**WIRESHARK ASSIGNMENT**

Wireshark:

tcp.stream eq 1

Right click on any TCP stream -> Follow -> TCP Stream

OUTPUT:

whoami

root

finger

Login Name Tty Idle Login Time Office Office Phone

root root tty2 19 Apr 21 12:08 (:1)

ls

Desktop

Documents

Downloads

index.html

index.html.1

Music

passhash.txt

Pictures

Public

Templates

Videos

VIP.txt

cat passhash.txt

root:!:16894:0:99999:7:::

daemon:\*:16848:0:99999:7:::

bin:\*:16848:0:99999:7:::

sys:\*:16848:0:99999:7:::

sync:\*:16848:0:99999:7:::

games:\*:16848:0:99999:7:::

man:\*:16848:0:99999:7:::

lp:\*:16848:0:99999:7:::

mail:\*:16848:0:99999:7:::

news:\*:16848:0:99999:7:::

uucp:\*:16848:0:99999:7:::

proxy:\*:16848:0:99999:7:::

www-data:\*:16848:0:99999:7:::

backup:\*:16848:0:99999:7:::

list:\*:16848:0:99999:7:::

irc:\*:16848:0:99999:7:::

gnats:\*:16848:0:99999:7:::

nobody:\*:16848:0:99999:7:::

libuuid:!:16848:0:99999:7:::

syslog:\*:16848:0:99999:7:::

messagebus:\*:16848:0:99999:7:::

usbmux:\*:16848:0:99999:7:::

dnsmasq:\*:16848:0:99999:7:::

avahi-autoipd:\*:16848:0:99999:7:::

kernoops:\*:16848:0:99999:7:::

rtkit:\*:16848:0:99999:7:::

saned:\*:16848:0:99999:7:::

whoopsie:\*:16848:0:99999:7:::

speech-dispatcher:!:16848:0:99999:7:::

avahi:\*:16848:0:99999:7:::

lightdm:\*:16848:0:99999:7:::

colord:\*:16848:0:99999:7:::

hplip:\*:16848:0:99999:7:::

pulse:\*:16848:0:99999:7:::

ubuntu:$6$AjFg.NqU$rBwznt4HkQgeZgQWBdVIPnBZ1KDEJryKc/twM7.kkg0T1aNj0vmEuVh8PFirlFLiWHVrBjx91djHvdBZHDP9S1:16894:0:99999:7:::

mysql:!:16894:0:99999:7:::

vboxadd:!:16894::::::

baduser:$6$DFgbmv4K$mlpIp3gie4qKcWz7EZf1AmoOfgt1QQq/odn90mtPQKM4NoGx0altbXwwb9O/u6ImXGfd0A5f/Cn6PdNRnmZeR/:16894:0:99999:7:::

baduser2:$6$WpxOCca.$o.062ugs8TE7ivyl.SePIXQypZ7q.aYfcekd5BvFaNCQ3Ts7xUSezhwr.A6bPccgU.t5ZJM8Yqtgvk8jEtKGO/:16894:0:99999:7:::

lameuser:$6$ononDTYO$LJxrY4Q8Hs/XyIqgVMgdCG0U9jGaJcnqyZbQxSYfE22MSIiqZDymVcSx0JCRNkxBfY68NMAVmxz9cIH8c5GSW1:16911:0:99999:7:::

lazyuser:$6$p0jnqsf0$IG.cLpkWnRctFb.y9mvRYihWzT1ytPKGXQEdaBJirpcY2o7SuYRUSSCur1XhT5yM4kH50gA8hvX05PU48Nb8M/:16911:0:99999:7:::

sportyuser:$6$cwPPktan$2IjOiAfrcZNXJr7lDmAdLv0Bz7gNfLHn9FC/DqoRx9JwMBXcAahYrIPqbGr.NbLf61rakDJPIw2UvGzaqwync0:16911:0:99999:7:::

spicyuser:$6$UYfPgPA6$a9aT0Mh6u5ptC9tiJ4juQ.Bk1IwiurMdg6bHELXHoevV5a.Jd8Q6a2gDvXi9xo15acluCdNEigqMsK0TGTAEx1:16911:0:99999:7:::

gardeninguser:$6$jWU8HNvu$PhBbnaUH8Gr2utcUMBvg6bXwuo3gR8.oFa1lUJ2R9xH/KAsIY..9LwOzJ8Mxo8ukxMnfXypLttd.4QU.WZHQo/:16911:0:99999:7:::

adduser marcelle

Adding user `marcelle' ...

Adding new group `marcelle' (1001) ...

Adding new user `marcelle' (1000) with group `marcelle' ...

Creating home directory `/home/marcelle' ...

Copying files from `/etc/skel' ...

password

password

Changing the user information for marcelle

Enter the new value, or press ENTER for the default

Full Name []:

Room Number []:

Work Phone []:

Home Phone []:

Other []:

Is the information correct? [Y/n] Y

cat /etc/shadow

root:$6$XHxtN5iB$5WOyg3gGfzr9QHPLo.7z0XIQIzEW6Q3/K7iipxG7ue04CmelkjC51SndpOcQlxTHmW4/AKKsKew4f3cb/.BK8/:16828:0:99999:7:::

daemon:\*:16820:0:99999:7:::

bin:\*:16820:0:99999:7:::

sys:\*:16820:0:99999:7:::

sync:\*:16820:0:99999:7:::

games:\*:16820:0:99999:7:::

man:\*:16820:0:99999:7:::

lp:\*:16820:0:99999:7:::

mail:\*:16820:0:99999:7:::

news:\*:16820:0:99999:7:::

uucp:\*:16820:0:99999:7:::

proxy:\*:16820:0:99999:7:::

www-data:\*:16820:0:99999:7:::

backup:\*:16820:0:99999:7:::

list:\*:16820:0:99999:7:::

irc:\*:16820:0:99999:7:::

gnats:\*:16820:0:99999:7:::

nobody:\*:16820:0:99999:7:::

systemd-timesync:\*:16820:0:99999:7:::

systemd-network:\*:16820:0:99999:7:::

systemd-resolve:\*:16820:0:99999:7:::

systemd-bus-proxy:\*:16820:0:99999:7:::

\_apt:\*:16820:0:99999:7:::

messagebus:\*:16820:0:99999:7:::

mysql:!:16820:0:99999:7:::

avahi:\*:16820:0:99999:7:::

miredo:\*:16820:0:99999:7:::

ntp:\*:16820:0:99999:7:::

stunnel4:!:16820:0:99999:7:::

uuidd:\*:16820:0:99999:7:::

Debian-exim:!:16820:0:99999:7:::

statd:\*:16820:0:99999:7:::

arpwatch:!:16820:0:99999:7:::

colord:\*:16820:0:99999:7:::

epmd:\*:16820:0:99999:7:::

couchdb:\*:16820:0:99999:7:::

dnsmasq:\*:16820:0:99999:7:::

geoclue:\*:16820:0:99999:7:::

pulse:\*:16820:0:99999:7:::

speech-dispatcher:!:16820:0:99999:7:::

sshd:\*:16820:0:99999:7:::

snmp:\*:16820:0:99999:7:::

postgres:\*:16820:0:99999:7:::

iodine:\*:16820:0:99999:7:::

king-phisher:\*:16820:0:99999:7:::

redsocks:!:16820:0:99999:7:::

rwhod:\*:16820:0:99999:7:::

sslh:!:16820:0:99999:7:::

rtkit:\*:16820:0:99999:7:::

saned:\*:16820:0:99999:7:::

usbmux:\*:16820:0:99999:7:::

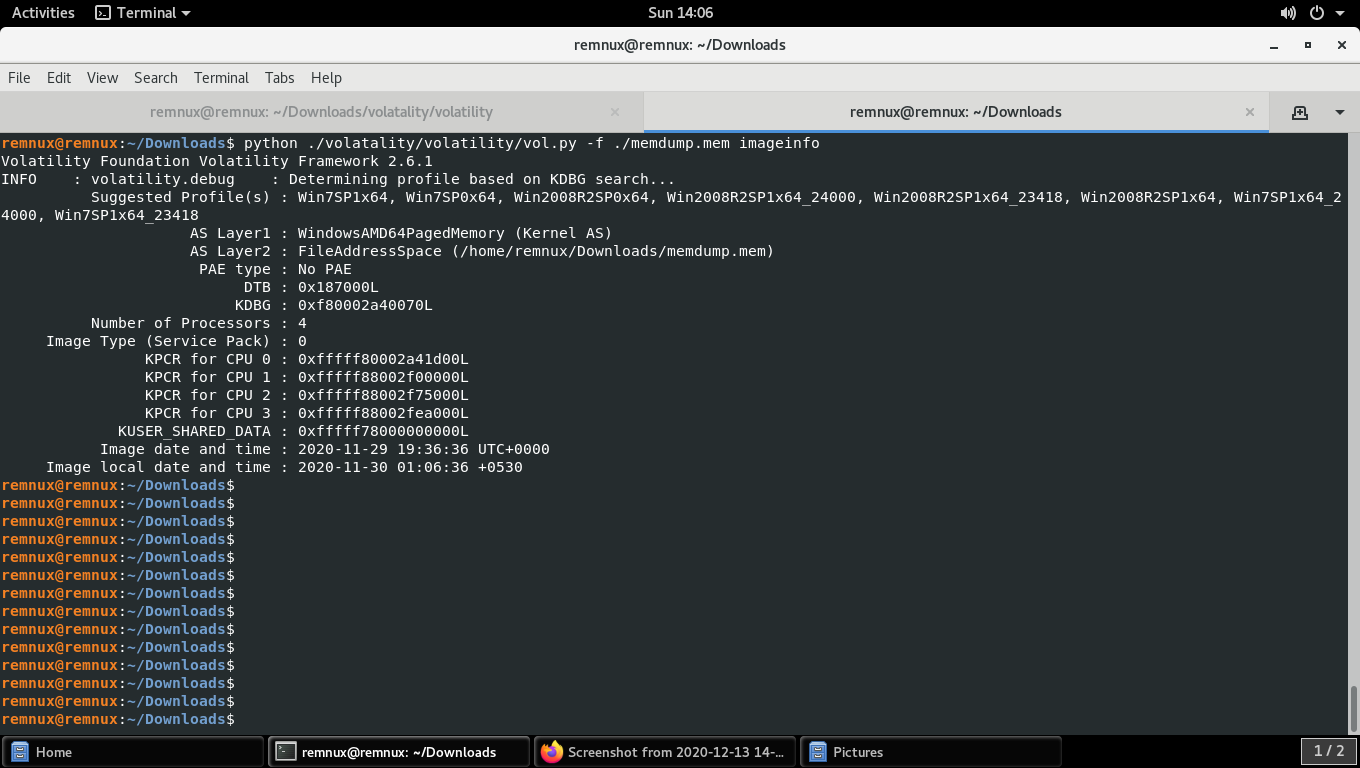
Debian-gdm:\*:16820:0:99999:7:::

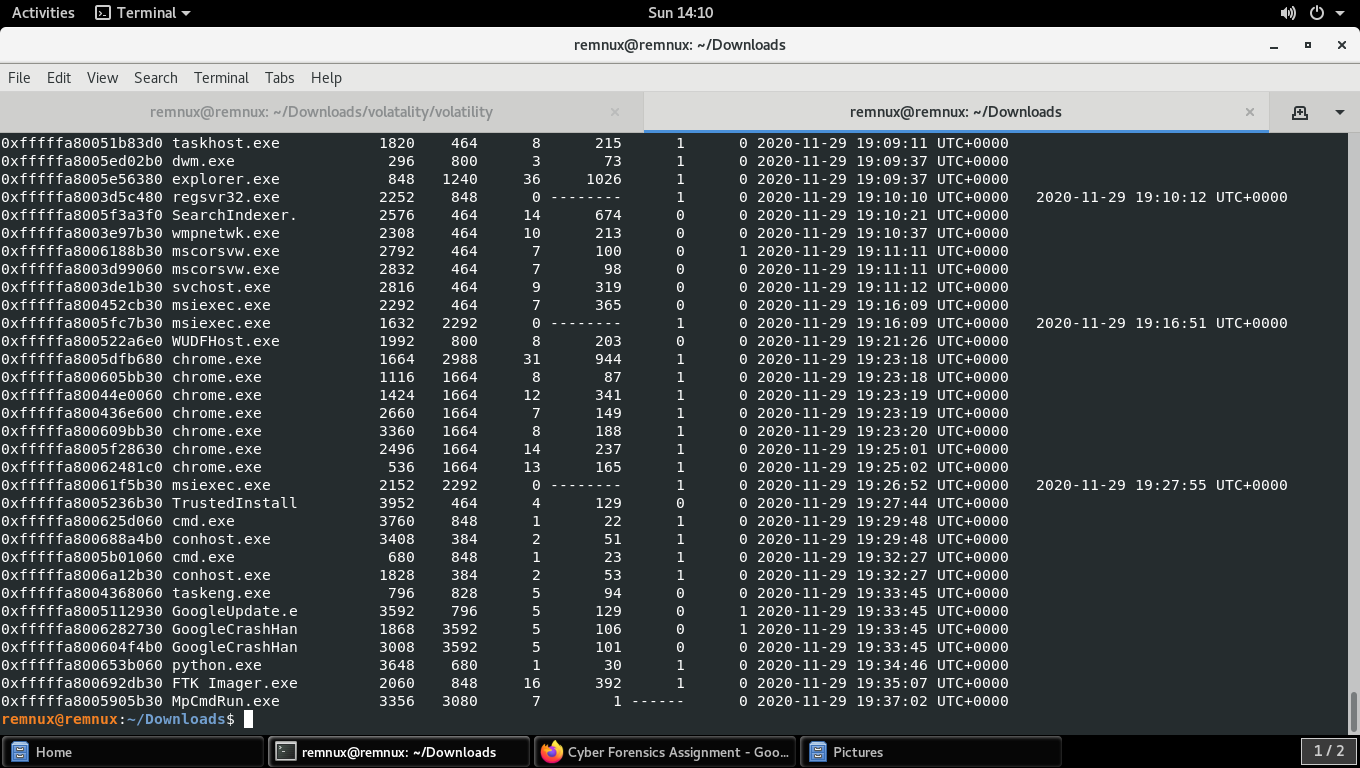
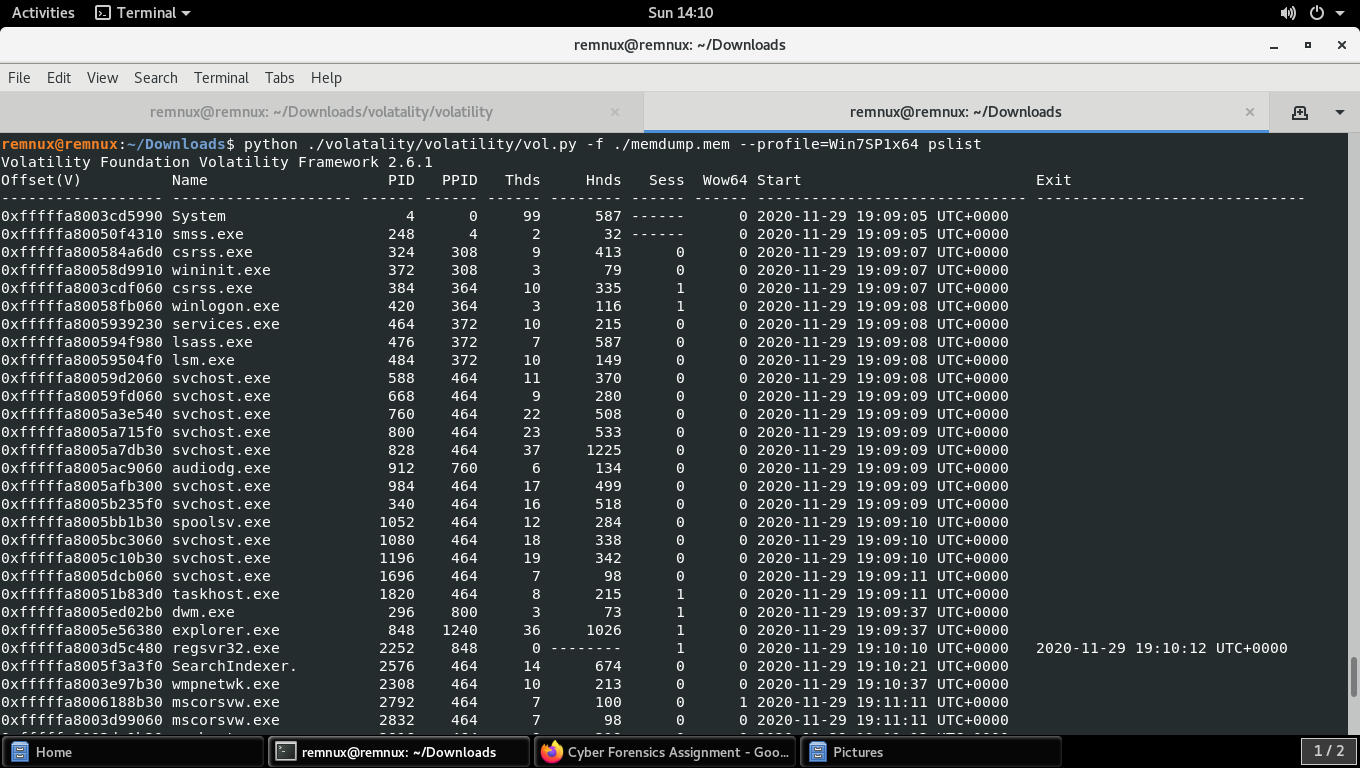
beef-xss:\*:16820:0:99999:7:::

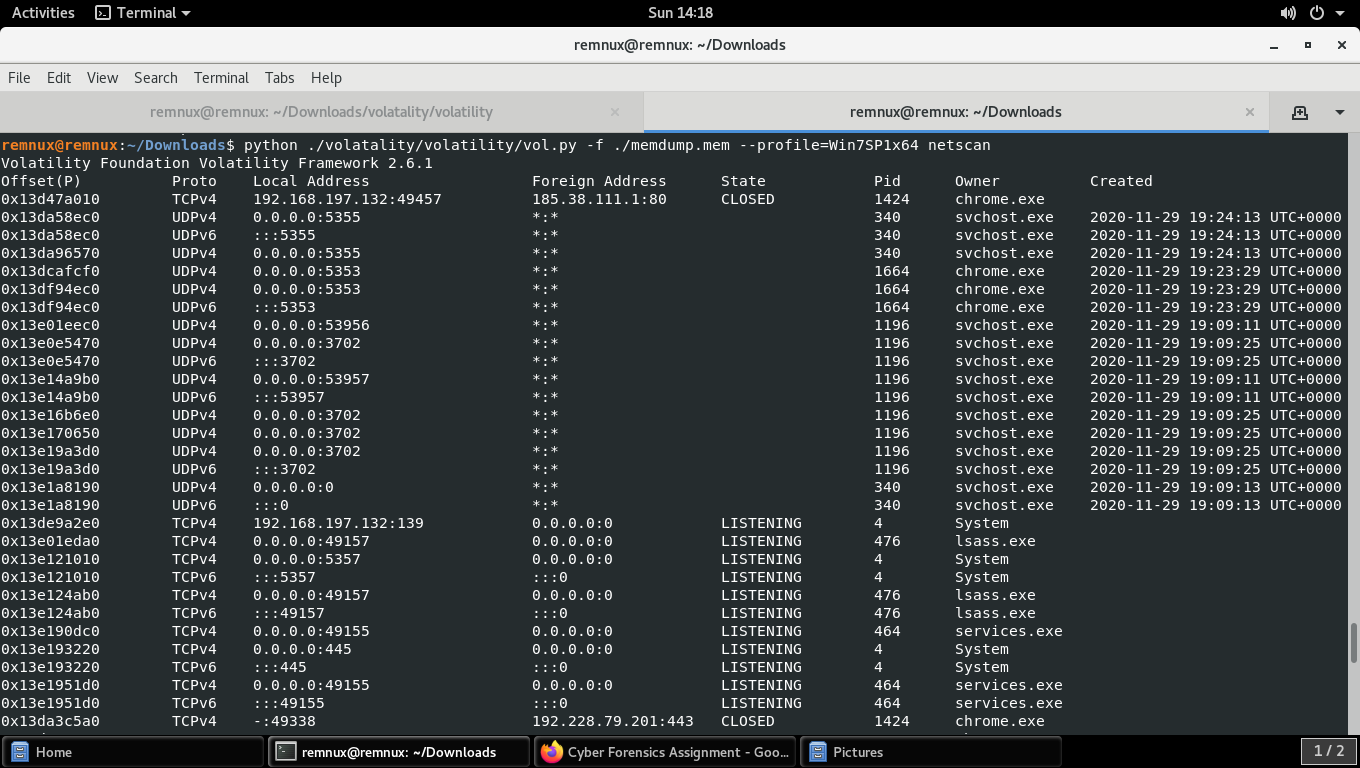
dradis:\*:16820:0:99999:7:::

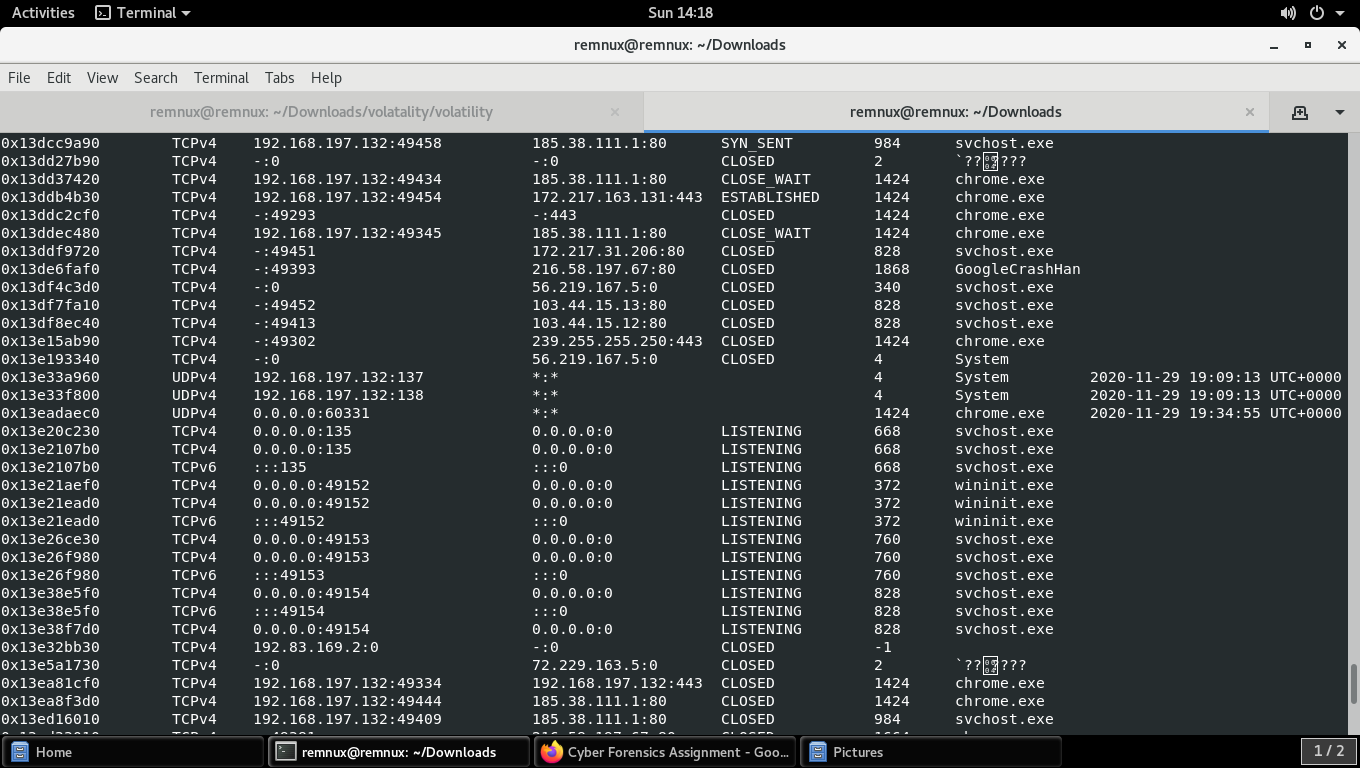
marcelle:$6$jWMiRdjv$HazXeOGL5LIrnYm8VbyaqEI0k/H18PDH33TL88beL2adha3NIdLmPXsiw.AoSk9q7STtOuK0w6XKBIEOamUnf0:16912:0:99999:7:::

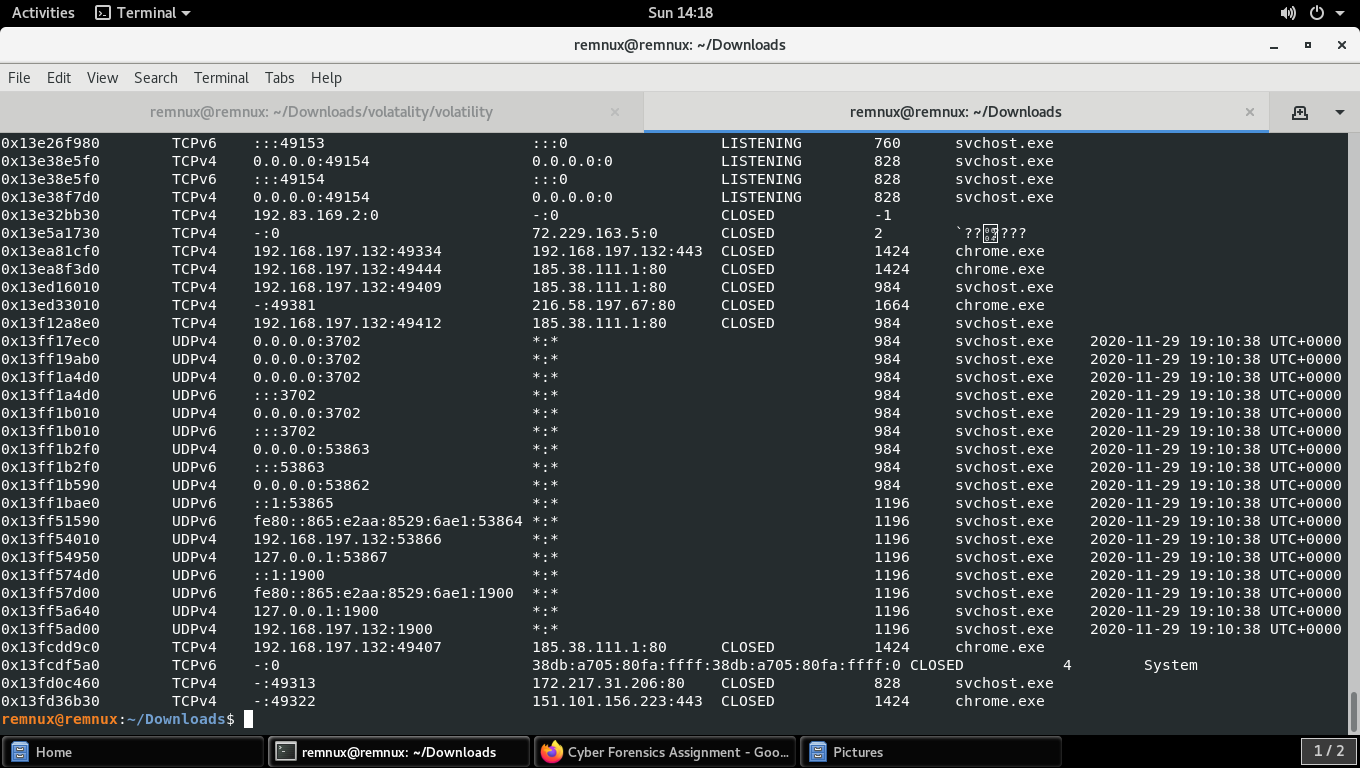
**REMUX (Volitality CTF Final):**











**remnux@remnux:~/Downloads$ python ./volatality/volatility/vol.py -f ./memdump.mem --profile=Win7SP1x64 iehistory**

Volatility Foundation Volatility Framework 2.6.1

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Process: 848 explorer.exe

Cache type "URL " at 0x3b86000

Record length: 0x180

Location: http://www.bing.com/favicon.ico

Last modified: 2020-11-22 16:38:29 UTC+0000

Last accessed: 2020-11-29 19:18:21 UTC+0000

File Offset: 0x180, Data Offset: 0x88, Data Length: 0x98

File: favicon[1].ico

Data: HTTP/1.1 200 OK

Content-Length: 237

Content-Type: image/x-icon

X-Cache: TCP\_HIT

X-MSEdge-Ref: Ref A: D423F8DCD55946CFB4FBC872A8404DB8 Ref B: MAA02EDGE0315 Ref C: 2020-11-30T08:48:21Z

~U:findme

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Process: 848 explorer.exe

Cache type "URL " at 0x3b86180

Record length: 0x180

Location: http://www.bing.com/favicon.ico

Last modified: 2020-11-22 16:38:29 UTC+0000

Last accessed: 2020-11-29 19:20:27 UTC+0000

File Offset: 0x180, Data Offset: 0x88, Data Length: 0x98

File: favicon[1].png

Data: HTTP/1.1 200 OK

Content-Length: 237

Content-Type: image/x-icon

X-Cache: TCP\_HIT

X-MSEdge-Ref: Ref A: D423F8DCD55946CFB4FBC872A8404DB8 Ref B: MAA02EDGE0315 Ref C: 2020-11-30T08:48:21Z

~U:findme

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Process: 848 explorer.exe

Cache type "URL " at 0x3b87000

Record length: 0x280

Location: https://www.google.com/favicon.ico

Last modified: 2019-10-22 18:30:00 UTC+0000

Last accessed: 2020-11-29 19:18:25 UTC+0000

File Offset: 0x280, Data Offset: 0x8c, Data Length: 0x9c

File: favicon[1].ico

Data: HTTP/1.1 200 OK

Content-Type: image/x-icon

Cross-Origin-Resource-Policy: cross-origin

X-Content-Type-Options: nosniff

X-XSS-Protection: 0

Alt-Svc: h3-29=":443"; ma=2592000,h3-T051=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43"

Content-Length: 5430

~U:findme

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Process: 848 explorer.exe

Cache type "URL " at 0x3b87280

Record length: 0x200

Location: https://ieonline.microsoft.com/favicon.ico

Last modified: 2020-11-25 15:45:41 UTC+0000

Last accessed: 2020-11-29 19:18:32 UTC+0000

File Offset: 0x200, Data Offset: 0x94, Data Length: 0xa4

File: favicon[1].ico

Data: HTTP/1.1 200 OK

Content-Length: 237

Content-Type: image/x-icon

Strict-Transport-Security: max-age=31536000; includeSubDomains; preload

X-MSEdge-Ref: Ref A: 90EB859642E444A5AF176D2A5600DB1F Ref B: MAA02EDGE0314 Ref C: 2020-11-30T08:48:32Z

~U:findme

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Process: 848 explorer.exe

Cache type "URL " at 0x3b87480

Record length: 0x200

Location: https://ieonline.microsoft.com/favicon.ico

Last modified: 2020-11-25 15:45:41 UTC+0000

Last accessed: 2020-11-29 19:18:32 UTC+0000

File Offset: 0x200, Data Offset: 0x94, Data Length: 0xa4

File: favicon[1].png

Data: HTTP/1.1 200 OK

Content-Length: 237

Content-Type: image/x-icon

Strict-Transport-Security: max-age=31536000; includeSubDomains; preload

X-MSEdge-Ref: Ref A: 90EB859642E444A5AF176D2A5600DB1F Ref B: MAA02EDGE0314 Ref C: 2020-11-30T08:48:32Z

~U:findme

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Process: 848 explorer.exe

Cache type "URL " at 0x4335000

Record length: 0x100

Location: :2020113020201201: Findme@file:///C:/Py\_exmple/hello\_vit.py

Last modified: 2020-11-30 01:01:05 UTC+0000

Last accessed: 2020-11-29 19:31:05 UTC+0000

File Offset: 0x100, Data Offset: 0x0, Data Length: 0x0

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Process: 848 explorer.exe

Cache type "URL " at 0x4335100

Record length: 0x100

Location: :2020113020201201: Findme@:Host: www.google.com

Last modified: 2020-11-30 00:48:10 UTC+0000

Last accessed: 2020-11-29 19:18:10 UTC+0000

File Offset: 0x100, Data Offset: 0x0, Data Length: 0x0

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Process: 848 explorer.exe

Cache type "URL " at 0x4335200

Record length: 0x100

Location: :2020113020201201: Findme@https://www.google.com/?gws\_rd=ssl

Last modified: 2020-11-30 00:50:06 UTC+0000

Last accessed: 2020-11-29 19:20:06 UTC+0000

File Offset: 0x100, Data Offset: 0x0, Data Length: 0x0

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Process: 848 explorer.exe

Cache type "URL " at 0x4335300

Record length: 0x100

Location: :2020113020201201: Findme@:Host: Computer

Last modified: 2020-11-30 01:01:05 UTC+0000

Last accessed: 2020-11-29 19:31:05 UTC+0000

File Offset: 0x100, Data Offset: 0x0, Data Length: 0x0

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Process: 848 explorer.exe

Cache type "DEST" at 0x4b7d8ad

Last modified: 2020-11-30 01:01:05 UTC+0000

Last accessed: 2020-11-29 19:31:06 UTC+0000

URL: Findme@file:///C:/Py\_exmple/hello\_vit.py

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Process: 848 explorer.exe

Cache type "URL " at 0x4745000

Record length: 0x100

Location: Visited: Findme@http://www.google.com

Last modified: 2020-11-29 19:17:15 UTC+0000

Last accessed: 2020-11-29 19:17:15 UTC+0000

File Offset: 0x100, Data Offset: 0x0, Data Length: 0x90

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Process: 848 explorer.exe

Cache type "URL " at 0x4745100

Record length: 0x100

Location: Visited: Findme@https://support.microsoft.com/internet-explorer

Last modified: 2020-11-29 19:18:17 UTC+0000

Last accessed: 2020-11-29 19:18:17 UTC+0000

File Offset: 0x100, Data Offset: 0x0, Data Length: 0xa8

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Process: 848 explorer.exe

Cache type "URL " at 0x4745200

Record length: 0x100

Location: Visited: Findme@http://google.com

Last modified: 2020-11-29 19:18:09 UTC+0000

Last accessed: 2020-11-29 19:18:09 UTC+0000

File Offset: 0x100, Data Offset: 0x0, Data Length: 0x8c

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Process: 848 explorer.exe

Cache type "URL " at 0x4745300

Record length: 0x100

Location: Visited: Findme@https://ieonline.microsoft.com/favicon.ico

Last modified: 2020-11-29 19:18:32 UTC+0000

Last accessed: 2020-11-29 19:18:32 UTC+0000

File Offset: 0x100, Data Offset: 0x0, Data Length: 0xa4

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Process: 848 explorer.exe

Cache type "URL " at 0x4745400

Record length: 0x100

Location: Visited: Findme@https://www.google.com/?gws\_rd=ssl

Last modified: 2020-11-29 19:23:22 UTC+0000

Last accessed: 2020-11-29 19:23:22 UTC+0000

File Offset: 0x100, Data Offset: 0x0, Data Length: 0x9c

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Process: 848 explorer.exe

Cache type "URL " at 0x4745500

Record length: 0x300

Location: Visited: Findme@https://www.google.com/sorry/index?continue=https://www.google.com/search%3Fhl%3Den-IN%26source%3Dhp%26q%3Dpython%26btnG%3DGoogle%2BSearch%26iflsig%3DAINFCbYAAAAAX8TAKTs2dioMnc7Esas-b2BwCskeM6Wr%26gbv%3D1&hl=en-IN&q=EgRnLA1BGMPkkv4FIhkA8aeDS7JPh8kiS-2IRvaL27FFFMs\_yzspMgFy

Last modified: 2020-11-29 19:20:11 UTC+0000

Last accessed: 2020-11-29 19:20:11 UTC+0000

File Offset: 0x300, Data Offset: 0x0, Data Length: 0x18c

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Process: 848 explorer.exe

Cache type "URL " at 0x4745800

Record length: 0x300

Location: Visited: Findme@https://www.google.com/sorry/index?continue=https://www.google.com/search%3Fhl%3Den-IN%26source%3Dhp%26q%3Dchrome%26iflsig%3DAINFCbYAAAAAX8TAKTs2dioMnc7Esas-b2BwCskeM6Wr%26gbv%3D1&hl=en-IN&q=EgRnLA1BGKDkkv4FIhkA8aeDS8PC1lDIX2rVDx\_27lZtROqyveSQMgFy

Last modified: 2020-11-29 19:19:45 UTC+0000

Last accessed: 2020-11-29 19:19:45 UTC+0000

File Offset: 0x300, Data Offset: 0x0, Data Length: 0x170

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Process: 848 explorer.exe

Cache type "URL " at 0x4745b00

Record length: 0x300

Location: Visited: Findme@https://www.google.com/sorry/index?continue=https://www.google.com/search%3Fhl%3Den-IN%26source%3Dhp%26q%3Dpython%26iflsig%3DAINFCbYAAAAAX8S\_2a-hxt1xgu0y32wpGuVlzhI1Qo5l%26gbv%3D1&hl=en-IN&q=EgRnLA1BGIPkkv4FIhkA8aeDS0lAzi8GNf2oAu2MfUXhHUou71SyMgFy

Last modified: 2020-11-29 19:19:51 UTC+0000

Last accessed: 2020-11-29 19:19:51 UTC+0000

File Offset: 0x300, Data Offset: 0x0, Data Length: 0x170

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Process: 848 explorer.exe

Cache type "URL " at 0x4745e00

Record length: 0x100

Location: Visited: Findme@https://www.msn.com/?ocid=iehp

Last modified: 2020-11-29 19:20:48 UTC+0000

Last accessed: 2020-11-29 19:20:48 UTC+0000

File Offset: 0x100, Data Offset: 0x0, Data Length: 0x98

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Process: 848 explorer.exe

Cache type "URL " at 0x4745f00

Record length: 0x100

Location: Visited: Findme@file:///C:/Py\_exmple/hello\_vit.py

Last modified: 2020-11-29 19:31:05 UTC+0000

Last accessed: 2020-11-29 19:31:05 UTC+0000

File Offset: 0x100, Data Offset: 0x0, Data Length: 0x9c

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Process: 848 explorer.exe

Cache type "URL " at 0x4746000

Record length: 0x300

Location: Visited: Findme@https://www.google.com/sorry/index?continue=https://www.google.com/search%3Fhl%3Den-IN%26source%3Dhp%26q%3Dpython%26btnG%3DGoogle%2BSearch%26iflsig%3DAINFCbYAAAAAX8TAKTs2dioMnc7Esas-b2BwCskeM6Wr%26gbv%3D1&hl=en-IN&q=EgRnLA1BGLjkkv4FIhkA8aeDS4I-Znd\_vF5gGp3vgEO7XDAdzSvhMgFy

Last modified: 2020-11-29 19:20:01 UTC+0000

Last accessed: 2020-11-29 19:20:01 UTC+0000

File Offset: 0x300, Data Offset: 0x0, Data Length: 0x18c

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Process: 848 explorer.exe

Cache type "URL " at 0x4746300

Record length: 0x100

Location: Visited: Findme@http://go.microsoft.com/fwlink/?LinkId=69157

Last modified: 2020-11-29 19:20:49 UTC+0000

Last accessed: 2020-11-29 19:20:49 UTC+0000

File Offset: 0x100, Data Offset: 0x0, Data Length: 0xa8

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Process: 848 explorer.exe

Cache type "URL " at 0x4746400

Record length: 0x180

Location: Visited: Findme@https://www.msn.com/en-in/?ocid=iehp

Last modified: 2020-11-29 19:21:23 UTC+0000

Last accessed: 2020-11-29 19:21:23 UTC+0000

File Offset: 0x180, Data Offset: 0x0, Data Length: 0xa0

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Process: 848 explorer.exe

Cache type "URL " at 0x4747000

Record length: 0x300

Location: Visited: Findme@https://www.google.com/sorry/index?continue=https://www.google.com/search%3Fhl%3Den-IN%26source%3Dhp%26q%3Dpython%26btnG%3DGoogle%2BSearch%26iflsig%3DAINFCbYAAAAAX8TAKTs2dioMnc7Esas-b2BwCskeM6Wr%26gbv%3D1&hl=en-IN&q=EgRnLA1BGMPkkv4FIhkA8aeDS7JPh8kiS-2IRvaL27FFFMs\_yzspMgFy

Last modified: 2020-11-29 19:20:11 UTC+0000

Last accessed: 2020-11-29 19:20:11 UTC+0000

File Offset: 0x300, Data Offset: 0x0, Data Length: 0x18c

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Process: 2060 FTK Imager.exe

Cache type "URL " at 0x3806000

Record length: 0x180

Location: http://www.bing.com/favicon.ico

Last modified: 2020-11-22 16:38:29 UTC+0000

Last accessed: 2020-11-29 19:18:21 UTC+0000

File Offset: 0x180, Data Offset: 0x88, Data Length: 0x98

File: favicon[1].ico

Data: HTTP/1.1 200 OK

Content-Length: 237

Content-Type: image/x-icon

X-Cache: TCP\_HIT

X-MSEdge-Ref: Ref A: D423F8DCD55946CFB4FBC872A8404DB8 Ref B: MAA02EDGE0315 Ref C: 2020-11-30T08:48:21Z

~U:findme

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Process: 2060 FTK Imager.exe

Cache type "URL " at 0x3806180

Record length: 0x180

Location: http://www.bing.com/favicon.ico

Last modified: 2020-11-22 16:38:29 UTC+0000

Last accessed: 2020-11-29 19:20:27 UTC+0000

File Offset: 0x180, Data Offset: 0x88, Data Length: 0x98

File: favicon[1].png

Data: HTTP/1.1 200 OK

Content-Length: 237

Content-Type: image/x-icon

X-Cache: TCP\_HIT

X-MSEdge-Ref: Ref A: D423F8DCD55946CFB4FBC872A8404DB8 Ref B: MAA02EDGE0315 Ref C: 2020-11-30T08:48:21Z

~U:findme

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Process: 2060 FTK Imager.exe

Cache type "URL " at 0x3807000

Record length: 0x280

Location: https://www.google.com/favicon.ico

Last modified: 2019-10-22 18:30:00 UTC+0000

Last accessed: 2020-11-29 19:18:25 UTC+0000

File Offset: 0x280, Data Offset: 0x8c, Data Length: 0x9c

File: favicon[1].ico

Data: HTTP/1.1 200 OK

Content-Type: image/x-icon

Cross-Origin-Resource-Policy: cross-origin

X-Content-Type-Options: nosniff

X-XSS-Protection: 0

Alt-Svc: h3-29=":443"; ma=2592000,h3-T051=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43"

Content-Length: 5430

~U:findme

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Process: 2060 FTK Imager.exe

Cache type "URL " at 0x3807280

Record length: 0x200

Location: https://ieonline.microsoft.com/favicon.ico

Last modified: 2020-11-25 15:45:41 UTC+0000

Last accessed: 2020-11-29 19:18:32 UTC+0000

File Offset: 0x200, Data Offset: 0x94, Data Length: 0xa4

File: favicon[1].ico

Data: HTTP/1.1 200 OK

Content-Length: 237

Content-Type: image/x-icon

Strict-Transport-Security: max-age=31536000; includeSubDomains; preload

X-MSEdge-Ref: Ref A: 90EB859642E444A5AF176D2A5600DB1F Ref B: MAA02EDGE0314 Ref C: 2020-11-30T08:48:32Z

~U:findme

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Process: 2060 FTK Imager.exe

Cache type "URL " at 0x3807480

Record length: 0x200

Location: https://ieonline.microsoft.com/favicon.ico

Last modified: 2020-11-25 15:45:41 UTC+0000

Last accessed: 2020-11-29 19:18:32 UTC+0000

File Offset: 0x200, Data Offset: 0x94, Data Length: 0xa4

File: favicon[1].png

Data: HTTP/1.1 200 OK

Content-Length: 237

Content-Type: image/x-icon

Strict-Transport-Security: max-age=31536000; includeSubDomains; preload

X-MSEdge-Ref: Ref A: 90EB859642E444A5AF176D2A5600DB1F Ref B: MAA02EDGE0314 Ref C: 2020-11-30T08:48:32Z

~U:findme

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Process: 2060 FTK Imager.exe

Cache type "URL " at 0x3825000

Record length: 0x100

Location: Visited: Findme@http://www.google.com

Last modified: 2020-11-29 19:17:15 UTC+0000

Last accessed: 2020-11-29 19:17:15 UTC+0000

File Offset: 0x100, Data Offset: 0x0, Data Length: 0x90

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Process: 2060 FTK Imager.exe

Cache type "URL " at 0x3825100

Record length: 0x100

Location: Visited: Findme@https://support.microsoft.com/internet-explorer

Last modified: 2020-11-29 19:18:17 UTC+0000

Last accessed: 2020-11-29 19:18:17 UTC+0000

File Offset: 0x100, Data Offset: 0x0, Data Length: 0xa8

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Process: 2060 FTK Imager.exe

Cache type "URL " at 0x3825200

Record length: 0x100

Location: Visited: Findme@http://google.com

Last modified: 2020-11-29 19:18:09 UTC+0000

Last accessed: 2020-11-29 19:18:09 UTC+0000

File Offset: 0x100, Data Offset: 0x0, Data Length: 0x8c

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Process: 2060 FTK Imager.exe

Cache type "URL " at 0x3825300

Record length: 0x100

Location: Visited: Findme@https://ieonline.microsoft.com/favicon.ico

Last modified: 2020-11-29 19:18:32 UTC+0000

Last accessed: 2020-11-29 19:18:32 UTC+0000

File Offset: 0x100, Data Offset: 0x0, Data Length: 0xa4

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Process: 2060 FTK Imager.exe

Cache type "URL " at 0x3825400

Record length: 0x100

Location: Visited: Findme@https://www.google.com/?gws\_rd=ssl

Last modified: 2020-11-29 19:23:22 UTC+0000

Last accessed: 2020-11-29 19:23:22 UTC+0000

File Offset: 0x100, Data Offset: 0x0, Data Length: 0x9c

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Process: 2060 FTK Imager.exe

Cache type "URL " at 0x3825500

Record length: 0x300

Location: Visited: Findme@https://www.google.com/sorry/index?continue=https://www.google.com/search%3Fhl%3Den-IN%26source%3Dhp%26q%3Dpython%26btnG%3DGoogle%2BSearch%26iflsig%3DAINFCbYAAAAAX8TAKTs2dioMnc7Esas-b2BwCskeM6Wr%26gbv%3D1&hl=en-IN&q=EgRnLA1BGMPkkv4FIhkA8aeDS7JPh8kiS-2IRvaL27FFFMs\_yzspMgFy

Last modified: 2020-11-29 19:20:11 UTC+0000

Last accessed: 2020-11-29 19:20:11 UTC+0000

File Offset: 0x300, Data Offset: 0x0, Data Length: 0x18c

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Process: 2060 FTK Imager.exe

Cache type "URL " at 0x3825800

Record length: 0x300

Location: Visited: Findme@https://www.google.com/sorry/index?continue=https://www.google.com/search%3Fhl%3Den-IN%26source%3Dhp%26q%3Dchrome%26iflsig%3DAINFCbYAAAAAX8TAKTs2dioMnc7Esas-b2BwCskeM6Wr%26gbv%3D1&hl=en-IN&q=EgRnLA1BGKDkkv4FIhkA8aeDS8PC1lDIX2rVDx\_27lZtROqyveSQMgFy

Last modified: 2020-11-29 19:19:45 UTC+0000

Last accessed: 2020-11-29 19:19:45 UTC+0000

File Offset: 0x300, Data Offset: 0x0, Data Length: 0x170

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Process: 2060 FTK Imager.exe

Cache type "URL " at 0x3825b00

Record length: 0x300

Location: Visited: Findme@https://www.google.com/sorry/index?continue=https://www.google.com/search%3Fhl%3Den-IN%26source%3Dhp%26q%3Dpython%26iflsig%3DAINFCbYAAAAAX8S\_2a-hxt1xgu0y32wpGuVlzhI1Qo5l%26gbv%3D1&hl=en-IN&q=EgRnLA1BGIPkkv4FIhkA8aeDS0lAzi8GNf2oAu2MfUXhHUou71SyMgFy

Last modified: 2020-11-29 19:19:51 UTC+0000

Last accessed: 2020-11-29 19:19:51 UTC+0000

File Offset: 0x300, Data Offset: 0x0, Data Length: 0x170

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Process: 2060 FTK Imager.exe

Cache type "URL " at 0x3825e00

Record length: 0x100

Location: Visited: Findme@https://www.msn.com/?ocid=iehp

Last modified: 2020-11-29 19:20:48 UTC+0000

Last accessed: 2020-11-29 19:20:48 UTC+0000

File Offset: 0x100, Data Offset: 0x0, Data Length: 0x98

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Process: 2060 FTK Imager.exe

Cache type "URL " at 0x3825f00

Record length: 0x100

Location: Visited: Findme@file:///C:/Py\_exmple/hello\_vit.py

Last modified: 2020-11-29 19:31:05 UTC+0000

Last accessed: 2020-11-29 19:31:05 UTC+0000

File Offset: 0x100, Data Offset: 0x0, Data Length: 0x9c

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Process: 2060 FTK Imager.exe

Cache type "URL " at 0x3826000

Record length: 0x300

Location: Visited: Findme@https://www.google.com/sorry/index?continue=https://www.google.com/search%3Fhl%3Den-IN%26source%3Dhp%26q%3Dpython%26btnG%3DGoogle%2BSearch%26iflsig%3DAINFCbYAAAAAX8TAKTs2dioMnc7Esas-b2BwCskeM6Wr%26gbv%3D1&hl=en-IN&q=EgRnLA1BGLjkkv4FIhkA8aeDS4I-Znd\_vF5gGp3vgEO7XDAdzSvhMgFy

Last modified: 2020-11-29 19:20:01 UTC+0000

Last accessed: 2020-11-29 19:20:01 UTC+0000

File Offset: 0x300, Data Offset: 0x0, Data Length: 0x18c

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Process: 2060 FTK Imager.exe

Cache type "URL " at 0x3826300

Record length: 0x100

Location: Visited: Findme@http://go.microsoft.com/fwlink/?LinkId=69157

Last modified: 2020-11-29 19:20:49 UTC+0000

Last accessed: 2020-11-29 19:20:49 UTC+0000

File Offset: 0x100, Data Offset: 0x0, Data Length: 0xa8

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Process: 2060 FTK Imager.exe

Cache type "URL " at 0x3826400

Record length: 0x180

Location: Visited: Findme@https://www.msn.com/en-in/?ocid=iehp

Last modified: 2020-11-29 19:21:23 UTC+0000

Last accessed: 2020-11-29 19:21:23 UTC+0000

File Offset: 0x180, Data Offset: 0x0, Data Length: 0xa0

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Process: 2060 FTK Imager.exe

Cache type "URL " at 0x3827000

Record length: 0x300

Location: Visited: Findme@https://www.google.com/sorry/index?continue=https://www.google.com/search%3Fhl%3Den-IN%26source%3Dhp%26q%3Dpython%26btnG%3DGoogle%2BSearch%26iflsig%3DAINFCbYAAAAAX8TAKTs2dioMnc7Esas-b2BwCskeM6Wr%26gbv%3D1&hl=en-IN&q=EgRnLA1BGMPkkv4FIhkA8aeDS7JPh8kiS-2IRvaL27FFFMs\_yzspMgFy

Last modified: 2020-11-29 19:20:11 UTC+0000

Last accessed: 2020-11-29 19:20:11 UTC+0000

File Offset: 0x300, Data Offset: 0x0, Data Length: 0x18c

remnux@remnux:~/Downloads$

remnux@remnux:~/Downloads$ **python ./volatality/volatility/vol.py -f ./memdump.mem --profile=Win7SP1x64 cmdscan**

Volatility Foundation Volatility Framework 2.6.1

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

CommandProcess: conhost.exe Pid: 3408

CommandHistory: 0x358b30 Application: cmd.exe Flags: Allocated, Reset

CommandCount: 3 LastAdded: 2 LastDisplayed: 2

FirstCommand: 0 CommandCountMax: 50

ProcessHandle: 0x60

Cmd #0 @ 0x357500: cd /

Cmd #1 @ 0x338a50: cd Py\_exmple

Cmd #2 @ 0x338a80: python hello\_vit.py

Cmd #15 @ 0x2f0158: 5

Cmd #16 @ 0x357c90: 5

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

CommandProcess: conhost.exe Pid: 1828

CommandHistory: 0x108b40 Application: cmd.exe Flags: Allocated, Reset

CommandCount: 1 LastAdded: 0 LastDisplayed: 0

FirstCommand: 0 CommandCountMax: 50

ProcessHandle: 0x60

Cmd #0 @ 0x1075c0: python

Cmd #15 @ 0xa0158:

Cmd #16 @ 0x107cb0:

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

CommandProcess: conhost.exe Pid: 1828

CommandHistory: 0x108e50 Application: python.exe Flags: Allocated, Reset

CommandCount: 1 LastAdded: 0 LastDisplayed: 0

FirstCommand: 0 CommandCountMax: 50

ProcessHandle: 0x88

Cmd #0 @ 0x105320: print"no one can find me"

remnux@remnux:~/Downloads$ **python ./volatality/volatility/vol.py -f ./memdump.mem --profile=Win7SP1x64 consoles**

Volatility Foundation Volatility Framework 2.6.1

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

ConsoleProcess: conhost.exe Pid: 3408

Console: 0xff3c6200 CommandHistorySize: 50

HistoryBufferCount: 2 HistoryBufferMax: 4

OriginalTitle: %SystemRoot%\system32\cmd.exe

Title: C:\Windows\system32\cmd.exe

AttachedProcess: cmd.exe Pid: 3760 Handle: 0x60

----

CommandHistory: 0x358e50 Application: python.exe Flags:

CommandCount: 0 LastAdded: -1 LastDisplayed: -1

FirstCommand: 0 CommandCountMax: 50

ProcessHandle: 0x0

----

CommandHistory: 0x358b30 Application: cmd.exe Flags: Allocated, Reset

CommandCount: 3 LastAdded: 2 LastDisplayed: 2

FirstCommand: 0 CommandCountMax: 50

ProcessHandle: 0x60

Cmd #0 at 0x357500: cd /

Cmd #1 at 0x338a50: cd Py\_exmple

Cmd #2 at 0x338a80: python hello\_vit.py

----

Screen 0x33b080 X:80 Y:300

Dump:

Microsoft Windows [Version 6.1.7600]

Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Findme>cd /

C:\>cd Py\_exmple

C:\Py\_exmple>python hello\_vit.py

VIT-AP University is now at Andhra

C:\Py\_exmple>

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

ConsoleProcess: conhost.exe Pid: 1828

Console: 0xff3c6200 CommandHistorySize: 50

HistoryBufferCount: 2 HistoryBufferMax: 4

OriginalTitle: %SystemRoot%\system32\cmd.exe

Title: C:\Windows\system32\cmd.exe - python

AttachedProcess: python.exe Pid: 3648 Handle: 0x88

AttachedProcess: cmd.exe Pid: 680 Handle: 0x60

----

CommandHistory: 0x108e50 Application: python.exe Flags: Allocated, Reset

CommandCount: 1 LastAdded: 0 LastDisplayed: 0

FirstCommand: 0 CommandCountMax: 50

ProcessHandle: 0x88

Cmd #0 at 0x105320: print"no one can find me"

----

CommandHistory: 0x108b40 Application: cmd.exe Flags: Allocated, Reset

CommandCount: 1 LastAdded: 0 LastDisplayed: 0

FirstCommand: 0 CommandCountMax: 50

ProcessHandle: 0x60

Cmd #0 at 0x1075c0: python

----

Screen 0xeb030 X:80 Y:300

Dump:

Microsoft Windows [Version 6.1.7600]

Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Findme>python

Python 2.7.18 (v2.7.18:8d21aa21f2, Apr 20 2020, 13:25:05) [MSC v.1500 64 bit (AM

D64)] on win32

Type "help", "copyright", "credits" or "license" for more information.

>>> print"no one can find me"

no one can find me

>>>

**remnux@remnux:~/Downloads$ python ./volatality/volatility/vol.py -f ./memdump.mem --profile=Win7SP1x64 clipboard**

Volatility Foundation Volatility Framework 2.6.1

Session WindowStation Format Handle Object Data

---------- ------------- ------------------ ------------------ ------------------ --------------------------------------------------

1 WinSta0 CF\_UNICODETEXT 0x8d028f 0xfffff900c1fc65b0 C:\Python27\Scripts

1 WinSta0 CF\_TEXT 0x10 ------------------

1 WinSta0 0x3301b1L 0x200000000000 ------------------

1 WinSta0 CF\_TEXT 0x1 ------------------

1 ------------- ------------------ 0x3301b1 0xfffff900c1a95ca0

**remnux@remnux:~/Downloads$ python ./volatality/volatility/vol.py -f ./memdump.mem --profile=Win7SP1x64 messagehooks**

Volatility Foundation Volatility Framework 2.6.1

Offset(V) Sess Desktop Thread Filter Flags Function Module

------------------ ------ -------------------- ------------------------------ -------------------- -------------------- ------------------ ------

0xfffff900c06011d0 0 WinSta0\Default <any> WH\_CALLWNDPROC HF\_GLOBAL 0x00000000000012d8 C:\Windows\system32\wls0wndh.dll

0xfffff900c06011d0 0 WinSta0\Default 1908 (spoolsv.exe 1052) WH\_CALLWNDPROC HF\_GLOBAL 0x00000000000012d8 C:\Windows\system32\wls0wndh.dll

0xfffff900c06011d0 0 WinSta0\Default 1892 (spoolsv.exe 1052) WH\_CALLWNDPROC HF\_GLOBAL 0x00000000000012d8 C:\Windows\system32\wls0wndh.dll

0xfffff900c06011d0 0 WinSta0\Default 1876 (spoolsv.exe 1052) WH\_CALLWNDPROC HF\_GLOBAL 0x00000000000012d8 C:\Windows\system32\wls0wndh.dll

0xfffff900c06011d0 0 WinSta0\Default 1076 (spoolsv.exe 1052) WH\_CALLWNDPROC HF\_GLOBAL 0x00000000000012d8 C:\Windows\system32\wls0wndh.dll

0xfffff900c06011d0 0 WinSta0\Default 1056 (spoolsv.exe 1052) WH\_CALLWNDPROC HF\_GLOBAL 0x00000000000012d8 C:\Windows\system32\wls0wndh.dll

0xfffff900c06011d0 0 WinSta0\Default 444 (csrss.exe 324) WH\_CALLWNDPROC HF\_GLOBAL 0x00000000000012d8 C:\Windows\system32\wls0wndh.dll

0xfffff900c06011d0 0 WinSta0\Default 440 (csrss.exe 324) WH\_CALLWNDPROC HF\_GLOBAL 0x00000000000012d8 C:\Windows\system32\wls0wndh.dll

0xfffff900c06011d0 0 WinSta0\Default 376 (wininit.exe 372) WH\_CALLWNDPROC HF\_GLOBAL 0x00000000000012d8 C:\Windows\system32\wls0wndh.dll

**remnux@remnux:~/Downloads$ python ./volatality/volatility/vol.py -f ./memdump.mem --profile=Win7SP1x64 sessions**

Volatility Foundation Volatility Framework 2.6.1

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Session(V): fffff88002cf4000 ID: 0 Processes: 30

PagedPoolStart: fffff900c0000000 PagedPoolEnd fffff920bfffffff

Process: 324 csrss.exe 2020-11-29 19:09:07 UTC+0000

Process: 372 wininit.exe 2020-11-29 19:09:07 UTC+0000

Process: 464 services.exe 2020-11-29 19:09:08 UTC+0000

Process: 476 lsass.exe 2020-11-29 19:09:08 UTC+0000

Process: 484 lsm.exe 2020-11-29 19:09:08 UTC+0000

Process: 588 svchost.exe 2020-11-29 19:09:08 UTC+0000

Process: 668 svchost.exe 2020-11-29 19:09:09 UTC+0000

Process: 760 svchost.exe 2020-11-29 19:09:09 UTC+0000

Process: 800 svchost.exe 2020-11-29 19:09:09 UTC+0000

Process: 828 svchost.exe 2020-11-29 19:09:09 UTC+0000

Process: 912 audiodg.exe 2020-11-29 19:09:09 UTC+0000

Process: 984 svchost.exe 2020-11-29 19:09:09 UTC+0000

Process: 340 svchost.exe 2020-11-29 19:09:09 UTC+0000

Process: 1052 spoolsv.exe 2020-11-29 19:09:10 UTC+0000

Process: 1080 svchost.exe 2020-11-29 19:09:10 UTC+0000

Process: 1196 svchost.exe 2020-11-29 19:09:10 UTC+0000

Process: 1696 svchost.exe 2020-11-29 19:09:11 UTC+0000

Process: 2576 SearchIndexer. 2020-11-29 19:10:21 UTC+0000

Process: 2308 wmpnetwk.exe 2020-11-29 19:10:37 UTC+0000

Process: 2792 mscorsvw.exe 2020-11-29 19:11:11 UTC+0000

Process: 2832 mscorsvw.exe 2020-11-29 19:11:11 UTC+0000

Process: 2816 svchost.exe 2020-11-29 19:11:12 UTC+0000

Process: 2292 msiexec.exe 2020-11-29 19:16:09 UTC+0000

Process: 1992 WUDFHost.exe 2020-11-29 19:21:26 UTC+0000

Process: 3952 TrustedInstall 2020-11-29 19:27:44 UTC+0000

Process: 796 taskeng.exe 2020-11-29 19:33:45 UTC+0000

Process: 3592 GoogleUpdate.e 2020-11-29 19:33:45 UTC+0000

Process: 1868 GoogleCrashHan 2020-11-29 19:33:45 UTC+0000

Process: 3008 GoogleCrashHan 2020-11-29 19:33:45 UTC+0000

Process: 3356 MpCmdRun.exe 2020-11-29 19:37:02 UTC+0000

Image: 0xfffffa8005116560, Address fffff96000060000, Name: win32k.sys

Image: 0xfffffa800583d300, Address fffff96000560000, Name: dxg.sys

Image: 0xfffffa8003d12140, Address fffff96000630000, Name: TSDDD.dll

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Session(V): fffff88003c13000 ID: 1 Processes: 21

PagedPoolStart: fffff900c0000000 PagedPoolEnd fffff920bfffffff

Process: 384 csrss.exe 2020-11-29 19:09:07 UTC+0000

Process: 420 winlogon.exe 2020-11-29 19:09:08 UTC+0000

Process: 1820 taskhost.exe 2020-11-29 19:09:11 UTC+0000

Process: 296 dwm.exe 2020-11-29 19:09:37 UTC+0000

Process: 848 explorer.exe 2020-11-29 19:09:37 UTC+0000

Process: 2252 regsvr32.exe 2020-11-29 19:10:10 UTC+0000

Process: 1632 msiexec.exe 2020-11-29 19:16:09 UTC+0000

Process: 1664 chrome.exe 2020-11-29 19:23:18 UTC+0000

Process: 1116 chrome.exe 2020-11-29 19:23:18 UTC+0000

Process: 1424 chrome.exe 2020-11-29 19:23:19 UTC+0000

Process: 2660 chrome.exe 2020-11-29 19:23:19 UTC+0000

Process: 3360 chrome.exe 2020-11-29 19:23:20 UTC+0000

Process: 2496 chrome.exe 2020-11-29 19:25:01 UTC+0000

Process: 536 chrome.exe 2020-11-29 19:25:02 UTC+0000

Process: 2152 msiexec.exe 2020-11-29 19:26:52 UTC+0000

Process: 3760 cmd.exe 2020-11-29 19:29:48 UTC+0000

Process: 3408 conhost.exe 2020-11-29 19:29:48 UTC+0000

Process: 680 cmd.exe 2020-11-29 19:32:27 UTC+0000

Process: 1828 conhost.exe 2020-11-29 19:32:27 UTC+0000

Process: 3648 python.exe 2020-11-29 19:34:46 UTC+0000

Process: 2060 FTK Imager.exe 2020-11-29 19:35:07 UTC+0000

Image: 0xfffffa800583cfc0, Address fffff96000060000, Name: win32k.sys

Image: 0xfffffa80058df230, Address fffff96000560000, Name: dxg.sys

Image: 0xfffffa80058e5a80, Address fffff960008e0000, Name: framebuf.dll

**remnux@remnux:~/Downloads$ python ./volatality/volatility/vol.py -f ./memdump.mem --profile=Win7SP1x64 hashdump**

Volatility Foundation Volatility Framework 2.6.1

Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

Findme:1000:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

**LAB Exercise 1/12/2020:**

remnux@remnux:~/Downloads$ python ./volatality/volatility/vol.py -f ./0zapftis.vmem imageinfo

Volatility Foundation Volatility Framework 2.6.1

INFO : volatility.debug : Determining profile based on KDBG search...

Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)

AS Layer1 : IA32PagedMemoryPae (Kernel AS)

AS Layer2 : FileAddressSpace (/home/remnux/Downloads/0zapftis.vmem)

PAE type : PAE

DTB : 0x319000L

KDBG : 0x80544ce0L

Number of Processors : 1

Image Type (Service Pack) : 2

KPCR for CPU 0 : 0xffdff000L

KUSER\_SHARED\_DATA : 0xffdf0000L

Image date and time : 2011-10-10 17:06:54 UTC+0000

Image local date and time : 2011-10-10 13:06:54 -0400