Experiment No:3

Aim: Use Wireshark to understand the operation of TCP/IP layers :

- Ethernet Layer : Frame header, Frame size etc.
- Data Link Layer : MAC address, ARP (IP and MAC address binding)
- Network Layer : IP Packet (header, fragmentation), ICMP (Query and Echo)
- Transport Layer: TCP Ports, TCP handshake segments etc.
- Application Layer: DHCP, FTP, HTTP header formats

Theory:

Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Wireshark is very similar to tcpdump, but has a graphical front-end, plus some integrated sorting and filtering options.

Wireshark allows the user to put the network interfaces that support promiscuous mode into that mode, in order to see all traffic visible on that interface, not just traffic addressed to one of the interface's configured addresses and broadcast/multicast traffic. However, when capturing with a packet analyzer in promiscuous mode on a port on a network switch, not all of the traffic traveling through the switch will necessarily be sent to the port on which the capture is being done, so capturing in promiscuous mode will not necessarily be sufficient to see all traffic on the network. Port mirroring or various network taps extend capture to any point on net; simple passive taps are extremely resistant to malware tampering.

Wireshark Installation steps:

1. Enter admin mode by following command. If not entered in admin mode then packets will not get captured in wireshark.
   sudo su

2. Command to install wireshark on ubuntu

sudo apt-get install wireshark

3. Double click on the wireshark icon. We get an open window as given below.

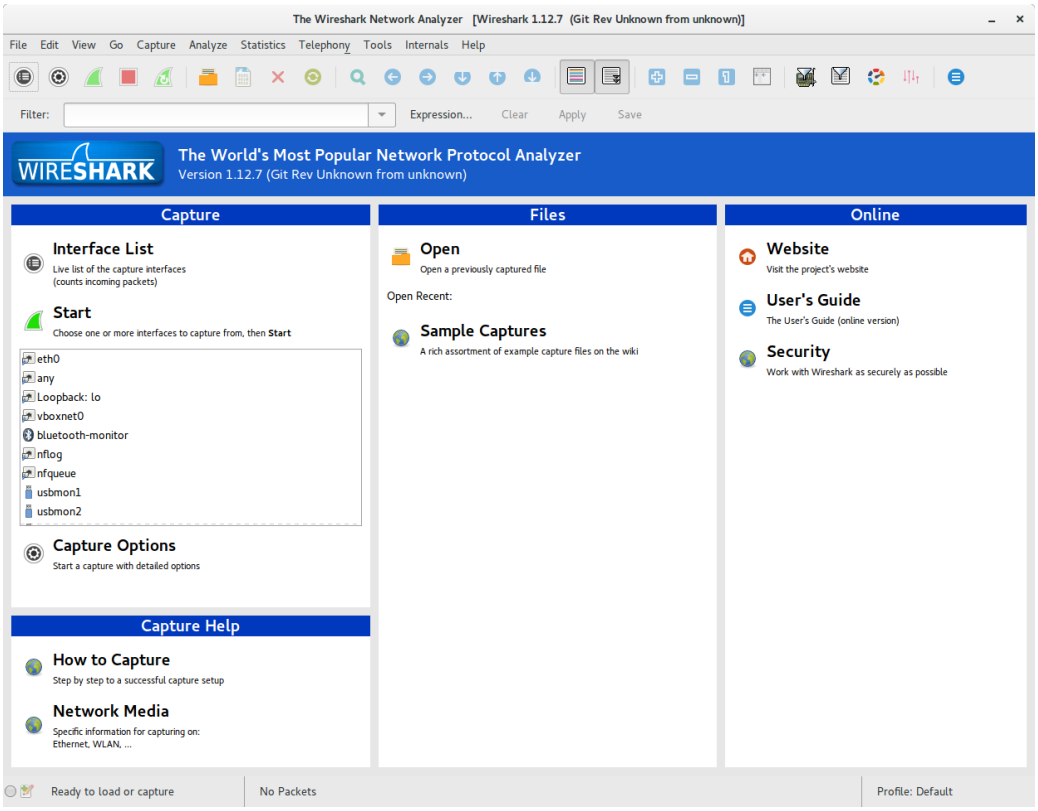


Figure 1.1: Wireshark initial showing interfaces (sudo mode)

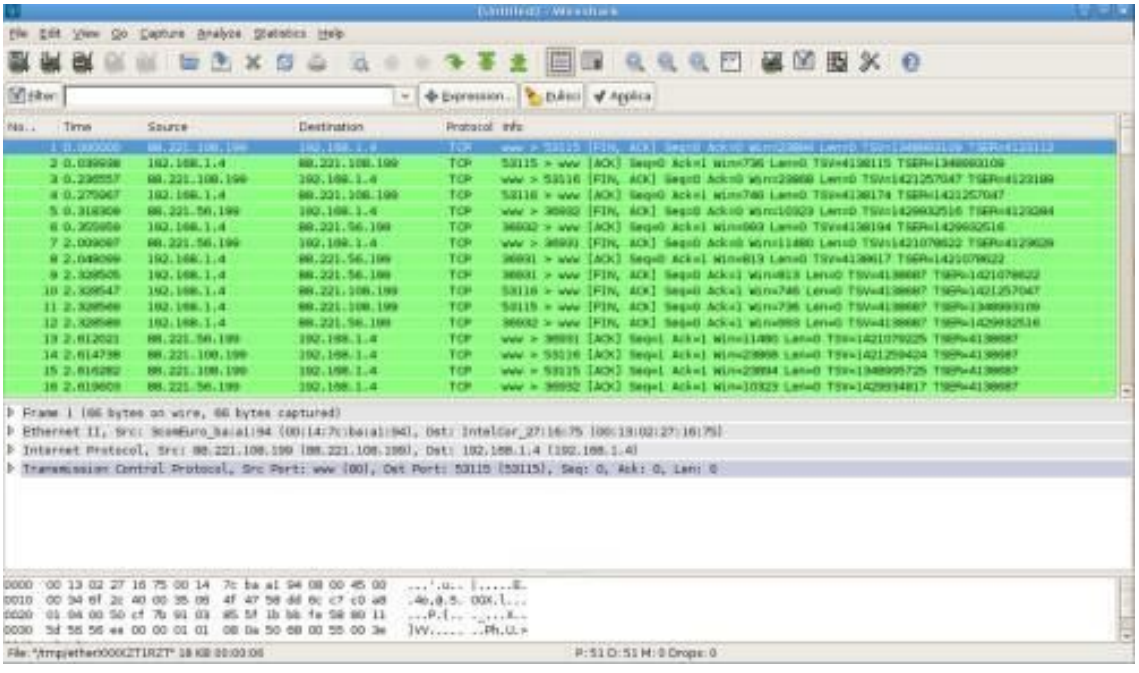


Figure 1.2. An example of a Wireshark capture.

Frame 4: 122 bytes on wire (976 bits), 122 bytes captured (976 bits)
Arrival Time: Jul 17, 2008 03:50:25.136434000 Eastern Daylight Time
Epoch Time: 1216281025.136434000 seconds
[Time delta from previous captured frame: 0.000188000 seconds]
[Time delta from previous displayed frame: 0.000188000 seconds]
[Time since reference or first frame: 0.000265000 seconds]
Frame Number: 4
Frame Length: 122 bytes (976 bits)
Capture Length: 122 bytes (976 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ip:tcp:mysql]
[Coloring Rule Name: TCP]
[Coloring Rule String: tcp]

Figure 2. The summary before the protocols in a Wireshark packet. Information about the packet characteristic.

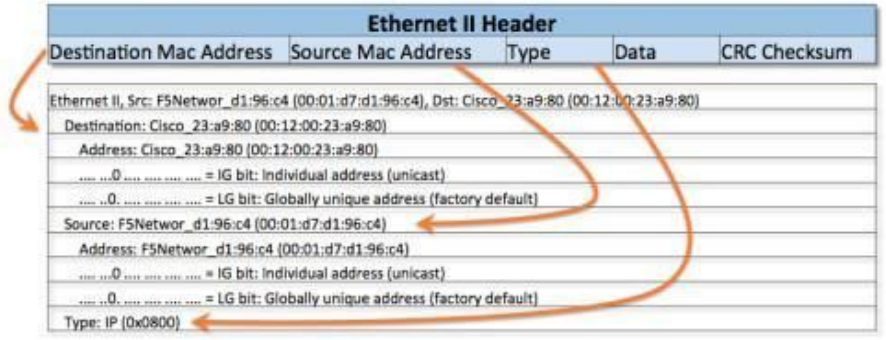


Figure 3. Ethernet II (Layer 2) header along with the Wireshark

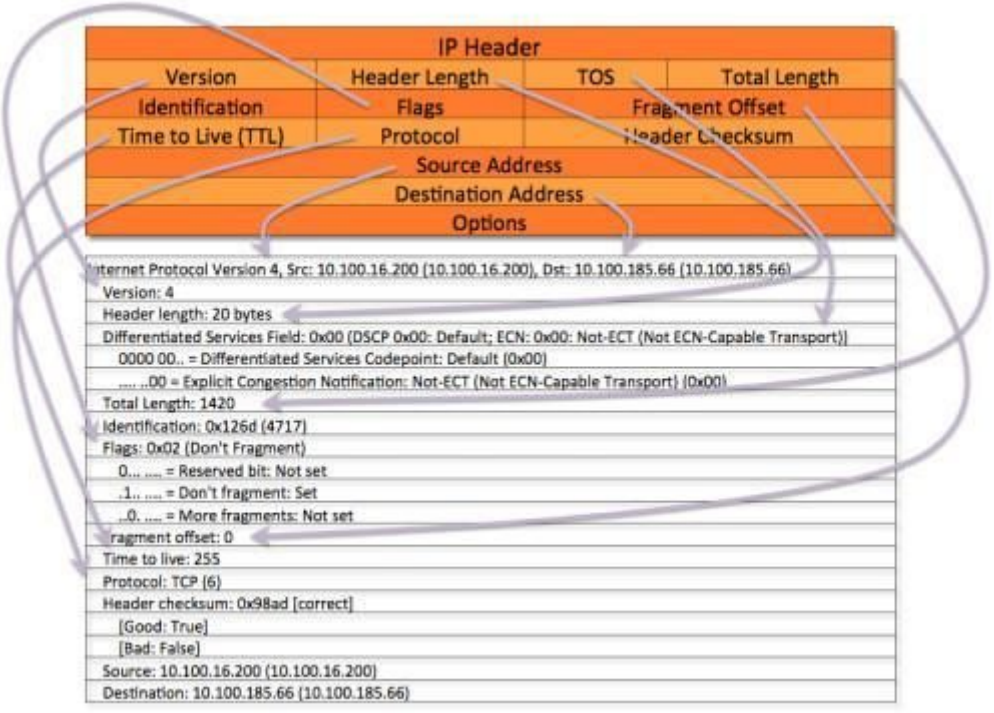


Figure 4. IP Header (Layer-3)

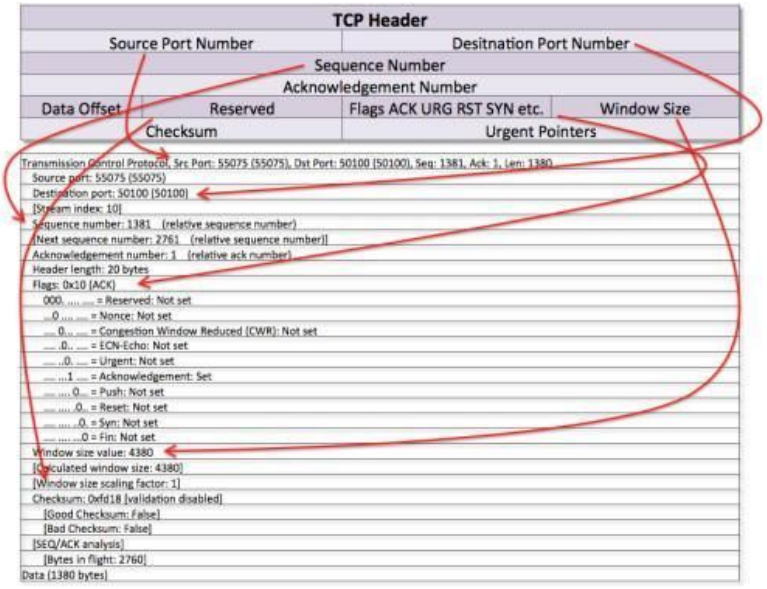
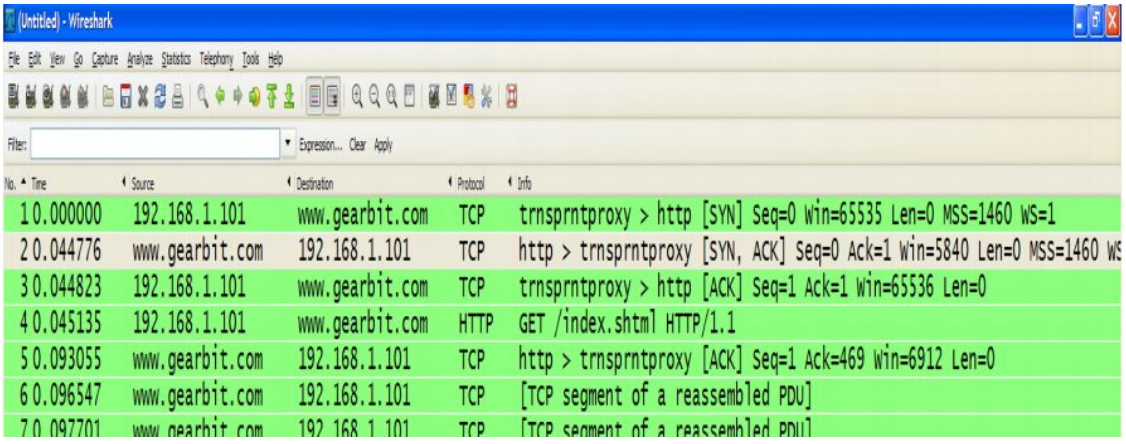


Figure 5. TCP headers.

TCP Three-way Handshake

The delta value between frames 1 and 2 can be used as a TCP transport connect baseline value. Other important information gathered from this handshake: • Window Size • SACK • Maximum Segment Size • Window Scale Option value



Conclusion: Hence we successfully studied the program of implementing wired shark.

Date:

Sign: **Grade:**