



## 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)**

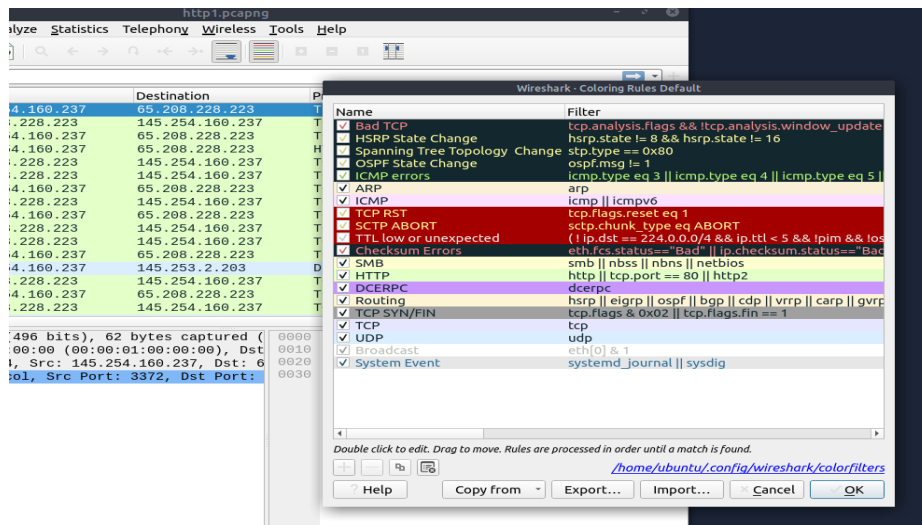
- is the standard file format used by Wireshark and other network analyzers to store data packets captured from a network
- To be able to analyze packages, you must upload a pcap (Packet Capture) file to Wireshark.

### **Colouring Packets**

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

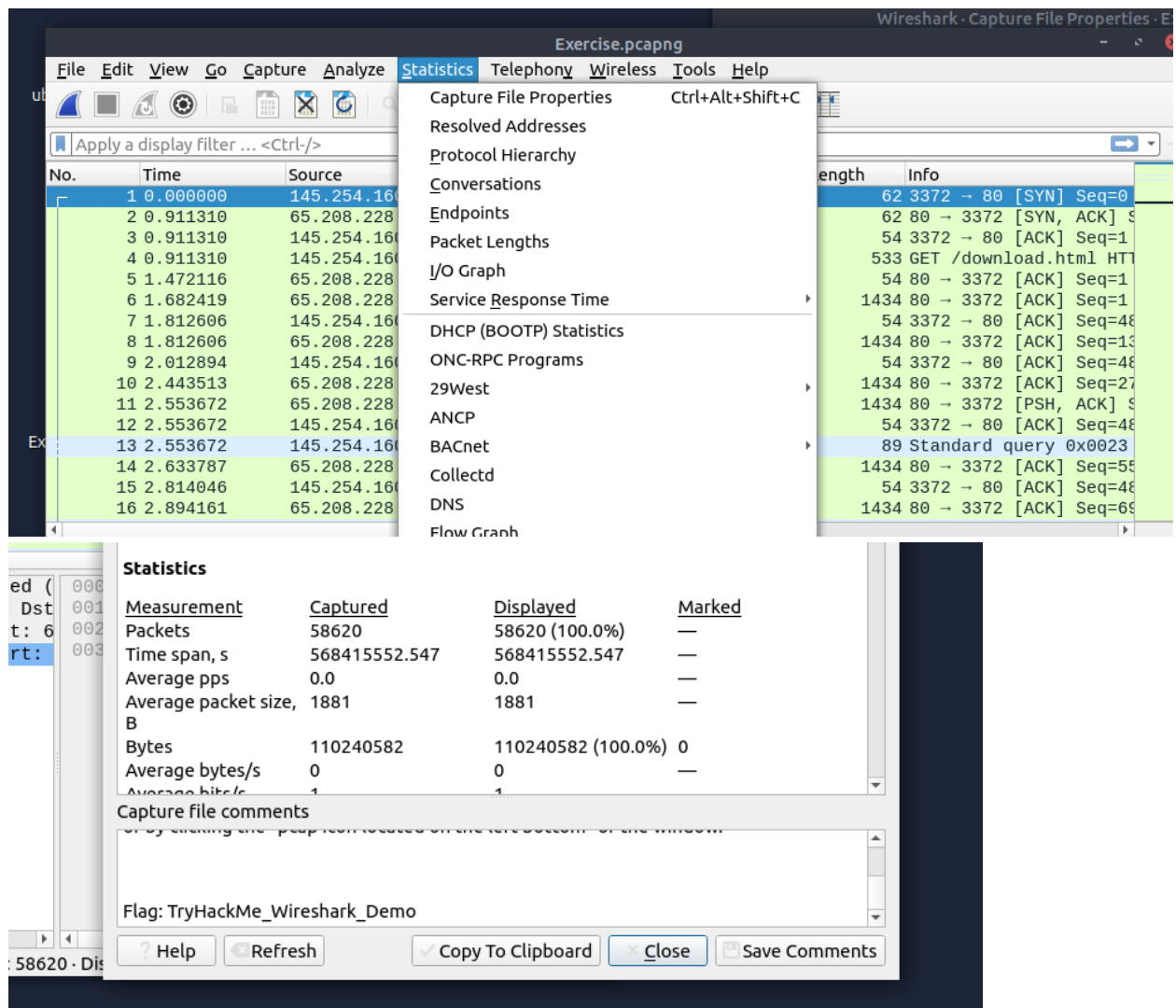
2 Methods:

- 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”

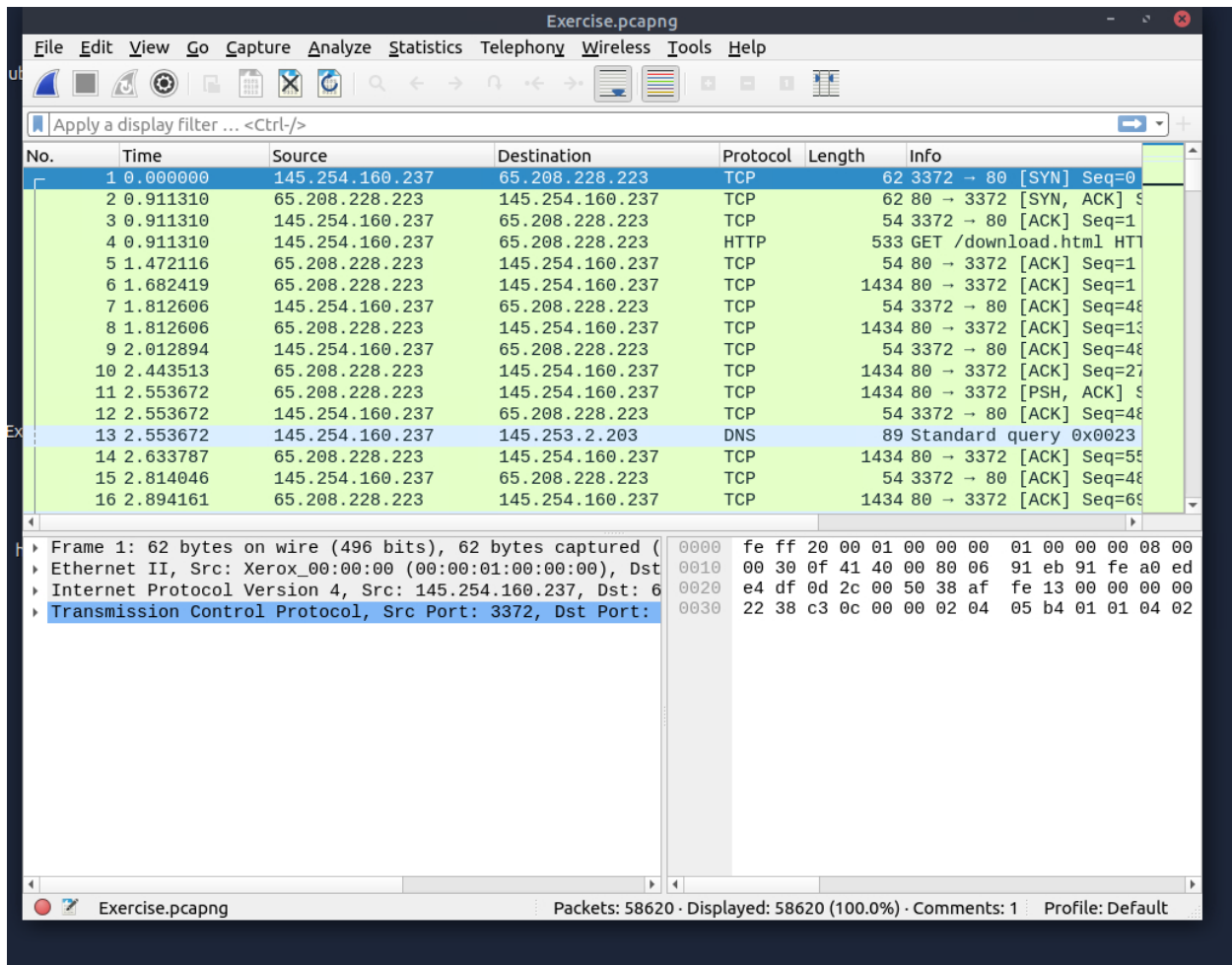


Answer: TryHackMe\_Wireshark\_Demo

- 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”

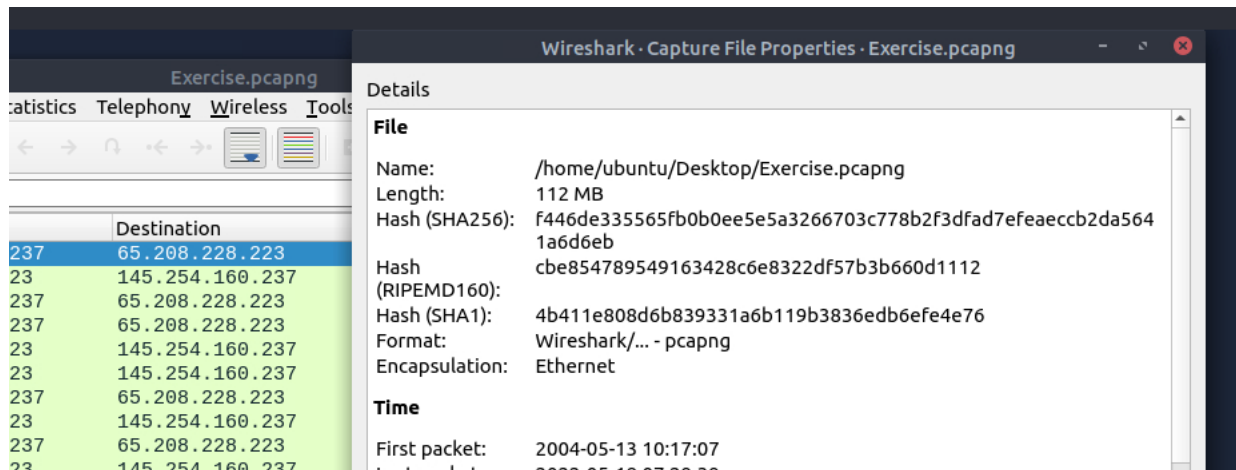


Answer: 58620

### 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: f446de335565fb0b0ee5e5a3266703c778b2f3dfad7efeaeccb2da5641a6d6eb

### Packet Dissection

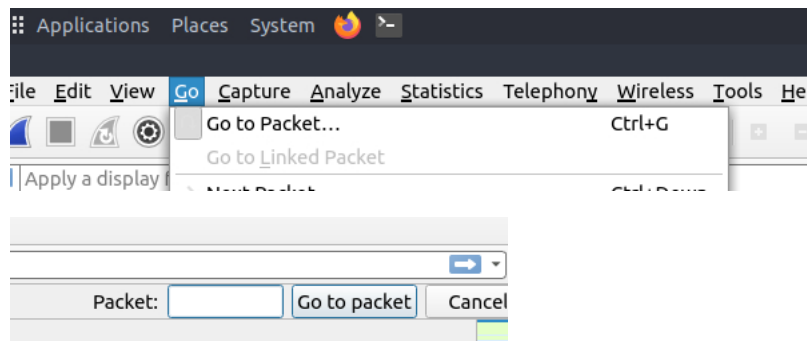
- Investigate packets for details by decoding available protocols and fields within Wireshark.

### 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.



Answer: eXtensible Markup Language

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

Answer: 05/13/2024

```

Ethernet II, Src: Te:FF:20:00:01:00 (Te:FF:20:00:01:00:00), Dst: 08:00:27:00:00:00 (08:00:27:00:00:00)
Internet Protocol Version 4, Src: 65.208.228.100, Dst: 10.0.2.15
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    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

- 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]”

Answer: 424

## 5. What is the e-tag value?

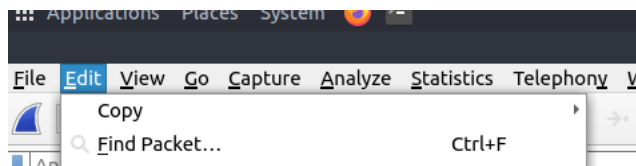
- You will be able to find the e-tag value in the “Hypertext Transfer Protocol” section and you will see “ETAG:”

```
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
    Date: Thu, 13 May 2004 10:17:12 GMT\r\n
    Server: Apache\r\n
    Last-Modified: Tue, 20 Apr 2004 13:17:00 GMT\r\n
    ETag: "9a01a-4696-7e354b00"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 18070\r\n
```

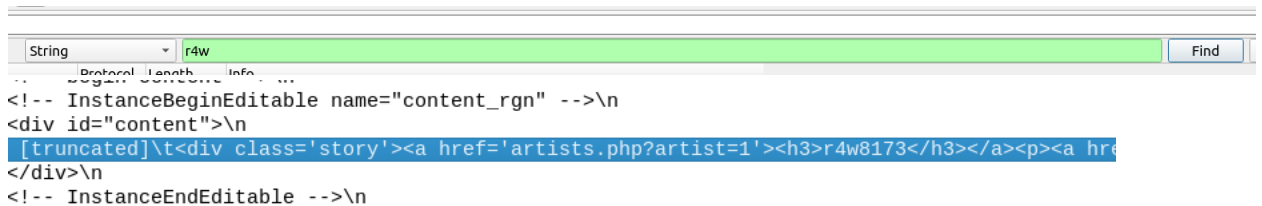
## Packet Navigation

### 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?

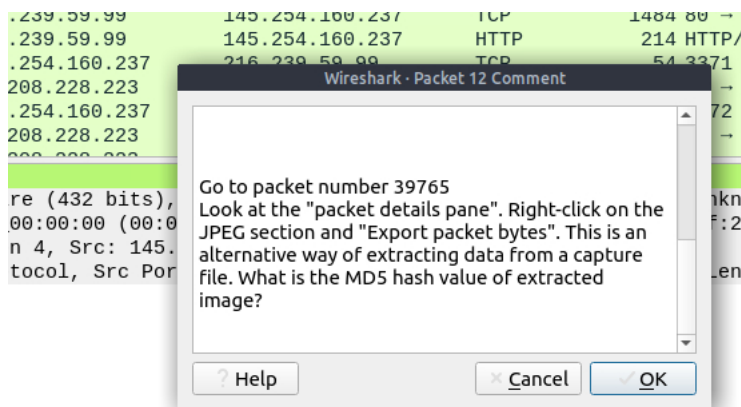
Note: use md5sum <filename> terminal command to get MD5 hash

- 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”

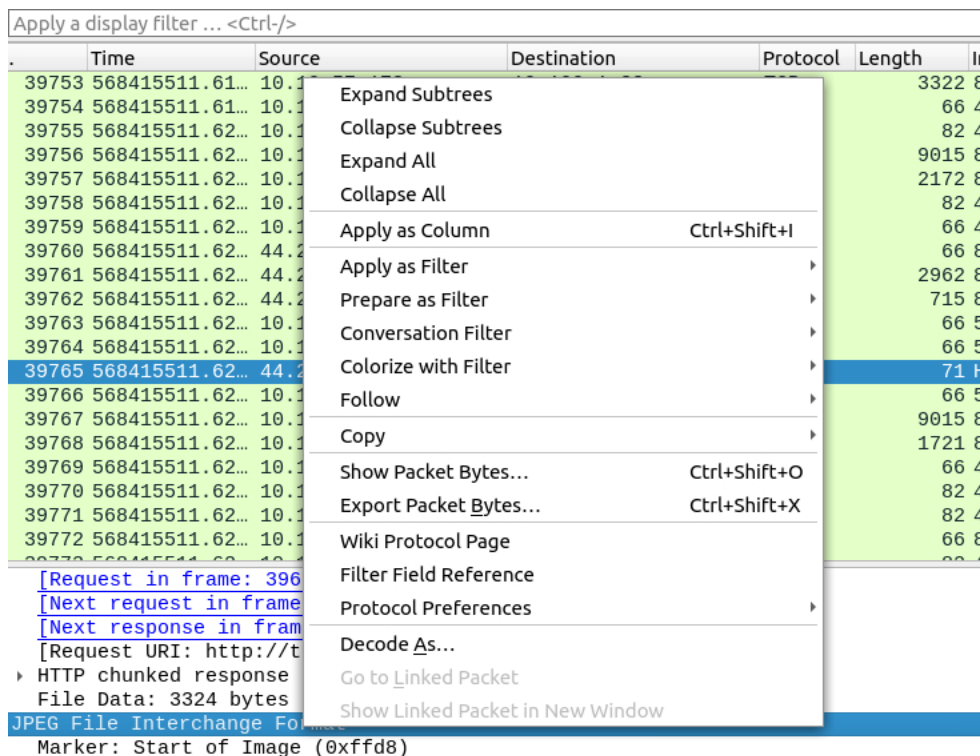
Apply a display filter ... <Ctrl-/>

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
13 2.553672	145.254.160.237	145.253.2.203			Mark/Unmark Packet(s) Ctrl+M
14 2.633787	65.208.228.223	145.254.160.237			Ignore/Unignore Packet(s) Ctrl+D
15 2.814046	145.254.160.237	65.208.228.223			Set/Unset Time Reference Ctrl+T
16 2.894161	65.208.228.223	145.254.160.237			Time Shift... Ctrl+Shift+T
17 2.914190	145.253.2.203	145.254.160.237			Packet Comment... Ctrl+Alt+C
18 2.984291	145.254.160.237	216.239.59.99			
19 3.014334	145.254.160.237	65.208.228.223			

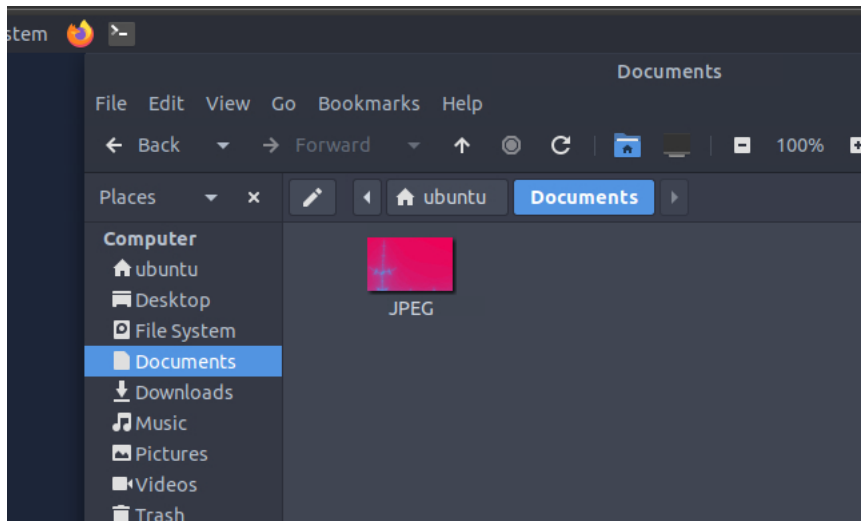
- Scroll to the bottom of the comments on the packet. There will be further instructions on determining the MD5 hash value.



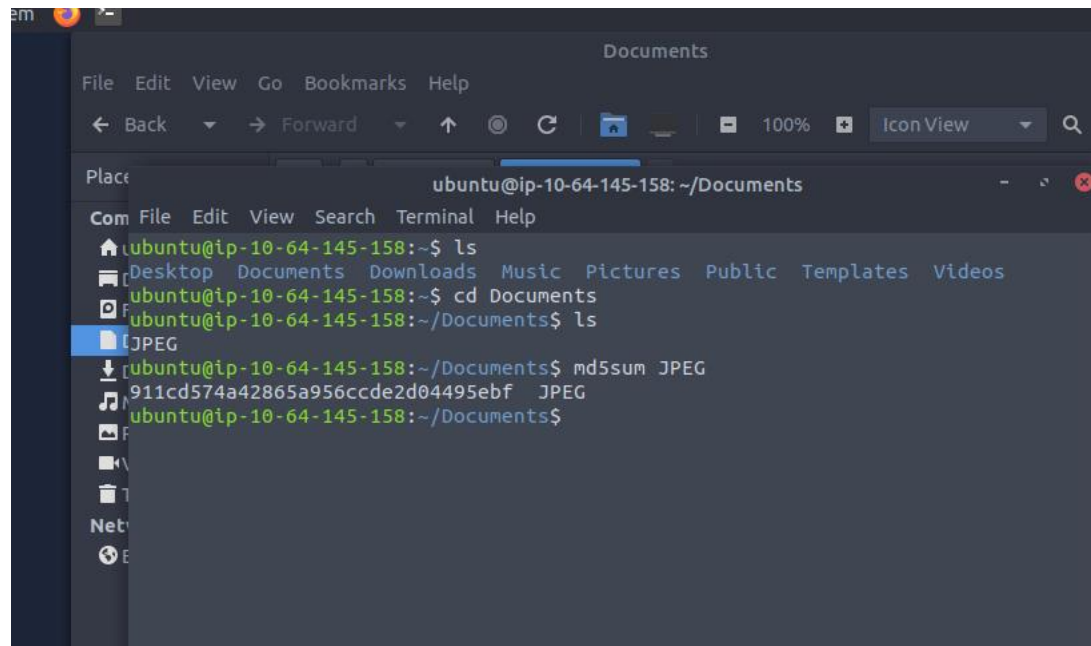
- Now we must navigate to packet: 39765 and follow the instructions to receive the MD5 hash value.
- Repeat the “Go to packet” Method
- As described, right-click on the JPEG file and click on the “Export Package Byte”.



- 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.



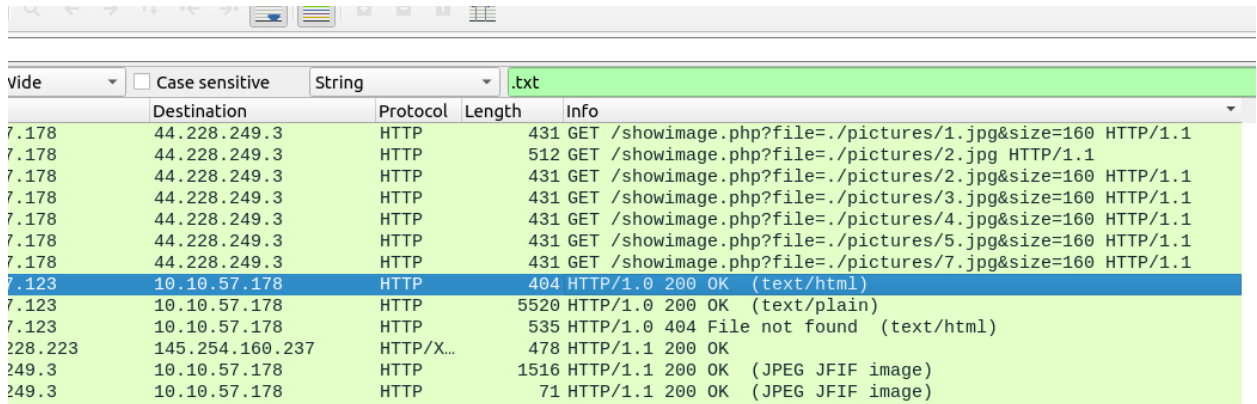
- Finally open the unix/linux terminal and navigate to the directory and run the command **md5sum <filename>**



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

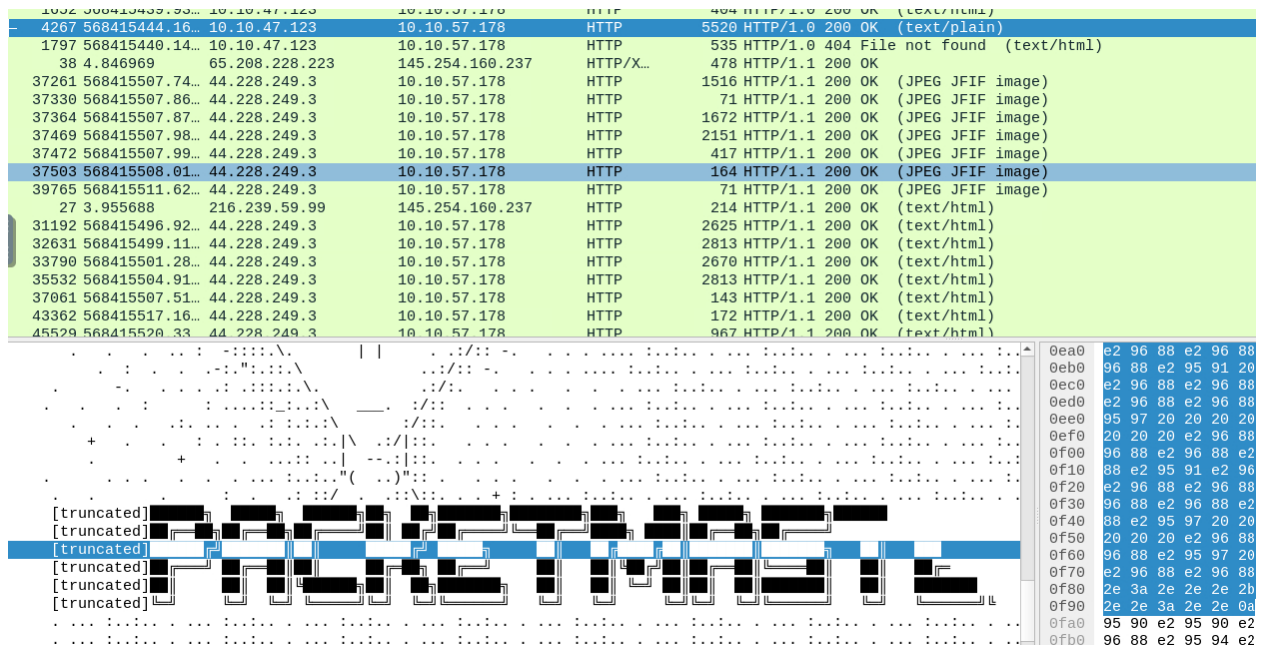


Wireshark packet list showing search results for ".txt". The search filter is ".txt". The results show several HTTP GET requests for image files (1.jpg to 7.jpg) and one HTTP 404 response for a file not found. The packet list is as follows:

No.	Time	Source	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)			

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

- There are two options.
  - Option 1: read the output of the plain text file on Wireshark



Wireshark packet list and packet details showing the output of the plain text file. The packet list is as follows:

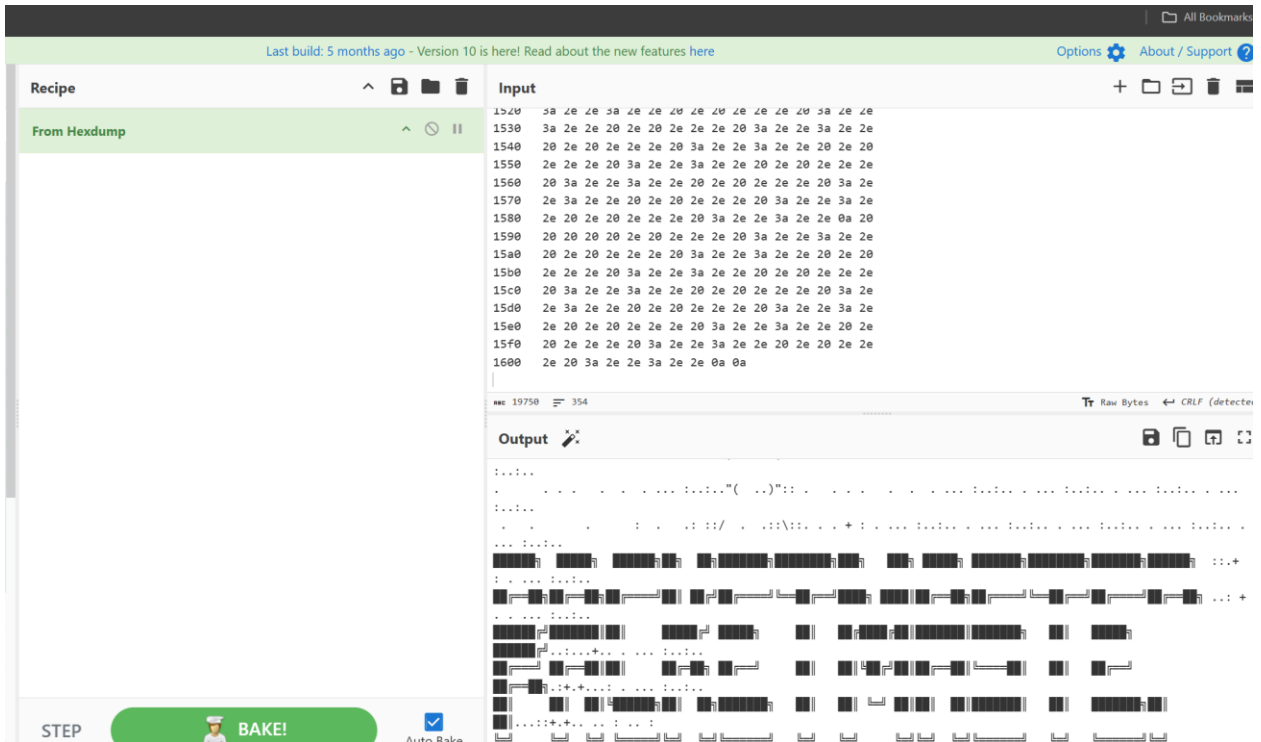
No.	Time	Source	Destination	Protocol	Length	Info
4267	568415444.16...	10.10.47.123	10.10.57.178	HTTP	5520	HTTP/1.0 200 OK (text/plain)
1797	568415440.14...	10.10.47.123	10.10.57.178	HTTP	535	HTTP/1.0 404 File not found (text/html)
38	4.846969	65.208.228.223	145.254.160.237	HTTP/X...	478	HTTP/1.1 200 OK
37261	568415507.74...	44.228.249.3	10.10.57.178	HTTP	1516	HTTP/1.1 200 OK (JPEG JFIF image)
37330	568415507.86...	44.228.249.3	10.10.57.178	HTTP	71	HTTP/1.1 200 OK (JPEG JFIF image)
37364	568415507.87...	44.228.249.3	10.10.57.178	HTTP	1672	HTTP/1.1 200 OK (JPEG JFIF image)
37469	568415507.98...	44.228.249.3	10.10.57.178	HTTP	2151	HTTP/1.1 200 OK (JPEG JFIF image)
37472	568415507.99...	44.228.249.3	10.10.57.178	HTTP	417	HTTP/1.1 200 OK (JPEG JFIF image)
37503	568415508.01...	44.228.249.3	10.10.57.178	HTTP	164	HTTP/1.1 200 OK (JPEG JFIF image)
39765	568415511.62...	44.228.249.3	10.10.57.178	HTTP	71	HTTP/1.1 200 OK (JPEG JFIF image)
27	3.955688	216.239.59.99	145.254.160.237	HTTP	214	HTTP/1.1 200 OK (text/html)
31192	568415496.92...	44.228.249.3	10.10.57.178	HTTP	2625	HTTP/1.1 200 OK (text/html)
32631	568415499.11...	44.228.249.3	10.10.57.178	HTTP	2813	HTTP/1.1 200 OK (text/html)
33790	568415501.28...	44.228.249.3	10.10.57.178	HTTP	2670	HTTP/1.1 200 OK (text/html)
35532	568415504.91...	44.228.249.3	10.10.57.178	HTTP	2813	HTTP/1.1 200 OK (text/html)
37061	568415507.51...	44.228.249.3	10.10.57.178	HTTP	143	HTTP/1.1 200 OK (text/html)
43362	568415517.16...	44.228.249.3	10.10.57.178	HTTP	172	HTTP/1.1 200 OK (text/html)
45529	568415520.33...	44.228.249.3	10.10.57.178	HTTP	967	HTTP/1.1 200 OK (text/html)

The packet details for the selected packet (4267) show the following structure:

- Frame 4267: 5520 bytes on wire (44160 bits) captured (0.000000000 seconds) on interface eth0
- Ethernet II, Src: Intel E1000 (08:00:00:00:00:00), Dst: Intel E1000 (08:00:00:00:00:00)
- Hypertext Transfer Protocol, Status Line: 200 OK (text/plain)
- Content-Type: text/plain
- Content-Length: 5520
- Transfer-Encoding: chunked
- HTTP/1.0 200 OK (text/plain)

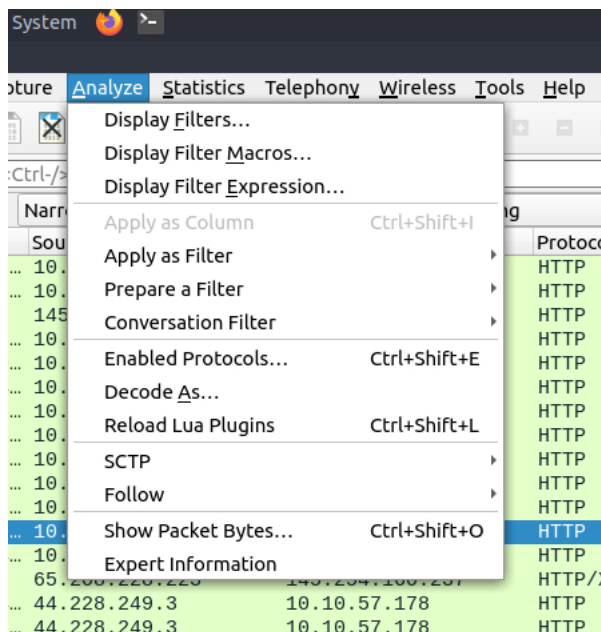
The packet bytes pane shows the raw data of the HTTP response, including the status line and the body content.

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



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

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



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	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”

The screenshot shows the Wireshark packet list with a right-click context menu open over the 'Hypertext Transfer Protocol' column. The menu options include 'Expand Subtrees', 'Collapse Subtrees', 'Expand All', 'Collapse All', 'Apply as Column', 'Apply as Filter', 'Prepare as Filter', and 'Conversation Filter'. The 'Apply as Filter' option is highlighted, and a submenu is visible showing 'Apply as Filter: http' as the selected filter query.

Answer: http

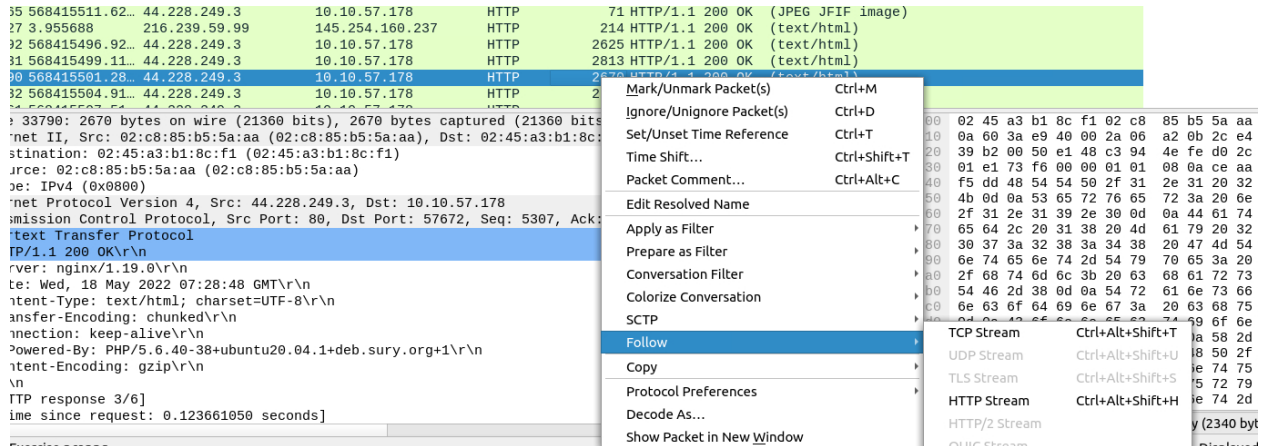
### 2. What is the number of displayed packets?

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

The screenshot shows the bottom status bar of Wireshark, which displays the total number of packets (58620), the number of packets currently displayed (1089), and the percentage of displayed packets (1.9%). It also shows the number of comments (1).

### 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"



Packet 33790: 2670 bytes on wire (21360 bits), 2670 bytes captured (21360 bits) on interface 0:08:00:27:00:00 (eth0), Src: 10.10.57.178, Dst: 10.10.57.178, Seq: 5307, Win: 0, Len: 0

Protocol: HTTP 1.1 200 OK

Host: 10.10.57.178

Content-Type: text/html; charset=UTF-8

Transfer-Encoding: chunked

Connection: keep-alive

Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1

Content-Encoding: gzip

HTTP response 3/6

Time since request: 0.123661050 seconds

Follow submenu:

- Follow
- Copy
- Protocol Preferences
- Decode As...
- Show Packet in New Window

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



Packet 33790: 2670 bytes on wire (21360 bits), 2670 bytes captured (21360 bits) on interface 0:08:00:27:00:00 (eth0), Src: 10.10.57.178, Dst: 10.10.57.178, Seq: 5307, Win: 0, Len: 0

Protocol: HTTP 1.1 200 OK

Host: 10.10.57.178

Content-Type: text/html; charset=UTF-8

Transfer-Encoding: chunked

Connection: keep-alive

Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1

Content-Encoding: gzip

HTTP response 3/6

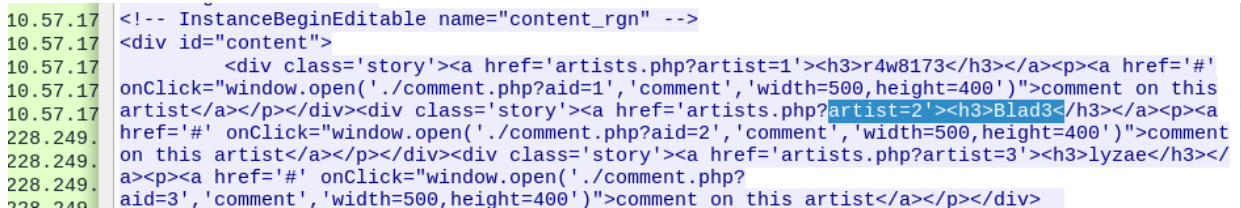
Time since request: 0.123661050 seconds

Follow submenu:

- Follow
- Copy
- Protocol Preferences
- Decode As...
- Show Packet in New Window

Answer: 3

### 4. What is the name of the 2<sup>nd</sup> artist?



Packet 33790: 2670 bytes on wire (21360 bits), 2670 bytes captured (21360 bits) on interface 0:08:00:27:00:00 (eth0), Src: 10.10.57.178, Dst: 10.10.57.178, Seq: 5307, Win: 0, Len: 0

Protocol: HTTP 1.1 200 OK

Host: 10.10.57.178

Content-Type: text/html; charset=UTF-8

Transfer-Encoding: chunked

Connection: keep-alive

Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1

Content-Encoding: gzip

HTTP response 3/6

Time since request: 0.123661050 seconds

Follow submenu:

- Follow
- Copy
- Protocol Preferences
- Decode As...
- Show Packet in New Window

Answer: Blad3