Getting Started With BHIS: SOC Analyst

John Strand

New Name!!!!

Getting Started With BHIS: MSP/SOC Analyst

John Strand

Big Thanks!!

LEVEL UP

The MSP Security Training Challenge

Presented by

The Cyber Call

Mission: Raise the collective security posture across the channel.

Our challenge for ourselves: Help 500 MSPs get training in 30 Days.

The channel needs more security practitioners.

That's why we've teamed up with vendors across the channel who are passionate about security to make some of the industry's best training more accessible and affordable.

Our Sponsors

Each one of our sponsors has contributed funds to help secure the course discount and tuition assistance for those needing financial help. In addition, they each will be providing free seats in the course to help us hit our goal of providing the training to as many MSPs as possible.

blackpoint

ninja RMM

datto

CISCO

ConnectWise

HUNTRESS

pax8

SKOUT CYBERSECURITY

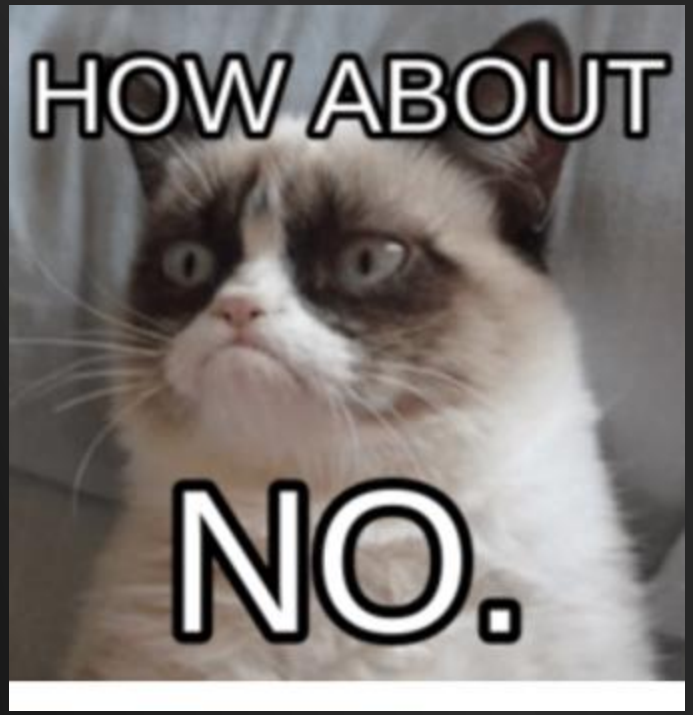
SOPHOS

THREATLOCKER

TruMethods A Kaseya COMPANY

What We Are Covering

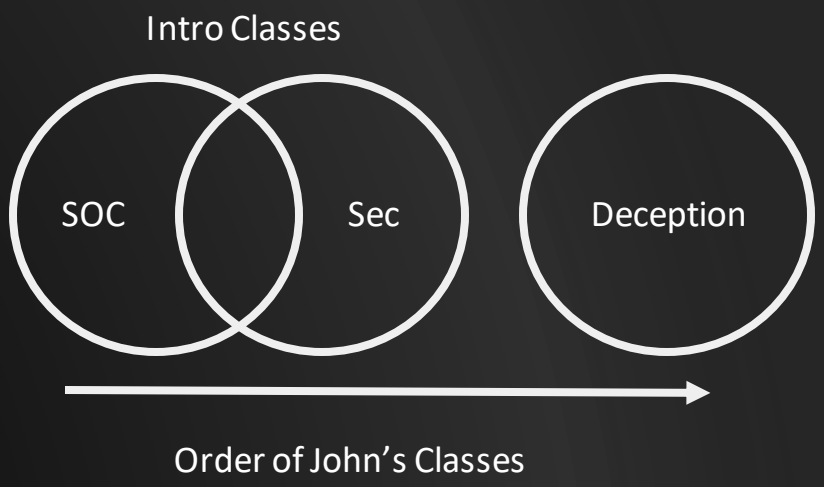
- Intro to Windows
- Intro to Linux
- Intro to TCP/IP
- Basics and fundamentals
- Core things to learn to work at the BHIS SOC
- This class is meant to feed into the Intro to Security class



Actually, yes. Today we are Grumpycat

A Note On Overlap

- For this iteration, there will be some overlap with the Intro to Security class
  - Turns out, there is overlap in the topics.. Who knew?
- In the future, this class will feed into the Intro to Security Class
- The Intro to Security Class will feed to Cyber Deception
- For the near future, any class taught by me will be pay what you can



5 Year Plan

24 SEP 2018

HOW-TO, INFORMATIONAL, INFOSEC 101, WEBCASTS · CAREER CHANGE, GETTING INTO INFOSEC, GETTING STARTED, HOW TO GET INTO INFOSEC, STARTING YOUR CAREER

Webcast: John Strand's 5 Year Plan into InfoSec, Part 2

John Strand talks about his own journey into information security and shares his suggestions for those wanting to get started from scratch or who are looking to change career tracks.

Special Guests: Randy Marchany, CISO of Virginia Tech & Director of the VA Tech IT Security Lab, and Ed Capizzi, SANS instructor.

Show Notes / Links: *Just a few of the specific things that were referenced in this show*

FOLLOW US

New to infosec?
START HERE

LOOKING FOR SOMETHING?

SUBSCRIBE TO THE BHISBLOG

Don't get left in the dark! Enter your email address and every time a post

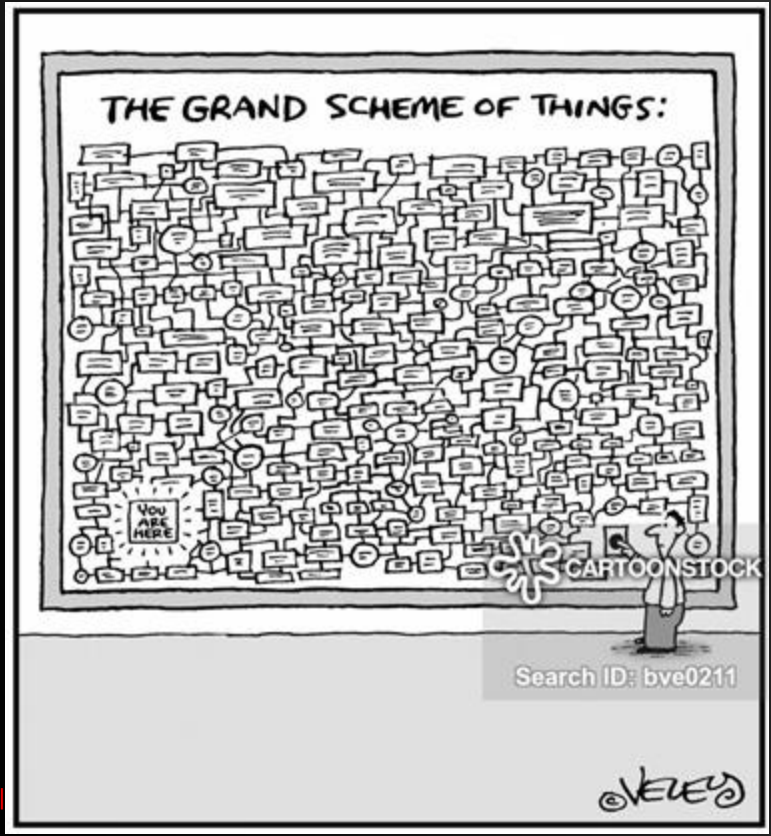
You Are Compromised? What Now?

A bad day in the SOC...

Why?

- First steps are tough..
- Mistakes and paralysis
- Need to keep moving
- Need to have a plan
- I want to cover some basic first steps

The Wrong Way…



The Right Way

IR “Legos”


BNB_CARDS_PRO-8.png
ENDPOINT ANALYSIS
This is where the defenders use their SANS IR
BNB_CARDS_PRO-4.png
NETFLOW, ZEEK/BRO, REAL INTELLIGENCE THREAT ANALYTICS (RITA) ANALYSIS
Does your organization capture and review
BNB_CARDS_PRO-10.png
CRISIS MANAGEMENT
Your Legal and Management Teams have procedures for effectively and ethically notifying impacted victims of compromises.
NOTES
BNB_CARDS_PRO-7.png
USER AND ENTITY BEHAVIOR ANALYTICS (UEBA)
BNB_CARDS_PRO-6.png
ENDPOINT SECURITY PROTECTION ANALYSIS
We know, you have AV. Great! Do you actually get alerts and logs? Do you immediately review them? Or, do you simply turn it on and walk away while the network explodes like you're in a bad action movie?
TOOLS
BNB_CARDS_PRO-9.png
ISOLATION
BNB_CARDS_PRO-5.png
BNB_CARDS_PRO-1.png
SERVER ANALYSIS
The ability to baseline a system and verify that it
INTERNAL SEGMENTATION
Turn on your host-based firewalls. Segment different organizational units. Treat the internal network as hostile, because it is.

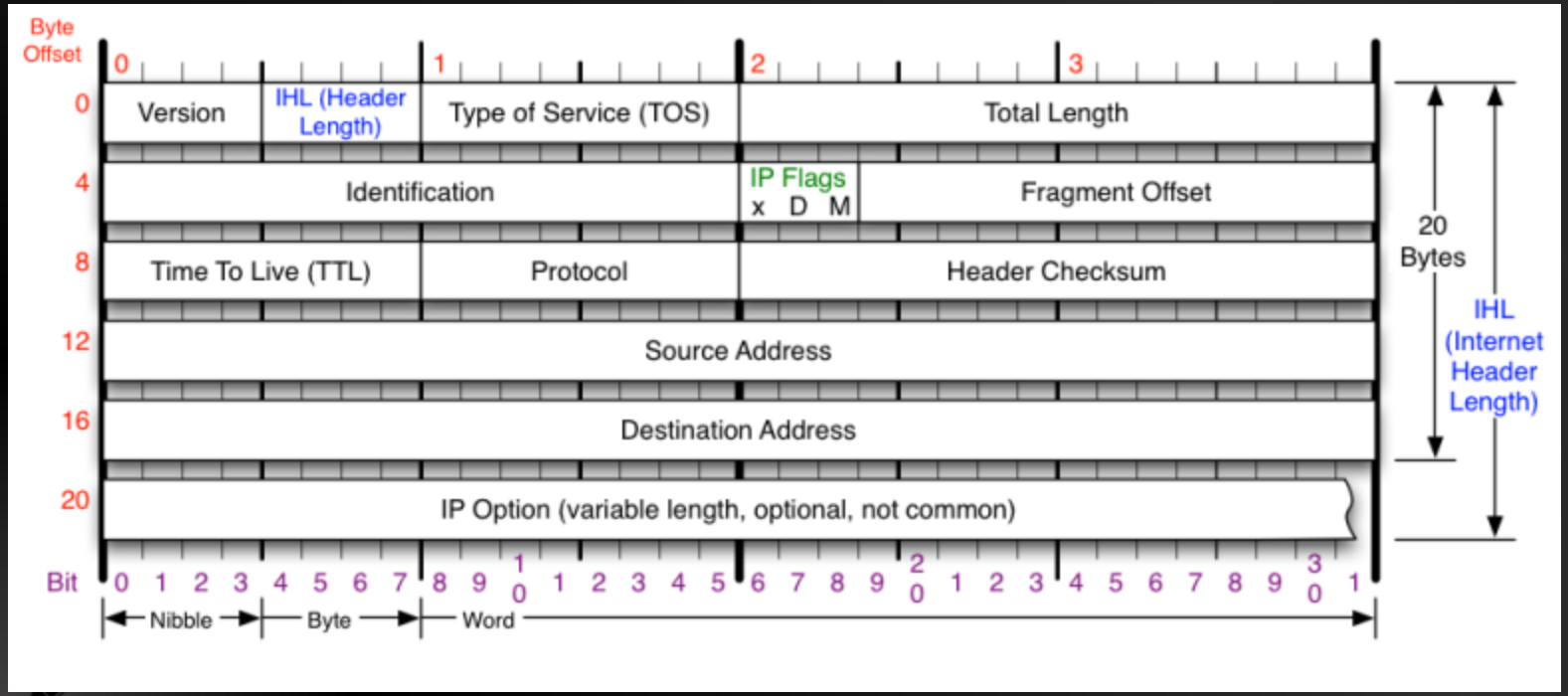
Don't Panic

- First step… Don’t freak out
- I said DON’T FREAK OUT…
- DON’T FREAK OUT!!!!!!!
- This only comes with practice
- Think weapons training
- Don't wait for an incident to try tools you have read about
- Memory forensics, Deep Blue CLI, IR Scripts, Logontracer, etc.

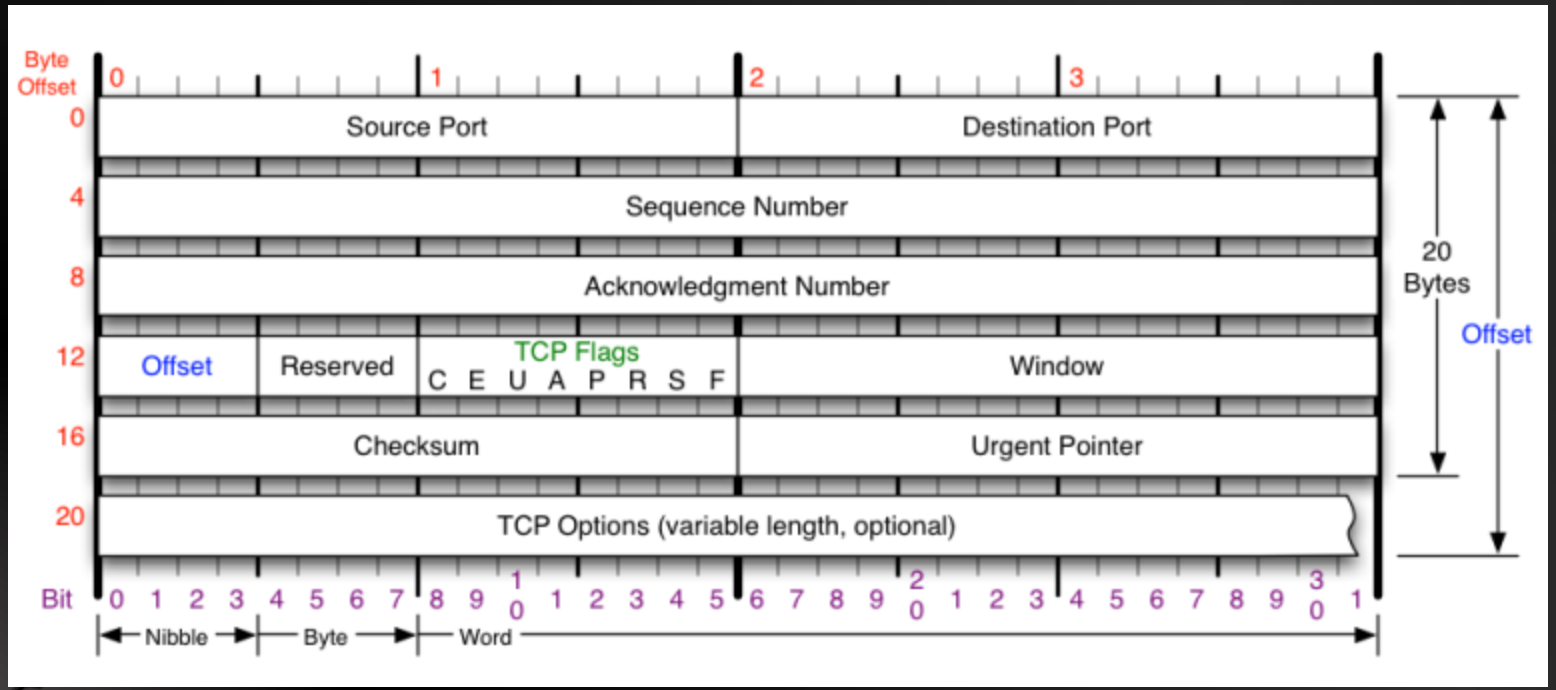
Networking!!!


LET'S START WITH TCP/IP
IT'S A VERY GOOD PLACE TO START
imgflip.com

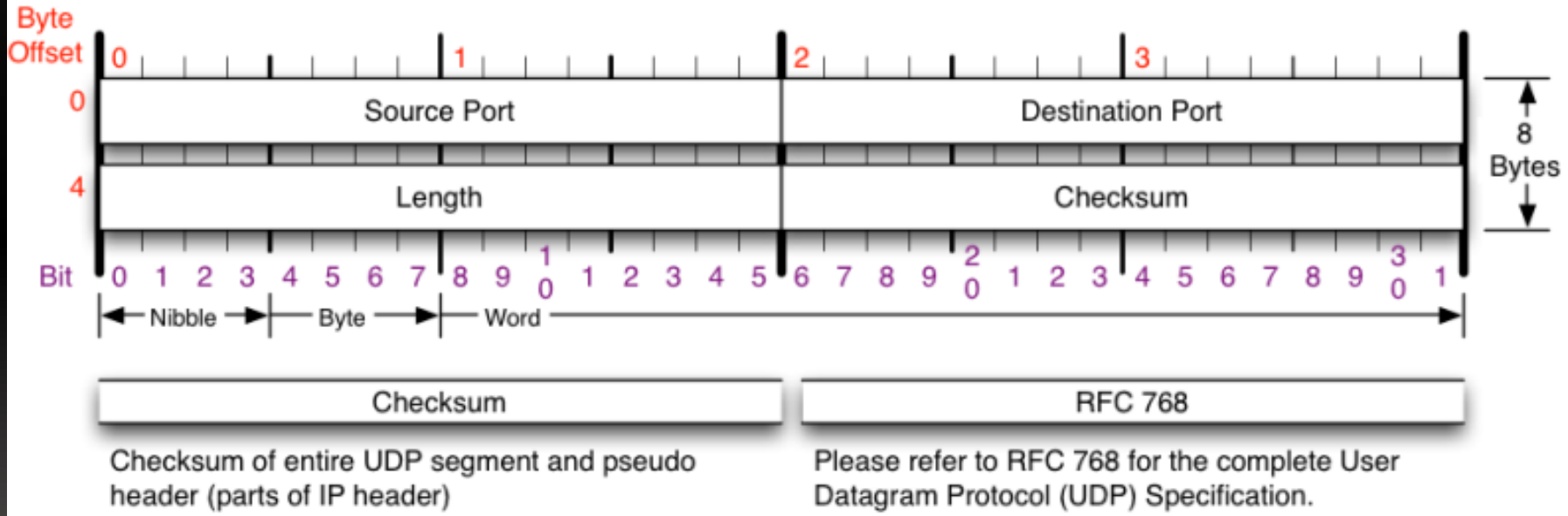
IP Header


Byte Offset
0
1
2
3
0
4
8
12
16
20
Version
IHL (Header Length)
Type of Service (TOS)
Total Length
Identification
IP Flags
x D M
Fragment Offset
Time To Live (TTL)
Protocol
Header Checksum
Source Address
Destination Address
IP Option (variable length, optional, not common)
20 Bytes
IHL (Internet Header Length)
Bit
0 1 2 3 4 5 6 7 8 9 10 1 2 3 4 5 6 7 8 9 20 1 2 3 4 5 6 7 8 9 30 1
Nibble
Byte
Word

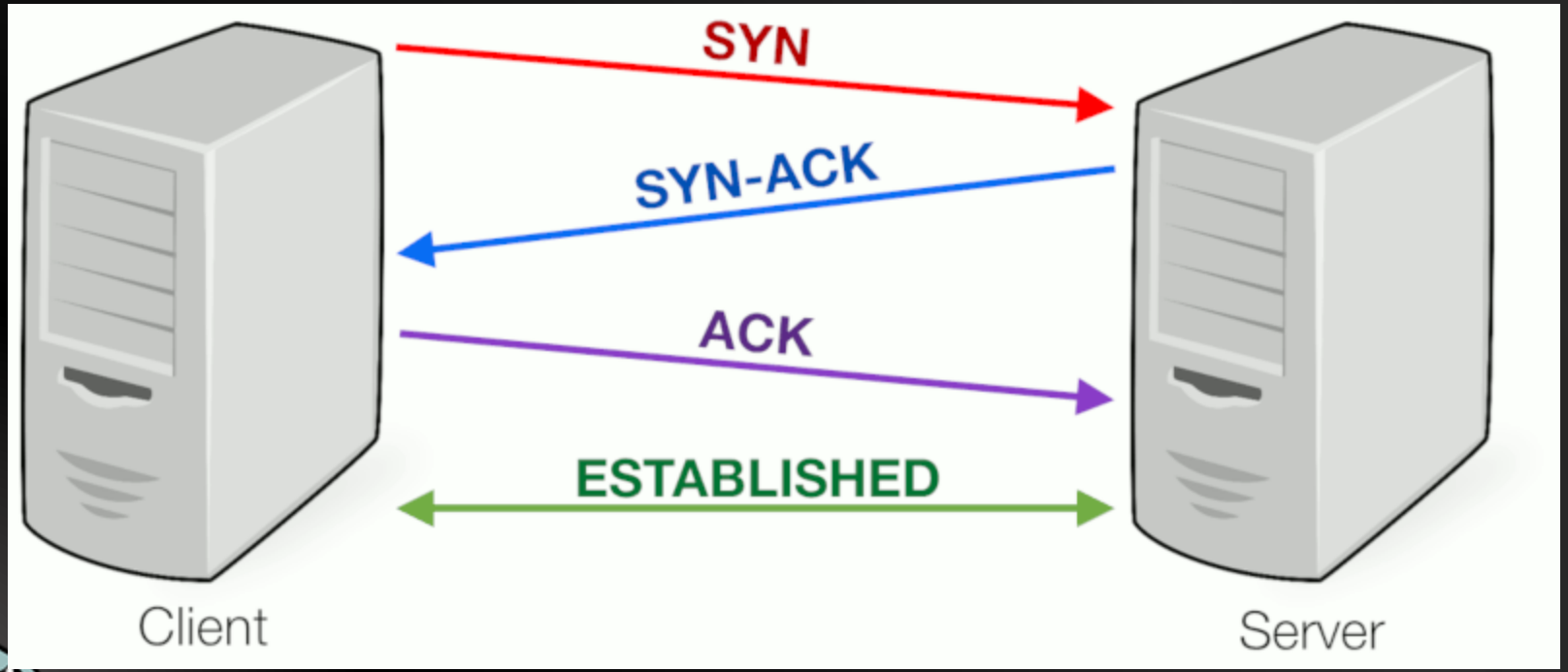
TCP Header


Byte Offset
0
1
2
3
0
Source Port
Destination Port
4
Sequence Number
8
Acknowledgment Number
12
Offset
Reserved
TCP Flags
C E U A P R S F
Window
16
Checksum
Urgent Pointer
20
TCP Options (variable length, optional)
20 Bytes
Offset
Bit
0 1 2 3 4 5 6 7 8 9 10 1 2 3 4 5 6 7 8 9 20 1 2 3 4 5 6 7 8 9 30 1
Nibble
Byte
Word

UDP Header


Byte Offset
0
1
2
3
0
Source Port
Destination Port
4
Length
Checksum
8 Bytes
Bit
0 1 2 3 4 5 6 7 8 9 10 1 2 3 4 5 6 7 8 9 20 1 2 3 4 5 6 7 8 9 30 1
Nibble
Byte
Word
Checksum
RFC 768
Checksum of entire UDP segment and pseudo header (parts of IP header)
Please refer to RFC 768 for the complete User Datagram Protocol (UDP) Specification.

TCP Three way Handshake



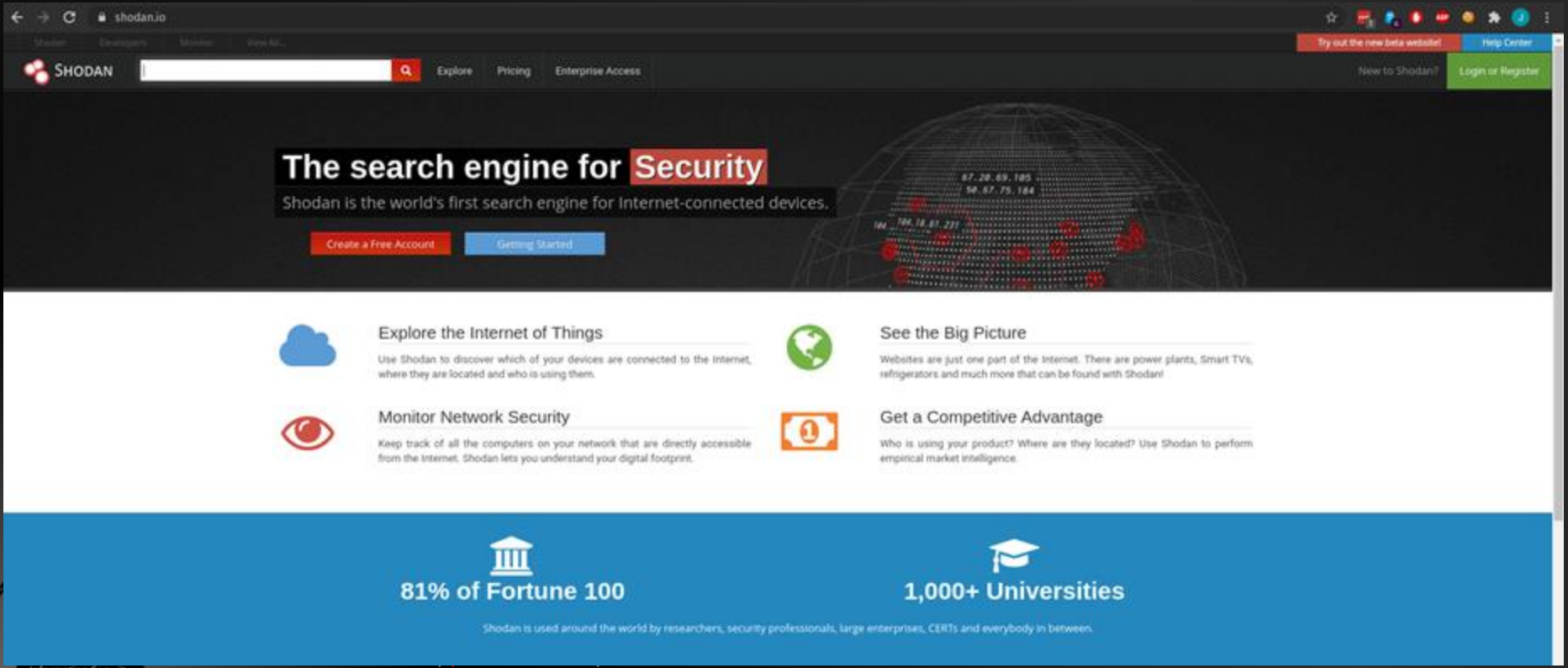
Top Ports

Insecure.Org

Top 10 TCP ports

- 80 (http)
- 23 (telnet)
- 22 (ssh)
- 443 (https)
- 3389 (ms-term-serv)
- 445 (microsoft-ds)
- 139 (netbios-ssn)
- 21 (ftp)
- 135 (msrpc)
- 25 (smtp)

Shodan



Shodan Ports

Shodan collects data mostly on **web** servers (HTTP/HTTPS – **ports** 80, 8080, 443, 8443), as well as FTP (**port** 21), SSH (**port** 22), Telnet (**port** 23), SNMP (**port** 161), IMAP (**ports** 143, or (encrypted) 993), SMTP (**port** 25), SIP (**port** 5060), and Real Time Streaming Protocol (RTSP, **port** 554).

en.wikipedia.org › wiki › Shodan_(website)

Shodan (website) - Wikipedia

tcpdump -D

```
john@john-onion ~/pcaps> tcpdump -D
1.docker0 [Up, Running]
2.veth9807ef0 [Up, Running]
3.vethba446cd [Up, Running]
4.veth07191f2 [Up, Running]
5.veth53bc0a7 [Up, Running]
6.veth6b6fe9e [Up, Running]
7.vethc06fe9e [Up, Running]
8.ens33 [Up, Running]
9.vethe5b4e39 [Up, Running]
10.veth7539a85 [Up, Running]
11.veth028a400 [Up, Running]
12.vethbd60970 [Up, Running]
13.br-0edb29070257 [Up, Running]
14.any (Pseudo-device that captures on all interfaces) [Up, Running]
15.lo [Up, Running, Loopback]
16.bluetooth0 (Bluetooth adapter number 0)
17.nflog (Linux netfilter log (NFLOG) interface)
18.nfqueue (Linux netfilter queue (NFQUEUE) interface)
19.usbmon1 (USB bus number 1)
20.usbmon2 (USB bus number 2)
john@john-onion ~/pcaps>
```

-D Lists Interfaces

tcpdump -X and -A

```
john@john-onion ~/pcaps> sudo tcpdump -i ens33 -XA
        0x0050:  3435 3637                                4567
19:28:09.078439 IP dns.google > john-onion: ICMP echo reply, id 58067, seq 2, length 64
        0x0000:  4500 0054 61b4 0000 8001 b9bc 0808 0808  E..Ta...........
        0x0010:  c0a8 4e80 0000 ae60 e2d3 0002 498a 135e  ..N....`....I..^
        0x0020:  0000 0000 530e 0000 0000 0000 1011 1213  ....S...........
        0x0030:  1415 1617 1819 1a1b 1c1d 1e1f 2021 2223  .............!"#
        0x0040:  2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
        0x0050:  3435 3637                                4567
19:28:10.005420 IP john-onion > dns.google: ICMP echo request, id 58067, seq 3, length 64
        0x0000:  4500 0054 55ac 4000 4001 c5c4 c0a8 4e80  E..TU.@.@.....N.
        0x0010:  0808 0808 0800 e558 e2d3 0003 4a8a 135e  .......X....J..^
        0x0020:  0000 0000 1315 0000 0000 0000 1011 1213  ................
        0x0030:  1415 1617 1819 1a1b 1c1d 1e1f 2021 2223  .............!"#
        0x0040:  2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
        0x0050:  3435 3637                                4567
19:28:10.145845 IP dns.google > john-onion: ICMP echo reply, id 58067, seq 3, length 64
        0x0000:  4500 0054 61b5 0000 8001 b9bb 0808 0808  E..Ta...........
        0x0010:  c0a8 4e80 0000 ed58 e2d3 0003 4a8a 135e  ..N....X....J..^
        0x0020:  0000 0000 1315 0000 0000 0000 1011 1213  ................
        0x0030:  1415 1617 1819 1a1b 1c1d 1e1f 2021 2223  .............!"#
        0x0040:  2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
        0x0050:  3435 3637                                4567
```

-X is for the Hex

-A is for the ASCII

tcpdump: host, port and -r

```
john@john-onion ~/pcaps> tcpdump -r taidoor_traffic_no_interaction.pcap -X -A host 10.0.2.
15 and port 80
```

-r = read a previous capture

```
16:09:36.179880 IP 10.0.2.15.49845 > 104.248.234.238.http: Flags [P.], seq 1:516, ack 1, w
in 65535, length 515: HTTP: GET /process.jsp?mn=IOEHPJEALJEPFPEDJDFMBLNHDBAFJCIECPOMOHMNFK
IPNMJIFBGHGLJIJOAMCBDBKBFPEONMJAFKMNKBGGJOPKHJPJOGGLPGBDNCKIOBDFOLKAODLKLBDDFLKFOHABGIKCDP
NNABOGHBDHCGIGBIPBHLHCHIKKOHAHIIFCAOHGNLDNKPBLEAHKAFOLOLHLPGBFOHIFDKNNCOGNHPDHIHLABKCMMBCG
OMBEIBAPHJIHGOCBHBBOGJHFENJNILIPMA HTTP/1.1
        0x0000:  4500 022b 0926 4000 8006 0000 0a00 020f  E..+.&@.........
        0x0010:  68f8 eaee c2b5 0050 57f5 8e78 27b7 f802  h......PW..x'...
        0x0020:  5018 ffff 6213 0000 4745 5420 2f70 726f  P...b...GET./pro
        0x0030:  6365 7373 2e6a 7370 3f6d 6e3d 494f 4548  cess.jsp?mn=IOEH
        0x0040:  504a 4541 4c4a 4550 4650 4544 4a44 464d  PJEALJEPFPEDJDFM
        0x0050:  424c 4e48 4442 4146 4a43 4945 4350 4f4d  BLNHDBAFJCIECPOM
        0x0060:  4f48 4d4e 464b 4950 4e4d 4a49 4642 4748  OHMNFKIPNMJIFBGH
        0x0070:  474c 4a49 4a4f 414d 4342 4442 4b42 4650  GLJIJOAMCBDBKBFP
        0x0080:  454f 4e4d 4a41 464b 4d4e 4b42 4747 4a4f  EONMJAFKMNKBGGJO
        0x0090:  504b 484a 504a 4f47 474c 5047 4244 4e43  PKHJPJOGGLPGBDNC
        0x00a0:  4b49 4f42 4446 4f4c 4b41 4f44 4c4b 4c42  KIOBDFOLKAODLKLB
        0x00b0:  4444 464c 4b46 4f48 4142 4749 4b43 4450  DDFLKFOHABGIKCDP
```

tcpdump -w

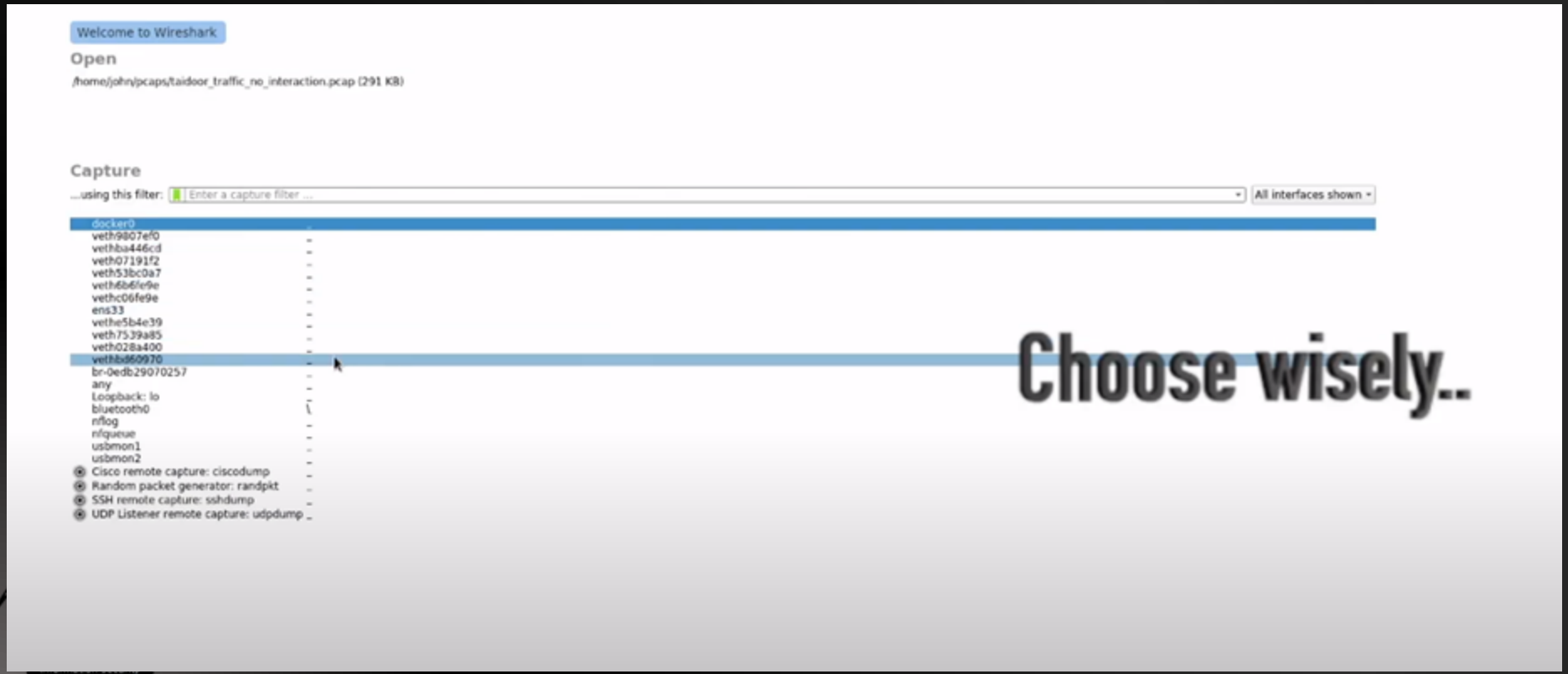
```
john@john-onion ~/pcaps> tcpdump -i ens33
```

-w is to write the data to a file

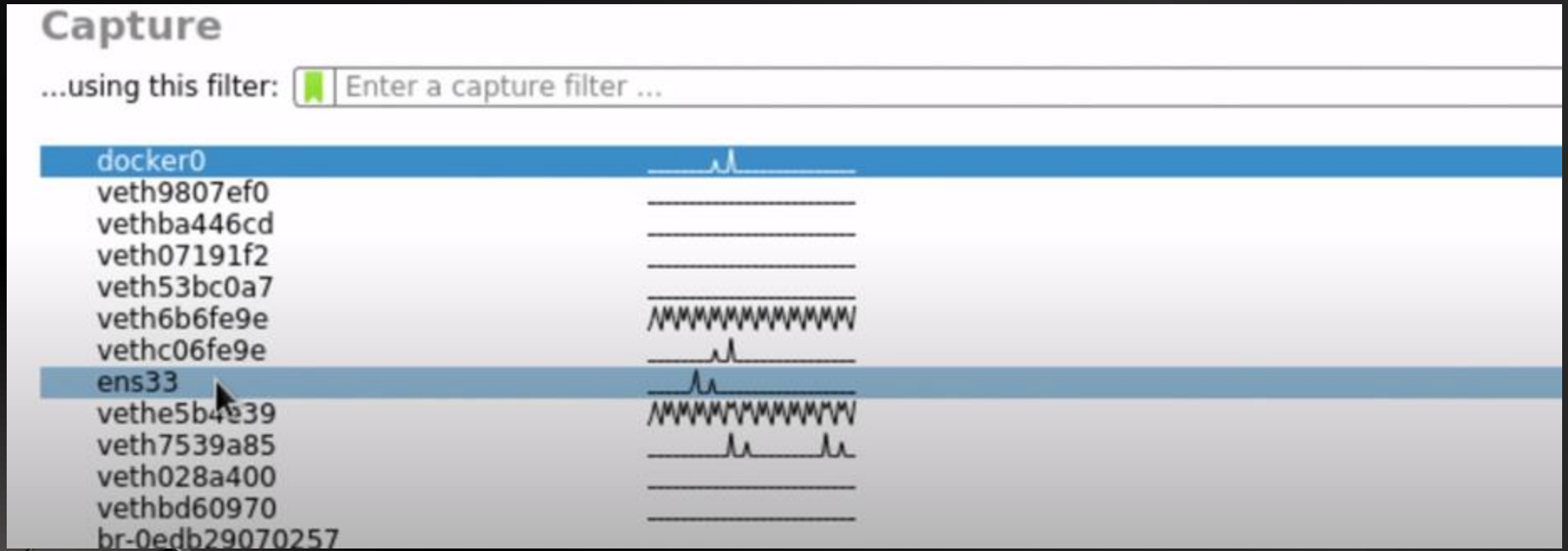
LAB: TCPDump

Wireshark

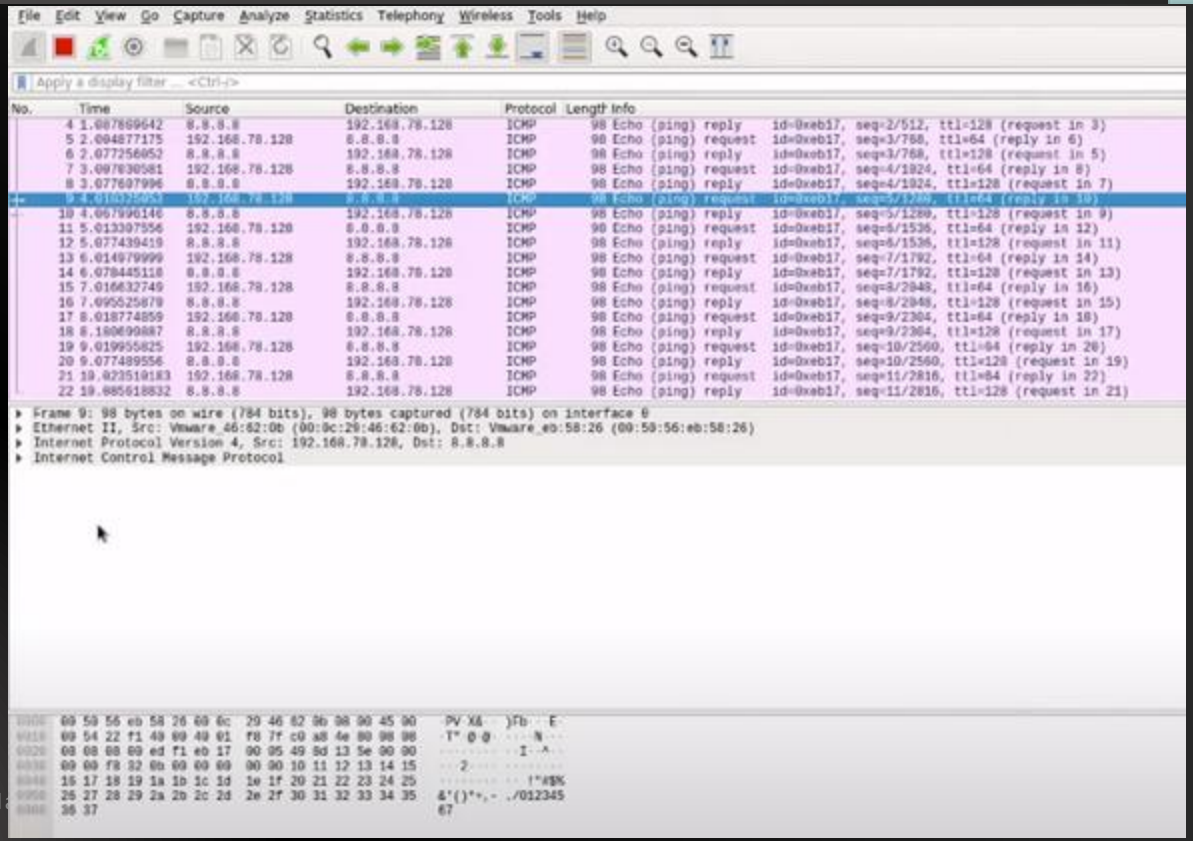
Wireshark and Interfaces



Watching the traffic



Wireshark and ping

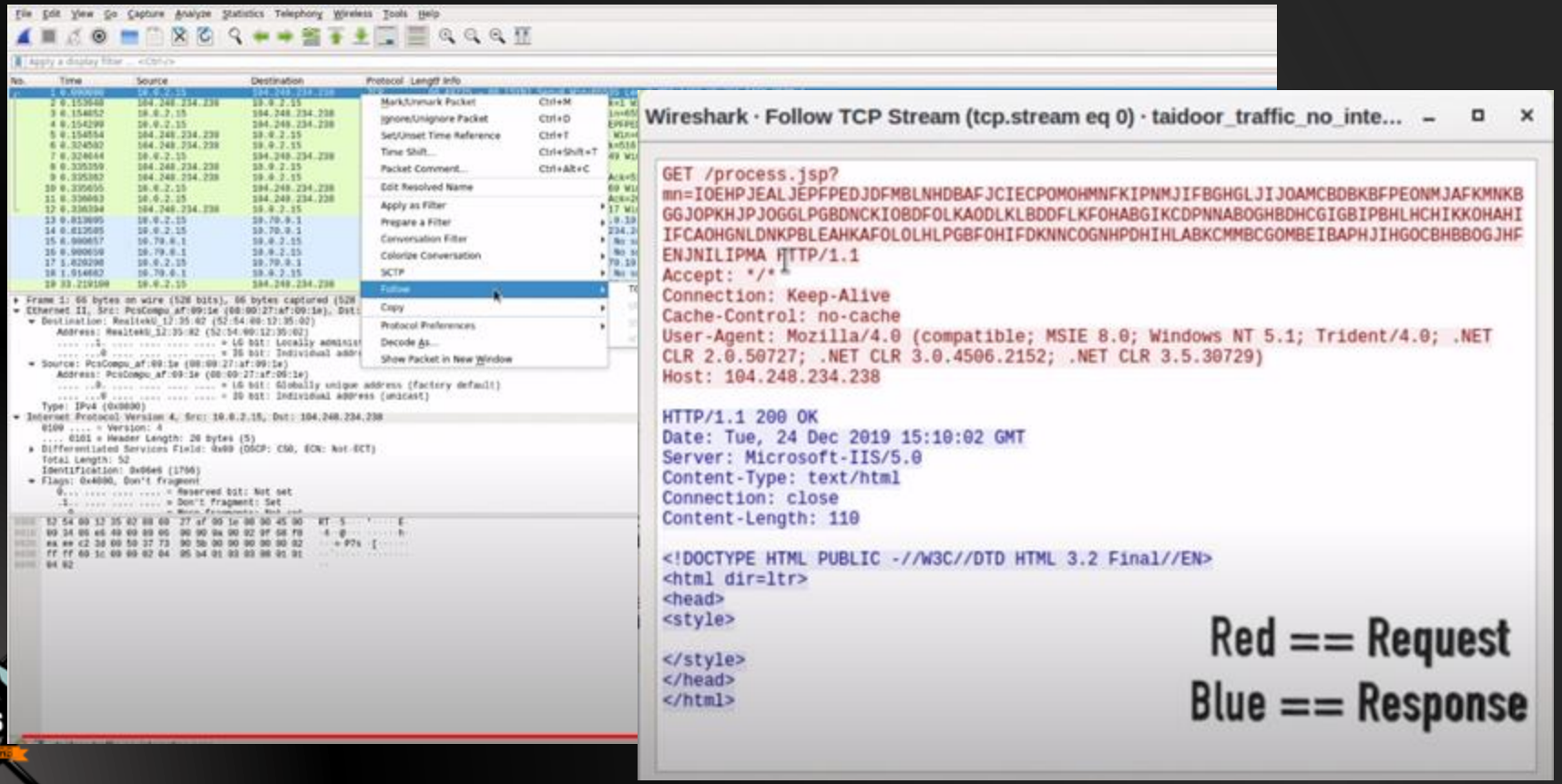


Packet Breakdown

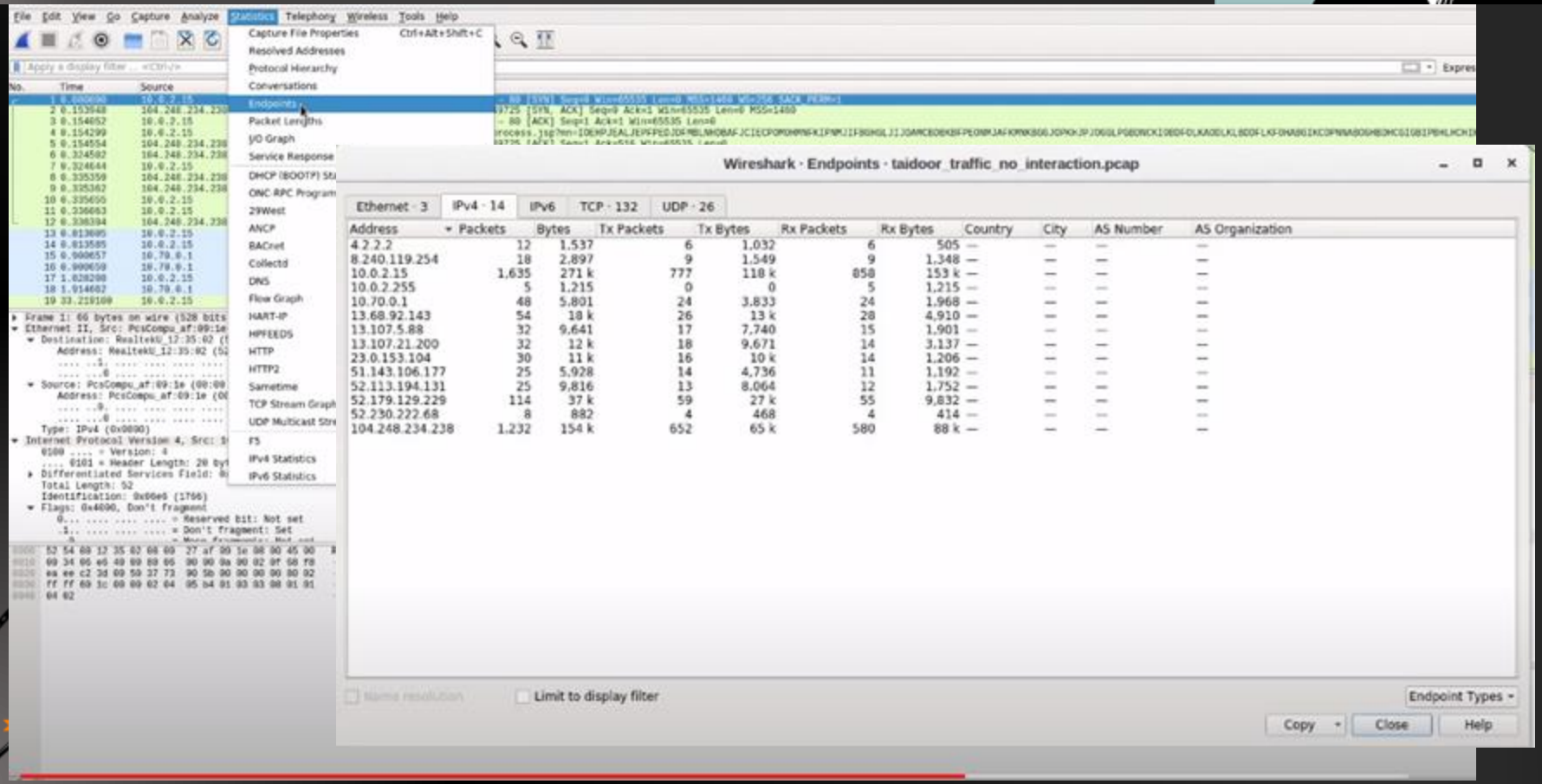
```
▸ Frame 9: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▾ Ethernet II, Src: Vmware_46:62:0b (00:0c:29:46:62:0b), Dst: Vmware_eb:58:26 (00:50:56:eb:58:26)
  ▾ Destination: Vmware_eb:58:26 (00:50:56:eb:58:26)
      Address: Vmware_eb:58:26 (00:50:56:eb:58:26)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▾ Source: Vmware_46:62:0b (00:0c:29:46:62:0b)
      Address: Vmware_46:62:0b (00:0c:29:46:62:0b)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
▾ Internet Protocol Version 4, Src: 192.168.78.128, Dst: 8.8.8.8
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x22f1 (8945)
  ▾ Flags: 0x4000, Don't fragment
      0... .... .... .... = Reserved bit: Not set
      .1.. .... .... .... = Don't fragment: Set
      ..0. .... .... .... = More fragments: Not set

0000  00 50 56 eb 58 26 00 0c  29 46 62 0b 08 00 45 00   ·PV·X&·· )Fb···E·
0010  00 54 22 f1 40 00 40 01  f8 7f c0 a8 4e 80 08 08   ·T"·@·@ ····N···
0020  08 08 08 00 ed f1 eb 17  00 05 49 8d 13 5e 00 00   ···· ···· ··I··^··
0030  00 00 f8 32 0b 00 00 00  00 00 10 11 12 13 14 15   ···2···· ····· ···
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ····· ··· ··· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                              67
```

Wireshark

Follow TCP Stream

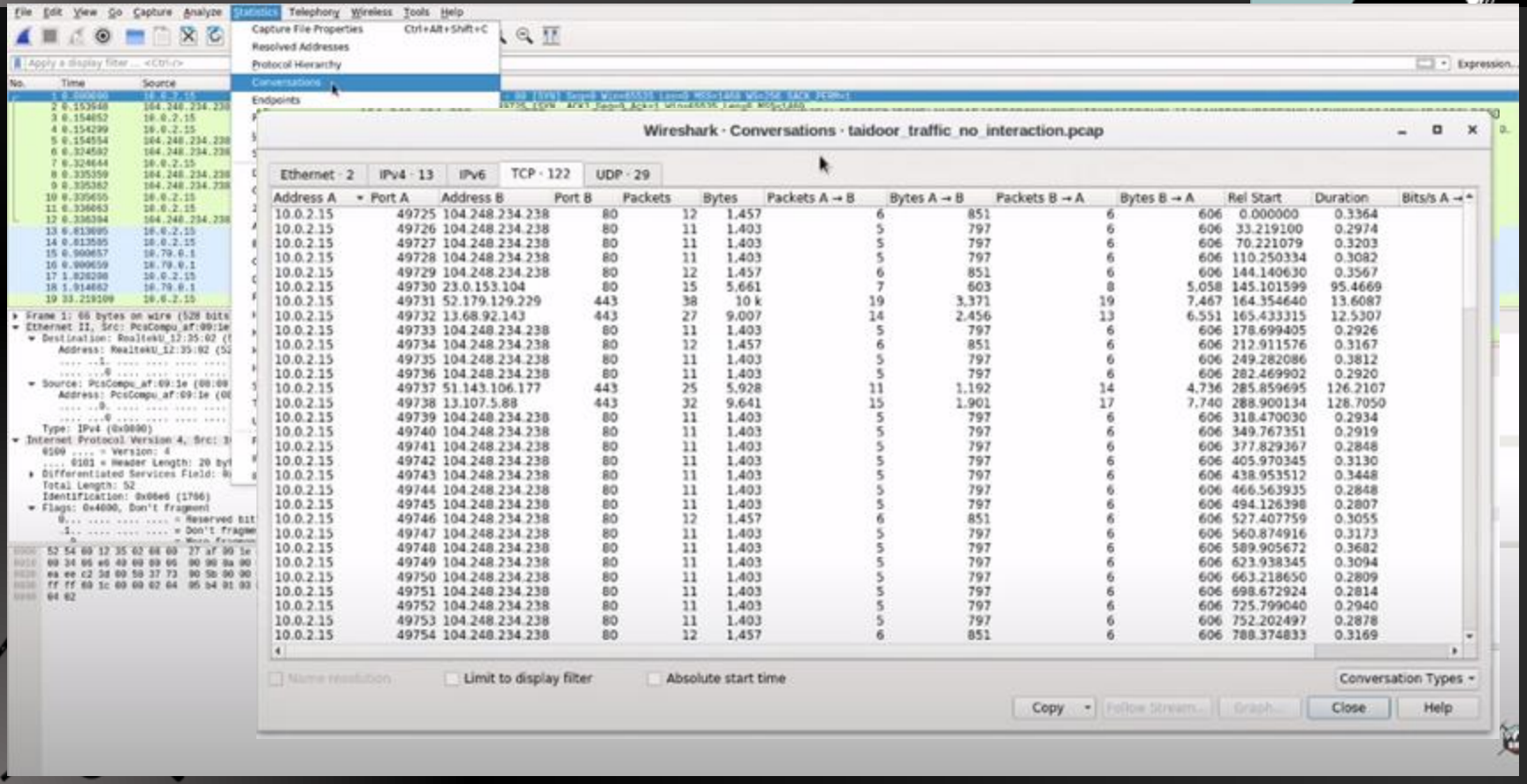


Statistics > Endpoints



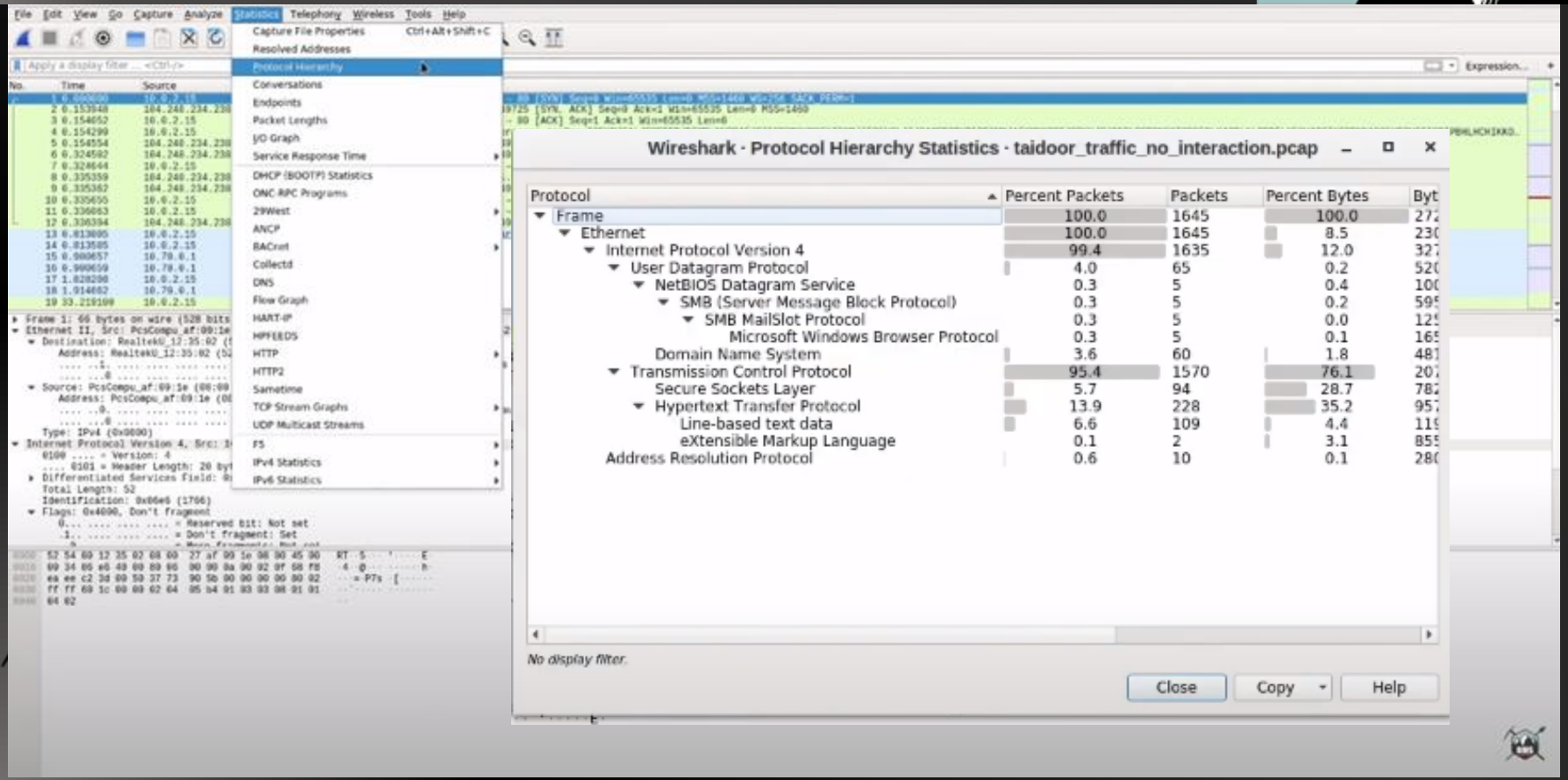
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number	AS Organization
4.2.2.2	12	1,537	6	1,032	6	505	—	—	—	—
8.240.119.254	18	2,897	9	1,549	9	1,348	—	—	—	—
10.0.2.15	1,635	271 k	777	118 k	858	153 k	—	—	—	—
10.0.2.255	5	1,215	0	0	5	1,215	—	—	—	—
10.70.0.1	48	5,801	24	3,833	24	1,968	—	—	—	—
13.68.92.143	54	18 k	26	13 k	28	4,910	—	—	—	—
13.107.5.88	32	9,641	17	7,740	15	1,901	—	—	—	—
13.107.21.200	32	12 k	18	9,671	14	3,137	—	—	—	—
23.0.153.104	30	11 k	16	10 k	14	1,206	—	—	—	—
51.143.106.177	25	5,928	14	4,736	11	1,192	—	—	—	—
52.113.194.131	25	9,816	13	8,064	12	1,752	—	—	—	—
52.179.129.229	114	37 k	59	27 k	55	9,832	—	—	—	—
52.230.222.68	8	882	4	468	4	414	—	—	—	—
104.248.234.238	1,232	154 k	652	65 k	580	88 k	—	—	—	—

Statistics > Conversations



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	Bits/s A →
10.0.2.15	49725	104.248.234.238	80	12	1,457	6	851	6	606	0.000000	0.3364	
10.0.2.15	49726	104.248.234.238	80	11	1,403	5	797	6	606	33.219100	0.2974	
10.0.2.15	49727	104.248.234.238	80	11	1,403	5	797	6	606	70.221079	0.3203	
10.0.2.15	49728	104.248.234.238	80	11	1,403	5	797	6	606	110.250334	0.3082	
10.0.2.15	49729	104.248.234.238	80	12	1,457	6	851	6	606	144.140630	0.3567	
10.0.2.15	49730	23.0.153.104	80	15	5,661	7	603	8	5,058	145.101599	95.4669	
10.0.2.15	49731	52.179.129.229	443	38	10 k	19	3,371	19	7,467	164.354640	13.6087	
10.0.2.15	49732	13.68.92.143	443	27	9,007	14	2,456	13	6,551	165.433315	12.5307	
10.0.2.15	49733	104.248.234.238	80	11	1,403	5	797	6	606	178.699405	0.2926	
10.0.2.15	49734	104.248.234.238	80	12	1,457	6	851	6	606	212.911576	0.3167	
10.0.2.15	49735	104.248.234.238	80	11	1,403	5	797	6	606	249.282086	0.3812	
10.0.2.15	49736	104.248.234.238	80	11	1,403	5	797	6	606	282.469902	0.2920	
10.0.2.15	49737	51.143.106.177	443	25	5,928	11	1,192	14	4,736	285.859695	126.2107	
10.0.2.15	49738	13.107.5.88	443	32	9,641	15	1,901	17	7,740	288.900134	128.7050	
10.0.2.15	49739	104.248.234.238	80	11	1,403	5	797	6	606	318.470030	0.2934	
10.0.2.15	49740	104.248.234.238	80	11	1,403	5	797	6	606	349.767351	0.2919	
10.0.2.15	49741	104.248.234.238	80	11	1,403	5	797	6	606	377.829367	0.2848	
10.0.2.15	49742	104.248.234.238	80	11	1,403	5	797	6	606	405.970345	0.3130	
10.0.2.15	49743	104.248.234.238	80	11	1,403	5	797	6	606	438.953512	0.3448	
10.0.2.15	49744	104.248.234.238	80	11	1,403	5	797	6	606	466.563935	0.2848	
10.0.2.15	49745	104.248.234.238	80	11	1,403	5	797	6	606	494.126398	0.2807	
10.0.2.15	49746	104.248.234.238	80	12	1,457	6	851	6	606	527.407759	0.3055	
10.0.2.15	49747	104.248.234.238	80	11	1,403	5	797	6	606	560.874916	0.3173	
10.0.2.15	49748	104.248.234.238	80	11	1,403	5	797	6	606	589.905672	0.3682	
10.0.2.15	49749	104.248.234.238	80	11	1,403	5	797	6	606	623.938345	0.3094	
10.0.2.15	49750	104.248.234.238	80	11	1,403	5	797	6	606	663.218650	0.2809	
10.0.2.15	49751	104.248.234.238	80	11	1,403	5	797	6	606	698.672924	0.2814	
10.0.2.15	49752	104.248.234.238	80	11	1,403	5	797	6	606	725.799040	0.2940	
10.0.2.15	49753	104.248.234.238	80	11	1,403	5	797	6	606	752.202497	0.2878	
10.0.2.15	49754	104.248.234.238	80	12	1,457	6	851	6	606	788.374833	0.3169	

Statistics > Protocol Hierarchy



Statistics > HTTP > Requests

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Statistics menu:
- Capture File Properties Ctrl+Alt+Shift+C
- Resolved Addresses
- Protocol Hierarchy
- Conversations
- Endpoints
- Packet Lengths
- I/O Graph
- Service Response Time
- DHCP (BOOTP) Statistics
- ONC-RPC Programs
- 29West
- ANCP
- BACnet
- Collectd
- DNS
- Flow Graph
- HART-IP
- HPFEEDS
- HTTP
  - Packet Counter
  - Requests
  - Load Distribution
  - Request Sequences
- HTTP2
- Sametime
- TCP Stream Graphs
- UDP Multicast Streams
- F5
- IPv4 Statistics
- IPv6 Statistics

Wireshark · Requests · taidoor_traffic_no_interaction.pcap

Topic / Item

- HTTP Requests by HTTP Host
  - tile-service.weather.microsoft.com
    - /en-US/livetile/preinstall?region=US&appid=C98EA5B0842DBB9405BBF071E1DA76512D21FE36&FORM=Threshold
  - ctldl.windowsupdate.com
    - /msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?13db202675b3f464
    - /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?b56e63a9af45dd80
    - /msdownload/update/v3/static/trustedr/en/authrootstl.cab?aac643d5e8c41bf9
  - 104.248.234.238
    - /process.jsp?mn=IOEHPJEALJEPPEDJDFMBLNHDBAFJCIECPOMOHMNFKIPNMJIFBGHGLJIJOAMCBDBKBFPEONMJAFKMNKB

Display filter: Enter a display filter ... Apply

Copy Save as... Close

LAB: Wireshark