ECSE 308:
Introduction to
Communication Systems and Networks

L4: IP & MAC

Tutorial: Wireshark
Part 1: IP
Part 2: Ethernet

CEAB Data – Engineering tools

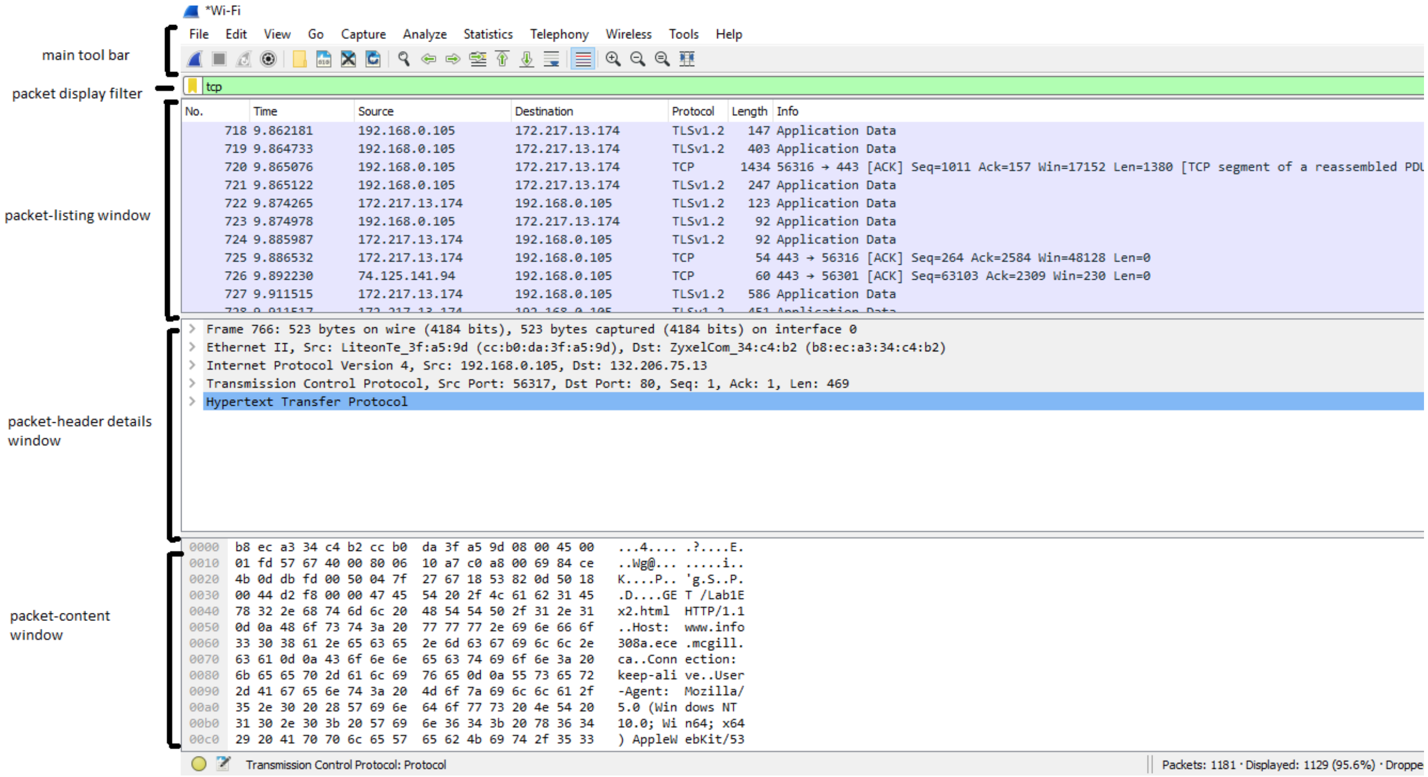
- The following engineering tools are used in this laboratory:
  - Wireshark network analyser
  - IP and ICMP protocol
  - Checksum calculation
  - Echo/reply command
  - Route tracer
  - Address resolution protocol

Wireshark: Introduction

- Wireshark is a free network packet analyzer which captures network packets and displays the contents of all fields within a packet.
- In fact, this tool allows you to observe the sequence of messages exchanged between two protocol entities which helps to obtain a deeper understanding of network protocol operations.
- This document provides information required to get Wireshark started. The contents are taken from the “Wireshark User’s Guide” available at https://www.wireshark.org/docs/wsug_html/.

Wireshark user interface: overview

- The Wireshark interface has five major components:



```
No.   Time      Source          Destination     Protocol Length Info
  718 9.862181  192.168.0.105   172.217.13.174  TLSv1.2   147 Application Data
  719 9.864733  192.168.0.105   172.217.13.174  TLSv1.2   403 Application Data
  720 9.865076  192.168.0.105   172.217.13.174  TCP      1434 56316 → 443 [ACK] Seq=1011 Ack=157 Win=17152 Len=1380 [TCP segment of a reassembled PDU
  721 9.865122  192.168.0.105   172.217.13.174  TLSv1.2   247 Application Data
  722 9.874265  172.217.13.174  192.168.0.105   TLSv1.2   123 Application Data
  723 9.874978  192.168.0.105   172.217.13.174  TLSv1.2    92 Application Data
  724 9.885987  172.217.13.174  192.168.0.105   TLSv1.2    92 Application Data
  725 9.886532  172.217.13.174  192.168.0.105   TCP        54 443 → 56316 [ACK] Seq=264 Ack=2584 Win=48128 Len=0
  726 9.892230  74.125.141.94   192.168.0.105   TCP        60 443 → 56301 [ACK] Seq=63103 Ack=2309 Win=230 Len=0
  727 9.911515  172.217.13.174  192.168.0.105   TLSv1.2   586 Application Data
  728 9.911517  172.217.13.174  192.168.0.105   TLSv1.2   451 Application Data
```

```
> Frame 766: 523 bytes on wire (4184 bits), 523 bytes captured (4184 bits) on interface 0
> Ethernet II, Src: LiteonTe_3f:a5:9d (cc:b0:da:3f:a5:9d), Dst: ZyxelCom_34:c4:b2 (b8:ec:a3:34:c4:b2)
> Internet Protocol Version 4, Src: 192.168.0.105, Dst: 132.206.75.13
> Transmission Control Protocol, Src Port: 56317, Dst Port: 80, Seq: 1, Ack: 1, Len: 469
> Hypertext Transfer Protocol
```

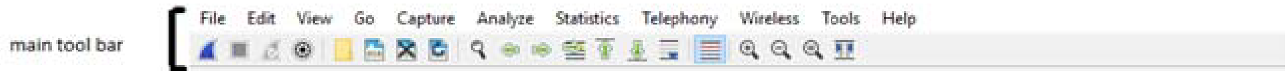
```
0000  b8 ec a3 34 c4 b2 cc b0  da 3f a5 9d 08 00 45 00   ...4.... .?....E.
0010  01 fd 57 67 40 00 80 06  10 a7 c0 a8 00 69 84 ce   ..Wg@... .....i..
0020  4b 0d db fd 00 50 04 7f  27 67 18 53 82 0d 50 18   K....P.. 'g.S..P.
0030  00 44 d2 f8 00 00 47 45  54 20 2f 4c 61 62 31 45   .D....GE T /Lab1E
0040  78 32 2e 68 74 6d 6c 20  48 54 54 50 2f 31 2e 31   x2.html  HTTP/1.1
0050  0d 0a 48 6f 73 74 3a 20  77 77 77 2e 69 6e 66 6f   ..Host:  www.info
0060  33 30 38 61 2e 65 63 65  2e 6d 63 67 69 6c 6c 2e   308a.ece .mcgill.
0070  63 61 0d 0a 43 6f 6e 6e  65 63 74 69 6f 6e 3a 20   ca..Conn ection:
0080  6b 65 65 70 2d 61 6c 69  76 65 0d 0a 55 73 65 72   keep-ali ve..User
0090  2d 41 67 65 6e 74 3a 20  4d 6f 7a 69 6c 6c 61 2f   -Agent:  Mozilla/
00a0  35 2e 30 20 28 57 69 6e  64 6f 77 73 20 4e 54 20   5.0 (Win dows NT
00b0  31 30 2e 30 3b 20 57 69  6e 36 34 3b 20 78 36 34   10.0; Wi n64; x64
00c0  29 20 41 70 70 6c 65 57  65 62 4b 69 74 2f 35 33   ) AppleW ebKit/53
```

Transmission Control Protocol: Protocol

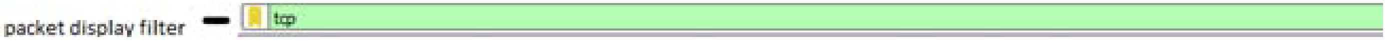
Packets: 1181 · Displayed: 1129 (95.6%) · Droppe

Main toolbar & Packet display filter

1. Main toolbar: The main toolbar provides quick access to frequently used items from the menu. This toolbar cannot be customized by the user, but it can be hidden using the View menu, if the space on the screen is needed to show even more packet data. Only the items useful in the current program state will be available. The others will be greyed out (e.g. you cannot save a capture file if you haven’t loaded one).



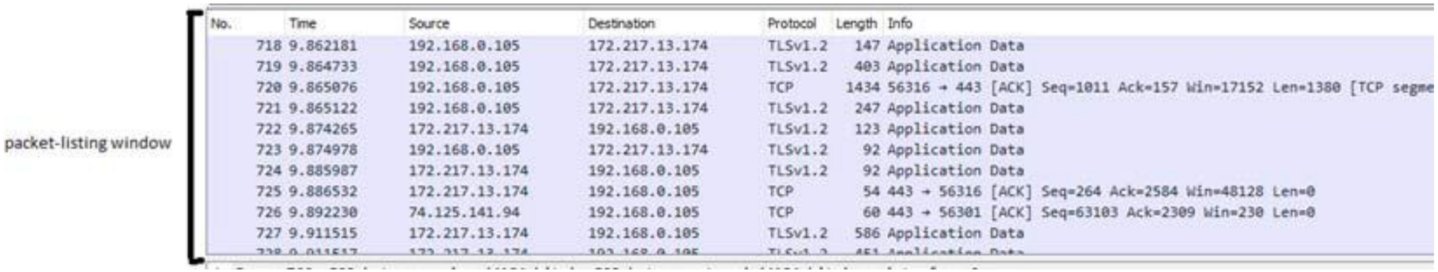
1. Packet display filter: You can enter a protocol name or other information into this field to filter the information displayed in the packet-listing window.



tcp

3. Packet-listing window:

- The packet-listing window displays all the packets in the current capture file. Each line in the packet list corresponds to one packet in the capture file. If you select a line in this window, more details will be displayed in the “Packet-header Details” and “Packet Content/Packet Byte” windows.
- While dissecting a packet, Wireshark will place information from the protocol dissectors into the columns. As higher level protocols might overwrite information from lower levels, you will typically see the information from the highest possible level only.



No.	Time	Source	Destination	Protocol	Length	Info
718	9.862181	192.168.0.105	172.217.13.174	TLSv1.2	147	Application Data
719	9.864733	192.168.0.105	172.217.13.174	TLSv1.2	403	Application Data
720	9.865076	192.168.0.105	172.217.13.174	TCP	1434	56316 → 443 [ACK] Seq=1011 Ack=157 Win=17152 Len=1380 [TCP segme
721	9.865122	192.168.0.105	172.217.13.174	TLSv1.2	247	Application Data
722	9.874265	172.217.13.174	192.168.0.105	TLSv1.2	123	Application Data
723	9.874978	192.168.0.105	172.217.13.174	TLSv1.2	92	Application Data
724	9.885987	172.217.13.174	192.168.0.105	TLSv1.2	92	Application Data
725	9.886532	172.217.13.174	192.168.0.105	TCP	54	443 → 56316 [ACK] Seq=264 Ack=2584 Win=48128 Len=0
726	9.892230	74.125.141.94	192.168.0.105	TCP	60	443 → 56301 [ACK] Seq=63103 Ack=2309 Win=230 Len=0
727	9.911515	172.217.13.174	192.168.0.105	TLSv1.2	586	Application Data
728	9.911517	172.217.13.174	192.168.0.105	TLSv1.2	451	Application Data

Default columns

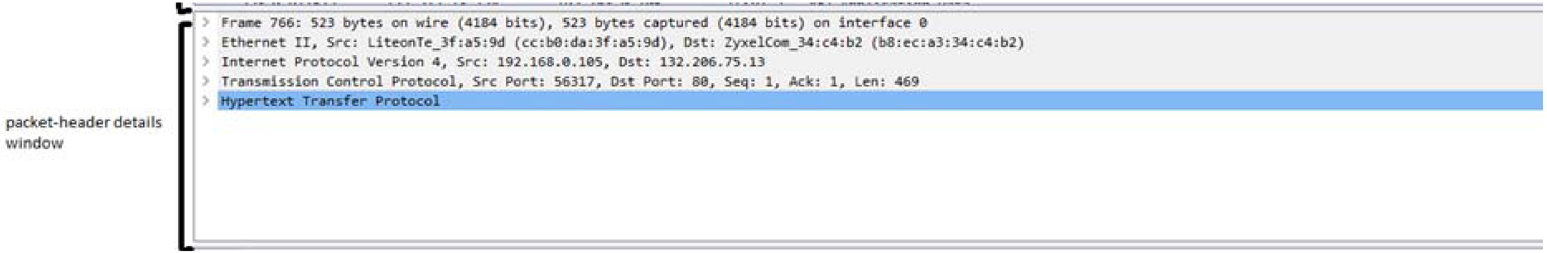
There are a lot of different columns available. The default columns will show:

- **No.:** The number of the packet in the capture file. This number won’t change, even if a display filter is used.
- **Time:** The timestamp of the packet.
- **Source:** The address where this packet is coming from.
- **Destination:** The address where this packet is going to.
- **Protocol:** The protocol name in a short (perhaps abbreviated) version.
- **Length:** The length of each packet.
- **Info:** Additional information about the packet content. The first column shows how each packet is related to the selected packet.

Packet-header details window

4. **Packet-header details window:**

   ○ The packet-header details window shows the current packet (selected in the packet-listing window) in a more detailed form. This window shows the protocols and protocol fields of the packet selected in the packet-listing window. The protocols and fields of the packet shown in a tree which can be expanded and collapsed.



```
> Frame 766: 523 bytes on wire (4184 bits), 523 bytes captured (4184 bits) on interface 0
> Ethernet II, Src: LiteonTe_3f:a5:9d (cc:b0:da:3f:a5:9d), Dst: ZyxelCom_34:c4:b2 (b8:ec:a3:34:c4:b2)
> Internet Protocol Version 4, Src: 192.168.0.105, Dst: 132.206.75.13
> Transmission Control Protocol, Src Port: 56317, Dst Port: 80, Seq: 1, Ack: 1, Len: 469
> Hypertext Transfer Protocol
```

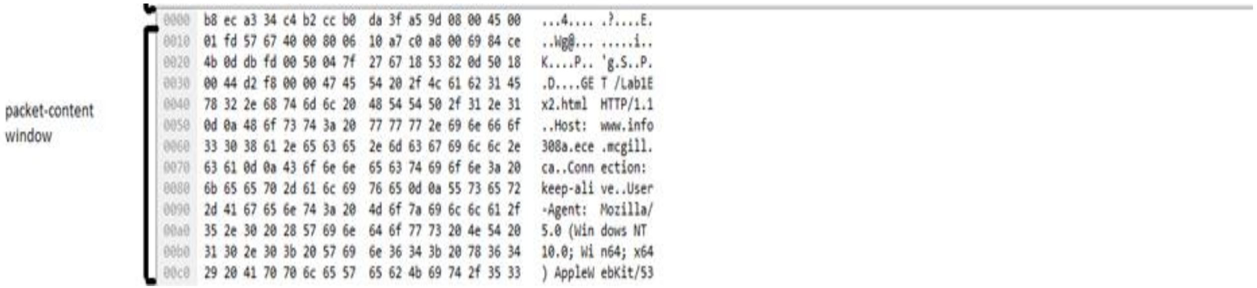
Generated fields & Links

Some protocol fields have special meanings.

- **Generated fields:** Wireshark itself will generate additional protocol information which isn’t present in the captured data. This information is enclosed in square brackets (‘[’ and ‘]’). Generated information includes response times, TCP analysis, GeoIP information, and checksum validation.
- **Links:** If Wireshark detects a relationship to another packet in the capture file it will generate a link to that packet. Links are underlined and displayed in blue. If you double-clicked on a link Wireshark will jump to the corresponding packet.

Packet-content window

5. **Packet-content window:** The packet-content window shows the data of the current packet (selected in the packet-listing window) in a hexdump style. Each line contains the data offset, sixteen hexadecimal bytes, and sixteen ASCII bytes. Non-printable bytes are replaced with a period (‘.’).

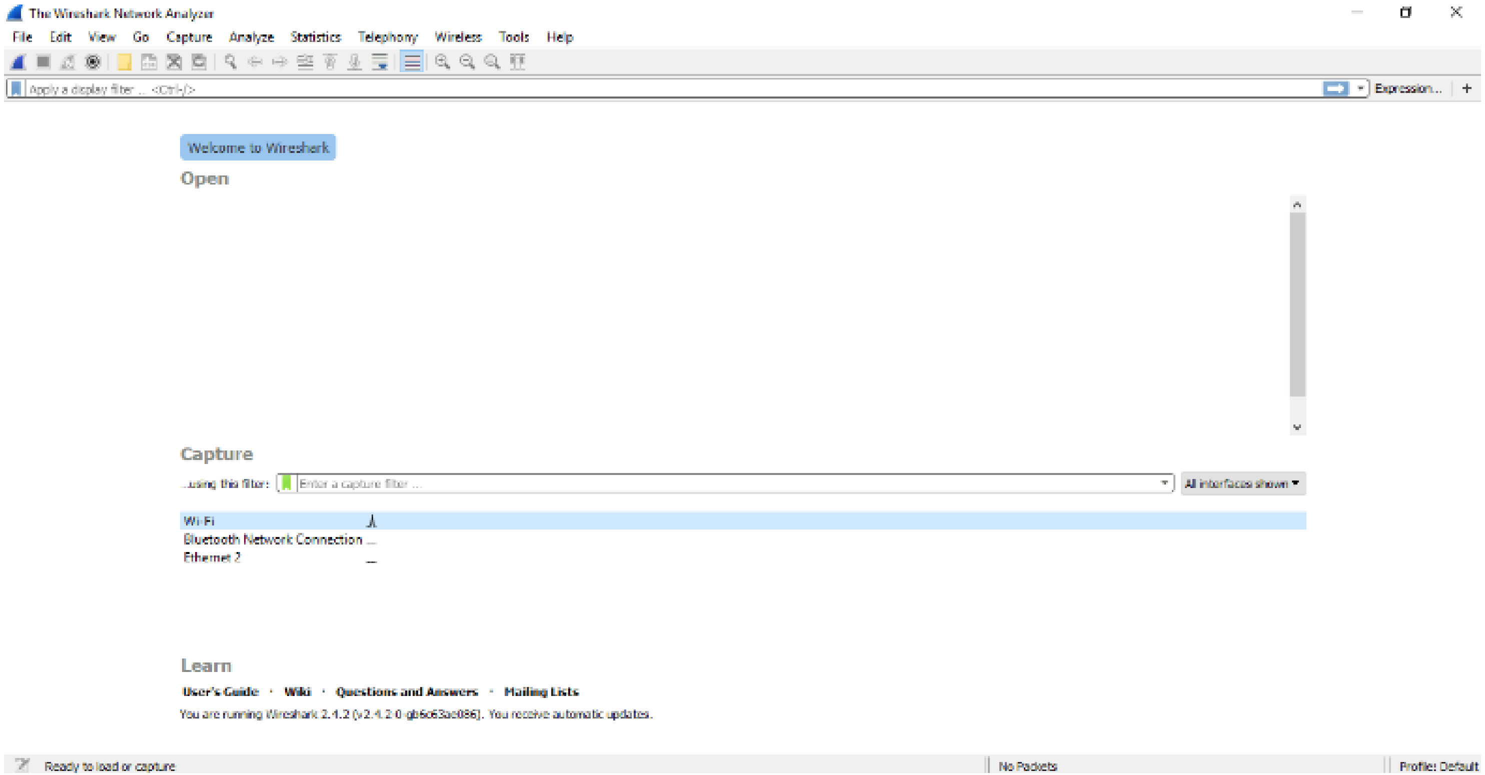


```
0000  b8 ec a3 34 c4 b2 cc b0  da 3f a5 9d 08 00 45 00   ...4.... .?....E.
0010  01 fd 57 67 40 00 80 06  10 a7 c0 a8 00 69 84 ce   ..Wg@... .....i..
0020  4b 0d db fd 00 50 04 7f  27 67 18 53 82 0d 50 18   K....P.. 'g.S..P.
0030  00 44 d2 f8 00 00 47 45  54 20 2f 4c 61 62 31 45   .D....GE T /Lab1E
0040  78 32 2e 68 74 6d 6c 20  48 54 54 50 2f 31 2e 31   x2.html  HTTP/1.1
0050  0d 0a 48 6f 73 74 3a 20  77 77 77 2e 69 6e 66 6f   ..Host:  www.info
0060  33 30 38 61 2e 65 63 65  2e 6d 63 67 69 6c 6c 2e   308a.ece .mcgill.
0070  63 61 0d 0a 43 6f 6e 6e  65 63 74 69 6f 6e 3a 20   ca..Conn ection: 
0080  6b 65 65 70 2d 61 6c 69  76 65 0d 0a 55 73 65 72   keep-ali ve..User
0090  2d 41 67 65 6e 74 3a 20  4d 6f 7a 69 6c 6c 61 2f   -Agent:  Mozilla/
00a0  35 2e 30 20 28 57 69 6e  64 6f 77 73 20 4e 54 20   5.0 (Win dows NT 
00b0  31 30 2e 30 3b 20 57 69  6e 36 34 3b 20 78 36 34   10.0; Wi n64; x64
00c0  29 20 41 70 70 6c 65 57  65 62 4b 69 74 2f 35 33   ) AppleW ebKit/53
```

Starting packet capturing (1/3)

- You can double-click on an interface in the main window.
- You can get an overview of the available interfaces using the “Capture Interfaces” dialog box (Capture → Options…). You can start a capture from this dialog box using the Start button.
- You can immediately start a capture using your current settings by selecting Capture → Start or by clicking the first toolbar button.

Starting packet capturing (2/3)



Wi-Fi

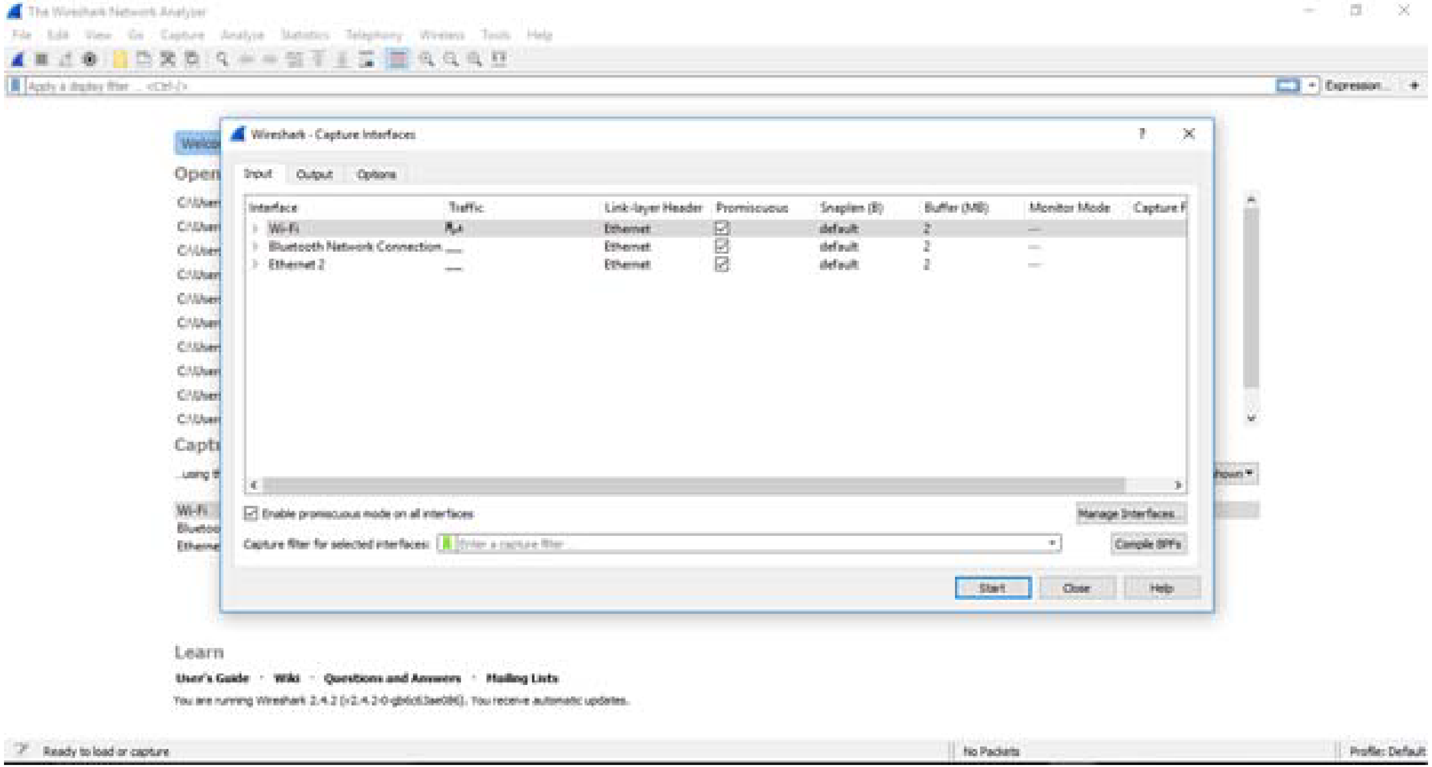
Bluetooth Network Connection

Ethernet 2

You are running Wireshark 2.4.2 (v2.4.2-0-gb6c63ae086). You receive automatic updates.

Ready to load or capture

Starting packet capturing (3/3)


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…
Wireshark - Capture Interfaces
Input
Output
Options
Manage Interfaces…
Compile BPFs
Start
Close
Help
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
Ready to load or capture
No Packets
Profile: Default

Interface	Traffic	Link-layer Header	Promiscuous	Snaplen (B)	Buffer (MB)	Monitor Mode	Capture F
Wi-Fi		Ethernet	☑	default	2	—	
Bluetooth Network Connection	__	Ethernet	☑	default	2	—	
Ethernet 2	__	Ethernet	☑	default	2	—	

☑ Enable promiscuous mode on all interfaces

Capture filter for selected interfaces: Enter a capture filter …

You are running Wireshark 2.4.2 (v2.4.2-0-gb6c63ae086). You receive automatic updates.

Part 1: Internet Protocol (IP)

Objectives:

- Use of the tracert utility to trace the routing path of Internet Protocol (IP) packets sent from your computer to the destination.

Internet Protocol (IP): Overview

- The Internet Protocol (IP), is used to route packets from source to destination based on logical (IP) addresses.
- ICMP can be used to get better understanding of how this protocol works
- Required commands are
  - tracert (windows) / traceroute (unix bases OSes)
  - ping

ICMP

- The Internet Control Message Protocol (ICMP) is a supporting protocol in the Internet protocol suite
- It is used by network devices, including routers, to send error messages and operational information indicating success or failure when communicating with another IP address, for example, an error is indicated when a requested service is not available or that a host or router could not be reached.
- ICMP differs from transport protocols such as TCP and UDP in that it is not typically used to exchange data between systems, nor is it regularly employed by end-user network applications (with the exception of some diagnostic tools like ping and traceroute).

PING

- Ping is a computer network administration software utility used to test the reachability of a host on an Internet Protocol (IP) network. It is available for virtually all operating systems that have networking capability, including most embedded network administration software.
- Ping measures the round-trip time for messages sent from the originating host to a destination computer that are echoed back to the source. The name comes from active sonar terminology that sends a pulse of sound and listens for the echo to detect objects under water.
- Ping operates by sending Internet Control Message Protocol (ICMP) echo request packets to the target host and waiting for an ICMP echo reply. The program reports errors, packet loss, and a statistical summary of the results, typically including the minimum, maximum, the mean round-trip times, and standard deviation of the mean.
- The command-line options of the ping utility and its output vary between the numerous implementations. Options may include the size of the payload, count of tests, limits for the number of network hops (TTL) that probes traverse, interval between the requests and time to wait for a response.
- A short explanation can be found here: https://www.paessler.com/it-explained/ping

PING: Instruction

- Open up the Wireshark.
- Start Packet Capture.
- Run Command Prompt and type:
  - ping -c 5 www.google.com (on linux and mac)
  - ping -n 5 www.google.com (on windows)
- Go back to the Wireshark and stop packet capture.
- In the filter field, type icmp and click apply.

- Alternatively, if ICMP is blocked on the network use the wireshark Capture file "pinggoogle.pcapng" to answer the questions
- In the filter field, type icmp and click apply.

Questions - PING

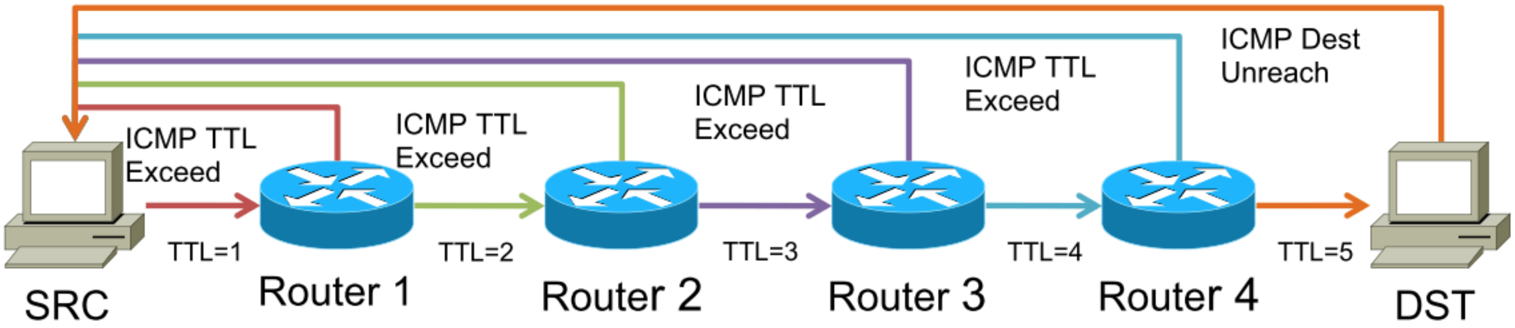
1. What is the IP address of your host? What is the IP address of the destination host?
2. Why is it that an ICMP packet does not have source and destination port numbers?
3. Examine one of the ping request packets sent by your host. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?

Examine the corresponding ping reply packet.

4. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?
5. What is the IP address of your host? What is the IP address of the target destination host?

Tracert (Traceroute)

- The tracert utility in Windows is a client-server program that sends ICMP echo messages encapsulated in IP packets with TTL values 1,2,3, and so on.
- When a router receives one of these packets, it decrements the value of TTL field by one and if this value reaches zeros, it transmits an ICMP message (type 11 – TTLexceeded) to the sending host.
- Thus, the packet with TTL i leads the router on i hop away from the host to transmit an ICMP message back to the sender.
- As a result, by receiving these ICMP messages, the tracert learns the identities of the routers between the host and the destination.
- The tracert procedure is shown in the following figure from http://www.keyboardbanger.com/understanding-the-traceroute-command/)



Tracert: Instruction

- Open up the Wireshark.
- Start Packet Capture.
- Run Command Prompt and type:
  - tracert –d www.google.com (on windows)
  - traceroute –I www.google.com (on mac)
- The –d option prevents tracert from resolving the IP addresses to their names.
- Go back to the Wireshark and stop packet capture.
- In the filter field, type icmp and click apply.

- Alternatively, if ICMP is blocked on the network use the wireshark Capture file “Traceroute-I.pcapng” to answer the questions.
- In the filter field, type icmp and click apply.

Questions - Tracert

6. How many ICMP packets are in the list plane?
7. How many probe packets are sent from the source to the destination for each TTL?
8. The last few echo-request ICMP packets are followed by the echo-reply ICMP packets. Compare one of them with the corresponding reply. Determine which fields are similar and which fields are different? Explain the reason.
9. What are the TTL values for these last few packets? Determine the number of routers between the source and destination based on these TTL values.
10. Examine the IP packet header of the last echo-request ICMP packet, what is the value in the “Protocol” field? What does this field indicate?
11. How many bytes are in this IP header? How many bytes are in the payload of this IP packet? Explain how you determined the number of payload bytes.
12. Has this IP packet been fragmented? Explain how you determined whether or not the packet has been fragmented.
13. How the IP address of www.google.com can be found? Determine the packet and the field in the packet that contains this information.
14. Examine the ICMP echo packet in your screenshot. Is this different from the ICMP ping query packets in the first half of this lab? If yes, how so?
15. Examine the ICMP error packet in your screenshot. It has more fields than the ICMP echo packet. What is included in those fields?
16. Examine the last three ICMP packets received by the source host. How are these packets different from the ICMP error packets? Why are they different?

Part 2: Ethernet

Objectives: To explore the details of Ethernet frames. Ethernet is a popular link layer protocol.

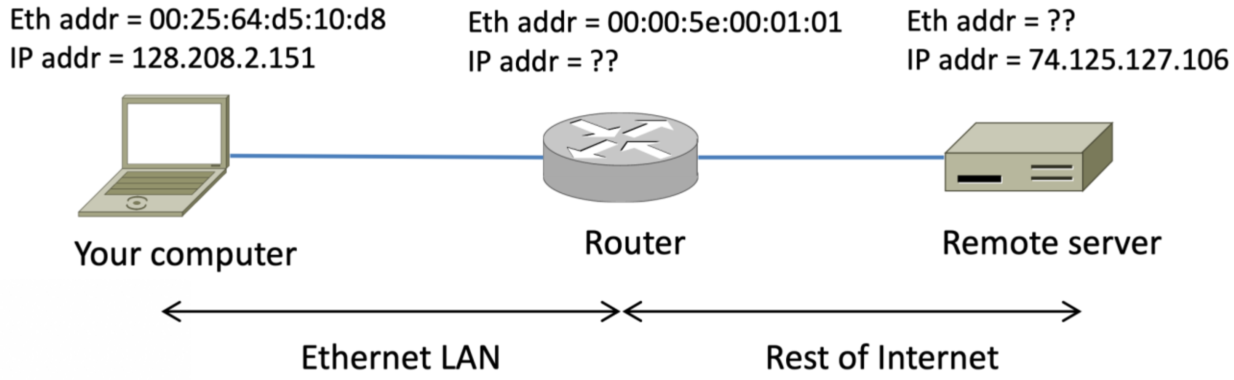
Ethernet Frame Structure

- When upper layer protocols communicate with each other, data flows down the Open Systems Interconnection (OSI) layers and is encapsulated into a Layer 2 frame. The frame composition is dependent on the media access type.
- For example, if the upper layer protocols are TCP and IP and the media access is Ethernet, then the Layer 2 frame encapsulation will be Ethernet II.
- This is typical for a LAN environment. When learning about Layer 2 concepts, it is helpful to analyze frame header information.

Preamble	Destination Address	Source Address	Frame Type	Data	FCS
8 Bytes	6 Bytes	6 Bytes	2 Bytes	46 – 1500 Bytes	4 Bytes

Scope of Ethernet Addresses

- Each Ethernet frame carries a source and destination address.
- One of these addresses is that of your computer.
- It is the source for frames that are sent, and the destination for frames that are received.
- But what is the other address? Assuming you pinged a remote Internet server, it cannot be the Ethernet ad-dress of the remote server because an Ethernet frame is only addressed to go within one LAN.
- Instead, it will be the Ethernet address of the router or default gateway



Capturing and analyzing Ethernet frames

- First, make sure your browser’s cache is empty.
- Start Packet Capture
- Enter the following URL into your browser https://wiki.wireshark.org/Ethernet
- Stop Wireshark packet capture.
- In the filter field, type http and click apply.

Ethernet Questions

1. What is the 48-bit Ethernet address of your computer?
2. What is the 48-bit destination address in the Ethernet frame?
3. Is this (destination address) the Ethernet address of https://wiki.wireshark.org/Ethernet?
4. What device has this as its Ethernet address?

Answe the following questions for the Ethernet frame containing the HTTP OK response

5. What is the value of the Ethernet source address? Is this the address of your computer, or of www.wireshark ? What device has this as its Ethernet address?
6. What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?

The Address Resolution Protocol

- When configuring a new network computer, each system is assigned an IP address for primary identification and communication. A computer also has a MAC address identity. Manufacturers embed the MAC address in the LAN card. The MAC address is also known as the computer's physical address.
- Before two computers communicate, each must know the other's relative IP or MAC addresses. If computer A only has computer B's MAC address, computer A can reveal its IP address by sending an ARP request to computer B. Computer B may then reply by attaching its IP address with ARP to computer A. This simple address translation and exchange process is the primary role of ARP.
- ARP tables can be stored to increase transmission rates by keeping track of addresses known to the network and transmitting any MAC or IP address changes via ARP. There is no authentication required at this level, so spoofing of IP and MAC addresses is possible. Additional software may be required to police the ARP tables and prevent malicious user attacks.

The Address Resolution Protocol

- Recall that the ARP protocol typically maintains a cache of IP-to-Ethernet address translation pairs on your computer The ***arp*** command (in both MSDOS and Linux/Unix) is used to view and manipulate the contents of this cache.
- Since the ***arp*** command and the ARP protocol have the same name, it's understandably easy to confuse them. But keep in mind that they are different - the arp command is used to view and manipulate the ARP cache contents, while the ARP protocol defines the format and meaning of the messages sent and received, and defines the actions taken on message transmission and receipt.
- The arp-a command will display the contents of the ARP cache on your computer.
- The arp –d * command will clear your ARP cache.
  - The –dflag indicates a deletion operation, and the * is the wildcard that says to delete all table entries.

ARP

- ○ Run Command Prompt and type:
- ○ arp-a

7. Take a screen shot of your computer’s ARP cache. What is the meaning of each column value?

- Obtain your PC’s IP address and share it with the group next to you (ipconfig)
- Write click on command prompt and click “run as administrator”
- Clear your ARP cache, by running arp –d * command
- Start Packet Capture
- Ping the IP address of the group next to you
  - Hint: ping x.x.x.x
- Stop Wireshark packet capture
- In the filter field, type arp and click apply

8. Run arp -a command and compare the list with your answer to question 7.

ARP Questions

- Find an arp request packet (MAC address matches your devices MAC address) and answer the following questions

9. How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?
10. What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP request is made?
11. Does the ARP message contain the IP address of the sender?
12. Where in the ARP request does the “question” appear – the Ethernet address of the machine whose corresponding IP address is being queried?

- Now find the ARP reply that was sent in response to the ARP request

13. How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?
14. What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP response is made?
15. Where in the ARP message does the “answer” to the earlier ARP request appear – the IP address of the machine having the Ethernet address whose corresponding IP address is being queried?