

Intro - Wireshark: The Basics

<https://tryhackme.com/room/wiresharkthebasics>

Opgaveinformation

Opgavens formål at opnå basisk viden om Wireshark.

Opgave + løsning

Task 1 - Introduction

Which file is used to simulate the screenshots?

- Svar: http1.pcapng

Which file is used to answer the questions?

- Svar: exercise.pcapng

Task 2 - Tool Overview

Use the "Exercise.pcapng" file to answer the questions. Read the "capture file comments".

What is the flag?

- Åben filen
- Gå ind i: Statistics -> Capture File Properties
- Svar: TryHackMe_Wireshark_Demo

Applications Places System >- Mon Feb 23, 09:39

Wireshark · Capture File Properties · Exercise.pcapng

Details

size, B			
Bytes	110240582	110240582	0
		(100.0%)	
Average bytes/s	0	0	—
Average bits/s	1	1	—

File Comment

Knowing the file details is helpful. Especially when working with multiple pcap files, sometimes you will need to know and recall the file details (File hash, capture time, capture file comments, interface and statistics) to identify the file, classify and prioritise it. You can view the details by following "Statistics --> Capture File Properties" or by clicking the "pcap icon located on the left bottom" of the window.

Flag: TryHackMe_Wireshark_Demo

Packet Comments

Frame 12:
This_is_Not_a_Flag_This_is_Not_a_Flag_This_is_Not_a_Flag_This_is_Not_a_Fl

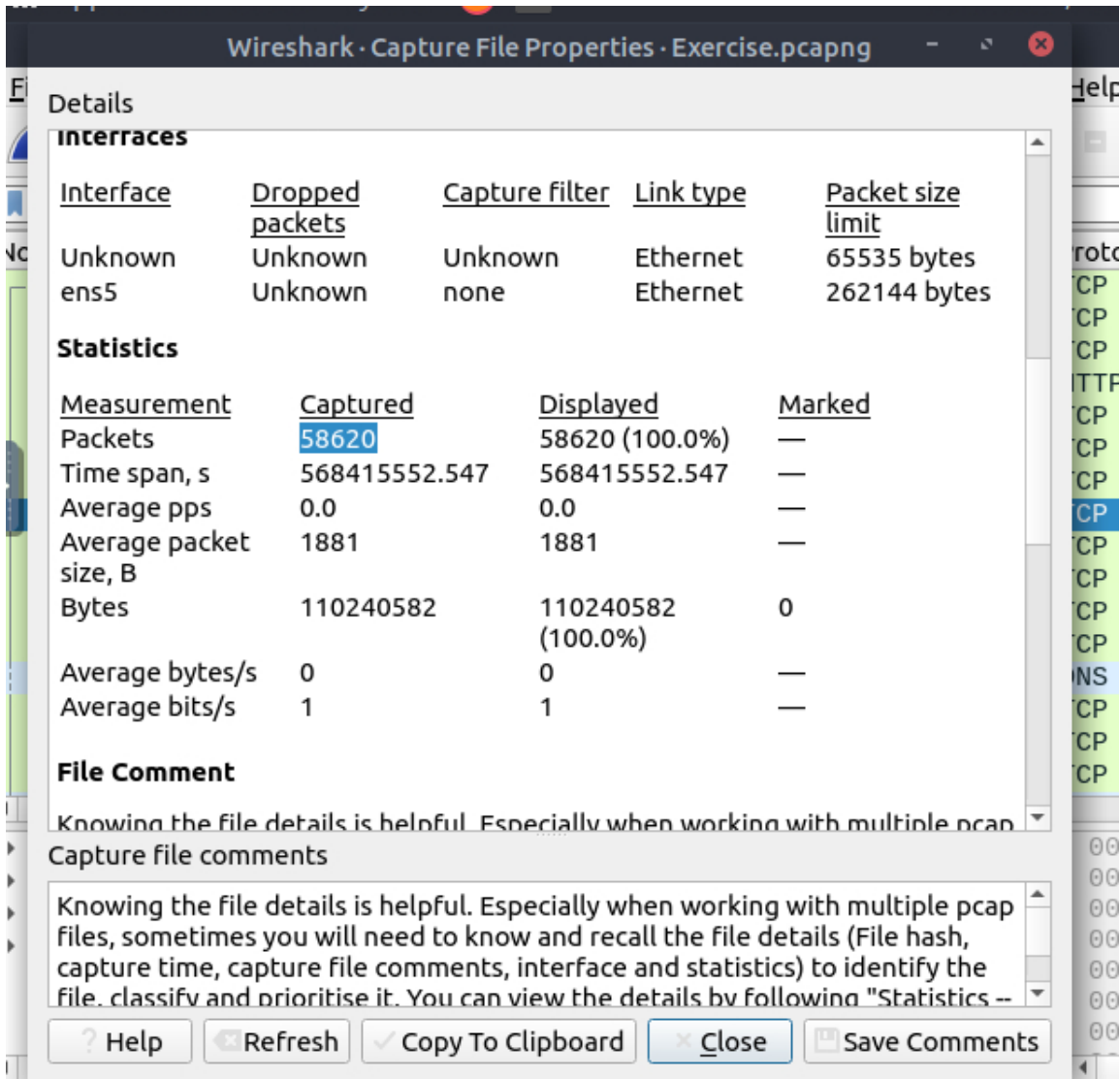
Capture file comments

Knowing the file details is helpful. Especially when working with multiple pcap files, sometimes you will need to know and recall the file details (File hash, capture time, capture file comments, interface and statistics) to identify the file. classifv and prioritise it. You can view the details by following "Statistics --

? Help Refresh Copy To Clipboard Close Save Comments

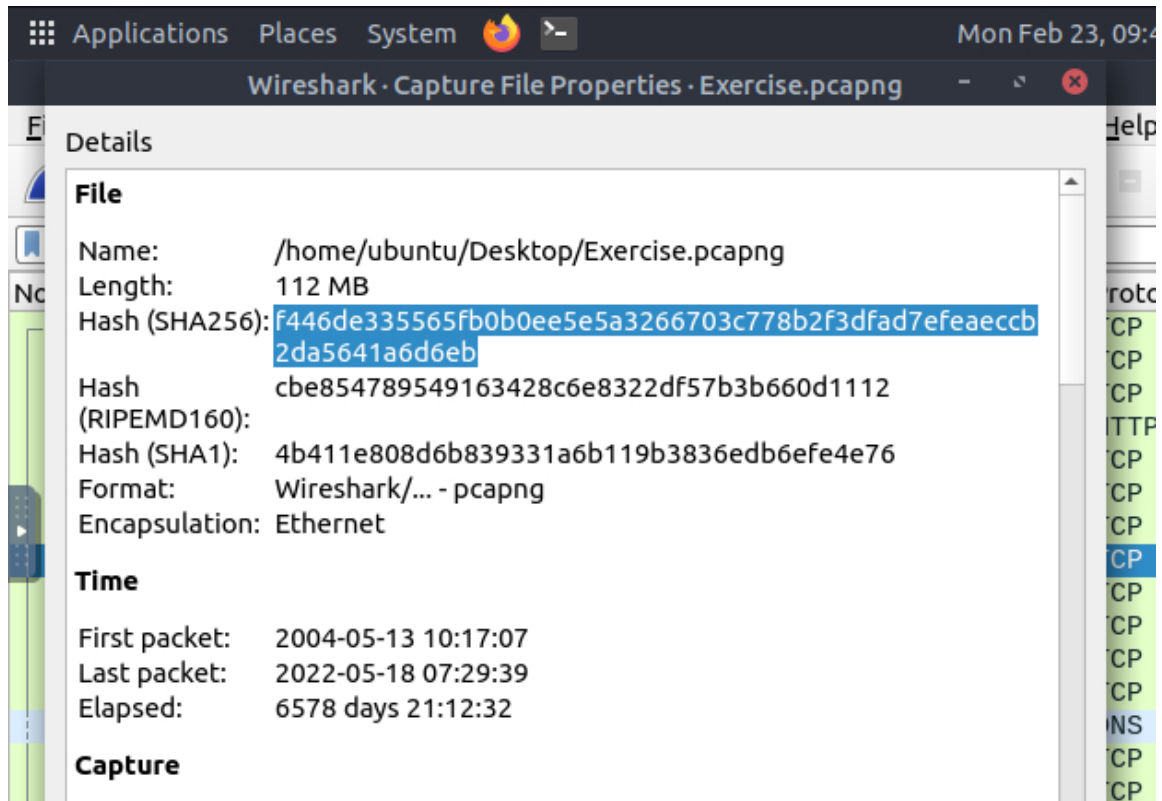
What is the total number of packets?

- Gå ind i: Statistics -> Capture File Properties
- Svar: 58620



What is the SHA256 hash value of the capture file?

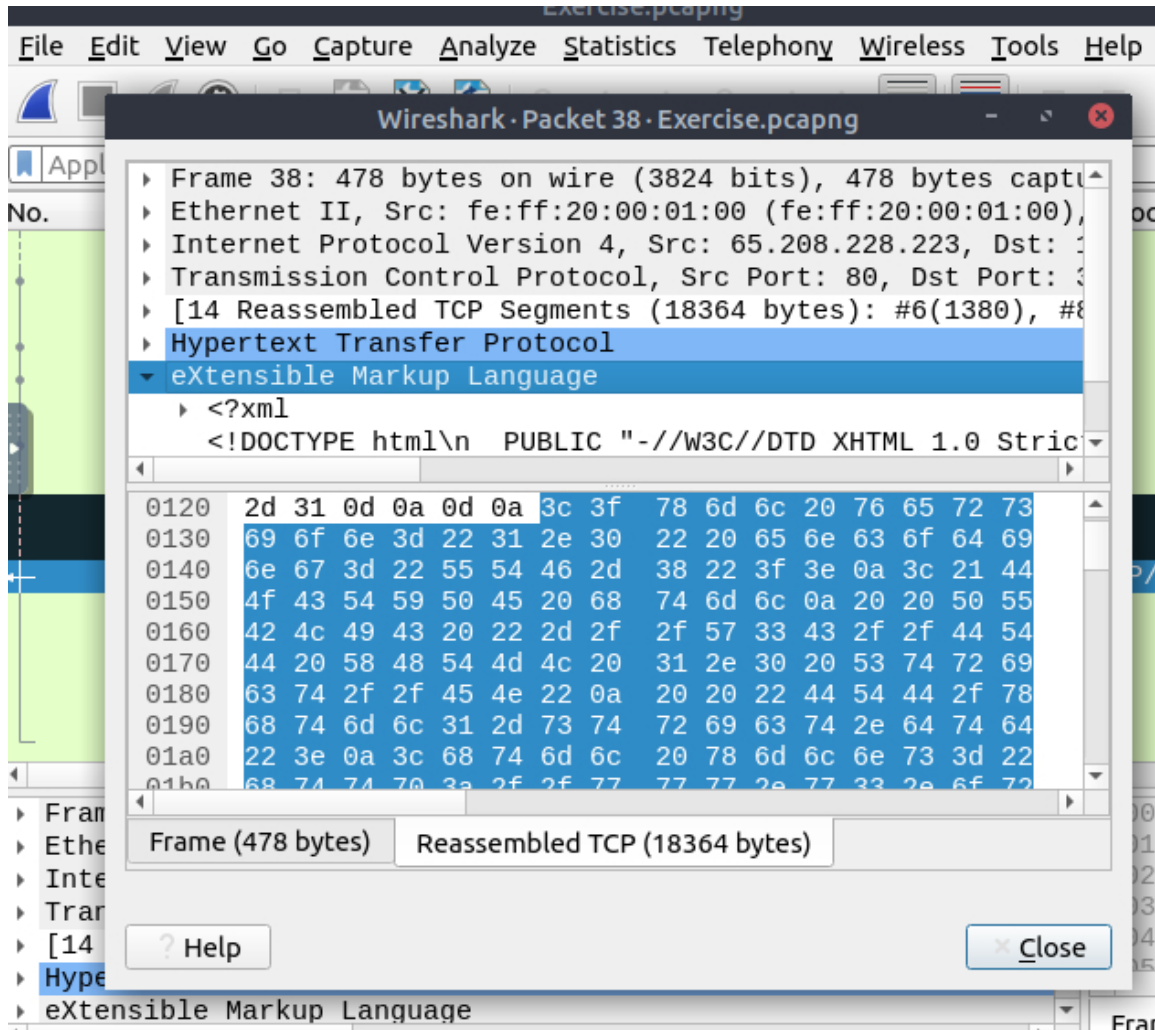
- Svar: f446de335565fb0b0ee5e5a3266703c778b2f3dfad7efeaeccb2da5641a6d6eb



Task 3 - Packet dissection

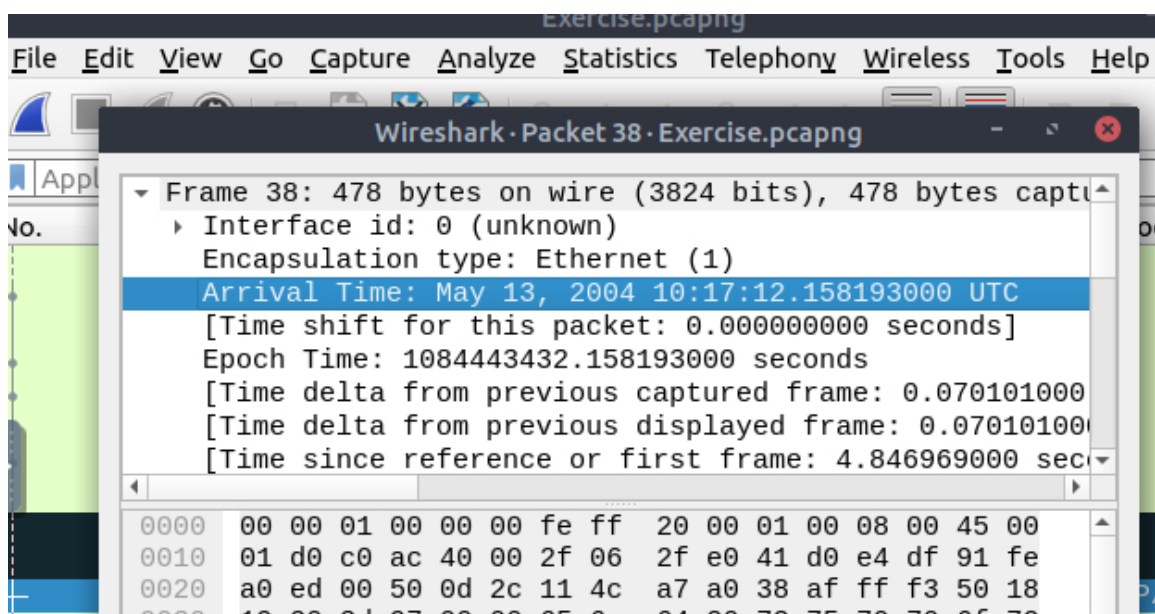
Use the "Exercise.pcapng" file to answer the questions. View packet number 38. Which markup language is used under the HTTP protocol?

- Svar: eXtensible Markup Language



What is the arrival date of the packet? (Answer format: Month/Day/Year)

- Svar: 05/13/2004



What is the TTL value?

- I samme menu som ovenfor, led efter "Time To Live"
- Svar: 47

What is the TCP payload size?

- I samme menu som ovenfor, led efter "TCP Payload"
- Svar: 424

What is the e-tag value?

- I samme menu som ovenfor, led efter "ETag"
- Svar: 9a01a-4696-7e354b00

Task 4 - Packet navigation

Use the "Exercise.pcapng" file to answer the questions. Search the "r4w" string in packet details. What is the name of artist 1?

- Svar: r4w8173

Go to packet 12 and read the packet comments. What is the answer? Note: use `md5sum <filename>` terminal command to get MD5 hash

- Packet 12 comment:

Go to packet number 39765
Look at the "packet details pane". Right-click on the JPEG section and "Export packet bytes". This is an alternative way of extracting data from a capture file. What is the MD5 hash value of extracted image?

- Svar: 911cd574a42865a956ccde2d04495ebf

```
ubuntu@ip-10-114-179-28: ~/Desktop
File Edit View Search Terminal Help
ubuntu@ip-10-114-179-28:~/Desktop$ md5sum bytes
911cd574a42865a956ccde2d04495ebf bytes
```

There is a ".txt" file inside the capture file. Find the file and read it; what is the alien's name?

- Gå til: file > export objects > http
- Svar: PACKETMASTER

Look at the expert info section. What is the number of warnings?

- Svar: 1636

Task 5 - Packet filtering

Use the "Exercise.pcapng" file to answer the questions. Go to packet number 4. Right-click on the "Hypertext Transfer Protocol" and apply it as a filter. Now, look at the filter pane. What is the filter query?

- Svar: http

What is the number of displayed packets?

- Svar: 1089

Go to packet number 33790, follow the HTTP stream, and look carefully at the responses. Looking at the web server's response, what is the total number of artists?

- Svar: 3

What is the name of the second artist?

- Svar: Blad3

🕒 2026-02-23 10:37:04