Wireshark: The Basics

Learn the basics of Wireshark and how to analyse protocols and PCAPs.

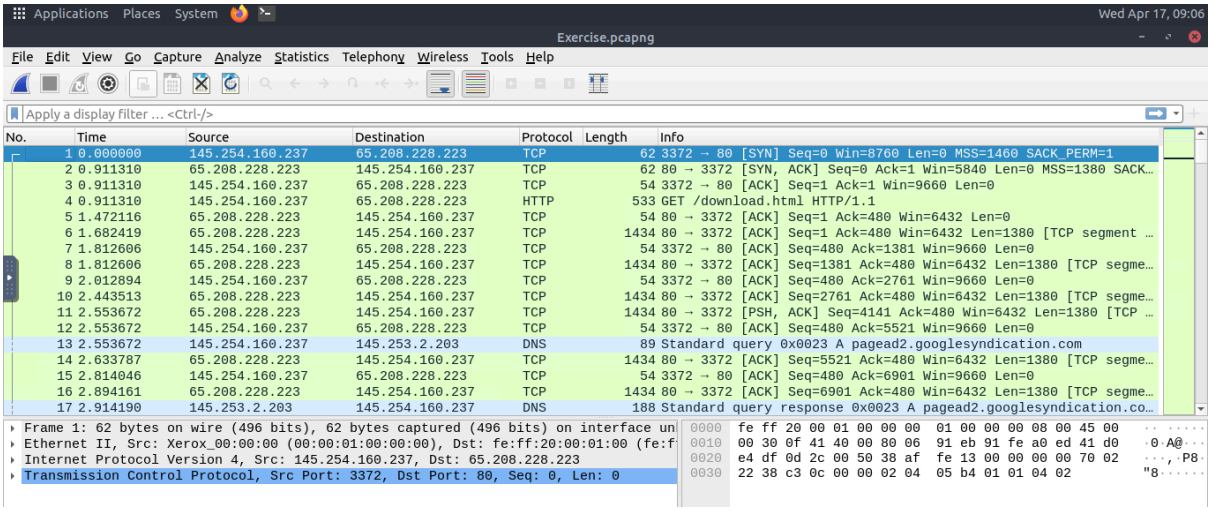
Task 1 Introduction

Question	Answer
Which file is used to simulate the screenshots?	http1.pcapng
Which file is used to answer the questions?	Exercise.pcapng

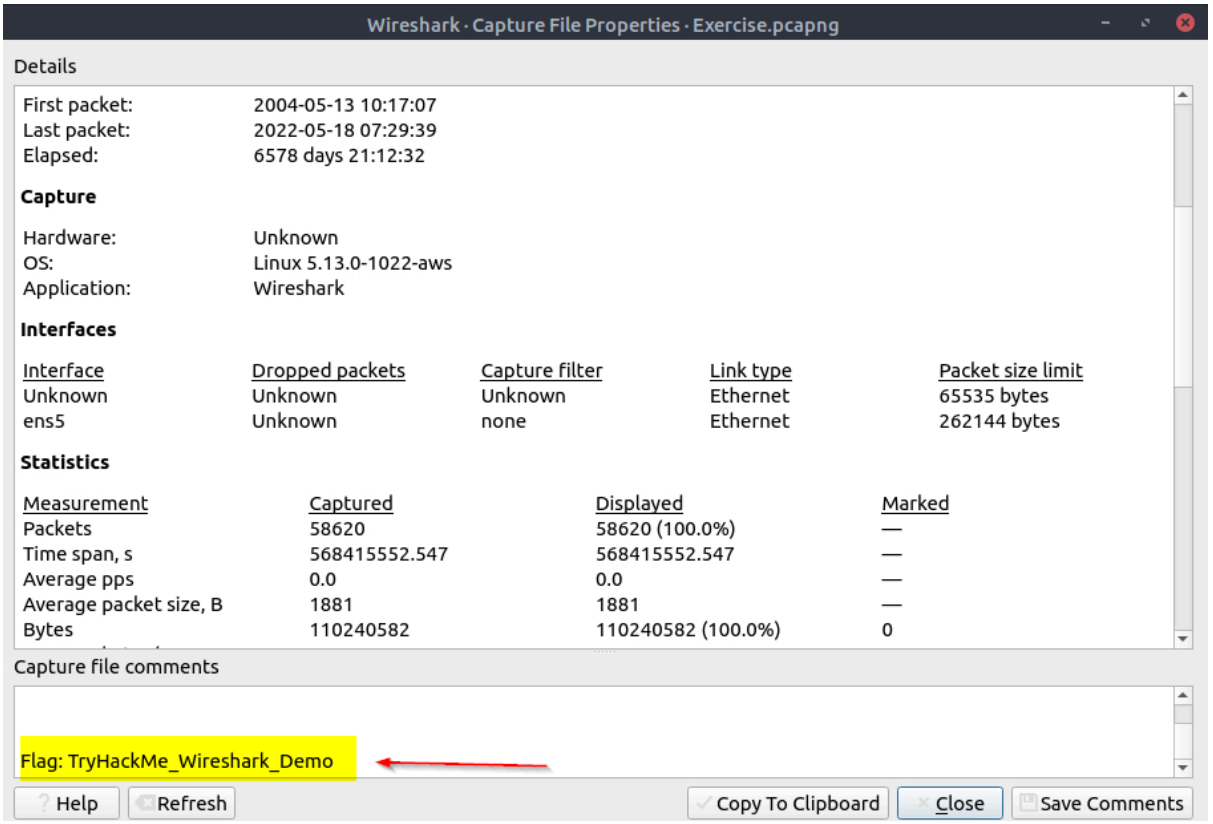
Task 2 Tool Overview

Read the "capture file comments". What is the flag?
Answer: **TryHackMe_Wireshark_Demo**

➔ I loaded the Exercise.pcapng file

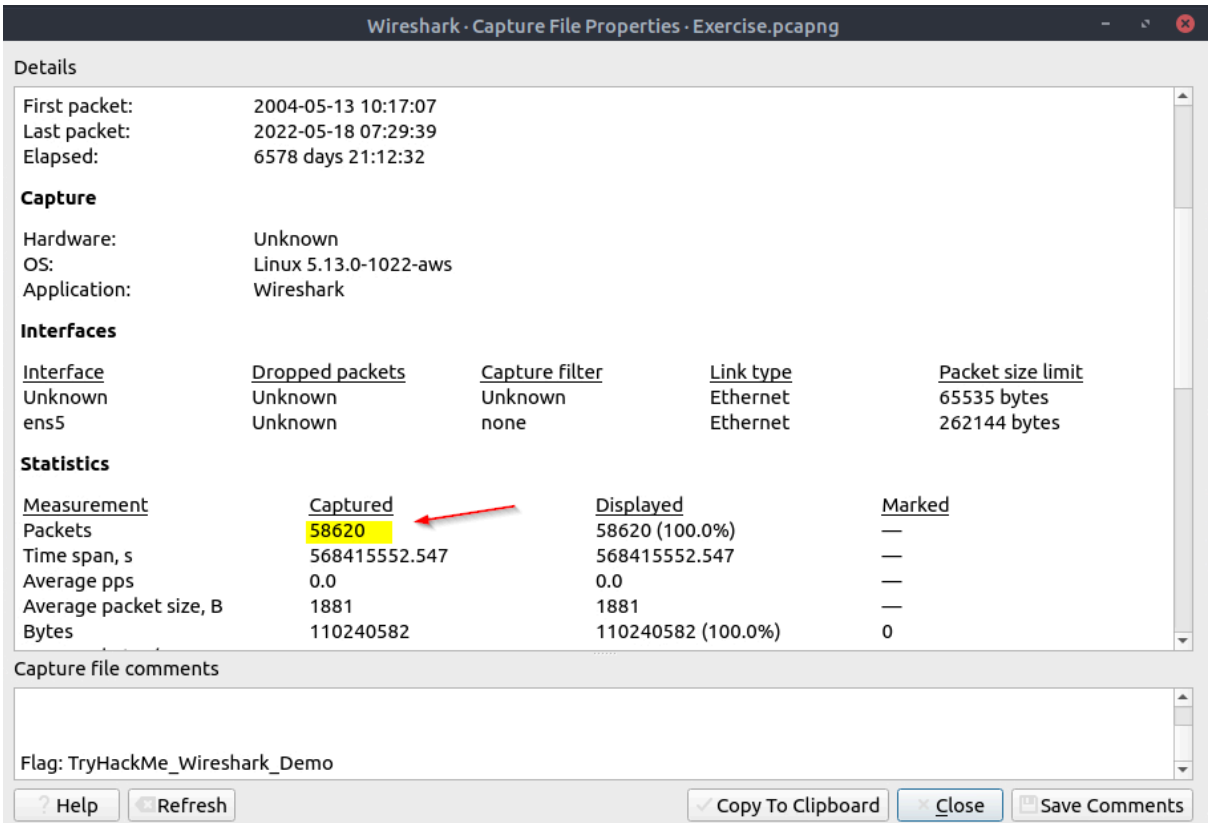


➔ I clicked on statistics tab then to capture file properties



What is the total number of packets?

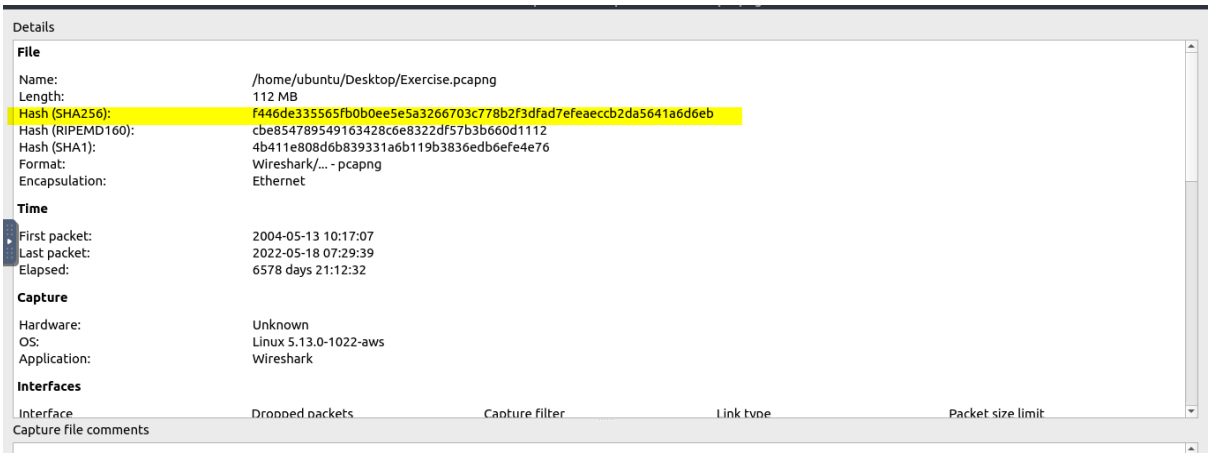
➔ Still in the capture file properties page



What is the SHA256 hash value of the capture file?

➔ Still in the capture file properties page

Answer:
f446de335565fb0b0ee5e5a3266703c778b2f3dfad7efeaeccb2da5641a6d6eb



Task 3 Packet Dissection

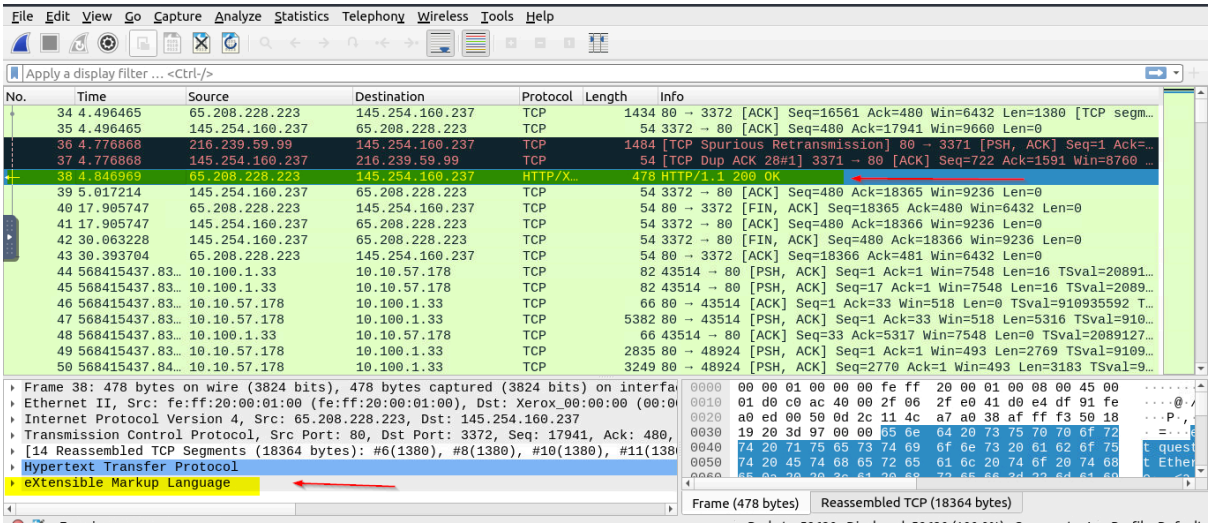
View packet number 38. Which markup language is used under the HTTP protocol?

➔ I pressed ctrl+g, then entered 38

➔ I clicked on packet number 38

➔ In the packet details pane, under the HTTP protocol

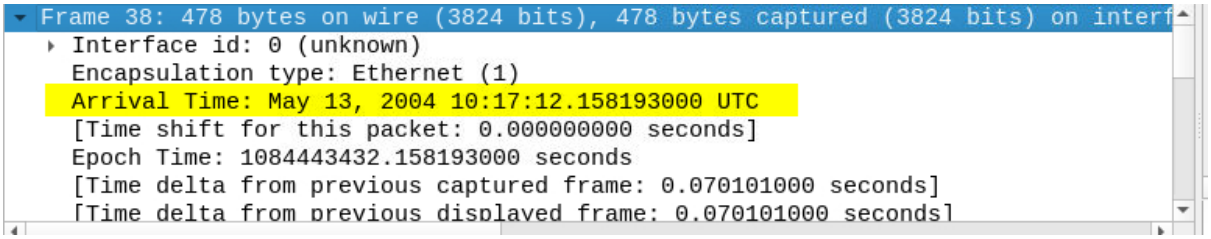
Answer: extensible markup language



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

Answer: **05/13/2004**

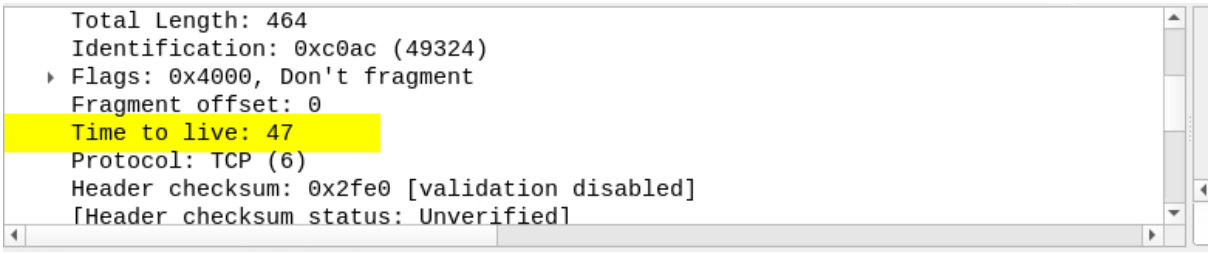
➔ Still on packet 38, I opened up the frame section.



What is the TTL value?

Answer: **47**

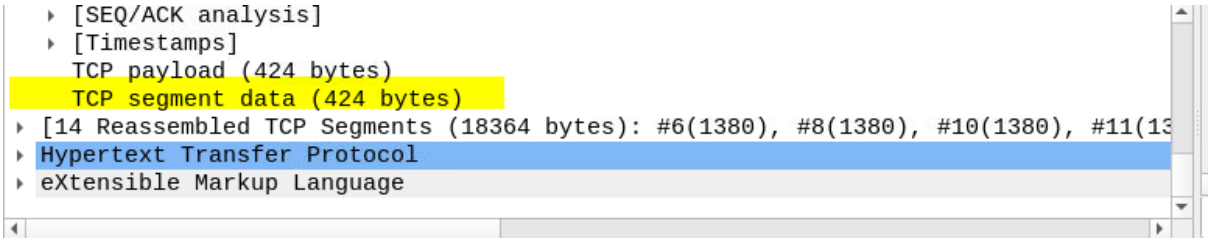
➔ I opened up the IP protocol section



What is the TCP payload size?

➔ I opened the TCP section

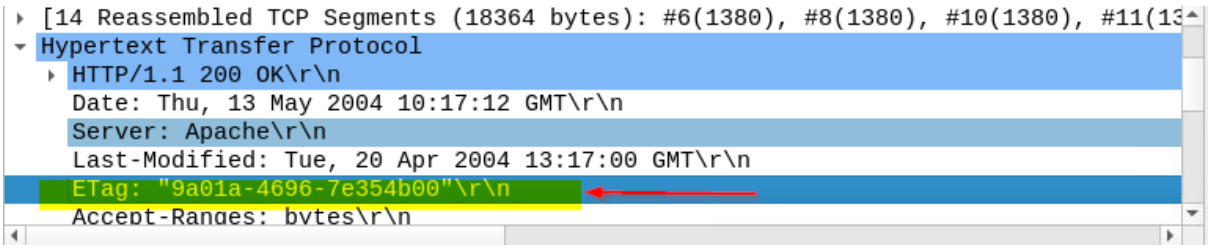
Answer: **424**



What is the e-tag value?

➔ i opened the hypertext transfer protocol

Answer: **9a01a-4696-7e354b00**

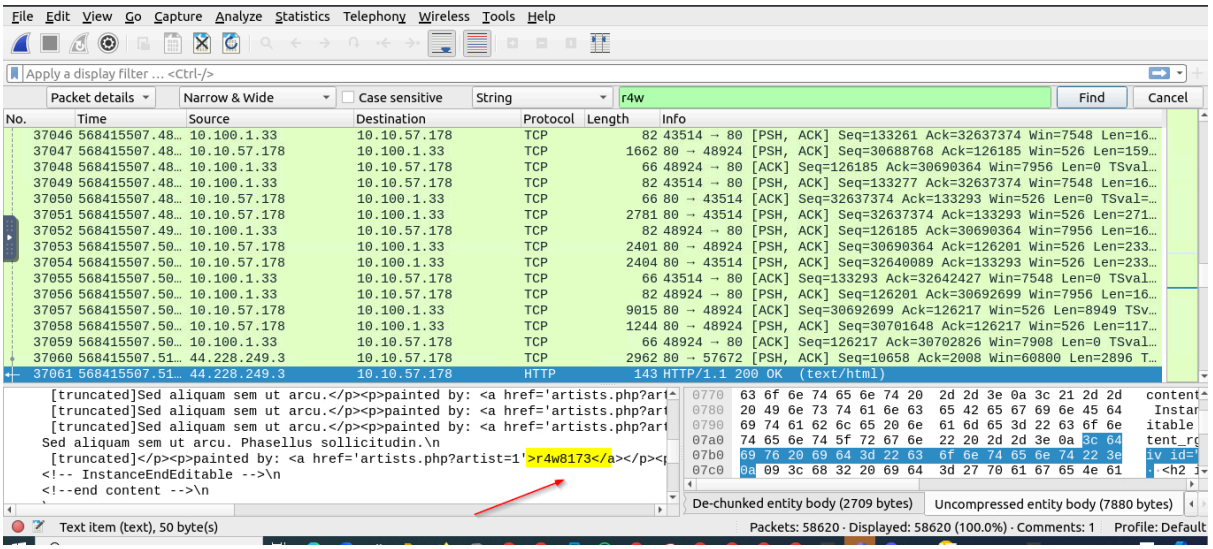


Task 4 Packet Navigation

Search the "r4w" string in packet details. What is the name of artist 1?

➔ I clicked on “edit” then to find packet, and inputted “r4w” in the search

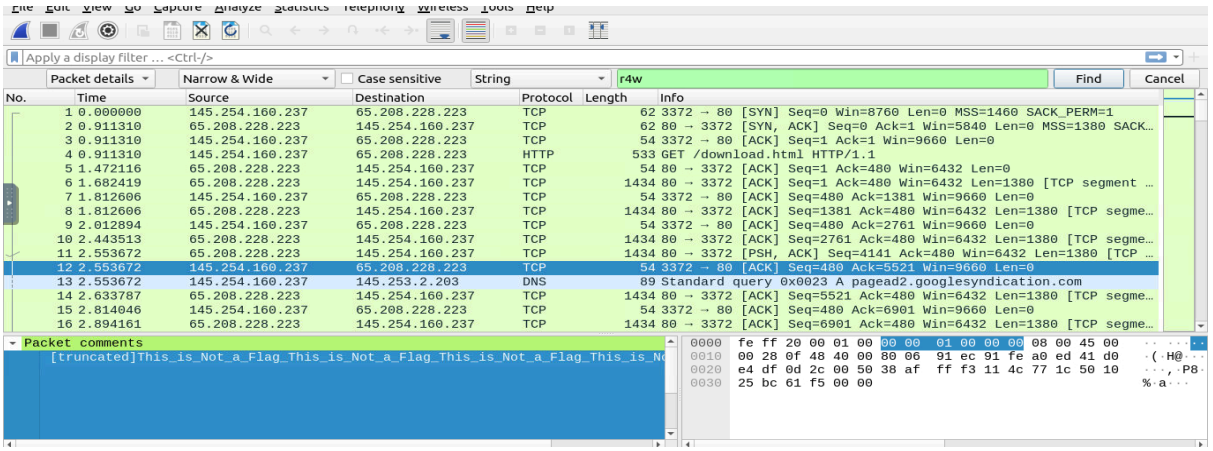
Answer: r4w8173



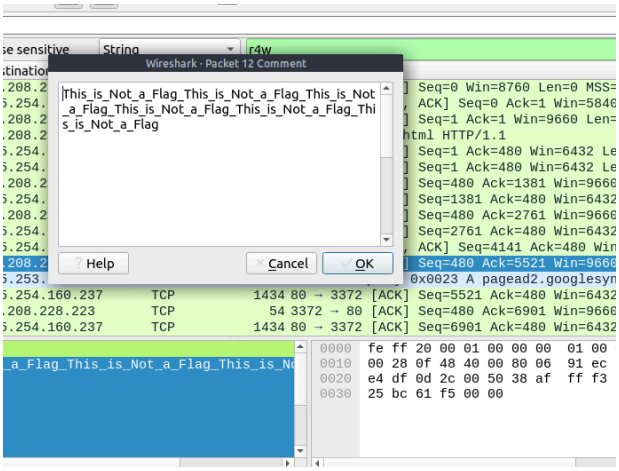
Go to packet 12 and read the comments. What is the answer?

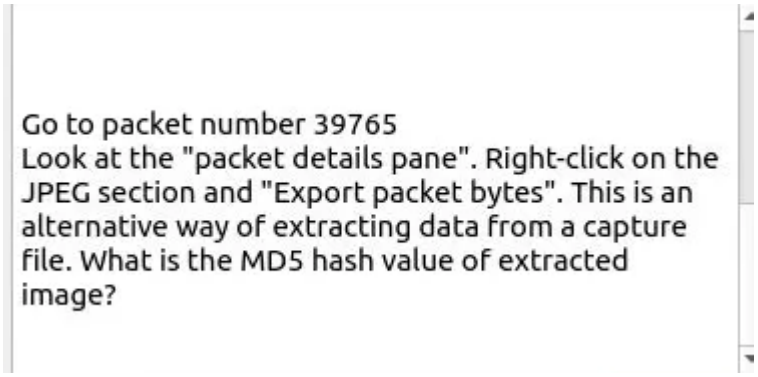
Answer: 911cd574a42865a956ccde2d04495ebf

➔ I clicked on packet 12 and found an incomplete comment in the details pane



➔ To read the comment, i clicked on edit tab, then packet comment

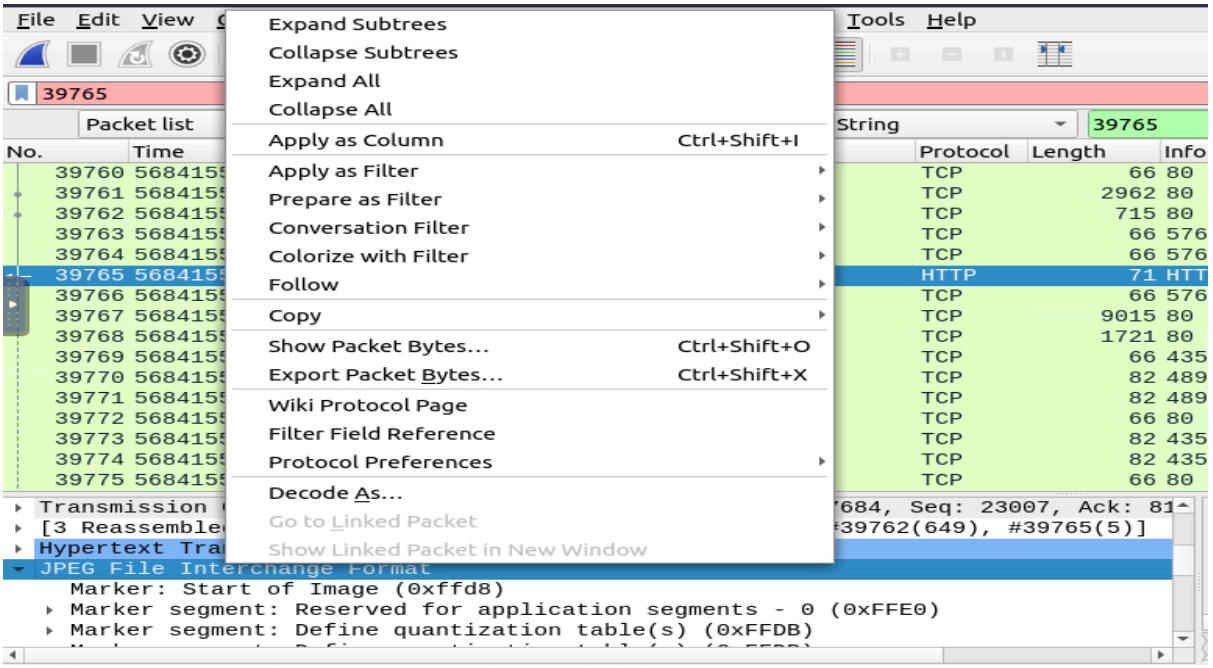




➔ Comment said i should go to packet 39765

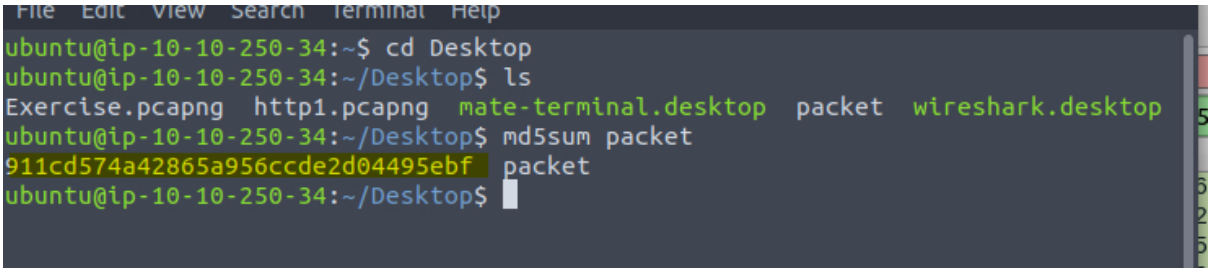
➔ On the packet details pane, I right-clicked on the JPEG section then to export packet bytes.

➔ I saved the JPEG file as “packet” in the Desktop directory



➔ I opened a terminal and extracted the MD5 hash value of the image.

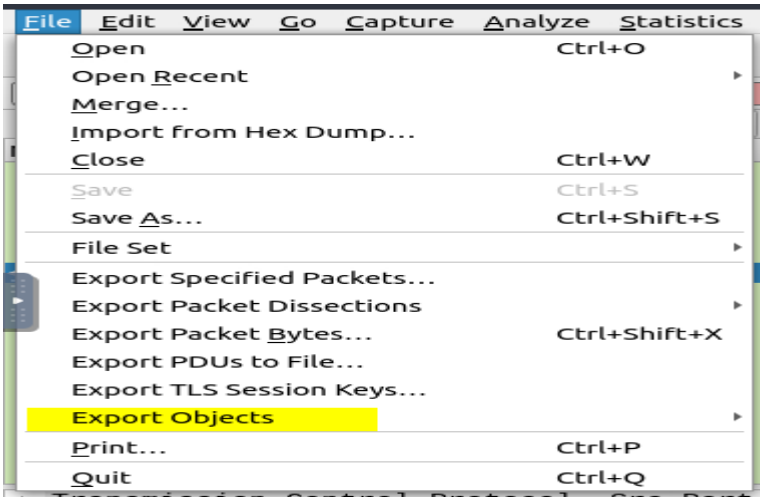
Command: md5sum packet

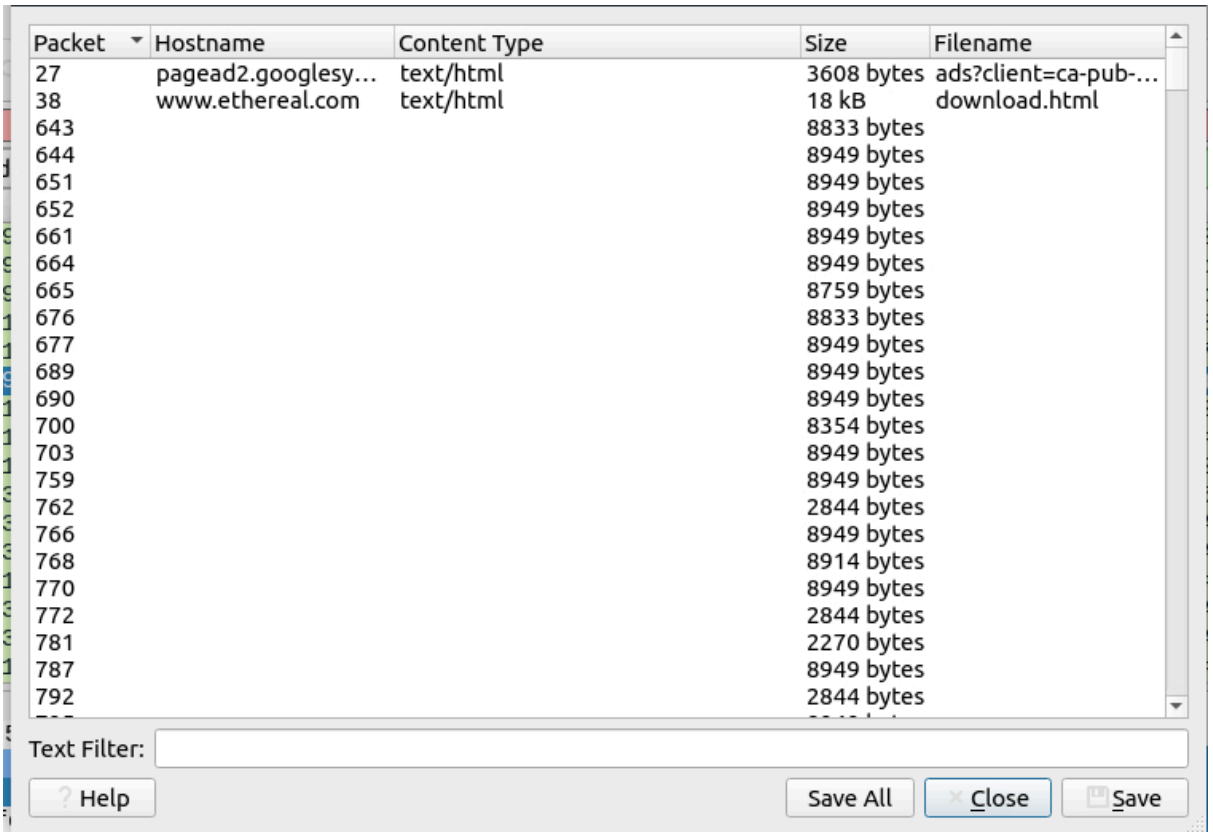


There is a ".txt" file inside the capture file. Find the file and read it; what is the alien's name?

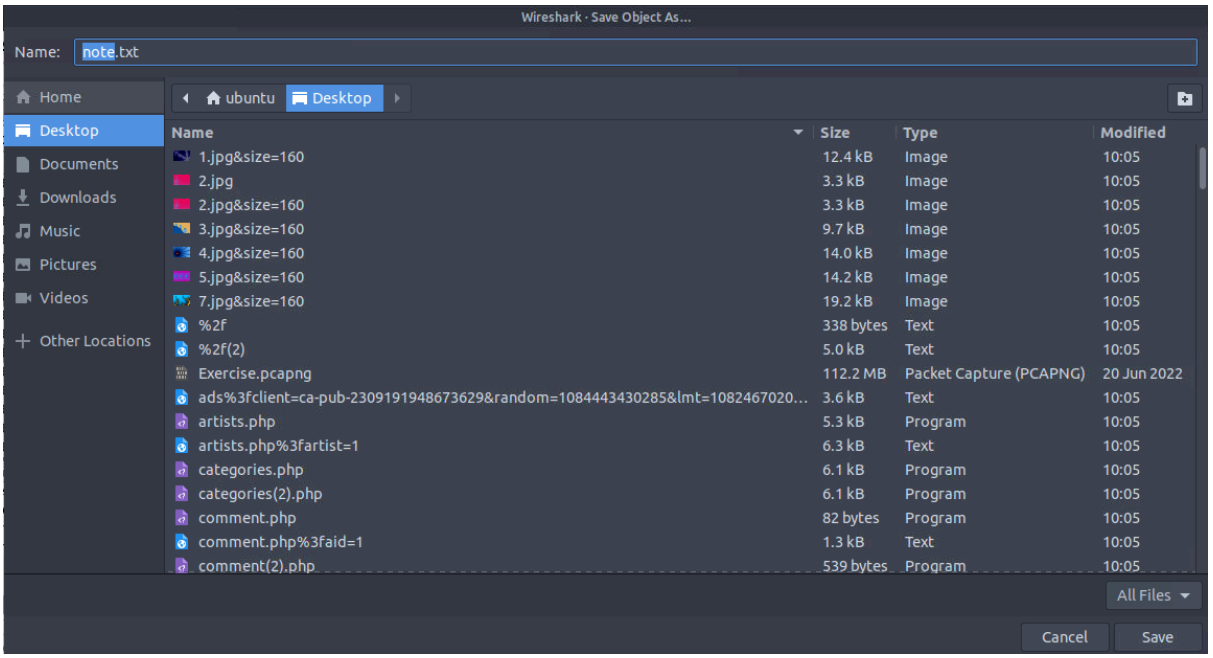
Answer: PACKETMASTER

➔ I clicked on File menu then selected Export Objects and then HTTP





➔ Then saved the note.txt file



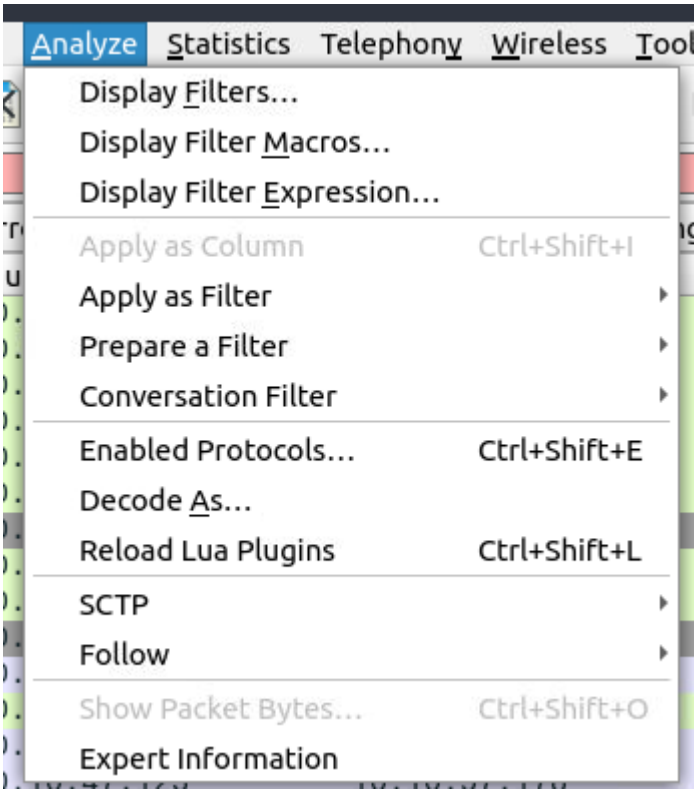
➔ I tried reading the content of the note.txt file

Command: cat note.txt

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

➔ I clicked on the Analyze Menu then select Expert Information

Answer: 1636



erity	Summary	Group	Protocol	Count
rror	Malformed Packet (Exception occurred)	Malformed	HTTP	13
rror	Malformed Packet (Exception occurred)	Malformed	JFIF (JPEG) ...	2
Varning	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
Chat	Connection establish request (SYN): server port 80	Sequence	TCP	12
Comment	Packet comments listed below.	Comment	Frame	1

Task 5 Packet Filtering

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?

Answer: **http**

- ➔ I Pressed ctrl+g and entered packet number 4
- ➔ I right clicked on the Hypertext Transfer Protocol and applied filter

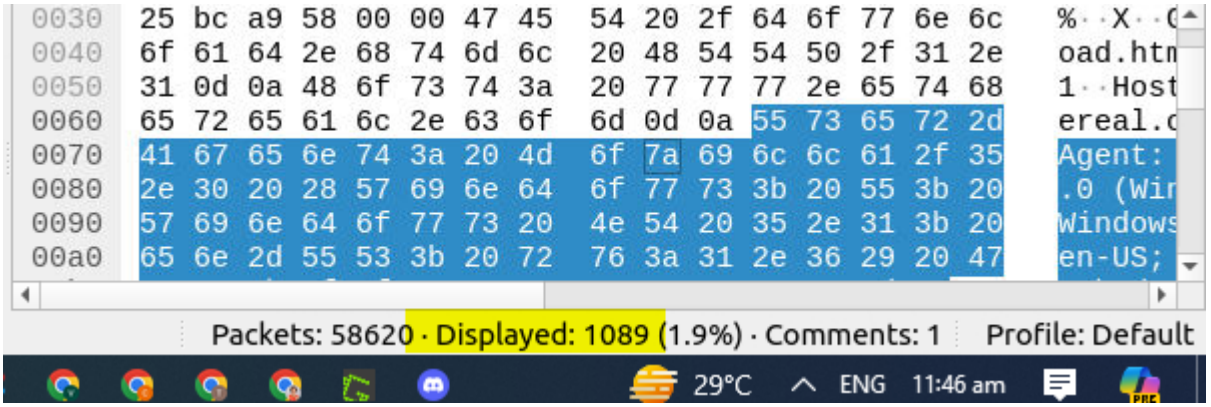
http

No.	Time	Source	Destination	Protocol	Length	Info
4	0.911310	145.254.160.237	65.208.228.223	HTTP	533	GET /download.html HTTP/1.1
18	2.984291	145.254.160.237	216.239.59.99	HTTP	775	GET /pagead/ads?client=ca-pub-2309191948673629&random=1084443…
27	3.955688	216.239.59.99	145.254.160.237	HTTP	214	HTTP/1.1 200 OK (text/html)
38	4.846969	65.208.228.223	145.254.160.237	HTTP/X…	478	HTTP/1.1 200 OK
643	568415438.43…	10.10.57.178	10.100.1.33	TCP	9015	80 → 48924 [PSH, ACK] Seq=244755 Ack=2749 Win=493 Len=8949 TS…
665	568415438.44…	10.10.57.178	10.100.1.33	TCP	9015	80 → 48924 [ACK] Seq=393627 Ack=2749 Win=493 Len=8949 TSval=9…
676	568415438.44…	10.10.57.178	10.100.1.33	TCP	9015	80 → 43514 [PSH, ACK] Seq=263440 Ack=3009 Win=518 Len=8949 TS…
700	568415438.44…	10.10.57.178	10.100.1.33	TCP	9015	80 → 43514 [ACK] Seq=394414 Ack=3073 Win=518 Len=8949 TSval=9…
768	568415438.63…	10.10.57.178	10.100.1.33	TCP	9015	80 → 48924 [ACK] Seq=505808 Ack=3165 Win=493 Len=8949 TSval=9…
797	568415438.64…	10.10.57.178	10.100.1.33	TCP	9015	80 → 43514 [ACK] Seq=524482 Ack=3329 Win=518 Len=8949 TSval=9…
821	568415438.80…	10.10.57.178	10.100.1.33	TCP	6747	80 → 43514 [PSH, ACK] Seq=610134 Ack=3361 Win=518 Len=6681 TS…
870	568415438.95…	10.10.57.178	10.100.1.33	TCP	9015	80 → 48924 [ACK] Seq=723434 Ack=3293 Win=493 Len=8949 TSval=9…
871	568415438.95…	10.10.57.178	10.100.1.33	TCP	9015	80 → 48924 [ACK] Seq=732383 Ack=3293 Win=493 Len=8949 TSval=9…
905	568415438.96…	10.10.57.178	10.100.1.33	TCP	9015	80 → 43514 [ACK] Seq=752599 Ack=3393 Win=518 Len=8949 TSval=9…
950	568415439.10…	10.10.57.178	10.100.1.33	TCP	9015	80 → 48924 [ACK] Seq=869863 Ack=3465 Win=493 Len=8949 TSval=9…
959	568415439.10…	10.10.57.178	10.100.1.33	TCP	9015	80 → 48924 [ACK] Seq=935350 Ack=3465 Win=493 Len=8949 TSval=9…
971	568415439.11…	10.10.57.178	10.100.1.33	TCP	9015	80 → 48924 [ACK] Seq=1009786 Ack=3465 Win=493 Len=8949 TSval=…

What is the number of displayed packets?

Answer: **1089**

- ➔ The answer is found at bottom right-side of the status bar



Go to packet number 33790 and follow the stream. What is the total number of artists?

Answer: 3

➔ I searched for the packet number 33790, right-clicked on the http, then follow and finally to http stream

```
        <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?
```

What is the name of the second artist?

Answer: Blad3

```
        <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?
```

END!!!