KJSCE/IT/SY/SEM III/DCN/2022-23



**Experiment No. 3**

**Title:** Application layer protocols.



(A Constituent College of Somaiya Vidyavihar University)

KJSCE/IT/SY/SEM III/DCN/2022-23

**Batch:A3 Roll No.: 16010421075Experiment No.:3 Aim:** To explore application layer protocols with packet analysis using Wireshark.

**Resources needed**: Internet, Wireshark software (downloaded from the official site)

**Theory**

**Background of Wireshark**

Wireshark is a network packet analyser. Any network packet analyser 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 very

expensive, proprietary. However, with the advent of Wire-shark, all that has changed. Wireshark is perhaps one of the best open source packet analysers 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**

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. The following are some of the 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.

(A Constituent College of Somaiya Vidyavihar University)

KJSCE/IT/SY/SEM III/DCN/2022-23

Create various statistics.  …and a lot more! 

However, to really appreciate its power we have to start using it. Here is a snapshot of Wireshark main menu.



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 support**

A. ATM - capture ATM traffic

B. Bluetooth- capture Bluetooth traffic .

C. Cisco HDLC links - capture on synchronous links using Cisco HDLC encapsulation. D. Ethernet- capture on different topologies, including

switched networks.

E. Framerelay – captures framerelay traffic.

F. IrDA capture IrDA traffic - currently limited to Linux.

G. PPP links - capture on dial-up lines, ISDN connections and PPP-over-Ethernet (PPPoe, e.g. ADSL)

H. Tokenring - capture on Tokenring adapters, promiscuous mode and switched networks

(A Constituent College of Somaiya Vidyavihar University)

I. USB- capture of raw USB traffic

KJSCE/IT/SY/SEM III/DCN/2022-23 

J. WLAN- capture on 802.11 (WLAN, Wi-Fi) interfaces, including "monitor mode" , raw 802.11 headers and radio information

**Virtual interfaces:**

**1.** Loopback - capture traffic from a machine to itself, including the IP address 127.0.0.1 **2.** Pipes - use UNIX pipes to capture from other applications (even remote!) **3.** VLAN – capture VLAN traffic, including VLAN tags.

In addition to this, Wireshark can do following things.

**1.**Import files from many other capture programs.

**2.**Wireshark can open packets captured from a large number of other capture programs. **3.**Export files for many other capture programs.

**4.**Wireshark can save packets captured in a large number of formats of other capture programs.

**5.**Can be used as a protocol decoder

**----------------------------------------------------------------------------------------------------------- Implementation:** 

1. Start the machine as an administrator.

2. Start internet.

3. Go to the official website of Wireshark. (www.wireshark.org) and download the old stable version of Wireshark for 32 bit windows operating system.

4. After successful installation you will get the blue icon of Wireshark on the desktop. 5. Click on the icon and start the software.

6. Choose an interface and start capturing the packets.

7. Study the packet details of any one application layer protocols.

8. Understand color code in details.

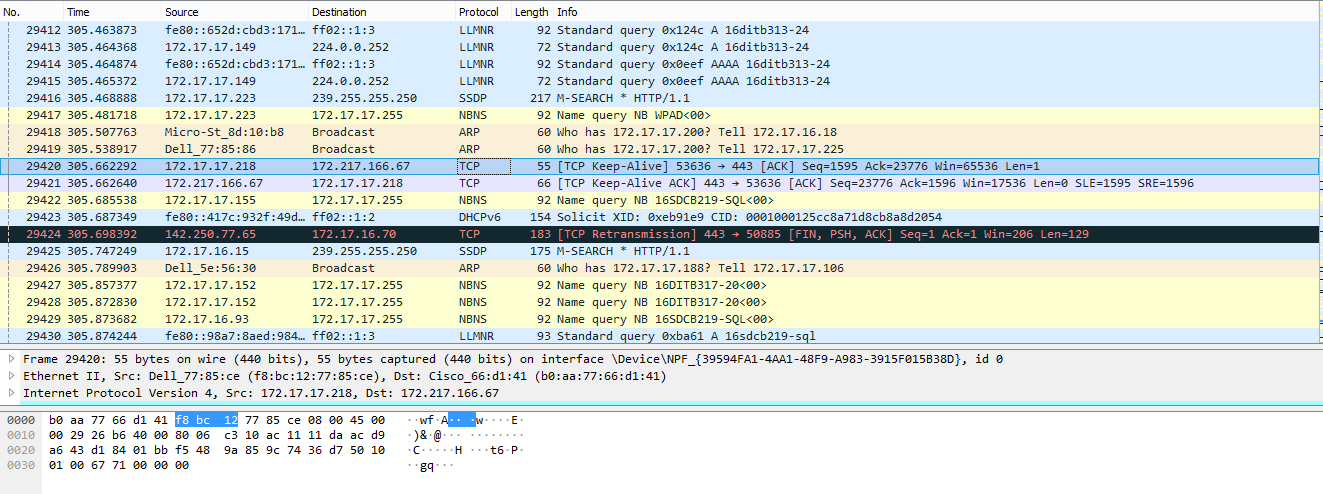
9. Perform the statistics for captured application layer protocol packet. (Every student should perform for different protocol.)

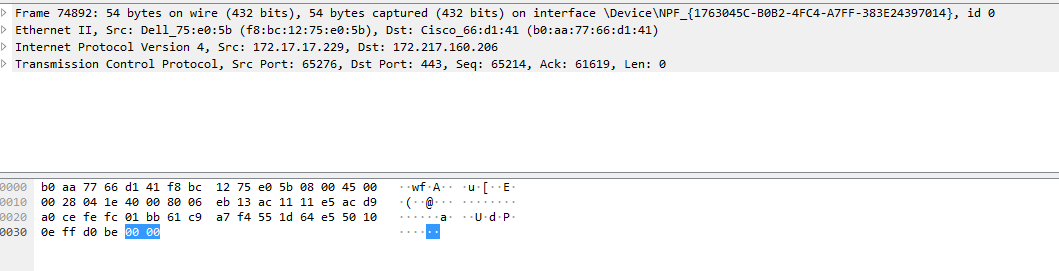
10. Show the output to the teacher and get it approved.

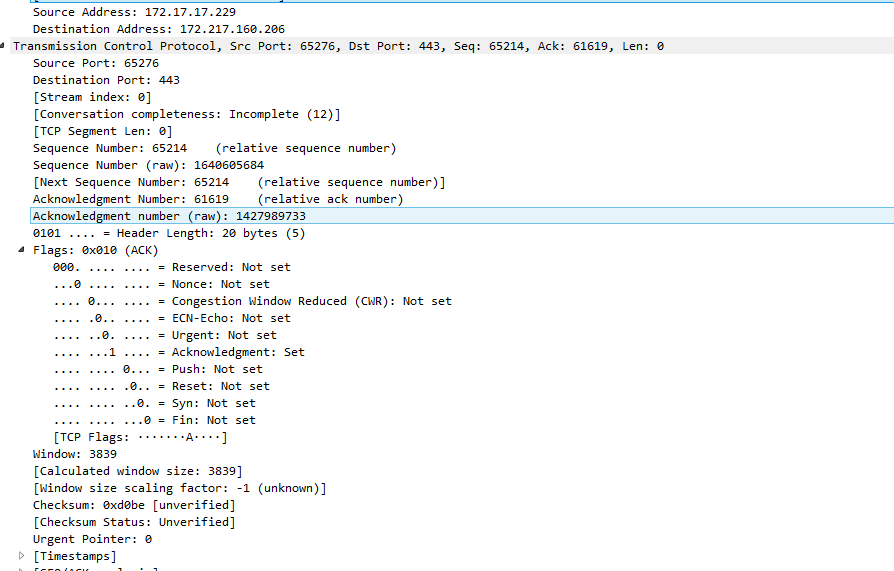
**----------------------------------------------------------------------------------------------------------- Results: (Program printout with output / Document printout as per the format)**

Screenshots for

1. Capturing a packet.







2. Color coding of different protocols.

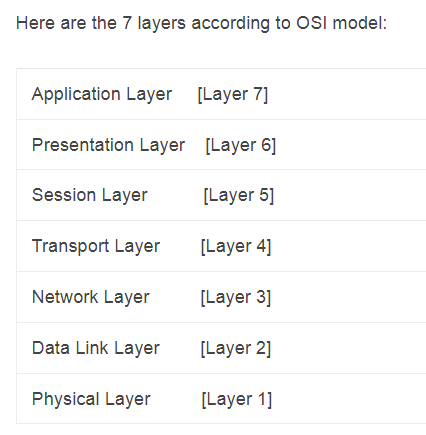
3. Statistics for the application layer protocol you have chosen.

**Questions:**

1. **What is the difference between Wireshark software and NMAP software?**

|  |  |  |
| --- | --- | --- |
| **Gerne of comparison** | **Wireshark** | **NMAP** |
| Purpose of use | Nmap is primarily chosen for the use case of network scanners. Network scanner enables information regarding groups, shares, services, usernames of the computers in the network to be fetched and saved for future processing. | Wireshark falls into the category of packet scanner. The objective is similar to network sniffing where network traffic that is a part of the entire larger network of the system is intercepted and logged for future processing. |
| Features | Nmap comprises various features very different from that of Wireshark in order to fulfill the task of network scanning. Some of the features include host discovery, scanning of ports, detecting versions of the applications, fingerprinting of TCP/IP stack, and scriptable interaction. | Wireshark makes sure it encompasses the required features in order to fulfill the task of packet scanning. These features include capturing packets of the different protocols, parsing, and displaying the fields from the capture only on the types of network that pcap supports. |
| Written in | Nmap is written in languages like C, C++, Python, Lua although it is a cross-platform tool | Wireshark is written only in C and C++ although it being a cross-platform tool. |

1. **At which of the OSI layer Wireshark runs?**





(A Constituent College of Somaiya Vidyavihar University)

KJSCE/IT/SY/SEM III/DCN/2022-23

1. **Just write down the names of the softwares which have similar functionality as Wireshark. (open source or proprietary)**

* tcpdump. CloudShark. ...
* Colasoft Capsa. ...
* Sysdig. ...
* Mojo Packets. ...
* SolarWinds RMM

**Outcomes:**

**CO3:**Enumerate the layers of the OSI model and TCP/IP model, their functions and Protocols

**Conclusion:**

**In this experiment we learned about the software wireshark which is network packet analyser and successfully implemented the mapping of tcp header structure using wireshark**

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

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

**References:**

1. Behrouz A Forouzan, “Data Communication and networking”, Tata McGraw hill, India, 4thEdition

2. http://www.wireshark.org

3. Wireshark user manual.



(A Constituent College of Somaiya Vidyavihar University)