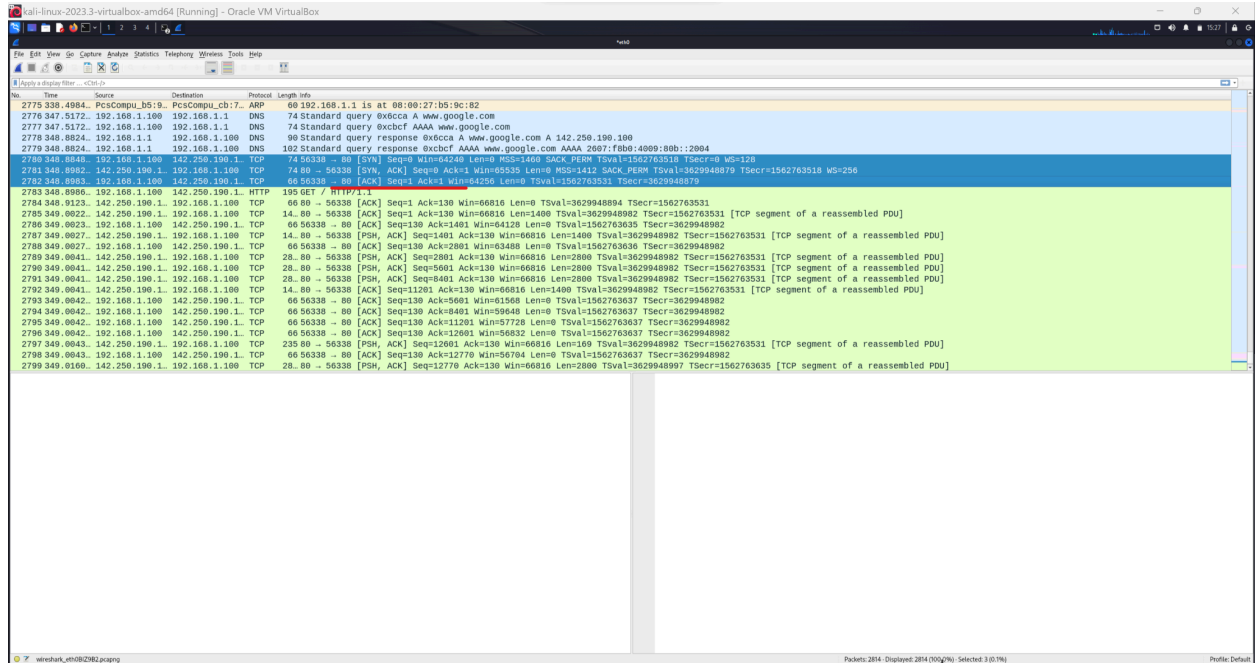
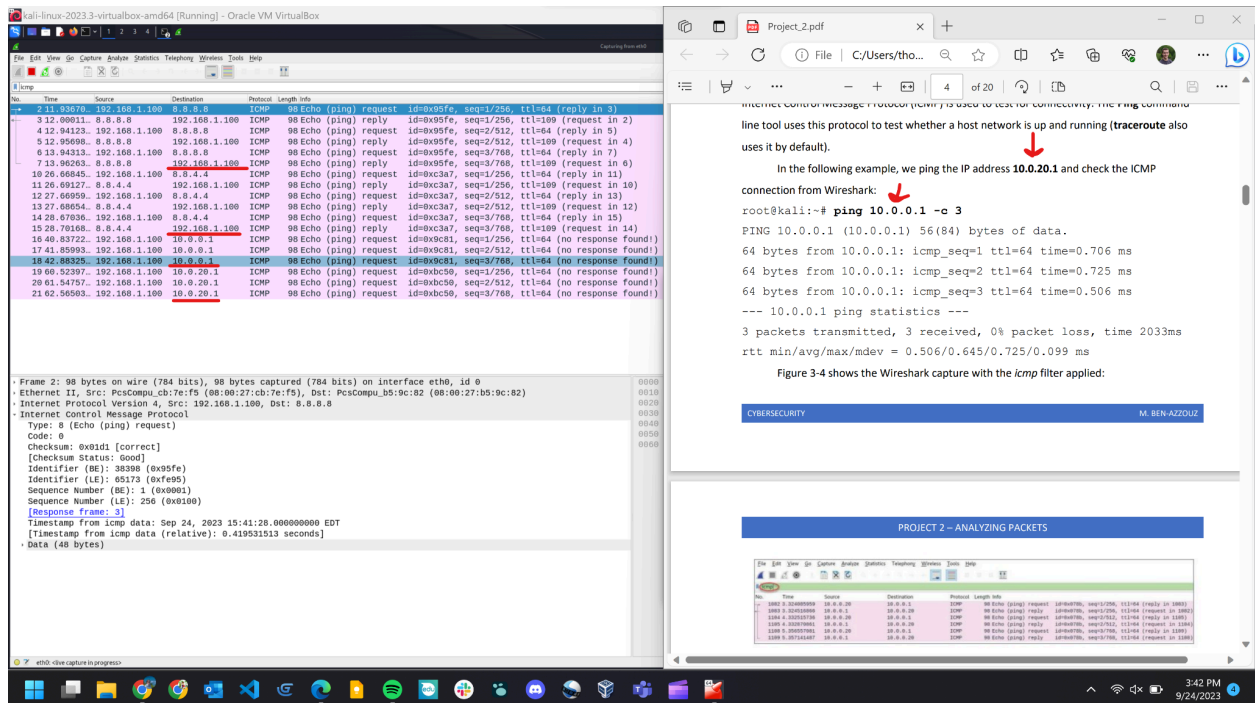


# Analyze WireShark Captures:

## Part 1: Analyze TCP networking protocols.



## Part 2: Analyze UDP networking protocols.



### Part 3: Analyze ARP networking protocols.

The screenshot shows a Wireshark packet capture in a virtual machine. The main packet list displays several packets, including a DNS query, an ARP request, and an ICMP Echo (ping) request. The packet details pane shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Domain Name System (query). The packet bytes pane shows the raw data of the selected packet. A terminal window in the foreground shows the execution of a ping command from root@kali: ~# ping 10.0.0.1 -c 3, resulting in 100% packet loss.

```
1 0.000000 192.168.1.100 → 192.168.1.1 DNS 111 Standard query 0xe2a6 PTR 1.1.168.192.in-addr.arpa PTR pfSense.home.arpa
2 0.000689 192.168.1.1 → 192.168.1.100 DNS 111 Standard query response 0xe2a6 PTR 1.1.168.192.in-addr.arpa PTR pfSense.home.arpa
3 5.032244 PcsCompu.cb:7: PcsCompu.b5:9 ARP 42 Who has 192.168.1.1? Tell 192.168.1.100
4 5.035266 PcsCompu.b5:9 PcsCompu.cb:7 ARP 60 192.168.1.1 is at 08:00:27:b5:9c:82
5 37.059966 f800::a00:27f::ff02::1 ICMP 110 Router Advertisement from 08:00:27:b5:9c:82
6 102.4872 f800::1b8:7b7::ff02::1:2 DHCP 110 Information-request XID: 0x60d5f CID: 000497f8f8facba2bdc0aa548ecc4307
```

Frame 1: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface eth0, id 0  
Ethernet II, Src: PcsCompu.cb:7e:ff (08:00:27:cb:7e:ff), Dst: PcsCompu.b5:9c:82 (08:00:27:b5:9c:82)  
Internet Protocol Version 4, Src: 192.168.1.100, Dst: 192.168.1.1  
User Datagram Protocol, Src Port: 59932, Dst Port: 53  
Domain Name System (query)

```
root@kali: ~# ping 10.0.0.1 -c 3
PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data:
--- 10.0.0.1 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2045ms

root@kali: ~# ping 10.0.20.1 -c 3
PING 10.0.20.1 (10.0.20.1) 56(84) bytes of data:
--- 10.0.20.1 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2040ms
```

### Part 4: Examine the reassembled TCP streams.

The screenshot shows a Wireshark packet capture in a virtual machine. The main packet list displays several packets, including a GET request, a 200 OK response, and a POST request. The packet details pane shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, and Hypertext Transfer Protocol. The packet bytes pane shows the raw data of the selected packet. A terminal window in the foreground shows the execution of a curl command from root@kali: ~# curl -X POST http://10.0.0.1:8080/submit, resulting in a 200 OK response.

```
1 0.000000 192.168.1.100 → 192.168.1.1 GET / HTTP/1.1
Host: 192.168.1.101
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/125.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

Frame 6192: 490 bytes on wire (3920 bits), 490 bytes captured (3920 bits) on interface eth0  
Ethernet II, Src: PcsCompu.0d:22:3d (08:00:27:0d:22:3d), Dst: PcsCompu.b5:9c:82 (08:00:27:b5:9c:82)  
Internet Protocol Version 4, Src: 192.168.1.100, Dst: 192.168.1.1  
Transmission Control Protocol, Src Port: 59932, Dst Port: 8080

```
root@kali: ~# curl -X POST http://10.0.0.1:8080/submit
200 OK
```

## Exercise 1: Changed Password & Traffic Graphs

The screenshot displays the pfSense web interface within a Kali Linux virtual machine. The left sidebar provides system details: Version 2.7.0-RELEASE (amd64), built on Wed Jun 28 03:53:34 UTC 2023, Firmware 14.0-CURRENT. Hardware crypto is inactive. The main content area shows the 'System / User Manager / Users' page. A table lists users, with 'admin' (System Administrator) having a checked status and belonging to the 'admins' group. Below the table, traffic graphs for WAN and LAN interfaces are shown, with the WAN graph indicating a peak in traffic around 36:40.

## Exercise 2: Method for getting deliverables.

The screenshot shows the Wireshark network protocol analyzer. The packet list on the left displays a packet at time 13744. The packet details pane on the right shows the structure of the ARP request, including Ethernet II, Internet Protocol Version 4, and Address Resolution Protocol. The packet bytes pane at the bottom shows the raw data.

## Deliverables:

Victim: 192.168.1.105 08:00:27:b8:f8:5a  
Attacker: 192.168.1.104 08:00:27:b8:b7:58  
Router: 192.168.1.1 08:00:27:5e:01:7c