

Ex. No: 4

04-08-25

Experiment on Packet capture tool using

Wifeshark

Object: To understand the working of wifeshark.

(contd.) Aim: To observe the working of wifeshark.

(also monitoring attack & mitigation)

Experiments on Packet capture tool wifeshark

What is wifeshark?

A network analysis tool that captures real-time network packets and displays them in human-readable format.

Key features:

- Real-time packet capture
- Protocol decoding using dissectors
- Filtering
- color coding for better analysis
- Traffic browsing and smart statistics

uses:-

- Network admins: Troubleshoot network issues
- Security engineer: Analyze security incidents
- Learners: Understand protocols, internets

How to get wifeshark and installed

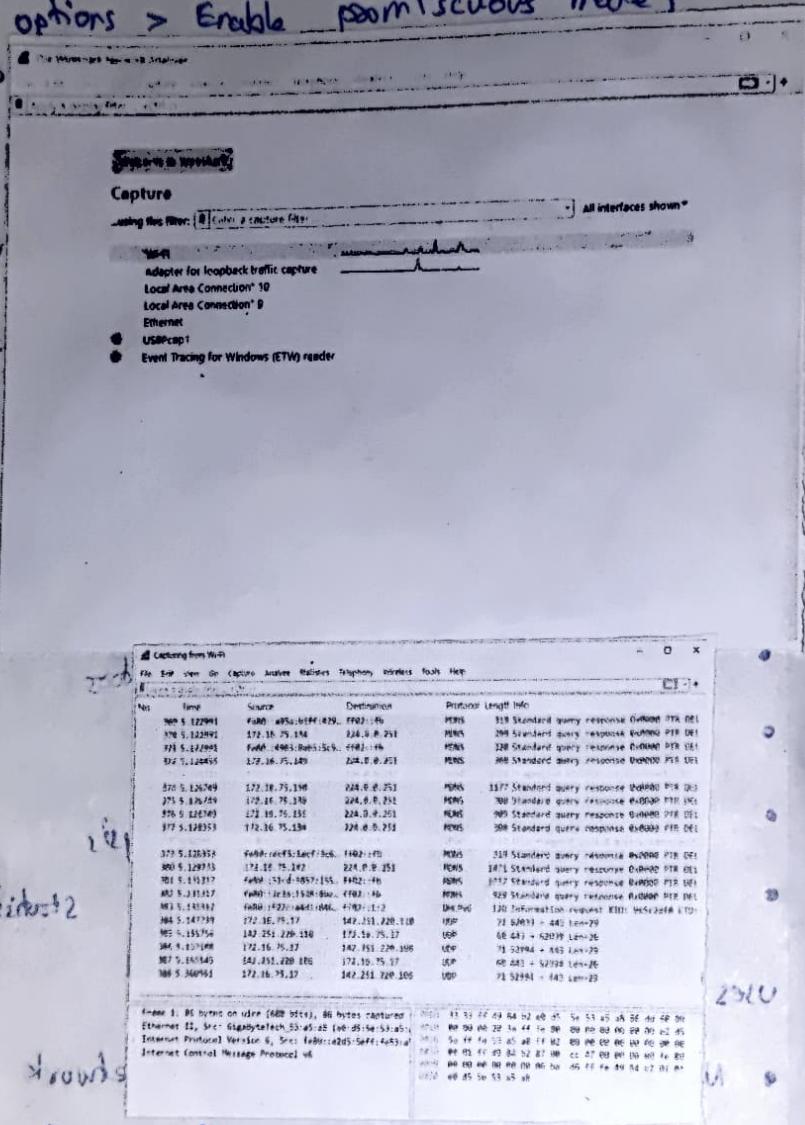
- windows/macos: Download from official website
- linux/ubuntu: Available in package manager of Ubuntu Software centre

Capturing Packets:

- Launch wifeshark and double click a network interface

Now lost weight to 20 lbs. b.w. 187-1

- Packets appear ~~> 1 packet~~ in real-time and include all traffic if promiscuous mode is enabled (Capture options > Enable promiscuous mode)



20228 1000's

The ~~old~~ Packet lines work nights & hours

- **Packet list pane:** lists all captured packets!

Selecting one shows more details of what

- Packet Byte Panel shows packet data in hex

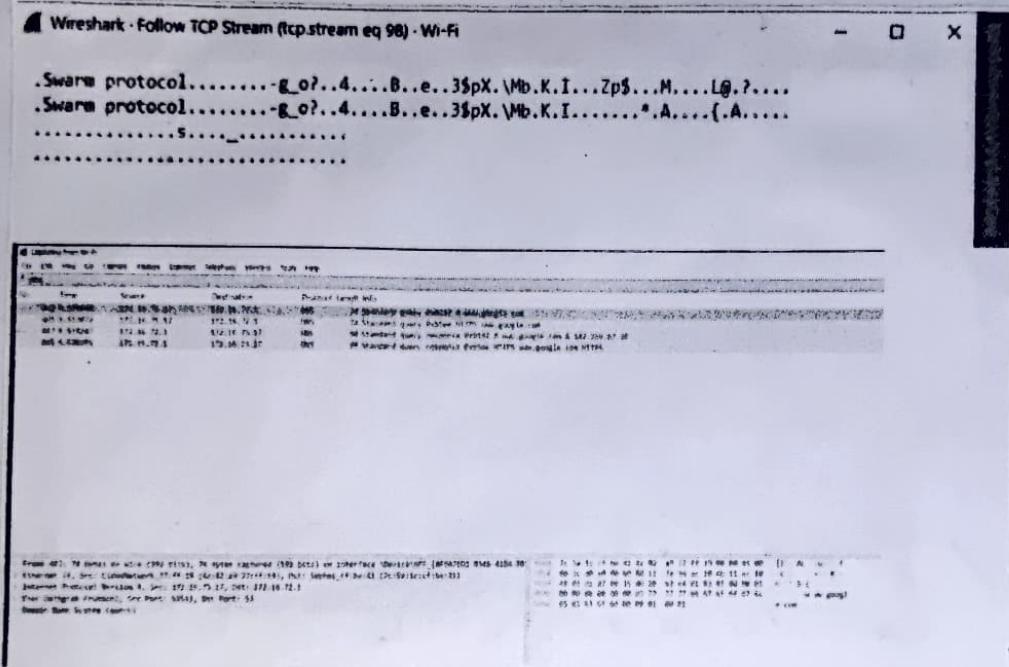
69 ~~suppose~~ ~~suppose~~ and ASC 11 in Malaysia : introduce / xin

class constraint structure

: ~~standard~~ periodique

color coding:

- Light purple = TCP
- Light blue = UDP
- Black = Error packets

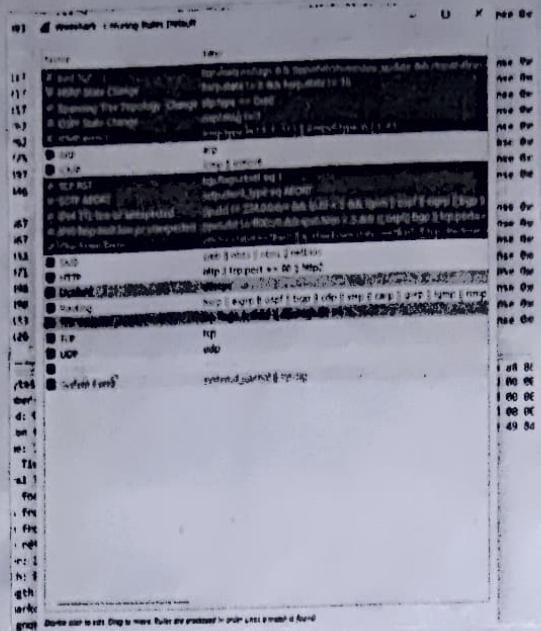


• Sample captures of switching off sites.

- Load sample captures from wireshark's wiki via File > open
- Save your own captures using File > save.

Filtering Packets:

- Use the filter bar to isolate traffic (e.g. type ~~dns~~ dns to see DNS packets).
- ~~Press Enter or click Apply to use the filter~~
- Access default/custom filter via Analyze > Display filters.



Following TCP streams!

- Right-click a packet → follow > TCP stream (or other protocols).
 - close the windows to ~~auto~~ → ^{selected} apply a filter

is also in conversation with Signal book.

~~negative~~ ~~affirmative~~

and π into complex numbers and back again.

• state policy

Inspecting Packets set off AB ab BB

- click a packet ~~to see it in detail~~
 - Right-click protocol ~~Predict~~ → ~~Apply as~~
~~filters to filter based on its IP~~

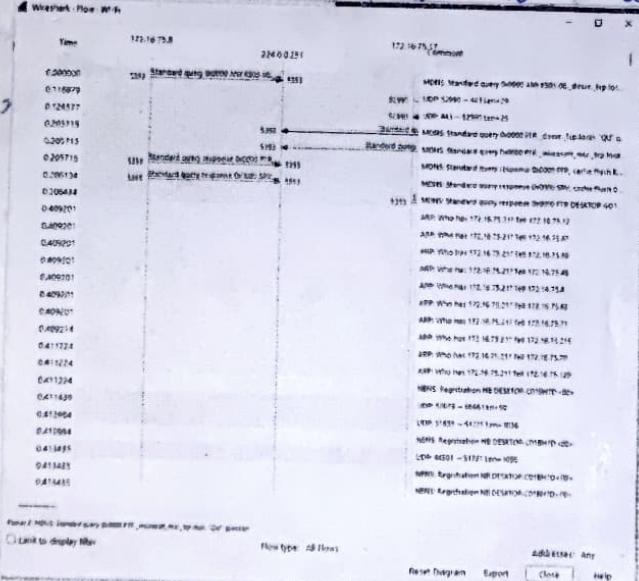
154

980 00 001 10002 1821 64128 47 8

Flow Graph

near' at dragon wall - esthetic s.

- Use Statistics > Flow graph to visualize



Capturing and analysing packets using wireshark

tool.

~~Task : Capture 100 packets from Ethernet Interface~~

~~Procedure~~

- Select local Area connection wolf 256kbit/s
 - Capture > options → Set Stop after 100 packets.

- click start

- save packets

1. Filter : Display TCP/UDP Packets & Show Flow Graph

Procedure

- start capture as above

- In filter bar, search tcp or udp

- Statistics > Flow Graph to view

• Save packets.

2. Filter : Display only ARP Packets

Procedure

- start capture as above

- In filter bar, type arp

- Save packets

3. Filter : Display only DNS Packets & Show Flow Graph

Procedure :

- start capture as above settings : start

- In filter bar, type dns

- Statistics > Flow Graph to view

- Save packets.

- 4) Filter: Display only HTTP Packets protocol.
 (ossible i.e. broadcast or not?)
- Start capture as above
 - In filter box, type http
 - Point right U, of web show (225.225)
 - Save packets.

student observation :

1) what is promiscuous mode?

Promiscuous mode allows a network card to capture all packets on a network.
 It's used in tools like wireshark for monitoring.

2) Does ARP packets have transport layer header?

Explain.

No, ARP works at the data link layer and does not use transport layer headers like TCP or UDP.

3) which transport layer protocol is used by DNS?

Dns primarily uses UDP on port 53 and uses TCP for larger data like zone transfer.

4) what is the port number used by http
Protocol?

The default port for HTTP protocol is

5) what is broadcast IP address?

A broadcast IP address (e.g., 255.255.255.255) sends data to all hosts in a local network.

→ broadcast traffic

(shown ~~broadcasting~~ in traffic)

Hosts → works shown 200002700000

Network → doing the subnets of 600

→ problem with broadcast will block in how the

(subset equal broadcast not doing 49A and (

→ in layer 2

two equal broadcast all the 200002700000

→ ARP after broadcast equal broadcast own from 2000

→ 9000

Result? → broadcast equal broadcast done (

but see, too) thus 90 the 100002700000 packet

network was 01110100000000000000000000000000

is executed and packets are captured.

→ if broadcast contains trap set in host (A)

→ 100002700000

→ interface 90 with set trap think 90