

Experiment No. 9

Title: Network Sniffing - Wireshark

**Batch: Roll No.: Experiment No.:**

**Aim:** To perform network sniffing using wire shark tool

**Resources needed:** Wire shark tool

# Theory

Wireshark is a network packet analyzer. Any network packet analyzer will try to capture network packets and will try to display that packet data as detailed as possible in human readable format. Wireshark is an open source software project, and is released under the GNU General Public License (GPL). We can freely use Wireshark on any number of computers, without worrying about license keys. In addition, all source code is freely available under the GPL. Because of that, it is very easy for people to add new protocols to Wireshark, either as plug-in, or built into the source code. In the past, such tools were either very expensive, proprietary. However, with the advent of Wire-shark, all that has changed. Wireshark is perhaps one of the best open source packet analyzers available today.

**What Wireshark is not......**

Here are some things Wireshark does not provide:

1. Wireshark isn’t an intrusion detection system. It will not warn us when someone does strange things on our network that he/she isn’t allowed to do. However, if strange things happen, Wireshark might help you figure out what is really going on.

2. Wireshark will not manipulate things on the network, it will only "measure" things from it. Wireshark doesn’t send packets on the network or do other active things.

**Applications of Wireshark**:

Here are some applications. Many people use Wireshark for doing following things,

* Network administrators use it to troubleshoot network problems.
* Network security engineers use it to examine security problems (Network Forensics.)
* Developers use it to debug protocol implementations.
* People use it to learn network protocol internals.

Beside these examples Wireshark can be helpful in many other situations too.

**Features of Wireshark:**

The following are some of the many features Wireshark has:

* Available for UNIX and Windows operating systems.
* Capture live packet data from a chosen network interface.
* Open files containing packet data captured with tcpdump/WinDump and a number of other packet capture programs.
* Import packets from text files containing hex dumps of packet data.
* Display packets with very detailed protocol information.
* Save packet data captured.
* Export some or all packets in a number of capture file formats.
* Filter packets on many criteria.
* Search for packets on many criteria.
* Colorize packet display based on filters.
* Create various statistics.

……and a lot more!

Most important menus are : 1) Capture 2) Analyze 3) Statistics

Students are expected to explore all these menus and sub-menus in details.

Wireshark can capture traffic from many different network media types including wireless LAN as well. Which media types are supported, depends on many things like the operating system we are using and the hardware support.

**Physical interfaces supported:**

* ATM - capture ATM traffic
* Bluetooth- capture Bluetooth traffic .
* Cisco HDLC links - capture on synchronous links using Cisco HDLC encapsulation.
* Ethernet- capture on different topologies, including switched networks.
* Framerelay – captures framerelay traffic.
* IrDA capture IrDA traffic - currently limited to Linux.
* PPP links - capture on dial-up lines, ISDN connections and PPP-over-Ethernet (PPPoe, e.g. ADSL)
* Tokenring - capture on Tokenring adapters, promiscuous mode and switched networks
* USB- capture of raw USB traffic
* WLAN- capture on 802.11 (WLAN, Wi-Fi) interfaces, including "monitor mode" , raw 802.11 headers and radio information

**Virtual interfaces :**

* Loopbak - capture traffic from a machine to itself, including the IP address 127.0.0.1
* Pipes - use UNIX pipes to capture from other applications (even remote!)
* VLAN – capture VLAN traffic, including VLAN tags.

**In addition to this, Wireshark can do following things.**

* Import files from many other capture programs.
* Wireshark can open packets captured from a large number of other capture programs.
* Export files for many other capture programs.
* Wireshark can save packets captured in a large number of formats of other capture programs.
* Can be used as a protocol decoder.

**Procedure / Approach /Algorithm / Activity Diagram:**

1. Go to the official website of Wireshark . ( www.wireshark.org) and download the stable version of Wireshark for 64 bit windows operating system.
2. After successful installation you will get the blue icon of Wireshark on the desktop.
3. Click on the icon and start the software.
4. Choose an interface and start capturing the packets.
5. Study the packet details of all the protocols.
6. Understand color code in details.
7. Perform the statistics for a particular protocol. (Every student should perform for different protocol. )

# Implementation:

Task1: Design your own registration and login pages (along with user database of registered users)

Task2: Run wire shark and capture the login page request data using wire shark and locate the captured password.

**Questions:**

1) What is the difference between Burp suite and wire shark tools.

**Result:** Task 1 implementation code and Task 2 screenshots.

**Outcomes:**

**Conclusion: (**Conclusion to be based on the objectives and outcomes achieved**)**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Grade: AA / AB / BB / BC / CC / CD /DD**

**Signature of faculty in-charge with date**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**References:**

**Books/ Journals/ Websites:**

1. [**https://www.wireshark.org/ \_(software)**](https://en.wikipedia.org/wiki/Cain_and_Abel_(software))
2. [**https://en.wikipedia.org/wiki/Wireshark**](https://en.wikipedia.org/wiki/Wireshark)
3. <https://www.wireshark.org/docs/>
4. https://www.youtube.com/watch?v=UBfSgjUCEi0