BEHOLDERISHERE

ШПАРГАЛКИ ЦИФРОВОГО ДЕТЕКТИВА.

ЧТО И ГДЕ ИСКАТЬ.

Краткий путеводитель по расположению цифровых артефактов в компьютерах и смартфонах.

T.ME/FORENSICTOOLS

Версия 0.7

январь 2024 г.

Оглавление

Раздел 1.

КРИМИНАЛИСТИЧЕСКИЕ АРТЕФАКТЫ WINDOWS

1. ИНФОРМАЦИЯ О УЧЕТНЫХ ЗАПИСЯХ

1.1. Последний вход в систему

Описание:
Перечисляет локальные учетные записи системы и их эквивалентные идентификаторы безопасности.

Расположение:

- C:\windows\system32\config\SAM
- SAM\Domains\Account\Users

Примечания:
В разделе реестра будет сохранено только время последнего входа в систему.

1.2. Последнее изменение пароля

Описание:
Отображает время последнего изменения пароля конкретного локального пользователя

Расположение:

- C:\windows\system32\config\SAM
- SAM\Domains\Account\Users

Примечания:
В разделе реестра будет сохранено только время последней смены пароля

1.3. Использование RDP

Описание:
Отслеживание входов в систему по протоколу удаленного рабочего стола на целевых компьютерах.

Расположение:
%SYSTEM ROOT%\System32\winevt\logs\Security.evtx

Примечания:

- Описание идентификаторов:
  - Event ID 4778 – Сеанс подключен/переподключен
  - Event ID 4779 – Сеанс отключен
- В журнале событий указаны имя хоста и IP-адрес удаленной машины, осуществляющей подключение
- На рабочих станциях вы часто будете видеть отключенный текущий сеанс консоли (4779), за которым следует подключение по протоколу RDP (4778)

1.4. Журнал запущенных сервисов

Описание:

- Анализ журналов на наличие подозрительных служб, запущенных во время загрузки
- Проверка служб, запущенных или остановленных примерно во время предполагаемого взлома

Расположение:
Все Event ID ссылаются на System Log

- 7034 – Служба неожиданно завершила работу
- 7035 – Служба отправила команду запуска/остановки
- 7036 – Служба запущена или остановлена
- 7040 – Изменен тип запуска (Загрузка | По запросу | Отключена)
- 7045 – В системе установлена служба (Win2008R2+)
- 4697 – В системе установлена служба (из журнала безопасности)
-

Примечания:

- Все Event ID, кроме 4697 ссылаются System Log
- Большое количество вредоносного ПО, запускается именно в виде Сервисов
- Сервисы могут неожиданно заканчивать свою работу из-за таких атак, как например process injection

1.5. Типы входа в систему

Описание:
Logon Events может дать нам конкретную информацию о характере авторизации учетной записи в системе. В дополнение к информации о даты, времени, имени пользователя, имени хоста и
статуса успешного/неудачного входа в систему анализ Logon Events так же позволит нам точно определить, с помощью каких средств была предпринята попытка входа в систему.

Расположение:
Event ID 4624

Примечания:
Типы входа и их описание:

- 2 Вход через консоль
- 3 Вход в сеть
- 4 Пакетный вход в систему
- 5 Вход в службу Windows
- 7 Учетные данные, используемые для разблокировки экрана
- 8 Учетные данные для отправки сетевого входа (открытый текст)
- 9 Используются учетные данные, отличные от зарегистрированного пользователя
- 10 Удаленный интерактивный вход в систему (RDP)
- 11 Кэшированные учетные данные, используемые для входа в систему
- 12 Кэшированные удаленные интерактивные данные (аналогично типу 10)
- 13 Кэшированная разблокировка (аналогично типу 7)

1.6. События аутентификации

Описание:
Механизмы аутентификации

Расположение:

- Запись расположена в системе, которая аутентифицировала учетные данные
    - Local Account/Workgroup - на самой рабочей станции
    - Domain/Active Directory - на контроллере домена

%SYSTEM ROOT%\System32\winevt\logs\Security.evtx

Примечания:

- Event ID (протокол NTLM)
    - 4776 - Успешная/неудачная аутентификация учетной записи.
- Event ID (протокол Kerberos)
    - 4768 - Выдача билета Билет был выдан (успешный вход в систему)
    - 4769 - Запрошен запрос на обслуживание (доступ к ресурсу сервера)
    - 4771 - Не удалось выполнить предварительную аутентификацию (неудачный вход в систему)

1.7. Выполненный/Неудачный вход в систему

Описание:
Определение, какие учетные записи использовались для попыток входа в систему. Отслеживание использование учетной записи для известных скомпрометированных учетных записей.

Расположение:
%system root%\System32\winevt\logs\Security.evtx

Примечания:
Описание Event ID:

- 4624 – Успешный вход в систему
- 4625 – Неудачный вход в систему
- 4634 или 4647 – Успешный выход из системы
- 4648 – Вход с использованием явных учетных данных (Run as)
- 4672 – Вход в учетную запись с правами суперпользователя (Администратора)
- 4720 – Создана учетная запись.

2. ДЕЙСТВИЯ С ФАЙЛАМИ И ПАПКАМИ

2.1. Открытие/Сохранение MRU

Описание:
MRU отслеживает файлы которые были открыты или сохранены через диалоговое окно Windows. Это достаточно большой набор данных и определенного контекста, который затрагивает как часто используемые сторонние приложения, так и встроенные приложения операционной системы.

Расположение:
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePIDlMRU

Примечания:

- Раздел «*» – отслеживает файлы с любым расширением, введенным в открытом диалоговом окне сохранения
- Раздел «.???» (где ??? - трехбуквенное расширение) –информация о файлах из открытого диалогового окна сохранения с определенным расширением.

2.2. Недавние файлы

Описание:
Раздел реестра, который отслеживает последние открытые файлы и папки. Используется для заполнения данных в меню «Недавние» меню «Пуск».

Расположение:
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

Примечания:

- **RecentDocs** – Общий раздел, в котором находятся последних 150 открытых файлов или папок. Список MRU будет отсортирован по времени открытия файлов или папки, в котором был открыт каждый файл/ папка.
- **.???** – В этом разделе хранятся последние файлы с определенным расширением, которые были открыты.
- **Folder** – в этом подразделе хранятся последние открытые папки.

2.3. Доступ к папкам

Описание:
Показывает к каким папкам был осуществлен доступ на локальном компьютере, в сети и/или на съемных устройствах. Содержит как данные о ранее существовавших папках после удаления/перезаписи, так и когда был осуществлен доступ к определенным папкам.

Расположение:

- Explorer Access:
    - USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\Bags
    - USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\BagMRU
- Desktop Access:
    - NTUSER.DAT\Software\Microsoft\Windows\Shell\BagMRU
    - NTUSER.DAT\Software\Microsoft\Windows\Shell\Bags
    -

Примечания:
Хранит информацию о том, какие папки были просмотрены пользователем в последний раз.

2.4. Ярлыки файлова (*lnk)

Описание:
Файлы ярлыков автоматически создаются операционной системой в разделе «Недавние», а также в качестве ссылок на документы без факта их копирования самими пользователями.

Расположение:

- %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\
- %USERPROFILE%\AppData\Roaming\Microsoft\Office\Recent\
-

Примечания:

- Свойства файла с расширением *lnk
    - Время изменения, доступа и создания целевого файла
    - Информация об объеме (имя, тип, серийный номер)
    - Информация о сетевом ресурсе
    - Исходное местоположение
    - Наименование системы
- Дата/время, когда файл с таким названием был открыт впервые
    - Дата создания файла быстрого доступа (LNK)

- Дата/время, когда файл с таким именем был открыт в последний раз
    - Дата последнего изменения файла быстрого доступа (LNK)

2.5. Диспетчер кэша

Описание:
- Повышает производительность системы за счет предварительной загрузки кода часто используемых приложений. Диспетчер кэша отслеживает все файлы и каталоги, на которые ссылается каждое приложение или процесс и отображает их в файл *.pf
- Ограничено 1024 файлами в Win8-11
- Именуется (exename)-(хэш).pf

Расположение:
C:\Windows\Prefetch

Примечания:
Каждый файл .pf может содержать дескрипторы файлов и дескрипторы устройств.

2.6. Последний просмотр MRU

Описание:
Показывает конкретный исполняемый файл, используемый приложением для открытия файлов, в разделе OpenSaveMRU. Кроме того, каждое значение также показывает местоположение каталога для последнего файла, к которому было обращено это приложение.

Расположение:
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU

Примечания:
Отслеживает исполняемые файлы приложения, используемые для открытия файлов в OpenSaveMRU, и последний использованный путь к файлу.

2.7. Файлы открываемые IE/Edge

Описание:
Нативный браузер хранит не только истории посещения сайтов, но и истории открытия некоторых видов файлов.

Расположение:
%USERPROFILE%\AppData\Local\Microsoft\Windows\WebCache\WebCacheV*.dat

Примечания:
Хранит в index.dat информацию в виде file://C:/directory/filename.ext

2.8. Недавние файлы MS Office

Описание:
Программы MS Office будут вести свой собственный список недавних файлов чтобы пользователям было легче запомнить последние файлы, который они редактировали.

Расположение:
NTUSER.DAT\Software\Microsoft\Office\VERSION
- VERSION – версия пакета MS OFFICE

NTUSER.DAT\Software\Microsoft\Office\VERSION\UserMRU\LiveID_####\FileMRU
- VERSION = 15.0 для облачного Office365
- LiveID_#### - идентификатор сетевой учетной записи Microsoft
-

Примечания:
Аналогично разделу «Недавние», позволяет отслеживать последние файлы, которые были открыты одним из приложений MS Office. Последней добавленной записью, согласно MRU, будет время последнего открытия файла конкретным приложением MS Office.

3. УДАЛЕННЫЕ ФАЙЛЫ ИЛИ ИНФОРМАЦИЯ О НИХ

3.1. Кэш миниатюр

Описание:
Миниатюры изображений, офисных документов и папок хранятся в базе данных, называемой thumbcache. У каждого пользователя - своя собственная база миниатюр с размером выбранным ранее самим пользователем.

Расположение:
C:\%USERPROFILE%\AppData\Local\Microsoft\Windows\Explorer

Примечания:

- Миниатюры создаются, когда пользователь переключает папку в режим миниатюр или просматривает изображения с помощью слайд-шоу. При этом все просматриваемые из системы файлы сохраняются в отдельную базу данных. Windows использует 4 размера для миниатюр, и файлы в папке кэша отражают это:
  - 32 - маленький
  - 96 - средний
  - 256 - большой
  - 1024 - очень большой
- Файл thumbcache сохранит уменьшенную копию изображения на основе размера миниатюры в содержимом соответствующего файла базы данных.

3.2. Thumbs.db

Описание:
Скрытый файл в каталоге, где находятся изображения, сохраненные в виде уменьшенных графических изображений. thumbs.db каталогизирует изображения в папке и сохраняет копию миниатюры, даже если изображения были удалены.

Расположение:
Автоматически создается в любом месте, где есть файлы документов или изображений.

Примечания:
Содержит в себе:
- Уменьшенное изображение исходного изображения
- Уменьшенное изображение документа – даже если оно удалено

3.3. Файлы открываемые IE/Edge

Описание:
Нативный браузер хранит не только истории посещения сайтов, но и истории открытия некоторых видов файлов. Даже если файл был удален, ссылка на него может остаться в кэше.

Расположение:
%USERPROFILE%\AppData\Local\Microsoft\Windows\WebCache\WebCacheV*.dat

Примечания:
Хранит в index.dat информацию в виде file://C:/directory/filename.ext

3.4. Поиск – история запросов.

Описание:
Слова, используемые в меню «ПОИСК» на панели задач или в меню «СТАРТ» (win 7/8).

Расположение:
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery

Примечания:
Ключевые слова добавляются в Юникоде и сортируются по дате и времени в списке MRU

3.5. Корзина.

Описание:
Корзина является очень важным местом в файловой системе Windows. Ее анализ может помочь вам при проведении криминалистического исследования, поскольку практически важный файл после удаления попадает именно туда.

Расположение:
Скрытая системная папка
C:\$Recycle.bin

  - Время удаления и исходное имя файла содержатся в отдельных файлах для каждого удаленного файла.

○

Примечания:

- SID может быть сопоставлен пользователю с помощью анализа реестра
- Файлы, перед которыми стоит $I###### файлы содержат:
    - Исходный ПУТЬ и имя
    - Дата/время удаления
- Файлы, перед которыми стоит $R####### файлы содержат
    - Данные необходимые для восстановления.

3.6. Последний просмотр MRU

Описание:
Показывает конкретный исполняемый файл, используемый приложением для открытия
файлов, в разделе OpenSaveMRU. Кроме того, каждое значение также показывает местоположение каталога для последнего файла, к которому было обращено это приложение.
Пример: Notepad.exe последний раз запускался с использованием папки C:\%USERPROFILE%\Desktop

Расположение:
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU

Примечания:
Отслеживает исполняемые файлы приложения, используемые для открытия файлов в OpenSaveMRU, и последний использованный путь к файлу.

4. СРЕДА ВЫПОЛНЕНИЯ ПРОГРАММ

4.1. UserAssist

Описание:
Программы, использующие графический интерфейс, отслеживаются в момент запуска в операционной системе.

Расположение:
NTUSER.DAT\Software\Microsoft\Windows\Currentversion\Explorer\UserAssist\{GUID}\Count

Примечания:
Все значения представлены в ROT-13

- CEBFF5CD – выполнение исполняемого файла
- F4E57C4B – выполнение через ярлык приложения

4.2. Windows 10 TimeLine / Activities (Win11)

Описание:
Win 10 записывает недавно использованные приложения и файлы на “TimeLine”, доступной с помощью клавиши “WIN+TAB”. В Win 11 используется для фиксации запущенных приложений. Данные записываются в базу данных SQLite.

Расположение:
%userprofile%\AppData\Local\ConnectedDevicesPlatform\<любое имя файла>\ActivitiesCache.db

Примечания:
Фиксируются:
Выполняемые приложения
Количество фокусировок (вызовов) для каждого окна приложения.

4.3. BAM/DAM

Описание:
Модератор фоновой активности Windows (BAM) Windows Background Activity Moderator

Расположение:

- SYSTEM\CurrentControlSet\Services\bam\UserSettings\{SID}
- SYSTEM\CurrentControlSet\Services\dam\UserSettings\{SID}

Примечания:
Предоставляет полный путь к исполняемому файлу, который был запущен в системе, и дату/время последнего запуска.

4.4. Кэш базы совместимости программ

Описание:

• База данных совместимости приложений Windows используется Windows для выявления возможных проблем совместимости приложений.
• Отслеживает имя исполняемого файла, размер файла, время последнего изменения.

Расположение:

SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache

Примечания:

В этой ветке реестра можно найти любой исполняемый файл, запущенный в системе Windows. Вы можете использовать это для идентификации систем, на которых могла быть запущено конкретное вредоносное ПО. Кроме того, отслеживая временные параметры, вы сможете определить время последнего запуска или его активности в системе.

4.5. Amcache.hve

Описание:

ProgramDataUpdater (задача, связанная с приложением Experience Service) использует файл реестра Amcache.hve для хранения данных во время создания процесса

Расположение:

C:\Windows\AppCompat\Programs\Amcache.hve

Примечания:

• Amcache.hve - Keys = Amcache.hve\Root\File\{Идентификатор тома}\#######
• Запись для каждого запуска запускаемого файла, в которой содержится информация о полном пути, стандартная информация о время последнего изменения файла и том диска, с которого был запущен исполняемый файл.
• Время первого запуска = Время последнего изменения ключа.
• Хэш SHA1 исполняемого файла, также содержащийся в ключе.

4.6. Монитор системных ресурсов (SRUM)

Описание:

Записывает данные о производительности системы за период от 30 до 60 дней. Запущенные приложения, учетная запись пользователя, из-под которых запускались приложения и количество байт, отправленные/полученные для каждого приложения в час.

Расположение:

SOFTWARE\Microsoft\WindowsNT\CurrentVersion\SRUM\Extensions {d10ca2fe-6fcf4f6d-848e-b2e99266fa89} = Application Resource Usage Provider C:\Windows\ System32\SRU\

Примечания:

Используйте такой инструмент, как srum_dump.exe (github.com/MarkBaggett/srum-dump), для перекрестной корреляции данных между разделами реестра и базой данных SERUM ESE.

4.7. Список быстрых переходов

Описание:

- Панель задач Windows (список переходов) спроектирована таким образом, чтобы пользователи могли быстро и легко получать доступ к элементам, которые они часто или недавно использовали.
- К данным, хранящимся в папке AutomaticDestinations, будет добавлен файл с идентификатором AppID соответствующего приложения.

Расположение:

%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations

Примечания:

- Время первого запуска приложения.
    - Время создания = Время первого добавления элемента в файл AppID.
- Время последнего выполнения приложения без открытия файла.
    - Время модификации = время последнего добавления элемента в файл AppID.
- Список идентификаторов списка переходов находится тут: https://dfir.to/EZJumpListПО.

4.8. Последний просмотр MRU

Описание:
Показывает конкретный исполняемый файл, используемый приложением для открытия файлов, в разделе OpenSaveMRU. Кроме того, каждое значение также показывает местоположение каталога для последнего файла, к которому было обращено это приложение.
Пример: Notepad.exe последний раз запускался с использованием папки C:\%USERPROFILE%\Desktop

Расположение:
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU

Примечания:
Отслеживает исполняемые файлы приложения, используемые для открытия файлов в OpenSaveMRU, и последний использованный путь к файлу.

4.9. Диспетчер кэша

Описание:

- Повышает производительность системы за счет предварительной загрузки кода часто используемых приложений. Диспетчер кэша отслеживает все файлы и каталоги, на которые ссылается каждое приложение или процесс и отображает их в файл *.pf
- Ограничено 1024 файлами в Win8-11
- Именуется (exename)-(хэш).pf

Расположение:
C:\Windows\Prefetch

Примечания:
Каждый файл .pf может содержать дескрипторы файлов и дескрипторы устройств.

5. СКАЧЕННЫЕ ФАЙЛЫ

5.1. Открытие/Сохранение MRU

Описание:
MRU отслеживает файлы которые были открыты или сохранены через диалоговое окно Windows. Это достаточно большой набор данных и определенного контекста, который затрагивает как часто используемые сторонние приложения, так и встроенные приложения операционной системы.

Расположение:
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePIDlMRU

Примечания:

- Раздел «*» – отслеживает файлы с любым расширением, введенным в открытом диалоговом окне сохранения
- Раздел «.???» (где ??? - трехбуквенное расширение) –информация о файлах из открытого диалогового окна сохранения с определенным расширением.

5.2. Почтовые вложения

Описание:
80% важных данных электронной почты хранится именно во вложениях, Так как стандарты электронной почты допускают только текст. Вложения закодированы в формате MIME/base64.

Расположение:
%USERPROFILE%\AppData\Local\Microsoft\Outlook

Примечания:
Файлы с данными MS Outlook, имеют расширения OST и PST.
Для их просмотра можно воспользоваться следующими программами:

- OST Viewer утилита для просмотра файлов OST Outlook без сервера Exchange.
- PST Viewer утилита для просмотра файлов PST Outlook без сервера Exchange.

5.3. История Skype

Описание:

История Skype сохраняется в журнал сеансов чата и скаченных файлов. Этот функционал обычно включён по умолчанию при установке.

Расположение:

%USERPROFILE%\AppData\Roaming\Skype\

Примечания:

Каждая запись будет содержать значение даты/времени и имя пользователя Skype, связанное с сеансом связи.

5.4. Скаченное из браузера

Описание:

Интернет-браузеры имеют свои менеджеры закачек, которые хранят историю каждого загруженного пользователем файла.

Расположение:

- CHROME:
  - %userprofile%\AppData\Local\Google\Chrome\User Data\Default\History
  - %userprofile%\AppData\Local\Google\Chrome\User Data\ChromeDefaultData\History
- EDGE:
  - %userprofile%\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat
- FIREFOX:
  - %userprofile%\AppData\Roaming\Mozilla\Firefox\Profiles\[profileID].default\downloads.sqlite

Примечания:

При загрузке будут указаны:

- Имя файла, размер и тип
- Веб-страница и ссылка на нее
- Местоположение сохраненного файла
- Приложение, используемое для открытия файла
- Время начала и окончания загрузки

5.5. История Microsoft Teams

Описание:

Средство для конференций Microsoft Teams является основным нативным приложением для командной работы в Windows. Большую часть логов Microsoft Teams хранит в облаке.

Расположение:

- Журнал собраний и звонков
  - **MS Teams 1.x (win10)** - %USERPROFILE%\AppData\Roaming\Microsoft\Teams\IndexedDB<url>.indexeddb.leveldb
  - **MS Teams 2.x (win11)** – %USERPROFILE%\AppData\Local\Packages\MicrosoftTeams_8wekyb3d8bbwe\LocalCache\Microsoft\MSTeams\EBWebView\Default\IndexedDB
- Скачанные файлы
  - C:\%USERPROFILE%\Downloads\Teams

Примечания:

Лог файлы хранятся в формате JSON. Для извлечения можно воспользоваться ms_teams_parser (https://github.com/lxndrblz/forensicsim)

6. СЕТЕВАЯ АКТИВНОСТЬ/ФИЗИЧЕСКОЕ МЕСТОПОЛОЖЕНИЕ

6.1. Временная зона

Описание:

Определяет текущий системный часовой пояс.

Расположение:

SYSTEM\CurrentControlSet\Control\TimeZoneInformation

Примечания:

- Время активности невероятно полезно для корреляции активности.

- Внутренние файлы журналов и метки даты/времени будут основаны на информации о системном часовом поясе.
- У вас могут быть другие сетевые устройства, и вам потребуется сопоставить информацию с информацией о часовом поясе.

6.2. Cookies

Описание:
Файлы cookie дают представление о том, какие веб-сайты были посещены и какие действия там могли происходить

Расположение:

- EDGE:
    - %userprofile%\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat
- FIREFOX:
    - %userprofile%\AppData\Roaming\Mozilla\Firefox\Profiles\[profileID].default\cookies.sqlite
- CHROME:
    - %userprofile%\AppData\Local\Google\Chrome\User Data\Default\Cookies
    - %userprofile%\AppData\Local\Google\Chrome\User Data\ChromeDefaultData\Cookies

Примечания:

- Все данные хранятся в виде баз данных. Для просмотра используйте:
- DB Browser for SQLite https://sqlitebrowser.org/ - Просмотрщик SQLite
- ESEDatabaseView https://www.nirsoft.net/utils/ese_database_view.html - Просмотрщик ESE

6.3. История сетевых подключений

Описание:
Определите сети, к которым был подключен компьютер

- Сети могут быть беспроводными или проводными
- Определите доменное имя/название интрасети
- Определите SSID
- Определите MAC-адрес шлюза

Расположение:

- SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged
- SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Managed
- SOFTWARE\Microsoft\WindowsNT\CurrentVersion\NetworkList\Nla\Cache

Примечания:

- Вы можете не только определить имя внутренней сети, но и определить время последнего подключения к ней на основе времени последней записи в реестре
- Здесь также будут перечислены все сети, к которым было подключение через VPN
- MAC-адрес SSID для шлюза может быть локализован через сервисы типа Shodan

6.4. Журнал событий WLAN

Описание:
Определите, к каким беспроводным сетям подключался компьютер, определите характеристики сети чтобы определить местоположение

Расположение:
Microsoft-Windows-WLAN-AutoConfig Operational.evtx

Примечания:

- Показывает историю подключений к беспроводной сети
- Содержит SSID и BSSID (MAC-адрес), которые можно использовать для геолокации точки доступа.
- Соответствующие Event ID:
    - 11000 – Запущено подключение к беспроводной сети
    - 8001 – Успешное подключение к беспроводной сети
    - 8002 – Сбой подключения к беспроводной сети
    - 8003 – Отключение от беспроводной сети
    - 6100 – Диагностика сети (системный журнал)

6.5. История поисковых запросов

Описание:

История посещений веб-сайтов по дате и времени. Информация сохраняется для каждой учетной записи локального пользователя. Фиксируется количество посещений и их периодичность. Также отслеживается доступ к локальным системным файлам. Это также будет включать в себя историю поиска веб-сайта по поисковым запросам в поисковых системах.

Расположение:

- EDGE:
    - %userprofile%\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat
- FIREFOX:
    - %userprofile%\AppData\Roaming\Mozilla\Firefox\ Profiles\.default\places.sqlite
- CHROME:
    - %userprofile%\AppData\Local\Google\Chrome\User Data\Default\History
    - %userprofile%\AppData\Local\Google\Chrome\User Data\ChromeDefaultData\History

Примечания:

-

7. ИСПОЛЬЗОВАНИЕ USB ИНТЕРФЕЙСОВ

7.1. Идентификация устройств

Описание:

Отслеживание usb устройств подключаемых к компьютеру

Расположение:

- SYSTEM\CurrentControlSet\Enum\USBSTOR
- SYSTEM\CurrentControlSet\Enum\USB

Примечания:

- Определите вендора, продукт и версию USB-устройства, подключенного к компьютеру
- Определите уникальное USB-устройство, подключенное к компьютеру
- Определите время, когда устройство было подключено к компьютеру
- Устройства, у которых нет уникального серийного номера, будут иметь символ “&” во втором символе серийного номера.

7.2. Время подключения/отключения

Описание:

Определите временный рамки использования USB-устройств, подключенных к компьютеру.

Расположение:

- C:\Windows\inf\setupapi.dev.log
- SYSTEM\CurrentControlSet\Enum\USBSTOR\Ven_Prod_Version\USBSerial#\Properties\ {83da6326-97a6-4088-9453-a19231573b29}\####

Примечания:

- Для лог-файла:
    - Поиск серийного номера устройства
    - Время в файле журнала указано в местном часовом поясе
- Event ID для ветки реестра:
    - 0064 = Первая установка (для Win7-11)
    - 0066 = Последнее подключение (для Win8-11)
    - 0067 = Последнее удаление (для Win8-11)

7.3. Пользователь

Описание:

Найдите пользователя, который использовал уникальное USB-устройство.

Расположение:

- Найдите GUID в SYSTEM\MountedDevices
- NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2

Примечания:

Далее этон GUID будет использован для идентификации пользователя, подключившего устройство. Время последней записи этого ключа реестра будет последнему факту подключению устройства к компьютеру этим пользователем. Ссылка на этот номер будет указана в личном ключе точек монтирования пользователя в ветке реестра NTUSER.DAT.

7.4. Журнал событий Plug and Play

Описание:

При попытке установки драйвера Plug and Play служба создает событие с идентификатором 20001 и выдает статус в рамках этого события. Важно отметить, что это событие сработает для любого устройства с поддержкой Plug and Play, включая устройствами USB, Firewire и т.п.

Расположение:

- Найдите GUID в SYSTEM\MountedDevices
- NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2

Примечания:

Event ID 20001 – попытка установки драйвера PnP
    - Временная метка
    - Информация об устройстве
    - Серийный номер устройства
    - Статус (0 если ошибок нет)

7.5. Серийный номер тома

Описание:

Найдите серийный номер тома раздела файловой системы на USB диске или флешке.

Расположение:

- SOFTWARE\Microsoft\WindowsNT\CurrentVersion\ENDMgmt

Используйте Volume Name и USB Serial Number для того, чтобы найти последнее целое число в строке и преобразовать десятеричный серийный номер в шестнадцатеричный.

Примечания:

- Файл ярлыка (LNK) содержит серийный номер и название тома
- Раздел реестра RecentDocs в большинстве случаев будет содержать имя тома при открытии USB-устройства с помощью проводника.

7.6. Буква диска и имя тома

Описание:

Найдите букву диска USB накопителя, когда оно было подключено к компьютеру в последний раз.

Расположение:

- SOFTWARE\Microsoft\Windows Portable Devices\Devices
- SYSTEM\MountedDevices

Изучите буквы дисков, просматривая данные о значениях, в поисках серийного номера

Примечания:

Определите USB-устройство, которое в последний раз было подключено с использование определенной буквой диска. Обратите внимание что, этот метод будет работать только для последнего подключенного диска. Он не содержит записей о каждой букве диска, подключенной к съемному диску.

7.7. Ярлыки файлов и носителей

Описание:

Файлы ярлыков автоматически создаются операционной системой в разделе «Недавние», а также в качестве ссылок на документы без факта их копирования самими пользователями.

Расположение:

- %USERPROFILE%\AppData\Roaming\Microsoft\Windows\ Recent
- %USERPROFILE%\AppData\Roaming\Microsoft\Office\Recent

Примечания:

- Свойства файла с расширением *lnk
    - Время изменения, доступа и создания целевого файла

    - Информация об объеме (имя, тип, серийный номер)
    - Информация о сетевом ресурсе
    - Исходное местоположение
    - Наименование системы
- Дата/время, когда файл с таким названием был открыт впервые
    - Дата создания файла быстрого доступа (LNK)
- Дата/время, когда файл с таким именем был открыт в последний раз
    - Дата последнего изменения файла быстрого доступа (LNK)

8. ИСПОЛЬЗОВАНИЕ ИНТЕРНЕТ-БРАУЗЕРОВ

8.1. История

Описание:
История посещений веб-сайтов по дате и времени. Информация сохраняется для каждой учетной записи локального пользователя. Фиксируется количество посещений и их периодичность. Также отслеживается доступ к локальным системным файлам. Это также будет включать в себя историю поиска веб-сайта по поисковым запросам в поисковых системах.

Расположение:
- EDGE:
    - %userprofile%\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat
- FIREFOX:
    - %userprofile%\AppData\Roaming\Mozilla\Firefox\ Profiles\.default\places.sqlite
- CHROME:
    - %userprofile%\AppData\Local\Google\Chrome\User Data\Default\History
    - %userprofile%\AppData\Local\Google\Chrome\User Data\ChromeDefaultData\History

Примечания:
-

8.2. Cookies

Описание:
Файлы cookie дают представление о том, какие веб-сайты были посещены и какие действия там могли происходить

Расположение:
- EDGE:
    - %userprofile%\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat
- FIREFOX:
    - %userprofile%\AppData\Roaming\Mozilla\Firefox\Profiles\[profileID].default\cookies.sqlite
- CHROME:
    - %userprofile%\AppData\Local\Google\Chrome\User Data\Default\Cookies
    - %userprofile%\AppData\Local\Google\Chrome\User Data\ChromeDefaultData\Cookies

Примечания:
- Все данные хранятся в виде баз данных. Для просмотра используйте:
- DB Browser for SQLite https://sqlitebrowser.org/ - Просмотрщик SQLite
- ESEDatabaseView https://www.nirsoft.net/utils/ese_database_view.html - Просмотрщик ESE

8.3. Cache

Описание:
Кэш — это место, где компоненты веб-страницы могут храниться локально для ускорения последующих посещений
• Предоставляет исследователю «отпечаток» того, что пользователь просматривал онлайн
    - Идентифицирует веб-сайты, которые были посещены
    - Предоставляет фактические файлы, просмотренные пользователем на данном веб-сайте
    - Кэшированные файлы привязаны к определенной локальной учетной записи пользователя
    - Временные метки показывают, когда сайт был впервые сохранен и просмотрен в последний раз.

Расположение:
- EDGE:
    - %USERPROFILE%\AppData\Local\Packages\microsoft. microsoftedge_\AC\MicrosoftEdge\Cache
- FIREFOX:
    - %USERPROFILE%\AppData\Local\Mozilla\Firefox\ Profiles\.default\Cache

- CHROME:
    - : %USERPROFILE%\AppData\Local\Google\Chrome\User Data\ Default\Cache\ - data_# and f_######

Примечания:

Все данные хранятся в виде баз данных. Для просмотра используйте:

- DB Browser for SQLite https://sqlitebrowser.org/ - Просмотрщик SQLite
- ESEDatabaseView https://www.nirsoft.net/utils/ese_database_view.html - Просмотрщик ESE

8.4. Super Cookies

Описание:

Локальные сохраненные объекты (LSO), или super cookie, стали повсеместными в большинстве систем из-за чрезвычайно высокого проникновения Flash и HTML5-приложений через Интернет. Они, как правило, гораздо более стойкие, поскольку срок их действия не истекает, и в браузере нет встроенного механизма для их удаления. На самом деле, многие сайты начали использовать lso для своих механизмов отслеживания, потому что они редко очищаются, как традиционные файлы cookie.

Расположение:

- EDGE:
    - **Локальное хранилище (Local Storage):** C:\Users\<имя пользователя>\AppData\Local\Microsoft\Edge\User Data\Default\Local Storage
    - **Кэш Flash-приложений:** C:\Users\<имя пользователя>\AppData\Roaming\Macromedia\Flash Player\#SharedObjects
    - **IndexedDB:** C:\Users\<имя пользователя>\AppData\Local\Microsoft\Edge\User Data\Default\IndexedDB
    - **LSO (Local Shared Objects):** C:\Users\<имя пользователя>\AppData\Roaming\Macromedia\Flash Player\macromedia.com\support\flashplayer\sys
    - **Web Storage:** C:\Users\<имя пользователя>\AppData\Local\Microsoft\Edge\User Data\Default\Local Storage
- FIREFOX:
    - **Локальное хранилище (Local Storage):** C:\Users\<имя пользователя>\AppData\Roaming\Mozilla\Firefox\Profiles\<профиль>\storage\default
    - **Кэш Flash-приложений:** C:\Users\<имя пользователя>\AppData\Roaming\Macromedia\Flash Player\#SharedObjects
    - **IndexedDB:** C:\Users\<имя пользователя>\AppData\Roaming\Mozilla\Firefox\Profiles\<профиль>\storage\default
    - **LSO (Local Shared Objects):** C:\Users\<имя пользователя>\AppData\Roaming\Macromedia\Flash Player\macromedia.com\support\flashplayer\sys
    - **Web Storage**: C:\Users\<имя пользователя>\AppData\Roaming\Mozilla\Firefox\Profiles\<профиль>\storage\default
- CHROME:
    - **Локальное хранилище (Local Storage):** C:\Users\<имя пользователя>\AppData\Local\Google\Chrome\User Data\Default\Local Storage
    - **Кэш Flash-приложений:** C:\Users\<имя пользователя>\AppData\Roaming\Macromedia\Flash Player\#SharedObjects
    - **IndexedDB**: C:\Users\<имя пользователя>\AppData\Local\Google\Chrome\User Data\Default\IndexedDB
    - **LSO (Local Shared Objects):** C:\Users\<имя пользователя>\AppData\Roaming\Macromedia\Flash Player\macromedia.com\support\flashplayer\sys
    - **Web Storage:** C:\Users\<имя пользователя>\AppData\Local\Google\Chrome\User Data\Default\Local Storage

Примечания:

Содержат в себе:

- Посещенные веб-сайты
- Учетная запись пользователя, используемая для посещения сайта
- Когда был создан файл cookie и осуществлялся последний доступ к нему

8.5. Восстановление сессий браузера

Описание:

Функции автоматического восстановления после сбоя встроены в браузер и могут быть отличным подспорьем для реконструкции того какие сайты просматривал пользователь.

Расположение:

- EDGE:

  - C:\Users\XX\AppData\Local\Packages\Microsoft.MicrosoftEdge_XXX\AC\MicrosoftEdge\User\Default\Recovery\Active
- FIREFOX:
  - C:\Users\XXX\AppData\Roaming\Mozilla\Firefox\Profiles\[profileID].default\sessionstore.jsonlz4
  - C:\Users\XXX\AppData\Roaming\Mozilla\Firefox\Profiles\[profileID].default\sessionstore-backups\
- CHROME:

Текущая сессия/Вкладки
  - C:\Users\XXX\AppData\Local\Google\Chrome\User Data\Default\Current Session
  - C:\Users\XXX\AppData\Local\Google\Chrome\User Data\ChromeDefaultData\Current Session
  - C:\Users\XXX\AppData\Local\Google\Chrome\User Data\Default\Current Tabs
  - C:\Users\XXX\AppData\Local\Google\Chrome\User Data\ChromeDefaultData\Current Tabs

Предыдущие сессии/Вкладки
  - C:\Users\XXX\AppData\Local\Google\Chrome\User Data\Default\Last Session
  - C:\Users\XXX\AppData\Local\Google\Chrome\User Data\ChromeDefaultData\Last Session
  - C:\Users\XXX\AppData\Local\Google\Chrome\User Data\Default\Last Tabs
  - C:\Users\XXX\AppData\Local\Google\Chrome\User Data\ChromeDefaultData\Last Tabs

Примечания:
- История посещений веб-сайтов, с перечнем открытых вкладок
- Одновременно открыты вкладки в браузере.
- Время окончания сеанса
- Время изменения файлов .data в последней активной папке
- Время открытия каждой вкладки (только при возникновении сбоя)
- Время создания файлов .data в активной папке

8.6. Сохраненные логины и пароли

Описание:
Часто браузеры содержат в себе сохраненные пользователями логины и пароли для входа на различные ресурсы. Они могут хранится как в открытом, так и в зашифрованном виде.

Расположение:
- EDGE:
  - C:\Users\XX \AppData\Local\Microsoft\Edge\User Data\Default\Login Data
- FIREFOX:
  - Логины C:\Users\XXX\AppData\Roaming\Mozilla\Firefox\Profiles\[profileID].default\logins.json
  - Пароли C:\Users\XXX\AppData\Roaming\Mozilla\Firefox\Profiles\[profileID].default\key4.db
- CHROME:
  - C:\Users\XXX\AppData\Local\Google\Chrome\User Data\ChromeDefaultData\Login Data

Примечания:
-

Раздел 2.

КРИМИНАЛИСТИЧЕСКИЕ АРТЕФАКТЫ ЭКОСИСТЕМЫ APPLE

9. LOG ФАЙЛЫ macOS

9.1. Apple System Log (ASL)

Расположение:

macOs 10.5.6+

- /private/var/log/asl/
    - YYYY.MM.DD.[UID].[GID].asl
    - Записи входа в систему (utmp, wtmp, lastlog) - BB.YYYY.MM.DD.[UID].[GID].asl

macOS 10.8+

Дополнительные каталоги данных системного журнала - AUX.YYYY.MM.DD

Примечания:

- Просмотр с помощью **Console.app** или команды **syslog**
- Сообщения, регистрируемые syslog: TTL составляет семь дней
- Сообщения, регистрируемые utmp, wtmp и lastlog: TTL составляет 366 дней
- Временные метки хранятся в UTC
- Сопоставить журналы: **syslog -F raw -T utc -d/private/var/log/asl/ > asl.log**
    - Открыть в консоли: **open -a Console asl.log**

9.2. Audit Logs

Расположение:

- /private/var/audit/<start_time YYYYMMDDHHMMSS>.<end_timeYYYYMMDDHHMMSS>

Конфигурация Audit log: /etc/security/audit_*

Примечания:

- Временные метки хранятся в UTC
- Команда praudit выводит временные метки по местному времени
- Сопоставить логи - **praudit -xn /private/var/audit/*.* > audit.log**
    - Открыть лог в консоли - **open -a Console audit.log**

9.3. System.log

Расположение:

macOS 10.13.1+:

- /private/var/log/system.log

Примечания:

Временные метки представлены по местному времени.

9.4. Unified Logs

Расположение:

macOS 10.13.1+:

- /private/var/db/diagnostics/*.tracev3
- /private/var/db/uuidtext/*

Сообщения, связанные с **SessionAgentNotificationCenter** показывают инициированные пользователем действия, относящиеся к событиям завершения работы системы.

Примечания:

- Временные метки хранятся в UTC
- Создайте бандл logarchive для анализа:
    - Создайте папку logarchive: ***sudo mkdir logs.logarchive***
    - Скопируйте файлы логов: ***cp -R /private/var/db/uuidtext/ /private/var/db/ diagnostics/ logs.logarchive***
    - Создайте формат: ***/usr/libexec/PlistBuddy -c "Add :OSArchiveVersion integer 4" logs.logarchive/Info.plist***

Анализ:

- Получить записи USBMSC: **log show logs.logarchive/ --timezone UTC--info --predicate 'eventMessage contains "USBMSC"'**
- Поиск устройств по имени: **log show logs.logarchive/ --timezone UTC --info --predicate 'eventMessage contains "VOL_NAME"**
- Экспорт unified logs в текстовый файл: **log show logs.logarchive/ --timezone UTC --info > galaga_logs.txt**
- Список отключений и перезагрузок: **log show logs.logarchive/ --timezone UTC --info --predicate 'eventMessage contains "com.apple.system.loginwindow" and eventMessage contains "SessionAgentNotificationCenter"'**

  - Способы отключения: **log show logs.logarchive/ --timezone UTC --info --predicate ‘eventMessage contains[c] “shutdown cause”’**
  - Получить лог бэкапа: **log show logs.logarchive/ --timezone UTC –info --predicate ‘process = “backupd” and category = “general”’**
  - Получить сетевой лог: **log show logs.logarchive/ --timezone UTC –info --predicate ‘senderImagePath contains[cd] “IPConfiguration” and (eventMessage contains[cd] “SSID” or eventMessage contains[cd] “Lease” or eventMessage contains[cd] “network changed”)’**

10. ВСТРОЕННЫЕ ПРИЛОЖЕНИЯ APPLE

10.1. Apple Mail – com.apple.mail / com.apple.mobilemail

Описание:

Это родное почтовое приложение, используемое по умолчанию, которое можно настроить для использования нескольких почтовых ящиков.

Расположение:

macOS:

- Почтовые ящики:

~/Library/Mail/V#/<GUIDE>/*.mbox

- Организация почтовых ящиков:

~/Library/Mail/V#/<GUID>/.mboxCache.plist
~/Library/Containers/com.apple.mail/

- Индекс конверта:

~/Library/Mail/V#/MailData/Envelope Index

- Загруженные вложения электронной почты могут храниться в

~/Library/Mail Downloads/
~/Library/Containers/com.apple.mail/Data/Library/MailDownloads/
~/Downloads/

- Расширенные атрибуты (найти используя ls -l@)

iOS:

- [/private/var]/mobile/Containers/Data/Application/<GUIDE>/
- [/private/var]/mobile/Library/Mail/
- Индекс конверта:
  [/private/var]/mobile/Library/Mail/Envelope Index

Примечания:

- В macOS номер версии отличается в зависимости от версии ОС:
  - V5 = macOS 10.13
  - V6 = macOS 10.14
  - V7 = macOS 10.15
  - V8 = mac OS 11
  - V9 = mac OS 12
  - V10 = mac OS 13
- Папки GUID могут быть соотнесены с базами данных Account3.sqlite/Account4.sqlite
- Почтовые ящики могут содержать вложенные почтовые ящики, сообщения и вложения
  - Папка "Сообщения" содержит сообщения электронной почты в формате EMLX с приложенным plist, содержащим метаданные сообщения
  - Папка "Вложения" содержит вложения файлов сообщений
- База данных sqlite с индексированным индексом конвертов содержит индексированные почтовые данные. Включает в себя флаги, показывающие, было ли электронное письмо прочитано, помечено или удалено
- Временные метки базы данных приведены в формате Unix Epoch

10.2. Сообщения – SMS и iMessage

Описание:

Это родное приложение для обмена сообщениями, которое можно использовать с различными протоколами

Расположение:

macOS:

- ~/Library/Messages/chat.db

iOS:

- [/private/var]/mobile/Library/SMS/sms.db
- [/private/var]/mobile/Library/SMS/Attachments/*

Примечания:

- SMS можно использовать только на iOS.
- Базы данных являются sqlite и включают сообщения и метаданные.
    - Временные метки указаны в формате Unix Epoch по местному времени
    - Транзакции Apple Pay записываются в поля атрибутированного тела (BLOB) и payload_data (встроенный plist)
    - поле **filename** показывает путь к вложению
    - **mime_type** показывает тип вложения

10.3. История звонков – Телефон и FaceTime

Описание:

Phone и FaceTime — это встроенные приложения для звонков на macOS и iOS.

Расположение:

macOS:

- ~/Library/Application Support/CallHistoryDB/CallHistory.storedata

iOS:

- [/private/var]/mobile/Library/CallHistoryDB/CallHistory.storedata

Примечания:

- Обратное DNS-имя телефона - com.apple.mobilephone.
- Обратное DNS-имя FaceTime - com.apple.facetime.
- База данных представлена в формате sqlite и включает принятые/отправленные вызовы и метаданные.
    - ZDATE - временные метки. Указаны в формате Mac Epoch по местному времени
    - ZADDRESS - номер телефона или адрес электронной почты
    - ZANSWERED - где 0 означает "Нет", 1 означает "Да"
    - ZCALLTYPE - где 1 означает обычный телефонный звонок, 8 означает FaceTime, 16 означает голосовой вызов FaceTime
    - ZORIGINATED - где 0 означает входящий, 1 означает исходящий с этим пользователем
    - ZDURATION - время в секундах для вызова
    - ZSERVICE_PROVIDER - приложение, используемое для вызова
- База данных macOS может хранить контактную информацию в зашифрованном двоичном объекте.
- Некоторые данные могут синхронизироваться между устройствами.
- Временные метки базы данных указаны в формате Unix Epoch по местному времени.

10.4. Календарь – Телефон и FaceTime

Описание:

Это встроенное приложение календаря на macOS и iOS, с помощью которого можно синхронизировать элементы из различных учетных записей. Оно может включать как личные, так и общие календари.

Расположение:

macOS:

- ~/Library/Calendars/.calendar
- ~/Library/Calendars/.caldav
- ~/Library/Calendars/Calendar Cache

iOS:

- [/private/var]/mobile/Library/Calendar/Calendar.sqlite

Примечания:

- Каждый каталог календаря содержит папку Events, в которой содержатся файлы календаря ICS, и файл Info.plist.
- Файлы **CalDAV Info.plist** и ICS могут содержать больше информации, чем в каталоге календаря.
- Кэш календаря (macOS) и **Calendar.sqlite** (iOS) — это базы данных sqlite, содержащие информацию о календаре.
    - - Названия таблиц со временем меняются
    - - Включает местоположения, общие события, заметки, контакты и многое другое
- Временные метки базы данных указаны в формате Unix Epoch по местному времени.

10.5. Напоминания – com.apple.reminders

Описание:

Напоминания были перенесены в их собственную базу данных в Mac OS 10.15 и iOS 13. Ранее они хранились в базе данных календаря

Расположение:

macOS:

- ~/Library/Reminders/../../Data-.sqlite
- ~/Library/Reminders/../../Data-local.sqlite

iOS:

- [/private/var]/mobile/Library/Reminders/../../Data-.sqlite
- [/private/var]/mobile/Library/Reminders/../../Data-local.sqlite

Примечания:

- Каждая база данных sqlite содержит напоминания из определенного источника (например, локального, iCloud).
- Каждый объект в базе данных имеет различное значение Z_ENT, которое меняется для разных версий базы данных.
    - - OBJECT_TYPE показывает, к какому типу относится каждый Z_ENT

10.6. Контакты – com.apple.AddressBook

Описание:

Приложение "Контакты", также известное как адресная книга, содержит контактную информацию пользователя. Оно может быть заполнено пользователем или другими приложениями.

Расположение:

macOS:

- ~/Library/Application Support/AddressBook/AddressBook-v22. abcddb
- ~/Library/Application Support/AddressBook/Sources// AddressBook-v22.abcddb
- ~/Library/Application Support/AddressBook/Sources// Metadata/*

iOS:

- [/private/var]/mobile/Library/AddressBook/AddressBook.sqlite
- [/private/var]/mobile/Library/AddressBook/Sources/*

Примечания:

- Каждый источник в папке Sources может иметь свой собственный связанный файл базы данных и папку метаданных.
    - Каталоги метаданных содержат двоичный файл plist для каждого пользователя (заканчивающийся на p), подписки (ов) или группы (g)
    - Переименуйте файлы метаданных в .plist, чтобы их можно было открыть с помощью XCode
- При поиске интересующего пользователя ищите его UID, а не только имя.
- Временные метки базы данных указаны в формате Unix Epoch по местному времени.

10.7. Кошелек и Apple Pay

Описание:

Приложение Wallet сохраняет билеты, карты и пропуска. Пользователь может добавить платежную карту в раздел приложения Apple Pay, чтобы использовать ее для покупок.

Расположение:

macOS:

- ~/Library/Passes/passes23.sqlite
- ~/Library/Passes/Cards/*.pkpass
- ~/Library/Mobile Documents/com~apple~shoebox/UbiquitousCards/*.pkpass – синхронизируемые данные с iCloud

iOS:

- /private/var/mobile/Library/Passes/passes23.sqlite
- /private/var/mobile/Library/Passes/Cards/*.pkpass
- /private/var/mobile/Library/Mobile Documents/com~apple~shoebox/UbiquitousCards/*.pkpass – синхронизируемые данные с iCloud

Примечания:

passes23.sqlite содержит:

- Временные метки базы данных приведены в формате Unix Epoch
- UNIQUE_ID в базе данных будет соответствовать имени файла .pkpass
- GROUP_ORDER показывает порядок пропусков в приложении, показаваемые пользователю (0 будет вверху)
- Транзакции с использованием сохраненных карт сохраняются в базе данных. Синхронизация транзакций между устройствами возможно только с Apple Card
- Поездки с использованием сохраненной транспортной карты регистрируются, включая начальную и
- конечную станции.

Файлы pkpass:

- Каждая карта представляет собой каталог в формате .pkpass.
    - pass.json хранит фактические данные пропуска или карты

10.8. Заметки – com.apple.notes/ com.apple.mobilenotes

Описание:

Заметки различных типов можно создавать в macOS, iOS и на iCloud.com. Их также можно синхронизировать со всеми устройствами, связанными с одной учетной записью iCloud.

Расположение:

macOS:

- ~/Library/Group Containers/group.com.apple.notes/NoteStore.sqlite
- Вложения: ~/Library/Group Containers/group.com.apple.notes/*
- legacy: ~/Library/Containers/com.apple.Notes/notes.sqlite

iOS:

- /private/var/mobile/Containers/Shared/AppGroup/NoteStore.sqlite
- Вложения: /private/var/mobile/Containers/Shared/AppGroup/*
- legacy: /private/var/mobile/Library/Notes/notes.sqlite

iOS Backup:

- /mobile/Applications/com.apple.notes/NoteStore.sqlite
- Вложения: /mobile/Applications/com.apple.notes/*
- legacy: /mobile/Applications/Notes/notes.sqlite

Примечания:

- При включенной синхронизации пользователь может выбрать создание локальных заметок, которые не будут синхронизироваться
- Вложения к заметкам хранятся в папке Мультимедиа
- Миниатюры заметок хранятся в папке предварительного просмотра
- В базе данных sqlite:
    - ZFILENAME - содержит имя файла вложения, хранящегося в папке мультимедиа
    - PROTECTED – 0 означает отсутствие шифрования, 1 – то что шифрование включено
    - ZDATA – хранит текст заметки в виде двоичного объекта, которым по факту является protobuf в архиве GZIP
    - Криптографический ключ хранится именно в этой базе данных, а не в связке ключей. Для расшифровки можно использовать Apple Cloud Notes Parser (https://github.com/threeplanetssoftware/apple_cloud_notes_parser)

10.9. Фото – com.apple.Photos

Описание:

Родное приложение для фотогалереи, включающее фотографии и видео, сделанные с помощью камеры и синхронизированное с фотогалерей телефона, скриншоты и синхронизированные медиафайлы.

Расположение:

macOS:

- ~/Pictures/Photos Library.photosLibrary/*
- ~/Pictures/Photos Library.photosLibrary/database/photos.db
- Оригиналы фото: ~/Pictures/Photos Library.photosLibrary/originals/*

iOS:

- [/private/var]/mobile/Media/PhotoData/*
- [/private/var]/mobile/Media/PhotoData/Photos.sqlite
- [/private/var]/mobile/Media/DCIM/*
- [/private/var]/mobile/Media/PhotoStreamsData/*
- [/private/var]/mobile/Media/PhotoCloudSharingData/*

Примечания:

- **Library.photosLibrary** в Mac OS — это каталог парепредставленный в виде пакетного файла.
- Расширенные атрибуты показывают, что файл был синхронизирован из iCloud, если **com.apple.quarantine** содержит **cloudphotosd**.
- Приложение Photos добавляет расширенный атрибут **com.apple.assetsd.***. который включает в себя исходное имя файла, местоположение, часовой пояс, флаги для “скрытого” и “избранного”, а также информацию о карантине
- Фотографии, сделанные с помощью версии iOS 11+, используют формат High Efficiency Image (HEIC).
- База данных содержит метаданные для каждого медиафайла, такие как, аннотации, информация о местоположении, а также обнаруженные лица и объекты

- Каждая подпапка DCIM может содержать до 999 файлов, имена которых последовательно начинаются с IMG_0001.

10.10. Карты – com.apple.Maps

Описание:
Это собственное картографическое приложение Apple. Картографические данные можно синхронизировать между устройствами.

Расположение:
macOS:
- ~/Library/Containers/com.apple.Maps/MapsSync.0.0.1

iOS:
- /private/var/mobile/Containers/Data/Application//Library/ Maps/MapsSync.0.0.1

iOS Backup:
- /mobile/Applications/com.apple.Maps/MapsSync.0.0.1

Примечания:
- Папка резервного копирования карт iOS может быть пустой.
- До macOS 11 и iOS 14 данные карт были разбросаны по всей файловой системе в виде файлов **.maps .data .plist**, в которых данные о местоположении хранились в виде встроенного protobuf.
- MapsSync.0.0.1 содержит ZMAPITEMSTORAGE который хранит данные о местоположение в виде protobuf

10.11. Health

Описание:
Информация о состоянии здоровья пользователя хранится в базе данных. Это может быть количество шагов, пройденное расстояние и частота сердечных сокращений, которые можно получить с помощью Apple Watch.

Расположение:
iOS:
• [/private/var]/mobile/Library/Health/healthdb_secure.sqlite

Примечания:
- База данных зашифрована в резервных копиях iOS, но отсутствует в полном дампе файловой системы.
- Используйте модули APOLLO health для извлечения данных о состоянии пользователя. (https://github.com/mac4n6/APOLLO)

11. ДАННЫЕ ПРИЛОЖЕНИЙ

11.1. Словарь клавиатуры

Описание:
Когда пользователь набирает слова на клавиатуре устройства, определенные слова записываются, чтобы помочь с автоматической коррекцией и функциями прогнозирования текста. Эти слова хранятся в файлах пользовательского словаря, которые могут дать представление о том, что вводил пользователь. Они не должны содержать ничего, введенного в конфиденциальные поля, такие
как пароли, хотя могут содержать конфиденциальные данные, которые пользователь мог ввести в незащищенных областях, таких как заметки.

Расположение:
macOS:
- ~/Library/Spelling/*dynamic-*.dat

iOS:
- [/private/var]/mobile/Library/Keyboard/*dynamic-*.dat

Примечания:
- Словари английского языка выглядит как dynamic-*.dat
- Другие языки имеют свои собственные файлы, и им будет предшествовать аббревиатура их языка (например, ru для русского).

11.2. Автозапуск приложений

Описание:
Приложения с автозапуском — это те, которые автоматически запускаются при входе пользователя в систему.

Расположение:

macOS 10.13+:

- ~/Library/ApplicationSupport/com.apple.backgroundtaskmanagementagent/backgrounditems.btm

- NSKeyedArchiver plist file

- /Applications/.app/Contents/Library/LoginItems/

macOS 10.4+:

- /System/Library/LaunchAgents/*.plist
- /Library/LaunchAgents/*.plist
- ~/Library/LaunchAgents/*.plist
- /System/Library/LaunchDaem

iOS:

- /Library/LaunchAgents/*.plist
- /System/Library/LaunchDaemons/
- /System/Library/NanoLaunchDaemons/
- /Library/LaunchDaemons/

- Необходим jailbreak для исследования.

Примечания:

- Элементы входа в систему могут быть скрыты от пользователя
- Демоны запуска являются фоновыми системными процессами
- Агенты запуска являются фоновыми пользовательскими процессами
- Имена файлов plist указаны в обратном формате DNS

11.3. Уведомления приложений

Описание:

Уведомления от различных приложений хранятся в самой графической оболочке операционной системы. У macOS она называется Finder; у iOS - SpringBoard.

Расположение:

macOS:

- /private/var/folders/<DARWIN_USER_DIR>/com.apple.notificationcenter/db2/db

iOS:

- [/private/var]/mobile/Library/UserNotifications/<app GUID>/*.plist

Примечания:

macOS:

- Путь к DARWIN_USER_DIR пользователя будет разным для каждого пользователя в системе
- Вложения к уведомлениям будут найдены в каталоге /**attachments**
- В база данных находятся дата и время доставки уведомления, идентификаторы пакетов приложений и его стиль
    - NOTIFICATION DATA- это BLOB файл, содержащий plist.

iOS:

- файлы plist находятся в формате **NSKeyedArchiver**.
- Уведомления, удаляемые пользователем, удаляются из файлов plist.
- Другие файлы в той же папке содержат элементы, относящиеся к интерфейсу, такие как- фоновые изображения, макеты значков и виджеты.
- Сопоставьте GUIDs приложения с соответствующим bandle ID, заглянув в **[/private/var]/mobile/Library/User Notifications Server/Library.plist**. Обратите внимание что, этот файл не включен в резервные копии iOS.

11.4. Установленные приложения и обновления.

Описание:

Определяем установленные приложения и обновления, включая временные метки, имена пакетов и программное обеспечение, используемое для установки приложения.

Расположение:

macOS 10.14:

~/Library/Caches/com.apple.appstoreagent/updates.plist

macOS 10.15:

- ~/Library/Caches/com.apple.appstoreagent/storeSystem.db
- /Library/Receipts/InstallHistory.plist
- /var/log/install.log
    - - поищите в файле “installed”, названия приложений и версии
- /var/db/receipts/

    - файл plist содержит временную метку установки, имя пакета и процесс установки.
    - файл спецификации содержит список файлов и метаданных для приложения.

iOS 10+:

- /private/var/installd/Library/Logs/MobileInstallation/mobile_installation.log.#
    - Поищите “Make container live” для поиска момент установки приложения
    - Поищите “Destroying container” для поиска момента удаления приложения
    - Поищите по bundle IDs моменты активности приложения

iOS:

- /private/var/mobile/Library/FrontBoard/applicationState.db
    - Содержит встроенные plist

Примечания:

- **InstallHistory.plist** названия процессов:
    - **macOS Installer** = Установка или обновление самой ОС
    - **softwareupdated** or **“Software Update”** = Установка системных обновлений или обновлений безопасности.
    - **storedownloadd** = Установка из App Store
    - **Installer** = Установка из стороннего инсталлера
- **bom file** (файл спецификации) можно посмотреть при помощи команды ***lsbom <bom file>***
- файл **install.log** может отсутствовать если установка программы была произведена путем перетаскивания.

11.5. Разрешения приложений - TCC

Описание:

Место, где фиксируется какие приложения запрашивают у пользователя разрешения для реализации различных возможностей в системе.

Расположение:

macOS:

- ~/Library/Application Support/com.apple.TCC/TCC.db
- /Library/Application Support/com.apple.TCC/TCC.db

iOS:

- [/private/var]/mobile/Library/TCC/TCC.db

Примечания:

- Приложения могут иметь доступ к таким разрешениям, как: Местоположение, Контакты, Календари, фотографии, Bluetooth, микрофон, камера
- Содержит временную метку **last_modified** для каждого разрешения для каждого приложения
- **auth_value** = 0 означает, что не разрешено, 2 означает, что разрешено
- Разрешение **kTCCServiceUbiquity** ассоциируется с iCloud

11.6. Сторонние расширения ядра

Описание:

Модули ядра часто используются в качестве драйверов устройств, сетевых фильтров или поддержки Сторонних файловых систем. Так же могут быть использованы для реализации различных атак.

Расположение:

macOS:

- /private/var/db/loadedkextmt.plist
- /Library/Apple/System/Library/Extensions/
- /System/Library/Extensions/
- /Library/Extensions/
- /Library/StagedExtensions/
- /Library/SystemExtensions/
- /Library/<Filesystems/macfuse.fs/Contents>/

Примечания:

- В действующей системе используйте команду **system extensions ctl list** для отображения списка загруженных системных расширений и команду **kmutil show loaded** для отображения списка загруженных расширений ядра
- Каждое расширение представляет собой bundle, содержащий файл Info.plist

12. ВЫПОЛНЕНИЕ ПРОГРАММ И ИСПОЛЬЗОВАНИЕ ПРИЛОЖЕНИЙ

12.1. История терминала – выполнение команд.

Описание:

Каждая учетная запись пользователя хранит в скрытом файле, находящемся в домашней папке список команд, выполняемых в терминале оболочки bash или zsh.

Расположение:

macOS:

- ~/bash_history

macOS 10.15+:

- ~/.zsh_history

macOS 11+:

- ~/.zsh_sessions/.history

macOS 10.11–10.14:

- ~/.bash_sessions/.history

Примечания:

- Это обычные текстовые файлы, содержащие до 1000 (zsh) или 500 (bash) команд, расположенных в порядке выполнения.
- Файлы создаются при первом запуске приложения терминала.
- Файлы истории не обновляются до тех пор, пока учетная запись пользователя не выйдет из системы. Файлы сеанса обновляются при запуске терминала.
- Файлы можно просматривать в текущей системе с помощью команды history.
- <GUID>.history содержат команды, выполненные в этом сеансе.

12.2. Время работы в приложениях

Описание:

Отслеживается время, проведенное пользователем в приложениях, и его реакция на уведомление в виде открытия приложения на определенном устройстве после получения уведомления. Поддерживается на устройствах с macOS версии 10.15 и выше и устройствах с iOS версии 13 и выше.

Расположение:

macOS 10.15+:

- /var/folders/<darwin_user_dir>/0/com.apple.ScreenTimeAgent/RMAdminStore-Cloud.sqlite
- /var/folders/<darwin_user_dir>/0/com.apple.ScreenTimeAgent/RMAdminStore-Local.sqlite

iOS 13+

- /private/var/mobile/Library/ApplicationSupport/com.apple.remotemanagementd/RMAdminStore-Cloud.sqlite
- /private/var/mobile/Library/ApplicationSupport/com.apple.remotemanagementd/RMAdminStore-Local.sqlite

Примечания:

Данные отсортированы по времени и категориям

Срок хранения этих данных составляет для iOS – 3 недели, для macOS – 5 недель

12.3. Использование приложений - KnowledgeC

Описание:

база данных KnowledgeC сохраняет данные об использование приложений, время запуска и выхода из него, а также способ запуска и некоторые данные работы этого приложения.

Расположение:

macOS:

- ~/Library/Application Support/Knowledge/knowledgeC.db

iOS:

- /private/var/mobile/Library/CoreDuet/knowedgeC.db

Примечания:

- Срок хранения данных – около 4 недель
- Вы можете использовать проект **APPOLO** (https://github.com/mac4n6/APOLLO) и его модули для извлечения этих данных:
  - **knowledge_app_in_Focus** - для извлечения времени использования приложения
  - **knowledge_app_intents** - для извлечения контекста использования приложения
  - **knowledge_audio_media_now** - для извлечения подробной информации о воспроизведении мультимедиа

12.4. Использование приложений - CurrentPowerlog

Описание:

Этот лог содержит информацию об использование приложения, состояние камеры (передней или задней) в случае использования мобильного устройства и ведет журнал вызовов.

Расположение:

macOS:
- /private/var/db/powerlog/Library/BatteryLife/CurrentPowerlog.PLSQL
- /private/var/db/powerlog/Library/BatteryLife/Archives/*

iOS:
- /private/var/Containers/Shared/SystemGroup/<GUID>/Library/BatteryLife/CurrentPowerlog.PLSQL
- /private/var/Containers/Shared/SystemGroup/<GUID>/Library/BatteryLife/Archives/*

Примечания:
- Срок хранения данных – около 3х дней
- Вы можете использовать проект APPOLO (https://github.com/mac4n6/APOLLO) и его модули для извлечения этих данных:
    - **power log_app_usage** для извлечения времени использования приложения
    - **power log_in call service** для извлечения журнала вызовов
    - **powerlog_camera_state** для извлечения информации о состояние камеры

13. ОТКРЫТИЕ ФАЙЛОВ И ПАПОК в macOS

13.1. Открытие DMG файлов – расширенные атрибуты.

Описание:

Двойной клик по файлу DMG создает два дополнительных расширенных атрибута для этого файла, которые относятся к данному действию и данному типу файла. Эти расширенные атрибуты показывают, что файл DMG был открыт по крайней мере один раз.

Расположение:

Смотрите везде расширенные имена атрибутов для файлов:
- ls -l@
    - **com.apple.diskimages.fsck** - дают информацию о проверке файловой системы
    - **com.apple.diskimages.recentcksum** - предоставляет информацию о контрольной сумме и дате загрузки (в формате Unix Epoch)
    -

Посмотреть расширенный атрибут файла можно командой **xattr -xl <имя файл>**

Примечания:

Первая временная метка из этого процесса записана в **~/Library/Logs/fsck_hfs.log**

13.2. Последний использованный файл – расширенные атрибуты.

Описание:

Этот расширенный атрибут обновляется при использовании файла в окне Finder или при открытии файла с помощью команды “open” в терминале

Расположение:

Присутствуют практически везде:
- ls -l@
    - **com.apple.lastuseddate#PS** – сохраняет временную метку последнего использования файла

Посмотреть расширенный атрибут файла можно командой **xattr -xl <имя файл>**

Примечания:

Обратите внимание что не все типы файлов обладают этим атрибутом.

13.3. Доступ к папке - .DS_Store

Описание:

Скрытые файлы DS_Store могут существовать во всех папках macOS. Они создаются, когда приложение Finder используется для доступа к каталогу

Расположение:

Присутствуют везде.
- .DS_Store

Примечания:

Для удаленных файлов **.DS_Store** содержит: исходное имя файла и исходный путь к файлу

13.4. Most Recently Used (MRU)

Описание:

Функция фиксации перечня исполняемых команд.

Расположение:

- ~/Library/Preferences/com.apple.finder.plist

macOS 10.12:

- ~/Library/ApplicationSupport/com.apple.sharedfilelist/com.apple.LSSharedFileList.ApplicationRecentDocuments/<bundle_id>.sfl

macOS 10.13+:

- ~/Library/ApplicationSupport/com.apple.sharedfilelist/com.apple.LSSharedFileList.ApplicationRecentDocuments/<bundle_id>.sfl2
- ~/Library/Application Support/com.apple.sharedfilelist/com.apple.LSSharedFileList.Recent*.sfl2

Примечания:

- Файлы SFL представляют собой plist, использующие формат **NSKeyedArchiver**.
- В большинстве собственных списков MRU по умолчанию сохраняются последние 10 элементов.
- Провести анализ MRU вы сможетепри помощи **macMRU-parser** (https://github.com/mac4n6/macMRU-Parser)

13.5. Недавние папки

Описание:

Отслеживаем папки к которым недавно был доступ от имени аккаунта пользователя

Расположение:

- ~/Library/Preferences/com.apple.finder.plist
  - FXRecentFolders содержит BLOB в файле закладке

Примечания:

- Пункт 0 является недавним, а пункт 9 - самым поздним.

13.6. Недавние элементы

Описание:

Это элементы, к которым недавно получила доступ учетная запись пользователя для каждого приложения.

Расположение:

- ~/Library/Application Support/com.apple.sharedfilelist/*.sfl2

Примечания:

- Список содержит как родные, так и сторонние приложения.
- Имена файлов указаны в обратном формате DNS.

14. ИСПОЛЬЗОВАНИЕ АККАУНТА

14.1. com.apple.loginwindow.plist.

Описание:

Данные о последнем вошедшем в систему пользователе, текущем вошедшем в систему пользователем (в действующей системе), пользователе с автоматическим входом в систему (если настроен) и другие настройки записываются в этот файл plist.

Расположение:

- /Library/Preferences/com.apple.loginwindow.plist

Примечания:

- Пароль пользователя хранится в /etc/kcpassword
- Автоматический вход в систему недоступен для использования учетных данных FileVault или iCloud

14.2. Учётные записи пользователей

Описание:

Это события успешного и неудачного входа в учетную запись пользователя и выхода из системы.

Расположение:

- System log

macOS 10.12+, iOS 10+:

- Unified Logs

macOS 10.5.6+:

- ASL

Примечания:

- События входа помечаются USER_PROCESS и идентификатором процесса
- События выхода из системы помечаются значением DEAD_PROCESS и идентификатором процесса
  - Тип входа определяется по:
    - loginwindow = вход через графический интерфейс пользователя
    - login = вход через терминал
    - ssh = вход через SSH

14.3. Audit Logs – su Logins

Описание:

Все удачные и неудачные попытки входа su (substitute user). По умолчанию - root

Расположение:

- Audit logs

Примечания:

Просмотр входов пользователя su : praudit -xn /var/audit/* - su

14.4. Audit Logs – создание аккаунта

Описание:

Записи в журнал аудита добавляются при создании учетной записи пользователя.

Расположение:

- Audit logs

Примечания:

Просмотр входов пользователя su : **praudit -xn /var/audit/* - su**

- **create user event** содержит имя нового пользователя и UID пользователя, который его создал.

14.5. Блокировка/Разблокировка экрана

Описание:

События создается, когда экран заблокирован или разблокирован.

Расположение:

- Unified Logs

Примечания:

- События блокировки экрана содержат - **com.apple.sessionagent.screenIsLocked**
- События разблокировки экрана содержат - **com.apple.sessionagent.screenIsUnlocked**
  - Сюда входят действия разблокировки с использованием обычного пароля, Touch ID или Apple Watch

14.6. Известные SSH хосты

Описание:

Это имена хостов, IP-адреса и открытые ключи для хостов, к которым эта система когда либо подключилась по SSH и для которых пользователь решил сохранить ключ.

Расположение:

- ~/.ssh/known_hosts
- ~/.ssh/authorized_hosts

Примечания:

По умолчанию имена хостов и IP-адреса будут доступны для чтения. Эти данные будут хэшированы, если для параметра **HashKnownHosts** установлено значение **yes** в файле **/etc/ssh/ssh_config**

14.7. Повышение привилегий для su пользователя

Описание:
Тут регистрируются пользователи с привилегиями su, а также журнал команд, которые были запущены от имени root.

Расположение:
Пользователи с правами root-уровня:
- /etc/sudoers
- Unified Logs

Примечания:
Ищите sudo или su процесс.

15. ФИЗИЧЕСКОЕ МЕСТОРАСПОЛОЖЕНИЕ

15.1. Приложение которые запрашивают информацию о месторасположение.

Описание:
Система фиксирует список приложений, которые запросили разрешение службы определения местоположения.

Расположение:
macOS:
- ~/Library/Application Support/com.apple.TCC/TCC.db
- /Library/Application Support/com.apple.TCC/TCC.db
- /private/var/db/location/clients.plist

iOS:
- [/private/var]/mobile/Library/TCC/TCC.db
- [/private/var]/root/Library/Caches/locationd/clients.plist

Примечания:
- TCC.db:
  - Включает временную метку **last_modified** для каждого разрешения каждого приложения
  - auth_value = 0 означает "не разрешено", 2 означает "разрешено"
  - Обычно предполагается, что разрешение **KTCCServiceLiverpool** является частью клиентов служб определения местоположения.
- Clients.plist:
  - Список всех приложений, которым были предоставлены разрешения служб определения местоположения
  - **Authorization** = 1 - никогда не выдавать разрешение, 2 - во время использования, 4 – разрешать всегда, no – запрашивать пользователя при необходимости.
  - В версии iOS 14 и старше: **CorrectiveCompensationEnabled** = 1 (или без ключа) – включено определение точного местоположения, 2 – выключено

15.2. Часто посещаемые и значимые места.

Описание:
Если параметр " Significant Locations " включен, то это позволяет устройству сохранять местоположения, которые оно посетило. Поддерживается в iOS версии 11 и старше.

Расположение:
- /private/var/mobile/Library/Caches/com.apple.routined/Cloud[-V2].sqlite
- /private/var/mobile/Library/Caches/com.apple.routined/Cache.sqlite
- /private/var/mobile/Library/Caches/com.apple.routined/Local.sqlite

Примечания:
- Функция включается и выключается через Settings → Privacy → Location Services → System Services → Significant Locations
- Алгоритм определения того, каким образом устройство помечает местоположение как “частое”, неизвестен.
- Cloud[-V2].sqlite – в этой базе данных содержаться факты посещения определенных мест.
- Cache.sqlite - база данных содержит очень подробные данные о местоположении глубиной примерно в неделю.
- Эти же данные также можно найти в macOS, однако они будут зашифрованы.
- Вы можете использовать модули проекта APOLLO (https://github.com/mac4n6/APOLLO):

    - **routined_cloud_visit_entry** - для извлечения посещений местоположения из Cloud[-V2].sqlite
    - **routined_cache_zrtcllocationmo** - модуль для извлечения посещений местоположения из базы данных кэша.

15.3. Местоположение по WIFI и мобильным сетям.

Описание:
Местоположение, привязанное к вышкам сотовой связи и Wi-Fi точкам доступа фиксируется в нескольких базах данных.

Расположение:
macOS:
- • /private/var/folders/*/<DARWIN_USER_DIR>/cache_encrypted*.db
- • /private/var/folders/*/<DARWIN_USER_DIR>/lockCache_encrypted*.db

iOS:
- • /private/var/root/Library/caches/locationd/cache_encrypted*.db
- • /private/var/root/Library/caches/locationd/lockCache_encrypted*.db

Примечания:
- Данные хранятся примерно одну неделю, но это зависит от таблицы.
    - Данные в таблице **WifiLocation** хранятся примерно четыре дня
- Временные метки хранятся в Mac Epoch
- Местоположения указаны примерно.
- MAC-адреса хранятся в формате Base10.
- Вы можете использовать модули проекта APOLLO (https://github.com/mac4n6/APOLLO): **locationd_cacheencryptedAB_ltecelllocation** для извлечения данных о геолокации.

16. ТОМА И ВНЕШНИЕ УСТРОЙСТВА / ИСПОЛЬЗОВАНИЕ USB

16.1. Finder – смонтированные тома.

Описание:
Приложение Finder в Mac OS хранит список томов, которые были смонтированы на рабочем столе, в файле plist. Он включает в себя имя тома с координатами X и Y томов, смонтированных на рабочем столе.

Расположение:
macOS:
- ~/Library/Preferences/com.apple.finder.plist
    - FXDesktopVolumesPositions key

Примечания:
- В нем не указана дата, когда был подключен том.
- Ключа не будет, если у пользователя в настройках Finder не настроено отображение элементов на рабочем столе
- Он содержит хост тома, USB-накопители и подключенные файлы DMG

16.2. Избранные тома.

Описание:
Это список избранных томов, включая название тома и его свойства.

Расположение:
macOS 10.13+:
- ~/Library/Application Support/com.apple.sharedfilelist/com.apple.LSSharedFileList.FavoriteVolumes.sfl2

Примечания:
NSKeyedArchiver plist файл содержт Bookmark BLOBs

16.3. Поиск журналов по томам.

Описание:

В журналах записывается, какие тома были смонтированы в системе. Может содержаться файл устройства, используемый томом, размер тома, имя и точка монтирования.

Расположение:

macOS 10.13.1+:

- /var/log/daily.out
- System log
- Unified logs

Примечания:

- Выполните поиск по “/Volumes/”, чтобы найти любые тома, подключенные к точке монтирования по умолчанию
- Вы можете выполнить поиск в system.log и унифицированных журналах для apfs, has, подключенных, размонтированных или disk#s#
- Поиск по названию тома позволяет найти действия, относящиеся к этому тому
- В ежедневных журналах записывается, какие тома были смонтированы в системе при запуске сценария ежедневного обслуживания
    - В старых версиях OS X daily.out может называться daily.log

16.4. Поиск журналов по подключенным USB устройствам.

Описание:

Идентификатор класса USB Mass Storage (USB MSC) можно использовать для поиска подключений устройств USB MSC в системном журнале и в унифицированных журналах, включая серийный номер устройства, информацию о вендоре и продукте.

Расположение:

macOS 10.12:

- System log
- Unified logs

Примечания:

• Ищите USBMSC

- Типичная структура этих записей: Идентификатор USBMSC (неуникальный): <серийный номер> <VID> <PID> <версия>

• Имейте в виду, что не все записи USBMSC инициируются пользователем.

• Вы также можете найти подключения к общему сетевому ресурсу, отсортировав Unified logs: **process = NetAuthSysAgent AND sender = loginsupport**

17. ОБЩИЙ ДОСТУП К ФАЙЛАМ И ПАПКАМ

17.1. AirDrop – расширенные атрибуты.

Описание:

AirDrop позволяет пользователям “сбрасывать” файлы на устройство другого пользователя используя Wi-Fi или Bluetooth, если это устройство находится поблизости. Расширенные атрибуты для файла будут показывать имя устройства, с которого файл был отправлен с помощью AirDrop.

Расположение:

macOS 10.7+:

Могут находится везде. Смотрите расширенные атрибуты файлов:

- ls -l@
    - **com.apple.metadata:kMDItemWhereFroms** - предоставляет название устройства, с которого был отправлен файл.

Посмотреть расширенные атрибуты файла: xattr -xl <имя файла>

Примечания:

Имейте в виду, что имя устройства может быть изменено пользователем.

17.2. Расширенные атрибуты.

Описание:

Несколько расширенных атрибутов могут указывать на общий доступ к файлам, включая отправителя, получателя и используемое приложение.

Расположение:

macOS 10.7+:

Могут находится везде. Смотрите расширенные атрибуты файлов:

- ls -l@
- **com.apple.metadata:kMDItemUserShared<Sent/Received>Date** – когда к файлу был предоставлен доступ
- **com.apple.metadata:kMDItemUserShared<Sent/Received>Sender** – показывает отправителя файла
- **com.apple.metadata:kMDItemUserShared<Sent/Received>SenderHandle** – показывает учетную запись отрапвителя
- **com.apple.metadata:kMDItemUserShared<Sent/Received>Recipient** – показывает получателя файла
- **com.apple.metadata:kMDItemUserShared<Sent/Received>ReceipientHandle** – показывает учетную запись получателя
- **com.apple.metadata:kMDItemUserShared<Sent/Received>Transport** – показывает используемое приложение для передачи/приема файла.
- **com.apple.metadata:kMDItemTransportService** – показывает используемое приложение для прима/передачи файла.
- **com.apple.metadata:kMDItemWhereFroms** – показывает время и используемое приложение, Например. “Received via Messages file transfer”

Посмотреть расширенные атрибуты файла: xattr -xl <имя файла>

Примечания:

• Тут отображаются файлы, которыми обмениваются с помощью AirDrop, электронной почты, сообщений и других приложений.

• В базе данных Spotlight можно выполнить поиск по этим атрибутам, чтобы найти доказательства совместного использования файлов.

17.3. Активность AirDrop – Unified Logs.

Описание:

Файлы, отправленные и полученные с помощью AirDrop, фиксируются в Unified Logs. В их состав входят такие данные как уникальный идентификатор транзакции (AirDrop ID), тип отправляемого файла, было ли принято соединение и возможно место, где оказался полученный файл.

Расположение:

macOS 10.12+ и iOS 10+:

- Unified Logs

Примечания:

- Проанализировав отправляющее и принимающее устройства, вы можете связать эти действия, используя AirDrop ID (ReceiverID). Если вам доступно только одно из устройств, атрибуция станет намного сложнее.
- Имейте в виду, что имена устройств можно легко изменить.
- Журнал показывает, было ли соединение “Принято” или “Отклонено".

17.4. Активность AirDrop – Aggregative Dictionary.

Описание:

База данных Aggregate Dictionary отслеживает активность за последние семь дней и включает в себя активность AirDrop

Расположение:

iOS:

- /private/var/mobile/Library/AggregateDictionary/ADDataStore. sqlitedb

Примечания:

Временный отпечатки даны в формате Unix Epoch.

• Используйте модули APOLLO (https://github.com/mac4n6/APOLLO) **aggregate_dictionary_scalars** для извлечения этих данных.

17.5. Общие папки.

Описание:

Информация и метаданные для общих папок в системе.

Расположение:

macOS:

- /private/var/db/com.apple.xpc.launchd/disabled.plist
- /private/var/db/launchd.db/com.apple.launchd/overrides.plist
- /private/var/db/dslocal/nodes/Default/sharepoints/*.plist
    - Список общих папок и их метаданных

Примечания:

- disabled.plist/overrides.plist:
    - По умолчанию ни один из этих параметров не включен
    - В качестве bundle ID для общих папок найдите com.apple.smbd и/или com.apple.AppleFileServer
- sharepoints/*.plist:
    - Каждая общая папка имеет свой собственный файл plist

17.6. Документы iCloud.

Описание:

iCloud хранит локальные копии документов, которыми можно поделиться с помощью различных приложений.

Расположение:

macOS:

- ~/Library/Mobile Documents/

iOS:

- /private/var/mobile/Library/Mobile Documents/

Примечания:

- Каждый подкаталог соответствует приложению и назван в обратном формате DNS, но с использованием тильд (~)
- Расширенные атрибуты для этих документов включают iCloud Person ID в com.apple.ubd.prsid.
- Скрытые файлы *.icloud соответствуют файлам, которые не были загружены на это устройство.
    - Это двоичные файлы plist, содержащие имя файла и его размер

18. ОБЩИЙ ДОСТУП К ФАЙЛАМ И ПАПКАМ

18.1. Поиск - Spotlight

Описание:

Spotlight индексирует систему, чтобы позволить пользователю быстро выполнять поиск файлов. Индексация включает метаданные файлов, расширенные атрибуты и содержимое некоторых типов файлов.

Расположение:

macOS 10.4:

Пользовательские ярлыки поиска:

- ~/Library/Application Support/com.apple.spotlight.Shortcuts

macOS 10.15+:

- ~/Library/Application Support/com.apple.spotlight/ com.apple.spotlight.Shortcuts.v3

Основные базы данных индексации Spotlight:

- /.Spotlight-V100/Store-V2/<GUID>
    - **VolumeConfiguration.plist** содержит исключения для индексации и другие данные конфигурации
    - **Cache** содержит подкаталоги текстовых версий исходных документов, каждая из которых названа в соответствии с индексом файла
    - **store.db** база данных содержащая индекс

macOS 10.13+

Пользовательский индекс: ~/Library/Metadata/CoreSpotlight/index.spotlightV3

Примечания:

- Том можно явно пометить для отключения индексации, поместив скрытый пустой файл с именем **.metadata_never_index** в корневой каталог тома.
- Некоторые места по умолчанию не индексируются, включая файлы DMG, компакт-диски, DVD-диски, скрытые файлы и системные каталоги.
- Файлы пользовательских ярлыков содержат слова, фактически введенные пользователем.

18.2. Корзина

Описание:

Любые файлы или папки, удаленные пользователем, сохраняются в скрытой папке корзины в корневом каталоге домашнего каталога этого пользователя.

Расположение:

macOS:

- ~/.Trash

Примечания:

- Некоторые удаленные файлы можно восстановить, используя опцию “Вернуть”.
    - Если в файле есть эта опция, данные можно найти в файле .DS_Store в корзине
- “Safe” файлы Safari отправляются непосредственно в корзину, поскольку они автоматически распаковываются при загрузке.
- В macOS версии 10.12 и старше доступна опция удаления файлов из корзины через 30 дней

18.3. База данных хранилища событий файловой системы

Описание:

В этой базе данных хранятся изменения файловой системы. Она включает в себя такие события, как создание файла/папки, действия по переименованию, распаковка файлов, удаление элементов, очистка корзины, а также монтирование и размонтирование томов.

Расположение:

macOS:

- /.fseventsd/

Примечания:

- Каталог содержит файлы в формате gzip, для распаковки и просмотра которых требуются права root.
- Он может быть удален во время сбоя системы или отключения питания.
- Он отслеживает изменения только на томах HFS и APFS, хотя вы можете увидеть там каталог на томах FAT.
- События не имеют связанных временных меток. Приблизительное время иногда можно оценить, используя имена файлов и пути к ним.

18.4. Версии документов

Описание:

Версии документов были введены в OS X 10.7 для автоматического резервного копирования определенных типов документов или для восстановления документов после сбоя системы. Версии создаются при сохранении документа, открытии, каждый час, когда документ открыт, и при частом редактировании. Эта функция поддерживается только определенными приложениями.

Расположение:

macOS 10.15+:

- /System/Volume/Data/.DocumentRevisions-V100
- /System/Volume/Data/.DocumentRevisions-V100/db-V1/db.sqlite - Содержит метаданные для версий документов
- /System/Volume/Data/.DocumentRevisions-V100/.cs/ChunkStorage/*

iOS:

- /private/var/.DocumentRevisions-V100
- /private/var/.DocumentRevisions-V100/db-V1/db.sqlite - Содержит метаданные для версий документов
- /private/var/.DocumentRevisions-V100/.cs/ChunkStorage/*

Примечания:

- Microsoft Office не поддерживает версии документов; для этого предусмотрена собственная функция автосохранения.
- Пользователи могут получить доступ к версиям документов в приложении через Файл → Вернуться к → Просмотреть все версии…
- Версии файлов сохраняются в хранилище фрагментов.
- Версии документов доступны только на томах, отформатированных в HFS+ и APFS
- Скрытая директория .DocumentRevisions-V100 содержит папку с именем Period или All UID.
    - Подкаталоги имеют имена <UID>, которые уникальны для всех UID на системных томах
- Подкаталоги <UID> содержат подкаталоги, названные в обратном формате DNS:
    - **com.apple.documentVersions** содержит версии для документов, сохраненных на локальном томе
    - **com.apple.ubiquity** содержит версии для документов, сохраненных на локальном томе и iCloud
    - **com.apple.thumbnails** содержит версии для миниатюр QuickLook
    - **com.apple.genstore.info** содержит встроенный двоичный plist, который может включать имя хоста системы, в которой была создана версия.
- Каждая версия файла или поколение имеет расширенные атрибуты, связанные с “genstore”.
    - **com.apple.genstore.origdisplayname** или **com.apple.genstore.posixname** хранят имя файла для этого поколения
- Обратите внимание, что версии файлов будут отображаться размером в ноль байт, поскольку их содержимое хранится в Chunk Storage.

19. ИНФОРМАЦИЯ О СИСТЕМЕ И ПОЛЬЗОВАТЕЛЯХ

19.1. Пользовательские аккаунты

Описание:
У каждого пользователя и группы есть свой собственный файл plist.

Расположение:
- /private/var/db/dslocal/nodes/Default/users/
- /private/var/db/dslocal/nodes/Default/groups/

Примечания:
Файлы могут быть двоичными или XML-файлами plist в зависимости от версии операционной системы
- Для доступа к этим каталогам требуются права суперпользователя.
- Каждый файл plist содержит метку времени создания учетной записи, время последнего сброса пароля, имя пользователя и, возможно, связанный с ним адрес электронной почты.
- Временные метки хранятся в формате Unix Epoch.
- Значения временных меток **failedLoginCount** и **failedLogin**, по-видимому, не обновляются.

19.2. Пароли пользовательских аккаунтов

Описание:
Хэши паролей учетных записей пользователей хранятся локально. Формат и расположение этих хэшей менялись в разных версиях macOS.

Расположение:
macOS 10.7+:
- /private/var/db/dslocal/nodes/Default/users/*
  - Ключ ShadowHashData в plist файле содержит хэш пароля

macOS 10.6:
/private/var/db/shadow/hash/.state

Примечания:
- macOS 10.6 использует хэш с солью SHA1
- macOS 10.7 использует хэш с солью SHA512
- macOS 10.8+ использует хэш с солью SHA512 PBKDF2
- **John The Ripper** (https://github.com/openwall/john) and **Hashcat** (https://hashcat.net/hashcat/) поддерживают подбор паролей для всех этих хэшей

19.3. Удаленые пользовательские аккаунты

Описание:
Если какие-либо учетные записи пользователей были удалены в системе, они будут перечислены в plist файле с ключом "**deletedUsers**". Этот файл может и не быть, если ни одна учетная запись не была удалена.

Расположение:
macOS:
- /Library/Preferences/com.apple.preferences.accounts.plist

Примечания:
- Перечислены имя пользователя, UID, логин и дата удаления для каждой учетной записи
- При удалении учетной записи доступны три варианта для данных пользователя:
  - Сохраняется папка пользователя в файл DMG, который сохраняется в **/Users/Deleted Users/**
  - Домашнюю папка остается на месте
  - Папка с пользовательскими данными удаляется.

19.4. iCloud – Синхронизация Аккаунтов и Настроек

Описание:
Каждая учетная запись iCloud, синхронизированная с системой, будет записана в виде файла с iCloud Person ID в папке iCloud Accounts. Этот же каталог содержит ссылки с именами для каждого адреса электронной почты, связанного с учетной записью iCloud, которые указывают на соответствующий идентификатор пользователя iCloud для этой учетной записи. Настройки также синхронизируются между устройствами в папке SyncedPreferences.

Расположение:

macOS:

- ~/Library/Application Support/iCloud/Accounts/*
- ~/Library/SyncedPreferences/
- ~/Library/Containers//Data/Library/SyncedPreferences/

iOS:

- /private/var/mobile/Containers/…
- /private/var/mobile/Library/SyncedPreferences/

Примечания:

Каждое приложение, синхронизирующиеся с iCloud, имеет свой собственный plist в папке **SyncedPreferences**

19.5. Управление профилями устройств.

Описание:

Устройствами можно управлять с помощью корпоративных систем управления мобильными устройствами или настроек, передаваемых на устройство организацией или оператором связи. На этих устройствах установлен профиль конфигурации, в котором указаны разрешенные действия и ограничения. Профили подготовки позволяют запускать приложения без загрузки из App Store.

Расположение:

macOS:

• /private/var/db/ConfigurationProfiles/

iOS:

Профили конфигурации:

- /private/var/mobile/Library/ConfigurationProfiles/
- /private/var/mobile/Library/UserConfigurationProfiles/
- /private/var/containers/Shared/SystemGroup/systemgroup.com. apple.configurationprofiles
- ./containers/Shared/SystemGroup/systemgroup.com.apple. configurationprofiles

Профили подготовки:

- /private/var/MobileDevice/ProvisioningProfiles/

Примечания:

- Используйте команду “profiles” для извлечения подробной конфигурации
- Вредоносные программы и джейлбрейк могут использовать профили подготовки, а также законные MDM решения. Найдите названия приложений, временные метки и сертификаты разработчика.
- plist профилей подготовки:
    - **CreationDate** - дата, когда приложение было загружено в стороннем режиме.
    - **ExpirationDate** - будет показан через семь дней для бесплатной учетной записи разработчика или через 365 дней для платной учетной записи
    - **ProvisioningDevices** - показывает UDID для всех устройств, на которых также установлено это приложение

19.6. Загрузка, перезагрузка и выключение системы.

Описание:

System Log и Unified Logs содержат записи о загрузке, перезагрузке и выключение системы. Их полнота зависит от версии macOS

Расположение:

macOS 10.13.1+:

System Log

- Ищите “BOOT_TIME” и “SHUTDOWN_TIME” для соответствующих временных меток Unix Epoch

Unified Logs

- Сообщения, связанные с Центром уведомлений агента сеанса, показывают инициированные пользователем действия, относящиеся к событиям завершения работы системы

Примечания:

- Обратите внимание, что сообщения о завершении работы не записываются ни в один журнал в macOS с 10.12.0 по 10.12.2
- Ищите “halt” обозначающее завершения работы и “reboot” обозначающее презагрузку
- Система записывает причину перехода в спящий режим/завершения работы как “Sleep Cause” или “ Shutdown Cause”
    - <0 = ошибка
    - 0 = гибернация (спящий режим) или извлечение батареи/вилки питания (выключение)

  - 3 = жесткое выключение (удерживается кнопка питания)
  - 5 = обычный режим сна / выключение

19.7. KnowledgeC – Блокировка/Разблокировка устройства и подключение зарядки.

Описание:
Помимо всего прочего, база данных знаний отслеживает, когда устройство заблокировано или разблокировано, а также когда оно подключается или отключается от сети питания.

Расположение:
macOS:
- ~/Library/Application Support/Knowledge/knowledgeC.db

iOS:
- /private/var/mobile/Library/CoreDuet/knowedgeC.db

Примечания:
- Данные хранятся примерно 4 недели.
- Вы можете использовать следующие модули APOLLO:
  - **knowledge_device_locked** – извлекает события блокировки и разблокировки экрана
  - **knowledge_device_pluggedin** – Извлекает события связанные с подключением и отключение питания

19.8. CurrentPowerlog – Уровень зарядки АКБ

Описание:
CurrentPowerlog отслеживает состояние батареи устройства и происходит ли процесс зарядки.

Расположение:
macOS:
- /private/var/db/powerlog/Library/BatteryLife/CurrentPowerlog.PLSQL
- /private/var/db/powerlog/Library/BatteryLife/Archives/*

iOS:
- /private/var/Containers/Shared/SystemGroup//Library/ BatteryLife/CurrentPowerlog.PLSQL
- /private/var/Containers/Shared/SystemGroup//Library/ BatteryLife/Archives/*

Примечания:
- Данные содержатся примерно за 3 дня.
- Будьте внимательны к временным меткам- некоторые из нах могут иметь смещение.
- Используйте модуль **APOLLO** (https://github.com/mac4n6/APOLLO) **powerlog_battery_level** для извлечения данной информации.

19.9. Установленные принтеры и задания на печать

Описание:
Здесь указаны принтеры и сканеры, установленные в системе и их конфигурации

Расположение:
macOS:
- /Library/Preferences/org.cups.printers.plist
  - Каждый ключ элемента относится к установленному принтеру
- /etc/cups/ppd/*.ppd
  - По одному файлу на принтер; содержит такие возможности, как размер страницы, разрешение и цвет.

- /private/var/spool/cups/c#####
  - Управляющие файлы задания печати, содержащие метаданные о задании печати, с ID соответствующим имени файла.
  - Постоянные файлы

- /private/var/spool/cups/d#####
  - Файлы данных PDF отправленных на печать, названные в соответствии с соответствующим управляющим файлом
  - Непостоянные файлы – должны быть удалены сразу после того, как задание на печать завершено, если только оно не было отменено или не произошла ошибка.

Примечания:

- Подсказки в **uri** устройства, такие как **dnssd** или **tcp.local**, указывают на принтер, подключенный к сети (а не через проводной интерфейс)
- Файлы управления заданиями печати содержат информацию о том, какой принтер использовался, исходную учетную запись пользователя, название задания и используемое приложение.

19.10. Общий доступ к экрану и настройки удаленного входа в систему.

Описание:

Это настройки для элементов, к которым можно предоставить общий доступ, включая общий доступ к экрану и удаленный доступ к системе.

Расположение:

macOS:

Настройки:

- /private/var/db/com.apple.xpc.launchd/disabled.plist
- /private/var/db/launchd.db/com.apple.launchd/overrides.plist
- /Library/Preferences/com.apple.RemoteManagement.plist
    - Создается, когда включены параметры общего доступа к экрану или удаленного управления
- /Library/Preferences/com.apple.VNCSettings.txt
    - Содержит XOR пароль для доступа к системе через VNC

События, связанные с доступом к экрану:

- Unified Logs
    - Ищите “screensharingd”

Примечания:

disabled.plist/overrides.plist:

- По умолчанию все эти настройки выключены
- **com.apple.screensharing** = NO (0) – общий доступ к экрану включен
- **com.openssh.sshd** = NO (0) – удаленный доступ включен
- Если идентификатор пакета для службы не отображается в списке, скорее всего, она никогда не была включена

19.11. Конфигурация Firewall.

Описание:

Брандмауэр прикладного уровня (ALF) по умолчанию отключен. Это один из двух брандмауэров по умолчанию в системах Mac OS. Второй - брандмауэр фильтрации IP/пакетов.

Расположение:

macOS:

Конфигурация ALF :

- /Library/Preferences/com.apple.alf.plist
    - **globalstate** = 1 - брандмауэр включен, 0 - брандмауэр отключен
    - **allowsignedenabled** = 1 означает разрешить подписанному программному обеспечению получать входящие подключения
    - **allowdownloadsignedenabled** = 1 означает разрешить загруженному подписанному программному обеспечению получать входящие подключения
    - **stealthenabled** = 1 - включен скрытый режим
    - в разделе "приложения" перечислены приложения, настроенные в брандмауэре
        - 0 - входящие подключения разрешены, 2 - они заблокированы

В macOS версии 10.7 и выше конфигурация фильтра пакетов фаервола находится в **/etc/pf.conf**

Примечания:

-

19.12. Связка ключей.

Описание:

Цепочки ключей в системе используются для хранения конфиденциальных данных, таких как имена пользователей, пароли и ключи шифрования.

Расположение:

macOS:

- ~/Library/Keychains/login.keychain-db

iCloud:

- ~/Library/Keychains/<Hardware UUID>/keychain-2.db

- /Library/Keychains/System.keychainmn

iOS:

- /private/var/Keychains/keychain-2.db

iOS backup:

- keychain-backup.plist

Примечания:

- **login.keychain-db** - может содержать пароли пользователей для точек доступа, Time Machine, приложений и веб-сайтов. По умолчанию пароль доступа к нему – пароль учетной записи пользователя.
- **System.keychain** - содержит пароли для VPN, точек доступа, Time Machine и приложений.
- **keychain-2.db** находящийся в iCloud может содержать информацию о других устройствах Apple
- При резервном копировании iOS связка ключей может храниться в папке **Keychain** или **KeychainDomain**, в зависимости от используемого средства сбора.
- Просмотрите файл Связки ключей с помощью приложения **Keychain Access.app** для Mac OS

19.13. Учетные записи настроенные в всистеме.

Описание:

Пользователь может настроить различные учетные записи в системе, такие как электронная почта, календарь, iCloud и подобные.

Расположение:

macOS:

- /Library/Preferences/SystemConfiguration/com.apple.accounts.exists.plist

macOS 10.11 и ранее:

- ~/Library/Accounts/Accounts3.sqlite

macOS 10.12 и позже:

- ~/Library/Accounts/Accounts4.sqlite

iOS:

- [/private/var]/mobile/Library/Accounts/Accounts3.sqlite
- [/private/var]/Preferences/SystemConfiguration/com.apple.accounts.exists.plist

Примечания:

Таблица ZACCOUNT содержащаяся в базах данных sqlite содержит информацию об учетных записях:

  - ZUSERNAME - имя пользователя учетной записи
  - ZACCOUNTTYPEDESCRIPTION - описание типа учетной записи
  - ZDATE – когда было последнее обновление настроек учетной записи (в формате Mac Epoch)
  - ZKEY - имя ключа конфигурации
  - ZVALUE - значение конфигурации в виде BLOB, содержащего двоичный plist

com.apple.accounts.exists.plist содержит два связанных между собой ключа для каждого аккаунта:

  - **Exists** - используется ли учетная запись
  - **Count** - сколько существует учетных записей этого типа

19.14. Данные Apple Watch

Описание:

Если Apple Watch сопряжены с iPhone (они могут сопрягаться только с ним), некоторые данные от них будут синхронизированы с этим iPhone.

Расположение:

iOS:

- [/private/var]/mobile/Library/DeviceRegistry/<GUID>/DeviceRegistry.state/historySecureProperties.plist
  - Содержит в себе серийный номер устройства, IMEI, mac адреса wifi и bt.
- [/private/var]/mobile/Library/DeviceRegistry/<GUID>/*

Примечания:

-

20. ИСПОЛЬЗОВАНИЕ БРАУЗЕРА И ЗАГРУЗКА ФАЙЛОВ

20.1. Восстановление сессии браузера Safari

Описание:

Функции автоматического восстановления после сбоя встроенная в браузер.

Расположение:

macOS:

- ~/Library/Safari/LastSession.plist
- ~/Library/Containers/com.apple.Safari/Data/Library/Caches/com. apple.Safari/TabSnapshots/*
- ~/Library/Containers/com.apple.Safari/Data/Library/Caches/com.apple.Safari/TabSnapshots/Metadata.db
    - Связывает URL-адрес с именем файла моментального снимка (UUID) в папке Tab Snapshots

iOS:

- /private/var/mobile/Library/Safari/BrowserState.db
- /private/var/mobile/Containers/Data/Application//Library/ Safari/Thumbnails/*.ktx

iOS backup:

- /mobile/Library/Safari/BrowserState.db

Примечания:

- **LastSession.plist:**
    - Двоичный plist, содержащий историю вкладок с последнего сеанса просмотра
    - Если **SessionStateIsEncrypted** = 0 - состояние сеанса будет иметь встроенный двоичный plist содержащий историю вкладок.
- **BrowserState.db**:
    - Временные метки - в Unix Epoch формате.
    - **order_index** – показывает порядок размещения вкладок.
    - **private_browsing** – показывает режимы просмотра 0 – обычный, 1 – приватный.
    - **session_data** – содержит BLOB
- **Thumbnail KTX files:**
    - Каждый скриншот представляет собой предварительный просмотр вкладки, даже если она была открыта в приватном режиме.
    - Показаны только те вкладки, которые были открыты, когда Safari в последний раз переводился в фоновый режим.

20.2. История браузера Safari

Описание:

Это история посещенных пользователем веб-сайтов. Она может быть синхронизирована через iCloud, если это было заранее включено на устройствах.

Расположение:

macOS:

- ~/Library/Safari/History.db
- ~/Library/Safari/CloudTabs.db

iOS:

- [/private/var]/mobile/Library/Safari/History.db
- [/private/var]/mobile/Library/Safari/CloudTabs.db

Примечания:

History.db:

- В iOS эти данные хранятся в течение примерно одного месяца, в macOS по умолчанию - в течение примерно одного года (но могут быть изменены)
- Временные метки посещений хранятся в формате Mac Epoch.
- **Origin** = 0 означает, что посещение произошло на этом устройстве, 1 - эта запись
- была синхронизирована из другой системы через iCloud

20.3. Расширенные атрибуты скаченных файлов.

Описание:

Apple использует файловый карантин для проверки файлов на наличие вредоносных программ и информирования пользователей о том, откуда был загружен файл. Эта информация хранится в расширенных атрибутах файла.

Расположение:

Присутствуют везде.

• ls -l@

- **com.apple.quarantine** - данные карантина для загруженных файлов, включая время загрузки (Unix Epoch в hex) и приложение, используемое для загрузки файла

- **com.apple.metadata:kMDItemDownloadedDate** – показывает дату загрузки в формате NSDate
- **com.apple.metadata:kMDItemWhereFroms** - предоставляет URL, с которого был загружен элемент

Посмотреть расширенные атрибуты файла: **xattr -xl <имя файла>**

Примечания:
Не все браузеры могут создавать такие атрибуты. Их наличие зависит от разработчика браузера.

20.4. Расширенные атрибуты скаченных файлов.

Описание:
При загрузке вложений электронной почты создаются некоторые расширенные атрибуты.

Расположение:
Присутствуют везде.
• ls -l@
- **com.apple.metadata:com_apple_mail_dateReceived** - показывает дату получения письма
- **com.apple.metadata:com_apple_mail_dateSent** – показывает дату отправки письма
- **com.apple.metadata:com_apple_mail_isRemoteAttachment** – показывает удаленное ли вложение (0) или локальное (1)
- **com.apple.quarantine** – показывает время скачивания и приложение которое использовалось для этого.

Посмотреть расширенные атрибуты файла: **xattr -xl <имя файла>**

Примечания:
-

20.5. Safari Cookies

Описание:
Файлы cookie дают представление о том, какие веб-сайты были посещены и какие действия могли там происходить.

Расположение:
macOS:
- ~/Library/Cookies/Cookies.binarycookies

Примечания:
Cookies могут быть собраны при помощи инструмента **Safari Binary Cookie Parser** (https://github.com/mdegrazia/Safari-Binary- Cookie-Parser)

20.6. Кэш браузера Safari

Описание:
Файлы, кэшированные браузером, перечисляются в базе данных, а также хранятся на устройстве.

Расположение:
macOS:
- ~/Library/Containers/com.apple.Safari/Data/Library/Caches/com. apple.Safari/Cache.db
- ~/Library/Containers/com.apple.Safari/Data/Library/Caches/com. apple.Safari/WebkitCache/Version ##/*
    - **Records/SubResources** - папка содержит список кэшированных элементов для каждого посещения веб-сайта и встроенные хэши SHA1 для каждого файла
    - **Records/Resources** - папка содержит кэшированные данные и метаданные, включая хэш SHA1 имени файла для связанного файла BLOB в папке.

iOS:
- /private/var/mobile/Containers/Data/Application/<GUID>/Library/Caches/Cache.db
- /private/var/mobile/Containers/Data/Application/<GUID>/Library/Caches/WebKit/Version ##/*
    - **Records/SubResources** - папка содержит список кэшированных элементов для каждого посещения веб-сайта и встроенные хэши SHA1 для каждого файла
    - **Records/Resources** - папка содержит кэшированные данные и метаданные, включая хэш SHA1 имени файла для связанного файла BLOB в папке.

Примечания:
- Каждый кэшированный файл, указанный в базе данных sqlite **Cache.db**, имеет соответствующее местоположение и дату загрузки
- Кэшированные файлы можно сопоставить с их метаданными, используя значение entry_ID.

20.7. Кэш браузера Safari

Описание:

Браузер Safari включают в себя встроенный менеджер загрузок, ведущий историю каждого загруженного файла. Этот артефакт браузера может предоставить отличную информацию о посещенных веб-сайтах и соответствующих загруженных элементах.

Расположение:

macOS:

- ~/Library/Safari/Downloads.plist

iOS:

- /private/var/mobile/Containers/Data/Application/<Apple Safari GUID/Library/Safari/Downloads/Downloads.plist

Примечания:

- - По умолчанию этот список очищается каждый день. Пользователь может самостоятельно изменить это выбрав из нескольких вариантов очистки: “При завершении работы Safari”, “После успешной загрузки” или “Вручную”.
- - **DownloadEntryURL** macOS and **sourceURL** iOS – содержит URL-адрес источника загрузки
- **DownloadEntryPath** macOS – указывает куда именно был загружен файл.
- **DownloadEntryDateAddedKey** macOS and **DateAdded** iOS – показывает дату начала загрузки
- **DownloadEntryDateFinishedKey** (macOS) and **DateFinished** (iOS) – показывает дата завершения загрузки.

21. СЕТЕВЫЕ НАСТРОЙКИ

21.1. Сетевые интерфейсы

Описание:

Сетевые интерфейсы в системе, типы интерфейсов и Mac-адреса.

Расположение:

macOS:

- /Library/Preferences/SystemConfiguration/NetworkInterfaces.plist
- /Library/Preferences/SystemConfiguration/preferences.plist

iOS:

- /private/var/preferences/SystemConfiguration/ NetworkInterfaces.plist
- [/private/var]/preferences/SystemConfiguration/preferences.plist

Примечания:

• У каждого интерфейса есть ключ элемента в **NetworkInterfaces.plist**
  - SCNetworkInterfaceType - IEEE802.11 для беспроводных, Ethernet – для проводных интерфейсов
  - Также содержит модель устройства

21.2. Настройки DHCP

Описание:

Последние известные сетевые настройки, выданные сетевым интерфейсам по DHCP

Расположение:

iOS:

- [/private/var]/db/dhcpclient/leases/

Примечания:

• Каждый файл в этом каталоге содержит информацию об аренде, MAC-адрес маршрутизатора, IP-адрес и SSID для указанного интерфейса.

21.3. Настройки беспроводных сетей

Описание:

Здесь перечислены подключения к точкам доступа, включая настройки беспроводной сети. Сюда входят точки доступа, добавленные с помощью меню Wi-Fi и те, которые синхронизированы с другого устройства.

Расположение:

macOS 11+/iOS 14+:

- /Library/Preferences/com.apple.wifi.known-networks.plist

macOS версии 11 и ранее:

- /Library/Preferences/SystemConfiguration/com.apple.airport.preferences.plist iOS версии 13 и ранее:

- [/private/var]/preferences/SystemConfiguration/com.apple.wifi.plist

Примечания:

com.apple.wifi.known-networks.plist содержит:

- **AddReason** - какие данные были синхронизированы
- **AddedAt** - когда была добавлена определённая точка доступа
- **JoinedByUserAt** – временная метка, когда пользователь вручную подключался к точке доступа.
- **JoinedBySystemAt** – временная метка, когда подключение к точке доступа произошло автоматически.

Синхронизируемые настройки:
added_by – имя устройства, которое добавило эту точку доступа.
added_at - указывает время добавления этой точки доступа в файл .plist

21.4. Известные сети

Описание:

Известные сети — это те, с которыми система ранее установила соединение и которые были сохранены в памяти. Каждая сеть хранится в своем собственном ключе, который включает SSID и время последнего подключения.

Расположение:

macOS 10.15 и ранее:

- /Library/Preferences/SystemConfiguration/com.apple.airport.preferences.plist

iOS версии 13 и ранее:

- [/private/var]/preferences/SystemConfiguration/com.apple.wifi.plist

Примечания:

- Похоже, что данные для этого списка удаляются только с помощью действий пользователя.
- **CaptiveNetwork,** для которого установлено значение “ДА”, относится к всплывающим экранам, которые вы получаете в публичных общественных сетях.

21.5. Использование сети – Unified Logs

Описание:

Unified Logs содержат записи о сетевых подключениях, выполненных в системе..

Расположение:

macOS 10.12+, iOS 10+:

- Unified Logs

macOS 10.8+:

- System log

Примечания:

- Найдите отправителя “IPConfiguration” и где сообщение журнала содержит “Lease” или “network changed”
    - Используйте для этого команду: **log show –info –predicate 'senderImagePath contains[cd] "IPConfiguration" and (eventMessage contains[cd] "SSID" or eventMessage contains[cd] "Lease" or eventMessage contains[cd] "network changed")'**
- Найдите в журналах “configd”, “SSID” или “en0” для более подробного просмотра активности беспроводной сети
- Найдите в журналах “country code”, чтобы отобразить коды стран , связанные с подключениями к беспроводной точке доступа
    - Код по умолчанию “X0”, если он недоступен

Раздел 3.

КРИМИНАЛИСТИЧЕСКИЕ АРТЕФАКТЫ ANDROID

Поскольку экосистема Android достаточно фрагментирована, в этих шпаргалках будут указаны общие пути расположения файлов и их назначения, актуальные как как для текущих версий, так и предыдущих без сортировки по версиям.

Обратите внимание что после установки, приложение на устройстве:

- APK-файл хранится в разделе USERDATA в папке /app
- Данные самого приложения хранятся в разделе USERRDATA в папке /data
- В папке данных приложения для обозначения имени приложения используется имя пакета (например: org.telegram.messenger)
- Информация о установленных пакетах находится в файле **/data/com.android.vending/database/localappstate.db** представляющим из себя базу данных SQlite
- После установки приложение может запросить доступ к папке /media в разделе USERDATA

22. ИНФОРМАЦИЯ ОБ УСТРОЙСТВЕ.

22.1. Информация об устройстве.

Описание:
Информация об устройстве (версия, обновления и т.п.)

Расположение:
System
/build.prop

22.2. Настройки блокировки.

Описание:
Файлы, содержащие в себе информацию о способах блокировки устройства при помощи пинкода, графического ключа и биометрии.

Расположение:
Userdata
- /data/com.android.providers.settings/databases/settings.db
- /data/com.android.providers.settings/databases/settings.db-WAL
- /data/com.android.providers.settings/databases/locksettings.db
- /data/com.android.providers.settings/databases/locksettings.db-WAL
- /system/locksettings.db
- /system/locksettings.db-WAL

22.3. Настройки безопасности.

Описание:
Файлы, содержащие в себе информацию о способах блокировки устройства при помощи пинкода, графического ключа и биометрии.

Расположение:
Userdata
- /system/device_policies.xml
    - Содержит требования к паролям и политикам безопасности. Может содержать информацию о синхронизации.
- system/users/0/settings_secure.xml
    - Настройки безопасности

22.4. Календарь и временные зоны.

Описание:

Файлы, содержащие в себе информацию о способах блокировки устройства при помощи пинкода, графического ключа и биометрии.

Расположение:
Userdata

- /data/com.android.providers.calendar/databases/calendar.db
  - Элементы календаря и временные зоны.
- /system/netpolicy.xml
  - Временный зоны
- /Property/persist.sys.timezone
  - Временные зоны до Android 8
- /Property/persistent_properties
  - Временные зоны с версии Android 9

22.5. SIM карта.

Описание:
Файлы, содержащие информацию, связанную с использованием SIM карты

Расположение:
Userdata

- /data/com.google.android.gms/shared_prefs/Checkin.xml
  - Активности системы, связанные с установленной симкартой (Google аккаунт, ICCID и т.п.)
- /system/SimCard.dat
  - Данные симкарты и телефонный номер.

22.6. Google Сервисы.

Описание:
Настройки, связанные с использованием Google сервисов (Сетевые настройки, активные сервисы и тп)

Расположение:
Userdata

- /data/com.google.android.gsf/databases/gservices.db

22.7. Настройки.

Описание:
Различные параметры настроек системы.

Расположение:
Userdata

- /system/users/0/settings_global.xml
- /system/users/0/settings_system.xml

22.8. Сеть.

Расположение:
Userdata

- /data/com.android.connectivity.metrics/databases/events.db
  - Таблица базы данных **completed_events_request** содержит информацию о USB, BT, NFC и других соединениях
- /data/com.google.android.gms/databases/herrevad
  - Содержит информацию о беспроводных сетях и их mac адресах
- misc/wifi/WifiConfigStore.xml
  - Настройки беспроводных сетей
- /data/com.google.android.locations/files/cache.cell
- /data/com.google.android.locations/files/cache.wif
  - История подключений к сотовым сетям и wifi точкам доступа.

23. МЕССЕНДЖЕРЫ.

23.1. Skype.

Расположение:

/data/com.skype.raider/
- /databases/s4l-live:<User_ID>.db
- /files/live#3/eascache.db
- /files/live#3/main.db
- /files/live#3/qik_main.db
- /files/live#3/media_messaging/*

/media/
- /Pictures/Skype/*

Примечания:

Все базы данных в формате SQlite

23.2. Telegram.

Расположение:

/data/org.telegram.messenger/
- /cache/ *
- /files/cache4.db
- /shared_prefs/userconfig.xml

/media/
- /Android/data/org.telegram.messenger/cache/*
- /Pictures/Telegram/*
- /Telegram/

Примечания:

Все базы данных в формате SQlite

23.3. Viber.

Расположение:

/data/com.viber.voip/
- /databases/viber_data
- /databases/viber_messages
- /databases/viber_prefs
- /shared_prefs/ com.viber.voip.ViberPrefs.xml

/media/
- /Android/data/com.viber.voip/cache/*
- /Pictures/Viber/*
- /Viber/*

Примечания:

Все базы данных в формате SQlite

23.4. WeChat.

Расположение:

/data/com.tencent.mm/
- /MicroMsg/<User_ID>/EnMicroMsg.db
- /MicroMsg/<User_ID>/ SnsMicroMsg.db

/media/
- /Tencent/MicroMsg/ *

Примечания:

Все базы данных в формате SQlite

23.5. WhatsApp.

Расположение:

/data/com.whatsapp/
- /databases/ axolotl.db
- /databases/ chatsettings.db
- /databases/ location.db

- /databases/ media.db
- /databases/ msgstore.db
- /databases/ wa.db
- /files/Avatars/ *
- /files/Logs/
- /shared_prefs/ com.whatsapp_preferences.xml
- /shared_prefs/ RegisterPhone.xml

/media/

- /WhatsApp/Backups/*
- /WhatsApp/Databases/*
- /WhatsApp/Media/*

Примечания:

- Все базы данных в формате SQlite
- Резервные копии содержатся в виде баз данных SQlite
- Лог файлы – в виде простого текста.

23.6. Wikr.

Расположение:

- /data/com.mywickr.wickr2/
  /cache/dec/ *
- /databases/ wickr_db

Примечания:

- Все базы данных в формате SQlite

23.7. Signal.

Расположение:

/data/org.thoughtcrime.securesms/

- /cache/log/ *
- /databases/signal.db
- /files/avatars/ *
- /shared_prefs/org.thoughtcrime.securesms_preferences.xml
- /shared_prefs/ SecureSMS-Preferences.xml

/media/
/Signal/*

Примечания

- Все базы данных в формате SQlite
- Логи – в виде текста
- Папка /files/avatars/ содержит JPG аватарок пользователей из записной книги

23.8. Line.

Расположение:

/data/jp.naver.line.android/

- /databases/call_history
- /databases/ naver_line
- /databases/ read_notification
- /databases/ search.sqlite

/media/

- /Pictures/LINE/ *

Примечания

- Все базы данных в формате SQlite

23.9. Facebook Messenger.

Расположение:

/data/com.facebook.orca/

- /app_light_prefs/ logged_in_<User_ID>

- /cache/audio/ *
- /cache/fb_temp/ *
- /cache/image/ *
- /databases/ call_logs_db
- /databases/ contacts_db2
- /databases/ omnistore_<User_ID>_v01.db
- /databases/ prefs_db
- /databases/ threads_db2
- /databases/ tican_db_<User_ID>
- /files/image/ *
- /files/ExoPlayerCacheDir/ *
- /shared_prefs/ com.facebook.orca_preferences.xml

/media/

- /Pictures/Messenger/*

Примечания

- Все базы данных в формате SQlite

23.10. Wire.

Расположение:

/data/com.wire/

- /databases/<User_ID>
- /files/assets/*
- /shared_prefs/com.wire.preferences.xml

Примечания

- Все базы данных в формате SQlite

23.11. Zoom.

Расположение:

- /data/us.zoom.videomeetings/
- /data/<User_ID>@xmpp.zoom.us/ <User_ID>@xmpp.zoom.us.asyn.db
- /data/<User_ID>@xmpp.zoom.us/ <User_ID>@xmpp.zoom.us.db
- /data/<User_ID>@xmpp.zoom.us/ <User_ID>@xmpp.zoom.us.idx.db
- /data/<User_ID>@xmpp.zoom.us/ <User_ID>@xmpp.zoom.us.sync.db
- /data/zoommeeting.db
- /data/zoomus.db

Примечания

- Все базы данных в формате SQlite

24. СОЦИАЛЬНЫЕ СЕТИ.

24.1. Facebook.

Расположение:

/data/com.facebook.katana/

- /app_compactdisk/*
- /app_light_prefs/ logged_in_<User_ID>
- /cache/compactdisk/ *
- /cache/org.chromium.android_webview/ *
- /databases/admined_pages_db
- /databases/bookmarks_db2
- /databases/contacts_db2
- /databases/data_usage_db
- /databases/events.db
- /databases/fb.db
- /databases/local_media_db
- /databases/nearbytiles_db
- /databases/newsfeed.db

- /databases/omnistore_<User_ID>_v01.db
- /databases/prefs_db
- /databases/search_bootstrap_db
- /databases/threads_db2
- /databases/time_in_app_<User_ID>.db
- /databases/uploadmanager.db
- /files/ExoPlayerCacheDir/ *
- /shared_prefs/com.facebook.orca_preferences.xml

/media/

- /DCIM/Facebook/*

24.2. Instagram.

Расположение:
/data/com.instagram.android/

- /cache/ ManifestFeed-<User_ID>.json
- /cache/ tmp_photo_*.jpg
- /cache/images/ *
- /cache/original_images/ *
- /databases/ contacts_db2
- /databases/ direct.db
- /databases/ fileregistry.db
- /databases/ time_in_app_<User_ID>.db
- /databases/ transactions.db
- /files/music/ *
- /files/pending_media_images/ *
- /files/rendered_videos/ *
- /shared_prefs/ <User_ID>.xml
- /shared_prefs/ <User_ID>_USER_PREFERENCES.xml
- /shared_prefs/ <User_ID>_usersBootstrapService.xml
- /shared_prefs/ com.instagram.android_preferences.xml

/media/

- /Movies/Instagram/ *
- /Pictures/Instagram/ *

Примечания

- Все базы данных в формате SQlite
- Изображения хранятся в jpeg формате
  Для получения доступа к папке необходимы root права

24.3. Instagram.

Расположение:
/data/com.zhiliaoapp.musically/

- /databases/<User_ID>_im.db
- /databases/aweme.db
- /databases/downloader.db
- /databases/db_im_xx
- /databases/TIKTOK.db
- /databases/video.db
- /files/ *
- /shared_prefs/aweme_user.xml

/media/

- /Android/data/com.zhiliaoapp.musically/cache/
- /Android/data/com.zhiliaoapp.musically/files/

Примечания

- Все базы данных в формате SQlite

24.4. Linkedin.

Расположение:
/data/com.linkedin.android/
- /databases/ linkedin_messenger.db
- /databases/ linkedin.db
- /databases/ linkedin_search.db
- /files/sso/ profile_pic.png
- /shared_prefs/ linkedInPrefsName.xml

Примечания
- Все базы данных в формате SQlite

25. ОБЛАЧНЫЕ ХРАНИЛИЩА И ОБМЕН ФАЙЛАМИ.

25.1. Google Drive.

Расположение:
/data/com.google.android.apps.docs/
- /app_cello/<User_Email>/ cello.db
- /cache/<User_ID>/ TopNContactsGrpc*.dat
- /cache/docs_glide/ *
- /databases/DocList.db
- /shared_prefs/GoogleDriveSharedPreferences.xml
- /shared_prefs/webview.xml

Примечания
- Все базы данных в формате SQlite
- База данных TopNContactsGrpc*.dat представляет из себя JSON файл.

25.2. OneDrive.

Расположение:
/data/com.microsoft.skydrive/
- /databases/metadata
- /databases/AriaStorage.db
- /files/aria/*

Примечания
- Все базы данных в формате SQlite

25.3. Dropbox.

Расположение:
/data/com.dropbox.android/
- /databases/ <User_ID>-db.db
- /databases/ <User_ID>-prefs.db
- /databases/ db.db
- /databases/ prefs.db
- /shared_prefs/ DropboxAccountPrefs.xml
- /shared_prefs/ DropboxPersistentPrefs.xml

Примечания
- Все базы данных в формате SQlite

25.4. SHAREit.

Расположение:
/data/com.lenovo.anyshare.gps/
/databases/ download.db
/databases/ history.db
/databases/ sharead.db
/shared_prefs/ Settings.xml

/media/
/SHAREit/ *

Примечания

- Все базы данных в формате SQlite

26. ПОЧТОВЫЕ СЕРВИСЫ.

26.1. Gmail.

Расположение:

/data/com.google.android.gm/

- /cache/<User_ID>/ TopNContactsGrpc*.dat
- /cache/org.chromium.android_webview/ *
- /cache/ <имя файла>.attachment
- /databases/<Email_Address>.db
- /databases/bigTopDataDB.-<User_ID>
- /databases/EmailProvider.db
- /databases/metadata.-<User_ID>
- /files/downloads/ *
- /shared_prefs/Gmail.xml
- /shared_prefs/MailAppProvider.xml

Примечания

- Все базы данных в формате SQlite
- База данных TopNContactsGrpc*.dat представляет из себя JSON файл.

26.2. Outlook.

Расположение:

/data/com.microsoft.office.outlook/

- /databases/ accompliAcct.db
- /databases/ acompli.db

Примечания

- Все базы данных в формате SQlite

26.3. ProtonMail.

Расположение:

/data/com.protonmail/

- /databases/ <User_ID>-AttachmentMetadataDatabase.db
- /databases/ <User_ID>-ContactsDatabase.db
- /databases/ <User_ID>-MessagesDatabase.db
- /databases/ <User_ID>-NotificationsDatabase.db
- /databases/ <User_ID>-PendingActionsDatabase.db
- /databases/ <User_ID>-UnreadCountersDatabase.db
- /files/ProtonMail/emb_att/ *
- /shared_prefs/ ch.protonmail.android_preferences.xml

Примечания

- Все базы данных в формате SQlite

27. GOOGLE ОФИС.

27.1. Google Docs.

Расположение:

/data/com.google.android.apps.docs.editor/

- /cache/docs_glide/ *
- /databases/ DocList.db
- /databases/ Storage.db
- /files/stashes/ *
- /shared_prefs/ GoogleDriveSharedPreferences.xml

Примечания

- Все базы данных в формате SQlite

27.2. Google Calendar.

Расположение:
/data/com.google.android.calendar/
- /databases/cal_v2a
- /databases/timelydata.db
- /files/notification_logs/*.log
- /files/sync_logs/*.log
- /shared_prefs/com.google.android.calendar_preferences.xml

Примечания
- Все базы данных в формате SQlite
- Лог файлы – в текстовом формате

27.3. Google Keep.

Расположение:
/data/com.google.android.keep/
- /cache/image_manager_disk_cache/*
- /shared_prefs/com.google.android.keep_preferences.xml

Примечания
- Все базы данных в формате SQlite
- Лог файлы – в текстовом формате

28. МУЛЬТИМЕДИА.

28.1. Google Photos.

Расположение:
/data/com.google.android.apps.photos/
- /cache/<User_ID>/TopNContactsGrpc*.dat
- /cache/glide-cache/*
- /databases/gphotos0.db
- /databases/gphotos-1.db
- /databases/local_trash.db
- /databases/media_store_extras
- /shared_prefs/accounts.xml

Примечания
- Все базы данных в формате SQlite
- База данных **TopNContactsGrpc*.dat** представляет из себя JSON файл.

28.2. YouTube.

Расположение:
/data/com.google.android.youtube/
- /cache/*.cache
- /databases/ identity.db

Примечания
- Все базы данных в формате SQlite

29. ИНТЕРНЕТ БРАУЗЕРЫ.

29.1. Google Chrome.

Расположение:
/data/com.android.chrome/
- /app_chrome/Default/ *
- /app_tabs/ *
- /shared_prefs/ com.android.chrome_preferences.xml

29.2. Firefox.

Расположение:

/data/org.mozilla.firefox/
- /cache/<ID>.default/cache2/entries/*
- /cache/mozac_browser_icons/icons/*
- /cache/mozac_browser_thumbnails/thumbnails/*
- /databases/logins.sqlite
- /databases/top_sites
- /files/mozilla/<ID>.default/*
- /files/places.sqlite

Примечания
- Все базы данных в формате SQlite
- Иконки и превью страниц – в виде JPG

29.3. Microsoft Edge.

Расположение:

/data/com.microsoft.emmx/
- /app_chrome/Default/*
- /cache/Cache/*
- /databases/BingSearchHistory.db
- /shared_prefs/com.microsoft.emmx_preferences.xml

29.4. Opera.

Расположение:

/data/com.opera.browser/
- /app_opera/*
- /cache/cache/*
- /shared_prefs/recent_searches.xml

29.5. Tor Браузер.

Расположение:

/data/org.torproject.torbrowser/
- /app_torservice/.tor/ state
- /files/mozilla/<ID>.default/

/media/
- /Android/data/org.torproject.torbrowser/files/*

СПАСИБО ВСЕМ, КТО ПОДДЕРЖАЛ ПРОЕКТ
ШПАРГАЛОК НА КАНАЛАХ

T.ME/BEHOLDERISHEREHUB
И
T.ME/FORENSICTOOLS

ПРОДОЛЖЕНИЕ СЛЕДУЕТ…