ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ «ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»

*Московский институт электроники и математики им. А.Н.Тихонова*

**Домашнее задание №1, вариант 2. Основы цифровой форензики.**

По направлению 10.04.01 – «Информационная безопасность»

Проверил:

преп. Сорокин А. В.

Подпись \_\_\_\_\_\_\_\_\_\_\_\_\_

Выполнил:

Новиков В. С. МКБ 241

Подпись \_\_\_\_\_\_\_\_\_\_\_\_\_

Москва 2025

### Задание «Вариант 1».

**Присутствующий на месте эксперт-криминалист провел первоначальный криминалистический анализ компьютера Джона и предал дамп памяти, который он создал на компьютере. Вы должны найти в нем следующую информацию.**

1. Определите семейство и версию операционной системы на компьютере Джона.
2. Какой процесс на компьютере Джона установил сетевое соединение с участием порта 554?
3. Устанавливались ли сетевые соединения компьютера Джона с участием локальных портов в диапазоне 135-140?
4. Если такие соединения устанавливались, укажите идентификаторы процессов, устанавливавших такие соединения.
5. Укажите идентификатор процессов-родителей данных процессов.
6. Укажите все процессы, порожденные процессами, устанавливавшими выявленные в пункте 3 соединения.
7. Установите, сколько различных процессов svchost.exe запускалось, приведите идентификаторы запущенных процессов.
8. Укажите имена исполняемых файлов, запустивших эти процессы.
9. Среди процессов, выявленных в пункте 7, определите те, которые содержат признаки заражения.
10. Установите, какое сообщение написал Джон в командной строке в ходе сеанса, в момент которого был создан дамп.

### Решение

#### Отчет по анализу дампа памяти (Volatility)

1. Определите семейство и версию операционной системы

**Ответ:** Win7SP1x64

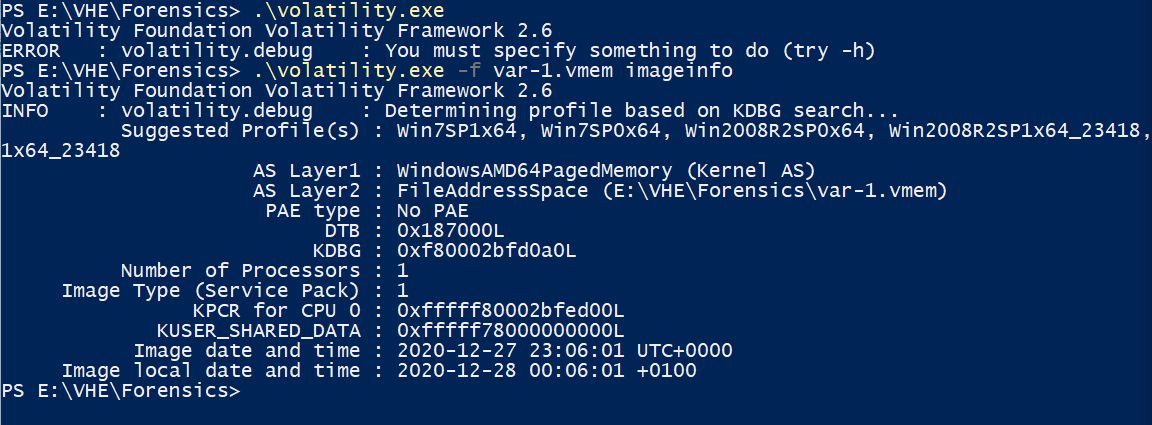


Рисунок 1. «imageinfo»

1. Процесс, установивший соединение на порту 554

**Ответ:** процесс **wmpnetwk.exe** (PID: 2368), порт: **554 (RTSP),** состояние: LISTENING (слушает входящие соединения на TCP порту 554)



Рисунок 2. «netscan»

1. Устанавливались ли соединения на портах 135-140?

**LISTENING** – это значит, что процесс слушает порт и ждёт входящие соединения.

**ESTABLISHED** - установленных соединений нет

Ответ: нет, соединения не устанавливались.

1. Идентификаторы процессов, установивших соединения (порты 135-140)

Ответ: отсутствуют (соединения не устанавливались).

1. Идентификаторы процессов-родителей

Ответ: отсутствуют (соединения не устанавливались).

1. Порожденные процессы (порты 135-140)

Ответ: отсутствуют (соединения не устанавливались).

1. Количество и PID процессов svchost.exe

**Ответ:** 11 процессов svchost.exe

**PID:** 896, 1408, 940, 296, 812, 700, 852, 2008, 1248, 612, 2632

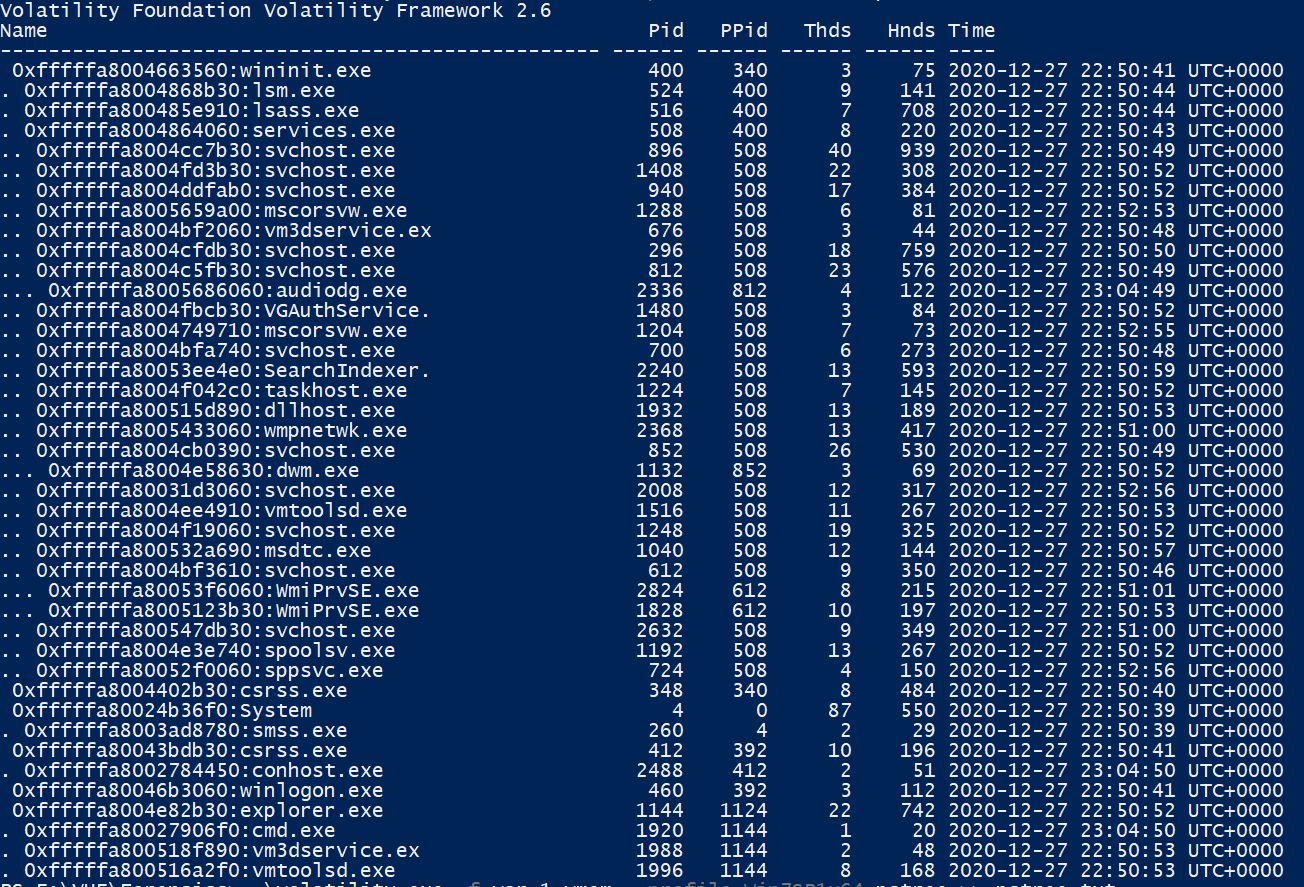


Рисунок 3. «pstree»

1. Имена исполняемых файлов, запустивших процессы svchost.exe

**Ответ:** все процессы svchost.exe были запущены процессом:

**services.exe** (PID: 508, путь: C:\Windows\system32\services.exe).

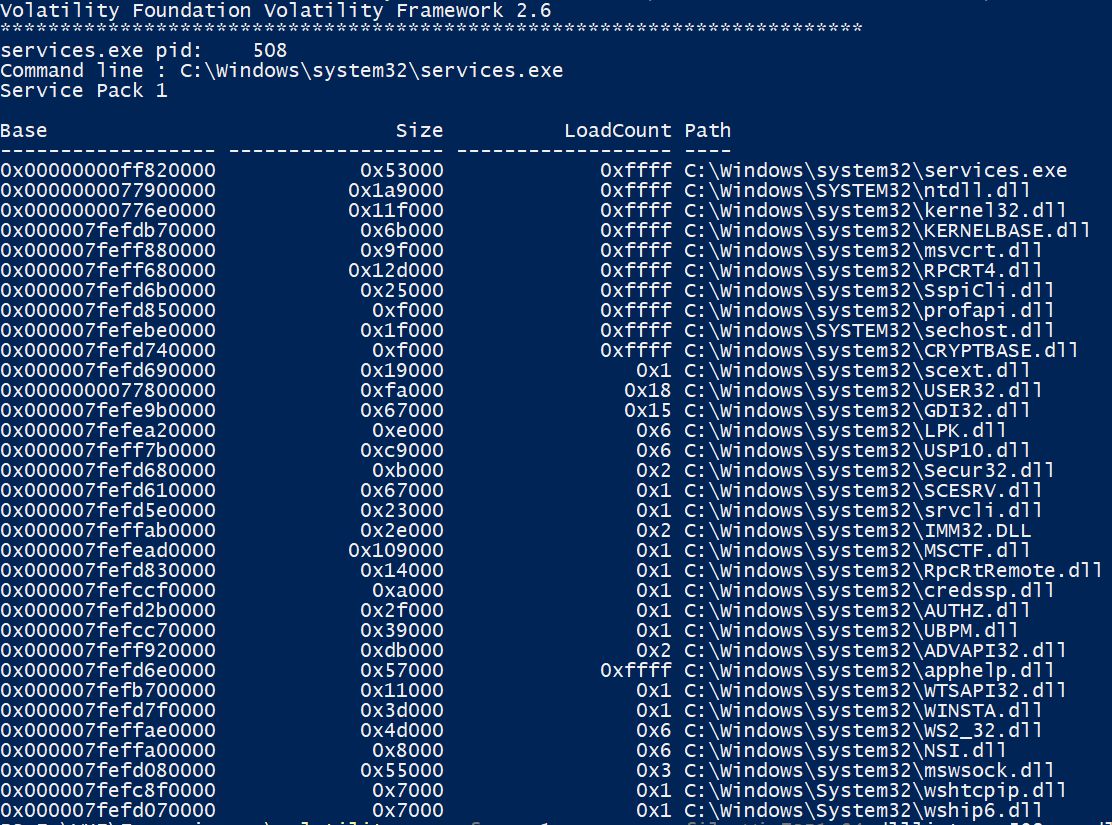
****

Рисунок 4. «dlllist -p 508»

1. Процессы svchost.exe с признаками заражения

Ответ: подозрительный код в памяти (PAGE\_EXECUTE\_READWRITE), представлен в таблице 1:

Таблица 1: процессы и их PID с адресами памяти.

|  |  |  |
| --- | --- | --- |
| **Процесс** | **PID** | **Адрес памяти** |
| svchost.exe | 812 | 0x1430000 |
| svchost.exe | 296 | 0xeb0000 |
| svchost.exe | 2008 | 0x2600000 |
| svchost.exe | 2008 | 0x4ea0000 |

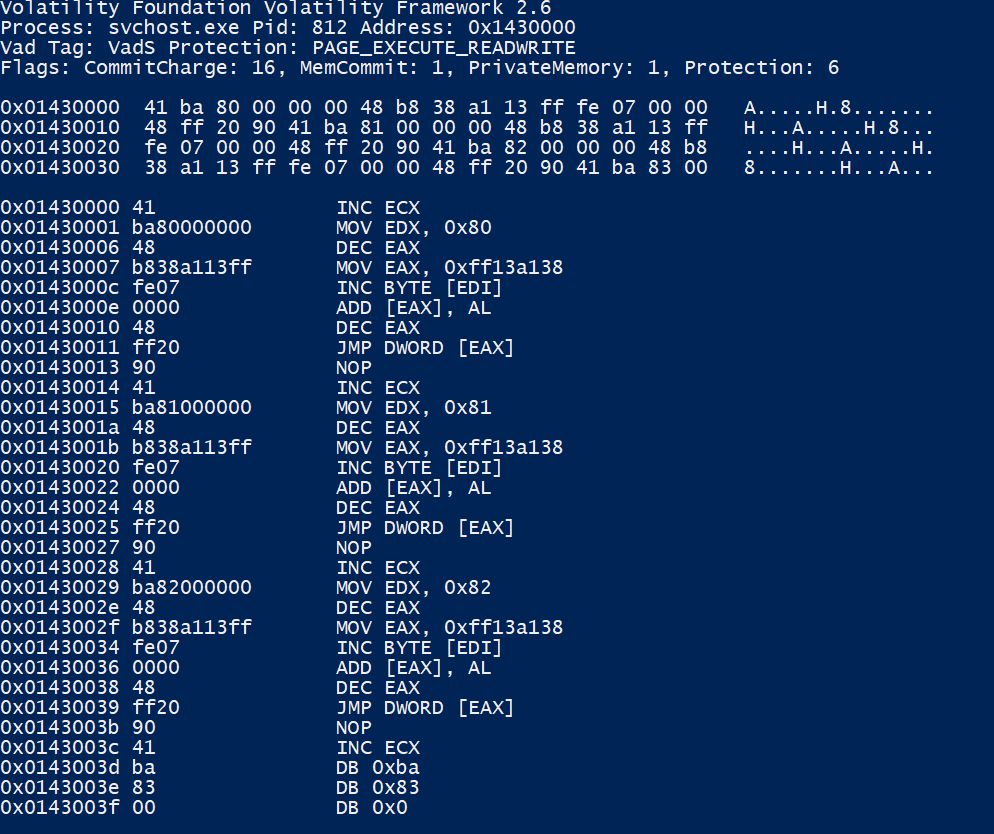


Рисунок 5.1 «malfind»

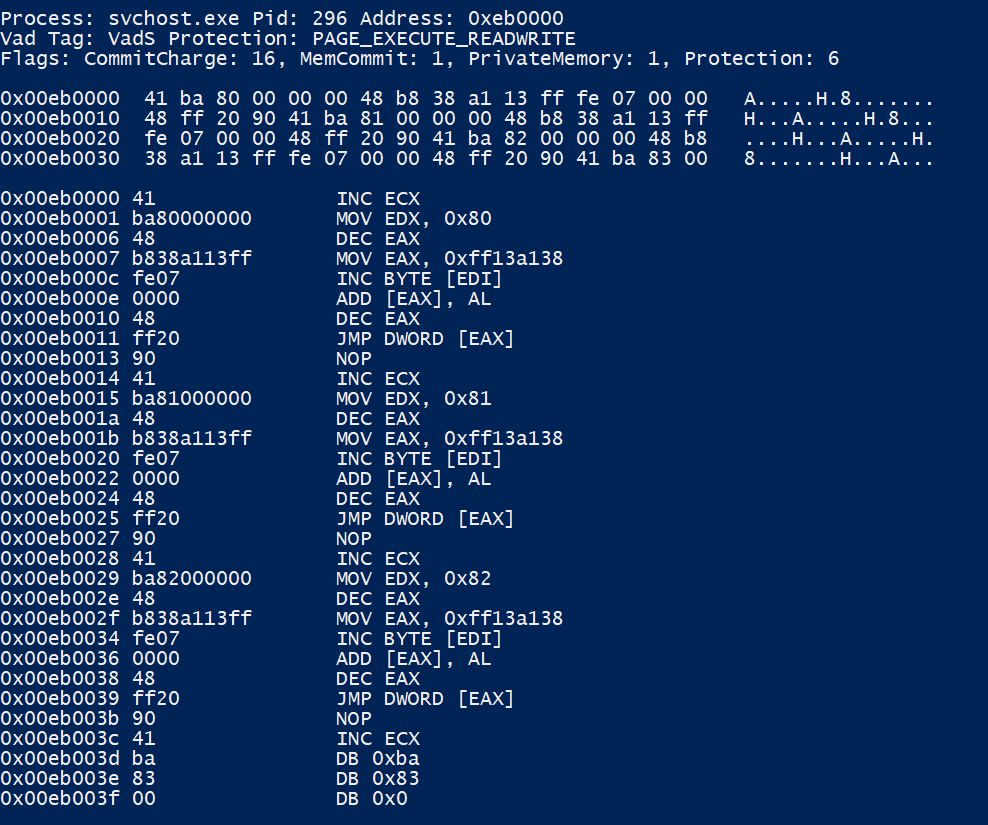


Рисунок 5.2 «malfind»

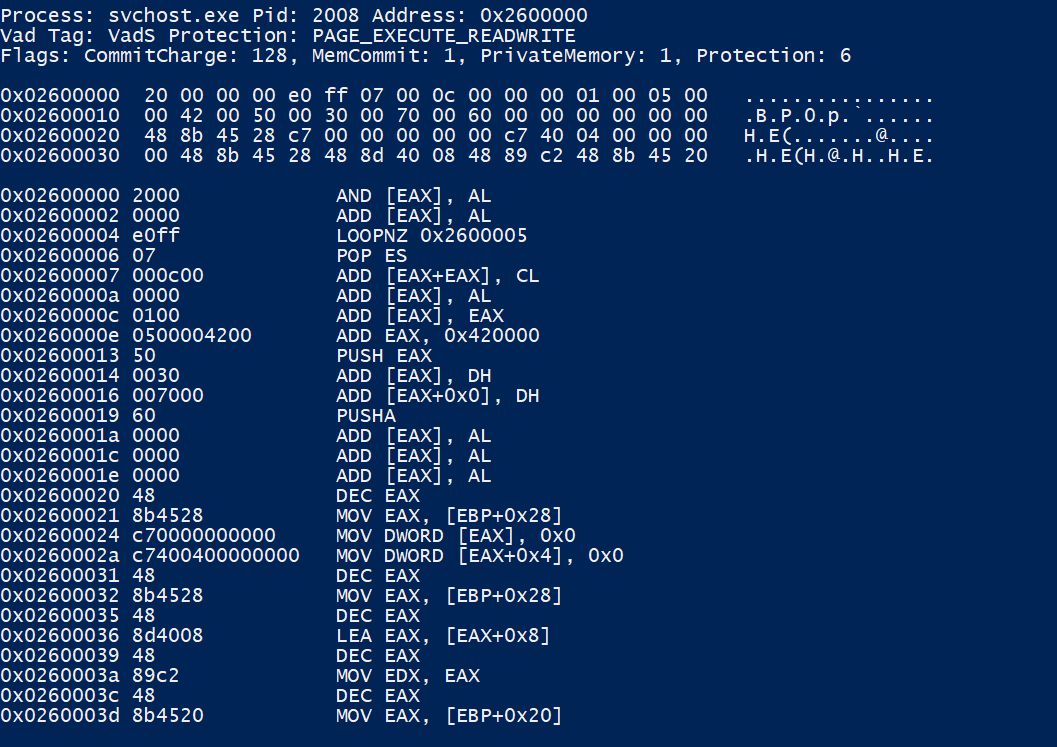


Рисунок 5.3 «malfind»

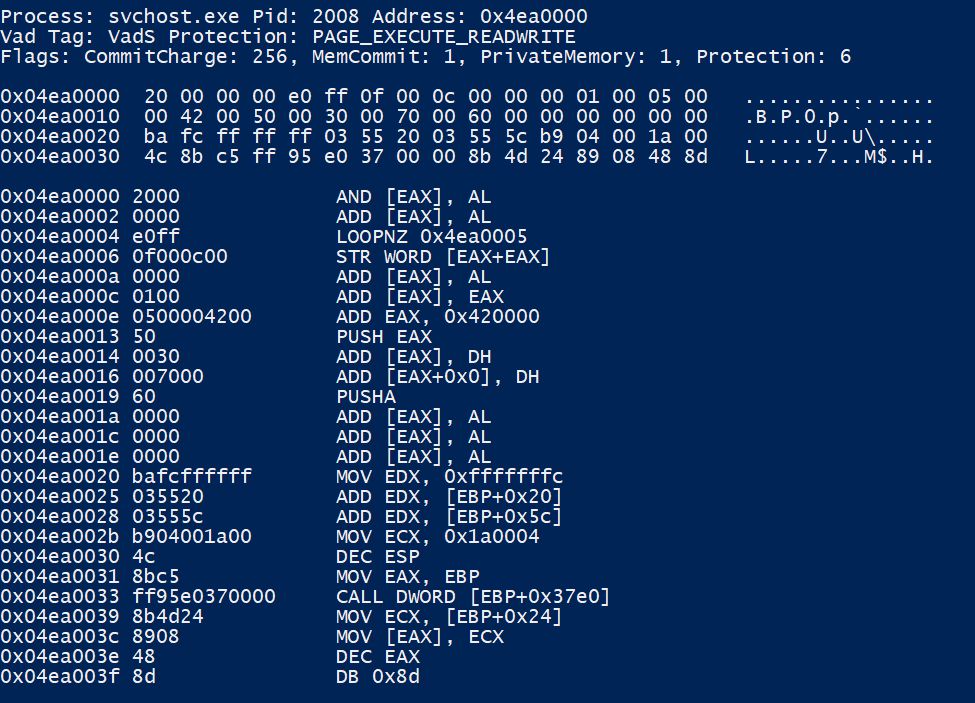


Рисунок 5.4 «malfind»

1. Сообщение, написанное Джоном в командной строке

Ответ: THM{You\_found\_me}

Другие команды (cd, dir, cls) не являются сообщениями.

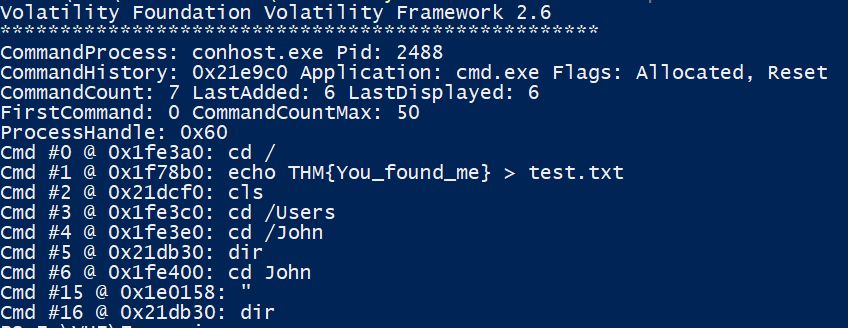
[](https://github.com/vit81g/Cybersecurity_HSE/blob/main/HomeWorks/Forensics/HW2/10_cmdscan.jpg)

Рисунок 6 «cmdscan»

### Приложение А

Все материалы и описания проводимых работ находятся на GitHub по адресу:

<https://github.com/vit81g/Cybersecurity_HSE/tree/main/HomeWorks/Forensics/HW2>