Department of Computer Engineering

TE: SEM V Subject: CN

Experiment: 02

Aim: Use Wireshark to understand the operation of TCP/IP layers :

Ethernet Layer : Frame header, ● Frame size etc.

● Data Link Layer : MAC address, ARP (IP and MAC address binding)

● Network Layer : IP Packet (header, fragmentation), ICMP (Query and Echo)

● Transport Layer: TCP Ports, TCP handshake segments etc.

● Application Layer: DHCP, FTP, HTTP header formats

Description:

Wireshark is an open source tool for profiling network traffic and analyzing packets. Such a tool is often referred to as a network analyzer, network protocol analyzer or sniffer.
Wireshark, formerly known as Ethereal, can be used to examine the details of traffic at a variety of levels ranging from connection-level information to the bits that make up a single packet.Packet capture can provide a network administrator with information about individual packets such as transmit time, source, destination, protocol type and header data. This information can be useful for evaluating security events and troubleshooting network security device issues.
Wireshark will typically display information in three panels. The top panel lists frames individually with key data on a single line. Any single frame selected in the top pane is further explained in the tool's middle panel. In this section of the display, Wireshark shows packet details, illustrating how various aspects of the frame can be understood as belonging to the data link layer, network layer, transport layer or application layer. Finally, Wireshark's bottom panel displays the raw frame, with a hexadecimal rendition on the left and the corresponding ASCII values on the right.
Wireshark has a rich feature set which includes the following:
• Deep inspection of hundreds of protocols, with more being added all the time
• Live capture and offline analysis
• Standard three-pane packet browser
• Multi-platform: Runs on Windows, Linux, OS X, Solaris, FreeBSD, NetBSD, and many others
• Captured network data can be browsed via a GUI, or via the TTY-mode TShark utility
• The most powerful display filters in the industry
• Rich VoIP analysis
• Read/write many different capture file formats: tcpdump (libpcap), Pcap NG, Catapult DCT2000, Cisco Secure IDS iplog, Microsoft Network Monitor, Network General Sniffer® (compressed and uncompressed), Sniffer® Pro, and NetXray®, Network Instruments Observer, NetScreen snoop, Novell LANalyzer, RADCOM

WAN/LAN Analyzer, Shomiti/Finisar Surveyor, Tektronix K12xx, Visual Networks Visual UpTime, WildPackets EtherPeek/TokenPeek/AiroPeek, 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, FDDI, and others (depending on your platform)

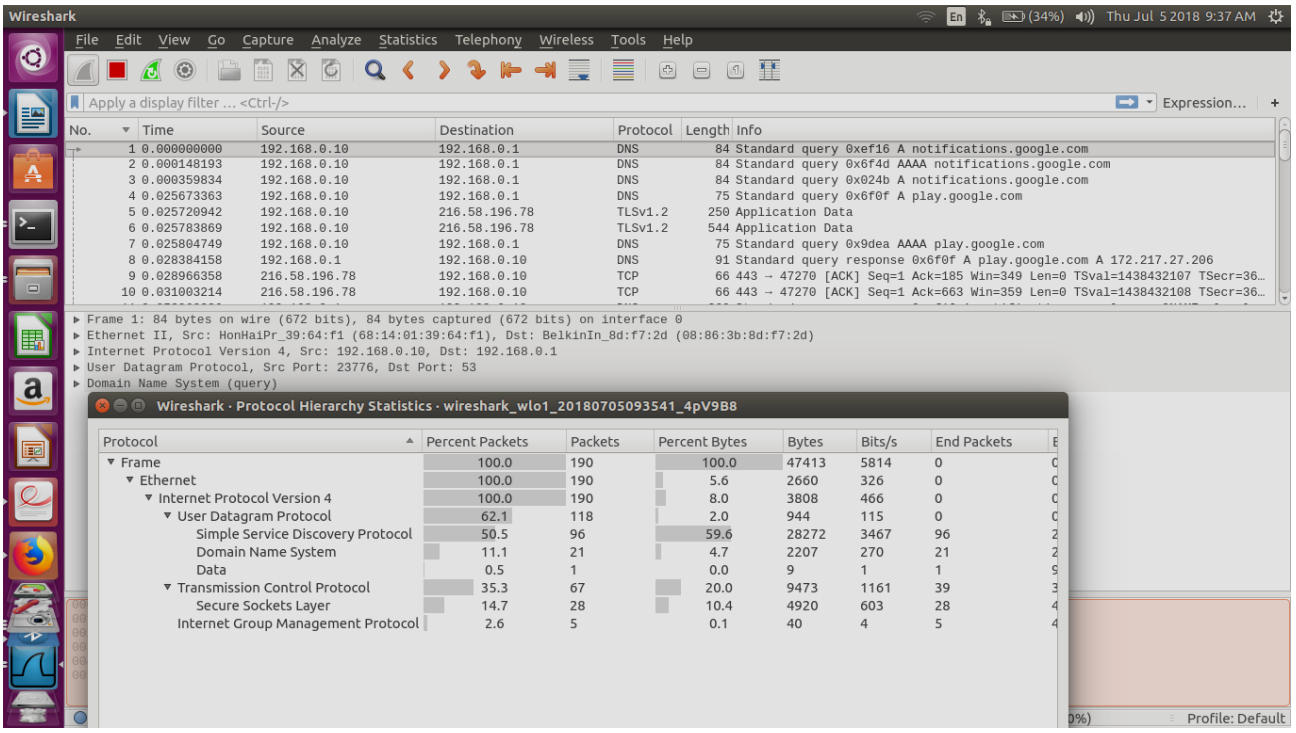
• Decryption support for many protocols, including IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP, and WPA/WPA2

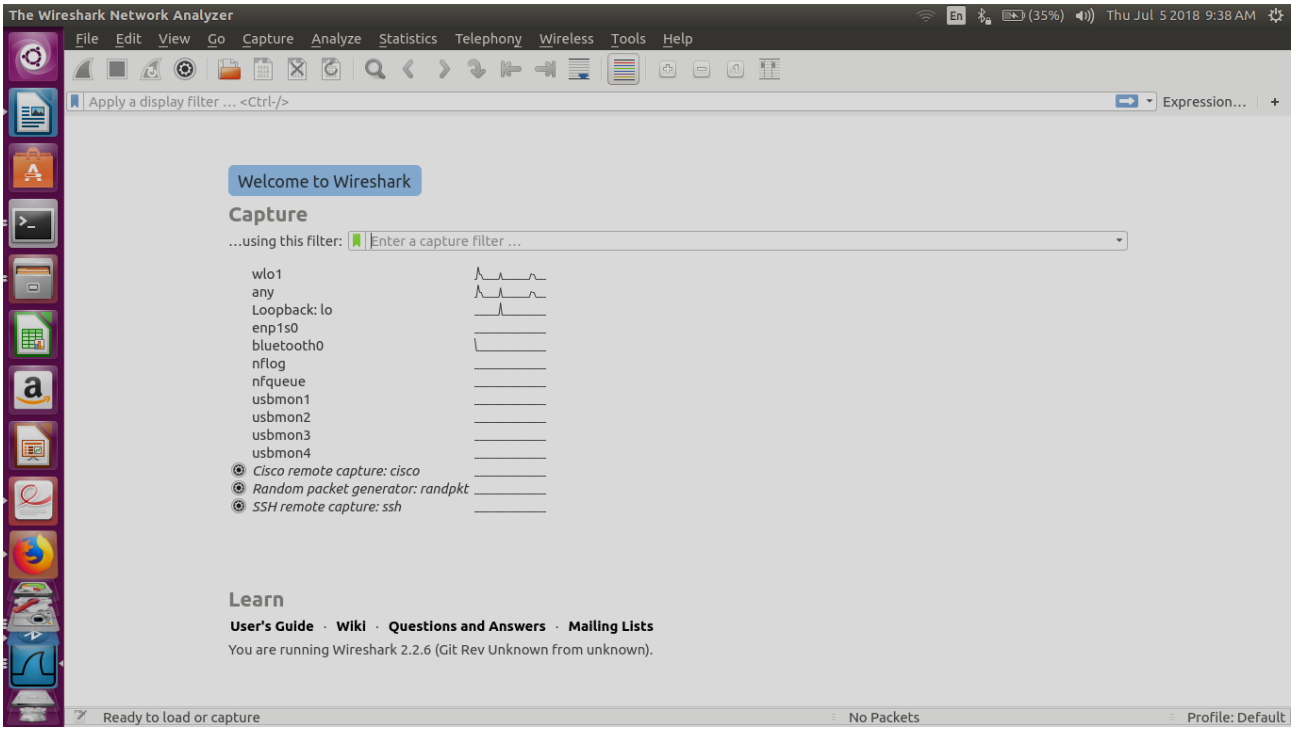
• Coloring rules can be applied to the packet list for quick, intuitive analysis

• Output can be exported to XML, PostScript®, CSV, or plain text

Installation

Sudo apt-get install wireshark





Packet List

The packet list pane, located at the top of the window, shows all packets found in the active capture file. Each packet has its own row and corresponding number assigned to it, along with each of these data points.

• Time: The timestamp of when the packet was captured is displayed in this column, with the default format being the number of seconds (or partial seconds) since this specific capture file was first created. To modify this format to something that may be a bit more useful, such as the actual time of day, select the Time Display Format option from Wireshark's View menu - located at the top of the main interface.

• Source: This column contains the address (IP or other) where the packet originated.

• Destination: This column contains the address that the packet is being sent to.

• Protocol: The packet's protocol name (i.e., TCP) can be found in this column.

• Length: The packet length, in bytes, is displayed in this column.

• Info: Additional details about the packet are presented here. The contents of this column can vary greatly depending on packet contents.

When a packet is selected in the top pane, you may notice one or more symbols appear in the first column. Open and/or closed brackets, as well as a straight horizontal line, can indicate whether or not a packet or group of packets are all part of the same back-and-forth conversation on the network. A broken horizontal line signifies that a packet is not part of said conversation.

Conclusion:

Studied Wireshark as a data analyser in TCP/IP layers.

Some filters :

```
ip.src == 10.0.0.5
ip.src != 10.0.0.5
frame.len > 10
frame.len < 128
sip.To contains "a1762"
ip.src==192.168.5.63&&192.168.10.5
arp
dns
http
tcp
udp
tcp.port == 80 || tcp.port == 443 || tcp.port == 8080
```