CS4150: Computer Networks Lab

Lab2

111901030
Mayank Singla

Q1. Set up the virtual network for this lab. This network has 8 VMs namely h1, h2, h3, h4, h5, r1, r2 and r3. The first 5 VMs are hosts and the rest are routers. In this lab, you only have access to machine h1, and the goal is to find out a message stored in host h4.

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

Pinging 5 packets to each of the domains using the command: **ping -c 5 <domain>**

```
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=0.841 ms
64 bytes from 192.168.1.3: seq=1 ttl=64 time=0.997 ms
64 bytes from 192.168.1.3: seq=2 ttl=64 time=1.024 ms
64 bytes from 192.168.1.3: seq=3 ttl=64 time=0.988 ms
64 bytes from 192.168.1.3: seq=4 ttl=64 time=1.013 ms

--- h2.virtnet.com ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.841/0.972/1.024 ms
tc@h1:~$
```

```
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=2.474 ms
64 bytes from 192.168.2.2: seq=1 ttl=62 time=2.783 ms
64 bytes from 192.168.2.2: seq=2 ttl=62 time=2.359 ms
64 bytes from 192.168.2.2: seq=3 ttl=62 time=2.743 ms
64 bytes from 192.168.2.2: seq=4 ttl=62 time=2.551 ms

--- h3.virtnet.com ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 2.359/2.582/2.783 ms
tc@h1:~$
```

```
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=3.192 ms
64 bytes from 192.168.2.3: seq=1 ttl=62 time=2.432 ms
64 bytes from 192.168.2.3: seq=2 ttl=62 time=2.643 ms
64 bytes from 192.168.2.3: seq=3 ttl=62 time=2.877 ms
64 bytes from 192.168.2.3: seq=4 ttl=62 time=2.615 ms

--- h4.virtnet.com ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 2.432/2.751/3.192 ms
tc@h1:~$
```

```
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=2.168 ms
64 bytes from 192.168.3.2: seq=1 ttl=62 time=2.664 ms
64 bytes from 192.168.3.2: seq=2 ttl=62 time=2.306 ms
64 bytes from 192.168.3.2: seq=3 ttl=62 time=2.620 ms
64 bytes from 192.168.3.2: seq=4 ttl=62 time=2.598 ms

--- h5.virtnet.com ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 2.168/2.471/2.664 ms
tc@h1:~$
```

Domain	Avg. Round Trip Time
h2.virtnet.com	0.972 ms
h3.virtnet.com	2.582 ms
h4.virtnet.com	2.751 ms
h5.virtnet.com	2.471 ms

(b) Host A is running an 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?

Doing an **nmap** scan on all the domains using the command: **nmap <domain>**

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

Starting Nmap 6.40 ( http://nmap.org ) at 2022-09-06 10:46 UTC
Nmap scan report for h2.virtnet.com (192.168.1.3)
Host is up (0.0013s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
21/tcp open  ftp

Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
tc@h1:~$
```

Host A is **h2**

Doing an **nmap** scan on all the domains in the given port range along with the version scan using the command: **sudo nmap -sV -p 8000-9000 <domain>**

```
tc@h1:~$ sudo nmap -sV -p 8000-9000 h3.virtnet.com

Starting Nmap 6.40 ( http://nmap.org ) at 2022-09-06 10:47 UTC
Nmap scan report for h3.virtnet.com (192.168.2.2)
Host is up (0.00027s latency).
Not shown: 999 closed ports
PORT     STATE SERVICE VERSION
8143/tcp open  http    lighttpd 1.4.54
8534/tcp open  http    lighttpd 1.4.54

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.20 seconds
tc@h1:~$
```

Host B is **h3**

Incoming ports of the HTTP servers on host B are **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. *Hint: directory listing is enabled on these servers.* Each of these files contains one-half of the password needed to log into the FTP server on host A. Write down this password.

Getting the files from the HTTP servers using the command:
wget -q <http://domain:port/path/…>

```
tc@h1:~$ wget -q http://h3.virtnet.com:8143/
tc@h1:~$ ls
index.html
tc@h1:~$ cat index.html
Explore the folder t32 on this web server
tc@h1:~$ rm -rf index.html
```

```
tc@h1:~$ wget -q http://h3.virtnet.com:8143/t32/
tc@h1:~$ ls
index.html
tc@h1:~$ exit
Connection to localhost closed.
cs4150@aha-acdgfl-058l:~/Downloads/lab2_network$ scp -P 14501 tc@localhost:/home/tc/index.html ./
tc@localhost's password:
index.html                                    100% 6189    19.2MB/s   00:00
cs4150@aha-acdgfl-058l:~/Downloads/lab2_network$
```

Index of /t32/

Name↓	Last Modified:	Size:	Type:
../		-	Directory
key.txt	2019-Aug-03 10:01:15	0.1K	text/plain

lighttpd/1.4.54

```
tc@h1:~$ wget -q http://h3.virtnet.com:8143/t32/key.txt
tc@h1:~$ ls
key.txt
tc@h1:~$ cat key.txt
The first half of the password is use
tc@h1:~$
```

```
tc@h1:~$ wget -q http://h3.virtnet.com:8534/
tc@h1:~$ ls
index.html
tc@h1:~$ cat index.html
Explore the folder t54 on this web server
tc@h1:~$ rm -rf index.html
```

```
tc@h1:~$ wget -q http://h3.virtnet.com:8534/t54/
tc@h1:~$ ls
index.html
tc@h1:~$ exit
Connection to localhost closed.
cs4150@aha-acdgfl-058l:~/Downloads/lab2_network$ scp -P 14501 tc@localhost:/home/tc/index.html ./
tc@localhost's password:
index.html                                    100% 6195     3.8MB/s   00:00
cs4150@aha-acdgfl-058l:~/Downloads/lab2_network$
```

Index of /t54/

Name↓	Last Modified:	Size:	Type:
../		-	Directory
keyone.txt	2019-Aug-03 10:01:59	0.1K	text/plain

lighttpd/1.4.54

```
tc@h1:~$ wget -q http://h3.virtnet.com:8534/t54/keyone.txt
tc@h1:~$ ls
keyone.txt
tc@h1:~$ cat keyone.txt
The second half of the password is er@487
tc@h1:~$
```

The actual password is **useer@487** and the working password is **user@487**

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

Getting the HTTP headers from the HTTP servers using the command:
wget -q -S <http://domain>

```
tc@h1:~$ wget -q -S http://h3.virtnet.com:8143/
  HTTP/1.0 200 OK
  Content-Type: text/html
  Accept-Ranges: bytes
  ETag: "3518547662"
  Last-Modified: Fri, 02 Aug 2019 08:14:13 GMT
  Content-Length: 42
  Connection: close
  Date: Tue, 06 Sep 2022 11:41:43 GMT
  Server: lighttpd/1.4.54

tc@h1:~$
```

```
tc@h1:~$ wget -q -S http://h3.virtnet.com:8534/
  HTTP/1.1 200 OK
  Content-Type: text/html
  Accept-Ranges: bytes
  ETag: "3518515822"
  Last-Modified: Fri, 02 Aug 2019 08:15:26 GMT
  Content-Length: 42
  Connection: close
  Date: Tue, 06 Sep 2022 11:42:47 GMT
  Server: lighttpd/1.4.54

tc@h1:~$
```

The port number **8143** runs **HTTP/1.0**
The port number **8534** runs **HTTP/1.1**

(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.

Downloading the file using the **pget** command in the interactive terminal

```
tc@h1:~$ lftp -u tc,user@487 h2.virtnet.com
lftp tc@h2.virtnet.com:~> find
./
./msg/
./msg/sol.txt
lftp tc@h2.virtnet.com:/> pget ./msg/sol.txt
lftp tc@h2.virtnet.com:/> exit
tc@h1:~$ ls
sol.txt
tc@h1:~$ cat sol.txt
The password for h5 is user@324
tc@h1:~$
```

The password for user "tc" on host h5 is **user@324**

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

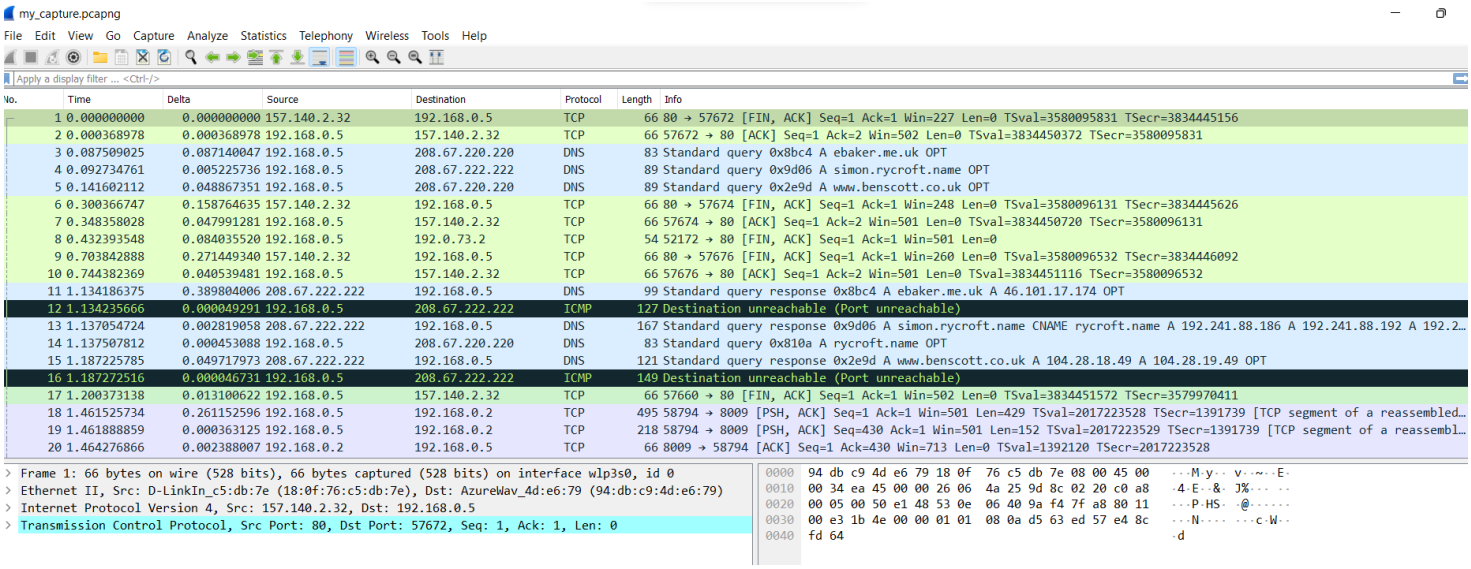
```
tc@h1:~$ ssh tc@h5.virtnet.com
The authenticity of host 'h5.virtnet.com (192.168.3.2)' can't be established.
ECDSA key fingerprint is SHA256:UTHWKQ7ZOcnnXJFeX3JboQ4wSdRUA2UGd1b01923oJo.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'h5.virtnet.com,192.168.3.2' (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:~$ ls
my_capture.pcapng
tc@h5:~$
```

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

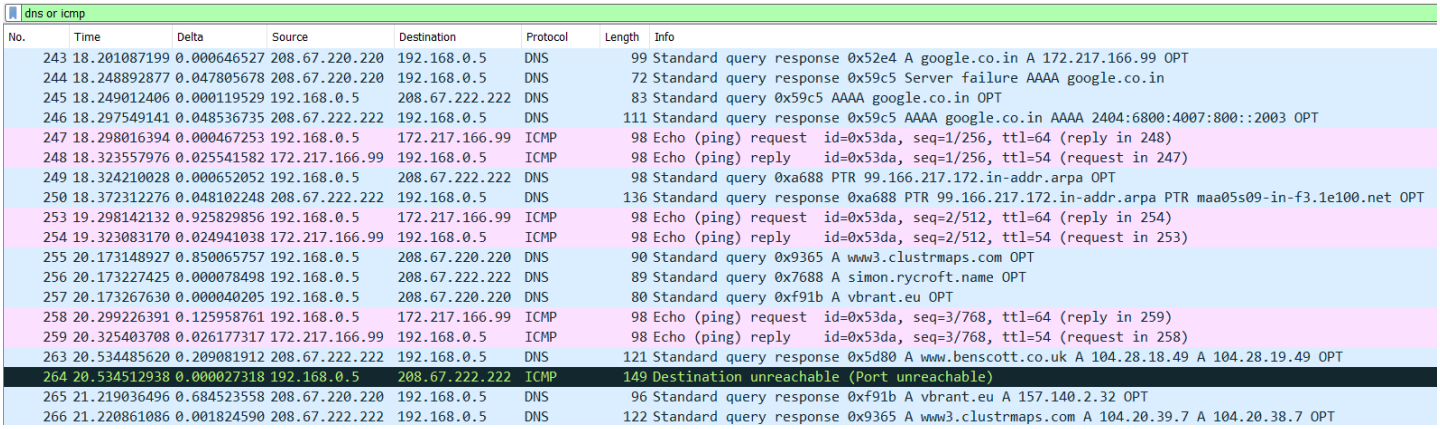
(g) Download this file to your physical host machine *(Hint: host h5 can be accessed via SSH on port 14505 on the loopback IP address of the physical host)* and open it with Wireshark.

Downloading the file using the **scp** command as below specifying the port and the file path on the remote

```
cs4150@aha-acdgfl-058l:~/Downloads/lab2_network$ ls
connect.sh  index.html  setupVMs.sh  startVMs.sh  stopVMs.sh  VirtualBox  VMImages
cs4150@aha-acdgfl-058l:~/Downloads/lab2_network$ scp -P 14505 tc@localhost:/home/tc/my_capture.pcapng ./
The authenticity of host '[localhost]:14505 ([127.0.0.1]:14505)' can't be established.
ECDSA key fingerprint is SHA256:UTHWKQ7ZOcnnXJFeX3JboQ4wSdRUA2UGd1b01923oJo.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[localhost]:14505' (ECDSA) to the list of known hosts.
tc@localhost's password:
my_capture.pcapng                                             100%  157KB  73.1MB/s   00:00
cs4150@aha-acdgfl-058l:~/Downloads/lab2_network$ ls
connect.sh  index.html  my_capture.pcapng  setupVMs.sh  startVMs.sh  stopVMs.sh  VirtualBox  VMImages
cs4150@aha-acdgfl-058l:~/Downloads/lab2_network$
```



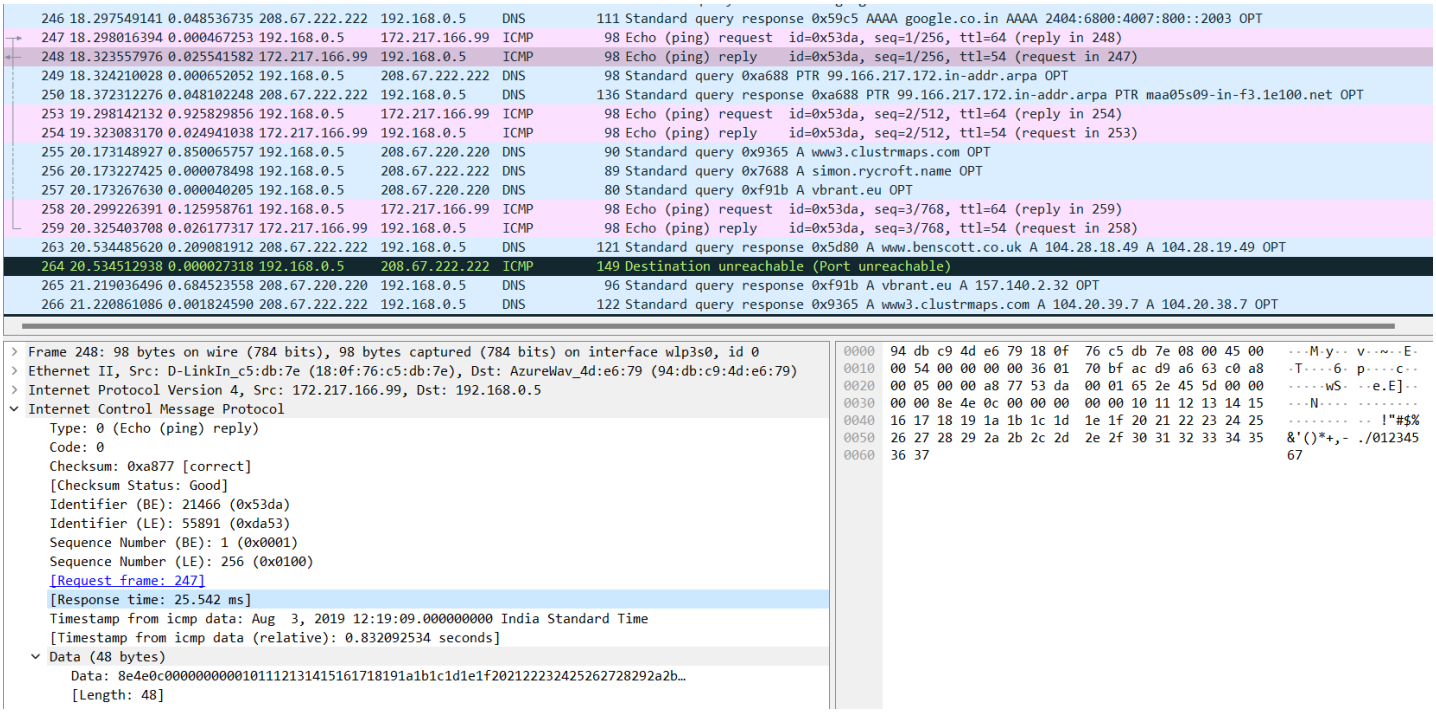
(h) What you now see in Wireshark is a sample packet capture. During the capture, a website was pinged, which host was pinged? What was the IP returned after DNS resolution? How many ping response packets were received? What was the minimum response time for these packets?



dns or icmp

No.	Time	Delta	Source	Destination	Protocol	Length	Info
243	18.201087199	0.000646527	208.67.220.220	192.168.0.5	DNS	99	Standard query response 0x52e4 A google.co.in A 172.217.166.99 OPT
244	18.248892877	0.047805678	208.67.220.220	192.168.0.5	DNS	72	Standard query response 0x59c5 Server failure AAAA google.co.in
245	18.249012406	0.000119529	192.168.0.5	208.67.222.222	DNS	83	Standard query 0x59c5 AAAA google.co.in OPT
246	18.297549141	0.048536735	208.67.222.222	192.168.0.5	DNS	111	Standard query response 0x59c5 AAAA google.co.in AAAA 2404:6800:4007:800::2003 OPT
247	18.298016394	0.000467253	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	0.025541582	172.217.166.99	192.168.0.5	ICMP	98	Echo (ping) reply id=0x53da, seq=1/256, ttl=54 (request in 247)
249	18.324210028	0.000652052	192.168.0.5	208.67.222.222	DNS	98	Standard query 0xa688 PTR 99.166.217.172.in-addr.arpa OPT
250	18.372312276	0.048102248	208.67.222.222	192.168.0.5	DNS	136	Standard query response 0xa688 PTR 99.166.217.172.in-addr.arpa PTR maa05s09-in-f3.1e100.net OPT
253	19.298142132	0.925829856	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	0.024941038	172.217.166.99	192.168.0.5	ICMP	98	Echo (ping) reply id=0x53da, seq=2/512, ttl=54 (request in 253)
255	20.173148927	0.850065757	192.168.0.5	208.67.220.220	DNS	90	Standard query 0x9365 A www3.clustrmaps.com OPT
256	20.173227425	0.000078498	192.168.0.5	208.67.222.222	DNS	89	Standard query 0x7688 A simon.rycroft.name OPT
257	20.173267630	0.000040205	192.168.0.5	208.67.220.220	DNS	80	Standard query 0xf91b A vbrant.eu OPT
258	20.299226391	0.125958761	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	0.026177317	172.217.166.99	192.168.0.5	ICMP	98	Echo (ping) reply id=0x53da, seq=3/768, ttl=54 (request in 258)
263	20.534485620	0.209081912	208.67.222.222	192.168.0.5	DNS	121	Standard query response 0x5d80 A www.benscott.co.uk A 104.28.18.49 A 104.28.19.49 OPT
264	20.534512938	0.000027318	192.168.0.5	208.67.222.222	ICMP	149	Destination unreachable (Port unreachable)
265	21.219036496	0.684523558	208.67.220.220	192.168.0.5	DNS	96	Standard query response 0xf91b A vbrant.eu A 157.140.2.32 OPT
266	21.220861086	0.001824590	208.67.222.222	192.168.0.5	DNS	122	Standard query response 0x9365 A www3.clustrmaps.com A 104.20.39.7 A 104.20.38.7 OPT

We can see from above (frame 243) that a standard query response for DNS protocol was sent to **google.co.in** and its IP address after DNS resolution was **172.217.166.99**
In the ICMP protocols, a ping request was sent to the above IP address as the destination IP address (frames 247, 253, 258).
We can see that there were a total of **3** ping response packets were received (frames 248, 254, 259).

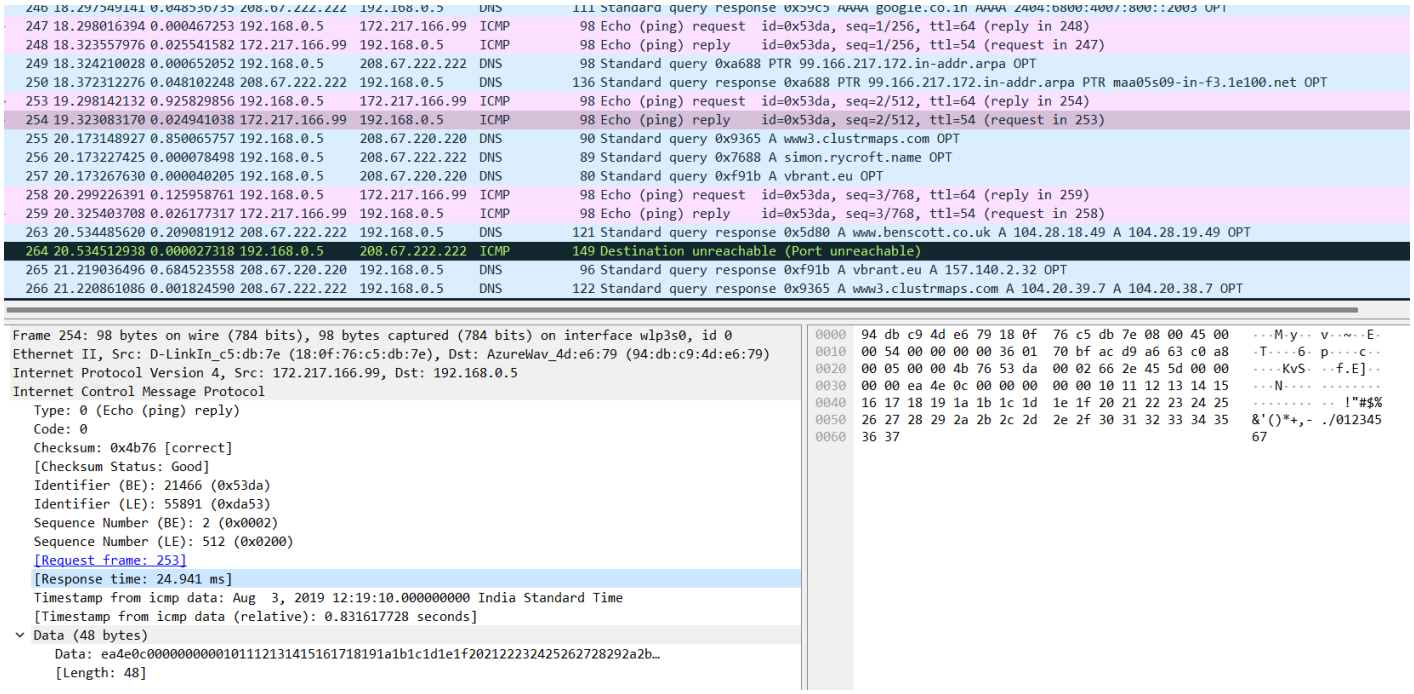


246	18.297549141	0.048536735	208.67.222.222	192.168.0.5	DNS	111	Standard query response 0x59c5 AAAA google.co.in AAAA 2404:6800:4007:800::2003 OPT
247	18.298016394	0.000467253	192.168.0.5	172.217.166.99	ICMP	98	Echo (ping) request id=0x53da, seq=1/256, ttl=64 (reply in 248)
248	18.323557976	0.025541582	172.217.166.99	192.168.0.5	ICMP	98	Echo (ping) reply id=0x53da, seq=1/256, ttl=54 (request in 247)
249	18.324210028	0.000652052	192.168.0.5	208.67.222.222	DNS	98	Standard query 0xa688 PTR 99.166.217.172.in-addr.arpa OPT
250	18.372312276	0.048102248	208.67.222.222	192.168.0.5	DNS	136	Standard query response 0xa688 PTR 99.166.217.172.in-addr.arpa PTR maa05s09-in-f3.1e100.net OPT
253	19.298142132	0.925829856	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	0.024941038	172.217.166.99	192.168.0.5	ICMP	98	Echo (ping) reply id=0x53da, seq=2/512, ttl=54 (request in 253)
255	20.173148927	0.850065757	192.168.0.5	208.67.220.220	DNS	90	Standard query 0x9365 A www3.clustrmaps.com OPT
256	20.173227425	0.000078498	192.168.0.5	208.67.222.222	DNS	89	Standard query 0x7688 A simon.rycroft.name OPT
257	20.173267630	0.000040205	192.168.0.5	208.67.220.220	DNS	80	Standard query 0xf91b A vbrant.eu OPT
258	20.299226391	0.125958761	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	0.026177317	172.217.166.99	192.168.0.5	ICMP	98	Echo (ping) reply id=0x53da, seq=3/768, ttl=54 (request in 258)
263	20.534485620	0.209081912	208.67.222.222	192.168.0.5	DNS	121	Standard query response 0x5d80 A www.benscott.co.uk A 104.28.18.49 A 104.28.19.49 OPT
264	20.534512938	0.000027318	192.168.0.5	208.67.222.222	ICMP	149	Destination unreachable (Port unreachable)
265	21.219036496	0.684523558	208.67.220.220	192.168.0.5	DNS	96	Standard query response 0xf91b A vbrant.eu A 157.140.2.32 OPT
266	21.220861086	0.001824590	208.67.222.222	192.168.0.5	DNS	122	Standard query response 0x9365 A www3.clustrmaps.com A 104.20.39.7 A 104.20.38.7 OPT

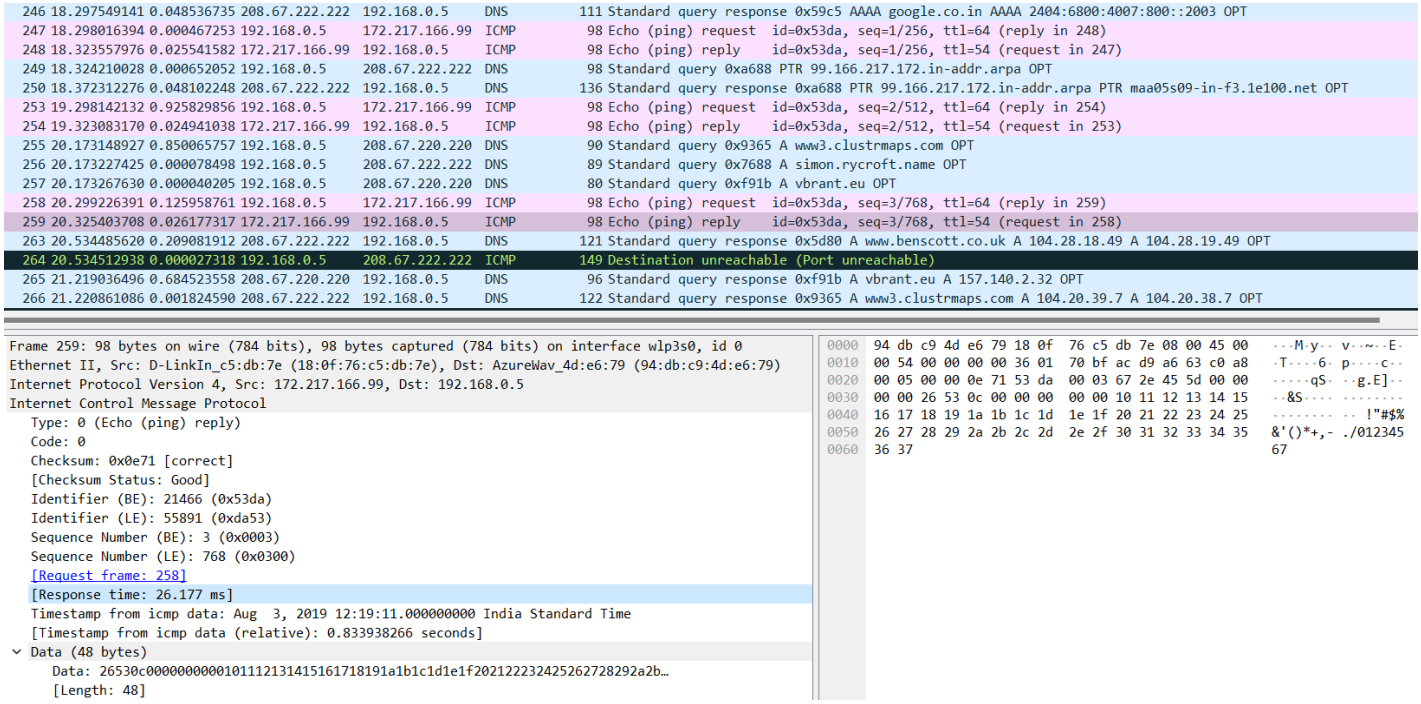
```
> Frame 248: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface wlp3s0, id 0
> Ethernet II, Src: D-LinkIn_c5:db:7e (18:0f:76:c5:db:7e), Dst: AzureWav_4d:e6:79 (94:db:c9:4d:e6:79)
> Internet Protocol Version 4, Src: 172.217.166.99, Dst: 192.168.0.5
v Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0xa877 [correct]
    [Checksum Status: Good]
    Identifier (BE): 21466 (0x53da)
    Identifier (LE): 55891 (0xda53)
    Sequence Number (BE): 1 (0x0001)
    Sequence Number (LE): 256 (0x0100)
    [Request frame: 247]
    [Response time: 25.542 ms]
    Timestamp from icmp data: Aug  3, 2019 12:19:09.000000000 India Standard Time
    [Timestamp from icmp data (relative): 0.832092534 seconds]
  v Data (48 bytes)
      Data: 8e4e0c0000000001011121314151617181 91a1b1c1d1e1f202122232425262728292a2b…
      [Length: 48]
```

```
0000  94 db c9 4d e6 79 18 0f  76 c5 db 7e 08 00 45 00   ···M·y·· v··~··E·
0010  00 54 00 00 00 00 36 01  70 bf ac d9 a6 63 c0 a8   ·T····6· p····c··
0020  00 05 00 00 a8 77 53 da  00 01 65 2e 45 5d 00 00   ·····wS· ··e.E]··
0030  00 00 8e 4e 0c 00 00 00  00 00 10 11 12 13 14 15   ···N···· ········
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ········ ·· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                             67
```

Response Time for the first ping response packet = **25.542 ms**



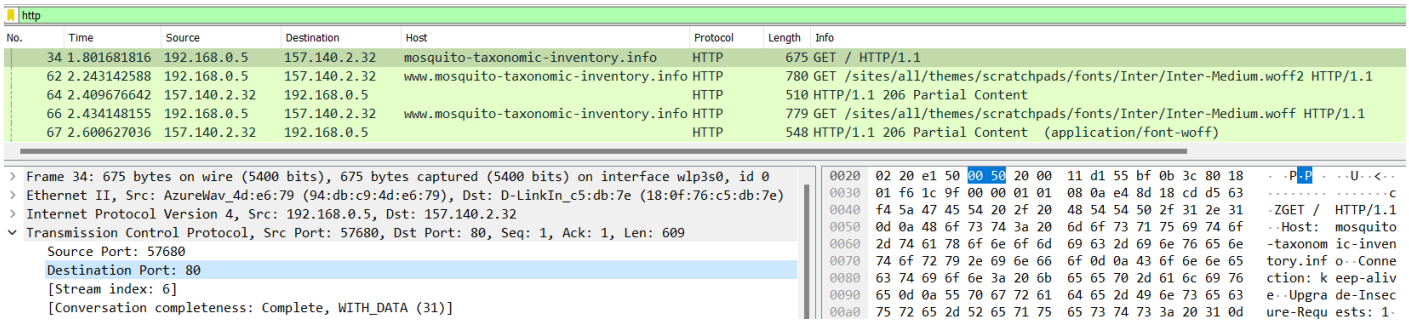
Response Time for the first ping response packet = **24.941 ms**



Response Time for the first ping response packet = **26.177 ms**

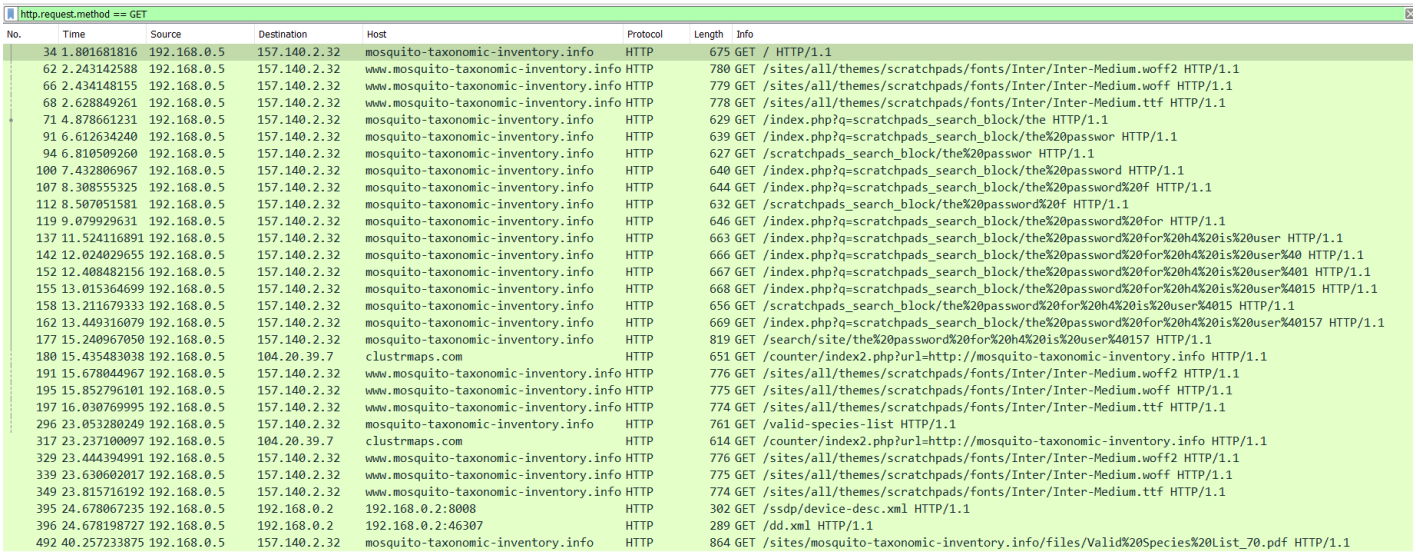
Hence, the minimum response time for these packets is **24.941 ms**

(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 sent during the packet capture. Find out and write down this password.



Here we can see that the HTTP GET request was made to **http://mosquito-taxonomic-inventory.info/** which has the Destination Port of **80** which means that this website was visited using a browser. We can see from the Host column that the hostname of this website is **mosquito-taxonomic-inventory.info**

Here is the list of all the HTTP GET requests that were made



Some of these files like font files (*.woff2, *.woff, *.ttf), XML files and PHP files might be downloaded when the website was first visited as part of initial loading of the website, but not the actual downloaded files.

We can then see a GET request to
/counter/index2.php?url=http://mosquito-taxonomic-inventory.info
whose response is in frame 232 which says **200 OK (PNG)**

```
180 15.435483038 192.168.0.5    104.20.39.7     clustrmaps.com                      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    www.mosquito-taxonomic-inventory.info 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 15.852796101 192.168.0.5    157.140.2.32    www.mosquito-taxonomic-inventory.info HTTP  775 GET /sites/all/themes/scratchpads/fonts/Inter/Inter-Medium.woff HTTP/1.1
196 16.016539158 157.140.2.32   192.168.0.5                                         HTTP    548 HTTP/1.1 206 Partial Content  (application/font-woff)
197 16.030769995 192.168.0.5    157.140.2.32    www.mosquito-taxonomic-inventory.info HTTP  774 GET /sites/all/themes/scratchpads/fonts/Inter/Inter-Medium.ttf HTTP/1.1
219 16.197049490 157.140.2.32   192.168.0.5                                         HTTP    548 HTTP/1.1 206 Partial Content  (application/font-sfnt)
232 16.346546288 104.20.39.7    192.168.0.5                                         HTTP     63 HTTP/1.1 200 OK  (PNG)
296 23.053280249 192.168.0.5    157.140.2.32    mosquito-taxonomic-inventory.info   HTTP    761 GET /valid-species-list HTTP/1.1
```

```
rame 180: 651 bytes on wire (5208 bits), 651 bytes captured (5208 bits) on interface wlp3s0, id 0
thernet II, Src: AzureWav_4d:e6:79 (94:db:c9:4d:e6:79), Dst: D-LinkIn_c5:db:7e (18:0f:76:c5:db:7e)
nternet Protocol Version 4, Src: 192.168.0.5, Dst: 104.20.39.7
ransmission Control Protocol, Src Port: 58062, Dst Port: 80, Seq: 1, Ack: 1, Len: 597
ypertext Transfer Protocol
> GET /counter/index2.php?url=http://mosquito-taxonomic-inventory.info HTTP/1.1\r\n
  Host: clustrmaps.com\r\n
  Connection: keep-alive\r\n
  User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.
  Accept: image/webp,image/apng,image/*,*/*;q=0.8\r\n
  Referer: http://mosquito-taxonomic-inventory.info/search/site/the%20password%20for%20h4%20is%20user%
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: en-GB,en-US;q=0.9,en;q=0.8\r\n
> Cookie: __cfduid=d75ef55c8146908fca3c11044d225f9911564814426; PHPSESSID=bmmmipm5u32u3b0qplrip0kh25;
  \r\n
  [Full request URI: http://clustrmaps.com/counter/index2.php?url=http://mosquito-taxonomic-inventory.
  [HTTP request 1/2]
  [Response in frame: 232]
  [Next request in frame: 317]
```

```
0030  04 c3 bb 95 00 00 47 45  54 20 2f 63 6f 75 6e 74   ......GE T /count
0040  65 72 2f 69 6e 64 65 78  32 2e 70 68 70 3f 75 72   er/index 2.php?ur
0050  6c 3d 68 74 74 70 3a 2f  2f 6d 6f 73 71 75 69 74   l=http:/ /mosquit
0060  6f 2d 74 61 78 6f 6e 6f  6d 69 63 2d 69 6e 76 65   o-taxono mic-inve
0070  6e 74 6f 72 79 2e 69 6e  66 6f 20 48 54 54 50 2f   ntory.in fo HTTP/
0080  31 2e 31 0d 0a 48 6f 73  74 3a 20 63 6c 75 73 74   1.1··Hos t: clust
0090  72 6d 61 70 73 2e 63 6f  6d 0d 0a 43 6f 6e 6e 65   rmaps.co m··Conne
00a0  63 74 69 6f 6e 3a 20 6b  65 65 70 2d 61 6c 69 76   ction: k eep-aliv
00b0  65 0d 0a 55 73 65 72 2d  41 67 65 6e 74 3a 20 4d   e··User- Agent: M
00c0  6f 7a 69 6c 6c 61 2f 35  2e 30 20 28 58 31 31 3b   ozilla/5 .0 (X11;
00d0  20 4c 69 6e 75 78 20 78  38 36 5f 36 34 29 20 41    Linux x 86_64) A
00e0  70 70 6c 65 57 65 62 4b  69 74 2f 35 33 37 2e 33   ppleWebK it/537.3
00f0  36 20 28 4b 48 54 4d 4c  2c 20 6c 69 6b 65 20 47   6 (KHTML , like G
0100  65 63 6b 6f 29 20 43 68  72 6f 6d 65 2f 37 36 2e   ecko) Ch rome/76.
0110  30 2e 33 38 30 39 2e 38  37 20 53 61 66 61 72 69   0.3809.8 7 Safari
0120  2f 35 33 37 2e 33 36 0d  0a 41 63 63 65 70 74 3a   /537.36· ·Accept:
0130  20 69 6d 61 67 65 2f 77  65 62 70 2c 69 6d 61 67    image/w ebp,imag
0140  65 2f 61 70 6e 67 2c 69  6d 61 67 65 2f 2a 2c 2a   e/apng,i mage/*,*
0150  2f 2a 3b 71 3d 30 2e 38  0d 0a 52 65 66 65 72 65   /*;q=0.8 ··Refere
0160  72 3a 20 68 74 74 70 3a  2f 2f 6d 6f 73 71 75 69   r: http: //mosqui
0170  74 6f 2d 74 61 78 6f 6e  6f 6d 69 63 2d 69 6e 76   to-taxon omic-inv
0180  65 6e 74 6f 72 79 2e 69  6e 66 6f 2f 73 65 61 72   entory.i nfo/sear
```

Also, in the exported HTTP object list, we are able to see that PNG image and can save and open that image which indicates that this file was downloaded

Wireshark · Export · HTTP object list

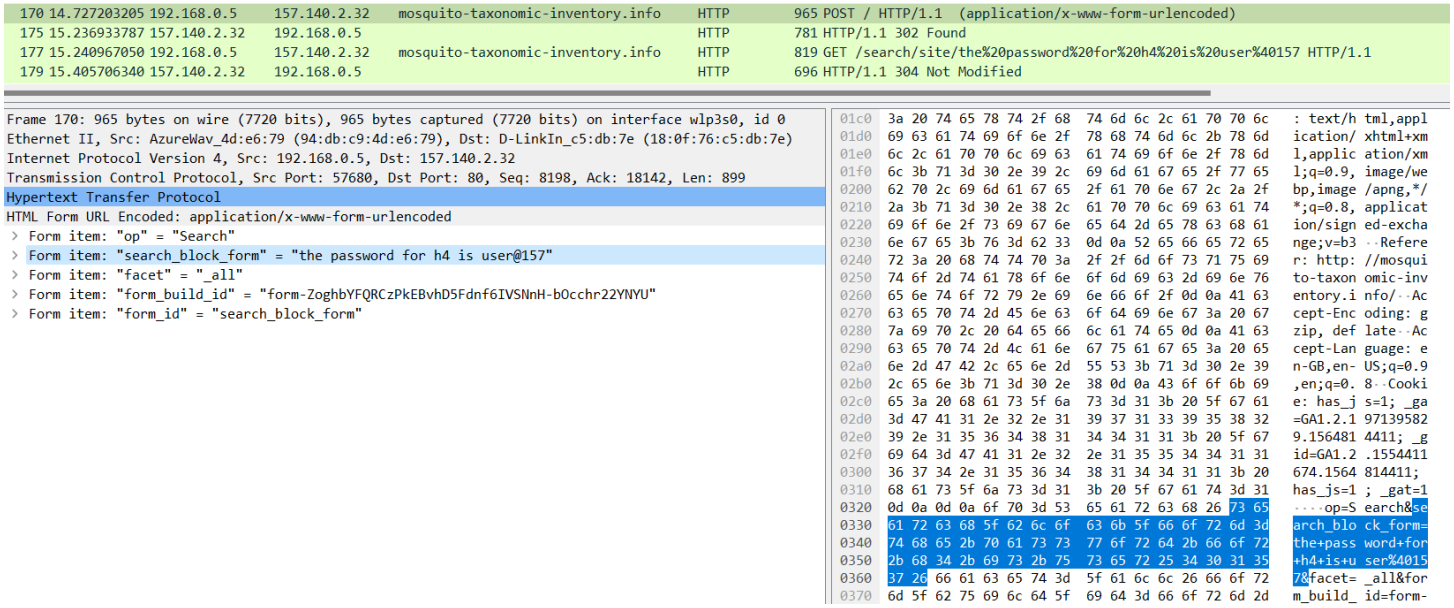
Text Filter:

Packet	Hostname	Content Type	Size	Filename
64	www.mosquito-taxonomic-inventory.info		1 bytes	Inter-Medium.woff2
67	www.mosquito-taxonomic-inventory.info	application/font-woff	1 bytes	Inter-Medium.woff
69	www.mosquito-taxonomic-inventory.info	application/font-sfnt	1 bytes	Inter-Medium.ttf
96	mosquito-taxonomic-inventory.info	application/json	2 bytes	the%20passwor
117	mosquito-taxonomic-inventory.info	application/json	2 bytes	the%20password%20f
161	mosquito-taxonomic-inventory.info	application/json	2 bytes	the%20password%20for%20h4%20is%20user%4015
170	mosquito-taxonomic-inventory.info	application/x-www-form-urlencoded	161 bytes	\
193	www.mosquito-taxonomic-inventory.info		1 bytes	Inter-Medium.woff2
196	www.mosquito-taxonomic-inventory.info	application/font-woff	1 bytes	Inter-Medium.woff
219	www.mosquito-taxonomic-inventory.info	application/font-sfnt	1 bytes	Inter-Medium.ttf
232	clustrmaps.com	image/png	18 kB	mosquito-taxonomic-inventory.info
320	mosquito-taxonomic-inventory.info	application/x-www-form-urlencoded	7 bytes	statistics.php
337	www.mosquito-taxonomic-inventory.info		1 bytes	Inter-Medium.woff2
348	www.mosquito-taxonomic-inventory.info	application/font-woff	1 bytes	Inter-Medium.woff
373	www.mosquito-taxonomic-inventory.info	application/font-sfnt	1 bytes	Inter-Medium.ttf
381	clustrmaps.com	image/png	18 kB	mosquito-taxonomic-inventory.info
402	192.168.0.2:46307	text/xml	1153 bytes	dd.xml
406	192.168.0.2:8008	application/xml	1069 bytes	device-desc.xml

This is the downloaded image whose filename is **mosquito-taxonomic-inventory.info**

We can then also see a GET request to
/sites/mosquito-taxonomic-inventory.info/files/Valid%20Species%20List_70.pdf
whose response is in frame 504 which says **304 Not Modified**
This indicates, that the file was not downloaded from this GET request

```
492 40.257233875 192.168.0.5    157.140.2.32    mosquito-taxonomic-inventory.info    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

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
Hypertext Transfer Protocol
  GET /sites/mosquito-taxonomic-inventory.info/files/Valid%20Species%20List_70.pdf HTTP/1.1\r\n
  Host: mosquito-taxonomic-inventory.info\r\n
  Connection: keep-alive\r\n
  Cache-Control: max-age=0\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.
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,applic
  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=
  If-None-Match: "a34a8-58a4048e2fdef"\r\n
  If-Modified-Since: Sat, 01 Jun 2019 10:06:28 GMT\r\n
  \r\n
  [Full request URI: http://mosquito-taxonomic-inventory.info/sites/mosquito-taxonomic-inventory.info/
  [HTTP request 1/1]
  [Response in frame: 504]

0040  8a 97 47 45 54 20 2f 73  69 74 65 73 2f 6d 6f 73   ··GET /s ites/mos
0050  71 75 69 74 6f 2d 74 61  78 6f 6e 6f 6d 69 63 2d   quito-ta xonomic-
0060  69 6e 76 65 6e 74 6f 72  79 2e 69 6e 66 6f 2f 66   inventor y.info/f
0070  69 6c 65 73 2f 56 61 6c  69 64 25 32 30 53 70 65   iles/Val id%20Spe
0080  63 69 65 73 25 32 30 4c  69 73 74 5f 37 30 2e 70   cies%20L ist_70.p
0090  64 66 20 48 54 54 50 2f  31 2e 31 0d 0a 48 6f 73   df HTTP/ 1.1··Hos
00a0  74 3a 20 6d 6f 73 71 75  69 74 6f 2d 74 61 78 6f   t: mosqu ito-taxo
00b0  6e 6f 6d 69 63 2d 69 6e  76 65 6e 74 6f 72 79 2e   nomic-in ventory.
00c0  69 6e 66 6f 0d 0a 43 6f  6e 6e 65 63 74 69 6f 6e   info··Co nnection
00d0  3a 20 6b 65 65 70 2d 61  6c 69 76 65 0d 0a 43 61   : keep-a live··Ca
00e0  63 68 65 2d 43 6f 6e 74  72 6f 6c 3a 20 6d 61 78   che-Cont rol: max
00f0  2d 61 67 65 3d 30 0d 0a  55 70 67 72 61 64 65 2d   -age=0·· Upgrade-
0100  49 6e 73 65 63 75 72 65  2d 52 65 71 75 65 73 74   Insecure -Request
0110  73 3a 20 31 0d 0a 55 73  65 72 2d 41 67 65 6e 74   s: 1··Us er-Agent
0120  3a 20 4d 6f 7a 69 6c 6c  61 2f 35 2e 30 20 28 58   : Mozill a/5.0 (X
0130  31 31 3b 20 4c 69 6e 75  78 20 78 38 36 5f 36 34   11; Linu x x86_64
0140  29 20 41 70 70 6c 65 57  65 62 4b 69 74 2f 35 33   ) AppleW ebKit/53
0150  37 2e 33 36 20 28 4b 48  54 4d 4c 2c 20 6c 69 6b   7.36 (KH TML, lik
0160  65 20 47 65 63 6b 6f 29  20 43 68 72 6f 6d 65 2f   e Gecko)  Chrome/
0170  37 36 2e 30 2e 33 38 30  39 2e 38 37 20 53 61 66   76.0.380 9.87 Saf
0180  61 72 69 2f 35 33 37 2e  33 36 0d 0a 41 63 63 65   ari/537. 36··Acce
0190  70 74 3a 20 74 65 78 74  2f 68 74 6d 6c 2c 61 70   pt: text /html,ap
01a0  70 6c 69 63 61 74 69 6f  6e 2f 78 68 74 6d 6c 2b   plicatio n/xhtml+
01b0  78 6d 6c 2c 61 70 70 6c  69 63 61 74 69 6f 6e 2f   xml,appl ication/
01c0  78 6d 6c 3b 71 3d 30 2e  39 2c 69 6d 61 67 65 2f   xml;q=0. 9,image/
```



We can see the POST request from a form (application/x-www-form-urlencoded), in which there is a form item **search_block_form** which clearly says the password for h4 is **user@157**

Also, below that we can see a GET request to
/search/site/the%20password%20for%20h4%20is%20user%40157
In this URL, the special characters are encoded as per web URL format where:

%20 is for **space** character
%40 is for **@** character

Hence, the password for 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?

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

The final message is **42**