если позволяет время, попытайтесь извлечь улики из смонтированных зашифрованных томов.

[39] https://www.elcomsoft.ru/efdd.html



Найден том TrueCrypt/VeraCrypt. Требуется дальнейшее исследование.



Найден том BitLocker. Требуется дальнейшее исследование.

Если смонтирован хотя бы один зашифрованный диск, обратите внимание на тип шифрования. Рекомендуем воспользоваться утилитой Elcomsoft Forensic Disk Decryptor[40]для создания образа оперативной памяти и поиска ключей шифрования, что позволит обойтись без попыток подобрать оригинальный пароль. Извлечение ключей шифрования из образа памяти может и вовсе оказаться единственным доступным методом для разблокировки томов BitLocker, защищённых некоторыми типами протекторов (например, TPM).

Если этот вариант не сработал, используйте Elcomsoft Distributed Password Recovery[41]для взлома пароля. EDPR реализует все возможные оптимизации с учётом человеческого фактора, но атака может оказаться достаточно длительной, так как перебор паролей к зашифрованным дискам может быть очень и очень медленным.

Elcomsoft Encrypted Disk Hunter можно скачать по ссылке с нашего сайта:

Скачать Elcomsoft Encrypted Disk Hunter[42]

Утилита доступна в виде ZIP-архива без установщика. В архиве содержится портативный исполняемый файл, подписанный цифровой подписью. Распакуйте архив, сохраните утилиту на USB-накопителе и используйте в системе с правами администратора. Настоятельно рекомендуем запускать инструмент непосредственно с USB-накопителя.

[40] https://www.elcomsoft.ru/efdd.html
[41] https://www.elcomsoft.com/edpr.html
[42] https://www.elcomsoft.com/download/eedh.zip

18.4. BitLocker

BitLocker — одно из наиболее продвинутых и самое популярное решение для шифрования дисков в Windows. BitLocker подробно документирован и отлично изучен. Время от времени в механизме обнаруживались уязвимости, но область их использования была весьма специфичной, а сами уязвимости исправлялись с очередным обновлением Windows. Тома BitLocker могут быть защищены одним или несколькими предохранителями, такими как аппаратный TPM, пароль пользователя, USB-ключ или их комбинация. Атака на пароль возможна только в одном из этих случаев, в то время как другие средства защиты требуют совсем другого набора атак. Ниже подробно разбираются стратегии и подходы, которые можно использовать для расшифровки томов BitLocker.

18.4.1. С чего начать

С защитой BitLocker проще всего работать, если есть доступ к авторизованной пользовательской сессии, а сложнее всего – если в распоряжении эксперта лишь сам диск или его образ. В зависимости от ряда условий могут применяться различные стратегии.

Авторизованная пользовательская сессия

Если в вашем распоряжении – компьютер с авторизованной пользовательской сессией (экран устройства не заблокирован), и при этом зашифрованный диск смонтирован, то могут быть доступны следующие способы анализа:

– при наличии административных привилегий: извлечь и сохранить ключи восстановления доступа BitLocker (см. ниже); создать образ смонтированного и расшифрованного диска, либо, если административного доступа нет, скопировать данные (папки и файлы) с диска на лабораторный накопитель;

– попытаться отключить защиту BitLocker в настройках системы (Control Panel – BitLocker Drive Encryption – Turn Off BitLocker). Этот вариант может оказаться недоступным, если используется BitLocker Device Encryption или в системе применяется политика безопасности.

Компьютер с зашифрованным системным разделом, TPM

При наличии модуля TPM или Intel PTT Windows может автоматически зашифровать системный раздел по методу BitLocker Device Encryption. В этом случае ключ восстановления доступа в обязательном порядке депонируется в учётную запись Microsoft Account. Ключ депонируется в учётную запись первого зашедшего в систему пользователя, обладающего административными привилегиями и использующего учётную запись Microsoft Account.

В этой ситуации имеет смысл запросить у Microsoft или извлечь из облака (через логин и пароль пользователя) депонированный ключ (см. соответствующий раздел ниже).

Если депонированный ключ не найден или недоступен, но в распоряжении есть весь компьютер (с оригинальным модулем TPM), то можно попробовать провести одну из атак на модуль TPM (см. соответствующий раздел).

В случае, если ни одна из атак не удалась, рекомендуется попытаться извлечь или восстановить пароль от одной из учётных записей компьютера. Обратите внимание: этот пароль невозможно использовать для расшифровки извлечённого из компьютера диска или его образа; вы сможете расшифровать диск исключительно на том же компьютере и в той же системе, в которой он был изначально установлен.

В случае, если в качестве протектора использовался модуль TPM, провести атаку на пароль к зашифрованному тому не удастся.

Зашифрованный диск или его образ

Самый сложный случай – попытка расшифровать отдельный диск или образ диска. Если такой диск был извлечён из компьютера, оборудованного модулем TPM, а в качестве протектора к тому BitLocker использовался TPM, то расшифровать такой диск можно с использованием депонированного ключа (Recovery Key). Атака на пароль в данном случае невозможна.

Если же зашифрован несистемный диск, то вероятность того, что в качестве протектора использовался именно пароль, достаточно высока (вы можете точно узнать, какой использовался протектор, в программе Elcomsoft Forensic Disk Decryptor). В этом случае используйте Elcomsoft Forensic Disk Decryptor для извлечения метаданных шифрования и Elcomsoft Distributed Password Recovery для атаки на пароль.

Обратите внимание: использование депонированного ключа – намного более надёжный и быстрый способ получить доступ к содержимому зашифрованного диска. Рекомендуем изучить все доступные источники (другие компьютеры пользователя, его мобильные устройства, а также данные облачных сервисов), в которых могут содержаться пароли. Если будет найден пароль от учётной записи Microsoft Account, вы можете попытаться найти депонированный ключ в учётной записи пользователя по ссылке https://account.microsoft.com/devices/recoverykey[43]

18.4.2. Как устроено шифрование диска BitLocker

Для защиты диска BitLocker последовательно использует несколько разных ключей, каждый из которых служит своей цели.

В документации Microsoft[44] описано, что данные на диске шифруются специальным ключом, который называется **полным ключом шифрования тома**. Этот ключ, в свою очередь, шифруется **основным ключом тома**. Уже основной ключ тома будет зашифрован при помощи одного из нескольких возможных методов в зависимости от типа протектора (двоичного ключа, пароля или модуля TPM).

Полный ключ шифрования тома шифруется основным ключом тома и хранится в заголовке зашифрованного диска (так называемые «метаданные шифрования»). Основной ключ тома также хранится на зашифрованном диске; он тоже зашифрован. Для шифрования основного ключа тома используется пароль пользователя (если речь идёт о сменном носителе), двоичный ключ или сертификат либо данные модуля TPM.

Что происходит, если защита BitLocker приостанавливается или пользователь отключает защиту, решив «расшифровать» диск? В этом случае данные физически не расшифровываются и не перезаписываются; однако система сохраняет в незащищённом виде ключ, которым шифруется основной ключ тома.

С точки зрения Microsoft, такая процедура хранения гарантирует, что основной ключ тома никогда не хранится без шифрования и всегда защищён, если не отключено шифрование BitLocker. Для обеспечения избыточности система сохраняет ещё две копии ключей в разных местах на диске.

---

[43] https://account.microsoft.com/devices/recoverykey
[44] https://docs.microsoft.com/ru-ru/windows/security/information-protection/bitlocker/bitlocker-key-management-faq

Может показаться, что схема шифрования BitLocker избыточно усложнена, то это не так. Использованная схема позволяет, к примеру, мгновенно изменить пароль от тома без перешифровки всего содержимого. Кроме того, удаление всего нескольких килобайт метаданных шифрования сделает расшифровку данных абсолютно невозможной, что позволяет быстро и безопасно очищать зашифрованные накопители без длительной процедуры перезаписи данных.

18.4.3. Автоматическое шифрование BitLocker Device Encryption

Система BitLocker доступна не всем пользователям Windows 10. Эта подсистема входит в профессиональную и корпоративную редакции, но не включена в редакцию Home для домашних пользователей. Тем не менее, эксперты часто сталкиваются с шифрованием системного раздела системой BitLocker на компьютерах, которые, казалось бы, не должны его поддерживать. Почему так происходит? Дело в том, что для защиты загрузочного накопителя в таких случаях используется несколько другая система: BitLocker Device Encryption (технические подробности – на сайте Microsoft[45]).

Для многих классов устройств использование Microsoft Account для входа в систему автоматически включит шифрование данных. Если устройство под управлением Windows 8.1, 10, 11 или версии Windows для ARM (планшет, ультрабук или устройство 2-в-1), то при выполнении некоторых условий, основные из которых – наличие модуля TPM2.0 или эмулятора Intel PTT (в процессорах Intel начиная с 8 поколения технология доступна по умолчанию), оно готово к использованию системы защиты данных BitLocker Device Encryption.

Для того, чтобы шифрование активировалось, пользователю не нужно предпринимать активных действий. Достаточно в процессе установки Windows ввести учётные данные Microsoft Account или в любой момент после добавить данные Microsoft Account к любой учётной записи с административными привилегиями – и Windows автоматически начнёт шифрование системного раздела. Пользователь может ничего не знать о шифровании, но оно будет активировано – точно так же, как это делается в современных смартфонах, содержимое которых зашифровано.

Вот как происходит процесс инициализации BitLocker Device Encryption по описанию Microsoft[46] (в тексте ниже исправлены ошибки автоматического перевода):

– после завершения чистой установки Windows 11 или Windows 10 компьютер готовится к первому использованию. В рамках этой подготовки производится инициализация шифрования устройств BitLocker на загрузочном диске операционной системы и фиксированных дисках на компьютере. На момент инициализации ключ шифрования ключа шифрования не защищён и хранится в открытом виде (эквивалент стандартного приостановленного состояния BitLocker). В этом состоянии диск отображается со значком предупреждения в Windows Explorer. Жёлтый значок предупреждения удаляется после создания протектора TPM и ключа восстановления доступа, как поясняется в следующих пунктах;

[45]https://learn.microsoft.com/ru-ru/windows/security/operating-system-security/data-protection/bitlocker/#device-encryption
[46]https://learn.microsoft.com/ru-ru/windows/security/operating-system-security/data-protection/bitlocker/#device-encryption

– если устройство не участвует в домене, требуется использовать учётную запись Майкрософт, которой были предоставлены права администратора на устройстве. Когда пользователь с правами локального администратора впервые использует учётную запись Майкрософт для входа в систему, незащищённый ключ удаляется, а ключ восстановления доступа депонируется в облачную учётную запись Microsoft. Далее создаётся протектор TPM. Если пользователю потребуется ключ восстановления, достаточно использовать любое другое устройство и перейти по специальной ссылке (см. ниже), чтобы извлечь его с использованием своих учётных данных. Извлечь депонированные ключи BitLocker и BitLocker Device Encryption можно из учётной записи пользователя, открыв страницу https://account.microsoft.com/devices/recoverykey [47];

– если пользователь использует для входа учётную запись домена, незащищённый ключ не удаляется до тех пор, пока пользователь не подсоединит устройство к домену и не выполнит успешное резервное копирование ключа восстановления в доменные службы Active Directory (AD DS). Необходимо включить параметр групповой политики «**Конфигурация компьютера\Административные шаблоны\Компоненты Windows\Шифрование диска BitLocker\Диски операционной системы»** и выбрать вариант «**Не включать BitLocker до сохранения данных восстановления в AD DS для дисков операционной системы»**. При такой конфигурации пароль восстановления создаётся автоматически, когда компьютер подключается к домену, а в AD DS создаётся резервная копия ключа восстановления. Затем создаётся механизм защиты TPM, а незащищённый ключ удаляется.

– аналогично входу по учётной записи домена незащищённый ключ удаляется, когда пользователь входит на устройство с использованием учётной записи Azure AD. Как описано выше, пароль восстановления создаётся автоматически, когда пользователь проходит аутентификацию в Azure AD. Затем выполняется резервное копирование ключа восстановления доступа в Azure AD, создаётся механизм защиты TPM, незащищённый ключ удаляется.

Для входа в систему и расшифровки данных теперь достаточно ввести пароль от учётной записи Microsoft Account или воспользоваться упрощённой системой аутентификации Windows Hello (вход с помощью короткого PIN-кода или биометрической аутентификации). Если устройство будет потеряно или украдено, у злоумышленника будет ограниченное число попыток логина с помощью PIN-кода и неограниченное – с помощью пароля к учётной записи Windows. Более того, при попытке извлечь жёсткий диск и подключить его к другому компьютеру потребуется ввести ключ восстановления доступа BitLocker – одних лишь данных учётной записи Microsoft Account уже недостаточно.

18.4.4. Где хранятся ключи

Полный ключ тома, защищённый основным ключом тома, хранится в заголовке контейнера (и двух дополнительных местах на диске) в зашифрованном виде. Это хранилище мы называем метаданными шифрования, и именно эти данные извлекают продукты Elcomsoft Forensic Disk Decryptor и Elcomsoft System Recovery для последующих атак. Основной ключ тома, зашифрованный паролем или другим протектором, сохраняется в них же. А вот протектор

[47] https://account.microsoft.com/devices/recoverykey

(пароль пользователя, данные модуля TPM, двоичный ключ или сертификат) в составе контейнера не хранятся: именно эти данные будут использованы для расшифровки цепочки ключей и, соответственно, данных на диске.

Необходимо отметить ещё один ключ, так называемый ключ восстановления доступа или Recovery Key. Этот ключ в обязательном порядке создаётся при включении шифрования BitLocker. Пользователь может сохранить его в файл на диске (за исключением того, который будет зашифрован), распечатать на принтере, либо сохранить в облако Microsoft Account (в этом случае ключ «депонируется», получая название «депонированного ключа»). Для корпоративных пользователей доступен вариант с сохранением ключа в Active Directory. Эти ключи могут использоваться для монтирования и расшифровки тома.

18.4.4.1. Где находится ключ восстановления доступа BitLocker

В Windows 10 и Windows 11 невозможно включить шифрование BitLocker без сохранения копии ключа восстановления доступа. В случае автоматического шифрования устройства BitLocker Device Encryption ключ восстановления автоматически сохраняется в облачной учётной записи первого пользователя, который входит в систему как системный администратор со учётной записью Microsoft (в отличие от локальной учётной записи Windows).

Обратите внимание: первый и текущий пользователи компьютера могут не совпадать, и ключ восстановления доступа BitLocker необходимо получить именно у того пользователя, в учётной записи которого он был сохранён.

Microsoft опубликовала статью для системных администраторов Руководство по восстановлению BitLocker (для Windows 10) — Windows security | Microsoft Docs[48], в которой подробно описаны способы получения ключа восстановления доступа. Ниже приводится выдержка из другой статьи компании, которая была написана для обычных пользователей.

BitLocker — это функция шифрования устройств в Windows. Если устройство запрашивает у вас ключ восстановления BitLocker, следующие инструкции помогут вам найти 48-значный ключ, который понадобится для разблокировки устройства. Ниже указаны некоторые места, в которых можно поискать ключ, если у вас его нет:

В учетной записи Майкрософт выполните Вход в учетную запись Майкрософт[49] на другом устройстве, чтобы найти ключ восстановления. Если на устройстве есть учетные записи других пользователей, вы можете попросить их войти в свою учетную запись Майкрософт, чтобы проверить, есть ли у них ключ.

Сохранён в виде распечатки: ключ восстановления может находиться на распечатке, сохраненной при активации BitLocker. Проверьте свои важные документы, относящиеся к компьютеру.

На USB-накопителе: подсоедините USB-накопитель к заблокированному компьютеру и следуйте инструкциям. Если ключ сохранен на устройстве флэш-памяти как текстовый файл, прочтите этот файл на другом компьютере.

---

[48]https://learn.microsoft.com/ru-ru/windows/security/operating-system-security/data-protection/bitlocker/recovery-overview

[49] https://account.microsoft.com/devices/recoverykey?refd=support.microsoft.com

В учетной записи Azure Active Directory: если ваше устройство было зарегистрировано в Организации с помощью рабочей или учебной учетной записи электронной почты, ваш ключ восстановления может храниться в учетной записи Azure AD[50] , связанной с вашим устройством. Возможно, вы сможете получить к ключу доступ самостоятельно либо вам может потребоваться обратиться к системному администратору.

Хранится у системного администратора: если устройство подключено к домену (обычно это рабочее или учебное устройство), обратитесь к системному администратору для ключа восстановления.

(Источник: Поиск ключа восстановления BitLocker (microsoft.com)[51])

18.4.4.2. Депонированные ключи в облаке и Active Directory

В момент, когда пользователь включает шифрование BitLocker либо в момент, когда система Windows 8, 8.1 или Windows 10 начинает шифровать загрузочный диск устройства посредством BitLocker Device Encryption, в обязательном порядке создаётся так называемый ключ восстановления доступа (Recovery Key). Этот ключ позволяет расшифровать том даже в случаях, когда жёсткий диск переносится с одного компьютера с модулем TPM на другой. Более того, этот ключ позволяет расшифровать том даже в тех случаях, когда используется несколько различных протекторов, некоторые из которых недоступны на момент расшифровки. Использование ключа восстановления позволяет быстро и без усилий получить доступ к информации. Таким образом, стоит приложить усилия к получению ключа восстановления доступа.

Ключи восстановления BitLocker могут быть сохранены следующим образом. Для стандартной схемы защиты BitLocker (в отличие от BitLocker Device Encryption) ключи восстановления могут быть распечатаны на принтере, сохранены в файл на другом носителе либо сохранены в облако Microsoft Account или Active Directory.

Интереснее обстоит дело с ключом, который создаётся в процессе автоматического шифрования BitLocker Device Encryption (о том, что это такое и как работает – в следующей главе). Такие ключи всегда депонируются либо в облако Microsoft Account первого пользователя, который вошёл в систему с административной учётной записи Microsoft Account, либо в Active Directory. Эти депонированные ключи могут использоваться для монтирования и расшифровки тома.

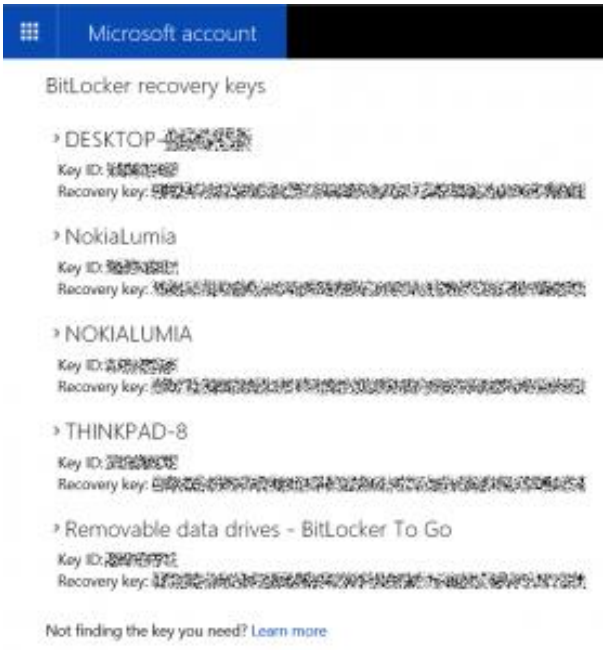
Извлечь депонированные ключи BitLocker и BitLocker Device Encryption можно из учётной записи пользователя, открыв следующую страницу:

https://account.microsoft.com/devices/recoverykey[52]

Для этого необходимо авторизоваться с учётной записью пользователя Microsoft Account (потребуется указать логин и пароль пользователя от учётной записи Microsoft; если в учётной

[50] https://aka.ms/aadrecoverykey
[51]https://support.microsoft.com/ru-ru/windows/поиск-ключа-восстановления-bitlocker-6b71ad27-0b89-ea08-f143-056f5ab347d6
[52] https://account.microsoft.com/devices/recoverykey

записи включён режим двухфакторной аутентификации, потребуется доступ к приложению-аутентификатору).



Все ключи шифрования пользователя будут показаны на одной странице. Идентифицировать нужный ключ можно по идентификатору устройства, которое выводится в тот момент, когда осуществляется попытка монтирования зашифрованного тома.

18.4.5. Способы получить пароль от Microsoft Account

Если диск зашифрован с помощью BitLocker или его «облегчённой» версии – **BitLocker Device Encryption**, и при этом в системе установлен модуль TPM 2.0, то **извлечь базу данных SAM** (для попытки подобрать пароль для входа в Windows) **будет невозможно** или **очень трудно.**

Очень часто у пользователей портативных устройств (напомним, BitLocker Device Encryption активируется автоматически именно в них) есть в наличии и полноразмерный компьютер, десктоп или ноутбук. Шифрование BitLocker Device Encryption на них может не присутствовать: не выполняется как минимум одно из условий для автоматической активации – несъёмная (распаянная) оперативная память. Таким образом, с помощью Elcomsoft System Recovery можно извлечь дамп базы данных SAM и попытаться восстановить пароль на вход в систему.

В Elcomsoft System Recovery есть встроенные средства, с помощью которых простой пароль можно попытаться восстановить «на месте». Если же пароль оказался длинным и сложным, программа позволяет извлечь хэши паролей и сохранить их в файле для перебора с помощью Elcomsoft Distributed Password Recovery.

Если доступен компьютер, системный раздел которого не зашифрован, то проводить длительную атаку на пароль для входа в систему может быть необязательно. Существует вероятность, что пользователь вводил пароль к Microsoft Account для проверки почты через браузер или для доступа к многочисленным онлайновым сервисам Microsoft. Пароль в этом случае может сохраняться браузером – Chrome, Edge, Firefox и др. Извлечь его из хранилища

браузера – задача намного проще той, которую приходится решать при восстановлении пароля на вход в систему.

Для мгновенного извлечения пароля от учётной записи используется Elcomsoft Quick Triage. С помощью этого инструмента можно проанализировать данные браузеров командой Web Passwords. Стоит обращать внимание на записи, соответствующие доменам microsoft.com, live.com, hotmail.com, outlook.com и другим доменам Microsoft. С большой вероятностью пароль будет найден и его можно будет использовать для доступа к системе.

18.4.6. Методы защиты

Как мы выяснили, основной ключ тома может быть зашифрован различными протекторами[53]. Некоторые из этих протекторов – аппаратные; чтобы разблокировать том и расшифровать данные, вам понадобится компьютер пользователя (и, в зависимости от типа атаки, аутентифицированная сессия Windows); атака на пароль методом перебора будет невозможна. Посмотрим, какие протекторы существуют, как они используются и как действовать в случае, если обнаружен один из них.

Во-первых, определим, есть ли в системе зашифрованные диски в принципе. Рекомендуем воспользоваться бесплатным инструментом Elcomsoft Encrypted Disk Hunter[54]для определения зашифрованных дисков.

Если найден зашифрованный том, то в Windows тип протектора тома можно определить, запустив следующую команду (зашифрованный том должен быть смонтирован):

```
manage-bde -protectors -get X:
```

Здесь **X**: — буква тома.

Если же в вашем распоряжении только диск или его образ, то используйте Elcomsoft Forensic Disk Decryptor для извлечения метаданных шифрования и Elcomsoft Distributed Password Recovery для попытки атаки.

18.4.7. Типы протекторов BitLocker

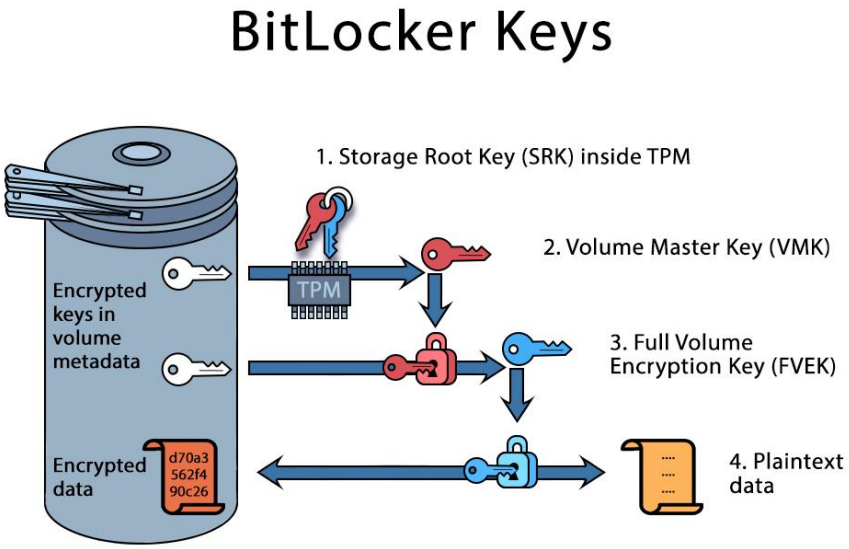
Рассмотрим возможные типы протекторов.

18.4.7.1. TPM

Аппаратные модули TPM часто используются в портативных компьютерах – ноутбуках, планшетах и устройствах 2-в-1. При использовании защиты TPM Windows загрузится до запроса входа в систему. Основной ключ тома будет расшифрован с помощью корневого ключа хранилища, который хранится в модуле TPM (или Intel PTT). Ключ будет выдан в том и только в том случае, если система проходит проверку безопасной загрузки. Этот вариант прозрачен для пользователя: пользователь может даже не подозревать, что ноутбук или планшет зашифрован.

---

[53] https://learn.microsoft.com/ru-ru/windows-server/administration/windows-commands/manage-bde-protectors
[54] https://blog.elcomsoft.com/2020/07/live-system-analysis-discovering-encrypted-disk-volumes/



Векторы атаки: ввиду отсутствия пароля шифрования для доступа к тому, защищённому аппаратным модулем TPM, используйте одну из следующих стратегий.

Ключ восстановления доступа BitLocker. Windows автоматически создаёт ключ восстановления при шифровании BitLocker Device Encryption; такие ключи восстановления автоматически загружаются в учётную запись Microsoft Account первого пользователя компьютера, который вошёл в систему с административными привилегиями. Вы можете запросить этот ключ у Microsoft или загрузить его, войдя в учётную запись Microsoft и перейдя по следующей ссылке: https://account.microsoft.com/devices/recoverykey[55]

Дополнительные варианты. Ключ восстановления доступа может храниться в других местах – например, в Active Directory: Где найти ключ восстановления BitLocker?[56]

Атака методом холодной загрузки. BitLocker в конфигурации по умолчанию использует доверенный платформенный модуль TPM (если таковой установлен), которому для расшифровки диска не требуется ни пин-код, ни внешний ключ. Когда операционная система загружается, BitLocker извлекает ключ из TPM без какого-либо взаимодействия с пользователем. Следовательно, можно просто включить машину, подождать, пока операционная система начнёт загрузку, а затем выполнить атаку методом холодной загрузки для извлечения ключа из оперативной памяти компьютера. Обратите внимание, что эта атака недоступна, если в дополнение к TPM использовался пароль или ключ.

Что такое ***атака методом холодной загрузки***? Это технически сложный вид атаки, в процессе которого производится заморозка чипов памяти жидким азотом или сжатым воздухом, после которой питание компьютера отключается, а модули памяти физически извлекаются (или производится загрузка с USB-накопителя) с целью доступа к содержимому оперативной памяти

[55] https://account.microsoft.com/devices/recoverykey
[56]https://support.microsoft.com/ru-ru/help/4530477/windows-10-finding-your-bitlocker-recovery-key

и поиска ключей шифрования. Помимо исключительной технической сложности этого типа атаки, у него есть и ещё один недостаток: он работает только с компьютерами, модули памяти в которых не распаяны (т.е. их физически можно извлечь).

Образ оперативной памяти. Если у вас есть доступ к компьютеру пользователя, и вы можете войти в систему или получить дамп памяти с помощью атаки через интерфейс FireWire/Thunderbolt, то можно извлечь получить ключи шифрования непосредственно из оперативной памяти компьютера. В состав Elcomsoft Forensic Disk Decryptor входит как утилита для снятия образа оперативной памяти, так и инструмент для его анализа с целью поиска ключей шифрования.

18.4.7.2. TPM + ПИН

В этом режиме для загрузки Windows потребуется не только модуль TPM, но и дополнительный ключ (ПИН-код или пароль). Модуль TPM выдаст ключ шифрования в том и только в том случае, если на вход будет подан правильный пароль (ПИН). Как правило, длина ПИН-кода не превышает 4 цифр, но после нескольких неудачных попыток модуль TPM заблокирует доступ к ключу шифрования.

Векторы атаки: режим TPM+ПИН – интерактивный: от пользователя требуется ввести ПИН-код, причём именно на том компьютере, на котором использовался зашифрованный диск. Сам по себе ПИН-код не используется для шифрования; он нужен для того, чтобы аппаратный модуль TPM выдал системе необходимый ключ. Перебор ПИН-кодов опасен: в зависимости от производителя и настроек модуля перебор может привести как к блокировке модуля TPM, так и к уничтожению ключа шифрования.

Ключ восстановления доступа BitLocker. Windows автоматически создаёт ключ восстановления при шифровании BitLocker Device Encryption; такие ключи восстановления автоматически загружаются в учётную запись Microsoft Account первого пользователя компьютера, который вошёл в систему с административными привилегиями. Вы можете запросить этот ключ у Microsoft или загрузить его, войдя в учётную запись Microsoft и перейдя по следующей ссылке: https://account.microsoft.com/devices/recoverykey[57]

Атака методом холодной загрузки сработает лишь в том случае, если вам известен ПИН-код. В противном случае система не загрузится, а ключ шифрования не попадёт в оперативную память.

Образ оперативной памяти. Сработает только в том случае, если компьютер уже загружен. Используйте Elcomsoft Forensic Disk Decryptor[58]для снятия образа оперативной памяти и его анализа с целью поиска ключей шифрования.

18.4.7.3. TPM + USB

Этот вариант для загрузки системы требует присутствия как TPM, так и USB-накопителя (или смарт-карты CCID). Это нестандартная, но возможная конфигурация.

Векторы атаки: режим TPM+USB требует наличия файла с ключом на USB-накопителе. Соответственно, вам потребуется доступ к этому накопителю (а точнее, к ключу на нём).

---

[57] https://account.microsoft.com/devices/recoverykey
[58] https://www.elcomsoft.com/efdd.html

Ключ восстановления доступа BitLocker. Никаких различий с предыдущим протектором.

Атака методом холодной загрузки сработает лишь в том случае, если в наличии есть USB накопитель с ключом. В противном случае система не загрузится, а ключ шифрования не попадёт в оперативную память.

Образ оперативной памяти. Сработает только в том случае, если компьютер уже загружен. Используйте Elcomsoft Forensic Disk Decryptor [59]для снятия образа оперативной памяти и его анализа с целью поиска ключей шифрования.

18.4.7.4. TPM + ПИН + USB

Довольно редкая реализация «параноидальной» защиты, комбинирующая два предыдущих метода. Уже из названия очевидно, что для загрузки системы потребуется и модуль TPM, и ввод ПИН-кода, и наличие USB накопителя с ключом.

Векторы атаки: режим TPM+USB требует наличия файла с ключом на USB-накопителе и ввода ПИН-кода в дополнение к аппаратному модулю TPM. Соответственно, для доступа к данным вам потребуется всё вышеперечисленное.

Ключ восстановления доступа BitLocker. Никаких различий с предыдущим протектором.

Атака методом холодной загрузки сработает лишь в том случае, если в наличии есть USB накопитель с ключом, а ПИН-код вам известен. В противном случае система не загрузится, а ключ шифрования не попадёт в оперативную память.

Образ оперативной памяти. Сработает только в том случае, если компьютер уже загружен. Используйте Elcomsoft Forensic Disk Decryptor для снятия образа оперативной памяти и его анализа с целью поиска ключей шифрования.

18.4.7.5. USB

Вариант с ключом на USB накопителе гораздо проще взломать по сравнению с использованием модулей TPM. Для расшифровки диска вам понадобится только USB накопитель с ключом.

Векторы атаки: пароля по-прежнему нет; для расшифровки диска нужен накопитель с ключом.

Ключ восстановления доступа BitLocker. Никаких различий с предыдущим протектором.

Атака методом холодной загрузки в данной ситуации лишена смысла. С одной стороны, атака сработает лишь в том случае, если в наличии есть USB накопитель с ключом. С другой — если в нашем распоряжении есть накопитель с ключом, то смонтировать зашифрованный раздел можно гораздо проще.

Образ оперативной памяти. Сработает только в том случае, если компьютер уже загружен. Используйте Elcomsoft Forensic Disk Decryptor для снятия образа оперативной памяти и его анализа с целью поиска ключей шифрования.

---

[59] https://www.elcomsoft.com/efdd.html

18.4.7.6. Только пароль

Наконец, мы подошли к единственному протектору, который можно взломать методом полного перебора. Протектор «только пароль» защищает ключ исключительно паролем пользователя – который можно подобрать при помощи Elcomsoft Distributed Password Recovery. Более того, атаку можно проводить в лаборатории как на сам диск, так и на его образ – модуль TPM в данной схеме не участвует, поэтому никаких ограничений на количество попыток или скорость перебора нет.

Векторы атаки: можно подобрать пароль, осуществить атаку методом холодной загрузки, воспользоваться ключом восстановления доступа или извлечь ключ шифрования из образа оперативной памяти. Как только из уравнения исключается аппаратный модуль TPM, получить доступ к зашифрованным данным становится значительно легче.

Ключ восстановления доступа BitLocker. Никаких различий с предыдущим протектором.

Атака методом холодной загрузки так же, как и в предыдущем случае, лишена смысла. С одной стороны, атака сработает лишь в том случае, если вы уже знаете пароль от зашифрованного тома. С другой — если вы знаете пароль, то и атака не нужна.

Образ оперативной памяти. Сработает только в том случае, если компьютер уже загружен. Используйте Elcomsoft Forensic Disk Decryptor для снятия образа оперативной памяти и его анализа с целью поиска ключей шифрования.

Перебор паролей. Используйте Elcomsoft Forensic Disk Decryptor для извлечения метаданных шифрования из самого диска или его образа. Метаданные шифрования откройте в Elcomsoft Distributed Password Recovery[60] для настройки атаки. Вы также можете использовать Elcomsoft System Recovery[61] для загрузки компьютера пользователя с USB накопителя с целью извлечения метаданных шифрования без разборки компьютера и извлечения самого диска.

18.4.8. Если диск защищён протектором, отличным от пароля

Если пароль не установлен или если пароль используется совместно с другим типом протектора, попытки подобрать пароль лишены смысла. Даже если вы извлекли метаданные шифрования и загрузили их в Elcomsoft Distributed Password Recovery, вы не сможете запустить атаку: продукт выдаст сообщение о несовместимом типе протектора. Таким образом развиваются события в случаях, когда в деле фигурирует модуль аппаратной защиты TPM.

Внимание: атака на пароль в случае, если том BitLocker зашифрован с протектором типа TPM, бессмысленна; расшифровать такой диск можно либо депонированным ключом (например, извлечённым из хранилища OneDrive в учётной записи пользователя Microsoft Account), либо ключом, который извлекается из оперативной памяти загруженного компьютера пользователя. Об этом – подробнее.

---

[60] https://www.elcomsoft.com/edpr.html
[61] https://www.elcomsoft.com/esr.html

18.4.9. Авторизованная пользовательская сессия

Что произойдёт, если мы имеем дело не с отдельным диском и не с его образом, а с уже загруженным компьютером, на котором смонтирован зашифрованный том BitLocker? В этом случае присутствует ещё один ключ, наличие которого не упоминается в документации. Этот ключ хранится в оперативной памяти компьютера и используется драйвером BitLocker для реализации «прозрачного» потокового шифрования. Подобным образом работают все утилиты шифрования диска, но если в некоторых сторонних решениях (например, VeraCrypt) пользователь может включить обфускацию этого ключа, что затрудняет его извлечение из оперативной памяти, то BitLocker не делает попыток «спрятать» ключ. Соответственно, при помощи специальных инструментов (таких как Elcomsoft Forensic Disk Decryptor) этот ключ можно извлечь из образа оперативной памяти, файла подкачки или файла гибернации (впрочем, если зашифрован системный том, то и эти файлы будут зашифрованы; остаётся лишь образ оперативной памяти). Извлечённый таким образом ключ можно использовать для мгновенного монтирования или расшифровки защищённого тома.

Извлечь ключи шифрования BitLocker при анализе авторизованной пользовательской сессии можно одним из двух способов.

Способ 1: используя встроенные в Windows инструменты командной строки или графического интерфейса (подробнее об этом способе – в следующей части).

Способ 2: с использованием Elcomsoft Forensic Disk Decryptor для снятия образа оперативной памяти и поиска ключей шифрования.

Каким бы способом вы ни воспользовались, вам потребуется административный доступ к системе. Соответственно, извлечь ключи от зашифрованного раздела BitLocker возможно в случаях, когда у авторизованного в системе пользователя есть административные привилегии.

Если сравнить два способа между собой, то первый из них – существенно проще и быстрее, а извлекаемые посредством него ключи можно использовать для монтирования зашифрованного диска как стандартными средствами Windows, так и в сторонних программах. Второй способ (с использованием Elcomsoft Forensic Disk Decryptor) сложнее и дольше, а найденные с его помощью ключи можно использовать только в Elcomsoft Forensic Disk Decryptor. В то же время наш продукт позволяет искать в образе оперативной памяти ключи не только от томов BitLocker, но и от дисков, зашифрованных другими продуктами – например, TrueCrypt или VeraCrypt, чего нельзя сделать встроенными в Windows инструментами.

Ваши действия:

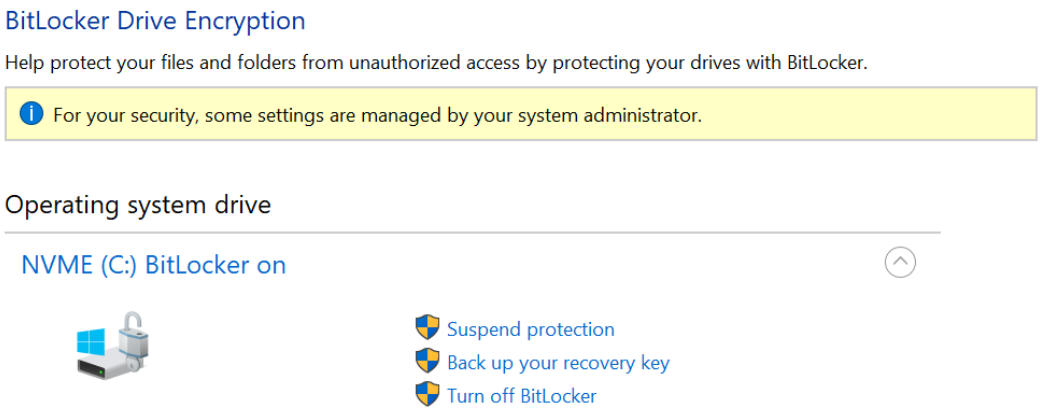
- на компьютере пользователя запустите Elcomsoft Forensic Disk Decryptor;
- создайте образ оперативной памяти;
- откройте его в Elcomsoft Forensic Disk Decryptor на своём компьютере и осуществите поиск ключей BitLocker;
- если ключи найдены, создайте образ зашифрованного диска и используйте Elcomsoft Forensic Disk Decryptor для его монтирования или расшифровки.

18.4.10. Извлечение ключей BitLocker из авторизованной пользовательской сессии

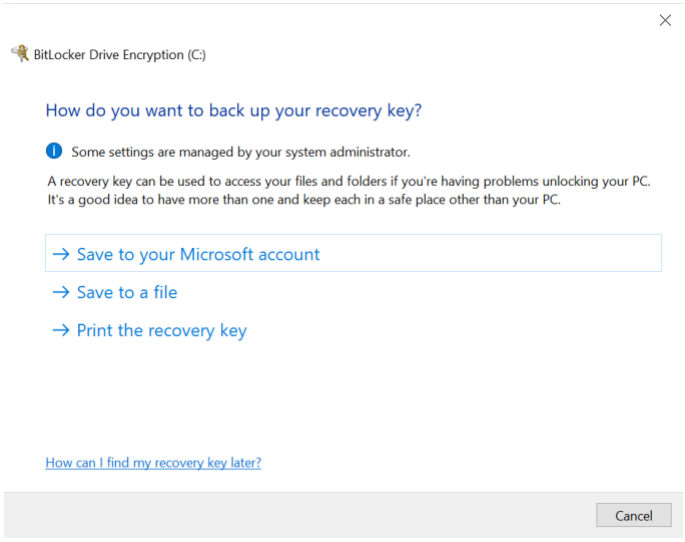
Сохранить ключ восстановления доступа можно как через графический интерфейс Windows, так и из командной строки. В любом случае вам потребуется **учётная запись с административными привилегиями**.

18.4.10.1. Сохранение ключа BitLocker через Windows GUI

Запустите апплет “BitLocker Drive Encryption” из панели управления Windows Control Panel. Проще всего это сделать, введя слово “bitlocker” в строку поиска в Windows.



Если системный диск зашифрован, вы увидите список возможных действий: Suspend protection, Backup your recovery key, Turn off BitLocker. Для сохранения резервной копии ключа используйте команду “Backup your recovery key”.



Ключ можно сохранить как в облако (если вы используете для входа в систему Microsoft account), так и в файл или в виде распечатки.

Обратите внимание: в Windows 10 начиная с версии 1903 и всех версиях Windows 11 система запомнит, когда и куда вы сохраняли ключ восстановления доступа. Эта информация выводится на экране блокировки BitLocker. Узнать её другим способом нельзя.

18.4.10.2. Сохранение ключа BitLocker из командной строки

Для сохранения копии ключа BitLocker из командной строки запустите cmd.exe с правами администратора (“Run as administrator”), после чего введите команду:

```
manage-bde -protectors -get C:
```

Будет выведена следующая информация:

```
C:\WINDOWS\system32>manage-bde -protectors -get C:

BitLocker Drive Encryption: Configuration Tool version 10.0.19041

Copyright (C) 2013 Microsoft Corporation. All rights reserved.

Volume C: [NVME]

All Key Protectors

TPM:

ID: {XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX}

PCR Validation Profile:

0, 2, 4, 11

Numerical Password:

ID: {YYYY-YYYY-YYYY-YYYY-YYYYYYYYYYYY}

Password:

123456-123456-123456-123456
```

Здесь поле “Numerical Password” и есть ключ восстановления доступа для ключа, идентифицируемого по key ID.

18.4.10.3. Сохранение ключа BitLocker из PowerShell

В Windows доступна замена командной строки в виде PowerShell. Для извлечения всех ключей BitLocker для всех зашифрованных дисков используйте следующий скрипт, сохранив его в файл с расширением .ps1 (например, "backup-bitlocker.ps1") и запустив из PowerShell с административными привилегиями.

```
# Export the BitLocker recovery keys for all drives and display them at the
Command Prompt.

$BitlockerVolumers = Get-BitLockerVolume

$BitlockerVolumers |

ForEach-Object {

$MountPoint = $_.MountPoint

$RecoveryKey = [string]($_.KeyProtector).RecoveryPassword

if ($RecoveryKey.Length -gt 5) {

Write-Output ("The drive $MountPoint has a BitLocker recovery key $RecoveryKey")

}

}
```

18.4.11. BitLocker в Windows 11

Ни сам механизм BitLocker, ни политики шифрования в Windows 11 не получили серьёзных изменений в сравнении с Windows 10. После анонса Windows 11 могло возникнуть ложное впечатление о том, что Microsoft будет шифровать системный раздел Windows 11 так же, как это делают производители смартфонов. Это не соответствует действительности. По умолчанию (посредством BitLocker Device Encryption) шифруются лишь оборудованные TPM или его эмуляторами портативные устройства — ноутбуки, планшеты и устройства два-в-одном, однако точно таким же образом шифрование включалось и в Windows 8, и в Windows 10. При установке Windows 11 на настольный компьютер шифрование по умолчанию не включается; более того, для того чтобы использовать BitLocker, требуется редакция Windows 11 Pro, Enterprise или Education. Для пользователей младшей редакции Home шифрование остаётся недоступным.

18.5. Извлечение ключей и метаданных шифрования

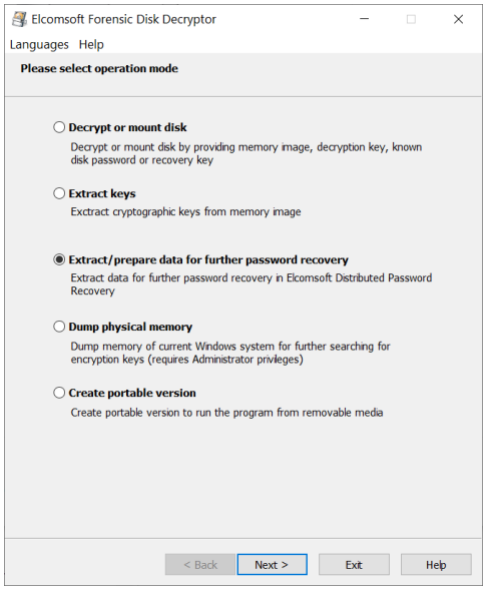
Опишем практические шаги по извлечению ключей и метаданных шифрования, которые упоминались выше.

Шаг 1.1. Извлечение метаданных шифрования BitLocker при помощи Elcomsoft Forensic Disk Decryptor.

Используйте Elcomsoft Distributed Password Recovery[62] для сохранения метаданных шифрования в файл.

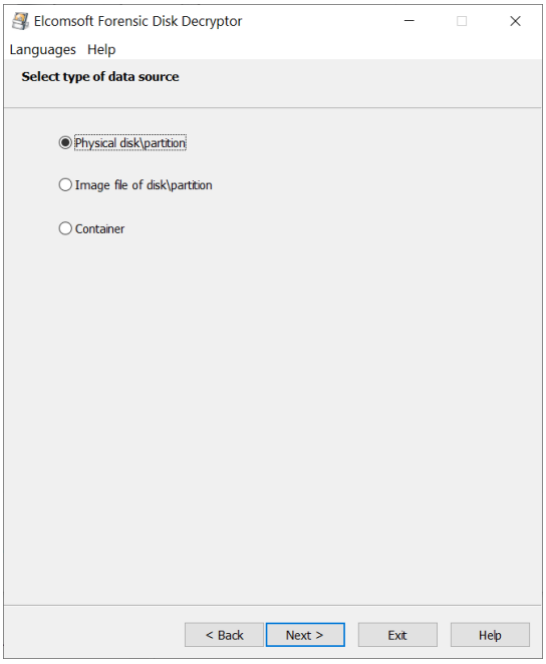
Запустите Elcomsoft Forensic Disk Decryptor.

Выберите опцию "**Extract/prepare data for further password recovery**".

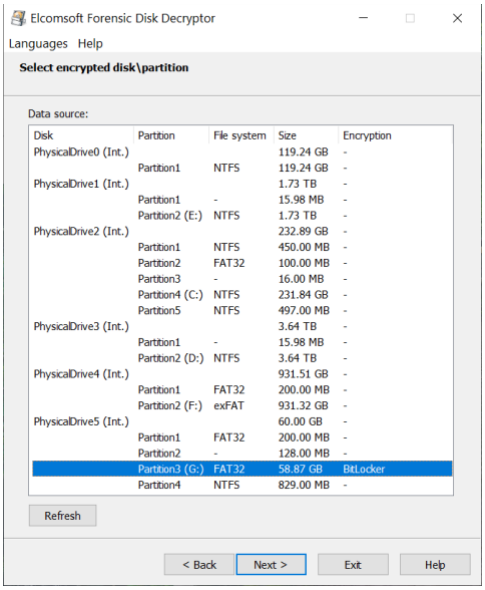


Откройте образ диска или сам диск (в примере ниже мы использовали физический жёсткий диск).

[62] https://www.elcomsoft.com/edpr.html

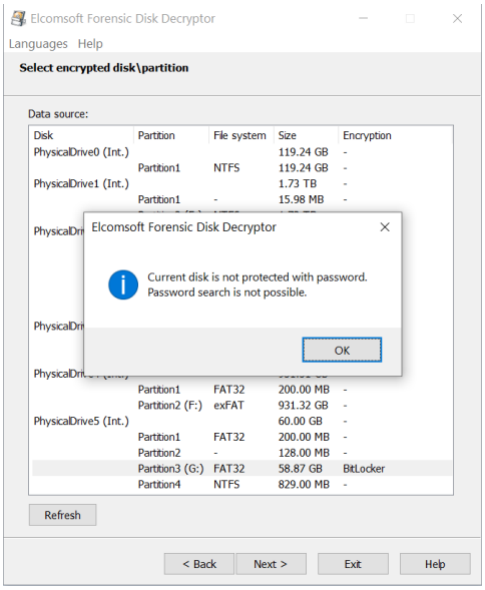


EFDD отобразит список зашифрованных томов. Выберите один из них.



Нажмите «Next» для сохранения метаданных шифрования.

Важно: подобрать пароль можно в том и только в том случае, если используется протектор "только пароль". Все остальные протекторы (с участием TPM, ключей или сертификатов) такой атаке не поддаются. Чтобы сэкономить ваше время, EFDD предупредит о подобных ситуациях:



Если такое произойдёт, используйте альтернативный вектор атаки.

Шаг 1.2. Извлечение метаданных шифрования BitLocker посредством Elcomsoft System Recovery.

Традиционный подход к извлечению информации требует разборки компьютера, извлечения жёстких дисков и создания их виртуальных образов. Однако для атаки на пароль зашифрованного тома достаточно нескольких килобайт метаданных шифрования. Метаданные можно извлечь значительно быстрее, не извлекая жёсткие диски.

Elcomsoft System Recovery позволяет сэкономить время, загрузив компьютер с портативного накопителя. Программа автоматически обнаруживает шифрование диска и позволяет извлечь метаданные шифрования, необходимые для подбора исходного пароля.

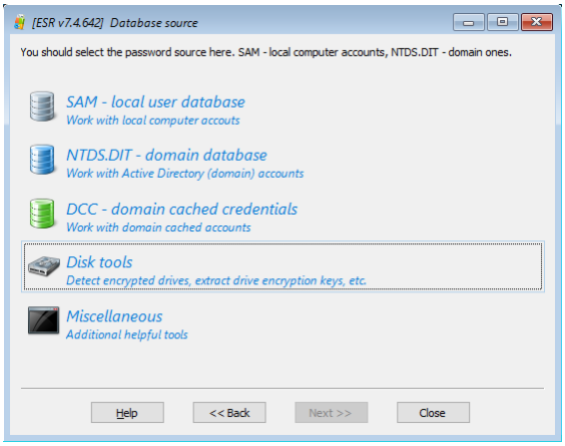
Установите Elcomsoft System Recovery[63] на ваш компьютер (не на компьютер подозреваемого!)

Создайте загрузочный накопитель. Обязательно укажите правильную конфигурацию целевой системы (BIOS или UEFI, 32-разрядная или 64-разрядная). Как правило, имеет смысл использовать быстрый USB-накопитель объёмом не менее 32 ГБ. Инструкция по созданию загрузочной флешки находится здесь[64].

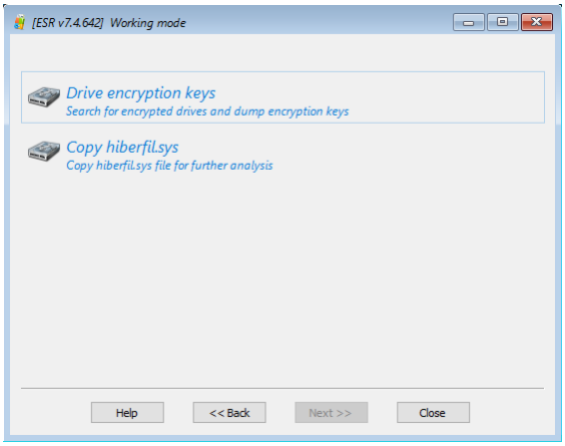
Загрузите с созданного накопителя компьютер, с которого нужно извлечь метаданные.

Elcomsoft System Recovery запустится автоматически. Выберите пункт **Disk tools**.

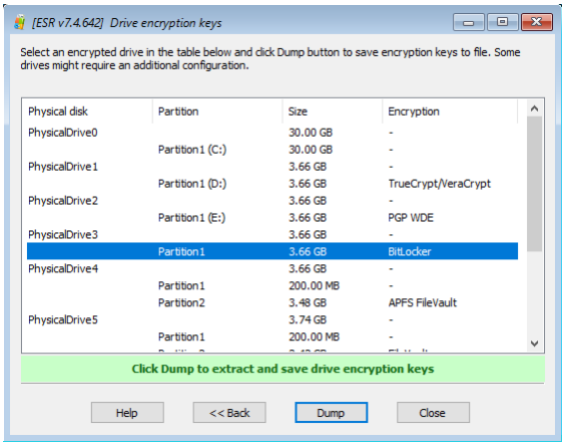
[63] https://www.elcomsoft.com/esr.html
[64] https://blog.elcomsoft.com/2019/04/a-bootable-flash-drive-to-extract-encrypted-volume-keys-break-full-disk-encryption/



Выберите пункт **Drive encryption keys**.



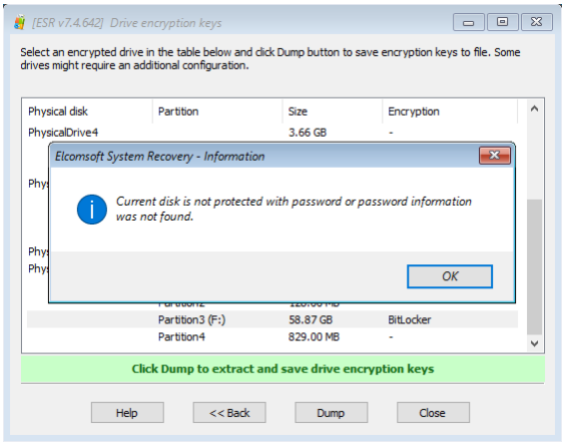
Elcomsoft System Recovery выведет список найденных разделов.



Выберите зашифрованный том.

Метаданные шифрования сохранятся на USB накопителе. Перенесите созданные файлы в Elcomsoft Distributed Password Recovery для настройки атаки.

Внимание: подобрать пароль можно в том и только в том случае, если используется протектор "только пароль". Все остальные протекторы (с участием TPM, ключей или сертификатов) такой атаке не поддаются. Чтобы сэкономить ваше время, ESR предупредит о подобных ситуациях:



Шаг 2. Восстановление оригинального пароля к тому в Elcomsoft Distributed Password Recovery

Запустите Elcomsoft Distributed Password Recovery

Откройте метаданные шифрования, сохранённые на предыдущем шаге.

Настройте и запустите атаку.

Хотя эти три шага кажутся простыми, выполнение атаки методом полного перебора — один из наименее эффективных способов взломать шифрование BitLocker. Мы настоятельно рекомендуем настроить интеллектуальную атаку на основе шаблонов, которые можно определить, проанализировав существующие пароли пользователя. Эти пароли можно извлечь из учётной записи пользователя Google, Связки ключей macOS, iOS или iCloud, учётной записи Microsoft или непосредственно с компьютера пользователя. Существующие пароли пользователя подсказывают, какие группы символов могут быть использованы.

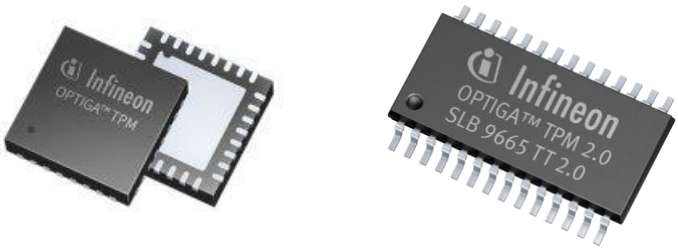
18.6. Расшифровка данных, защищённых модулем TPM

Исследование компьютера, системный накопитель которого зашифрован посредством BitLocker, может оказаться намного сложнее, если ключ шифрования основан не на установленном пользователем пароле, а на данных, которые защищены аппаратным модулем TPM. В этом разделе рассказывается об особенностях защиты ключей в TPM и возможных способах обхода этой защиты.

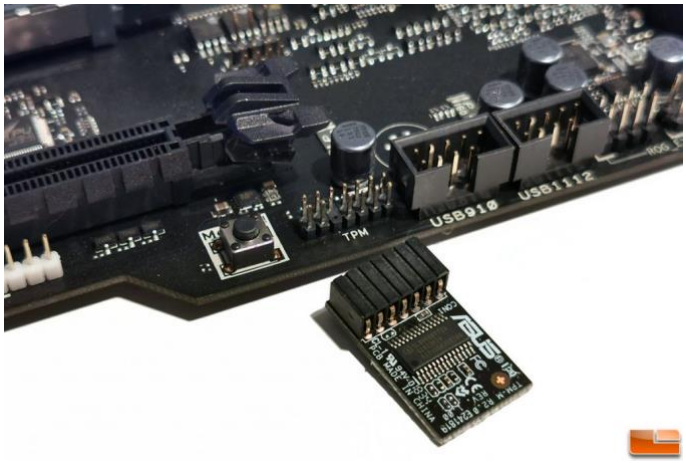
18.6.1. Что такое TPM?

Trusted Platform Module (TPM) – аппаратно-программная подсистема безопасности, использующаяся BitLocker для хранения криптографических ключей в персональных компьютерах. Она может быть реализована как в виде отдельного чипа, установленного на материнской плате компьютера, так и являться частью центрального процессора (технология Intel PTT). В мобильных устройствах чип TPM чаще всего распаян на материнской плате, в то время как для настольных компьютерах чип поставляется опционально в виде отдельного модулем.

Чипы TPM Infineon Optiga:



Отдельный модуль TPM для материнских плат Asus:



Система состоит из криптографического процессора и встроенной памяти. Официально устройства с TPM в Россию не поставляются, так как содержат несертифицированные средства шифрования. Несмотря на это, российские эксперты регулярно сталкиваются с компьютерами, на которых этот чип присутствует либо в аппаратном виде, либо в виде эмулятора Intel PTT.

С точки зрения шифрования BitLocker, TPM обеспечивает безопасные генерацию, хранение и ограничение использования криптографических ключей. Операционные системы предоставляют разработчикам интерфейсы для работы с TPM, а также используют TPM для работы с ключами шифрования.

При проектировании системы шифрования дисков разработчики Windows использовали модель угроз, предотвращающую следующие события:

- авторизованный вход в операционную систему в обход пароля пользователя;
- перенос диска на другой компьютер и его анализ;
- изменение конфигурации компьютера с целью анализа диска;
- запуск на компьютере других операционных систем для доступа к диску.

При этом для пользователя использование системы не представляет никаких неудобств, и в большинстве случаев ему достаточно просто включить компьютер и ввести пароль от учётной записи. Защиту можно усилить, установив на BitLocker дополнительный PIN-код или сохранив секретный элемент на USB накопителе.

18.6.2. Как устроена защита

BitLocker использует симметричное шифрование диска, как и остальные подобные приложения. Шифрование данных осуществляется средствами центрального процессора.

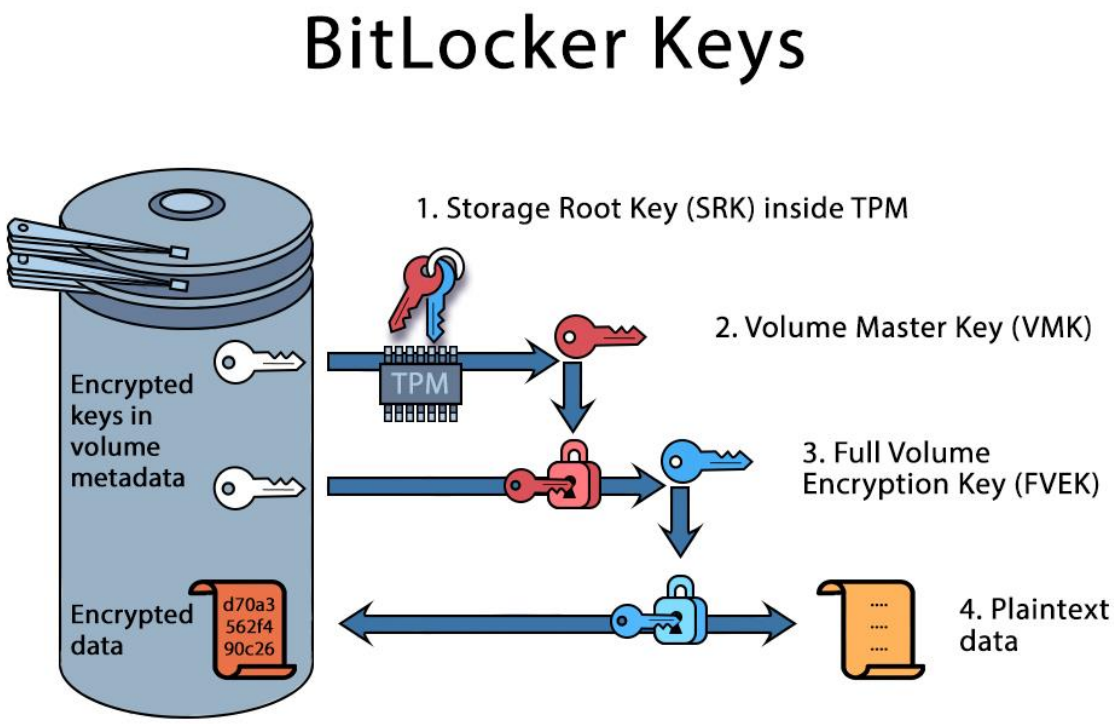
Основным секретным элементом является мастер-ключ, который может быть получен следующими способами:

– расшифрован паролем на диск, если используется такая защита;

– расшифрован ключом восстановления (Recovery Key). Ключ восстановления генерируется при создании любого контейнера или диска BitLocker и сохраняется пользователем либо в файл, либо в облако Microsoft. При некоторых условиях ключ сохраняется в облако Microsoft автоматически, без уведомления пользователя;

– извлечён из модуля TPM при соблюдении определенных условий.

Схема работы BitLocker с системой TPM:



В процессе работы модуля TPM выстраивается «цепочка доверия», которая сохраняется в регистрах PCR (Platform Configuration Register).

Рассмотрим работу TPM модуля по шагам:

1. Включается питание компьютера. Управление передаётся первому «доверенному» модулю, который имеет название SRTM (Static root of trust for measures). Обычно этот модуль находится в ПЗУ материнской платы и не может быть изменён. Уязвимость в этом модуле может поставить под угрозу всю систему безопасности. Эффект подобной уязвимости можно наблюдать в эксплоите checkm8 для платформы Apple iOS. SRTM делает первую запись в цепочке: подсчитывает хэш (контрольную сумму) от программного кода BIOS и записывает его в регистр PCR.

2. Управление передаётся UEFI BIOS, который формирует дальнейшие компоненты цепочки. Анализируется конфигурация компьютера, разбивка жёсткого диска, загрузчик (boot

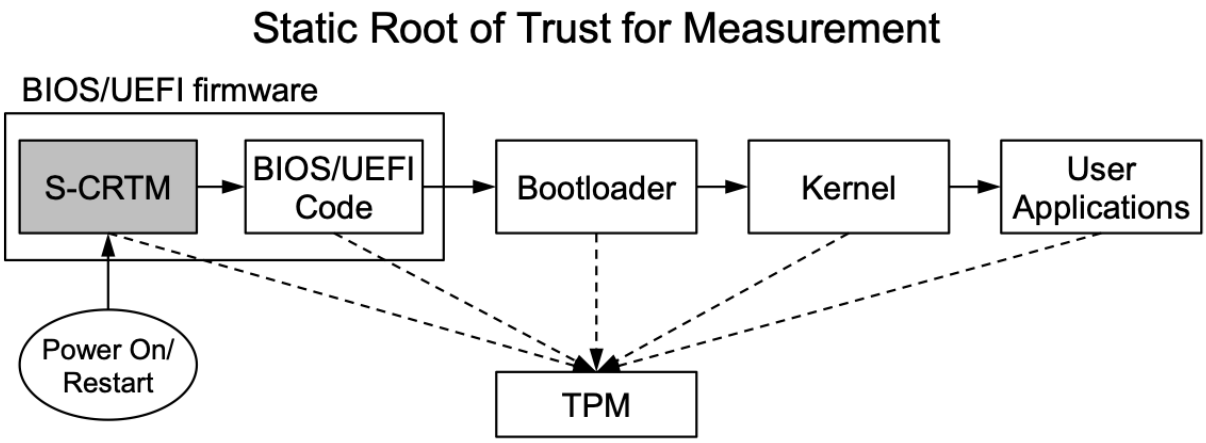
loader), загрузочные секторы диска (Master Boot Record) и множество других параметров. При этом в хешировании полученных данных участвует и предыдущий регистр PCR. Таким образом, все компоненты цепочки связаны между собой и любое нарушение приведёт к изменению содержимого PCR регистров.

3. Заполнив несколько PCR регистров, BIOS передаёт управление загрузчику, который запускает код из MBR жёсткого диска. В цепочке загрузки появляется ещё несколько записей.

4. Наконец, запускается ядро операционной системы, которое тоже записывает в цепочку свои параметры.

Таким образом, при загруженной операционной системе будет получен уникальный набор контрольных сумм, хранящихся в PCR регистрах модуля TPM. Модуль TPM не позволяет произвольным образом изменить содержимое PCR регистров; можно лишь добавить очередной компонент цепочки.

Загрузка компьютера с TPM модулем:



18.6.3. Включение шифрования BitLocker

В момент, когда пользователь включает шифрование жёсткого диска BitLocker, по закону случайных чисел генерируется мастер-ключ, а также ключ восстановления. Мастер-ключ записывается в модуль TPM, а также шифруется при помощи ключа восстановления и в таком виде сохраняется в заголовке диска. При перезапуске компьютера происходит следующее:

1. Все PCR регистры обнуляются.
2. Происходит инициализация, запуск BIOS, bootloader, MBR, ядра операционной системы.
3. Операционная система пытается получить ключ шифрования диска из TPM. При запросе TPM чип анализирует содержимое цепочки, хранящейся в регистрах PCR. Если цепочка повреждена, ключ шифрования не выдаётся, в результате чего операционной системой выдаётся сообщение о необходимости ввода ключа восстановления.

Таким образом, при выключенном компьютере ключ шифрования диска можно получить из модуля TPM только в случае запуска оригинальной системы. Изменение любого компонента системы приведёт к необходимости ввода Recovery ключа.

18.6.4. Как работать с защитой TPM?

Чаще всего в лабораторию попадает выключенный компьютер, о конфигурации которого ничего неизвестно. Самый первый шаг, который необходимо сделать в этой ситуации – снять образ диска. Это можно сделать, например, при помощи утилиты Elcomsoft System Recovery. Перед снятием образа будет отображён список разделов диска, а также способ шифрования разделов, если шифрование присутствует. Если включена защита диска при помощи TPM, программа сообщит, что диск зашифрован BitLocker-ом, но хэш пароля извлечь невозможно. Для расшифровки диска понадобится найти либо ключ восстановления, либо мастер-ключ, хранящийся в TPM модуле. О том, как извлечь ключ восстановления из облака, мы уже рассказали в предыдущих разделах. Ниже мы поговорим о том, как получить ключ из других источников.

18.6.5. Получение мастер-ключа из памяти компьютера

После снятия образа диска можно попробовать включить компьютер и загрузиться с основного диска, защищённого BitLocker-ом. Если пользователь не установил пароль на вход в операционную систему, либо этот пароль известен, диск расшифруется полученным из TPM ключом. Исключение составляет ситуация, когда доступ к модулю TPM защищён дополнительным PIN-кодом. При нескольких попытках неправильного ввода такого кода модуль TPM блокирует доступ к мастер-ключу и доступ к диску становится возможным только при вводе ключа Recovery. Если попытка загрузить ОС и войти в систему оказалась успешной, мастер-ключ BitLocker-а будет находиться в оперативной памяти компьютера. Его можно найти, используя портативную версию Elcomsoft Forensic Disk Decryptor. Этой же программой можно подключить снятый образ диска для анализа.

Конечно же, в этом случае возможен и анализ загруженной системы с активной пользовательской сессией. Но получение мастер-ключа и работа с образом более надёжна; помимо прочего, будет получен абсолютно точный образ системы, которая была изъята, без изменений, произошедших при старте ОС.

18.6.6. Атаки методами холодной загрузки и через порты FireWire/Thunderbolt

Если загрузка ОС произошла успешно, но невозможно войти в систему, так как неизвестен пароль пользователя, можно попробовать прочитать содержимое памяти компьютера. Существует два известных способа: прямой доступ к памяти через шину PCI и метод «холодной загрузки» (cold boot).

Интерфейсы FireWire, Thunderbolt и PC Card имеют прямой доступ к шине PCI, которая, в свою очередь, имеет прямой доступ к памяти компьютера (Direct Memory Access или DMA). Компьютеры с ОС Windows довольно редко оснащены такими интерфейсами, но в ряде случаев такие интерфейсы присутствуют (например, на компьютерах Intel NUC или при установке Windows на Мак с помощью драйверов Bootcamp). Для снятия образа памяти компьютера через

шину PCI можно воспользоваться бесплатной утилитой inception[65], установив её на любой компьютер с Linux.

К сожалению, такой способ работает только для Windows 7 и 8. В более старших версиях Windows доступ DMA через Thunderbolt уже закрыт. Образ памяти, сделанный в inception, можно загрузить в Elcomsoft Forensic Disk Decryptor и, как уже было описано выше, найти мастер-ключ, с помощью которого можно либо полностью расшифровать образ диска, либо подключить его к системе для анализа.

Ещё один вид атаки основан на том, что содержимое оперативной памяти компьютера обнуляется не мгновенно, а лишь спустя несколько секунд после выключения питания. Многие модули памяти способны сохранять своё состояние в течение нескольких минут, если их охладить до отрицательной температуры. На этом их свойстве и основана атака методом «холодной загрузки» (cold boot). Для атаки потребуется любой баллончик с хладагентом, например, предназначенный для тестирования термонестабильных электронных компонентов.
Последовательность действий следующая. Включается исследуемый компьютер, память замораживается при помощи баллончика, сразу отключается питание (ни в коем случае нельзя делать штатный shutdown средствами операционной системы). Далее следует перезагрузка с USB накопителя с Linux, на котором установлено расширение ядра LiME[66]. Наконец, создаётся образ оперативной памяти.

На практике этот способ достаточно сложен, и рекомендуется к использованию в качестве последней меры.

18.6.7. Атака на TPM модуль через Sleep Mode

В любых системах обеспечения безопасности встречаются уязвимости. Не избежали этой участи и модули TPM. В 2018 году корейские исследователи Seunghun Han, Wook Shin, Jun-Hyeok Park и HyoungChun Kim из National Security Research Institute представили на конференции Usenix научную работу под названием «Страшный сон»[67].

Когда компьютер уходит в «спящий режим», TPM сохраняет своё состояние в NVRAM, а при выходе из этого режима восстанавливает его. И вот в этот момент некоторые модели модулей

[65] https://github.com/carmaa/inception
[66] https://github.com/504ensicsLabs/LiME
[67] https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-han.pdf

TPM позволяют подменить содержимое PCR регистров. Модуль TPM также ведёт свой внутренний журнал, что позволяет узнать всю «цепочку доверия» в тот момент, когда в штатном режиме загружалась Windows, и модуль отдавал мастер-ключ шифрования диска. Исследователи тут же поставили в известность крупнейших производителей материнских плат: Intel, Lenovo, Gigabyte, Dell, hp. Уязвимость была закрыта в обновлениях BIOS. Однако очень немногие пользователи устанавливают обновления BIOS, так что в мире ещё много компьютеров, уязвимых к этой атаке.

Seunghun Han написал две утилиты:

Napper for TPM: https://github.com/kkamagui/napper-for-tpm[68]

Имеет смысл запустить сначала эту программу. Это утилита для проверки TPM модуля на предмет наличия уязвимости «страшных снов». На странице есть ссылка на скачивание образа Live CD; достаточно записать его на USB накопитель (для этих целей можно воспользоваться отечественной программой Rufus) и загрузить с неё исследуемый компьютер.

Вторая утилита – это сам эксплойт: https://github.com/kkamagui/bitleaker[69]

К сожалению, её нет в виде Live CD, поэтому придётся установить Ubuntu на USB накопитель или внешний диск, а потом собрать и установить Bitleaker согласно инструкции. Для загрузки этой системы нужно либо отключить Secure Boot, либо подписать модифицированные загрузчик и ядро своей подписью и внести публичный ключ в BIOS компьютера. Подробную инструкцию можно найти, например, здесь[70].

Учтите, что добавление нового доверенного сертификата тоже изменяет содержимое регистров PCR, поэтому мы рекомендуем просто отключить Secure Boot при загрузке.

18.6.8. Атака на TPM путем анализа сигналов

Модуль TPM «общается» с компьютером через шину данных LPC (Low Pin Count). Эта шина используется для передачи данных от «медленных» устройств, к примеру, последовательных портов COM, и имеет частоту всего 33 МГц. Передаваемые по шине данные никак не зашифрованы, поэтому есть возможность перехватить передаваемый мастер-ключ путём анализа сигналов. Denis Andzakovic демонстрирует, как у него это получилось для TPM версий 1.2 и 2.0[71].

Для версии TPM 1.2 он использует логический анализатор DSLogic Plus (цена в России около 10 тыс рублей), имеющий интерфейс USB и позволяющий анализировать до 16 каналов одновременно. Впрочем, этот анализатор автор не советует использовать, так как пришлось решать проблемы с синхронизацией и даже модифицировать его прошивку. Но, тем не менее, результат получен и мастер-ключ успешно извлечён из модуля.

Для версии TPM 2.0 использовалось ещё более дешёвое устройство — Lattice ICEStick. Это FPGA модуль с интерфейсом USB, в который можно загрузить прошивку, предназначенную специально для сниффинга TPM модулей[72].

---

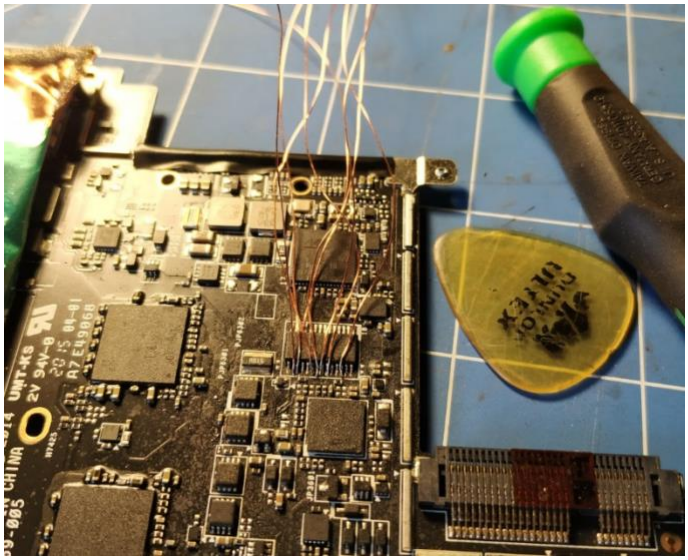
[68] https://github.com/kkamagui/napper-for-tpm
[69] https://github.com/kkamagui/bitleaker
[70] https://ubuntu.com/blog/how-to-sign-things-for-secure-boot
[71] https://pulsesecurity.co.nz/articles/TPM-sniffing
[72] https://github.com/denandz/lpc_sniffer_tpm

Осталось лишь аккуратно припаять проводки к нужным ножкам TPM чипа (для материнских плат, в которых модуль TPM вставляется в специальный разъём, достаточно просто подключиться между разъёмом и модулем), включить сниффер и получить мастер-ключ.

Конечно же, если BitLocker защищён ещё и PIN-кодом, такой способ не сработает. Очевидно, что этот способ не работает и для Intel PTT, так как в этом случае нет физического доступа к интерфейсу модуля.

FPGA Lattice iCEStick:

Подключение TPM чипа:



Модуль TPM в сочетании с BitLocker обеспечивает достаточно стойкую защиту дисков от несанкционированного доступа. Несмотря на то, что сам чип не занимается шифрованием диска, в отличие от, например, чипа T2, получить доступ к ключу шифрования — непростая задача. Все описанные способы извлечения, безусловно, должны быть в арсенале эксперта-криминалиста и использоваться в соответствии с ситуацией.

18.7. VeraCrypt и TrueCrypt

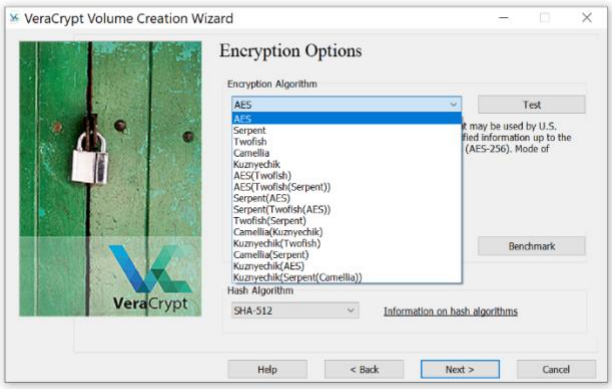
VeraCrypt – фактическая замена популярной программе шифрования дисков TrueCrypt и самый распространённый на сегодняшний день крипто-контейнер. В сравнении с TrueCrypt, VeraCrypt предлагает более широкий выбор алгоритмов шифрования и хеширования паролей.

VeraCrypt использует собственный формат контейнеров, отличный от формата контейнеров TrueCrypt. В то же время подходы, описанные для VeraCrypt, можно использовать и для расшифровки контейнеров TrueCrypt.

18.7.1. Алгоритмы шифрования VeraCrypt

В TrueCrypt пользователям предлагался выбор из нескольких алгоритмов шифрования, в том числе несколько вариантов с последовательным шифрованием данных несколькими

алгоритмами. В VeraCrypt пользователю предлагается на выбор пять алгоритмов шифрования (AES, Serpent, Twofish, Camellia и «Кузнечик») и десять вариантов их последовательного использования.



Все поддерживаемые алгоритмы и их комбинации различаются в скорости работы, однако атака на ключ шифрования бесполезна как в случае с шифром по умолчанию, в роли которого выступает AES-256, так и в случае выбора любого другого алгоритма или их последовательности. Таким образом, выбор алгоритма шифрования способен повлиять на скорость доступа к зашифрованным данным, но не на скорость перебора паролей.

VeraCrypt не сохраняет информацию об использованном алгоритме шифрования в заголовке крипто-контейнера. Из-за этого в процессе настройки атаки необходимо правильно указать алгоритм, которым зашифрованы данные (если он неизвестен, то в первую очередь выбрать AES как опцию по умолчанию, во вторую – список из всех доступных алгоритмов). Если алгоритм шифрования будет указан неверно, то пароль не будет найден. В то же время выбор всего списка поддерживаемых алгоритмов пропорционально замедлит скорость атаки.

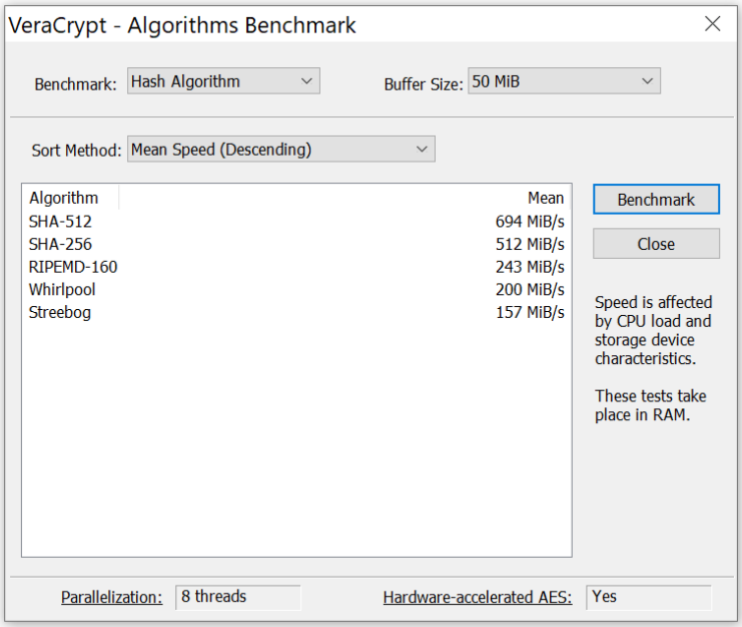
18.7.2. Функции преобразования пароля (хэш-функции)

В процессе работы VeraCrypt использует двоичный ключ переменной длины, так называемый Data Encryption Key или Media Encryption Key (MEK), который получается в результате нескольких преобразований, в одном из которых участвует пароль пользователя. Media Encryption Key для единожды созданного контейнера неизменен; он хранится в зашифрованном (точнее, «обёрнутом», wrapped) виде в составе контейнера, а в «развёрнутом» виде используется для доступа к данным.

Ключ шифрования данных MEK в обязательном порядке шифруется так называемым «ключом шифрования ключа шифрования» **Key Encryption Key (KEK)**. Без KEK невозможно расшифровать MEK, а без MEK невозможно расшифровать данные. Такая многоступенчатая схема нужна для того, чтобы пользователь имел возможность сменить пароль от зашифрованного диска без обязательной расшифровки и перешифровки всего содержимого. Однако роль пары ключей MEK/KEK этим сценарием не ограничивается, обеспечивая также возможность моментального и безвозвратного уничтожения данных. Пользователю достаточно уничтожить несколько блоков данных в заголовке контейнера (физически перезаписав область, в которой хранится MEK), и расшифровать контейнер не удастся, даже если точно известен пароль. Эта операция занимает меньше секунды.

Ключ KEK получается следующим образом. VeraCrypt проводит циклическую последовательность односторонних (необратимых) математических преобразований – хэш-функций, причём количество циклов достаточно велико: по умолчанию преобразование производится 500,000 раз. Таким образом, с настройками по умолчанию на вычисление ключа KEK на основе введённого пароля VeraCrypt потратит от одной до 5-6 секунд.

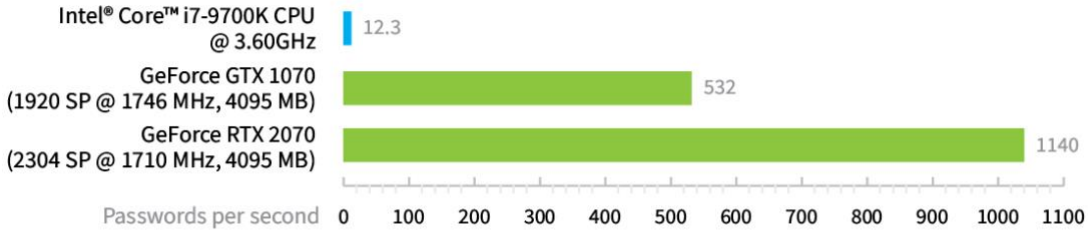
Выбор алгоритма хэширования сильнейшим образом влияет на скорость атаки: самый нестандартный и самый медленный алгоритм оказывается и наиболее трудоёмким в процессе перебора. Производительность алгоритмов хэширования на единственном CPU Intel i7-9700K выглядит следующим образом:



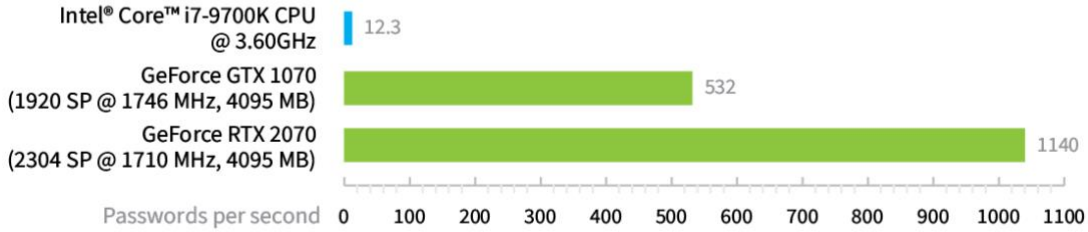
Так же, как и в случае с алгоритмами шифрования, для проведения атаки на зашифрованный диск необходимо указать точный алгоритм хэширования либо провести атаку на весь спектр алгоритмов.

Elcomsoft Distributed Password Recovery демонстрирует следующие цифры производительности для различных алгоритмов хэширования:

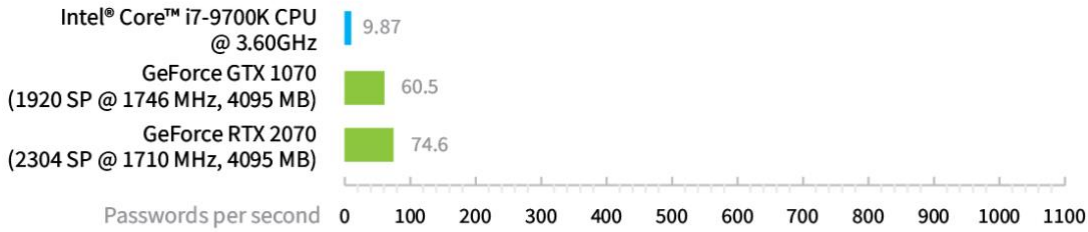
VeraCrypt STANDARD SHA512 AES



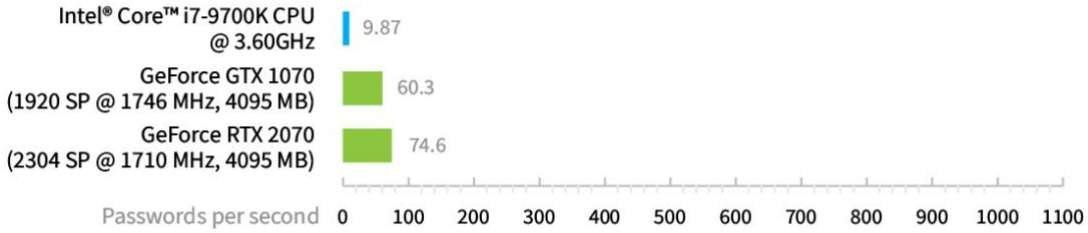
VeraCrypt STANDARD SHA512 SERPENT



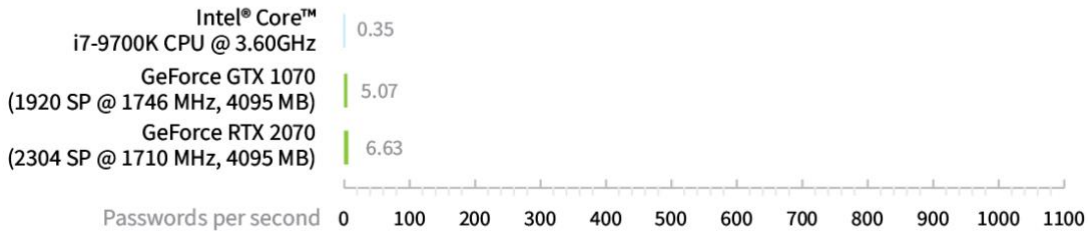
VeraCrypt STANDARD WHIRLPOOL AES



VeraCrypt STANDARD WHIRLPOOL SERPENT

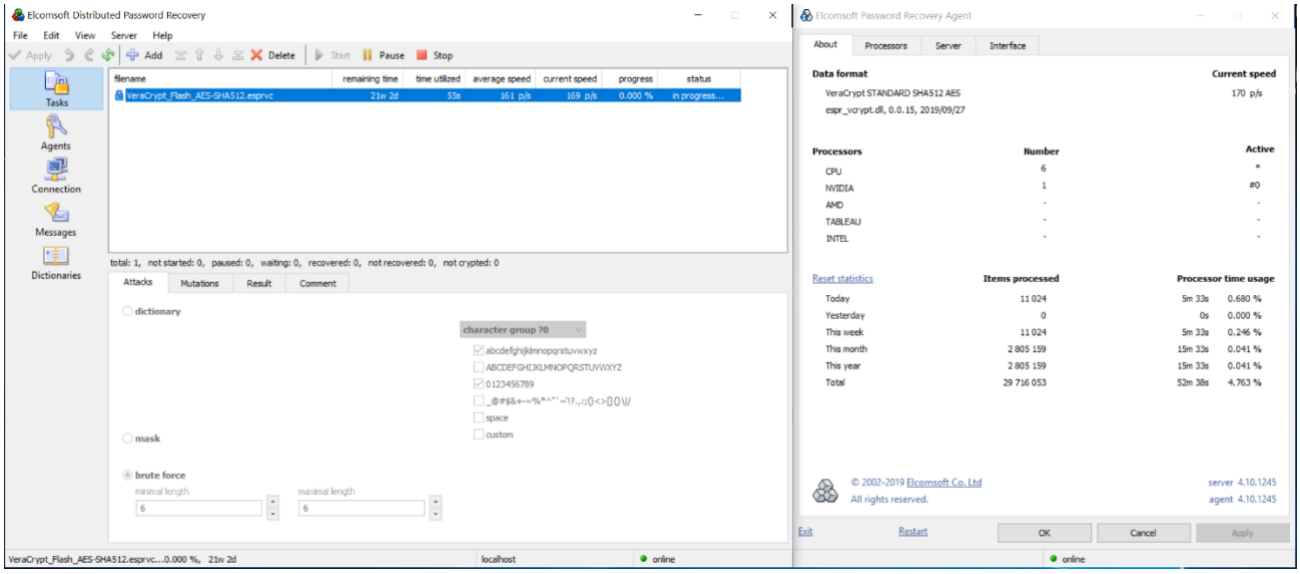


VeraCrypt STANDARD UNKNOWN- HASH UNKNOWN-ENCRYPT



Как можно заметить, скорость перебора в гораздо большей степени зависит от функции хеширования и в меньшей – от алгоритма шифрования. Последовательное использование нескольких шифров уменьшит скорость перебора, но разница несравнима влиянием, которое на скорость перебора оказывает выбор хэш-функции. Так, выбор Whirlpool вместо SHA-512 замедляет скорость перебора с 1 140 до 74,6 паролей в секунду. Самой медленной будет атака по всему спектру возможностей: 6,63 паролей в секунду, в 171 раз медленнее атаки с настройками по умолчанию.

Скорость атаки в стандартной конфигурации (алгоритм шифрования AES, хэш-функция – SHA-512) – 1 140 паролей в секунду с загрузкой всех ядер процессора и использованием вычислительных ресурсов видеокарты NVIDIA GeForce 2 070.



18.7.3. Число итераций PIM

VeraCrypt позволяет изменять количество итераций хэша путём настройки множителя PIM (Personal Iterations Multiplier). Значение множителя PIM определяет количество итераций, используемых для получения ключа шифрования из введённого пароля. Это значение пользователь может указать как в процессе создания зашифрованного контейнера, так и в любой другой момент. Для хэш-функций SHA-512 и Whirlpool VeraCrypt по умолчанию вычисляет число итераций как 15 000 + (PIM x 1 000).

Так же, как и алгоритмы шифрования и хэширования, значение множителя PIM не сохраняется в метаданных зашифрованного диска. В отличие от алгоритмов, которые VeraCrypt определяет автоматически в процессе монтирования крипто-контейнера, множитель PIM пользователю необходимо вводить вручную каждый раз во время монтирования зашифрованного диска.

В процессе настройки атаки необходимо указать точное значение множителя PIM, если оно отличается от стандартного. Если пользователь указал нестандартное значение множителя PIM, и это значение вам неизвестно, восстановление пароля к зашифрованному диску будет невозможно.

18.7.4. Использование Elcomsoft Distributed Password Recovery для восстановления паролей VeraCrypt

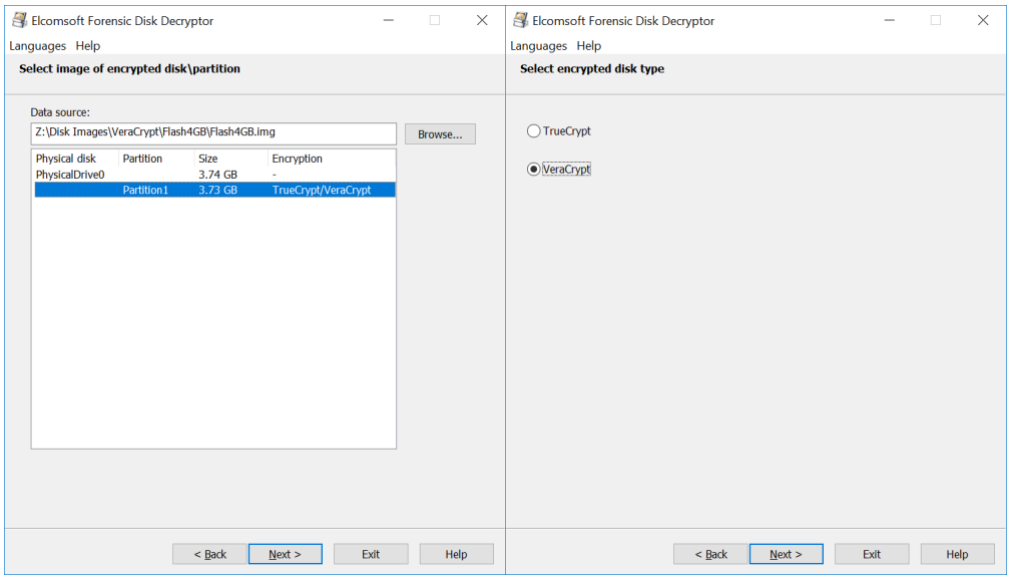
Elcomsoft Distributed Password Recovery поддерживает все возможные комбинации алгоритмов шифрования и хеширования, включая атаку по всему спектру вариантов. Настройка атаки осуществляется в приложении Elcomsoft Forensic Disk Decryptor на этапе извлечения заголовка от зашифрованного диска. Таким образом для того, чтобы настроить атаку на зашифрованный диск VeraCrypt или TrueCrypt, необходимы два этапа, в которых используется два различных инструмента.

Этап 1: извлечение метаданных шифрования

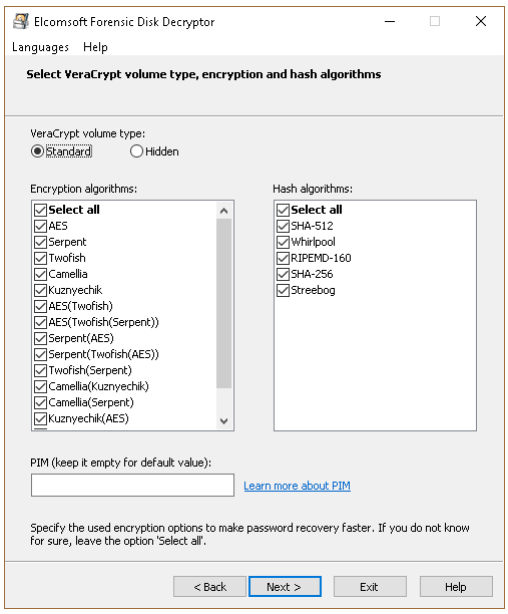
Как было рассказано выше, корректный выбор алгоритма шифрования, хэш-функции и множителя итераций PIM напрямую влияет на возможность восстановления пароля.

Выбор алгоритма или списка алгоритмов шифрования и хэширования осуществляется в процессе извлечения метаданных шифрования утилитой Elcomsoft Forensic Disk Decryptor следующим образом.

Запустите Elcomsoft Forensic Disk Decryptor и выберите зашифрованный диск или его образ. Укажите, TrueCrypt или VeraCrypt использовался для шифрования.



В окне выбора алгоритма шифрования укажите алгоритм, если он известен, или Unknown для того, чтобы в процессе атаки опробовать все алгоритмы. Также укажите алгоритм хэш-функции, если он известен, или Unknown, чтобы опробовать все хэш-функции. Наконец, в поле “PIM” вы можете опционально указать значение множителя PIM, если оно отличается от стандартного и точно известно. Если множитель PIM отличается от стандартного, а его значение – неизвестно, результат атаки будет неудачным, а пароль от зашифрованного диска восстановить не удастся.



Параметр PIM – опциональный; указывать его не обязательно. Если значение PIM не вводить, то будет использоваться значение по умолчанию:

– если зашифрован системный раздел, который использует хэш-функцию SHA-256: количество итераций = 200 000;

– если зашифрован системный раздел, который использует хэш-функцию RIPEMD-160: количество итераций = 327 661;

– если зашифрован несистемный раздел либо атака производится на стандартный крипто-контейнер, использующий хэш-функцию RIPEMD-160: количество итераций= 655 331;

– если зашифрован несистемный раздел либо атака производится на стандартный крипто-контейнер, использующий хэш-функцию SHA-256, SHA-512 или Whirlpool: количество итераций= 500 000.

Множитель PIM используется в VeraCrypt с версии 1.12. TrueCrypt и более старые версии VeraCrypt не используют множитель, и число итераций для созданных в этих программах контейнерах всегда стандартно.

Этап 2: восстановление оригинального пароля в Elcomsoft Distributed Password Recovery

Elcomsoft Distributed Password Recovery позволяет проводить атаки с использованием как аппаратного ускорения (видеокарт AMD и NVIDIA), так и с использованием множества компьютеров, объединённых в единую вычислительную сеть. Тем не менее, если атака проводится на зашифрованный диск с неизвестными параметрами защиты, имеет смысл воспользоваться возможностями «умных» атак на основе как стандартных словарей, так и словарей, составленных из известных паролей пользователя.

Для начала атаки откройте в Elcomsoft Distributed Password Recovery метаданные шифрования, извлечённые на предыдущем шаге утилитой Elcomsoft Forensic Disk Decryptor. Настройки атаки (алгоритм или список алгоритмов шифрования и хэширования, значение множителя PIM) задаются на этапе извлечения метаданных шифрования в программе Elcomsoft Forensic Disk Decryptor; соответственно, дополнительные настройки в Elcomsoft Distributed Password Recovery указывать не потребуется.

Далее настройте и запустите последовательность атак. Подробно об этом рассказывается в соответствующих разделах.

Этап 3: монтирование или расшифровка диска в Elcomsoft Forensic Disk Decryptor.

После того, как пароль к зашифрованному диску будет восстановлен, вы сможете смонтировать или расшифровать диск в утилите Elcomsoft Forensic Disk Decryptor. Программа поддерживает физические диски, образы дисков и крипто-контейнеры.

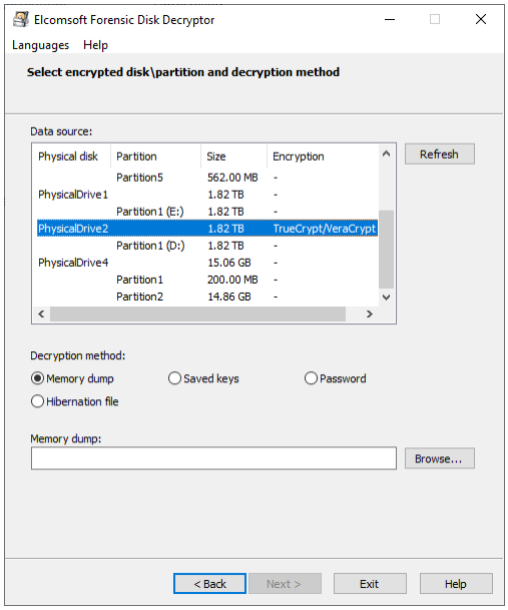
Внимание: с целью расшифровки или монтирования диска запускайте Elcomsoft Forensic Disk Decryptor на лабораторном компьютере, а не на исследуемом ПК. Потребуется установленная (а не портативная) версия Elcomsoft Forensic Disk Decryptor, т.к. в процессе установки также устанавливается драйвер виртуальных дисков, использующийся для монтирования зашифрованных дисков.

Поддерживаемые образы дисков:

- RAW/DD;
- EnCase .E01;
- VHD/VHDX (для работы с этими образами требуется Windows 8.1 или выше).

EFDD выводит подключенные устройства хранения и разделы, автоматически определяя тип шифрования. Вы можете либо расшифровать, либо смонтировать раздел для немедленного доступа. Последнее реализуется через ImDisk virtual disk driver установленный на ПК вместе с EFDD.

При монтировании или расшифровке диска потребуется любой пункт из списка:



- дамп памяти;
- сохранённый ключ;
- пароль, восстановленный на предыдущем шаге;
- файл гибернации;
- файл Active Directory (только BitLocker);
- ключ восстановления (для BitLocker, PGP WDE, FileVault2).

Выберите пункт «Password», после чего диск будет смонтирован или расшифрован на выбор.

18.7.5. Альтернативные способы расшифровки VeraCrypt

В ряде случаев восстановление оригинального пароля к контейнеру в разумные сроки не представляется возможным. В таких случаях стоит рассмотреть альтернативные варианты.

Извлечь готовый ключ шифрования и с его помощью смонтировать (или расшифровать целиком) зашифрованный раздел – самый быстрый и эффективный способ, которым можно воспользоваться. Суть его заключается в следующем.

Ключ шифрования данных хранится в оперативной памяти компьютера; он же попадает в файлы гибернации и подкачки. Наличие ключа в оперативной памяти требуется для того, чтобы программа-крипто-контейнер могла получить доступ к зашифрованным данным. Обратите внимание: ключ шифрования хранится в оперативной памяти независимо от того, какой алгоритм шифрования и хэширования пользователь выбрал в настройках контейнера. Таким образом, сложность этой атаки мало зависит как от выбора алгоритма шифрования, так и от способа преобразования пароля в двоичный ключ.

Существует несколько способов извлечения ключей шифрования. Если зашифрованный том был смонтирован во время изъятия компьютера, могут быть доступны следующие способы:

– **анализ оперативной памяти компьютера (ОЗУ).** Ключ шифрования хранится в оперативной памяти в течение всего времени, когда зашифрованный диск смонтирован;

– **файл(ы) подкачки.** Ключ шифрования может попадать или не попадать в файл подкачки. Тем не менее, их анализ (сканирование) занимает от нескольких минут до нескольких часов (что несравнимо с днями и неделями, которые потребуются для взлома пароля);

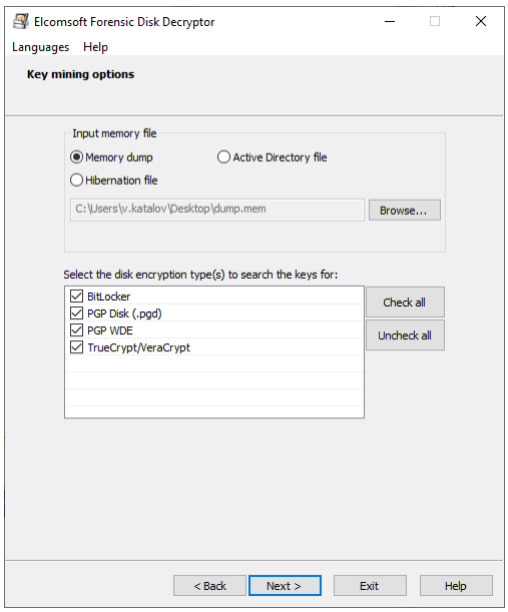
– **файл гибернации.** Windows использует файл гибернации для выгрузки части оперативной памяти компьютера на жёсткий диск, когда компьютер находится в спящем режиме (если включён гибридный спящий режим, а он включён по умолчанию). Кроме того, файл гибернации создаётся, когда компьютер находится в режиме гибернации (который по умолчанию отключён) и когда компьютер выключается (если активна функция быстрого запуска, которая включена по умолчанию).

Для извлечения ключей, снятия и анализа образа оперативной памяти используйте Elcomsoft Forensic Disk Decryptor. Внимание: образ оперативной памяти необходимо извлечь из компьютера пользователя в момент, когда зашифрованный диск смонтирован. Для этого требуется утилита из состава Elcomsoft Forensic Disk Decryptor; запускать утилиту необходимо на компьютере пользователя (требуется авторизованная пользовательская сессия с административными привилегиями).

Извлечение ключей шифрования

Для того, чтобы извлечь ключи шифрования, вам понадобится или несколько источников. Соответственно, в Elcomsoft Forensic Disk Decryptor нужно выбрать источник ключей шифрования (дамп памяти (memory dump) или файл гибернации hiberfil.sys) и тип шифрования (BitLocker, PGP или TrueCrypt/VeraCrypt).

О том, как создать снимок (дамп) оперативной памяти компьютера, рассказано в разделе, посвящённом Elcomsoft Forensic Disk Decryptor.

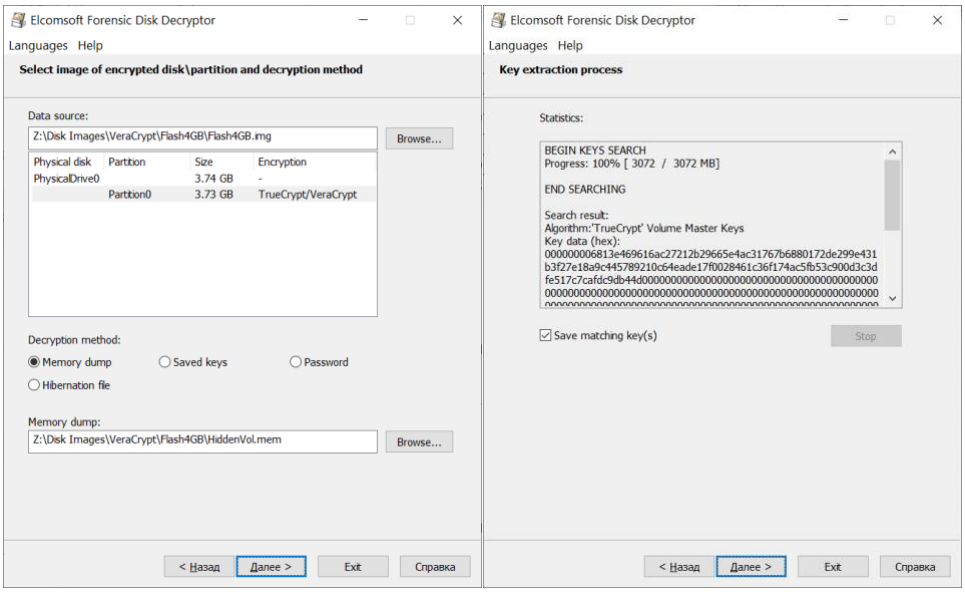


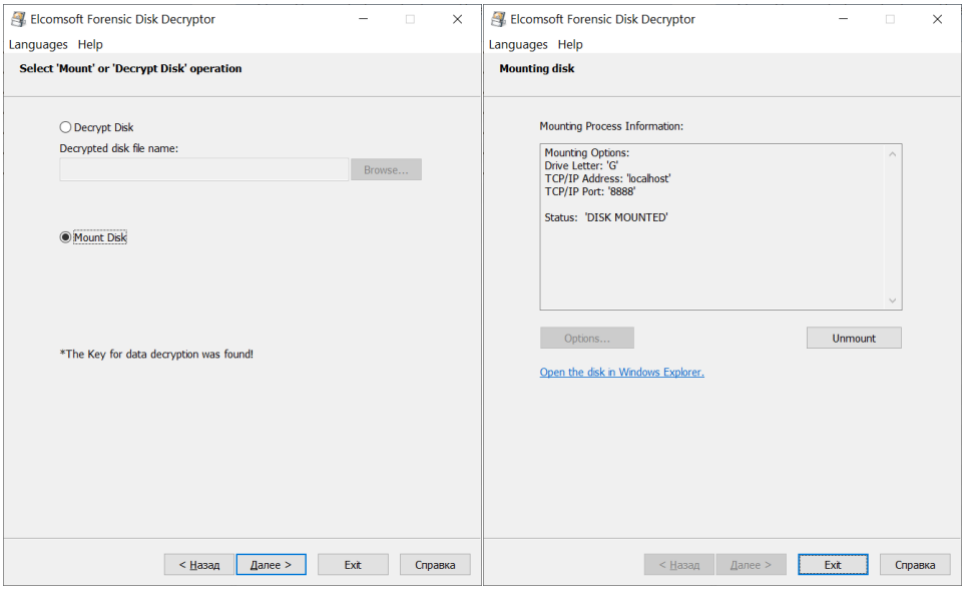
Если атака производится на диск BitLocker, то вы можете выбрать файл Active Directory (ntds.dit) в качестве источника.

После завершения процесса поиска отобразится список ключей. Вы можете сохранить их в файл для дальнейшего использования – монтирования или расшифровки диска.

Обратите внимание: при создании образа оперативной памяти зашифрованный диск должен быть смонтирован (разблокирован). Файл гибернации, соответственно, можно использовать, если компьютер переведён в состояние гибернации или «гибридного» сна. В противном случае ключи не сохраняются в памяти.

Поиск ключей – длительный и ресурсоёмкий процесс, поэтому рекомендуется ограничить поиск конкретными типами ключей.

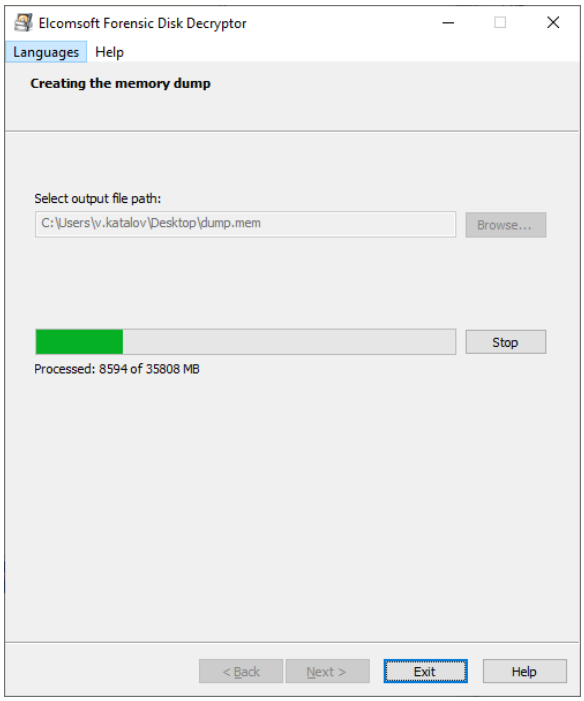




Создание образа оперативной памяти

В предыдущем разделе говорится об извлечении ключей шифрования из образа оперативной памяти компьютера.

После того, как диск смонтирован в систему (разблокирован), система сохраняет ключи шифрования в ОЗУ. Если у вас есть доступ к активной системе, в этом случае ключи можно вытащить простым способом. Выберите файл, в который нужно сделать дамп памяти, и нажмите Старт (Start). Для этой операции требуются права администратора.



Создание портативную версию (Create portable version).

Эта опция позволяет создать портативную версию программы, которая может запускаться со съёмного диска. Между обычной и портативной версиями есть следующие различия:

- портативная версия не требует установки; запустите 'efdd.exe' для работы;
- портативная версия не включает возможность создания другой портативной версии;
- портативная версия не может монтировать диски (может только расшифровать).

18.8. Защита от аппаратного ускорения перебора на примере Jetico BestCrypt Volume Encryption 4 и 5

Продукт BestCrypt Volume Encryption, разработанный финской компанией Jetico, представляет собой кроссплатформенный коммерческий инструмент для шифрования разделов дисков. Сам по себе BestCrypt имеет относительно небольшое распространение; вероятность столкнуться с ним на компьютере пользователя невелика.

В то же время от других продуктов шифрования дисков BestCrypt Volume Encryption отличается использованием нового алгоритма хеширования Scrypt, использующегося для преобразования пароля пользователя в двоичный ключ шифрования, который спроектирован таким образом, чтобы исключить возможность аппаратного ускорения перебора паролей с использованием видеокарт. Эта особенность оказывает влияние на методы, которые используются для доступа к зашифрованным данным.

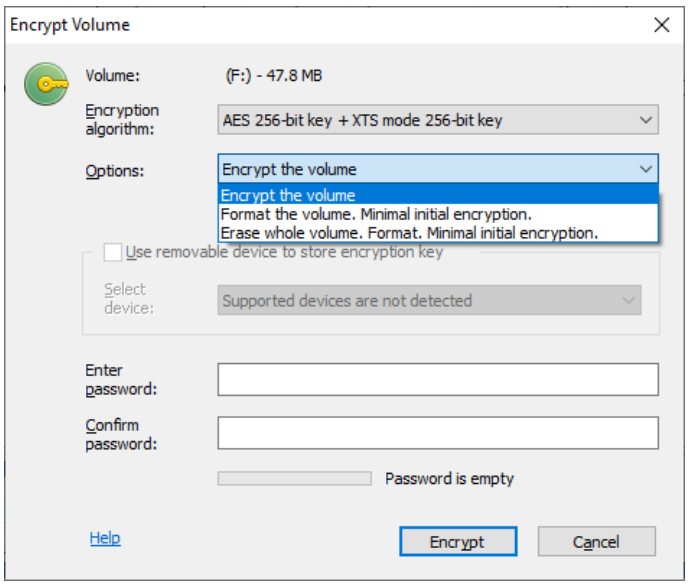
18.8.1. Алгоритм Scrypt исключает аппаратное ускорение перебора

От других продуктов шифрования дисков BestCrypt Volume Encryption отличается использованием нового алгоритма хеширования Scrypt, использующегося для преобразования пароля пользователя в двоичный ключ шифрования. Алгоритм Scrypt специально разработан для предотвращения атак, использующих аппаратное ускорение. В результате перебор паролей к BestCrypt Volume Encryption реализован только средствами центрального процессора; ускорение на GPU недоступно.

18.8.2. Алгоритмы шифрования

Так же, как и большинство других средств шифрования диска (в частности, VeraCrypt), BestCrypt поддерживает выбор алгоритмов шифрования. Поддерживаются алгоритмы AES, ARIA, Camellia, Serpent и Twofish. Разработчики BestCrypt утверждают, что каждый алгоритм реализован в максимально безопасной конфигурации, с ключом максимальной длины, в режиме шифрования XTS. Напомним, что реальная безопасность зашифрованного диска (и скорость перебора паролей к нему) совершенно не зависит от выбранного алгоритма шифрования.

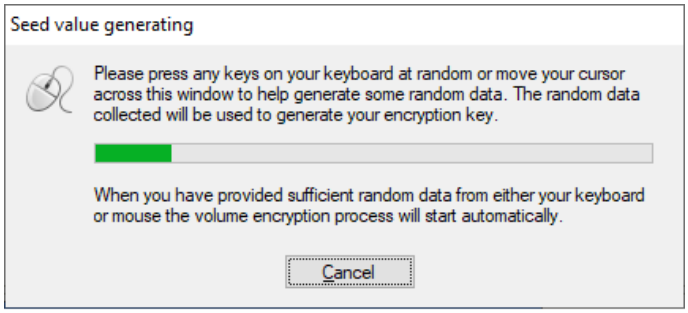
Выбор шифра влияет исключительно на скорость доступа к файлам и загрузку процессора: из всего списка AES — единственный алгоритм с аппаратным ускорением инструкциями AES-NI. Все остальные алгоритмы реализуются на современных процессорах программным способом, и чтение-запись файлов будут происходить заметно медленнее.



На безопасность влияет выбор хэш-функции для преобразования пароля в ключ, а также число итераций этой хэш-функции.

Хэш-функция.

Важнейший момент, необходимый для понимания принципа работы современных средств шифрования диска, заключается в том, что пароль пользователя не используется для шифрования данных — ни напрямую, ни в виде хэша. Данные зашифрованы двоичным ключом, который генерируется случайным образом:



Для чего тогда нужен пароль? Паролем пользователя (а точнее — двоичным ключом, полученным на его основе в результате многочисленных раундов одностороннего математического преобразования) будет зашифрован тот самый ключ, которым шифруются данные. Более того, в некоторых продуктах (например, BitLocker) используется ещё один ключ-посредник, который шифрует ключ шифрования данных, а сам защищается ключом, сгенерированным на основе пароля пользователя.

Как видим, для успешного подбора пароля нет необходимости расшифровывать данные, хранящиеся в зашифрованном диске; достаточно расшифровать ключ шифрования данных. Соответственно, для настройки атаки нет необходимости открывать весь зашифрованный раздел или контейнер — достаточно небольшого файла, в котором содержатся метаданные шифрования.

Однако вернёмся к хэш-функции. Традиционно в программах шифрования дисков используются хорошо изученные хэш-функции — SHA-512, SHA-256, Whirlpool (512-бит), а временами даже устаревшая и небезопасная SHA-1. Скорость вычисления этих функций высокая, атака получилась бы очень быстрой. Чтобы замедлить скорость подбора паролей, производители

средств шифрования используют многочисленные (десятки и сотни тысяч) итерации хеширования.

Разумеется, разработчики инструментов для взлома паролей не могли остаться в стороне. Так, в наших продуктах используется аппаратное ускорение средствами бытовых видеокарт, что даёт прирост скорости перебора в 50-500 раз в зависимости от формата и аппаратного обеспечения.

Этот факт, в свою очередь, не устроил разработчиков BestCrypt.

18.8.3. Отсутствие аппаратного ускорения

Если запустить перебор не на центральном процессоре компьютера, а на обычной бытовой видеокарте, даже встроенной в CPU, процесс перебора можно ускорить в 25-500 раз, что кратно снижает безопасность зашифрованного диска и требует использования более длинных и сложных паролей. Разработчики BestCrypt решили исключить возможность аппаратного использования, выбрав для функции преобразования пароля новый алгоритм хеширования Scrypt[73]. Этот алгоритм сравним по скорости вычисления на центральном процессоре с традиционным SHA-256, однако был спроектирован таким образом, чтобы для него невозможно (или очень сложно и дорого) было бы реализовать атаку с аппаратным ускорением. Суть аппаратного ускорения — в распараллеливании потоков, а для вычисления хэша Scrypt требуется большое количество оперативной памяти. Объём оперативной памяти в современных видеокартах позволяет одновременно запускать очень небольшое количество потоков, вычисляющих значение хэш-функции Scrypt; накладные расходы при этом заметно превышают выгоду от использования видеокарты.

В результате перебор паролей к дискам BestCrypt можно выполнять только средствами центрального процессора. Перебор получается небыстрый: 18 паролей в секунду на Intel Core i7-7700HQ CPU @ 2.80GHz (8 потоков) или 25 п/с на Intel Core i7-3930K CPU 3.20GHz (12 потоков). Соответственно, методом прямого перебора можно найти только самые простые пароли. Для атаки на более сложные пароли используются способы, учитывающие человеческий фактор.

Для сравнения, на том же процессоре Intel Core i7-3930K 3.2GHz x12 пароли к контейнерам BestCrypt Container Encryption находятся заметно быстрее.

BestCrypt Container Encryption, Intel Core i7-3930K CPU 3.20GHz (12 потоков):

```
sha3-512        53 п/с
Whirlpool-512   150 п/с
sha-512         196 п/с
Skein-512       262 п/с
sha-256         273 п/с
```

BestCrypt Volume Encryption, Intel Core i7-3930K CPU 3.20GHz (12 потоков):

```
Scrypt          25 п/с
```

[73] https://github.com/technion/libscrypt/blob/master/crypto_scrypt-nosse.c

18.8.4. Нет извлечения ключей из оперативной памяти

Для многих зашифрованных дисков извлечение ключа шифрования непосредственно из оперативной памяти устройства, файла подкачки или гибернации — самый быстрый способ добраться до информации. При соблюдении ряда условий можно выгрузить содержимое ОЗУ компьютера в файл и сканировать этот файл на предмет ключей шифрования, которые можно использовать для монтирования или расшифровки данных.

В настоящий момент мы не поддерживаем извлечение ключей BestCrypt из оперативной памяти. Эта функция в разработке.

18.8.5. BestCrypt Volume Encryption 4 и 5: пошаговое руководство

Наши инструменты могут взламывать пароли BestCrypt Volume Encryption 4 и 5, которые защищены шифрованием на основе паролей. Для этого выполните следующие действия.

Извлечение метаданных шифрования.

Первый шаг атаки — извлечение метаданных шифрования диска при помощи утилиты Elcomsoft Forensic Disk Decryptor, ограниченная версия которой входит в состав Elcomsoft Distributed Password Recovery.

Извлечение метаданных шифрования с использованием Elcomsoft Forensic Disk Decryptor:

1. Запустите Elcomsoft Forensic Disk Decryptor.
2. Выберите диск BestCrypt.
3. Сохраните метаданные шифрования в файл.
4. Откройте метаданные шифрования в Elcomsoft Distributed Password Recovery.
5. Альтернативный способ — использование загрузочного диска Elcomsoft System Recovery:
6. Подготовьте загрузочный USB накопитель в Elcomsoft System Recovery, запущенном на вашем компьютере (не на том, который будет исследоваться).
7. Загрузите исследуемый компьютер с созданного накопителя.
8. В Elcomsoft System Recovery выберите диск BestCrypt.
9. Сохраните метаданные шифрования в файл.
10. Перенесите метаданные шифрования на свой компьютер и откройте их в Elcomsoft Distributed Password Recovery.

Дальнейшая работа в Elcomsoft Distributed Password Recovery ведётся с метаданными шифрования. При настройке атаки имейте в виду невысокую скорость перебора; аппаратное ускорение перебора будет недоступно.

19. Зашифрованные виртуальные машины

Виртуальные машины, защищённые стойким шифрованием, получили широкое распространение в криминальной среде. Использование не оставляющих цифрового следа зашифрованных виртуальных машин позволяет злоумышленникам минимизировать утечку инкриминирующих данных. Количество преступников, использующих в своей деятельности специальным образом настроенные и защищённые виртуальные машины, трудно переоценить. Массовое использование виртуальных машин преступниками затрудняет работу органов правосудия. Инкриминирующие улики не покидают пределов контейнеров, защищённых

стойким шифрованием. Для того, чтобы получить доступ к уликам, потребуется восстановить оригинальный пароль, которым зашифрован образ виртуальной машины.

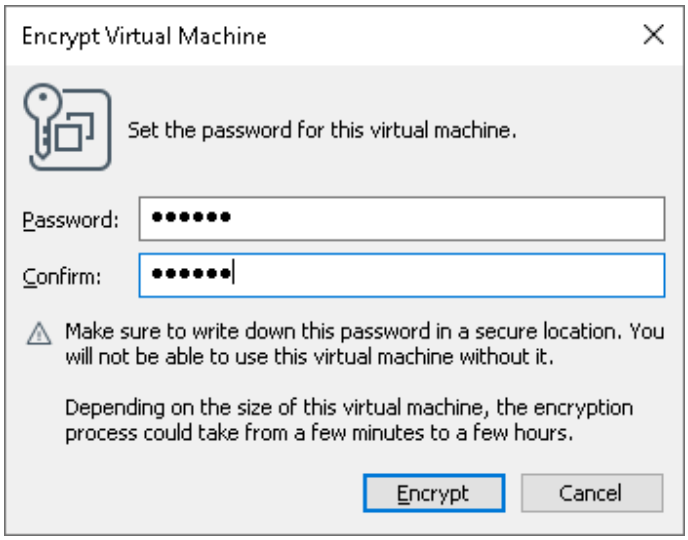
Поиск и расшифровка таких виртуальных машин – одна из важных задач эксперта-криминалиста. Elcomsoft System Recovery позволяет ускорить процесс путём автоматического поиска зашифрованных виртуальных машин. При их обнаружении продукт сохраняет метаданные шифрования, необходимые для восстановления пароля посредством Elcomsoft Distributed Password Recovery.

19.1. Восстановление паролей к виртуальным машинам

VMware, Parallels и VirtualBox – самые распространённые виртуальные машины из числа тех, которые поддерживают шифрование. Несмотря на то, что каждый из трёх производителей говорит о шифровании алгоритмом AES, фактическая стойкость защиты этих виртуальных машин различается даже не в разы, а на порядки.

19.1.1. Parallels

Наименее стойкая защита – у виртуальных машин Parallels.



Для преобразования пароля в ключ шифрования используется всего две итерации хеширования с использованием хеш-функции MD5. Несмотря на использование алгоритма AES-128 CBC для шифрования образа, фактическая стойкость защиты невелика: даже использование единственного процессора Intel i7 позволяет пользователям Elcomsoft Distributed Password Recovery достичь скорости перебора порядка 19 миллионов паролей/сек. В такой ситуации в кратчайшие сроки могут быть восстановлены даже относительно сложные пароли.

19.1.2. VMWare

Следующая по стойкости защиты виртуальная машина – VMware. Её разработчики постарались замедлить скорость атаки на пароль, использовав 10000 итераций более стойкой функции PBKDF-SHA1. При том, что для шифрования данных используется тот же алгоритм AES-128, что и в Parallels, скорость восстановления пароля резко снижается: использование единственного процессора не позволяет превысить порог в 10 000 паролей в секунду. Для ускорения атаки в Elcomsoft Distributed Password Recovery реализован алгоритм, использующий установленные в компьютер видеокарты AMD и NVIDIA для ускорения перебора. Итоговый

результат — порядка 1,6 миллиона паролей в секунду с использованием видеокарты NVIDIA GeForce 2 070 RTX.

19.1.3. VirtualBox

Самая стойкая защита реализована в Oracle VirtualBox. В реализации от Oracle может использоваться шифрование AES-XTS128-PLAIN64 или AES-XTS256-PLAIN64, а в качестве алгоритма хеширования выбран SHA-256. Использование шифрования с переменной длиной ключа и числом итераций, достигающим 1,2 миллиона, ограничивает скорость атаки силами центрального процессора всего 16 паролями в секунду. Исправляет ситуацию функция аппаратного ускорения, позволяющая пользователям Elcomsoft Distributed Password Recovery добиться существенно более высоких скоростей — до 2 700 паролей в секунду на NVIDIA GeForce 2070 RTX. Рекомендуем использовать атаки по словарю, мутации и гибридные атаки.

19.1.4. Методология и настройка атаки

Для восстановления оригинального пароля шифрования виртуальной машины воспользуемся программой Elcomsoft Distributed Password Recovery.

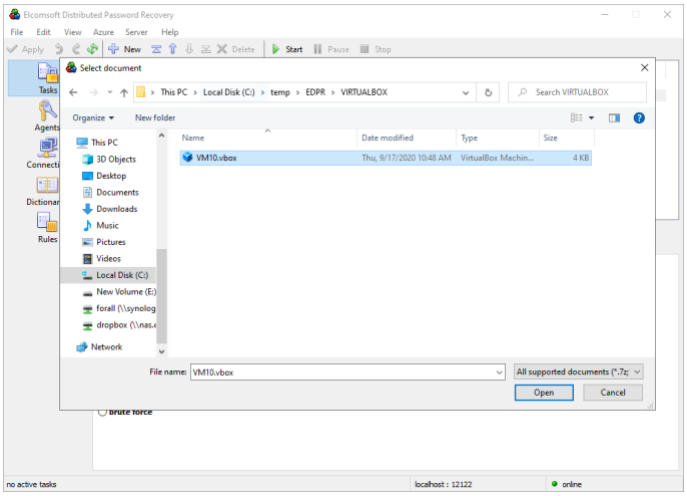
Подготовка к работе.

Обратите внимание: для настройки атаки нет необходимости открывать в EDPR весь образ виртуальной машины целиком. Вместо этого используется небольшой файл, в котором содержатся метаданные шифрования, который можно скопировать из папки с файлами виртуальной машины. Для Parallels используйте файл config.pvs. Для VirtualBox – файл с расширением.vbox. Для VMware – файл с расширением «.vmx». Объем этих файлов не превышает нескольких килобайт; в них содержится всё необходимое для запуска атаки.

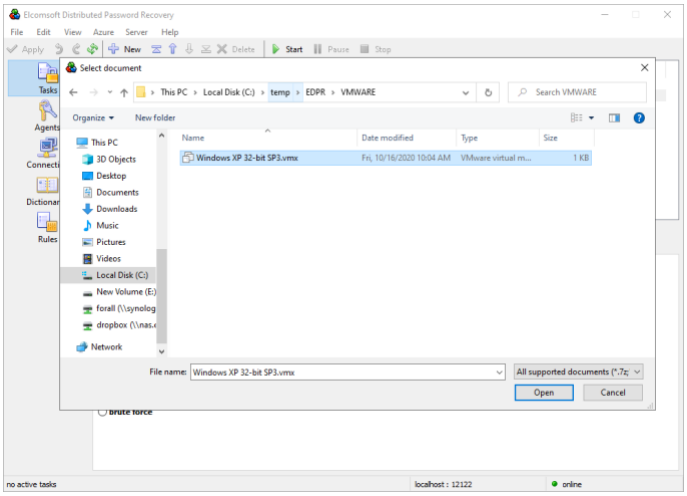
Далее запустите Elcomsoft Distributed Password Recovery (потребуется версия 4.30 или более новая).

В EDPR откройте файл с метаданными шифрования. Для каждого типа виртуальных машин используйте соответствующий файл.

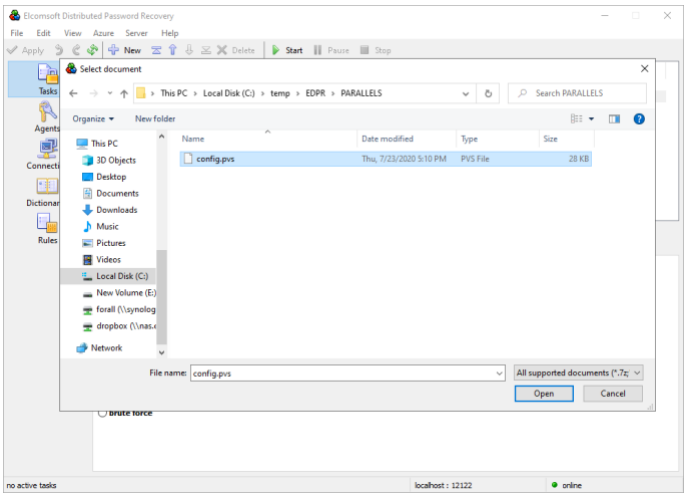
К примеру, при настройке атаки на виртуальную машину Virtualbox откройте файл с расширением «.vbox»:



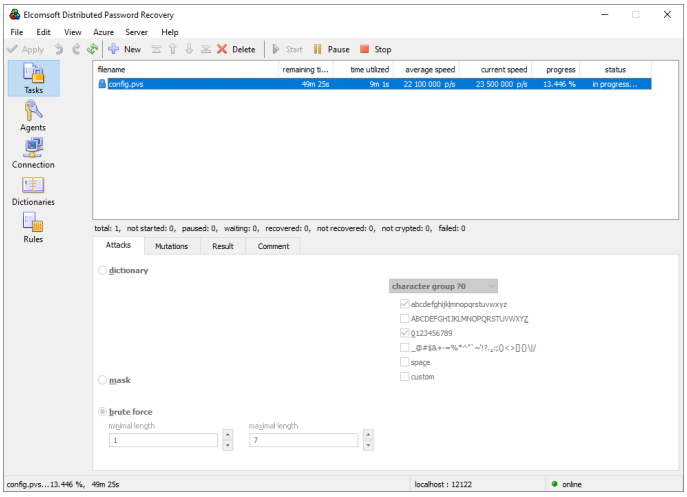
Для VMware откройте файл «.vmx»:



Для Parallels откройте файл config.pvs из папки виртуальной машины.



Далее настройте атаку с использованием словарей, мутаций либо правил гибридной атаки. После запуска атаки будет отображена её скорость. Перебор паролей к виртуальным машинам Parallels работает быстрее всего:



20. Архивы: ZIP, RAR и многие другие

В составе набора доступны два продукта, которые могут быть использованы для восстановления паролей к архивам. Между ними есть существенные различия.

– **Elcomsoft Distributed Password Recovery**: восстановление оригинального пароля методом перебора. Доступны аппаратное ускорение, «умные» и распределённые атаки. Недоступны варианты быстрой расшифровки, использующие известные уязвимости;

– **Elcomsoft Archive Password Recovery**: этот продукт не стоит применять для атаки на пароль. Сильная сторона продукта – использование известных нам уязвимостей в шифровании, обнаруженных в некоторых версиях WinZip и в классическом шифровании архивов ZIP.

Использование Elcomsoft Distributed Password Recovery для восстановления паролей к архивам мало отличается от атаки других документов за следующим исключением: рекомендуем использовать Elcomsoft Hash Extractor (EHE), чтобы проводить атаки не на весь файл с архивом, который может быть очень большого размера, а на извлечённые инструментом EHE метаданные шифрования.

Уникальность Advanced Archive Password Recovery — в поддержке специализированных атак, использующих известные нам уязвимости в шифровании ZIP, благодаря некоторые архивы удаётся расшифровать без полного перебора всех возможных комбинаций паролей.

20.1. Уязвимости шифрования формата ZIP

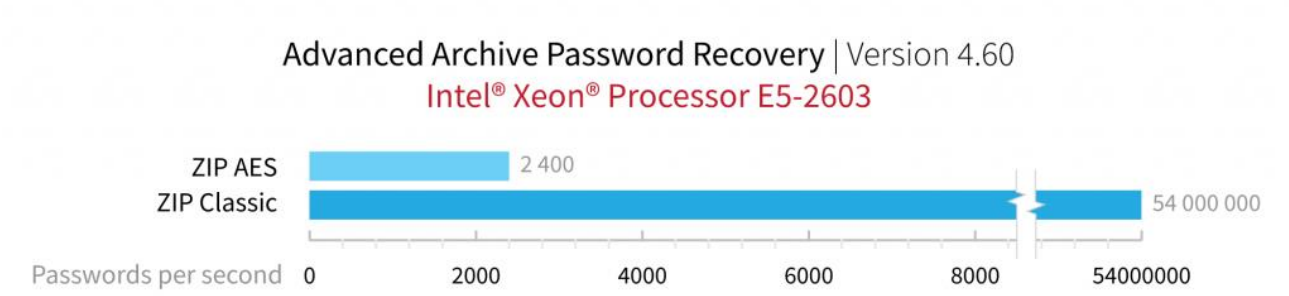
Для архивов в формате ZIP доступно два стандартных способа шифрования: классический метод Zip 2.0 (Legacy) и более современный стандарт AES, для которого, в свою очередь, существуют варианты с ключами длиной 128 и 256 бит. Компания WinZip опубликовала подробный разбор стандартов шифрования, в котором, в частности, не рекомендуется использование устаревшего "классического" способа шифрования:

– *“Legacy (Zip 2.0) encryption: this older encryption technique provides a measure of protection against casual users who do not have the password and are trying to determine the contents of the files. However, the Zip 2.0 encryption format is known to be relatively weak and cannot be expected to provide protection from individuals with access to specialized password recovery tools.”*

– *“You should not rely on Zip 2.0 encryption to provide strong security for your data. If you have important security requirements for your data, you should instead consider using WinZip's AES encryption, described above.”*

Стандарт шифрования AES используется уже несколько десятилетий. Если пользователь решит установить пароль на архив, WinZip использует именно этот способ шифрования по умолчанию. Для чего нужно знать об устаревшем, небезопасном «классическом» стандарте шифрования ZIP? Многие продукты, для которых архивация и шифрование данных не являются основными функциями, для реализации поддержки формата ZIP используют библиотеки с открытым исходным кодом. Среди подобных компонентов попадаются и такие, которые используют исключительно устаревшие методы шифрования — в частности, "классический" вариант шифрования ZIP. На выходе получается архив, зашифрованный по стандарту Zip 2.0 (Legacy). В нашей практике архивы, зашифрованные по "классической" схеме, встречаются практически с той же периодичностью, что и архивы, зашифрованные по стандарту AES.

«Классический» метод шифрования ZIP небезопасен. Использование процессора Xeon E5-2603 без графического ускорителя даёт скорость перебора в 54 миллиона паролей в секунду. Для сравнения, на том же процессоре скорость перебора паролей к архиву, зашифрованному новым стандартом AES, составляет порядка 2400 паролей в секунду, что в 22500 раз медленнее. Для нового метода шифрования доступно ускорение при помощи графических карт (в Elcomsoft Distributed Password Recovery). Ускоритель NVIDIA GTX 1080 демонстрирует скорость перебора паролей ZIP, зашифрованных алгоритмом AES, в 203000 паролей в секунду, что в 85 раз превышает скорость атаки средствами центрального процессора, но даже не приближается к скорости атаки «классического» шифрования.



Исключительно высокая скорость перебора паролей "классического" шифрования ZIP — не единственная проблема этого метода. Известны две уязвимости, позволяющие расшифровать архив ещё быстрее.

20.1.1. ZIP: атака с известным открытым текстом

Атака с известным открытым текстом (known plaintext attack) позволяет расшифровать некоторые типы архивов в формате ZIP без восстановления оригинального пароля. Эта атака доступна только для архивов, защищённых «классическим» шифрованием, и не работает для архивов, зашифрованных AES.

Требование к этой атаке — наличие хотя бы одного незашифрованного файла или его части, совпадающей с содержимым зашифрованного архива. Если у вас есть такой файл, а также ZIP-архиватор, использующий тот же устаревший алгоритм шифрования, вы сможете использовать атаку по известному тексту в Advanced Archive Password Recovery. Для этой атаки нет необходимости в восстановлении исходного пароля: для расшифровки архива он не понадобится. Тем не менее, короткие пароли можно восстановить достаточно быстро.

Инструкции для проведения атаки:

– найдите незашифрованный файл, который также существует в защищённом паролем архиве;

– сожмите его тем же методом и тем же архиватором ZIP, что и зашифрованный архив. Это необходимо, поскольку Advanced Archive Password Recovery проверяет размеры файлов и контрольные суммы файлов. Атаку по открытому тексту можно использовать и для части файла; см. описание ниже.

– запустите Advanced Archive Password Recovery, выберите зашифрованный архив, затем выберите атаку «plain text» и выберите архив, содержащий незашифрованный файл.

После этого Advanced Archive Password Recovery проверит файлы и, если совпадение обнаружено, начнёт атаку.

Программа может найти или не найти оригинальный пароль. В случае, когда оригинальный пароль не может быть найден, вместо него будет выведен ключ, который может быть использован для расшифровки архива.

Атака по части файла.

В некоторых случаях в вашем распоряжении может оказаться в незашифрованном виде другая версия файла, отличная от версии, хранящейся в зашифрованном архиве. Если вы считаете, что начало обычного текстового файла идентично началу зашифрованного, вы можете выполнить так называемую атаку по частичному открытому тексту на основе первых N символов имеющегося в вашем распоряжении файла. Для этого обязательно сохраните единственный файл в защищённом паролем архиве и единственный файл в архиве с открытым текстом. Запустите атаку, и ARCHPR попросит подтвердить «частичную» атаку. Подтвердите выбор и укажите количество байтов для использования в качестве открытого текста. Рекомендуется начинать с 1-3 КБ и уменьшать это число, если ARCHPR не может найти ключи шифрования.

Заметки:

– минимальный размер файла с открытым текстом — 12 байт;

– сохранить атаку можно на втором этапе. После перезапуска атаки первый этап будет выполнен заново;

– длительность первого этапа атаки непредсказуема, но не должна занять дольше нескольких минут.

20.1.2. ZIP: гарантированное восстановление для некоторых версий WinZip

В конце 1990-х и начале 2000-х годов WinZip и другие программы, основанные на исходных кодах Info-ZIP того периода, имели уязвимость в генераторе случайных чисел. Эта уязвимость позволила создать атаку, похожую на атаку с использованием известного открытого текста, но не требующую наличия каких-либо файлов из архива. Единственным ограничением стало количество файлов в архиве: для использования этой атаки в архиве должно не менее 5 файлов. WinZip исправил эту уязвимость в версии 8.1, выпущенной в августе 2001 года.

Данная атака поможет взломать порядка 99,6% поддерживаемых ZIP-архивов, созданных с помощью уязвимой версии WinZip, или 255 из 256 архивов.

Обратите внимание: в архивах ZIP с шифрованием AES этой уязвимости нет, как нет и каких-либо других известных уязвимостей.

20.2. Особенности форматов RAR4, RAR5 и 7Zip

Шифрование в архиваторах RAR и 7Zip не имеет известных уязвимостей. Чтобы расшифровать архив в формате RAR или 7Zip, необходимо подобрать исходный пароль методом полного перебора, словарной или гибридной атаки.

И RAR, и 7Zip используют шифрование AES, различаясь в деталях реализации. Сильнее всего между собой различаются реализации защиты в «старом» и «новом» форматах RAR (соответственно RAR4 и RAR5).

20.2.1. Шифрование в RAR4

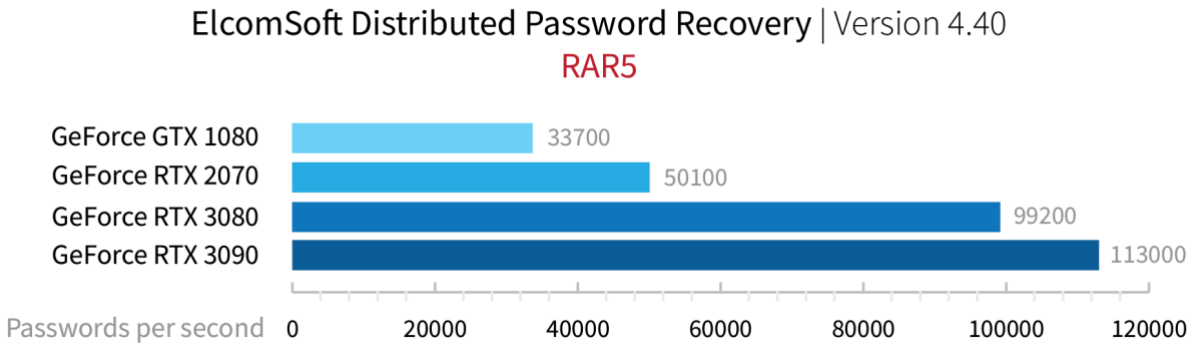
В формате RAR4 архиватор WinRAR использовал шифрование AES с 128-битными или 256-битными ключами. Однако при попытке расшифровать архив архиватор не проверял вводимый пароль, пытаясь расшифровать файлы и проверяя контрольную сумму только в самом конце процесса, когда файл был полностью расшифрован.

Перебор паролей для архивов в этом формате исключительно медленный: для проверки каждого варианта пароля нужно целиком расшифровать хотя бы один файл из архива. Для ускорения перебора в наших утилитах реализована оптимизация: атака производится на самый маленький файл в архиве. Если в архиве хранится единственный крупный файл, подобрать пароль становится практически невозможно.

20.2.2. Шифрование в RAR5

В новом формате RAR5 архиватор сохраняет хэш пароля в составе архива, проверяя каждый пароль перед тем, как приступать к расшифровке файлов. По заявлениям разработчиков, это было сделано с целью ускорить распаковку зашифрованных архивов; разработчики также сообщили, что выбранная ими хэш-функция была достаточно медленной и основана на PBKDF2 для замедления атак. Несмотря на это, скорость восстановления паролей к архивам в новом формате RAR5 намного превышает скорость восстановления паролей к старому формату RAR4.

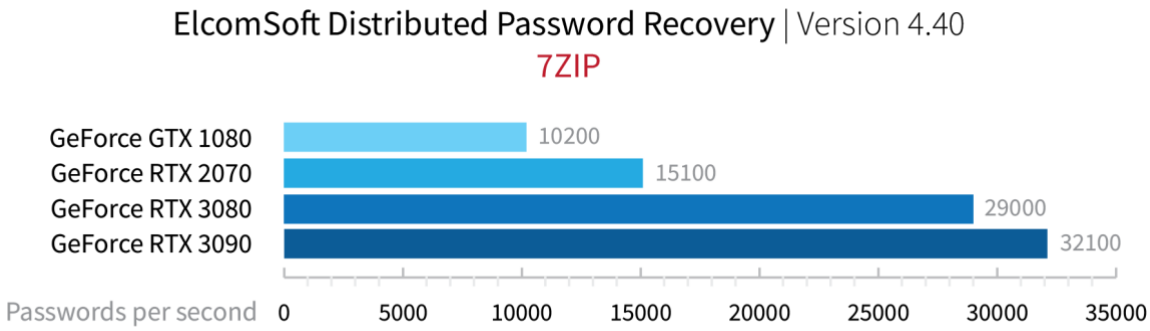
В данном случае невозможно точно сказать, насколько именно повысилась скорость атак на формат RAR5 по сравнению с RAR4. Если скорость атаки на архив в формате RAR5 можно замерить (цифры приводятся на графике ниже), то провести подобные измерения для архивов в формате RAR4 невозможно: скорость атаки различается от одного архива к другому в зависимости от того, какого размера файлы находятся внутри.



20.3. Шифрование 7Zip

7Zip использует алгоритм шифрования AES-256 в режиме CBC. Ключ шифрования получается в результате 524 288 (2^19^) итераций хэш-функции SHA-256. На данный момент в 7Zip не используется криптографическая соль, что представляется серьёзным упущением с точки зрения безопасности (единожды обращённый хэш однозначно идентифицирует архивы, защищённые тем же паролем).

Скорость восстановления паролей к 7Zip ниже средней (а, следовательно, стойкость шифрования таких архивов — выше средней). Если сравнивать форматы RAR5 и 7Zip, то атаки на последний выполняются примерно в 3,5 раза медленнее. При использовании Elcomsoft Distributed Password Recovery с графическим ускорителем получаются следующие цифры:



21. Резервные копии в качестве источника цифровых улик

Резервные копии – основной способ сохранить ценную, уникальную информацию. Резервные копии создаются на современных смартфонах автоматически; на компьютерах Windows за этот процесс отвечают многочисленные встроенные и сторонние приложения, многие из которых используют стойкое шифрование. Исследование резервных копий – важный шаг в процессе расследования, для чего необходимо в первую очередь расшифровать данные.

Резервные копии устройств и приложений могут содержать ценные улики, относящиеся к исследуемому периоду времени. Современные мобильные устройства, являющиеся частью экосистемы Apple или Google, успешно автоматизировали процесс, создавая и поддерживая в актуальном виде резервные копии в соответствующих облачных сервисах. Резервные копии есть и у смартфонов Android, и у Apple iPhone, которые сохраняют резервные копии в облаке iCloud. Наша компания была первой на рынке, предложившей решение в виде продукта Elcomsoft Phone Breaker для извлечения резервных копий из iCloud.

21.1. Мобильные резервные копии

Для смартфонов и планшетов Apple есть и возможность создавать резервные копии локально, на собственном диске. Для этого используется приложение iTunes (в Windows и старых версиях macOS) или Finder (в современных версиях macOS).

Резервные копии iTunes обладают одним интересным свойством: доступность их содержимого различается в зависимости от того, была ли резервная копия защищена паролем. В случае, если пароль на резервную копию не установлен, из незашифрованной резервной копии можно извлечь практически все данные за исключением самых ценных: связки ключей, в которой содержатся сохранённые пароли пользователя.

Если же пользователь установил пароль на локальные резервные копии, то данные будут передаваться из устройства в виде уже зашифрованного потока. За шифрование в этом случае будет отвечать сопроцессор безопасности Secure Enclave, который не позволит незашифрованным данным покинуть устройство. В iOS существует возможность сбросить пароль от резервных копий iTunes, но ранее созданные резервные копии таким образом расшифровать не удастся: они по-прежнему останутся зашифрованными.

Именно зашифрованные паролем резервные копии iTunes представляют наибольший интерес для сотрудников правоохранительных органов и экспертов-криминалистов. В таких резервных копиях пароль используется как для защиты основного контента, так и для шифрования связки ключей. Стоит подобрать к резервной копии пароль, как открывается доступ не только к содержимому самой резервной копии, но и к многочисленным учётным записям

пользователя, пароли к которым хранятся в связке ключей. Расследование всей цепочки учётных записей, в свою очередь, позволяет добраться до огромных массивов данных, которые остались бы недоступными в любом другом случае.

В то же время резервные копии хорошо защищены от лобовых атак. Именно так обстояло дело до выхода десятой версии iOS. При выпуске iOS 10.0 разработчики Apple допустили ошибку, в результате которой нам удалось разработать уникальный способ сверхбыстрого перебора паролей – скорость работы достигала миллионов паролей в секунду на единственном центральном процессоре!

Впрочем, ошибка была оперативно устранена, и в одном из последующих обновлений ОС разработчики Apple увеличили стойкость защиты сразу в миллион раз. Теперь к защищённым паролем резервным копиям iTunes невозможно подойти без мощного графического ускорителя, но даже с ним скорость атаки не превышает нескольких десятков паролей в секунду.

Такая скорость означает одно: прямолинейными атаками методом полного перебора результата в разумные сроки добиться не удастся. Имеет смысл использовать атаки с учётом человеческого фактора: подключать целевые словари, использовать словари из утечек, а на основе известных паролей пользователя настраивать интеллектуальные атаки, поддерживаемые Elcomsoft Distributed Password Recovery.

21.2. Резервные копии компьютеров

Производители экосистем для мобильных устройств давно реализовали поддержку резервных копий в облаке, в случае Apple — продавая дополнительное место в iCloud (Google хранит резервные копии Android бесплатно, не учитывая их объём в облачном пространстве). Для смартфонов и планшетов Apple доступно создание и локальных резервных копий через приложение iTunes (Finder в новых версиях macOS), причём, как мы выяснили, шифрование таких резервных копий является исключительно стойким. А как обстоят дела на компьютерах?

21.2.1. Резервные копии macOS

Для macOS всё предельно просто: существует встроенный сервис резервного копирования Time Machine, который также может использовать шифрование. А вот для Windows подобного встроенного сервиса не существует. Со времён Windows 7 в системе доступна служба Backup and Restore (Windows 7), функционал которой предельно ограничен, а шифрование не поддерживается в принципе (Microsoft рекомендует сохранять резервные копии на диске, зашифрованном BitLocker). Из современных вариантов пользователям предлагается подсистема File History, которая не создаёт полноценных резервных копий на уровне системы. Фактическое отсутствие важнейшего системного компонента привлекло многочисленных сторонних разработчиков: в инструментах резервного копирования для Windows не только нет недостатка, но и выбрать тот единственный, который будет использоваться, нелегко из-за слишком широкого выбора. О некоторых подобных инструментах, о том, как в них защищены данные и о том, как эту защиту взломать, мы поговорим в следующий раз.

Следите за новостями: в январском обновлении ожидается поддержка паролей к нескольким популярным инструментам резервного копирования.

21.3. Резервные копии Windows

Резервные копии Windows нечасто становятся объектом внимания экспертов-криминалистов. В то же время в резервных копиях могут содержаться уникальные данные,

которые могут отсутствовать в актуальной версии системы. Встроенный в Windows механизм резервного копирования примитивен и не обладает возможностью шифрования, однако такая возможность существует в сторонних инструментах для резервного копирования Windows. Рассмотрим защиту резервных копий Acronis, Macrium и Veeam и способы её преодоления.

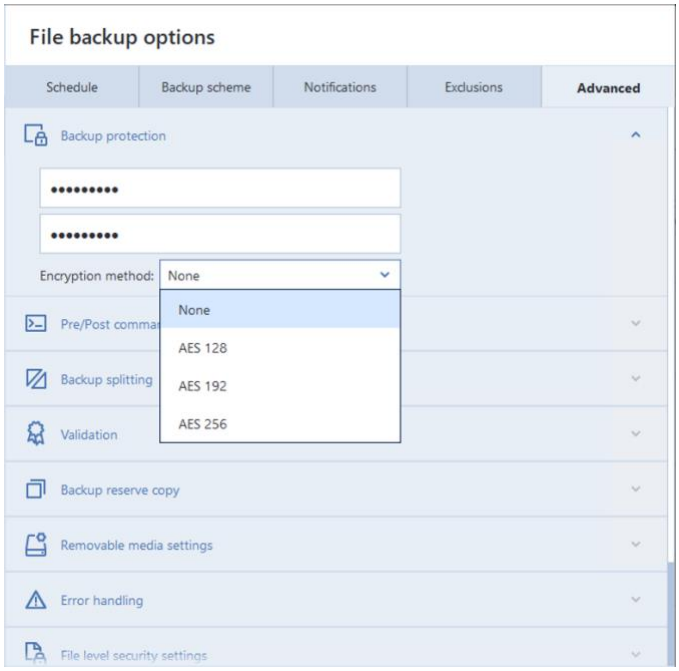
21.3.1. Резервное копирование Windows: сторонние инструменты

Пользователям экосистемы Apple доступна универсальная система резервного копирования. Для компьютеров с macOS в этом качестве выступает Time Machine, своеобразная «машина времени», встроенная в систему. У пользователей Windows подобной встроенной системы нет. Инструмент “Backup and Restore (Windows 7)” устарел на несколько поколений; его функционал ограничен, а шифрование отсутствует как класс (Microsoft предлагает сохранять резервные копии на зашифрованный диск).

Отсутствие адекватной встроенной системы резервного копирования в Windows стимулировало многочисленных сторонних разработчиков; на рынке появились десятки, а потом и сотни утилит резервного копирования. Далеко не все из них получили распространение; некоторые были заброшены разработчиками. Сегодня мы рассмотрим три системы резервного копирования разработки компаний Acronis, Macrium и Veeam, пользующихся заслуженной популярностью.

21.3.2. Acronis True Image и Acronis Cyber Protect Home Office

Продукты Acronis пользуются заслуженной популярностью. Компания сообщает о 5,5 миллионах домашних пользователей и полумиллионе корпоративных. В линейку продуктов Acronis входят такие инструменты резервного копирования, как Acronis True Image 2020, Acronis True Image 2021 и получивший новое имя Acronis Cyber Protect Home Office 2022. Резервные копии Acronis хранятся в файлах «.tib» или «.tibx» в зависимости от версии.



Разработчики Acronis используют для шифрования алгоритм AES, разрешая пользователю выбрать длину ключа: 128, 192 или 256 бит. Смысл такого выбора не вполне понятен. Что должно побудить пользователя выбрать шифрование с менее стойким ключом?

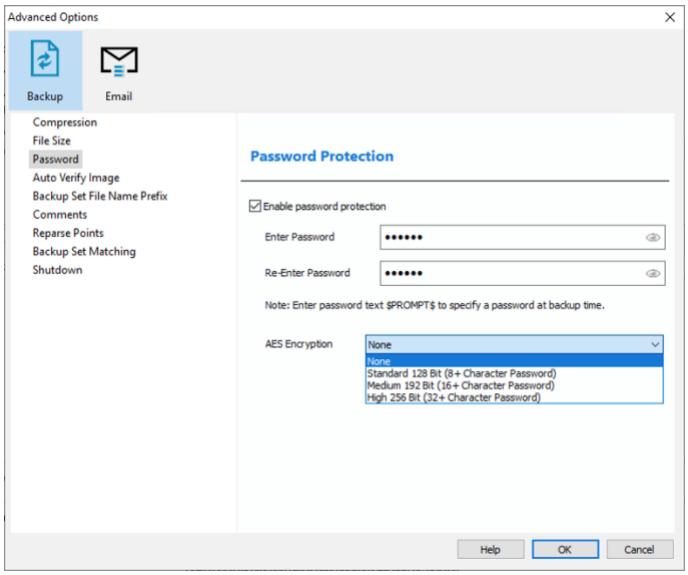
Скорость поточного шифрования (как и скорость атаки на пароль) на современном оборудовании совершенно одинакова независимо от длины ключа.

В более старом формате «.tib» для преобразования пароля в ключ используется устаревший алгоритм MD5; результирующая скорость атаки получается очень высокой, порядка 55,000 в секунду на обычном центральном процессоре без аппаратного ускорения. В более современных форматах используется другая функция преобразования, в результате скорость атаки существенно падает (а защита становится более стойкой).

21.3.3. Macrium Reflect

Macrium не сообщает о количестве пользователей своих продуктов. Инструменты компании нацелены в первую очередь на корпоративных пользователей и специалистов в сфере высоких технологий, среди которых достаточно популярны.

Существует бесплатная версия Macrium Reflect, но шифрование резервных копий доступно только в платной редакции. Разработчики предлагают на выбор варианты шифрования AES-128, AES-192 и AES-256. Этот выбор, однако, реализован достаточно странным образом: пользователи, выбирающие пароль длиной от 8 до 15 символов, могут зашифровать свои данные 128-битным ключом. С выбором пароля длиной от 16 символов становится доступным шифрование 192-битным ключом, а стандартный на сегодняшний день алгоритм AES-256 доступен тем немногим, кто установит пароль длиной от 32 символов.

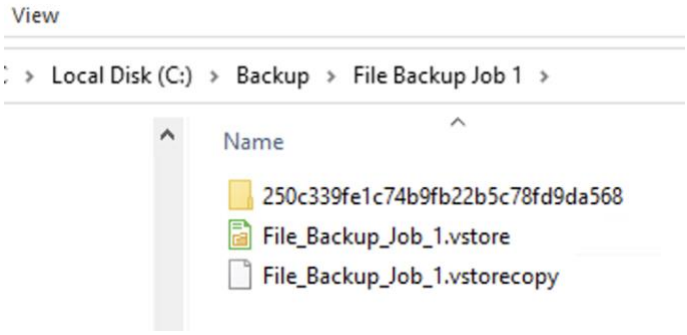


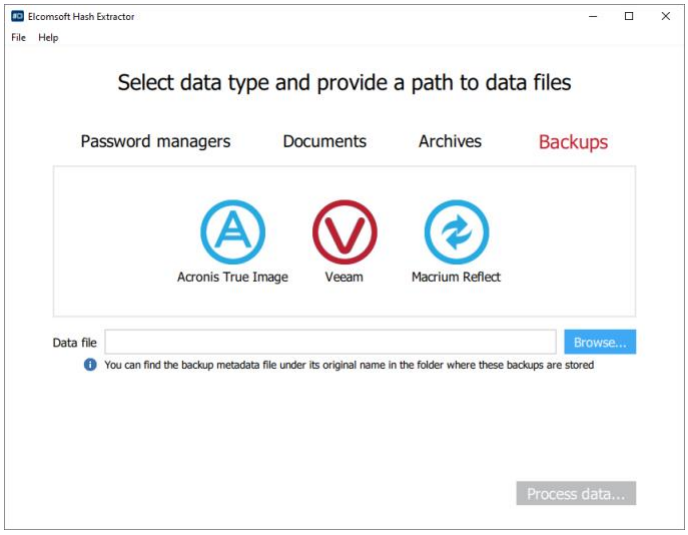
С нашей точки зрения такая система порочна и контрпродуктивна: современный тренд – компенсация короткой длины пароля стойкими, исключительно медленными для взлома алгоритмами шифрования. Использование менее стойкого алгоритма шифрования в комбинации с паролями небольшой длины – не лучший вариант. Впрочем, оказалось, что на практике скорость атаки на пароль от длины ключа не зависит: скорость перебора средствами процессора Intel i7-9700K CPU составляет 457 паролей в секунду, а использование видеокарты позволяет достичь скоростей в 2 500 – 7 100 п/с на протестированном оборудовании; в зависимости от модели могут получиться и более высокие скорости.

21.3.4. Veeam Backup & Replication

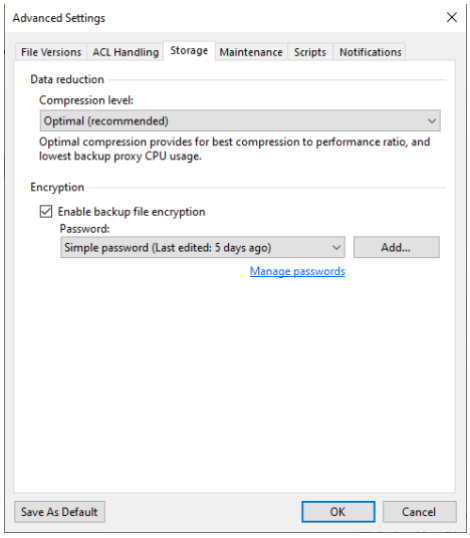
Пользователей Veeam – более 400,000, что делает Veeam Backup & Replication одним из самых распространённых решений для резервного копирования Windows.

В процессе создания резервной копии Veeam Backup & Replication создаёт несколько файлов. Как правило, это файлы.vbm (в них содержатся метаданные резервной копии) и .vbk для полных и .vib для инкрементных резервных копий. Впрочем, фактические расширения файлов могут отличаться в зависимости от ряда условий (виртуальные и физические машины, NAS и т.п.; на скриншоте ниже показан NAS).





Если пользователь установит пароль, Veeam Backup & Replication зашифрует данные алгоритмом AES-256 в режиме CBC.

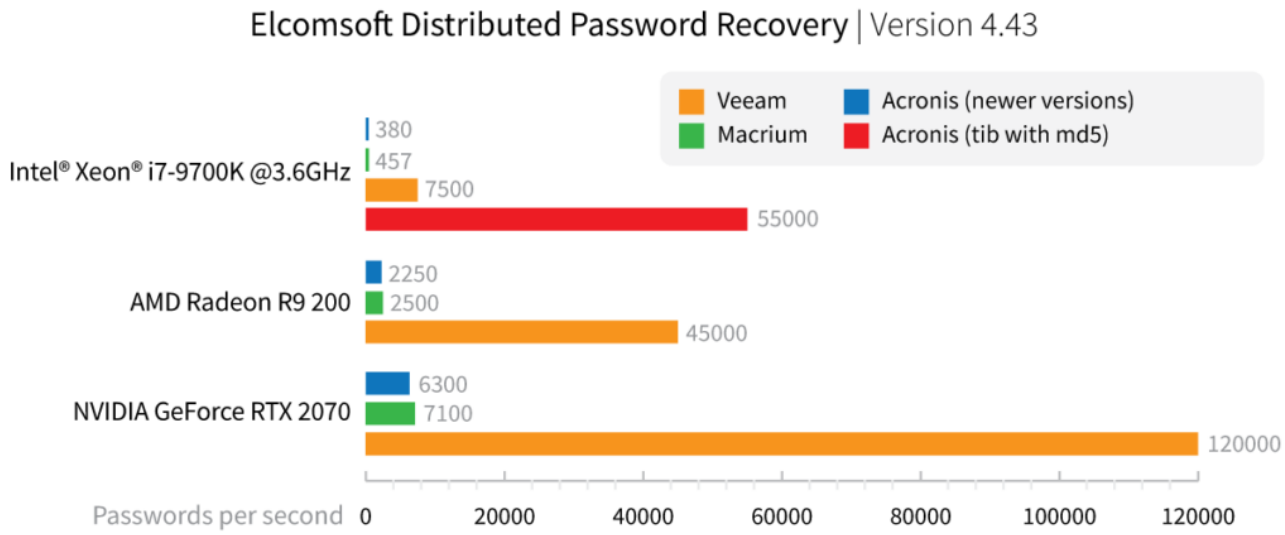


Выбора алгоритма шифрования или длины ключа нет, и в данном случае это к лучшему. В функции преобразования пароля используется хэш SHA1, который считается небезопасным из-за недавно обнаруженных коллизий. Результирующая скорость атаки – высокая: на

процессоре Intel i7-9700K скорость перебора 7 500 паролей в секунду, а использование видеокарты в качестве аппаратного ускорителя поднимает скорость до 45 000 – 120 000 п/с в зависимости от модели.

21.3.5. Замеры скоростей

Ниже приводятся скорости восстановления паролей к описанным форматам на различных аппаратных конфигурациях.



Самым небезопасным является старый формат Acronis «.tib», для которого достижима скорость перебора 55 000 п/с на обычном центральном процессоре. Защита резервных копий Veeam относительно слабая при использовании видеокарт. Macrium Reflect и свежие версии Acronis обладают сравнимой степенью защиты.

21.3.6. Последовательность действий

Привычный сценарий атаки на пароль – загрузить файл или документ в EDPR, после чего настроить и запустить атаку. В этом сценарии есть два недостатка. Во-первых, при передаче на компьютер эксперта существует риск утечки персональной информации. Во-вторых, передача файлов резервных копий объёмом в несколько гигабайт непрактична.

Встроенный в продукт инструмент Elcomsoft Hash Extractor решает обе этих проблемы. Этот инструмент позволяет извлечь метаданные шифрования и сохранить их в отдельном небольшом файле. Использование таких файлов для восстановления пароля к резервной копии позволяет передавать на компьютеры на много порядков меньшие объёмы данных, при этом само содержимое резервной копии не попадает на компьютер, на котором проводится атака.

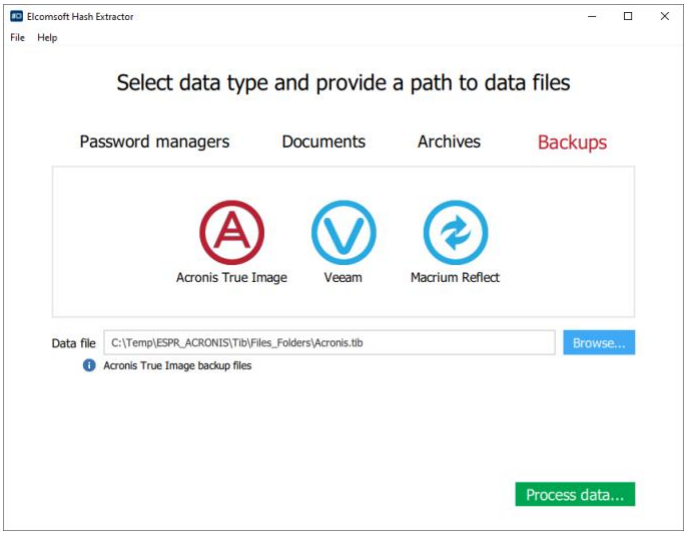
Elcomsoft Hash Extractor доступен в составе Elcomsoft Distributed Password Recovery[74]; он может использоваться и в качестве портативной утилиты, позволяющей извлечь из файлов метаданные шифрования непосредственно из исследуемого компьютера.

[74] https://www.elcomsoft.ru/edpr.html

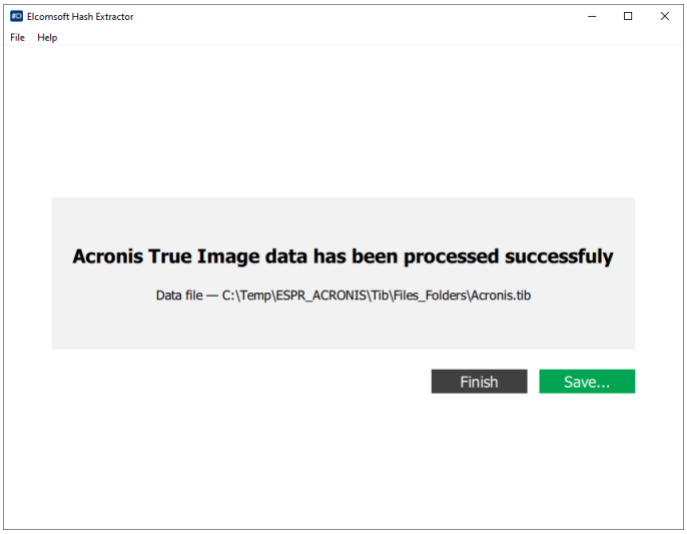
Таким образом, первым шагом для начала атаки на резервные копии Macrium или Veeam станет извлечение метаданных шифрования утилитой Elcomsoft Hash Extractor.

Для извлечения метаданных шифрования:

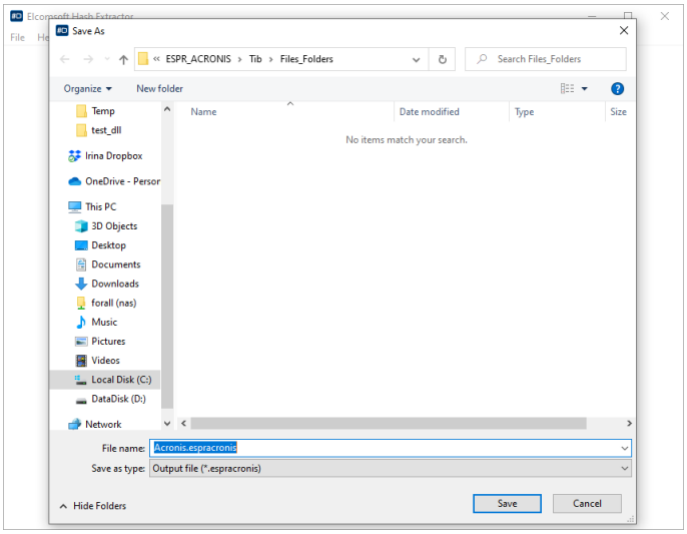
1. Запустите Elcomsoft Hash Extractor.
2. На главном окне выберите иконку “Backups”, после чего откройте файл резервной копии.



3. Нажмите Process data.



4. После завершения процесса сохраните файл с метаданными (кнопка Save).

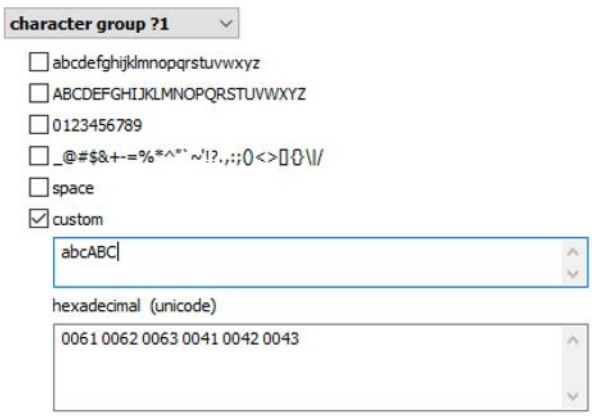


Метаданные шифрования будут сохранены в отдельном файле, который необходимо открыть в Elcomsoft Distributed Password Recovery. Далее настройте и запустите атаку в Elcomsoft Distributed Password Recovery (см. следующий раздел).

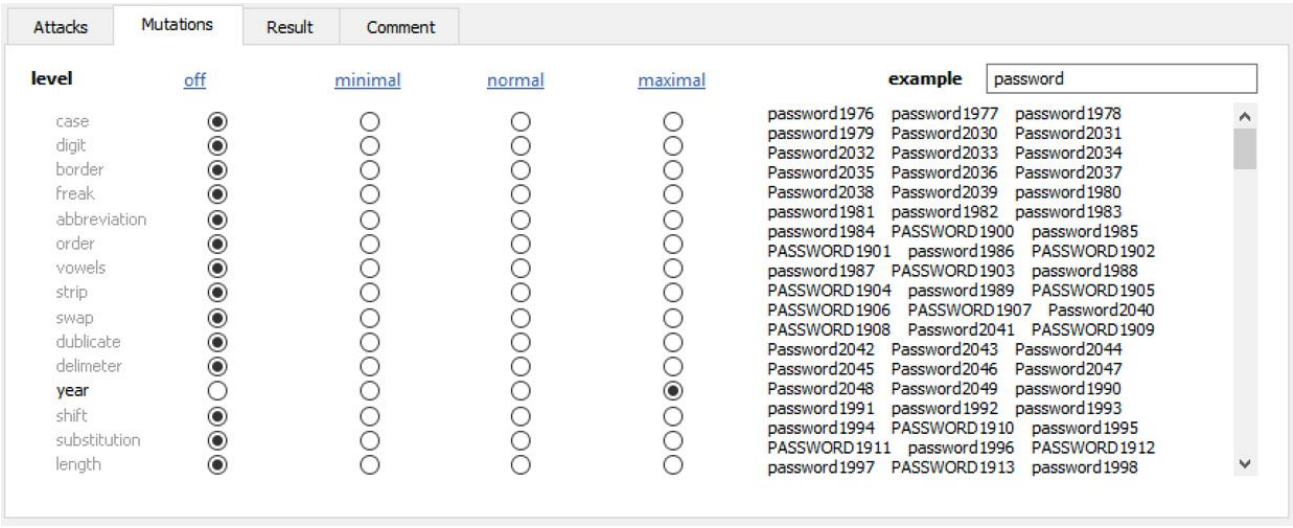
21.3.7. Атака в Elcomsoft Distributed Password Recovery

Как уже упоминалось выше, прямой перебор может оказаться недостаточным даже с использованием мощных графических ускорителей. Для форматов со стойким шифрованием необходимо использовать атаки, нацеленные на человеческий фактор. Таких атак существует множество: здесь и целевые словари, созданные на основе известных паролей пользователя, и словари, составленные из утечек паролей из популярных онлайновых сервисов, и автоматизированные атаки с мутациями и прочие интеллектуальные атаки, поддерживаемые Elcomsoft Distributed Password Recovery.

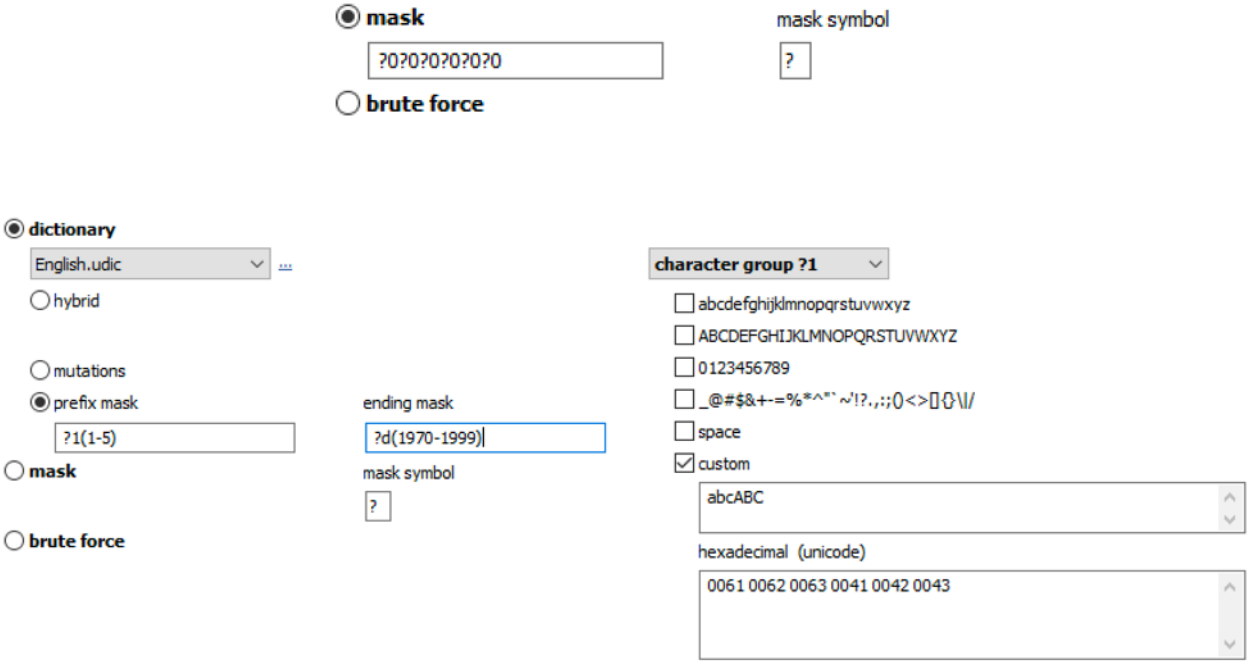
Существующие пароли пользователя, извлечённые из связки ключей или браузера пользователя посредством Elcomsoft Quick Triage — отличная отправная точка. Эти пароли можно извлечь из учётной записи пользователя Google, связки ключей macOS, iOS или iCloud, учётной записи Microsoft или просто извлечь из компьютера пользователя. Существующие пароли пользователя подсказывают, какие группы символов могут быть использованы.



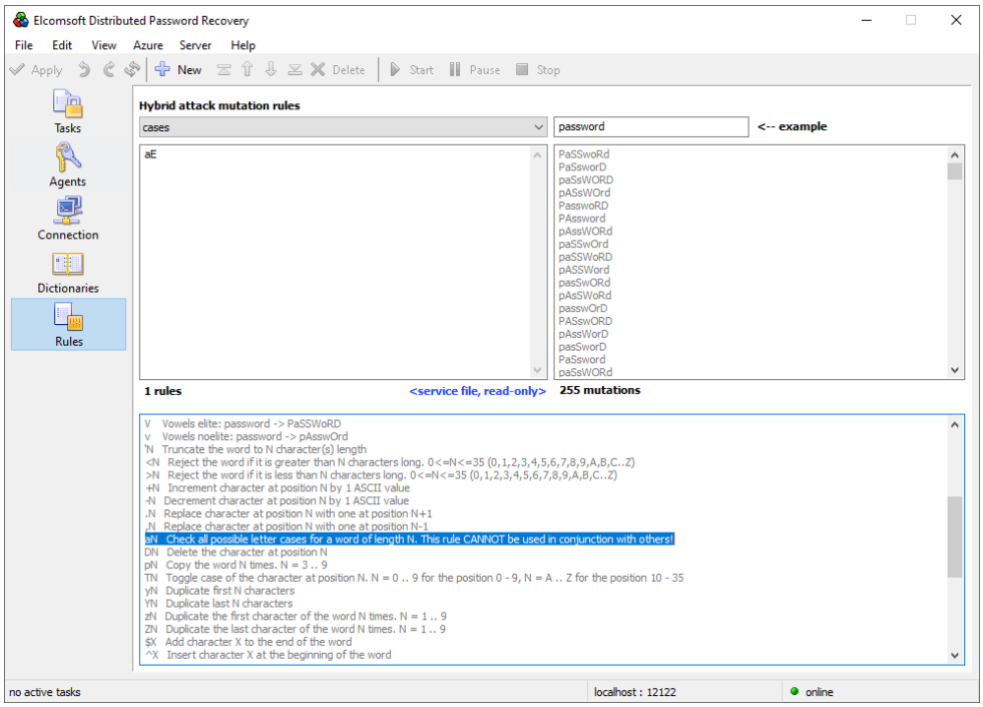
Elcomsoft Distributed Password Recovery поддерживает многочисленные мутации слов из словаря (например, Password1, password1967 или pa$$w0rd):



Если удалось определить шаблон, по которому пользователь составляет свои пароли, то можно использовать маски:



Продвинутые атаки с использованием гибридных правил:



Резервные копии – ценный источник цифровых улик, доступ к которым может быть защищён стойким шифрованием. Для того, чтобы получить доступ к зашифрованным уликам, придётся воспользоваться как аппаратными способами ускорить перебор, так и разнообразными «умными» атаками, которые учитывают человеческий фактор.

22. Документы: Microsoft Office

Первая версия Microsoft Office вышла 1988 году. За прошедшие годы Microsoft Office превратился из простого текстового редактора в мощный пакет приложений и облачных сервисов с более чем 1,2 миллиардами пользователей. Форматы файлов Microsoft Office являются стандартом де-факто в документообороте.

С выходом Word 2.0 в 1991 году в офисных продуктах Microsoft появилось шифрование. Некоторые виды паролей и по сей день можно просто удалить, но расшифровать зашифрованные файлы становится всё сложнее с каждым новым поколением Office. В этом разделе объясняется разница между различными видами паролей в разных версиях продуктов Microsoft.

Тип пароля	Приложение	Шифрование	Скорость атаки
Пароль на открытие	Все кроме Outlook	Да	В зависимости от версии
Защита от записи	Word, Excel, PowerPoint	Нет	Мгновенно
Защита документа	Word	Нет	Мгновенно
Пароль Book	Excel	Нет	Мгновенно
Пароль Shared Book	Excel	Нет	Мгновенно
Пароль на таблицу	Excel	Нет	Мгновенно
Пароль VBA		Нет	В зависимости от версии

22.1. Word 2.0 – 95, Excel 4.0 – 95

В этих версиях Microsoft Office использовался простейший алгоритм XOR. Даже в момент выхода этой версии Microsoft Office этот тип шифрования считался имитацией защиты; расшифровать защищённые документы и тогда, и сейчас можно мгновенно; в длительных атаках нет никакой необходимости. Этот тип защиты продержался вплоть до версии Office 95 включительно.

Итог: мгновенная расшифровка.

22.2. Office 97 и 2000

На момент выхода Office 97 в компании Microsoft уже знали, каким должно быть шифрование. Тем не менее, Office 97 вышел с намеренно ослабленной защитой. Причиной стали экспортные ограничения США. В версии продукта для американского рынка пользователи могли самостоятельно настроить стойкое шифрование, однако этого почти никогда не происходило в силу ограничений совместимости.

С технической точки зрения в Office 97 использовался поточный шифр RC4 и функция хеширования MD5. Для защиты использовался 40-битный ключ и единственная итерация хеш-функции. На момент выхода такая защита считалась слабой; сегодня защищённые таким образом документы можно быстро расшифровать без использования аппаратных ускорителей и распределённых атака.

Более того, для снятия защиты и расшифровки документов не нужен и перебор. Мы разработали алгоритм, использующий патентованные таблицы Elcomsoft Thunder Tables ™, позволяющий расшифровать любые документы Word 97 и порядка 97% таблиц Excel 97 за считанные секунды.

Для расшифровки документов не требуется восстановление оригинального пароля: достаточно ключа, восстановленного при помощи указанных таблиц. Если же оригинальный пароль необходимо восстановить, то это можно сделать методом полного перебора. Использование современных графических ускорителей позволяет добиться скоростей перебора в десятки миллионов паролей в секунду.

Шифрование в Microsoft Office 2000 идентично тому, которое использовалось в версии трёхлетней давности.

Итог: мгновенная расшифровка таблицами Thunder Tables либо исключительно быстрый перебор для восстановления оригинального пароля.

22.3. Office XP и 2003 с шифрованием по умолчанию

К 2000 году ограничения экспортного контроля были практически полностью сняты, однако Microsoft продолжала использовать слабое шифрование ещё несколько лет в двух поколениях офисных продуктов: Office XP и 2003. В этих версиях Microsoft Office по умолчанию используются алгоритмы шифрования и хеширования из Office 97. В результате большинство документов Office XP и 2003 можно расшифровать практически мгновенно с помощью Elcomsoft Advanced Office Recovery[75] и таблиц Thunder Tables.

[75] https://www.elcomsoft.ru/aopr.html

С выходом Office XP Microsoft позволяет использовать внешние криптографические провайдеры. Если используется внешний криптографический провайдер (что встречается достаточно редко), то вместо восстановления 40-битного ключа шифрования необходим перебор пароля. В то же время важно отметить, что выбор внешнего криптографического провайдера влияет на длину ключа шифрования, но никак не влияет на алгоритм хеширования пароля — что означает, что скорость перебора паролей остаётся прежней. Независимо от выбранного провайдера криптографии скорость парольной атаки будет фиксированной и не будет зависеть от выбранной длины ключа шифрования. Время, необходимое для взлома пароля, зависит исключительно от длины и сложности самого пароля, но не от выбора провайдера криптографии. В результате простые пароли можно восстановить почти мгновенно, в то время как атака на 7-значный буквенно-цифровой пароль может занять около полутора дней.

Использование внешних криптографических провайдеров не исправило ситуацию с шифрованием: защита в Office XP и Office 2003 как была, так и осталась очень слабой. Средний процессор Intel Core i7 потребительского уровня обеспечивает скорость перебора порядка 3 миллионов паролей в секунду. Графический ускоритель ускорит перебор в 250-500 раз в зависимости от оборудования; в современных условиях такая скорость перебора указывает на исключительно слабую защиту.

Итог: документы, сохранённые в режиме шифрования по умолчанию, расшифровываются мгновенно с использованием таблиц Thunder Tables. Атака на оригинальный пароль исключительно быстрая и не зависит от выбора провайдера криптографии.

22.4. Office 2007: появление стойкого шифрования

Спустя семь лет после снятия ограничений на экспорт стойкой криптографии в Microsoft отказались от использования 40-битного шифрования. Однако новая схема шифрования стала не единственным нововведением в Office 2007.

Начиная с поколения 2007 года, в обновлённых версиях Word и Excel (а также многих других приложений Microsoft Office) радикально изменился формат файлов. Для Microsoft Word расширение файла было изменено с DOC на DOCX, а таблицы Excel теперь сохраняются как файлы XLSX вместо XLS. Новые форматы стали не просто расширенными версиями исходных форматов файлов на основе OLE, родом из 1990-х годов. Дополнительный символ «X» обозначает стандарт Office Open XML (не путать с форматом файлов XML OpenOffice.org). С точки зрения восстановления паролей имеет значение то, что в новых форматах файлов применена совершенно новая система шифрования.

Вместо 40-битного RC4 и единственной итерации хеширования MD5 Microsoft использовала промышленный стандарт AES-128 и хеширование посредством 50,000 итераций SHA-1. Использование длинного ключа шифрования делает невозможными атаки на ключ. Теперь для расшифровки документа необходимо восстановить исходный пароль, что, в свою очередь, означает необходимость атаки методом полного перебора (или атаки на основе словаря, мутаций и т.п.)

Даже сегодня документы, зашифрованные с помощью Office 2007 (и не сохранённые в режиме совместимости), являются умеренно безопасными. Типичный процессор Intel Core i7 обеспечивает скорость восстановления около 1 000 паролей в секунду, в то время как атаки с использованием графического процессора обеспечивают скорость перебора порядка 200 000 паролей в секунду (NVIDIA Tesla V100). Для восстановления паролей рекомендуем использовать интеллектуальные словарные атаки.

Итог: новый формат файла и новый метод шифрования. Мгновенная расшифровка документа невозможна. Скорость атаки средняя. Относительно сложные пароли требуют умных словарных атак.

22.5. Office 2010: вдвое безопаснее

В Office 2010 используется та же модель шифрования, что и в предыдущем поколении. Новый Office по-прежнему использует AES-128 для шифрования и SHA-1 для хеширования. Однако количество итераций хеширования было увеличено вдвое: с 50 000 в Office 2007 до 100 000 в Office 2010. Это было сделано для того, чтобы учесть эволюцию аппаратного обеспечения и обеспечить аналогичный уровень безопасности.

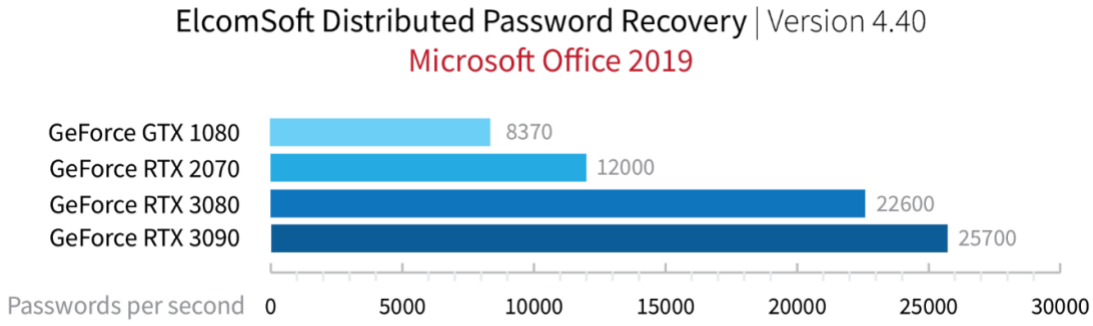
На сегодняшнем оборудовании скорость перебора паролей к файлам, сохранённым в Office 2010, составляет порядка 500 комбинаций в секунду на процессоре Intel Core i7. Использование графического ускорителя позволяет увеличить скорость атаки до 100 000 паролей в секунду (NVIDIA Tesla V100). На данном этапе атаки методом полного перебора становятся невозможными для всех паролей, кроме самых коротких; рекомендуется атака по словарю.

Итог: алгоритмы из Office 2007, но число итераций хеш-функции удвоено; скорость перебора падает вдвое в сравнении с Office 2007.

22.6. Office 2013, 2016, 2019

В последующих поколениях Office Microsoft продолжает увеличивать стойкость шифрования; созданные в новых версиях Office документы совместимы с более ранними версиями в обе стороны.

В Office 2013 были представлены новый метод шифрования (AES-256) и новый алгоритм хеширования (SHA-512). Office 2013, 2016 и 2016 используют шифрование AES-128 или AES-256 и 100 000 итераций SHA-512 для хеширования пароля. Это привело к резкому снижению скорости перебора, которая теперь составляет порядка 50 паролей в секунду на современном процессоре Intel Core i7. Использование графического ускорителя NVIDIA RTX 3 090 увеличивает скорость восстановления примерно до 25 700 паролей в секунду.



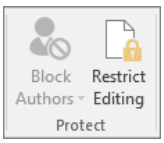
Такая скорость означает, что пароль, состоящий из 7 букв одного регистра, можно восстановить методом полного перебора за 5 дней; пароль из 10 цифр — за 6 дней. Для более сложных паролей «умные» атаки и использование графических ускорителей являются

обязательными условиями. Для взлома длинных и сложных паролей рекомендуются распределённые атаки (Elcomsoft Distributed Password Recovery[76]).

Итог: скорость перебора упала ещё сильнее. Низкая скорость атак. Полный перебор с использованием графического ускорителя позволяет восстанавливать пароли длиной до 3 символов. Более сложные пароли требуют продвинутых словарных атак, в то время как длинные и сложные пароли можно восстановить с использованием распределённых вычислений.

22.7. Моментальное снятие паролей ограничений с документов Microsoft Office

Многие виды паролей в документах Microsoft Office не подразумевают шифрования содержимого документа, являясь своего рода атрибутами, посредством которых приложению (Microsoft Word, Excel и т.п.) сообщается о допустимости или недопустимости тех или иных действий над документом. Так, документ или таблицу можно защитить от редактирования, и соответствующее приложение Microsoft Office откроет его в режиме «только для чтения».



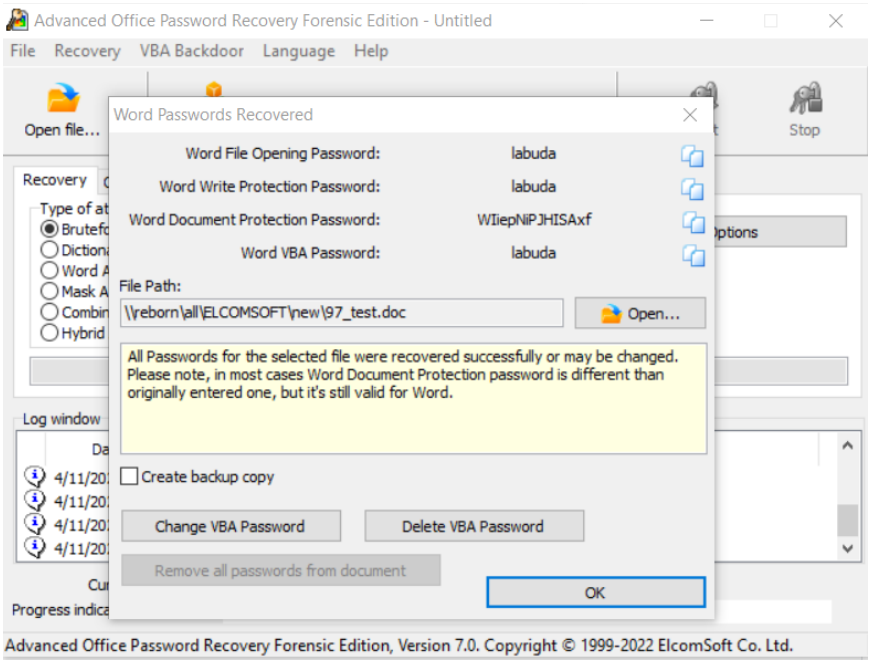
Существуют и другие ограничения – например, ограничения на просмотр и редактирование исходного кода макросов VBA. Отметим, что исходные коды макросов в любом случае не шифруются.

Большую часть ограничений можно снять за считанные секунды, воспользовавшись продуктом Advanced Office Password Recovery. В таблице приводится информация о том, какие именно типы защиты можно снять мгновенно, а какие потребуют восстановления оригинального пароля.

Тип пароля	Приложение	Шифрование	Восстановление или сброс
Пароль на открытие	Все, кроме Outlook	Да	В зависимости от версии
Пароль на защиту от редактирования	Word, Excel, PowerPoint	Нет	Мгновенно
Пароль ограничений	Word	Нет	Мгновенно
Пароль Book Password	Excel	Нет	Мгновенно
Пароль Shared Book Password	Excel	Нет	Мгновенно
Пароль Sheet Password	Excel	Нет	Мгновенно
Пароль VBA	Все	Нет	В зависимости от версии

[76] https://www.elcomsoft.com/edpr.html

Для снятия ограничений и/или восстановления оригинального пароля достаточно открыть документ в Advanced Office Password Recovery. Программа автоматически определит установленные ограничения, отобразит найденные пароли и сообщит о возможности снятия ограничений.



22.8. Гарантированное снятие защиты с документов Microsoft Office: 40-битное шифрование

Вместо восстановления исходного пароля *при помощи таблиц Thunder Tables* атакуется 40-битный ключ шифрования, что позволяет гарантированно расшифровывать документы Microsoft Word 97/2000 и порядка 97% таблиц Excel.

Информация в этом разделе относится к документам Microsoft Office, сохранённым в режиме совместимости. К таким документам относятся файлы с расширениями .doc (Microsoft Word) и .xls (Microsoft Excel). Для файлов, в которых используется 40-битное шифрование, технология Thunder Tables позволяет произвести гарантированное восстановление доступа за считанные секунды. Для восстановления доступа к зашифрованным данным используйте Advanced Office Password Recovery.

Обратите внимание: если файл имеет расширение «.docx» или «.xlsx» (с окончанием на букву «x»), то он был сохранён в современном формате и использует другой тип защиты, для снятия которого необходимо восстановить оригинальный пароль посредством атаки в Elcomsoft Distributed Password Recovery.

22.8.1. Форматы «.doc» и «.xls» используют слабое шифрование

Файлы, сохранённые в режиме совместимости с Microsoft Word и Microsoft Excel версий 97 и 2000, имеют расширения «.doc» (для документов Word) и «.xls» (для таблиц Excel) соответственно. Несмотря на десятилетия, прошедшие со момента перехода Microsoft на современные форматы, использующие расширения «.docx»/«.xlsx», многие организации до сих пор ведут документооборот именно в этом формате.

В рассматриваемых форматах файлов Microsoft до сих пор использует слабое шифрование с ключом длиной в 40 бит, причём даже четверть века назад такой шифр не считался безопасным. Причина этого имеет исторические корни.

На момент выхода Office 97 существовали достаточно надёжные алгоритмы шифрования и хеширования. Известно, что в Microsoft могли пользоваться этими инструментами: в офисном пакете, предназначенном для американского рынка, существовала возможность настроить стойкое шифрование. Для остальных стран поставлялась версия Office 97 с ослабленной защитой. Причиной на тот момент стали экспортные ограничения США, которыми объясняется такой выбор защиты. На момент выхода Microsoft Office 2000 экспортные ограничения на стойкую криптографию были практически полностью отменены, но в Microsoft не стали менять отлаженную схему: в Office 2000 по-прежнему используется 40-битное шифрование.

С технической точки зрения в Office 97 использовался поточный шифр RC4 и функция хеширования MD5. Данные были защищены 40-битным ключом и единственной итерацией хеш-функции. Для сравнения, сегодня в шифровании используются ключи длиной 256 бит и сотни тысяч, а иногда – миллионы итераций хеширования. На момент выхода Microsoft Office 2000 такая защита считалась слабой; сегодня же защищённые таким образом документы можно расшифровать, даже не прибегая к аппаратному ускорению.

40-битное шифрование используется в следующих приложениях и форматах файлов:

– Microsoft Office 97и 2000 – только 40-битное шифрование;

– Microsoft Office XP и 2003 – по умолчанию используется 40-битное шифрование, но появилась поддержка дополнительных крипто-провайдеров CSP;

– более новые версии Microsoft Office – при сохранении файлов в «совместимом» формате «Office 97 — 2003» (файлы с расширениями «.doc», «.xls») используется 40-битное шифрование.

Для расшифровки файлов, сохранённых в таких форматах, оригинальный пароль не требуется. В сравнении с современными 256-битными ключами, пространство 40-битных ключей кажется очень ограниченным, и это действительно так: перебрать все возможные 40-битные ключи на современном компьютере можно быстрее, чем пытаться подобрать пароль пользователя, который может быть длинным и сложным. Существует и более быстрый способ, позволяющий расшифровать документ с 40-битным шифрованием за несколько секунд.

В комплект поставки Advanced Office Password Recovery в редакции Forensic (входит в состав набора) включены таблицы Thunder Tables, с помощью которых можно расшифровать любые документы в формате Word 97 и порядка 97% таблиц в формате Excel 97 за считанные секунды. Подробнее о технологии можно прочитать в нашей статье Thunder Tables™ Explained.[77] Таблицы доступны пользователям редакции Forensic. Пользователи «домашней» редакции Home смогут запустить перебор всего пространства 40-битных ключей.

Необходимо отметить ещё один момент, связанный с таблицами Thunder Tables. Ранее таблицы нужно было устанавливать вручную. В актуальных версиях Advanced Office Password Recovery таблицы можно установить непосредственно из программы; нужные данные будут

[77] https://blog.elcomsoft.com/2009/05/thunder-tables/

скачаны автоматически. Более того, актуальная версия Advanced Office Password Recovery автоматически определит формат файла и тип шифрования и предложит использовать таблицы для моментальной расшифровки.

По умолчанию таблицы загружаются в каталог **%APPDATA%\Elcomsoft Password Recovery\Thunder Tables**, который, как правило, находится на системном диске. Если вы не хотите хранить довольно объёмные (несколько гигабайт) таблицы на загрузочном диске, вы можете указать альтернативный путь, отредактировав реестре следующий ключ:

Computer\HKEY_CURRENT_USER\SOFTWARE\Elcomsoft\Advanced Office Password Recovery\TTPath

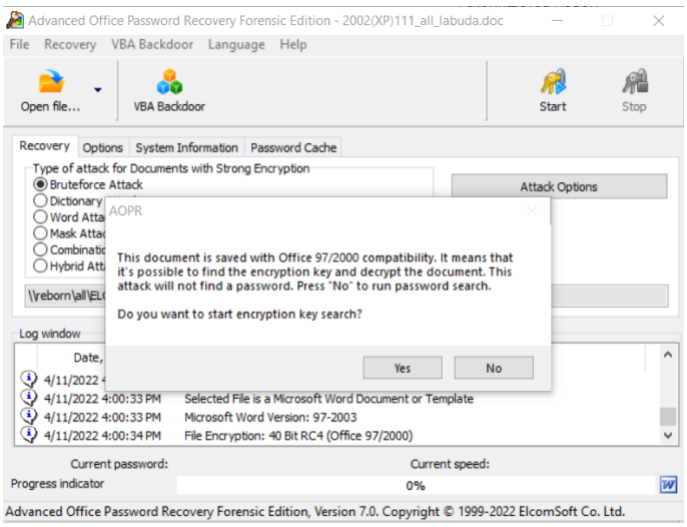
Независимо от того, каким из двух способов восстановления доступа к документу вы воспользуетесь, для его расшифровки не понадобится пароль. Вместо пароля восстанавливается двоичный 40-битный ключ, восстановленный прямым перебором (несколько часов) или при помощи таблиц Thunder Tables (несколько секунд). Если же оригинальный пароль необходимо восстановить, то это можно сделать методом полного перебора. Использование современных графических ускорителей и умышленно слабое хеширование, использованное Microsoft для преобразования текстового пароля в ключ шифрования, позволяет добиться скоростей перебора в десятки миллионов паролей в секунду, восстанавливая достаточно длинные и сложные пароли.

Подведём итог. В новой версии Advanced Office Password Recovery стали доступны функции перебора 40-битных ключей шифрования к документам, сохранённым в «совместимом» с Office 97/2000 формате. Новый функционал позволяет расшифровать совместимые документы за считанные часы, а с использованием таблиц Thunder Tables, доступных пользователям редакции Forensic, — за секунды.

22.8.2. Расшифровка документов DOC/XLS: последовательность шагов

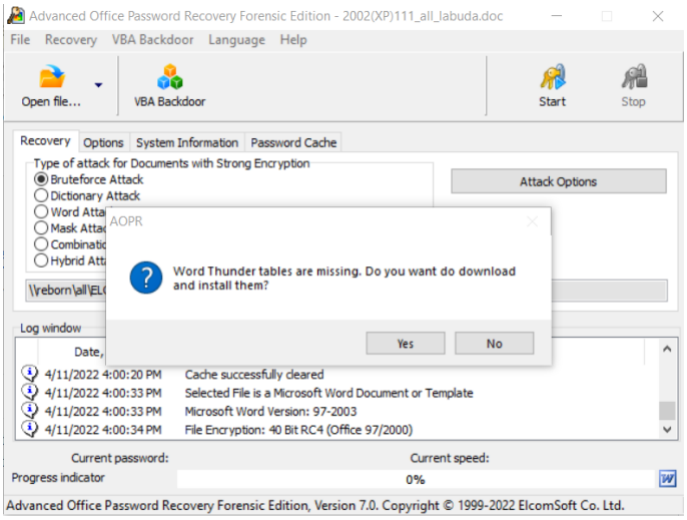
Чтобы снять защиту с документа, защищённого 40-битным шифрованием, проделайте следующие шаги:

1. Запустите Advanced Office Password Recovery.
2. Откройте документ .doc или таблицу «.xls». Программа автоматически определит тип шифрования. Если документ или таблица защищены 40-битным шифрованием, вы увидите следующее сообщение:

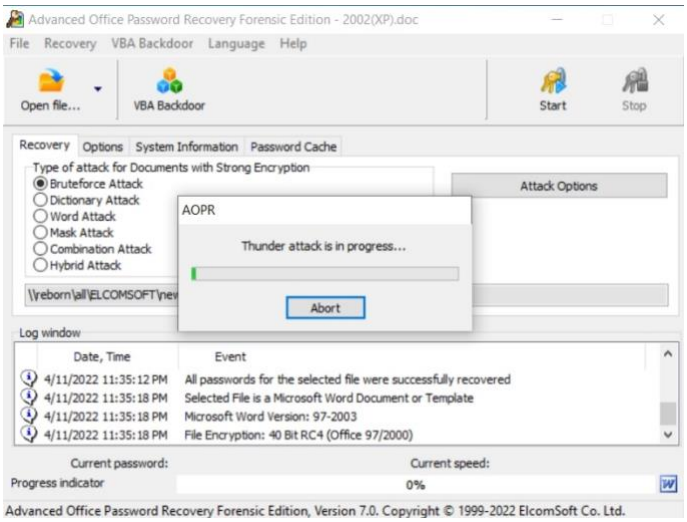


3. Если таблицы Thunder tables на вашем компьютере уже установлены, поиск ключа начнётся автоматически. В противном случае программа предложит скачать таблицы.

4. Обратите внимание: размер таблиц – порядка несколько гигабайт; в зависимости от скорости вашего соединения с интернет их скачивание может занять некоторое время. Кроме того, необходимо убедиться, что на диске C: достаточно свободного места для скачивания таблиц. Если это не так, закройте программу и отредактируйте в реестре Windows Registry ключ, указав желаемый путь к папке, после чего снова запустите программу. *Computer\HKEY_CURRENT_USER\SOFTWARE\Elcomsoft\Advanced Office Password Recovery\TTPath*

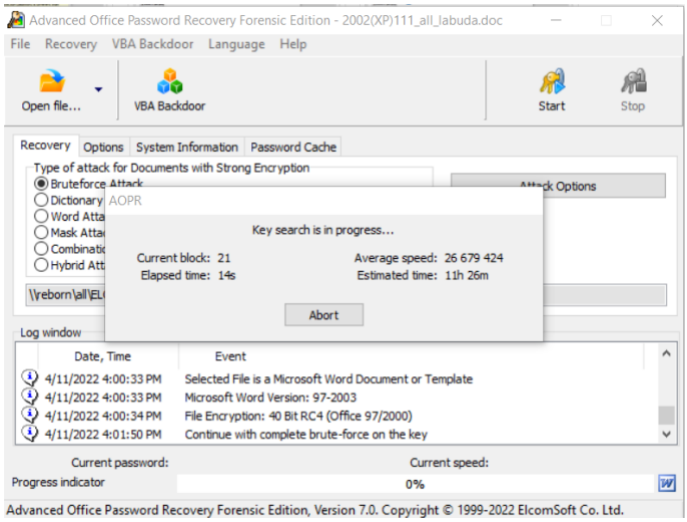


5. После того, как таблицы Thunder tables будут скачаны, поиск ключа начнётся автоматически.



6. С таблицами Thunder tables вероятность нахождения ключа к документам Word «.doc» составляет 100%, а к таблицам Excel «.xls» – 97%. В случае, если ключ к таблице «.xls» не находится при помощи Thunder tables, повторите атаку, использовав метод полного перебора.

7. Атаку методом полного перебора можно запустить как самостоятельно, так и автоматически, если вы откажетесь от скачивания таблиц Thunder tables. Поиск ключа может занять от нескольких минут до нескольких часов в зависимости от скорости центрального процессора вашего компьютера.



8. После того, как ключ будет найден, документ будет расшифрован автоматически. Оригинальный текстовый пароль не восстанавливается и не требуется для расшифровки. Если необходимо восстановить оригинальный пароль, проведите атаку в Elcomsoft Distributed Password Recovery.

22.9. Подводя итоги

Стандарт шифрования, используемый в Microsoft Office 2007 и более поздних версиях, сделал мгновенное восстановление паролей и мгновенную расшифровку данных невозможным (если документ не был сохранен в старом формате в режиме совместимости). Для всех версий Microsoft Office, сохраняющих файлы с расширениями «DOCX» и «XLSX», необходимо восстанавливать пароль вместо ключа шифрования.

Современные версии Microsoft Office хорошо защищены от лобовой атаки, что делает невозможными атаки методом полного перебора. Рекомендуем использовать интеллектуальные словарные атаки, ускорение с помощью графического процессора и распределённых вычислений.

Elcomsoft Distributed Password Recovery поддерживает аппаратное ускорение на большинстве современных видеокарт, позволяя использовать компьютеры, оборудованные до 8 графическими процессорами каждый. Доступен режим распределённых атак с использованием нескольких компьютеров или виртуальных машин.

23. Документы WordPerfect, Lotus SmartSuite

Для расшифровки документов WordPerfect и Lotus SmartSuite больше используется Advanced Office Password Recovery, в который был интегрирован функционал двух ранее независимых продуктов. Расшифровка документов в формате WordPerfect Office и Lotus происходит мгновенно либо занимает нескольких минут независимо от сложности пароля.

В Advanced Office Password Recovery доступны возможности по восстановлению доступа и расшифровке документов, сохранённых в офисных приложениях из наборов WordPerfect Office и Lotus. Ранее в продуктовой линейке нашей компании были представлены отдельные продукты для работы с файлами WordPerfect и Lotus, функционал которых вошёл в состав единого универсального продукта. Advanced Office Password Recovery поддерживает форматы Microsoft

Office всех версий (включая расшифровку документов, сохранённых в «совместимом» режиме), OpenDocument (используется в большом числе офисных пакетов, поддерживающих стандарт), отечественного инструментария «МойОфис«, Apple iWork, корейский пакет Hangul/Hancell Office, а теперь — и WordPerfect Office и Lotus.

Advanced Office Password Recovery используется для расшифровки документов и снятия парольной защиты. В ряде случаев это можно сделать мгновенно. Если для расшифровки документа требуется восстановить оригинальный пароль, продукт предлагает выбор из множества вариантов атак, для ускорения которых используются вычислительные устройства (GPU) бытовых видеокарт. В продукте доступна поддержка форматов IBM/Lotus SmartSuite, Lotus Organizer, Lotus WordPro, Lotus 1-2-3, Lotus Approach и Freelance Graphics, а также линейки продуктов Corel WordPerfect Office, WordPerfect, Paradox и Corel WordPerfect Lightning.

23.1. WordPerfect: проприетарные форматы со слабой защитой

Продукты WordPerfect часто используются для документооборота юридическими конторами за рубежом. Несмотря на сценарий использования, подразумевающий обмен конфиденциальными данными, в собственных форматах WordPerfect разработчик так и не внедрил стойкое шифрование, что позволяет снять защиту и расшифровать документы в течение 10–15 минут, а во многих случаях — и вовсе мгновенно.

В зависимости от того, какой версией продукта был сохранён файл, а также от настроек защиты, возможны разные сценарии восстановления доступа к данным. В ряде случаев парольную защиту можно снять мгновенно, но иногда может потребоваться поиск оригинального пароля, который может занять несколько минут (до 10–15 минут в самых сложных случаях). В других случаях документ можно расшифровать, не прибегая к поиску оригинального пароля.

Единственное ограничение продукта — отсутствие возможности расшифровки файлов QuattroPro после того, как для них будет найден пароль. Расшифровывать файлы в этом формате с найденным в Advanced Office Password Recovery паролем придётся с использованием оригинального приложения QuattroPro.

23.2. Lotus SmartSuite

В своё время набор офисных приложений Lotus SmartSuite был широко распространён, однако в 2009 году его поддержка была прекращена. Тем не менее, файлы в этом формате всё ещё встречаются на компьютерах пользователей — как у частных лиц, так и в организациях. Производитель так и не успел реализовать стойкую защиту для форматов Lotus, что позволяет пользователям Advanced Office Password Recovery снимать защиту с таких файлов в считанные секунды. В Elcomsoft Advanced Office Password Recovery поддерживаются все приложения, компоненты и форматы Lotus SmartSuite, включая Lotus Organizer, Lotus WordPro, Lotus 1-2-3, Lotus Approach и Freelance Graphics.

Обратите внимание: файлы Lotus Notes в Advanced Office Password Recovery не поддерживаются. Несмотря на похожее название, Lotus Notes сильно отличается от Lotus SmartSuite, являясь представителем совершенно другой продуктовой линейки. Продукт HCL Notes, ранее известный под названием Lotus Notes, до сих пор поддерживается производителем и продолжает активно развиваться. В этом формате предусмотрена стойкая защита, снять которую можно лишь перебором паролей, для чего, в свою очередь, потребуется Elcomsoft Distributed Password Recovery.

Таким образом, в Advanced Office Password Recovery доступны возможности восстановления доступа к документам в форматах WordPerfect Office и Lotus SmartSuite. Функционал продукта позволяет расшифровать совместимые документы за считанные минуты, а в ряде случаев — мгновенно. Благодаря поддержке всё новых форматов Elcomsoft Advanced Office Password Recovery становится универсальным инструментом для снятия защиты и расшифровки офисных документов во всех распространённых форматах, как использующихся сегодня, так и популярных в недавнем прошлом.

24. Работа на выезде и анализ активных устройств

Распространение шифрования как на уровне накопителей, так и виртуальных машин может как затруднить анализ данных в лаборатории, так и сделать его невозможным. Зачастую оптимальной стратегией при работе на выезде является анализ «по горячим следам», включающий анализ цифровой техники в активном состоянии с авторизованной пользовательской сессией. Такой анализ позволит получить доступ к зашифрованным данным в момент, когда доступ к ним был разблокирован самим пользователем, а также предпринять необходимые меры для защиты доступа к зашифрованным уликам прежде, чем компьютер подозреваемого будет обесточен.

24.1. Быстрый анализ загруженного компьютера в Elcomsoft Quick Triage

Elcomsoft Quick Triage - новый инструмент в арсенале эксперта-криминалиста, позволяющий быстро извлечь и проанализировать самые важные данные с исследуемого компьютера или образа как на выездных мероприятиях, так и в лаборатории. С использованием Quick Triage можно просмотреть сохранённые пароли и историю посещений активного пользователя системы, исследовать содержимое других учётных записей на компьютере, а также проанализировать данные в образах дисков.

Извлечение данных на лету:

– быстрый сбор и анализ критических данных, системной информации и настроек, учётных записей Windows, настроек и состояния дисков по данным S.M.A.R.T.;

– извлечение критической информации из всех популярных браузеров [1], включая сохранённые логины и пароли, историю поисковых запросов и посещений, список скачанных файлов, закладки, а также информацию о сохранённых платёжных средствах;

– извлечение паролей из почтовых клиентов Microsoft Outlook и Mozilla Thunderbird;

– сбор информации о системной активности пользователя, включая список запущенных приложений и документов, к которым осуществлялся доступ;

– полный список установленных приложений;

– список устройств, которые подключались к портам USB.

Расширенный функционал:

– глобальный поиск по всем категориям извлечённых данных;

– фильтры по датам и времени;

– создание готовых словарей из найденных паролей пользователя;

– экспорт отчетов в формат MS Excel и Adobe PDF.

24.2. Анализ компьютера с авторизованной пользовательской сессией

В процессе анализа компьютера с авторизованной пользовательской сессией имеет смысл проделать следующие операции создать образ (дамп) оперативной памяти, который в дальнейшем используется для поиска ключей шифрования к зашифрованным дискам и крипто-контейнерам.

Для снятия образа оперативной памяти используется инструмент Elcomsoft Forensic Disk Decryptor (EFDD) в виде портативной версии. Соответственно, весь процесс поиска ключей к зашифрованным дискам при условии наличия авторизованной пользовательской сессии (компьютер загружен и разблокирован, есть возможность запуска программ) сводится к следующим шагам:

1. Создание портативной версии EFDD.

2. Запуск портативной версии EFDD на компьютере пользователя (внимание: требуются администраторские привилегии!)

3. Снятие образа оперативной памяти и его сохранение на портативный носитель.

4. Исследование образа оперативной памяти в лаборатории.

Создание портативной версии EFDD.

Опция «Создать портативную версию» (Create portable version) позволяет создать портативную версию программы, которая может запускаться со сменного накопителя (внешнего диска или USB-накопителя). Между обычной и портативной версиями есть следующие различия:

– портативная версия предназначена для запуска на компьютере пользователя с авторизованной пользовательской сессией;

– портативная версия не требует установки; запустите 'efdd.exe' для работы;

– портативная версия не включает возможность создания другой портативной версии;

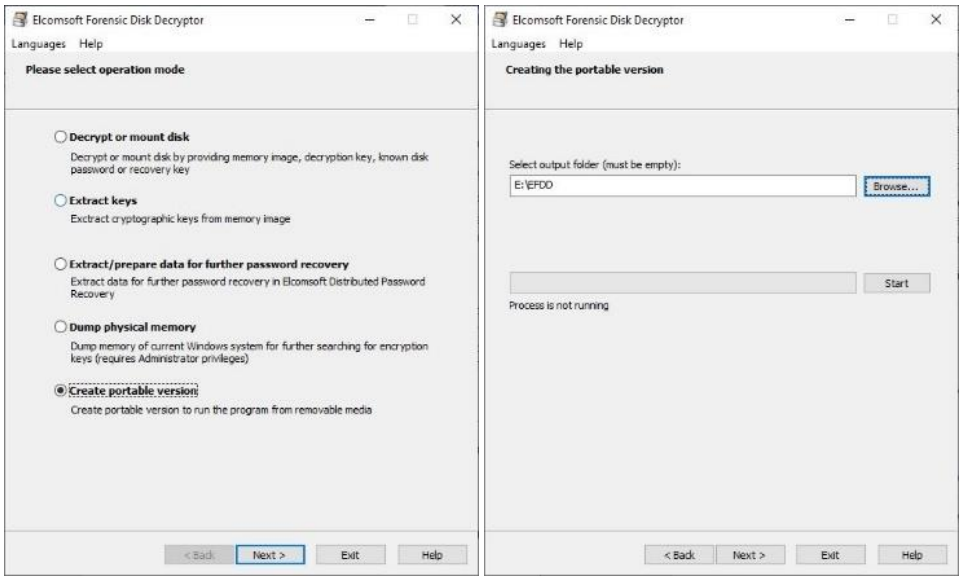
– портативная версия не может монтировать диски (может только расшифровать).

Для создания портативной версии EFDD проделайте следующие шаги:

1. Вставьте USB накопитель и отформатируйте его с файловой системой NTFS. Внимание: категорически не рекомендуется использовать FAT32, т. к. в этой файловой системе нельзя создавать файлы, размер которых превышает 4ГБ (размер файла с образом оперативной памяти объёмом 4ГБ превышает этот размер из-за дополнительной сервисной информации). Допускается использование файловой системы exFAT, если компьютер пользователя поддерживает эту файловую систему (в список совместимых входят системы Windows 10, Windows 8 и 8.1, Windows 7, а также Windows Vista Service Pack 1 или 2). Рекомендуем использовать быстрые накопители достаточного объёма, превышающего ожидаемый объём оперативной памяти компьютера, с которого будет сниматься образ. Например, если компьютер пользователя оборудован 16ГБ оперативной памяти, используйте накопитель объёмом 32ГБ или больше.

2. Запустите EFDD.

3. Создайте портативный накопитель командой Create portable version на главном экране программы. При создании портативного накопителя можно выбрать либо путь к накопителю, либо выходную папку, содержимое которой можно скопировать на внешний накопитель вручную.

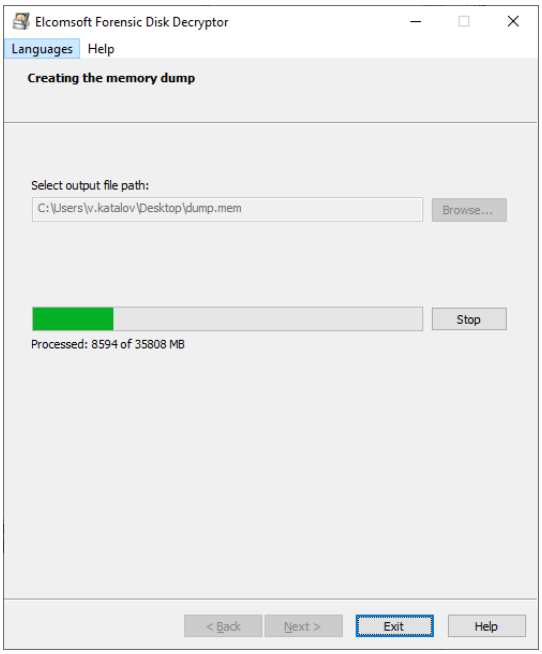


Снятие образа оперативной памяти (запускается на компьютере пользователя)

Если зашифрованный диск разблокирован, ключи шифрования будут храниться в оперативной памяти системы (ОЗУ). Это сделано для того, чтобы механизм шифрования (BitLocker, VeraCrypt и подобные) имел постоянный доступ к ключу шифрования для прозрачного доступа к зашифрованным данным. В системе BitLocker не предусмотрено никаких способов защиты ключа шифрования; в VeraCrypt присутствуют опциональные механизмы, позволяющие затруднить или сделать невозможным поиск ключа шифрования в оперативной памяти. По умолчанию эти механизмы неактивны, а их включение требует вмешательства пользователя.

Использование EFDD позволяет создать образ оперативной памяти компьютера, из которого впоследствии извлекаются ключи шифрования дисков. Для снятия образа оперативной памяти на компьютере пользователя потребуются **права доступа администратора**.

Для того, чтобы создать образ оперативной памяти, воспользуйтесь соответствующим мастером:



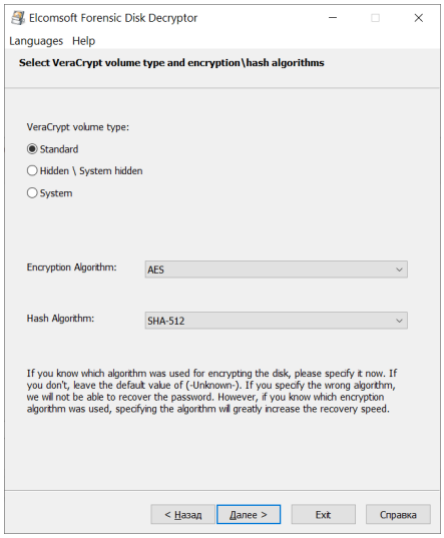
Исследование образа оперативной памяти в лаборатории

Цель лабораторного исследования образа оперативной памяти – доступ к данным зашифрованных дисков и/или контейнеров путём извлечения из образа ключа шифрования. Извлечение ключа шифрования и монтирование (или полная расшифровка) диска с его помощью – самый быстрый и эффективный способ, которым можно воспользоваться.

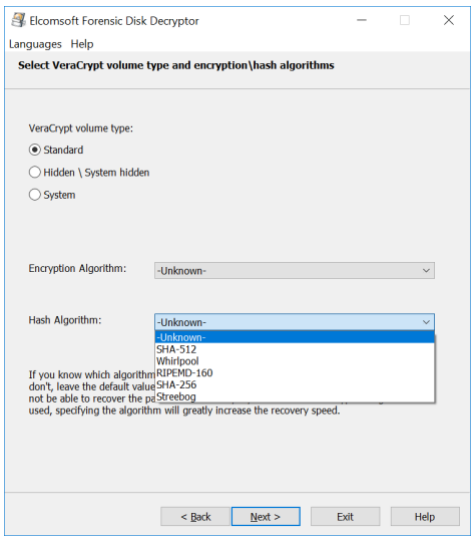
Для обращения к зашифрованным данным программа шифрования диска использует двоичный ключ переменной длины, так называемый Data Encryption Key или Media Encryption Key (MEK). Этот ключ шифрования (MEK) хранится в оперативной памяти компьютера; он же попадает в файлы гибернации и подкачки. Наличие ключа в оперативной памяти требуется для того, чтобы программа-криптоконтейнер могла получить доступ к зашифрованным данным. Обратите внимание: ключ шифрования хранится в оперативной памяти независимо от того, какой алгоритм шифрования пользователь выбрал в настройках контейнера. AES, TwoFish, Serpent, «Кузнечик» или любая комбинация алгоритмов – независимо от выбора пользователя, ключи шифрования будут храниться в оперативной памяти, а сложность и скорость их извлечения практически одинакова.

Для извлечения ключей шифрования посредством Elcomsoft Forensic Disk Decryptor воспользуйтесь следующей инструкцией:

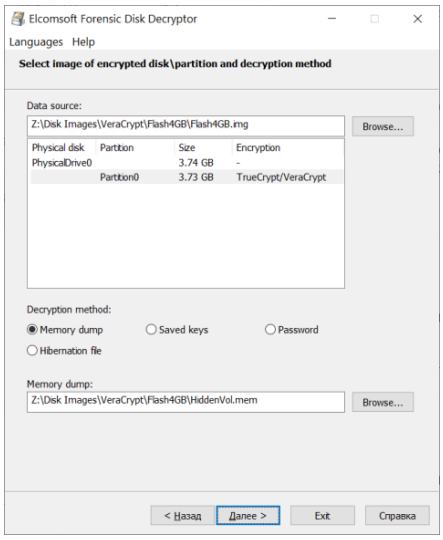
1. Выберите тип контейнера. Если точно известны параметры шифрования и алгоритм преобразования пароля, укажите их для увеличения скорости сканирования. Обратите внимание: при указании неверных параметров ключ шифрования не будет обнаружен; если это произошло, повторите сканирование, указав параметры по умолчанию.



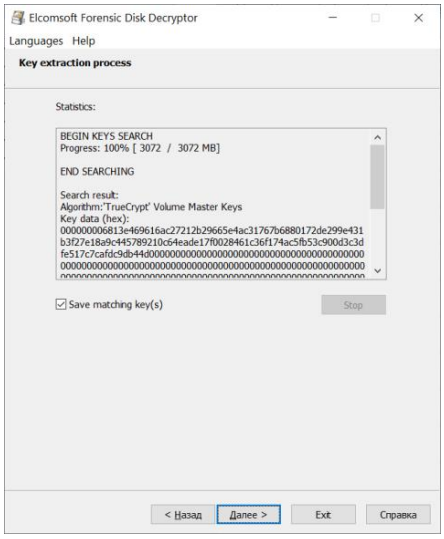
Если параметры неизвестны, оставьте параметры по умолчанию. В этом случае программа будет искать все возможные комбинации.



2. Укажите путь к файлу с образом оперативной памяти и нажмите Next:

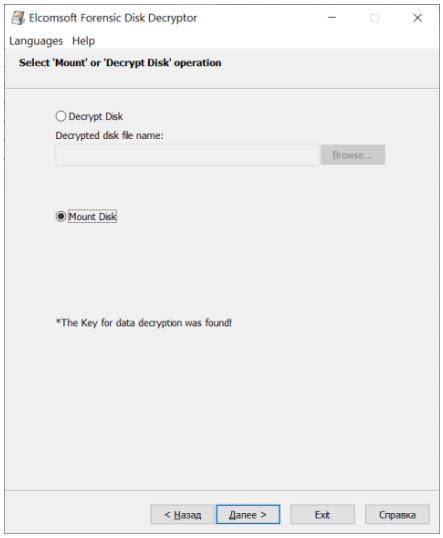


В процессе поиска отображается прогресс.

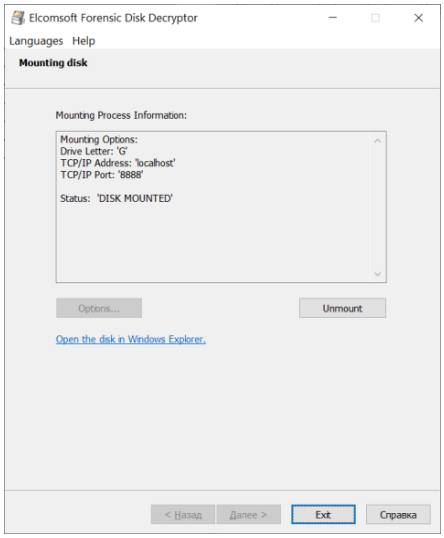


После того, как ключ будет найден, программа предложит расшифровать или смонтировать зашифрованный диск. Монтирование диска осуществляется практически

мгновенно. Расшифровка, помимо временных затрат, потребует наличия накопителя с достаточным количеством свободного места.



После монтирования зашифрованного диска ему автоматически назначается буква.



24.3. Анализ компьютера с использованием внешнего загрузочного накопителя

Исследование заблокированного компьютера отличается от исследования компьютера с авторизованной пользовательской сессией. Традиционно эксперты-криминалисты используют подход с извлечением дисков и исследованием виртуального образа. В то же время этот подход не всегда оптимален с точки зрения времени, затраченного на исследование. С его помощью трудно или невозможно получить доступ к зашифрованным файлам и паролям пользователя. Существует альтернативный способ исследования компьютеров на выезде, который поможет сэкономить время и получить доступ к данным, недоступным при использовании традиционного подхода. Метод подразумевает загрузку оригинального пользовательского компьютера с внешнего накопителя с набором программ для анализа, которым является продукт Elcomsoft System Recovery (ESR).

24.3.1. Условия применимости метода

Метод с загрузкой с внешнего накопителя применим в случаях, когда необходимо исследовать компьютер, питание которого выключено. Для работы необходим свободный порт USB и доступ к BIOS/UEFI компьютера (для загрузки с внешнего накопителя).

24.3.2. Аутентичность исследования и неизменность данных

При работе на выезде определяющим фактором зачастую является время, затраченное на поиск и анализ улик. В то же время важно обеспечить чистоту собранных в процессе анализа данных с правовой точки зрения. При создании образов дисков необходимо обеспечить как неизменность изначальных данных и доказательное соответствие снятого образа оригиналу, так и неизменность самого образа в процессе его хранения и обработки. Начиная с восьмой версии продукта, функционал Elcomsoft System Recovery[78] облегчит достижение этих целей.

24.3.3. Доступ в режиме "только для чтения"

Обеспечение целостности и неизменности данных на исследуемом компьютере — важнейшая часть процесса криминалистического анализа. В ESR 8.0 появился новый режим, позволяющий монтировать накопители исследуемого компьютера в режиме "только для чтения". В этом режиме любые попытки записи на исследуемый компьютер блокируются, гарантируя неизменность исследуемых данных. В этом режиме можно создавать образы дисков (на внешний накопитель), извлекать метаданные шифрования и исследовать файлы и папки. Такие функции, как сброс пароля к учётной записи Windows, в этом режиме недоступны, так как для них требуется возможность записи.

Новый режим включается умолчанию. Для его отключения потребуется вручную отключить соответствующую настройку в момент запуска Elcomsoft System Recovery.

24.3.4. Подписанные образы дисков

Для создаваемых образов диска доступны функции создания контрольных сумм с использованием хэш-функций MD5, SHA1 и SHA-256, а также поддержка формата образов дисков «.E01», который был разработан специально для нужд судебно-криминалистической экспертизы и поддерживается большинством криминалистических программ. Создание подписанных образов позволит экспертам правильно оформлять извлечённые данные, гарантируя целостность и неизменность снятых образов дисков в ходе следственных действий.

Пара контрольных сумм MD5 и SHA1 создаётся автоматически при снятии образа диска для всех поддерживаемых форматов (RAW/DD/.E01); хэш SHA-256 можно включить дополнительно. Обратите внимание: при создании образа в формате RAW/DD контрольная сумма вычисляется автоматически в процессе создания, в то время как данные в образах «.E01» сжимаются; соответственно, для образов в формате .E01 контрольная сумма вычисляется в самом конце и занимает дополнительное время.

[78] https://www.elcomsoft.ru/esr.html

С технической точки зрения контрольные суммы с использование хэш-функций MD5, SHA1 и SHA-256 не являются полноценными цифровыми подписями и требуют соответствующего документального оформления.

24.3.5. Проверка целостности данных

Для проверки контрольной суммы рекомендуем использовать утилиту командной строки certutil в следующем формате:

```
certutil -hashfile FILENAME md5|sha1|sha256
```

При успешном прохождении проверки выводится следующий результат:

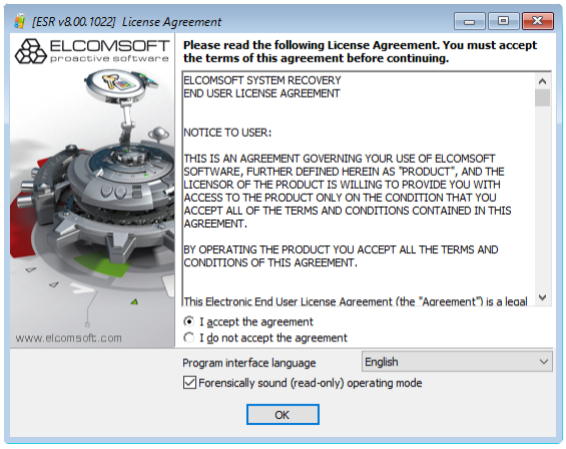
```
MD5 hash of disk.e01: 0d8a7ca3d87bf6c202c26dc363983836

CertUtil: -hashfile command completed successfully
```

24.3.6. Последовательность шагов

Для создания образа дисков с гарантией неизменности данных на исследуемом компьютере проделайте следующую последовательность действий:

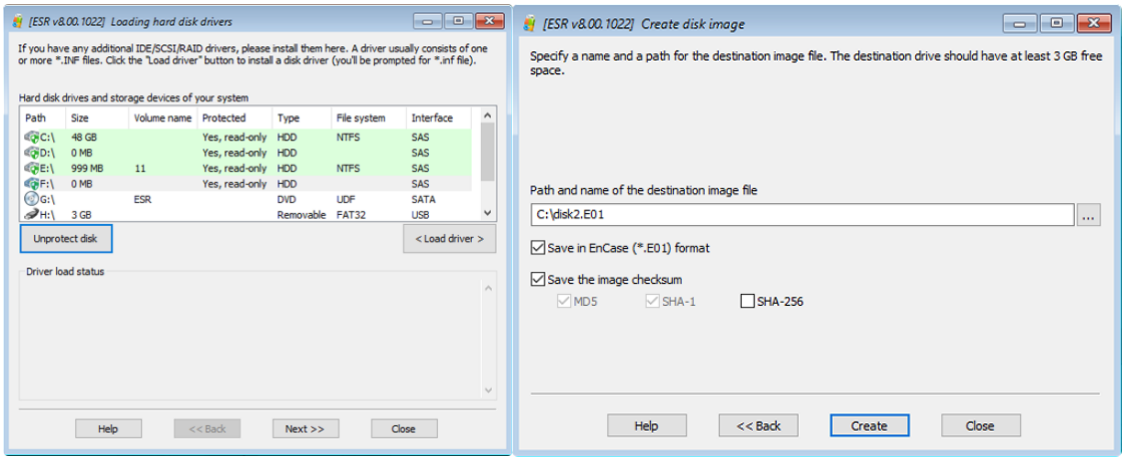
1. Скачайте и запустите Elcomsoft System Recovery 8.0 или более новой версии на вашем компьютере (не на том, который будет исследоваться).
2. Подготовьте загрузочный накопитель. Инструкции — в статье Elcomsoft System Recovery: загрузочный накопитель для исследования компьютеров[79].
3. На исследуемом компьютере измените очерёдность загрузки, разрешив загрузку с USB накопителя.
4. Загрузите исследуемый компьютер с накопителя с установленным Elcomsoft System Recovery.
5. В момент презентации лицензионного соглашения будет доступен выбор режима "только для чтения". Этот пункт отмечен по умолчанию; нажмите Next, чтобы продолжить работу.



6. В режиме "только для чтения" можно снять образы дисков. Рекомендуем сохранять создаваемые диски в специализированном формате .E01, который поддерживает сжатие данных. Проверка целостности данных обеспечивается контрольными суммами.

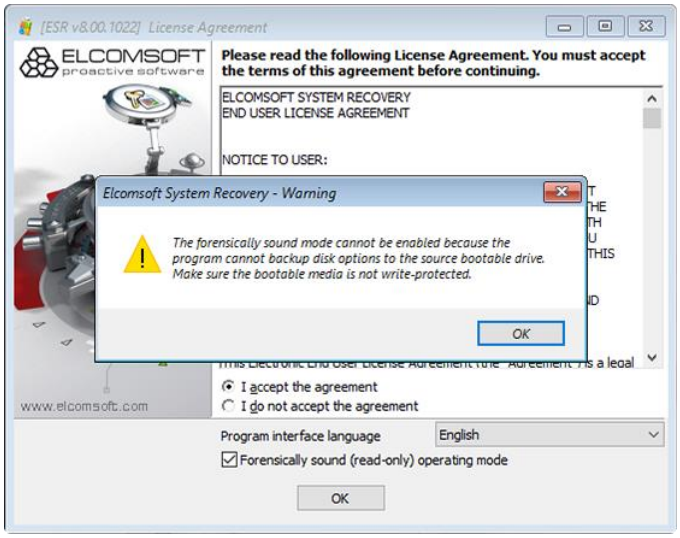
---

[79] https://blog.elcomsoft.ru/2020/11/elcomsoft-system-recovery-zagruzochnyj-nakopitel-dlya-issledovaniya-kompyuterov/



В некоторых случаях Elcomsoft System Recovery не сможет подключить некоторые диски в режиме "только для чтения". Такое возможно при следующих обстоятельствах:

1. Elcomsoft System Recovery загружается с накопителя, доступного только для чтения (например, с CD или DVD диска, USB накопителя или внешнего SSD с блокировкой записи), либо на загрузочном накопителе недостаточно свободного места. Рекомендуем устанавливать Elcomsoft System Recovery на внешний накопитель без защиты от записи и с достаточным объёмом свободного дискового пространства.



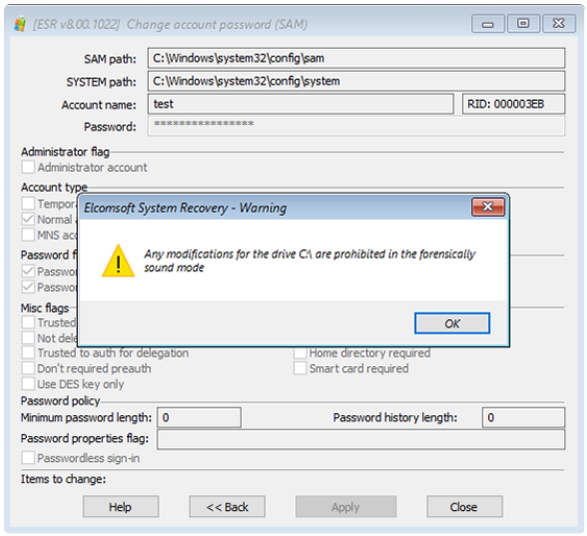
2. Накопитель обозначен буквой "X". В режиме "только для чтения" можно смонтировать все накопители, кроме тех, которые обозначены как "диск X:", что является ограничением подсистемы Windows PE.

В этих случаях произойдёт следующее:

1. Если Elcomsoft System Recovery не сможет смонтировать диски в режиме "только для чтения", программа предупредит об ошибке.

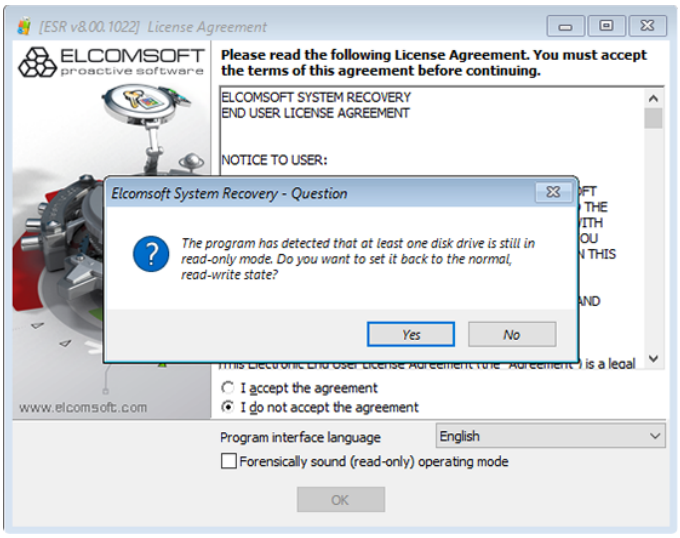
2. Под опцией "только для чтения" появится надпись, поясняющая дальнейшие действия. Вы сможете либо прекратить использование Elcomsoft System Recovery, либо продолжить работу в стандартном режиме (доступ к дискам на чтение-запись).

В режиме "только для чтения" недоступен ряд функций Elcomsoft System Recovery, включая функции сброса паролей к учётным записям Windows. При попытке их использования выводится сообщение об ошибке.



24.3.7. Диски BitLocker

Зашифрованные диски BitLocker будут смонтированы в режиме "только для чтения", если этот режим был активирован изначально. Режим "только для чтения" отключается автоматически при штатном выходе из Elcomsoft System Recovery. В нештатных ситуациях (отключение питания, перезагрузка компьютера) диски остаются смонтированными в режиме "только для чтения", что делает невозможной корректную загрузку компьютера. Для восстановления работоспособности компьютера необходимо смонтировать диски в стандартном режиме, для чего нужно снова загрузить компьютер в Elcomsoft System Recovery, после чего программа выдаст сообщение с предложением смонтировать диски в стандартном режиме.



24.3.8. Инструкции по использованию Elcomsoft System Recovery

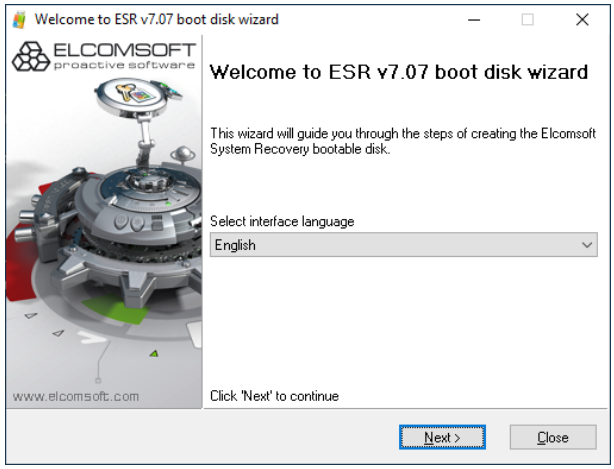
Использование Elcomsoft System Recovery[80] позволяет решать широкий спектр задач. Если системный диск не зашифрован, рекомендуем следующую последовательность действий:

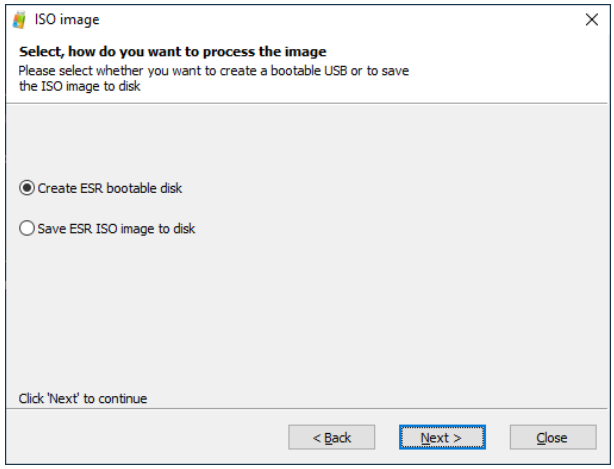
[80] https://www.elcomsoft.com/esr.html

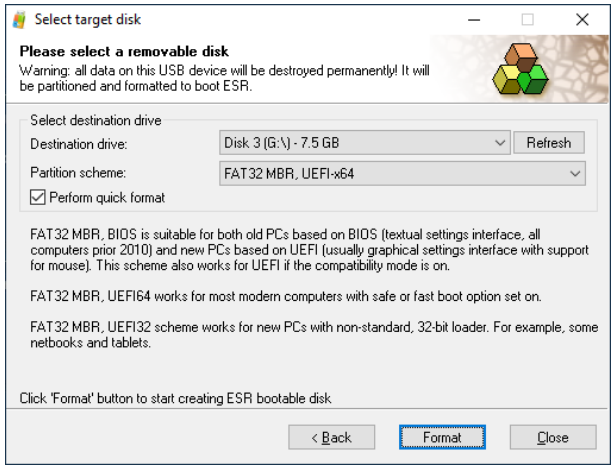
1. Подготовьте загрузочный USB-накопитель ESR.
2. Настройте исследуемый компьютер для загрузки с внешнего накопителя.
3. Загрузите компьютер в ESR.
4. ESR попытается собрать существующие пароли.
5. ESR выполнит быструю предварительную атаку на обнаруженные учётные записи Windows.
6. Извлеките метаданные шифрования от учётных записей Windows (если пароль не был обнаружен на предыдущем шаге) для последующих атак.
7. Извлеките файлы подкачки и гибернации.
8. Осуществите поиск зашифрованных дисков. Если таковые будут найдены, извлеките метаданные шифрования.
9. Осуществите поиск зашифрованных виртуальных машин. В случае обнаружения извлеките метаданные шифрования для последующей атаки.
10. Снимите образы дисков для дальнейшего анализа.
11. Опционально: вы можете сбросить пароль к выбранной учётной записи, загрузиться в основную систему и войти в систему с новым паролем.

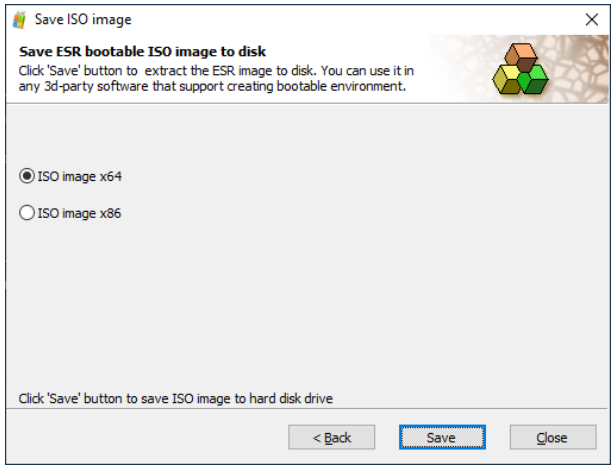
24.3.8.1. Подготовка загрузочного накопителя

Процесс подготовки загрузочного накопителя сводится к запуску программы установки Elcomsoft System Recovery на лабораторном компьютере (не на компьютере, который вы собираетесь исследовать) и следованию инструкциям мастера установки. Для установки потребуется достаточно объёмный и быстрый USB накопитель (32 ГБ или больше).









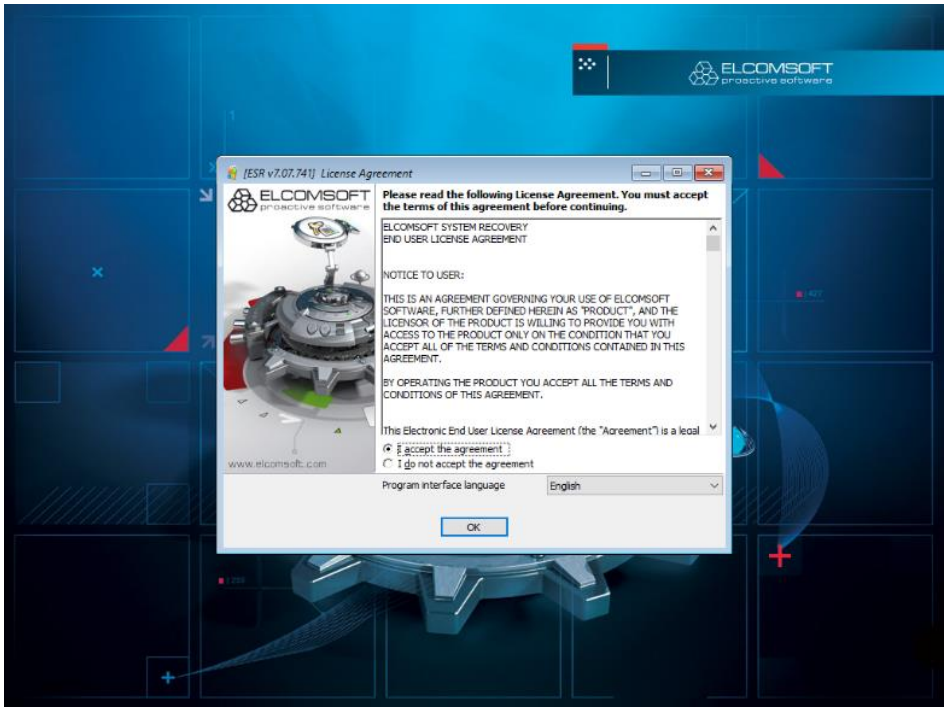
После создания загрузочного накопителя вставьте его в свободный разъём USB компьютера, который собираетесь исследовать.

24.3.8.2. Подготовка компьютера к загрузке

Для загрузки с накопителя вам потребуется изменить соответствующую настройку в BIOS/UEFI исследуемого компьютера. Как правило, по умолчанию загрузка с устройств USB запрещена. Добавьте USB накопитель на первую позицию в списке устройств для загрузки. Войти в BIOS на большинстве систем можно в первые секунды после включения нажатием клавиши Del либо другой клавиши в зависимости от системы (например, F10, F11 или F12). На некоторых компьютерах нажатие кнопки F2 вызывает меню, позволяющее выбрать устройство, с которого будет осуществляться загрузка.

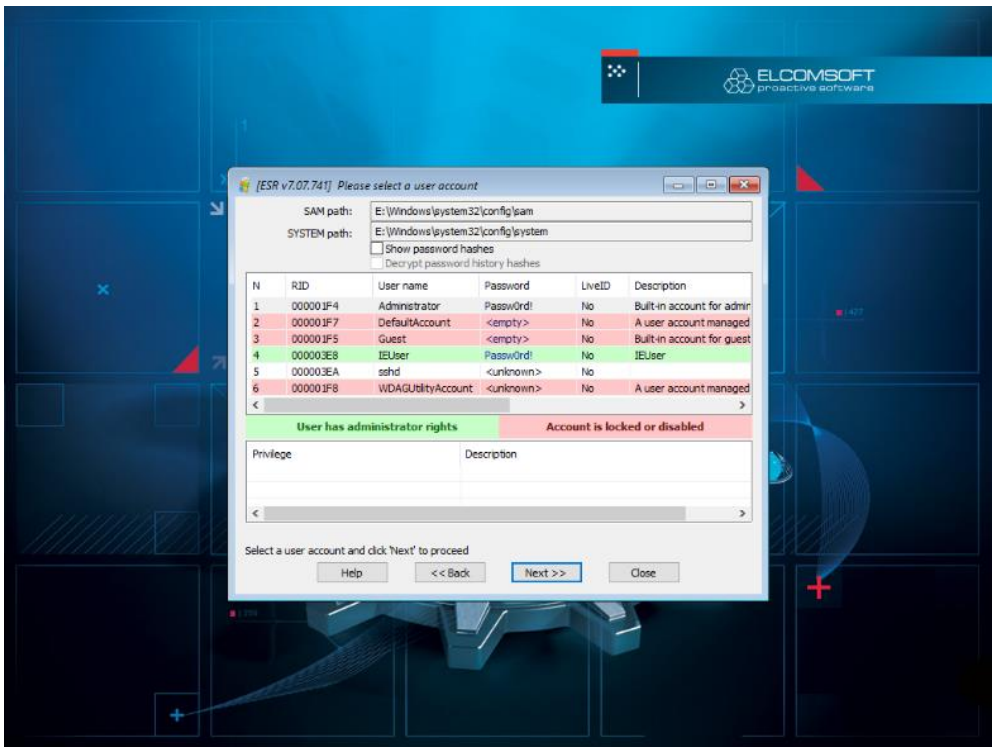
24.3.8.3. Загрузка с USB накопителя

Убедившись, что USB-накопитель с ESR на первом месте в списке загрузочных устройств, сохраните настройки и выйдите из BIOS. Должен начаться процесс загрузки. После того, как ESR загрузится, примите условия лицензионного соглашения и нажмите ОК для начала работы.



24.3.8.4. Автоматический подбор паролей

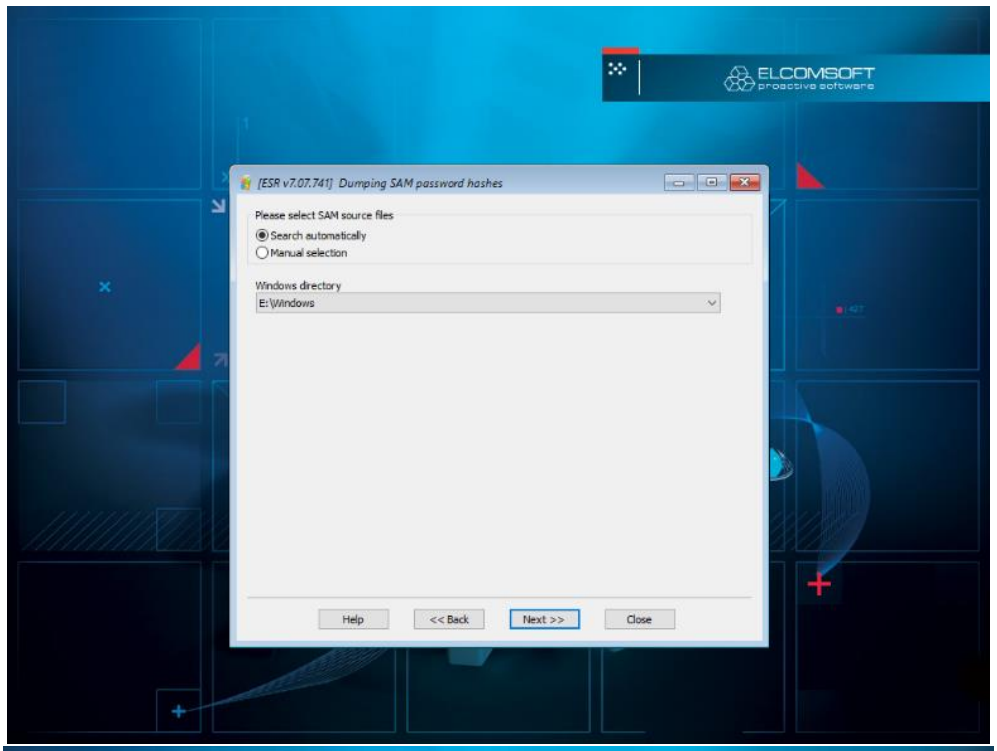
После запуска Elcomsoft System Recovery инструмент автоматически сканирует систему на наличие доступных паролей и запускает быструю предварительную атаку, которая может выявить учётные записи со слабыми паролями. Найденные пароли будут автоматически отображаться в окне ESR.

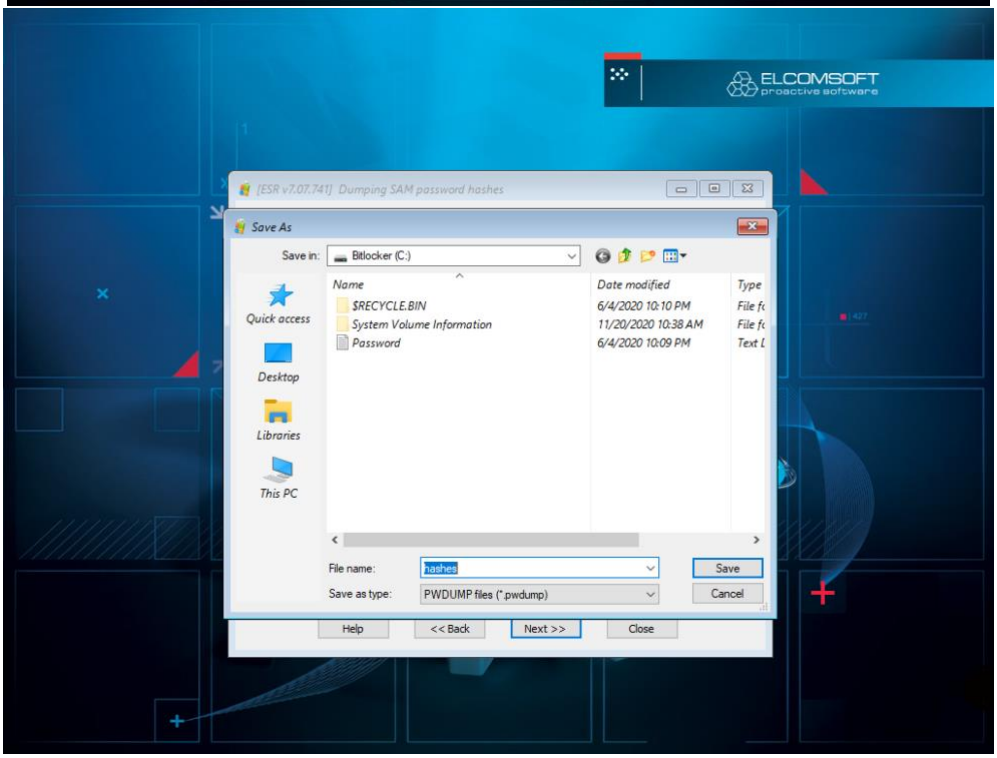


24.3.8.5. Извлечение метаданных для восстановления паролей к учётным записям

Для тех учётных записей, пароли к которым не были найдены в процессе предварительной атаки, можно извлечь метаданные шифрования. Эти данные можно использовать в Elcomsoft Distributed Password Recovery[81] для восстановления пароля к учётной записи.

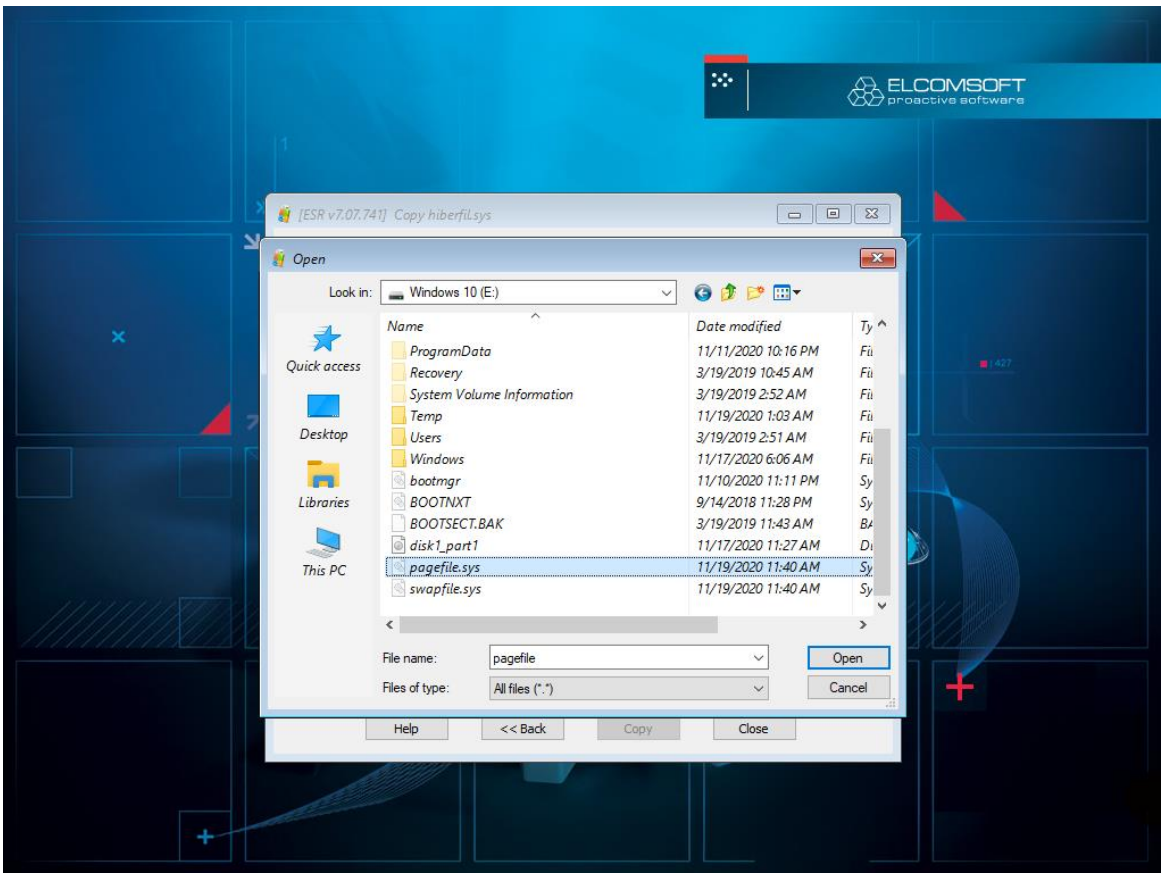
[81] https://www.elcomsoft.com/edpr.html





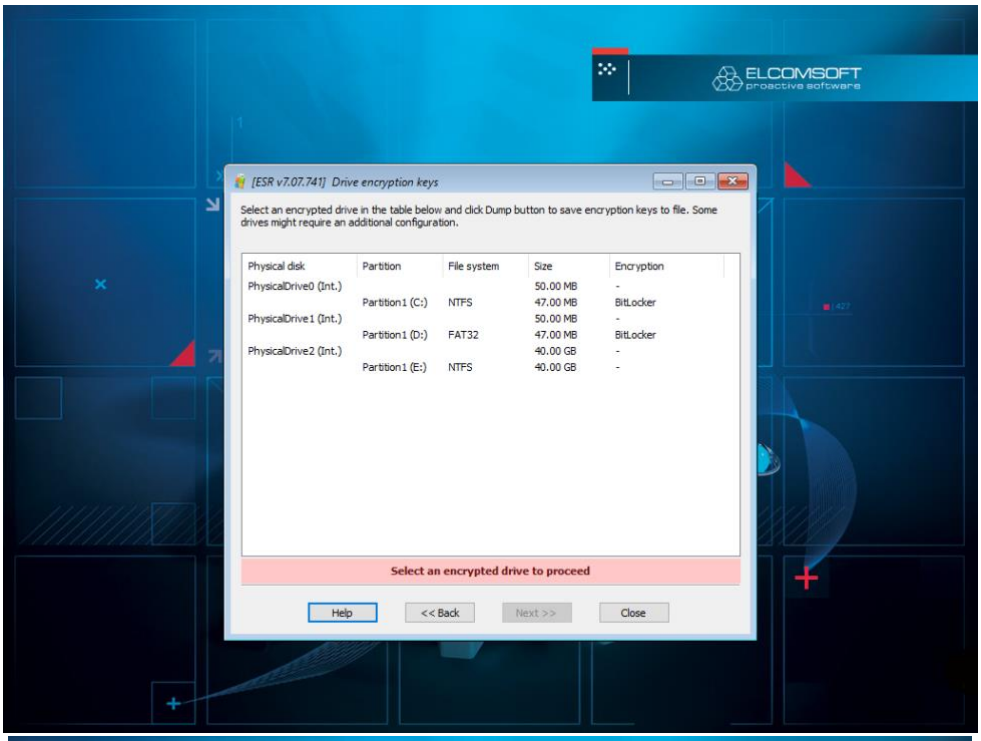
24.3.8.6. Файлы подкачки и гибернации

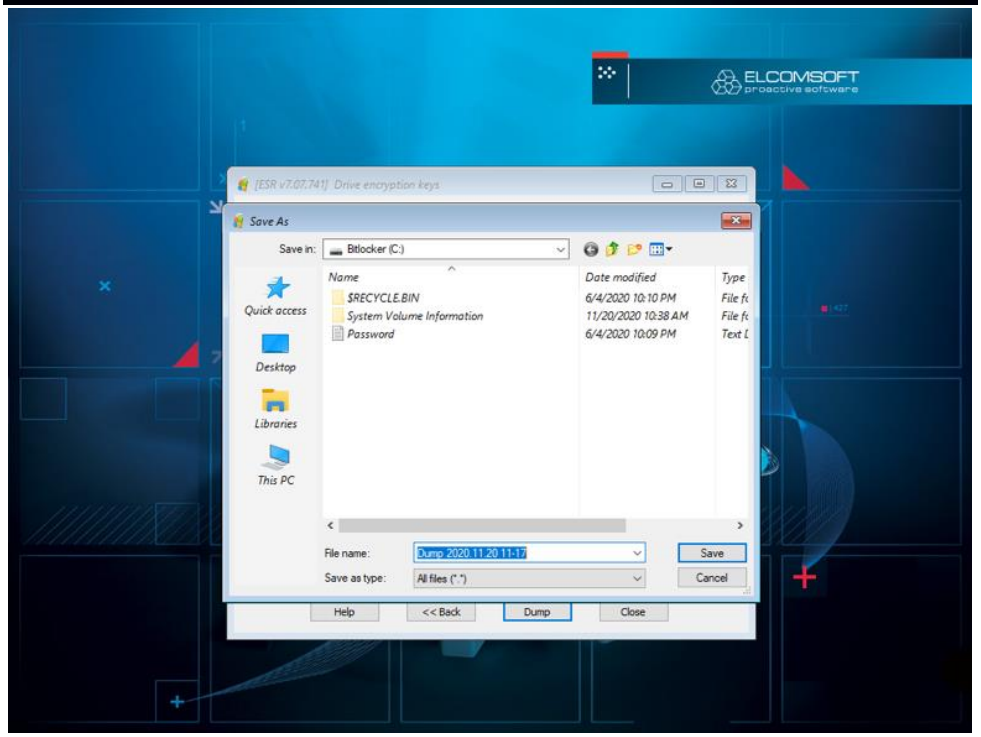
В этих файлах могут содержаться ключи шифрования, которыми защищаются зашифрованные диски VeraCrypt, TrueCrypt, PGP и BitLocker, если те были смонтированы перед выключением компьютера или погружением его в режим гибернации. Рекомендуем извлечь эти файлы и проанализировать их содержимое утилитой Elcomsoft Forensic Disk Decryptor.


ELCOMSOFT
proactive software
[ESR v7.07.741] Copy hiberfil.sys
Open
Look in: Windows 10 (E:)
Quick access
Desktop
Libraries
This PC
Name
Date modified
ProgramData 11/11/2020 10:16 PM
Recovery 3/19/2019 10:45 AM
System Volume Information 3/19/2019 2:52 AM
Temp 11/19/2020 1:03 AM
Users 3/19/2019 2:51 AM
Windows 11/17/2020 6:06 AM
bootmgr 11/10/2020 11:11 PM
BOOTNXT 9/14/2018 11:28 PM
BOOTSECT.BAK 3/19/2019 11:43 AM
disk1_part1 11/17/2020 11:27 AM
pagefile.sys 11/19/2020 11:40 AM
swapfile.sys 11/19/2020 11:40 AM
File name: pagefile
Files of type: All files (*.*)
Open
Cancel
Help
<< Back
Copy
Close

24.3.8.7. Поиск зашифрованных дисков

Зашифрованные диски часто используются в криминальной среде. ESR обладает возможностью автоматического поиска зашифрованных дисков — как смонтированных, так и размонтированных. В большинстве случаев извлечённые из заголовков таких дисков метаданные можно использовать для восстановления пароля шифрования.

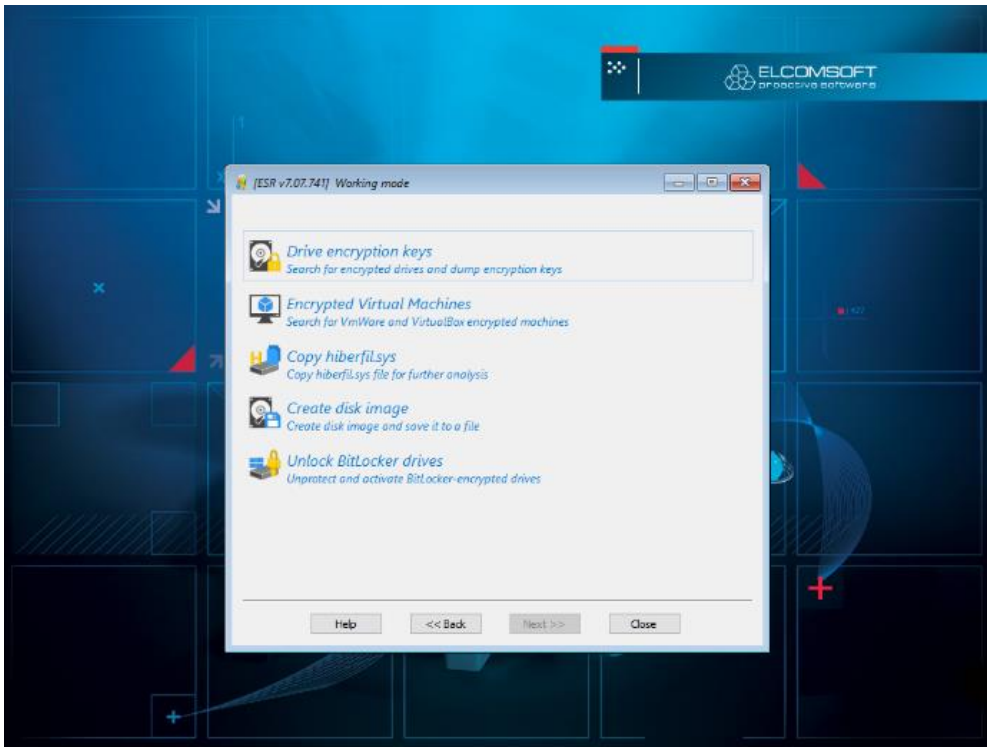


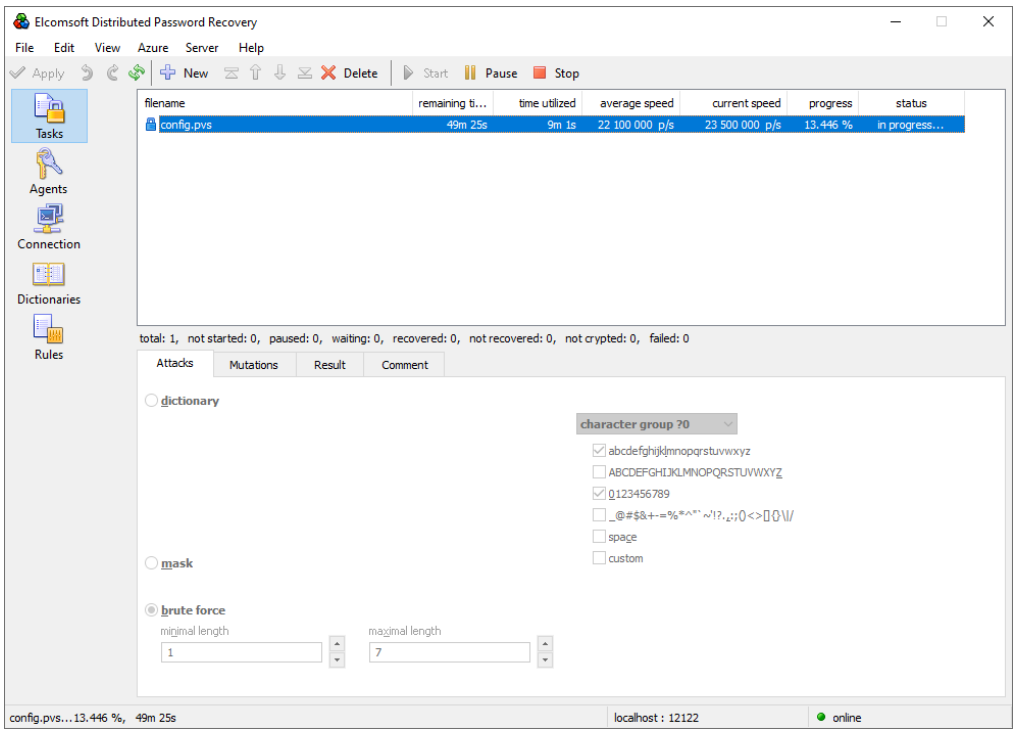


Внимание: если зашифрованный диск был смонтирован непосредственно перед анализом, в файлах подкачки и гибернации могут присутствовать двоичные ключи шифрования. Просканируйте эти файлы в Elcomsoft Forensic Disk Decryptor.

24.3.8.8. Поиск зашифрованных виртуальных машин

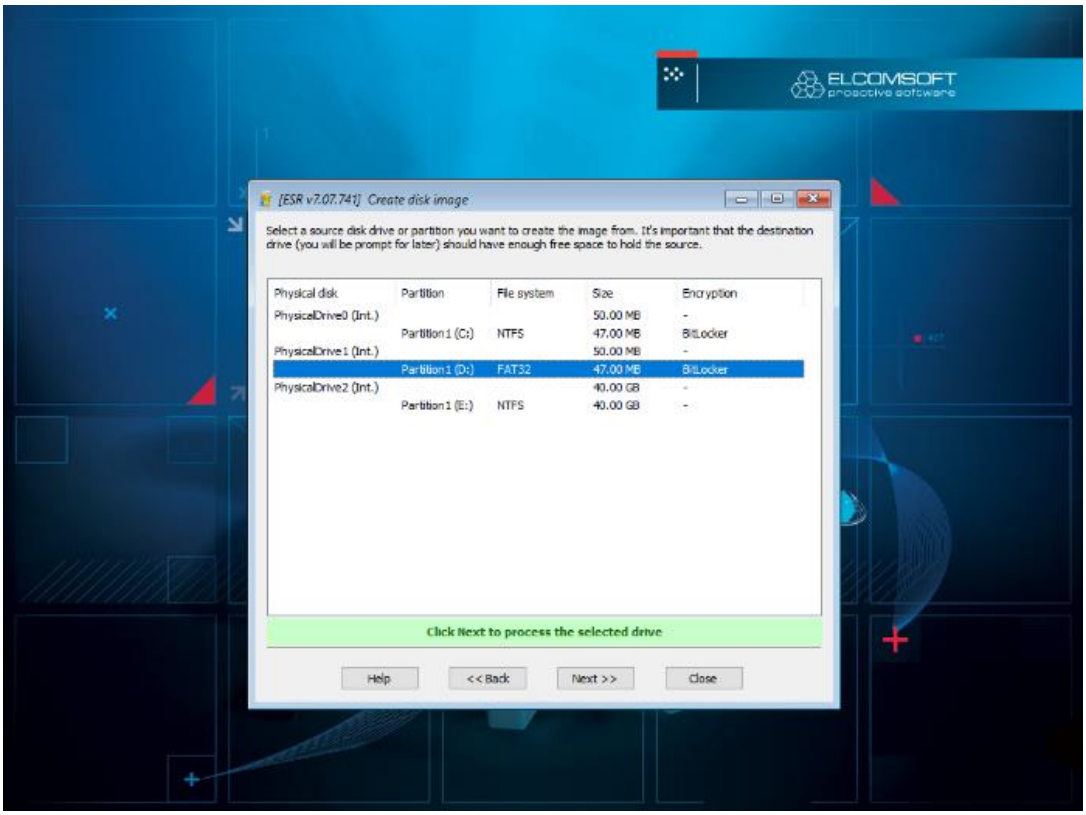
Виртуальные машины, защищённые стойким шифрованием, получили широкое распространение в криминальной среде. Использование не оставляющих цифрового следа зашифрованных виртуальных машин позволяет злоумышленникам минимизировать утечку инкриминирующих данных. ESR автоматизирует процесс поиска зашифрованных виртуальных машин. Для начала сканирования выберите пункт Encrypted Virtual Machines. При обнаружении зашифрованных виртуальных машин ESR сохраняет метаданные шифрования, необходимые для восстановления пароля посредством Elcomsoft Distributed Password Recovery.

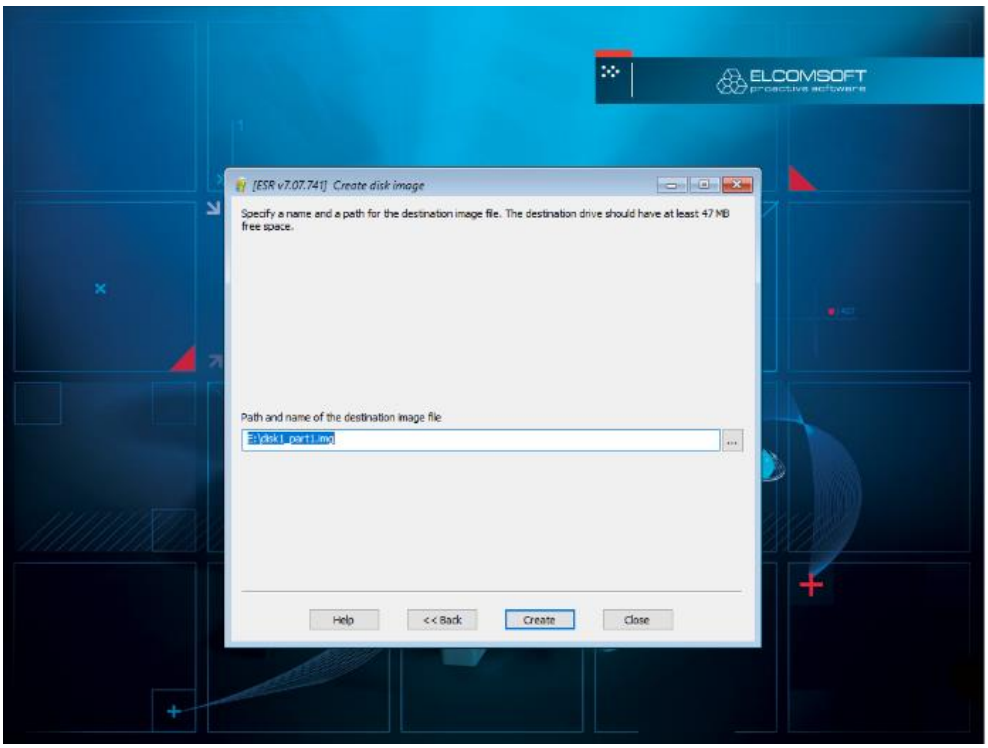


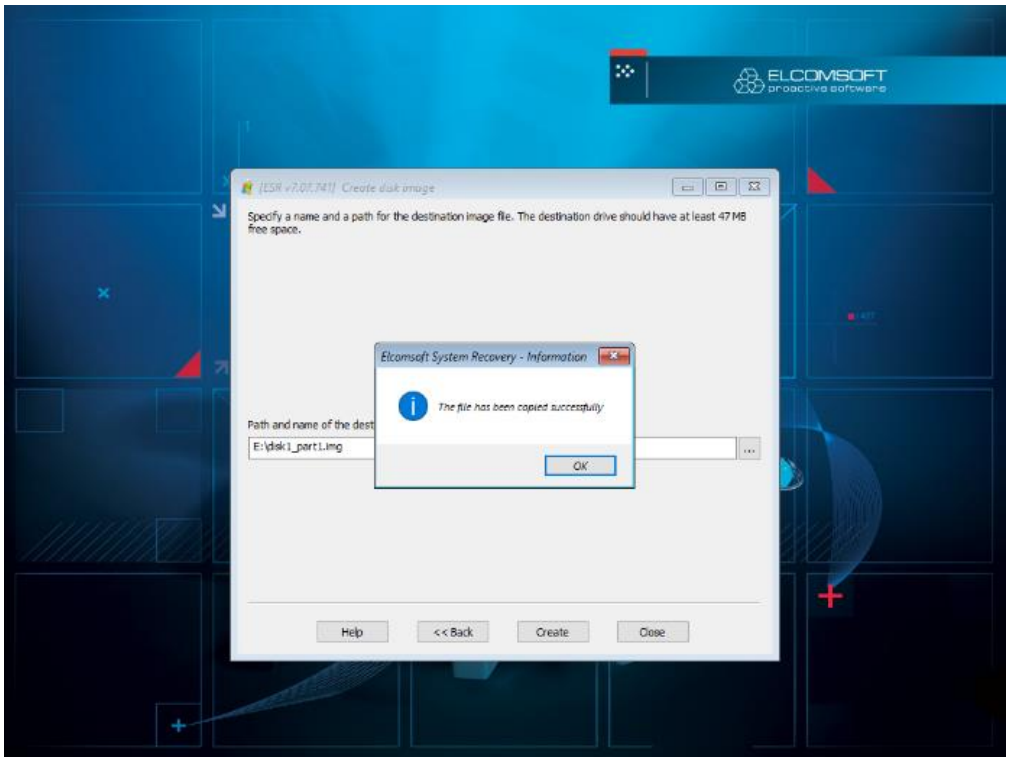


24.3.8.9. Создание образа диска

Распространённая практика судебной экспертизы – анализ образов дисков, а не физических устройств. И если традиционный подход к анализу предполагает извлечение жёсткого диска из корпуса компьютера, то Elcomsoft System Recovery позволяет создавать образы дисков, не извлекая накопители. Обратите внимание: для создания образа диска к компьютеру необходимо подключить дополнительный накопитель с достаточным количеством свободного места. Рекомендуем использовать накопители, отформатированные в NTFS или exFAT. Использование файловой системы FAT32 приведёт к ошибке при создании образов, размер которых превышает 4ГБ.

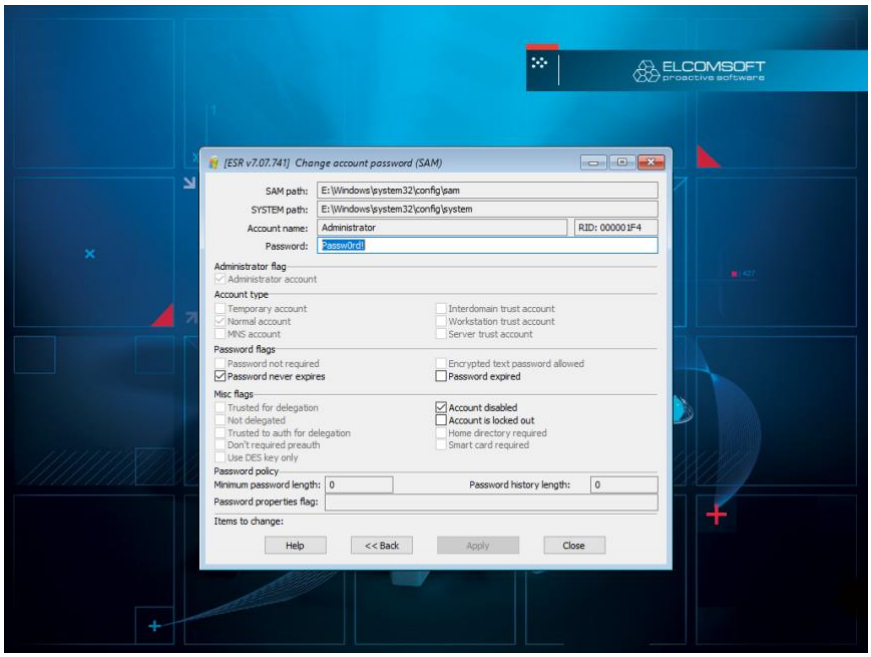



ELCOMSOFT
proactive software
[ESR v7.07.741] Create disk image
Specify a name and a path for the destination image file. The destination drive should have at least 47 MB free space.
Path and name of the destination image file
E:\disk1_part1.img
Help
<< Back
Create
Close


ELCOMSOFT
proactive software
Specify a name and a path for the destination image file. The destination drive should have at least 47 MB free space.
Elcomsoft System Recovery - Information
The file has been copied successfully
OK
Path and name of the dest
E:\disk1_part1.img
Help
<< Back
Create
Close

24.3.8.10. Дополнительно: анализ системы с авторизованной пользовательской сессией

В некоторых случаях может потребоваться выполнить анализ сеанса аутентифицированного пользователя. Если ESR удалось восстановить исходный пароль для одной из учетных записей пользователей, вы можете использовать этот пароль для входа в систему. Кроме того, в ESR доступна возможность сброса паролей учётных записей Windows.



24.3.8.11. Последствия сброса пароля учётной записи Windows

Если вы решите сбросить пароль какого-либо пользователя системы, вы потеряете доступ к информации, защищённой с помощью DPAPI (Windows Data Protection API). Эта информация включает:

– файлы, зашифрованные EFS (Encrypted File System). Ключи шифрования к таким файлам будут безвозвратно утрачены при сбросе пароля;

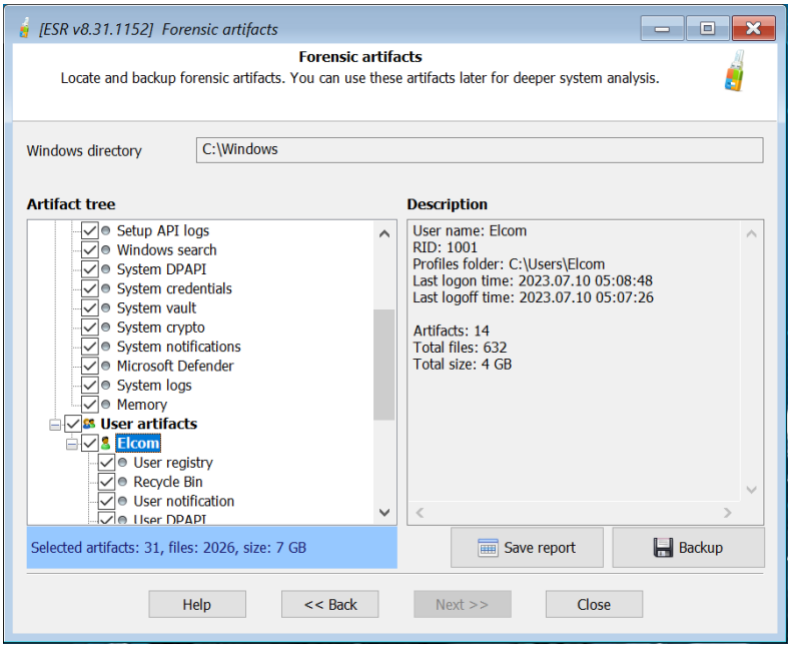
– пароли пользователя, сохранённые в браузерах Microsoft Edge, Google Chrome и других. Пароли к сетевым папкам и почтовым учётным записям.

Для доступа к любым из этих данных вам потребуется исходный пароль учётной записи пользователя.

24.4. Набор криминалистических инструментов

В составе продукта доступен набор инструментов для поиска, сбора и анализа цифровых улик при работе на выезде, с помощью которого можно быстро просканировать систему, собрать и просмотреть самые важные артефакты. Загрузив исследуемый компьютер с внешнего накопителя, эксперт сможет использовать новые функции инструментария для извлечения и анализа таких данных, как системные журналы и журнал событий Windows, сертификаты и ключи DPAPI, а также извлекать файлы гибернации и подкачки для последующего сканирования на предмет ключей к дискам, зашифрованным BitLocker и сторонними криптоконтейнерами. Кроме того, эксперт сможет использовать функции просмотра списка установленных в системе приложений и анализа действий пользователей на компьютере с привязкой к временной шкале.

Также доступен инструмент, позволяющий узнать, к каким файлам и папкам пользователь недавно обращался. Для проведения анализа не потребуются пароли пользователей.



Извлекаются данные из нескольких десятков категорий, которые мы отобрали по критериям важности для расследования и скорости, с которой их можно извлечь. Инструмент использует стратегию «низко висящего фрукта», позволяя эксперту за считанные минуты провести предварительный анализ и сохранить на внешний накопитель ключи шифрования и другие артефакты, которые позволят в дальнейшем получить доступ к зашифрованным уликам и всё это без необходимости извлекать из компьютера диски и создавать их образы.

Elcomsoft System Recovery не просто извлекает некоторое количество цифровых артефактов. С использованием нового функционала эксперт сможет получить всестороннее представление об активности пользователя как онлайн, так и офлайн. Так, с использованием встроенного инструментария можно быстро извлечь пароли пользователя, важные документы, информацию о запущенных приложениях и файлах, к которым обращался пользователь. Полный список собираемых данных включает несколько десятков категорий и постоянно расширяется.

Системные артефакты:

- System Registry;
- Active Directory;
- Amcache;
- Program Compatibility Assistant;
- Energy reports;
- Microsoft Store logs;
- Shimcache;
- SRUM (System Resource Utilization Monitor);
- Microsoft User Access Logs;
- Scheduled tasks;
- Windows events;
- Windows prefetch;
- setup.api logs;

- Recycle Bin;
- WER (Windows Error Reporting);
- WiFi network configs and passwords;
- Windows search database;
- System DPAPI;
- System credentials;
- System vault;
- System crypto keys and certificates;
- Windows notifications;
- Defender logs;
- System logs;
- NGC keys;
- Memory dumps.

Пользовательские данные:

- User Registry;
- ActivitiesCache;
- Recycle Bin;
- Notifications;
- RDP cache;
- Crash dumps;
- DPAPI keys;
- PowerShell console history;
- User credentials;
- User vault;
- User crypto keys and certificates;
- Files in Desktop/Documents/Downloads/Videos folders;
- Jumplist (Recent files);
- Files in Videos folder
- Windows Mail/calendar/phone/contacts database;
- Данные веб-браузеров:
    - **Chromium:** Amigo, Xpom, Kometa, Nichrome, Torch, Blisk, Orbitum, Slimjet, QIP Surf, Kinza, BlackHawk, Superbird, Sidekick, Iridium, Vivaldi, SRWare Iron, GhostBrowser, CentBrowser, Xvast, Chedot, SuperBird, SalamWeb, Elements, Chrome, CocCoc, QQBrowser, 360Browser, 360, Comodo Dragon, Brave, Epic Privacy, AVAST Software, Citrio, Uran, Coowon, 7Star, Chrome Canary, CoolNovo, Sputnik, Microsoft Edge, Atom, AVG, CCleaner, CryptoTab, Maxthon, Netbox, Swing, UR, ViaSat, Yandex, UCBrowser;
    - **Mozilla:** Firefox, Slim, Pale Moon, Waterfox, Cyberfox, BlackHawk, IceCat, Thunderbird, PostboxApp, Comodo IceDragon, SeaMonkey, Basilisk, BitTube, Cliqz, K-Meleon, Falkon;
    - **Microsoft Edge;**
    - **Safari.**

Инструментарий доступен в виде вкладки “Forensic artifacts”. Встроенные в Elcomsoft System Recovery инструменты для поиска цифровых улик позволяют значительно ускорить начальную стадию расследования за счёт сокращения издержек по созданию образа диска и его последующего подробного анализа.

24.5. Особенности анализа компьютеров с ОС Windows 11

В системных требованиях Windows 11 появилось обязательное наличие в компьютере модуля безопасности TPM. Это требование способно радикально изменить модель безопасности новой версии ОС. В то же время обязательного шифрования системного раздела настольных компьютерах по-прежнему не наблюдается. Для чего в Windows 11 используется TPM, как именно усилена безопасность и можно ли обойти эти меры в процессе криминалистического исследования компьютера? Об этом — в нашем исследовании.

24.5.1. Windows 11: учётные записи с безопасной авторизацией без пароля

Традиционный способ входа в учётную запись Windows — пароль. Вплоть до выхода Windows 8 пароль оставался единственным способом войти в систему по локальной учётной записи (рассмотрение доменных учётных записей отложим на будущее).

В Windows 8 появился дополнительный способ авторизации. Теперь для входа в систему можно использовать не только локальную учётную запись, но и учётную запись Microsoft Account — ту самую, посредством которой осуществляется доступ к онлайновому почтовому сервису Hotmail, мессенджеру Skype, облачному хранилищу OneDrive, подписке на Office 365 и многим другим сервисам компании Microsoft. В последующих выпусках Windows учётным записям Microsoft Account придавался всё больший вес, а возможность установки ОС без неё становилась всё более сложной. В младших редакциях Windows использование локального логина и пароля и вовсе ограничили: настроить систему при установке можно исключительно с использованием онлайновой учётной записи.

Первый вход в учётную запись Microsoft Account требует наличия активного соединения с интернетом. Данные учётной записи проверяются Microsoft на удалённом сервере, после чего хэш от пароля сохраняется (кэшируется) на компьютере; это позволяет впоследствии входить в учётную запись при отсутствии соединения. У такого поведения есть и обратная сторона: хэш от пароля можно извлечь из соответствующей базы данных на компьютере, после чего восстановить оригинальный пароль посредством быстрой офлайновой атаки. Подчеркнём, что восстанавливается именно пароль от учётной записи Microsoft Account, посредством которого можно авторизоваться не только на исследуемом компьютере, но и в онлайновых сервисах Microsoft — получив, таким образом, доступ к переписке пользователя в Hotmail, чатам Skype, файлам OneDrive и массе другой информации. Более того, в учётных записях Microsoft хранятся в том числе и депонированные ключи BitLocker, использующиеся для восстановления доступа к зашифрованным дискам. Добавлю, что скорость атаки на пароли Windows исключительно высокая, что позволяет в разумные сроки восстанавливать даже

достаточно сложные пароли. Мы писали о такой уязвимости в нашем блоге: Microsoft Account: удобство или дыра в безопасности?[82]

Использование двухфакторной аутентификации может помочь защитить содержимое онлайновой учётной записи, однако восстановленный пароль позволяет разблокировать и компьютер пользователя, получив, таким образом, доступ к такой информации, как пароли из браузера Edge, файлам в облачном хранилище OneDrive и всей той информации, для доступа к которой в ином случае потребовалось бы пройти двухфакторную проверку.

Разработчики Microsoft предложили дополнительные способы авторизации — вход по PIN-коду и при помощи биометрических данных (подсистема Windows Hello), о которых мы расскажем ниже. Ни один из этих способов не решил основной проблемы — возможности восстановления оригинального пароля от онлайновой учётной записи посредством сверхбыстрой офлайновой атаки.

В Windows 11 добавился новый тип учётных записей с входом без пароля. При использовании таких учётных записей для входа в систему не нужно (и невозможно) вводить пароль от учётной записи Microsoft Account; вместо пароля используется PIN-код или биометрические данные подсистемы Windows Hello (например, видеопоток с сертифицированной инфракрасной стереокамеры или данные датчика отпечатков пальцев). О том, где хранится PIN-код и почему такой способ авторизации заметно безопаснее входа по паролю будет рассказано далее по тексту; сейчас же перечислим доступные в Windows 11 для обычного (не доменного) пользователя способы входа в систему.

– [**используется по умолчанию**] Учётная запись Microsoft Account без пароля. Пароль для входа в систему использовать невозможно; поддерживается вход по PIN-коду (TPM), Windows Hello или через авторизацию в приложении Microsoft Authenticator (онлайн);

– [так было в Windows 10, и так остаётся при обновлении Windows 10 > Windows 11] Учётная запись Microsoft Account с паролем. Хэш пароля к учётной записи хранится локально и не защищается TPM. Поддерживается вход по PIN-коду (TPM), Windows Hello;

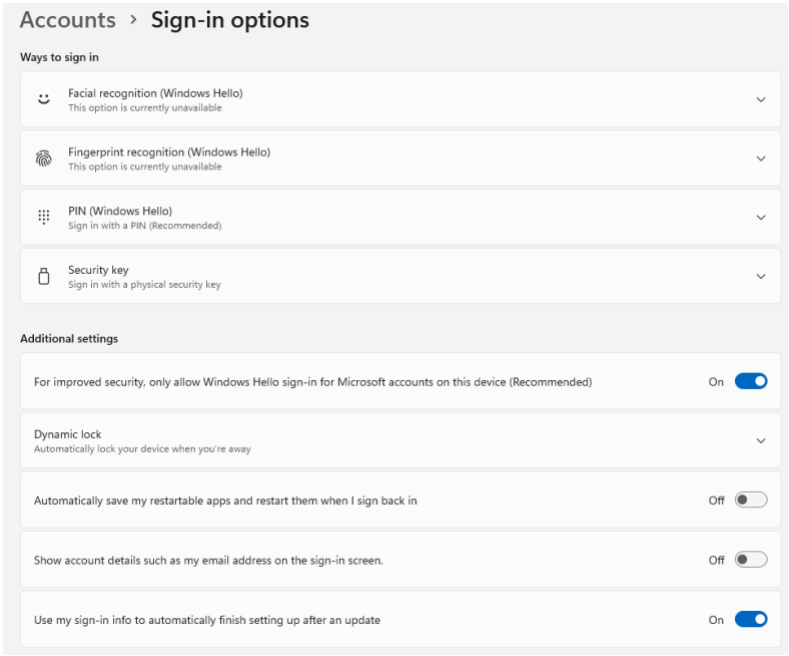
– локальная учётная запись Windows (вход по паролю). Для входа может использоваться локальный пароль (его хэш хранится в системе, не защищается TPM), PIN (TPM) или Windows Hello.

24.5.2. В каких случаях в Windows 11 используется вход без пароля?

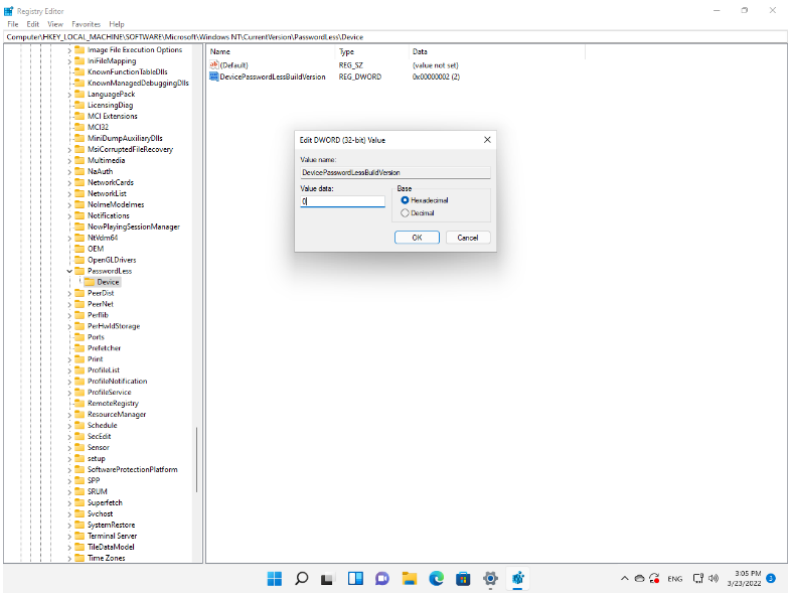
В Windows 11 поддерживаются способы входа как по паролю, так и без него. Режим входа без пароля используется в новом типе учётных записей и включается по умолчанию как во время установки Windows 11 на новый компьютер, так и при создании новой учётной записи на компьютерах, на которых Windows 11 была установлена в виде обновления с Windows 10. В то же время существующие в Windows 10 учётные записи, в которых для входа использовался пароль, остаются в Windows 11 в неизменном виде.

[82] https://blog.elcomsoft.ru/2017/02/microsoft-account-udobstvo-ili-dyira-v-bezopasnosti/

Для того, чтобы включить вход без пароля, пользователю необходимо включить соответствующую опцию в настройках системы (Sign-in options):



Также этот способ входа можно активировать через Windows Registry:



Подытожим:

– при установке Windows 11 на новый компьютер: Microsoft Account, вход без пароля;

– при обновлении с Windows 10: используется тот же способ входа, что и в оригинальной ОС Windows 10;

– новые учётные записи, создаваемые в Windows 11, установленной любым способом: Microsoft Account, вход без пароля.

24.5.3. Использовался ли TPM в Windows 10?

Да, в Windows 10 также используется модуль безопасности TPM2.0. Разница между Windows 10 и Windows 11 не в масштабах использования TPM (здесь мы не увидели принципиальной разницы), а в том, что в Windows 11 TPM обязателен, а в Windows 10 — нет. Эта, казалось бы, небольшая разница, приводит к глобальным последствиям в области безопасности при использовании входа по PIN-коду вместо пароля. Подробно об этом Microsoft рассказывает в статье (на английском языке) Why a PIN is better than an online password (Windows) — Windows security, с содержанием которой можно ознакомиться в переводе Почему ПИН-код лучше, чем пароль в Интернете (Windows) — Windows security | Microsoft Docs. В этой статье Microsoft делает несколько не вполне корректных утверждений, очевидная интерпретация которых оставляет ложное впечатление. Разберём подробности. Ниже приводится цитата из статьи в Microsoft Documentation[83](сохранена оригинальная орфография):

ПИН-код привязан к устройству

Одно важное отличие между онлайн-паролем и ПИН-кодом Hello состоит в том, что ПИН-код привязан к определённому устройству, на котором он был настроен. ПИН-код не может использоваться без конкретного оборудования. Кто-то, кто крадёт ваш пароль в Интернете, может войти в вашу учётную запись из любого места, но, если он украдёт ПИН-код, им также придётся украсть ваше физическое устройство!

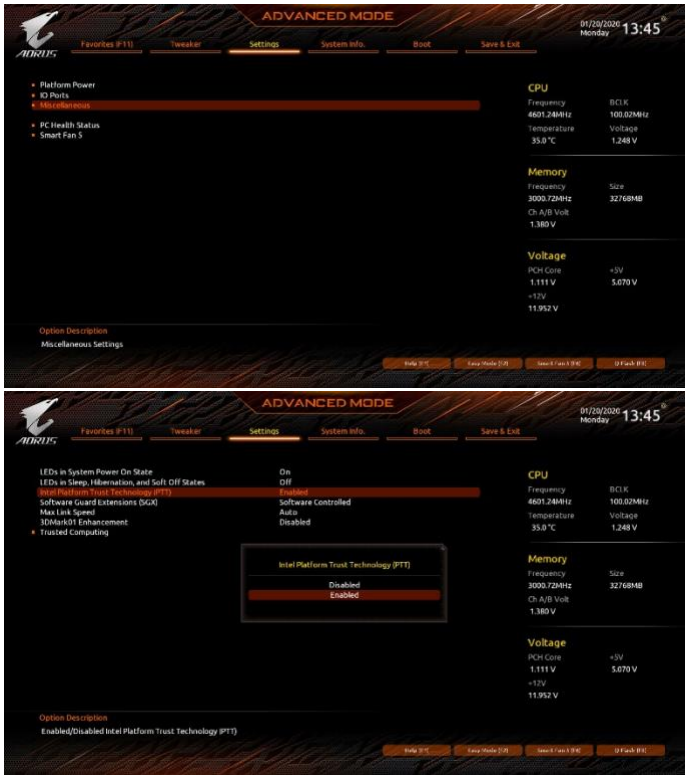
ПИН-код поддерживается оборудованием

ПИН-код Hello поддерживается микросхемой доверенного платформенного модуля (TPM), представляющей собой надежный криптографический процессор для выполнения операций шифрования. Эта микросхема содержит несколько механизмов физической защиты для предотвращения взлома, и вредоносные программы не могут обойти функции безопасности TPM. Многие современные устройства имеют TPM. Windows 10, с другой стороны, имеет дефект, не связывающий локальные пароли с TPM. Именно по этой причине ПИН-коды считаются более безопасными, чем локальные пароли.

Если воспринимать информацию буквально, создаётся ложное ощущение, будто PIN-код является своеобразной панацеей, всегда хранится в модуле TPM и не может быть взломан. Это утверждение соответствует действительности лишь в ограниченных условиях; в общем же случае это не так. Дело в том, что Windows 10 может работать как на компьютерах с модулем TPM, так и без него, причём пользователю об этом система не сообщает.

[83] https://learn.microsoft.com/ru-ru/windows/security/identity-protection/hello-for-business/

Более того, даже на компьютерах, в прошивке которых присутствует эмуляция TPM, эта эмуляция чаще всего по умолчанию отключена — пользователю предлагается самостоятельно зайти в UEFI BIOS, отыскать меню "Miscellaneous" и включить настройку, которая может называться, к примеру, “Intel Platform Trust Technology (PTT)”. Сколько пользователей включит эту настройку, а какое количество оставит её неизменной или просто не узнает о её существовании?



Если TPM в системе отсутствует или не включён в UEFI BIOS, Windows 10 всё равно предложит использовать для входа PIN-код, а Microsoft всё так же будет убеждать, что этот способ входа более безопасен по сравнению с паролем. Это не так. Пароль от учётной записи в виде хэша всё так же хранится на диске, а сам PIN-код с компьютера без TPM можно взломать простым перебором (цифровые PIN-коды, даже шестизначные, можно перебрать за считанные секунды).

Без модуля TPM вход в Windows по PIN-коду небезопасен, а сам цифровой PIN-код можно подобрать с использованием соответствующего ПО намного быстрее, чем подбирается буквенно-символьный пароль.

Совсем иначе дела обстоят в случае, если в системе присутствует и активирован модуль TPM2.0 в физическом виде либо в виде процессорной эмуляции. Рассмотрим поведение системы в следующих сценариях, которые мы протестировали в нашей лаборатории.

Сценарий 1: Система с Windows 10 (вход по PIN-коду) без TPM переносится на другой компьютер без TPM. Переносится физический диск с установленной ОС. Результат: вход по PIN-коду срабатывает на новом компьютере так же, как и на старом.

Сценарий 2: Система с Windows 10 (вход по PIN-коду) без TPM переносится на другой компьютер без TPM. Переносится только копия раздела с установленной ОС; аппаратное

обеспечение между двумя компьютерами не совпадает ни по одной позиции. Результат: вход по PIN-коду срабатывает на новом компьютере так же, как и на старом.

Сценарий 3: Система с Windows 10 (вход по PIN-коду) без TPM переносится на компьютер с установленным и активным модулем TPM. Переносится только копия раздела с установленной ОС; аппаратное обеспечение между двумя компьютерами не совпадает ни по одной позиции. Результат: вход по PIN-коду срабатывает на новом компьютере так же, как и на старом.

Сценарий 4: Система с Windows 10 (вход по PIN-коду) с активным модулем TPM переносится на другой компьютер с активным модулем TPM. Переносится копия раздела с установленной ОС; аппаратное обеспечение между двумя компьютерами не совпадает. Результат: вход по PIN-коду на новом компьютере не срабатывает; для входа требуется пароль от учётной записи; для использования PIN-кода потребовалось удалить старый PIN и настроить новый.

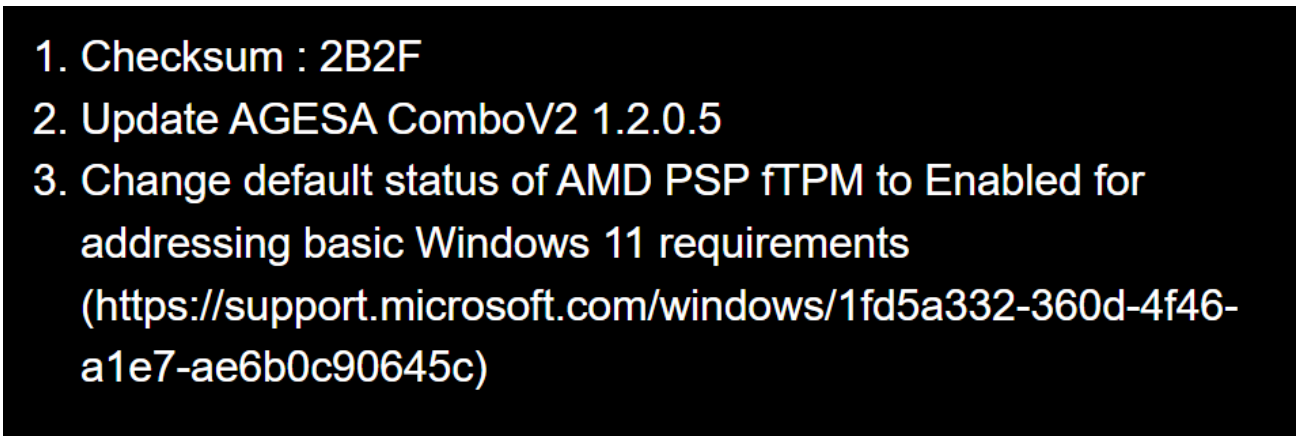
Очевидно, что только четвёртый сценарий соответствует модели безопасности, описанной Microsoft в статье Почему ПИН-код лучше, чем пароль в Интернете (Windows) — Windows security | Microsoft Docs.[84]

24.5.4. Оборудован ли исследуемый компьютер модулем TPM?

Модули TPM (как правило, в виде процессорной эмуляции, что не оказывает влияния на реальную безопасность системы) присутствуют в большинстве портативных компьютеров (ноутбуки, планшеты с Windows, устройства два-в-одном и т.п.), оборудованных процессором Intel 8-го поколения и более новыми либо процессором AMD с архитектурой Zen и более новыми. В ноутбуках TPM, как правило, активен по умолчанию.

Для настольных компьютеров ситуация отличается. Процессорная эмуляция TPM по-прежнему доступна в системах с процессором Intel 8-го поколения и более новыми либо процессором AMD с архитектурой Zen и более новыми, однако поддержка TPM, как правило, выключена по умолчанию на уровне настроек UEFI BIOS. Ситуация стала меняться с выходом платформы Intel 12-го поколения (Alder Lake), а производители системных плат для платформ AMD с сокетом AM4 стали публиковать прошивки, в которых fTPM (firmware TPM) активируется по умолчанию.

[84]https://learn.microsoft.com/ru-ru/windows/security/identity-protection/hello-for-business/

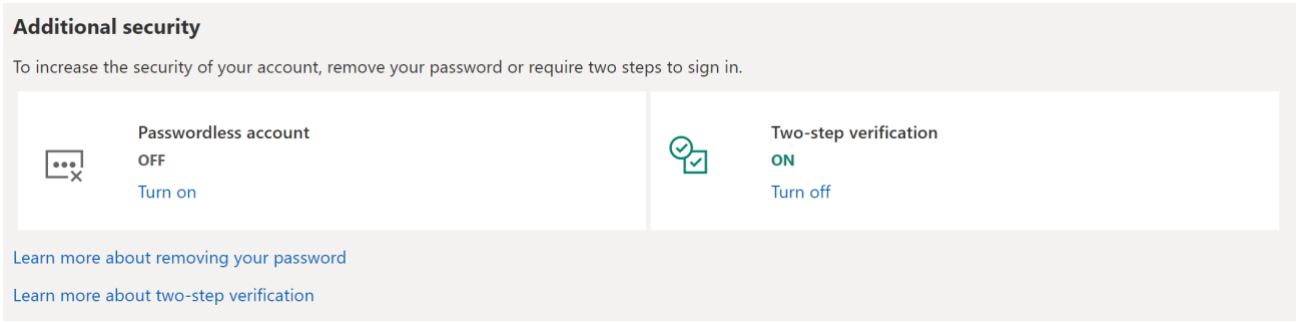


Проверить наличие модуля TPM можно в настройках системы (при анализе авторизованной пользовательской сессии) либо в настройках UEFI BIOS (если используется загрузочный накопитель).

24.5.5. Экзотические конфигурации: вход без пароля в Windows 10

Необходимо отметить существование такой экзотической конфигурации, как системы Windows 10, использующие учётные записи Microsoft с входом без пароля.

В сентябре 2021 года компания анонсировала своё видение будущего без паролей[85]. Пользователям очередной сборки Windows 10 предлагалось изменить настройки учётной записи Microsoft Account, запретив вход в учётную запись по паролю. Использование такой учётной записи для входа в систему позволяло избавиться от хранения хэша пароля на локальном компьютере. В то же время пользователь терял возможность войти в учётную запись Microsoft по логину и паролю; для успешного входа требовался доступ к доверенному телефонному номеру или ранее авторизованному устройству с установленным на нём приложением Microsoft Authenticator. С учётом того, что данное приложение доступно исключительно для смартфонов на iOS и Android (но не для компьютеров под управлением Windows), целесообразность данного нововведения представляется несколько сомнительной. (Инструкция: How to go passwordless with your Microsoft Account)[86]. Новшество не получило заметного распространения из-за неочевидных преимуществ и существенного неудобства использования.



[85]https://www.microsoft.com/en-us/security/blog/2021/09/15/the-passwordless-future-is-here-for-your-microsoft-account/
[86]https://support.microsoft.com/en-us/account-billing/how-to-go-passwordless-with-your-microsoft-account-674ce301-3574-4387-a93d-916751764c43

24.5.6. Каким образом Windows 11 использует TPM при авторизации входа в систему

В документации Microsoft (How Windows uses the TPM — Windows security | Microsoft Docs)[87] описаны способы, которыми Windows может использовать аппаратный модуль безопасности. Реальность значительно скромнее: "может" не означает "использует". Так, пароли, которые пользователь хранит в браузере Microsoft Edge, защищены механизмом DPAPI, но ключ шифрования хранится на системном диске (он зашифрован данными учётной записи) и не защищается TPM, что позволяет извлечь эти пароли из образа диска, если известен пароль от учётной записи пользователя.

Вместо того, чтобы использовать TPM для хранения всё большего количества данных, в Microsoft попытались обойти проблему, представив способ входа в учётную запись без пароля. Именно этот способ — и только на системах с TPM! — позволяет говорить о безопасности учётной записи: теперь защищённые DPAPI данные невозможно расшифровать, не войдя в систему, а войти в систему можно исключительно по PIN-коду (или через Windows Hello), который будет проверяться аппаратным модулем TPM. Любое изменение в конфигурации системы (как изменение аппаратной части, так и загрузка с внешнего накопителя) приведут к тому, что модуль TPM не отдаст нужный ключ, и защищённые данные расшифровать не удастся.

Подведём итог:

В Windows 11 с TPM невозможно взломать PIN-код. Для нового типа учётных записей с авторизацией без пароля невозможно ни подобрать пароль, ни использовать пароль к Microsoft Account, извлечённый из другого компьютера или учётной записи.

Существует техническая возможность конвертации учётной записи из нового типа в локальную, для которой вход будет осуществляться по известному паролю. При такой конвертации (например, в программе Elcomsoft System Recovery) будет утрачен доступ к зашифрованным в NTFS файлам и папкам, а также данным, защищённым DPAPI. В то же время такая конвертация может оказаться полезной для исследования системы пользователя.

24.5.7. Монтирование зашифрованных дисков BitLocker в Windows 11

Ни сам механизм BitLocker, ни политики шифрования в Windows 11 не получили серьёзных изменений в сравнении с Windows 10. После анонса Windows 11 у многих обозревателей возникло впечатление, что Microsoft будет шифровать системный раздел Windows 11 так же, как это делают производители смартфонов. Оказалось, что это не так. По умолчанию (посредством BitLocker Device Encryption) шифруются лишь оборудованные TPM портативные устройства — ноутбуки, планшеты и устройства два-в-одном, однако точно таким же образом шифрование включалось и в Windows 8, и в Windows 10. При установке Windows 11 на настольный компьютер шифрование по умолчанию не включается. Для того, чтобы использовать BitLocker, требуется редакция Windows 11 Pro, Enterprise или Education. Для пользователей младшей редакции Home шифрование остаётся недоступным.

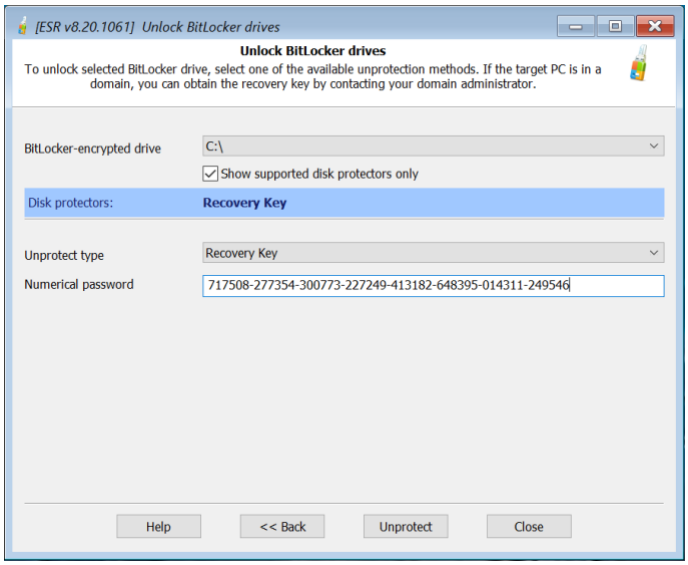
Что делать, если в исследуемой системе активно шифрование BitLocker? При использовании Elcomsoft System Recovery вам потребуется сначала смонтировать

[87] https://learn.microsoft.com/en-us/windows/security/hardware-security/tpm/how-windows-uses-the-tpm

зашифрованный раздел, введя депонированный код восстановления доступа BitLocker Recovery Key (подробности — в статье Механизмы защиты BitLocker: какие диски можно, а какие нельзя взломать)[88]. При использовании TPM разблокировать зашифрованный диск можно или так, или загрузившись и авторизовавшись в оригинальную установку Windows на том же самом компьютере в неизменной аппаратной конфигурации. Создать образ раздела и разблокировать его паролем (или PIN-кодом) не удастся: ни PIN, ни пароль не участвуют в шифровании, а ключ хранится в модуле TPM, извлечь его из которого невозможно.

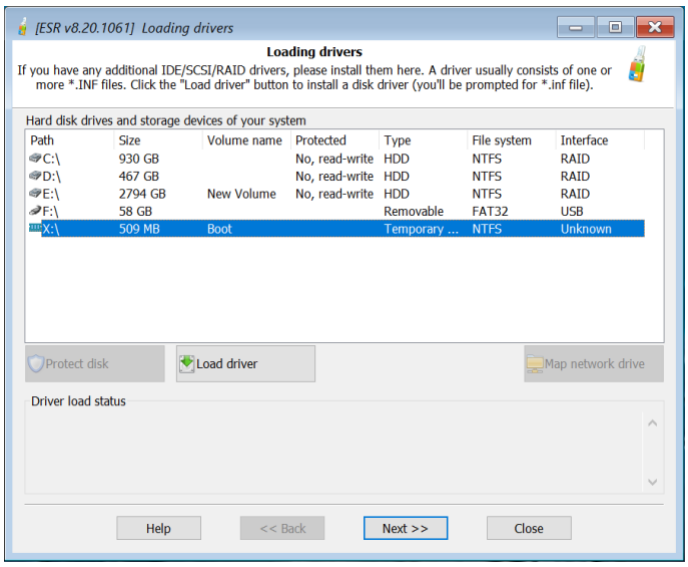
Единственный способ разблокировать такие тома BitLocker — использовать ключ восстановления BitLocker. Для портативных устройств с BitLocker Device Encryption Windows автоматически создаёт ключ восстановления при шифровании системного раздела; ключ восстановления будет так же автоматически загружен в учётную запись Microsoft первого же пользователя, который войдёт в систему на этом компьютере с правами администратора и использует учётные данные Microsoft для входа в систему. Этот ключ можно запросить у Microsoft или загрузить его, войдя в учётную запись Microsoft пользователя и перейдя по следующей ссылке: https://account.microsoft.com/devices/recoverykey[89]

При помощи депонированного ключа диск разблокируется:



Обратите внимание: после разблокировки диску назначается новая буква.

[88]https://blog.elcomsoft.ru/2020/09/mehanizmy-zashhity-bitlocker-kakie-diski-mozhno-a-kakie-nelzya-vzlomat/
[89]https://account.microsoft.com/devices/recoverykey



После этого можно приступать к конвертации учётных записей.

24.5.8. Разблокировка и конвертация учётных записей Windows 11 с авторизацией без пароля

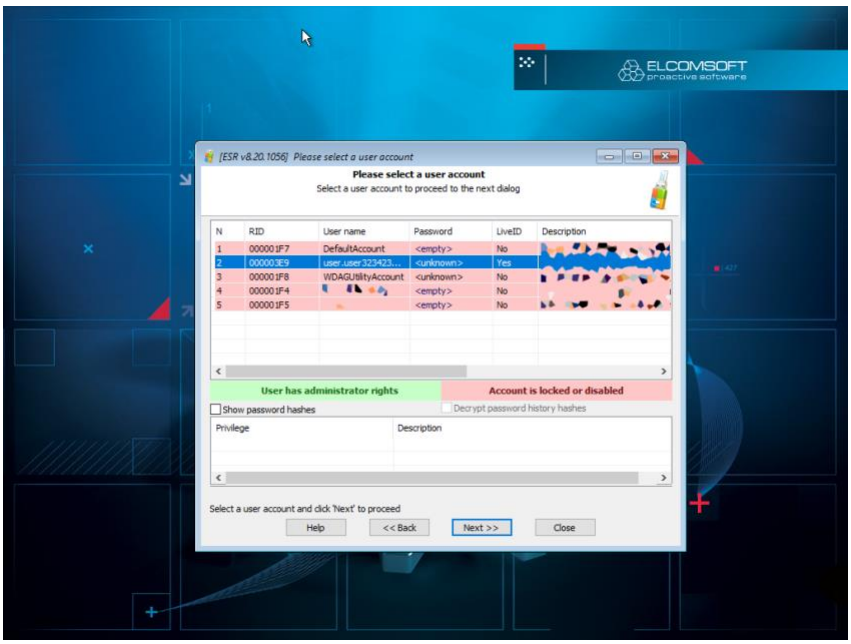
Чтобы разблокировать учётную запись Windows 11 с авторизацией без пароля, её необходимо сконвертировать в обычную локальную учётную запись с паролем, установив собственный пароль. Для этого нужно загрузить компьютер с USB-накопителя Elcomsoft System Recovery. Создать загрузочный накопитель Elcomsoft System Recovery можно, воспользовавшись инструкциями в статье Elcomsoft System Recovery: загрузочный накопитель для исследования компьютеров[90].

После загрузки Elcomsoft System Recovery необходимо выбрать стандартный режим работы (по умолчанию программа запускается в режиме "только для чтения", в котором запрещены любые модификации данных).

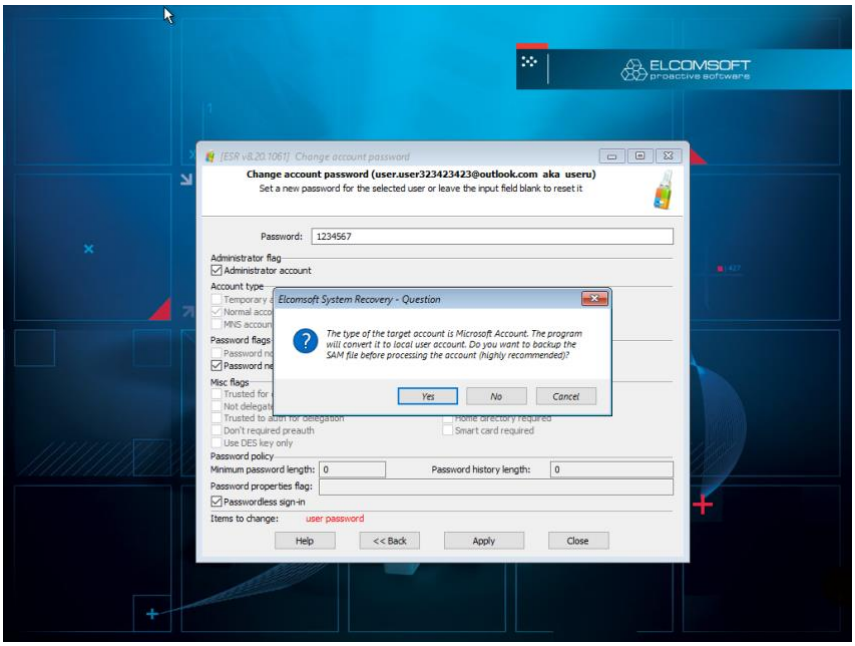
Для конвертации учётной записи Microsoft Account с авторизацией без пароля в обычную локальную учётную запись воспользуйтесь следующей инструкцией.

Выберите учётную запись для конвертации.

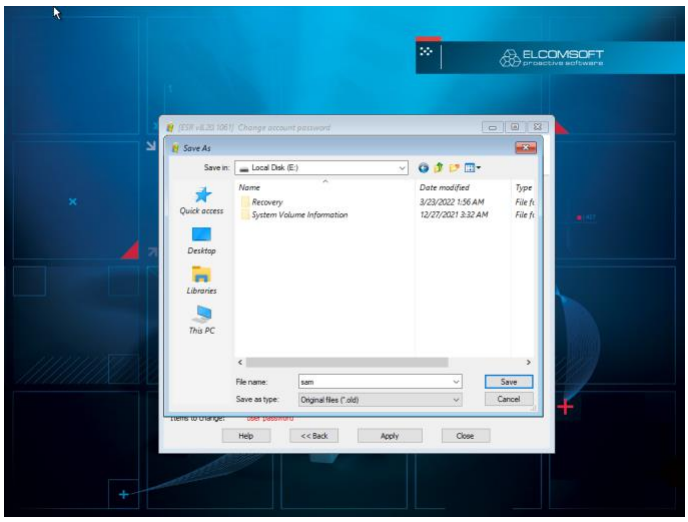
[90]https://blog.elcomsoft.ru/2020/11/elcomsoft-system-recovery-zagruzochnyj-nakopitel-dlya-issledovaniya-kompyuterov/



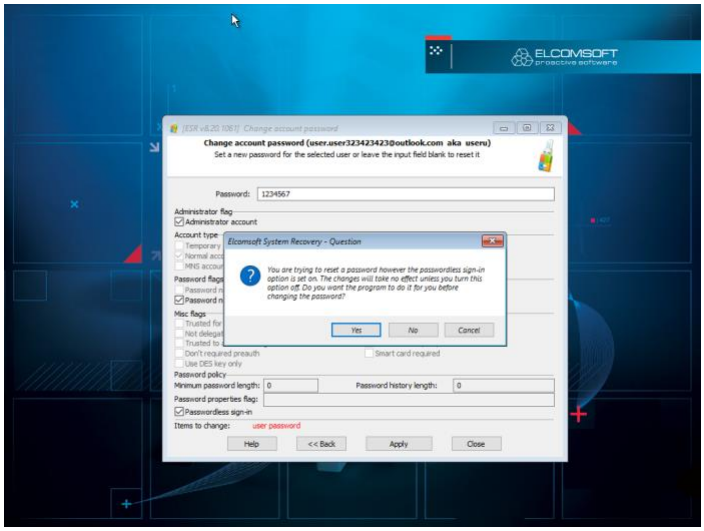
Укажите пароль, который будет установлен в учётной записи.



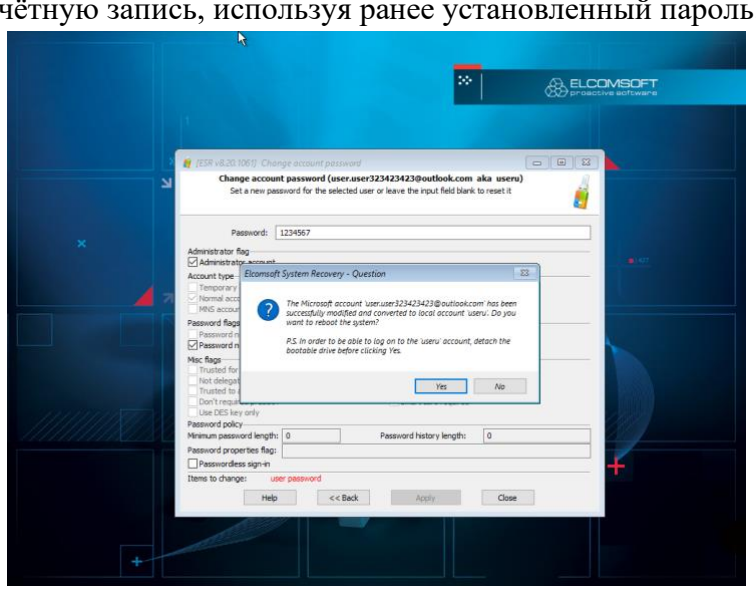
Не забудьте создать резервную копию оригинальной базы данных SAM.



Программа автоматически определит тип учётной записи с авторизацией без пароля и предложит удалить эту опцию. Вы не сможете продолжить конвертацию, если отклоните запрос.



Elcomsoft System Recovery уведомит о потенциальных последствиях конвертации (см. ниже) и внесёт изменения в базу данных SAM. После этого вы сможете загрузить компьютер в Windows и войти в учётную запись, используя ранее установленный пароль.



Обратите внимание: после конвертации учётной записи станут недоступными ключи и данные, защищённые DPAPI. Сюда входят пароли браузера Microsoft Edge, файлы и папки, зашифрованные в NTFS, и некоторые другие данные.

Подведём итог. Несмотря на бесчисленные копья, сломанные в спорах о явно завышенных системных требованиях Windows 11, разработчики Microsoft сделали шаг в верном направлении. Обязательное требование наличия TPM совместно с новым способом авторизации устраняют серьёзную уязвимость в механизме авторизации Windows при входе в учётную запись. В то же время мы не заметили изменений в политике шифрования Windows 11. На портативных устройствах всё так же используется BitLocker Device Encryption, а в настольных компьютерах шифрование по-прежнему остаётся опциональным; для доступа к зашифрованным данным всё так же используется депонированный в Microsoft Account ключ BitLocker Recovery Key.

25. Аудит безопасности беспроводных точек доступа

Современные беспроводные сети защищены от несанкционированного доступа по стандарту WPA/WPA2. Наиболее часто используемый метод защиты доступа к беспроводной сети — это заранее заданная парольная фраза, текстовый пароль. По стандарту WPA, минимальная длина пароля – 8 символов. С учётом этого атаки на данный тип паролей методом полного перебора сравнительно малоэффективны, даже если они выполняются в сети компьютеров с GPU-ускорением. В то же время пароли к беспроводным сетям регулярно компрометируются или «утекают» с различных устройств.

Elcomsoft Wireless Security Auditor позволяет проверить защищённость корпоративной сети Wi-Fi, её устойчивость к внешним и инсайдерским атакам. Встроенный перехватчик и анализатор беспроводного трафика и технология аппаратного ускорения с использованием вычислительных возможностей современных видеокарт позволяют симулировать атаку на беспроводную сеть с попыткой восстановления пароля WPA/WPA2-PSK. Попытка взлома пароля к сети Wi-Fi в течение заданного временного промежутка поможет определить степень устойчивости беспроводной сети к внешним атакам.

Принцип работы Elcomsoft Wireless Security Auditor – проверка безопасности беспроводной сети атакой на оригинальный текстовый пароль Wi-Fi. Работа Elcomsoft Wireless Security Auditor никак не отражается на обычном функционировании проверяемой беспроводной сети. Встроенный анализатор трафика перехватывает пакеты, которыми обмениваются точка доступа и устройства в момент их подключения к беспроводной сети, после чего приложение пытается восстановить сохраненные пароли WPA/WPA2-PSK. Возможен полностью офлайновый вариант атаки, при котором анализируется дамп сетевых сообщений в формате tcpdump, собранный сторонним приложением. Аудит проводится в рамках заданных временных ограничений. В случае, если в течение заданного времени подобрать пароль к беспроводной сети не удаётся, беспроводная сеть признаётся устойчивой к данному типу атак (что не отменяет необходимости проверки пароля на предмет его утечки).

25.1. Захват контрольного пакета WPA

Прежде всего, вам понадобится дамп ***«рукопожатия» (handshake)*** WPA/WPA2. Этот дамп представляет собой файл, который загружается в приложение для восстановления пароля. Чтобы перехватить нужный пакет, используйте встроенный в Elcomsoft Wireless Security Auditor сниффер Wi-Fi.

Традиционный подход к захвату рукопожатия WPA/WPA2 заключался в использовании специального беспроводного адаптера AirPCap и специального программного обеспечения. В нашем продукте поддерживаются адаптеры AirPCap, однако в большинстве случаев используется чисто программное решение для прослушивания Wi-Fi, которое работает с обычными адаптерами Wi-Fi.

Для того, чтобы обычные беспроводные адаптеры, встроенные в современные ноутбуки и настольные компьютеры, можно было использовать для перехвата отдельных пакетов, мы разработали специальный низкоуровневый драйвер NDIS. Драйвер доступен для 32-разрядных и 64-разрядных версий Windows, подписан цифровой подписью Microsoft и может быть установлен на все совместимые версии Windows. С его помощью вы сможете автоматически перехватывать трафик Wi-Fi и запустить атаку на выбранные сети.

Остановимся на моменте "рукопожатия" (handhske) подробнее. В процессе авторизации устройства в беспроводной сети участвует не один, а четыре пакета. Если подходить к вопросу формально, то нужно проводить анализ всех четырёх пакетов. Здесь, однако, **есть некоторые проблемы:**

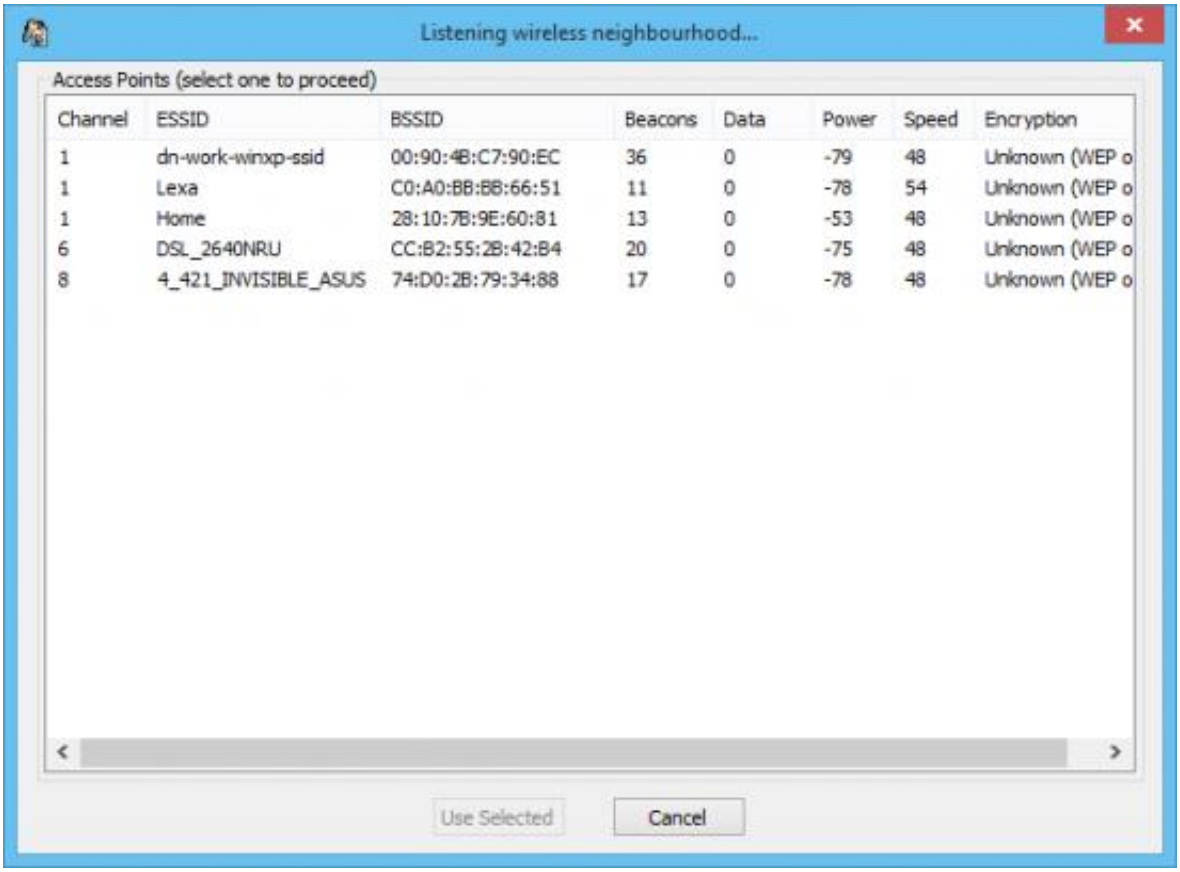
- пакеты могут идти вразнобой, т.е. ранее отправленные приходить позже;
- пакеты могут дублироваться с обновлёнными значениями;
- эти пакеты аутентификации могут перебиваться пакетами окончания сессии (часто они шлются со второго беспроводного устройства специально, с целью заставить клиент переподключиться).

В теории, хэш можно извлечь из двух пакетов, а не из четырёх, и именно таким образом устроен наш продукт. В то же время по описанным выше причинам хэш может формироваться некорректным. Время от времени нам задают вопрос: удалось подобрать пароль по хэндшейку, а он не подходит; почему? Как правило, дело в том, что устройство пыталось подключиться к точке доступа с неверным паролем. Представим ситуацию, когда пароль к точке доступа — "12345678", но какое-то устройство пытается подключиться к сети с паролем "0000000000". EWSA перехватывает пакеты рукопожатия с "0000000000", сформировал хэш, был запущен перебор и обнаружен пароль "0000000000". Но он неверный!

В новых версиях продукта была добавлена поддержка ещё одного формата — pmkid. В строгом смысле слова, это не является хэндшейком. В pmkid содержится верный хэш.

Технические ограничения: продукт поддерживает стандарты безопасности WPA/PSK и WPA2/PSK в сетях Wi-Fi до пятого поколения включительно (Wi-Fi 5 или 802.11ac). Поддерживаются только сети, работающие на частоте 2.4ГГц; сети, работающие на частоте 5ГГц, не поддерживаются.

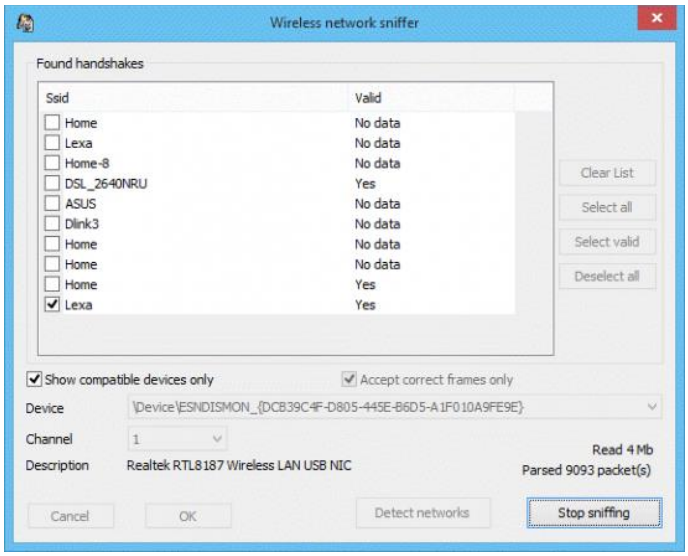
Обратите внимание: для работы системы необходимо установить драйвер WinPCap нашей разработки. Соответствующий драйвер WinPCap поставляется в составе Elcomsoft Wireless Security Auditor. Подробности – в руководстве Elcomsoft Wireless Security Auditor.



Наличие драйвера WinPCap не гарантирует поддержку всех без исключения беспроводных адаптеров Wi-Fi. Причин может быть несколько. В ряде случаев низкоуровневый драйвер устройства может не поддерживать режим мониторинга адаптера, либо режим мониторинга работает некорректно (к примеру, пакеты рукопожатий не регистрируются). Это не относится к специализированным адаптерам AirPCap, только к обычным адаптерам Wi-Fi, которые можно обнаружить в любом ноутбуке и во множестве современных настольных компьютеров. В ряде случаев для того, чтобы заработал режим мониторинга, достаточно установить другой драйвер либо обновить или переустановить имеющийся. Может помочь использование драйвера из набора драйверов системной логики, а не драйвера, который поставляет производитель адаптера, и наоборот. В то же время адаптеры, построенные на некоторых наборах системной логики, могут не работать в режиме мониторинга независимо от версии драйвера.

Посредством драйвера NDIS осуществляется перехват беспроводного трафика из всех сетей Wi-Fi, работающих на определённом канале Wi-Fi. Сразу после выбора сети Wi-Fi продукт начнёт отслеживать её трафик, ожидая подключения нового устройства. Как только новое устройство подключается к беспроводной сети, оно отправляет специальный пакет, содержащий хешированный пароль.

Данный пакет перехватывается, из него извлекается хэш пароля, после чего на этот хэш проводится атака для восстановления исходного пароля.



После захвата хэш-дампа вы можете запустить атаку на одном компьютере с помощью Elcomsoft Wireless Security Auditor или использовать Elcomsoft Distributed Password Recovery для распределённой атаки с аппаратным ускорением.

25.2. Продвинутые атаки

Минимально возможная длина пароля WPA – 8 символов, что делает прямой перебор малоэффективным. Elcomsoft Wireless Security Auditor поддерживает несколько видов продвинутых атак, позволяющих проверить слабые и часто используемые пароли.

Номера телефонов

В некоторых случаях (порядка 1-3% сетей) в качестве пароля к беспроводной сети используется номер телефона. Рекомендуем провести атаку по номерам телефонов: она не займёт много времени, но позволит установить слабые пароли.

Пароли, состоящие из одних цифр

Ещё один вид слабых паролей – пароли, состоящие из одних цифр. Рекомендуем провести атаку на пароли, составленные из 8 цифр. С учётом скорости перебора на современных видеокартах длительность такой атаки не превысит нескольких минут.

Утечки паролей

Пароли Wi-Fi выдаются многочисленным пользователям и используются на самых разнообразных устройствах, что делает их подверженными утечкам (например, Popular ‘WiFi Finder’ App Leaks 2 Million+ Passwords — Security Boulevard)[91]. В процессе аудита безопасности беспроводной сети обязательно проверьте актуальный пароль на предмет утечек.

Человеческий фактор

Пароли Wi-Fi предназначены для совместного использования. Часто эти пароли делаются лёгкими для запоминания и ввода, особенно на мобильных устройствах. В результате многие пароли основаны на комбинациях от одного до трех словарных слов, нескольких цифр и очень

[91] https://securityboulevard.com/2019/04/popular-wifi-finder-app-leaks-2-million-passwords/

небольшого количества специальных символов. Мы рекомендуем проверять стойкость паролей Wi-Fi с использованием автоматически настраиваемых словарных атак. Если беспроводная сеть может выдержать такую атаку в течение заданного периода времени, то пароль можно считать устойчивым по отношению к такому типу атак (что не отменяет необходимости проверки пароля на предмет утечки).

Полный перебор

Стандартом WPA/PSK установлена минимальная длина пароля в 8 символов. С учётом относительно невысокой скорости атаки полный перебор паролей даже минимально допустимой длины является практически невозможной задачей.

Пароль, состоящий из восьми знаков латинского алфавита (заглавные и прописные буквы) и включающий цифры и специальные символы, содержит 6,634,204,312,890,625 возможных комбинаций. На карте NVIDIA Tesla V100 скорость перебора паролей WPA/WPA2 составляет порядка 650,000 паролей в секунду; требуемое время на перебор всего пространства паролей – порядка 323 лет. Это время можно сократить, использовав более современные ускорители или подключив дополнительные вычислительные ресурсы (например, в виде распределённых атак в Elcomsoft Distributed Password Recovery), однако такая задача лишена практического смысла.

26. Заключение

В нашем пособии «Методическое руководство по восстановлению паролей и расшифровке данных» мы постарались рассказать об основных способах, подходах и методах, которые могут быть использованы сотрудниками правоохранительных органов и специалистами по информационной безопасности для того, чтобы получить доступ к зашифрованной информации. Мы постарались избежать превращения этого пособия в сборник технической документации к продуктам нашей компании, сосредоточившись на целях, подходах и методах их достижения. В то же время для иллюстрации практической реализации описанных подходов мы использовали продукты нашей собственной разработки – ведь именно их возможности мы знаем досконально. Надеемся, что это пособие окажется полезным читателю!

О компании

Компания «ЭлкомСофт» основана в 1990 году в Москве. С 1997 года ЭлкомСофт специализируется на разработке решений в сфере информационной безопасности и цифровой криминалистики.

Решения для цифровой и мобильной криминалистики

В компании «ЭлкомСофт» разработана полноценная линейка продуктов для извлечения информации из ряда мобильных устройств и получения доступа к зашифрованной информации, хранящейся как в мобильных устройствах, так и на персональных компьютерах. В состав линейки продуктов «ЭлкомСофт» как программы для восстановления доступа к определённым типам данных (например, документам Adobe PDF, Microsoft Office всех версий, Lotus Notes, Quicken, архивам ZIP и RAR, криптоконтейнерам BitLocker, PGP и TrueCrypt), так и корпоративные решения «всё в одном», позволяющие организовать масштабный перебор паролей с использованием всех ресурсов распределённой вычислительной сети. В ряде случаев доступ к зашифрованным данным может быть получен мгновенно путём извлечения ключа шифрования непосредственно из оперативной памяти исследуемого компьютера.

Продукты ЭлкомСофт зарегистрированы в Едином реестре российских программ для электронных вычислительных машин и баз данных с присвоением класса программного обеспечения, к которому относятся «Средства обеспечения информационной безопасности, Информационные системы для решения специфических отраслевых задач», «Программное обеспечение, обеспечивающее выполнение установленных действий при проведении оперативно-розыскных мероприятий».

- Elcomsoft Premium Forensic Bundle, **№11766 от 18.10.2021**
- Elcomsoft Desktop Forensic Bundle, **№11768 от 18.10.2021**
- Elcomsoft Password Recovery Bundle, **№6446 от 07.04.2020**
- Elcomsoft Mobile Forensic Bundle, **№7320 от 30.11.2020**
- Elcomsoft iOS Forensic Toolkit, **№7361 от 30.11.2020**
- Elcomsoft Distributed Password Recovery, **№11632 от 28.09.2021**

Контакты

сайт: **www.elcomsoft.ru**

блог: **blog.elcomsoft.ru**

электронная почта: **info@elcomsoft.com**