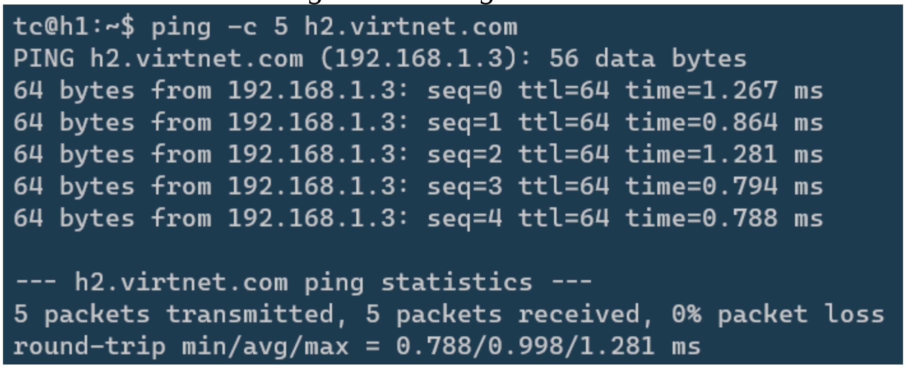
CS4150 Computer Networks Laboratory – Assignment 2

Subhash S – 111801042
Computer Science and Engineering, IIT Palakkad

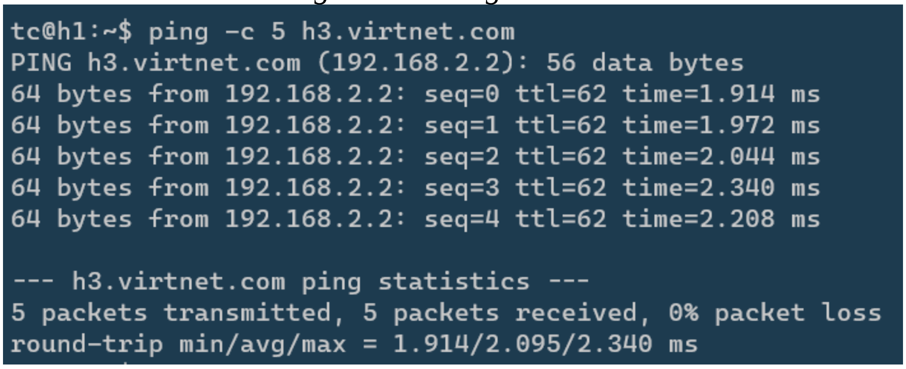
(a) Connect to host h1. Ensure that you are able to ping x.virtnet.com for all x in {h2, h3, h4, h5}. Send 5 ping packets to each of these hosts and report the respective average round-trip time.

Figure 1: h2 avg: 0.998ms



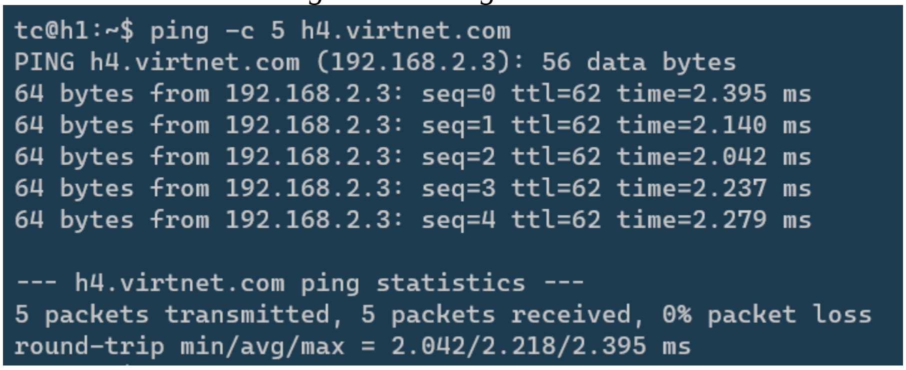
```
tc@h1:~$ ping -c 5 h2.virtnet.com
PING h2.virtnet.com (192.168.1.3): 56 data bytes
64 bytes from 192.168.1.3: seq=0 ttl=64 time=1.267 ms
64 bytes from 192.168.1.3: seq=1 ttl=64 time=0.864 ms
64 bytes from 192.168.1.3: seq=2 ttl=64 time=1.281 ms
64 bytes from 192.168.1.3: seq=3 ttl=64 time=0.794 ms
64 bytes from 192.168.1.3: seq=4 ttl=64 time=0.788 ms

--- h2.virtnet.com ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.788/0.998/1.281 ms
```

Figure 2: h3 avg 2.095ms



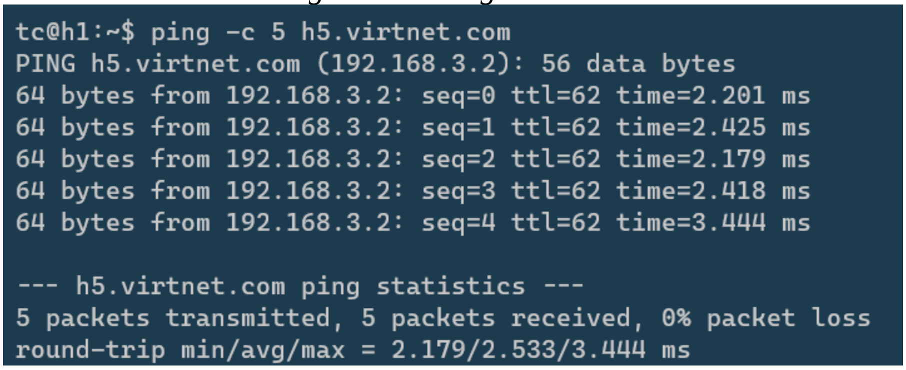
```
tc@h1:~$ ping -c 5 h3.virtnet.com
PING h3.virtnet.com (192.168.2.2): 56 data bytes
64 bytes from 192.168.2.2: seq=0 ttl=62 time=1.914 ms
64 bytes from 192.168.2.2: seq=1 ttl=62 time=1.972 ms
64 bytes from 192.168.2.2: seq=2 ttl=62 time=2.044 ms
64 bytes from 192.168.2.2: seq=3 ttl=62 time=2.340 ms
64 bytes from 192.168.2.2: seq=4 ttl=62 time=2.208 ms

--- h3.virtnet.com ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.914/2.095/2.340 ms
```

Figure 3: h4 avg: 2.218ms



```
tc@h1:~$ ping -c 5 h4.virtnet.com
PING h4.virtnet.com (192.168.2.3): 56 data bytes
64 bytes from 192.168.2.3: seq=0 ttl=62 time=2.395 ms
64 bytes from 192.168.2.3: seq=1 ttl=62 time=2.140 ms
64 bytes from 192.168.2.3: seq=2 ttl=62 time=2.042 ms
64 bytes from 192.168.2.3: seq=3 ttl=62 time=2.237 ms
64 bytes from 192.168.2.3: seq=4 ttl=62 time=2.279 ms

--- h4.virtnet.com ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 2.042/2.218/2.395 ms
```

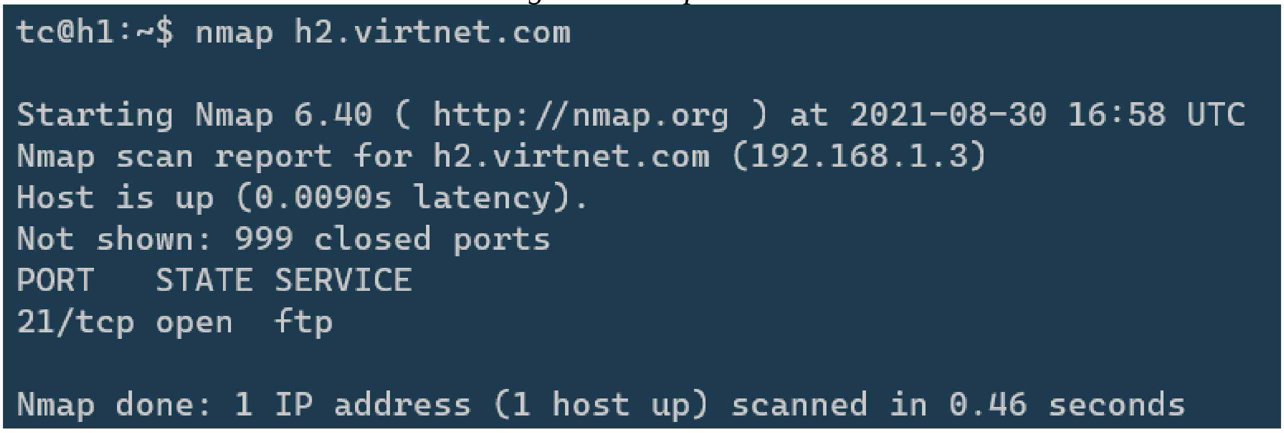
Figure 4: h5 avg: 2.533ms



```
tc@h1:~$ ping -c 5 h5.virtnet.com
PING h5.virtnet.com (192.168.3.2): 56 data bytes
64 bytes from 192.168.3.2: seq=0 ttl=62 time=2.201 ms
64 bytes from 192.168.3.2: seq=1 ttl=62 time=2.425 ms
64 bytes from 192.168.3.2: seq=2 ttl=62 time=2.179 ms
64 bytes from 192.168.3.2: seq=3 ttl=62 time=2.418 ms
64 bytes from 192.168.3.2: seq=4 ttl=62 time=3.444 ms

--- h5.virtnet.com ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 2.179/2.533/3.444 ms
```

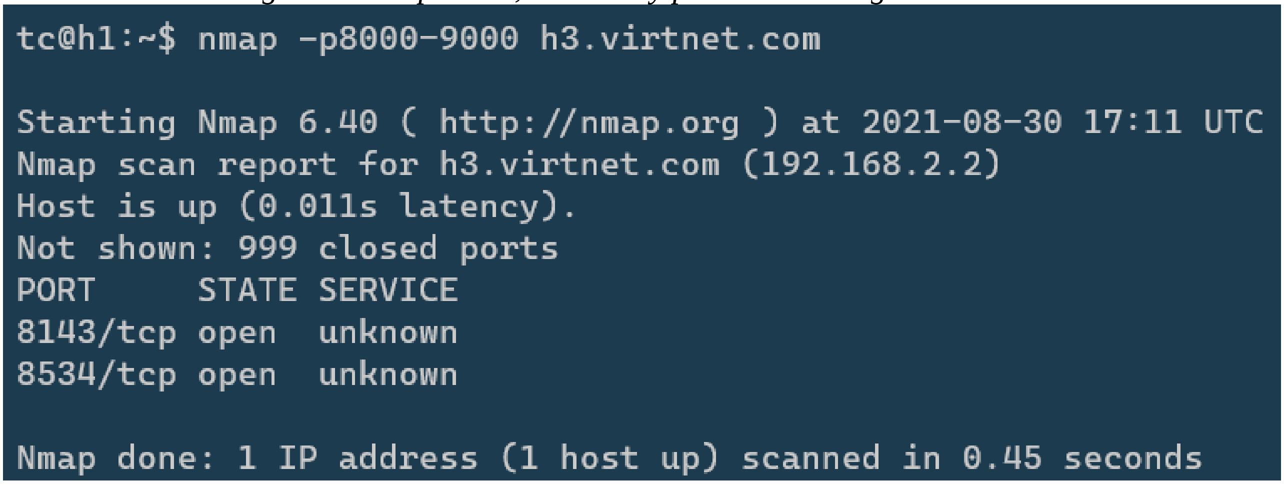
(b) ***Host A is running a FTP server, whereas Host B is simultaneously running two HTTP servers on port numbers in the range 8000 to 9000. Identify hosts A and B. What are the incoming ports of the HTTP servers on host B?***

Figure 5: nmap on h2



```
tc@h1:~$ nmap h2.virtnet.com

Starting Nmap 6.40 ( http://nmap.org ) at 2021-08-30 16:58 UTC
Nmap scan report for h2.virtnet.com (192.168.1.3)
Host is up (0.0090s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
21/tcp open  ftp

Nmap done: 1 IP address (1 host up) scanned in 0.46 seconds
```

Figure 6: nmap on h3, scans only ports in the range 8000-9000



```
tc@h1:~$ nmap -p8000-9000 h3.virtnet.com

Starting Nmap 6.40 ( http://nmap.org ) at 2021-08-30 17:11 UTC
Nmap scan report for h3.virtnet.com (192.168.2.2)
Host is up (0.011s latency).
Not shown: 999 closed ports
PORT     STATE SERVICE
8143/tcp open  unknown
8534/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.45 seconds
```

1. From Figure 5 we can see that the host ***h2*** is running a FTP server on port *21*.

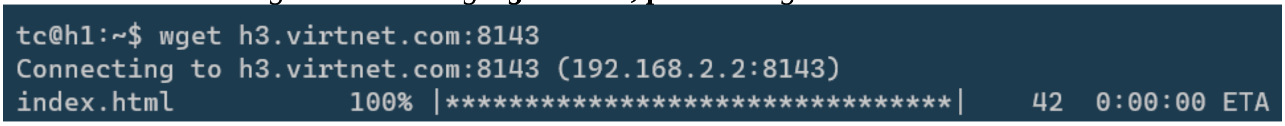
2. From Figure 6 we can see that the host ***h3*** is running the HTTP servers on the TCP ports ***8143*** and ***8534.***

(c) Let us call the HTTP servers running on host B as S1 and S2. On each of these servers there are two text files (within some directory). Download these files. Each of these files contains one half of the password needed to log into the FTP server on host A. Write down this password.

1. From Figure 6 we can observe that:
   1.1. The host **B** is **h3**.
   1.2. The server **S1** is running on port **8143**.
   1.3. The server **S2** is running on port **8534**.

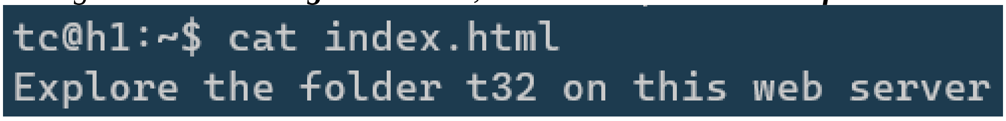
2. Extract password from **S1**

*Figure 7: Running **wget on h3, port 8143** gives us **index.html**.*



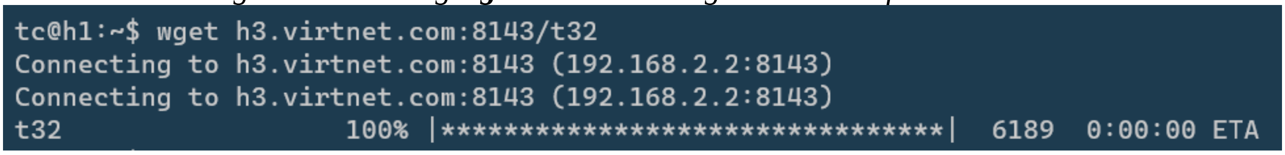
```
tc@h1:~$ wget h3.virtnet.com:8143
Connecting to h3.virtnet.com:8143 (192.168.2.2:8143)
index.html           100% |********************************|    42  0:00:00 ETA
```

*Figure 8: On **reading index.html**, it hints us to look into the **folder t32**.*



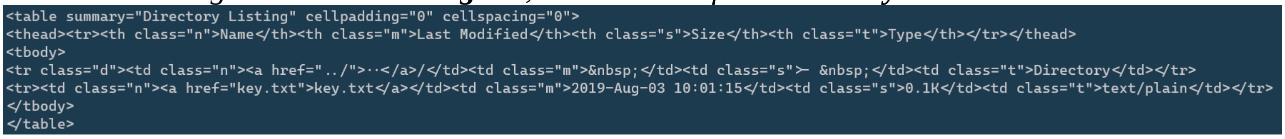
```
tc@h1:~$ cat index.html
Explore the folder t32 on this web server
```

*Figure 9: Running **wget on route /t32** gives another file named **t32**.*



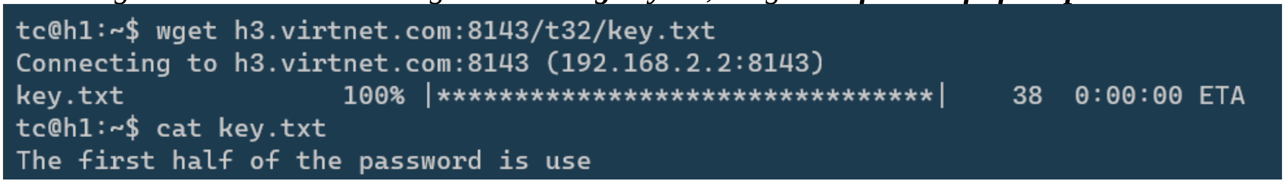
```
tc@h1:~$ wget h3.virtnet.com:8143/t32
Connecting to h3.virtnet.com:8143 (192.168.2.2:8143)
Connecting to h3.virtnet.com:8143 (192.168.2.2:8143)
t32                  100% |********************************|  6189  0:00:00 ETA
```

*Figure 10: On **reading t32**, we can see a file named **key.txt** in the table.*



```
<table summary="Directory Listing" cellpadding="0" cellspacing="0">
<thead><tr><th class="n">Name</th><th class="m">Last Modified</th><th class="s">Size</th><th class="t">Type</th></tr></thead>
<tbody>
<tr class="d"><td class="n"><a href="../">..</a>/</td><td class="m">&nbsp;</td><td class="s">- &nbsp;</td><td class="t">Directory</td></tr>
<tr><td class="n"><a href="key.txt">key.txt</a></td><td class="m">2019-Aug-03 10:01:15</td><td class="s">0.1K</td><td class="t">text/plain</td></tr>
</tbody>
</table>
```

*Figure 11: On downloading and **reading key.txt**, we get the **first half of the password**.*

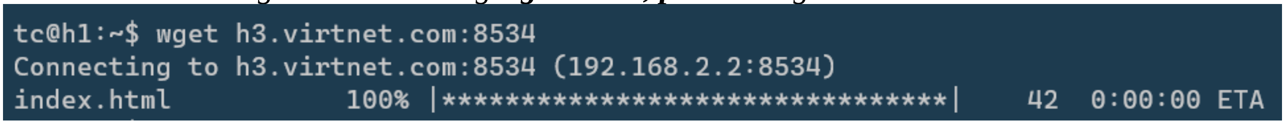


```
tc@h1:~$ wget h3.virtnet.com:8143/t32/key.txt
Connecting to h3.virtnet.com:8143 (192.168.2.2:8143)
key.txt              100% |********************************|    38  0:00:00 ETA
tc@h1:~$ cat key.txt
The first half of the password is use
```

*The first half of the password is **use** as shown in Figure 11.*

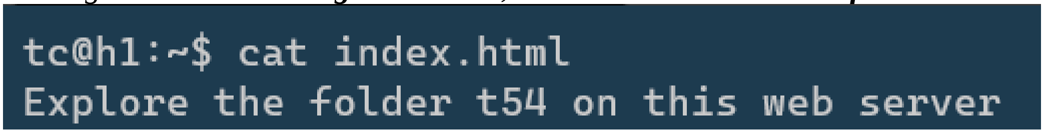
3. Extract password from **S2**

*Figure 12: Running **wget on h3, port 8534** gives us **index.html**.*



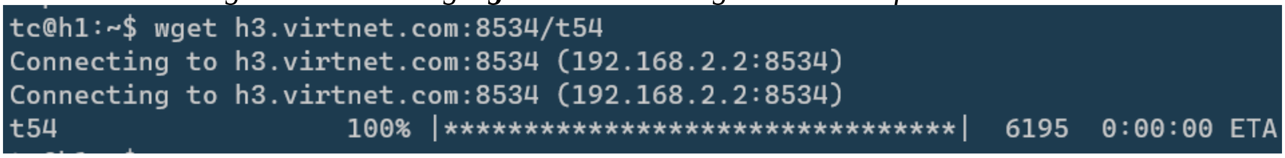
```
tc@h1:~$ wget h3.virtnet.com:8534
Connecting to h3.virtnet.com:8534 (192.168.2.2:8534)
index.html           100% |********************************|    42  0:00:00 ETA
```

*Figure 13: On **reading index.html**, it hints us to look into the **folder t54**.*



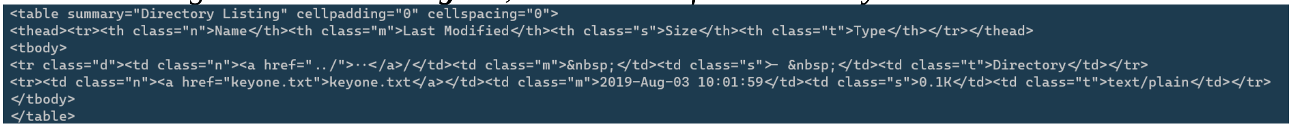
```
tc@h1:~$ cat index.html
Explore the folder t54 on this web server
```

*Figure 14: Running **wget on route /t32** gives another file named **t54**.*



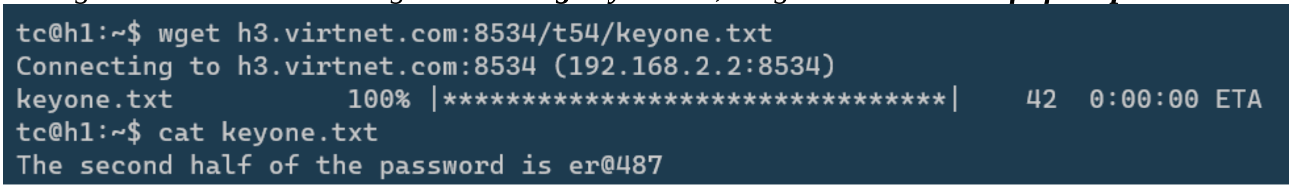
```
tc@h1:~$ wget h3.virtnet.com:8534/t54
Connecting to h3.virtnet.com:8534 (192.168.2.2:8534)
Connecting to h3.virtnet.com:8534 (192.168.2.2:8534)
t54                  100% |********************************|  6195  0:00:00 ETA
```

*Figure 15: On **reading t54**, we can see a file named **keyone.txt** in the table.*



```
<table summary="Directory Listing" cellpadding="0" cellspacing="0">
<thead><tr><th class="n">Name</th><th class="m">Last Modified</th><th class="s">Size</th><th class="t">Type</th></tr></thead>
<tbody>
<tr class="d"><td class="n"><a href="../">..</a>/</td><td class="m">&nbsp;</td><td class="s">- &nbsp;</td><td class="t">Directory</td></tr>
<tr><td class="n"><a href="keyone.txt">keyone.txt</a></td><td class="m">2019-Aug-03 10:01:59</td><td class="s">0.1K</td><td class="t">text/plain</td></tr>
</tbody>
</table>
```

*Figure 16: On downloading and **reading keyone.txt**, we get the **second half of the password**.*



```
tc@h1:~$ wget h3.virtnet.com:8534/t54/keyone.txt
Connecting to h3.virtnet.com:8534 (192.168.2.2:8534)
keyone.txt           100% |********************************|    42  0:00:00 ETA
tc@h1:~$ cat keyone.txt
The second half of the password is er@487
```

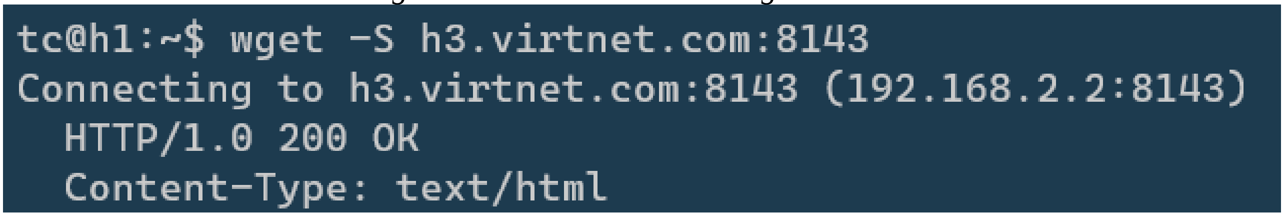
*The second half of the password is **er@487** as shown in Figure 16.*

From the above two results,

Password for FTP server running on host ***h1*** is ***useer@487***.

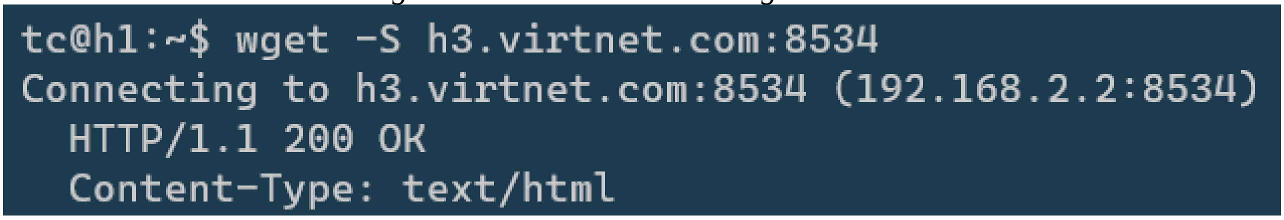
(d) One of the HTTP server on host B runs HTTP/1.0 and the other runs HTTP/1.1. Match the port number of the servers to corresponding HTTP versions.

*Figure 17: Port **8143** is running **HTTP/1.0***



```
tc@h1:~$ wget -S h3.virtnet.com:8143
Connecting to h3.virtnet.com:8143 (192.168.2.2:8143)
  HTTP/1.0 200 OK
  Content-Type: text/html
```

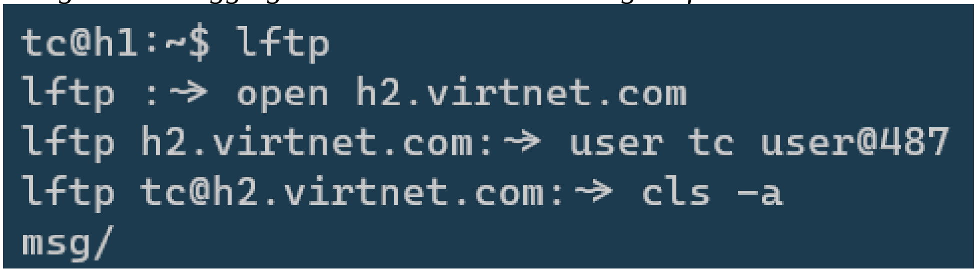
*Figure 18: Port **8534** is running **HTTP/1.1***



```
tc@h1:~$ wget -S h3.virtnet.com:8534
Connecting to h3.virtnet.com:8534 (192.168.2.2:8534)
  HTTP/1.1 200 OK
  Content-Type: text/html
```

(e) Using command lftp, FTP into host A using username \tc" and the password obtained in step (c). There is a file called "sol.txt" (within a directory) on this machine. Download it and look at its contents. This file contains the password for user "tc" on host h5. Write down this password.

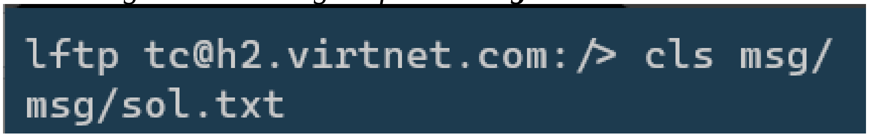
Figure 19: Logging into FTP server and listing all files and directories



```
tc@h1:~$ lftp
lftp :~> open h2.virtnet.com
lftp h2.virtnet.com:~> user tc user@487
lftp tc@h2.virtnet.com:~> cls -a
msg/
```

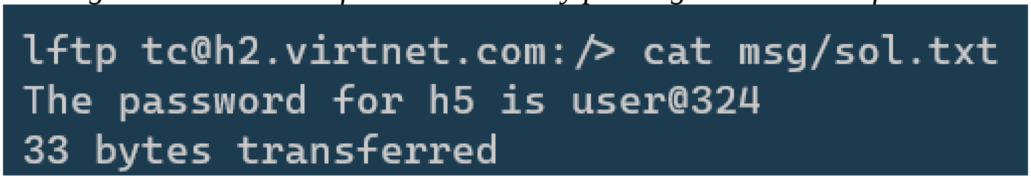
From the above figure,
We can see that there is a directory named ***msg/*** on the FTP server.

*Figure 20: Listing all files in **msg/** reveals the **sol.txt***



```
lftp tc@h2.virtnet.com:/> cls msg/
msg/sol.txt
```

Figure 21: Password for h5 obtained by printing the contents of sol.txt

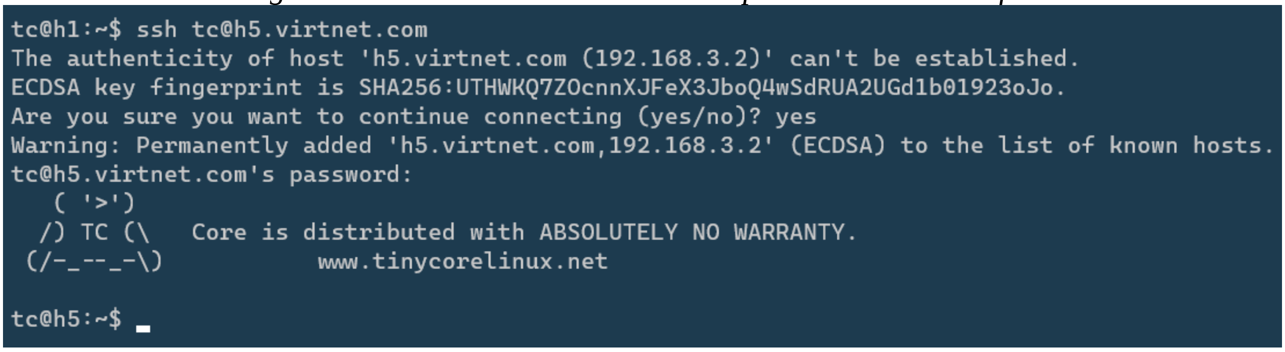


```
lftp tc@h2.virtnet.com:/> cat msg/sol.txt
The password for h5 is user@324
33 bytes transferred
```

From the above figure,
Password for the host ***h5*** is ***user@324***

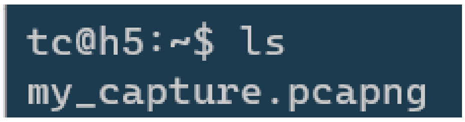
(f) SSH into host h5 using username "tc" and the password obtained in the previous step. There is file with the extension ".pcapng" in the home directory of user "tc". What is the name of this file?

Figure 22: SSH into h5 with the above password is successful.



```
tc@h1:~$ ssh tc@h5.virtnet.com
The authenticity of host 'h5.virtnet.com (192.168.3.2)' can't be established.
ECDSA key fingerprint is SHA256:UTHWKQ7ZOcnnXJFeX3JboQ4wSdRUA2UGd1b01923oJo.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'h5.virtnet.com,192.168.3.2' (ECDSA) to the list of known hosts.
tc@h5.virtnet.com's password:
   ( '>')
  /) TC (\   Core is distributed with ABSOLUTELY NO WARRANTY.
 (/-_--_-\)           www.tinycorelinux.net

tc@h5:~$
```

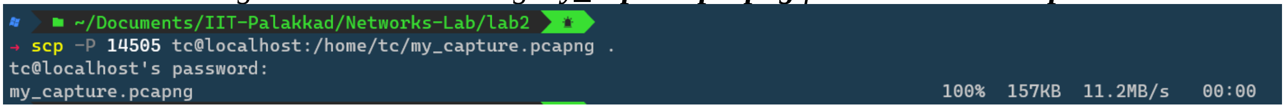
The name of the packet capture file is ***my_capture.pcapng.***



```
tc@h5:~$ ls
my_capture.pcapng
```

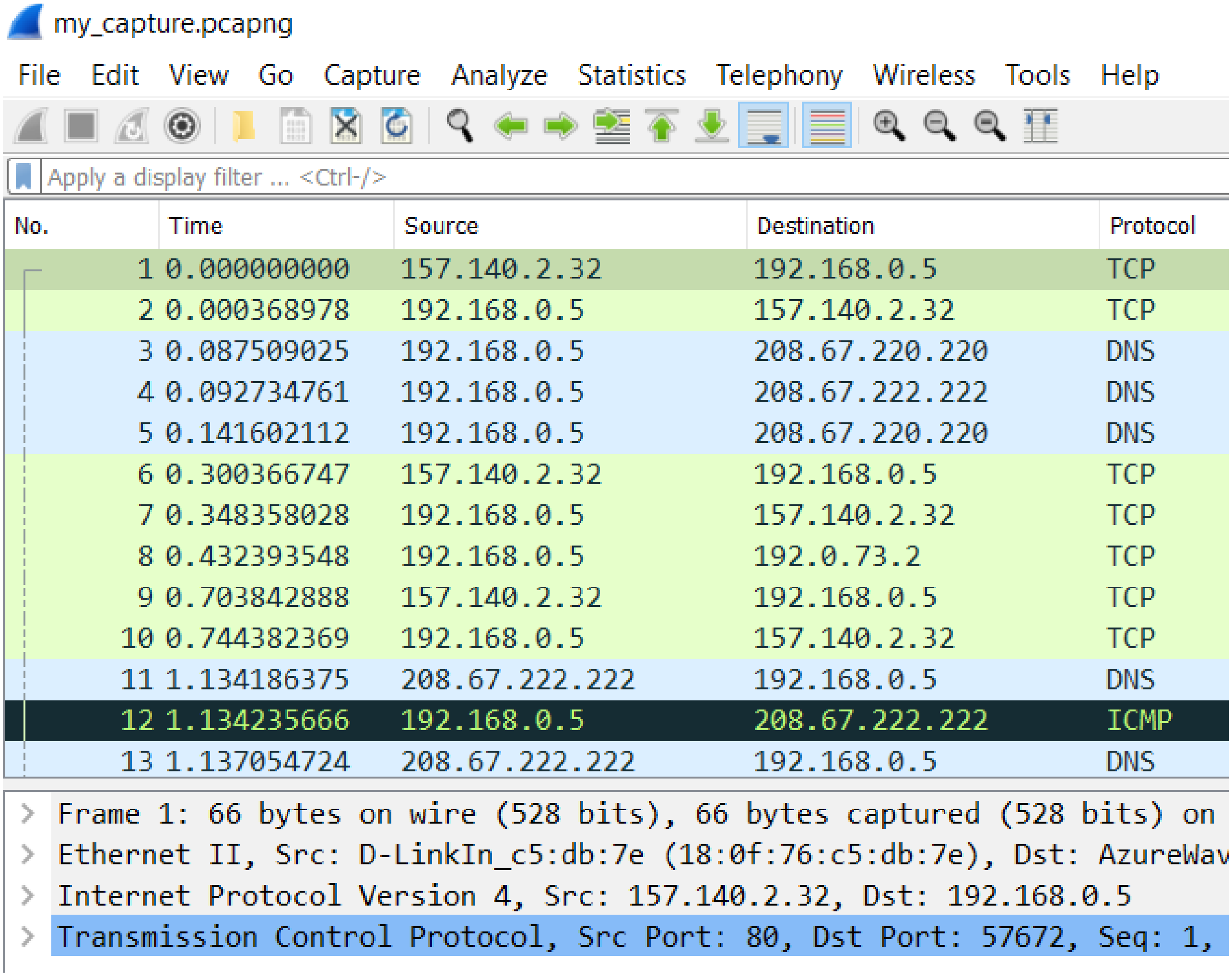
(g) Download this file to your physical host machine and open it with wireshark.

Figure 23: Downloading **my_capture.pcapng** from host **h5** via *scp*.



```
~/Documents/IIT-Palakkad/Networks-Lab/lab2
→ scp -P 14505 tc@localhost:/home/tc/my_capture.pcapng .
tc@localhost's password:
my_capture.pcapng                                                    100%  157KB  11.2MB/s   00:00
```

Figure 24: Opening **my_capture.pcapng** on **wireshark.**



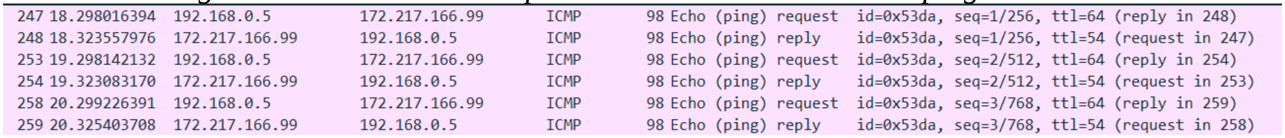
my_capture.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol
1	0.000000000	157.140.2.32	192.168.0.5	TCP
2	0.000368978	192.168.0.5	157.140.2.32	TCP
3	0.087509025	192.168.0.5	208.67.220.220	DNS
4	0.092734761	192.168.0.5	208.67.222.222	DNS
5	0.141602112	192.168.0.5	208.67.220.220	DNS
6	0.300366747	157.140.2.32	192.168.0.5	TCP
7	0.348358028	192.168.0.5	157.140.2.32	TCP
8	0.432393548	192.168.0.5	192.0.73.2	TCP
9	0.703842888	157.140.2.32	192.168.0.5	TCP
10	0.744382369	192.168.0.5	157.140.2.32	TCP
11	1.134186375	208.67.222.222	192.168.0.5	DNS
12	1.134235666	192.168.0.5	208.67.222.222	ICMP
13	1.137054724	208.67.222.222	192.168.0.5	DNS

```
> Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on
> Ethernet II, Src: D-LinkIn_c5:db:7e (18:0f:76:c5:db:7e), Dst: AzureWav
> Internet Protocol Version 4, Src: 157.140.2.32, Dst: 192.168.0.5
> Transmission Control Protocol, Src Port: 80, Dst Port: 57672, Seq: 1,
```

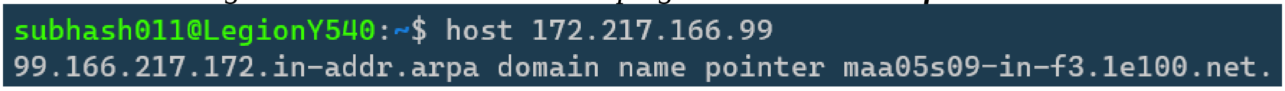
(h) ***What you now see in wireshark is a sample packet capture. During the capture, a website was pinged, which host was pinged? What was the IP returned after DNS resolution? How many ping response packets were received? What was the minimum response time for these packets?***

Figure 25: ***ICMP Protocol*** *proves that this was due to the ping command*



```
247 18.298016394  192.168.0.5          172.217.166.99       ICMP        98 Echo (ping) request  id=0x53da, seq=1/256, ttl=64 (reply in 248)
248 18.323557976  172.217.166.99       192.168.0.5          ICMP        98 Echo (ping) reply    id=0x53da, seq=1/256, ttl=54 (request in 247)
253 19.298142132  192.168.0.5          172.217.166.99       ICMP        98 Echo (ping) request  id=0x53da, seq=2/512, ttl=64 (reply in 254)
254 19.323083170  172.217.166.99       192.168.0.5          ICMP        98 Echo (ping) reply    id=0x53da, seq=2/512, ttl=54 (request in 253)
258 20.299226391  192.168.0.5          172.217.166.99       ICMP        98 Echo (ping) request  id=0x53da, seq=3/768, ttl=64 (reply in 259)
259 20.325403708  172.217.166.99       192.168.0.5          ICMP        98 Echo (ping) reply    id=0x53da, seq=3/768, ttl=54 (request in 258)
```

Figure 26: The website that was pinged is ***maa05s09-in-f3.1e100.net***



```
subhash011@LegionY540:~$ host 172.217.166.99
99.166.217.172.in-addr.arpa domain name pointer maa05s09-in-f3.1e100.net.
```

From the above figures, we can infer the following:

1. A total of 3 ping responses were obtained from the destination.

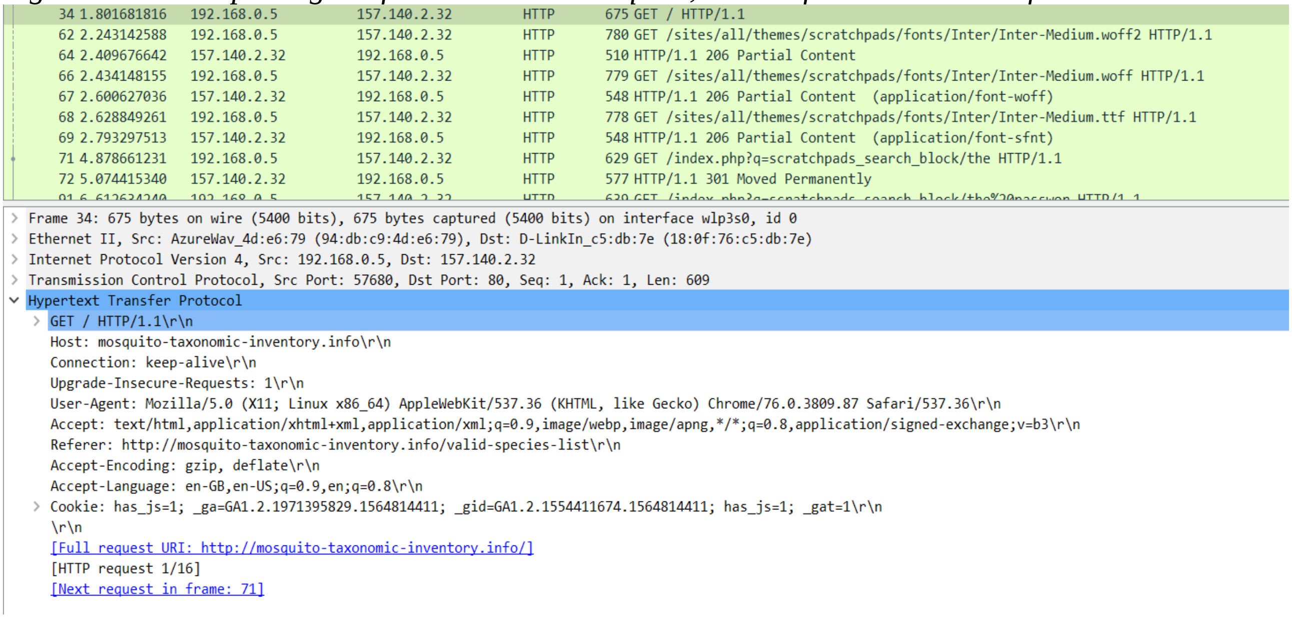
2. The website that was pinged is ***maa05s09-in-f3.1e100.net.***

3. The IP address returned after DNS resolution is ***172.217.166.99.***

4. On further inspecting the response frames, we find that the response times were 25.542ms, 24.941ms and 26.177ms respectively. So the minimum response time is ***24.941ms.***

(i) During the capture, a website was also visited using a browser. What is the hostname of this website? A file was also downloaded from this website. What was the name of this file? The password of host h4 for user “tc” is embedded within HTTP GET requests send during the packet capture. Find out and write down this password.

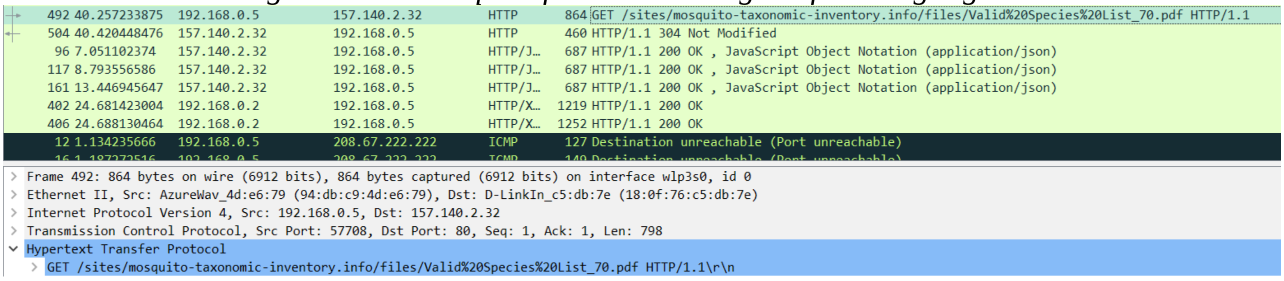
Figure 27: On inspecting the first HTTP GET request, we can find the domain of the website visited.



```
   34 1.801681816    192.168.0.5        157.140.2.32       HTTP      675 GET / HTTP/1.1
   62 2.243142588    192.168.0.5        157.140.2.32       HTTP      780 GET /sites/all/themes/scratchpads/fonts/Inter/Inter-Medium.woff2 HTTP/1.1
   64 2.409676642    157.140.2.32       192.168.0.5        HTTP      510 HTTP/1.1 206 Partial Content
   66 2.434148155    192.168.0.5        157.140.2.32       HTTP      779 GET /sites/all/themes/scratchpads/fonts/Inter/Inter-Medium.woff HTTP/1.1
   67 2.600627036    157.140.2.32       192.168.0.5        HTTP      548 HTTP/1.1 206 Partial Content  (application/font-woff)
   68 2.628849261    192.168.0.5        157.140.2.32       HTTP      778 GET /sites/all/themes/scratchpads/fonts/Inter/Inter-Medium.ttf HTTP/1.1
   69 2.793297513    157.140.2.32       192.168.0.5        HTTP      548 HTTP/1.1 206 Partial Content  (application/font-sfnt)
   71 4.878661231    192.168.0.5        157.140.2.32       HTTP      629 GET /index.php?q=scratchpads_search_block/the HTTP/1.1
   72 5.074415340    157.140.2.32       192.168.0.5        HTTP      577 HTTP/1.1 301 Moved Permanently
   91 6.612634240    192.168.0.5        157.140.2.32       HTTP      630 GET /index.php?q=scratchpads_search_block/the%20passwon HTTP/1.1

> Frame 34: 675 bytes on wire (5400 bits), 675 bytes captured (5400 bits) on interface wlp3s0, id 0
> Ethernet II, Src: AzureWav_4d:e6:79 (94:db:c9:4d:e6:79), Dst: D-LinkIn_c5:db:7e (18:0f:76:c5:db:7e)
> Internet Protocol Version 4, Src: 192.168.0.5, Dst: 157.140.2.32
> Transmission Control Protocol, Src Port: 57680, Dst Port: 80, Seq: 1, Ack: 1, Len: 609
v Hypertext Transfer Protocol
  > GET / HTTP/1.1\r\n
    Host: mosquito-taxonomic-inventory.info\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.87 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3\r\n
    Referer: http://mosquito-taxonomic-inventory.info/valid-species-list\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-GB,en-US;q=0.9,en;q=0.8\r\n
  > Cookie: has_js=1; _ga=GA1.2.1971395829.1564814411; _gid=GA1.2.1554411674.1564814411; has_js=1; _gat=1\r\n
    \r\n
    [Full request URI: http://mosquito-taxonomic-inventory.info/]
    [HTTP request 1/16]
    [Next request in frame: 71]
```

The domain name of the website visited is ***mosquito-taxonomic-inventory.info.***

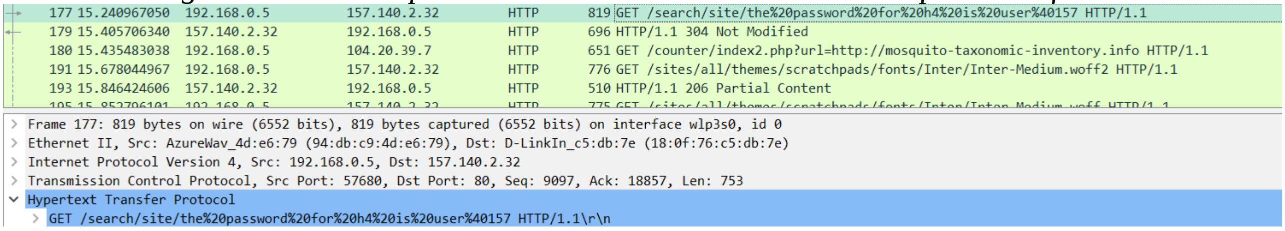
Figure 28: The request for downloading the file is highlighted.



```
  492 40.257233875  192.168.0.5        157.140.2.32       HTTP      864 GET /sites/mosquito-taxonomic-inventory.info/files/Valid%20Species%20List_70.pdf HTTP/1.1
  504 40.420448476  157.140.2.32       192.168.0.5        HTTP      460 HTTP/1.1 304 Not Modified
   96 7.051102374   157.140.2.32       192.168.0.5        HTTP/J…   687 HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
  117 8.793556586   157.140.2.32       192.168.0.5        HTTP/J…   687 HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
  161 13.446945647  157.140.2.32       192.168.0.5        HTTP/J…   687 HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
  402 24.681423004  192.168.0.2        192.168.0.5        HTTP/X…  1219 HTTP/1.1 200 OK
  406 24.688130464  192.168.0.2        192.168.0.5        HTTP/X…  1252 HTTP/1.1 200 OK
   12 1.134235666   192.168.0.5        208.67.222.222     ICMP      127 Destination unreachable (Port unreachable)
   16 1.187272516   192.168.0.5        208.67.222.222     ICMP      140 Destination unreachable (Port unreachable)

> Frame 492: 864 bytes on wire (6912 bits), 864 bytes captured (6912 bits) on interface wlp3s0, id 0
> Ethernet II, Src: AzureWav_4d:e6:79 (94:db:c9:4d:e6:79), Dst: D-LinkIn_c5:db:7e (18:0f:76:c5:db:7e)
> Internet Protocol Version 4, Src: 192.168.0.5, Dst: 157.140.2.32
> Transmission Control Protocol, Src Port: 57708, Dst Port: 80, Seq: 1, Ack: 1, Len: 798
v Hypertext Transfer Protocol
  > GET /sites/mosquito-taxonomic-inventory.info/files/Valid%20Species%20List_70.pdf HTTP/1.1\r\n
```

The name of the file downloaded can be obtained by decoding the last parameter in the URI, which turns out to be ***Valid Species List_70.pdf***

Figure 29: The last parameter in the URI here contains the password for h4



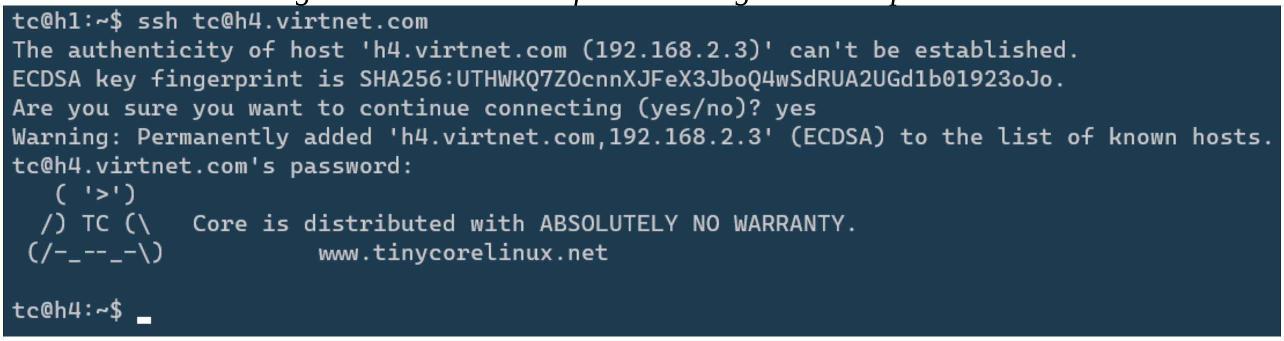
```
 177 15.240967050  192.168.0.5    157.140.2.32   HTTP   819 GET /search/site/the%20password%20for%20h4%20is%20user%40157 HTTP/1.1
 179 15.405706340  157.140.2.32   192.168.0.5    HTTP   696 HTTP/1.1 304 Not Modified
 180 15.435483038  192.168.0.5    104.20.39.7    HTTP   651 GET /counter/index2.php?url=http://mosquito-taxonomic-inventory.info HTTP/1.1
 191 15.678044967  192.168.0.5    157.140.2.32   HTTP   776 GET /sites/all/themes/scratchpads/fonts/Inter/Inter-Medium.woff2 HTTP/1.1
 193 15.846424606  157.140.2.32   192.168.0.5    HTTP   510 HTTP/1.1 206 Partial Content
 195 15.852706101  192.168.0.5    157.140.2.32   HTTP   775 GET /sites/all/themes/scratchpads/fonts/Inter/Inter-Medium.woff HTTP/1.1

> Frame 177: 819 bytes on wire (6552 bits), 819 bytes captured (6552 bits) on interface wlp3s0, id 0
> Ethernet II, Src: AzureWav_4d:e6:79 (94:db:c9:4d:e6:79), Dst: D-LinkIn_c5:db:7e (18:0f:76:c5:db:7e)
> Internet Protocol Version 4, Src: 192.168.0.5, Dst: 157.140.2.32
> Transmission Control Protocol, Src Port: 57680, Dst Port: 80, Seq: 9097, Ack: 18857, Len: 753
v Hypertext Transfer Protocol
  > GET /search/site/the%20password%20for%20h4%20is%20user%40157 HTTP/1.1\r\n
```

Original Parameter: *the%20password%20for%20h4%20is%20user%40157*
After decoding: *the password for h4 is user@157*

*The password for the host **h4** is **user@157**.*

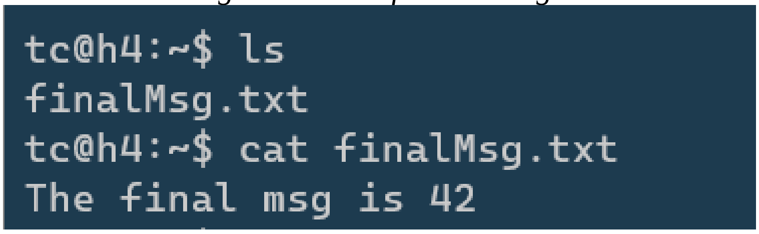
(j) Connect to h1, and then ssh to host h4 with the user name “tc” and the password obtained from the previous step. The final message is placed within a text file in the home directory of user “tc”. What is this message?

Figure 30: SSH into h4 from h1 using the above password



```
tc@h1:~$ ssh tc@h4.virtnet.com
The authenticity of host 'h4.virtnet.com (192.168.2.3)' can't be established.
ECDSA key fingerprint is SHA256:UTHWKQ7ZOcnnXJFeX3JboQ4wSdRUA2UGd1b01923oJo.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'h4.virtnet.com,192.168.2.3' (ECDSA) to the list of known hosts.
tc@h4.virtnet.com's password:
   ( '>')
  /) TC (\   Core is distributed with ABSOLUTELY NO WARRANTY.
 (/-_--_-\)           www.tinycorelinux.net

tc@h4:~$ _
```

Figure 31: The final message



```
tc@h4:~$ ls
finalMsg.txt
tc@h4:~$ cat finalMsg.txt
The final msg is 42
```