WIRESHARK

CPSC 441 - Winter 2020
University of Calgary

Sina Keshvadi

In this presentation, I used slides from **Reza Gholizadeh** and Prof. **Mea Wang**.

What is Wireshark?

UNIVERSITY OF CALGARY

- **Wireshark is an open source packet analyzer**
  - Runs in Linux, Mac and Windows
  - Free of cost

- It is used for network troubleshooting, analysis, software and communication protocol development, and education.

- It is installed in lab machines, but need root access for full features

Wireshark Installation

UNIVERSITY OF CALGARY

- Unix System:
  - sudo apt-get install wireshark
- Windows:
  - http://www.wireshark.org/download.html
  - Tutorial in next slide

UNIVERSITY OF CALGARY

tshark

UNIVERSITY OF CALGARY

- Terminal version of Wireshark
- Typically used when interactive user interface is not available

Install on Unix Machines by:

- sudo apt-get install tshark

BEFORE CAPTURING

UNIVERSITY OF CALGARY

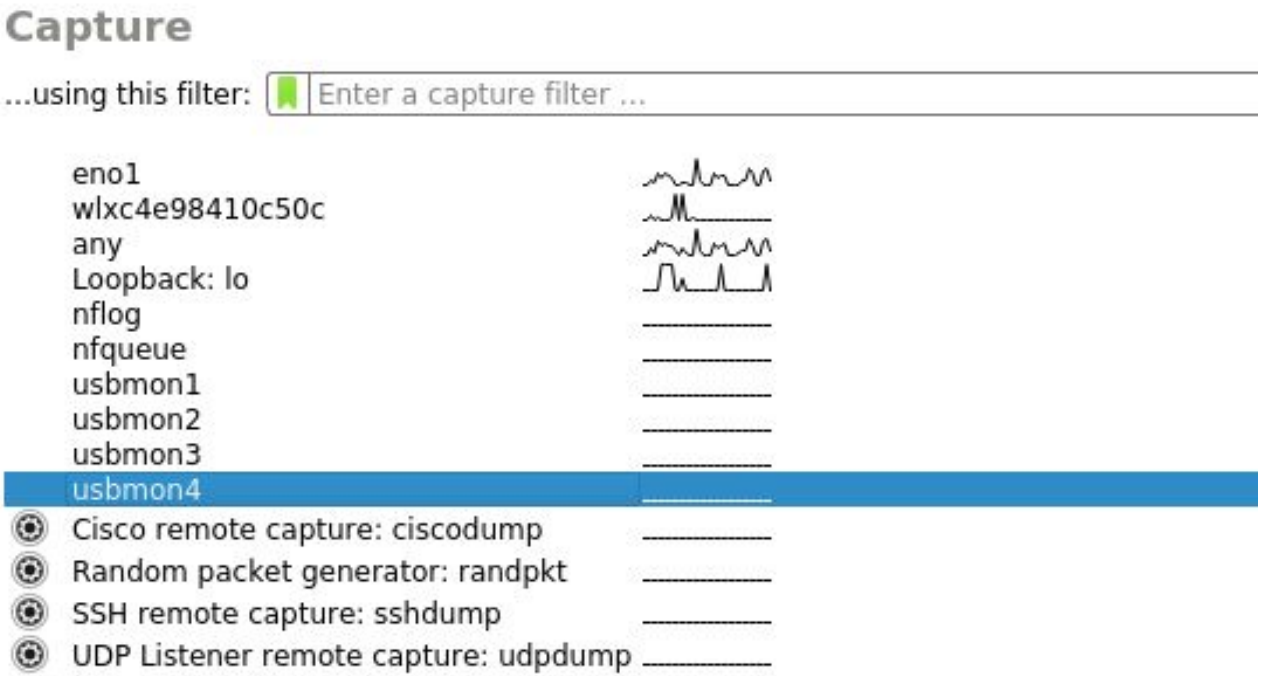
Are you allowed to do this?

- Ensure that you have permission to capture packets from the network you are connected with
- Corporate policies or applicable laws may prohibit capturing data from the network

General Setup

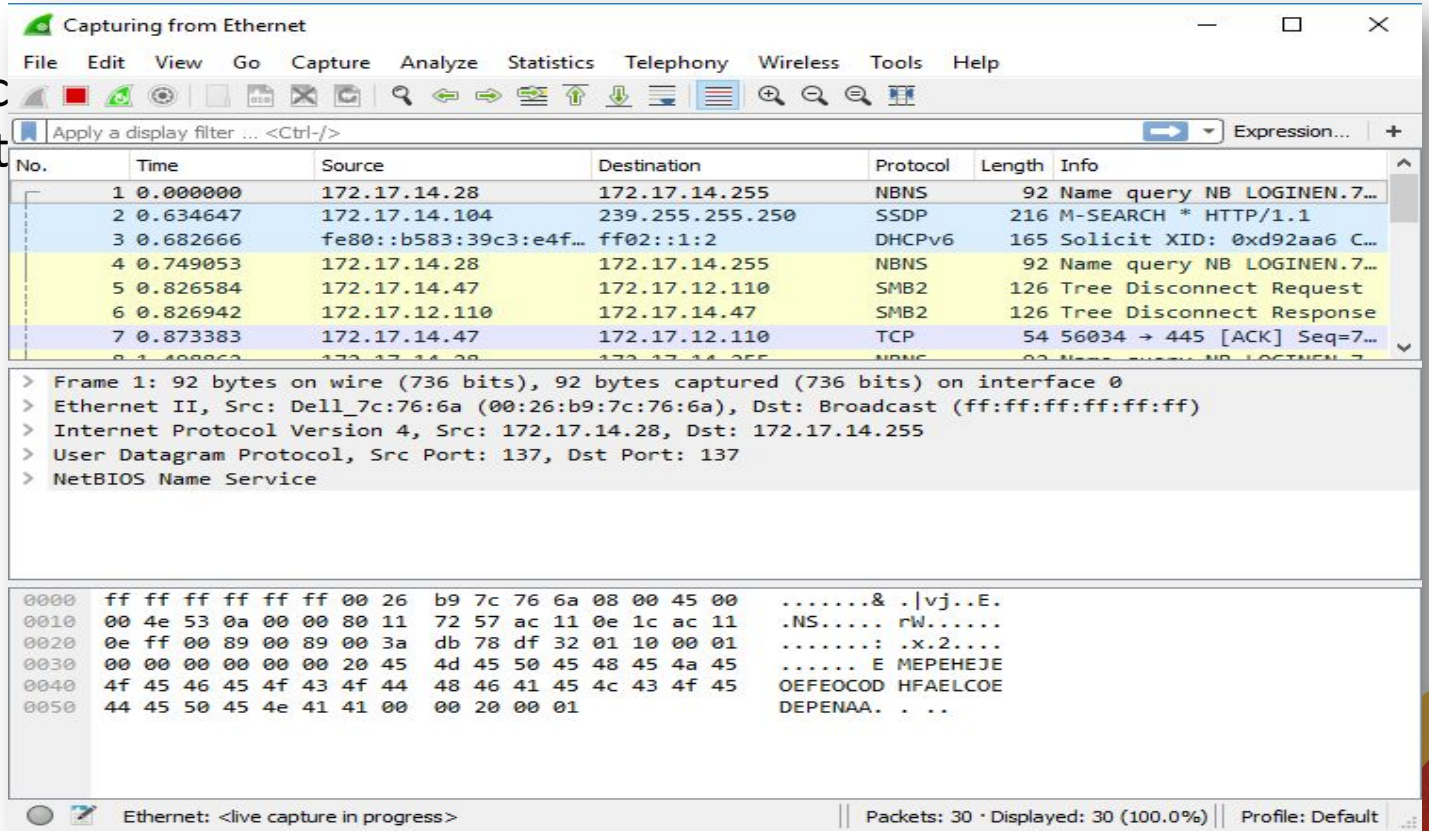
- Operating system must support packet capturing, e.g. capture support is enabled
- You must have sufficient privileges to capture packets, e.g. root / administrator privileges
- Your computer's time and time zone settings should be correct

Choosing the Network Interface



START CAPTURING PACKETS

After c
packet



ANALYZE CAPTURED PACKETS

UNIVERSITY OF CALGARY

Download the sample packet trace from my webpage and we will analyze that traffic.

https://pages.cpsc.ucalgary.ca/~sina.keshvadi1/cpsc441/

Capture Traffic

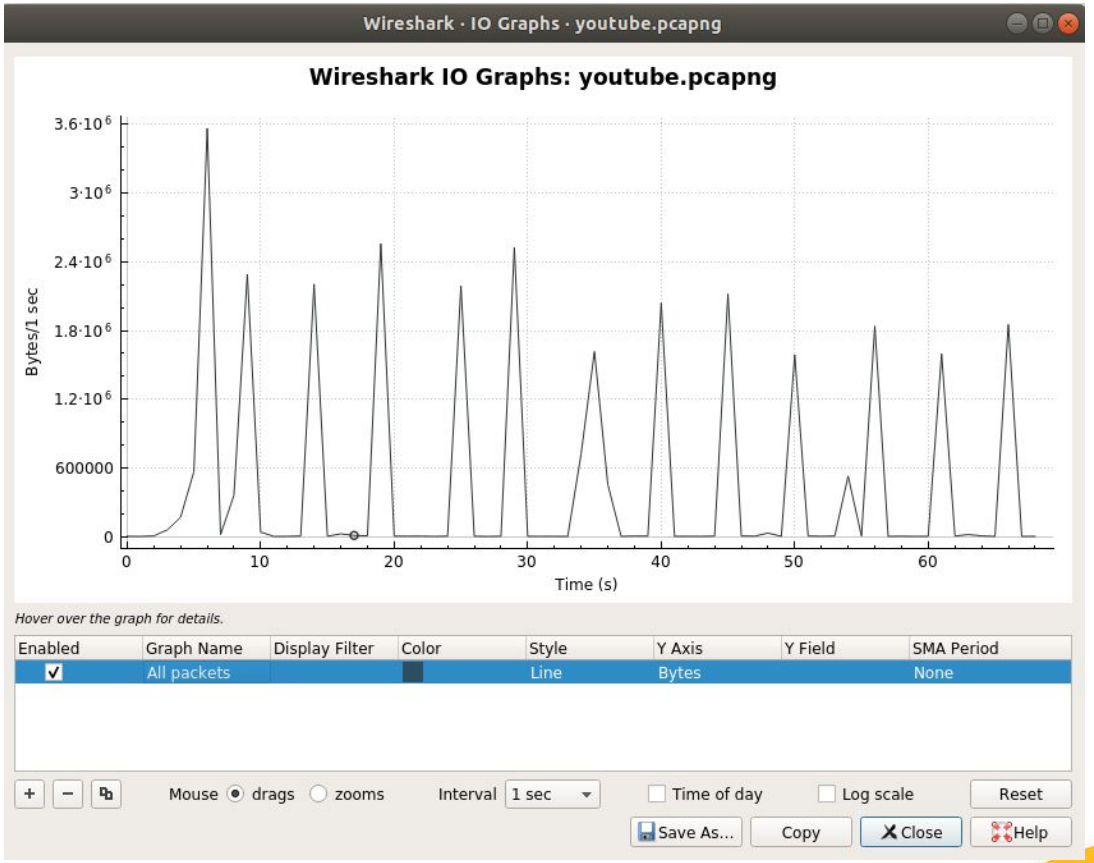
- From TED.Com
- From YouTube.com

Analyze Traffic

UNIVERSITY OF CALGARY

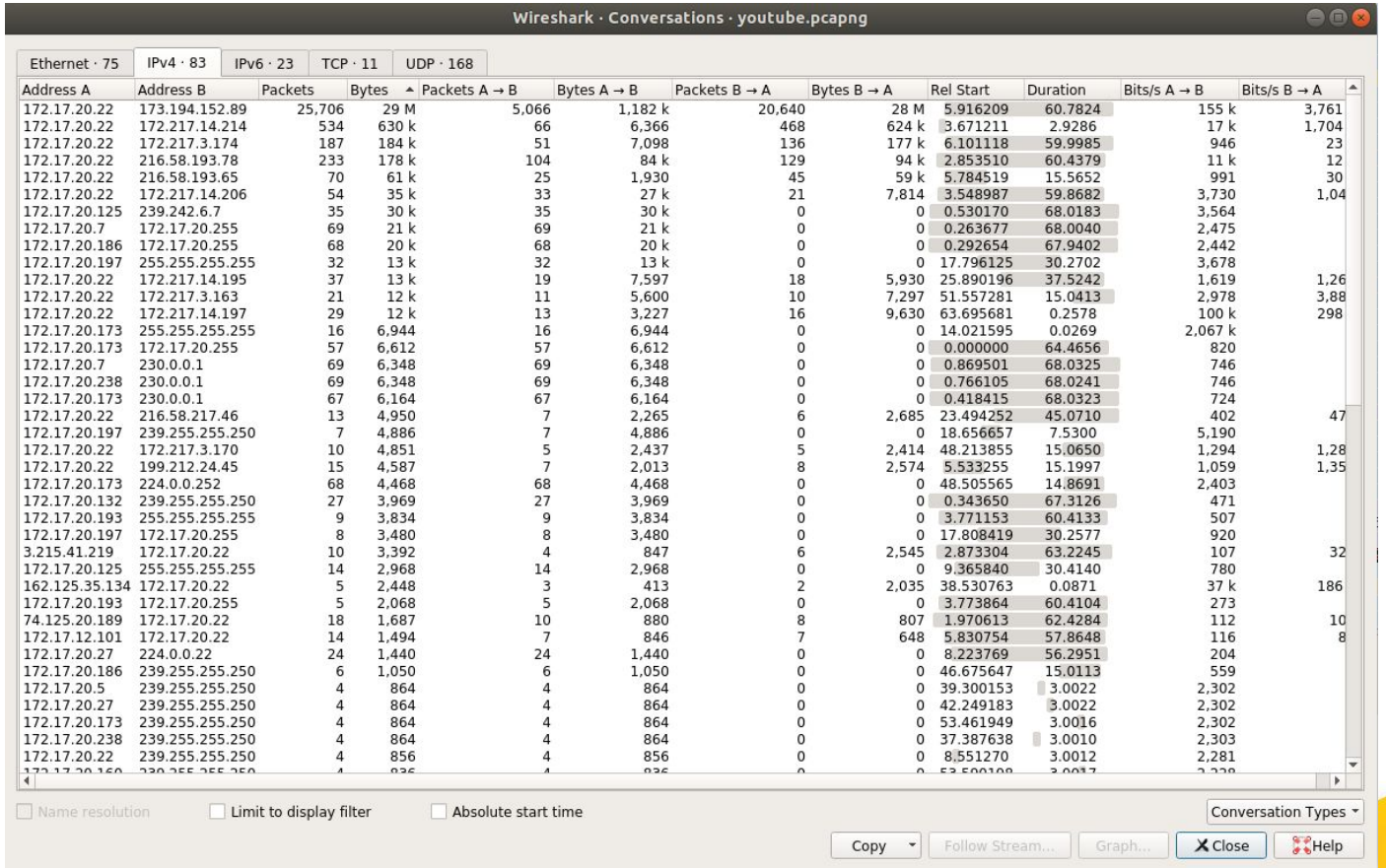
- Statistics -> I/O Graph
- Statistics -> Conversations
- Apply as Filters
- Follow -> TCP Stream
- Colors in Wireshark
- Packet Details

Statistics -> I/O Graph



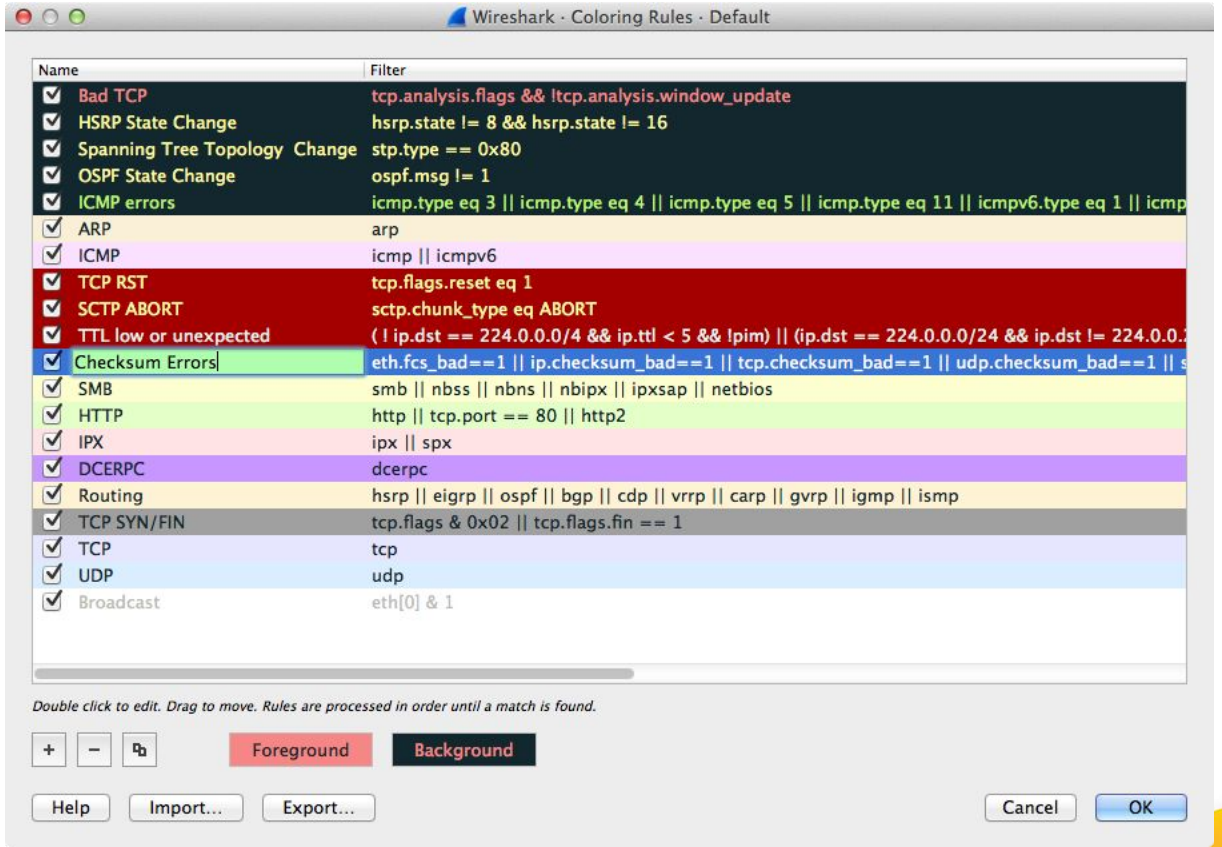
Statistics -> Conversations

UNIVERSITY OF CALGARY

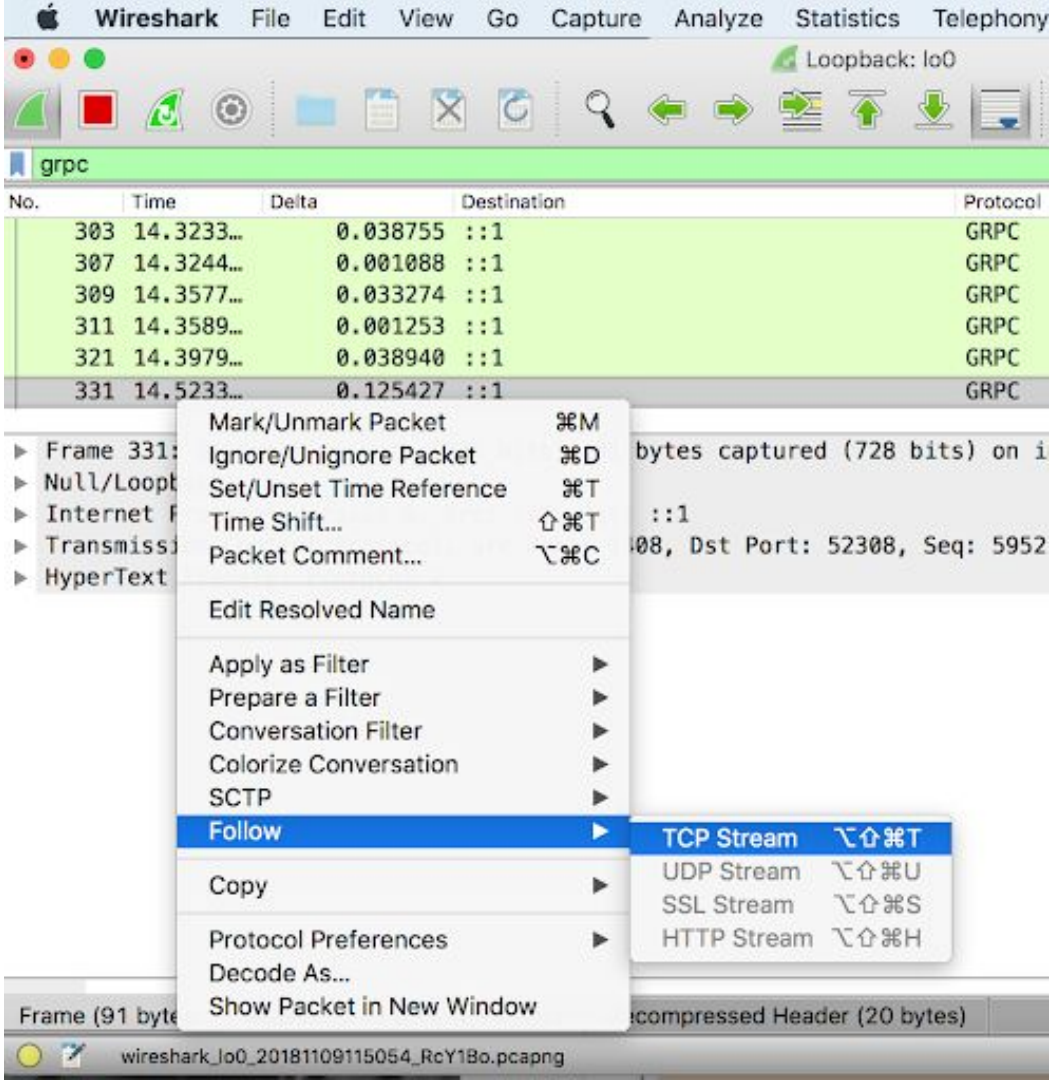


Wireshark Coloring Rules

UNIVERSITY OF CALGARY

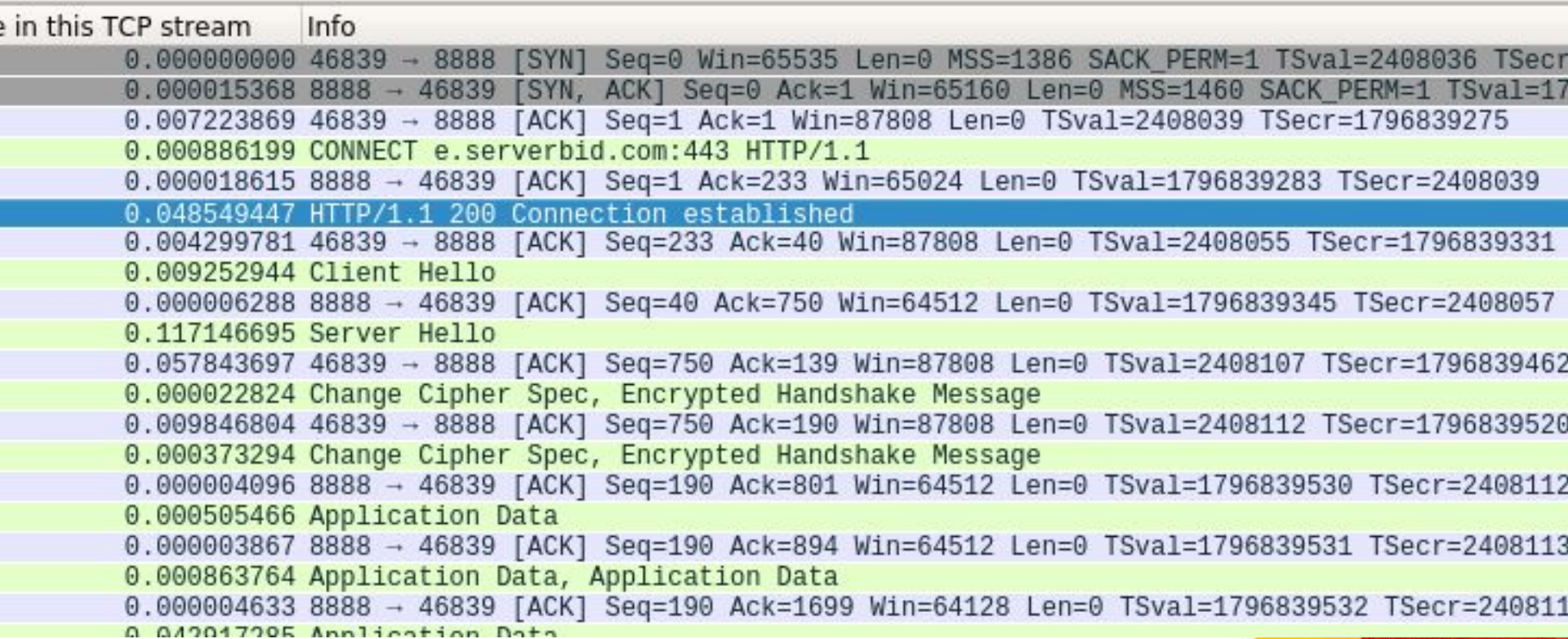


Follow a TCP stream



Handshaking in a TCP stream

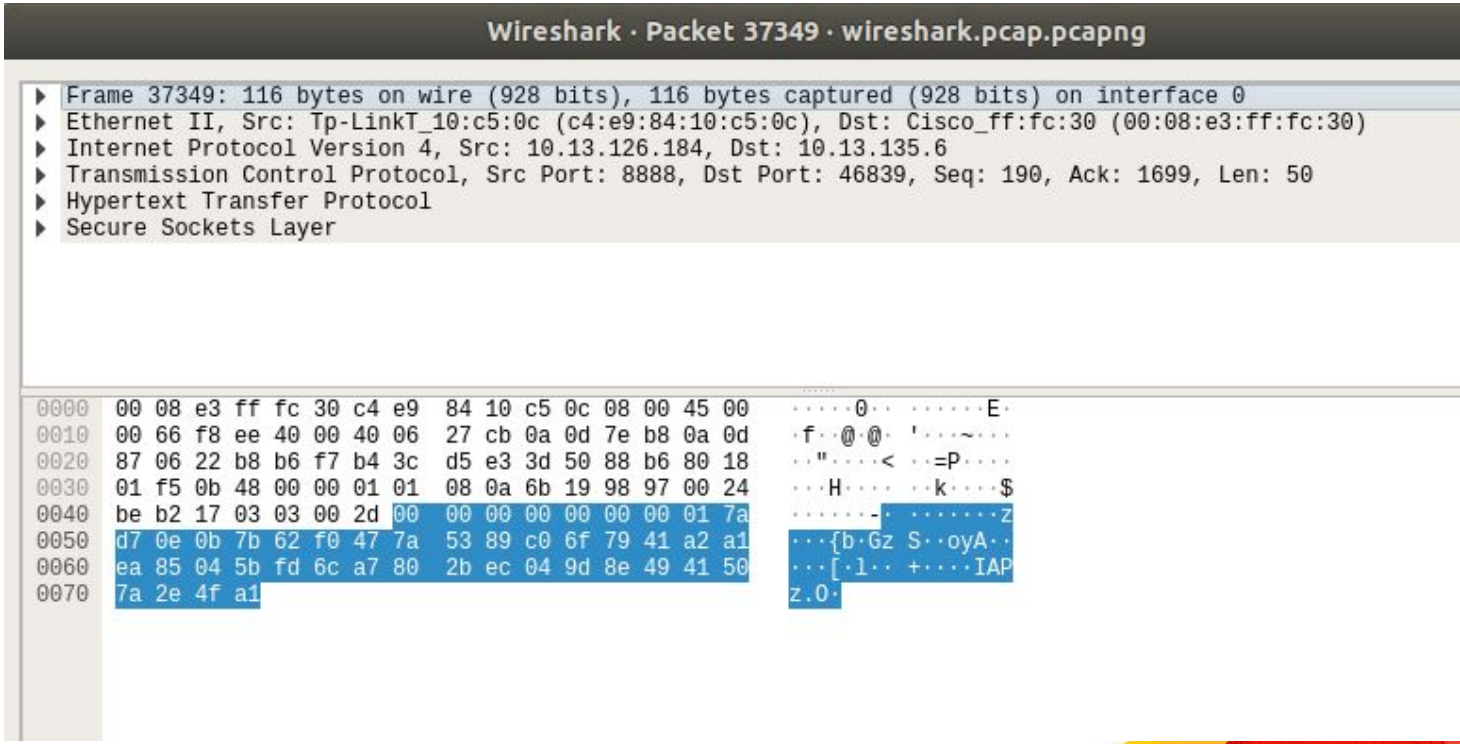
UNIVERSITY OF CALGARY



e in this TCP stream	Info
0.000000000	46839 → 8888 [SYN] Seq=0 Win=65535 Len=0 MSS=1386 SACK_PERM=1 TSval=2408036 TSecr
0.000015368	8888 → 46839 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=17
0.007223869	46839 → 8888 [ACK] Seq=1 Ack=1 Win=87808 Len=0 TSval=2408039 TSecr=1796839275
0.000886199	CONNECT e.serverbid.com:443 HTTP/1.1
0.000018615	8888 → 46839 [ACK] Seq=1 Ack=233 Win=65024 Len=0 TSval=1796839283 TSecr=2408039
0.048549447	HTTP/1.1 200 Connection established
0.004299781	46839 → 8888 [ACK] Seq=233 Ack=40 Win=87808 Len=0 TSval=2408055 TSecr=1796839331
0.009252944	Client Hello
0.000006288	8888 → 46839 [ACK] Seq=40 Ack=750 Win=64512 Len=0 TSval=1796839345 TSecr=2408057
0.117146695	Server Hello
0.057843697	46839 → 8888 [ACK] Seq=750 Ack=139 Win=87808 Len=0 TSval=2408107 TSecr=1796839462
0.000022824	Change Cipher Spec, Encrypted Handshake Message
0.009846804	46839 → 8888 [ACK] Seq=750 Ack=190 Win=87808 Len=0 TSval=2408112 TSecr=1796839520
0.000373294	Change Cipher Spec, Encrypted Handshake Message
0.000004096	8888 → 46839 [ACK] Seq=190 Ack=801 Win=64512 Len=0 TSval=1796839530 TSecr=2408112
0.000505466	Application Data
0.000003867	8888 → 46839 [ACK] Seq=190 Ack=894 Win=64512 Len=0 TSval=1796839531 TSecr=2408113
0.000863764	Application Data, Application Data
0.000004633	8888 → 46839 [ACK] Seq=190 Ack=1699 Win=64128 Len=0 TSval=1796839532 TSecr=240811
0.042917285	Application Data

Packet in network layers

- Layers
  - Frame
  - Ethernet
  - IP
  - TCP



WIRESHARK FILTERS

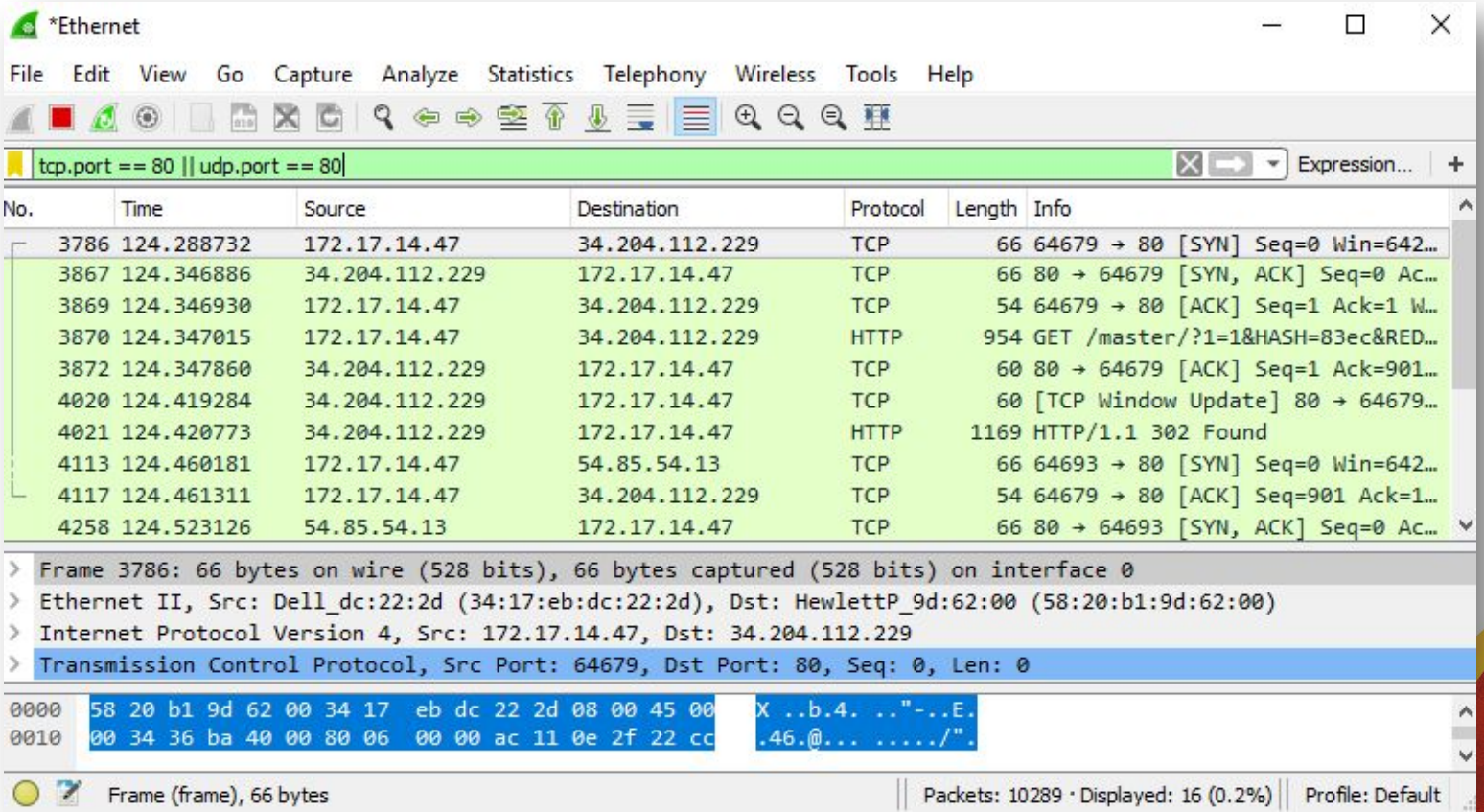
UNIVERSITY OF CALGARY

- Capture Filters
  - Removes unwanted packets from a packet trace and only retrieve the packets of interest

- Display Filters
  - Hides unwanted packets based on your filter definition

DISPLAY FILTER EXAMPLE

UNIVERSITY OF CALGARY

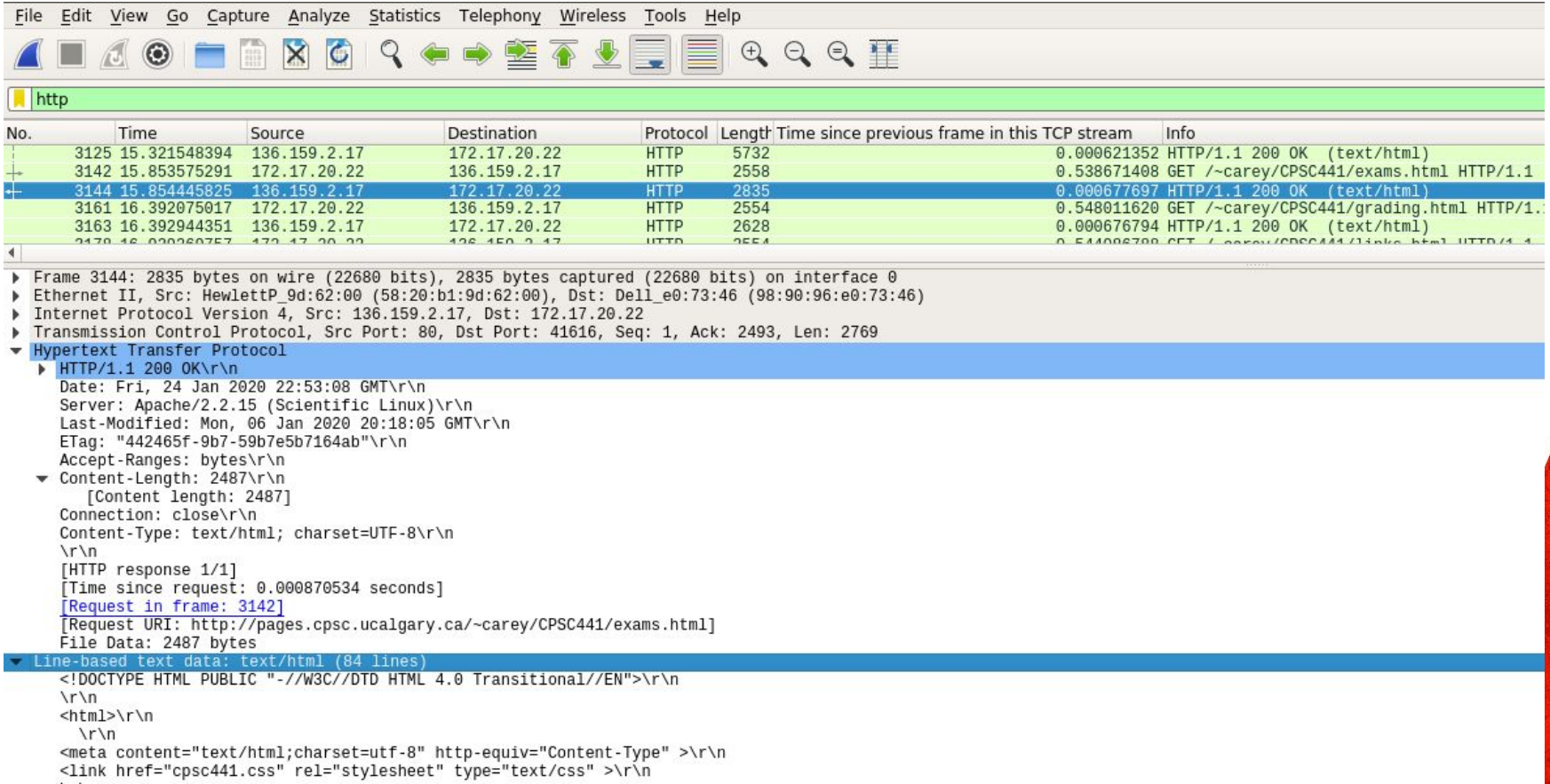


ANALYZE web.pcap file

- Write ***http*** as filter
- Find request to Prof. Carey's page
- Right click on it and then Follow → TCP Stream
  - Could you recognize handshaking?
  - SYN and ACK?
  - GET request?
  - Response?
  - Could you read the transferred data? Why?
  - ***Not Modified!*** What means?

ANALYZE A HTTP REQUEST

UNIVERSITY OF CALGARY



Filters

- tcp.port == 443
- ip.addr == 10.43.54.65
- ip.src == 10.43.54.65
- ip.dst == 10.43.54.65
- ip.addr != 10.43.54.65
- http
- dns
- http.request.method == "GET"

FILTER EXAMPLES

UNIVERSITY OF CALGARY

In display Filter

- tcp.port == 80
- eth.addr == 00:00:5e:00:53:00
- tcp.port == 80 || udp.port == 80
- tcp.port == 80 && ip.src == 172.17.14.47
- http.request.version=="HTTP/1.1”
- tcp.dstport == 25

In capture filter

- tcp port 80
- ip src host 136.159.5.20
- host 136.159.5.1 (source/destination)
- (src host 23.36.178.81 and not dst host 172.17.14.47) and tcp dst portrange 200-10000

Capture Traffic

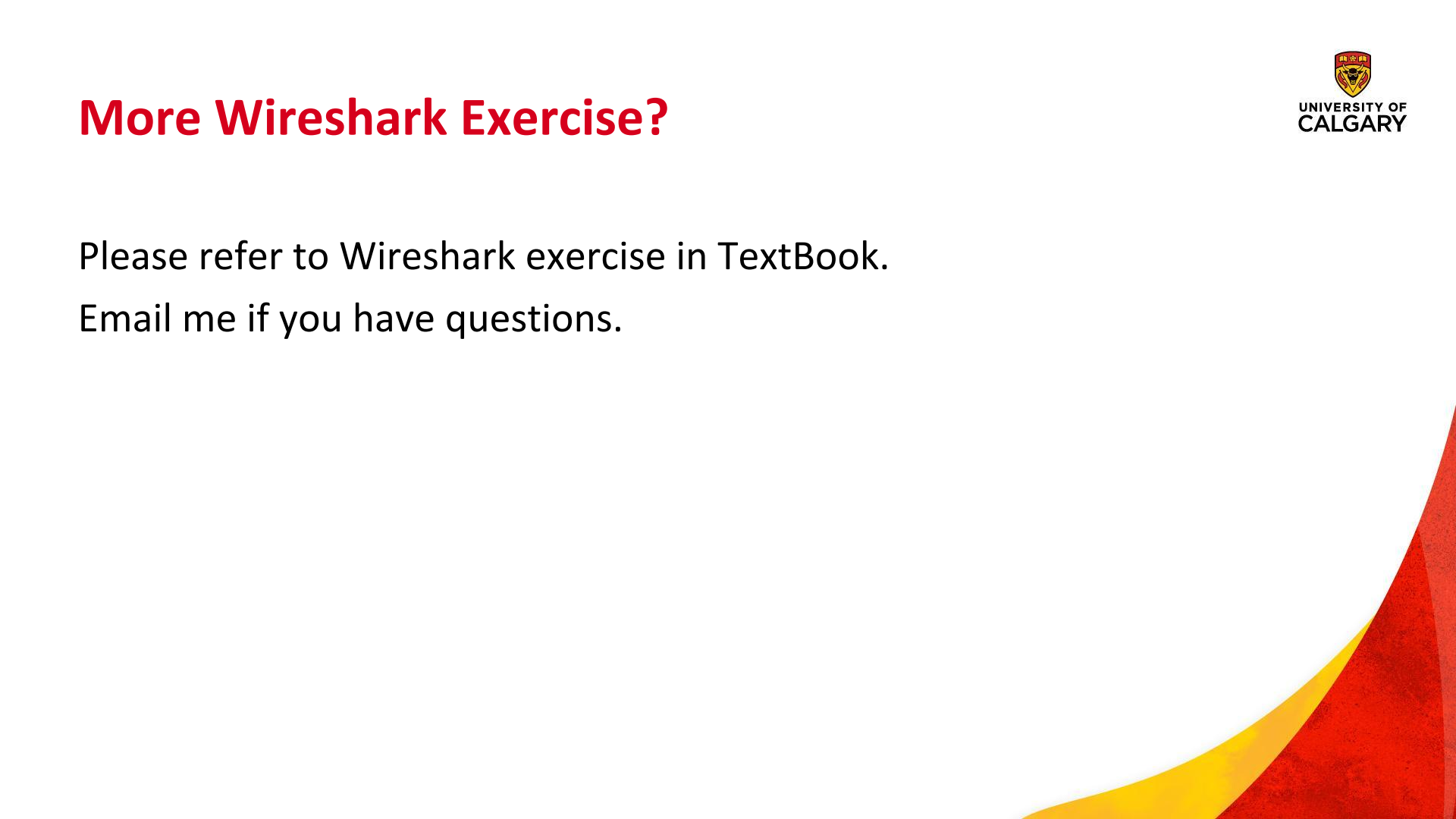
UNIVERSITY OF CALGARY

- tshark has to be run with “root” privileges
  - sudo (superuser mode) while running tshark
- Identify the network interface to monitor
  - To list all interfaces in a machine: ifconfig -a
- Create a destination folder to save the packet trace file
  - In your home directory (/home/ubuntu): mkdir dump
  - Change ownership of the dump folder to root: sudo chown -R root dump
- Capture traffic
- sudo tshark -i eth0 -w dump/filedump0
  - Option “i” to specify interface name
  - Option “w” to specify destination of packet trace file

More Wireshark Exercise?

Please refer to Wireshark exercise in TextBook.

Email me if you have questions.



REFERENCES

UNIVERSITY OF CALGARY

- https://en.wikipedia.org/wiki/Wireshark
- https://wiki.wireshark.org
- https://www.wireshark.org