MP4: Network Security

CS461 / ECE422 – UIUC Spring 2016

Simon Kim

Introduction

Goals

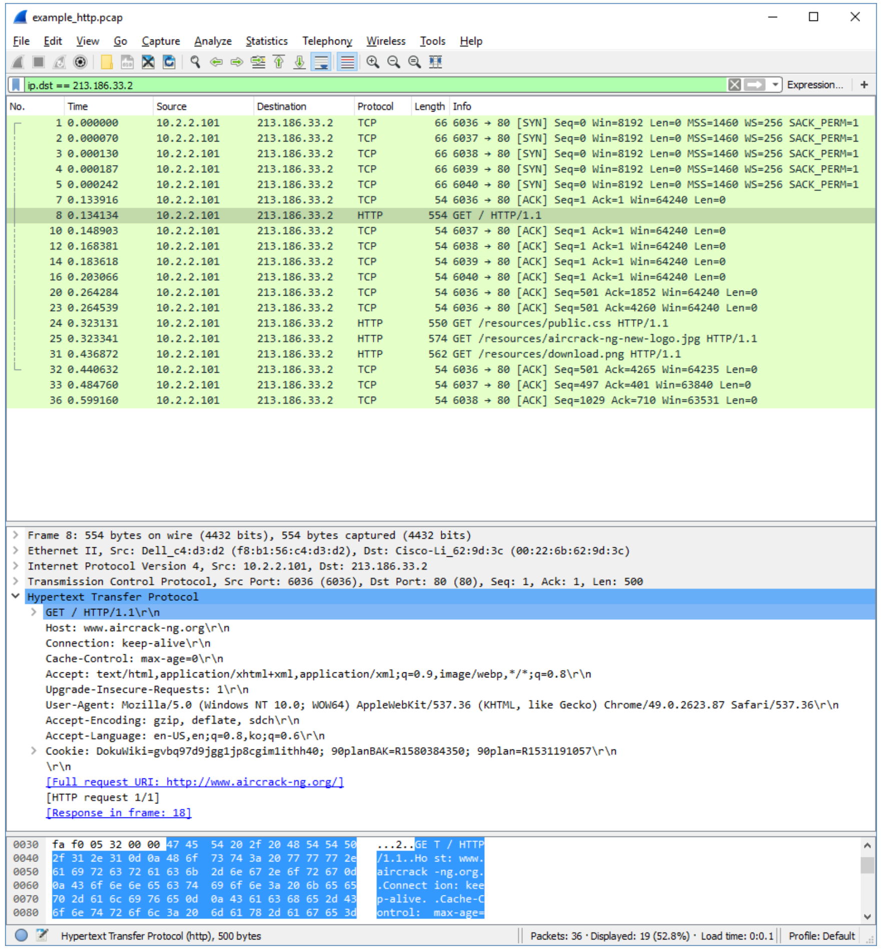
- Checkpoint 1
  - Learn how to use Wireshark
  - Identify network activities
  - Identify attacks or vulnerabilities
- Checkpoint 2
  - Attack a network and extract information
  - Programmatically detect attacks from network traces

Required Tools

- Checkpoint 1
  - Wireshark – any version of Wireshark is fine
- Checkpoint 2
  - Wireshark 32 bit
  - Aircrack-ng Suite
  - nmap
  - Python 2.7
  - dpkt Python library

Checkpoint 1: How to use Wireshark

- Dig through “Packet Details”
- “Apply a display filter”
- Add your own columns to display
- Use other built-in features found in menus



```
ip.dst == 213.186.33.2
```

```
No.   Time      Source      Destination   Protocol  Length Info
    1 0.000000  10.2.2.101  213.186.33.2  TCP         66 6036 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
    2 0.000070  10.2.2.101  213.186.33.2  TCP         66 6037 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
    3 0.000130  10.2.2.101  213.186.33.2  TCP         66 6038 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
    4 0.000187  10.2.2.101  213.186.33.2  TCP         66 6039 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
    5 0.000242  10.2.2.101  213.186.33.2  TCP         66 6040 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
    7 0.133916  10.2.2.101  213.186.33.2  TCP         54 6036 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
    8 0.134134  10.2.2.101  213.186.33.2  HTTP       554 GET / HTTP/1.1
   10 0.148903  10.2.2.101  213.186.33.2  TCP         54 6037 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
   12 0.168381  10.2.2.101  213.186.33.2  TCP         54 6038 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
   14 0.183618  10.2.2.101  213.186.33.2  TCP         54 6039 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
   16 0.203066  10.2.2.101  213.186.33.2  TCP         54 6040 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
   20 0.264284  10.2.2.101  213.186.33.2  TCP         54 6036 → 80 [ACK] Seq=501 Ack=1852 Win=64240 Len=0
   23 0.264539  10.2.2.101  213.186.33.2  TCP         54 6036 → 80 [ACK] Seq=501 Ack=4260 Win=64240 Len=0
   24 0.323131  10.2.2.101  213.186.33.2  HTTP       550 GET /resources/public.css HTTP/1.1
   25 0.323341  10.2.2.101  213.186.33.2  HTTP       574 GET /resources/aircrack-ng-new-logo.jpg HTTP/1.1
   31 0.436872  10.2.2.101  213.186.33.2  HTTP       562 GET /resources/download.png HTTP/1.1
   32 0.440632  10.2.2.101  213.186.33.2  TCP         54 6036 → 80 [ACK] Seq=501 Ack=4265 Win=64235 Len=0
   33 0.484760  10.2.2.101  213.186.33.2  TCP         54 6037 → 80 [ACK] Seq=497 Ack=401 Win=63840 Len=0
   36 0.599160  10.2.2.101  213.186.33.2  TCP         54 6038 → 80 [ACK] Seq=1029 Ack=710 Win=63531 Len=0
```

```
> Frame 8: 554 bytes on wire (4432 bits), 554 bytes captured (4432 bits)
> Ethernet II, Src: Dell_c4:d3:d2 (f8:b1:56:c4:d3:d2), Dst: Cisco-Li_62:9d:3c (00:22:6b:62:9d:3c)
> Internet Protocol Version 4, Src: 10.2.2.101, Dst: 213.186.33.2
> Transmission Control Protocol, Src Port: 6036 (6036), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 500
v Hypertext Transfer Protocol
  > GET / HTTP/1.1\r\n
    Host: www.aircrack-ng.org\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/49.0.2623.87 Safari/537.36\r\n
    Accept-Encoding: gzip, deflate, sdch\r\n
    Accept-Language: en-US,en;q=0.8,ko;q=0.6\r\n
  > Cookie: DokuWiki=gvbq97d9jgg1jp8cgim1ithh40; 90planBAK=R1580384350; 90plan=R1531191057\r\n
    \r\n
    [Full request URI: http://www.aircrack-ng.org/]
    [HTTP request 1/1]
    [Response in frame: 18]
```

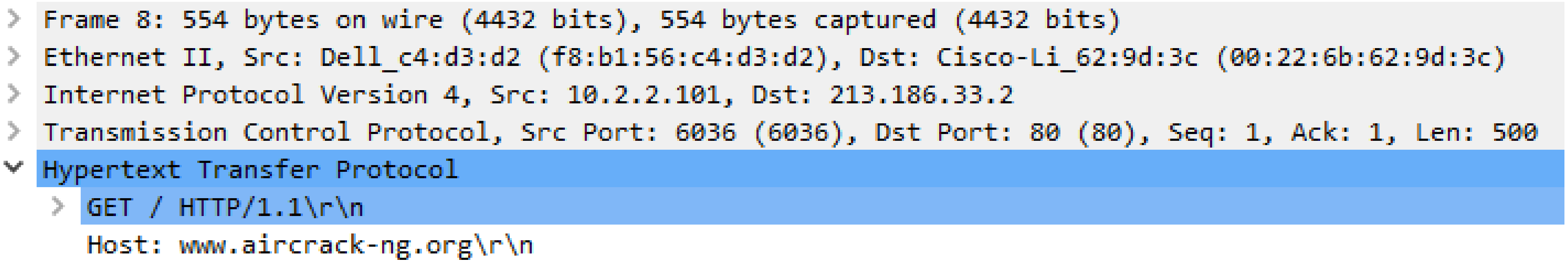
```
0030  fa f0 05 32 00 00 47 45  54 20 2f 20 48 54 54 50   ...2..GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 77 77 77 2e   /1.1..Ho st: www.
0050  61 69 72 63 72 61 63 6b  2d 6e 67 2e 6f 72 67 0d   aircrack -ng.org.
0060  0a 43 6f 6e 6e 65 63 74  69 6f 6e 3a 20 6b 65 65   .Connect ion: kee
0070  70 2d 61 6c 69 76 65 0d  0a 43 61 63 68 65 2d 43   p-alive. .Cache-C
0080  6f 6e 74 72 6f 6c 3a 20  6d 61 78 2d 61 67 65 3d   ontrol:  max-age=
```

Hypertext Transfer Protocol (http), 500 bytes

Packets: 36 · Displayed: 19 (52.8%) · Load time: 0:0.1

Profile: Default

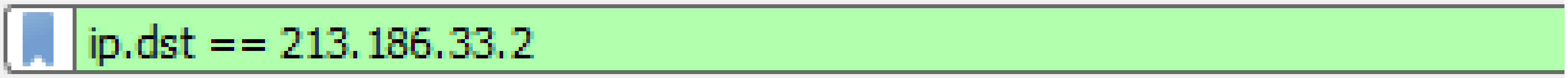
Packet Details



```
> Frame 8: 554 bytes on wire (4432 bits), 554 bytes captured (4432 bits)
> Ethernet II, Src: Dell_c4:d3:d2 (f8:b1:56:c4:d3:d2), Dst: Cisco-Li_62:9d:3c (00:22:6b:62:9d:3c)
> Internet Protocol Version 4, Src: 10.2.2.101, Dst: 213.186.33.2
> Transmission Control Protocol, Src Port: 6036 (6036), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 500
v Hypertext Transfer Protocol
  > GET / HTTP/1.1\r\n
    Host: www.aircrack-ng.org\r\n
```

- Everything that Wireshark can tell you about the packet
  - IP address, port numbers, MAC address, hostname, data, etc.

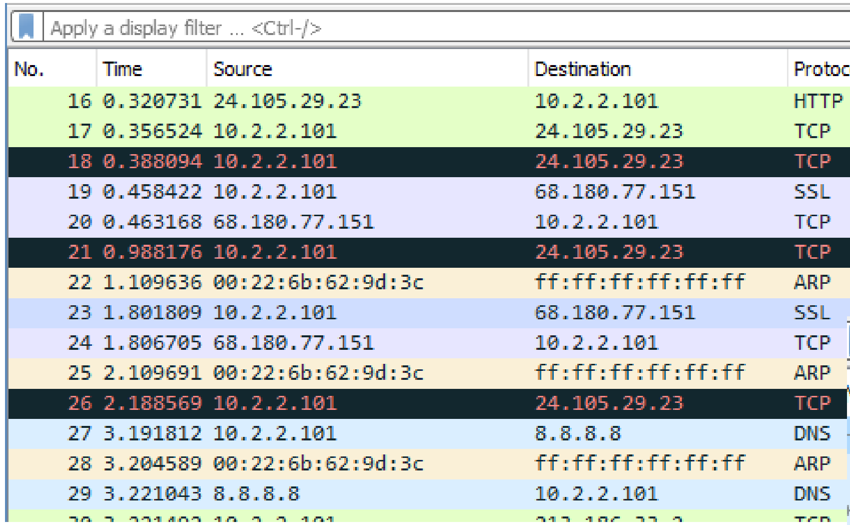
Apply a display filter



```
ip.dst == 213.186.33.2
```

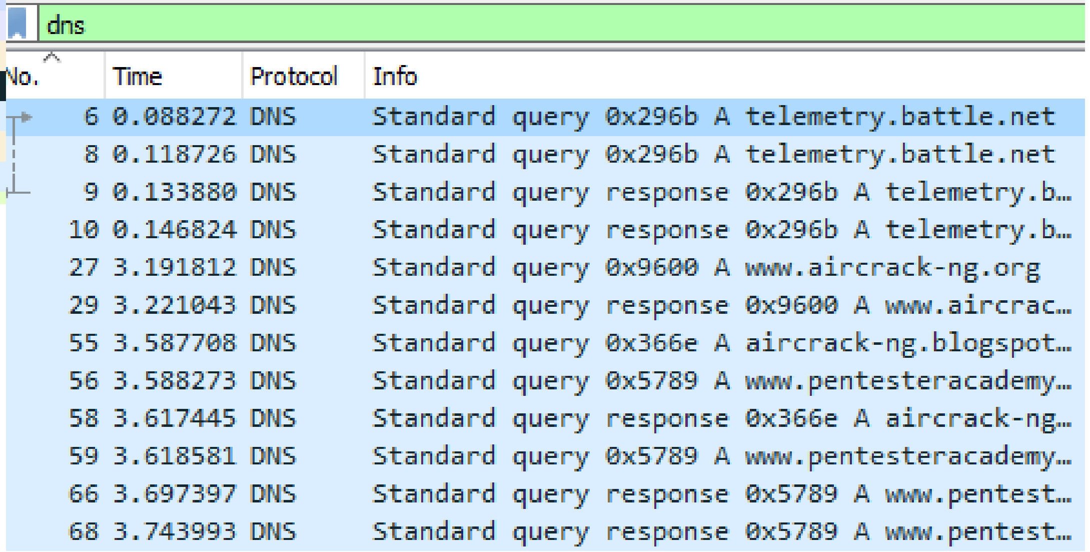
- Shows packets that contain the information you are interested
  - Examples: https://wiki.wireshark.org/DisplayFilters
- Filter expression basics and syntax: https://www.wireshark.org/docs/wsug_html_chunked/ChWorkBuildDisplayFilterSection.html
- Filter Reference: https://www.wireshark.org/docs/dfref/
  - Ex) ip.addr, ip.src, ip.dst

Ex) dns



Apply a display filter ... <Ctrl-/>

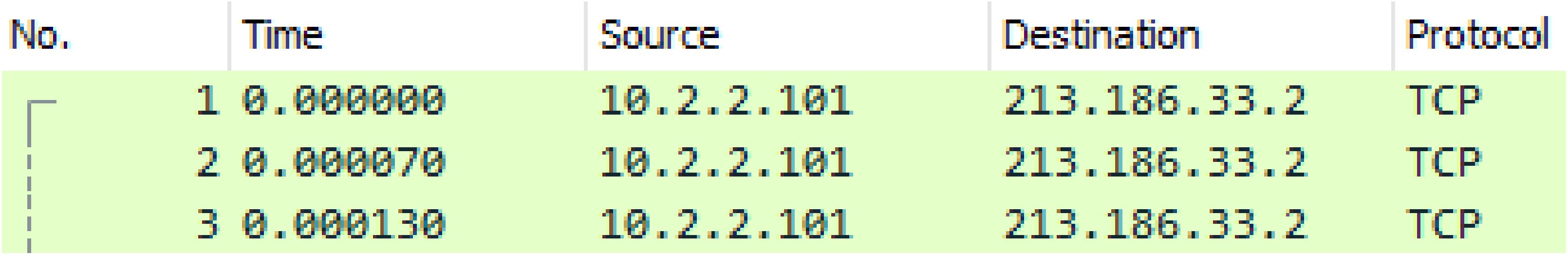
No.	Time	Source	Destination	Protocol
16	0.320731	24.105.29.23	10.2.2.101	HTTP
17	0.356524	10.2.2.101	24.105.29.23	TCP
18	0.388094	10.2.2.101	24.105.29.23	TCP
19	0.458422	10.2.2.101	68.180.77.151	SSL
20	0.463168	68.180.77.151	10.2.2.101	TCP
21	0.988176	10.2.2.101	24.105.29.23	TCP
22	1.109636	00:22:6b:62:9d:3c	ff:ff:ff:ff:ff:ff	ARP
23	1.801809	10.2.2.101	68.180.77.151	SSL
24	1.806705	68.180.77.151	10.2.2.101	TCP
25	2.109691	00:22:6b:62:9d:3c	ff:ff:ff:ff:ff:ff	ARP
26	2.188569	10.2.2.101	24.105.29.23	TCP
27	3.191812	10.2.2.101	8.8.8.8	DNS
28	3.204589	00:22:6b:62:9d:3c	ff:ff:ff:ff:ff:ff	ARP
29	3.221043	8.8.8.8	10.2.2.101	DNS



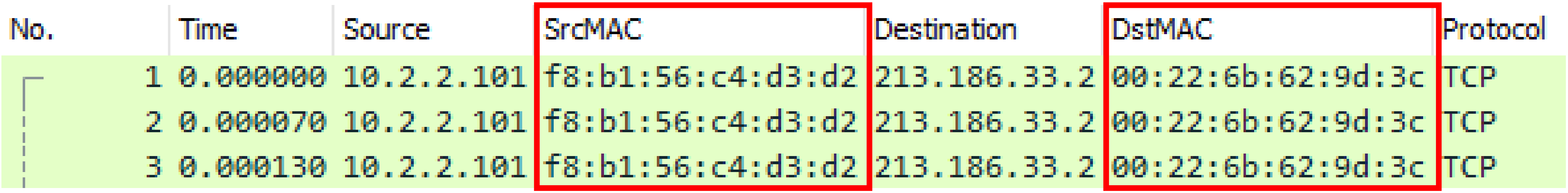
dns

No.	Time	Protocol	Info
6	0.088272	DNS	Standard query 0x296b A telemetry.battle.net
8	0.118726	DNS	Standard query 0x296b A telemetry.battle.net
9	0.133880	DNS	Standard query response 0x296b A telemetry.b…
10	0.146824	DNS	Standard query response 0x296b A telemetry.b…
27	3.191812	DNS	Standard query 0x9600 A www.aircrack-ng.org
29	3.221043	DNS	Standard query response 0x9600 A www.aircrac…
55	3.587708	DNS	Standard query 0x366e A aircrack-ng.blogspot…
56	3.588273	DNS	Standard query 0x5789 A www.pentesteracademy…
58	3.617445	DNS	Standard query response 0x366e A aircrack-ng…
59	3.618581	DNS	Standard query 0x5789 A www.pentesteracademy…
66	3.697397	DNS	Standard query response 0x5789 A www.pentest…
68	3.743993	DNS	Standard query response 0x5789 A www.pentest…

Add your own columns



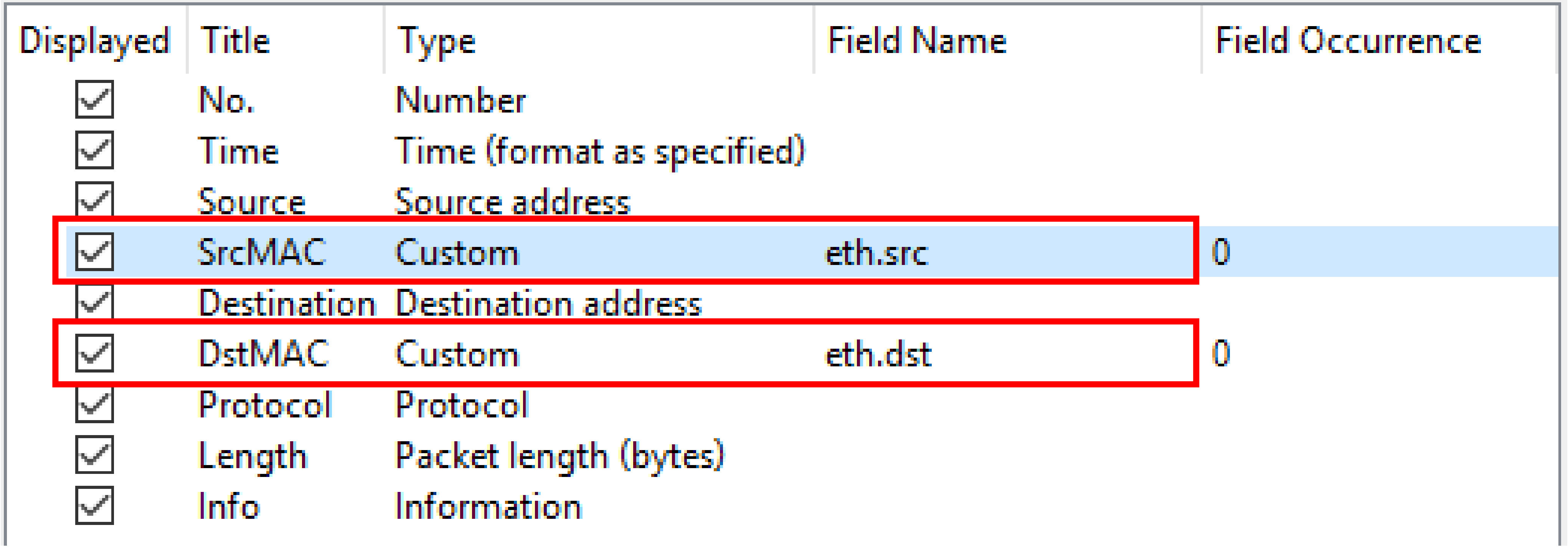
No.	Time	Source	Destination	Protocol
1	0.000000	10.2.2.101	213.186.33.2	TCP
2	0.000070	10.2.2.101	213.186.33.2	TCP
3	0.000130	10.2.2.101	213.186.33.2	TCP



No.	Time	Source	SrcMAC	Destination	DstMAC	Protocol
1	0.000000	10.2.2.101	f8:b1:56:c4:d3:d2	213.186.33.2	00:22:6b:62:9d:3c	TCP
2	0.000070	10.2.2.101	f8:b1:56:c4:d3:d2	213.186.33.2	00:22:6b:62:9d:3c	TCP
3	0.000130	10.2.2.101	f8:b1:56:c4:d3:d2	213.186.33.2	00:22:6b:62:9d:3c	TCP

Add your own columns

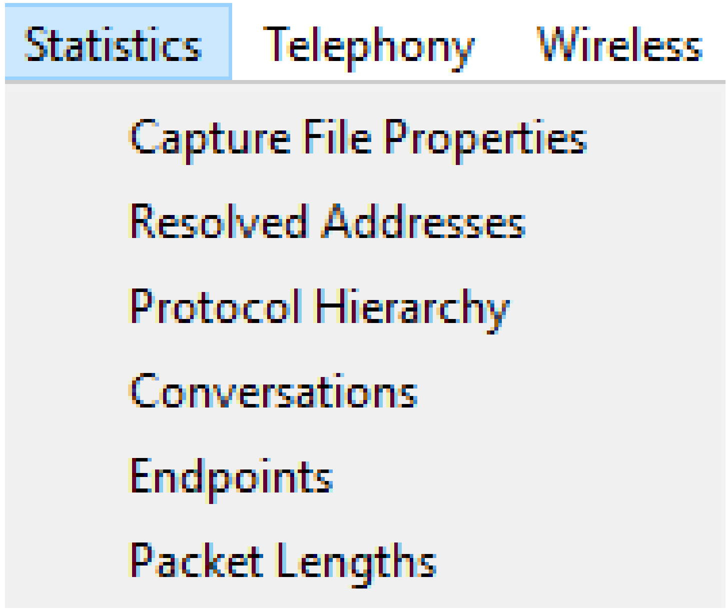
- Right-click column header > Column Preferences
  or Edit > Preferences > Appearance: Columns

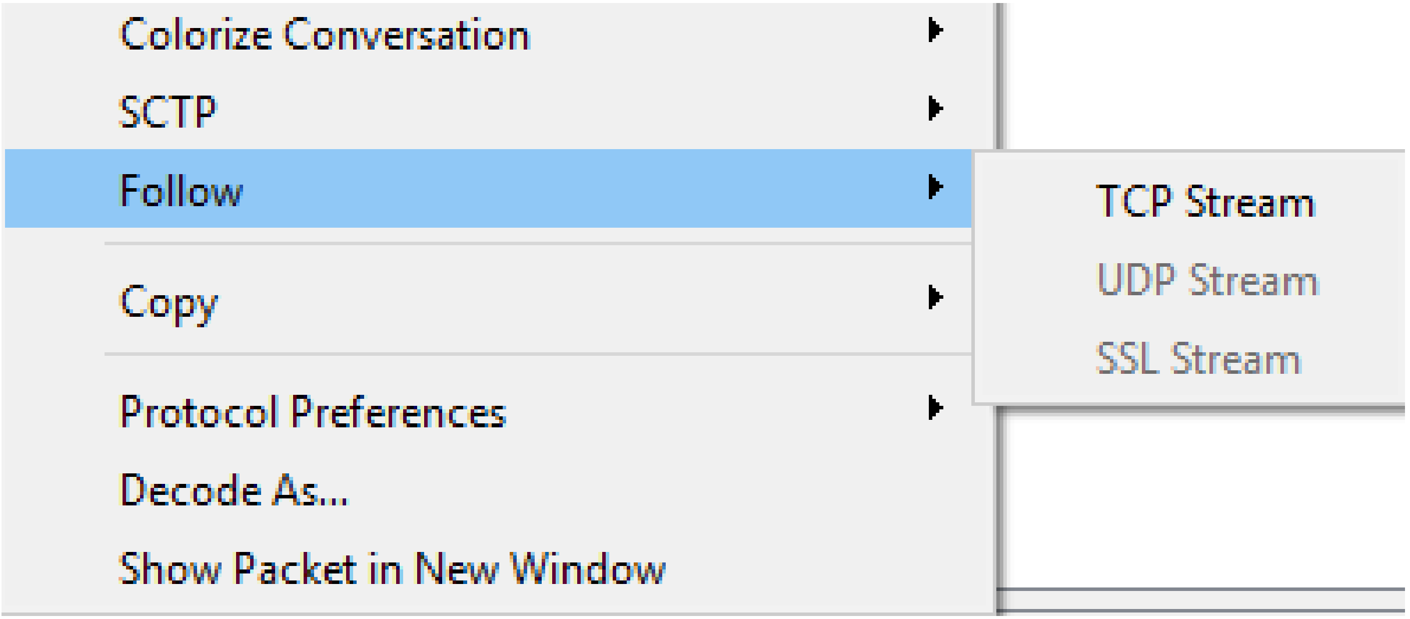


Displayed	Title	Type	Field Name	Field Occurrence
☑	No.	Number		
☑	Time	Time (format as specified)		
☑	Source	Source address		
☑	SrcMAC	Custom	eth.src	0
☑	Destination	Destination address		
☑	DstMAC	Custom	eth.dst	0
☑	Protocol	Protocol		
☑	Length	Packet length (bytes)		
☑	Info	Information		

Use built-in features

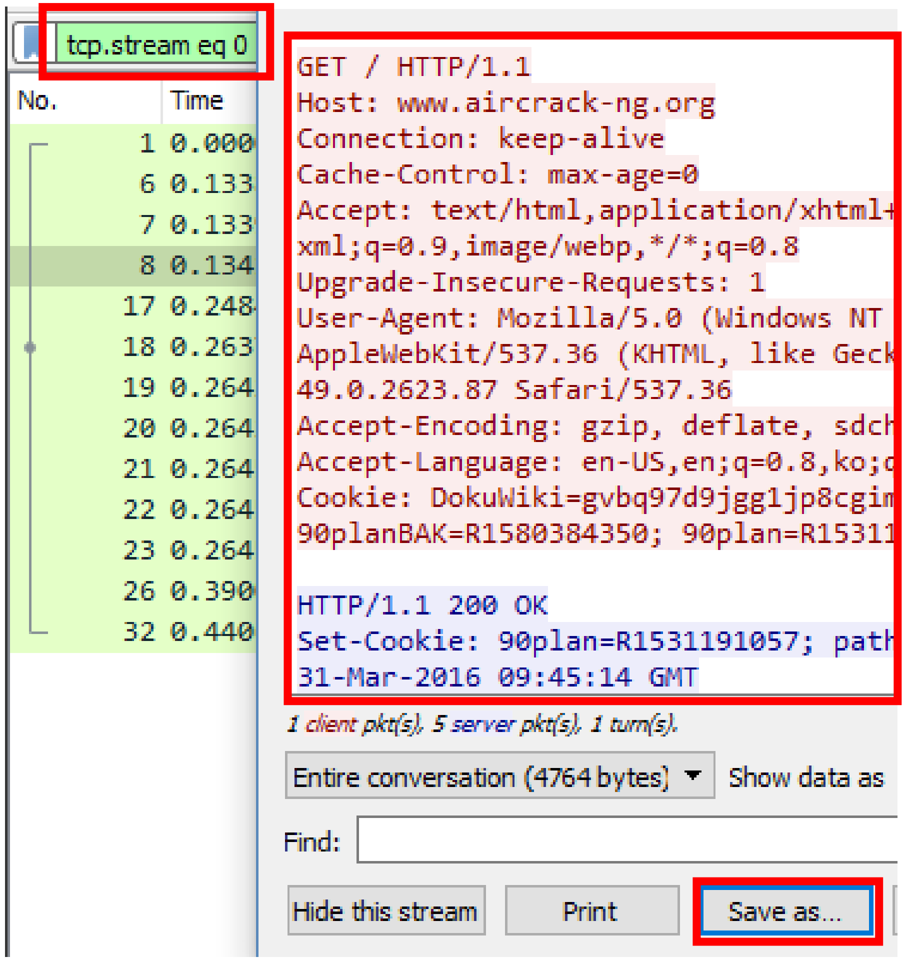
- Menu (e.g. Statistics)
- Packet/Packet Details Right-click menu (e.g. Follow TCP Stream)





Ex) Follow TCP Stream

- Shows all packets in the same TCP stream: tcp.stream eq x
- Opens a new window that shows contents of all packets in readable format
- Option to save to a file



tcp.stream eq 0

```
No.   Time
  1 0.000
  6 0.133
  7 0.133
  8 0.134
 17 0.248
 18 0.263
 19 0.264
 20 0.264
 21 0.264
 22 0.264
 23 0.264
 26 0.390
 32 0.440
```

```
GET / HTTP/1.1
Host: www.aircrack-ng.org
Connection: keep-alive
Cache-Control: max-age=0
Accept: text/html,application/xhtml+
xml;q=0.9,image/webp,*/*;q=0.8
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT
AppleWebKit/537.36 (KHTML, like Geck
49.0.2623.87 Safari/537.36
Accept-Encoding: gzip, deflate, sdch
Accept-Language: en-US,en;q=0.8,ko;q
Cookie: DokuWiki=gvbq97d9jgg1jp8cgim
90planBAK=R1580384350; 90plan=R15311

HTTP/1.1 200 OK
Set-Cookie: 90plan=R1531191057; path
31-Mar-2016 09:45:14 GMT
```

1 client pkt(s), 5 server pkt(s), 1 turn(s).

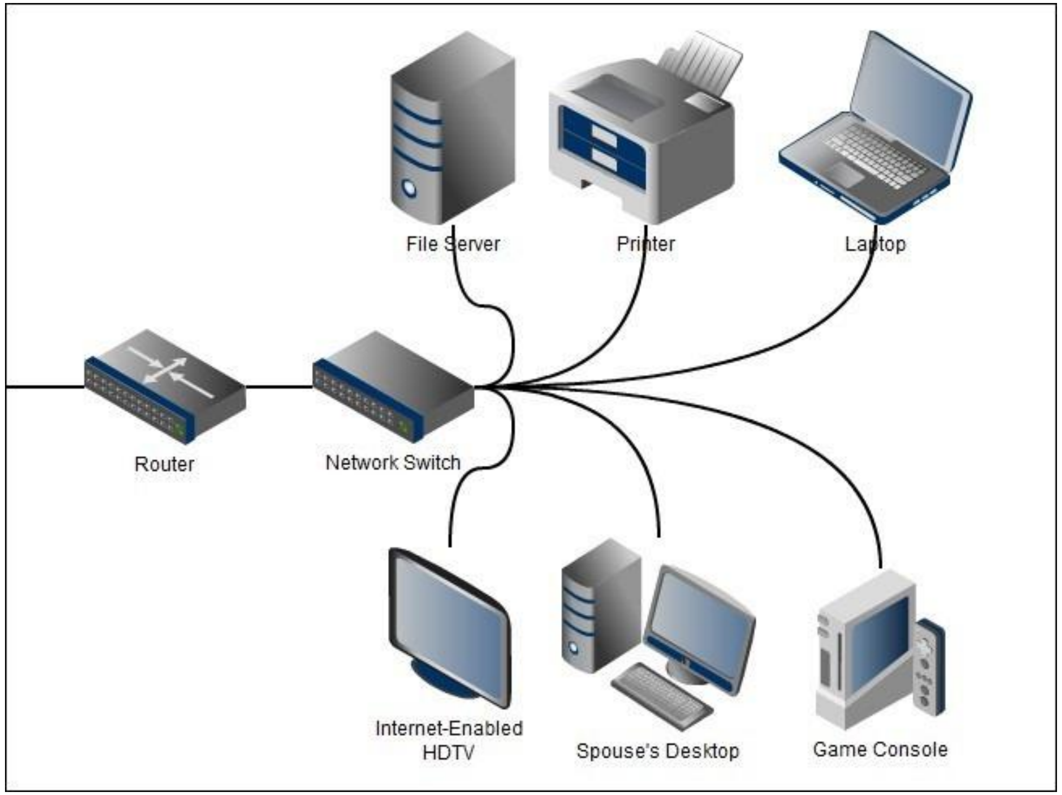
Entire conversation (4764 bytes)

Checkpoint 1: Identify network activities

- What is a gateway?
- Active vs. Passive FTP
- HTTPS connections

What is a gateway?

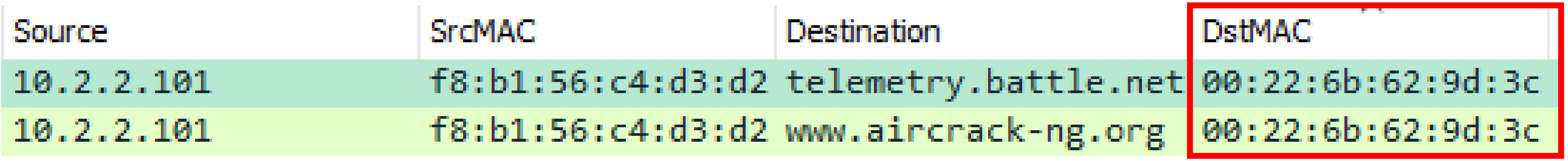
- “A default gateway … [forwards] packets on to other networks. … The gateway is by definition a router.” (https://en.wikipedia.org/wiki/Default_gateway)
- “A router is a networking device that forwards data packets between computer networks.” (https://en.wikipedia.org/wiki/Router_(computing))



Source: http://www.howtogeek.com/wp-content/uploads/2011/11/2011-11-29_132204.jpg

How to identify a gateway

- All traffics have to go through the network’s gateway.
- Look at the packets between a local host and a number of different external hosts (e.g. websites).
  Check the MAC addresses of the external hosts. Are they different?
- See what other IP addresses are mapped with that MAC address.



Source	SrcMAC	Destination	DstMAC
10.2.2.101	f8:b1:56:c4:d3:d2	telemetry.battle.net	00:22:6b:62:9d:3c
10.2.2.101	f8:b1:56:c4:d3:d2	www.aircrack-ng.org	00:22:6b:62:9d:3c

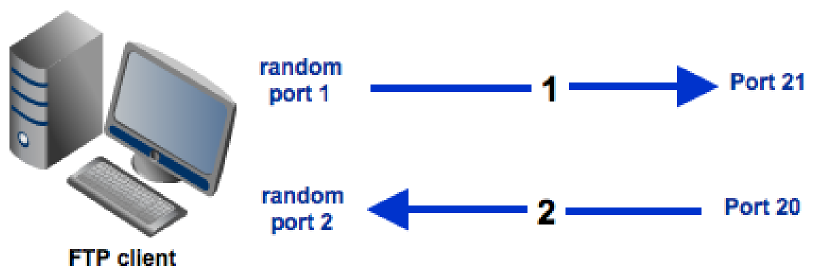
Sidenote: IP-MAC address mapping

- Not necessarily 1:1 mapping.
- 1 MAC address can be mapped to multiple IP addresses, as shown in the previous slide.
- 1 IP address can be mapped to multiple MAC addresses (e.g. IP spoofing).
- How to see the complete mapping:
  - Filter by source/destination MAC address
  - Sort on IP address
  - Or use tshark: https://ask.wireshark.org/questions/27577/how-to-see-ip-to-macmapping-from-a-trace

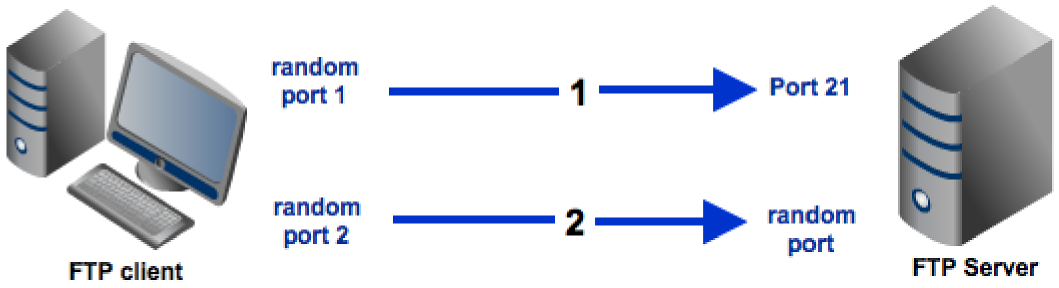
Sidenote: Name Resolution

- View > Name Resolution > Resolve Physical/Network/Transport Address
- Wireshark converts numerical addresses into (more) human readable formats. (https://www.wireshark.org/docs/wsug_html_chunked/ChAdvNameResolutionSection.html)
- While useful, the conversion often fails and may give you wrong information (e.g. wrong hostname).
- Try “Resolve Network Address” on 4.1.1.pcap. Try it on IllinoisNet, then try again on different network (e.g. home).

Active vs. Passive FTP



Active FTP



Passive FTP

- Explanation: http://www.jscape.com/blog/bid/80512/Active-v-s-Passive-FTP-Simplified
- With FTP session examples: http://slacksite.com/other/ftp.html

HTTPS connections

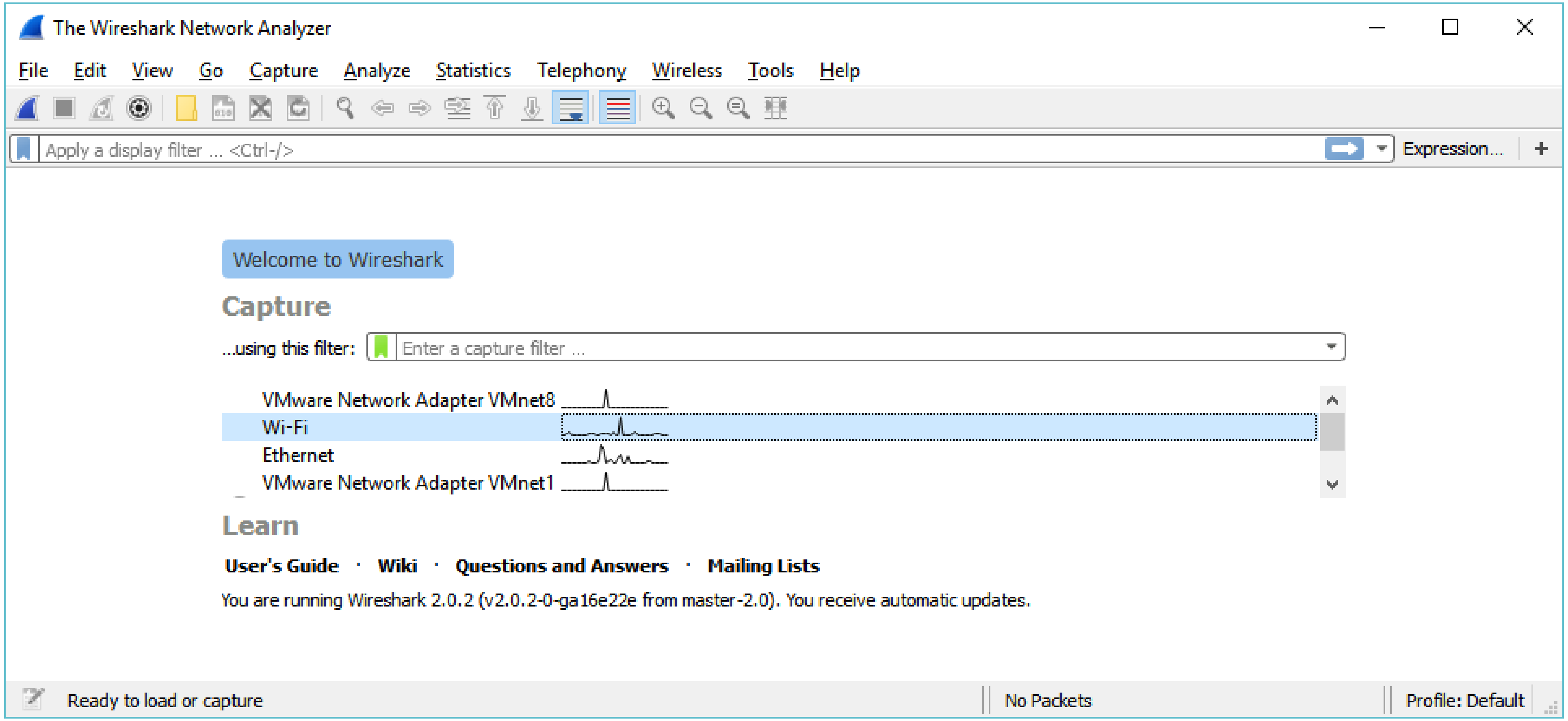
- TLS Handshake (https://courses.engr.illinois.edu/cs461/secure/ECE422-Spring2016-Lecture-13-TLS.pdf)
- The First Few Milliseconds of an HTTPS Connection (http://www.moserware.com/2009/06/first-few-milliseconds-of-https.html)

Tips

- Try to understand the result shown by Wireshark and make sure it is as expected.
- Get familiar with filter syntax and take advantage of it. Expressions made of multiple filters will save you from tedious scrolling.
- Try capturing your own network traffic and analyze it.
- Don’t make assumptions and limit your search from the beginning. For example, an IP address not within the standard private network address space could still be a private IP address in the local network.

Capturing your own traffic

- Make sure you choose the correct network interface.



The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…
+
Welcome to Wireshark
Capture
…using this filter:
Enter a capture filter …
VMware Network Adapter VMnet8
Wi-Fi
Ethernet
VMware Network Adapter VMnet1
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists

You are running Wireshark 2.0.2 (v2.0.2-0-ga16e22e from master-2.0). You receive automatic updates.

Ready to load or capture

No Packets

Profile: Default