

Batch: A2

Roll No.: 16010121045

Experiment / assignment / tutorial No. _____

Grade: AA / AB / BB / BC / CC / CD / DD

Signature of the Staff In-charge with date

Experiment No.:10

TITLE: Study of Packet Analyzer tool: Wireshark

AIM: To study and analyse various Protocols using Packet Analyzer tool: Wireshark

Expected Outcome of Experiment:

CO:

Books/ Journals/ Websites referred:

1. A. S. Tanenbaum, "Computer Networks", Pearson Education, Fourth Edition
2. B. A. Forouzan, "Data Communications and Networking", TMH, Fourth Edition

Pre Lab/ Prior Concepts:

IPv4 Addressing, Subnetting, Link State Protocol, Router configuration Commands

New Concepts to be learned: Packet Analyzer tool: Wireshark.

THEORY:

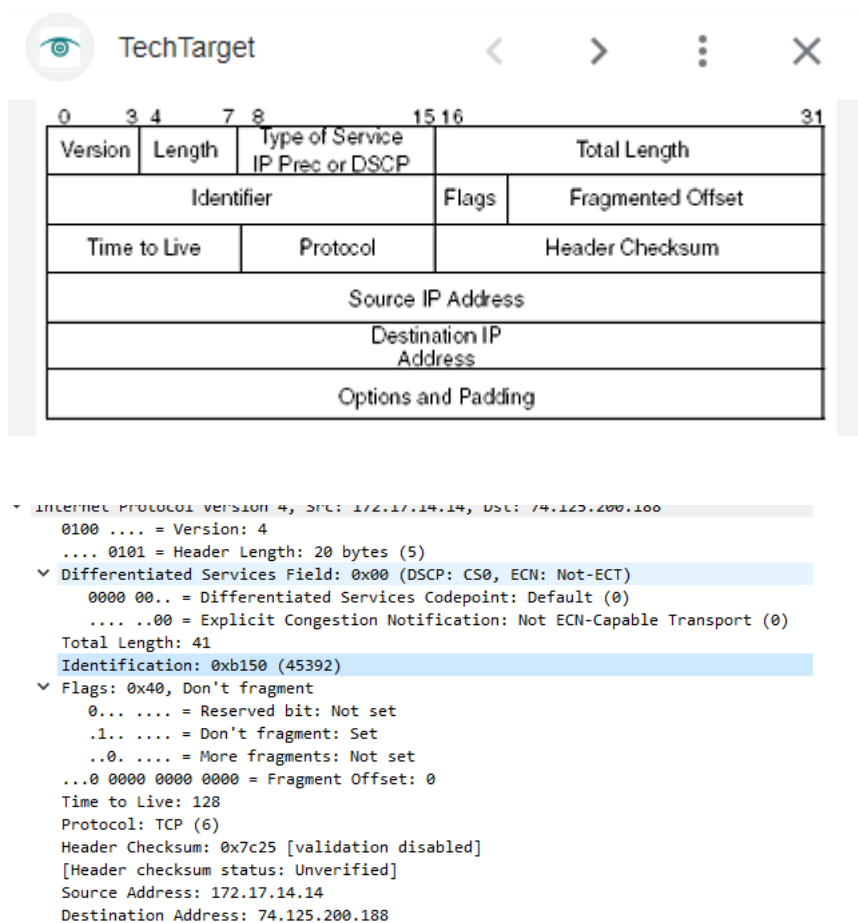
Wireshark is an open-source packet analyzer, which is used for education, analysis, software development, communication protocol development, and network troubleshooting. It is used to track the packets so that each one is filtered to meet our specific needs. It is commonly called as a sniffer, network protocol analyzer, and network analyzer. It is also used by network security engineers to examine security problems. Wireshark is a free to use application which is used to apprehend the data back and forth. It is often

called as a free packet sniffer computer application. It puts the network card into an unselective mode, i.e., to accept all the packets which it receives.

Uses of Wireshark

1. It is used by network security engineers to examine security problems.
2. It allows the users to watch all the traffic being passed over the network.
3. It is used by network engineers to troubleshoot network issues.
4. It also helps to troubleshoot latency issues and malicious activities on your network.
5. It can also analyze dropped packets.
6. It helps us to know how all the devices like laptop, mobile phones, desktop, switch, routers, etc., communicate in a local network or the rest of the world.

IMPLEMENTATION:



TechTarget

0	3	4	7	8	15	16	31
Version		Length		Type of Service IP Prec or DSCP		Total Length	
Identifier				Flags		Fragmented Offset	
Time to Live		Protocol		Header Checksum			
Source IP Address							
Destination IP Address							
Options and Padding							

```

Internet Protocol Version 4, Src: 172.17.14.14, Dst: 74.125.200.188
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    0000 00.. = Differentiated Services Codepoint: Default (0)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 41
  Identification: 0xb150 (45392)
  Flags: 0x40, Don't fragment
    0... .... = Reserved bit: Not set
    .1.. .... = Don't fragment: Set
    ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 128
  Protocol: TCP (6)
  Header Checksum: 0x7c25 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 172.17.14.14
  Destination Address: 74.125.200.188
  
```

Using the ip header :

Version:4

Header length:5 (20 bytes)

Different types of services: dscp ecn

Identifier:0xb150

Flags: 0x40

Fragments :reserved (not set),don't fragment (set)

Time to live:128

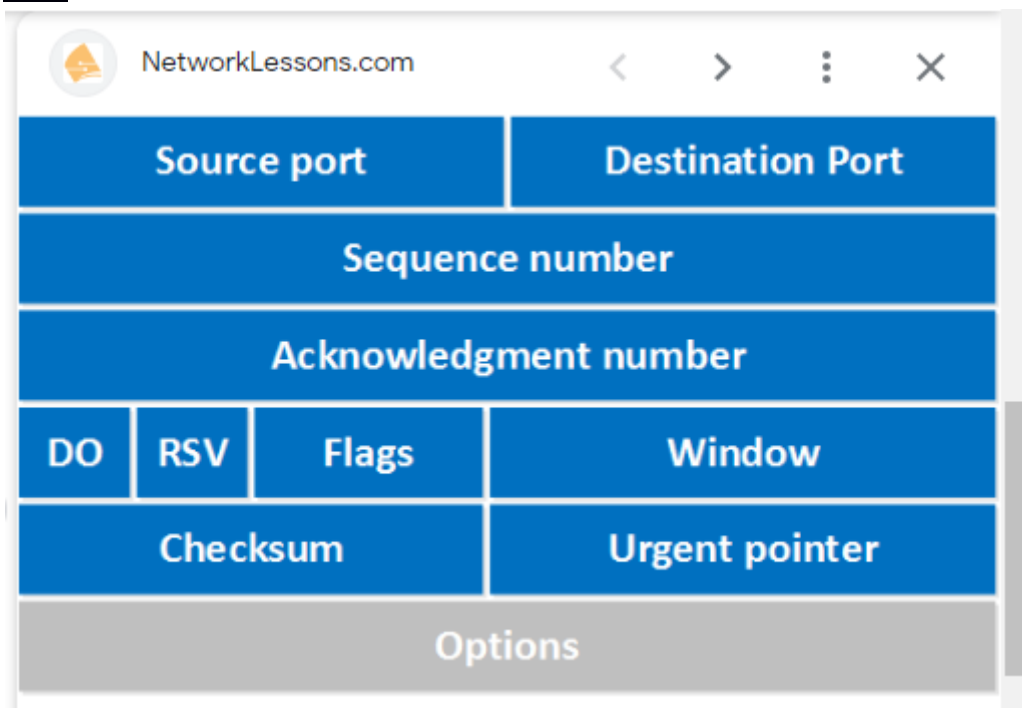
Protocol:tcp

Headerchecksum:0x7c25

Source ip:172.17.14.14

Destination ip :74.125.200.188

Tcp:



```

Transmission Control Protocol, Src Port: 49924, Dst Port: 5228, Seq: 1, Ack: 1, Len: 1
  Source Port: 49924
  Destination Port: 5228
  [Stream index: 25]
  [Conversation completeness: Incomplete (12)]
  [TCP Segment Len: 1]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 2690947899
  [Next Sequence Number: 2 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 1391422250
  0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x010 (ACK)
  Window: 1023
  [Calculated window size: 1023]
  [Window size scaling factor: -1 (unknown)]
  Checksum: 0x0d51 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  > [Timestamps]
  > [SEQ/ACK analysis]
  TCP payload (1 byte)
  Data (1 byte)

```

Source port:49924

Destination:5228

Sequence no:

```

Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 2690947899
[Next Sequence Number: 2 (relative sequence number)]

```

Acknowledgement:

```

Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 1391422250
0101 .... = Header Length: 20 bytes (5)

```

Flags:

```

Flags: 0x010 (ACK)
000. .... = Reserved: Not set
...0 .... = Nonce: Not set
.... 0... = Congestion Window Reduced (CWR): Not set
.... .0.. = ECN-Echo: Not set
.... ..0. = Urgent: Not set
.... ...1 = Acknowledgment: Set
.... .... 0... = Push: Not set
.... .... .0.. = Reset: Not set
.... .... ..0. = Syn: Not set
.... .... ...0 = Fin: Not set
[TCP Flags: .....A....]

```

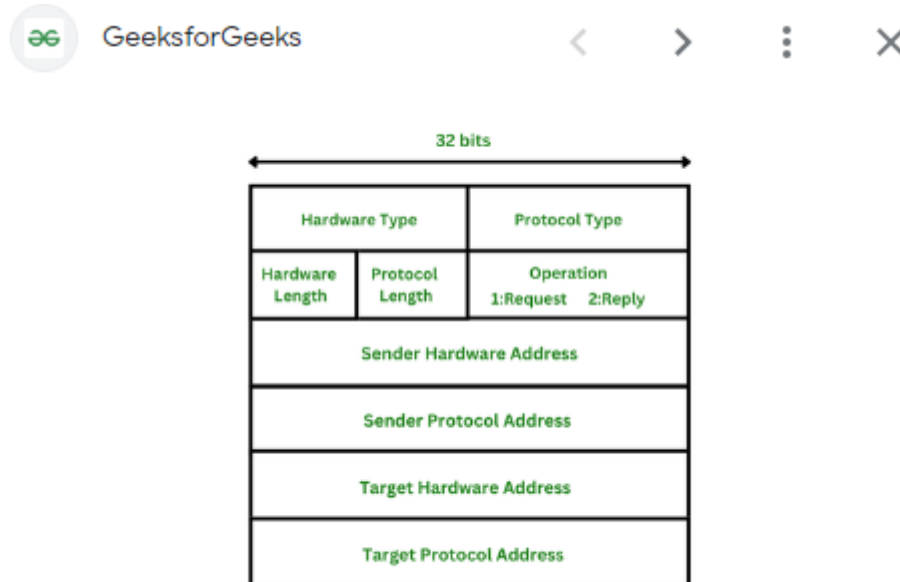
Window:1023

Checksum:

Checksum: 0x0d51 [unverified]
[Checksum Status: Unverified]

Urgent pointer :0

ARP:



```
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: request (1)
Sender MAC address: Cisco_66:d1:41 (b0:aa:77:66:d1:41)
Sender IP address: 172.17.15.254
Target MAC address: Broadcast (ff:ff:ff:ff:ff:ff)
Target IP address: 172.17.15.3
```

Arp takes place in frames as the data travels where only the sender and receivers
Where the sender and recievers address is noted.

UDP:

The image shows a Wireshark packet capture interface. At the top, there's a packet list showing a packet from 'Imperva, Inc.' with a source port of 59060 and a destination port of 3702. The packet details pane on the right shows the structure of the UDP packet:

- UDP Header:**
 - Source Port
 - Destination Port
 - Length
 - Checksum
- Data:** (The payload of the packet)

Below the diagram, the packet details pane shows the following information:

- User Datagram Protocol, Src Port: 59060, Dst Port: 3702
- Source Port: 59060
- Destination Port: 3702
- Length: 664
- Checksum: 0x2c23 [unverified]
- [Checksum Status: Unverified]
- [Stream index: 3597]
- [Timestamps]
- UDP payload (656 bytes)

CONCLUSION:

Thus we have implemented the wireshark experiment

Date: _____

Signature of faculty in-charge