Report for ECE4016 assignment 3

Feng Yutong 120090266

Task 1: Network test commands

Commands meaning

1. ifconfig

- Function: view the IP address and NIC information of the current host
- Capture:

```
(base) thea@fengdeMacBook-Air ~ % ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
        options=1203<RXCSUM,TXCSUM,TXSTATUS,SW_TIMESTAMP>
        inet 127.0.0.1 netmask 0xff000000
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
        nd6 options=201<PERFORMNUD,DAD>
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
stf0: flags=0<> mtu 1280
anpi1: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=400<CHANNEL_IO>
        ether 66:75:e9:83:3e:e9
        inet6 fe80::6475:e9ff:fe83:3ee9%anpi1 prefixlen 64 scopeid 0x4
        nd6 options=201<PERFORMNUD,DAD>
        media: none
        status: inactive
anpi0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=400<CHANNEL_IO>
        ether 66:75:e9:83:3e:e8
        inet6 fe80::6475:e9ff:fe83:3ee8%anpi0 prefixlen 64 scopeid 0x5
        nd6 options=201<PERFORMNUD,DAD>
        media: none
        status: inactive
en3: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=400<CHANNEL_IO>
        ether 66:75:e9:83:3e:c8
        nd6 options=201<PERFORMNUD,DAD>
        media: none
        status: inactive
en4: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=400<CHANNEL_IO>
        ether 66:75:e9:83:3e:c9
        nd6 options=201<PERFORMNUD,DAD>
        media: none
        status: inactive
en1: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
        options=460<TSO4,TSO6,CHANNEL_IO>
        ether 36:cd:13:76:1f:40
        media: autoselect <full-duplex>
        status: inactive
en2: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
        options=460<TSO4,TSO6,CHANNEL_IO>
        ether 36:cd:13:76:1f:44
        media: autoselect <full-duplex>
        status: inactive
ap1: flags=8802<BROADCAST,SIMPLEX,MULTICAST> mtu 1500
        options=400<CHANNEL_IO>
        ether f2:88:0c:6a:d3:2e
        media: autoselect
        status: inactive
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=6463<RXCSUM,TXCSUM,TSO4,TSO6,CHANNEL_IO,PARTIAL_CSUM,ZEROINVERT_CSUM>
        ether d0:88:0c:6a:d3:2e
        inet6 fe80::858:ac:e401:a40f%en0 prefixlen 64 secured scopeid 0xb
        inet 10.31.161.211 netmask 0xfffff000 broadcast 10.31.175.255
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect
        status: active
```

```
bridge0: flags=8822<BROADCAST,SMART,SIMPLEX,MULTICAST> mtu 1500
        options=63<RXCSUM,TXCSUM,TSO4,TSO6>
        ether 36:cd:13:76:1f:40
        Configuration:
                id 0:0:0:0:0:0 priority 0 hellotime 0 fwddelay 0
                maxage 0 holdcnt 0 proto stp maxaddr 100 timeout 1200
                root id 0:0:0:0:0:0 priority 0 ifcost 0 port 0
                ipfilter disabled flags 0x0
        member: en1 flags=3<LEARNING,DISCOVER>
                ifmaxaddr 0 port 8 priority 0 path cost 0
        member: en2 flags=3<LEARNING,DISCOVER>
                ifmaxaddr 0 port 9 priority 0 path cost 0
        media: <unknown type>
        status: inactive
awdl0: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
        options=400<CHANNEL_IO>
        ether ae:94:6c:fa:b4:a2
        inet6 fe80::ac94:6cff:fefa:b4a2%awdl0 prefixlen 64 scopeid 0xd
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect
        status: active
llw0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=400<CHANNEL_IO>
        ether ae:94:6c:fa:b4:a2
        inet6 fe80::ac94:6cff:fefa:b4a2%llw0 prefixlen 64 scopeid 0xe
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect
        status: active
utun0: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 2000
        inet6 fe80::5486:ada2:d3f1:c524%utun0 prefixlen 64 scopeid 0xf
        nd6 options=201<PERFORMNUD,DAD>
utun1: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1000
        inet6 fe80::ce81:b1c:bd2c:69e%utun1 prefixlen 64 scopeid 0x10
        nd6 options=201<PERFORMNUD,DAD>
utun2: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1380
        inet6 fe80::c891:6899:e11f:39b3%utun2 prefixlen 64 scopeid 0x11
        nd6 options=201<PERFORMNUD,DAD>
```

- Explanation:

```
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
options=1203<RXCSUM,TXCSUM,TXSTATUS,SW_TIMESTAMP>
\\ lo: loopback address
\\ flag: network device status identifier
\\ UP: network card is in the boot state
\\ LOOPBACK: packets are sent back to the local machine,
usually used to test network configuration and communication
between local applications
\\ RUNNING: network cable representing the network card is
connected
\\ MULTICAS: The network card can send multicast packets
\\ mtu: maximum transmission unit
```

```
\\ options: parameters
    inet 127.0.0.1 netmask 0xff000000
    \\ inet: IPV4 address, netmask: subnet netmask
    inet6 ::1 prefixlen 128
    inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
    \\ inet6: IPV6 address
    nd6 options=201<PERFORMNUD,DAD>
```

```
gif: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
\\ gif0: software network interface
\\ POINTOPOINT: allows direct point-to-point connection
between 2 machines
```

```
stf0: flags=0<> mtu 1280
\\ stf: IPV6 to IPV4 tunnel interface
```

```
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST>
mtu 1500
options=6463<RXCSUM,TXCSUM,TSO4,TSO6,CHANNEL_IO,PARTIAL_CSUM,Z
EROINVERT_CSUM>
\\ en: ethernet (en0: WIFI, en1,en2...: thunderbolt)
\\ BROADCAST: Supports broadcast packets
ether d0:88:0c:6a:d3:2e
inet6 fe80::858:ac:e401:a40f%en0 prefixlen 64 secured scopeid
0xb
inet 10.31.161.211 netmask 0xfffff000 broadcast 10.31.175.255
\\ inet: IPV4 address, netmask: subnet mask, broadcast:
broadcast address
nd6 options=201<PERFORMNUD,DAD>
media: autoselect
status: active
```

```
bridge0: flags=8822<BROADCAST,SMART,SIMPLEX,MULTICAST> mtu
1500
```

```
  options=63<RXCSUM,TXCSUM,TSO4,TSO6>
  \\ bridge: a bridge interface creates a logical link between
two or more Ethernet interfaces or encapsulation interfaces
  ether 36:cd:13:76:1f:40
  Configuration:
      id 0:0:0:0:0:0 priority 0 hellotime 0 fwddelay 0
      maxage 0 holdcnt 0 proto stp maxaddr 100 timeout 1200
      root id 0:0:0:0:0:0 priority 0 ifcost 0 port 0
      ipfilter disabled flags 0x0
  member: en1 flags=3<LEARNING,DISCOVER>
          ifmaxaddr 0 port 8 priority 0 path cost 0
  member: en2 flags=3<LEARNING,DISCOVER>
          ifmaxaddr 0 port 9 priority 0 path cost 0
  media: <unknown type>
  status: inactive
```

```
awdl0:
flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu
1500
\\ awdl: airdrop peer to peer(a mesh network), specific to
apple airdrop devices
\\ PROMISC: promiscuous mode allowed (all data will be
received by the interface)
  ...
```

```
llw0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST>
mtu 1500
\\ llw: WLAN low-latency interface with an access point
  ...
```

```
utun0: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 2000
\\ utun: used for "Back to My Mac"
  ...
```

2. ping (ICMP)

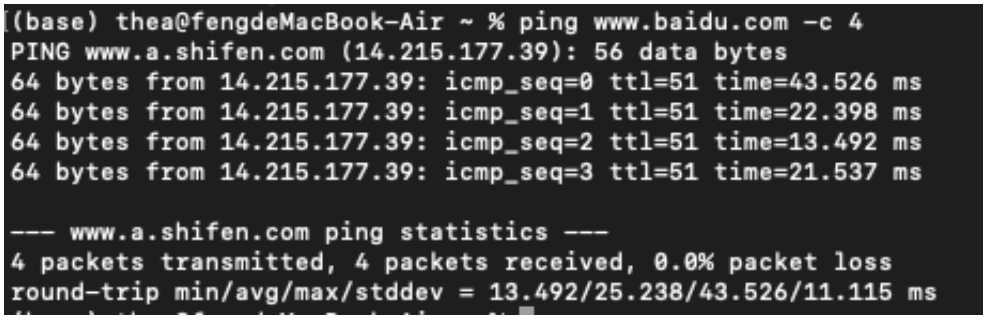
- Function: to detect the time required for a frame to be transmitted from the current host to the destination host; to determine whether the network between two computers is connected; predicting failures and determining the source of failure is very effective.
- Common options:

```
-c Count: the number of callback signal requests to send or receive
-s PacketSize
```

- Return Value

```
icmp_seq: ICMP packet sequence number
ttl: packet lifetime
time: time between sending a packet to receiving information
```

- Capture (BAIDU as example)



3. arp (address resolution protocol)

- Function: a TCP/IP protocol for obtaining a physical address from an IP address. When a host sends a message, it broadcasts an ARP request containing the target IP address to all hosts in the network, and receives a response message to determine the physical address of the target.
- Common option

```
arp -a: display arp cache
// To prevent ARP attacks, use the arp-s command to bind the IP
address and MAC address and then arp-a to display static
```

- Capture

```
(base) thea@fengdeMacBook-Air ~ % arp -a
? (10.31.1.28) at d4:94:e8:19:83:7 on en0 ifscope [ethernet]
? (10.31.1.37) at d4:94:e8:19:83:7 on en0 ifscope [ethernet]
? (10.31.2.122) at d4:94:e8:19:83:7 on en0 ifscope [ethernet]
? (10.31.4.43) at d4:94:e8:19:83:7 on en0 ifscope [ethernet]
? (10.31.5.0) at d4:94:e8:19:83:7 on en0 ifscope [ethernet]
? (10.31.5.8) at d4:94:e8:19:83:7 on en0 ifscope [ethernet]
? (10.31.5.169) at d4:94:e8:19:83:7 on en0 ifscope [ethernet]
? (10.31.5.249) at d4:94:e8:19:83:7 on en0 ifscope [ethernet]
? (10.31.6.102) at d4:94:e8:19:83:7 on en0 ifscope [ethernet]
? (10.31.6.111) at d4:94:e8:19:83:7 on en0 ifscope [ethernet]
? (10.31.6.142) at d4:94:e8:19:83:7 on en0 ifscope [ethernet]
? (10.31.7.108) at d4:94:e8:19:83:7 on en0 ifscope [ethernet]
? (10.31.7.140) at d4:94:e8:19:83:7 on en0 ifscope [ethernet]
? (10.31.7.254) at d4:94:e8:19:83:7 on en0 ifscope [ethernet]
? (10.31.7.255) at ff:ff:ff:ff:ff:ff on en0 ifscope [ethernet]
? (224.0.0.251) at 1:0:5e:0:0:fb on en0 ifscope permanent [ethernet]
? (239.255.255.250) at 1:0:5e:7f:ff:fa on en0 ifscope permanent [ethernet]
```

4. nslookup (name server lookup)

- Function: a tool for querying internet domain name information or diagnosing problems with DNS servers

```
(base) thea@fengdeMacBook-Air ~ % nslookup www.baidu.com
Server:         10.20.232.47
Address:        10.20.232.47#53

Non-authoritative answer:
www.baidu.com   canonical name = www.a.shifen.com.
Name:   www.a.shifen.com
Address: 14.215.177.39
Name:   www.a.shifen.com
Address: 14.215.177.38
```

- Capture (BAIDU as example)
- Return value: domain name, IP address, CNAME

5. netstat (TCP)

- Function: show overall usage of the network; display detailed information about the active network connection, such as protocol and connection status
- Common options

```
-a shows all session data
-i lists each network card defined by the system
-r shows the computer's current route list
-s shows the current network protocol statistics
-t or -tcp: displays the connection status for TCP
-u or -udp: This indicates the connection status for UDP
```

- Status list
  - LISTEN, ESTABLISHED, TIME_WAIT, CLOSE_WAIT...
- Capture

```
(base) thea@fengdeMacBook-Air ~ % netstat -t
Active Internet connections
Proto Recv-Q Send-Q  Local Address          Foreign Address        (state)
tcp4       0      0  10.31.5.43.56007       113.96.142.1.https     ESTABLISHED
tcp4       0      0  localhost.4780         localhost.56006        ESTABLISHED
tcp4       0      0  localhost.56006        localhost.4780         ESTABLISHED
tcp4       0      0  10.31.5.43.55998       36.139.105.105.10059   ESTABLISHED
tcp4       0      0  localhost.4780         localhost.55997        ESTABLISHED
tcp4       0      0  localhost.55997        localhost.4780         ESTABLISHED
tcp4       0      0  10.31.5.43.55962       36.139.105.105.10059   ESTABLISHED
tcp4       0      0  localhost.4780         localhost.55959        ESTABLISHED
tcp4       0      0  localhost.55959        localhost.4780         ESTABLISHED
tcp4       0      0  10.31.5.43.55571       36.139.105.105.10059   ESTABLISHED
tcp4       0      0  localhost.4781         localhost.55570        ESTABLISHED
tcp4       0      0  localhost.55570        localhost.4781         ESTABLISHED
tcp4       0      0  10.31.5.43.55487       36.139.105.105.10059   ESTABLISHED
tcp4       0      0  localhost.4780         localhost.55486        ESTABLISHED
tcp4       0      0  localhost.55486        localhost.4780         ESTABLISHED
tcp4       0      0  10.31.5.43.55111       110.43.67.241.http     CLOSE_WAIT
tcp4       0      0  10.31.5.43.54673       ecs-119-3-227-18.vce   ESTABLISHED
tcp4       0      0  localhost.4781         localhost.54672        ESTABLISHED
tcp4       0      0  localhost.54672        localhost.4781         ESTABLISHED
tcp4       0      0  10.31.5.43.54656       17.57.145.165.5223     ESTABLISHED
tcp4       0      0  10.31.5.43.54458       40.99.33.178.https     ESTABLISHED
tcp4       0      0  localhost.4780         localhost.54457        ESTABLISHED
tcp4       0      0  localhost.54457        localhost.4780         ESTABLISHED
tcp4      31      0  10.31.5.43.54432       110.43.120.18.https    CLOSE_WAIT
tcp4      31      0  10.31.5.43.54431       110.43.120.18.https    CLOSE_WAIT
tcp4      31      0  10.31.5.43.54429       110.43.120.18.https    CLOSE_WAIT
tcp4      31      0  10.31.5.43.54428       110.43.120.18.https    CLOSE_WAIT
tcp4       0      0  10.31.5.43.53835       40.99.8.194.https      ESTABLISHED
tcp4       0      0  localhost.4780         localhost.53834        ESTABLISHED
tcp4       0      0  localhost.53834        localhost.4780         ESTABLISHED
tcp4       0      0  10.31.5.43.53546       36.139.105.105.10059   ESTABLISHED
tcp4       0      0  localhost.4780         localhost.53545        ESTABLISHED
tcp4       0      0  localhost.53545        localhost.4780         ESTABLISHED
tcp4       0      0  10.31.5.43.53544       36.139.105.105.10059   ESTABLISHED
tcp4       0      0  localhost.4780         localhost.53543        ESTABLISHED
tcp4       0      0  localhost.53543        localhost.4780         ESTABLISHED
tcp4       0      0  10.31.5.43.53542       36.139.105.105.10059   ESTABLISHED
tcp4       0      0  localhost.4780         localhost.53541        ESTABLISHED
tcp4       0      0  localhost.53541        localhost.4780         ESTABLISHED
tcp4       0      0  10.31.5.43.53441       220.181.43.8.http      ESTABLISHED
tcp4       0      0  10.31.5.43.53301       157.148.62.239.http    ESTABLISHED
tcp4    1018      0  10.31.5.43.53300       reverse.gdsz.cnc.http  CLOSE_WAIT
tcp4       0      0  localhost.4788         localhost.53272        ESTABLISHED
tcp4       0      0  localhost.53272        localhost.4788         ESTABLISHED
tcp4       0      0  10.31.5.43.53255       175.24.155.20.https    ESTABLISHED
tcp4       0      0  localhost.4780         localhost.53249        ESTABLISHED
tcp4       0      0  localhost.53249        localhost.4780         ESTABLISHED
tcp4      31      0  10.31.5.43.53246       ecs-124-70-24-18.https CLOSE_WAIT
tcp4      31      0  10.31.5.43.53233       36.25.241.123.https    CLOSE_WAIT
tcp4      31      0  10.31.5.43.53177       120.92.74.246.https    CLOSE_WAIT
tcp4       0      0  10.31.5.43.53083       ecs-121-36-83-10.http  CLOSE_WAIT
tcp4      31      0  10.31.5.43.53067       ecs-121-36-23-20.https CLOSE_WAIT
tcp4       0      0  10.31.5.43.53023       115.236.118.34.https   ESTABLISHED
tcp4       0      0  localhost.4780         localhost.53022        ESTABLISHED
```

```
(base) thea@fengdeMacBook-Air ~ % netstat -i
Name       Mtu   Network       Address            Ipkts Ierrs    Opkts Oerrs  Coll
lo0        16384 <Link#1>                       1378602     0  1378602     0     0
lo0        16384 127           localhost        1378602     -  1378602     -     -
lo0        16384 localhost   ::1                1378602     -  1378602     -     -
lo0        16384 fengdemacbo fe80:1::1          1378602     -  1378602     -     -
gif0*      1280  <Link#2>                             0     0        0     0     0
stf0*      1280  <Link#3>                             0     0        0     0     0
anpi1      1500  <Link#4>    66:75:e9:83:3e:e9        0     0        0     0     0
anpi1      1500  fengdemacbo fe80:4::6475:e9ff        0     -        0     -     -
anpi0      1500  <Link#5>    66:75:e9:83:3e:e8        0     0        0     0     0
anpi0      1500  fengdemacbo fe80:5::6475:e9ff        0     -        0     -     -
en3        1500  <Link#6>    66:75:e9:83:3e:c8        0     0        0     0     0
en4        1500  <Link#7>    66:75:e9:83:3e:c9        0     0        0     0     0
en1        1500  <Link#8>    36:cd:13:76:1f:40        0     0        0     0     0
en2        1500  <Link#9>    36:cd:13:76:1f:44        0     0        0     0     0
ap1*       1500  <Link#10>   f2:88:0c:6a:d3:2e        0     0        0     0     0
en0        1500  <Link#11>   d0:88:0c:6a:d3:2e  4209445     0  1634007     0     0
en0        1500  fengdemacbo fe80:b::858:ac:e4  4209445     -  1634007     -     -
en0        1500  10.31/21      10.31.5.43       4209445     -  1634007     -     -
bridge0*   1500  <Link#12>   36:cd:13:76:1f:40        0     0        0     0     0
awdl0      1500  <Link#13>   ca:ee:dd:77:0e:66   608000     0     4355     0     0
awdl0      1500  fe80::c8ee: fe80:d::c8ee:ddff   608000     -     4355     -     -
llw0       1500  <Link#14>   ca:ee:dd:77:0e:66        0     0        0     0     0
llw0       1500  fe80::c8ee: fe80:e::c8ee:ddff        0     -        0     -     -
utun0      2000  <Link#15>                            0     0       13     0     0
utun0      2000  fengdemacbo fe80:f::5486:ada2        0     -       13     -     -
utun1      1000  <Link#16>                            0     0       13     0     0
utun1      1000  fengdemacbo fe80:10::ce81:b1c        0     -       13     -     -
utun2      1380  <Link#17>                            0     0       13     0     0
utun2      1380  fengdemacbo fe80:11::c891:689        0     -       13     -     -
```

6. tracert/traceroute (ICMP)

- Function: displays the path between the locol host and the destination host
- Capture

```
(base) thea@fengdeMacBook-Air ~ % traceroute www.baidu.com
traceroute: Warning: www.baidu.com has multiple addresses; using 14.215.177.39
traceroute to www.a.shifen.com (14.215.177.39), 64 hops max, 52 byte packets
 1  10.31.7.254 (10.31.7.254)  27.677 ms  16.172 ms  10.234 ms
 2  10.40.0.53 (10.40.0.53)  20.028 ms  12.399 ms  8.337 ms
 3  10.20.238.25 (10.20.238.25)  21.764 ms  20.743 ms  23.672 ms
 4  10.20.238.1 (10.20.238.1)  30.782 ms  21.756 ms  18.446 ms
 5  10.20.238.19 (10.20.238.19)  36.288 ms  8.923 ms  11.133 ms
 6  58.250.174.65 (58.250.174.65)  22.269 ms  20.519 ms  64.453 ms
 7  120.80.158.133 (120.80.158.133)  62.885 ms
    120.80.158.129 (120.80.158.129)  49.557 ms
    120.80.198.145 (120.80.198.145)  19.832 ms
 8  * * 157.148.0.189 (157.148.0.189)  42.531 ms
 9  219.158.9.38 (219.158.9.38)  26.005 ms
    219.158.9.34 (219.158.9.34)  63.329 ms
    219.158.9.30 (219.158.9.30)  35.362 ms
10  202.97.16.9 (202.97.16.9)  30.674 ms *  32.722 ms
11  202.97.95.129 (202.97.95.129)  25.019 ms  24.736 ms  21.811 ms
12  * * *
13  113.96.11.78 (113.96.11.78)  51.586 ms  14.617 ms  17.585 ms
14  14.215.32.126 (14.215.32.126)  27.595 ms
    14.29.117.246 (14.29.117.246)  25.721 ms
    14.29.117.242 (14.29.117.242)  30.383 ms
```

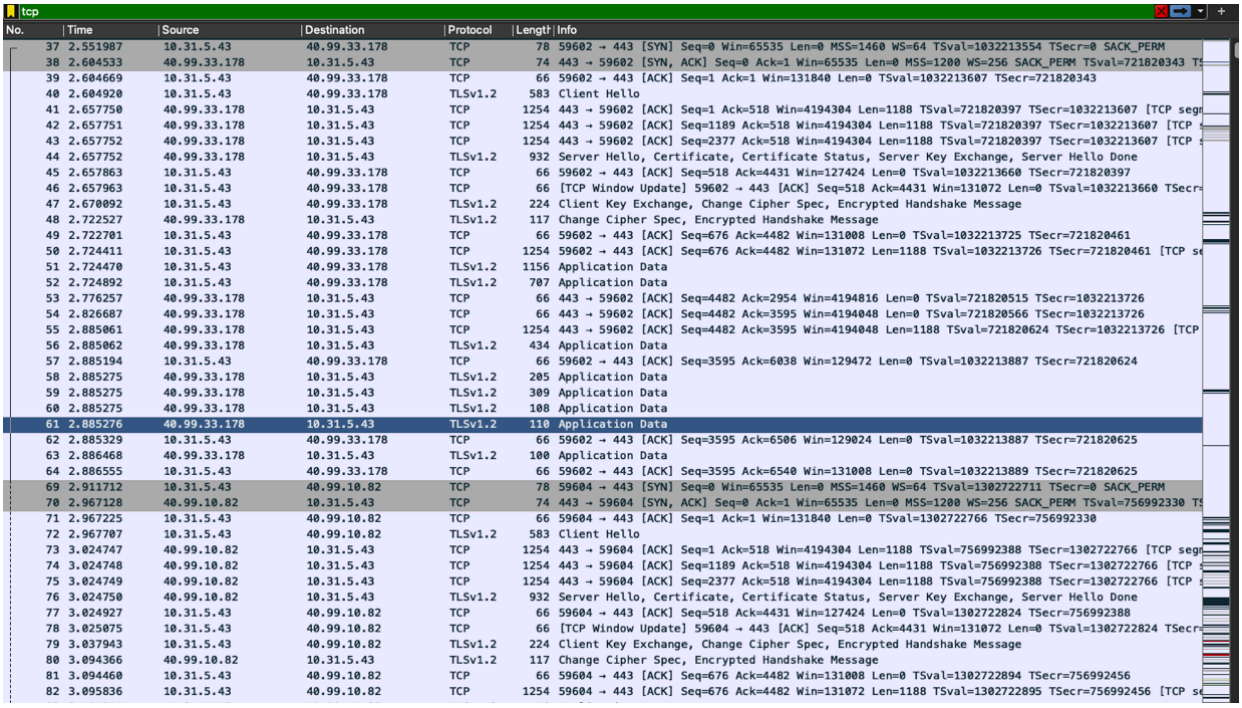
- Explanation: return routes passed by and the corresponding latency (* is caused by timeout)

TCP/UDP Capture (For part below, the No. in analysis part is chose from Wireshark capture)

- TCP
  - Tshark

```
(base) thea@fengdeMacBook-Air ~ % tshark -i en0 -f 'tcp'
Capturing on 'Wi-Fi: en0'
 ** (tshark:15363) 18:45:31.959832 [Main MESSAGE] -- Capture started.
 ** (tshark:15363) 18:45:31.960195 [Main MESSAGE] -- File: "/var/folders/n6/pjddxglj74vc5hxx_jss8d6w0000gn/T/wireshark_Wi-FiCXG7W1.pcapng"
    1   0.000000 10.31.185.96 → 10.31.5.43   TCP 78 53828 → 7000 [SYN] Seq=0 Win=65535 Len=0 MSS=1380 WS=32 TSval=1486456596 TSecr=0 SACK_PERM
    2   0.000217   10.31.5.43 → 10.31.185.96 TCP 78 7000 → 53828 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=64 TSval=4263679616 TSecr=1486456596 SACK_PERM
    3   0.019131 10.31.185.96 → 10.31.5.43   TCP 66 53828 → 7000 [ACK] Seq=1 Ack=1 Win=131328 Len=0 TSval=1486456607 TSecr=4263679616
    4   0.019133 10.31.185.96 → 10.31.5.43   TCP 107 53828 → 7000 [PSH, ACK] Seq=1 Ack=1 Win=131328 Len=41 TSval=1486456607 TSecr=4263679616 [TCP segment of a reassembled PDU]
    5   0.019260   10.31.5.43 → 10.31.185.96 TCP 66 7000 → 53828 [ACK] Seq=1 Ack=42 Win=131264 Len=0 TSval=4263679635 TSecr=1486456607
    6   0.026155   10.31.5.43 → 10.31.185.96 TCP 1434 7000 → 53828 [ACK] Seq=1 Ack=42 Win=131264 Len=1368 TSval=4263679642 TSecr=1486456607 [TCP segment of a reassembled PDU]
    7   0.026265   10.31.5.43 → 10.31.185.96 TCP 382 7000 → 53828 [PSH, ACK] Seq=1369 Ack=42 Win=131264 Len=316 TSval=4263679642 TSecr=1486456607 [TCP segment of a reassembled PDU]
    8   0.040876 10.31.185.96 → 10.31.5.43   TCP 66 53828 → 7000 [ACK] Seq=42 Ack=1685 Win=129632 Len=0 TSval=1486456629 TSecr=4263679642
    9   0.040878 10.31.185.96 → 10.31.5.43   TCP 66 53828 → 7000 [FIN, ACK] Seq=42 Ack=1685 Win=131072 Len=0 TSval=1486456630 TSecr=4263679642
   10   0.040991   10.31.5.43 → 10.31.185.96 TCP 66 7000 → 53828 [ACK] Seq=1685 Ack=43 Win=131264 Len=0 TSval=4263679657 TSecr=1486456630
   11   0.041131   10.31.5.43 → 10.31.185.96 TCP 66 7000 → 53828 [FIN, ACK] Seq=1685 Ack=43 Win=131264 Len=0 TSval=4263679657 TSecr=1486456630
   12   0.052914 10.31.185.96 → 10.31.5.43   TCP 66 53828 → 7000 [ACK] Seq=43 Ack=1686 Win=131072 Len=0 TSval=1486456642 TSecr=4263679657
   13   0.275927   10.31.5.43 → 120.46.209.149 TCP 54 64266 → 443 [ACK] Seq=1 Ack=1 Win=4096 Len=0
   14   0.333695 120.46.209.149 → 10.31.5.43   TCP 60 [TCP ACKed unseen segment] 443 → 64266 [ACK] Seq=1 Ack=2 Win=274 Len=0
   15   0.377384   10.31.5.43 → 36.139.105.105 TCP 54 62269 → 10059 [ACK] Seq=1 Ack=1 Win=2048 Len=0
   16   0.410013 36.139.105.105 → 10.31.5.43   TCP 66 [TCP ACKed unseen segment] 10059 → 62269 [ACK] Seq=1 Ack=2 Win=21 Len=0 TSval=2900482170 TSecr=4037473717
   17   1.059177 157.255.174.106 → 10.31.5.43   SSL 95 Continuation Data
   18   1.059315   10.31.5.43 → 157.255.174.106 TCP 54 62235 → 443 [ACK] Seq=1 Ack=42 Win=4095 Len=0
   19   1.075186   10.31.5.43 → 58.251.100.100 TCP 78 64354 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=1656059305 TSecr=0 SACK_PERM
   20   1.081988   10.31.5.43 → 157.255.174.106 SSL 437 Continuation Data
   21   1.088149 58.251.100.100 → 10.31.5.43   TCP 66 80 → 64354 [SYN, ACK] Seq=0 Ack=1 Win=64800 Len=0 MSS=1200 SACK_PERM WS=128
   22   1.088304   10.31.5.43 → 58.251.100.100 TCP 54 64354 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
   23   1.089120   10.31.5.43 → 58.251.100.100 HTTP 1021 POST /mmtls/2303874e HTTP/1.1
   24   1.104067 58.251.100.100 → 10.31.5.43   TCP 60 80 → 64354 [ACK] Seq=1 Ack=968 Win=64128 Len=0
   25   1.110648 157.255.174.106 → 10.31.5.43   SSL 95 Continuation Data
   26   1.110809   10.31.5.43 → 157.255.174.106 TCP 54 62235 → 443 [ACK] Seq=384 Ack=83 Win=4095 Len=0
   27   1.207095 58.251.100.100 → 10.31.5.43   HTTP 1120 HTTP/1.1 200 OK
   28   1.207097 58.251.100.100 → 10.31.5.43   TCP 60 80 → 64354 [FIN, ACK] Seq=1067 Ack=968 Win=64128 Len=0
   29   1.207205   10.31.5.43 → 58.251.100.100 TCP 54 64354 → 80 [ACK] Seq=968 Ack=1067 Win=261056 Len=0
   30   1.207264   10.31.5.43 → 58.251.100.100 TCP 54 64354 → 80 [ACK] Seq=968 Ack=1068 Win=261056 Len=0
   31   1.208092   10.31.5.43 → 58.251.100.100 TCP 54 64354 → 80 [FIN, ACK] Seq=968 Ack=1068 Win=262144 Len=0
   32   1.222825 58.251.100.100 → 10.31.5.43   TCP 60 80 → 64354 [RST] Seq=1068 Win=0 Len=0
   33   1.226797 157.255.174.106 → 10.31.5.43   SSL 1254 Continuation Data
   34   1.226799 157.255.174.106 → 10.31.5.43   SSL 1254 Continuation Data
   35   1.226800 157.255.174.106 → 10.31.5.43   SSL 1254 Continuation Data
   36   1.226801 157.255.174.106 → 10.31.5.43   SSL 946 Continuation Data
   37   1.226902   10.31.5.43 → 157.255.174.106 TCP 54 62235 → 443 [ACK] Seq=384 Ack=4575 Win=4025 Len=0
   38   1.226998   10.31.5.43 → 157.255.174.106 TCP 54 [TCP Window Update] 62235 → 443 [ACK] Seq=384 Ack=4575 Win=4096 Len=0
   39   1.239445   10.31.5.43 → 157.148.41.237 TCP 78 64355 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=1343111878 TSecr=0 SACK_PERM
   40   1.246038   10.31.5.43 → 58.251.100.100 TCP 78 64356 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=1275804609 TSecr=0 SACK_PERM
   41   1.253833 157.148.41.237 → 10.31.5.43   TCP 60 80 → 64355 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1200
```

  - Wireshark



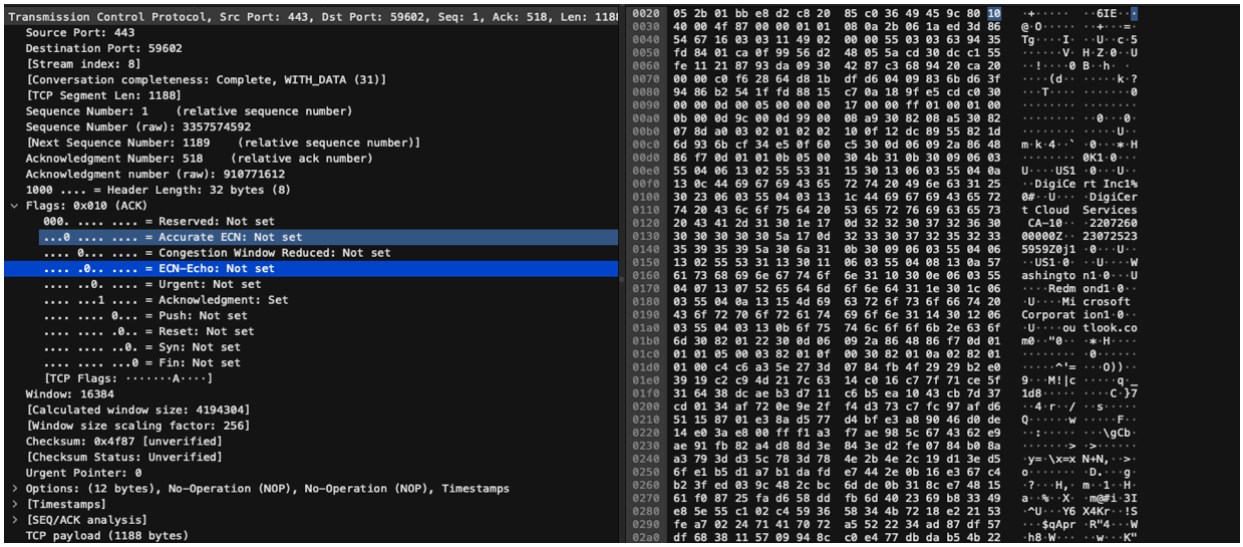
No.	Time	Source	Destination	Protocol	Length	Info
37	2.551987	10.31.5.43	40.99.33.178	TCP	78	59602 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=1032213554 TSecr=0 SACK_PERM
38	2.604533	40.99.33.178	10.31.5.43	TCP	74	443 → 59602 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1200 WS=256 SACK_PERM TSval=721820343 TS
39	2.604669	10.31.5.43	40.99.33.178	TCP	66	59602 → 443 [ACK] Seq=1 Ack=1 Win=131840 Len=0 TSval=1032213607 TSecr=721820343
40	2.604920	10.31.5.43	40.99.33.178	TLSv1.2	583	Client Hello
41	2.657750	40.99.33.178	10.31.5.43	TCP	1254	443 → 59602 [ACK] Seq=1 Ack=518 Win=4194304 Len=1188 TSval=721820397 TSecr=1032213607 [TCP segr
42	2.657751	40.99.33.178	10.31.5.43	TCP	1254	443 → 59602 [ACK] Seq=1189 Ack=518 Win=4194304 Len=1188 TSval=721820397 TSecr=1032213607 [TCP s
43	2.657752	40.99.33.178	10.31.5.43	TCP	1254	443 → 59602 [ACK] Seq=2377 Ack=518 Win=4194304 Len=1188 TSval=721820397 TSecr=1032213607 [TCP s
44	2.657752	40.99.33.178	10.31.5.43	TLSv1.2	932	Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done
45	2.657863	10.31.5.43	40.99.33.178	TCP	66	59602 → 443 [ACK] Seq=518 Ack=4431 Win=127424 Len=0 TSval=1032213660 TSecr=721820397
46	2.657963	10.31.5.43	40.99.33.178	TCP	66	[TCP Window Update] 59602 → 443 [ACK] Seq=518 Ack=4431 Win=131072 Len=0 TSval=1032213660 TSecr=
47	2.670092	10.31.5.43	40.99.33.178	TLSv1.2	224	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
48	2.722527	40.99.33.178	10.31.5.43	TLSv1.2	117	Change Cipher Spec, Encrypted Handshake Message
49	2.722701	10.31.5.43	40.99.33.178	TCP	66	59602 → 443 [ACK] Seq=676 Ack=4482 Win=131008 Len=0 TSval=1032213725 TSecr=721820461
50	2.724411	10.31.5.43	40.99.33.178	TCP	1254	59602 → 443 [ACK] Seq=676 Ack=4482 Win=131072 Len=1188 TSval=1032213726 TSecr=721820461 [TCP se
51	2.724470	10.31.5.43	40.99.33.178	TLSv1.2	1156	Application Data
52	2.724892	10.31.5.43	40.99.33.178	TLSv1.2	707	Application Data
53	2.776257	40.99.33.178	10.31.5.43	TCP	66	443 → 59602 [ACK] Seq=4482 Ack=2954 Win=4194816 Len=0 TSval=721820515 TSecr=1032213726
54	2.826687	40.99.33.178	10.31.5.43	TCP	66	443 → 59602 [ACK] Seq=4482 Ack=3595 Win=4194048 Len=0 TSval=721820566 TSecr=1032213726
55	2.885061	40.99.33.178	10.31.5.43	TCP	1254	443 → 59602 [ACK] Seq=4482 Ack=3595 Win=4194048 Len=1188 TSval=721820624 TSecr=1032213726 [TCP
56	2.885062	40.99.33.178	10.31.5.43	TLSv1.2	434	Application Data
57	2.885194	10.31.5.43	40.99.33.178	TCP	66	59602 → 443 [ACK] Seq=3595 Ack=6038 Win=129472 Len=0 TSval=1032213887 TSecr=721820624
58	2.885275	40.99.33.178	10.31.5.43	TLSv1.2	205	Application Data
59	2.885275	40.99.33.178	10.31.5.43	TLSv1.2	309	Application Data
60	2.885275	40.99.33.178	10.31.5.43	TLSv1.2	108	Application Data
61	2.885276	40.99.33.178	10.31.5.43	TLSv1.2	110	Application Data
62	2.885329	10.31.5.43	40.99.33.178	TCP	66	59602 → 443 [ACK] Seq=3595 Ack=6506 Win=129024 Len=0 TSval=1032213887 TSecr=721820625
63	2.886468	40.99.33.178	10.31.5.43	TLSv1.2	100	Application Data
64	2.886555	10.31.5.43	40.99.33.178	TCP	66	59602 → 443 [ACK] Seq=3595 Ack=6540 Win=131008 Len=0 TSval=1032213889 TSecr=721820625
69	2.911712	10.31.5.43	40.99.10.82	TCP	78	59604 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=1302722711 TSecr=0 SACK_PERM
70	2.967128	40.99.10.82	10.31.5.43	TCP	74	443 → 59604 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1200 WS=256 SACK_PERM TSval=756992330 TS
71	2.967225	10.31.5.43	40.99.10.82	TCP	66	59604 → 443 [ACK] Seq=1 Ack=1 Win=131840 Len=0 TSval=1302722766 TSecr=756992330
72	2.967707	10.31.5.43	40.99.10.82	TLSv1.2	583	Client Hello
73	3.024747	40.99.10.82	10.31.5.43	TCP	1254	443 → 59604 [ACK] Seq=1 Ack=518 Win=4194304 Len=1188 TSval=756992388 TSecr=1302722766 [TCP segr
74	3.024748	40.99.10.82	10.31.5.43	TCP	1254	443 → 59604 [ACK] Seq=1189 Ack=518 Win=4194304 Len=1188 TSval=756992388 TSecr=1302722766 [TCP s
75	3.024749	40.99.10.82	10.31.5.43	TCP	1254	443 → 59604 [ACK] Seq=2377 Ack=518 Win=4194304 Len=1188 TSval=756992388 TSecr=1302722766 [TCP s
76	3.024750	40.99.10.82	10.31.5.43	TLSv1.2	932	Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done
77	3.024927	10.31.5.43	40.99.10.82	TCP	66	59604 → 443 [ACK] Seq=518 Ack=4431 Win=127424 Len=0 TSval=1302722824 TSecr=756992388
78	3.025075	10.31.5.43	40.99.10.82	TCP	66	[TCP Window Update] 59604 → 443 [ACK] Seq=518 Ack=4431 Win=131072 Len=0 TSval=1302722824 TSecr=
79	3.037943	10.31.5.43	40.99.10.82	TLSv1.2	224	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
80	3.094366	40.99.10.82	10.31.5.43	TLSv1.2	117	Change Cipher Spec, Encrypted Handshake Message
81	3.094460	10.31.5.43	40.99.10.82	TCP	66	59604 → 443 [ACK] Seq=676 Ack=4482 Win=131008 Len=0 TSval=1302722894 TSecr=756992456
82	3.095836	10.31.5.43	40.99.10.82	TCP	1254	59604 → 443 [ACK] Seq=676 Ack=4482 Win=131072 Len=1188 TSval=1302722895 TSecr=756992456 [TCP se

  - Explanation No. 37-39 and No. 69-71 shows three-way handshake to establish a connection.

    1. Host A (10.31.5.43) sends a SYN = x to host B (40.99.33.178); SYN = 0 representing the client request a connection
    2. Host B returns a SYN ACK, SYN = y, ACK = x + 1

3. Host A sends an ACK = y + 1 to acknowledge the SYN ACK

After the three-way handshake, host A and host B can send data,



TCP packet (No. 41 as an example):

- source port: identify sending host
- destination port: identify receiving end
- Sequence number: the first sequence number of the first data byte in the packet; ISN randomly selected by the host
- Acknowledgment Number: contains the next sequence number that the acknowledge side expects to receive; thus should be the last receiving SYN + 1
- Header length
- Flags
    - Urgent Pointer Field Significant (URG): to ensure that the TCP connection is not interrupted and to urge intermediaries to process the data as soon as possible
    - ACK(Acknowledgement Field Signigicant): 1 means that the ACK will be included in the TCP packe
    - PSH(Push Function): means that the data is pushed to the application as soon as it is received by the receiver instead of queuing it in a buffer
    - RST(Reset the connection): resets the connection
    - SYN(Synchronize sequence numbers): used to initiate a connection request
    - FIN(No more data from sender): means that the sender has completed the sending task (disconnected).
- Window: window size
- Right Part: data section

- TLSv1.2: wireshark also captures TLS, which is mostly built on TCP. No. 40, 44, 47, 48 shows the handshaking phase, No. 51,52... (Application Data) shows communication by secret key.
    - TLS handshake
        - client -> server: Client Hello
        - server -> client: Server Hello, Certificate, Server Key Exchange, Server Hello Done
        - client -> server: Client Key Exchange, Chnage Cipher Spec, Encrypted Handshake Message
        - server -> client: Change Cipher Spec, Encrypted Handshake Message
    - TSL function:
        - Identity authentication: Certificate authentication is used to confirm the identity of the other party to prevent attacks
        - Data privacy: Use a symmetric key to encrypt the transmitted data
        - Data integrity: The message-digest algorithm is used to prevent data from being tampered or lost
- UDP
    - Tshark

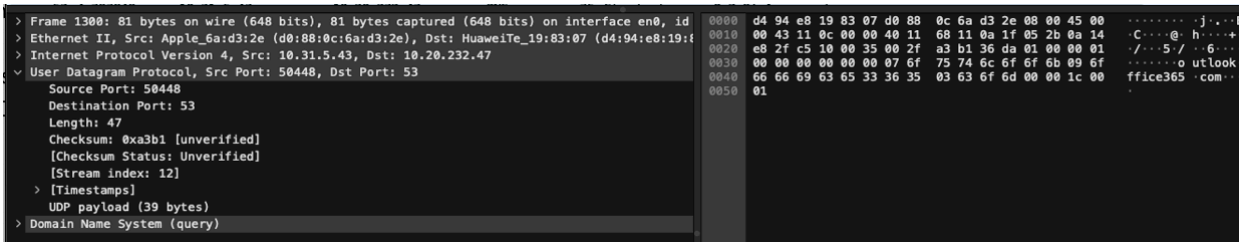
```
(base) thea@fengdeMacBook-Air ~ % tshark -i en0 -f 'udp'
Capturing on 'Wi-Fi: en0'
 ** (tshark:15400) 18:48:35.635753 [Main MESSAGE] -- Capture started.
 ** (tshark:15400) 18:48:35.636155 [Main MESSAGE] -- File: "/var/folders/n6/pjddxglj74vc5hxx_jss8d6w0000gn/T/wireshark_Wi-Fi39RBX1.pcapng"
    1   0.000000   10.31.5.43 → 10.20.232.47 DNS 72 Standard query 0x8aea AAAA drive.wps.cn
    2   0.000166   10.31.5.43 → 10.20.232.47 DNS 72 Standard query 0xb9f1 A drive.wps.cn
    3   0.016305 10.20.232.47 → 10.31.5.43   DNS 118 Standard query response 0xb9f1 A drive.wps.cn CNAME drive.wpsdns.com A 110.43.67.231
    4   0.016309 10.20.232.47 → 10.31.5.43   DNS 130 Standard query response 0x8aea AAAA drive.wps.cn CNAME drive.wpsdns.com AAAA 2401:1d40:ff:22::688:111
```

    - Wireshark

udp

No.	Time	Source	Destination	Protocol	Length	Info
52	4.797774	10.31.5.43	10.20.232.47	DNS	75	Standard query 0x5c09 AAAA wxapp.tc.qq.com
53	4.797849	10.31.5.43	10.20.232.47	DNS	75	Standard query 0x2c9f A wxapp.tc.qq.com
54	4.806471	10.20.232.47	10.31.5.43	DNS	312	Standard query response 0x2c9f A wxapp.tc.qq.com CNAME socwxsns.video.qq.com A 11
55	4.806471	10.20.232.47	10.31.5.43	DNS	356	Standard query response 0x5c09 AAAA wxapp.tc.qq.com CNAME socwxsns.video.qq.com A
311	14.721188	10.31.5.43	10.20.232.47	DNS	75	Standard query 0x5080 AAAA wxapp.tc.qq.com
312	14.721338	10.31.5.43	10.20.232.47	DNS	75	Standard query 0x7e1d A wxapp.tc.qq.com
313	14.730695	10.20.232.47	10.31.5.43	DNS	356	Standard query response 0x5080 AAAA wxapp.tc.qq.com CNAME socwxsns.video.qq.com A
314	14.730696	10.20.232.47	10.31.5.43	DNS	312	Standard query response 0x7e1d A wxapp.tc.qq.com CNAME socwxsns.video.qq.com A 11
401	16.872227	10.31.5.43	10.20.232.47	DNS	78	Standard query 0x7152 A vweixinf.tc.qq.com
402	16.872411	10.31.5.43	10.20.232.47	DNS	78	Standard query 0x9ff6 AAAA vweixinf.tc.qq.com
403	16.892133	10.20.232.47	10.31.5.43	DNS	343	Standard query response 0x7152 A vweixinf.tc.qq.com CNAME vweixinf.tcdn.qq.com CN
404	16.892134	10.20.232.47	10.31.5.43	DNS	387	Standard query response 0x9ff6 AAAA vweixinf.tc.qq.com CNAME vweixinf.tcdn.qq.com
472	17.025770	10.31.5.43	10.20.232.47	DNS	78	Standard query 0x0ed3 A vweixinf.tc.qq.com
473	17.025886	10.31.5.43	10.20.232.47	DNS	78	Standard query 0x788f AAAA vweixinf.tc.qq.com
474	17.033366	10.20.232.47	10.31.5.43	DNS	343	Standard query response 0x0ed3 A vweixinf.tc.qq.com CNAME vweixinf.tcdn.qq.com CN
475	17.033367	10.20.232.47	10.31.5.43	DNS	387	Standard query response 0x788f AAAA vweixinf.tc.qq.com CNAME vweixinf.tcdn.qq.com
1187	40.945274	10.31.5.43	10.20.232.47	DNS	77	Standard query 0x184d A diskapi.baidu.com
1188	40.958698	10.20.232.47	10.31.5.43	DNS	124	Standard query response 0x184d A diskapi.baidu.com CNAME diskapi.n.shifen.com A 2
1253	60.755846	10.31.5.43	224.0.0.251	MDNS	150	Standard query 0x0000 PTR _afpovertcp._tcp.local, "QU" question PTR _smb._tcp.loc
1254	60.755855	10.31.5.43	224.0.0.251	MDNS	150	Standard query 0x0000 PTR _afpovertcp._tcp.local, "QU" question PTR _smb._tcp.loc
1255	60.758756	fe80::858:ac:e401:…	ff02::fb	MDNS	170	Standard query 0x0000 PTR _afpovertcp._tcp.local, "QU" question PTR _smb._tcp.loc
1256	60.758764	fe80::858:ac:e401:…	ff02::fb	MDNS	170	Standard query 0x0000 PTR _afpovertcp._tcp.local, "QU" question PTR _smb._tcp.loc
1257	60.758820	fe80::858:ac:e401:…	ff02::fb	MDNS	170	Standard query 0x0000 PTR _afpovertcp._tcp.local, "QU" question PTR _smb._tcp.loc
1258	60.758822	fe80::858:ac:e401:…	ff02::fb	MDNS	170	Standard query 0x0000 PTR _afpovertcp._tcp.local, "QU" question PTR _smb._tcp.loc
1259	61.756158	10.31.5.43	224.0.0.251	MDNS	150	Standard query 0x0000 PTR _afpovertcp._tcp.local, "QM" question PTR _smb._tcp.loc
1260	61.756242	fe80::858:ac:e401:…	ff02::fb	MDNS	170	Standard query 0x0000 PTR _afpovertcp._tcp.local, "QM" question PTR _smb._tcp.loc
1261	62.395538	10.31.5.43	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
1264	63.396384	10.31.5.43	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1

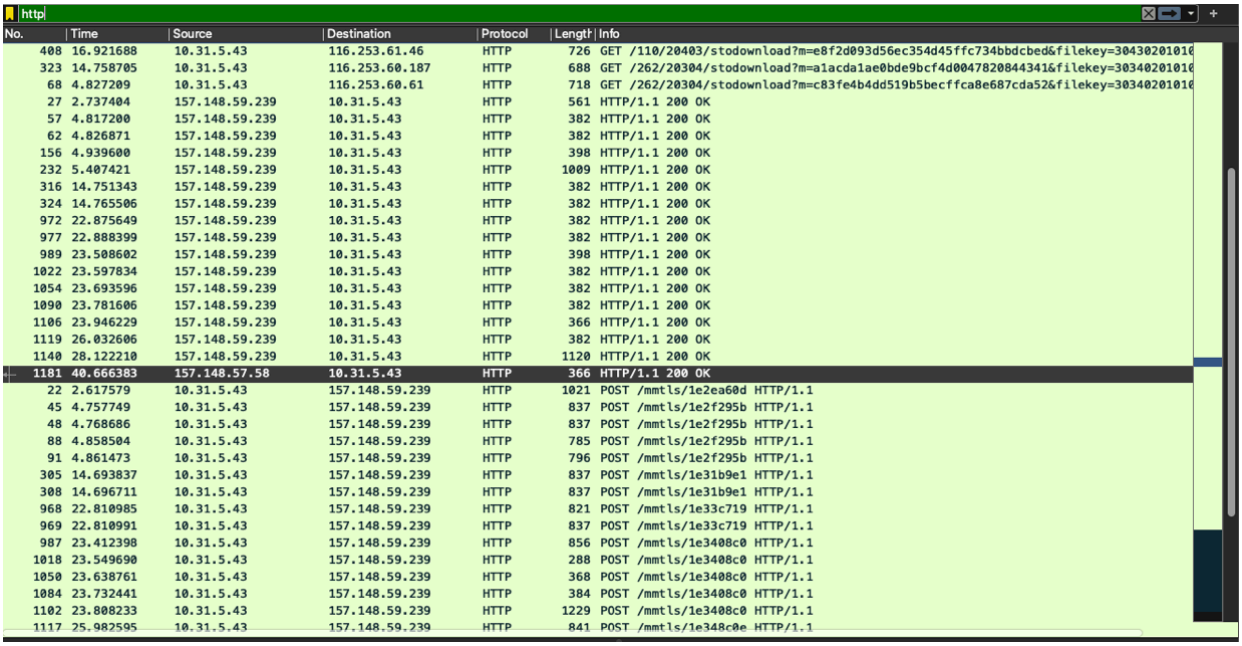
    - DNS, MDNS, and SSDP is based on UDP. The communication of UDP is much simpler than TCP. It does not need to establish connection and send acknowledgement. Without flow control and retransmission, lightweight protocol UDP is widely used in qq, wechat, video, network TV and other scenes. For example, in the capture `vweixinf.tc.qq.com` and `vwapp.tc.qq.com`. However, it is easy to lose packet.



As we can see, UDP packet contains source port, distination port, length, (checksum). It does not support flow control and retransmission.

Other Wireshark and Tshark Cpature

- Http
  - Before Http start, Web browser first establishes a connection with the web server based on TCP. Http is stateless. Client request message from sever and server reponse to client. Two common type: GET and POST.



For example (No. 408), client (10.31.5.43) request downloading picture from server (116.253.61.46)

In http header, it specifies http version(HTTP/1.1), request URI, User-Agent (wechat), request content type (image) and so on

No. 27 is a response. `HTTP/1.1 200 OK` consists of version and status code.

- Tshark

```
(base) thea@fengdeMacBook-Air ~ % tshark -i en0 -Y http.request -f "tcp port 80"
Capturing on 'Wi-Fi: en0'
 ** (tshark:15830) 19:25:32.432808 [Main MESSAGE] -- Capture started.
 ** (tshark:15830) 19:25:32.433111 [Main MESSAGE] -- File: "/var/folders/n6/pjddxglj74vc5hxx_jss8d6w0000gn/T/wireshark_Wi-FiRNIWW1.pcapng"
    4   0.015194   10.31.5.43 → 58.251.100.100 HTTP 1021 POST /mmtls/256bc9e3 HTTP/1.1
   18  11.153263   10.31.5.43 → 58.251.100.100 HTTP 1021 POST /mmtls/256e9c10 HTTP/1.1
   30  12.811054   10.31.5.43 → 58.251.100.100 HTTP 1021 POST /mmtls/256eddb7 HTTP/1.1
   42  15.583120   10.31.5.43 → 58.251.100.100 HTTP 1021 POST /mmtls/256fa2ac HTTP/1.1
   54  16.912145   10.31.5.43 → 58.251.100.100 HTTP 1021 POST /mmtls/257025fa HTTP/1.1
   70  27.805266   10.31.5.43 → 58.251.100.100 HTTP 1021 POST /mmtls/2572b680 HTTP/1.1
   82  29.745180   10.31.5.43 → 58.251.100.100 HTTP 888 POST /mmtls/257339ce HTTP/1.1
   95  53.131712   10.31.5.43 → 58.251.100.100 HTTP 1021 POST /mmtls/25796176 HTTP/1.1
```

- DNS
  - Tshark: example of WPS drive and Neteast music

```
(base) thea@fengdeMacBook-Air ~ % tshark -i en0  -o "ip.use_geoip:TRUE" -Y "udp.dstport == 53" -T fields -E separator='|' -e ip.src -e ip.geoip.src_country -e ip.geoip.src_asnum -e dns.flags -e dns.id
-e dns.qry.name -e dns.qry.type -e  dns.count.answers  -e dns.count.answers -e dns.flags.rcode  -e  ip.len
Capturing on 'Wi-Fi: en0'
 ** (tshark:15654) 19:02:36.066774 [Main MESSAGE] -- Capture started.
 ** (tshark:15654) 19:02:36.067146 [Main MESSAGE] -- File: "/var/folders/n6/pjddxglj74vc5hxx_jss8d6w0000gn/T/wireshark_Wi-Fi5OXZW1.pcapng"
10.31.5.43|||0x0100|0x99b3|drive.wps.cn|28||0||58
10.31.5.43|||0x0100|0x4c64|drive.wps.cn|1||0||58
10.31.5.43|||0x0100|0x5d57|music.163.com|28||0||59
10.31.5.43|||0x0100|0xb68e|music.163.com|1||0||59
```

  - Wireshark: example of Neteast music, WPS drive and Itunes

dns

No.	Time	Source	Destination	Protocol	Length	Info
26	5.407901	10.31.5.43	10.20.232.47	DNS	73	Standard query 0x8b05 A music.163.com
27	5.408028	10.31.5.43	10.20.232.47	DNS	73	Standard query 0xab5f AAAA music.163.com
30	5.413886	10.20.232.47	10.31.5.43	DNS	184	Standard query response 0xab5f AAAA music.163.com CNAME music.ntes53.netease.com CNAME telv6.music…
31	5.413886	10.20.232.47	10.31.5.43	DNS	160	Standard query response 0x8b05 A music.163.com CNAME music.ntes53.netease.com CNAME telv6.music.nt…
149	35.153245	10.31.5.43	10.20.232.47	DNS	82	Standard query 0xe68c A az764295.vo.msecnd.net
150	35.153313	10.31.5.43	10.20.232.47	DNS	82	Standard query 0x2599 AAAA az764295.vo.msecnd.net
155	35.222336	10.20.232.47	10.31.5.43	DNS	127	Standard query response 0xe68c A az764295.vo.msecnd.net CNAME cs22.wpc.v0cdn.net A 117.18.232.200
156	35.222338	10.20.232.47	10.31.5.43	DNS	167	Standard query response 0x2599 AAAA az764295.vo.msecnd.net CNAME cs22.wpc.v0cdn.net SOA ns1.v0cdn.…
196	40.163752	10.31.5.43	10.20.232.47	DNS	82	Standard query 0x832e AAAA az764295.vo.msecnd.net
197	40.163931	10.31.5.43	10.20.232.47	DNS	82	Standard query 0x49a0 A az764295.vo.msecnd.net
198	40.183182	10.20.232.47	10.31.5.43	DNS	127	Standard query response 0x49a0 A az764295.vo.msecnd.net CNAME cs22.wpc.v0cdn.net A 117.18.232.200
199	40.183185	10.20.232.47	10.31.5.43	DNS	167	Standard query response 0x832e AAAA az764295.vo.msecnd.net CNAME cs22.wpc.v0cdn.net SOA ns1.v0cdn.…
645	96.533145	10.31.5.43	10.20.232.47	DNS	75	Standard query 0x4519 A ocsp2.apple.com
646	96.533251	10.31.5.43	10.20.232.47	DNS	75	Standard query 0x3619 AAAA ocsp2.apple.com
647	96.550852	10.20.232.47	10.31.5.43	DNS	234	Standard query response 0x3619 AAAA ocsp2.apple.com CNAME ocsp2-lb.apple.com.akadns.net CNAME ocsp…
648	96.550853	10.20.232.47	10.31.5.43	DNS	205	Standard query response 0x4519 A ocsp2.apple.com CNAME ocsp2-lb.apple.com.akadns.net CNAME ocsp2-c…
673	96.804272	10.31.5.43	10.20.232.47	DNS	80	Standard query 0x85fd A bag.itunes.apple.com
674	96.804511	10.31.5.43	10.20.232.47	DNS	80	Standard query 0x3dfe AAAA bag.itunes.apple.com
675	96.812703	10.20.232.47	10.31.5.43	DNS	216	Standard query response 0x85fd A bag.itunes.apple.com CNAME init-cdn.itunes-apple.com.akadns.net C…
676	96.812704	10.20.232.47	10.31.5.43	DNS	245	Standard query response 0x3dfe AAAA bag.itunes.apple.com CNAME init-cdn.itunes-apple.com.akadns.ne…
710	97.639552	10.31.5.43	10.20.232.47	DNS	72	Standard query 0x7dd0 AAAA drive.wps.cn
711	97.639704	10.31.5.43	10.20.232.47	DNS	72	Standard query 0xbc79 A drive.wps.cn
712	97.681459	10.20.232.47	10.31.5.43	DNS	182	Standard query response 0xbc79 A drive.wps.cn CNAME drive.wpsdns.com A 121.36.106.50 A 121.36.2.16…
713	97.681461	10.20.232.47	10.31.5.43	DNS	130	Standard query response 0x7dd0 AAAA drive.wps.cn CNAME drive.wpsdns.com AAAA 2401:1d40:ff:22::688:…

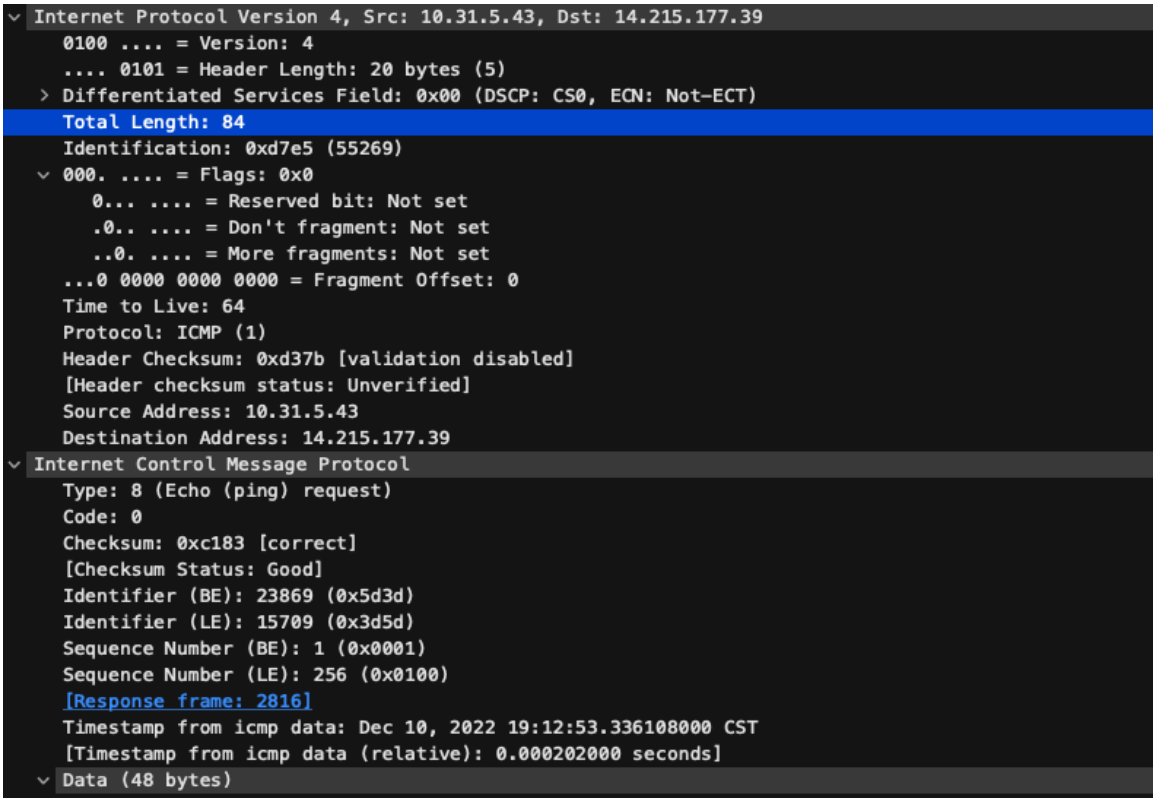
DNS is based on UDP as we analysed before. DNS is used to convert a domain name into an IP address

- ICMP
- Wireshark: Use `ping www.baidu.com` to incur ICMP

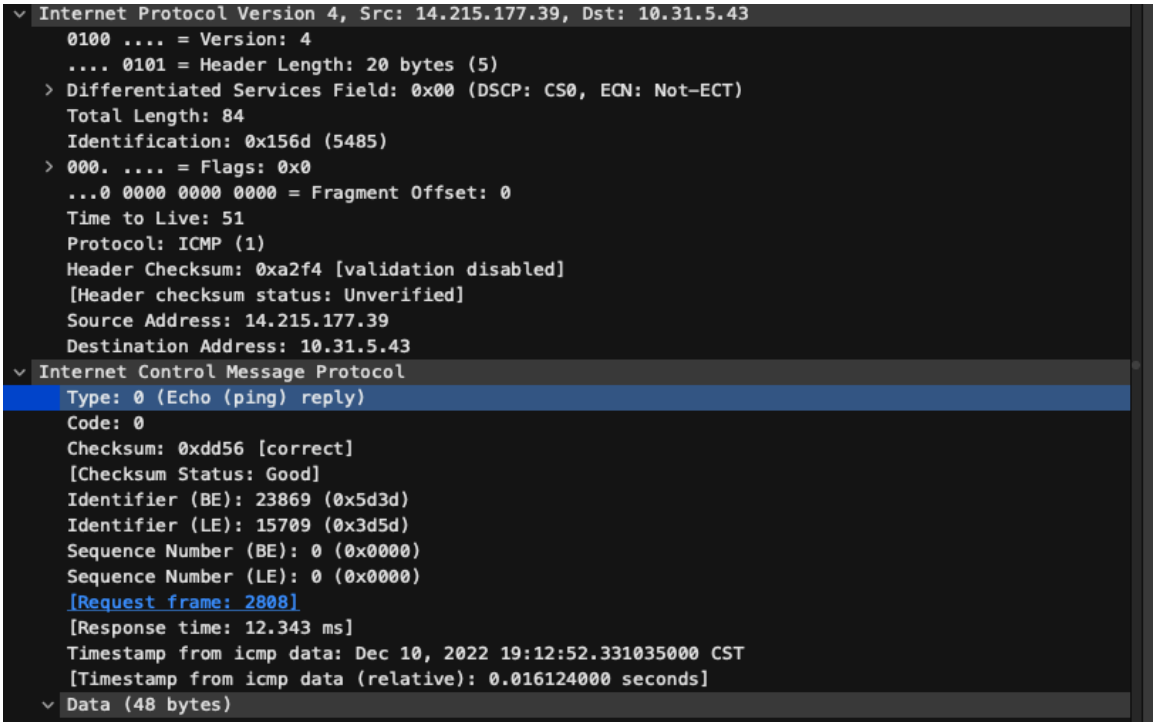
icmp

No.	Time	Source	Destination	Protocol	Length	Info
2808	38.381123	10.31.5.43	14.215.177.39	ICMP	98	Echo (ping) request id=0x5d3d, seq=0/0, ttl=64 (reply in 2810)
2810	38.393466	14.215.177.39	10.31.5.43	ICMP	98	Echo (ping) reply id=0x5d3d, seq=0/0, ttl=51 (request in 2808)
2815	39.382617	10.31.5.43	14.215.177.39	ICMP	98	Echo (ping) request id=0x5d3d, seq=1/256, ttl=64 (reply in 2816)
2816	39.408409	14.215.177.39	10.31.5.43	ICMP	98	Echo (ping) reply id=0x5d3d, seq=1/256, ttl=51 (request in 2815)
2844	40.385752	10.31.5.43	14.215.177.39	ICMP	98	Echo (ping) request id=0x5d3d, seq=2/512, ttl=64 (reply in 2851)
2851	40.401740	14.215.177.39	10.31.5.43	ICMP	98	Echo (ping) reply id=0x5d3d, seq=2/512, ttl=51 (request in 2844)
2864	41.391157	10.31.5.43	14.215.177.39	ICMP	98	Echo (ping) request id=0x5d3d, seq=3/768, ttl=64 (reply in 2865)
2865	41.412802	14.215.177.39	10.31.5.43	ICMP	98	Echo (ping) reply id=0x5d3d, seq=3/768, ttl=51 (request in 2864)
2876	42.394525	10.31.5.43	14.215.177.39	ICMP	98	Echo (ping) request id=0x5d3d, seq=4/1024, ttl=64 (reply in 2877)
2877	42.408924	14.215.177.39	10.31.5.43	ICMP	98	Echo (ping) reply id=0x5d3d, seq=4/1024, ttl=51 (request in 2876)
2880	43.398587	10.31.5.43	14.215.177.39	ICMP	98	Echo (ping) request id=0x5d3d, seq=5/1280, ttl=64 (reply in 2881)
2881	43.424745	14.215.177.39	10.31.5.43	ICMP	98	Echo (ping) reply id=0x5d3d, seq=5/1280, ttl=51 (request in 2880)
2884	44.403987	10.31.5.43	14.215.177.39	ICMP	98	Echo (ping) request id=0x5d3d, seq=6/1536, ttl=64 (reply in 2885)
2885	44.422673	14.215.177.39	10.31.5.43	ICMP	98	Echo (ping) reply id=0x5d3d, seq=6/1536, ttl=51 (request in 2884)
2907	45.409386	10.31.5.43	14.215.177.39	ICMP	98	Echo (ping) request id=0x5d3d, seq=7/1792, ttl=64 (reply in 2908)
2908	45.421963	14.215.177.39	10.31.5.43	ICMP	98	Echo (ping) reply id=0x5d3d, seq=7/1792, ttl=51 (request in 2907)
2909	46.411137	10.31.5.43	14.215.177.39	ICMP	98	Echo (ping) request id=0x5d3d, seq=8/2048, ttl=64 (reply in 2910)
2910	46.435757	14.215.177.39	10.31.5.43	ICMP	98	Echo (ping) reply id=0x5d3d, seq=8/2048, ttl=51 (request in 2909)
2913	47.416433	10.31.5.43	14.215.177.39	ICMP	98	Echo (ping) request id=0x5d3d, seq=9/2304, ttl=64 (reply in 2914)
2914	47.440331	14.215.177.39	10.31.5.43	ICMP	98	Echo (ping) reply id=0x5d3d, seq=9/2304, ttl=51 (request in 2913)
2915	48.416906	10.31.5.43	14.215.177.39	ICMP	98	Echo (ping) request id=0x5d3d, seq=10/2560, ttl=64 (reply in 2920)
2920	48.439792	14.215.177.39	10.31.5.43	ICMP	98	Echo (ping) reply id=0x5d3d, seq=10/2560, ttl=49 (request in 2915)
2923	49.420883	10.31.5.43	14.215.177.39	ICMP	98	Echo (ping) request id=0x5d3d, seq=11/2816, ttl=64 (reply in 2924)
2924	49.445911	14.215.177.39	10.31.5.43	ICMP	98	Echo (ping) reply id=0x5d3d, seq=11/2816, ttl=51 (request in 2923)
3034	50.426222	10.31.5.43	14.215.177.39	ICMP	98	Echo (ping) request id=0x5d3d, seq=12/3072, ttl=64 (reply in 3035)

1. Source (10.31.5.43) sends an echo (request) to the destination server (14.215.177.39). Packet includes type 8, code 0 and timestamp.



2. Destination sends an echo (reply) to source; type indicates response to 0.



- Tshark

```
/Users/thea/.zshrc:source:81: no such file or directory: Users/thea/.oh-my-zsh/oh-my-zsh.sh
(base) thea@fengdeMacBook-Air ~ % tshark -f "icmp"
Capturing on 'Wi-Fi: en0'
 ** (tshark:15789) 19:23:59.761594 [Main MESSAGE] -- Capture started.
 ** (tshark:15789) 19:23:59.761924 [Main MESSAGE] -- File: "/var/folders/n6/pjddxglj74vc5hxx_jss8d6w0000gn/T/wireshark_Wi-FiG2REX1.pcapng"
    1   0.000000   10.31.5.43 → 14.215.177.38 ICMP 98 Echo (ping) request  id=0xbc3d, seq=0/0, ttl=64
    2   0.029240 14.215.177.38 → 10.31.5.43   ICMP 98 Echo (ping) reply    id=0xbc3d, seq=0/0, ttl=51 (request in 1)
    3   0.997904   10.31.5.43 → 14.215.177.38 ICMP 98 Echo (ping) request  id=0xbc3d, seq=1/256, ttl=64
    4   1.015039 14.215.177.38 → 10.31.5.43   ICMP 98 Echo (ping) reply    id=0xbc3d, seq=1/256, ttl=51 (request in 3)
    5   1.999585   10.31.5.43 → 14.215.177.38 ICMP 98 Echo (ping) request  id=0xbc3d, seq=2/512, ttl=64
    6   2.013293 14.215.177.38 → 10.31.5.43   ICMP 98 Echo (ping) reply    id=0xbc3d, seq=2/512, ttl=51 (request in 5)
    7   3.004128   10.31.5.43 → 14.215.177.38 ICMP 98 Echo (ping) request  id=0xbc3d, seq=3/768, ttl=64
    8   3.019695 14.215.177.38 → 10.31.5.43   ICMP 98 Echo (ping) reply    id=0xbc3d, seq=3/768, ttl=51 (request in 7)
    9   4.009450   10.31.5.43 → 14.215.177.38 ICMP 98 Echo (ping) request  id=0xbc3d, seq=4/1024, ttl=64
   10   4.037477 14.215.177.38 → 10.31.5.43   ICMP 98 Echo (ping) reply    id=0xbc3d, seq=4/1024, ttl=51 (request in 9)
   11   5.014809   10.31.5.43 → 14.215.177.38 ICMP 98 Echo (ping) request  id=0xbc3d, seq=5/1280, ttl=64
   12   5.042417 14.215.177.38 → 10.31.5.43   ICMP 98 Echo (ping) reply    id=0xbc3d, seq=5/1280, ttl=51 (request in 11)
   13   6.020007   10.31.5.43 → 14.215.177.38 ICMP 98 Echo (ping) request  id=0xbc3d, seq=6/1536, ttl=64
   14   6.039987 14.215.177.38 → 10.31.5.43   ICMP 98 Echo (ping) reply    id=0xbc3d, seq=6/1536, ttl=51 (request in 13)
   15   7.025353   10.31.5.43 → 14.215.177.38 ICMP 98 Echo (ping) request  id=0xbc3d, seq=7/1792, ttl=64
   16   7.056889 14.215.177.38 → 10.31.5.43   ICMP 98 Echo (ping) reply    id=0xbc3d, seq=7/1792, ttl=51 (request in 15)
   17   8.030716   10.31.5.43 → 14.215.177.38 ICMP 98 Echo (ping) request  id=0xbc3d, seq=8/2048, ttl=64
```

- ARP
  - Wireshark

No.	Time	Source	Destination	Protocol	Length	Info
2751	30.926336	HuaweiTe_19:83:07	Apple_6a:d3:2e	ARP	60	10.31.7.254 is at d4:94:e8:19:83:07
3789	120.925608	HuaweiTe_19:83:07	Apple_6a:d3:2e	ARP	60	10.31.7.254 is at d4:94:e8:19:83:07
4673	210.926013	HuaweiTe_19:83:07	Apple_6a:d3:2e	ARP	60	10.31.7.254 is at d4:94:e8:19:83:07
5792	300.935603	HuaweiTe_19:83:07	Apple_6a:d3:2e	ARP	60	10.31.7.254 is at d4:94:e8:19:83:07
6320	389.125307	Apple_63:f0:4b	Broadcast	RARP	60	Who is ff:ff:ff:ff:ff:ff? Tell 54:99:63:63:f0:4b
6323	390.936942	HuaweiTe_19:83:07	Apple_6a:d3:2e	ARP	60	10.31.7.254 is at d4:94:e8:19:83:07
6679	480.931574	HuaweiTe_19:83:07	Apple_6a:d3:2e	ARP	60	10.31.7.254 is at d4:94:e8:19:83:07
7192	540.280550	Apple_6a:d3:2e	Broadcast	ARP	42	Who has 10.31.6.142? Tell 10.31.5.43
7193	540.288623	HuaweiTe_19:83:07	Apple_6a:d3:2e	ARP	60	10.31.6.142 is at d4:94:e8:19:83:07
7412	570.933892	HuaweiTe_19:83:07	Apple_6a:d3:2e	ARP	60	10.31.7.254 is at d4:94:e8:19:83:07
8237	660.944287	HuaweiTe_19:83:07	Apple_6a:d3:2e	ARP	60	10.31.7.254 is at d4:94:e8:19:83:07
8621	738.608729	Apple_6a:d3:2e	Broadcast	ARP	42	Who has 10.31.1.37? Tell 10.31.5.43
8622	738.617390	HuaweiTe_19:83:07	Apple_6a:d3:2e	ARP	60	10.31.1.37 is at d4:94:e8:19:83:07
8732	750.942947	HuaweiTe_19:83:07	Apple_6a:d3:2e	ARP	60	10.31.7.254 is at d4:94:e8:19:83:07
125…	840.946664	HuaweiTe_19:83:07	Apple_6a:d3:2e	ARP	60	10.31.7.254 is at d4:94:e8:19:83:07
155…	930.908388	HuaweiTe_19:83:07	Apple_6a:d3:2e	ARP	60	10.31.7.254 is at d4:94:e8:19:83:07
197…	1020.920461	HuaweiTe_19:83:07	Apple_6a:d3:2e	ARP	60	10.31.7.254 is at d4:94:e8:19:83:07
203…	1070.207196	Apple_6a:d3:2e	HuaweiTe_19:83:07	ARP	42	Who has 10.31.6.142? Tell 10.31.5.43
203…	1070.222725	HuaweiTe_19:83:07	Apple_6a:d3:2e	ARP	60	10.31.6.142 is at d4:94:e8:19:83:07

  - Tshark

```
(base) thea@fengdeMacBook-Air ~ % tshark -f "arp"
Capturing on 'Wi-Fi: en0'
 ** (tshark:15922) 19:31:54.857933 [Main MESSAGE] -- Capture started.
 ** (tshark:15922) 19:31:54.858201 [Main MESSAGE] -- File: "/var/folders/n6/pjddxglj74vc5hxx_jss8d6w0000gn/T/wireshark_Wi-FiKSN5W1.pcapng"
    1   0.000000 HuaweiTe_19:83:07 → Apple_6a:d3:2e ARP 60 10.31.7.254 is at d4:94:e8:19:83:07
    2  90.002711 HuaweiTe_19:83:07 → Apple_6a:d3:2e ARP 60 10.31.7.254 is at d4:94:e8:19:83:07
    3 180.006537 HuaweiTe_19:83:07 → Apple_6a:d3:2e ARP 60 10.31.7.254 is at d4:94:e8:19:83:07
    4 270.003720 HuaweiTe_19:83:07 → Apple_6a:d3:2e ARP 60 10.31.7.254 is at d4:94:e8:19:83:07
```

  - The working principle is to send the MAC address of the destination through broadcast. After the host in the same broadcast domain as the sender receiving the request:
    - If the query IP is local, it unicasts the MAC address of the itself.
    - Else not respond.
  - For example, Apple_6a (No. 7192) ask (broadcast) `who has 10.31.6.142? Tell 10.31.5.43`, HuaweiTe_19 replies the MAC address.

Encapsulation and Decapsulation

Encapsulation adds header to a packet as it travels to its destination. Decapsulation reverses the process by removing the header, so a destination device can read the original data. For example, HTTP packet includes http, tcp, ip,ethernet header while TCP packet includes tcp, ip ethernet header.