



Wireshark Basics

Wireshark is one of the most defined traffic analyzers used.

- Detecting and troubleshooting network problems, such as network load failure points and congestion.
- Detecting security anomalies, such as rogue hosts, abnormal port usage, and suspicious traffic/
- Investigating and learning protocol details, such as responses codes and payload data.

pcap (Packet Capture)

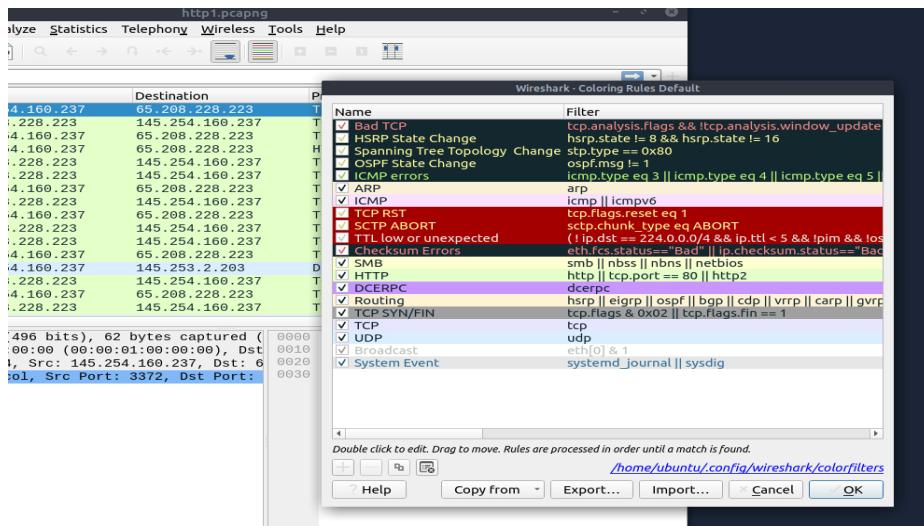
- is the standard file format used by Wireshark and other network analyzers to store data packets captured from a network
- To be able to analyze packages, you must upload a pcap (Packet Capture) file to Wireshark.

Colouring Packets

- Wireshark also color packets to differentiate conditions and can be customized based on the user.

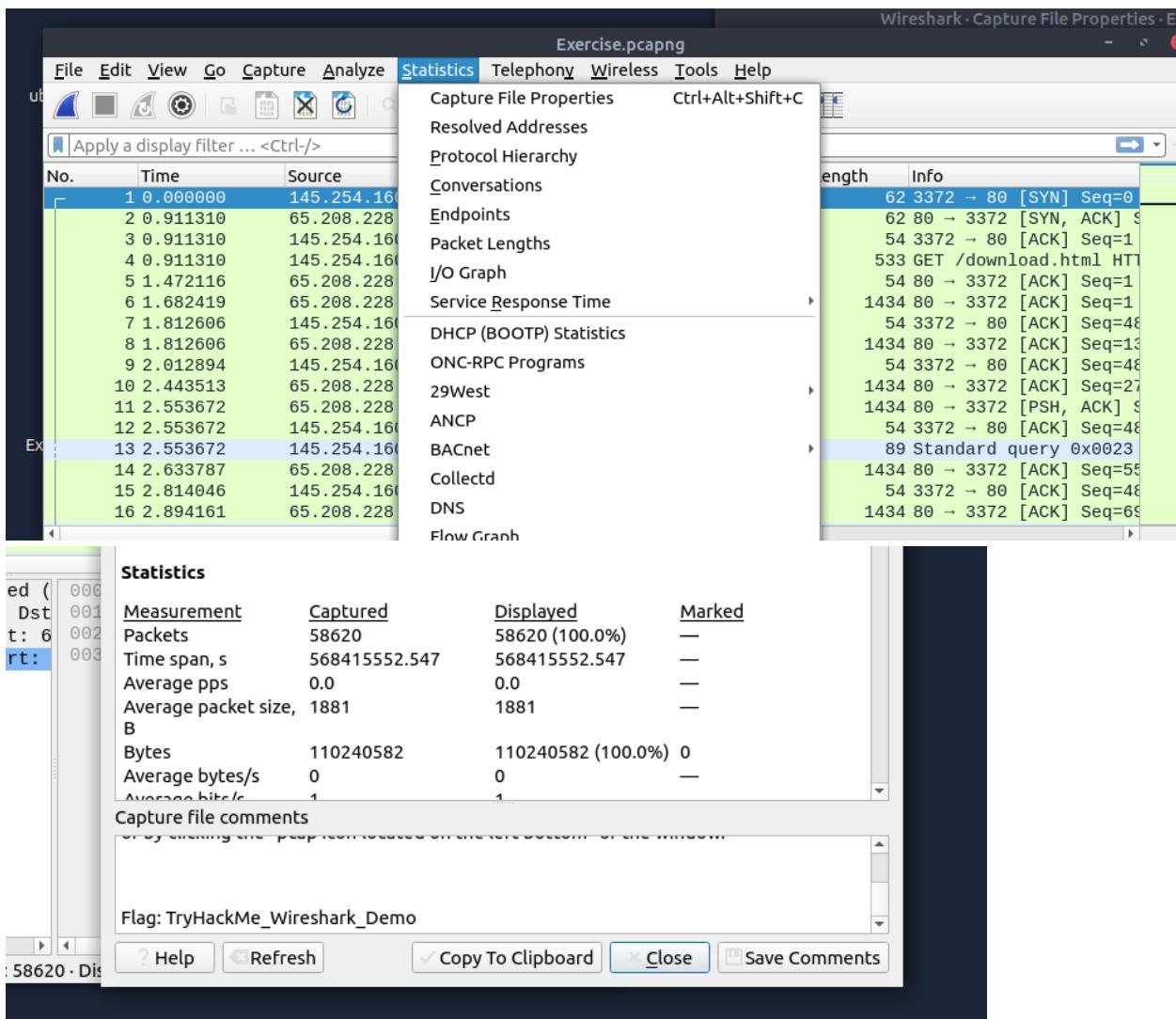
2 Methods:

- a. Temporary rules are only available during a program session.
- b. Permanent rules that are saved under the preference file (profile).



1. Using the exercise.pcapng file to answer the question. Read the “capture file comments” and find the flag?

- To read the capture file comment, first go to statistics and then view “Capture File Properties”

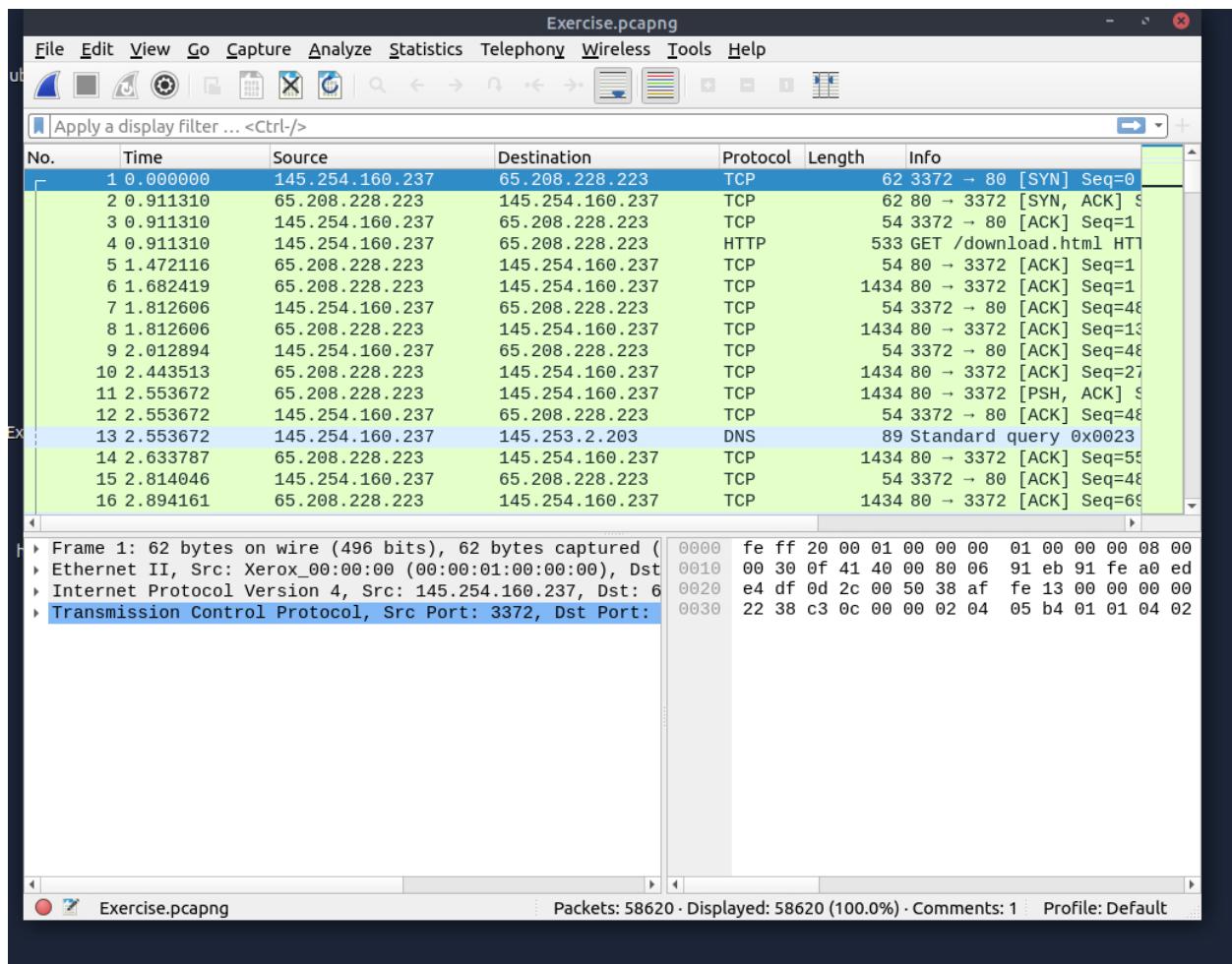


Answer: TryHackMe_Wireshark_Demo

- A screen will pop-up and in the “Capture file comments” scroll to the bottom of the comments.

2. What is the total number of packets?

- At the bottom of the Wireshark screen, you will see a bar that have information regarding “Packets” and “Displayed”

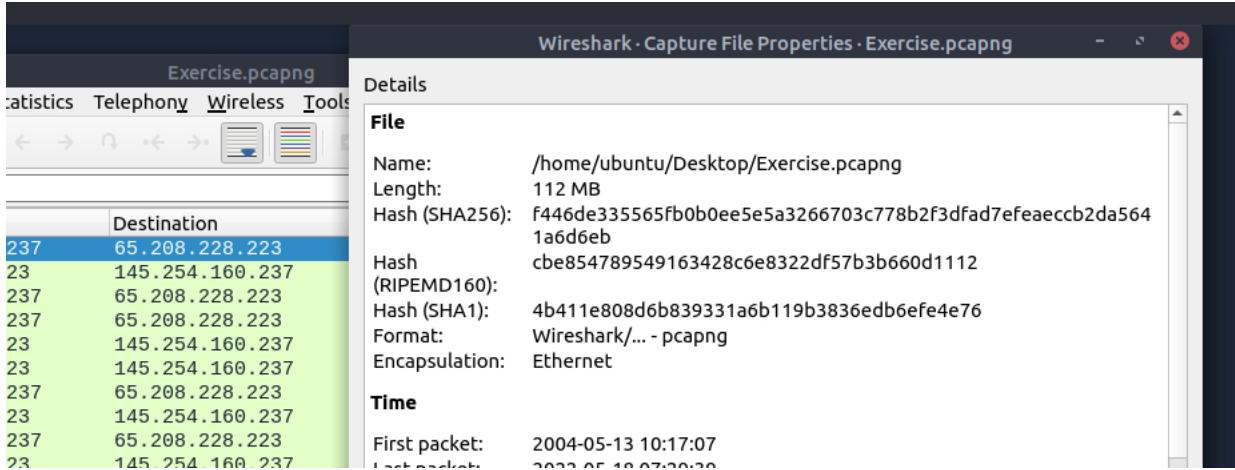


Answer: 58620

3. What is the SHA256 hash value of the capture file?

- A SHA256 hash is a cryptographic hash function that takes any size input and produces a unique 64 hexadecimal character.

- To identify the SHA256 hash, go back to the “Capture File Properties” and the sha256 value will be displayed.



Answer: f446de335565fb0b0ee5e5a3266703c778b2f3dfad7efeaecb2da5641a6d6eb

Packet Dissection

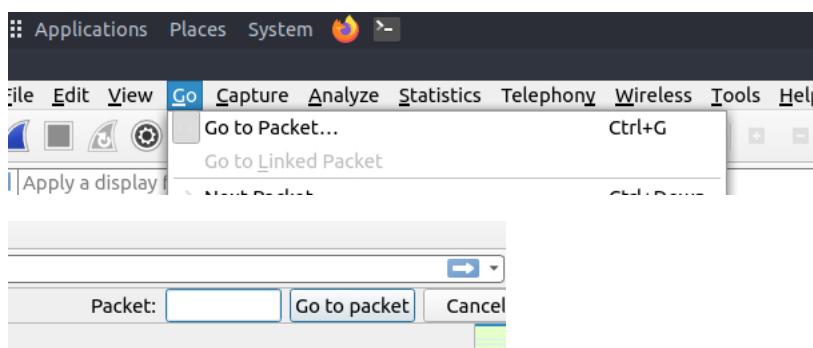
- Investigate packets for details by decoding available protocols and fields within Wireshark.

Packet Details

- By clicking on a packet, you can view the details (by double-clicking it; a new window will pop.)

1. Using the Exercise.pcapng, View packet number 38 and type the markup language is used under the HTTP protocol.

- To find a particular packet, click on the “Go menu” and select “Go to Packet” or scroll until you reach the desired packet.



```

TRANSMISSION CONTROL PROTOCOL, Src Port: 80, Dst Port: 3372, Seq: 17941, Ack: 480, Len: 424
[14 Reassembled TCP Segments (18364 bytes): #6(1380), #8(1380), #10(1380), #11(1380), #14(1380), #16(1380), #20(1380), #22(1380), #24(1380), #26(1380), #28(1380), #30(1380), #32(1380), #34(1380), #36(1380)]
Hypertext Transfer Protocol
eXtensible Markup Language

```

Answer: eXtensible Markup Language

2. What is the arrival date of the packet?

- Under that same packet number, you can find the arrival date in the “Frame” section.

```

35 4.496465 145.254.160.237 65.208.228.223 TCP 54 3372 -> 80 [ACK] Seq=480 Ack=17941 Win=9660 Len=0
36 4.776868 216.239.59.99 145.254.160.237 TCP 1484 [TCP Spurious Retransmission] 80 -> 3371 [PSH, ACK] Seq=1 Ack=...
37 4.776868 145.254.160.237 216.239.59.99 TCP 54 [TCP Dup ACK 28#1] 3371 -> 80 [ACK] Seq=722 Ack=1591 Win=8760 ...
38 4.846969 65.208.228.223 145.254.160.237 HTTP/X.. 478 HTTP/1.1 200 OK
39 5.017214 145.254.160.237 65.208.228.223 TCP 54 3372 -> 80 [ACK] Seq=480 Ack=18365 Win=9236 Len=0
40 5.017214 65.208.228.223 145.254.160.237 TCP 54 3372 -> 80 [ACK] Seq=480 Ack=18365 Win=9236 Len=0
Frame 38: 478 bytes on wire (3824 bits), 478 bytes captured (3824 bits) on interface unknown, id 0
  ▶ Interface id: 0 (unknown)
  ▶ Encapsulation type: Ethernet (1)
  Arrival Time: May 13, 2004 10:17:12.158193000 UTC
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1084443432.158193000 seconds
    [Time delta from previous captured frame: 0.070101000 seconds]
    [Time delta from previous displayed frame: 0.070101000 seconds]

```

Answer: 05/13/2024

3. What is the TTL value?

- You can find the Time To Live in the “Internet Protocol Version” section.

```

Ethernet II, Src: Te:TT:Z:Z (Te:TT:Z:Z)
Internet Protocol Version 4, Src: 65.208.228
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP:
    Total Length: 464
    Identification: 0xc0ac (49324)
  ▶ Flags: 0x4000, Don't fragment
    Fragment offset: 0
  Time to live: 47
  Protocol: TCP (6)
  Header checksum: 0x2fe0 [validation disabled]
    [Header checksum status: Unverified]

```

Answer: 47

4. What is the TCP payload size?

- You will be able to find the TCP payload size in the “Transmission Control Protocol” section.
- It will be displayed as “Len:123” or in the “[TCP Segment Len:123]”

```

Transmission Control Protocol, Src Port: 80, Dst Port: 3372, Seq: 17941, Ack: 480, Len: 424
  Source Port: 80
  Destination Port: 3372
  [Stream index: 0]
  [TCP Segment Len: 424]

```

Answer: 424

5. What is the e-tag value?

- You will be able to find the e-tag value in the “Hypertext Transfer Protocol” section and you will see “ETAG:”

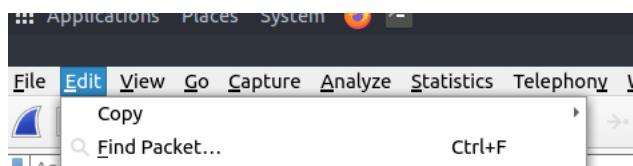
```
HTTP/1.1 200 OK\r\nDate: Thu, 13 May 2004 10:17:12 GMT\r\nServer: Apache\r\nLast-Modified: Tue, 20 Apr 2004 13:17:00 GMT\r\nETag: "9a01a-4696-7e354b00"\r\nAccept-Ranges: bytes\r\nContent-Length: 18070\r\n
```

Packet Navigation

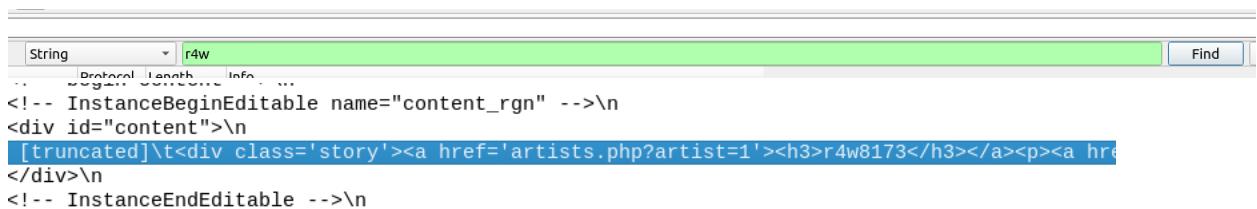
1. Using the “Exercise.pcapng” file, Search the “r4w” string in the packet details.

What is the name of artist 1?

- To find the artist within the packets. First go to the “Edit” -“Find packet”.



- In the search bar of “String”, type “r4w” and the n Wireshark will highlight the packet containing the “r4w” string.



Answer: r4w8173

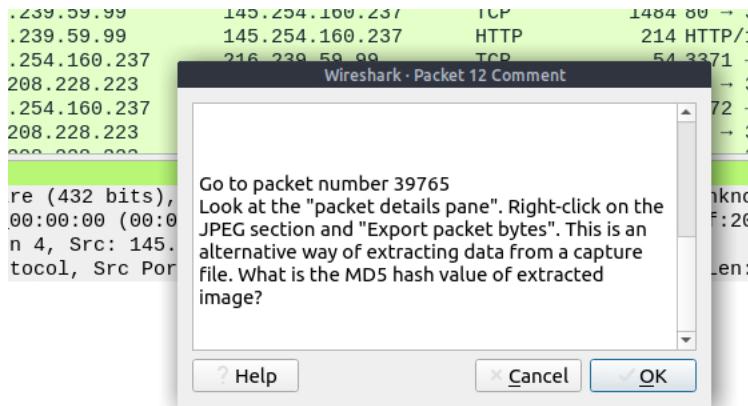
2. Go to packet 12 and read the packet comments. What is the answer?

Note: use md5sum <filename> terminal command to get MD5 hash

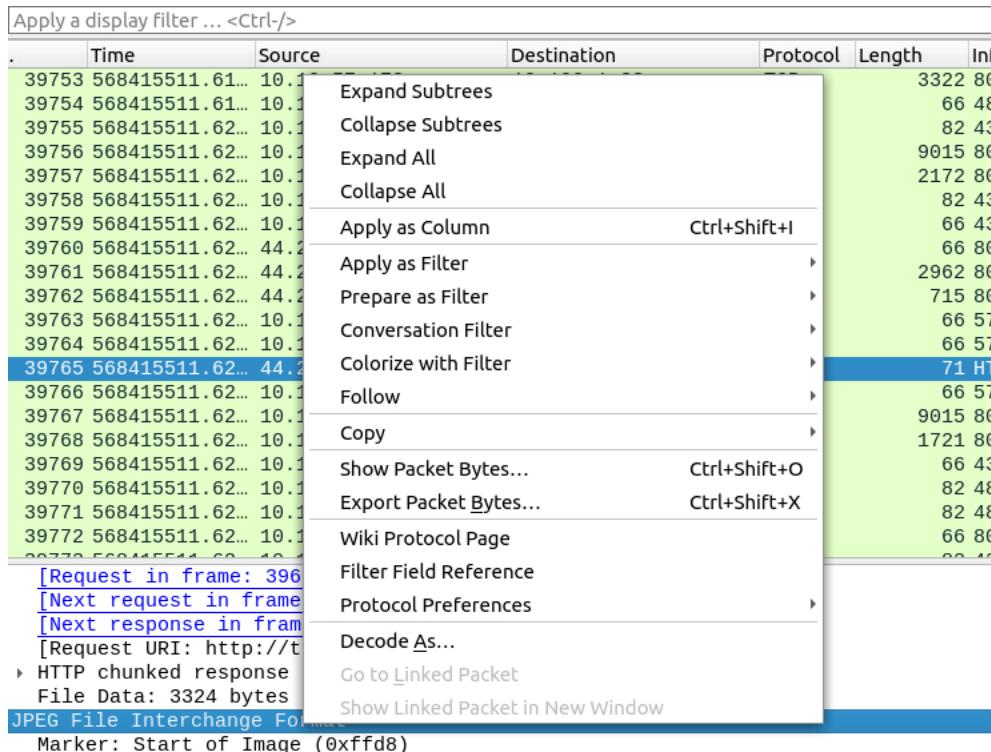
- First, let navigate to packet 12. Same method when looking for packet 38 (Go-Go to Packet – Type in the number of the packet)
- Next click on the “Packet comment to view the comment of the packet”

Apply a display filter ... <Ctrl-/>						
Time	Source	Destination	Protocol	Length	Info	
12 2.553672	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [ACK] Seq=480 Ack=5521 Win=9660 Len=0	Mark/Unmark Packet(s) Ignore/Unignore Packet(s) Set/Unset Time Reference Time Shift... Packet Comment...
13 2.553672	145.254.160.237	145.253.2.203				Ctrl+M Ctrl+D Ctrl+T Ctrl+Shift+T Ctrl+Alt+C
14 2.633787	65.208.228.223	145.254.160.237				A pagead2.googlesyndication.co 21 Ack=480 Win=6432 Len=1380 0 Ack=6901 Win=9660 Len=0 91 Ack=480 Win=6432 Len=1380 e 0x0023 A pagead2.googlesyndicat
15 2.814046	145.254.160.237	65.208.228.223				ca-pub-2309191948673629&rand
16 2.894161	65.208.228.223	145.254.160.237				9 Ack=8281 Win=9660 Len=0
17 2.914190	145.253.2.203	145.254.160.237				
18 2.984291	145.254.160.237	216.239.59.99				
19 3.014334	145.254.160.237	65.208.228.223				

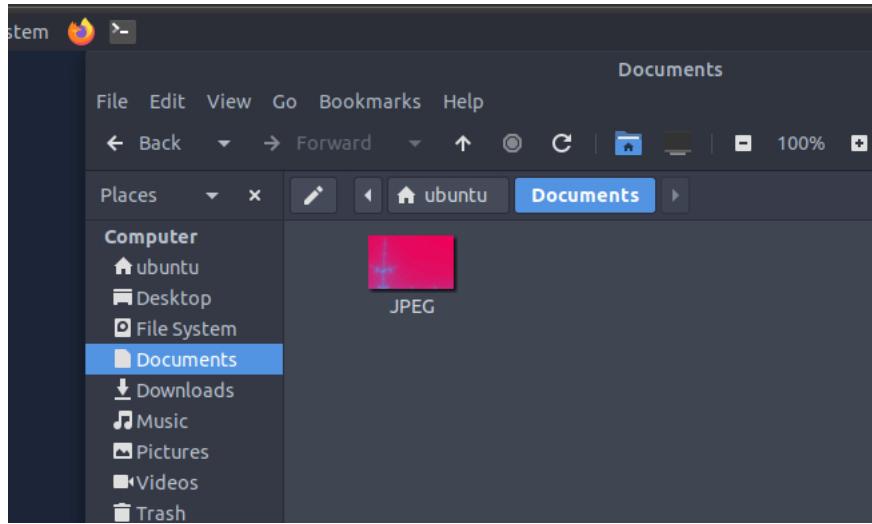
- Scroll to the bottom of the comments on the packet. There will be further instructions on determining the MD5 hash value.



- Now we must navigate to packet: 39765 and follow the instructions to receive the MD5 hash value.
- Repeat the “Go to packet” Method
- As described, right-click on the JPEG file and click on the “Export Package Byte”.



- Once exported, save the file in a directory. In the case, I saved it in the Documents directory and must give the file a name.



- Finally open the unix/linux terminal and navigate to the directory and run the command **md5sum <filename>**

```
Documents
File Edit View Go Bookmarks Help
← Back → Forward ↑ ⌘ C | ⌘ ⌘ 100% + 
Places ubuntu Documents
Computer
  ↗ ubuntu
  ↗ Desktop
  ↗ File System
  ↗ Documents
  ↗ Downloads
  ↗ Music
  ↗ Pictures
  ↗ Videos
  ↗ Trash
Documents
Icon View
Places
ubuntu@ip-10-64-145-158:~/Documents
Com File Edit View Search Terminal Help
↑ubuntu@ip-10-64-145-158:~$ ls
[Desktop Documents Downloads Music Pictures Public Templates Videos
↑ubuntu@ip-10-64-145-158:~$ cd Documents
↑ubuntu@ip-10-64-145-158:~/Documents$ ls
JPEG
↑ubuntu@ip-10-64-145-158:~/Documents$ md5sum JPEG
911cd574a42865a956ccde2d04495ebf  JPEG
↑ubuntu@ip-10-64-145-158:~/Documents$
```

Answer: 911cd574a42865a956ccde2d04495ebf

3. There is a “.txt” file inside the capture file. Find the file and read it: what is the alien’s name?

- Go to the “Go to Packet” and search for the “.txt” file

vide	Case sensitive	String	.txt	
	Destination	Protocol	Length	Info
7.178	44.228.249.3	HTTP	431	GET /showimage.php?file=../pictures/1.jpg&size=160 HTTP/1.1
7.178	44.228.249.3	HTTP	512	GET /showimage.php?file=../pictures/2.jpg HTTP/1.1
7.178	44.228.249.3	HTTP	431	GET /showimage.php?file=../pictures/2.jpg&size=160 HTTP/1.1
7.178	44.228.249.3	HTTP	431	GET /showimage.php?file=../pictures/3.jpg&size=160 HTTP/1.1
7.178	44.228.249.3	HTTP	431	GET /showimage.php?file=../pictures/4.jpg&size=160 HTTP/1.1
7.178	44.228.249.3	HTTP	431	GET /showimage.php?file=../pictures/5.jpg&size=160 HTTP/1.1
7.178	44.228.249.3	HTTP	431	GET /showimage.php?file=../pictures/7.jpg&size=160 HTTP/1.1
7.123	10.10.57.178	HTTP	404	HTTP/1.0 200 OK (text/html)
7.123	10.10.57.178	HTTP	5520	HTTP/1.0 200 OK (text/plain)
7.123	10.10.57.178	HTTP	535	HTTP/1.0 404 File not found (text/html)
228.223	145.254.160.237	HTTP/X...	478	HTTP/1.1 200 OK
249.3	10.10.57.178	HTTP	1516	HTTP/1.1 200 OK (JPEG JFIF image)
249.3	10.10.57.178	HTTP	71	HTTP/1.1 200 OK (JPEG JFIF image)
249.3	10.10.57.178	HTTP	1515	HTTP/1.1 200 OK (JPEG JFIF image)

- Notice, there is a plain text file right beneath the “.txt” file. Let click on it and observe its output.

- There are two options.

- a. Option 1: read the output of the plain text file on Wireshark

- b. Option 2: copy the hexadecimal and use Cyberchef to decode Hex dump

The screenshot shows the CyberChef interface. In the 'Input' pane, there is a large block of hex data starting with 1520 and ending with 1600. The 'Output' pane shows the corresponding ASCII text, which includes a JSON object and some binary data represented as black squares. At the bottom of the interface, there is a green button labeled 'BAKE!'. The CyberChef interface has a clean, modern design with a light blue header and a white main area.

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

- To locate the number of warnings, go to “Analyze-Expert Information”

The screenshot shows the Wireshark interface with the 'Expert' tab selected. A list of warnings is displayed, with one specific warning highlighted in yellow. The warning text is: "HTTP: Invalid response code 'HTTP/2'". Other items in the list include "HTTP: Invalid response code 'HTTP/2'" (unhighlighted), "HTTP: Invalid response code 'HTTP/2'" (unhighlighted), "HTTP: Invalid response code 'HTTP/2'" (unhighlighted), and "HTTP: Invalid response code 'HTTP/2'" (unhighlighted). The Wireshark interface has a dark theme with a light blue header and a white main area.

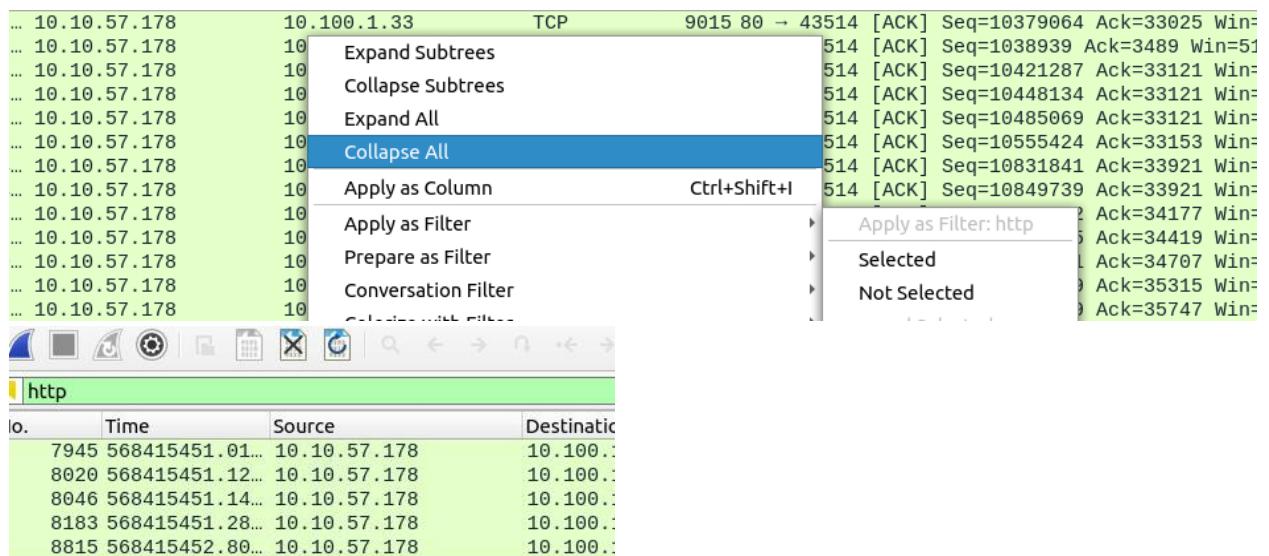
Wireshark - Expert Information - Exercise.pcapng				
Severity	Summary	Group	Protocol	Count
> Error	Malformed Packet (Exception occurred)	Malformed	HTTP	13
> Error	Malformed Packet (Exception occurred)	Malformed	JFIF (JPEG) ...	2
> Warning	Illegal characters found in header name	Protocol	HTTP	1636
> Note	ACK to a TCP keep-alive segment	Sequence	TCP	23
> Note	TCP keep-alive segment	Sequence	TCP	23
> Note	Duplicate ACK (#1)	Sequence	TCP	1
> Note	This frame is a (suspected) spurious retransmission	Sequence	TCP	1
> Note	This frame is a (suspected) retransmission	Sequence	TCP	1
> Chat	Connection finish (FIN)	Sequence	TCP	12
> Chat	GET /download.html HTTP/1.1\r\n	Sequence	HTTP	40
> Chat	Connection establish acknowledge (SYN+ACK): server port 80	Sequence	TCP	1
				12

Answer: 1636

Packet Filtering

1. Go to packet number 4. Right-Click on the “Hypertext Transfer Protocol” and apply it as a filter. What is the filter query?

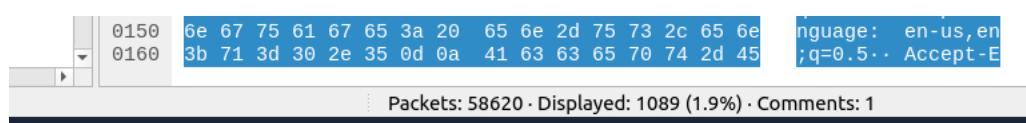
- Let first navigate to the packet using “Go to Packet”
- Once we get to the packet, let's go to the Hypertext Transfer Protocol and right-click, then select “Apply as Filter”



Answer: http

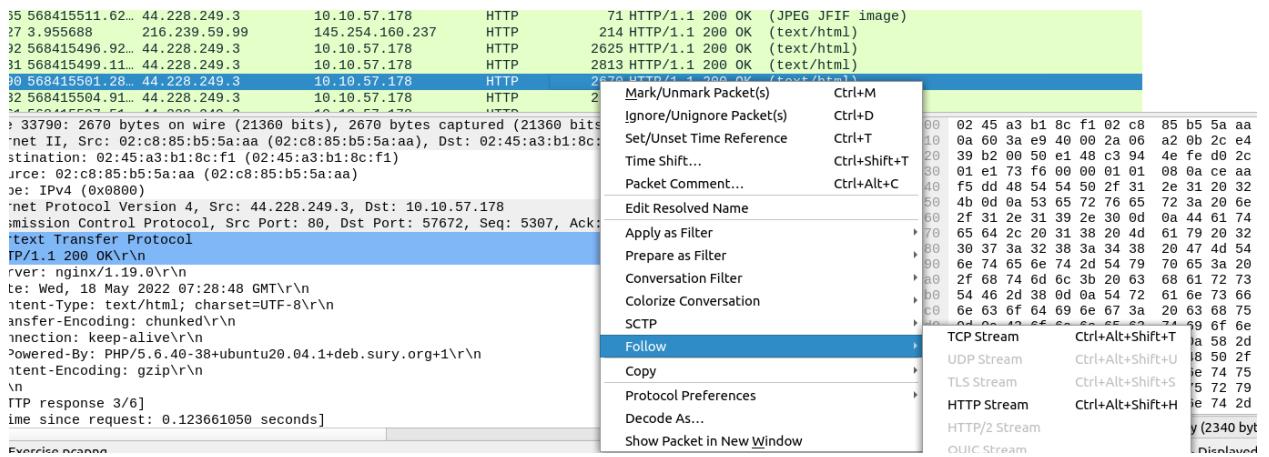
2. What is the number of displayed packets?

- You will find this at the bottom on the bar.



3. 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?

- Same method, navigate to 33790 packet using “Go to Packet”
- Right-click on the packet and select the “Follow - HTTP stream”



- At this stage, we must analyze the http stream to determine the number of Artist.
- Usually represented as “Artist=1” and so forth.

```

<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
    <div class='story'><a href='artists.php?artist=1'><h3>r4w8173</h3></a><p><a href='#'
onClick="window.open('./comment.php?aid=1','comment','width=500,height=400')">comment on this
artist</a></p></div><div class='story'><a href='artists.php?artist=2'><h3>Blad3</h3></a><p><a
href='#' onClick="window.open('./comment.php?aid=2','comment','width=500,height=400')">comment
on this artist</a></p></div><div class='story'><a href='artists.php?artist=3'><h3>lyzae</h3></a><p><a href='#'
onClick="window.open('./comment.php?
aid=3','comment','width=500,height=400')">comment on this artist</a></p></div>
</div>
<!-- InstanceEndEditable -->
<!--end content -->
<div id="navBar">
    <div id="search">

```

Answer: 3

4. What is the name of the 2nd artist?

```

10.57.17 <!-- InstanceBeginEditable name="content_rgn" -->
10.57.17 <div id="content">
10.57.17     <div class='story'><a href='artists.php?artist=1'><h3>r4w8173</h3></a><p><a href='#'
10.57.17     onClick="window.open('./comment.php?aid=1','comment','width=500,height=400')">comment on this
10.57.17     artist</a></p></div><div class='story'><a href='artists.php?artist=2'><h3>Blad3</h3></a><p><a
228.249. href='#' onClick="window.open('./comment.php?aid=2','comment','width=500,height=400')">comment
228.249. on this artist</a></p></div><div class='story'><a href='artists.php?artist=3'><h3>lyzae</h3></a><p><a href='#'
228.249.     onClick="window.open('./comment.php?
228.249.     aid=3','comment','width=500,height=400')">comment on this artist</a></p></div>

```

Answer: Blad3