NETWORKING & SYSTEM ADMINISTRATION LAB

Name: vismaya

Roll No: 54

Batch: B

Date: 06-06-2022

Experiment No: 26

Aim

Wireshark

Procedure

Commands:

$ sudo apt update

```
mca@T70:~$ sudo apt update
[sudo] password for mca:
Err:1 http://ppa.launchpad.net/jonathonf/python-3.6/ubuntu bionic InRelease
  403  Forbidden [IP: 185.125.190.52 80]
Get:2 https://dl.google.com/linux/chrome/deb stable InRelease [1,811 B]
Hit:3 http://archive.ubuntu.com/ubuntu bionic InRelease
Hit:4 http://ppa.launchpad.net/webupd8team/java/ubuntu bionic InRelease
Get:5 https://dl.google.com/linux/chrome/deb stable/main amd64 Packages [1,097 B]
Reading package lists... Done
E: Failed to fetch http://ppa.launchpad.net/jonathonf/python-3.6/ubuntu/dists/bionic/InRelease  403  F
E: The repository 'http://ppa.launchpad.net/jonathonf/python-3.6/ubuntu bionic InRelease' is no longer
N: Updating from such a repository can't be done securely, and is therefore disabled by default.
N: See apt-secure(8) manpage for repository creation and user configuration details.
```

$ sudo apt install wireshark

```
mca@T70:~$ sudo apt install wireshark
Reading package lists... Done
Building dependency tree
Reading state information... Done
wireshark is already the newest version (2.4.5-1).
The following packages were automatically installed and are no longer required:
  debhelper dh-autoreconf dh-strip-nondeterminism libarchive-cpio-perl
  libfile-stripnondeterminism-perl libmail-sendmail-perl libpcre16-3
  libpcre3-dev libpcre32-3 libpcrecpp0v5 libssl-dev libssl-doc
  libsys-hostname-long-perl php-common php-pear php-xml php7.2-cli
  php7.2-common php7.2-json php7.2-opcache php7.2-readline php7.2-xml
  pkg-php-tools po-debconf shtool
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

$ sudo adduser $mca wireshark

```
mca@T70:~$ sudo adduser $mca wireshark
adduser: The group `wireshark' already exists.
```

$ sudo wireshark

No.	Time	Source	Destination	Protocol	Length	Info
361	16.097477381	142.250.193.110	192.168.6.224	QUIC	68	443 → 41231 Len=26[Malformed Packet]
362	16.318072351	Sophos_6b:54:cf	Broadcast	ARP	60	Who has 192.168.6.94? Tell 192.168.6.100
363	16.438971664	192.168.6.74	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
364	16.498148339	192.168.6.224	142.250.193.110	QUIC	75	41231 → 443 Len=33[Malformed Packet]
365	16.517895311	142.250.193.110	192.168.6.224	QUIC	68	Payload (Encrypted), PKN: 13691
366	16.574050085	Sophos_6b:54:cf	Broadcast	ARP	60	Who has 192.168.6.17? Tell 192.168.6.100
367	16.634001154	fe80::3cf5:bd56:74d…	ff02::1:ffc6:78d5	ICMPv6	86	Neighbor Solicitation for fe80::1ccb:d3e:e4c6:78d5 f
368	16.666927225	Sophos_6b:54:cf	Broadcast	ARP	60	Who has 192.168.6.22? Tell 192.168.6.100
369	16.751027809	88:3a:30:6f:3d:da	Spanning-tree-(for-…	STP	119	MST. Root = 32768/0/08:36:c9:16:1d:25 Cost = 20000
370	16.832926565	HewlettP_a7:c0:55	Broadcast	ARP	60	Who has 192.168.90.1? Tell 192.168.90.60
371	16.906308342	192.168.6.198	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1

▶ Frame 1: 217 bytes on wire (1736 bits), 217 bytes captured (1736 bits) on interface 0
▶ Ethernet II, Src: 0c:9d:92:0f:6b:e2 (0c:9d:92:0f:6b:e2), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
▶ Internet Protocol Version 4, Src: 192.168.6.93, Dst: 239.255.255.250
▶ User Datagram Protocol, Src Port: 55077, Dst Port: 1900
▶ Simple Service Discovery Protocol