WIRESHARK

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)

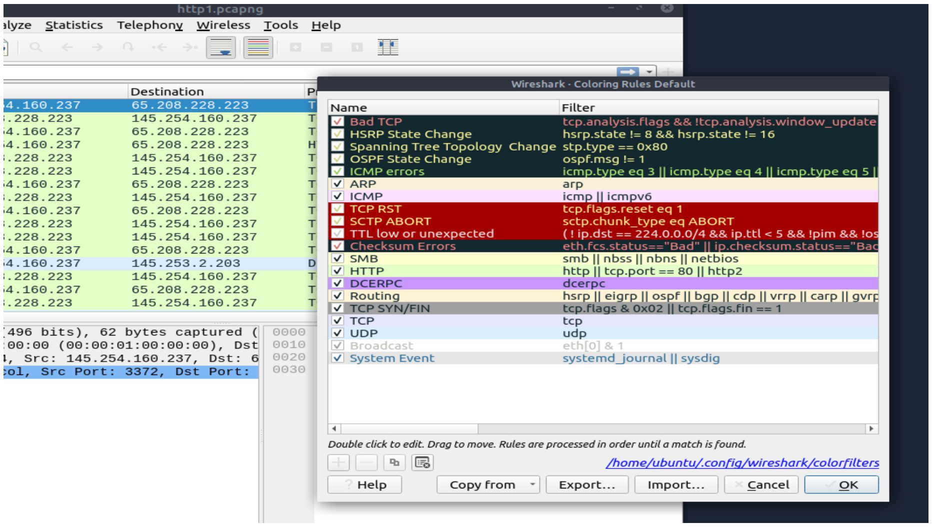
- is the standard file format used by Wireshark and other network analyzers to store data packets captured from a network
- To be able to analyze packages, you must upload a pcap (Packet Capture) file to Wireshark.

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).


http1.pcapng
alyze Statistics Telephony Wireless Tools Help
Wireshark · Coloring Rules Default
Help
Copy from
Export…
Import…
Cancel
OK

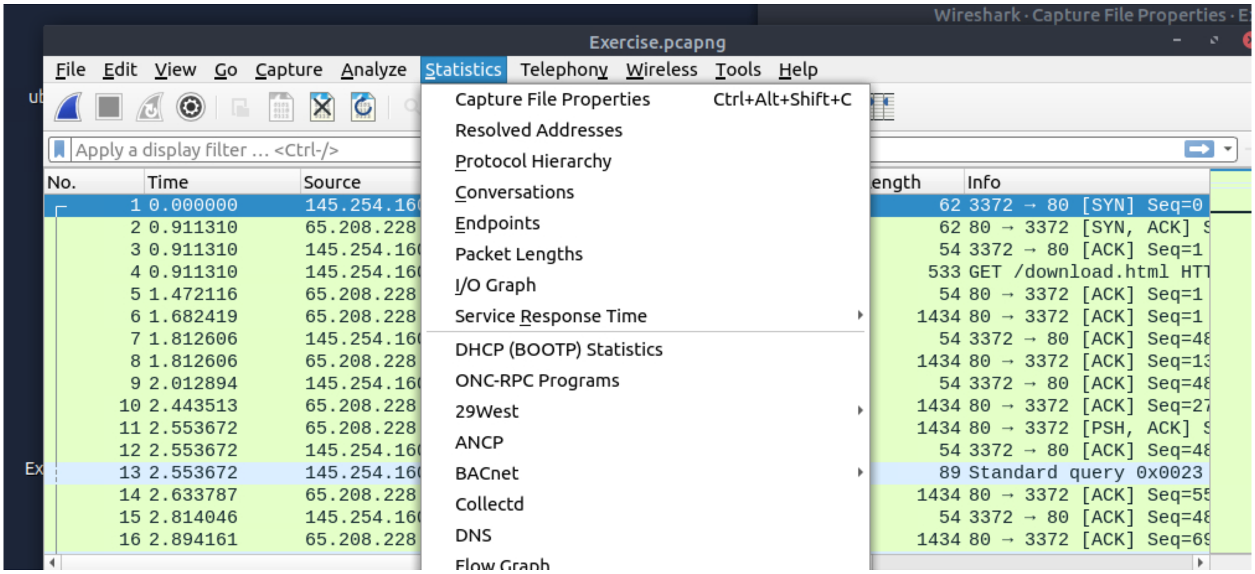
```
                 Destination          P
4.160.237       65.208.228.223       T
.228.223        145.254.160.237      T
4.160.237       65.208.228.223       T
4.160.237       65.208.228.223       H
.228.223        145.254.160.237      T
.228.223        145.254.160.237      T
4.160.237       65.208.228.223       T
.228.223        145.254.160.237      T
4.160.237       65.208.228.223       T
.228.223        145.254.160.237      T
.228.223        145.254.160.237      T
4.160.237       65.208.228.223       T
4.160.237       145.253.2.203        D
.228.223        145.254.160.237      T
4.160.237       65.208.228.223       T
.228.223        145.254.160.237      T

(496 bits), 62 bytes captured (      0000
00:00 (00:00:01:00:00:00), Dst       0010
, Src: 145.254.160.237, Dst: 6       0020
col, Src Port: 3372, Dst Port:       0030
```

Name	Filter
☑ Bad TCP	tcp.analysis.flags && !tcp.analysis.window_update
☑ HSRP State Change	hsrp.state != 8 && hsrp.state != 16
☑ Spanning Tree Topology Change	stp.type == 0x80
☑ OSPF State Change	ospf.msg != 1
☑ ICMP errors	icmp.type eq 3 || icmp.type eq 4 || icmp.type eq 5 ||
☑ ARP	arp
☑ ICMP	icmp || icmpv6
☑ TCP RST	tcp.flags.reset eq 1
☑ SCTP ABORT	sctp.chunk_type eq ABORT
☑ TTL low or unexpected	(! ip.dst == 224.0.0.0/4 && ip.ttl < 5 && !pim && !os
☑ Checksum Errors	eth.fcs.status=="Bad" || ip.checksum.status=="Bac
☑ SMB	smb || nbss || nbns || netbios
☑ HTTP	http || tcp.port == 80 || http2
☑ DCERPC	dcerpc
☑ Routing	hsrp || eigrp || ospf || bgp || cdp || vrrp || carp || gvrp
☑ TCP SYN/FIN	tcp.flags & 0x02 || tcp.flags.fin == 1
☑ TCP	tcp
☑ UDP	udp
☑ Broadcast	eth[0] & 1
☑ System Event	systemd_journal || sysdig

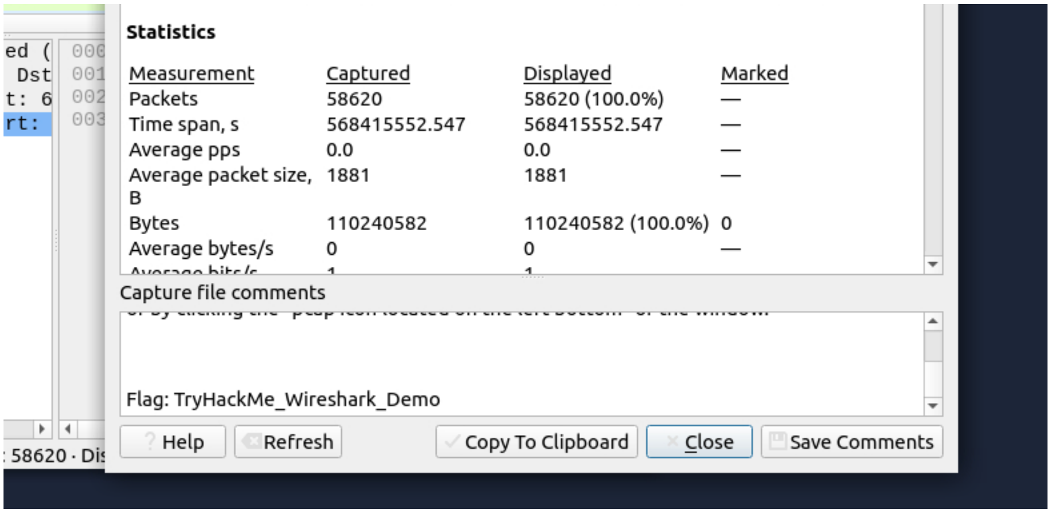
Double click to edit. Drag to move. Rules are processed in order until a match is found.

/home/ubuntu/.config/wireshark/colorfilters

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"



```
No.   Time        Source          ength  Info
  1 0.000000   145.254.16(         62 3372 → 80 [SYN] Seq=0
  2 0.911310   65.208.228          62 80 → 3372 [SYN, ACK] S
  3 0.911310   145.254.16(         54 3372 → 80 [ACK] Seq=1
  4 0.911310   145.254.16(        533 GET /download.html HTT
  5 1.472116   65.208.228          54 80 → 3372 [ACK] Seq=1
  6 1.682419   65.208.228        1434 80 → 3372 [ACK] Seq=1
  7 1.812606   145.254.16(         54 3372 → 80 [ACK] Seq=48
  8 1.812606   65.208.228        1434 80 → 3372 [ACK] Seq=13
  9 2.012894   145.254.16(         54 3372 → 80 [ACK] Seq=48
 10 2.443513   65.208.228        1434 80 → 3372 [ACK] Seq=27
 11 2.553672   65.208.228        1434 80 → 3372 [PSH, ACK] S
 12 2.553672   145.254.16(         54 3372 → 80 [ACK] Seq=48
 13 2.553672   145.254.16(         89 Standard query 0x0023
 14 2.633787   65.208.228        1434 80 → 3372 [ACK] Seq=55
 15 2.814046   145.254.16(         54 3372 → 80 [ACK] Seq=48
 16 2.894161   65.208.228        1434 80 → 3372 [ACK] Seq=69
```



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
Average bytes/s	0	0	—
Average bits/s	1	1	

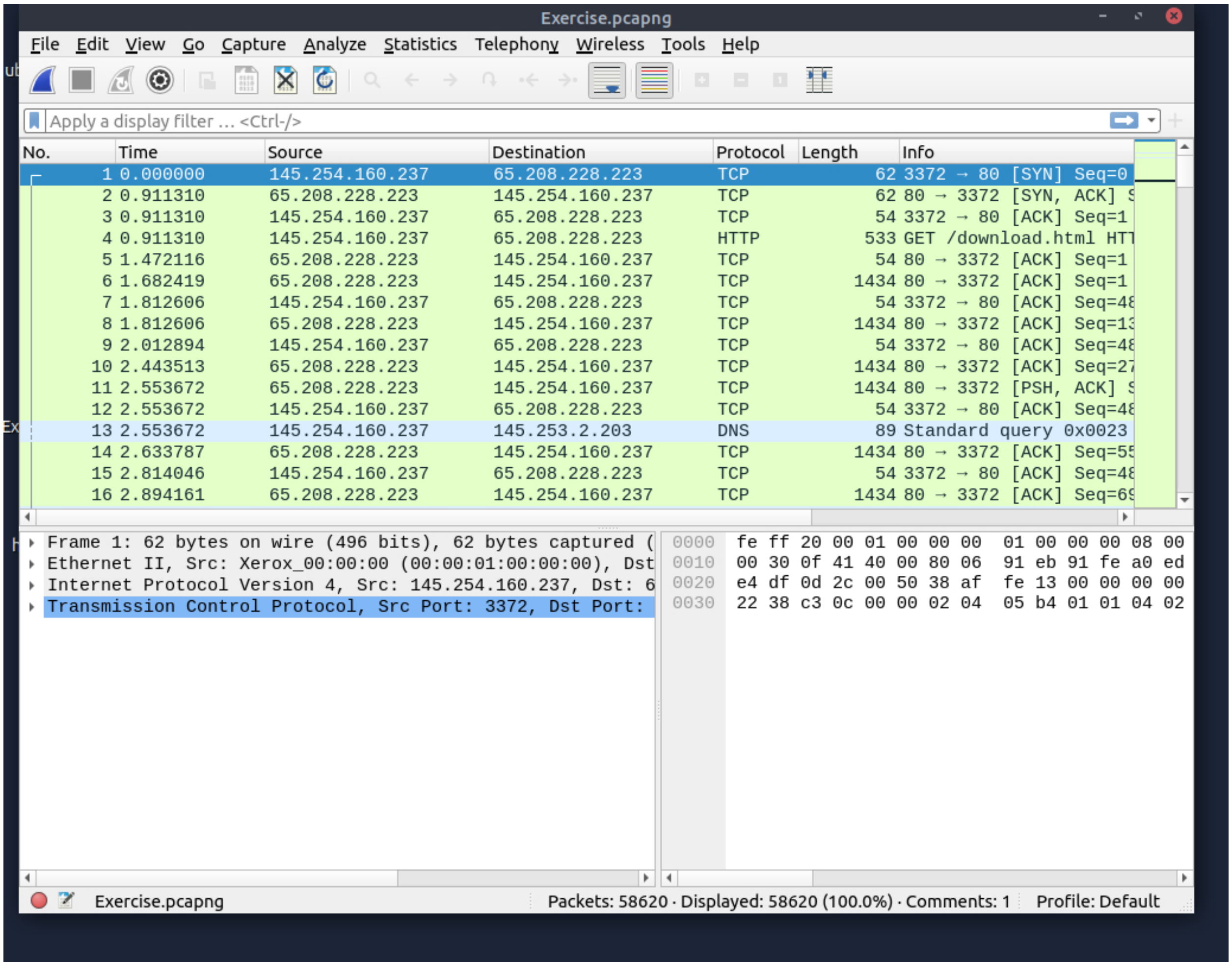
Capture file comments

Flag: TryHackMe_Wireshark_Demo

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"



```
No.   Time      Source          Destination     Protocol Length Info
    1 0.000000  145.254.160.237 65.208.228.223  TCP          62 3372 → 80 [SYN] Seq=0
    2 0.911310  65.208.228.223  145.254.160.237 TCP          62 80 → 3372 [SYN, ACK] S
    3 0.911310  145.254.160.237 65.208.228.223  TCP          54 3372 → 80 [ACK] Seq=1
    4 0.911310  145.254.160.237 65.208.228.223  HTTP        533 GET /download.html HTT
    5 1.472116  65.208.228.223  145.254.160.237 TCP          54 80 → 3372 [ACK] Seq=1
    6 1.682419  65.208.228.223  145.254.160.237 TCP        1434 80 → 3372 [ACK] Seq=1
    7 1.812606  145.254.160.237 65.208.228.223  TCP          54 3372 → 80 [ACK] Seq=48
    8 1.812606  65.208.228.223  145.254.160.237 TCP        1434 80 → 3372 [ACK] Seq=13
    9 2.012894  145.254.160.237 65.208.228.223  TCP          54 3372 → 80 [ACK] Seq=48
   10 2.443513  65.208.228.223  145.254.160.237 TCP        1434 80 → 3372 [ACK] Seq=27
   11 2.553672  65.208.228.223  145.254.160.237 TCP        1434 80 → 3372 [PSH, ACK] S
   12 2.553672  145.254.160.237 65.208.228.223  TCP          54 3372 → 80 [ACK] Seq=48
   13 2.553672  145.254.160.237 145.253.2.203   DNS          89 Standard query 0x0023
   14 2.633787  65.208.228.223  145.254.160.237 TCP        1434 80 → 3372 [ACK] Seq=55
   15 2.814046  145.254.160.237 65.208.228.223  TCP          54 3372 → 80 [ACK] Seq=48
   16 2.894161  65.208.228.223  145.254.160.237 TCP        1434 80 → 3372 [ACK] Seq=69
```

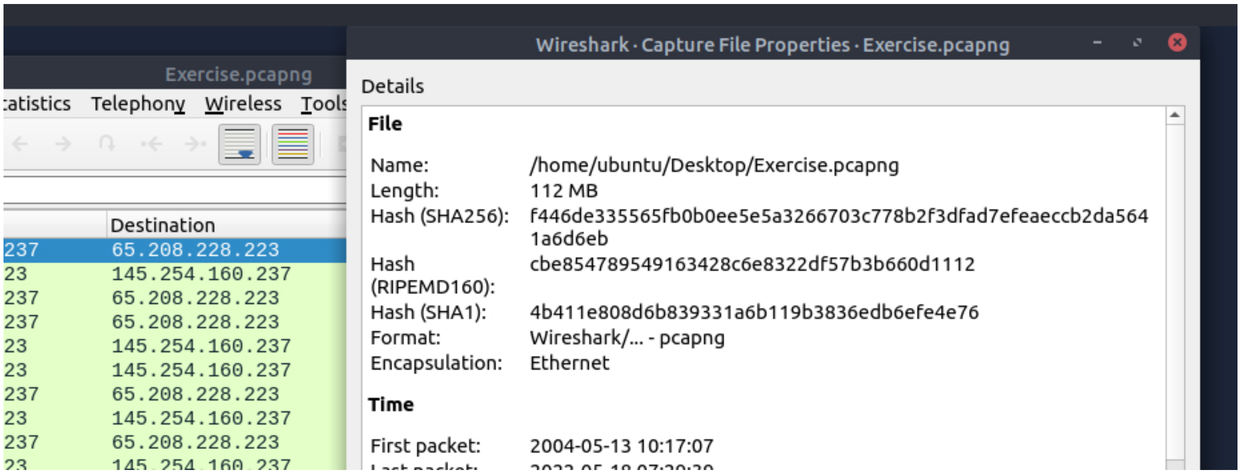
```
› Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (
› Ethernet II, Src: Xerox_00:00:00 (00:00:01:00:00:00), Dst
› Internet Protocol Version 4, Src: 145.254.160.237, Dst: 6
› Transmission Control Protocol, Src Port: 3372, Dst Port:
```

```
0000  fe ff 20 00 01 00 00 00  01 00 00 00 08 00
0010  00 30 0f 41 40 00 80 06  91 eb 91 fe a0 ed
0020  e4 df 0d 2c 00 50 38 af  fe 13 00 00 00 00
0030  22 38 c3 0c 00 00 02 04  05 b4 01 01 04 02
```

Exercise.pcapng · Packets: 58620 · Displayed: 58620 (100.0%) · Comments: 1 · Profile: Default

Answer: 58620

3. **What is the SHA256 hash value of the capture file?**
   - A SHA256 hash is a 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.



Destination
65.208.228.223
145.254.160.237
65.208.228.223
65.208.228.223
145.254.160.237
145.254.160.237
65.208.228.223
145.254.160.237
65.208.228.223

File

Name:	/home/ubuntu/Desktop/Exercise.pcapng
Length:	112 MB
Hash (SHA256):	f446de335565fb0b0ee5e5a3266703c778b2f3dfad7efeaeccb2da564 1a6d6eb
Hash (RIPEMD160):	cbe854789549163428c6e8322df57b3b660d1112
Hash (SHA1):	4b411e808d6b839331a6b119b3836edb6efe4e76
Format:	Wireshark/... - pcapng
Encapsulation:	Ethernet

Time

First packet:	2004-05-13 10:17:07

Answer: f446de335565fb0b0ee5e5a3266703c778b2f3dfad7efeaeccb2da5641a6d6eb

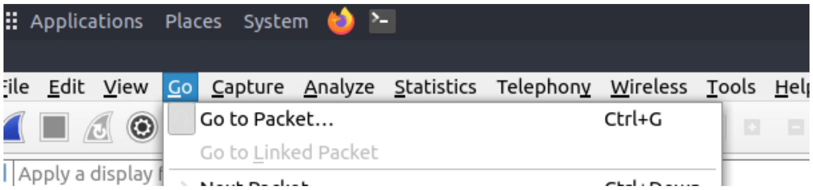
Packet Dissection

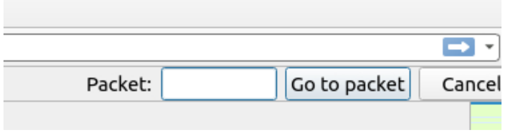
- Investigate packets for details by decoding available protocols and fields within Wireshark.

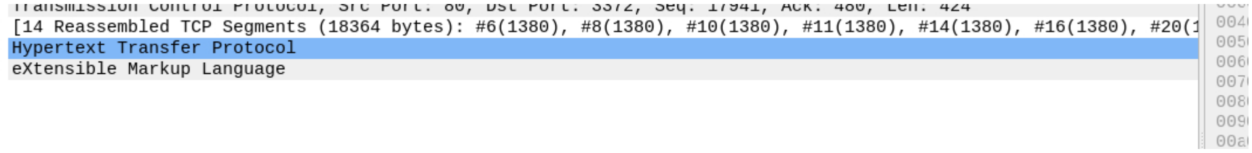
Packet Details

- 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.

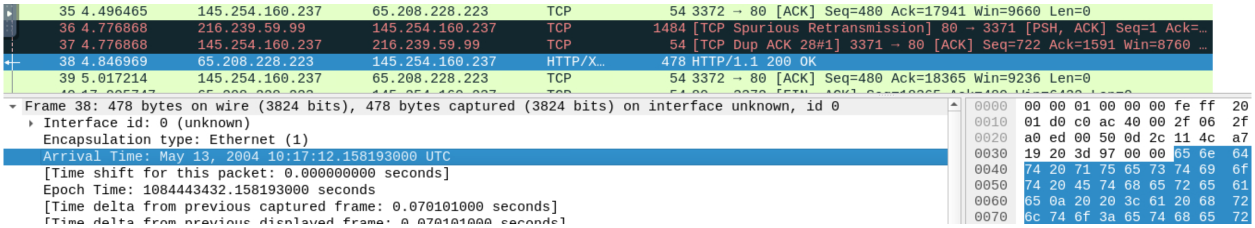





```
Transmission Control Protocol, Src Port: 80, Dst Port: 3372, Seq: 17941, Ack: 480, Len: 424
[14 Reassembled TCP Segments (18364 bytes): #6(1380), #8(1380), #10(1380), #11(1380), #14(1380), #16(1380), #20(1
Hypertext Transfer Protocol
eXtensible Markup Language
```

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.

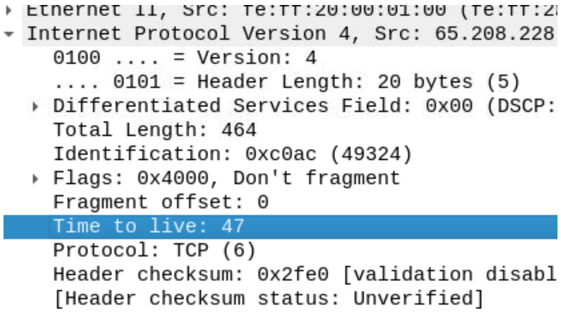

```
35 4.496465   145.254.160.237   65.208.228.223    TCP        54 3372 → 80 [ACK] Seq=480 Ack=17941 Win=9660 Len=0
36 4.776868   216.239.59.99     145.254.160.237   TCP      1484 [TCP Spurious Retransmission] 80 → 3371 [PSH, ACK] Seq=1 Ack=…
37 4.776868   145.254.160.237   216.239.59.99     TCP        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
```

```
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]
```

```
0000  00 00 01 00 00 00 fe ff  20
0010  01 d0 c0 ac 40 00 2f 06  2f
0020  a0 ed 00 50 0d 2c 11 4c  a7
0030  19 20 3d 97 00 00 65 6e  64
0040  74 20 71 75 65 73 74 69  6f
0050  74 20 45 74 68 65 72 65  61
0060  65 0a 20 20 3c 61 20 68  72
0070  6c 74 6f 3a 65 74 68 65  72
```

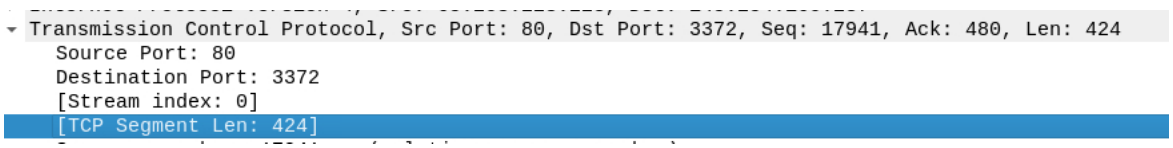
Answer: 05/13/2024

3. **What is the TTL value?**
   - You can find the Time To Live in the “Internet Protocol Version” section.


```
Ethernet II, Src: fe:ff:20:00:01:00 (fe:ff:2
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 disabl
  [Header checksum status: Unverified]
```

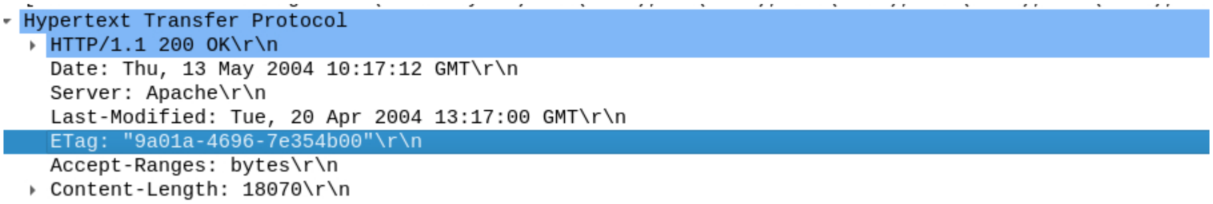
Answer: 47

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

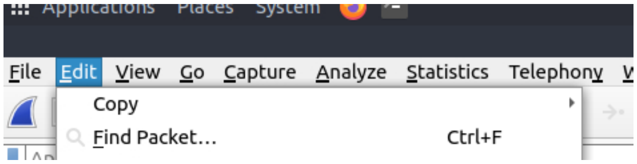
5. **What is the e-tag value?**
    - You will be able to find the e-tag value in the “Hypertext Transfer Protocol” section and you will see “ETAG:”



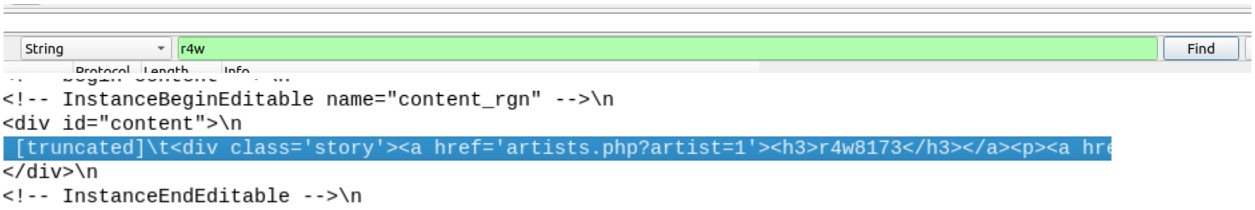
```
▾ Hypertext Transfer Protocol
  ▸ HTTP/1.1 200 OK\r\n
    Date: Thu, 13 May 2004 10:17:12 GMT\r\n
    Server: Apache\r\n
    Last-Modified: Tue, 20 Apr 2004 13:17:00 GMT\r\n
    ETag: "9a01a-4696-7e354b00"\r\n
    Accept-Ranges: bytes\r\n
  ▸ Content-Length: 18070\r\n
```

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.



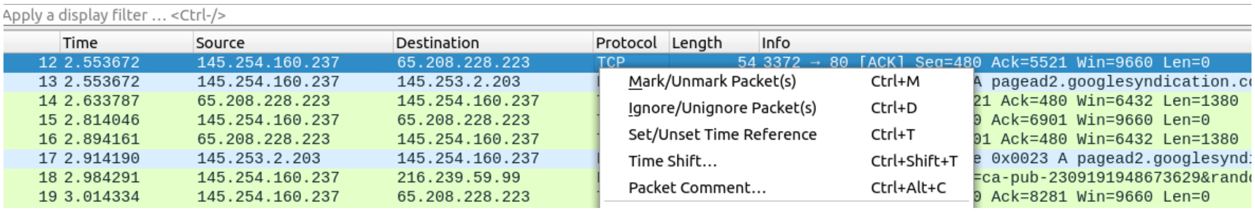
```
<!-- InstanceBeginEditable name="content_rgn" -->\n
<div id="content">\n
 [truncated]\t<div class='story'><a href='artists.php?artist=1'><h3>r4w8173</h3></a><p><a hre
</div>\n
<!-- InstanceEndEditable -->\n
```

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

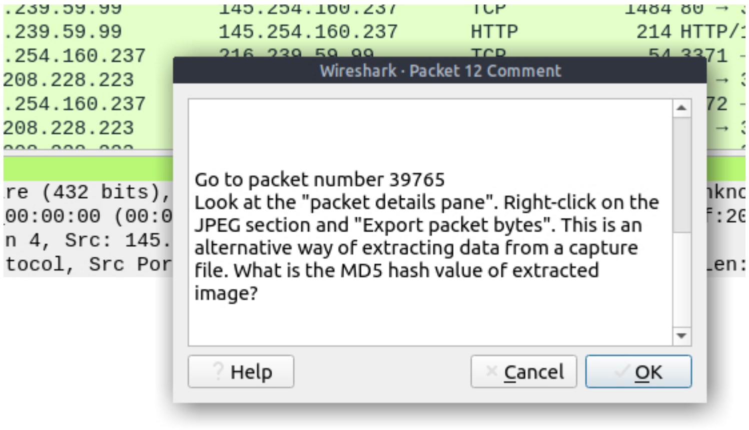
   - First, let navigate to packet 12. Same method when looking for packet 38 (Go-Go to Packet – Type in the number of the packet)
   - Next click on the "Packet comment to view the comment of the packet"



Apply a display filter … <Ctrl-/>
Mark/Unmark Packet(s) Ctrl+M
Ignore/Unignore Packet(s) Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift… Ctrl+Shift+T
Packet Comment… Ctrl+Alt+C

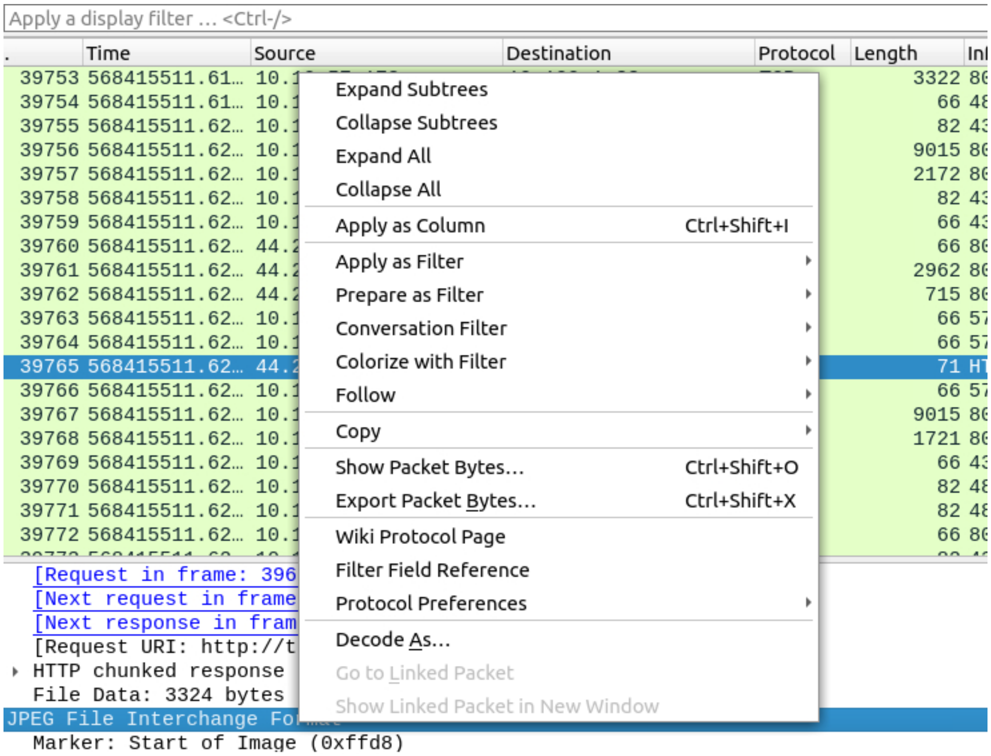
```
    Time        Source           Destination      Protocol Length  Info
 12 2.553672    145.254.160.237  65.208.228.223   TCP          54 3372 → 80 [ACK] Seq=480 Ack=5521 Win=9660 Len=0
 13 2.553672    145.254.160.237  145.253.2.203                    A pagead2.googlesyndication.c
 14 2.633787    65.208.228.223   145.254.160.237                  21 Ack=480 Win=6432 Len=1380
 15 2.814046    145.254.160.237  65.208.228.223                   0 Ack=6901 Win=9660 Len=0
 16 2.894161    65.208.228.223   145.254.160.237                  01 Ack=480 Win=6432 Len=1380
 17 2.914190    145.253.2.203    145.254.160.237                  e 0x0023 A pagead2.googlesynd
 18 2.984291    145.254.160.237  216.239.59.99                    =ca-pub-2309191948673629&rand
 19 3.014334    145.254.160.237  65.208.228.223                   0 Ack=8281 Win=9660 Len=0
```

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



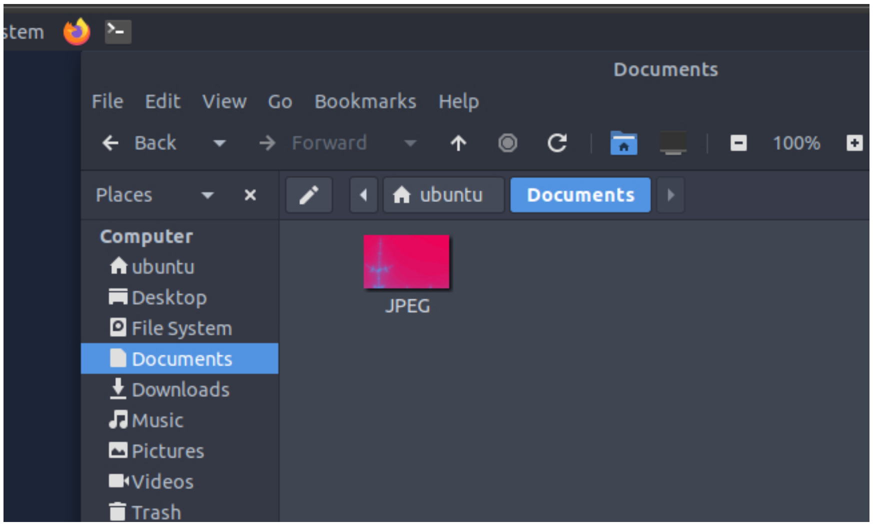
Go to packet number 39765
Look at the "packet details pane". Right-click on the JPEG section and "Export packet bytes". This is an alternative way of extracting data from a capture file. What is the MD5 hash value of extracted image?

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

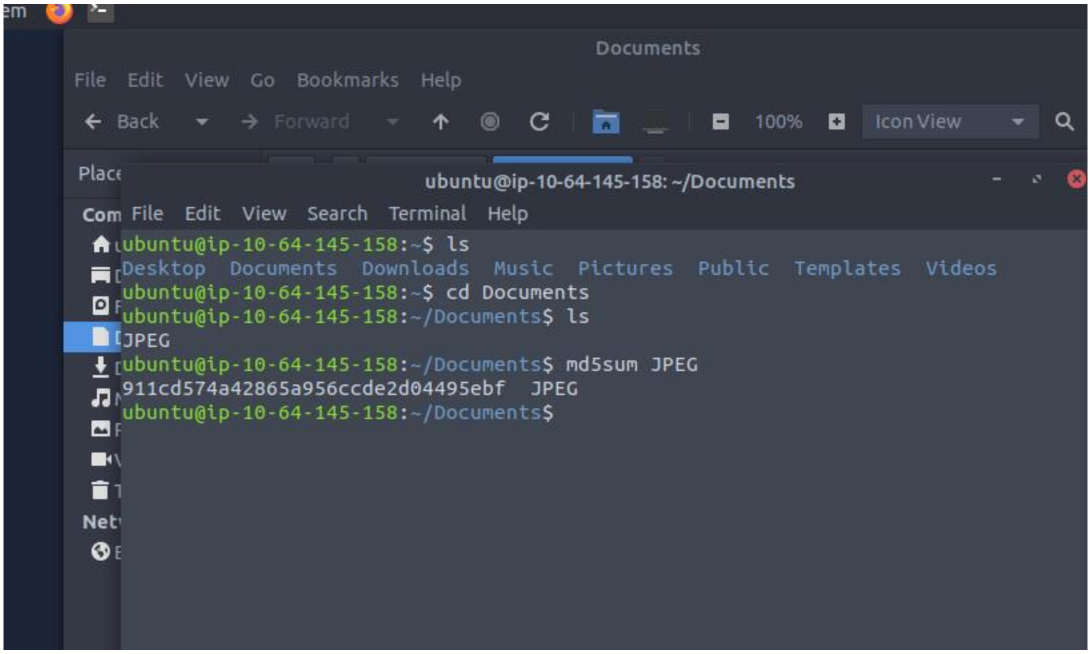


```
Apply a display filter … <Ctrl-/>
.      Time              Source                                        Length  Inl
39753 568415511.61… 10.1                                                 3322 80
39754 568415511.61… 10.1                                                   66 48
39755 568415511.62… 10.1                                                   82 43
39756 568415511.62… 10.1                                                 9015 80
39757 568415511.62… 10.1                                                 2172 80
39758 568415511.62… 10.1                                                   82 43
39759 568415511.62… 10.1                                                   66 43
39760 568415511.62… 44.2                                                   66 80
39761 568415511.62… 44.2                                                 2962 80
39762 568415511.62… 44.2                                                  715 80
39763 568415511.62… 10.1                                                   66 57
39764 568415511.62… 10.1                                                   66 57
39765 568415511.62… 44.2                                                   71 HT
39766 568415511.62… 10.1                                                   66 57
39767 568415511.62… 10.1                                                 9015 80
39768 568415511.62… 10.1                                                 1721 80
39769 568415511.62… 10.1                                                   66 43
39770 568415511.62… 10.1                                                   82 48
39771 568415511.62… 10.1                                                   82 48
39772 568415511.62… 10.1                                                   66 80
   [Request in frame: 396
   [Next request in frame
   [Next response in fram
   [Request URI: http://t
 › HTTP chunked response
   File Data: 3324 bytes
JPEG File Interchange Fo
   Marker: Start of Image (0xffd8)
```

- 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.



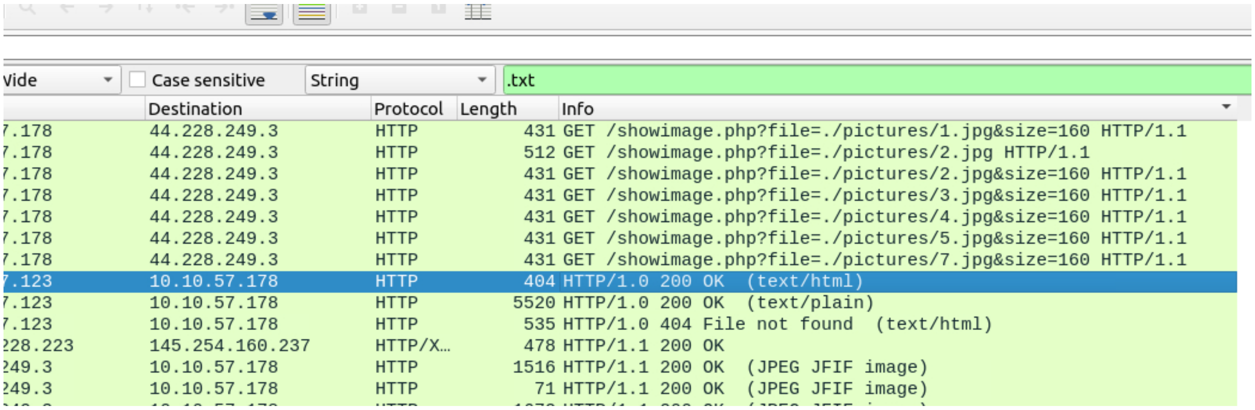
- Finally open the unix/linux terminal and navigate to the directory and run the command md5sum <filename>


Documents
File Edit View Go Bookmarks Help
Back
Forward
100%
Icon View
Place
Com
Net
ubuntu@ip-10-64-145-158: ~/Documents
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

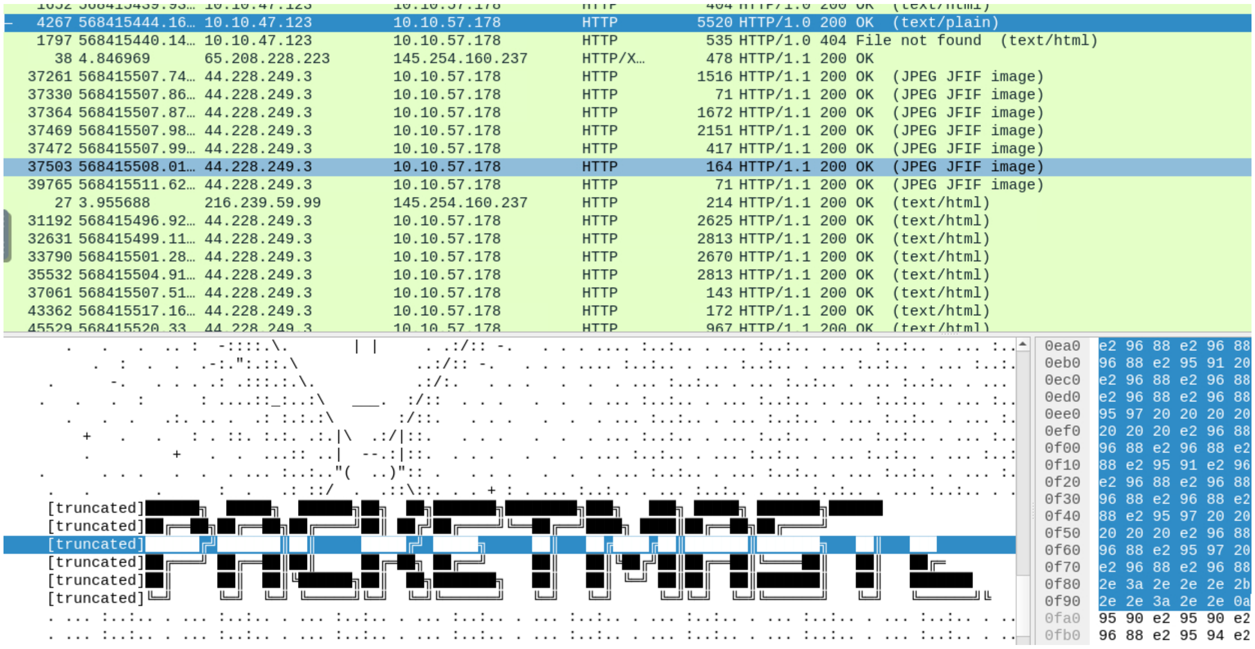
3. **There is a ".txt" file inside the capture file. Find the file and read it: what is the alien's name?**
   - Go to the "Go to Packet" and search for the ".txt" file



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

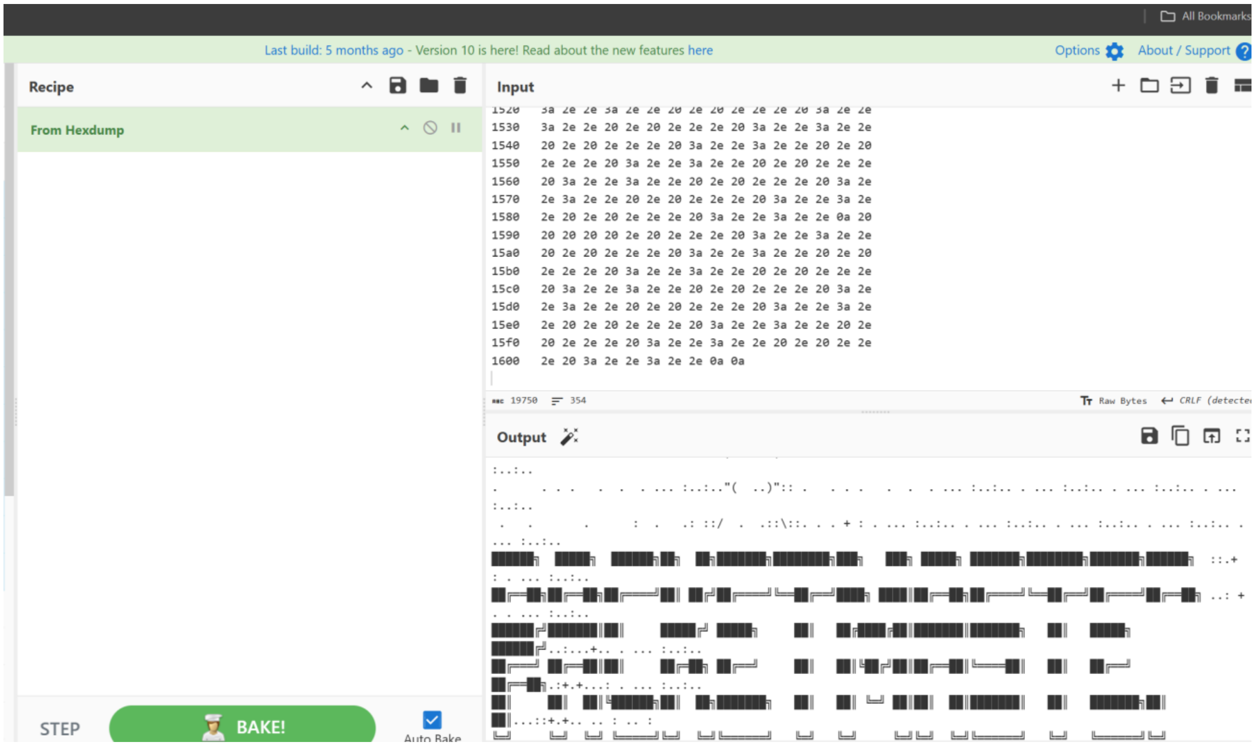


```
 4267 568415444.16… 10.10.47.123   10.10.57.178    HTTP    5520 HTTP/1.0 200 OK  (text/plain)
 1797 568415440.14… 10.10.47.123   10.10.57.178    HTTP     535 HTTP/1.0 404 File not found  (text/html)
   38 4.846969      65.208.228.223 145.254.160.237 HTTP/X…  478 HTTP/1.1 200 OK
37261 568415507.74… 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)
```

```
[truncated]
[truncated]
[truncated]
[truncated]
[truncated]
[truncated]
```

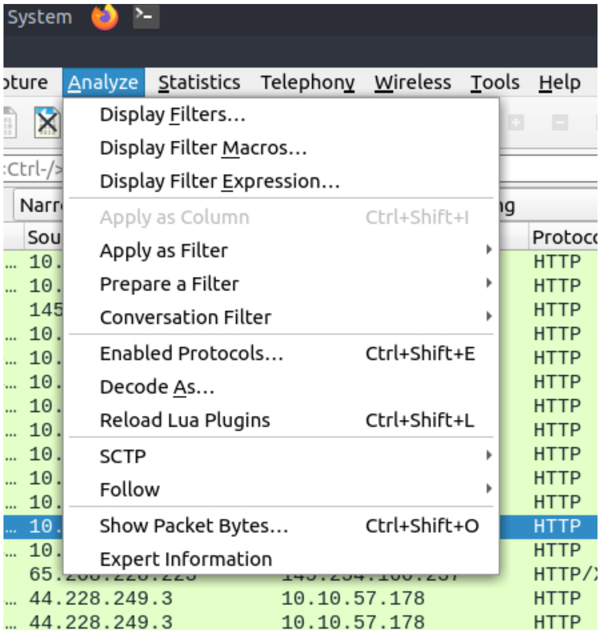
```
0ea0  e2 96 88 e2 96 88
0eb0  96 88 e2 95 91 20
0ec0  e2 96 88 e2 96 88
0ed0  e2 96 88 e2 96 88
0ee0  95 97 20 20 20 20
0ef0  20 20 20 e2 96 88
0f00  96 88 e2 96 88 e2
0f10  88 e2 95 91 e2 96
0f20  e2 96 88 e2 96 88
0f30  96 88 e2 96 88 e2
0f40  88 e2 95 97 20 20
0f50  20 20 20 e2 96 88
0f60  96 88 e2 95 97 20
0f70  e2 96 88 e2 96 88
0f80  2e 3a 2e 2e 2e 2b
0f90  2e 2e 3a 2e 2e 0a
0fa0  95 90 e2 95 90 e2
0fb0  96 88 e2 95 94 e2
```

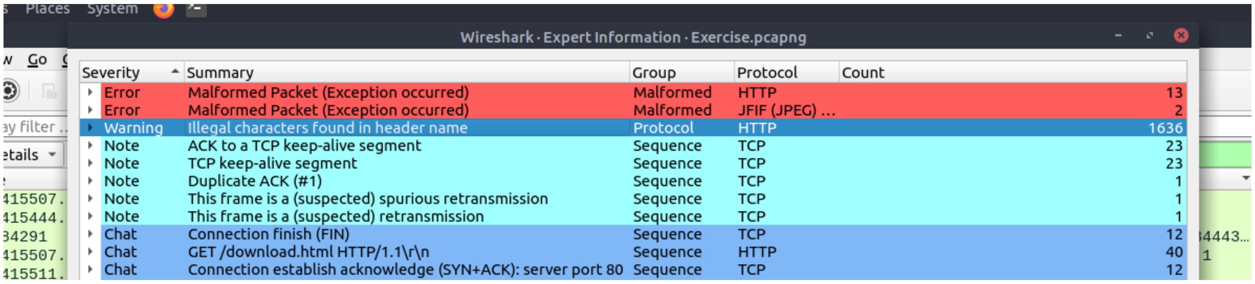
   b. Option 2: copy the hexadecimal and use Cyberchef to decode Hex dump



```
1520   3a 2e 2e 3a 2e 2e 20 2e 20 2e 2e 2e 20 3a 2e 2e
1530   3a 2e 2e 20 2e 20 2e 2e 2e 20 3a 2e 2e 3a 2e 2e
1540   20 2e 20 2e 2e 2e 20 3a 2e 2e 3a 2e 2e 20 2e 20
1550   2e 2e 2e 20 3a 2e 2e 3a 2e 2e 20 2e 20 2e 2e 2e
1560   20 3a 2e 2e 3a 2e 2e 20 2e 20 2e 2e 2e 20 3a 2e
1570   2e 3a 2e 2e 20 2e 20 2e 2e 2e 20 3a 2e 2e 3a 2e
1580   2e 20 2e 20 2e 2e 2e 20 3a 2e 2e 3a 2e 2e 0a 20
1590   20 20 20 20 2e 20 2e 2e 2e 20 3a 2e 2e 3a 2e 2e
15a0   20 2e 20 2e 2e 2e 20 3a 2e 2e 3a 2e 2e 20 2e 20
15b0   2e 2e 2e 20 3a 2e 2e 3a 2e 2e 20 2e 20 2e 2e 2e
15c0   20 3a 2e 2e 3a 2e 2e 20 2e 20 2e 2e 2e 20 3a 2e
15d0   2e 3a 2e 2e 20 2e 20 2e 2e 2e 20 3a 2e 2e 3a 2e
15e0   2e 20 2e 20 2e 2e 2e 20 3a 2e 2e 3a 2e 2e 20 2e
15f0   20 2e 2e 2e 20 3a 2e 2e 3a 2e 2e 20 2e 20 2e 2e
1600   2e 20 3a 2e 2e 3a 2e 2e 0a 0a

19750   354
```

4. **Look at the expert info section. What is the number of warnings?**
    - To locate the number of warnings, go to “Analyze-Expert Information”



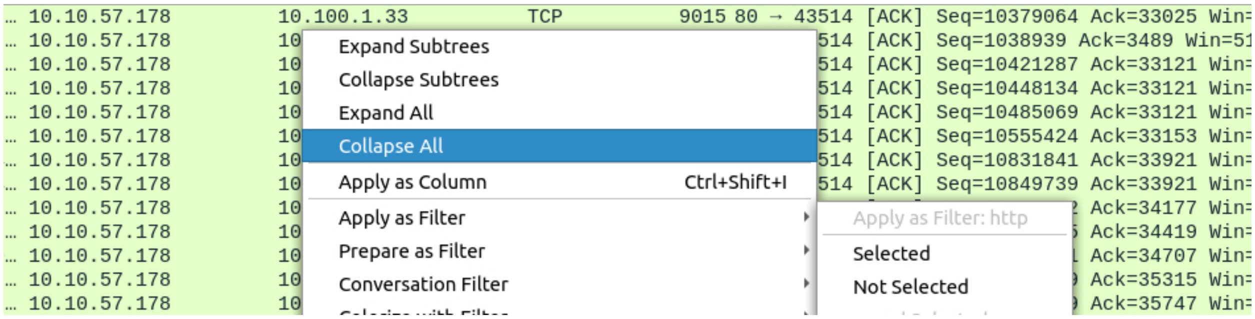


Severity	Summary	Group	Protocol	Count
Error	Malformed Packet (Exception occurred)	Malformed	HTTP	13
Error	Malformed Packet (Exception occurred)	Malformed	JFIF (JPEG) ...	2
Warning	Illegal characters found in header name	Protocol	HTTP	1636
Note	ACK to a TCP keep-alive segment	Sequence	TCP	23
Note	TCP 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

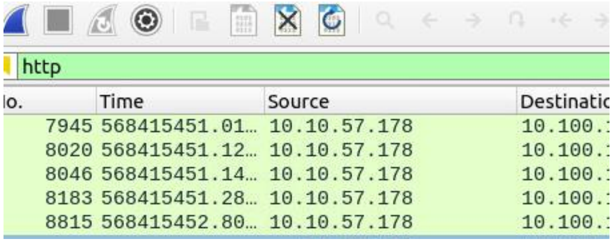
Answer: 1636

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"



```
… 10.10.57.178        10.100.1.33       TCP      9015 80 → 43514 [ACK] Seq=10379064 Ack=33025 Win=
… 10.10.57.178        10                              514 [ACK] Seq=1038939 Ack=3489 Win=51
… 10.10.57.178        10                              514 [ACK] Seq=10421287 Ack=33121 Win=
… 10.10.57.178        10                              514 [ACK] Seq=10448134 Ack=33121 Win=
… 10.10.57.178        10                              514 [ACK] Seq=10485069 Ack=33121 Win=
… 10.10.57.178        10                              514 [ACK] Seq=10555424 Ack=33153 Win=
… 10.10.57.178        10                              514 [ACK] Seq=10831841 Ack=33921 Win=
… 10.10.57.178        10                              514 [ACK] Seq=10849739 Ack=33921 Win=
… 10.10.57.178        10                                                     Ack=34177 Win=
… 10.10.57.178        10                                                     Ack=34419 Win=
… 10.10.57.178        10                                                     Ack=34707 Win=
… 10.10.57.178        10                                                     Ack=35315 Win=
… 10.10.57.178        10                                                     Ack=35747 Win=
```

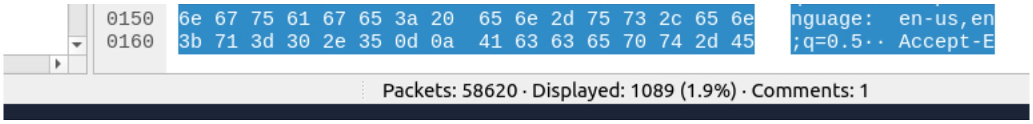


```
http
```

```
No.   Time              Source          Destinatic
 7945 568415451.01…     10.10.57.178    10.100.:
 8020 568415451.12…     10.10.57.178    10.100.:
 8046 568415451.14…     10.10.57.178    10.100.:
 8183 568415451.28…     10.10.57.178    10.100.:
 8815 568415452.80…     10.10.57.178    10.100.:
```

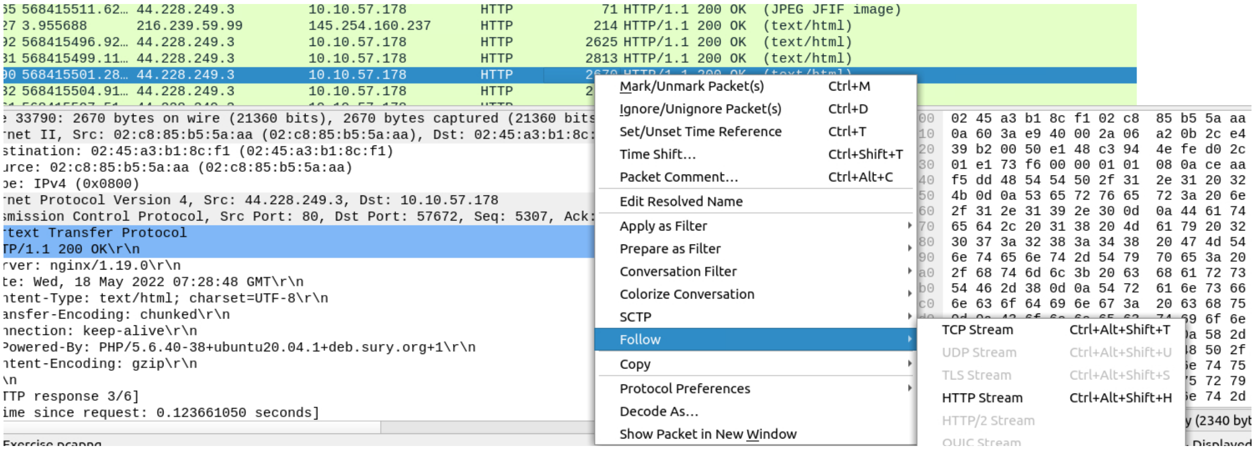
Answer: http

2. **What is the number of displayed packets?**
   - You will find this on the bar at the bottom of the screen.



```
0150  6e 67 75 61 67 65 3a 20  65 6e 2d 75 73 2c 65 6e   nguage:  en-us,en
0160  3b 71 3d 30 2e 35 0d 0a  41 63 63 65 70 74 2d 45   ;q=0.5·· Accept-E

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

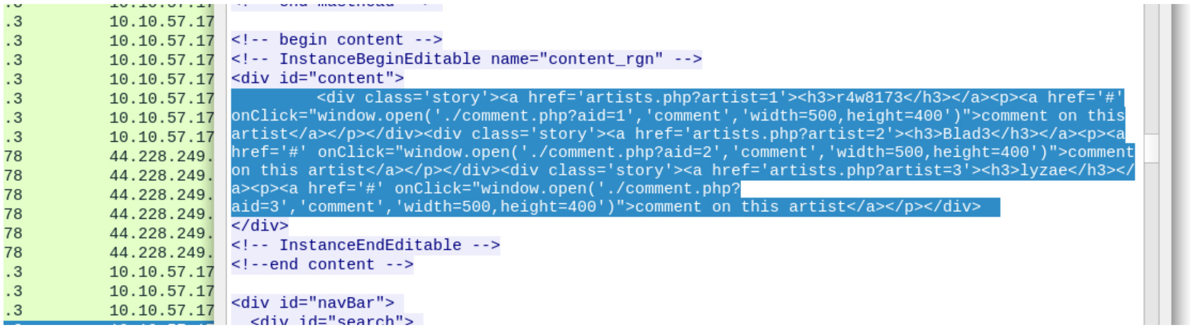
3. **Go to packet number 33790, follow the HTTP stream, and look carefully at the responses. Looking at the web server's response, what is the total number of artists?**
    - Same method, navigate to 33790 packet using "Go to Packet"
    - Right-click on the packet and select the "Follow - HTTP stream"



```
55 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)
92 568415496.92… 44.228.249.3     10.10.57.178     HTTP    2625 HTTP/1.1 200 OK  (text/html)
31 568415499.11… 44.228.249.3     10.10.57.178     HTTP    2813 HTTP/1.1 200 OK  (text/html)
90 568415501.28… 44.228.249.3     10.10.57.178     HTTP    2670 HTTP/1.1 200 OK  (text/html)
32 568415504.91… 44.228.249.3     10.10.57.178     HTTP    2

e 33790: 2670 bytes on wire (21360 bits), 2670 bytes captured (21360 bits
rnet II, Src: 02:c8:85:b5:5a:aa (02:c8:85:b5:5a:aa), Dst: 02:45:a3:b1:8c:
stination: 02:45:a3:b1:8c:f1 (02:45:a3:b1:8c:f1)
urce: 02:c8:85:b5:5a:aa (02:c8:85:b5:5a:aa)
pe: IPv4 (0x0800)
rnet Protocol Version 4, Src: 44.228.249.3, Dst: 10.10.57.178
smission Control Protocol, Src Port: 80, Dst Port: 57672, Seq: 5307, Ack:
rtext Transfer Protocol
TP/1.1 200 OK\r\n
rver: nginx/1.19.0\r\n
te: Wed, 18 May 2022 07:28:48 GMT\r\n
ntent-Type: text/html; charset=UTF-8\r\n
ansfer-Encoding: chunked\r\n
nnection: keep-alive\r\n
Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1\r\n
ntent-Encoding: gzip\r\n
\n
TTP response 3/6]
ime since request: 0.123661050 seconds]

00  02 45 a3 b1 8c f1 02 c8   85 b5 5a aa
10  0a 60 3a e9 40 00 2a 06   a2 0b 2c e4
20  39 b2 00 50 e1 48 c3 94   4e fe d0 2c
30  01 e1 73 f6 00 00 01 01   08 0a ce aa
40  f5 dd 48 54 54 50 2f 31   2e 31 20 32
50  4b 0d 0a 53 65 72 76 65   72 3a 20 6e
60  2f 31 2e 31 39 2e 30 0d   0a 44 61 74
70  65 64 2c 20 31 38 20 4d   61 79 20 32
80  30 37 3a 32 38 3a 34 38   20 47 4d 54
90  6e 74 65 6e 74 2d 54 79   70 65 3a 20
a0  2f 68 74 6d 6c 3b 20 63   68 61 72 73
b0  54 46 2d 38 0d 0a 54 72   61 6e 73 66
c0  6e 63 6f 64 69 6e 67 3a   20 63 68 75
```

Mark/Unmark Packet(s) Ctrl+M
Ignore/Unignore Packet(s) Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift… Ctrl+Shift+T
Packet Comment… Ctrl+Alt+C
Edit Resolved Name
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As…
Show Packet in New Window
TCP Stream Ctrl+Alt+Shift+T
UDP Stream Ctrl+Alt+Shift+U
TLS Stream Ctrl+Alt+Shift+S
HTTP Stream Ctrl+Alt+Shift+H
HTTP/2 Stream
QUIC Stream
Exercise.pcapng
(2340 byt
Displayed

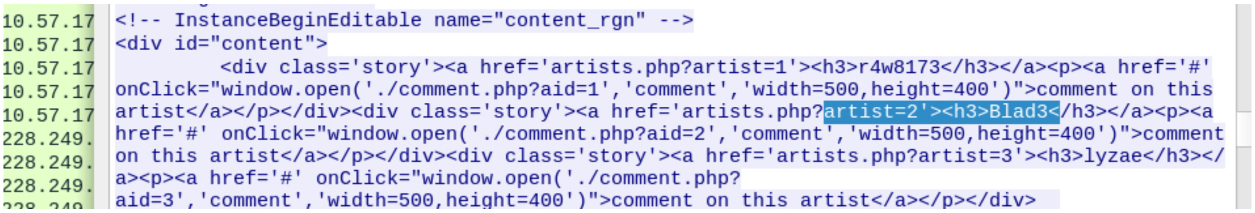
- At this stage, we must analyze the http stream to determine the number of Artist.
- Usually represented as "Artist=1" and so forth.



```
<!-- 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?**



```
<!-- 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>
```

Answer: Blad3