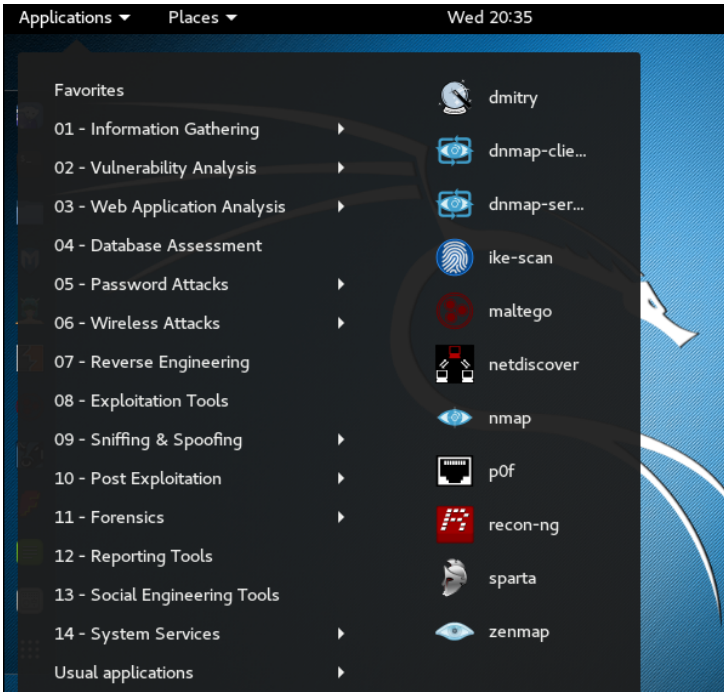
Lab 3: Packet Analysis II

- The due date and time is 4:00 Thur, September 21 (Sec 01) / 7:00 Thur, September 21 (Sec 76).
- This is an individual assignment, and is worth 20 points.
- You should provide the answers using the accompanying outcome file. Change the file name following the naming convention suggested below.
- The 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.
- You should not scan any live servers using Nmap and hping3. For violation, you may be expelled from the school (not a joke!).

Prep

- Study Nmap using the following sites.
    - http://nmap.org/
    - http://www.cyberciti.biz/networking/nmap-command-examples-tutorials/
- In Kali, Nmap can be found via the navigation path of Applications > 01- Information Gathering > nmap. Or, launch a Terminal and type "nmap" on the command shell.



Task 1. Figuring out the IP addresses

- You have to know the IP addresses of your host and the Kali before you conduct the next tasks.

- Task
  1) Report the IP address of your host and the subnet mask (use ipconfig /all). If you use wireless, the IP address of "Wireless LAN adapter Wi-Fi" is the active physical interface. Report with a screenshot.
  2) Report the IP address of your Kali (use ifconfig). Report with a screenshot.

Task 2. Analyzing FTP Signatures

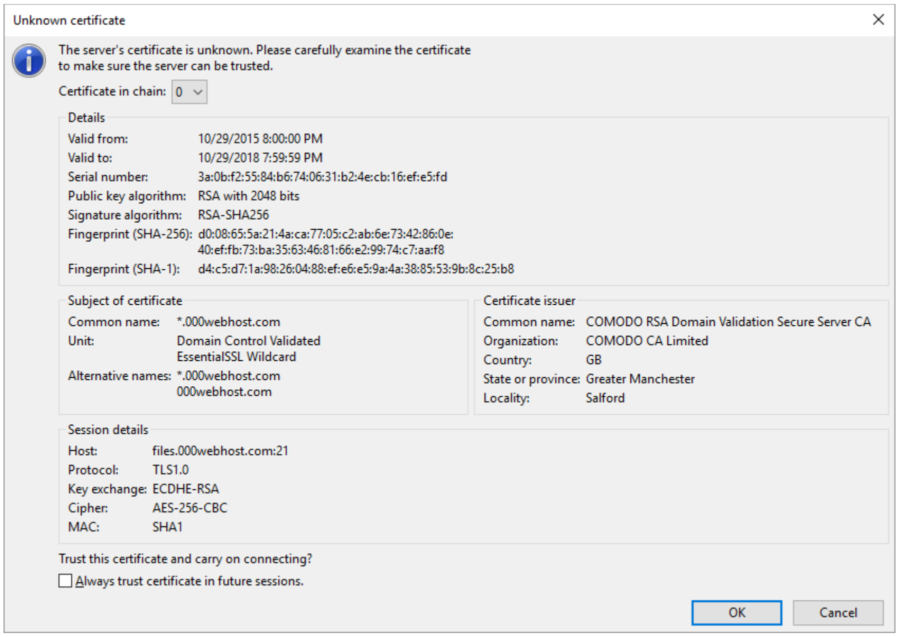
- Upload the text file (LittlePrince.txt) to the designated site and capture the packets for this activity with Wireshark.
- First, you should install the ftp client FileZilla on your host. The Mac version is also available.
- Persona-SQL has FileZilla and Wireshark installation. However, I recommend you to do this task at home. The school network generates too many irrelevant packets.

- The ftp server and account information:

Host	files.000webhost.com
Username	liquid-seamanship
Password	louisville9
Folder to upload files	public_html/CIS480

- Steps:
  1) Close any browser, email, etc on your host that can generate internet traffic.
  2) Change the name of the textfile to "LittlePrince-[your-lastname].txt."
  3) Launch FileZilla.
  4) Turn on Wireshark on the host by following Capture > Options > Input > Select Interface > Start.
  5) Connect to the ftp server.
  6) Upload the textfile to the designated directory.
  7) After the uploading is successful, stop Wireshark.
  8) Save the captured traffic as "*.pcapng."

- Note
  - If you see the following screen on ftp login, click on OK. The site is using a certificate for encryption.



Unknown certificate

The server's certificate is unknown. Please carefully examine the certificate
to make sure the server can be trusted.

Certificate in chain: 0

Details

Valid from:	10/29/2015 8:00:00 PM
Valid to:	10/29/2018 7:59:59 PM
Serial number:	3a:0b:f2:55:84:b6:74:06:31:b2:4e:cb:16:ef:e5:fd
Public key algorithm:	RSA with 2048 bits
Signature algorithm:	RSA-SHA256
Fingerprint (SHA-256):	d0:08:65:5a:21:4a:ca:77:05:c2:ab:6e:73:42:86:0e: 40:ef:fb:73:ba:35:63:46:81:66:e2:99:74:c7:aa:f8
Fingerprint (SHA-1):	d4:c5:d7:1a:98:26:04:88:ef:e6:e5:9a:4a:38:85:53:9b:8c:25:b8

Subject of certificate

Common name:	*.000webhost.com
Unit:	Domain Control Validated EssentialSSL Wildcard
Alternative names:	*.000webhost.com 000webhost.com

Certificate issuer

Common name:	COMODO RSA Domain Validation Secure Server CA
Organization:	COMODO CA Limited
Country:	GB
State or province:	Greater Manchester
Locality:	Salford

Session details

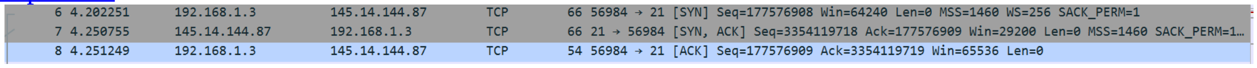
Host:	files.000webhost.com:21
Protocol:	TLS1.0
Key exchange:	ECDHE-RSA
Cipher:	AES-256-CBC
MAC:	SHA1

Trust this certificate and carry on connecting?

☐ Always trust certificate in future sessions.

- Task

1) Identify the three TCP packets used for the initial 3-way handshaking. Take a screenshot of the TCP packets.

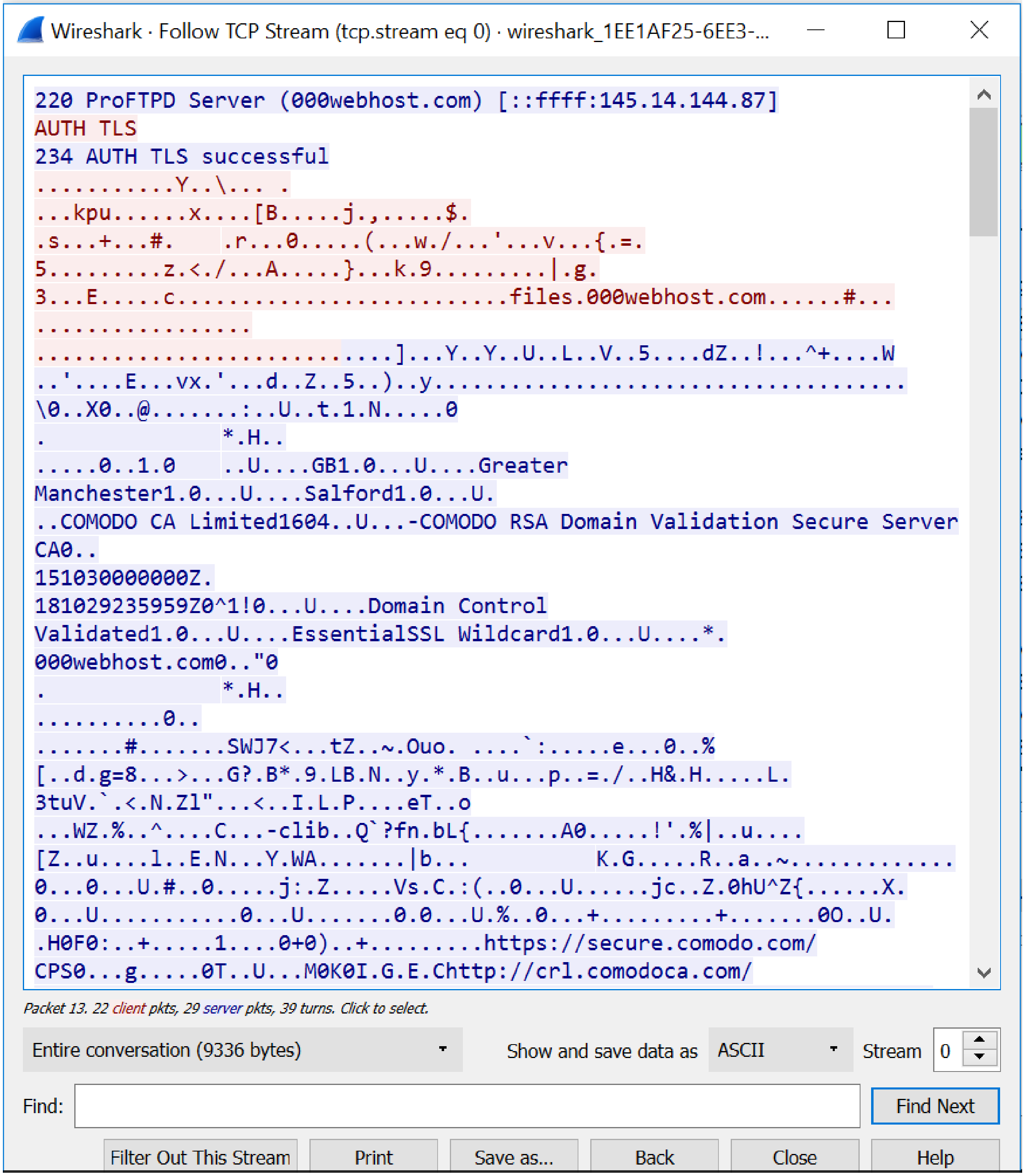


```
 6 4.202251   192.168.1.3    145.14.144.87  TCP  66 56984 → 21 [SYN] Seq=177576908 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 7 4.250755   145.14.144.87  192.168.1.3    TCP  66 21 → 56984 [SYN, ACK] Seq=3354119718 Ack=177576909 Win=29200 Len=0 MSS=1460 SACK_PERM=1…
 8 4.251249   192.168.1.3    145.14.144.87  TCP  54 56984 → 21 [ACK] Seq=177576909 Ack=3354119719 Win=65536 Len=0
```

   - **Hint**: These packets are placed right before ftp packets.

2) Identify the FTP packets that show the Username and the Password. In fact, the Username and the Password are encrypted and we cannot figure it out. However, we can guess which packets have that information. Follow the TCP stream and take a screenshot of the TCP stream.

   - **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.



Wireshark · Follow TCP Stream (tcp.stream eq 0) · wireshark_1EE1AF25-6EE3-...

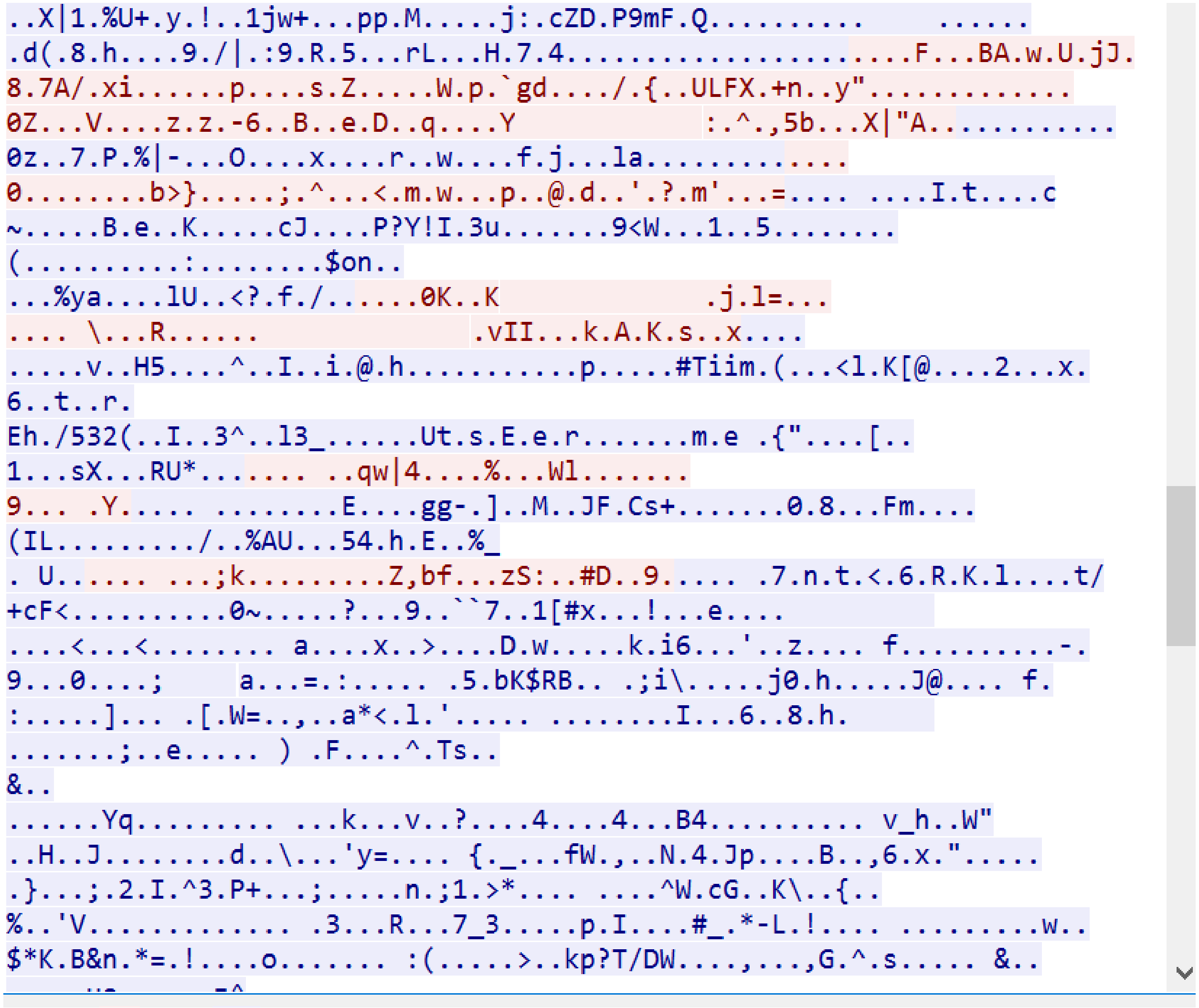
```
220 ProFTPD Server (000webhost.com) [::ffff:145.14.144.87]
AUTH TLS
234 AUTH TLS successful
...........Y..\... .
...kpu......x....[B.....j.,.....$.
.s...+...#.     .r...0.....(...w./...'...v...{.=.
5.........z.<./...A.....}...k.9.........|.g.
3...E.....c.........................files.000webhost.com......#...
.................
............................]...Y..Y..U..L..V..5....dZ..!...^+....W
..'....E...vx.'...d..Z..5..)..y....................................
\0..X0..@.......:..U..t.1.N.....0
.               *.H..
.....0..1.0     ..U....GB1.0...U....Greater
Manchester1.0...U....Salford1.0...U.
..COMODO CA Limited1604..U...-COMODO RSA Domain Validation Secure Server
CA0..
151030000000Z.
181029235959Z0^1!0...U....Domain Control
Validated1.0...U....EssentialSSL Wildcard1.0...U....*.
000webhost.com0.."0
.               *.H..
..........0..
.......#.......SWJ7<...tZ..~.Ouo. ....`:.....e...0..%
[..d.g=8...>...G?.B*.9.LB.N..y.*.B..u...p..=./..H&.H.....L.
3tuV.`.<.N.Zl"...<..I.L.P....eT..o
...WZ.%..^....C...-clib..Q`?fn.bL{.......A0.....!'.%|..u....
[Z..u....l..E.N...Y.WA.......|b...          K.G.....R..a..~.............
0...0...U.#..0.....j:.Z.....Vs.C.:(..0...U......jc..Z.0hU^Z{......X.
0...U...........0...U.......0.0...U.%..0...+.........+.......0O..U.
.H0F0:..+.....1....0+0)..+.........https://secure.comodo.com/
CPS0...g.....0T..U...M0K0I.G.E.Chttp://crl.comodoca.com/
```

Packet 13. 22 client pkts, 29 server pkts, 39 turns. Click to select.

Entire conversation (9336 bytes)   Show and save data as: ASCII   Stream: 0

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

- **Hint**: You need to check out TCP packets after FTP packets.



```
..X|1.%U+.y.!..1jw+...pp.M.....j:.cZD.P9mF.Q..........     ......
.d(.8.h....9./|.:9.R.5...rL...H.7.4.......................F...BA.w.U.jJ.
8.7A/.xi......p....s.Z.....W.p.`gd..../.{..ULFX.+n..y".............
0Z...V....z.z.-6..B..e.D..q....Y             :.^.,5b...X|"A............
0z..7.P.%|-...O....x....r..w....f.j...la..............
0........b>}.....;.^...<.m.w...p..@.d..'.?.m'...=.... ....I.t....c
~.....B.e..K.....cJ....P?Y!I.3u.......9<W...1..5........
(.........:........$on..
...%ya....lU..<?.f./.......0K..K             .j.l=...
.... \...R......              .vII...k.A.K.s..x....
.....v..H5....^..I..i.@.h...........p.....#Tiim.(...<l.K[@....2...x.
6..t..r.
Eh./532(..I..3^..l3_......Ut.s.E.e.r.......m.e .{"....[..
1...sX...RU*........ ..qw|4....%...Wl.......
9... .Y..... ........E....gg-.]..M..JF.Cs+.......0.8...Fm....
(IL........./..%AU...54.h.E..%_
. U...... ...;k.........Z,bf...zS:..#D..9..... .7.n.t.<.6.R.K.l....t/
+cF<..........0~.....?...9..``7..1[#x...!...e....
....<...<........ a....x..>....D.w.....k.i6...'..z.... f..........-.
9...0....;     a...=.:..... .5.bK$RB.. .;i\.....j0.h.....J@.... f.
:.....]... .[.W=..,..a*<.l.'..... ........I...6..8.h.
.......;..e..... ) .F....^.Ts..
&..
......Yq......... ...k...v..?....4....4...B4.......... v_h..W"
..H..J........d..\...'y=.... {._...fW.,..N.4.Jp....B..,6.x.".....
.}...;.2.I.^3.P+...;.....n.;1.>*.... ....^W.cG..K\..{..
%..'V............. .3...R...7_3.....p.I....#_.*-L.!.... .........w..
$*K.B&n.*=.!....o........ :(.....>..kp?T/DW....,...,G.^.s..... &..
```

- Note:

  1) If you don’t capture the traffic on Wireshark, it is possible that you have not selected the right interface.

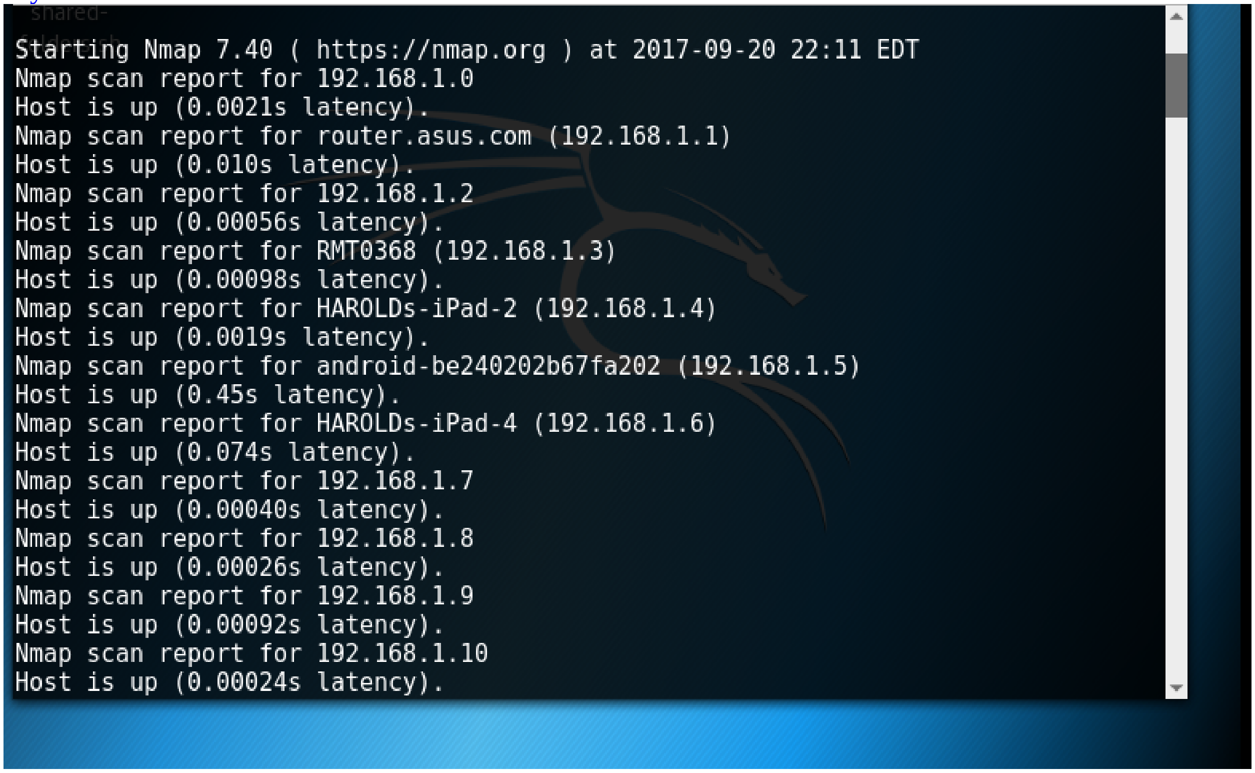
Task 3. Ping Sweeping

- Perform a ping sweeping attack with Nmap by sending a series of ICMP echo request packets to a range of IP addresses on a network.
- Pick a random private network address on your host and scan the network using the Kali.
- For ping sweeping, you have to provide the “network address”/“CIDR notation of the subnet mask.”

  (e.g., 192.168.10.0/24). Use **-sP** flag for ping sweeping. It takes a while and so be patient.
- In general, this is the command we use for Ping Sweeping.
  - o $ nmap -sP x.x.x.0/24 , where x.x.x.0 is the IP address of the network.
  - o (Example) $ nmap -sP 192.168.10.0/24 , where x.x.x.0 is the IP address of the network.
- Task

  1) Report your result in a screenshot like below.

My Screenshot



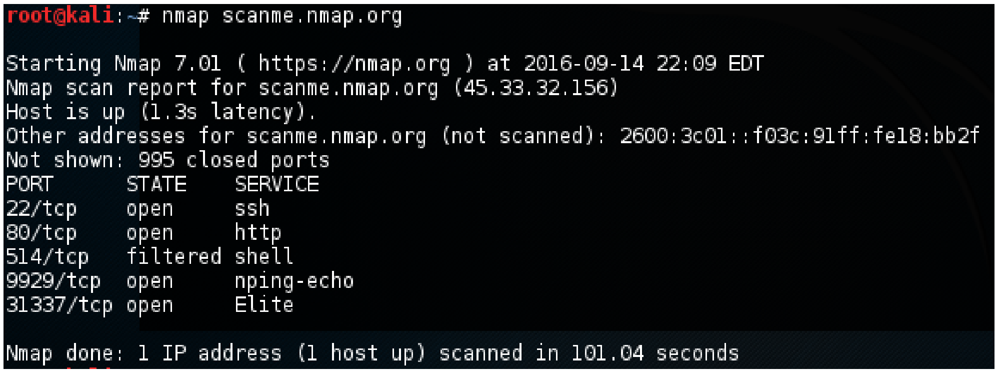
```
Starting Nmap 7.40 ( https://nmap.org ) at 2017-09-20 22:11 EDT
Nmap scan report for 192.168.1.0
Host is up (0.0021s latency).
Nmap scan report for router.asus.com (192.168.1.1)
Host is up (0.010s latency).
Nmap scan report for 192.168.1.2
Host is up (0.00056s latency).
Nmap scan report for RMT0368 (192.168.1.3)
Host is up (0.00098s latency).
Nmap scan report for HAROLDs-iPad-2 (192.168.1.4)
Host is up (0.0019s latency).
Nmap scan report for android-be240202b67fa202 (192.168.1.5)
Host is up (0.45s latency).
Nmap scan report for HAROLDs-iPad-4 (192.168.1.6)
Host is up (0.074s latency).
Nmap scan report for 192.168.1.7
Host is up (0.00040s latency).
Nmap scan report for 192.168.1.8
Host is up (0.00026s latency).
Nmap scan report for 192.168.1.9
Host is up (0.00092s latency).
Nmap scan report for 192.168.1.10
Host is up (0.00024s latency).
```

Task 4. Port Scanning

- Port scanning is an attempt to connect to a computer's ports to see whether any ports are active and listening.
- Scan the target (scanme.nmp.org) from your Kali and capture the packets with Wireshark on Kali.

- Steps:

1) Start Wireshark on your Kali after selecting the proper interface. To launch Wireshark, type "wireshark" on the command shell.
2) Run the following command and wait until you get the following result. Then, stop Wireshark by pressing the red button.



```
root@kali:~# nmap scanme.nmap.org

Starting Nmap 7.01 ( https://nmap.org ) at 2016-09-14 22:09 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (1.3s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 995 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
80/tcp    open     http
514/tcp   filtered shell
9929/tcp  open     nping-echo
31337/tcp open     Elite

Nmap done: 1 IP address (1 host up) scanned in 101.04 seconds
```

- Task

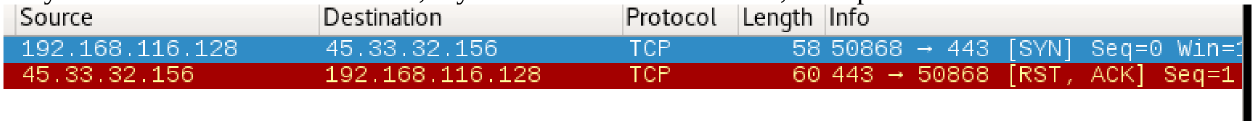
Answer the following questions. Provide a screenshot for each question to support your answer. For the answers, use the display filter “tcp.stream eq xx” (replace xx with the integer) as necessary.

1) Which type of TCP packet (e.g., SYN, SYN/ACK, or ACK) was sent from your Kali to the victim?

As you can see in the screenshot below question 2 (from tcp stream 0) my Kali box sent a SYN request

2) Which type of TCP packet (e.g., SYN, SYN/ACK, or ACK) was received from the victim to the Kali in response?

As you can see from the screenshot, my Kali box received an RST,ACK packet from the victim.



Source	Destination	Protocol	Length	Info
192.168.116.128	45.33.32.156	TCP	58	50868 → 443 [SYN] Seq=0 Win=1
45.33.32.156	192.168.116.128	TCP	60	443 → 50868 [RST, ACK] Seq=1

Task 5. SYN Flooding Attack

- Perform a SYN flooding attack using **hping3** against your host from your Kali. The detailed info of Hping3 can be found here: http://linux.die.net/man/8/hping3.

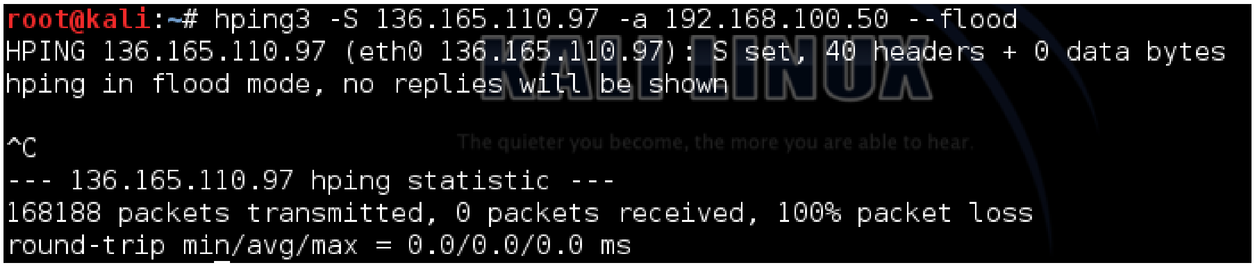
- **Steps**

1) Start Wireshark on the Kali.
2) Create a command using the following template (you should type the command on the command shell. No copying and pasting!):
   a. **Hping3 -S target_ip_addr -a spoofed_ip_addr --flood**

```
-S  --syn       set SYN flag
-a  --spoof     spoofed source address (use a private IP address: 192.168.x.x)
-p  --destportdestination port (default 0)
-i  --interval  wait (uX for X microseconds, for example -i u1000)
    --fast                  alias for -i u10000 (10 packets for second)
    --faster    alias for -i u1000 (100 packets for second)
    --flood     send packets as fast as possible. Don't show replies. (usage: -i flood, or --flood)
```

target_ip_addr: provide the IP address of your host
spoofed_ip_addr: provide a random private IP address

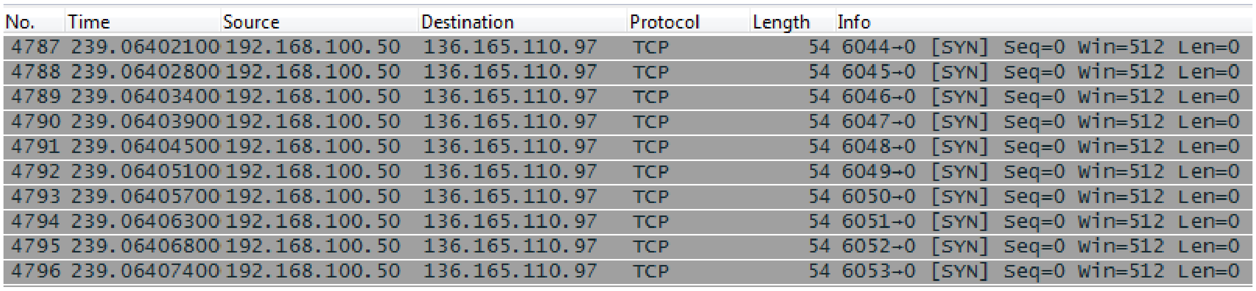
- In the example below, 136.165.110.97 is the victim’s IP address and 192.168.100.50 is the spoofed IP address (a random IP address).



```
root@kali:~# hping3 -S 136.165.110.97 -a 192.168.100.50 --flood
HPING 136.165.110.97 (eth0 136.165.110.97): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown

^C
--- 136.165.110.97 hping statistic ---
168188 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

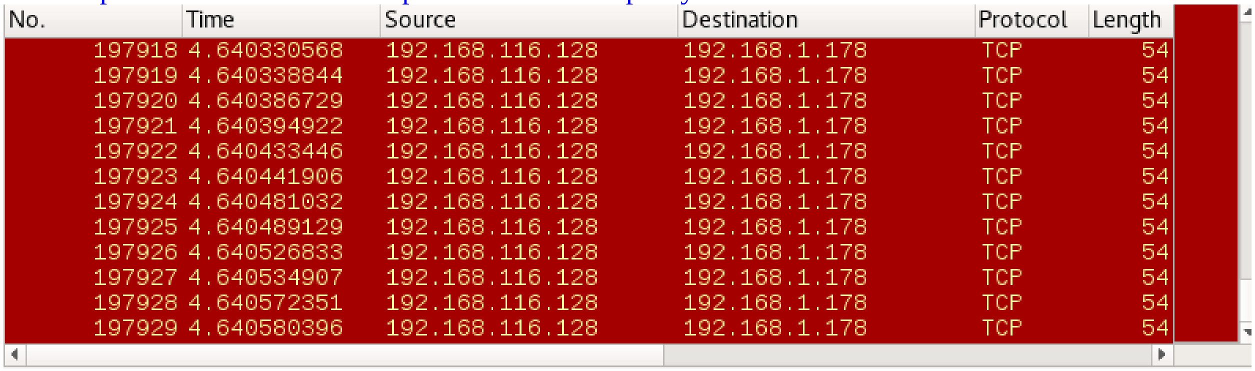
- The following is the packets captured with Wireshark. You should stop the Kali by pressing CNTL+C to prevent the crash of the host.



No.	Time	Source	Destination	Protocol	Length	Info
4787	239.06402100	192.168.100.50	136.165.110.97	TCP	54	6044→0 [SYN] Seq=0 Win=512 Len=0
4788	239.06402800	192.168.100.50	136.165.110.97	TCP	54	6045→0 [SYN] Seq=0 Win=512 Len=0
4789	239.06403400	192.168.100.50	136.165.110.97	TCP	54	6046→0 [SYN] Seq=0 Win=512 Len=0
4790	239.06403900	192.168.100.50	136.165.110.97	TCP	54	6047→0 [SYN] Seq=0 Win=512 Len=0
4791	239.06404500	192.168.100.50	136.165.110.97	TCP	54	6048→0 [SYN] Seq=0 Win=512 Len=0
4792	239.06405100	192.168.100.50	136.165.110.97	TCP	54	6049→0 [SYN] Seq=0 Win=512 Len=0
4793	239.06405700	192.168.100.50	136.165.110.97	TCP	54	6050→0 [SYN] Seq=0 Win=512 Len=0
4794	239.06406300	192.168.100.50	136.165.110.97	TCP	54	6051→0 [SYN] Seq=0 Win=512 Len=0
4795	239.06406800	192.168.100.50	136.165.110.97	TCP	54	6052→0 [SYN] Seq=0 Win=512 Len=0
4796	239.06407400	192.168.100.50	136.165.110.97	TCP	54	6053→0 [SYN] Seq=0 Win=512 Len=0

- Task

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



No.	Time	Source	Destination	Protocol	Length
197918	4.640330568	192.168.116.128	192.168.1.178	TCP	54
197919	4.640338844	192.168.116.128	192.168.1.178	TCP	54
197920	4.640386729	192.168.116.128	192.168.1.178	TCP	54
197921	4.640394922	192.168.116.128	192.168.1.178	TCP	54
197922	4.640433446	192.168.116.128	192.168.1.178	TCP	54
197923	4.640441906	192.168.116.128	192.168.1.178	TCP	54
197924	4.640481032	192.168.116.128	192.168.1.178	TCP	54
197925	4.640489129	192.168.116.128	192.168.1.178	TCP	54
197926	4.640526833	192.168.116.128	192.168.1.178	TCP	54
197927	4.640534907	192.168.116.128	192.168.1.178	TCP	54
197928	4.640572351	192.168.116.128	192.168.1.178	TCP	54
197929	4.640580396	192.168.116.128	192.168.1.178	TCP	54