D. B. J. COLLEGE, CHIPLUN

Page No. : _____

DEPARTMENT OF COMPUTER SCIENCE

Expt. No.

Name : Piyush Pandurang Burate Class : TYCS Roll No.: 523

Title of Experiment : Capturing and analysing network packet using Wireshark.

Date

Sub titles : Assignment/ Problem Solution, Flow chart/Algorithm, Problem Listing, Input Screen, Output Screen, Comments (If any)

Aim :- Capturing and analyzing network packet using Wireshark :

- Identification of the live network.
- Capture packets
- Analyzed the capture packets.

Software/Hardware Requirements :-

Wireshark , Computer , printer.

Theory :-

Wireshark is the world's foremost and widely used N/W protocal 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.

Wireshark has a rich feature set which includes the following :-

- Deep inspiration of hundreds of protocals with more being added all the time.

Remark

Signature

- Live capture and offline analysis
- Standard three-pane packet brow
- Multi-platform : Runon 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 fill formats: tcpdump, pcapNG, catpull, DCT2000 asco secure IDS 1° plag, microsoft, Network monitor, Network general snitter and many others.
- Capture files compressed with gzip can be decompressed on the fig.
- 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, Kebemos, 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.

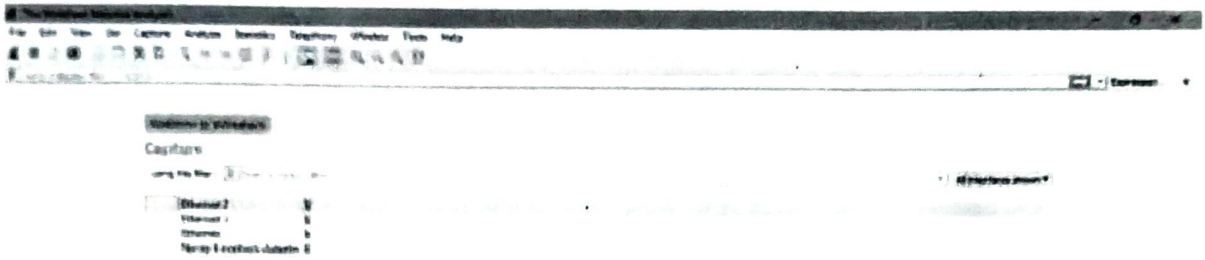
Conclusion :-

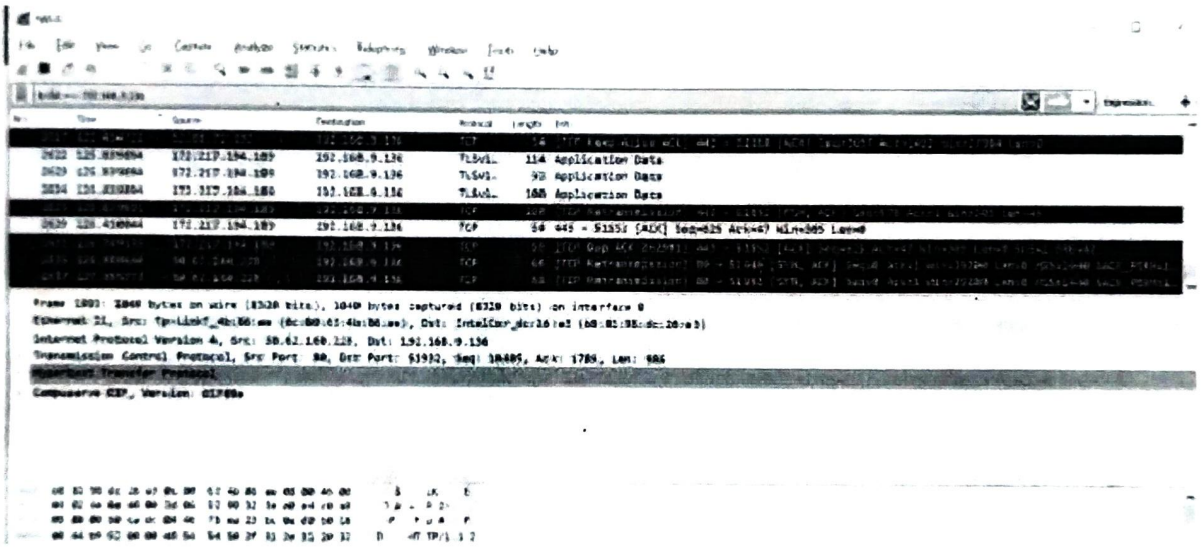
By using Wireshark we capture and analyzed packets.

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

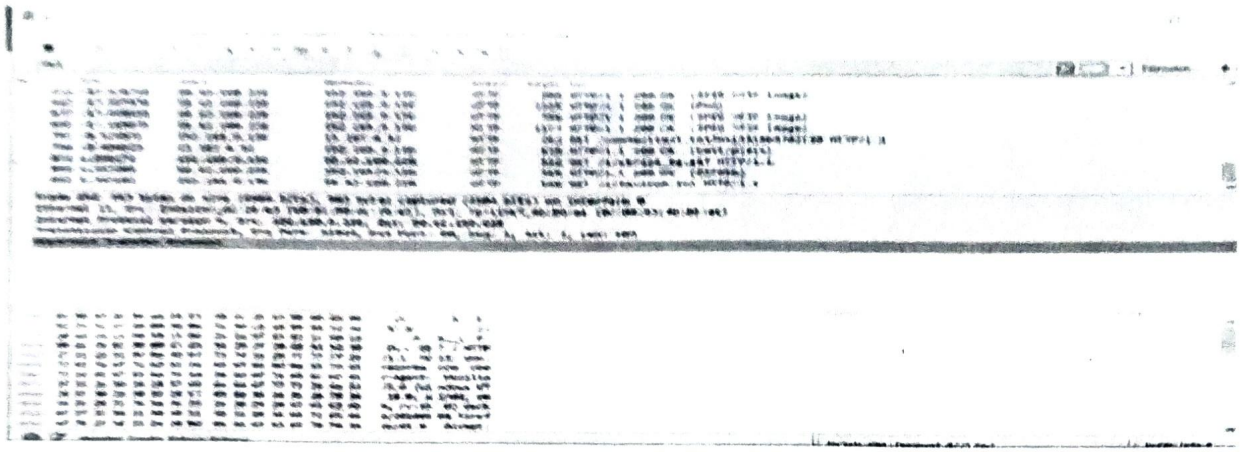
Steps:

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.



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