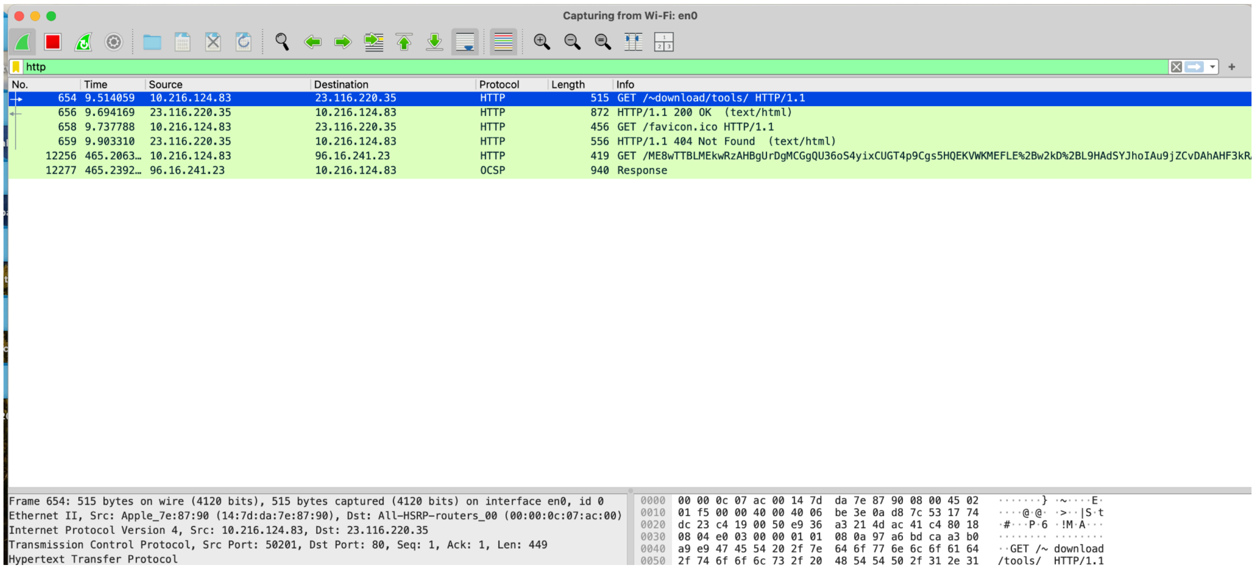
Robert Jones
rtj19

Homework 1

1).

a.



```
http

No.     Time        Source          Destination     Protocol  Length  Info
   654  9.514059    10.216.124.83   23.116.220.35   HTTP         515  GET /~download/tools/ HTTP/1.1
   656  9.694169    23.116.220.35   10.216.124.83   HTTP         872  HTTP/1.1 200 OK  (text/html)
   658  9.737788    10.216.124.83   23.116.220.35   HTTP         456  GET /favicon.ico HTTP/1.1
   659  9.903310    23.116.220.35   10.216.124.83   HTTP         556  HTTP/1.1 404 Not Found  (text/html)
 12256  465.2063…   10.216.124.83   96.16.241.23    HTTP         419  GET /ME8wTTBLMEkwRzAHBgUrDgMCGgQU36oS4yixCUGT4p9Cgs5HQEKVWKMEFLE%2Bw2kD%2BL9HAdSYJhoIAu9jZCvDAhAHF3kR
 12277  465.2392…   96.16.241.23    10.216.124.83   OCSP         940  Response
```

```
Frame 654: 515 bytes on wire (4120 bits), 515 bytes captured (4120 bits) on interface en0, id 0
Ethernet II, Src: Apple_7e:87:90 (14:7d:da:7e:87:90), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00)
Internet Protocol Version 4, Src: 10.216.124.83, Dst: 23.116.220.35
Transmission Control Protocol, Src Port: 50201, Dst Port: 80, Seq: 1, Ack: 1, Len: 449
Hypertext Transfer Protocol
```

```
0000  00 00 0c 07 ac 00 14 7d  da 7e 87 90 08 00 45 02   ·······} ·~····E·
0010  01 f5 00 00 40 00 40 06  be 3e 0a d8 7c 53 17 74   ····@·@· ·>··|S·t
0020  dc 23 c4 19 00 50 e9 36  a3 21 4d ac 41 c4 80 18   ·#···P·6 ·!M·A···
0030  08 04 e0 03 00 00 01 01  08 0a 97 a6 bd ca a3 b0   ········ ········
0040  a9 e9 47 45 54 20 2f 7e  64 6f 77 6e 6c 6f 61 64   ··GET /~ download
0050  2f 74 6f 6f 6c 73 2f 20  48 54 54 50 2f 31 2e 31   /tools/  HTTP/1.1
```

b. Source of MAC header: Apple_7e:87:90
Destination: ALL-HSRP-routers_00 (00:00:0c:07:ac:00)

These represent the MAC addresses of the physical devices sending and receiving the data packet at the data link layer.

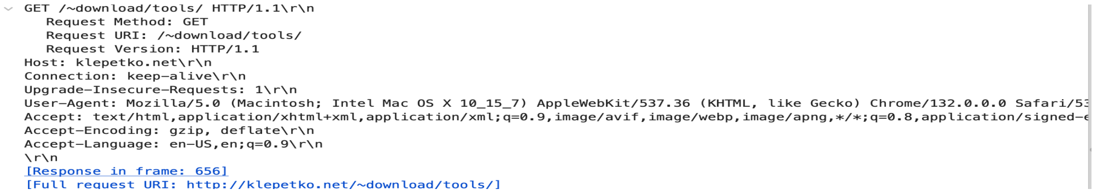
c. Source of IP Header: 10.216.124.83
Destination: 23.116.220.35

These represent the IP address of my device and the IP address of the web server receiving the data at the network layer.

d. Source port of TCP: 50201
Destination port: 80

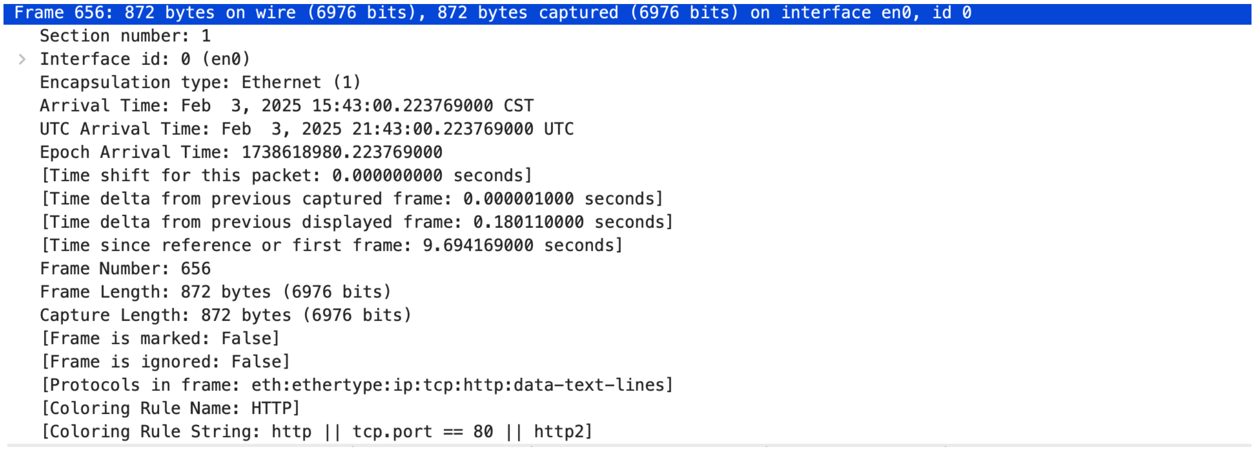
These represent the port number of my device sending data and the port number the web server receiving the data at the transport layer.

e.



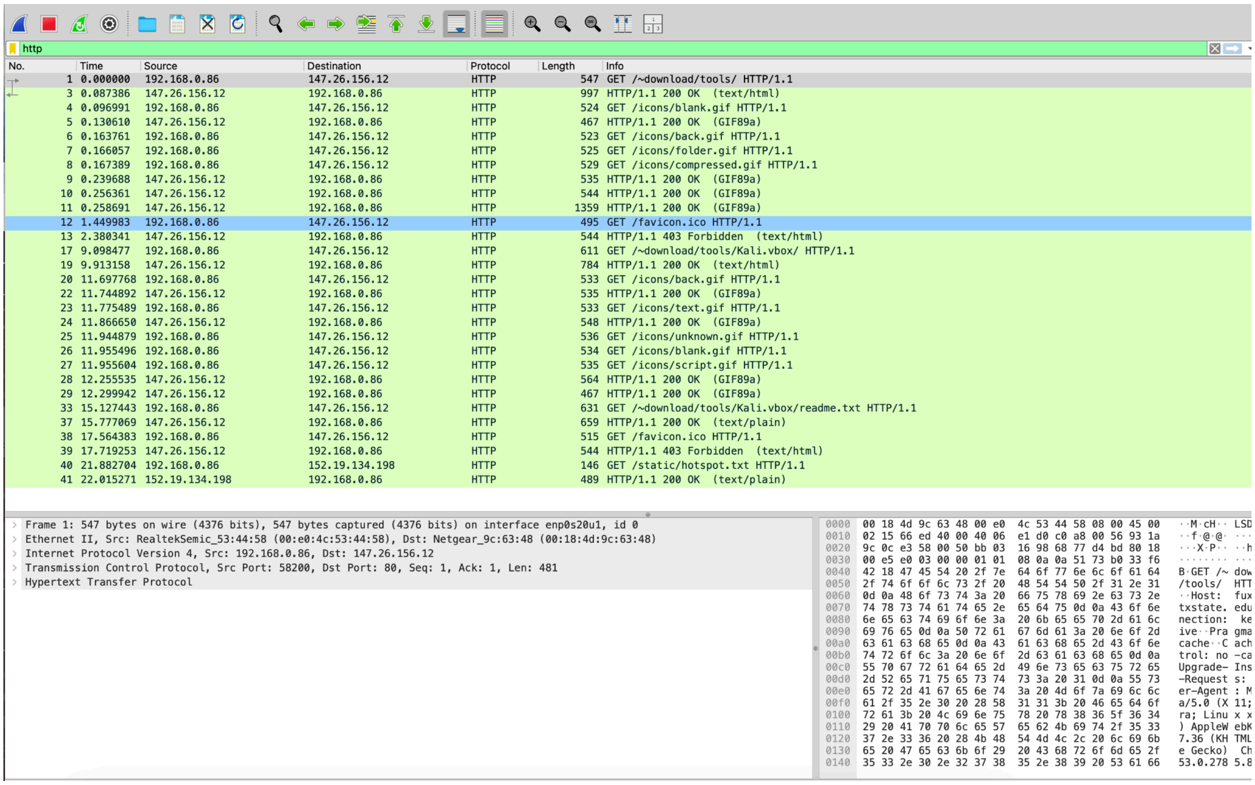
```
⌄ GET /~download/tools/ HTTP/1.1\r\n
    Request Method: GET
    Request URI: /~download/tools/
    Request Version: HTTP/1.1
  Host: klepetko.net\r\n
  Connection: keep-alive\r\n
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari/53
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-e
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: en-US,en;q=0.9\r\n
  \r\n
  [Response in frame: 656]
  [Full request URI: http://klepetko.net/~download/tools/]
```

f.



```
Frame 656: 872 bytes on wire (6976 bits), 872 bytes captured (6976 bits) on interface en0, id 0
    Section number: 1
  > Interface id: 0 (en0)
    Encapsulation type: Ethernet (1)
    Arrival Time: Feb  3, 2025 15:43:00.223769000 CST
    UTC Arrival Time: Feb  3, 2025 21:43:00.223769000 UTC
    Epoch Arrival Time: 1738618980.223769000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.000001000 seconds]
    [Time delta from previous displayed frame: 0.180110000 seconds]
    [Time since reference or first frame: 9.694169000 seconds]
    Frame Number: 656
    Frame Length: 872 bytes (6976 bits)
    Capture Length: 872 bytes (6976 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http:data-text-lines]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
```

2).



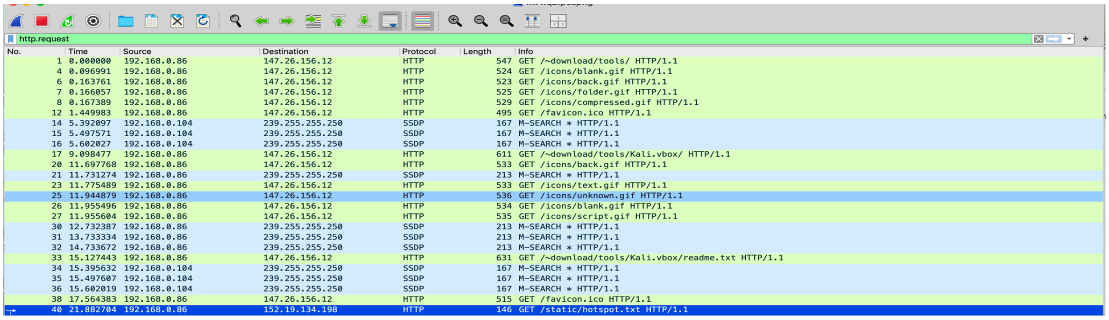
```
No.     Time        Source           Destination      Protocol  Length  Info
      1 0.000000    192.168.0.86     147.26.156.12    HTTP         547  GET /~download/tools/ HTTP/1.1
      3 0.087386    147.26.156.12    192.168.0.86     HTTP         997  HTTP/1.1 200 OK  (text/html)
      4 0.096991    192.168.0.86     147.26.156.12    HTTP         524  GET /icons/blank.gif HTTP/1.1
      5 0.130610    147.26.156.12    192.168.0.86     HTTP         467  HTTP/1.1 200 OK  (GIF89a)
      6 0.163761    192.168.0.86     147.26.156.12    HTTP         523  GET /icons/back.gif HTTP/1.1
      7 0.166057    192.168.0.86     147.26.156.12    HTTP         525  GET /icons/folder.gif HTTP/1.1
      8 0.167389    192.168.0.86     147.26.156.12    HTTP         529  GET /icons/compressed.gif HTTP/1.1
      9 0.239688    147.26.156.12    192.168.0.86     HTTP         535  HTTP/1.1 200 OK  (GIF89a)
     10 0.256361    147.26.156.12    192.168.0.86     HTTP         544  HTTP/1.1 200 OK  (GIF89a)
     11 0.258691    147.26.156.12    192.168.0.86     HTTP        1359  HTTP/1.1 200 OK  (GIF89a)
     12 1.449983    192.168.0.86     147.26.156.12    HTTP         495  GET /favicon.ico HTTP/1.1
     13 2.380341    147.26.156.12    192.168.0.86     HTTP         544  HTTP/1.1 403 Forbidden  (text/html)
     17 9.098477    192.168.0.86     147.26.156.12    HTTP         611  GET /~download/tools/Kali.vbox/ HTTP/1.1
     19 9.913158    147.26.156.12    192.168.0.86     HTTP         784  HTTP/1.1 200 OK  (text/html)
     20 11.697768   192.168.0.86     147.26.156.12    HTTP         533  GET /icons/back.gif HTTP/1.1
     22 11.744892   147.26.156.12    192.168.0.86     HTTP         535  HTTP/1.1 200 OK  (GIF89a)
     23 11.775489   192.168.0.86     147.26.156.12    HTTP         533  GET /icons/text.gif HTTP/1.1
     24 11.866650   147.26.156.12    192.168.0.86     HTTP         548  HTTP/1.1 200 OK  (GIF89a)
     25 11.944879   192.168.0.86     147.26.156.12    HTTP         536  GET /icons/unknown.gif HTTP/1.1
     26 11.955496   192.168.0.86     147.26.156.12    HTTP         534  GET /icons/blank.gif HTTP/1.1
     27 11.955604   192.168.0.86     147.26.156.12    HTTP         535  GET /icons/script.gif HTTP/1.1
     28 12.255535   147.26.156.12    192.168.0.86     HTTP         564  HTTP/1.1 200 OK  (GIF89a)
     29 12.299942   147.26.156.12    192.168.0.86     HTTP         467  HTTP/1.1 200 OK  (GIF89a)
     33 15.127443   192.168.0.86     147.26.156.12    HTTP         631  GET /~download/tools/Kali.vbox/readme.txt HTTP/1.1
     37 15.777069   147.26.156.12    192.168.0.86     HTTP         659  HTTP/1.1 200 OK  (text/plain)
     38 17.564383   192.168.0.86     147.26.156.12    HTTP         515  GET /favicon.ico HTTP/1.1
     39 17.719253   147.26.156.12    192.168.0.86     HTTP         544  HTTP/1.1 403 Forbidden  (text/html)
     40 21.882704   192.168.0.86     152.19.134.198   HTTP         146  GET /static/hotspot.txt HTTP/1.1
     41 22.015271   152.19.134.198   192.168.0.86     HTTP         489  HTTP/1.1 200 OK  (text/plain)
```

```
> Frame 1: 547 bytes on wire (4376 bits), 547 bytes captured (4376 bits) on interface enp0s20u1, id 0
> Ethernet II, Src: RealtekSemic_53:44:58 (00:e0:4c:53:44:58), Dst: Netgear_9c:63:48 (00:18:4d:9c:63:48)
> Internet Protocol Version 4, Src: 192.168.0.86, Dst: 147.26.156.12
> Transmission Control Protocol, Src Port: 58200, Dst Port: 80, Seq: 1, Ack: 1, Len: 481
> Hypertext Transfer Protocol
```

```
0000  00 18 4d 9c 63 48 00 e0  4c 53 44 58 08 00 45 00   ··M·cH·· LSD
0010  02 15 66 ed 40 00 40 06  e1 d0 c0 a8 00 56 93 1a   ··f·@·@· ···
0020  9c 0c e3 58 00 50 bb 03  16 98 68 77 d4 bd 80 18   ···X·P·· ··h
0030  00 e5 e0 03 00 00 01 01  08 0a 0a 51 73 b0 33 f6   ········ ···
0040  42 18 47 45 54 20 2f 7e  64 6f 77 6e 6c 6f 61 64   B·GET /~ dow
0050  2f 74 6f 6f 6c 73 2f 20  48 54 54 50 2f 31 2e 31   /tools/  HTT
0060  0d 0a 48 6f 73 74 3a 20  66 75 78 69 2e 63 73 2e   ··Host:  fux
0070  74 78 73 74 61 74 65 2e  65 64 75 0d 0a 43 6f 6e   txstate. edu
0080  6e 65 63 74 69 6f 6e 3a  20 6b 65 65 70 2d 61 6c   nection:  ke
0090  69 76 65 0d 0a 50 72 61  67 6d 61 3a 20 6e 6f 2d   ive··Pra gma
00a0  63 61 63 68 65 0d 0a 43  61 63 68 65 2d 43 6f 6e   cache··C ach
00b0  74 72 6f 6c 3a 20 6e 6f  2d 63 61 63 68 65 0d 0a   trol: no -ca
00c0  55 70 67 72 61 64 65 2d  49 6e 73 65 63 75 72 65   Upgrade- Ins
00d0  2d 52 65 71 75 65 73 74  73 3a 20 31 0d 0a 55 73   -Request s:
00e0  65 72 2d 41 67 65 6e 74  3a 20 4d 6f 7a 69 6c 6c   er-Agent : M
00f0  61 2f 35 2e 30 20 28 58  31 31 3b 20 46 65 64 6f   a/5.0 (X 11;
0100  72 61 3b 20 4c 69 6e 75  78 20 78 38 36 5f 36 34   ra; Linu x x
0110  29 20 41 70 70 6c 65 57  65 62 4b 69 74 2f 35 33   ) AppleW ebK
0120  37 2e 33 36 20 28 4b 48  54 4d 4c 2c 20 6c 69 6b   7.36 (KH TML
0130  65 20 47 65 63 6b 6f 29  20 43 68 72 6f 6d 65 2f   e Gecko)  Ch
0140  35 33 2e 30 2e 32 37 38  35 2e 38 39 20 53 61 66   53.0.278 5.8
```

a. 147.26.156.12

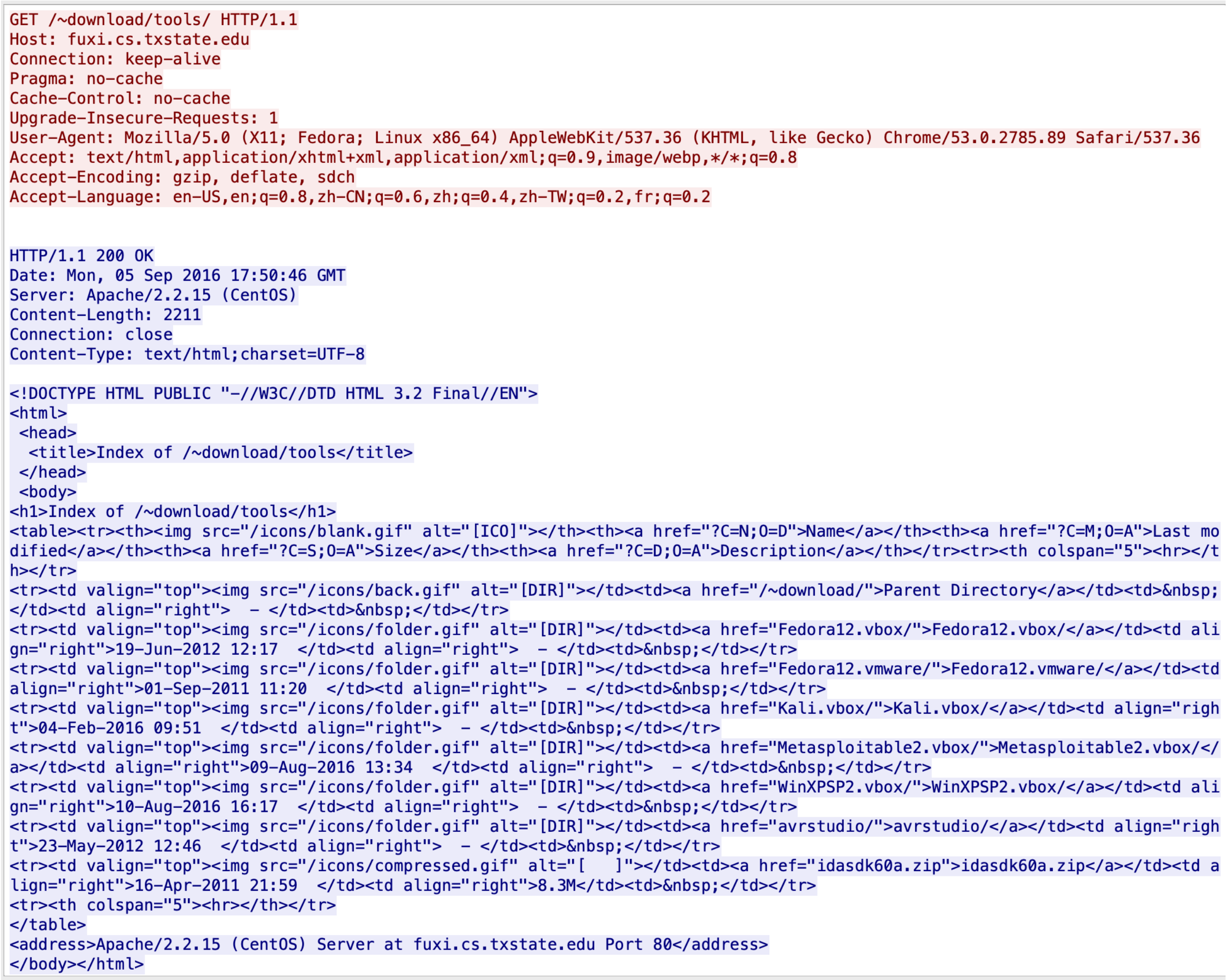
b. All green GET rows



http.request

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.86	147.26.156.12	HTTP	547	GET /~download/tools/ HTTP/1.1
4	0.096991	192.168.0.86	147.26.156.12	HTTP	524	GET /icons/blank.gif HTTP/1.1
6	0.163761	192.168.0.86	147.26.156.12	HTTP	523	GET /icons/back.gif HTTP/1.1
7	0.166057	192.168.0.86	147.26.156.12	HTTP	525	GET /icons/folder.gif HTTP/1.1
8	0.167389	192.168.0.86	147.26.156.12	HTTP	529	GET /icons/compressed.gif HTTP/1.1
12	1.449983	192.168.0.86	147.26.156.12	HTTP	495	GET /favicon.ico HTTP/1.1
14	5.392097	192.168.0.104	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
15	5.497571	192.168.0.104	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
16	5.602027	192.168.0.104	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
17	9.098477	192.168.0.86	147.26.156.12	HTTP	611	GET /~download/tools/Kali.vbox/ HTTP/1.1
20	11.697768	192.168.0.86	147.26.156.12	HTTP	533	GET /icons/back.gif HTTP/1.1
21	11.731274	192.168.0.86	239.255.255.250	SSDP	213	M-SEARCH * HTTP/1.1
23	11.775489	192.168.0.86	147.26.156.12	HTTP	533	GET /icons/text.gif HTTP/1.1
25	11.944879	192.168.0.86	147.26.156.12	HTTP	536	GET /icons/unknown.gif HTTP/1.1
26	11.955496	192.168.0.86	147.26.156.12	HTTP	534	GET /icons/blank.gif HTTP/1.1
27	11.955604	192.168.0.86	147.26.156.12	HTTP	535	GET /icons/script.gif HTTP/1.1
30	12.732387	192.168.0.86	239.255.255.250	SSDP	213	M-SEARCH * HTTP/1.1
31	13.733334	192.168.0.86	239.255.255.250	SSDP	213	M-SEARCH * HTTP/1.1
32	14.733672	192.168.0.86	239.255.255.250	SSDP	213	M-SEARCH * HTTP/1.1
33	15.127443	192.168.0.86	147.26.156.12	HTTP	631	GET /~download/tools/Kali.vbox/readme.txt HTTP/1.1
34	15.395632	192.168.0.104	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
35	15.497607	192.168.0.104	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
36	15.602019	192.168.0.104	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
38	17.564383	192.168.0.86	147.26.156.12	HTTP	515	GET /favicon.ico HTTP/1.1
40	21.882704	192.168.0.86	152.19.134.198	HTTP	146	GET /static/hotspot.txt HTTP/1.1

c.

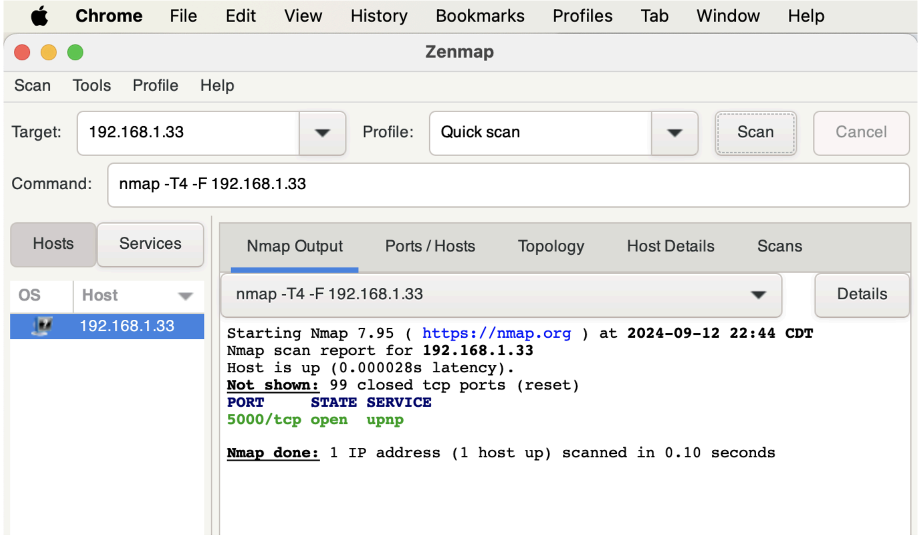


```
GET /~download/tools/ HTTP/1.1
Host: fuxi.cs.txstate.edu
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Fedora; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.89 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate, sdch
Accept-Language: en-US,en;q=0.8,zh-CN;q=0.6,zh;q=0.4,zh-TW;q=0.2,fr;q=0.2


HTTP/1.1 200 OK
Date: Mon, 05 Sep 2016 17:50:46 GMT
Server: Apache/2.2.15 (CentOS)
Content-Length: 2211
Connection: close
Content-Type: text/html;charset=UTF-8

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
 <head>
  <title>Index of /~download/tools</title>
 </head>
 <body>
<h1>Index of /~download/tools</h1>
<table><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th><a href="?C=M;O=A">Last mo
dified</a></th><th><a href="?C=S;O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr><tr><th colspan="5"><hr></t
h></tr>
<tr><td valign="top"><img src="/icons/back.gif" alt="[DIR]"></td><td><a href="/~download/">Parent Directory</a></td><td>&nbsp;
</td><td align="right">  - </td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="Fedora12.vbox/">Fedora12.vbox/</a></td><td ali
gn="right">19-Jun-2012 12:17  </td><td align="right">  - </td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="Fedora12.vmware/">Fedora12.vmware/</a></td><td
align="right">01-Sep-2011 11:20  </td><td align="right">  - </td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="Kali.vbox/">Kali.vbox/</a></td><td align="righ
t">04-Feb-2016 09:51  </td><td align="right">  - </td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="Metasploitable2.vbox/">Metasploitable2.vbox/</
a></td><td align="right">09-Aug-2016 13:34  </td><td align="right">  - </td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="WinXPSP2.vbox/">WinXPSP2.vbox/</a></td><td ali
gn="right">10-Aug-2016 16:17  </td><td align="right">  - </td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="avrstudio/">avrstudio/</a></td><td align="righ
t">23-May-2012 12:46  </td><td align="right">  - </td><td>&nbsp;</td></tr>
<tr><td valign="top"><img src="/icons/compressed.gif" alt="[   ]"></td><td><a href="idasdk60a.zip">idasdk60a.zip</a></td><td a
lign="right">16-Apr-2011 21:59  </td><td align="right">8.3M</td><td>&nbsp;</td></tr>
<tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.2.15 (CentOS) Server at fuxi.cs.txstate.edu Port 80</address>
</body></html>
```

3).

192.168.1.33

a. Quick Scan



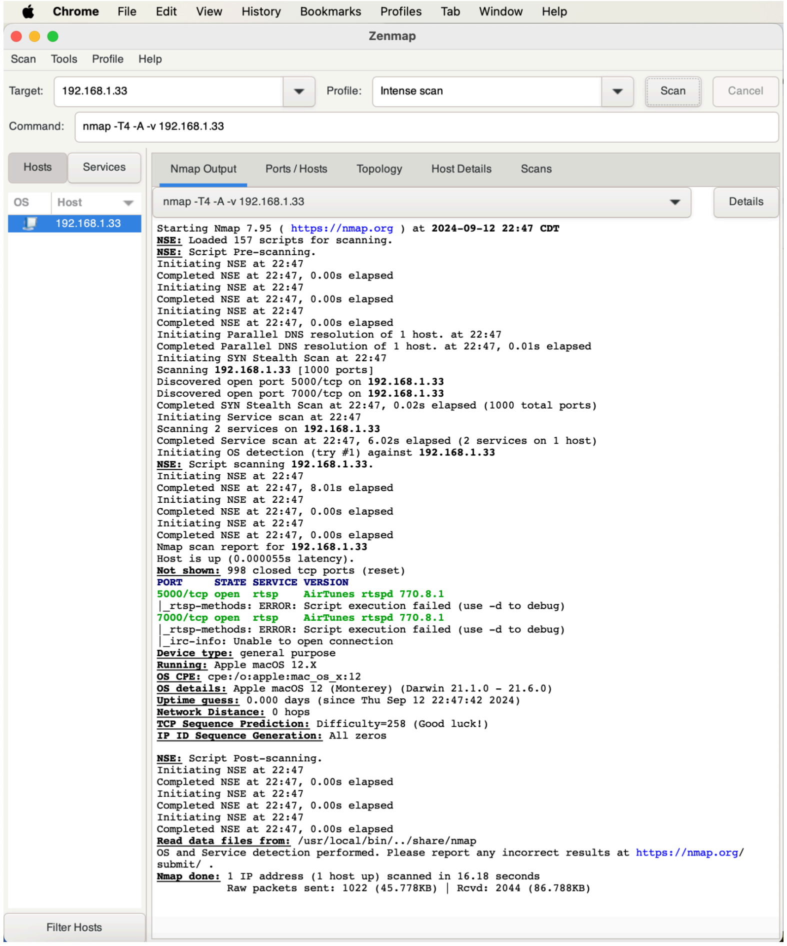
Target: 192.168.1.33

Profile: Quick scan

Command: nmap -T4 -F 192.168.1.33

```
nmap -T4 -F 192.168.1.33

Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-12 22:44 CDT
Nmap scan report for 192.168.1.33
Host is up (0.000028s latency).
Not shown: 99 closed tcp ports (reset)
PORT     STATE SERVICE
5000/tcp open  upnp

Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
```

b. Intense scan



Target: 192.168.1.33

Profile: Intense scan

Command: nmap -T4 -A -v 192.168.1.33

```
nmap -T4 -A -v 192.168.1.33

Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-12 22:47 CDT
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 22:47
Completed NSE at 22:47, 0.00s elapsed
Initiating NSE at 22:47
Completed NSE at 22:47, 0.00s elapsed
Initiating NSE at 22:47
Completed NSE at 22:47, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 22:47
Completed Parallel DNS resolution of 1 host. at 22:47, 0.01s elapsed
Initiating SYN Stealth Scan at 22:47
Scanning 192.168.1.33 [1000 ports]
Discovered open port 5000/tcp on 192.168.1.33
Discovered open port 7000/tcp on 192.168.1.33
Completed SYN Stealth Scan at 22:47, 0.02s elapsed (1000 total ports)
Initiating Service scan at 22:47
Scanning 2 services on 192.168.1.33
Completed Service scan at 22:47, 6.02s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against 192.168.1.33
NSE: Script scanning 192.168.1.33.
Initiating NSE at 22:47
Completed NSE at 22:47, 8.01s elapsed
Initiating NSE at 22:47
Completed NSE at 22:47, 0.00s elapsed
Initiating NSE at 22:47
Completed NSE at 22:47, 0.00s elapsed
Nmap scan report for 192.168.1.33
Host is up (0.000055s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
5000/tcp open  rtsp    AirTunes rtspd 770.8.1
|_rtsp-methods: ERROR: Script execution failed (use -d to debug)
7000/tcp open  rtsp    AirTunes rtspd 770.8.1
|_rtsp-methods: ERROR: Script execution failed (use -d to debug)
|_irc-info: Unable to open connection
Device type: general purpose
Running: Apple macOS 12.X
OS CPE: cpe:/o:apple:mac_os_x:12
OS details: Apple macOS 12 (Monterey) (Darwin 21.1.0 - 21.6.0)
Uptime guess: 0.000 days (since Thu Sep 12 22:47:42 2024)
Network Distance: 0 hops
TCP Sequence Prediction: Difficulty=258 (Good luck!)
IP ID Sequence Generation: All zeros

NSE: Script Post-scanning.
Initiating NSE at 22:47
Completed NSE at 22:47, 0.00s elapsed
Initiating NSE at 22:47
Completed NSE at 22:47, 0.00s elapsed
Initiating NSE at 22:47
Completed NSE at 22:47, 0.00s elapsed
Read data files from: /usr/local/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.18 seconds
           Raw packets sent: 1022 (45.778KB) | Rcvd: 2044 (86.788KB)
```

c. Port 7000 was found in the intense scan but not the quick scan.

4).

a. Availability: Limit access where only authorized staff have necessary privileges.
b. Confidentiality: Use a system like wireshark to detect discrepancies in your IP activity.
c. Integrity: Apply access control where few authorized personnel have access to the checks. With two different people processing the check amount due to hours, and someone checking the amount when paying out to have 2 step verification.
d. Confidentiality: The assignments can be handled on a source like github where the professor can allow sub repositories for each student that only the professor and student have access to.
e. Availability: Linda can regularly back up her system to prevent loss if it crashes.
f. Integrity: Having a passkey for the signature process like in the FASFA system could prevent unauthorized signing.
g. Confidentiality: Use encryption to protect data during transport
h. Integrity: Implement transaction verification using 2 step-varification