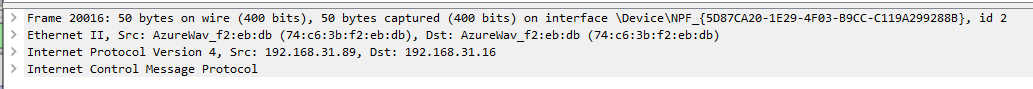
Cyber Security Essentials

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.

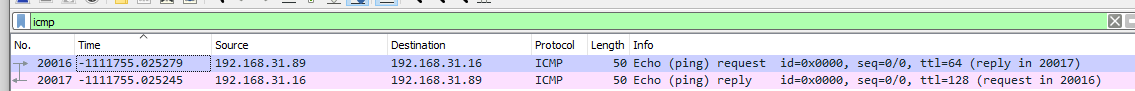
a. What is the frame number of 1st packet (Ping Request)?

Frame number: 20016



b. How many packets are available with applied filter?

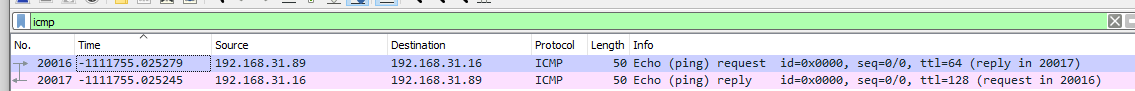
2 packets are available after the filter is applied.



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



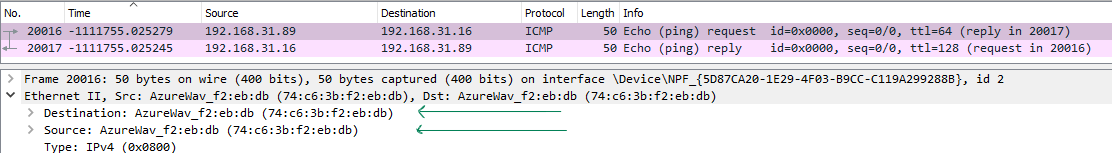
d. What is the data size (in Bytes)?

Data size is 50 bytes.

e. What is the source and destination MAC address?

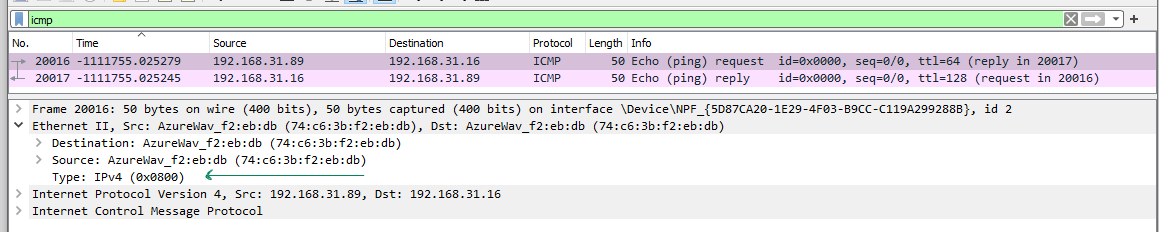
Destination: AzureWav\_f2:eb:db (74:c6:3b:f2:eb:db)

Source: AzureWav\_f2:eb:db (74:c6:3b:f2:eb:db)



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

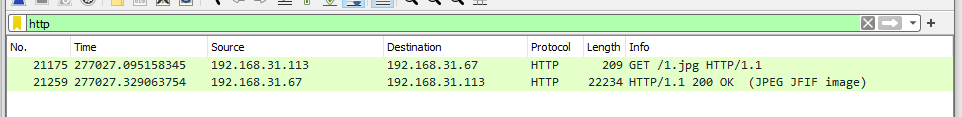
IPV4 is used here.



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.

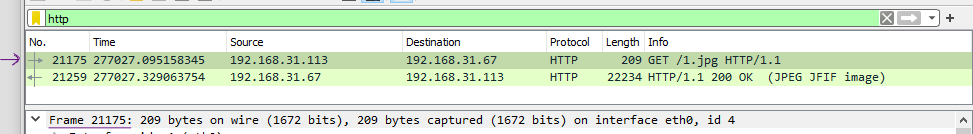
a. How many packets are found after filtering using required filter?

2 packets are found after filter is applied.



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

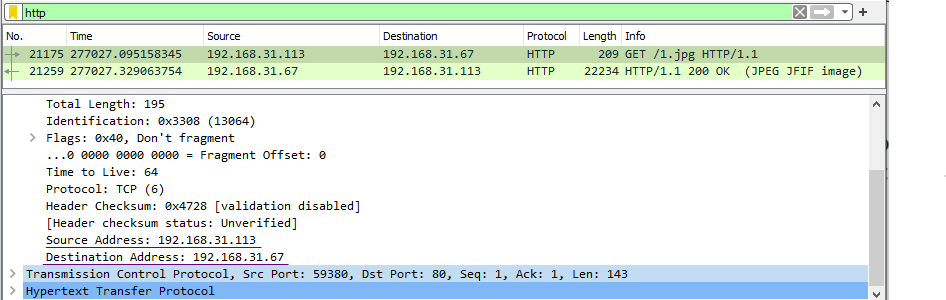
Frame number: 21175

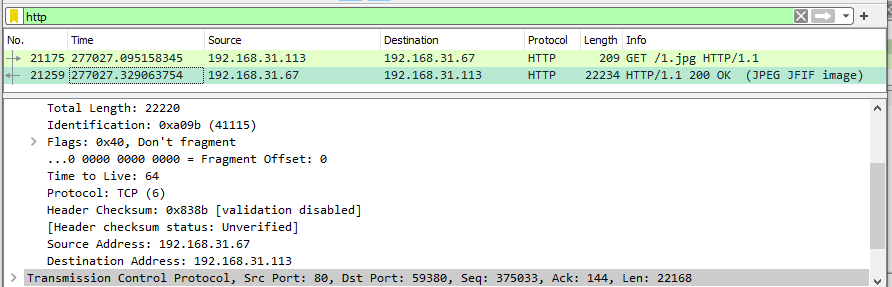


c. What is the source and destination IP address?

Source Address: 192.168.31.113

Destination Address: 192.168.31.67

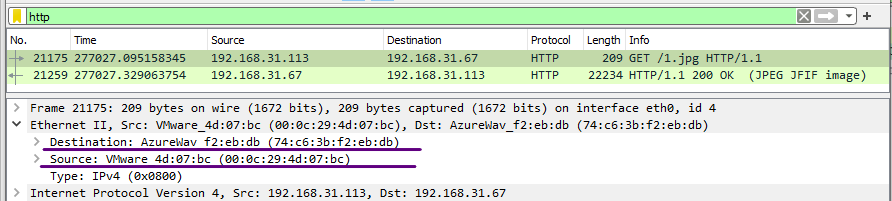
Request packet:

Response packet:

d. What is the source and destination MAC address?

Destination: AzureWav\_f2:eb:db (74:c6:3b:f2:eb:db)

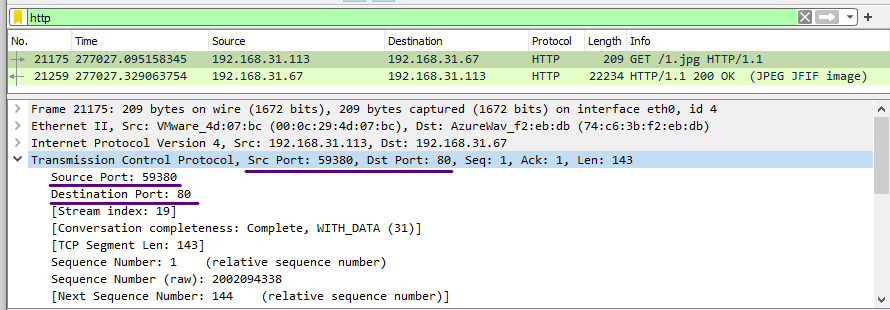
Source: VMware\_4d:07:bc (00:0c:29:4d:07:bc)



e. What is the source and destination port numbers?

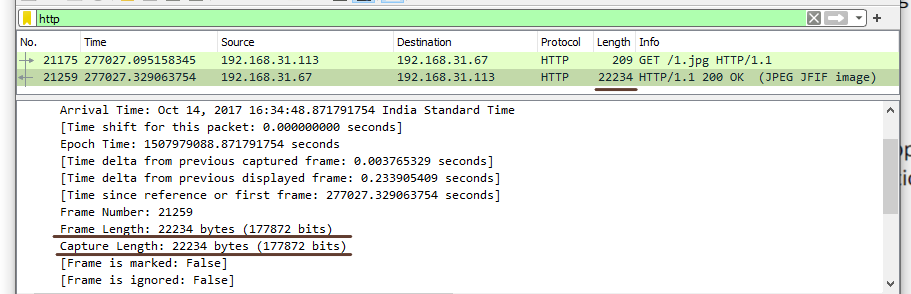
Source Port: 59380

Destination Port: 80



f. What is the length of the response packet?

Length of response packet is 22234.

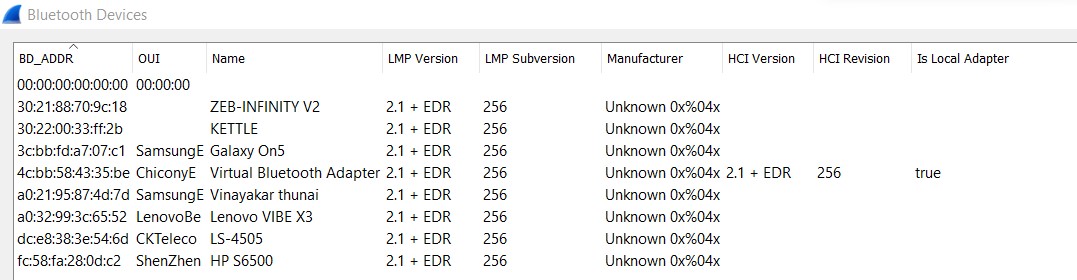


g. What is the name of the file which is downloaded from that webpage?

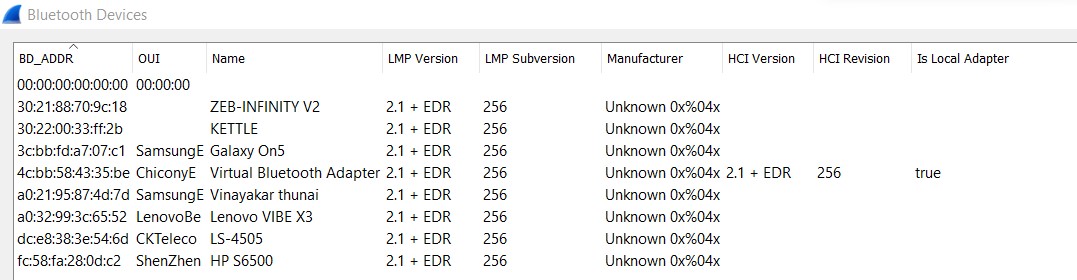
1.jpg is the name of the file which is downloaded.

3. Find the number of Bluetooth devices captured?

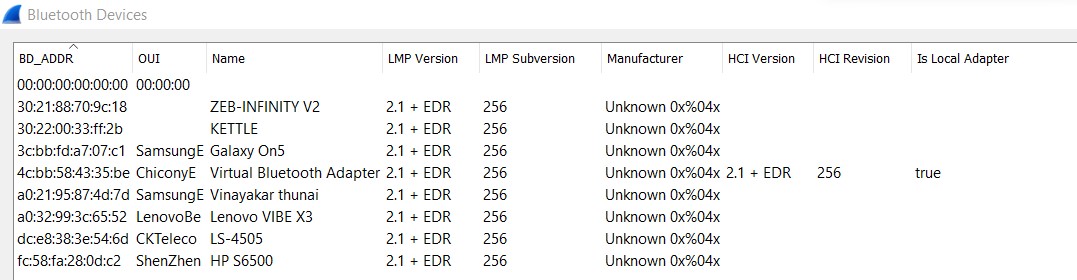
8 devices are captured.



a. List the MAC address of all Bluetooth devices.



b. Find the name of Local Bluetooth adapter.



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

