Digital Forensics

Wireshark Network Analyze

By:

Putri Anastasya (001202200131)

PRESIDENT UNIVERSITY

Faculty of Computing:

Information Technology Study Program

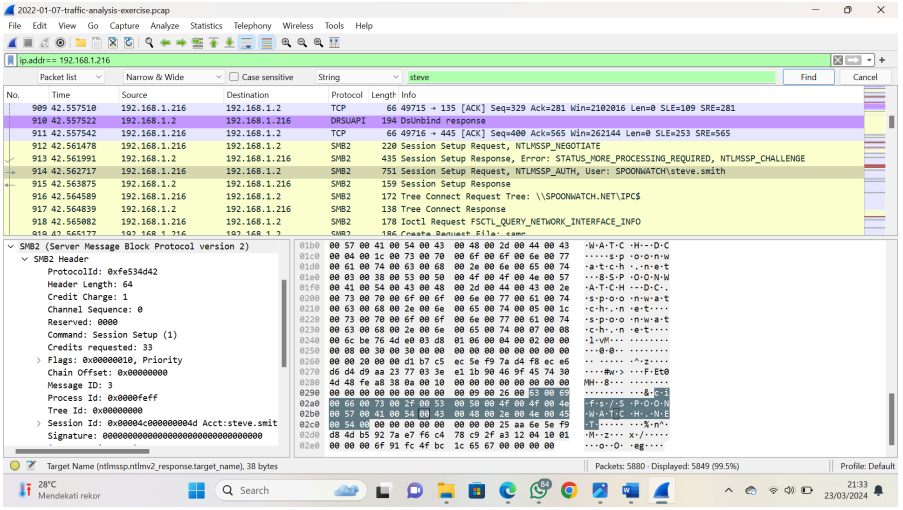
2022-01-07-TRAFFIC ANALYSIS QUIZ ANSWERS

Executive Summary

On 2022-01-07 at approximately 16:07 UTC, a Windows host used by Steve Smith was infected with OskiStealer malware.

Details

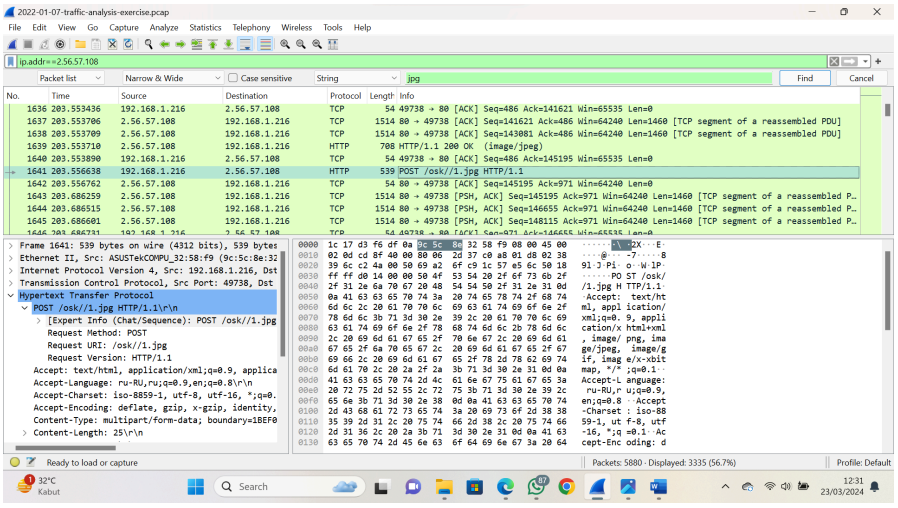
MAC address: 95:5c:8e:32:58:f9
IP address: 192.168.1.216
Host name: DESKTOP-GXMYNO2
Windows user account: steve.smith



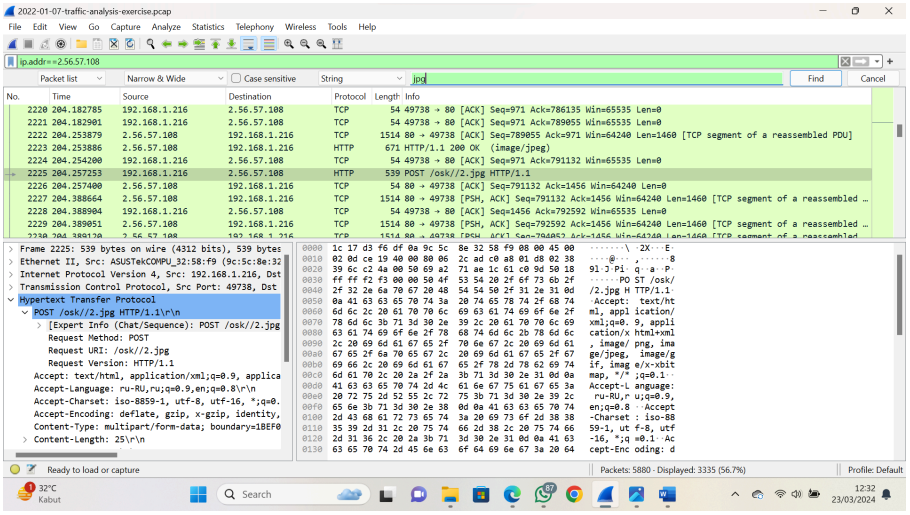
Indicators of Compromise (IOCs)

Malicious traffic:

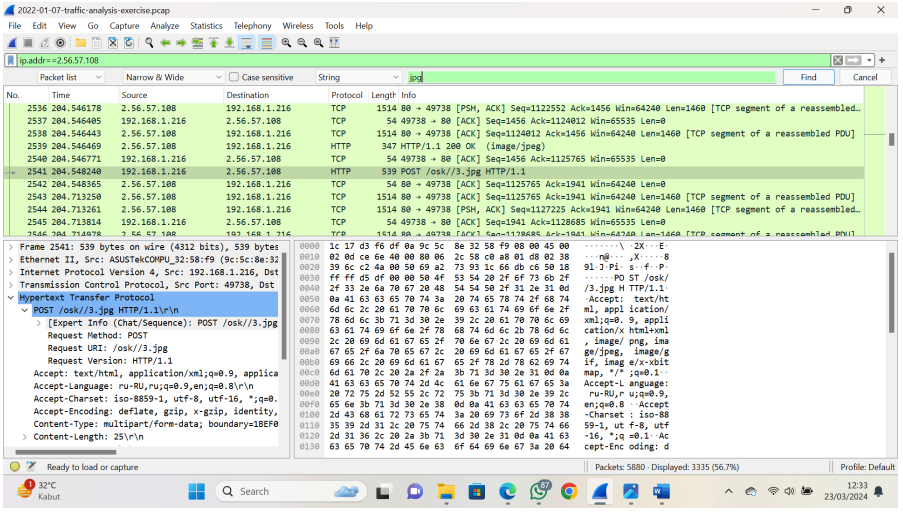
2.56.57.108 port 80 - 2.56.57.108 - POST /osk//1.jpg HTTP/1.1



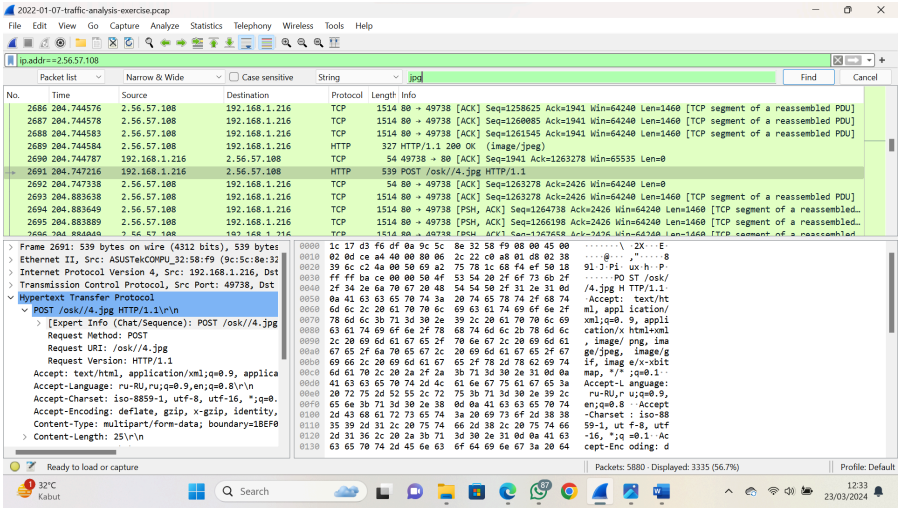
2.56.57.108 port 80 - 2.56.57.108 - POST /osk//2.jpg HTTP/1.1



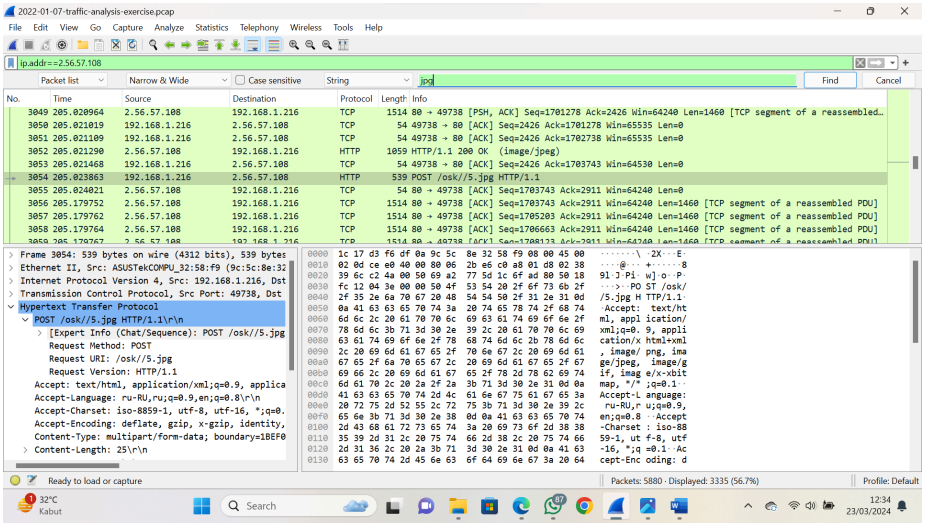
2.56.57.108 port 80 - 2.56.57.108 - POST /osk//3.jpg HTTP/1.1



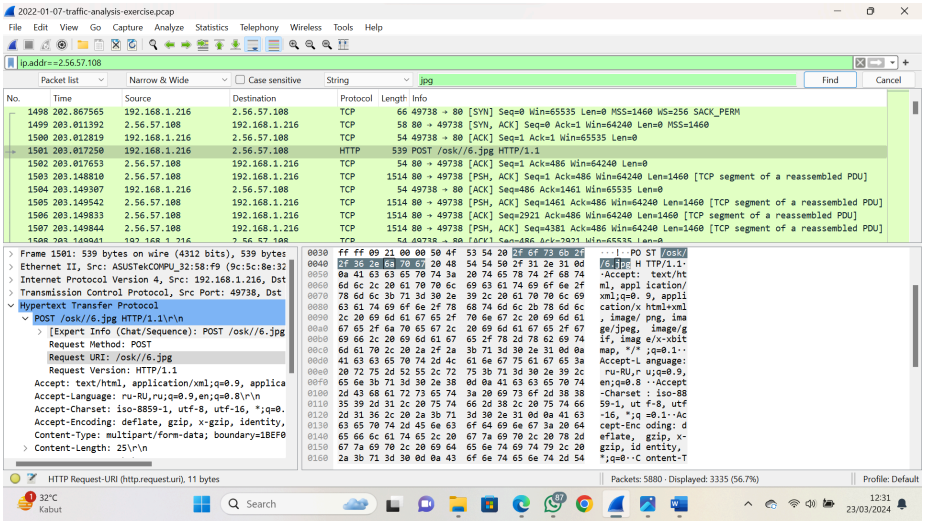
2.56.57.108 port 80 - 2.56.57.108 - POST /osk//4.jpg HTTP/1.1



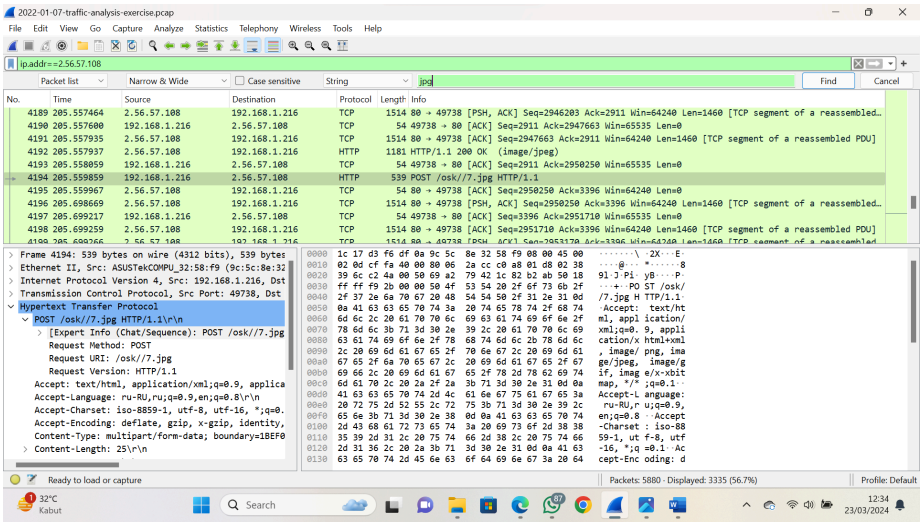
2.56.57.108 port 80 - 2.56.57.108 - POST /osk//5.jpg HTTP/1.1



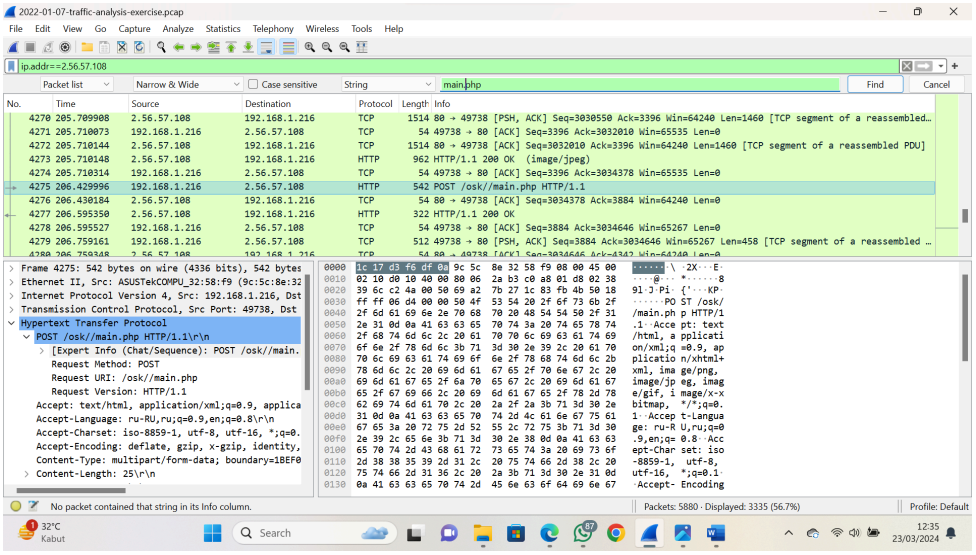
2.56.57.108 port 80 - 2.56.57.108 - POST /osk//6.jpg HTTP/1.1



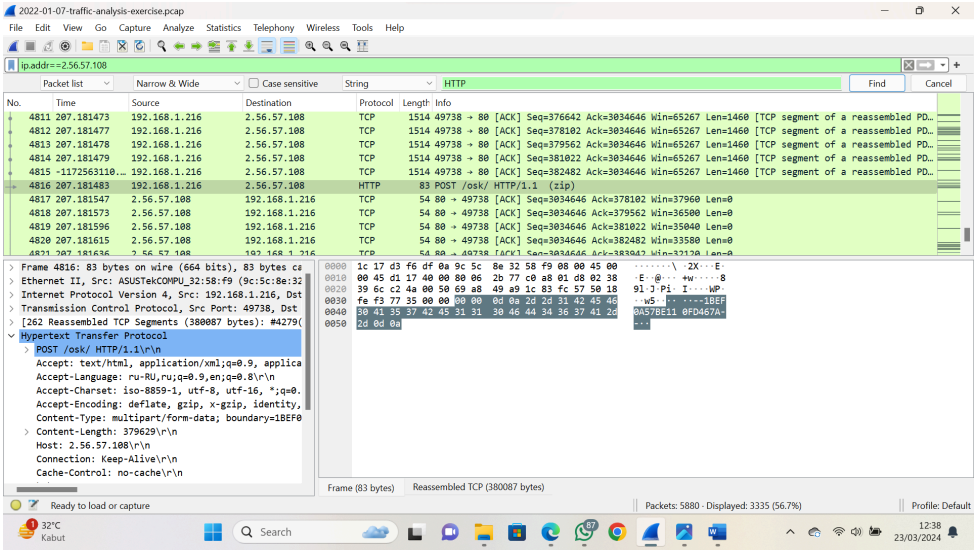
2.56.57.108 port 80 - 2.56.57.108 - POST /osk//7.jpg HTTP/1.1



2.56.57.108 port 80 - 2.56.57.108 - POST /osk//main.php HTTP/1.1



2.56.57.108 port 80 - 2.56.57.108 - POST /osk/ HTTP/1.1 (zip)



2022-03-21-TRAFFIC ANALYSIS EXERCOSE ANSWERS

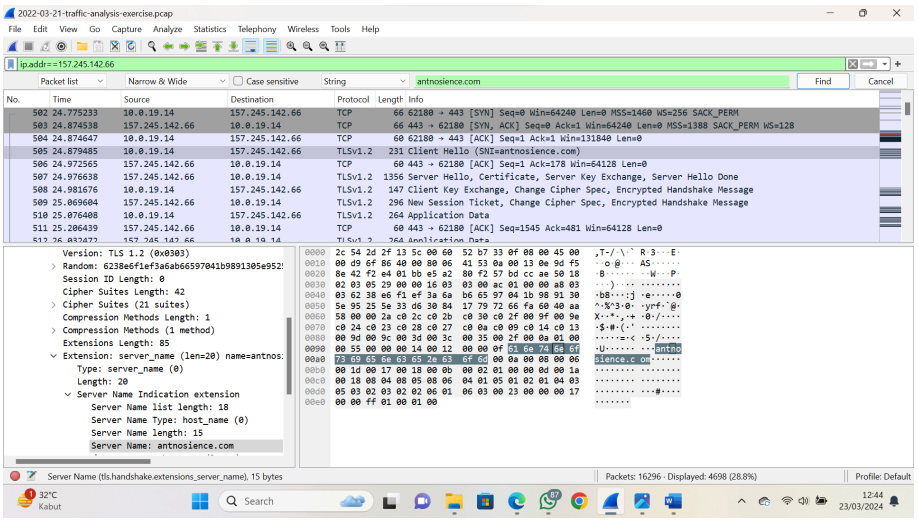
Executive Summary:
On Monday 2022-03-21 at approximately 20:58 UTC, a Windows host used by Patrick Zimmerman was infected with IcedID (Bokbot) malware that led to Cobalt Strike.

Details:
Host name: DESKTOP-5QS3D5D
IP address: 10.0.18.14
MAC address: 00:60:52:b7:33:0f
Windows user account name: patrick.zimmerman

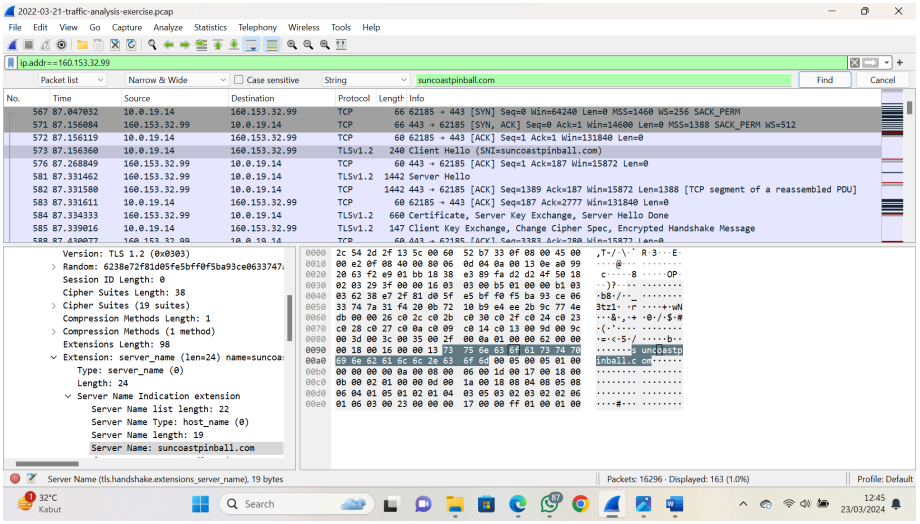
Indicators of Compromise (IOCs):
Domains and IP addresses for IcedID (Bokbot):
188.166.154.118 port 80 - oceriesfornot.top - GET /

188.166.154.118	215	0,0000	1,40%	0,0400	0,676
TCP	215	0,0000	100,00%	0,0400	0,676
80	215	0,0000	100,00%	0,0400	0,676
oceriesfornot.top			1		0,0000
/			1		0,0000

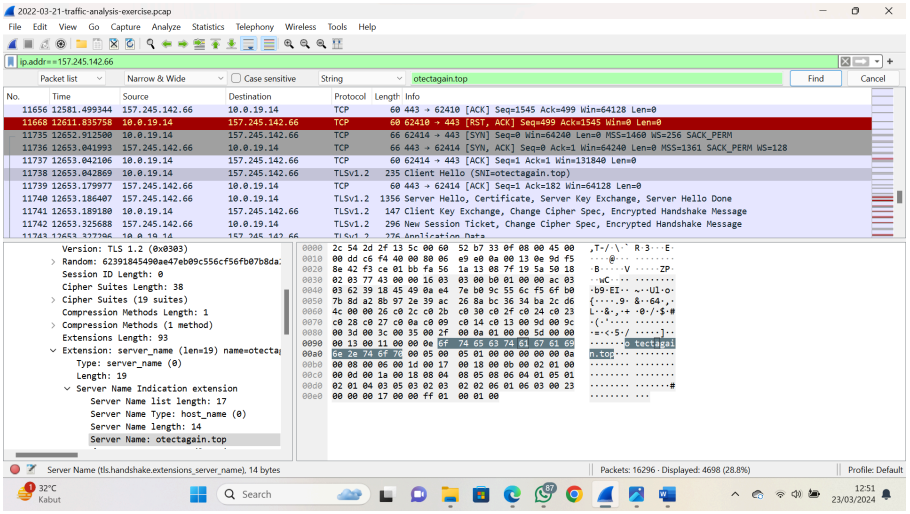
157.245.142.66 port 443 - antnosience.com - HTTPS traffic



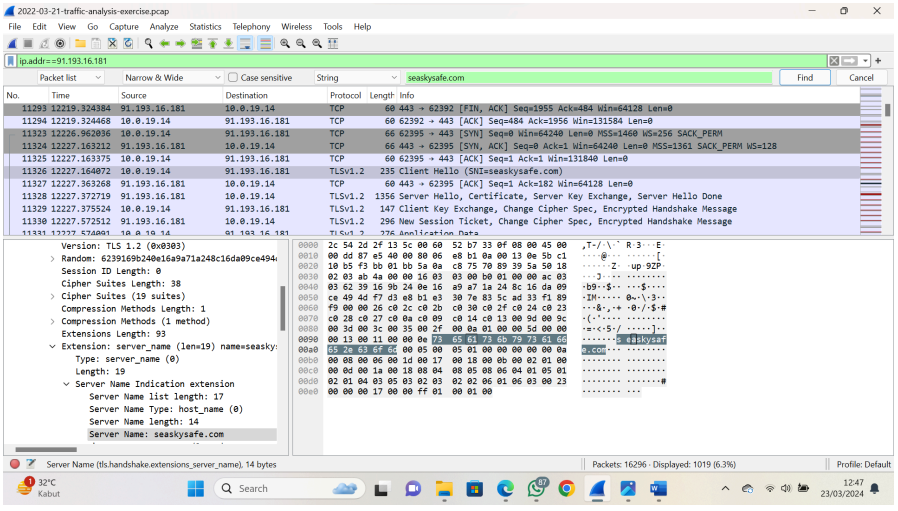
160.153.32.99 port 443 - suncoastpinball.com - HTTPS traffic



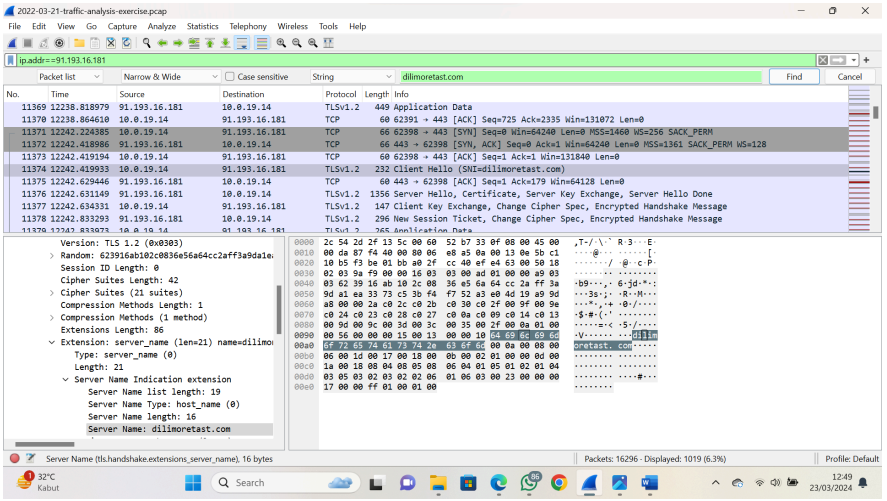
157.245.142.66 port 443 - otectagain.top - HTTPS traffic



91.193.16.181 port 443 - seaskysafe.com - HTTPS traffic

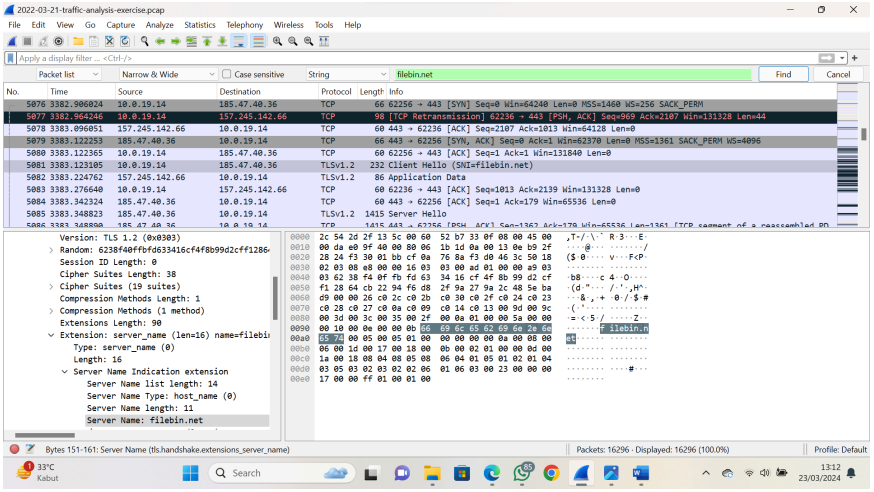


91.193.16.181 port 443 - dilimoretast.com - HTTPS traffic

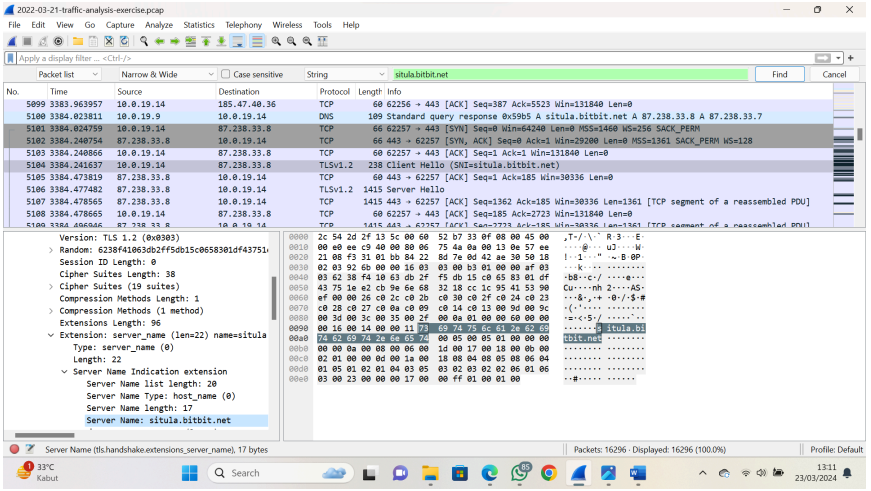


Suspicious traffic to file sharing domains:

port 443 - filebin.net - HTTPS traffic

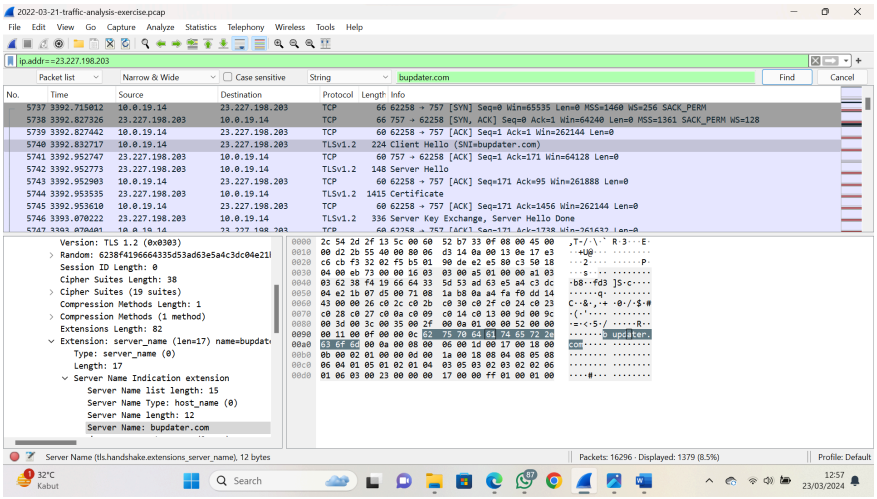


port 443 - situla.bitbit.net - HTTPS traffic



Domains and IP addresses for Cobalt Strike:

23.227.198.203 port 757 - bupdater.com - HTTPS traffic

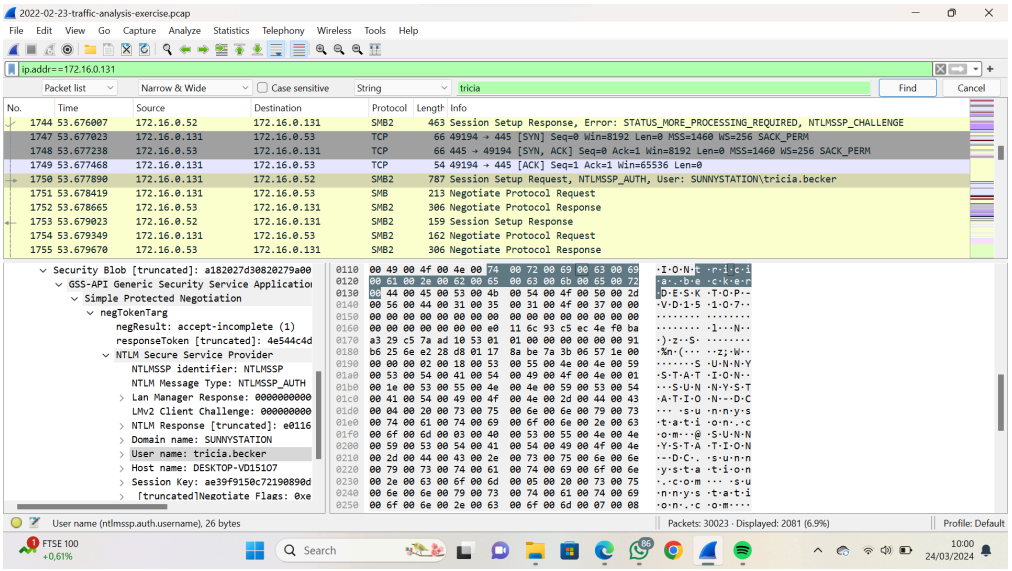


2022-02-23-TRAFFIC ANALYSIS EXERCOSE ANSWERS

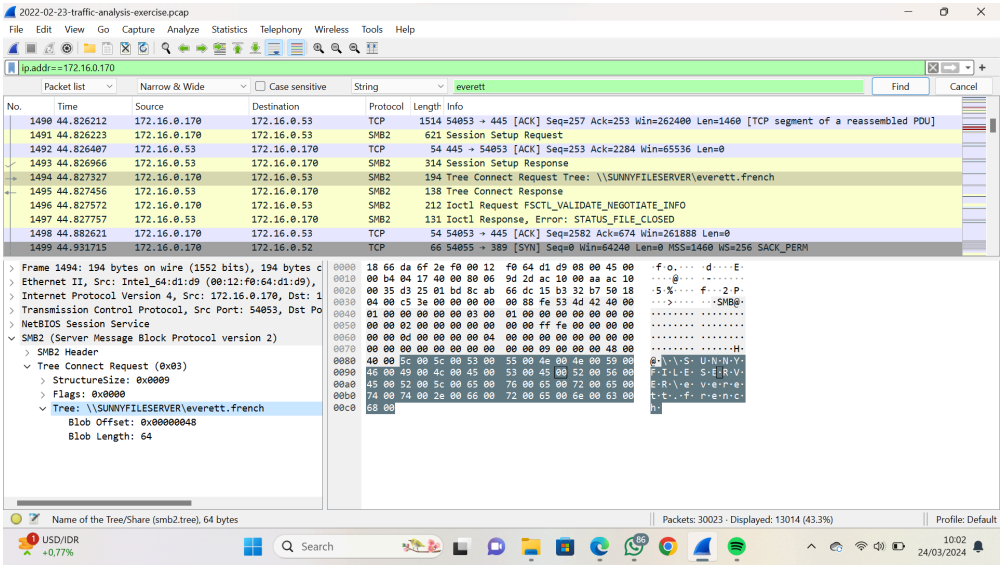
Hosts/usernames

(Read: MAC address - IP address - host name - Windows account name)

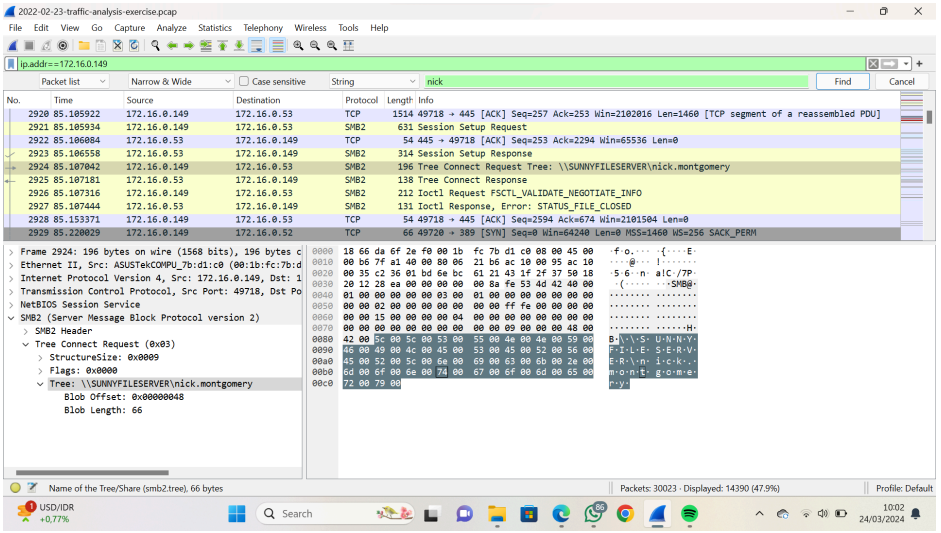
2c:27:d7:d2:06:f5 - 172.16.0.131 - DESKTOP-VD151O7 - tricia.becker



00:12:f0:64:d1:d9 - 172.16.0.170 - DESKTOP-W5TFTQY - everett.french



00:1b:fc:7b:d1:c0 - 172.16.0.149 - DESKTOP-KPQ9FDB - nick.montgomery



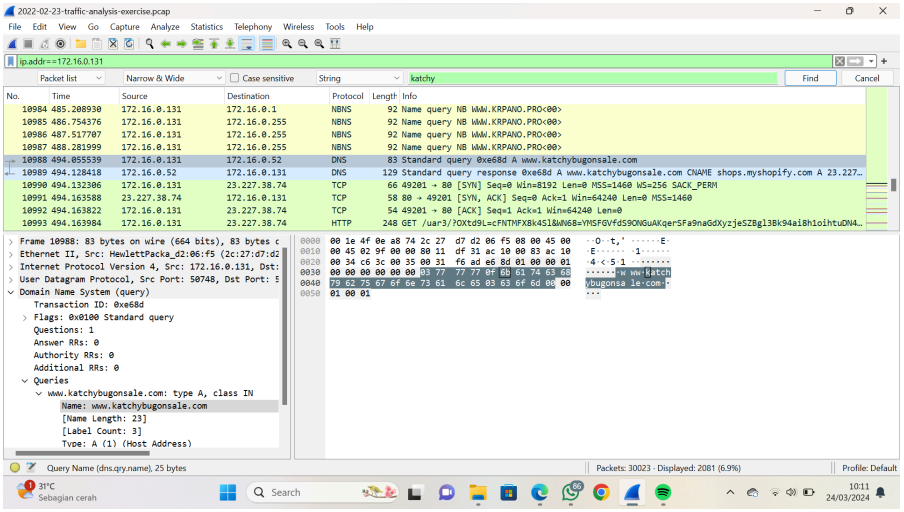
Malware infections:

(Read: IP address - malware infection - start date/time)

172.16.0.131 - Formbook (XLoader) - 2022-02-23 at 18:29 UTC

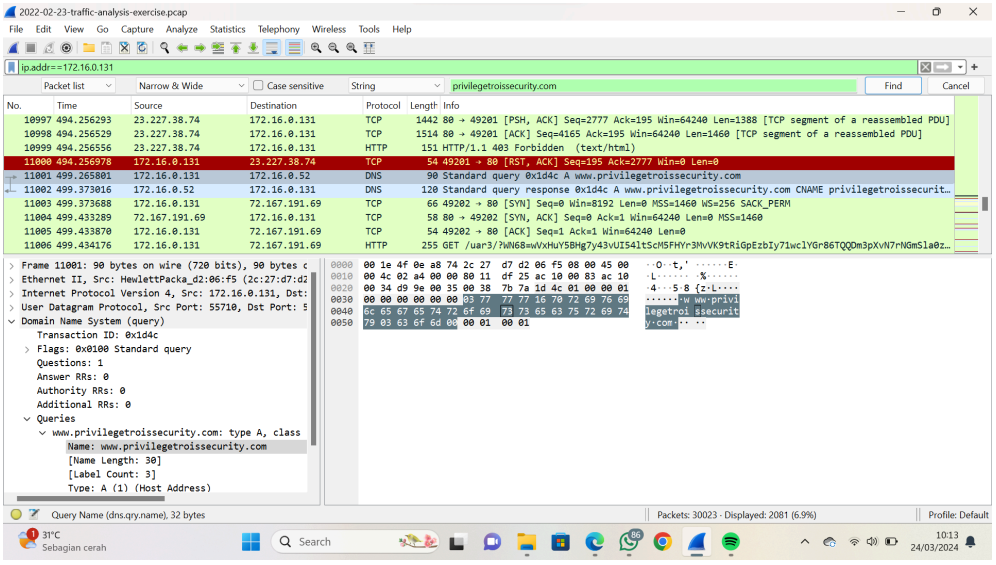
Formbook/XLoader C2 traffic:

23.227.38.74:80 - www.katchybugonsale.com - GET /uar3/?[base64 style string]



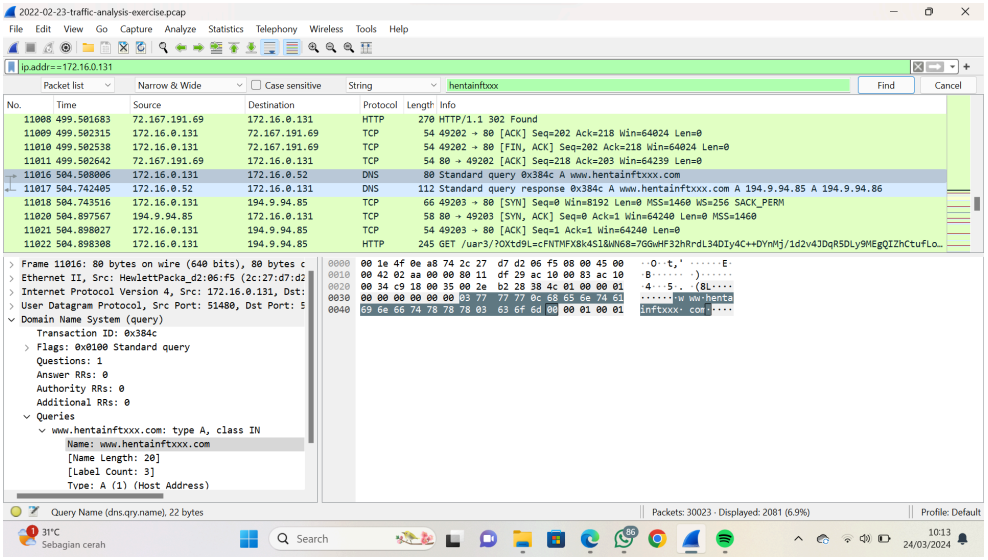

```
GET /uar3/?OXtd9L=cFNTMFX8k4Sl&WN68=YMSFGVfdS9ONGuAKqerSFa9naGdXyzjeSZBgl3Bk94ai8h1oihtuDN4qXdcs1YMbgxqWO7UijFru
1VtwMrj0Yg== HTTP/1.1
Host: www.katchybugonsale.com
Connection: close
```

72.167.191.69:80 - www.privilegetroissecurity.com - GET /uar3/?[base64 style string]



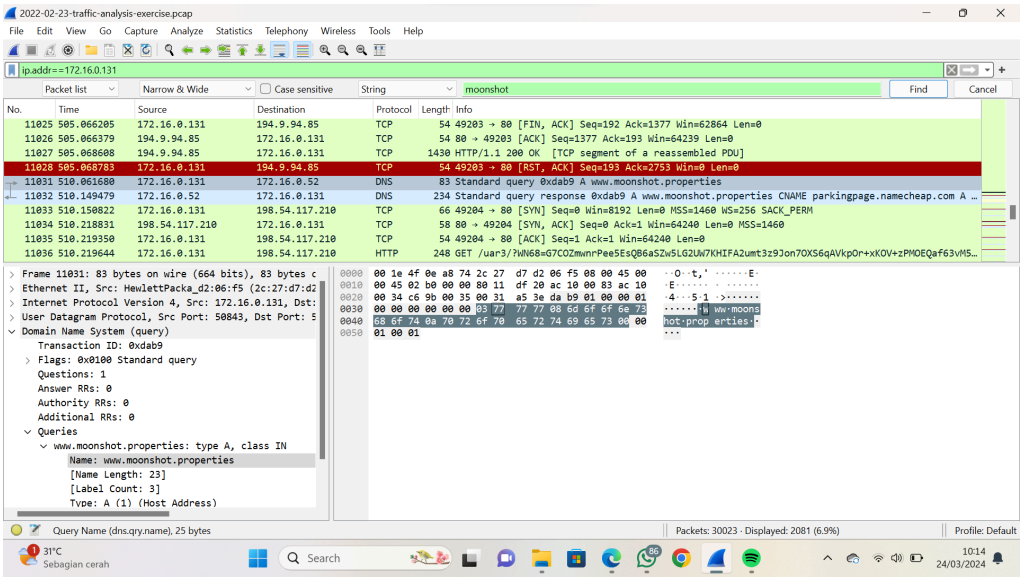

```
GET /uar3/?WN68=wVxHuY5BHg7y43vUI54ltScM5FHYr3MvVK9tRiGpEzbIy71wclYGr86TQQDm3pXvN7rNGmSla0zZHvUrNEOd8Q==&OXtd9L=cF
NTMFX8k4Sl HTTP/1.1
Host: www.privilegetroissecurity.com
Connection: close
```

194.9.94.85:80 - www.hentainftxxx.com - GET /uar3/?[base64 style string]



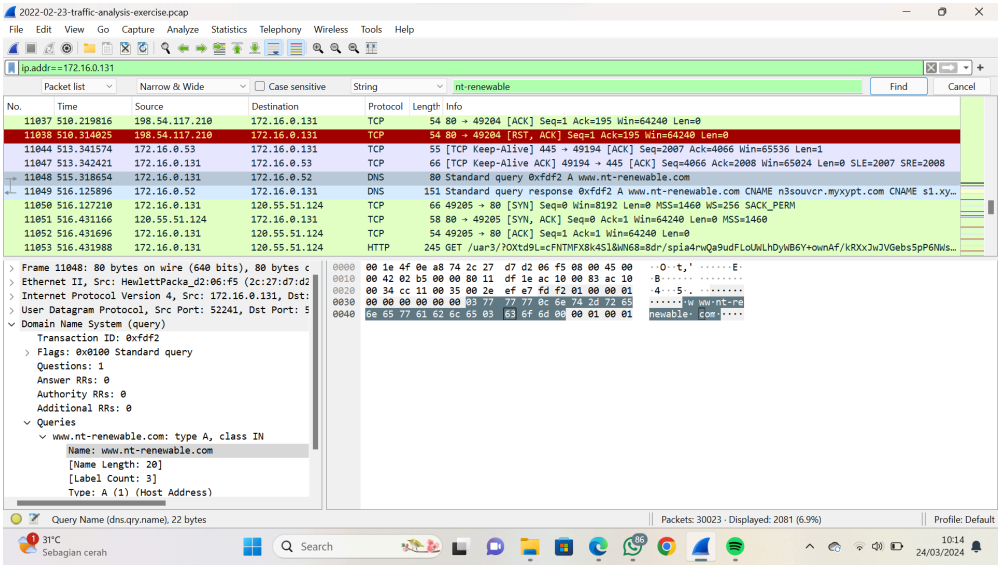

```
GET /uar3/?OXtd9L=cFNTMFX8k4Sl&WN68=7GGwHF32hRrdL34DIy4C++DYnMj/1d2v4JDqR5DLy9MEgQIZhCtufLoZXudHqPtA4E9sAhQJ5Izw
CvVbNJKdoQ== HTTP/1.1
Host: www.hentainftxxx.com
Connection: close
```

198.54.117.210:80 - www.moonshot.properties - GET /uar3/?[base64 style string]



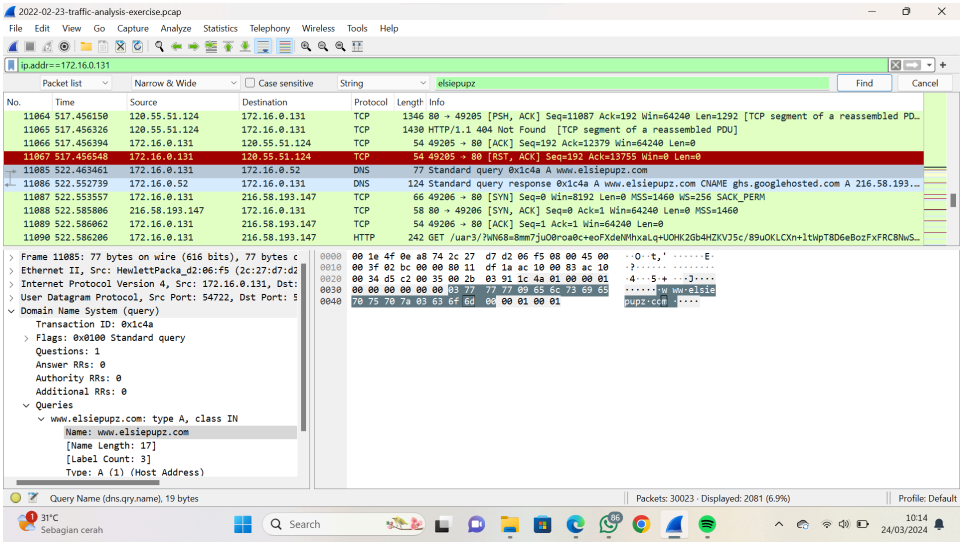

```
GET /uar3/?WN68=G7COZmwnrPee5EsQB6aSZw5LG2UW7KHIFA2umt3z9Jon7OXS6qAVkpOr+xKOV+zPMOEQaf63vM5y0TRfGLX9kw==&OXtd9L=cF
NTMFX8k4Sl HTTP/1.1
Host: www.moonshot.properties
Connection: close
```

120.55.51.124:80 - www.nt-renewable.com - GET /uar3/?[base64 style string]



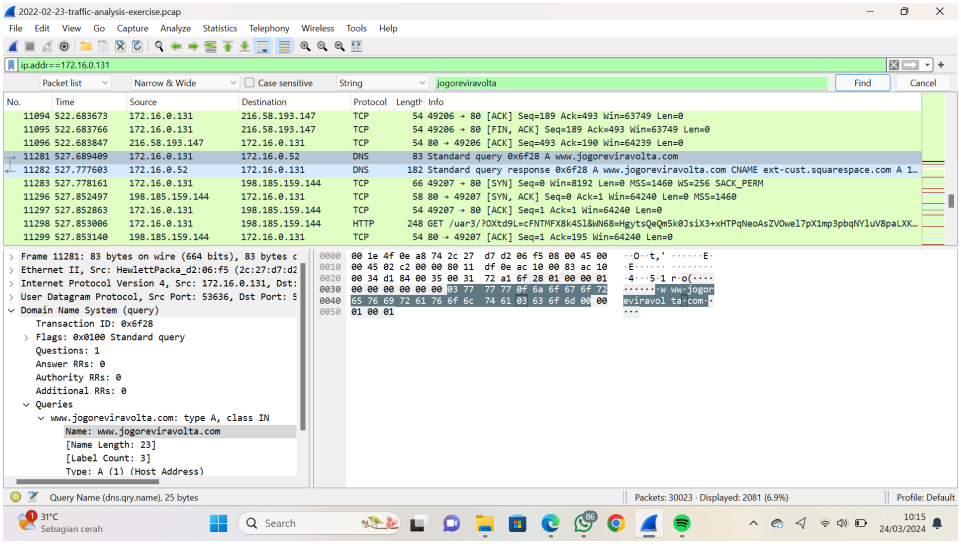

```
GET /uar3/?OXtd9L=cFNTMFX8k4Sl&WN68=8dr/spia4rwQa9udFLoUWLhDyWB6Y+ownAf/kRXxJwJVGebs5pP6NWs1hg+O5/59UnRkE2LClKUd
c3S/D+UP/w== HTTP/1.1
Host: www.nt-renewable.com
Connection: close
```

216.58.193.147:80 - www.elsiepupz.com - GET /uar3/?[base64 style string]



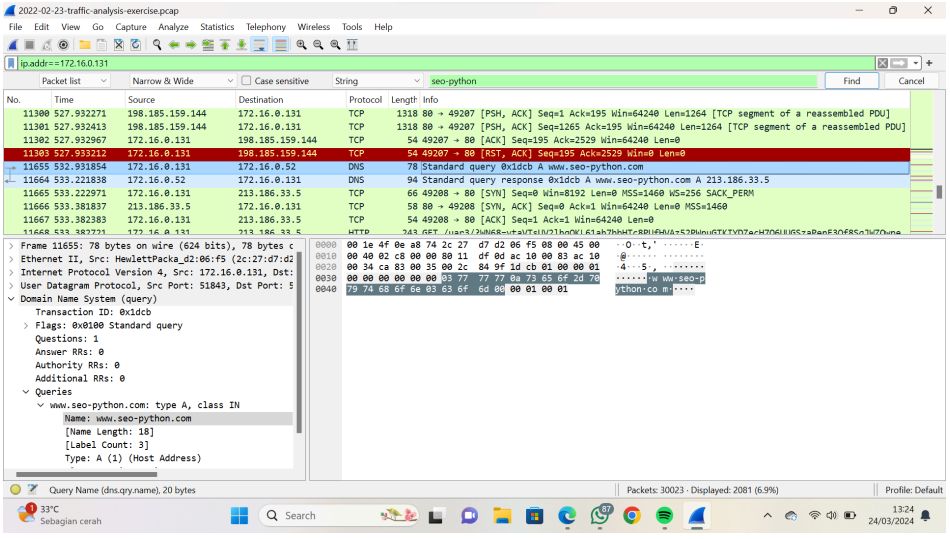

```
GET /uar3/?WN68=8mm7juO0roa0c+eoFXdeNMhxaLq+UOHK2Gb4HZKVJ5c/89uOKLCXn+ltWpT8D6eBozFxFRC8NwSE5MNPGjBvbw==&OXtd9L=cF
NTMFX8k4Sl HTTP/1.1
Host: www.elsiepupz.com
Connection: close
```

198.185.159.144:80 - www.jogoreviravolta.com - GET /uar3/?[base64 style string]



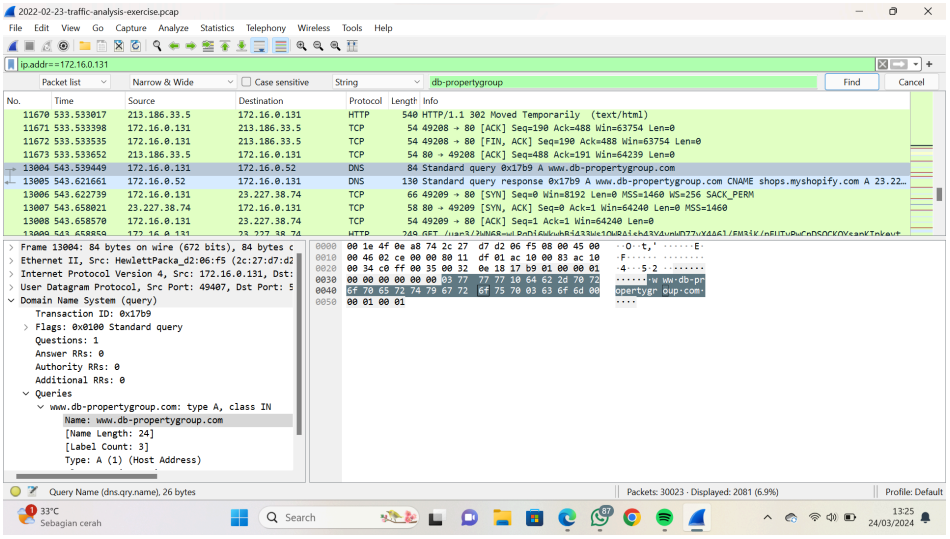

```
GET /uar3/?OXtd9L=cFNTMFX8k4Sl&WN68=HgytsQeQm5k0JsiX3+xHTPqNeoAsZVOwel7pX1mp3pbqNY1uV8paLXKGPRTm0h2A1X7YRo+hCzAHabyaXGya1Q== HTTP/1.1
Host: www.jogoreviravolta.com
Connection: close
```

213.186.33.5:80 - www.seo-python.com - GET /uar3/?[base64 style string]

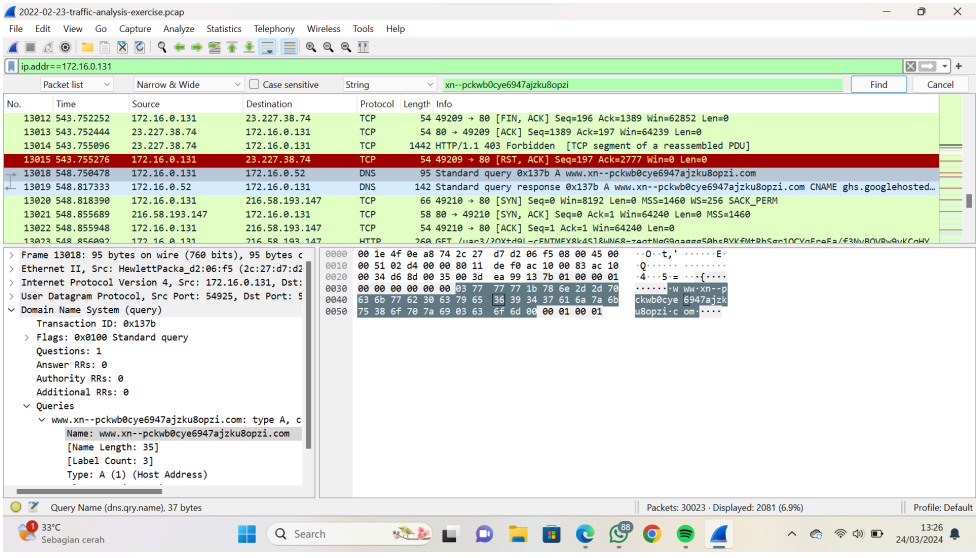



```
GET /uar3/?WN68=ytaVTsUV2lhqQKL61ah7bbHTc8PUfHVAz52PWpuGTKIYDZecH7Q6UUGSzaPenE3Of8SqJWZQwpeASzStGycgxA==&OXtd9L=cFNTMFX8k4Sl HTTP/1.1
Host: www.seo-python.com
Connection: close
```

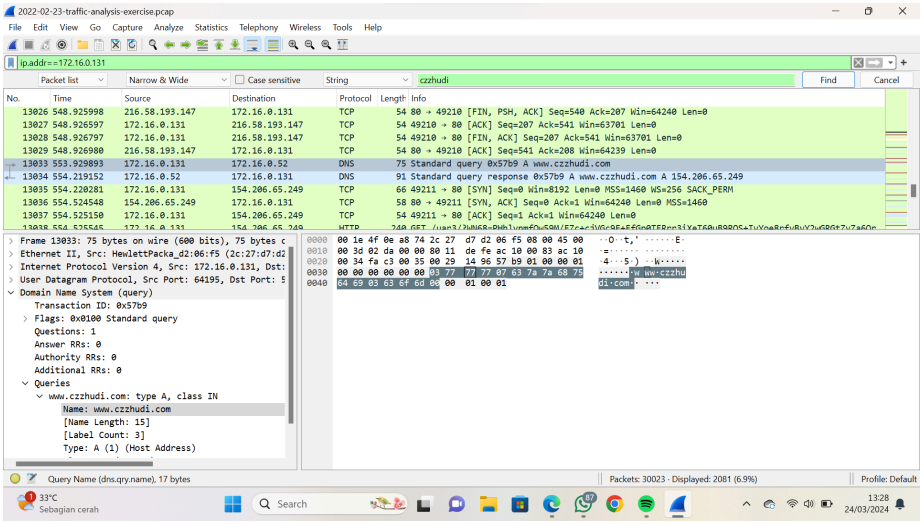
23.227.38.74:80 - www.db-propertygroup.com - GET /uar3/?[base64 style string]



216.58.193.147:80 - www.xn--pckwb0cye6947ajzku8opzi.com - GET /uar3/?[base64 style string]

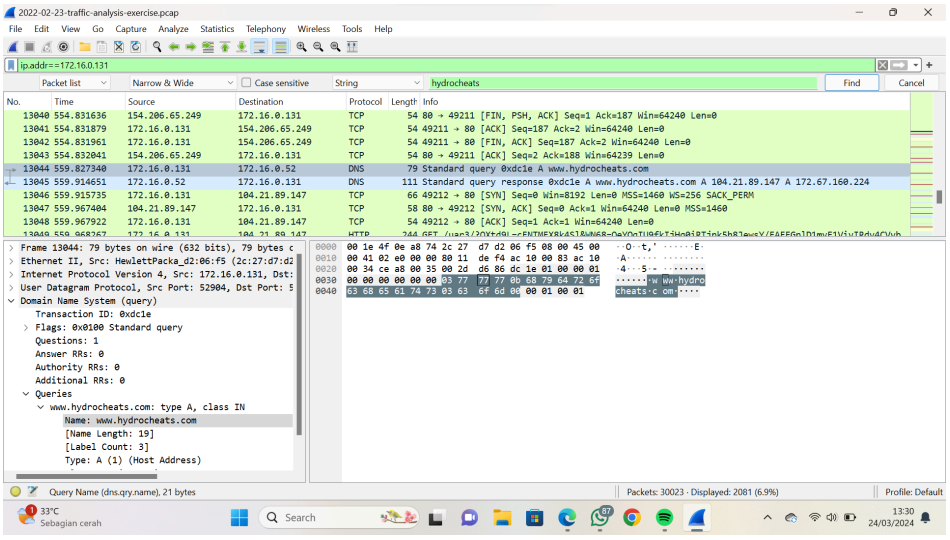


154.206.65.249:80 - www.czzhudi.com - GET /uar3/?[base64 style string]



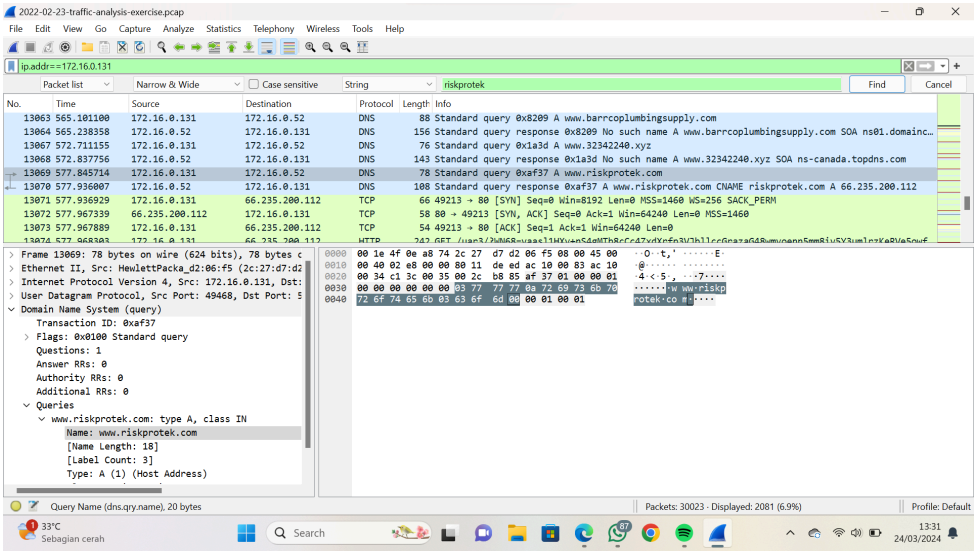

```
GET /uar3/?WN68=PHhlvnmfOw59M/FZc+cjVGc9E+FfGp0TERrr3iXeT60uB9RQS+IvYoe8rfvBvY2wGRGtZyZa6OrSqVXvPAs7JA==&OXtd9L=cF
NTMFX8k4Sl HTTP/1.1
Host: www.czzhudi.com
Connection: close
```

104.21.89.147:80 - www.hydrocheats.com - GET /uar3/?[base64 style string]



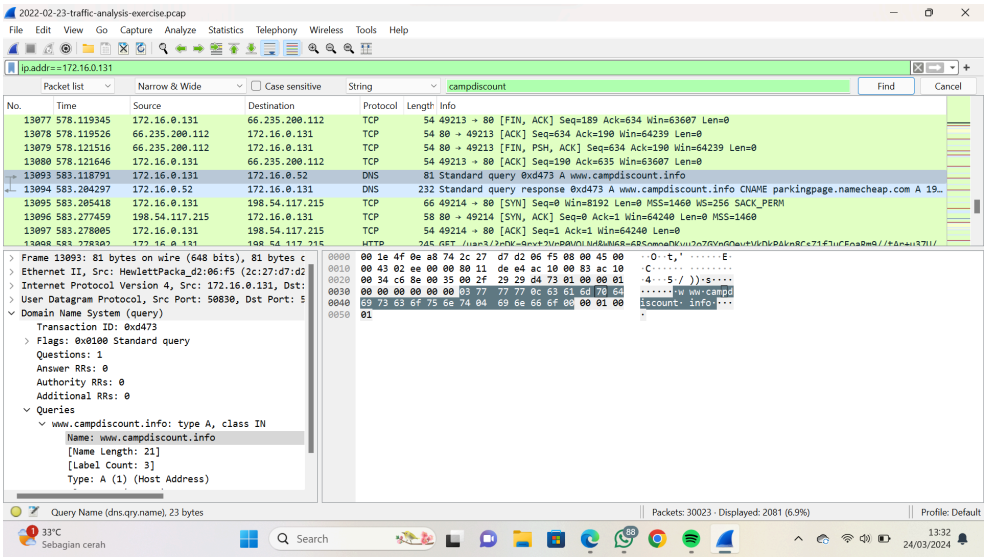

```
GET /uar3/?OXtd9L=cFNTMFX8k4Sl&WN68=OeYQqIU9fkIjHq0iRTjpk5h8JewsY/FAEEGplD1myE1VivIRdy4CVvbuzuyXb7LJfyhf2G3tozH0
TabGGRXNyg== HTTP/1.1
Host: www.hydrocheats.com
Connection: close
```

66.235.200.112:80 - www.riskprotek.com - GET /uar3/?[base64 style string]



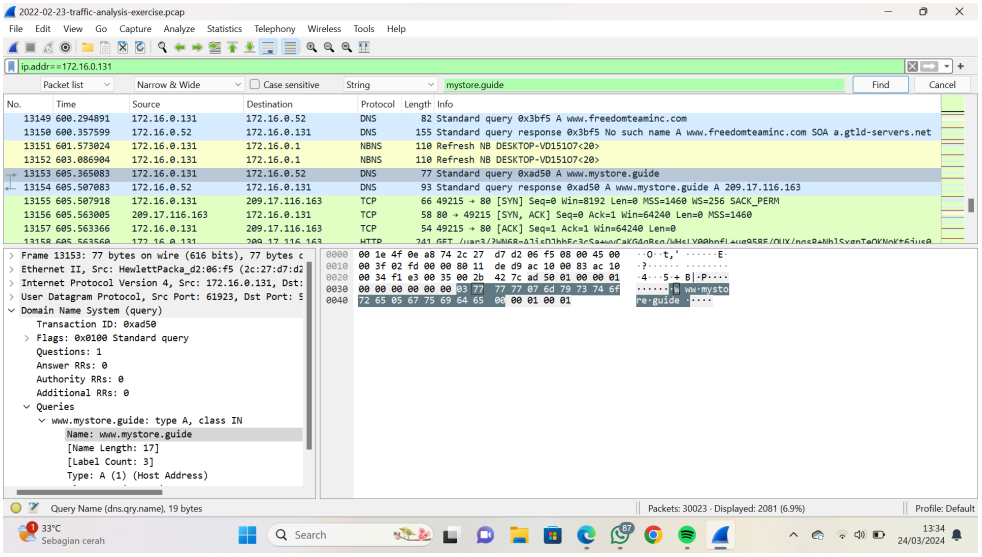

```
GET /uar3/?WN68=vaasl1HXy+nS4gMTb8cCc4ZxdXrfp3VJbllccGrazaG48wmyoenn5mm8iv5Y3umlrzKeRVe5owfjDaqVto7ySQ==&rDK=9rxt2
VrP0VOLNd HTTP/1.1
Host: www.riskprotek.com
Connection: close
```

198.54.117.215:80 - www.campdiscount.info - GET /uar3/?[base64 style string]



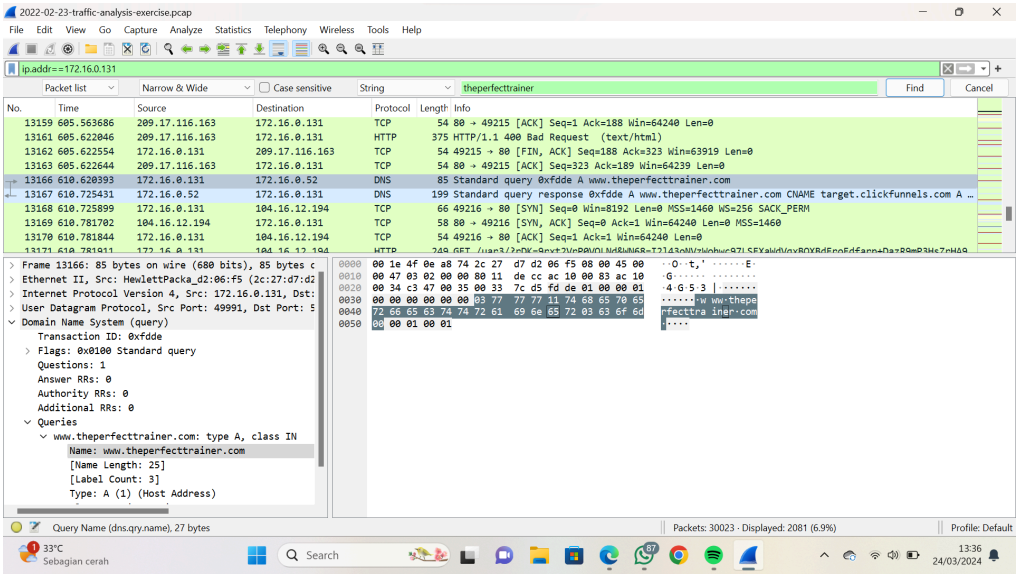

```
GET /uar3/?rDK=9rxt2VrP0VOLNd&WN68=6RSomoeDKvu2oZGYnGQevtVkDkPAkn8CsZ1fJuCFoaRm9//tAr+u37U/QCD2qVC/dAHjd57BD2t/Oxw
5fT4Nlw== HTTP/1.1
Host: www.campdiscount.info
Connection: close
```

209.17.116.163:80 - www.mystore.guide - GET /uar3/?[base64 style string]



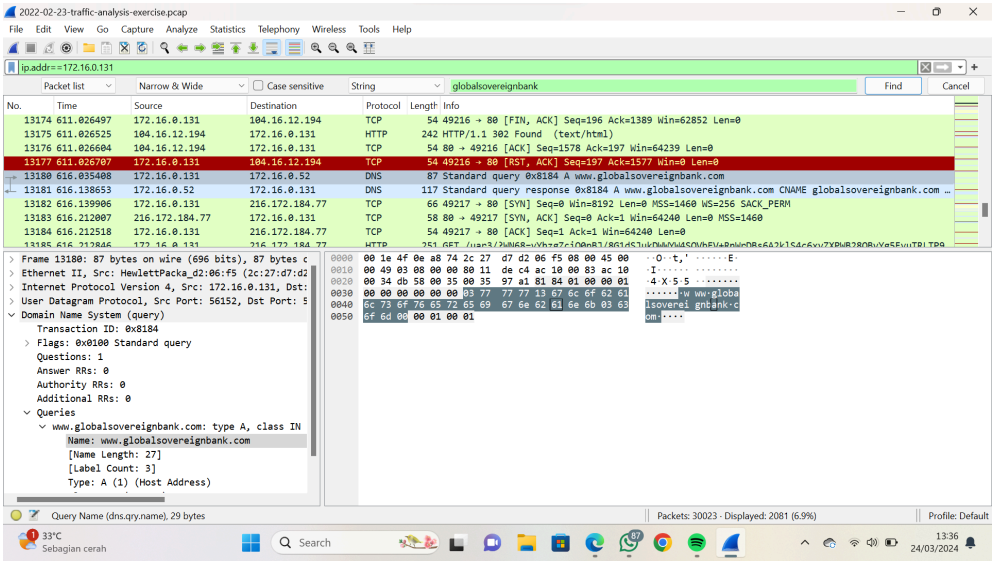

```
GET /uar3/?WN68=AJisDJhbFc3cSa+wvCaKG4qBsq/WHsLY00hpfL+ug958E/QUX/nqsR+NhlSxgpTeQKNoKt6jus0BQP11eAYtlQ==&rDK=9rxt2
VrP0VOLNd HTTP/1.1
Host: www.mystore.guide
Connection: close
```

104.16.12.194:80 - www.theperfecttrainer.com - GET /uar3/?[base64 style string]



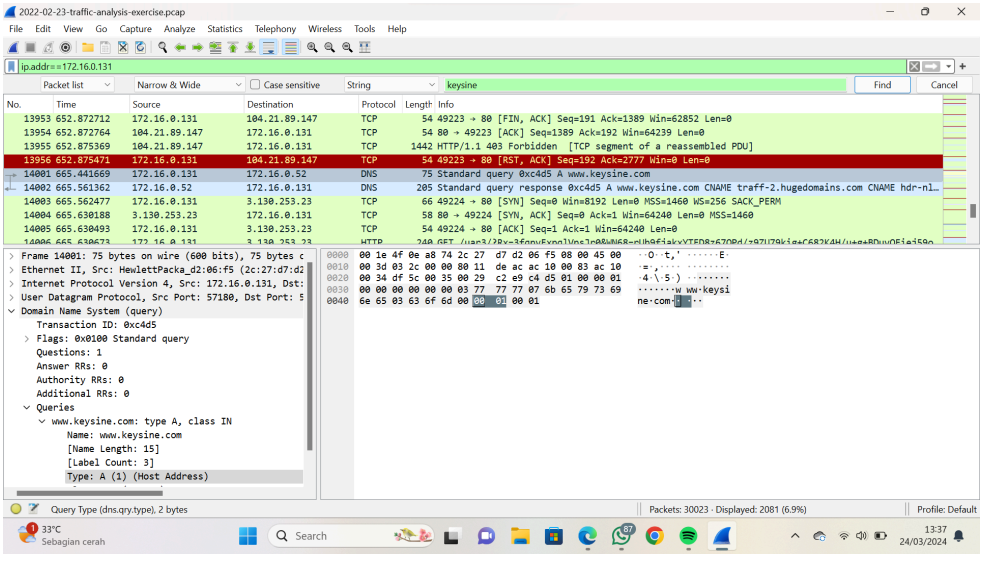

```
GET /uar3/?rDK=9rxt2VrP0VOLNd&WN68=I2l43oNVzWohwc97LSEXaWdVqxBOXBdEroFdfarp+DazR9mP3HsZrHA9P20czBHo7A9Q6BtLZHoFB
Mxs+Q0aUA== HTTP/1.1
Host: www.theperfecttrainer.com
Connection: close
```

216.172.184.77:80 - www.globalsovereignbank.com - GET /uar3/?[base64 style string]



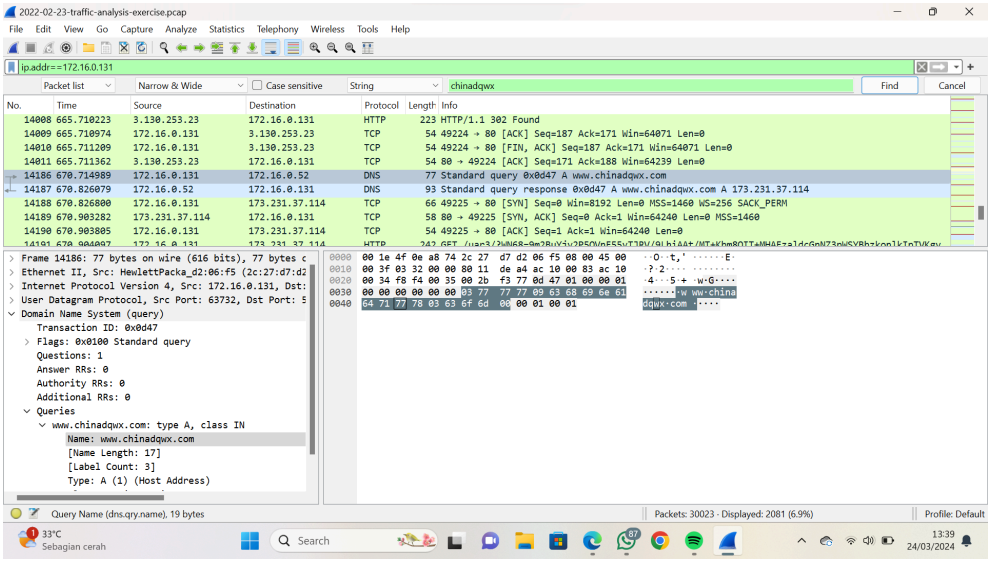

```
GET /uar3/?WN68=yYhzgZciQ0pBJ/8G1dSJukDWWYW4SQVbEV+RnWrDBs6A2klS4c6xvZXPWB28QBvYg5FyuTRLTP9+/gPb7Dyx9A==&rDK=9rxt2VrP0VOLNd HTTP/1.1
Host: www.globalsovereignbank.com
Connection: close
```

3.130.253.23:80 - www.keysine.com - GET /uar3/?[base64 style string]



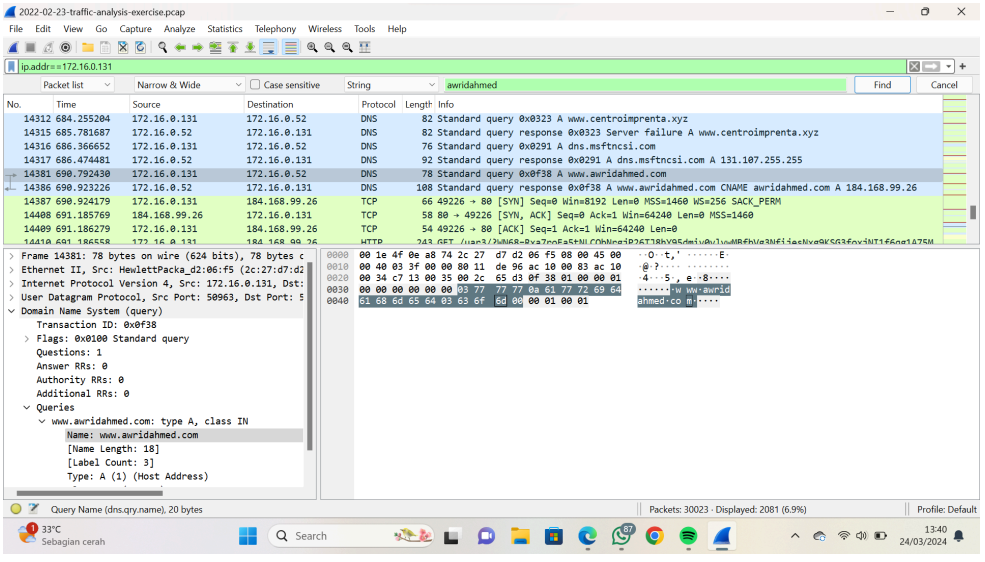

```
GET /uar3/?Rx=3fqpvFxpqlVpsJr0&WN68=rUb9fjakxYTFD8z67QPd/z9ZU79kig+C682K4H/u+g+BDuvQEiej59oCwTmjTn3VIgEsDrJTMHhelfjdUr/lOQ== HTTP/1.1
Host: www.keysine.com
Connection: close
```

173.231.37.114:80 - www.chinadqwx.com - GET /uar3/?[base64 style string]



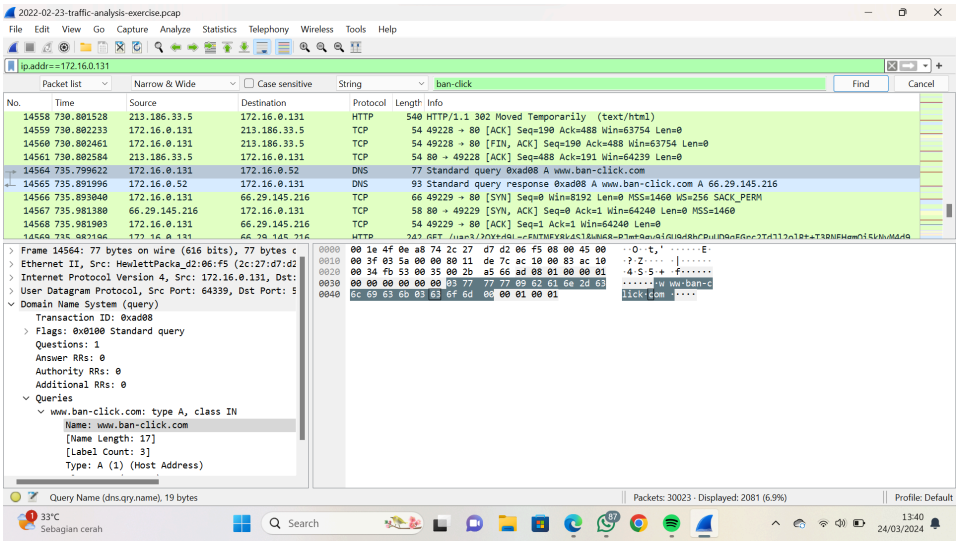

```
GET /uar3/?WN68=9m2BuYjy2P5QVnF55yTJRV/9LhiAAt/MT+Kbm8QIT+MHAFzaldcGnNZ3pWSYBbzkonlkIpTVKgvisutZzhPqOw==&Rx=3fqp
vFxpqlVpsJr0 HTTP/1.1
Host: www.chinadqwx.com
Connection: close
```

184.168.99.26:80 - www.awridahmed.com - GET /uar3/?[base64 style string]



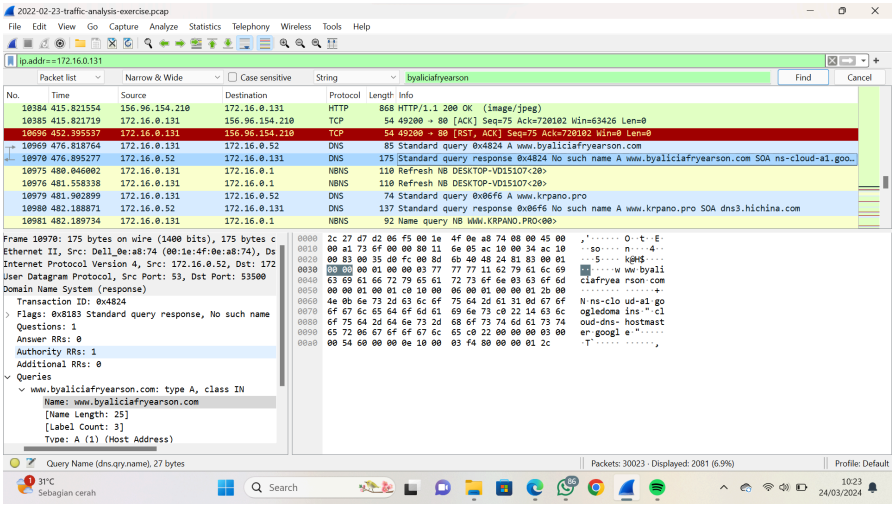

```
GET /uar3/?WN68=Rxa7roEa5tNLCQbNrgjP26TJ8hY95dmiy0vlywMBfbVg3NfijesNxg9KSG3foxjNI1f6qg1A75MBHEYl1CRNww==&Rx=3fqp
vFxpqlVpsJr0 HTTP/1.1
Host: www.awridahmed.com
Connection: close
```

66.29.145.216:80 - www.ban-click.com - GET /uar3/?[base64 style string]

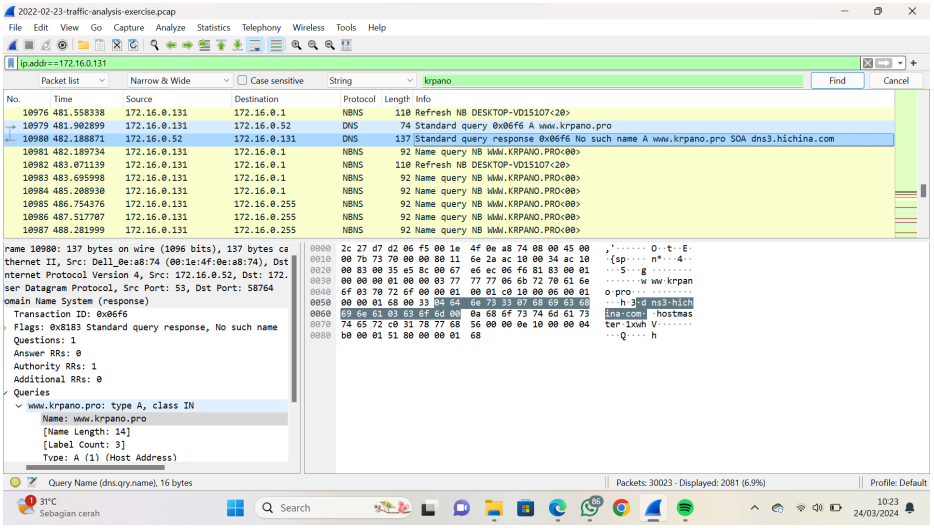



```
GET /uar3/?OXtd9L=cFNTMFX8k4Sl&WN68=PJmt9gv9iGU9d8hCPuUD9qFGrc2TdJl2olRt+T3RNFHgmOi5kNyM4d9HjU8Ipcbb+g/FLincIuHx0S
3I0xIWfw== HTTP/1.1
Host: www.ban-click.com
Connection: close
```

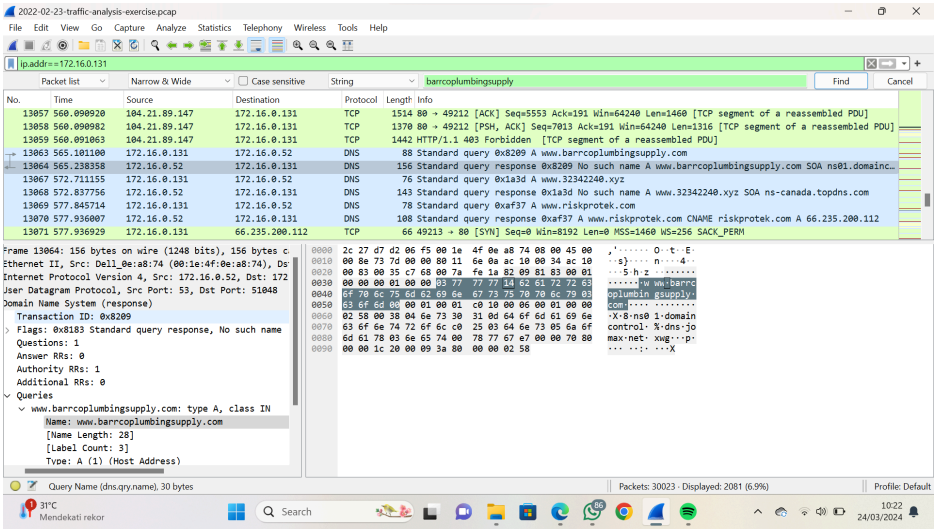
DNS queries for Formbook/XLoader C2 traffic:
www.byaliciafryearson.com - response: No such name



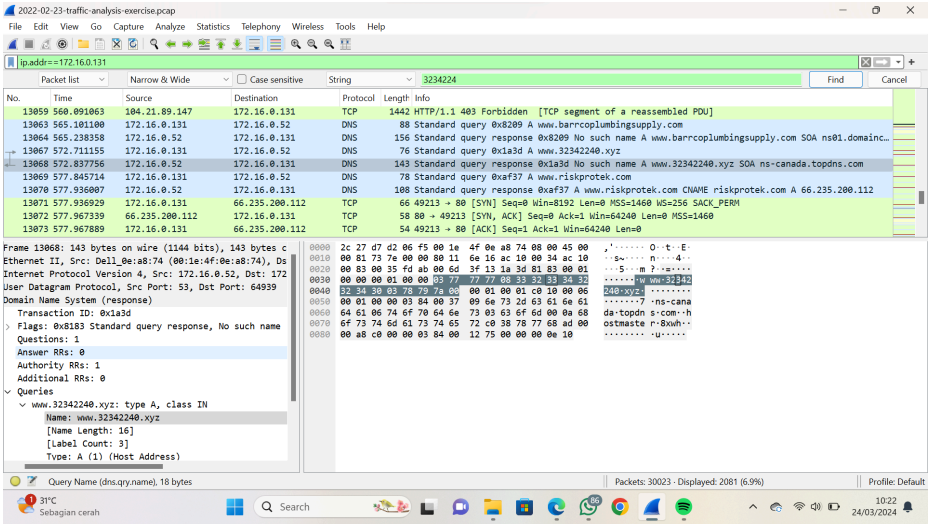
www.krpano.pro - response: No such name



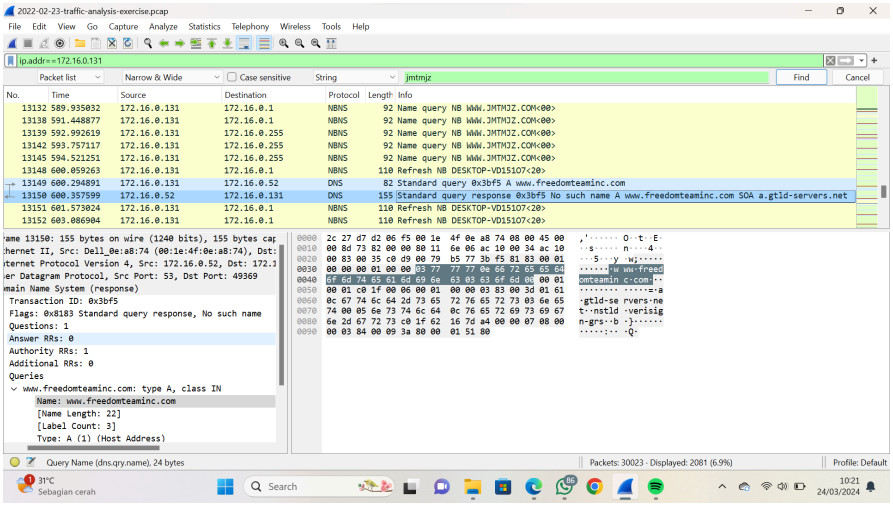
www.barrcoplumbingsupply.com - response: No such name



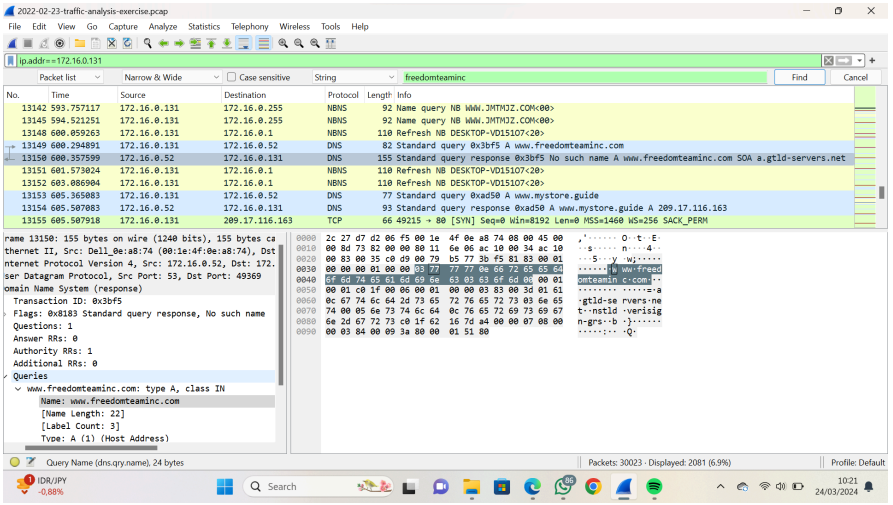
www.32342240.xyz - response: No such name



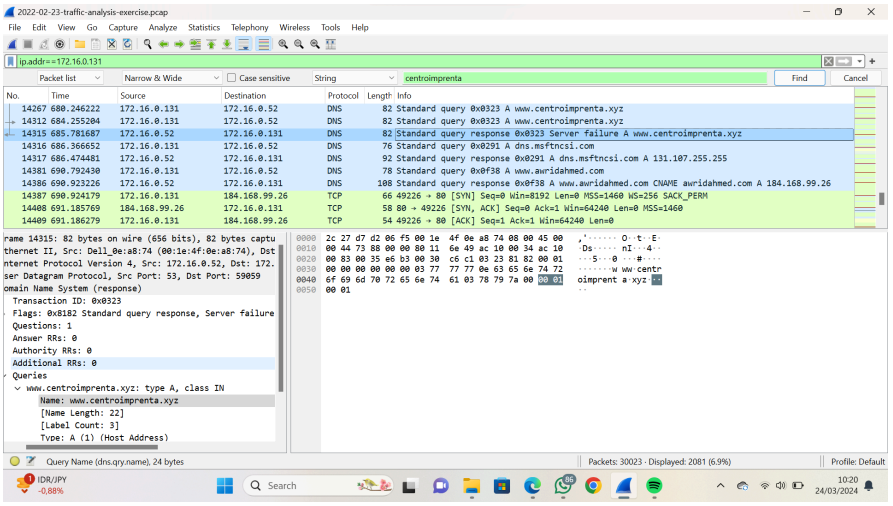
www.jmtmjz.com - response: No such name



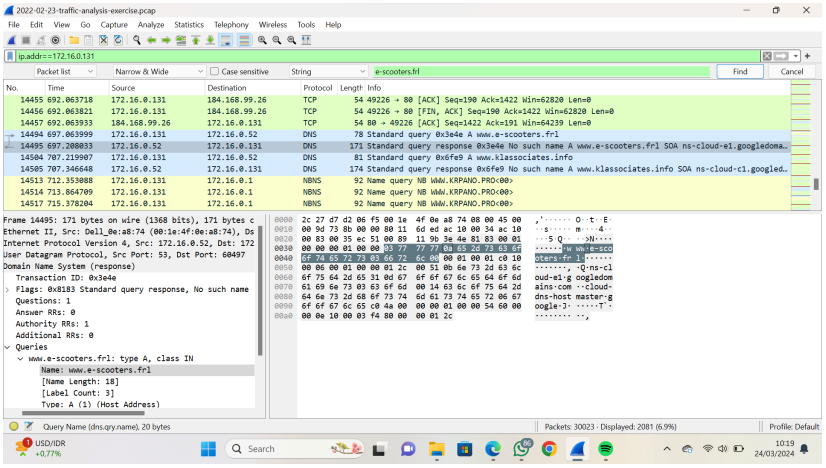
www.freedomteaminc.com - response: No such name



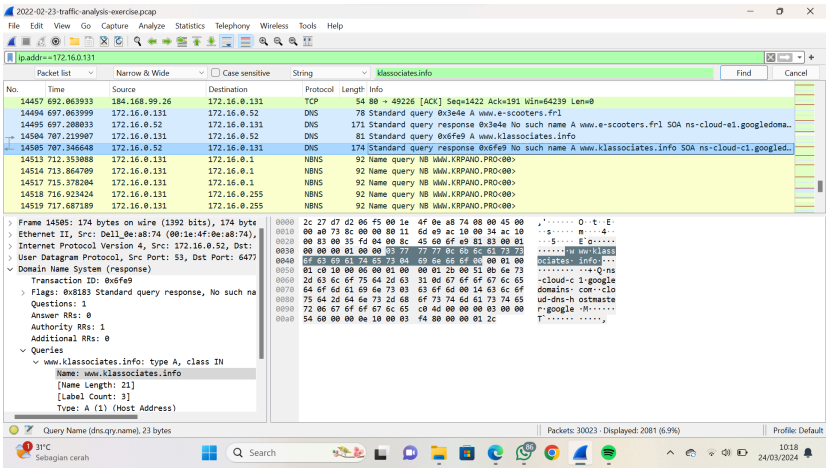
www.centroimprenta.xyz - response: Server failure



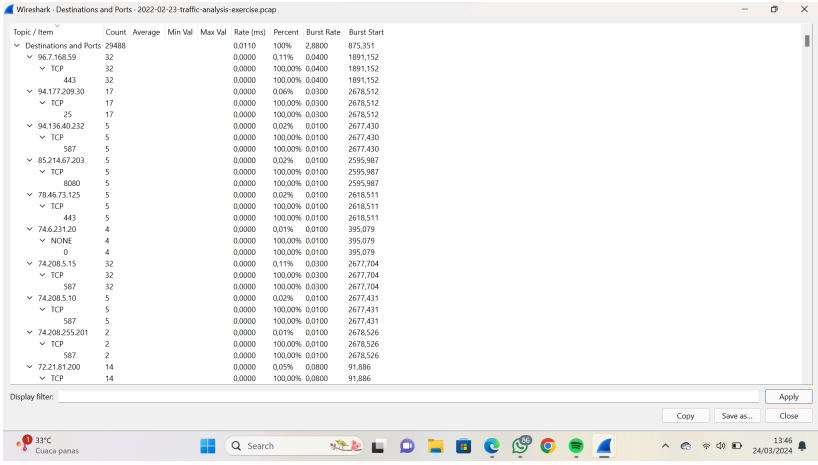
www.e-scooters.frl - response: No such name

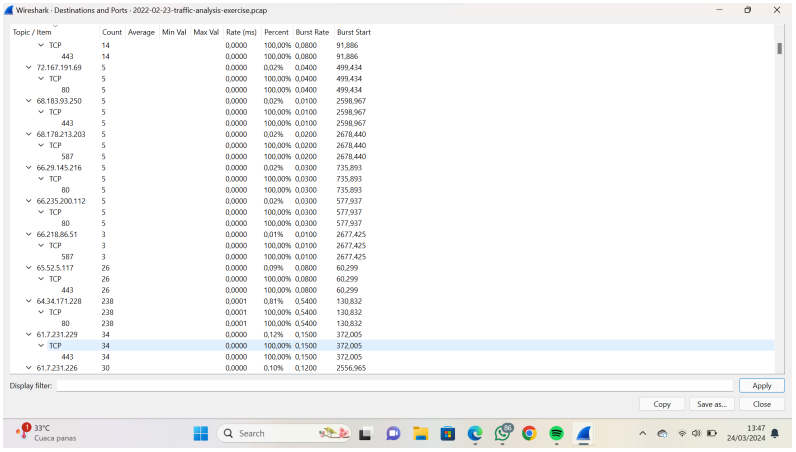


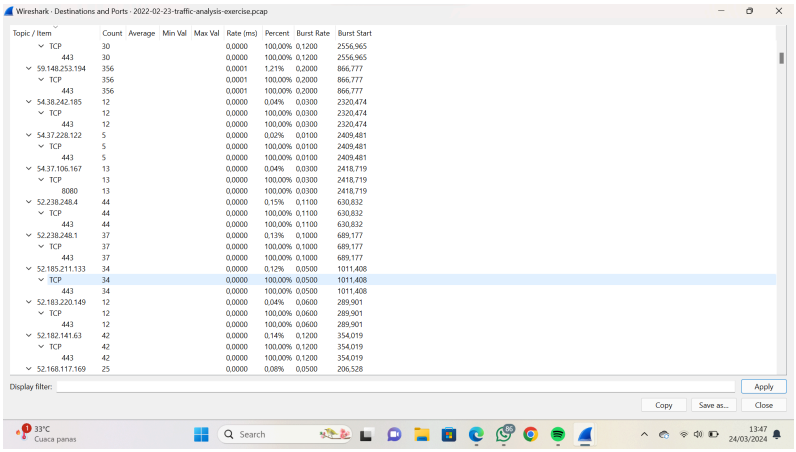
www.klassociates.info - response: No such name

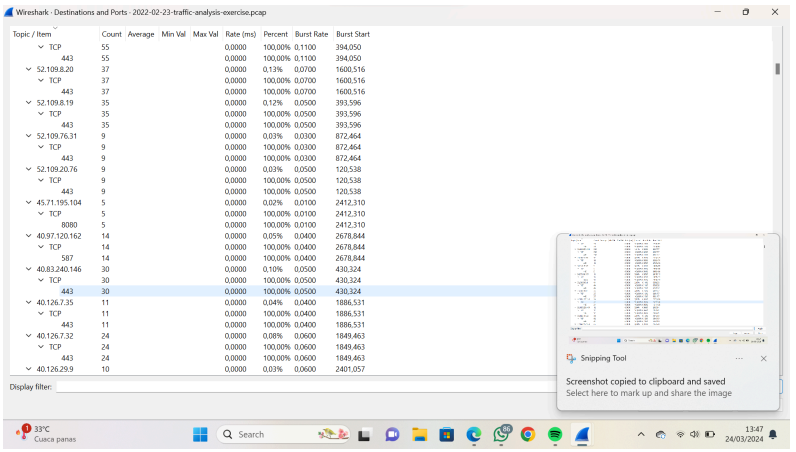


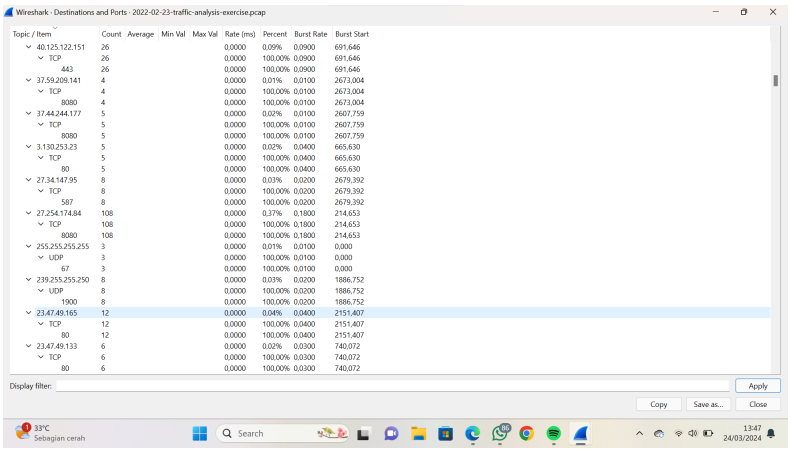
172.16.0.170 - Emotet - 2022-02-23 at 18:25 UTC

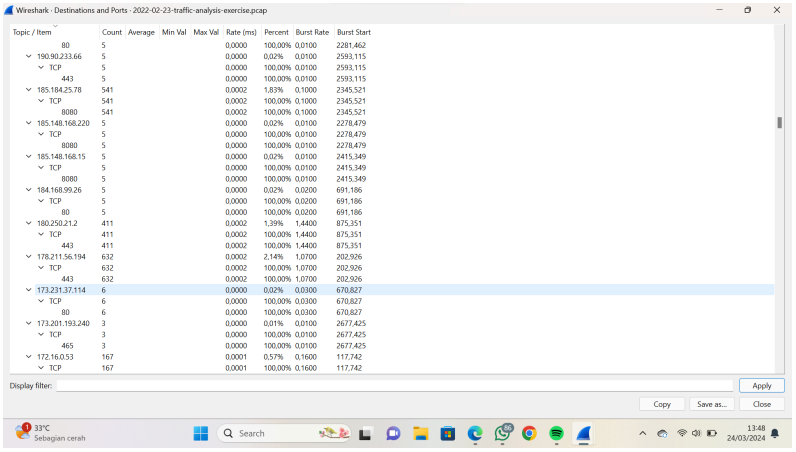



Wireshark · Destinations and Ports · 2022-02-23-traffic-analysis-exercise.pcap
Topic / Item | Count | Average | Min Val | Max Val | Rate (ms) | Percent | Burst Rate | Burst Start
TCP 14 0,0000 100,00% 0,0800 91,886
443 14 0,0000 100,00% 0,0800 91,886
72.167.191.69 5 0,0000 0,02% 0,0400 499,434
TCP 5 0,0000 100,00% 0,0400 499,434
80 5 0,0000 100,00% 0,0400 499,434
68.183.93.250 5 0,0000 0,02% 0,0100 2598,967
TCP 5 0,0000 100,00% 0,0100 2598,967
443 5 0,0000 100,00% 0,0100 2598,967
68.178.213.203 5 0,0000 0,02% 0,0200 2678,440
TCP 5 0,0000 100,00% 0,0200 2678,440
587 5 0,0000 100,00% 0,0200 2678,440
66.29.145.216 5 0,0000 0,02% 0,0300 735,893
TCP 5 0,0000 100,00% 0,0300 735,893
80 5 0,0000 100,00% 0,0300 735,893
66.235.200.112 5 0,0000 0,02% 0,0300 577,937
TCP 5 0,0000 100,00% 0,0300 577,937
80 5 0,0000 100,00% 0,0300 577,937
66.218.86.51 3 0,0000 0,01% 0,0100 2677,425
TCP 3 0,0000 100,00% 0,0100 2677,425
587 3 0,0000 100,00% 0,0100 2677,425
65.52.5.117 26 0,0000 0,09% 0,0800 60,299
TCP 26 0,0000 100,00% 0,0800 60,299
443 26 0,0000 100,00% 0,0800 60,299
64.34.171.228 238 0,0001 0,81% 0,5400 130,832
TCP 238 0,0001 100,00% 0,5400 130,832
80 238 0,0001 100,00% 0,5400 130,832
61.7.231.229 34 0,0000 0,12% 0,1500 372,005
TCP 34 0,0000 100,00% 0,1500 372,005
443 34 0,0000 100,00% 0,1500 372,005
61.7.231.226 30 0,0000 0,10% 0,1200 2556,965
Display filter:
Apply
Copy
Save as...
Close
33°C
Cuaca panas
Search
13:47
24/03/2024


Wireshark · Destinations and Ports · 2022-02-23-traffic-analysis-exercise.pcap
Topic / Item | Count | Average | Min Val | Max Val | Rate (ms) | Percent | Burst Rate | Burst Start
TCP 30 0,0000 100,00% 0,1200 2556,965
443 30 0,0000 100,00% 0,1200 2556,965
59.148.253.194 356 0,0001 1,21% 0,2000 866,777
TCP 356 0,0001 100,00% 0,2000 866,777
443 356 0,0001 100,00% 0,2000 866,777
54.38.242.185 12 0,0000 0,04% 0,0300 2320,474
TCP 12 0,0000 100,00% 0,0300 2320,474
443 12 0,0000 100,00% 0,0300 2320,474
54.37.228.122 5 0,0000 0,02% 0,0100 2409,481
TCP 5 0,0000 100,00% 0,0100 2409,481
443 5 0,0000 100,00% 0,0100 2409,481
54.37.106.167 13 0,0000 0,04% 0,0300 2418,719
TCP 13 0,0000 100,00% 0,0300 2418,719
8080 13 0,0000 100,00% 0,0300 2418,719
52.238.248.4 44 0,0000 0,15% 0,1100 630,832
TCP 44 0,0000 100,00% 0,1100 630,832
443 44 0,0000 100,00% 0,1100 630,832
52.238.248.1 37 0,0000 0,13% 0,1000 689,177
TCP 37 0,0000 100,00% 0,1000 689,177
443 37 0,0000 100,00% 0,1000 689,177
52.185.211.133 34 0,0000 0,12% 0,0500 1011,408
TCP 34 0,0000 100,00% 0,0500 1011,408
443 34 0,0000 100,00% 0,0500 1011,408
52.183.220.149 12 0,0000 0,04% 0,0600 289,901
TCP 12 0,0000 100,00% 0,0600 289,901
443 12 0,0000 100,00% 0,0600 289,901
52.182.141.63 42 0,0000 0,14% 0,1200 354,019
TCP 42 0,0000 100,00% 0,1200 354,019
443 42 0,0000 100,00% 0,1200 354,019
52.168.117.169 25 0,0000 0,08% 0,0500 206,528
Display filter:
Apply
Copy
Save as...
Close
33°C
Cuaca panas
Search
13:47
24/03/2024


Wireshark · Destinations and Ports · 2022-02-23-traffic-analysis-exercise.pcap
Topic / Item | Count | Average | Min Val | Max Val | Rate (ms) | Percent | Burst Rate | Burst Start
TCP 55 0,0000 100,00% 0,1100 394,050
443 55 0,0000 100,00% 0,1100 394,050
52.109.8.20 37 0,0000 0,13% 0,0700 1600,516
TCP 37 0,0000 100,00% 0,0700 1600,516
443 37 0,0000 100,00% 0,0700 1600,516
52.109.8.19 35 0,0000 0,12% 0,0500 393,596
TCP 35 0,0000 100,00% 0,0500 393,596
443 35 0,0000 100,00% 0,0500 393,596
52.109.76.31 9 0,0000 0,03% 0,0300 872,464
TCP 9 0,0000 100,00% 0,0300 872,464
443 9 0,0000 100,00% 0,0300 872,464
52.109.20.76 9 0,0000 0,03% 0,0500 120,538
TCP 9 0,0000 100,00% 0,0500 120,538
443 9 0,0000 100,00% 0,0500 120,538
45.71.195.104 5 0,0000 0,02% 0,0100 2412,310
TCP 5 0,0000 100,00% 0,0100 2412,310
8080 5 0,0000 100,00% 0,0100 2412,310
40.97.120.162 14 0,0000 0,05% 0,0400 2678,844
TCP 14 0,0000 100,00% 0,0400 2678,844
587 14 0,0000 100,00% 0,0400 2678,844
40.83.240.146 30 0,0000 0,10% 0,0500 430,324
TCP 30 0,0000 100,00% 0,0500 430,324
443 30 0,0000 100,00% 0,0500 430,324
40.126.7.35 11 0,0000 0,04% 0,0400 1886,531
TCP 11 0,0000 100,00% 0,0400 1886,531
443 11 0,0000 100,00% 0,0400 1886,531
40.126.7.32 24 0,0000 0,08% 0,0600 1849,463
TCP 24 0,0000 100,00% 0,0600 1849,463
443 24 0,0000 100,00% 0,0600 1849,463
40.126.29.9 10 0,0000 0,03% 0,0600 2401,057
Snipping Tool
Screenshot copied to clipboard and saved
Select here to mark up and share the image
Display filter:
33°C
Cuaca panas
Search
13:47
24/03/2024

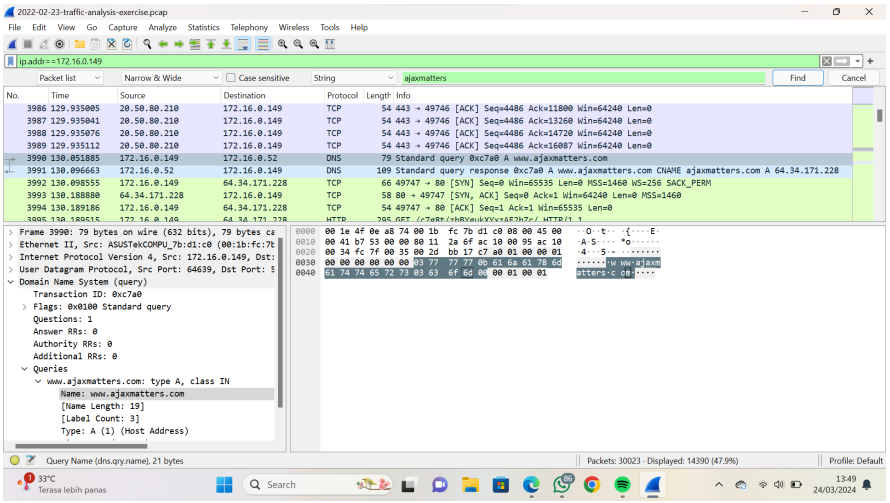

Wireshark · Destinations and Ports · 2022-02-23-traffic-analysis-exercise.pcap
Topic / Item | Count | Average | Min Val | Max Val | Rate (ms) | Percent | Burst Rate | Burst Start
40.125.122.151 26 0,0000 0,09% 0,0900 691,646
TCP 26 0,0000 100,00% 0,0900 691,646
443 26 0,0000 100,00% 0,0900 691,646
37.59.209.141 4 0,0000 0,01% 0,0100 2673,004
TCP 4 0,0000 100,00% 0,0100 2673,004
8080 4 0,0000 100,00% 0,0100 2673,004
37.44.244.177 5 0,0000 0,02% 0,0100 2607,759
TCP 5 0,0000 100,00% 0,0100 2607,759
8080 5 0,0000 100,00% 0,0100 2607,759
3.130.253.23 5 0,0000 0,02% 0,0400 665,630
TCP 5 0,0000 100,00% 0,0400 665,630
80 5 0,0000 100,00% 0,0400 665,630
27.34.147.95 8 0,0000 0,03% 0,0200 2679,392
TCP 8 0,0000 100,00% 0,0200 2679,392
587 8 0,0000 100,00% 0,0200 2679,392
27.254.174.84 108 0,0000 0,37% 0,1800 214,653
TCP 108 0,0000 100,00% 0,1800 214,653
8080 108 0,0000 100,00% 0,1800 214,653
255.255.255.255 3 0,0000 0,01% 0,0100 0,000
UDP 3 0,0000 100,00% 0,0100 0,000
67 3 0,0000 100,00% 0,0100 0,000
239.255.255.250 8 0,0000 0,03% 0,0200 1886,752
UDP 8 0,0000 100,00% 0,0200 1886,752
1900 8 0,0000 100,00% 0,0200 1886,752
23.47.49.165 12 0,0000 0,04% 0,0400 2151,407
TCP 12 0,0000 100,00% 0,0400 2151,407
80 12 0,0000 100,00% 0,0400 2151,407
23.47.49.133 6 0,0000 0,02% 0,0300 740,072
TCP 6 0,0000 100,00% 0,0300 740,072
80 6 0,0000 100,00% 0,0300 740,072
Display filter:
Apply
Copy
Save as...
Close
33°C
Sebagian cerah
Search
13:47
24/03/2024



172.16.0.149 - Emotet with spambot activity - 2022-02-23 at 18:24 UTC

Emotet DLL:

www.ajaxmatters.com - GET /c7g8t/zbBYgukXYxzAF2hZc/




```
GET /c7g8t/zbBYgukXYxzAF2hZc/ HTTP/1.1
Accept: */*
UA-CPU: AMD64
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko
Host: www.ajaxmatters.com
Connection: Keep-Alive
```

Emotet C2:

144.217.88.125	811	0,0003	2,75%	1,4400	1595,686
TCP	811	0,0003	100,00%	1,4400	1595,686
443	811	0,0003	100,00%	1,4400	1595,686
142.250.138.109	16	0,0000	0,05%	0,0400	2678,828
139.196.72.155	223	0,0001	0,76%	0,0900	2246,179
136.143.191.104	3	0,0000	0,01%	0,0100	2677,425
135.148.121.246	3157	0,0012	10,71%	1,0700	334,381
TCP	3157	0,0012	100,00%	1,0700	334,381
8080	3157	0,0012	100,00%	1,0700	334,381
134.209.156.68	342	0,0001	1,16%	0,2800	2677,323
TCP	342	0,0001	100,00%	0,2800	2677,323
443	342	0,0001	100,00%	0,2800	2677,323