MP4.1 Networking

ECE 422/CS 461

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 (either 32 bit or 64 bit version)

Checkpoint 2

- Wireshark (**32 bit**)
- Aircrack-ng Suite
- Nmap
- Python 2.7
- dpkt Python library

Objective

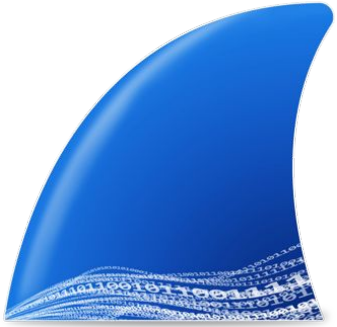
Learn how to use Wireshark

- Packets details
- Filters
- Built-in features

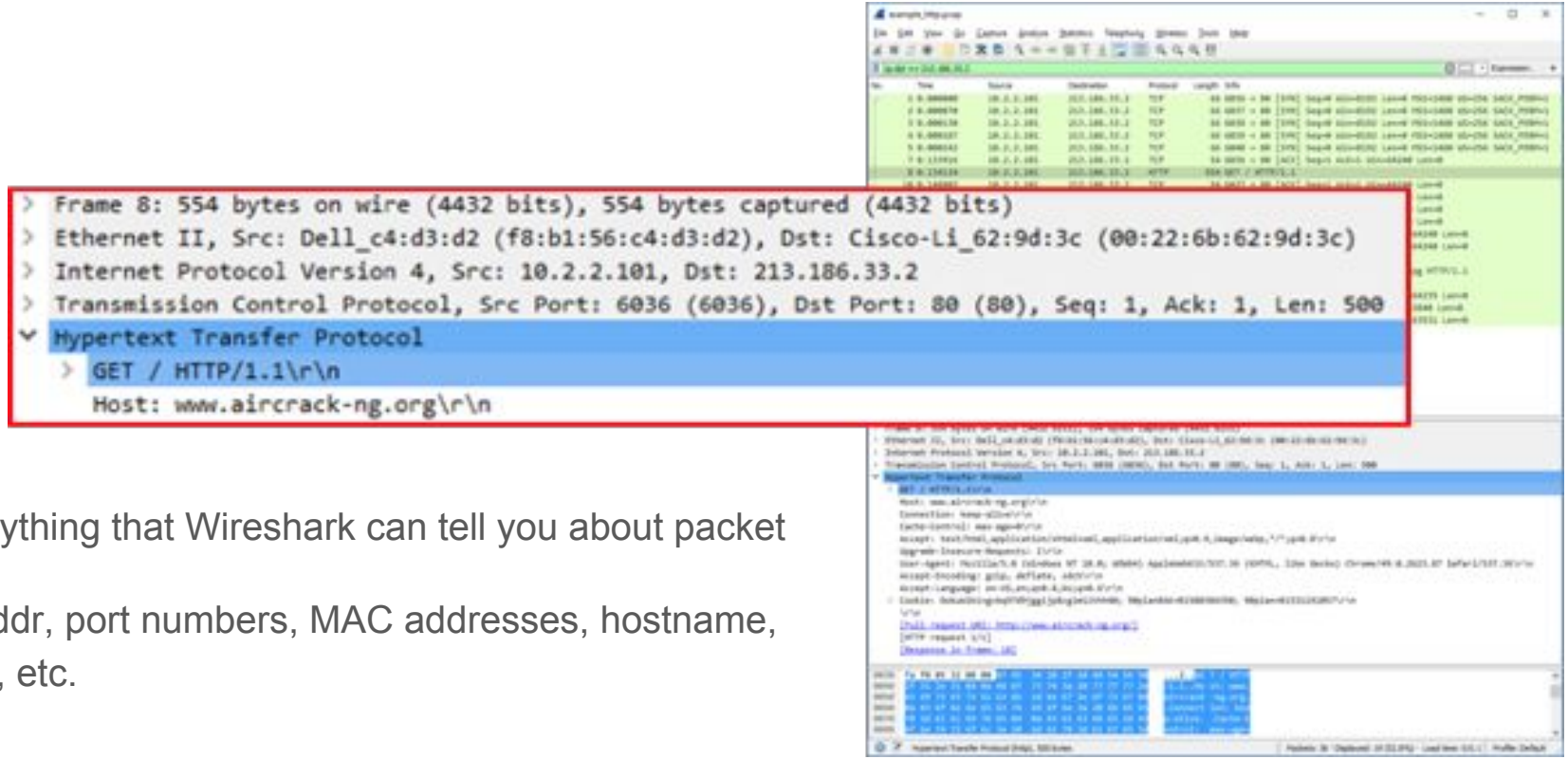
Identify network activities

- Gateway
- Active vs. passive FTP
- HTTPS connection

Wireshark



Digging through “packet details”



Everything that Wireshark can tell you about packet

IP addr, port numbers, MAC addresses, hostname, data, etc.

Display Filters

Apply a display filter ... <⌘/> Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
121	0.195554	10.183.158.36	10.183.158.4	FTP-D…	128	FTP Data: 62 bytes
122	0.195559	10.183.158.4	10.183.158.36	TCP	66	36328 → 10895 [ACK] Seq=1 Ack=63 Win=29312 Len=0 TSval=316609339 TSecr=3166093
123	0.195569	10.183.158.36	10.183.158.4	TCP	66	10895 → 36328 [FIN, ACK] Seq=63 Ack=1 Win=29056 Len=0 TSval=316609339 TSecr=31
124	0.195666	10.183.158.4	10.183.158.36	TCP	66	36328 → 10895 [FIN, ACK] Seq=1 Ack=64 Win=29312 Len=0 TSval=316609339 TSecr=31
125	0.195736	10.183.158.36	10.183.158.4	TCP	66	10895 → 36328 [ACK] Seq=64 Ack=2 Win=29056 Len=0 TSval=316609339 TSecr=3166093
126	0.195789	10.183.158.36	10.183.158.4	FTP	90	Response: 226 Transfer complete.
127	0.195861	10.183.158.4	10.183.158.36	TCP	66	46540 → 21 [ACK] Seq=85 Ack=289 Win=29312 Len=0 TSval=316609339 TSecr=31660933
128	0.195916	10.183.158.4	10.183.158.36	TCP	66	46540 → 21 [FIN, ACK] Seq=85 Ack=289 Win=29312 Len=0 TSval=316609339 TSecr=316
129	0.195942	10.183.158.36	10.183.158.4	TCP	66	21 → 46540 [FIN, ACK] Seq=289 Ack=86 Win=29056 Len=0 TSval=316609339 TSecr=316
130	0.195953	10.183.158.4	10.183.158.36	TCP	66	46540 → 21 [ACK] Seq=86 Ack=290 Win=29312 Len=0 TSval=316609339 TSecr=31660933
131	0.682124	10.183.158.23				
132	0.682141	10.183.158.68				
133	0.682154	10.183.158.23				
134	0.682159	10.183.158.68				
135	0.682168	10.183.158.23				
136	0.682173	10.183.158.68				
137	0.682181	10.183.158.23				
138	0.682185	10.183.158.68				
139	0.682193	10.183.158.23				
140	0.682197	10.183.158.68				
141	0.682204	10.183.158.23				

tcp Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
110	0.194500	10.183.158.4	10.183.158.36	FTP	74	Request: TYPE I
111	0.194578	10.183.158.36	10.183.158.4	FTP	97	Response: 200 Switching to Binary mode.
112	0.194634	10.183.158.4	10.183.158.36	FTP	81	Request: SIZE flag.txt
113	0.194715	10.183.158.36	10.183.158.4	FTP	74	Response: 213 62
114	0.194777	10.183.158.4	10.183.158.36	FTP	72	Request: PASV
115	0.195022	10.183.158.36	10.183.158.4	FTP	117	Response: 227 Entering Passive Mode (10,183,158,36,42,143).
116	0.195090	10.183.158.4	10.183.158.36	TCP	74	36328 → 10895 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=316609339
117	0.195103	10.183.158.36	10.183.158.4	TCP	74	10895 → 36328 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSva
118	0.195112	10.183.158.4	10.183.158.36	TCP	66	36328 → 10895 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=316609339 TSecr=31660933
119	0.195125	10.183.158.4	10.183.158.36	FTP	81	Request: RETR flag.txt
120	0.195512	10.183.158.36	10.183.158.4	FTP	132	Response: 150 Opening BINARY mode data connection for flag.txt (62 bytes).
121	0.195554	10.183.158.36	10.183.158.4	FTP-D…	128	FTP Data: 62 bytes
122	0.195559	10.183.158.4	10.183.158.36	TCP	66	36328 → 10895 [ACK] Seq=1 Ack=63 Win=29312 Len=0 TSval=316609339 TSecr=3166093
123	0.195569	10.183.158.36	10.183.158.4	TCP	66	10895 → 36328 [FIN, ACK] Seq=63 Ack=1 Win=29056 Len=0 TSval=316609339 TSecr=31
124	0.195666	10.183.158.4	10.183.158.36	TCP	66	36328 → 10895 [FIN, ACK] Seq=1 Ack=64 Win=29312 Len=0 TSval=316609339 TSecr=31
125	0.195736	10.183.158.36	10.183.158.4	TCP	66	10895 → 36328 [ACK] Seq=64 Ack=2 Win=29056 Len=0 TSval=316609339 TSecr=3166093
126	0.195789	10.183.158.36	10.183.158.4	FTP	90	Response: 226 Transfer complete.
127	0.195861	10.183.158.4	10.183.158.36	TCP	66	46540 → 21 [ACK] Seq=85 Ack=289 Win=29312 Len=0 TSval=316609339 TSecr=31660933
128	0.195916	10.183.158.4	10.183.158.36	TCP	66	46540 → 21 [FIN, ACK] Seq=85 Ack=289 Win=29312 Len=0 TSval=316609339 TSecr=316
129	0.195942	10.183.158.36	10.183.158.4	TCP	66	21 → 46540 [FIN, ACK] Seq=289 Ack=86 Win=29056 Len=0 TSval=316609339 TSecr=316
130	0.195953	10.183.158.4	10.183.158.36	TCP	66	46540 → 21 [ACK] Seq=86 Ack=290 Win=29312 Len=0 TSval=316609339 TSecr=31660933

Display Filters

Shows packets that contain the information you are interested in

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/

What if you want to see MAC addresses of all packets instead of filtering by specific one?

Custom Columns

No.	Time	Source	Destination	Length	Protocol
23	1.801809	10.2.2.101	68.180.77.151	55	SSL
24	1.806705	68.180.77.151	10.2.2.101	66	TCP
25	2.109691	00:22:6b:62:9d:3c	ff:ff:ff:ff:ff:ff	60	ARP

No.	Time	Source	Destination	SrcMAC	DstMAC	Length	Protocol
23	1.801809	10.2.2.101	68.180.77.151	f8:b1:56:c4:d3:d2	00:22:6b:62:9d:3c	55	SSL
24	1.806705	68.180.77.151	10.2.2.101	00:22:6b:62:9d:3c	f8:b1:56:c4:d3:d2	66	TCP
25	2.109691	00:22:6b:62:9d:3c	ff:ff:ff:ff:ff:ff	00:22:6b:62:9d:3c	ff:ff:ff:ff:ff:ff	60	ARP

Custom Columns

Right-click column header > Column preferences

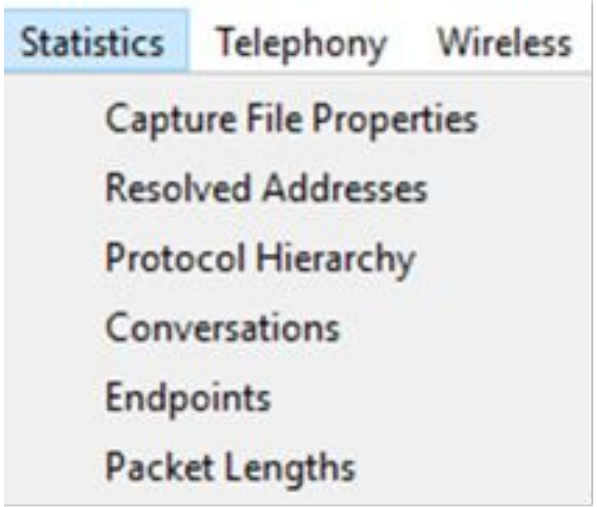
or Edit > Preferences > Appearance: Columns

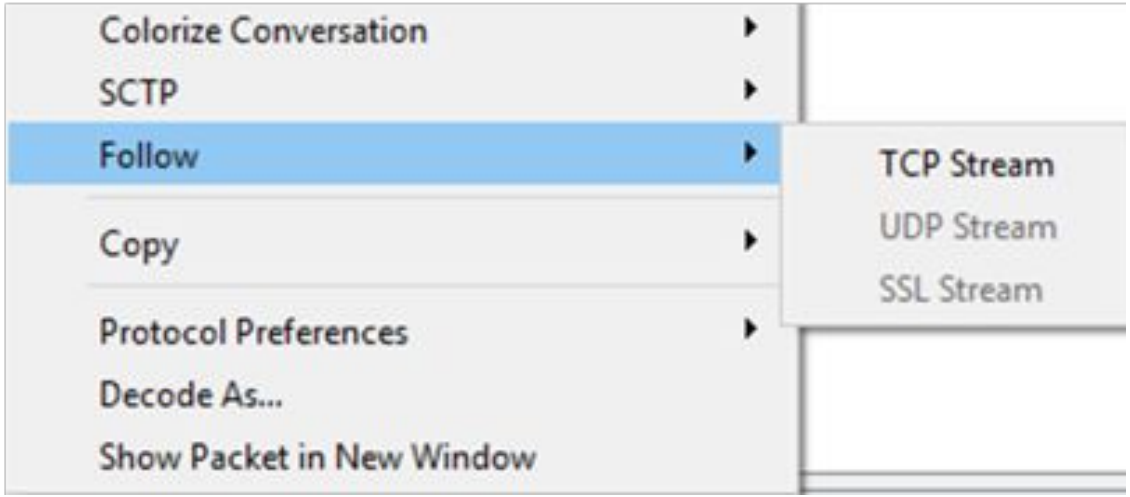
Displayed	Title	Type	Field Name	Field Occurrence
☑	No.	Number		
☑	Time	Time (format as specified)		
☑	Source	Source address		
☑	SrcMAC	Custom	eth.src	0
☑	Destination	Destination address		
☑	DstMAC	Custom	eth.dst	0
☑	Protocol	Protocol		
☑	Length	Packet length (bytes)		
☑	Info	Information		

Built-in Features

Menu (e.g. Statistics)

Packets/Packet details (e.g. Follow TCP stream)





Ex) Follow TCP Stream

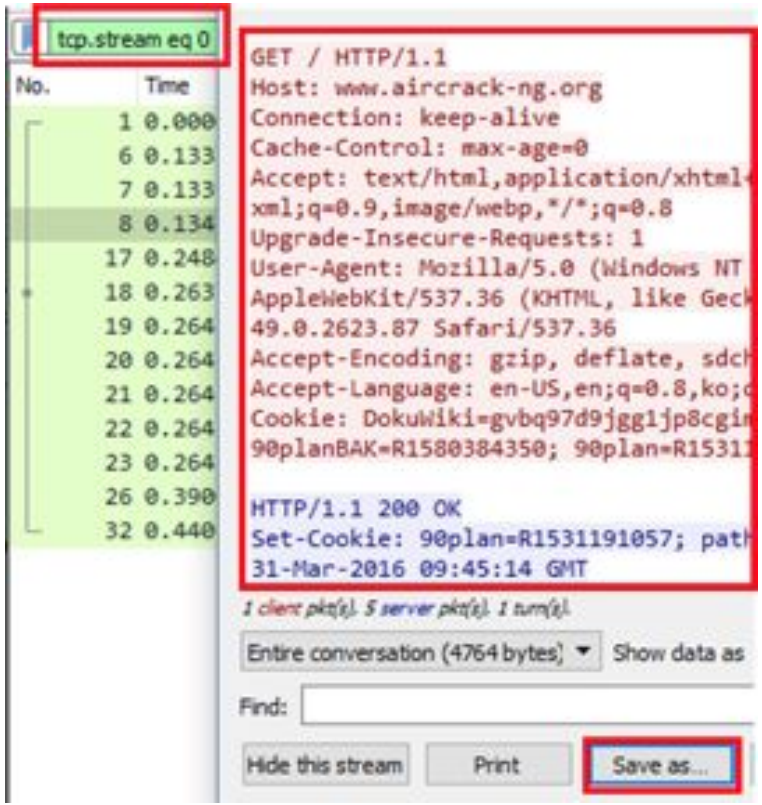
Shows all packets in the same TCP stream tcp.stream eq x

Opens a new window that shows content of all relevant packets in readable format

Option to save a file

What information does Wireshark use to detect different conversations?

- IP address, port, sequence number



Built-in Features - 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)

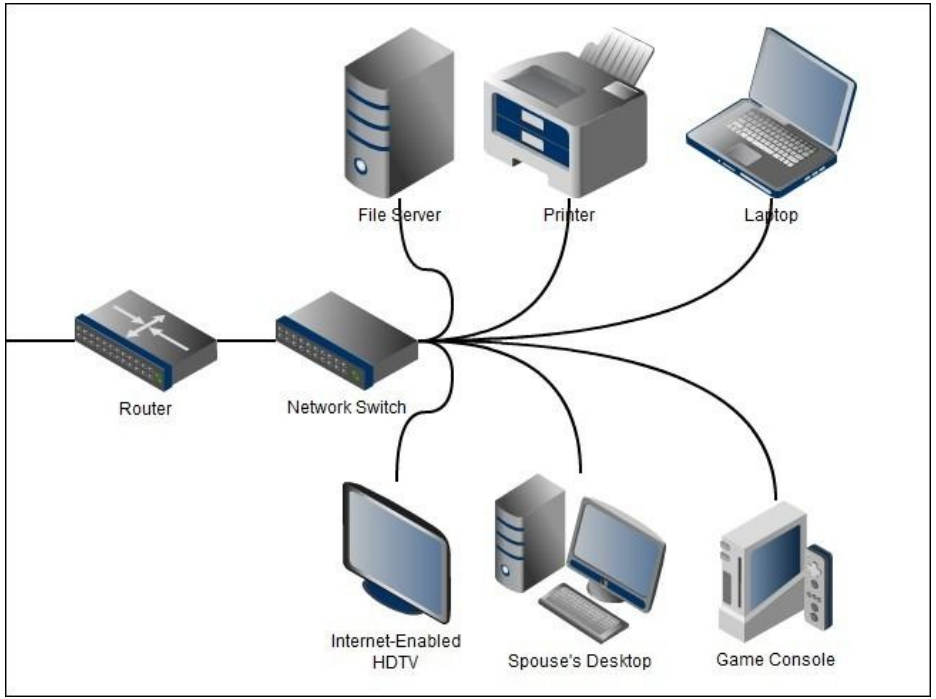
Try “Resolve Network Address” on 4.1.1.pcap. Try it on IllinoisNet. Try it at home.

Common Network Activities

Gateway

A default gateway… [forwards] packets on to other networks… The gateway is by definition a router.

A router is a networking device that forwards data packets between computer networks.



https://en.wikipedia.org/wiki/Default_gateway
https://en.wikipedia.org/wiki/Router_(computing)

Identifying a gateway

Assumption: all external traffic goes 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 to 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

Why is MAC addr. not used to detect TCP streams?

IP-to-MAC not necessarily a 1:1 mapping

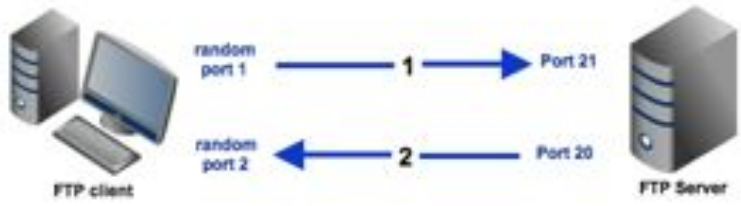
1 MAC address can be mapped to multiple IP addresses (like in previous slide)

1 IP address can be mapped to multiple MAC addresses (e.g. IP spoofing)

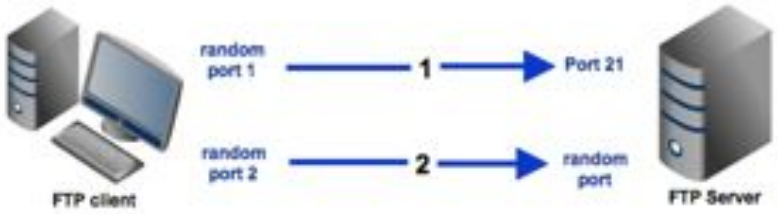
How to see the complete mapping?

- Filter by source/destination MAC address
- Sort on IP address

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

- Client sends a Client Hello offers a list of Cipher Suites
- Server responds with Server Hello that contains chosen Cipher Suite

The first few milliseconds of an HTTPS connections (http://www.moserware.com/2009/06/first-few-milliseconds-of-https.html)

Tips

Start focusing on one conversation.

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.

Reminders

Do NOT use lab computers, for your own good

Please read the Checkpoint 2 setup and start setting up your environment as soon as possible

- Some parts are easier when there are less people working on them at the same time