Ex. No: 14
30|9|25

Capture, save and Analyze Network traffic

Aim:

To capture live network traffic, save the capture and analyze protocol-specific flows using wineshark.

Procedure:

1. open wineshark
2. select Interface to capture
3. set capture filter
4. start capture
5. Generate traffic
6. stop capture
7. save capture
8. Analyze using Display Filters
9. Protocol - Specific analysis actions.

Commands:

```
sudo tshark -i -etho- w lab14-capture.pcap
sudo tshark -i etho - s "Post 53 or Post 67".
tshark -r lab14 -capture.pcapng - y http -y
tshark -r lab14.capture.pcapng -y dns.qy.r
```

Result:

Thus live traffic has been captured succesfully using wireshark & tshark.

Output.

Packet List - HTTP Example.

No.	Time	Source	Destination	Protocol
34	12.3456	192.168.1.10	93.184.216.34	HTTP
35	12.3460	93.184.216.34	192.168.1.10	HTTP