ВВЕДЕНИЕ В КИБЕРБЕЗ

Цифровая криминалистика

Что такое Форензика?

Форензика

Форензика (digital forensics) — это раздел *информационной безопасности*, занимающийся исследованием цифровых устройств и данных с целью выяснения обстоятельств *компьютерных инцидентов, кибератак, преступлений, мошенничества и других нарушений*

Форензика

Благодаря форензике эксперты могут:

- Расследовать киберпреступления
- Собирать доказательства для суда
- Восстанавливать удалённые или повреждённые данные
- Анализировать утечки информации
- Определять источник атаки (**атрибуция**)

Этапы расследования

Этапы расследования

Как и везде, в форензике расследование проходит по определенным этапам:

- **Идентификация:**
  > Что произошло? (взлом, вирус, утечка)
  > Какие устройства или системы затронуты?
- **Сбор данных**
  > Сохраняем "цифровую сцену преступления"
  > Не допускаем изменений в исходных данных
  > Используем write blocker (аппаратную защиту от записи)
- **Сохранение доказательств (imaging)**
  > Создание битовой копии носителя (диска, телефона)
  > Контроль целостности с помощью хеш-функций (MD5, SHA256)

Этапы расследования

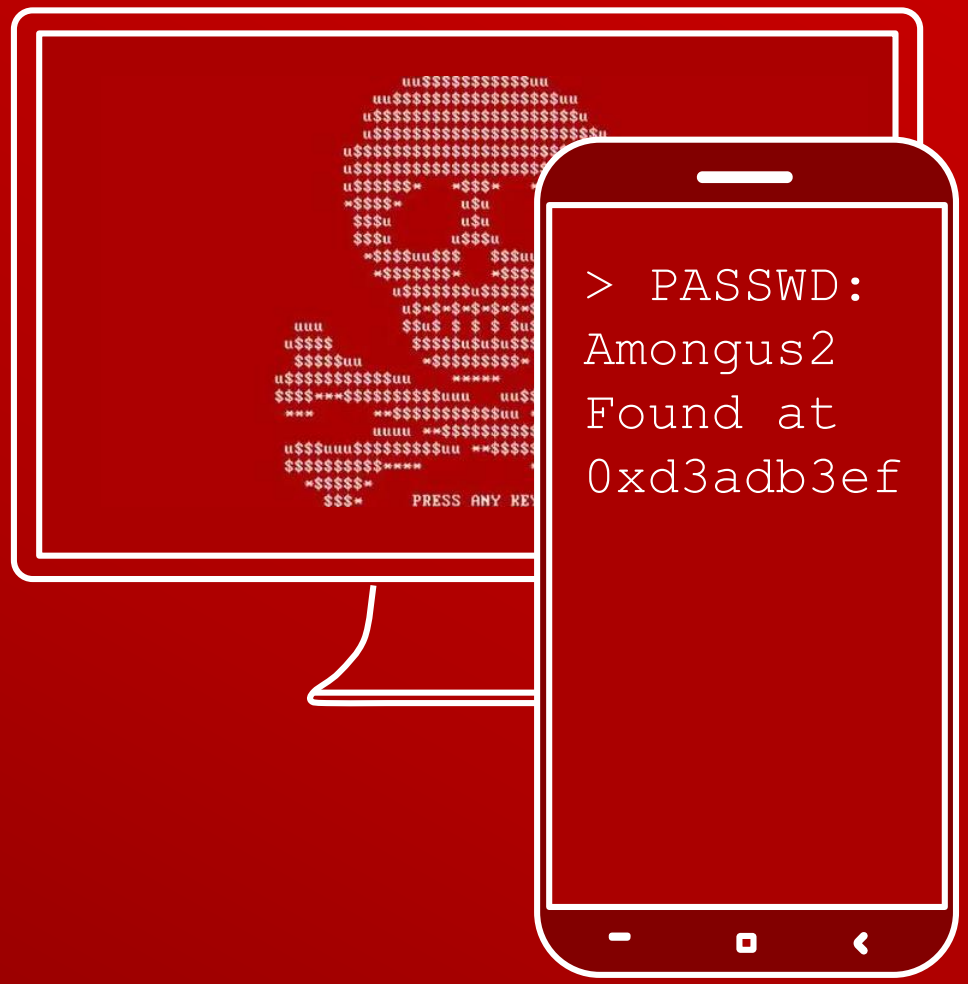
Как и везде, в форензике расследование проходит по определенным этапам:

- **Анализ:**
  > Изучение файловой системы, журналов событий (логов)
  > Поиск следов активности (время доступа, удалённые файлы)
  > Анализ сетевого трафика, памяти (**RAM**), логов приложений
- **Документация**
  > Записываем каждый шаг
  > Оформляем отчёт для суда или внутреннего расследования)
- **Презентация результатов**
  > Доклад для менеджмента, полиции, суда или заказчика)

Основные типы задач

Анализ файловых систем
Анализ сетевых дампов (PCAP)
Анализ дампов памяти
Анализ логов

Обработка и анализ изображений**



Анализ файловых систем

Файловая система может содержать скрытую информацию, такие как **удалённые файлы** или **метаданные**. Задачи могут включать восстановление удалённых данных или поиск скрытых файлов

Пример задачки: восстановление удалённого документа из файловой системы или анализ метаданных изображения для нахождения скрытой информации

Анализ сетевых дампов

Обычно такие задачки связаны с изучением **дампов** (файлов PCAP), которые содержат данные о сетевых взаимодействиях. Это может включать восстановление переданных файлов, **анализ пакетов** или **нахождение атак** в **сетевом трафике**

Пример задачки: проанализировать сетевой дамп для нахождения скомпрометированных данных или утечек информации

Анализ логов

Иногда могут подсунуть задачу на анализ логов для нахождения аномальных действий или следов взлома

Пример задачи: анализировать журналы доступа к серверу, чтобы найти попытки несанкционированного доступа и вычислить IP нарушителя

Анализ дампа памяти

Мы так же можем работать с дампом памяти некоторой ОС. Обычно мы будем расследовать дампы **Windows**, но может попасться и **Linux**

*Пример задачи: создать отчет с полной последовательностью заражения системы. Узнать как, чем, почему и когда заразилась тачка. Найти адрес **C2 сервера***

Инструментарий

Инструменты

На теории далеко не уедешь, а чтобы практиковаться, надо знать, что тыкать. Для эффективного решения задач по форензике я рекоменую освоить несколько инструментов:

- **Autopsy**: Мощный инструмент для **анализа файловых систем** и восстановления данных.
- **Wireshark**: Популярная утилита для **анализа сетевых дампов** и пакетов.
- **Binwalk**: Инструмент для анализа и **извлечения** данных из **бинарных файлов** и изображений.
- **foremost**: Программа для **восстановления удалённых файлов** из образов дисков.

foremost

Утилита для восстановления удалённых файлов из образов дисков или флешек. Ищет и восстанавливает файлы по сигнатурам: jpg, png, pdf, doc, zip и тд

Примеры команд:

```
$ foremost -i disk.img # Восстановление
```

```
$ foremost -i disk.img -t jpg,pdf # Восстановление
```

```
$ foremost -i disk.img # Восстановление
```

foremost

Основные параметры:

- **-i:** Входной файл (образ)
- **-o:** Папка вывода
- **-t:** Типы файлов (через запятую)
- **-v:** Verbose режим
- **-c**: Использовать пользовательский конфиг

foremost

Добавьте кастом сигнатуру

1. Откроем конфиг:

```
$ sudo nano /etc/foremost.conf
```

2. Запишем сигнатуру:

```
ext       EXE
  y       500000
  MZ
  \x00\x00\x00
```

3. Выполним поиск

```
$ foremost -t exe -i
evidence.dd
```

foremost

- Скачайте образ:
- https://cfreds-archive.nist.gov/FileCarving/Images/L0_Graphic.dd.bz2

- 1. Восстановите файлы
- 2. Проверьте их валидность (команда `file output/jpg/*`)

foremost

- Скачайте образ:
- https://cfreds-archive.nist.gov/FileCarving/Images/L3_Graphic.dd.bz2

- 1. Восстановите файлы
- 2. Можете ли вы открыть их?
- 3. Воспользуйтесь утилитой `photorec. мб поможет)`

Autopsy

Графический интерфейс к мощному набору **Sleuth Kit**. Позволяет анализировать образы дисков, искать удалённые файлы, изучать активность пользователя, работать с временными метками, логами, браузерами и многим другим

```
$ sudo autopsy
```

Autopsy запускается как веб-приложение (по умолчанию на http://localhost:9999)

Более новая версия: https://github.com/sleuthkit/autopsy/releases/

WARNING: Your browser currently has Java Script enabled.

You do not need Java Script to use Autopsy and it is recommended that it be turned off for security reasons.

Autopsy Forensic Browser 2.24

http://www.sleuthkit.org/autopsy/

OPEN CASE | NEW CASE | HELP

Autopsy

Графический интерфейс к мощному набору **Sleuth Kit**. Позволяет анализировать образы дисков, искать удалённые файлы, изучать активность пользователя, работать с временными метками, логами, браузерами и многим другим

```
$ sudo autopsy
```

Autopsy (старая версия) запускается как веб-приложение (по умолчанию на http://localhost:9999)

Более новая версия: https://github.com/sleuthkit/autopsy/releases/

Интересные файлы винды

Интересные файлы

NTUSER.DAT - C:\Users\<username>\NTUSER.DAT

SAM - C:\Windows\System32\config\SAM

USRCLASS.DAT - Users\<имя>\AppData\Local\Microsoft\Windows\UsrClass.dat

*Больше файлов в pdf доке

Практика

Потыкаем autopsy и посмотрим что он умеет

Для этого придется скачать образ:

https://cfreds-archive.nist.gov/Hacking_Case.html

Придется скачать **все 7 чанков**

Далее объединим их в один образ:

```
$ touch hacking_case.dd
$ for i in {1..8}; do
    cat “SCHARDT.00$i” >> hacking_case.dd
  done
```

What is the image hash? Does the acquisition and verification hash match?
2. What operating system was used on the computer?
3. When was the install date?
4. What is the timezone settings?
5. Who is the registered owner?
6. What is the computer account name?
7. What is the primary domain name?
13. List the network cards used by this computer
14. This same file reports the IP address and MAC address of the computer. What are they?
15. An internet search for vendor name/model of NIC cards by MAC address can be used to find out which network interface was used. In the above answer, the first 3 hex characters of the MAC address report the vendor of the card. Which NIC card was used during the installation and set-up for LOOK@LAN?
16. Find 6 installed programs that may be used for hacking.
17. What is the SMTP email address for Mr. Evil?
20. List 5 newsgroups that Mr. Evil has subscribed to?
21. A popular IRC (Internet Relay Chat) program called MIRC was installed. What are the user settings that was shown when the user was online and in a chat channel?
24. What websites was the victim accessing?
26. Search for the main users web based email address. What is it?
27. Yahoo mail, a popular web based email service, saves copies of the email under what file name?
28. How many executable files are in the recycle bin?
29. Are these files really deleted?

Volatility

Мощный фреймворк для анализа дампов оперативной памяти. Позволяет извлекать информацию о:

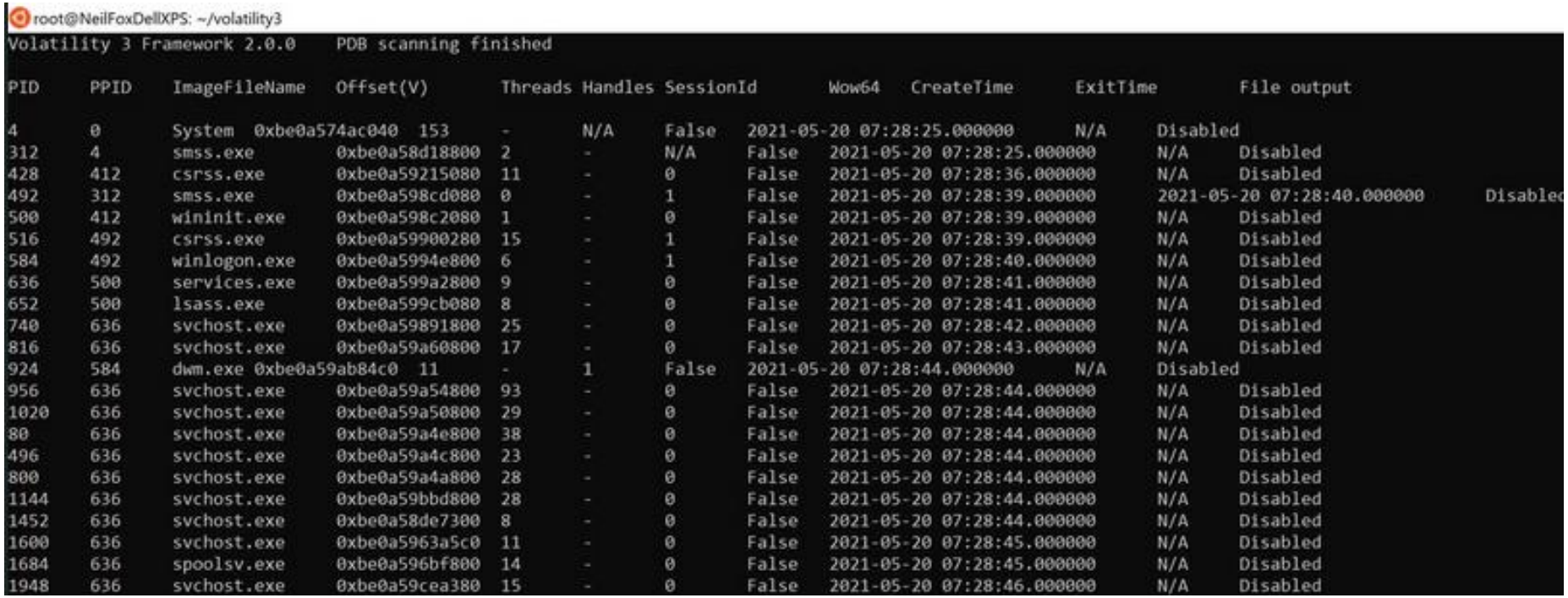
- процессах,
- сетевых соединениях,
- открытых файлах,
- пользовательских действиях,
- инъекциях вредоносного ПО,
- и даже **паролях и командах**, выполнявшихся в cmd/powershell.

Volatility

Подготовка дампа памяти

Volatility работает с форматами:

•.raw, .dd, .mem, .vmem (VMware), .lime, .bin, .elf, .core



root@NeilFoxDellXPS: ~/volatility3

```
Volatility 3 Framework 2.0.0    PDB scanning finished

PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

4       0       System  0xbe0a574ac040  153     -       N/A     False   2021-05-20 07:28:25.000000      N/A     Disabled
312     4       smss.exe        0xbe0a58d18800  2       -       N/A     False   2021-05-20 07:28:25.000000      N/A     Disabled
428     412     csrss.exe       0xbe0a59215080  11      -       0       False   2021-05-20 07:28:36.000000      N/A     Disabled
492     312     smss.exe        0xbe0a598cd080  0       -       1       False   2021-05-20 07:28:39.000000      2021-05-20 07:28:40.000000      Disablec
500     412     wininit.exe     0xbe0a598c2080  1       -       0       False   2021-05-20 07:28:39.000000      N/A     Disabled
516     492     csrss.exe       0xbe0a59900280  15      -       1       False   2021-05-20 07:28:39.000000      N/A     Disabled
584     492     winlogon.exe    0xbe0a5994e800  6       -       1       False   2021-05-20 07:28:40.000000      N/A     Disabled
636     500     services.exe    0xbe0a599a2800  9       -       0       False   2021-05-20 07:28:41.000000      N/A     Disabled
652     500     lsass.exe       0xbe0a599cb080  8       -       0       False   2021-05-20 07:28:41.000000      N/A     Disabled
740     636     svchost.exe     0xbe0a59891800  25      -       0       False   2021-05-20 07:28:42.000000      N/A     Disabled
816     636     svchost.exe     0xbe0a59a60800  17      -       0       False   2021-05-20 07:28:43.000000      N/A     Disabled
924     584     dwm.exe 0xbe0a59ab84c0  11      -       1       False   2021-05-20 07:28:44.000000      N/A     Disabled
956     636     svchost.exe     0xbe0a59a54800  93      -       0       False   2021-05-20 07:28:44.000000      N/A     Disabled
1020    636     svchost.exe     0xbe0a59a50800  29      -       0       False   2021-05-20 07:28:44.000000      N/A     Disabled
80      636     svchost.exe     0xbe0a59a4e800  38      -       0       False   2021-05-20 07:28:44.000000      N/A     Disabled
496     636     svchost.exe     0xbe0a59a4c800  23      -       0       False   2021-05-20 07:28:44.000000      N/A     Disabled
800     636     svchost.exe     0xbe0a59a4a800  28      -       0       False   2021-05-20 07:28:44.000000      N/A     Disabled
1144    636     svchost.exe     0xbe0a59bbd800  28      -       0       False   2021-05-20 07:28:44.000000      N/A     Disabled
1452    636     svchost.exe     0xbe0a58de7300  8       -       0       False   2021-05-20 07:28:44.000000      N/A     Disabled
1600    636     svchost.exe     0xbe0a5963a5c0  11      -       0       False   2021-05-20 07:28:45.000000      N/A     Disabled
1684    636     spoolsv.exe     0xbe0a596bf800  14      -       0       False   2021-05-20 07:28:45.000000      N/A     Disabled
1948    636     svchost.exe     0xbe0a59cea380  15      -       0       False   2021-05-20 07:28:46.000000      N/A     Disabled
```

Volatility

Установка:

Линух

```
$ python3 -m venv myenv
$ source myenv/bin/activate
$ pip3 install volatility
```

Винда:

```
$ pip3 install volatility
```

Volatility

Пример анализа пошагово:

- Узнать параметры ОС (важно!!!!):

```
$ volatility3 -f mem.raw imageinfo
```

Можно узнать профиль ручками:

```
$ grep -a windows mem.raw
```

```
$ volatility3 -f mem.raw windows.info
```

Volatility

Пример анализа пошагово:

- Посмотреть процессы:

```
$ volatility3 -f mem.raw windows.pslist
```

- Дерево процессов::

```
$ volatility3 -f mem.raw windows.pstree
```

- Найти подозрительные процессы или инъекции:

```
$ volatility3 -f mem.raw windows.malfind
```

Volatility

Пример анализа пошагово:

- Извлечь исполняемый файл из памяти:

```
$ volatility3 -f mem.raw windows.dumpfiles --pid 1234 -D output/
```

- Пароли из памяти:

```
$ volatility3 -f mem.raw windows.hashdump
```

- Посмотреть команды PowerShell или cmd:

```
$ volatility3 -f mem.raw windows.cmdline
```

Volatility

А что мы собсна ищем?

- **Необычные процессы** без родителя (PID 0 или svchost, но имя подозрительное)
- **Службы**, которых не должно быть (flashplayer.exe)
- **Модули и DLL**, загруженные не из C:\Windows\
- **Shell-код** в процессе (malfind в помощь)
- **Кражу буфера обмена**
- **Вызовы к IP/портам**, которых быть не должно, сетевые процессы

Практика

Скачать дамп Cridex

Цель: проанализировать дамп памяти, найти запущенный процесс трояна, извлечь сетевую активность и увидеть подозрительные артефакты. Составить подробный отчет