2018 TRAFFIC ANALYSIS WORKSHOP

http://malware-traffic-analysis.net/2018/workshop/AusCERT/

Brad Duncan
Threat Intelligence Analyst
@malware_traffic

unit42

2018 Traffic Analysis Workshop - Outline

- **Block 1 - Intro and setting up Wireshark**
- **Block 2 - Identifying host & users**
- **Block 3 - Malware infections**
- **Block 4 - Bad web traffic**
- **Block 5 - Policy violations**
- **Block 6 - Root causes & false positives**
- **Block 7 - Writing incident reports**
- **Block 8 - Evaluation**

2018 TRAFFIC ANALYSIS WORKSHOP

Block 1: Introduction and setting up Wireshark

Block 1 - Overview

- Network Security Monitoring (NSM)
- Wireshark & other pcap analysis tools
- A few words about incident reporting
- Wireshark setup

Network Security Monitoring (NSM)

Different levels of NSM

- Activity logs gathered from individual hosts
- Alerts on network traffic with some of the network information
- Netflow data
- Full packet capture

Network Security Monitoring (NSM)

Different levels of NSM

- Activity logs gathered from individual hosts
- Alerts on network traffic with some of the network information
- Netflow data
- Full packet capture

SIEM

Network Security Monitoring (NSM)

2018-traffic-analysis-workshop-block-1-01.pcap

2018-05-11 15:52 UTC
Src: 10.5.11.101 port 49220
Dst: 95.142.39.26 port 80

ET CURRENT_EVENTS RIG EK URI Struct Jun 13 2017

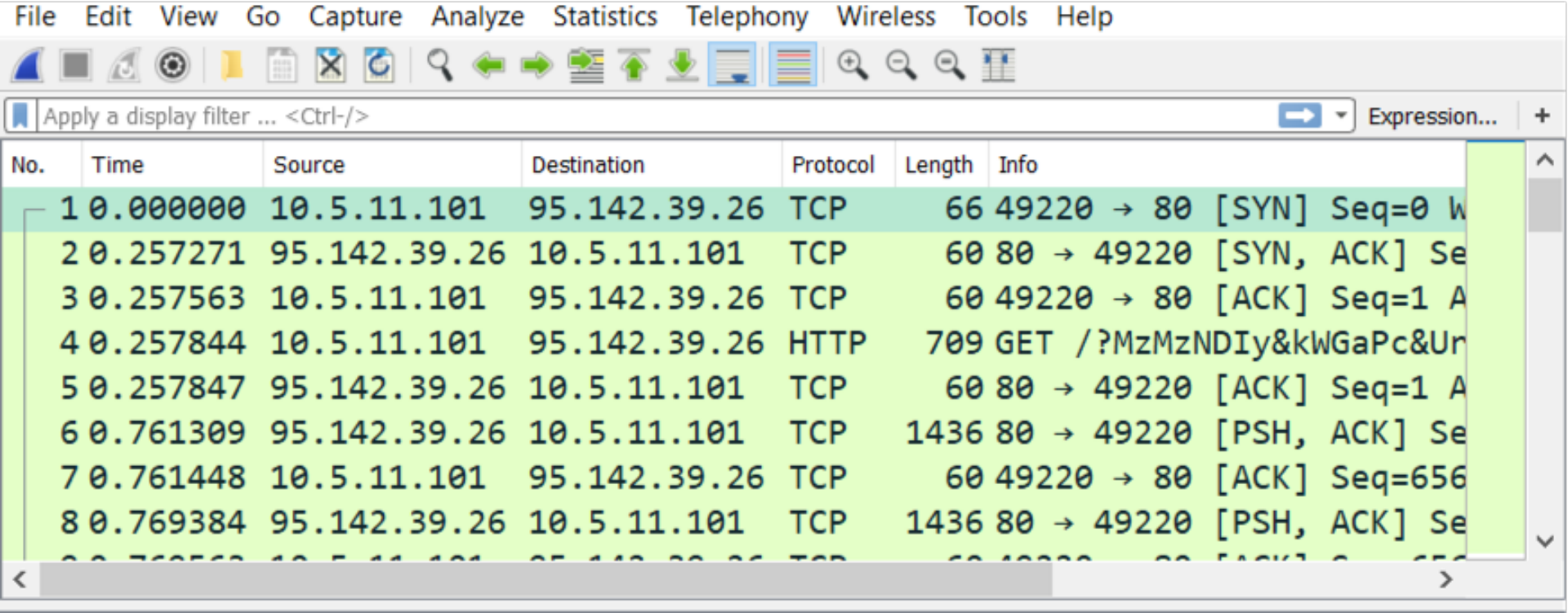
Network Security Monitoring (NSM)

```
Date flow start                 Duration  Proto
2018-05-11 11:52:05.103  1.911     TCP
2018-05-11 11:52:05.361  1.653     TCP

Src IP Addr:Port -> Dst IP Addr:Port
10.5.11.101:49220 -> 95.142.39.26:80
95.142.39.26:80 -> 10.5.11.101:49220

Packets  Bytes  Flows
31         2332   1
31        65813   1
```

FLOW DATA

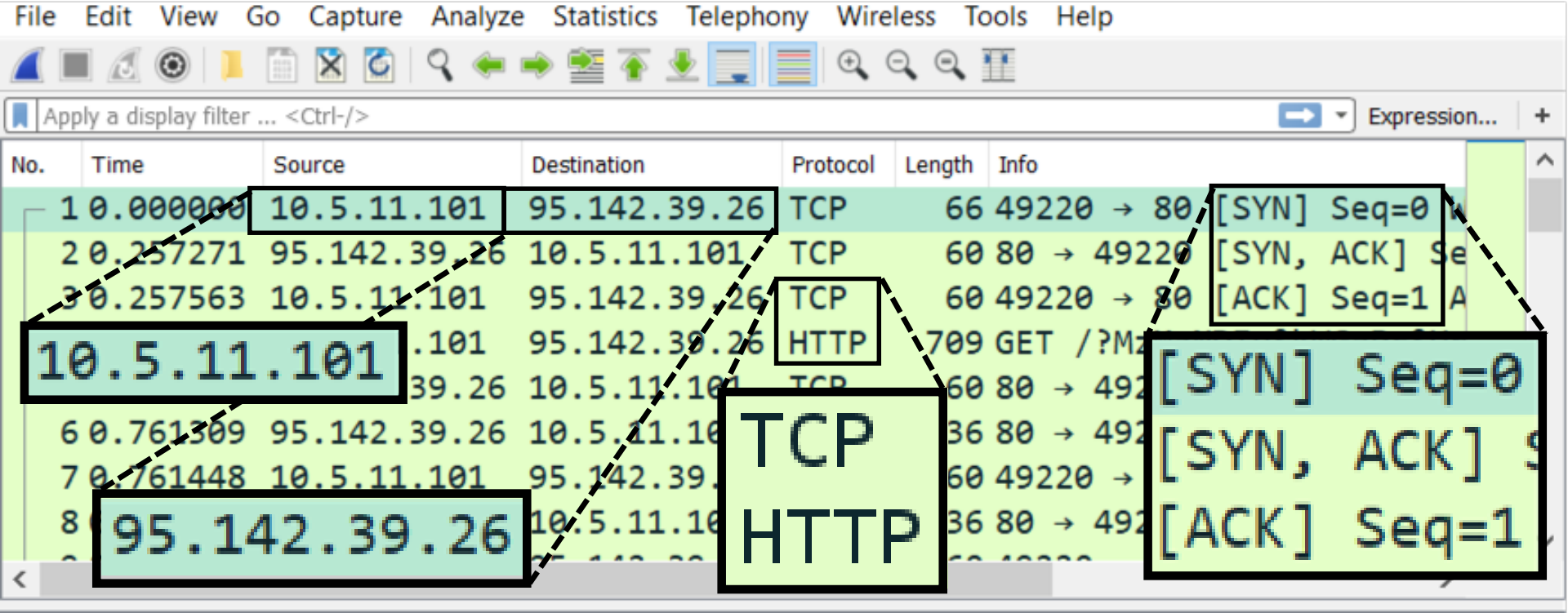
Network Security Monitoring (NSM)

2018-traffic-analysis-workshop-block-1-01.pcap



Network Security Monitoring (NSM)

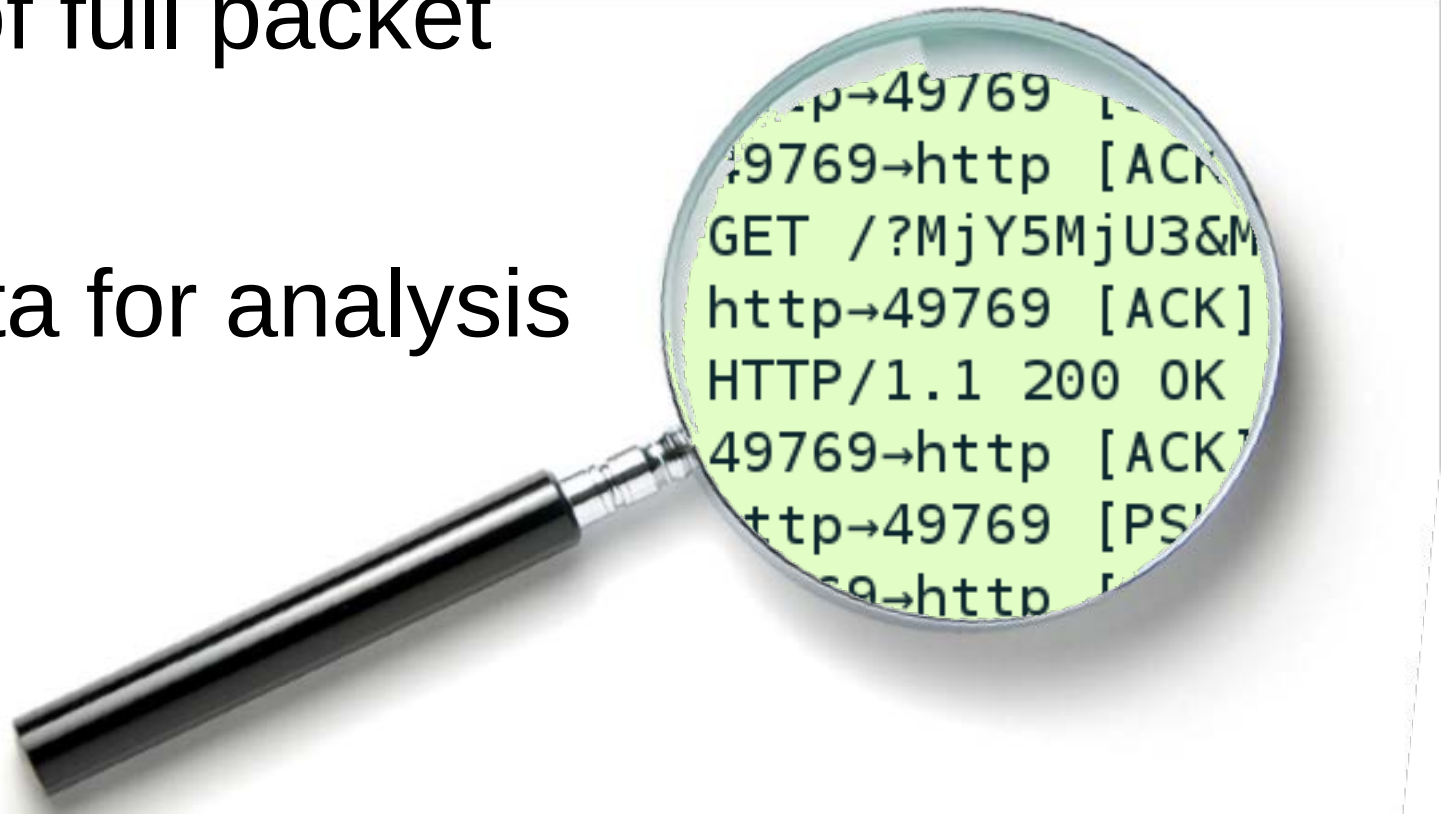
2018-traffic-analysis-workshop-block-1-01.pcap



Network Security Monitoring (NSM)

Benefit of full packet capture:

More data for analysis



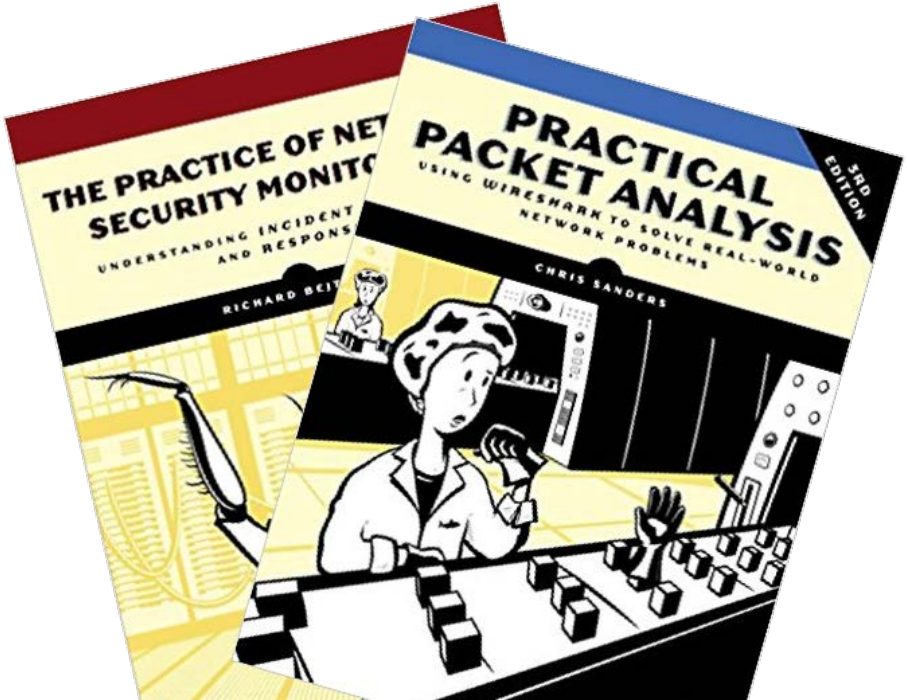
Network Security Monitoring (NSM)

Drawback of full packet capture:

More data to store

Network Security Monitoring (NSM)

Final drawback of full packet capture:

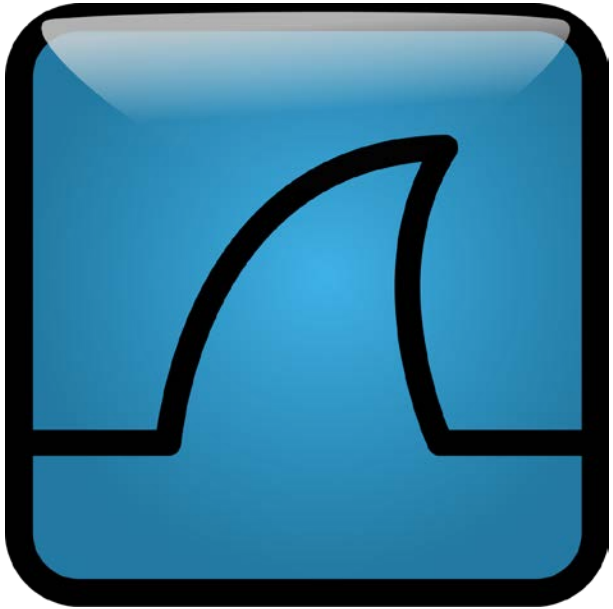


The need for trained or experienced personnel

Block 1 - Up next...

- Network Security Monitoring (NSM)
- **Wireshark & other pcap analysis tools**
- A few words about Incident reporting
- Wireshark setup

Wireshark & other pcap analysis tools



Wireshark has a customizable graphical user interface (GUI) that makes it extremely easy to find out what's going on in a pcap.

Wireshark & other pcap analysis tools

Other tools to review pcaps:

- Text-based tools like **tcpdump** or **tshark**
- Automated tools like **NetworkMiner**
- Online tools like **PacketTotal**

Wireshark & other pcap analysis tools

https://packettotal.com/

PacketTotal

Simple, free, high-quality PCAP analysis

2018-traffic-analysis-workshop-block-1-01.pcap

Drag .pcap files here or click to upload.

(Accepts .pcap and .pcapng files. Limit 50 MB.)

Wireshark & other pcap analysis tools

File Metadata

Name: 2018trafficanalysiswor.pcap **MD5:** c3622b3fa78e51efd30ffb6a4c4a67ec

Size: 0.070961 MB **Submitted:** United States

Malicious Activity | Connections | HTTP | Transferred Files | Similar Packet Captures

Search in results

Timestamp	Alert Signature	Sender IP	Sender Port	Target IP
2018-05-11 15:52:05	ET CURRENT_EVENTS RIG EK URI Struct Jun 13 2017	10.5.11.101	49220	95.142.39.26

Block 1 - Up next...

- Network Security Monitoring (NSM)
- Wireshark & other pcap analysis tools
- **A few words about incident reporting**
- Wireshark setup

A few words about incident reporting

What is an incident?

An event that impairs the confidentiality, integrity, or availability of your IT systems or network.

A few words about incident reporting

Examples:

- Computer infected with malware
- Attacker exploits vulnerability and gains admin access to a server
- Victim of a phishing email gives out login credentials

A few words about incident reporting

An incident report gives the reader a clear idea of what happened.

A few words about incident reporting

When?

Who?

What?

Block 1 - Up next...

- Network Security Monitoring (NSM)
- Wireshark & other pcap analysis tools
- A few words about incident reporting
- **Wireshark setup**

Block 1 - Wireshark setup

- Web traffic & default Wireshark display
- Removing and adding columns
- Changing time to UTC date and time
- Adding custom columns
- Hiding columns

Web traffic & default Wireshark display

RSS feed About this blog @malware_traffic on Twitter

Click here -- for some tutorials that will help for these exercises.

Since the summer of 2013, this site has published over 1,300 blog entries about malicious network traffic. Almost every post on this site has pcap files or malware samples (or both).

Traffic Analysis Exercises

- **Click here** -- for training exercises to analyze pcap files of network traffic.

Click here -- for some tutorials that will help for these exercises.

My Technical Blog Posts

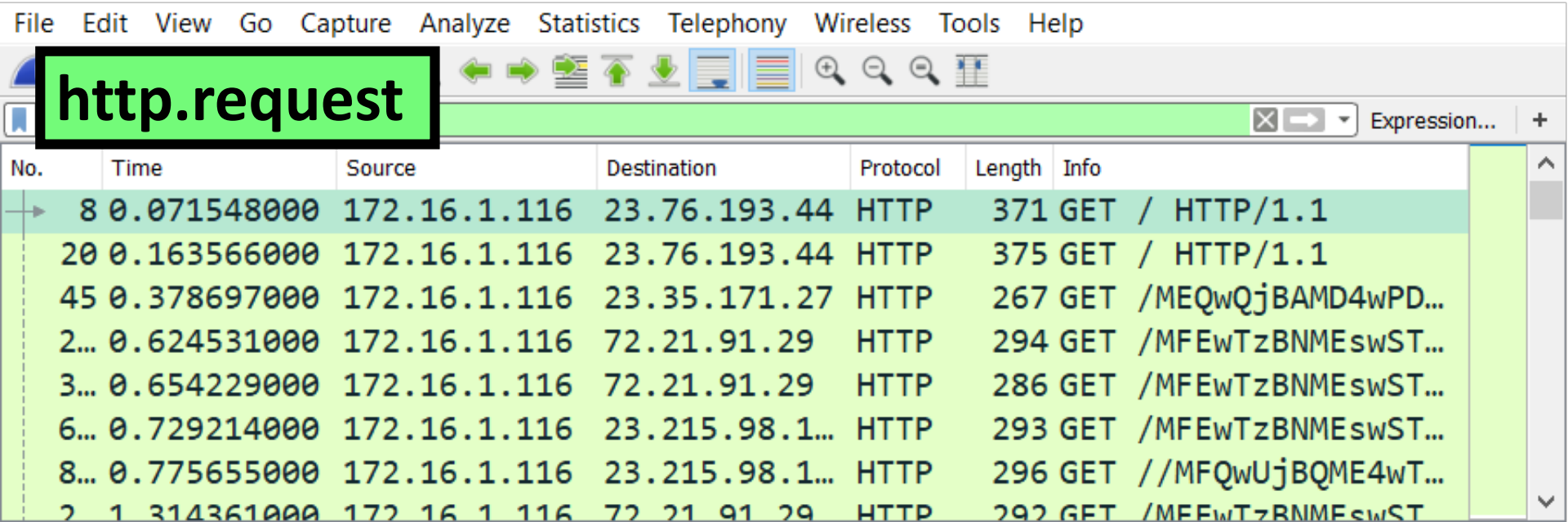
- Click on the appropriate year for the blog posts I've done - [**2013**] - [**2014**] - [**2015**] - [**2016**] - [**2017**] - [**2018**]

My Non-Technical Blog Posts

Web traffic & default Wireshark display

2018-traffic-analysis-workshop-block-1-02.pcap

Default column display not ideal for HTTP traffic



Web traffic & default Wireshark display

What should we see instead?

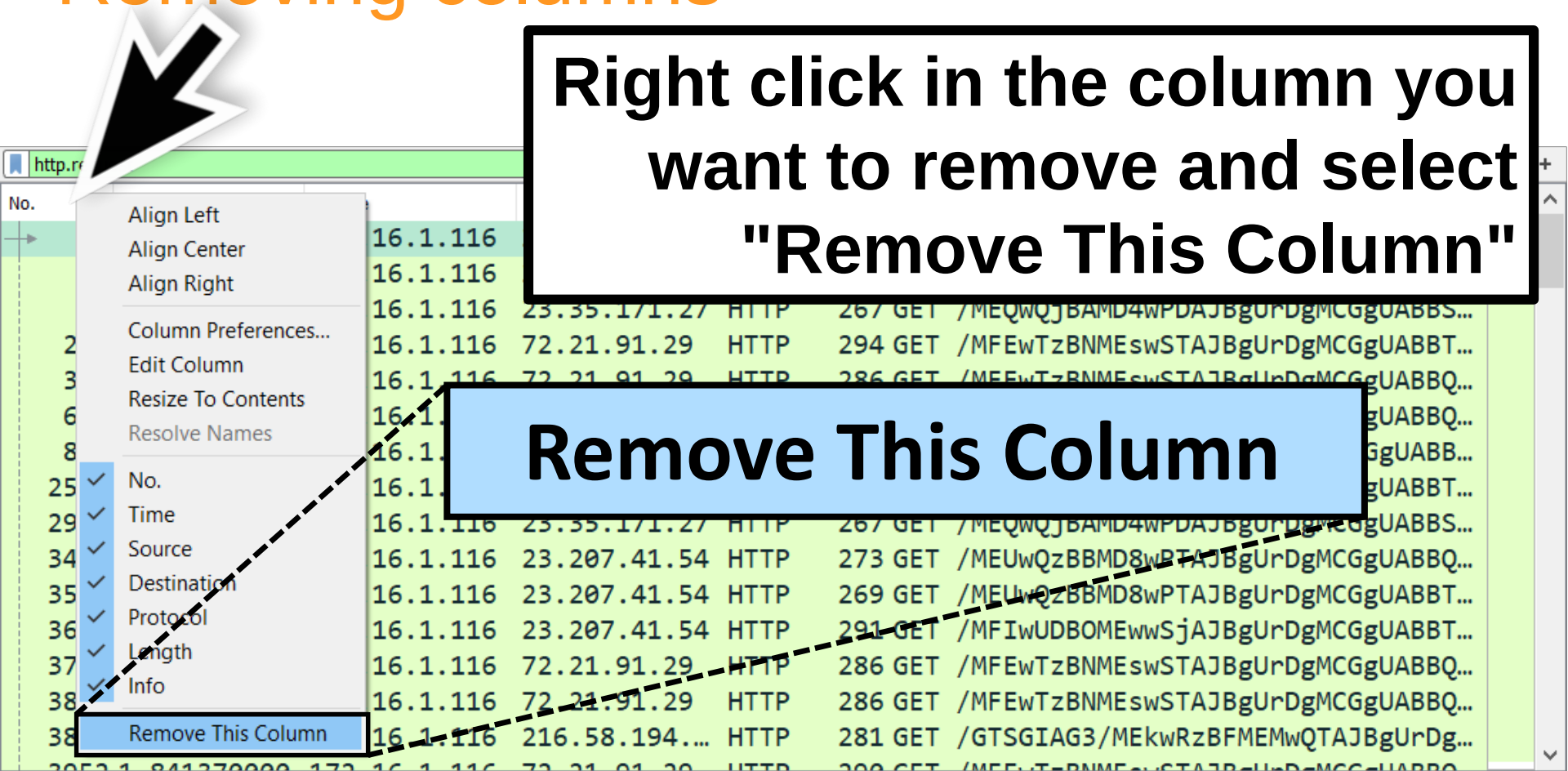
- Date & time in UTC
- Source IP and source port
- Destination IP and destination port
- HTTP host
- HTTPS server
- Info

Up next...

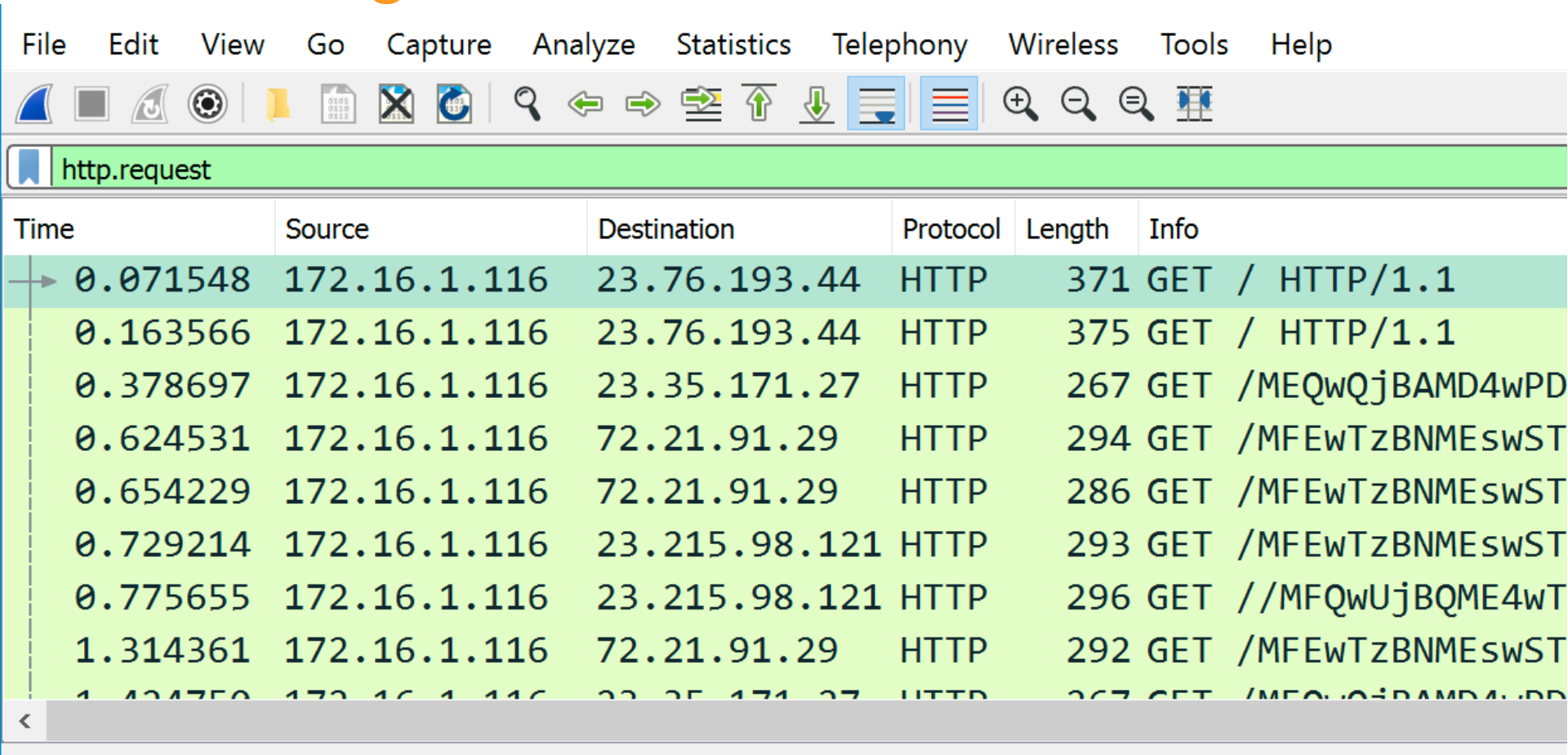
- Web traffic & default Wireshark display
- **Removing and adding columns**
- Changing time to UTC date and time
- Adding custom columns
- Hiding columns

Removing columns

Right click in the column you want to remove and select "Remove This Column"

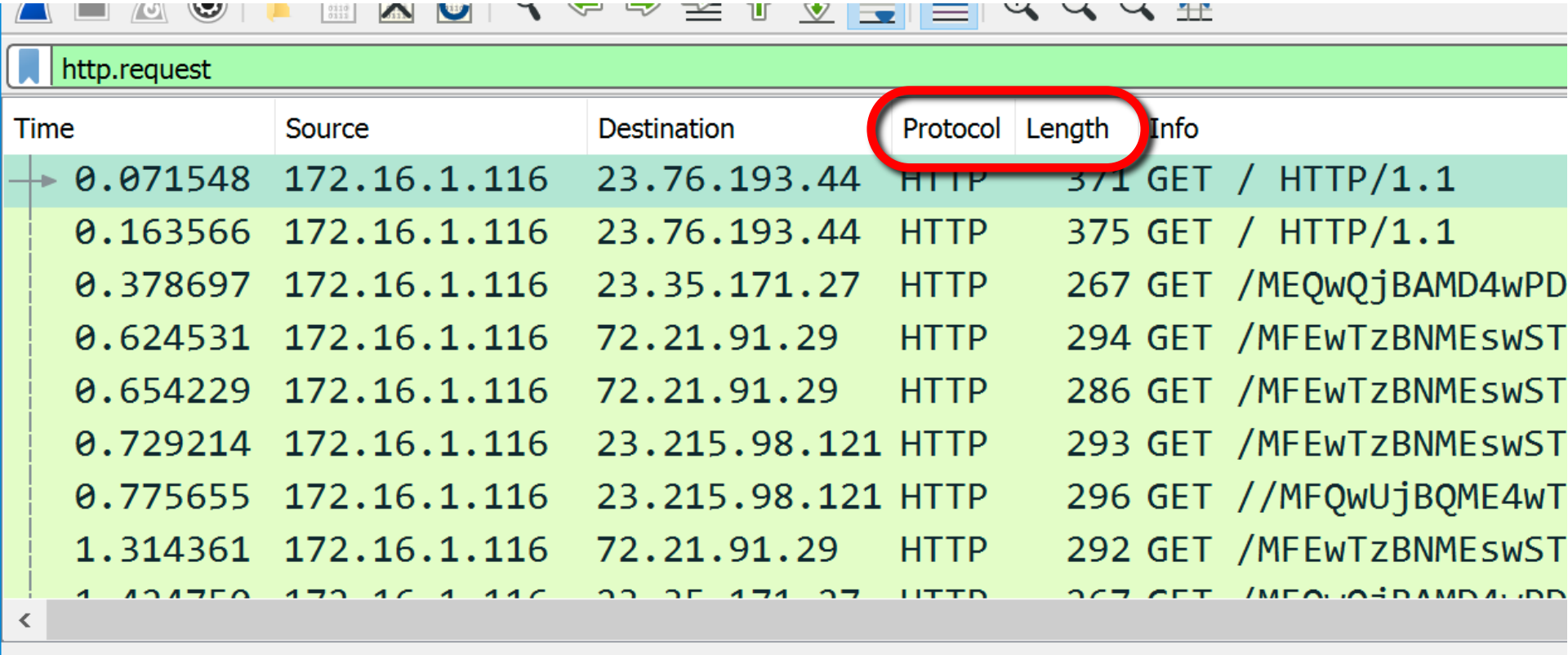


Removing columns



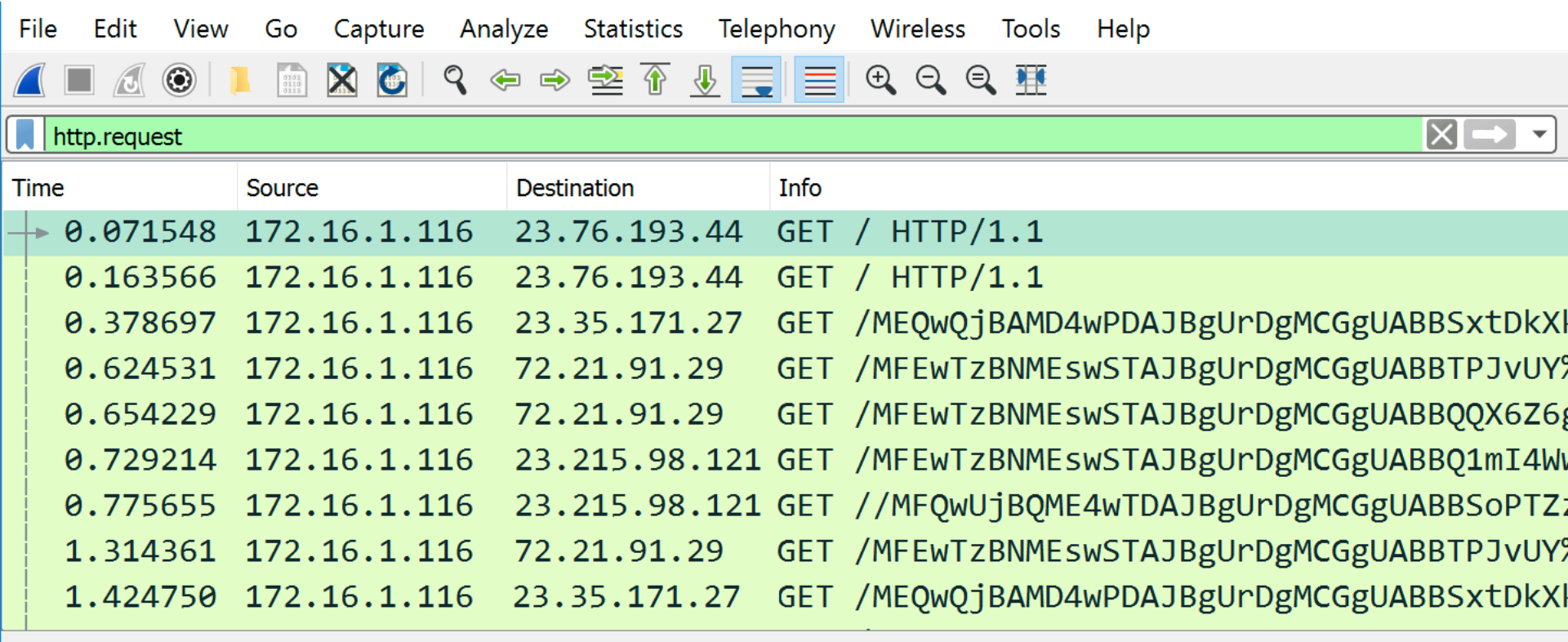
Removing columns

Do the same thing for **Protocol** and **Length**



Removing columns

Remaining: **Time**, **Source**, **Destination**, & **Info**

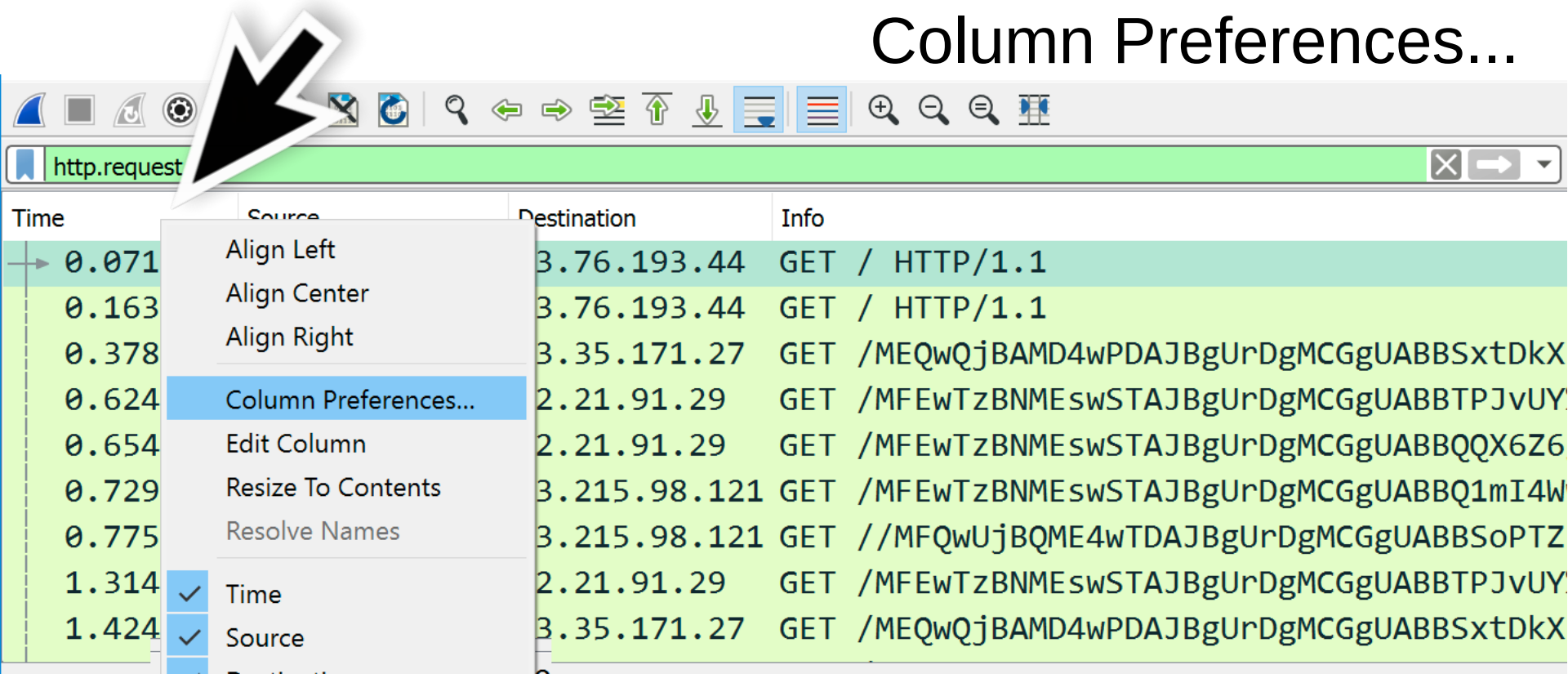


Adding columns

- Removing columns 
- **Adding columns**

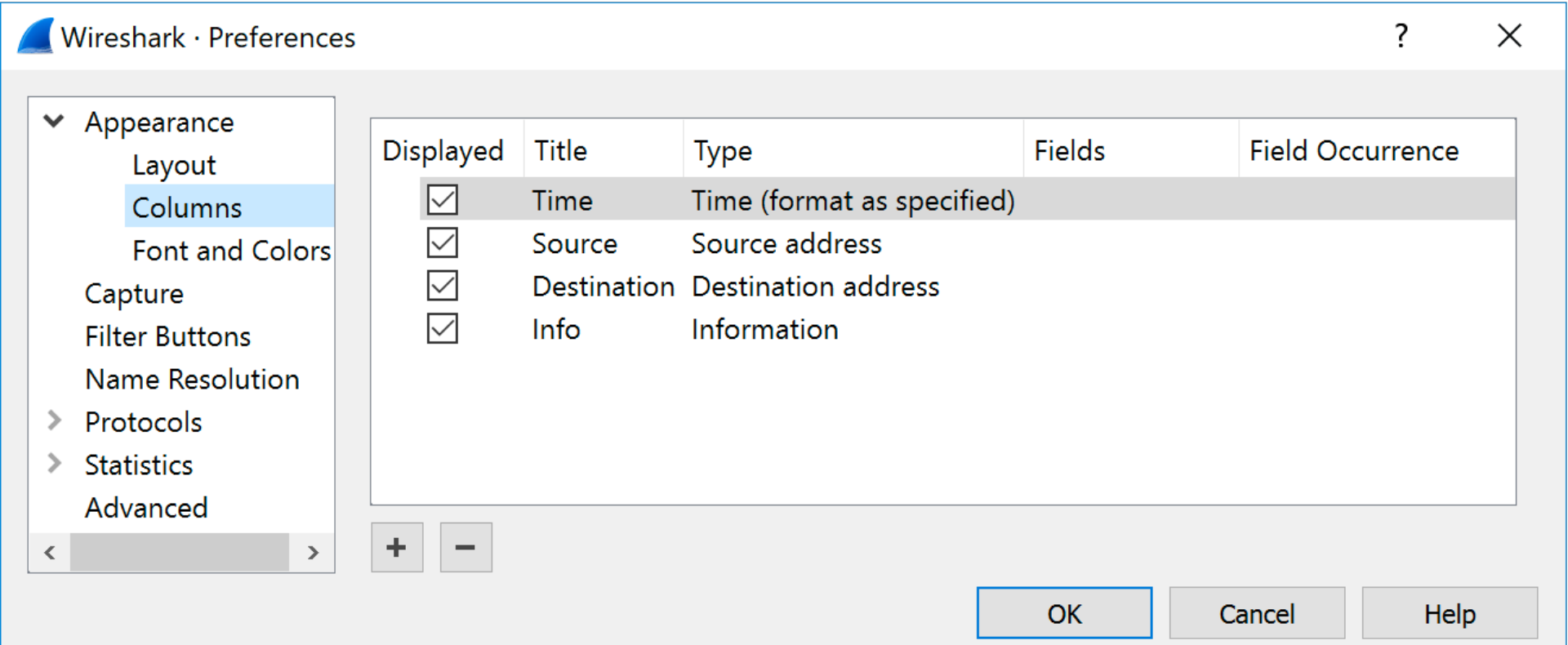
Adding columns

Right click any of the column headers and select Column Preferences...

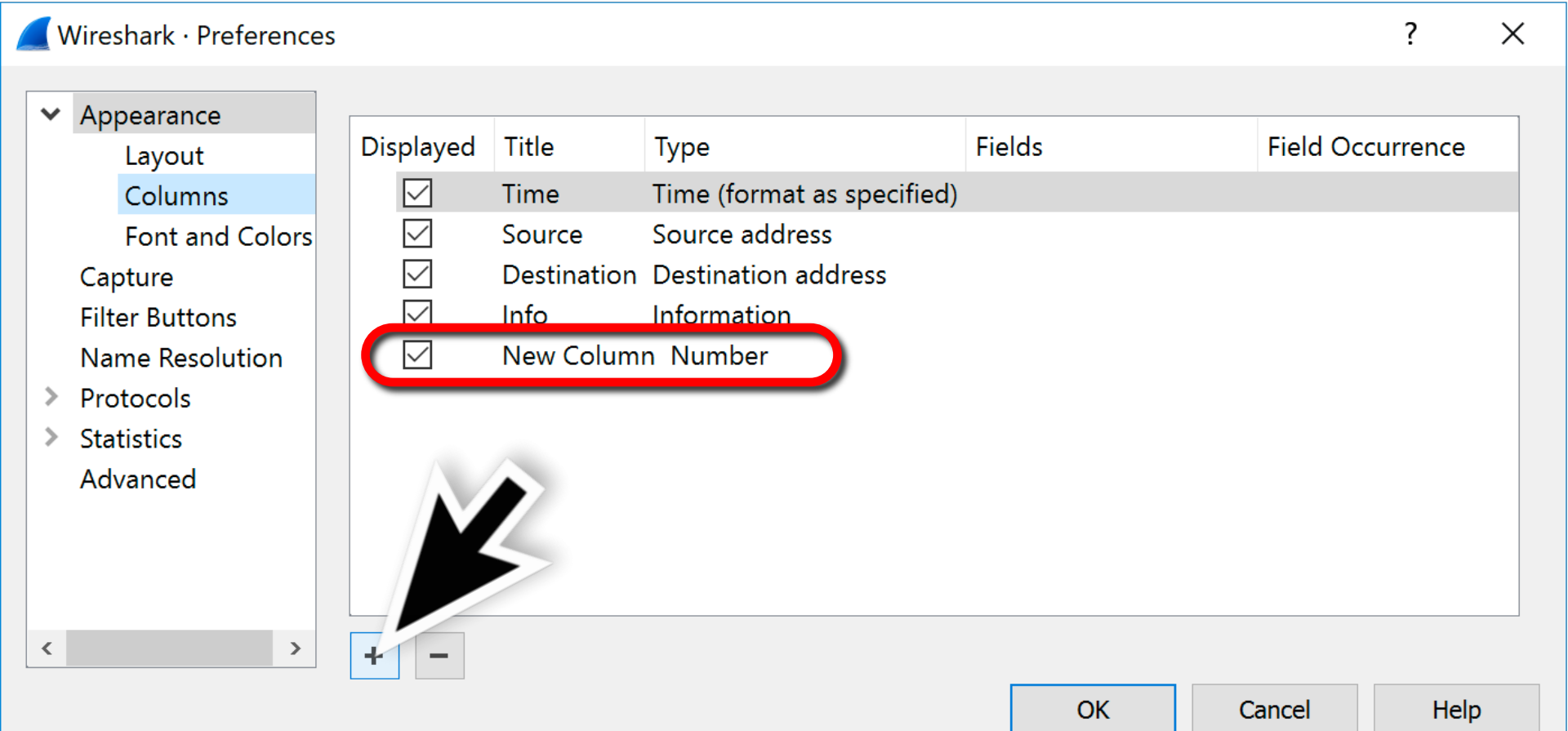


Adding columns

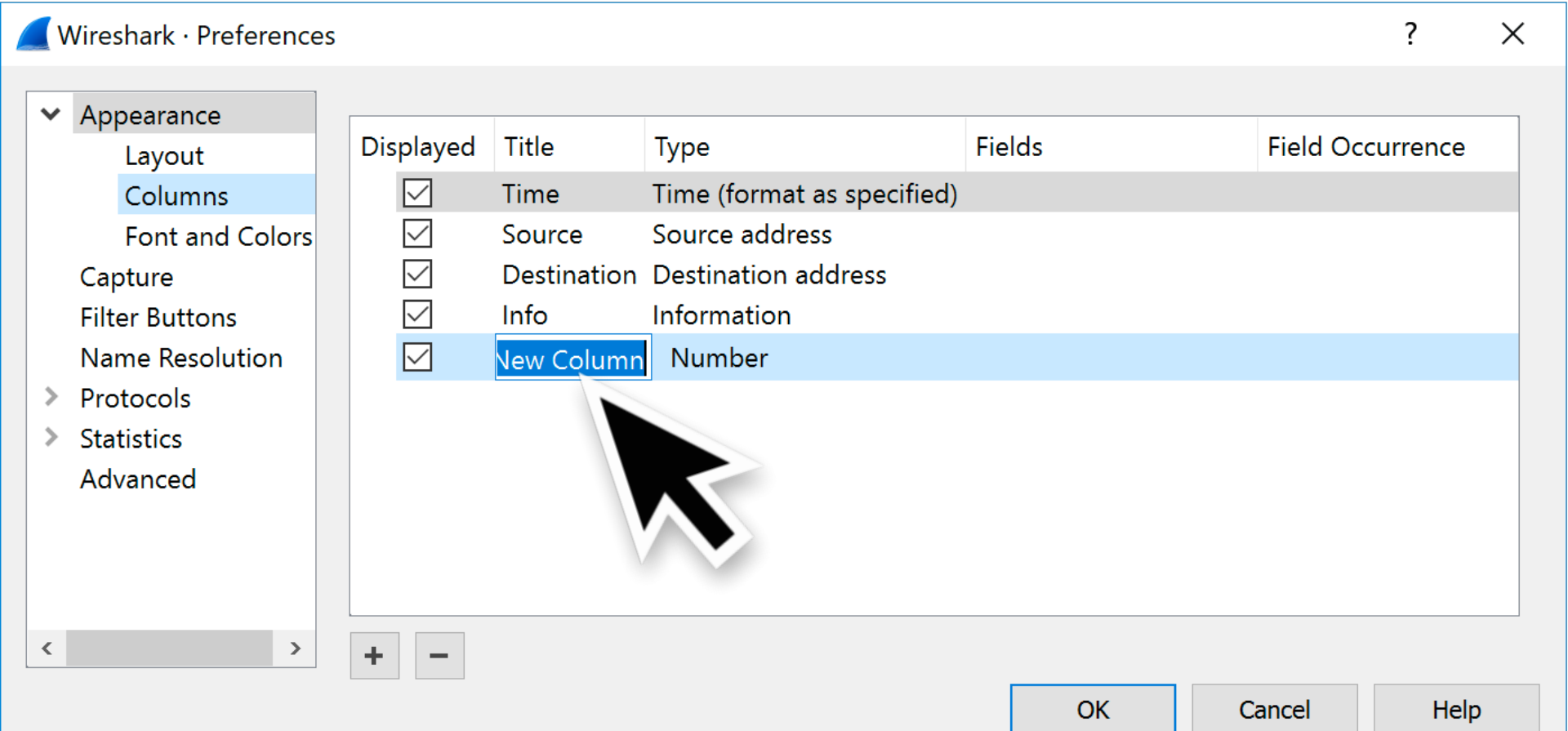
This takes you directly to the column settings



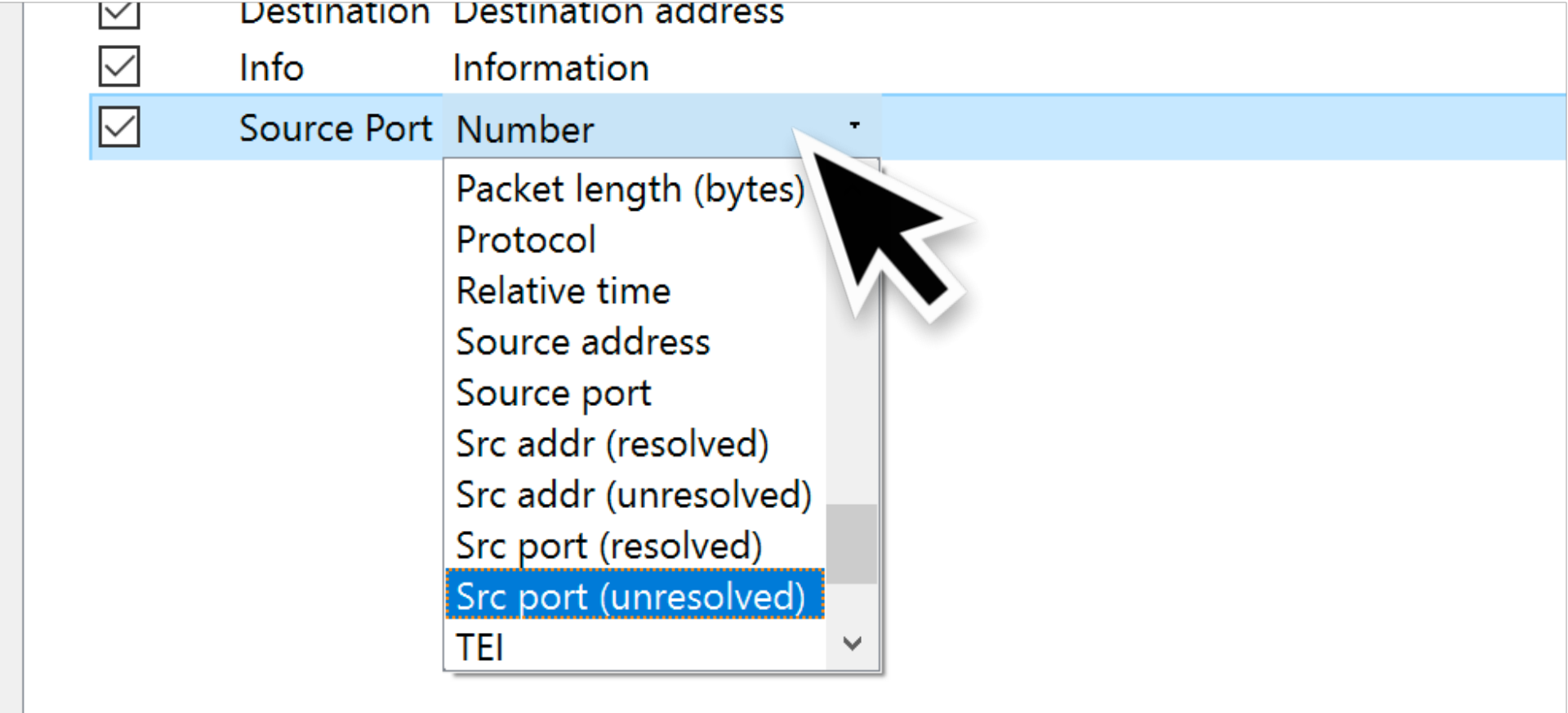
Adding columns



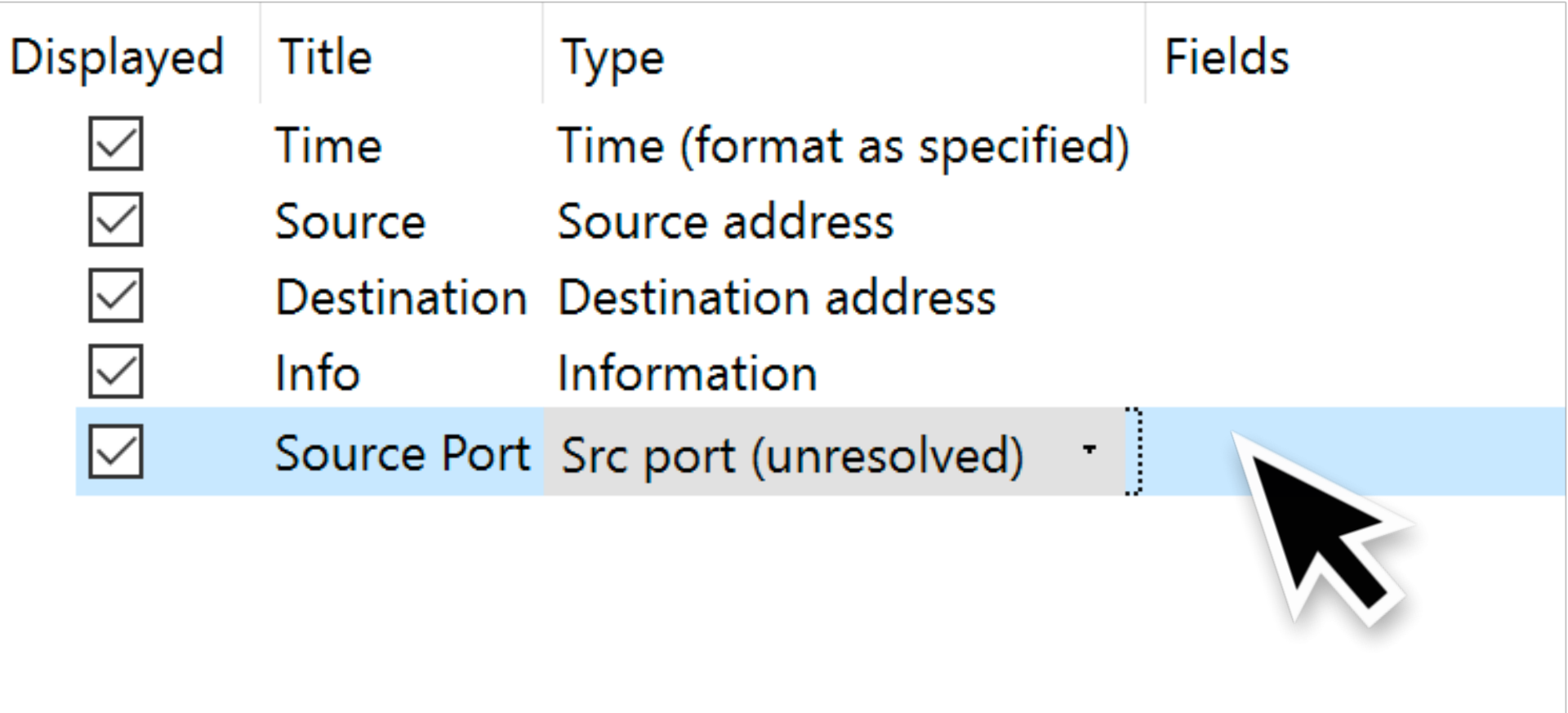
Adding columns



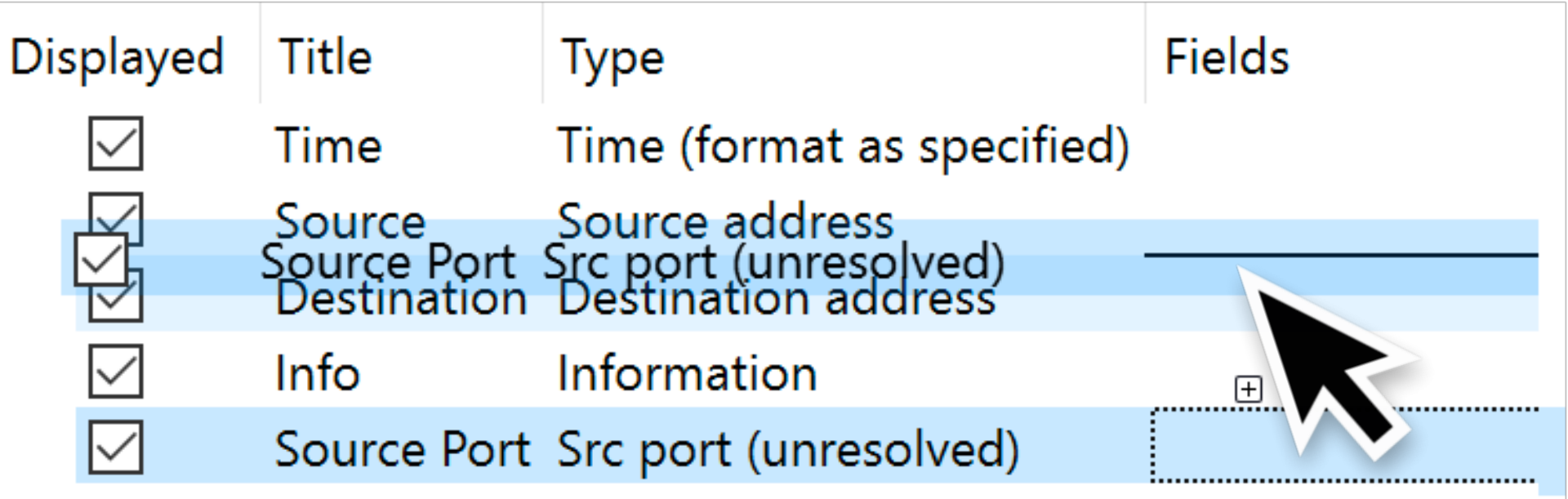
Adding columns



Adding columns



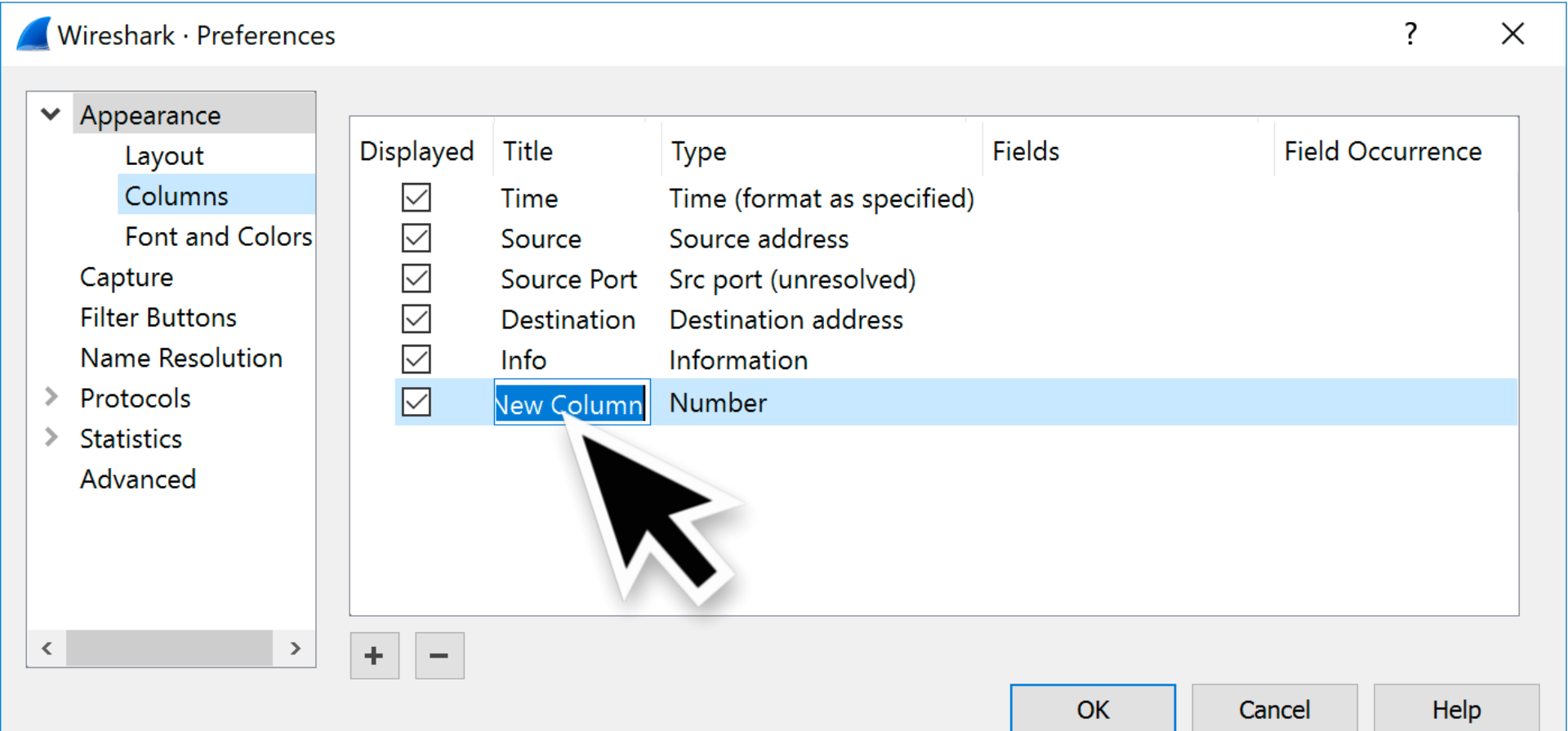
Adding columns



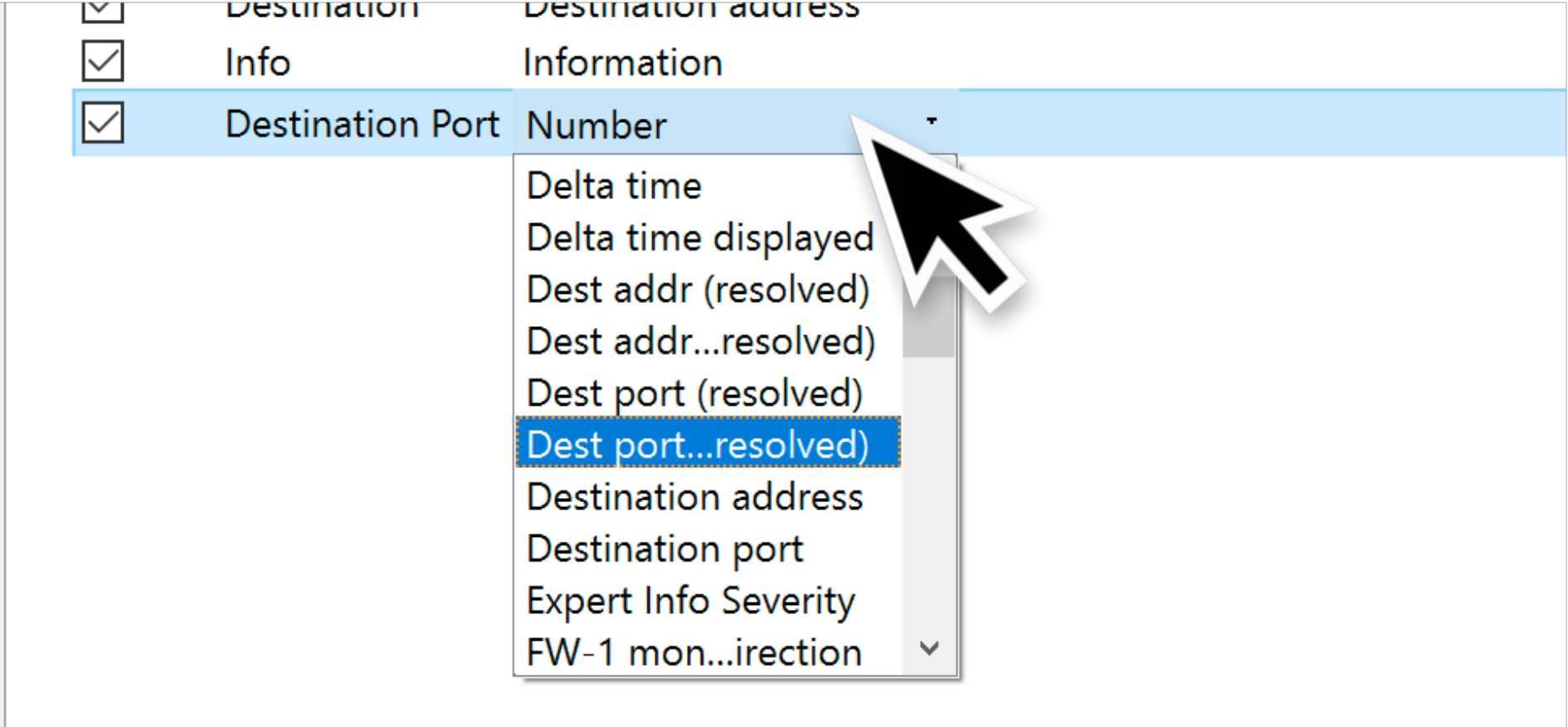
Adding columns

Displayed	Title	Type	Fields
☑	Time	Time (format as specified)	
☑	Source	Source address	
☑	Source Port	Src port (unresolved)	
☑	Destination	Destination address	
☑	Info	Information	

Adding columns



Adding columns



Adding columns

Displayed	Title	Type	Fields
☑	Time	Time (format as specified)	
☑	Source	Source address	
☑	Source Port	Src port (unresolved)	
☑	Destination	Destination address	
☑	Destination Port	Dest port (unresolved)	
☑	Info	Information	
☑	Destination Port	Dest port (unresolved)	

Adding columns

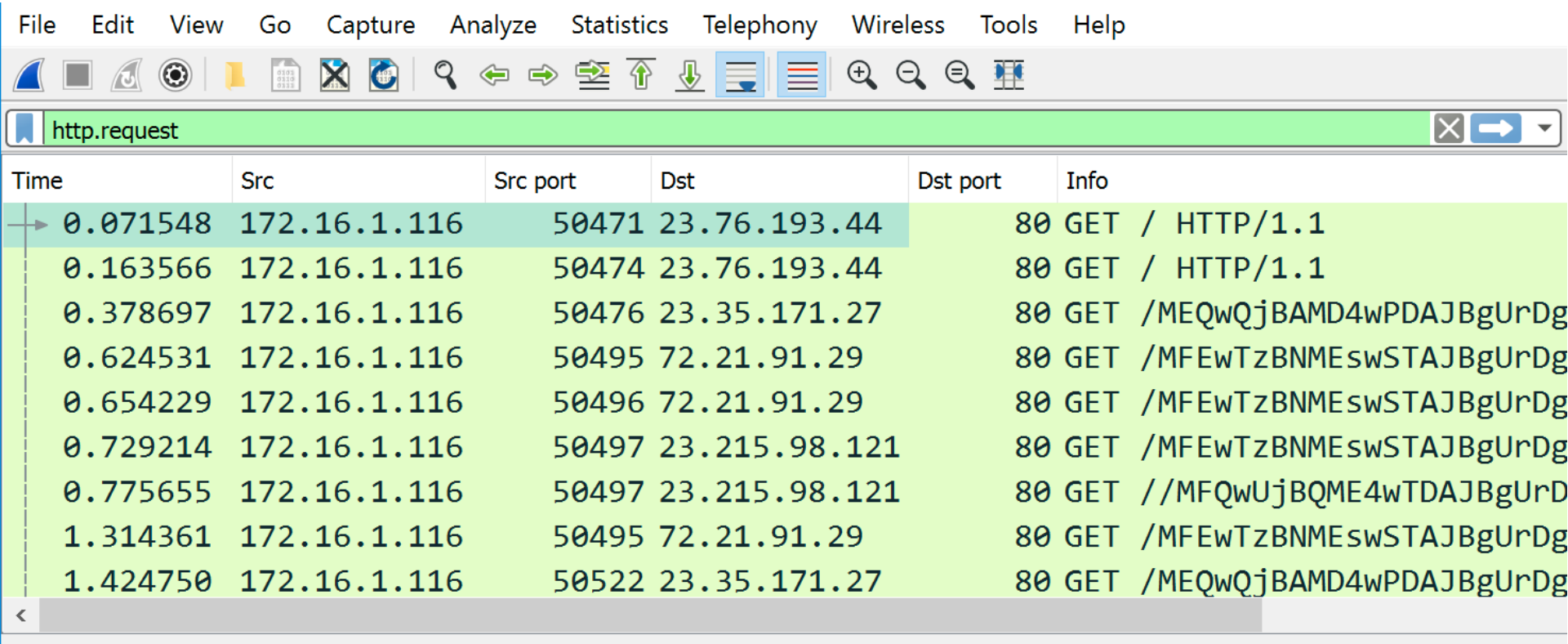
Displayed	Title	Type	Fields
☑	Time	Time (format as specified)	
☑	Source	Source address	
☑	Source Port	Src port (unresolved)	
☑	Destination	Destination address	
☑	Destination Port	Dest port (unresolved)	
☑	Info	Information	

Adding columns

Displayed	Title	Type	Fields
☑	Time	Time (format as specified)	
☑	Src	Src addr (unresolved)	
☑	Src port	Src port (unresolved)	
☑	Dst	Dest addr (unresolved)	
☑	Dst port	Dest port (unresolved)	
☑	Info	Information	

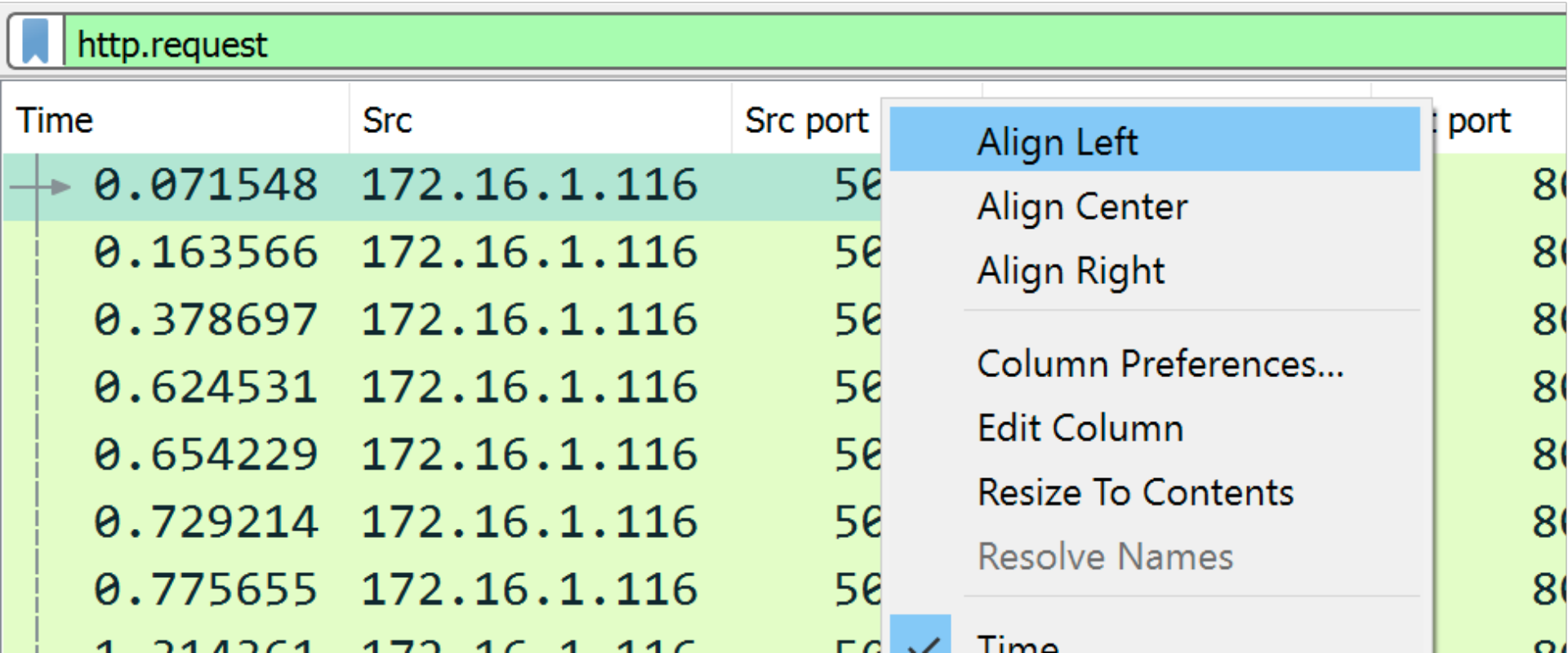
Adding columns

Src and Dst port columns are aligned to the right



Adding columns

Right-click in the column and "Align Left"



Adding columns

- Time
- Src IP
- Src port
- Dst IP
- Dst port
- Info

http.request

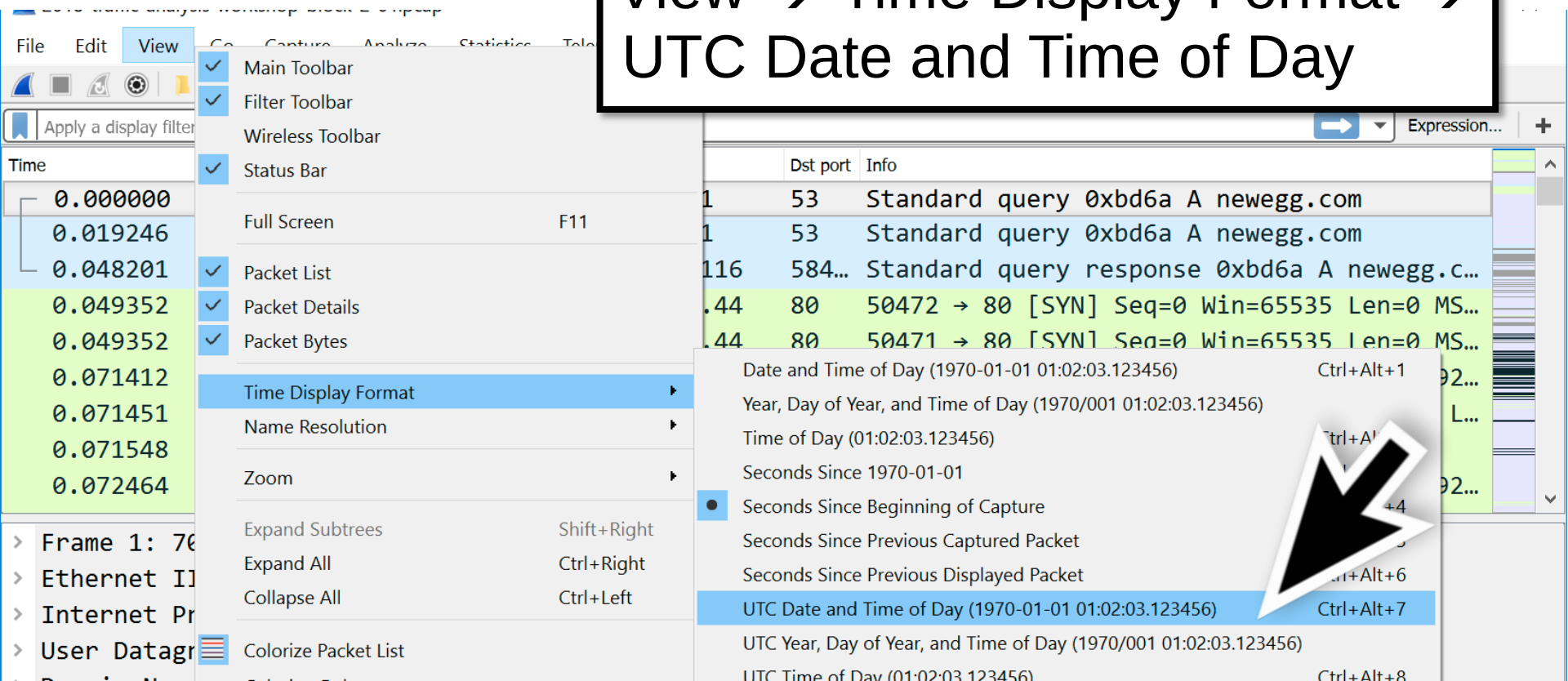
Time	Src	Src port	Dst	Dst port	Info
0.071548	172.16.1.116	50471	23.76.193.44	80	GET /
0.163566	172.16.1.116	50474	23.76.193.44	80	GET /
0.378697	172.16.1.116	50476	23.35.171.27	80	GET /
0.624531	172.16.1.116	50495	72.21.91.29	80	GET /
0.654229	172.16.1.116	50496	72.21.91.29	80	GET /
0.729214	172.16.1.116	50497	23.215.98.121	80	GET /
0.775655	172.16.1.116	50497	23.215.98.121	80	GET /
1.314361	172.16.1.116	50495	72.21.91.29	80	GET /

Up next...

- Web traffic & default Wireshark display
- Removing and adding columns
- **Changing time to UTC date and time**
- Adding custom columns
- Hiding columns

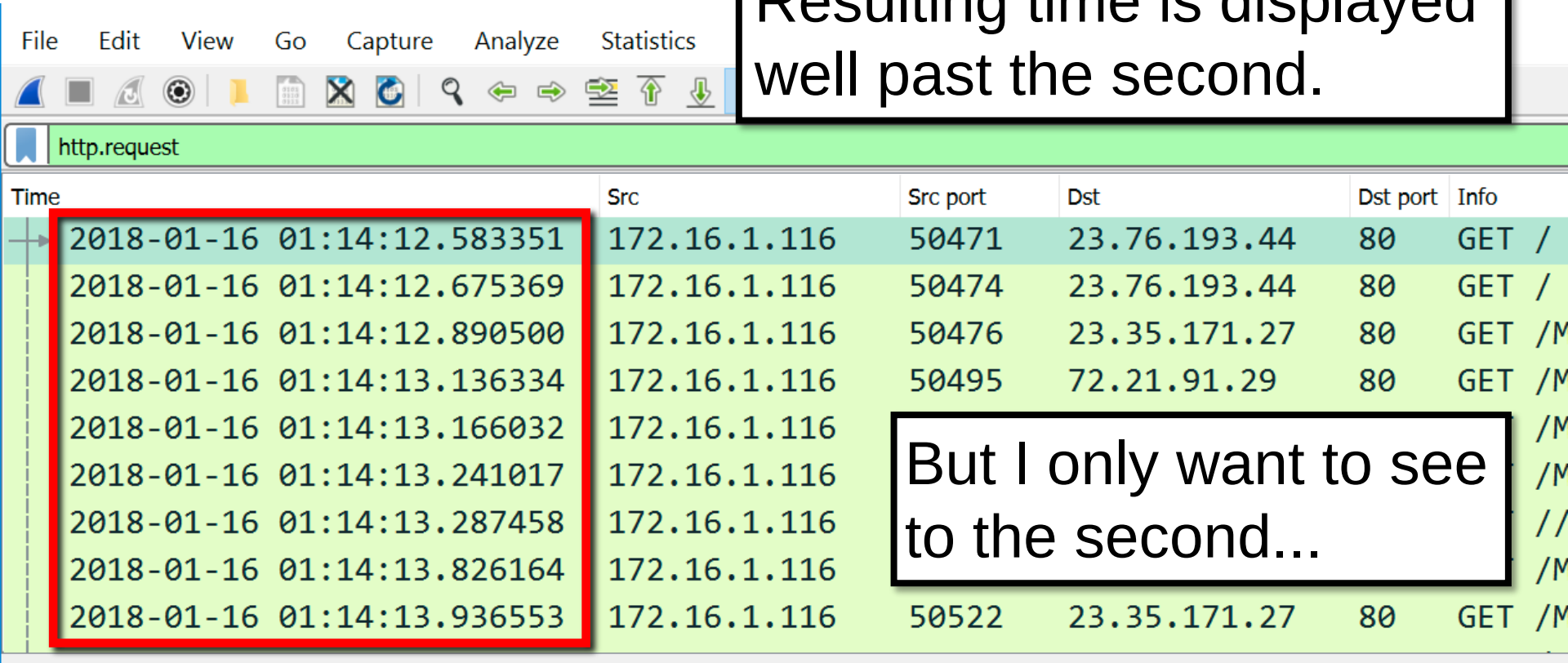
Changing time to UTC date and time

View → Time Display Format → UTC Date and Time of Day

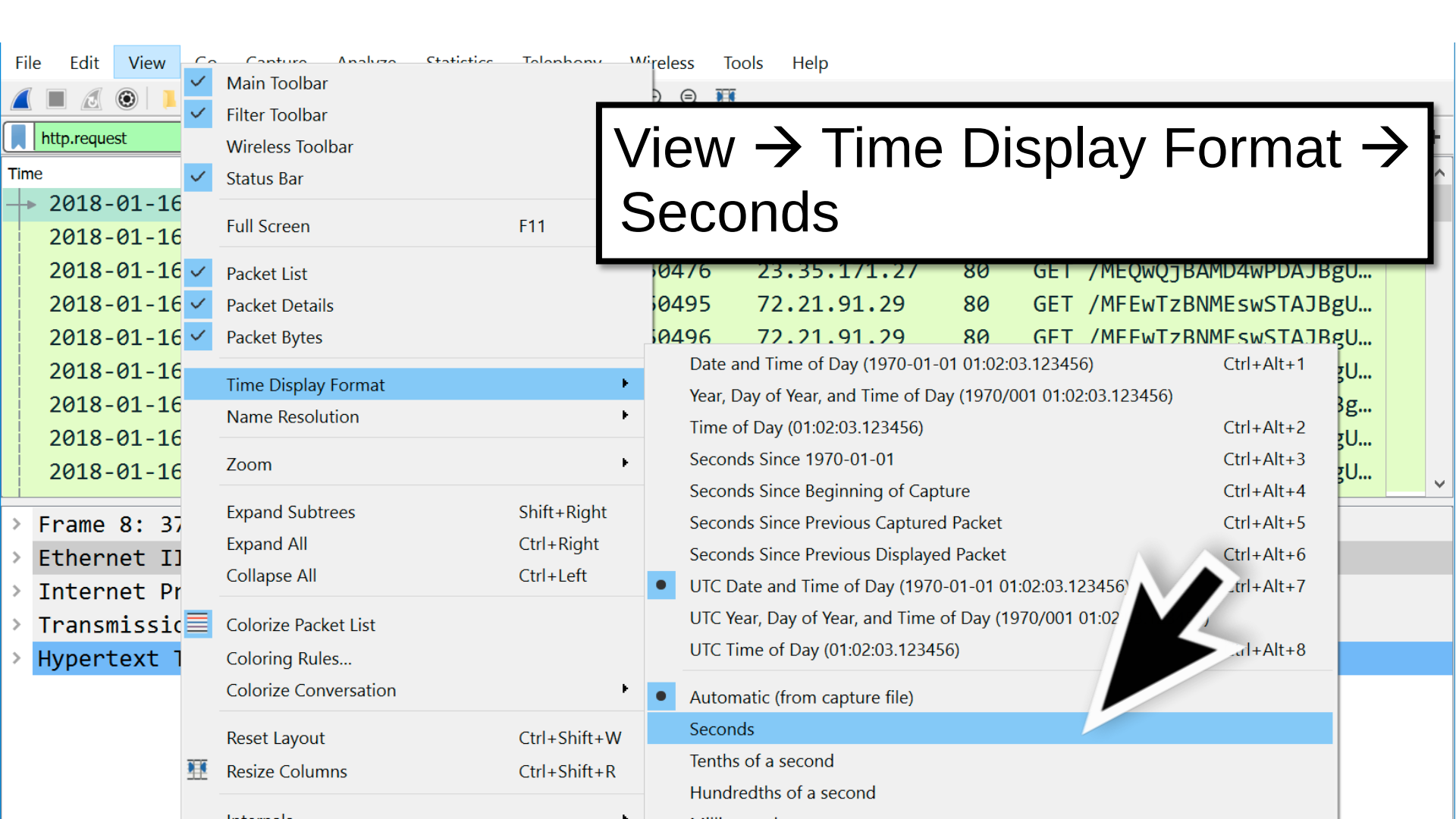


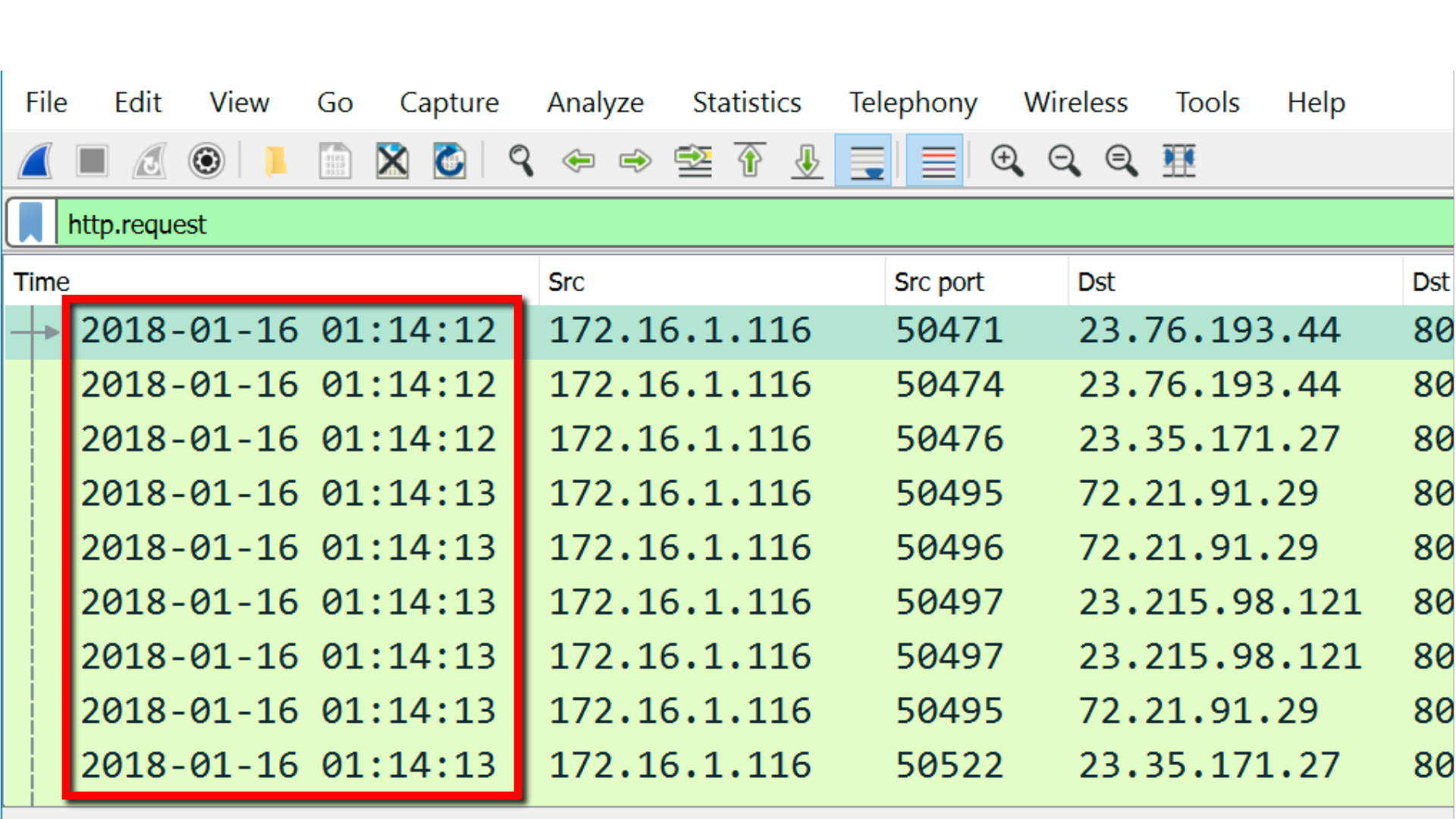
Changing time to UTC date and time

Resulting time is displayed well past the second.



But I only want to see to the second...


File
Edit
View
Tools
Help
Main Toolbar
Filter Toolbar
Wireless Toolbar
Status Bar
Full Screen F11
Packet List
Packet Details
Packet Bytes
Time Display Format
Name Resolution
Zoom
Expand Subtrees Shift+Right
Expand All Ctrl+Right
Collapse All Ctrl+Left
Colorize Packet List
Coloring Rules...
Colorize Conversation
Reset Layout Ctrl+Shift+W
Resize Columns Ctrl+Shift+R
Date and Time of Day (1970-01-01 01:02:03.123456) Ctrl+Alt+1
Year, Day of Year, and Time of Day (1970/001 01:02:03.123456)
Time of Day (01:02:03.123456) Ctrl+Alt+2
Seconds Since 1970-01-01 Ctrl+Alt+3
Seconds Since Beginning of Capture Ctrl+Alt+4
Seconds Since Previous Captured Packet Ctrl+Alt+5
Seconds Since Previous Displayed Packet Ctrl+Alt+6
UTC Date and Time of Day (1970-01-01 01:02:03.123456) Ctrl+Alt+7
UTC Year, Day of Year, and Time of Day (1970/001 01:02
UTC Time of Day (01:02:03.123456) Ctrl+Alt+8
Automatic (from capture file)
Seconds
Tenths of a second
Hundredths of a second
View → Time Display Format → Seconds


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.request
Time Src Src port Dst Dst
2018-01-16 01:14:12 172.16.1.116 50471 23.76.193.44 80
2018-01-16 01:14:12 172.16.1.116 50474 23.76.193.44 80
2018-01-16 01:14:12 172.16.1.116 50476 23.35.171.27 80
2018-01-16 01:14:13 172.16.1.116 50495 72.21.91.29 80
2018-01-16 01:14:13 172.16.1.116 50496 72.21.91.29 80
2018-01-16 01:14:13 172.16.1.116 50497 23.215.98.121 80
2018-01-16 01:14:13 172.16.1.116 50497 23.215.98.121 80
2018-01-16 01:14:13 172.16.1.116 50495 72.21.91.29 80
2018-01-16 01:14:13 172.16.1.116 50522 23.35.171.27 80

Up next...

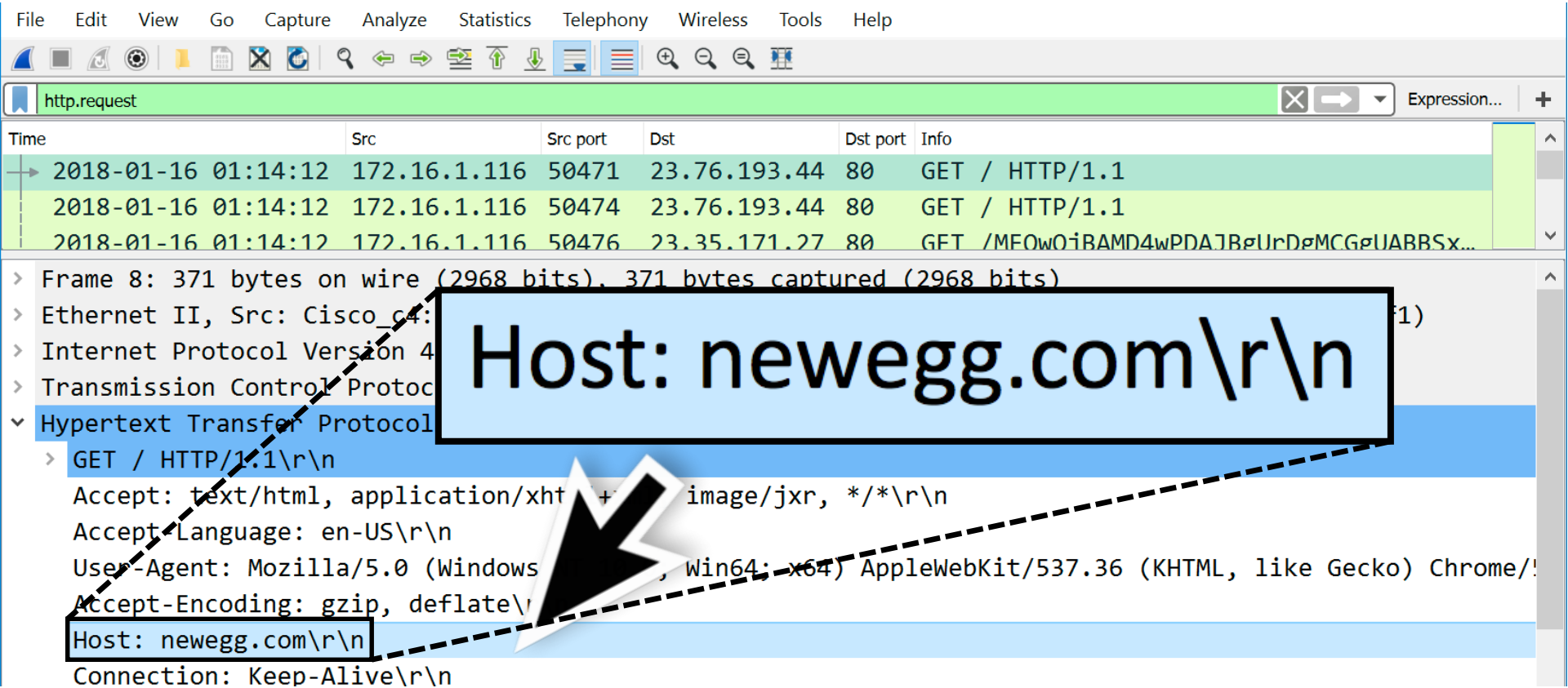
- Web traffic & default Wireshark display
- Removing and adding columns
- Changing time to UTC date and time
- **Adding custom columns**
- Hiding columns

Adding custom columns

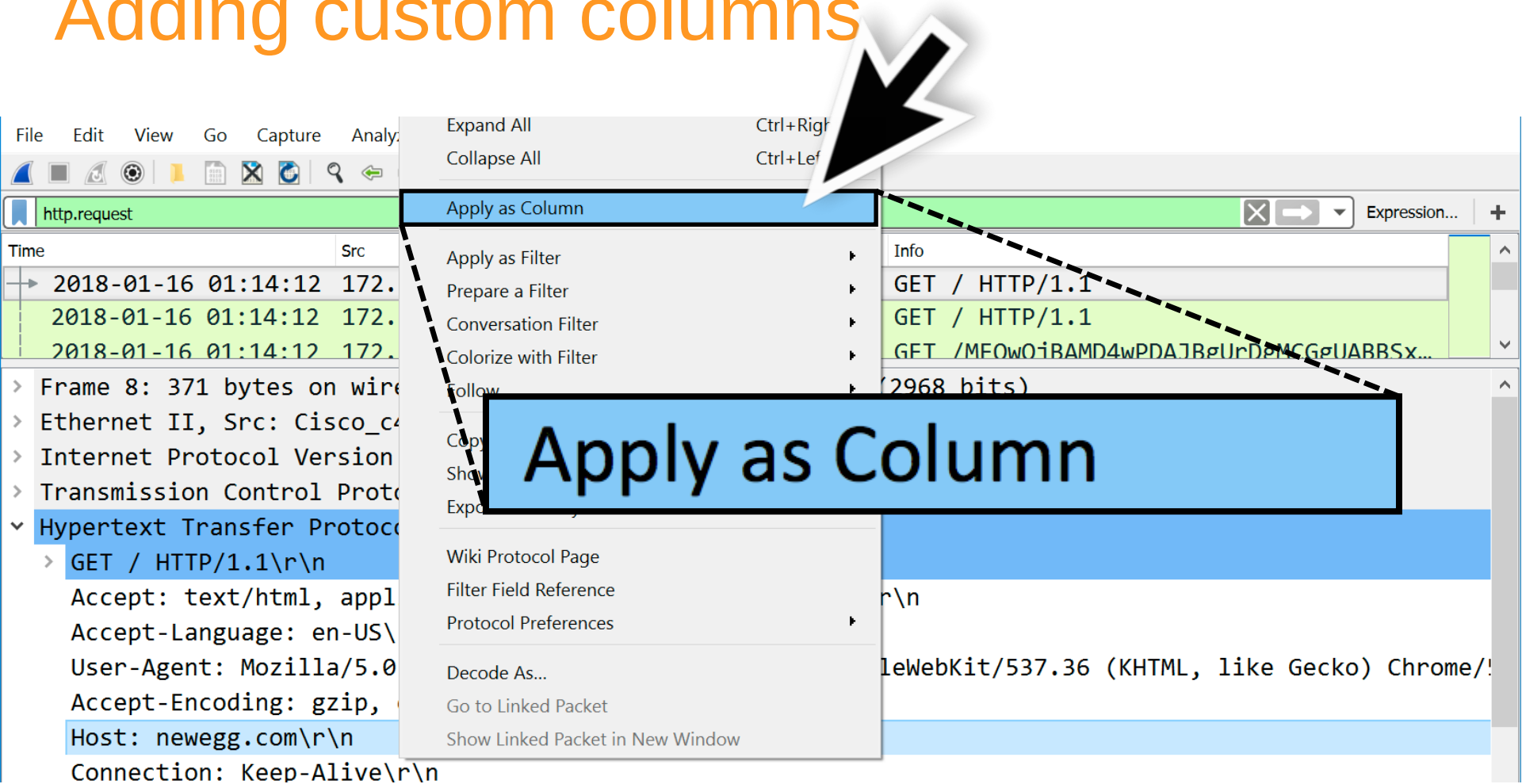
What else do we want in our column display?

- HTTP host names
- HTTPS server names

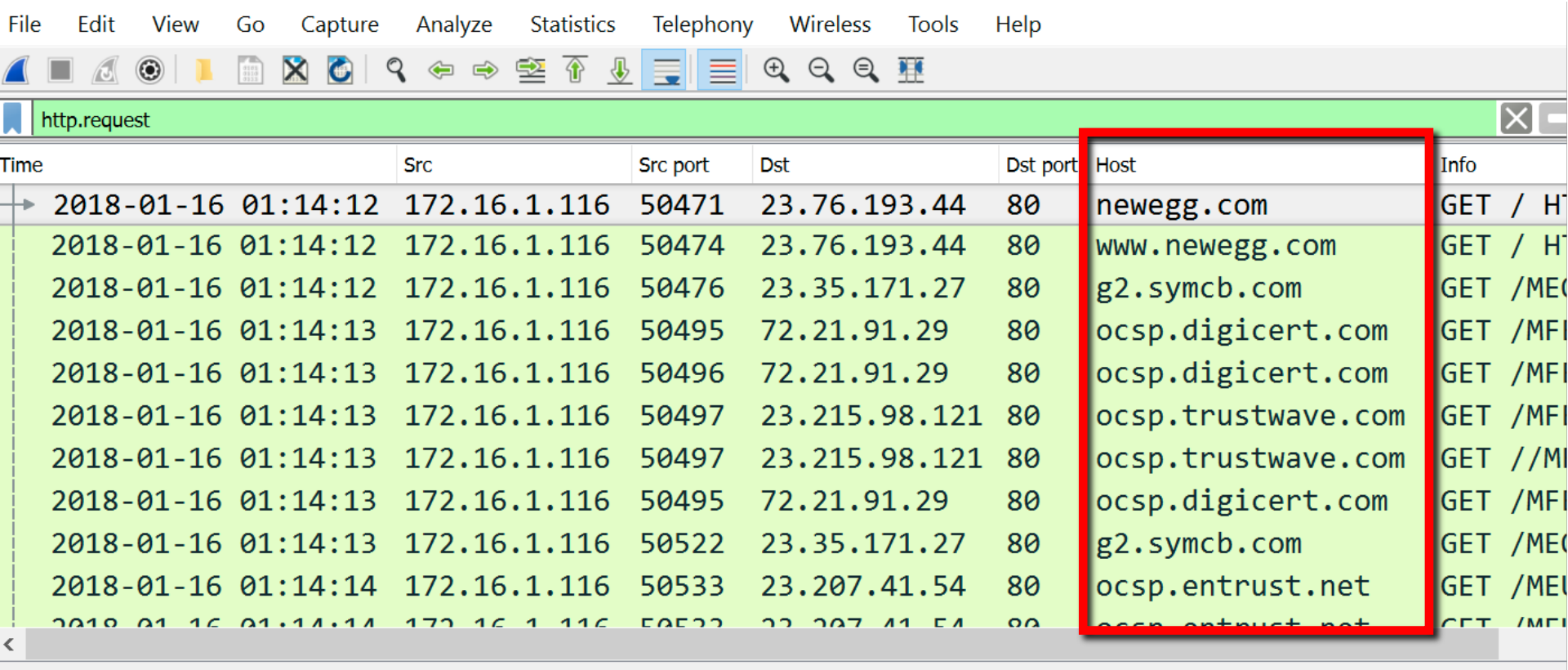
Adding custom columns



Adding custom columns



Adding custom columns

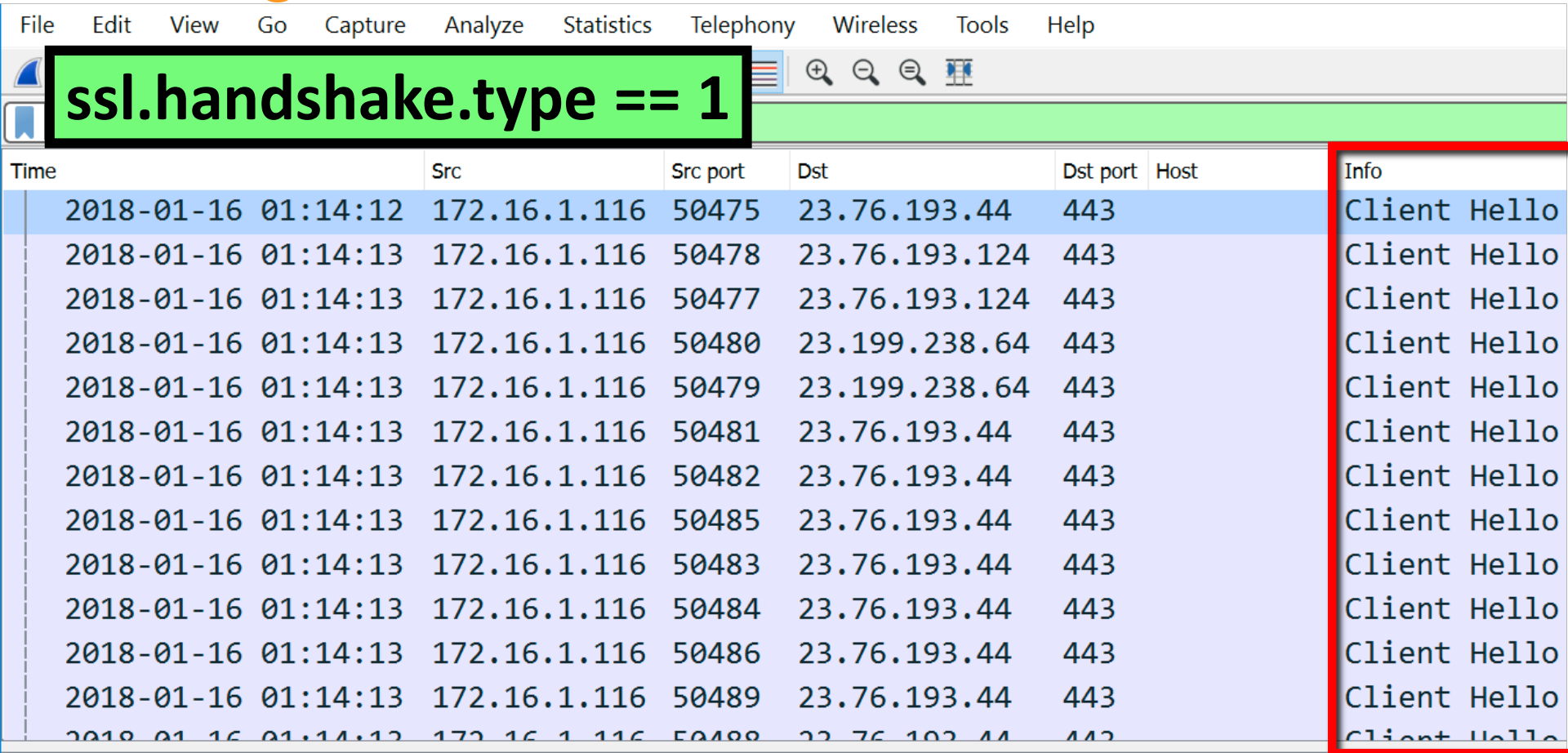


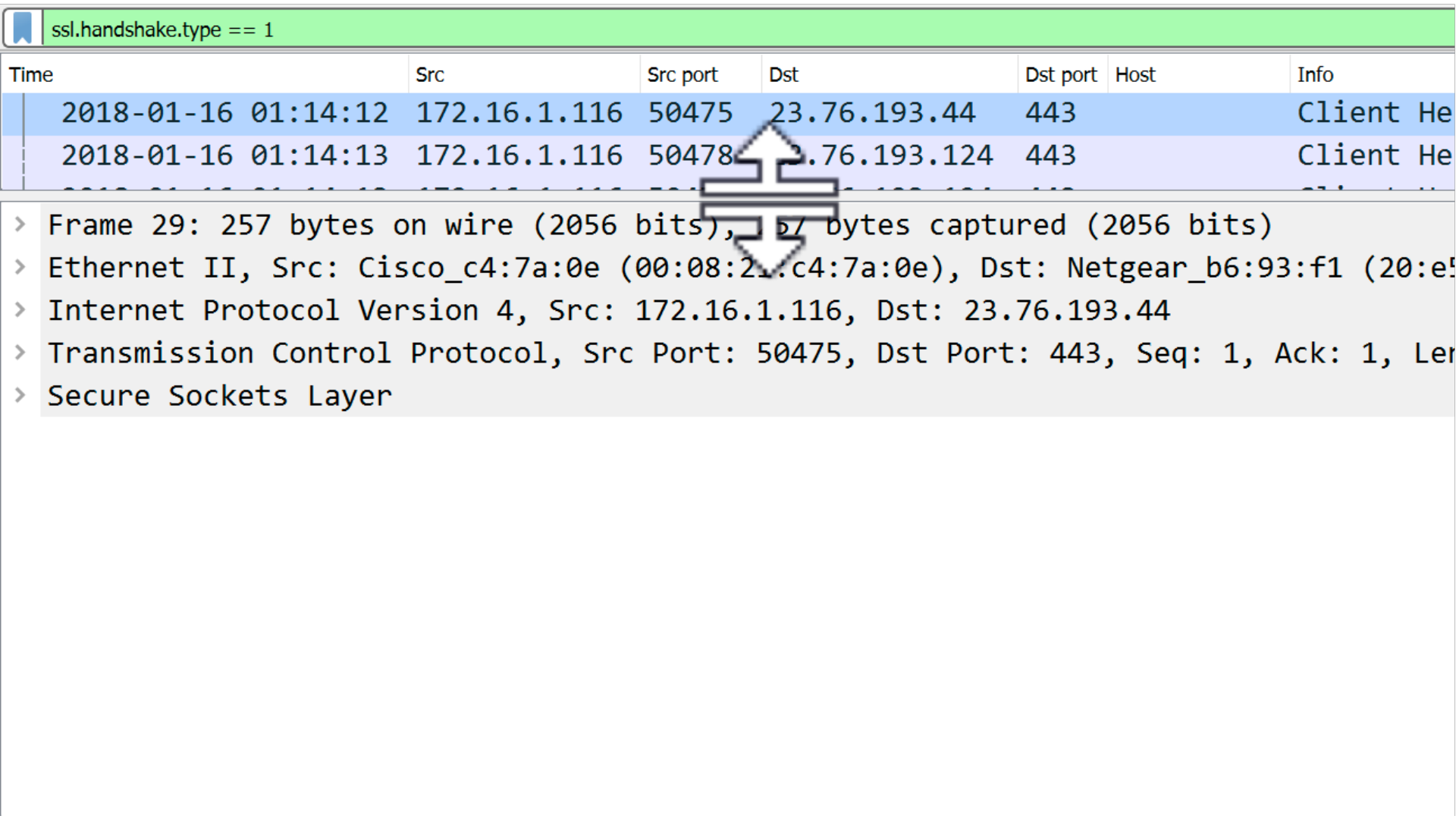
Adding custom columns

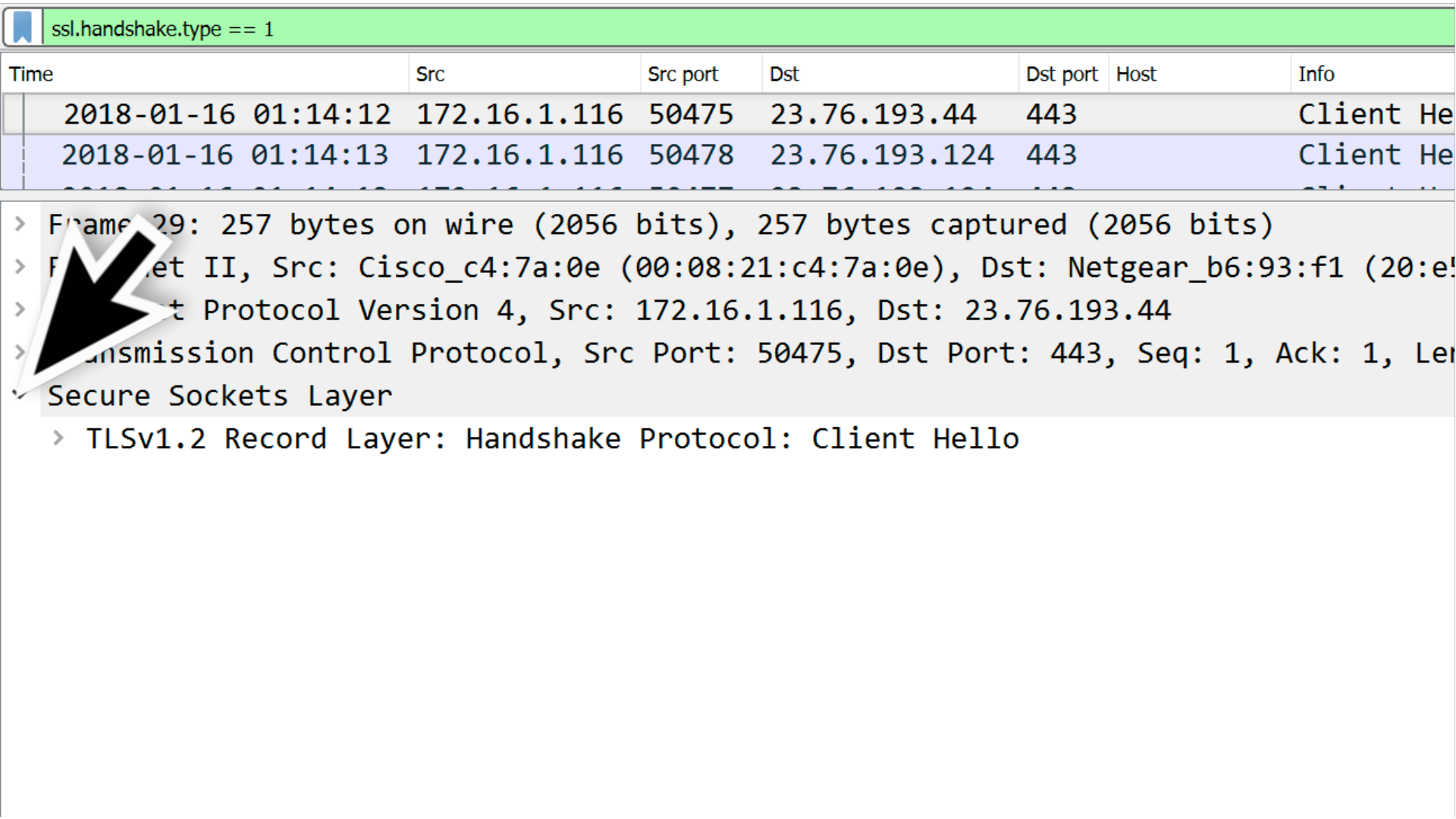
What else do we want in our column display?

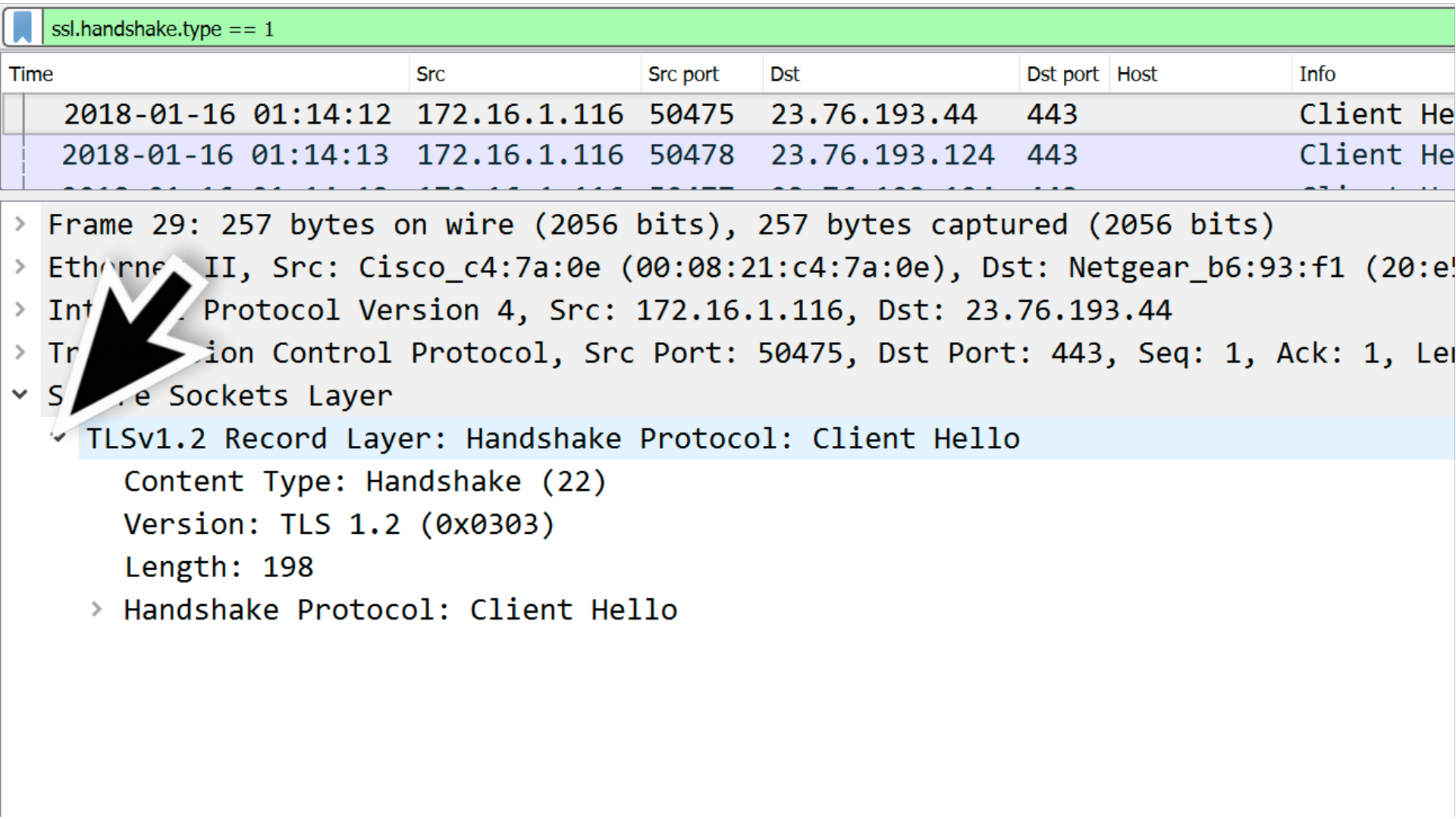
- HTTP host names 
- **HTTPS server names**

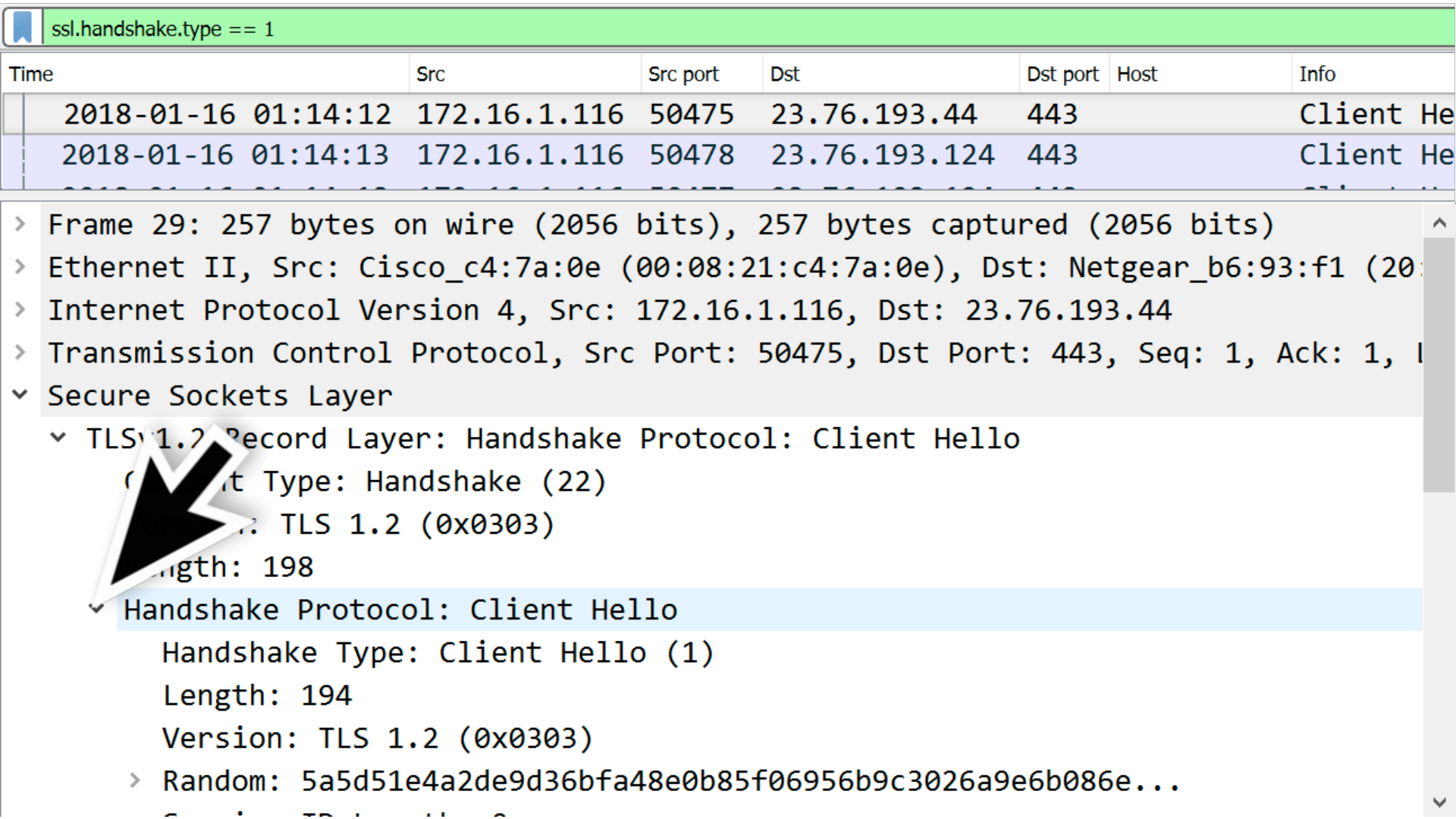
Adding custom columns




ssl.handshake.type == 1
Time
Src
Src port
Dst
Dst port
Host
Info
2018-01-16 01:14:12 172.16.1.116 50475 23.76.193.44 443 Client He
2018-01-16 01:14:13 172.16.1.116 50478 .76.193.124 443 Client He
Frame 29: 257 bytes on wire (2056 bits), 257 bytes captured (2056 bits)
Ethernet II, Src: Cisco_c4:7a:0e (00:08:2 c4:7a:0e), Dst: Netgear_b6:93:f1 (20:e
Internet Protocol Version 4, Src: 172.16.1.116, Dst: 23.76.193.44
Transmission Control Protocol, Src Port: 50475, Dst Port: 443, Seq: 1, Ack: 1, Le
Secure Sockets Layer


ssl.handshake.type == 1
Time
Src
Src port
Dst
Dst port
Host
Info
2018-01-16 01:14:12 172.16.1.116 50475 23.76.193.44 443 Client He
2018-01-16 01:14:13 172.16.1.116 50478 23.76.193.124 443 Client He
Frame 29: 257 bytes on wire (2056 bits), 257 bytes captured (2056 bits)
Ethernet II, Src: Cisco_c4:7a:0e (00:08:21:c4:7a:0e), Dst: Netgear_b6:93:f1 (20:e5
Internet Protocol Version 4, Src: 172.16.1.116, Dst: 23.76.193.44
Transmission Control Protocol, Src Port: 50475, Dst Port: 443, Seq: 1, Ack: 1, Len
Secure Sockets Layer
TLSv1.2 Record Layer: Handshake Protocol: Client Hello

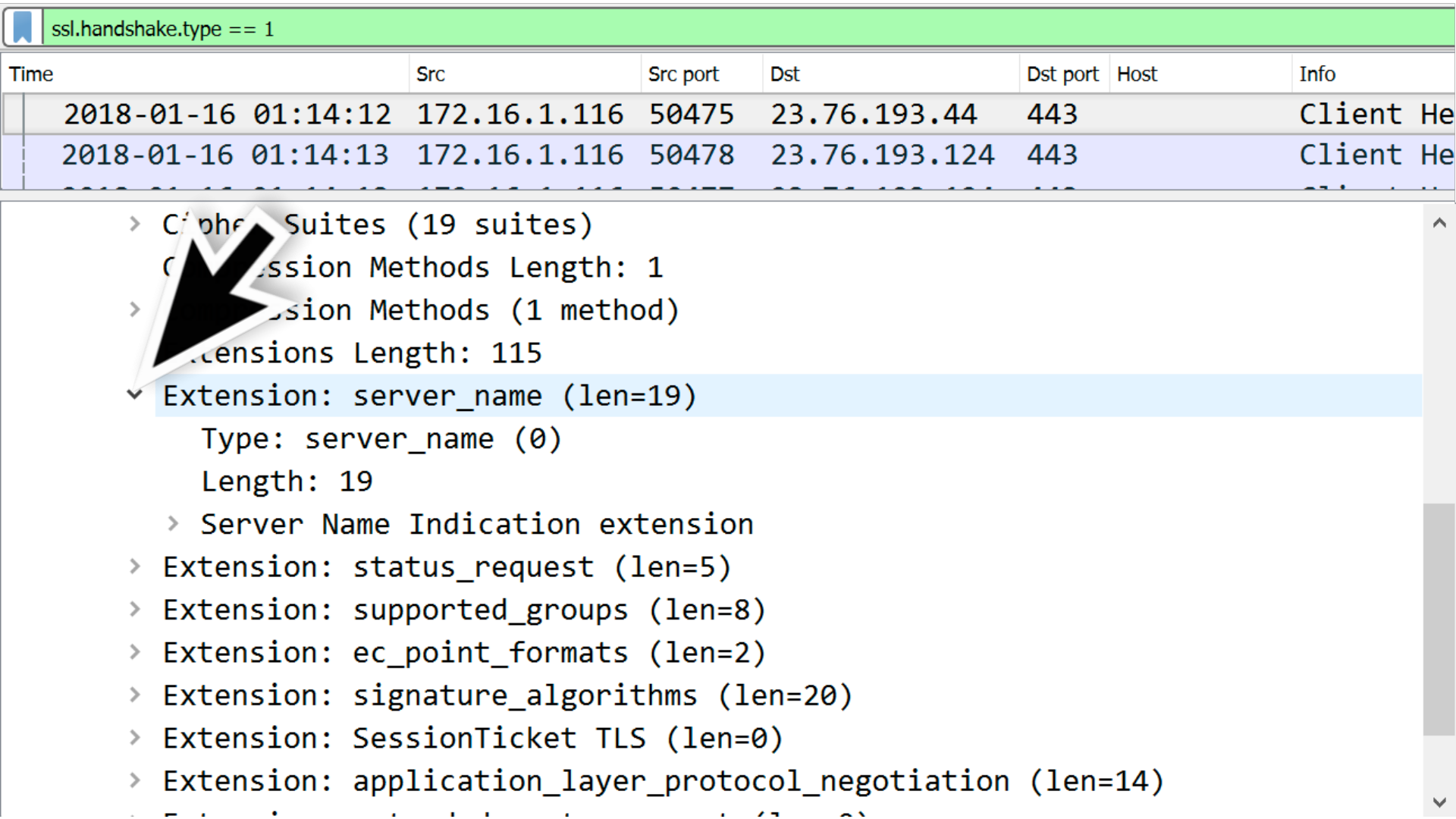

ssl.handshake.type == 1
Time
Src
Src port
Dst
Dst port
Host
Info
2018-01-16 01:14:12 172.16.1.116 50475 23.76.193.44 443 Client He
2018-01-16 01:14:13 172.16.1.116 50478 23.76.193.124 443 Client He
Frame 29: 257 bytes on wire (2056 bits), 257 bytes captured (2056 bits)
Ethernet II, Src: Cisco_c4:7a:0e (00:08:21:c4:7a:0e), Dst: Netgear_b6:93:f1 (20:e
Internet Protocol Version 4, Src: 172.16.1.116, Dst: 23.76.193.44
Transmission Control Protocol, Src Port: 50475, Dst Port: 443, Seq: 1, Ack: 1, Le
Secure Sockets Layer
TLSv1.2 Record Layer: Handshake Protocol: Client Hello
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 198
Handshake Protocol: Client Hello

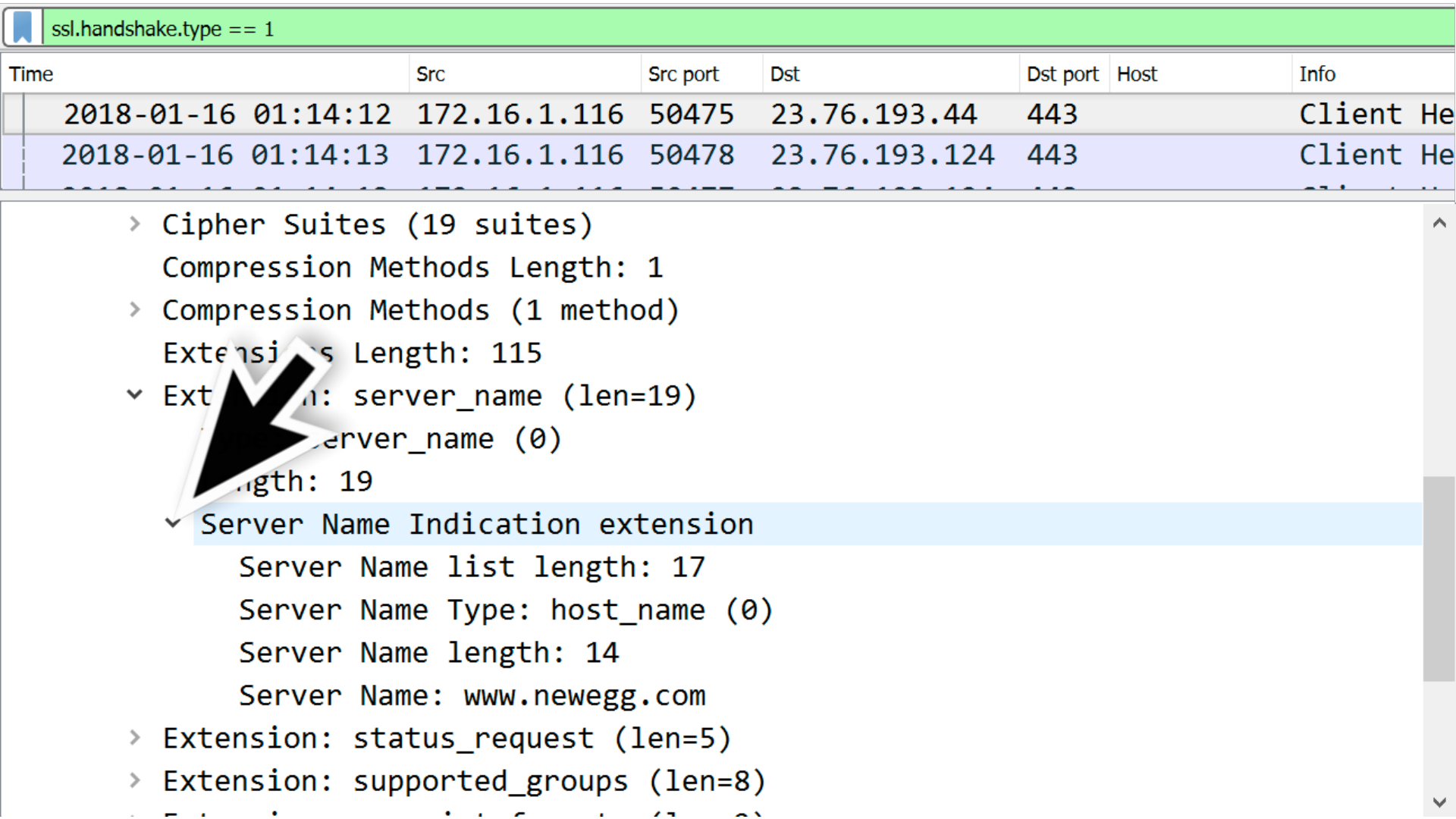

ssl.handshake.type == 1
Time
Src
Src port
Dst
Dst port
Host
Info
2018-01-16 01:14:12 172.16.1.116 50475 23.76.193.44 443 Client He
2018-01-16 01:14:13 172.16.1.116 50478 23.76.193.124 443 Client He
Frame 29: 257 bytes on wire (2056 bits), 257 bytes captured (2056 bits)
Ethernet II, Src: Cisco_c4:7a:0e (00:08:21:c4:7a:0e), Dst: Netgear_b6:93:f1 (20
Internet Protocol Version 4, Src: 172.16.1.116, Dst: 23.76.193.44
Transmission Control Protocol, Src Port: 50475, Dst Port: 443, Seq: 1, Ack: 1,
Secure Sockets Layer
TLS 1.2 Record Layer: Handshake Protocol: Client Hello
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 198
Handshake Protocol: Client Hello
Handshake Type: Client Hello (1)
Length: 194
Version: TLS 1.2 (0x0303)
Random: 5a5d51e4a2de9d36bfa48e0b85f06956b9c3026a9e6b086e...

ssl.handshake.type == 1

Time	Src	Src port	Dst	Dst port	Host	Info
2018-01-16 01:14:12	172.16.1.116	50475	23.76.193.44	443		Client He
2018-01-16 01:14:13	172.16.1.116	50478	23.76.193.124	443		Client He

```
> Cipher Suites (19 suites)
  Compression Methods Length: 1
> Compression Methods (1 method)
> Extension: server_name (len=19)
> Extension: supported_groups (len=8)
> Extension: ec_point_formats (len=2)
> Extension: signature_algorithms (len=20)
> Extension: SessionTicket TLS (len=0)
> Extension: application_layer_protocol_negotiation (len=14)
> Extension: extended_master_secret (len=0)
> Extension: token_binding (len=6)
> Extension: renegotiation_info (len=1)
```

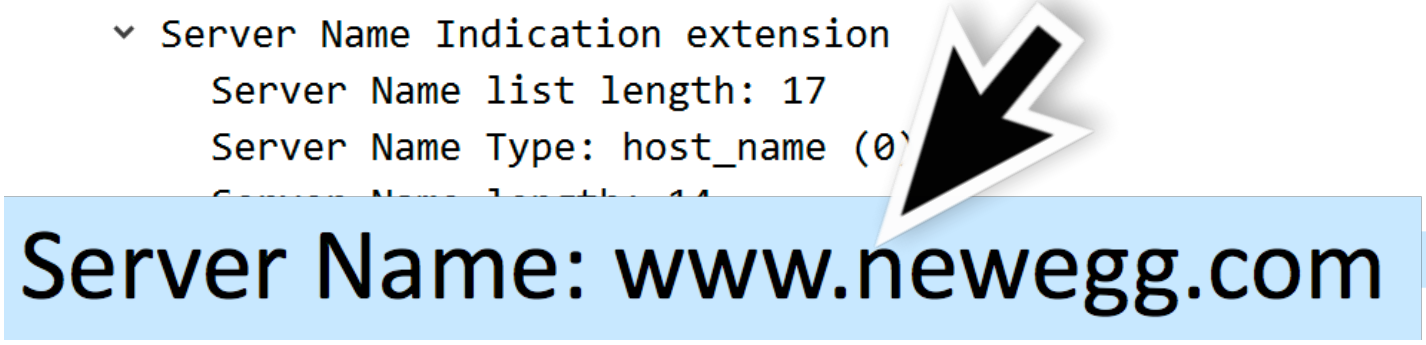

ssl.handshake.type == 1
Time
Src
Src port
Dst
Dst port
Host
Info
2018-01-16 01:14:12 172.16.1.116 50475 23.76.193.44 443 Client He
2018-01-16 01:14:13 172.16.1.116 50478 23.76.193.124 443 Client He
Suites (19 suites)
ssion Methods Length: 1
ssion Methods (1 method)
tensions Length: 115
Extension: server_name (len=19)
Type: server_name (0)
Length: 19
Server Name Indication extension
Extension: status_request (len=5)
Extension: supported_groups (len=8)
Extension: ec_point_formats (len=2)
Extension: signature_algorithms (len=20)
Extension: SessionTicket TLS (len=0)
Extension: application_layer_protocol_negotiation (len=14)

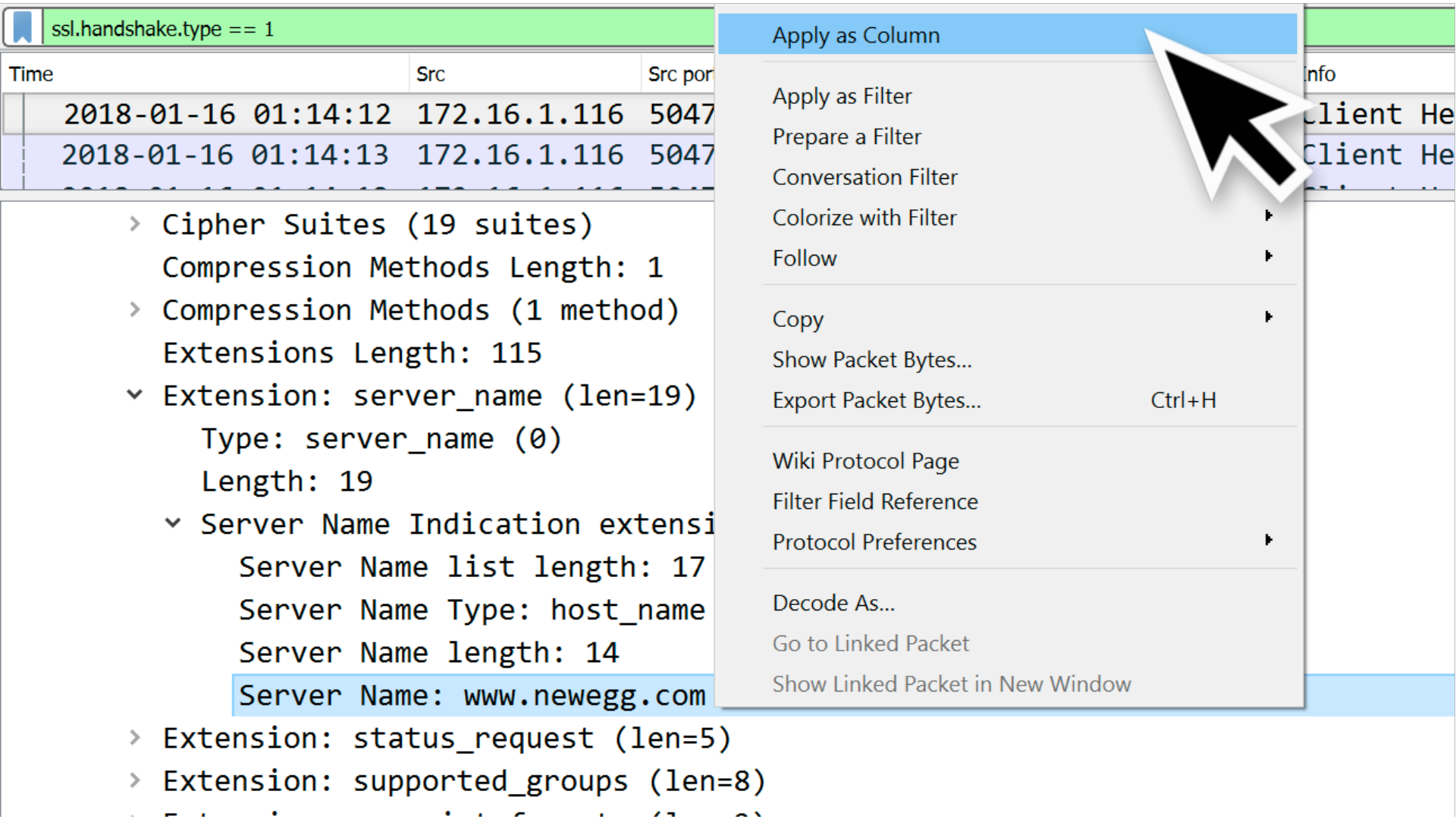

ssl.handshake.type == 1
Time
Src
Src port
Dst
Dst port
Host
Info
2018-01-16 01:14:12 172.16.1.116 50475 23.76.193.44 443 Client He
2018-01-16 01:14:13 172.16.1.116 50478 23.76.193.124 443 Client He
Cipher Suites (19 suites)
Compression Methods Length: 1
Compression Methods (1 method)
Length: 115
: server_name (len=19)
erver_name (0)
gth: 19
Server Name Indication extension
Server Name list length: 17
Server Name Type: host_name (0)
Server Name length: 14
Server Name: www.newegg.com
Extension: status_request (len=5)
Extension: supported_groups (len=8)

ssl.handshake.type == 1

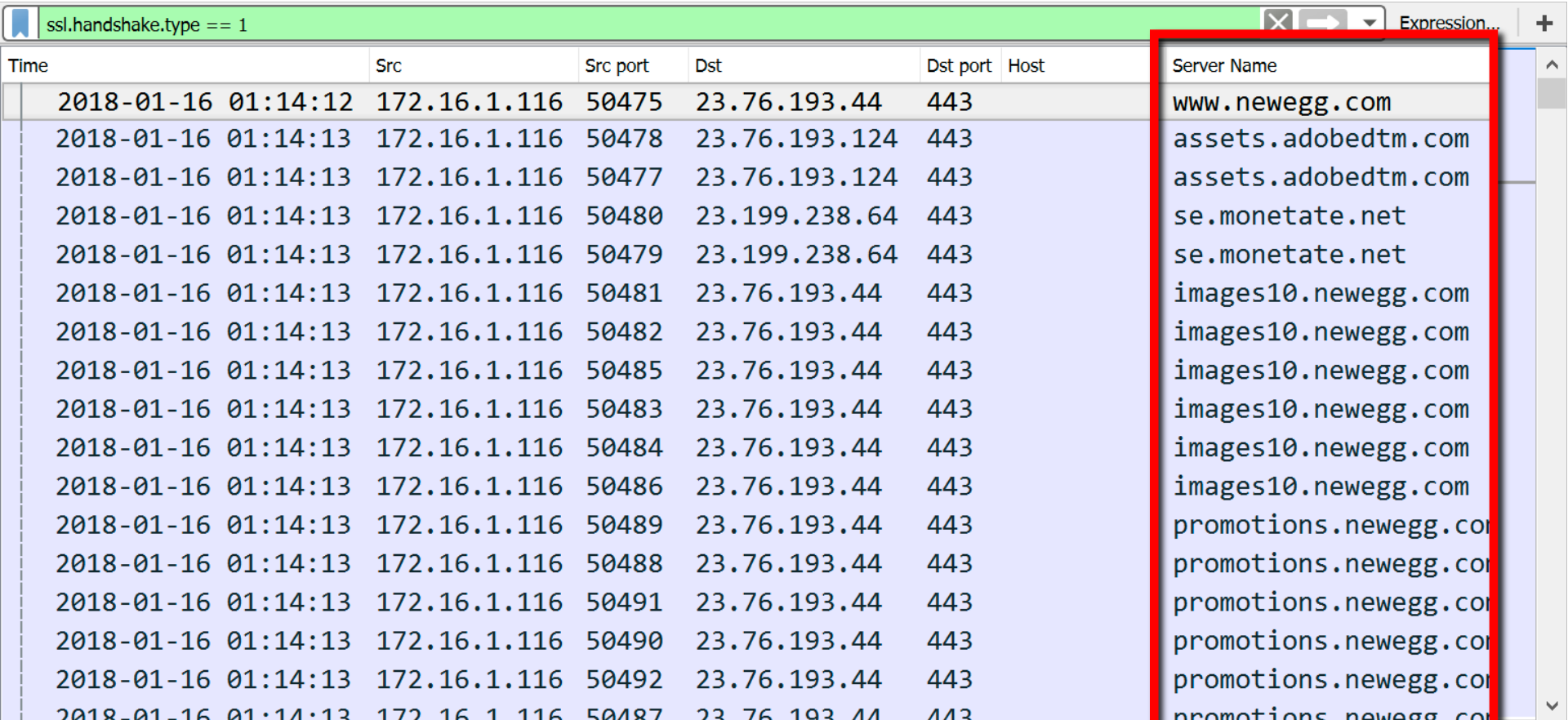
Time	Src	Src port	Dst	Dst port	Host	Info
2018-01-16 01:14:12	172.16.1.116	50475	23.76.193.44	443		Client He
2018-01-16 01:14:13	172.16.1.116	50478	23.76.193.124	443		Client He

```
    > Cipher Suites (19 suites)
      Compression Methods Length: 1
    > Compression Methods (1 method)
      Extensions Length: 115
    v Extension: server_name (len=19)
        Type: server_name (0)
        Length: 19
      v Server Name Indication extension
          Server Name list length: 17
          Server Name Type: host_name (0)
          Server Name length: 14
    > Extension: supported_groups (len=8)
```




ssl.handshake.type == 1
Time
Src
Src por
Info
2018-01-16 01:14:12 172.16.1.116 5047
2018-01-16 01:14:13 172.16.1.116 5047
Cipher Suites (19 suites)
Compression Methods Length: 1
Compression Methods (1 method)
Extensions Length: 115
Extension: server_name (len=19)
Type: server_name (0)
Length: 19
Server Name Indication extensi
Server Name list length: 17
Server Name Type: host_name
Server Name length: 14
Server Name: www.newegg.com
Extension: status_request (len=5)
Extension: supported_groups (len=8)
Apply as Column
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize with Filter
Follow
Copy
Show Packet Bytes...
Export Packet Bytes... Ctrl+H
Wiki Protocol Page
Filter Field Reference
Protocol Preferences
Decode As...
Go to Linked Packet
Show Linked Packet in New Window

Adding custom columns



Up next...

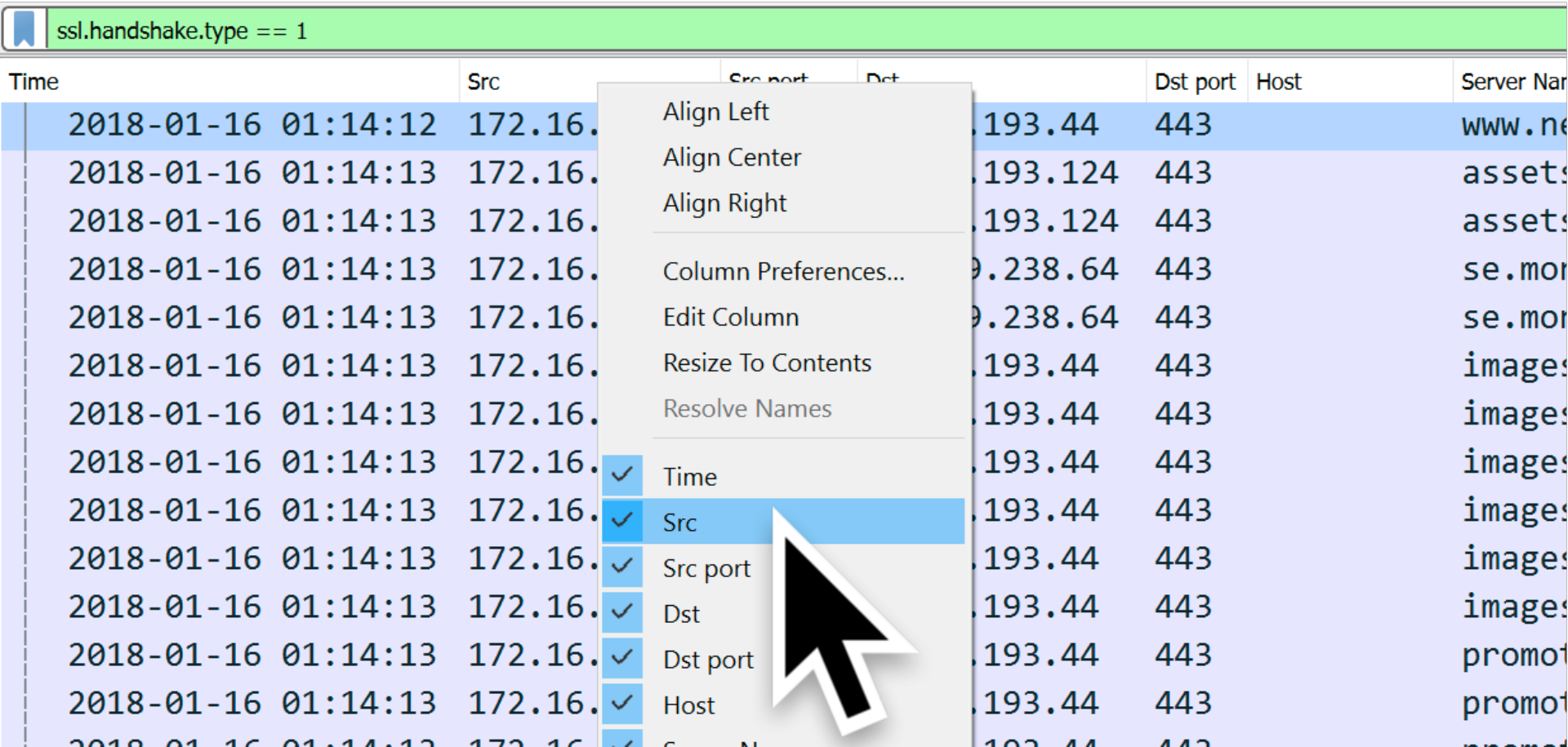
- Web traffic & default Wireshark display
- Removing and adding columns
- Changing time to UTC date and time
- Adding custom columns
- **Hiding columns**

Hiding columns

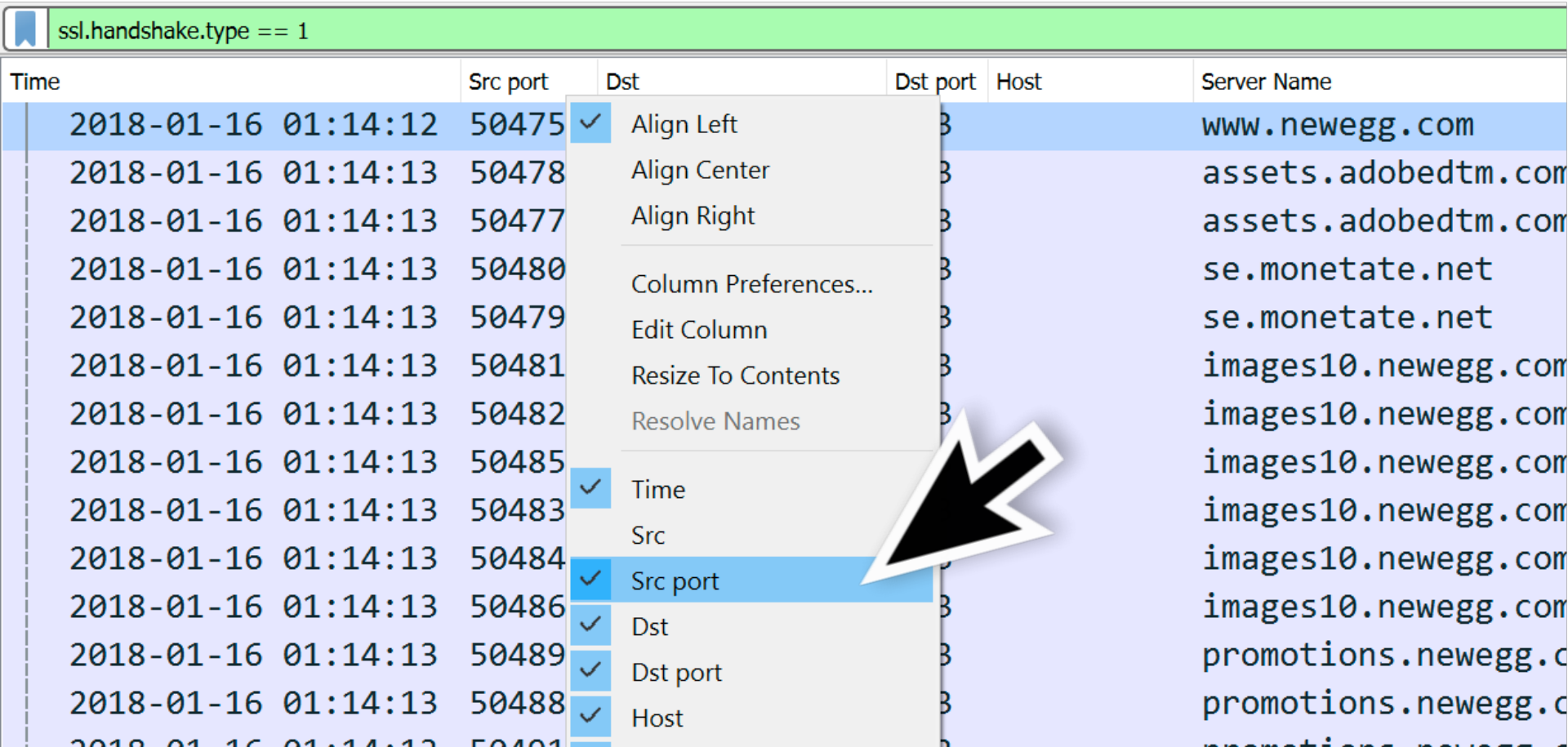
ssl.handshake.type == 1

Time	Src	Src port	Dst	Dst port	Host	Server Nar
2018-01-16 01:14:12	172.16.1 16	50475	23.76.193.44	443		www.ne
2018-01-16 01:14:13	172.16.1	50478	23.76.193.124	443		assets
2018-01-16 01:14:13	172.16.1	50477	23.76.193.124	443		assets
2018-01-16 01:14:13	172.16.1.11	50480	23.199.238.64	443		se.mor
2018-01-16 01:14:13	172.16.1.116	50479	23.199.238.64	443		se.mor
2018-01-16 01:14:13	172.16.1.116	50481	23.76.193.44	443		images
2018-01-16 01:14:13	172.16.1.116	50482	23.76.193.44	443		images
2018-01-16 01:14:13	172.16.1.116	50485	23.76.193.44	443		images
2018-01-16 01:14:13	172.16.1.116	50483	23.76.193.44	443		images
2018-01-16 01:14:13	172.16.1.116	50484	23.76.193.44	443		images
2018-01-16 01:14:13	172.16.1.116	50486	23.76.193.44	443		images
2018-01-16 01:14:13	172.16.1.116	50489	23.76.193.44	443		promot
2018-01-16 01:14:13	172.16.1.116	50488	23.76.193.44	443		promot

Hiding columns



Hiding columns



Hiding columns

- Time
- Dst IP
- Dst port
- Host
- Server Name
- Info

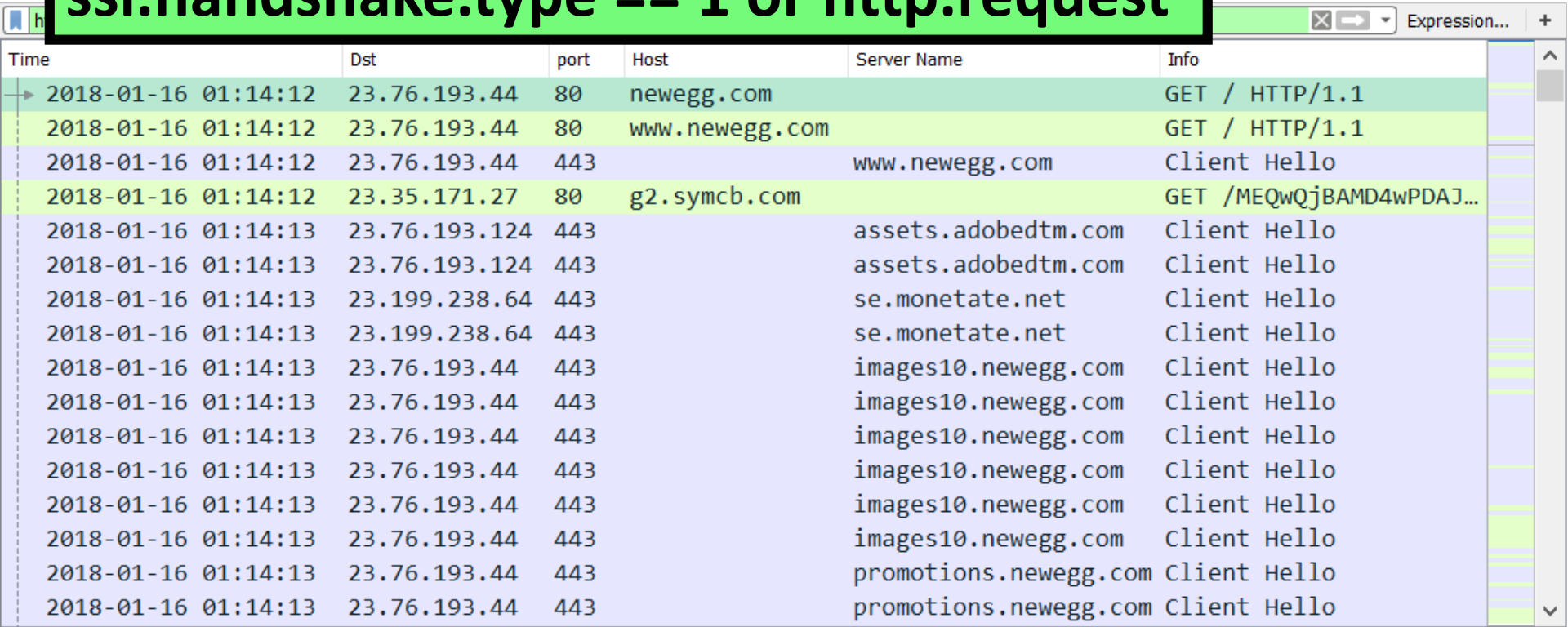
ssl.handshake.type == 1 Expression... +

Time	Dst	port	Host	Server Name	Info
2018-01-16 01:14:12	23.76.193.44	443		www.newegg.com	Client Hello
2018-01-16 01:14:13	23.76.193.124	443		assets.adobedtm.com	Client Hello
2018-01-16 01:14:13	23.76.193.124	443		assets.adobedtm.com	Client Hello
2018-01-16 01:14:13	23.199.238.64	443		se.monetate.net	Client Hello
2018-01-16 01:14:13	23.199.238.64	443		se.monetate.net	Client Hello
2018-01-16 01:14:13	23.76.193.44	443		images10.newegg.com	Client Hello
2018-01-16 01:14:13	23.76.193.44	443		images10.newegg.com	Client Hello
2018-01-16 01:14:13	23.76.193.44	443		images10.newegg.com	Client Hello
2018-01-16 01:14:13	23.76.193.44	443		images10.newegg.com	Client Hello
2018-01-16 01:14:13	23.76.193.44	443		images10.newegg.com	Client Hello
2018-01-16 01:14:13	23.76.193.44	443		images10.newegg.com	Client Hello
2018-01-16 01:14:13	23.76.193.44	443		promotions.newegg.com	Client Hello
2018-01-16 01:14:13	23.76.193.44	443		promotions.newegg.com	Client Hello
2018-01-16 01:14:13	23.76.193.44	443		promotions.newegg.com	Client Hello
2018-01-16 01:14:13	23.76.193.44	443		promotions.newegg.com	Client Hello
2018-01-16 01:14:13	23.76.193.44	443		promotions.newegg.com	Client Hello

Hiding columns

Now we have a better idea of the web traffic in the pcap!

ssl.handshake.type == 1 or http.request



Expression...

Time	Dst	port	Host	Server Name	Info
2018-01-16 01:14:12	23.76.193.44	80	newegg.com		GET / HTTP/1.1
2018-01-16 01:14:12	23.76.193.44	80	www.newegg.com		GET / HTTP/1.1
2018-01-16 01:14:12	23.76.193.44	443		www.newegg.com	Client Hello
2018-01-16 01:14:12	23.35.171.27	80	g2.symcb.com		GET /MEQwQjBAMD4wPDAJ…
2018-01-16 01:14:13	23.76.193.124	443		assets.adobedtm.com	Client Hello
2018-01-16 01:14:13	23.76.193.124	443		assets.adobedtm.com	Client Hello
2018-01-16 01:14:13	23.199.238.64	443		se.monetate.net	Client Hello
2018-01-16 01:14:13	23.199.238.64	443		se.monetate.net	Client Hello
2018-01-16 01:14:13	23.76.193.44	443		images10.newegg.com	Client Hello
2018-01-16 01:14:13	23.76.193.44	443		images10.newegg.com	Client Hello
2018-01-16 01:14:13	23.76.193.44	443		images10.newegg.com	Client Hello
2018-01-16 01:14:13	23.76.193.44	443		images10.newegg.com	Client Hello
2018-01-16 01:14:13	23.76.193.44	443		images10.newegg.com	Client Hello
2018-01-16 01:14:13	23.76.193.44	443		images10.newegg.com	Client Hello
2018-01-16 01:14:13	23.76.193.44	443		promotions.newegg.com	Client Hello
2018-01-16 01:14:13	23.76.193.44	443		promotions.newegg.com	Client Hello

Block 1 - Review

- Network Security Monitoring (NSM)
- Wireshark & other pcap analysis tools
- Incident reporting
- Wireshark setup

2018 TRAFFIC ANALYSIS WORKSHOP

Up next...

Block 2: Identifying hosts and users

Block 2 - Overview

- Host information
- Operating system and web browser
- User information
- Hand-on exercises

Host information

- MAC address
- IP address
- Host name

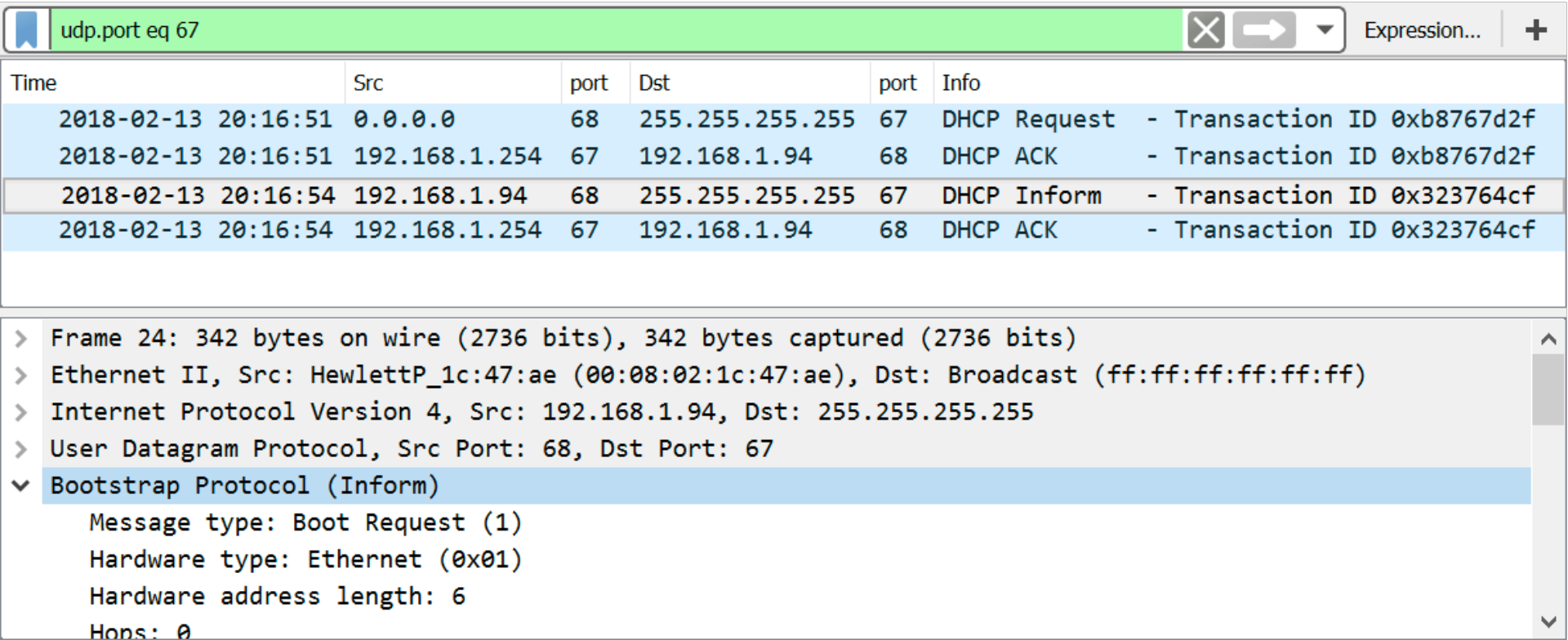
Host information

2018-traffic-analysis-workshop-block-2-01.pcap

Time	Src	port	Dst	port	Info
2018-02-13 20:16:51	0.0.0.0	68	255.255.255.255	67	DHCP Request - Transaction ID 0…
2018-02-13 20:16:51	192.168.1.254	67	192.168.1.94	68	DHCP ACK - Transaction ID 0…
2018-02-13 20:16:51	192.168.1.94		224.0.0.22		Membership Report / Leave group …
2018-02-13 20:16:51	192.168.1.94		224.0.0.22		Membership Report / Join group 2…
2018-02-13 20:16:51	192.168.1.94	57413	224.0.0.252	53…	Standard query 0xbba2 ANY Spider…
2018-02-13 20:16:51	192.168.1.94	137	192.168.1.1	137	Registration NB SPIDER-MAN-PC<00>
2018-02-13 20:16:51	192.168.1.94	137	192.168.1.1	137	Registration NB WORKGROUP<00>
2018-02-13 20:16:51	192.168.1.94	137	192.168.1.1	137	Registration NB SPIDER-MAN-PC<20>
2018-02-13 20:16:51	192.168.1.94	57413	224.0.0.252	53…	Standard query 0xbba2 ANY Spider…
2018-02-13 20:16:51	192.168.1.94		224.0.0.22		Membership Report / Join group 2…
2018-02-13 20:16:52	192.168.1.94	65264	192.168.1.1	53	Standard query 0x961e A isatap.l…
2018-02-13 20:16:53	192.168.1.94	137	192.168.1.1	137	Registration NB SPIDER-MAN-PC<00>
2018-02-13 20:16:53	192.168.1.94	137	192.168.1.1	137	Registration NB WORKGROUP<00>
2018-02-13 20:16:53	192.168.1.94	137	192.168.1.1	137	Registration NB SPIDER-MAN-PC<20>
2018-02-13 20:16:53	192.168.1.94	65264	192.168.1.1	53	Standard query 0x961e A isatap.l…
2018-02-13 20:16:54	192.168.1.94	56118	192.168.1.1	53	Standard query 0x1d08 A teredo.i…

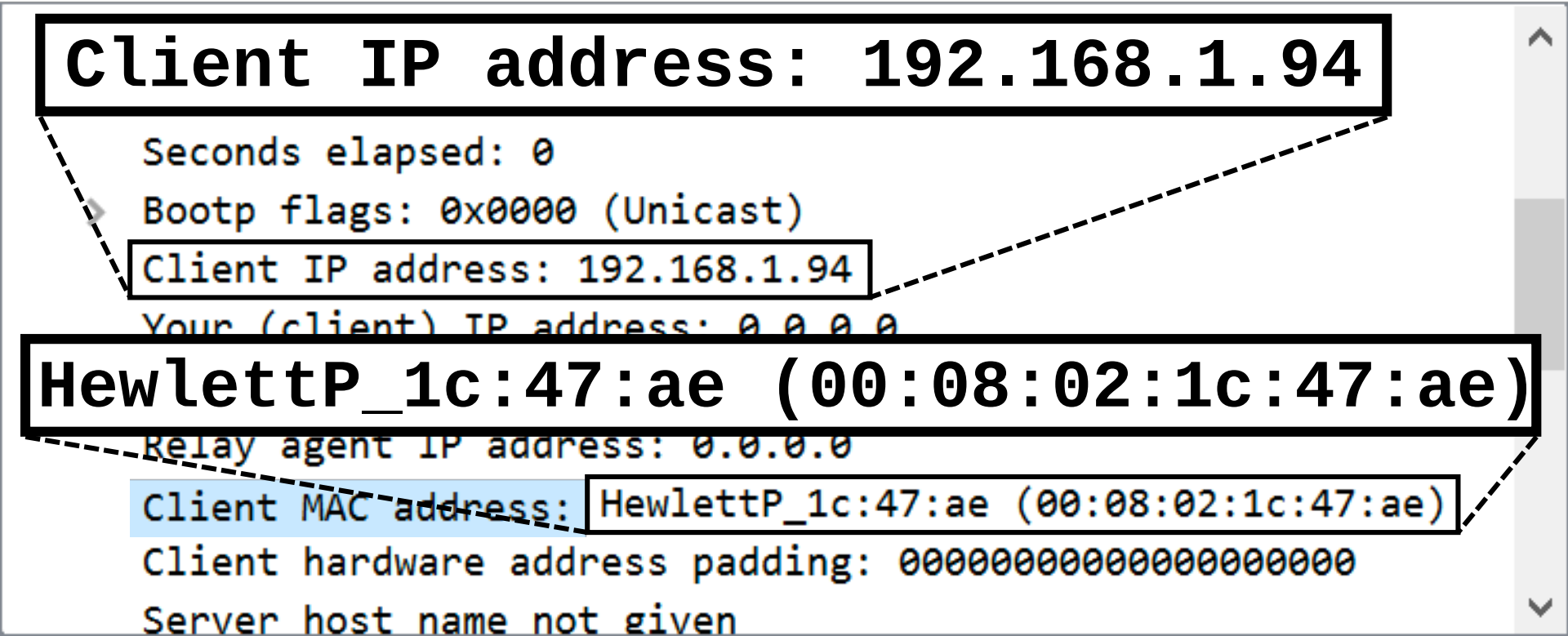
Host information

- DHCP filter: **udp.port eq 67**

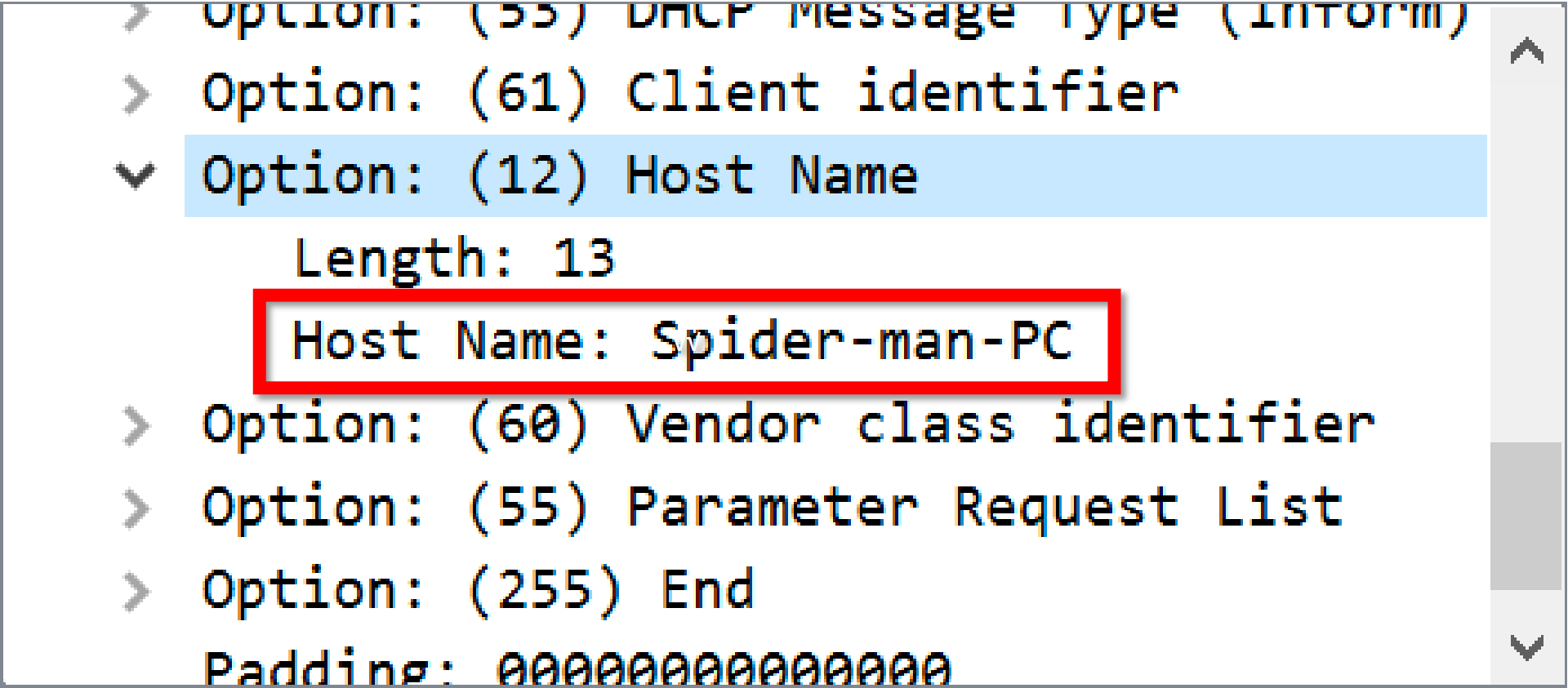


Host information

- Client IP address
- Client MAC address

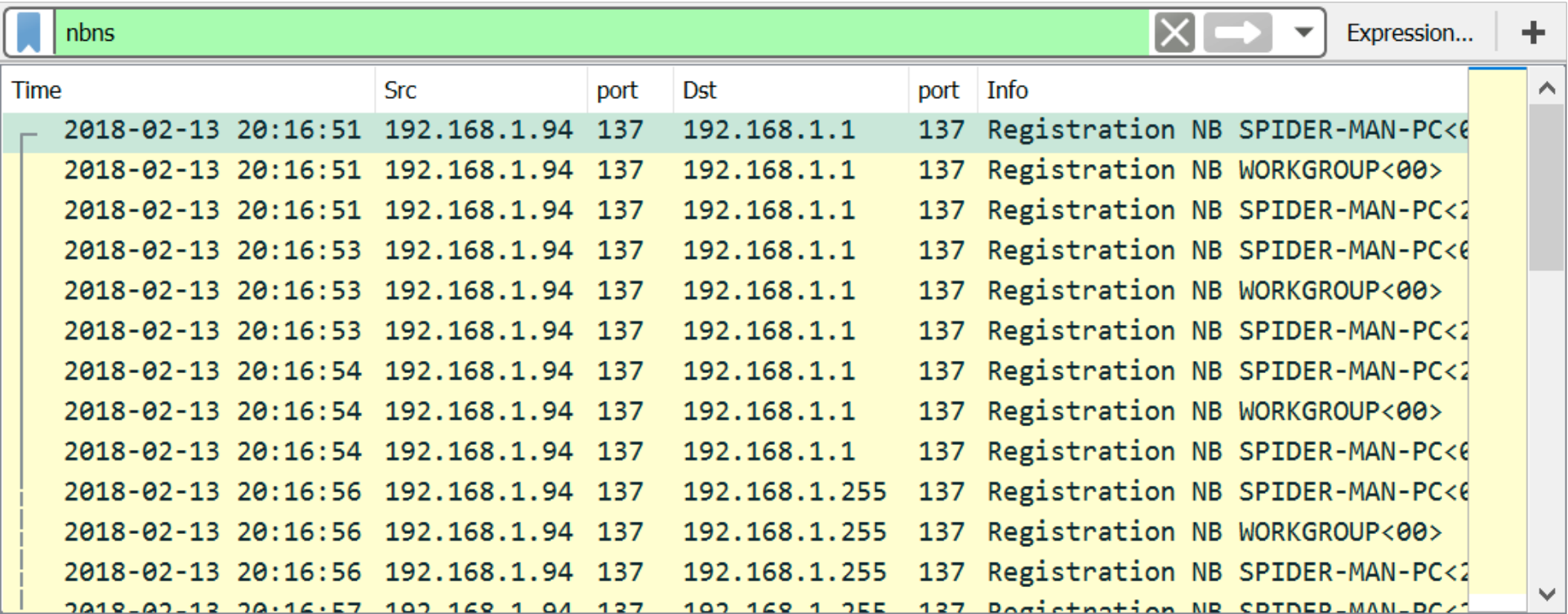


Host information

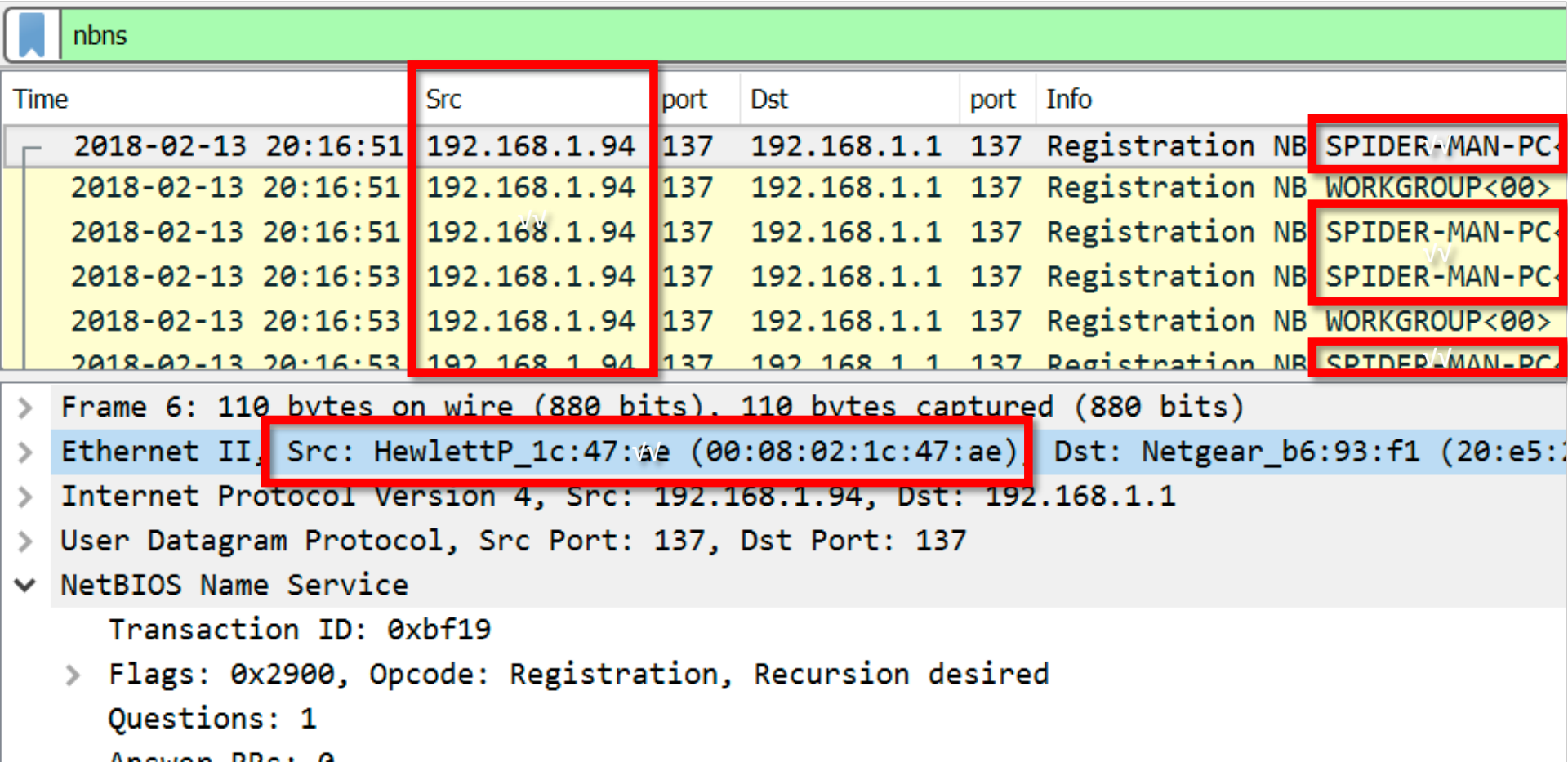


Host information - Windows hosts

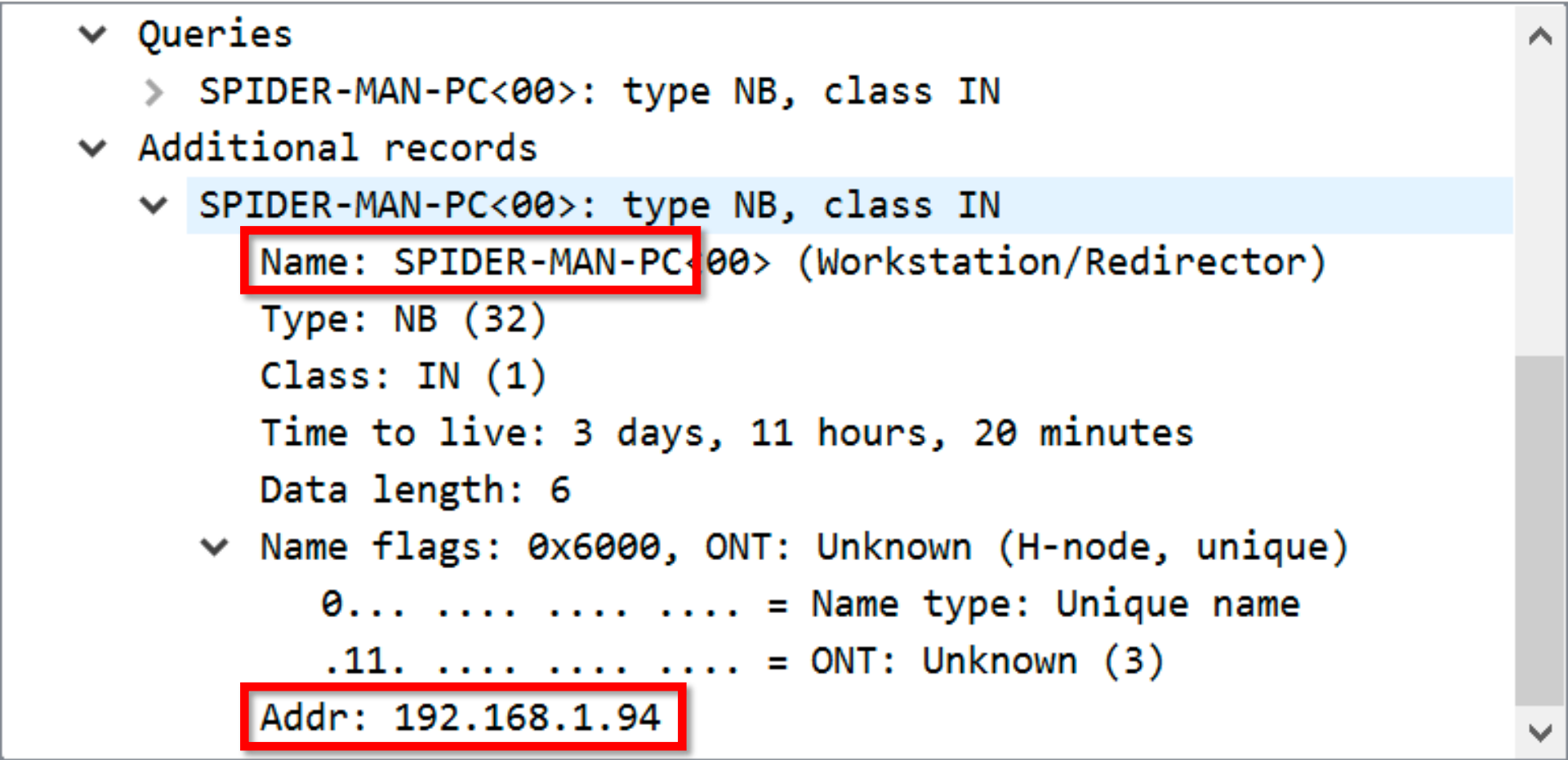
- Wireshark filter: **nbns**



Host information - Windows hosts



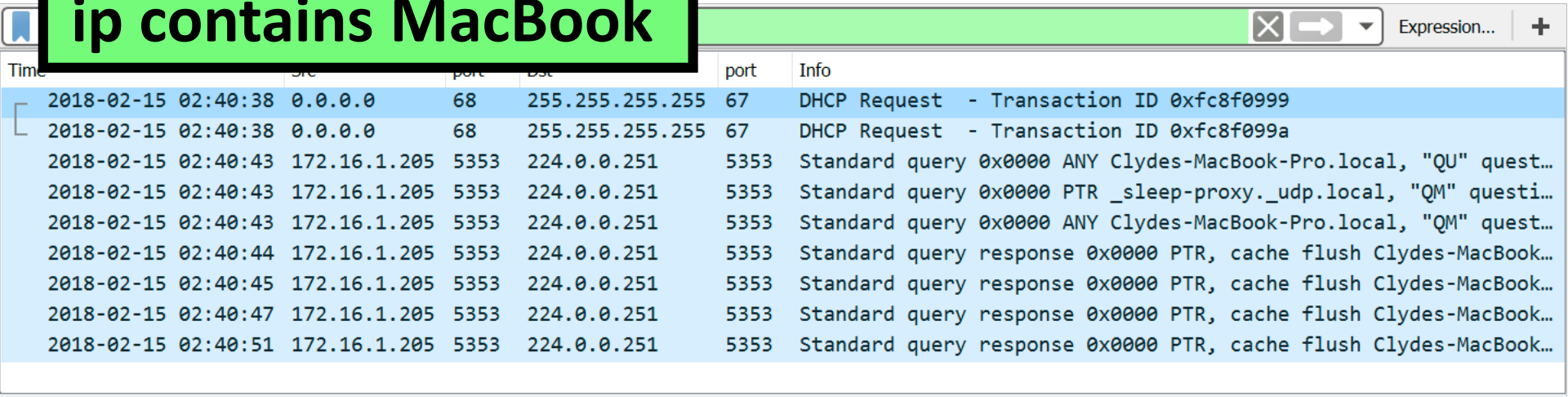
Host information - Windows hosts



Host information - Apple MacBook

2018-traffic-analysis-workshop-block-2-02.pcap

ip contains MacBook

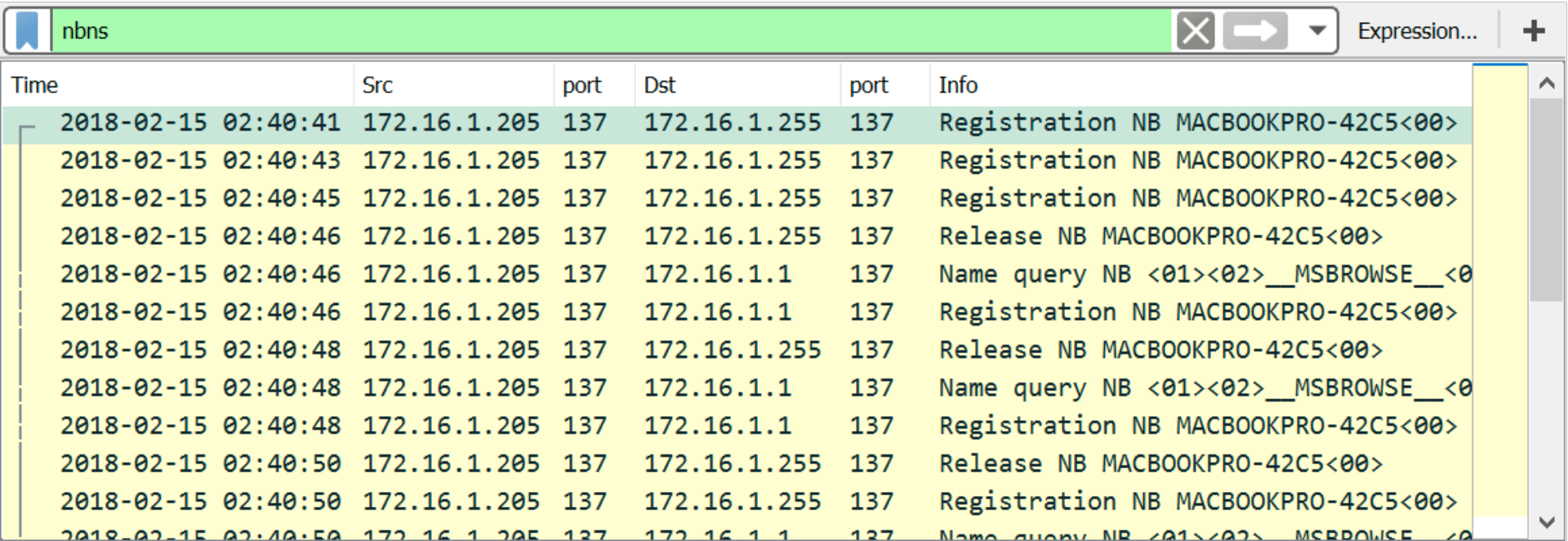


Clydes-MacBook-Pro

Host information - Apple MacBook

- Wireshark filter: **nbns**

MACBOOKPRO-42C5

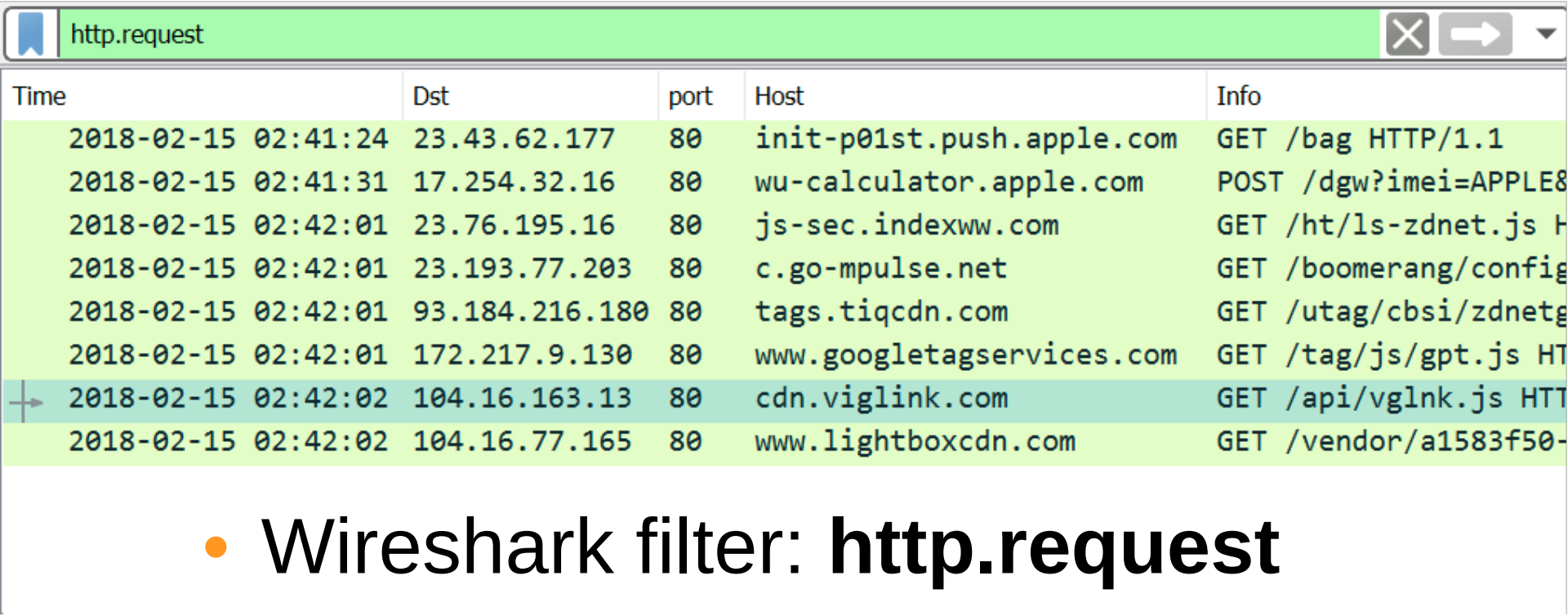


Block 2 - Up next...

- Host information
- **Operating system and web browser**
- User information
- Hands-on exercises

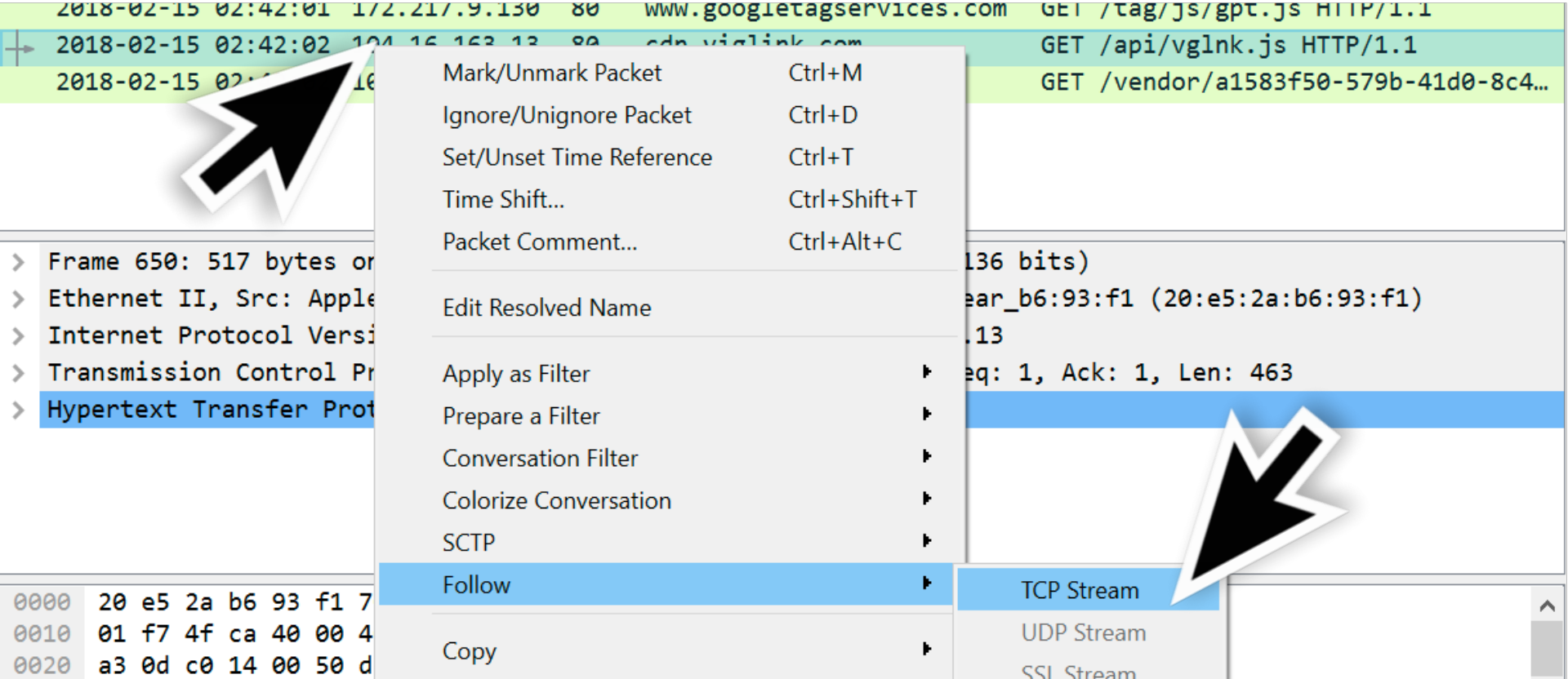
OS and browser - MacBook

2018-traffic-analysis-workshop-block-2-02.pcap



- Wireshark filter: **http.request**

OS and browser - MacBook



OS and browser - MacBook

```
GET /api/vglnk.js HTTP/1.1
Host: cdn.viglink.com
Connection: keep-alive
If-None-Match: "f6b2b7244e312a43e1a926d2b0e97fc3"
Accept: */*
If-Modified-Since: Tue, 13 Feb 2018 21:03:56 GMT
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/601.7.7 (KHTML,
like Gecko) Version/9.1.2 Safari/601.7.7
Accept-Language: en-us
Referer: http://www.zdnet.com/product/apple-macbook-pro-with-touch-bar-13-inch-2017/
Accept-Encoding: gzip, deflate

HTTP/1.1 304 Not Modified
Date: Thu, 15 Feb 2018 02:42:02 GMT
Connection: keep-alive
Set-Cookie: __cfduid=df502aaed589f62b2a6006aa9184c54ec1518662522; expires=Fri, 15-
Feb-19 02:42:02 GMT; path=/; domain=.cdn.viglink.com; HttpOnly
```

Mac OS X 10_11_6

2 client pkts, 3 server pkts, 3 turns

OS and browser - Windows

2018-traffic-analysis-workshop-block-2-03.pcap

Time	Src	port	Dst	port	Host	Info
2018-02-15 04:20:33	10.2.15.101	49162	151.101.1.67	80		49162 → 80 [SYN] Se
2018-02-15 04:20:33	151.101.1.67	80	10.2.15.101	49162		80 → 49162 [SYN, AC
2018-02-15 04:20:33	10.2.15.101	49162	151.101.1.67	80		49162 → 80 [ACK] Se
2018-02-15 04:20:33	10.2.15.101	49162	151.101.1.67	80	www.cnn.com	GET / HTTP/1.1
2018-02-15 04:20:33	151.101.1.67	80	10.2.15.101	49162		80 → 49162 [ACK] Se
2018-02-15 04:20:33	151.101.1.67	80	10.2.15.101	49162		HTTP/1.1 301 Moved
2018-02-15 04:20:33	151.101.1.67	80	10.2.15.101	49162		80 → 49162 [FIN, PS
2018-02-15 04:20:33	10.2.15.101	49162	151.101.1.67	80		49162 → 80 [FIN, AC
2018-02-15 04:20:33	151.101.1.67	80	10.2.15.101	49162		80 → 49162 [ACK] Se
2018-02-15 04:20:33	10.2.15.101	49162	151.101.1.67	80		49162 → 80 [ACK] Se

Right click anywhere & follow TCP stream

OS and browser - Windows

```
GET / HTTP/1.1
Host: www.cnn.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
64.0.3282.140 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: countryCode=US; geoData=tustin|CA|92780|US|NA

HTTP/1.1 301 Moved Permanently
Server: Varnish
Retry-After: 0
Content-Length: 0
Cache-Control: public, max-age=600
Location: https://www.cnn.com/
```

Windows NT 6.1

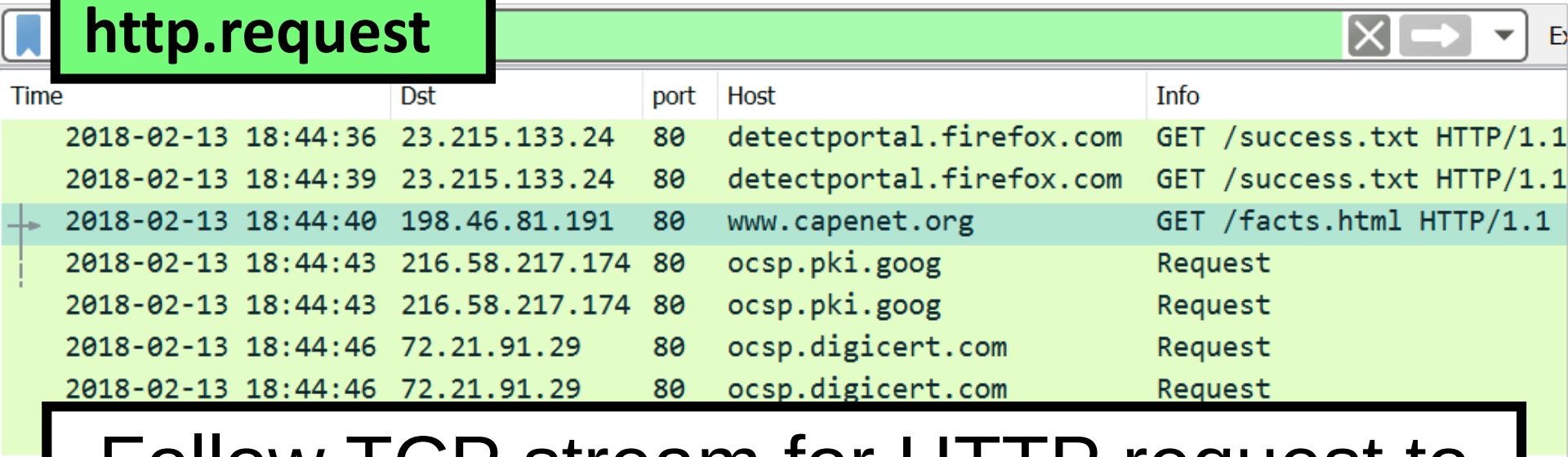
OS and browser - Windows

- **`Windows NT 5.1`** - Windows XP
- **`Windows NT 6.0`** - Windows Vista
- **`Windows NT 6.1`** - Windows 7
- **`Windows NT 6.2`** - Windows 8
- **`Windows NT 6.3`** - Windows 8.1
- **`Windows NT 10.0`** - Windows 10

OS and browser - Linux distros

2018-traffic-analysis-workshop-block-2-04.pcap

http.request



Time	Dst	port	Host	Info
2018-02-13 18:44:36	23.215.133.24	80	detectportal.firefox.com	GET /success.txt HTTP/1.1
2018-02-13 18:44:39	23.215.133.24	80	detectportal.firefox.com	GET /success.txt HTTP/1.1
2018-02-13 18:44:40	198.46.81.191	80	www.capenet.org	GET /facts.html HTTP/1.1
2018-02-13 18:44:43	216.58.217.174	80	ocsp.pki.goog	Request
2018-02-13 18:44:43	216.58.217.174	80	ocsp.pki.goog	Request
2018-02-13 18:44:46	72.21.91.29	80	ocsp.digicert.com	Request
2018-02-13 18:44:46	72.21.91.29	80	ocsp.digicert.com	Request

Follow TCP stream for HTTP request to **www.capenet.org**

OS and browser - Linux distros

```
GET /facts.html HTTP/1.1
Host: www.capenet.org
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:54.0) Gecko/20100101 Firefox/54.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: __utma=91993864.1811908442.1518547318.1518547318.1518547318.1;
__utmb=91993864.1.10.1518547318; __utmz=91993864.1518547318.1.1.utmcsr=google|
utmccn=(organic)|utmcmd=organic|utmctr=(not%20provided); __utmt=1
Connection: keep-alive
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Date: Tue, 13 Feb 2018 18:44:38 GMT
Server: Apache
Upgrade: h2,h2c
Connection: Upgrade, Keep-Alive
```

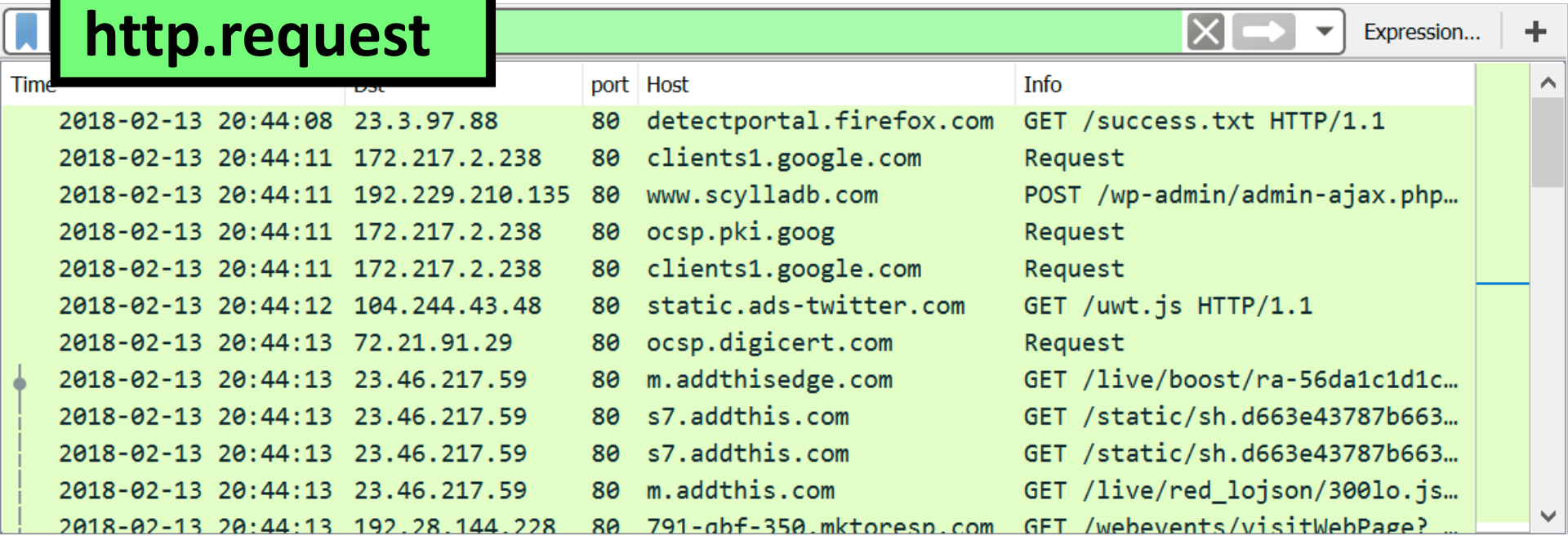
X11; Ubuntu; Linux x86_64

2 client pkts, 56 server pkts, 2 turns

OS and browser - Linux distros - CentOS

2018-traffic-analysis-workshop-block-2-05.pcap

http.request



Follow TCP stream for any of the HTTP requests

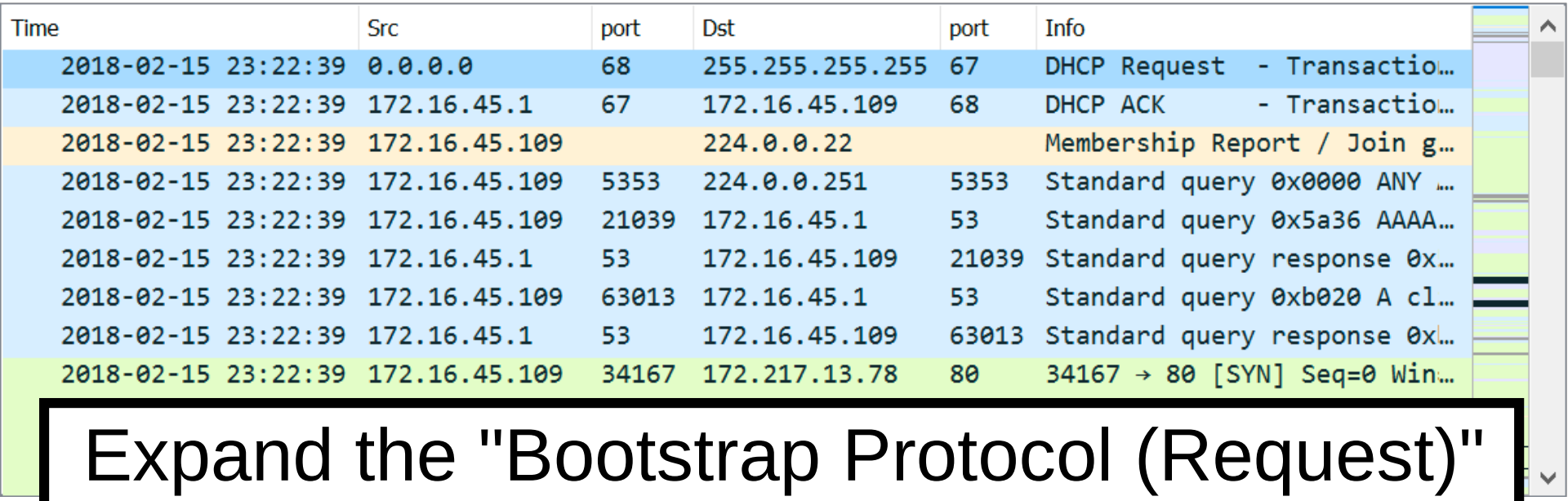
OS and browser - Linux distros - CentOS

```
GET /static/sh.d663e43787b663d5491cf753.html HTTP/1.1
Host: s7.addthis.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.scylladb.com/enterprise-download/centos_rpm/
Cookie: uid=5a834d306f6516bf; uvc=2%7C7; ssc=google%3B1;
loc=NzcwMDFOQVVTVFgyMDk4MDg0NjYxODMzNjAw; mus=0; na_tc=Y
Connection: keep-alive
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Server: nginx
Content-Type: text/html; charset=UTF-8
Content-Length: 24525
Last-Modified: Wed, 03 Jan 2018 15:59:09 GMT
```

X11; Linux x86_64

OS and browser - Android phones

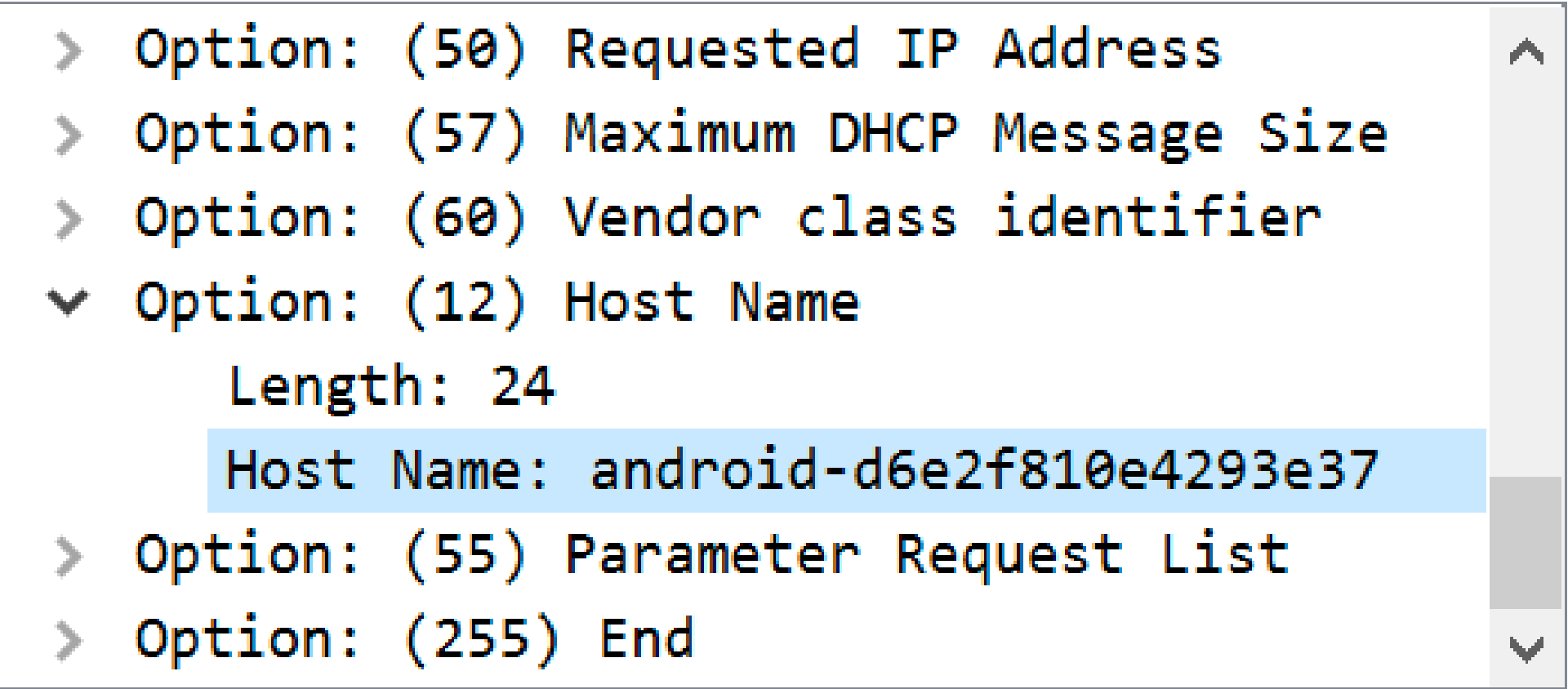
2018-traffic-analysis-workshop-block-2-06.pcap



Time	Src	port	Dst	port	Info
2018-02-15 23:22:39	0.0.0.0	68	255.255.255.255	67	DHCP Request - Transactio…
2018-02-15 23:22:39	172.16.45.1	67	172.16.45.109	68	DHCP ACK - Transactio…
2018-02-15 23:22:39	172.16.45.109		224.0.0.22		Membership Report / Join g…
2018-02-15 23:22:39	172.16.45.109	5353	224.0.0.251	5353	Standard query 0x0000 ANY …
2018-02-15 23:22:39	172.16.45.109	21039	172.16.45.1	53	Standard query 0x5a36 AAAA…
2018-02-15 23:22:39	172.16.45.1	53	172.16.45.109	21039	Standard query response 0x…
2018-02-15 23:22:39	172.16.45.109	63013	172.16.45.1	53	Standard query 0xb020 A cl…
2018-02-15 23:22:39	172.16.45.1	53	172.16.45.109	63013	Standard query response 0x…
2018-02-15 23:22:39	172.16.45.109	34167	172.217.13.78	80	34167 → 80 [SYN] Seq=0 Win…

Expand the "Bootstrap Protocol (Request)" line in window for the first frame

OS and browser - Android phones



OS and browser - Android phones

http.request

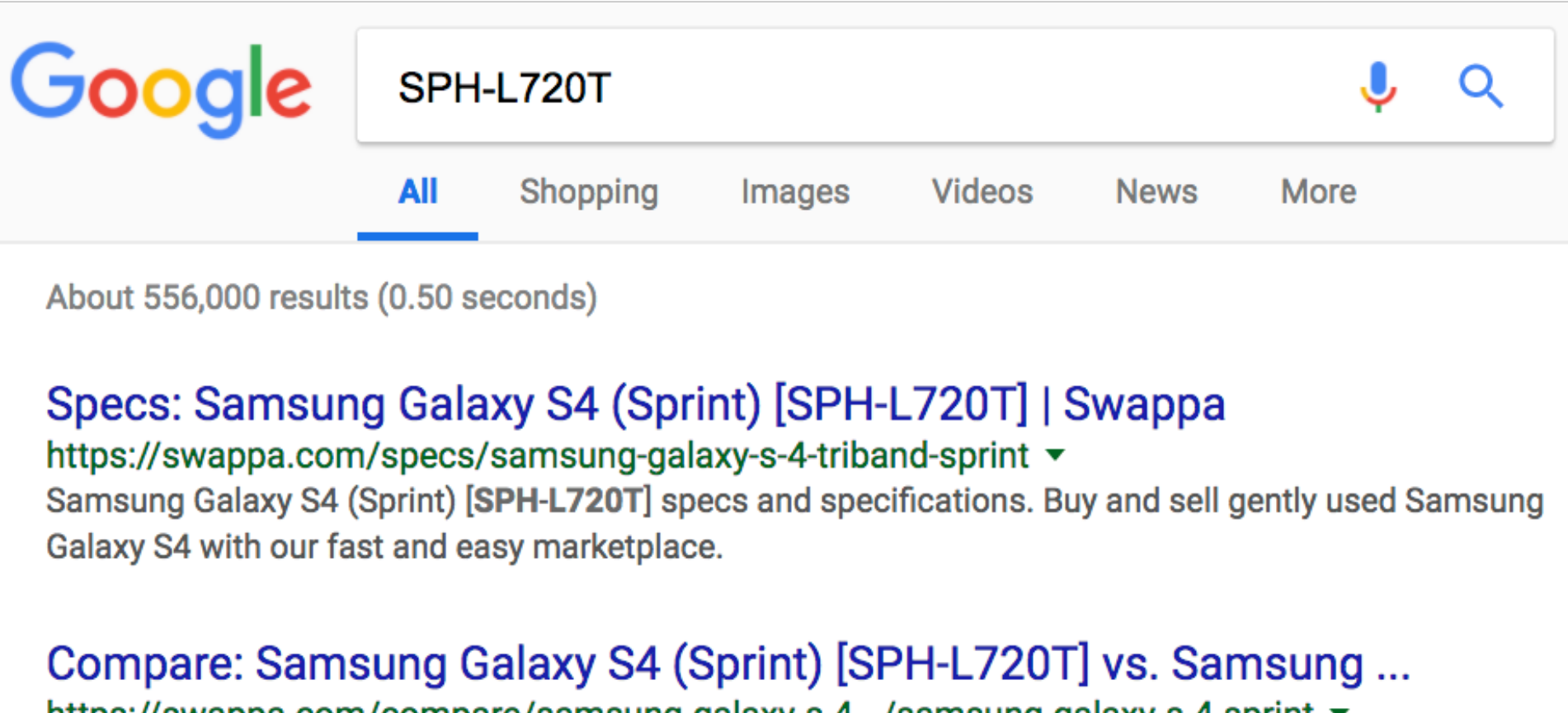
Expression...

Time	Dst	port	Host	Info
2018-02-15 23:22:39	172.217.13.78	80	clients3.google.com	GET /generate_204 HTTP/1.1
2018-02-15 23:22:42	172.217.13.78	80	clients3.google.com	GET /generate_204 HTTP/1.1
2018-02-15 23:22:43	172.217.13.78	80	clients3.google.com	GET /generate_204 HTTP/1.1
2018-02-15 23:22:48	104.154.89.105	80	expired.badssl.com	GET / HTTP/1.1
2018-02-15 23:22:48	52.6.20.199	80	usersync.videoamp.com	GET /usersync/lr0 HTTP/1.1
2018-02-15 23:22:48	74.217.250.89	80	soundwave.bnmla.com	GET /usersync?sspid=1001&r…
2018-02-15 23:22:48	54.68.97.193	80	pixels.sbal4kp.com	GET /ob/lr HTTP/1.1
2018-02-15 23:22:49	34.234.98.90	80	l-idsync.rlcdn.com	GET /462936.gif?served_by=…
2018-02-15 23:22:49	34.234.98.90	80	l-idsync.rlcdn.com	GET /462726.gif?served_by=…
2018-02-15 23:22:49	34.234.98.90	80	l-idsync.rlcdn.com	GET /462666.gif?served_by=…
2018-02-15 23:22:49	34.234.98.90	80	l-idsync.rlcdn.com	GET /462646.gif?served_by=…
2018-02-15 23:22:49	34.234.98.90	80	l-idsync.rlcdn.com	GET /462546.gif?served_by=…

Follow TCP stream for first HTTP request

OS and browser - Android phones

OS and browser - Android phones

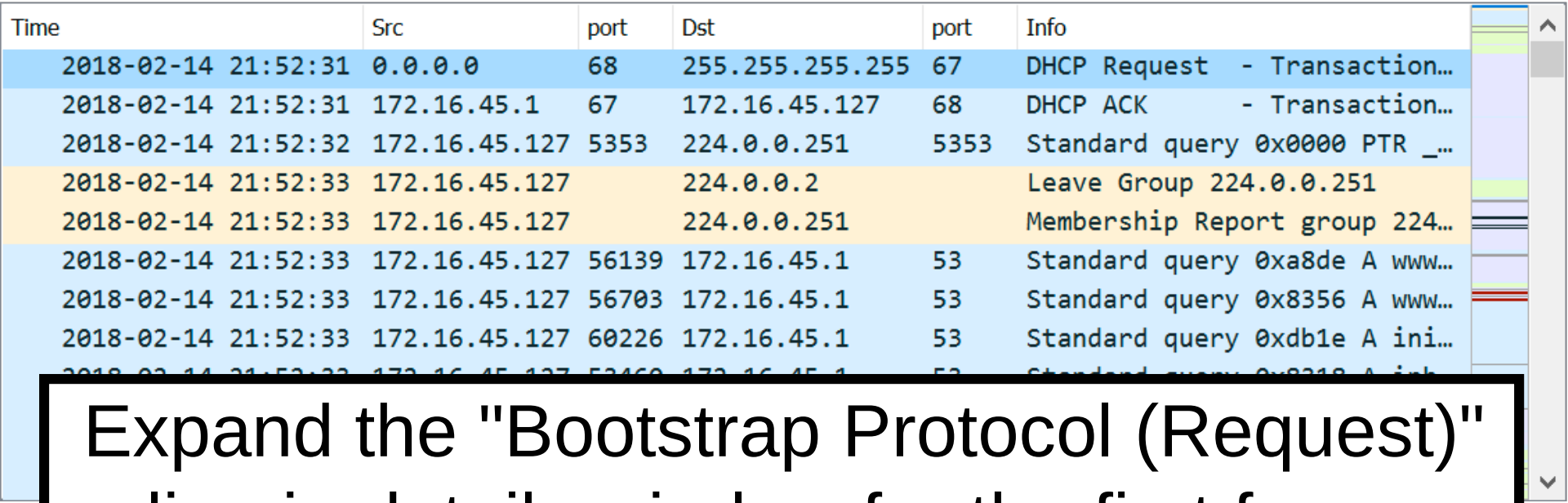


OS and browser - Android phones

- **SCH-I545** - Verizon Galaxy S4
- **SCH-R970** - U.S. Cellular Galaxy S4
- **SGH-I337** - AT&T Galaxy S4
- **SGH-M919** - T-Mobile Galaxy S4
- **SPH-L720** - Sprint Galaxy S4

OS and browser - iPhones

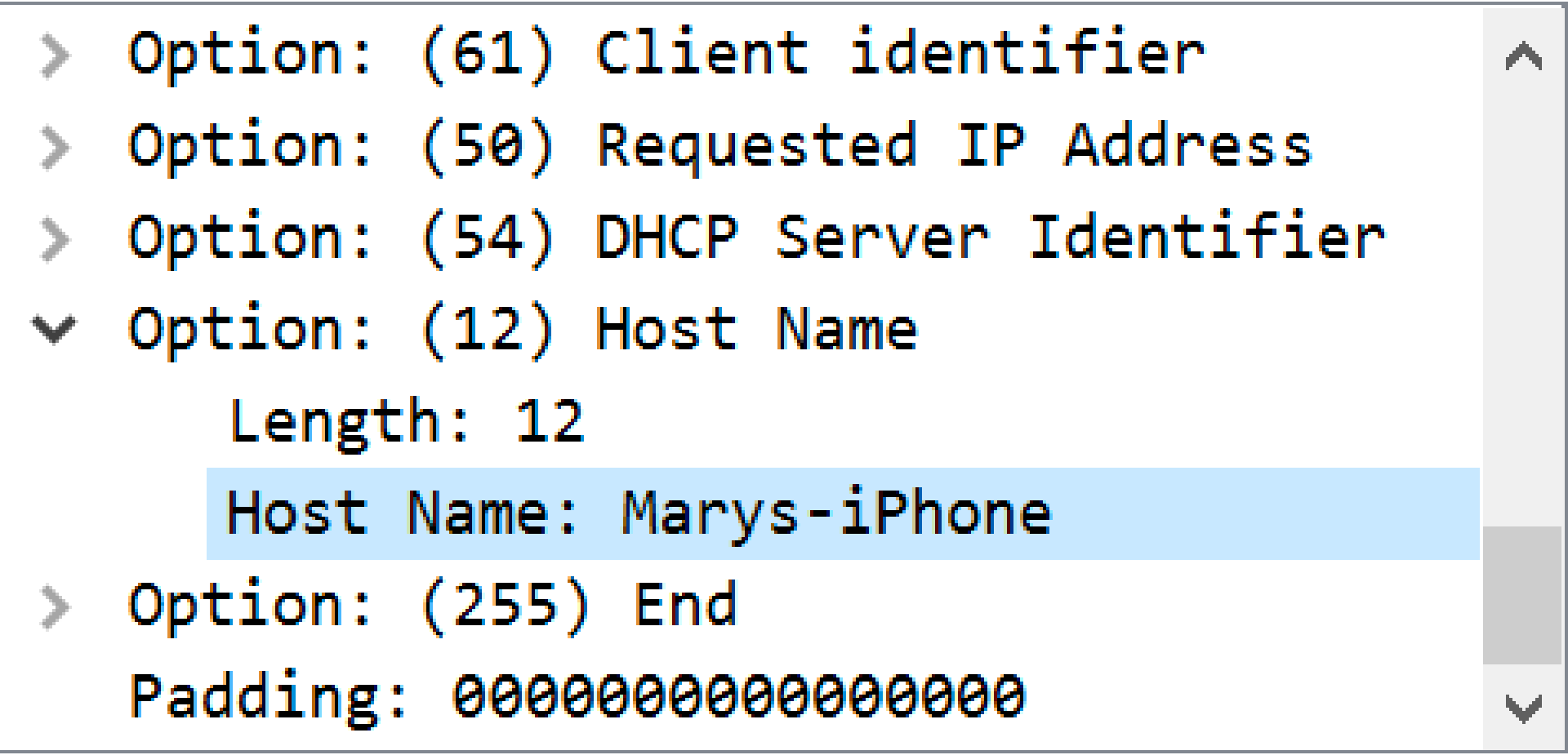
2018-traffic-analysis-workshop-block-2-07.pcap



Time	Src	port	Dst	port	Info
2018-02-14 21:52:31	0.0.0.0	68	255.255.255.255	67	DHCP Request - Transaction…
2018-02-14 21:52:31	172.16.45.1	67	172.16.45.127	68	DHCP ACK - Transaction…
2018-02-14 21:52:32	172.16.45.127	5353	224.0.0.251	5353	Standard query 0x0000 PTR _…
2018-02-14 21:52:33	172.16.45.127		224.0.0.2		Leave Group 224.0.0.251
2018-02-14 21:52:33	172.16.45.127		224.0.0.251		Membership Report group 224…
2018-02-14 21:52:33	172.16.45.127	56139	172.16.45.1	53	Standard query 0xa8de A www…
2018-02-14 21:52:33	172.16.45.127	56703	172.16.45.1	53	Standard query 0x8356 A www…
2018-02-14 21:52:33	172.16.45.127	60226	172.16.45.1	53	Standard query 0xdb1e A ini…

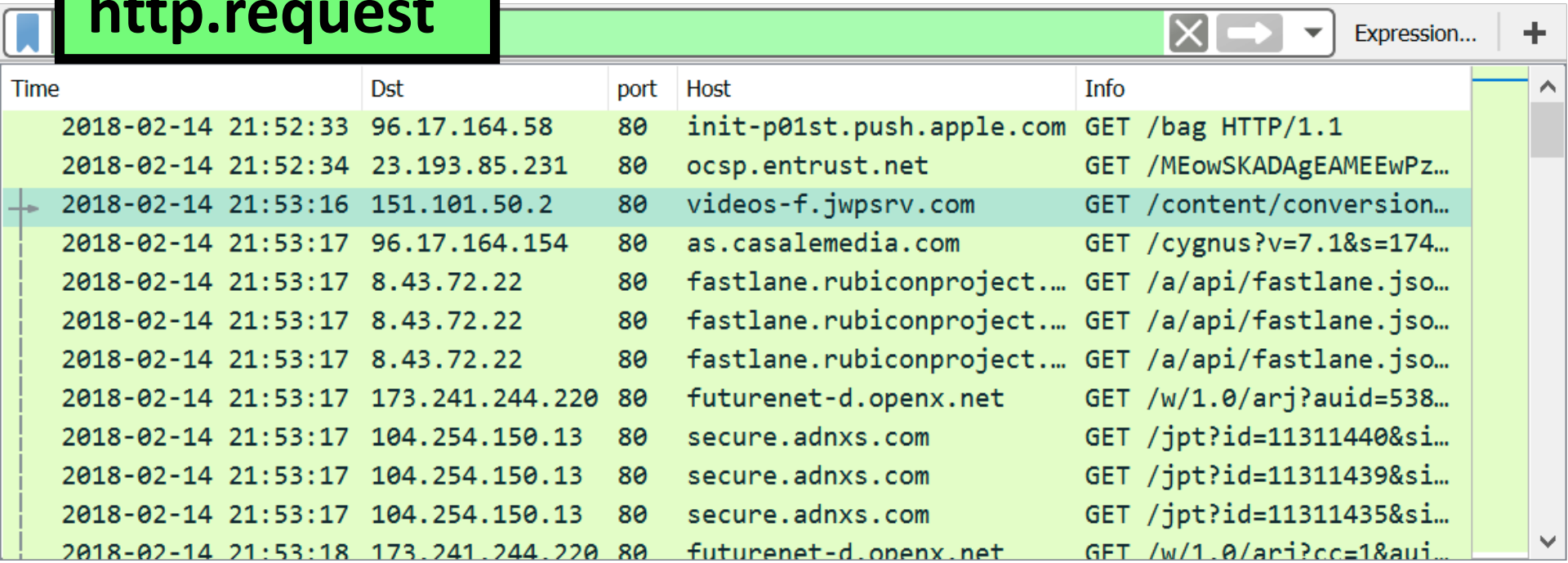
Expand the "Bootstrap Protocol (Request)" line in details window for the first frame

OS and browser - iPhones



OS and browser - iPhones

http.request



Follow TCP stream for 3rd HTTP request

OS and browser - iPhones

```
GET /content/conversions/QWFH4BVQ/videos/xnZe7xJJ-31058985.mp4.m3u8?
token=0_5a84d919_0xc10f0119e04eb5f1bff263a9e42f9485813129be HTTP/1.1
Host: videos-f.jwpsrv.com
Accept-Language: en-us
X-Playback-Session-Id: 341346D7-2AD0-4622-8FF8-D716383D43F6
If-None-Match: "yGVBqCCXf9ocklNDAG1xDZBJuO3YqfSmmmSM-
zjuRp5WX9px7lFLE-7MYPIidf5UHyKeWedi27qXioQqjPimX3zQbA"
Accept: */*
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 11_1_2 like Mac OS X) AppleWebKit/604.3.5
(KHTML, like Gecko) Version/11.0 Mobile/15B202 Safari/604.1
Referer: http://www.techradar.com/reviews/iphone[illegible]-plus-review
Accept-Encoding: identity
Connection: keep-alive

HTTP/1.1 304 Not Modified
Date: Wed, 14 Feb 2018 21:53:16 GMT
Via: 1.1 varnish
```

iPhone OS 11_1_2

Block 2 - Up next...

- Host information
- Operating system and web browser
- **User information**
- Hands-on exercises

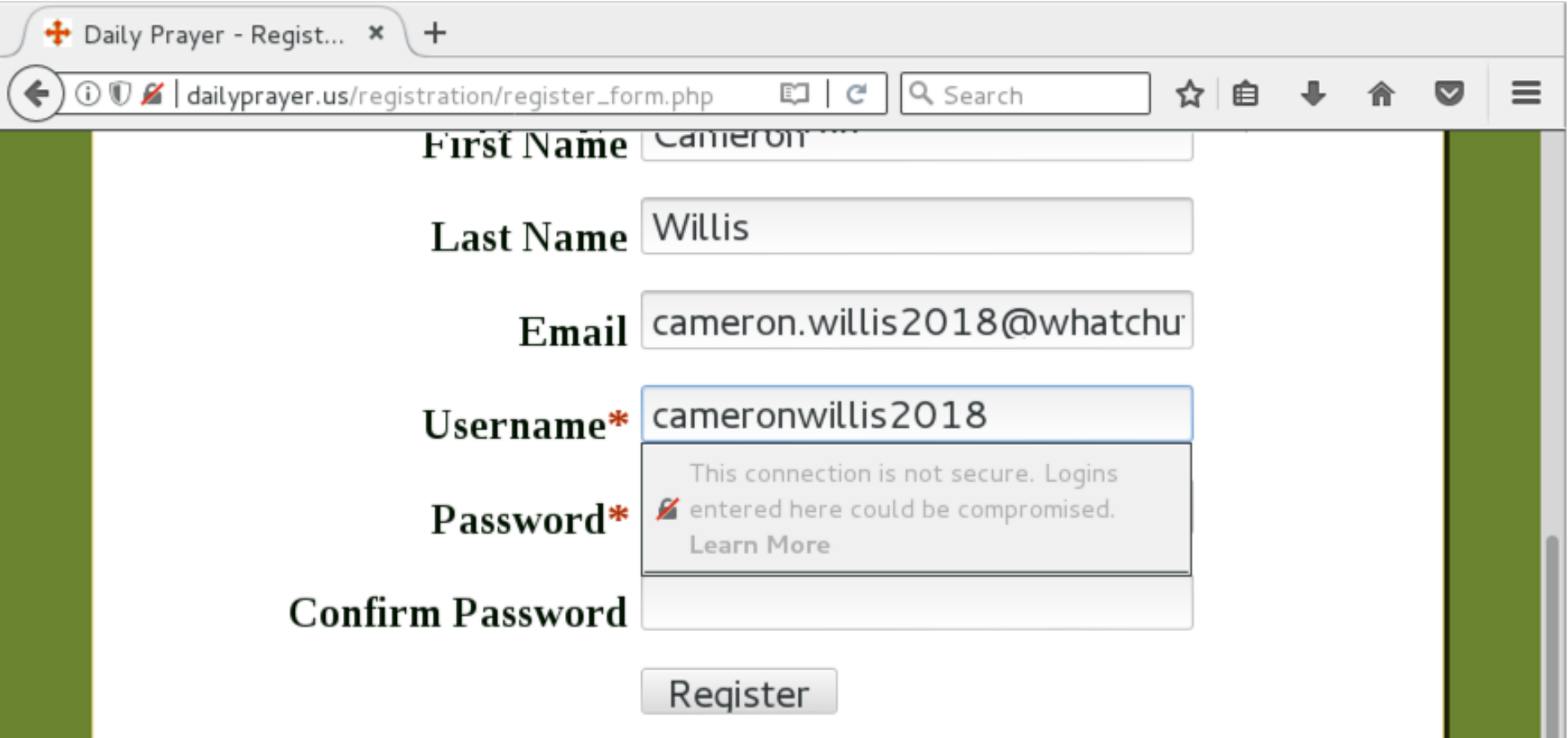
User information

Two ways you might run into user names

Unencrypted web logins

Kerberos traffic when logging into a Windows environment with a domain controller

User information - Web logins: legitimate



User information - Web logins: legitimate

2018-traffic-analysis-workshop-block-2-08.pcap

Time	Src	port	Dst	port	Host	Info
2018-02-16 00:54:01	10.2.16.101	58555	209.200.244.33	80		58555 → 80 [SYN] Seq=0 …
2018-02-16 00:54:01	209.200.244.33	80	10.2.16.101	58555		80 → 58555 [SYN, ACK] S…
2018-02-16 00:54:01	10.2.16.101	58555	209.200.244.33	80		58555 → 80 [ACK] Seq=1 …
2018-02-16 00:54:01	10.2.16.101	58555	209.200.244.33	80	dailyprayer.us	POST /registration/regi…
2018-02-16 00:54:01	209.200.244.33	80	10.2.16.101	58555		80 → 58555 [ACK] Seq=1 …
2018-02-16 00:54:01	209.200.244.33	80	10.2.16.101	58555		HTTP/1.1 302 Moved Temp…
2018-02-16 00:54:01	10.2.16.101	58555	209.200.244.33	80		58555 → 80 [ACK] Seq=73…
2018-02-16 00:54:01	209.200.244.33	80	10.2.16.101	58555		80 → 58555 [FIN, PSH, A…
2018-02-16 00:54:01	10.2.16.101	58555	209.200.244.33	80		58555 → 80 [FIN, ACK] S…
2018-02-16 00:54:01	209.200.244.33	80	10.2.16.101	58555		80 → 58555 [ACK] Seq=37…

Right click anywhere & follow TCP stream

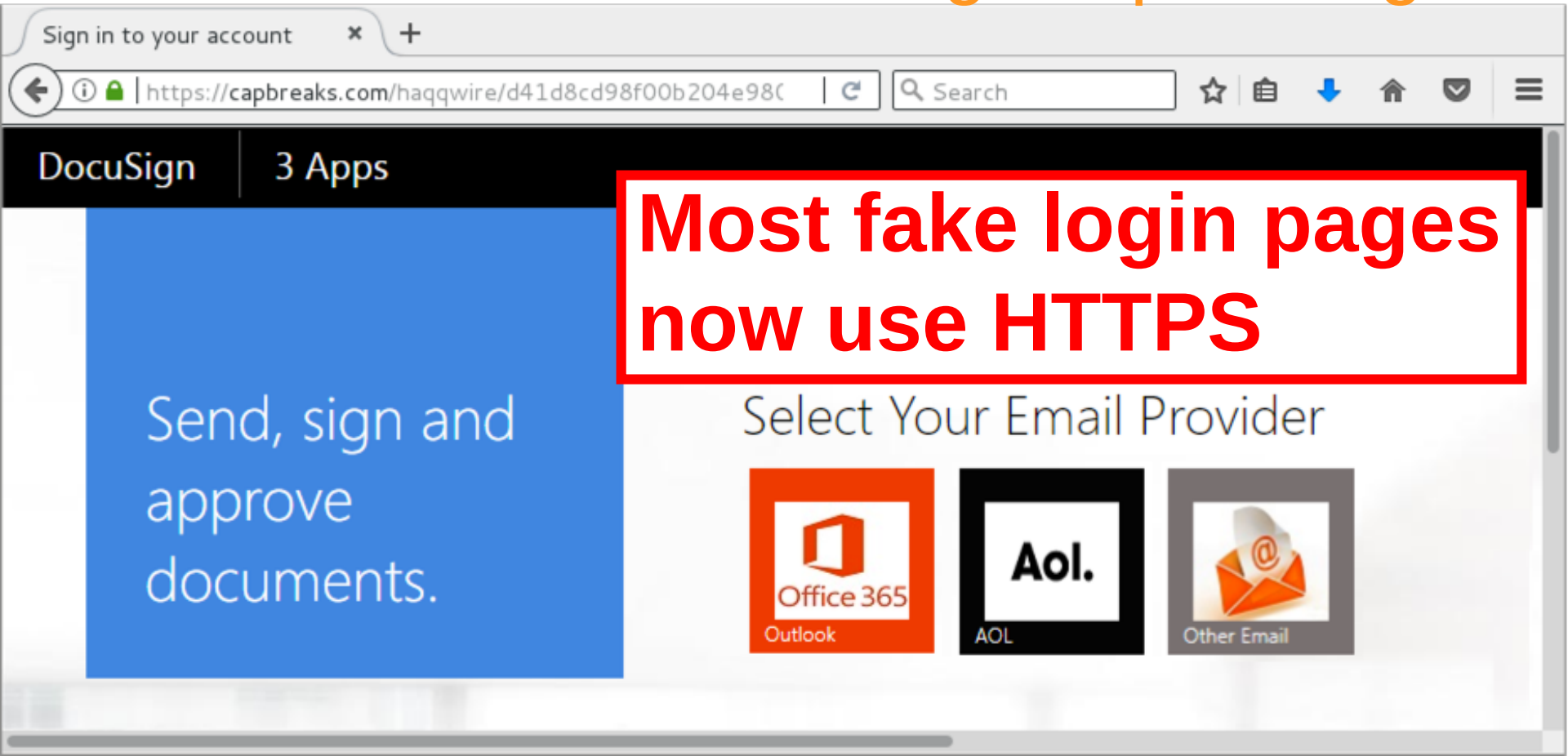
User information - Web logins: legitimate

Wireshark · Follow TCP Stream (tcp.stream eq 0) · 2018-traffic-analysis-workshop-block-3-08

```
POST /registration/register_exec.php HTTP/1.1
Host: dailyprayer.us
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://dailyprayer.us/registration/register_form.php
Cookie: PHPSESSID=5mackm53o3975l7ekfiiv6hme2
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 201

salutation=Mr.&fname=Cameron&lname=Willis&email=cameron.willis2018%40whatchutalkinboutwillis.com
&login=cameronwillis2018&password=whatchutalkinbout12345&cpassword=whatchutalkinbout12345&Submit
=RegisterHTTP/1.1 302 Moved Temporarily
Date: Fri, 16 Feb 2018 00:54:00 GMT
Server: Apache/2.2.3 (CentOS)
```

registration info

User information - Web logins: phishing



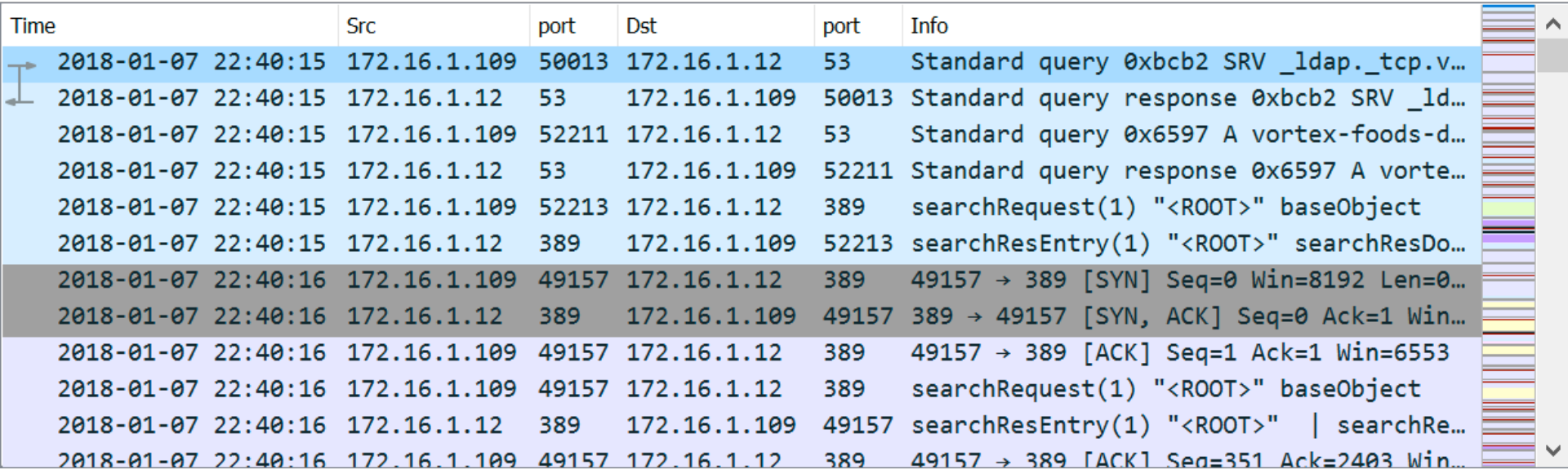
User information: Kerberos info

2018-traffic-analysis-workshop-block-2-09.pcap

- Domain: vortexfoods.com
- Domain controller: **172.16.1.12**
  Vortex-Foods-DC
- Windows client: **172.16.1.109**
  Oakland-1a8f-PC

User information: Kerberos info

2018-traffic-analysis-workshop-block-2-09.pcap



Time	Src	port	Dst	port	Info
2018-01-07 22:40:15	172.16.1.109	50013	172.16.1.12	53	Standard query 0xbcb2 SRV _ldap._tcp.v…
2018-01-07 22:40:15	172.16.1.12	53	172.16.1.109	50013	Standard query response 0xbcb2 SRV _ld…
2018-01-07 22:40:15	172.16.1.109	52211	172.16.1.12	53	Standard query 0x6597 A vortex-foods-d…
2018-01-07 22:40:15	172.16.1.12	53	172.16.1.109	52211	Standard query response 0x6597 A vorte…
2018-01-07 22:40:15	172.16.1.109	52213	172.16.1.12	389	searchRequest(1) "<ROOT>" baseObject
2018-01-07 22:40:15	172.16.1.12	389	172.16.1.109	52213	searchResEntry(1) "<ROOT>" searchResDo…
2018-01-07 22:40:16	172.16.1.109	49157	172.16.1.12	389	49157 → 389 [SYN] Seq=0 Win=8192 Len=0…
2018-01-07 22:40:16	172.16.1.12	389	172.16.1.109	49157	389 → 49157 [SYN, ACK] Seq=0 Ack=1 Win…
2018-01-07 22:40:16	172.16.1.109	49157	172.16.1.12	389	49157 → 389 [ACK] Seq=1 Ack=1 Win=6553
2018-01-07 22:40:16	172.16.1.109	49157	172.16.1.12	389	searchRequest(1) "<ROOT>" baseObject
2018-01-07 22:40:16	172.16.1.12	389	172.16.1.109	49157	searchResEntry(1) "<ROOT>" | searchRe…
2018-01-07 22:40:16	172.16.1.109	49157	172.16.1.12	389	49157 → 389 [ACK] Seq=351 Ack=2403 Win…

Need to filter for Kerberos

User information: Kerberos info

kerberos

Expression...

Time	Src	port	Dst	port	Info
2018-01-07 22:40:16	172.16.1.109	49158	172.16.1.12	88	AS-REQ
2018-01-07 22:40:16	172.16.1.12	88	172.16.1.109	49158	KRB Error: KRB5KDC_ERR_PREAUTH…
2018-01-07 22:40:16	172.16.1.109	49159	172.16.1.12	88	AS-REQ
2018-01-07 22:40:16	172.16.1.12	88	172.16.1.109	49159	AS-REP
2018-01-07 22:40:16	172.16.1.109	49160	172.16.1.12	88	TGS-REQ
2018-01-07 22:40:16	172.16.1.12	88	172.16.1.109	49160	TGS-REP
2018-01-07 22:40:16	172.16.1.109	49157	172.16.1.12	389	bindRequest(3) "<ROOT>" sasl
2018-01-07 22:40:16	172.16.1.12	389	172.16.1.109	49157	bindResponse(3) success
2018-01-07 22:40:16	172.16.1.109	49161	172.16.1.12	389	bindRequest(10) "<ROOT>" sasl
2018-01-07 22:40:16	172.16.1.12	389	172.16.1.109	49161	bindResponse(10) success
2018-01-07 22:40:16	172.16.1.109	49162	172.16.1.12	88	AS-REQ
2018-01-07 22:40:16	172.16.1.12	88	172.16.1.109	49162	KRB Error: KRB5KDC_ERR_PREAUTH…

- AS-REQ
- AS-REP
- TGS-REQ
- TGS-REP

User information: Kerberos info

To find a user account name:

kerberos.CNameString and !(kerberos.CNameString contains $)

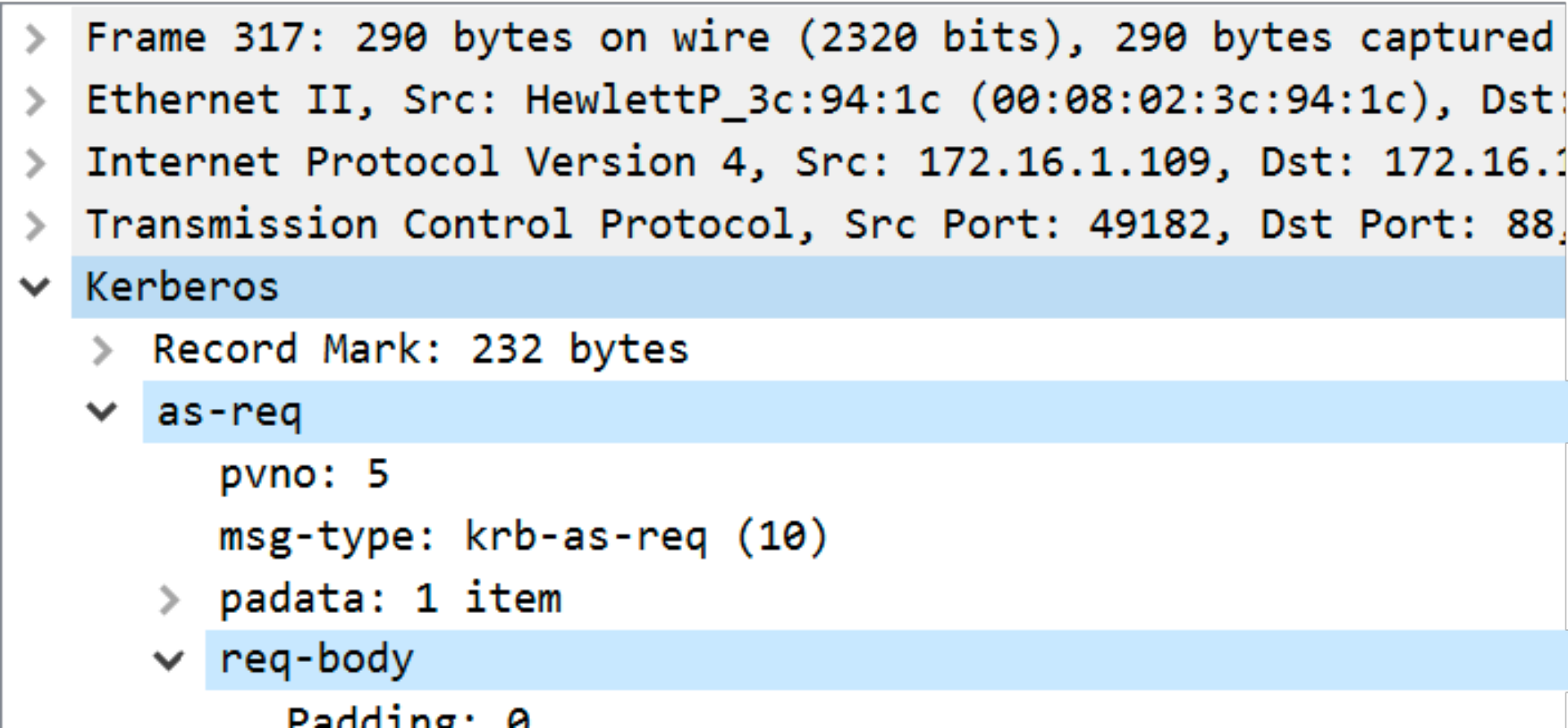
User information: Kerberos info

kerberos.CNameString and !(kerberos.CNameString contains $)

Time	Src	port	Dst	port	Info
2018-01-07 22:40:44	172.16.1.109	49182	172.16.1.12	88	AS-REQ
2018-01-07 22:40:44	172.16.1.109	49183	172.16.1.12	88	AS-REQ
2018-01-07 22:40:44	172.16.1.12	88	172.16.1.109	49183	AS-REP
2018-01-07 22:40:44	172.16.1.12	88	172.16.1.109	49184	TGS-REP
2018-01-07 22:40:44	172.16.1.12	88	172.16.1.109	49185	TGS-REP
2018-01-07 22:40:45	172.16.1.12	88	172.16.1.109	49188	TGS-REP
2018-01-07 22:40:45	172.16.1.12	88	172.16.1.109	49191	TGS-REP
2018-01-07 22:40:45	172.16.1.12	88	172.16.1.109	49192	TGS-REP

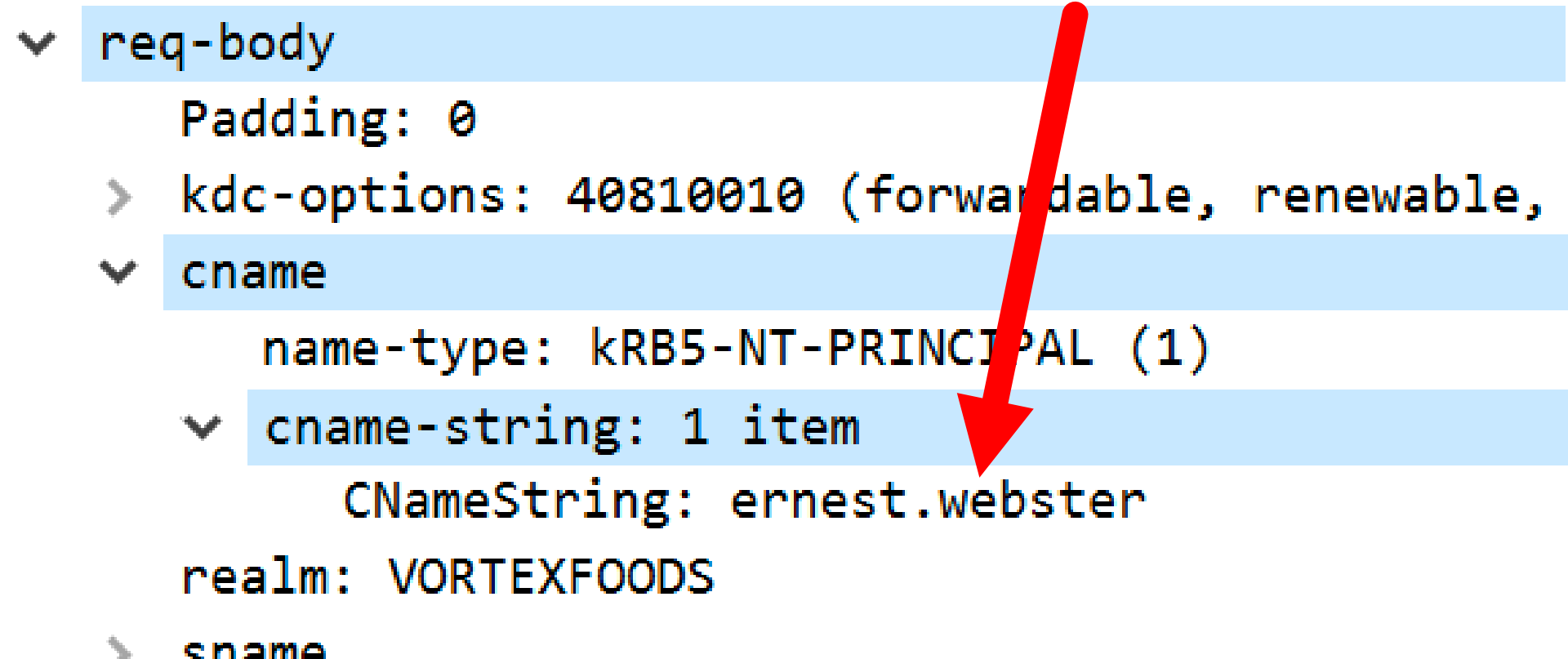
```
> Frame 317: 290 bytes on wire (2320 bits), 290 bytes captured (2320 bits)
> Ethernet II, Src: HewlettP_3c:94:1c (00:08:02:3c:94:1c), Dst: Dell_84:ab:2d (00:1
> Internet Protocol Version 4, Src: 172.16.1.109, Dst: 172.16.1.12
```

User information: Kerberos info



User information: Kerberos info

CNameString: ernest.webster



Block 2 - Review

- Host information
- Operating system and web browser
- User information
- Hand-on exercises (5 pcaps)

2018 TRAFFIC ANALYSIS WORKSHOP

Up next...

Block 3: Malware infection traffic

Block 3 - Overview

- Windows malware: HTTP traffic
- Windows malware: encrypted traffic
- Windows malware: SMB traffic
- Windows malware: FTP and IRC traffic
- Exercise and bonus pcaps

Windows malware: HTTP traffic

2018-traffic-analysis-workshop-block-3-01.pcap

LOKIBOT

- Also called "Loki bot" or "Loki-bot”
- Windows-based information stealing malware
- Advertised in underground forums as early as 2015
- Increase in publicly-reported samples during 2017

Windows malware: HTTP traffic

2018-traffic-analysis-workshop-block-3-01.pcap

http.request

Expression...

Time	Dst	port	Host	Info
2018-02-15 16:30:49	184.24.98.184	80	www.msftncsi.com	GET /ncsi.txt HTTP/1.1
2018-02-15 16:33:56	31.220.104.230	80	www.speedneedoxyz.xyz	POST /calis/fre.php HTTP/1.0
2018-02-15 16:33:56	31.220.104.230	80	www.speedneedoxyz.xyz	POST /calis/fre.php HTTP/1.0
2018-02-15 16:33:56	31.220.104.230	80	www.speedneedoxyz.xyz	POST /calis/fre.php HTTP/1.0
2018-02-15 16:34:57	31.220.104.230	80	www.speedneedoxyz.xyz	POST /calis/fre.php HTTP/1.0
2018-02-15 16:35:57	31.220.104.230	80	www.speedneedoxyz.xyz	POST /calis/fre.php HTTP/1.0
2018-02-15 16:36:57	31.220.104.230	80	www.speedneedoxyz.xyz	POST /calis/fre.php HTTP/1.0
2018-02-15 16:37:58	31.220.104.230	80	www.speedneedoxyz.xyz	POST /calis/fre.php HTTP/1.0
2018-02-15 16:38:58	31.220.104.230	80	www.speedneedoxyz.xyz	POST /calis/fre.php HTTP/1.0
2018-02-15 16:39:58	31.220.104.230	80	www.speedneedoxyz.xyz	POST /calis/fre.php HTTP/1.0
2018-02-15 16:40:59	31.220.104.230	80	www.speedneedoxyz.xyz	POST /calis/fre.php HTTP/1.0
2018-02-15 16:41:59	31.220.104.230	80	www.speedneedoxyz.xyz	POST /calis/fre.php HTTP/1.0

Windows malware: HTTP traffic

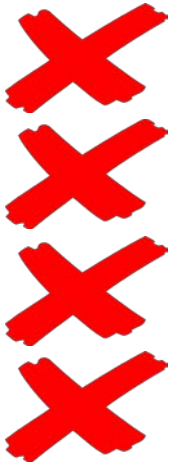
```
POST /calis/fre.php HTTP/1.0
User-Agent: Mozilla/4.08 (Charon; Inferno)
Accept: */*
Content-Type: application/octet-stream
Content-Encoding: binary
Content-Key: 3A9D9D22
Content-Length: 196
Connection: close

..'.......ckav.ru......m.a.r.k...h.a.r.m.o.n.......H.A.R.M.O.N.-.P.C.......H.A.R.M.O.N.-.P
.C.....................k.................0...3.8.4.6.2.6.2.0.2.2.0.5.4.0.2.7.4.E.B.4.1.B.
1.E.....vHT2K....HTTP/1.1 404 Not Found
Server: openresty
Date: Thu, 15 Feb 2018 16:33:56 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
X-Powered-By: PHP/7.0.25

File not found.
```

m.a.r.k...h.a.r.m.o.n

H.A.R.M.O.N.-.P.C

Windows malware: HTTP traffic

How can we tell this is **LOKIBOT**?



- Snort/Suricata based alerts
- Submit the pcap to PacketTotal
- Submit the pcap to VirusTotal
- Sandboxes like Reverse.it can also provide info

Windows malware: HTTP traffic

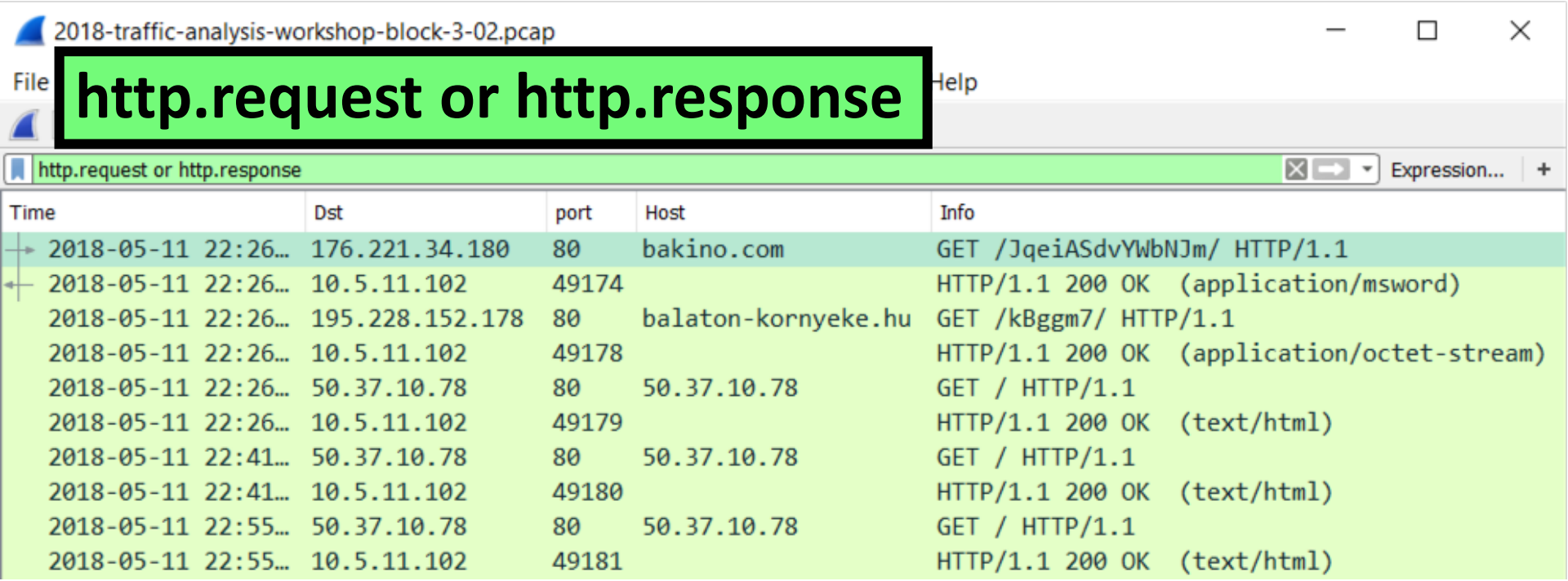
2018-traffic-analysis-workshop-block-3-02.pcap

EMOTET

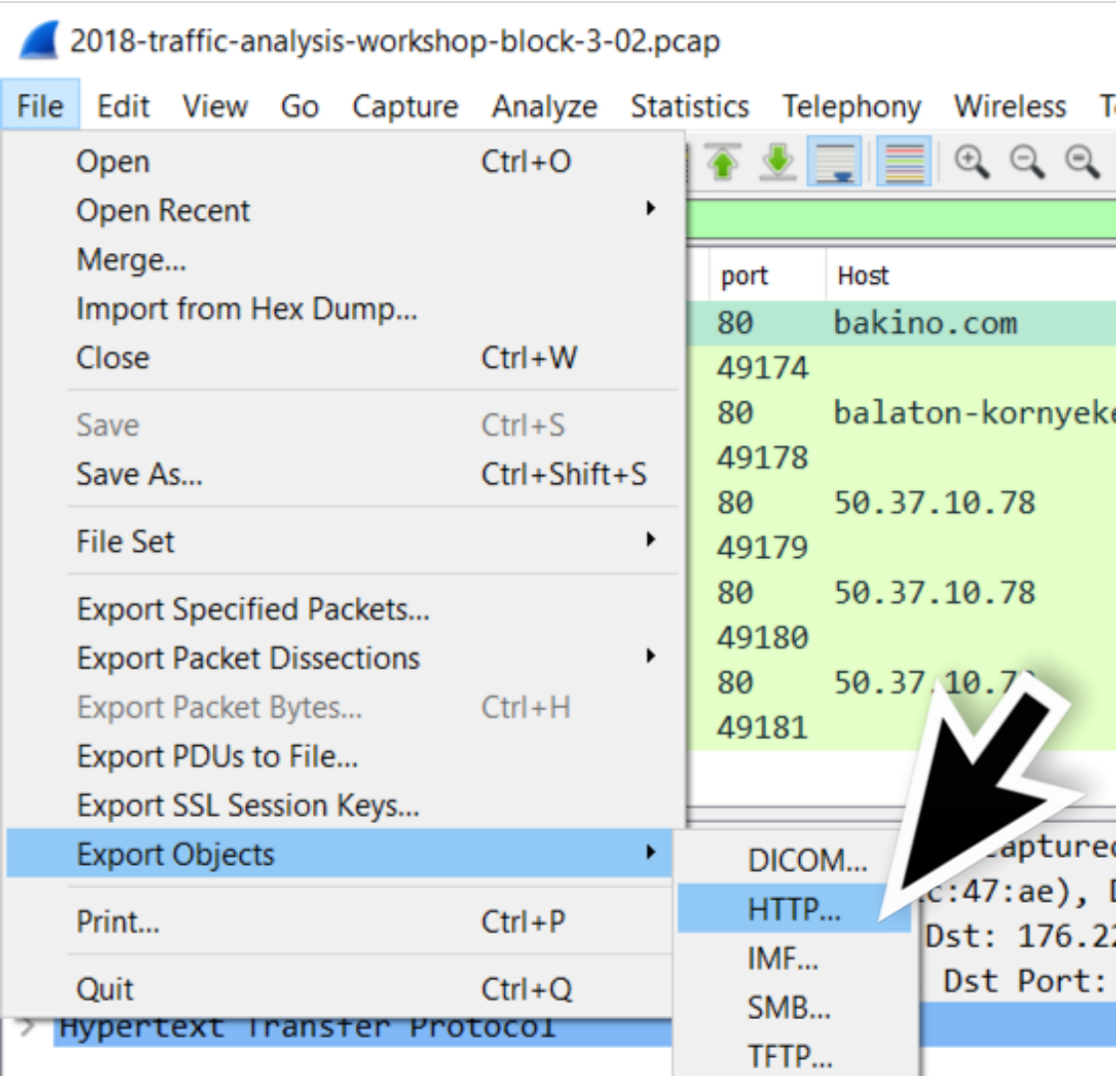
- Windows banking malware first reported in 2014
- Seen daily through invoice-themed malspam
- Emails have a link that returns a Word doc
- Word doc has macro that retrieves & installs Emotet

Windows malware: HTTP traffic

2018-traffic-analysis-workshop-block-3-02.pcap

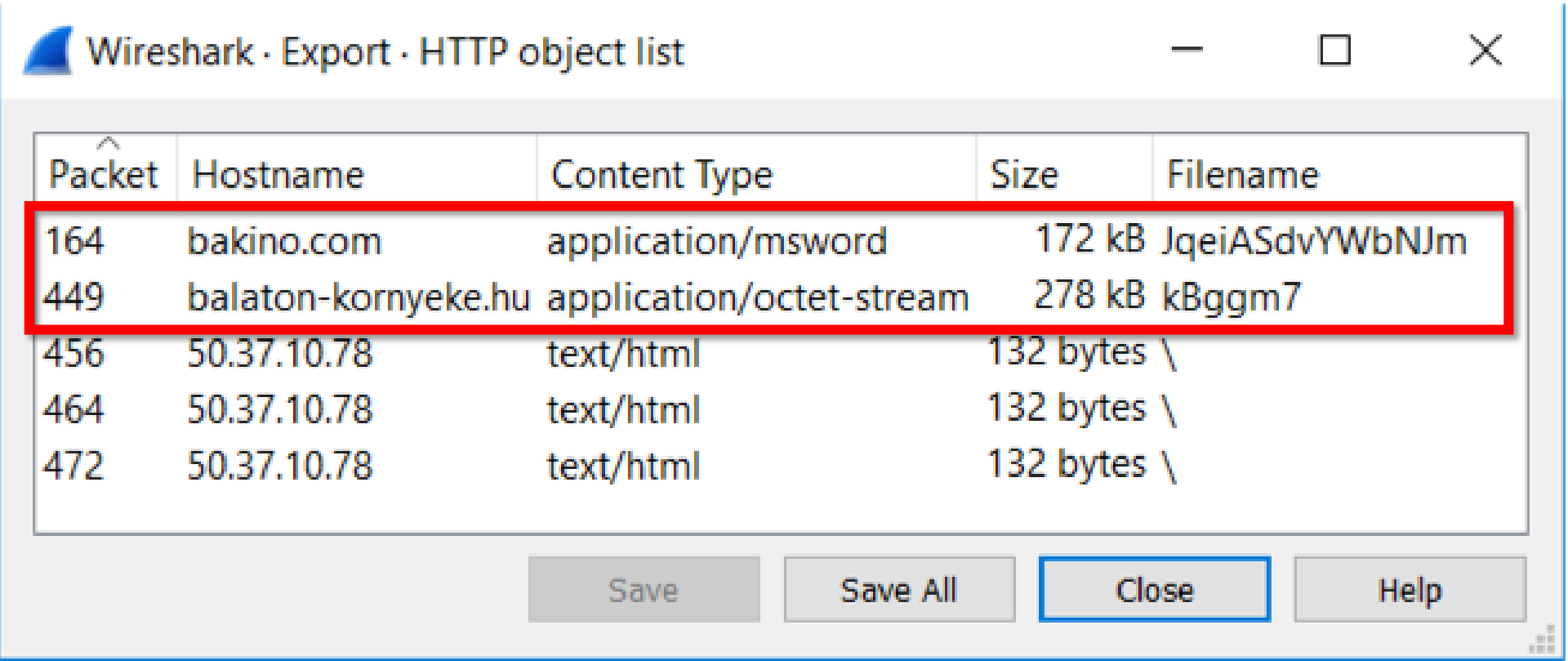


Time	Dst	port	Host	Info
2018-05-11 22:26…	176.221.34.180	80	bakino.com	GET /JqeiASdvYWbNJm/ HTTP/1.1
2018-05-11 22:26…	10.5.11.102	49174		HTTP/1.1 200 OK (application/msword)
2018-05-11 22:26…	195.228.152.178	80	balaton-kornyeke.hu	GET /kBggm7/ HTTP/1.1
2018-05-11 22:26…	10.5.11.102	49178		HTTP/1.1 200 OK (application/octet-stream)
2018-05-11 22:26…	50.37.10.78	80	50.37.10.78	GET / HTTP/1.1
2018-05-11 22:26…	10.5.11.102	49179		HTTP/1.1 200 OK (text/html)
2018-05-11 22:41…	50.37.10.78	80	50.37.10.78	GET / HTTP/1.1
2018-05-11 22:41…	10.5.11.102	49180		HTTP/1.1 200 OK (text/html)
2018-05-11 22:55…	50.37.10.78	80	50.37.10.78	GET / HTTP/1.1
2018-05-11 22:55…	10.5.11.102	49181		HTTP/1.1 200 OK (text/html)



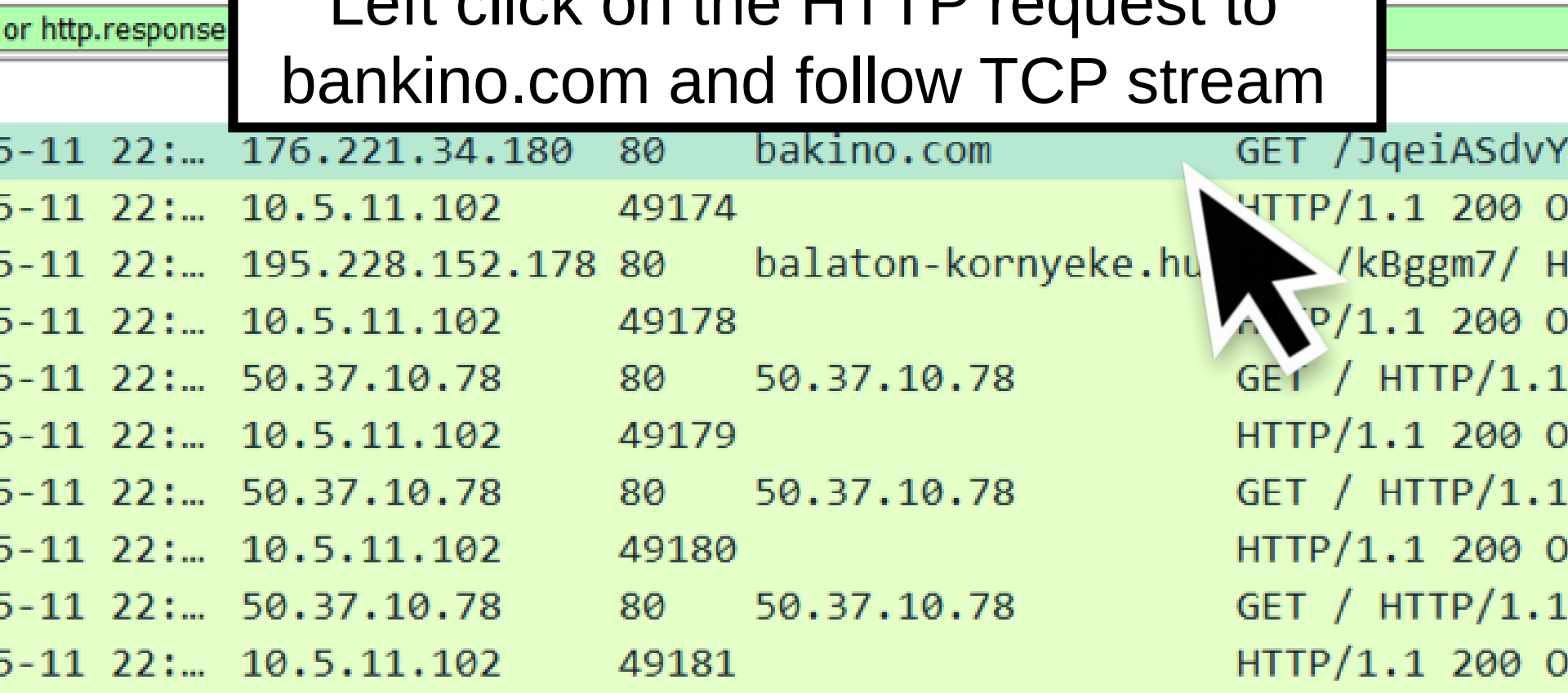
File →
Export Objects
→ HTTP

Windows malware: HTTP traffic



Windows malware: HTTP traffic

Left click on the HTTP request to bankino.com and follow TCP stream

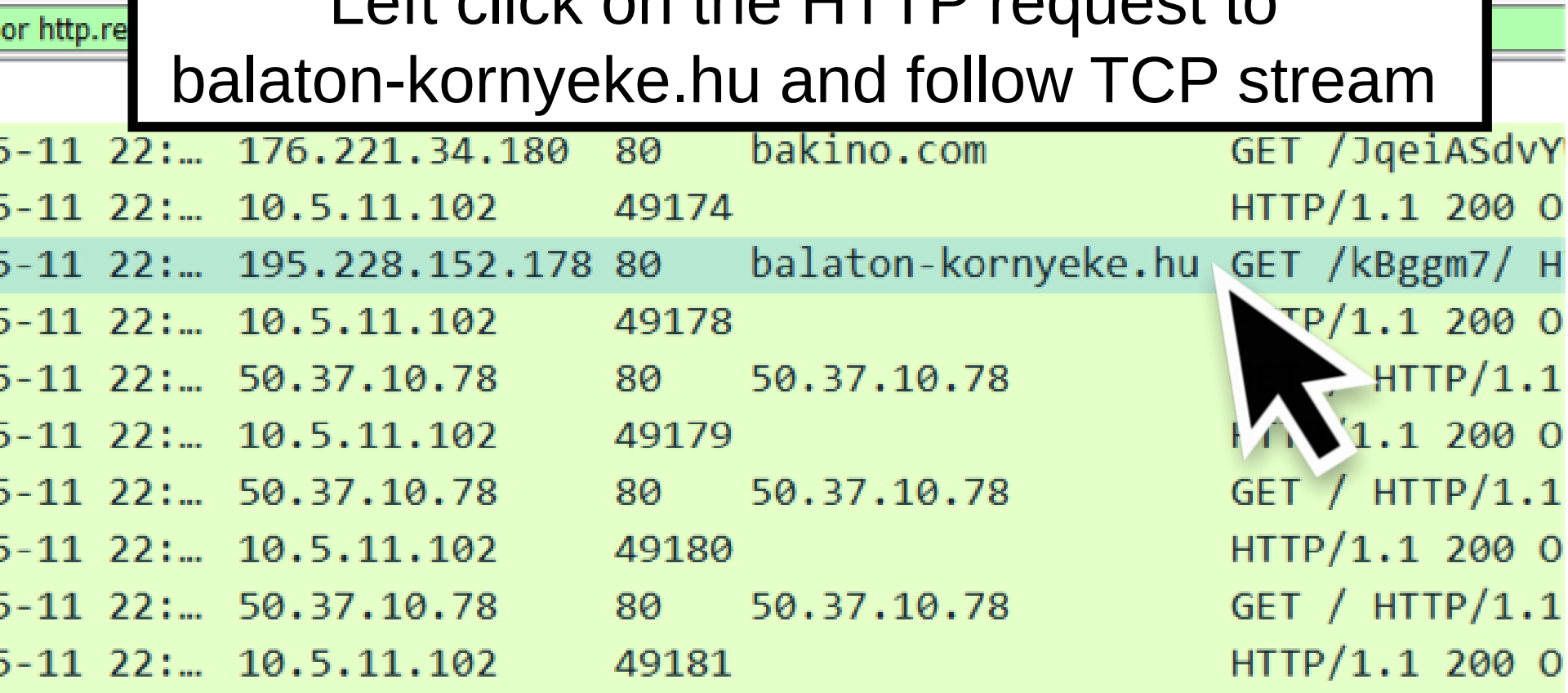


Windows malware: HTTP traffic

```
GET /JqeiASdvYWbNJm/ HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: bakino.com
DNT: 1
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Fri, 11 May 2018 22:26:08 GMT
Server: Apache
Cache-Control: no-cache, no-store, max-age=0, must-revalida
Pragma: no-cache
Content-Disposition: attachment; filename="Invoice #2858742.doc"
Content-Transfer-Encoding: binary
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: application/msword
```

Windows malware: HTTP traffic

Left click on the HTTP request to balaton-kornyeke.hu and follow TCP stream



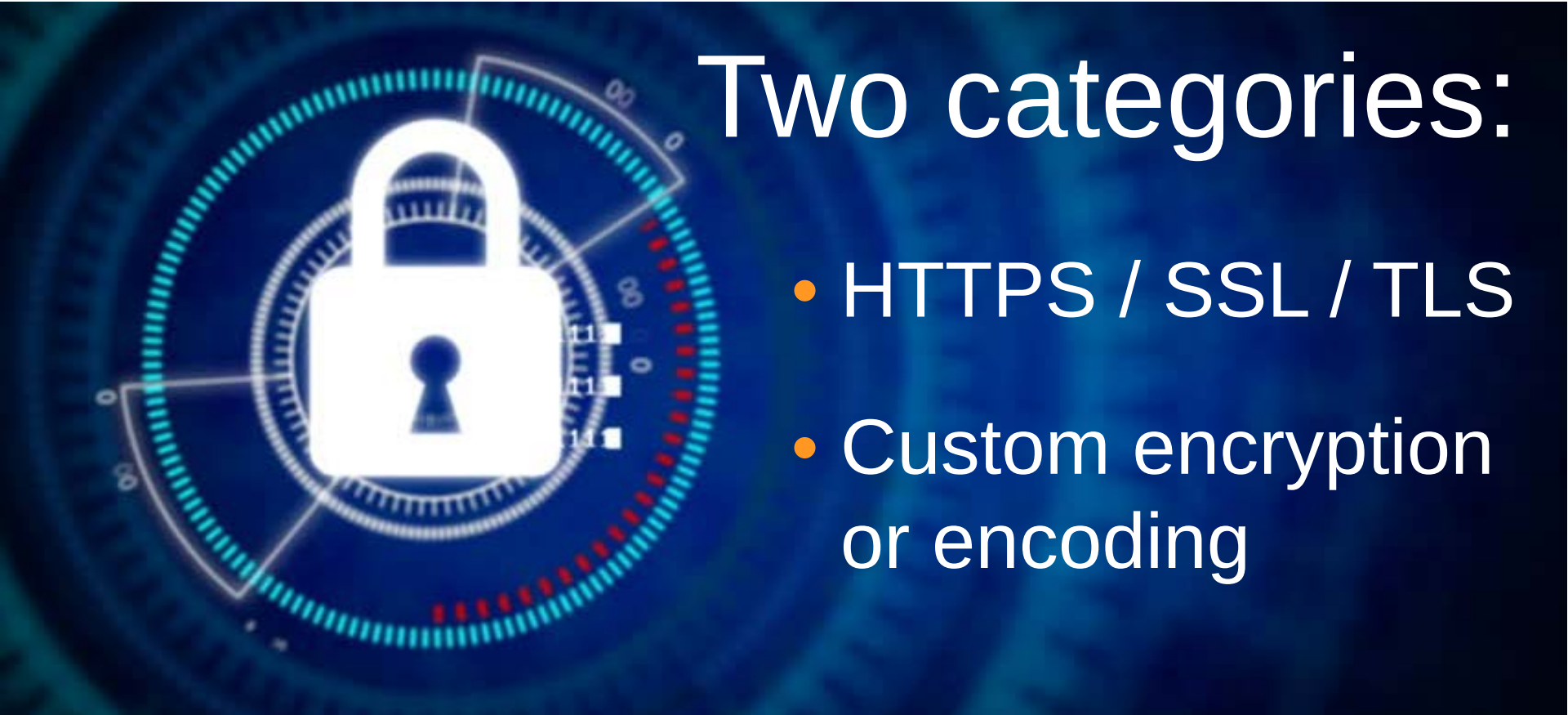
Windows malware: HTTP traffic

```
GET /kBggm7/ HTTP/1.1
Host: balaton-kornyeke.hu
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx
Date: Fri, 11 May 2018 22:26:39 GMT
Content-Type: application/octet-stream
Transfer-Encoding: chunked
Connection: keep-alive
Cache-Control: no-cache, no-store, max-age=0, must-re idate
Pragma: no-cache
Content-Disposition: attachment; filename="2392.exe"
Conten Transfer-Encoding: binary

fec
MZ.....@.....  .!..L.!This
program cannot be run in DOS mode.

$.......Vx.............}.......}
```

Block 3 - Up next...

- Windows malware: HTTP traffic
- **Windows malware: encrypted traffic**
- Windows malware: SMB traffic
- Windows malware: FTP and IRC traffic
- Exercise and bonus pcaps

Windows malware: encrypted traffic

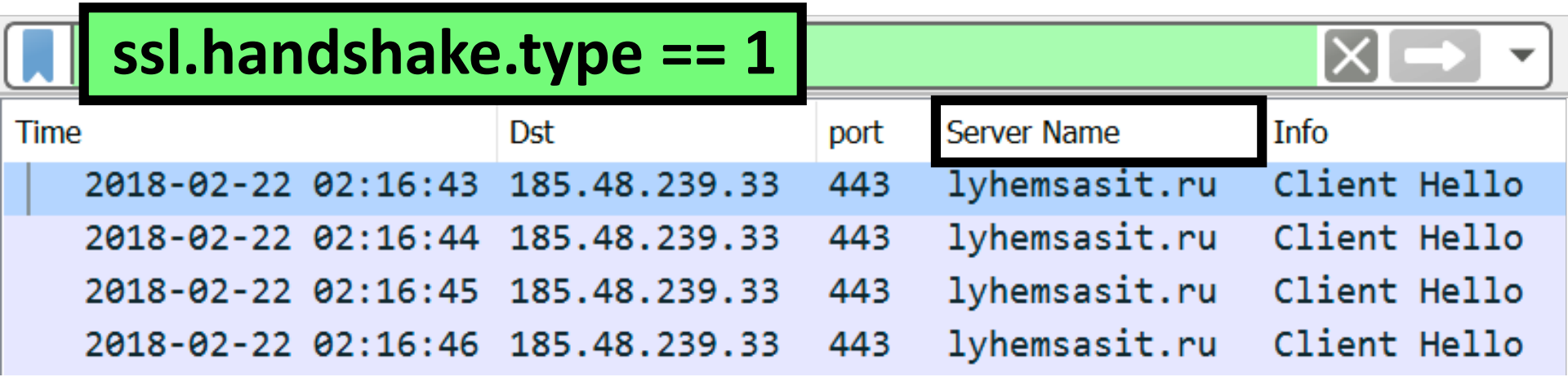


Two categories:

- HTTPS / SSL / TLS
- Custom encryption or encoding

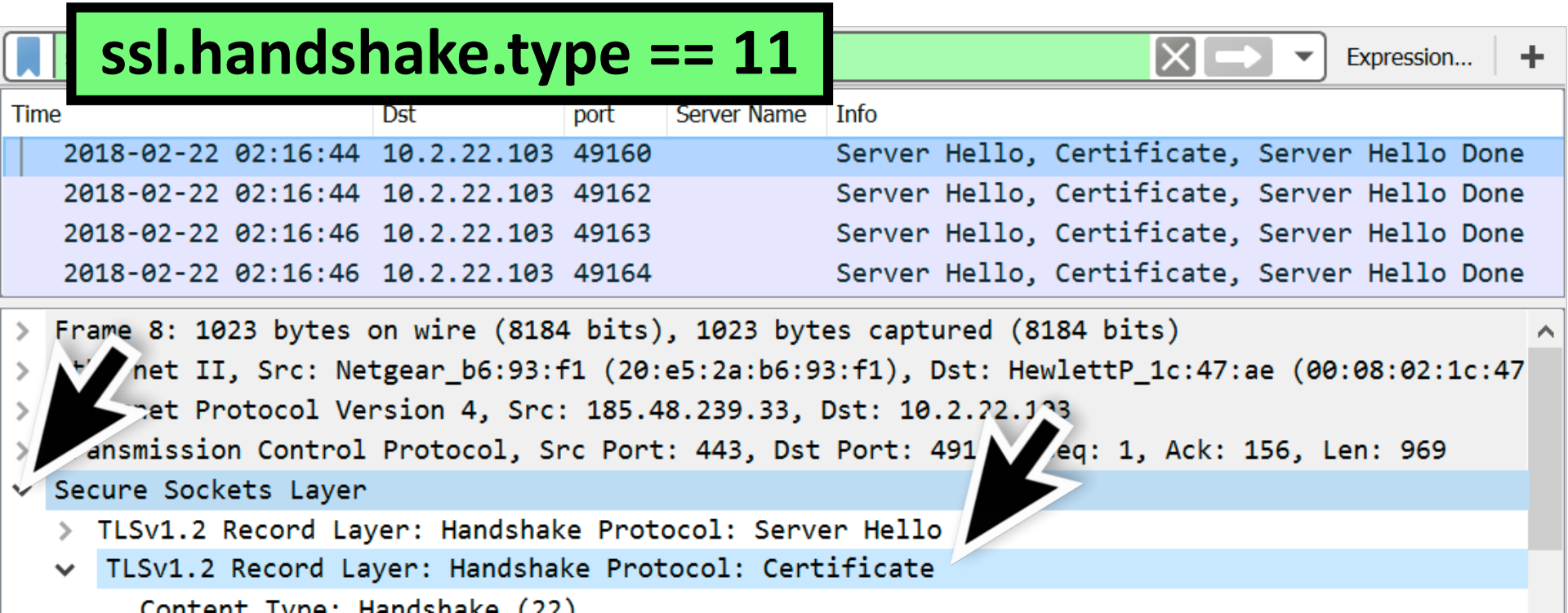
Windows malware: HTTPS traffic

2018-traffic-analysis-workshop-block-3-03.pcap

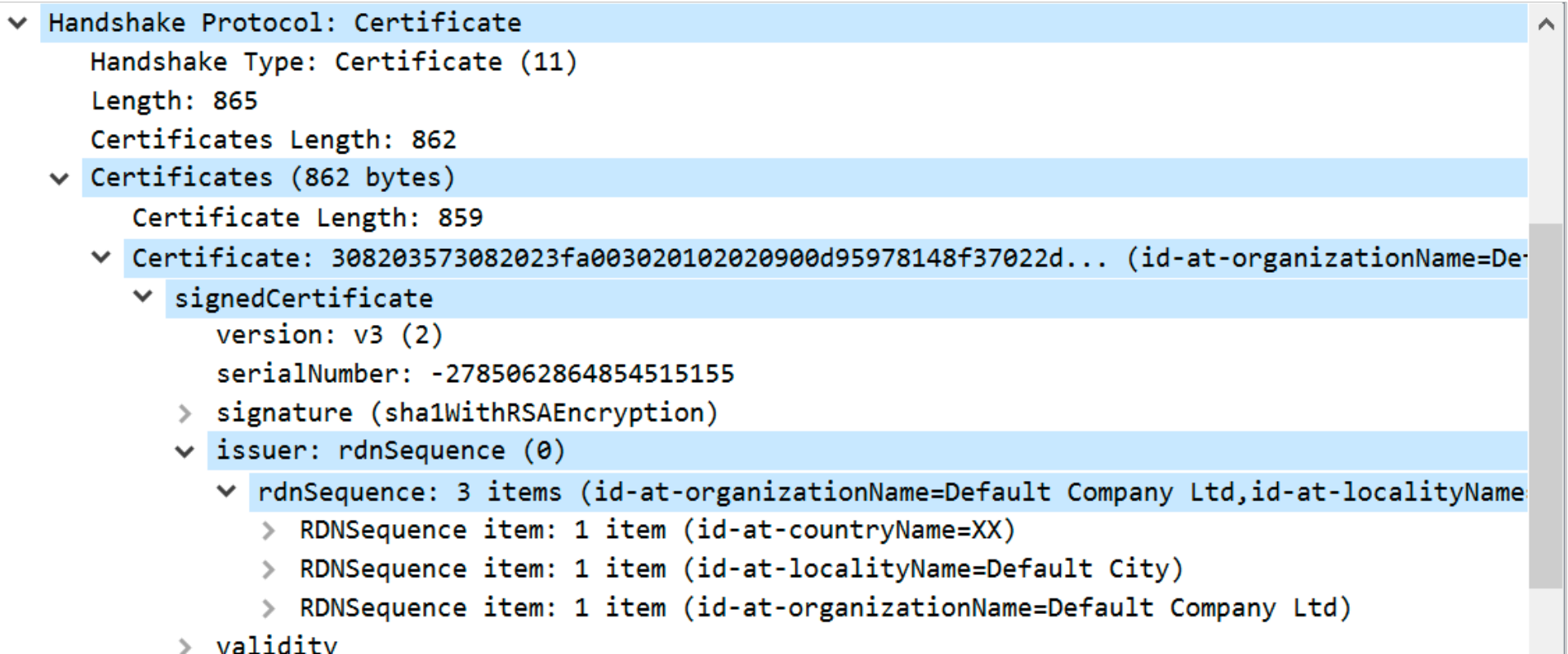


ZEUS PANDA BANKER

Windows malware: HTTPS traffic



Windows malware: encrypted traffic



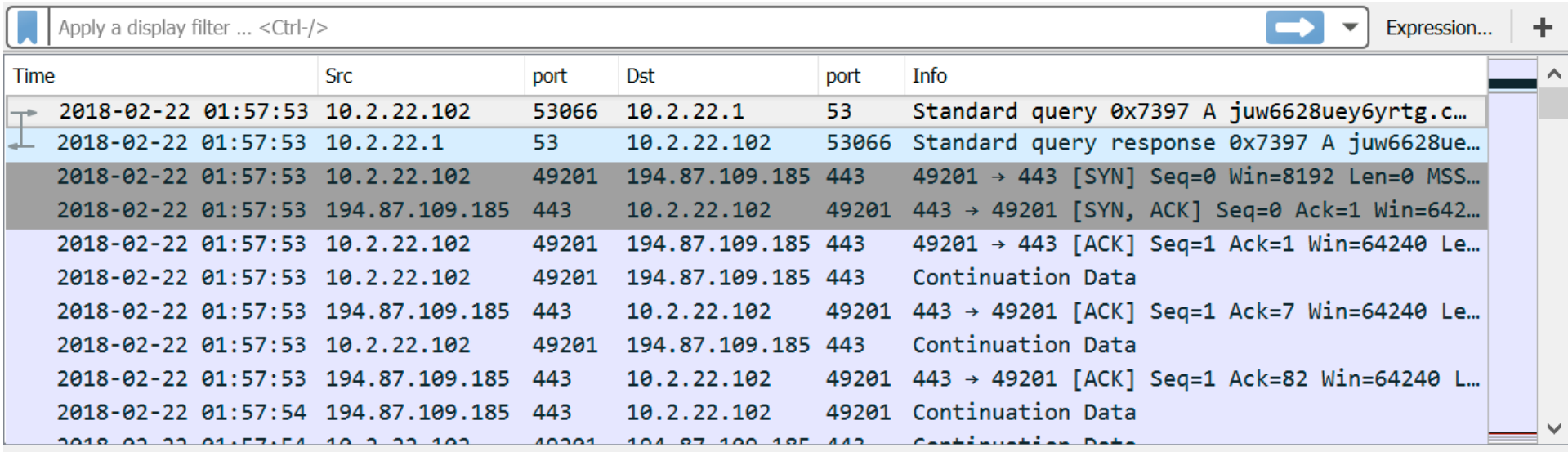
Windows malware: encrypted traffic

rdnSequence items

- (id-at-countryName=XX)
- (id-at-localityName=Default City)
- (id-at-organizationName=Default Company Ltd)

Windows malware: encrypted traffic

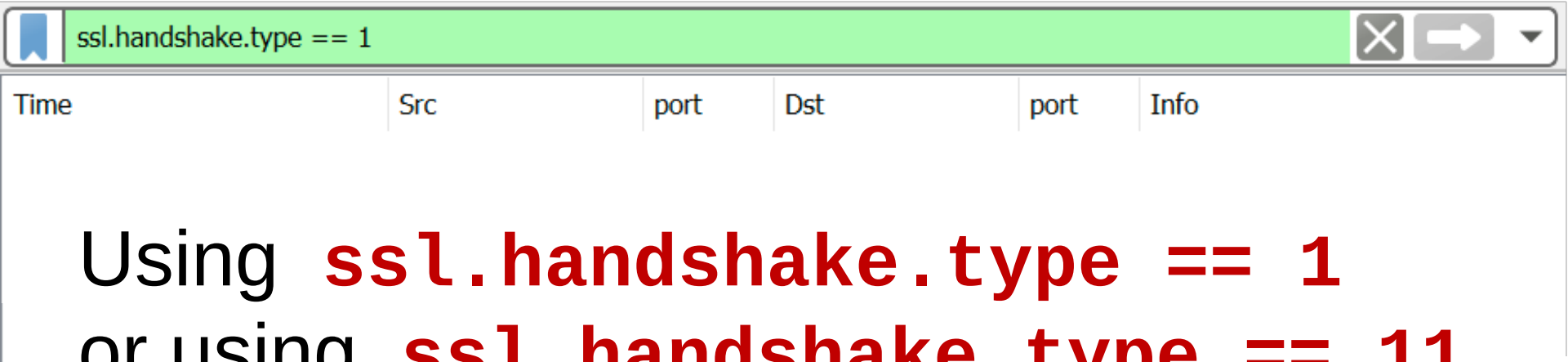
2018-traffic-analysis-workshop-block-3-04.pcap



Time	Src	port	Dst	port	Info
2018-02-22 01:57:53	10.2.22.102	53066	10.2.22.1	53	Standard query 0x7397 A juw6628uey6yrtg.c…
2018-02-22 01:57:53	10.2.22.1	53	10.2.22.102	53066	Standard query response 0x7397 A juw6628ue…
2018-02-22 01:57:53	10.2.22.102	49201	194.87.109.185	443	49201 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS…
2018-02-22 01:57:53	194.87.109.185	443	10.2.22.102	49201	443 → 49201 [SYN, ACK] Seq=0 Ack=1 Win=642…
2018-02-22 01:57:53	10.2.22.102	49201	194.87.109.185	443	49201 → 443 [ACK] Seq=1 Ack=1 Win=64240 Le…
2018-02-22 01:57:53	10.2.22.102	49201	194.87.109.185	443	Continuation Data
2018-02-22 01:57:53	194.87.109.185	443	10.2.22.102	49201	443 → 49201 [ACK] Seq=1 Ack=7 Win=64240 Le…
2018-02-22 01:57:53	10.2.22.102	49201	194.87.109.185	443	Continuation Data
2018-02-22 01:57:53	194.87.109.185	443	10.2.22.102	49201	443 → 49201 [ACK] Seq=1 Ack=82 Win=64240 L…
2018-02-22 01:57:54	194.87.109.185	443	10.2.22.102	49201	Continuation Data

RAMNIT

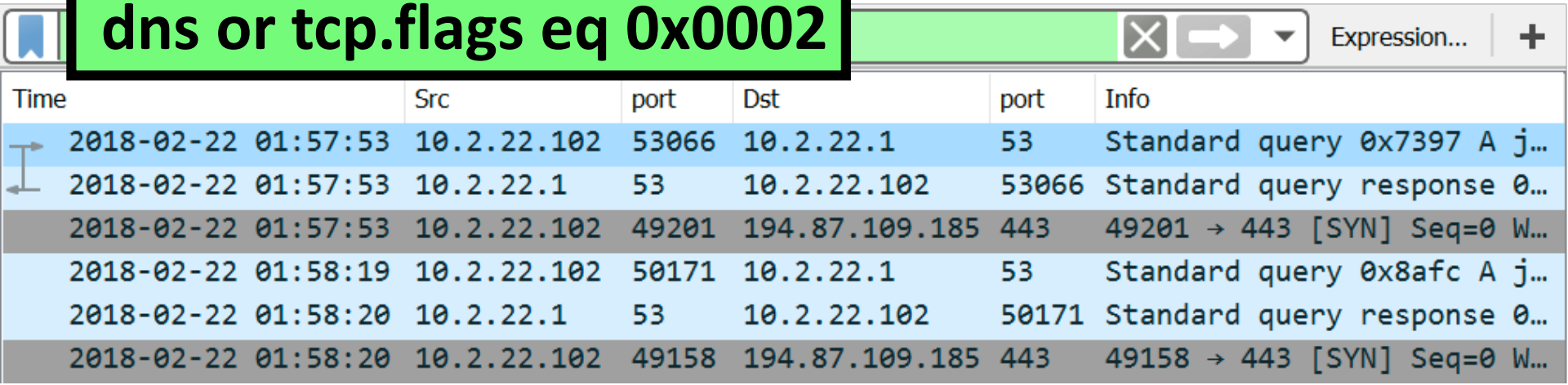
Windows malware: encrypted traffic



Using **`ssl.handshake.type == 1`**
or using **`ssl.handshake.type == 11`**
does not return any results

Windows malware: encrypted traffic

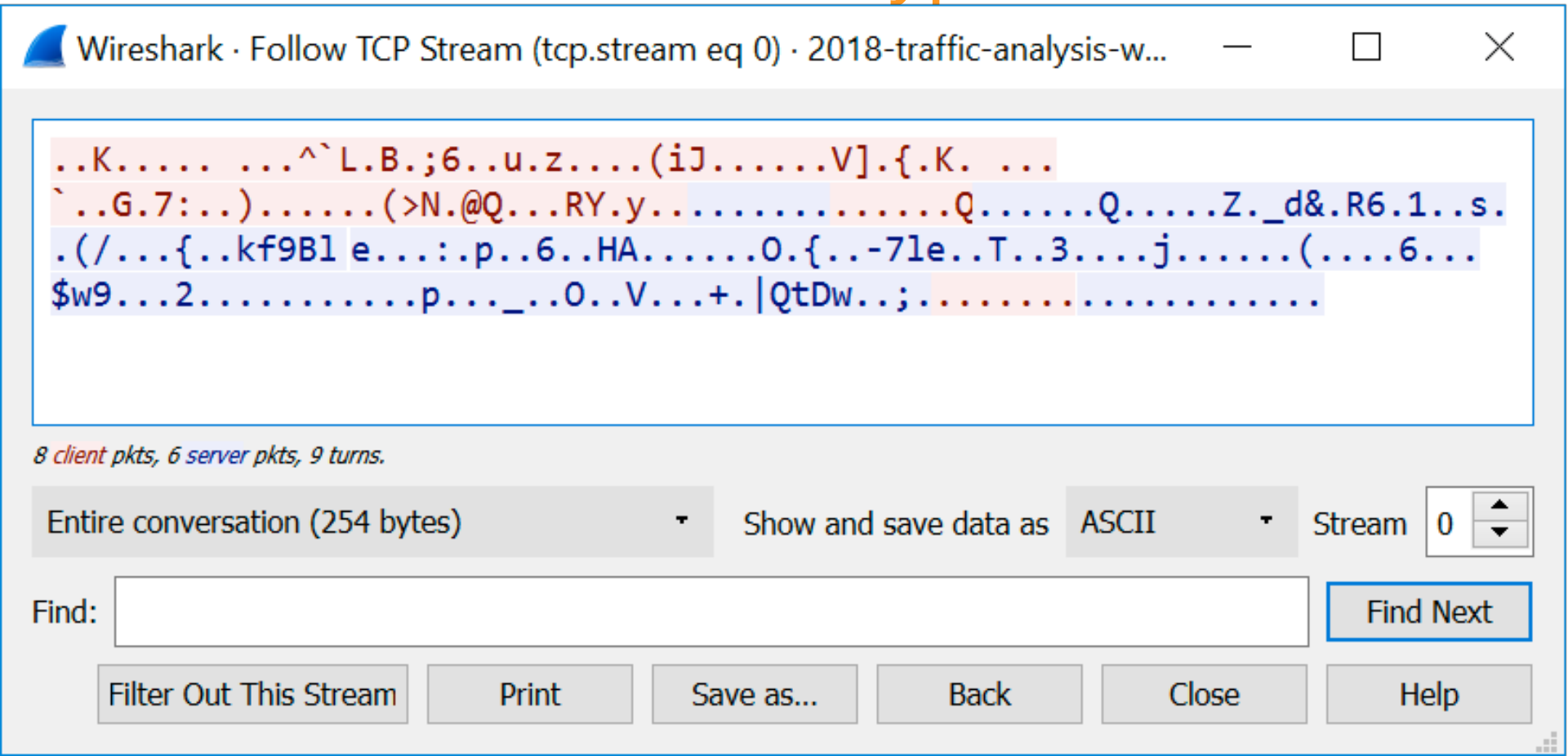
dns or tcp.flags eq 0x0002



Expression...

Time	Src	port	Dst	port	Info
2018-02-22 01:57:53	10.2.22.102	53066	10.2.22.1	53	Standard query 0x7397 A j…
2018-02-22 01:57:53	10.2.22.1	53	10.2.22.102	53066	Standard query response 0…
2018-02-22 01:57:53	10.2.22.102	49201	194.87.109.185	443	49201 → 443 [SYN] Seq=0 W…
2018-02-22 01:58:19	10.2.22.102	50171	10.2.22.1	53	Standard query 0x8afc A j…
2018-02-22 01:58:20	10.2.22.1	53	10.2.22.102	50171	Standard query response 0…
2018-02-22 01:58:20	10.2.22.102	49158	194.87.109.185	443	49158 → 443 [SYN] Seq=0 W…

Windows malware: encrypted traffic



Block 3 - Up next...

- Windows malware: HTTP traffic
- Windows malware: encrypted traffic
- **Windows malware: SMB traffic**
- Windows malware: FTP and IRC traffic
- Exercise and bonus pcaps

Windows malware: SMB traffic

2018-traffic-analysis-workshop-block-3-05.pcap

smb2

Expression...

Time	Dst	port	Info
2018-02-14 16:26:30	10.2.14.101	49158	Negotiate Protocol Response
2018-02-14 16:26:30	185.82.200.46	445	Negotiate Protocol Request
2018-02-14 16:26:30	10.2.14.101	49158	Negotiate Protocol Response
2018-02-14 16:26:30	185.82.200.46	445	Session Setup Request, NTLMSSP_NEGOTIATE
2018-02-14 16:26:30	10.2.14.101	49158	Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRE…
2018-02-14 16:26:30	185.82.200.46	445	Session Setup Request, NTLMSSP_AUTH, User: MOON-DAWG-PC\mdawg
2018-02-14 16:26:30	10.2.14.101	49158	Session Setup Response
2018-02-14 16:26:30	185.82.200.46	445	Tree Connect Request Tree: \\185.82.200.46\IPC$
2018-02-14 16:26:30	10.2.14.101	49158	Tree Connect Response
2018-02-14 16:26:30	185.82.200.46	445	Ioctl Request FSCTL_DFS_GET_REFERRALS, File: \185.82.200.46\k
2018-02-14 16:26:30	10.2.14.101	49158	Ioctl Response, Error: STATUS_NOT_FOUND
2018-02-14 16:26:30	185.82.200.46	445	Tree Connect Request Tree: \\185.82.200.46\k
2018-02-14 16:26:30	10.2.14.101	49158	Tree Connect Response

Windows malware: SMB traffic

```
Session Setup Request, NTLMSSP_AUTH, User: MOON-DAWG-PC\mdawg
Session Setup Response
Tree Connect Request Tree: \\185.82.200.46\IPC$
Tree Connect Response
Ioctl Request FSCTL_DFS_GET_REFERRALS, File: \185.82.200.46\k
Ioctl Response, Error: STATUS_NOT_FOUND
Tree Connect Request Tree: \\185.82.200.46\k
Tree Connect Response
```

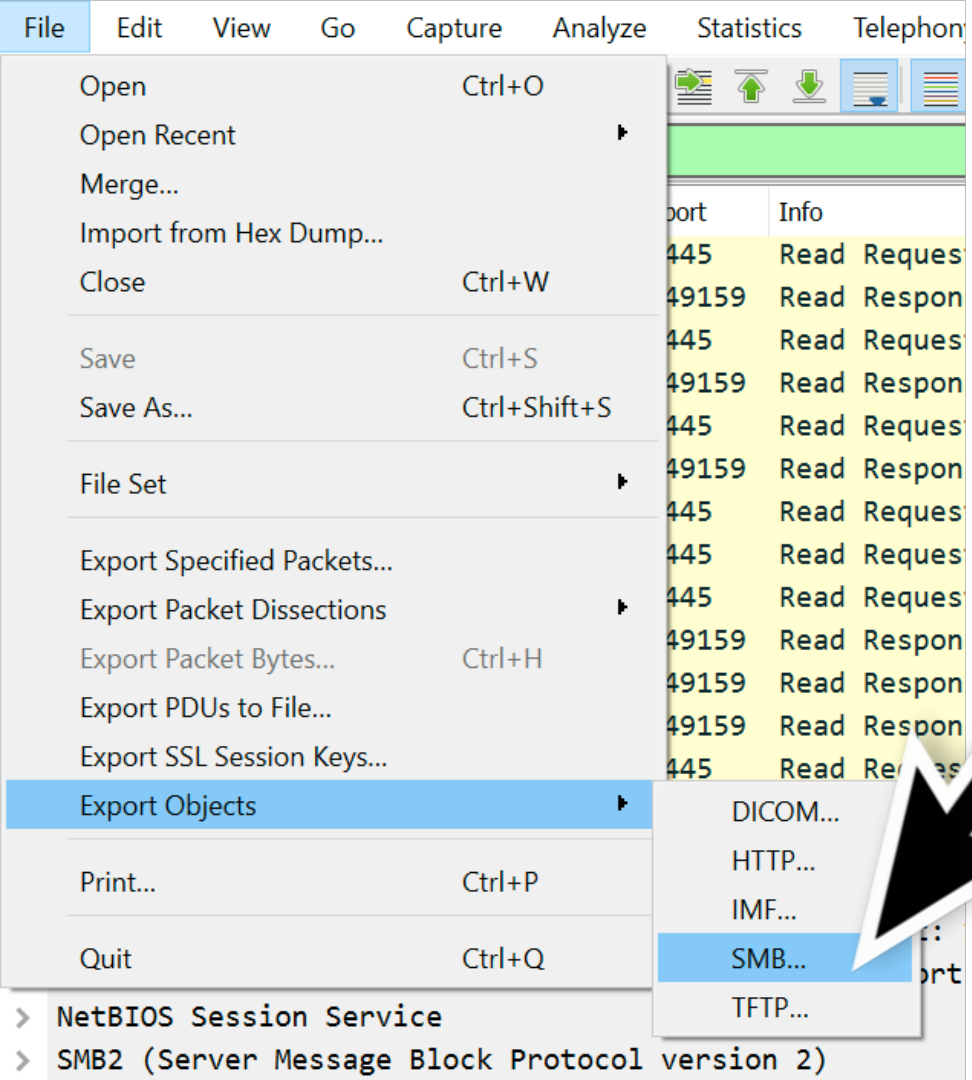
User: MOON-DAWG-PC\mdawg

\\185.82.200.46\k

Windows malware: SMB traffic

```
Create Request File: yu.EXE
Create Response File: yu.EXE
```

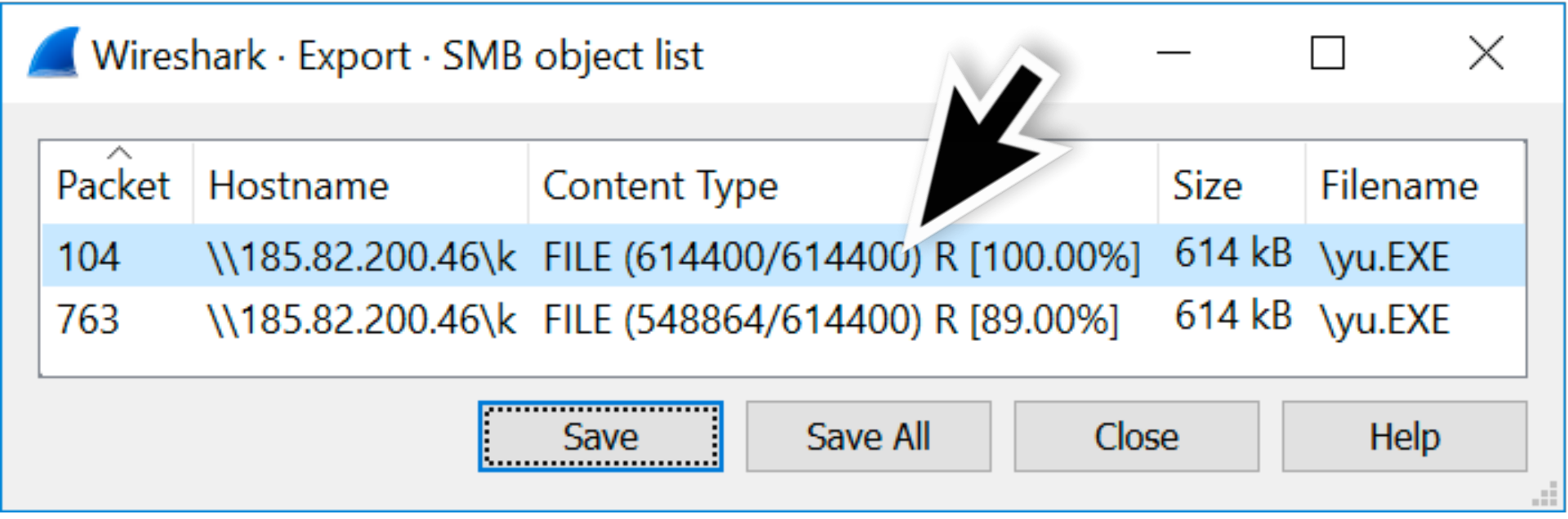
Retrieved **yu.EXE** from **\\185.82.200.46\k**



File →
Export Objects
→ SMB

Windows malware: SMB traffic

Select the entry that shows 100 %



Block 3 - Up next...

- Windows malware: HTTP traffic
- Windows malware: encrypted traffic
- Windows malware: SMB traffic
- **Windows malware: FTP and IRC traffic**
- Exercise and bonus pcaps

Windows malware: FTP and IRC traffic

2018-traffic-analysis-workshop-block-3-06.pcap

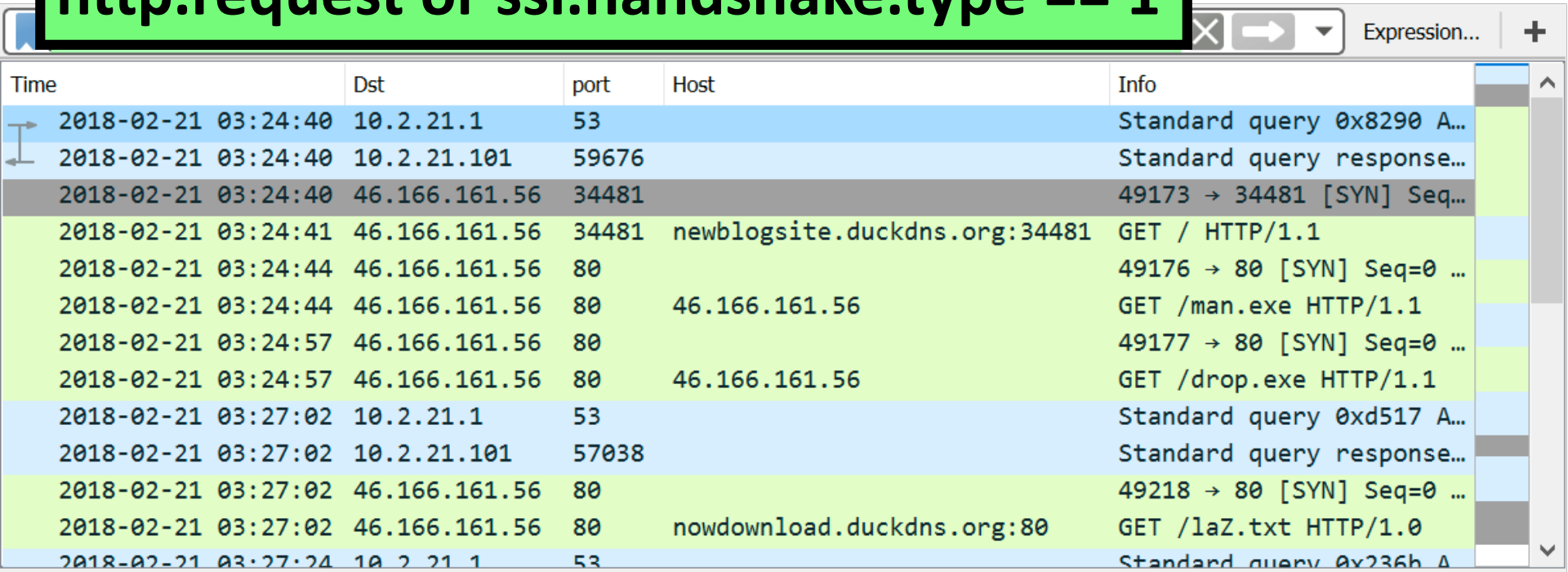
dns or tcp.flags eq 0x0002

Expression...

Tim				
2018-02-21 03:24:40	10.2.21.1	53	Standard query 0x8290 A newblogsite.duckdns.org
2018-02-21 03:24:40	10.2.21.101	59676	Standard query response 0x8290 A newblogsite.duckdns.org A 46.16…
2018-02-21 03:24:40	46.166.161.56	34481	49173 → 34481 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PE…
2018-02-21 03:24:44	46.166.161.56	80	49176 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
2018-02-21 03:24:57	46.166.161.56	80	49177 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
2018-02-21 03:27:02	10.2.21.1	53	Standard query 0xd517 A nowdownload.duckdns.org
2018-02-21 03:27:02	10.2.21.101	57038	Standard query response 0xd517 A nowdownload.duckdns.org A 46.16…
2018-02-21 03:27:02	46.166.161.56	80	49218 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
2018-02-21 03:27:24	10.2.21.1	53	Standard query 0x236b A nowdownload.duckdns.org
2018-02-21 03:27:24	10.2.21.101	54216	Standard query response 0x236b A nowdownload.duckdns.org A 46.16…
2018-02-21 03:27:24	46.166.161.56	80	49219 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
2018-02-21 03:27:25	10.2.21.1	53	Standard query 0xad42 A newcanbernew.duckdns.org
2018-02-21 03:27:25	10.2.21.101	53195	Standard query response 0xad42 A newcanbernew.duckdns.org A 62.1…
2018-02-21 03:27:25	62.102.148.185	25909	49220 → 25909 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PE…
2018-02-21 03:27:26	10.2.21.1	53	Standard query 0xd073 A files.000webhost.com

Windows malware: FTP and IRC traffic

dns or tcp.flags eq 0x0002 or http.request or ssl.handshake.type == 1



Windows malware: FTP and IRC traffic

Dst	port	Host	Info
46.166.161.56	34481		49173 → 34481 [SYN]
46.166.161.56	34481	newblogsite.duckdns.org:34481	GET / HTTP/1.1

- First HTTP request is on a non-standard port (not port 80).
- Instead, it uses TCP port 34481

Windows malware: FTP and IRC traffic

```
GET / HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: newblogsite.duckdns.org:34481
DNT: 1
Connection: Keep-Alive

HTTP/1.1 200 OK
Host: newblogsite.duckdns.org:34481
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 3886

<html>
<head>
    <!-- saved from url=(0014)about:internet -->
    <meta http-equiv="X-UA-Compatible" content="IE=10">
```

It returns a page with VBscript that causes further requests for malware

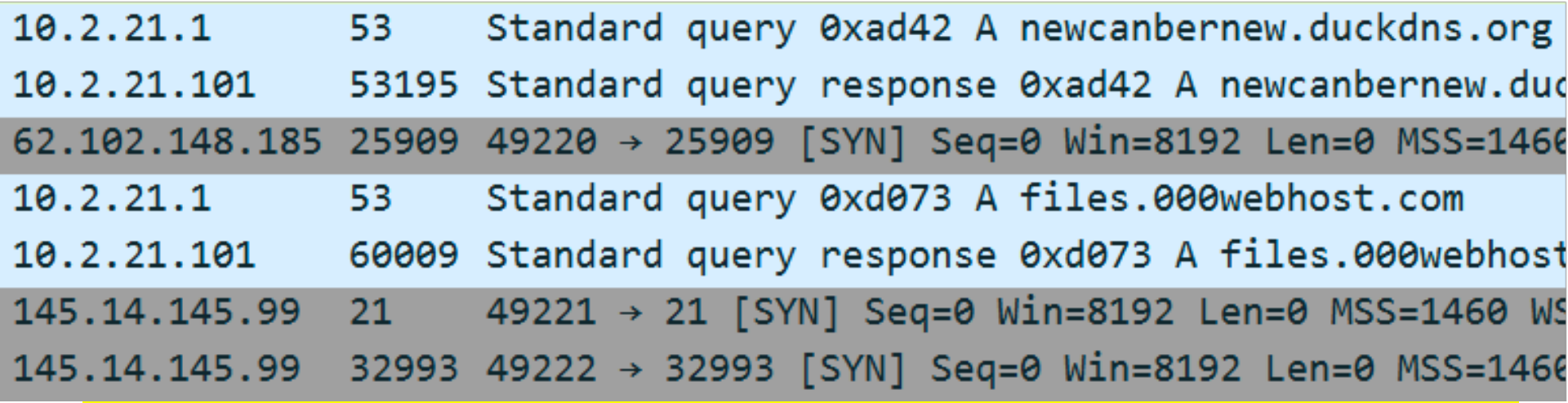
Windows malware: FTP and IRC traffic

dns or tcp.flags eq 0x0002 or
http.request or ssl.handshake.type == 1

Scroll to the bottom

```
10.2.21.1       53    Standard query 0xad42 A newcanbernew.duckdns.org
10.2.21.101     53195 Standard query response 0xad42 A newcanbernew.duc
62.102.148.185  25909 49220 → 25909 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
10.2.21.1       53    Standard query 0xd073 A files.000webhost.com
10.2.21.101     60009 Standard query response 0xd073 A files.000webhost
145.14.145.99   21    49221 → 21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS
145.14.145.99   32993 49222 → 32993 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
```

Windows malware: FTP and IRC traffic



- **newcanbernew.duckdns.org** over TCP port 25909
- FTP traffic to **files.000webhost.com**

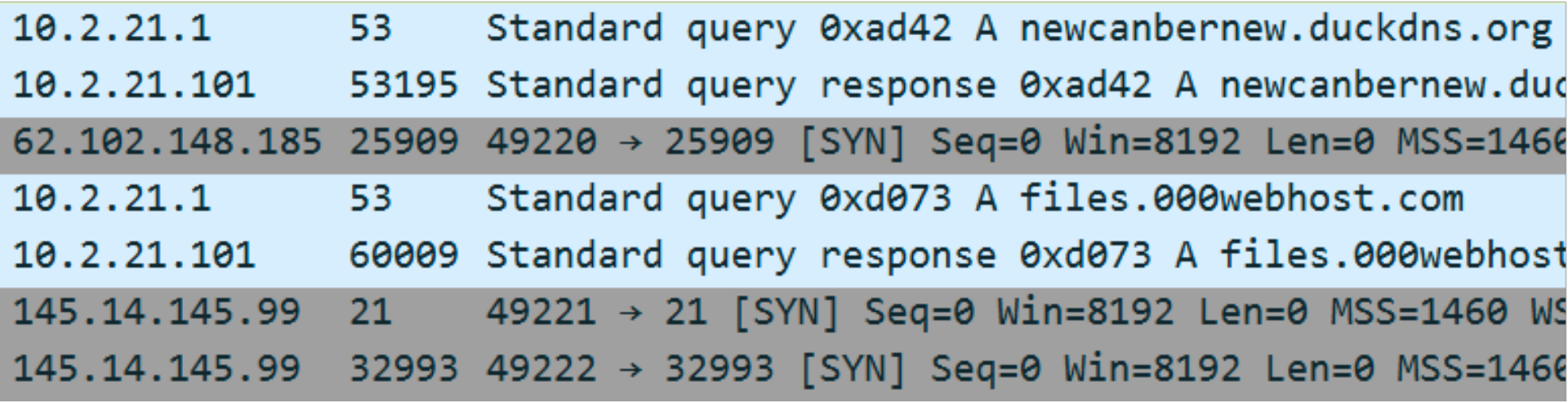
Windows malware: FTP and IRC traffic

Time	Dst	port	Info
2018-02-21 03:27:26	62.102.148.185	25909	49220 → 25909 [PSH, ACK] Seq=107 Ack=6

Wireshark · Follow TCP Stream (tcp.stream eq 5) · 2018-traffic-analysis-worksh...

```
NICK                    bot0221201860452
USER                    Bots 0 * :                    OhOhOh
:irc.foonet.com NOTICE * :*** Looking up your hostname...
PONG :irc.foonet.com NOTICE * :*** Looking up your hostname...
:irc.foonet.com NOTICE * :*** Couldn't resolve your hostname; using your
IP address instead
PING :BBBECE11
PONG :irc.foonet.com NOTICE * :*** Couldn't resolve your hostname; using
your IP address instead
PING :BBBECE11
:BBBECE11!nospoof@irc.foonet.com PRIVMSG bot0221201860452 :.VERSION.
PONG :BBBECE11!nospoof@irc.foonet.com PRIVMSG bot0221201860452 :.VERSION.
```

Windows malware: FTP and IRC traffic



```
10.2.21.1       53    Standard query 0xad42 A newcanbernew.duckdns.org
10.2.21.101     53195 Standard query response 0xad42 A newcanbernew.duc
62.102.148.185  25909 49220 → 25909 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
10.2.21.1       53    Standard query 0xd073 A files.000webhost.com
10.2.21.101     60009 Standard query response 0xd073 A files.000webhost
145.14.145.99   21    49221 → 21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS
145.14.145.99   32993 49222 → 32993 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
```

- **newcanbernew.duckdns.org** over TCP port 25909
- FTP traffic to **files.000webhost.com**

Windows malware: FTP and IRC traffic

FTP traffic

- **TCP port 21** - control channel
- **Ephemeral TCP port** - data channel

```
145.14.145.99   21
145.14.145.99   32993
```

Windows malware: FTP and IRC traffic

Time	Dst	port	Info
2018-02-21 03:27:26	145.14.145.99	21	49221 → 21 [ACK] Seq=1 Ack=1 Win=64240

Wireshark · Follow TCP Stream (tcp.stream eq 6) · 2018-traffic-analysis-worksh...

```
220 ProFTPD Server (000webhost.com) [::ffff:145.14.145.99]
USER seomarketiing
331 User seomarketiing OK. Password required
PASS 123456789Aa**
230-Your bandwidth usage is restricted
230 OK. Current restricted directory is /
TYPE I
200 TYPE is now 8-bit binary
PASV
227 Entering Passive Mode (145,14,145,99,128,225).
STOR /public_html/bot0221201860452.txt
150 Connecting to port 52303
```

Windows malware: FTP and IRC traffic

Time	Dst	port	Info
2018-02-21 03:27:27	145.14.145.99	32993	FTP Data: 99 bytes

Wireshark · Follow TCP Stream (tcp.stream eq 7) · 2018-traffic-analy...

```
##################  User: simon.bennett ##################
No passwords found for this user !
```

3 client pkts, 4 server pkts, 3 turns.

Entire conversation (99 bytes) | Show and save data as ASCII | Stream 7

Windows malware: FTP and IRC traffic

What did the malware do?

- Used IRC for botnet command & control
- Sent any passwords it found to an FTP server

Block 3 - review

- Windows malware: HTTP traffic
- Windows malware: encrypted traffic
- Windows malware: SMB traffic
- Windows malware: FTP and IRC traffic
- Exercise and 3 bonus pcaps

2018 TRAFFIC ANALYSIS WORKSHOP

Up next...

Block 4: Bad web traffic

Block 4 - Overview

- Phishing pages
- Tech support scams
- Pop-ups/unexpected web pages
- Exploit kits
- Hands-on exercises

Phishing pages

- Criminals compromise legitimate websites and set up new directories with fake pages to steal a victim's login credentials.
- Links to these sites are sent to potential victims through phishing emails.

Phishing pages

Subject: DOCUMENT

From: Laxmi Ghale <laxmighale@siddharthservices.com>

Date: Wed, 2018-03-14 16:03 UTC

Good day,

Laxmi Ghale Office has shared a Docusign file with you. To view it, click the link below.

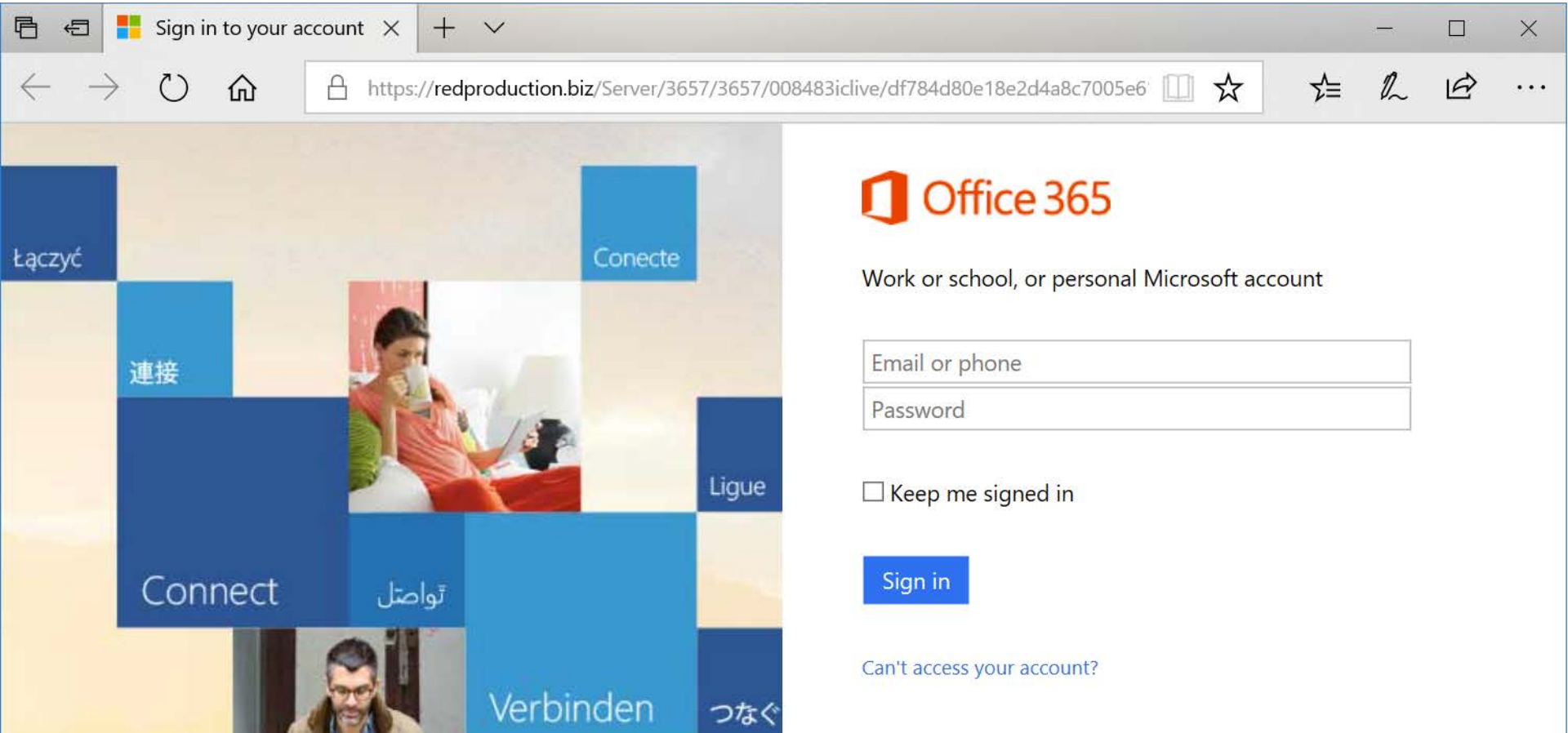
REVIEW DOCUMENT

Please let me know if you have any c

Thanks & Regards
Laxmi Ghale

https://redproduction.biz/Server/3657/3657/008483iclive/df784d80e18e2d4a8c7005e61fde6dce/

Phishing pages



Phishing pages

2018-traffic-analysis-workshop-block-4-01.pcap

http.request

Expression...

Time	Dst	port	Host	Info
2018-03-14 21:01:12	23.229.153.228	80	abcontracting.us	GET /Gn/ HTTP/1.1
2018-03-14 21:01:12	23.229.153.228	80	abcontracting.us	GET /Gn/Office%20365_files/Gem…
2018-03-14 21:01:12	23.229.153.228	80	abcontracting.us	GET /Gn/icc.ico HTTP/1.1
2018-03-14 21:01:12	23.229.153.228	80	abcontracting.us	GET /Gn/Office%20365_files/con…
2018-03-14 21:01:12	23.229.153.228	80	abcontracting.us	GET /Gn/Office%20365_files/App…
2018-03-14 21:01:12	23.229.153.228	80	abcontracting.us	GET /Gn/Office%20365_files/Emb…
2018-03-14 21:01:12	23.229.153.228	80	abcontracting.us	GET /Gn/Office%20365_files/Mas…
2018-03-14 21:01:12	23.229.153.228	80	abcontracting.us	GET /Gn/Office%20365_files/Mas…
2018-03-14 21:01:12	23.229.153.228	80	abcontracting.us	GET /Gn/Office%20365_files/she…
2018-03-14 21:01:12	23.229.153.228	80	abcontracting.us	GET /Gn/Office%20365_files/she…
2018-03-14 21:01:12	23.229.153.228	80	abcontracting.us	GET /Gn/Office%20365_files/dat…
2018-03-14 21:01:12	23.229.153.228	80	abcontracting.us	GET /Gn/Office%20365_files/she…

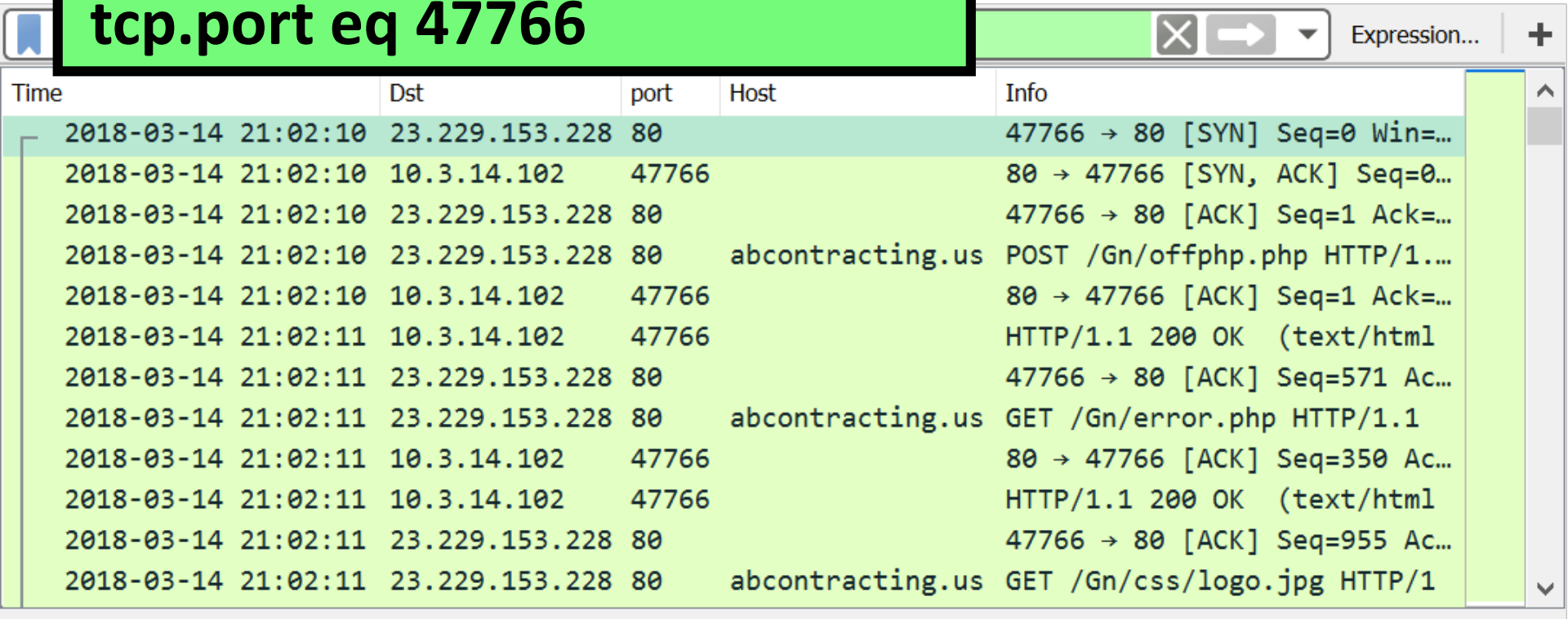
Phishing pages

Src IP	SPort	Dst IP	DPort	Pr
23.229.153.228	80	10.3.14.102	47718	6
10.3.14.102	47766	23.229.153.228	80	6
10.3.14.102	47766	23.229.153.228	80	6

Event Message
ET CURRENT_EVENTS Possible Docusign Phishing Landing
ETPRO CURRENT_EVENTS Successful Docusign/O365 Phish
ET POLICY Http Client Body contains password= in cleartext

Phishing pages

ip.addr eq 23.229.153.228 and tcp.port eq 47766



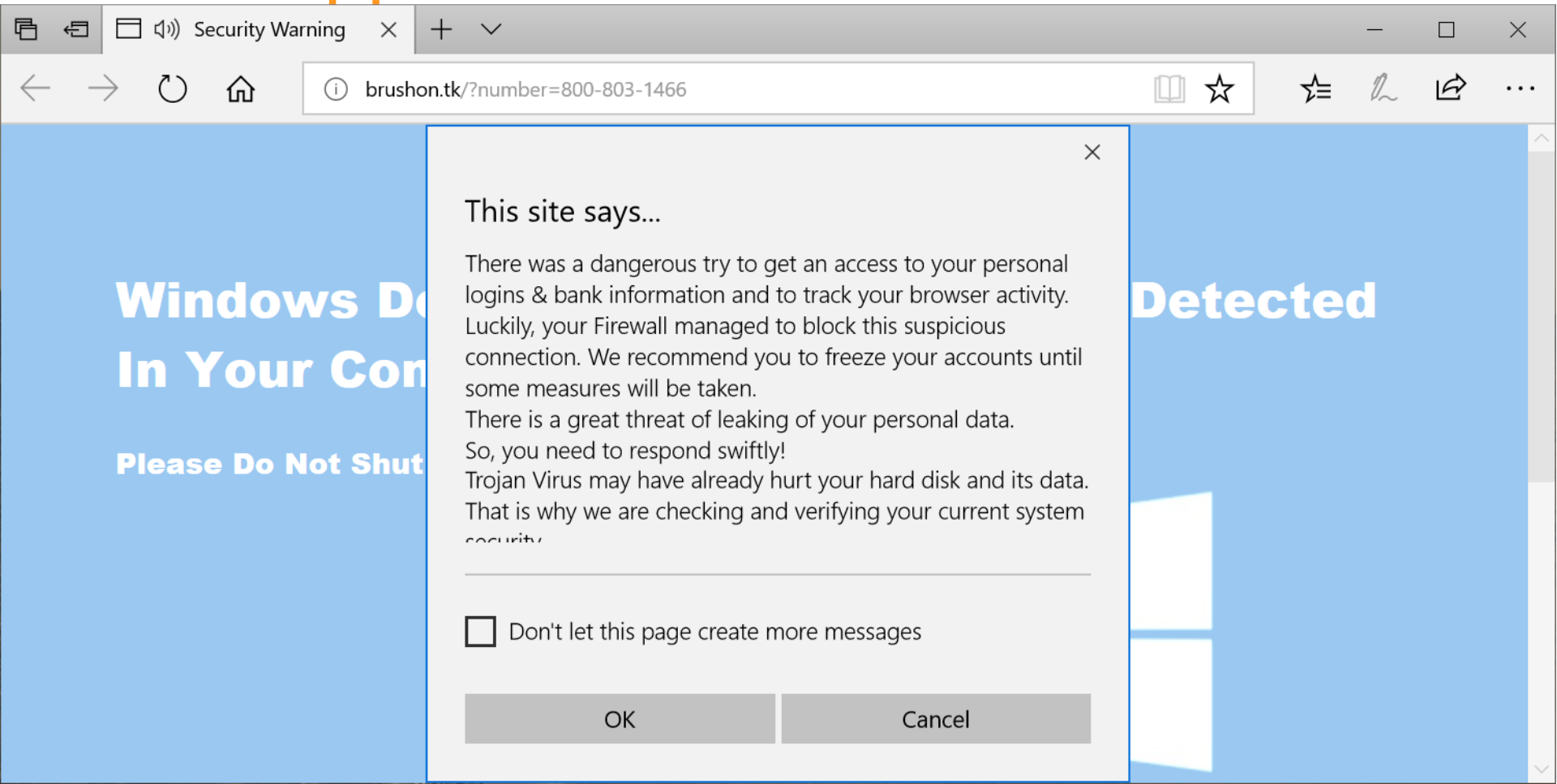
Phishing pages

```
POST /Gn/offphp.php HTTP/1.1
Host: abcontracting.us
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://abcontracting.us/Gn/office.php
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 114

UserName=dean.mcmillian%40tenderloin-
wareshouse.com&Password=tenderloinahoy12345%24&AuthMethod=FormsAuthenticationHTTP/
1.1 200 OK
Date: Wed, 14 Mar 2018 21:02:10 GMT
```

Block 4 - Up next...

- Phishing pages
- **Tech support scams**
- Pop-ups/unexpected web pages
- Exploit kits
- Hands-on exercises

Tech support scams



Tech support scams

2018-traffic-analysis-workshop-block-4-02.pcap

http.request

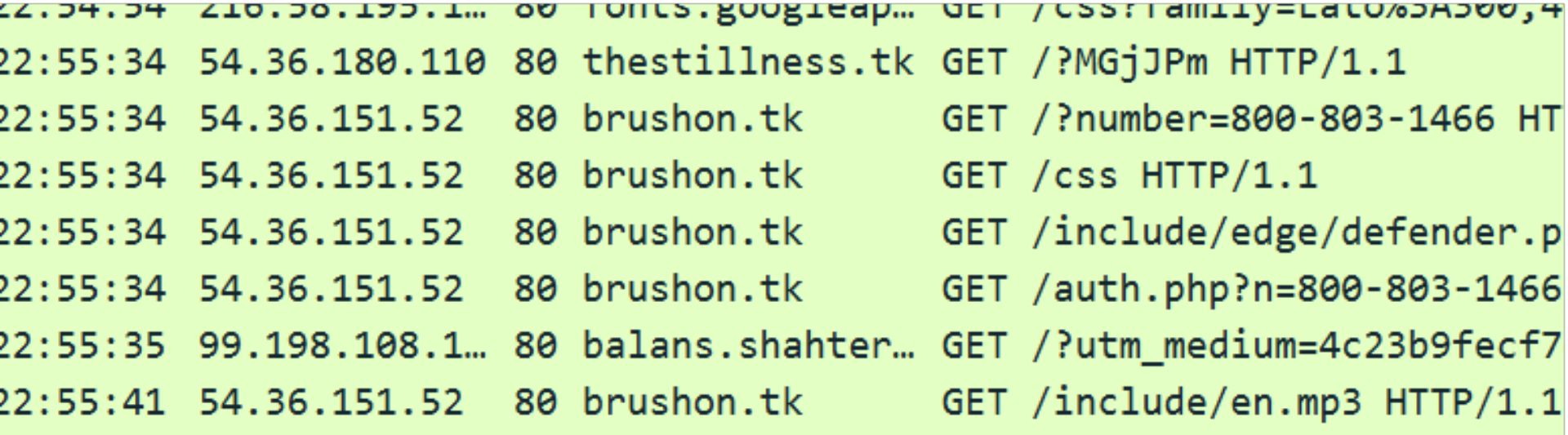
Expression...

Time	Dst	port	Host	Info
2018-03-14 22:54:07	123.100.241.176	80	www.b9dental.com	GET / HTTP/1.1
2018-03-14 22:54:09	123.100.241.176	80	www.b9dental.com	GET /wp-content/the…
2018-03-14 22:54:09	216.58.195.138	80	fonts.googleapi…	GET /css?family=Lat…
2018-03-14 22:54:09	123.100.241.176	80	www.b9dental.com	GET /wp-content/the…
2018-03-14 22:54:09	123.100.241.176	80	www.b9dental.com	GET /wp-content/plu…
2018-03-14 22:54:09	123.100.241.176	80	www.b9dental.com	GET /wp-content/the…
2018-03-14 22:54:09	123.100.241.176	80	www.b9dental.com	GET /wp-content/the…
2018-03-14 22:54:09	123.100.241.176	80	www.b9dental.com	GET /wp-content/plu…
2018-03-14 22:54:09	123.100.241.176	80	www.b9dental.com	GET /wp-content/the…
2018-03-14 22:54:09	123.100.241.176	80	www.b9dental.com	GET /wp-content/the…
2018-03-14 22:54:09	123.100.241.176	80	www.b9dental.com	GET /wp-includes/js…
2018-03-14 22:54:09	123.100.241.176	80	b9dental.com	GET /wp-content/upl…

Tech support scams

Scroll to the bottom, where you'll find:

- brushon.tk - GET /?number=800-803-1466

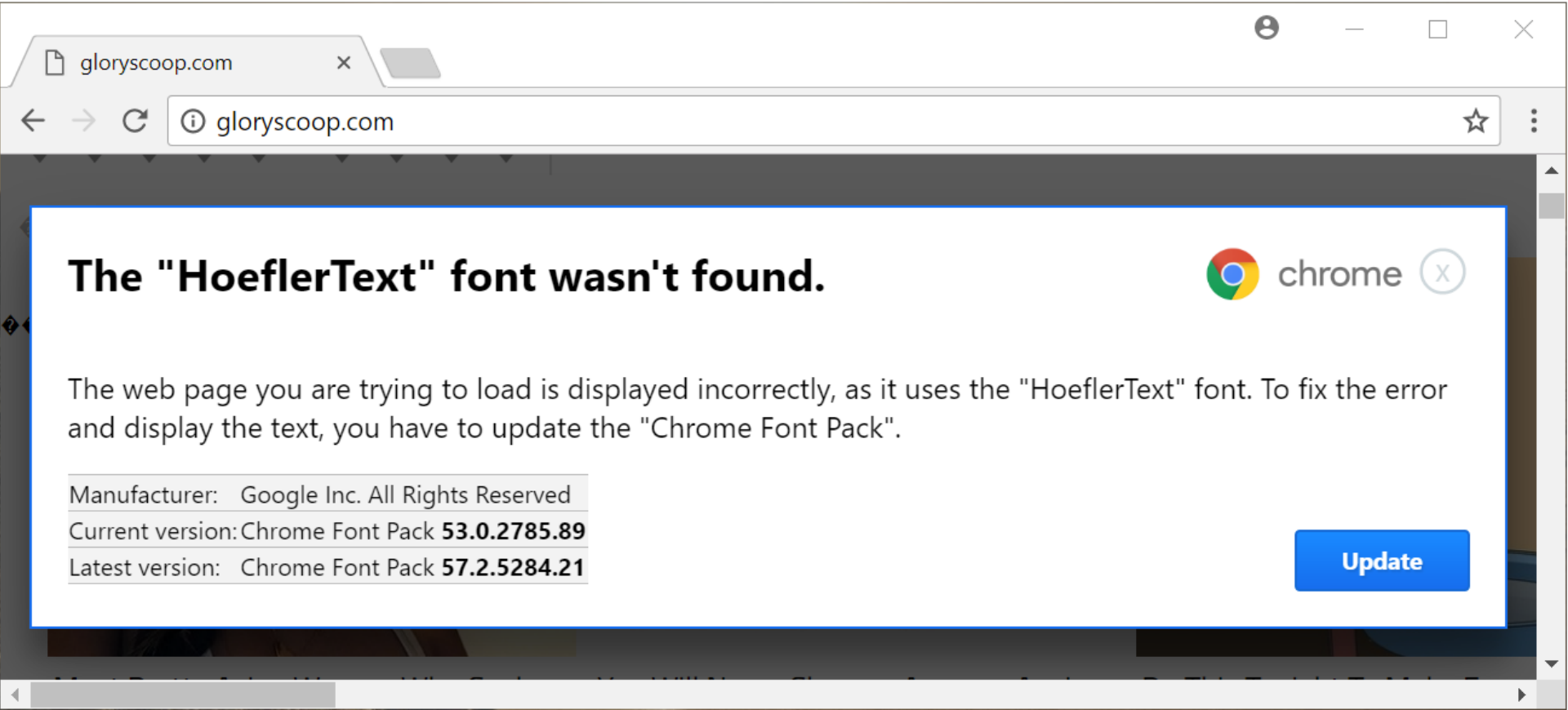


```
189f
<!DOCTYPE html>
<html>
<head>
                <meta http-equiv="Content-Type" content="text/html; charset=UTF-8"><meta
charset="utf-8">
                                <title>Security Warning</title>
                                <meta content="width=device-width, initial-scale=1.0, user-
scalable=1" name="viewport">
                                <meta name="robots" content="noindex, nofollow">
<script type="text/javascript">

                var leysti = "There was a dangerous try to get an access to your personal
logins & bank information and to track your browser activity.\nLuckily, your Firewall
managed to block this suspicious connection. We recommend you to freeze your accounts
until some measures will be taken.\nThere is a great threat of leaking of your personal
data.\nSo, you need to respond swiftly!\nTrojan Virus may have already hurt your hard
disk and its data.\nThat is why we are checking and verifying your current system
security.\nDo not waste your time and consult one of our service centers or call us.
\n----------------------------------------------------\nContact Number: 800-803-1466
```

Block 4 - Up next...

- Phishing pages
- Tech support scams
- **Pop-ups/unexpected web pages**
- Exploit kits
- Hands-on exercises

Popups/unexpected web pages



Popups/unexpected web pages

This type of file can harm your computer. Do you want to keep **Font update.exe** anyway?

Th eflerText" font wasn't found.

chrome

Ste bottom left corner of the screen you'll see the download bar. **Click on the Chrome_Font.exe** iter

(Run) in order to see the correct content on the web page.

javascript:void(0)

This type of file can harm your computer. Do you want to keep Font update.exe anyway?

Keep

Discard

Show all

Popups/unexpected web pages

2018-traffic-analysis-workshop-block-4-03.pcap

http.request or ssl.handshake.type == 1

Expression... +

Time	Dst	port	Host	Server Name	Info
2018-03-14 23:41:21	107.181.172.1…	80	gloryscoop.com		GET / HTTP/1.1
2018-03-14 23:41:23	107.181.172.1…	80	gloryscoop.com		GET /wp-conten…
2018-03-14 23:41:23	107.181.172.1…	80	gloryscoop.com		GET /wp-conten…
2018-03-14 23:41:23	107.181.172.1…	80	gloryscoop.com		GET /wp-conten…
2018-03-14 23:41:23	216.58.216.106	80	fonts.googleapi…		GET /css?famil…
2018-03-14 23:41:23	94.31.29.16	80	maxcdn.bootstra…		GET /font-awes…
2018-03-14 23:41:23	107.181.172.1…	80	gloryscoop.com		GET /wp-includ…
2018-03-14 23:41:23	107.181.172.1…	80	gloryscoop.com		GET /wp-conten…
2018-03-14 23:41:23	107.181.172.1…	80	gloryscoop.com		GET /wp-conten…
2018-03-14 23:41:23	107.181.172.1…	80	gloryscoop.com		GET /wp-conten…
2018-03-14 23:41:23	107.181.172.1…	80	gloryscoop.com		GET /wp-conten…

Popups/unexpected web pages

ip contains "Font update.exe"

Time	Src	port	Dst	port	Info
2018-03-14 23:42:17	185.38.45.99	80	10.3.14.105	50982	80 → 50982 [PSH, ACK

ip contains "This program cannot be run in DOS mode"

Time	Src	port	Dst	port	Info
2018-03-14 23:42:17	185.38.45.99	80	10.3.14.105	50982	80 → 50982 [PSH, ACK

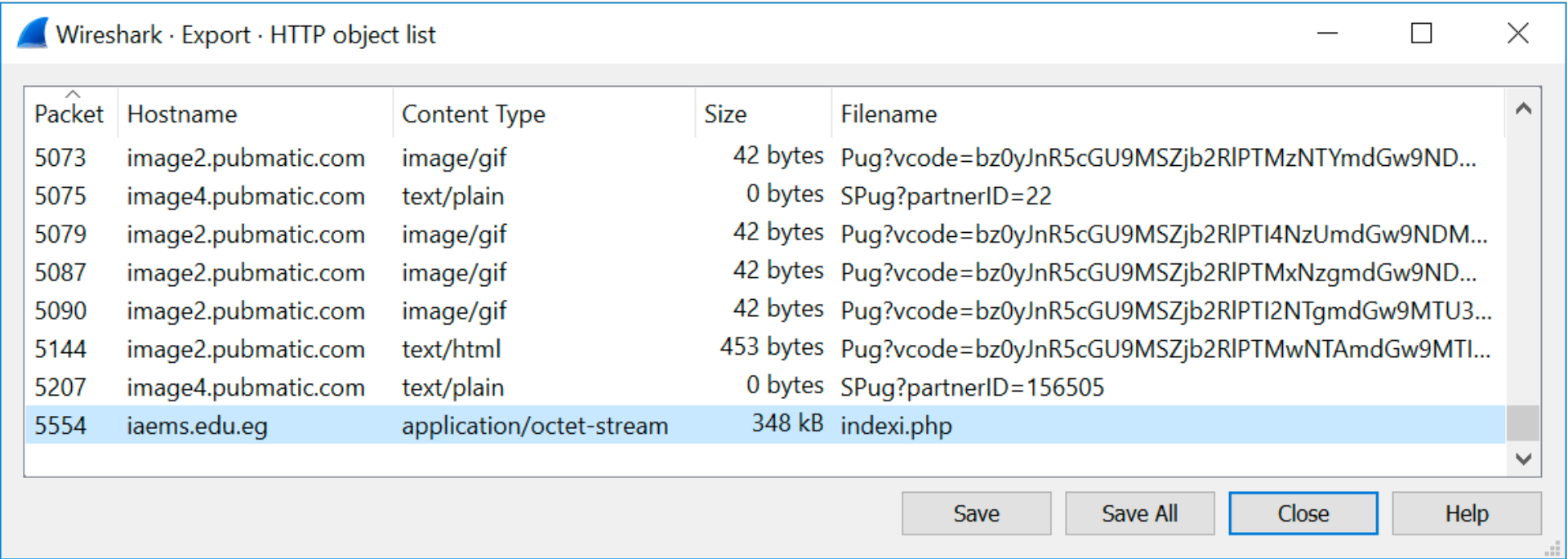
Wireshark · Follow TCP Stream (tcp.stream eq 239) · 2018-traffic-analysis-workshop-block-4-03.pcap

```
GET /indexi.php HTTP/1.1
Host: iaems.edu.eg
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/65.0.3325.162 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://gloryscoop.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200 OK
Content-Type: application/octet-stream
Accept-Ranges: bytes
Content-Disposition: attachment; filename=Font update.exe
Content-Length: 348182
Date: Wed, 14 Mar 2018 23:42:14 GMT
Server: LiteSpeed
Connection: Keep-Alive

MZ.....@.....  .!..L.!This program
cannot be run in DOS mode.
```

3 client pkts, 125 server pkts, 3 turns.

Popups/unexpected web pages

- File → Export Object → HTTP...



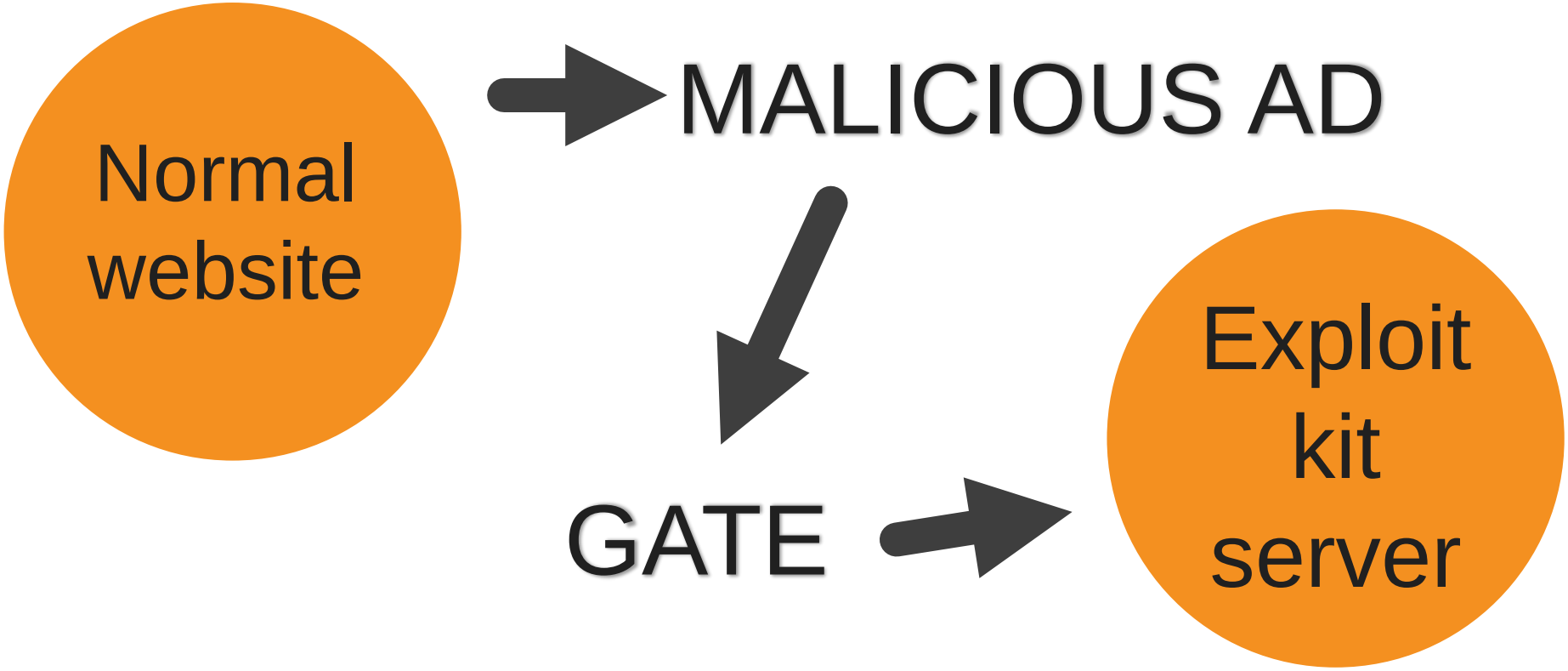
Block 4 - Up next...

- Phishing pages
- Tech support scams
- Pop-ups/unexpected web pages
- **Exploit kits**
- Hands-on exercises

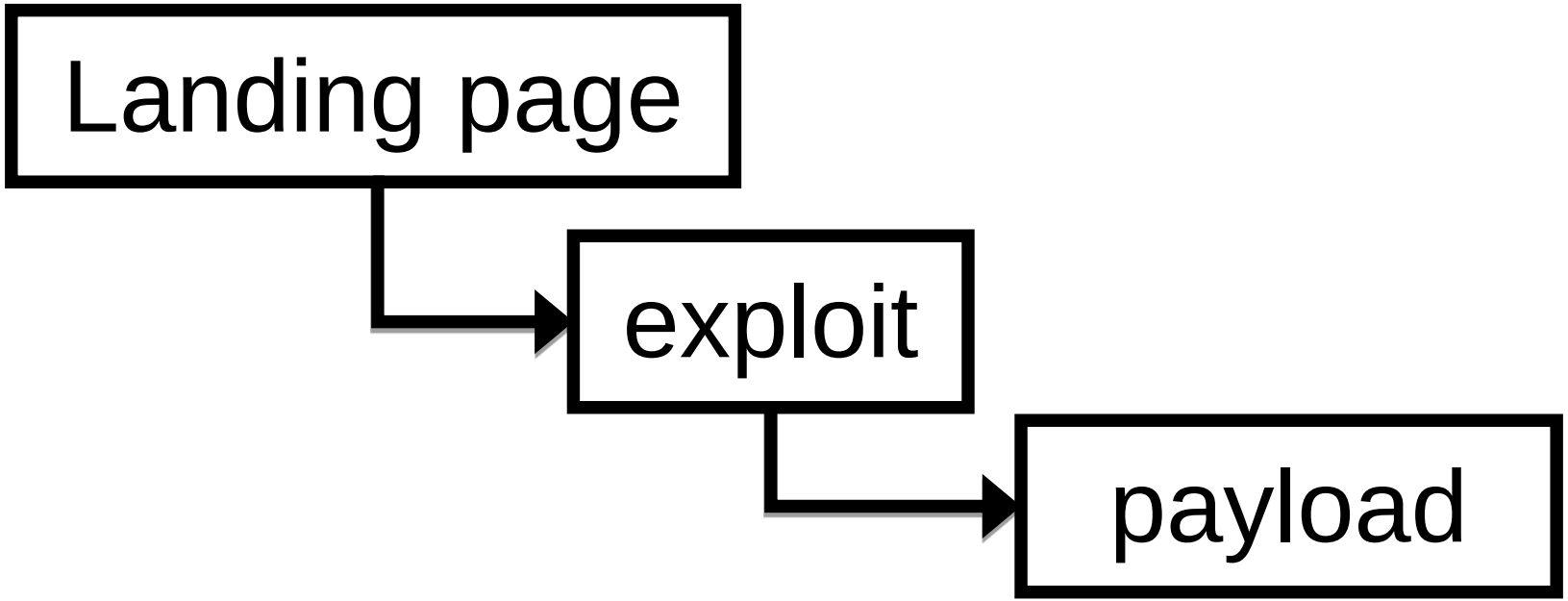
Exploit kits

Exploit kits are web servers that use exploits to take advantage of vulnerabilities in browser-based applications to infect a Windows computer without the user's knowledge.

Exploit kits



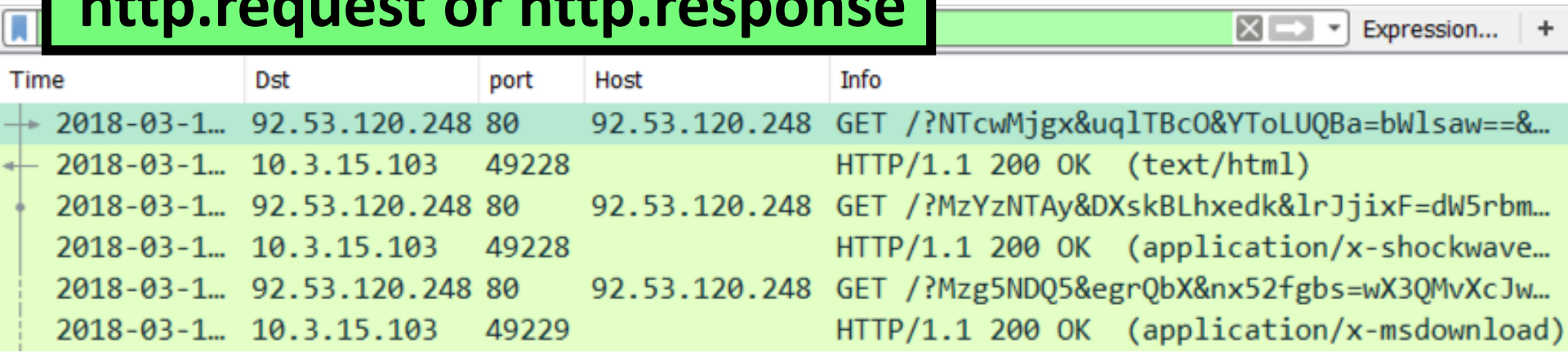
Exploit kits



Exploit kits

2018-traffic-analysis-workshop-block-4-04.pcap

http.request or http.response



Wireshark · Follow TCP Stream (tcp.stream eq 1) · 2018-traffic-analysis-workshop-block-4-04.pcap

```
GET /?
Mzg5NDQ5&egrQbX&nx52fgbs=wX3QMvXcJwDQDIbGMvrESLtANknQA0KK2Ir2_dqyEoH9fmnihNzUSkr26B2aCm3Q&iQa
ceqPy=bG9jYXRlZA==&WFbiql=cG9wdWxhcg==&otlXHkxtoPP=Y2FwaXRhbA==&ucRDtdAUrUgpBr=dW5rbm93bg==&F
CKSPTJQVNgLlDB=dW5rbm93bg==&KjOlcvKI=dGFraW5n&zLdswYxtDNTopNt=Y2FwaXRhbA==&thdd3d2d=8PYoJOYCa
FW0i0OELVZpz4xeBwwQpa-ti0fdnx_P0ZXU_kGKUQNC95OQHYFmmF7F HTTP/1.1
Connection: Keep-Alive
Accept: */*
User-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR
3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; rv:11.0) like Gecko
Host: 92.53.120.248

HTTP/1.1 200 OK
Server: nginx/1.2.1
Date: Thu, 15 Mar 2018 16:54:54 GMT
Content-Type: application/x-msdownload
Content-Length: 217608
Connection: keep-alive
Accept-Ranges: bytes

_u..*f.......OG.....2....B...AH*.."..t...LL.p"..,1..C..!K...|.:.5.!&..
)V...Z]..9..YeO.....|.
/$........s9.?........$.>.HUc@...tK...o.0.<.v.m..e|<..rV....VcDZ..n...C..[{..#..}
ZC.T..........j.m#[.g..x(..4G......g.l..Df..C.z?g5D.....U!.sP....VeE#   /...G.C.<.?B.
```

3 client pkts, 66 server pkts, 3 turns.

Block 4 - Review

- Phishing pages
- Tech support scams
- Pop-ups/unexpected web pages
- Exploit kits
- Hands-on exercises (4 pcaps)

2018 TRAFFIC ANALYSIS WORKSHOP

Up next...

Block 5: Policy violations

Block 5 - Overview

- Prohibited activity on your network
- Torrent traffic
- Hands on exercises

Prohibited activity

- Activity like online gambling, pornography, an illegal file sharing sites may be explicitly prohibited by your organization.

- Generally, security analysts do not actively search for policy violations.

Block 5 - Up next...

- Prohibited activity on your network
- **Torrent traffic**
- Hands on exercises

Torrent traffic

- After downloading a file using a torrent client, that client often will share the file.

- It's trivially easy for content creators to find out who is sharing illegal copies of their work.

DMCA notice

We are writing this message on behalf of HOME BOX OFFICE, INC. ("HBO"), with physical offices located at 1100 Avenue of the Americas, New York, NY 10036, United States (Attention: Director of Anti-Piracy).

DMCA notice

- ---------- Infringement Details ----------
Title: Game of Thrones
Timestamp: 2017-07-12T19:20
IP Address: *[recipient's public IP address]*
Port: 57382
Type: BitTorrent
Torrent Hash: ae30ec73d67bc3ca1afa07cfb9fbeccbe14fe55c
File Name: Game.of.Thrones.S07E01.720p.WEB.h264-TBS[eztv].mkv
File Size: 1,282 MB
- ----------

Torrent traffic

2018-traffic-analysis-workshop-block-5-01.pcap

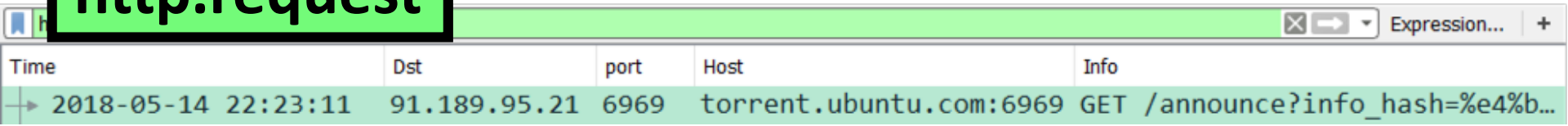
udp and !(dns)

Expression... +

Time	Src	port	Dst	port	Info
2018-05-14 22:22:58	95.165.174.130	54152	10.5.14.102	51413	54152 → 51413 Len…
2018-05-14 22:22:58	95.165.174.130	54152	10.5.14.102	51413	54152 → 51413 Len…
2018-05-14 22:22:58	190.228.253.165	51413	10.5.14.102	51413	51413 → 51413 Len…
2018-05-14 22:22:58	71.204.2.155	1454	10.5.14.102	51413	1454 → 51413 Len=…
2018-05-14 22:23:00	84.136.113.216	8999	10.5.14.102	51413	8999 → 51413 Len=…
2018-05-14 22:23:01	91.89.170.181	51515	10.5.14.102	51413	51515 → 51413 Len…
2018-05-14 22:23:02	189.13.84.110	18128	10.5.14.102	51413	18128 → 51413 Len…
2018-05-14 22:23:02	190.228.253.165	51413	10.5.14.102	51413	51413 → 51413 Len…
2018-05-14 22:23:02	36.81.44.185	60920	10.5.14.102	51413	60920 → 51413 Len…
2018-05-14 22:23:02	136.56.8.100	61596	10.5.14.102	51413	61596 → 51413 Len…
2018-05-14 22:23:02	186.182.161.29	31595	10.5.14.102	51413	31595 → 51413 Len…
2018-05-14 22:23:03	178.64.95.166	55426	10.5.14.102	51413	55426 → 51413 Len…
2018-05-14 22:23:04	95.165.174.130	54152	10.5.14.102	51413	54152 → 51413 Len

Torrent traffic

http.request



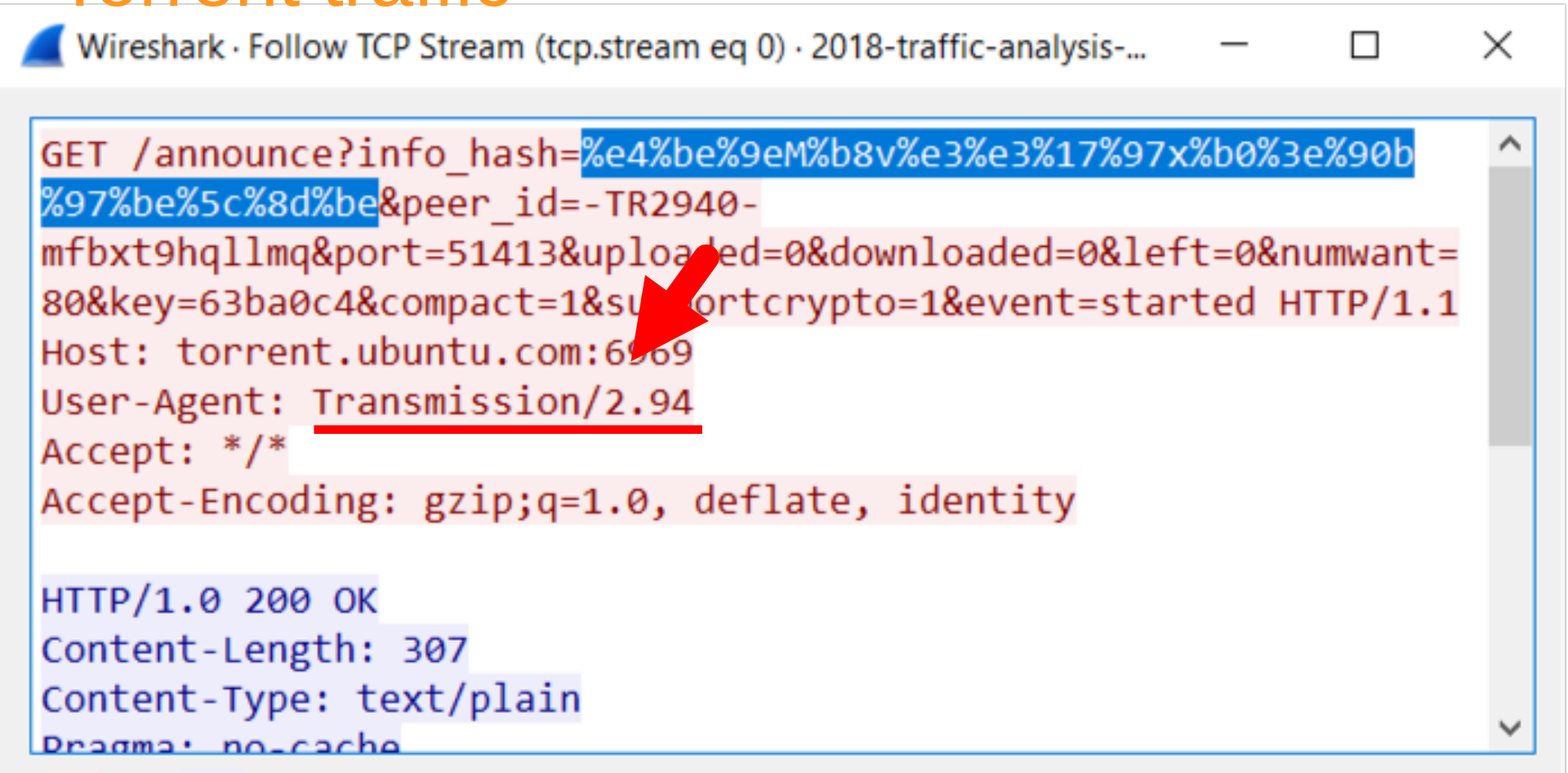
`torrent.ubuntu.com:6969`

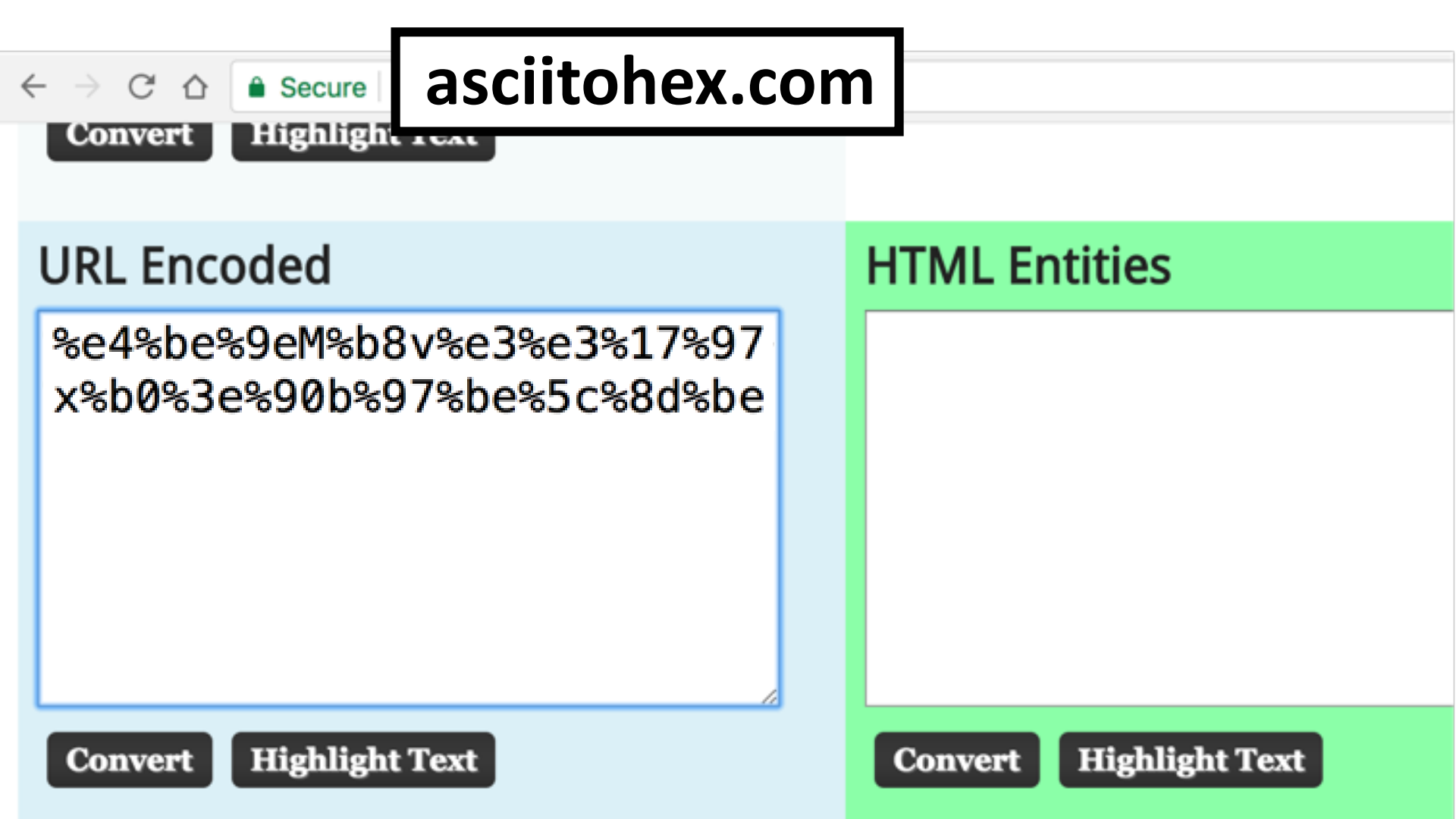
- **`GET /announce?info_hash=`**

In similar traffic, you might also see:

- **`GET /scrape?info_hash=`**

Torrent traffic




asciitohex.com
Secure
Convert
URL Encoded
%e4%be%9eM%b8v%e3%e3%17%97
x%b0%3e%90b%97%be%5c%8d%be
Convert
Highlight Text
HTML Entities
Convert
Highlight Text

001011 00000101 10000100
111011 11001011 00110101
010111 01001000 10001101
000110 00100011 11010000

ht Text

Hexadecimal

e4 be 9e 4d b8 76 e3 e3 17 97
78 b0 3e 90 62 97 be 5c 8d be

Convert | Highlight Text

Decimal

e4be9e4db876e3e3179778b03e906297be5c8dbe

All Maps Videos Images Shopping More Settings Tools

6 results (0.52 seconds)

BitTorrent download info

torrent.ubuntu.com:6969/

... 418, 10, 3844, 2.75TiB. **e4be9e4db876e3e3179778b03e906297be5c8dbe**, ubuntu-18.04-desktop-amd64.iso, 1.78GiB, 6097, 219, 85784, 149.94TiB.

ubuntu-18.04-desktop-amd64 at Linuxtracker

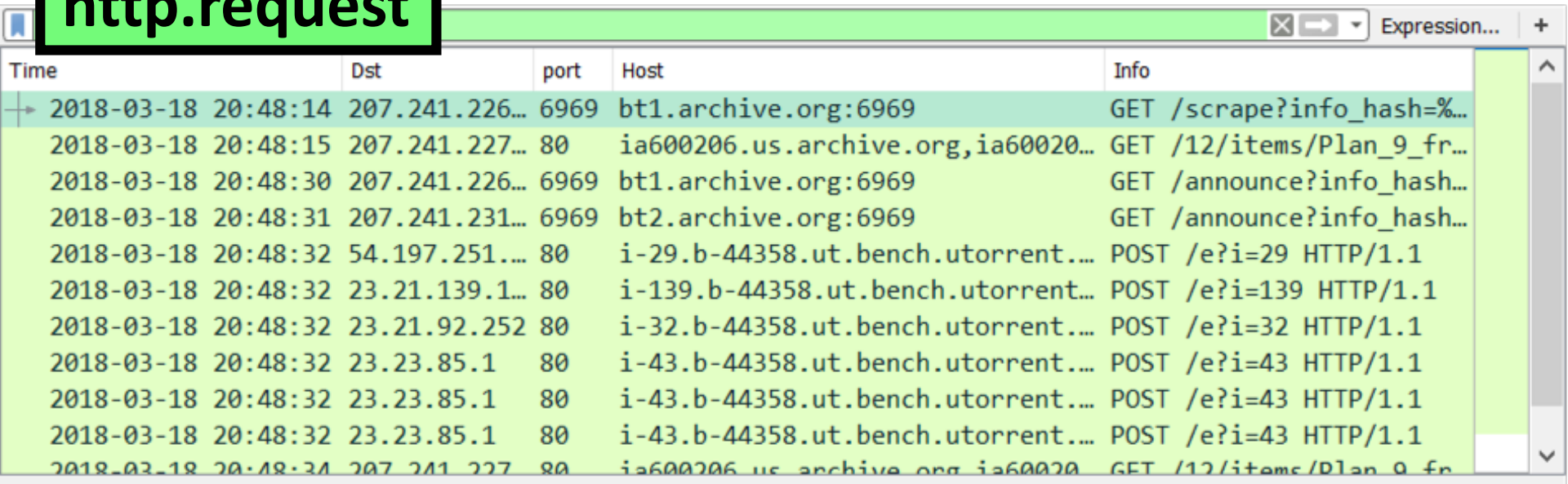
linuxtracker.org/index.php?page...e4be9e4db876e3e3179778b03e906297be5c8dbe

Apr 30, 2018 - Info Hash, **e4be9e4db876e3e3179778b03e906297be5c8dbe**. Who thanks. tokopan BRFoton gerinho sverre26. Description, Ubuntu is a ...

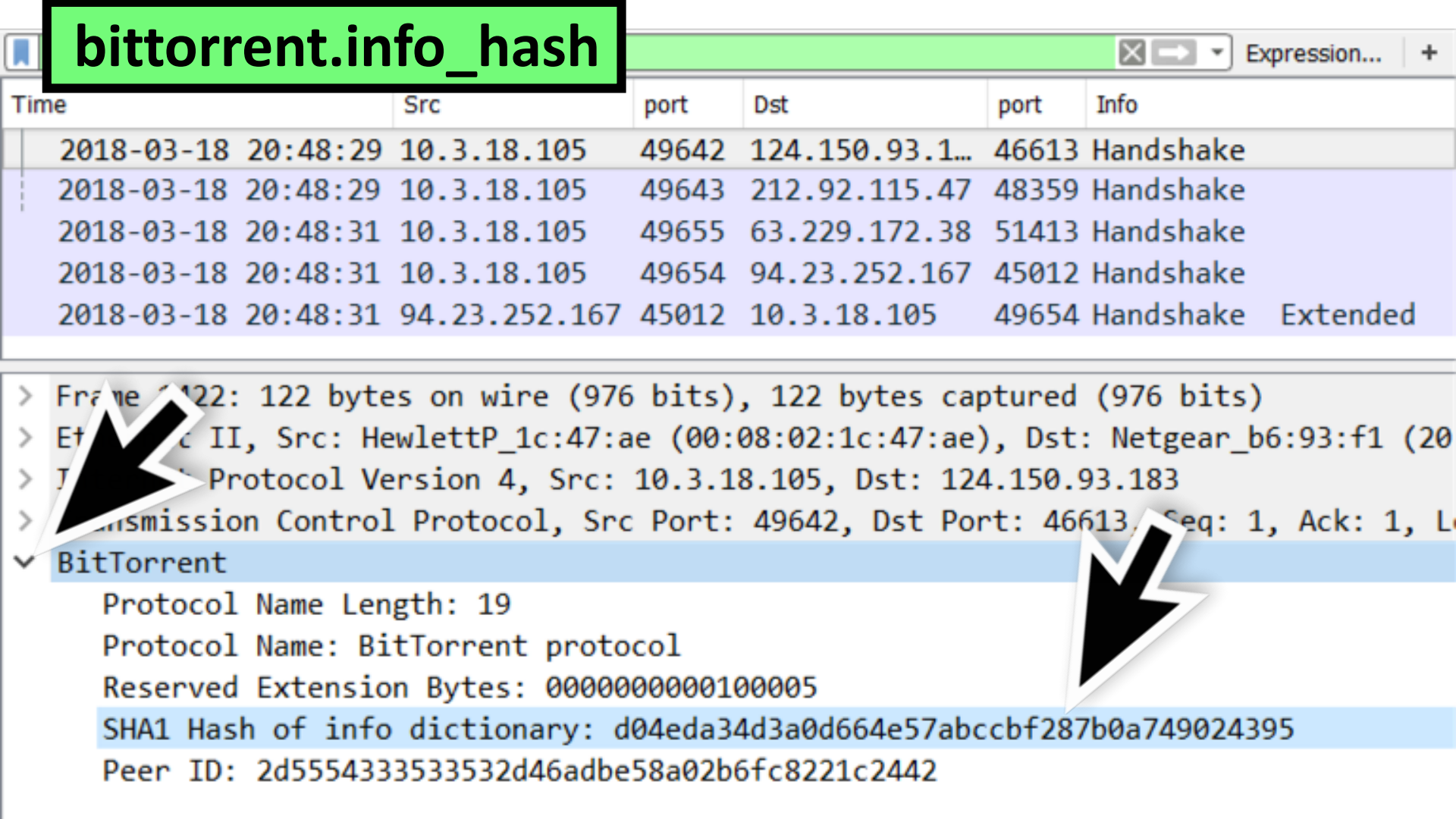
Torrent traffic

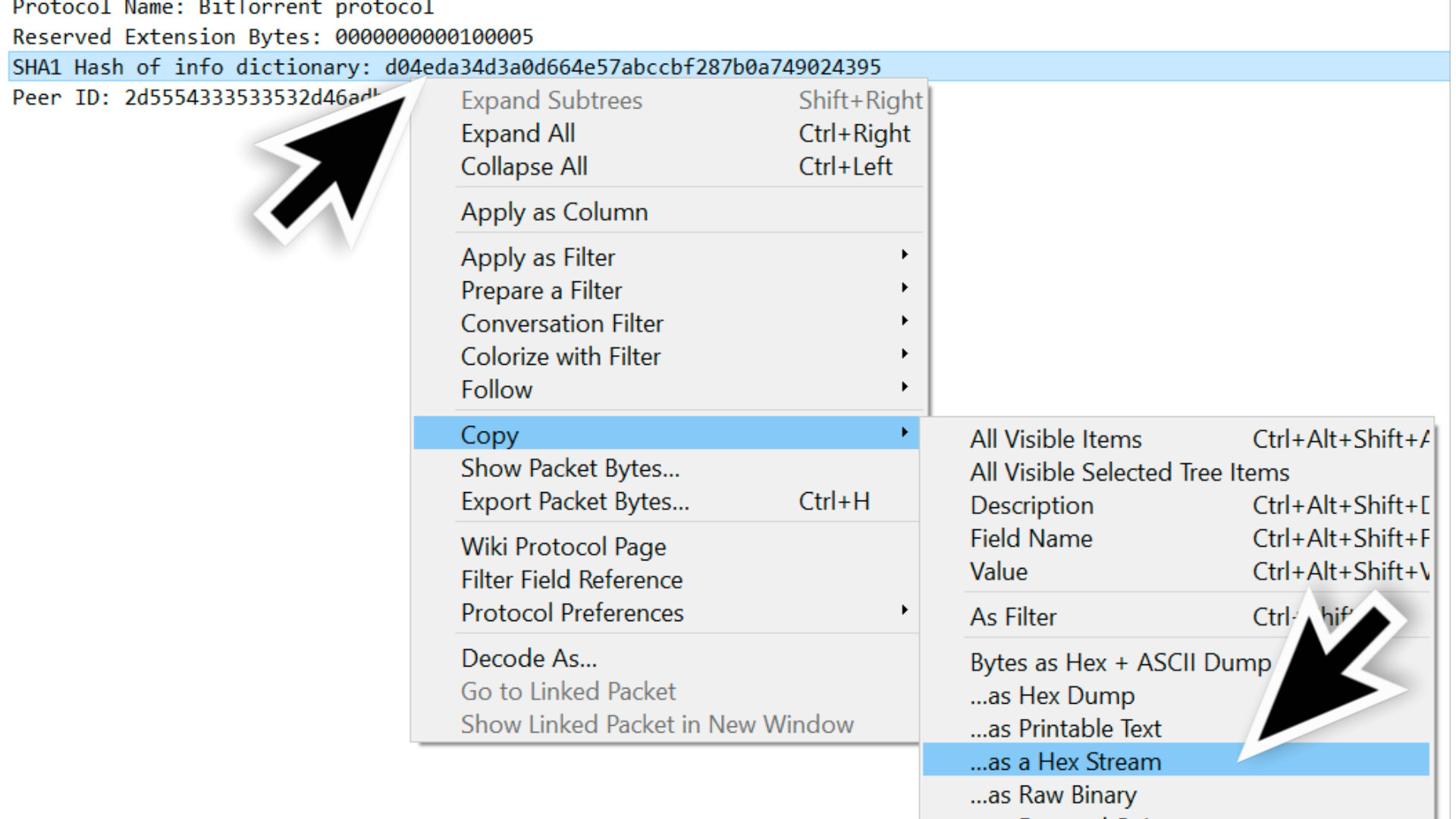
2018-traffic-analysis-workshop-block-5-02.pcap

http.request



Time	Dst	port	Host	Info
2018-03-18 20:48:14	207.241.226…	6969	bt1.archive.org:6969	GET /scrape?info_hash=%…
2018-03-18 20:48:15	207.241.227…	80	ia600206.us.archive.org,ia60020…	GET /12/items/Plan_9_fr…
2018-03-18 20:48:30	207.241.226…	6969	bt1.archive.org:6969	GET /announce?info_hash…
2018-03-18 20:48:31	207.241.231…	6969	bt2.archive.org:6969	GET /announce?info_hash…
2018-03-18 20:48:32	54.197.251.…	80	i-29.b-44358.ut.bench.utorrent.…	POST /e?i=29 HTTP/1.1
2018-03-18 20:48:32	23.21.139.1…	80	i-139.b-44358.ut.bench.utorrent…	POST /e?i=139 HTTP/1.1
2018-03-18 20:48:32	23.21.92.252	80	i-32.b-44358.ut.bench.utorrent.…	POST /e?i=32 HTTP/1.1
2018-03-18 20:48:32	23.23.85.1	80	i-43.b-44358.ut.bench.utorrent.…	POST /e?i=43 HTTP/1.1
2018-03-18 20:48:32	23.23.85.1	80	i-43.b-44358.ut.bench.utorrent.…	POST /e?i=43 HTTP/1.1
2018-03-18 20:48:32	23.23.85.1	80	i-43.b-44358.ut.bench.utorrent.…	POST /e?i=43 HTTP/1.1
2018-03-18 20:48:34	207.241.227…	80	ia600206.us.archive.org,ia60020…	GET /12/items/Plan_9_fr…


bittorrent.info_hash
Expression...
Time Src port Dst port Info
2018-03-18 20:48:29 10.3.18.105 49642 124.150.93.1… 46613 Handshake
2018-03-18 20:48:29 10.3.18.105 49643 212.92.115.47 48359 Handshake
2018-03-18 20:48:31 10.3.18.105 49655 63.229.172.38 51413 Handshake
2018-03-18 20:48:31 10.3.18.105 49654 94.23.252.167 45012 Handshake
2018-03-18 20:48:31 94.23.252.167 45012 10.3.18.105 49654 Handshake Extended
Protocol Version 4, Src: 10.3.18.105, Dst: 124.150.93.183
BitTorrent
Protocol Name Length: 19
Protocol Name: BitTorrent protocol
Reserved Extension Bytes: 0000000000100005
SHA1 Hash of info dictionary: d04eda34d3a0d664e57abccbf287b0a749024395
Peer ID: 2d5554333533532d46adbe58a02b6fc8221c2442


Protocol Name: BitTorrent protocol
Reserved Extension Bytes: 0000000000100005
SHA1 Hash of info dictionary: d04eda34d3a0d664e57abccbf287b0a749024395
Peer ID: 2d5554333533532d46ad
Expand Subtrees Shift+Right
Expand All Ctrl+Right
Collapse All Ctrl+Left
Apply as Column
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize with Filter
Follow
Copy
Show Packet Bytes...
Export Packet Bytes... Ctrl+H
Wiki Protocol Page
Filter Field Reference
Protocol Preferences
Decode As...
Go to Linked Packet
Show Linked Packet in New Window
All Visible Items Ctrl+Alt+Shift+A
All Visible Selected Tree Items
Description Ctrl+Alt+Shift+D
Field Name Ctrl+Alt+Shift+F
Value Ctrl+Alt+Shift+V
As Filter
Bytes as Hex + ASCII Dump
...as Hex Dump
...as Printable Text
...as a Hex Stream
...as Raw Binary

d04eda34d3a0d664e57abccbf287b0a749024395

All Maps Videos Images Shopping More Settings Tools

2 results (0.32 seconds)

bt1.us.archive.org hotlist - Internet Archive

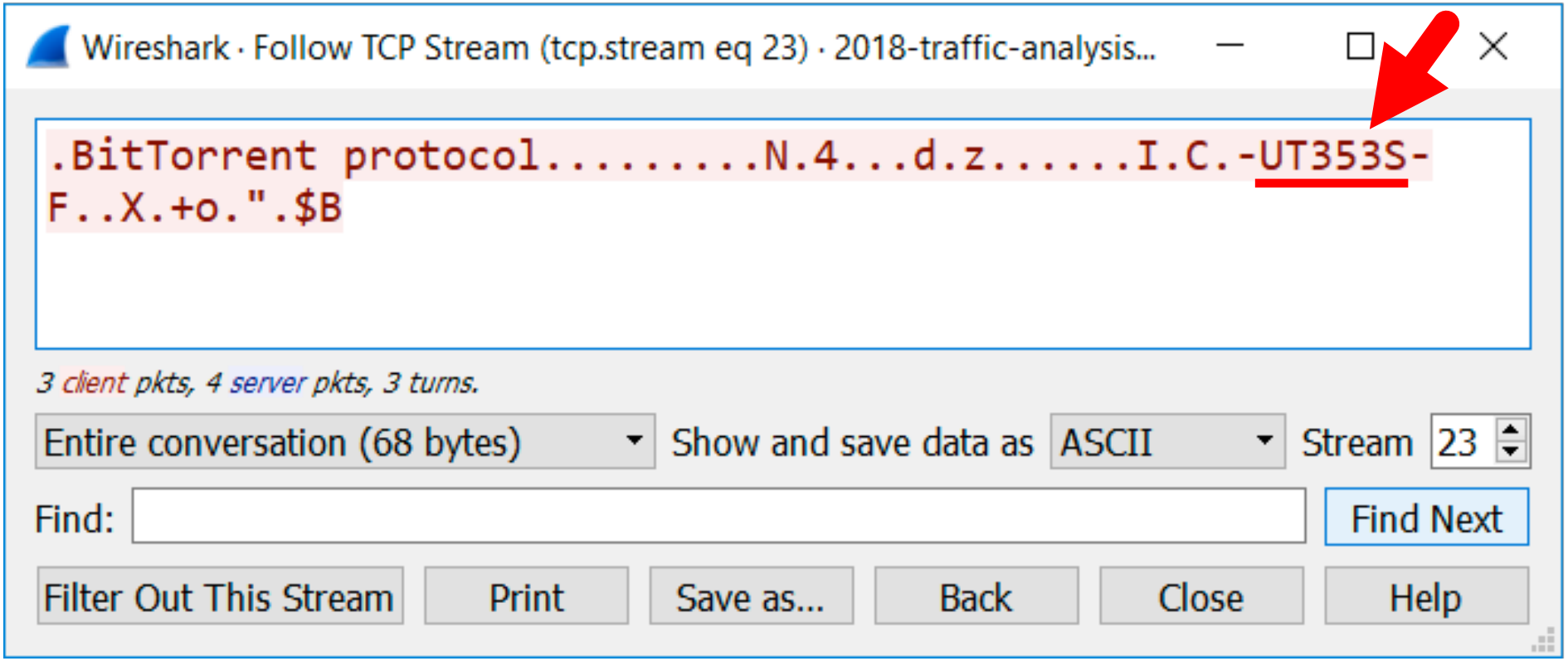
https://bt1.archive.org/hotlist.php ▾

... 1964 60FPS Build - GoldenEye/Perfect Dark Edition15150138 f0696de7e7a7cd719f873b0dec6f00fa71277fe3; Windows Live Essentials 2012 (offline setup)15150264d1b26e66dc54dd01760a01ad631958e08ef5dac3; Plan 9 from Outer Space15132167**d04eda34d3a0d664e57abccbf287b0a749024395**; Fanfiction.net ...

Outerspace,磁力链接,种子下载,迅雷下载资源-BTAMO

https://www.btamo.com/s/Outerspace.html ▾ Translate this page

Outerspace磁力链接,Outerspace种子下载,Outerspace百度云,Outerspace迅雷下载,Outerspace全部资源


Wireshark · Follow TCP Stream (tcp.stream eq 23) · 2018-traffic-analysis...
.BitTorrent protocol.....N.4...d.z.....I.C.-UT353S-
F..X.+o.".$B
3 client pkts, 4 server pkts, 3 turns.
Entire conversation (68 bytes)
Show and save data as
ASCII
Stream
23
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help

Block 5 - Review

- Prohibited activity on your network
- Torrent traffic
- Hands on exercises (2 pcaps)

2018 TRAFFIC ANALYSIS WORKSHOP

Up next...

Block 6: Root causes and false positives

Block 6 - Overview

- Root causes from web traffic
- Root causes from malspam campaigns
- False positives
- Hands-on exercises

Root causes from web traffic

2018-traffic-analysis-workshop-block-6-01.pcap

Src IP	SPort	Dst IP	DPort	Pr
10.4.22.101	62392	185.17.122.212	80	6

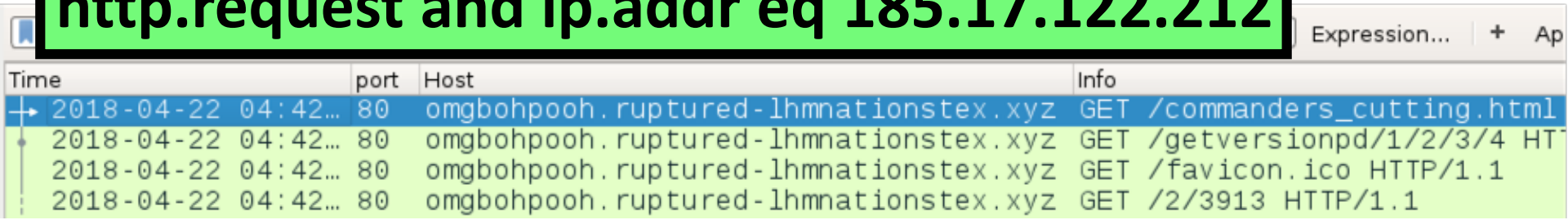
Event Message
ETPRO CURRENT_EVENTS Grandsoft EK Exploit Request 2018-04-20

Grandsoft EK on 185.17.122.212

Root causes from web traffic

2018-traffic-analysis-workshop-block-6-01.pcap

http.request and ip.addr eq 185.17.122.212



omgbohpooh.ruptured-lhmnationstex.xyz

Left click on the last HTTP GET request and follow TCP stream or HTTP stream

Root causes from web traffic

http.request or ssl.handshake.type == 1

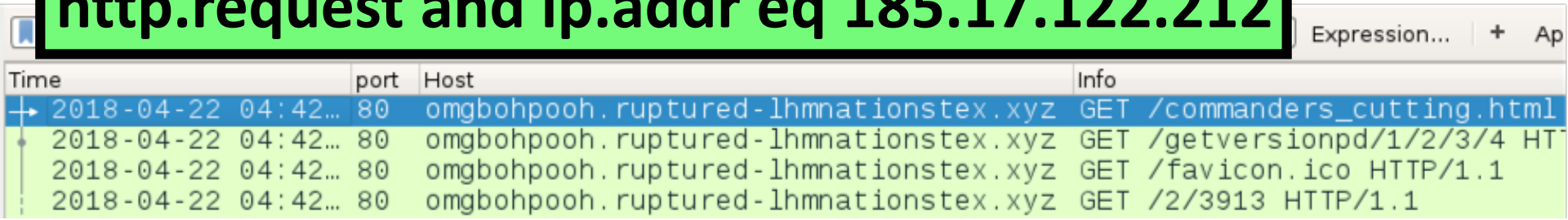
ssion... + Apply this filter

Time	port	Host	Server Name	Info
2018-04-22 04:42…	80	elitegol.me		GET / HTTP/1.1
2018-04-22 04:42…	80	www.elitegol.me		GET / HTTP/1.1
2018-04-22 04:42…	80	www.elitegol.me		GET /elitegol/style/general.
2018-04-22 04:42…	80	www.elitegol.me		GET /elitegol/style/mensaje.
2018-04-22 04:42…	80	www.elitegol.me		GET /elitegol/style/mensaje.
2018-04-22 04:42…	80	www.elitegol.me		GET /elitegol/img/logo.png H
2018-04-22 04:42…	80	4.bp.blogspot.com		GET /-5gFdEJACSuI/Ui2M5enBwM
2018-04-22 04:42…	80	2.bp.blogspot.com		GET /-5MO7aTt7R4Y/Ui2UgUyn_E
2018-04-22 04:42…	80	2.bp.blogspot.com		GET /-_dSXbJpAqGM/UQM1baugHS
2018-04-22 04:42…	80	3.bp.blogspot.com		GET /-rOsfBHt7XIU/UQMlgPaSqM
2018-04-22 04:42…	80	lh6.ggpht.com		GET /_gKQKwLZ8XUs/TIvsZTMx7t

The first HTTP request is to **elitegol.me**, and the last few HTTP requests are for Grandsoft EK

Root causes from web traffic

http.request and ip.addr eq 185.17.122.212



omgbohpooh.ruptured-lhmnationstex.xyz

Left click on the **first** HTTP GET request and follow TCP stream or HTTP stream

Root causes from web traffic

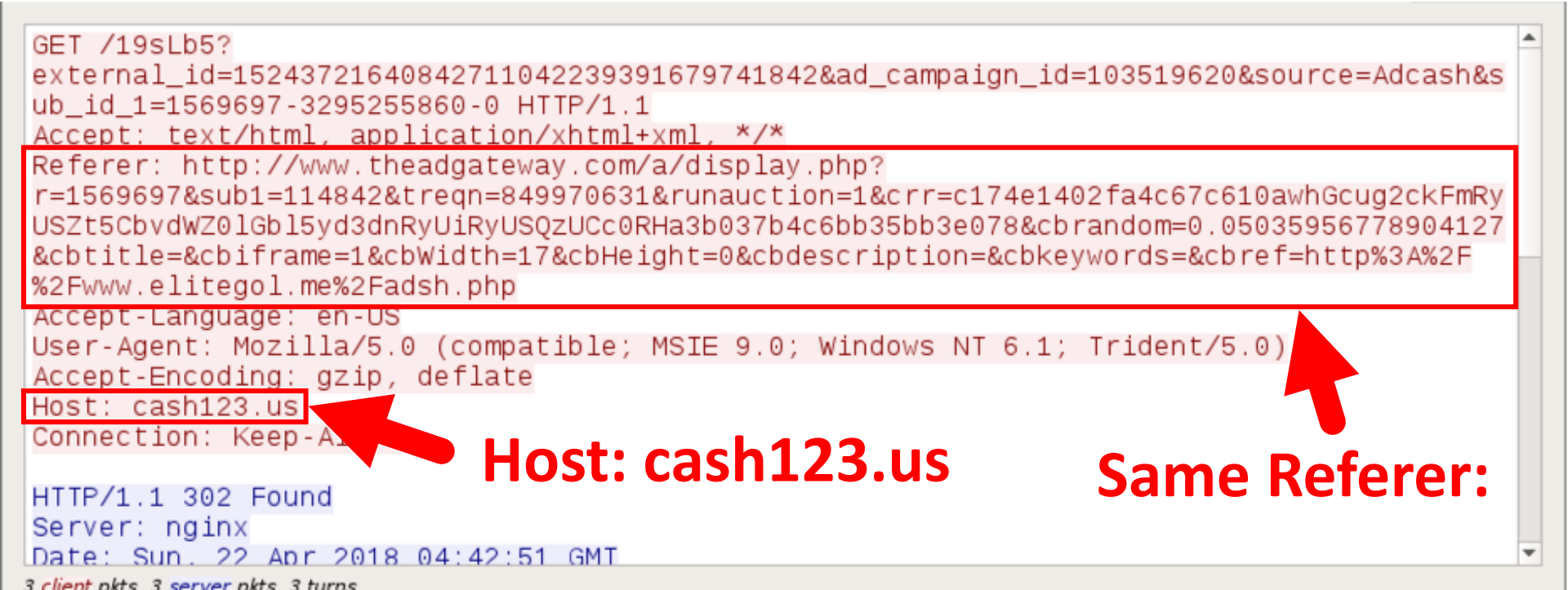
Root causes from web traffic

ip contains omgbohpooh.ruptured-lhmnationstex.xyz

HTTP/1.1 302 found

Root causes from web-based infections

Referer lines may not contain all requests in the chain



Root causes from web traffic

- **www.elitegol.me**
- **www.elitegol.me - GET /adsh.php**
- **URL to xml.pdn-1.com**
- **URL to www.theadgateway.com**
- **URL to cash123.us**
- **Landing page for Grandsoft EK**

Root causes from web traffic

2018-traffic-analysis-workshop-block-6-02.pcap

People are getting hit by a fake AV pages. They merely have to kill their browser process to fix things, but how does it happen?

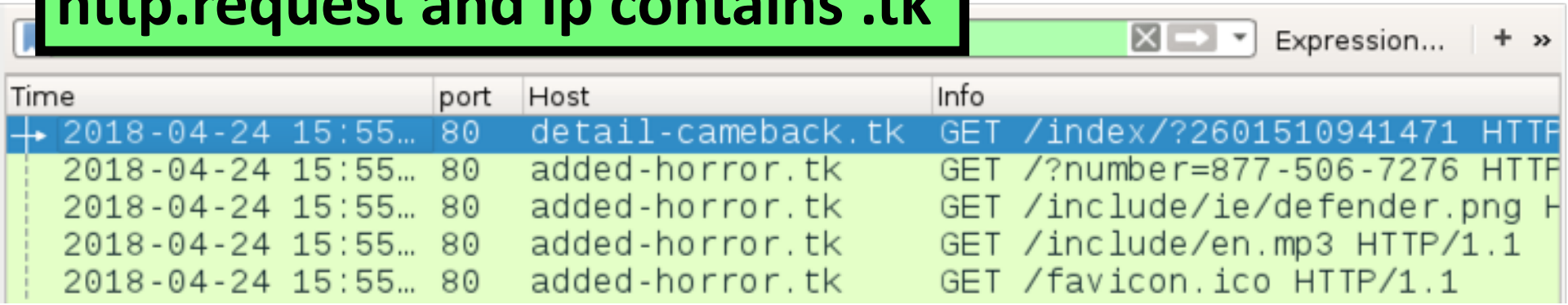
Root causes from web traffic

Src IP	SPort	Dst IP	DPort	Pr
172.16.100.37	64226	172.16.100.1	53	17
172.16.100.37	49231	185.224.215.251	80	6

Event Message
ET DNS Query to a .tk domain - Likely Hostile
ET POLICY HTTP Request to a *.tk domain

Root causes from web traffic

http.request and ip contains .tk



- **detail-cameback.tk - GET /index/?2601510941471**
- **added-horror.tk - GET /?number=877-506-7276**

Root causes from web traffic

Follow the HTTP stream for the first HTTP request to coaching-journey.com

<script>window.location.replace("http://detail-cameback.tk/index/?2601510941471");window.location.href = "http://detail-cameback.tk/index/?2601510941471";</script>
<!DOCTYPE html>
<html lang="en-US" prefix="og: http://ogp.me/ns#">
<head >

Block 6 - Up next...

- Root causes from web traffic
- **Root causes from malspam campaigns**
- False positives
- Hands-on exercises

Root causes from malspam campaigns

2018-traffic-analysis-workshop-block-6-03.pcap

- NOTE: This and the remaining pcaps contain various other traffic not directly related to the infection (NBNS, DHCP, windows update traffic, etc).

Root causes from malspam campaigns

2018-traffic-analysis-workshop-block-6-03.pcap

Src IP	SPort	Dst IP	DPort	Pr	Event Message
107.180.25.48	80	172.16.100.49	49158	6	ET POLICY Binary Download Smaller than 1 MB Likely Hostile
1					ET POLICY PE EXE or DLL Windows file download HTTP
1					ET INFO Executable Retrieved With Minimal HTTP Headers -...
172.16.100.49	49159	216.239.36.21	80	6	ET POLICY Possible External IP Lookup ipinfo.io
172.16.100.49	49161	54.221.221.65	80	6	ET POLICY External IP Lookup api.ipify.org
93.181.186.127	451	172.16.100.49	49167	6	ET POLICY OpenSSL Demo CA - Internet Widgits Pty (O)
78.155.219.199	447	172.16.100.49	49169	6	ETPRO TROJAN Trickbot SSL Certificate Detected
207.140.15.87	449	172.16.100.49	49170	6	ET POLICY OpenSSL Demo CA - Internet Widgits Pty (O)

78.155.219.199 447

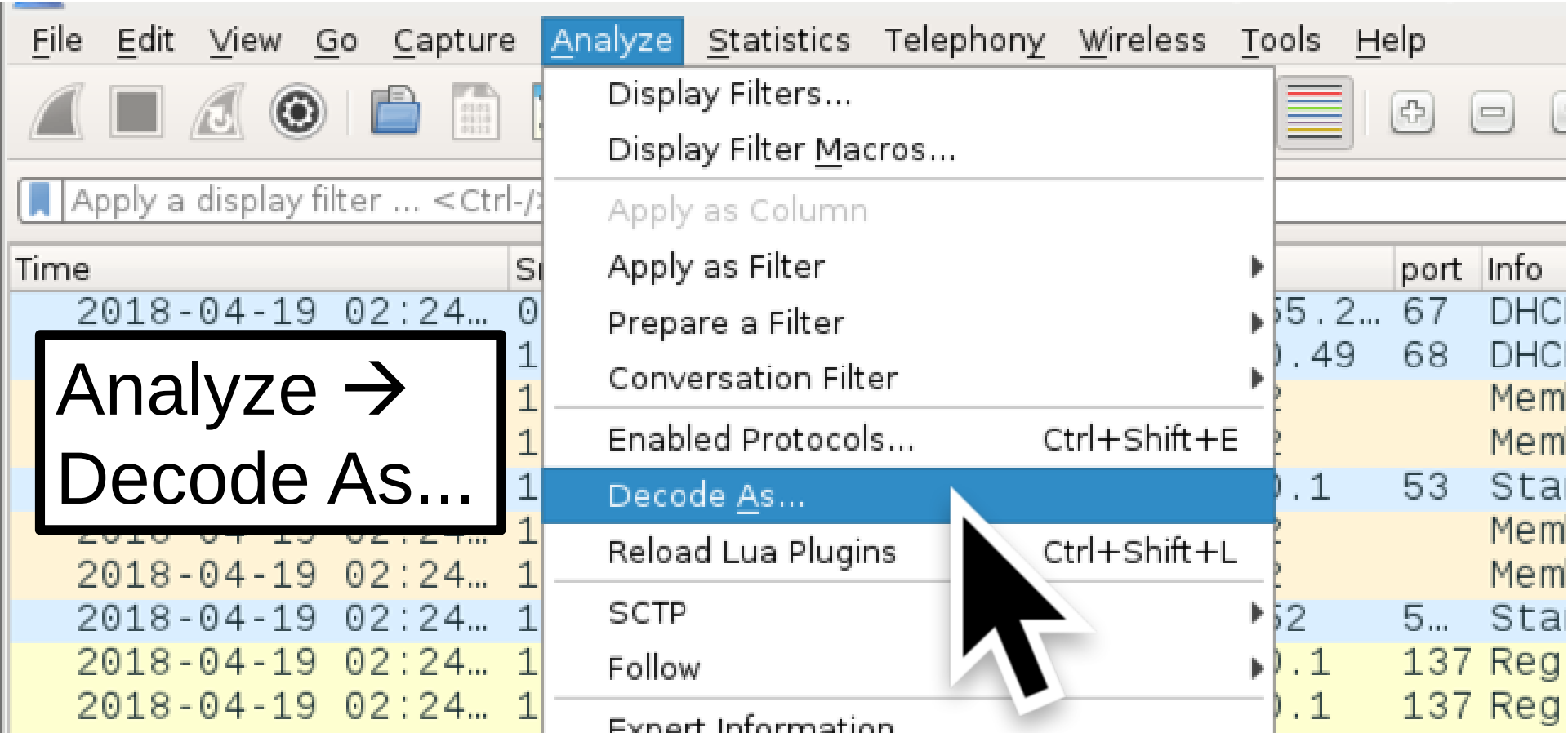
ETPRO TROJAN Trickbot SSL Certificate Detected

Root causes from malspam campaigns

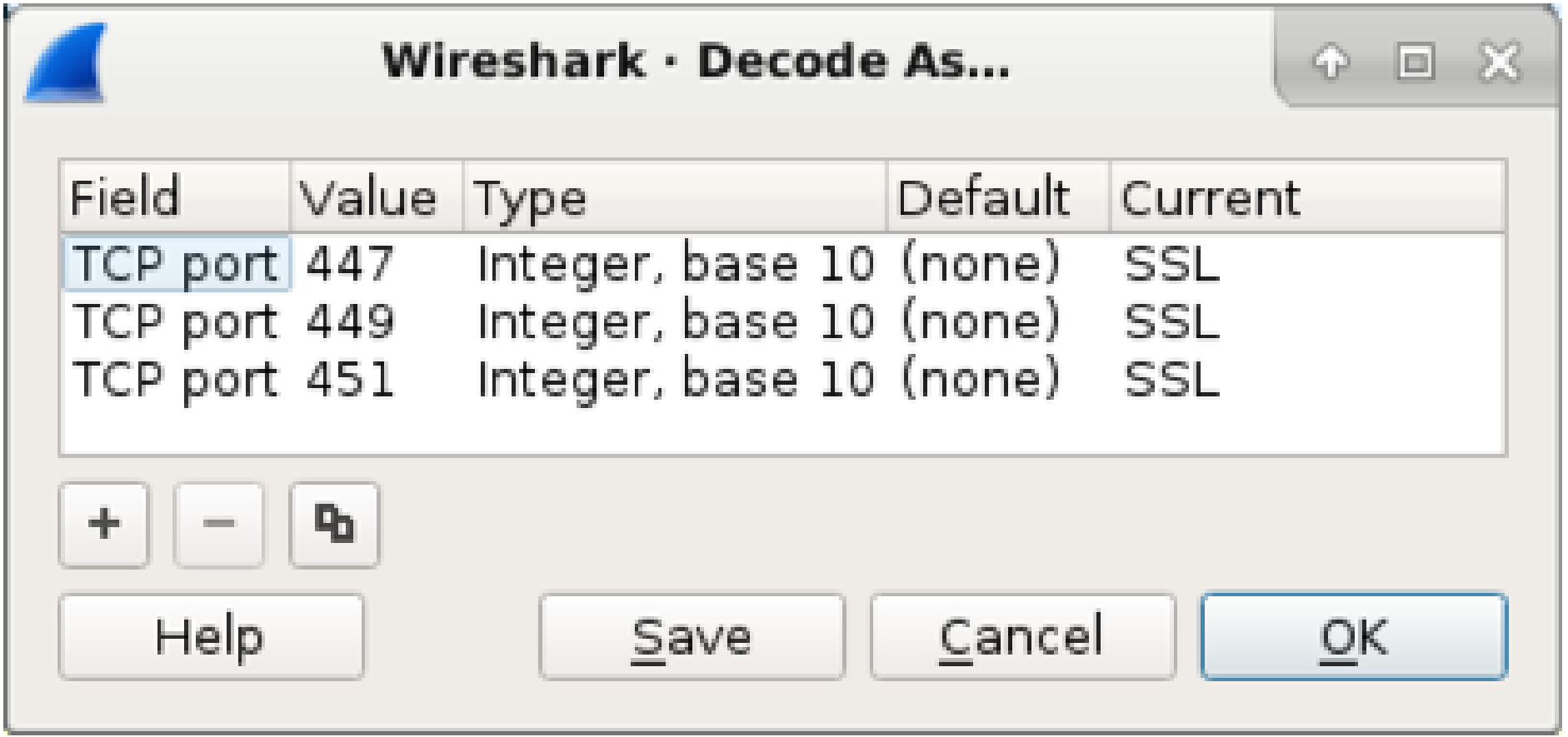
2018-traffic-analysis-workshop-block-6-03.pcap

- 107.180.25.48: EXE or DLL download
- ET POLICY OpenSSL Demo CA
  - 93.181.186.127 - TCP port 451
  - Various IP addresses - TCP port 449

Root causes from malspam campaigns



Root causes from malspam campaigns



Root causes from malspam campaigns

(http.request or ssl.handshake.type == 1) and !(udp.port eq 1900)

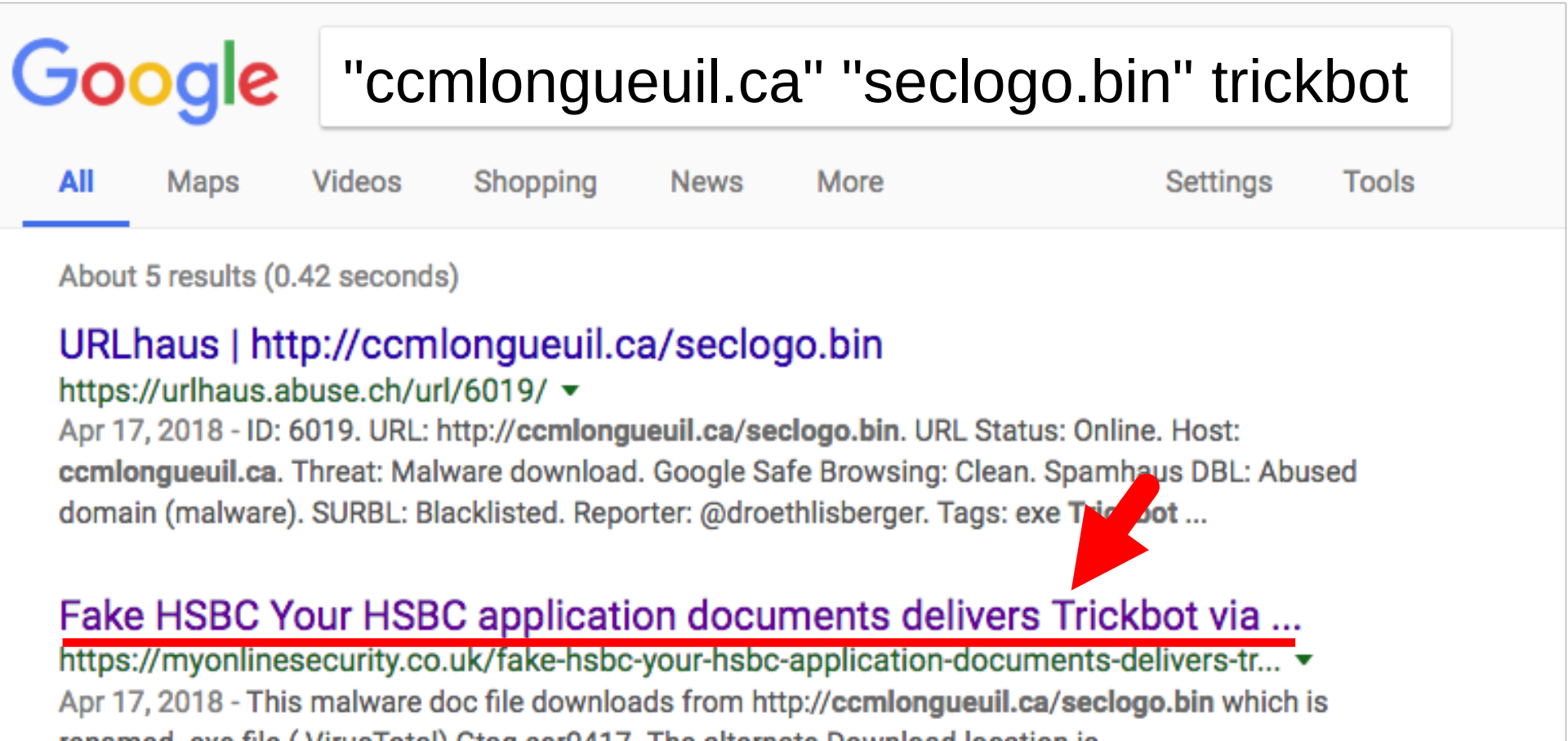
Apply this filter

Time				
2				HTTP/1.1
2018-04-19 02:25…	107.180.25.48	80	ccmlongueuil.ca	GET /seclogo.bin HTTP/1.1
2018-04-19 02:27…	216.239.36.21	80	ipinfo.io	GET /ip HTTP/1.1
2018-04-19 02:27…	54.221.221.65	80	api.ipify.org	GET / HTTP/1.1
2018-04-19 02:29…	93.181.186.127	451		Client Hello
2018-04-19 02:29…	173.205.30.73	80	www.download.windowsupdate.com	GET /msdownload/update/v3/
2018-04-19 02:29…	78.155.219.199	447		Client Hello
2018-04-19 02:30…	207.140.15.87	449		Client Hello
2018-04-19 02:30…	173.205.30.115	80	www.download.windowsupdate.com	GET /msdownload/update/v3/
2018-04-19 02:30…	68.227.31.46	449		Client Hello
2018-04-19 02:30…	173.205.30.113	80	www.download.windowsupdate.com	GET /msdownload/update/v3/
2018-04-19 02:30…	68.227.31.46	449		Client Hello
2018-04-19 02:30…	173.205.30.113	80	www.download.windowsupdate.com	GET /msdownload/update/v3/
2018-04-19 02:31…	46.20.207.204	449		Client Hello
2018-04-19 02:31…	46.20.207.204	449		Client Hello
2018-04-19 02:31…	46.20.207.204	449		Client Hello
2018-04-19 02:31…	46.20.207.204	449		Client Hello
2018-04-19 02:31…	8.253.112.121	80	www.download.windowsupdate.com	GET /msdownload/update/v3/
2018-04-19 02:31…	8.253.112.121	80	www.download.windowsupdate.com	GET /msdownload/update/v3/
2018-04-19 02:31…	8.253.112.121	80	www.download.windowsupdate.com	GET /msdownload/update/v3/
2018-04-19 02:31…	8.253.112.121	80	www.download.windowsupdate.com	GET /msdownload/update/v3/
2018-04-19 02:32…	194.87.103.45	447		Client Hello

Root causes from malspam campaigns

- **ccmlongueuil.ca - GET /seclogo.bin**
  - **93.181.186.27 port 451**
  - **78.155.219.199 port 447**
  - **207.140.15.87 port 449**
  - **26.20.207.204 port 449**
  - **194.87.103.45 port 447**

Root causes from malspam campaigns



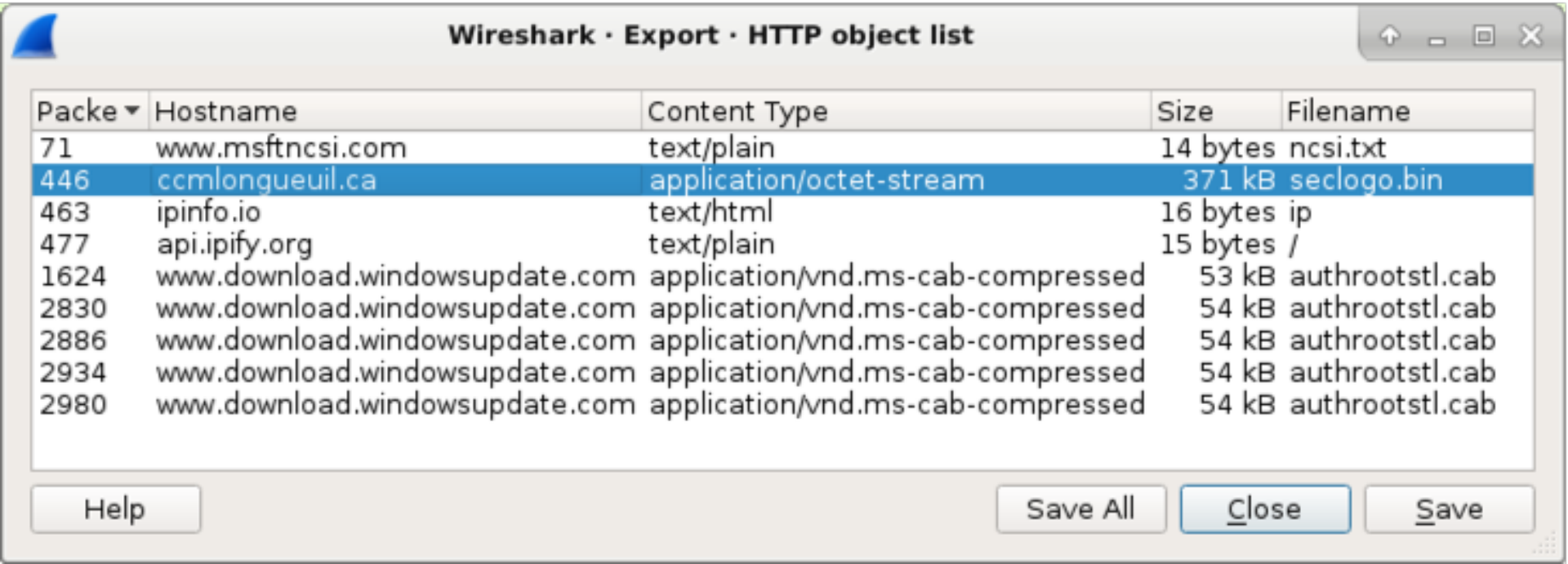
Root causes from malspam campaigns

```
GET /seclogo.bin HTTP/1.1
Host: ccmlongueuil.ca
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Thu, 19 Apr 2018 02:24:40 GMT
Server: Apache
Last-Modified: Tue, 17 Apr 2018 11:26:57 GMT
ETag: "69c02de-5ac00-56a099db9e630"
Accept-Ranges: bytes
Content-Length: 371712
Vary: Accept-Encoding,User-Agent
Keep-Alive: timeout=5
Connection: Keep-Alive
Content-Type: application/octet-stream

MZ.....@.....  .!..L.!
This program cannot be run in DOS mode.

$
```

3 client pkts, 257 server pkts, 3 turns

Root causes from malspam campaigns

File → Export Objects → HTTP...



Root causes from malspam campaigns

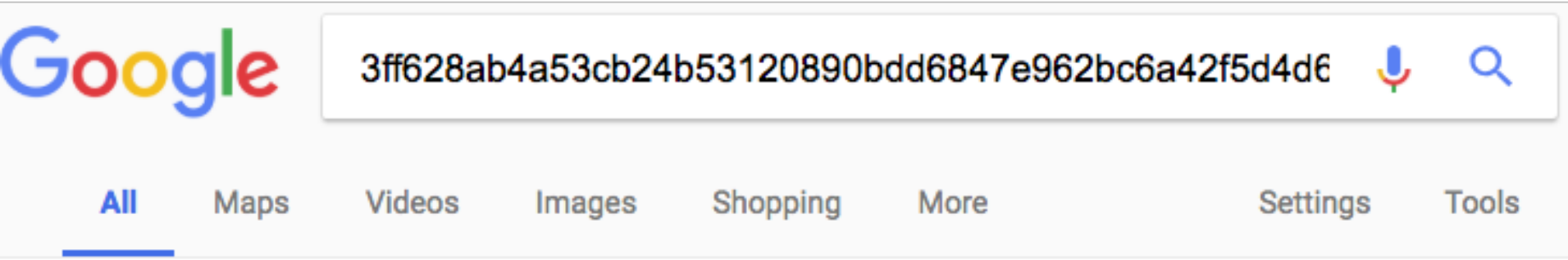
```
$ file seclogo.bin

seclogo.bin: PE32 executable (GUI)
Intel 80386, for MS Windows

$ shasum -a 256 seclogo.bin

3ff628ab4a53cb24b53120890bdd6847e962
bc6a42f5d4d6aed1e23b38850a3e
```

Root causes from malspam campaigns

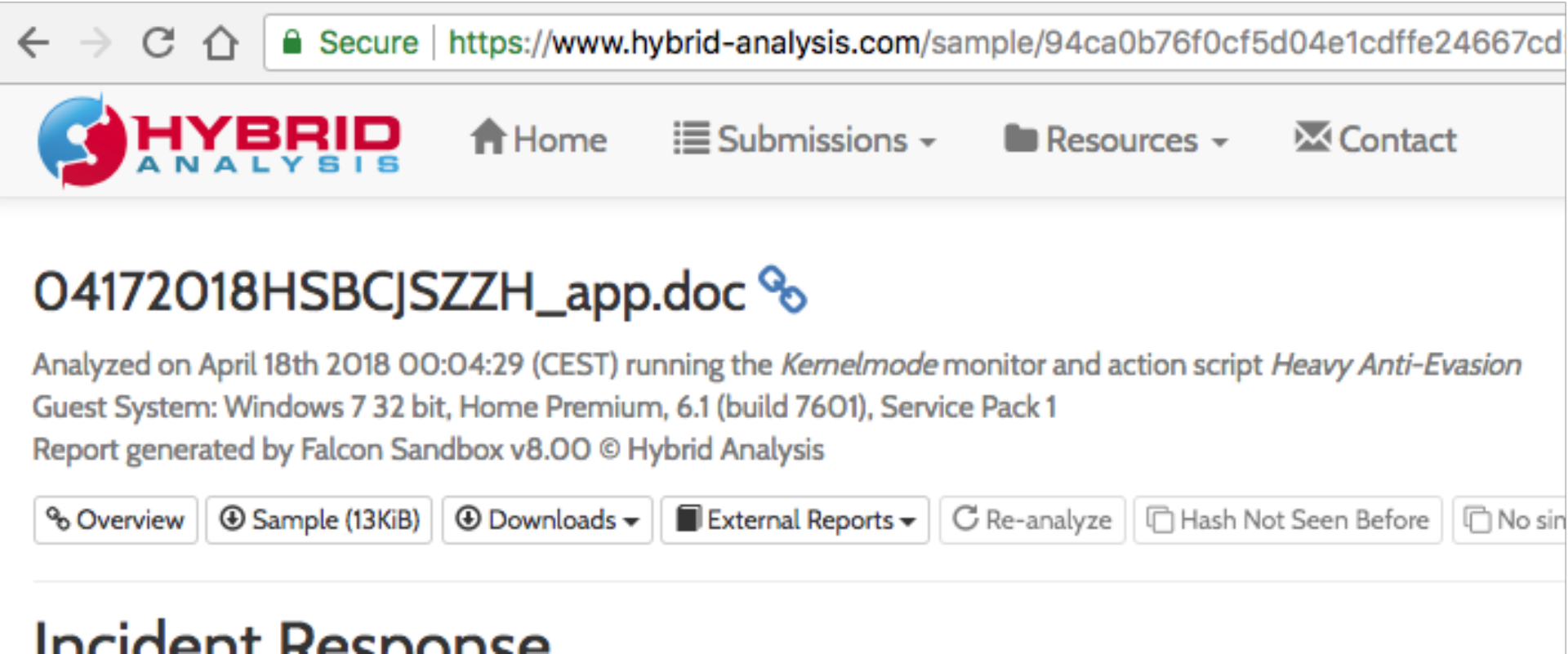
Google search:

3ff628ab4a53cb24b53120890bdd6847e962bc6a42f5d4d6aed1e23b38850a3e site:www.hybrid-analysis.com

Root causes from malspam campaigns



Root causes from malspam campaigns



Block 6 - Up next...

- Root causes from web traffic
- Root causes from malspam campaigns
- **False positives**
- Hands-on exercises

False positives

False positives

An alert may be a true positive, but it doesn't mean something bad happened.

For example, a "malvertisement redirection" alert in web traffic could have happened, but the follow-up malicious traffic never occurred.

False positives

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ET CURRENT_EVENTS RIG EK Landing URI Struct"; flow:established,to_server; content:"/?PHPSSESID=njr"; http_uri; fast_pattern:only; classtype:trojan-activity; sid:2019072; rev:3;)

Block 6 - Review

- Root causes from web traffic
- Root causes from malspam campaigns
- False positives
- Hands-on exercises (2 pcaps)

2018 TRAFFIC ANALYSIS WORKSHOP

Up next...

Block 7: Bringing it all together: Writing incident reports

Block 7 - Overview

- Incident report format
- Internal network description
- Exercise 1
- Exercise 2
- Exercise 3
- Exercise 4

Incident reporting format

WHEN

WHO

WHAT

Incident reporting format

FORMAT

- Executive summary
- Details
- Indicators of compromise (IOCs)

Incident reporting format

EXECUTIVE SUMMARY

On 2018-04-24 at ***??:??*** UTC, a Windows computer used by ***???*** was infected with ***???***

- *Sentence: origin of infection, if known*
- *Sentence: corrective actions taken*

Incident reporting format

DETAILS

- victim's IP address
- victim's host name
- victim's MAC address
- victim's Windows account name

Incident reporting format

IOCs

- IP addresses and ports
- Domain names
- File hashes

Block 7 - Up next...

- Incident report format
- **Internal network description**
- Exercise 1
- Exercise 2
- Exercise 3
- Exercise 4

Internal network: thunderlife.net

- Domain: **thunderlife.net**
- Network segment: **172.16.1.0/24**
- Domain controller: **172.16.1.8**
  THUNDERLIFE-DC
- Segment gateway: **172.16.1.1**
- Broadcast address: **172.16.1.255**

Block 7 - Up next...

- Incident report format
- Internal network description
- **Exercise 1**
- Exercise 2
- Exercise 3
- Exercise 4

Block 7 - Exercise 1

2018-traffic-analysis-workshop-block-7-exercise-1.pcap

On 2018-04-24 at ***??:??*** UTC, a Windows computer used by ***???*** was infected with ***???***

- *Sentence: ~~origin of infection, if known~~*
- *Sentence: ~~corrective actions taken~~*

Block 7 - Exercise 1

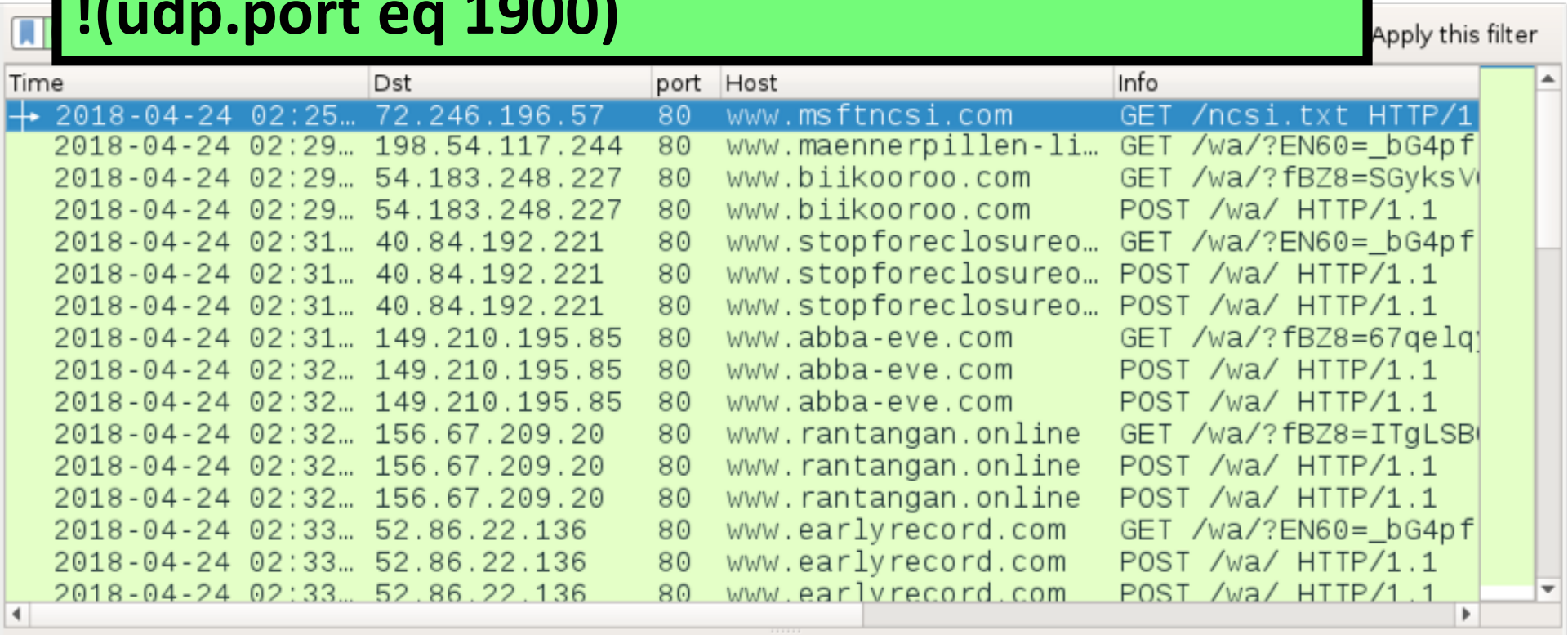
ALERTS

Src IP	SPort	Dst IP	DPort	Pr	Event Message
172.16.1.115	49200	54.183.248.227	80	6	ETPRO TROJAN FormBook CnC Checkin (POST)
172.16.1.115	49203	40.84.192.221	80	6	ETPRO TROJAN FormBook CnC Checkin (POST)
172.16.1.115	49206	149.210.195.85	80	6	ETPRO TROJAN FormBook CnC Checkin (POST)
172.16.1.115	49209	156.67.209.20	80	6	ETPRO TROJAN FormBook CnC Checkin (POST)
172.16.1.115	49212	52.86.22.136	80	6	ETPRO TROJAN FormBook CnC Checkin (POST)
172.16.1.115	49215	162.213.249.164	80	6	ETPRO TROJAN FormBook CnC Checkin (POST)
172.16.1.115	49221	107.164.17.51	80	6	ETPRO TROJAN FormBook CnC Checkin (POST)
172.16.1.115	49224	198.54.117.217	80	6	ETPRO TROJAN FormBook CnC Checkin (POST)
172.16.1.115	49227	23.245.187.10	80	6	ETPRO TROJAN FormBook CnC Checkin (POST)
172.16.1.115	49230	52.212.175.227	80	6	ETPRO TROJAN FormBook CnC Checkin (POST)

ETPRO TROJAN Formbook CnC Checkin (POST)

Block 7 - Exercise 1

(http.request or ssl.handshake.type == 1) and !(udp.port eq 1900)



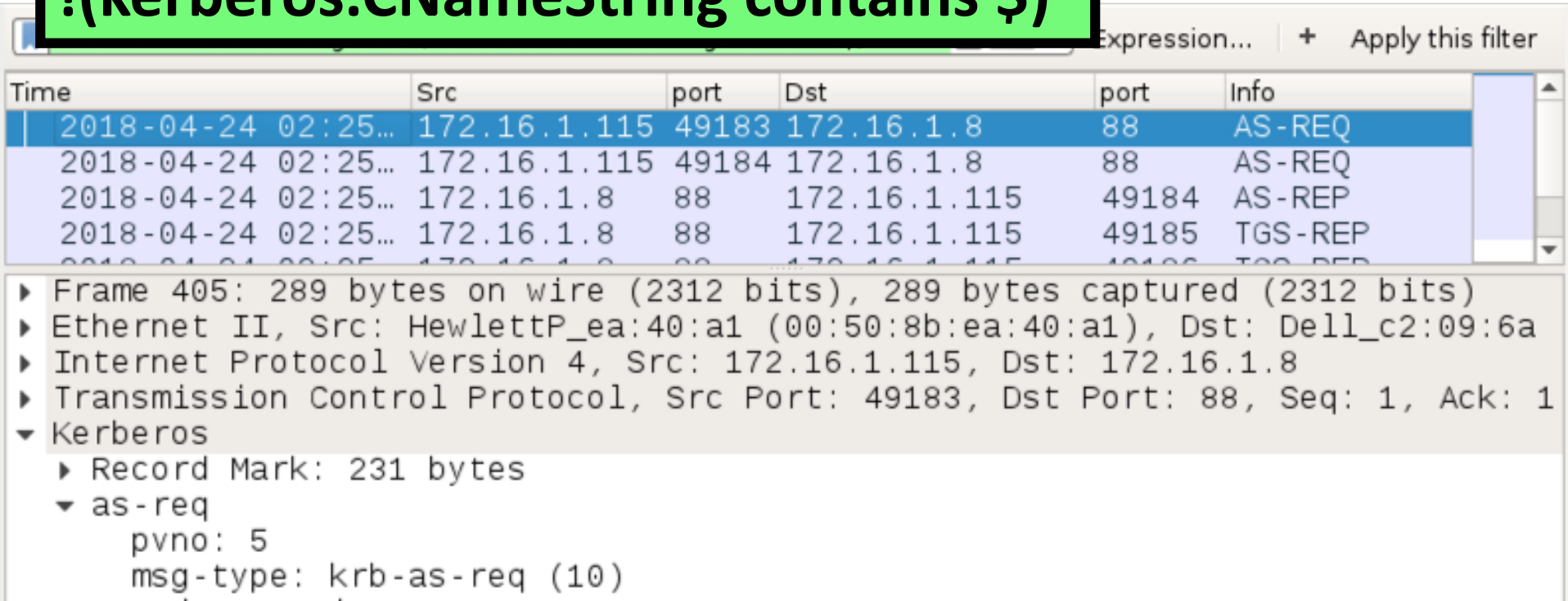
Block 7 - Exercise 1

WHEN ***WHO*** *WHAT*

kerberos.CNameString and !(kerberos.CNameString contains $)

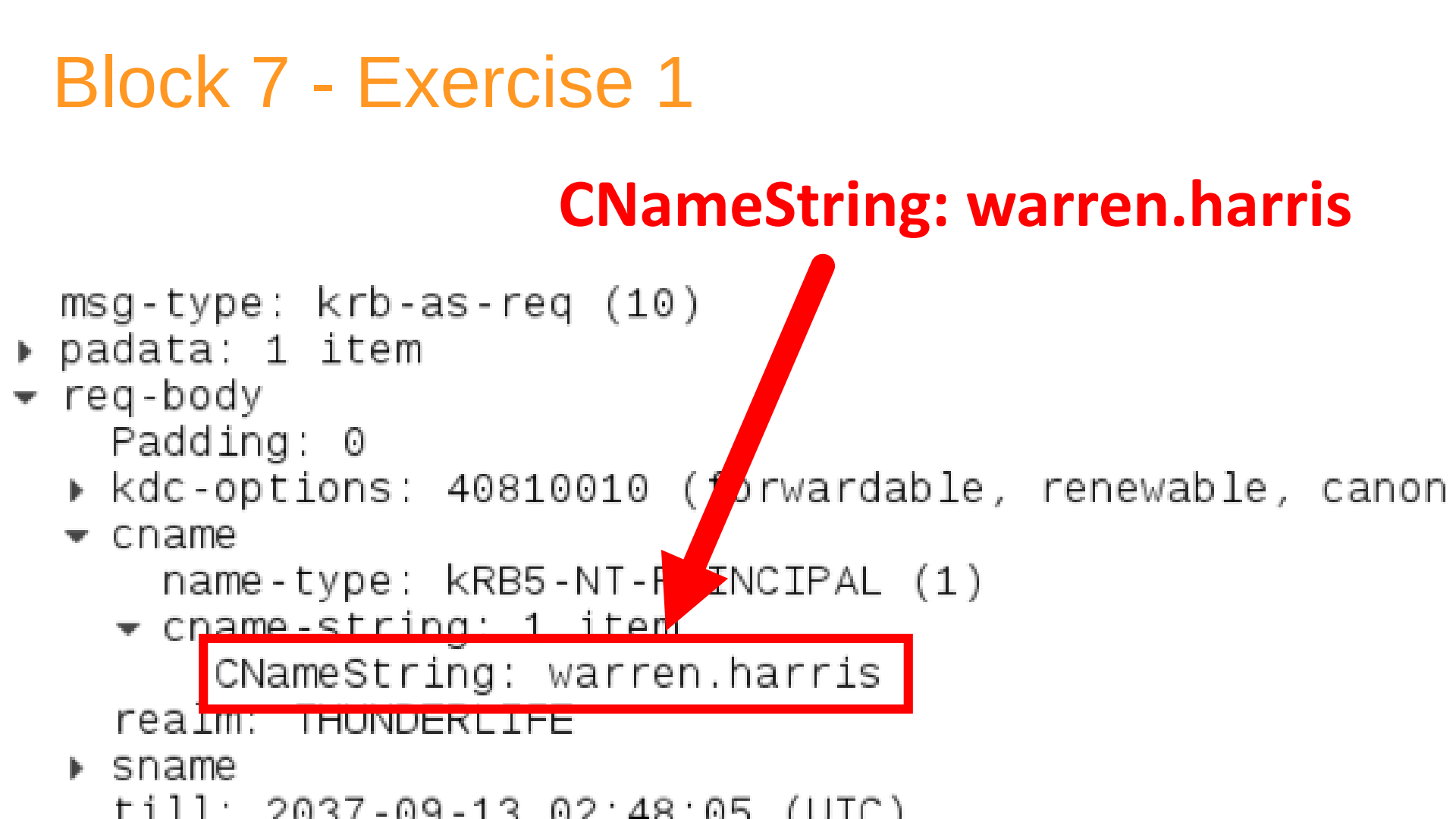
Block 7 - Exercise 1

kerberos.CNameString and !(kerberos.CNameString contains $)



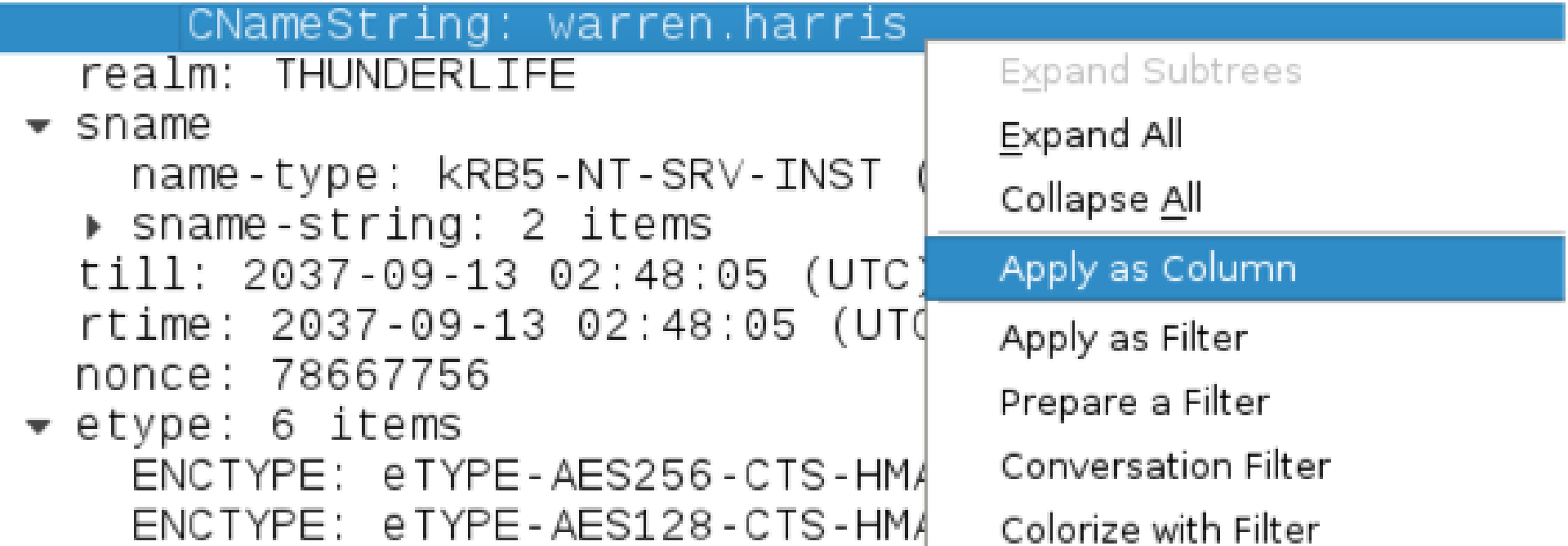
Block 7 - Exercise 1

CNameString: warren.harris



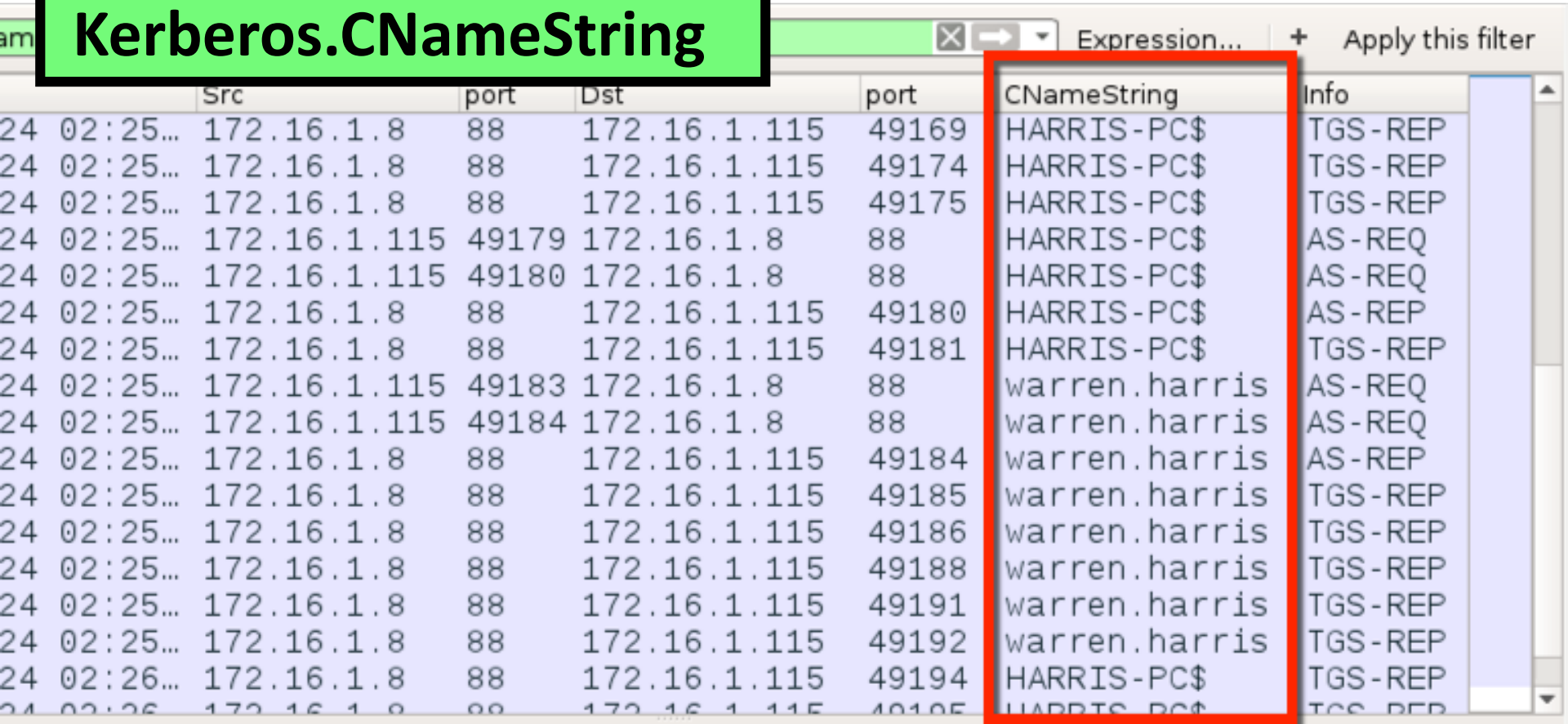
Block 7 - Exercise 1

Select the CNameString field and "Apply as Column"



Block 7 - Exercise 1

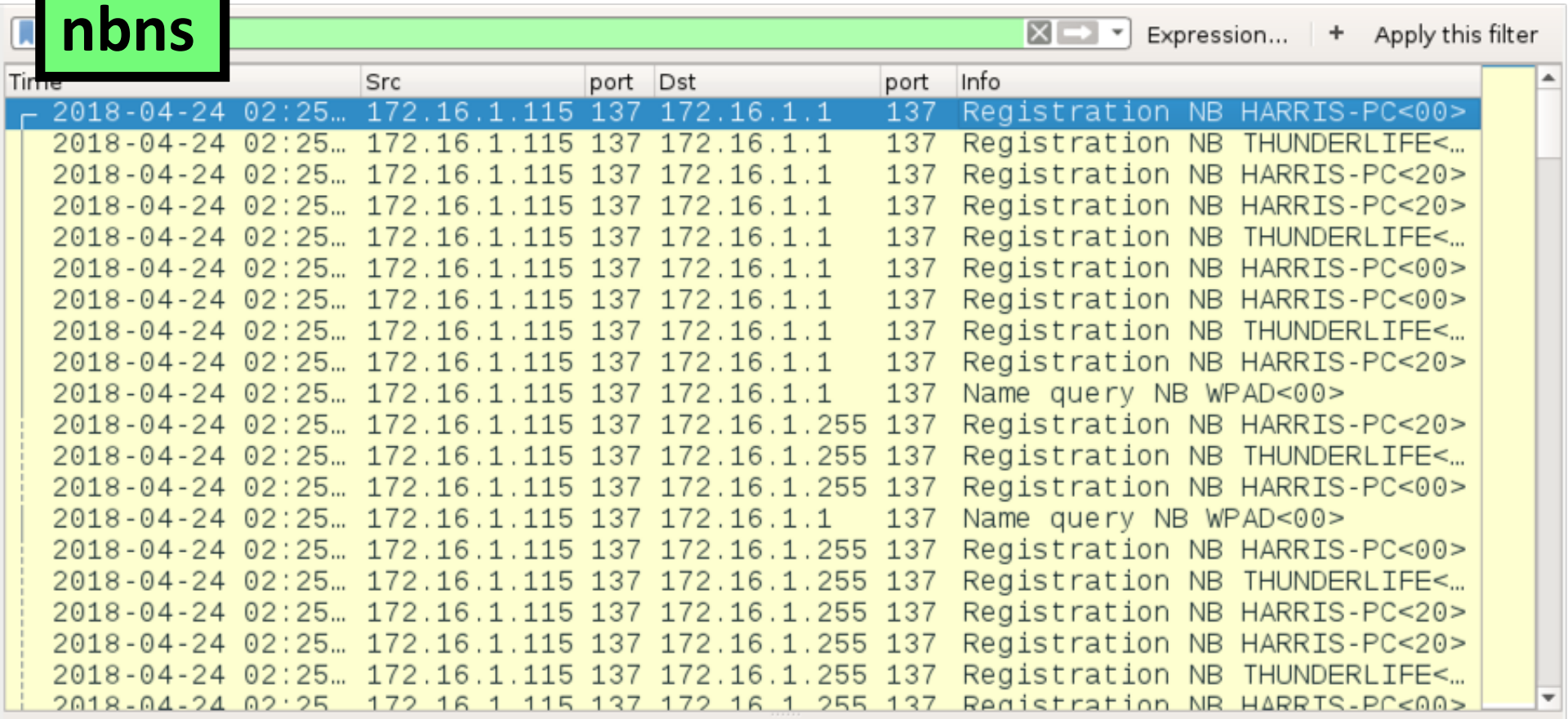
Kerberos.CNameString



	Src	port	Dst	port	CNameString	Info
24 02:25…	172.16.1.8	88	172.16.1.115	49169	HARRIS-PC$	TGS-REP
24 02:25…	172.16.1.8	88	172.16.1.115	49174	HARRIS-PC$	TGS-REP
24 02:25…	172.16.1.8	88	172.16.1.115	49175	HARRIS-PC$	TGS-REP
24 02:25…	172.16.1.115	49179	172.16.1.8	88	HARRIS-PC$	AS-REQ
24 02:25…	172.16.1.115	49180	172.16.1.8	88	HARRIS-PC$	AS-REQ
24 02:25…	172.16.1.8	88	172.16.1.115	49180	HARRIS-PC$	AS-REP
24 02:25…	172.16.1.8	88	172.16.1.115	49181	HARRIS-PC$	TGS-REP
24 02:25…	172.16.1.115	49183	172.16.1.8	88	warren.harris	AS-REQ
24 02:25…	172.16.1.115	49184	172.16.1.8	88	warren.harris	AS-REQ
24 02:25…	172.16.1.8	88	172.16.1.115	49184	warren.harris	AS-REP
24 02:25…	172.16.1.8	88	172.16.1.115	49185	warren.harris	TGS-REP
24 02:25…	172.16.1.8	88	172.16.1.115	49186	warren.harris	TGS-REP
24 02:25…	172.16.1.8	88	172.16.1.115	49188	warren.harris	TGS-REP
24 02:25…	172.16.1.8	88	172.16.1.115	49191	warren.harris	TGS-REP
24 02:25…	172.16.1.8	88	172.16.1.115	49192	warren.harris	TGS-REP
24 02:26…	172.16.1.8	88	172.16.1.115	49194	HARRIS-PC$	TGS-REP

Block 7 - Exercise 1

nbns



Time	Src	port	Dst	port	Info
2018-04-24 02:25…	172.16.1.115	137	172.16.1.1	137	Registration NB HARRIS-PC<00>
2018-04-24 02:25…	172.16.1.115	137	172.16.1.1	137	Registration NB THUNDERLIFE<…
2018-04-24 02:25…	172.16.1.115	137	172.16.1.1	137	Registration NB HARRIS-PC<20>
2018-04-24 02:25…	172.16.1.115	137	172.16.1.1	137	Registration NB HARRIS-PC<20>
2018-04-24 02:25…	172.16.1.115	137	172.16.1.1	137	Registration NB THUNDERLIFE<…
2018-04-24 02:25…	172.16.1.115	137	172.16.1.1	137	Registration NB HARRIS-PC<00>
2018-04-24 02:25…	172.16.1.115	137	172.16.1.1	137	Registration NB HARRIS-PC<00>
2018-04-24 02:25…	172.16.1.115	137	172.16.1.1	137	Registration NB THUNDERLIFE<…
2018-04-24 02:25…	172.16.1.115	137	172.16.1.1	137	Registration NB HARRIS-PC<20>
2018-04-24 02:25…	172.16.1.115	137	172.16.1.1	137	Name query NB WPAD<00>
2018-04-24 02:25…	172.16.1.115	137	172.16.1.255	137	Registration NB HARRIS-PC<20>
2018-04-24 02:25…	172.16.1.115	137	172.16.1.255	137	Registration NB THUNDERLIFE<…
2018-04-24 02:25…	172.16.1.115	137	172.16.1.255	137	Registration NB HARRIS-PC<00>
2018-04-24 02:25…	172.16.1.115	137	172.16.1.1	137	Name query NB WPAD<00>
2018-04-24 02:25…	172.16.1.115	137	172.16.1.255	137	Registration NB HARRIS-PC<00>
2018-04-24 02:25…	172.16.1.115	137	172.16.1.255	137	Registration NB THUNDERLIFE<…
2018-04-24 02:25…	172.16.1.115	137	172.16.1.255	137	Registration NB HARRIS-PC<20>
2018-04-24 02:25…	172.16.1.115	137	172.16.1.255	137	Registration NB HARRIS-PC<20>
2018-04-24 02:25…	172.16.1.115	137	172.16.1.255	137	Registration NB THUNDERLIFE<…
2018-04-24 02:25…	172.16.1.115	137	172.16.1.255	137	Registration NB HARRIS-PC<00>

Block 7 - Exercise 1 - Executive Summary

On 2018-04-24 at ***02:29*** UTC, a Windows computer used by ***Warren Harris*** showed signs of infection from a ***Formbook information stealer***.

- *Sentence: ~~origin of infection, if known~~*
- *Sentence: ~~corrective actions taken~~*

Block 7 - Exercise 1 - Details

IP address: **172.16.1.115**

MAC address: **00:50:8b:ea:40:a1**

Host name: **HARRIS-PC**

User account name: **warren.harris**

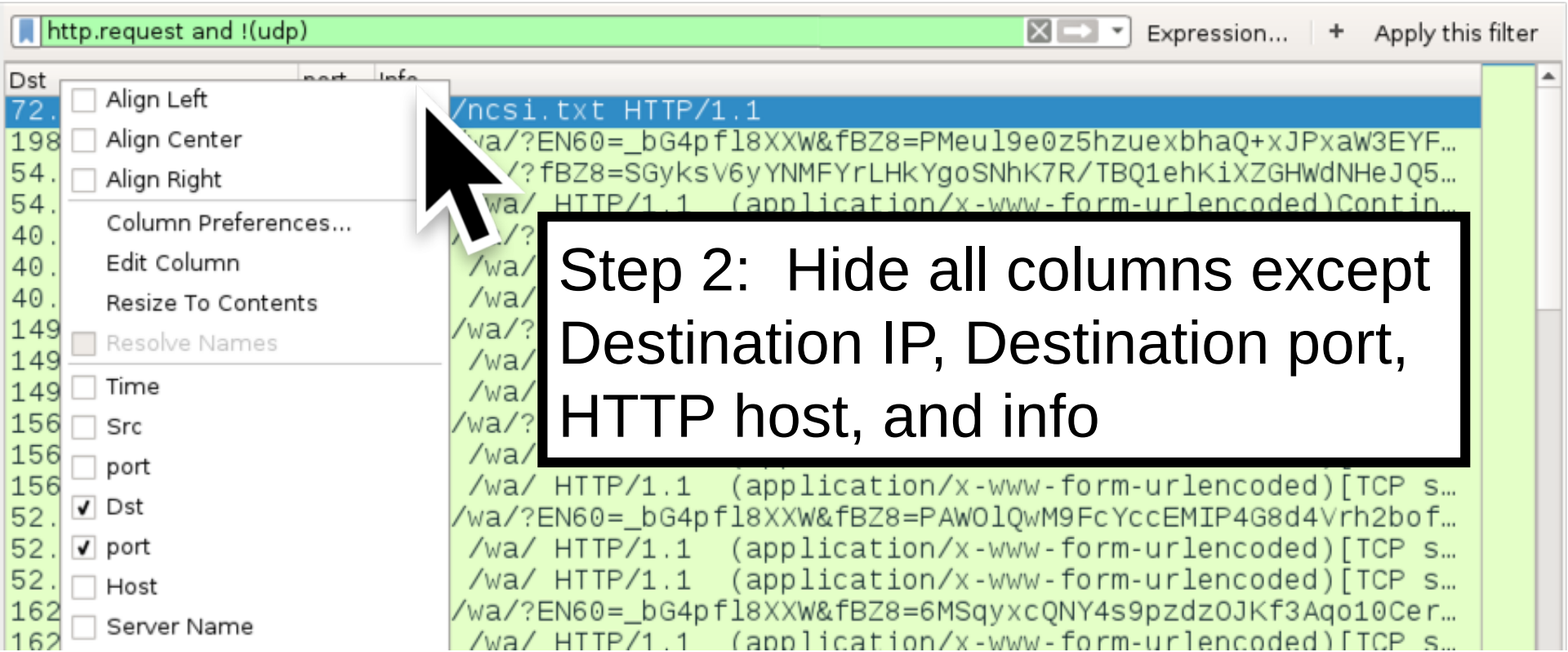
Block 7 - Exercise 1 - IOCs

PACKET DISSECTIONS

- Step 1: Filter as necessary
- Step 2: Only show columns you want to print
- Step 3: File → Export Packet Dissections → As Plain Text
- Step 4: Make sure you un-check the Details box
- Step 5: Save the packet dissections as a text file

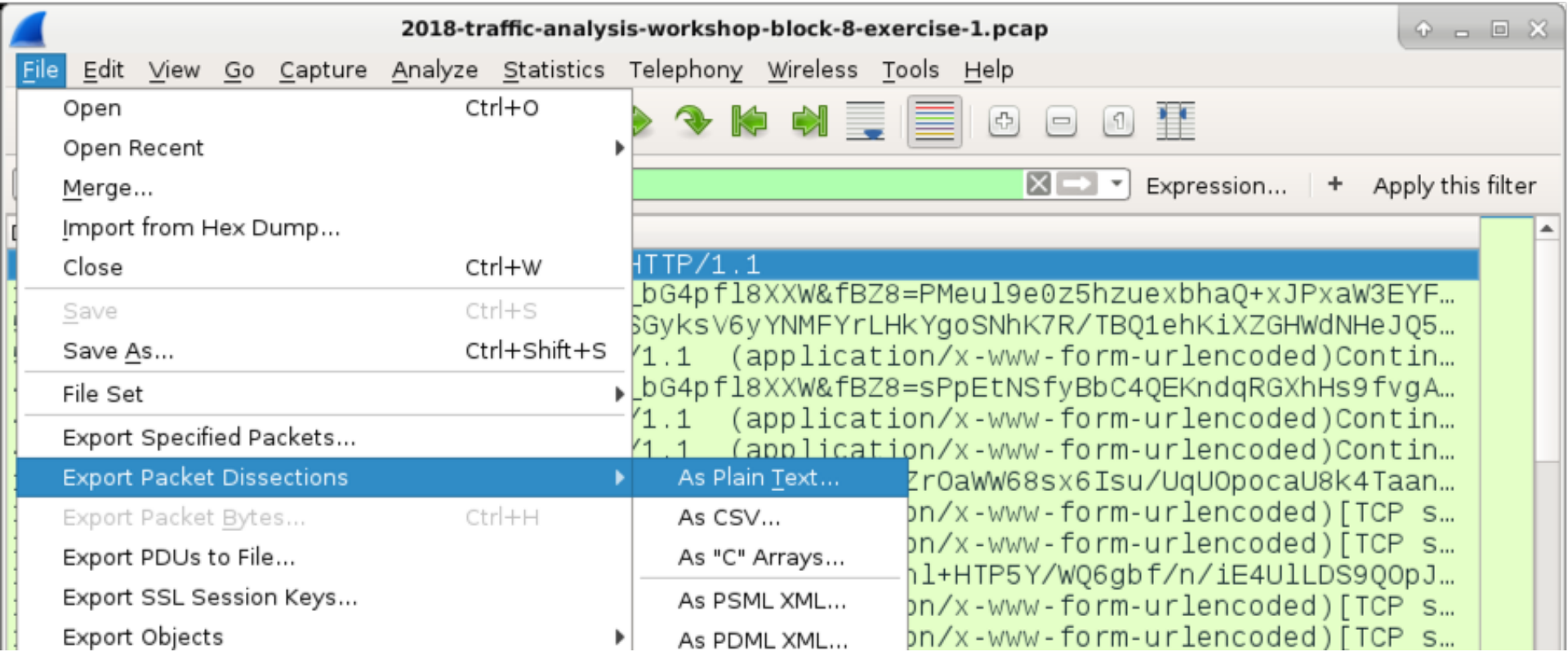
Block 7 - Exercise 1 - IOCs

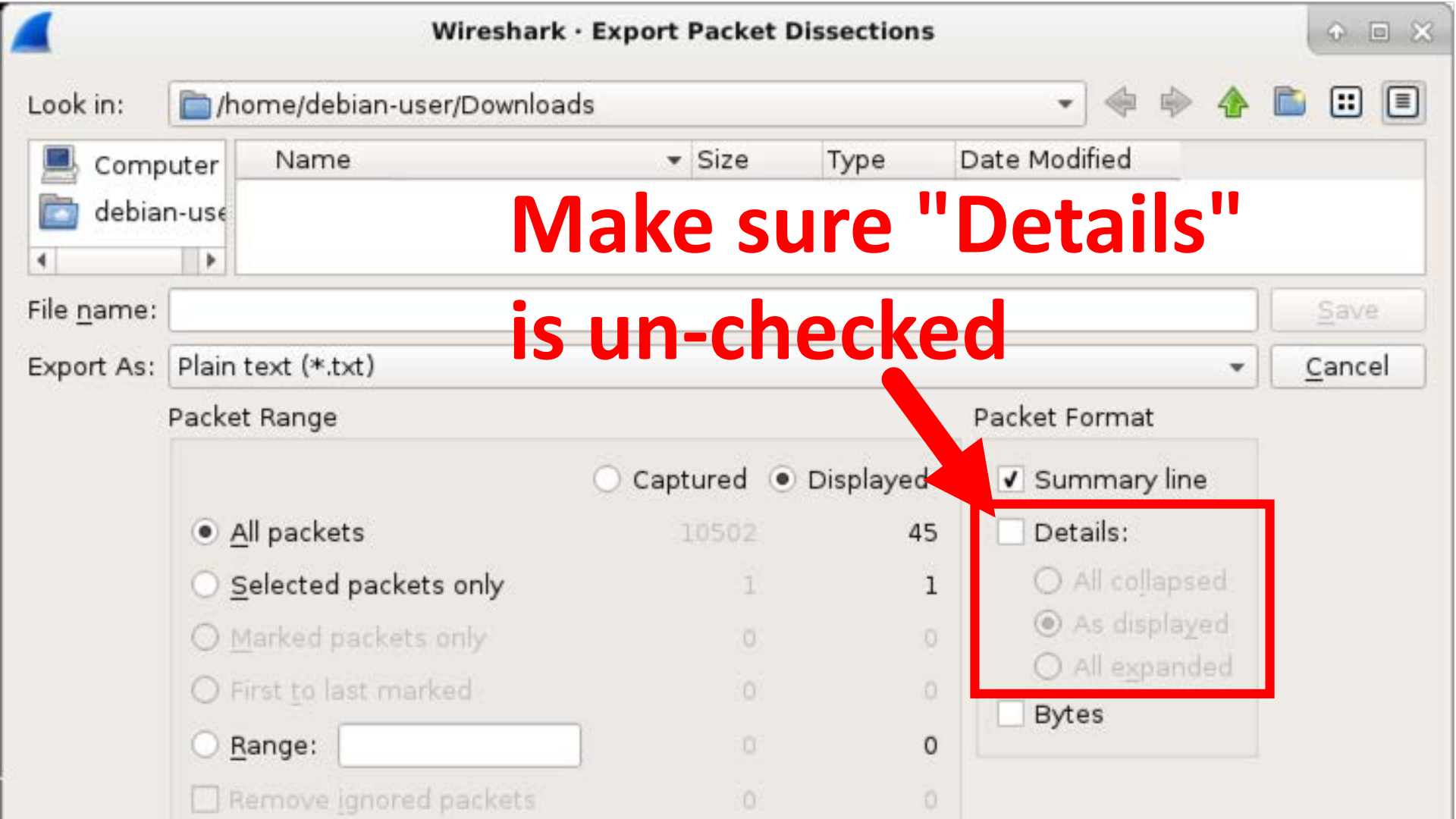
Step 1: Filter on ***http.request and !(udp)***



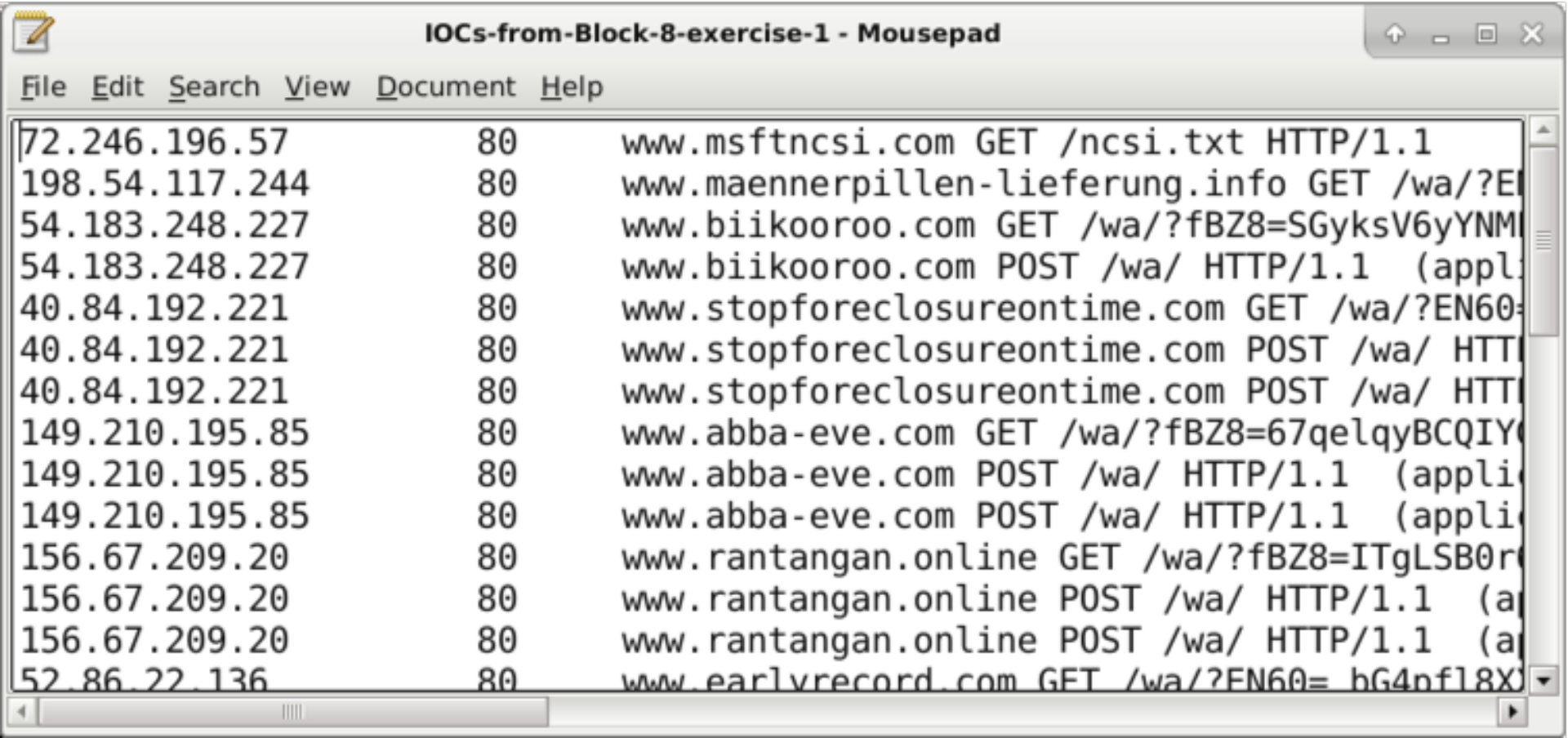
Block 7 - Exercise 1 - IOCs

Step 3: File → Export Packet Dissections → As Plain Text




Wireshark · Export Packet Dissections
Look in:
/home/debian-user/Downloads
Computer
debian-use
Name
Size
Type
Date Modified
Make sure "Details"
is un-checked
File name:
Save
Export As:
Plain text (*.txt)
Cancel
Packet Range
Captured
Displayed
All packets
10502
45
Selected packets only
1
1
Marked packets only
0
0
First to last marked
0
0
Range:
0
0
Remove ignored packets
0
0
Packet Format
Summary line
Details:
All collapsed
As displayed
All expanded
Bytes

Block 7 - Exercise 1 - IOCs



Block 7 - Exercise 1 - IOCs

198.54.117.244 port 80 - www.maennerpillen-lieferung.info - GET /wa/?[long string]
54.183.248.227 port 80 - www.biikooroo.com - GET /wa/?[long string]
54.183.248.227 port 80 - www.biikooroo.com - POST /wa/
40.84.192.221 port 80 - www.stopforeclosureontime.com - GET /wa/?[long string]
40.84.192.221 port 80 - www.stopforeclosureontime.com - POST /wa/
149.210.195.85 port 80 - www.abba-eve.com - GET /wa/?[long string]
149.210.195.85 port 80 - www.abba-eve.com - POST /wa/
156.67.209.20 port 80 - www.rantangan.online - GET /wa/?[long string]
156.67.209.20 port 80 - www.rantangan.online - POST /wa/
52.86.22.136 port 80 - www.earlyrecord.com - GET /wa/?[long string]
162.213.249.164 port 80 - www.91ruitue.com - GET /wa/?[long string]
162.213.249.164 port 80 - www.91ruitue.com - POST /wa/
205.178.189.131 port 80 - www.isidentsu.net - GET /wa/?[long string]
107.164.17.51 port 80 - www.tg88vip.com - GET /wa/?[long string]
and so on...

Block 7 - Up next...

- Incident report format
- Internal network description
- Exercise 1
- **Exercise 2**
- Exercise 3
- Exercise 4

Block 7 - Exercise 2

2018-traffic-analysis-workshop-block-7-exercise-2.pcap

On 2018-04-24 at ***??:??*** UTC, a Windows computer used by ***???*** was infected with ***???***

- *Sentence: ~~origin of infection, if known~~*
- *Sentence: ~~corrective actions taken~~*

Block 7 - Exercise 2

ALERTS

Src IP	SPort	Dst IP	DPort	Pr	Event Message
178.18.132.32	80	172.16.1.97	49201	6	ETPRO EXPLOIT Multiple Vendor Malformed ZIP Archive
202.218.245.19	80	172.16.1.97	49209	6	ET POLICY PE EXE or DLL Windows file download HTTP
202.218.245.19	80	172.16.1.97	49209	6	ET INFO Executable Retrieved With Minimal HTTP Head
202.218.245.19	80	172.16.1.97	49209	6	ET INFO EXE - Served Attached HTTP
172.16.1.97	49210	220.227.247.45	443	6	ET CNC Feodo Tracker Reported CnC Server group 14
172.16.1.97	49212	87.106.37.146	8080	6	ET CNC Feodo Tracker Reported CnC Server group 23
172.16		46	8080	6	ET POLICY HTTP Request on Unusual Port Possibly Host
172.16		46	8080	6	ETPRO TROJAN W32/Emotet.v4 Checkin
172.16		46	808	6	ETPRO TROJAN W32/Emotet.v4 Checkin 2
172.16		46	8080	6	ETPRO TROJAN W32/Emotet.v4 Checkin 3

Alerts for Emotet

Block 7 - Exercise 2 - Executive Summary

On 2018-04-24 at ***03:52*** UTC, a Windows computer used by ***Kayla Yates*** was infected with ***Emotet***

Block 7 - Exercise 2 - Details

IP address: **172.16.1.97**

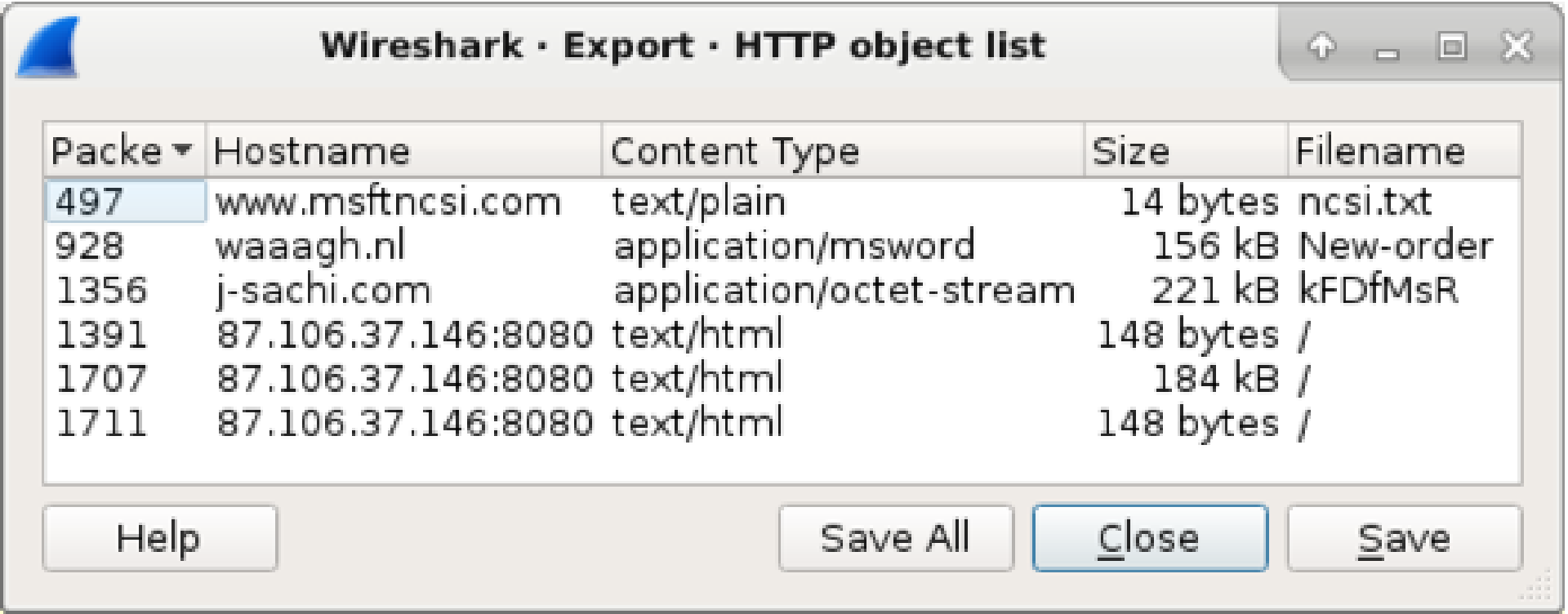
MAC address: **00:1f:cf:2e:a7:6c**

Host name: **YATES-PC**

User account name: **kayla.yates**

Block 7 - Exercise 2 - IOCs

File → Export Objects → HTTP...



Block 7 - Exercise 2 - IOCs

Export the application/msword and the application/octet-stream objects.

Do a file command on each object to confirm they are a Word document and a Windows executable.

Do the shasum -a 256 command to get the SHA256 hashes and search the hashes on Google or check them in VirusTotal.

Block 7 - Exercise 2 - IOCs

SHA256: 6082e675708630a1483130f614717dc24322c47926600228f401626cd05b5e8a
File description: Word doc with macro for Emotet

SHA256: bb12951d05e914887391fe9b023ec23600c2b200f476a61e56dd12accf7abda6
File description: Emotet binary

178.18.132.32 port 80 - **waaag.nl** - GET /New-order/
202.218.245.19 port 80 - **j-sachi.com** - GET /kDFfMsR/
87.106.37.146 port 8080 - **87.106.37.146:8080** - GET /

Block 7 - Up next...

- Incident report format
- Internal network description
- Exercise 1
- Exercise 2
- **Exercise 3**
- Exercise 4

Block 7 - Exercise 3

2018-traffic-analysis-workshop-block-7-exercise-3.pcap

On 2018-04-24 at ***??:??*** UTC, a Windows computer used by ***???*** was infected with ***???***

- *Sentence: ~~origin of infection, if known~~*
- *Sentence: ~~corrective actions taken~~*

Block 7 - Exercise 3

ALERTS

Src IP	SPort	Dst IP	DPort	Pr	Event Message
46.30.42.225	80	172.16.1.201	49200	6	ETPRO CURRENT_EVENTS RIG EK Landing Apr 04 2017 M5
46.3			9200		ET CURRENT_EVENTS SunDown EK RIP Landing M1 B641
46.3			9200	6	ETPRO CURRENT_EVENTS SunDown EK Landing Feb 13 20...
46.3			9200	6	ETPRO CURRENT_EVENTS CVE-2015-2419 M1 (b642) Obs...
46.30.42.225	80	172.16.1.201	49200	6	ET CURRENT_EVENTS SunDown EK RIP Landing M4 B641
172.16.1.201	49201	46.30.42.225	80	6	ET CURRENT_EVENTS RIG EK URI Struct Jun 13 2017
46.30.45.78	80	172.16.1.201	49197	6	ETPRO CURRENT_EVENTS BlackTDS Cookie Set
46.30.42.225	80	172.16.1.201	49200	6	ETPRO CURRENT_EVENTS RIG EK Flash Exploit Mar 29 2016
172.16.1.201	49207	66.171.248.178	80	6	ETPRO TROJAN Win32/GandCrab Ransomware IP Addres...
172.16.1.201	60939	94.249.60.127	53	17	ET TROJAN Observed GandCrab Ransomware Domain (z...

Rig EK alerts

Alerts for GandCrab ransomware

Block 7 - Exercise 3 - Executive Summary

On 2018-04-24 at ***03:27*** UTC, a Windows computer used by ***Myron Dennis*** was infected with ***GandCrab ransomware***

Block 7 - Exercise 3 - Details

IP address: **172.16.1.201**

MAC address: **b8:97:5a:d6:8a:24**

Host name: **DENNIS-PC**

User account name: **myron.dennis**

Block 7 - Exercise 3 - IOCs

46.30.45.78 port 80 - **someinit.cf** - gate to Rig EK

46.30.42.225 port 80 - **46.30.42.225** - Rig EK

DNS queries for **zonealarm.bit**

66.171.248.178 port 80 - **ransomware.bit** - Gandcrab

217.75.83.218 port 80 - **ransomware.bit** - Gandcrab

193.33.1.19 port 80 - **ransomware.bit** - Gandcrab

Block 7 - Up next...

- Incident report format
- Internal network description
- Exercise 1
- Exercise 2
- Exercise 3
- **Exercise 4**

Block 7 - Exercise 4

2018-traffic-analysis-workshop-block-7-exercise-2.pcap

On 2018-04-24 at ***??:??*** UTC, a Windows computer used by ***???*** was infected with ***???***

- *Sentence: ~~origin of infection, if known~~*
- *Sentence: ~~corrective actions taken~~*

Block 7 - Exercise 4

ALERTS

Src IP	SPort	Dst IP	DPort	Pr	Event Message
199.30.241.139	80	172.16.1.149	49199	6	ET POLICY Binary Download Smaller than 1 M...
199.30.241.139	80	172.16.1.149	49199	6	ET POLICY PE EXE or DLL Windows file downloa...
207.140.15.87	449	172.16.1.149	49204	6	ET POLICY OpenSSL Demo CA - Internet Widgit...
185.228.232.218	447	172.16.1.149	49212	6	ETPRO TROJAN Trickbot SSL Certificate Detected

Trickbot alert for IP address 172.16.1.149

Block 7 - Exercise 4

There are **two** Windows clients in this pcap.

- 172.16.1.131
- 172.16.1.149

You only need to investigate the one with the Trickbot alert.

Block 7 - Exercise 4 - Executive Summary

On 2018-04-24 at ***14:55*** UTC, a Windows computer used by ***Edwin Henderson*** was infected with ***Trickbot***

Block 7 - Exercise 4 - Details

IP address: **172.16.1.149**

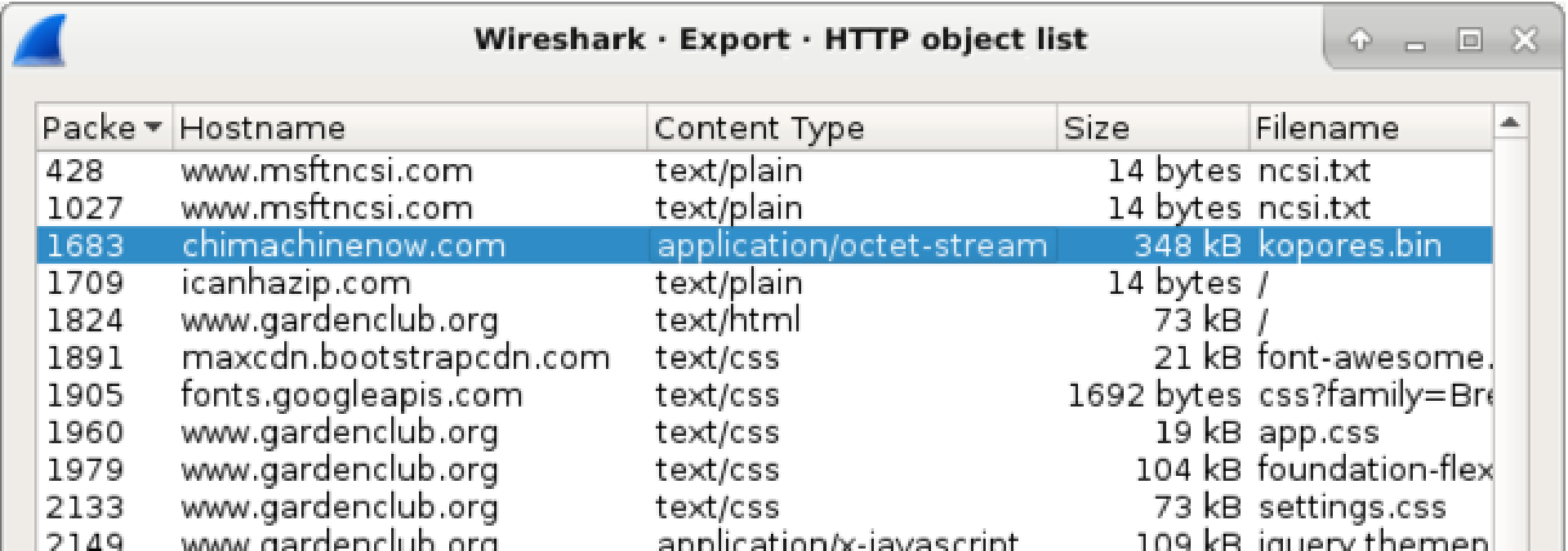
MAC address: **00:13:d4:b9:cd:56**

Host name: **HENDERSON-PC**

User account name: **edwin.henderson**

Block 7 - Exercise 4 - IOCs

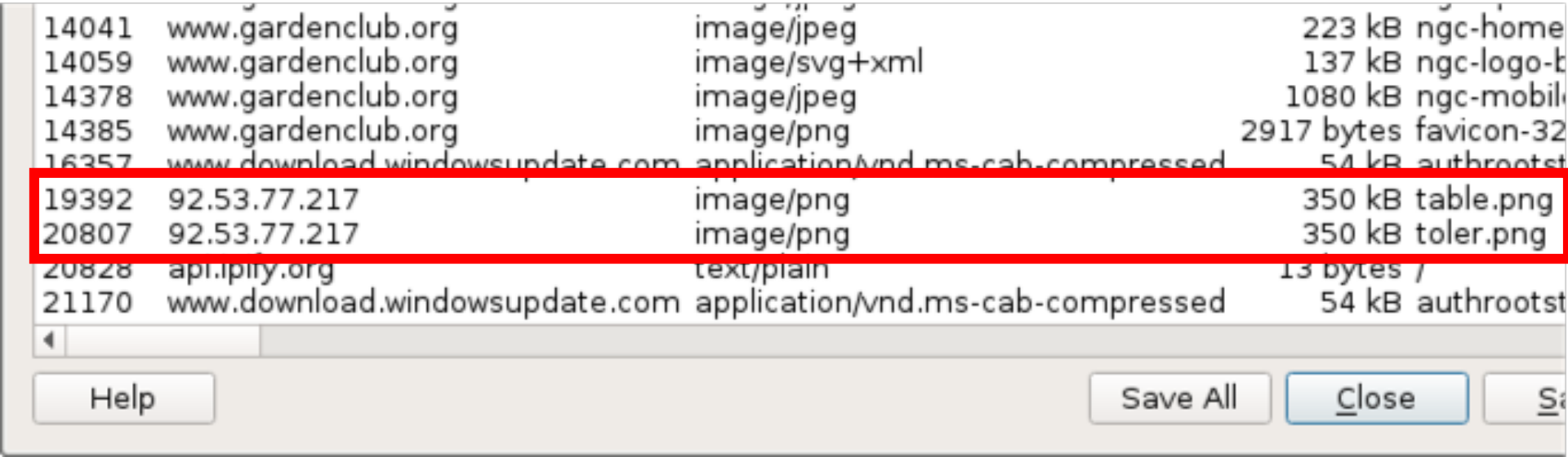
chimachinenow.com application/octet-stream 384kB kopores.bin



Block 7 - Exercise 4 - IOCs

92.53.77.217 image/png 350kB table.png

92.53.77.217 image/png 350kB toler.png



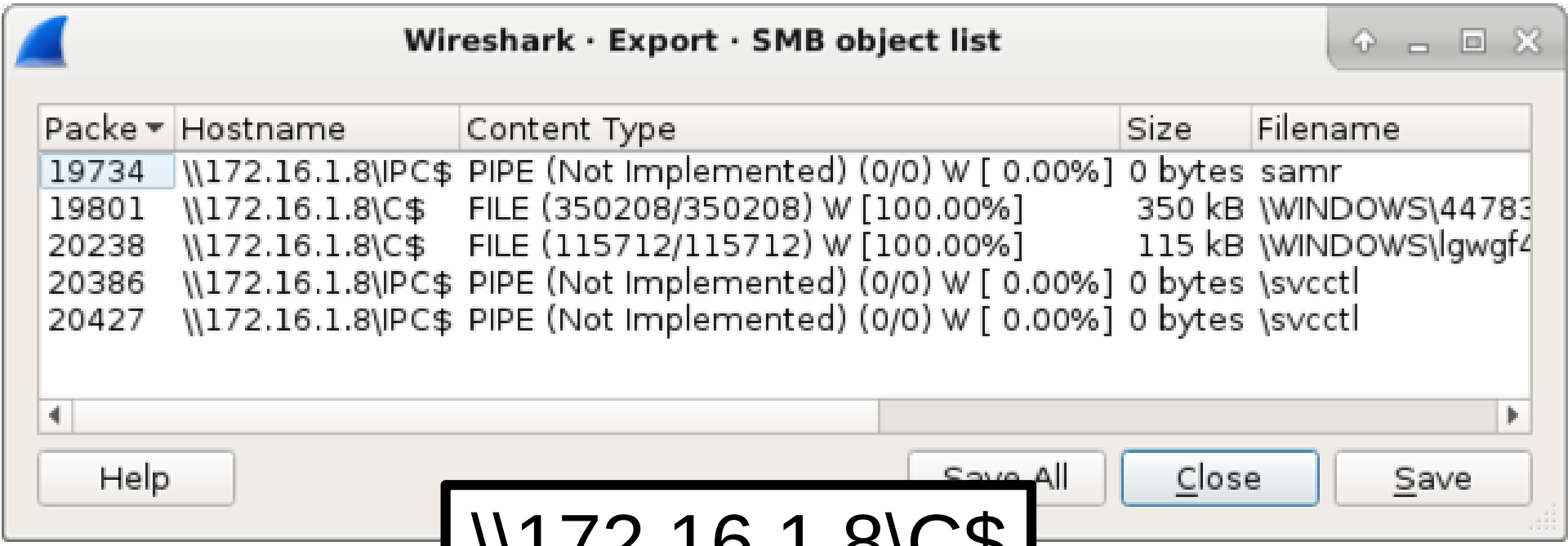
Block 7 - Exercise 4 - Additional info!

172.16.1.149 infected the domain controller at **172.16.1.8** through SMB.

Src IP	SPort	Dst IP	DPort	Event Message
172.16.1.149	49407	172.16.1.8	445	ET INFO Potentially unsafe SMBv1 protocol...
172.16.1.149	49407	172.16.1.8	445	GPL NETBIOS SMB-DS IPC$ share access
172.16.1.149	49407	172.16.1.8	445	GPL NETBIOS SMB-DS C$ share access
172.16.1.8	61708	50.19.222.19	80	ET POLICY External IP Lookup api.ipify.org
172.16.1.8	61739	80.93.182.178	447	PADS New Asset - ssl TLS 1.0 Client Hello
80.93.182.178	447	172.16.1.8	61739	ETPRO TROJAN Trickbot SSL Certificate Det...

Block 7 - Exercise 4 - Bonus!

File → Export Objects → SMB...



\\172.16.1.8\C$

Block 7 - Exercise 4 - Bonus!

ip.addr eq 172.16.1.8 and !(ip.addr eq 172.16.1.149) and !(ip.addr eq 172.16.1.131) and (http.request or ssl.handshake.type == 1)

Block 7 - Review

- Incident report format
- Internal network description
- Exercise 1
- Exercise 2
- Exercise 3
- Exercise 4

2018 TRAFFIC ANALYSIS WORKSHOP

Up next...

Block 8: Evaluation

Block 8 - Overview

2018-traffic-analysis-workshop-block-8-final-exercise.pcap

- Network segment parameters
- Host and user identification
- Evaluation: find the malicious traffic
- Review

Network segment parameters

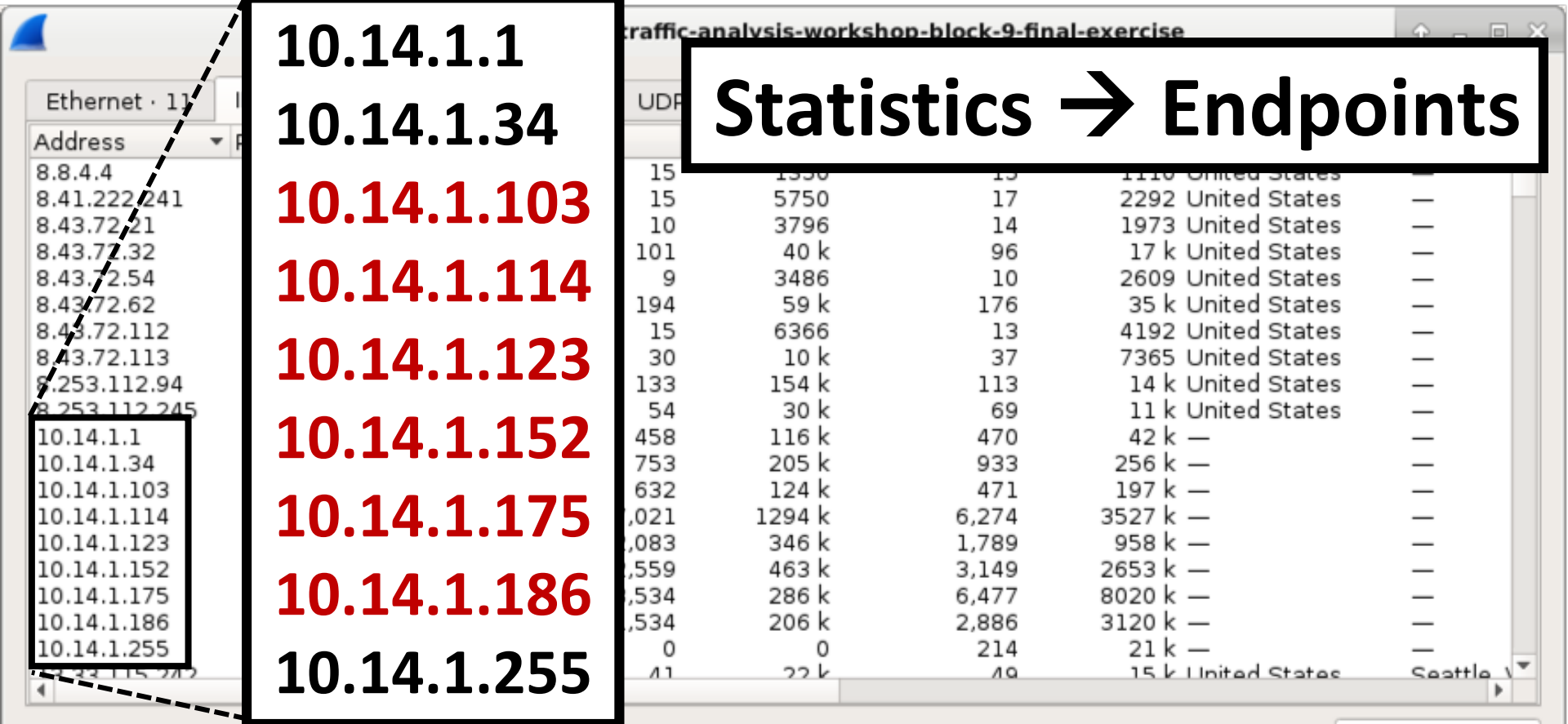
- Domain: **apox-sports.com**
- Network segment: **10.14.1.0/24**
- Domain controller: **10.14.1.34**
  APOX-SPORTS-DC
- Segment gateway: **10.14.1.1**
- Broadcast address: **10.14.1.255**

Up next...

2018-traffic-analysis-workshop-block-8-final-exercise.pcap

- Network segment parameters
- **Host and user identification**
- Evaluation: find the malicious traffic
- Review

Host and user identification



Up next...

2018-traffic-analysis-workshop-block-8-final-exercise.pcap

- Network segment parameters
- Host and user identification
- **Evaluation: find the malicious traffic**
- Review

Evaluation

Of the six hosts, figure out which one has malicious activity or an infection. Hint: focus on the Windows clients.

Evaluation

185.16.41.95 over TCP port 80

Alerts:

- **ET TROJAN KINS/ZeusVM Variant Retrieving Config**
- **ET TROJAN Trojan Generic - POST to gate.php with no referer**
- **ETPRO TROJAN Win32/Terdot.A / ZLoader Checkin**

Up next...

2018-traffic-analysis-workshop-block-8-final-exercise.pcap

- Network segment parameters
- Host and user identification
- Evaluation: find the malicious traffic
- **Review**

Review

The six clients

10.14.1.103 - Vienna-8C57-PC - earnestine.matsuoka
10.14.1.114 - MacBook Pro (macOS)
10.14.1.123 - Samsung Galaxy S6 (Android 7.0)
10.14.1.152 - Tacoma-f82c-PC - stanley.debenham
10.14.1.175 - Austin-4fb2-PC - unknown user
10.14.1.186 - Albany-635e-PC - yarik.rhodes

Evaluation

185.16.41.95 over TCP port 80

Alerts:

- **ET TROJAN KINS/ZeusVM Variant Retrieving Config**
- **ET TROJAN Trojan Generic - POST to gate.php with no referer**
- **ETPRO TROJAN Win32/Terdot.A / ZLoader Checkin**

Review

http.request and ip.addr eq 185.16.41.95

Expression... +

Time	Dst	port	Host	Info
2018-02-10 23:52:34	185.16.41.95	80	munachi.ru	GET /ratty/config.jpg H…
2018-02-10 23:52:43	185.16.41.95	80	munachi.ru	POST /ratty/gate.php HT…
2018-02-10 23:53:43	185.16.41.95	80	munachi.ru	GET /ratty/config.jpg H…
2018-02-10 23:53:44	185.16.41.95	80	munachi.ru	POST /ratty/gate.php HT…
2018-02-10 23:54:45	185.16.41.95	80	munachi.ru	GET /ratty/config.jpg H…
2018-02-10 23:54:46	185.16.41.95	80	munachi.ru	POST /ratty/gate.php HT…
2018-02-10 23:55:47	185.16.41.95	80	munachi.ru	GET /ratty/config.jpg H…
2018-02-10 23:55:48	185.16.41.95	80	munachi.ru	POST /ratty/gate.php HT…
2018-02-10 23:56:48	185.16.41.95	80	munachi.ru	GET /ratty/config.jpg H…
2018-02-10 23:56:49	185.16.41.95	80	munachi.ru	POST /ratty/gate.php HT…
2018-02-10 23:57:50	185.16.41.95	80	munachi.ru	GET /ratty/config.jpg H…
2018-02-10 23:57:51	185.16.41.95	80	munachi.ru	POST /ratty/gate.php HT…
2018-02-10 23:58:52	185.16.41.95	80	munachi.ru	GET /ratty/config.jpg H…

Review

The six clients

10.14.1.103 - Vienna-8C57-PC - earnestine.matsuoka

10.14.1.114 - MacBook Pro (macOS)

10.14.1.123 - Samsung Galaxy S6 (Android 7.0)

10.14.1.152 - Tacoma-f82c-PC - stanley.debenham

10.14.1.175 - Austin-4fb2-PC - unknown user

10.14.1.186 - Albany-635e-PC - yarik.rhodes

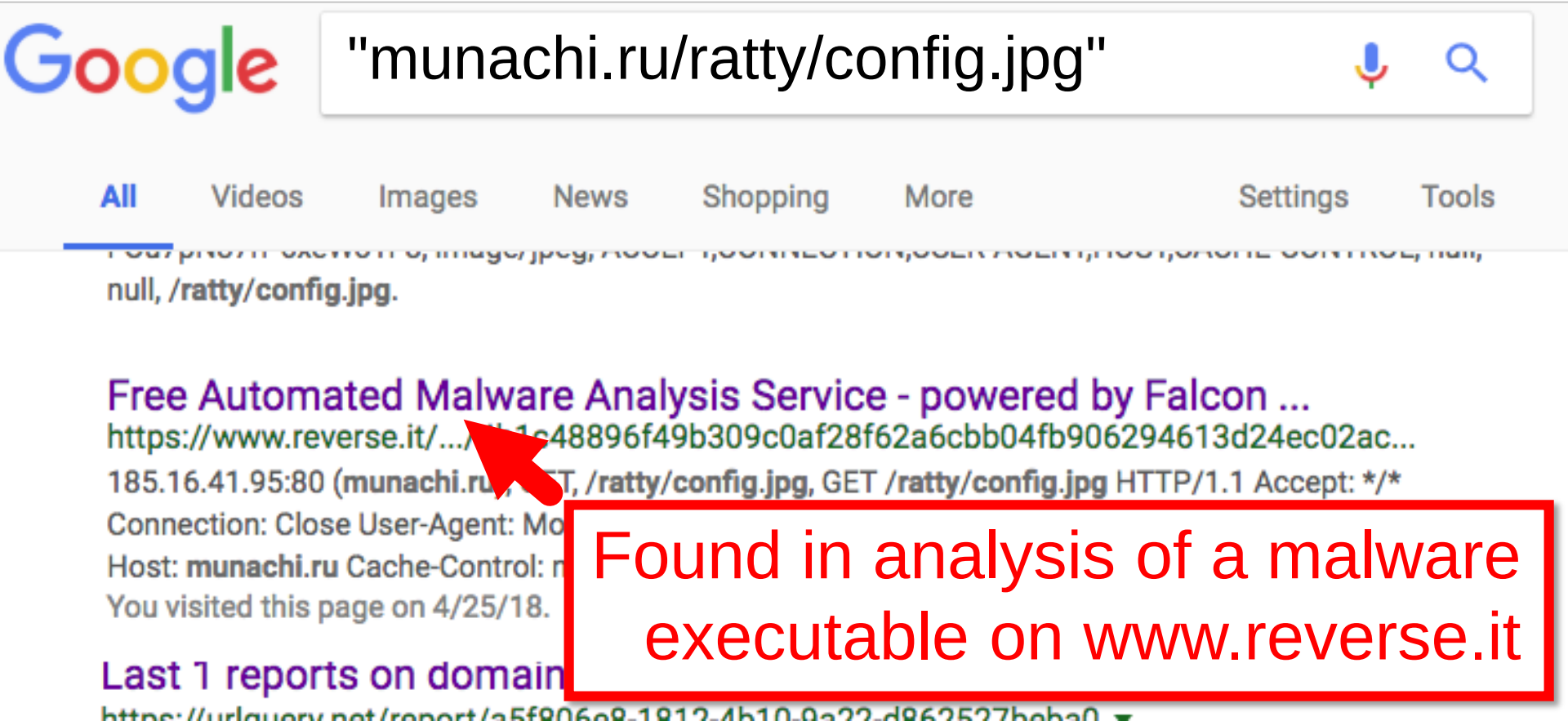
Review

Suspicious URLs

- **munachi.ru - GET /ratty/config.jpg**
- **munachi.ru - GET /ratty/gate.php**

Look up the info on Google!

The malicious traffic



The malicious traffic

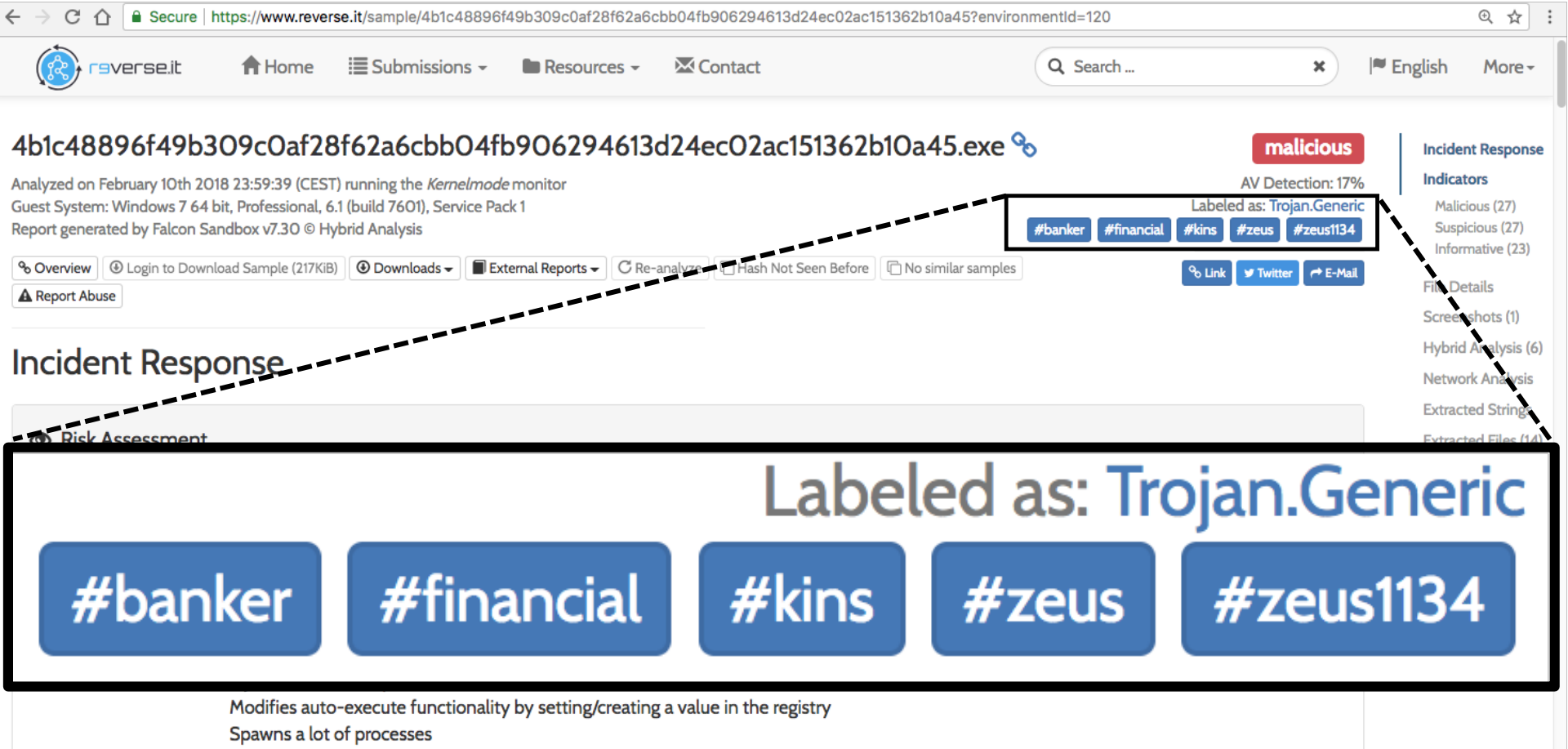
Analysis for this executable has the same traffic seen in our pcap.

HTTP Traffic

S3WnKX734%3D

185.16.41.95:80 (munachi.ru)	POST	/ratty/gate.php	POST /ratty/gate.php HTTP/1.1 Accept: */* Cache-Control: no-cache User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: munachi.ru Content-Length: 345 Connection: Close More Details
185.16.41.95:80 (munachi.ru)	GET	/ratty/config.jpg	GET /ratty/config.jpg HTTP/1.1 Accept: */* Connection: Close User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: munachi.ru Cache-Control: no-cache More Details
185.16.41.95:80 (munachi.ru)	POST	/ratty/gate.php	POST /ratty/gate.php HTTP/1.1 Accept: */* Cache-Control: no-cache User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: munachi.ru Content-Length: 345 Connection:

Review


Secure | https://www.reverse.it/sample/4b1c48896f49b309c0af28f62a6cbb04fb906294613d24ec02ac151362b10a45?environmentId=120
reverse.it
Home
Submissions
Resources
Contact
Search ...
English
More
4b1c48896f49b309c0af28f62a6cbb04fb906294613d24ec02ac151362b10a45.exe
malicious
Analyzed on February 10th 2018 23:59:39 (CEST) running the Kernelmode monitor
Guest System: Windows 7 64 bit, Professional, 6.1 (build 7601), Service Pack 1
Report generated by Falcon Sandbox v7.30 © Hybrid Analysis
AV Detection: 17%
Labeled as: Trojan.Generic
#banker #financial #kins #zeus #zeus1134
Overview
Login to Download Sample (217KiB)
Downloads
External Reports
Re-analyze
Hash Not Seen Before
No similar samples
Report Abuse
Link
Twitter
E-Mail
Incident Response
Indicators
Malicious (27)
Suspicious (27)
Informative (23)
File Details
Screenshots (1)
Hybrid Analysis (6)
Network Analysis
Extracted Strings
Extracted Files (14)
Incident Response
Risk Assessment
Labeled as: Trojan.Generic
#banker
#financial
#kins
#zeus
#zeus1134
Modifies auto-execute functionality by setting/creating a value in the registry
Spawns a lot of processes

Review

EXECUTIVE SUMMARY

On 2018-02-10 at ***23:52*** UTC, a Windows computer used by ***Stanley Debanham*** generated network traffic indicating it was infected with ***banking malware***.

- *Sentence: Origin of infection is unknown.*
- *Sentence: host was wiped / re-imaged, etc.*

Review

DETAILS

IP address: **10.14.1.152**

MAC address: **00:14:38:1a:d8:66**

Host name: **Tacoma-f82c-PC**

User account name: **stanley.debanham**

Review

INDICATORS

IP address, domain, and URLS:

- 185.16.41.95 - munachi.ru - GET /ratty/config.jpg
- 185.16.41.95 - munachi.ru - GET /ratty/gate.php

SHA256 has of related executable:

- 4b1c48896f49b309c0af28f62a6cbb04fb906294613d24ec02ac151362b10a45

Block 8 - Review

2018-traffic-analysis-workshop-block-8-final-exercise.pcap

- Network segment parameters
- Host and user identification
- Evaluation: find the malicious traffic
- Review

2018 TRAFFIC ANALYSIS WORKSHOP

Congratulations!

You have finished the 2018 Traffic Analysis Workshop!

Brad Duncan
Threat Intelligence Analyst
@malware_traffic

unit42