

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.

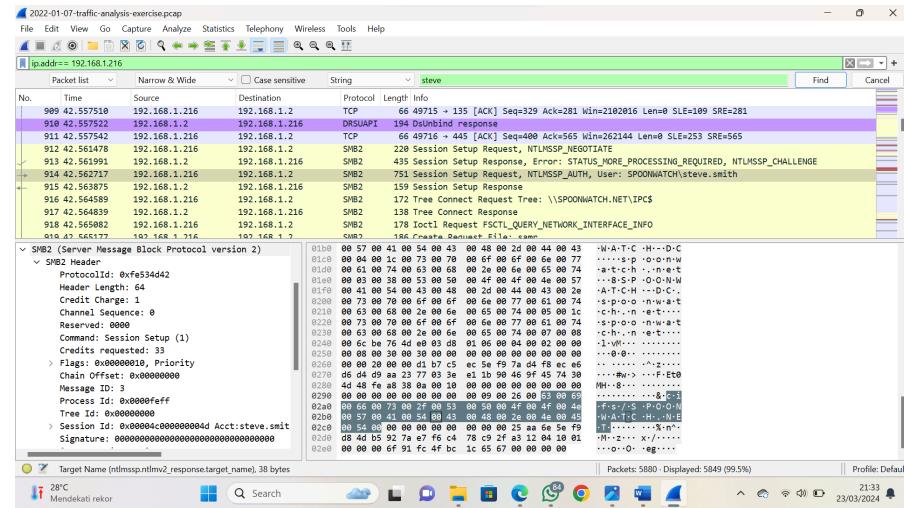
Details

MAC address: 95:5c:8e:32:58:f9

IP address: 192.168.1.216

Host name: DESKTOP-GXMYNO2

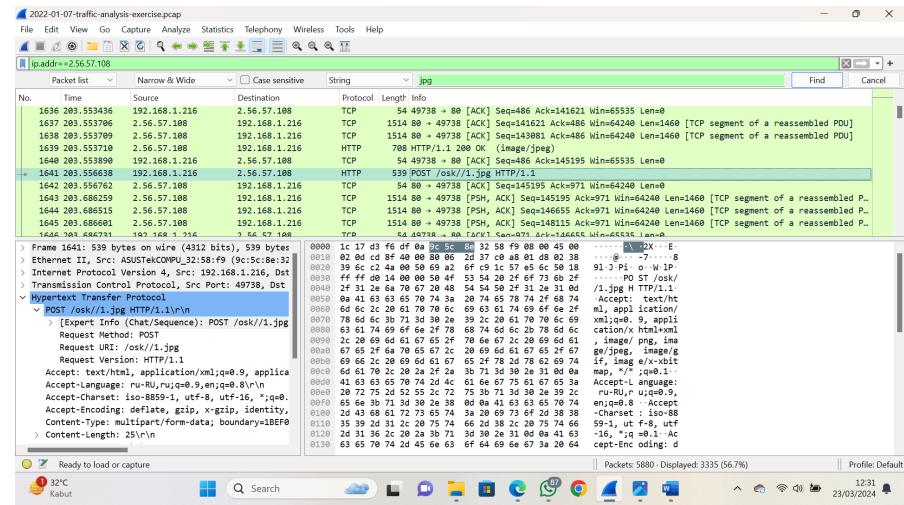
Windows user account: steve.smith



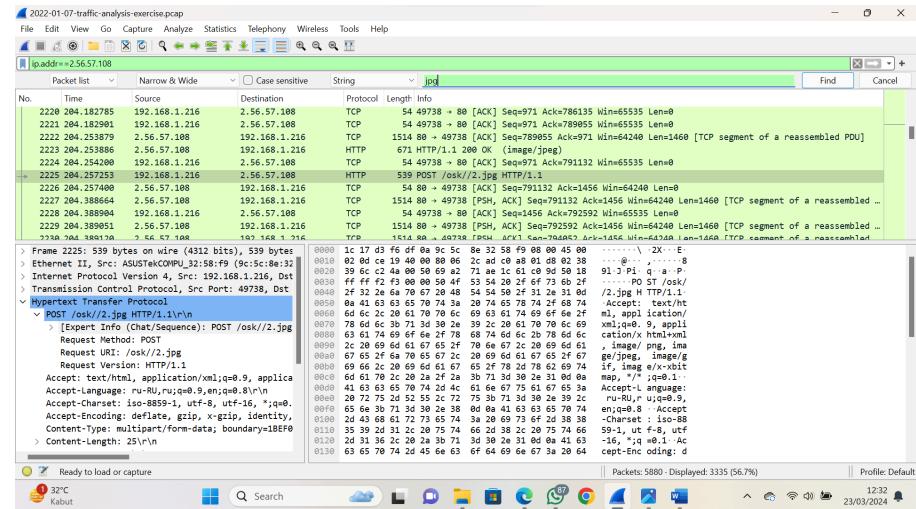
Indicators of Compromise (IOCs)

Malicious traffic:

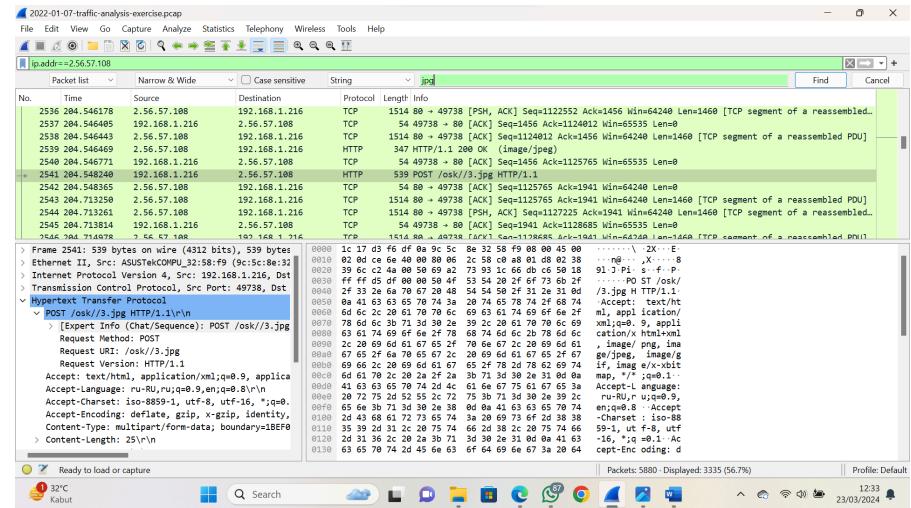
2.56.57.108 port 80 - 2.56.57.108 - POST /osk//1.jpg HTTP/1.1



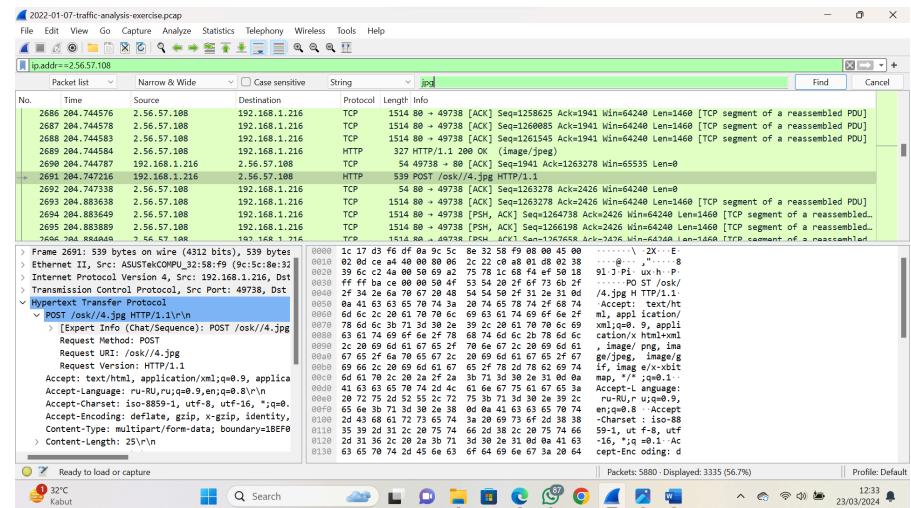
2.56.57.108 port 80 - 2.56.57.108 - POST /osk//2.jpg HTTP/1.1



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

2022-01-07-traffic-analysis-exercise.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ipaddr==2.56.57.108

No.	Time	Source	Destination	Protocol	Length	Info
3849 205.029964	2.56.57.108	192.168.1.216	TCP	1514 80 → 49738 [PSH, ACK] Seq=1761278 Ack=2426 Win=64240 Len=1460 [TCP segment of a reassembled PDU]		
3850 205.022018	192.168.1.216	2.56.57.108	TCP	54 49738 → 80 [ACK] Seq=2424 Ack=1701278 Win=6535 Len=0		
3851 205.022108	192.168.1.216	2.56.57.108	TCP	54 49738 → 80 [ACK] Seq=2424 Ack=1702738 Win=6535 Len=0		
3852 205.022129	192.168.1.216	2.56.57.108	HTTP	1892 HTTP/1.1 200 OK (image/jpeg)		
3853 205.022138	192.168.1.216	2.56.57.108	TCP	54 49738 → 80 [ACK] Seq=2424 Ack=1703743 Win=64530 Len=0		
3854 205.022863	192.168.1.216	2.56.57.108	HTTP	539 POST /osk//5.jpg HTTP/1.1		
3855 205.024821	2.56.57.108	192.168.1.216	TCP	54 80 → 49738 [ACK] Seq=1763743 Ack=2111 Win=64240 Len=0		
3856 205.179752	192.168.1.216	2.56.57.108	TCP	1514 80 → 49738 [ACK] Seq=1763743 Ack=2111 Win=64240 Len=1460 [TCP segment of a reassembled PDU]		
3857 205.179762	2.56.57.108	192.168.1.216	TCP	1514 80 → 49738 [ACK] Seq=1765203 Ack=2111 Win=64240 Len=1460 [TCP segment of a reassembled PDU]		
3858 205.179764	2.56.57.108	192.168.1.216	TCP	1514 80 → 49738 [ACK] Seq=1766663 Ack=2111 Win=64240 Len=1460 [TCP segment of a reassembled PDU]		
3859 205.179767	2.56.57.108	192.168.1.216	TCP	1514 80 → 49738 [ACK] Seq=1768113 Ack=2111 Win=64240 Len=1460 [TCP segment of a reassembled PDU]		

> Frame 3054: 539 bytes on wire (4312 bits), 539 bytes captured

> Ethernet II, Src: ASUSTekCPU_32:58:f9 (9c:5c:8e:32)

> Internet Protocol Version 4, Src: 192.168.1.216, Dst: 2.56.57.108

> Transmission Control Protocol, Src Port: 49738, Dst Port: 80

> Hypertext Transfer Protocol

> > [Expert Info (Sequence): POST /osk//5.jpg HTTP/1.1]

> > [Expert Info (Sequence): POST /osk//5.jpg HTTP/1.1]

Request Method: POST

Request URI: /osk//5.jpg

Request Version: HTTP/1.1

Accept: text/html,application/xhtml+xml;q=0.9, applica

Accept-Language: ru-RU,ru;q=0.9,en;q=0.8,rn

Accept-Charset: iso-8859-1, utf-8, utf-16, ;q=0.9

Accept-Encoding: deflate, gzip, x-gzip, identity,

Content-Type: multipart/form-data; boundary=1BEF0

Content-Length: 25\r\n

Packets: 5880 - Displayed: 3335 (56.7%)

Profile: Default

Ready to load or capture

32°C Kabut

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

2022-01-07-traffic-analysis-exercise.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ipaddr==2.56.57.108

No.	Time	Source	Destination	Protocol	Length	Info
1498 202.867565	192.168.1.216	2.56.57.108	TCP	66 49738 → 80 [SYN] Seq=0 Win=6535 Len=0 MSS=1460 WS=256 SACK_PERM		
1499 203.011392	192.168.1.216	2.56.57.108	TCP	58 80 → 49738 [SYN, ACK] Seq=1 Win=64240 Len=0 MSS=1460		
1500 203.012819	192.168.1.216	2.56.57.108	TCP	54 49738 → 80 [ACK] Seq=1 Ack=1 Win=6535 Len=0		
1501 203.017259	192.168.1.216	2.56.57.108	HTTP	539 POST /osk//6.jpg HTTP/1.1		
1502 203.017653	2.56.57.108	192.168.1.216	TCP	54 80 → 49738 [ACK] Seq=1 Ack=486 Win=64240 Len=0		
1503 203.148814	192.168.1.216	2.56.57.108	TCP	1514 80 → 49738 [PSH, ACK] Seq=1 Ack=486 Win=64240 Len=1460 [TCP segment of a reassembled PDU]		
1504 203.149387	192.168.1.216	2.56.57.108	TCP	54 49738 → 80 [ACK] Seq=486 Ack=1461 Win=6535 Len=0		
1505 203.149542	192.168.1.216	2.56.57.108	TCP	1514 80 → 49738 [PSH, ACK] Seq=1461 Ack=486 Win=64240 Len=1460 [TCP segment of a reassembled PDU]		
1506 203.149833	2.56.57.108	192.168.1.216	TCP	1514 80 → 49738 [ACK] Seq=2924 Ack=486 Win=64240 Len=1460 [TCP segment of a reassembled PDU]		
1507 203.150002	192.168.1.216	2.56.57.108	TCP	1514 80 → 49738 [ACK] Seq=3381 Ack=486 Win=64240 Len=1460 [TCP segment of a reassembled PDU]		

> Frame 1501: 539 bytes on wire (4312 bits), 539 bytes captured

> Ethernet II, Src: ASUSTekCPU_32:58:f9 (9c:5c:8e:32)

> Internet Protocol Version 4, Src: 192.168.1.216, Dst: 2.56.57.108

> Transmission Control Protocol, Src Port: 49738, Dst Port: 80

> Hypertext Transfer Protocol

> > [Expert Info (Sequence): POST /osk//6.jpg HTTP/1.1]

> > [Expert Info (Sequence): POST /osk//6.jpg HTTP/1.1]

Request Method: POST

Request URI: /osk//6.jpg

Request Version: HTTP/1.1

Accept: text/html,application/xhtml+xml;q=0.9, applica

Accept-Language: ru-RU,ru;q=0.9,en;q=0.8,rn

Accept-Charset: iso-8859-1, utf-8, utf-16, ;q=0.9

Accept-Encoding: deflate, gzip, x-gzip, identity,

Content-Type: multipart/form-data; boundary=1BEF0

Content-Length: 25\r\n

Packets: 5880 - Displayed: 3335 (56.7%)

Profile: Default

HTTP Request-URI (http.requesturi), 11 bytes

32°C Kabut

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

2022-01-07-traffic-analysis-exercise.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ipaddr==2.56.57.108

No.	Time	Source	Destination	Protocol	Length	Info
4189 205.557464	2.56.57.108	192.168.1.216	TCP	1514 80 → 49738 [PSH, ACK] Seq=2946283 Ack=2111 Win=64240 Len=1460 [TCP segment of a reassembled PDU]		
4190 205.557686	192.168.1.216	2.56.57.108	TCP	54 49738 → 80 [ACK] Seq=2947663 Ack=2111 Win=6535 Len=0		
4191 205.557705	2.56.57.108	192.168.1.216	HTTP	1892 HTTP/1.1 200 OK (image/jpeg)		
4192 205.557937	192.168.1.216	2.56.57.108	TCP	54 49738 → 80 [ACK] Seq=2947683 Ack=2111 Win=64240 Len=1460 [TCP segment of a reassembled PDU]		
4193 205.558099	192.168.1.216	2.56.57.108	TCP	1514 80 → 49738 [PSH, ACK] Seq=2950250 Ack=2111 Win=6535 Len=0		
4194 205.558859	192.168.1.216	2.56.57.108	HTTP	539 POST /osk//7.jpg HTTP/1.1		
4195 205.559967	2.56.57.108	192.168.1.216	TCP	54 80 → 49738 [ACK] Seq=2950250 Ack=3396 Win=64240 Len=0		
4196 205.698667	2.56.57.108	192.168.1.216	TCP	1514 80 → 49738 [PSH, ACK] Seq=2950250 Ack=3396 Win=64240 Len=1460 [TCP segment of a reassembled PDU]		
4197 205.699217	192.168.1.216	2.56.57.108	TCP	54 49738 → 80 [ACK] Seq=3399 Ack=259170 Win=6535 Len=0		
4198 205.699259	2.56.57.108	192.168.1.216	TCP	1514 80 → 49738 [ACK] Seq=295170 Ack=3399 Win=64240 Len=1460 [TCP segment of a reassembled PDU]		

> Frame 4194: 539 bytes on wire (4312 bits), 539 bytes captured

> Ethernet II, Src: ASUSTekCPU_32:58:f9 (9c:5c:8e:32)

> Internet Protocol Version 4, Src: 192.168.1.216, Dst: 2.56.57.108

> Transmission Control Protocol, Src Port: 49738, Dst Port: 80

> Hypertext Transfer Protocol

> > [Expert Info (Sequence): POST /osk//7.jpg HTTP/1.1]

> > [Expert Info (Sequence): POST /osk//7.jpg HTTP/1.1]

Request Method: POST

Request URI: /osk//7.jpg

Request Version: HTTP/1.1

Accept: text/html,application/xhtml+xml;q=0.9, applica

Accept-Language: ru-RU,ru;q=0.9,en;q=0.8,rn

Accept-Charset: iso-8859-1, utf-8, utf-16, ;q=0.9

Accept-Encoding: deflate, gzip, x-gzip, identity,

Content-Type: multipart/form-data; boundary=1BEF0

Content-Length: 25\r\n

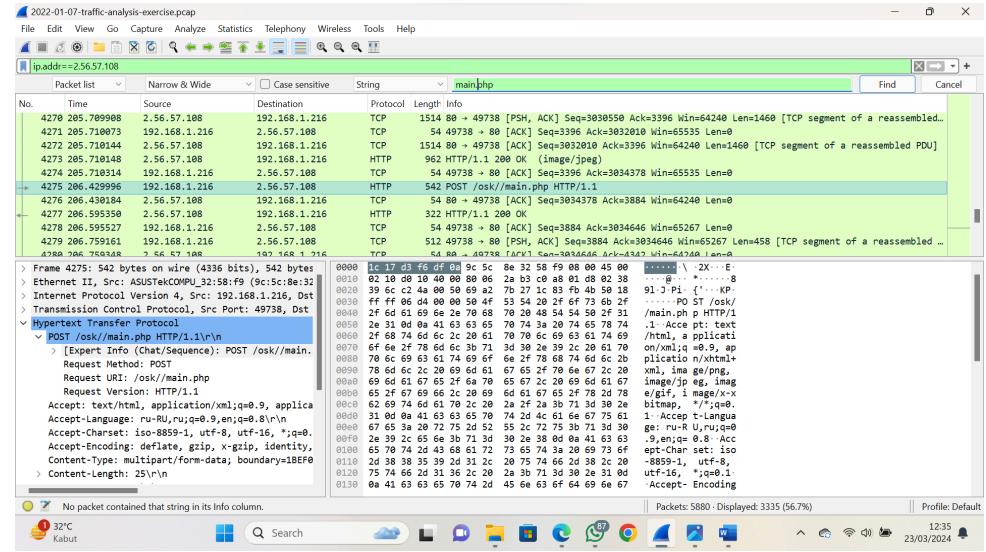
Packets: 5880 - Displayed: 3335 (56.7%)

Profile: Default

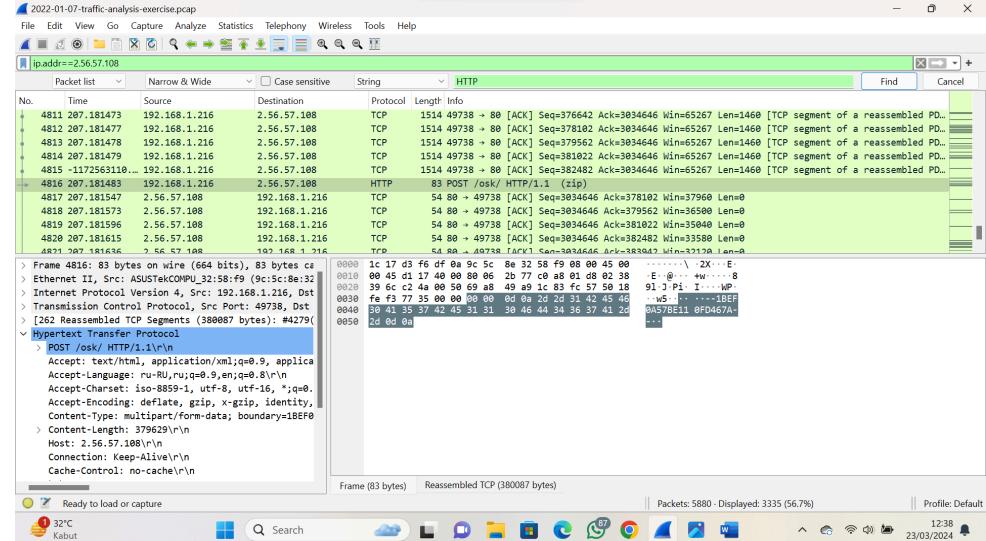
Ready to load or capture

32°C Kabut

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 EXERCISE 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

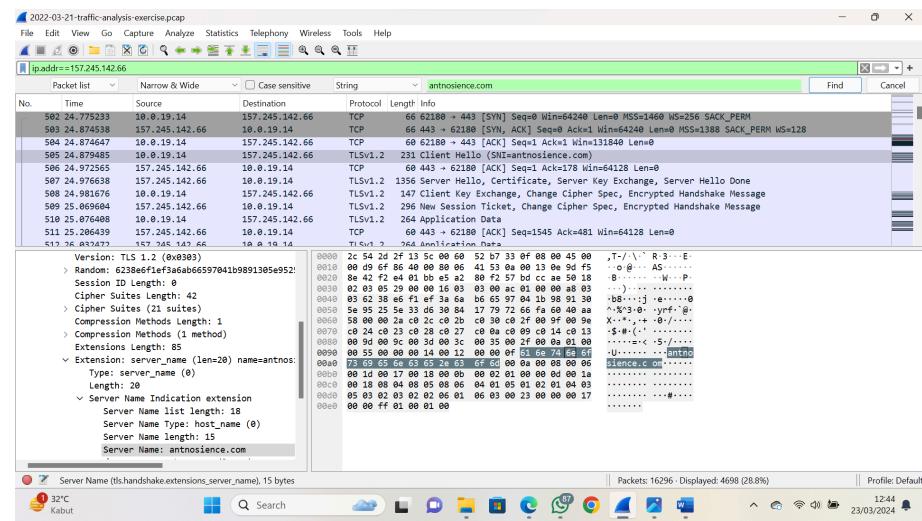
Indicators of Compromise (IOCs):

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

Screenshot of Wireshark showing HTTPS traffic to suncoastpinball.com. The session details pane shows the handshake process, including the Client Hello, Server Hello, and Certificate messages. The packet list pane shows the raw hex and ASCII data for each message.

Session Details:

- Protocol: TCP
- Length: 16296 bytes
- Server Name (tlshandshake.extensions_server_name): suncoastpinball.com
- Client Hello (TLSv1.2):
 - Version: TLS 1.2 (0x0303)
 - Random: 6238e72f81d05fe5bf0f5ba93ce0633747
 - Session ID Length: 0
 - Cipher Suites Length: 38
 - Compression Methods Length: 1
 - Extensions Length: 98
 - Extension: server_name (len=24) name=suncoastpinball.com
 - Type: server_name (0)
 - Length: 24
 - Server Name Indication extension:
 - Server Name list length: 22
 - Server Name Type: host_name (0)
 - Server Name length: 19
 - Server Name: suncoastpinball.com
- Server Hello (TLSv1.2):
 - Version: TLS 1.2 (0x0303)
 - Random: 6238e72f81d05fe5bf0f5ba93ce0633747
 - Session ID Length: 0
 - Cipher Suites Length: 38
 - Compression Methods Length: 1
 - Extensions Length: 98
 - Extension: server_name (len=24) name=suncoastpinball.com
 - Type: server_name (0)
 - Length: 24
 - Server Name Indication extension:
 - Server Name list length: 22
 - Server Name Type: host_name (0)
 - Server Name length: 19
 - Server Name: suncoastpinball.com
- Certificate (TLSv1.2):
 - Version: TLS 1.2 (0x0303)
 - Random: 6238e72f81d05fe5bf0f5ba93ce0633747
 - Session ID Length: 0
 - Cipher Suites Length: 38
 - Compression Methods Length: 1
 - Extensions Length: 98
 - Extension: server_name (len=24) name=suncoastpinball.com
 - Type: server_name (0)
 - Length: 24
 - Server Name Indication extension:
 - Server Name list length: 22
 - Server Name Type: host_name (0)
 - Server Name length: 19
 - Server Name: suncoastpinball.com

157.245.142.66 port 443 - otectagain.top - HTTPS traffic

Screenshot of Wireshark showing HTTPS traffic to otectagain.top. The session details pane shows the handshake process, including the Client Hello, Server Hello, and Certificate messages. The packet list pane shows the raw hex and ASCII data for each message.

Session Details:

- Protocol: TCP
- Length: 16296 bytes
- Server Name (tlshandshake.extensions_server_name): otectagain.top
- Client Hello (TLSv1.2):
 - Version: TLS 1.2 (0x0303)
 - Random: 62391845490aa47eb09c556cf56fb07b78da
 - Session ID Length: 0
 - Cipher Suites Length: 38
 - Compression Methods Length: 1
 - Extensions Length: 93
 - Extension: server_name (len=19) name=otectagain.top
 - Type: server_name (0)
 - Length: 19
 - Server Name Indication extension:
 - Server Name list length: 17
 - Server Name Type: host_name (0)
 - Server Name length: 14
 - Server Name: otectagain.top
- Server Hello (TLSv1.2):
 - Version: TLS 1.2 (0x0303)
 - Random: 62391845490aa47eb09c556cf56fb07b78da
 - Session ID Length: 0
 - Cipher Suites Length: 38
 - Compression Methods Length: 1
 - Extensions Length: 93
 - Extension: server_name (len=19) name=otectagain.top
 - Type: server_name (0)
 - Length: 19
 - Server Name Indication extension:
 - Server Name list length: 17
 - Server Name Type: host_name (0)
 - Server Name length: 14
 - Server Name: otectagain.top
- Certificate (TLSv1.2):
 - Version: TLS 1.2 (0x0303)
 - Random: 62391845490aa47eb09c556cf56fb07b78da
 - Session ID Length: 0
 - Cipher Suites Length: 38
 - Compression Methods Length: 1
 - Extensions Length: 93
 - Extension: server_name (len=19) name=otectagain.top
 - Type: server_name (0)
 - Length: 19
 - Server Name Indication extension:
 - Server Name list length: 17
 - Server Name Type: host_name (0)
 - Server Name length: 14
 - Server Name: otectagain.top

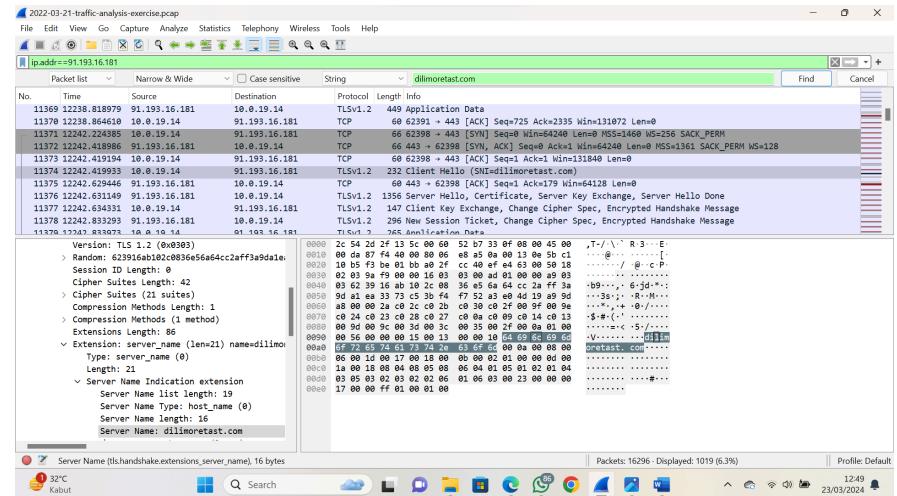
91.193.16.181 port 443 - seaskysafe.com - HTTPS traffic

Screenshot of Wireshark showing HTTPS traffic to seaskysafe.com. The session details pane shows the handshake process, including the Client Hello, Server Hello, and Certificate messages. The packet list pane shows the raw hex and ASCII data for each message.

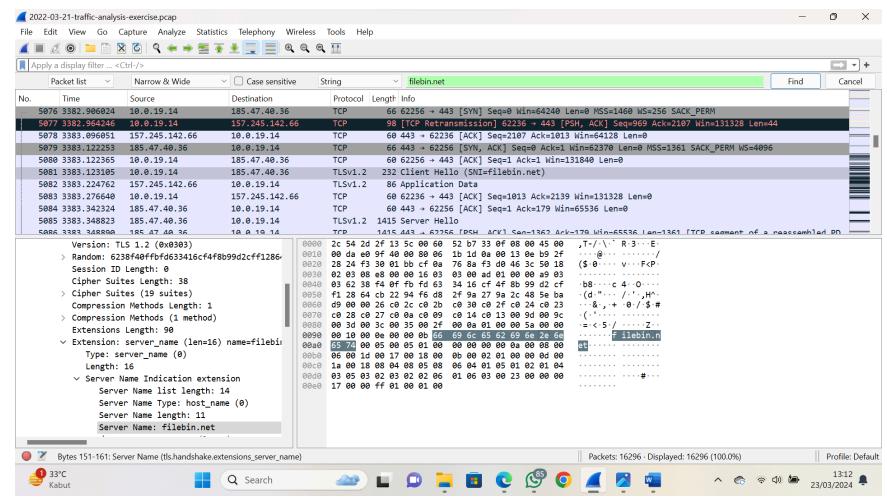
Session Details:

- Protocol: TCP
- Length: 16296 bytes
- Server Name (tlshandshake.extensions_server_name): seaskysafe.com
- Client Hello (TLSv1.2):
 - Version: TLS 1.2 (0x0303)
 - Random: 6239169b249164971a248c16d09ce494
 - Session ID Length: 0
 - Cipher Suites Length: 38
 - Compression Methods Length: 1
 - Extensions Length: 93
 - Extension: server_name (len=19) name=seaskysafe.com
 - Type: server_name (0)
 - Length: 19
 - Server Name Indication extension:
 - Server Name list length: 17
 - Server Name Type: host_name (0)
 - Server Name length: 14
 - Server Name: seaskysafe.com
- Server Hello (TLSv1.2):
 - Version: TLS 1.2 (0x0303)
 - Random: 6239169b249164971a248c16d09ce494
 - Session ID Length: 0
 - Cipher Suites Length: 38
 - Compression Methods Length: 1
 - Extensions Length: 93
 - Extension: server_name (len=19) name=seaskysafe.com
 - Type: server_name (0)
 - Length: 19
 - Server Name Indication extension:
 - Server Name list length: 17
 - Server Name Type: host_name (0)
 - Server Name length: 14
 - Server Name: seaskysafe.com
- Certificate (TLSv1.2):
 - Version: TLS 1.2 (0x0303)
 - Random: 6239169b249164971a248c16d09ce494
 - Session ID Length: 0
 - Cipher Suites Length: 38
 - Compression Methods Length: 1
 - Extensions Length: 93
 - Extension: server_name (len=19) name=seaskysafe.com
 - Type: server_name (0)
 - Length: 19
 - Server Name Indication extension:
 - Server Name list length: 17
 - Server Name Type: host_name (0)
 - Server Name length: 14
 - Server Name: seaskysafe.com

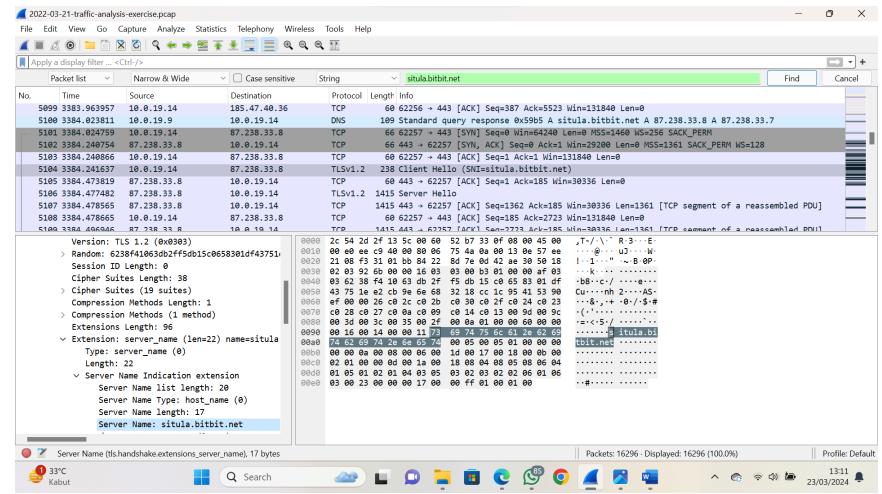
91.193.16.181 port 443 - dilimoretast.com - HTTPS traffic



Suspicious traffic to file sharing domains: port 443 - filebin.net - HTTPS traffic

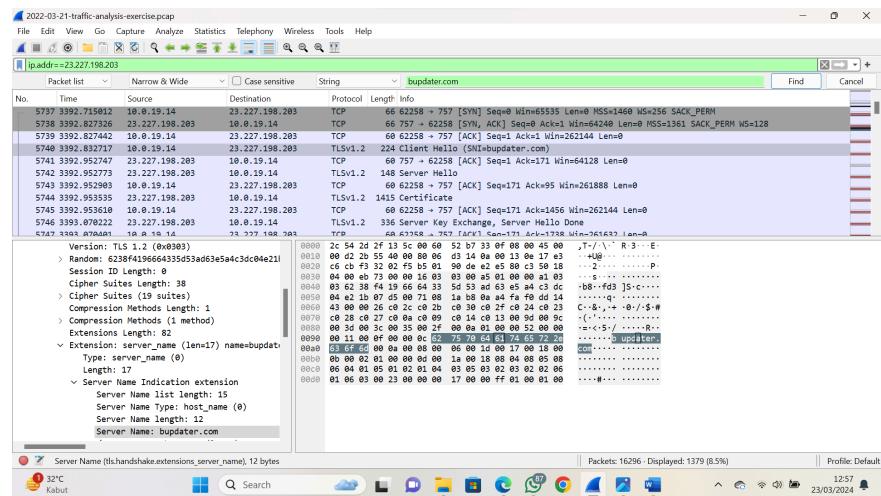


port 443 - situla.bitbit.net - HTTPS traffic



Domains and IP addresses for Cobalt Strike:

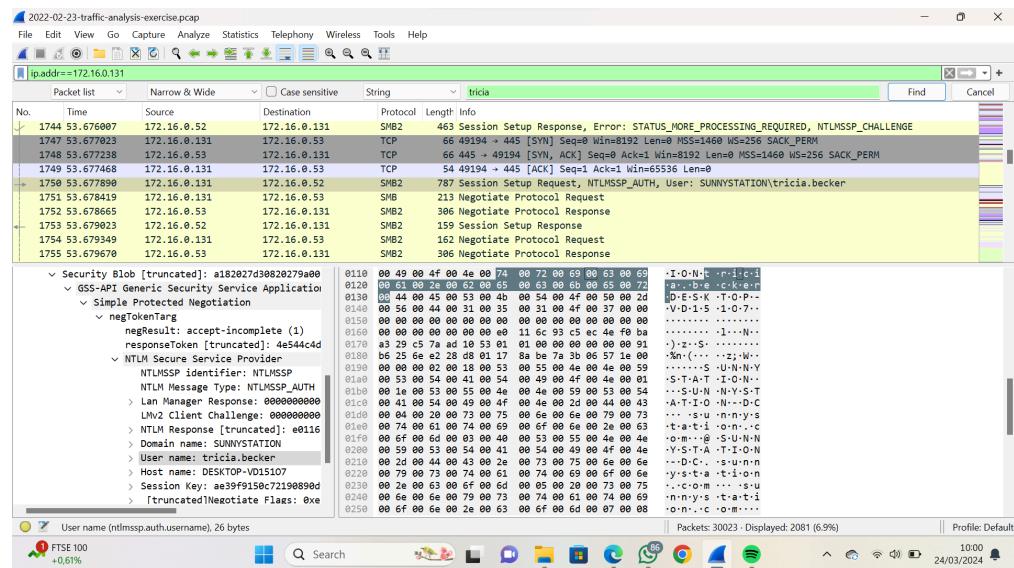
23.227.198.203 port 757 - bupdater.com - HTTPS traffic



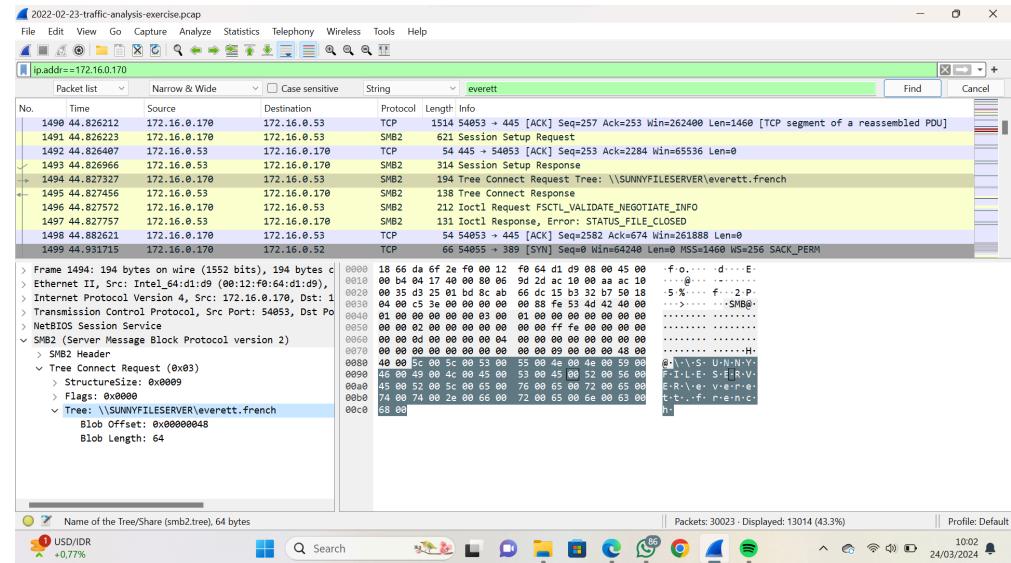
2022-02-23-TRAFFIC ANALYSIS EXERCISE ANSWERS

Hosts/usernames

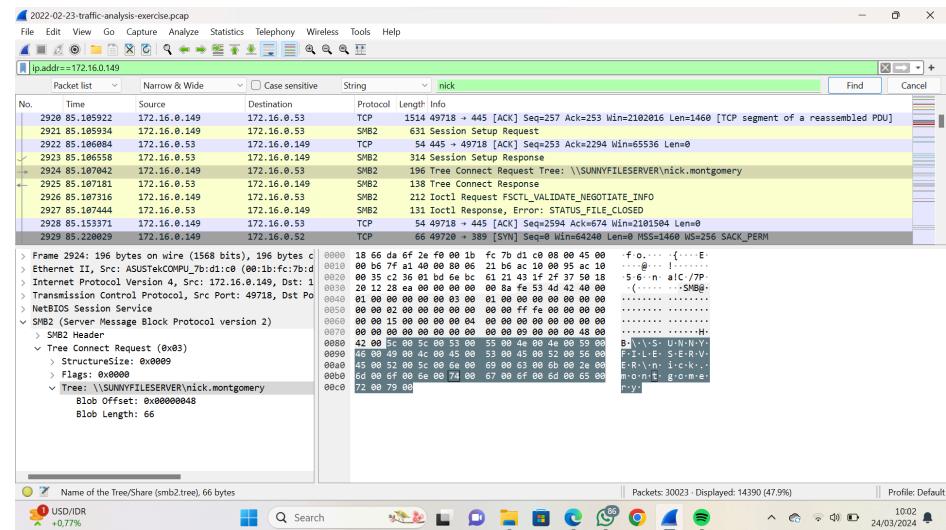
(Read: MAC address - IP address - host name - Windows account name)
2c:27:d7:d2:06:f5 - 172.16.0.131 - DESKTOP-VD151O7 - tricia.becker



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



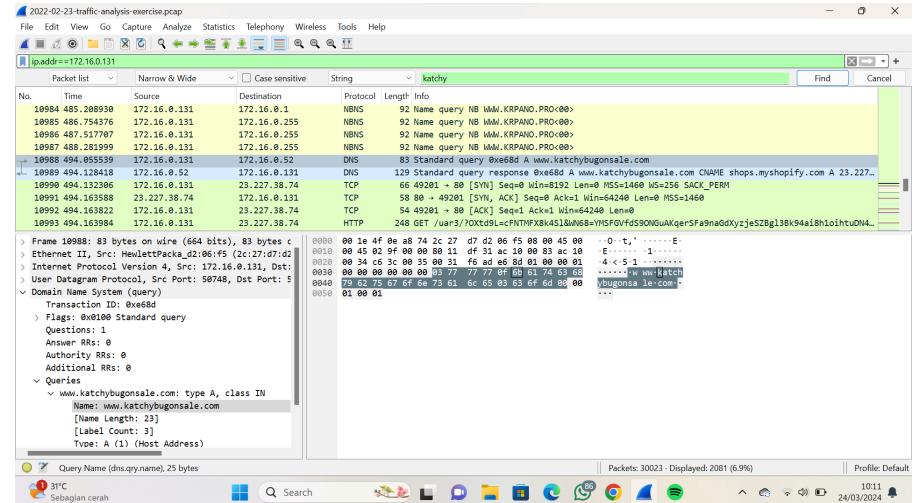
Malware infections:

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

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

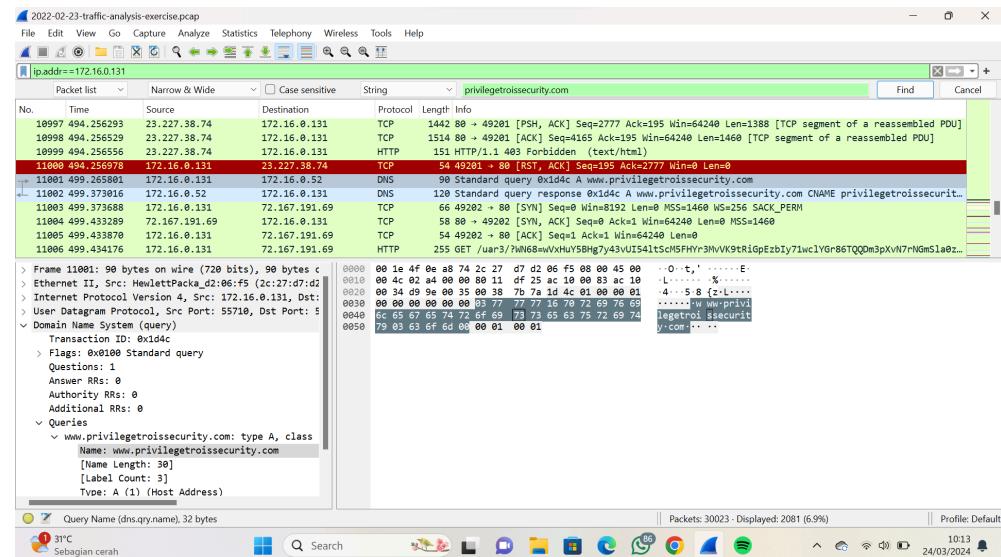
Formbook/XLoader C2 traffic:

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



```
GET /uar3/?OXt9L=cFNTMFX8k4S1&WN68=YMSFGVfdS90NGuAKqerSFa9naGdXyzjeSZBg13Bk94ai8h1oihtuDN4qXdc51YMbqxW07UiJFru1VtwMrj0Ygg== 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=wVxHuY5Bhg7y43vUI541tScM5FHYr3MvVK9tRiGpEzbIy71wc1YGr86TQQDm3pXvN7rNgmSla0zZhUrNE0d8Q==&0xt9l=cF  
NTMFX8k451 HTTP/1.1  
Host: www.privelegetroissecurity.com  
Connection: close
```

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

Screenshot of NetworkMiner tool showing traffic analysis for the specified connection.

Packets:

- No. 10808: 499.501683 (72.167.191.69) → 172.16.0.131 (TCP, Seq=202, Ack=218, Win=64024, Len=0)
- No. 10809: 499.502315 (72.16.0.131) → 72.167.191.69 (TCP, Seq=202, Ack=218, Win=64024, Len=0)
- No. 10810: 499.502538 (72.16.0.131) → 72.167.191.69 (TCP, Seq=202, Ack=218, Win=64024, Len=0)
- No. 10811: 499.502642 (72.167.191.69) → 172.16.0.131 (TCP, Seq=203, Ack=218, Win=64239, Len=0)
- No. 10816: 504.508806 (72.16.0.131) → 172.16.0.131 (DNS, 88 bytes, Standard query, 0x384c, A www.hentainftxxx.com)
- No. 10817: 504.742485 (172.16.0.131) → 172.16.0.131 (DNS, 112 bytes, Standard query response, 0x384c, A www.hentainftxxx.com A 194.9.94.85 A 194.9.94.86)
- No. 10818: 504.743516 (172.16.0.131) → 194.9.94.85 (TCP, 66 bytes, Seq=9, ACK=10, Win=1460, MSS=1460, WS=256, SACK_PERM)
- No. 10820: 504.897567 (194.9.94.85) → 172.16.0.131 (TCP, 58 bytes, Seq=9, ACK=11, Win=64240, Len=0, MSS=1460)
- No. 10821: 504.898827 (172.16.0.131) → 194.9.94.85 (TCP, 54 bytes, Seq=10, ACK=12, Win=64240, Len=0, MSS=1460)
- No. 10822: 504.898308 (172.16.0.131) → 194.9.94.85 (HTTP, 245 bytes, GET, /uar3/?[base64 style string])

Selected Packets:

- 0080: 00 1e 4f 0e a8 74 2c 27 d7 d2 06 f5 08 00 45 00 -O-t,'.....E-
- 0010: 00 42 02 aa 00 00 00 11 df 29 ac 10 00 83 ac 10 -4-5-,(8L....
- 0020: 00 34 c6 9b 00 35 00 2e b2 28 38 4c 01 00 00 01 -.....w www-henta...
- 0030: 00 00 00 00 00 03 77 77 0c 68 65 60 74 01 -infxxx.com:....
- 0040: 09 6e 66 74 78 78 03 63 6f 6d 00 00 01 00 01 infxxx.com:....

Selected DNS Query:

Query Name (dnsqry.name), 22 bytes
www.hentainftxxx.com

Selected HTTP Request:

```
GET /uar3/?0Xtd9L=cFNTMF8k4S1&WN68=7GGwHF32hRrdL34DIy4C++DYNMj/1d2v4JDqR5DLy9MEgQIZhCtuLoZxudHqPtA4E9sAhQJ5Izw
CVbNJKdQ== HTTP/1.1
Host: www.hentainftxxx.com
Connection: close
```

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

Screenshot of NetworkMiner tool showing traffic analysis for the specified connection.

Packets:

- No. 11025: 505.066205 (172.16.0.131) → 194.9.94.85 (TCP, Seq=192, Ack=197, Win=62864, Len=0)
- No. 11026: 505.066379 (194.9.94.85) → 172.16.0.131 (TCP, Seq=193, Ack=193, Win=64239, Len=0)
- No. 11027: 505.068680 (194.9.94.85) → 172.16.0.131 (TCP, 1438 bytes, [TCP segment of a reassembled PDU])
- No. 11028: 505.068783 (172.16.0.131) → 194.9.94.85 (TCP, 54 bytes, Seq=193, Ack=253, Win=0, Len=0)
- No. 11031: 510.061580 (172.16.0.131) → 172.16.0.131 (DNS, 83 bytes, Standard query, 0xdab9, A www.moonshot.properties)
- No. 11032: 510.149479 (172.16.0.131) → 172.16.0.131 (DNS, 234 bytes, Standard query response, 0xdab9, A www.moonshot.properties CNAME parkingpage.namecheap.com A ...)
- No. 11033: 510.150822 (172.16.0.131) → 198.54.117.210 (TCP, 66 bytes, Seq=193, ACK=194, Win=1460, MSS=1460, WS=256, SACK_PERM)
- No. 11034: 510.218831 (198.54.117.210) → 172.16.0.131 (TCP, 58 bytes, Seq=194, ACK=195, Win=64240, Len=0, MSS=1460)
- No. 11035: 510.219358 (172.16.0.131) → 198.54.117.210 (TCP, 54 bytes, Seq=195, ACK=196, Win=64240, Len=0)
- No. 11036: 510.219644 (172.16.0.131) → 198.54.117.210 (HTTP, 245 bytes, GET, /uar3/?WN68=G7COZmwnrPee5EsQB6aSzW5LG2Uw7KHIFA2umt3z9J0n70XS6qAVkpOr+xKOV+zPMOEQaf63vM5y0TRfGLX9kw==&0Xtd9L=cFNTMF8k4S1 HTTP/1.1)

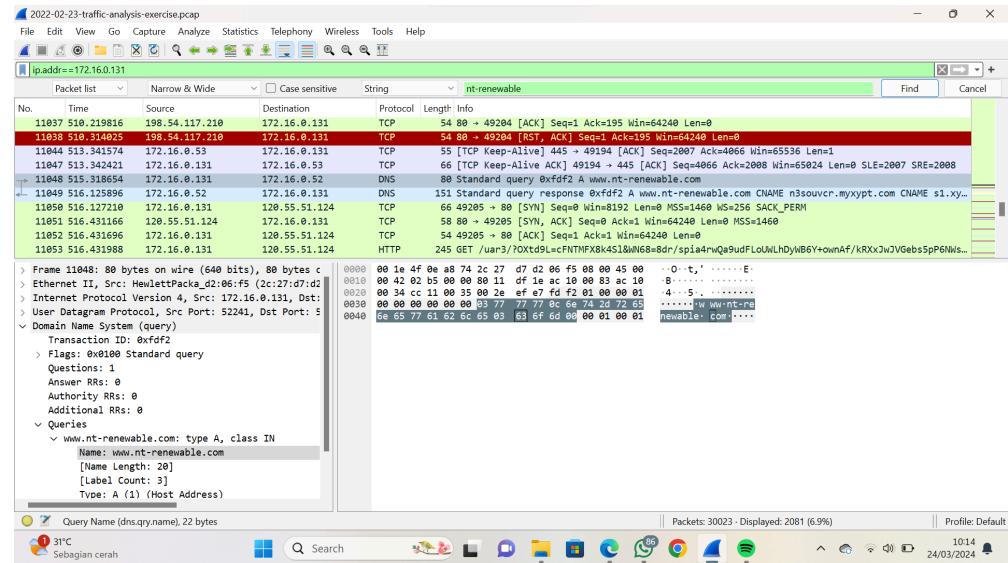
Selected DNS Query:

Query Name (dnsqry.name), 25 bytes
www.moonshot.properties

Selected HTTP Request:

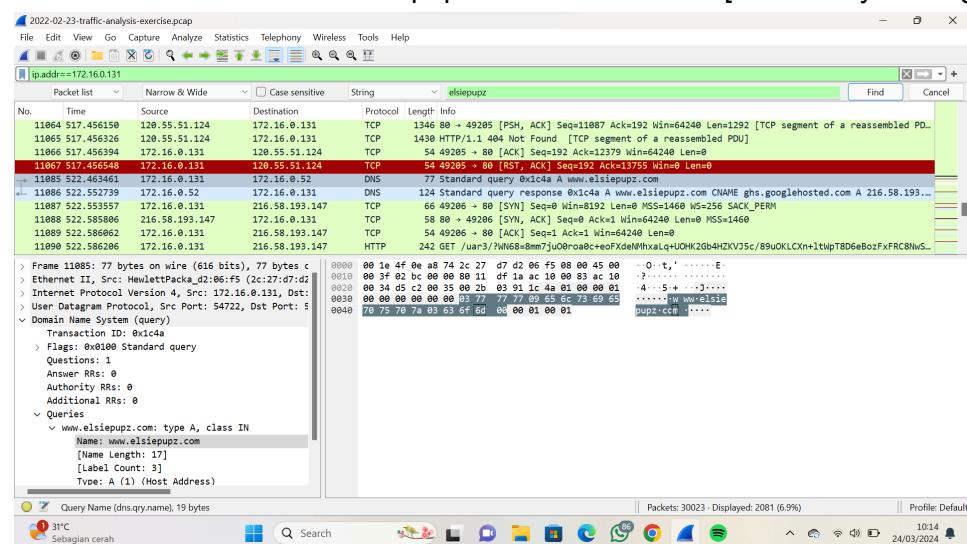
```
GET /uar3/?WN68=G7COZmwnrPee5EsQB6aSzW5LG2Uw7KHIFA2umt3z9J0n70XS6qAVkpOr+xKOV+zPMOEQaf63vM5y0TRfGLX9kw==&0Xtd9L=cFNTMF8k4S1 HTTP/1.1
Host: www.moonshot.properties
Connection: close
```

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



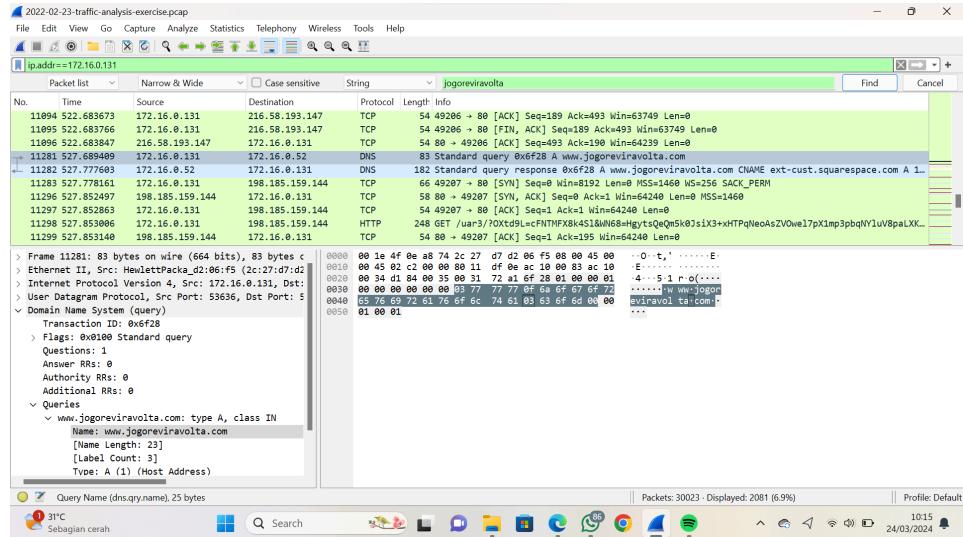
```
GET /uar3/?0Xtd9L=cFNTMF8xk4S1&Wn68=8dr/spia4rwQa9udFLoUWLhDyWB6Y+ownAf/kRXxJwJVGebs5pP6Nws1hg+05/59UnRkE2Lc1Kud  
c3S/D+UP/w== HTTP/1.1  
Host: www.nt-renewable.com  
Connection: close
```

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



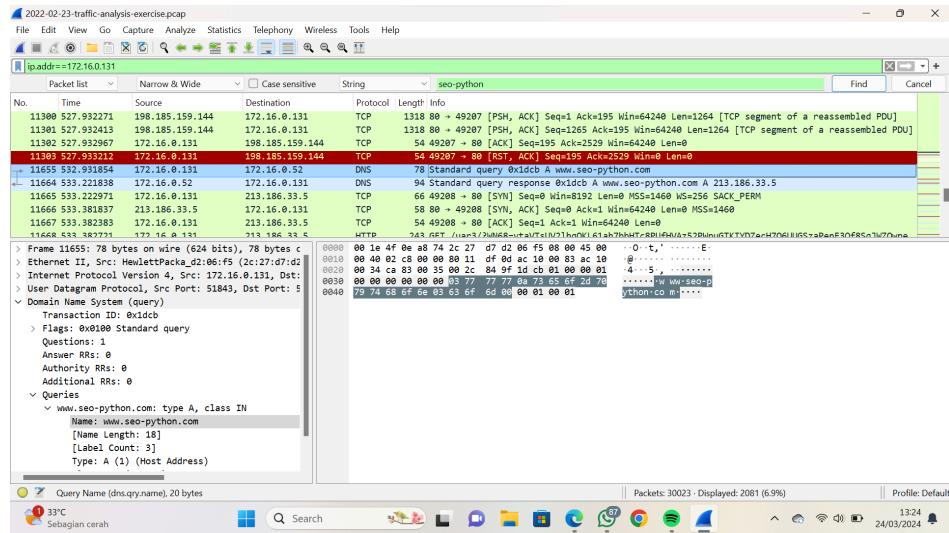
```
GET /uar3/?WN68=8mm7ju0roa0c+eoFXdeNMhxLq+UOHK26b4HZKVJ5c/89uOKLCNx+lWpT8D6eBozFxFRC8NwSE5MNPGjBvbw==&Oxt9L=cFNTMFXk4S1 HTTP/1.1
Host: www.eisiepupz.com
Connection: close
```

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



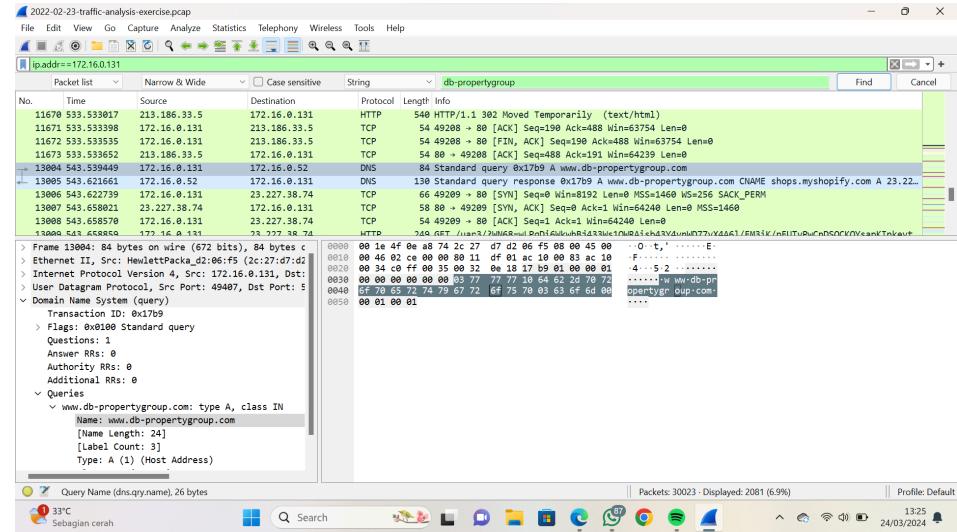
```
GET /uar3/?OXtd9L=cFNTMF8k4S1&WN68=HgystsQeQm5k0JsiX3+xHTPqNeoAsZVowel7pXimp3pbqNYluV8paLXKGRTm0h2A1X7YRo+hCzAH
abyaXGya1Q== HTTP/1.1
Host: www.jogoreviravolta.com
Connection: close
```

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



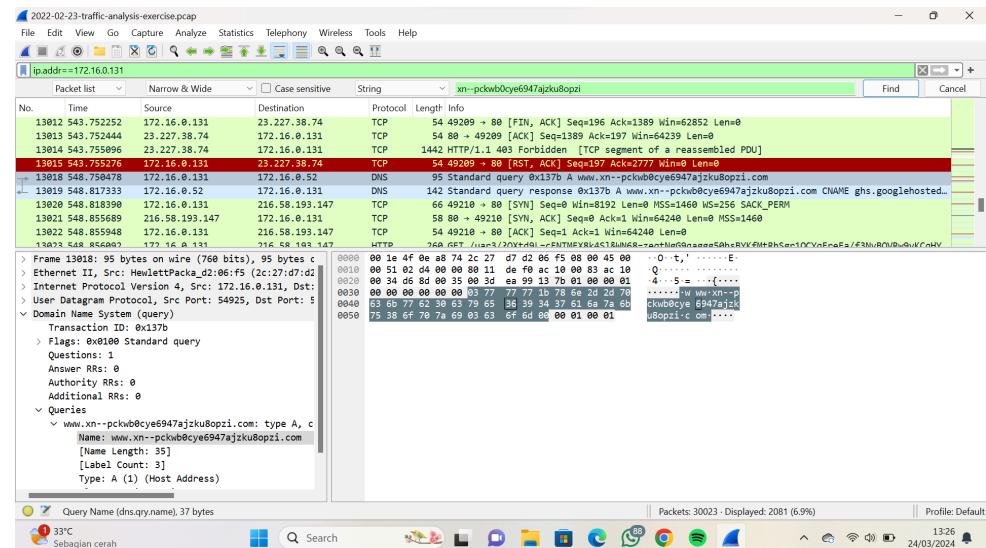
```
GET /uar3/?WN68=ytaVTsUV21hqQKL61ah7bbHTc8PUFHVAz52PwpuGtKIYDZech7Q6UUGSzaPenE30f8SqJWZQweASzStGycgxA==&OXtd9L=cF
NTMF8k4S1 HTTP/1.1
Host: www.seo-python.com
Connection: close
```

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



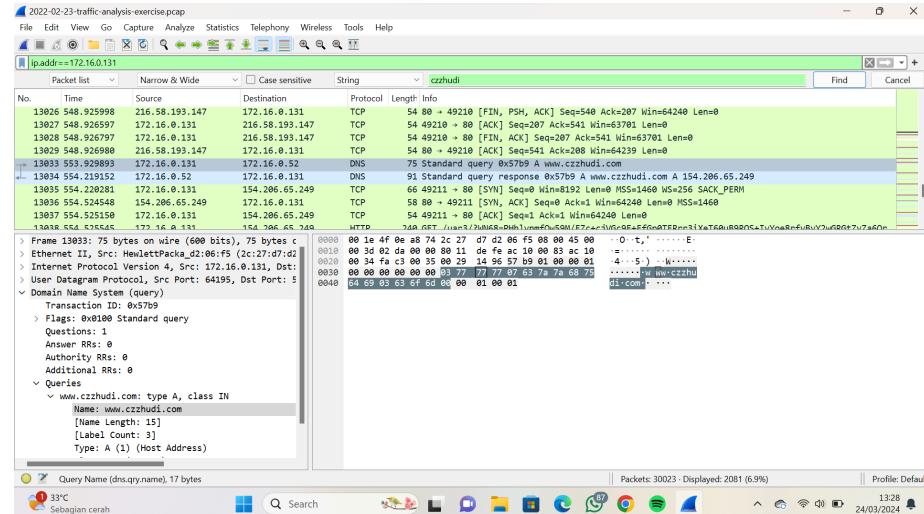
```
GET /uar3/?WN68=wLPqDi6WkwhBj433Ws1QWRAisb43Y4vnWlD77yX4A61/EM3iK/pFUTvPwCnDSQCKQysapKIpkeyt25I1F4noK8Q==&0Xtd9L=cfNTMFX8K4S1 HTTP/1.1
Host: www.db-propertygroup.com
Connection: close
```

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



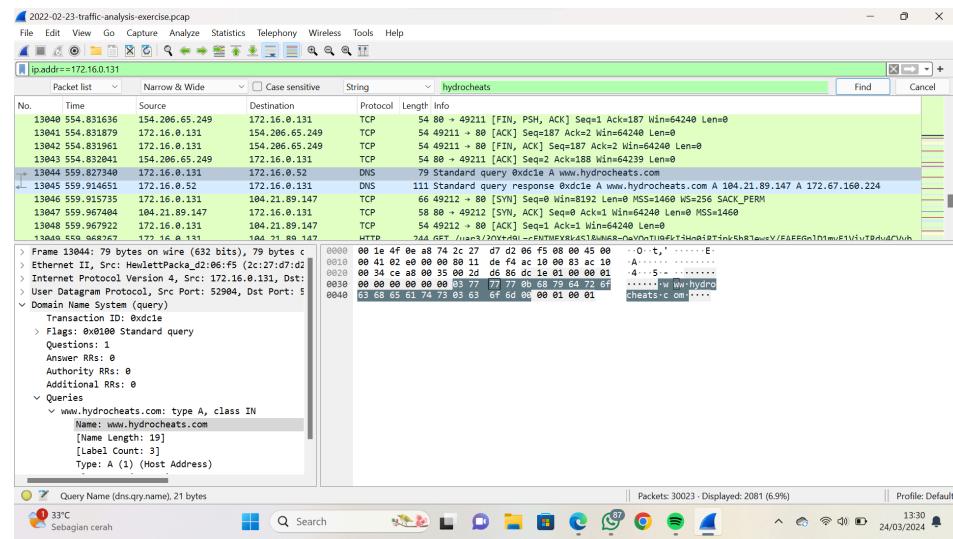
GET /uar3/?0Xtd9L=cFNTMFx8k4S1&WN68=zeqtNg9qaggg50hsBYKfMtRhSgr1QCYqFrEa/f3NyBOVrw9vKCqHY5UvVd0GGhktXMCmx/YKDQN950Cu04g== HTTP/1.1
Host: www.xn--pckwb0cye6947ajzku8opzi.com
Connection: close

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



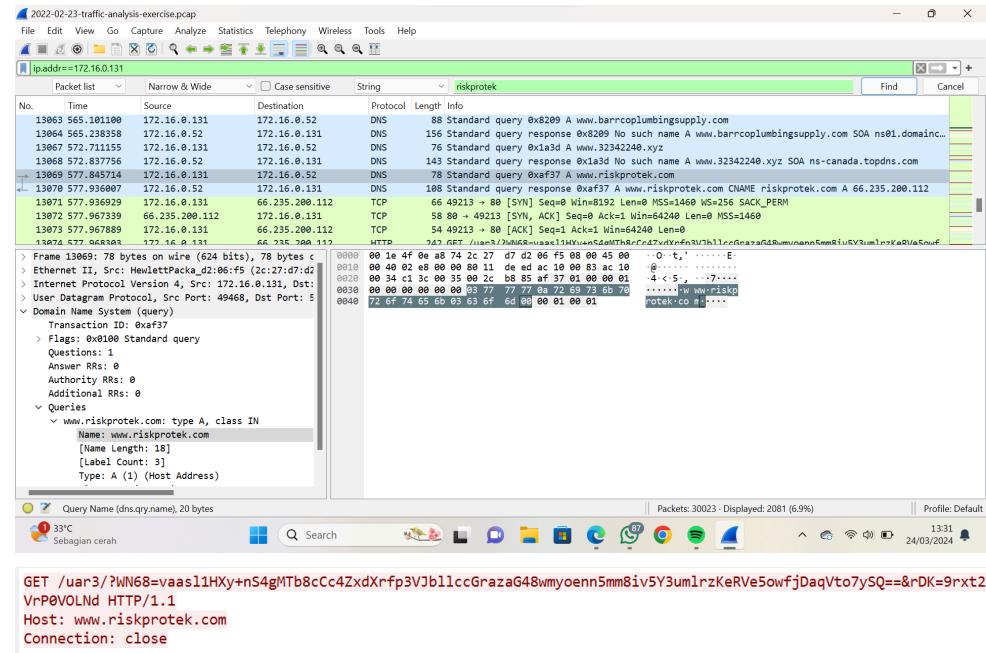
```
GET /uar3/?WN68=PHh1vnmf0w59M/FZc+cjVGc9E+FfGp0TERrr3ixE60uB9RQS+IvYoe8rfvBvY2wGRGtZyza6OrSqVxvPAst7JA==&0xt9d9L=cF  
NTMFXb4s1 HTTP/1.1  
Host: www.czzhudicom  
Connection: close
```

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

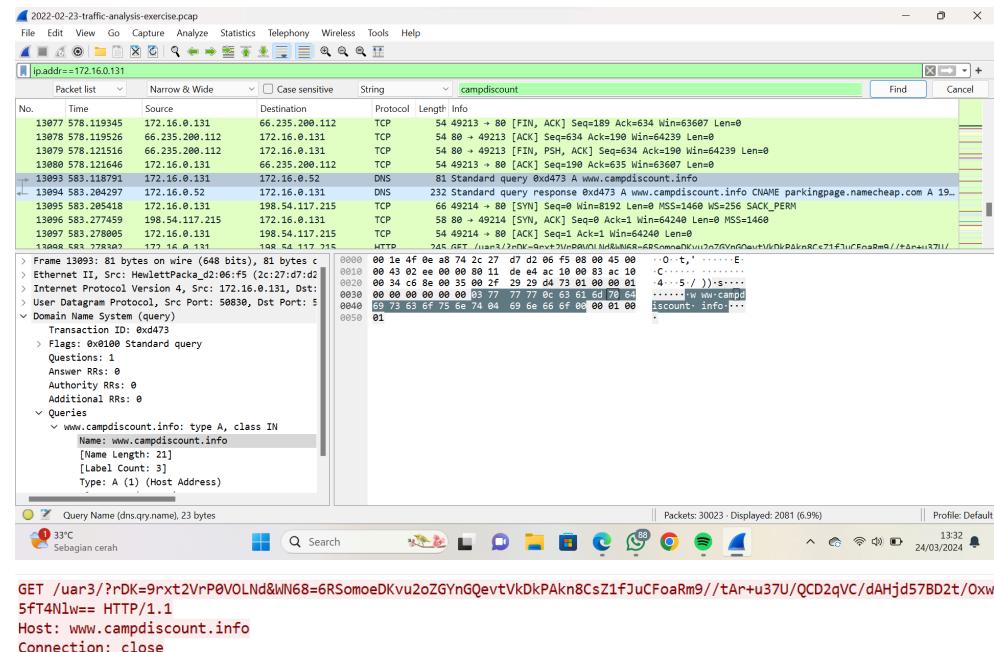


```
GET /uar3/?OXTd9L=cFNTMFX8k4S1&wN68=0eYqjU9fk1JhQ0irTjpk5h8JewsY/FAEEGplD1myE1VivIRdy4CVvbuuzyXb7LJfyhf2G3t0zH0
TabGGRXXlyg== HTTP/1.1
Host: www.hydrocheats.com
Connection: close
```

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



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



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

Screenshot of Wireshark showing network traffic analysis for the IP address 172.16.0.131. The search bar at the top contains "mystore.guide". The packet list shows several DNS queries and responses, with one specific DNS query highlighted. The details pane shows the query for "www.mystore.guide" with a transaction ID of 0x0100 and a question for the A record. The bytes pane shows the raw HTTP request:

```
GET /uar3/?Wn68=AjjsDjhFc3cSa+wvCaKG4qBsq/WHsLY00hpfl+ug958E/QUX/nqsR+NhlSxpTeQKNoKt6jus0BQP11eAYtlQ==&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]

Screenshot of Wireshark showing network traffic analysis for the IP address 172.16.0.131. The search bar at the top contains "theperfecttrainer". The packet list shows several DNS queries and responses, with one specific DNS query highlighted. The details pane shows the query for "www.theperfecttrainer.com" with a transaction ID of 0x0100 and a question for the A record. The bytes pane shows the raw HTTP request:

```
GET /uar3/?rDK=9rxt2VrP0VOLNd&Wn68=I2143oNVzWohwc97LSExaWdVqxBOXBdEroFdfarp+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]

Screenshot of Wireshark showing network traffic analysis for the specified host and port.

Packets: 30023 - Displayed: 2081 (6.9%) | Profile: Default

Selected Packet: No. 13177 (172.16.0.131) | Time: 2022-02-23 13:36:24.136000 | Source: 172.16.0.131 | Destination: www.globalsovereignbank.com | Protocol: TCP | Length: 80

String: globalsovereignbank

Details:

```

Frame 13177: 172.16.0.131 > www.globalsovereignbank.com [TCP: 54.49216 + 80 [RST, ACK] Seq=197 Ack=1577 Win=9 Len=0]
  0000  00 1e 4f 0e a8 74 2c 27 d7 d2 06 f5 08 00 45 00  -O t,'.....E
  0001  00 49 03 00 00 00 88 11 de c4 ac 10 00 83 ac 10  I.....
  0020  00 34 db 58 00 35 05 97 a1 81 84 01 00 00 01 00  4 X-5-
  0030  00 00 00 00 00 00 00 03 77 77 77 13 67 6c 6f 62 61  ....www.globa
  0040  6c 73 0f 76 65 72 65 69 67 6e 62 61 6e 6b 63 63  lsovereignbank.c
  0050  ef 6d 09 00 01 00 01 00 00 00 00 00 00 00 00 00  om.....

```

Selected Query: Query Name (dns.qry.name), 29 bytes

Selected Response: www.globalsovereignbank.com, 27 bytes

Selected Data:

```

GET /uar3/?WN68=yHzgZciQ0pBj/8G1dSJukDWWY4SQVbEV+RnWrDBs6A2k1s4c6xvZXPb28QBvYg5FyuTRLTP9+/gPb7Dyx9A==&rDK=9rxt2
VrP0VOLND HTTP/1.1
Host: www.globalsovereignbank.com
Connection: close

```

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

Screenshot of Wireshark showing network traffic analysis for the specified host and port.

Packets: 30023 - Displayed: 2081 (6.9%) | Profile: Default

Selected Packet: No. 13956 (172.16.0.131) | Time: 2022-02-23 13:37:24.136000 | Source: 172.16.0.131 | Destination: www.keysine.com | Protocol: TCP | Length: 80

String: keysine

Details:

```

Frame 13956: 172.16.0.131 > www.keysine.com [TCP: 54.49223 + 80 [RST, ACK] Seq=192 Ack=2777 Win=9 Len=0]
  0000  00 1e 4f 0e a8 74 2c 27 d7 d2 06 f5 08 00 45 00  -O t,'.....E
  0001  00 49 03 00 00 00 88 11 de c4 ac 10 00 83 ac 10  I.....
  0020  00 34 db 58 00 35 05 97 a1 81 84 01 00 00 01 00  4 X-5-
  0030  00 00 00 00 00 00 00 03 77 77 77 13 67 6c 6f 62 61  ....www.keys
  0040  6c 73 0f 76 65 72 65 69 67 6e 62 61 6e 6b 63 63  ne.com.....

```

Selected Query: Query Type (dns.qry.type), 2 bytes

Selected Response: www.keysine.com, 15 bytes

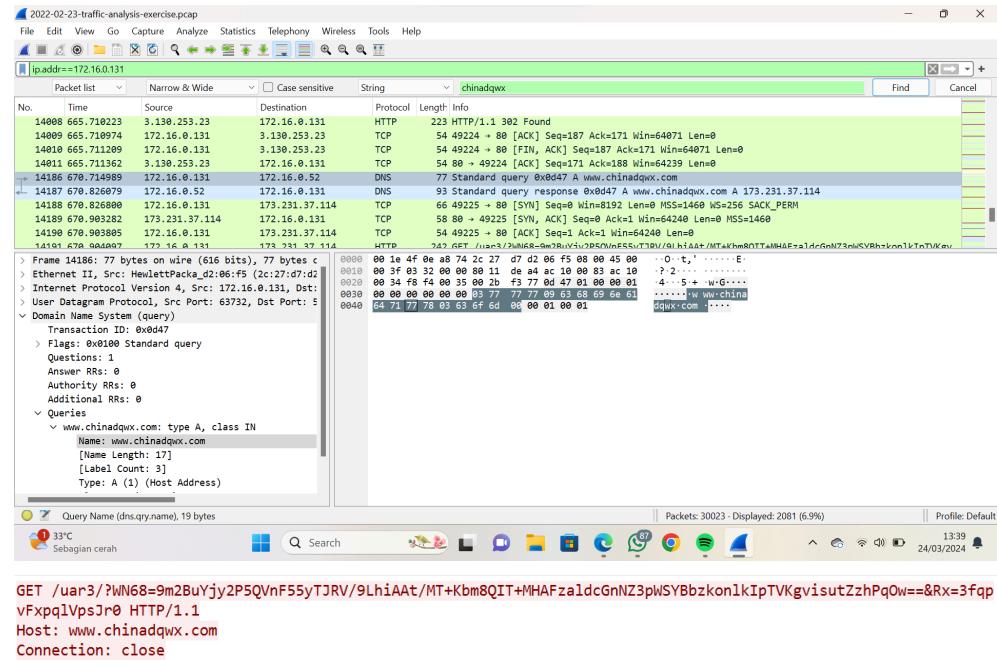
Selected Data:

```

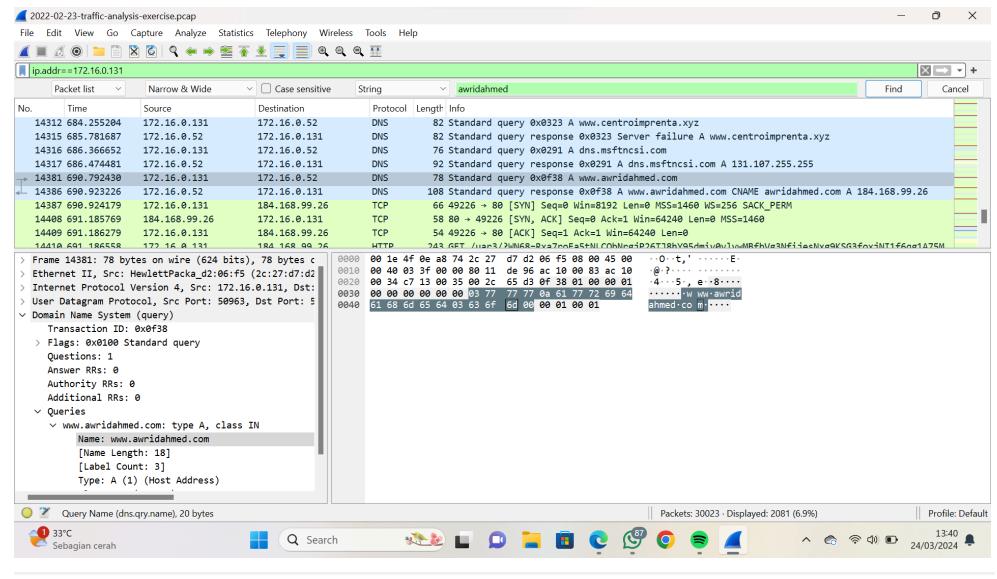
GET /uar3/?Rx=3fqpvFxpqlVpsJr&WN68=rUb9fjakxYTFD8z67QPd/z9ZU79Kig+C682K4H/u+g+BDuvQEiej59oCwTmjTn3VIgEsDrJTMhelf
jdUr/10Q== HTTP/1.1
Host: www.keysine.com
Connection: close

```

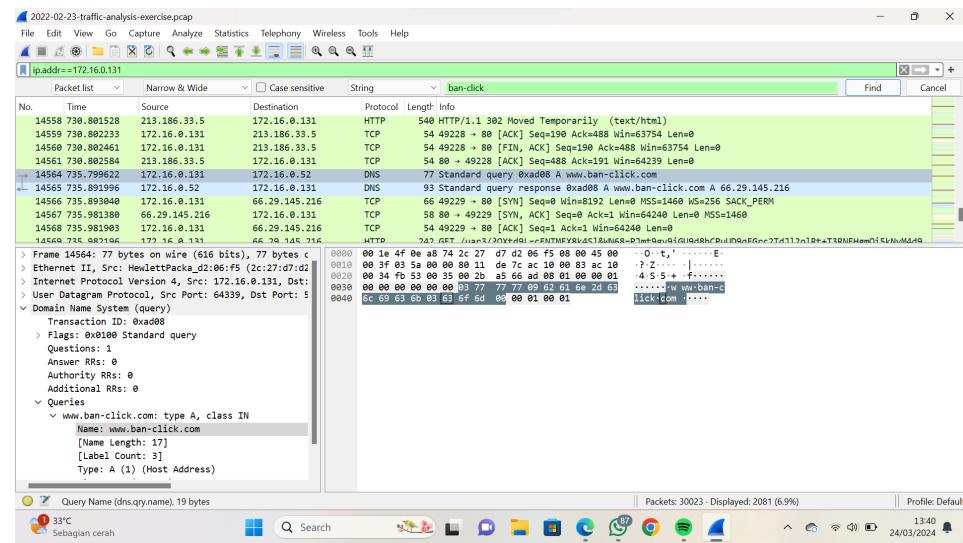
173.231.37.114:80 - www.chinadqwx.com - GET /uar3/?[base64 style string]



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

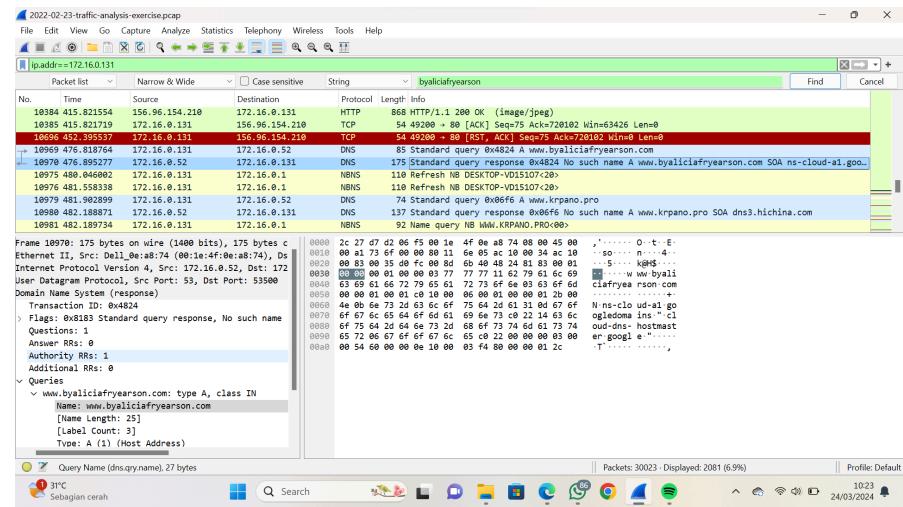


66.29.145.216:80 - www.ban-click.com - GET /uar3/?[base64 style string]

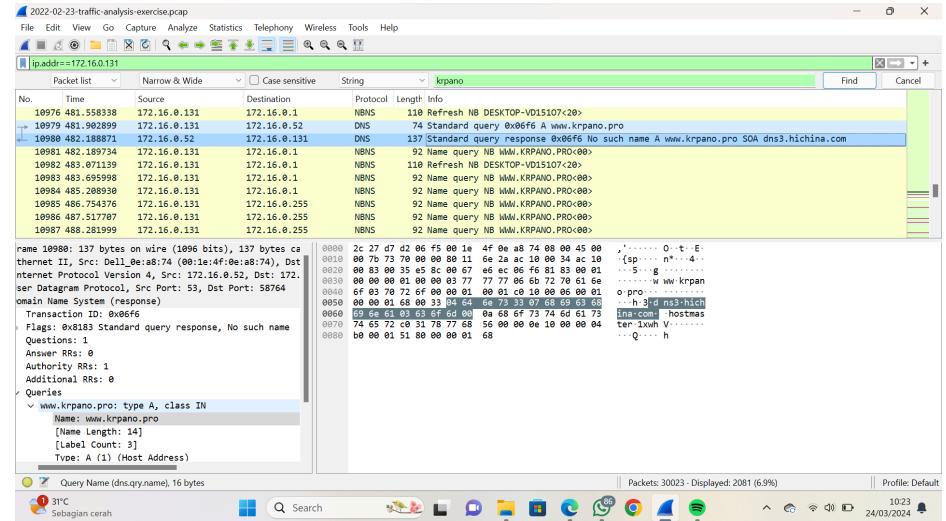


```
GET /uar3/?OXtd9L=cFNTMFX8k4S1&wN68=PJmt9gv9iGU9d8hCPuUD9qFGrc2TdJ12o1Rt+T3RNFHgmOis5kNyM4d9HjU8Ipcbb+g/FLincIuHx0$310!wNfw== HTTP/1.1
Host: www.ban-click.com
Connection: close
```

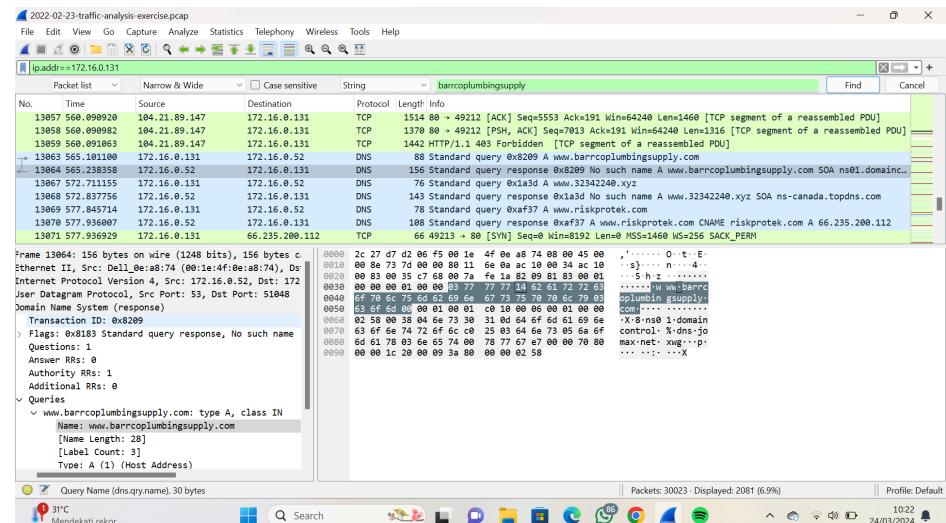
DNS queries for Formbook/XLoader C2 traffic:
www.byaliciafryearson.com - response: No such name



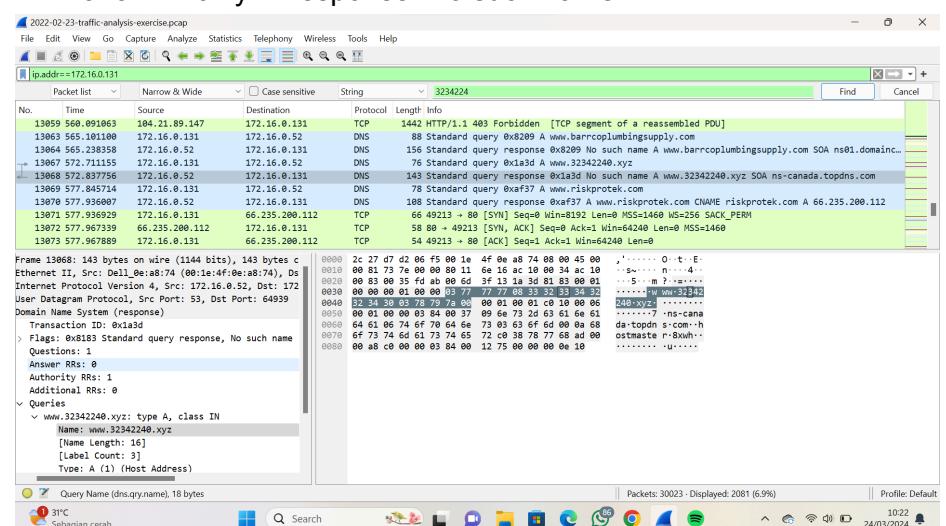
www.krpano.pro - response: No such name



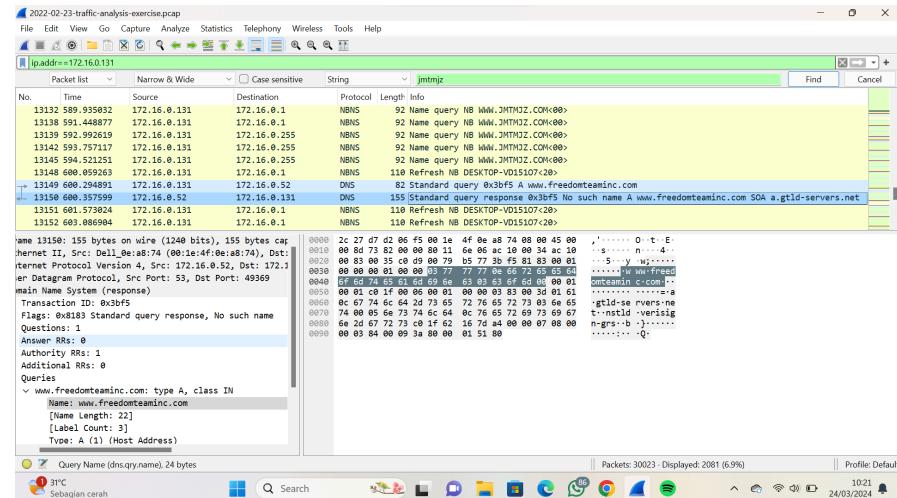
www.barrcoplumbingsupply.com - response: No such name



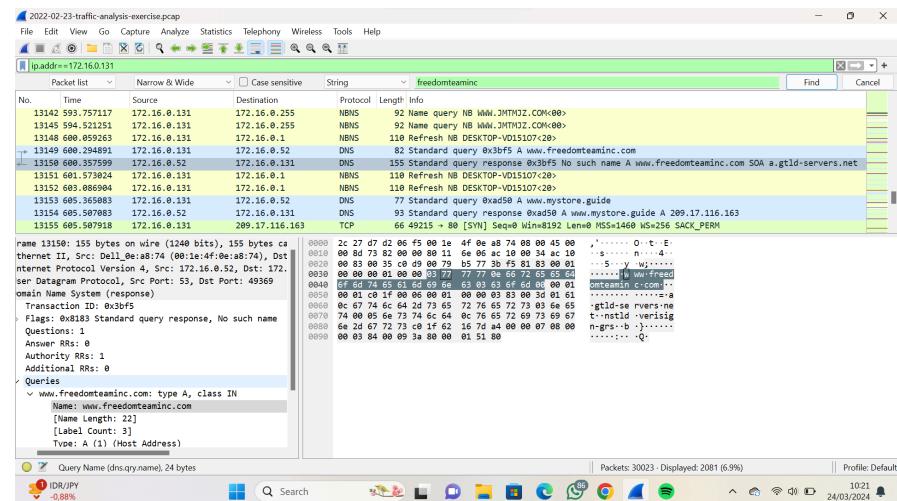
www.32342240.xyz - response: No such name



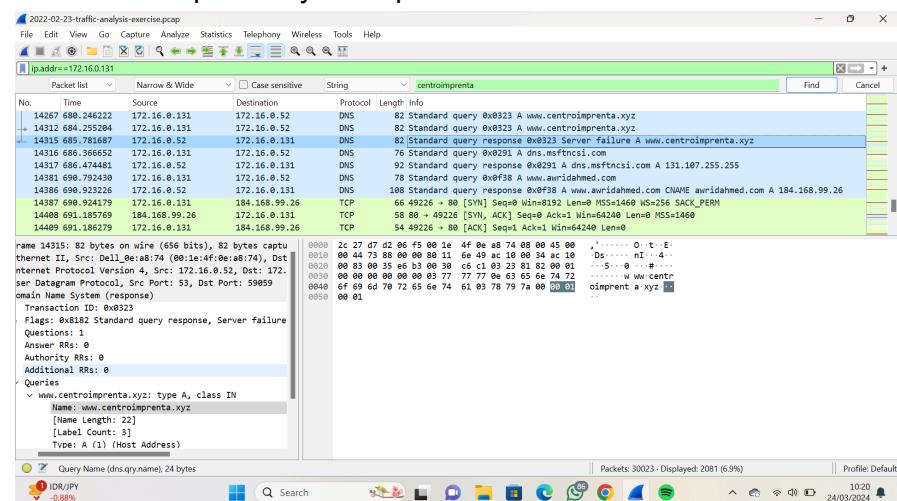
www.jmtmjz.com - response: No such name



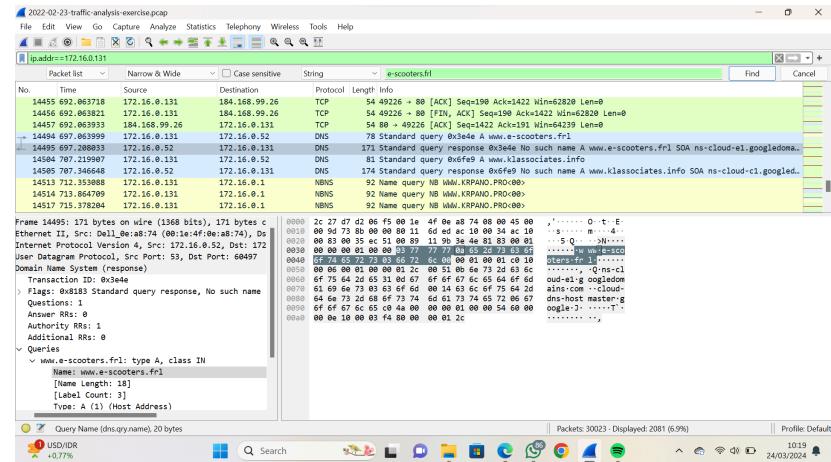
www.freedomteaminc.com - response: No such name



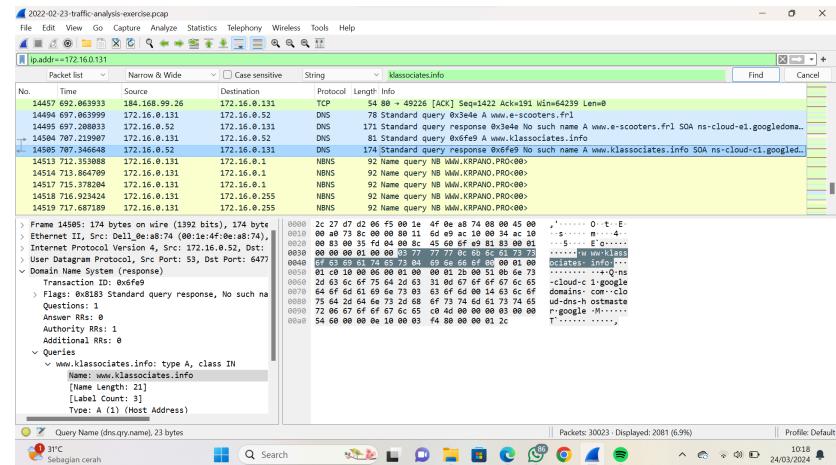
www.centroimprenta.xyz - response: Server failure



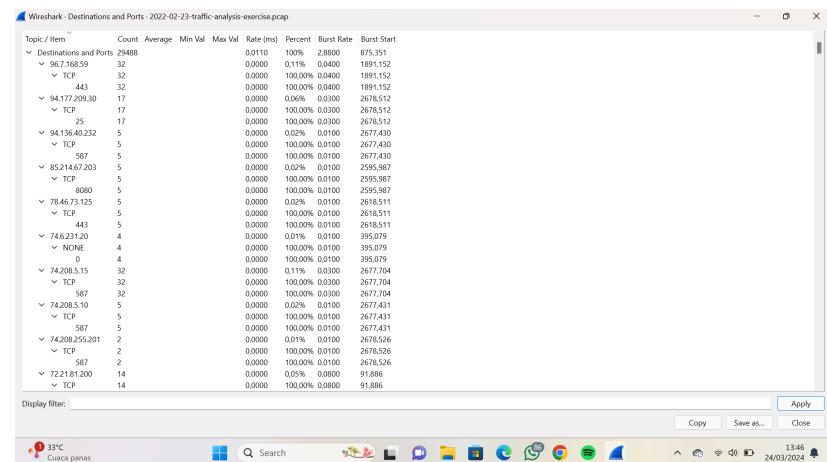
www.e-scooters.frl - response: No such name



www.klassociates.info - response: No such name



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



Display filter: Apply Copy Save as... Close



13:47
24/03/2023

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
▼ TCP	30				0.0000	100.00%	0.1200	255.9845
▼ TCP	443	30			0.0001	100.00%	0.1200	255.9845
▼ 50.14.62.23.194	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
▼ 54.83.342.185	12				0.0000	0.00%	0.2000	2320.474
▼ TCP	12				0.0000	100.00%	0.2000	2320.474
▼ 443	12				0.0000	100.00%	0.3000	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%	0.3000	2418.719
▼ TCP	13				0.0000	100.00%	0.3000	2418.719
▼ 443	13				0.0000	100.00%	0.3000	2418.719
▼ 52.238.248.44	44				0.0000	0.12%	0.1000	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
▼ 52.165.21.1133	34				0.0000	0.12%	0.5000	101.1408
▼ TCP	34				0.0000	100.00%	0.5000	101.1408
▼ 443	34				0.0000	100.00%	0.5000	101.1408
▼ 52.16.123.20.149	42				0.0000	0.04%	0.0600	385.9501
▼ TCP	42				0.0000	100.00%	0.0600	385.9501
▼ 443	42				0.0000	100.00%	0.0600	385.9501
▼ 52.16.124.16.1	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
▼ 52.16.181.17.69	25				0.0000	0.06%	0.5000	206.528

The taskbar at the bottom of the screen displays several pinned icons, including the Start button, File Explorer, Task View, Mail, Photos, OneDrive, Edge, and a few others. To the right, there are icons for battery level (15%), signal strength, and a date/time stamp (24/07/2023, 15:57). A search bar is also present.

Wireshark - Destinations and Ports - 2022-02-23-traffic-analysis-exercise-23

Topic / Item	Count	Average	Min Val	Max Val	Rate (m/s)	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	0.11%	0.1100		1680.516	
TCP	37		0.0000	0.11%	0.1100		1680.516	
443	37		0.0000	100.00%	0.0700		1680.516	
52.109.19	35		0.0000	0.12%	0.0900		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		168.464	
TCP	9		0.0000	100.00%	0.0300		168.464	
443	9		0.0000	100.00%	0.0300		168.464	
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	
8000	5		0.0000	100.00%	0.0100		2412.310	
40.93.162.162	14		0.0000	0.05%	0.0400		2678.844	
TCP	14		0.0000	100.00%	0.0400		2678.844	
507	14		0.0000	100.00%	0.0400		2678.844	
40.83.240.146	30		0.0000	0.1%	0.0500		430.324	
TCP	30		0.0000	100.00%	0.0500		430.324	
443	30		0.0000	100.00%	0.0500		430.324	
40.152.6.75	11		0.0000	0.04%	0.0400		1088.531	
TCP	11		0.0000	100.00%	0.0400		1088.531	
443	11		0.0000	100.00%	0.0400		1088.531	
40.152.5.32	24		0.0000	0.08%	0.0600		1840.463	
TCP	24		0.0000	100.00%	0.0600		1840.463	
443	24		0.0000	100.00%	0.0600		1840.463	
40.126.25.9	10		0.0000	0.03%	0.0600		2401.057	

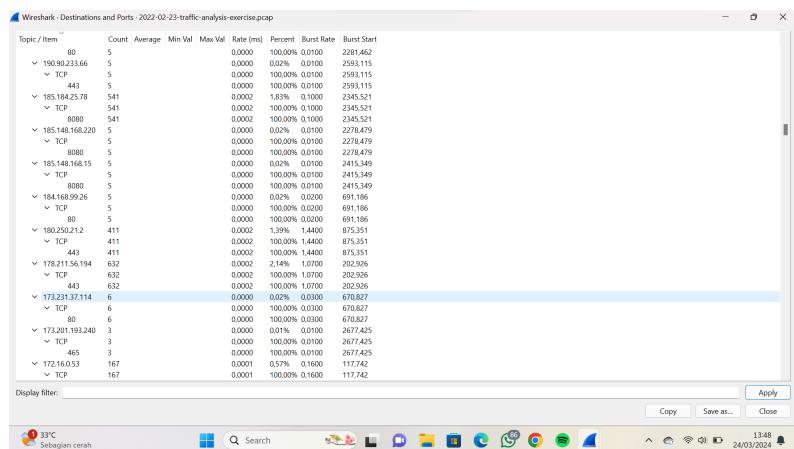
Display filter: `(not _source == 192.168.1.1) and (port 80 or port 443)`

Screenshot copied to clipboard and saved
Selbsttest bearbeitet und abrechnen sieger

13:47
24/03/2024

Protocol / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
46 152.122.151	1	0.0000	0.0596	0.0590	691.646			
TCP	1	0.0000	100.00%	0.0590	691.646			
26	1	0.0000	100.00%	0.0590	691.646			
443	1	0.0000	100.00%	0.0590	691.646			
37.59.209.141	4	0.0000	0.01%	0.0100	2671.004			
TCP	4	0.0000	100.00%	0.0100	2671.004			
8080	4	0.0000	100.00%	0.0100	2671.004			
4444.44.177.5	5	0.0000	0.01%	0.0100	2671.759			
TCP	5	0.0000	100.00%	0.0100	2671.759			
8080	5	0.0000	100.00%	0.0100	2671.759			
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	5	0.0000	0.03%	0.0200	2679.392			
TCP	8	0.0000	100.00%	0.0200	2679.392			
507	8	0.0000	100.00%	0.0200	2679.392			
21.252.14.84	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	0.00%	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			
192.168.0.6	8	0.0000	0.00%	0.0200	1886.752			
192.168.0.5	8	0.0000	0.00%	0.0200	1886.752			
13.47.49.165	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			

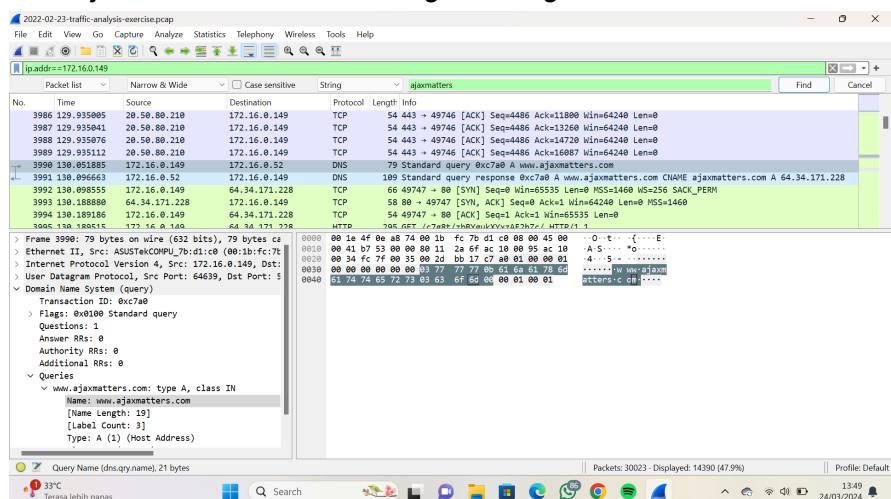
33°C Sebagian cerah ⌂ Search ⌂ Save... ⌂ Close ⌂ Copy ⌂ 13:47 ⌂ 24/03/2024



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