« Снятие дампа ЖМД, сбор артефактов с ЖМД, анализ журналов событий Windows »

Новосибирск 2023

Оглавление

1. Снятие дампа ЖМД..... 3
2. Сбор основных артефактов с ЖМД. 10
3. Анализ журналов событий ОС Windows 12
Домашнее задание..... 17
Полезные ссылки..... 18

1. Снятие дампа ЖМД

Приступим к изучению порядка снятия дампа ЖМД.

Для снятия дампов ЖМД с ОС Windows мы будем использовать уже знакомый нам FTK Imager.

Порядок снятия дампа, следующий:

Выберем источник для исследования. Для этого нажмем кнопку «*Add evidence item*» в появившемся меню выберите пункт «Physical Drive» и нажмите «Далее». Данный пункт означает, что в качестве источника будет выбран физический диск (другие варианты позволяют выбрать логический диск, образ диска .iso, или какую-либо директорию на диске) (рисунок 1).

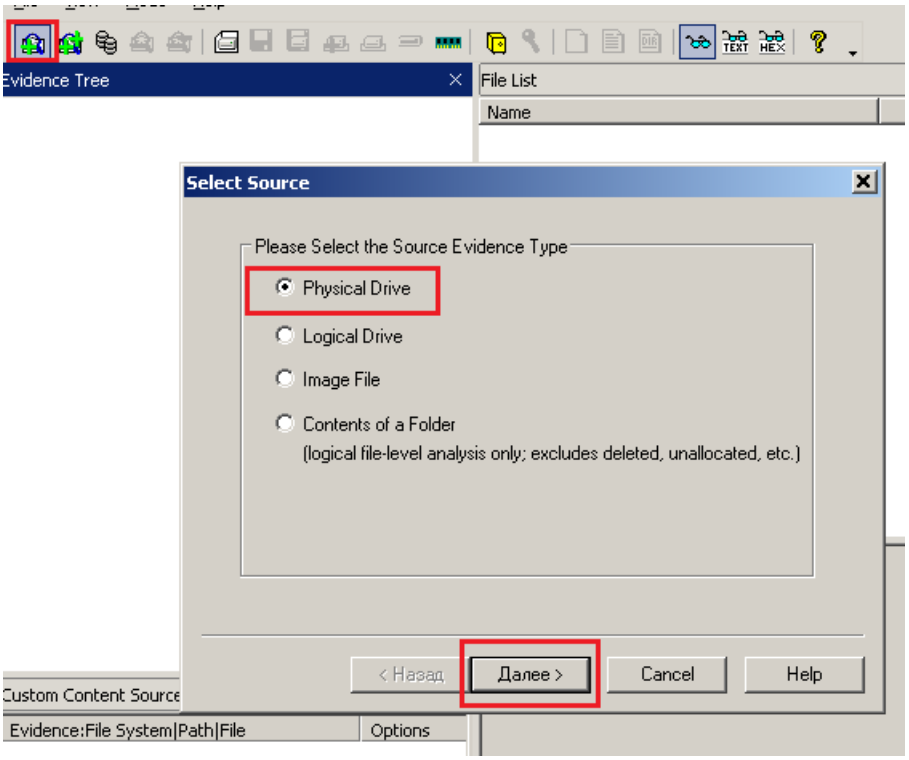

Рисунок 1 - Выбор источника для исследования

В следующем меню выберите устройство из списка и нажмите «Finish» (Рисунок 2).

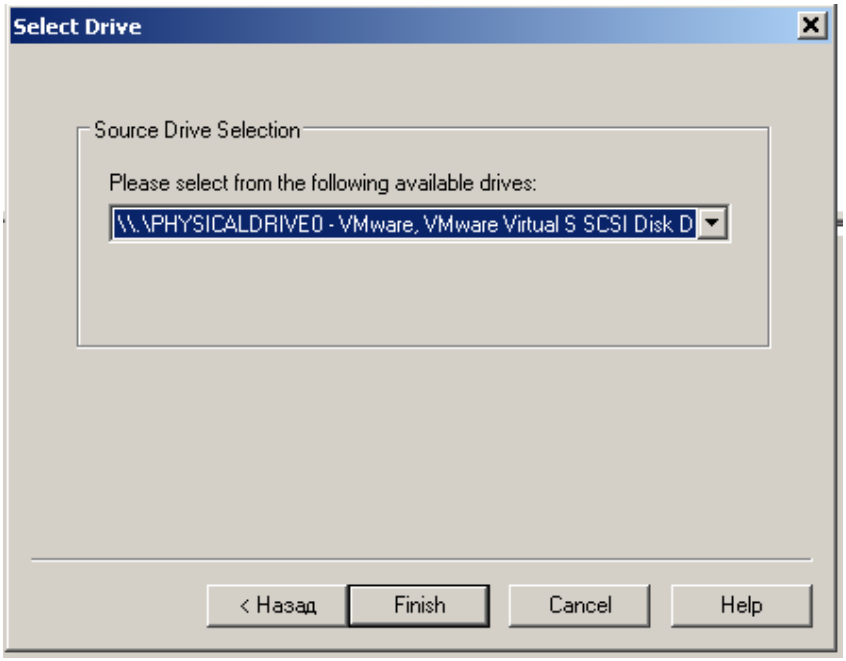

Рисунок 2 - Выбор источника для исследования

В результате в FTK Imager будут подгружены данные с ЖМД (рисунок 3).

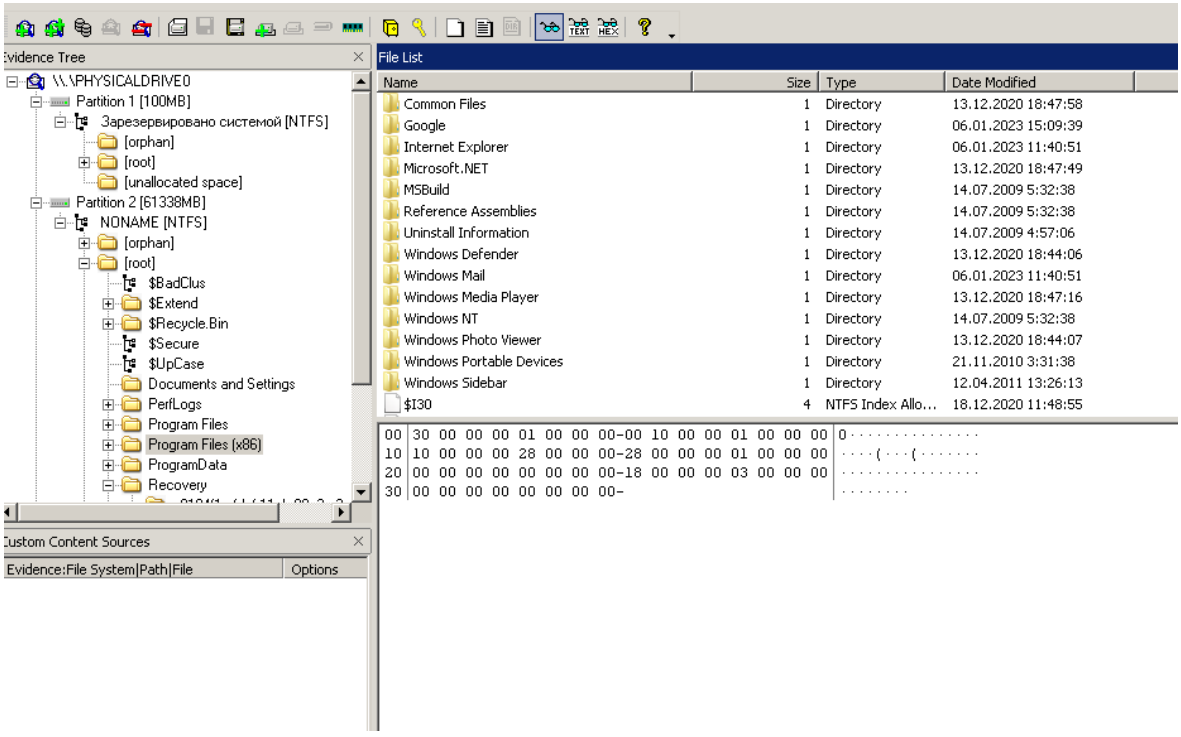

Рисунок 3 – Источник подгружен

Начнем снятие дампа, в меню выберите «Create Disk Image» (Рисунок 4).

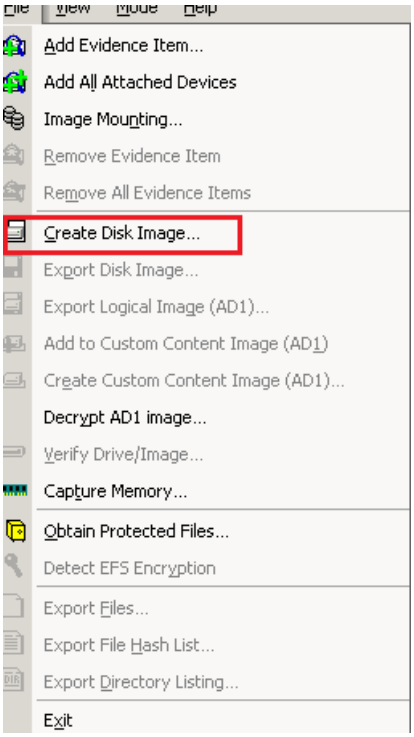

Рисунок 4 – Кнопка создания образа диска

Нас попросят снова повторить выбор устройства, затем необходимо будет указать куда сохранять дамп (Рисунок 5) для этого нажмите кнопку «Add».

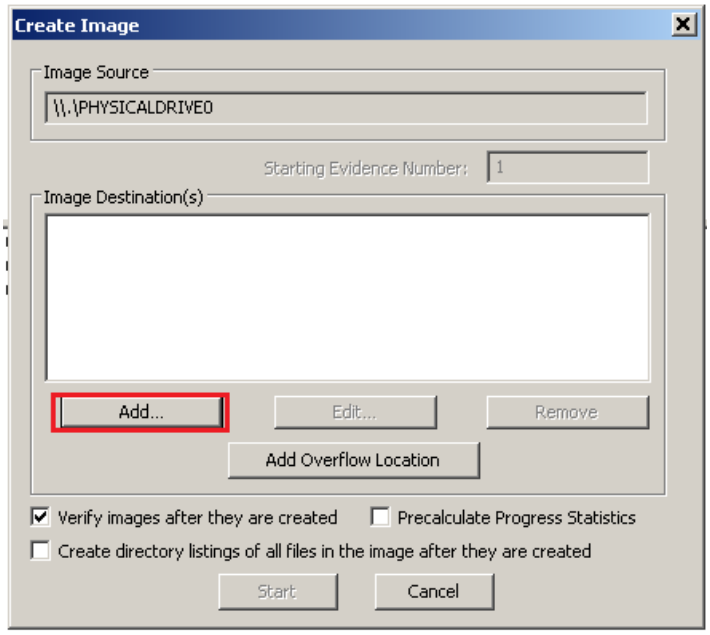

Рисунок 5 – Выбор места сохранения дампа

После нас попросят выбрать тип дампа (Рисунок 6). **Raw (dd)** – это дамп в чистом виде (сырой); **SMART** – специальный тип, уже давно не используется; **E01, AFF** – специальные типы, содержат дополнительную информацию об образе из FTK Imager (в целом особого смысла для нашей задачи неимеют).

Выберите Raw(dd), нажмите «Далее».

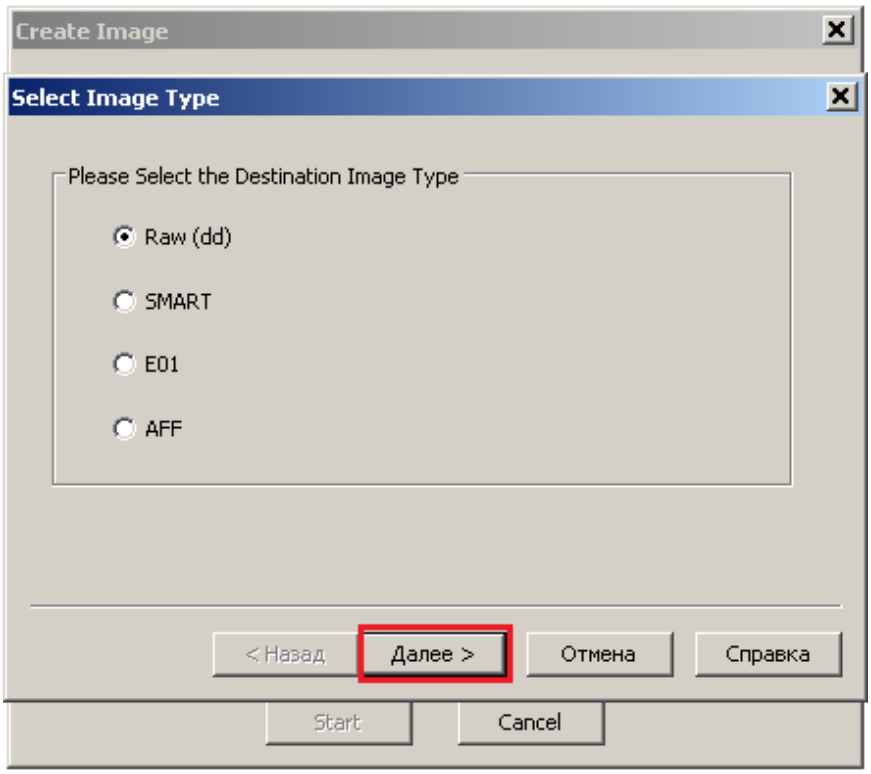

Рисунок 6 – Выбор типа дампа

Далее необходимо будет заполнить информацию о дампе но можете и ничего не писать, затем нажмите «Далее» (Рисунок 7).

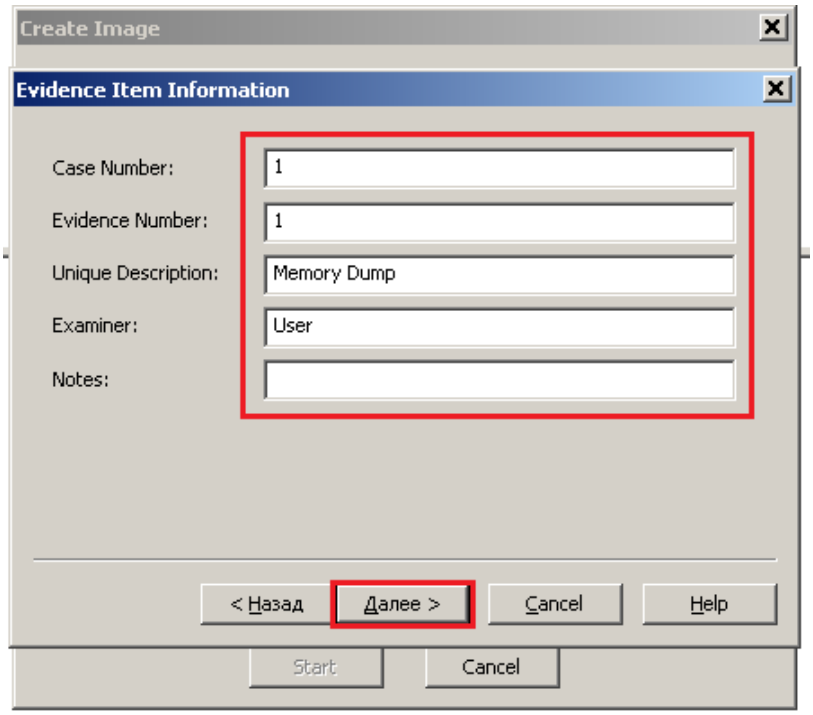

Рисунок 7 – Дополнительная информация о дампе

Теперь вам предложат выбрать место сохранения дампа и его имя и размер фрагмента (рекомендуется оставить 0 –не фрагментировать) (рисунок 8), выберите и нажмите «Finish».

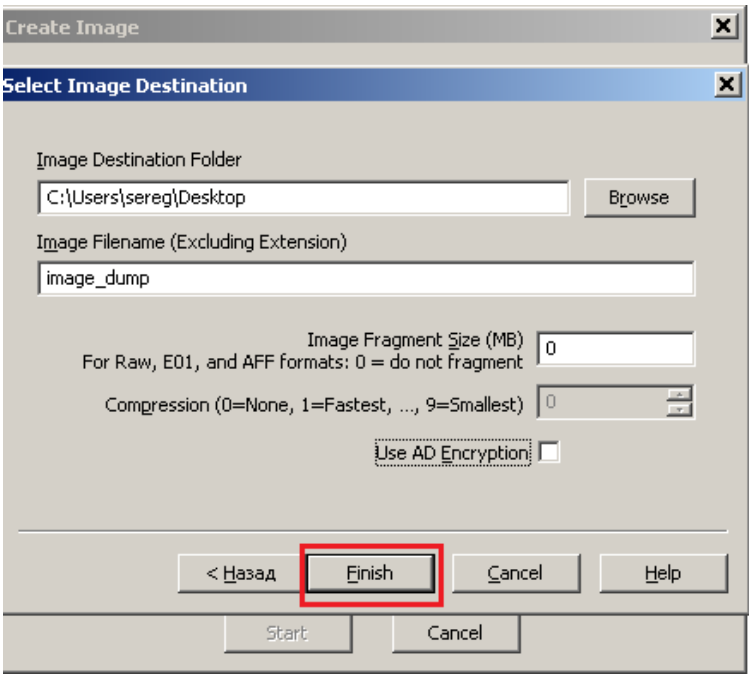

Рисунок 8 – Место сохранения и имя дампа

Немного подождем и дамп ЖМД снят. Рассмотрим снятие дампа ЖМД с ОС Linux.

Первоначально необходимо получить список всех разделов, выполним команду (рисунок 9):

fdisk -l

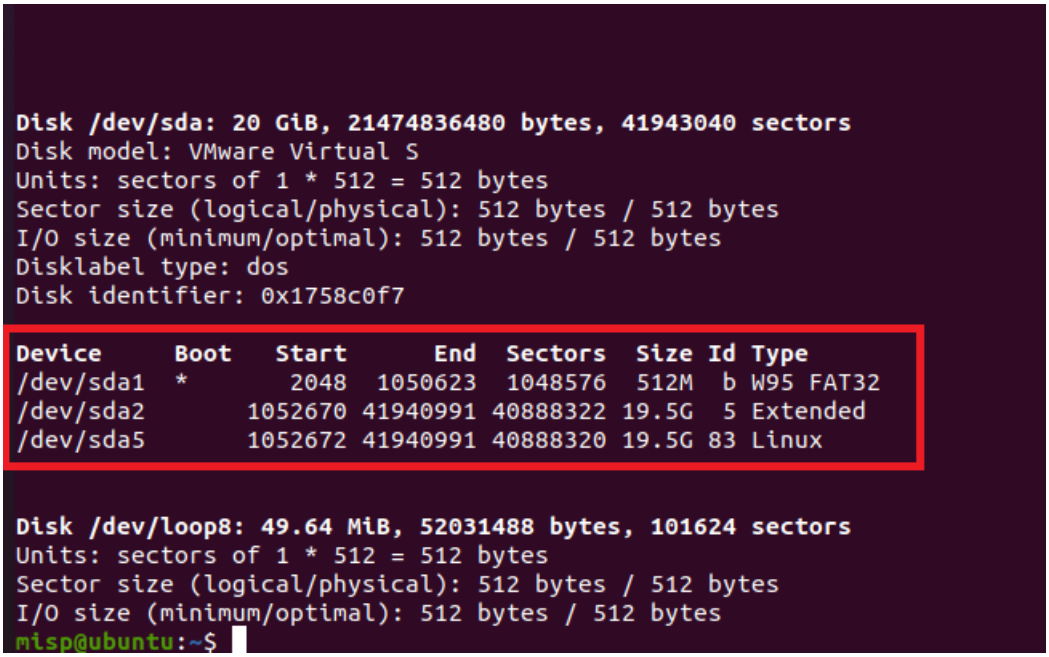

Рисунок 9 – Список разделов

Для снятия дампа будем использовать утилиту dcfldd, она устанавливается из репозитория Debian командой:

sudo apt install dcfldd

Пример выполнения команды:

dcfldd if=/dev/sda1 hash=md5

of=/media/forensic_disk_image.dd bs=512 noerror

, где if= – указывает на устройство, дамп которого необходимо снять; of – указывает на расположение выходного файла, hash – алгоритм контроля целостности, bs – размер кластера диска, с которого снимаем дамп noerror – не обращать внимания на ошибки при создании дампа.

Итак, вы изучили способы снятия дампа ЖМД с ОС семейства Windows и Linux. Теперь рассмотрим работу с основными артефактами ОС Windows.

2. Сбор основных артефактов с ЖМД.

Для анализа ЖМД будем также использовать утилиту FTK Imager.

Будет удобно сначала сделать таблицу с названием основных артефактов и их местом нахождения, после чего поочередно разберем их. Полный список всех возможных артефактов (как полезных так и не очень) находится тут.

Таблица 1. Основные артефакты ОС Windows

№	Название	Тип	Место нахождения
1	Master File Table	Файл	[root]\
2	UsnJrnl		[root]\$Extend\$UsnJrnl\ (скопировать $j)
3	Prefetch		[root]\Windows\Prefetch (копировать всю папку)
4	JumpLists		[root]\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations (+CustomDestinations)
5	LNK файлы		[root]\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Recent (копировать все lnk файлы)
6	Журналы событий		[root]\Windows\System32\winevt\Logs (копировать всю папку)
7	hiberfil.sys		[root]\Windows\
8	SAM	Куст реестра	[root]\Windows\System32\config (лучше дампить всю папку)
9	SECURITY		[root]\Windows\System32\config
10	SOFTWARE		[root]\Windows\System32\config
11	SYSTEM		[root]\Windows\System32\config

Будет полезно также снять копию всей папки пользователя ([root]\Users\%USERNAME%\).

Теперь обо всем по-порядку:

Master File Table – это один из ключевых элементов файловой системы NTFS, содержащий служебную информацию обо всех файлах в системе. **Для расследования значимыми являются время создания и изменения файла**.

UsnJrnl – это журнал выполняемых действий в файловой системе. Соответственно, он **позволяет восстановить алгоритм действий злоумышленника в файловой системе**.

Prefetcher – это компонент ОС Windows, ускоряющий процесс загрузки ОС и запуска программ. Файлы **Prefetch** позволяют выявить **факты и время вредоносной активности в системе.**

JumpLists – специализированная функция ОС Windows, позволяющая получить быстрый доступ к недавно открытым файлам и запущенным приложениям. Информация **JumpLists** полезна при выявлении действий пользователя или злоумышленника в системе, **так как хранит информацию о временных метках работы с приложениями**.

LNK-файлы – это ссылки на программы и файлы, размещенные в другом месте файловой системы. Они могут создаваться как самой ОС, так и пользователями. **Это полезный источник информации о файлах, которые раньше использовались в системе**.

hiberfil.sys – это файл гибернации (образ ОП записанный на ЖМД). Анализ образов ОП мы уже рассматривали.

В ходе занятия мы использовали ручной способ сбора артефактов с ЖМД. Однако, есть некоторые программы, автоматизирующие их сбор, к примеру: IRTriage, CyLR. В реальной работе время очень ценно. Вы можете воспользоваться этими программами, а можете найти (или написать) свое

решение.

3. Анализ журналов событий ОС Windows

Рассмотрим журналы событий в ОС Windows (таблица 2):

Таблица 2. Основные журналы аудита ОС Windows

№	Название	Описание
1	Application	Журнал, содержащий информацию о работе приложений, функционирующих в системе
2	Security	Журнал, содержащий события безопасности системы
3	System	Журнал, содержащий события, зарегистрированные системными компонентами Windows
4	Setup	Журнал, содержащий сведения об установке приложений
5	HardwareEvents	Журнал, содержащий события, генерируемые аппаратными компонентами и устройствами

Наибольшее внимание при анализе стоит обратить на журнал Security, его основные события представлены в таблице 3:

Таблица 3. Основные события журнала Security

ID события	Описание
4768	Успешная аутентификация доменного пользователя
4771	Неудачная аутентификация доменного пользователя
4624	Успешная аутентификация локального пользователя
4625	Неудачная аутентификация локального пользователя

4672	Успешная аутентификация с правами локального администратора
4634, 4647	Выход пользователя из системы
4778	Подключение (переподключение) по RDP
4779	Отключение от RDP-сессии
4720	Создание новой учетной записи пользователя
4742	Изменение учетной записи пользователя
4726	Удаление учетной записи пользователя
4698	Создано запланированное событие
4700	Запланированное событие активировано
4688	Создан новый процесс
1102	Очистка журнала

Основные события журнала System представлены в таблице 4.

Таблица 4. Основные события журнала System

ID события	Описание
7045, 4697	Создание службы
7036	Запуск или остановка службы
7034	Аварийная остановка службы
20001	Установка драйвера устройства
104	Очистка журнала событий

В ОС Windows присутствуют также Operational-журналы аудита. Их достаточно много, мы рассмотрим наиболее интересные для анализа.

Таблица 5. Operational-журналы ОС Windows

№	Название	Описание
1	PowerShell-Operational	Журнал, содержащий информацию о функционировании PowerShell
2	NetworkProfile-Operational	Журнал, содержащий информацию о подключении к сетям
3	GroupPolicy-Operational	Журнал, содержащий события, связанные с взаимодействием с групповыми политиками безопасности
4	Bits-Client-Operational	Журнал, содержащий сведения, связанные с работой Background Intelligence Transfer Service
5	DriverFrameworks-UserMode-Operational	Журнал, содержащий события, связанные с взаимодействием с внешними устройствами

Рассмотрим основные события журнала PowerShell- Operational (таблица 6).

Таблица 6. Основные события журнала PowerShell- Operational

ID события	Описание
4103	Выполнение сценария PowerShell (с сохранением пользовательского контекста)
4104	Выполнение сценария PowerShell (без сохранения пользовательского контекста)

Рассмотрим основные события журнала NetworkProfile- Operational (таблица 7).

Таблица 7. Основные события журнала PowerShell- Operational

ID события	Описание
10000	Установка соединения с сетью

Рассмотрим основные события журнала GroupPolicy- Operational (таблица 8).

Таблица 8. Основные события журнала GroupPolicy- Operational

ID события	Описание
4016	Начало обработки объектов групповой политики безопасности
5016	Окончание обработки объектов групповой политики безопасности
5312	Перечень объектов групповой политики безопасности, которые будут применены

Рассмотрим основные события журнала Bits-Client- Operational (таблица 9).

Таблица 9. Основные события журнала Bits-Client-Operational

ID события	Описание
3	Создание задания службы BITS
59	Запуск задания службы BITS
60	Статус задания службы BITS
4	Окончание задания службы BITS

Рассмотрим основные события журнала Bits-Client- Operational (таблица 10).

Таблица 10. Основные события журнала DriverFrameworks- UserMode-Operational

ID события	Описание
1003, 1004, 2000, 2001, 2003, 2004, 2005, 2006, 2010, 2100, 2101, 2105, 2016	Подключение USB-устройства

1006, 1008, 2100, 2101, 2102, 2105, 2106, 2900, 2901	Отключение USB-устройства

Больше событий с их описанием можно найти вот тут.

Домашнее задание

1. Снимите дамп жесткого диска **ВМ из 3 ЛР**, при помощи утилиты *dcfldd*. Откройте получившийся дамп при помощи FTK Imager, соберите 1-2 артефакта (все не нужно, так как процесс аналогичный).

2. Вам будет дан образ с уже собранными артефактами, а также ПО, необходимым для анализа. Проведите анализ журналов **Security, System, PowerShell-Operational, NetworkProfile-Operational, GroupPolicy-Operational, Bits-Client-Operational**. Рассмотрите также журналы ОС Windows, которые не рассматривались в ходе занятия.

Полезные ссылки

https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/ - энциклопедия с кодами событий Windows

https://www.makeuseof.com/windows-10-jump-lists-guide/ - статья про JumpLists

https://github.com/AJMartel/IRTriage - вариант автоматизации сбора артефактов

https://github.com/orlikoski/CyLR - вариант автоматизации сбора артефактов