



D. B. J. COLLEGE, CHIPLUN
DEPARTMENT OF COMPUTER SCIENCE

Page No. : _____

| | |
|-----------|---|
| Expt. No. | Name : <u>Piyush Pandurang Burate</u> Class : <u>TYCS</u> Roll No. : <u>523</u> |
| Date | Title of Experiment : <u>Capturing and analysing network packet using Wireshark.</u> |
| | Sub titles : Assignment/ Problem Solution, Flow chart/Algorithm, Problem Listing, Input Screen, Output Screen, Comments (If any) |
| | <u>Aim :-</u> Capturing and analyzing network packet using Wireshark : <ul style="list-style-type: none">• Identification of the live network.• Capture packets• Analyzed the capture packets. |
| | <u>Software/Hardware Requirements :-</u> Wireshark , Computer , printer. |
| | <u>Theory :-</u> <p>Wireshark is the world's foremost and widely used N/W protocol analyzer. It lets you see whats happening on your network at a microscopic level and is the defacto standard across many commercial and non-profit enterprizes , government agencies, and educational institution wireshark development thrives thanks to the volunteer contributions of networking experts around the globe and is the continuation of project started by gerald combs in 1998.</p> |
| Remark | Wireshark has a rich feature set which includes the following :- |
| Signature | <ul style="list-style-type: none">• Deep inspiration of hundreds of protocols with more being added all the time. |

- Live capture and offline analysis
- Standard three-pane packet browser
- Multi-platform: Run on windows, Linux, Solaris, Free BSD, Net BSD and many others.
- Capture network data can be browsed via a GUI or via the TTY-mode TShark
- The most powerful display filters in the industry.
- Rich VOIP analysis
- Read/write many different capture file formats: tcpdump, pcapNG, catpull, DCT2000, asco secure IDS 1° plug, microsoft, Network monitor, Network general snitter and many others.
- Capture files compressed with gzip can be decompressed on the fly.
- Live data can be read from ethernet, IEEE 802.11, ppp/HDLC, ATM, Bluetooth, USB, Token Ring, Frame relay, FDDT and others.
- Decryption support for many protocols, including IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS
- Coloring rule can be applied to the packet list for quick, intuitive analysis.
- Output can be exported to XML, postscript, CSV, or plain text.

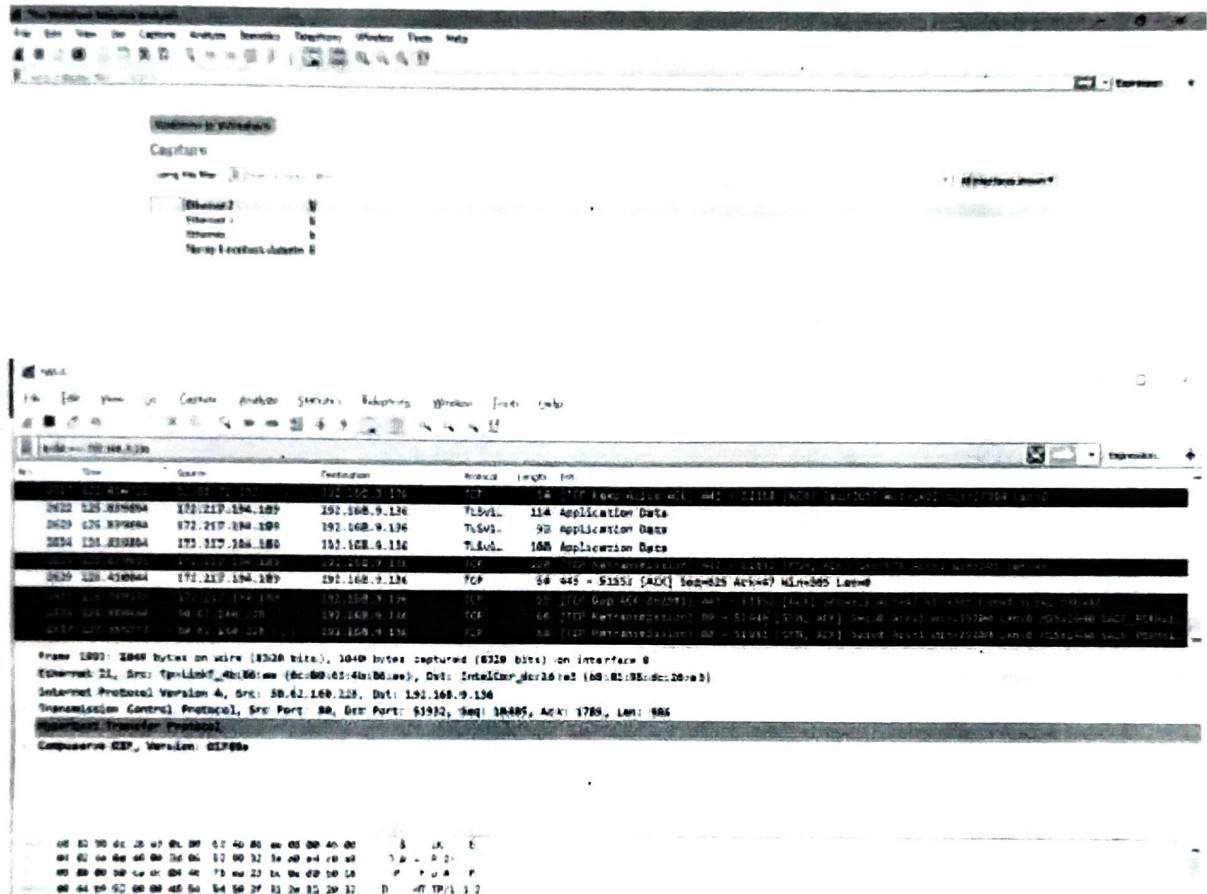
Conclusion :-

By using Wireshark we capture and analyzed packets.

Practical 4: Capturing and analyzing network packets using Wireshark (Fundamentals):

Steps:

1. Open Wireshark and click on Ethernet.



2. Now go on browser and open any unsecured website i.e www.razorba.com and perform some activity on the website..
3. Now come back to Wireshark and enter http in the search bar.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|---------------|---------------|----------|--------|--------------------|
| 1 | 0.000000 | 192.168.1.100 | 192.168.1.1 | HTTP | 1000 | GET / HTTP/1.1 |
| 2 | 0.000000 | 192.168.1.1 | 192.168.1.100 | HTTP | 1000 | 200 OK (text/html) |
| 3 | 0.000000 | 192.168.1.100 | 192.168.1.1 | HTTP | 1000 | GET / HTTP/1.1 |
| 4 | 0.000000 | 192.168.1.1 | 192.168.1.100 | HTTP | 1000 | 200 OK (text/html) |
| 5 | 0.000000 | 192.168.1.100 | 192.168.1.1 | HTTP | 1000 | GET / HTTP/1.1 |
| 6 | 0.000000 | 192.168.1.1 | 192.168.1.100 | HTTP | 1000 | 200 OK (text/html) |
| 7 | 0.000000 | 192.168.1.100 | 192.168.1.1 | HTTP | 1000 | GET / HTTP/1.1 |
| 8 | 0.000000 | 192.168.1.1 | 192.168.1.100 | HTTP | 1000 | 200 OK (text/html) |
| 9 | 0.000000 | 192.168.1.100 | 192.168.1.1 | HTTP | 1000 | GET / HTTP/1.1 |
| 10 | 0.000000 | 192.168.1.1 | 192.168.1.100 | HTTP | 1000 | 200 OK (text/html) |

4. Now click on the get request and see the details.

Wireshark 2.10.0 (64-bit) - Ethernet II, Src: Intel(R) Gigabit Ethernet Controller, Dst: 08:00:27:00:00:00, Length: 1000, Captured on eth0

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|---------------|---------------|----------|--------|--------------------|
| 1 | 0.000000 | 192.168.1.100 | 192.168.1.1 | HTTP | 1000 | GET / HTTP/1.1 |
| 2 | 0.000000 | 192.168.1.1 | 192.168.1.100 | HTTP | 1000 | 200 OK (text/html) |
| 3 | 0.000000 | 192.168.1.100 | 192.168.1.1 | HTTP | 1000 | GET / HTTP/1.1 |
| 4 | 0.000000 | 192.168.1.1 | 192.168.1.100 | HTTP | 1000 | 200 OK (text/html) |
| 5 | 0.000000 | 192.168.1.100 | 192.168.1.1 | HTTP | 1000 | GET / HTTP/1.1 |
| 6 | 0.000000 | 192.168.1.1 | 192.168.1.100 | HTTP | 1000 | 200 OK (text/html) |
| 7 | 0.000000 | 192.168.1.100 | 192.168.1.1 | HTTP | 1000 | GET / HTTP/1.1 |
| 8 | 0.000000 | 192.168.1.1 | 192.168.1.100 | HTTP | 1000 | 200 OK (text/html) |
| 9 | 0.000000 | 192.168.1.100 | 192.168.1.1 | HTTP | 1000 | GET / HTTP/1.1 |
| 10 | 0.000000 | 192.168.1.1 | 192.168.1.100 | HTTP | 1000 | 200 OK (text/html) |

Frame 1: 1000 bytes on wire (8000 bits), 1000 bytes captured (8000 bits) on interface eth0

Ethernet II, Src: Intel(R) Gigabit Ethernet Controller (82:00:27:00:00:00), Dst: 08:00:27:00:00:00, Length: 1000

Internet Protocol Version 4, Src: 192.168.1.100, Dst: 192.168.1.1

Transmission Control Protocol, Src Port: 52000, Dst Port: 80, Seq: 500, Ack: 5631, Len: 512

Hypertext Transfer Protocol

Host: www.facebook.com

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:55.0) Gecko/20100101 Firefox/55.0

Accept: text/css,*/*;q=0.1

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Referer: http://www.facebook.com/

Connection: keep-alive

Cookie: ...

GET / HTTP/1.1