Aldel Education Trust's
St. John College of Engineering and Management, Palghar
(A Christian Religious Minority Institution)
Approved by AICTE and DTE, Affiliated to University of Mumbai/MSBTE
St. John Technical Campus, Vevoor, Manor Road, Palghar (E), Dist. Palghar, Maharashtra-401404
NAAC Accredited with Grade 'A'

DEPARTMENT OF COMPUTER ENGINEERING

Lab code: CSL602   **Class:** T.E./COMP/A2 & A3

Course name: Cryptography & System Security Lab

EXPERIMENT 5

Aim: Study of packet sniffer tools: Wireshark [LO3]

1. Download and install Wireshark and capture ICMP, TCP, and HTTP packets in promiscuous mode.
2. Explore how the packets can be traced based on different filters.

Theory:

Include following points in the theory,

1. What is Wireshark?
2. Purpose of such software, which type of attack it can launch?
3. Explain the features of Wireshark that you have studied.

Note: Use user guide of Wireshark.

Implementation:

1) Install Wireshark tool on the system.
2) Learn how to capture all the packets flowing through the network.
3) Filter TCP packets.
4) Open a site and give username and password.
5) Try to capture the username and password through Wireshark tool.
6) Capture TCP stream data revealing login credentials.

Output: Printout of the Wireshark screen shot showing TCP packet details. Highlight the important packet details that we have discussed during practical.

Conclusion: Mention your conclusion here

Viva Questions:

1. List other available sniffer tools.
2. How can Wireshark be used for malicious attacks?

Faculty In-charge:

Mr. Vivian Lobo