

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 $h \in \{h2, h3, h4, h5\}$. 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-0581:~/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-0581:~/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-0581:~/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-0581:~/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:UTHWKQ7Z0cnnXJFeX3JboQ4wSdRUA2UGd1b01923oJo.
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-0581:~/Downloads/lab2_network$ ls
connect.sh index.html setupVMs.sh startVMs.sh stopVMs.sh VirtualBox VMImages
cs4150@aha-acdgfl-0581:~/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:UTHWKQ7Z0cnnXJFeX3JboQ4wSdRUA2UGd1b01923oJo.
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-0581:~/Downloads/lab2_network$ ls
connect.sh index.html my_capture.pcapng setupVMs.sh startVMs.sh stopVMs.sh VirtualBox VMImages
cs4150@aha-acdgfl-0581:~/Downloads/lab2_network$
```

my_capture.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

No.	Time	Delta	Source	Destination	Protocol	Length	Info
1	0.000000000	0.000000000	157.140.2.32	192.168.0.5	TCP	66	80 → 57672 [FIN, ACK] Seq=1 Ack=1 Win=227 Len=0 TSval=3580095831 TSecr=3834445156
2	0.000368978	0.000368978	192.168.0.5	157.140.2.32	TCP	66	57672 → 80 [ACK] Seq=1 Ack=2 Win=502 Len=0 TSval=3834450372 TSecr=3580095831
3	0.087509025	0.087140047	192.168.0.5	208.67.220.220	DNS	83	Standard query 0x8bc4 A ebaker.me.uk OPT
4	0.092734761	0.005225736	192.168.0.5	208.67.222.222	DNS	89	Standard query 0x9d06 A simon.rycroft.name OPT
5	0.141602112	0.048867351	192.168.0.5	208.67.220.220	DNS	89	Standard query 0x2e9d A www.benscott.co.uk OPT
6	0.300366747	0.158764635	157.140.2.32	192.168.0.5	TCP	66	80 → 57674 [FIN, ACK] Seq=1 Ack=1 Win=248 Len=0 TSval=3580096131 TSecr=3834445626
7	0.348358028	0.047991281	192.168.0.5	157.140.2.32	TCP	66	57674 → 80 [ACK] Seq=1 Ack=2 Win=501 Len=0 TSval=3834450720 TSecr=3580096131
8	0.432393548	0.084035520	192.168.0.5	192.0.73.2	TCP	54	52172 → 80 [FIN, ACK] Seq=1 Ack=1 Win=501 Len=0
9	0.703842888	0.271449340	157.140.2.32	192.168.0.5	TCP	66	80 → 57676 [FIN, ACK] Seq=1 Ack=1 Win=260 Len=0 TSval=3580096532 TSecr=3834446092
10	0.744382369	0.040539481	192.168.0.5	157.140.2.32	TCP	66	57676 → 80 [ACK] Seq=1 Ack=2 Win=501 Len=0 TSval=3834451116 TSecr=3580096532
11	1.134186375	0.389804006	208.67.222.222	192.168.0.5	DNS	99	Standard query response 0x8bc4 A ebaker.me.uk A 46.101.17.174 OPT
12	1.134235666	0.000049291	192.168.0.5	208.67.222.222	ICMP	127	Destination unreachable (Port unreachable)
13	1.137054724	0.002819058	208.67.222.222	192.168.0.5	DNS	167	Standard query response 0x9d06 A simon.rycroft.name CNAME rycroft.name A 192.241.88.186 A 192.241.88.192 A 192.241.88.194
14	1.137057812	0.000453088	192.168.0.5	208.67.220.220	DNS	83	Standard query 0x810a A rycroft.name OPT
15	1.187225785	0.049717973	208.67.222.222	192.168.0.5	DNS	121	Standard query response 0x2e9d A www.benscott.co.uk A 104.28.18.49 A 104.28.19.49 OPT
16	1.187272516	0.000046731	192.168.0.5	208.67.222.222	ICMP	149	Destination unreachable (Port unreachable)
17	1.200373138	0.013100622	192.168.0.5	157.140.2.32	TCP	66	57660 → 80 [FIN, ACK] Seq=1 Ack=1 Win=502 Len=0 TSval=3834451572 TSecr=3579970411
18	1.461525734	0.261152596	192.168.0.5	192.168.0.2	TCP	495	58794 → 8009 [PSH, ACK] Seq=1 Ack=1 Win=501 Len=429 TSval=2017223528 TSecr=1391739 [TCP segment of a reassembled...
19	1.461888859	0.000363125	192.168.0.5	192.168.0.2	TCP	218	58794 → 8009 [PSH, ACK] Seq=430 Ack=1 Win=501 Len=152 TSval=2017223529 TSecr=1391739 [TCP segment of a reassembled...
20	1.464276866	0.002388007	192.168.0.2	192.168.0.5	TCP	66	8009 → 58794 [ACK] Seq=1 Ack=430 Win=713 Len=0 TSval=1392120 TSecr=2017223528

> Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 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: 157.140.2.32, Dst: 192.168.0.5

> Transmission Control Protocol, Src Port: 80, Dst Port: 57672, Seq: 1, Ack: 1, Len: 0

0000 94 db c9 4d e6 79 18 0f 76 c5 db 7e 08 00 45 00 ...M.y...v...E...
0010 00 34 ea 45 00 00 26 06 4a 25 9d 8c 02 20 c0 a8 ...4.E...&...
0020 00 05 00 50 e1 48 53 0e 06 40 9a f4 7f a8 80 11 ...P.HS...@...
0030 00 e3 1b 4e 00 00 01 01 08 0a d5 63 ed 57 e4 8c ...N....c.W...
0040 fd 64 d

(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?

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](https://www.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

> Internet Protocol 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]

> Data (48 bytes)

Data: 8e4e0c000000000010112131415161718191a1b1c1d1e1f202122232425262728292a2b...

[Length: 48]

```

0000  94 db c9 4d e6 79 18 0f 76 c5 db 7e 00 00 45 00  ..M-y- v.....E-
0010  00 04 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  ....&'()*+,-./012345
0050  26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35  ..
0060  36 37                                     67

```

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

240 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	

<p>Frame 254: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface wlp3s0, id 0</p> <p>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)</p> <p>Internet Protocol Version 4, Src: 172.217.166.99, Dst: 192.168.0.5</p> <p>Internet Control Message Protocol</p> <p>Type: 0 (Echo (ping) reply)</p> <p>Code: 0</p> <p>Checksum: 0x4b76 [correct]</p> <p>[Checksum Status: Good]</p> <p>Identifier (BE): 21466 (0x53da)</p> <p>Identifier (LE): 55891 (0xda53)</p> <p>Sequence Number (BE): 2 (0x0002)</p> <p>Sequence Number (LE): 512 (0x0200)</p> <p>[Request frame: 253]</p> <p>[Response time: 24.941 ms]</p> <p>Timestamp from icmp data: Aug 3, 2019 12:19:10.000000000 India Standard Time</p> <p>[Timestamp from icmp data (relative): 0.831617728 seconds]</p> <p>▼ Data (48 bytes)</p> <p>Data: ea4e0c000000000101112131415161718191a1b1c1d1e1f202122232425262728292a2b...</p> <p>[Length: 48]</p>	<pre> 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 4b 76 53 da 00 02 66 2e 45 5d 00 00 qS- ..g.E].. 0030 00 00 ea 4e 0c 00 00 00 00 00 10 11 12 13 14 15 ..&S..... 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 </pre>
---	--

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

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	

<p>Frame 259: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface wlp3s0, id 0</p> <p>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)</p> <p>Internet Protocol Version 4, Src: 172.217.166.99, Dst: 192.168.0.5</p> <p>Internet Control Message Protocol</p> <p>Type: 0 (Echo (ping) reply)</p> <p>Code: 0</p> <p>Checksum: 0x0e71 [correct]</p> <p>[Checksum Status: Good]</p> <p>Identifier (BE): 21466 (0x53da)</p> <p>Identifier (LE): 55891 (0xda53)</p> <p>Sequence Number (BE): 3 (0x0003)</p> <p>Sequence Number (LE): 768 (0x0300)</p> <p>[Request frame: 258]</p> <p>[Response time: 26.177 ms]</p> <p>Timestamp from icmp data: Aug 3, 2019 12:19:11.000000000 India Standard Time</p> <p>[Timestamp from icmp data (relative): 0.833938266 seconds]</p> <p>▼ Data (48 bytes)</p> <p>Data: 26530c000000000101112131415161718191a1b1c1d1e1f202122232425262728292a2b...</p> <p>[Length: 48]</p>	<pre> 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 0e 71 53 da 00 03 67 2e 45 5d 00 00 qS- ..g.E].. 0030 00 00 26 53 0c 00 00 00 00 00 10 11 12 13 14 15 ..&S..... 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 </pre>
---	--

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.

No.	Time	Source	Destination	Host	Protocol	Length	Info
34	1.801681816	192.168.0.5	157.140.2.32	mosquito-taxonomic-inventory.info	HTTP	675	GET / HTTP/1.1
62	2.243142588	192.168.0.5	157.140.2.32	www.mosquito-taxonomic-inventory.info	HTTP	780	GET /sites/all/themes/scrachpads/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	www.mosquito-taxonomic-inventory.info	HTTP	779	GET /sites/all/themes/scrachpads/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)

> Frame 34: 675 bytes on wire (5400 bits), 675 bytes captured (5400 bits) on interface wlp3s0, id 0

> Ethernet II, Src: Azurelaxv_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

Source Port: 57680

Destination Port: 80

[Stream index: 6]

[Conversation completeness: Complete, WITH_DATA (31)]

```

0020 02 20 e1 50 00 50 20 00 11 d1 55 bf 0b 3c 80 18  ..P...U...<...
0030 01 f6 1c 9f 00 00 01 01 08 0a e4 8d 18 cd d5 63  .....c
0040 f4 5a 47 45 54 20 2f 20 48 54 54 50 2f 31 2e 31  -ZGET / HTTP/1.1
0050 0d 0a 48 6f 73 74 3a 20 6d 6f 73 71 75 69 74 6f  --Host: mosquito
0060 2d 74 61 78 6f 6e 6f 6d 69 63 2d 69 6e 76 65 6e  -taxonom ic-inven
0070 74 6f 72 79 2e 69 6e 66 6f 0d 0a 43 6f 6e 6e 65  tory.inf o--Conne
0080 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76  ction: k eep-aliv
0090 65 0d 0a 55 70 67 72 61 64 65 2d 49 6e 73 65 63  e--Upgra de-Insec
00a0 75 72 65 2d 52 65 71 75 65 73 74 73 3a 20 31 0d  ure-Requ ests: 1-

```

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

No.	Time	Source	Destination	Host	Protocol	Length	Info
34	1.801681816	192.168.0.5	157.140.2.32	mosquito-taxonomic-inventory.info	HTTP	675	GET / HTTP/1.1
62	2.243142588	192.168.0.5	157.140.2.32	www.mosquito-taxonomic-inventory.info	HTTP	780	GET /sites/all/themes/scrachpads/fonts/Inter/Inter-Medium.woff2 HTTP/1.1
66	2.434148155	192.168.0.5	157.140.2.32	www.mosquito-taxonomic-inventory.info	HTTP	779	GET /sites/all/themes/scrachpads/fonts/Inter/Inter-Medium.woff HTTP/1.1
68	2.628849261	192.168.0.5	157.140.2.32	www.mosquito-taxonomic-inventory.info	HTTP	778	GET /sites/all/themes/scrachpads/fonts/Inter/Inter-Medium.ttf HTTP/1.1
71	4.878661231	192.168.0.5	157.140.2.32	mosquito-taxonomic-inventory.info	HTTP	629	GET /index.php?q=scrachpads_search_block/the HTTP/1.1
91	6.612634240	192.168.0.5	157.140.2.32	mosquito-taxonomic-inventory.info	HTTP	639	GET /index.php?q=scrachpads_search_block/the%20passwor HTTP/1.1
94	6.810509260	192.168.0.5	157.140.2.32	mosquito-taxonomic-inventory.info	HTTP	627	GET /scrachpads_search_block/the%20passwor HTTP/1.1
100	7.432806967	192.168.0.5	157.140.2.32	mosquito-taxonomic-inventory.info	HTTP	640	GET /index.php?q=scrachpads_search_block/the%20password HTTP/1.1
107	8.308555325	192.168.0.5	157.140.2.32	mosquito-taxonomic-inventory.info	HTTP	644	GET /index.php?q=scrachpads_search_block/the%20password%20f HTTP/1.1
112	8.507051581	192.168.0.5	157.140.2.32	mosquito-taxonomic-inventory.info	HTTP	632	GET /scrachpads_search_block/the%20password%20f HTTP/1.1
119	9.079929631	192.168.0.5	157.140.2.32	mosquito-taxonomic-inventory.info	HTTP	646	GET /index.php?q=scrachpads_search_block/the%20password%20for HTTP/1.1
137	11.524116891	192.168.0.5	157.140.2.32	mosquito-taxonomic-inventory.info	HTTP	663	GET /index.php?q=scrachpads_search_block/the%20password%20for%20h4%20is%20user HTTP/1.1
142	12.024029655	192.168.0.5	157.140.2.32	mosquito-taxonomic-inventory.info	HTTP	666	GET /index.php?q=scrachpads_search_block/the%20password%20for%20h4%20is%20user%40 HTTP/1.1
152	12.408482156	192.168.0.5	157.140.2.32	mosquito-taxonomic-inventory.info	HTTP	667	GET /index.php?q=scrachpads_search_block/the%20password%20for%20h4%20is%20user%401 HTTP/1.1
155	13.015364699	192.168.0.5	157.140.2.32	mosquito-taxonomic-inventory.info	HTTP	668	GET /index.php?q=scrachpads_search_block/the%20password%20for%20h4%20is%20user%4015 HTTP/1.1
158	13.211679333	192.168.0.5	157.140.2.32	mosquito-taxonomic-inventory.info	HTTP	656	GET /scrachpads_search_block/the%20password%20for%20h4%20is%20user%4015 HTTP/1.1
162	13.449316079	192.168.0.5	157.140.2.32	mosquito-taxonomic-inventory.info	HTTP	619	GET /index.php?q=scrachpads_search_block/the%20password%20for%20h4%20is%20user%40157 HTTP/1.1
177	15.240967050	192.168.0.5	157.140.2.32	mosquito-taxonomic-inventory.info	HTTP	869	GET /search/site/the%20password%20for%20h4%20is%20user%40157 HTTP/1.1
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/scrachpads/fonts/Inter/Inter-Medium.woff2 HTTP/1.1
195	15.852796101	192.168.0.5	157.140.2.32	www.mosquito-taxonomic-inventory.info	HTTP	775	GET /sites/all/themes/scrachpads/fonts/Inter/Inter-Medium.woff HTTP/1.1
197	16.030769995	192.168.0.5	157.140.2.32	www.mosquito-taxonomic-inventory.info	HTTP	774	GET /sites/all/themes/scrachpads/fonts/Inter/Inter-Medium.ttf HTTP/1.1
296	23.053280249	192.168.0.5	157.140.2.32	mosquito-taxonomic-inventory.info	HTTP	761	GET /valid-species-list HTTP/1.1
317	23.237100097	192.168.0.5	104.20.39.7	clustrmaps.com	HTTP	614	GET /counter/index2.php?url=http://mosquito-taxonomic-inventory.info HTTP/1.1
329	23.444394991	192.168.0.5	157.140.2.32	www.mosquito-taxonomic-inventory.info	HTTP	776	GET /sites/all/themes/scrachpads/fonts/Inter/Inter-Medium.woff2 HTTP/1.1
339	23.630602017	192.168.0.5	157.140.2.32	www.mosquito-taxonomic-inventory.info	HTTP	775	GET /sites/all/themes/scrachpads/fonts/Inter/Inter-Medium.woff HTTP/1.1
349	23.815716192	192.168.0.5	157.140.2.32	www.mosquito-taxonomic-inventory.info	HTTP	774	GET /sites/all/themes/scrachpads/fonts/Inter/Inter-Medium.ttf HTTP/1.1
395	24.678067235	192.168.0.5	192.168.0.2	192.168.0.2:8008	HTTP	302	GET /sddp/device-desc.xml HTTP/1.1
396	24.678198727	192.168.0.5	192.168.0.2	192.168.0.2:46307	HTTP	289	GET /dd.xml HTTP/1.1
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

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](http://mosquito-taxonomic-inventory.info/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

```

Frame 180: 651 bytes on wire (5208 bits), 651 bytes captured (5208 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: 104.20.39.7
Transmission Control Protocol, Src Port: 58062, Dst Port: 80, Seq: 1, Ack: 1, Len: 597
Hypertext 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/76.0.3809.87 Safari/537.36\r\n
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%204015\r\n
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=bmmmpm5u32u3b0qplrip0kh25;\r\n
[Full request URI: http://clustrmaps.com/counter/index2.php?url=http://mosquito-taxonomic-inventory.info/]
[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 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 -Host: 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 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

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

170 14.727203205 192.168.0.5	157.140.2.32	mosquito-taxonomic-inventory.info	HTTP	965 POST / HTTP/1.1 (application/x-www-form-urlencoded)
175 15.236933787 157.140.2.32	192.168.0.5		HTTP	781 HTTP/1.1 302 Found
177 15.240967050 192.168.0.5	157.140.2.32	mosquito-taxonomic-inventory.info	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

<p>Frame 170: 965 bytes on wire (7720 bits), 965 bytes captured (7720 bits) on interface wlp3s0, id 0</p> <p>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)</p> <p>Internet Protocol Version 4, Src: 192.168.0.5, Dst: 157.140.2.32</p> <p>Transmission Control Protocol, Src Port: 57680, Dst Port: 80, Seq: 8198, Ack: 18142, Len: 899</p> <p>Hypertext Transfer Protocol</p> <p>HTML Form URL Encoded: application/x-www-form-urlencoded</p> <ul style="list-style-type: none"> > Form item: "op" = "Search" > Form item: "search_block_form" = "the password for h4 is user@157" > Form item: "facet" = "_all" > Form item: "form_build_id" = "form-ZoghbfYQRCzPkEBvhD5Fdnf6IVSNnH-b0cchr22YNYU" > Form item: "form_id" = "search_block_form" 	<pre> 01c0 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 61 70 70 6c : text/html,application/xhtml+xml 01d0 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b 78 6d ication/html+xml 01e0 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 6d l,application/xm 01f0 6c 3b 71 3d 30 2e 39 2c 69 6d 61 67 65 2f 77 65 l;q=0.9,image/webp,image/apng,* 0200 62 70 2c 69 6d 61 67 65 2f 61 70 6e 67 2c 2a 2f ;q=0.8,application/sign 0210 2a 3b 71 3d 30 2e 38 2c 61 70 70 6c 69 63 61 74 ion/sign-ed-excha 0220 69 6f 6e 2f 73 69 67 6e 65 64 2d 65 78 63 68 61 nge;v=b3..Refere 0230 6e 67 65 3b 76 3d 62 33 0d 0a 52 65 66 65 72 65 r: http://mosqui 0240 72 3a 20 68 74 74 70 3a 2f 2f 6d 6f 73 71 75 69 to:taxon-omic-inv 0250 74 6f 2d 74 61 78 6f 6e 6f 6d 69 63 2d 69 6e 76 entory.info/.Ac 0260 65 6e 74 6f 72 79 2e 69 6e 66 6f 2f 0d 0a 41 63 cept-Encoding: g 0270 63 65 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 zip, deflate..Ac 0280 7a 69 70 2c 20 64 65 66 6c 61 74 65 0d 0a 41 63 cept-Language: e 0290 63 65 70 74 2d 4c 61 6e 67 75 61 67 65 3a 20 65 n-GB,en-US;q=0.9 02a0 6e 2d 47 42 2c 65 6e 2d 55 53 3b 71 3d 30 2e 39 ,en;q=0.8..Cooki 02b0 2c 65 6e 3b 71 3d 30 2e 38 0d 0a 43 6f 6f 6b 69 e: has_js=1; _ga 02c0 65 3a 20 68 61 73 5f 6a 73 3d 31 3b 20 5f 67 61 =GA1.2.1.97139582 02d0 3d 47 41 31 2e 32 2e 31 39 37 31 33 39 35 38 32 9.156481.4411; _g 02e0 39 2e 31 35 36 34 38 31 34 34 31 31 3b 20 5f 67 id=GA1.2.1554411 02f0 69 64 3d 47 41 31 2e 32 2e 31 35 35 34 34 31 31 674.1564.814411; 0300 36 37 34 2e 31 35 36 34 38 31 34 34 31 31 3b 20 has_js=1; _gat=1 0310 68 61 73 5f 6a 73 3d 31 3b 20 5f 67 61 74 3d 31 ...op=Search&se 0320 0d 0a 0d 0a 6f 70 3d 53 65 61 72 63 68 26 73 65 arch_block_form= 0330 61 72 63 68 5f 62 6c 6f 63 6b 5f 66 6f 72 6d 3d the+pass+word+for 0340 74 68 65 2b 70 61 73 73 77 6f 72 64 2b 66 6f 72 +h4+is+user%4015 0350 2b 68 34 2b 69 73 2b 75 73 65 72 25 34 30 31 35 7&facet=_all&for 0360 37 26 66 61 63 65 74 3d 5f 61 6c 6c 26 66 6f 72 m_build_id=form- 0370 6d 5f 62 75 69 6c 64 5f 69 64 3d 66 6f 72 6d 2d </pre>
---	---

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:UTHWKQ7Z0cnnXJFeX3JboQ4wSdRUA2UGd1b019230Jo.
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**