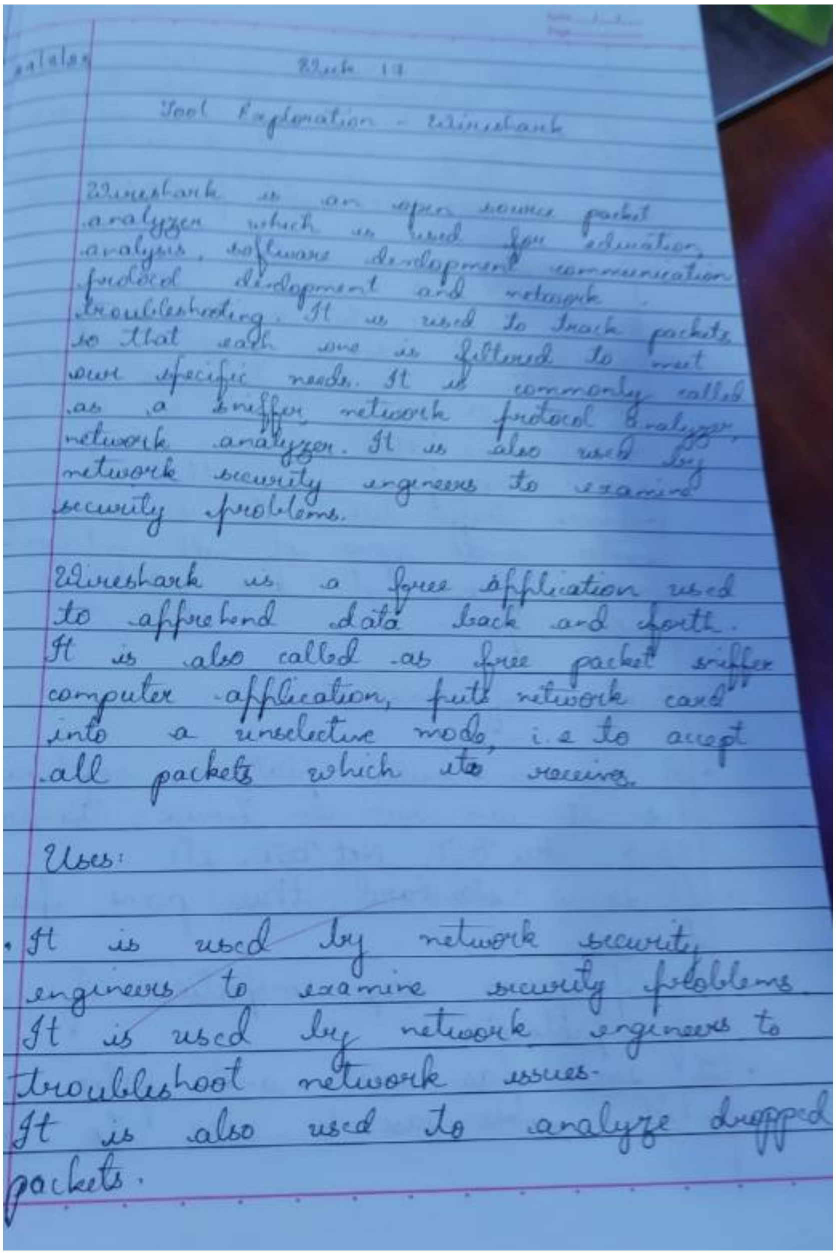
Week 17

Wireshark

Observation :



Week 17

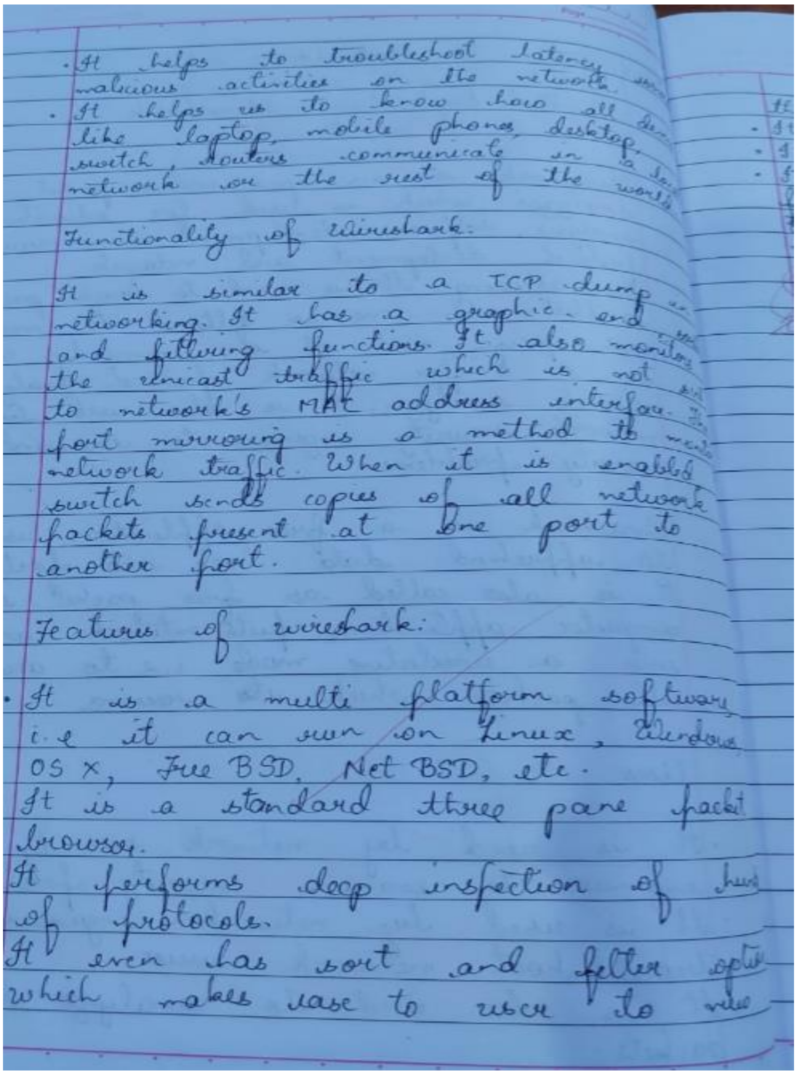
Tool Exploration - Wireshark

Wireshark is an open source packet analyzer which is used for education, analysis, software development communication protocol development and network troubleshooting. It is used to track packets so that each one is filtered to meet our specific needs. It is commonly called as a sniffer, network protocol analyzer, network analyzer. It is also used by network security engineers to examine security problems.

Wireshark is a free application used to apprehend data back and forth. It is also called as free packet sniffer computer application, puts network card into a unselective mode, i.e to accept all packets which its receive.

Uses:

- It is used by network security engineers to examine security problems.
It is used by network engineers to troubleshoot network issues.
It is also used to analyze dropped packets.



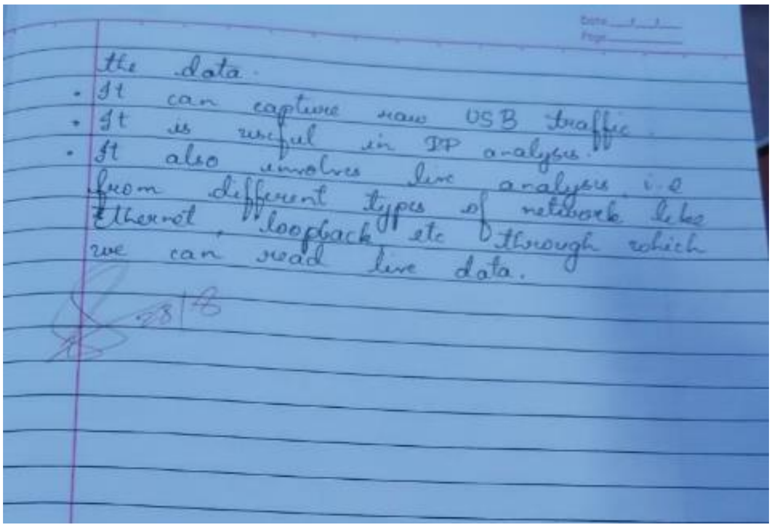
- It helps to troubleshoot latency malicious activities on the network.
- It helps us to know how all de like laptop, mobile phones, desktop, switch, routers communicate in a lo network or the rest of the world.

Functionality of Wireshark:

It is similar to a TCP dump in networking. It has a graphic end and filtering functions. It also monitors the unicast traffic which is not se to network's MAC address interface. Port mirroring is a method to mo network traffic. When it is enabled switch sends copies of all network packets present at one port to another port.

Features of wireshark:

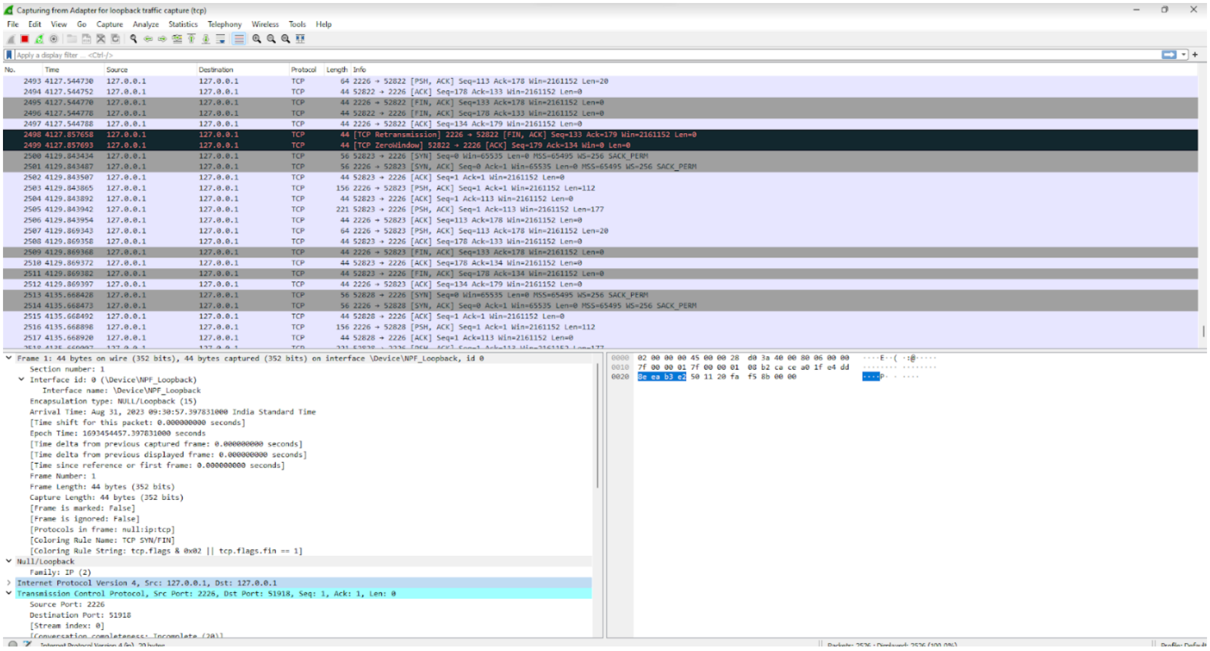
- It is a multi platform software i.e it can run on Linux, Windows OS X, Free BSD, Net BSD, etc.
  It is a standard three pane packet browser.
  It performs deep inspection of hun of protocols.
  It even has sort and filter optio which makes ease to user to view



the data.
- It can capture raw USB traffic.
- It is useful in IP analysis.
- It also involves live analysis i.e from different types of network like Ethernet, loopback etc through which we can read live data.

28/8

Output :



Capturing from Adapter for loopback traffic capture (tcp)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time         Source      Destination  Protocol Length Info
2493 4127.544730  127.0.0.1   127.0.0.1    TCP       64 2226 → 52822 [PSH, ACK] Seq=113 Ack=178 Win=2161152 Len=20
2494 4127.544752  127.0.0.1   127.0.0.1    TCP       44 52822 → 2226 [ACK] Seq=178 Ack=133 Win=2161152 Len=0
2495 4127.544770  127.0.0.1   127.0.0.1    TCP       44 2226 → 52822 [FIN, ACK] Seq=133 Ack=178 Win=2161152 Len=0
2496 4127.544778  127.0.0.1   127.0.0.1    TCP       44 52822 → 2226 [FIN, ACK] Seq=178 Ack=133 Win=2161152 Len=0
2497 4127.544788  127.0.0.1   127.0.0.1    TCP       44 2226 → 52822 [ACK] Seq=134 Ack=179 Win=2161152 Len=0
2498 4127.857658  127.0.0.1   127.0.0.1    TCP       44 [TCP Retransmission] 2226 → 52822 [FIN, ACK] Seq=133 Ack=179 Win=2161152 Len=0
2499 4127.857693  127.0.0.1   127.0.0.1    TCP       44 [TCP ZeroWindow] 52822 → 2226 [ACK] Seq=179 Ack=134 Win=0 Len=0
2500 4129.843434  127.0.0.1   127.0.0.1    TCP       56 52823 → 2226 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
2501 4129.843487  127.0.0.1   127.0.0.1    TCP       56 2226 → 52823 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
2502 4129.843507  127.0.0.1   127.0.0.1    TCP       44 52823 → 2226 [ACK] Seq=1 Ack=1 Win=2161152 Len=0
2503 4129.843865  127.0.0.1   127.0.0.1    TCP      156 2226 → 52823 [PSH, ACK] Seq=1 Ack=1 Win=2161152 Len=112
2504 4129.843892  127.0.0.1   127.0.0.1    TCP       44 52823 → 2226 [ACK] Seq=1 Ack=113 Win=2161152 Len=0
2505 4129.843942  127.0.0.1   127.0.0.1    TCP      221 52823 → 2226 [PSH, ACK] Seq=1 Ack=113 Win=2161152 Len=177
2506 4129.843954  127.0.0.1   127.0.0.1    TCP       44 2226 → 52823 [ACK] Seq=113 Ack=178 Win=2161152 Len=0
2507 4129.869343  127.0.0.1   127.0.0.1    TCP       64 2226 → 52823 [PSH, ACK] Seq=113 Ack=178 Win=2161152 Len=20
2508 4129.869358  127.0.0.1   127.0.0.1    TCP       44 52823 → 2226 [ACK] Seq=178 Ack=133 Win=2161152 Len=0
2509 4129.869368  127.0.0.1   127.0.0.1    TCP       44 2226 → 52823 [FIN, ACK] Seq=133 Ack=178 Win=2161152 Len=0
2510 4129.869372  127.0.0.1   127.0.0.1    TCP       44 52823 → 2226 [ACK] Seq=178 Ack=134 Win=2161152 Len=0
2511 4129.869382  127.0.0.1   127.0.0.1    TCP       44 52823 → 2226 [FIN, ACK] Seq=178 Ack=134 Win=2161152 Len=0
2512 4129.869397  127.0.0.1   127.0.0.1    TCP       44 2226 → 52823 [ACK] Seq=134 Ack=179 Win=2161152 Len=0
2513 4135.668428  127.0.0.1   127.0.0.1    TCP       56 52828 → 2226 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
2514 4135.668473  127.0.0.1   127.0.0.1    TCP       56 2226 → 52828 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
2515 4135.668492  127.0.0.1   127.0.0.1    TCP       44 52828 → 2226 [ACK] Seq=1 Ack=1 Win=2161152 Len=0
2516 4135.668898  127.0.0.1   127.0.0.1    TCP      156 2226 → 52828 [PSH, ACK] Seq=1 Ack=1 Win=2161152 Len=112
2517 4135.668920  127.0.0.1   127.0.0.1    TCP       44 52828 → 2226 [ACK] Seq=1 Ack=113 Win=2161152 Len=0
2518 4135.669007  127.0.0.1   127.0.0.1    TCP      221 52828 → 2226 [PSH, ACK] Seq=1 Ack=113 Win=2161152 Len=177
```

```
Frame 1: 44 bytes on wire (352 bits), 44 bytes captured (352 bits) on interface \Device\NPF_Loopback, id 0
    Section number: 1
  Interface id: 0 (\Device\NPF_Loopback)
      Interface name: \Device\NPF_Loopback
    Encapsulation type: NULL/Loopback (15)
    Arrival Time: Aug 31, 2023 09:30:57.397831000 India Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1693454457.397831000 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 44 bytes (352 bits)
    Capture Length: 44 bytes (352 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: null:ip:tcp]
    [Coloring Rule Name: TCP SYN/FIN]
    [Coloring Rule String: tcp.flags & 0x02 || tcp.flags.fin == 1]
Null/Loopback
    Family: IP (2)
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
Transmission Control Protocol, Src Port: 2226, Dst Port: 51918, Seq: 1, Ack: 1, Len: 0
    Source Port: 2226
    Destination Port: 51918
    [Stream index: 0]
    [Conversation completeness: Incomplete (20)]
```

```
0000  02 00 00 00 45 00 00 28  d0 3a 40 00 80 06 00 00   ····E··( ·:@·····
0010  7f 00 00 01 7f 00 00 01  08 b2 ca ce a0 1f e4 dd   ········ ········
0020  8e ea b3 e2 50 11 20 fa  f5 8b 00 00               ····P· · ····
```

Internet Protocol Version 4 (ip), 20 bytes
Packets: 2526 · Displayed: 2526 (100.0%)
Profile: Default