ECE4016

Computer Network

117010437

Hajun Lee

(0) Be proficient in using commands such as ifconfig, ping, nslookup, arp, netstat, tracert, etc., and try to explain what protocol they are all done with.

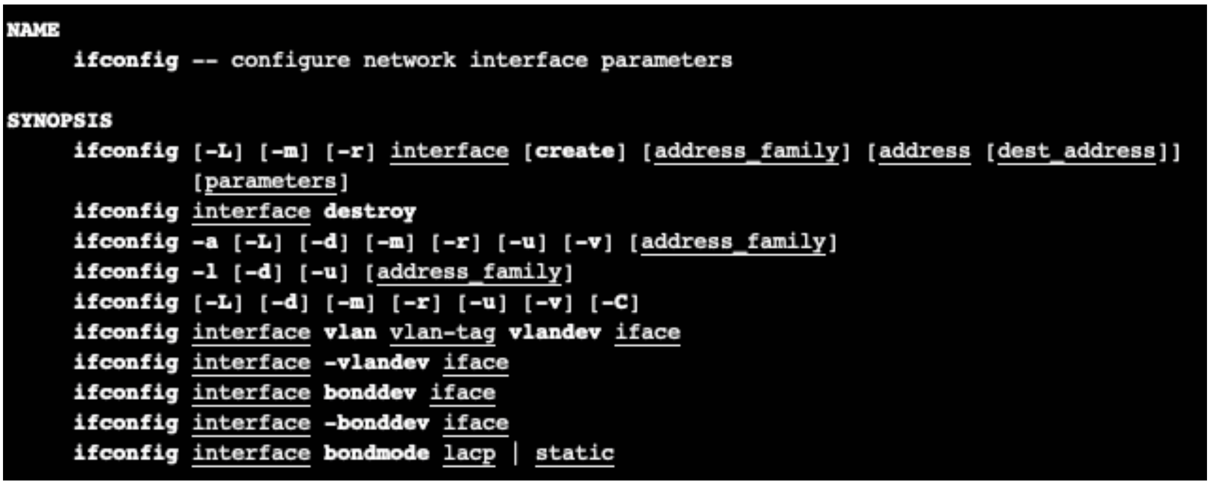
Ifconfig

Description

ifconfig stands for interface configuration. It is used to view and change the configuration of the network interfaces on the system. Ifconfig command is use the Address Resolution Protocol (ARP).

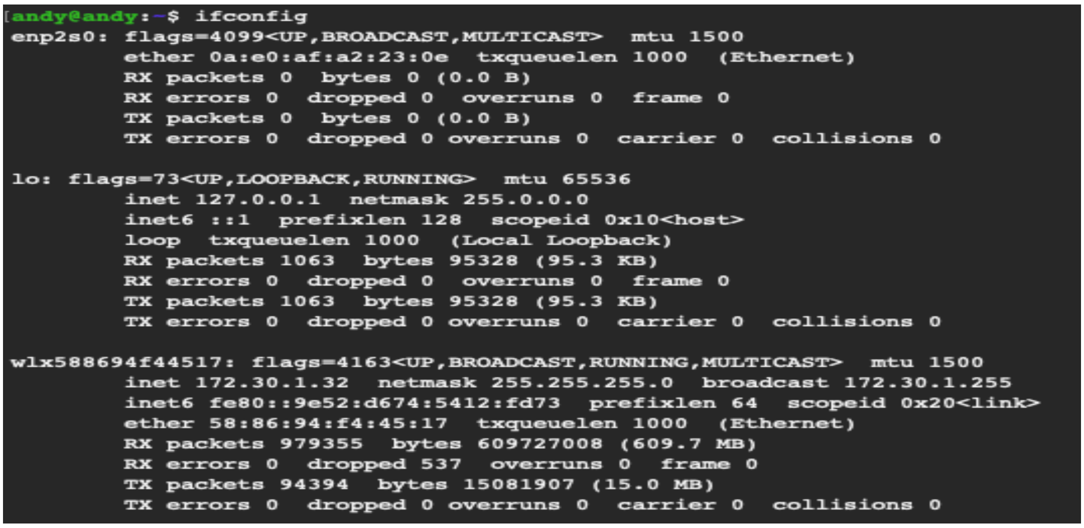
- eth0 is the first ethernet interface. (Additional Ethernet interfaces would be named eth1, eth2, etc). This type of interface is usually network interface card or ethernet card and network adapter connected to the network
- lo is the loopback interface. This is a special network interface that the system uses to communicate with itself.
- wlan0 is the name of the first wireless network interface on the system. (Additional wireless interfaces would be named wlan1, wlan2, etc.)

Usage / more option command in “man ipconfig”



```
NAME
     ifconfig -- configure network interface parameters

SYNOPSIS
     ifconfig [-L] [-m] [-r] interface [create] [address_family] [address [dest_address]]
              [parameters]
     ifconfig interface destroy
     ifconfig -a [-L] [-d] [-m] [-r] [-u] [-v] [address_family]
     ifconfig -l [-d] [-u] [address_family]
     ifconfig [-L] [-d] [-m] [-r] [-u] [-v] [-C]
     ifconfig interface vlan vlan-tag vlandev iface
     ifconfig interface -vlandev iface
     ifconfig interface bonddev iface
     ifconfig interface -bonddev iface
     ifconfig interface bondmode lacp | static
```

Example



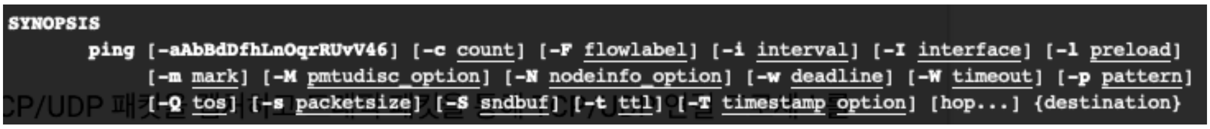
```
andy@andy:~$ ifconfig
enp2s0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 0a:e0:af:a2:23:0e  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 1063  bytes 95328 (95.3 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1063  bytes 95328 (95.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlx588694f44517: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.30.1.32  netmask 255.255.255.0  broadcast 172.30.1.255
        inet6 fe80::9e52:d674:5412:fd73  prefixlen 64  scopeid 0x20<link>
        ether 58:86:94:f4:45:17  txqueuelen 1000  (Ethernet)
        RX packets 979355  bytes 609727008 (609.7 MB)
        RX errors 0  dropped 537  overruns 0  frame 0
        TX packets 94394  bytes 15081907 (15.0 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Ping

Description

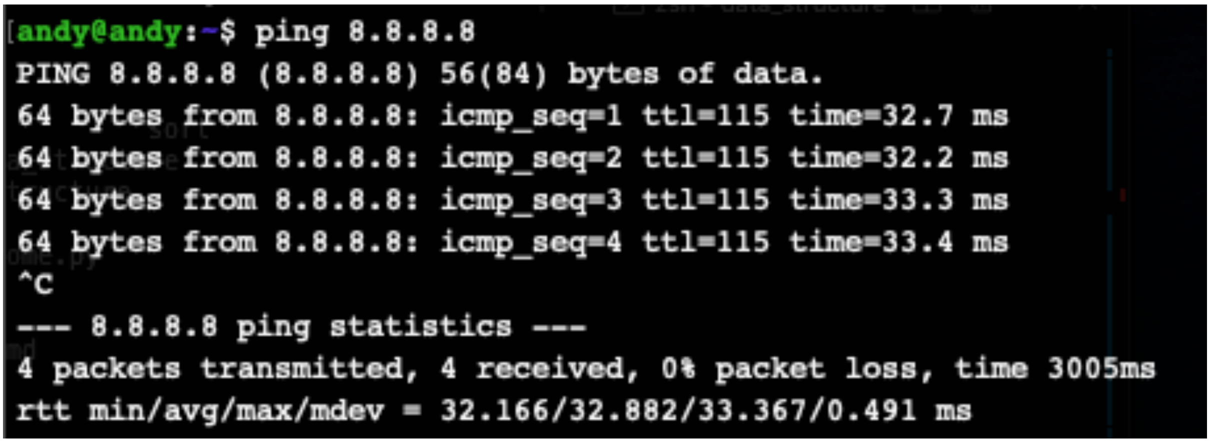
Ping (Packet internet or inter-network groper) is a networking utility for checking if a remote computer or node is reachable by a host on a network. Default protocol used for a network is internet protocol (IP). Several layers in an IP stack such as Internet Control Message Protocol (ICMP), Address Resolution Protocol (ARP) are involved in the ping process.

Usage / more option command in “man ping”



```
SYNOPSIS
       ping [-aAbBdDfhLnOqrRUvV46] [-c count] [-F flowlabel] [-i interval] [-I interface] [-l preload]
            [-m mark] [-M pmtudisc_option] [-N nodeinfo_option] [-w deadline] [-W timeout] [-p pattern]
            [-Q tos] [-s packetsize] [-S sndbuf] [-t ttl] [-T timestamp option] [hop...] {destination}
```

example



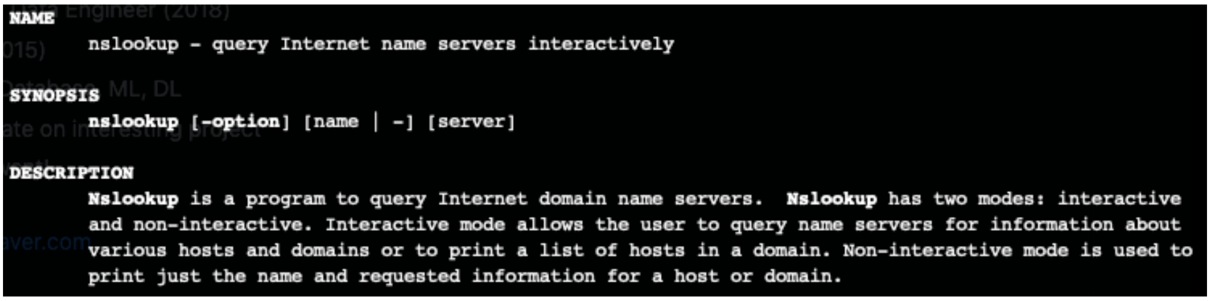
```
[andy@andy:~$ ping 8.8.8.8
 PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
 64 bytes from 8.8.8.8: icmp_seq=1 ttl=115 time=32.7 ms
 64 bytes from 8.8.8.8: icmp_seq=2 ttl=115 time=32.2 ms
 64 bytes from 8.8.8.8: icmp_seq=3 ttl=115 time=33.3 ms
 64 bytes from 8.8.8.8: icmp_seq=4 ttl=115 time=33.4 ms
 ^C
 --- 8.8.8.8 ping statistics ---
 4 packets transmitted, 4 received, 0% packet loss, time 3005ms
 rtt min/avg/max/mdev = 32.166/32.882/33.367/0.491 ms
```

nslookup

Description

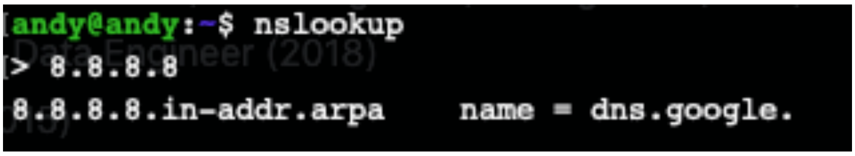
Nslookup is the name of a program that lets an internet server administrator or any computer user enter a host name and find out the corresponding IP address or domain name system (DNS) record. The user can also enter a command for it to do a reverse DNS lookup and find the host name for an IP addres s that is specified.

Usage / more option command in “man nslookup”



```
NAME
       nslookup - query Internet name servers interactively

SYNOPSIS
       nslookup [-option] [name | -] [server]

DESCRIPTION
       Nslookup is a program to query Internet domain name servers.  Nslookup has two modes: interactive
       and non-interactive. Interactive mode allows the user to query name servers for information about
       various hosts and domains or to print a list of hosts in a domain. Non-interactive mode is used to
       print just the name and requested information for a host or domain.
```

Example



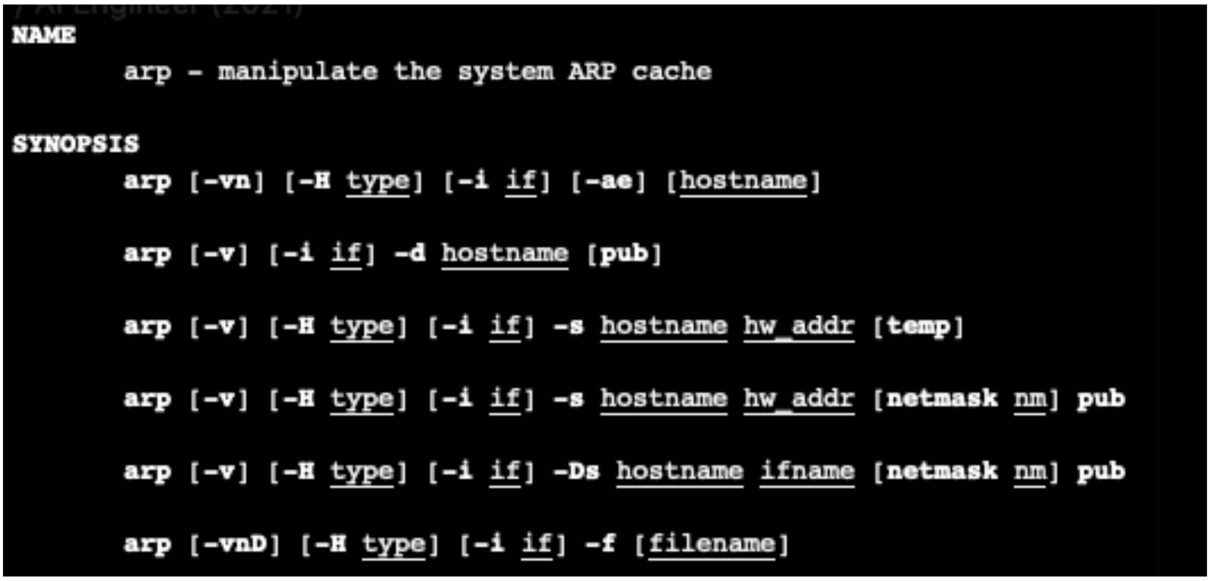
```
andy@andy:~$ nslookup
> 8.8.8.8
8.8.8.8.in-addr.arpa	name = dns.google.
```

Arp

Description

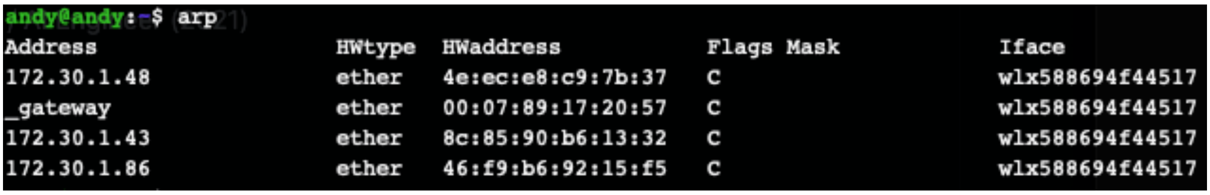
Address Resolution Protocol (ARP) is a protocol for mapping an IP address to a physical MAC address on a local area network. ARP command is a TCP/IP utility used for viewing and modifying the local ARP cache.

Usage / more option command in “man arp”



```
NAME
       arp - manipulate the system ARP cache

SYNOPSIS
       arp [-vn] [-H type] [-i if] [-ae] [hostname]

       arp [-v] [-i if] -d hostname [pub]

       arp [-v] [-H type] [-i if] -s hostname hw_addr [temp]

       arp [-v] [-H type] [-i if] -s hostname hw_addr [netmask nm] pub

       arp [-v] [-H type] [-i if] -Ds hostname ifname [netmask nm] pub

       arp [-vnD] [-H type] [-i if] -f [filename]
```

Example



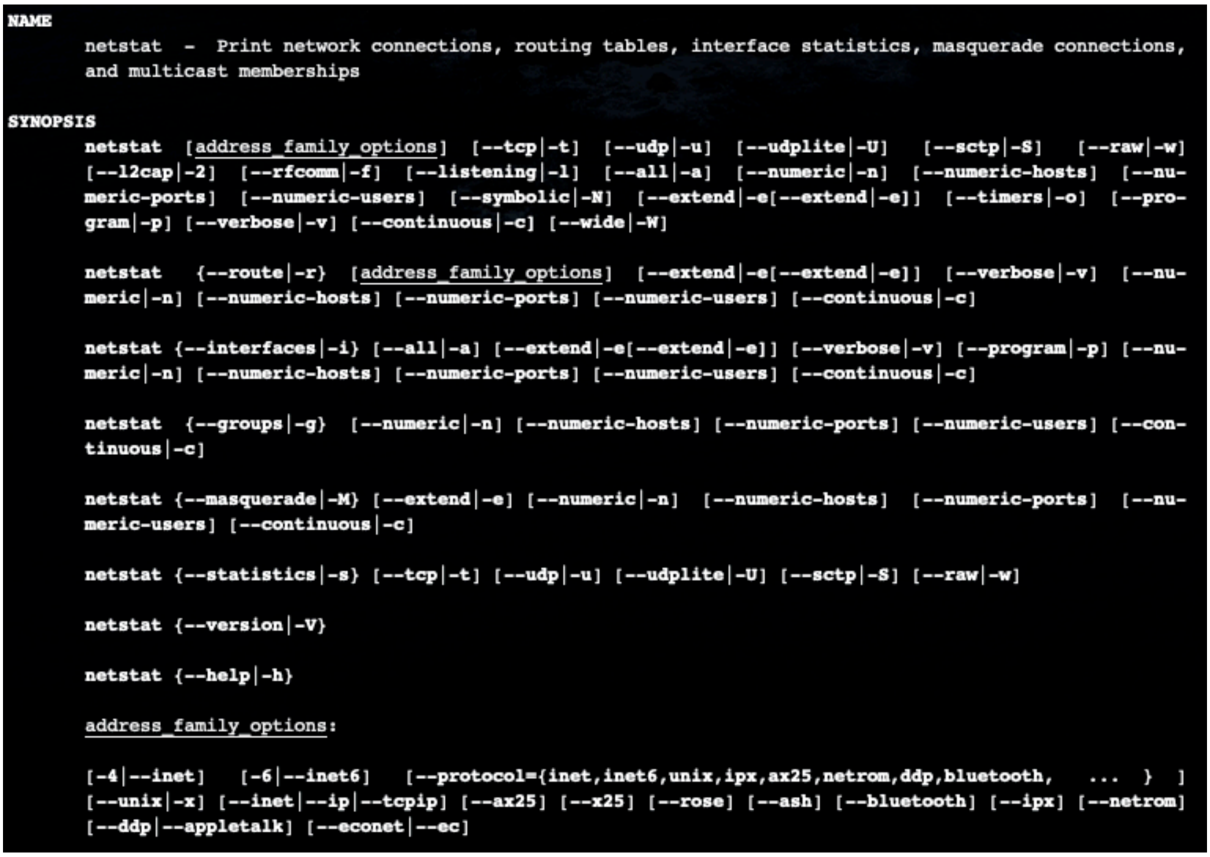
```
andy@andy:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
172.30.1.48              ether   4e:ec:e8:c9:7b:37   C                     wlx588694f44517
_gateway                 ether   00:07:89:17:20:57   C                     wlx588694f44517
172.30.1.43              ether   8c:85:90:b6:13:32   C                     wlx588694f44517
172.30.1.86              ether   46:f9:b6:92:15:f5   C                     wlx588694f44517
```

netstat

Description

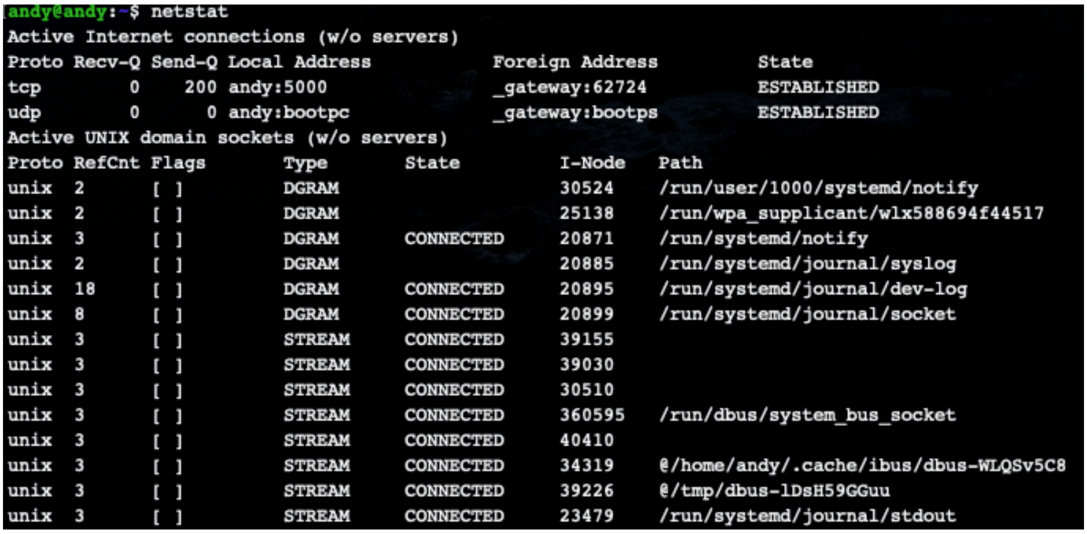
netstat command generates displays that show network status and protocol statistics. It can display the status of TCP and UDP endpoints in table format, routing table information, and interface information.

Usage / more option command in “man netstat”



```
NAME
       netstat  -  Print network connections, routing tables, interface statistics, masquerade connections,
       and multicast memberships

SYNOPSIS
       netstat  [address_family_options]  [--tcp|-t]  [--udp|-u]  [--udplite|-U]   [--sctp|-S]   [--raw|-w]
       [--l2cap|-2]  [--rfcomm|-f]  [--listening|-l]  [--all|-a]  [--numeric|-n]  [--numeric-hosts]  [--nu-
       meric-ports]  [--numeric-users]  [--symbolic|-N]  [--extend|-e[--extend|-e]]  [--timers|-o]  [--pro-
       gram|-p] [--verbose|-v] [--continuous|-c] [--wide|-W]

       netstat   {--route|-r}  [address_family_options]  [--extend|-e[--extend|-e]]  [--verbose|-v]  [--nu-
       meric|-n] [--numeric-hosts] [--numeric-ports] [--numeric-users] [--continuous|-c]

       netstat {--interfaces|-i} [--all|-a] [--extend|-e[--extend|-e]] [--verbose|-v] [--program|-p] [--nu-
       meric|-n] [--numeric-hosts] [--numeric-ports] [--numeric-users] [--continuous|-c]

       netstat  {--groups|-g}  [--numeric|-n] [--numeric-hosts] [--numeric-ports] [--numeric-users] [--con-
       tinuous|-c]

       netstat {--masquerade|-M} [--extend|-e] [--numeric|-n]  [--numeric-hosts]  [--numeric-ports]  [--nu-
       meric-users] [--continuous|-c]

       netstat {--statistics|-s} [--tcp|-t] [--udp|-u] [--udplite|-U] [--sctp|-S] [--raw|-w]

       netstat {--version|-V}

       netstat {--help|-h}

       address_family_options:

       [-4|--inet]   [-6|--inet6]   [--protocol={inet,inet6,unix,ipx,ax25,netrom,ddp,bluetooth,   ...  }  ]
       [--unix|-x] [--inet|--ip|--tcpip] [--ax25] [--x25] [--rose] [--ash] [--bluetooth] [--ipx] [--netrom]
       [--ddp|--appletalk] [--econet|--ec]
```

Example



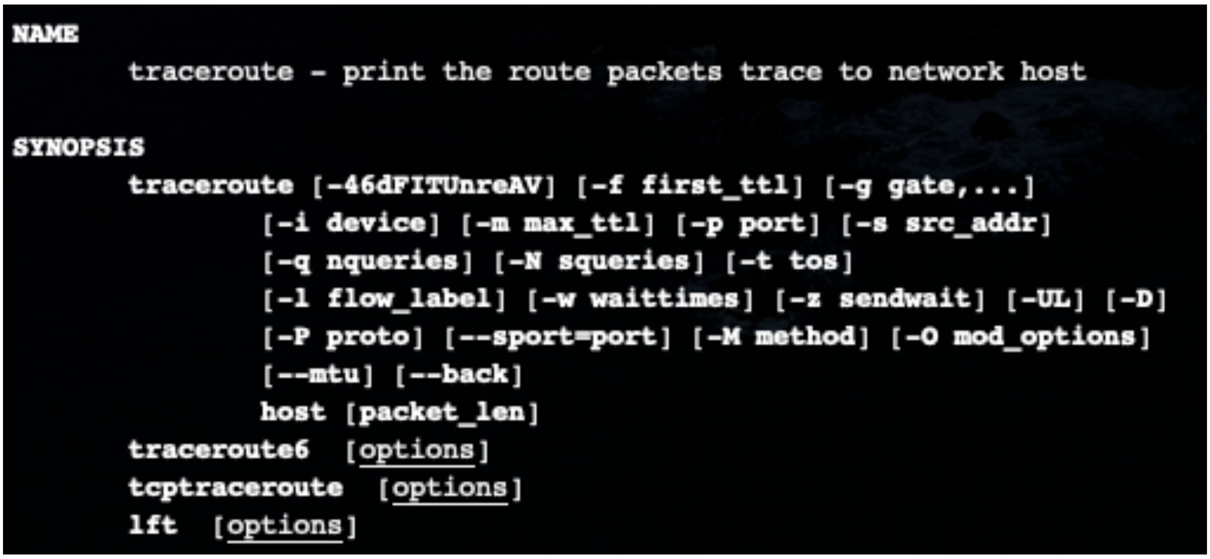
```
andy@andy:~$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0    200 andy:5000               _gateway:62724          ESTABLISHED
udp        0      0 andy:bootpc             _gateway:bootps         ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ]         DGRAM                    30524    /run/user/1000/systemd/notify
unix  2      [ ]         DGRAM                    25138    /run/wpa_supplicant/wlx588694f44517
unix  3      [ ]         DGRAM      CONNECTED     20871    /run/systemd/notify
unix  2      [ ]         DGRAM                    20885    /run/systemd/journal/syslog
unix  18     [ ]         DGRAM      CONNECTED     20895    /run/systemd/journal/dev-log
unix  8      [ ]         DGRAM      CONNECTED     20899    /run/systemd/journal/socket
unix  3      [ ]         STREAM     CONNECTED     39155
unix  3      [ ]         STREAM     CONNECTED     39030
unix  3      [ ]         STREAM     CONNECTED     30510
unix  3      [ ]         STREAM     CONNECTED     360595   /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     40410
unix  3      [ ]         STREAM     CONNECTED     34319    @/home/andy/.cache/ibus/dbus-WLQSv5C8
unix  3      [ ]         STREAM     CONNECTED     39226    @/tmp/dbus-1DsH59GGuu
unix  3      [ ]         STREAM     CONNECTED     23479    /run/systemd/journal/stdout
```

Tracert / traceroute

Description

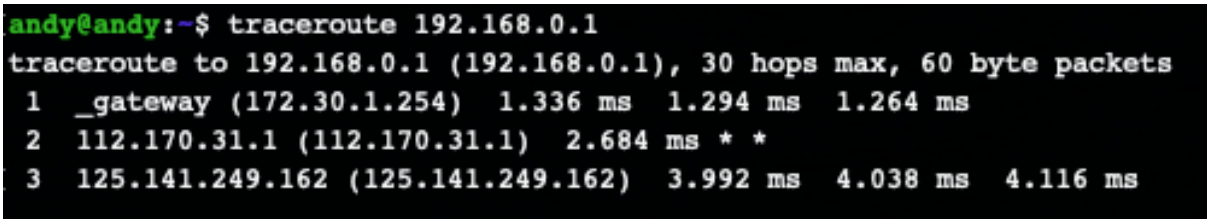
A Traceroute command is a command that is generally used to locate the destination path from the host in the network. Traceroute most commonly uses Internet Control Message Protocol (ICMP) echo packets with variable time to live (TTL) values. The response time of each hop is calculated.

Usage / more option command in "man traceroute"
(you should install command "sudo apt install traceroute")



```
NAME
       traceroute - print the route packets trace to network host

SYNOPSIS
       traceroute [-46dFITUnreAV] [-f first_ttl] [-g gate,...]
               [-i device] [-m max_ttl] [-p port] [-s src_addr]
               [-q nqueries] [-N squeries] [-t tos]
               [-l flow_label] [-w waittimes] [-z sendwait] [-UL] [-D]
               [-P proto] [--sport=port] [-M method] [-O mod_options]
               [--mtu] [--back]
               host [packet_len]
       traceroute6  [options]
       tcptraceroute  [options]
       lft  [options]
```

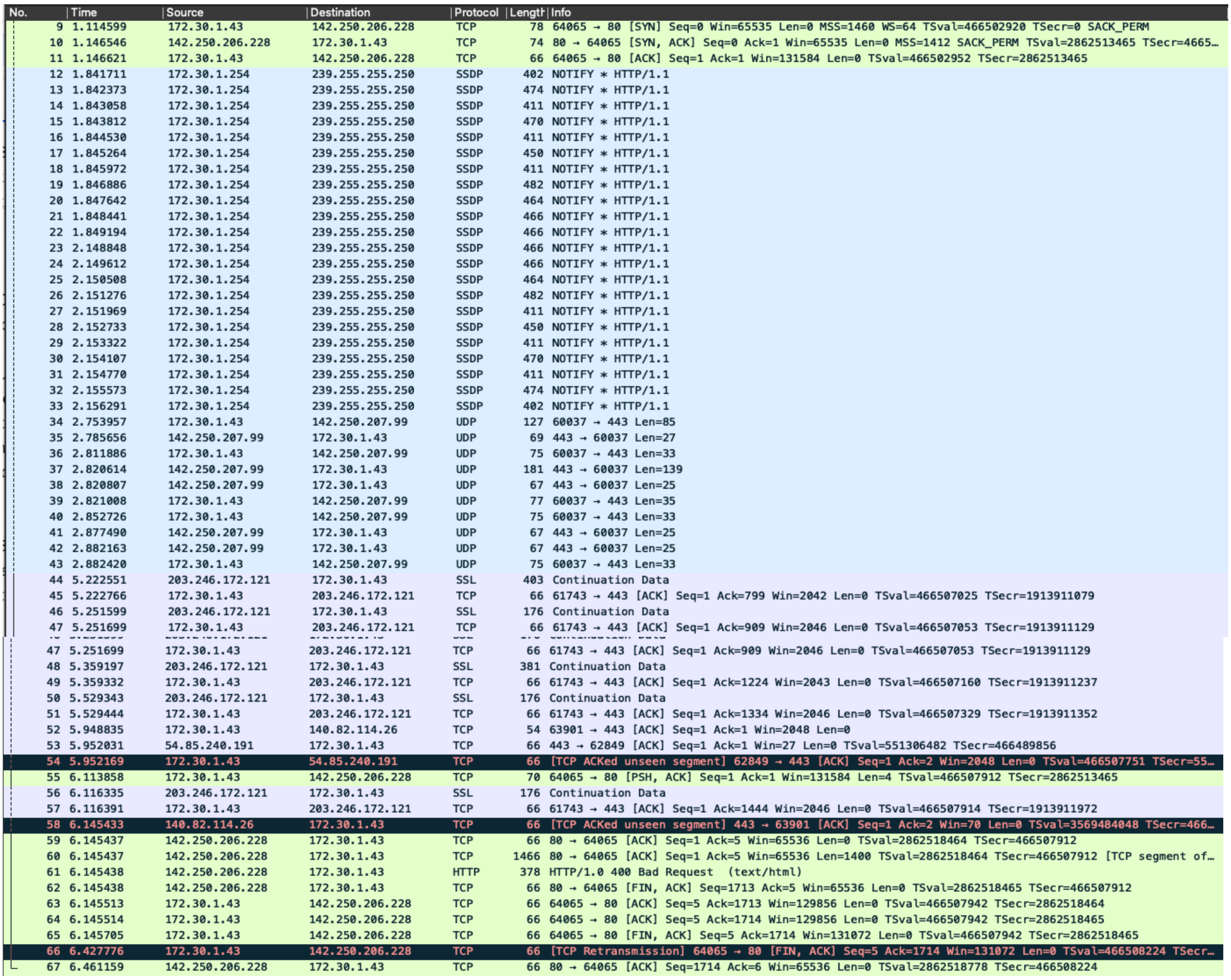
Example



```
andy@andy:~$ traceroute 192.168.0.1
traceroute to 192.168.0.1 (192.168.0.1), 30 hops max, 60 byte packets
 1  _gateway (172.30.1.254)  1.336 ms  1.294 ms  1.264 ms
 2  112.170.31.1 (112.170.31.1)  2.684 ms * *
 3  125.141.249.162 (125.141.249.162)  3.992 ms  4.038 ms  4.116 ms
```

(1) Capture the TCP/UDP packet and explain the TCP/UDP connection process through the traffic packet.

1. Start a Wireshark capture.
2. Open a command prompt.
3. Type telnet www.google.com 80 and press Enter.
4. Close the command prompt to close the TCP/UDP connection.
5. Stop the Wireshark capture.

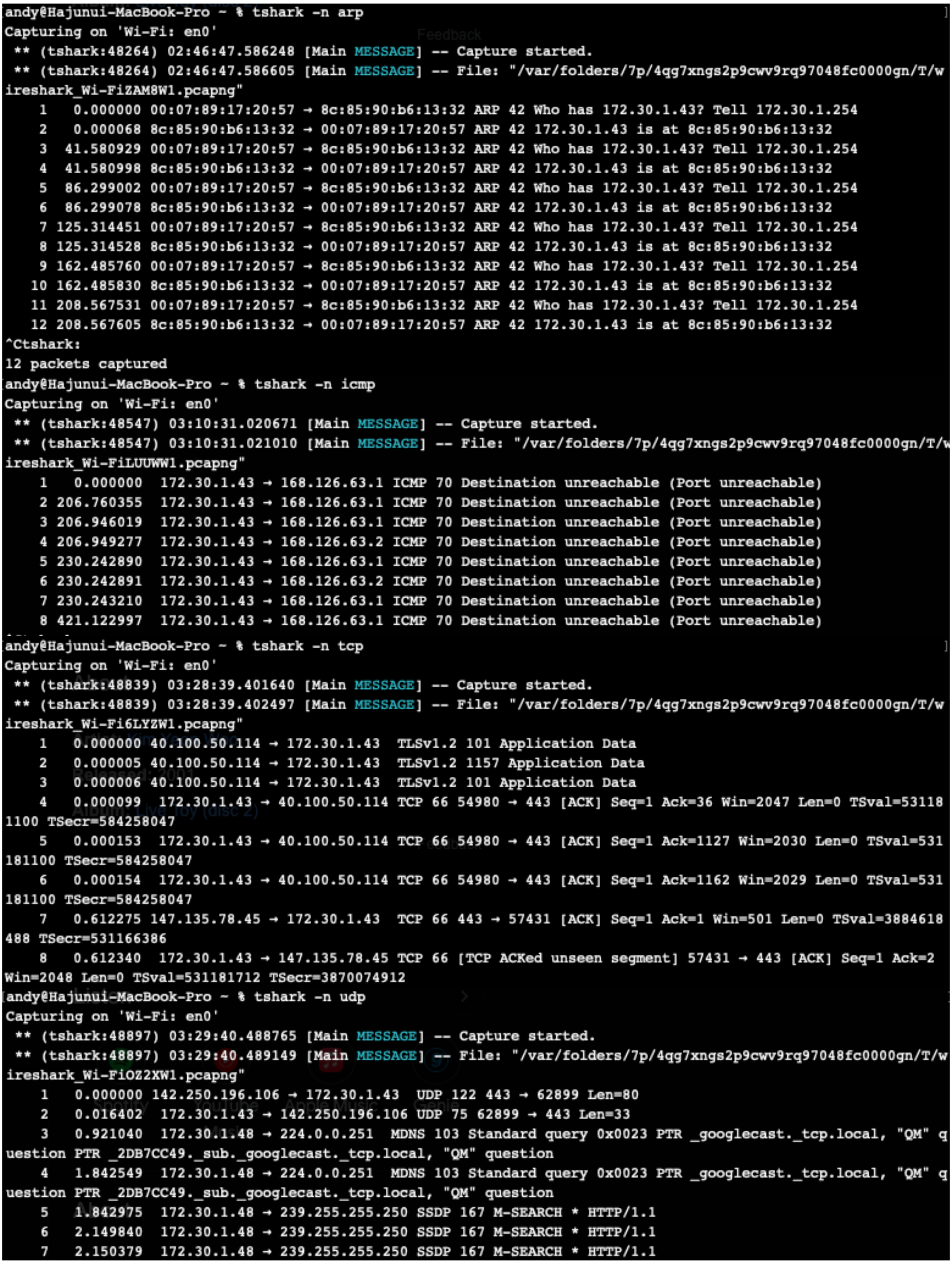


No.	Time	Source	Destination	Protocol	Lengtł	Info
9	1.114599	172.30.1.43	142.250.206.228	TCP	78	64065 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=466502920 TSecr=0 SACK_PERM
10	1.146546	142.250.206.228	172.30.1.43	TCP	74	80 → 64065 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM TSval=2862513465 TSecr=4665…
11	1.146621	172.30.1.43	142.250.206.228	TCP	66	64065 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0 TSval=466502952 TSecr=2862513465
12	1.841711	172.30.1.254	239.255.255.250	SSDP	402	NOTIFY * HTTP/1.1
13	1.842373	172.30.1.254	239.255.255.250	SSDP	474	NOTIFY * HTTP/1.1
14	1.843058	172.30.1.254	239.255.255.250	SSDP	411	NOTIFY * HTTP/1.1
15	1.843812	172.30.1.254	239.255.255.250	SSDP	470	NOTIFY * HTTP/1.1
16	1.844530	172.30.1.254	239.255.255.250	SSDP	411	NOTIFY * HTTP/1.1
17	1.845264	172.30.1.254	239.255.255.250	SSDP	450	NOTIFY * HTTP/1.1
18	1.845972	172.30.1.254	239.255.255.250	SSDP	411	NOTIFY * HTTP/1.1
19	1.846886	172.30.1.254	239.255.255.250	SSDP	482	NOTIFY * HTTP/1.1
20	1.847642	172.30.1.254	239.255.255.250	SSDP	464	NOTIFY * HTTP/1.1
21	1.848441	172.30.1.254	239.255.255.250	SSDP	466	NOTIFY * HTTP/1.1
22	1.849194	172.30.1.254	239.255.255.250	SSDP	466	NOTIFY * HTTP/1.1
23	2.148848	172.30.1.254	239.255.255.250	SSDP	466	NOTIFY * HTTP/1.1
24	2.149612	172.30.1.254	239.255.255.250	SSDP	466	NOTIFY * HTTP/1.1
25	2.150508	172.30.1.254	239.255.255.250	SSDP	464	NOTIFY * HTTP/1.1
26	2.151276	172.30.1.254	239.255.255.250	SSDP	482	NOTIFY * HTTP/1.1
27	2.151969	172.30.1.254	239.255.255.250	SSDP	411	NOTIFY * HTTP/1.1
28	2.152733	172.30.1.254	239.255.255.250	SSDP	450	NOTIFY * HTTP/1.1
29	2.153322	172.30.1.254	239.255.255.250	SSDP	411	NOTIFY * HTTP/1.1
30	2.154107	172.30.1.254	239.255.255.250	SSDP	470	NOTIFY * HTTP/1.1
31	2.154770	172.30.1.254	239.255.255.250	SSDP	411	NOTIFY * HTTP/1.1
32	2.155573	172.30.1.254	239.255.255.250	SSDP	474	NOTIFY * HTTP/1.1
33	2.156291	172.30.1.254	239.255.255.250	SSDP	402	NOTIFY * HTTP/1.1
34	2.753957	172.30.1.43	142.250.207.99	UDP	127	60037 → 443 Len=85
35	2.785656	142.250.207.99	172.30.1.43	UDP	69	443 → 60037 Len=27
36	2.811886	172.30.1.43	142.250.207.99	UDP	75	60037 → 443 Len=33
37	2.820614	142.250.207.99	172.30.1.43	UDP	181	443 → 60037 Len=139
38	2.820807	142.250.207.99	172.30.1.43	UDP	67	443 → 60037 Len=25
39	2.821008	172.30.1.43	142.250.207.99	UDP	77	60037 → 443 Len=35
40	2.852726	172.30.1.43	142.250.207.99	UDP	75	60037 → 443 Len=33
41	2.877490	142.250.207.99	172.30.1.43	UDP	67	443 → 60037 Len=25
42	2.882163	142.250.207.99	172.30.1.43	UDP	67	443 → 60037 Len=25
43	2.882420	172.30.1.43	142.250.207.99	UDP	75	60037 → 443 Len=33
44	5.222551	203.246.172.121	172.30.1.43	SSL	403	Continuation Data
45	5.222766	172.30.1.43	203.246.172.121	TCP	66	61743 → 443 [ACK] Seq=1 Ack=799 Win=2042 Len=0 TSval=466507025 TSecr=1913911079
46	5.251599	203.246.172.121	172.30.1.43	SSL	176	Continuation Data
47	5.251699	172.30.1.43	203.246.172.121	TCP	66	61743 → 443 [ACK] Seq=1 Ack=909 Win=2046 Len=0 TSval=466507053 TSecr=1913911129
47	5.251699	172.30.1.43	203.246.172.121	TCP	66	61743 → 443 [ACK] Seq=1 Ack=909 Win=2046 Len=0 TSval=466507053 TSecr=1913911129
48	5.359197	203.246.172.121	172.30.1.43	SSL	381	Continuation Data
49	5.359332	172.30.1.43	203.246.172.121	TCP	66	61743 → 443 [ACK] Seq=1 Ack=1224 Win=2043 Len=0 TSval=466507160 TSecr=1913911237
50	5.529343	203.246.172.121	172.30.1.43	SSL	176	Continuation Data
51	5.529444	172.30.1.43	203.246.172.121	TCP	66	61743 → 443 [ACK] Seq=1 Ack=1334 Win=2046 Len=0 TSval=466507329 TSecr=1913911352
52	5.948835	172.30.1.43	140.82.114.26	TCP	54	63901 → 443 [ACK] Seq=1 Ack=1 Win=2048 Len=0
53	5.952031	54.85.240.191	172.30.1.43	TCP	66	443 → 62849 [ACK] Seq=1 Ack=1 Win=27 Len=0 TSval=551306482 TSecr=466489856
54	5.952169	172.30.1.43	54.85.240.191	TCP	66	[TCP ACKed unseen segment] 62849 → 443 [ACK] Seq=1 Ack=2 Win=2048 Len=0 TSval=466507751 TSecr=55…
55	6.113858	172.30.1.43	142.250.206.228	TCP	70	64065 → 80 [PSH, ACK] Seq=1 Ack=1 Win=131584 Len=4 TSval=466507912 TSecr=2862513465
56	6.116335	203.246.172.121	172.30.1.43	SSL	176	Continuation Data
57	6.116391	172.30.1.43	203.246.172.121	TCP	66	61743 → 443 [ACK] Seq=1 Ack=1444 Win=2046 Len=0 TSval=466507914 TSecr=1913911972
58	6.145433	140.82.114.26	172.30.1.43	TCP	66	[TCP ACKed unseen segment] 443 → 63901 [ACK] Seq=1 Ack=2 Win=70 Len=0 TSval=3569484048 TSecr=466…
59	6.145437	142.250.206.228	172.30.1.43	TCP	66	80 → 64065 [ACK] Seq=1 Ack=5 Win=65536 Len=0 TSval=2862518464 TSecr=466507912
60	6.145437	142.250.206.228	172.30.1.43	TCP	1466	80 → 64065 [ACK] Seq=1 Ack=5 Win=65536 Len=1400 TSval=2862518464 TSecr=466507912 [TCP segment of…
61	6.145438	142.250.206.228	172.30.1.43	HTTP	378	HTTP/1.0 400 Bad Request (text/html)
62	6.145438	142.250.206.228	172.30.1.43	TCP	66	80 → 64065 [FIN, ACK] Seq=1713 Ack=5 Win=65536 Len=0 TSval=2862518465 TSecr=466507912
63	6.145513	172.30.1.43	142.250.206.228	TCP	66	64065 → 80 [ACK] Seq=5 Ack=1713 Win=129856 Len=0 TSval=466507942 TSecr=2862518464
64	6.145514	172.30.1.43	142.250.206.228	TCP	66	64065 → 80 [ACK] Seq=5 Ack=1714 Win=129856 Len=0 TSval=466507942 TSecr=2862518465
65	6.145705	172.30.1.43	142.250.206.228	TCP	66	64065 → 80 [FIN, ACK] Seq=5 Ack=1714 Win=131072 Len=0 TSval=466507942 TSecr=2862518465
66	6.427776	172.30.1.43	142.250.206.228	TCP	66	[TCP Retransmission] 64065 → 80 [FIN, ACK] Seq=5 Ack=1714 Win=131072 Len=0 TSval=466508224 TSecr…
67	6.461159	142.250.206.228	172.30.1.43	TCP	66	80 → 64065 [ACK] Seq=1714 Ack=6 Win=65536 Len=0 TSval=2862518778 TSecr=466508224

TCP is connection oriented, it creates a connection for the transmission to take place, and when transfer is over that connection is terminated.

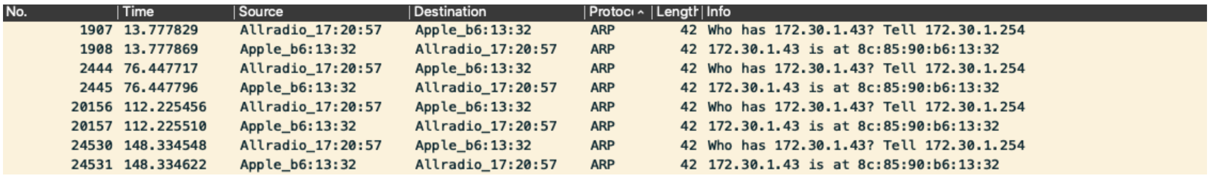
However, UDP is connectionless just like IP

(2) Use the wireshark (GUI) and the tshark (command) packet capture tool to grab ARP, ICMP, DNS, HTTP, TCP, UDP and other packets, and parse the packet information content in the packet. (The contents of the bag you caught may not be the same as what you learned, please explain why?)



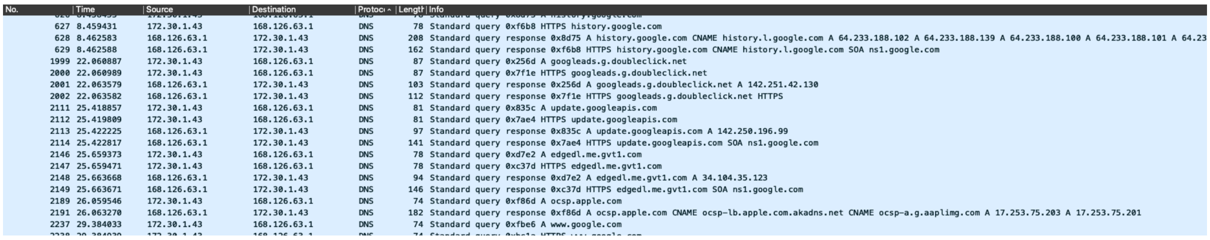
```
andy@Hajunui-MacBook-Pro ~ % tshark -n arp
Capturing on 'Wi-Fi: en0'
 ** (tshark:48264) 02:46:47.586248 [Main MESSAGE] -- Capture started.
 ** (tshark:48264) 02:46:47.586605 [Main MESSAGE] -- File: "/var/folders/7p/4qg7xngs2p9cwv9rq97048fc0000gn/T/w
ireshark_Wi-FiZAM8W1.pcapng"
    1   0.000000 00:07:89:17:20:57 → 8c:85:90:b6:13:32 ARP 42 Who has 172.30.1.43? Tell 172.30.1.254
    2   0.000068 8c:85:90:b6:13:32 → 00:07:89:17:20:57 ARP 42 172.30.1.43 is at 8c:85:90:b6:13:32
    3  41.580929 00:07:89:17:20:57 → 8c:85:90:b6:13:32 ARP 42 Who has 172.30.1.43? Tell 172.30.1.254
    4  41.580998 8c:85:90:b6:13:32 → 00:07:89:17:20:57 ARP 42 172.30.1.43 is at 8c:85:90:b6:13:32
    5  86.299002 00:07:89:17:20:57 → 8c:85:90:b6:13:32 ARP 42 Who has 172.30.1.43? Tell 172.30.1.254
    6  86.299078 8c:85:90:b6:13:32 → 00:07:89:17:20:57 ARP 42 172.30.1.43 is at 8c:85:90:b6:13:32
    7 125.314451 00:07:89:17:20:57 → 8c:85:90:b6:13:32 ARP 42 Who has 172.30.1.43? Tell 172.30.1.254
    8 125.314528 8c:85:90:b6:13:32 → 00:07:89:17:20:57 ARP 42 172.30.1.43 is at 8c:85:90:b6:13:32
    9 162.485760 00:07:89:17:20:57 → 8c:85:90:b6:13:32 ARP 42 Who has 172.30.1.43? Tell 172.30.1.254
   10 162.485830 8c:85:90:b6:13:32 → 00:07:89:17:20:57 ARP 42 172.30.1.43 is at 8c:85:90:b6:13:32
   11 208.567531 00:07:89:17:20:57 → 8c:85:90:b6:13:32 ARP 42 Who has 172.30.1.43? Tell 172.30.1.254
   12 208.567605 8c:85:90:b6:13:32 → 00:07:89:17:20:57 ARP 42 172.30.1.43 is at 8c:85:90:b6:13:32
^Ctshark:
12 packets captured
andy@Hajunui-MacBook-Pro ~ % tshark -n icmp
Capturing on 'Wi-Fi: en0'
 ** (tshark:48547) 03:10:31.020671 [Main MESSAGE] -- Capture started.
 ** (tshark:48547) 03:10:31.021010 [Main MESSAGE] -- File: "/var/folders/7p/4qg7xngs2p9cwv9rq97048fc0000gn/T/w
ireshark_Wi-FiLUUWW1.pcapng"
    1   0.000000  172.30.1.43 → 168.126.63.1 ICMP 70 Destination unreachable (Port unreachable)
    2 206.760355  172.30.1.43 → 168.126.63.1 ICMP 70 Destination unreachable (Port unreachable)
    3 206.946019  172.30.1.43 → 168.126.63.1 ICMP 70 Destination unreachable (Port unreachable)
    4 206.949277  172.30.1.43 → 168.126.63.2 ICMP 70 Destination unreachable (Port unreachable)
    5 230.242890  172.30.1.43 → 168.126.63.1 ICMP 70 Destination unreachable (Port unreachable)
    6 230.242891  172.30.1.43 → 168.126.63.2 ICMP 70 Destination unreachable (Port unreachable)
    7 230.243210  172.30.1.43 → 168.126.63.1 ICMP 70 Destination unreachable (Port unreachable)
    8 421.122997  172.30.1.43 → 168.126.63.1 ICMP 70 Destination unreachable (Port unreachable)
andy@Hajunui-MacBook-Pro ~ % tshark -n tcp
Capturing on 'Wi-Fi: en0'
 ** (tshark:48839) 03:28:39.401640 [Main MESSAGE] -- Capture started.
 ** (tshark:48839) 03:28:39.402497 [Main MESSAGE] -- File: "/var/folders/7p/4qg7xngs2p9cwv9rq97048fc0000gn/T/w
ireshark_Wi-Fi6LYZW1.pcapng"
    1   0.000000 40.100.50.114 → 172.30.1.43  TLSv1.2 101 Application Data
    2   0.000005 40.100.50.114 → 172.30.1.43  TLSv1.2 1157 Application Data
    3   0.000006 40.100.50.114 → 172.30.1.43  TLSv1.2 101 Application Data
    4   0.000099  172.30.1.43 → 40.100.50.114 TCP 66 54980 → 443 [ACK] Seq=1 Ack=36 Win=2047 Len=0 TSval=53118
1100 TSecr=584258047
    5   0.000153  172.30.1.43 → 40.100.50.114 TCP 66 54980 → 443 [ACK] Seq=1 Ack=1127 Win=2030 Len=0 TSval=531
181100 TSecr=584258047
    6   0.000154  172.30.1.43 → 40.100.50.114 TCP 66 54980 → 443 [ACK] Seq=1 Ack=1162 Win=2029 Len=0 TSval=531
181100 TSecr=584258047
    7   0.612275 147.135.78.45 → 172.30.1.43  TCP 66 443 → 57431 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=3884618
488 TSecr=531166386
    8   0.612340  172.30.1.43 → 147.135.78.45 TCP 66 [TCP ACKed unseen segment] 57431 → 443 [ACK] Seq=1 Ack=2
Win=2048 Len=0 TSval=531181712 TSecr=3870074912
andy@Hajunui-MacBook-Pro ~ % tshark -n udp
Capturing on 'Wi-Fi: en0'
 ** (tshark:48897) 03:29:40.488765 [Main MESSAGE] -- Capture started.
 ** (tshark:48897) 03:29:40.489149 [Main MESSAGE] -- File: "/var/folders/7p/4qg7xngs2p9cwv9rq97048fc0000gn/T/w
ireshark_Wi-FiOZ2XW1.pcapng"
    1   0.000000 142.250.196.106 → 172.30.1.43  UDP 122 443 → 62899 Len=80
    2   0.016402  172.30.1.43 → 142.250.196.106 UDP 75 62899 → 443 Len=33
    3   0.921040  172.30.1.48 → 224.0.0.251  MDNS 103 Standard query 0x0023 PTR _googlecast._tcp.local, "QM" q
uestion PTR _2DB7CC49._sub._googlecast._tcp.local, "QM" question
    4   1.842549  172.30.1.48 → 224.0.0.251  MDNS 103 Standard query 0x0023 PTR _googlecast._tcp.local, "QM" q
uestion PTR _2DB7CC49._sub._googlecast._tcp.local, "QM" question
    5   1.842975  172.30.1.48 → 239.255.255.250 SSDP 167 M-SEARCH * HTTP/1.1
    6   2.149840  172.30.1.48 → 239.255.255.250 SSDP 167 M-SEARCH * HTTP/1.1
    7   2.150379  172.30.1.48 → 239.255.255.250 SSDP 167 M-SEARCH * HTTP/1.1
```

Arp



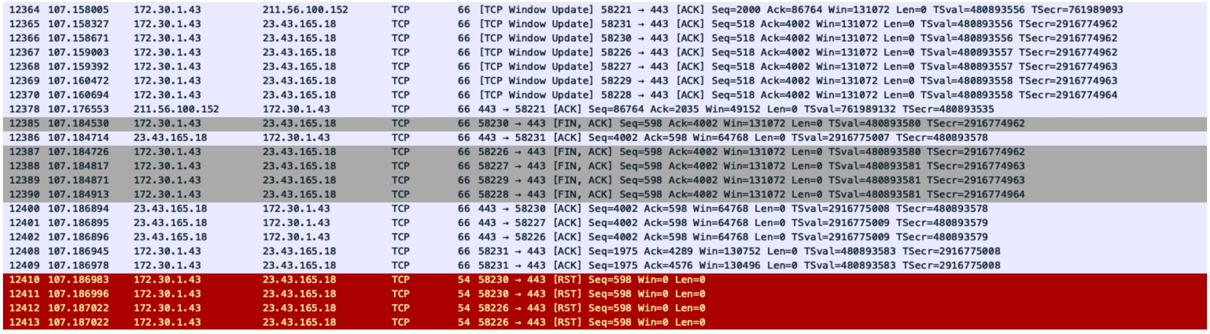
```
No.      Time        Source              Destination         Protoc ^ Length Info
   1907  13.777829   Allradio_17:20:57   Apple_b6:13:32      ARP      42  Who has 172.30.1.43? Tell 172.30.1.254
   1908  13.777869   Apple_b6:13:32      Allradio_17:20:57   ARP      42  172.30.1.43 is at 8c:85:90:b6:13:32
   2444  76.447717   Allradio_17:20:57   Apple_b6:13:32      ARP      42  Who has 172.30.1.43? Tell 172.30.1.254
   2445  76.447796   Apple_b6:13:32      Allradio_17:20:57   ARP      42  172.30.1.43 is at 8c:85:90:b6:13:32
  20156  112.225456  Allradio_17:20:57   Apple_b6:13:32      ARP      42  Who has 172.30.1.43? Tell 172.30.1.254
  20157  112.225510  Apple_b6:13:32      Allradio_17:20:57   ARP      42  172.30.1.43 is at 8c:85:90:b6:13:32
  24530  148.334548  Allradio_17:20:57   Apple_b6:13:32      ARP      42  Who has 172.30.1.43? Tell 172.30.1.254
  24531  148.334622  Apple_b6:13:32      Allradio_17:20:57   ARP      42  172.30.1.43 is at 8c:85:90:b6:13:32
```

Dns



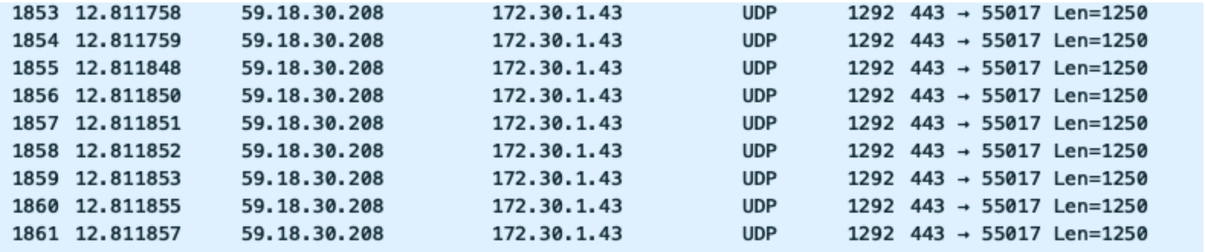
```
No.       Time        Source          Destination     Protoc ^ Length Info
    627  8.459431   172.30.1.43     168.126.63.1    DNS      78  Standard query 0xf6b8 HTTPS history.google.com
    628  8.462583   168.126.63.1    172.30.1.43     DNS     208  Standard query response 0x8d75 A history.google.com CNAME history.l.google.com A 64.233.188.102 A 64.233.188.139 A 64.233.188.100 A 64.233.188.101 A 64.23
    629  8.462588   168.126.63.1    172.30.1.43     DNS     162  Standard query response 0xf6b8 HTTPS history.google.com CNAME history.l.google.com SOA ns1.google.com
   1999  22.060887  172.30.1.43     168.126.63.1    DNS      87  Standard query 0x256d A googleads.g.doubleclick.net
   2000  22.060989  172.30.1.43     168.126.63.1    DNS      87  Standard query 0x7f1e HTTPS googleads.g.doubleclick.net
   2001  22.063579  168.126.63.1    172.30.1.43     DNS     103  Standard query response 0x256d A googleads.g.doubleclick.net A 142.251.42.130
   2002  22.063582  168.126.63.1    172.30.1.43     DNS     112  Standard query response 0x7f1e HTTPS googleads.g.doubleclick.net HTTPS
   2111  25.418857  172.30.1.43     168.126.63.1    DNS      81  Standard query 0x835c A update.googleapis.com
   2112  25.419809  172.30.1.43     168.126.63.1    DNS      81  Standard query 0x7ae4 HTTPS update.googleapis.com
   2113  25.422225  168.126.63.1    172.30.1.43     DNS      97  Standard query response 0x835c A update.googleapis.com A 142.250.196.99
   2114  25.422817  168.126.63.1    172.30.1.43     DNS     141  Standard query response 0x7ae4 HTTPS update.googleapis.com SOA ns1.google.com
   2146  25.659373  172.30.1.43     168.126.63.1    DNS      78  Standard query 0xd7e2 A edgedl.me.gvt1.com
   2147  25.659471  172.30.1.43     168.126.63.1    DNS      78  Standard query 0xc37d HTTPS edgedl.me.gvt1.com
   2148  25.663668  168.126.63.1    172.30.1.43     DNS      94  Standard query response 0xd7e2 A edgedl.me.gvt1.com A 34.104.35.123
   2149  25.663671  168.126.63.1    172.30.1.43     DNS     146  Standard query response 0xc37d HTTPS edgedl.me.gvt1.com SOA ns1.google.com
   2189  26.059546  172.30.1.43     168.126.63.1    DNS      74  Standard query 0xf86d A ocsp.apple.com
   2191  26.063270  168.126.63.1    172.30.1.43     DNS     182  Standard query response 0xf86d A ocsp.apple.com CNAME ocsp-lb.apple.com.akadns.net CNAME ocsp-a.g.aaplimg.com A 17.253.75.203 A 17.253.75.201
   2237  29.384033  172.30.1.43     168.126.63.1    DNS      74  Standard query 0xfbe6 A www.google.com
```

Tcp



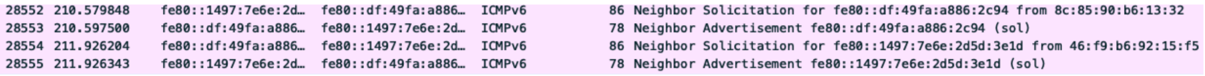
```
12364 107.158005  172.30.1.43     211.56.100.152  TCP  66 [TCP Window Update] 58221 → 443 [ACK] Seq=2000 Ack=86764 Win=131072 Len=0 TSval=480893556 TSecr=761989093
12365 107.158327  172.30.1.43     23.43.165.18    TCP  66 [TCP Window Update] 58231 → 443 [ACK] Seq=518 Ack=4002 Win=131072 Len=0 TSval=480893556 TSecr=2916774962
12366 107.158671  172.30.1.43     23.43.165.18    TCP  66 [TCP Window Update] 58230 → 443 [ACK] Seq=518 Ack=4002 Win=131072 Len=0 TSval=480893556 TSecr=2916774962
12367 107.159003  172.30.1.43     23.43.165.18    TCP  66 [TCP Window Update] 58226 → 443 [ACK] Seq=518 Ack=4002 Win=131072 Len=0 TSval=480893557 TSecr=2916774962
12368 107.159392  172.30.1.43     23.43.165.18    TCP  66 [TCP Window Update] 58227 → 443 [ACK] Seq=518 Ack=4002 Win=131072 Len=0 TSval=480893557 TSecr=2916774963
12369 107.160472  172.30.1.43     23.43.165.18    TCP  66 [TCP Window Update] 58229 → 443 [ACK] Seq=518 Ack=4002 Win=131072 Len=0 TSval=480893558 TSecr=2916774963
12370 107.160694  172.30.1.43     23.43.165.18    TCP  66 [TCP Window Update] 58228 → 443 [ACK] Seq=518 Ack=4002 Win=131072 Len=0 TSval=480893558 TSecr=2916774964
12378 107.176553  211.56.100.152  172.30.1.43     TCP  66 443 → 58221 [ACK] Seq=86764 Ack=2035 Win=49152 Len=0 TSval=761989132 TSecr=480893535
12385 107.184530  172.30.1.43     23.43.165.18    TCP  66 58230 → 443 [FIN, ACK] Seq=598 Ack=4002 Win=131072 Len=0 TSval=480893580 TSecr=2916774962
12386 107.184714  23.43.165.18    172.30.1.43     TCP  66 443 → 58231 [ACK] Seq=4002 Ack=598 Win=64768 Len=0 TSval=2916775007 TSecr=480893578
12387 107.184726  172.30.1.43     23.43.165.18    TCP  66 58226 → 443 [FIN, ACK] Seq=598 Ack=4002 Win=131072 Len=0 TSval=480893580 TSecr=2916774962
12388 107.184817  172.30.1.43     23.43.165.18    TCP  66 58227 → 443 [FIN, ACK] Seq=598 Ack=4002 Win=131072 Len=0 TSval=480893581 TSecr=2916774963
12389 107.184871  172.30.1.43     23.43.165.18    TCP  66 58229 → 443 [FIN, ACK] Seq=598 Ack=4002 Win=131072 Len=0 TSval=480893581 TSecr=2916774963
12390 107.184913  172.30.1.43     23.43.165.18    TCP  66 58228 → 443 [FIN, ACK] Seq=598 Ack=4002 Win=131072 Len=0 TSval=480893581 TSecr=2916774964
12400 107.186894  23.43.165.18    172.30.1.43     TCP  66 443 → 58230 [ACK] Seq=4002 Ack=598 Win=64768 Len=0 TSval=2916775008 TSecr=480893578
12401 107.186895  23.43.165.18    172.30.1.43     TCP  66 443 → 58227 [ACK] Seq=4002 Ack=598 Win=64768 Len=0 TSval=2916775009 TSecr=480893579
12402 107.186896  23.43.165.18    172.30.1.43     TCP  66 443 → 58226 [ACK] Seq=4002 Ack=598 Win=64768 Len=0 TSval=2916775009 TSecr=480893579
12408 107.186945  172.30.1.43     23.43.165.18    TCP  66 58231 → 443 [ACK] Seq=1975 Ack=4289 Win=130752 Len=0 TSval=480893583 TSecr=2916775008
12409 107.186978  172.30.1.43     23.43.165.18    TCP  66 58231 → 443 [ACK] Seq=1975 Ack=4576 Win=130496 Len=0 TSval=480893583 TSecr=2916775008
12410 107.186983  172.30.1.43     23.43.165.18    TCP  54 58230 → 443 [RST] Seq=598 Win=0 Len=0
12411 107.186996  172.30.1.43     23.43.165.18    TCP  54 58230 → 443 [RST] Seq=598 Win=0 Len=0
12412 107.187022  172.30.1.43     23.43.165.18    TCP  54 58226 → 443 [RST] Seq=598 Win=0 Len=0
12413 107.187022  172.30.1.43     23.43.165.18    TCP  54 58226 → 443 [RST] Seq=598 Win=0 Len=0
```

Udp



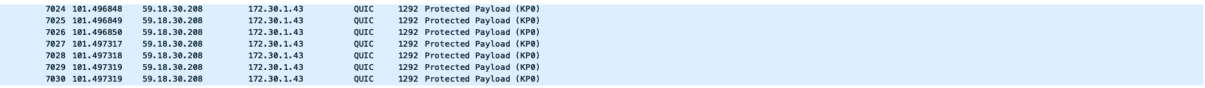
```
1853  12.811758   59.18.30.208   172.30.1.43   UDP   1292  443 → 55017 Len=1250
1854  12.811759   59.18.30.208   172.30.1.43   UDP   1292  443 → 55017 Len=1250
1855  12.811848   59.18.30.208   172.30.1.43   UDP   1292  443 → 55017 Len=1250
1856  12.811850   59.18.30.208   172.30.1.43   UDP   1292  443 → 55017 Len=1250
1857  12.811851   59.18.30.208   172.30.1.43   UDP   1292  443 → 55017 Len=1250
1858  12.811852   59.18.30.208   172.30.1.43   UDP   1292  443 → 55017 Len=1250
1859  12.811853   59.18.30.208   172.30.1.43   UDP   1292  443 → 55017 Len=1250
1860  12.811855   59.18.30.208   172.30.1.43   UDP   1292  443 → 55017 Len=1250
1861  12.811857   59.18.30.208   172.30.1.43   UDP   1292  443 → 55017 Len=1250
```

Icmp

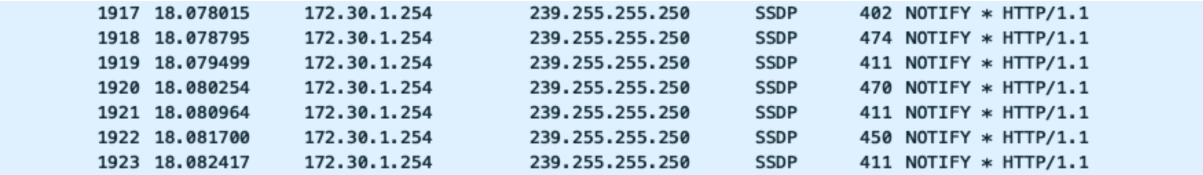


```
28552  210.579848   fe80::1497:7e6e:2d…  fe80::df:49fa:a886…  ICMPv6   86 Neighbor Solicitation for fe80::df:49fa:a886:2c94 from 8c:85:90:b6:13:32
28553  210.597500   fe80::df:49fa:a886…  fe80::1497:7e6e:2d…  ICMPv6   78 Neighbor Advertisement fe80::df:49fa:a886:2c94 (sol)
28554  211.926204   fe80::df:49fa:a886…  fe80::1497:7e6e:2d…  ICMPv6   86 Neighbor Solicitation for fe80::1497:7e6e:2d5d:3e1d from 46:f9:b6:92:15:f5
28555  211.926343   fe80::1497:7e6e:2d…  fe80::df:49fa:a886…  ICMPv6   78 Neighbor Advertisement fe80::1497:7e6e:2d5d:3e1d (sol)
```

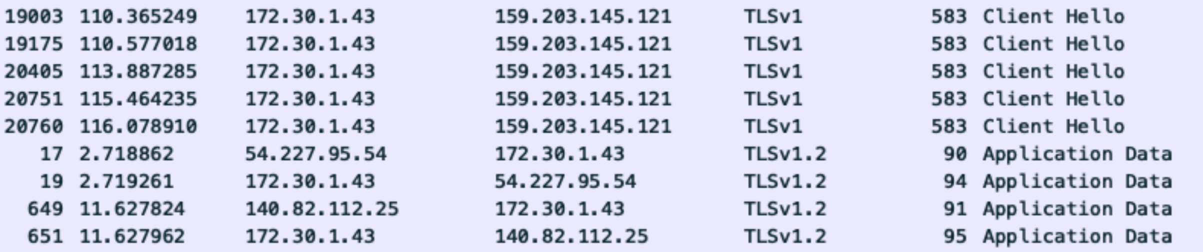
Others (quic, ssdp, tlsv1)



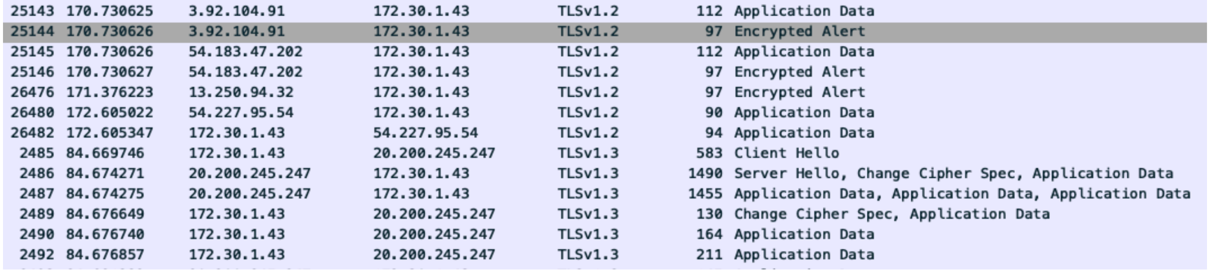
```
   7024 101.496848   59.18.30.208    172.30.1.43    QUIC   1292 Protected Payload (KP0)
   7025 101.496849   59.18.30.208    172.30.1.43    QUIC   1292 Protected Payload (KP0)
   7026 101.496850   59.18.30.208    172.30.1.43    QUIC   1292 Protected Payload (KP0)
   7027 101.497317   59.18.30.208    172.30.1.43    QUIC   1292 Protected Payload (KP0)
   7028 101.497318   59.18.30.208    172.30.1.43    QUIC   1292 Protected Payload (KP0)
   7029 101.497319   59.18.30.208    172.30.1.43    QUIC   1292 Protected Payload (KP0)
   7030 101.497319   59.18.30.208    172.30.1.43    QUIC   1292 Protected Payload (KP0)
```



```
 1917 18.078015   172.30.1.254    239.255.255.250   SSDP   402 NOTIFY * HTTP/1.1
 1918 18.078795   172.30.1.254    239.255.255.250   SSDP   474 NOTIFY * HTTP/1.1
 1919 18.079499   172.30.1.254    239.255.255.250   SSDP   411 NOTIFY * HTTP/1.1
 1920 18.080254   172.30.1.254    239.255.255.250   SSDP   470 NOTIFY * HTTP/1.1
 1921 18.080964   172.30.1.254    239.255.255.250   SSDP   411 NOTIFY * HTTP/1.1
 1922 18.081700   172.30.1.254    239.255.255.250   SSDP   450 NOTIFY * HTTP/1.1
 1923 18.082417   172.30.1.254    239.255.255.250   SSDP   411 NOTIFY * HTTP/1.1
```



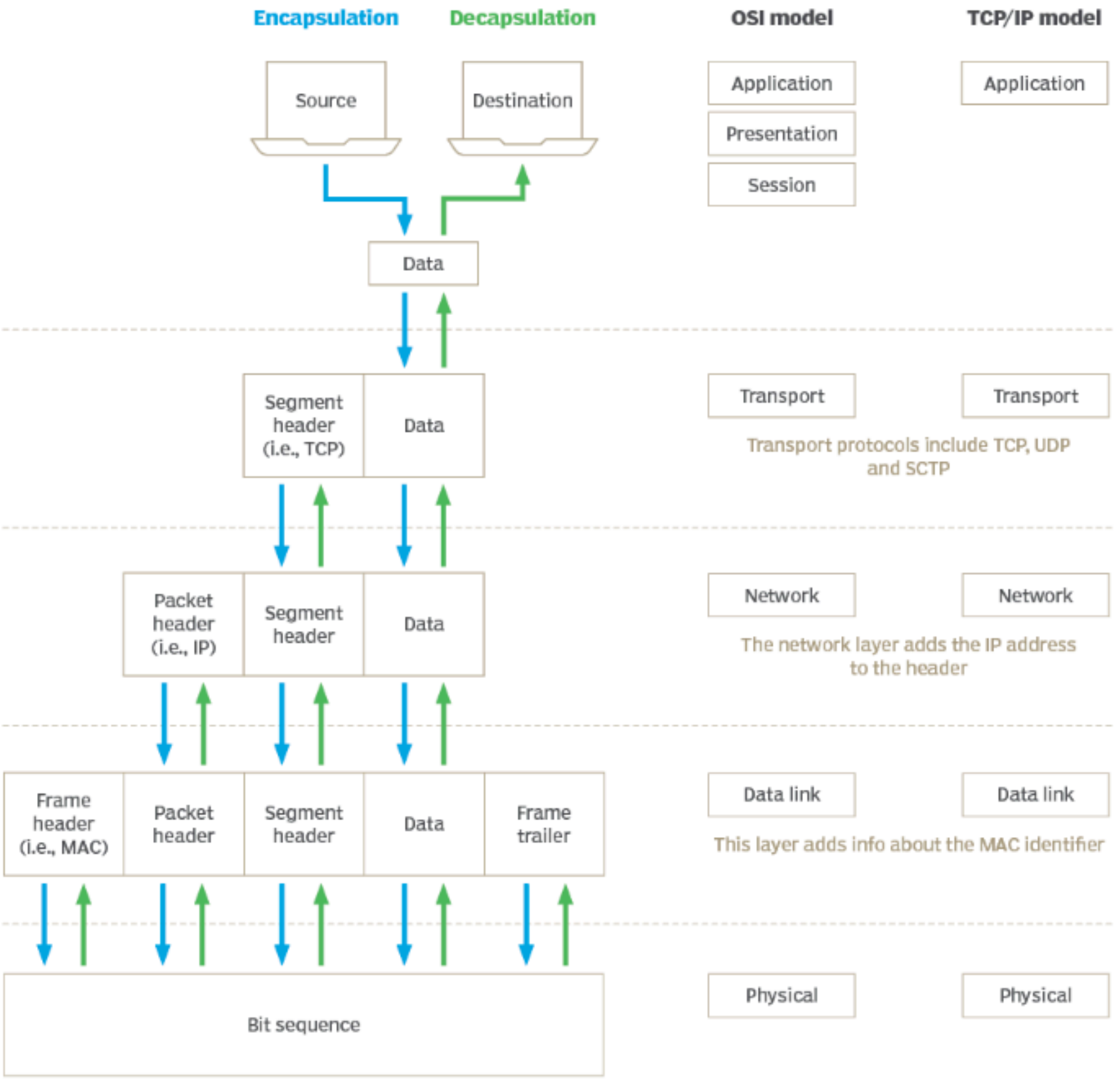
```
19003 110.365249  172.30.1.43    159.203.145.121  TLSv1      583 Client Hello
19175 110.577018  172.30.1.43    159.203.145.121  TLSv1      583 Client Hello
20405 113.887285  172.30.1.43    159.203.145.121  TLSv1      583 Client Hello
20751 115.464235  172.30.1.43    159.203.145.121  TLSv1      583 Client Hello
20760 116.078910  172.30.1.43    159.203.145.121  TLSv1      583 Client Hello
   17 2.718862    54.227.95.54   172.30.1.43      TLSv1.2     90 Application Data
   19 2.719261    172.30.1.43    54.227.95.54     TLSv1.2     94 Application Data
  649 11.627824   140.82.112.25  172.30.1.43      TLSv1.2     91 Application Data
  651 11.627962   172.30.1.43    140.82.112.25    TLSv1.2     95 Application Data
```



```
25143 170.730625   3.92.104.91      172.30.1.43      TLSv1.2   112 Application Data
25144 170.730626   3.92.104.91      172.30.1.43      TLSv1.2    97 Encrypted Alert
25145 170.730626   54.183.47.202    172.30.1.43      TLSv1.2   112 Application Data
25146 170.730627   54.183.47.202    172.30.1.43      TLSv1.2    97 Encrypted Alert
26476 171.376223   13.250.94.32     172.30.1.43      TLSv1.2    97 Encrypted Alert
26480 172.605022   54.227.95.54     172.30.1.43      TLSv1.2    90 Application Data
26482 172.605347   172.30.1.43      54.227.95.54     TLSv1.2    94 Application Data
 2485 84.669746    172.30.1.43      20.200.245.247   TLSv1.3   583 Client Hello
 2486 84.674271    20.200.245.247   172.30.1.43      TLSv1.3  1490 Server Hello, Change Cipher Spec, Application Data
 2487 84.674275    20.200.245.247   172.30.1.43      TLSv1.3  1455 Application Data, Application Data, Application Data
 2489 84.676649    172.30.1.43      20.200.245.247   TLSv1.3   130 Change Cipher Spec, Application Data
 2490 84.676740    172.30.1.43      20.200.245.247   TLSv1.3   164 Application Data
 2492 84.676857    172.30.1.43      20.200.245.247   TLSv1.3   211 Application Data
```

(3) By capturing packets, explain the process of encapsulating and decapsulating packets.

Encapsulation adds information to a packet as it travels to its destination.
Decapsulation reverses the process by removing the info, so a destination device can read the original data.



Encapsulation
Decapsulation
OSI model
TCP/IP model
Source
Destination
Application
Presentation
Session
Application
Data
Segment header (i.e., TCP)
Data
Transport
Transport
Transport protocols include TCP, UDP and SCTP
Packet header (i.e., IP)
Segment header
Data
Network
Network
The network layer adds the IP address to the header
Frame header (i.e., MAC)
Packet header
Segment header
Data
Frame trailer
Data link
Data link
This layer adds info about the MAC identifier
Bit sequence
Physical
Physical