Lecture 7 Exercises

September 23, 2024

Petar Popovski Junya Shiraishi and João H. Inacio de Souza



Agenda



Exercises

Petar Popovski

Getting to know Wire shark

Introduction

Getting to know Wire shark

Exercises

Installation

Introduction



Exercises

Petar Popovski

Introduction

Getting to know Wire shark

Exercises



To troubleshoot and understand, we need some kind of tool which allows us to see what is going on inside the network.





Petar Popovski

Introduction
Installation

Getting to know Wire shark

xercises

Wireshark is the oscilloscope of network engineering.

It makes it easy to perform:

- Packet capture
- Dissecting
- Analysis

All in a nice and relatively user friendly interface. Best of all. It is free!



Installation



Exercises

Petar Popovski

Installation

Getting to know Wire shark

xercises

Wireshark supports most popular operating systems.

- ► Linux: Get it from your package manager
- ► Windows and MacOs: https://www.wireshark.org/#download

Note: On Windows it will ask to install WinPCAP which is required for Wireshark to work, so make sure to install it. Sometimes a reboot might be required for it to start correctly.

Getting to know Wireshark



DENMARK Exercises

Petar Popovski

Installation

Getting to know Wire

shark

Wireshark requires root/administrator access to work. On Windows it should ask with a UAC prompt. On linux you might need to launch it from the terminal using *sudo wireshark*

Getting to know Wireshark The startup screen

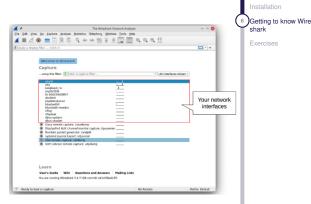
LBORG UNIVERSIT

Exercises
Petar Popovski

On the startup screen you can see the capture filter and a list of your network interfaces.

Notice the little squiggly line next to each interface. It shows network activity.

To start a capture, simply double-click an interface.



Getting to know Wireshark



Exercises
Petar Popovski

troduction

Getting to know Wire shark

Exercises

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help DAS Auto Stop Restart Search 69 Standard query 8xddb4 AAAA an scroll 197 6.526825555 76 Standard guery 0xe2d3 AAAA ar-199 6.530465968 200 6.530582124 101 Standard query 0x46f3 AAAA ar-204 6.533144265 69 Standard query 8x2f57 AAAA ar-Frame 1: 264 bytes on wire (2112 bits), 264 bytes captured (2112 bits) on interface wland, id 0 Etharmat II, Src: IntelCor 97:66:10 (24:76:697:66:30), Dat: Cisco 97:00:00 (00:00:0c:0f:f0:00) Interret Protocol Version 4. Src: 172.26.50.141, Dat: 34.107.155.225 Transmission Control Protocol, Src Port: 56818, Dst Port: 443, Seq: 1, Ack: 1, Len: 198 Transport Layer Security @ 2 wland: capture in progress: Packets: 207 - Displayed: 207 (100.0%) Profile: Default

The top bar has some basic controls for starting, stopping, restarting and searching.

Searching makes it possible to find packages with specific contents. For example bytes or strings.

Getting to know Wireshark Packet capture

AALBORG UNIVERSITY

The display filter is one of the most important parts of Wireshark. Here you can apply a filter to what is displayed. In most cases filtering is a necessity in order to make

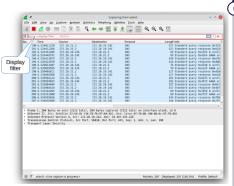
Examples of useful filters

sense of what is going on.

► IP address: ip.addr == 192.0.2.1

Protocol: icmp

► Port and IP: tcp.port == 80 && ip.src == 192.168.2.2



Exercises

Petar Popovski

Getting to know Wire

xercises

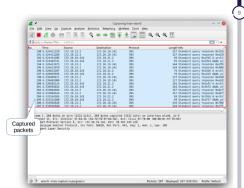
shark

Getting to know Wireshark



The packet view is a live view of the captured packets.

Each row represents a captured packet. Clicking one selects it and decodes the content.



Exercises
Petar Popovski

traduction

Getting to know Wire shark

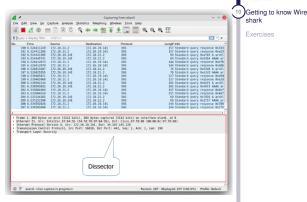
xercises

Getting to know Wireshark Packet capture



DENMARK Exercises Petar Popovski

shark



The dissector view shows the content of the currently selected packet. Wireshark will attempt to decode and show each of the encapsulated packets.

Usefull features



Exercises

Petar Popovski

Getting to know Wire shark

Exercises

The Statistics menu has many useful items. Some of my favorites are:

- ► Conversations
- ► I/O Graphs
- ► Flow graph



Exercises

Petar Popovski

troduction

stallation

Getting to know Wire shark

Exercises

Install Wireshark on your computer

- 1. Disconnect from the Wi-Fi
- Start a new capture in Wireshark on your Wi-Fi interface and reconnect to the Wi-Fi
- 3. Filter the view for dhcp messages
- 4. Which IP address are you getting assigned?
- 5. How long are you allowed to use this address?
- 6. Can you change it?



Exercises

Petar Popovski

troduction

stallation

Getting to know Wire shark

13 Exercises

The file ping.pcap contains the capture of a computer measuring the round trip delay to another computer using the ping tool.

- 1. Download and open ping.pcap
- 2. Find the MAC and IP addresses of the two computers
- 3. Which protocols are involved in the capture?
- 4. Make a flow diagram/graph of the traffic between the computers
- 5. What is the payload size of the packets



DENMARK Exercises

Petar Popovski

troduction

stallation

Getting to know Wire shark

Exercises

1. Find your computer's MAC and IP addresses

1.1 Linux: ip addr

1.2 MacOs: ifconfig1.3 Windows: ipconfig

2. Start a new capture in Wireshark and go to https://www.gnu.org/

2.1 Can you find your computer's DNS lookup for www.gnu.org? (If not, can you guess why?)

2.2 From the DNS reply, find the IP address of www.gnu.org and apply it as a view filter.

2.3 Identify the start and end of a TCP stream. (Hint look for the three-way handshake).

2.4 By inspecting the packet contents, find a stream that downloads an image file (Hint try the search function)