Practical-7

AIM: Traffic Data Analysis using Wireshark

Tools required:
1. Desktop computer
2. Wireshark

Submission: Written file submission (starting from page no. 4) is expected.
Rubrics: Nicely drafted document with clarity in answers leads to full marks. Otherwise, submission carries proportional marks. Same day submission will be evaluated from 10 marks otherwise submission will be evaluated from 7 marks.

References
Wireshark Installation : Wireshark Tutorial for Beginners - Installation
Wireshark Walkthrough : https://www.youtube.com/watch?v=lb1Dw0elw0Q

Wireshark Videos:
- Edit Windows
- Canvas Window
- Capturing Data
- Interpreting data in Wireshark
- Ethernet Frame
- IP Frame
- Throughput
- Flow diagram

Understanding Require
- IP Address
- URL
- Finding IP address from URL
- Finding location from IP Address

Wireshark for Windows

Install wireshark from below link

https://www.wireshark.org/#download

Wireshark for Linux

Installing Wireshark on Linux can be a little different depending on the Linux distribution.
From a terminal prompt, run these commands:
sudo apt-get install wireshark
sudo dpkg-reconfigure wireshark-common
sudo adduser $USER wireshark

Those commands download the package, update the package, and add user privileges to run Wireshark.

Capturing Data Packets on Wireshark

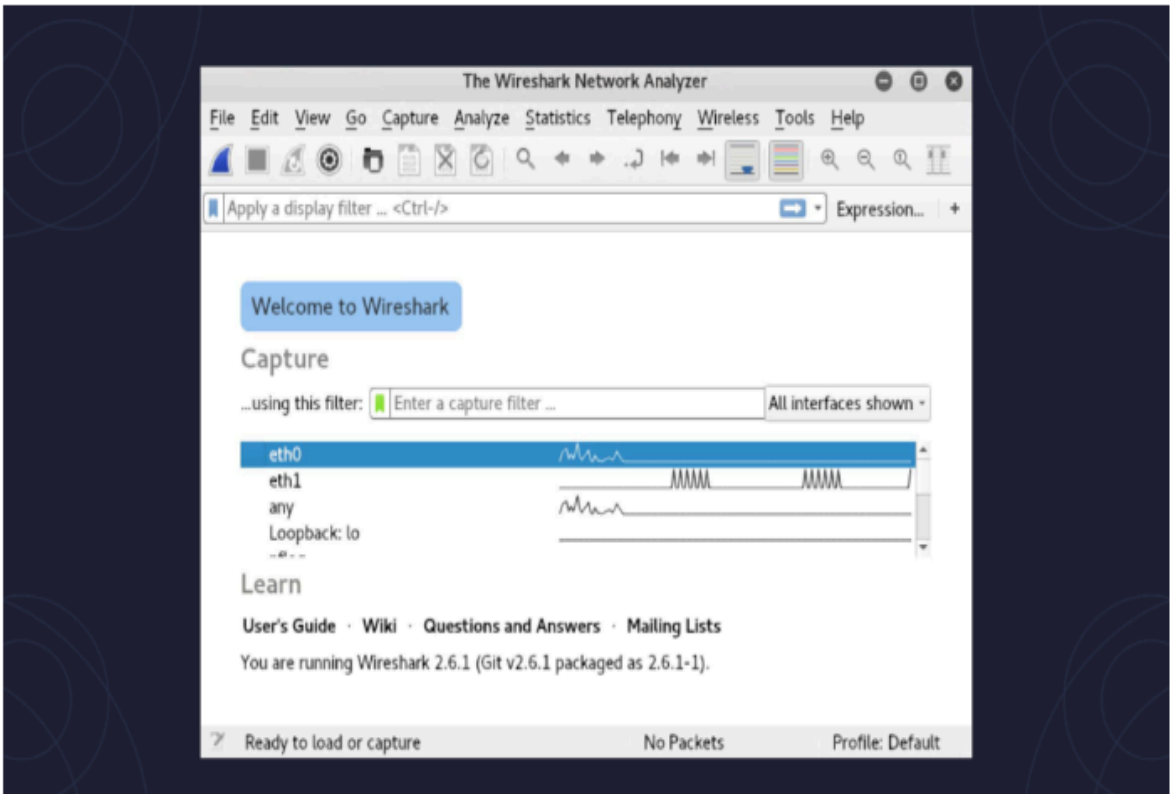


Figure - 7.1

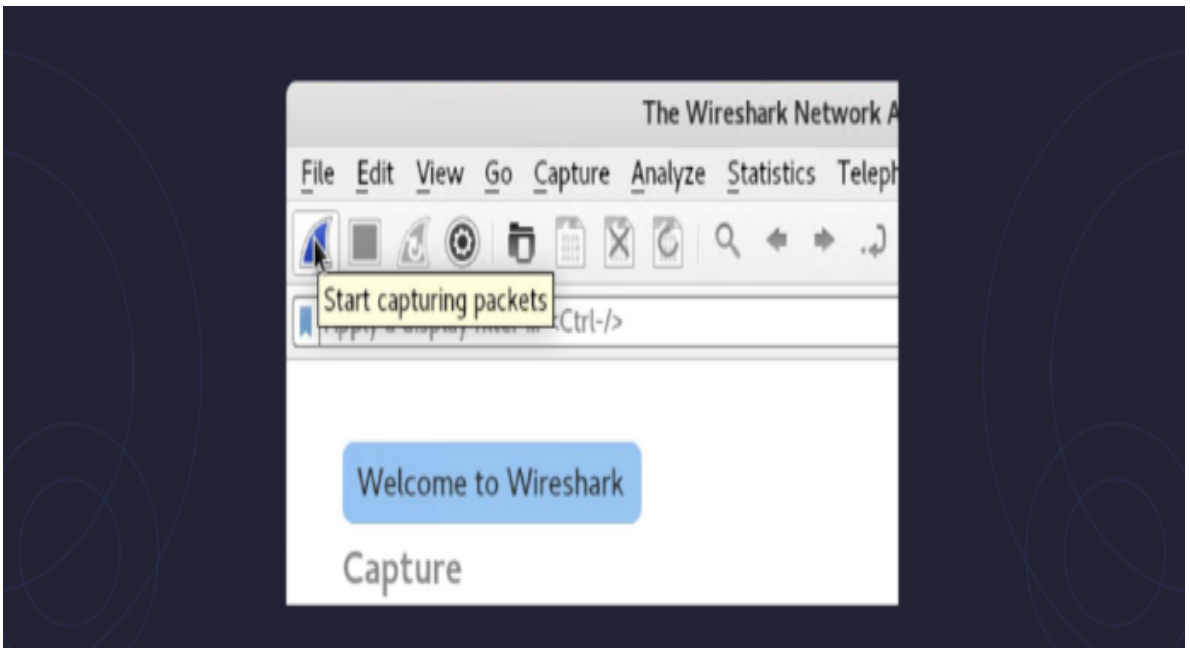


Figure -7.2

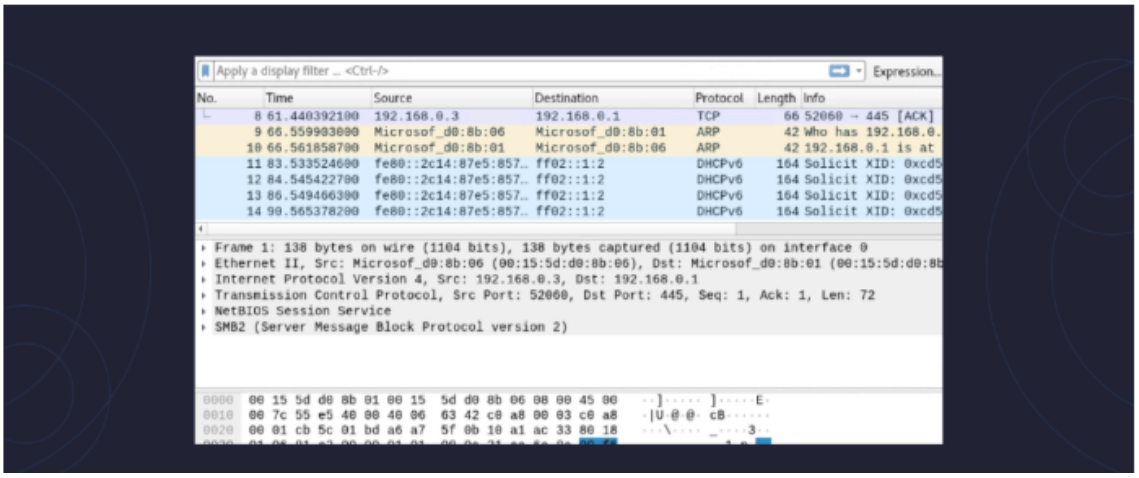

Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
8 61.440392100 192.168.0.3 192.168.0.1 TCP 66 52060 → 445 [ACK]
9 66.559903000 Microsof_d0:8b:06 Microsof_d0:8b:01 ARP 42 Who has 192.168.0.
10 66.561858700 Microsof_d0:8b:01 Microsof_d0:8b:06 ARP 42 192.168.0.1 is at
11 83.533524600 fe80::2c14:87e5:857… ff02::1:2 DHCPv6 164 Solicit XID: 0xcd5
12 84.545422700 fe80::2c14:87e5:857… ff02::1:2 DHCPv6 164 Solicit XID: 0xcd5
13 86.549466300 fe80::2c14:87e5:857… ff02::1:2 DHCPv6 164 Solicit XID: 0xcd5
14 90.565378200 fe80::2c14:87e5:857… ff02::1:2 DHCPv6 164 Solicit XID: 0xcd5
Frame 1: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits) on interface 0
Ethernet II, Src: Microsof_d0:8b:06 (00:15:5d:d0:8b:06), Dst: Microsof_d0:8b:01 (00:15:5d:d0:8b
Internet Protocol Version 4, Src: 192.168.0.3, Dst: 192.168.0.1
Transmission Control Protocol, Src Port: 52060, Dst Port: 445, Seq: 1, Ack: 1, Len: 72
NetBIOS Session Service
SMB2 (Server Message Block Protocol version 2)
0000 00 15 5d d0 8b 01 00 15 5d d0 8b 06 08 00 45 00
0010 00 7c 55 e5 40 00 40 06 63 42 c0 a8 00 03 c0 a8
0020 00 01 cb 5c 01 bd a6 a7 5f 0b 10 a1 ac 33 80 18

Figure - 7.3

Practical-7

AIM: Traffic Data Analysis using Wireshark

Tools required:

1. Desktop computer
2. Wireshark

Exercise

1. Turn on wireshark.
2. Then select your respective network adapter (eg. Ethernet) and start( ) capturing the data.
3. Now, go to your browser.
4. Type 172.16.12.25 in your search engine.
5. After 2 seconds go to wireshark and stop( ) capturing data.
6. Go to the wireshark file menu and click on save.
7. Save your file as pr-7_sample1.
8. Repeat steps 1,2,3.
9. Type 172.16.0.1:8090 in your search engine.
10. After 2 seconds go to wireshark and stop( ) capturing data.
11. Go to the wireshark file menu and click on save.
12. Save your file as pr-7_sample2.

Based on this above steps answer the following questions and fill the below tables with respect to fields.

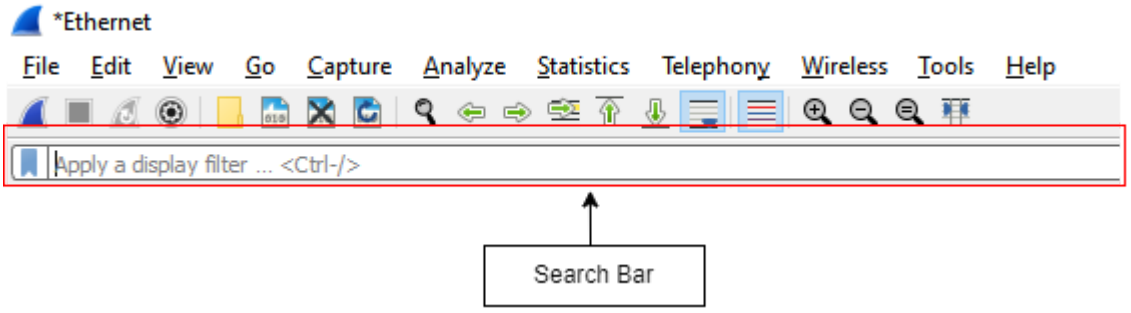
Observe the columns and write its purpose in the table below.



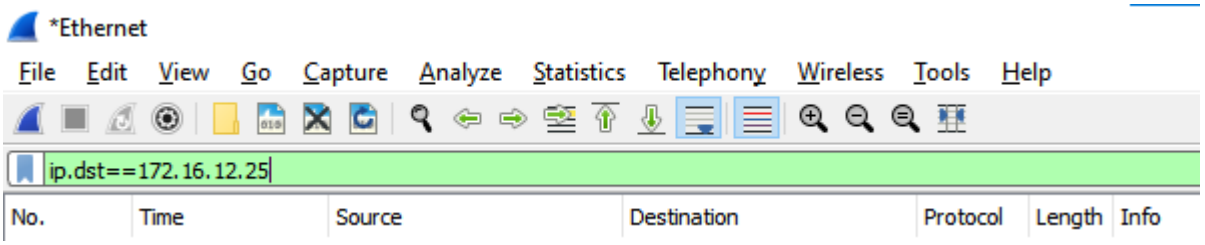
Fields	Description
No.	
Time	
Source	
Destination	
Protocol	
Length	
Info	

Observe the capture data and write description as per following table for sample 1.

Fields	Description/Answer
Time difference between packet no. 1 and packet no. 10	
Time difference between packet no. 15 and packet no. 40	
Source of packet no. 1	
Destination of packet no.1	
Transport layer protocol of packet no. 1	
Network layer protocol of packet no. 1	
Data link layer(Layer 2) protocol of packet no. 1	



Use Different Filters and write the description in the table below for sample 1.



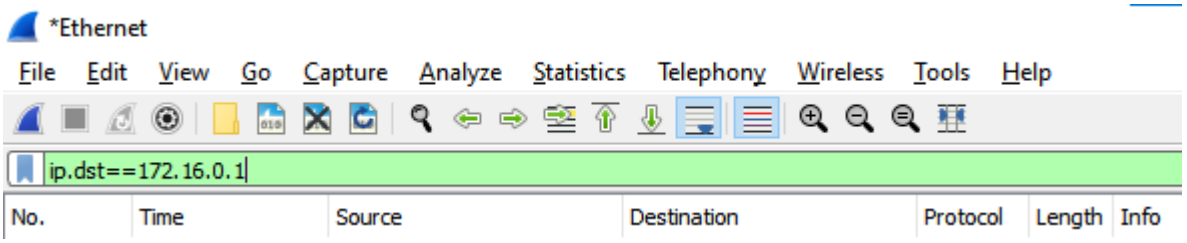
Fields	Description/Answer
First packet No. sent by your PC(Source). (Query : ip.src==<<your PC's IP address>>)	
First packet received from destination (Query : ip.dst==172.16.12.25).	

Time of packet sent by your PC (Query : ip.src==<<your PC's IP address>>).	
Time of packet received from destination (Query : ip.dst==172.16.12.25)	
Total number of ARP packets (Query : arp)	
Total number of TCP packets (Query : tcp)	
Total number of HTTP/HTTPS packets (Query : http || https)	
Time at which first TCP packet sent (Query : tcp)	
Time at which HTTP request sent (Query : http)	
Time at which HTTP reply received (Query : http)	
Time difference between first TCP packet and first HTTP packet (Query : http || tcp)	
Time difference between http request and http reply (Query : http)	

Observe the capture data and write description as per following table for sample 2.

Fields	Description/Answer
Time difference between packet no. 1 and packet no. 10	
Time difference between packet no. 15 and packet no. 40	
Source of packet no. 1	
Destination of packet no.1	
Transport layer protocol of packet no. 1	
Network layer protocol of packet no. 1	
Data link layer(Layer 2) protocol of packet no. 1	

Use Different Filters and write the description in the table below for sample 2.



Fields	Description/Answer
First packet No. sent by your PC(Source). (Query : ip.src==<<your PC's IP address>>)	
First packet received from destination (Query : ip.dst==172.16.0.1).	
Time of packet sent by your PC (Query : ip.src==<<your PC's IP address>>).	
Time of packet received from destination (Query : ip.dst==172.16.0.1)	
Total number of ARP packets (Query : arp)	
Total number of TCP packets (Query : tcp)	

Total number of HTTP/HTTPS packets (Query : http || https)	
Time at which first TCP packet sent (Query : tcp)	
Time at which HTTP request sent (Query : http)	
Time at which HTTP reply received (Query : http)	
Time difference between first TCP packet and first HTTP packet (Query : http || tcp)	
Time difference between http request and http reply (Query : http)	

Questions:

1. A user is unable to ping a system on the network. How can wireshark be used to solve the problem? [Hint : ping any machine then go to wireshark and observe the screen]
   Ans.

2. Which wireshark filter can be used to monitor outgoing packets from a specific system on the network.
   Ans.

3. Which query should you use to filter all web traffic?
   Ans.

4. A user raises a ticket stating that he is unable to access any websites, but is able to ping any IP address on the internet. How would you use wireshark to identify the problem?
   [Hint : type query as dns and observe the dns packets and write description as you understood.]
   Ans.

5. Is it possible to find out if any packet was lost while capturing data with Wireshark? If yes, then how? [Hint : go to wireshark statistics>summary and look at the parameters.]
   Ans.

6. Which query would you search to remove all packets that were captured before and after a specific time range?
   Ans.

7. List out examples where wireshark can be used.
   Ans.

8. Why do you think it's important to monitor network traffic on enterprise systems?
   Ans.

9. Which wireshark filter(query) can be used to check all incoming requests to a HTTP Web server
   Ans.