Report
Threat Hunting

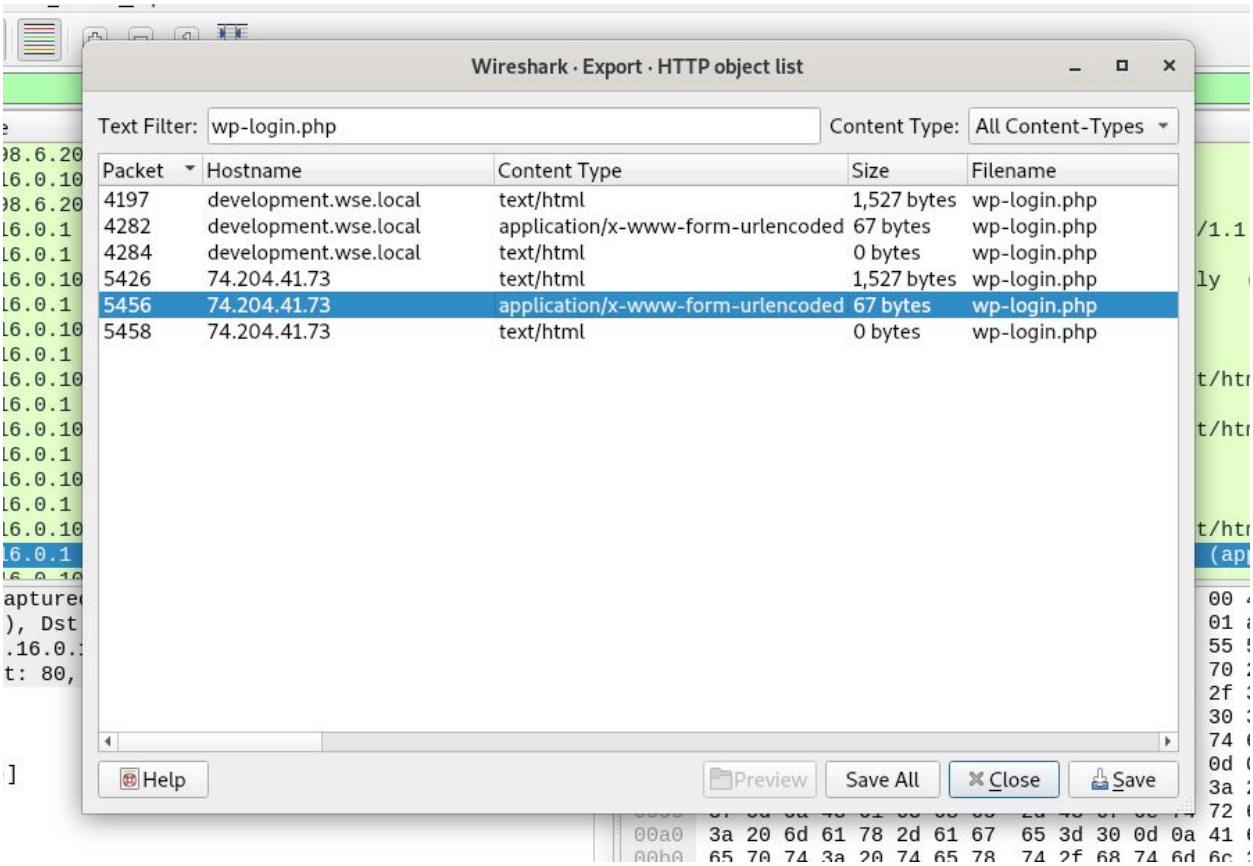
Scenario
Everyone has heard about targeted attacks. Detecting this can be a challenge, and responding to it can be even more challenging. This scenario will test your network and host-based analysis skills as a social analyst to find out who, what, where, when, and how this incident occurred. There's definitely something for all skill levels and the only thing you'll need to complete this challenge

Use Tools :

- Volatility
- Wireshark
- Networkminer
- Brimsecurity

1. Analyst PCAP: Development.wse.local is a critical asset for the Wayne and Stark Enterprises, where the company stores new top-secret designs on weapons. Jon Smith has access to the website and we believe it may have been compromised, according to the IDS alert we received earlier today. First, determine the Public IP Address of the webserver?

From the HTTP traffic, I've noticed that the website is made using WordPress.



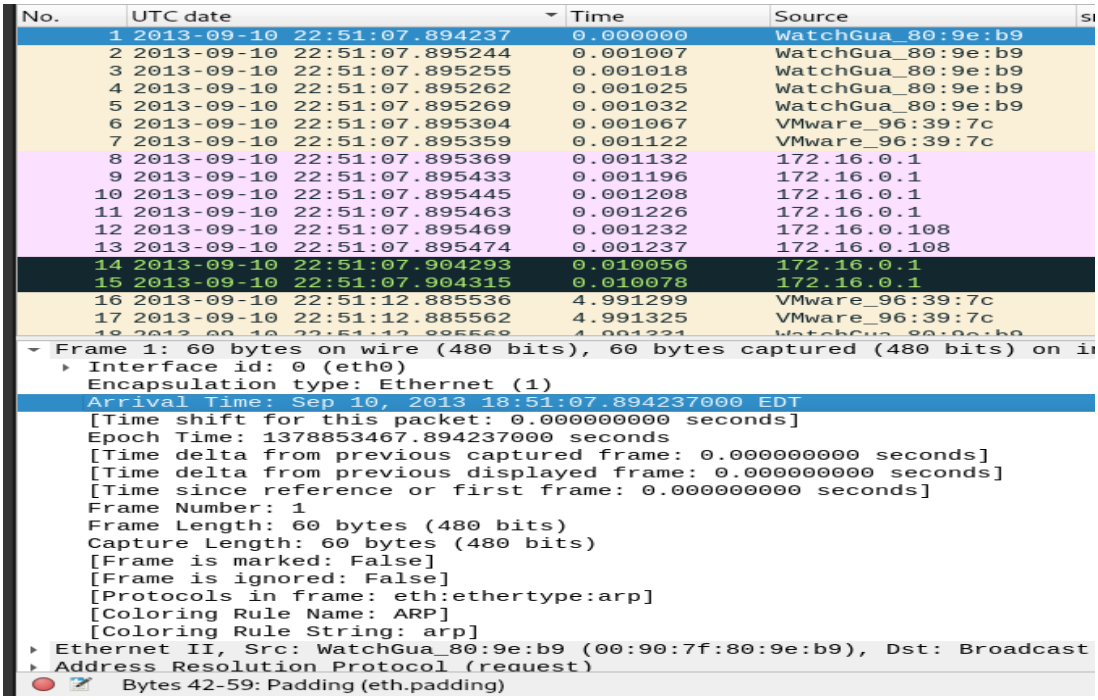
One way to access the WordPress dashboard is to add wp-login.php at the end of your site URL.
I checked the HTTP object list and entered wp-login.php from the Text Filter field. The image below shows the Public IP address of the web server under Hostname.

Navigate to File > Export Objects > HTTP to view the HTTP Object list.

Public IP Address of the webserver **: 74.204.41.73**

2. Analyst PCAP: Alright, now we need you to determine a starting point for the timeline that will be useful in mapping out the incident. Please determine the arrival time of frame 1 in the "GrrCON.pcapng" evidence file.

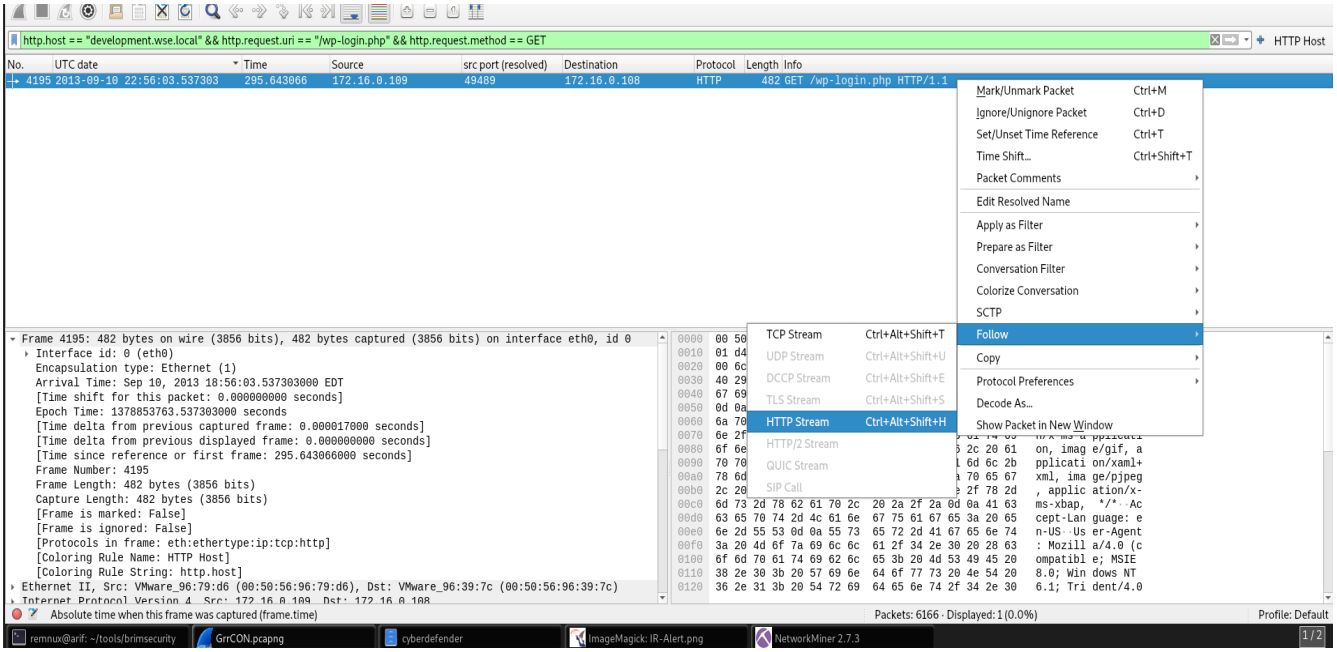
I used the filter below to sort the timestamp by ascending.



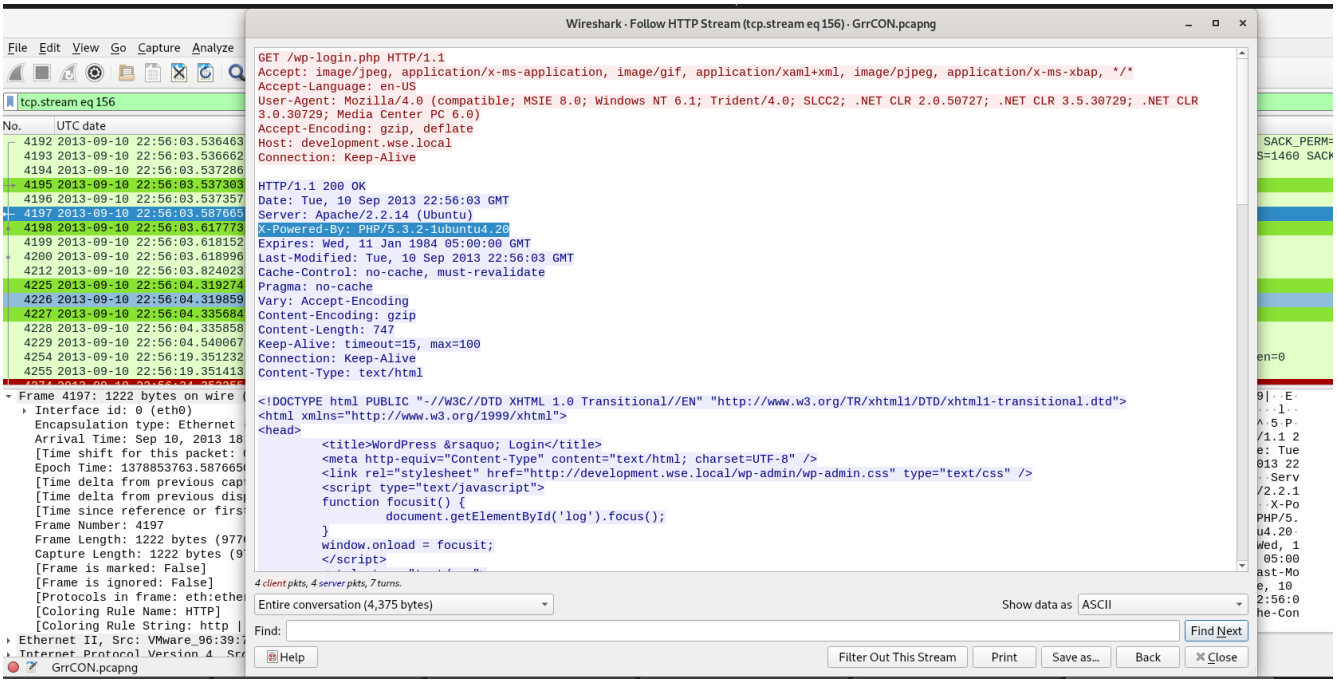
In Wireshark, check the first packet and set the time format into UTC.
22:51:07 UTC

3. Analyst PCAP: What version number of PHP is the development.wse.local server running?
The filter below will display the HTTP GET request from the host development.wse.local with URI /wp-login.php. Then I used the Follow HTTP Stream option to view the HTTP header.

Wireshark Search
http.host == "development.wse.local" && http.request.uri == "/wp-login.php" && http.request.method == GET

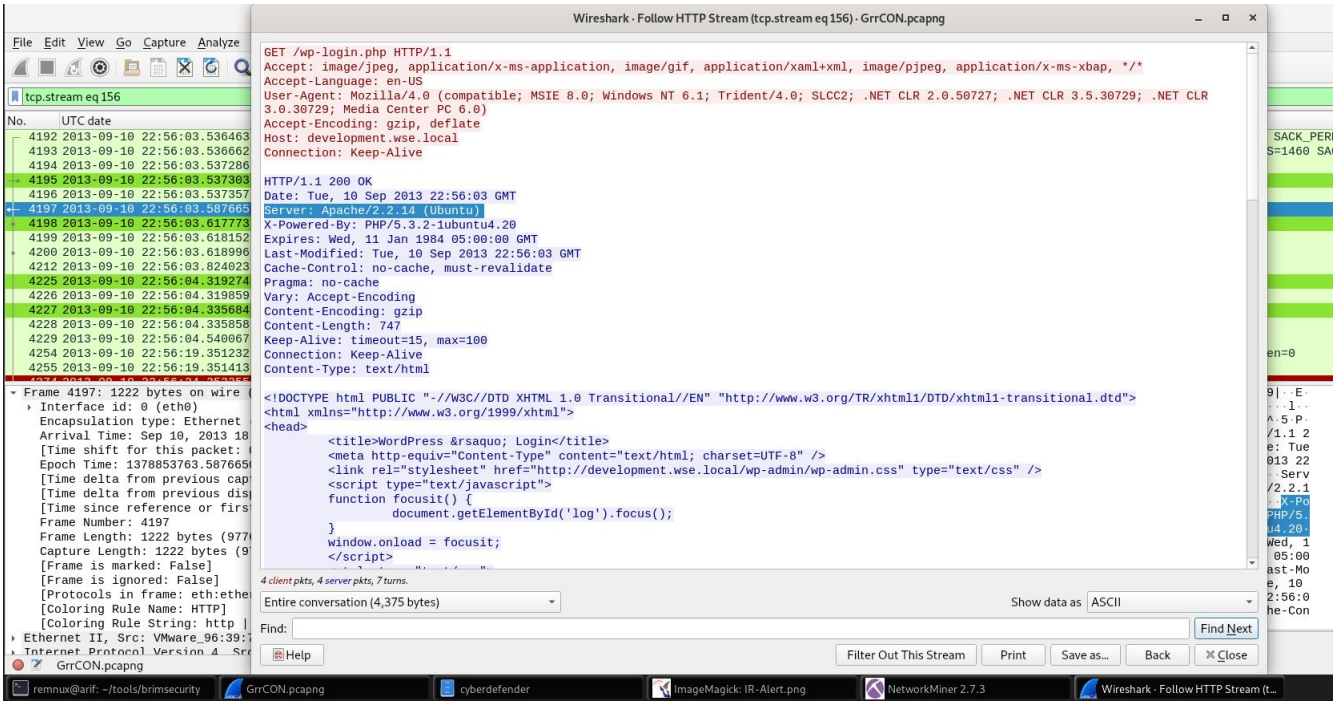


Right-click on the packet, then select Follow > HTTP Stream.
X-Powered-By is the HTTP header field that specifies the technology and version that supports the web application.



version number of PHP **: 5.3.2**

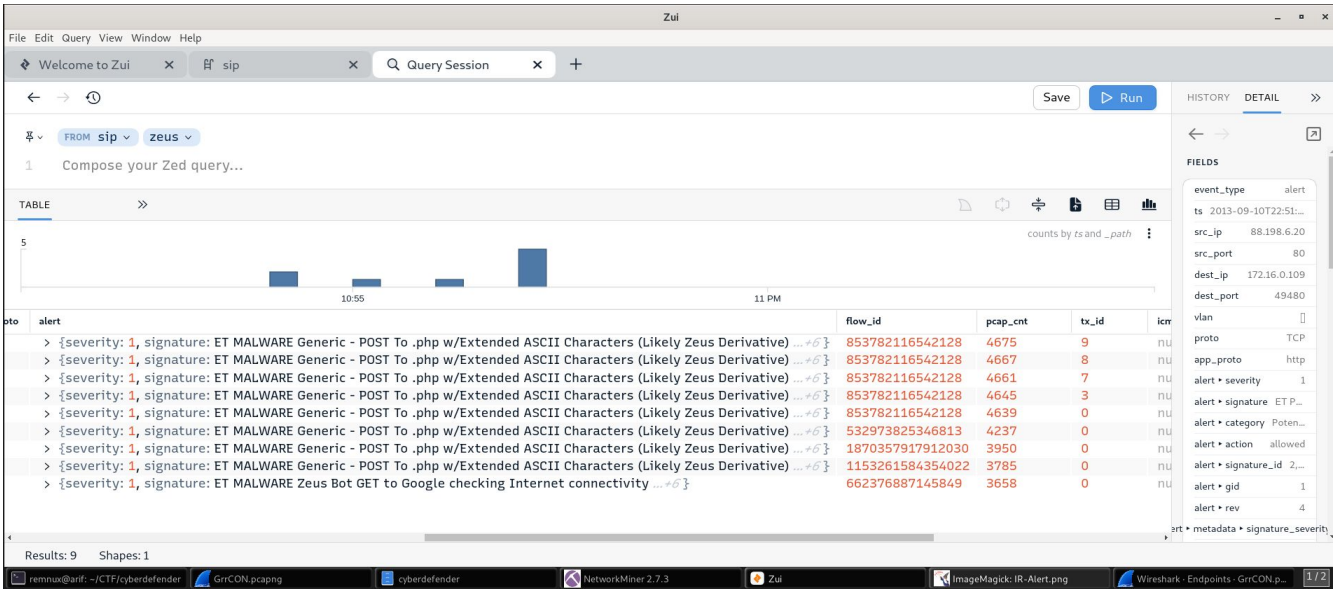
4. Analyst PCAP: What version number of Apache is the development.wse.local web server using?
The same process from Q.3.



The version of Apache the web server is using **: 2.2.14**

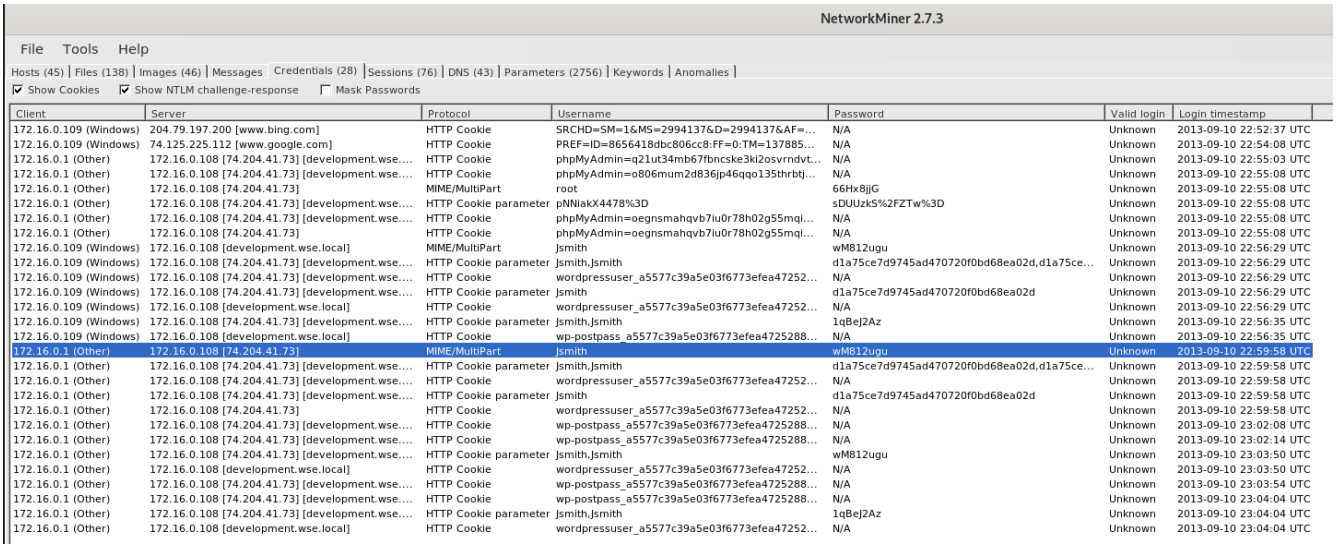
The Server field specifies the software and version used.

5. IR: What is the common name of the malware reported by the IDS alert provided?
I identified the malware name from the URL provided under References.



Malware name **: zeus**

6. Analyst PCAP: Please identify the Gateway IP address of the LAN because the infrastructure team reported a potential problem with the IDS server that could have corrupted the PCAP
I checked all the IPv4 addresses by navigating to Statistics > Endpoints > IPv4 in Wireshark. The .1 IP address is commonly used for Gateway IP address.

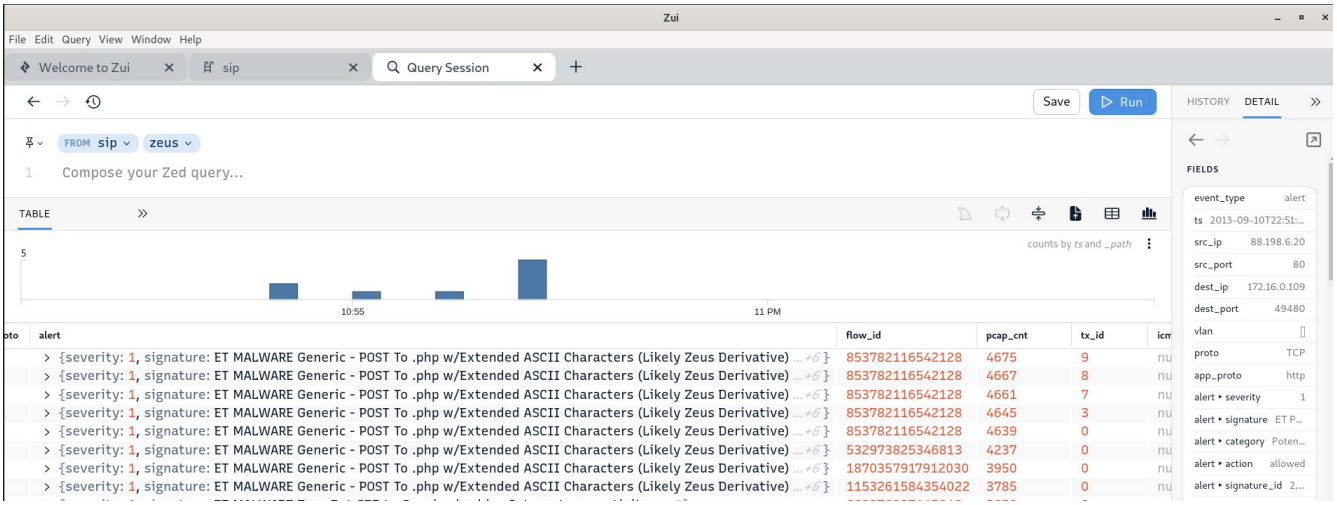


Client	Server	Protocol	Username	Password	Valid login	Login timestamp
172.16.0.109 (Windows)	204.79.197.200 [www.bing.com]	HTTP Cookie	SRCHD=SM=1&MS=2994137&D=2994137&AF=...	N/A	Unknown	2013-09-10 22:52:37 UTC
172.16.0.109 (Windows)	74.125.225.112 [www.google.com]	HTTP Cookie	PREF=ID=8656418dbc806cc8:FF=0:TM=137885...	N/A	Unknown	2013-09-10 22:54:08 UTC
172.16.0.1 (Other)	172.16.0.108 [74.204.41.73] [development.wse....	HTTP Cookie	phpMyAdmin=q21ut34mb67fbncske3ki2osvrndvt...	N/A	Unknown	2013-09-10 22:55:03 UTC
172.16.0.1 (Other)	172.16.0.108 [74.204.41.73] [development.wse....	HTTP Cookie	phpMyAdmin=o806mum2d836jp46qqo135thrbtj...	N/A	Unknown	2013-09-10 22:55:08 UTC
172.16.0.1 (Other)	172.16.0.108 [74.204.41.73]	MIME/MultiPart	root	66Hx8jjG	Unknown	2013-09-10 22:55:08 UTC
172.16.0.1 (Other)	172.16.0.108 [74.204.41.73] [development.wse....	HTTP Cookie parameter	pNNiakX4478%3D	sDUUzkS%2FZTw%3D	Unknown	2013-09-10 22:55:08 UTC
172.16.0.1 (Other)	172.16.0.108 [74.204.41.73] [development.wse....	HTTP Cookie	phpMyAdmin=oegnsmahqvb7iu0r78h02g55mqi...	N/A	Unknown	2013-09-10 22:55:08 UTC
172.16.0.1 (Other)	172.16.0.108 [74.204.41.73]	HTTP Cookie	phpMyAdmin=oegnsmahqvb7iu0r78h02g55mqi...	N/A	Unknown	2013-09-10 22:55:08 UTC
172.16.0.109 (Windows)	172.16.0.108 [development.wse.local]	MIME/MultiPart	Jsmith	wM812ugu	Unknown	2013-09-10 22:56:29 UTC
172.16.0.109 (Windows)	172.16.0.108 [74.204.41.73] [development.wse....	HTTP Cookie parameter	Jsmith,Jsmith	d1a75ce7d9745ad470720f0bd68ea02d,d1a75ce...	Unknown	2013-09-10 22:56:29 UTC
172.16.0.109 (Windows)	172.16.0.108 [74.204.41.73] [development.wse....	HTTP Cookie	wordpressuser_a5577c39a5e03f6773efea47252...	N/A	Unknown	2013-09-10 22:56:29 UTC
172.16.0.109 (Windows)	172.16.0.108 [74.204.41.73] [development.wse....	HTTP Cookie parameter	Jsmith	d1a75ce7d9745ad470720f0bd68ea02d	Unknown	2013-09-10 22:56:29 UTC
172.16.0.109 (Windows)	172.16.0.108 [development.wse.local]	HTTP Cookie	wordpressuser_a5577c39a5e03f6773efea47252...	N/A	Unknown	2013-09-10 22:56:29 UTC
172.16.0.109 (Windows)	172.16.0.108 [74.204.41.73] [development.wse....	HTTP Cookie parameter	Jsmith,Jsmith	1qBeJ2Az	Unknown	2013-09-10 22:56:35 UTC
172.16.0.109 (Windows)	172.16.0.108 [development.wse.local]	HTTP Cookie	wp-postpass_a5577c39a5e03f6773efea4725288...	N/A	Unknown	2013-09-10 22:56:35 UTC
172.16.0.1 (Other)	172.16.0.108 [74.204.41.73]	MIME/MultiPart	Jsmith	wM812ugu	Unknown	2013-09-10 22:59:58 UTC
172.16.0.1 (Other)	172.16.0.108 [74.204.41.73] [development.wse....	HTTP Cookie parameter	Jsmith,Jsmith	d1a75ce7d9745ad470720f0bd68ea02d,d1a75ce...	Unknown	2013-09-10 22:59:58 UTC
172.16.0.1 (Other)	172.16.0.108 [74.204.41.73] [development.wse....	HTTP Cookie	wordpressuser_a5577c39a5e03f6773efea47252...	N/A	Unknown	2013-09-10 22:59:58 UTC
172.16.0.1 (Other)	172.16.0.108 [74.204.41.73] [development.wse....	HTTP Cookie parameter	Jsmith	d1a75ce7d9745ad470720f0bd68ea02d	Unknown	2013-09-10 22:59:58 UTC
172.16.0.1 (Other)	172.16.0.108 [74.204.41.73]	HTTP Cookie	wordpressuser_a5577c39a5e03f6773efea47252...	N/A	Unknown	2013-09-10 22:59:58 UTC
172.16.0.1 (Other)	172.16.0.108 [74.204.41.73] [development.wse....	HTTP Cookie	wp-postpass_a5577c39a5e03f6773efea4725288...	N/A	Unknown	2013-09-10 23:02:08 UTC
172.16.0.1 (Other)	172.16.0.108 [74.204.41.73] [development.wse....	HTTP Cookie	wp-postpass_a5577c39a5e03f6773efea4725288...	N/A	Unknown	2013-09-10 23:02:14 UTC
172.16.0.1 (Other)	172.16.0.108 [74.204.41.73] [development.wse....	HTTP Cookie parameter	Jsmith,Jsmith	wM812ugu	Unknown	2013-09-10 23:03:50 UTC
172.16.0.1 (Other)	172.16.0.108 [development.wse.local]	HTTP Cookie	wordpressuser_a5577c39a5e03f6773efea47252...	N/A	Unknown	2013-09-10 23:03:50 UTC
172.16.0.1 (Other)	172.16.0.108 [74.204.41.73] [development.wse....	HTTP Cookie	wp-postpass_a5577c39a5e03f6773efea4725288...	N/A	Unknown	2013-09-10 23:03:54 UTC
172.16.0.1 (Other)	172.16.0.108 [74.204.41.73] [development.wse....	HTTP Cookie	wp-postpass_a5577c39a5e03f6773efea4725288...	N/A	Unknown	2013-09-10 23:04:04 UTC
172.16.0.1 (Other)	172.16.0.108 [74.204.41.73] [development.wse....	HTTP Cookie parameter	Jsmith,Jsmith	1qBeJ2Az	Unknown	2013-09-10 23:04:04 UTC
172.16.0.1 (Other)	172.16.0.108 [development.wse.local]	HTTP Cookie	wordpressuser_a5577c39a5e03f6773efea47252...	N/A	Unknown	2013-09-10 23:04:04 UTC

IP Gateway LAN **: 172.16.0.1**

You can also find the gateway IP address by analyzing the ARP traffic.

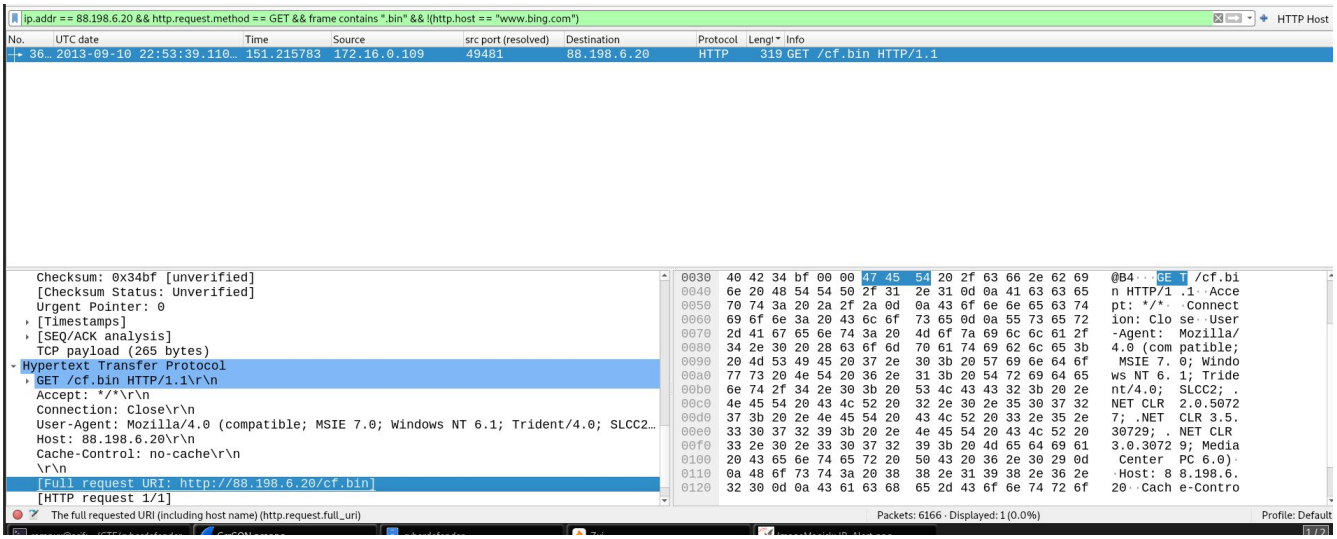
8. Analyst PCAP: It's critical to the infrastructure team to identify the Zeus Bot CNC server IP address so they can block communication in the firewall as soon as possible. Please provide the IP address?
The signature ET MALWARE Zbot POST Request to C2 in Suricata shows the Zeus CNC server IP address.
Suricata Alerts by Category > Malware Command and Control Activity Detected > Pivot to logs.

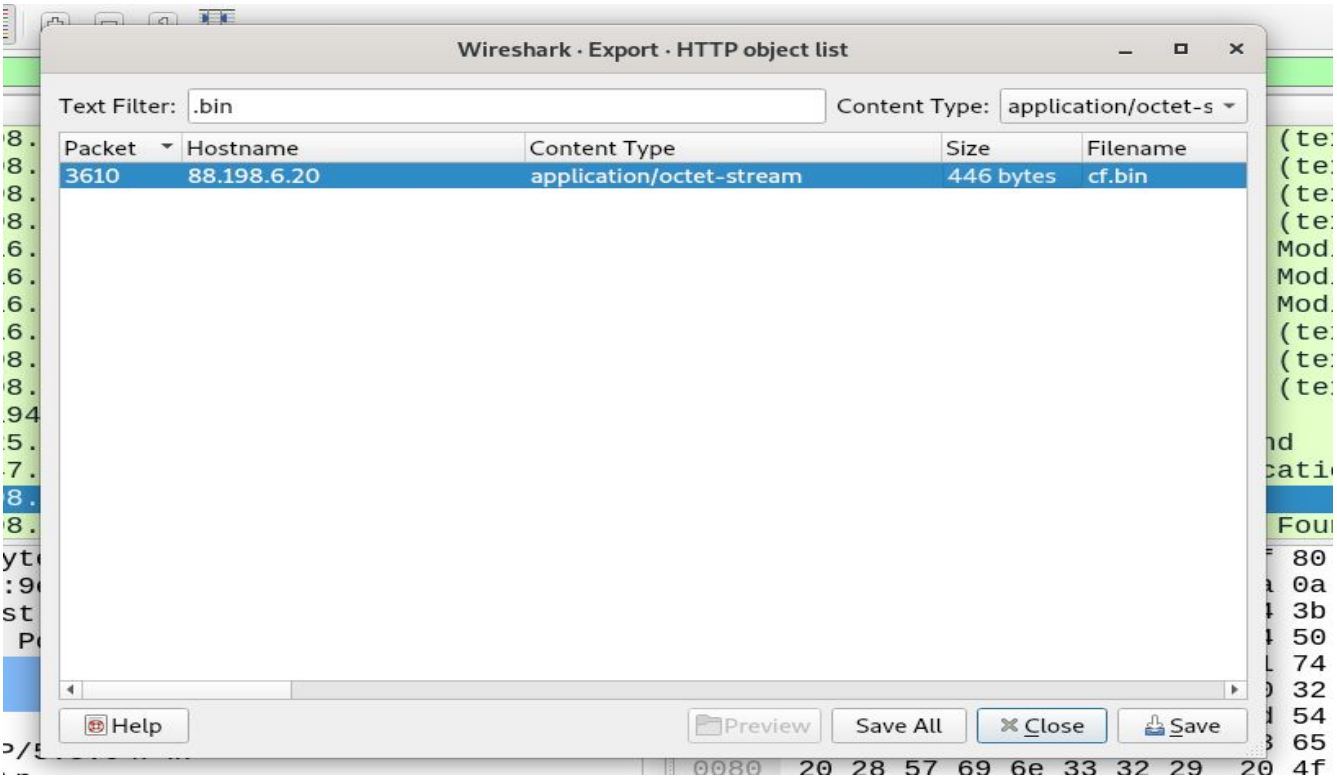


Zeus Bot CNC server IP address **: 88.198.6.20**

9. Analyst PCAP: The infrastructure team also requests that you identify the filename of the ".bin" configuration file that the Zeus bot downloaded right after the infection. Please provide the file name?
I found the filename by navigating to File > Export Objects > HTTP, filtering the results to only display .bin files, and then selecting Content-Type: as application/octet-stream.

Or use the filter below Wireshark.
ip.addr == 88.198.6.20 && http.request.method == GET && frame contains ".bin" && !(http.host == "www.bing.com")



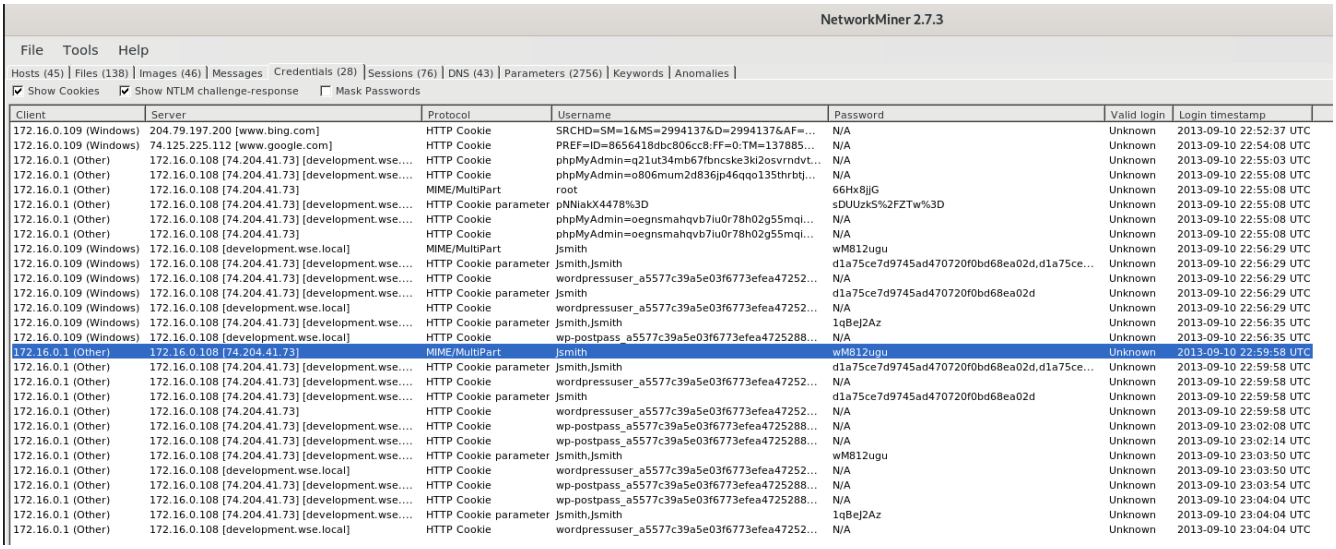


which the Zeus bot downloads the file **: cf.bin**

10. Analyst PCAP: No other users accessed the development.wse.local WordPress site during the timeline of the incident and the reports indicate that an account successfully logged in from the external interface. Please provide the password they used to log in to the WordPress page around 6:59 PM EST?
I converted first the GrrCON.pcapng into a .pcap since I'm using a free version of NetworkMiner — no need to convert if you are using the NetworMiner Professional.
To convert into .pcap, open the file using Wireshark, then go to File > Save As > Choose Wireshark/tcpdump … — pcap as type > then click Save.

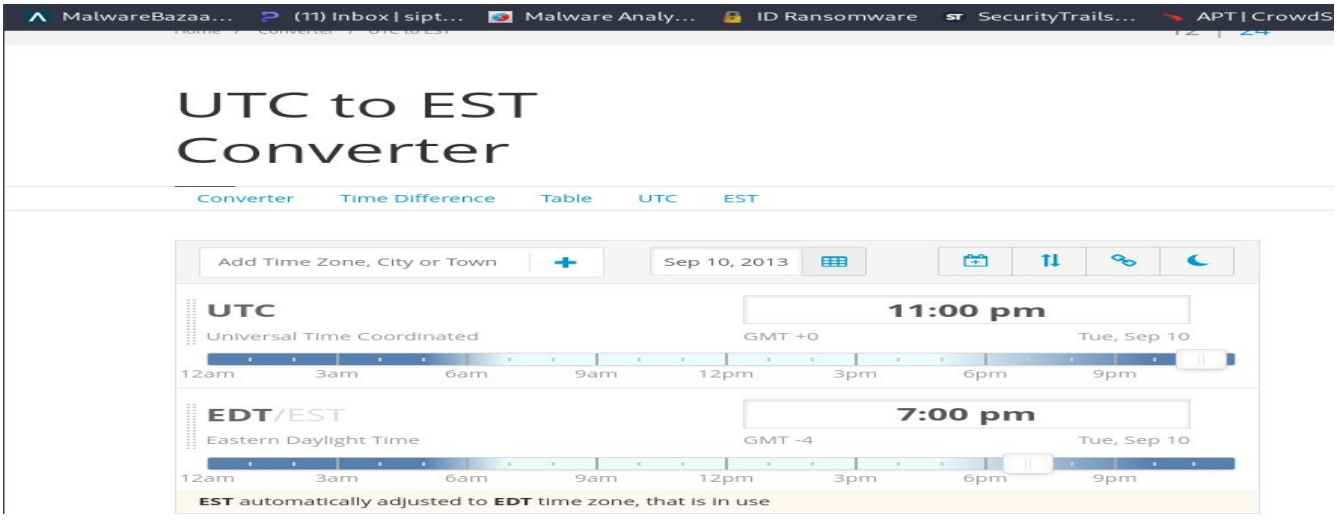
Open the .pcap file using NeworkMiner, click the Credentials tab, then uncheck Show Cookies.

the password they used to log in to the WordPress page at around 6:59pm EST **: wM812ugu**



Client	Server	Protocol	Username	Password	Valid login	Login timestamp
172.16.0.109 (Windows)	204.79.197.200 [www.bing.com]	HTTP Cookie	SRCHD=SM=1&MS=2994137&D=2994137&AF=...	N/A	Unknown	2013-09-10 22:52:37 UTC
172.16.0.109 (Windows)	74.125.225.112 [www.google.com]	HTTP Cookie	PREF=ID=8656418dbc806cc8:FF=0:TM=137885...	N/A	Unknown	2013-09-10 22:54:08 UTC
172.16.0.1 (Other)	172.16.0.108 [74.204.41.73] [development.wse....	HTTP Cookie	phpMyAdmin=q21ut34mb67fbncske3ki2osvrndvt...	N/A	Unknown	2013-09-10 22:55:03 UTC
172.16.0.1 (Other)	172.16.0.108 [74.204.41.73] [development.wse....	HTTP Cookie	phpMyAdmin=o806mum2d836jp46qqo135thrbtj...	N/A	Unknown	2013-09-10 22:55:08 UTC
172.16.0.1 (Other)	172.16.0.108 [74.204.41.73]	MIME/MultiPart	root	66Hx8jjG	Unknown	2013-09-10 22:55:08 UTC
172.16.0.1 (Other)	172.16.0.108 [74.204.41.73] [development.wse....	HTTP Cookie parameter	pNNiakX4478%3D	sDUUzkS%2FZTw%3D	Unknown	2013-09-10 22:55:08 UTC
172.16.0.1 (Other)	172.16.0.108 [74.204.41.73] [development.wse....	HTTP Cookie	phpMyAdmin=oegnsmahqvb7iu0r78h02g55mqi...	N/A	Unknown	2013-09-10 22:55:08 UTC
172.16.0.1 (Other)	172.16.0.108 [74.204.41.73]	HTTP Cookie	phpMyAdmin=oegnsmahqvb7iu0r78h02g55mqi...	N/A	Unknown	2013-09-10 22:55:08 UTC
172.16.0.109 (Windows)	172.16.0.108 [development.wse.local]	MIME/MultiPart	Jsmith	wM812ugu	Unknown	2013-09-10 22:56:29 UTC
172.16.0.109 (Windows)	172.16.0.108 [74.204.41.73] [development.wse....	HTTP Cookie parameter	Jsmith,Jsmith	d1a75ce7d9745ad470720f0bd68ea02d,d1a75ce...	Unknown	2013-09-10 22:56:29 UTC
172.16.0.109 (Windows)	172.16.0.108 [74.204.41.73] [development.wse....	HTTP Cookie	wordpressuser_a5577c39a5e03f6773efea47252...	N/A	Unknown	2013-09-10 22:56:29 UTC
172.16.0.109 (Windows)	172.16.0.108 [74.204.41.73] [development.wse....	HTTP Cookie parameter	Jsmith	d1a75ce7d9745ad470720f0bd68ea02d	Unknown	2013-09-10 22:56:29 UTC
172.16.0.109 (Windows)	172.16.0.108 [development.wse.local]	HTTP Cookie	wordpressuser_a5577c39a5e03f6773efea47252...	N/A	Unknown	2013-09-10 22:56:29 UTC
172.16.0.109 (Windows)	172.16.0.108 [74.204.41.73] [development.wse....	HTTP Cookie parameter	Jsmith,Jsmith	1qBeJ2Az	Unknown	2013-09-10 22:56:35 UTC
172.16.0.109 (Windows)	172.16.0.108 [development.wse.local]	HTTP Cookie	wp-postpass_a5577c39a5e03f6773efea4725288...	N/A	Unknown	2013-09-10 22:56:35 UTC
172.16.0.1 (Other)	172.16.0.108 [74.204.41.73]	MIME/MultiPart	Jsmith	wM812ugu	Unknown	2013-09-10 22:59:58 UTC
172.16.0.1 (Other)	172.16.0.108 [74.204.41.73] [development.wse....	HTTP Cookie parameter	Jsmith,Jsmith	d1a75ce7d9745ad470720f0bd68ea02d,d1a75ce...	Unknown	2013-09-10 22:59:58 UTC
172.16.0.1 (Other)	172.16.0.108 [74.204.41.73] [development.wse....	HTTP Cookie	wordpressuser_a5577c39a5e03f6773efea47252...	N/A	Unknown	2013-09-10 22:59:58 UTC
172.16.0.1 (Other)	172.16.0.108 [74.204.41.73] [development.wse....	HTTP Cookie parameter	Jsmith	d1a75ce7d9745ad470720f0bd68ea02d	Unknown	2013-09-10 22:59:58 UTC
172.16.0.1 (Other)	172.16.0.108 [74.204.41.73]	HTTP Cookie	wordpressuser_a5577c39a5e03f6773efea47252...	N/A	Unknown	2013-09-10 22:59:58 UTC
172.16.0.1 (Other)	172.16.0.108 [74.204.41.73] [development.wse....	HTTP Cookie	wp-postpass_a5577c39a5e03f6773efea4725288...	N/A	Unknown	2013-09-10 23:02:08 UTC
172.16.0.1 (Other)	172.16.0.108 [74.204.41.73] [development.wse....	HTTP Cookie	wp-postpass_a5577c39a5e03f6773efea4725288...	N/A	Unknown	2013-09-10 23:02:14 UTC
172.16.0.1 (Other)	172.16.0.108 [74.204.41.73] [development.wse....	HTTP Cookie parameter	Jsmith,Jsmith	wM812ugu	Unknown	2013-09-10 23:03:50 UTC
172.16.0.1 (Other)	172.16.0.108 [development.wse.local]	HTTP Cookie	wordpressuser_a5577c39a5e03f6773efea47252...	N/A	Unknown	2013-09-10 23:03:50 UTC
172.16.0.1 (Other)	172.16.0.108 [74.204.41.73] [development.wse....	HTTP Cookie	wp-postpass_a5577c39a5e03f6773efea4725288...	N/A	Unknown	2013-09-10 23:03:54 UTC
172.16.0.1 (Other)	172.16.0.108 [74.204.41.73] [development.wse....	HTTP Cookie	wp-postpass_a5577c39a5e03f6773efea4725288...	N/A	Unknown	2013-09-10 23:04:04 UTC
172.16.0.1 (Other)	172.16.0.108 [74.204.41.73] [development.wse....	HTTP Cookie parameter	Jsmith,Jsmith	1qBeJ2Az	Unknown	2013-09-10 23:04:04 UTC
172.16.0.1 (Other)	172.16.0.108 [development.wse.local]	HTTP Cookie	wordpressuser_a5577c39a5e03f6773efea47252...	N/A	Unknown	2013-09-10 23:04:04 UTC

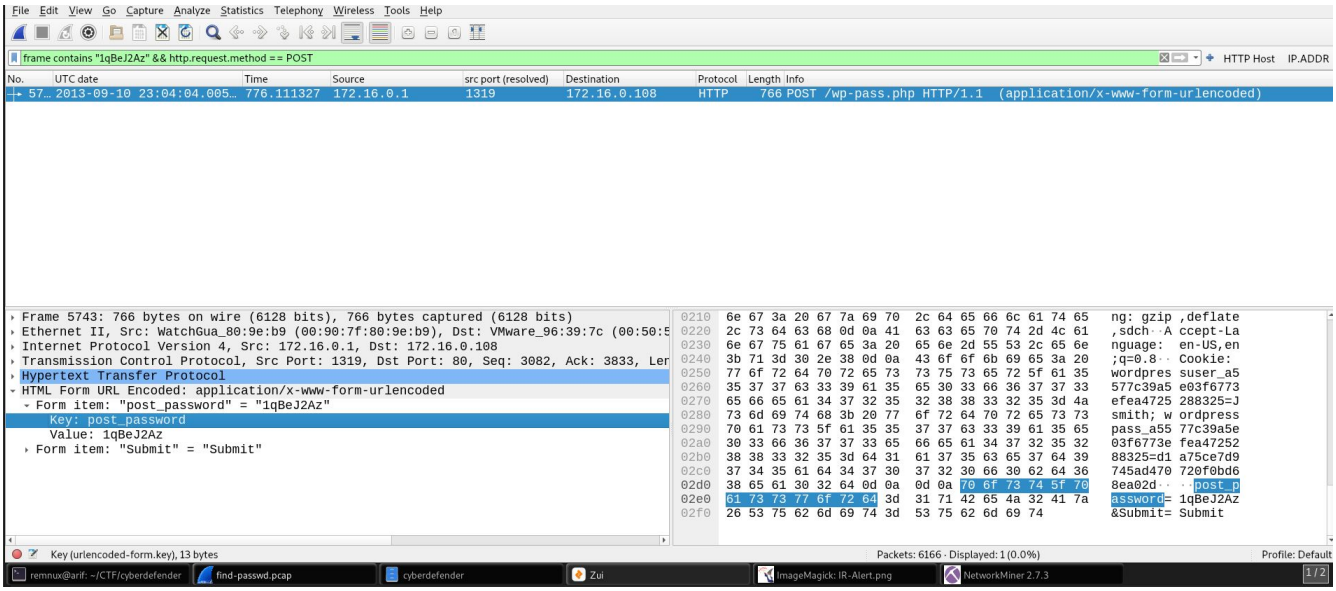
NetworkMiner is in UTC. The image below shows the conversion from UTC to EDT/EST.



11. Analyst PCAP: After reporting that the WordPress page was indeed accessed from an external connection, your boss comes to you in a rage over the potential loss of confidential top-secret documents. He calms down enough to admit that the design's page has a separate access code outside to ensure the security of their information. Before storming off he provided the password to the designs page "1qBeJ2Az" and told you to find a timestamp of the access time or you will be fired. Please provide the time of the accessed Designs page?

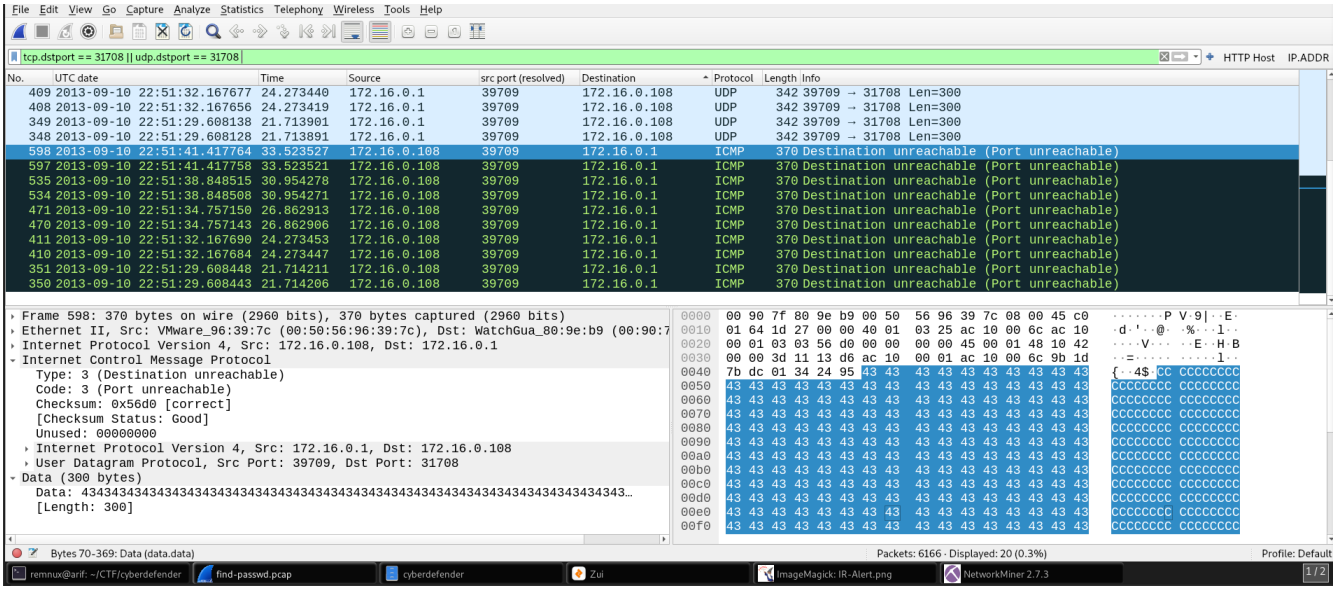
The filter below will display the POST HTTP request that contains 1qBeJ2Az. I used the POST method because this is often used to submit a password form.

Wireshark Search:
frame contains "1qBeJ2Az" && http.request.method == POST



The time the Design page was accessed **: 23:04:04 UTC**

12. Analyst PCAP: What is the source port number in the shellcode exploit? Dest Port was 31708 IDS Signature GPL SHELLCODE x86 inc ebx NOOP
I searched about the IDS signature and found out that the content of SHELLCODE x86 inc ebx NOOP has a lot of character "C" in it.
Then I used the filter below to display all the packets with destination port number 31708.
tcp.dstport == 31708 || udp.dstport == 31708

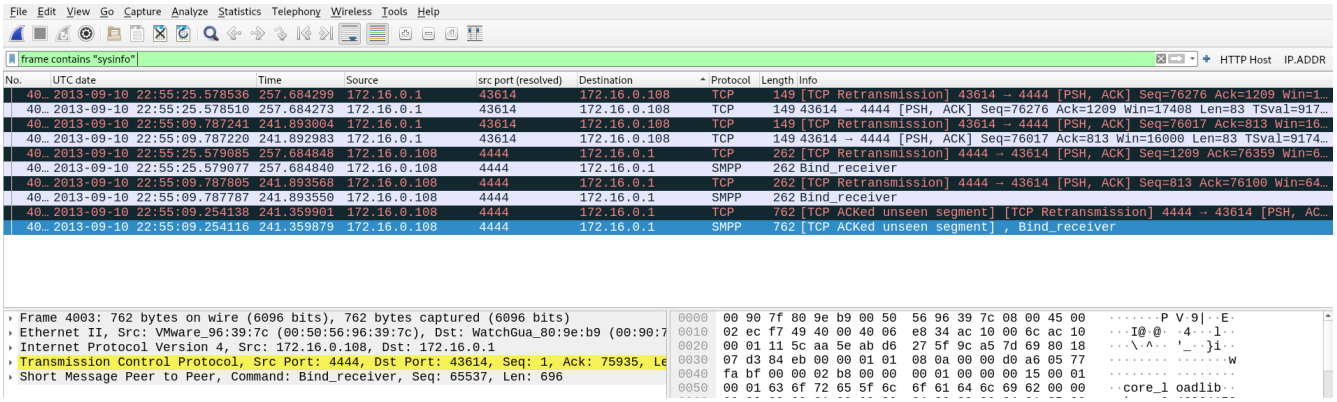


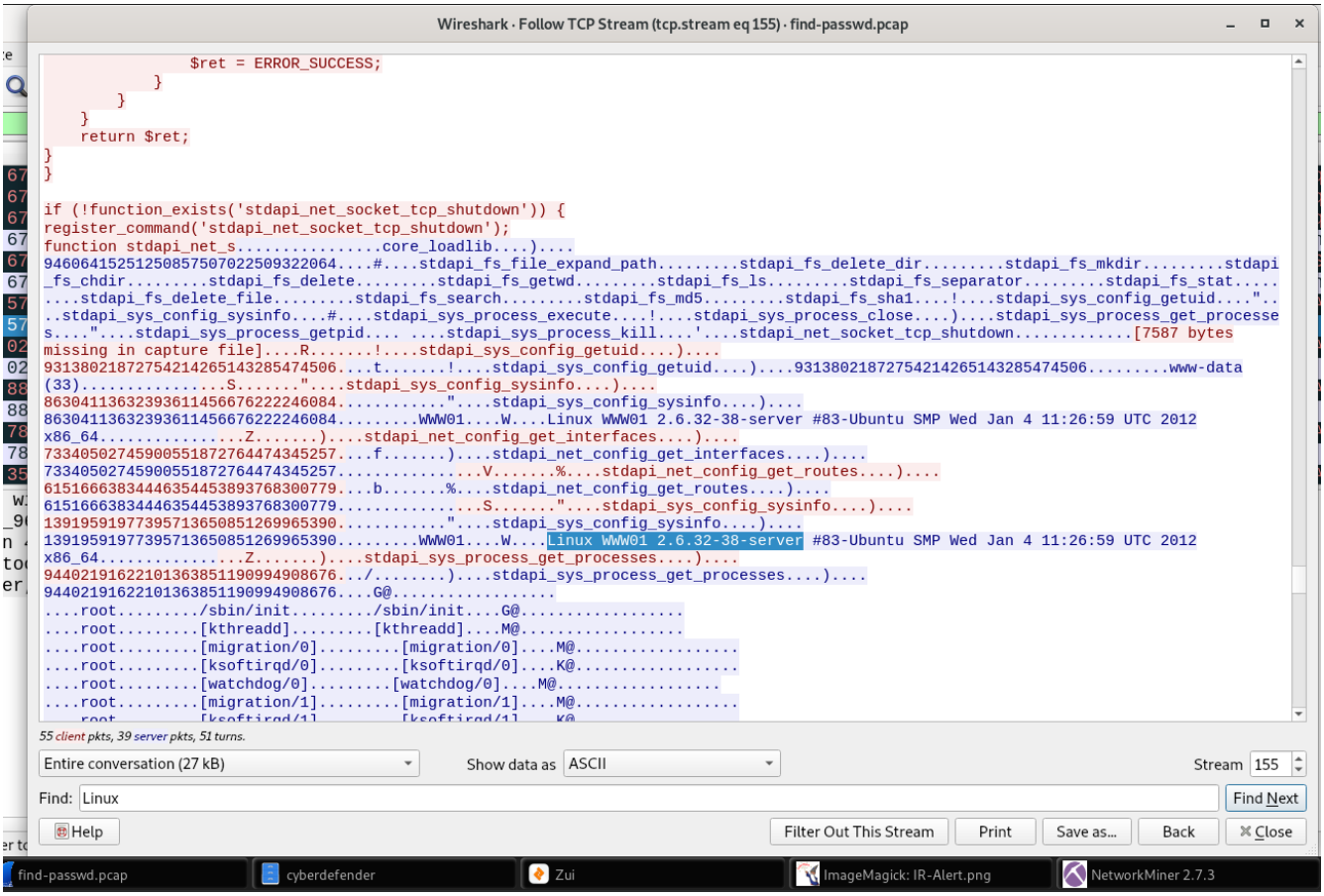
Nomor port sumber dalam eksploitasi shellcode **: 39709**

The packet bytes pane shows the content type of the IDS Signature. The Source Port number can be found in the Frame or Column details.

13. Analyst PCAP: What was the Linux kernel version returned from the meterpreter sysinfo command run by the attacker?
I used the filter below to display all the packets that contain “sysinfo”.
frame contains "sysinfo"

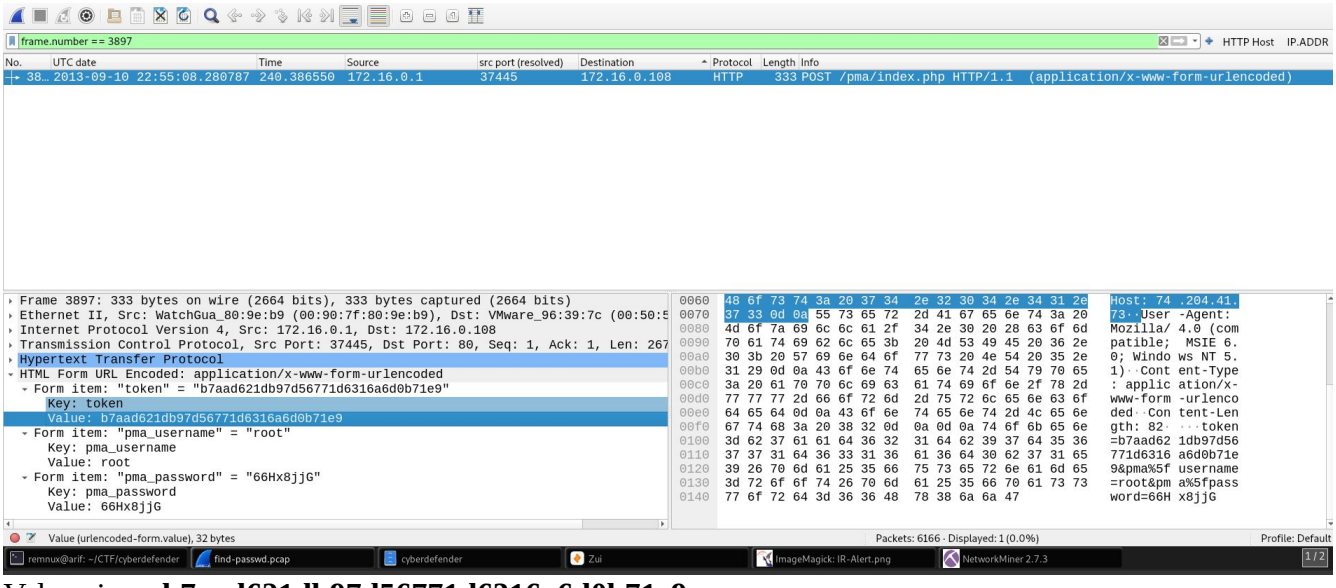
Then I used the Follow TCP Stream option by right-clicking the first packet and navigating to Follow > TCP Stream. The Find feature will quickly find the string “linux” from the results.





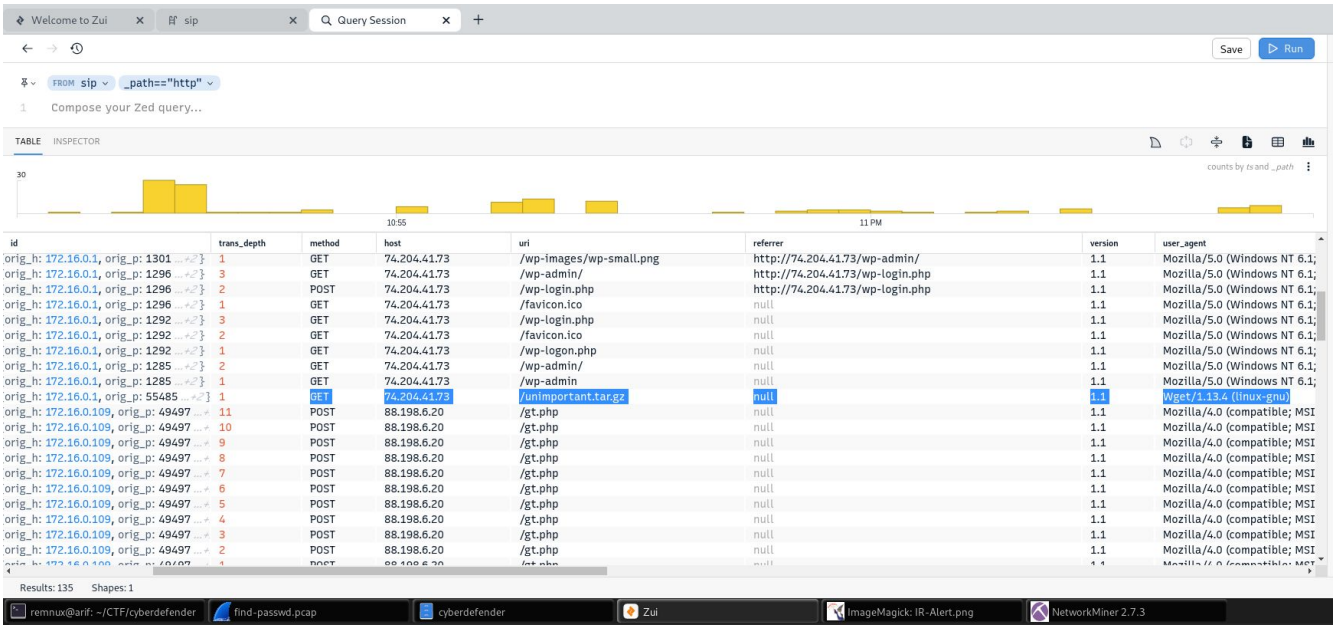
Linux kernel version **: 2.6.32-38-server**

14. Analyst PCAP: What is the value of the token passed in frame 3897?
The filter below will display frame 3897. Expand the HTML Form URL Encoded section for the token value.
frame.number == 3897



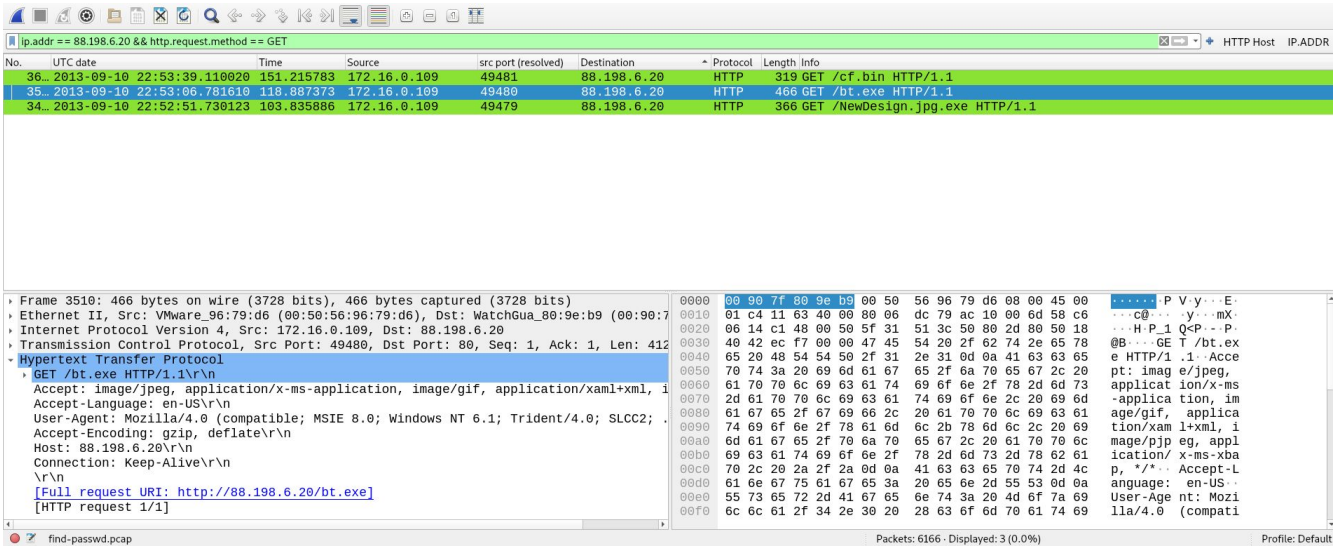
Value sign : **b7aad621db97d56771d6316a6d0b71e9**

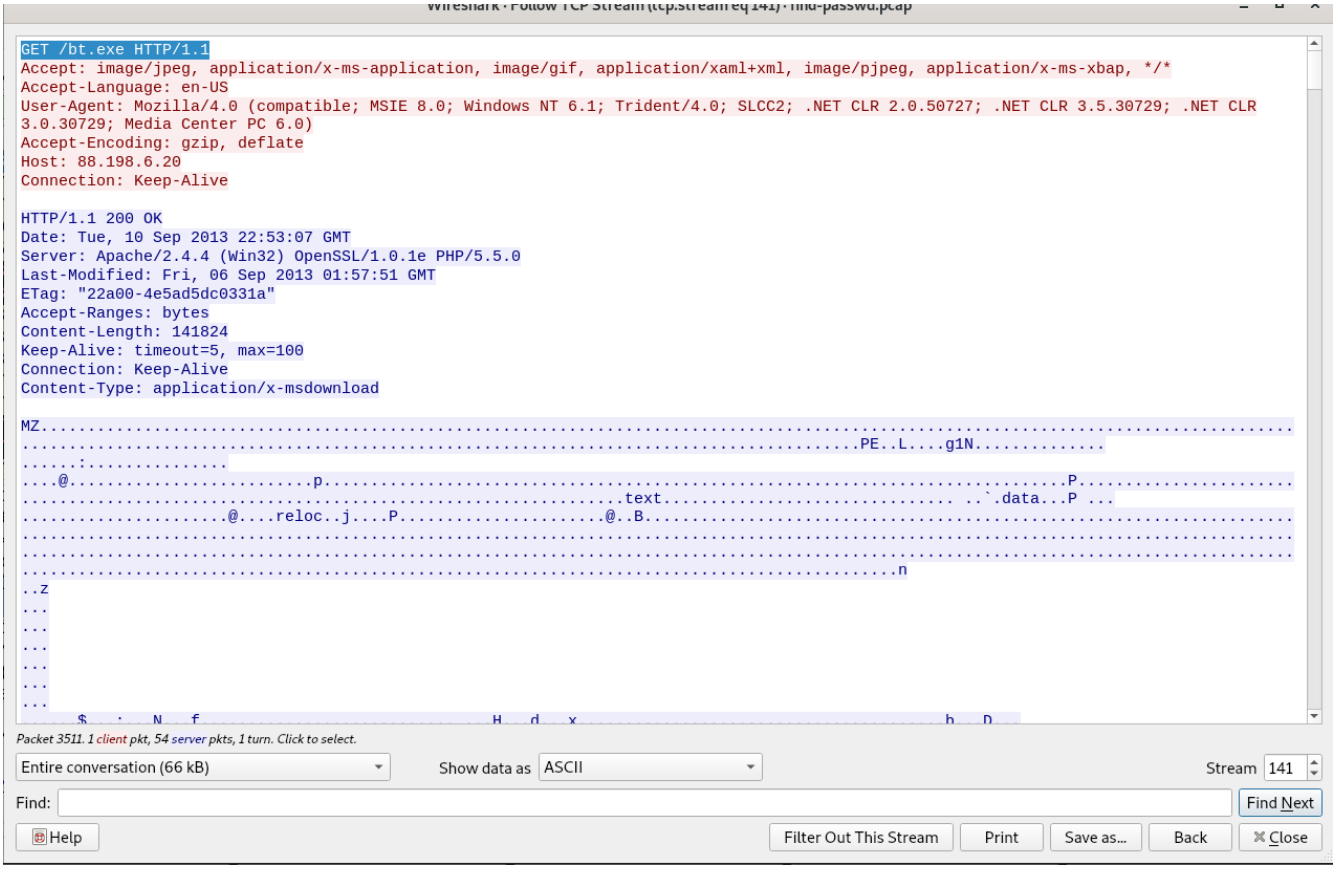
15. Analyst PCAP: What was the tool that was used to download a compressed file from the webserver?
I used the filter _path==”http” in Brim and found the compressed file (unimportant.tar.gz) under the URI field. The user_agent field shows the tool used to download the compressed file.



download files using tools **: wget**

16. Analyst PCAP: What is the download file name the user launched the Zeus bot?
Since I already know the CNC server IP address, I used it to filter and view all the HTTP GET requests from that Server.
ip.addr == 88.198.6.20 && http.request.method == GET





The image above shows the IP address 172.16.0.109 is trying to retrieve 3 files from the CNC server. Analyzing the first file NewDesign.jpg.exe using the Follow TCP Steam option shows the HTTP request has a 404 Not Found response indicating the CNC server cannot find NewDesign.jpg.exe.

Filename download user launches Zeus bot **: bt.exe**

The third file cf.bin is the configuration file that the Zeus bot downloaded after the infection.

17. Analyst Memory: What is the full file path of the system shell spawned through the attacker's meterpreter session?
This article demonstrates how to generate a profile in Linux using Volatility 2. Read here.
The author of this challenge already provided the zip file containing module.dwarf and System.map.

The next step is to move the zip file into the volatility plugin. If you don't know the path, use the command below.

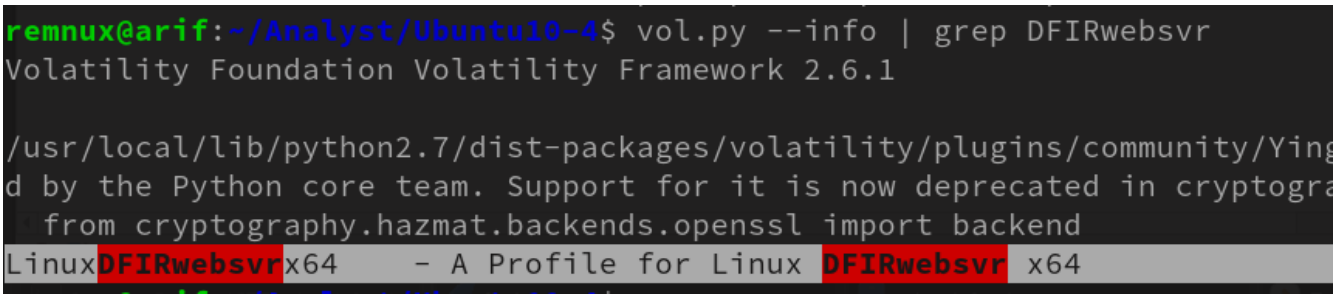
locate volatility/plugins/overlays/linux

In my case, this is the path of my volatility plugin.
/usr/local/lib/python2.7/dist-packages/volatility/plugins/overlays/linux
To move the zip file, use the command below.

sudo mv DFIRwebsvr.zip /usr/local/lib/python2.7/dist-packages/volatility/plugins/overlays/linux

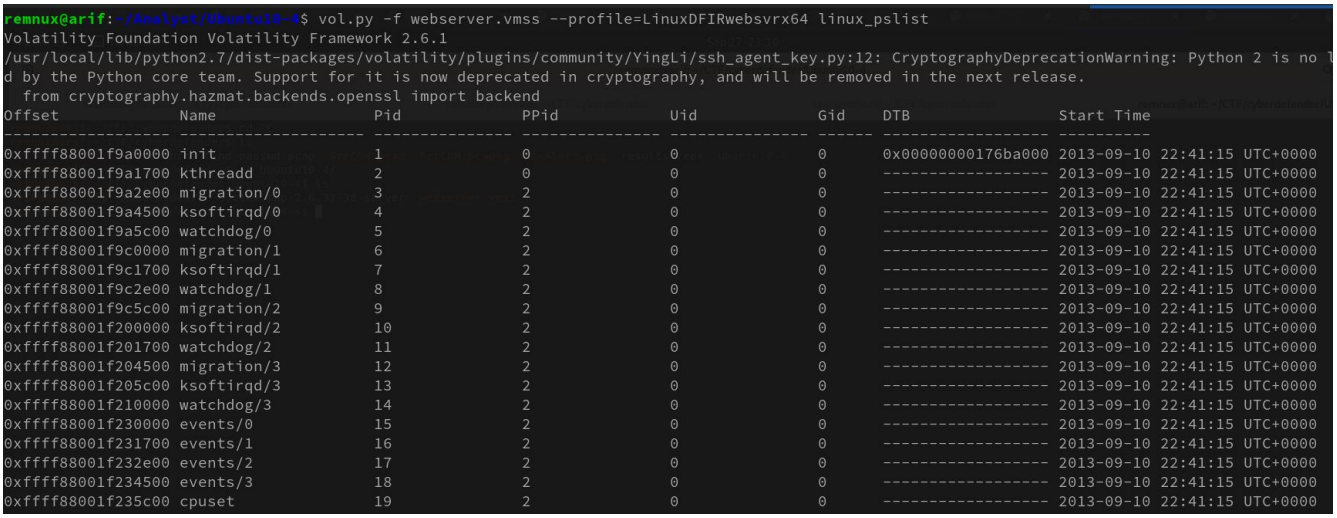
The command below prints the profile of the provided memory image.

vol.py --info | grep DFIRwebsvr

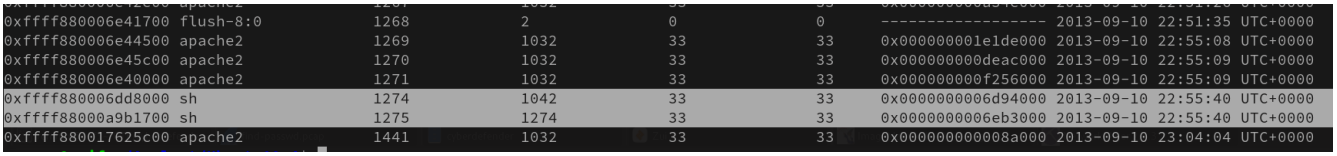


Now that I know the profile of the memory sample, I used the linux_pslist plugin to list all the running processes.

vol.py -f webserver.vmss --profile=LinuxDFIRwebsvrx64 linux_pslist



The below image shows the 2 sh and their Process ID.



Now that I know the Process ID, I used the linux_psaux plugin to gather more information like the command line arguments. I also used the command grep 127 to only display the line that contains 127.

vol.py -f webserver.vmss --profile=LinuxDFIRwebsvrx64 linux_psaux | grep 127

```
remnux@arif:~/Analyst/Ubuntu10-4$ vol.py -f webserver.vmss --profile=LinuxDFIRwebsvrx64 linux_psaux | grep 127
Volatility Foundation Volatility Framework 2.6.1
/usr/local/lib/python2.7/dist-packages/volatility/plugins/community/YingLi/ssh_agent_key.py:12: CryptographyDepre
d by the Python core team. Support for it is now deprecated in cryptography, and will be removed in the next rele
  from cryptography.hazmat.backends.openssl import backend
1270   33     33     /usr/sbin/apache2 -k start
1271   33     33     /usr/sbin/apache2 -k start
1274   33     33     sh -c /bin/sh
1275   33     33     /bin/sh
```

The output shows the command and file path of the 2 sh.

a system shell generated via an attacker's meterpreter session **: /bin/sh**

18. Analyst Memory: What is the Parent Process ID of the two ‘sh’ sessions?
The plugin linux_pstree will display the process parent/child relationship, and the command grep sh -C 3 will display 3 lines before and after the “sh”.

vol.py -f webserver.vmss --profile=LinuxDFIRwebsvrx64 linux_pstree | grep sh -C 3

```
remnux@arif:~/Analyst/Ubuntu10-4$ vol.py -f webserver.vmss --profile=LinuxDFIRwebsvrx64 linux_pstree | grep sh -C 3
Volatility Foundation Volatility Framework 2.6.1
/usr/local/lib/python2.7/dist-packages/volatility/plugins/community/YingLi/ssh_agent_key.py:12: CryptographyDeprecat
d by the Python core team. Support for it is now deprecated in cryptography, and will be removed in the next release
  from cryptography.hazmat.backends.openssl import backend
.udevd                 349
..udevd                461
..udevd                462
.sshd                  736
.dbus-daemon           744             103
.rsyslogd              742             101
.rsyslogd              749             101
--
.apache2               1032
..apache2              1040            33
..apache2              1042            33
...sh                  1274            33
....sh                 1275            33
..apache2              1043            33
..apache2              1045            33
..apache2              1047            33
--
.[ext4-dio-unwrit]     286
.[ext4-dio-unwrit]     287
.[kpsmoused]           505
.[flush-8:0]           1268
```

Parent Process ID of the two 'sh sessions **: 1042**

The image above shows the parent and process ID of the 2 sh.

19. Analyst Memory: What is the latency_record_count for PID 1274?
First, I need to get the Offset of the PID 1274.
The command below will display the information of Process ID 1274, including its Offset.

vol.py -f webserver.vmss --profile=LinuxDFIRwebsvrx64 linux_pslist | grep 1274

```
remnux@arif:~/Analyst/Ubuntu10-4$ vol.py -f webserver.vmss --profile=LinuxDFIRwebsvrx64 linux_pslist | grep 1274
Volatility Foundation Volatility Framework 2.6.1
/usr/local/lib/python2.7/dist-packages/volatility/plugins/community/YingLi/ssh_agent_key.py:12: CryptographyDeprecationWarning: Python 2 is no l
d by the Python core team. Support for it is now deprecated in cryptography, and will be removed in the next release.
  from cryptography.hazmat.backends.openssl import backend
0xffff880006dd8000 sh                 1274           1042             33             33     0x0000000006d94000 2013-09-10 22:55:40 UTC+0000
0xffff88000a9b1700 sh                 1275           1274             33             33     0x0000000006eb3000 2013-09-10 22:55:40 UTC+0000
```

Then I used the plugin linux_volshell to open the interactive shell in the memory image.

vol.py -f webserver.vmss --profile=LinuxDFIRwebsvrx64 linux_volshell

```
remnux@arif:~/Analyst/Ubuntu10-4$ vol.py -f webserver.vmss --profile=LinuxDFIRwebsvrx64 linux_volshell
Volatility Foundation Volatility Framework 2.6.1
/usr/local/lib/python2.7/dist-packages/volatility/plugins/community/YingLi/ssh_agent_key.py:12: Cryptograph
d by the Python core team. Support for it is now deprecated in cryptography, and will be removed in the ne
  from cryptography.hazmat.backends.openssl import backend
Current context: process init, pid=1 DTB=0x176ba000
Welcome to volshell! Current memory image is:
file:///home/remnux/Analyst/Ubuntu10-4/webserver.vmss
To get help, type 'hh()'
>>> dt("task_struct",0xffff880006dd8000)
```

To view the structures, you can use the dt command.
The command below will display the structure of the offset 0xffff880006dd8000

dt("task_struct",0xffff880006dd8000)

```
0x788 : splice_pipe                    0
0x790 : delays                         0
0x798 : dirties                        18446612132429399960
0x7b0 : latency_record_count           0
0x7b8 : latency_record                 -
0x16b8: timer_slack_ns                 50000
```

latency_record_count for PID 1274 **: 0**

20. Analyst Memory: For the PID 1274, what is the first mapped file path?
The linux_proc_maps plugin prints the process map information.

```
remnux@arif:~/Analyst/Ubuntu10-4$ vol.py -f webserver.vmss --profile=LinuxDFIRwebsvrx64 linux_proc_maps -p 1274
Volatility Foundation Volatility Framework 2.6.1
/usr/local/lib/python2.7/dist-packages/volatility/plugins/community/YingLi/ssh_agent_key.py:12: CryptographyDeprecationWarning: Python 2 is no longer supporte
d by the Python core team. Support for it is now deprecated in cryptography, and will be removed in the next release.
  from cryptography.hazmat.backends.openssl import backend
Offset             Pid      Name                 Start              End                Flags Pgoff Major  Minor  Inode      File Path
------------------ -------- -------------------- ------------------ ------------------ ----- ------------------ ------ ------ ---------- ---------
0xffff880006dd8000     1274 sh                   0x0000000000400000 0x0000000000418000 r-x                0x0      8      1     651536 /bin/dash
0xffff880006dd8000     1274 sh                   0x0000000000617000 0x0000000000618000 r--            0x17000      8      1     651536 /bin/dash
0xffff880006dd8000     1274 sh                   0x0000000000618000 0x0000000000619000 rw-            0x18000      8      1     651536 /bin/dash
0xffff880006dd8000     1274 sh                   0x0000000000619000 0x000000000061c000 rw-                0x0      0      0          0
0xffff880006dd8000     1274 sh                   0x000000000151a000 0x000000000153b000 rw-                0x0      0      0          0 [heap]
0xffff880006dd8000     1274 sh                   0x00007f878ac5f000 0x00007f878addc000 r-x                0x0      8      1     652393 /lib/libc-2.11.1.so
0xffff880006dd8000     1274 sh                   0x00007f878addc000 0x00007f878afdb000 ---            0x17d000      8      1     652393 /lib/libc-2.11.1.so
0xffff880006dd8000     1274 sh                   0x00007f878afdb000 0x00007f878afdf000 r--            0x17c000      8      1     652393 /lib/libc-2.11.1.so
0xffff880006dd8000     1274 sh                   0x00007f878afdf000 0x00007f878afe0000 rw-            0x180000      8      1     652393 /lib/libc-2.11.1.so
```

The image above shows the first mapped file path of Process ID 1274.
first mapped file path : **/bin/dash**

21. Analyst Memory: What is the md5hash of the receive.1105.3 file out of the per-process packet queue?
The plugin linux_pkt_queues will enumerate and recover queues out to disk.

vol.py -f webserver.vmss --profile=LinuxDFIRwebsvrx64 linux_pkt_queues -D /home/remnux/Documents/

```
remnux@arif:~/Analyst/Ubuntu10-4$ vol.py -f webserver.vmss --profile=LinuxDFIRwebsvrx64 linux_pkt_queues -D /home/remnux/Documents/
Volatility Foundation Volatility Framework 2.6.1
/usr/local/lib/python2.7/dist-packages/volatility/plugins/community/YingLi/ssh_agent_key.py:12: CryptographyDeprecationWarning: Pytho
d by the Python core team. Support for it is now deprecated in cryptography, and will be removed in the next release.
  from cryptography.hazmat.backends.openssl import backend
Wrote 32 bytes to receive.930.10
Wrote 32 bytes to receive.1105.3
```

md5sum command prints the md5 hash of receive.1105.3.

```
remnux@arif:~/Analyst/Ubuntu10-4$ md5sum /home/remnux/Documents/receive.1105.3
184c8748cfcfe8c0e24d7d80cac6e9bd  /home/remnux/Documents/receive.1105.3
```

md5hash file receiver.1105.3 out of the packet queue per process :
184c8748cfcfe8c0e24d7d80cac6e9bd

Thankyou.

Regards,

M Arif