

INDEX

NAME: A. Kavin

STD 11 ^{month} not year

GSE-B
SEC. :

ROLL NO. 22070122

[illegible]

Exp. NO 05
Date : 09-08-2024

Practical-5

Aim

Experiments on packet capture tool :
Wireshark

Packet Sniffer

- * Sniffs message being sent/received from/by your computer
- * Store and display the contents of the various protocol fields in the messages
- * Passive program
 - never sends packets itself
 - no packets addressed to it
 - receives a copy of all packets

Packet sniffer structure diagnostic tool

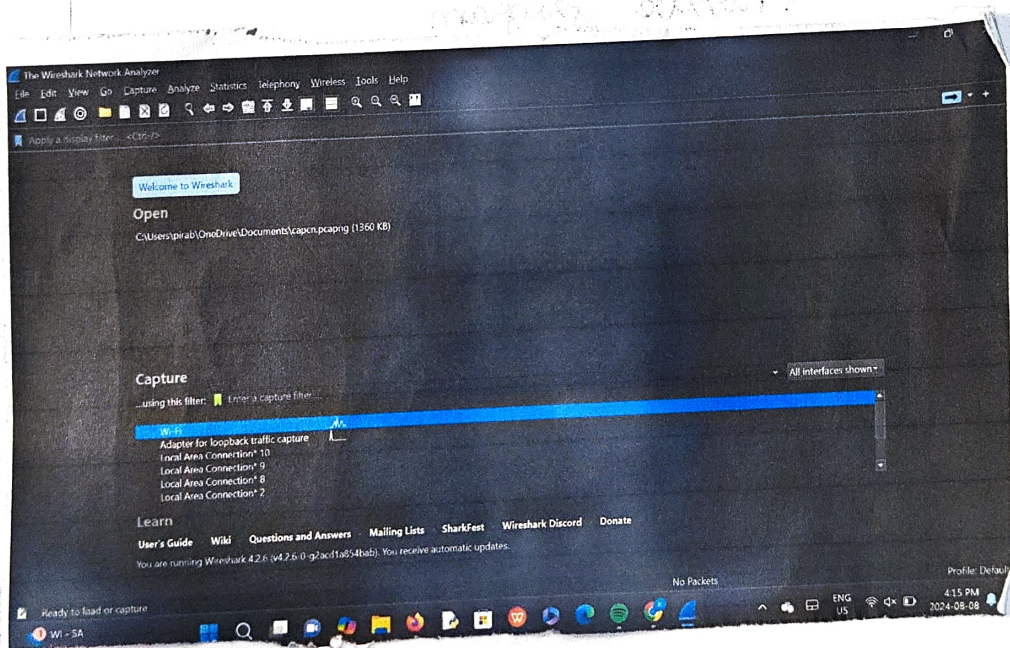
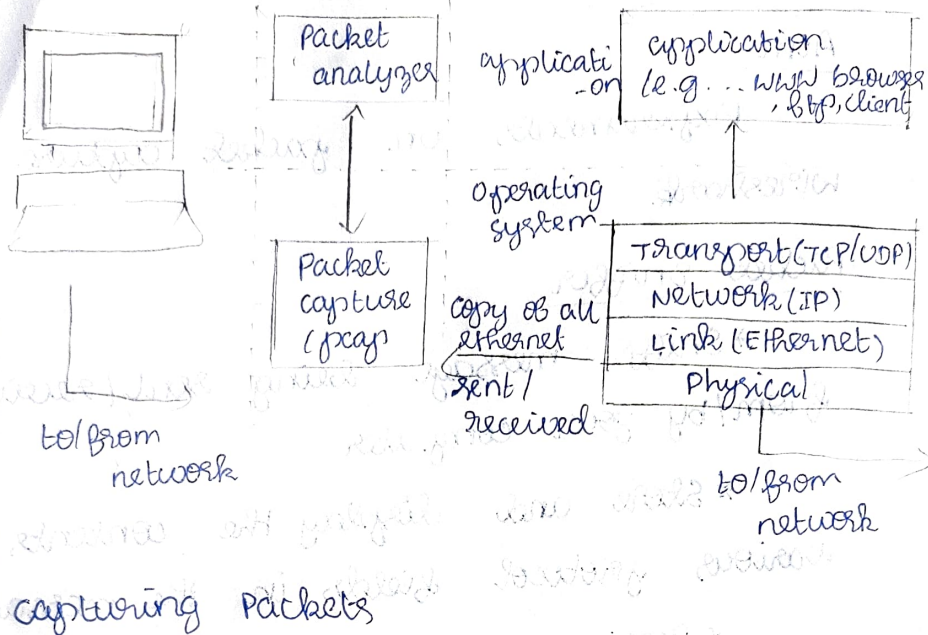
* Tcpdump

- E.g. tcpdump -nn host 10.129.41.2 -w exe3.out

* Wireshark

- ~~wireshark~~ -n exe3.out

Packet sniffer



Packet lists, details and bytes

The image shows the Wireshark interface with a packet list on the left and packet details on the right. The packet list shows a series of TCP packets, with packet 155 highlighted. The details pane shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The TCP section shows a sequence number of 2833889402 and an acknowledgment number of 1396168509.

No.	Time	Source	Destination	Protocol	Length	Info
1547	195.000475	2620.1ec.bbf:58	2400:afef:3a:1037:2	TCP	74	453 → 40078 [ACK] Seq=5850 Ack=1023 Win=2496 Len=0
1548	195.000475	2620.1ec.bbf:58	2400:afef:3a:1037:2	TLSv1.3	153	Application Data
1549	195.000475	2400:afef:3a:1037:2	2620.1ec.bbf:58	TCP	74	40078 → 453 [ACK] Seq=1921 Ack=6088 Win=130816 Len=0
1551	195.000475	2400:afef:3a:1037:2	2620.1ec.bbf:58	TLSv1.3	107	Application Data
1552	195.174546	2400:afef:3a:1037:2	2620.1ec.bbf:58	TCP	74	40078 → 453 [ACK] Seq=628 Ack=4254 Win=130560 Len=0
1553	195.417230	2400:afef:3a:1037:2	2620.1ec.bbf:58	TCP	74	40078 → 453 [ACK] Seq=628 Ack=4254 Win=130560 Len=0
1554	195.417230	2400:afef:3a:1037:2	2620.1ec.bbf:58	TCP	74	40078 → 453 [ACK] Seq=628 Ack=4254 Win=130560 Len=0
1555	195.417230	2400:afef:3a:1037:2	2620.1ec.bbf:58	TCP	74	40078 → 453 [ACK] Seq=628 Ack=4254 Win=130560 Len=0
1556	195.417230	2400:afef:3a:1037:2	2620.1ec.bbf:58	TCP	74	40078 → 453 [ACK] Seq=628 Ack=4254 Win=130560 Len=0
1557	195.417230	2400:afef:3a:1037:2	2620.1ec.bbf:58	TCP	74	40078 → 453 [ACK] Seq=628 Ack=4254 Win=130560 Len=0
1558	195.417230	2400:afef:3a:1037:2	2620.1ec.bbf:58	TCP	74	40078 → 453 [ACK] Seq=628 Ack=4254 Win=130560 Len=0

Frame 1: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface 11, Src: 2620.1ec.bbf:58, Dst: 2400:afef:3a:1037:2

Internet Protocol Version 4, Src: 2620.1ec.bbf:58, Dst: 2400:afef:3a:1037:2

Transmission Control Protocol, Src Port: 58, Dst Port: 453

Source Port: 58

Destination Port: 453

(Stream index: 0)

Conversation completeness: Incomplete (8)

TCP Segment Len: 74

Sequence Number: 1 (relative sequence num)

Sequence Number (raw): 2833889402

Next Sequence Number: 2 (relative sequence num)

Acknowledgment Number: 1 (relative ack num)

Acknowledgment Number (raw): 1396168509

0101 ... = Header Length: 20 bytes (5)

Flags: 0x018 (PSH, ACK)

Window: 128

[Calculated window size: 128]

[Window size scaling factor: -1 (unknown)]

capturing Filters

The image shows the Wireshark capture filter dialog box. The filter name is "Wireshark Capture Filters". The filter expression is "ethernet address 00:00:5e:00:53:00". The filter is applied to the capture filter. The dialog box also shows the packet list and details pane.

Filter Name: Wireshark Capture Filters

Filter Expression: ethernet address 00:00:5e:00:53:00

Filter: ethernet address 00:00:5e:00:53:00

Filter: ethernet type 0x0800 (ARP)

Filter: not broadcast and not multicast

Filter: not arp

Filter: host 192.0.2.1

Filter: ip6

Filter: host 2001:db8:1

Filter: tcp

Filter: udp

Filter: not port 53

Filter: port 80

Filter: tcp port http

Filter: not arp and port not 53

Filter: Non-HTTP and non-SMTP to/from www.wireshark.org

Filter: not port 80 and not port 25 and host www.wireshark.org

OK Cancel Help

The image shows the Wireshark interface with a packet list on the left and packet details on the right. The packet list shows a series of DNS queries and responses, with packet 1547 highlighted. The details pane shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The DNS section shows a query for "google".

No.	Time	Source	Destination	Protocol	Length	Info
1547	283.298386	192.168.34.236	192.168.34.45	DNS	107	Standard query 0x2131 HTTPS optimizationguide-pa.googleapis.com
1548	283.298513	192.168.34.236	192.168.34.45	DNS	107	Standard query 0x2131 AAAA optimizationguide-pa.googleapis.com
1549	283.298622	192.168.34.236	192.168.34.45	DNS	107	Standard query 0x2131 AAAA optimizationguide-pa.googleapis.com
1550	283.298731	192.168.34.45	192.168.34.236	DNS	165	Standard query response 0x2131 HTTPS optimizationguide-pa.googleapis.com SOA nsl.google.com
1551	283.298840	192.168.34.45	192.168.34.236	DNS	220	Standard query response 0x2131 AAAA optimizationguide-pa.googleapis.com
1552	283.298949	192.168.34.45	192.168.34.236	DNS	364	Standard query response 0x2131 AAAA optimizationguide-pa.googleapis.com
1553	283.299058	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1554	283.299167	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1555	283.299276	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1556	283.299385	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1557	283.299494	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1558	283.299603	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1559	283.299712	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1560	283.299821	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1561	283.299930	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1562	283.300039	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1563	283.300148	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1564	283.300257	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1565	283.300366	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1566	283.300475	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1567	283.300584	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1568	283.300693	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1569	283.300802	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1570	283.300911	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1571	283.301020	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1572	283.301129	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1573	283.301238	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1574	283.301347	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1575	283.301456	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1576	283.301565	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1577	283.301674	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1578	283.301783	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1579	283.301892	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1580	283.302001	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1581	283.302110	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1582	283.302219	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1583	283.302328	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1584	283.302437	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1585	283.302546	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1586	283.302655	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1587	283.302764	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1588	283.302873	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1589	283.302982	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1590	283.303091	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1591	283.303200	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1592	283.303309	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1593	283.303418	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1594	283.303527	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1595	283.303636	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1596	283.303745	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1597	283.303854	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1598	283.303963	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1599	283.304072	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1600	283.304181	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1601	283.304290	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1602	283.304399	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1603	283.304508	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1604	283.304617	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1605	283.304726	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1606	283.304835	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1607	283.304944	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1608	283.305053	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1609	283.305162	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1610	283.305271	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1611	283.305380	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1612	283.305489	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1613	283.305598	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1614	283.305707	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1615	283.305816	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1616	283.305925	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1617	283.306034	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1618	283.306143	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1619	283.306252	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1620	283.306361	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1621	283.306470	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1622	283.306579	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1623	283.306688	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1624	283.306797	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1625	283.306906	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1626	283.307015	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1627	283.307124	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1628	283.307233	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1629	283.307342	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1630	283.307451	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1631	283.307560	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1632	283.307669	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1633	283.307778	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1634	283.307887	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1635	283.307996	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1636	283.308105	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1637	283.308214	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1638	283.308323	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1639	283.308432	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1640	283.308541	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1641	283.308650	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1642	283.308759	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1643	283.308868	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1644	283.308977	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1645	283.309086	192.168.34.45	192.168.34.236	DNS	95	Standard query 0x2131 A spclient.wg.spotify.com
1646	283.309195	192.168.34.45	192.168.34.236</			

The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, and Help. The toolbar contains icons for various functions like opening files, saving, and analyzing. The main window is divided into three panes:

- Packet List:** Shows a list of captured packets. The selected packet is #451, an HTTP GET request from 192.168.34.236 to 192.168.34.45.
- Packet Details:** Displays the hierarchical structure of the selected packet. It includes Ethernet II (Source: Intel_Net177C, Destination: 192.168.34.45), Internet Protocol Version 4 (Source: 192.168.34.236, Destination: 192.168.34.45), and Transmission Control Protocol (Source Port: 60038, Destination Port: 80).
- Packet Bytes:** Shows the raw data of the selected packet in hexadecimal and ASCII. The data represents an HTTP GET request for the resource "/".

The status bar at the bottom indicates that 4355 packets are displayed, with the current packet being #451.

[illegible][illegible]

Student's observation

1. Promiscuous mode is a network interface setting that allows card to intercept and read all network packets on network segment
2. NO ARP packets do not have transport layer header
3. DNS primary user UDP for its transport layer protocol
4. HTTP protocol uses port number 80 by default
5. It is a broadcast IP address which is used to send packets to all devices on a specific network segment

Result

9/8/24

Thus the experiments on packet capture tool Wireshark is studied and observed.