Lab7 Networking

Haorui Chen chenhr@bu.edu

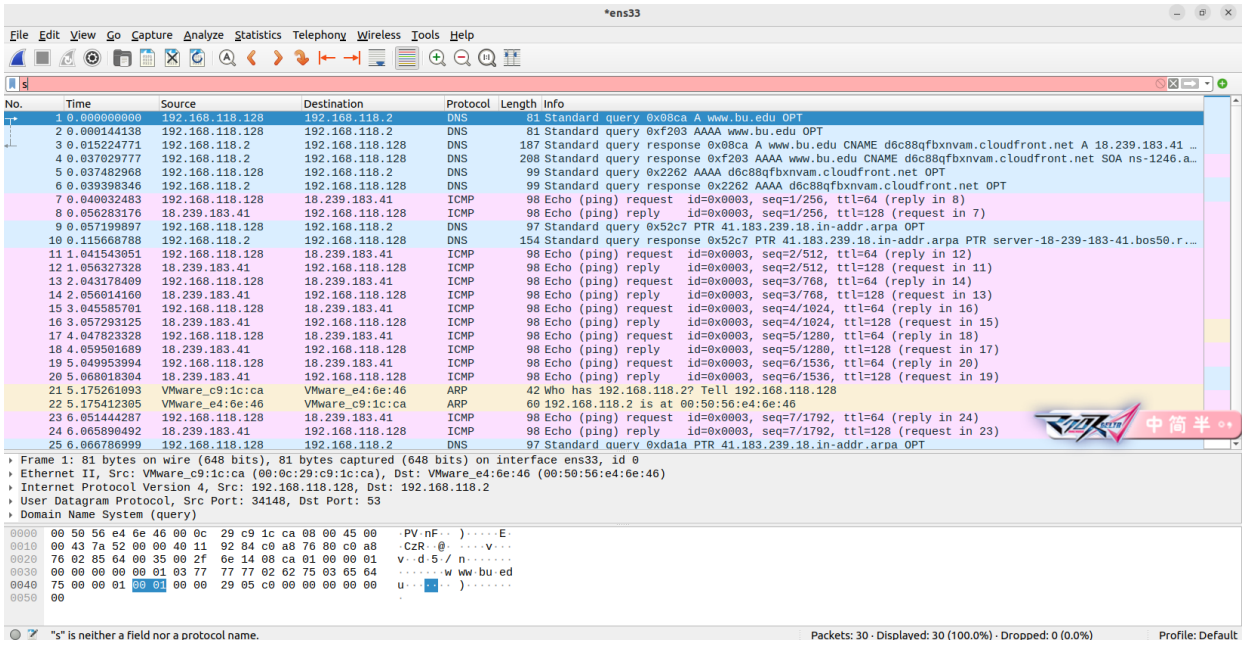
Task1

input command ip addr

```
blenguin@blenguin-virtual-machine:~/Desktop$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gro
up default qlen 1000
    link/ether 00:0c:29:c9:1c:ca brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.118.128/24 brd 192.168.118.255 scope global dynamic noprefixrou
te ens33
       valid_lft 1156sec preferred_lft 1156sec
    inet6 fe80::42c6:f0be:f51e:12f0/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOW
N group default
    link/ether 02:42:36:b7:5a:83 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
       valid_lft forever preferred_lft forever
```

ip addr

trace ping www.bu.edu



trace ping

Q1:What kind of protocol is used when performing a ping command?

A1: ICMP（Internet Control Message Protocol）.ICMP (Internet Control Message Protocol) is a network layer protocol used for sending error messages and operational information, primarily for network diagnostics. It helps determine whether data is reaching its intended destination by sending "echo request" and receiving "echo reply" messages, commonly seen in commands like `ping`. Unlike TCP or UDP, ICMP is not used for exchanging user data but for troubleshooting and reporting network issues.

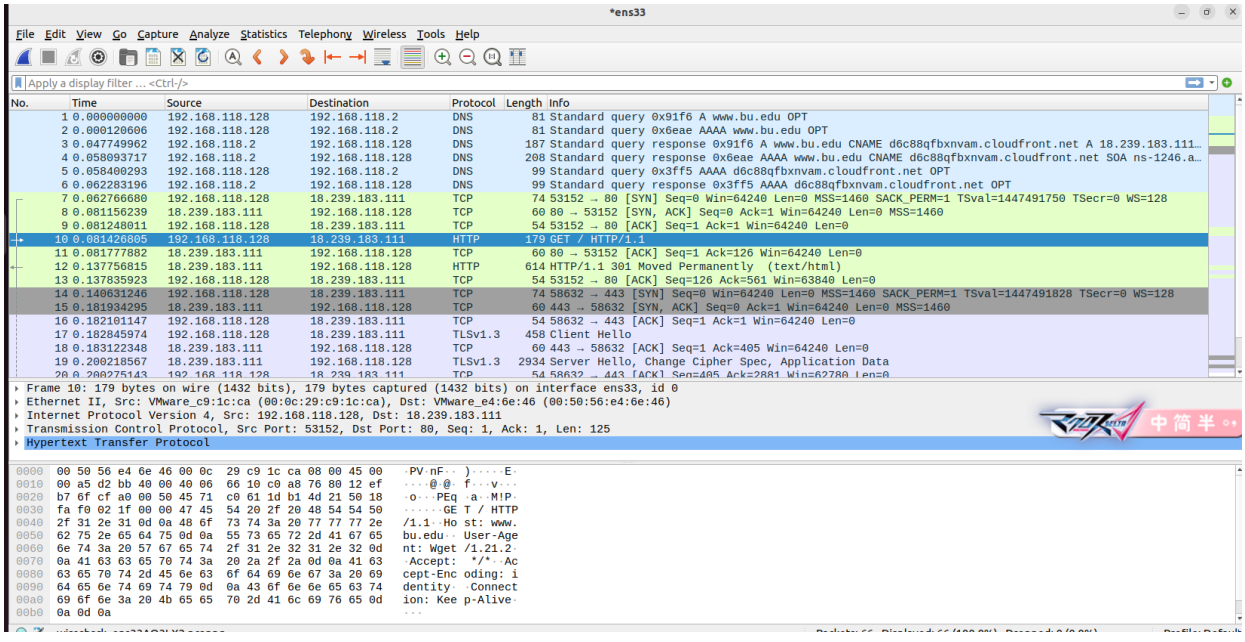
Q2:What information is transferred in this protocol?

A2:In the ICMP (Internet Control Message Protocol), the following types of information are transferred:

1. **Error Messages**: ICMP communicates errors that occur when packets cannot be delivered. For example, "Destination Unreachable" messages inform the sender that a destination is unreachable due to network issues or configuration problems.
2. **Diagnostic Messages**: ICMP is used for diagnostic purposes, such as with `ping` or `traceroute`. These tools send Echo Request and Echo Reply messages to check if a host is reachable and measure the round-trip time.
3. **Control and Status Messages**: ICMP also provides information about the status of the network. This includes messages like Time Exceeded, which indicates that a packet's time-to-live (TTL) expired in transit, or Redirect messages, which inform a host of a better route for sending packets.

Task2

wget www.bu.edu



HTTP GET

Q1: Specify the source and destination IP address

A1: Source IP Address: 192.168.118.128
Destination IP Address: 18.239.183.111

Q2: Source and Destination MAC Address

A2: Source MAC Address: 00:0c:29:e4:6e:46 (VMware virtual adapter)
Destination MAC Address: 00:50:56:e4:6e:46

Q3: Internet Protocol Version

A3: IPv4

Q4: Source and Destination Port

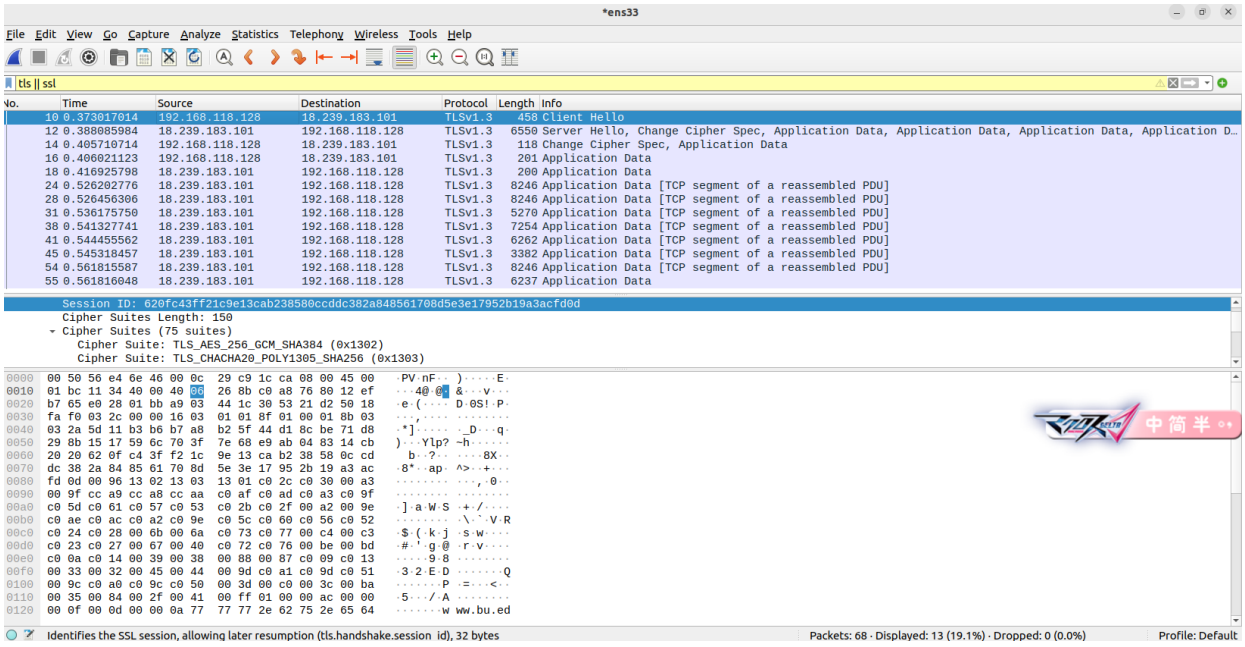
A4: Source Port: 53152
Destination Port: 80

Q5: Version of wget
A5: Wget/1.21.2.

Q6: TCP Flags
A6: ACK

Task3

wget https://www.bu.edu



wget https://www.bu.edu

Q1: List the packets sent between two machines and the purpose of each packet.

A1:

- **Client Hello (Packet 10)**: The client initiates the TLS handshake by proposing encryption settings.
- **Server Hello, Change Cipher Spec, Application Data (Packet 12)**: The server selects encryption settings, notifies that future communication will be encrypted, and starts sending encrypted data.
- **Change Cipher Spec, Application Data (Packet 14)**: The client acknowledges the encryption setup and starts sending encrypted data.

- **Application Data (Packets 16-55)**: Encrypted data is exchanged between the client and server.

Task4

Q1: Which IP addresses are in the trace?

A1:

1. **192.168.1.17** (Client)
2. **192.168.1.1** (Local Gateway)
3. **74.125.29.189** (Google Server)
4. **216.58.219.238** (Google Server)
5. **128.197.26.34, 128.197.26.35, 128.197.26.4, 128.197.26.3** (Boston University Servers)

Q2: Which IP is the client?

A2: **192.168.1.17** is the client IP address.

Q3: What domains are being accessed?

A3:

1. **goo.gl** (Google's URL shortening service)
2. **www.bu.edu** (Boston University official website)

Q4:Using Wireshark, get a copy of the image file and include it in the write-up

A4:

BUPC-Logo-black