

Name : Amr Khaled Elgendy
Group : AMIT - Cyber Security Online 87
Task :Wireshark 101

Wireshark, a tool used for creating and analyzing PCAPs (network packet capture files), is commonly used as one of the best packet analysis tools.

ARP Traffic

What is the Opcode for Packet 6?
Request (1)

This capture has multiple protocols so you may need to use your knowledge of filtering from previous tasks; once you're ready, begin analysis of the capture.

Answer the questions below

What is the Opcode for Packet 6?

Request (1) ✓ Correct Answer

What is the source MAC Address of Packet 19?

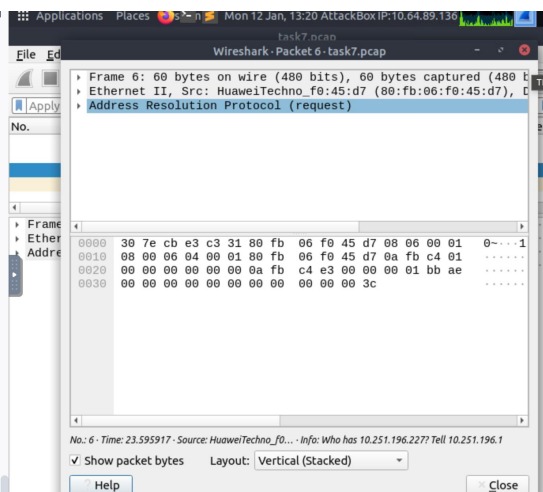
Check

What 4 packets are Reply packets?

Check

What IP Address is at 80:fb:06:f0:45:d7?

Check



What is the source MAC Address of Packet 19?
80:fb:06:f0:45:d7

Practical ARP Packet Analysis

Now that you know what ARP packets and normal traffic look, let's dive into an exercise. Start the AttackBox, and go to the folder /root/Rooms/Wireshark101 and double click the task7.pcap file to open it in Wireshark; you can also download the provided PCAP on the task.

This capture has multiple protocols so you may need to use your knowledge of filtering from previous tasks; once you're ready, begin analysis of the capture.

Answer the questions below

What is the Opcode for Packet 6?

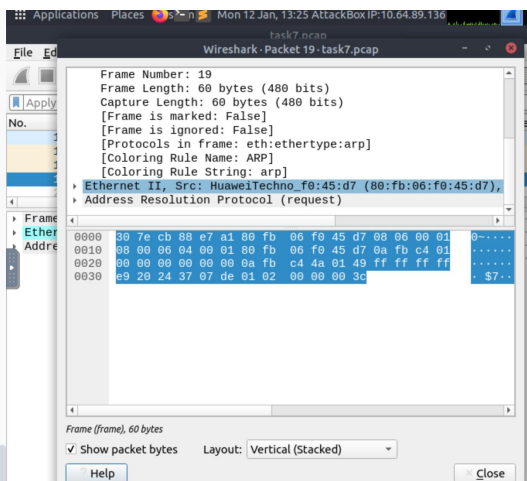
Request (1) ✓ Correct Answer

What is the source MAC Address of Packet 19?

Check

What 4 packets are Reply packets?

Check



What 4 packets are Reply packets?

76,400,459,520

Explanation :

1st - Filter by Protocol based on "ARP"

2nd - Scroll through each packet and look for "Opcode: reply (2)"

What IP Address is at 80:fb:06:f0:45:d7?

10.251.23.1

Explanation :

1st - Filter by Protocol based on "ARP"

arp && eth.addr == 80:fb:06:f0:45:d7

ICMP Traffic

What is the type for packet 4?

8

Room progress (41%)

Practical ICMP Packet Analysis

Now that you understand how an ICMP packet is formed and what it contains, we can begin hands-on practical analysis of ICMP packets. Go to the folder /root/Rooms/Wireshark101 on the AttackBox and double click the task8.pcap file to open it in Wireshark; you can also download the pcap on this task.

This network capture only has two protocols so it is up to you whether or not you decide to filter the ICMP protocol or not.

Answer the questions below

What is the type for packet 4?

8 ✓ Correct Answer

What is the type for packet 5?

— Check

What is the timestamp for packet 12, only including month day and year?

note: Wireshark bases it's time off of your devices time zone, if your answer is wrong try one day more or less.

Applications Place Mon 12 Jan, 14:17 AttackBox IP: 10.64.111.156

task8.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools

icmp

No.	Time	Source	Destination
4	5.013334	192.168.43.9	8.8.8.8
5	5.505538	8.8.8.8	192.168.43.9
6	6.019290	192.168.43.9	8.8.8.8
7	6.153653	8.8.8.8	192.168.43.9
8	7.015108	192.168.43.9	8.8.8.8

Frame 4: 98 bytes on wire (784 bits), 98 bytes captured on interface 0
Ethernet II, Src: Apple_13:c5:58 (60:33:4b:13:c5:58), Dst: 08:00:20:00:00:00
Internet Protocol Version 4, Src: 192.168.43.9, Dst: 8.8.8.8
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0xbbb3 [correct]
[Checksum Status: Good]
Identifier (BE): 55099 (0xd73b)
Identifier (LE): 15319 (0x3bd7)
Sequence Number (BE): 0 (0x0000)
Sequence Number (LE): 0 (0x0000)
[Request frame: 4]
[Response frame: 5]
Timestamp from icmp data: May 30, 2013 23:45:17.28
[Timestamp from icmp data (relative): 0.000079000]
Data (48 bytes)

What is the type for packet 5?

0

Room progress (41%)

Practical ICMP Packet Analysis

Now that you understand how an ICMP packet is formed and what it contains, we can begin hands-on practical analysis of ICMP packets. Go to the folder /root/Rooms/Wireshark101 on the AttackBox and double click the task8.pcap file to open it in Wireshark; you can also download the pcap on this task.

This network capture only has two protocols so it is up to you whether or not you decide to filter the ICMP protocol or not.

Answer the questions below

What is the type for packet 4?

8 ✓ Correct Answer

What is the type for packet 5?

— Check

What is the timestamp for packet 12, only including month day and year?

Applications Place Mon 12 Jan, 14:19 AttackBox IP: 10.64.111.156

task8.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools

icmp

No.	Time	Source	Destination
4	5.013334	192.168.43.9	8.8.8.8
5	5.505538	8.8.8.8	192.168.43.9
6	6.019290	192.168.43.9	8.8.8.8
7	6.153653	8.8.8.8	192.168.43.9
8	7.015108	192.168.43.9	8.8.8.8

Frame 5: 98 bytes on wire (784 bits), 98 bytes captured on interface 0
Ethernet II, Src: MS-NLB-PhysServer-26_11:f0:c8:3b (08:00:20:00:00:00), Dst: 08:00:20:00:00:00
Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.43.9
Internet Control Message Protocol
Type: 0 (Echo (ping) reply)
Code: 0
Checksum: 0xc3b3 [correct]
[Checksum Status: Good]
Identifier (BE): 55099 (0xd73b)
Identifier (LE): 15319 (0x3bd7)
Sequence Number (BE): 0 (0x0000)
Sequence Number (LE): 0 (0x0000)
[Request frame: 4]
[Response time: 492.204 ms]
Timestamp from icmp data: May 30, 2013 23:45:17.28
[Timestamp from icmp data (relative): 0.492203000]
Data (48 bytes)

What is the timestamp for packet 12, only including month day and year?
note: Wireshark bases it's time off of your devices time zone, if your
answer is wrong try one day more or less.

May 30,2013

Room progress (48%)

on practical analysis of ICMP packets. Go to the folder /root/Rooms/Wireshark101 on the AttackBox and double click the task8.pcap file to open it in Wireshark; you can also download the pcap on this task.

This network capture only has two protocols so it is up to you whether or not you decide to filter the ICMP protocol or not.

Answer the questions below

What is the type for packet 4?

✓ Correct Answer

What is the type for packet 5?

✓ Correct Answer

What is the timestamp for packet 12, only including month day and year?

note: Wireshark bases it's time off of your devices time zone, if your answer is wrong try one day more or less.

✓ Correct Answer

Applications Place Mon 12 Jan, 14:20 AttackBox IP:10.64.111.156

task8.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools

icmp

No.	Time	Source	Destination
7	6.153653	8.8.8.8	192.168.43.9
8	7.015108	192.168.43.9	8.8.8.8
9	7.781987	8.8.8.8	192.168.43.9
12	7.983593	192.168.43.9	8.8.4.4
13	8.984437	192.168.43.9	8.8.4.4

Frame 12: 98 bytes on wire (784 bits), 98 bytes captured on interface 0
Ethernet II, Src: Apple_13:c5:58 (60:33:4b:13:c5:58), Dst: 8.8.4.4
Internet Protocol Version 4, Src: 192.168.43.9, Dst: 8.8.4.4
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x2bfd [correct]
[Checksum Status: Good]
Identifier (BE): 56123 (0xdb3b)
Identifier (LE): 15323 (0x3bdb)
Sequence Number (BE): 0 (0x0000)
Sequence Number (LE): 0 (0x0000)
[No response seen]
Timestamp from icmp data: May 30, 2013 23:45:20.25
[Timestamp from icmp data (relative): 0.000110000 seconds]
Data (48 bytes)

What is the full data string for packet 18?
08090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f202122232425
262728292a2b2c2d2e2f3031323334353637

✓ Correct Answer

What is the full data string for packet 18?

✓ Correct Answer

Code: 0
Checksum: 0xb6d2 [correct]
[Checksum Status: Good]
Identifier (BE): 56635 (0xdd3b)
Identifier (LE): 15325 (0x3bdd)
Sequence Number (BE): 0 (0x0000)
Sequence Number (LE): 0 (0x0000)
[Response frame: 19]
Timestamp from icmp data: May 30, 2013 23:45:24.348349000 BST
[Timestamp from icmp data (relative): 0.000092000 seconds]
Data (48 bytes)
Data: 08090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f202122232425262728292a2b2c2d2e2f3031323334353637
[Length: 48]

What is being queried in packet 1?
8.8.8.8.in-addr.arpa

[illegible]

What site is being queried in packet 26?
www.wireshark.org

dns						
No.	Time	Source	Destination	Protocol	Length	Info
17	12.073341	192.168.43.1	192.168.43.9	DNS	116	Standard query response
24	15.289472	192.168.43.9	192.168.43.1	DNS	77	Standard query 0x2121
25	15.703377	192.168.43.1	192.168.43.9	DNS	93	Standard query response
26	15.722009	192.168.43.9	192.168.43.1	DNS	77	Standard query 0x2c58
27	15.865643	192.168.43.1	192.168.43.9	DNS	93	Standard query response

▶ Frame 26: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface en1, in 0.000000 seconds on the interface
 ▶ Ethernet II, Src: Apple_13:c5:58 (60:33:4b:13:c5:58), Dst: MS-NLB-PhysServer-26_11:f0:c2:00:00:00
 ▶ Internet Protocol Version 4, Src: 192.168.43.9, Dst: 192.168.43.1
 ▶ User Datagram Protocol, Src Port: 54627, Dst Port: 53
 ▶ Domain Name System (query)
 Transaction ID: 0x2c58
 Flags: 0x0100 Standard query
 Questions: 1
 Answer RRs: 0
 Authority RRs: 0
 Additional RRs: 0
 Queries
 ▶ www.wireshark.org: type A, class IN
 [Response In: 27]

What is the Transaction ID for packet 26?
0x2c58

dns						
No.	Time	Source	Destination	Protocol	Length	Info
17	12.073341	192.168.43.1	192.168.43.9	DNS	116	Standard
24	15.289472	192.168.43.9	192.168.43.1	DNS	77	Standard
25	15.703377	192.168.43.1	192.168.43.9	DNS	93	Standard
26	15.722009	192.168.43.9	192.168.43.1	DNS	77	Standard
27	15.865643	192.168.43.1	192.168.43.9	DNS	93	Standard

Frame 26: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface en1,
Ethernet II, Src: Apple_13:c5:58 (60:33:4b:13:c5:58), Dst: MS-NLB-PhysServer-26_11:f6
Internet Protocol Version 4, Src: 192.168.43.9, Dst: 192.168.43.1
User Datagram Protocol, Src Port: 54627, Dst Port: 53
Domain Name System (query)
Transaction ID: 0x2c58
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
www.wireshark.org: type A, class IN

HTTP Traffic

What percent of packets originate from Domain Name System?

4.7

Navigate to "Statistics" > "Protocol Hierarchy"

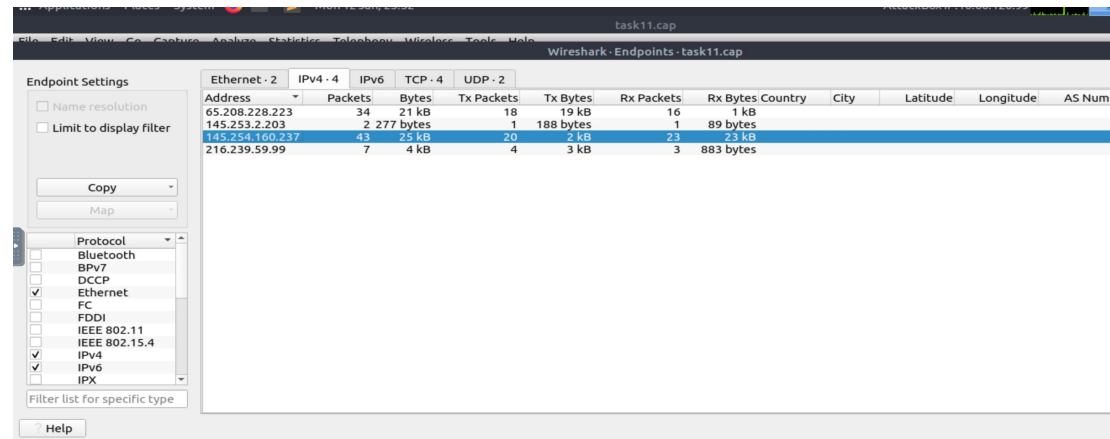
Wireshark - Protocol Hierarchy Statistics - task11.cap									
Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PD
Frame	100.0	43	100.0	25091	6,604	0	0	0	43
Ethernet	100.0	43	2.4	602	158	0	0	0	43
Internet Protocol Version 4	100.0	43	3.4	860	226	0	0	0	43
User Datagram Protocol	4.7	2	0.1	16	4	0	0	0	2
Domain Name System	4.7	2	0.8	193	50	2	193	50	2
Transmission Control Protocol	95.3	41	3.3	836	220	37	756	198	41
Hypertext Transfer Protocol	9.3	4	7.2	1812	476	2	1200	315	4
Line-based text data	2.3	1	14.4	3608	949	1	3608	949	1
eXtensible Markup Language	2.3	1	72.0	18070	4,756	1	18070	4,756	1

Frame 38: 478
Ethernet II,
Internet Prot
Transmission
[14 Reassembl
Hypertext Tra
eXtensible Ma

No display filter.

What endpoint ends in .237?
145.254.160.237

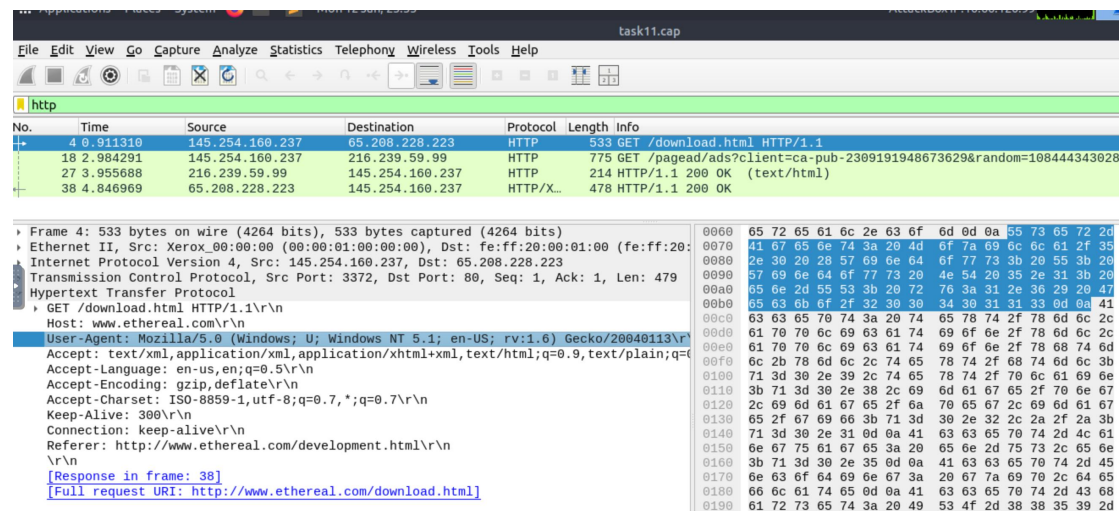
Navigate to "Statistics" > "Endpoints" > "IPv4•4



The screenshot shows the Wireshark 'Endpoints' window for 'task11.cap'. The 'IPv4 - 4' tab is selected, showing a table of endpoints. The endpoint 145.254.160.237 is highlighted in blue. The 'Endpoint Settings' panel on the left shows 'Name resolution' and 'Limit to display filter' are unchecked. The 'Protocol' list on the left has 'Ethernet', 'IPv4', and 'IPv6' checked.

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	Latitude	Longitude	AS Num
65.208.228.223	34	21 kB	18	19 kB	16	1 kB					
145.253.2.203	2	277 bytes	1	188 bytes	1	89 bytes					
145.254.160.237	43	23 kB	20	2 kB	23	23 kB					
216.239.59.99	7	4 kB	4	3 kB	3	883 bytes					

What is the user-agent listed in packet 4?
Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.6)
Gecko/20040113\r\n



The screenshot shows the details of packet 4 in Wireshark. The 'http' filter is applied. The packet list shows packet 4 with a GET request to /download.html. The packet details show the 'User-Agent' field with the value 'Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.6) Gecko/20040113\r\n'. The packet bytes pane shows the raw data of the packet.

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=1084443430285
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

Frame 4: 533 bytes on wire (4264 bits), 533 bytes captured (4264 bits)
Ethernet II, Src: Xerox_00:00:00:00:00:00, Dst: fe:ff:20:00:01:00 (fe:ff:20:00:01:00)
Internet Protocol Version 4, Src: 145.254.160.237, Dst: 65.208.228.223
Transmission Control Protocol, Src Port: 3372, Dst Port: 80, Seq: 1, Ack: 1, Len: 479
Hypertext Transfer Protocol
GET /download.html HTTP/1.1\r\nHost: www.ethereal.com\r\nUser-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.6) Gecko/20040113\r\nAccept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,application/javascript;q=0.8\r\nAccept-Encoding: gzip,deflate\r\nAccept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\nKeep-Alive: 300\r\nConnection: keep-alive\r\nReferer: http://www.ethereal.com/development.html\r\n\r\n[Response in frame: 38]
[Full request URI: http://www.ethereal.com/download.html]

Looking at the data stream what is the full request URI from packet 18?
http://pagead2.googlesyndication.com/pagead/ads?client=ca-pub-2309191948673629&random=1084443430285&lmt=1082467020&format=468x60_as&output=html&url=http%3A%2F%2Fwww.ethereal.com%2Fdownload.html&color_bg=FFFFFF&color_text=333333&color_link=000000&color_url=666633&color_border=666633

What domain name was requested from packet 38?

```
[Reassembled TCP Data [...]: 4854545027312e3120323030204740000a44b1/4653a205408/52C20
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
    Response Version: HTTP/1.1
    Status Code: 200
    [Status Code Description: OK]
    Response Phrase: OK
    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
    Keep-Alive: timeout=15, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=ISO-8859-1\r\n
    \r\n
    [Request in frame: 4]
    [Time since request: 3.935659000 seconds]
    [Request URI: /download.html]
    [Full request URI: http://www.ethereal.com/download.html]
    File Data: 18070 bytes
  Extensible Markup Language
```

Looking at the data stream what is the full request URI from packet 38?
<http://www.ethereal.com/download.htm>

HTTPS Traffic

Looking at the data stream what is the full request URI for packet 31?
https://localhost/icons/apache_pb.png

Navigate to "Edit" > "Preferences" > "Protocols" > "TLS" > RSA Keys
List [Edit] IP Address: 127.0.0.1
Port: start_tls
Protocol: http
Key File: The file location of rsasnakeoil2.key

The image shows a Wireshark packet capture of an HTTPS transaction. The packet list on the left shows packets 31 through 35. Packet 31 is a GET request for /icons/apache_pb.png. The packet details pane on the right shows the structure of the packet, including the TLS record and the HTTP request. The full request URI is highlighted as https://localhost/icons/apache_pb.png.

```
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
31 2.993840 127.0.0.1 127.0.0.1 HTTP 471 GET /icons/apache_pb.png
32 2.994179 127.0.0.1 127.0.0.1 HTTP 1828 HTTP/1.1 200 OK (PNG)
33 3.004256 127.0.0.1 127.0.0.1 TCP 66 443 -> 38713 [ACK] Seq=78
34 3.033250 127.0.0.1 127.0.0.1 TCP 66 38714 -> 443 [ACK] Seq=10
35 3.501643 127.0.0.1 127.0.0.1 HTTP 588 HTTP/1.1 404 Not Found
4
  [Timestamps]
  [SEQ/ACK analysis]
  TCP payload (405 bytes)
  Transport Layer Security
    SSLv3 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
      Content Type: Application Data (23)
      Version: SSL 3.0 (0x0300)
      Length: 400
      Encrypted Application Data [...]: f946d967cbab62eefc408452b6d37fa68f0531f64566b017e
      [Application Data Protocol: Hypertext Transfer Protocol]
    Hypertext Transfer Protocol
      GET /icons/apache_pb.png HTTP/1.1\r\n
      Host: localhost\r\n
      User-Agent: Mozilla/5.0 (X11; U; Linux i686; fr; rv:1.8.0.2) Gecko/20060308 Firefox
      Accept: image/png,*/*;q=0.5\r\n
      Accept-Language: fr,fr-fr;q=0.8,en-us;q=0.5,en;q=0.3\r\n
      Accept-Encoding: gzip,deflate\r\n
      Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
      Keep-Alive: 300\r\n
      Connection: keep-alive\r\n
      Referer: https://localhost/\r\n
      \r\n
      [Response in frame: 32]
      [Full request URI: https://localhost/icons/apache_pb.png]
```

Looking at the data stream what is the full request URI for packet 50?
https://localhost/icons/back.gif

What is the User-Agent listed in packet 50?
Mozilla/5.0 (X11; U; Linux i686; fr; rv:1.8.0.2) Gecko/20060308
Firefox/1.5.0.2\r\n

No.	Time	Source	Destination	Protocol	Length	Info
47	9.232586	127.0.0.1	127.0.0.1	HTTP	511	GET /test2/ HTTP/1.1
48	9.235911	127.0.0.1	127.0.0.1	HTTP	836	HTTP/1.1 200 OK (text/h
49	9.245287	127.0.0.1	127.0.0.1	TCP	66	38713 → 443 [ACK] Seq=24
50	9.318572	127.0.0.1	127.0.0.1	HTTP	479	GET /icons/back.gif HTTP
51	9.323495	127.0.0.1	127.0.0.1	HTTP	479	GET /icons/blank.gif HT

[Timestamps]

[SEQ/ACK analysis]

TCP payload (413 bytes)

Transport Layer Security

SSLv3 Record Layer: Application Data Protocol: Hypertext Transfer Protocol

Content Type: Application Data (23)

Version: SSL 3.0 (0x0300)

Length: 408

Encrypted Application Data [...]: 842f81ccd99765c1ac2ac1b6ce9250d339bc7454c8a623fc5

[Application Data Protocol: Hypertext Transfer Protocol]

Hypertext Transfer Protocol

GET /icons/back.gif HTTP/1.1\r\n

Host: localhost\r\n

User-Agent: Mozilla/5.0 (X11; U; Linux i686; fr; rv:1.8.0.2) Gecko/20060308 Firefox

Accept: image/png, */*;q=0.5\r\n

Accept-Language: fr, fr-fr;q=0.8, en-us;q=0.5, en;q=0.3\r\n

Accept-Encoding: gzip, deflate\r\n

Accept-Charset: ISO-8859-1, utf-8;q=0.7, *;q=0.7\r\n

Keep-Alive: 300\r\n

Connection: keep-alive\r\n

Referer: https://localhost/test2/\r\n

\r\n

[Response in frame: 52]

[Full request URI: https://localhost/icons/back.gif]

0000 47 45 5

0010 67 69 6

0020 73 74 3

0030 73 65 7

0040 6c 61 2

0050 4c 69 6

0060 72 76 3

0070 6f 2f 3

0080 6f 78 2

0090 70 74 3

00a0 2a 3b 7

00b0 4c 61 6

00c0 66 72 3

00d0 3d 30 2

00e0 63 63 6

00f0 67 7a 6

0100 63 65 7

0110 4f 2d 3

0120 3d 30 2

0130 65 70 2

0140 6f 6e 6

0150 61 6c 6

0160 68 74 7

0170 74 2f 7

Frame (479 bytes)