

Computación en Internet I

Andrés A. Aristizábal P.
aaaristizabal@icesi.edu.co

Departamento de Tecnologías de Información y Comunicaciones



2023-1

1 Introduction to Wireshark

- Basic notions
- Understanding Wireshark
- Running Wireshark

2 Workshop

1 Introduction to Wireshark

- Basic notions
- Understanding Wireshark
- Running Wireshark

2 Workshop

What is a packet sniffer?

What is a packet sniffer?

- Basic tool for observing the messages exchanged between executing protocol entities.

What is a packet sniffer?

- Basic tool for observing the messages exchanged between executing protocol entities.
- Captures ("sniffs") messages being sent/received from/by a computer.

What is a packet sniffer?

- Basic tool for observing the messages exchanged between executing protocol entities.
- Captures ("sniffs") messages being sent/received from/by a computer.
- It will also typically store and/or display the contents of the various protocol fields in the captured messages.

What is a packet sniffer?

- Basic tool for observing the messages exchanged between executing protocol entities.
- Captures ("sniffs") messages being sent/received from/by a computer.
- It will also typically store and/or display the contents of the various protocol fields in the captured messages.
- It observes messages being sent and received by applications and protocols running on a computer, but never sends packets itself.

What is a packet sniffer?

- Basic tool for observing the messages exchanged between executing protocol entities.
- Captures ("sniffs") messages being sent/received from/by a computer.
- It will also typically store and/or display the contents of the various protocol fields in the captured messages.
- It observes messages being sent and received by applications and protocols running on a computer, but never sends packets itself.
- Received packets are never explicitly addressed to the packet sniffer.

What is a packet sniffer?

- Basic tool for observing the messages exchanged between executing protocol entities.
- Captures ("sniffs") messages being sent/received from/by a computer.
- It will also typically store and/or display the contents of the various protocol fields in the captured messages.
- It observes messages being sent and received by applications and protocols running on a computer, but never sends packets itself.
- Received packets are never explicitly addressed to the packet sniffer.
- It receives a copy of packets that are sent/received from/by application and protocols executing on the machine.

What is the structure of a packet sniffer?

What is the structure of a packet sniffer?

- Consists of two parts.

What is the structure of a packet sniffer?

- Consists of two parts.
- The packet capture library.

What is the structure of a packet sniffer?

- Consists of two parts.
- The packet capture library.
 - ▶ Receives a copy of every link-layer frame that is sent from or received by the computer over a given interface.
 - ▶ Capturing all link-layer frames gives all messages sent/received across the monitored link from/by all protocols and applications executing on the computer.

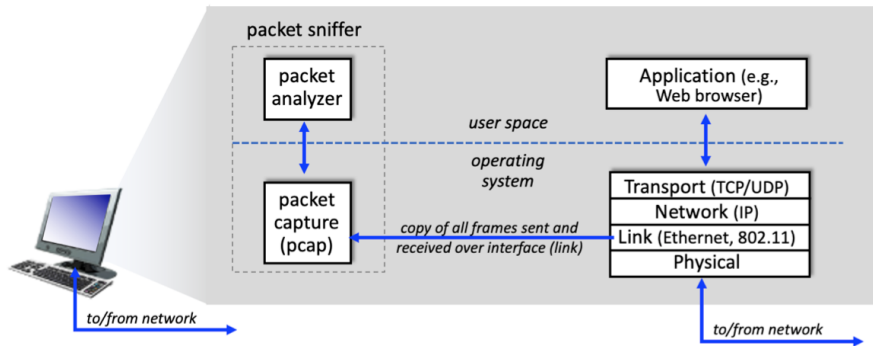
What is the structure of a packet sniffer?

- Consists of two parts.
- The packet capture library.
 - ▶ Receives a copy of every link-layer frame that is sent from or received by the computer over a given interface.
 - ▶ Capturing all link-layer frames gives all messages sent/received across the monitored link from/by all protocols and applications executing on the computer.
- The packet analyzer.

What is the structure of a packet sniffer?

- Consists of two parts.
- The packet capture library.
 - ▶ Receives a copy of every link-layer frame that is sent from or received by the computer over a given interface.
 - ▶ Capturing all link-layer frames gives all messages sent/received across the monitored link from/by all protocols and applications executing on the computer.
- The packet analyzer.
 - ▶ Displays the contents of all fields within a protocol message.
 - ▶ Understands the structure of all messages exchanged by protocols

What is the structure of a packet sniffer?



1 Introduction to Wireshark

- Basic notions
- Understanding Wireshark
- Running Wireshark

2 Workshop

What is Wireshark?

What is Wireshark?

- It is a packet analyzer that uses a packet capture library in the computer.

What is Wireshark?

- It is a packet analyzer that uses a packet capture library in the computer.
- Captures link-layer frames.

What is Wireshark?

- It is a packet analyzer that uses a packet capture library in the computer.
- Captures link-layer frames.
- Uses the generic term "packet" to refer to link-layer frames, network-layer datagrams, transport-layer segments, and application-layer messages.

What is Wireshark?

- It is a packet analyzer that uses a packet capture library in the computer.
- Captures link-layer frames.
- Uses the generic term "packet" to refer to link-layer frames, network-layer datagrams, transport-layer segments, and application-layer messages.
- It is a free network protocol analyzer that runs on Windows, Mac, and Linux/Unix computers.

What is Wireshark?

- It is a packet analyzer that uses a packet capture library in the computer.
- Captures link-layer frames.
- Uses the generic term "packet" to refer to link-layer frames, network-layer datagrams, transport-layer segments, and application-layer messages.
- It is a free network protocol analyzer that runs on Windows, Mac, and Linux/Unix computers.
- It is stable.

What is Wireshark?

- It is a packet analyzer that uses a packet capture library in the computer.
- Captures link-layer frames.
- Uses the generic term "packet" to refer to link-layer frames, network-layer datagrams, transport-layer segments, and application-layer messages.
- It is a free network protocol analyzer that runs on Windows, Mac, and Linux/Unix computers.
- It is stable.
- Has a large user base and well-documented support that includes a user-guide.

What is Wireshark?

- It is a packet analyzer that uses a packet capture library in the computer.
- Captures link-layer frames.
- Uses the generic term "packet" to refer to link-layer frames, network-layer datagrams, transport-layer segments, and application-layer messages.
- It is a free network protocol analyzer that runs on Windows, Mac, and Linux/Unix computers.
- It is stable.
- Has a large user base and well-documented support that includes a user-guide.
- Has a rich functionality that includes the capability to analyze hundreds of protocols.

What is Wireshark?

- It is a packet analyzer that uses a packet capture library in the computer.
- Captures link-layer frames.
- Uses the generic term "packet" to refer to link-layer frames, network-layer datagrams, transport-layer segments, and application-layer messages.
- It is a free network protocol analyzer that runs on Windows, Mac, and Linux/Unix computers.
- It is stable.
- Has a large user base and well-documented support that includes a user-guide.
- Has a rich functionality that includes the capability to analyze hundreds of protocols.
- It operates in computers using many link-layer technologies.

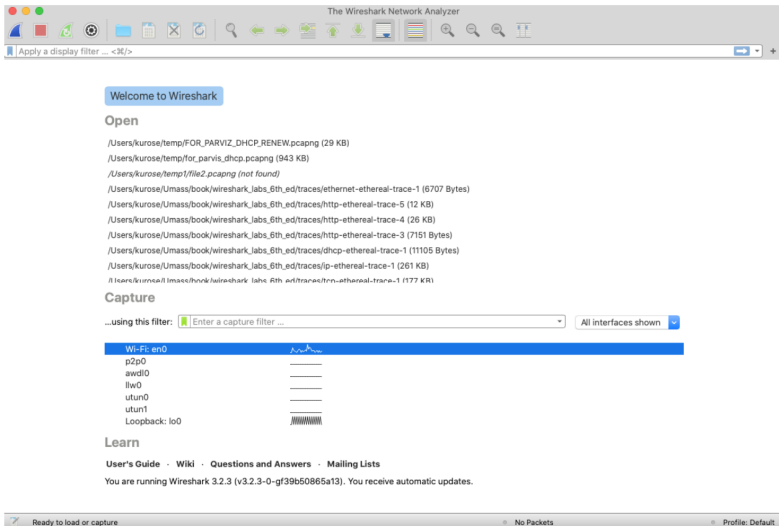
1 Introduction to Wireshark

- Basic notions
- Understanding Wireshark
- Running Wireshark

2 Workshop

Running Wireshark

Initial screen



Taking it out for a spin

Taking it out for a spin

- Under the Capture section, there is a list of so-called interfaces.

Taking it out for a spin

- Under the Capture section, there is a list of so-called interfaces.
- All packets to/from the computer will pass through the Wi-Fi interface.

Taking it out for a spin

- Under the Capture section, there is a list of so-called interfaces.
- All packets to/from the computer will pass through the Wi-Fi interface.
- Select that interface.

Running Wireshark

Taking it out for a spin

- Under the Capture section, there is a list of so-called interfaces.
- All packets to/from the computer will pass through the Wi-Fi interface.
- Select that interface.

command menus

display filter specification

listing of captured packets

Details of selected packet

packet content (in hexadecimal and ASCII)

Wireshark File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter --<36>

No.	Time	Source	Destination	Protocol	Length	Info
55	9.523398	128.119.245.12	192.168.0.15	TCP	74	80 → 55621 [SYN, ACK, ECN] Seq=0 Ack=1 Win=28
56	9.523490	192.168.0.15	128.119.245.12	TCP	66	55621 → 80 [ACK] Seq=1 Ack=1 Win=133712 Len=0
57	9.523911	192.168.0.15	128.119.245.12	HTTP	697	GET /Wireshark/Labs/Intro-Wireshark/1104.Wireshark
58	9.525361	128.119.245.12	192.168.0.15	TCP	74	80 → 55622 [SYN, ACK, ECN] Seq=0 Ack=1 Win=28
59	9.525418	192.168.0.15	128.119.245.12	TCP	66	55622 → 80 [ACK] Seq=1 Ack=1 Win=133712 Len=0
60	9.610688	35.166.241.18	192.168.0.15	TLV1.2	117	Change Cipher Spec, Encrypted Handshake Messag
61	9.610613	128.119.245.12	192.168.0.15	TCP	66	80 → 55621 [ACK] Seq=1 Ack=32 Win=38336 Len=0
62	9.610712	192.168.0.15	35.166.241.18	TCP	66	55620 → 643 [ACK] Seq=644 Ack=3451 Win=131008
63	9.616465	128.119.245.12	192.168.0.15	HTTP	305	HTTP/1.1 304 Not Modified
64	9.616562	192.168.0.15	128.119.245.12	TCP	66	55621 → 80 [ACK] Seq=632 Ack=248 Win=131520 L
65	9.690975	192.168.0.15	192.168.0.254	DNS	99	Standard query 80648 AAAA captive-cdn.origin
66	9.691048	192.168.0.15	192.168.0.254	DNS	99	Standard query 80647 A captive-cdn.origin-apple

Frame 57: 697 bytes on wire (5576 bits), 697 bytes captured (5576 bits) on interface en0, id 0

Ethernet II, Src: Apple_98:d9:27 (78:4f:43:98:d9:27), Dst: Freebox_aa:0f:e4 (80:24:d4:aa:0f:e4)

Internet Protocol Version 4, Src: 192.168.0.15, Dst: 128.119.245.12

.... 0101 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x02 (DSCP: CS0, ECN: ECT(0))

Total Length: 683

Identification: 0x0000 (0)

Flags: 0x0000, Don't fragment

Fragment offset: 0

Time to live: 64

0010 82 ab 00 00 40 00 00 06 02 10 c0 00 0f 80 77 ... @ ... w

0020 15 8c 09 45 80 50 15 e5 a0 3d df b1 a3 4c 80 18E.P.L.

0030 00 0a 20 1d 00 00 01 85 00 0a 0a 95 91 2a 09 0b

0040 ac e2 47 45 54 28 2f 7f 69 72 65 73 68 61 72 60 ... GET /w/reshark

0050 2d 6c 61 62 73 2f 49 4e 54 52 4f 2d 7f 69 72 65 ... -labs/IN TRO-wire

0060 73 68 61 72 60 2d 66 69 6c 65 31 2e 68 74 6d 6c ... shark-Fi let.html

0070 20 48 54 54 50 2f 31 2e 31 8d 0a 48 6f 73 74 3a ... HTTP/1.1 Host:

0080 20 67 61 69 61 2e 63 73 2e 75 6d 61 73 73 2e 65 ... gaia.cs.umass.e

0090 64 75 80 8a 55 73 65 72 2d 41 67 65 6e 74 3a 28 ... du User-Agent:

00a0 6d 67 7a 69 6c 6c 61 2f 35 2e 30 20 2d 4d 61 63 ... Mozilla/5.0 (Mac

00b0 69 6e 74 67 73 68 3b 2d 49 6e 74 65 6c 2d 4d 61 ...intosh; Intel Ma

00c0 63 20 4f 53 58 58 31 38 2e 31 35 3b 28 72 76 ... C OS X 10.15; rv

00d0 3a 37 35 2e 38 29 28 47 65 63 6b 6f 2f 32 30 31 ...;75.0) Gecko/201

00e0 30 31 38 31 28 46 69 72 65 66 6f 78 2f 37 35 ...00181 Firefox/75

00f0 2e 38 8d 8a 41 63 63 65 78 74 3a 2d 74 65 78 740 Accel-pte: text

Time to live (to 16), 1 byte

Packets: 90 / Displayed: 90 (100.0%) / Dropped: 0 (0.0%) / Profile: Default

What are the five main components of Wireshark?

What are the five main components of Wireshark?

- The command menus.

What are the five main components of Wireshark?

- The command menus.
- The packet-listing window.

What are the five main components of Wireshark?

- The command menus.
- The packet-listing window.
- The packet-header details window.

What are the five main components of Wireshark?

- The command menus.
- The packet-listing window.
- The packet-header details window.
- The packet-contents window.

What are the five main components of Wireshark?

- The command menus.
- The packet-listing window.
- The packet-header details window.
- The packet-contents window.
- The packet display filter field.

Command menus

Command menus

- Standard pulldown menus located at the top of the Wireshark window.

Command menus

- Standard pulldown menus located at the top of the Wireshark window.
- The File menu allows saving captured packet data, opening a file containing previously captured packet data and exiting the Wireshark application.

Command menus

- Standard pulldown menus located at the top of the Wireshark window.
- The File menu allows saving captured packet data, opening a file containing previously captured packet data and exiting the Wireshark application.
- The Capture menu allows starting packet capture.

Packet-listing window



Packet-listing window

- Displays a one-line summary for each packet captured:

Packet-listing window

- Displays a one-line summary for each packet captured:
 - ▶ Packet number.

Packet-listing window

- Displays a one-line summary for each packet captured:
 - ▶ Packet number.
 - ▶ Time at which the packet was captured.

Packet-listing window

- Displays a one-line summary for each packet captured:
 - ▶ Packet number.
 - ▶ Time at which the packet was captured.
 - ▶ The packet's source and destination addresses.

Packet-listing window

- Displays a one-line summary for each packet captured:
 - ▶ Packet number.
 - ▶ Time at which the packet was captured.
 - ▶ The packet's source and destination addresses.
 - ▶ The protocol type.

Packet-listing window

- Displays a one-line summary for each packet captured:
 - ▶ Packet number.
 - ▶ Time at which the packet was captured.
 - ▶ The packet's source and destination addresses.
 - ▶ The protocol type.
 - ▶ Protocol-specific information contained in the packet.

Packet-listing window

- Displays a one-line summary for each packet captured:
 - ▶ Packet number.
 - ▶ Time at which the packet was captured.
 - ▶ The packet's source and destination addresses.
 - ▶ The protocol type.
 - ▶ Protocol-specific information contained in the packet.
- The packet listing can be sorted according to any of these categories.

Packet-listing window

- Displays a one-line summary for each packet captured:
 - ▶ Packet number.
 - ▶ Time at which the packet was captured.
 - ▶ The packet's source and destination addresses.
 - ▶ The protocol type.
 - ▶ Protocol-specific information contained in the packet.
- The packet listing can be sorted according to any of these categories.
- The protocol type field lists the highest-level protocol that sent or received this packet.

Packet-header details window



Packet-header details window

- Provides details about the packet selected in the packet-listing window.

Packet-header details window

- Provides details about the packet selected in the packet-listing window.
 - ▶ Ethernet frame.

Packet-header details window

- Provides details about the packet selected in the packet-listing window.
 - ▶ Ethernet frame.
 - ▶ IP datagram that contains this packet.

Packet-header details window

- Provides details about the packet selected in the packet-listing window.
 - ▶ Ethernet frame.
 - ▶ IP datagram that contains this packet.
 - ▶ If the packet has been carried over TCP or UDP, TCP or UDP details will also be displayed.

Packet-header details window

- Provides details about the packet selected in the packet-listing window.
 - ▶ Ethernet frame.
 - ▶ IP datagram that contains this packet.
 - ▶ If the packet has been carried over TCP or UDP, TCP or UDP details will also be displayed.
 - ▶ Details about the highest-level protocol that sent or received this packet are also provided.

Packet-contents window

Packet-contents window

- A protocol name or other data can be entered in order to filter the information displayed in the packet-listing window.

Packet-contents window

- A protocol name or other data can be entered in order to filter the information displayed in the packet-listing window.

Packet display filter field

Packet-contents window

- A protocol name or other data can be entered in order to filter the information displayed in the packet-listing window.

Packet display filter field

- Displays the entire contents of the captured frame, in both ASCII and hexadecimal format.

Workshop

Complete workshop for today's class. To be handed in the next class.