Lab 3: Packet Analysis II

- You should not scan any live servers using Nmap and hping3. For violation, you may be expelled from the school (not a joke!).
- This is an individual assignment, and is worth 20 points.
- You need to provide the answers using the accompanying outcome file. Change the file name following the naming convention suggested below.
- Naming convention is as follows: homework, underscore, last name, first initial, and extension (e.g., Lab 1_ImG.docx). If you do not follow the convention, I will deduct 1.
- Do not copy any of the sample screenshots provided as illustrations.

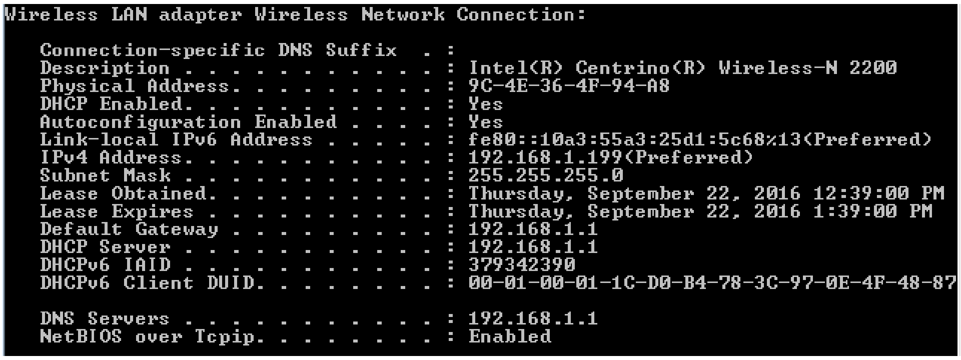
Task 1. Figuring out the IP addresses

- Task

1) Report the IP address of your host and the subnet mask (use ipconfig /all). Also, report the network address of your host. If you find many IP addresses, the IP address of "Wireless LAN adapter Wi-Fi" may be the active physical interface. Report with a screenshot.

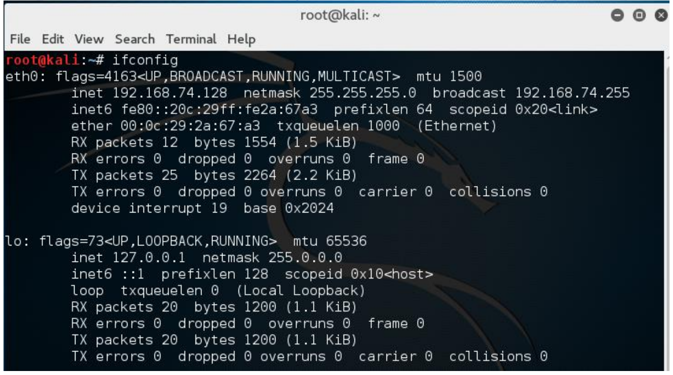
Ip Address:192.168.1.199

Network address: 192.168.1.199/24



```
Wireless LAN adapter Wireless Network Connection:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Centrino(R) Wireless-N 2200
   Physical Address. . . . . . . . . : 9C-4E-36-4F-94-A8
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::10a3:55a3:25d1:5c68%13(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.199(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Thursday, September 22, 2016 12:39:00 PM
   Lease Expires . . . . . . . . . . : Thursday, September 22, 2016 1:39:00 PM
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 379342390
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-1C-D0-B4-78-3C-97-0E-4F-48-87

   DNS Servers . . . . . . . . . . . : 192.168.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

2) Report the IP address of your Kali (use ifconfig). Report with a screenshot.



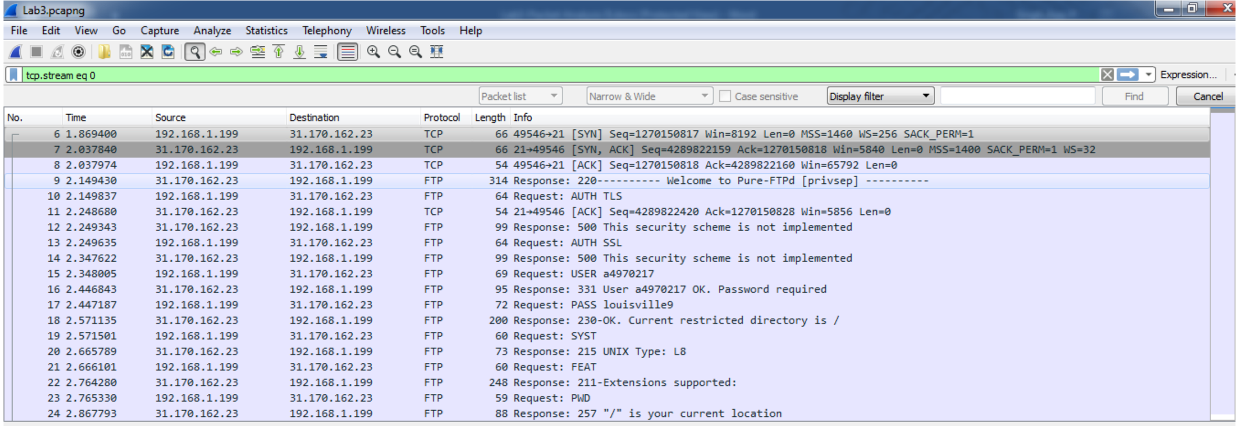
```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.74.128  netmask 255.255.255.0  broadcast 192.168.74.255
        inet6 fe80::20c:29ff:fe2a:67a3  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:2a:67:a3  txqueuelen 1000  (Ethernet)
        RX packets 12  bytes 1554 (1.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 25  bytes 2264 (2.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 19  base 0x2024

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 0  (Local Loopback)
        RX packets 20  bytes 1200 (1.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20  bytes 1200 (1.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

192.168.74.128

Task 2. Analyzing FTP Signatures

- Task

1) Identify the three TCP packets used for the initial 3-way handshaking. <u>Take a screenshot of the TCP packets</u>. **Hint**: Use the display filter “ftp.” And right-click on the packet of your interest and Follow > TCP Stream to understand the data flow. Use the IP address of the ftp server to recognize the relevant TCP stream. Use the display filter “tcp.stream eq xx” (replace xx with the integer) as necessary.

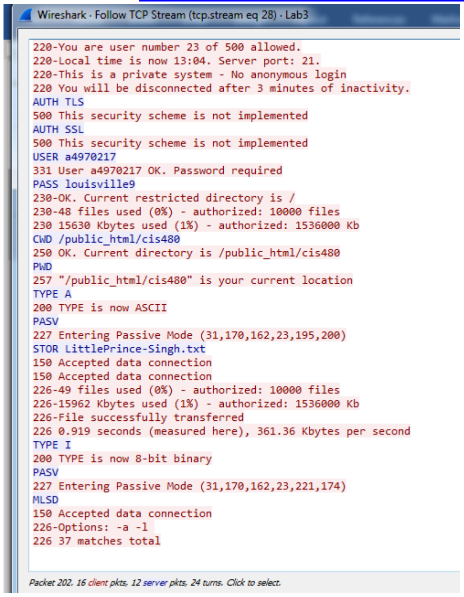


tcp.stream eq 0

```
No.   Time        Source          Destination     Protocol  Length Info
    6 1.869400    192.168.1.199   31.170.162.23   TCP        66 49546→21 [SYN] Seq=1270150817 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
    7 2.037840    31.170.162.23   192.168.1.199   TCP        66 21→49546 [SYN, ACK] Seq=4289822159 Ack=1270150818 Win=5840 Len=0 MSS=1400 SACK_PERM=1 WS=32
    8 2.037974    192.168.1.199   31.170.162.23   TCP        54 49546→21 [ACK] Seq=1270150818 Ack=4289822160 Win=65792 Len=0
    9 2.149430    31.170.162.23   192.168.1.199   FTP       314 Response: 220---------- Welcome to Pure-FTPd [privsep] ----------
   10 2.149837    192.168.1.199   31.170.162.23   FTP        64 Request: AUTH TLS
   11 2.248680    31.170.162.23   192.168.1.199   TCP        54 21→49546 [ACK] Seq=4289822420 Ack=1270150828 Win=5856 Len=0
   12 2.249343    31.170.162.23   192.168.1.199   FTP        99 Response: 500 This security scheme is not implemented
   13 2.249635    192.168.1.199   31.170.162.23   FTP        64 Request: AUTH SSL
   14 2.347622    31.170.162.23   192.168.1.199   FTP        99 Response: 500 This security scheme is not implemented
   15 2.348005    192.168.1.199   31.170.162.23   FTP        69 Request: USER a4970217
   16 2.446843    31.170.162.23   192.168.1.199   FTP        95 Response: 331 User a4970217 OK. Password required
   17 2.447187    192.168.1.199   31.170.162.23   FTP        72 Request: PASS louisville9
   18 2.571135    31.170.162.23   192.168.1.199   FTP       200 Response: 230-OK. Current restricted directory is /
   19 2.571501    192.168.1.199   31.170.162.23   FTP        60 Request: SYST
   20 2.665789    31.170.162.23   192.168.1.199   FTP        73 Response: 215 UNIX Type: L8
   21 2.666101    192.168.1.199   31.170.162.23   FTP        60 Request: FEAT
   22 2.764280    31.170.162.23   192.168.1.199   FTP       248 Response: 211-Extensions supported:
   23 2.765330    192.168.1.199   31.170.162.23   FTP        59 Request: PWD
   24 2.867793    31.170.162.23   192.168.1.199   FTP        88 Response: 257 "/" is your current location
```

6, 7, 8. TCP stream eq 0

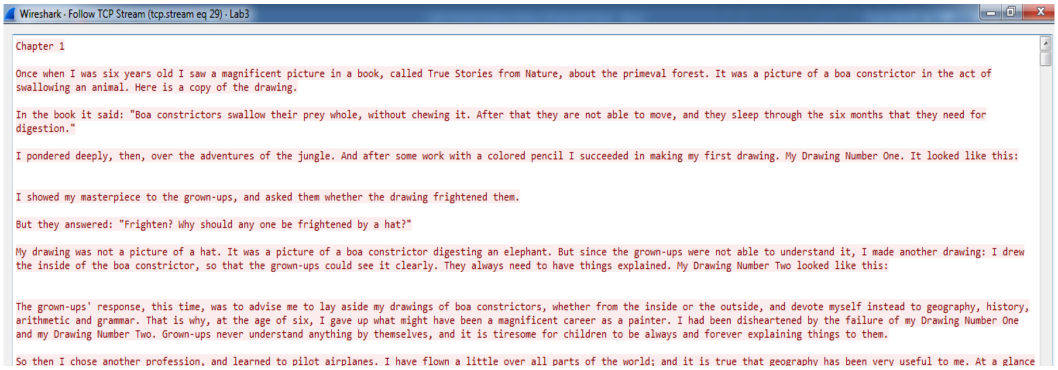
2) Identify the FTP packets that show the Username and the Password in plaintext. Follow the TCP stream and <u>take a screenshot of the TCP stream</u>.



```
220-You are user number 23 of 500 allowed.
220-Local time is now 13:04. Server port: 21.
220-This is a private system - No anonymous login
220 You will be disconnected after 3 minutes of inactivity.
AUTH TLS
500 This security scheme is not implemented
AUTH SSL
500 This security scheme is not implemented
USER a4970217
331 User a4970217 OK. Password required
PASS louisville9
230-OK. Current restricted directory is /
230-48 files used (0%) - authorized: 10000 files
230 15630 Kbytes used (1%) - authorized: 1536000 Kb
CWD /public_html/cis480
250 OK. Current directory is /public_html/cis480
PWD
257 "/public_html/cis480" is your current location
TYPE A
200 TYPE is now ASCII
PASV
227 Entering Passive Mode (31,170,162,23,195,200)
STOR LittlePrince-Singh.txt
150 Accepted data connection
150 Accepted data connection
226-49 files used (0%) - authorized: 10000 files
226-15962 Kbytes used (1%) - authorized: 1536000 Kb
226-File successfully transferred
226 0.919 seconds (measured here), 361.36 Kbytes per second
TYPE I
200 TYPE is now 8-bit binary
PASV
227 Entering Passive Mode (31,170,162,23,221,174)
MLSD
150 Accepted data connection
226-Options: -a -l
226 37 matches total
```

Packet 202. 16 client pkts, 12 server pkts, 24 turns. Click to select.

3) Identify the FTP-DATA packets used for the textfile uploading. Follow the TCP stream and <u>take a screenshot of the TCP stream</u>. The textfile is uploaded across many FTP-DATA packets. So, any part of the data is okay.

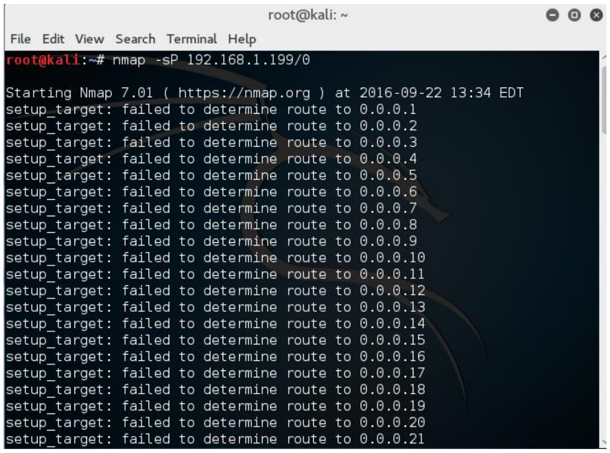


```
Chapter 1

Once when I was six years old I saw a magnificent picture in a book, called True Stories from Nature, about the primeval forest. It was a picture of a boa constrictor in the act of
swallowing an animal. Here is a copy of the drawing.

In the book it said: "Boa constrictors swallow their prey whole, without chewing it. After that they are not able to move, and they sleep through the six months that they need for
digestion."

I pondered deeply, then, over the adventures of the jungle. And after some work with a colored pencil I succeeded in making my first drawing. My Drawing Number One. It looked like this:


I showed my masterpiece to the grown-ups, and asked them whether the drawing frightened them.

But they answered: "Frighten? Why should any one be frightened by a hat?"

My drawing was not a picture of a hat. It was a picture of a boa constrictor digesting an elephant. But since the grown-ups were not able to understand it, I made another drawing: I drew
the inside of the boa constrictor, so that the grown-ups could see it clearly. They always need to have things explained. My Drawing Number Two looked like this:


The grown-ups' response, this time, was to advise me to lay aside my drawings of boa constrictors, whether from the inside or the outside, and devote myself instead to geography, history,
arithmetic and grammar. That is why, at the age of six, I gave up what might have been a magnificent career as a painter. I had been disheartened by the failure of my Drawing Number One
and my Drawing Number Two. Grown-ups never understand anything by themselves, and it is tiresome for children to be always and forever explaining things to them.

So then I chose another profession, and learned to pilot airplanes. I have flown a little over all parts of the world; and it is true that geography has been very useful to me. At a glance
```

Task 3. Ping Sweeping

- Task

1) Report your result in a screenshot like below.

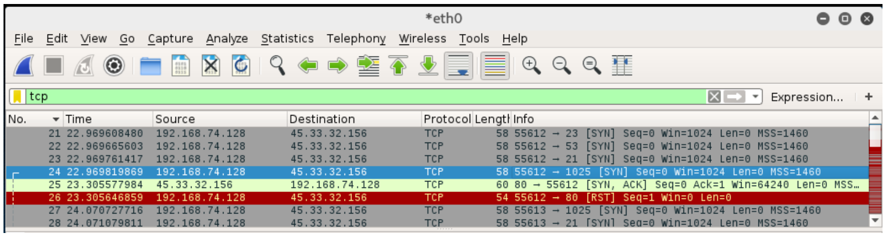


```
root@kali:~# nmap -sP 192.168.1.199/0

Starting Nmap 7.01 ( https://nmap.org ) at 2016-09-22 13:34 EDT
setup_target: failed to determine route to 0.0.0.1
setup_target: failed to determine route to 0.0.0.2
setup_target: failed to determine route to 0.0.0.3
setup_target: failed to determine route to 0.0.0.4
setup_target: failed to determine route to 0.0.0.5
setup_target: failed to determine route to 0.0.0.6
setup_target: failed to determine route to 0.0.0.7
setup_target: failed to determine route to 0.0.0.8
setup_target: failed to determine route to 0.0.0.9
setup_target: failed to determine route to 0.0.0.10
setup_target: failed to determine route to 0.0.0.11
setup_target: failed to determine route to 0.0.0.12
setup_target: failed to determine route to 0.0.0.13
setup_target: failed to determine route to 0.0.0.14
setup_target: failed to determine route to 0.0.0.15
setup_target: failed to determine route to 0.0.0.16
setup_target: failed to determine route to 0.0.0.17
setup_target: failed to determine route to 0.0.0.18
setup_target: failed to determine route to 0.0.0.19
setup_target: failed to determine route to 0.0.0.20
setup_target: failed to determine route to 0.0.0.21
```

Task 4. Port Scanning

- Task

1) Answer the following questions. Provide a screenshot for each question to support your answer. For the answers, use the display filter "tcp.stream eq xx" (replace xx with the integer) as necessary.
   - Which TCP packet (e.g., SYN, SYN/ACK, ACK, etc.) was sent from the Kali to the victim?
   - Which TCP packet was received from the victim to the Kali in response?


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+

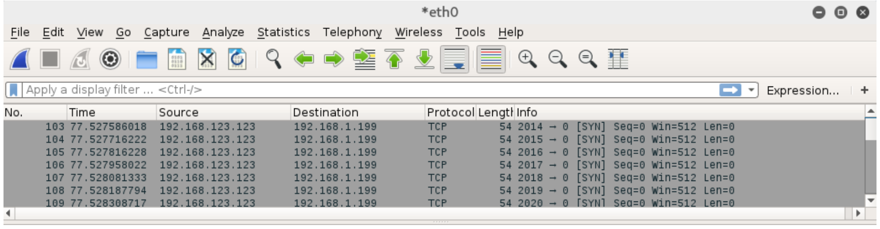
```
tcp
No.     Time          Source           Destination      Protocol Lengtl Info
     21 22.969608480  192.168.74.128   45.33.32.156     TCP        58 55612 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
     22 22.969665603  192.168.74.128   45.33.32.156     TCP        58 55612 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
     23 22.969761417  192.168.74.128   45.33.32.156     TCP        58 55612 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
     24 22.969819869  192.168.74.128   45.33.32.156     TCP        58 55612 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
     25 23.305577984  45.33.32.156     192.168.74.128   TCP        60 80 → 55612 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS…
     26 23.305646859  192.168.74.128   45.33.32.156     TCP        54 55612 → 80 [RST] Seq=1 Win=0 Len=0
     27 24.070727716  192.168.74.128   45.33.32.156     TCP        58 55613 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
     28 24.071079811  192.168.74.128   45.33.32.156     TCP        58 55613 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
```

Packet 24 was sent to victim and packet 25 was received in response.

Task 5. SYN Flooding Attack

- Task

1) Launch a SYN flooding attack using the IP address of your host as the victim and an arbitrary private IP address as the spoofed address.
    - Report your result in a screenshot.



```
No.    Time         Source           Destination     Protocol Lengtł Info
   103 77.527586018 192.168.123.123  192.168.1.199   TCP        54 2014 → 0 [SYN] Seq=0 Win=512 Len=0
   104 77.527716222 192.168.123.123  192.168.1.199   TCP        54 2015 → 0 [SYN] Seq=0 Win=512 Len=0
   105 77.527816228 192.168.123.123  192.168.1.199   TCP        54 2016 → 0 [SYN] Seq=0 Win=512 Len=0
   106 77.527958022 192.168.123.123  192.168.1.199   TCP        54 2017 → 0 [SYN] Seq=0 Win=512 Len=0
   107 77.528081333 192.168.123.123  192.168.1.199   TCP        54 2018 → 0 [SYN] Seq=0 Win=512 Len=0
   108 77.528187794 192.168.123.123  192.168.1.199   TCP        54 2019 → 0 [SYN] Seq=0 Win=512 Len=0
   109 77.528308717 192.168.123.123  192.168.1.199   TCP        54 2020 → 0 [SYN] Seq=0 Win=512 Len=0
```