Protocol Analysis

Wireshark Lab

Requirements: webserver as target

Work on in lab, or as homework (using your IP address)

- Protocol/Packet/Network Analyzers (aka Network Sniffers) capture and decode network traffic
- Captures can be saved for later review (.pcap)
  - Analyze network problems
  - Debug client/server problems [Coder tool]
  - Monitor malware activity
- Wireshark is free www.wireshark.org
  - Multiple platforms w32, w64, OS x
  - Wireshark works on most wireless LANs
  - Wireshark can capture raw USB and Bluetooth traffic
- Microsoft Network Monitor is another free protocol analyzer

Protocol Analysis

Learning Objectives

Upon completion of this exercise, students will be able to demonstrate:

- How to use a protocol analyzer to capture network traffic
- How a TCP segment is constructed and explain the segment fields
- How a TCP segment is constructed and explain the segment fields
- How to interpret packet decodes for protocols and applications

Additional Resources

Video Tutorials & Docs. at: http://www.wireshark.org/docs/

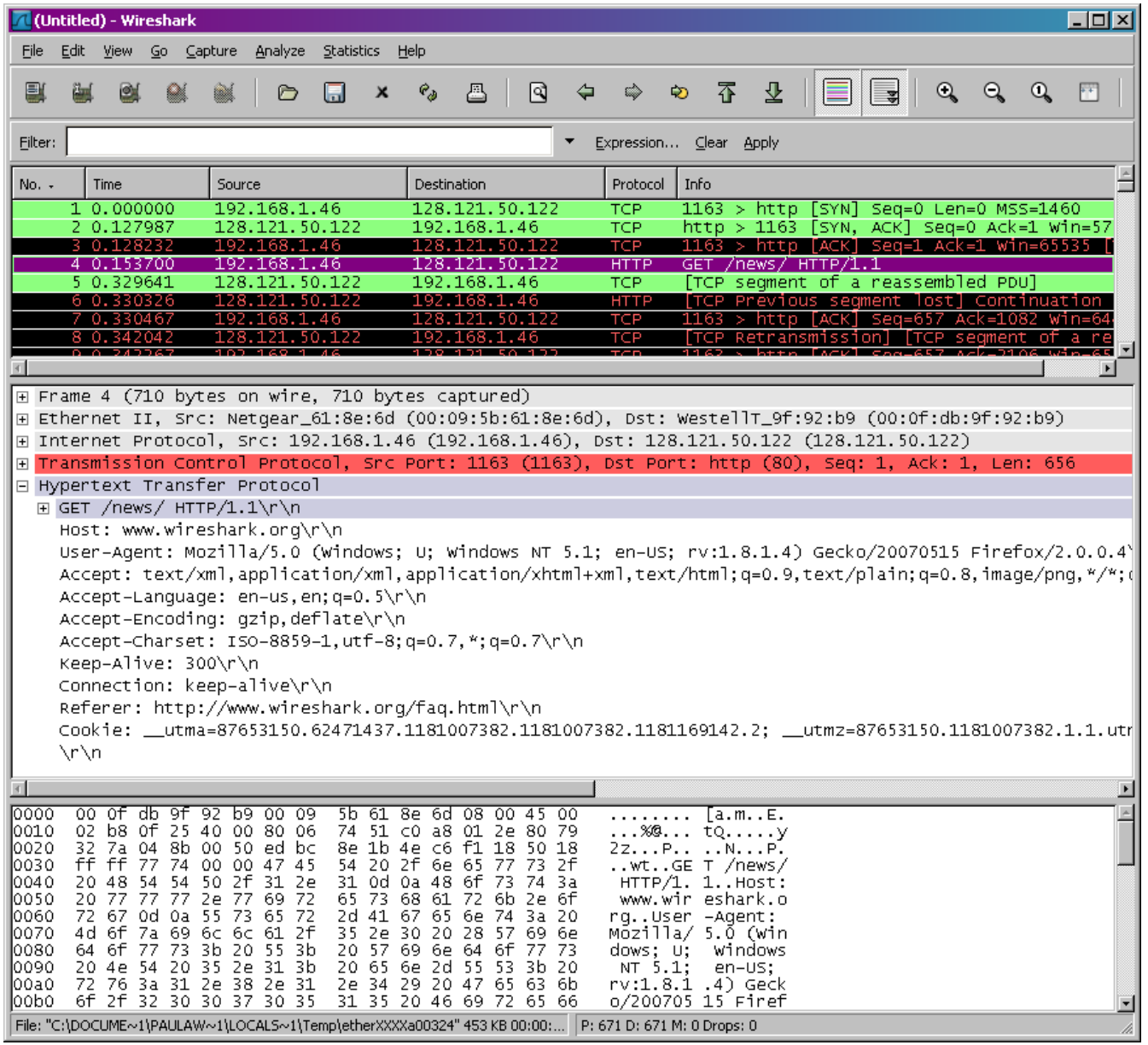
- Introduction to Wireshark
- The Case of the Missing Download
- The Case of the Slow Network
- The Case of the Slow Web Server
- Lab Configuration

Packet Analysis

List of packets captured

Details of the selected packet header

Contents of the packet in hexadecimal and ASCII

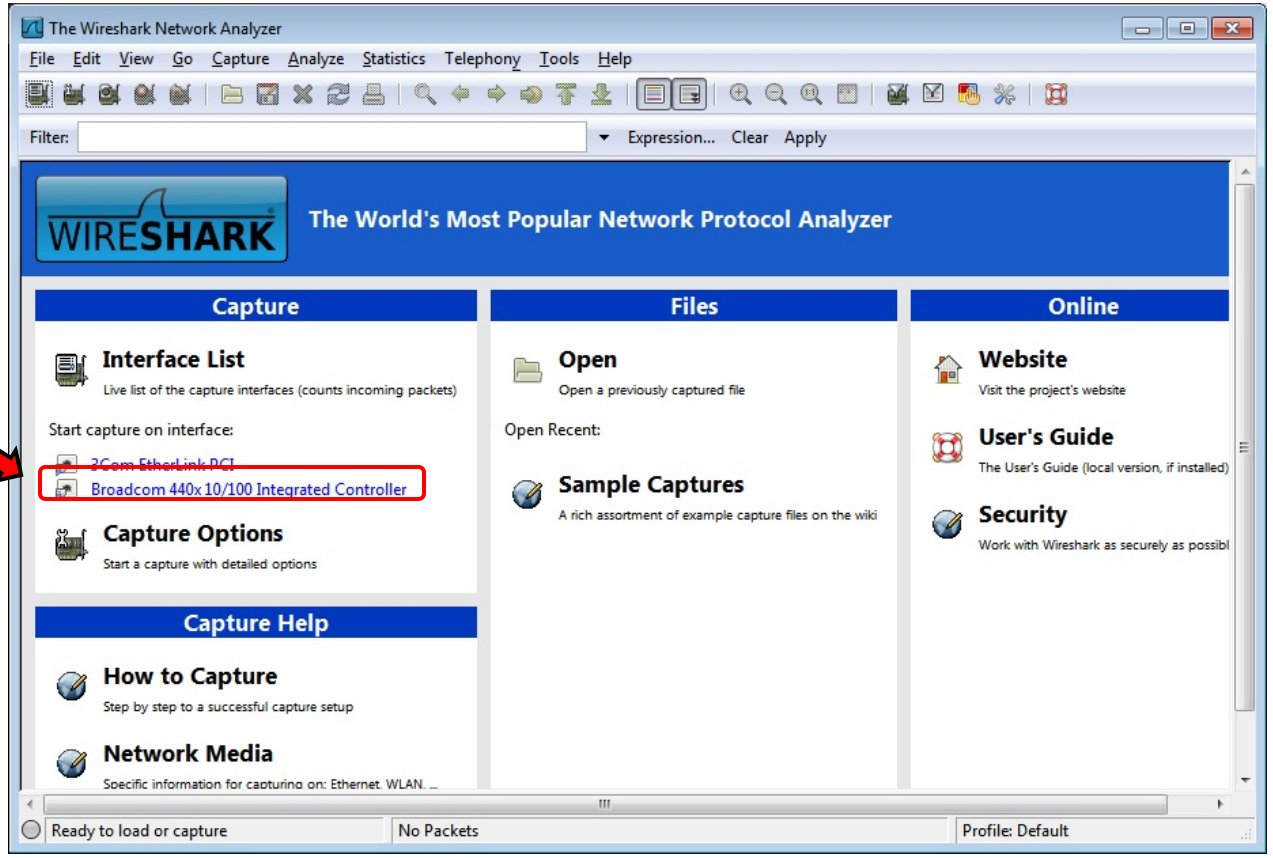


Protocol Analysis

Use either the Windows 7 partition or boot from a BackTrack DVD
Note: Lab computers have multiple network cards – only the built in NIC (eth0) is connected. Verify that the computer has a correct network address, BackTrack will need to be manually configured.
If there is no shortcut, look for Wireshark in c:\tools

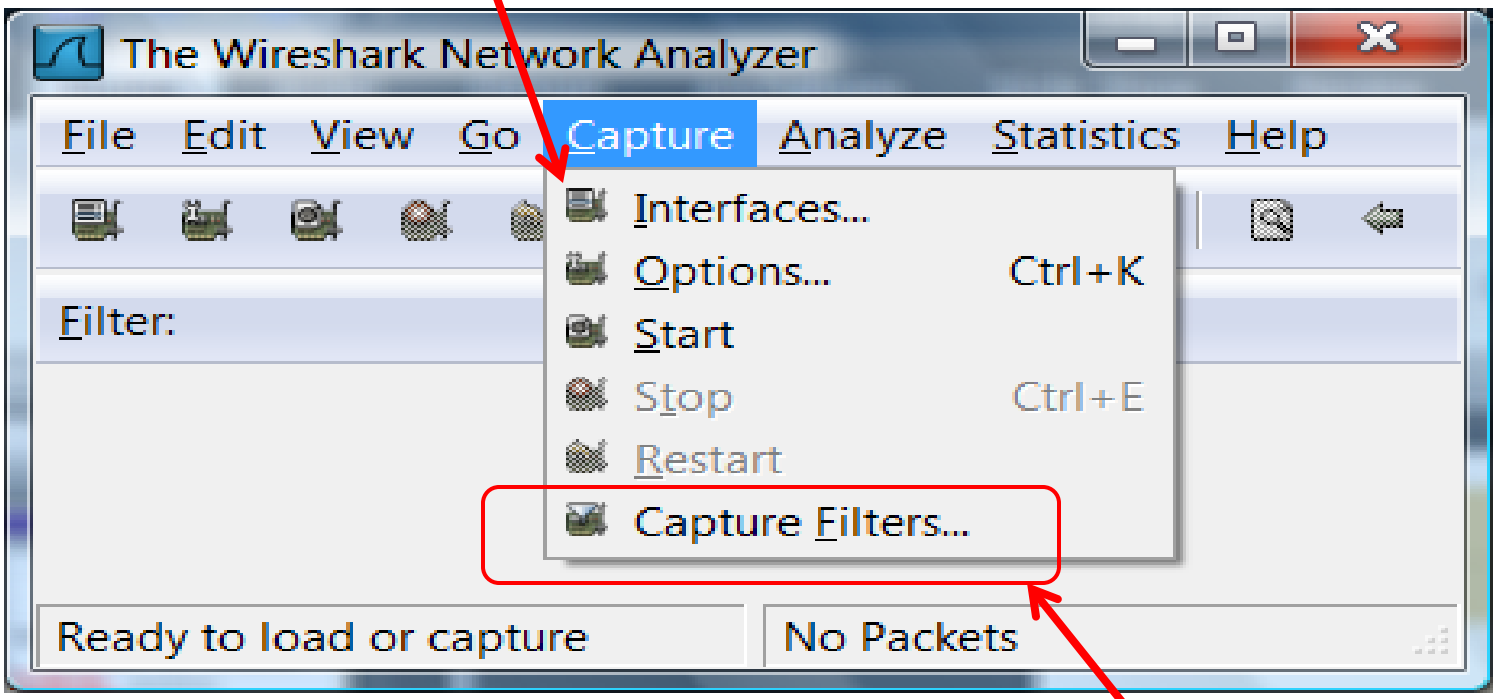
Use built-in NIC

Shortcuts to start capturing



Protocol Analysis

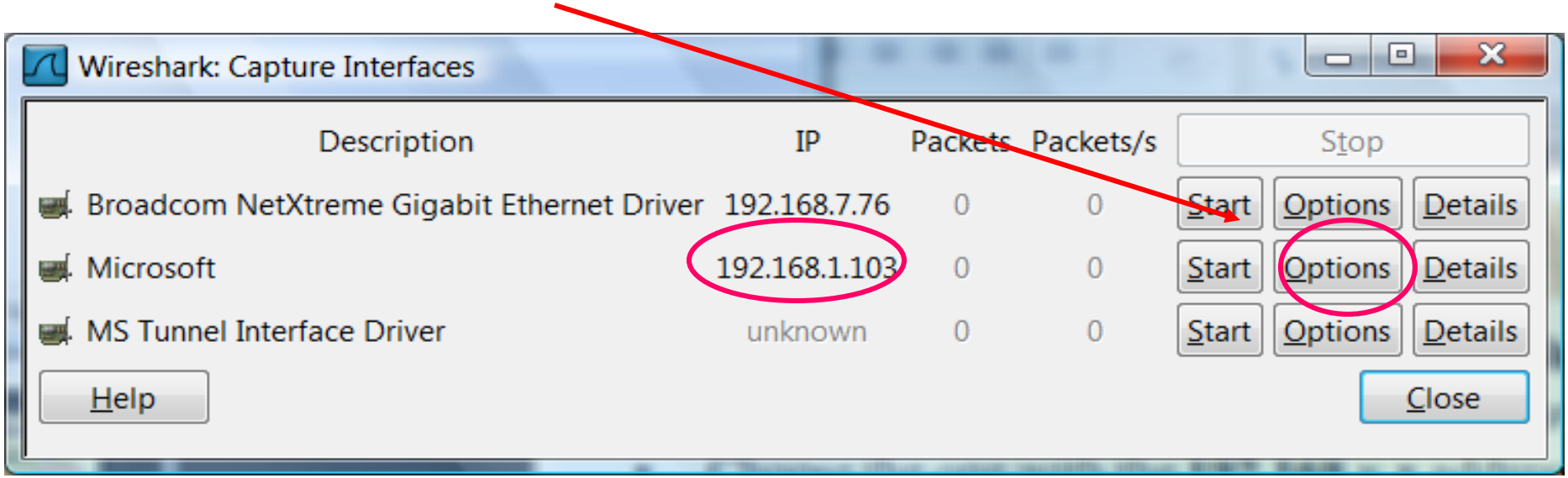
- You can also use the menu for starting captures
  - Start Wireshark
  - Select Capture/Interfaces



Explore how filters work – then set them here

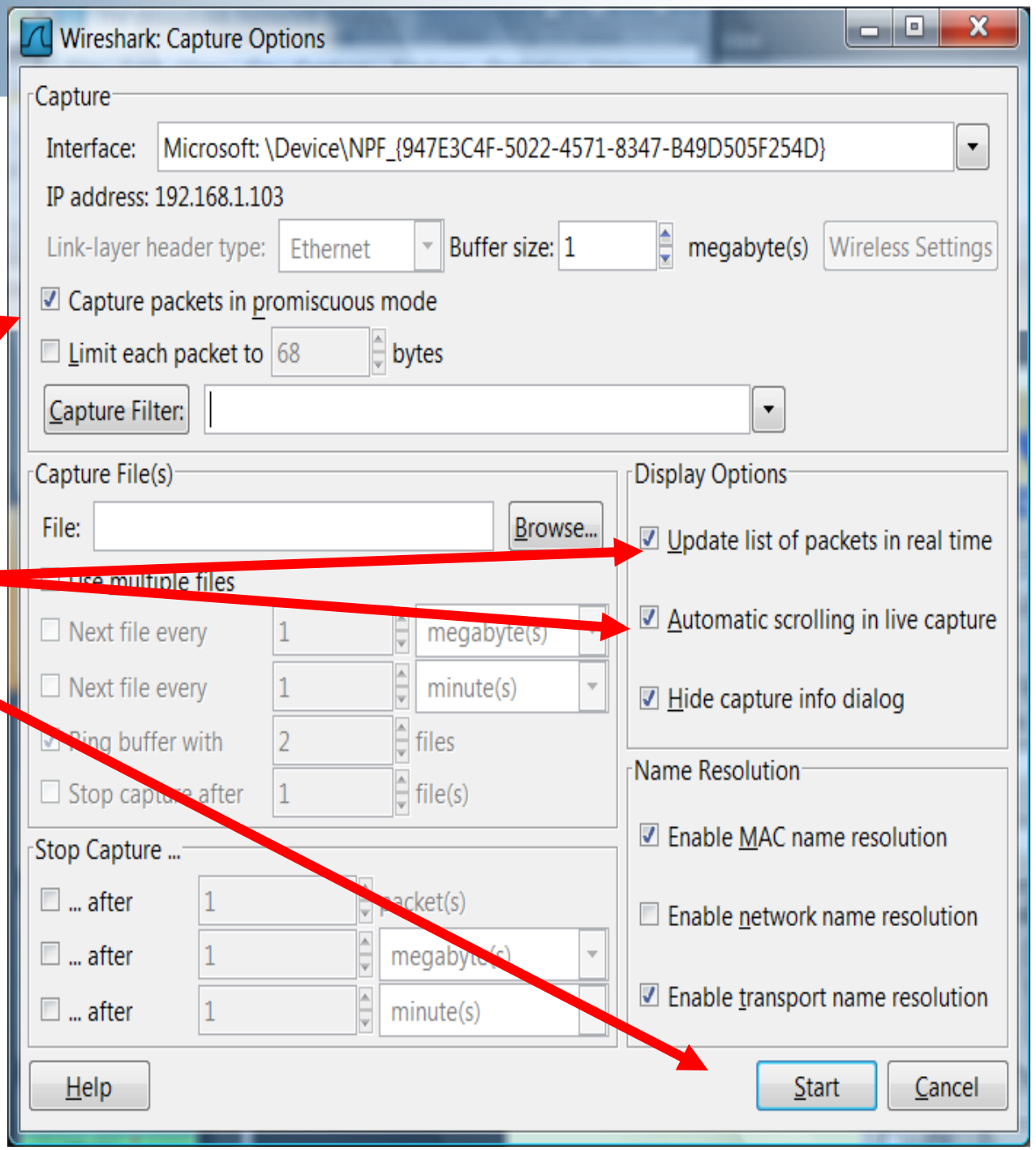
Protocol Analysis

- Make sure the lab computer has a 192.168.11.x address
- Select the interface with that address in Wireshark
- The names of the network interfaces will vary!
- Choose the one with the 192.168.11.x address
- If in doubt, ask! x = 101 to 199
- Click on the Options for that interface



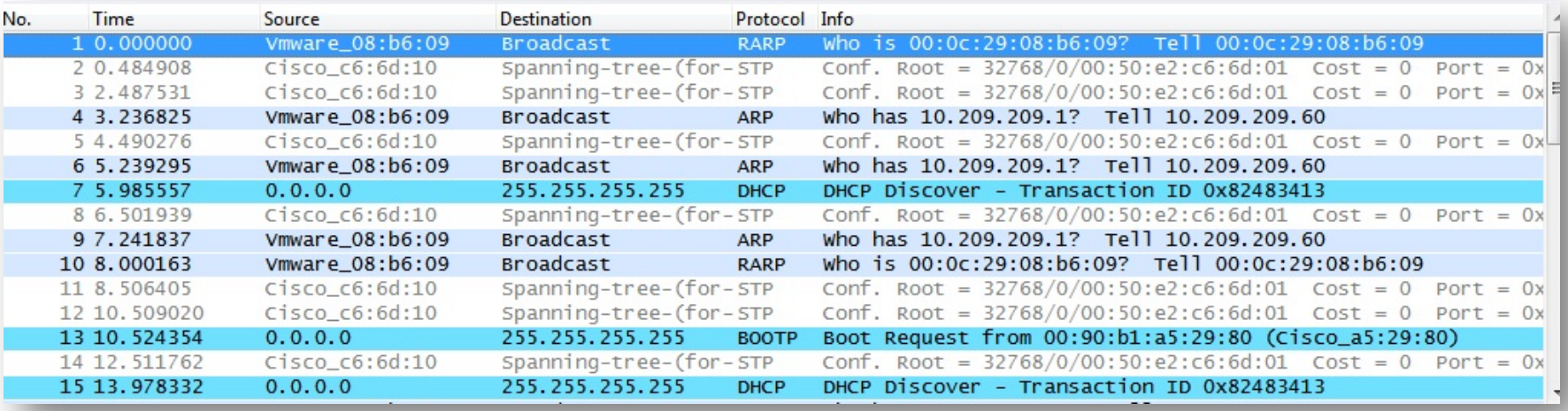
This window appears:

- “Capture packets in promiscuous mode” is set by default
- Check these
- Click on Start



Protocol Analysis

- Wireshark uses the NIC in promiscuous mode, e.g. the NIC will pass all traffic on the wire to Wireshark
- Filters can help improve the signal to noise ratio
- The below example of lab traffic shows:
  - A VM with an incorrect static IP
  - DHCP requests – but no server is running to reply
  - Cisco spanning tree protocol
  - Collectively: *Noise* Filters reduce noise



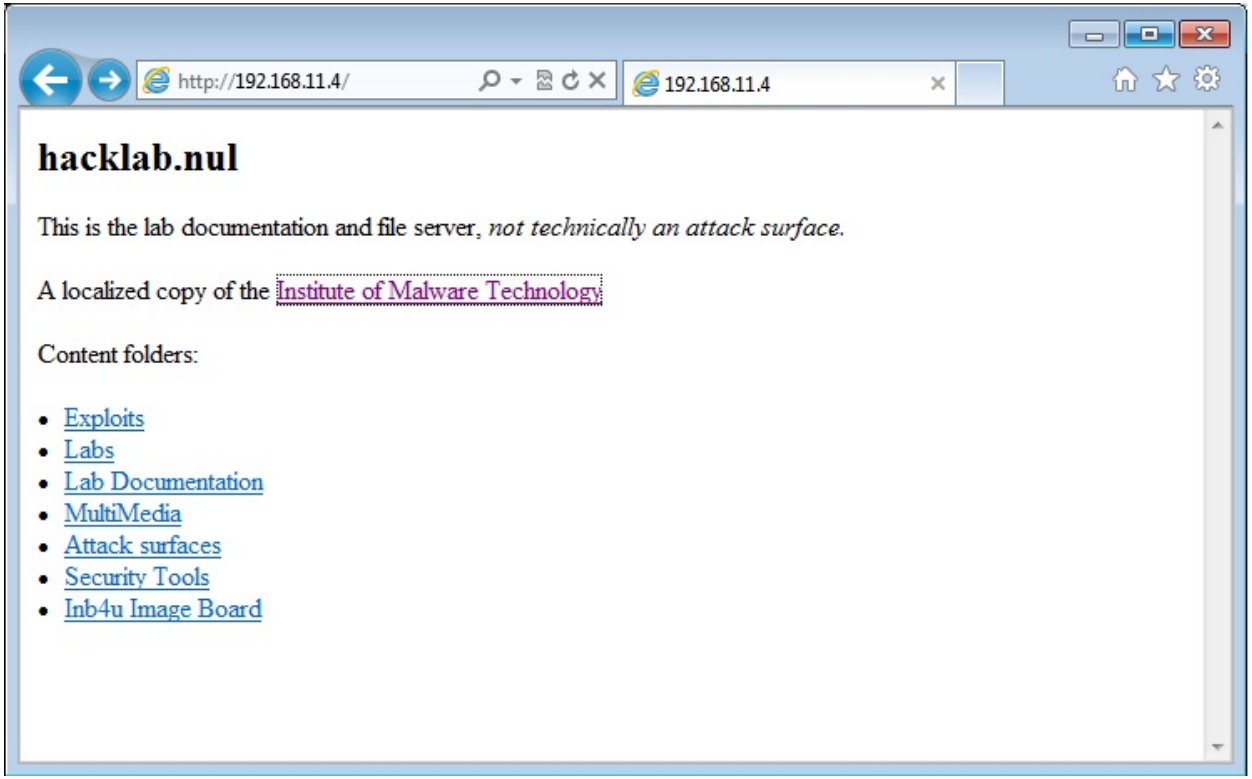
No.	Time	Source	Destination	Protocol	Info
1	0.000000	Vmware_08:b6:09	Broadcast	RARP	Who is 00:0c:29:08:b6:09? Tell 00:0c:29:08:b6:09
2	0.484908	Cisco_c6:6d:10	Spanning-tree-(for-	STP	Conf. Root = 32768/0/00:50:e2:c6:6d:01 Cost = 0 Port = 0x
3	2.487531	Cisco_c6:6d:10	Spanning-tree-(for-	STP	Conf. Root = 32768/0/00:50:e2:c6:6d:01 Cost = 0 Port = 0x
4	3.236825	Vmware_08:b6:09	Broadcast	ARP	Who has 10.209.209.1? Tell 10.209.209.60
5	4.490276	Cisco_c6:6d:10	Spanning-tree-(for-	STP	Conf. Root = 32768/0/00:50:e2:c6:6d:01 Cost = 0 Port = 0x
6	5.239295	Vmware_08:b6:09	Broadcast	ARP	Who has 10.209.209.1? Tell 10.209.209.60
7	5.985557	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x82483413
8	6.501939	Cisco_c6:6d:10	Spanning-tree-(for-	STP	Conf. Root = 32768/0/00:50:e2:c6:6d:01 Cost = 0 Port = 0x
9	7.241837	Vmware_08:b6:09	Broadcast	ARP	Who has 10.209.209.1? Tell 10.209.209.60
10	8.000163	Vmware_08:b6:09	Broadcast	RARP	Who is 00:0c:29:08:b6:09? Tell 00:0c:29:08:b6:09
11	8.506405	Cisco_c6:6d:10	Spanning-tree-(for-	STP	Conf. Root = 32768/0/00:50:e2:c6:6d:01 Cost = 0 Port = 0x
12	10.509020	Cisco_c6:6d:10	Spanning-tree-(for-	STP	Conf. Root = 32768/0/00:50:e2:c6:6d:01 Cost = 0 Port = 0x
13	10.524354	0.0.0.0	255.255.255.255	BOOTP	Boot Request from 00:90:b1:a5:29:80 (Cisco_a5:29:80)
14	12.511762	Cisco_c6:6d:10	Spanning-tree-(for-	STP	Conf. Root = 32768/0/00:50:e2:c6:6d:01 Cost = 0 Port = 0x
15	13.978332	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x82483413

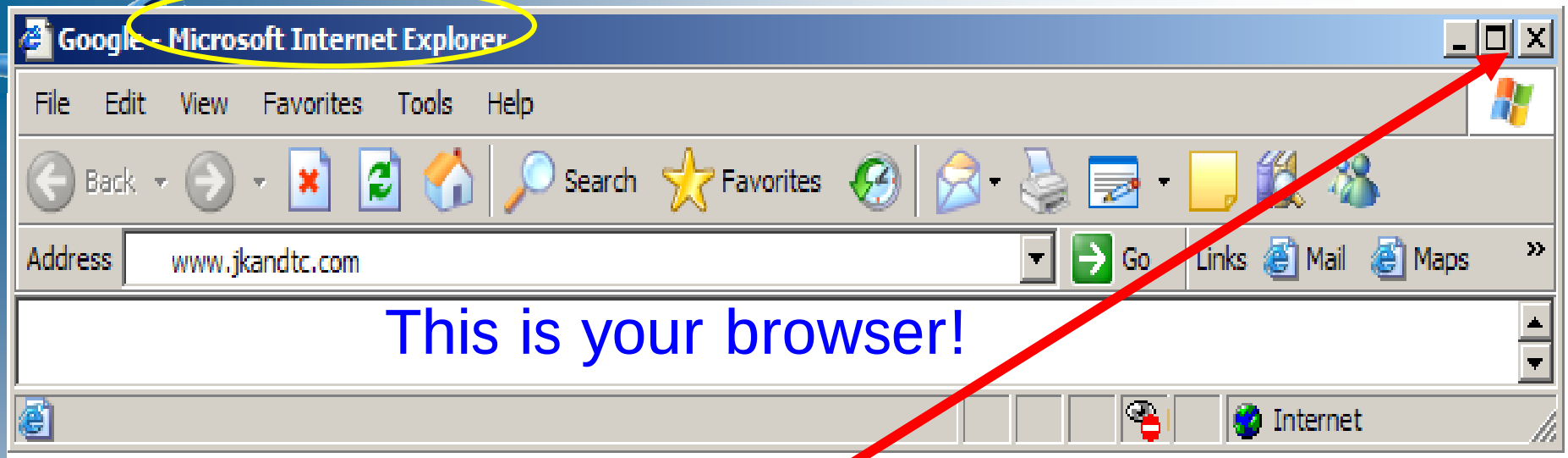
Protocol Analysis

You need a webserver to establish a TCP connection with

Use the webserver at 192.168.11.4

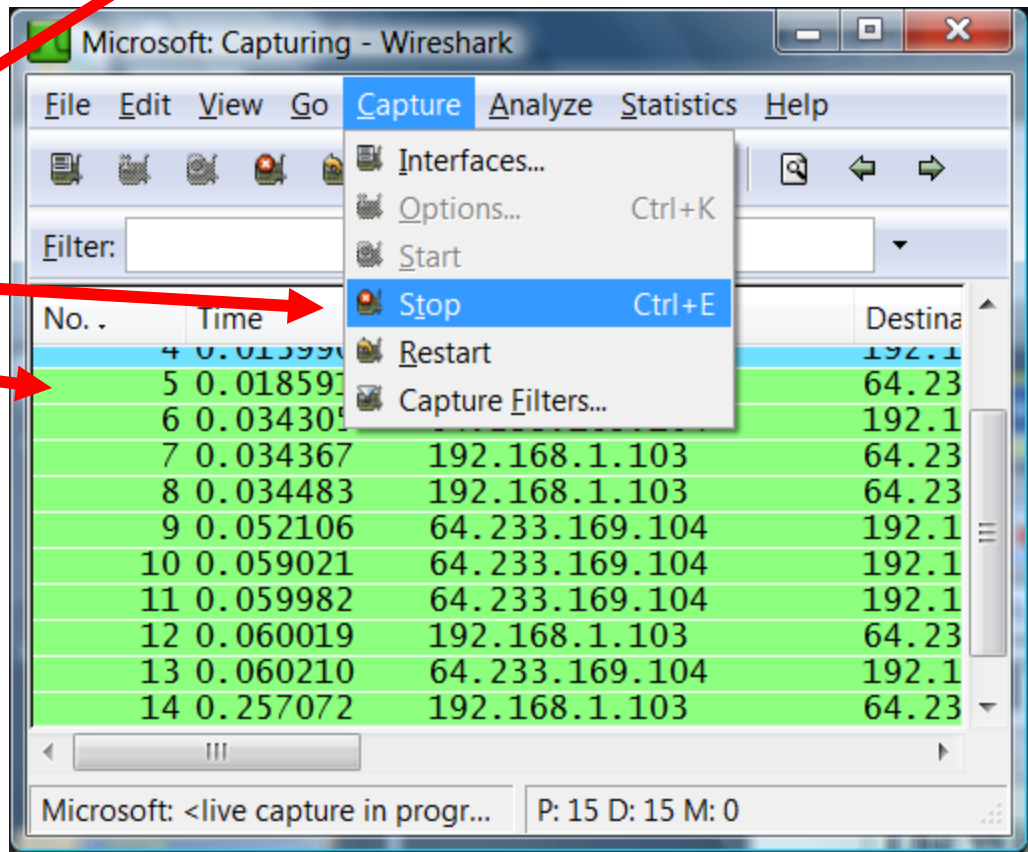
If homework – use any webserver

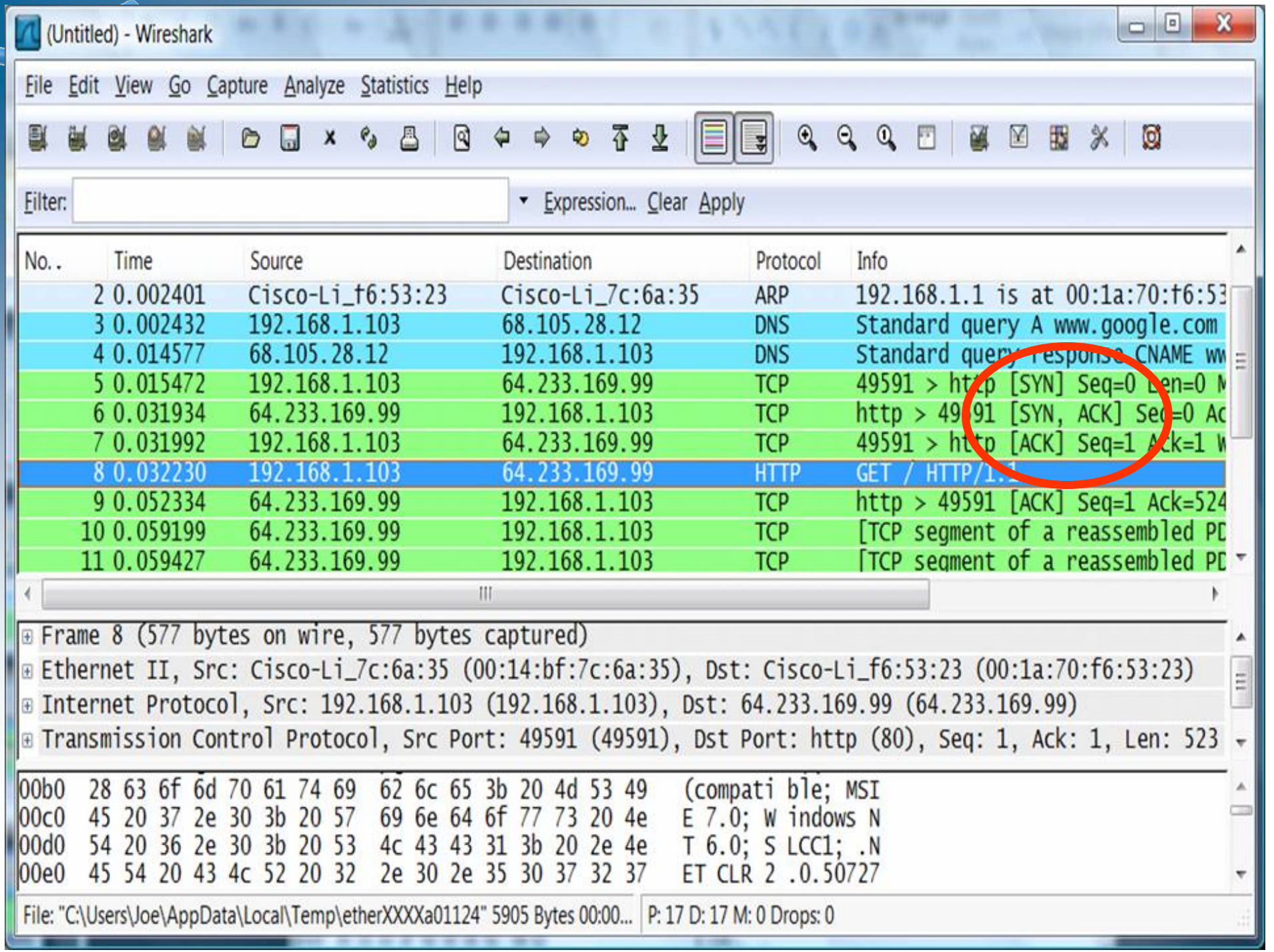


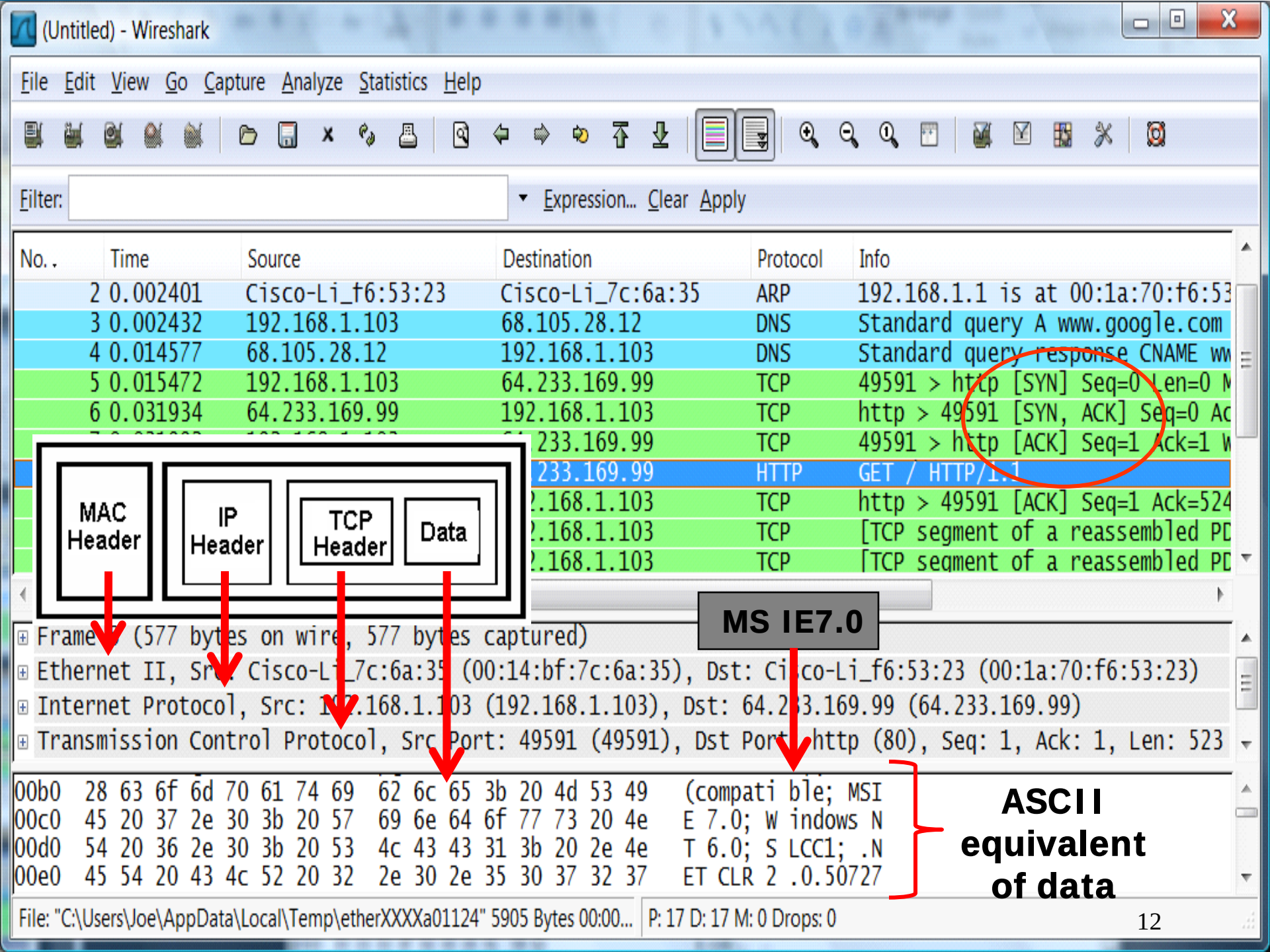


- Once 'capture' window appears
- Open up a web browser
- Visit: *
- Close the website (x)
- Click on Capture/Stop
- Results window appears

- See lab assistant ..it will be a webserver in the target address range – use it's IP address

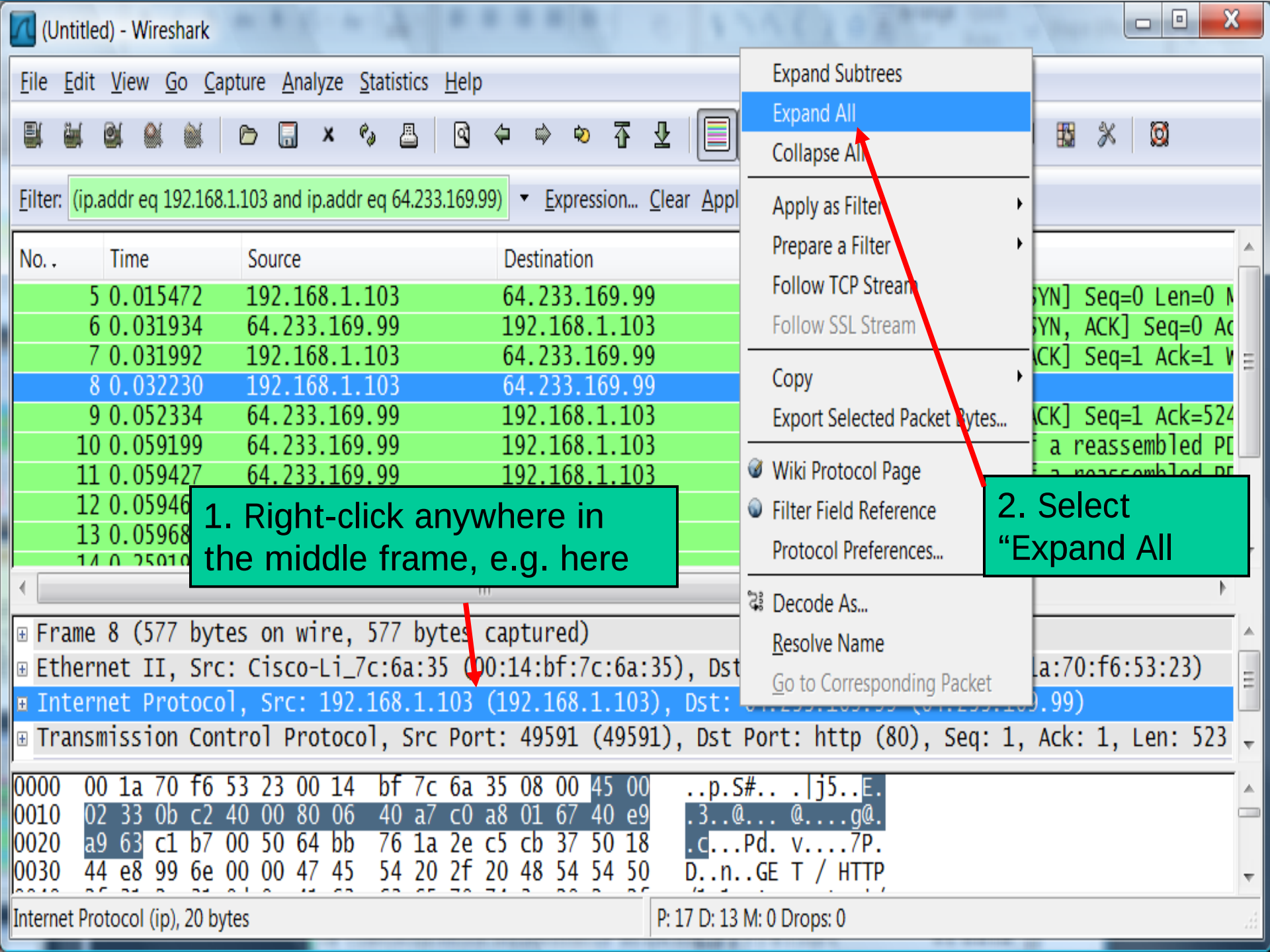


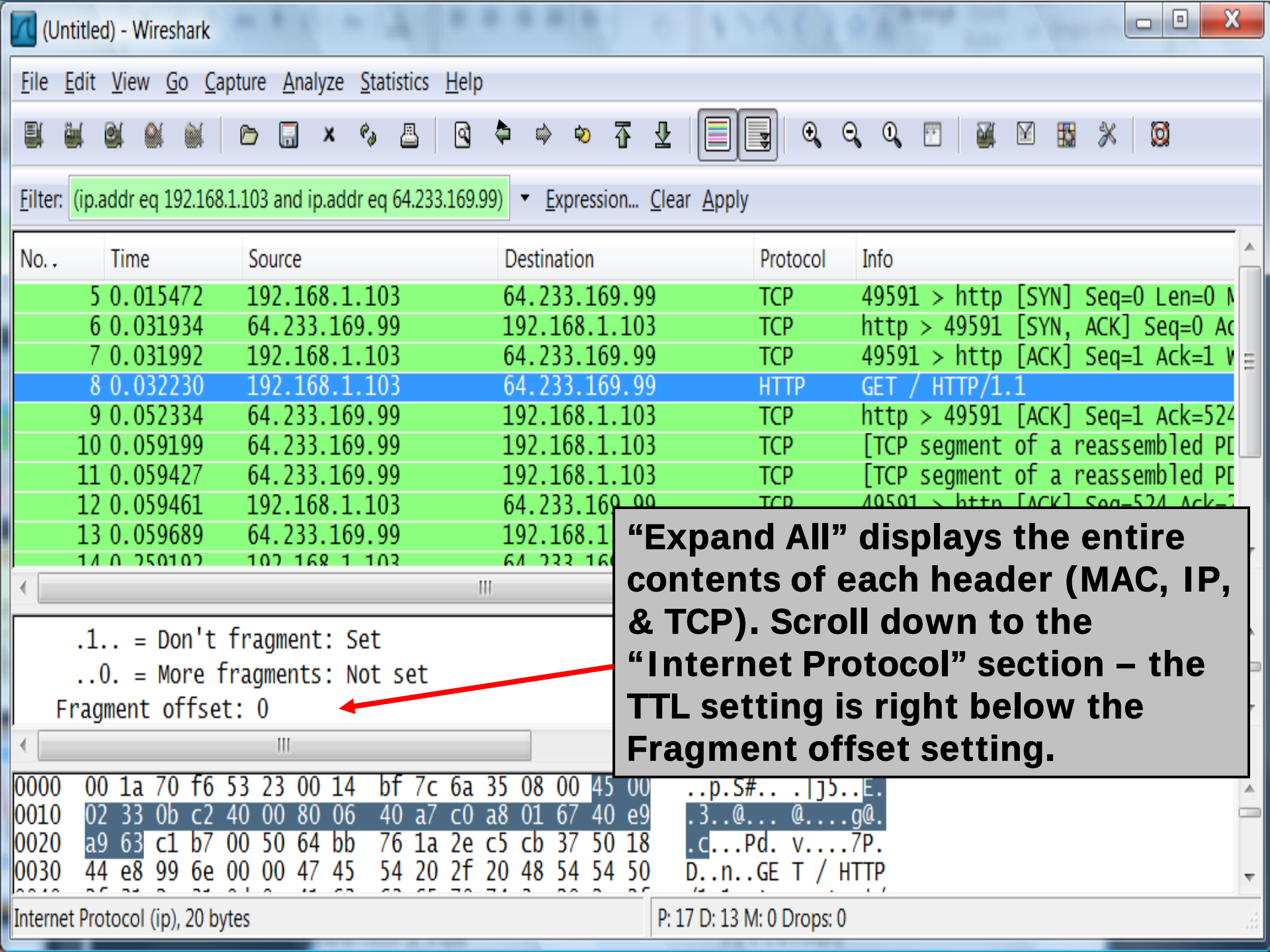

(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
2 0.002401 Cisco-Li_f6:53:23 Cisco-Li_7c:6a:35 ARP 192.168.1.1 is at 00:1a:70:f6:53
3 0.002432 192.168.1.103 68.105.28.12 DNS Standard query A www.google.com
4 0.014577 68.105.28.12 192.168.1.103 DNS Standard query response CNAME ww
5 0.015472 192.168.1.103 64.233.169.99 TCP 49591 > http [SYN] Seq=0 Len=0 M
6 0.031934 64.233.169.99 192.168.1.103 TCP http > 49591 [SYN, ACK] Seq=0 Ac
7 0.031992 192.168.1.103 64.233.169.99 TCP 49591 > http [ACK] Seq=1 Ack=1 W
8 0.032230 192.168.1.103 64.233.169.99 HTTP GET / HTTP/1.1
9 0.052334 64.233.169.99 192.168.1.103 TCP http > 49591 [ACK] Seq=1 Ack=524
10 0.059199 64.233.169.99 192.168.1.103 TCP [TCP segment of a reassembled PD
11 0.059427 64.233.169.99 192.168.1.103 TCP [TCP segment of a reassembled PD
Frame 8 (577 bytes on wire, 577 bytes captured)
Ethernet II, Src: Cisco-Li_7c:6a:35 (00:14:bf:7c:6a:35), Dst: Cisco-Li_f6:53:23 (00:1a:70:f6:53:23)
Internet Protocol, Src: 192.168.1.103 (192.168.1.103), Dst: 64.233.169.99 (64.233.169.99)
Transmission Control Protocol, Src Port: 49591 (49591), Dst Port: http (80), Seq: 1, Ack: 1, Len: 523
00b0 28 63 6f 6d 70 61 74 69 62 6c 65 3b 20 4d 53 49 (compati ble; MSI
00c0 45 20 37 2e 30 3b 20 57 69 6e 64 6f 77 73 20 4e E 7.0; W indows N
00d0 54 20 36 2e 30 3b 20 53 4c 43 43 31 3b 20 2e 4e T 6.0; S LCC1; .N
00e0 45 54 20 43 4c 52 20 32 2e 30 2e 35 30 37 32 37 ET CLR 2 .0.50727
File: "C:\Users\Joe\AppData\Local\Temp\etherXXXXa01124" 5905 Bytes 00:00...
P: 17 D: 17 M: 0 Drops: 0


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
2 0.002401 Cisco-Li_f6:53:23 Cisco-Li_7c:6a:35 ARP 192.168.1.1 is at 00:1a:70:f6:53
3 0.002432 192.168.1.103 68.105.28.12 DNS Standard query A www.google.com
4 0.014577 68.105.28.12 192.168.1.103 DNS Standard query response CNAME ww
5 0.015472 192.168.1.103 64.233.169.99 TCP 49591 > http [SYN] Seq=0 Len=0 M
6 0.031934 64.233.169.99 192.168.1.103 TCP http > 49591 [SYN, ACK] Seq=0 Ac
TCP 49591 > http [ACK] Seq=1 Ack=1 W
HTTP GET / HTTP/1.1
TCP http > 49591 [ACK] Seq=1 Ack=524
TCP [TCP segment of a reassembled PD
TCP [TCP segment of a reassembled PD
MAC Header
IP Header
TCP Header
Data
MS IE7.0
Frame (577 bytes on wire, 577 bytes captured)
Ethernet II, Src: Cisco-Li_7c:6a:35 (00:14:bf:7c:6a:35), Dst: Cisco-Li_f6:53:23 (00:1a:70:f6:53:23)
Internet Protocol, Src: 192.168.1.103 (192.168.1.103), Dst: 64.233.169.99 (64.233.169.99)
Transmission Control Protocol, Src Port: 49591 (49591), Dst Port: http (80), Seq: 1, Ack: 1, Len: 523
00b0 28 63 6f 6d 70 61 74 69 62 6c 65 3b 20 4d 53 49 (compati ble; MSI
00c0 45 20 37 2e 30 3b 20 57 69 6e 64 6f 77 73 20 4e E 7.0; W indows N
00d0 54 20 36 2e 30 3b 20 53 4c 43 43 31 3b 20 2e 4e T 6.0; S LCC1; .N
00e0 45 54 20 43 4c 52 20 32 2e 30 2e 35 30 37 32 37 ET CLR 2 .0.50727
ASCII equivalent of data
File: "C:\Users\Joe\AppData\Local\Temp\etherXXXXa01124" 5905 Bytes 00:00...
P: 17 D: 17 M: 0 Drops: 0

Protocol Analysis

- **Select the SYN packet**
- In the middle frame, see: **Frame** & **Ethernet** sections
  - Here find the source (your) MAC address
  - Look for something like 00:11:43:a8:0c:22
- An **Internet Protocol** section
  - Find the value of the “Time to live” (TTL) flag
  - What is the value?
- A **Transmission Control Protocol** section
- Here find the Header Length (it’s not 20 bytes – what was added in the Options field? Hint: Your client is telling the server something.)
- Repeat, looking at SYN-ACK packet sent by server
- Note: Maximum Segment Size (MSS) = largest packet you can send


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: (ip.addr eq 192.168.1.103 and ip.addr eq 64.233.169.99)
Expression... Clear Appl
No. . Time Source Destination
5 0.015472 192.168.1.103 64.233.169.99
6 0.031934 64.233.169.99 192.168.1.103
7 0.031992 192.168.1.103 64.233.169.99
8 0.032230 192.168.1.103 64.233.169.99
9 0.052334 64.233.169.99 192.168.1.103
10 0.059199 64.233.169.99 192.168.1.103
11 0.059427 64.233.169.99 192.168.1.103
12 0.05946
13 0.05968
Expand Subtrees
Expand All
Collapse All
Apply as Filter
Prepare a Filter
Follow TCP Stream
Follow SSL Stream
Copy
Export Selected Packet Bytes...
Wiki Protocol Page
Filter Field Reference
Protocol Preferences...
Decode As...
Resolve Name
Go to Corresponding Packet
1. Right-click anywhere in the middle frame, e.g. here
2. Select "Expand All
Frame 8 (577 bytes on wire, 577 bytes captured)
Ethernet II, Src: Cisco-Li_7c:6a:35 (00:14:bf:7c:6a:35), Dst
Internet Protocol, Src: 192.168.1.103 (192.168.1.103), Dst:
Transmission Control Protocol, Src Port: 49591 (49591), Dst Port: http (80), Seq: 1, Ack: 1, Len: 523
0000 00 1a 70 f6 53 23 00 14 bf 7c 6a 35 08 00 45 00
0010 02 33 0b c2 40 00 80 06 40 a7 c0 a8 01 67 40 e9
0020 a9 63 c1 b7 00 50 64 bb 76 1a 2e c5 cb 37 50 18
0030 44 e8 99 6e 00 00 47 45 54 20 2f 20 48 54 54 50
Internet Protocol (ip), 20 bytes
P: 17 D: 13 M: 0 Drops: 0



"Expand All" displays the entire contents of each header (MAC, IP, & TCP). Scroll down to the "Internet Protocol" section – the TTL setting is right below the Fragment offset setting.

Lab Objectives

Easier than C++ ?

Initial Exercise

Obtain the following information:

- The source IP address
- The IP address of the Web server
- The source (your) MAC address
- The value of the IP TTL (Time to Live) field

If you have any problems finding the above
– work with the Lab Assistant

Penultimate Exercise

- Start capturing packets in Wireshark
- Ping one of the servers or lab computers
- When the Ping program is done, stop the Wireshark packet capture
- The capture window shows Ping queries and responses
  - What is the Internet Protocol number for ICMP?

Protocol Analysis

Lab Exercise (continued)

- Start capturing packets in Wireshark. Have your host send and receive several UDP packets. After stopping packet capture, set your packet filter so that only UDP packets sent and received at your host are displayed. Select one UDP packet and expand the fields in the details window.
- Select one packet. From this packet, determine how many fields there are in the UDP header. Name the fields.
- From the packet content field, determine the length (in bytes) of each of the UDP header fields.
- The value in the Length field is the length of what?
- What is the largest possible source port number? Why?
- What is the protocol number for UDP?

Lab Assignment

Name:

1. Source IP address
2. Destination IP address
3. Source MAC address
4. IP TTL
5. IP Protocol number for ICMP
6. Names of UDP header fields
7. Length of the UDP header fields (in bytes)
8. Value of length field is the length of what?
9. Value of largest possible source port number?
10. Why?
11. UDP Protocol number