

13th lab of Forensics

Rodrigo Castillo

November 9, 2020



1 Read the section "Recopilación de evidencias" at page 19, and explain in your own words the order in which evidences must be gathered

the idea beside gathering evidences is to take a state of the system as close as can be possible, however, there are information that is more volatile than other, so the idea of gathering evidence is to prioritize the gathering of information that is more volatile before information that is not and can be gathered later.
the information that must be gathered is ...

1. content in the memory
2. connection state
3. state of process of execution
4. content inside the hard disks
5. content in hard drives

inside of volatile evidence , is important to check as fast as possible is...

1. date
2. processes that are running on the machine (top)
3. network processes
4. ports opened (TCP/UDP)
5. users connected remotely


2 captures

for the following task, i'll make one script that will execute all the commands listed on the table and then i'll explain every command on the table. The script...

```
netstat -a > netstat.txt
date > date.txt
cat /proc/version > version.txt
cat /proc/uptime > uptime.txt
netstat -l -p > netstat2.txt
history > historial.txt
df -k > df.txt

#ahora comprimo todo
zip -r evidence.zip .

#ahora muestro los procesos
top
```



1 captur

```
total 152
-rw-rw-r-- 1 r r 29 nov 9 16:44 date.txt
-rw-rw-r-- 1 r r 532 nov 9 16:44 df.txt
-rw-rw-r-- 1 r r 15797 nov 9 16:44 evidence.zip
-rw-rw-r-- 1 r r 20939 nov 9 16:44 historial.txt
-rwxrwxr-x 1 r r 220 nov 9 16:44 labforensics.sh
-rw-rw-r-- 1 r r 6752 nov 9 16:44 netstat2.txt
-rw-rw-r-- 1 r r 51384 nov 9 16:44 netstat.txt
-rw-rw-r-- 1 r r 32293 nov 9 16:43 procesos.txt
-rw-rw-r-- 1 r r 0 nov 9 16:44 top.txt
-rw-rw-r-- 1 r r 17 nov 9 16:44 uptime.txt
-rw-rw-r-- 1 r r 158 nov 9 16:44 version.txt
```

Figure 1: script and result

date: returns the current date .
df: returns the current state of the disks .
history: return the history of bash commands .
netstat: return the current state of wireless conexions.
top: return the current processes running.
uptime return the quantity of time that the machine has been on.
version return the linux version.

3 Practical part

```
Volatility Foundation Volatility Framework 2.6
INFO : volatility.debug : Determining profile based on KDBG search...
      Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
      AS Layer1 : IA32PagedMemoryPae (Kernel AS)
      AS Layer2 : FileAddressSpace (/home/r/Downloads/Windows XP Professional.vmem)
      PAE type : PAE
      DTB : 0x319000L
      KDBG : 0x80545b60L
      Number of Processors : 1
      Image Type (Service Pack) : 3
      KPCR for CPU 0 : 0xffdf000L
      KUSER_SHARED_DATA : 0xffdf000L
      Image date and time : 2011-09-30 00:26:30 UTC+0000
      Image local date and time : 2011-09-29 20:26:30 -0400
```

Figure 2: image info

```
r@r-Octopus:~/Downloads$ volatility pstree -t Windows\ XP\ Professional.vmem
Volatility Foundation Volatility Framework 2.6
```

Name	Pid	PPid	Thds	Hnds	Time
0x819cc830: System	4	0	60	209	1970-01-01 00:00:00 UTC+0000
. 0x818efda0: smss.exe	384	4	3	19	2011-09-26 01:33:32 UTC+0000
.. 0x81616ab8: csrss.exe	612	384	12	473	2011-09-26 01:33:35 UTC+0000
... 0x814c9b40: winlogon.exe	636	384	16	498	2011-09-26 01:33:35 UTC+0000
.... 0x81794d08: services.exe	680	636	15	271	2011-09-26 01:33:35 UTC+0000
..... 0x813685e0: spoolsv.exe	1516	680	14	159	2011-09-26 01:33:39 UTC+0000
..... 0x813a0458: MsMpEng.exe	1040	680	16	322	2011-09-26 01:33:36 UTC+0000
..... 0x815c9638: svchost.exe	1812	680	4	102	2011-09-26 01:33:46 UTC+0000
..... 0x812c1718: TPAutoConnSvc.e	2068	680	5	99	2011-09-26 01:33:55 UTC+0000
..... 0x81324020: TPAutoConnect.e	3372	2068	3	90	2011-09-26 01:33:59 UTC+0000
..... 0x818b5248: svchost.exe	944	680	11	274	2011-09-26 01:33:36 UTC+0000
..... 0x817f7548: svchost.exe	1200	680	6	81	2011-09-26 01:33:37 UTC+0000
..... 0x8169a1d0: svchost.exe	1336	680	14	172	2011-09-26 01:33:37 UTC+0000
..... 0x816b7020: svchost.exe	1076	680	87	1477	2011-09-26 01:33:36 UTC+0000
..... 0x812d6020: wscntfy.exe	2028	1076	3	63	2011-09-26 01:33:55 UTC+0000
..... 0x812b03e0: alg.exe	2272	680	7	112	2011-09-26 01:33:55 UTC+0000
..... 0x81336638: vmtoolsd.exe	200	680	5	234	2011-09-26 01:33:47 UTC+0000
..... 0x812f59a8: cmd.exe	3128	200	0	0	2011-09-30 00:26:30 UTC+0000
..... 0x813a5b28: svchost.exe	2000	680	6	119	2011-09-26 01:33:47 UTC+0000
..... 0x815c2630: vmacthlp.exe	852	680	1	25	2011-09-26 01:33:35 UTC+0000
..... 0x81470020: svchost.exe	868	680	17	199	2011-09-26 01:33:35 UTC+0000
..... 0x814e7b38: msisexec.exe	2396	680	5	127	2011-09-26 01:34:45 UTC+0000
..... 0x81329b28: VMUpgradeHelper	424	680	5	100	2011-09-26 01:33:48 UTC+0000
... 0x814a2cd0: lsass.exe	692	636	24	356	2011-09-26 01:33:35 UTC+0000
. 0x818f5cd0: explorer.exe	1752	1696	32	680	2011-09-26 01:33:45 UTC+0000
. 0x814db608: cmd.exe	3756	1752	3	56	2011-09-30 00:20:44 UTC+0000
. 0x818f6458: VMwareUser.exe	1888	1752	9	245	2011-09-26 01:33:47 UTC+0000
. 0x8164a020: mssec.exe	1900	1752	11	205	2011-09-26 01:33:47 UTC+0000
. 0x81717370: ctfmon.exe	1912	1752	3	93	2011-09-26 01:33:47 UTC+0000
. 0x8192d7f0: VMwareTray.exe	1876	1752	3	84	2011-09-26 01:33:46 UTC+0000

Figure 3: pstree

```
r@r-Octopus:~/Downloads$ volatility connscan -f Windows\ XP\ Professional.vmem
Volatility Foundation Volatility Framework 2.6
```

Offset(P)	Local Address	Remote Address	Pid
0x014f6ab0	10.0.0.109:1072	209.190.4.84:443	1752
0x01507380	10.0.0.109:1073	209.190.4.84:443	1752
0x016c2b00	10.0.0.109:1065	184.173.252.227:443	1752
0x017028a0	10.0.0.109:1067	184.173.252.227:443	1752
0x01858cb0	10.0.0.109:1068	209.190.4.84:443	1752

Figure 4: connscan

```
r@r-Octopus:~/Downloads$ volatility sockets -f Windows\ XP\ Professional.vmem
```

Volatility Foundation Volatility Framework 2.6						
Offset(V)	PID	Port	Proto	Protocol	Address	Create Time
0x812b15d0	4	0	47	GRE	0.0.0.0	2011-09-26 01:33:56 UTC+0000
0x812a8008	4	1030	6	TCP	0.0.0.0	2011-09-26 01:33:56 UTC+0000
0x813a5728	692	500	17	UDP	0.0.0.0	2011-09-26 01:33:47 UTC+0000
0x812a9b60	2272	1028	6	TCP	127.0.0.1	2011-09-26 01:33:56 UTC+0000
0x814c4008	1752	1073	6	TCP	0.0.0.0	2011-09-30 00:25:39 UTC+0000
0x818a3bf8	4	445	6	TCP	0.0.0.0	2011-09-26 01:33:32 UTC+0000
0x8179e730	944	135	6	TCP	0.0.0.0	2011-09-26 01:33:36 UTC+0000
0x812ade38	1076	1076	17	UDP	127.0.0.1	2011-09-30 00:26:30 UTC+0000
0x813a4e98	1752	1070	6	TCP	0.0.0.0	2011-09-30 00:25:34 UTC+0000
0x816711c8	1076	123	17	UDP	127.0.0.1	2011-09-30 00:26:30 UTC+0000
0x816757d0	692	0	255	Reserved	0.0.0.0	2011-09-26 01:33:47 UTC+0000
0x815bb708	1752	1067	6	TCP	0.0.0.0	2011-09-30 00:25:33 UTC+0000
0x812bb008	1336	1900	17	UDP	127.0.0.1	2011-09-30 00:26:30 UTC+0000
0x81904478	692	4500	17	UDP	0.0.0.0	2011-09-26 01:33:47 UTC+0000
0x814c9008	4	445	17	UDP	0.0.0.0	2011-09-26 01:33:32 UTC+0000

Figure 5: sockets

```
r@r-Octopus:~/Downloads$ volatility malfind -f Windows\ XP\ Professional.vmem
Volatility Foundation Volatility Framework 2.6
Process: csrcss.exe Pid: 612 Address: 0x7f6f0000
Vad Tag: Vad Protection: PAGE_EXECUTE_READWRITE
Flags: Protection: 6

0x7f6f0000 c8 00 00 00 5c 01 00 00 ff ee ff ee 08 70 00 00 .....p..
0x7f6f0010 08 00 00 00 00 fe 00 00 00 10 00 00 20 00 00 .....
0x7f6f0020 00 02 00 00 00 20 00 00 8d 01 00 00 ff ef fd 7f .....
0x7f6f0030 03 00 08 06 00 00 00 00 00 00 00 00 00 00 00 .....

0x7f6f0000 c8000000 ENTER 0x0, 0x0
0x7f6f0004 5c POP ESP
0x7f6f0005 0100 ADD [EAX], EAX
0x7f6f0007 00ff ADD BH, BH
0x7f6f0009 ee OUT DX, AL
0x7f6f000a ff DB 0xff
0x7f6f000b ee OUT DX, AL
0x7f6f000c 087000 OR [EAX+0x0], DH
0x7f6f000f 0008 ADD [EAX], CL
0x7f6f0011 0000 ADD [EAX], AL
0x7f6f0013 0000 ADD [EAX], AL
0x7f6f0015 fe00 INC BYTE [EAX]
0x7f6f0017 0000 ADD [EAX], AL
0x7f6f0019 0010 ADD [EAX], DL
0x7f6f001b 0000 ADD [EAX], AL
0x7f6f001d 2000 AND [EAX], AL
0x7f6f001f 0000 ADD [EAX], AL
0x7f6f0021 0200 ADD AL, [EAX]
0x7f6f0023 0000 ADD [EAX], AL
0x7f6f0025 2000 AND [EAX], AL
0x7f6f0027 008d010000ff ADD [EBP-0xfffff], CL
0x7f6f002d ef OUT DX, EAX
0x7f6f002e fd STD
0x7f6f002f 7f03 JG 0x7f6f0034
0x7f6f0031 0008 ADD [EAX], CL
0x7f6f0033 06 PUSH ES
0x7f6f0034 0000 ADD [EAX], AL
0x7f6f0036 0000 ADD [EAX], AL
0x7f6f0038 0000 ADD [EAX], AL
0x7f6f003a 0000 ADD [EAX], AL
0x7f6f003c 0000 ADD [EAX], AL
0x7f6f003e 0000 ADD [EAX], AL

Process: winlogon.exe Pid: 636 Address: 0x177a0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 4, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x177a0000 cc ac 00 00 0c 00 00 00 00 00 00 00 00 00 00 .....
0x177a0010 53 00 00 00 00 00 00 00 00 00 00 00 00 00 00 S.....
0x177a0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x177a0030 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa .....
```

Figure 6: nombre

```
r@r-Octopus:~/Downloads$ volatility -n |grep procdump
Volatility Foundation Volatility Framework 2.6
procdump Dump a process to an executable file sample
r@r-Octopus:~/Downloads$
```

Figure 7: manual of the procdump flag