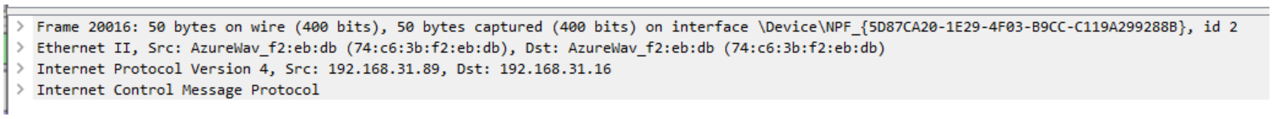
Cyber Security Essentials

Lab 5 - Wireshark Fundamentals

1. Open the given evidence.pcap file. Use display filter to identify only the traffic which are related to PING. (HINT – ICMP). After filtering the respective traffic answer the following questions.

a. What is the frame number of 1st packet (Ping Request)?

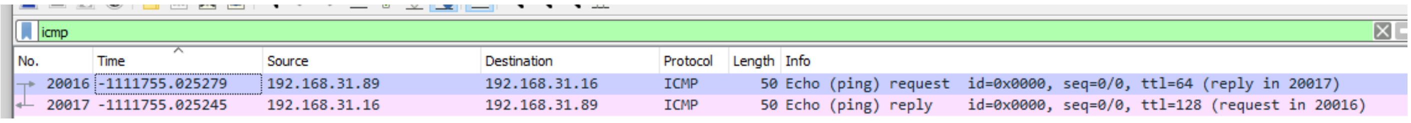
Frame number: 20016



```
> Frame 20016: 50 bytes on wire (400 bits), 50 bytes captured (400 bits) on interface \Device\NPF_{5D87CA20-1E29-4F03-B9CC-C119A299288B}, id 2
> Ethernet II, Src: AzureWav_f2:eb:db (74:c6:3b:f2:eb:db), Dst: AzureWav_f2:eb:db (74:c6:3b:f2:eb:db)
> Internet Protocol Version 4, Src: 192.168.31.89, Dst: 192.168.31.16
> Internet Control Message Protocol
```

b. How many packets are available with applied filter?

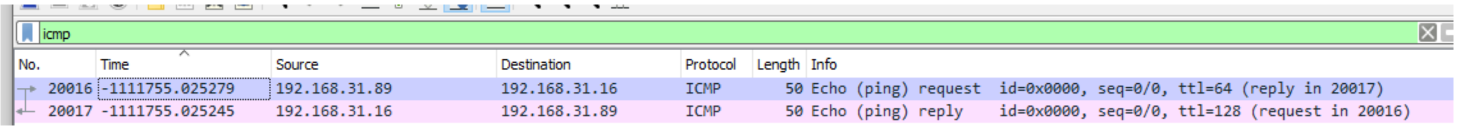
2 packets are available after the filter is applied.



```
icmp
No.    Time             Source          Destination     Protocol  Length  Info
20016  -1111755.025279  192.168.31.89   192.168.31.16   ICMP      50      Echo (ping) request  id=0x0000, seq=0/0, ttl=64 (reply in 20017)
20017  -1111755.025245  192.168.31.16   192.168.31.89   ICMP      50      Echo (ping) reply    id=0x0000, seq=0/0, ttl=128 (request in 20016)
```

c. What is the source and destination IP address of the 1st packet (ping Request)?

Source Address: 192.168.31.89
Destination Address: 192.168.31.16



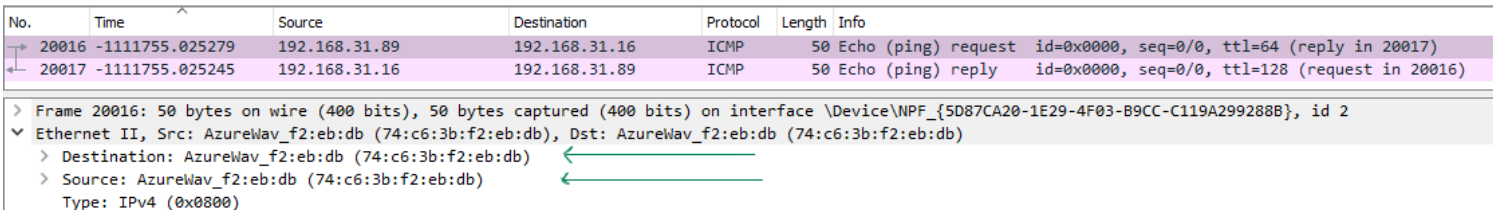
```
icmp
No.    Time             Source          Destination     Protocol  Length  Info
20016  -1111755.025279  192.168.31.89   192.168.31.16   ICMP      50      Echo (ping) request  id=0x0000, seq=0/0, ttl=64 (reply in 20017)
20017  -1111755.025245  192.168.31.16   192.168.31.89   ICMP      50      Echo (ping) reply    id=0x0000, seq=0/0, ttl=128 (request in 20016)
```

d. What is the data size (in Bytes)?

Data size is 50 bytes.

e. What is the source and destination MAC address?

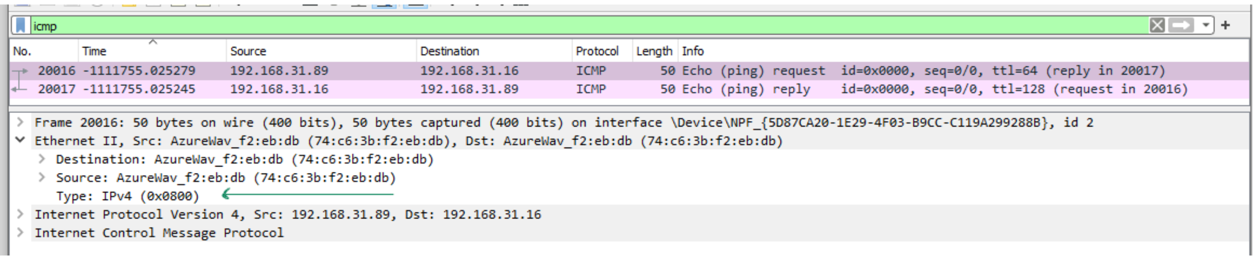
Destination: AzureWav_f2:eb:db (74:c6:3b:f2:eb:db)
Source: AzureWav_f2:eb:db (74:c6:3b:f2:eb:db)



```
No.    Time              Source          Destination     Protocol  Length  Info
20016 -1111755.025279   192.168.31.89   192.168.31.16   ICMP        50 Echo (ping) request  id=0x0000, seq=0/0, ttl=64 (reply in 20017)
20017 -1111755.025245   192.168.31.16   192.168.31.89   ICMP        50 Echo (ping) reply    id=0x0000, seq=0/0, ttl=128 (request in 20016)

> Frame 20016: 50 bytes on wire (400 bits), 50 bytes captured (400 bits) on interface \Device\NPF_{5D87CA20-1E29-4F03-B9CC-C119A299288B}, id 2
v Ethernet II, Src: AzureWav_f2:eb:db (74:c6:3b:f2:eb:db), Dst: AzureWav_f2:eb:db (74:c6:3b:f2:eb:db)
  > Destination: AzureWav_f2:eb:db (74:c6:3b:f2:eb:db)
  > Source: AzureWav_f2:eb:db (74:c6:3b:f2:eb:db)
    Type: IPv4 (0x0800)
```

f. Which version of IP is been used here : IPV4 or IPV6?

IPV4 is used here.

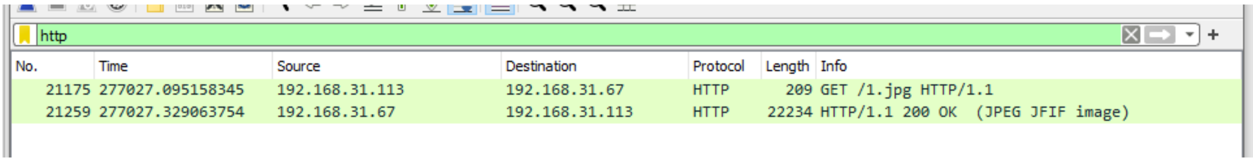


```
icmp
No.    Time              Source          Destination     Protocol  Length  Info
20016 -1111755.025279   192.168.31.89   192.168.31.16   ICMP        50 Echo (ping) request  id=0x0000, seq=0/0, ttl=64 (reply in 20017)
20017 -1111755.025245   192.168.31.16   192.168.31.89   ICMP        50 Echo (ping) reply    id=0x0000, seq=0/0, ttl=128 (request in 20016)

> Frame 20016: 50 bytes on wire (400 bits), 50 bytes captured (400 bits) on interface \Device\NPF_{5D87CA20-1E29-4F03-B9CC-C119A299288B}, id 2
v Ethernet II, Src: AzureWav_f2:eb:db (74:c6:3b:f2:eb:db), Dst: AzureWav_f2:eb:db (74:c6:3b:f2:eb:db)
  > Destination: AzureWav_f2:eb:db (74:c6:3b:f2:eb:db)
  > Source: AzureWav_f2:eb:db (74:c6:3b:f2:eb:db)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.31.89, Dst: 192.168.31.16
> Internet Control Message Protocol
```

2. Here is some unencrypted web traffic has been captured. Use the appropriate filter to identify that traffic. After filtering the traffic answer the following questions.

a. How many packets are found after filtering using required filter?

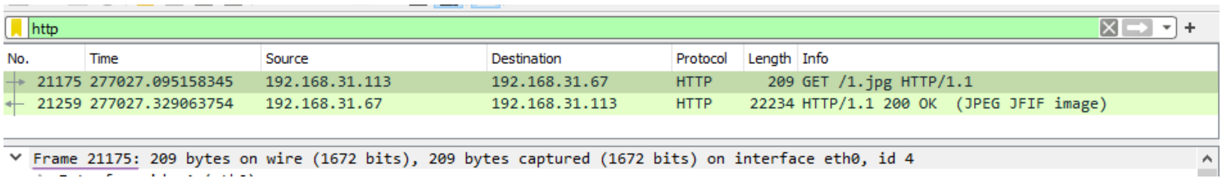
2 packets are found after filter is applied.



```
http
No.     Time                Source           Destination      Protocol  Length  Info
  21175 277027.095158345    192.168.31.113   192.168.31.67    HTTP         209  GET /1.jpg HTTP/1.1
  21259 277027.329063754    192.168.31.67    192.168.31.113   HTTP       22234  HTTP/1.1 200 OK  (JPEG JFIF image)
```

b. What is the frame number of 1st packet?

Frame number: 21175

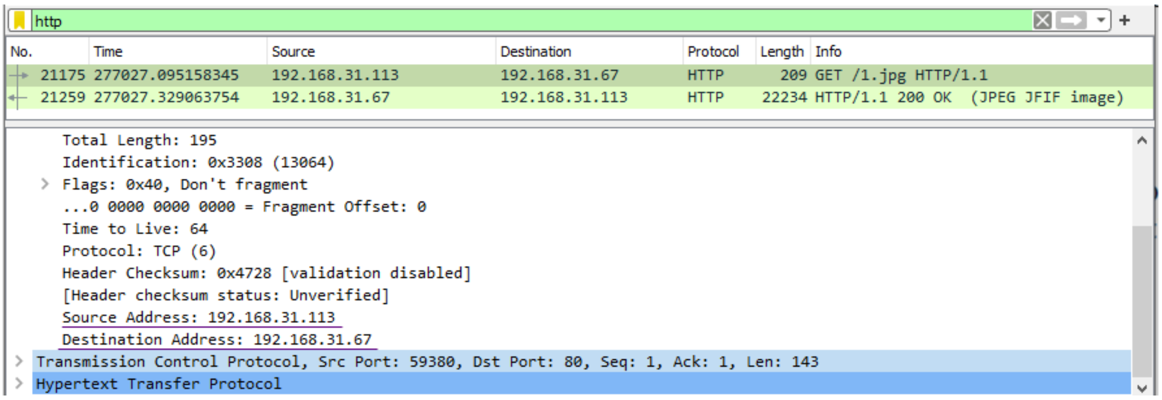


```
http
No.     Time                Source           Destination      Protocol  Length  Info
  21175 277027.095158345    192.168.31.113   192.168.31.67    HTTP         209  GET /1.jpg HTTP/1.1
  21259 277027.329063754    192.168.31.67    192.168.31.113   HTTP       22234  HTTP/1.1 200 OK  (JPEG JFIF image)

Frame 21175: 209 bytes on wire (1672 bits), 209 bytes captured (1672 bits) on interface eth0, id 4
```

c. What is the source and destination IP address?

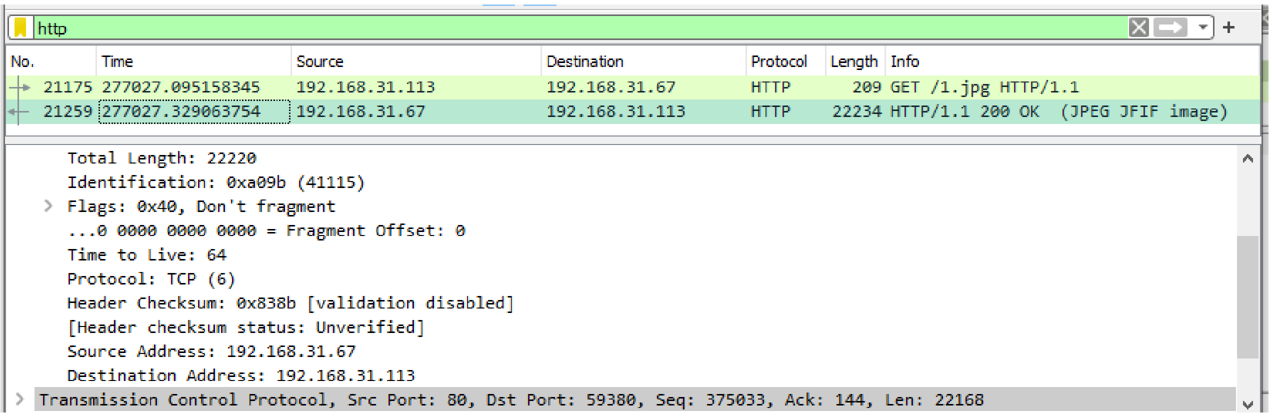
Source Address: 192.168.31.113
Destination Address: 192.168.31.67

Request packet:



```
http
No.    Time              Source          Destination     Protocol  Length  Info
21175  277027.095158345  192.168.31.113  192.168.31.67   HTTP         209  GET /1.jpg HTTP/1.1
21259  277027.329063754  192.168.31.67   192.168.31.113  HTTP       22234  HTTP/1.1 200 OK  (JPEG JFIF image)

      Total Length: 195
      Identification: 0x3308 (13064)
    > Flags: 0x40, Don't fragment
      ...0 0000 0000 0000 = Fragment Offset: 0
      Time to Live: 64
      Protocol: TCP (6)
      Header Checksum: 0x4728 [validation disabled]
      [Header checksum status: Unverified]
      Source Address: 192.168.31.113
      Destination Address: 192.168.31.67
  > Transmission Control Protocol, Src Port: 59380, Dst Port: 80, Seq: 1, Ack: 1, Len: 143
  > Hypertext Transfer Protocol
```

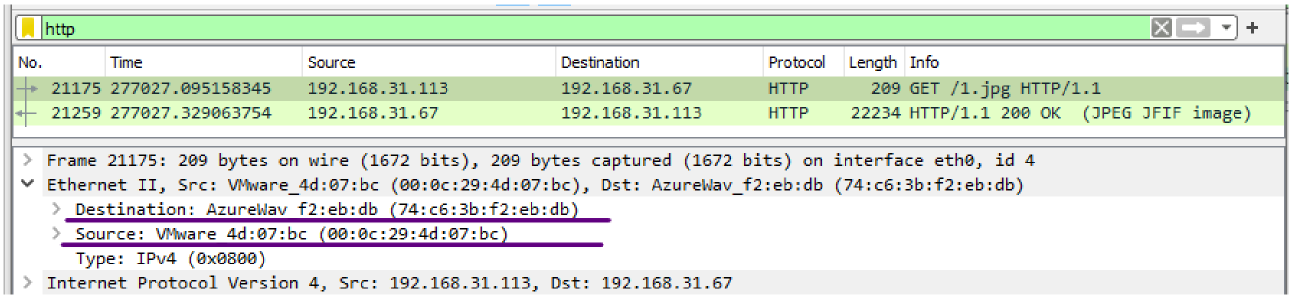
Response packet:



```
http
No.    Time              Source          Destination     Protocol  Length  Info
21175  277027.095158345  192.168.31.113  192.168.31.67   HTTP         209  GET /1.jpg HTTP/1.1
21259  277027.329063754  192.168.31.67   192.168.31.113  HTTP       22234  HTTP/1.1 200 OK  (JPEG JFIF image)

      Total Length: 22220
      Identification: 0xa09b (41115)
    > Flags: 0x40, Don't fragment
      ...0 0000 0000 0000 = Fragment Offset: 0
      Time to Live: 64
      Protocol: TCP (6)
      Header Checksum: 0x838b [validation disabled]
      [Header checksum status: Unverified]
      Source Address: 192.168.31.67
      Destination Address: 192.168.31.113
  > Transmission Control Protocol, Src Port: 80, Dst Port: 59380, Seq: 375033, Ack: 144, Len: 22168
```

d. What is the source and destination MAC address?

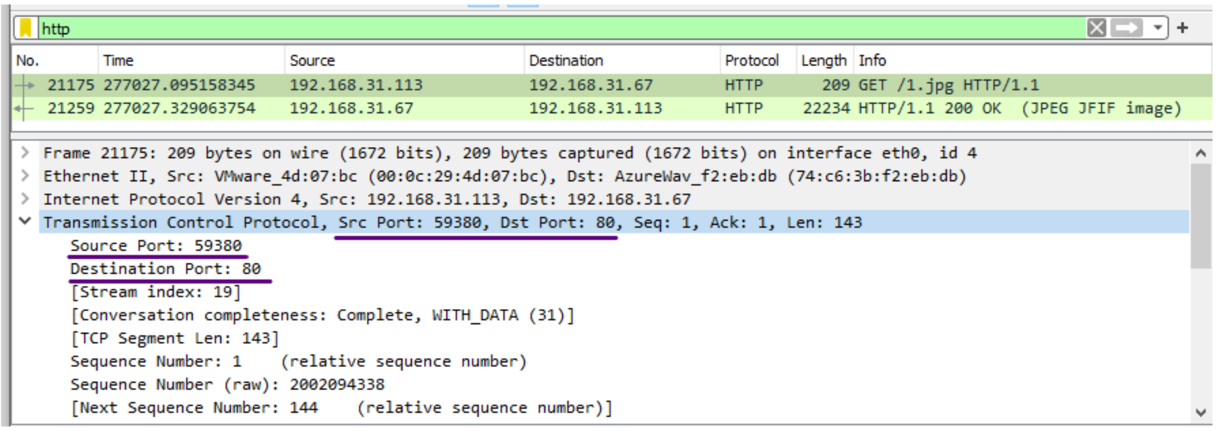
Destination: AzureWav_f2:eb:db (74:c6:3b:f2:eb:db)
Source: VMware_4d:07:bc (00:0c:29:4d:07:bc)



```
http
No.    Time              Source          Destination     Protocol  Length  Info
21175  277027.095158345  192.168.31.113  192.168.31.67   HTTP         209  GET /1.jpg HTTP/1.1
21259  277027.329063754  192.168.31.67   192.168.31.113  HTTP       22234  HTTP/1.1 200 OK  (JPEG JFIF image)

> Frame 21175: 209 bytes on wire (1672 bits), 209 bytes captured (1672 bits) on interface eth0, id 4
v Ethernet II, Src: VMware_4d:07:bc (00:0c:29:4d:07:bc), Dst: AzureWav_f2:eb:db (74:c6:3b:f2:eb:db)
  > Destination: AzureWav_f2:eb:db (74:c6:3b:f2:eb:db)
  > Source: VMware_4d:07:bc (00:0c:29:4d:07:bc)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.31.113, Dst: 192.168.31.67
```

e. What is the source and destination port numbers?

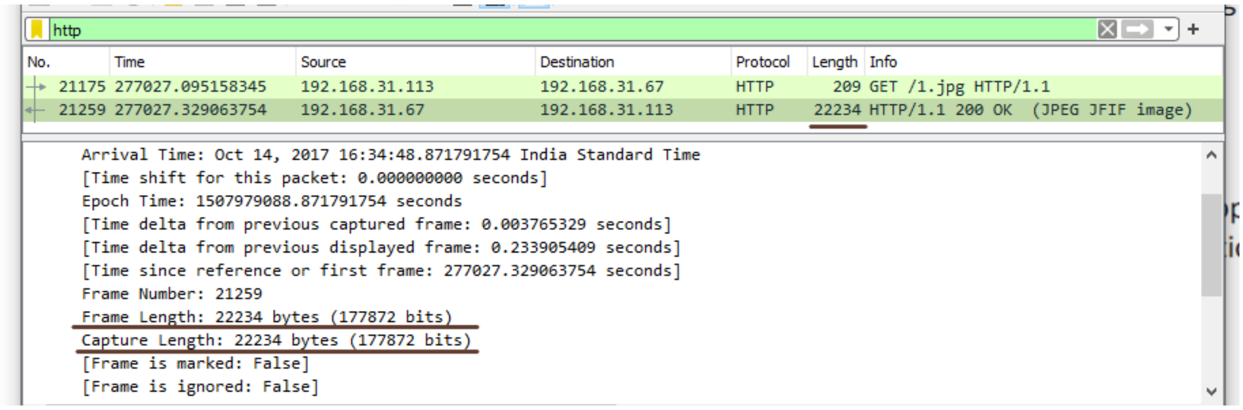
Source Port: 59380
Destination Port: 80



```
http
No.    Time                 Source           Destination      Protocol  Length  Info
21175  277027.095158345     192.168.31.113   192.168.31.67    HTTP         209  GET /1.jpg HTTP/1.1
21259  277027.329063754     192.168.31.67    192.168.31.113   HTTP       22234  HTTP/1.1 200 OK  (JPEG JFIF image)

> Frame 21175: 209 bytes on wire (1672 bits), 209 bytes captured (1672 bits) on interface eth0, id 4
> Ethernet II, Src: VMware_4d:07:bc (00:0c:29:4d:07:bc), Dst: AzureWav_f2:eb:db (74:c6:3b:f2:eb:db)
> Internet Protocol Version 4, Src: 192.168.31.113, Dst: 192.168.31.67
v Transmission Control Protocol, Src Port: 59380, Dst Port: 80, Seq: 1, Ack: 1, Len: 143
    Source Port: 59380
    Destination Port: 80
    [Stream index: 19]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 143]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 2002094338
    [Next Sequence Number: 144    (relative sequence number)]
```

f. What is the length of the response packet?

Length of response packet is 22234.



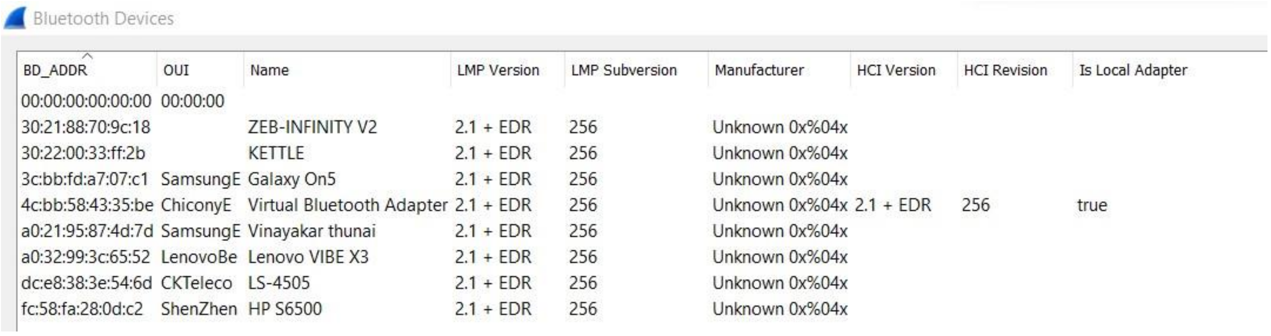
```
http
No.    Time                 Source           Destination      Protocol  Length  Info
21175  277027.095158345     192.168.31.113   192.168.31.67    HTTP         209  GET /1.jpg HTTP/1.1
21259  277027.329063754     192.168.31.67    192.168.31.113   HTTP       22234  HTTP/1.1 200 OK  (JPEG JFIF image)

    Arrival Time: Oct 14, 2017 16:34:48.871791754 India Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1507979088.871791754 seconds
    [Time delta from previous captured frame: 0.003765329 seconds]
    [Time delta from previous displayed frame: 0.233905409 seconds]
    [Time since reference or first frame: 277027.329063754 seconds]
    Frame Number: 21259
    Frame Length: 22234 bytes (177872 bits)
    Capture Length: 22234 bytes (177872 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
```

g. What is the name of the file which is downloaded from that webpage?

1.jpg is the name of the file which is downloaded.

3. Find the number of Bluetooth devices captured?

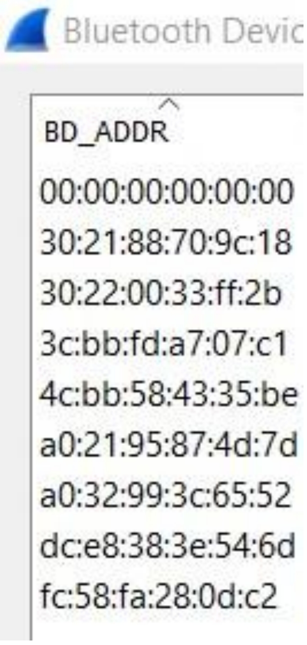
8 devices are captured.



Bluetooth Devices

BD_ADDR	OUI	Name	LMP Version	LMP Subversion	Manufacturer	HCI Version	HCI Revision	Is Local Adapter
00:00:00:00:00:00	00:00:00							
30:21:88:70:9c:18		ZEB-INFINITY V2	2.1 + EDR	256	Unknown 0x%04x			
30:22:00:33:ff:2b		KETTLE	2.1 + EDR	256	Unknown 0x%04x			
3c:bb:fd:a7:07:c1	SamsungE	Galaxy On5	2.1 + EDR	256	Unknown 0x%04x			
4c:bb:58:43:35:be	ChiconyE	Virtual Bluetooth Adapter	2.1 + EDR	256	Unknown 0x%04x	2.1 + EDR	256	true
a0:21:95:87:4d:7d	SamsungE	Vinayakar thunai	2.1 + EDR	256	Unknown 0x%04x			
a0:32:99:3c:65:52	LenovoBe	Lenovo VIBE X3	2.1 + EDR	256	Unknown 0x%04x			
dc:e8:38:3e:54:6d	CKTeleco	LS-4505	2.1 + EDR	256	Unknown 0x%04x			
fc:58:fa:28:0d:c2	ShenZhen	HP S6500	2.1 + EDR	256	Unknown 0x%04x			

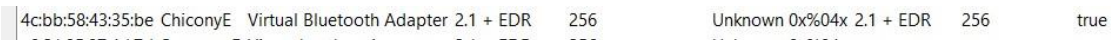
a. List the MAC address of all Bluetooth devices.



Bluetooth Devic

BD_ADDR
00:00:00:00:00:00
30:21:88:70:9c:18
30:22:00:33:ff:2b
3c:bb:fd:a7:07:c1
4c:bb:58:43:35:be
a0:21:95:87:4d:7d
a0:32:99:3c:65:52
dc:e8:38:3e:54:6d
fc:58:fa:28:0d:c2

b. Find the name of Local Bluetooth adapter.

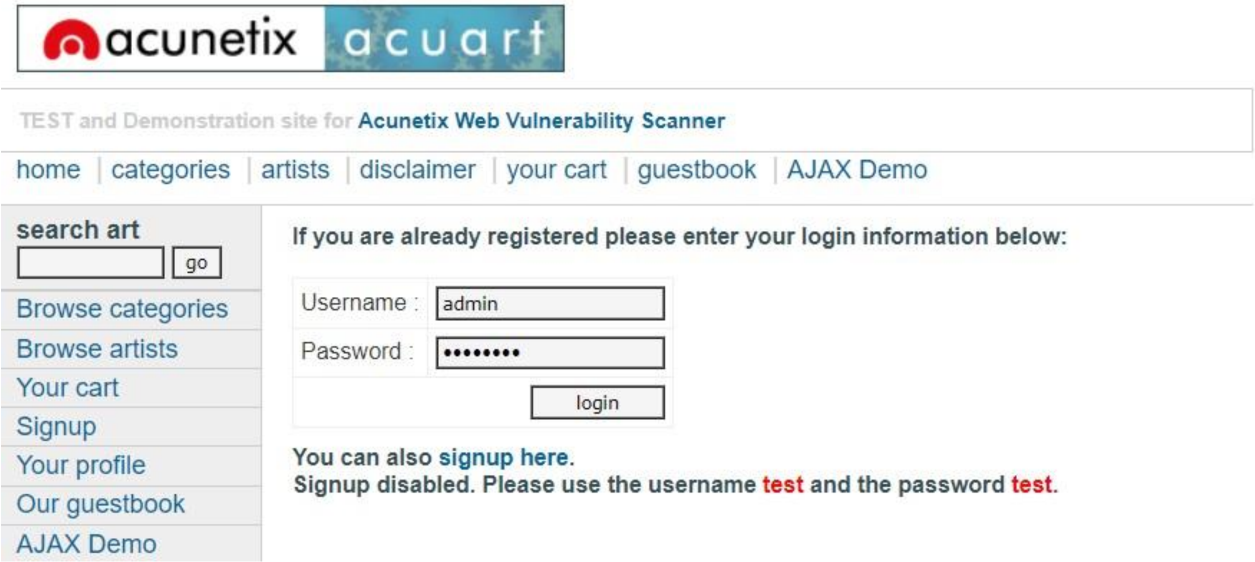


4c:bb:58:43:35:be	ChiconyE	Virtual Bluetooth Adapter	2.1 + EDR	256	Unknown 0x%04x	2.1 + EDR	256	true

c. Apply the respective display filter to find out how many packets related to Bluetooth are captured in this evidence.pcap file.

1152 are the number of Bluetooth devices captured.

4. Capture live traffic using Wireshark on your own network interface with capture filter as “tcp port http”. Then visit this page http://testphp.vulnweb.com/login.php in your browser with Wireshark running in background. Enter any random username and password in that login page. Then stop the capture in Wireshark. Analyse the packets captured to find the username and password that you have entered in the website



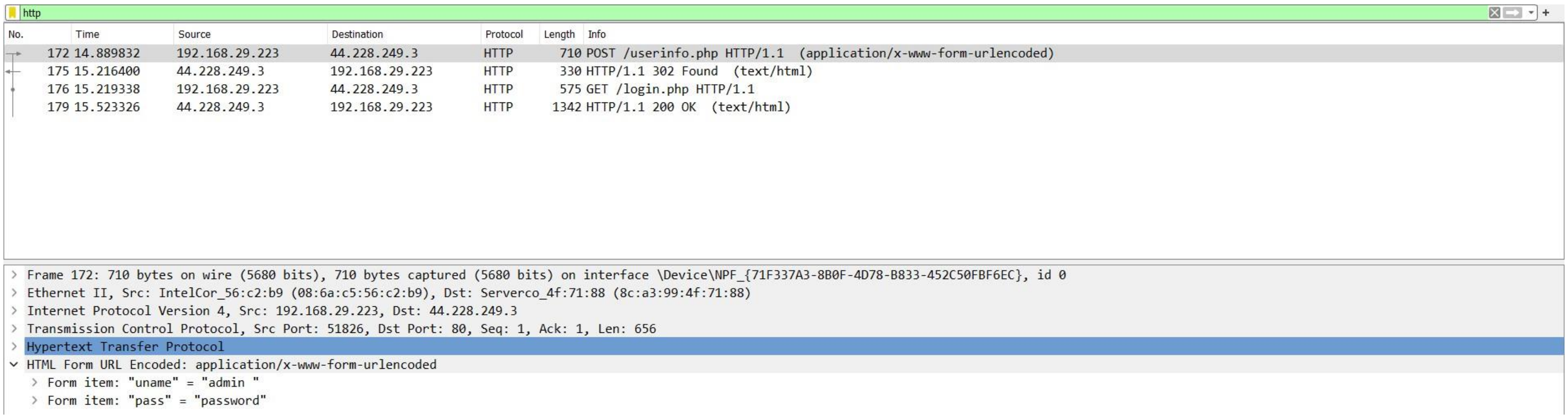
TEST and Demonstration site for Acunetix Web Vulnerability Scanner

If you are already registered please enter your login information below:

Username : admin

Password : •••••••••

You can also signup here.
Signup disabled. Please use the username test and the password test.



```
http

No.     Time        Source           Destination      Protocol  Length  Info
  172 14.889832   192.168.29.223   44.228.249.3     HTTP       710 POST /userinfo.php HTTP/1.1  (application/x-www-form-urlencoded)
  175 15.216400   44.228.249.3     192.168.29.223   HTTP       330 HTTP/1.1 302 Found  (text/html)
  176 15.219338   192.168.29.223   44.228.249.3     HTTP       575 GET /login.php HTTP/1.1
  179 15.523326   44.228.249.3     192.168.29.223   HTTP      1342 HTTP/1.1 200 OK  (text/html)
```

```
> Frame 172: 710 bytes on wire (5680 bits), 710 bytes captured (5680 bits) on interface \Device\NPF_{71F337A3-8B0F-4D78-B833-452C50FBF6EC}, id 0
> Ethernet II, Src: IntelCor_56:c2:b9 (08:6a:c5:56:c2:b9), Dst: Serverco_4f:71:88 (8c:a3:99:4f:71:88)
> Internet Protocol Version 4, Src: 192.168.29.223, Dst: 44.228.249.3
> Transmission Control Protocol, Src Port: 51826, Dst Port: 80, Seq: 1, Ack: 1, Len: 656
> Hypertext Transfer Protocol
v HTML Form URL Encoded: application/x-www-form-urlencoded
   > Form item: "uname" = "admin "
   > Form item: "pass" = "password"
```