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

```
PS E:\VHE\Forensics> .\volatility.exe
Volatility Foundation Volatility Framework 2.6
ERROR   : volatility.debug    : You must specify something to do (try -h)
PS E:\VHE\Forensics> .\volatility.exe -f var-1.vmem imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_23418,
1x64_23418
                     AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (E:\VHE\Forensics\var-1.vmem)
                      PAE type : No PAE
                           DTB : 0x187000L
                          KDBG : 0xf80002bfd0a0L
          Number of Processors : 1
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0xfffff80002bfed00L
             KUSER_SHARED_DATA : 0xfffff78000000000L
           Image date and time : 2020-12-27 23:06:01 UTC+0000
     Image local date and time : 2020-12-28 00:06:01 +0100
PS E:\VHE\Forensics>
```

Рисунок 1. «imageinfo»

2. Процесс, установивший соединение на порту 554

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

```
PS E:\VHE\Forensics> .\volatility.exe -f var-1.vmem --profile=Win7SP1x64 netscan
Volatility Foundation Volatility Framework 2.6
Offset(P)          Proto    Local Address                  Foreign Address      State            Pid      Owner          Created
0x33c9470          TCPv4    0.0.0.0:49154                  0.0.0.0:0            LISTENING        896      svchost.exe
0x33c9470          TCPv6    :::49154                       :::0                 LISTENING        896      svchost.exe
0x33c9da0          TCPv4    0.0.0.0:49154                  0.0.0.0:0            LISTENING        896      svchost.exe
0x7bf6720          TCPv4    0.0.0.0:3587                   0.0.0.0:0            LISTENING        2632     svchost.exe
0x7bf6720          TCPv6    :::3587                        :::0                 LISTENING        2632     svchost.exe
0xa76f150          TCPv4    0.0.0.0:49156                  0.0.0.0:0            LISTENING        516      lsass.exe
0xcd6a520          UDPv4    0.0.0.0:3702                   *:*                                   296      svchost.exe    2020-12-27 22:52:12 UTC+0000
0xcd6a520          UDPv6    :::3702                        *:*                                   296      svchost.exe    2020-12-27 22:52:12 UTC+0000
0xc9614d0          TCPv4    0.0.0.0:2869                   0.0.0.0:0            LISTENING        4        System
0xc9614d0          TCPv6    :::2869                        :::0                 LISTENING        4        System
0xded3900          UDPv4    127.0.0.1:62336                *:*                                   1408     svchost.exe    2020-12-27 22:51:00 UTC+0000
0xded3ec0          UDPv6    ::1:62334                      *:*                                   1408     svchost.exe    2020-12-27 22:51:00 UTC+0000
0x217751c0         UDPv4    0.0.0.0:3702                   *:*                                   1408     svchost.exe    2020-12-27 22:52:12 UTC+0000
0x21a6dcb0         UDPv4    0.0.0.0:0                      *:*                                   2632     svchost.exe    2020-12-27 22:51:11 UTC+0000
0x21a6dcb0         UDPv6    :::0                           *:*                                   2632     svchost.exe    2020-12-27 22:51:11 UTC+0000
0x246dc440         TCPv4    0.0.0.0:10243                  0.0.0.0:0            LISTENING        4        System
0x246dc440         TCPv6    :::10243                       :::0                 LISTENING        4        System
0x24d5c8c0         TCPv4    0.0.0.0:554                    0.0.0.0:0            LISTENING        2368     wmpnetwk.exe
0x24eea010         TCPv6    ::1:2869                       ::1:49160            CLOSED           4        System
```

Рисунок 2. «netscan»

3. 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.

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

Ответ: отсутствуют (соединения не устанавливались).

5. Идентификаторы процессов-родителей

Ответ: отсутствуют (соединения не устанавливались).

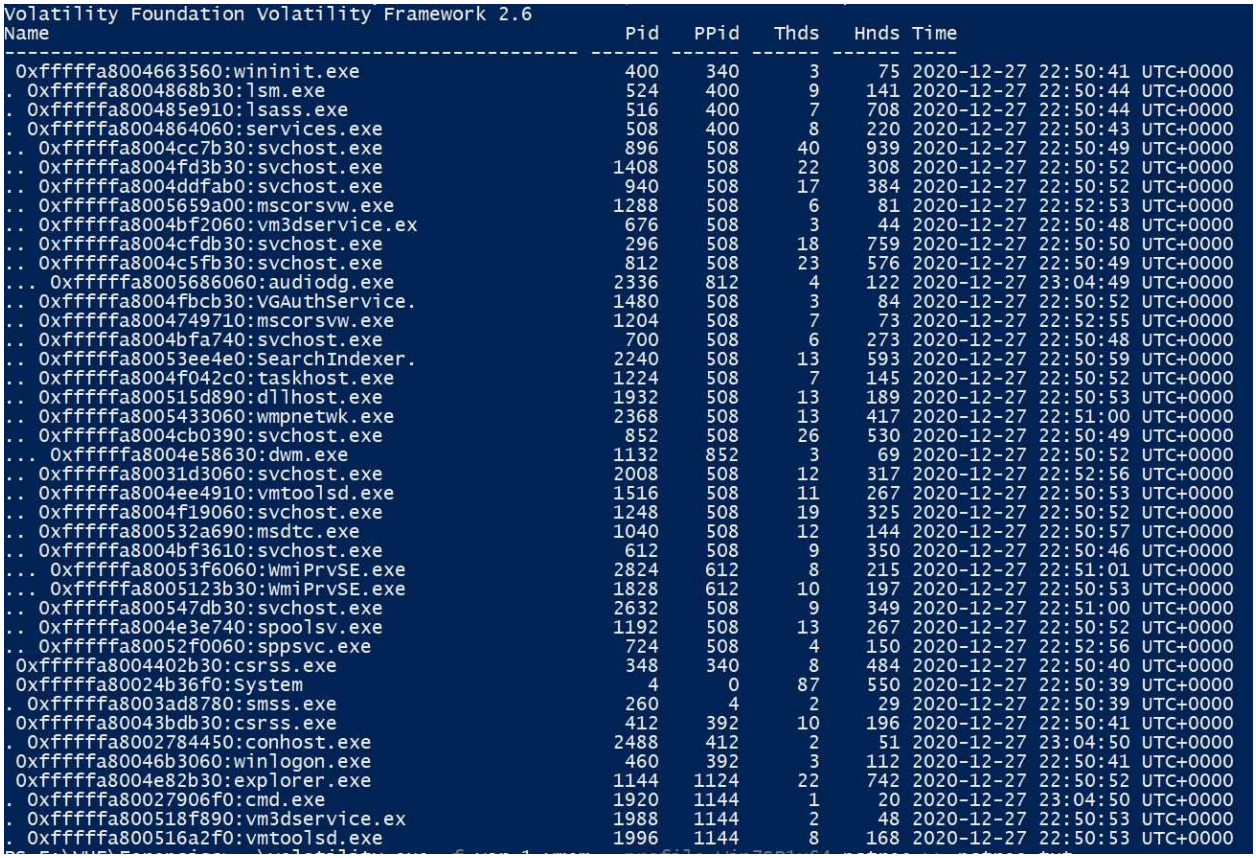
6. Порожденные процессы (порты 135-140)

Ответ: отсутствуют (соединения не устанавливались).

7. Количество и PID процессов svchost.exe

Ответ**:** 11 процессов svchost.exe

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



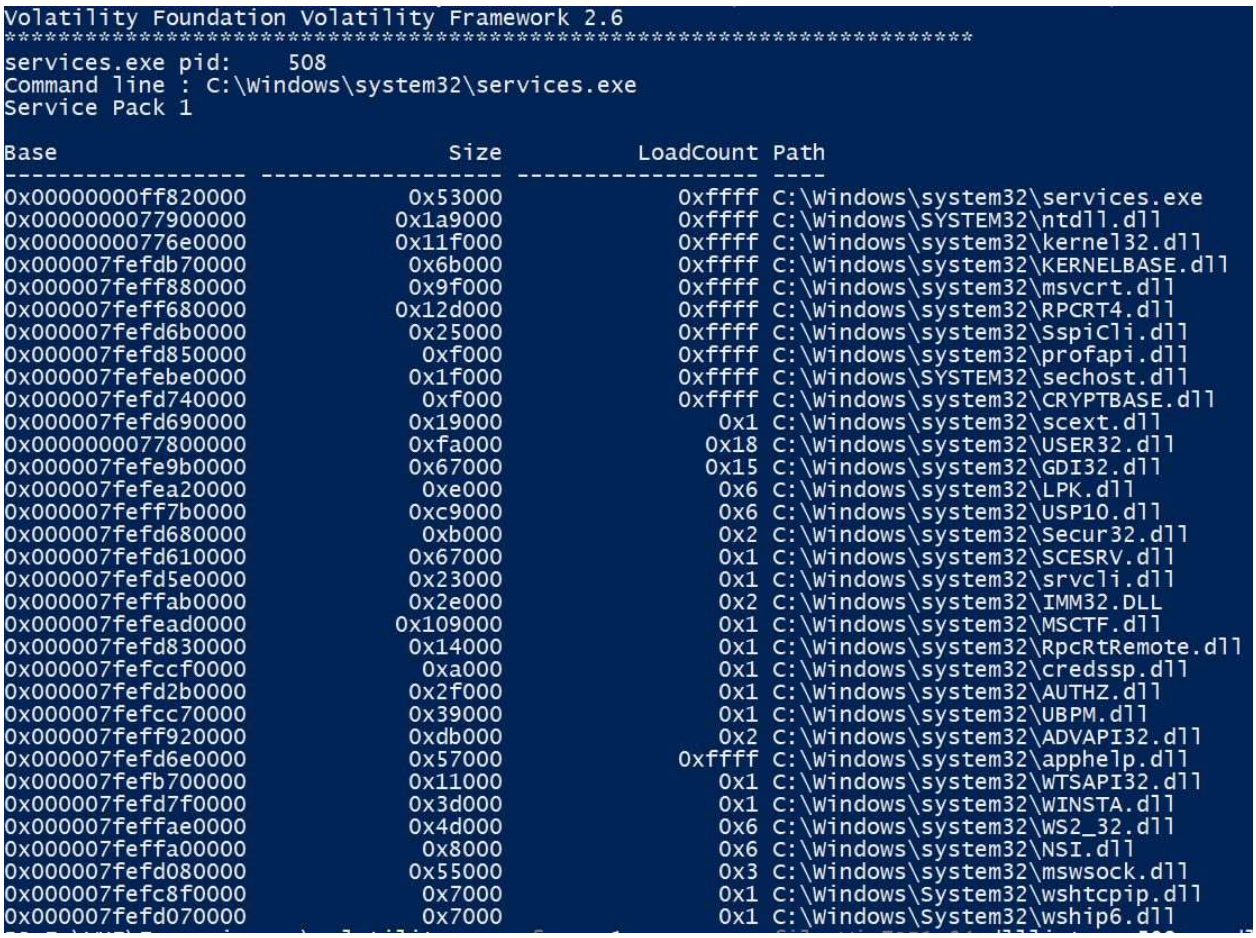
```
Volatility Foundation Volatility Framework 2.6
Name                                                 Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0xfffffa8004663560:wininit.exe                       400    340      3     75 2020-12-27 22:50:41 UTC+0000
. 0xfffffa8004868b30:lsm.exe                          524    400      9    141 2020-12-27 22:50:44 UTC+0000
. 0xfffffa800485e910:lsass.exe                        516    400      7    708 2020-12-27 22:50:44 UTC+0000
. 0xfffffa8004864060:services.exe                     508    400      8    220 2020-12-27 22:50:43 UTC+0000
.. 0xfffffa8004cc7b30:svchost.exe                     896    508     40    939 2020-12-27 22:50:49 UTC+0000
.. 0xfffffa8004fd3b30:svchost.exe                    1408    508     22    308 2020-12-27 22:50:52 UTC+0000
.. 0xfffffa8004ddfab0:svchost.exe                     940    508     17    384 2020-12-27 22:50:52 UTC+0000
.. 0xfffffa8005659a00:mscorsvw.exe                   1288    508      6     81 2020-12-27 22:52:53 UTC+0000
.. 0xfffffa8004bf2060:vm3dservice.ex                  676    508      3     44 2020-12-27 22:50:48 UTC+0000
.. 0xfffffa8004cfdb30:svchost.exe                     296    508     18    759 2020-12-27 22:50:50 UTC+0000
.. 0xfffffa8004c5fb30:svchost.exe                     812    508     23    576 2020-12-27 22:50:49 UTC+0000
... 0xfffffa8005686060:audiodg.exe                   2336    812      4    122 2020-12-27 23:04:49 UTC+0000
.. 0xfffffa8004fbcb30:VGAuthService.                 1480    508      3     84 2020-12-27 22:50:52 UTC+0000
.. 0xfffffa8004749710:mscorsvw.exe                   1204    508      7     73 2020-12-27 22:52:55 UTC+0000
.. 0xfffffa8004bfa740:svchost.exe                     700    508      6    273 2020-12-27 22:50:48 UTC+0000
.. 0xfffffa80053ee4e0:SearchIndexer.                 2240    508     13    593 2020-12-27 22:50:59 UTC+0000
.. 0xfffffa8004f042c0:taskhost.exe                   1224    508      7    145 2020-12-27 22:50:52 UTC+0000
.. 0xfffffa800515d890:dllhost.exe                    1932    508     13    189 2020-12-27 22:50:53 UTC+0000
.. 0xfffffa8005433060:wmpnetwk.exe                   2368    508     13    417 2020-12-27 22:51:00 UTC+0000
.. 0xfffffa8004cb0390:svchost.exe                     852    508     26    530 2020-12-27 22:50:49 UTC+0000
... 0xfffffa8004e58630:dwm.exe                       1132    852      3     69 2020-12-27 22:50:52 UTC+0000
.. 0xfffffa80031d3060:svchost.exe                    2008    508     12    317 2020-12-27 22:52:56 UTC+0000
.. 0xfffffa8004ee4910:vmtoolsd.exe                   1516    508     11    267 2020-12-27 22:50:53 UTC+0000
.. 0xfffffa8004f19060:svchost.exe                    1248    508     19    325 2020-12-27 22:50:52 UTC+0000
.. 0xfffffa800532a690:msdtc.exe                      1040    508     12    144 2020-12-27 22:50:57 UTC+0000
.. 0xfffffa8004bf3610:svchost.exe                     612    508      9    350 2020-12-27 22:50:46 UTC+0000
... 0xfffffa80053f6060:WmiPrvSE.exe                  2824    612      8    215 2020-12-27 22:51:01 UTC+0000
... 0xfffffa8005123b30:WmiPrvSE.exe                  1828    612     10    197 2020-12-27 22:50:53 UTC+0000
.. 0xfffffa800547db30:svchost.exe                    2632    508      9    349 2020-12-27 22:51:00 UTC+0000
.. 0xfffffa8004e3e740:spoolsv.exe                    1192    508     13    267 2020-12-27 22:50:52 UTC+0000
.. 0xfffffa80052f0060:sppsvc.exe                      724    508      4    150 2020-12-27 22:52:56 UTC+0000
 0xfffffa8004402b30:csrss.exe                         348    340      8    484 2020-12-27 22:50:40 UTC+0000
 0xfffffa80024b36f0:System                              4      0     87    550 2020-12-27 22:50:39 UTC+0000
. 0xfffffa8003ad8780:smss.exe                         260      4      2     29 2020-12-27 22:50:39 UTC+0000
 0xfffffa80043bdb30:csrss.exe                         412    392     10    196 2020-12-27 22:50:41 UTC+0000
. 0xfffffa8002784450:conhost.exe                     2488    412      2     51 2020-12-27 23:04:50 UTC+0000
 0xfffffa80046b3060:winlogon.exe                      460    392      3    112 2020-12-27 22:50:41 UTC+0000
 0xfffffa8004e82b30:explorer.exe                     1144   1124     22    742 2020-12-27 22:50:52 UTC+0000
. 0xfffffa80027906f0:cmd.exe                         1920   1144      1     20 2020-12-27 23:04:50 UTC+0000
. 0xfffffa800518f890:vm3dservice.ex                  1988   1144      2     48 2020-12-27 22:50:53 UTC+0000
. 0xfffffa800516a2f0:vmtoolsd.exe                    1996   1144      8    168 2020-12-27 22:50:53 UTC+0000
```

Рисунок 3. «pstree»

8. 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).



```
Volatility Foundation Volatility Framework 2.6
************************************************************************
services.exe pid:    508
Command line : C:\Windows\system32\services.exe
Service Pack 1

Base                             Size          LoadCount Path
------------------ ------------------ ------------------ ----
0x00000000ff820000            0x53000             0xffff C:\Windows\system32\services.exe
0x0000000077900000            0x1a9000            0xffff C:\Windows\SYSTEM32\ntdll.dll
0x0000000000776e0000          0x11f000            0xffff C:\Windows\system32\kernel32.dll
0x000007fefdb70000             0x6b000            0xffff C:\Windows\system32\KERNELBASE.dll
0x000007feff880000             0x9f000            0xffff C:\Windows\system32\msvcrt.dll
0x000007feff680000            0x12d000            0xffff C:\Windows\system32\RPCRT4.dll
0x000007fefd6b0000             0x25000            0xffff C:\Windows\system32\SspiCli.dll
0x000007fefd850000              0xf000            0xffff C:\Windows\system32\profapi.dll
0x000007fefebe0000             0x1f000            0xffff C:\Windows\SYSTEM32\sechost.dll
0x000007fefd740000              0xf000            0xffff C:\Windows\system32\CRYPTBASE.dll
0x000007fefd690000             0x19000               0x1 C:\Windows\system32\scext.dll
0x0000000077800000             0xfa000              0x18 C:\Windows\system32\USER32.dll
0x000007fefe9b0000             0x67000              0x15 C:\Windows\system32\GDI32.dll
0x000007fefea20000              0xe000               0x6 C:\Windows\system32\LPK.dll
0x000007feff7b0000             0xc9000               0x6 C:\Windows\system32\USP10.dll
0x000007fefd680000              0xb000               0x2 C:\Windows\system32\Secur32.dll
0x000007fefd610000             0x67000               0x1 C:\Windows\system32\SCESRV.dll
0x000007fefd5e0000             0x23000               0x1 C:\Windows\system32\srvcli.dll
0x000007feffab0000             0x2e000               0x2 C:\Windows\system32\IMM32.DLL
0x000007fefead0000            0x109000               0x1 C:\Windows\system32\MSCTF.dll
0x000007fefd830000             0x14000               0x1 C:\Windows\system32\RpcRtRemote.dll
0x000007fefccf0000              0xa000               0x1 C:\Windows\system32\credssp.dll
0x000007fefd2b0000             0x2f000               0x1 C:\Windows\system32\AUTHZ.dll
0x000007fefcc70000             0x39000               0x1 C:\Windows\system32\UBPM.dll
0x000007feff920000             0xdb000               0x2 C:\Windows\system32\ADVAPI32.dll
0x000007fefd6e0000             0x57000             0xffff C:\Windows\system32\apphelp.dll
0x000007fefb700000             0x11000               0x1 C:\Windows\system32\WTSAPI32.dll
0x000007fefd7f0000             0x3d000               0x1 C:\Windows\system32\WINSTA.dll
0x000007feffae0000             0x4d000               0x6 C:\Windows\system32\WS2_32.dll
0x000007feffa00000              0x8000               0x6 C:\Windows\system32\NSI.dll
0x000007fefd080000             0x55000               0x3 C:\Windows\system32\mswsock.dll
0x000007fefc8f0000              0x7000               0x1 C:\Windows\System32\wshtcpip.dll
0x000007fefd070000              0x7000               0x1 C:\Windows\System32\wship6.dll
```

Рисунок 4. «dlllist -p 508»

9. 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

```
Volatility Foundation Volatility Framework 2.6
Process: svchost.exe Pid: 812 Address: 0x1430000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 16, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x01430000  41 ba 80 00 00 00 48 b8 38 a1 13 ff fe 07 00 00   A.....H.8.......
0x01430010  48 ff 20 90 41 ba 81 00 00 00 48 b8 38 a1 13 ff   H...A.....H.8...
0x01430020  fe 07 00 00 48 ff 20 90 41 ba 82 00 00 00 48 b8   ....H...A.....H.
0x01430030  38 a1 13 ff fe 07 00 00 48 ff 20 90 41 ba 83 00   8.......H...A...

0x01430000 41              INC ECX
0x01430001 ba80000000      MOV EDX, 0x80
0x01430006 48              DEC EAX
0x01430007 b838a113ff      MOV EAX, 0xff13a138
0x0143000c fe07            INC BYTE [EDI]
0x0143000e 0000            ADD [EAX], AL
0x01430010 48              DEC EAX
0x01430011 ff20            JMP DWORD [EAX]
0x01430013 90              NOP
0x01430014 41              INC ECX
0x01430015 ba81000000      MOV EDX, 0x81
0x0143001a 48              DEC EAX
0x0143001b b838a113ff      MOV EAX, 0xff13a138
0x01430020 fe07            INC BYTE [EDI]
0x01430022 0000            ADD [EAX], AL
0x01430024 48              DEC EAX
0x01430025 ff20            JMP DWORD [EAX]
0x01430027 90              NOP
0x01430028 41              INC ECX
0x01430029 ba82000000      MOV EDX, 0x82
0x0143002e 48              DEC EAX
0x0143002f b838a113ff      MOV EAX, 0xff13a138
0x01430034 fe07            INC BYTE [EDI]
0x01430036 0000            ADD [EAX], AL
0x01430038 48              DEC EAX
0x01430039 ff20            JMP DWORD [EAX]
0x0143003b 90              NOP
0x0143003c 41              INC ECX
0x0143003d ba              DB 0xba
0x0143003e 83              DB 0x83
0x0143003f 00              DB 0x0
```

Рисунок 5.1 «malfind»

```
Process: svchost.exe Pid: 296 Address: 0xeb0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 16, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x00eb0000  41 ba 80 00 00 00 48 b8 38 a1 13 ff fe 07 00 00   A.....H.8.......
0x00eb0010  48 ff 20 90 41 ba 81 00 00 00 48 b8 38 a1 13 ff   H...A.....H.8...
0x00eb0020  fe 07 00 00 48 ff 20 90 41 ba 82 00 00 00 48 b8   ....H...A.....H.
0x00eb0030  38 a1 13 ff fe 07 00 00 48 ff 20 90 41 ba 83 00   8.......H...A...

0x00eb0000 41              INC ECX
0x00eb0001 ba80000000      MOV EDX, 0x80
0x00eb0006 48              DEC EAX
0x00eb0007 b838a113ff      MOV EAX, 0xff13a138
0x00eb000c fe07            INC BYTE [EDI]
0x00eb000e 0000            ADD [EAX], AL
0x00eb0010 48              DEC EAX
0x00eb0011 ff20            JMP DWORD [EAX]
0x00eb0013 90              NOP
0x00eb0014 41              INC ECX
0x00eb0015 ba81000000      MOV EDX, 0x81
0x00eb001a 48              DEC EAX
0x00eb001b b838a113ff      MOV EAX, 0xff13a138
0x00eb0020 fe07            INC BYTE [EDI]
0x00eb0022 0000            ADD [EAX], AL
0x00eb0024 48              DEC EAX
0x00eb0025 ff20            JMP DWORD [EAX]
0x00eb0027 90              NOP
0x00eb0028 41              INC ECX
0x00eb0029 ba82000000      MOV EDX, 0x82
0x00eb002e 48              DEC EAX
0x00eb002f b838a113ff      MOV EAX, 0xff13a138
0x00eb0034 fe07            INC BYTE [EDI]
0x00eb0036 0000            ADD [EAX], AL
0x00eb0038 48              DEC EAX
0x00eb0039 ff20            JMP DWORD [EAX]
0x00eb003b 90              NOP
0x00eb003c 41              INC ECX
0x00eb003d ba              DB 0xba
0x00eb003e 83              DB 0x83
0x00eb003f 00              DB 0x0
```

Рисунок 5.2 «malfind»

```
Process: svchost.exe Pid: 2008 Address: 0x2600000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 128, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x02600000  20 00 00 00 e0 ff 07 00 0c 00 00 00 01 00 05 00   ................
0x02600010  00 42 00 50 00 30 00 70 00 60 00 00 00 00 00 00   .B.P.0.p.`......
0x02600020  48 8b 45 28 c7 00 00 00 00 00 c7 40 04 00 00 00   H.E(.......@....
0x02600030  00 48 8b 45 28 48 8d 40 08 48 89 c2 48 8b 45 20   .H.E(H.@.H..H.E

0x02600000 2000             AND [EAX], AL
0x02600002 0000             ADD [EAX], AL
0x02600004 e0ff             LOOPNZ 0x2600005
0x02600006 07               POP ES
0x02600007 000c00           ADD [EAX+EAX], CL
0x0260000a 0000             ADD [EAX], AL
0x0260000c 0100             ADD [EAX], EAX
0x0260000e 0500004200       ADD EAX, 0x420000
0x02600013 50               PUSH EAX
0x02600014 0030             ADD [EAX], DH
0x02600016 007000           ADD [EAX+0x0], DH
0x02600019 60               PUSHA
0x0260001a 0000             ADD [EAX], AL
0x0260001c 0000             ADD [EAX], AL
0x0260001e 0000             ADD [EAX], AL
0x02600020 48               DEC EAX
0x02600021 8b4528           MOV EAX, [EBP+0x28]
0x02600024 c70000000000     MOV DWORD [EAX], 0x0
0x0260002a c7400400000000   MOV DWORD [EAX+0x4], 0x0
0x02600031 48               DEC EAX
0x02600032 8b4528           MOV EAX, [EBP+0x28]
0x02600035 48               DEC EAX
0x02600036 8d4008           LEA EAX, [EAX+0x8]
0x02600039 48               DEC EAX
0x0260003a 89c2             MOV EDX, EAX
0x0260003c 48               DEC EAX
0x0260003d 8b4520           MOV EAX, [EBP+0x20]
```

Рисунок 5.3 «malfind»

```
Process: svchost.exe Pid: 2008 Address: 0x4ea0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 256, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x04ea0000  20 00 00 00 e0 ff 0f 00 0c 00 00 00 01 00 05 00   ................
0x04ea0010  00 42 00 50 00 30 00 70 00 60 00 00 00 00 00 00   .B.P.0.p.`......
0x04ea0020  ba fc ff ff ff 03 55 20 03 55 5c b9 04 00 1a 00   ......U..U\.....
0x04ea0030  4c 8b c5 ff 95 e0 37 00 00 8b 4d 24 89 08 48 8d   L.....7...M$..H.

0x04ea0000 2000             AND [EAX], AL
0x04ea0002 0000             ADD [EAX], AL
0x04ea0004 e0ff             LOOPNZ 0x4ea0005
0x04ea0006 0f000c00         STR WORD [EAX+EAX]
0x04ea000a 0000             ADD [EAX], AL
0x04ea000c 0100             ADD [EAX], EAX
0x04ea000e 0500004200       ADD EAX, 0x420000
0x04ea0013 50               PUSH EAX
0x04ea0014 0030             ADD [EAX], DH
0x04ea0016 007000           ADD [EAX+0x0], DH
0x04ea0019 60               PUSHA
0x04ea001a 0000             ADD [EAX], AL
0x04ea001c 0000             ADD [EAX], AL
0x04ea001e 0000             ADD [EAX], AL
0x04ea0020 bafcffffff       MOV EDX, 0xfffffffc
0x04ea0025 035520           ADD EDX, [EBP+0x20]
0x04ea0028 03555c           ADD EDX, [EBP+0x5c]
0x04ea002b b904001a00       MOV ECX, 0x1a0004
0x04ea0030 4c               DEC ESP
0x04ea0031 8bc5             MOV EAX, EBP
0x04ea0033 ff95e0370000     CALL DWORD [EBP+0x37e0]
0x04ea0039 8b4d24           MOV ECX, [EBP+0x24]
0x04ea003c 8908             MOV [EAX], ECX
0x04ea003e 48               DEC EAX
0x04ea003f 8d               DB 0x8d
```

Рисунок 5.4 «malfind»

10. Сообщение, написанное Джоном в командной строке

Ответ: THM{You_found_me}

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

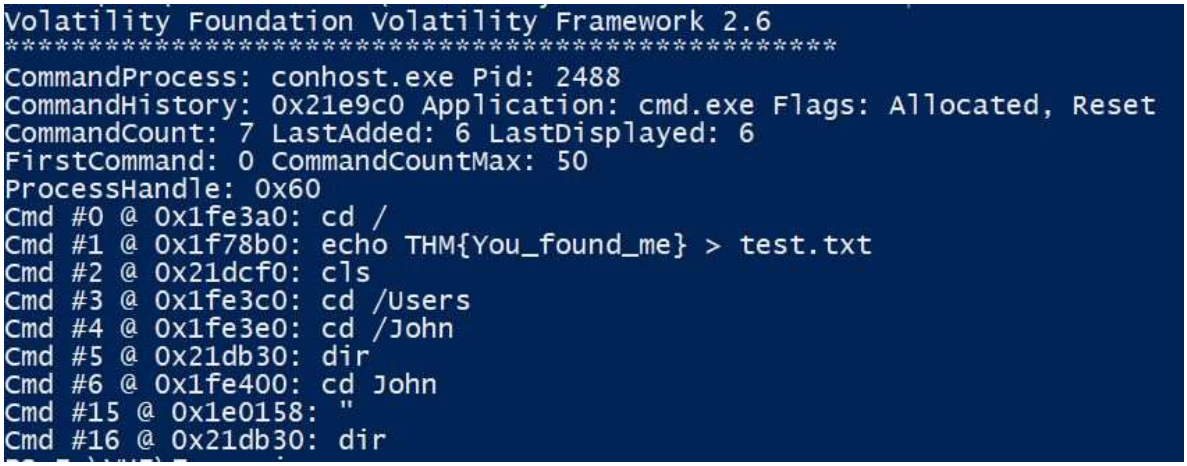


Рисунок 6 «cmdscan»

Приложение А

Все материалы и описания проводимых работ находятся на GitHub по адресу:
https://github.com/vit81g/Cybersecurity_HSE/tree/main/HomeWorks/Forensics/HW2