Computación en Internet I

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

Departamento de Tecnologías de Información y Comunicaciones

2023-1

Agenda

1. **Introduction to Wireshark**
   - Basic notions
   - Understanding Wireshark
   - Running Wireshark
2. **Workshop**

Agenda del día

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.

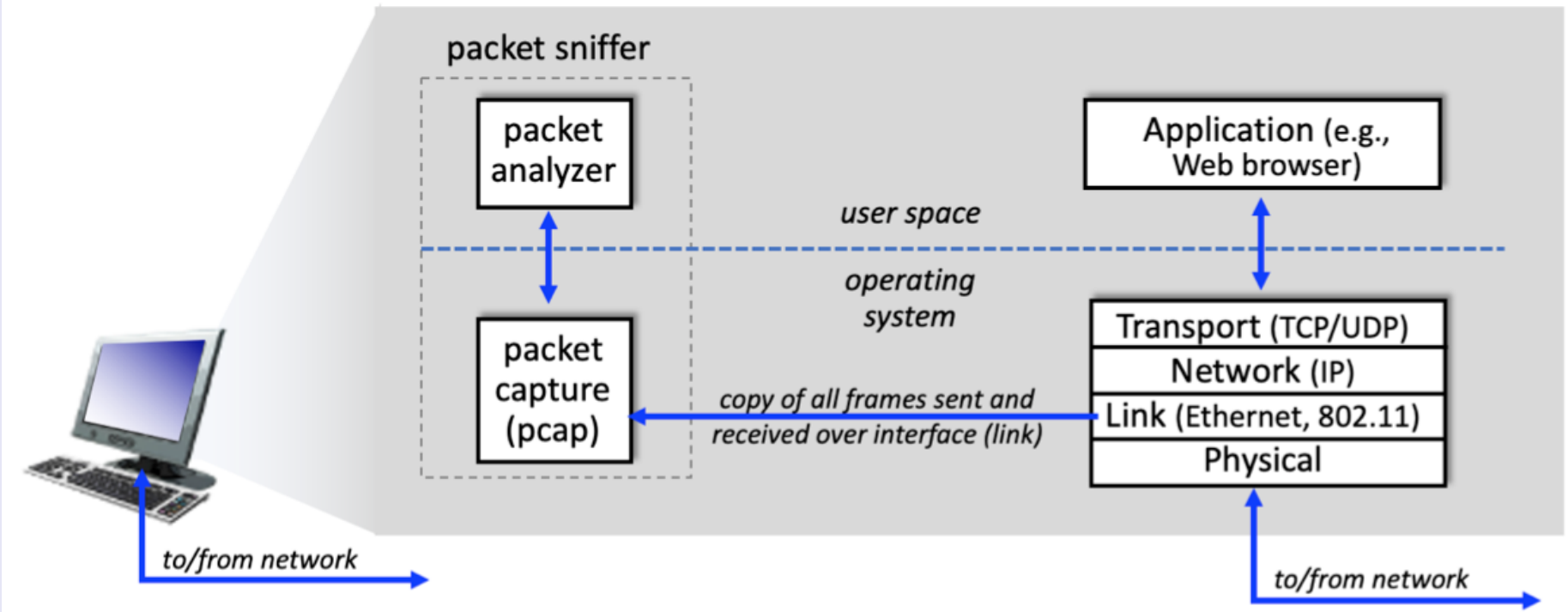
What is the structure of a packet sniffer?

- 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?



Agenda del día

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.

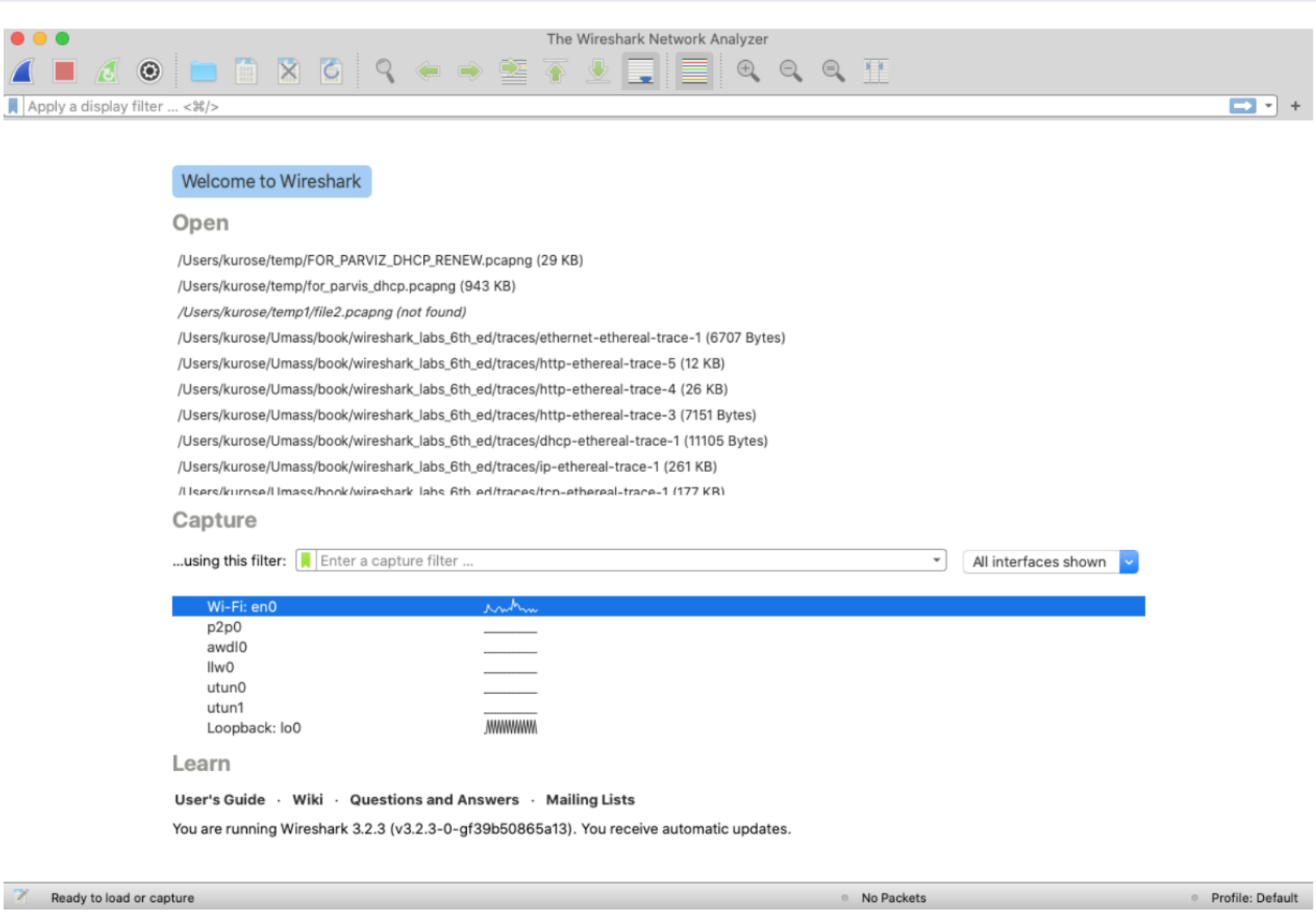
What is Wireshark?

- 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.

Agenda del día

1. **Introduction to Wireshark**
   - Basic notions
   - Understanding Wireshark
   - Running Wireshark
2. **Workshop**

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

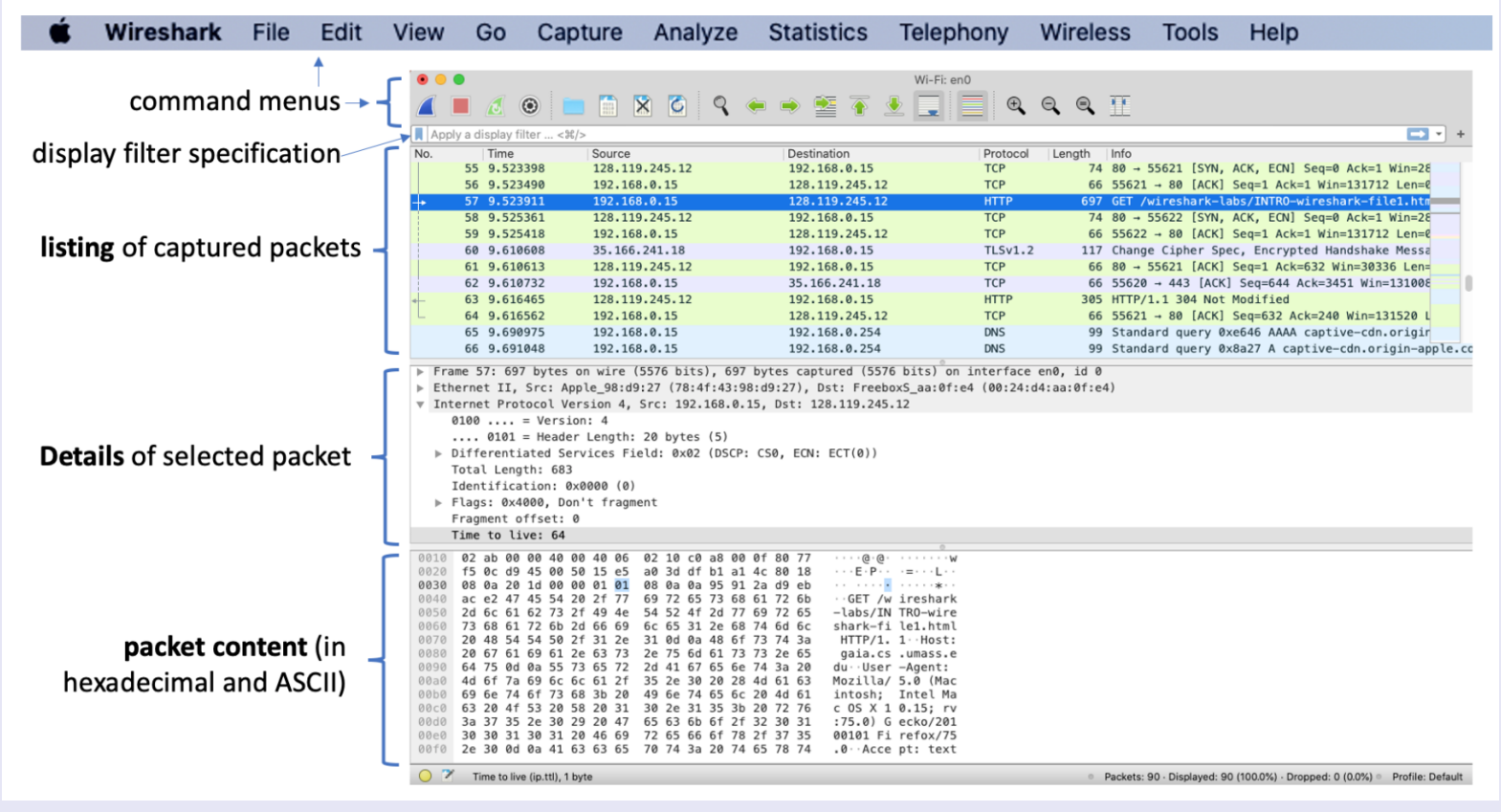
- Under the Capture section, there is a list of so-called interfaces.
- All packets to/from the computer will pass through the Wi-Fi interface.

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.

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.



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

Workshop

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