CS315 Lab 1 Writeup

孙永康　11911409

1.Carefully read the lab instructions and finish all tasks above.

yes, I have finish all task in the lab material, but I still have problem about a part of "wireshark" which is named "follow *** stream". I wonder how to read those words and what is the meaning of those information.

2.If a packet is highlighted by black, what does it mean for the packet?

TCP packets with problems

3.What is the filter command for listing all outgoing http traffic?

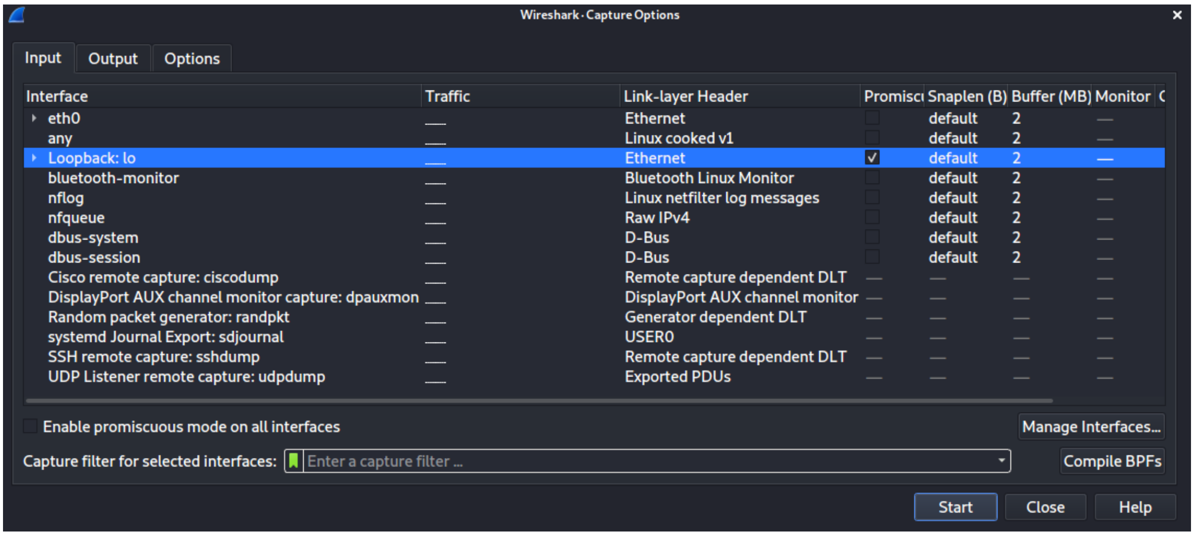
http and ip.src == your network IP

4.Why does DNS use Follow UDP Stream while HTTP use Follow TCP Stream?

DNS use UDP protocol which is faster but unstable. HTTP use TCP protocol since 'http' need accurate data transportation but not speed.

5.Using Wireshark to capture the FTP password.

choose to right settings: because of the ftp server is at 127.0.0.1, so we choose to catch pack delivered by loopback network card.



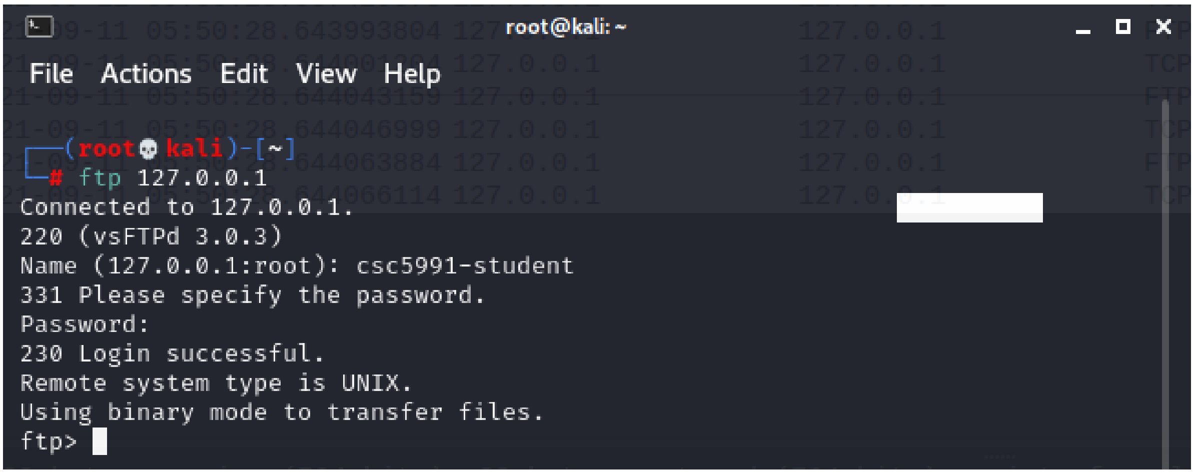
Wireshark · Capture Options

Interface	Traffic	Link-layer Header	Promisc	Snaplen (B)	Buffer (MB)	Monitor	C
eth0	___	Ethernet	□	default	2	—	
any	___	Linux cooked v1	□	default	2	—	
Loopback: lo	___	Ethernet	☑	default	2	—	
bluetooth-monitor	___	Bluetooth Linux Monitor	□	default	2	—	
nflog	___	Linux netfilter log messages	□	default	2	—	
nfqueue	___	Raw IPv4	□	default	2	—	
dbus-system	___	D-Bus	□	default	2	—	
dbus-session	___	D-Bus	□	default	2	—	
Cisco remote capture: ciscodump	___	Remote capture dependent DLT	—	—	—	—	
DisplayPort AUX channel monitor capture: dpauxmon	___	DisplayPort AUX channel monitor	—	—	—	—	
Random packet generator: randpkt	___	Generator dependent DLT	—	—	—	—	
systemd Journal Export: sdjournal	___	USER0	—	—	—	—	
SSH remote capture: sshdump	___	Remote capture dependent DLT	—	—	—	—	
UDP Listener remote capture: udpdump	___	Exported PDUs	—	—	—	—	

□ Enable promiscuous mode on all interfaces

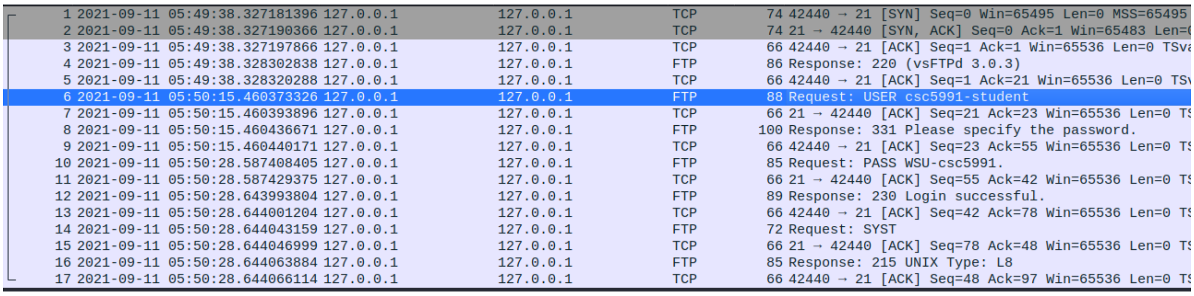
Capture filter for selected interfaces: Enter a capture filter ...

then we start connecting ftp server with terminal.



```
┌──(root💀kali)-[~]
└─# ftp 127.0.0.1
Connected to 127.0.0.1.
220 (vsFTPd 3.0.3)
Name (127.0.0.1:root): csc5991-student
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> 
```

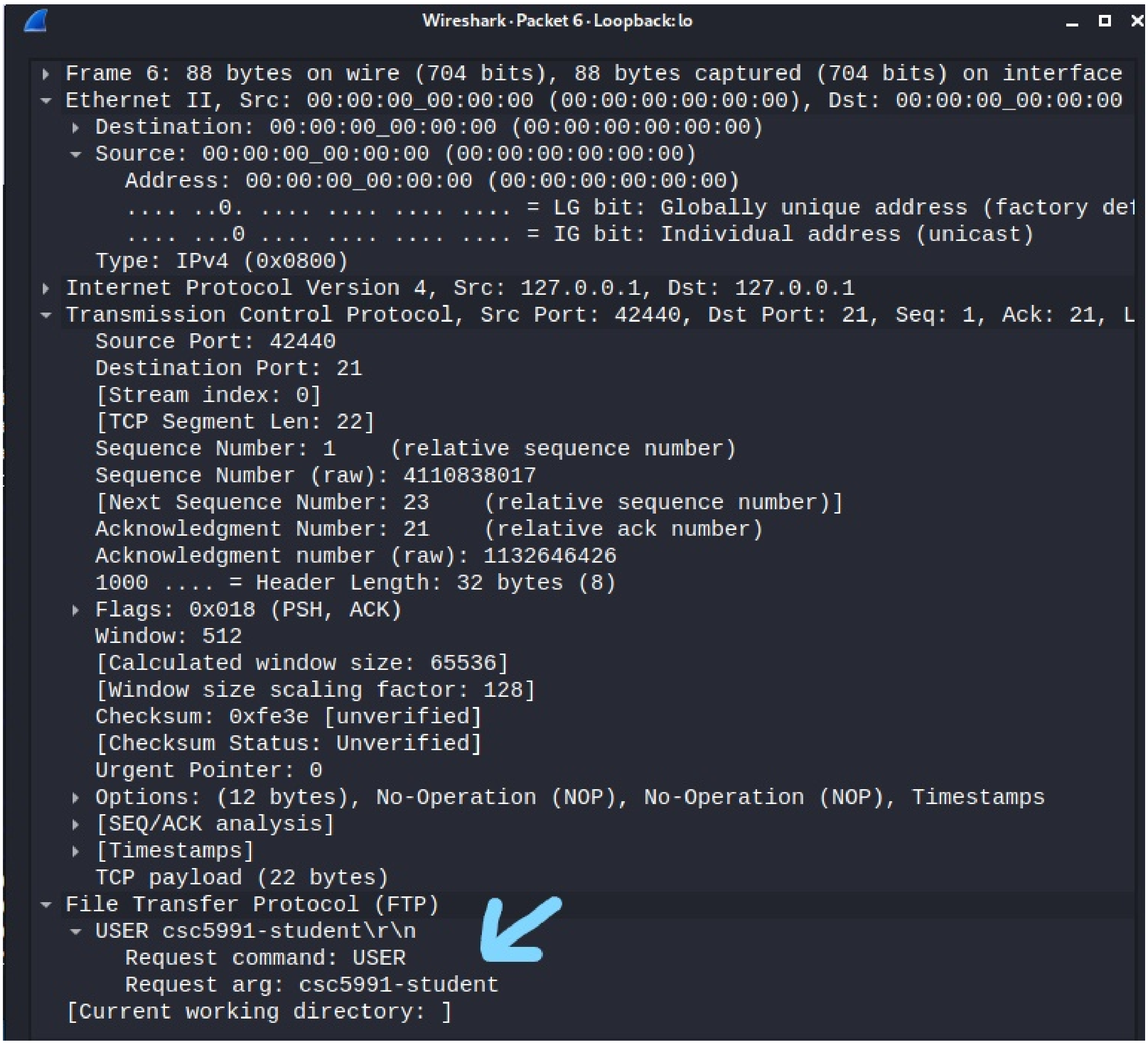
that is all pack wireshark caught when I register in FTP server.



```
 1 2021-09-11 05:49:38.327181396 127.0.0.1    127.0.0.1    TCP   74 42440 → 21 [SYN] Seq=0 Win=65495 Len=0 MSS=65495
 2 2021-09-11 05:49:38.327190366 127.0.0.1    127.0.0.1    TCP   74 21 → 42440 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=
 3 2021-09-11 05:49:38.327197866 127.0.0.1    127.0.0.1    TCP   66 42440 → 21 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSva
 4 2021-09-11 05:49:38.328302838 127.0.0.1    127.0.0.1    FTP   86 Response: 220 (vsFTPd 3.0.3)
 5 2021-09-11 05:49:38.328320288 127.0.0.1    127.0.0.1    TCP   66 42440 → 21 [ACK] Seq=1 Ack=21 Win=65536 Len=0 TSv
 6 2021-09-11 05:50:15.460373326 127.0.0.1    127.0.0.1    FTP   88 Request: USER csc5991-student
 7 2021-09-11 05:50:15.460393896 127.0.0.1    127.0.0.1    TCP   66 21 → 42440 [ACK] Seq=21 Ack=23 Win=65536 Len=0 TS
 8 2021-09-11 05:50:15.460436671 127.0.0.1    127.0.0.1    FTP  100 Response: 331 Please specify the password.
 9 2021-09-11 05:50:15.460440171 127.0.0.1    127.0.0.1    TCP   66 42440 → 21 [ACK] Seq=23 Ack=55 Win=65536 Len=0 TS
10 2021-09-11 05:50:28.587408405 127.0.0.1    127.0.0.1    FTP   85 Request: PASS WSU-csc5991.
11 2021-09-11 05:50:28.587429375 127.0.0.1    127.0.0.1    TCP   66 21 → 42440 [ACK] Seq=55 Ack=42 Win=65536 Len=0 TS
12 2021-09-11 05:50:28.643993804 127.0.0.1    127.0.0.1    FTP   89 Response: 230 Login successful.
13 2021-09-11 05:50:28.644001204 127.0.0.1    127.0.0.1    TCP   66 42440 → 21 [ACK] Seq=42 Ack=78 Win=65536 Len=0 TS
14 2021-09-11 05:50:28.644043159 127.0.0.1    127.0.0.1    FTP   72 Request: SYST
15 2021-09-11 05:50:28.644046999 127.0.0.1    127.0.0.1    TCP   66 21 → 42440 [ACK] Seq=78 Ack=48 Win=65536 Len=0 TS
16 2021-09-11 05:50:28.644063884 127.0.0.1    127.0.0.1    FTP   85 Response: 215 UNIX Type: L8
17 2021-09-11 05:50:28.644066114 127.0.0.1    127.0.0.1    TCP   66 42440 → 21 [ACK] Seq=48 Ack=97 Win=65536 Len=0 TS
```

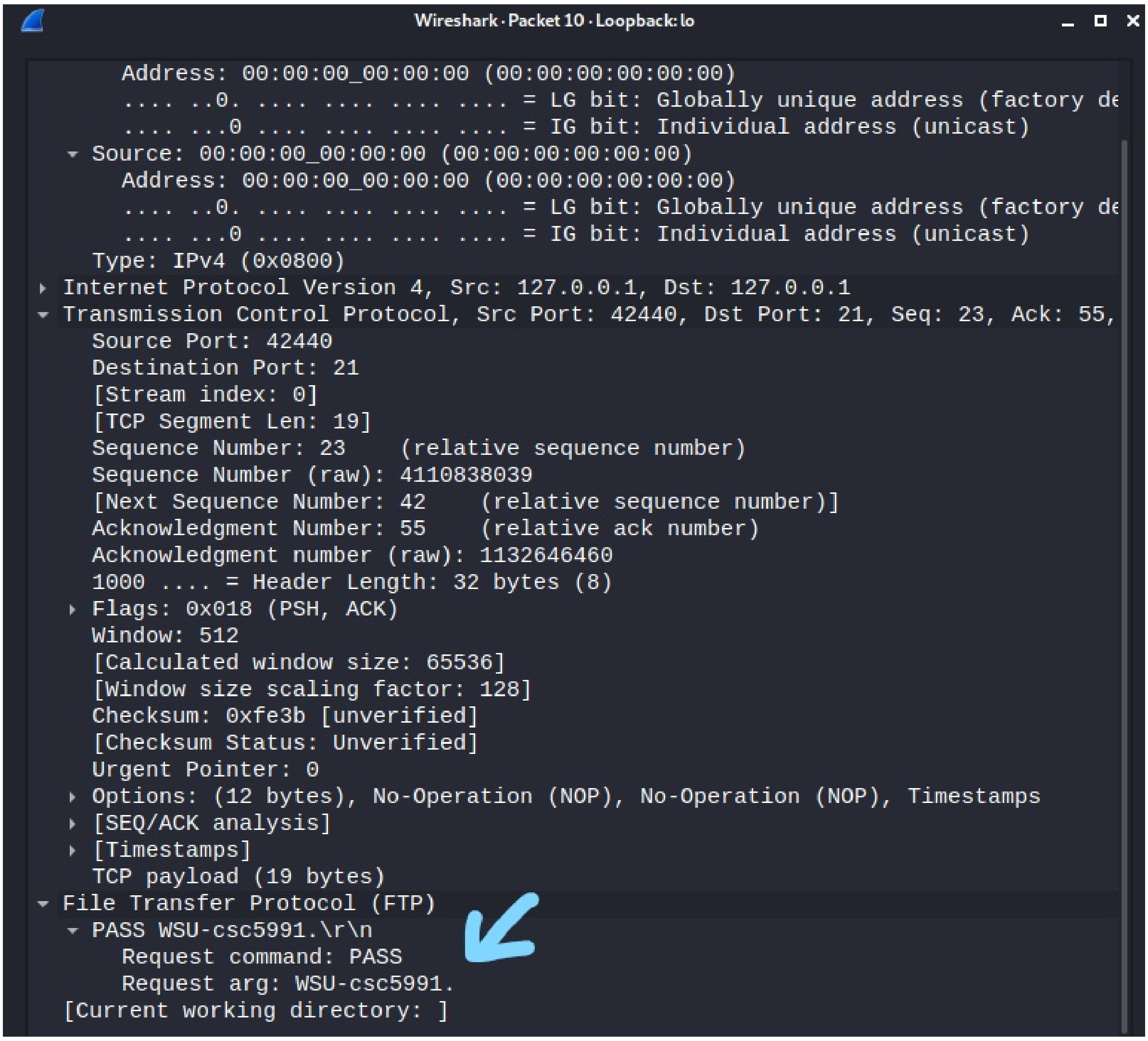
As we can see, the pack 6 and pack 10 has the information we want.

username:



```
▸ Frame 6: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface
▾ Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00
  ▸ Destination: 00:00:00_00:00:00 (00:00:00:00:00:00)
  ▾ Source: 00:00:00_00:00:00 (00:00:00:00:00:00)
      Address: 00:00:00_00:00:00 (00:00:00:00:00:00)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory def
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
▸ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
▾ Transmission Control Protocol, Src Port: 42440, Dst Port: 21, Seq: 1, Ack: 21, L
    Source Port: 42440
    Destination Port: 21
    [Stream index: 0]
    [TCP Segment Len: 22]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 4110838017
    [Next Sequence Number: 23    (relative sequence number)]
    Acknowledgment Number: 21    (relative ack number)
    Acknowledgment number (raw): 1132646426
    1000 .... = Header Length: 32 bytes (8)
  ▸ Flags: 0x018 (PSH, ACK)
    Window: 512
    [Calculated window size: 65536]
    [Window size scaling factor: 128]
    Checksum: 0xfe3e [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  ▸ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  ▸ [SEQ/ACK analysis]
  ▸ [Timestamps]
    TCP payload (22 bytes)
▾ File Transfer Protocol (FTP)
  ▾ USER csc5991-student\r\n
      Request command: USER
      Request arg: csc5991-student
  [Current working directory: ]
```

password:



```
      Address: 00:00:00_00:00:00 (00:00:00:00:00:00)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory de
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▾ Source: 00:00:00_00:00:00 (00:00:00:00:00:00)
      Address: 00:00:00_00:00:00 (00:00:00:00:00:00)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory de
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
▸ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
▾ Transmission Control Protocol, Src Port: 42440, Dst Port: 21, Seq: 23, Ack: 55,
    Source Port: 42440
    Destination Port: 21
    [Stream index: 0]
    [TCP Segment Len: 19]
    Sequence Number: 23    (relative sequence number)
    Sequence Number (raw): 4110838039
    [Next Sequence Number: 42    (relative sequence number)]
    Acknowledgment Number: 55    (relative ack number)
    Acknowledgment number (raw): 1132646460
    1000 .... = Header Length: 32 bytes (8)
  ▸ Flags: 0x018 (PSH, ACK)
    Window: 512
    [Calculated window size: 65536]
    [Window size scaling factor: 128]
    Checksum: 0xfe3b [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  ▸ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  ▸ [SEQ/ACK analysis]
  ▸ [Timestamps]
    TCP payload (19 bytes)
▾ File Transfer Protocol (FTP)
  ▾ PASS WSU-csc5991.\r\n
      Request command: PASS
      Request arg: WSU-csc5991.
  [Current working directory: ]
```

By the there are other TCP protocol packs along with FTP packs. the first three of those are used to shake hands with the server.