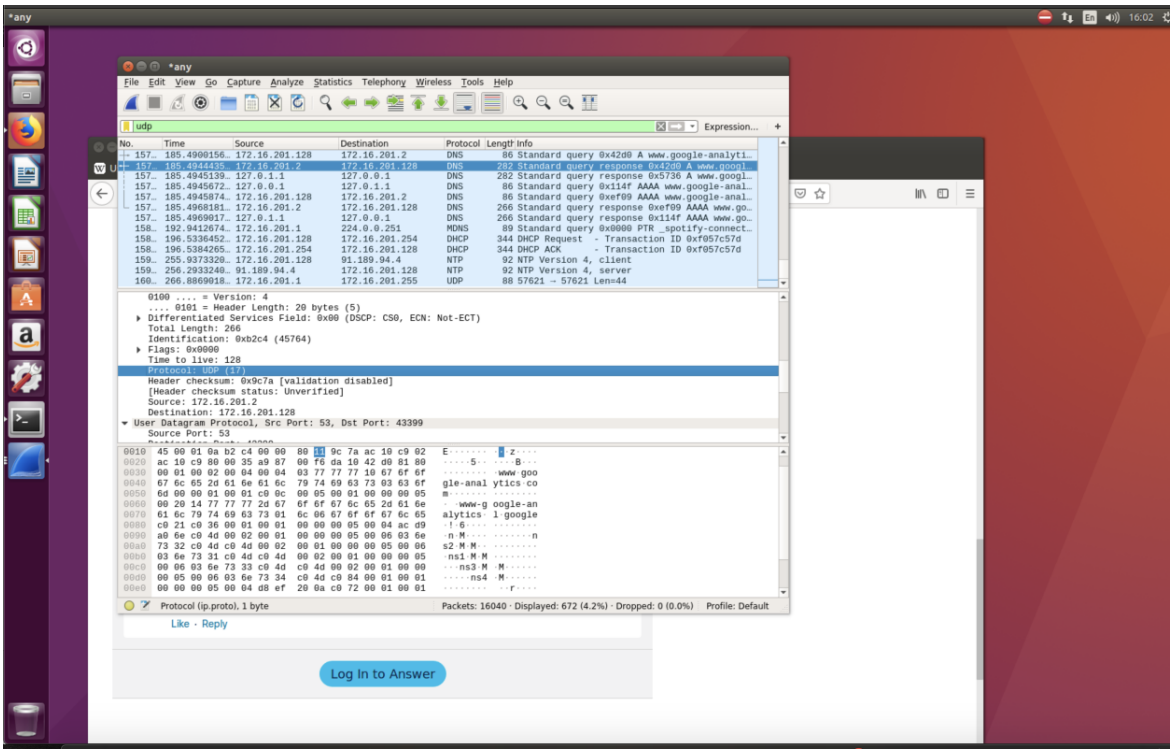
CN homework#1

b07902076
資工三 許世儒

Analysis of UDP packets

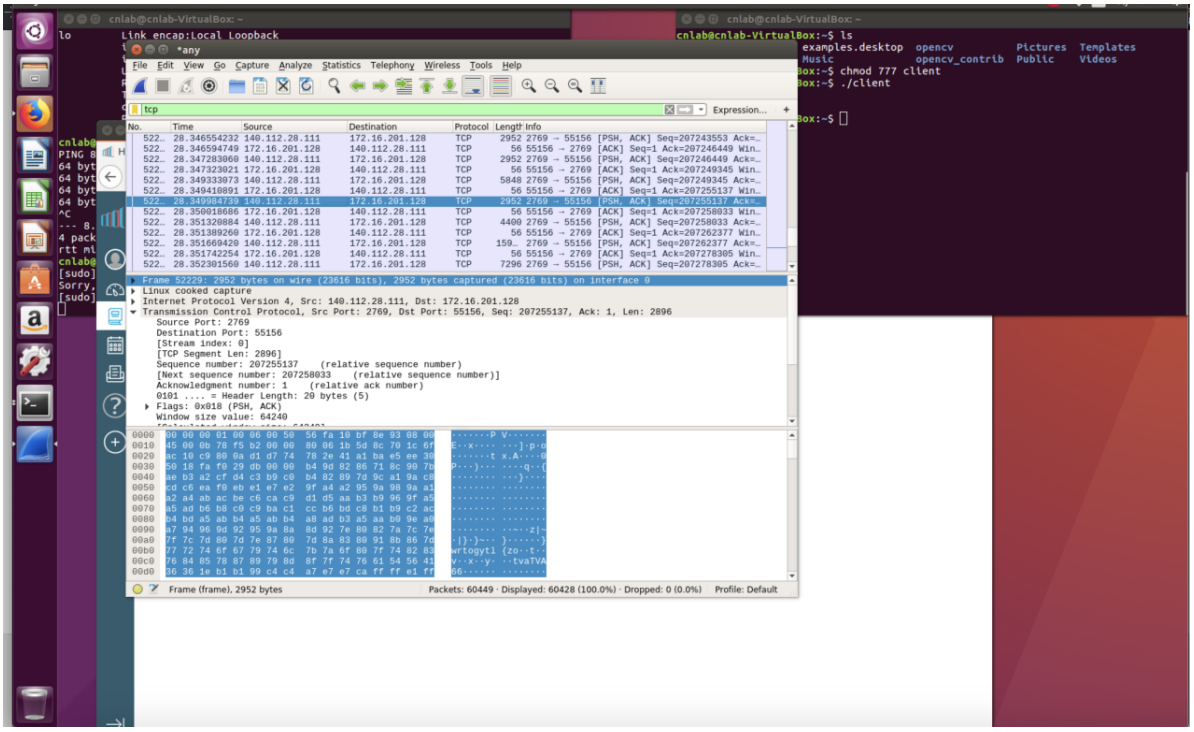


This is a DNS packet using UDP protocol. The packet was sent from a DNS server. DNS packets help users to translate hostname into IP address. The main reason for using UDP protocol is because

1. UDP is faster than TCP.
2. The Data packets of DNS are usually small compared to others.

Note that UDP is not reliable, but it can be strengthened by the application layer like using timeout and resend.

Analysis of TCP packets

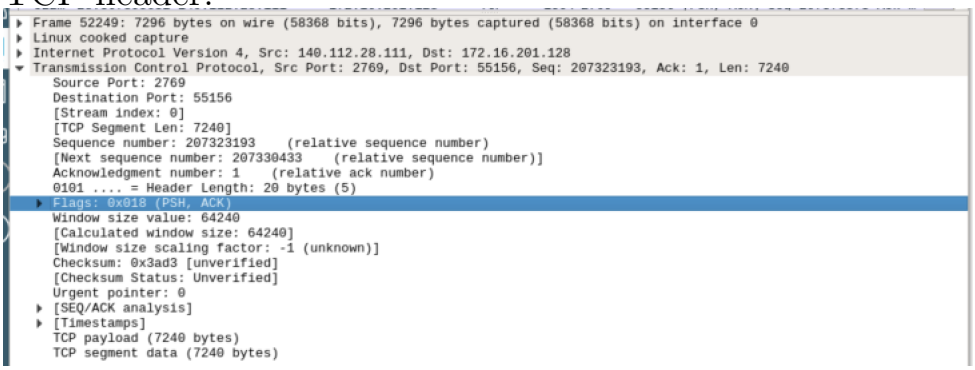


The server uses port 2769 for this application as the below screenshot shows.

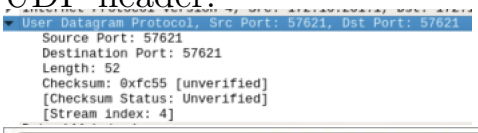
```
▾ Transmission Control Protocol, Src Port: 2769, Dst Port: 55156, Seq: 207255137, Ack: 1, Len: 289
    Source Port: 2769
    Destination Port: 55156
```

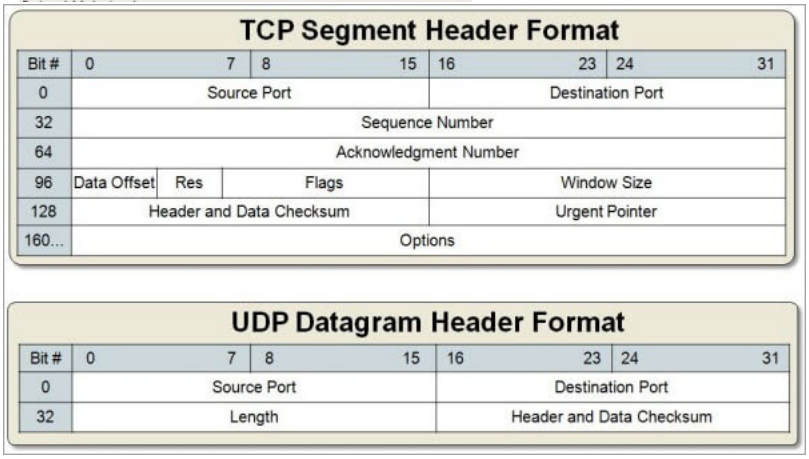
Compare the headers of transport layer between TCP and UDP

TCP header:



UDP header:





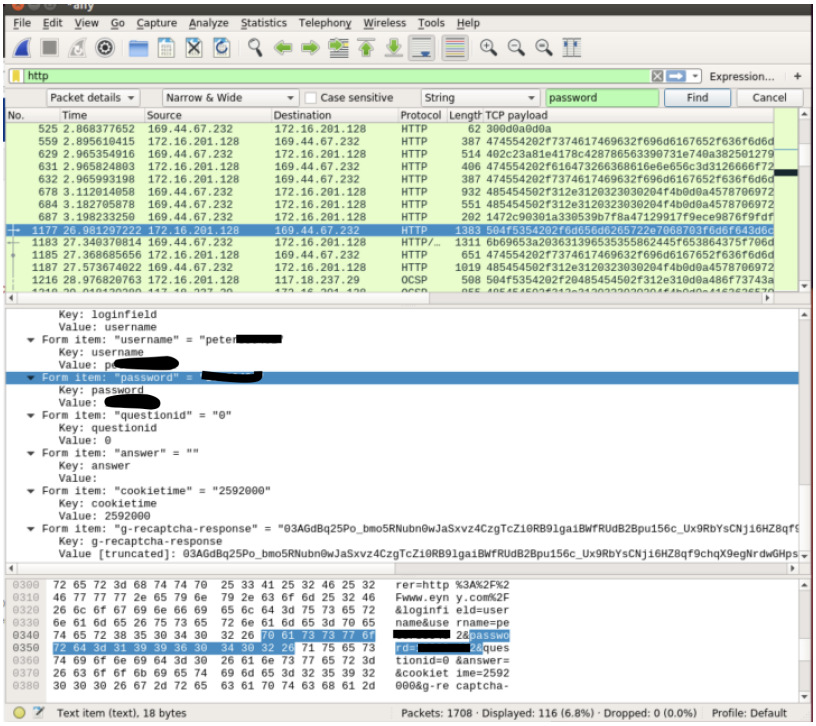
As we can see, the header of TCP contains the fields of Sequence Number, Header length, Acknowledgement number, Flags, Window field, Urgent pointer and Option which are not in the UDP header.

It's obvious that TCP header contains more information than UDP. The main difference is that TCP has the Sequence Number field and it's because it sends and receives packets of information as a stream of bytes. It may not arrive the destination at the same time, so they have a Sequence Number field to assemble the packets. Besides, the Acknowledgement Number field allows senders to determine whether the receivers lost packets and when to retransmit those packets.

With these two fields and error checksum field make TCP relatively reliable but more data overhead and latency. In contrast, UDP doesn't require to establish a

connection with 3-way handshake before any data transfering. It just sends the packets, so it has much lower bandwidth overhead and latency but some packets may be lost.

Find out a plaintext password



I found that the website of eyny sends plaintext password packets.

url: http://www.eyny.com/

This is unsafe because

(1) some bad guys may sniff our packets then get our password.

(2) if we connect to the Internet through proxy servers, then our password can be readable by them.

Observation: The situation of sending plaintext password mostly happen in http protocol. This kind of problem usually can be solved when using https protocol.