

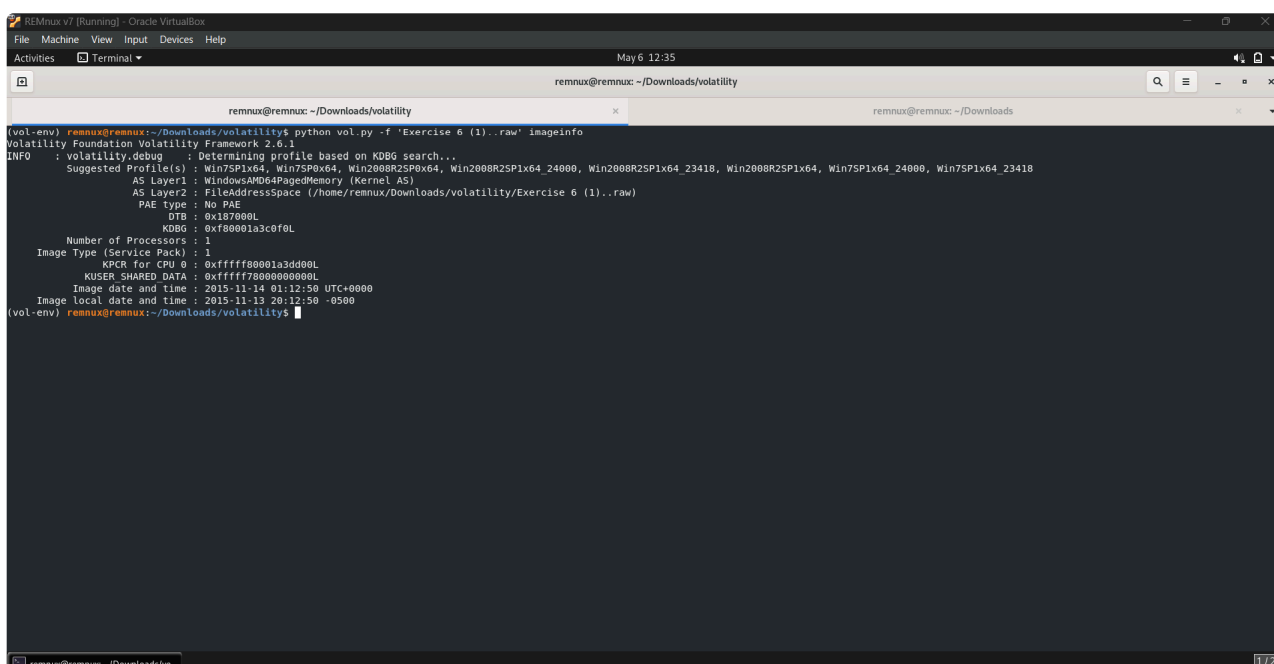
Digital Forensics Lab - Task #7

Memory Image Forensics

1. What is the first suggested profile to use on this memory image?

The suggested profile can be extracted through the following command:

```
python vol.py -f 'Exercise 6 (1)..raw' imageinfo
```



```
(vol-env) remnux@remnux:~/Downloads/volatility$ python vol.py -f 'Exercise 6 (1)..raw' imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO : volatility.debug : Determining profile based on KDBG search...
Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_24000, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_24000, Win7SP1x64_23418
AS Layer1 : WindowsAMD64PagedMemory (kernel AS)
AS Layer2 : FileAddressSpace (/home/remnux/Downloads/volatility/Exercise 6 (1)..raw)
PAE type : No PAE
DTB : 0x187000L
KDBG : 0xf80001a3c0f0L
Number of Processors : 1
Image Type (Service Pack) : 1
KPCR for CPU 0 : 0xfffff80001a3dd00L
KUSER_SHARED_DATA : 0xfffff78000000000L
Image date and time : 2015-11-14 01:12:50 UTC+0000
Image local date and time : 2015-11-13 20:12:50 -0500
(vol-env) remnux@remnux:~/Downloads/volatility$
```

As seen from the screenshot, the first suggested profile is `Win7SP1x64`. The first suggested profile is mostly the profile that is used later on in the analysis.

2. What folder was copied and contained within the system's clipboard?

To check the folder/file that was copied on the clipboard, the command used is given as follows:

```
python vol.py -f 'Exercise 6 (1)..raw' --profile=Win7SP1x64 clipboard
```

```
REMnux v7 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities Terminal May 6 12:18
remnux@remnux: ~/Downloads/volatility
remnux@remnux: ~/Downloads
vol-env) remnux@remnux:~/Downloads/volatility$ "C
(vol-env) remnux@remnux:~/Downloads/volatility$ python vol.py -f 'Exercise 6 (1)..raw' --profile=Win7SP1x64 clipboard
Volatility Foundation Volatility Framework 2.6.1
Session WindowStation Format Handle Object Data
-----
1 WinSta0 0xc009L 0x1b0091 0xfffff900c270c260
1 WinSta0 CF TEXT 0x7400000001 0xfffff900c2602cc0
1 WinSta0 0xc078L 0xa02ef 0xfffff900c2602cc0
1 WinSta0 CF TEXT 0x1 0xfffff900c00ec9f0
1 WinSta0 0xc199L 0x2002f 0xfffff900c00ec9f0
1 WinSta0 CF TEXT 0x1 0xfffff900c00eb260
1 WinSta0 0xc1aaL 0x150303 0xfffff900c00eb260
1 WinSta0 CF TEXT 0xfffff9000000001 0xfffff900c00eb190
1 WinSta0 CF HDR0P 0x1302d7 0xfffff900c00eb190
1 WinSta0 CF TEXT 0xfe0000000 0xfffff900c26f2370
1 WinSta0 0xc0dbL 0x3101c3 0xfffff900c26f2370
1 WinSta0 CF TEXT 0x2000000001 0xfffff900c1e1a300
1 WinSta0 0xc006L 0x250277 0xfffff900c1e1a300
1 WinSta0 CF TEXT 0x1 0xfffff900c01cb260
1 0x1402e9 0xfffff900c01cb260
1 0x7032d 0xfffff900c26f0370
1 0x13032b 0xfffff900c01fe30
1 0xc0315 0xfffff900c1cce010
1 0x1e02d5 0xfffff900c26cc770
1 0x00313 0xfffff900c06af010
1 0xa02ff 0xfffff900c06af010
(vol-env) remnux@remnux:~/Downloads/volatility$
```

3. What directories were explored from the command prompt?

Following command can be used to check which directories were explored from the command prompt:

```
python vol.py -f 'Exercise 6 (1)..raw' --profile=Win7SP1x64 consoles
```

```
REMnux v7 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities Terminal May 6 12:20
remnux@remnux: ~/Downloads/volatility
remnux@remnux: ~/Downloads/volatility
remnux@remnux: ~/Downloads
vol -emu remnux@remnux:~/Downloads/volatility$ python vol.py -f 'Exercise 6 (1)..raw' --profile=Win7SP1x64 consoles
Volatility Foundation Volatility Framework 2.6.1
*****
ConsoleProcess: conhost.exe Pid: 2852
Console: 0xffff6a200 CommandHistorySize: 50
HistoryBufferCount: 1 HistoryBufferMax: 4
OriginalTitle: %SystemRoot%\system32\cmd.exe
Title: Administrator: C:\Windows\system32\cmd.exe
AttachedProcess: cmd.exe Pid: 1544 Handle: 0x60
-----
CommandHistory: 0x214820 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 5 LastAdded: 4 LastDisplayed: 4
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x60
-----
Cmd #0 at 0x213350: e:
Cmd #1 at 0x206a00: cd secret
Cmd #2 at 0x206a20: cd fraud
Cmd #3 at 0x1cb5a0: cd smoking_gun_evidence
Cmd #4 at 0x213190: dir
-----
Screen 0x1f1440 X:00 Y:300
Dump:
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\djprice>e:

E:\>cd secret

E:\secret>cd fraud

E:\secret\fraud>cd smoking_gun_evidence

E:\secret\fraud\smoking_gun_evidence>dir
Volume in drive E is In class
Volume Serial Number is 14A6-AE72

Directory of E:\secret\fraud\smoking_gun_evidence

11/13/15 08:10 PM <DIR> .
11/13/15 08:10 PM <DIR> ..
11/13/15 07:49 PM 58 evidence.txt
11/13/15 08:10 PM 0 New Text Document.txt

2 File(s) 58 bytes
2 Dir(s) 15,991,169,024 bytes free

remnux@remnux: ~/Downloads/volatility
```

```
REMnux v7 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities Terminal May 6 12:21
remnux@remnux: ~/Downloads/volatility
remnux@remnux: ~/Downloads/volatility
remnux@remnux: ~/Downloads
11/13/15 08:10 PM 0 New Text Document.txt
2 File(s) 58 bytes
2 Dir(s) 15,991,169,024 bytes free

E:\secret\fraud\smoking_gun_evidence>
*****
ConsoleProcess: conhost.exe Pid: 1908
Console: 0xffff6a200 CommandHistorySize: 50
HistoryBufferCount: 2 HistoryBufferMax: 4
OriginalTitle: %SystemRoot%\system32\cmd.exe
Title: Administrator: C:\Windows\system32\cmd.exe - winpmem.exe inclass.raw
AttachedProcess: winpmem.exe Pid: 860 Handle: 0x8c
AttachedProcess: cmd.exe Pid: 2280 Handle: 0x60
-----
CommandHistory: 0x1f4b70 Application: winpmem.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x8c
-----
CommandHistory: 0x1f4820 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 2 LastAdded: 1 LastDisplayed: 1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x60
-----
Cmd #0 at 0x1e6a10: cd..
Cmd #1 at 0x1cb5b0: winpmem.exe inclass.raw
-----
Screen 0x1d1450 X:00 Y:300
Dump:
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\djprice>cd..

C:\Users>cd..

C:\>winpmem.exe inclass.raw
Extracting driver to C:\Users\djprice\AppData\Local\Temp\pme740.tmp
Driver Unloaded.
Loaded Driver C:\Users\djprice\AppData\Local\Temp\pme740.tmp.
Deleting C:\Users\djprice\AppData\Local\Temp\pme740.tmp
Will generate a RAW image
CR3: 0x0000137000
2 memory ranges:
Start 0x00001000 - len0th 0x00000000

remnux@remnux: ~/Downloads/volatility
```

Analysis of the provided memory image using the Volatility Framework revealed command-line activity indicative of user navigation to a sensitive directory and subsequent listing of its contents. One console session was associated with the process `conhost.exe` (PID 2852), which was attached to a `cmd.exe` process (PID 1544). The recovered command history shows the user executing the following commands: `e:`, `cd secret`, `cd fraud`, `cd smoking_gun_evidence`, and `dir`. These commands indicate deliberate navigation to a deeply nested folder structure, culminating in a directory listing of `E:\secret\fraud\smoking_gun_evidence`.

The screen buffer content confirms the execution of these commands and displays the contents of the directory at the time of acquisition. The folder contained two files: `evidence.txt` (58 bytes) and `New Text Document.txt` (0 bytes). The naming of the folder (`smoking_gun_evidence`) and the file (`evidence.txt`) suggests the potential presence of critical or incriminating data.

A separate console session was also identified, associated with another instance of `conhost.exe` (PID 1908), attached to both `cmd.exe` (PID 2280) and `winpmem.exe` (PID 860). The command history for this

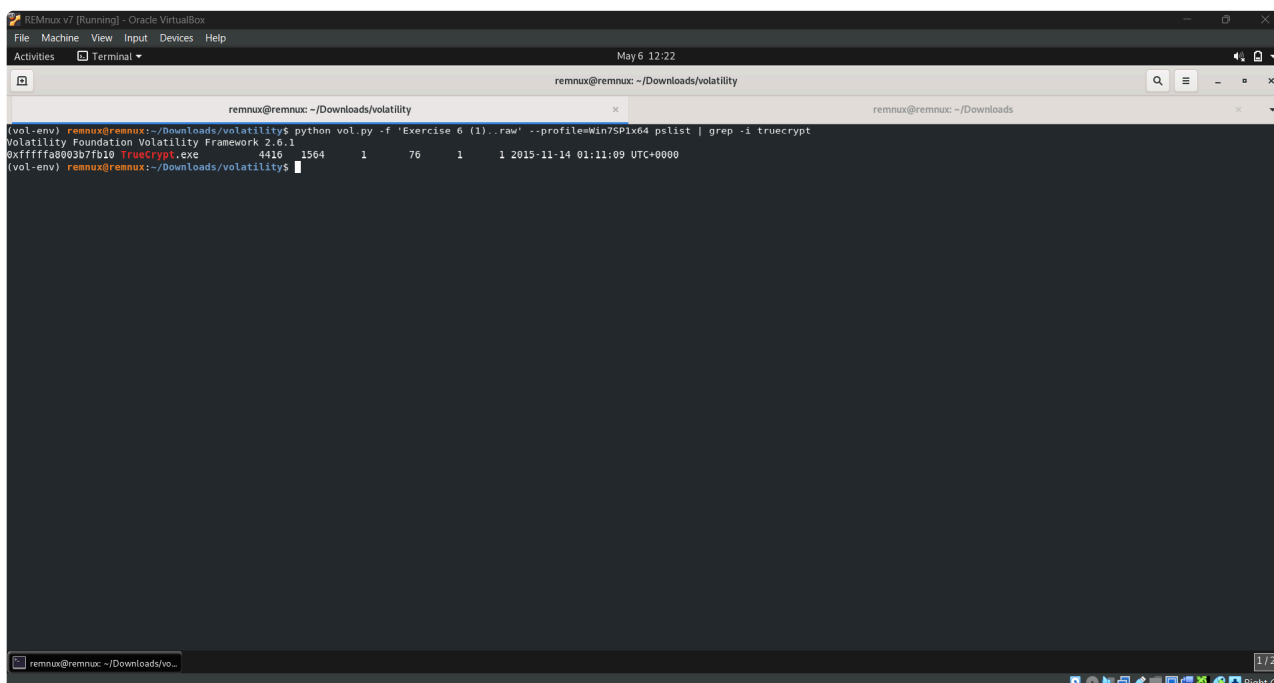
session included `cd..` and `winpmem.exe inclass.raw`, indicating that the user initiated memory acquisition using the WinPMEM tool. The screen buffer further supports this, showing typical WinPMEM output such as driver extraction, memory range detection, and progress indicators for raw memory dump creation.

The sequence of events—accessing a potentially sensitive folder followed by memory acquisition—suggests an attempt to either preserve digital evidence or obscure user activity. It is recommended to conduct further analysis of the memory image, particularly focusing on recovering the contents of `evidence.txt`, to validate the significance of the data located in the referenced directory.

4. Was TrueCrypt running at the time of memory acquisition?

Following command confirms if `TrueCrypt` was running at the time of acquisition:

```
python vol.py -f 'Exercise 6 (1)..raw' --profile=Win7SP1x64 pslist | grep -i truecrypt
```



```
remnux@remnux: ~/Downloads/volatility
(vol-env) remnux@remnux:~/Downloads/volatility$ python vol.py -f 'Exercise 6 (1)..raw' --profile=Win7SP1x64 pslist | grep -i truecrypt
Volatility Foundation Volatility Framework 2.6.1
0xfffffa0000000000 TrueCrypt.exe 4416 1564 1 76 1 1 2015-11-14 01:11:09 UTC+0000
(vol-env) remnux@remnux:~/Downloads/volatility$
```

5. If so, what was the process ID?

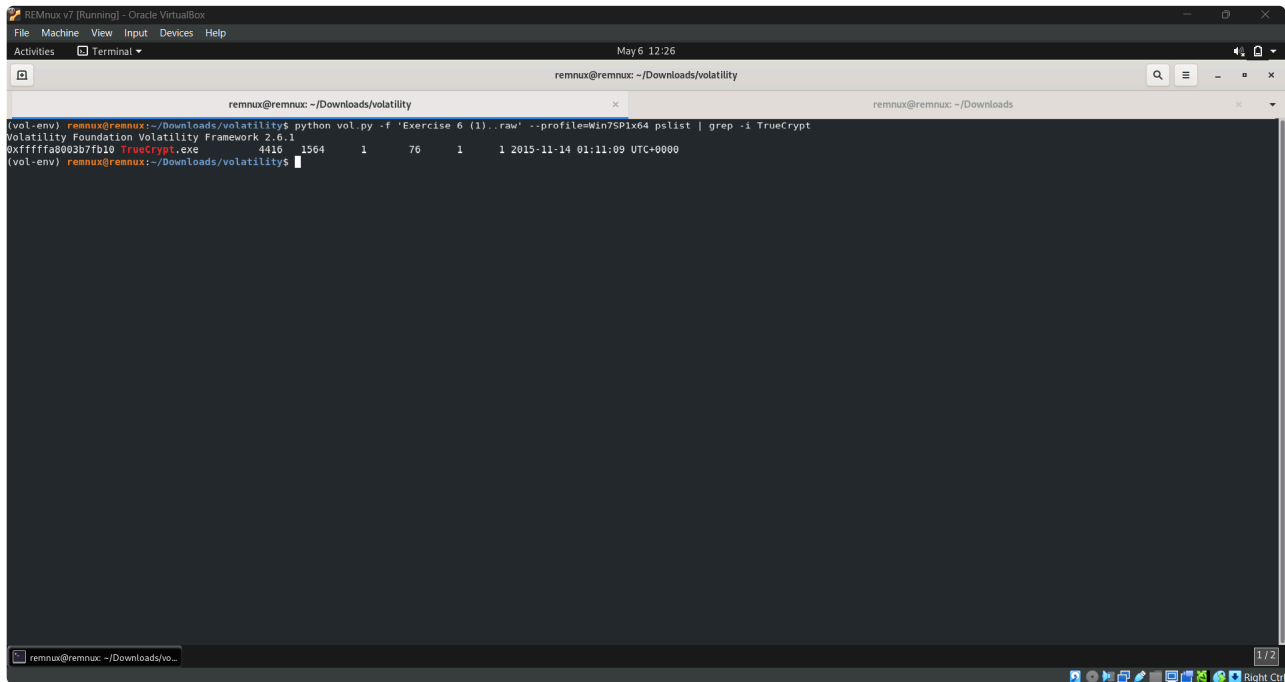
The process ID is `4416`.

6. How many times had TrueCrypt been executed?

Used command is given as:

```
python vol.py -f 'Exercise 6 (1)..raw' --profile=Win7SP1x64 pslist |
grep -i truecrypt
```

As seen from the screenshot, TrueCrypt is shown to be run only once in the complete session. Proof is:

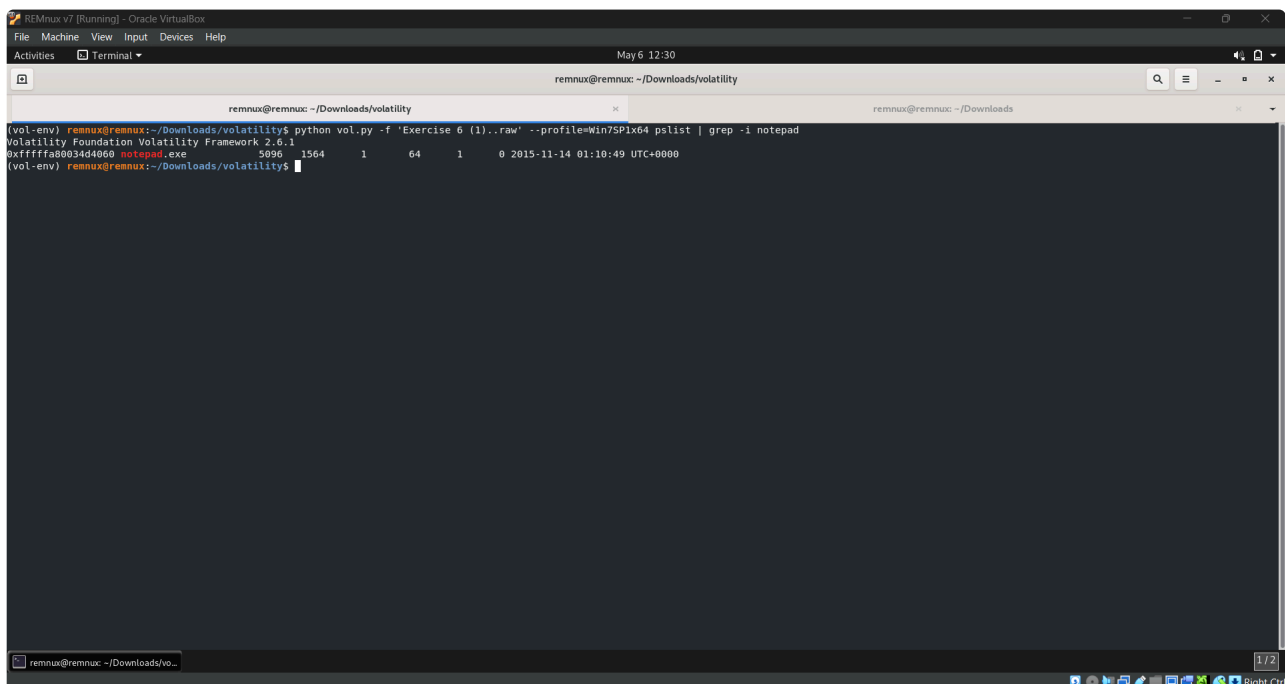


```
remnux@remnux: ~/Downloads/volatility
(vol-env) remnux@remnux:~/Downloads/volatility$ python vol.py -f 'Exercise 6 (1)..raw' --profile=Win7SP1x64 pslist | grep -i TrueCrypt
Volatility Foundation Volatility Framework 2.6.1
0xfffffa80b3b7fb10 TrueCrypt.exe 4416 1564 1 76 1 1 2015-11-14 01:11:09 UTC+0000
(vol-env) remnux@remnux:~/Downloads/volatility$
```

7. What was the parent process associated with notepad.exe?

Command to determine the Parent Process ID with `notepad.exe` is given as follows:

```
python vol.py -f 'Exercise 6 (1)..raw' --
profile=Win7SP1x64 pslist | grep -i notepad
```



```
remnux@remnux: ~/Downloads/volatility
(vol-env) remnux@remnux:~/Downloads/volatility$ python vol.py -f 'Exercise 6 (1)..raw' --profile=Win7SP1x64 pslist | grep -i notepad
Volatility Foundation Volatility Framework 2.6.1
0xfffffa80b3d4d400 notepad.exe 5096 1564 1 64 1 0 2015-11-14 01:10:49 UTC+0000
(vol-env) remnux@remnux:~/Downloads/volatility$
```

From the screenshot, we can see that the Parent Process ID for `notepad.exe` is `1564`.

8. How many DLL files are associated with Notepad.exe?

Following is the command that gives the number of DLL files that are associated with Notepad.exe:

```
python vol.py -f 'Exercise 6 (1)..raw' --profile=Win7SP1x64 dlllist -p <PID> | grep 'Base' | wc -l
```

```
remnux@remnux: ~/Downloads/volatility
(vol-env) remnux@remnux:~/Downloads/volatility$ python vol.py -f 'Exercise 6 (1)..raw' --profile=Win7SP1x64 dlllist -p 1564 | grep 'Base' | wc -l
1
(vol-env) remnux@remnux:~/Downloads/volatility$
```

9. What is the Local IP address and Foreign IP address associated with the first ESTABLISHED chrome.exe connection?

The command that demonstrate the first connection with chrome.exe is given as follows:

```
python vol.py -f 'Exercise 6 (1)..raw' --profile=Win7SP1x64 netscan | grep -i chrome
```

```
remnux@remnux: ~/Downloads/volatility
(vol-env) remnux@remnux:~/Downloads/volatility$ python vol.py -f 'Exercise 6 (1)..raw' --profile=Win7SP1x64 netscan | grep -i chrome
Volatility Foundation Volatility Framework 2.6.1
0x29fd8540 TCPv4 10.211.55.3:49171 74.125.21.94:443 ESTABLISHED 3012 chrome.exe
0x3de4c4f0 TCPv4 10.211.55.3:49197 74.125.21.94:443 CLOSED 3012 chrome.exe
0x3e0d3d70 UDPv4 0.0.0.0:54079 *:~ 3012 chrome.exe
0x3e311cb0 UDPv4 :~ *:~ 3012 chrome.exe
0x3de8ccf0 TCPv4 10.211.55.3:49200 74.125.21.102:443 CLOSED 3012 chrome.exe
0x3de20700 TCPv4 10.211.55.3:49203 64.232.176.113:443 ESTABLISHED 3012 chrome.exe
0x3e138010 TCPv4 10.211.55.3:49199 173.194.208.103:443 CLOSED 3012 chrome.exe
0x3e16f370 TCPv4 10.211.55.3:49172 74.125.21.113:443 CLOSED 3012 chrome.exe
0x3e48dcf0 TCPv4 :~49159 74.125.21.84:443 CLOSED 3012 chrome.exe
0x3e411cf0 TCPv4 10.211.55.3:49160 74.125.21.102:443 CLOSED 3012 chrome.exe
0x3e5a8320 TCPv4 10.211.55.3:49164 74.125.21.190:443 ESTABLISHED 3012 chrome.exe
0x3ef16b20 TCPv4 :~49157 74.125.196.95:443 CLOSED 3012 chrome.exe
0x3efc8a60 TCPv4 10.211.55.3:49176 74.125.21.188:5228 ESTABLISHED 3012 chrome.exe
0x3f0ca60 TCPv4 10.211.55.3:49176 74.125.21.188:5228 ESTABLISHED 3012 chrome.exe
(vol-env) remnux@remnux:~/Downloads/volatility$
```

The local IP address is 10.211.55.3 and the foreign IP address is 74.125.21.94 .