2018-10-31 - TRAFFIC ANALYSIS EXERCISE - HAPPY HALLOWEEN!

Course Name: Malware Analysis and Reverse Engineering (IAM302)
Student Name: Nguyễn Trần Vinh – SE160258
Instructor Name: Mai Hoàng Đỉnh

SCENARIO

Review the pcap and draft an incident report. Your report should contain:

- Date and time of the activity (in GMT or UTC)
- The account name or username from the infected Windows computer
- The host name of the infected Windows computer
- The MAC address of the infected Windows computer
- SHA256 file hashes for any malware from the pcap
- What type of infection this is

Answer:
#1: Date and time of the activity (in GMT or UTC)
- 2018-10-31 15:33:05 UTC

#2: The account name or username from the infected Windows computer
- ichabod.crane

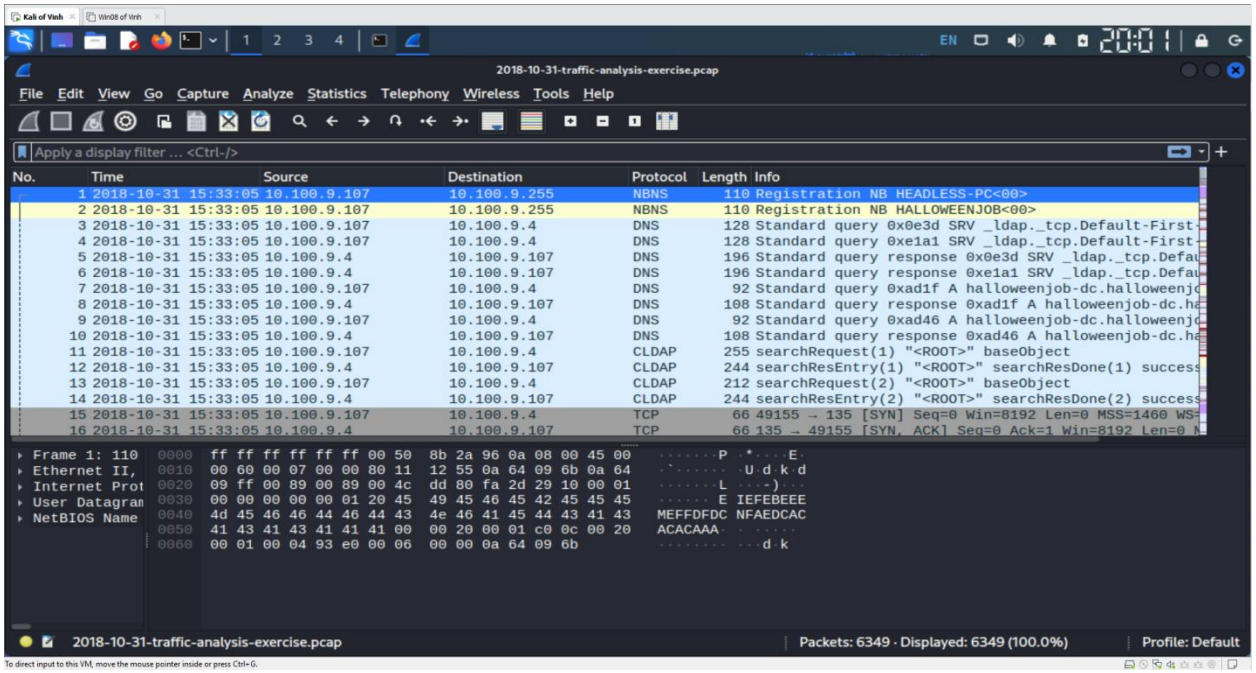
#3: The host name of the infected Windows computer
- Headless-PC

#4: The MAC address of the infected Windows computer
- 00:50:8b:2a:96:0a

#5: SHA256 file hashes for any malware from the pcap
- 396223eeec49493a52dd9d8ba5348a332bf064483a358db79d8bb8d22e6eb62c

#6: Type of infection
- Trickbot

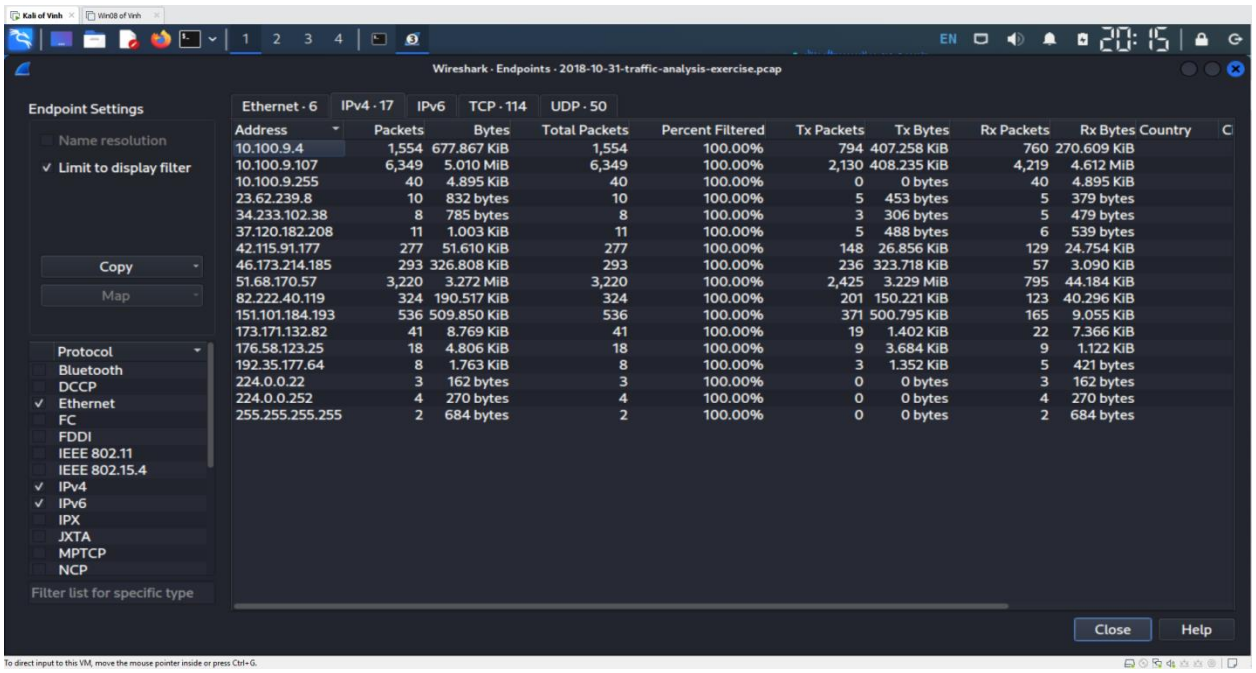
Detail:
- First frame: 2018-10-31 15:33:05 UTC



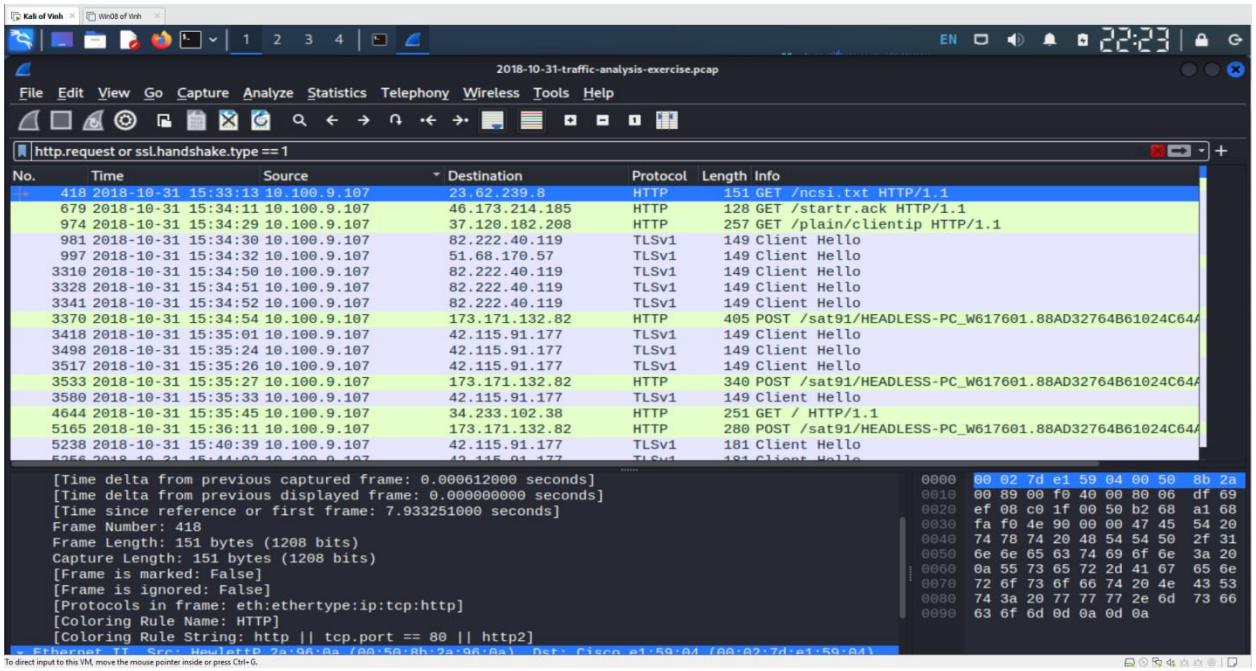
- Listing all participants of unique conversations within .pcap file:

```
┌──(TouristV㉿kali)-[~/Downloads]
└─$ tshark -r 2018-10-31-traffic-analysis-exercise.pcap -T fields -e ip.addr | sort | uniq
10.100.9.107,10.100.9.255
10.100.9.107,10.100.9.4
10.100.9.107,151.101.184.193
10.100.9.107,173.171.132.82
10.100.9.107,176.58.123.25
10.100.9.107,192.35.177.64
10.100.9.107,224.0.0.22
10.100.9.107,224.0.0.252
10.100.9.107,23.62.239.8
10.100.9.107,255.255.255.255
10.100.9.107,34.233.102.38
10.100.9.107,37.120.182.208
10.100.9.107,42.115.91.177
10.100.9.107,46.173.214.185
10.100.9.107,51.68.170.57
10.100.9.107,82.222.40.119
10.100.9.4,10.100.9.107
151.101.184.193,10.100.9.107
173.171.132.82,10.100.9.107
176.58.123.25,10.100.9.107
192.35.177.64,10.100.9.107
23.62.239.8,10.100.9.107
34.233.102.38,10.100.9.107
37.120.182.208,10.100.9.107
42.115.91.177,10.100.9.107
46.173.214.185,10.100.9.107
51.68.170.57,10.100.9.107
82.222.40.119,10.100.9.107
```

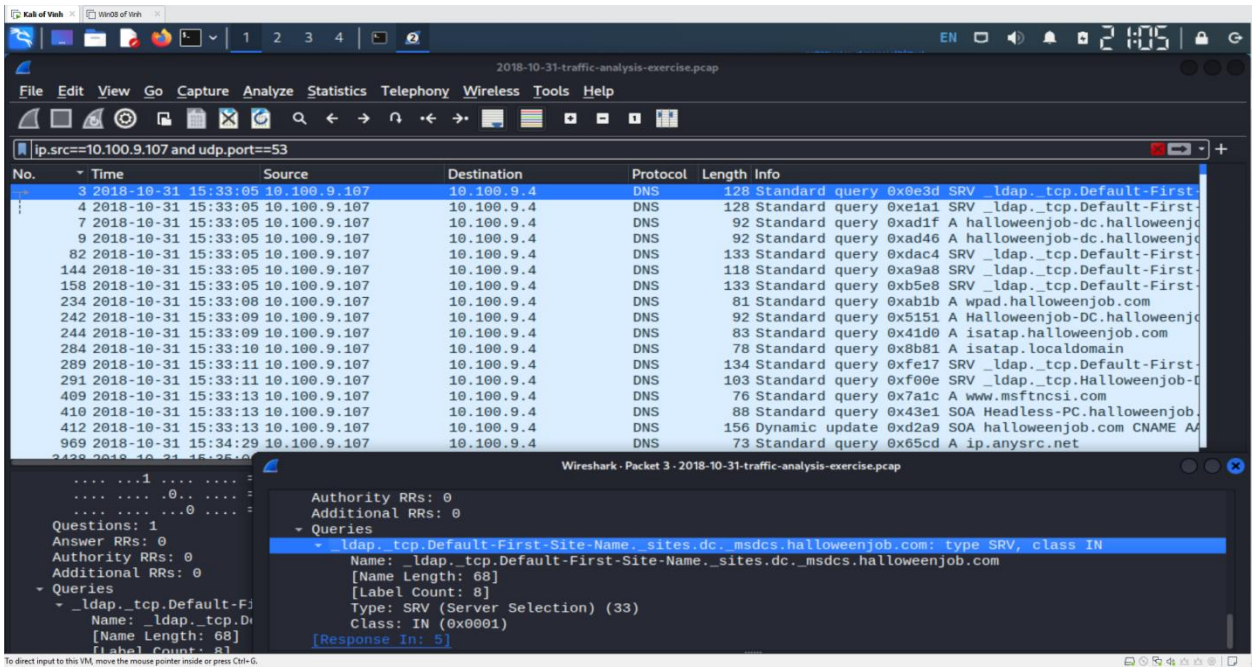
- Check endpoints:



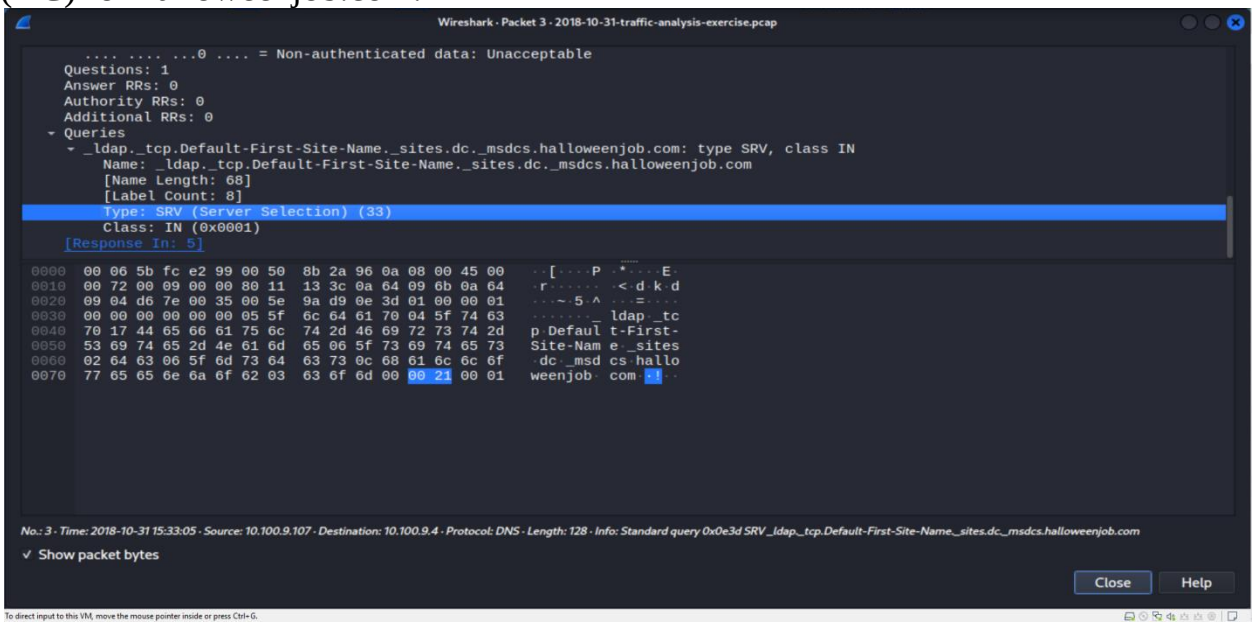
- Filter on http.request or ssl.handshake.type == 1 for web-based traffic, and I find the source IP address is 10.100.9.107. That's the Windows client.



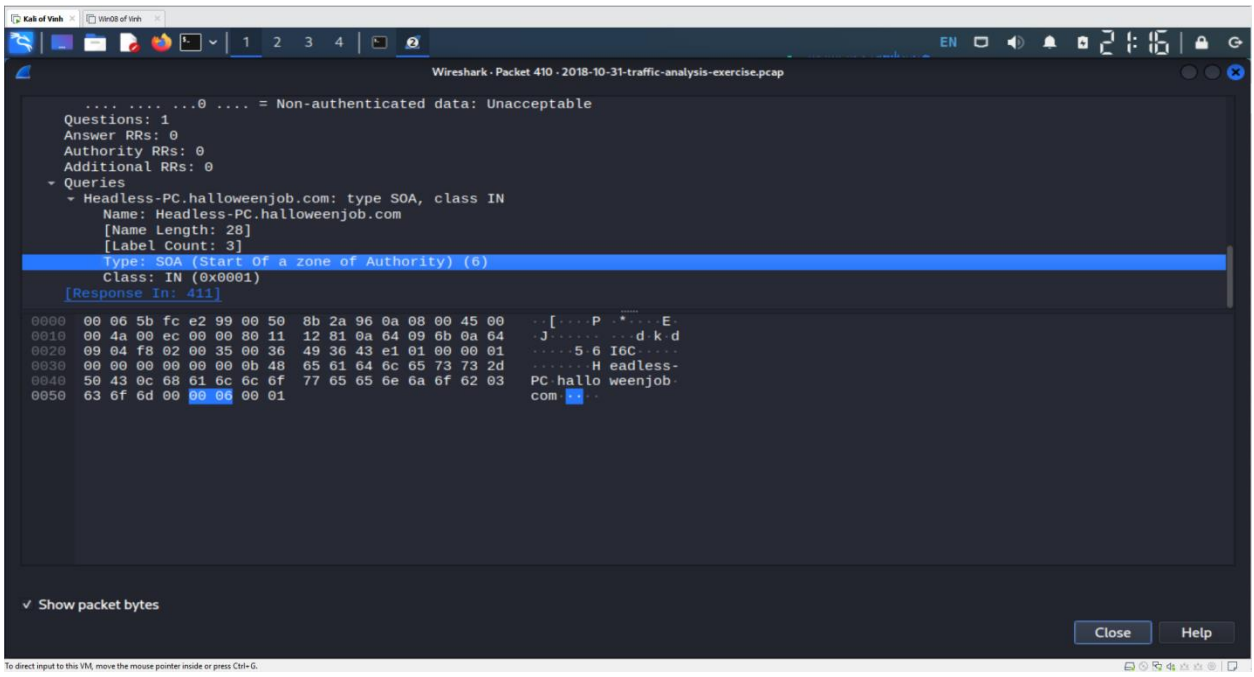
- Let’s say IP 10.100.9.107 is the victim's computer while IP 10.100.9.4 is another local node of some sort. Let's prove this assumption by filtering DNS query packets with a source address of 10.100.9.107. The resulting output will show the source address polling its DNS server, usually done before authenticating to a domain and/or communicating with HTTP servers.

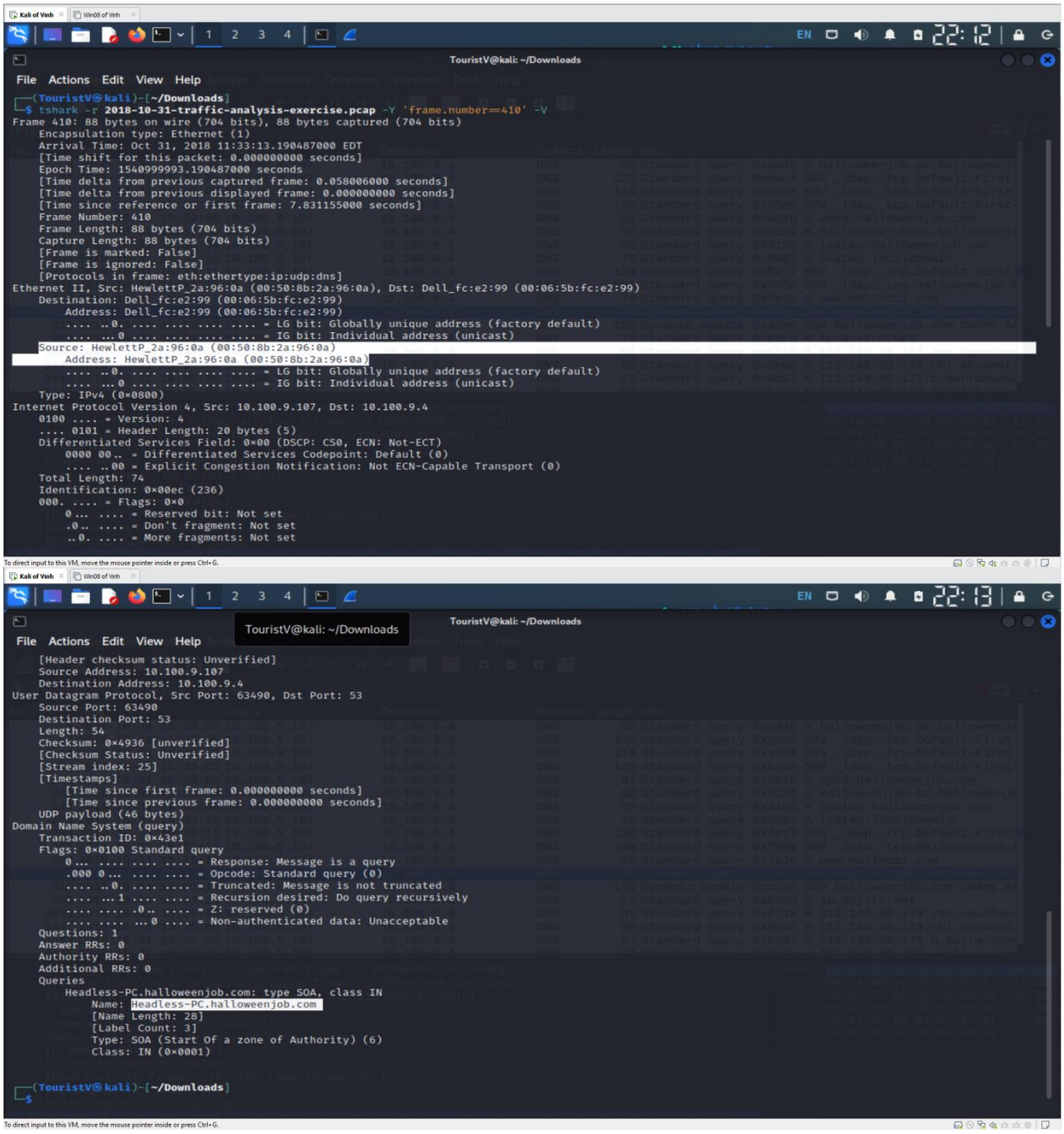


- With this result, I can now start to deduce some things. For example, we see 10.100.9.4 used exclusively by 10,100.9.107 to resolve multiple IP addresses. I also see a few queries for SRV records used to determine which nodes are serving different applications. Example frame #3 shows looking for a Domain Controller (DC) for halloweenjob.com.



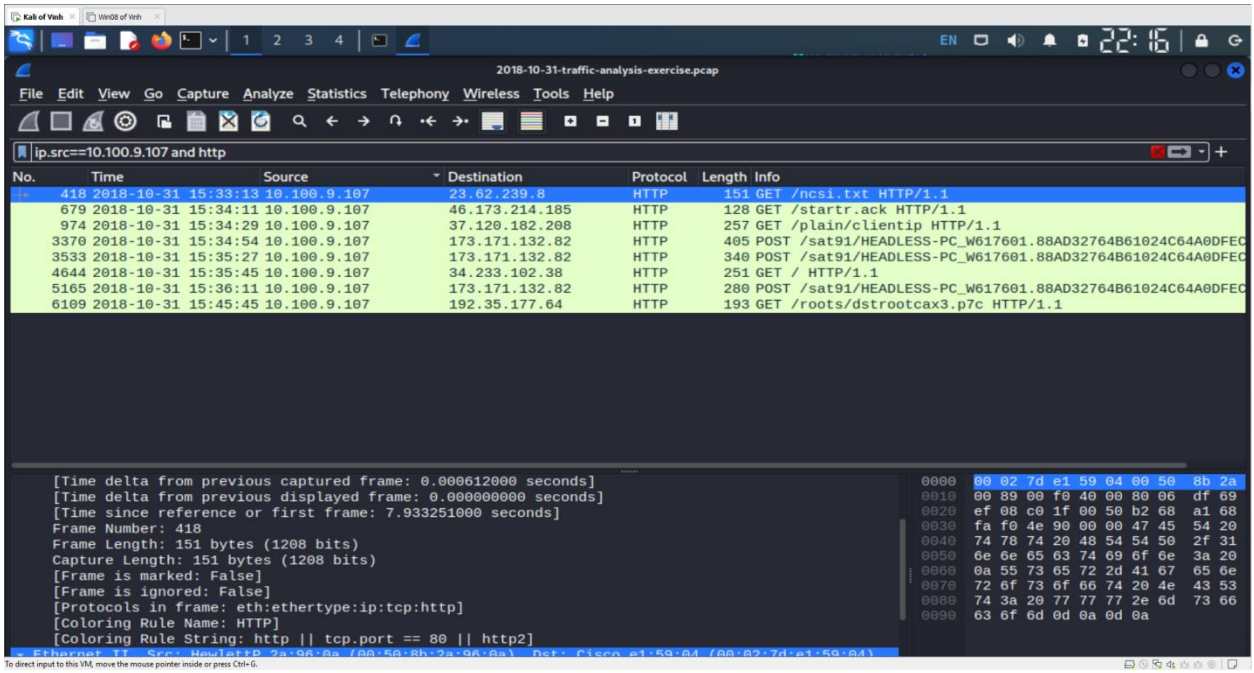
- Frame #410, I also see a single Dynamic update for a SOA record.


Kali of Vinh
Win08 of Vinh
1 2 3 4
EN
21:16
Wireshark · Packet 410 · 2018-10-31-traffic-analysis-exercise.pcap
....0 .... = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
Headless-PC.halloweenjob.com: type SOA, class IN
Name: Headless-PC.halloweenjob.com
[Name Length: 28]
[Label Count: 3]
Type: SOA (Start Of a zone of Authority) (6)
Class: IN (0x0001)
[Response In: 411]
0000 00 06 5b fc e2 99 00 50 8b 2a 96 0a 08 00 45 00
0010 00 4a 00 ec 00 00 80 11 12 81 0a 64 09 6b 0a 64
0020 09 04 f8 02 00 35 00 36 49 36 43 e1 01 00 00 01
0030 00 00 00 00 00 00 0b 48 65 61 64 6c 65 73 73 2d
0040 50 43 0c 68 61 6c 6c 6f 77 65 65 6e 6a 6f 62 03
0050 63 6f 6d 00 00 06 00 01
Show packet bytes
Close
Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



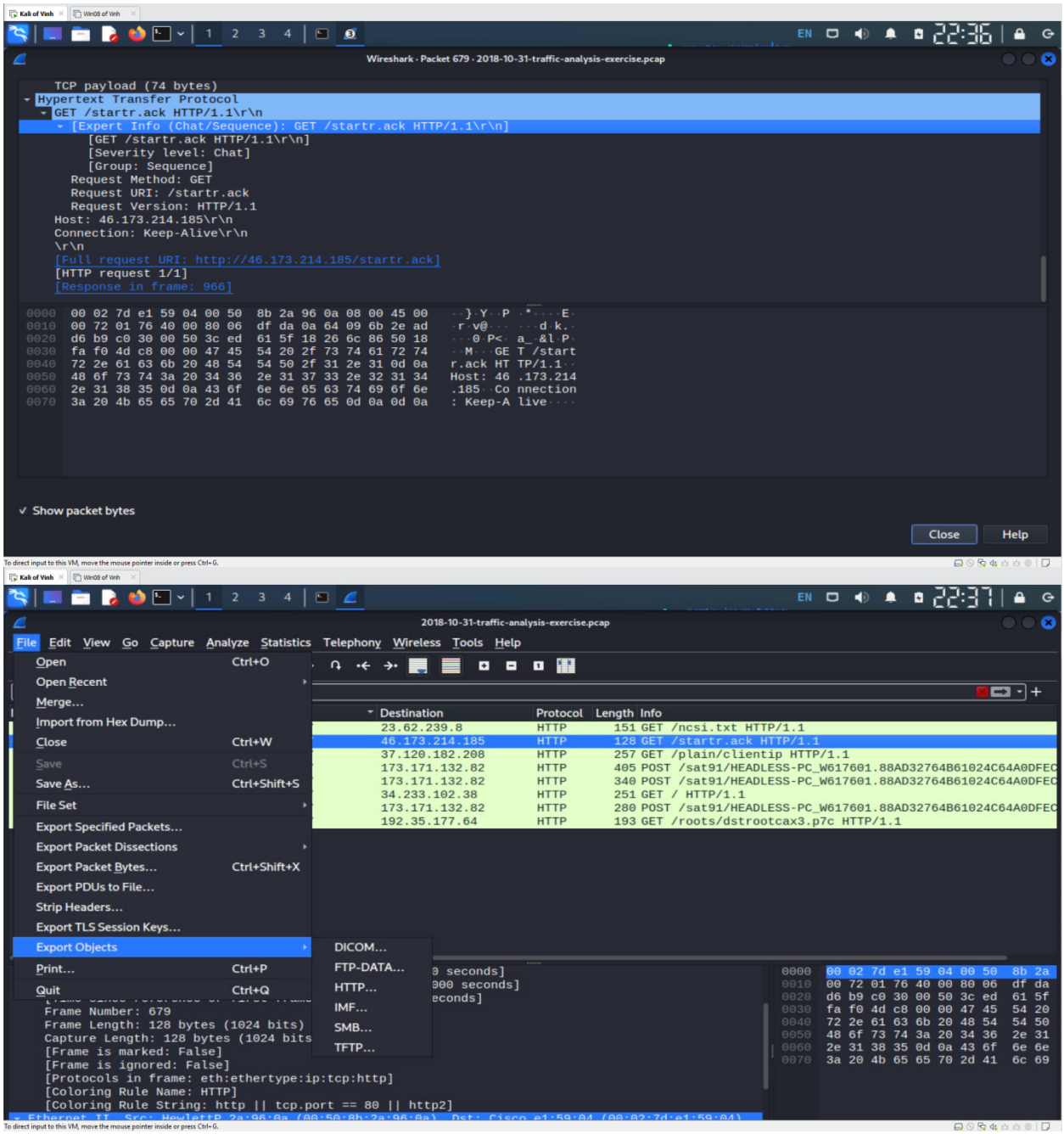
➔ The Dynamic update is 10.100.9.107 giving its MAC address (00:50:8b:2a:96:0a) and hostname (Headless-PC) to the local DNS server.

- Search the .pcap for HTTP requests

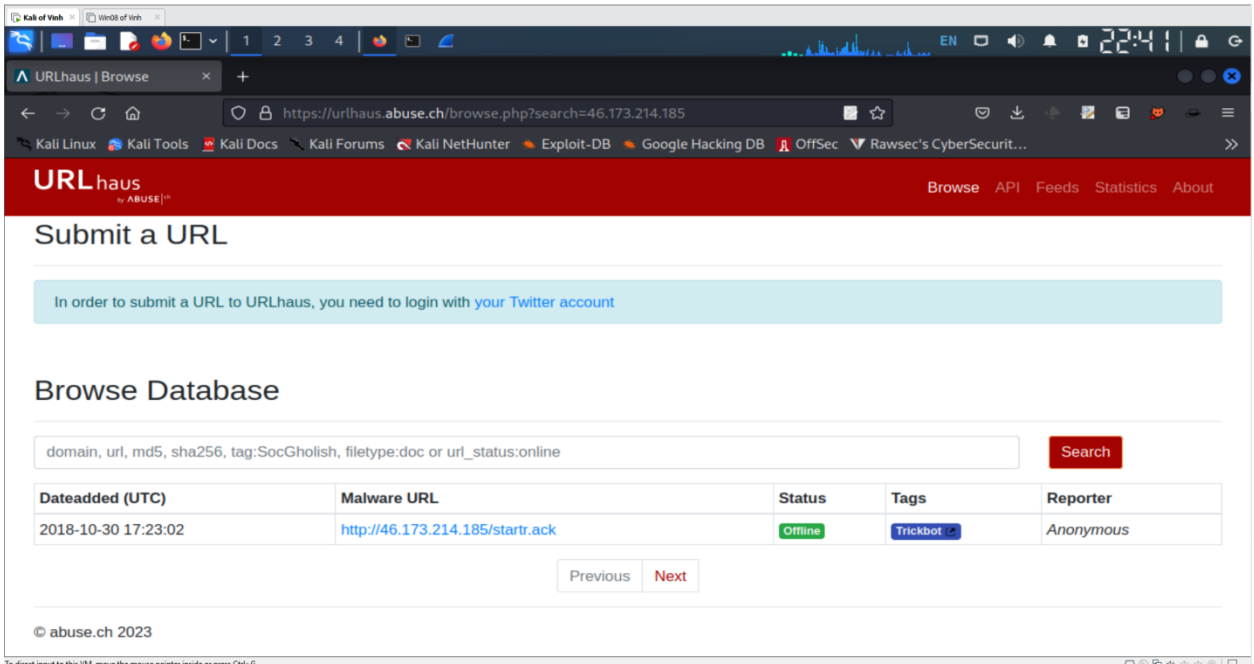


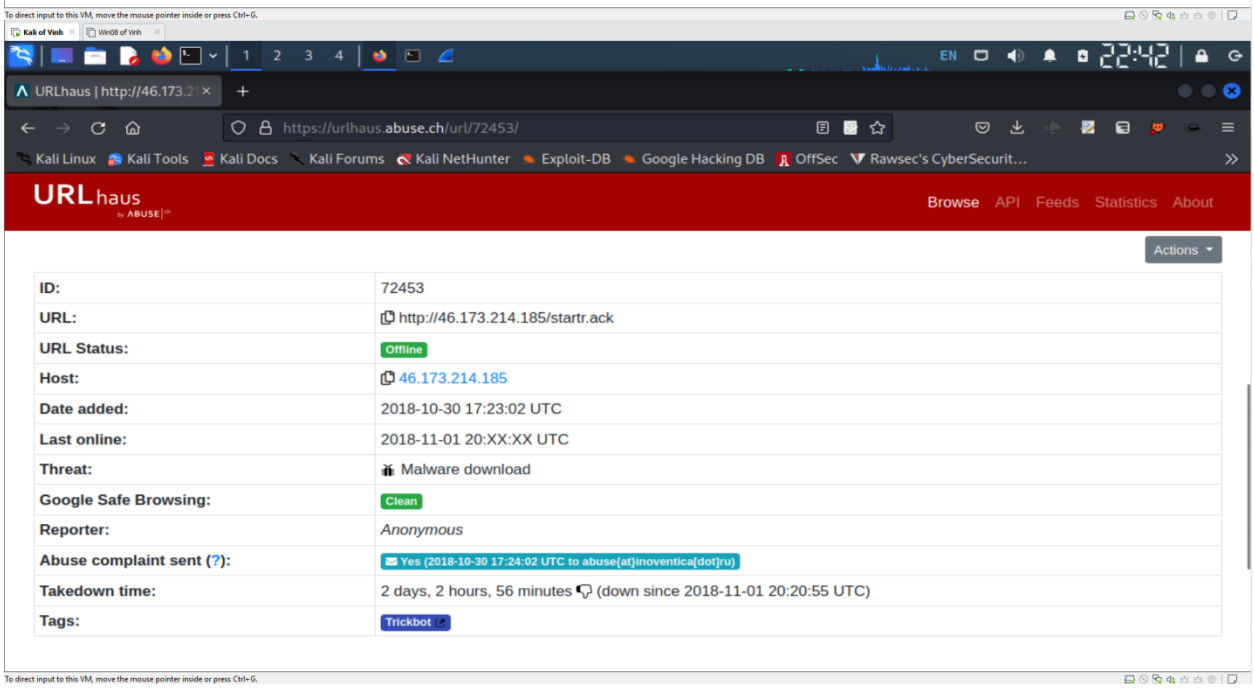
- The first HTTP request is frame #418 could be of interest as it is only a few frames away from the previous DNS query we analyzed is #410. Yet, it's actually benign as Microsoft systems are typically configured with a service called [Network Connectivity Status Indicator (NCSI).]

- The second HTTP request however (frame #679), is not benign. Let's download a .csv file containing a list of known malicious IP addresses to search it for the HTTP server at 46.173.214.185.

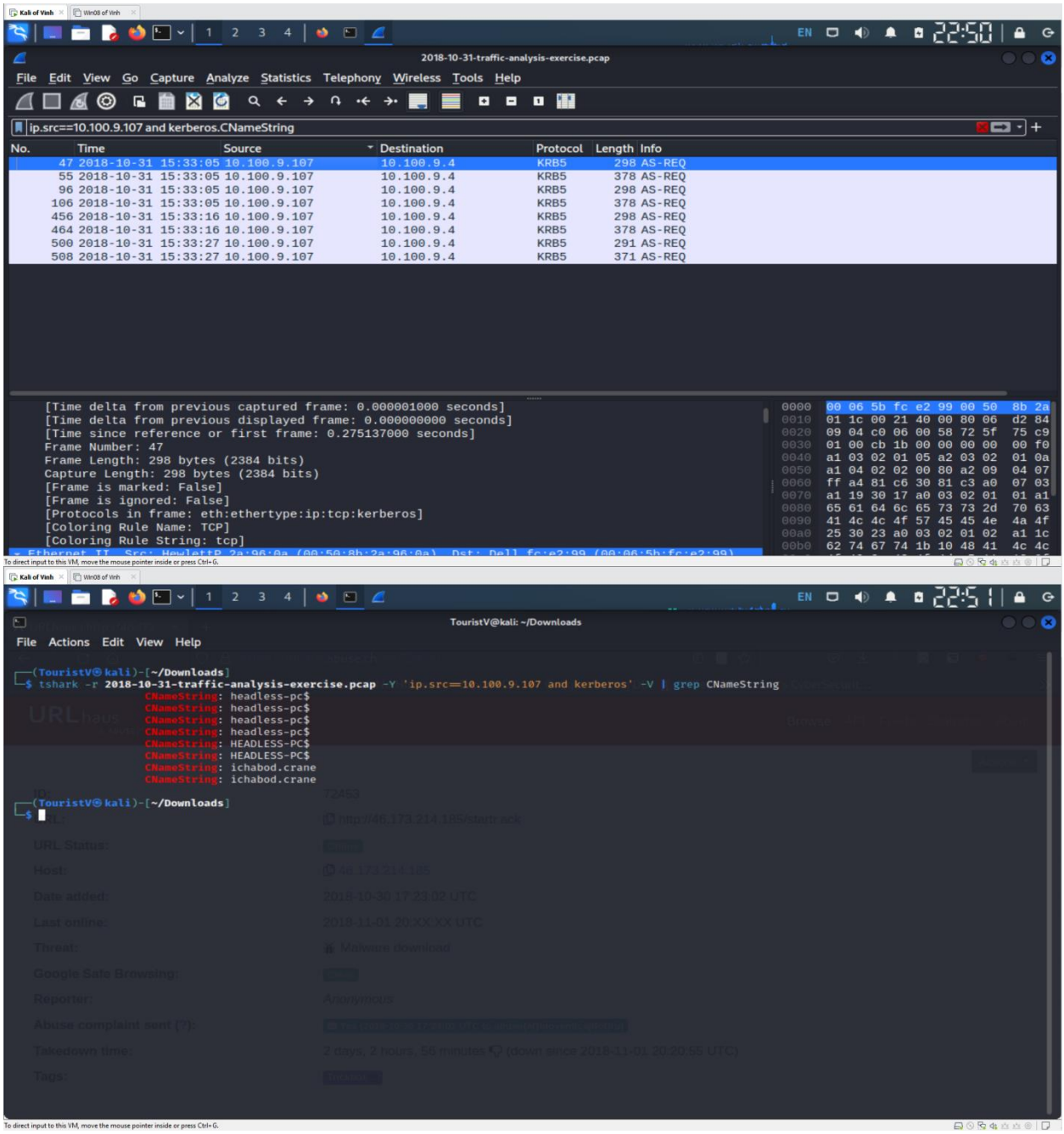


- Find IP 46.173.214.185 on [URLhaus | Browse (abuse.ch)] and see detail

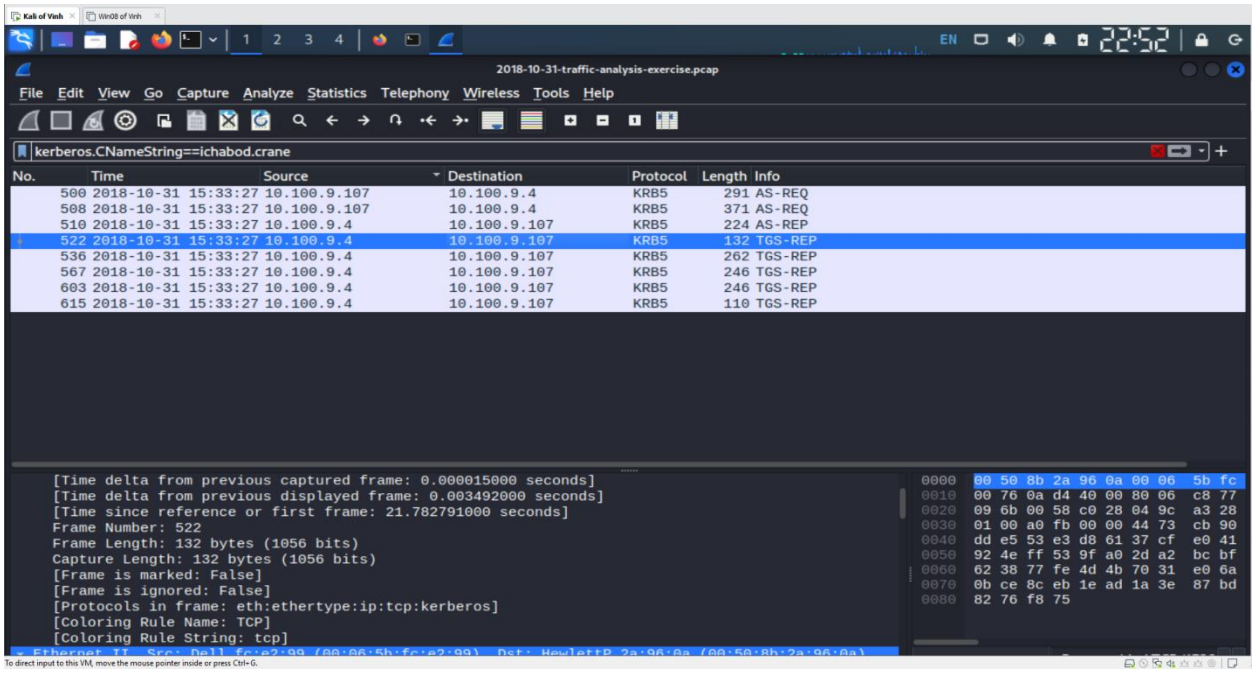




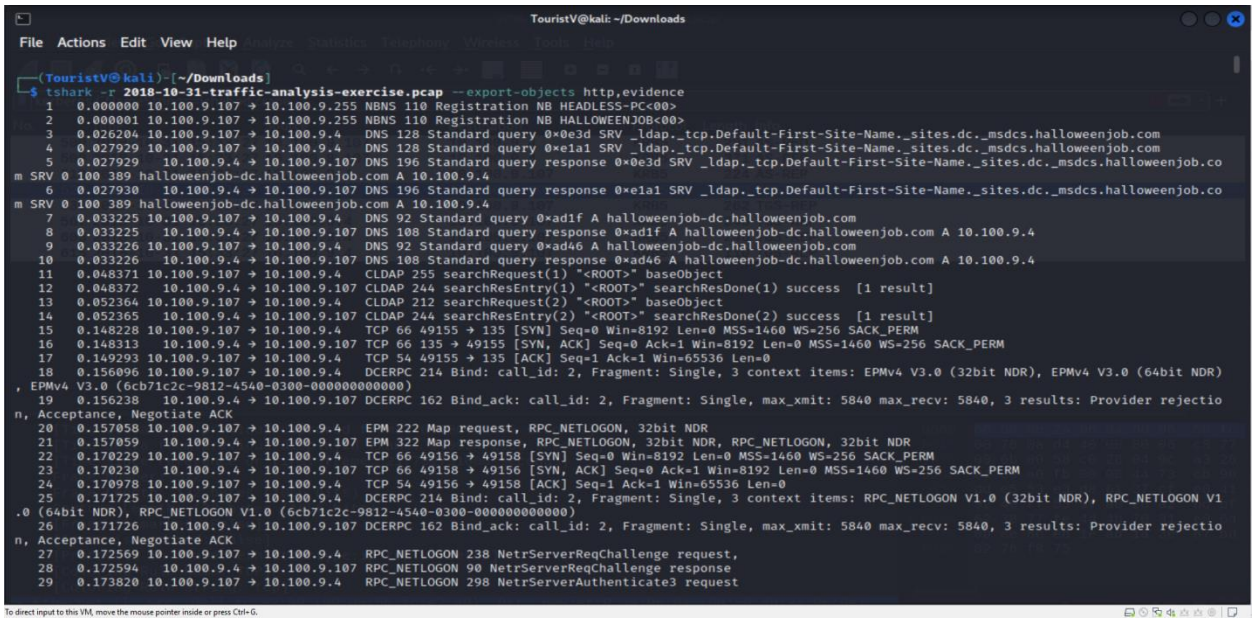
- Find who downloaded the malware

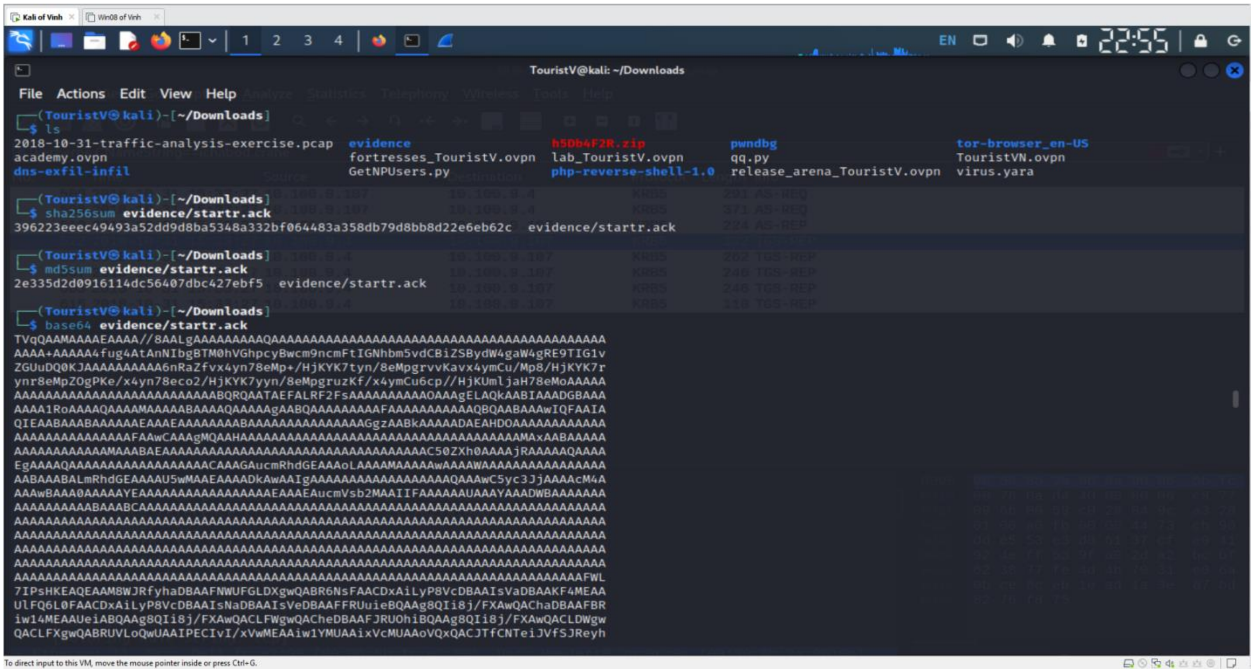


- Let’s take a step back and filter for frames containing this username for reference.



- the SHA256 file hash




Kali of Vinh
Win08 of Vinh
TouristV@kali: ~/Downloads
File Actions Edit View Help
┌──(TouristV㉿kali)-[~/Downloads]
└─$ ls
2018-10-31-traffic-analysis-exercise.pcap evidence h5Db4F2R.zip pwndbg tor-browser_en-US
academy.ovpn fortresses_TouristV.ovpn lab_TouristV.ovpn qq.py TouristVN.ovpn
dns-exfil-infil GetNPUsers.py php-reverse-shell-1.0 release_arena_TouristV.ovpn virus.yara
┌──(TouristV㉿kali)-[~/Downloads]
└─$ sha256sum evidence/startr.ack
396223eeec49493a52dd9d8ba5348a332bf064483a358db79d8bb8d22e6eb62c evidence/startr.ack
┌──(TouristV㉿kali)-[~/Downloads]
└─$ md5sum evidence/startr.ack
2e335d2d0916114dc56407dbc427ebf5 evidence/startr.ack
┌──(TouristV㉿kali)-[~/Downloads]
└─$ base64 evidence/startr.ack
TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAA+AAAAA4fug4AtAnNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5vdCBiZSBydW4gaW4gRE9TIG1v
ZGUuDQ0KJAAAAAAAAAA6nRaZfvx4yn78eMp+/HjKYK7tyn/8eMpgrvvKavx4ymCu/Mp8/HjKYK7r
ynr8eMpZOgPKe/x4yn78eco2/HjKYK7yyn/8eMpgruzKf/x4ymCu6cp//HjKUmljaH78eMoAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAABQRQAATAEFALRF2FsAAAAAAAAAAOAAAgELAQkAABIAAADGBAAA
AAAA1RoAAAAQAAAAMAAAAABAAAAQAAAAgAABQAAAAAAAAAFAAAAAAAAAAQBQAABAAAwIQFAAIA
QIEAABAAABAAAAAAEAAAEAAAAAAAABAAAAAAAAAAAAAAAAGgzAABkAAAAADAEAHDOAAAAAAAAAAAAA
AAAAAAAAAAAAAAAFAAwCAAAgMQAAHAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAMAxAABAAAAA
AAAAAAAAAAAMAAABAEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAC50ZXh0AAAAjRAAAAAQAAAA
EgAAAAQAAAAAAAAAAAAAAAAAAACAAAGAucmRhdGEAAAoLAAAAMAAAAAwAAAAWAAAAAAAAAAAAAAAAA
AABAAABALmRhdGEAAAAU5wMAAEAAAADkAwAAIgAAAAAAAAAAAAAAAAAAAAQAAAwC5yc3JjAAAAcM4A
AAAwBAAA0AAAAAYEAAAAAAAAAAAAAAAAAAEAAAEAucmVsb2MAAIIFAAAAAAUAAAYAAADWBAAAAAAA
AAAAAAAAABAAABCAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAFWL
7IPsHKEAQEAAM8WJRfyhaDBAAFNWUFGLDXgwQABR6NsFAACDxAiLyP8VcDBAAIsVaDBAAKF4MEAA
UlFQ6L0FAACDxAiLyP8VcDBAAIsNaDBAAIsVeDBAAFFRUuieBQAAg8QIi8j/FXAwQAChaDBAAFBR
iw14MEAAUeiABQAAg8QIi8j/FXAwQACLFWgwQACheDBAAFJRUOhiBQAAg8QIi8j/FXAwQACLDWgw
QACLFXgwQABRUVLoQwUAAIPECIvI/xVwMEAAiw1YMUAAixVcMUAAoVQxQACJTfCNTeiJVfSJReyh
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.