Muhammad Faizan Arshad - 221577

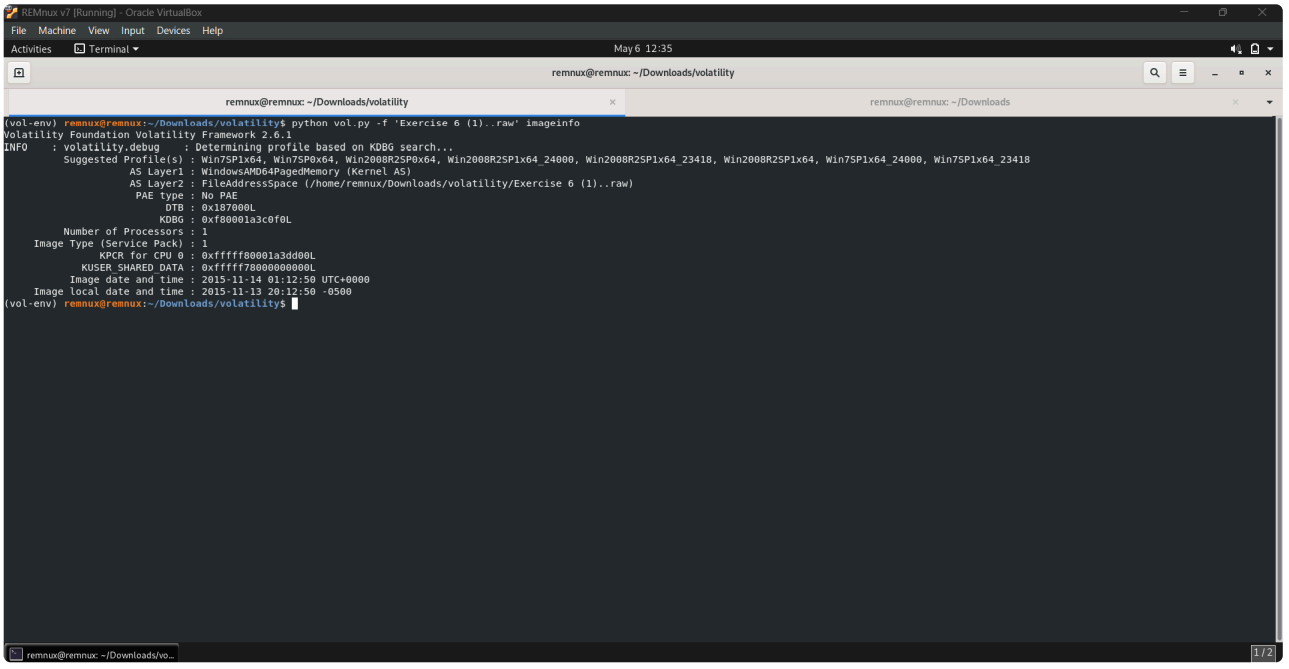
Digital Forensics Lab - Task #7

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
```

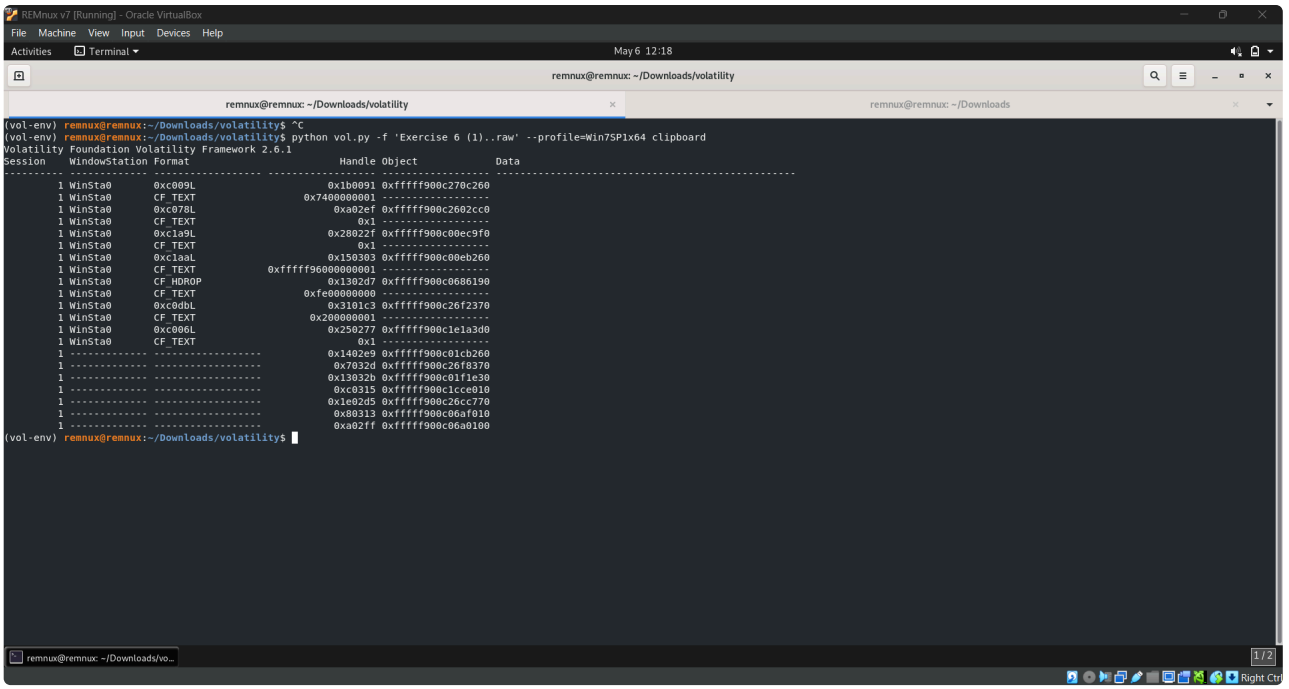


As seen from the screenshot, the first suggested profile is `Win7SP1x64`. The first suggested profile is mostly the profile that is used later on in the analysis.

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
```



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
```

```
(vol-env) 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: 0xff6a6200 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 0x1eb5a0: cd smoking_gun_evidence
Cmd #4 at 0x213190: dir
----
Screen 0x1f1440 X:80 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
```

```
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: 0xff6a6200 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:80 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: 0x0000187000
 2 memory ranges:
Start 0x00001000 - Length 0x0009D000
```

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

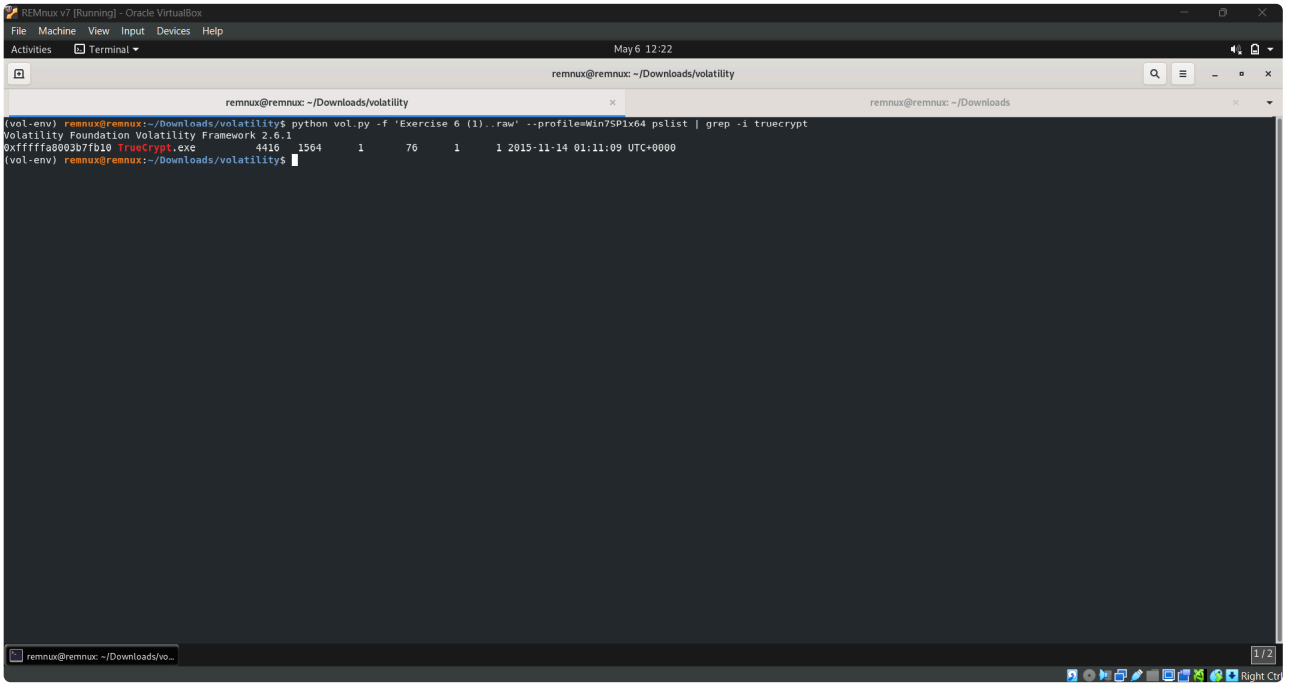
session included `cd..` and `winpmem.exe inclass.raw`, indicating that the user initiated memory acquisition using the WinPMEM tool. The screen buffer further supports this, showing typical WinPMEM output such as driver extraction, memory range detection, and progress indicators for raw memory dump creation.

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
```



5. If so, what was the process ID?

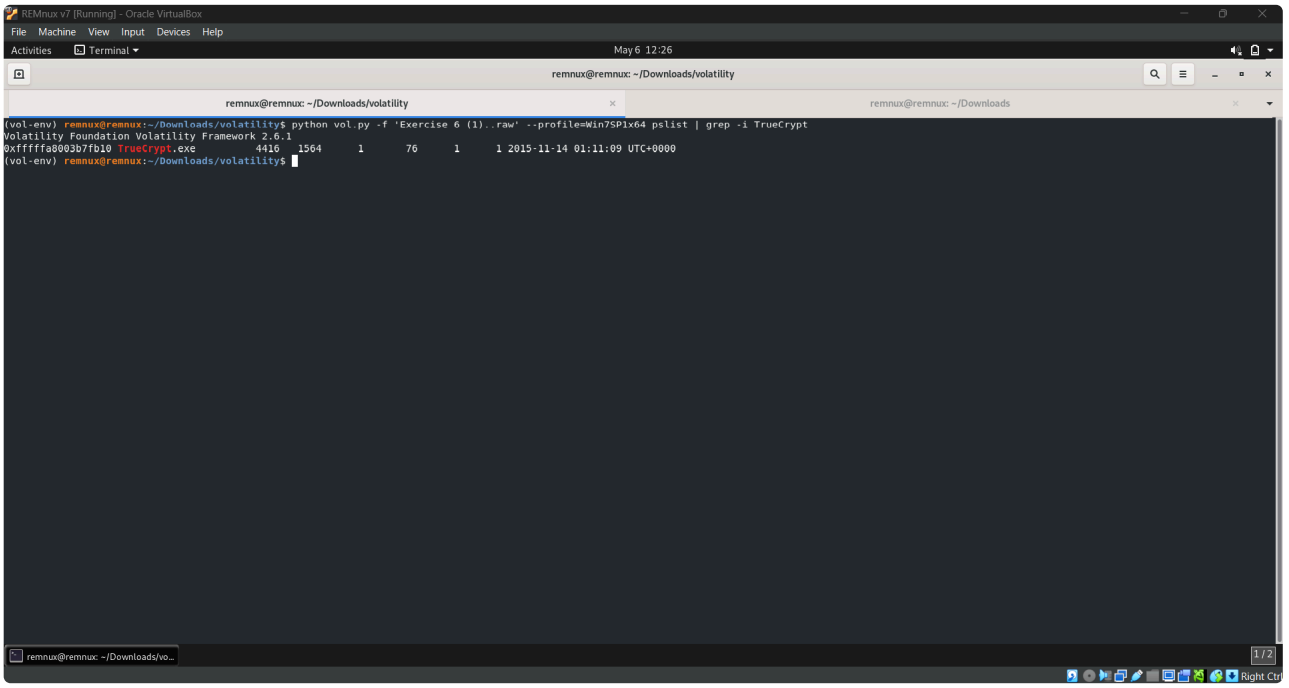
The process ID is `4416`.

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
```

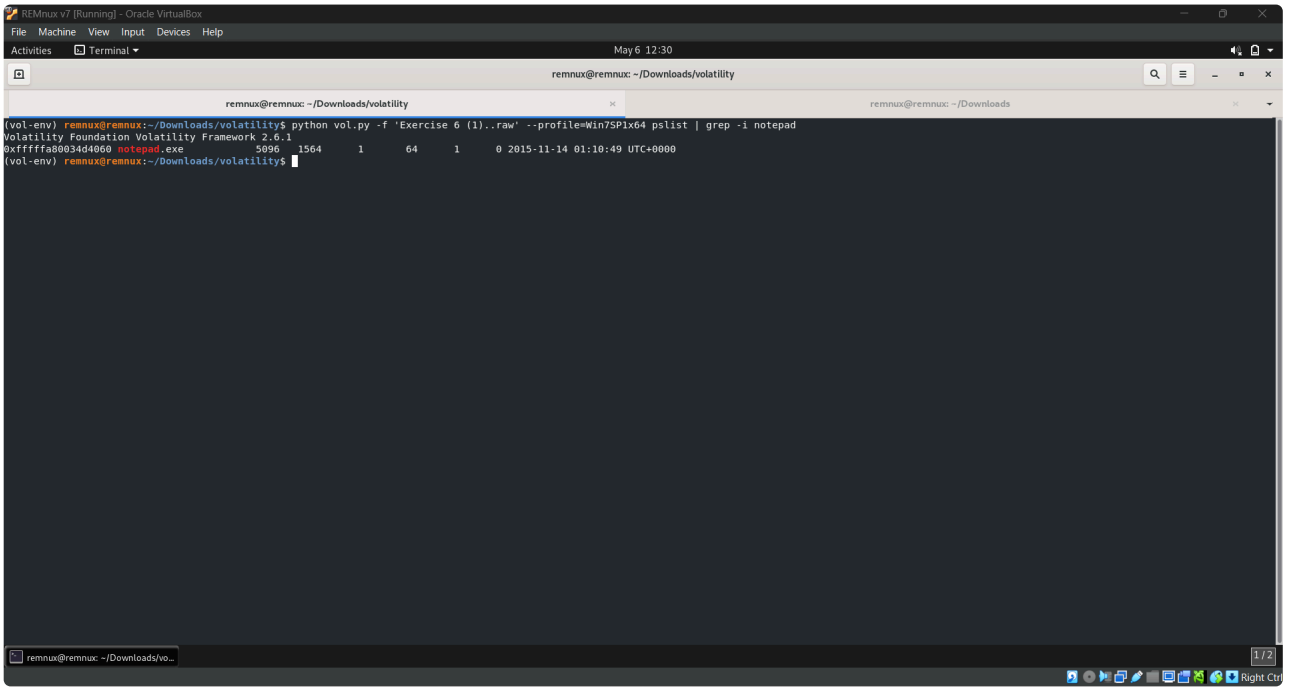
As seen from the screenshot, TrueCrypt is shown to be run only once in the complete session. Proof is:



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
```

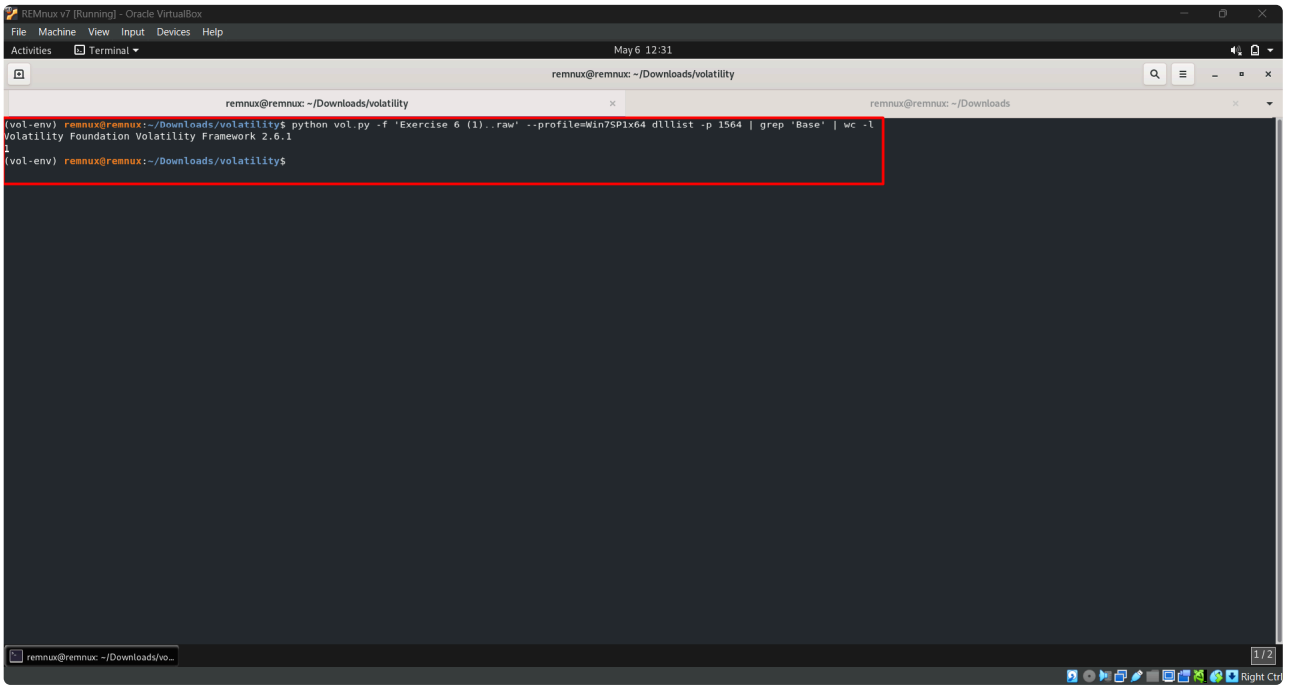


From the screenshot, we can see that the Parent Process ID for `notepad.exe` is `1564`.

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:

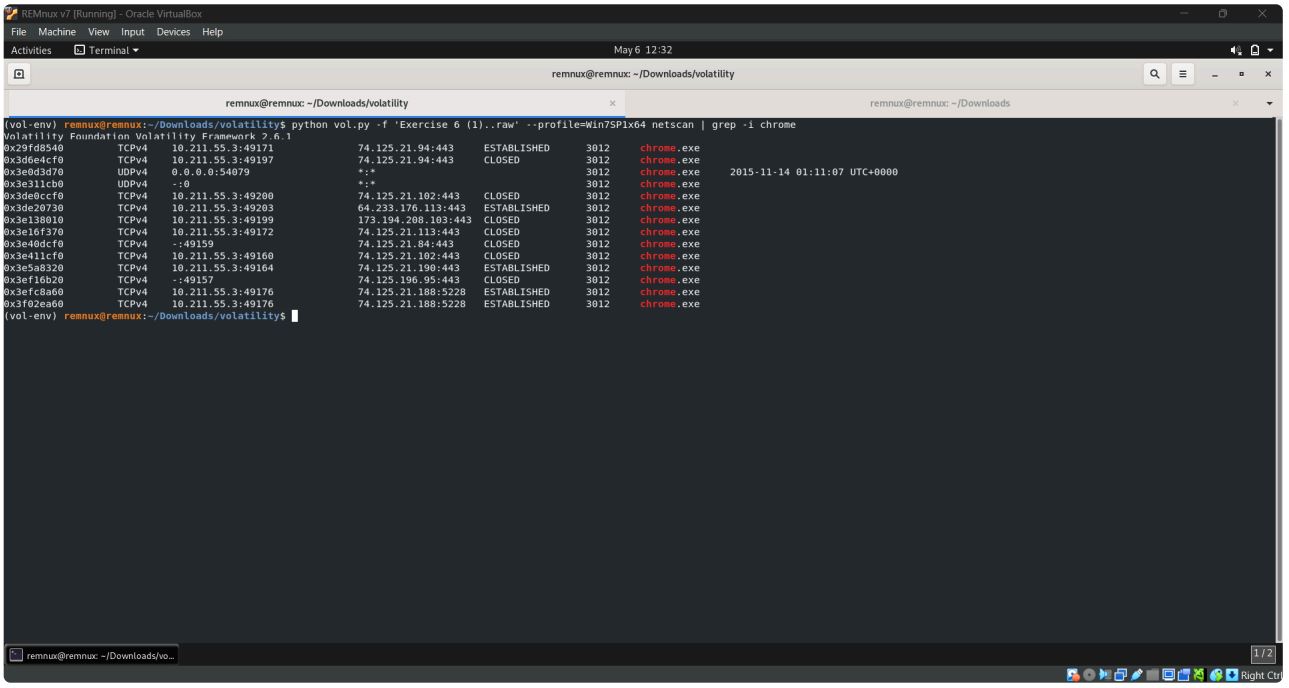
```
python vol.py -f 'Exercise 6 (1)..raw' --profile=Win7SP1x64 dlllist -p <PID> | grep
'Base' | wc -l
```



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
```



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