Lab # 10.3 — Assessment Worksheet

Course Name and Number: FRS301

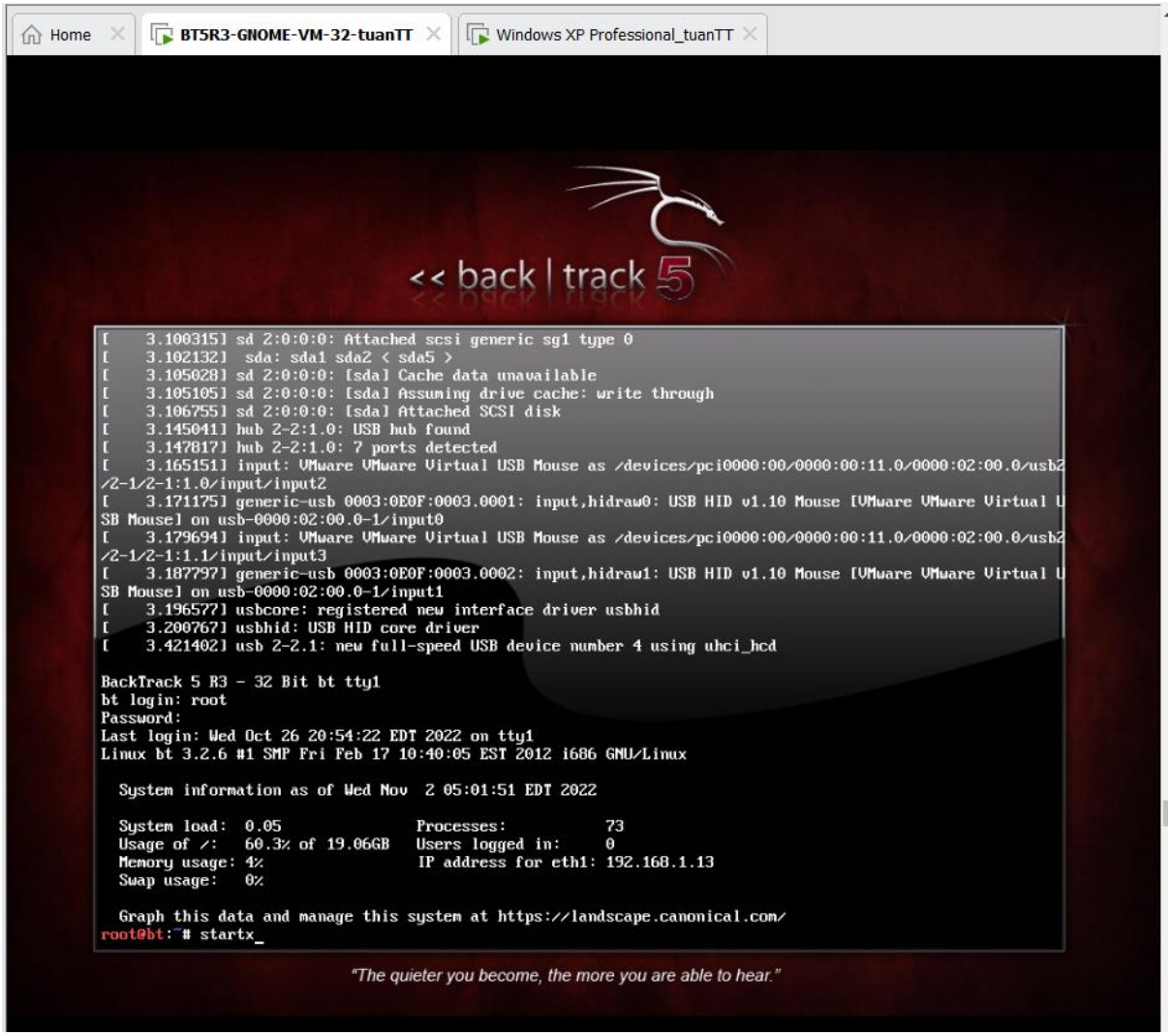
Student Name: Tran Thanh Tuan

Student Id: SE161095

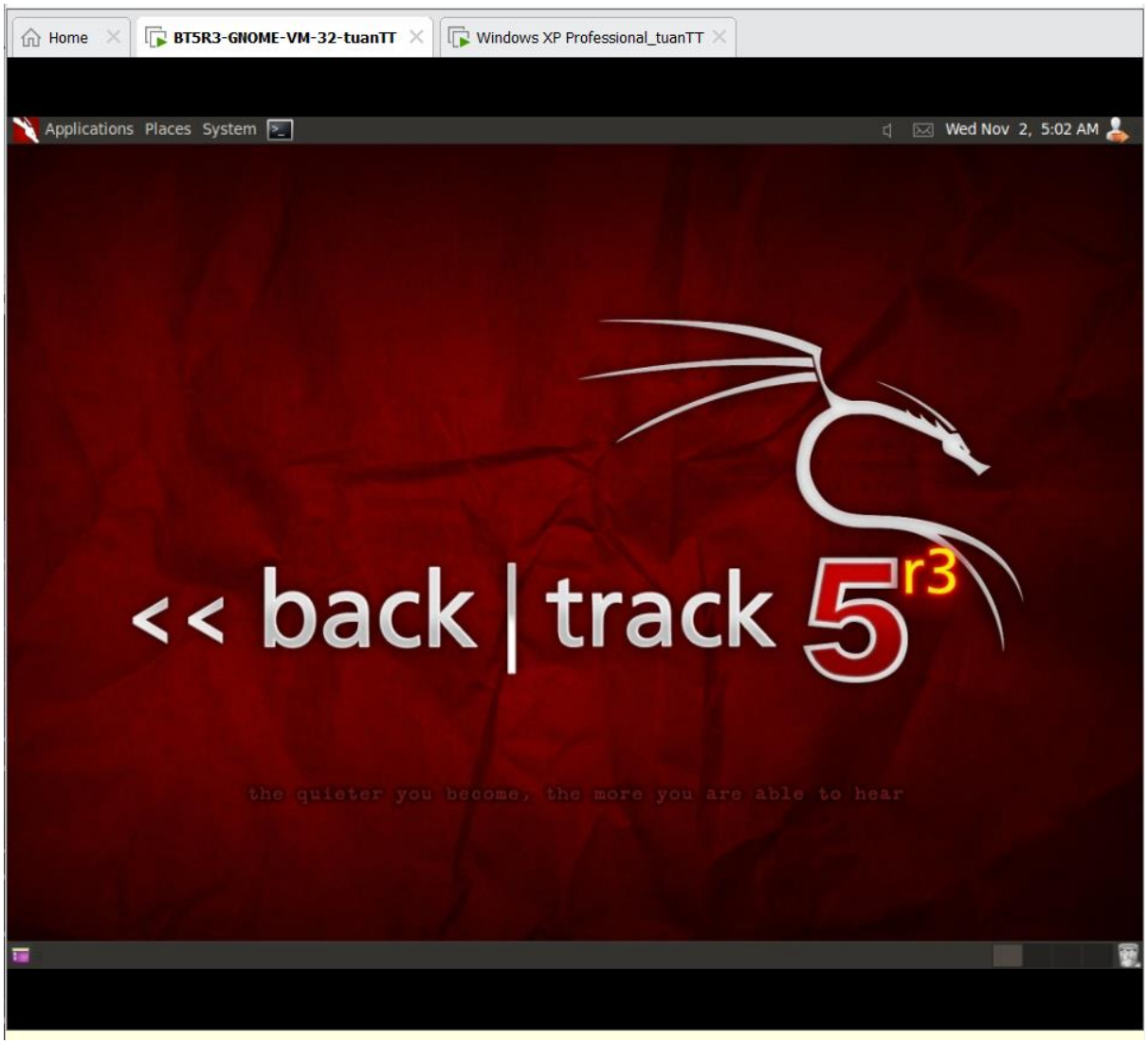
Instructor Name: Nguyen Van Vinh

Analyzing A SET Memory Capture from Windows XP SP2

Section 1. Login to BackTrack

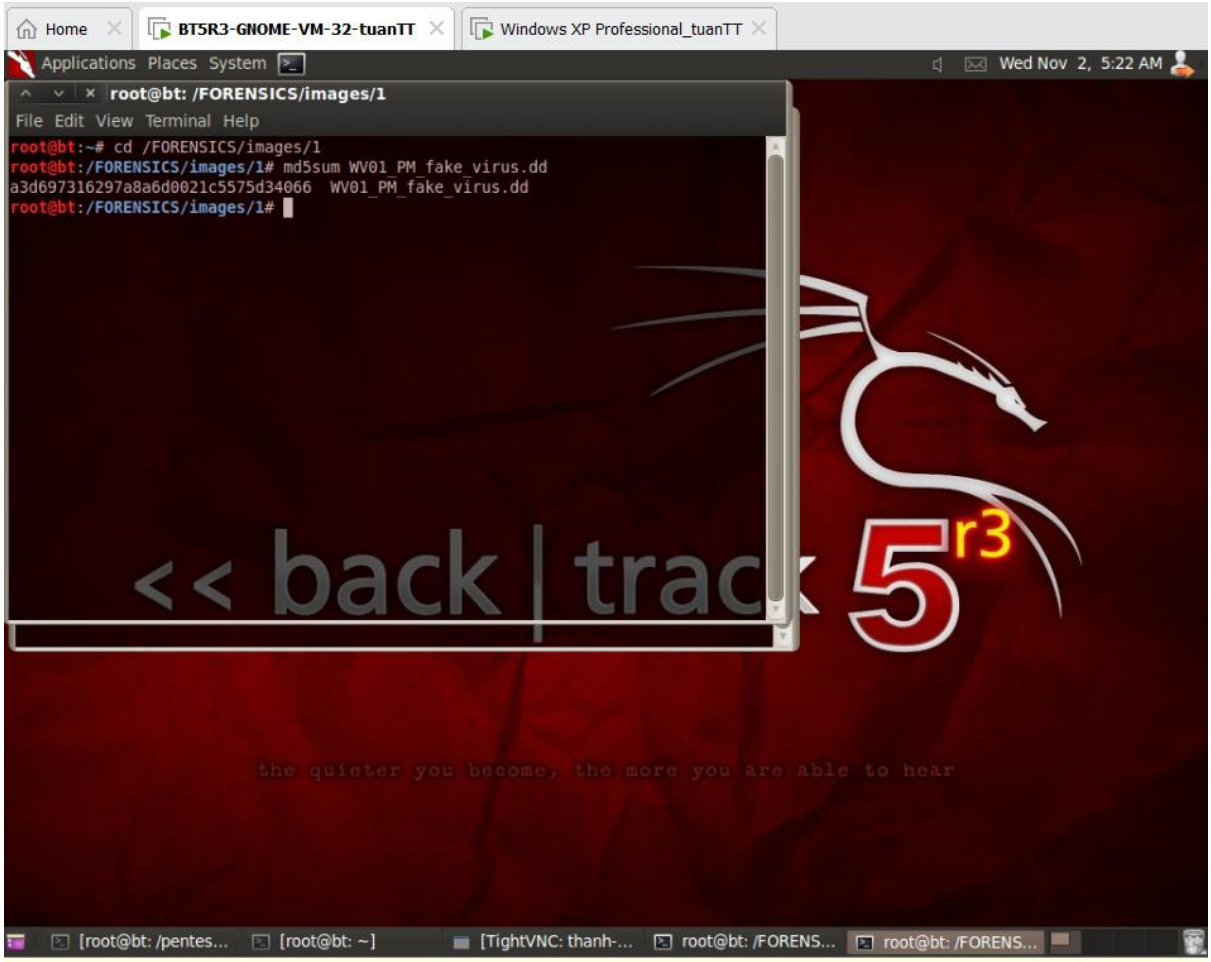


Section 2. Bring up a console terminal

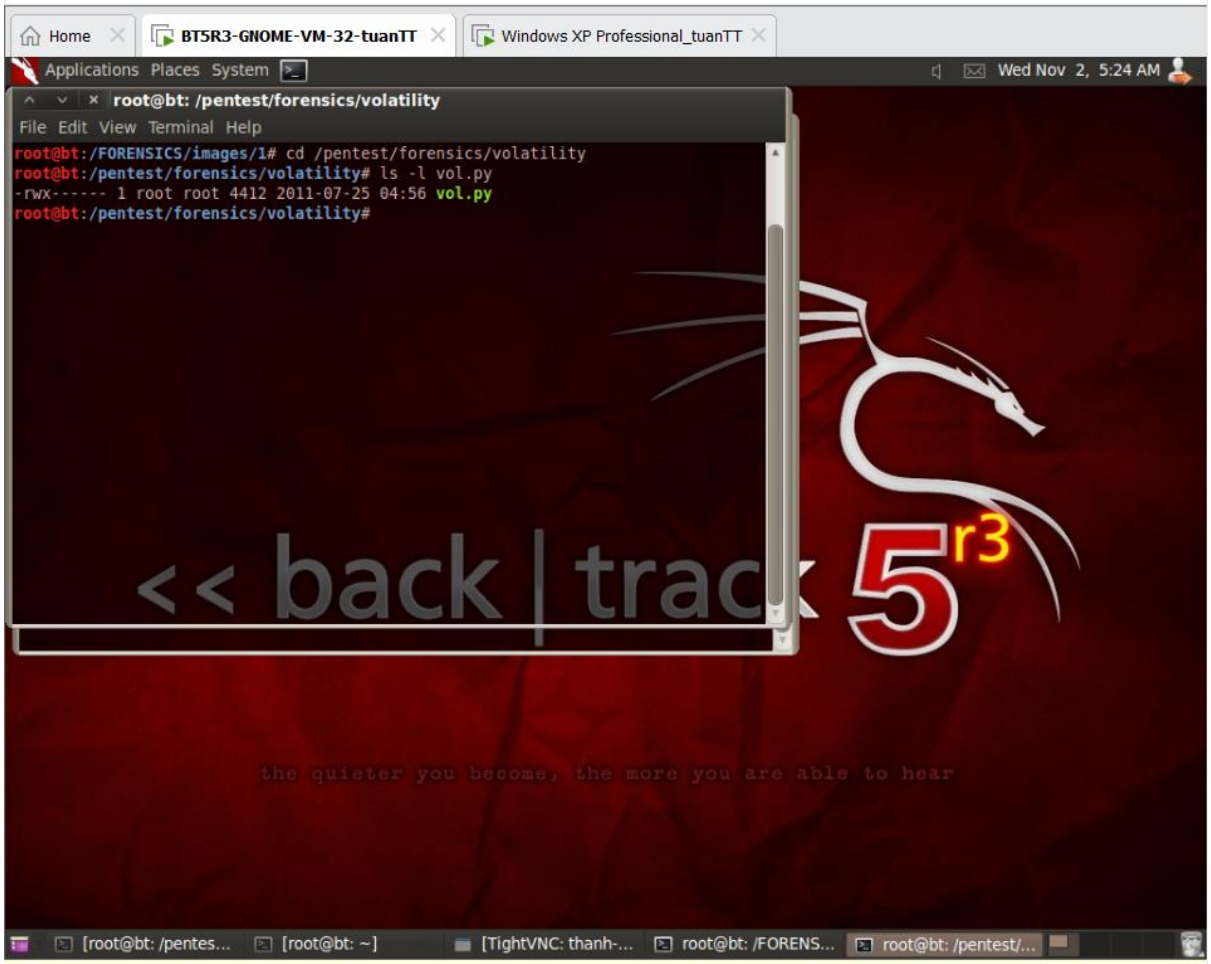


Section 3. Using Volatility

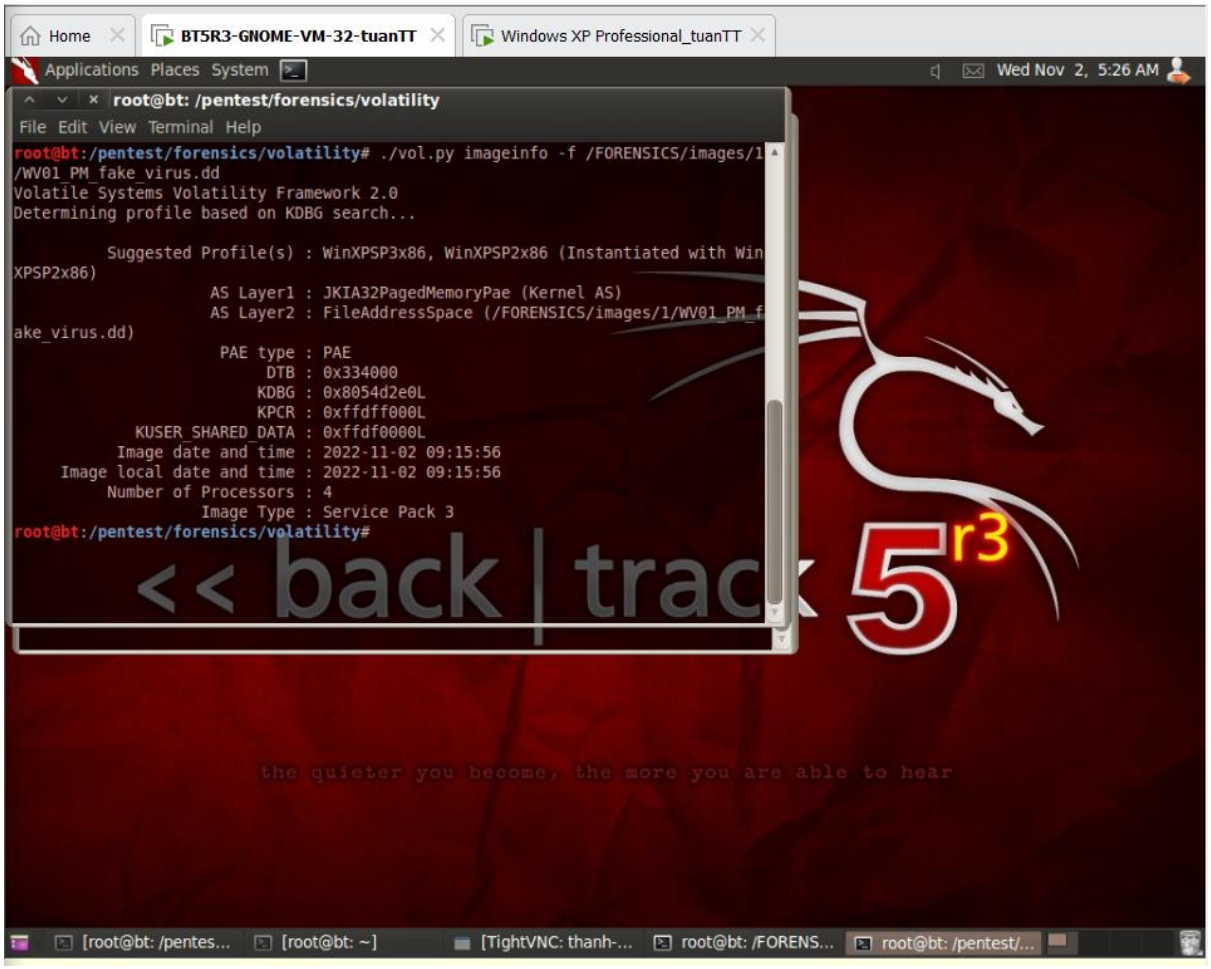
1. **Navigate to Forensic Image**



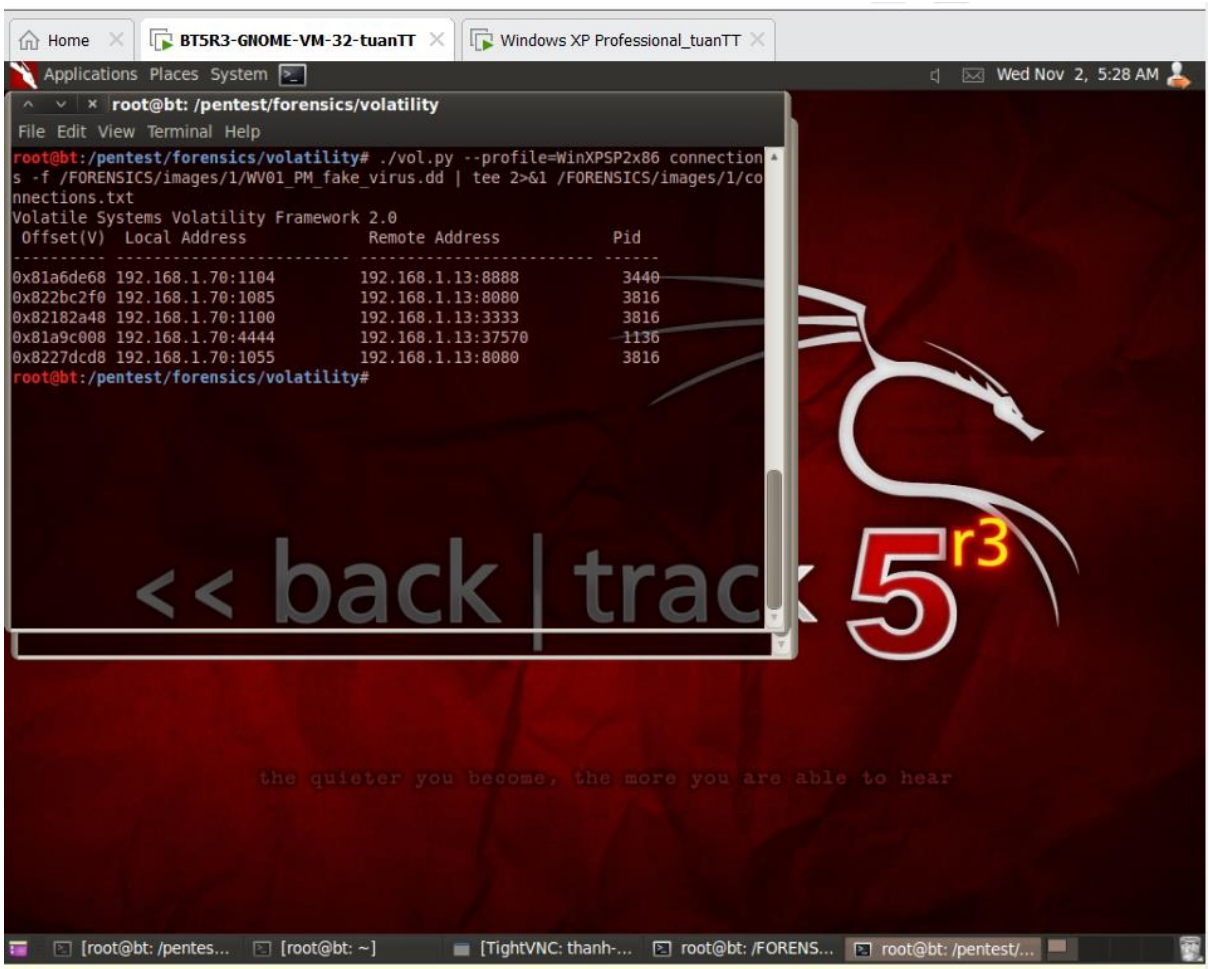
2. Navigate to Volatility



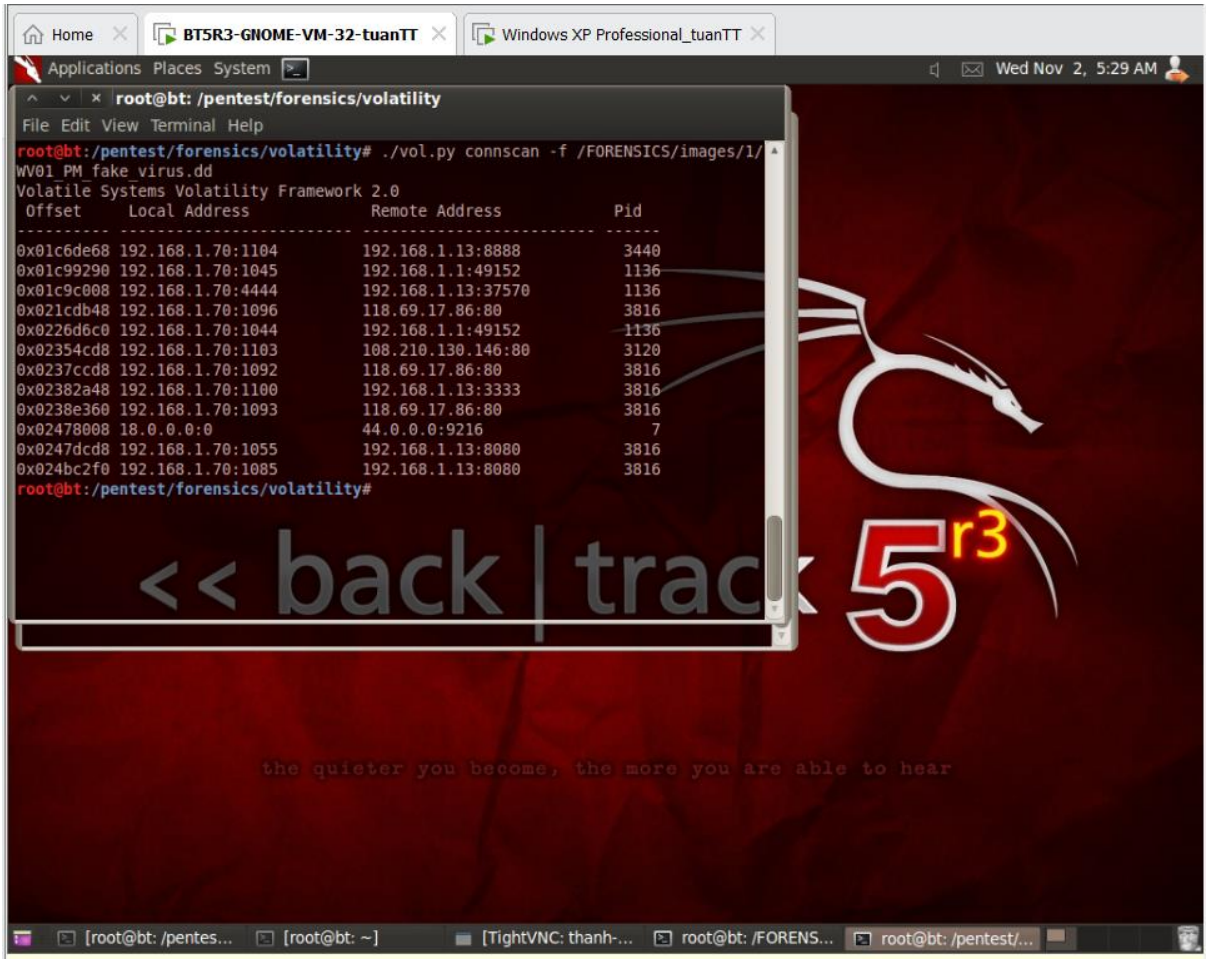
3. Obtain the image profile



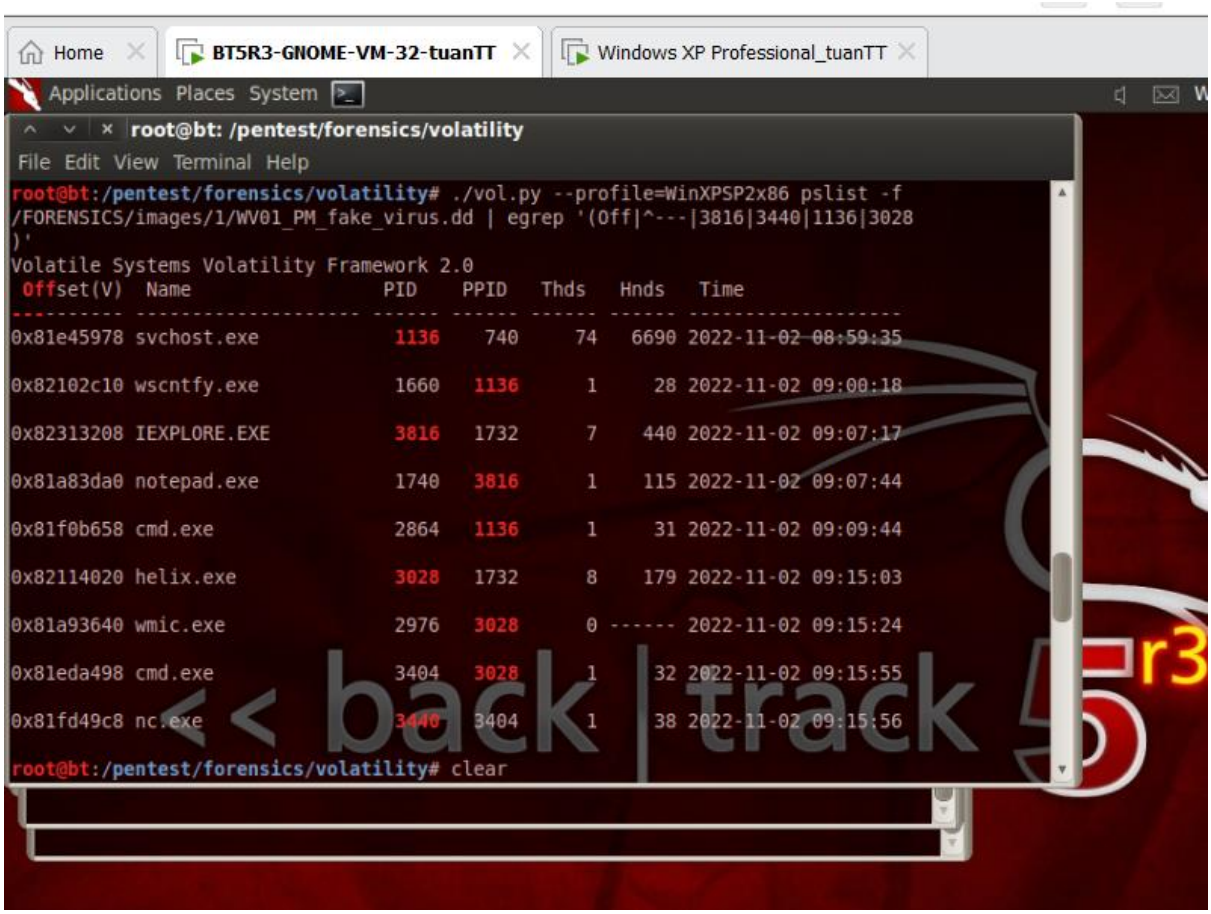
4. View Open Connections with Volatility

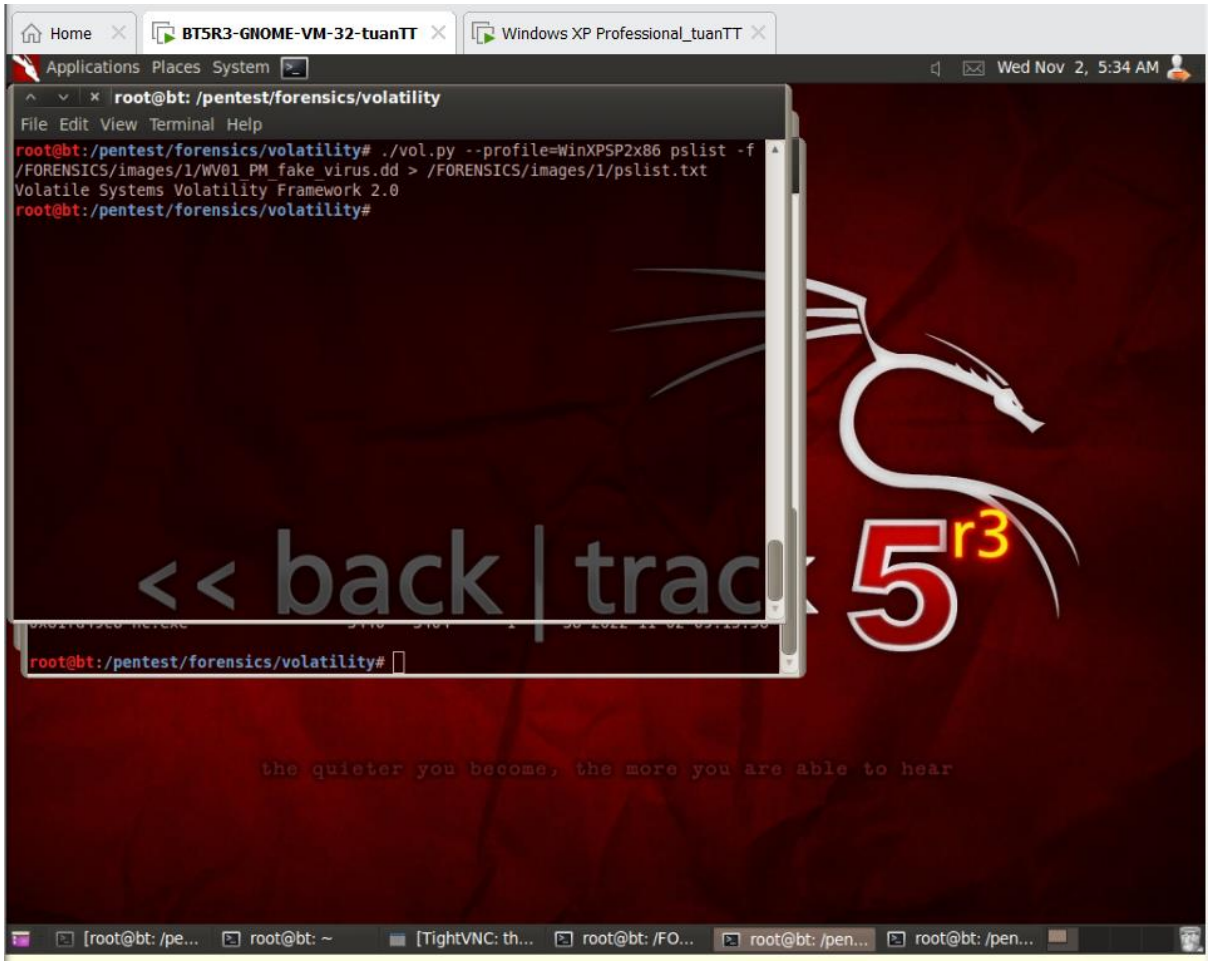


5. View Open and Dead Connections with Volatility

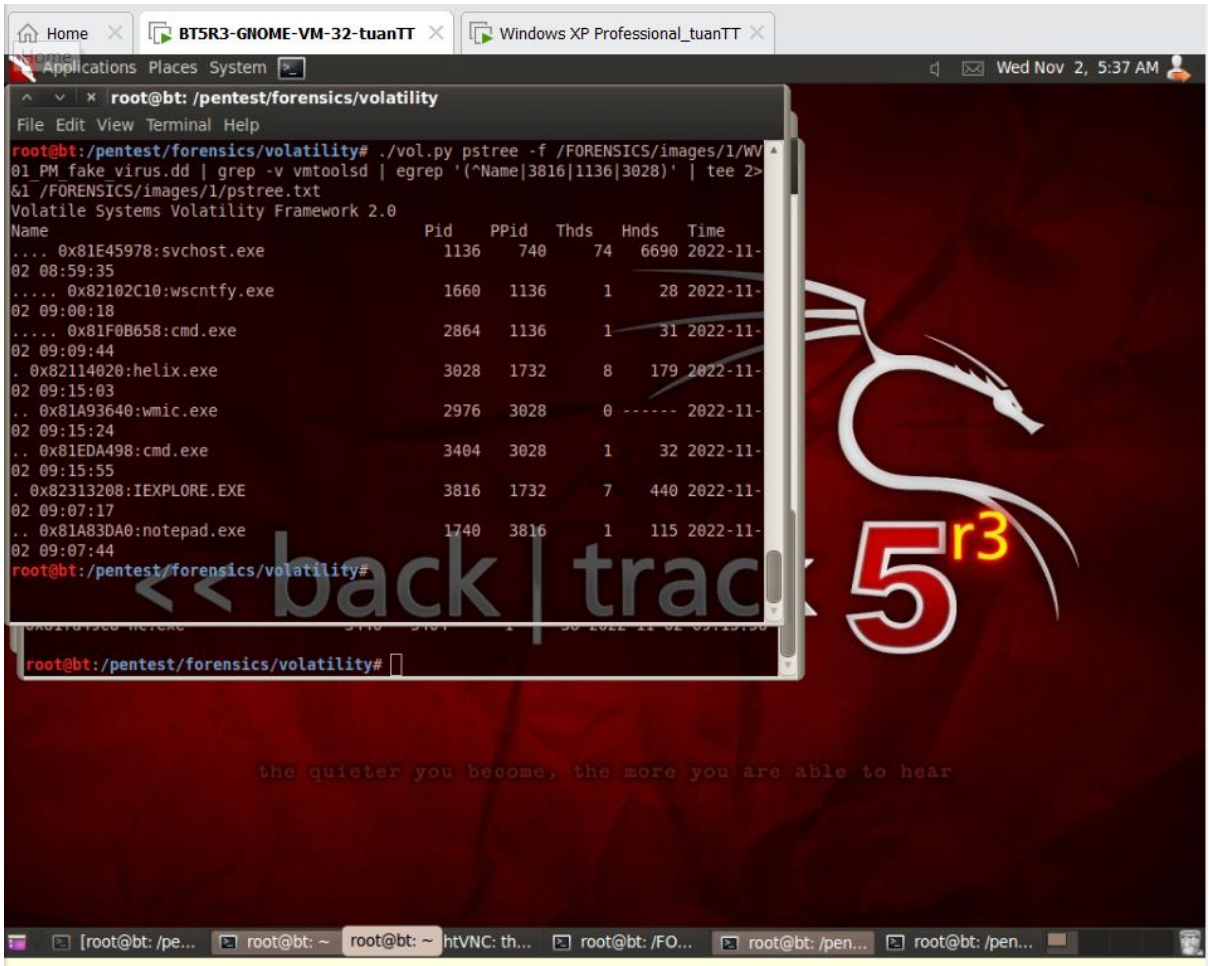


6. View Processes with Volatility

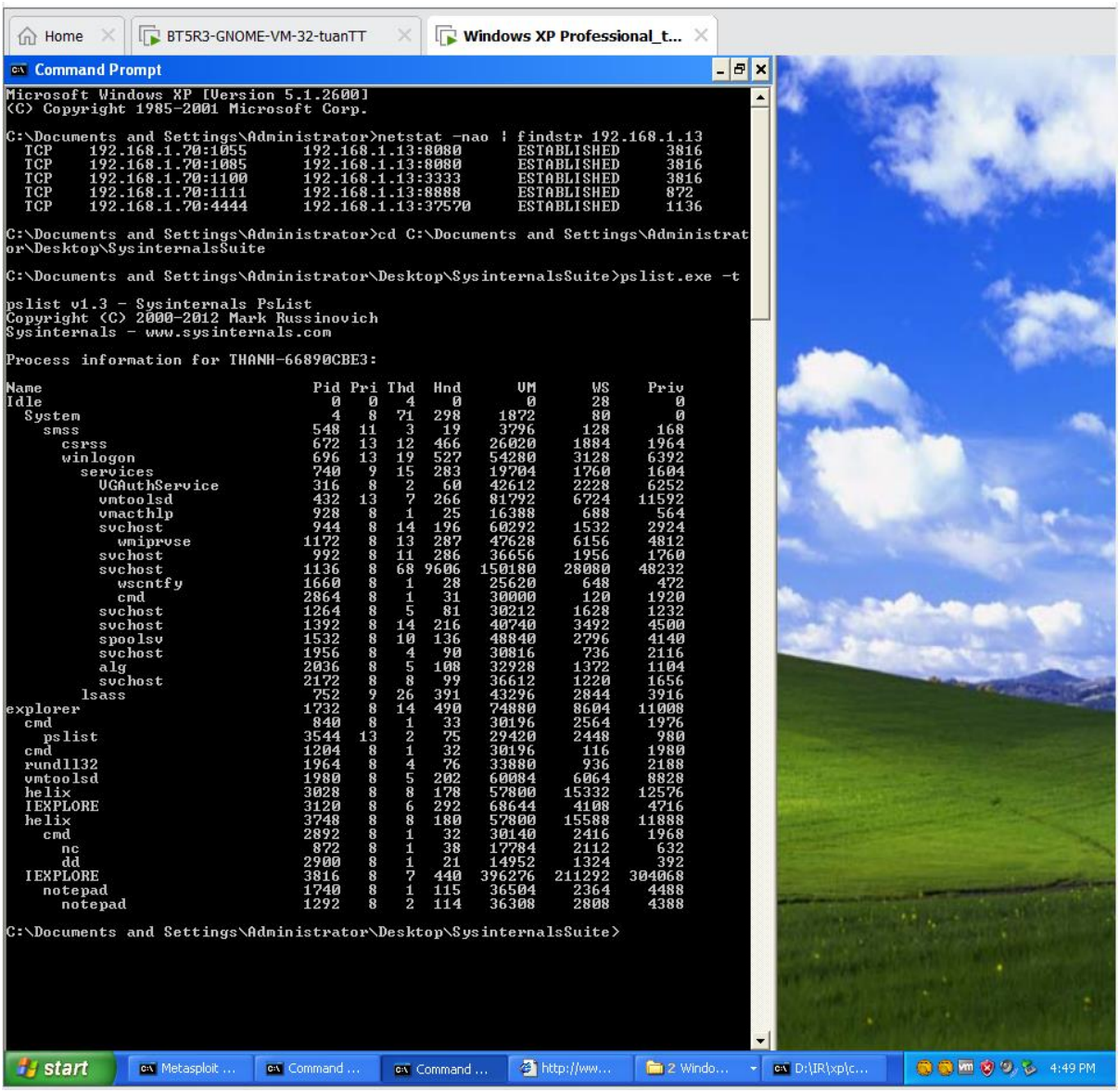

Home
BT5R3-GNOME-VM-32-tuanTT
Windows XP Professional_tuanTT
Applications Places System
root@bt: /pentest/forensics/volatility
File Edit View Terminal Help
root@bt:/pentest/forensics/volatility# ./vol.py --profile=WinXPSP2x86 pslist -f /FORENSICS/images/1/WV01_PM_fake_virus.dd | egrep '(Off|^---|3816|3440|1136|3028)'
Volatile Systems Volatility Framework 2.0
Offset(V) Name PID PPID Thds Hnds Time
0x81e45978 svchost.exe 1136 740 74 6690 2022-11-02 08:59:35
0x82102c10 wscntfy.exe 1660 1136 1 28 2022-11-02 09:00:18
0x82313208 IEXPLORE.EXE 3816 1732 7 440 2022-11-02 09:07:17
0x81a83da0 notepad.exe 1740 3816 1 115 2022-11-02 09:07:44
0x81f0b658 cmd.exe 2864 1136 1 31 2022-11-02 09:09:44
0x82114020 helix.exe 3028 1732 8 179 2022-11-02 09:15:03
0x81a93640 wmic.exe 2976 3028 0 ------ 2022-11-02 09:15:24
0x81eda498 cmd.exe 3404 3028 1 32 2022-11-02 09:15:55
0x81fd49c8 nc.exe 3440 3404 1 38 2022-11-02 09:15:56
root@bt:/pentest/forensics/volatility# clear
back | track
r3



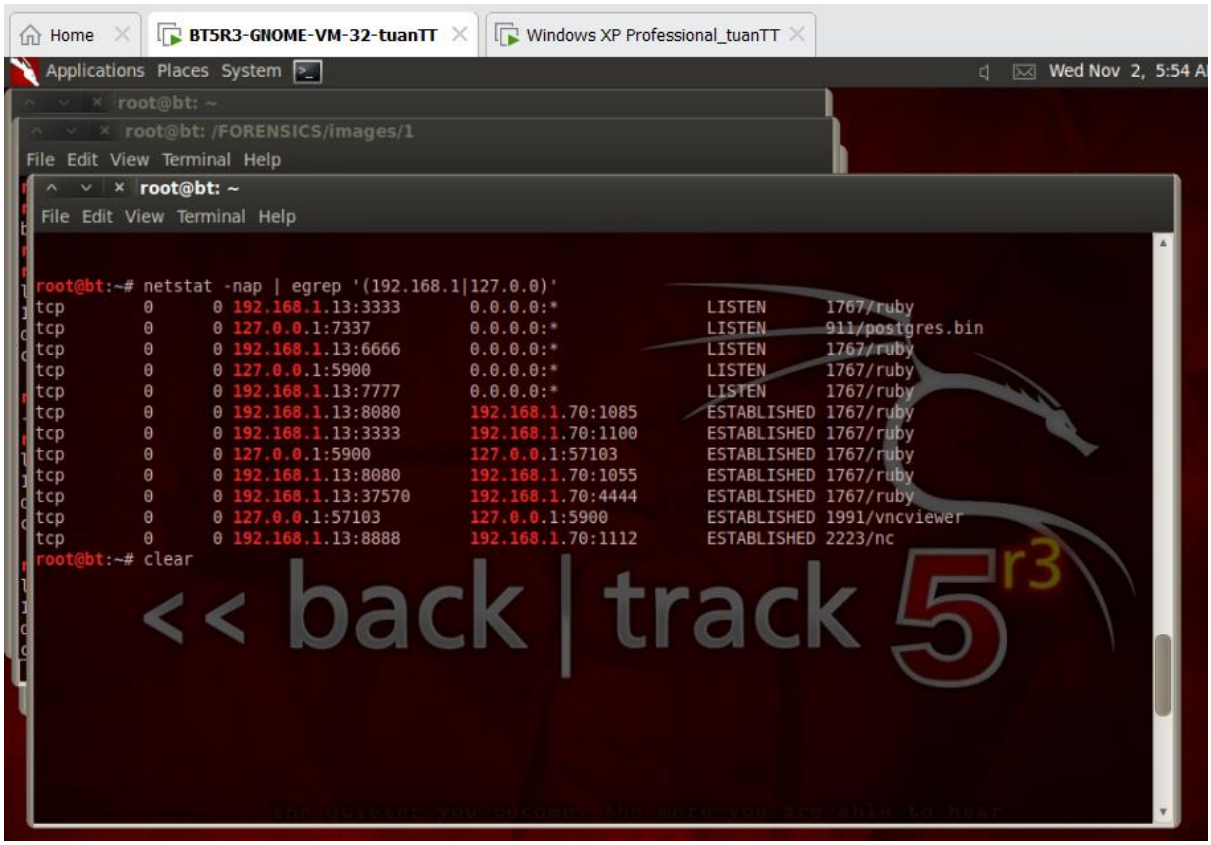
7. View Open Connections with Volatility

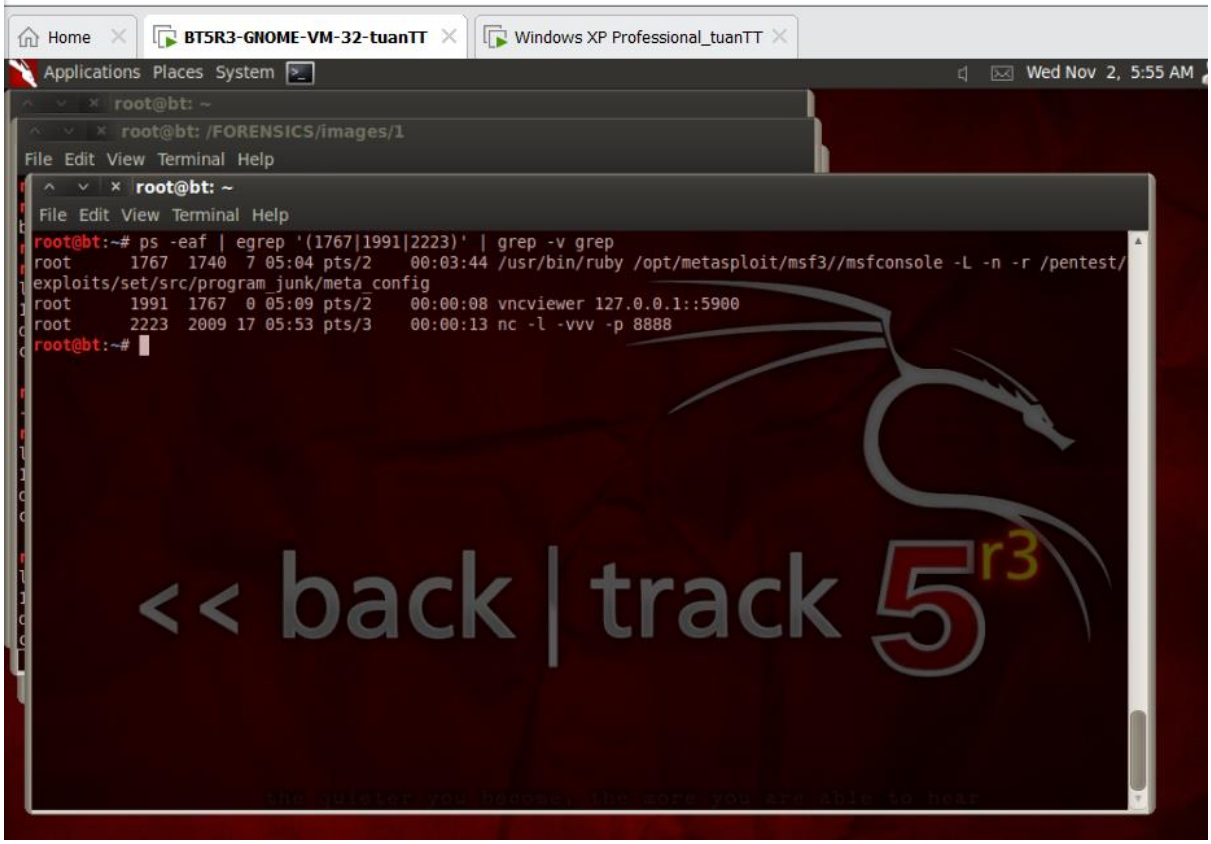


8. Comparing Volatility to netstat and pslist on the Victim Machine

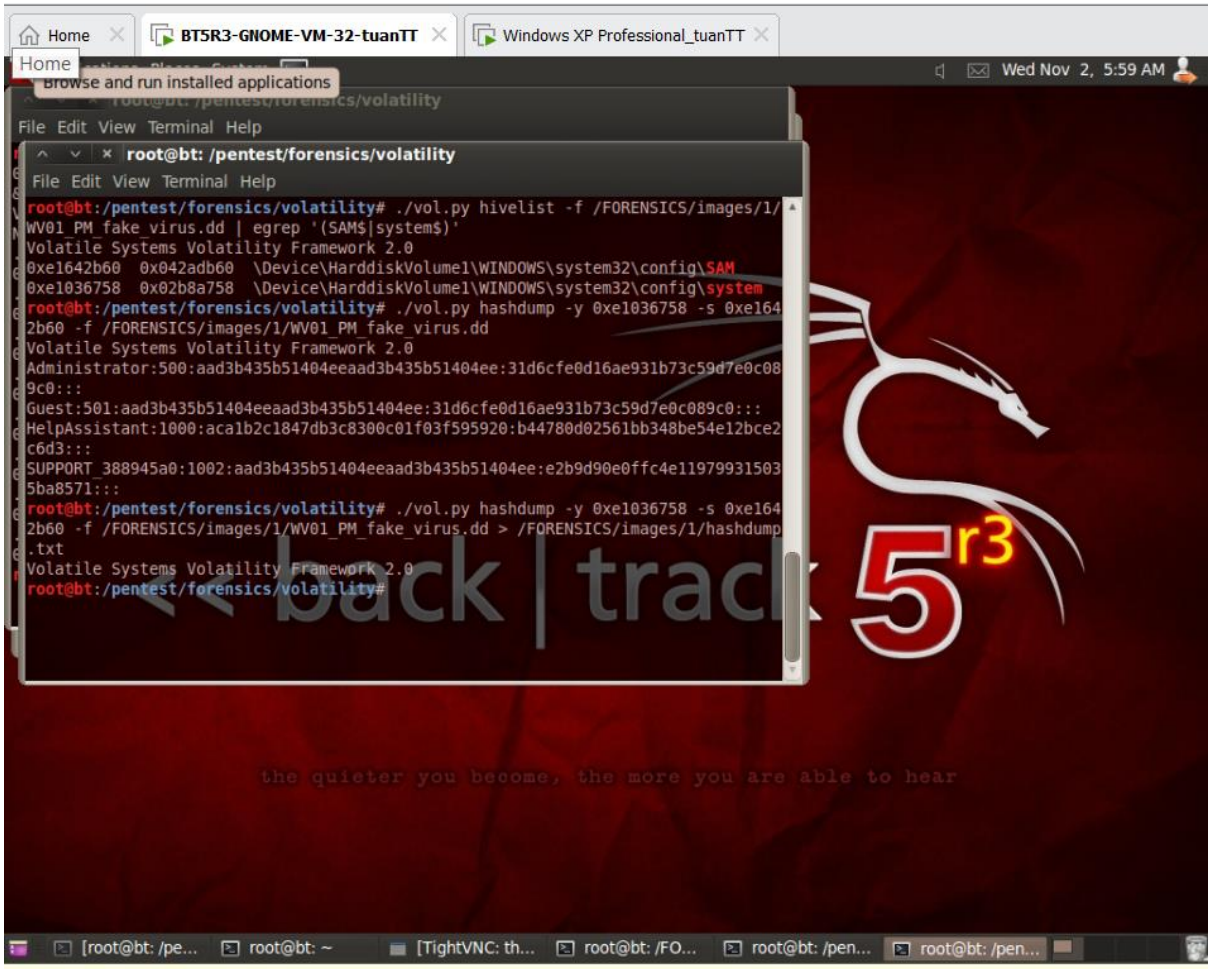


9. Let's Analyze what the Attacker's Network Connections

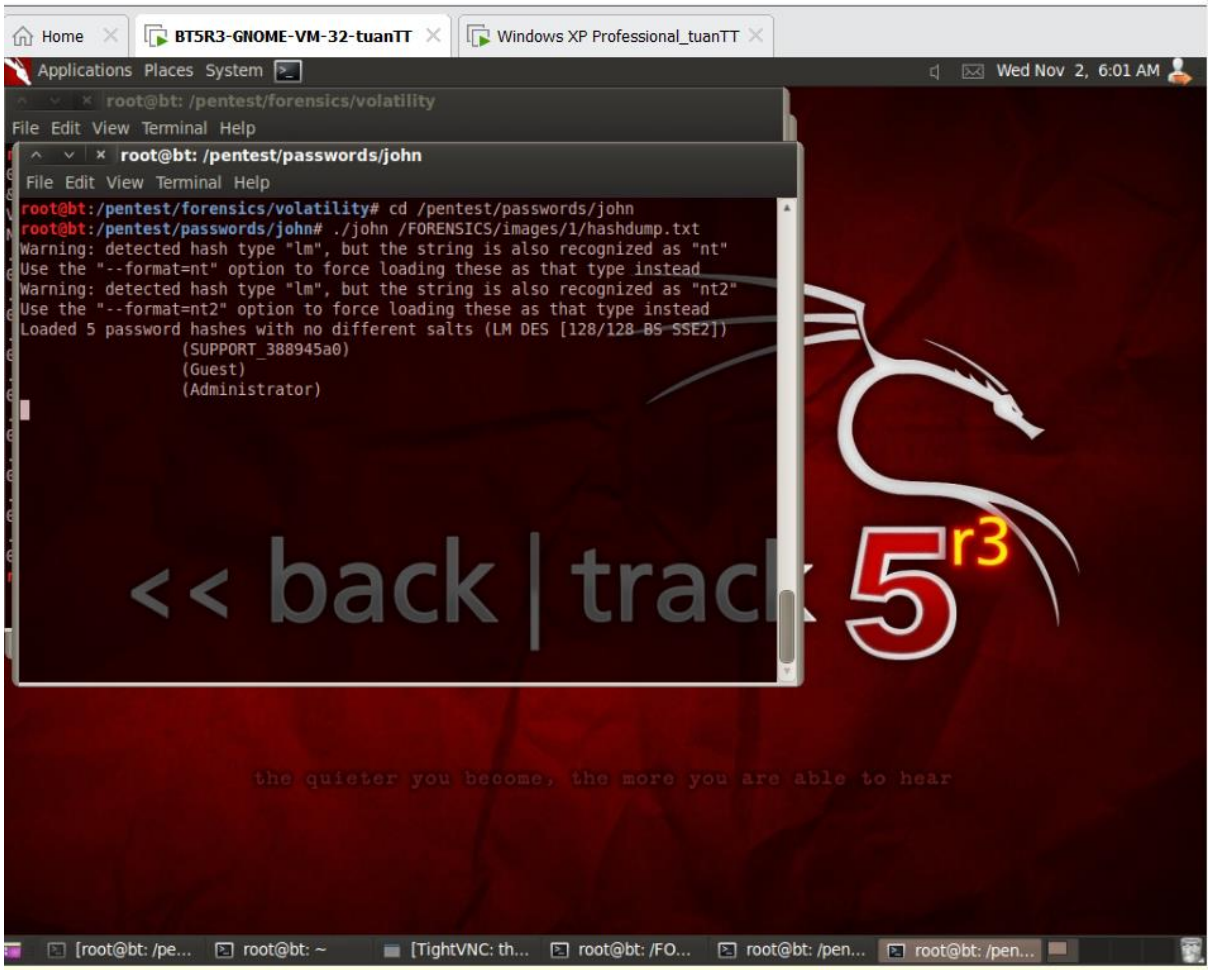




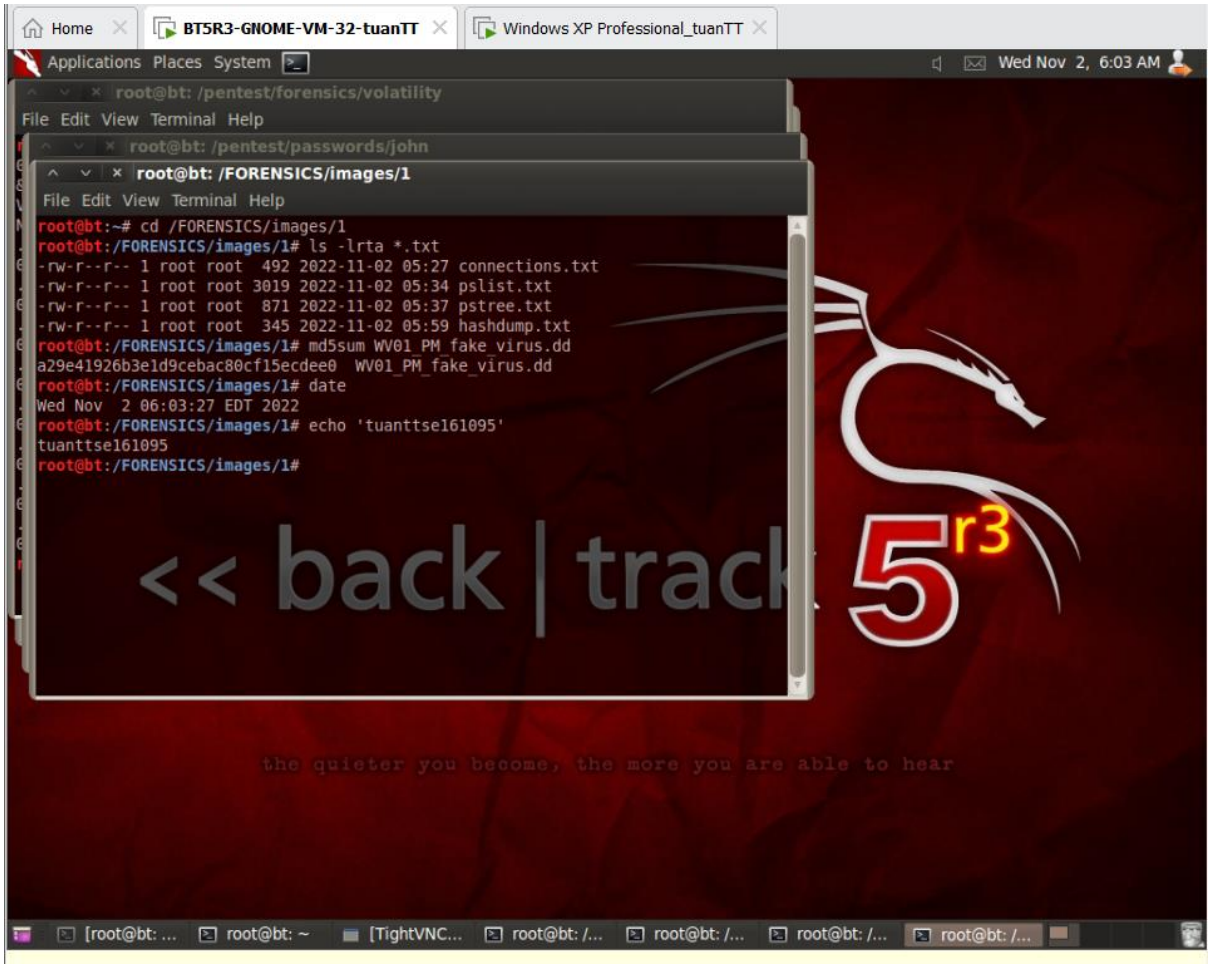
10. Using Volatilities' hivelist and hashdump



11. Using John the Ripper to crack the hashdump



Section 4. Proof of Lab


Home
BT5R3-GNOME-VM-32-tuanTT
Windows XP Professional_tuanTT
Applications Places System
Wed Nov 2, 6:03 AM
root@bt: /pentest/forensics/volatility
File Edit View Terminal Help
root@bt: /pentest/passwords/john
root@bt: /FORENSICS/images/1
File Edit View Terminal Help
root@bt:~# cd /FORENSICS/images/1
root@bt:/FORENSICS/images/1# ls -lrta *.txt
-rw-r--r-- 1 root root 492 2022-11-02 05:27 connections.txt
-rw-r--r-- 1 root root 3019 2022-11-02 05:34 pslist.txt
-rw-r--r-- 1 root root 871 2022-11-02 05:37 pstree.txt
-rw-r--r-- 1 root root 345 2022-11-02 05:59 hashdump.txt
root@bt:/FORENSICS/images/1# md5sum WV01_PM_fake_virus.dd
a29e41926b3e1d9cebac80cf15ecdee0 WV01_PM_fake_virus.dd
root@bt:/FORENSICS/images/1# date
Wed Nov 2 06:03:27 EDT 2022
root@bt:/FORENSICS/images/1# echo 'tuanttse161095'
tuanttse161095
root@bt:/FORENSICS/images/1#
<< back | track
5r3
the quieter you become, the more you are able to hear
[root@bt: ...
root@bt: ~
[TightVNC...
root@bt: /...
root@bt: /...
root@bt: /...
root@bt: /...