Basic Linux
& Wireshark Tutorial

ECE6363 LAB 1

LAB1 OBJECTIVES

- Get familiar with **Ubuntu** and **Linux commands**
- Learn the network measurement tool: **Wireshark**
  - Get fundamental understanding of cloud computing
  - Compare Dropbox and Google drive

Ubuntu

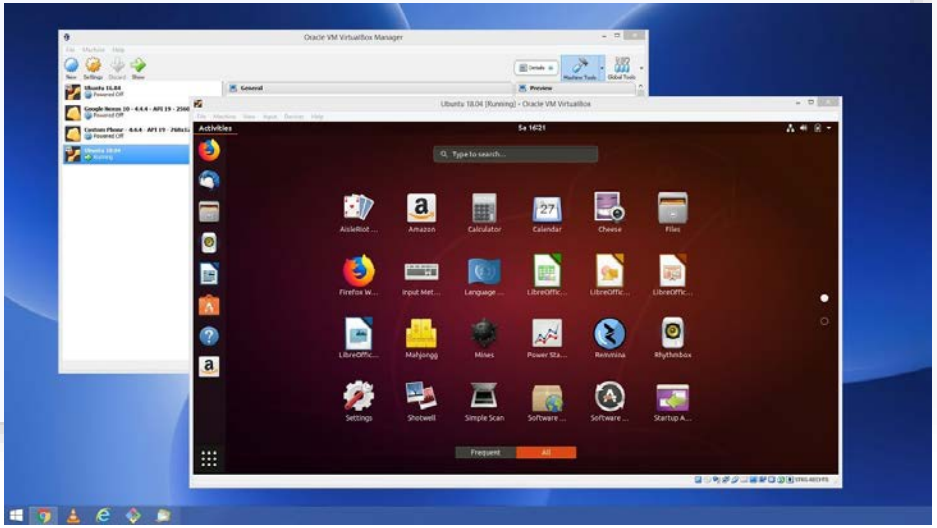
Linux System & Network Debugging Tools

- To install a Linux system on your computer (Ubuntu)

1. Install VirtualBox (preferred, https://www.virtualbox.org/) or VMWare
2. Download Ubuntu Desktop (https://ubuntu.com/download/desktop) or server

   Ubuntu 16 is recommended. There might be some issues with Ubuntu 20 with the following lab.

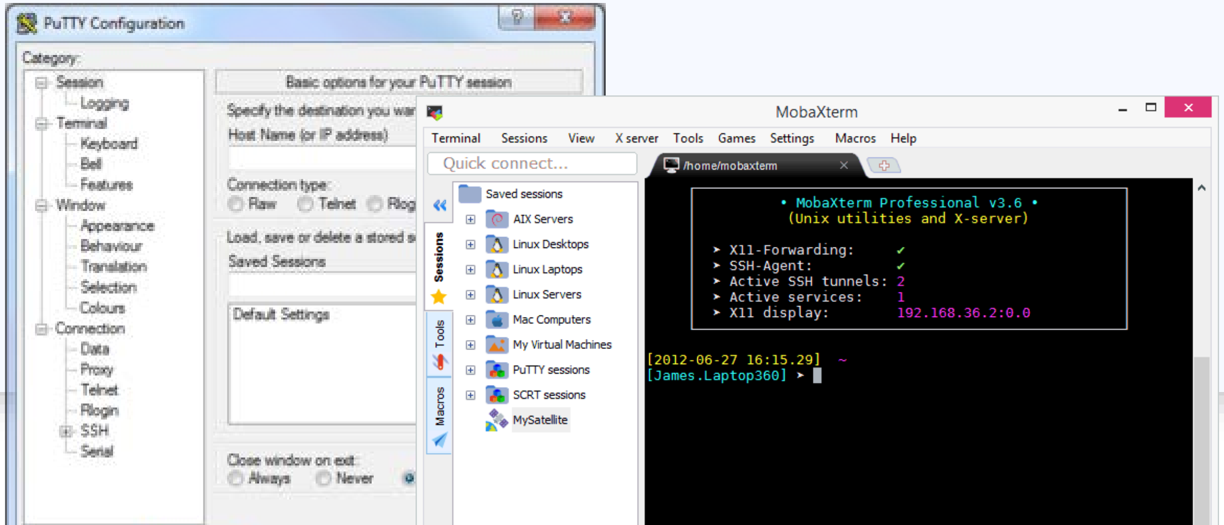
3. Install Ubuntu as a **Virtual Machine** in VirtualBox (https://brb.nci.nih.gov/seqtools/installUbuntu.html)



Linux System & Network Debugging Tools

- To install a Linux system on your computer (Ubuntu)

1. Install VirtualBox (preferred, https://www.virtualbox.org/) or VMWare
2. Download Ubuntu Desktop (https://ubuntu.com/download/desktop) or server
3. Install Ubuntu as a **Virtual Machine** in VirtualBox (https://brb.nci.nih.gov/seqtools/installUbuntu.html)
4. Learn to use SSH clients to connect to the remote server
   - Putty
   - MobaXterm
   - SmarTTY

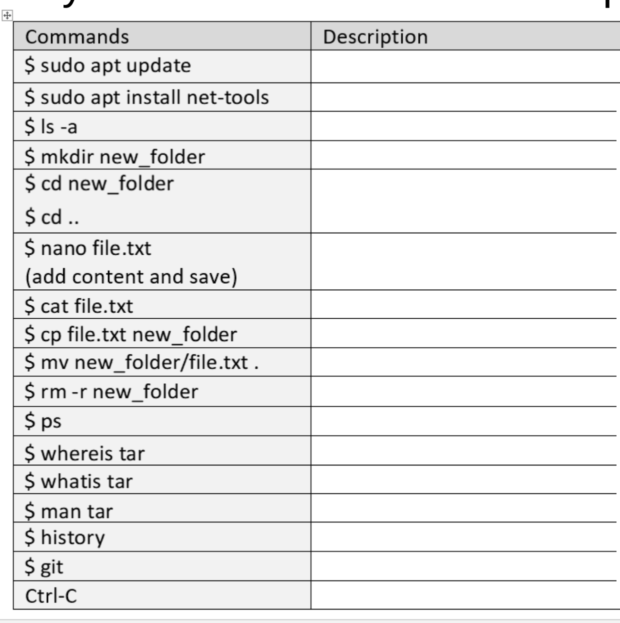


```
         • MobaXterm Professional v3.6 •
          (Unix utilities and X-server)

  ➤ X11-Forwarding:     ✓
  ➤ SSH-Agent:          ✓
  ➤ Active SSH tunnels: 2
  ➤ Active services:    1
  ➤ X11 display:        192.168.36.2:0.0

[2012-06-27 16:15.29]  ~
[James.Laptop360] ➤
```

Linux System & Network Debugging Tools

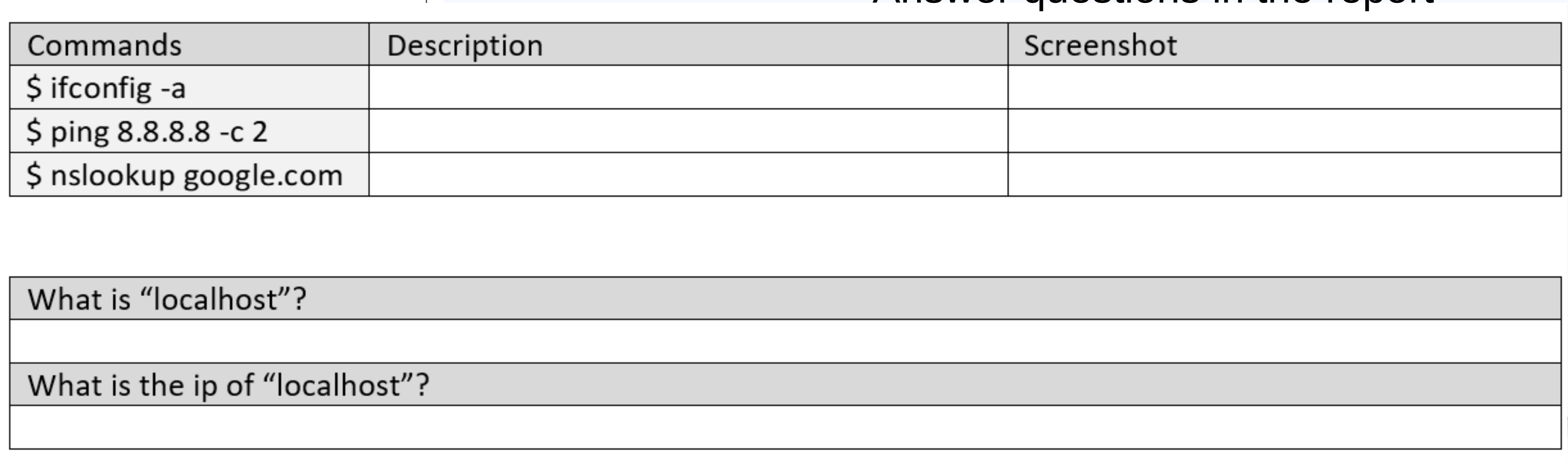
- This semester, you'll learn:
  - configuring network in Datacenter
  - playing with cloud services
- Most of the platform is on Linux. You'll learn basic commands of Ubuntu in lab 1.

Play with the commands and explain these command yourself



Commands	Description
$ sudo apt update	
$ sudo apt install net-tools	
$ ls -a	
$ mkdir new_folder	
$ cd new_folder $ cd ..	
$ nano file.txt (add content and save)	
$ cat file.txt	
$ cp file.txt new_folder	
$ mv new_folder/file.txt .	
$ rm -r new_folder	
$ ps	
$ whereis tar	
$ whatis tar	
$ man tar	
$ history	
$ git	
Ctrl-C	

Answer questions in the report



Commands	Description	Screenshot
$ ifconfig -a		
$ ping 8.8.8.8 -c 2		
$ nslookup google.com		

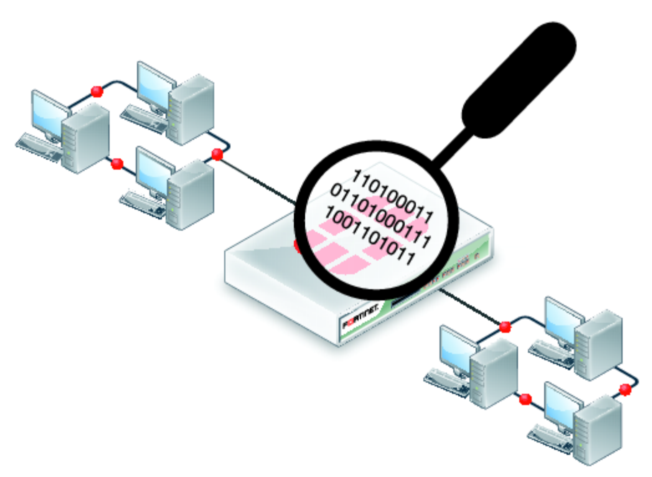
What is "localhost"?
What is the ip of "localhost"?

WireShark

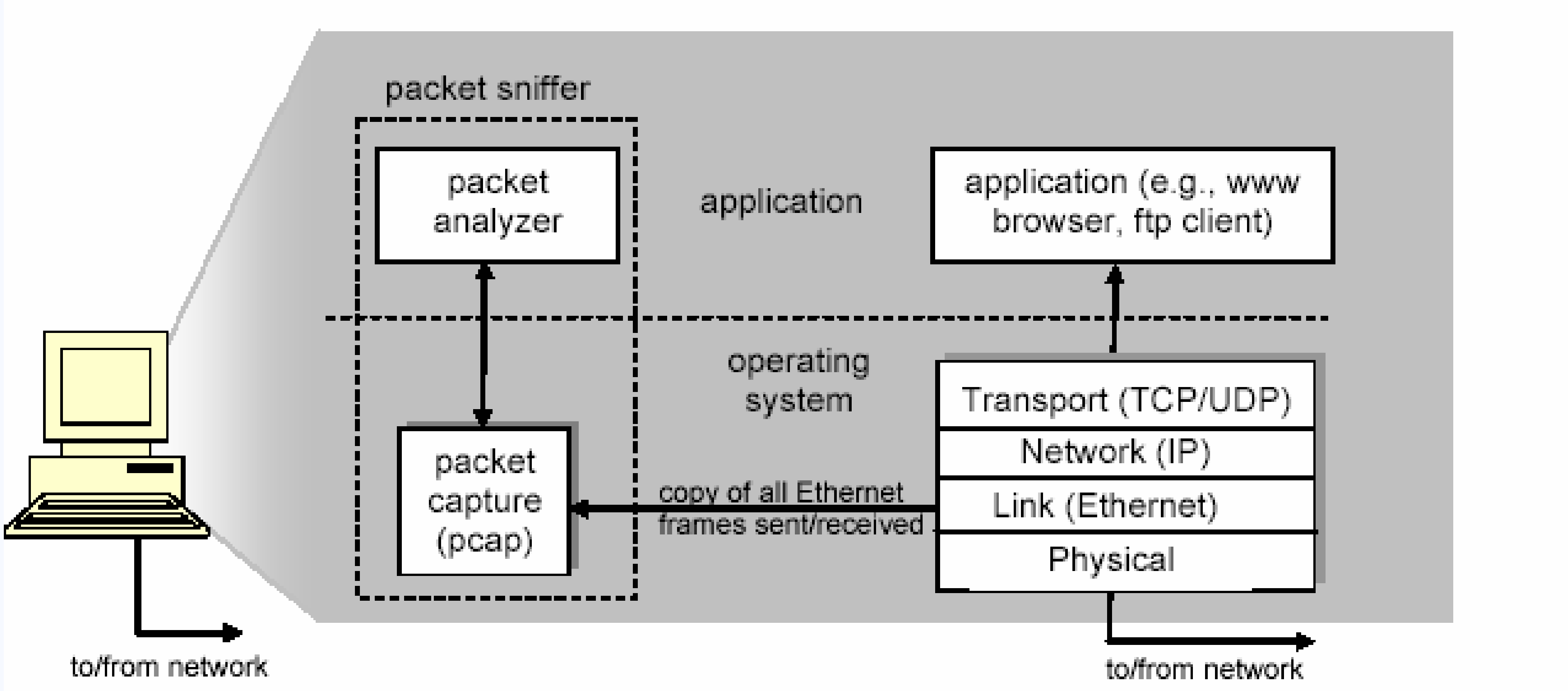
WireShark

- **Packet Sniffer**: For observing the messages exchanged between executing protocol entities.
  - Store and/or display the contents of the various protocol fields in these captured messages.

- **Packet Analyzer**: A component of packet sniffer which displays the contents of all fields within a protocol message.

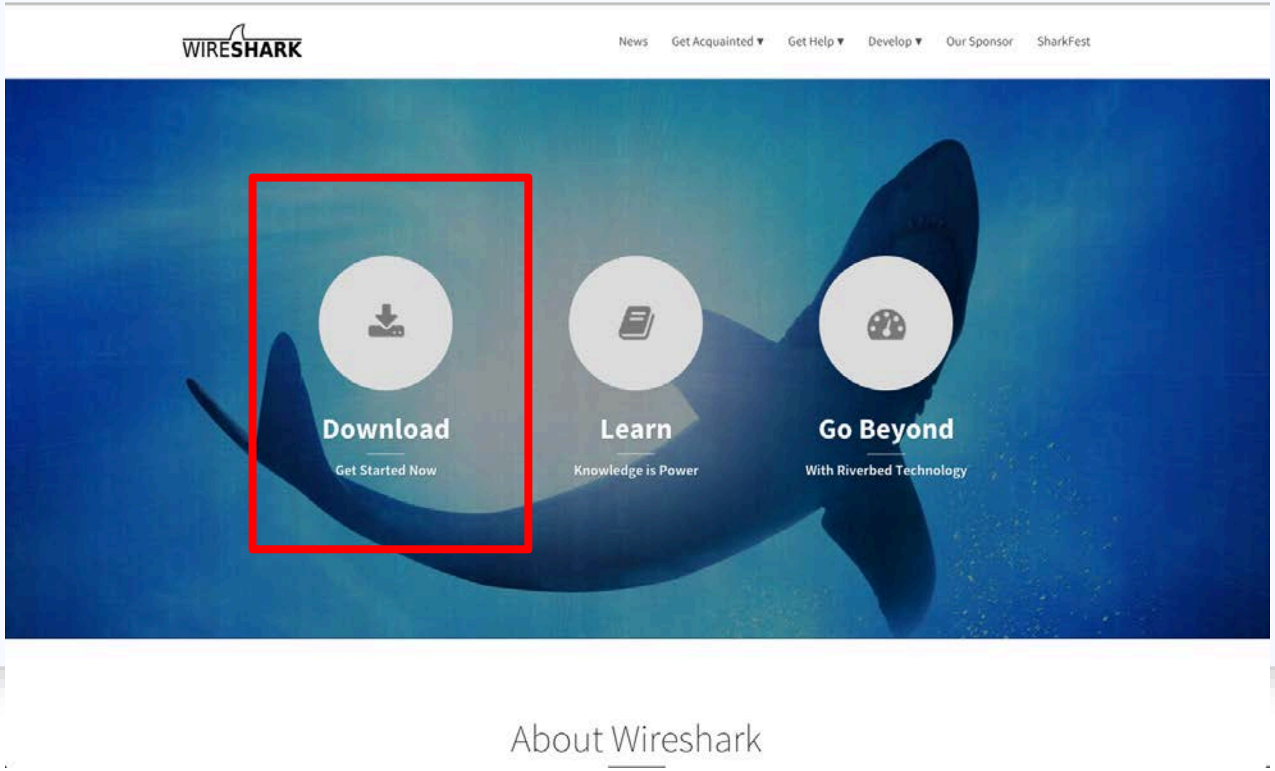


TYPICAL PACKET SNIFFER



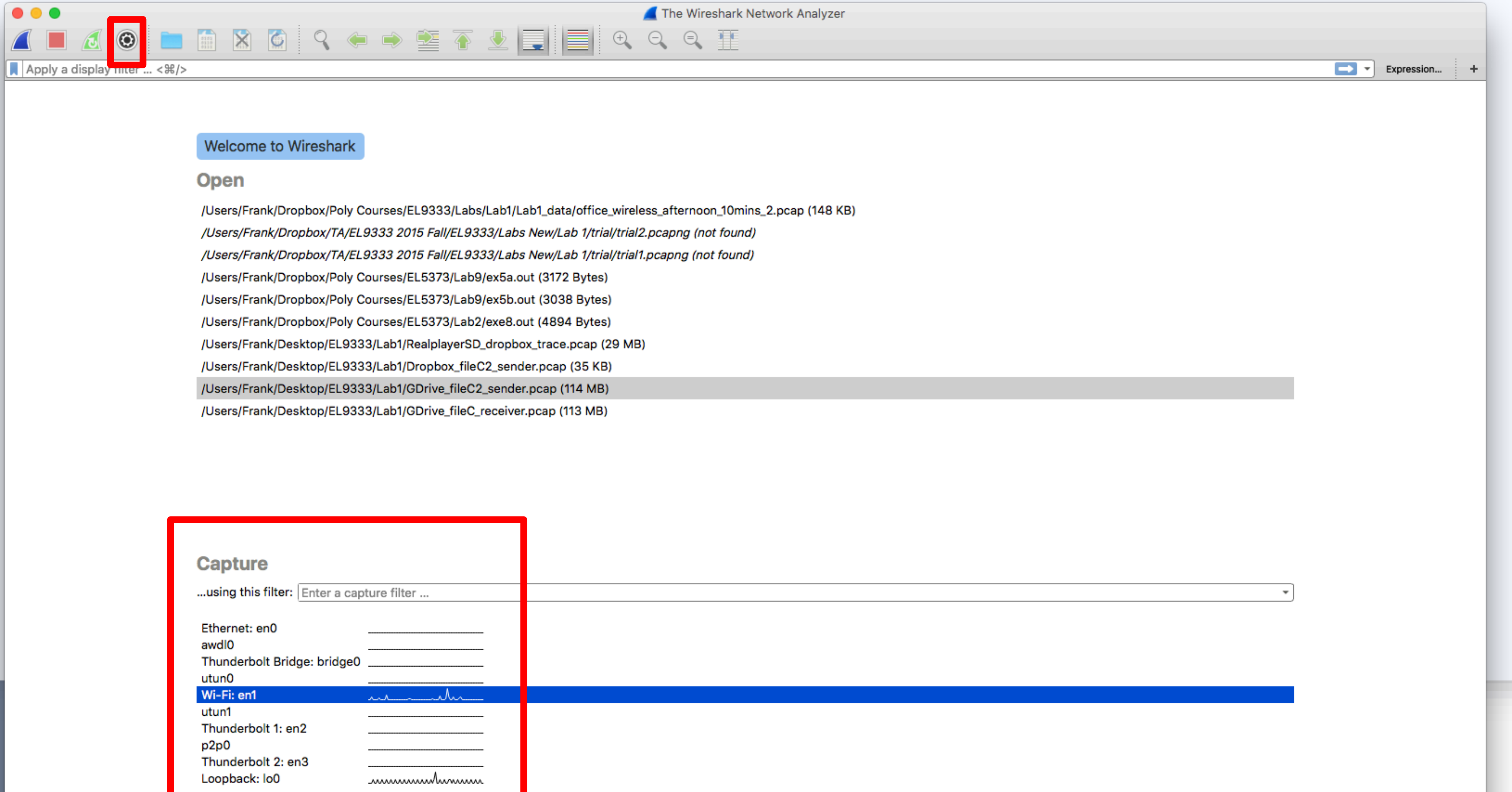
Download WireShark

- (Windows, Mac) Visit https://www.wireshark.org/
- (Linux) apt install wireshark



WireShark

- Choose the network interface you want to capture



The Wireshark Network Analyzer
Apply a display filter ... <⌘/>
Expression...
+

Welcome to Wireshark

Open

/Users/Frank/Dropbox/Poly Courses/EL9333/Labs/Lab1/Lab1_data/office_wireless_afternoon_10mins_2.pcap (148 KB)

/Users/Frank/Dropbox/TA/EL9333 2015 Fall/EL9333/Labs New/Lab 1/trial/trial2.pcapng (not found)

/Users/Frank/Dropbox/TA/EL9333 2015 Fall/EL9333/Labs New/Lab 1/trial/trial1.pcapng (not found)

/Users/Frank/Dropbox/Poly Courses/EL5373/Lab9/ex5a.out (3172 Bytes)

/Users/Frank/Dropbox/Poly Courses/EL5373/Lab9/ex5b.out (3038 Bytes)

/Users/Frank/Dropbox/Poly Courses/EL5373/Lab2/exe8.out (4894 Bytes)

/Users/Frank/Desktop/EL9333/Lab1/RealplayerSD_dropbox_trace.pcap (29 MB)

/Users/Frank/Desktop/EL9333/Lab1/Dropbox_fileC2_sender.pcap (35 KB)

/Users/Frank/Desktop/EL9333/Lab1/GDrive_fileC2_sender.pcap (114 MB)

/Users/Frank/Desktop/EL9333/Lab1/GDrive_fileC_receiver.pcap (113 MB)

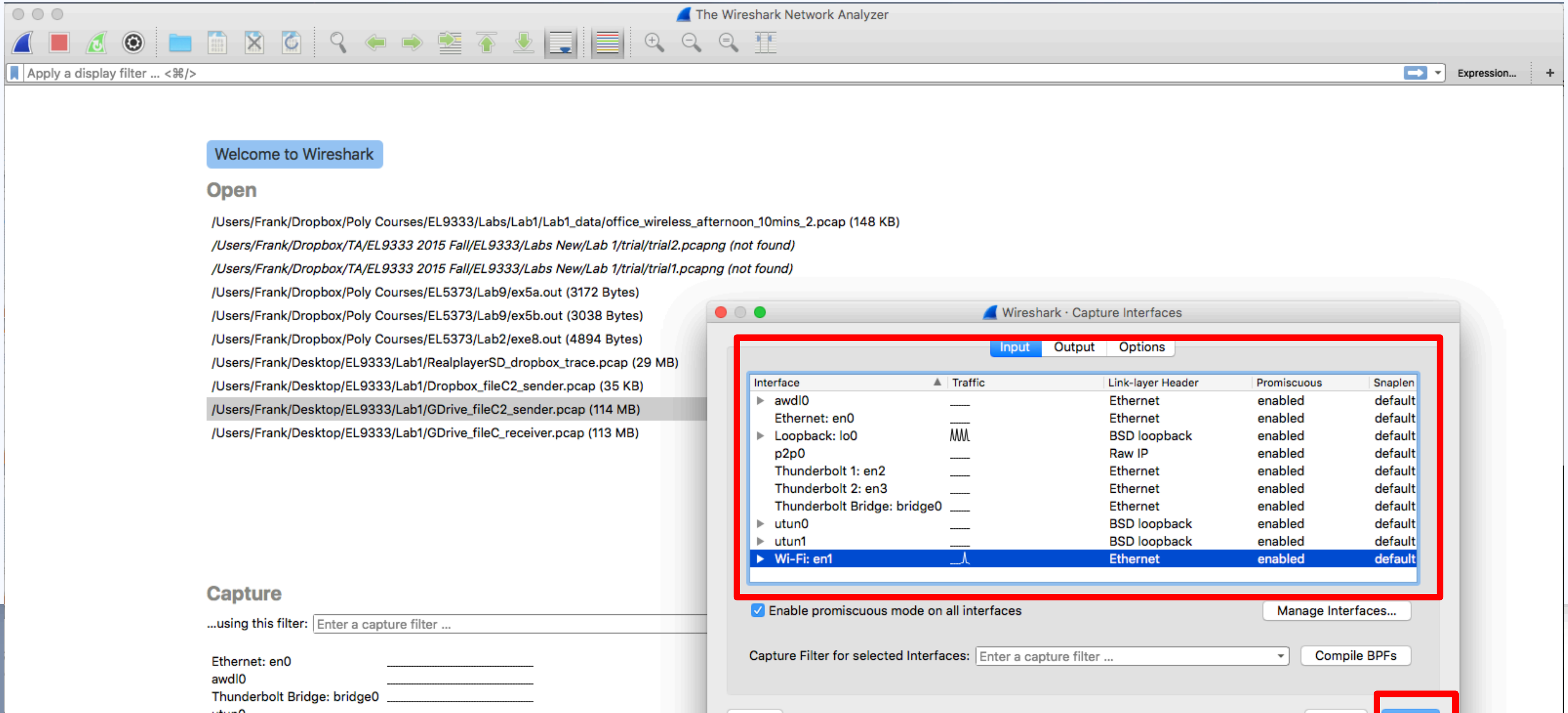
Capture

...using this filter: Enter a capture filter ...

Ethernet: en0
awdl0
Thunderbolt Bridge: bridge0
utun0
Wi-Fi: en1
utun1
Thunderbolt 1: en2
p2p0
Thunderbolt 2: en3
Loopback: lo0

WireShark

- Choose the network interface you want to capture
- Start Wireshark



The Wireshark Network Analyzer
Apply a display filter ... <⌘/>
Expression...
+
Welcome to Wireshark

Open

/Users/Frank/Dropbox/Poly Courses/EL9333/Labs/Lab1/Lab1_data/office_wireless_afternoon_10mins_2.pcap (148 KB)
/Users/Frank/Dropbox/TA/EL9333 2015 Fall/EL9333/Labs New/Lab 1/trial/trial2.pcapng (not found)
/Users/Frank/Dropbox/TA/EL9333 2015 Fall/EL9333/Labs New/Lab 1/trial/trial1.pcapng (not found)
/Users/Frank/Dropbox/Poly Courses/EL5373/Lab9/ex5a.out (3172 Bytes)
/Users/Frank/Dropbox/Poly Courses/EL5373/Lab9/ex5b.out (3038 Bytes)
/Users/Frank/Dropbox/Poly Courses/EL5373/Lab2/exe8.out (4894 Bytes)
/Users/Frank/Desktop/EL9333/Lab1/RealplayerSD_dropbox_trace.pcap (29 MB)
/Users/Frank/Desktop/EL9333/Lab1/Dropbox_fileC2_sender.pcap (35 KB)
/Users/Frank/Desktop/EL9333/Lab1/GDrive_fileC2_sender.pcap (114 MB)
/Users/Frank/Desktop/EL9333/Lab1/GDrive_fileC_receiver.pcap (113 MB)

Capture

...using this filter: Enter a capture filter ...

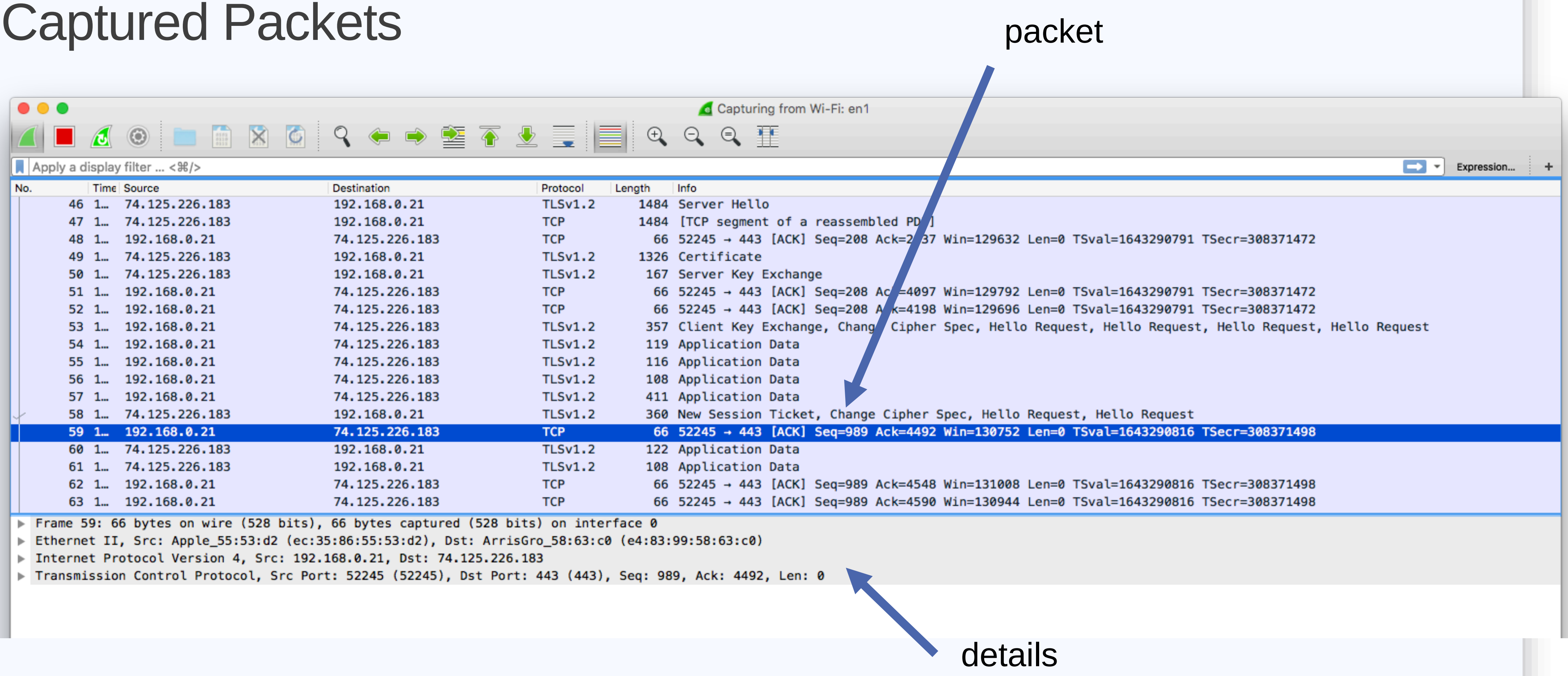
Ethernet: en0
awdl0
Thunderbolt Bridge: bridge0

Interface	Traffic	Link-layer Header	Promiscuous	Snaplen
▶ awdl0		Ethernet	enabled	default
Ethernet: en0		Ethernet	enabled	default
▶ Loopback: lo0		BSD loopback	enabled	default
p2p0		Raw IP	enabled	default
Thunderbolt 1: en2		Ethernet	enabled	default
Thunderbolt 2: en3		Ethernet	enabled	default
Thunderbolt Bridge: bridge0		Ethernet	enabled	default
▶ utun0		BSD loopback	enabled	default
▶ utun1		BSD loopback	enabled	default
▶ Wi-Fi: en1		Ethernet	enabled	default

☑ Enable promiscuous mode on all interfaces

Capture Filter for selected Interfaces: Enter a capture filter ...

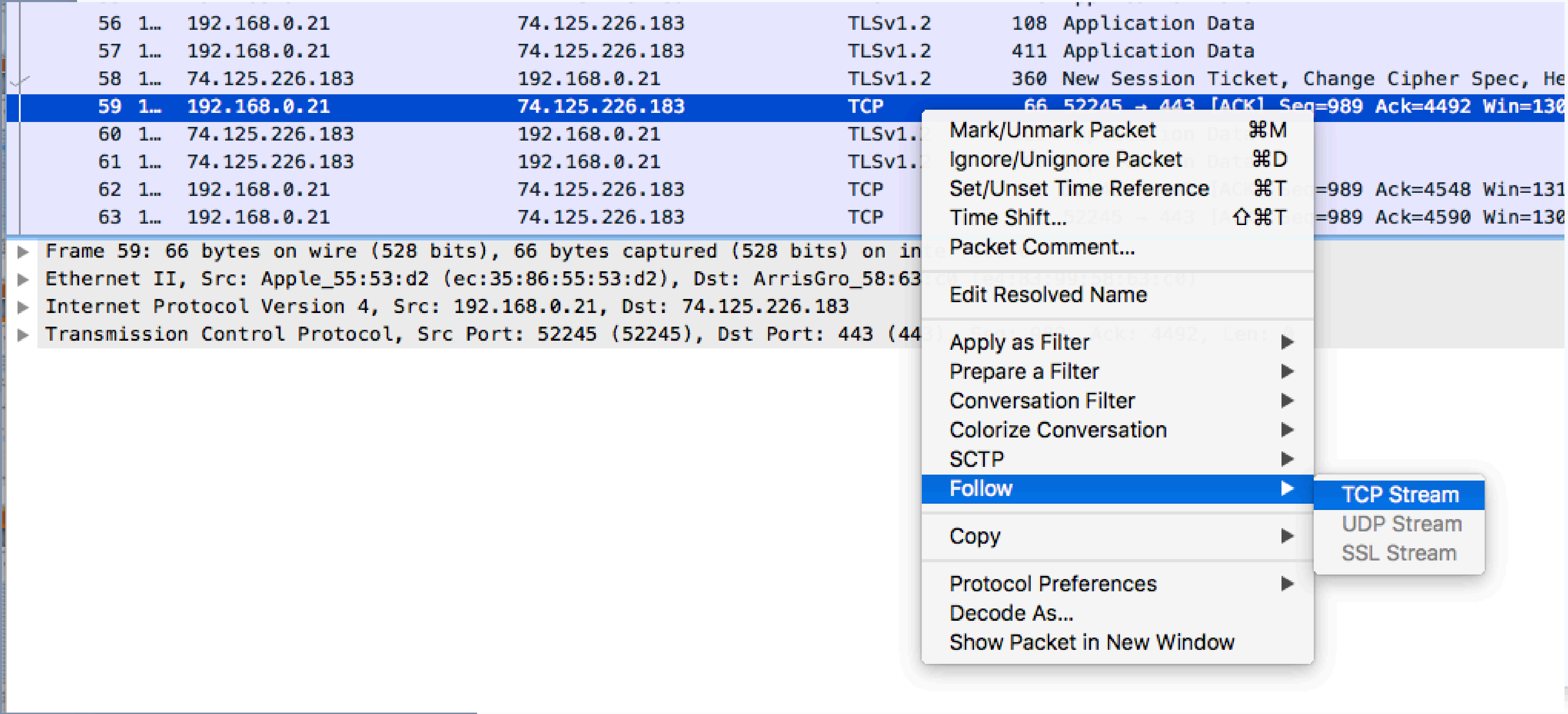
Captured Packets



```
No.   Time Source           Destination      Protocol  Length  Info
   46 1…   74.125.226.183   192.168.0.21     TLSv1.2     1484  Server Hello
   47 1…   74.125.226.183   192.168.0.21     TCP         1484  [TCP segment of a reassembled PDU]
   48 1…   192.168.0.21     74.125.226.183   TCP           66  52245 → 443 [ACK] Seq=208 Ack=2837 Win=129632 Len=0 TSval=1643290791 TSecr=308371472
   49 1…   74.125.226.183   192.168.0.21     TLSv1.2     1326  Certificate
   50 1…   74.125.226.183   192.168.0.21     TLSv1.2      167  Server Key Exchange
   51 1…   192.168.0.21     74.125.226.183   TCP           66  52245 → 443 [ACK] Seq=208 Ack=4097 Win=129792 Len=0 TSval=1643290791 TSecr=308371472
   52 1…   192.168.0.21     74.125.226.183   TCP           66  52245 → 443 [ACK] Seq=208 Ack=4198 Win=129696 Len=0 TSval=1643290791 TSecr=308371472
   53 1…   192.168.0.21     74.125.226.183   TLSv1.2      357  Client Key Exchange, Change Cipher Spec, Hello Request, Hello Request, Hello Request, Hello Request
   54 1…   192.168.0.21     74.125.226.183   TLSv1.2      119  Application Data
   55 1…   192.168.0.21     74.125.226.183   TLSv1.2      116  Application Data
   56 1…   192.168.0.21     74.125.226.183   TLSv1.2      108  Application Data
   57 1…   192.168.0.21     74.125.226.183   TLSv1.2      411  Application Data
   58 1…   74.125.226.183   192.168.0.21     TLSv1.2      360  New Session Ticket, Change Cipher Spec, Hello Request, Hello Request
   59 1…   192.168.0.21     74.125.226.183   TCP           66  52245 → 443 [ACK] Seq=989 Ack=4492 Win=130752 Len=0 TSval=1643290816 TSecr=308371498
   60 1…   74.125.226.183   192.168.0.21     TLSv1.2      122  Application Data
   61 1…   74.125.226.183   192.168.0.21     TLSv1.2      108  Application Data
   62 1…   192.168.0.21     74.125.226.183   TCP           66  52245 → 443 [ACK] Seq=989 Ack=4548 Win=131008 Len=0 TSval=1643290816 TSecr=308371498
   63 1…   192.168.0.21     74.125.226.183   TCP           66  52245 → 443 [ACK] Seq=989 Ack=4590 Win=130944 Len=0 TSval=1643290816 TSecr=308371498
```

```
▶ Frame 59: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
▶ Ethernet II, Src: Apple_55:53:d2 (ec:35:86:55:53:d2), Dst: ArrisGro_58:63:c0 (e4:83:99:58:63:c0)
▶ Internet Protocol Version 4, Src: 192.168.0.21, Dst: 74.125.226.183
▶ Transmission Control Protocol, Src Port: 52245 (52245), Dst Port: 443 (443), Seq: 989, Ack: 4492, Len: 0
```

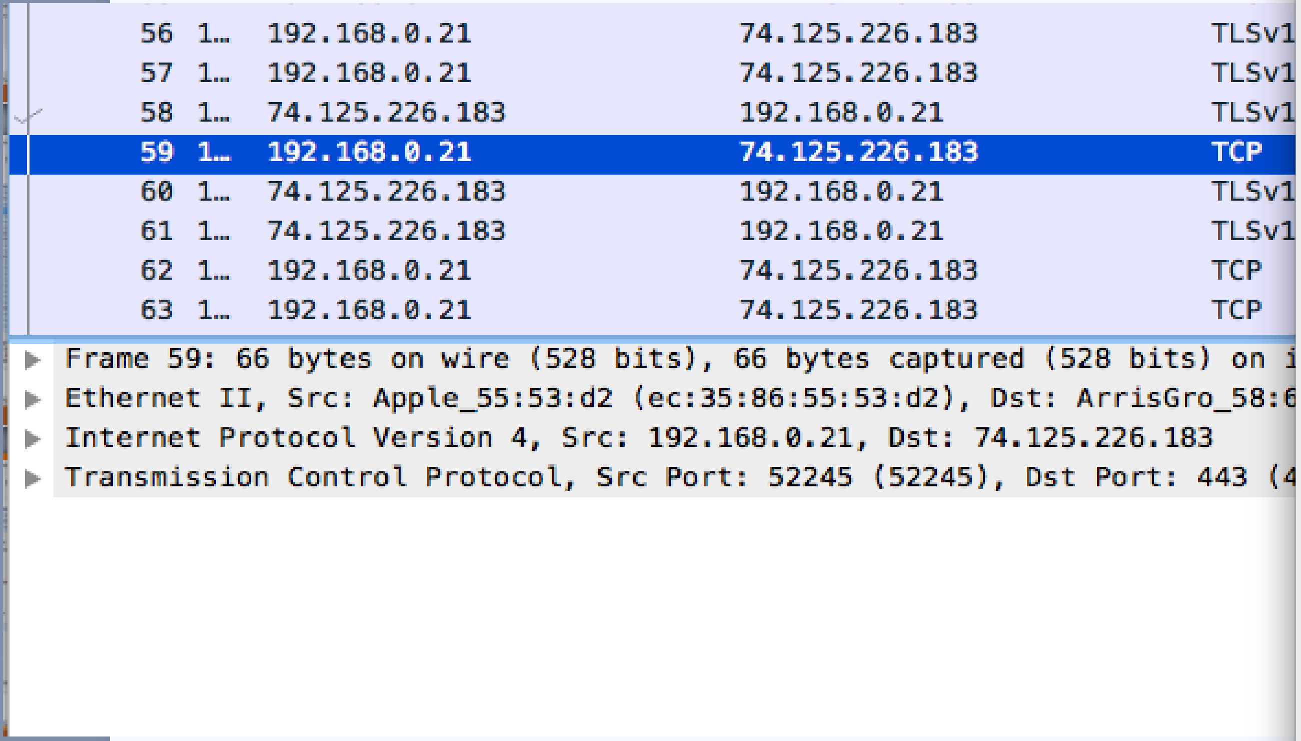
Follow a TCP Stream



```
56 1…  192.168.0.21      74.125.226.183   TLSv1.2   108 Application Data
57 1…  192.168.0.21      74.125.226.183   TLSv1.2   411 Application Data
58 1…  74.125.226.183    192.168.0.21     TLSv1.2   360 New Session Ticket, Change Cipher Spec, He
59 1…  192.168.0.21      74.125.226.183   TCP        66 52245 → 443 [ACK] Seq=989 Ack=4492 Win=130
60 1…  74.125.226.183    192.168.0.21     TLSv1.
61 1…  74.125.226.183    192.168.0.21     TLSv1.
62 1…  192.168.0.21      74.125.226.183   TCP                            =989 Ack=4548 Win=131
63 1…  192.168.0.21      74.125.226.183   TCP                            =989 Ack=4590 Win=130
```

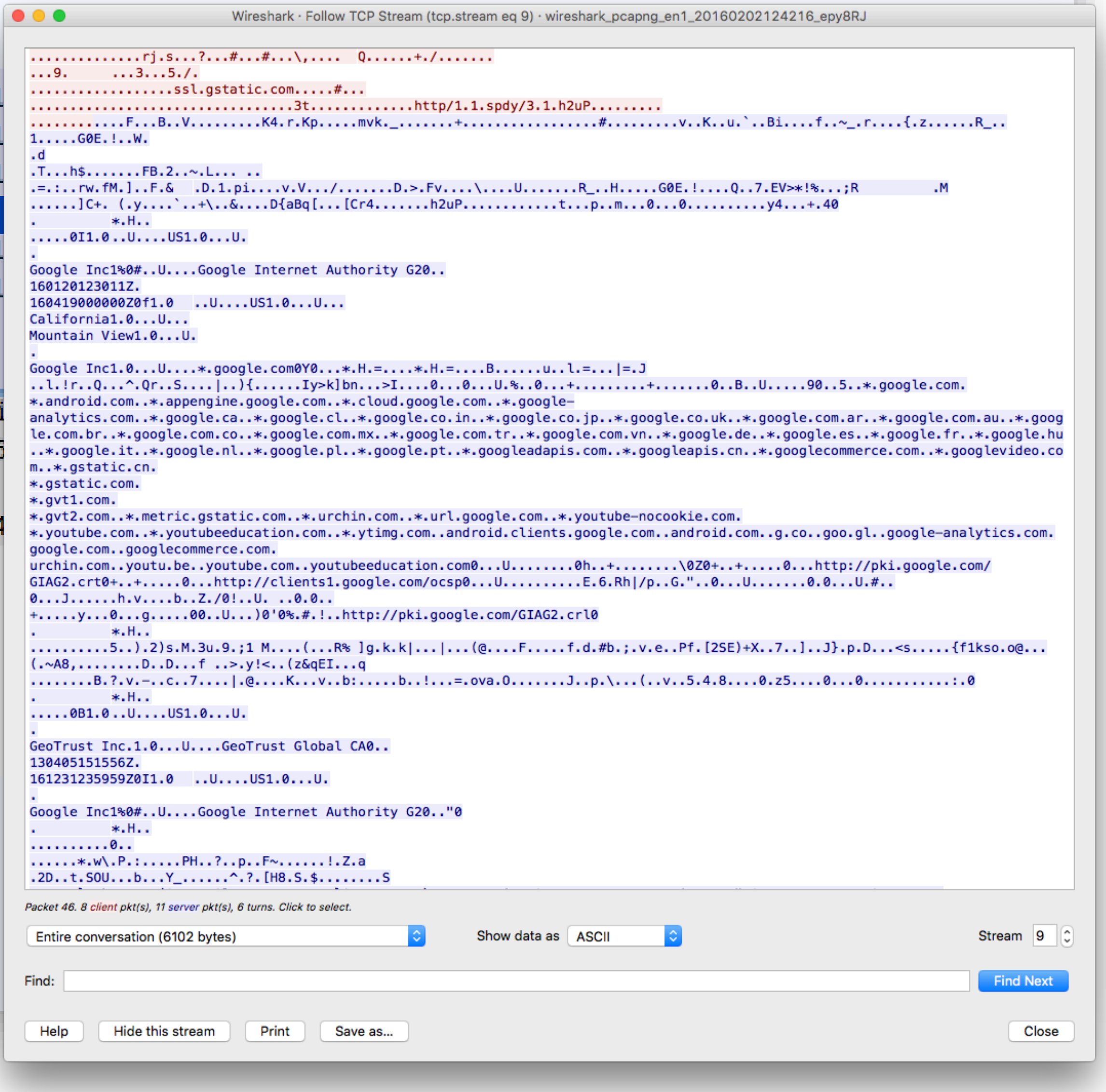
```
▶ Frame 59: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on in
▶ Ethernet II, Src: Apple_55:53:d2 (ec:35:86:55:53:d2), Dst: ArrisGro_58:63
▶ Internet Protocol Version 4, Src: 192.168.0.21, Dst: 74.125.226.183
▶ Transmission Control Protocol, Src Port: 52245 (52245), Dst Port: 443 (44
```

Certain TCP Stream



```
56  1…  192.168.0.21      74.125.226.183    TLSv1
57  1…  192.168.0.21      74.125.226.183    TLSv1
58  1…  74.125.226.183    192.168.0.21      TLSv1
59  1…  192.168.0.21      74.125.226.183    TCP
60  1…  74.125.226.183    192.168.0.21      TLSv1
61  1…  74.125.226.183    192.168.0.21      TLSv1
62  1…  192.168.0.21      74.125.226.183    TCP
63  1…  192.168.0.21      74.125.226.183    TCP
```

```
▶ Frame 59: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on i
▶ Ethernet II, Src: Apple_55:53:d2 (ec:35:86:55:53:d2), Dst: ArrisGro_58:6
▶ Internet Protocol Version 4, Src: 192.168.0.21, Dst: 74.125.226.183
▶ Transmission Control Protocol, Src Port: 52245 (52245), Dst Port: 443 (4
```



Wireshark · Follow TCP Stream (tcp.stream eq 9) · wireshark_pcapng_en1_20160202124216_epy8RJ

```
..............rj.s...?...#...#...\,....  Q......+./.......
...9.     ...3...5./.
..................ssl.gstatic.com.....#...
.................................3t.............http/1.1.spdy/3.1.h2uP.........
..............F...B..V.........K4.r.Kp.....mvk._.......+................#.........v..K..u.`..Bi....f..~_.r....{.z......R_..
1.....G0E.!..W.
.d
.T...h$.......FB.2..~.L... ..
.=.:..rw.fM.]..F.&   .D.1.pi....v.V.../.......D.>.Fv....\....U.......R_..H.....G0E.!....Q..7.EV>*!%...;R         .M
......]C+. (.y....`..+\..&....D{aBq[...[Cr4.......h2uP............t...p..m...0...0.........y4...+.40
.         *.H..
.....0I1.0..U....US1.0...U.
.
Google Inc1%0#..U....Google Internet Authority G20..
160120123011Z.
160419000000Z0f1.0   ..U....US1.0...U...
California1.0...U...
Mountain View1.0...U.
.
Google Inc1.0...U....*.google.com0Y0...*.H.=....*.H.=....B......u..l.=...|=.J
..l.!r..Q...^.Qr..S....|..){......Iy>k]bn...>I....0...0...U.%..0...+.........+.......0..B..U.....90..5..*.google.com.
*.android.com..*.appengine.google.com..*.cloud.google.com..*.google-
analytics.com..*.google.ca..*.google.cl..*.google.co.in..*.google.co.jp..*.google.co.uk..*.google.com.ar..*.google.com.au..*.goog
le.com.br..*.google.com.co..*.google.com.mx..*.google.com.tr..*.google.com.vn..*.google.de..*.google.es..*.google.fr..*.google.hu
..*.google.it..*.google.nl..*.google.pl..*.google.pt..*.googleadapis.com..*.googleapis.cn..*.googlecommerce.com..*.googlevideo.co
m..*.gstatic.cn.
*.gstatic.com.
*.gvt1.com.
*.gvt2.com..*.metric.gstatic.com..*.urchin.com..*.url.google.com..*.youtube-nocookie.com.
*.youtube.com..*.youtubeeducation.com..*.ytimg.com..android.clients.google.com..android.com..g.co..goo.gl..google-analytics.com.
google.com..googlecommerce.com.
urchin.com..youtu.be..youtube.com..youtubeeducation.com0...U........0h..+........\0Z0+..+.....0...http://pki.google.com/
GIAG2.crt0+..+.....0...http://clients1.google.com/ocsp0...U..........E.6.Rh|/p..G."..0...U.......0.0...U.#..
0...J......h.v....b..Z./0!..U. ..0.0..
+.....y...0...g.....00..U...)0'0%.#.!..http://pki.google.com/GIAG2.crl0
.         *.H..
..........5..).2)s.M.3u.9.;1 M....(...R% ]g.k.k|...|...(@....F.....f.d.#b.;.v.e..Pf.[2SE)+X..7..]..J}.p.D...<s.....{f1kso.o@...
(.~A8,........D..D...f ..>.y!<..(z&qEI...q
........B.?.v.-..c..7....|.@....K...v..b:.....b..!...=.ova.O.......J..p.\...(..v..5.4.8....0.z5....0...0...........:.0
.         *.H..
.....0B1.0..U....US1.0...U.
.
GeoTrust Inc.1.0...U....GeoTrust Global CA0..
130405151556Z.
161231235959Z0I1.0   ..U....US1.0...U.
.
Google Inc1%0#..U....Google Internet Authority G20.."0
.         *.H..
..........0..
......*.w\.P.:.....PH..?..p..F~......!.Z.a
.2D..t.SOU...b...Y_......^.?.[H8.S.$........S
```

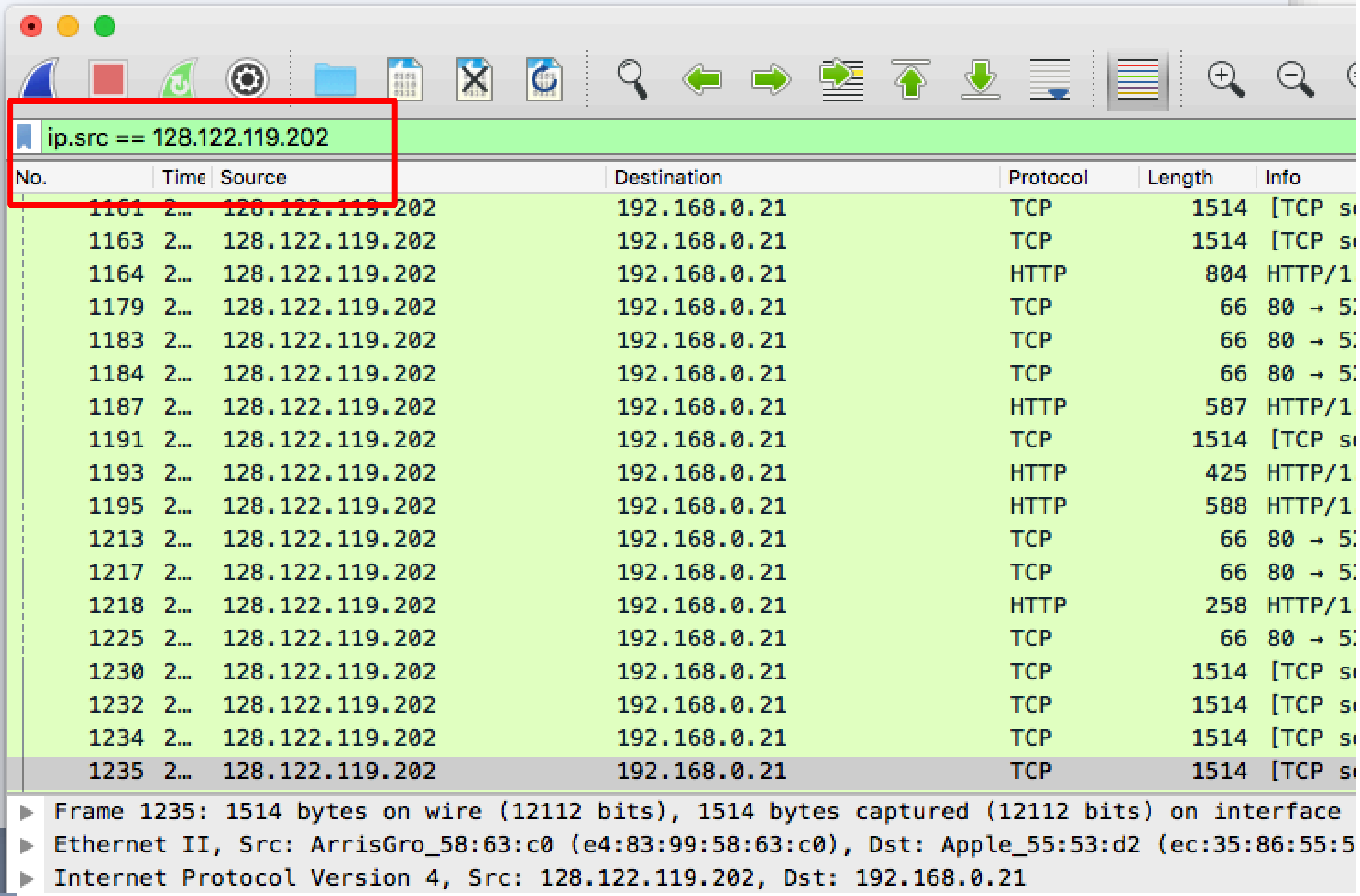
Packet 46. 8 client pkt(s), 11 server pkt(s), 6 turns. Click to select.

Entire conversation (6102 bytes)

Show data as: ASCII

Stream: 9

Filters



ip.src == 128.122.119.202

No.	Time	Source	Destination	Protocol	Length	Info
1161	2…	128.122.119.202	192.168.0.21	TCP	1514	[TCP s
1163	2…	128.122.119.202	192.168.0.21	TCP	1514	[TCP s
1164	2…	128.122.119.202	192.168.0.21	HTTP	804	HTTP/1
1179	2…	128.122.119.202	192.168.0.21	TCP	66	80 → 5
1183	2…	128.122.119.202	192.168.0.21	TCP	66	80 → 5
1184	2…	128.122.119.202	192.168.0.21	TCP	66	80 → 5
1187	2…	128.122.119.202	192.168.0.21	HTTP	587	HTTP/1
1191	2…	128.122.119.202	192.168.0.21	TCP	1514	[TCP s
1193	2…	128.122.119.202	192.168.0.21	HTTP	425	HTTP/1
1195	2…	128.122.119.202	192.168.0.21	HTTP	588	HTTP/1
1213	2…	128.122.119.202	192.168.0.21	TCP	66	80 → 5
1217	2…	128.122.119.202	192.168.0.21	TCP	66	80 → 5
1218	2…	128.122.119.202	192.168.0.21	HTTP	258	HTTP/1
1225	2…	128.122.119.202	192.168.0.21	TCP	66	80 → 5
1230	2…	128.122.119.202	192.168.0.21	TCP	1514	[TCP s
1232	2…	128.122.119.202	192.168.0.21	TCP	1514	[TCP s
1234	2…	128.122.119.202	192.168.0.21	TCP	1514	[TCP s
1235	2…	128.122.119.202	192.168.0.21	TCP	1514	[TCP s

```
▶ Frame 1235: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface
▶ Ethernet II, Src: ArrisGro_58:63:c0 (e4:83:99:58:63:c0), Dst: Apple_55:53:d2 (ec:35:86:55:5
▶ Internet Protocol Version 4, Src: 128.122.119.202, Dst: 192.168.0.21
```

FILTERS

Display filters: for general packet filtering while viewing packets.

Examples:

Show only traffic in the LAN (192.168.x.x), between workstations and servers -- no Internet:

ip.src==192.168.0.0/16 and ip.dst==192.168.0.0/16

Filter out any traffic to or from 10.43.54.65:

ip.addr != 10.43.54.65

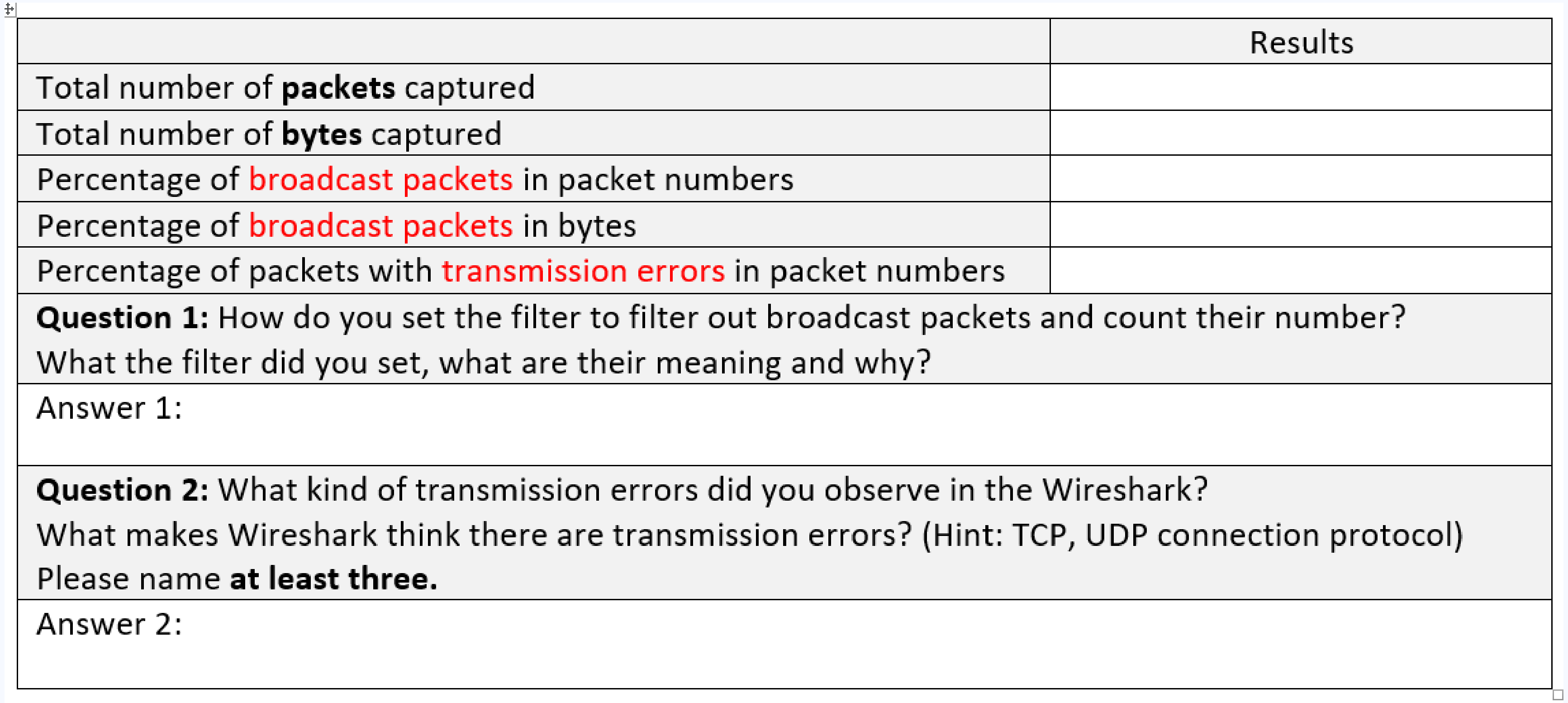
Follow a UDP Flow:

(ip.addr eq 192.168.1.15 and ip.addr eq 192.168.1.9) and (udp.port eq 58445 and udp.port eq 52068)

More info on: http://wiki.wireshark.org/DisplayFilters

TASK 1- WireShark Sniffing (Table 1)

- Capture packets in your network environment **for ten minute**. (Wireless environment is preferred.)
- Analyze each measurement result and provide the following statistics.



	Results
Total number of **packets** captured	
Total number of **bytes** captured	
Percentage of broadcast packets in packet numbers	
Percentage of broadcast packets in bytes	
Percentage of packets with transmission errors in packet numbers	
Question 1: How do you set the filter to filter out broadcast packets and count their number? What the filter did you set, what are their meaning and why?	
Answer 1:	
Question 2: What kind of transmission errors did you observe in the Wireshark? What makes Wireshark think there are transmission errors? (Hint: TCP, UDP connection protocol) Please name **at least three.**	
Answer 2:	

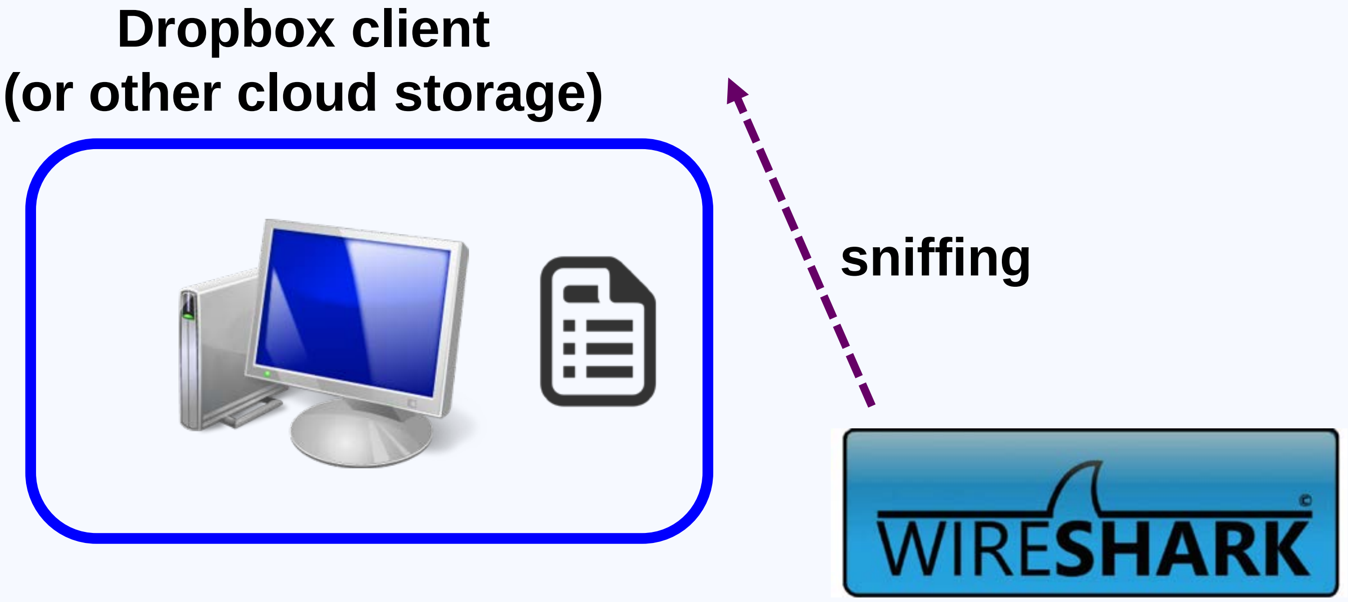
TASK 2- Capture Dropbox Operations (Table 2)

1. **Install a Dropbox client**
(or other cloud storage client)

DO NOT USE the browser!!!

Dropbox client
(or other cloud storage)

TASK 2- Capture Dropbox Operations (Table 2)

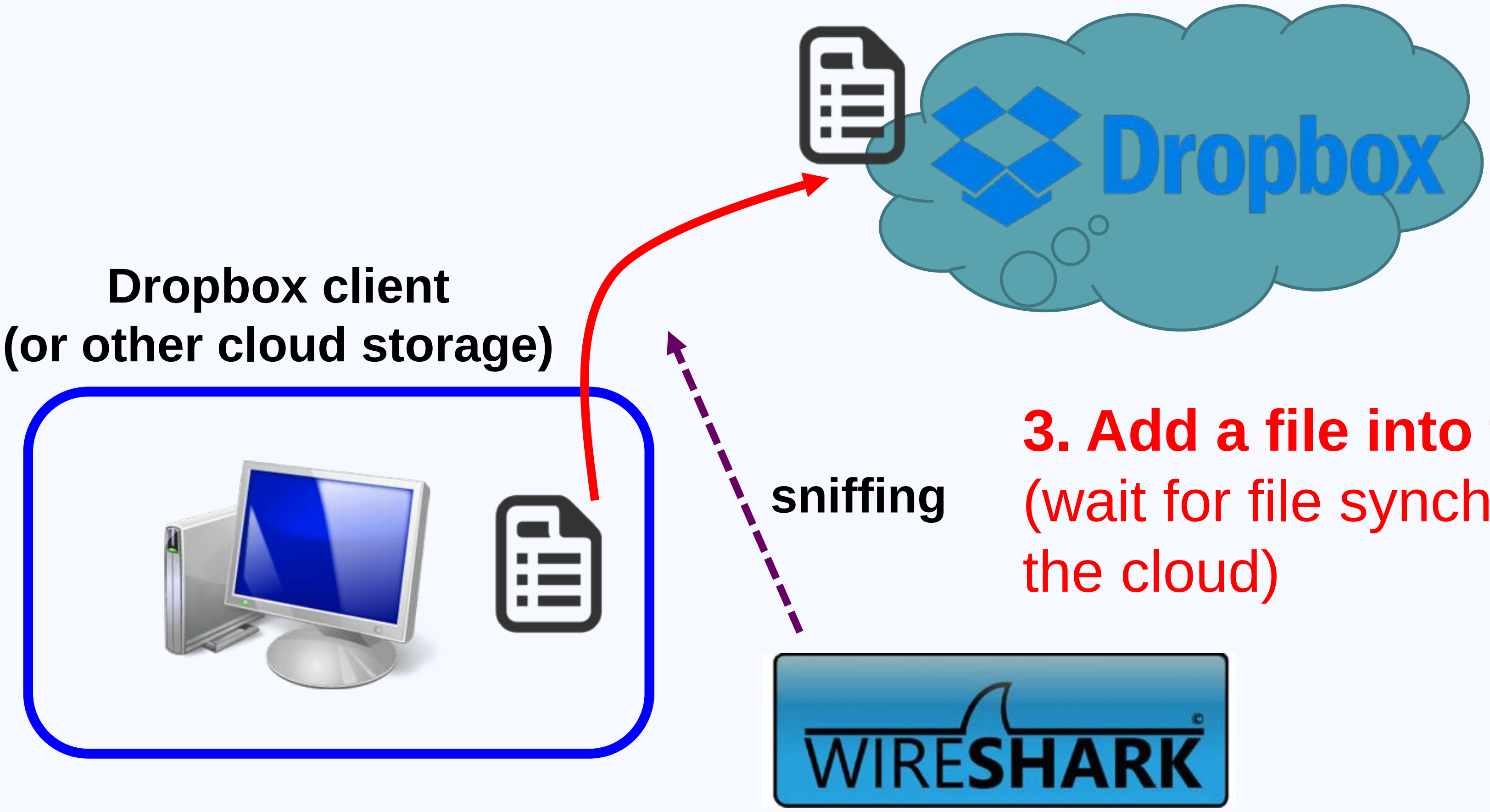


Dropbox client
(or other cloud storage)

sniffing

2. Open Wireshark
Start sniffing

TASK 2- Capture Dropbox Operations (Table 2)

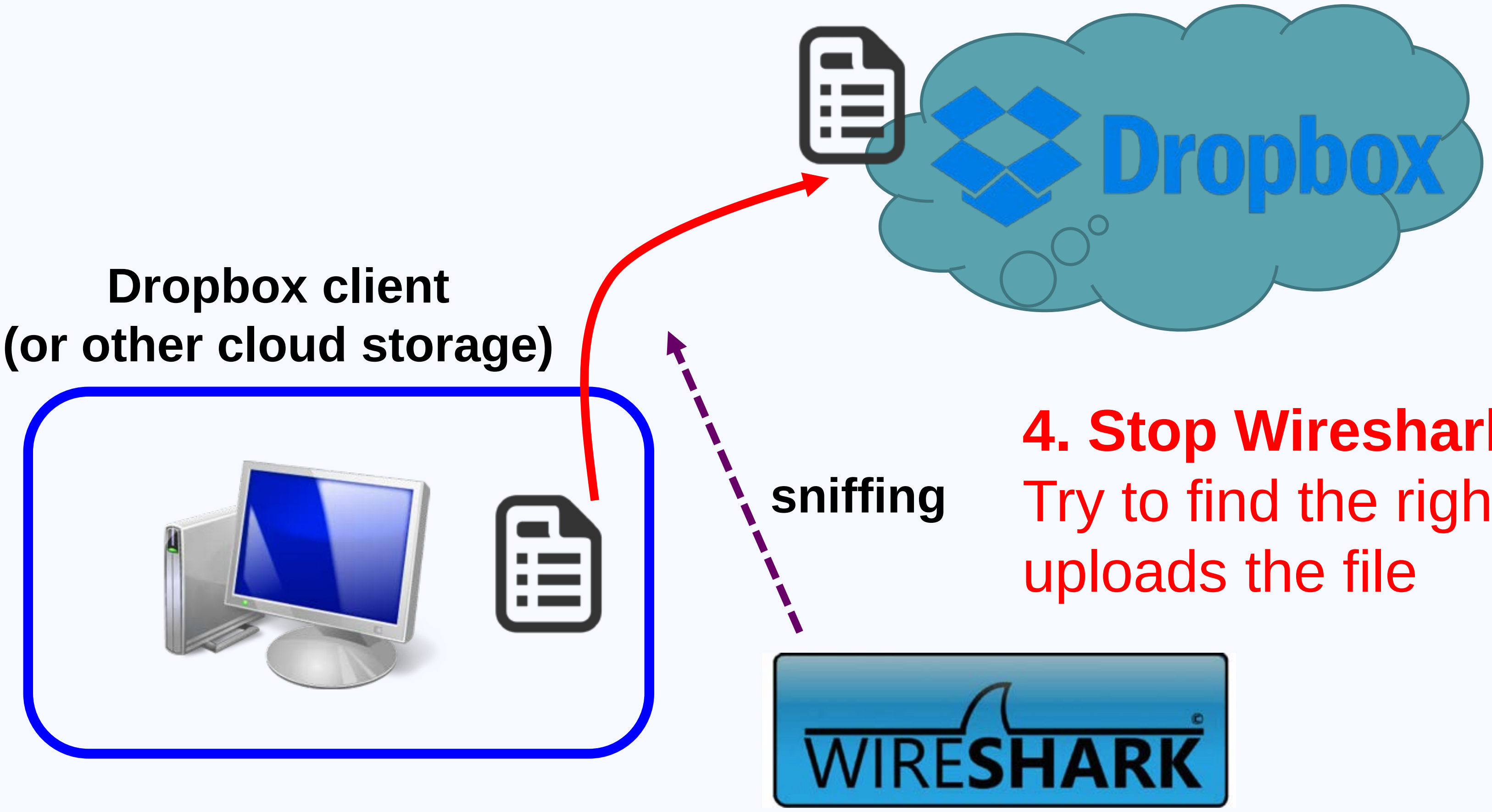


Dropbox client
(or other cloud storage)

sniffing

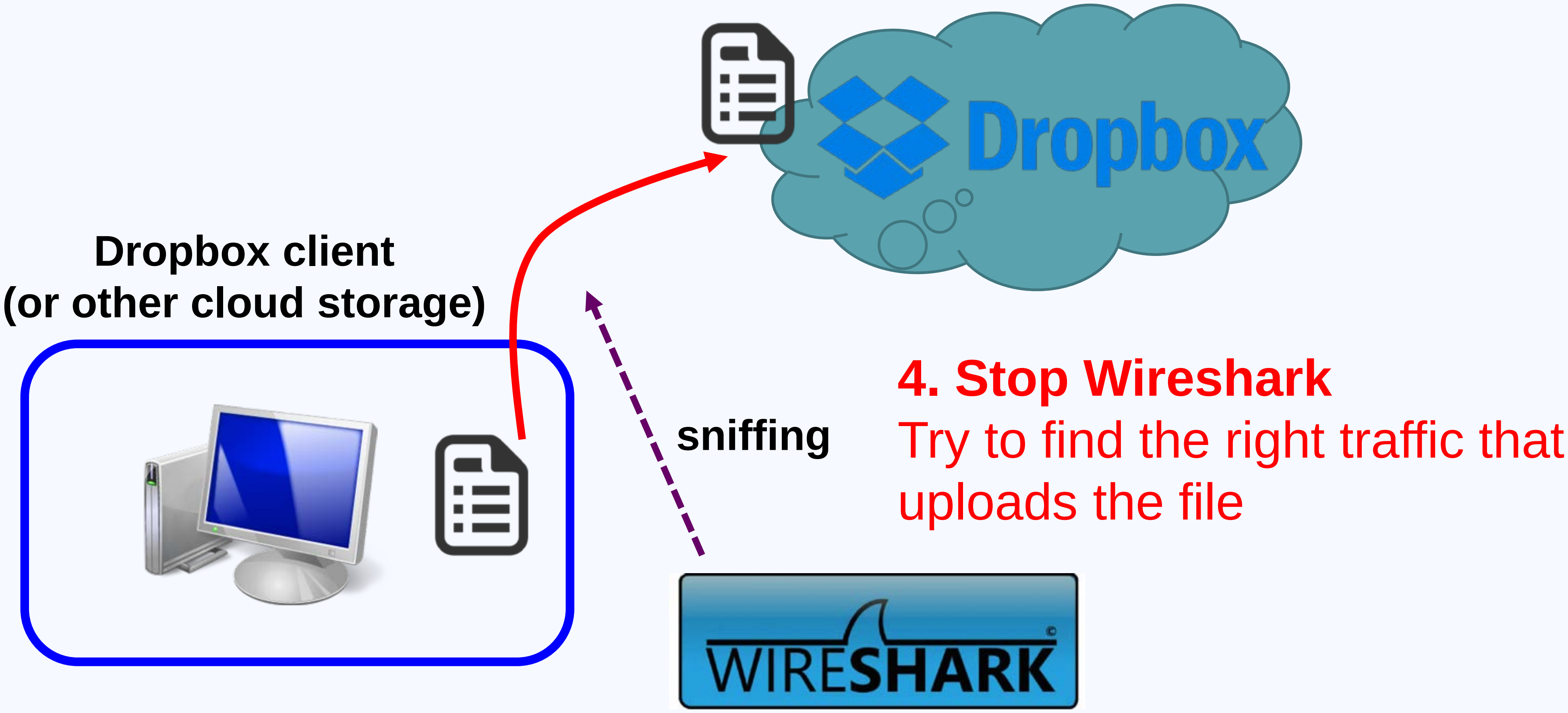
3. Add a file into the client
(wait for file synchronization to the cloud)

TASK 2- Capture Dropbox Operations (Table 2)



4. Stop Wireshark
Try to find the right traffic that uploads the file

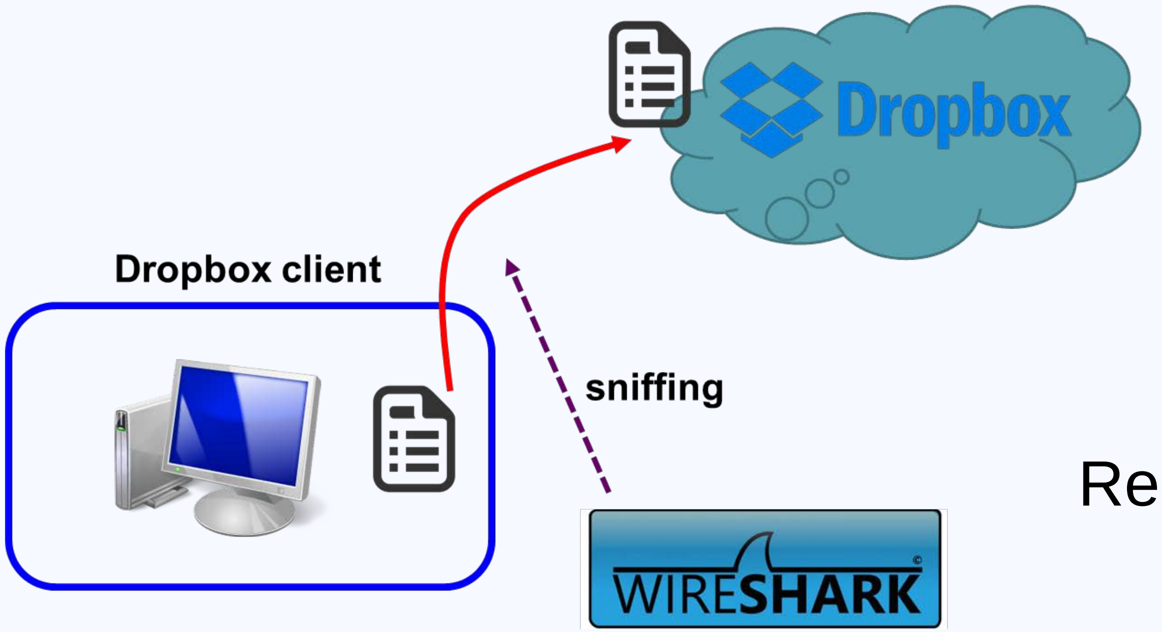
TASK 2- Capture Dropbox Operations (Table 2)



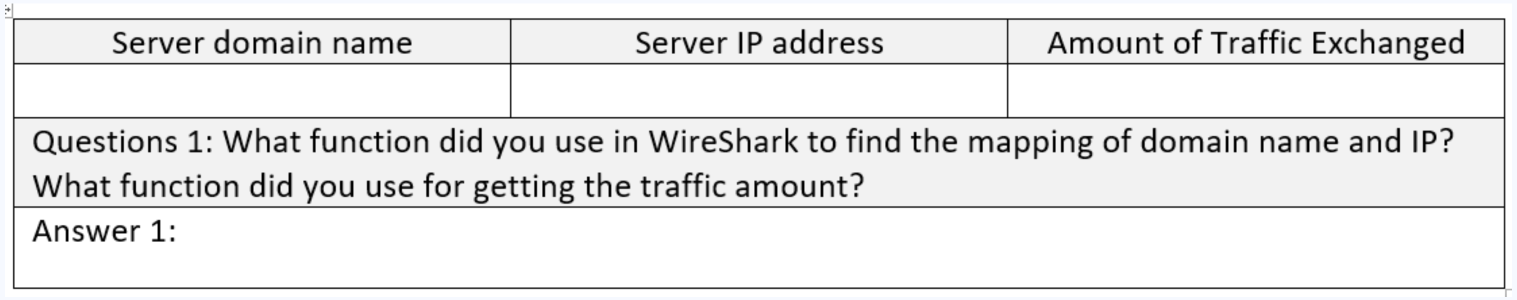
4. Stop Wireshark

Try to find the right traffic that uploads the file

TASK 2- Capture Dropbox Operations (Table 2)

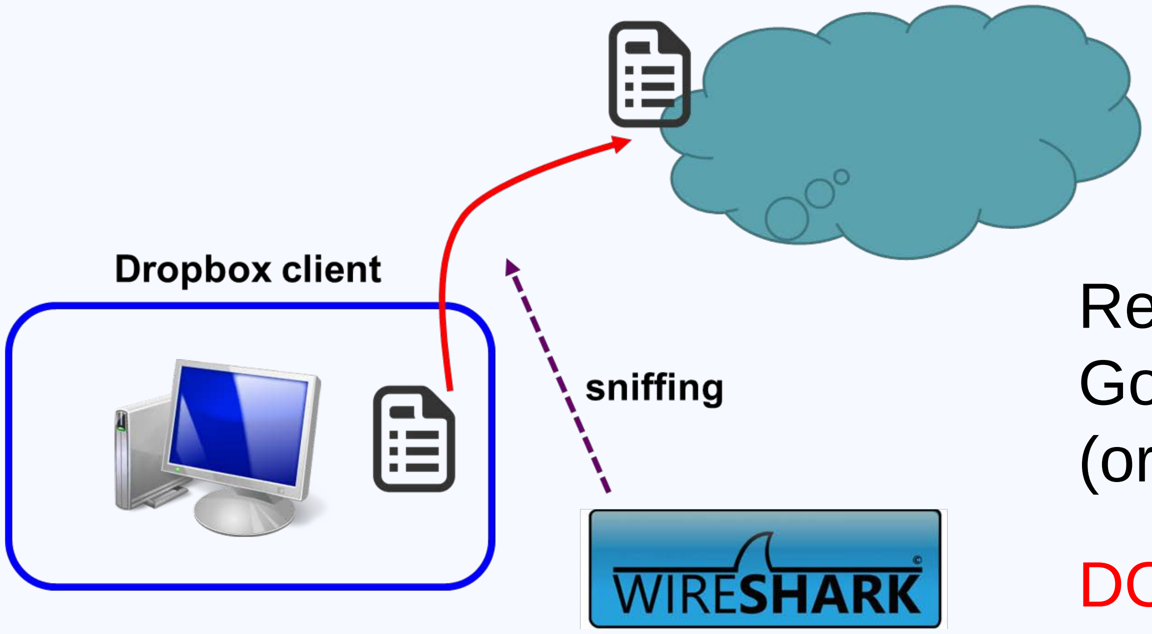


Record the result in your report



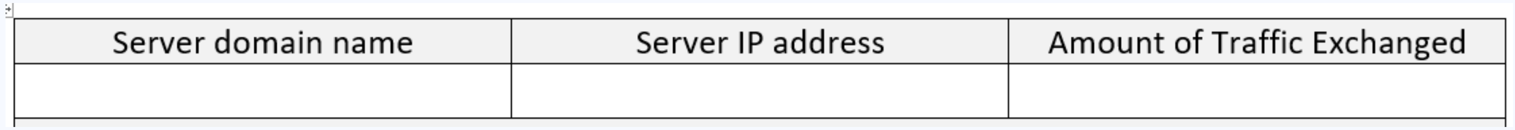
Server domain name	Server IP address	Amount of Traffic Exchanged
Questions 1: What function did you use in WireShark to find the mapping of domain name and IP? What function did you use for getting the traffic amount?		
Answer 1:		

TASK 2.2- Capture Google Drive Operations (Table 3)



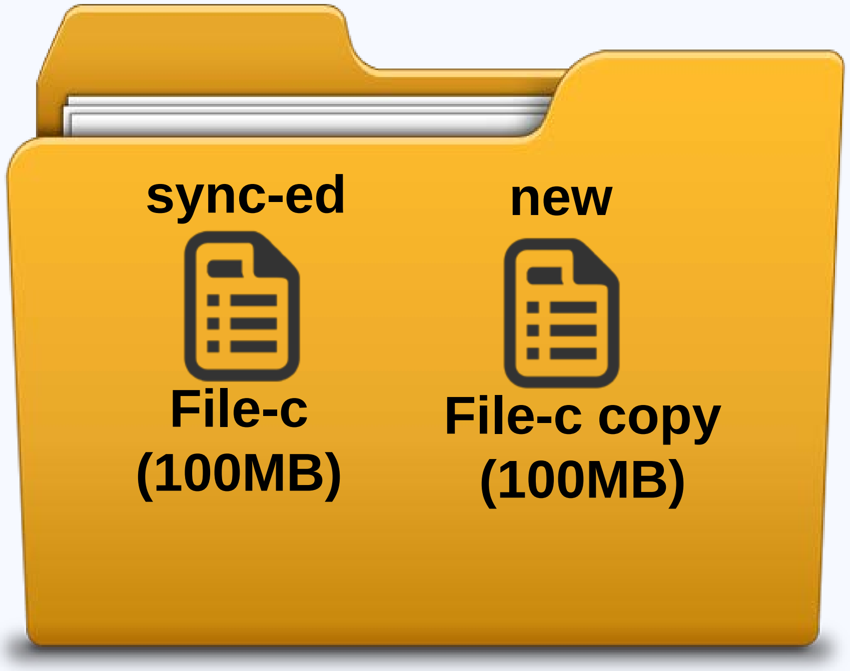
Repeat previous steps with Google Drive
(or another cloud storage)

DO NOT USE the browser!!!



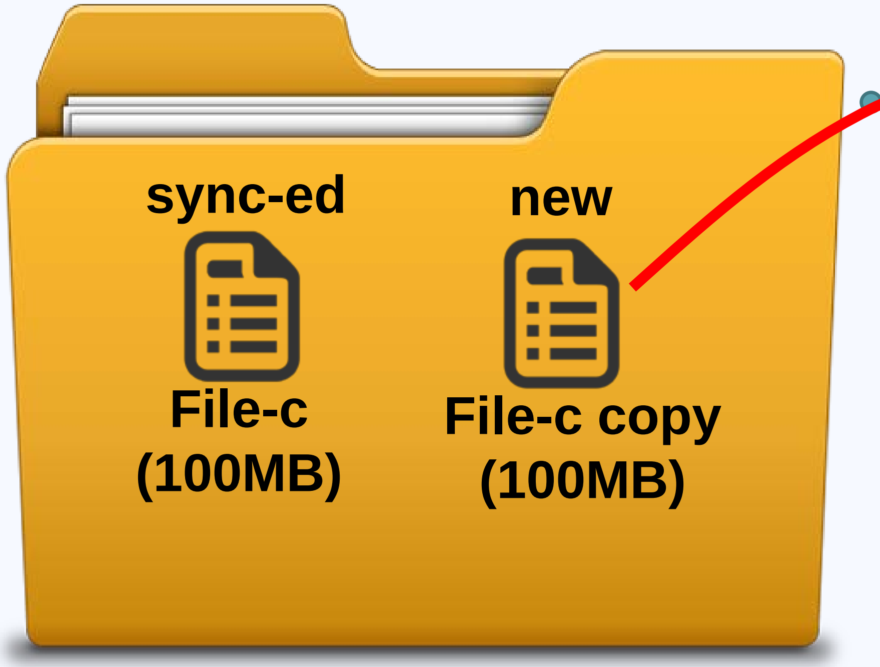
Server domain name	Server IP address	Amount of Traffic Exchanged

TASK 3- Dropbox and GoogleDrive Comparison (Table 4)



1. **Put a 100MB file in the client**
2. **Start Wireshark**
3. **Copy the file and paste in the same folder**
4. **Wait for the synchronization**
5. **Stop Wireshark**

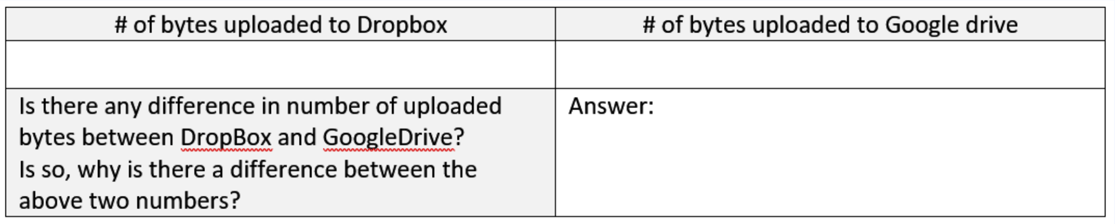
TASK 3- Dropbox and GoogleDrive Comparison (Table 4)



Google Drive
Dropbox

how many bytes transferred?

You'll find <u>something different</u> between the two cloud service.



# of bytes uploaded to Dropbox	# of bytes uploaded to Google drive
Is there any difference in number of uploaded bytes between DropBox and GoogleDrive? Is so, why is there a difference between the above two numbers?	Answer:

NOTE!

- You can use other cloud service for this lab.

e.g.百度网盘, 腾讯微云

- **Please avoid VPN**, because the packet capturing may show the VPN information instead of the cloud services.