

# Lab # 8 — Assessment Worksheet

**Course Name and Number: FRS301**

**Student Name: Tran Thanh Tuan**

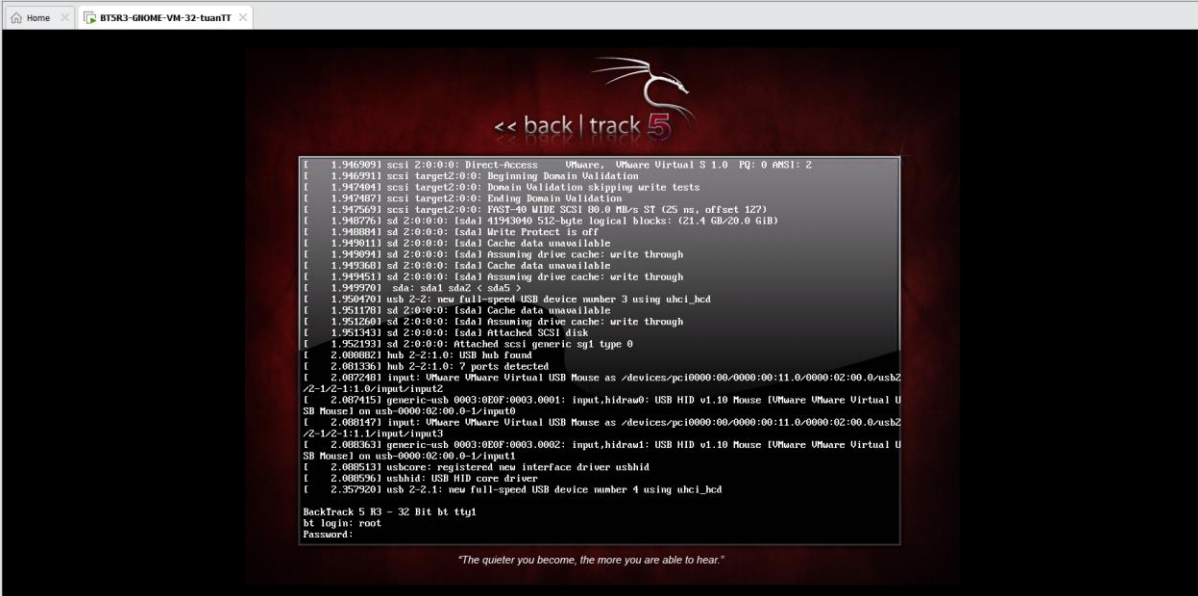
**Student Id: SE161095**

**Instructor Name: Nguyen Van Vinh**

## Analyzing Memory Capture for Windows XP SP2

### *Section 1: Login to BackTrack*

#### 1. Login to BackTrack



The screenshot shows a terminal window titled "BTSR3-GROME-VM-32-tuanTT". The terminal displays the BackTrack 5 logo at the top. Below the logo, a series of system boot logs are visible, including SCSI and USB device initialization messages. The logs indicate that the system has successfully detected and initialized various hardware components, including a USB mouse and a USB keyboard. At the bottom of the terminal, the prompt "BackTrack 5 R3 - 32 Bit bt tty1" is shown, followed by the login prompt "bt login: root" and the password prompt "Password:". The terminal also displays a quote: "The quieter you become, the more you are able to hear."

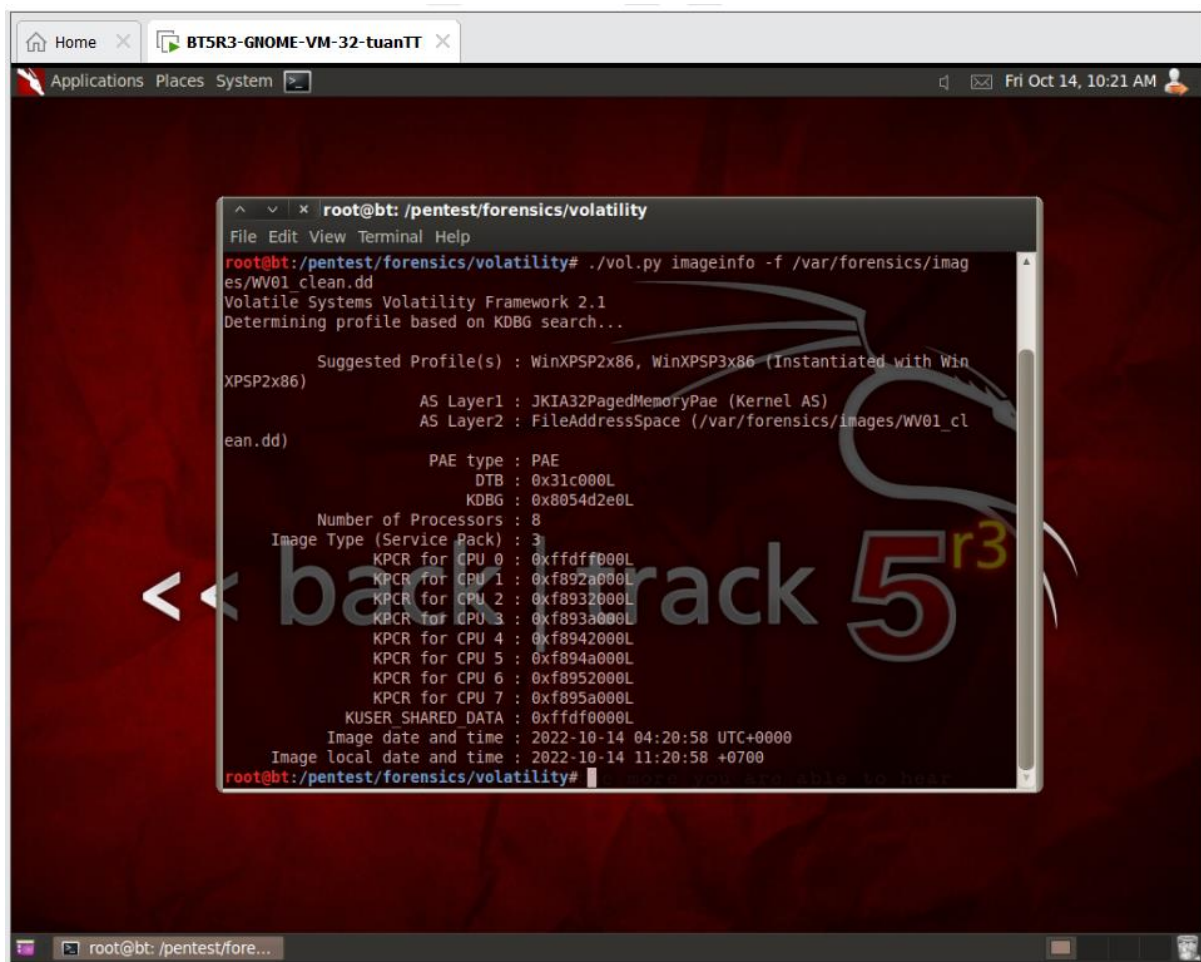
```
[ 1.946509] scsi 2:0:0:0: Direct-access VMware: VMware Virtual S 1.0 PQ: 0 ANSI: 2
[ 1.946591] scsi target2:0:0: Beginning Domain Validation
[ 1.947404] scsi target2:0:0: Domain Validation skipping write tests
[ 1.947407] scsi target2:0:0: Ending Domain Validation
[ 1.947269] scsi target2:0:0: SCSI-40 MIB SCSI 00.0 MB/s ST (25 ns, offset 127)
[ 1.948776] sd 2:0:0:0: [sdal] 41943040 512-byte logical blocks: (21.4 GB/20.0 GiB)
[ 1.948884] sd 2:0:0:0: [sdal] Write Protect is off
[ 1.949411] sd 2:0:0:0: [sdal] Cache data unavailable
[ 1.949894] sd 2:0:0:0: [sdal] Assuming drive cache: write through
[ 1.949360] sd 2:0:0:0: [sdal] Cache data unavailable
[ 1.949451] sd 2:0:0:0: [sdal] Assuming drive cache: write through
[ 1.949970] sda: sda1 sda2 < sda5 >
[ 1.950470] usb 2-2: new full-speed USB device number 3 using uhci_hcd
[ 1.951170] sd 2:0:0:0: [sdal] Cache data unavailable
[ 1.951260] sd 2:0:0:0: [sdal] Assuming drive cache: write through
[ 1.951343] sd 2:0:0:0: [sdal] Attached SCSI disk
[ 1.952193] sd 2:0:0:0: Attached scsi generic sgl type 0
[ 2.008802] hub 2-2:1.0: USB hub found
[ 2.081336] hub 2-2:1.0: 7 ports detected
[ 2.087240] input: VMware VMware Virtual USB Mouse as /devices/pci0000:00/0000:00:11.0/0000:02:00.0/usb2
[ 2-1/2-1:1.0/input/input2
[ 2.087415] generic-usb 0003:0E0F:0003.0001: input,hidraw0: USB HID v1.10 Mouse [VMware VMware Virtual U
SB Mouse] on usb-0000:02:00.0-l/input0
[ 2.088147] input: VMware VMware Virtual USB Mouse as /devices/pci0000:00/0000:00:11.0/0000:02:00.0/usb2
[ 2-1/2-1:1.1/input/input3
[ 2.088363] generic-usb 0003:0E0F:0003.0002: input,hidraw1: USB HID v1.10 Mouse [VMware VMware Virtual U
SB Mouse] on usb-0000:02:00.0-l/input1
[ 2.088513] usbcore: registered new interface driver ushid
[ 2.088596] ushid: USB HID core driver
[ 2.357920] usb 2-2:1: new full-speed USB device number 4 using uhci_hcd

BackTrack 5 R3 - 32 Bit bt tty1
bt login: root
Password:

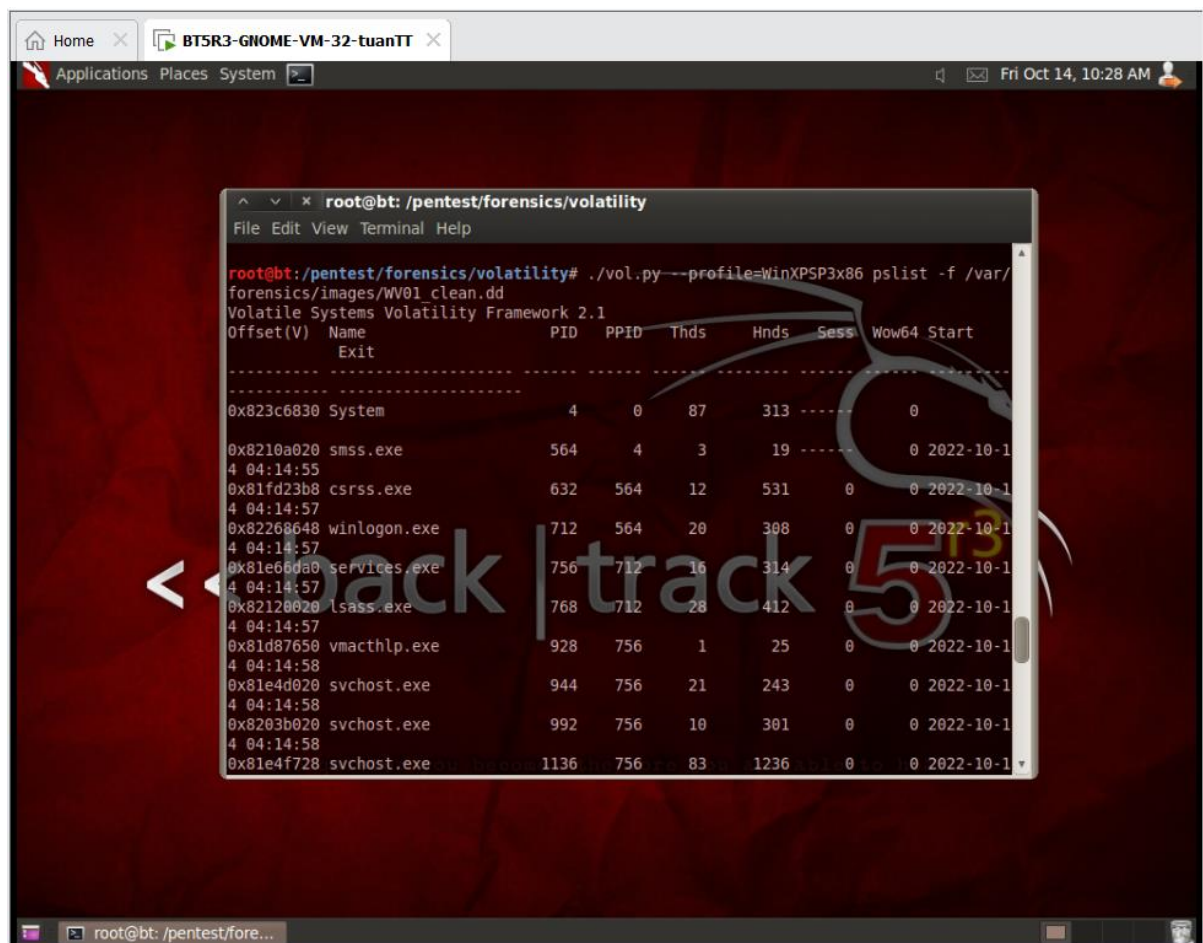
"The quieter you become, the more you are able to hear."
```

#### 2. Bring up the GNOME

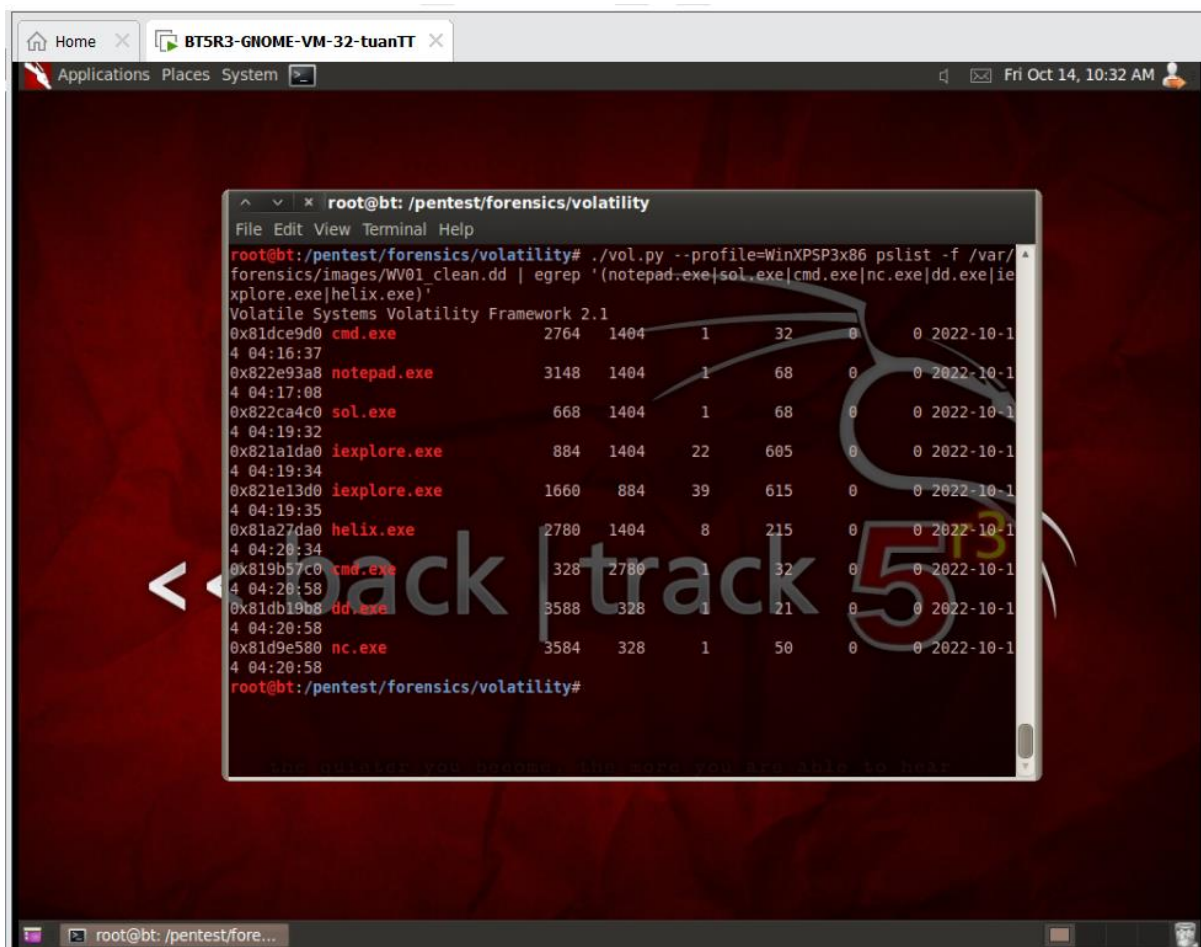




### 3. View Running Processes

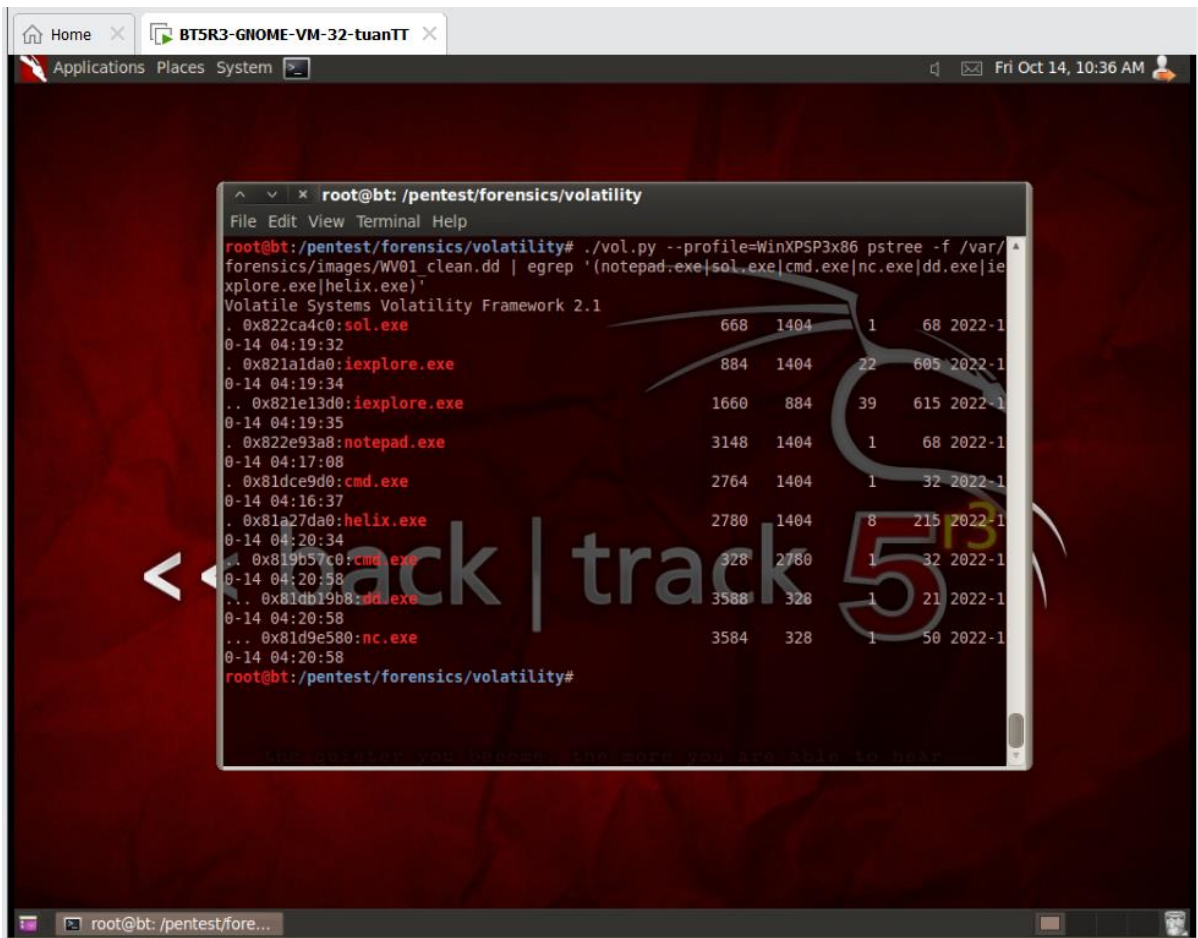


#### 4. Searching for Specific Processes

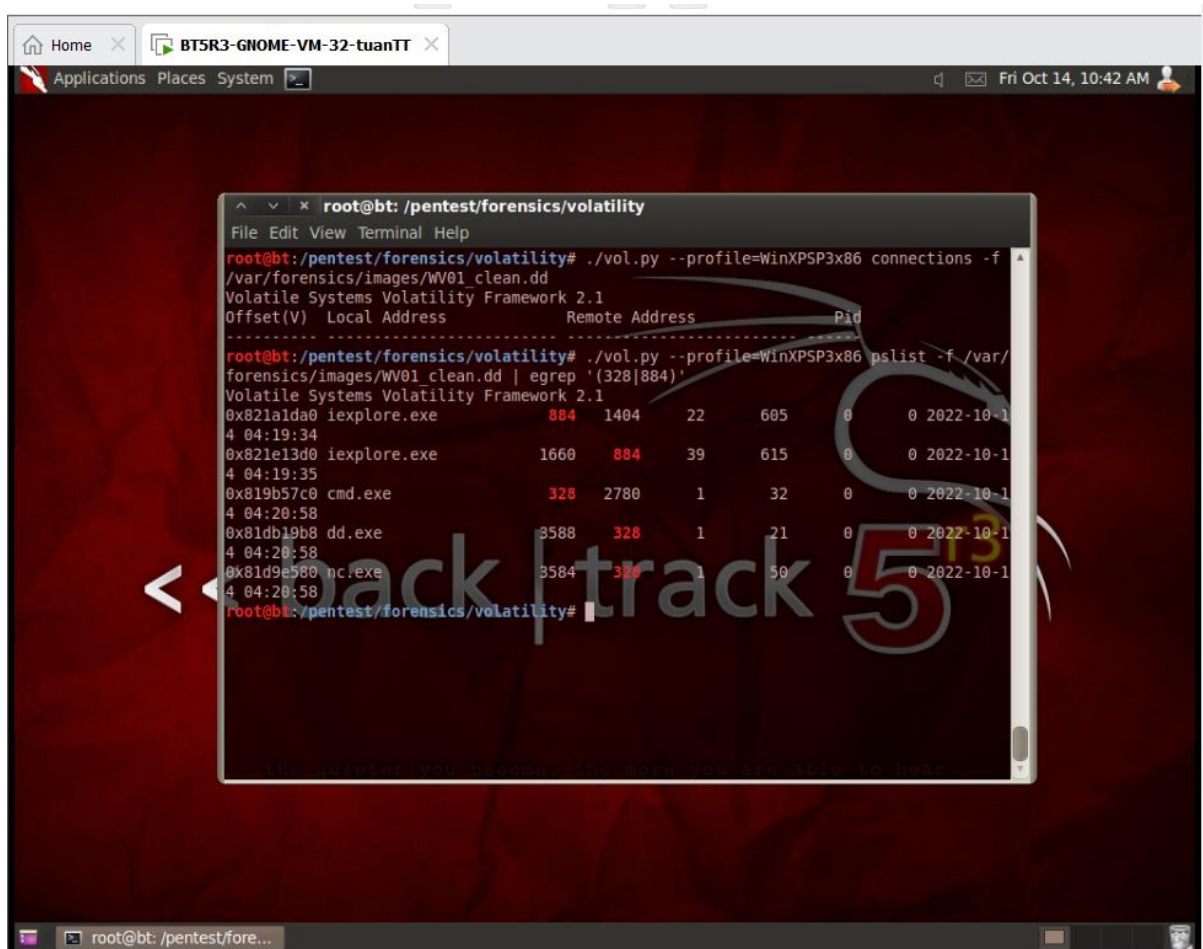


## 5. Associating Parent and Child Processes

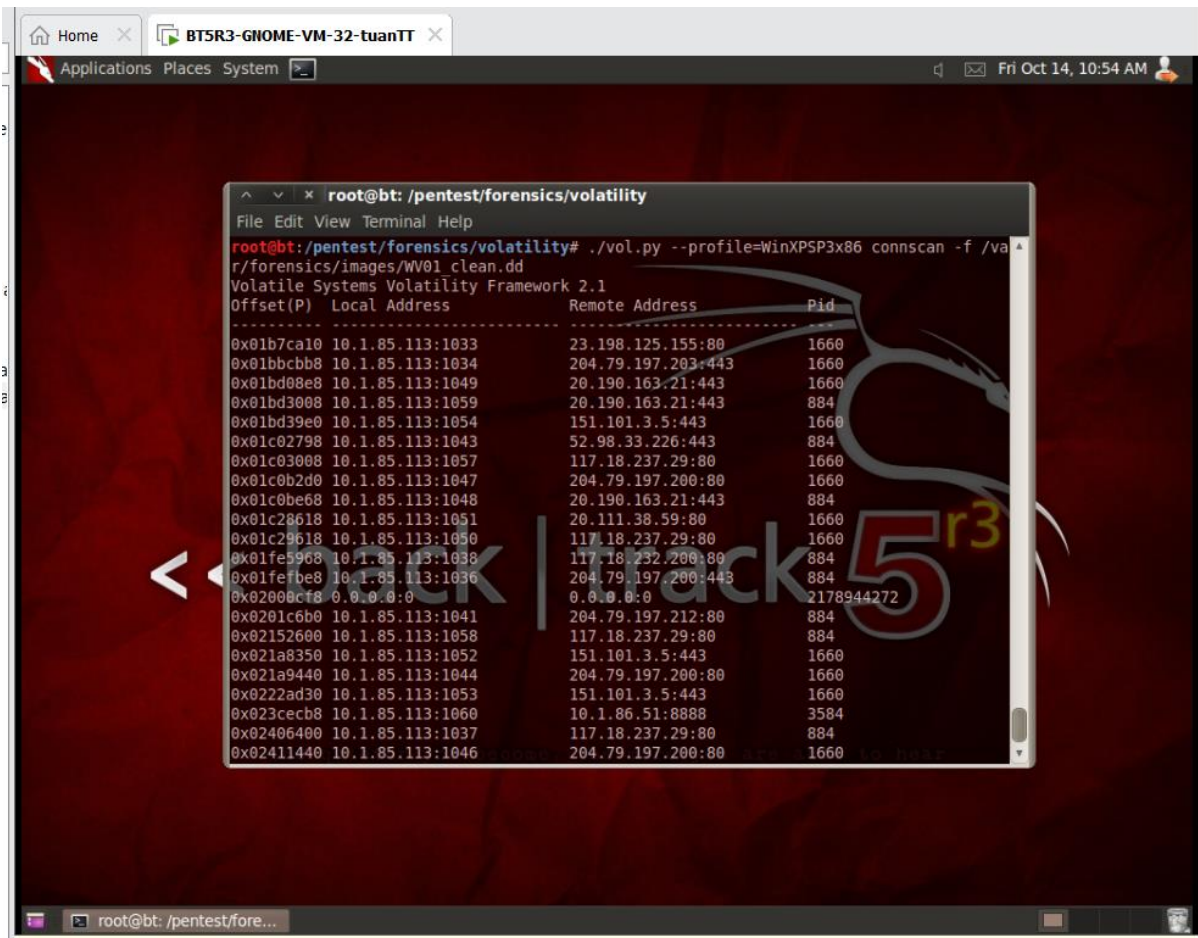




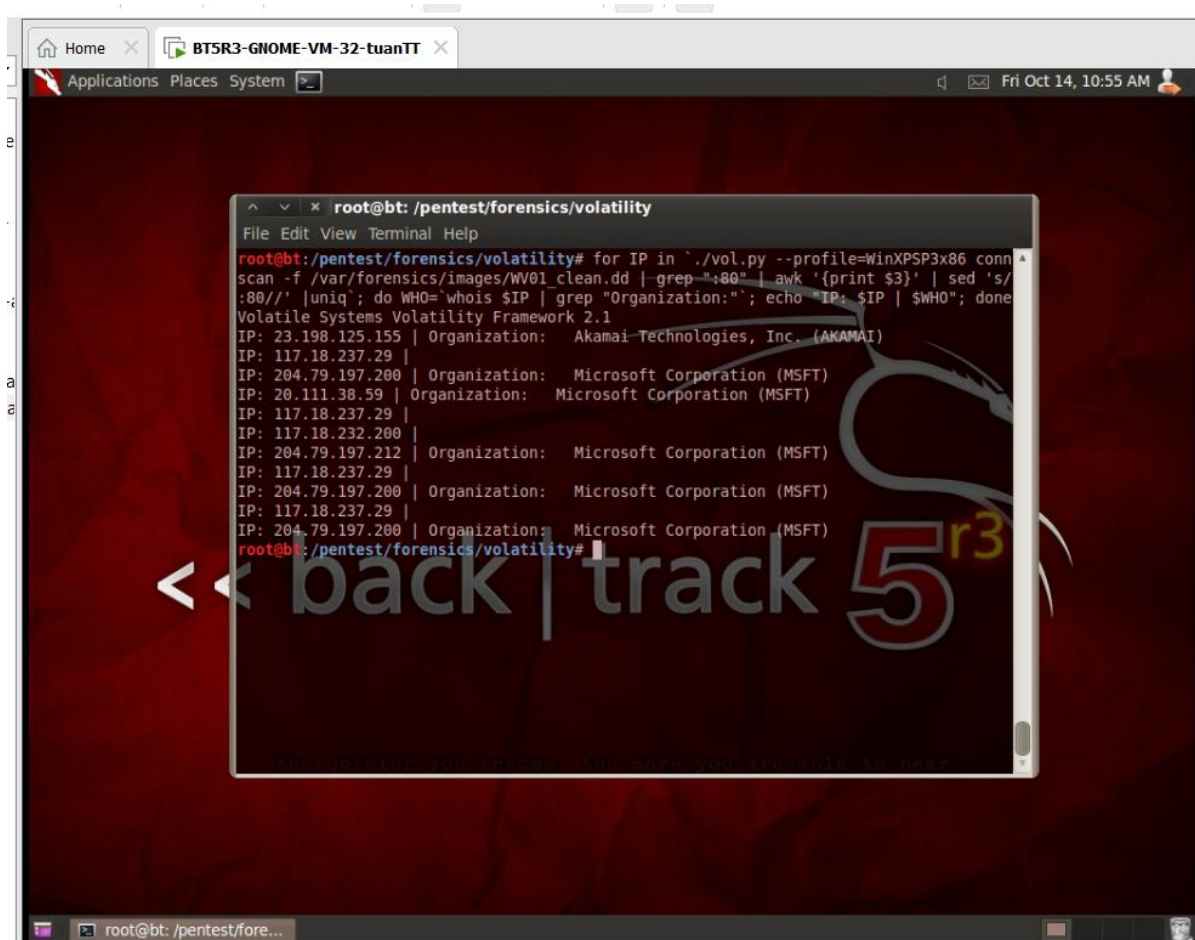
## 6. View Network Connections and Tie to Running Processes



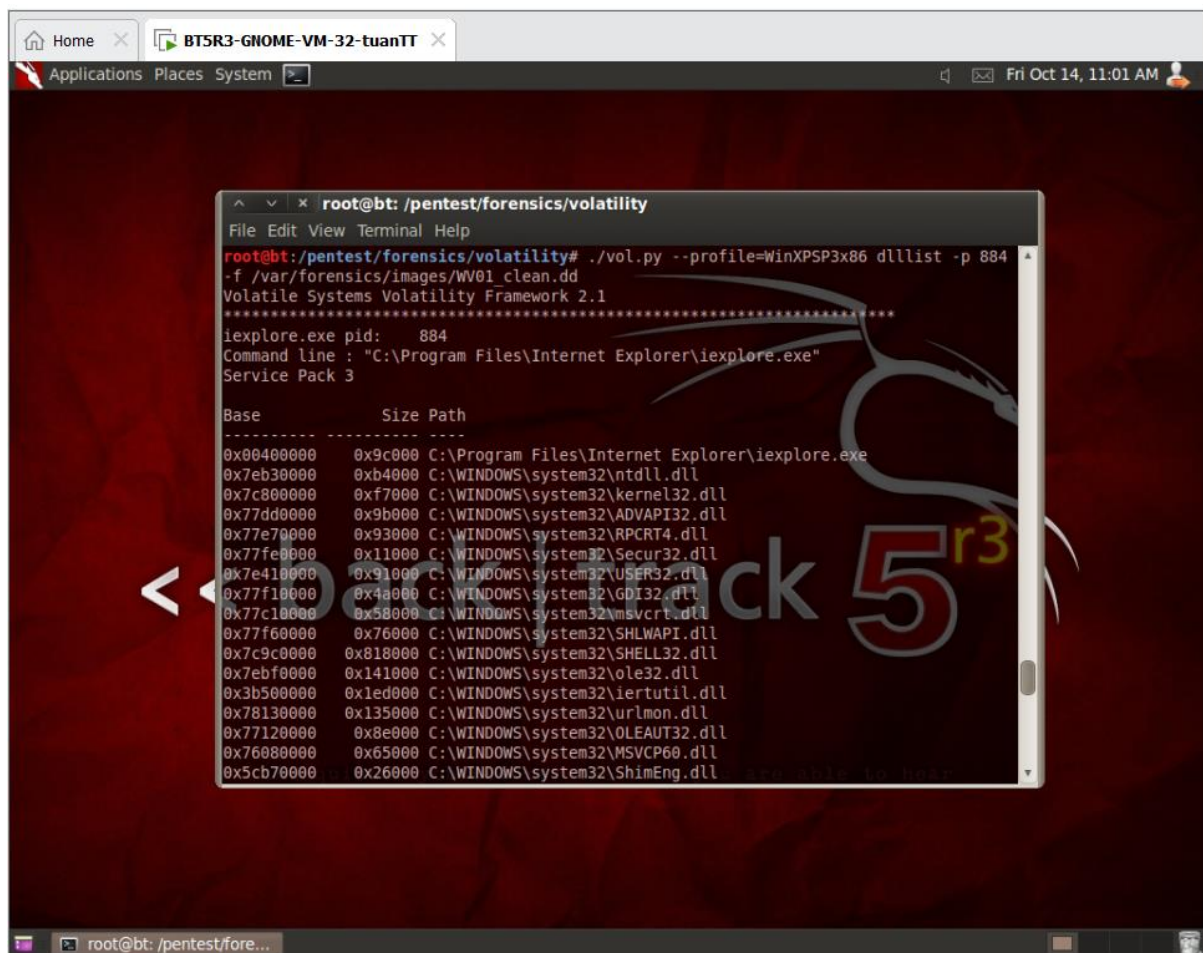
## 7. View and Interrogate Network Connections







## 8. View DLL used by a Running Processes



The screenshot shows a Kali Linux desktop with a terminal window titled "root@bt: /pentest/forensics/volatility". The terminal output shows the command `./vol.py --profile=WinXPSP3x86 dlllist -p 884 -f /var/forensics/images/WV01_clean.dd` and the resulting list of loaded DLLs for `ieexplore.exe` (pid 884).

```
root@bt: /pentest/forensics/volatility# ./vol.py --profile=WinXPSP3x86 dlllist -p 884 -f /var/forensics/images/WV01_clean.dd
Volatile Systems Volatility Framework 2.1
*****
ieexplore.exe pid: 884
Command line : "C:\Program Files\Internet Explorer\ieexplore.exe"
Service Pack 3

Base          Size Path
-----
0x00400000    0x9c000 C:\Program Files\Internet Explorer\ieexplore.exe
0x7eb30000    0xb4000 C:\WINDOWS\system32\ntdll.dll
0x7c800000    0xf7000 C:\WINDOWS\system32\kernel32.dll
0x77dd0000    0x9b000 C:\WINDOWS\system32\ADVAPI32.dll
0x77e70000    0x93000 C:\WINDOWS\system32\RPCRT4.dll
0x77fe0000    0x11000 C:\WINDOWS\system32\Secur32.dll
0x7e410000    0x91000 C:\WINDOWS\system32\USER32.dll
0x77f10000    0x4a000 C:\WINDOWS\system32\GDI32.dll
0x77c10000    0x58000 C:\WINDOWS\system32\Nmsvcrt.dll
0x77f60000    0x76000 C:\WINDOWS\system32\SHLWAPI.dll
0x7c9c0000    0x81800 C:\WINDOWS\system32\SHELL32.dll
0x7ebf0000    0x141000 C:\WINDOWS\system32\ole32.dll
0x3b500000    0x1ed000 C:\WINDOWS\system32\iertutil.dll
0x78130000    0x135000 C:\WINDOWS\system32\urlmon.dll
0x77120000    0x8e000 C:\WINDOWS\system32\OLEAUT32.dll
0x76080000    0x65000 C:\WINDOWS\system32\MSVCP60.dll
0x5cb70000    0x26000 C:\WINDOWS\system32\ShimEng.dll
```

## Section 5: Proof of Lab

