

Домашняя работа №2

Анализ дампа оперативной памяти.

Шараев Евгений

Задание:

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.

```
In [1]: # Дамп оперативной памяти в файле var-1.vmem
# Также я буду использовать две версии volatility:
# под Python2 и под Python3
```

```
!ls -l
```

```
total 1049196
drwxr-xr-x 14 evgeny evgeny      4096 Apr 11 17:06 distorm
drwxr-xr-x 14 evgeny evgeny      4096 Apr 11 17:14 distorm3
drwxr-xr-x  7 evgeny evgeny      4096 Apr  2 11:13 env
-rw-r--r--  1 evgeny evgeny    100910 Apr 12 12:38 sharaev_evgeny_
hw2.ipynb
-rw-r--r--  1 evgeny evgeny      504048 Apr 12 12:18 sharaev_evgeny_
hw2.pdf
-rw-r--r--  1 evgeny evgeny 1073741824 May 25  2023 var-1.vmem
drwxr-xr-x  8 evgeny evgeny      4096 Apr 11 16:10 volatility
drwxr-xr-x  8 evgeny evgeny      4096 Apr  2 10:17 volatility3
```

```
In [2]: # Для этого у меня установлено сразу обе версии интерпретаторов

!python2.7 --version
!python3 --version

Python 2.7.13
Python 3.11.2
```

```
In [3]: # Используемая мной версия программы volatility

!python2.7 volatility/vol.py -h | grep "Framework 2"
!python3 volatility3/vol.py -h | grep " Framework 2"

Volatility Foundation Volatility Framework 2.6.1
Volatility 3 Framework 2.7.0
```

```
In [4]: # 1. Определите семейство и версию операционной системы на компьютере
# Джона.

!python2.7 volatility/vol.py -f var-1.vmem imageinfo | grep -v Failed

Volatility Foundation Volatility Framework 2.6.1
INFO      : volatility.debug      : Determining profile based on KDBG s
earch...
          Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2S
P0x64, Win2008R2SP1x64_24000, Win2008R2SP1x64_23418, Win2008R2SP1x6
4, Win7SP1x64_24000, Win7SP1x64_23418
          AS Layer1 : WindowsAMD64PagedMemory (Kernel A
S)
          AS Layer2 : FileAddressSpace (/home/evgeny/Pro
jects/forensic/var-1.vmem)
          PAE type  : No PAE
          DTB       : 0x187000L
          KDBG      : 0xf80002bfd0a0L
          Number of Processors : 1
          Image Type (Service Pack) : 1
          KPCR for CPU 0 : 0xffffffff80002bfed00L
          KUSER_SHARED_DATA : 0xffffffff78000000000L
          Image date and time : 2020-12-27 23:06:01 UTC+0000
          Image local date and time : 2020-12-28 00:06:01 +0100
```

```
In [5]: # Ответ: Наиболее вероятно Windows 7
```

```
In [6]: # 2. Какой процесс на компьютере Джона установил сетевое соединение
# с участием порта 554?

!python3 volatility3/vol.py \
  --filters LocalPort,554 \
  --file var-1.vmem \
  windows.netscan.NetScan
```

Volatility 3 Framework 2.7.0
WARNING volatility3.framework.layers.vmware: No metadata file found alongside VMEM file. A VMSS or VMSN file may be required to correctly process a VMEM file. These should be placed in the same directory with the same file name, e.g. var-1.vmem and var-1.vmss.
Progress: 100.00 PDB scanning finished

Offset	Proto	LocalAddr	LocalPort	ForeignAddr	ForeignPort	State	PID	Owner	Created
0x24d5c8c0	TCPv4	0.0.0.0	554	0.0.0.0	0	LISTENING			
2368		wmpnetwk.exe	-						
0x37a47480	TCPv4	0.0.0.0	554	0.0.0.0	0	LISTENING			
2368		wmpnetwk.exe	-						
0x37a47480	TCPv6	::	554	::	0	LISTENING			
2368		wmpnetwk.exe	-						

```
In [7]: # Проверяем на версии 2

!python2.7 volatility/vol.py \
  --file var-1.vmem \
  --profile Win7SP1x64 \
  netscan | grep -v "Failed" | grep 554
```

Offset(P) Proto Local Address Foreign Address

Offset(P)	Proto	Local Address	Foreign Address
0x24d5c8c0	TCPv4	0.0.0.0:554	0.0.0.0:
0	LISTENING	2368 wmpnetwk.exe	
0x37a47480	TCPv4	0.0.0.0:554	0.0.0.0:
0	LISTENING	2368 wmpnetwk.exe	
0x37a47480	TCPv6	:::554	:::0
LISTENING	2368	wmpnetwk.exe	

```
In [8]: # Ответ: Процесс PID 2368
```

In [9]: *# 3. Устанавливались ли сетевые соединения компьютера Джона
с участием локальных портов в диапазоне 135-140?*

```
!python3 volatility3/vol.py \  
--filters LocalPort,135 \  
--filters LocalPort,136 \  
--filters LocalPort,137 \  
--filters LocalPort,138 \  
--filters LocalPort,139 \  
--filters LocalPort,140 \  
--file var-1.vmem \  
windows.netscan.NetScan
```


Volatility 3 Framework 2.7.0
WARNING volatility3.framework.layers.vmware: No metadata file found alongside VMEM file. A VMSS or VMSN file may be required to correctly process a VMEM file. These should be placed in the same directory with the same file name, e.g. var-1.vmem and var-1.vmss.
Progress: 100.00 PDB scanning finished

Offset	Proto	LocalAddr	LocalPort	ForeignAddr	ForeignPort	State	PID	Owner	Created
0x3692a6d0	UDPv4	0.0.0.0	51351	*	0				940
svchost.exe		2020-12-27 23:05:56.000000							
0x3692a6d0	UDPv6	::	51351	*	0				940
svchost.exe		2020-12-27 23:05:56.000000							
0x3d6072c0	TCPv4	0.0.0.0	135	0.0.0.0	0	LISTENING			
700	svchost.exe	-							
0x3d6075c0	TCPv4	0.0.0.0	135	0.0.0.0	0	LISTENING			
700	svchost.exe	-							
0x3d6075c0	TCPv6	::	135	::	0	LISTENING			
700	svchost.exe	-							
0x3d721e20	UDPv4	192.168.136.131	137	*	0				
4	System	2020-12-27 22:50:58.000000							
0x3d7331c0	TCPv4	192.168.136.131	139	0.0.0.0	0	LIS			
TENING	4	System	-						
0x3d736010	UDPv4	192.168.136.131	138	*	0				
4	System	2020-12-27 22:50:58.000000							

In [10]: *# Проверяем на версии 2*

```
!python2.7 volatility/vol.py \  
--file var-1.vmem \  
--profile Win7SP1x64 \  
netscan | grep -v "Failed" | grep -e "135" -e "136" -e "137" -e
```

<i># Offset(P)</i>	<i>Proto</i>	<i>Local Address</i>	<i>Foreign</i>
--------------------	--------------	----------------------	----------------



```

Volatility Foundation Volatility Framework 2.6.1
0 added 3900      UDPv4      127.0.0.1:62336      *: *
1408      svchost.exe      2020-12-27 22:51:00 UTC+0000
0 added 3ec0      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
0x29a53010      UDPv6      ::1:1900      *: *
1408      svchost.exe      2020-12-27 22:51:00 UTC+0000
0x29a53290      UDPv4      127.0.0.1:1900      *: *
1408      svchost.exe      2020-12-27 22:51:00 UTC+0000
0x29a53950      UDPv4      192.168.136.131:1900      *: *
1408      svchost.exe      2020-12-27 22:51:00 UTC+0000
0x2a453010      UDPv6      fe80::bda1:b28:fab2:a38c:62333      *: *
1408      svchost.exe      2020-12-27 22:51:00 UTC+0000
0x2a453800      UDPv6      fe80::bda1:b28:fab2:a38c:1900      *: *
1408      svchost.exe      2020-12-27 22:51:00 UTC+0000
0x2afd7450      UDPv4      0.0.0.0:3702      *: *
1408      svchost.exe      2020-12-27 22:52:12 UTC+0000
0x2b7e58e0      UDPv4      0.0.0.0:3702      *: *
1408      svchost.exe      2020-12-27 22:52:12 UTC+0000
0x2b7e58e0      UDPv6      ::3702      *: *
1408      svchost.exe      2020-12-27 22:52:12 UTC+0000
0x308d3ec0      UDPv4      192.168.136.131:62335      *: *
1408      svchost.exe      2020-12-27 22:51:00 UTC+0000
0x32726010      UDPv4      0.0.0.0:55377      *: *
1408      svchost.exe      2020-12-27 22:50:53 UTC+0000
0x32726010      UDPv6      ::55377      *: *
1408      svchost.exe      2020-12-27 22:50:53 UTC+0000
0x343a8010      UDPv4      0.0.0.0:55376      *: *
1408      svchost.exe      2020-12-27 22:50:53 UTC+0000
0x3692a6d0      UDPv4      0.0.0.0:51351      *: *
940      svchost.exe      2020-12-27 23:05:56 UTC+0000
0x3692a6d0      UDPv6      ::51351      *: *
940      svchost.exe      2020-12-27 23:05:56 UTC+0000
0x3d64e320      UDPv4      0.0.0.0:3702      *: *
1408      svchost.exe      2020-12-27 22:52:12 UTC+0000
0x3d64e320      UDPv6      ::3702      *: *
1408      svchost.exe      2020-12-27 22:52:12 UTC+0000
0x3d721e20      UDPv4      192.168.136.131:137      *: *
4      System      2020-12-27 22:50:58 UTC+0000
0x3d736010      UDPv4      192.168.136.131:138      *: *
4      System      2020-12-27 22:50:58 UTC+0000
0x3d6072c0      TCPv4      0.0.0.0:135      0.0.0.0:
0      LISTENING      700      svchost.exe
0x3d6075c0      TCPv4      0.0.0.0:135      0.0.0.0:
0      LISTENING      700      svchost.exe
0x3d6075c0      TCPv6      :::135      :::0
LISTENING      700      svchost.exe
0x3d7331c0      TCPv4      192.168.136.131:139      0.0.0.0:
0      LISTENING      4      System

```

In [11]: # Ответ: да, устанавливались.

In [12]: # 4. Если такие соединения устанавливались, укажите идентификаторы
процессов, устанавливавших такие соединения.

In [13]: # Ответ: PID 4, PID 700

In [14]: # 5. Укажите идентификатор процессов-родителей данных процессов.

```
!python3 volatility3/vol.py \
  --filters PID,700 \
  --filters PID,4 \
  --file var-1.vmem \
  windows.pslist
```

Volatility 3 Framework 2.7.0

WARNING volatility3.framework.layers.vmware: No metadata file found alongside VMEM file. A VMSS or VMSN file may be required to correctly process a VMEM file. These should be placed in the same directory with the same file name, e.g. var-1.vmem and var-1.vmss.

Progress: 100.00

PDB scanning finished

PID	PPID	ImageFileName	Offset(V)	Threads	Handles	Ses
sionId	Wow64	CreateTime	ExitTime	File output		
4	0	System	0xfa80024b36f0	87	550	N/A
se	2020-12-27 22:50:39.000000		N/A	Disabled		
348	340	csrss.exe	0xfa8004402b30	8	484	0
False	2020-12-27 22:50:40.000000		N/A	Disabled		
400	340	wininit.exe	0xfa8004663560	3	75	0
False	2020-12-27 22:50:41.000000		N/A	Disabled		
412	392	csrss.exe	0xfa80043bdb30	10	196	1
False	2020-12-27 22:50:41.000000		N/A	Disabled		
460	392	winlogon.exe	0xfa80046b3060	3	112	1
False	2020-12-27 22:50:41.000000		N/A	Disabled		
524	400	lsmd.exe	0xfa8004868b30	9	141	0
se	2020-12-27 22:50:44.000000		N/A	Disabled		
700	508	svchost.exe	0xfa8004bfa740	6	273	0
False	2020-12-27 22:50:48.000000		N/A	Disabled		
940	508	svchost.exe	0xfa8004ddfab0	17	384	0
False	2020-12-27 22:50:52.000000		N/A	Disabled		
1144	1124	explorer.exe	0xfa8004e82b30	22	742	1
False	2020-12-27 22:50:52.000000		N/A	Disabled		
1224	508	taskhost.exe	0xfa8004f042c0	7	145	1
False	2020-12-27 22:50:52.000000		N/A	Disabled		
1248	508	svchost.exe	0xfa8004f19060	19	325	0
False	2020-12-27 22:50:52.000000		N/A	Disabled		
1408	508	svchost.exe	0xfa8004fd3b30	22	308	0
False	2020-12-27 22:50:52.000000		N/A	Disabled		
1480	508	VGAAuthService.	0xfa8004fbc3b30	3	84	0
False	2020-12-27 22:50:52.000000		N/A	Disabled		
1040	508	msdtc.exe	0xfa800532a690	12	144	0
False	2020-12-27 22:50:57.000000		N/A	Disabled		
2240	508	SearchIndexer.	0xfa80053ee4e0	13	593	0
False	2020-12-27 22:50:59.000000		N/A	Disabled		
2824	612	WmiPrvSE.exe	0xfa80053f6060	8	215	0
False	2020-12-27 22:51:01.000000		N/A	Disabled		
1204	508	mscorsvw.exe	0xfa8004749710	7	73	0
False	2020-12-27 22:52:55.000000		N/A	Disabled		
724	508	sppsvc.exe	0xfa80052f0060	4	150	0
False	2020-12-27 22:52:56.000000		N/A	Disabled		
2488	412	conhost.exe	0xfa8002784450	2	51	1
False	2020-12-27 23:04:50.000000		N/A	Disabled		

In [15]: *# Проверяем на версии 2*

```
!python2.7 volatility/vol.py \  
--file var-1.vmem \  
--profile Win7SP1x64 \  
pslist | grep -v "Failed" | grep -e "4" -e "700"
```

<i>#</i>	<i>Offset(V)</i>	<i>Name</i>	<i>PID</i>	<i>PPID</i>	<i>Thds</i>	<i>H</i>
----------	------------------	-------------	------------	-------------	-------------	----------

Volatility Foundation Volatility Framework 2.6.1

Offset(V)	Name	PID	PPID	Thds	Hn
ds Sess Wow64 Start			Exit		
0xffffffffa80024b36f0	System	4	0	87	5
50 -----	0 2020-12-27 22:50:39 UTC+0000				
0xffffffffa8003ad8780	smss.exe	260	4	2	
29 -----	0 2020-12-27 22:50:39 UTC+0000				
0xffffffffa8004402b30	csrss.exe	348	340	8	4
84 0	0 2020-12-27 22:50:40 UTC+0000				
0xffffffffa8004663560	wininit.exe	400	340	3	
75 0	0 2020-12-27 22:50:41 UTC+0000				
0xffffffffa80043bdb30	csrss.exe	412	392	10	1
96 1	0 2020-12-27 22:50:41 UTC+0000				
0xffffffffa80046b3060	winlogon.exe	460	392	3	1
12 1	0 2020-12-27 22:50:41 UTC+0000				
0xffffffffa8004864060	services.exe	508	400	8	2
20 0	0 2020-12-27 22:50:43 UTC+0000				
0xffffffffa800485e910	lsass.exe	516	400	7	7
08 0	0 2020-12-27 22:50:44 UTC+0000				
0xffffffffa8004868b30	lsmd.exe	524	400	9	1
41 0	0 2020-12-27 22:50:44 UTC+0000				
0xffffffffa8004bf3610	svchost.exe	612	508	9	3
50 0	0 2020-12-27 22:50:46 UTC+0000				
0xffffffffa8004bf2060	vm3dservice.ex	676	508	3	
44 0	0 2020-12-27 22:50:48 UTC+0000				
0xffffffffa8004bfa740	svchost.exe	700	508	6	2
73 0	0 2020-12-27 22:50:48 UTC+0000				
0xffffffffa8004c5fb30	svchost.exe	812	508	23	5
76 0	0 2020-12-27 22:50:49 UTC+0000				
0xffffffffa8004cb0390	svchost.exe	852	508	26	5
30 0	0 2020-12-27 22:50:49 UTC+0000				
0xffffffffa8004cc7b30	svchost.exe	896	508	40	9
39 0	0 2020-12-27 22:50:49 UTC+0000				
0xffffffffa8004cfdb30	svchost.exe	296	508	18	7
59 0	0 2020-12-27 22:50:50 UTC+0000				
0xffffffffa8004ddf0b0	svchost.exe	940	508	17	3
84 0	0 2020-12-27 22:50:52 UTC+0000				
0xffffffffa8004e58630	dwm.exe	1132	852	3	
69 1	0 2020-12-27 22:50:52 UTC+0000				
0xffffffffa8004e82b30	explorer.exe	1144	1124	22	7
42 1	0 2020-12-27 22:50:52 UTC+0000				
0xffffffffa8004e3e740	spoolsv.exe	1192	508	13	2
67 0	0 2020-12-27 22:50:52 UTC+0000				
0xffffffffa8004f042c0	taskhost.exe	1224	508	7	1
45 1	0 2020-12-27 22:50:52 UTC+0000				
0xffffffffa8004f19060	svchost.exe	1248	508	19	3
25 0	0 2020-12-27 22:50:52 UTC+0000				
0xffffffffa8004fd3b30	svchost.exe	1408	508	22	3
08 0	0 2020-12-27 22:50:52 UTC+0000				
0xffffffffa8004fbcb30	VGAuthService.	1480	508	3	
84 0	0 2020-12-27 22:50:52 UTC+0000				
0xffffffffa8004ee4910	vmtoolsd.exe	1516	508	11	2
67 0	0 2020-12-27 22:50:53 UTC+0000				
0xffffffffa800518f890	vm3dservice.ex	1988	1144	2	
48 1	0 2020-12-27 22:50:53 UTC+0000				
0xffffffffa800516a2f0	vmtoolsd.exe	1996	1144	8	1
68 1	0 2020-12-27 22:50:53 UTC+0000				
0xffffffffa800532a690	msdtc.exe	1040	508	12	1
44 0	0 2020-12-27 22:50:57 UTC+0000				
0xffffffffa80053ee4e0	SearchIndexer.	2240	508	13	5
93 0	0 2020-12-27 22:50:59 UTC+0000				

0xffffffffa8005433060	wmpnetwk.exe	2368	508	13	4
17 0 0 2020-12-27 22:51:00 UTC+0000					
0xffffffffa800547db30	svchost.exe	2632	508	9	3
49 0 0 2020-12-27 22:51:00 UTC+0000					
0xffffffffa80053f6060	WmiPrvSE.exe	2824	612	8	2
15 0 0 2020-12-27 22:51:01 UTC+0000					
0xffffffffa8004749710	mscorsvw.exe	1204	508	7	
73 0 0 2020-12-27 22:52:55 UTC+0000					
0xffffffffa80052f0060	sppsvc.exe	724	508	4	1
50 0 0 2020-12-27 22:52:56 UTC+0000					
0xffffffffa8005686060	audiodg.exe	2336	812	4	1
22 0 0 2020-12-27 23:04:49 UTC+0000					
0xffffffffa80027906f0	cmd.exe	1920	1144	1	
20 1 0 2020-12-27 23:04:50 UTC+0000					
0xffffffffa8002784450	conhost.exe	2488	412	2	
51 1 0 2020-12-27 23:04:50 UTC+0000					

```
In [16]: # Ответ
# PPID(PID 4) --> PID 0
# PPID(PID 700) --> PID 508
```

```
In [17]: # 6. Укажите все процессы, порожденные процессами, устанавливавшими
# выявленные в пункте 3 соединения.
# Если соединения породили PID 4 и 700 то порожденные ими процессы -
# это их дети и в колонке PPID они будут иметь процессы 700 и 4

!python3 volatility3/vol.py \
  --filters PPID,700 \
  --filters PPID,4 \
  --file var-1.vmem \
  windows.pslist
```

Volatility 3 Framework 2.7.0

WARNING volatility3.framework.layers.vmware: No metadata file found alongside VMEM file. A VMSS or VMSN file may be required to correctly process a VMEM file. These should be placed in the same directory with the same file name, e.g. var-1.vmem and var-1.vmss.

Progress: 100.00

PDB scanning finished

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

260	4	smss.exe	0xfa8003ad8780	2	29	N/A
False	2020-12-27 22:50:39.000000		N/A	Disabled		
348	340	csrss.exe	0xfa8004402b30	8	484	0
False	2020-12-27 22:50:40.000000		N/A	Disabled		
400	340	wininit.exe	0xfa8004663560	3	75	0
False	2020-12-27 22:50:41.000000		N/A	Disabled		
508	400	services.exe	0xfa8004864060	8	220	0
False	2020-12-27 22:50:43.000000		N/A	Disabled		
516	400	lsass.exe	0xfa800485e910	7	708	0
False	2020-12-27 22:50:44.000000		N/A	Disabled		
524	400	lsmd.exe	0xfa8004868b30	9	141	0
False	2020-12-27 22:50:44.000000		N/A	Disabled		
1144	1124	explorer.exe	0xfa8004e82b30	22	742	1
False	2020-12-27 22:50:52.000000		N/A	Disabled		
1988	1144	vm3dservice.exe	0xfa800518f890	2	48	1
False	2020-12-27 22:50:53.000000		N/A	Disabled		
1996	1144	vmtoolsd.exe	0xfa800516a2f0	8	168	1
False	2020-12-27 22:50:53.000000		N/A	Disabled		
1920	1144	cmd.exe	0xfa80027906f0	1	20	1
False	2020-12-27 23:04:50.000000		N/A	Disabled		
2488	412	conhost.exe	0xfa8002784450	2	51	1
False	2020-12-27 23:04:50.000000		N/A	Disabled		

In [18]: *# Также проверю в плагине pstree*

```
!python3 volatility3/vol.py \  
  --filters PPID,4 \  
  --filters PPID,700 \  
  --file var-1.vmem \  
  windows.pstree
```

Volatility 3 Framework 2.7.0

WARNING volatility3.framework.layers.vmware: No metadata file found alongside VMEM file. A VMSS or VMSN file may be required to correctly process a VMEM file. These should be placed in the same directory with the same file name, e.g. var-1.vmem and var-1.vsss.

Progress: 100.00 PDB scanning finished

PID	PPID	ImageFileName	Offset(V)	Threads	Handles	Ses
sionId	Wow64	CreateTime	ExitTime	Audit	Cmd	Pat
h						

* 260	4	smss.exe	0xfa8003ad8780	2	29	N/A
False	2020-12-27 22:50:39.000000	N/A	\Device\HarddiskVol			
		ume2\Windows\System32\smss.exe	\SystemRoot\System32\smss.exe	\Sy		
		systemRoot\System32\smss.exe				
348	340	csrss.exe	0xfa8004402b30	8	484	0
False	2020-12-27 22:50:40.000000	N/A	\Device\HarddiskVol			
		ume2\Windows\System32\csrss.exe	%SystemRoot%\system32\csrss.exe	Obj		
			ectDirectory=\Windows SharedSection=1024,20480,768	Windows=On	SubSy	
			stemType=Windows	ServerDll=basesrv,1	ServerDll=winsrv:UserServerDll	
			Initialization,3	ServerDll=winsrv:ConServerDllInitialization,2	Serv	
			erDll=sxssrv,4	ProfileControl=Off	MaxRequestThreads=16	C:\Windows
			\system32\csrss.exe			
400	340	wininit.exe	0xfa8004663560	3	75	0
False	2020-12-27 22:50:41.000000	N/A	\Device\HarddiskVol			
		ume2\Windows\System32\wininit.exe	wininit.exe	C:\Windows		
			\system32\wininit.exe			
* 524	400	lsmd.exe	0xfa8004868b30	9	141	0
False	2020-12-27 22:50:44.000000	N/A	\Device\HarddiskVol			
		ume2\Windows\System32\lsmd.exe	C:\Windows\system32\lsmd.exe			
			C:\Windows\system32\lsmd.exe			
* 508	400	services.exe	0xfa8004864060	8	220	0
False	2020-12-27 22:50:43.000000	N/A	\Device\HarddiskVol			
		ume2\Windows\System32\services.exe	C:\Windows\system32\service			
		s.exe	C:\Windows\system32\services.exe			
* 516	400	lsass.exe	0xfa800485e910	7	708	0
False	2020-12-27 22:50:44.000000	N/A	\Device\HarddiskVol			
		ume2\Windows\System32\lsass.exe	C:\Windows\system32\lsass.exe			
			C:\Windows\system32\lsass.exe			
* 2488	412	conhost.exe	0xfa8002784450	2	51	1
False	2020-12-27 23:04:50.000000	N/A	\Device\HarddiskVol			
		ume2\Windows\System32\conhost.exe	\\??\C:\Windows\system32\con			
		host.exe	C:\Windows\system32\conhost.exe			
1144	1124	explorer.exe	0xfa8004e82b30	22	742	1
False	2020-12-27 22:50:52.000000	N/A	\Device\HarddiskVol			
		ume2\Windows\explorer.exe	C:\Windows\Explorer.EXE	C:\Windows		
			\Explorer.EXE			
* 1920	1144	cmd.exe	0xfa80027906f0	1	20	1
False	2020-12-27 23:04:50.000000	N/A	\Device\HarddiskVol			
		ume2\Windows\System32\cmd.exe	"C:\Windows\System32\cmd.exe"			
			C:\Windows\System32\cmd.exe			
* 1996	1144	vmtoolsd.exe	0xfa800516a2f0	8	168	1
False	2020-12-27 22:50:53.000000	N/A	\Device\HarddiskVol			
		ume2\Program Files\VMware\VMware Tools\vmtoolsd.exe	"C:\Program			
		Files\VMware\VMware Tools\vmtoolsd.exe"	-n vmusr	C:\Program		
		Files\VMware\VMware Tools\vmtoolsd.exe				
* 1988	1144	vm3dservice.ex	0xfa800518f890	2	48	1
False	2020-12-27 22:50:53.000000	N/A	\Device\HarddiskVol			
		ume2\Windows\System32\vm3dservice.exe	"C:\Windows\System32\vm3dse			
		rvice.exe" -u	C:\Windows\System32\vm3dservice.exe			

```
In [19]: # Ответ:  
# PID 4 породил процесс PID 260  
# PID 700 не породил ни одного процесса
```

In [20]: *# А какие процессы были порождены процессом породившим процесс 700?*
То есть у каких процессов PPID 508

```
!python3 volatility3/vol.py \  
  --filters PPID,508 \  
  --file var-1.vmem \  
  windows.pslist
```

Volatility 3 Framework 2.7.0

WARNING volatility3.framework.layers.vmware: No metadata file found alongside VMEM file. A VMSS or VMSN file may be required to correctly process a VMEM file. These should be placed in the same directory with the same file name, e.g. var-1.vmem and var-1.vsss.

Progress: 100.00

PDB scanning finished

PID	PPID	ImageFileName	Offset(V)	Threads	Handles	Ses
sionId	Wow64	CreateTime	ExitTime	File	output	
612	508	svchost.exe	0xfa8004bf3610	9	350	0
False	2020-12-27 22:50:46.000000	N/A	Disabled			
676	508	vm3dservice.ex	0xfa8004bf2060	3	44	0
False	2020-12-27 22:50:48.000000	N/A	Disabled			
700	508	svchost.exe	0xfa8004bfa740	6	273	0
False	2020-12-27 22:50:48.000000	N/A	Disabled			
812	508	svchost.exe	0xfa8004c5fb30	23	576	0
False	2020-12-27 22:50:49.000000	N/A	Disabled			
852	508	svchost.exe	0xfa8004cb0390	26	530	0
False	2020-12-27 22:50:49.000000	N/A	Disabled			
896	508	svchost.exe	0xfa8004cc7b30	40	939	0
False	2020-12-27 22:50:49.000000	N/A	Disabled			
296	508	svchost.exe	0xfa8004cfdb30	18	759	0
False	2020-12-27 22:50:50.000000	N/A	Disabled			
940	508	svchost.exe	0xfa8004ddfab0	17	384	0
False	2020-12-27 22:50:52.000000	N/A	Disabled			
1192	508	spoolsv.exe	0xfa8004e3e740	13	267	0
False	2020-12-27 22:50:52.000000	N/A	Disabled			
1224	508	taskhost.exe	0xfa8004f042c0	7	145	1
False	2020-12-27 22:50:52.000000	N/A	Disabled			
1248	508	svchost.exe	0xfa8004f19060	19	325	0
False	2020-12-27 22:50:52.000000	N/A	Disabled			
1408	508	svchost.exe	0xfa8004fd3b30	22	308	0
False	2020-12-27 22:50:52.000000	N/A	Disabled			
1480	508	VGAAuthService.	0xfa8004fbc30	3	84	0
False	2020-12-27 22:50:52.000000	N/A	Disabled			
1516	508	vmtoolsd.exe	0xfa8004ee4910	11	267	0
False	2020-12-27 22:50:53.000000	N/A	Disabled			
1932	508	dllhost.exe	0xfa800515d890	13	189	0
False	2020-12-27 22:50:53.000000	N/A	Disabled			
1040	508	msdtc.exe	0xfa800532a690	12	144	0
False	2020-12-27 22:50:57.000000	N/A	Disabled			
2240	508	SearchIndexer.	0xfa80053ee4e0	13	593	0
False	2020-12-27 22:50:59.000000	N/A	Disabled			
2368	508	wmpnetwk.exe	0xfa8005433060	13	417	0
False	2020-12-27 22:51:00.000000	N/A	Disabled			
2632	508	svchost.exe	0xfa800547db30	9	349	0
False	2020-12-27 22:51:00.000000	N/A	Disabled			
1288	508	mscorsvw.exe	0xfa8005659a00	6	81	0
True	2020-12-27 22:52:53.000000	N/A	Disabled			
1204	508	mscorsvw.exe	0xfa8004749710	7	73	0
False	2020-12-27 22:52:55.000000	N/A	Disabled			
724	508	sppsvc.exe	0xfa80052f0060	4	150	0
False	2020-12-27 22:52:56.000000	N/A	Disabled			
2008	508	svchost.exe	0xfa80031d3060	12	317	0
False	2020-12-27 22:52:56.000000	N/A	Disabled			

In [21]: # А ВОТ ТУТ МНОГО ВСЕГО

In [22]: *# 7. Установите, сколько различных процессов svchost.exe запускалось
приведите идентификаторы запущенных процессов.*

```
!python3 volatility3/vol.py \
  --filters ImageFileName,svchost.exe \
  --file var-1.vmem \
  windows.pslist
```

Volatility 3 Framework 2.7.0

WARNING volatility3.framework.layers.vmware: No metadata file found alongside VMEM file. A VMSS or VMSN file may be required to correctly process a VMEM file. These should be placed in the same directory with the same file name, e.g. var-1.vmem and var-1.vms.

Progress: 100.00

PDB scanning finished

PID	PPID	ImageFileName	Offset(V)	Threads	Handles	Ses
sionId	Wow64	CreateTime	ExitTime	File output		
612	508	svchost.exe	0xfa8004bf3610	9	350	0
False	2020-12-27 22:50:46.000000		N/A	Disabled		
700	508	svchost.exe	0xfa8004bfa740	6	273	0
False	2020-12-27 22:50:48.000000		N/A	Disabled		
812	508	svchost.exe	0xfa8004c5fb30	23	576	0
False	2020-12-27 22:50:49.000000		N/A	Disabled		
852	508	svchost.exe	0xfa8004cb0390	26	530	0
False	2020-12-27 22:50:49.000000		N/A	Disabled		
896	508	svchost.exe	0xfa8004cc7b30	40	939	0
False	2020-12-27 22:50:49.000000		N/A	Disabled		
296	508	svchost.exe	0xfa8004cfdb30	18	759	0
False	2020-12-27 22:50:50.000000		N/A	Disabled		
940	508	svchost.exe	0xfa8004ddf0b0	17	384	0
False	2020-12-27 22:50:52.000000		N/A	Disabled		
1248	508	svchost.exe	0xfa8004f19060	19	325	0
False	2020-12-27 22:50:52.000000		N/A	Disabled		
1408	508	svchost.exe	0xfa8004fd3b30	22	308	0
False	2020-12-27 22:50:52.000000		N/A	Disabled		
2632	508	svchost.exe	0xfa800547db30	9	349	0
False	2020-12-27 22:51:00.000000		N/A	Disabled		
2008	508	svchost.exe	0xfa80031d3060	12	317	0
False	2020-12-27 22:52:56.000000		N/A	Disabled		

In [23]: *# Ответ:
Всего 11 процессов с таким названием
PID 612, 700, 812, 852, 896, 296, 940, 1248, 1408, 2632, 2008*

In [24]: *# 8. Укажите имена исполняемых файлов, запустивших эти процессы.*

```
!python3 volatility3/vol.py \  
  --filters ImageFileName,svchost.exe \  
  --file var-1.vmem \  
  windows.pstree
```

Volatility 3 Framework 2.7.0

WARNING volatility3.framework.layers.vmware: No metadata file found alongside VMEM file. A VMSS or VMSN file may be required to correctly process a VMEM file. These should be placed in the same directory with the same file name, e.g. var-1.vmem and var-1.vsss.

Progress: 100.00 PDB scanning finished

PID	PPID	ImageFileName	Offset(V)	Threads	Handles	Ses
sionId	Wow64	CreateTime	ExitTime	Audit	Cmd	Pat

** 896	508	svchost.exe	0xfa8004cc7b30	40	939	0
False	2020-12-27 22:50:49.000000	N/A	\Device\HarddiskVol			
ume2\Windows\System32\svchost.exe		C:\Windows\system32\svchos				
t.exe -k netsvcs		C:\Windows\system32\svchost.exe				
** 1408	508	svchost.exe	0xfa8004fd3b30	22	308	0
False	2020-12-27 22:50:52.000000	N/A	\Device\HarddiskVol			
ume2\Windows\System32\svchost.exe		C:\Windows\system32\svchos				
t.exe -k LocalServiceAndNoImpersonation		C:\Windows\system32\svchos				
t.exe						
** 296	508	svchost.exe	0xfa8004cfd3b30	18	759	0
False	2020-12-27 22:50:50.000000	N/A	\Device\HarddiskVol			
ume2\Windows\System32\svchost.exe		C:\Windows\system32\svchos				
t.exe -k LocalService		C:\Windows\system32\svchost.exe				
** 812	508	svchost.exe	0xfa8004c5fb30	23	576	0
False	2020-12-27 22:50:49.000000	N/A	\Device\HarddiskVol			
ume2\Windows\System32\svchost.exe		C:\Windows\System32\svchos				
t.exe -k LocalServiceNetworkRestricted		C:\Windows\System32\svchos				
t.exe						
** 940	508	svchost.exe	0xfa8004ddfab0	17	384	0
False	2020-12-27 22:50:52.000000	N/A	\Device\HarddiskVol			
ume2\Windows\System32\svchost.exe		C:\Windows\system32\svchos				
t.exe -k NetworkService		C:\Windows\system32\svchost.exe				
** 700	508	svchost.exe	0xfa8004bfa740	6	273	0
False	2020-12-27 22:50:48.000000	N/A	\Device\HarddiskVol			
ume2\Windows\System32\svchost.exe		C:\Windows\system32\svchos				
t.exe -k RPCSS		C:\Windows\system32\svchost.exe				
** 2632	508	svchost.exe	0xfa800547db30	9	349	0
False	2020-12-27 22:51:00.000000	N/A	\Device\HarddiskVol			
ume2\Windows\System32\svchost.exe		C:\Windows\System32\svchos				
t.exe -k LocalServicePeerNet		C:\Windows\System32\svchost.exe				
** 852	508	svchost.exe	0xfa8004cb0390	26	530	0
False	2020-12-27 22:50:49.000000	N/A	\Device\HarddiskVol			
ume2\Windows\System32\svchost.exe		C:\Windows\System32\svchos				
t.exe -k LocalSystemNetworkRestricted		C:\Windows\System32\svchos				
t.exe						
** 2008	508	svchost.exe	0xfa80031d3060	12	317	0
False	2020-12-27 22:52:56.000000	N/A	\Device\HarddiskVol			
ume2\Windows\System32\svchost.exe		C:\Windows\System32\svchos				
t.exe -k secsvcs		C:\Windows\System32\svchost.exe				
** 1248	508	svchost.exe	0xfa8004f19060	19	325	0
False	2020-12-27 22:50:52.000000	N/A	\Device\HarddiskVol			
ume2\Windows\System32\svchost.exe		C:\Windows\system32\svchos				
t.exe -k LocalServiceNoNetwork		C:\Windows\system32\svchost.exe				
** 612	508	svchost.exe	0xfa8004bf3610	9	350	0
False	2020-12-27 22:50:46.000000	N/A	\Device\HarddiskVol			
ume2\Windows\System32\svchost.exe		C:\Windows\system32\svchos				
t.exe -k DcomLaunch		C:\Windows\system32\svchost.exe				

In [25]: *# Проверю эти данные в cmdline*

```
!python2.7 volatility/vol.py \  
  --file var-1.vmem \  
  --profile Win7SP1x64 \  
  cmdline | grep -v "Failed" | grep svchost.exe
```

```
Volatility Foundation Volatility Framework 2.6.1  
svchost.exe pid: 612  
Command line : C:\Windows\system32\svchost.exe -k DcomLaunch  
svchost.exe pid: 700  
Command line : C:\Windows\system32\svchost.exe -k RPCSS  
svchost.exe pid: 812  
Command line : C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted  
svchost.exe pid: 852  
Command line : C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted  
svchost.exe pid: 896  
Command line : C:\Windows\system32\svchost.exe -k netsvcs  
svchost.exe pid: 296  
Command line : C:\Windows\system32\svchost.exe -k LocalService  
svchost.exe pid: 940  
Command line : C:\Windows\system32\svchost.exe -k NetworkService  
svchost.exe pid: 1248  
Command line : C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork  
svchost.exe pid: 1408  
Command line : C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation  
svchost.exe pid: 2632  
Command line : C:\Windows\System32\svchost.exe -k LocalServicePeerNetwork  
svchost.exe pid: 2008  
Command line : C:\Windows\System32\svchost.exe -k secsvcs
```

In [26]: *# Ответ:*

```
# Все процессы svchost.exe были запущены из файла  
# C:\Windows\system32\svchost.exe
```

In [27]: *# 9. Среди процессов, выявленных в пункте 7, определите те, которые
содержат признаки заражения.*

PID 612 - Нет признаков заражения

```
!python3 volatility3/vol.py \
  --file var-1.vmem \
  windows.malfind.Malfind \
  --pid 612
```

Volatility 3 Framework 2.7.0

WARNING volatility3.framework.layers.vmware: No metadata file found alongside VMEM file. A VMSS or VMSN file may be required to correctly process a VMEM file. These should be placed in the same directory with the same file name, e.g. var-1.vmem and var-1.vmss.

Progress: 100.00

PDB scanning finished

PID	Process	Start VPN	End VPN	Tag	Protection	CommitCharge	PrivateMemory	File output	Notes	Hexdump	Disasm

In [28]: *# PID 700 - Нет признаков заражения*

```
!python3 volatility3/vol.py \
  --file var-1.vmem \
  windows.malfind.Malfind \
  --pid 700
```

Volatility 3 Framework 2.7.0

WARNING volatility3.framework.layers.vmware: No metadata file found alongside VMEM file. A VMSS or VMSN file may be required to correctly process a VMEM file. These should be placed in the same directory with the same file name, e.g. var-1.vmem and var-1.vmss.

Progress: 100.00

PDB scanning finished

PID	Process	Start VPN	End VPN	Tag	Protection	CommitCharge	PrivateMemory	File output	Notes	Hexdump	Disasm

In [29]: *# PID 812 - Есть признаки заражения*

```
!python3 volatility3/vol.py \
  --file var-1.vmem \
  windows.malfind.Malfind \
  --pid 812
```

Volatility 3 Framework 2.7.0

WARNING volatility3.framework.layers.vmware: No metadata file found alongside VMEM file. A VMSS or VMSN file may be required to correctly process a VMEM file. These should be placed in the same directory with the same file name, e.g. var-1.vmem and var-1.vmss.

Progress: 100.00

PDB scanning finished

PID	Process	Start VPN	End VPN	Tag	Protection	Com
mitCharge	PrivateMemory	File output	Notes	Hexdump	Dis	asm

812	svchost.exe	0x1430000	0x143ffff	VadS	PAG	
E_EXECUTE_READWRITE	16	1	Disabled	N/A		
41 ba 80 00 00 00 48 b8	A.....H.					
38 a1 13 ff fe 07 00 00	8.....					
48 ff 20 90 41 ba 81 00	H...A...					
00 00 48 b8 38 a1 13 ff	..H.8...					
fe 07 00 00 48 ff 20 90H...					
41 ba 82 00 00 00 48 b8	A.....H.					
38 a1 13 ff fe 07 00 00	8.....					
48 ff 20 90 41 ba 83 00	H...A...					
0x1430000:	mov r10d, 0x80					
0x1430006:	movabs rax, 0x7feff13a138					
0x1430010:	jmp qword ptr [rax]					
0x1430013:	nop					
0x1430014:	mov r10d, 0x81					
0x143001a:	movabs rax, 0x7feff13a138					
0x1430024:	jmp qword ptr [rax]					
0x1430027:	nop					
0x1430028:	mov r10d, 0x82					
0x143002e:	movabs rax, 0x7feff13a138					
0x1430038:	jmp qword ptr [rax]					
0x143003b:	nop					

In [30]: *# PID 852 - Нет признаков заражения*

```
!python3 volatility3/vol.py \
  --file var-1.vmem \
  windows.malfind.Malfind \
  --pid 852
```

Volatility 3 Framework 2.7.0

WARNING volatility3.framework.layers.vmware: No metadata file found alongside VMEM file. A VMSS or VMSN file may be required to correctly process a VMEM file. These should be placed in the same directory with the same file name, e.g. var-1.vmem and var-1.vmss.

Progress: 100.00

PDB scanning finished

PID	Process	Start VPN	End VPN	Tag	Protection	Com
mitCharge	PrivateMemory	File output	Notes	Hexdump	Dis	asm

In [31]: *# PID 896 - Нет признаков заражения*

```
!python3 volatility3/vol.py \
  --file var-1.vmem \
  windows.malfind.Malfind \
  --pid 896
```

Volatility 3 Framework 2.7.0

WARNING volatility3.framework.layers.vmware: No metadata file found alongside VMEM file. A VMSS or VMSN file may be required to correctly process a VMEM file. These should be placed in the same directory with the same file name, e.g. var-1.vmem and var-1.vms.

Progress: 100.00

PDB scanning finished

PID	Process	Start VPN	End VPN	Tag	Protection	Com
mitCharge	PrivateMemory	File output	Notes	Hexdump	Dis	asm

In [32]: *# PID 296 - Есть признаки заражения*

```
!python3 volatility3/vol.py \
  --file var-1.vmem \
  windows.malfind.Malfind \
  --pid 296
```

Volatility 3 Framework 2.7.0

WARNING volatility3.framework.layers.vmware: No metadata file found alongside VMEM file. A VMSS or VMSN file may be required to correctly process a VMEM file. These should be placed in the same directory with the same file name, e.g. var-1.vmem and var-1.vms.

Progress: 100.00

PDB scanning finished

PID	Process	Start VPN	End VPN	Tag	Protection	Com
mitCharge	PrivateMemory	File output	Notes	Hexdump	Dis	asm

296	svchost.exe	0xeb0000	0xebffff	VadS	PAG
E_EXECUTE_READWRITE	16	1	Disabled	N/A	
41 ba 80 00 00 00 48 b8	A.....H.				
38 a1 13 ff fe 07 00 00	8.....				
48 ff 20 90 41 ba 81 00	H...A...				
00 00 48 b8 38 a1 13 ff	..H.8...				
fe 07 00 00 48 ff 20 90H...				
41 ba 82 00 00 00 48 b8	A.....H.				
38 a1 13 ff fe 07 00 00	8.....				
48 ff 20 90 41 ba 83 00	H...A...				
0xeb0000:	mov	r10d, 0x80			
0xeb0006:	movabs	rax, 0x7feff13a138			
0xeb0010:	jmp	qword ptr [rax]			
0xeb0013:	nop				
0xeb0014:	mov	r10d, 0x81			
0xeb001a:	movabs	rax, 0x7feff13a138			
0xeb0024:	jmp	qword ptr [rax]			
0xeb0027:	nop				
0xeb0028:	mov	r10d, 0x82			
0xeb002e:	movabs	rax, 0x7feff13a138			
0xeb0038:	jmp	qword ptr [rax]			
0xeb003b:	nop				

In [33]: *# PID 940 - Нет признаков заражения*

```
!python3 volatility3/vol.py \  
  --file var-1.vmem \  
  windows.malfind.Malfind \  
  --pid 940
```

Volatility 3 Framework 2.7.0
WARNING volatility3.framework.layers.vmware: No metadata file found alongside VMEM file. A VMSS or VMSN file may be required to correctly process a VMEM file. These should be placed in the same directory with the same file name, e.g. var-1.vmem and var-1.vmss.
Progress: 100.00 PDB scanning finished
PID Process Start VPN End VPN Tag Protection Com
mitCharge PrivateMemory File output Notes Hexdump Dis
asm

In [34]: *# PID 1248 - Нет признаков заражения*

```
!python3 volatility3/vol.py \  
  --file var-1.vmem \  
  windows.malfind.Malfind \  
  --pid 1248
```

Volatility 3 Framework 2.7.0
WARNING volatility3.framework.layers.vmware: No metadata file found alongside VMEM file. A VMSS or VMSN file may be required to correctly process a VMEM file. These should be placed in the same directory with the same file name, e.g. var-1.vmem and var-1.vmss.
Progress: 100.00 PDB scanning finished
PID Process Start VPN End VPN Tag Protection Com
mitCharge PrivateMemory File output Notes Hexdump Dis
asm

In [35]: *# PID 1408 - Нет признаков заражения*

```
!python3 volatility3/vol.py \  
  --file var-1.vmem \  
  windows.malfind.Malfind \  
  --pid 1408
```

Volatility 3 Framework 2.7.0
WARNING volatility3.framework.layers.vmware: No metadata file found alongside VMEM file. A VMSS or VMSN file may be required to correctly process a VMEM file. These should be placed in the same directory with the same file name, e.g. var-1.vmem and var-1.vmss.
Progress: 100.00 PDB scanning finished
PID Process Start VPN End VPN Tag Protection Com
mitCharge PrivateMemory File output Notes Hexdump Dis
asm

In [36]: *# PID 2362 - Нет признаков заражения*

```
!python3 volatility3/vol.py \  
  --file var-1.vmem \  
  windows.malfind.Malfind \  
  --pid 2632
```

Volatility 3 Framework 2.7.0

WARNING volatility3.framework.layers.vmware: No metadata file found alongside VMEM file. A VMSS or VMSN file may be required to correctly process a VMEM file. These should be placed in the same directory with the same file name, e.g. var-1.vmem and var-1.vmss.

Progress: 100.00

PDB scanning finished

PID	Process	Start VPN	End VPN	Tag	Protection	Com
mitCharge	PrivateMemory	File output	Notes	Hexdump	Dis	asm

In [37]: # PID 2008 - Есть признаки заражения

```
!python3 volatility3/vol.py \  
--file var-1.vmem \  
windows.malfind.Malfind \  
--pid 2008
```

```
Volatility 3 Framework 2.7.0  
WARNING volatility3.framework.layers.vmware: No metadata file found  
alongside VMEM file. A VMSS or VMSN file may be required to correctly  
process a VMEM file. These should be placed in the same directory with  
the same file name, e.g. var-1.vmem and var-1.vsss.  
Progress: 100.00 PDB scanning finished  
PID Process Start VPN End VPN Tag Protection Com  
mitCharge PrivateMemory File output Notes Hexdump Dis  
asm  
  
2008 svchost.exe 0x2600000 0x267ffff VadS PAG  
E_EXECUTE_READWRITE 128 1 Disabled N/A  
20 00 00 00 e0 ff 07 00 .....  
0c 00 00 00 01 00 05 00 .....  
00 42 00 50 00 30 00 70 .B.P.0.p  
00 60 00 00 00 00 00 00 .`.....  
48 8b 45 28 c7 00 00 00 H.E(....  
00 00 c7 40 04 00 00 00 ...@....  
00 48 8b 45 28 48 8d 40 .H.E(H.@  
08 48 89 c2 48 8b 45 20 .H..H.E.  
0x2600000: and byte ptr [rax], al  
0x2600002: add byte ptr [rax], al  
0x2600004: loopne 0x2600005  
2008 svchost.exe 0x4ea0000 0x4f9ffff VadS PAG  
E_EXECUTE_READWRITE 256 1 Disabled N/A  
20 00 00 00 e0 ff 0f 00 .....  
0c 00 00 00 01 00 05 00 .....  
00 42 00 50 00 30 00 70 .B.P.0.p  
00 60 00 00 00 00 00 00 .`.....  
ba fc ff ff ff 03 55 20 .....U.  
03 55 5c b9 04 00 1a 00 .U\.....  
4c 8b c5 ff 95 e0 37 00 L.....7.  
00 8b 4d 24 89 08 48 8d ..M$..H.  
0x4ea0000: and byte ptr [rax], al  
0x4ea0002: add byte ptr [rax], al  
0x4ea0004: loopne 0x4ea0005  
0x4ea0006: str word ptr [rax + rax]  
0x4ea000a: add byte ptr [rax], al  
0x4ea000c: add dword ptr [rax], eax  
0x4ea000e: add eax, 0x420000  
0x4ea0013: push rax  
0x4ea0014: add byte ptr [rax], dh  
0x4ea0016: add byte ptr [rax], dh
```

In [38]: *# 10. Установите, какое сообщение написал Джон в командной строке
в ходе сеанса, в момент которого был создан дамп.*

```
!python2.7 volatility/vol.py \  
  --file var-1.vmem \  
  --profile Win7SP1x64 \  
  consoles | grep -v "Failed"
```

Volatility Foundation Volatility Framework 2.6.1

ConsoleProcess: conhost.exe Pid: 2488

Console: 0xffa66200 CommandHistorySize: 50

HistoryBufferCount: 1 HistoryBufferMax: 4

OriginalTitle: %SystemRoot%\System32\cmd.exe

Title: Administrator: C:\Windows\System32\cmd.exe

AttachedProcess: cmd.exe Pid: 1920 Handle: 0x60

CommandHistory: 0x21e9c0 Application: cmd.exe Flags: Allocated, Res
et

CommandCount: 7 LastAdded: 6 LastDisplayed: 6

FirstCommand: 0 CommandCountMax: 50

ProcessHandle: 0x60

Cmd #0 at 0x1fe3a0: cd /

Cmd #1 at 0x1f78b0: echo THM{You_found_me} > test.txt

Cmd #2 at 0x21dcf0: cls

Cmd #3 at 0x1fe3c0: cd /Users

Cmd #4 at 0x1fe3e0: cd /John

Cmd #5 at 0x21db30: dir

Cmd #6 at 0x1fe400: cd John

Screen 0x200f70 X:80 Y:300

Dump:

C:\>cd /Users

C:\Users>cd /John

The system cannot find the path specified.

C:\Users>dir

Volume in drive C has no label.

Volume Serial Number is 1602-421F

Directory of C:\Users

12/27/2020	02:20 AM	<DIR>	.
12/27/2020	02:20 AM	<DIR>	..
12/27/2020	02:21 AM	<DIR>	John
04/12/2011	08:45 AM	<DIR>	Public
		0 File(s)	0 bytes
		4 Dir(s)	54,565,433,344 bytes free

C:\Users>cd John

C:\Users\John>

```
In [39]: # Ответ:
# Cmd #0 at 0x1fe3a0: cd /
# Cmd #1 at 0x1f78b0: echo THM{You_found_me} > test.txt
# Cmd #2 at 0x21dcf0: cls
# Cmd #3 at 0x1fe3c0: cd /Users
# Cmd #4 at 0x1fe3e0: cd /John
# Cmd #5 at 0x21db30: dir
# Cmd #6 at 0x1fe400: cd John
```