

2018 TRAFFIC ANALYSIS WORKSHOP

**[http://malware-traffic-analysis.net/2018/
workshop/AusCERT/](http://malware-traffic-analysis.net/2018/workshop/AusCERT/)**

Brad Duncan
Threat Intelligence Analyst
@malware_traffic



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

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help									
Apply a display filter ... <Ctrl-/> Expression...									
No.	Time	Source	Destination	Protocol	Length	Info			
1	0.000000	10.5.11.101	95.142.39.26	TCP	66	49220 → 80	[SYN]	Seq=0	W
2	0.257271	95.142.39.26	10.5.11.101	TCP	60	80 → 49220	[SYN, ACK]	Se	
3	0.257563	10.5.11.101	95.142.39.26	TCP	60	49220 → 80	[ACK]	Seq=1	A
4	0.257844	10.5.11.101	95.142.39.26	HTTP	709	GET /?MzMzNDIy&kWGaPc&Ur			
5	0.257847	95.142.39.26	10.5.11.101	TCP	60	80 → 49220	[ACK]	Seq=1	A
6	0.761309	95.142.39.26	10.5.11.101	TCP	1436	80 → 49220	[PSH, ACK]	Se	
7	0.761448	10.5.11.101	95.142.39.26	TCP	60	49220 → 80	[ACK]	Seq=656	
8	0.769384	95.142.39.26	10.5.11.101	TCP	1436	80 → 49220	[PSH, ACK]	Se	
9	0.769560	10.5.11.101	95.142.39.26	TCP	60	49220 → 80	[ACK]	Seq=656	

Network Security Monitoring (NSM)

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

The image shows a Wireshark packet capture interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons. A display filter bar shows 'Apply a display filter ... <Ctrl-/>'. The main packet list table is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.5.11.101	95.142.39.26	TCP	66	49220 → 80 [SYN] Seq=0
2	0.257271	95.142.39.26	10.5.11.101	TCP	60	80 → 49220 [SYN, ACK] Seq=1
3	0.257563	10.5.11.101	95.142.39.26	TCP	60	49220 → 80 [ACK] Seq=1
4	0.257563	10.5.11.101	95.142.39.26	HTTP	709	GET /?M...
5	0.257563	10.5.11.101	95.142.39.26	TCP	60	80 → 49220 [SYN] Seq=0
6	0.761309	95.142.39.26	10.5.11.101	TCP	36	80 → 49220 [SYN, ACK] Seq=1
7	0.761448	10.5.11.101	95.142.39.26	TCP	60	49220 → 80 [ACK] Seq=1
8	0.761448	95.142.39.26	10.5.11.101	TCP	36	80 → 49220 [ACK] Seq=1

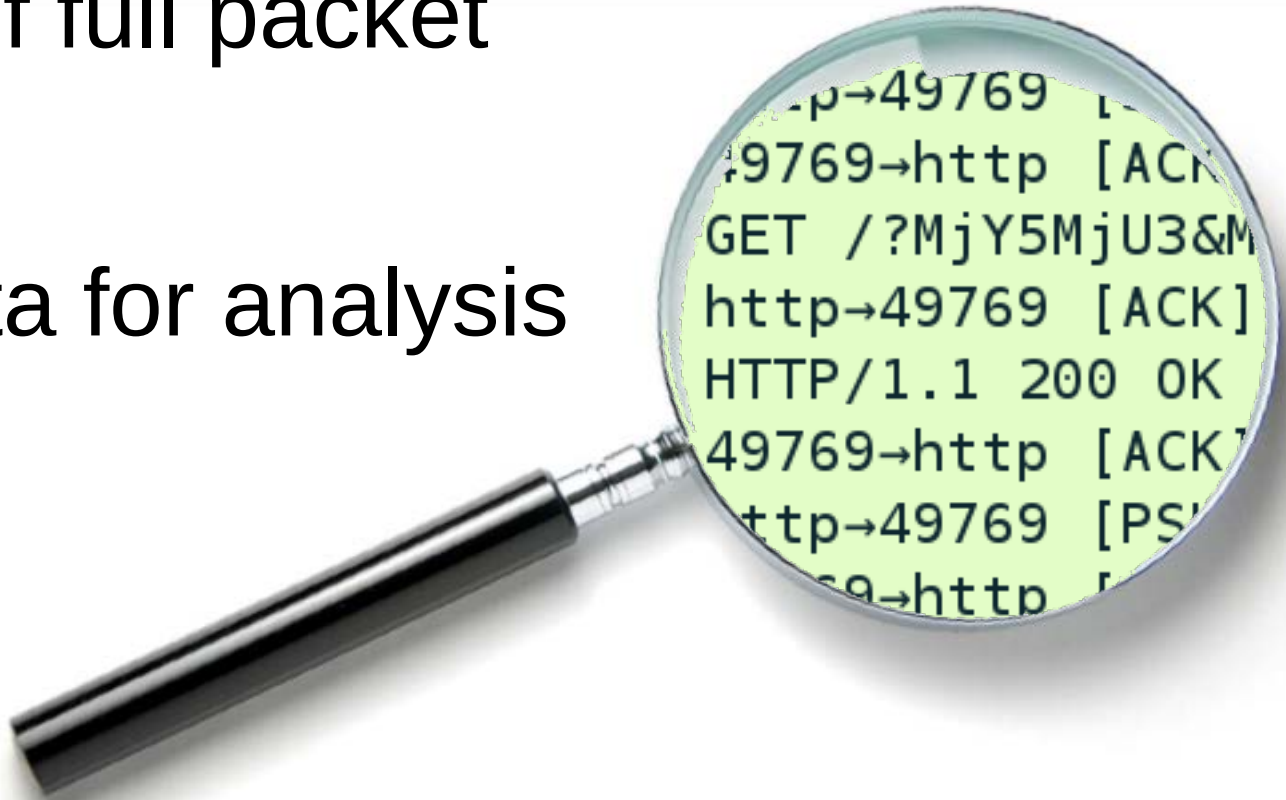
Annotations in the image include:

- A dashed line connecting the source IP '10.5.11.101' in packet 1 to a box labeled '10.5.11.101'.
- A dashed line connecting the destination IP '95.142.39.26' in packet 1 to a box labeled '95.142.39.26'.
- A dashed line connecting the protocol 'TCP' in packet 1 to a box labeled 'TCP'.
- A dashed line connecting the protocol 'HTTP' in packet 4 to a box labeled 'HTTP'.
- A dashed line connecting the protocol 'TCP' in packet 5 to a box labeled 'TCP'.
- A dashed line connecting the protocol 'TCP' in packet 6 to a box labeled 'TCP'.
- A dashed line connecting the protocol 'TCP' in packet 7 to a box labeled 'TCP'.
- A dashed line connecting the protocol 'TCP' in packet 8 to a box labeled 'TCP'.

Network Security Monitoring (NSM)

Benefit of full packet
capture:

More data for analysis





Network Security Monitoring (NSM)

Drawback of full packet capture:

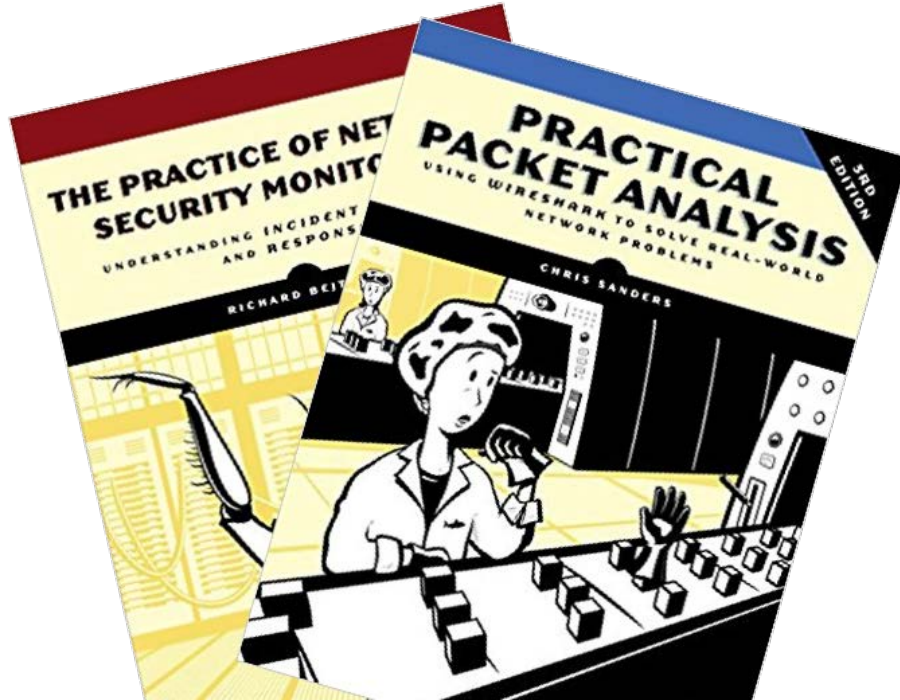
More data to store





Network Security Monitoring (NSM)

Final drawback of full packet capture:



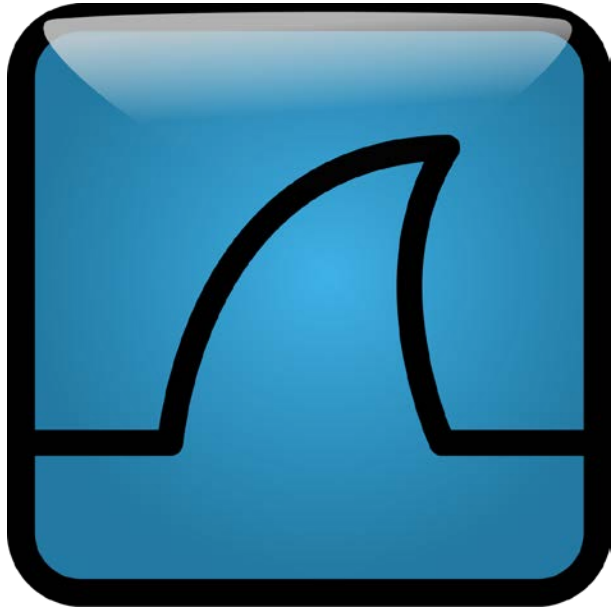
The need for
trained or
experienced
personnel

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



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

MALWARE-TRAFFIC-ANALYSIS.NET



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

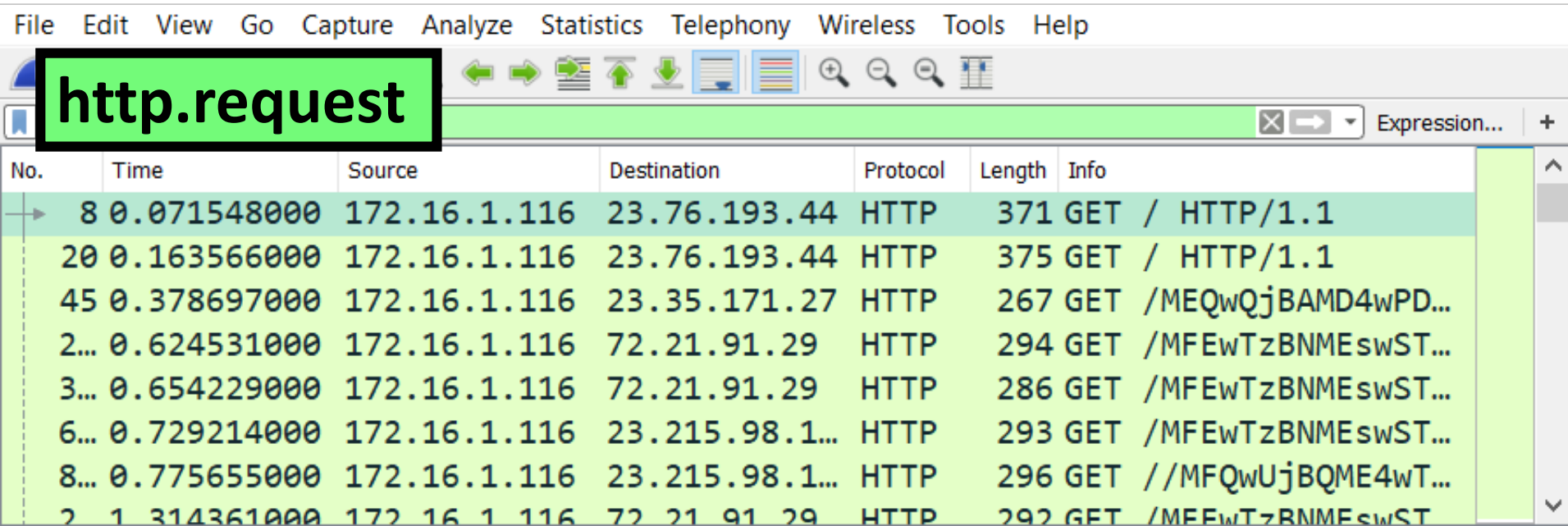
- Click on the appropriate year for the blog posts I've done - [**2013**] - [**2014**] - [**2015**] - [**2016**] - [**2017**] - [**2018**]

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



The image shows the Wireshark network protocol analyzer interface. The menu bar at the top includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for navigation and analysis. A green filter box on the left contains the text **http.request**. The packet list pane on the right displays a table of captured packets, with the first packet selected. The table has columns for No., Time, Source, Destination, Protocol, Length, and Info. The first packet is an HTTP GET request to / HTTP/1.1 from 172.16.1.116 to 23.76.193.44.

No.	Time	Source	Destination	Protocol	Length	Info
8	0.071548000	172.16.1.116	23.76.193.44	HTTP	371	GET / HTTP/1.1
20	0.163566000	172.16.1.116	23.76.193.44	HTTP	375	GET / HTTP/1.1
45	0.378697000	172.16.1.116	23.35.171.27	HTTP	267	GET /MEQwQjBAMD4wPD...
2...	0.624531000	172.16.1.116	72.21.91.29	HTTP	294	GET /MFEwTzBNMEswST...
3...	0.654229000	172.16.1.116	72.21.91.29	HTTP	286	GET /MFEwTzBNMEswST...
6...	0.729214000	172.16.1.116	23.215.98.1...	HTTP	293	GET /MFEwTzBNMEswST...
8...	0.775655000	172.16.1.116	23.215.98.1...	HTTP	296	//MFQwUjBQME4wT...
2	1.314361000	172.16.1.116	72.21.91.29	HTTP	292	GET /MFEwTzBNMEswST...

Web traffic & default Wireshark display

What should we see instead?

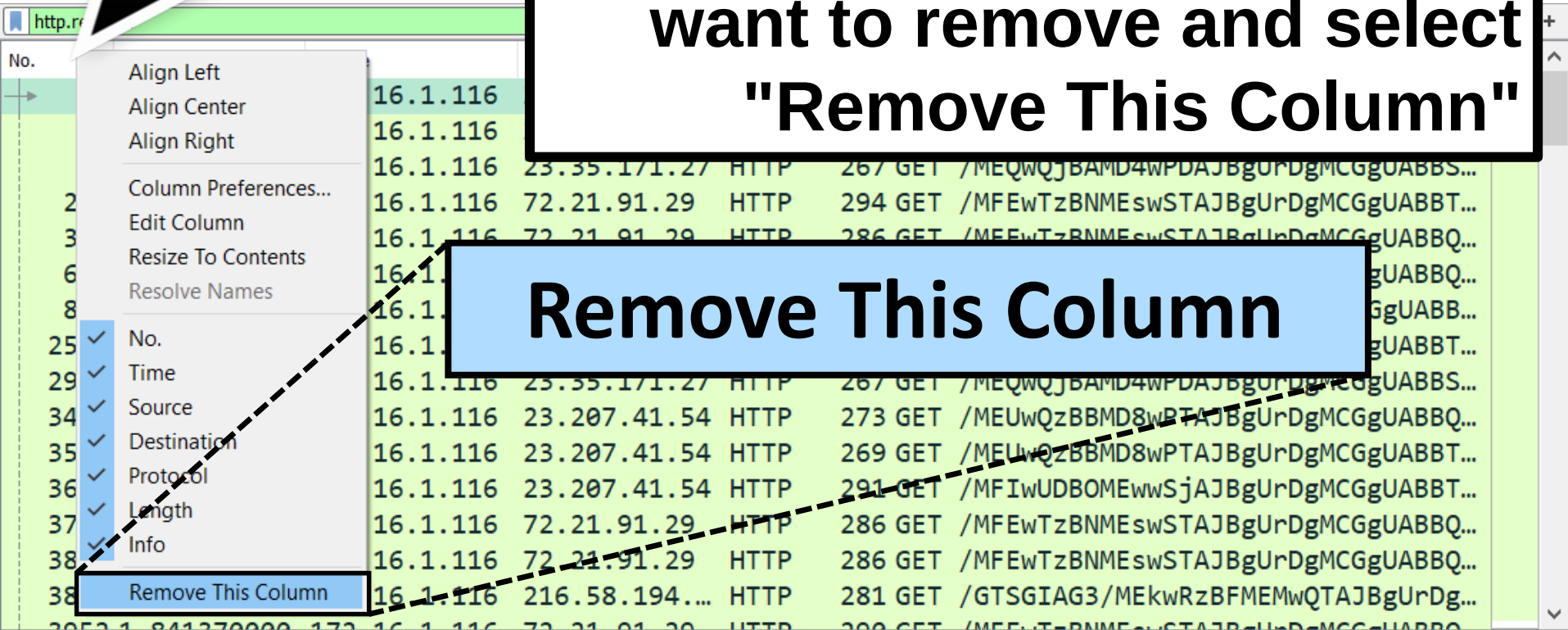
- Date & time in UTC
- Source IP and source port
- Destination IP and destination port
- HTTP host
- HTTPS server
- Info

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"



The screenshot shows a network log viewer interface. A context menu is open over the 'No.' column header, which is highlighted in blue. The menu options are: Align Left, Align Center, Align Right, Column Preferences..., Edit Column, Resize To Contents, Resolve Names, No. (checked), Time (checked), Source (checked), Destination (checked), Protocol (checked), Length (checked), Info (checked), and Remove This Column (highlighted in blue). A dashed line points from the 'Remove This Column' option to a blue box containing the text 'Remove This Column'. The background shows a list of network log entries with columns for No., Time, Source, Destination, Protocol, Length, and Info.

No.	Time	Source	Destination	Protocol	Length	Info
16.1.116	16.1.116	16.1.116	23.35.17/1.27	HTTP	267	GET /MEQWQJBAMD4WPDAJBgUrDgMCGgUABBS...
16.1.116	16.1.116	16.1.116	72.21.91.29	HTTP	294	GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBT...
16.1.116	16.1.116	16.1.116	72.21.91.29	HTTP	286	GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBT...
16.1.116	16.1.116	16.1.116	23.207.41.54	HTTP	273	GET /MEUwQzBBMD8wPTAJBgUrDgMCGgUABBT...
16.1.116	16.1.116	16.1.116	23.207.41.54	HTTP	269	GET /MEUwQzBBMD8wPTAJBgUrDgMCGgUABBT...
16.1.116	16.1.116	16.1.116	23.207.41.54	HTTP	291	GET /MFIwUDBOMEwwSjAJBgUrDgMCGgUABBT...
16.1.116	16.1.116	16.1.116	72.21.91.29	HTTP	286	GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBT...
16.1.116	16.1.116	16.1.116	72.21.91.29	HTTP	286	GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBT...
16.1.116	16.1.116	16.1.116	216.58.194....	HTTP	281	GET /GTSGIAG3/MEkwRzBFMEMwQTAJBgUrDg...

Removing columns

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

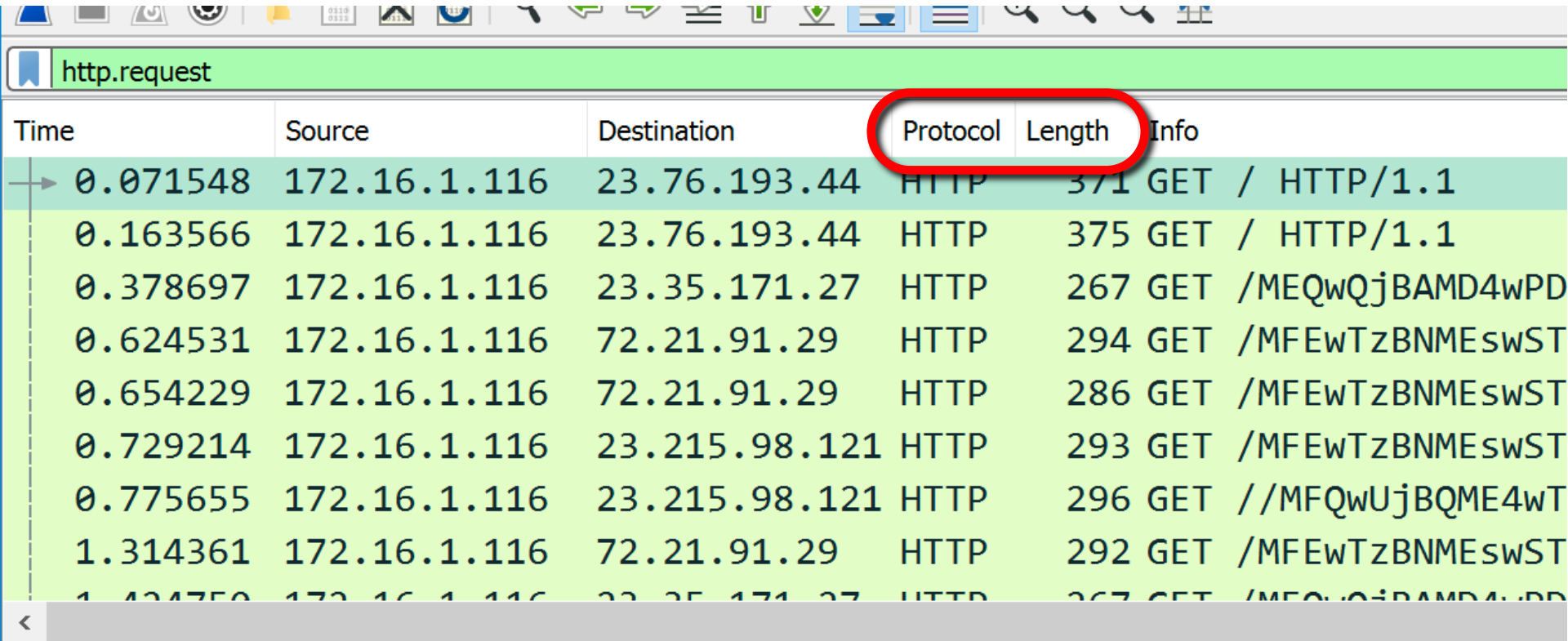


http.request

Time	Source	Destination	Protocol	Length	Info
0.071548	172.16.1.116	23.76.193.44	HTTP	371	GET / HTTP/1.1
0.163566	172.16.1.116	23.76.193.44	HTTP	375	GET / HTTP/1.1
0.378697	172.16.1.116	23.35.171.27	HTTP	267	GET /MEQwQjBAMD4wPD
0.624531	172.16.1.116	72.21.91.29	HTTP	294	GET /MFEwTzBNMEswST
0.654229	172.16.1.116	72.21.91.29	HTTP	286	GET /MFEwTzBNMEswST
0.729214	172.16.1.116	23.215.98.121	HTTP	293	GET /MFEwTzBNMEswST
0.775655	172.16.1.116	23.215.98.121	HTTP	296	GET //MFQwUjBQME4wT
1.314361	172.16.1.116	72.21.91.29	HTTP	292	GET /MFEwTzBNMEswST
1.424750	172.16.1.116	23.35.171.27	HTTP	267	GET /MEQwQjBAMD4wPD

Removing columns

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

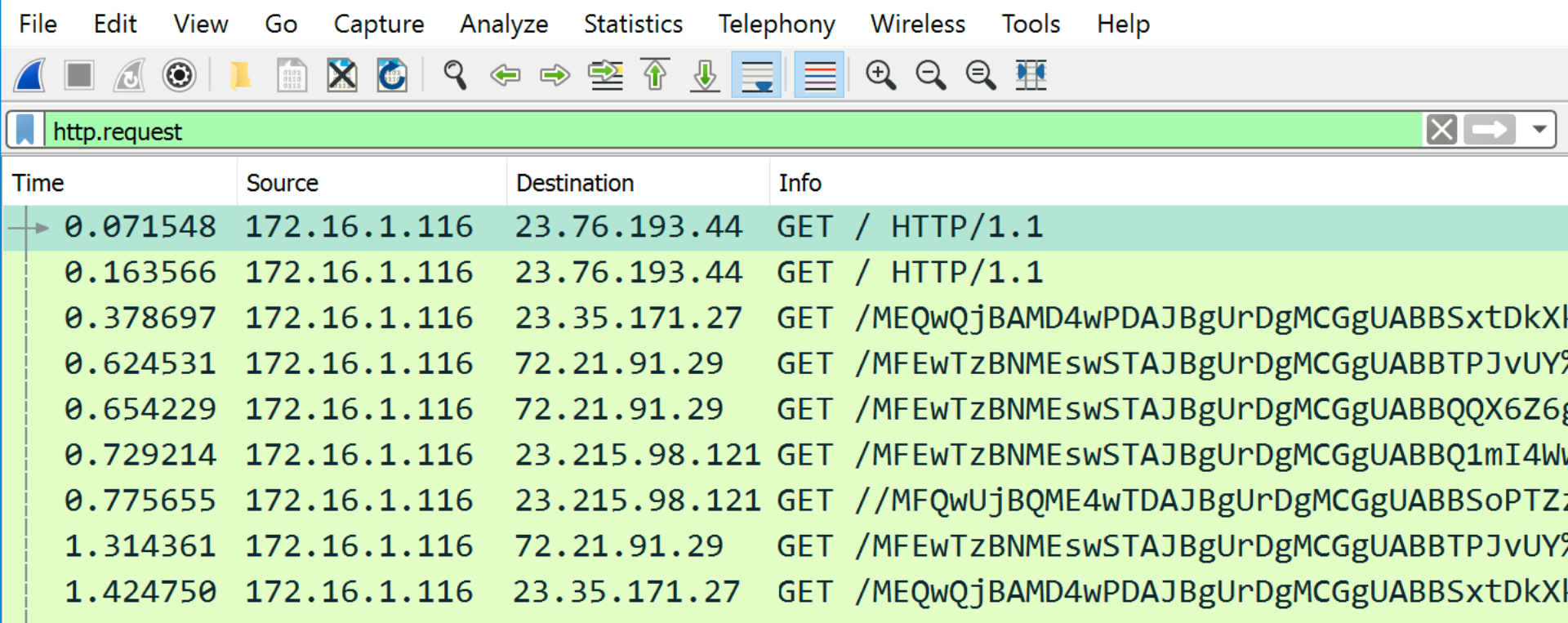


The image shows a Wireshark packet capture window for 'http.request'. The packet list table is displayed with the following columns: Time, Source, Destination, Protocol, Length, and Info. The 'Protocol' and 'Length' columns are circled in red, indicating they are the focus of the 'Removing columns' action.

Time	Source	Destination	Protocol	Length	Info
0.071548	172.16.1.116	23.76.193.44	HTTP	371	GET / HTTP/1.1
0.163566	172.16.1.116	23.76.193.44	HTTP	375	GET / HTTP/1.1
0.378697	172.16.1.116	23.35.171.27	HTTP	267	GET /MEQwQjBAMD4wPD
0.624531	172.16.1.116	72.21.91.29	HTTP	294	GET /MFEwTzBNMEswST
0.654229	172.16.1.116	72.21.91.29	HTTP	286	GET /MFEwTzBNMEswST
0.729214	172.16.1.116	23.215.98.121	HTTP	293	GET /MFEwTzBNMEswST
0.775655	172.16.1.116	23.215.98.121	HTTP	296	GET //MFQwUjBQME4wT
1.314361	172.16.1.116	72.21.91.29	HTTP	292	GET /MFEwTzBNMEswST
1.424750	172.16.1.116	23.35.171.27	HTTP	267	GET /MEQwQjBAMD4wPD

Removing columns

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



The image shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for file operations, navigation, and analysis. The packet list pane shows a single packet selected, with the address bar displaying 'http.request'. The main packet list table is visible, showing columns for Time, Source, Destination, and Info. The table contains 9 rows of data, representing HTTP requests from 172.16.1.116 to various destinations.

Time	Source	Destination	Info
0.071548	172.16.1.116	23.76.193.44	GET / HTTP/1.1
0.163566	172.16.1.116	23.76.193.44	GET / HTTP/1.1
0.378697	172.16.1.116	23.35.171.27	GET /MEQwQjBAMD4wPDAJBgUrDgMCGgUABBSxtDkXl
0.624531	172.16.1.116	72.21.91.29	GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTPJvUY%
0.654229	172.16.1.116	72.21.91.29	GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBQQX6Z6g
0.729214	172.16.1.116	23.215.98.121	GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ1mI4Ww
0.775655	172.16.1.116	23.215.98.121	GET //MFQwUjBQME4wTDAJBgUrDgMCGgUABBSOPTYZ
1.314361	172.16.1.116	72.21.91.29	GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTPJvUY%
1.424750	172.16.1.116	23.35.171.27	GET /MEQwQjBAMD4wPDAJBgUrDgMCGgUABBSxtDkXl

Adding columns

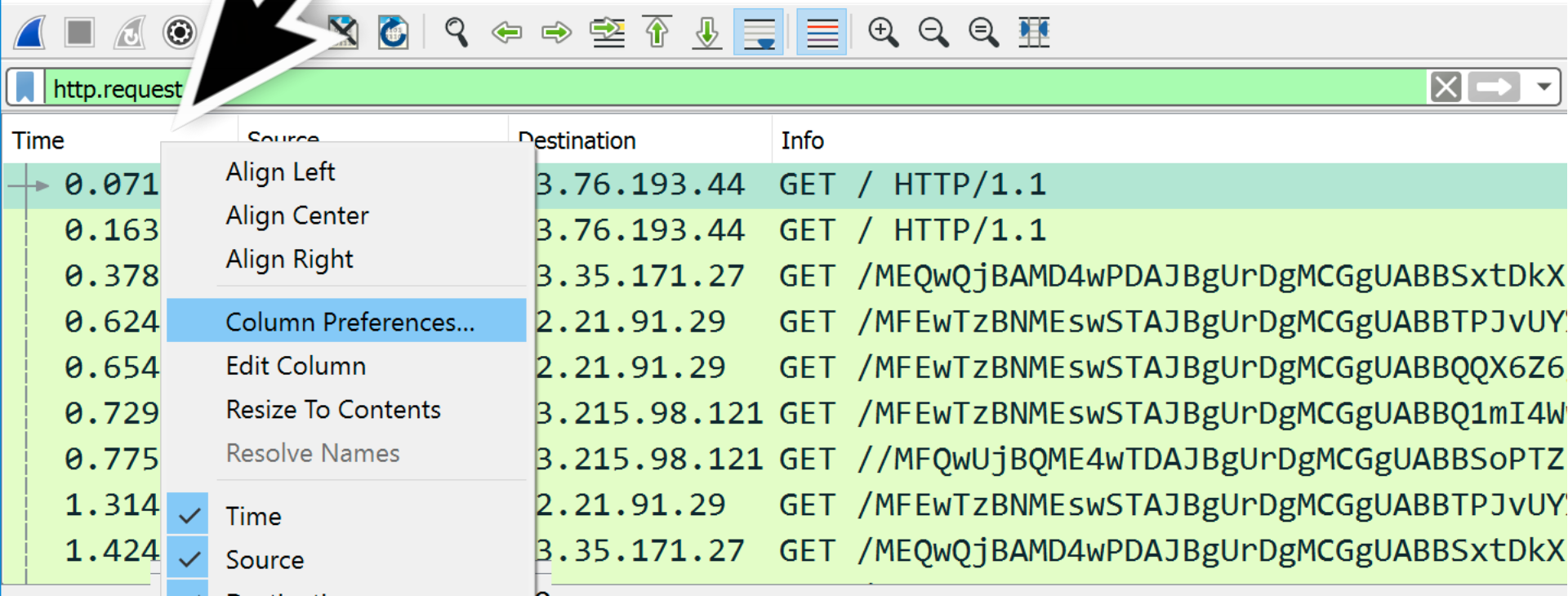
- Removing columns



- **Adding columns**

Adding columns

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

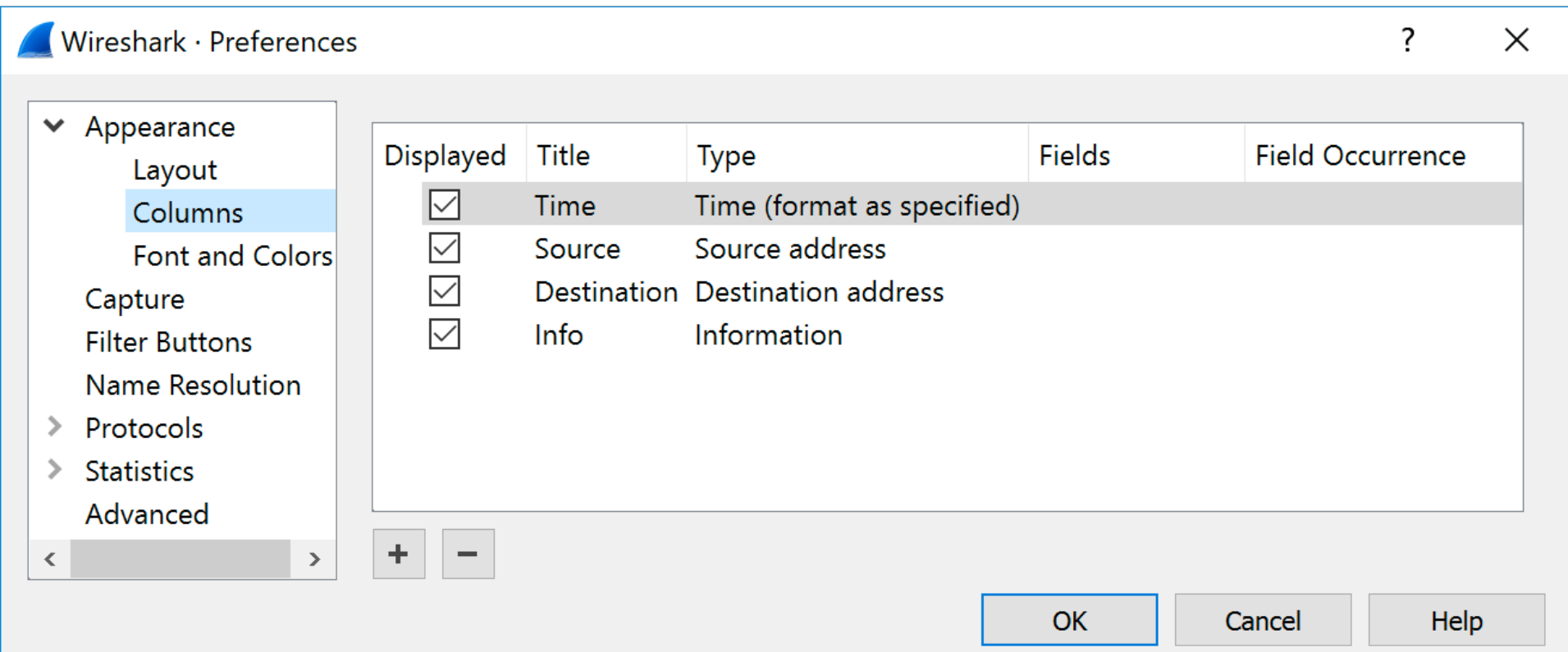


The screenshot shows a network traffic analysis tool interface. A large black arrow points to the 'Time' column header. A right-click context menu is open over the 'Time' header, with 'Column Preferences...' selected. The menu also includes options for alignment (Align Left, Align Center, Align Right), editing (Edit Column), resizing (Resize To Contents), and resolving names. The background shows a table of network traffic data with columns for Time, Source, Destination, and Info.

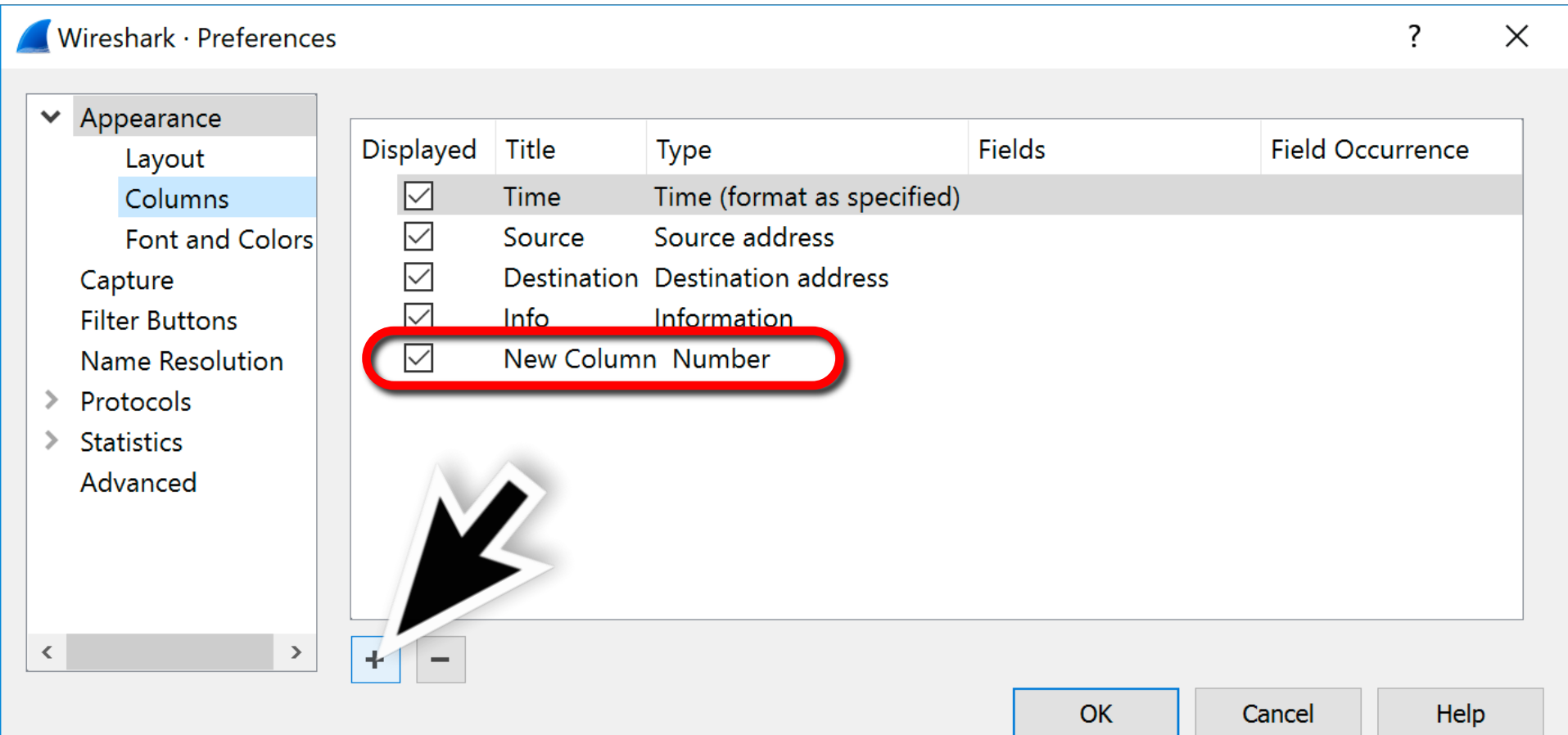
Time	Source	Destination	Info
0.071	3.76.193.44	GET / HTTP/1.1	
0.163	3.76.193.44	GET / HTTP/1.1	
0.378	3.35.171.27	GET /MEQwQjBAMD4wPDAJBgUrDgMCGgUABBSxtDkX	
0.624	2.21.91.29	GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTPJvUY	
0.654	2.21.91.29	GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBQQX6Z6	
0.729	3.215.98.121	GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ1mI4W	
0.775	3.215.98.121	GET //MFQwUjBQME4wTDAJBgUrDgMCGgUABBSOPTZ	
1.314	2.21.91.29	GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTPJvUY	
1.424	3.35.171.27	GET /MEQwQjBAMD4wPDAJBgUrDgMCGgUABBSxtDkX	

Adding columns

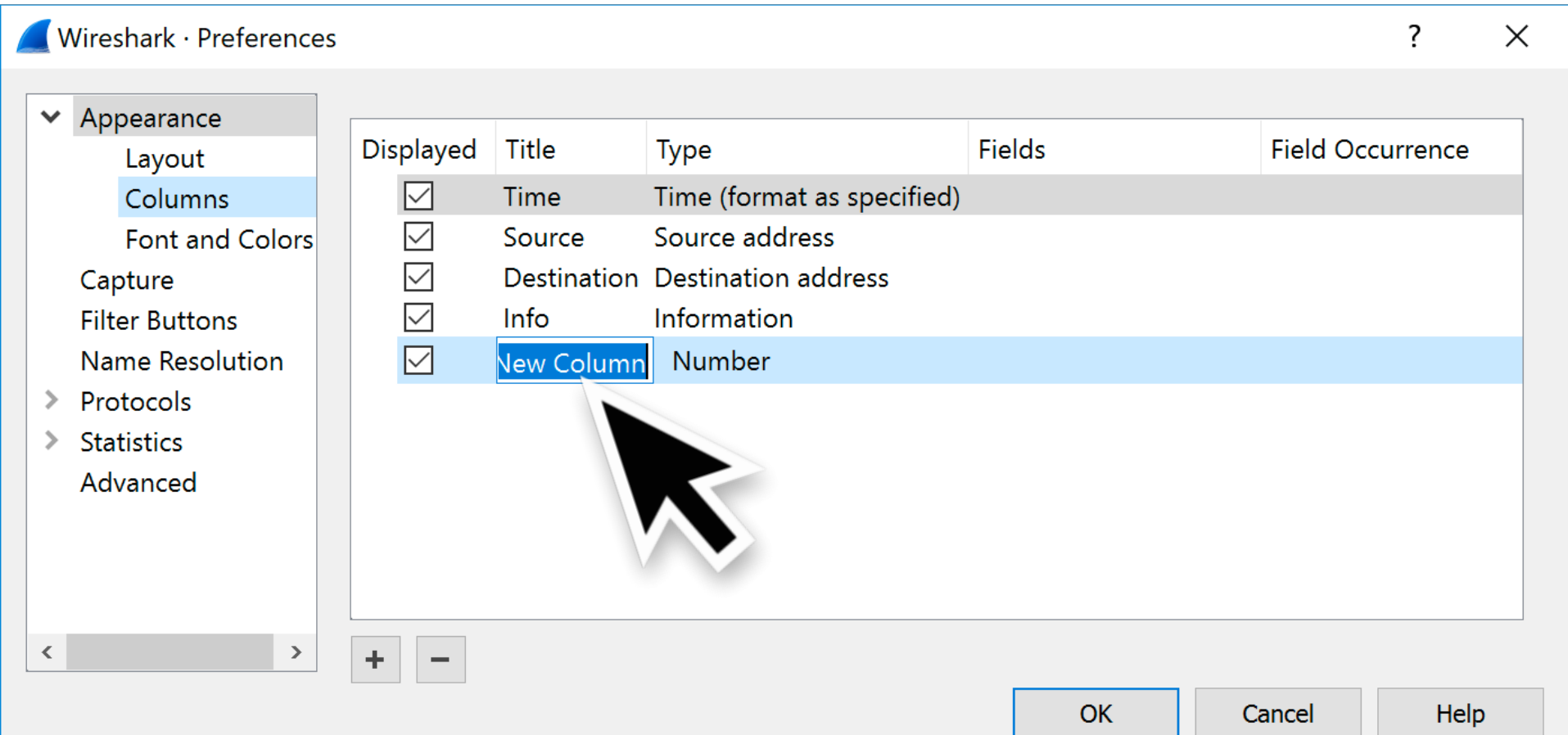
This takes you directly to the column settings



Adding columns



Adding columns



Adding columns

☒ Destination Destination address

☒ Info Information

☒ Source Port Number

Packet length (bytes)

Protocol

Relative time

Source address

Source port

Src addr (resolved)

Src addr (unresolved)

Src port (resolved)

Src port (unresolved)

TEI

Adding columns

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



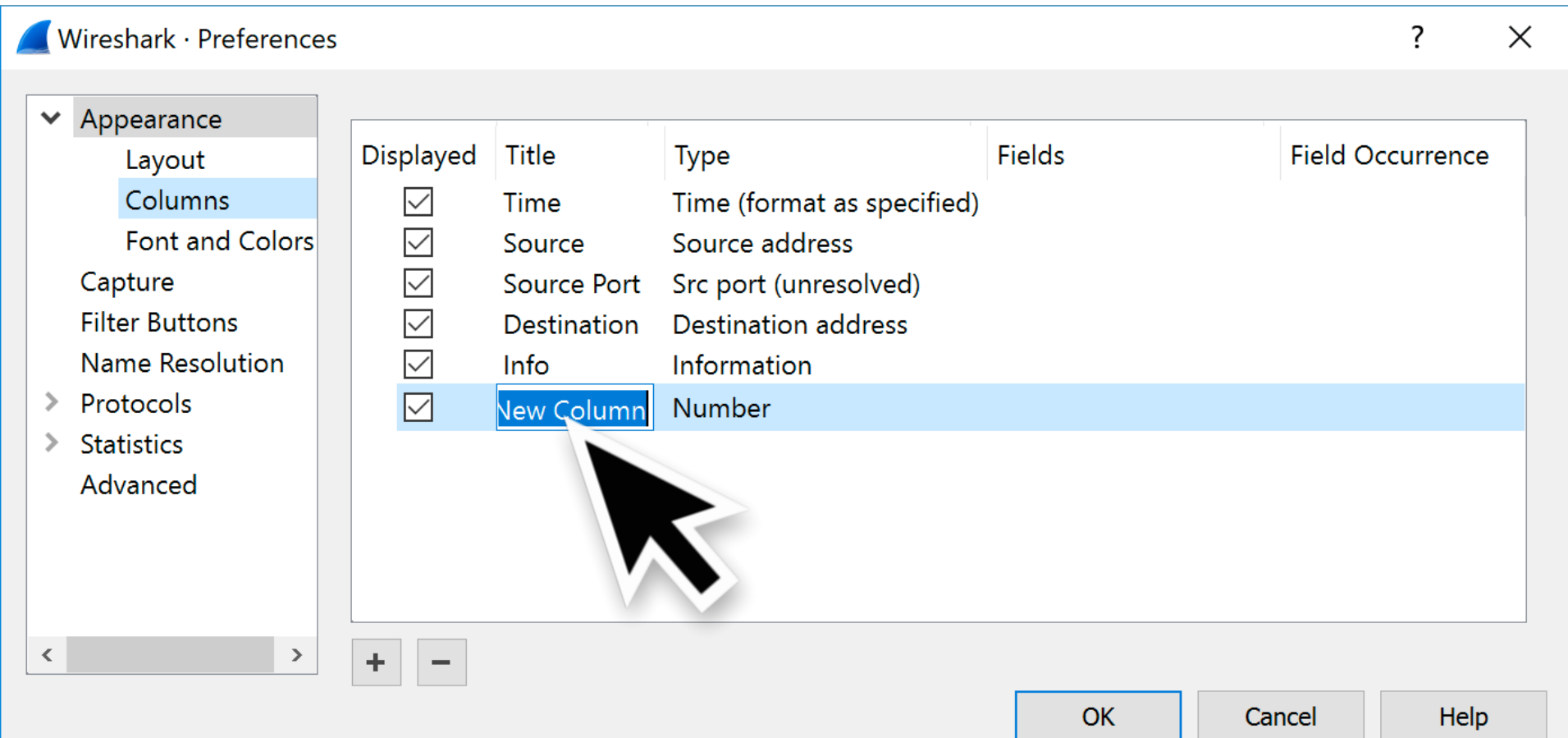
Adding columns

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

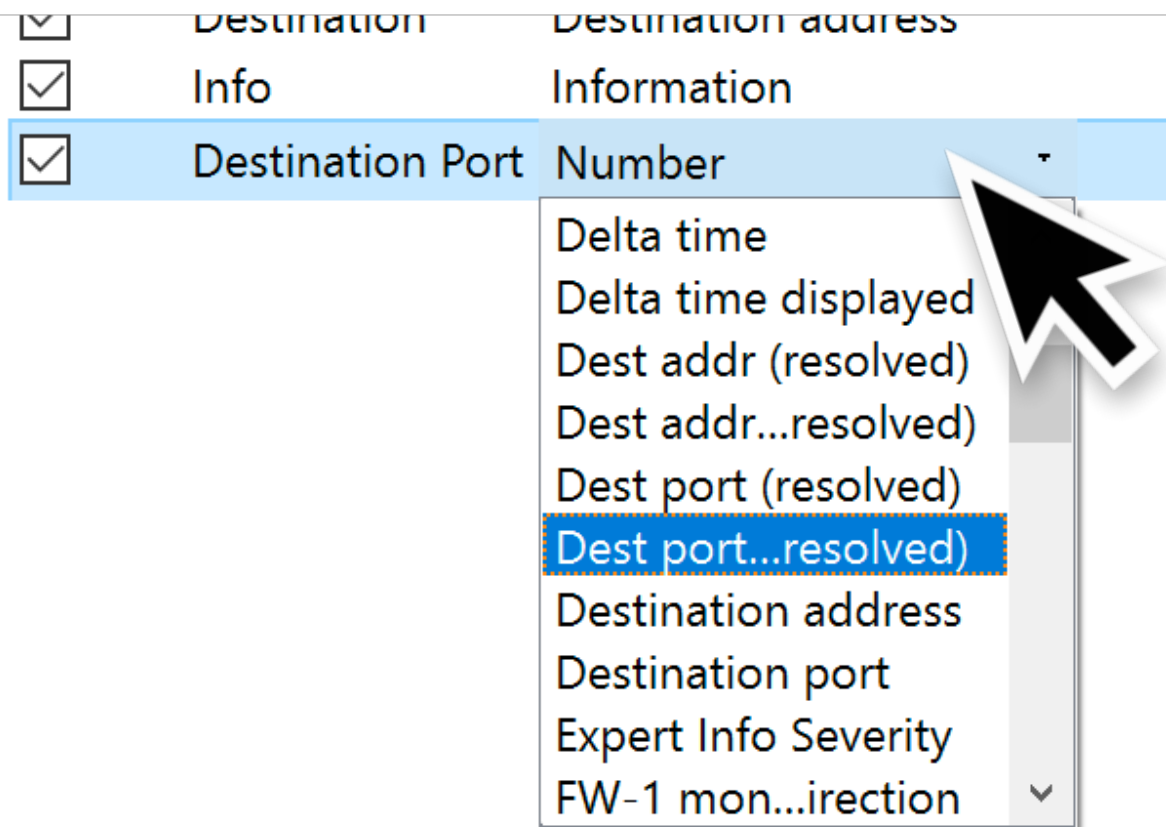
Adding columns

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

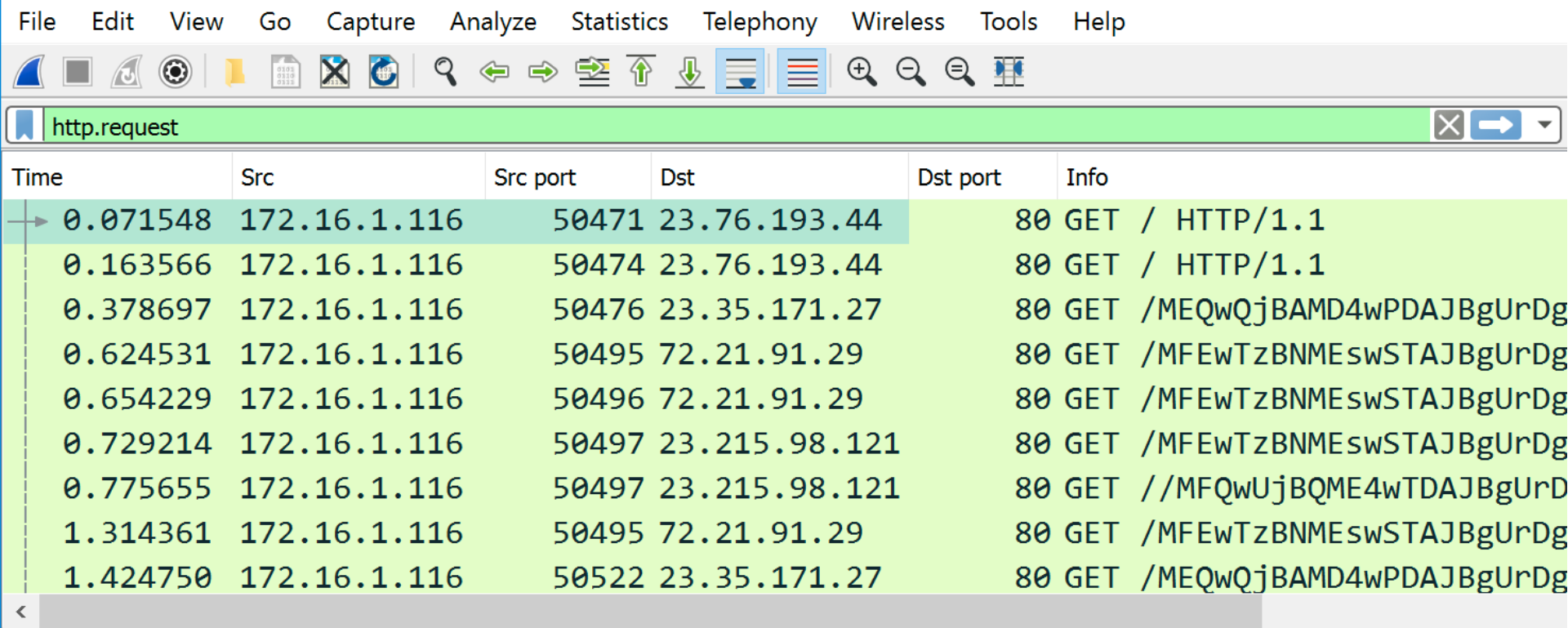
Displayed	Title	Type	Fields
☒	Time	Time (format as specified)	
☒	Source	Source address	
☒	Source Port	Src port (unresolved)	
☒	Destination	Destination address	
☒	Destination Port	Dest port (unresolved)	
☒	Info	Information	

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



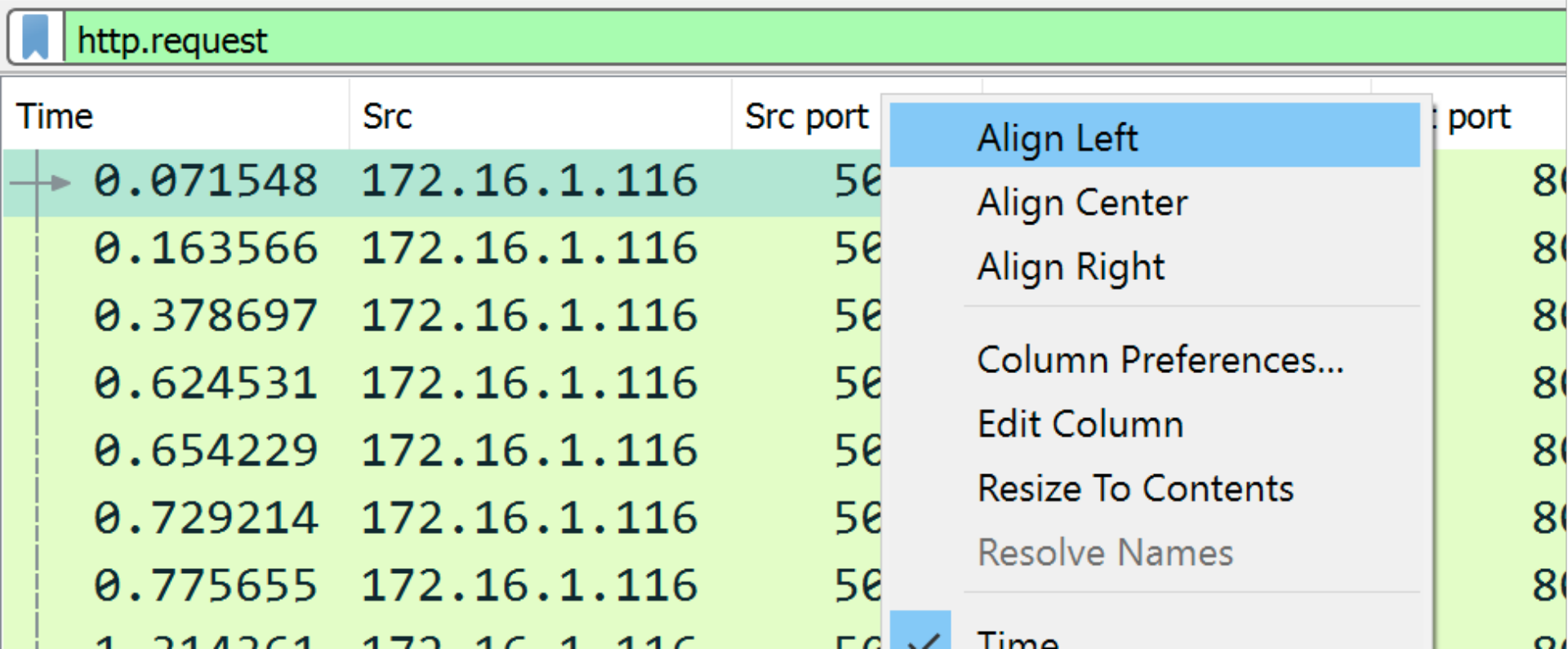
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.request

Time	Src	Src port	Dst	Dst port	Info
0.071548	172.16.1.116	50471	23.76.193.44	80	GET / HTTP/1.1
0.163566	172.16.1.116	50474	23.76.193.44	80	GET / HTTP/1.1
0.378697	172.16.1.116	50476	23.35.171.27	80	GET /MEQwQjBAMD4wPDAJBgUrDg
0.624531	172.16.1.116	50495	72.21.91.29	80	GET /MFEwTzBNMEswSTAJBgUrDg
0.654229	172.16.1.116	50496	72.21.91.29	80	GET /MFEwTzBNMEswSTAJBgUrDg
0.729214	172.16.1.116	50497	23.215.98.121	80	GET /MFEwTzBNMEswSTAJBgUrDg
0.775655	172.16.1.116	50497	23.215.98.121	80	GET //MFQwUjBQME4wTDAJBgUrD
1.314361	172.16.1.116	50495	72.21.91.29	80	GET /MFEwTzBNMEswSTAJBgUrDg
1.424750	172.16.1.116	50522	23.35.171.27	80	GET /MEQwQjBAMD4wPDAJBgUrDg

Adding columns

Right-click in the column and "Align Left"



The screenshot shows a network packet capture tool interface. At the top, a green header bar contains a blue bookmark icon and the text "http.request". Below this is a table with columns: "Time", "Src", "Src port", and "port". The table contains several rows of data. A right-click context menu is open over the "Src" column, with the "Align Left" option selected and highlighted in blue. The menu also includes options for "Align Center", "Align Right", "Column Preferences...", "Edit Column", "Resize To Contents", "Resolve Names", and "Time".

Time	Src	Src port	port
0.071548	172.16.1.116	50	80
0.163566	172.16.1.116	50	80
0.378697	172.16.1.116	50	80
0.624531	172.16.1.116	50	80
0.654229	172.16.1.116	50	80
0.729214	172.16.1.116	50	80
0.775655	172.16.1.116	50	80
1.314361	172.16.1.116	50	80

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

The screenshot shows the Wireshark network protocol analyzer interface. The 'View' menu is open, and the 'Time Display Format' option is selected, which has opened a sub-menu. In the sub-menu, the option 'UTC Date and Time of Day (1970-01-01 01:02:03.123456)' is highlighted. A large white arrow with a black outline points to this option. The background shows the packet list and packet details panes.

View Menu Options:

- ✓ Main Toolbar
- ✓ Filter Toolbar
- Wireless Toolbar
- ✓ Status Bar
- Full Screen (F11)
- ✓ Packet List
- ✓ Packet Details
- ✓ Packet Bytes
- Time Display Format** (selected)
- Name Resolution
- Zoom
- Expand Subtrees (Shift+Right)
- Expand All (Ctrl+Right)
- Collapse All (Ctrl+Left)
- Colorize Packet List

Time Display Format Sub-menu Options:

- 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)
- Seconds Since 1970-01-01
- Seconds Since Beginning of Capture
- Seconds Since Previous Captured Packet
- Seconds Since Previous Displayed Packet
- 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 01:02:03.123456)
- UTC Time of Day (01:02:03.123456) (Ctrl+Alt+8)

Packet List:

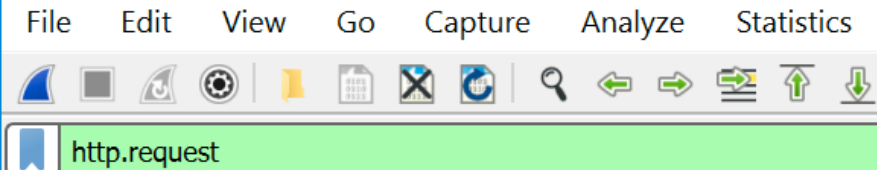
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.1	192.168.1.100	Standard query	53	Standard query 0xbd6a A newegg.com
1	0.019246	192.168.1.100	192.168.1.1	Standard query	53	Standard query 0xbd6a A newegg.com
116	0.048201	192.168.1.1	192.168.1.100	Standard query response	584...	Standard query response 0xbd6a A newegg.c...
144	0.049352	192.168.1.100	192.168.1.1	TCP	80	50472 → 80 [SYN] Seq=0 Win=65535 Len=0 MS...
144	0.049352	192.168.1.100	192.168.1.1	TCP	80	50471 → 80 [SYN] Seq=0 Win=65535 Len=0 MS...

Packet Details (Frame 1):

- Ethernet II
- Internet Protocol Version 4
- User Datagram Protocol

Changing time to UTC date and time

Resulting time is displayed well past the second.



Time	Src	Src port	Dst	Dst port	Info
2018-01-16 01:14:12.583351	172.16.1.116	50471	23.76.193.44	80	GET /
2018-01-16 01:14:12.675369	172.16.1.116	50474	23.76.193.44	80	GET /
2018-01-16 01:14:12.890500	172.16.1.116	50476	23.35.171.27	80	GET /M
2018-01-16 01:14:13.136334	172.16.1.116	50495	72.21.91.29	80	GET /M
2018-01-16 01:14:13.166032	172.16.1.116				/M
2018-01-16 01:14:13.241017	172.16.1.116				/M
2018-01-16 01:14:13.287458	172.16.1.116				//
2018-01-16 01:14:13.826164	172.16.1.116				/M
2018-01-16 01:14:13.936553	172.16.1.116	50522	23.35.171.27	80	GET /M

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

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.request

Time

2018-01-16
2018-01-16
2018-01-16
2018-01-16
2018-01-16
2018-01-16
2018-01-16
2018-01-16
2018-01-16

> Frame 8: 37
> Ethernet II
> Internet Pr
> Transmissi
> Hypertext 1

- ✓ 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

View → Time Display Format → Seconds

0476 23.35.171.27 80 GET /MEQWQJBAMD4WPDAJBgU...
0495 72.21.91.29 80 GET /MFEwTzBNMEswSTAJBgU...
0496 72.21.91.29 80 GET /MFEwTzBNMEswSTAJBgU...

- 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 01:02:03.123456)
- UTC Time of Day (01:02:03.123456) Ctrl+Alt+8
- Automatic (from capture file)
- Seconds
- Tenths of a second
- Hundredths of a second



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

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.request

Time	Src	Src port	Dst	Dst port	Info
2018-01-16 01:14:12	172.16.1.116	50471	23.76.193.44	80	GET / HTTP/1.1
2018-01-16 01:14:12	172.16.1.116	50474	23.76.193.44	80	GET / HTTP/1.1
2018-01-16 01:14:12	172.16.1.116	50476	23.35.171.27	80	GET /ME0wOiBAMD4wPDA7BglrDgMCGelUABBSx...

> Frame 8: 371 bytes on wire (2968 bits), 371 bytes captured (2968 bits)

> Ethernet II, Src: Cisco_c4:

> Internet Protocol Version 4

> Transmission Control Protocol

> Hypertext Transfer Protocol

> GET / HTTP/1.1\r\n

Accept: text/html, application/xhtml+xml, image/jxr, */*\r\n

Accept-Language: en-US\r\n

User-Agent: Mozilla/5.0 (Windows; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/!

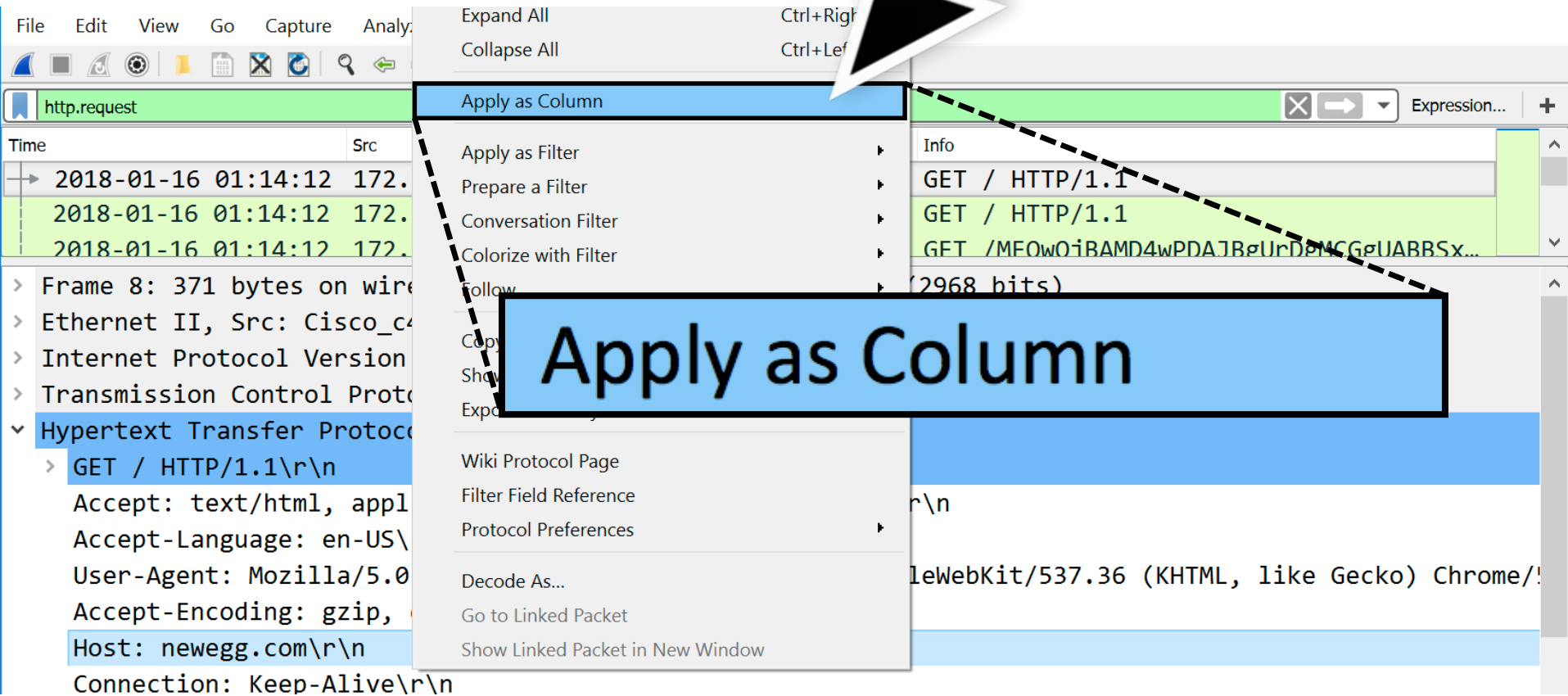
Accept-Encoding: gzip, deflate\r\n

Host: newegg.com\r\n

Connection: Keep-Alive\r\n

Host: newegg.com\r\n

Adding custom columns



The image shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, and Analyze. The toolbar contains icons for various functions. The packet list on the left shows three packets, with the first packet selected. The packet details pane on the right shows the selected packet's structure, including Ethernet II, Internet Protocol Version 4, and Hypertext Transfer Protocol. The context menu for the selected packet is open, and the 'Apply as Column' option is highlighted. A large blue box with the text 'Apply as Column' is overlaid on the menu. A dashed line points from the 'Apply as Column' option in the menu to the 'Apply as Column' button in the toolbar.

File Edit View Go Capture Analyze

Expand All Ctrl+Right
Collapse All Ctrl+Left

http.request

Time Src

2018-01-16 01:14:12 172.20.10.1

2018-01-16 01:14:12 172.20.10.1

2018-01-16 01:14:12 172.20.10.1

Frame 8: 371 bytes on wire (2968 bits) captured (2968 bits) on eth0

Ethernet II, Src: Cisco_Cat6500_000000000000, Dst: 172.20.10.1

Internet Protocol Version 4, Src: 172.20.10.1, Dst: 172.20.10.1

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

Hypertext Transfer Protocol

GET / HTTP/1.1\r\n

Accept: text/html, application/xhtml+xml, text/css\r\n

Accept-Language: en-US\r\n

User-Agent: Mozilla/5.0 (Windows NT 6.0; rv:2.0) Gecko/20100101 Firefox/4.0\r\n

Accept-Encoding: gzip, deflate\r\n

Host: newegg.com\r\n

Connection: Keep-Alive\r\n

Apply as Column

Apply as Filter
Prepare a Filter
Conversation Filter
Colorize with Filter
Follow
Copy
Show
Expand

Info
GET / HTTP/1.1
GET / HTTP/1.1
GET /ME0wOiBAMD4wPDA7BqUjDpMCGpUABBSx... (2968 bits)

Wiki Protocol Page
Filter Field Reference
Protocol Preferences
Decode As...
Go to Linked Packet
Show Linked Packet in New Window

leWebKit/537.36 (KHTML, like Gecko) Chrome/!

Adding custom columns

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help



http.request

Time	Src	Src port	Dst	Dst port	Host	Info
2018-01-16 01:14:12	172.16.1.116	50471	23.76.193.44	80	newegg.com	GET / H
2018-01-16 01:14:12	172.16.1.116	50474	23.76.193.44	80	www.newegg.com	GET / H
2018-01-16 01:14:12	172.16.1.116	50476	23.35.171.27	80	g2.symcb.com	GET /MEC
2018-01-16 01:14:13	172.16.1.116	50495	72.21.91.29	80	ocsp.digicert.com	GET /MFI
2018-01-16 01:14:13	172.16.1.116	50496	72.21.91.29	80	ocsp.digicert.com	GET /MFI
2018-01-16 01:14:13	172.16.1.116	50497	23.215.98.121	80	ocsp.trustwave.com	GET /MFI
2018-01-16 01:14:13	172.16.1.116	50497	23.215.98.121	80	ocsp.trustwave.com	GET //MI
2018-01-16 01:14:13	172.16.1.116	50495	72.21.91.29	80	ocsp.digicert.com	GET /MFI
2018-01-16 01:14:13	172.16.1.116	50522	23.35.171.27	80	g2.symcb.com	GET /MEC
2018-01-16 01:14:14	172.16.1.116	50533	23.207.41.54	80	ocsp.entrust.net	GET /MEC
2018-01-16 01:14:14	172.16.1.116	50533	23.207.41.54	80	ocsp.entrust.net	GET /MEC

Adding custom columns

What else do we want in our column display?

- HTTP host names



- **HTTPS server names**

Adding custom columns

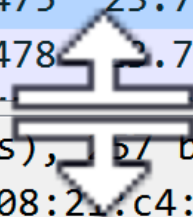
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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 Hello
2018-01-16 01:14:13	172.16.1.116	50478	23.76.193.124	443		Client Hello
2018-01-16 01:14:13	172.16.1.116	50477	23.76.193.124	443		Client Hello
2018-01-16 01:14:13	172.16.1.116	50480	23.199.238.64	443		Client Hello
2018-01-16 01:14:13	172.16.1.116	50479	23.199.238.64	443		Client Hello
2018-01-16 01:14:13	172.16.1.116	50481	23.76.193.44	443		Client Hello
2018-01-16 01:14:13	172.16.1.116	50482	23.76.193.44	443		Client Hello
2018-01-16 01:14:13	172.16.1.116	50485	23.76.193.44	443		Client Hello
2018-01-16 01:14:13	172.16.1.116	50483	23.76.193.44	443		Client Hello
2018-01-16 01:14:13	172.16.1.116	50484	23.76.193.44	443		Client Hello
2018-01-16 01:14:13	172.16.1.116	50486	23.76.193.44	443		Client Hello
2018-01-16 01:14:13	172.16.1.116	50489	23.76.193.44	443		Client Hello
2018-01-16 01:14:13	172.16.1.116	50488	23.76.193.44	443		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), 67 bytes captured (2056 bits)
- > Ethernet II, Src: Cisco_c4:7a:0e (00:08:21:c4:7a:0e), Dst: Netgear_b6:93:f1 (20:e5:69:b6:93:f1)
- > 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: 0
- > 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:e8:8a:b6:93:f1)
- > 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: 0
- ✓ 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:e8:8a:b6:93:f1)
- > 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: 0
- ▼ 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 (20:08:00:07:09:f1)
- > 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: 0
- ▼ 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
 - Handshake Type: Client Hello (1)
 - Length: 194
 - Version: TLS 1.2 (0x0303)
 - > Random: 5a5d51e4a2de9d36bfa48e0b85f06956b9c3026a9e6b086e...

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)

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
- ✓ 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)
- > Extension: ... (len=0)

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

▼ Extension: server_name (len=19)

Server Name list length: 19

Server Name Type: host_name (0)

▼ 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)

› Extension: supported_versions (len=3)

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

▼ Extension: server_name (len=19)

Type: server_name (0)

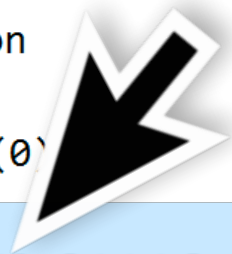
Length: 19

▼ Server Name Indication extension

Server Name list length: 17

Server Name Type: host_name (0)

Server Name Length: 14



Server Name: www.newegg.com

> Extension: supported_groups (len=8)

Extension: supported_groups (len=8)

ssl.handshake.type == 1				
Time		Src		Src port
	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 extension - 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

ssl.handshake.type == 1							Expression...
Time	Src	Src port	Dst	Dst port	Host	Server Name	
2018-01-16 01:14:12	172.16.1.116	50475	23.76.193.44	443		www.newegg.com	
2018-01-16 01:14:13	172.16.1.116	50478	23.76.193.124	443		assets.adobedtm.com	
2018-01-16 01:14:13	172.16.1.116	50477	23.76.193.124	443		assets.adobedtm.com	
2018-01-16 01:14:13	172.16.1.116	50480	23.199.238.64	443		se.monetate.net	
2018-01-16 01:14:13	172.16.1.116	50479	23.199.238.64	443		se.monetate.net	
2018-01-16 01:14:13	172.16.1.116	50481	23.76.193.44	443		images10.newegg.com	
2018-01-16 01:14:13	172.16.1.116	50482	23.76.193.44	443		images10.newegg.com	
2018-01-16 01:14:13	172.16.1.116	50485	23.76.193.44	443		images10.newegg.com	
2018-01-16 01:14:13	172.16.1.116	50483	23.76.193.44	443		images10.newegg.com	
2018-01-16 01:14:13	172.16.1.116	50484	23.76.193.44	443		images10.newegg.com	
2018-01-16 01:14:13	172.16.1.116	50486	23.76.193.44	443		images10.newegg.com	
2018-01-16 01:14:13	172.16.1.116	50489	23.76.193.44	443		promotions.newegg.com	
2018-01-16 01:14:13	172.16.1.116	50488	23.76.193.44	443		promotions.newegg.com	
2018-01-16 01:14:13	172.16.1.116	50491	23.76.193.44	443		promotions.newegg.com	
2018-01-16 01:14:13	172.16.1.116	50490	23.76.193.44	443		promotions.newegg.com	
2018-01-16 01:14:13	172.16.1.116	50492	23.76.193.44	443		promotions.newegg.com	
2018-01-16 01:14:13	172.16.1.116	50487	23.76.193.44	443		promotions.newegg.com	

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 Name
2018-01-16 01:14:12		172.16.1.116	50475	23.76.193.44	443		www.netflix.com
2018-01-16 01:14:13		172.16.1.116	50478	23.76.193.124	443		assets.netflix.com
2018-01-16 01:14:13		172.16.1.116	50477	23.76.193.124	443		assets.netflix.com
2018-01-16 01:14:13		172.16.1.116	50480	23.199.238.64	443		se.monster.com
2018-01-16 01:14:13		172.16.1.116	50479	23.199.238.64	443		se.monster.com
2018-01-16 01:14:13		172.16.1.116	50481	23.76.193.44	443		images.netflix.com
2018-01-16 01:14:13		172.16.1.116	50482	23.76.193.44	443		images.netflix.com
2018-01-16 01:14:13		172.16.1.116	50485	23.76.193.44	443		images.netflix.com
2018-01-16 01:14:13		172.16.1.116	50483	23.76.193.44	443		images.netflix.com
2018-01-16 01:14:13		172.16.1.116	50484	23.76.193.44	443		images.netflix.com
2018-01-16 01:14:13		172.16.1.116	50486	23.76.193.44	443		images.netflix.com
2018-01-16 01:14:13		172.16.1.116	50489	23.76.193.44	443		promo.netflix.com
2018-01-16 01:14:13		172.16.1.116	50488	23.76.193.44	443		promo.netflix.com
2018-01-16 01:14:13		172.16.1.116	50491	23.76.193.44	443		promo.netflix.com

Hiding columns

ssl.handshake.type == 1						
Time	Src port	Dst	Dst port	Host	Server Name	
2018-01-16 01:14:12	50475	✓ Align Left	3		www.newegg.com	
2018-01-16 01:14:13	50478	Align Center	3		assets.adobedtm.com	
2018-01-16 01:14:13	50477	Align Right	3		assets.adobedtm.com	
2018-01-16 01:14:13	50480	Column Preferences...	3		se.monetate.net	
2018-01-16 01:14:13	50479	Edit Column	3		se.monetate.net	
2018-01-16 01:14:13	50481	Resize To Contents	3		images10.newegg.com	
2018-01-16 01:14:13	50482	Resolve Names	3		images10.newegg.com	
2018-01-16 01:14:13	50485	✓ Time			images10.newegg.com	
2018-01-16 01:14:13	50483	Src			images10.newegg.com	
2018-01-16 01:14:13	50484	✓ Src port			images10.newegg.com	
2018-01-16 01:14:13	50486	✓ Dst	3		images10.newegg.com	
2018-01-16 01:14:13	50489	✓ Dst port	3		promotions.newegg.c	
2018-01-16 01:14:13	50488	✓ Host	3		promotions.newegg.c	
2018-01-16 01:14:13	50401		3		promotions.newegg.c	

Hiding columns

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

[illegible]

Hiding columns

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

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

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***

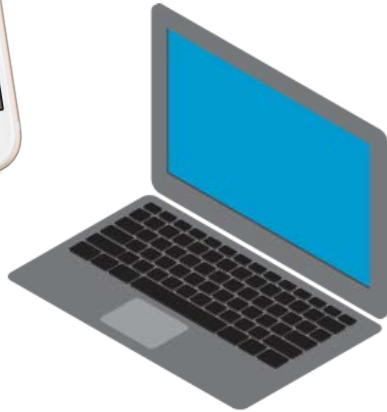


Block 2 - Overview

- 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**

udp.port eq 67

✕ → ▾

Expression... +

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 0xb8767d2f
2018-02-13 20:16:51	192.168.1.254	67	192.168.1.94	68	DHCP ACK - Transaction ID 0xb8767d2f
2018-02-13 20:16:54	192.168.1.94	68	255.255.255.255	67	DHCP Inform - Transaction ID 0x323764cf
2018-02-13 20:16:54	192.168.1.254	67	192.168.1.94	68	DHCP ACK - Transaction ID 0x323764cf

> Frame 24: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)

> Ethernet II, Src: HewlettP_1c:47:ae (00:08:02:1c:47:ae), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

> Internet Protocol Version 4, Src: 192.168.1.94, Dst: 255.255.255.255

> User Datagram Protocol, Src Port: 68, Dst Port: 67

▼ Bootstrap Protocol (Inform)

Message type: Boot Request (1)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0

Host information

- Client IP address
- Client MAC address

Client IP address: 192.168.1.94

Seconds elapsed: 0

Bootp flags: 0x0000 (Unicast)

Client IP address: 192.168.1.94

Your (client) IP address: 0.0.0.0

HewlettP_1c:47:ae (00:08:02:1c:47:ae)

Relay agent IP address: 0.0.0.0

Client MAC address: HewlettP_1c:47:ae (00:08:02:1c:47:ae)

Client hardware address padding: 00000000000000000000

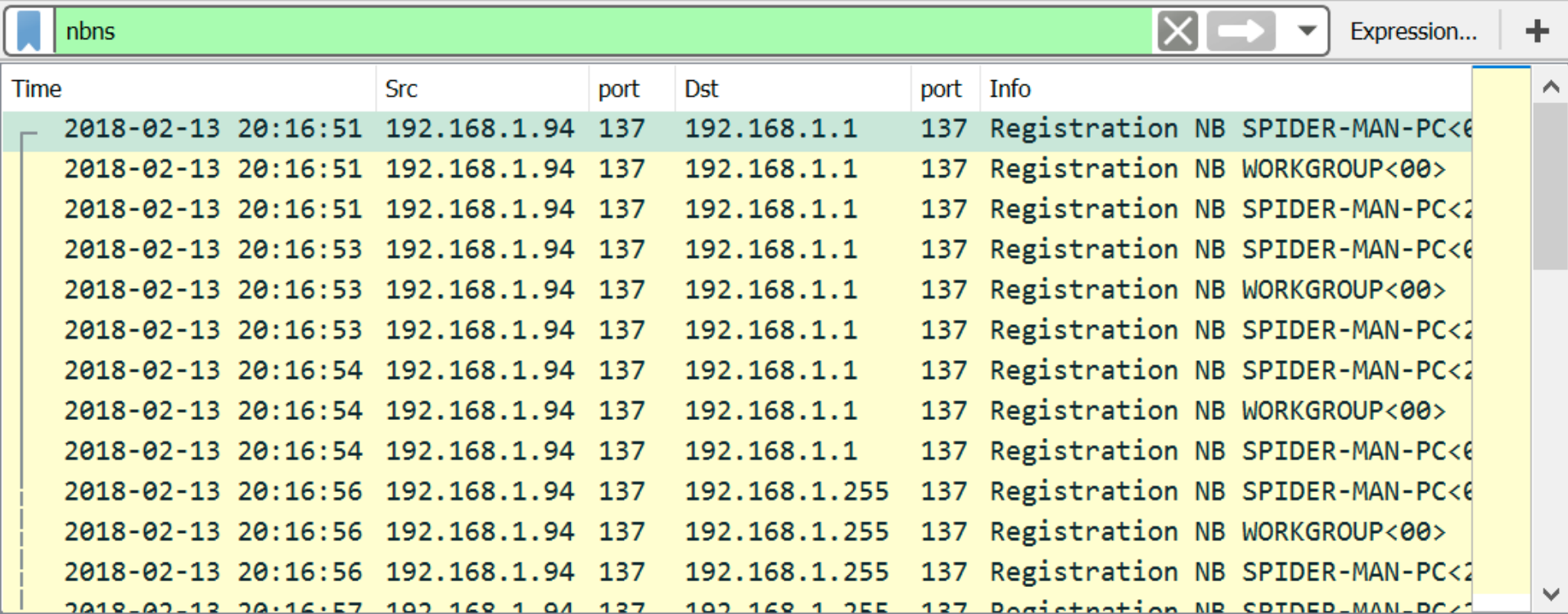
Server host name not given

Host information

- Option: (55) DHCP Message Type (Inform)
- Option: (61) Client identifier
- ▼ Option: (12) Host Name
 - Length: 13
 - Host Name: Spider-man-PC
- Option: (60) Vendor class identifier
- Option: (55) Parameter Request List
- Option: (255) End
- Padding: 0000000000000000

Host information - Windows hosts

- Wireshark filter: **nbns**



Time	Src	port	Dst	port	Info
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 20:16:53	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 20:16:54	192.168.1.94	137	192.168.1.1	137	Registration NB SPIDER-MAN-PC<20>
2018-02-13 20:16:54	192.168.1.94	137	192.168.1.1	137	Registration NB WORKGROUP<00>
2018-02-13 20:16:54	192.168.1.94	137	192.168.1.1	137	Registration NB SPIDER-MAN-PC<00>
2018-02-13 20:16:56	192.168.1.94	137	192.168.1.255	137	Registration NB SPIDER-MAN-PC<00>
2018-02-13 20:16:56	192.168.1.94	137	192.168.1.255	137	Registration NB WORKGROUP<00>
2018-02-13 20:16:56	192.168.1.94	137	192.168.1.255	137	Registration NB SPIDER-MAN-PC<20>
2018-02-13 20:16:57	192.168.1.94	137	192.168.1.255	137	Registration NB SPIDER-MAN-PC<20>

Host information - Windows hosts

Time	Src	port	Dst	port	Info
2018-02-13 20:16:51	192.168.1.94	137	192.168.1.1	137	Registration NB SPIDER-MAN-PC
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
2018-02-13 20:16:53	192.168.1.94	137	192.168.1.1	137	Registration NB SPIDER-MAN-PC
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

> Frame 6: 110 bytes on wire (880 bits). 110 bytes captured (880 bits)
 > Ethernet II, Src: HewlettP_1c:47:ae (00:08:02:1c:47:ae) Dst: Netgear_b6:93:f1 (20:e5:)
 > Internet Protocol Version 4, Src: 192.168.1.94, Dst: 192.168.1.1
 > User Datagram Protocol, Src Port: 137, Dst Port: 137
 > NetBIOS Name Service
 Transaction ID: 0xbf19
 > Flags: 0x2900, Opcode: Registration, Recursion desired
 Questions: 1
 Answer RRs: 0

Host information - Windows hosts

- ▼ Queries

- > SPIDER-MAN-PC<00>: type NB, class IN

- ▼ Additional records

- ▼ SPIDER-MAN-PC<00>: type NB, class IN

- Name: SPIDER-MAN-PC<00> (Workstation/Redirector)

- Type: NB (32)

- Class: IN (1)

- Time to live: 3 days, 11 hours, 20 minutes

- Data length: 6

- ▼ Name flags: 0x6000, ONT: Unknown (H-node, unique)

- 0... .. = Name type: Unique name

- .11. = ONT: Unknown (3)

- Addr: 192.168.1.94

Host information - Apple MacBook

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

ip contains MacBook

Time	src	port	dst	port	Info
2018-02-15 02:40:38	0.0.0.0	68	255.255.255.255	67	DHCP Request - Transaction ID 0xfc8f0999
2018-02-15 02:40:38	0.0.0.0	68	255.255.255.255	67	DHCP Request - Transaction ID 0xfc8f099a
2018-02-15 02:40:43	172.16.1.205	5353	224.0.0.251	5353	Standard query 0x0000 ANY Clydes-MacBook-Pro.local, "QU" quest...
2018-02-15 02:40:43	172.16.1.205	5353	224.0.0.251	5353	Standard query 0x0000 PTR _sleep-proxy._udp.local, "QM" questi...
2018-02-15 02:40:43	172.16.1.205	5353	224.0.0.251	5353	Standard query 0x0000 ANY Clydes-MacBook-Pro.local, "QM" quest...
2018-02-15 02:40:44	172.16.1.205	5353	224.0.0.251	5353	Standard query response 0x0000 PTR, cache flush Clydes-MacBook...
2018-02-15 02:40:45	172.16.1.205	5353	224.0.0.251	5353	Standard query response 0x0000 PTR, cache flush Clydes-MacBook...
2018-02-15 02:40:47	172.16.1.205	5353	224.0.0.251	5353	Standard query response 0x0000 PTR, cache flush Clydes-MacBook...
2018-02-15 02:40:51	172.16.1.205	5353	224.0.0.251	5353	Standard query response 0x0000 PTR, cache flush Clydes-MacBook...

- > Option: (61) Client identifier
- > Option: (50) Requested IP Address
- > Option: (51) IP Address Lease Time
- ▼ Option: (12) Host Name
 - Length: 18
 - Host Name: Clydes-MacBook-Pro
- > Option: (255) End

Clydes - MacBook - Pro

Host information - Apple MacBook

- Wireshark filter: nbns

MACBOOKPRO-42C5

nbns							Expression...	+
Time	Src	port	Dst	port	Info			
2018-02-15 02:40:41	172.16.1.205	137	172.16.1.255	137	Registration NB MACBOOKPRO-42C5<00>			
2018-02-15 02:40:43	172.16.1.205	137	172.16.1.255	137	Registration NB MACBOOKPRO-42C5<00>			
2018-02-15 02:40:45	172.16.1.205	137	172.16.1.255	137	Registration NB MACBOOKPRO-42C5<00>			
2018-02-15 02:40:46	172.16.1.205	137	172.16.1.255	137	Release NB MACBOOKPRO-42C5<00>			
2018-02-15 02:40:46	172.16.1.205	137	172.16.1.1	137	Name query NB <01><02>__MSBROWSE__<0			
2018-02-15 02:40:46	172.16.1.205	137	172.16.1.1	137	Registration NB MACBOOKPRO-42C5<00>			
2018-02-15 02:40:48	172.16.1.205	137	172.16.1.255	137	Release NB MACBOOKPRO-42C5<00>			
2018-02-15 02:40:48	172.16.1.205	137	172.16.1.1	137	Name query NB <01><02>__MSBROWSE__<0			
2018-02-15 02:40:48	172.16.1.205	137	172.16.1.1	137	Registration NB MACBOOKPRO-42C5<00>			
2018-02-15 02:40:50	172.16.1.205	137	172.16.1.255	137	Release NB MACBOOKPRO-42C5<00>			
2018-02-15 02:40:50	172.16.1.205	137	172.16.1.255	137	Registration NB MACBOOKPRO-42C5<00>			
2018-02-15 02:40:50	172.16.1.205	137	172.16.1.1	137	Name query NB <01><02>__MSBROWSE__<0			

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

http.request						
Time	Dst		port	Host		Info
2018-02-15 02:41:24	23.43.62.177		80	init-p01st.push.apple.com		GET /bag HTTP/1.1
2018-02-15 02:41:31	17.254.32.16		80	wu-calculator.apple.com		POST /dgw?imei=APPLE8
2018-02-15 02:42:01	23.76.195.16		80	js-sec.indexww.com		GET /ht/ls-zdnet.js H
2018-02-15 02:42:01	23.193.77.203		80	c.go-mpulse.net		GET /boomerang/config
2018-02-15 02:42:01	93.184.216.180		80	tags.tiqcdn.com		GET /utag/cbsi/zdnetg
2018-02-15 02:42:01	172.217.9.130		80	www.googletagservices.com		GET /tag/js/gpt.js HT
2018-02-15 02:42:02	104.16.163.13		80	cdn.viglink.com		GET /api/vglnk.js HT
2018-02-15 02:42:02	104.16.77.165		80	www.lightboxcdn.com		GET /vendor/a1583f50-

- Wireshark filter: **http.request**

OS and browser - MacBook

2018-02-15 02:42:01 172.217.9.130 80 www.googletagmanager.com GET /tag/js/gpt.js HTTP/1.1

2018-02-15 02:42:02 104.16.163.13 80 cdn.viglink.com GET /api/vglnk.js HTTP/1.1

2018-02-15 02:42:02 104.16.163.13 80 cdn.viglink.com GET /vendor/a1583f50-579b-41d0-8c4...

Frame 650: 517 bytes on wire (4136 bits)
Ethernet II, Src: Apple [08:00:2e:14:61:00], Dst: 20:e5:2a:b6:93:f1 (20:e5:2a:b6:93:f1)
Internet Protocol Version 4, Src: 10.0.1.1, Dst: 104.16.163.13
Transmission Control Protocol, Src Port: 54321, Dst Port: 80, Seq: 1, Ack: 1, Len: 463
Hypertext Transfer Protocol

Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comment... Ctrl+Alt+C
Edit Resolved Name
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy

TCP Stream
UDP Stream
SSL Stream

0000 20 e5 2a b6 93 f1 7
0010 01 f7 4f ca 40 00 4
0020 a3 0d c0 14 00 50 d

OS and browser - MacBook

Mac OS X 10_11_6



```
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
```

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] Seq
2018-02-15 04:20:33	151.101.1.67	80	10.2.15.101	49162		80 → 49162 [SYN, ACK]
2018-02-15 04:20:33	10.2.15.101	49162	151.101.1.67	80		49162 → 80 [ACK] Seq
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] Seq
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, ACK]
2018-02-15 04:20:33	151.101.1.67	80	10.2.15.101	49162		80 → 49162 [ACK] Seq
2018-02-15 04:20:33	10.2.15.101	49162	151.101.1.67	80		49162 → 80 [ACK] Seq

Right click anywhere & follow TCP stream

OS and browser - Windows

Windows NT 6.1



```
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/
Accept-Ranges: bytes
```

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

OS and browser - Linux distros - CentOS

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

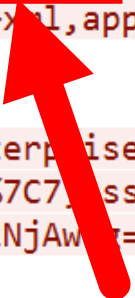
http.request

Time	Src	port	Host	Info
2018-02-13 20:44:08	23.3.97.88	80	detectportal.firefox.com	GET /success.txt HTTP/1.1
2018-02-13 20:44:11	172.217.2.238	80	clients1.google.com	Request
2018-02-13 20:44:11	192.229.210.135	80	www.scylladb.com	POST /wp-admin/admin-ajax.php...
2018-02-13 20:44:11	172.217.2.238	80	ocsp.pki.goog	Request
2018-02-13 20:44:11	172.217.2.238	80	clients1.google.com	Request
2018-02-13 20:44:12	104.244.43.48	80	static.ads-twitter.com	GET /uwt.js HTTP/1.1
2018-02-13 20:44:13	72.21.91.29	80	ocsp.digicert.com	Request
2018-02-13 20:44:13	23.46.217.59	80	m.addthisedge.com	GET /live/boost/ra-56da1c1d1c...
2018-02-13 20:44:13	23.46.217.59	80	s7.addthis.com	GET /static/sh.d663e43787b663...
2018-02-13 20:44:13	23.46.217.59	80	s7.addthis.com	GET /static/sh.d663e43787b663...
2018-02-13 20:44:13	23.46.217.59	80	m.addthis.com	GET /live/red_lojson/300lo.js...
2018-02-13 20:44:13	192.28.144.228	80	791-qbf-350.mktoresp.com	GET /webevents/visitWebPage? ...

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=NzcmMDFOQVVTVFgyMDk4MDg0NjYxODMzNjAw; mus=0; na_tc=Y
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```



X11; Linux x86_64

```
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
```

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 - Transaction...
2018-02-15 23:22:39	172.16.45.1	67	172.16.45.109	68	DHCP ACK - Transaction...
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

- > Option: (50) Requested IP Address
- > Option: (57) Maximum DHCP Message Size
- > Option: (60) Vendor class identifier
- ▼ Option: (12) Host Name
 - Length: 24
 - Host Name: android-d6e2f810e4293e37
- > Option: (55) Parameter Request List
- > Option: (255) End

OS and browser - Android phones

http.request

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

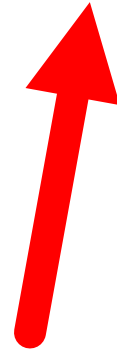


Wireshark · Follow TCP Stream (tcp.stream eq 0) · 2018-traffic-analysis-work...



```
GET /generate_204 HTTP/1.1
User-Agent: Dalvik/2.1.0 (Linux; U; Android 5.0.1; SPH-L720T Build/LRX22C)
Host: clients3.google.com
Connection: Keep-Alive
Accept-Encoding: gzip
```

```
HTTP/1.1 204 No Content
Content-Length: 0
Date: Thu, 15 Feb 2018 23:22:39 GMT
```



Android 5.0.1; SPH-L720T

OS and browser - Android phones



SPH-L720T



All

Shopping

Images

Videos

News

More

About 556,000 results (0.50 seconds)

Specs: Samsung Galaxy S4 (Sprint) [SPH-L720T] | Swappa

<https://swappa.com/specs/samsung-galaxy-s-4-triband-sprint> ▼

Samsung Galaxy S4 (Sprint) [SPH-L720T] specs and specifications. Buy and sell gently used Samsung Galaxy S4 with our fast and easy marketplace.

Compare: Samsung Galaxy S4 (Sprint) [SPH-L720T] vs. Samsung ...

<https://swappa.com/compare/samsung-galaxy-s-4-triband-sprint/samsung-galaxy-s-4-triband-sprint> ▼

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...
2018-02-14 21:52:33	172.16.45.127	52160	172.16.45.1	53	Standard query 0x8310 A i...

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

OS and browser - iPhones

- > Option: (61) Client identifier
- > Option: (50) Requested IP Address
- > Option: (54) DHCP Server Identifier
- ▼ Option: (12) Host Name
 - Length: 12
 - Host Name: Marys-iPhone
- > Option: (255) End
 - Padding: 00000000000000000000

OS and browser - iPhones

http.request

Time	Dst	port	Host	Info
2018-02-14 21:52:33	96.17.164.58	80	init-p01st.push.apple.com	GET /bag HTTP/1.1
2018-02-14 21:52:34	23.193.85.231	80	ocsp.entrust.net	GET /MEowSKADAgEAMEEwPz...
2018-02-14 21:53:16	151.101.50.2	80	videos-f.jwpsrv.com	GET /content/conversion...
2018-02-14 21:53:17	96.17.164.154	80	as.casalemedia.com	GET /cygnus?v=7.1&s=174...
2018-02-14 21:53:17	8.43.72.22	80	fastlane.rubiconproject...	GET /a/api/fastlane.jso...
2018-02-14 21:53:17	8.43.72.22	80	fastlane.rubiconproject...	GET /a/api/fastlane.jso...
2018-02-14 21:53:17	8.43.72.22	80	fastlane.rubiconproject...	GET /a/api/fastlane.jso...
2018-02-14 21:53:17	173.241.244.220	80	futurenet-d.openx.net	GET /w/1.0/arj?audid=538...
2018-02-14 21:53:17	104.254.150.13	80	secure.adnxs.com	GET /jpt?id=11311440&si...
2018-02-14 21:53:17	104.254.150.13	80	secure.adnxs.com	GET /jpt?id=11311439&si...
2018-02-14 21:53:17	104.254.150.13	80	secure.adnxs.com	GET /jpt?id=11311435&si...
2018-02-14 21:53:18	173.241.244.220	80	futurenet-d.openx.net	GET /w/1.0/ari?cc=1&au...

Follow TCP stream for 3rd HTTP request

OS and browser - iPhones

```
GET /content/conversions/QWFH4BVQ/videos/xnZe7xJJ-31058985.mp4.m3u8?
token=0_5a84d919_0xc10f0119e04eb5f1bfff263a9e42f9485813129be 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-8-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

The screenshot shows a web browser window with a single tab titled "Daily Prayer - Regist...". The address bar displays the URL "dailyprayer.us/registration/register_form.php". The browser's toolbar includes a back button, a search bar, and several icons for bookmarks, downloads, and home. The registration form itself is titled "First Name" and "Last Name" and contains the following fields:

- First Name:** Cameron
- Last Name:** Willis
- Email:** cameron.willis2018@whatchu
- Username*:** cameronwillis2018
- Password*:** [Redacted]
- Confirm Password:** [Redacted]

A security warning is displayed below the Username field, stating: "This connection is not secure. Logins entered here could be compromised. Learn More". A "Register" button is located at the bottom of the form.

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

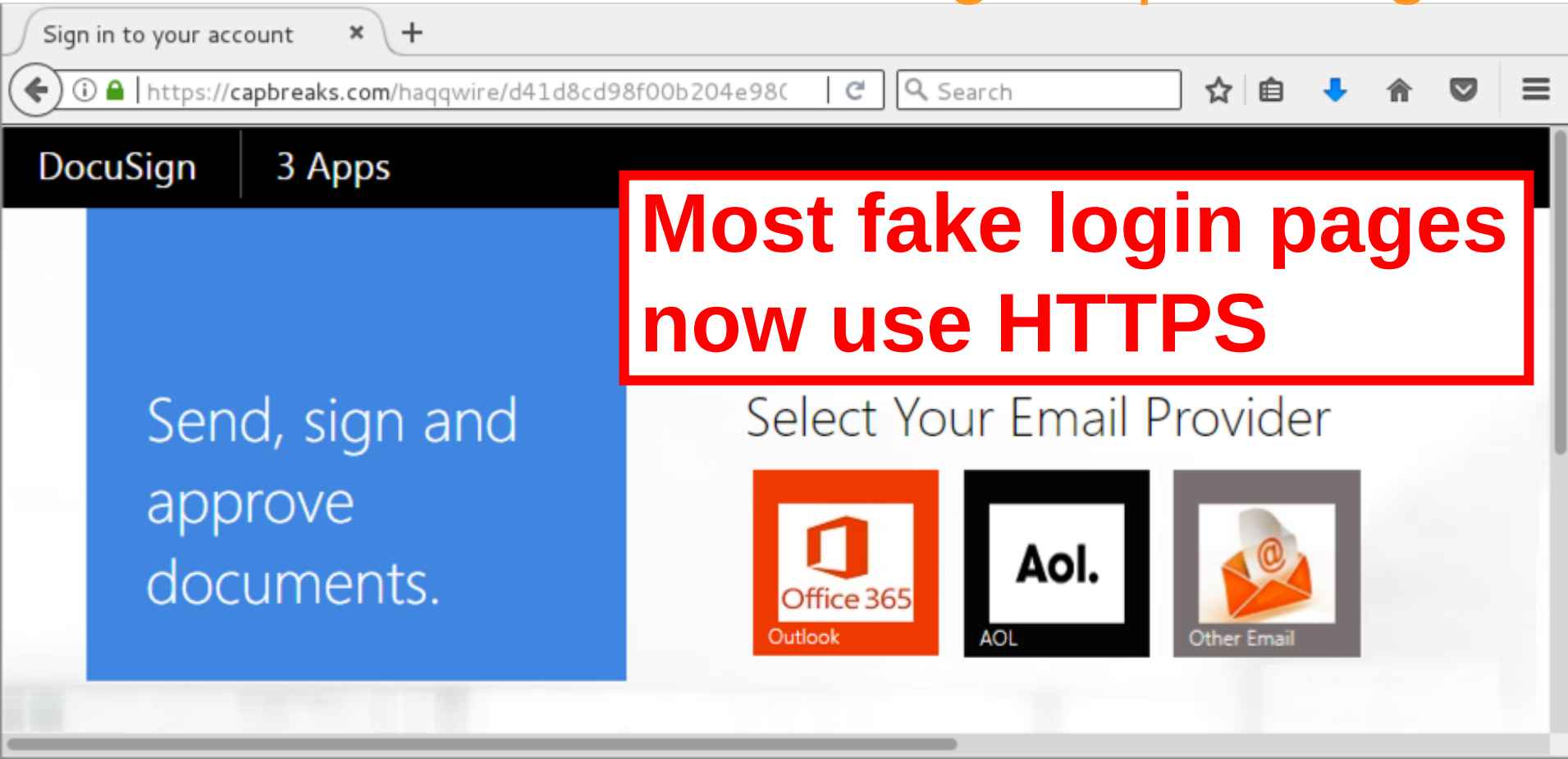
```
POST /registration/register_exec.php HTTP/1.1
Host: dailyprayer.us
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://dailyprayer.us/registration/register_form.php
Cookie: PHPSESSID=5mackm53o397517ekfiiv6hme2
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&cpassoword=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

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

- > Frame 317: 290 bytes on wire (2320 bits), 290 bytes captured
- > Ethernet II, Src: HewlettP_3c:94:1c (00:08:02:3c:94:1c), Dst:
- > Internet Protocol Version 4, Src: 172.16.1.109, Dst: 172.16.1.109
- > Transmission Control Protocol, Src Port: 49182, Dst Port: 88
- ▼ Kerberos
 - > Record Mark: 232 bytes
 - ▼ as-req
 - pvno: 5
 - msg-type: krb-as-req (10)
 - > padata: 1 item
 - ▼ req-body
 - Padding: 0

User information: Kerberos info

CNameString: ernest.webster

- ▼ req-body
 - Padding: 0
 - > kdc-options: 40810010 (forwardable, renewable,
 - ▼ cname
 - name-type: KRB5-NT-PRINCIPAL (1)
 - ▼ cname-string: 1 item
 - CNameString: ernest.webster
 - realm: VORTEXFOODS
 - > sname
- 

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

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.speedneedooxyz.xyz	POST /calis/fre.php HTTP/1.0
2018-02-15 16:33:56	31.220.104.230	80	www.speedneedooxyz.xyz	POST /calis/fre.php HTTP/1.0
2018-02-15 16:33:56	31.220.104.230	80	www.speedneedooxyz.xyz	POST /calis/fre.php HTTP/1.0
2018-02-15 16:34:57	31.220.104.230	80	www.speedneedooxyz.xyz	POST /calis/fre.php HTTP/1.0
2018-02-15 16:35:57	31.220.104.230	80	www.speedneedooxyz.xyz	POST /calis/fre.php HTTP/1.0
2018-02-15 16:36:57	31.220.104.230	80	www.speedneedooxyz.xyz	POST /calis/fre.php HTTP/1.0
2018-02-15 16:37:58	31.220.104.230	80	www.speedneedooxyz.xyz	POST /calis/fre.php HTTP/1.0
2018-02-15 16:38:58	31.220.104.230	80	www.speedneedooxyz.xyz	POST /calis/fre.php HTTP/1.0
2018-02-15 16:39:58	31.220.104.230	80	www.speedneedooxyz.xyz	POST /calis/fre.php HTTP/1.0
2018-02-15 16:40:59	31.220.104.230	80	www.speedneedooxyz.xyz	POST /calis/fre.php HTTP/1.0
2018-02-15 16:41:59	31.220.104.230	80	www.speedneedooxyz.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

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

..'.....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.....
.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

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

File not found.

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

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

File Help

http.request or http.response

http.request or http.response

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 Edit View Go Capture Analyze Statistics Telephony Wireless T

Open Ctrl+O

Open Recent

Merge...

Import from Hex Dump...

Close Ctrl+W

Save Ctrl+S

Save As... Ctrl+Shift+S

File Set

Export Specified Packets...

Export Packet Dissections

Export Packet Bytes... Ctrl+H

Export PDUs to File...

Export SSL Session Keys...

Export Objects

Print... Ctrl+P

Quit Ctrl+Q

Hypertext Transfer Protocol

port	Host
80	bakino.com
49174	
80	balaton-kornyeka
49178	
80	50.37.10.78
49179	
80	50.37.10.78
49180	
80	50.37.10.7
49181	

DICOM... Captured

HTTP... (c:47:ae), I

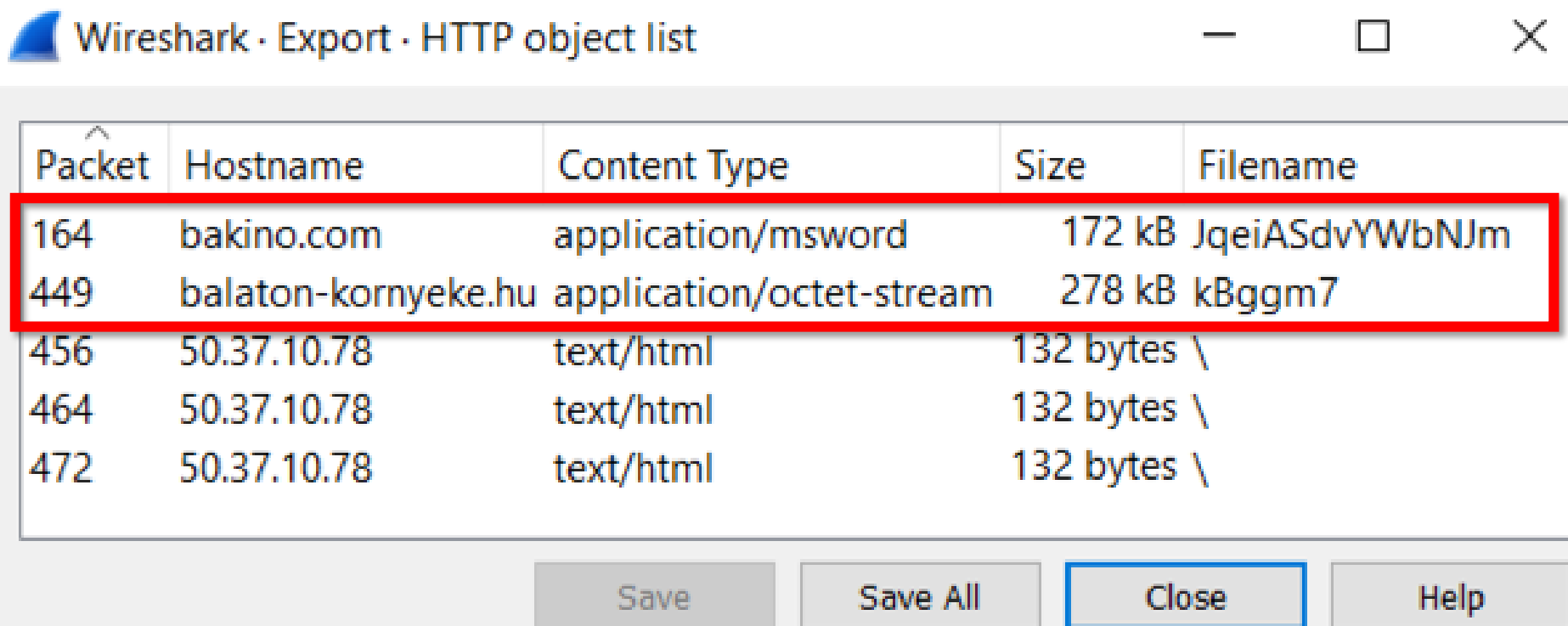
IMF... Dst: 176.2

SMB... Dst Port:

TFTP...

File →
Export Objects
→ HTTP

Windows malware: HTTP traffic



A screenshot of the 'Wireshark · Export · HTTP object list' dialog box. The dialog has a title bar with a blue icon, the text 'Wireshark · Export · HTTP object list', and standard window controls (minimize, maximize, close). Below the title bar is a table with five columns: Packet, Hostname, Content Type, Size, and Filename. The table contains five rows of data. The first two rows are highlighted with a red border. At the bottom of the dialog are four buttons: 'Save', 'Save All', 'Close', and 'Help'. The 'Close' button is highlighted with a blue border.

Packet	Hostname	Content Type	Size	Filename
164	bakino.com	application/msword	172 kB	JqeiASdvYWbNJm
449	balaton-kornyeke.hu	application/octet-stream	278 kB	kBggm7
456	50.37.10.78	text/html	132 bytes	\
464	50.37.10.78	text/html	132 bytes	\
472	50.37.10.78	text/html	132 bytes	\

Save Save All Close Help

Windows malware: HTTP traffic

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

or http.response

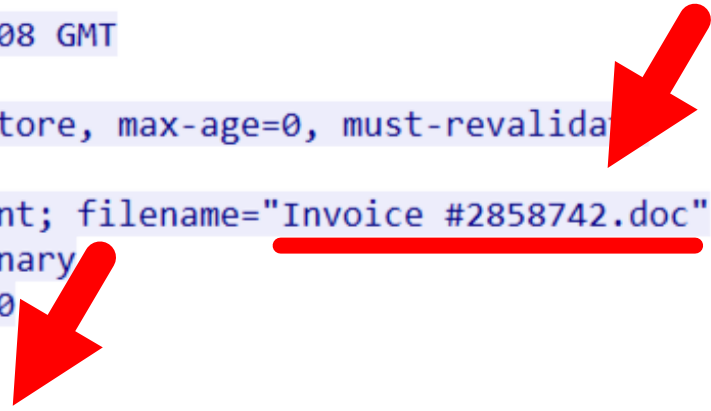
5-11	22:...	176.221.34.180	80	bankino.com	GET /JqeiASdvY
5-11	22:...	10.5.11.102	49174		HTTP/1.1 200 O
5-11	22:...	195.228.152.178	80	balaton-kornyeke.hu	/kBggm7/ H
5-11	22:...	10.5.11.102	49178		HTTP/1.1 200 O
5-11	22:...	50.37.10.78	80	50.37.10.78	GET / HTTP/1.1
5-11	22:...	10.5.11.102	49179		HTTP/1.1 200 O
5-11	22:...	50.37.10.78	80	50.37.10.78	GET / HTTP/1.1
5-11	22:...	10.5.11.102	49180		HTTP/1.1 200 O
5-11	22:...	50.37.10.78	80	50.37.10.78	GET / HTTP/1.1
5-11	22:...	10.5.11.102	49181		HTTP/1.1 200 O



Windows malware: HTTP traffic

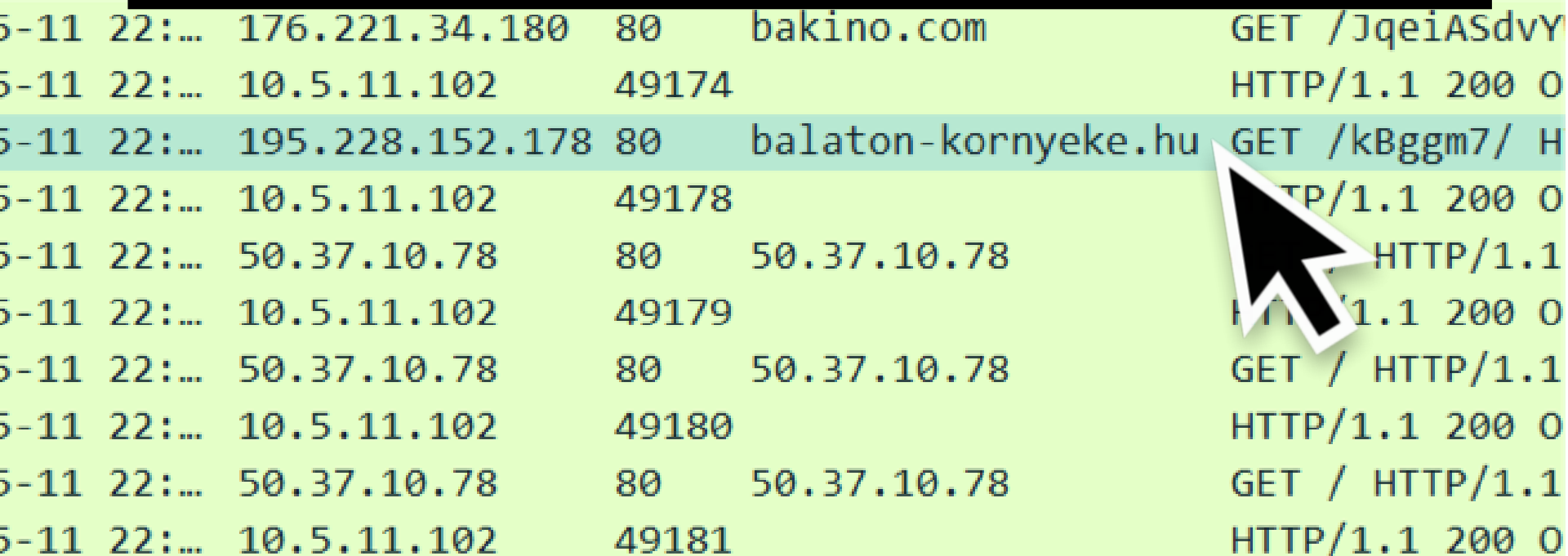
```
GET /JqeiASdvYwbNjM/ HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: bakino.com
DNT: 1
Connection: Keep-Alive
```

```
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-revalidate
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
```

Two red arrows are present. One arrow points from the right side of the image towards the filename 'Invoice #2858742.doc' in the 'Content-Disposition' header. The other arrow points from the bottom right towards the 'Content-Type: application/msword' line. The filename and the content type are underlined in red.

Windows malware: HTTP traffic

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



5-11	22:...	176.221.34.180	80	bakino.com	GET /JqeiASdvY
5-11	22:...	10.5.11.102	49174		HTTP/1.1 200 O
5-11	22:...	195.228.152.178	80	balaton-kornyeke.hu	GET /kBggm7/ H
5-11	22:...	10.5.11.102	49178		HTTP/1.1 200 O
5-11	22:...	50.37.10.78	80	50.37.10.78	HTTP/1.1
5-11	22:...	10.5.11.102	49179		HTTP/1.1 200 O
5-11	22:...	50.37.10.78	80	50.37.10.78	GET / HTTP/1.1
5-11	22:...	10.5.11.102	49180		HTTP/1.1 200 O
5-11	22:...	50.37.10.78	80	50.37.10.78	GET / HTTP/1.1
5-11	22:...	10.5.11.102	49181		HTTP/1.1 200 O

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-revalidate
Pragma: no-cache
Content-Disposition: attachment; filename="2392.exe"
Content-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

ssl.handshake.type == 1

Time	Dst	port	Server Name	Info
2018-02-22 02:16:43	185.48.239.33	443	lyhemsasit.ru	Client Hello
2018-02-22 02:16:44	185.48.239.33	443	lyhemsasit.ru	Client Hello
2018-02-22 02:16:45	185.48.239.33	443	lyhemsasit.ru	Client Hello
2018-02-22 02:16:46	185.48.239.33	443	lyhemsasit.ru	Client Hello

ZEUS PANDA BANKER

Windows malware: HTTPS traffic

ssl.handshake.type == 11

Time	Dst	port	Server Name	Info
2018-02-22 02:16:44	10.2.22.103	49160		Server Hello, Certificate, Server Hello Done
2018-02-22 02:16:44	10.2.22.103	49162		Server Hello, Certificate, Server Hello Done
2018-02-22 02:16:46	10.2.22.103	49163		Server Hello, Certificate, Server Hello Done
2018-02-22 02:16:46	10.2.22.103	49164		Server Hello, Certificate, Server Hello Done

>	Frame 8: 1023 bytes on wire (8184 bits), 1023 bytes captured (8184 bits)
>	Ethernet II, Src: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1), Dst: HewlettP_1c:47:ae (00:08:02:1c:47:ae)
>	Internet Protocol Version 4, Src: 185.48.239.33, Dst: 10.2.22.103
>	Transmission Control Protocol, Src Port: 443, Dst Port: 49164, Seq: 1, Ack: 156, Len: 969
✓	Secure Sockets Layer
>	TLSv1.2 Record Layer: Handshake Protocol: Server Hello
✓	TLSv1.2 Record Layer: Handshake Protocol: Certificate
	Content Type: Handshake (22)

Windows malware: encrypted traffic

- ▼ Handshake Protocol: Certificate
 - Handshake Type: Certificate (11)
 - Length: 865
 - Certificates Length: 862
- ▼ Certificates (862 bytes)
 - Certificate Length: 859
 - ▼ Certificate: 308203573082023fa003020102020900d95978148f37022d... (id-at-organizationName=De-
 - ▼ signedCertificate
 - version: v3 (2)
 - serialNumber: -2785062864854515155
 - > signature (sha1WithRSAEncryption)
 - ▼ issuer: rdnSequence (0)
 - ▼ rdnSequence: 3 items (id-at-organizationName=Default Company Ltd,id-at-localityName
 - > RDNSequence item: 1 item (id-at-countryName=XX)
 - > RDNSequence item: 1 item (id-at-localityName=Default City)
 - > RDNSequence item: 1 item (id-at-organizationName=Default Company Ltd)
 - > validity

Windows malware: encrypted traffic

rdnSequence items

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

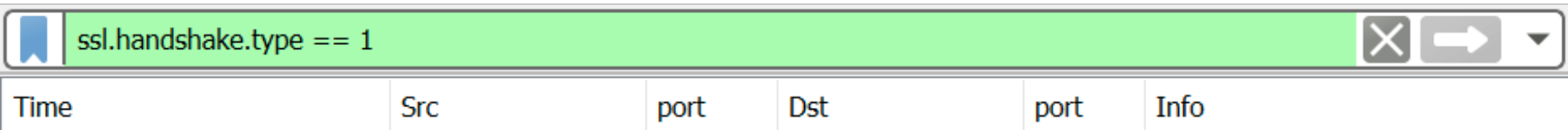
Windows malware: encrypted traffic

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

Apply a display filter ... <Ctrl-/>							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 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			
2018-02-22 01:57:54	10.2.22.102	49201	194.87.109.185	443	Continuation Data			

RAMNIT

Windows malware: encrypted traffic



A screenshot of the Wireshark network protocol analyzer interface. The top section shows a green capture filter bar with the text `ssl.handshake.type == 1`. Below this, the packet list pane is visible, showing a table with columns: Time, Src, port, Dst, port, and Info. The table is currently empty.

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

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

Wireshark · Follow TCP Stream (tcp.stream eq 0) · 2018-traffic-analysis-w... — □ ×

```
..K..... ^`L.B.;6..u.z....(iJ.....V].{.K. ...  
`..G.7:...).....(>N.@Q...RY.y.....Q.....Q.....Z._d&.R6.1..s.  
.(/...{..kf9B1 e...:..p..6..HA.....O.{..-7le..T..3....j.....(....6...  
$w9...2.....p..._..O..V...+.|QtDw...;.....
```

8 client pkts, 6 server pkts, 9 turns.

Entire conversation (254 bytes) ▾ Show and save data as ASCII ▾ Stream 0 ▴ ▾

Find:

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

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
2018-02-14 16:26:30	185.82.200.46	445	Create Request File:

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

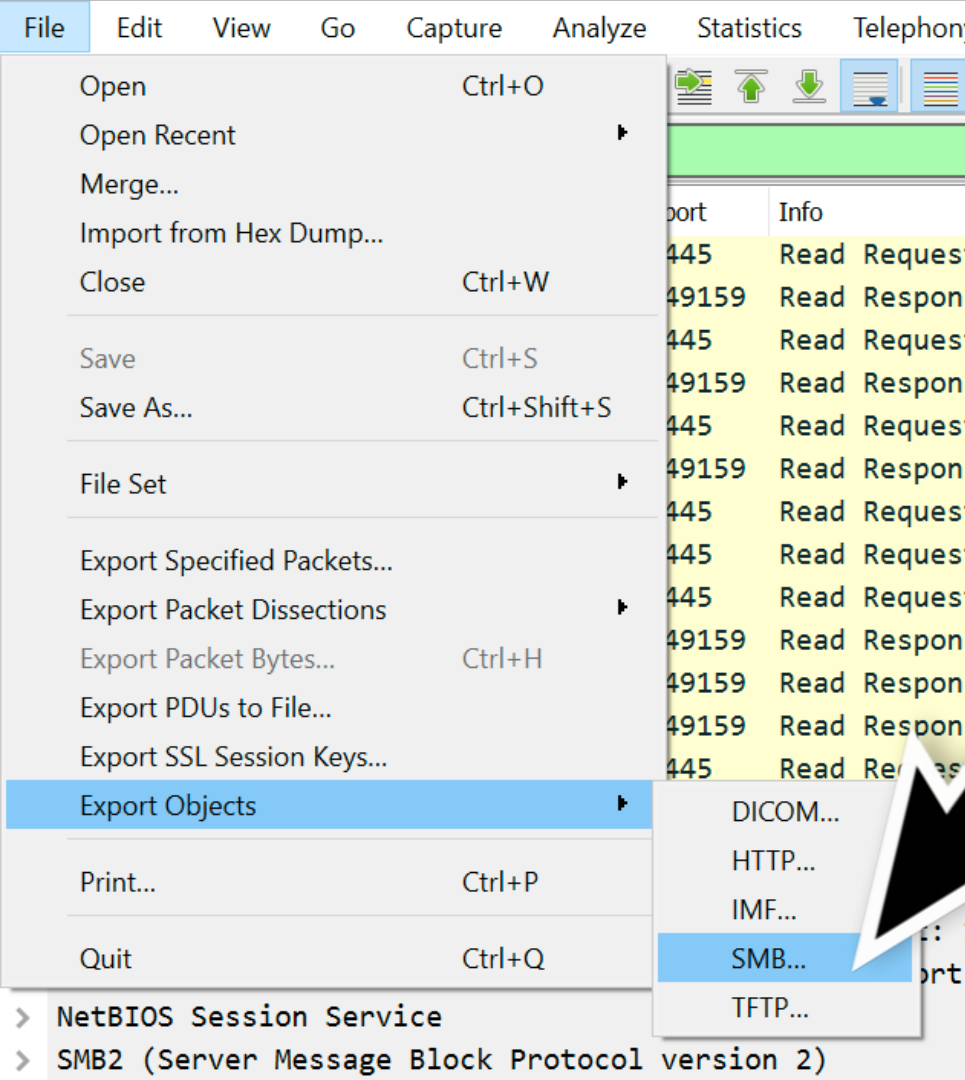
\\185.82.200.46\k

Windows malware: SMB traffic

Create Request File: yu.EXE

Create Response File: yu.EXE

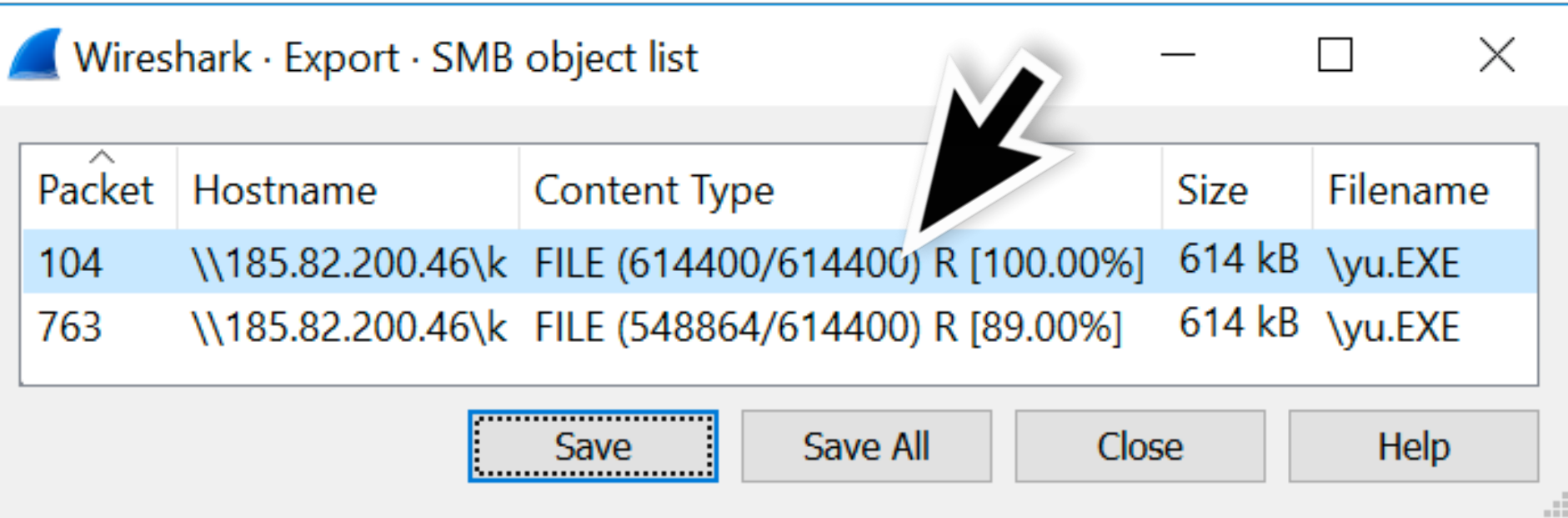
Retrieved **yu.EXE** from **\\185.82.200.46\k**



File →
Export Objects
→ SMB

Windows malware: SMB traffic

Select the entry that shows 100 %



Wireshark · Export · SMB object list

Packet	Hostname	Content Type	Size	Filename
104	\\185.82.200.46\k	FILE (614400/614400) R [100.00%]	614 kB	\yu.EXE
763	\\185.82.200.46\k	FILE (548864/614400) R [89.00%]	614 kB	\yu.EXE

Save Save All Close Help

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

Time	Source IP	Destination IP	Source Port	Destination Port	Protocol	Details
2018-02-21 03:24:40	10.2.21.1	10.2.21.101	53	59676	DNS	Standard query 0x8290 A newblogsite.duckdns.org
2018-02-21 03:24:40	10.2.21.101	10.2.21.1	59676	53	DNS	Standard query response 0x8290 A newblogsite.duckdns.org A 46.16...
2018-02-21 03:24:40	46.166.161.56	10.2.21.1	34481	49173	TCP	49173 → 34481 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
2018-02-21 03:24:44	46.166.161.56	10.2.21.1	80	49176	TCP	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	10.2.21.1	80	49177	TCP	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	10.2.21.101	53	57038	DNS	Standard query 0xd517 A nowdownload.duckdns.org
2018-02-21 03:27:02	10.2.21.101	10.2.21.1	57038	53	DNS	Standard query response 0xd517 A nowdownload.duckdns.org A 46.16...
2018-02-21 03:27:02	46.166.161.56	10.2.21.1	80	49218	TCP	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	10.2.21.101	53	54216	DNS	Standard query 0x236b A nowdownload.duckdns.org
2018-02-21 03:27:24	10.2.21.101	10.2.21.1	54216	53	DNS	Standard query response 0x236b A nowdownload.duckdns.org A 46.16...
2018-02-21 03:27:24	46.166.161.56	10.2.21.1	80	49219	TCP	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	10.2.21.101	53	53195	DNS	Standard query 0xad42 A newcanbernew.duckdns.org
2018-02-21 03:27:25	10.2.21.101	10.2.21.1	53195	53	DNS	Standard query response 0xad42 A newcanbernew.duckdns.org A 62.1...
2018-02-21 03:27:25	62.102.148.185	10.2.21.1	25909	49220	TCP	49220 → 25909 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
2018-02-21 03:27:26	10.2.21.1	10.2.21.101	53	53195	DNS	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**

Time	Dst	port	Host	Info
2018-02-21 03:24:40	10.2.21.1	53		Standard query 0x8290 A...
2018-02-21 03:24:40	10.2.21.101	59676		Standard query response...
2018-02-21 03:24:40	46.166.161.56	34481		49173 → 34481 [SYN] Seq...
2018-02-21 03:24:41	46.166.161.56	34481	newblogsite.duckdns.org:34481	GET / HTTP/1.1
2018-02-21 03:24:44	46.166.161.56	80		49176 → 80 [SYN] Seq=0 ...
2018-02-21 03:24:44	46.166.161.56	80	46.166.161.56	GET /man.exe HTTP/1.1
2018-02-21 03:24:57	46.166.161.56	80		49177 → 80 [SYN] Seq=0 ...
2018-02-21 03:24:57	46.166.161.56	80	46.166.161.56	GET /drop.exe HTTP/1.1
2018-02-21 03:27:02	10.2.21.1	53		Standard query 0xd517 A...
2018-02-21 03:27:02	10.2.21.101	57038		Standard query response...
2018-02-21 03:27:02	46.166.161.56	80		49218 → 80 [SYN] Seq=0 ...
2018-02-21 03:27:02	46.166.161.56	80	nowdownload.duckdns.org:80	GET /laZ.txt HTTP/1.0
2018-02-21 03:27:24	10.2.21.1	53		Standard query 0x236b A...

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

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

Time	Dst	port	Info
2018-02-21 03:27:26	62.102.148.185	25909	49220 → 25909 [PSH, ACK] Seq=107 Ack=60

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 seomarketing

331 User seomarketing 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 questions.

Thanks & Regards
Laxmi Ghale



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

Phishing pages

Sign in to your account

https://redproduction.biz/Server/3657/3657/008483iclive/df784d80e18e2d4a8c7005e6

Office 365

Work or school, or personal Microsoft account

Email or phone

Password

☐ Keep me signed in

Sign in

[Can't access your account?](#)

Łączyć

Conecte

連接

Ligue

Connect

تواصل

Verbinden

つなぐ

Phishing pages

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

http.request

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

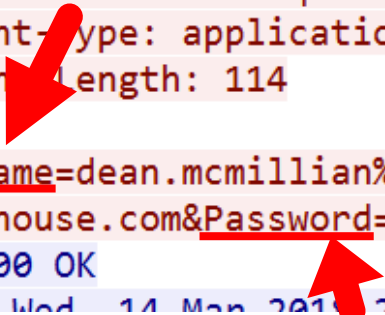
**ip.addr eq 23.229.153.228 and
tcp.port eq 47766**

Time	Dst	port	Host	Info
2018-03-14 21:02:10	23.229.153.228	80		47766 → 80 [SYN] Seq=0 Win=...
2018-03-14 21:02:10	10.3.14.102	47766		80 → 47766 [SYN, ACK] Seq=0...
2018-03-14 21:02:10	23.229.153.228	80		47766 → 80 [ACK] Seq=1 Ack=...
2018-03-14 21:02:10	23.229.153.228	80	abcontracting.us	POST /Gn/offphp.php HTTP/1...
2018-03-14 21:02:10	10.3.14.102	47766		80 → 47766 [ACK] Seq=1 Ack=...
2018-03-14 21:02:11	10.3.14.102	47766		HTTP/1.1 200 OK (text/html
2018-03-14 21:02:11	23.229.153.228	80		47766 → 80 [ACK] Seq=571 Ac...
2018-03-14 21:02:11	23.229.153.228	80	abcontracting.us	GET /Gn/error.php HTTP/1.1
2018-03-14 21:02:11	10.3.14.102	47766		80 → 47766 [ACK] Seq=350 Ac...
2018-03-14 21:02:11	10.3.14.102	47766		HTTP/1.1 200 OK (text/html
2018-03-14 21:02:11	23.229.153.228	80		47766 → 80 [ACK] Seq=955 Ac...
2018-03-14 21:02:11	23.229.153.228	80	abcontracting.us	GET /Gn/css/logo.jpg HTTP/1

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

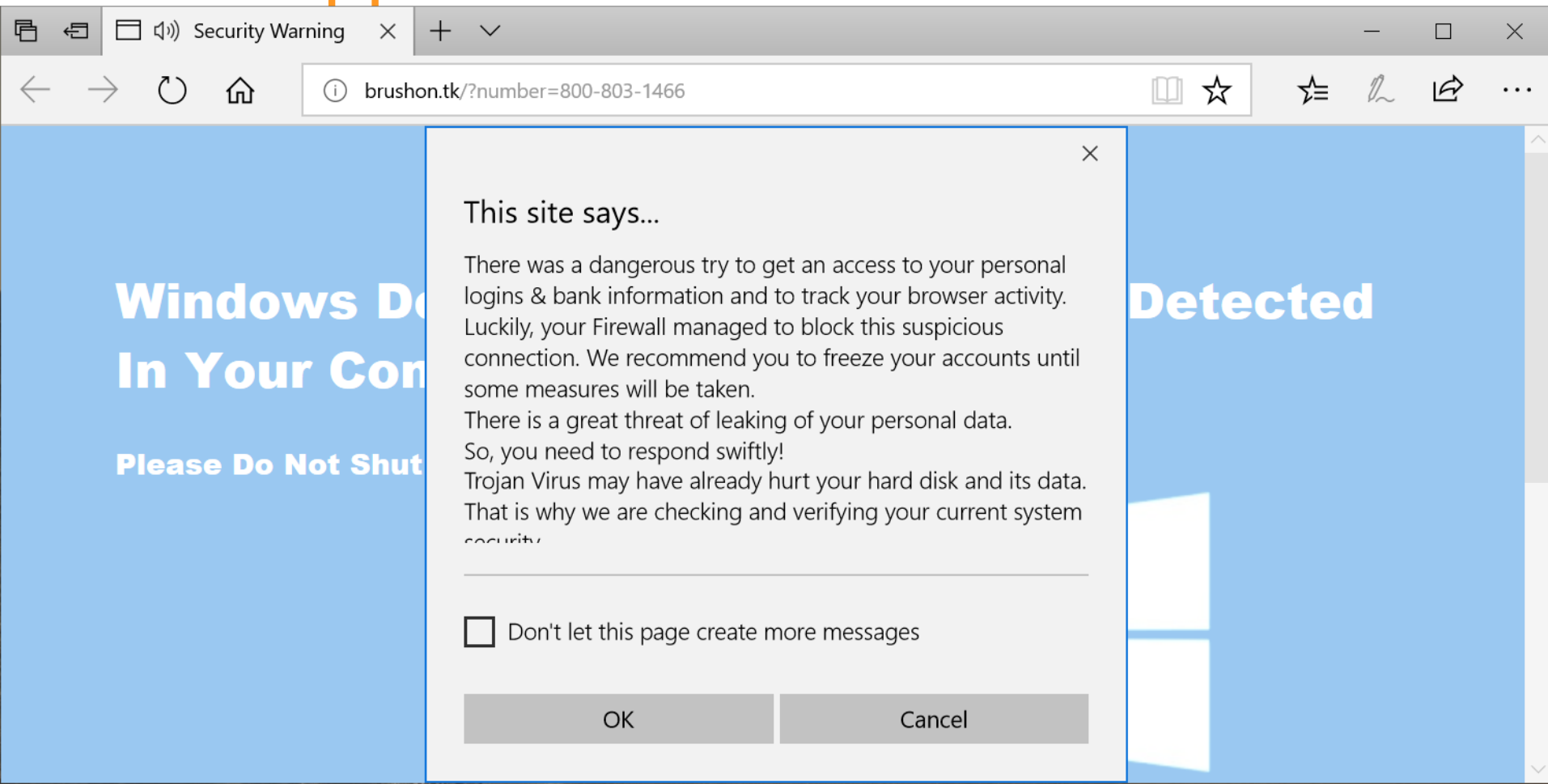
UserName=dean.mcmillian%40tenderloin-
warehouse.com&Password=tenderloinahoy12345%24&AuthMethod=FormsAuthenticationHTTP/
1.1 200 OK
Date: Wed, 14 Mar 2016 21:02:10 GMT
```



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

Time	Src	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.googleapis...	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

```
22:54:34 218.58.195.1... 80 fonts.googleap... GET /css?family=Lato%3A500,4
22:55:34 54.36.180.110 80 thestillness.tk GET /?MGjJPm HTTP/1.1
22:55:34 54.36.151.52 80 brushon.tk GET /?number=800-803-1466 HT
22:55:34 54.36.151.52 80 brushon.tk GET /css HTTP/1.1
22:55:34 54.36.151.52 80 brushon.tk GET /include/edge/defender.p
22:55:34 54.36.151.52 80 brushon.tk GET /auth.php?n=800-803-1466
22:55:35 99.198.108.1... 80 balans.shahter... GET /?utm_medium=4c23b9fecf7
22:55:41 54.36.151.52 80 brushon.tk GET /include/en.mp3 HTTP/1.1
```

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">
```

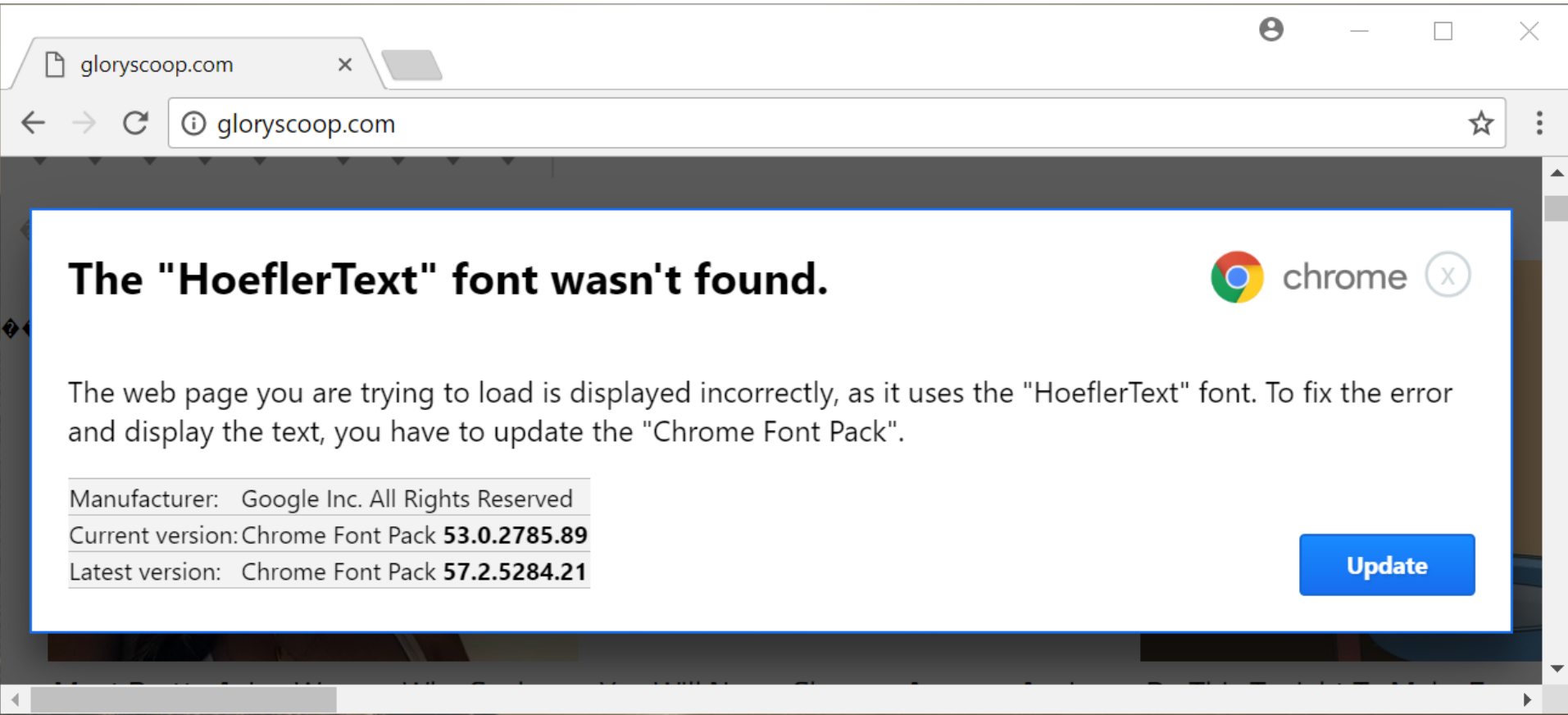
```
<script type="text/javascript">
```

```
    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

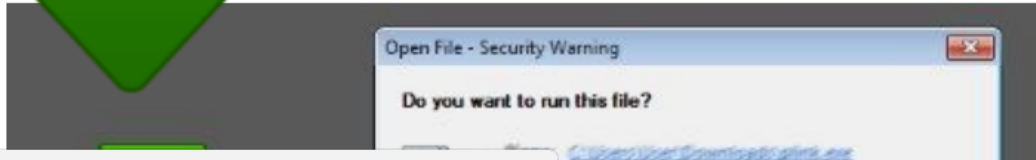
This type of file can harm your computer. Do you want to keep **Font update.exe** anyway?

The "eflerText" font wasn't found.



Step 1: In the bottom left corner of the screen you'll see the download bar. **Click on the Chrome_Font.exe** item.

Step 2: Click on the **(Run)** button 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



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]

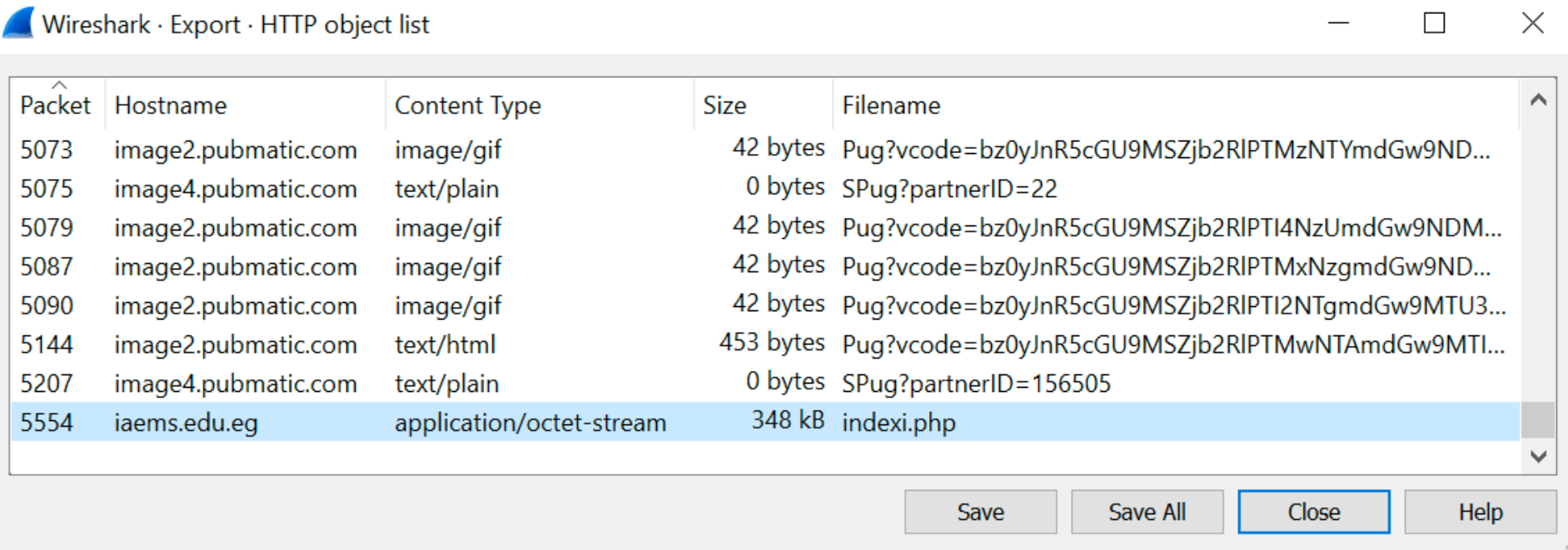
```
GET /indexi.php HTTP/1.1
Host: iaems.edu.eg
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/65.0.3325.162 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8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

Popups/unexpected web pages

- File → Export Object → HTTP...

The image shows a screenshot of the 'Wireshark · Export · HTTP object list' dialog box. It features a table with five columns: Packet, Hostname, Content Type, Size, and Filename. The table lists several HTTP objects, with the last one (Packet 5554) highlighted in blue. At the bottom of the dialog are four buttons: 'Save', 'Save All', 'Close', and 'Help'. The 'Close' button is currently selected with a blue border.

Packet	Hostname	Content Type	Size	Filename
5073	image2.pubmatic.com	image/gif	42 bytes	Pug?vcode=bz0yJnR5cGU9MSZjb2RIPTMzNTYmdGw9ND...
5075	image4.pubmatic.com	text/plain	0 bytes	SPug?partnerID=22
5079	image2.pubmatic.com	image/gif	42 bytes	Pug?vcode=bz0yJnR5cGU9MSZjb2RIPTI4NzUmdGw9NDM...
5087	image2.pubmatic.com	image/gif	42 bytes	Pug?vcode=bz0yJnR5cGU9MSZjb2RIPTMxNzgmdGw9ND...
5090	image2.pubmatic.com	image/gif	42 bytes	Pug?vcode=bz0yJnR5cGU9MSZjb2RIPTI2NTgmdGw9MTU3...
5144	image2.pubmatic.com	text/html	453 bytes	Pug?vcode=bz0yJnR5cGU9MSZjb2RIPTMwNTAmdGw9MTI...
5207	image4.pubmatic.com	text/plain	0 bytes	SPug?partnerID=156505
5554	iaems.edu.eg	application/octet-stream	348 kB	indexi.php

Save Save All Close Help

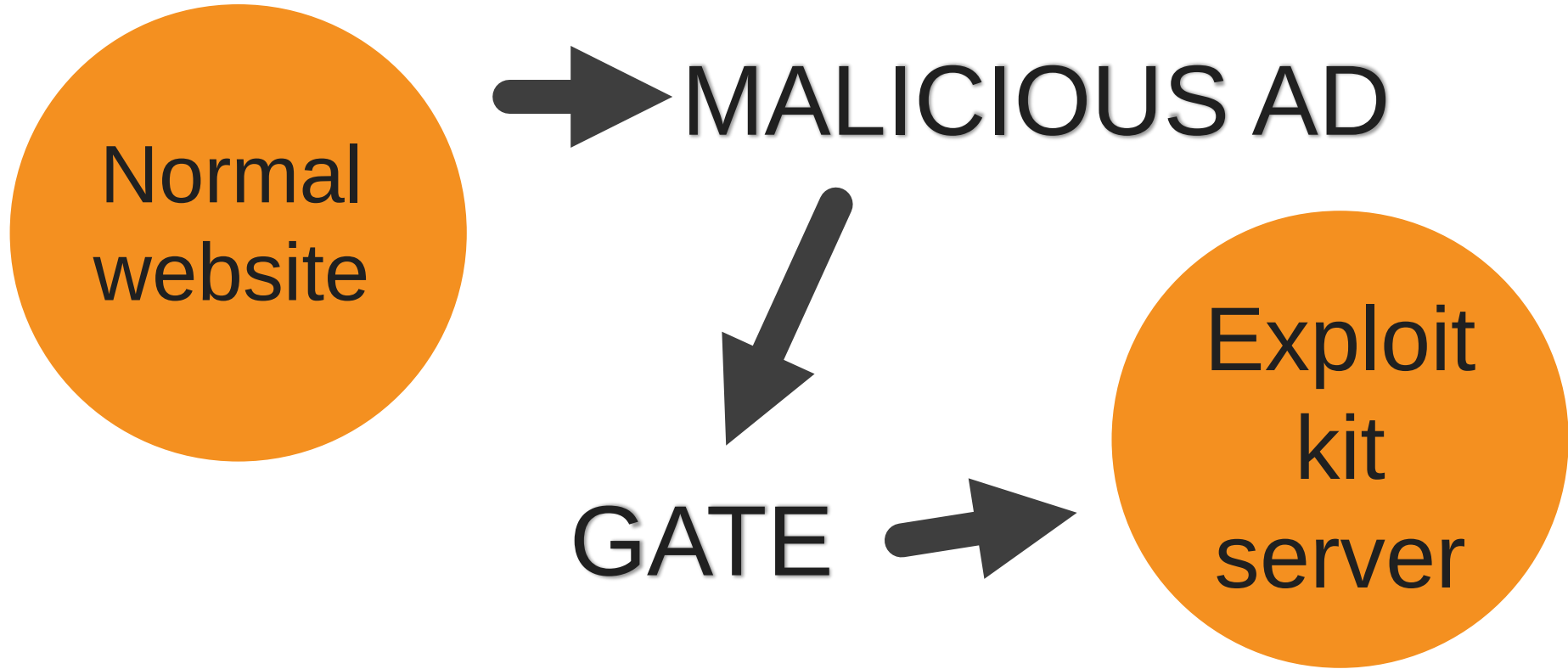
Block 4 - Up next...

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

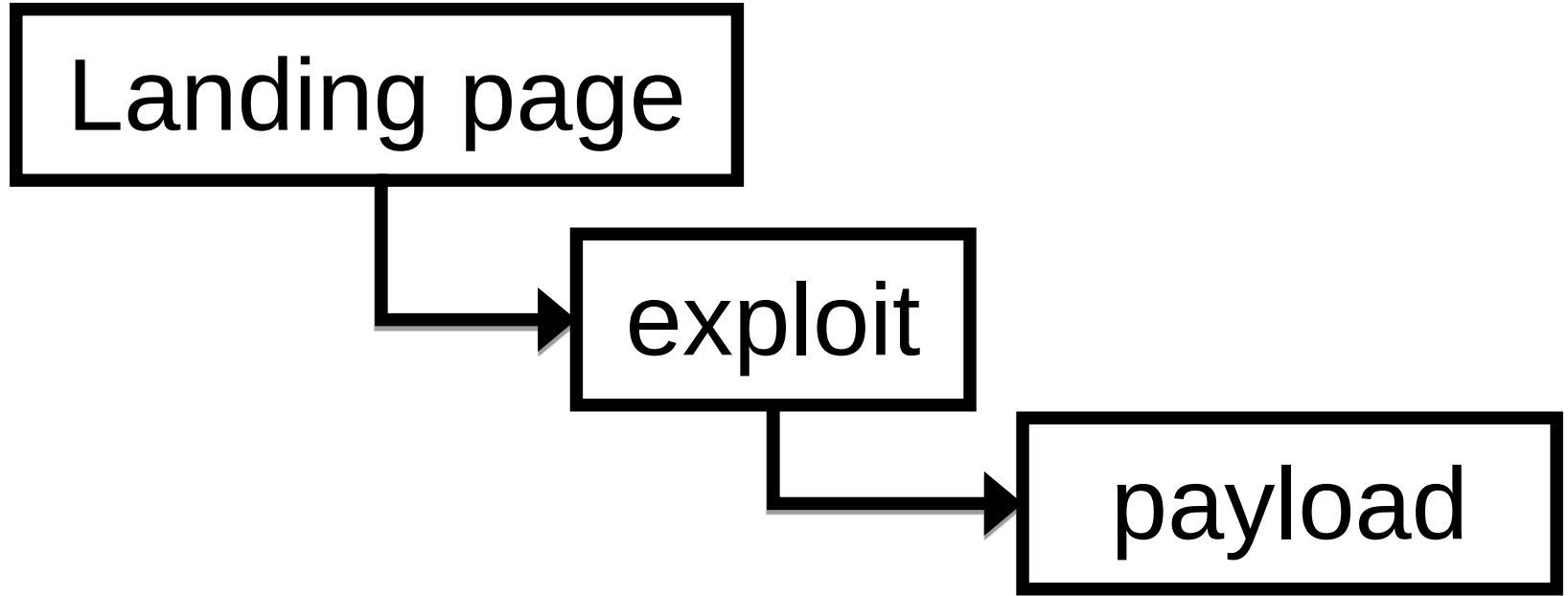
Exploit kits

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

Time	Dst	port	Host	Info
2018-03-1...	92.53.120.248	80	92.53.120.248	GET /?NTcwMjgx&uqlTBc0&YToLUQBa=bWlsaw==&...
2018-03-1...	10.3.15.103	49228		HTTP/1.1 200 OK (text/html)
2018-03-1...	92.53.120.248	80	92.53.120.248	GET /?MzYzNTAy&DXskBLhxedk&lRjixF=dW5rbm...
2018-03-1...	10.3.15.103	49228		HTTP/1.1 200 OK (application/x-shockwave...
2018-03-1...	92.53.120.248	80	92.53.120.248	GET /?Mzg5NDQ5&egrQbX&nx52fgbs=wX3QMvXcJw...
2018-03-1...	10.3.15.103	49229		HTTP/1.1 200 OK (application/x-msdownload)

```
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_kGKUQNC950QHfmmF7F 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...Ye0.....|.
/$.....s9.?.....$.>.HUc@...tK...o.0.<.v.m..e|<..rV....VcDZ...n...C..[{...#...}
ZC.T.....j.m#[.g..x(..4G.....g.1..Df...C.z?g5D.....U!.sP....VeE# /...G.C.<..?B.
```

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: ae30ec73d67bc3ca1afa07cfb9fbecbbe14fe55c

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)

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

Time	Dst	port	Host	Info
2018-05-14 22:23:11	91.189.95.21	6969	torrent.ubuntu.com:6969	GET /announce?info_hash=%e4%b...

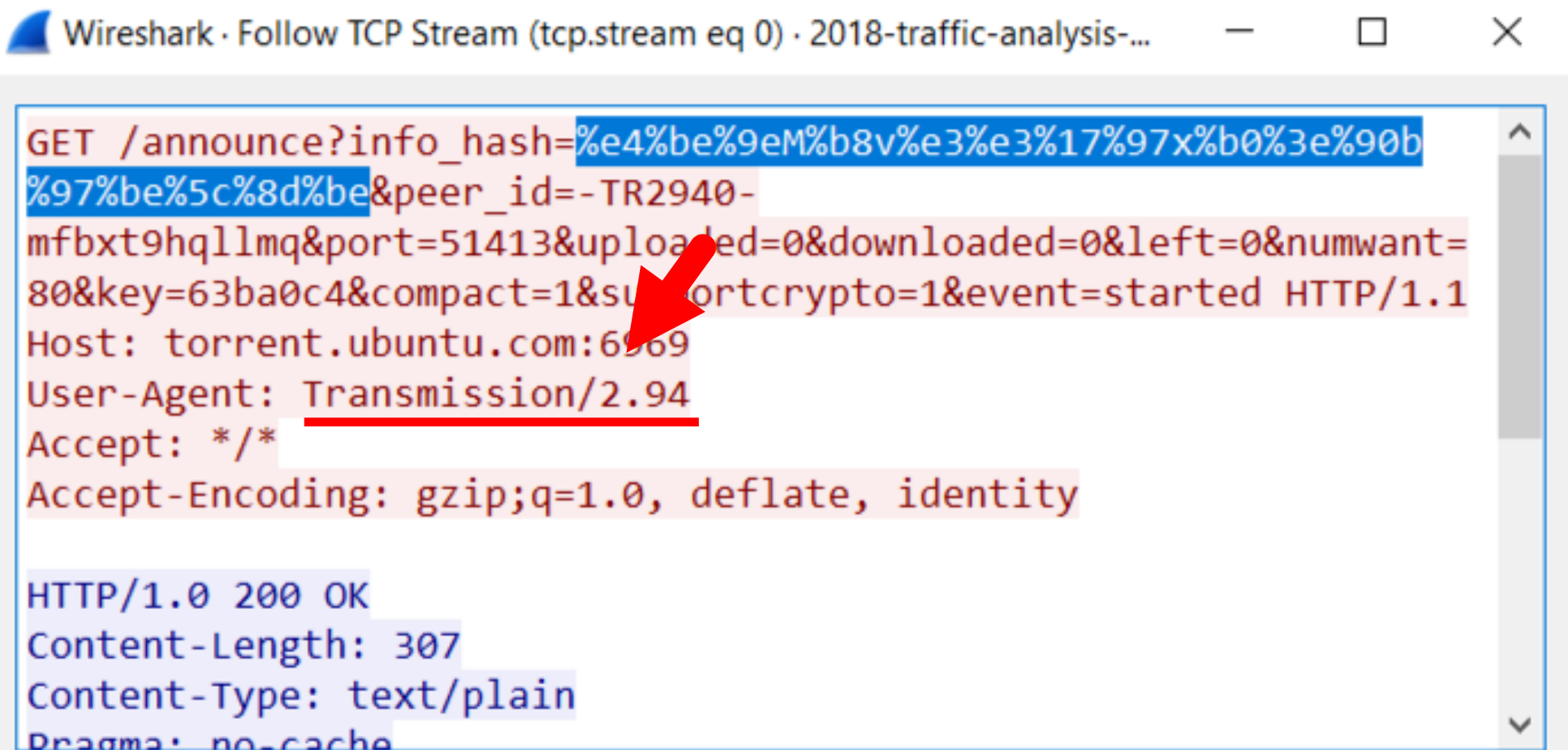
torrent.ubuntu.com:6969

- **GET /announce?info_hash=**

In similar traffic, you might also see:

- **GET /scrape?info_hash=**

Torrent traffic



asciitohex.com

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

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

> Frame 122: 122 bytes on wire (976 bits), 122 bytes captured (976 bits)
> Ethernet II, Src: HewlettP_1c:47:ae (00:08:02:1c:47:ae), Dst: Netgear_b6:93:f1 (20:08:00:07:63:00)
> Internet Protocol Version 4, Src: 10.3.18.105, Dst: 124.150.93.183
> Transmission Control Protocol, Src Port: 49642, Dst Port: 46613, Seq: 1, Ack: 1, Len: 0

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 Ctrl+Shift+F

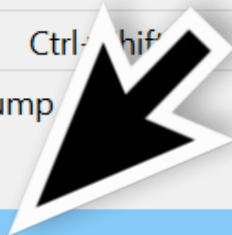
Bytes as Hex + ASCII Dump

...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
Space15132167d04eda34d3a0d664e57abccbf287b0a749024395; 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

.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

Time	port	Host	Info
2018-04-22 04:42...	80	omgbohpooh.ruptured-lhmnationstex.xyz	GET /commanders_cutting.html
2018-04-22 04:42...	80	omgbohpooh.ruptured-lhmnationstex.xyz	GET /getversionpd/1/2/3/4 HT
2018-04-22 04:42...	80	omgbohpooh.ruptured-lhmnationstex.xyz	GET /favicon.ico HTTP/1.1
2018-04-22 04:42...	80	omgbohpooh.ruptured-lhmnationstex.xyz	GET /2/3913 HTTP/1.1

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



A screenshot of a Wireshark packet capture table. The table has five columns: Time, port, Host, Server Name, and Info. It displays a list of HTTP GET requests. The first request is to elitegol.me, and the subsequent ones are to various subdomains ofblogspot.com. The table is filtered with the expression 'http.request or ssl.handshake.type == 1'.

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 /-5M07aTt7R4Y/Ui2UgUyn_E
2018-04-22 04:42...	80	2.bp.blogspot.com		GET /-_dSxbJpAqGM/UQM1baugH9
2018-04-22 04:42...	80	3.bp.blogspot.com		GET /-r0sfBHt7XIU/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

Time	port	Host	Info
2018-04-22 04:42...	80	omgbohpooh.ruptured-lhmnationstex.xyz	GET /commanders_cutting.html
2018-04-22 04:42...	80	omgbohpooh.ruptured-lhmnationstex.xyz	GET /getversionpd/1/2/3/4 HT
2018-04-22 04:42...	80	omgbohpooh.ruptured-lhmnationstex.xyz	GET /favicon.ico HTTP/1.1
2018-04-22 04:42...	80	omgbohpooh.ruptured-lhmnationstex.xyz	GET /2/3913 HTTP/1.1

omgbohpooh.ruptured-lhmnationstex.xyz

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

Root causes from web traffic

```
GET /commanders_cutting.html HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Referer: http://www.theadgateway.com/a/display.php?
r=1569697&sub1=114842&treqn=849970631&runauction=1&curr=c174e1402fa4c67c610awhGcug2ckFmRy
USZt5CbvdWZ0lGbl5yd3dnRyUiRyUSQzUCc0RHa3b037b4c6bb35bb3e078&cbrandom=0.05035956778904127
&cbtitle=&cbiframe=1&cbwidth=17&cbheight=0&cbdescription=&cbkeywords=&cbref=http%3A%2F
%2Fwww.elitegol.me%2Fadsh.php
Accept-Language: en-US
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)
Accept-Encoding: gzip, deflate
Host: omgbohpooh.ruptured-lhmnationstex.xyz
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Sun, 22 Apr 2018 04:42:57 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
```



Referer:

Root causes from web traffic

ip contains omgbohpooh.ruptured-lhmnationstex.xyz

ip contains omgbohpooh.ruptured-lhmnationstex.xyz					Expression...	+ Apply this filter
Time	port	Host	Info			
2018-04-22 04:42...	62...		HTTP/1.1 302 Found (te			
2018-04-22 04:42...	80	omgbohpooh.ruptured-lhmnationstex.xyz	GET /commanders_cutting			
2018-04-22 04:42...	80	omgbohpooh.ruptured-lhmnationstex.xyz	GET /getversionpd/1/2/3			
2018-04-22 04:42...	80	omgbohpooh.ruptured-lhmnationstex.xyz	GET /favicon.ico HTTP/1			
2018-04-22 04:42...	80	omgbohpooh.ruptured-lhmnationstex.xyz	GE /2/3913 HTTP/1.1			

HTTP/1.1 302 found

Root causes from web-based infections

Referer lines may not contain all requests in the chain

```
GET /19sLb5?  
external_id=15243721640842711042239391679741842&ad_campaign_id=103519620&source=Adcash&s  
ub_id_1=1569697-3295255860-0 HTTP/1.1  
Accept: text/html, application/xhtml+xml, */*  
Referer: http://www.theadgateway.com/a/display.php?  
r=1569697&sub1=114842&treqn=849970631&runauction=1&crr=c174e1402fa4c67c610awhGcug2ckFmRy  
USZt5CbvdWZ0lGbl5yd3dnRyUiRyUSQzUCC0RHa3b037b4c6bb35bb3e078&cbrandom=0.05035956778904127  
&cbtitle=&cbiframe=1&cbWidth=17&cbHeight=0&cbdescription=&cbkeywords=&cbref=http%3A%2F  
%2Fwww.elitegol.me%2Fadsh.php  
Accept-Language: en-US  
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)  
Accept-Encoding: gzip, deflate  
Host: cash123.us  
Connection: Keep-Alive
```

Host: cash123.us

Same Referer:

```
HTTP/1.1 302 Found  
Server: nginx  
Date: Sun, 22 Apr 2018 04:42:51 GMT  
3 client pkts, 3 server pkts, 3 turns
```

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

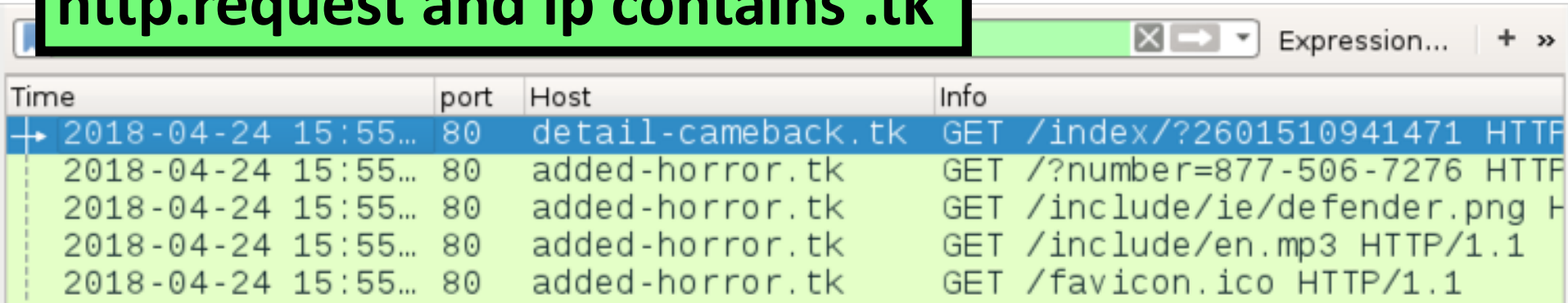
Event Message

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



Wireshark packet capture interface showing a list of HTTP requests. The first packet is highlighted in blue.

Time	port	Host	Info
2018-04-24 15:55...	80	detail-cameback.tk	GET /index/?2601510941471 HTTP/1.1
2018-04-24 15:55...	80	added-horror.tk	GET /?number=877-506-7276 HTTP/1.1
2018-04-24 15:55...	80	added-horror.tk	GET /include/ie/defender.png HTTP/1.1
2018-04-24 15:55...	80	added-horror.tk	GET /include/en.mp3 HTTP/1.1
2018-04-24 15:55...	80	added-horror.tk	GET /favicon.ico HTTP/1.1

- **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
78.155.219.199	447				ET POLICY PE EXE or DLL Windows file download HTTP
					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)

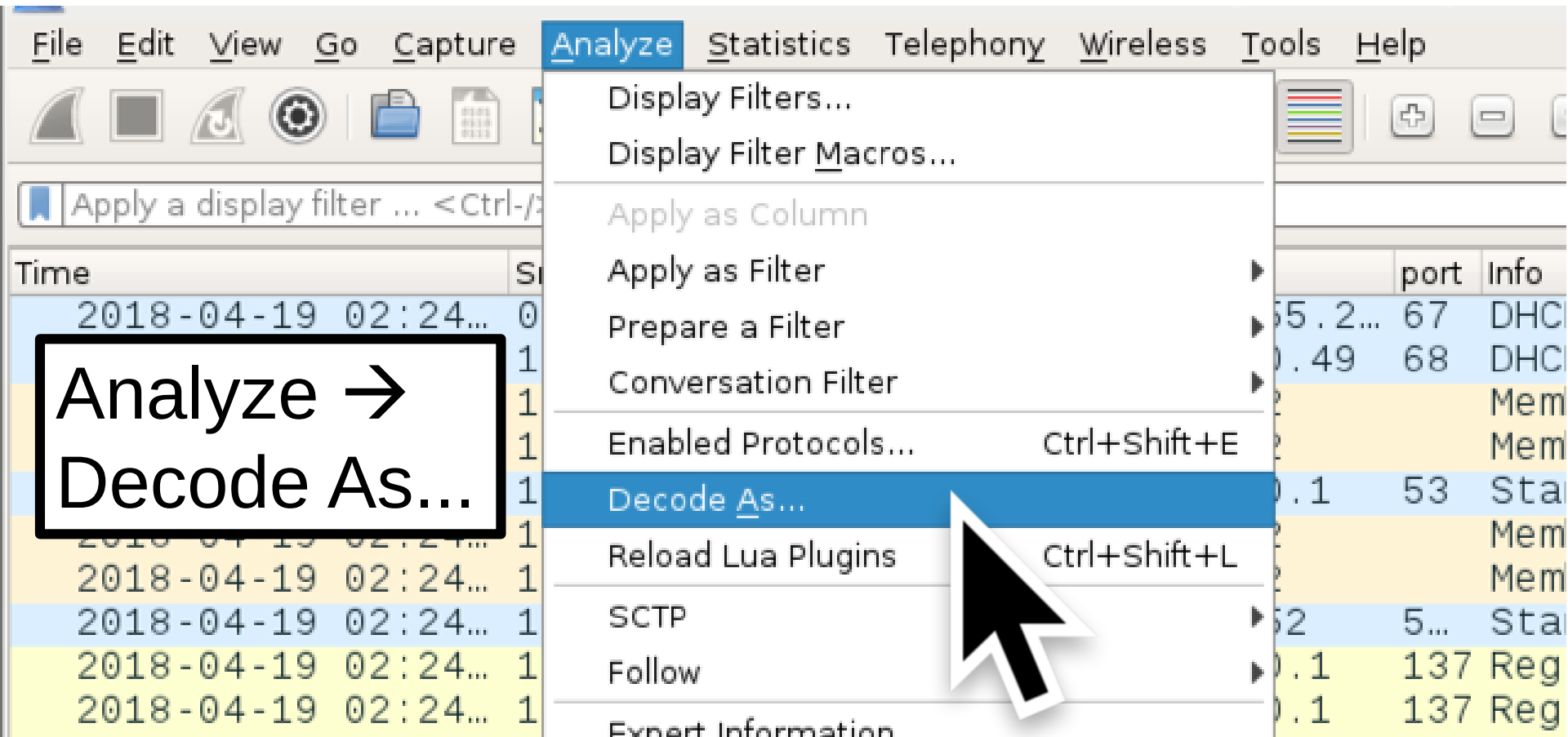
ETPRO TROJAN Trickbot SSL Certificate Detected

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

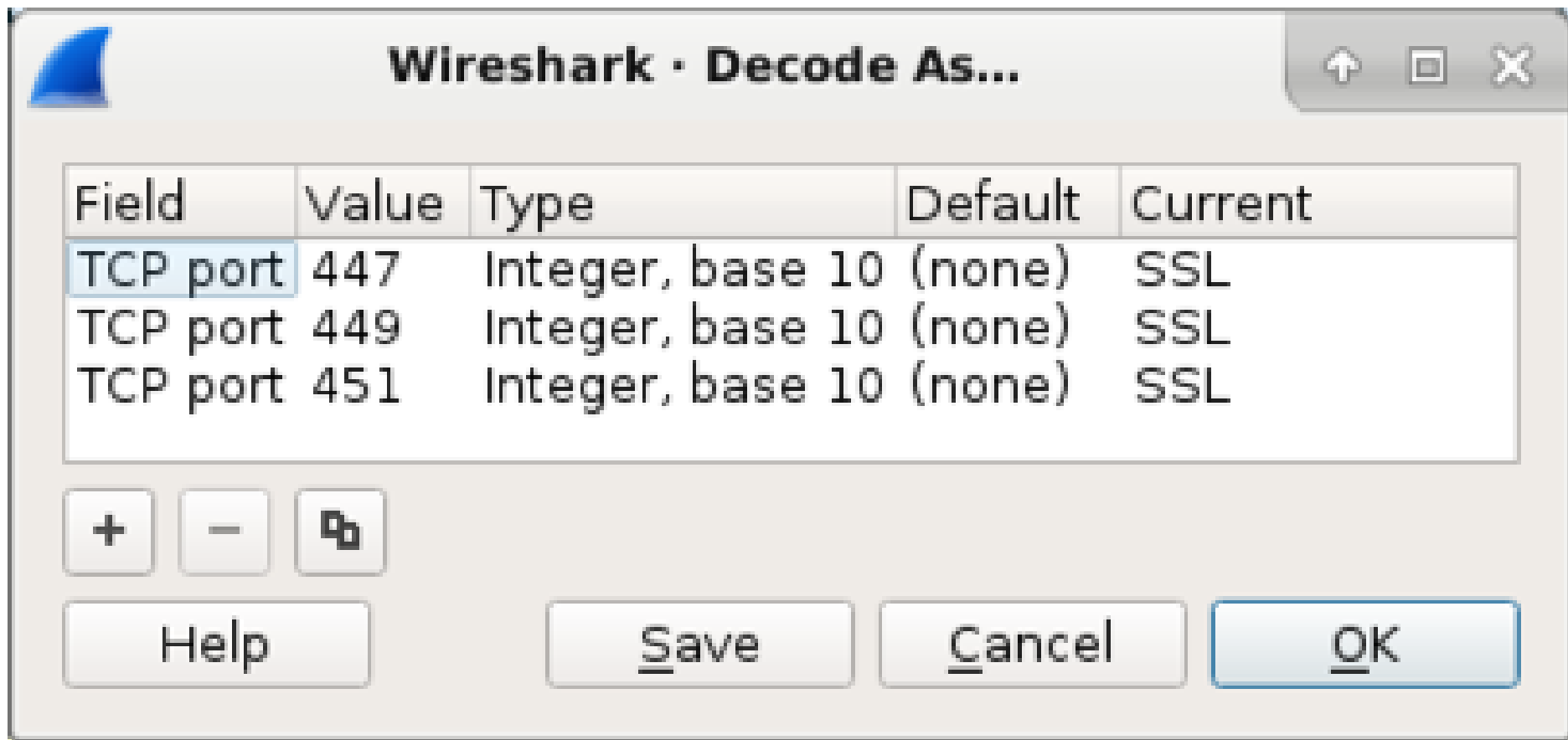


The image shows the Wireshark network protocol analyzer interface. The 'Analyze' menu is open, and the 'Decode As...' option is highlighted. A mouse cursor is pointing at the 'Decode As...' option. A text box on the left side of the interface contains the text 'Analyze → Decode As...'. The background shows a packet list table with columns for Time, Size, and Protocol. The selected packet is a DHCP packet (port 67) from 192.168.1.1 to 192.168.1.100.

Analyze → Decode As...

Time	Size	Protocol	port	Info
2018-04-19 02:24...	0	DHCP	67	DHC
2018-04-19 02:24...	1	DHCP	68	DHC
2018-04-19 02:24...	1	Mem		Mem
2018-04-19 02:24...	1	Mem		Mem
2018-04-19 02:24...	1	Sta	53	Sta
2018-04-19 02:24...	1	Mem		Mem
2018-04-19 02:24...	1	Mem		Mem
2018-04-19 02:24...	1	SCTP	5...	Sta
2018-04-19 02:24...	1	Follow	137	Reg
2018-04-19 02:24...	1	Expert Information	137	Reg

Root causes from malspam campaigns



Root causes from malspam campaigns

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

Time	Source IP	Destination IP	Port	Host	Request	Response
2018-04-19 02:25...	107.180.25.48	80	ccmlongueuil.ca	GET /seclogo.bin	HTTP/1.1	200 OK
2018-04-19 02:27...	216.239.36.21	80	ipinfo.io	GET /ip	HTTP/1.1	200 OK
2018-04-19 02:27...	54.221.221.65	80	api.ipify.org	GET /	HTTP/1.1	200 OK
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/		200 OK
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/		200 OK
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/		200 OK
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/		200 OK
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/		200 OK
2018-04-19 02:31...	8.253.112.121	80	www.download.windowsupdate.com	GET /msdownload/update/v3/		200 OK
2018-04-19 02:31...	8.253.112.121	80	www.download.windowsupdate.com	GET /msdownload/update/v3/		200 OK
2018-04-19 02:31...	8.253.112.121	80	www.download.windowsupdate.com	GET /msdownload/update/v3/		200 OK
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



"ccmlongueuil.ca" "seclogo.bin" trickbot

All

Maps

Videos

Shopping

News

More

Settings

Tools

About 5 results (0.42 seconds)

URLhaus | <http://ccmlongueuil.ca/seclogo.bin>

<https://urlhaus.abuse.ch/url/6019/> ▼

Apr 17, 2018 - ID: 6019. URL: <http://ccmlongueuil.ca/seclogo.bin>. URL Status: Online. Host: **ccmlongueuil.ca**. Threat: Malware download. Google Safe Browsing: Clean. Spamhaus DBL: Abused domain (malware). SURBL: Blacklisted. Reporter: @droethlisberger. Tags: exe Trickbot ...

Fake HSBC Your HSBC application documents delivers Trickbot via ...

<https://myonlinesecurity.co.uk/fake-hsbc-your-hsbc-application-documents-delivers-tr...> ▼

Apr 17, 2018 - This malware doc file downloads from <http://ccmlongueuil.ca/seclogo.bin> which is renamed .exe file (VirusTotal) Ctag: car0417. The alternate Download location is

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
```

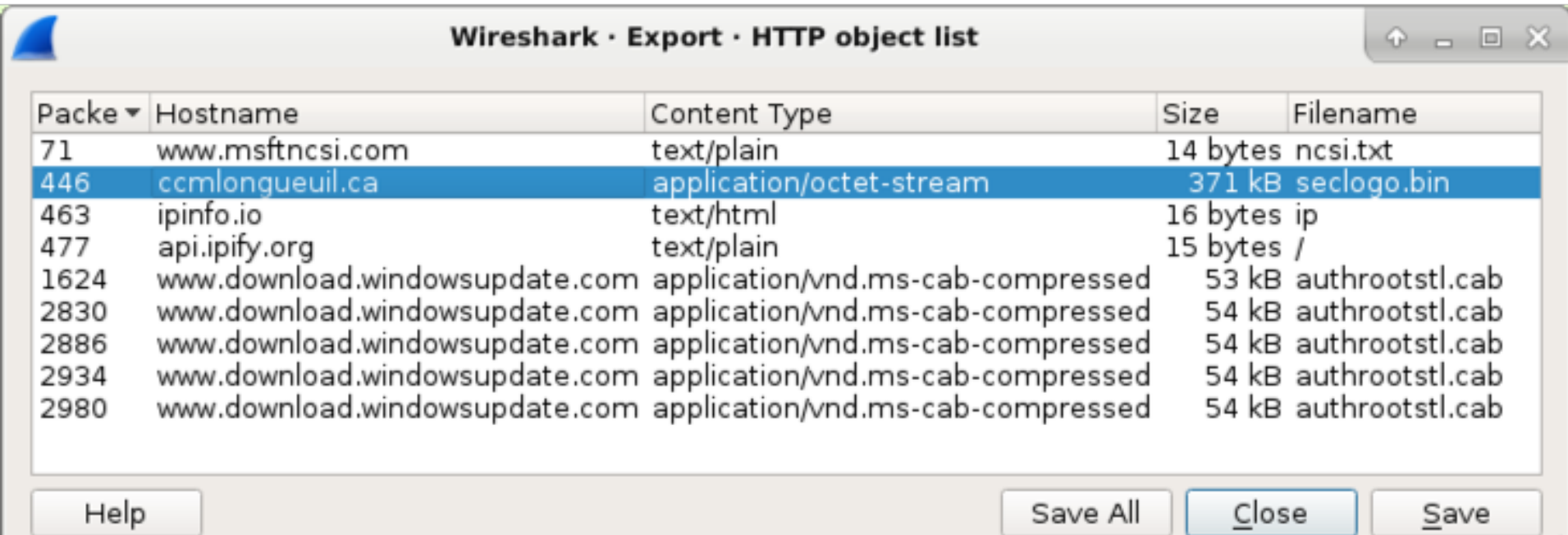
```
MZ.....@.....!..L..!
```

```
This program cannot be run in DOS mode.
```

```
$
```

Root causes from malspam campaigns

File → Export Objects → HTTP...

A screenshot of the Wireshark 'Export · HTTP object list' window. The window has a title bar with the Wireshark logo and standard window controls. It contains a table with five columns: 'Packe' (with a dropdown arrow), 'Hostname', 'Content Type', 'Size', and 'Filename'. The table lists several HTTP objects, with the one from 'ccmlongueuil.ca' highlighted in blue. At the bottom of the window are three buttons: 'Help', 'Save All', and 'Close', followed by a 'Save' button that is partially visible.

Packe ▾	Hostname	Content Type	Size	Filename
71	www.msftncsi.com	text/plain	14 bytes	ncsi.txt
446	ccmlongueuil.ca	application/octet-stream	371 kB	seclogo.bin
463	ipinfo.io	text/html	16 bytes	ip
477	api.ipify.org	text/plain	15 bytes	/
1624	www.download.windowsupdate.com	application/vnd.ms-cab-compressed	53 kB	authrootstl.cab
2830	www.download.windowsupdate.com	application/vnd.ms-cab-compressed	54 kB	authrootstl.cab
2886	www.download.windowsupdate.com	application/vnd.ms-cab-compressed	54 kB	authrootstl.cab
2934	www.download.windowsupdate.com	application/vnd.ms-cab-compressed	54 kB	authrootstl.cab
2980	www.download.windowsupdate.com	application/vnd.ms-cab-compressed	54 kB	authrootstl.cab

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:

**3ff628ab4a53cb24b53120890bdd
6847e962bc6a42f5d4d6aed1e23b
38850a3e site:www.hybrid-
analysis.com**

Root causes from malspam campaigns



3ff628ab4a53cb24b53120890bdd6847e962bc6a42f5d4d6



All

Maps

Videos

Images

Shopping

More

Settings

Tools

1 result (0.29 seconds)

Free Automated Malware Analysis Service - powered by Falcon ...

<https://www.hybrid-analysis.com/.../94ca0b76f0cf5d04e1cdf24667cd261dc2c3c4853f...>

Apr 18, 2018 - ... PE32 executable (GUI) Intel 80386, for MS Windows; Context: <http://ccmlongueuil.ca/seclogo.bin>; MD5; 0dc94f956e517ea69f4a3cd623bebb59; SHA1;

0c8791cc4ef4e78cbbce018a0774eeb8e5bb3e76; SHA256;

3ff628ab4a53cb24b53120890bdd6847e962bc6a42f5d4d6aed1e23b38850a3e ...

Root causes from malspam campaigns

← → ↻ 🏠 **Secure** | <https://www.hybrid-analysis.com/sample/94ca0b76f0cf5d04e1cdf24667cd>

 **HYBRID**
ANALYSIS

[🏠 Home](#) [☰ Submissions ▼](#) [📁 Resources ▼](#) [✉ Contact](#)

04172018HSBCJSZZH_app.doc 🔗

Analyzed on April 18th 2018 00:04:29 (CEST) running the *Kernelmode* monitor and action script *Heavy Anti-Evasion*
Guest System: Windows 7 32 bit, Home Premium, 6.1 (build 7601), Service Pack 1
Report generated by Falcon Sandbox v8.00 © Hybrid Analysis

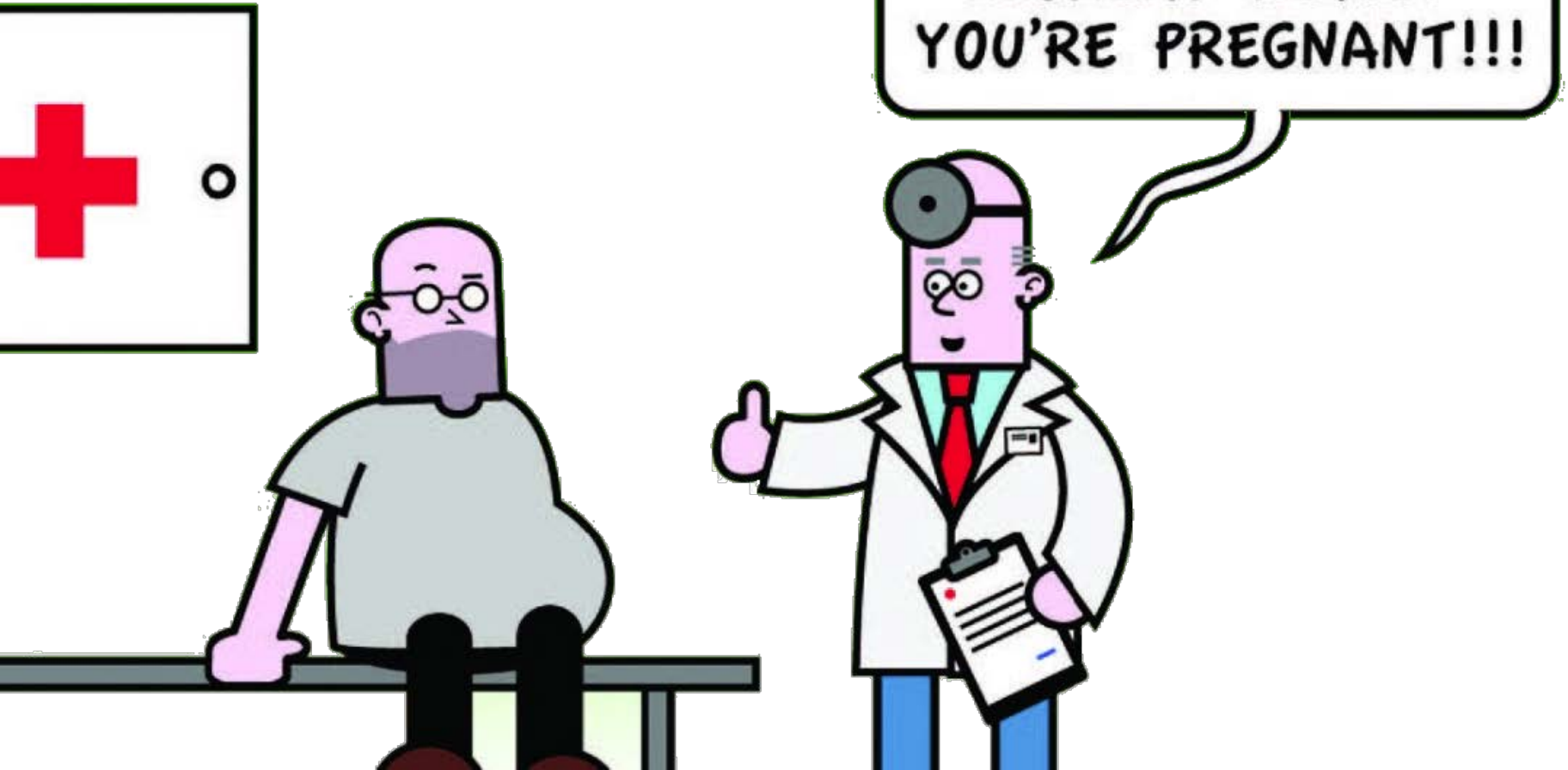
[🔗 Overview](#) [📎 Sample \(13KiB\)](#) [📄 Downloads ▼](#) [📄 External Reports ▼](#) [🔄 Re-analyze](#) [📄 Hash Not Seen Before](#) [📄 No sin](#)

Incident Response

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:"/?PHPSESSID=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)**

Apply this filter

Time	Dst	port	Host	Info
2018-04-24 02:25...	72.246.196.57	80	www.msftncsi.com	GET /ncsi.txt HTTP/1
2018-04-24 02:29...	198.54.117.244	80	www.maennerpillen-li...	GET /wa/?EN60=_bG4pf
2018-04-24 02:29...	54.183.248.227	80	www.biikooroo.com	GET /wa/?fBZ8=SGyksV
2018-04-24 02:29...	54.183.248.227	80	www.biikooroo.com	POST /wa/ HTTP/1.1
2018-04-24 02:31...	40.84.192.221	80	www.stopforeclosureo...	GET /wa/?EN60=_bG4pf
2018-04-24 02:31...	40.84.192.221	80	www.stopforeclosureo...	POST /wa/ HTTP/1.1
2018-04-24 02:31...	40.84.192.221	80	www.stopforeclosureo...	POST /wa/ HTTP/1.1
2018-04-24 02:31...	149.210.195.85	80	www.abba-eve.com	GET /wa/?fBZ8=67qelq
2018-04-24 02:32...	149.210.195.85	80	www.abba-eve.com	POST /wa/ HTTP/1.1
2018-04-24 02:32...	149.210.195.85	80	www.abba-eve.com	POST /wa/ HTTP/1.1
2018-04-24 02:32...	156.67.209.20	80	www.rantangan.online	GET /wa/?fBZ8=ITgLSB
2018-04-24 02:32...	156.67.209.20	80	www.rantangan.online	POST /wa/ HTTP/1.1
2018-04-24 02:32...	156.67.209.20	80	www.rantangan.online	POST /wa/ HTTP/1.1
2018-04-24 02:33...	52.86.22.136	80	www.earlyrecord.com	GET /wa/?EN60=_bG4pf
2018-04-24 02:33...	52.86.22.136	80	www.earlyrecord.com	POST /wa/ HTTP/1.1
2018-04-24 02:33...	52.86.22.136	80	www.earlyrecord.com	POST /wa/ HTTP/1.1

Block 7 - Exercise 1

WHEN WHO WHAT

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

Block 7 - Exercise 1

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

Time	Src	port	Dst	port	Info
2018-04-24 02:25...	172.16.1.115	49183	172.16.1.8	88	AS-REQ
2018-04-24 02:25...	172.16.1.115	49184	172.16.1.8	88	AS-REQ
2018-04-24 02:25...	172.16.1.8	88	172.16.1.115	49184	AS-REP
2018-04-24 02:25...	172.16.1.8	88	172.16.1.115	49185	TGS-REP
2018-04-24 02:25...	172.16.1.8	88	172.16.1.115	49186	TGS-REP

▶ Frame 405: 289 bytes on wire (2312 bits), 289 bytes captured (2312 bits)

▶ Ethernet II, Src: HewlettP_ea:40:a1 (00:50:8b:ea:40:a1), Dst: Dell_c2:09:6a

▶ Internet Protocol Version 4, Src: 172.16.1.115, Dst: 172.16.1.8

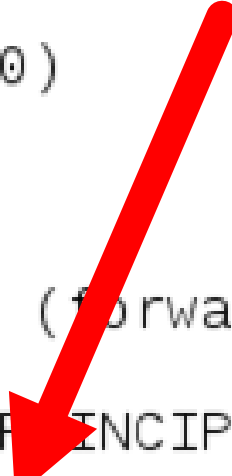
▶ Transmission Control Protocol, Src Port: 49183, Dst Port: 88, Seq: 1, Ack: 1

▼ Kerberos

- ▶ Record Mark: 231 bytes
- ▼ as-req
 - pvno: 5
 - msg-type: krb-as-req (10)

Block 7 - Exercise 1

CNameString: warren.harris



```
msg-type: krb-as-req (10)
▶ padata: 1 item
▼ req-body
  Padding: 0
  ▶ kdc-options: 40810010 (forwardable, renewable, canon
  ▼ cname
    name-type: KRB5-NT-PRINCIPAL (1)
    ▼ cname-string: 1 item
      CNameString: warren.harris
    realm: THUNDERLIFE
  ▶ sname
    till: 2037-09-13 02:48:05 (UTC)
```

Block 7 - Exercise 1

**Select the CNameString field and
"Apply as Column"**

CNameString: warren.harris

realm: THUNDERLIFE

▼ sname

name-type: kRB5-NT-SRV-INST

▶ sname-string: 2 items

till: 2037-09-13 02:48:05 (UTC)

rtime: 2037-09-13 02:48:05 (UTC)

nonce: 78667756

▼ etype: 6 items

ENCTYPE: eTYPE-AES256-CTS-HMA

ENCTYPE: eTYPE-AES128-CTS-HMA

Expand Subtrees

Expand All

Collapse All

Apply as Column

Apply as Filter

Prepare a Filter

Conversation Filter

Colorize with Filter

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
24	02:26...	172.16.1.8	88	172.16.1.115	49195	HARRIS-PC\$	TGS-REP

Block 7 - Exercise 1

nbns

nbns							Expression...	+ Apply this filter
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 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**

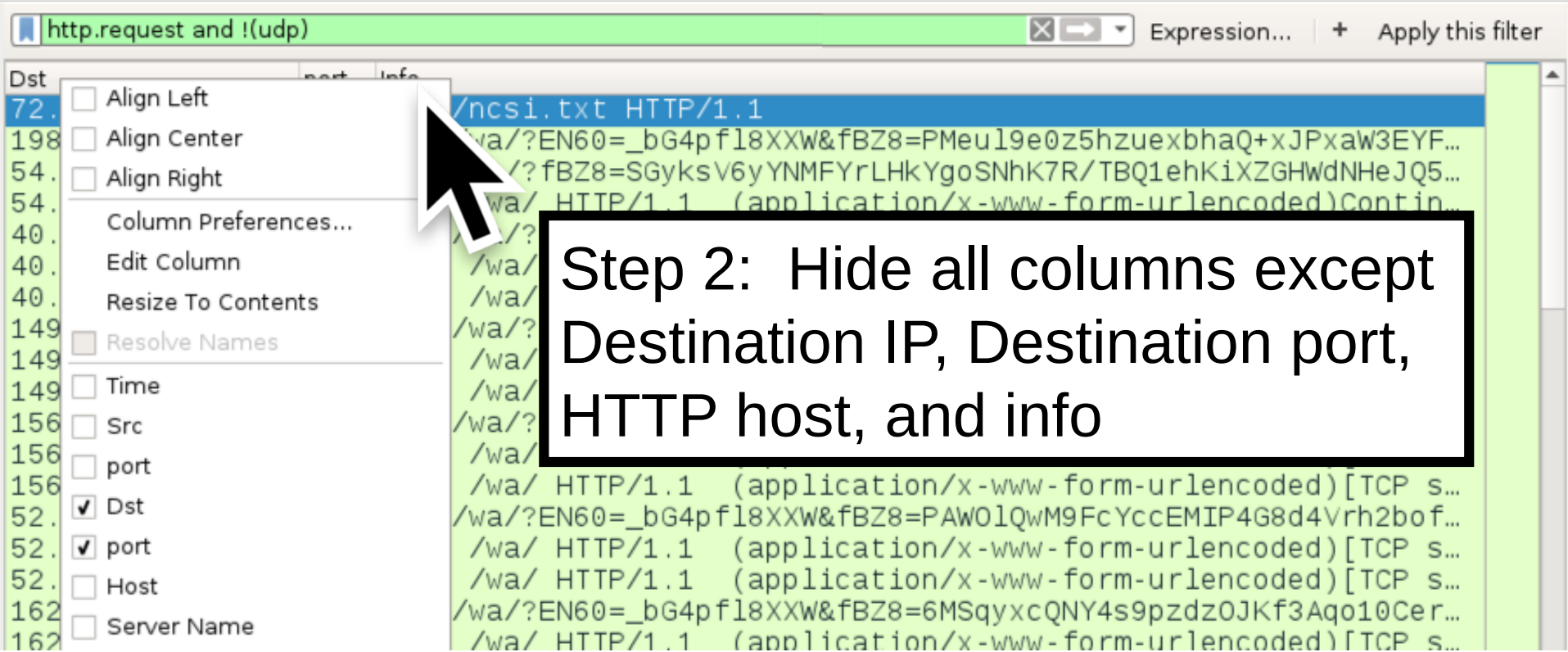
Block 7 - Exercise 1 - IOCs

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)*



The screenshot shows a network traffic analysis interface. At the top, a green filter bar contains the text "http.request and !(udp)". Below this, a list of network packets is visible, with the first packet selected and highlighted in blue. A context menu is open over the first packet, showing options for alignment (Left, Center, Right), column preferences, editing the column, resizing to contents, resolving names, and selecting columns. The "Dst" and "port" columns are currently selected, indicated by checkmarks. A large black arrow points to the "Dst" option in the menu. A text box with a black border is overlaid on the right side of the interface, containing the text "Step 2: Hide all columns except Destination IP, Destination port, HTTP host, and info".

http.request and !(udp)

Align Left

Align Center

Align Right

Column Preferences...

Edit Column

Resize To Contents

Resolve Names

Time

Src

port

☒ Dst

☒ port

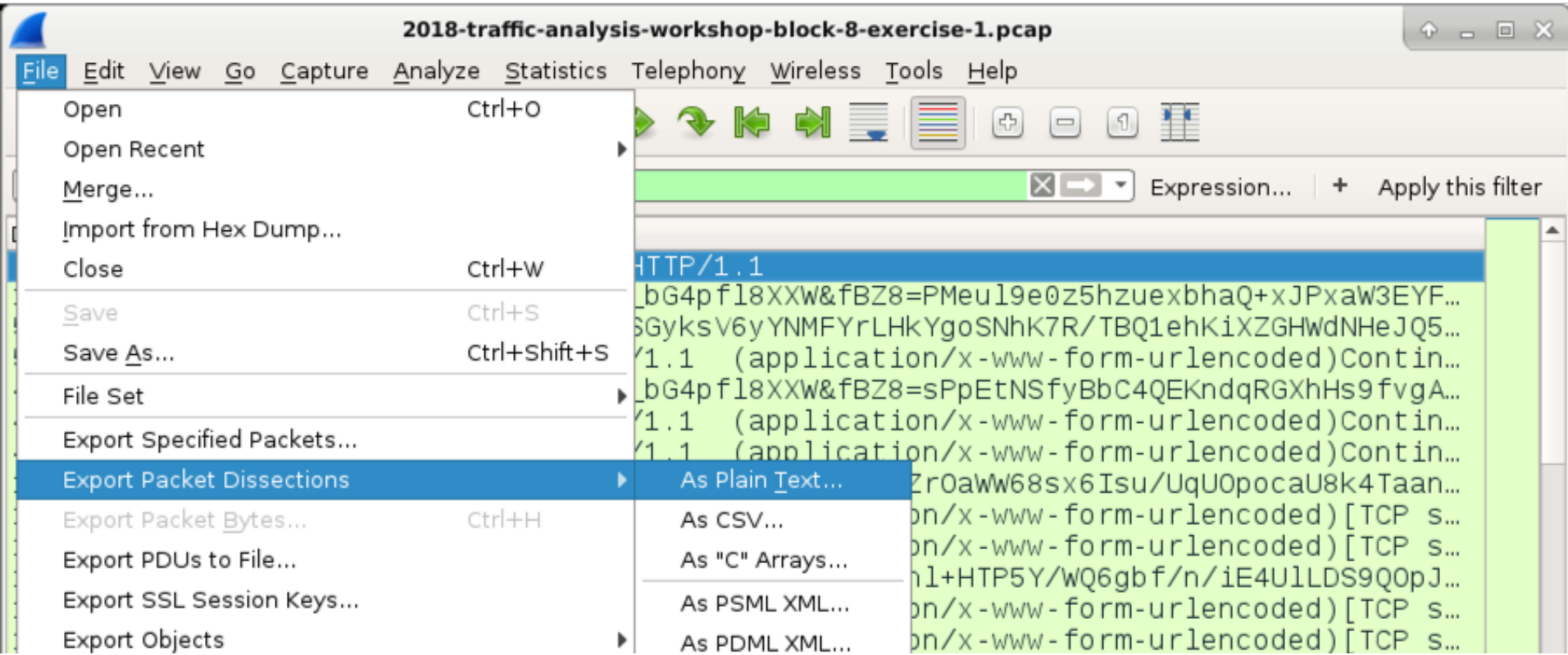
Host

Server Name

Step 2: Hide all columns except Destination IP, Destination port, HTTP host, and info

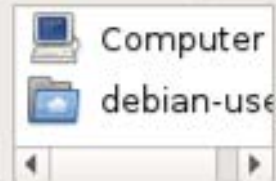
Block 7 - Exercise 1 - IOCs

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



Wireshark · Export Packet Dissections

Look in: /home/debian-user/Downloads



Name	Size	Type	Date Modified

File name:

Save

Export As:

Plain text (*.txt)

Cancel

Make sure "Details" is un-checked

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: <input type="text"/> | 0 | 0 |
| ☐ Remove ignored packets | 0 | 0 |

Packet Format

☒ Summary line

☐ Details:

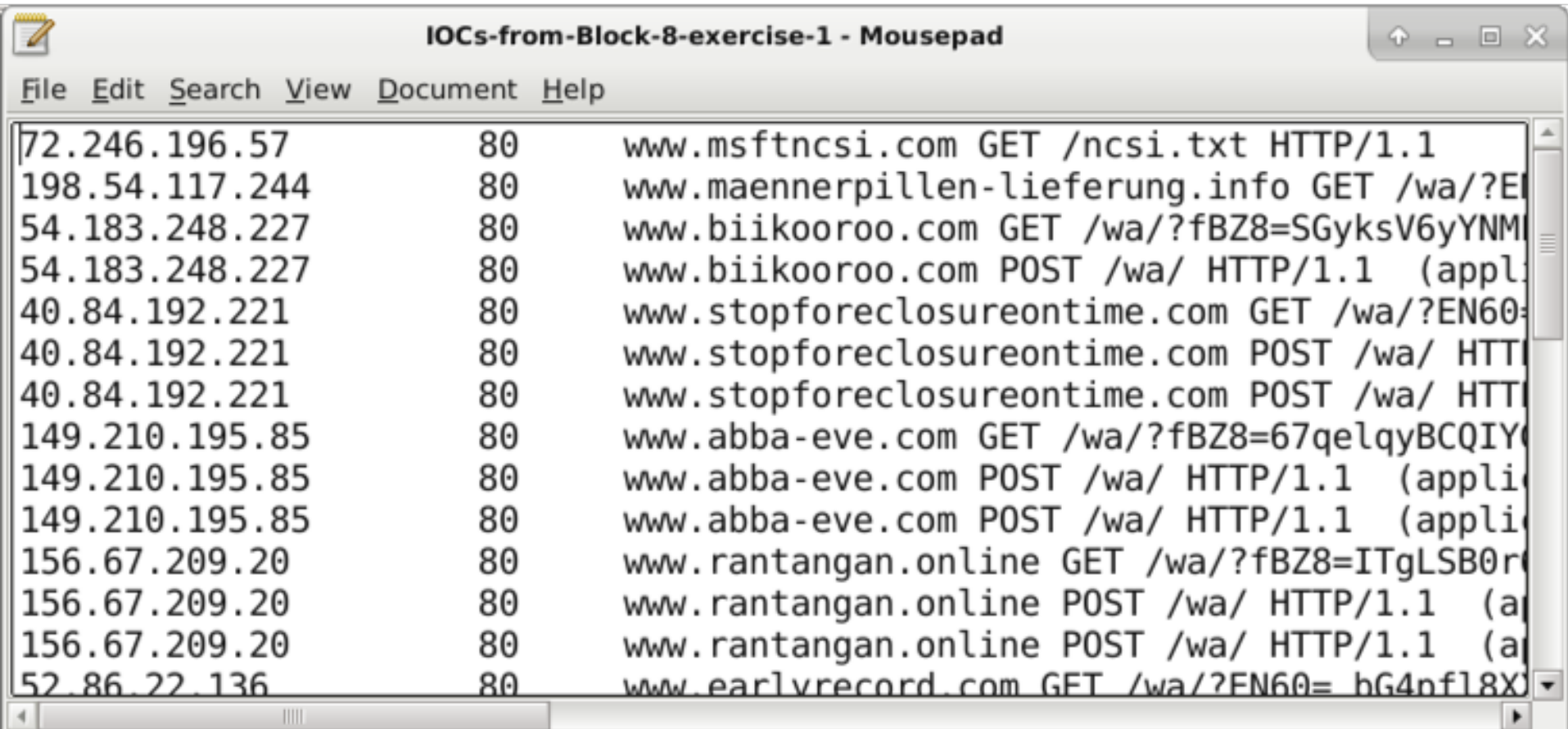
☐ All collapsed

☒ As displayed

☐ All expanded

☐ Bytes

Block 7 - Exercise 1 - IOCs



IOCs-from-Block-8-exercise-1 - Mousepad

File	Edit	Search	View	Document	Help
72.246.196.57	80	www.msftncsi.com	GET /ncsi.txt	HTTP/1.1	
198.54.117.244	80	www.maennerpillen-lieferung.info	GET /wa/?E		
54.183.248.227	80	www.biikooroo.com	GET /wa/?fBZ8=SGyksV6yYNM		
54.183.248.227	80	www.biikooroo.com	POST /wa/	HTTP/1.1 (appl	
40.84.192.221	80	www.stopforeclosureontime.com	GET /wa/?EN60=		
40.84.192.221	80	www.stopforeclosureontime.com	POST /wa/	HTTP	
40.84.192.221	80	www.stopforeclosureontime.com	POST /wa/	HTTP	
149.210.195.85	80	www.abba-eve.com	GET /wa/?fBZ8=67qelqyBCQIY		
149.210.195.85	80	www.abba-eve.com	POST /wa/	HTTP/1.1 (applic	
149.210.195.85	80	www.abba-eve.com	POST /wa/	HTTP/1.1 (applic	
156.67.209.20	80	www.rantangan.online	GET /wa/?fBZ8=ITgLSB0r		
156.67.209.20	80	www.rantangan.online	POST /wa/	HTTP/1.1 (a	
156.67.209.20	80	www.rantangan.online	POST /wa/	HTTP/1.1 (a	
52.86.22.136	80	www.earlyrecord.com	GET /wa/?EN60= bG4nf18X		

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 Archiv
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
172.16.1.97	46	8080	6	6	ET POLICY HTTP Request on Unusual Port Possibly Host
172.16.1.97	46	8080	6	6	ETPRO TROJAN W32/Emotet.v4 Checkin
172.16.1.97	46	8080	6	6	ETPRO TROJAN W32/Emotet.v4 Checkin 2
172.16.1.97	46	8080	6	6	ETPRO TROJAN W32/Emotet.v4 Checkin 3

**Alerts for
Emotet**



ETPRO TROJAN W32/Emotet.v4 Checkin
ETPRO TROJAN W32/Emotet.v4 Checkin 2
ETPRO TROJAN W32/Emotet.v4 Checkin 3

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**

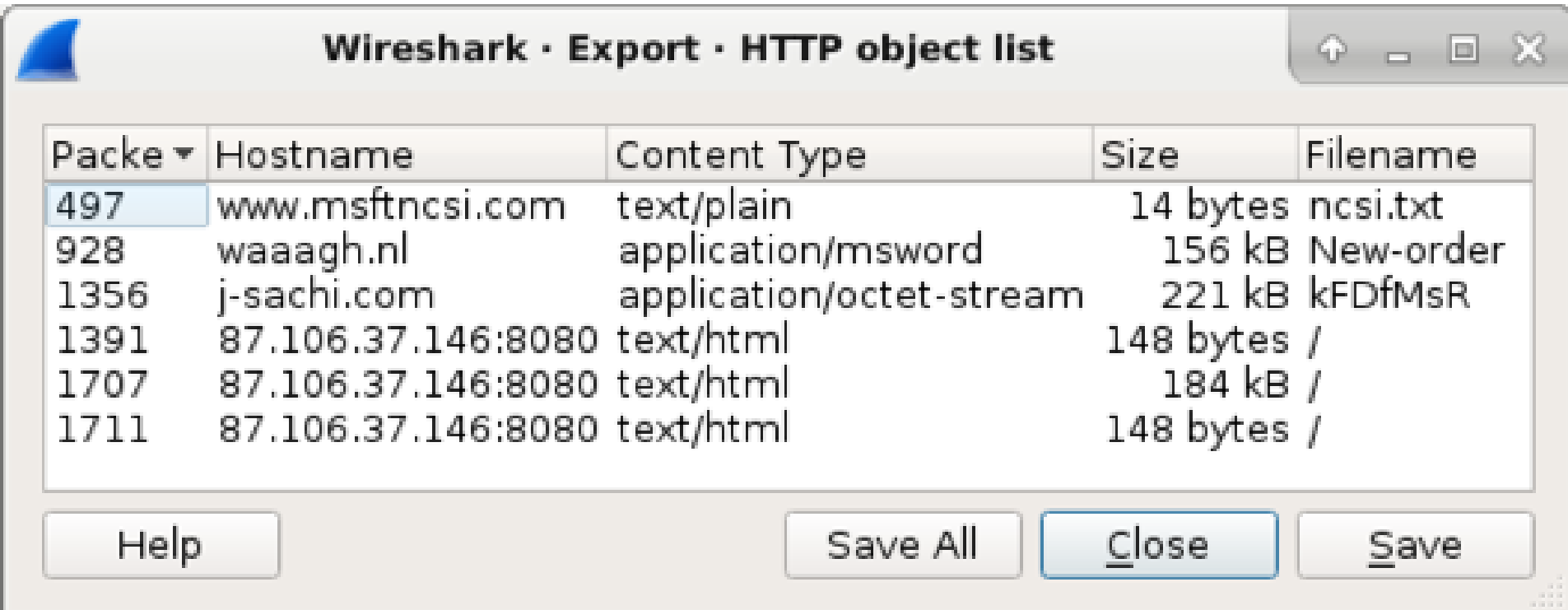
MAC address: **00:1f:cf:2e:a7:6c**

Host name: **YATES-PC**

User account name: **kayla.yates**

Block 7 - Exercise 2 - IOCs

File → Export Objects → HTTP...



The image shows a screenshot of the 'Wireshark · Export · HTTP object list' dialog box. The dialog has a title bar with standard window controls (minimize, maximize, close) and a blue Wireshark logo on the left. Below the title bar is a table with five columns: 'Pac~~k~~ets', 'Hostname', 'Content Type', 'Size', and 'Filename'. The table contains six rows of data. The first row is highlighted with a blue background. Below the table are four buttons: 'Help', 'Save All', 'Close', and 'Save'.

Pac k ets	Hostname	Content Type	Size	Filename
497	www.msftncsi.com	text/plain	14 bytes	ncsi.txt
928	waaagh.nl	application/msword	156 kB	New-order
1356	j-sachi.com	application/octet-stream	221 kB	kFDfMsR
1391	87.106.37.146:8080	text/html	148 bytes	/
1707	87.106.37.146:8080	text/html	184 kB	/
1711	87.106.37.146:8080	text/html	148 bytes	/

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
46.30.42.225	80	172.16.1.201	49200	6	ET CURRENT_EVENTS SunDown EK RIP Landing M1 B641
46.30.42.225	80	172.16.1.201	49200	6	ETPRO CURRENT_EVENTS SunDown EK Landing Feb 13 20...
46.30.42.225	80	172.16.1.201	49200	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**

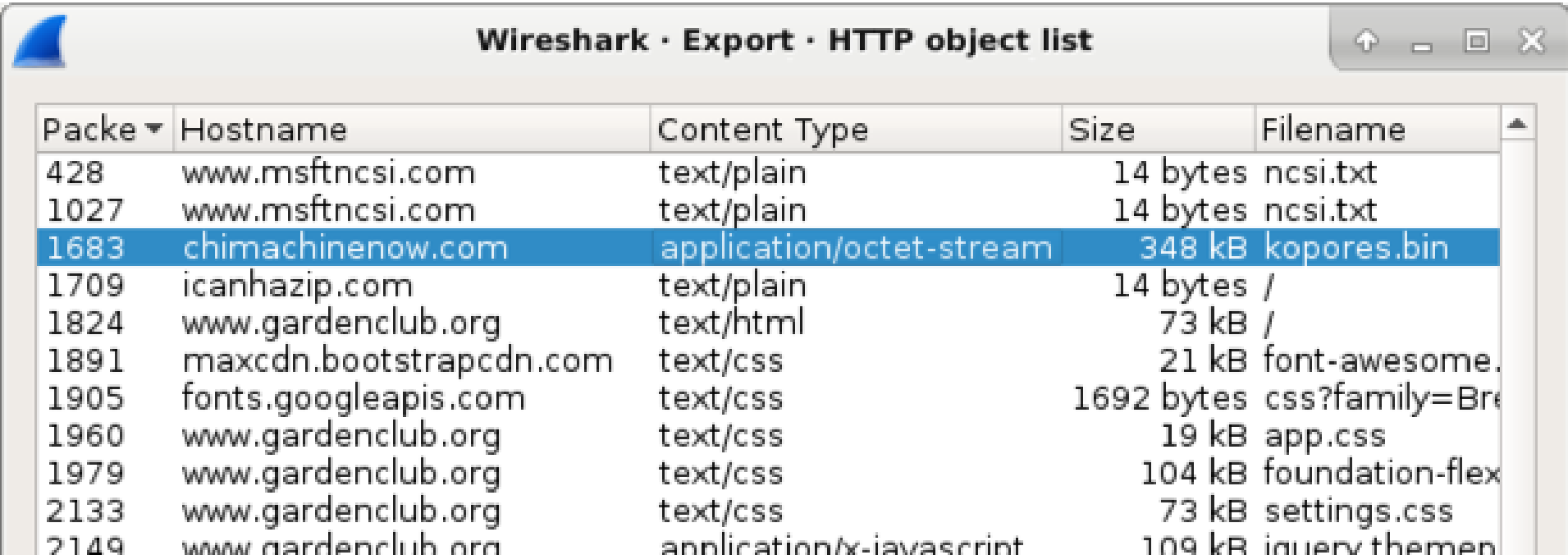
MAC address: **00:13:d4:b9:cd:56**

Host name: **HENDERSON-PC**

User account name: **edwin.henderson**

Block 7 - Exercise 4 - IOCs

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



The image shows a screenshot of the 'Wireshark · Export · HTTP object list' window. The window has a title bar with standard OS controls (up, down, maximize, close). Below the title bar is a table with five columns: 'Packe' (with a dropdown arrow), 'Hostname', 'Content Type', 'Size', and 'Filename'. The table contains several rows of data. The row with index 1683 is highlighted in blue. This row corresponds to the IOC data provided in the text above: 'chimachinenow.com', 'application/octet-stream', '348 kB', and 'kopores.bin'. Other rows include data from 'www.msftncsi.com', 'icanhazip.com', 'www.gardenclub.org', and 'maxcdn.bootstrapcdn.com'.

Packe ▾	Hostname	Content Type	Size	Filename
428	www.msftncsi.com	text/plain	14 bytes	ncsi.txt
1027	www.msftncsi.com	text/plain	14 bytes	ncsi.txt
1683	chimachinenow.com	application/octet-stream	348 kB	kopores.bin
1709	icanhazip.com	text/plain	14 bytes	/
1824	www.gardenclub.org	text/html	73 kB	/
1891	maxcdn.bootstrapcdn.com	text/css	21 kB	font-awesome.
1905	fonts.googleapis.com	text/css	1692 bytes	css?family=Bre
1960	www.gardenclub.org	text/css	19 kB	app.css
1979	www.gardenclub.org	text/css	104 kB	foundation-flex
2133	www.gardenclub.org	text/css	73 kB	settings.css
2149	www.gardenclub.org	application/x-javascript	109 kB	jquery.themen

Block 7 - Exercise 4 - IOCs

92.53.77.217 image/png 350kB table.png

92.53.77.217 image/png 350kB toler.png

14041	www.gardenclub.org	image/jpeg	223 kB	ngc-home
14059	www.gardenclub.org	image/svg+xml	137 kB	ngc-logo-b
14378	www.gardenclub.org	image/jpeg	1080 kB	ngc-mobil
14385	www.gardenclub.org	image/png	2917 bytes	favicon-32
16357	www.download.windowsupdate.com	application/vnd.ms-cab-compressed	54 kB	authrootst
19392	92.53.77.217	image/png	350 kB	table.png
20807	92.53.77.217	image/png	350 kB	toler.png
20828	api.ipify.org	text/plain	13 bytes	/
21170	www.download.windowsupdate.com	application/vnd.ms-cab-compressed	54 kB	authrootst

Help Save All Close Sa

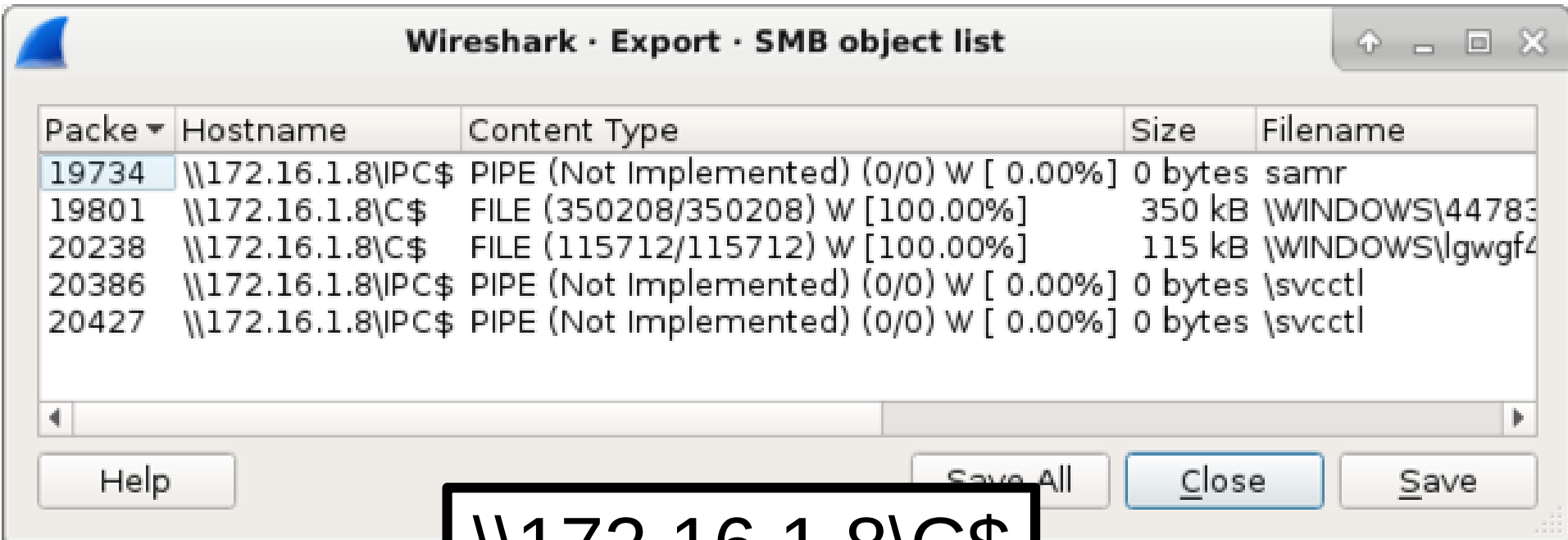
Block 7 - Exercise 4 - Additional info!

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...



The image shows a screenshot of the 'Wireshark · Export · SMB object list' dialog box. It contains a table with 5 columns: 'Pac...', 'Hostname', 'Content Type', 'Size', and 'Filename'. The table lists several SMB objects, with the first row highlighted. Below the table are buttons for 'Help', 'Save All', 'Close', and 'Save'. A black box with white text is overlaid on the bottom of the dialog, containing the text '\\172.16.1.8\C\$'.

Pac...	Hostname	Content Type	Size	Filename
19734	\\172.16.1.8\IPC\$	PIPE (Not Implemented) (0/0) W [0.00%]	0 bytes	samr
19801	\\172.16.1.8\C\$	FILE (350208/350208) W [100.00%]	350 kB	\WINDOWS\44783
20238	\\172.16.1.8\C\$	FILE (115712/115712) W [100.00%]	115 kB	\WINDOWS\lgwgf4
20386	\\172.16.1.8\IPC\$	PIPE (Not Implemented) (0/0) W [0.00%]	0 bytes	\svcctl
20427	\\172.16.1.8\IPC\$	PIPE (Not Implemented) (0/0) W [0.00%]	0 bytes	\svcctl

\\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

10.14.1.1

10.14.1.34

10.14.1.103

10.14.1.114

10.14.1.123

10.14.1.152

10.14.1.175

10.14.1.186

10.14.1.255

Statistics → Endpoints

Ethernet · 11

Address

8.8.4.4

8.41.222.241

8.43.72.21

8.43.72.32

8.43.72.54

8.43.72.62

8.43.72.112

8.43.72.113

8.253.112.94

8.253.112.245

10.14.1.1

10.14.1.34

10.14.1.103

10.14.1.114

10.14.1.123

10.14.1.152

10.14.1.175

10.14.1.186

10.14.1.255

traffic-analysis-workshop-block-9-final-exercise

UDP

15

15

10

101

9

194

15

30

133

54

458

753

632

1,021

1,083

1,559

1,534

1,534

0

41

1550

5750

3796

40 k

3486

59 k

6366

10 k

154 k

30 k

116 k

205 k

124 k

1294 k

346 k

463 k

286 k

206 k

0

22 k

15

17

14

96

10

176

13

37

113

69

470

933

471

6,274

1,789

3,149

6,477

2,886

214

49

1110

2292

1973

17 k

2609

35 k

4192

7365

14 k

11 k

42 k

256 k

197 k

3527 k

958 k

2653 k

8020 k

3120 k

21 k

15 k

United States

United States

United States

United States

United States

United States

United States

United States

United States

United States

United States

United States

United States

United States

United States

United States

United States

United States

United States

United States

—

—

—

—

—

—

—

—

—

—

—

—

—

—

—

—

—

—

—

—

Seattle

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

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

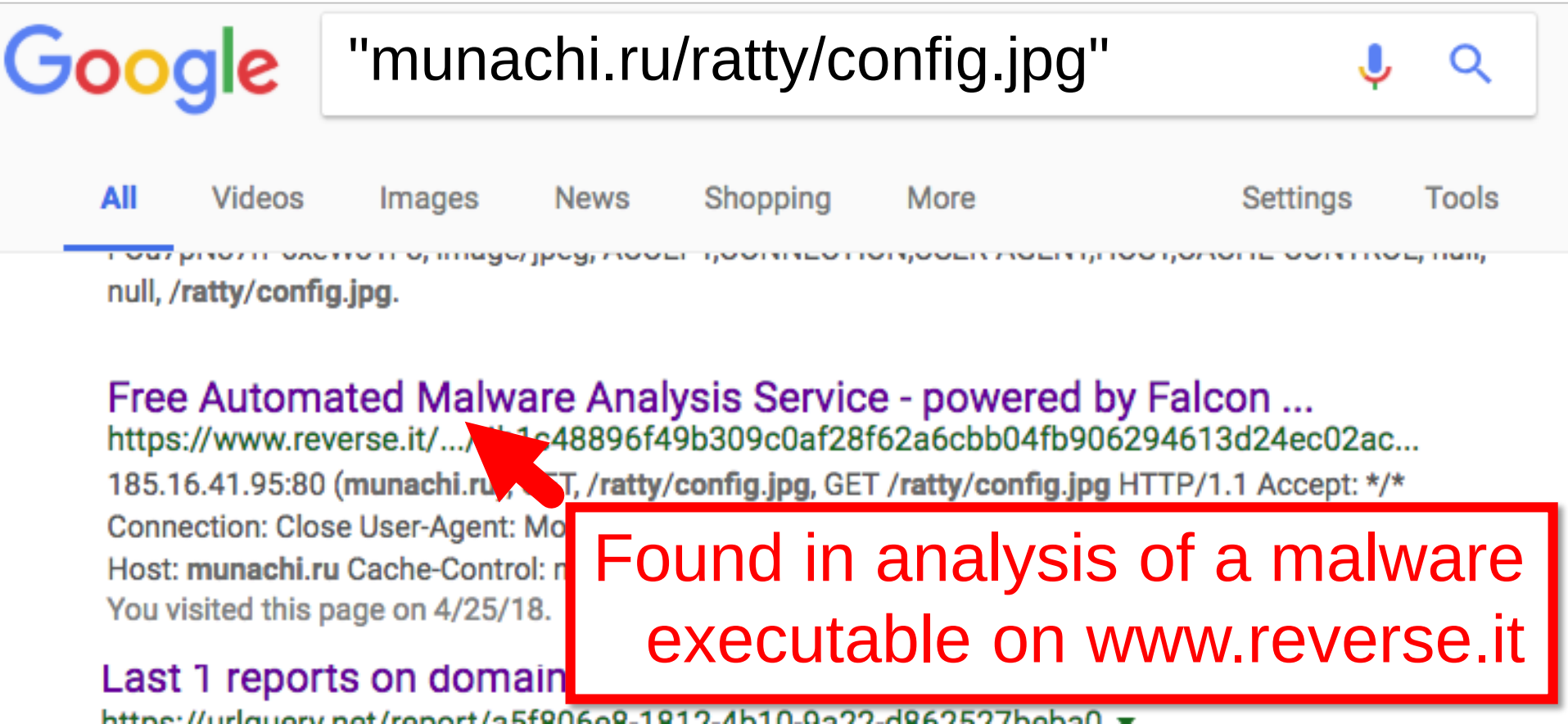
Review

Suspicious URLs

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

Look up the info on Google!

The malicious traffic



Google "munachi.ru/ratty/config.jpg"  

[All](#) [Videos](#) [Images](#) [News](#) [Shopping](#) [More](#) [Settings](#) [Tools](#)

.../ratty/config.jpg.

Free Automated Malware Analysis Service - powered by Falcon ...
<https://www.reverse.it/.../1e48896f49b309c0af28f62a6cbb04fb906294613d24ec02ac...>
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 6.0; rv:2.0) Gecko/20100101 Firefox/4.0
Host: munachi.ru Cache-Control: no-cache
You visited this page on 4/25/18.

Last 1 reports on domain
<https://urlquery.net/report/a5f806e8-1812-4b10-9a22-d862527baba0>

Found in analysis of a malware executable on www.reverse.it

The malicious traffic

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

HTTP Traffic

33W711KX/34703D

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

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

malicious AV Detection: 17%

Labeled as: Trojan.Generic

#banker #financial #kins #zeus #zeus1134

Link Twitter E-Mail

Incident Response Indicators

- Malicious (27)
- Suspicious (27)
- Informative (23)

File Details

- Screen shots (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.*

IP address: **10.14.1.152**

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

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

User account name: **stanley.debanham**

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:

- **4b1c48896f49b309c0af28f62a6cbb04fb90629461
3d24ec02ac151362b10a45**

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

