

# Wireshark: The Basics

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

## Task 1 Introduction

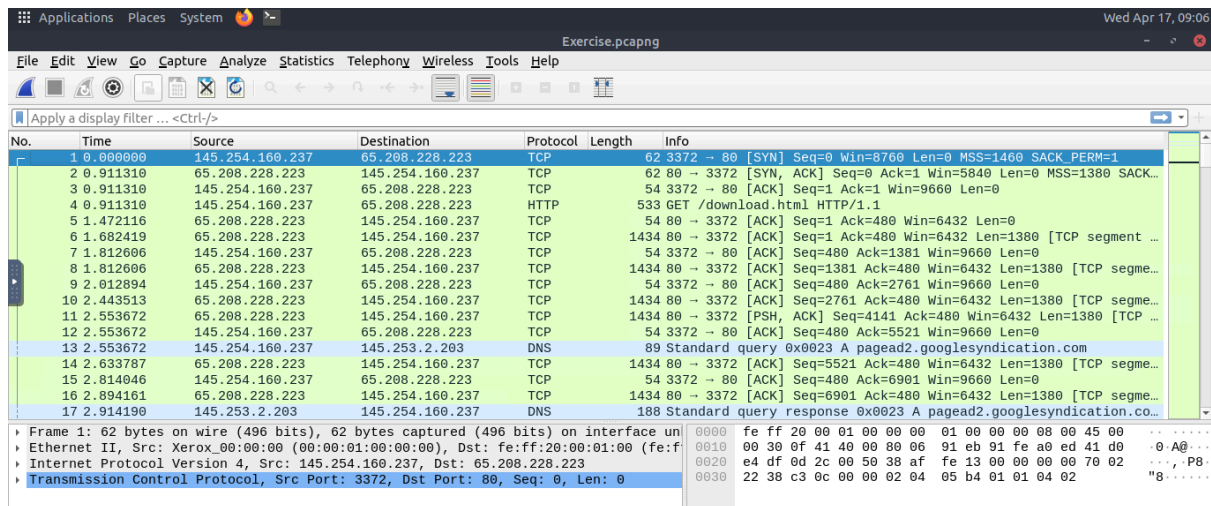
Question	Answer
Which file is used to simulate the screenshots?	http1.pcapng
Which file is used to answer the questions?	Exercise.pcapng

## 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

Wireshark · Capture File Properties · Exercise.pcapng

Details

First packet: 2004-05-13 10:17:07  
Last packet: 2022-05-18 07:29:39  
Elapsed: 6578 days 21:12:32

**Capture**

Hardware: Unknown  
OS: Linux 5.13.0-1022-aws  
Application: Wireshark

**Interfaces**

Interface	Dropped packets	Capture filter	Link type	Packet size limit
Unknown	Unknown	Unknown	Ethernet	65535 bytes
ens5	Unknown	none	Ethernet	262144 bytes

**Statistics**

Measurement	Captured	Displayed	Marked
Packets	58620	58620 (100.0%)	—
Time span, s	568415552.547	568415552.547	—
Average pps	0.0	0.0	—
Average packet size, B	1881	1881	—
Bytes	110240582	110240582 (100.0%)	0

Capture file comments

Flag: TryHackMe\_Wireshark\_Demo

? Help Refresh Copy To Clipboard Close Save Comments

What is the total number of packets?

→ Still in the capture file properties page

Wireshark · Capture File Properties · Exercise.pcapng

Details

First packet: 2004-05-13 10:17:07  
Last packet: 2022-05-18 07:29:39  
Elapsed: 6578 days 21:12:32

**Capture**

Hardware: Unknown  
OS: Linux 5.13.0-1022-aws  
Application: Wireshark

**Interfaces**

Interface	Dropped packets	Capture filter	Link type	Packet size limit
Unknown	Unknown	Unknown	Ethernet	65535 bytes
ens5	Unknown	none	Ethernet	262144 bytes

**Statistics**

Measurement	Captured	Displayed	Marked
Packets	58620	58620 (100.0%)	—
Time span, s	568415552.547	568415552.547	—
Average pps	0.0	0.0	—
Average packet size, B	1881	1881	—
Bytes	110240582	110240582 (100.0%)	0

Capture file comments

Flag: TryHackMe\_Wireshark\_Demo

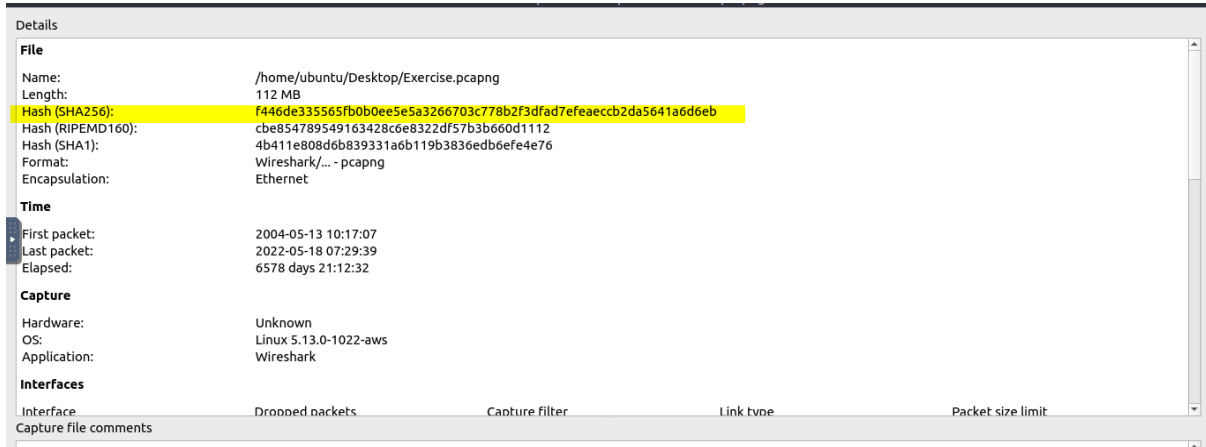
? Help Refresh Copy To Clipboard Close Save Comments

What is the SHA256 hash value of the capture file?

→ Still in the capture file properties page

Answer:

**f446de335565fb0b0ee5e5a3266703c778b2f3dfad7efeaeccb2da5641a6d6eb**



## Task 3 Packet Dissection

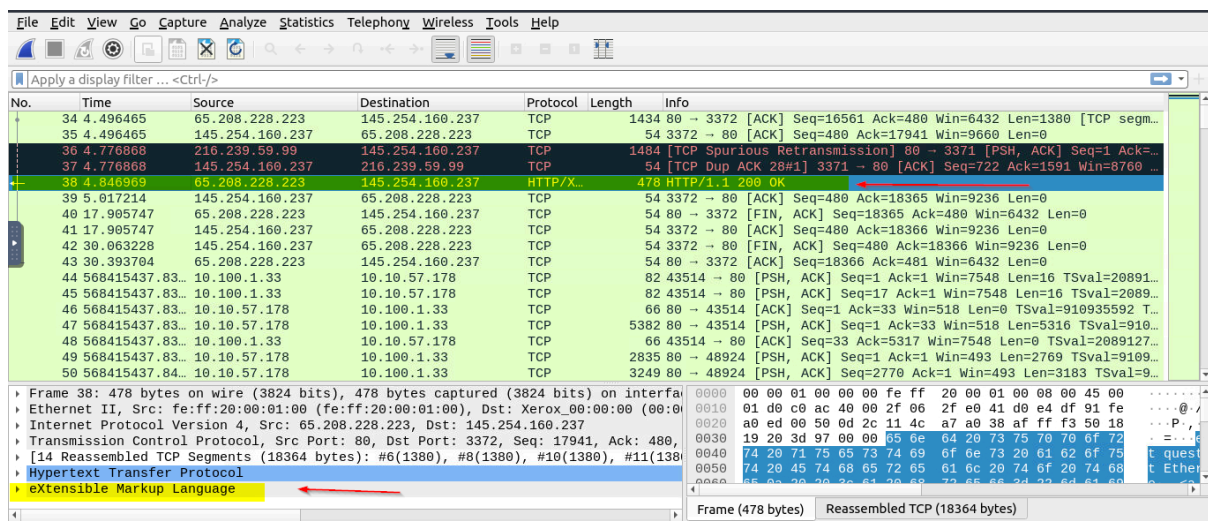
View packet number 38. Which markup language is used under the HTTP protocol?

→ I pressed ctrl+g, then entered 38

→ I clicked on packet number 38

→ In the packet details pane, under the HTTP protocol

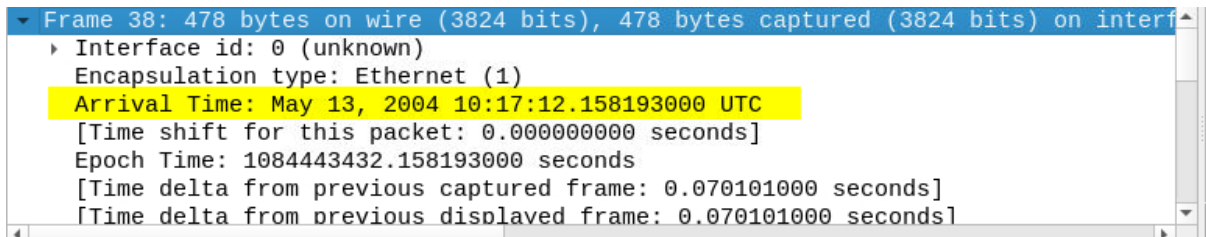
Answer: **extensible markup language**



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

**Answer: 05/13/2004**

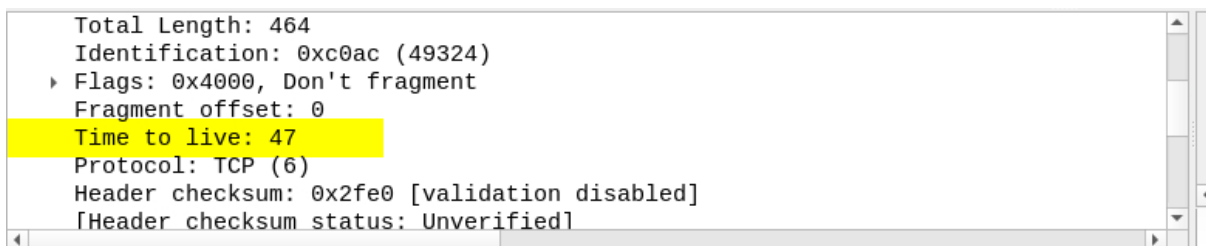
→ Still on packet 38, I opened up the frame section.



What is the TTL value?

**Answer: 47**

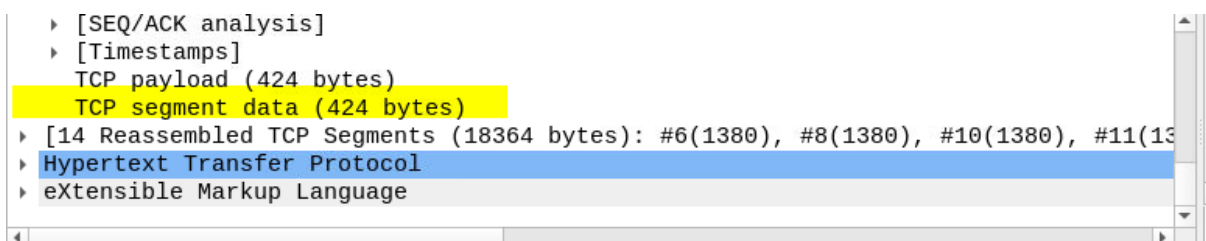
→ I opened up the IP protocol section



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**

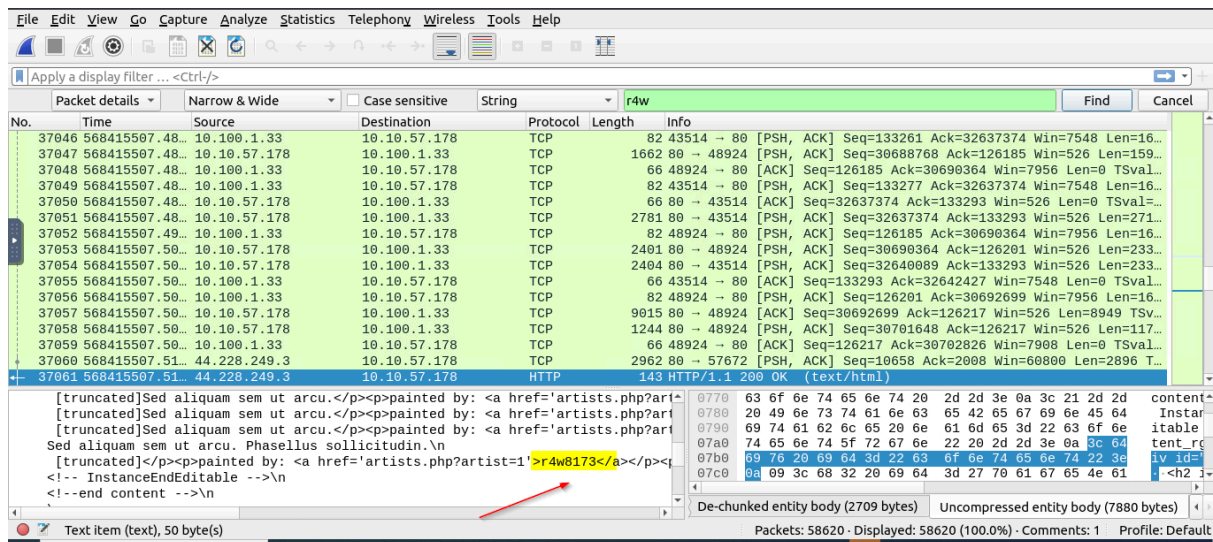
```
[14 Reassembled TCP Segments (18364 bytes): #6(1380), #8(1380), #10(1380), #11(1380)
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  Date: Thu, 13 May 2004 10:17:12 GMT\r\n
  Server: Apache\r\n
  Last-Modified: Tue, 20 Apr 2004 13:17:00 GMT\r\n
  ETag: "9a01a-4696-7e354b00"\r\n
  Accept-Ranges: bytes\r\n
```

## 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**



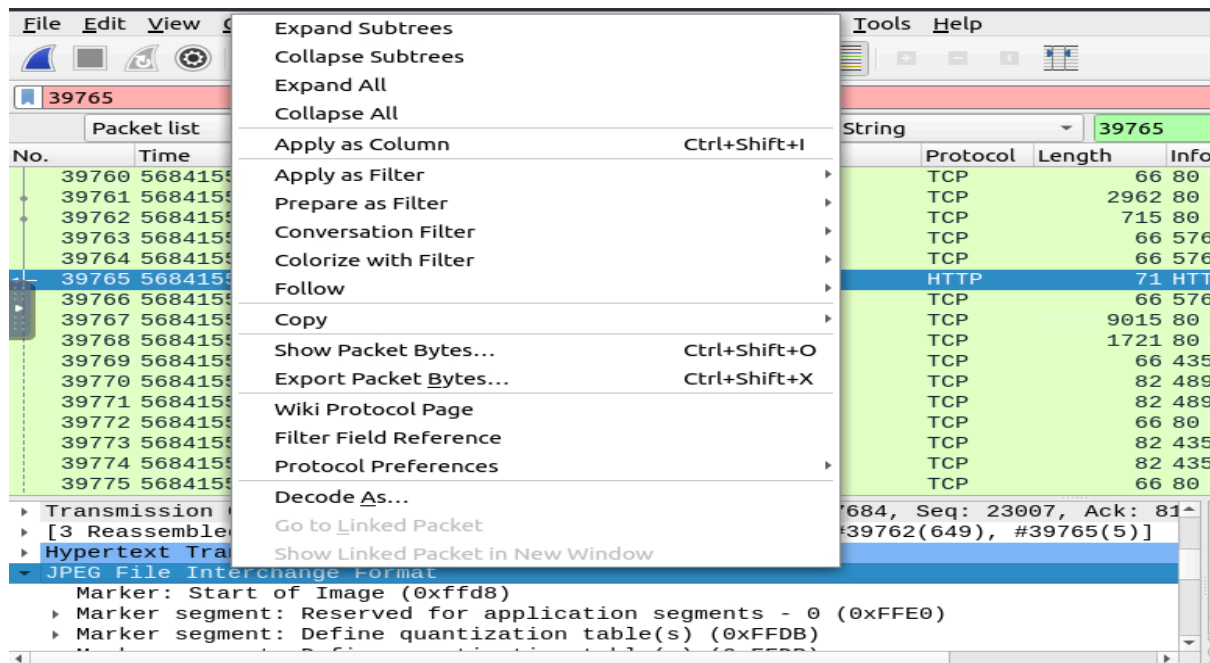
Go to packet 12 and read the comments. What is the answer?

**Answer: 911cd574a42865a956ccde2d04495ebf**

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

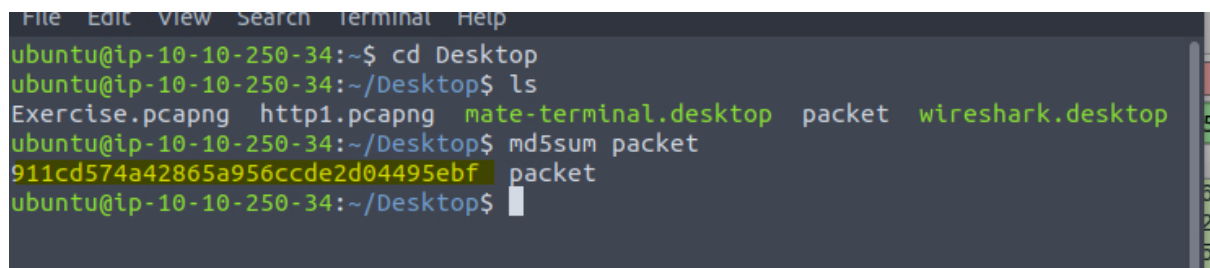






→ I opened a terminal and extracted the MD5 hash value of the image.

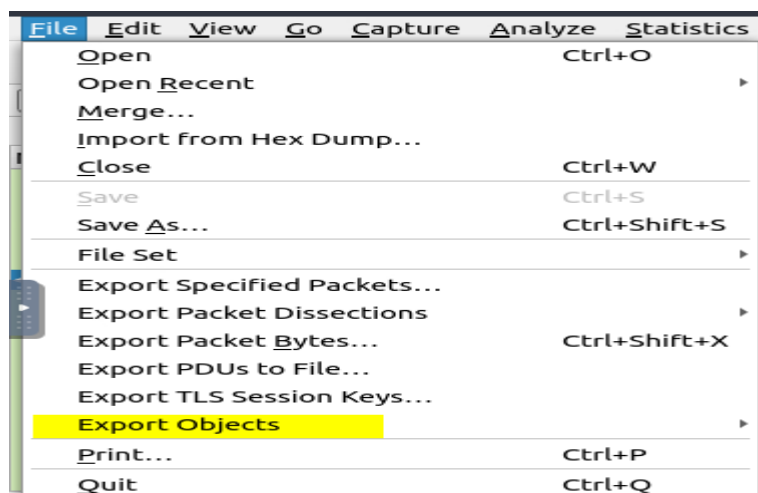
**Command: md5sum packet**



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

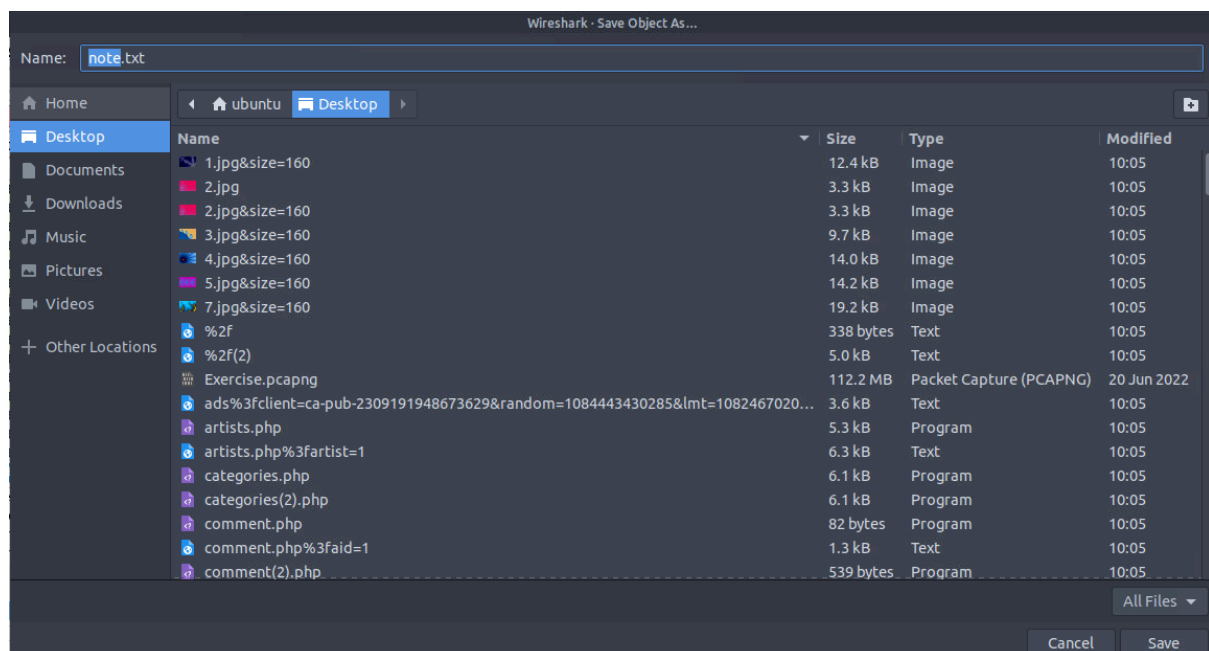


Packet	Hostname	Content Type	Size	Filename
27	pagead2.googlesy...	text/html	3608 bytes	ads?client=ca-pub-...
38	www.ethereal.com	text/html	18 kB	download.html
643			8833 bytes	
644			8949 bytes	
651			8949 bytes	
652			8949 bytes	
661			8949 bytes	
664			8949 bytes	
665			8759 bytes	
676			8833 bytes	
677			8949 bytes	
689			8949 bytes	
690			8949 bytes	
700			8354 bytes	
703			8949 bytes	
759			8949 bytes	
762			2844 bytes	
766			8949 bytes	
768			8914 bytes	
770			8949 bytes	
772			2844 bytes	
781			2270 bytes	
787			8949 bytes	
792			2844 bytes	

Text Filter:

? Help Save All Close Save

→ Then saved the note.txt file



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

Command: **cat note.txt**

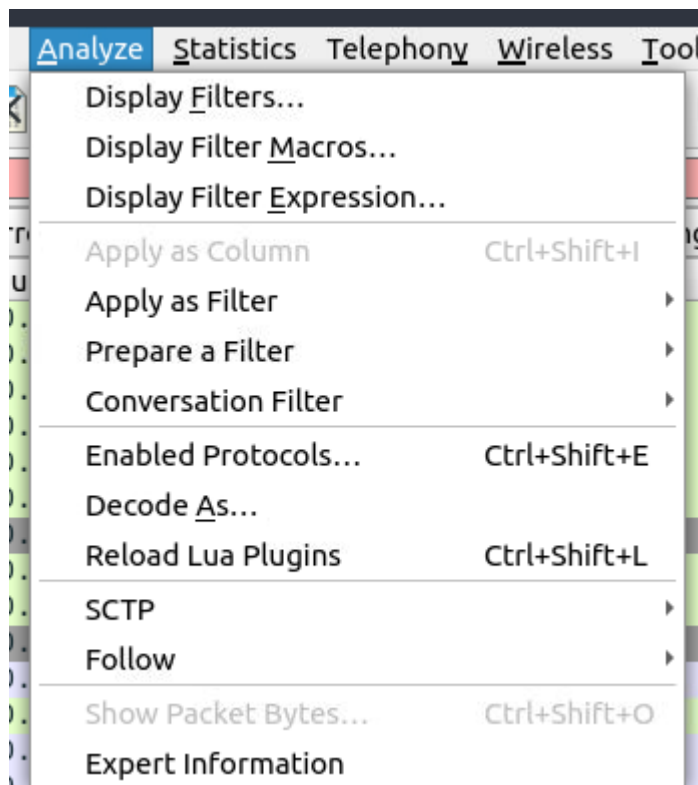




Look at the expert info section. What is the number of warnings?

→ I clicked on the Analyze Menu then select Expert Information

**Answer: 1636**



Priority	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
That	Connection finish (FIN)	Sequence	TCP	12
That	GET /download.html HTTP/1.1\r\n	Sequence	HTTP	40
That	Connection establish acknowledge (SYN+ACK): server port 80	Sequence	TCP	12
That	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

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

0030	25	bc	a9	58	00	00	47	45	54	20	2f	64	6f	77	6e	6c	% · X · C
0040	6f	61	64	2e	68	74	6d	6c	20	48	54	54	50	2f	31	2e	oad.htm
0050	31	0d	0a	48	6f	73	74	3a	20	77	77	77	2e	65	74	68	1 · Host
0060	65	72	65	61	6c	2e	63	6f	6d	0d	0a	55	73	65	72	2d	ereal.c
0070	41	67	65	6e	74	3a	20	4d	6f	7a	69	6c	6c	61	2f	35	Agent:
0080	2e	30	20	28	57	69	6e	64	6f	77	73	3b	20	55	3b	20	.0 (Win
0090	57	69	6e	64	6f	77	73	20	4e	54	20	35	2e	31	3b	20	Windows
00a0	65	6e	2d	55	53	3b	20	72	76	3a	31	2e	36	29	20	47	en-US;

Packets: 58620 · Displayed: 1089 (1.9%) · Comments: 1 · Profile: Default

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!!!**