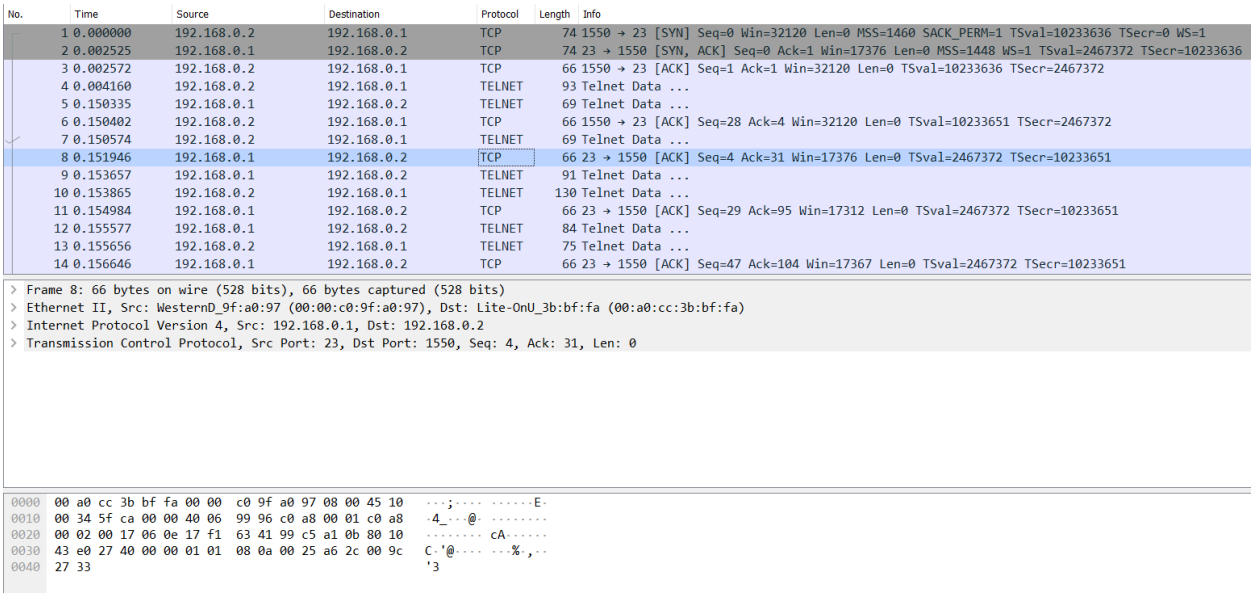
Austin Brown

CPE 434-01

3/16/2021

Lab 10

Subtask 1



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.2	192.168.0.1	TCP	74	1550 → 23 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM=1 TSval=10233636 TSecr=0 WS=1
2	0.002525	192.168.0.1	192.168.0.2	TCP	74	23 → 1550 [SYN, ACK] Seq=0 Ack=1 Win=17376 Len=0 MSS=1448 WS=1 TSval=2467372 TSecr=10233636
3	0.002572	192.168.0.2	192.168.0.1	TCP	66	1550 → 23 [ACK] Seq=1 Ack=1 Win=32120 Len=0 TSval=10233636 TSecr=2467372
4	0.004160	192.168.0.2	192.168.0.1	TELNET	93	Telnet Data ...
5	0.150335	192.168.0.1	192.168.0.2	TELNET	69	Telnet Data ...
6	0.150402	192.168.0.2	192.168.0.1	TCP	66	1550 → 23 [ACK] Seq=28 Ack=4 Win=32120 Len=0 TSval=10233651 TSecr=2467372
7	0.150574	192.168.0.2	192.168.0.1	TELNET	69	Telnet Data ...
8	0.151946	192.168.0.1	192.168.0.2	TCP	66	23 → 1550 [ACK] Seq=4 Ack=31 Win=17376 Len=0 TSval=2467372 TSecr=10233651
9	0.153657	192.168.0.1	192.168.0.2	TELNET	91	Telnet Data ...
10	0.153865	192.168.0.2	192.168.0.1	TELNET	130	Telnet Data ...
11	0.154984	192.168.0.1	192.168.0.2	TCP	66	23 → 1550 [ACK] Seq=29 Ack=95 Win=17312 Len=0 TSval=2467372 TSecr=10233651
12	0.155577	192.168.0.1	192.168.0.2	TELNET	84	Telnet Data ...
13	0.155656	192.168.0.2	192.168.0.1	TELNET	75	Telnet Data ...
14	0.156646	192.168.0.1	192.168.0.2	TCP	66	23 → 1550 [ACK] Seq=47 Ack=104 Win=17367 Len=0 TSval=2467372 TSecr=10233651

```
> Frame 8: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
> Ethernet II, Src: WesternD_9f:a0:97 (00:00:c0:9f:a0:97), Dst: Lite-OnU_3b:bf:fa (00:a0:cc:3b:bf:fa)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.2
> Transmission Control Protocol, Src Port: 23, Dst Port: 1550, Seq: 4, Ack: 31, Len: 0
```

```
0000  00 a0 cc 3b bf fa 00 00  c0 9f a0 97 08 00 45 10   ···;···· ·····E·
0010  00 34 5f ca 00 00 40 06  99 96 c0 a8 00 01 c0 a8   ·4_···@· ········
0020  00 02 00 17 06 0e 17 f1  63 41 99 c5 a1 0b 80 10   ········ cA······
0030  43 e0 27 40 00 00 01 01  08 0a 00 25 a6 2c 00 9c   C·'@···· ···%·,··
0040  27 33                                             '3
```

1. There are 92 packets in the capture.

2. The client has an address of 192.168.0.2. It is communicating with a telnet server. It has an address of 198.168.0.1. The client is using 3m-image-lm as a source port and telnet as the destination. The server uses telnet as the source and 3m-image-lm as the destination.

3. They are using telnet and TCP.

4. The arrival of the first frame is at 20:12:38.387203000.

```
Encapsulation type: Ethernet (1)
Arrival Time: Nov 27, 1999 20:12:38.387203000 Central Standard Time
[Time shift for this packet: 0.000000000 seconds]
```

The arrival of the last frame is 20:13:17.958477.

```
Arrival Time: Nov 27, 1999 20:13:17.958477000 Central Standard Time
```

The total transmission time is 39.571274 seconds.

5. Frame 47 is 554 bytes. The telnet server sends it to the client.

Subtask 2

6. It is sent by the telnet server to client.

```
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.2
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x10 (DSCP: Unknown, ECN: Not-ECT)
    Total Length: 52
    Identification: 0x5fca (24522)
  > Flags: 0x00
    Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x9996 [validation disabled]
    [Header checksum status: Unverified]
```

7. The time to live is how long until the frame is discarded. It is 64 as per the last screenshot.

8. I can see the username and password. They are fake and user.

```
..... ..!.."..'.....#..%..
%..... ..!.."..".....P. ...."....b.....b.....B.
.....".....'.....#..&..&..$..&..&..$.. .....#.....'..... .
9600,9600....#.bam.zing.org:0.0....'..DISPLAY.bam.zing.org:0.0.....xterm-
color.....!.....".....
OpenBSD/i386 (oof) (ttyp2)

login: fake
......Password:user

......Last login: Sat Nov 27 20:11:43 on ttyp2 from bam.zing.org
Warning: no Kerberos tickets issued.
OpenBSD 2.6-beta (OOF) #4: Tue Oct 12 20:42:32 CDT 1999

Welcome to OpenBSD: The proactively secure Unix-like operating system.

Please use the sendbug(1) utility to report bugs in the system.
Before reporting a bug, please try to reproduce it with the latest
version of the code.  With bug reports, please try to ensure that
enough information to reproduce the problem is enclosed, and if a
known fix for it exists, include that as well.
```

9.

The username is ..” .....”ffaakkee. The password is user.

10. The information is stored as plaintext. Secret information should be encrypted.

11. UTFP is an encrypted file transfer protocol. It can send to multiple receivers at once. The sender is uftp_v3_transfer.pcapng. It has an ip of 10.0.0.1. The receiving group has an ip of 230.4.4.1.

12. UDP essentially just sends data out into the void. It does not care if anything is listening and does not check for it. This can result in packet loss. TCP relies on a 3-way handshake. This ensures that there is a receiver at the other end.

Subtask 3

12. http is unsecured. https uses transport layer security to encrypt connections.

13. This file is not encrypted. I can read data in packet 34.

```
0020  00 fe 0c ea db 62 cd 34  98 ab cc d8 bd 36 80 18   ·····b·4 ·····6··
0030  02 11 84 31 00 00 01 01  08 0a 00 f1 80 54 00 f1   ···1···· ·····T··
0040  80 53 01 00 00 01 03 24  00 00 02 03 64 65 66 04   ·S·····$ ····def·
0050  74 65 73 74 03 66 6f 6f  03 66 6f 6f 02 69 64 02   test·foo ·foo·id·
0060  69 64 0c 3f 00 0a 00 00  00 08 23 42 00 00 00 2c   id·?···· ··#B···,
0070  00 00 03 03 64 65 66 04  74 65 73 74 03 66 6f 6f   ····def· test·foo
0080  03 66 6f 6f 06 61 6e 69  6d 61 6c 06 61 6e 69 6d   ·foo·ani mal·anim
0090  61 6c 0c 21 00 c0 00 00  00 fd 01 10 00 00 00 28   al·!···· ·······(
00a0  00 00 04 03 64 65 66 04  74 65 73 74 03 66 6f 6f   ····def· test·foo
00b0  03 66 6f 6f 04 6e 61 6d  65 04 6e 61 6d 65 0c 21   ·foo·nam e·name·!
00c0  00 c0 00 00 00 fd 00 00  00 00 00 05 00 00 05 fe   ·------- --------
00d0  00 00 22 00 0c 00 00 06  01 31 03 64 6f 67 05 47   ··"····· ·1·dog·G
00e0  6f 6f 66 79 0f 00 00 07  01 32 03 63 61 74 08 47   oofy···· ·2·cat·G
00f0  61 72 66 69 65 6c 64 05  00 00 08 fe 00 00 22 00   arfield· ------".
```

14. This file is encrypted. The file is unreadable.

```
0000  00 11 0a 18 01 14 00 90  f5 aa 83 da 08 00 45 08   -------- ------E·
0010  00 ce 24 a0 40 00 40 06  8f 66 c0 a8 02 66 c0 a8   ··$·@·@· ·f···f··
0020  02 65 86 ef 0c ea 10 b7  61 45 56 de d7 d4 80 18   ·e------ aEV-----
0030  01 0e 86 dc 00 00 01 01  08 0a 2a 4a 7b c3 0c ab   --------  --*J{---
0040  e2 69 17 03 01 00 20 01  66 fd 1a 1b 1b 18 ed 04   ·i---- · f-------
0050  76 81 58 d2 63 ef ea e6  62 fb fb 5a bd c9 62 17   v·X·c··· b··Z··b·
0060  1e 1a 15 ef ef 4b 07 17  03 01 00 70 18 15 de 62   -----K-- ---p---b
0070  8c 1d 26 15 cb f6 85 7f  b0 11 40 81 0b 50 3d bb   ··&----- ··@··P=·
0080  32 09 4b a1 76 32 9a 45  0c 9b 9f 63 e0 49 6c 10   2·K·v2·E ---c·Il·
0090  37 4a 9e 0c aa d4 09 bc  1d 0e 60 32 07 c4 72 d7   7J------ --`2--r·
00a0  a8 b9 01 68 30 68 1b d0  46 d0 5d 75 73 03 2b 8d   ---h0h-- F·]us·+·
00b0  c4 01 36 d0 5c ff 12 b5  63 eb ab 43 f6 e7 d6 53   --6·\--- c--C---S
00c0  2e 58 20 ca 2d 61 72 7c  06 4f cb 15 a2 f6 33 03   .X --ar| ·O----3·
00d0  f3 fd 8a 4d 25 66 43 04  dc c1 2f 0a              ---M%fC· --/·
```

15. This file is encrypted. Several packets have security layers listed.

```
> Frame 11: 503 bytes on wire (4024 bits), 503 bytes captured (4024 bits)
> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 38713, Dst Port: 443, Seq: 318, Ack: 1005, Len: 437
v Transport Layer Security
  > SSLv3 Record Layer: Application Data Protocol: http-over-tls
```

16. The decryption of the file is below.

```
0050  3b 20 55 3b 20 4c 69 6e  75 78 20 69 36 38 36 3b   ; U; Lin ux
0060  20 66 72 3b 20 72 76 3a  31 2e 38 2e 30 2e 32 29    fr; rv:
0070  20 47 65 63 6b 6f 2f 32  30 30 36 30 33 30 38 20    Gecko/2 0060308
0080  46 69 72 65 66 6f 78 2f  31 2e 35 2e 30 2e 32 0d   Firefox/
0090  0a 41 63 63 65 70 74 3a  20 69 6d 61 67 65 2f 70   ·Accept:  image/
00a0  6e 67 2c 2a 2f 2a 3b 71  3d 30 2e 35 0d 0a 41 63   ng,*/*;q
00b0  63 65 70 74 2d 4c 61 6e  67 75 61 67 65 3a 20 66   cept-Lan guage:
00c0  72 2c 66 72 2d 66 72 3b  71 3d 30 2e 38 2c 65 6e   r,fr-fr;
00d0  2d 75 73 3b 71 3d 30 2e  35 2c 65 6e 3b 71 3d 30   -us;q=0.
00e0  2e 33 0d 0a 41 63 63 65  70 74 2d 45 6e 63 6f 64   .3··Acce pt-
00f0  69 6e 67 3a 20 67 7a 69  70 2c 64 65 66 6c 61 74   ing: gzi
0100  65 0d 0a 41 63 63 65 70  74 2d 43 68 61 72 73 65   e··Accep t-
0110  74 3a 20 49 53 4f 2d 38  38 35 39 2d 31 2c 75 74   t: ISO-8
0120  66 2d 38 3b 71 3d 30 2e  37 2c 2a 3b 71 3d 30 2e   f-8;q=0.
0130  37 0d 0a 4b 65 65 70 2d  41 6c 69 76 65 3a 20 33   7··Keep- Alive:
0140  30 30 0d 0a 43 6f 6e 6e  65 63 74 69 6f 6e 3a 20   00··Conn ection:
```

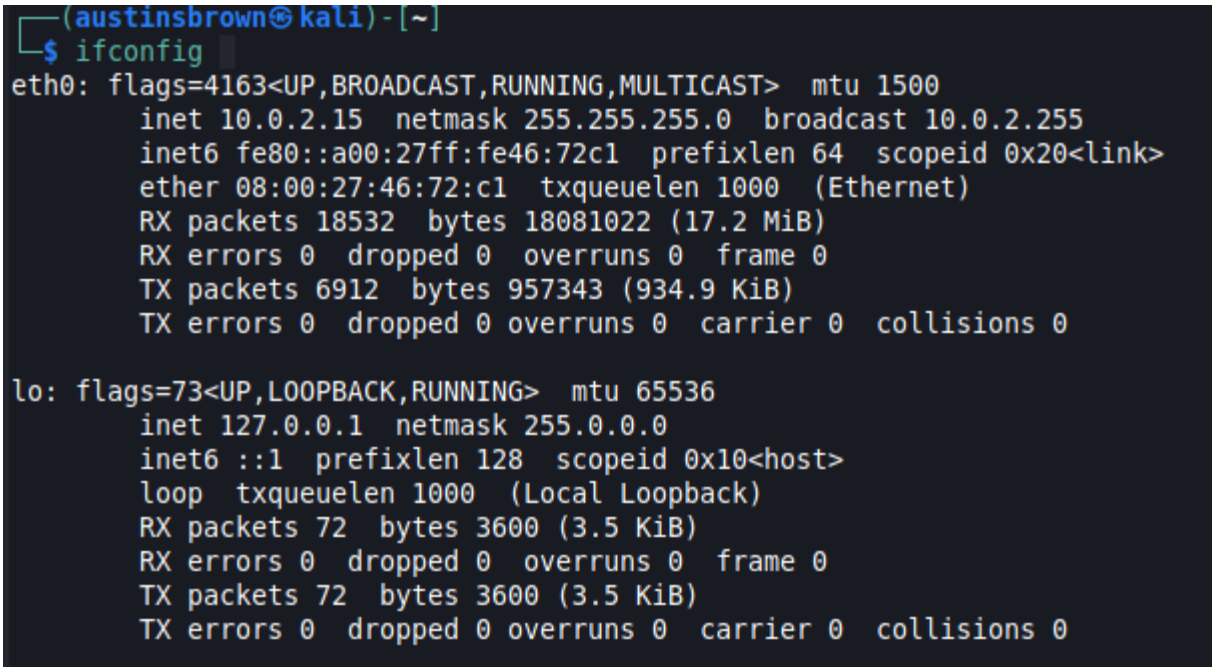
1. The image is requested in frame 31.

2. It responds with 200.

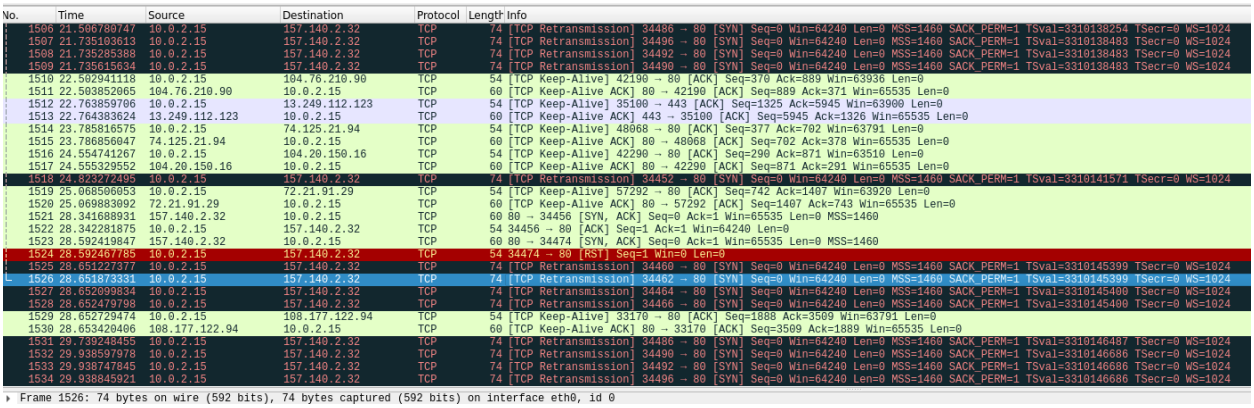
3.

Subtask 4

18.



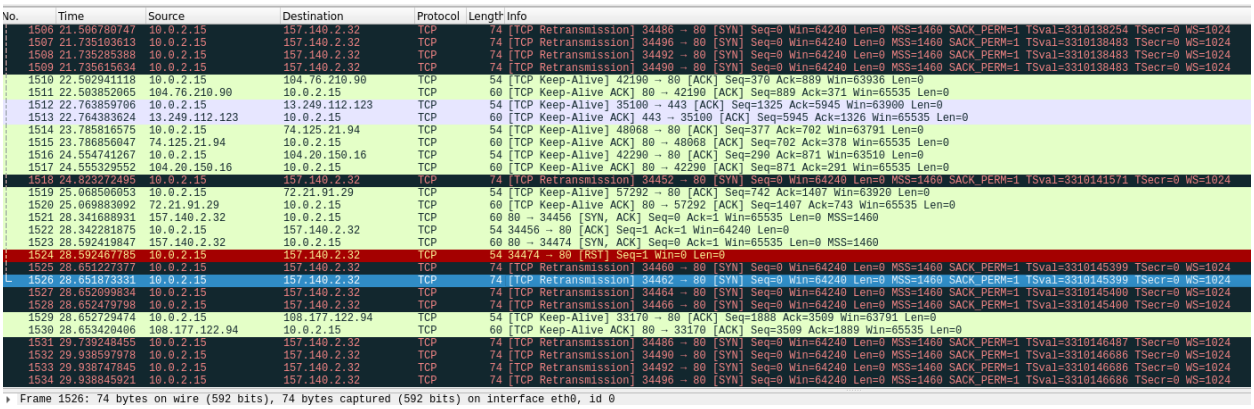
```
┌──(austinsbrown㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe46:72c1  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:46:72:c1  txqueuelen 1000  (Ethernet)
        RX packets 18532  bytes 18081022 (17.2 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 6912  bytes 957343 (934.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 72  bytes 3600 (3.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 72  bytes 3600 (3.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```



No.	Time	Source	Destination	Protocol	Length	Info
1506	21.506780747	10.0.2.15	157.140.2.32	TCP	74	[TCP Retransmission] 34486 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3310138254 TSecr=0 WS=1024
1507	21.735103613	10.0.2.15	157.140.2.32	TCP	74	[TCP Retransmission] 34496 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3310138483 TSecr=0 WS=1024
1508	21.735285388	10.0.2.15	157.140.2.32	TCP	74	[TCP Retransmission] 34492 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3310138483 TSecr=0 WS=1024
1509	21.735615634	10.0.2.15	157.140.2.32	TCP	74	[TCP Retransmission] 34490 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3310138483 TSecr=0 WS=1024
1510	22.502941118	10.0.2.15	104.76.210.90	TCP	54	[TCP Keep-Alive] 42190 → 80 [ACK] Seq=370 Ack=889 Win=63936 Len=0
1511	22.503852065	104.76.210.90	10.0.2.15	TCP	60	[TCP Keep-Alive ACK] 80 → 42190 [ACK] Seq=889 Ack=371 Win=65535 Len=0
1512	22.763859706	10.0.2.15	13.249.112.123	TCP	54	[TCP Keep-Alive] 35100 → 443 [ACK] Seq=1325 Ack=5945 Win=63900 Len=0
1513	22.764383624	13.249.112.123	10.0.2.15	TCP	60	[TCP Keep-Alive ACK] 443 → 35100 [ACK] Seq=5945 Ack=1326 Win=65535 Len=0
1514	23.785816575	10.0.2.15	74.125.21.94	TCP	54	[TCP Keep-Alive] 48068 → 80 [ACK] Seq=377 Ack=702 Win=63791 Len=0
1515	23.786856047	74.125.21.94	10.0.2.15	TCP	60	[TCP Keep-Alive ACK] 80 → 48068 [ACK] Seq=702 Ack=378 Win=65535 Len=0
1516	24.554741267	10.0.2.15	104.20.150.16	TCP	54	[TCP Keep-Alive] 42290 → 80 [ACK] Seq=290 Ack=871 Win=63510 Len=0
1517	24.555329552	104.20.150.16	10.0.2.15	TCP	60	[TCP Keep-Alive ACK] 80 → 42290 [ACK] Seq=871 Ack=291 Win=65535 Len=0
1518	24.923272495	10.0.2.15	157.140.2.32	TCP	74	[TCP Retransmission] 34452 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3310141571 TSecr=0 WS=1024
1519	25.068506053	10.0.2.15	72.21.91.29	TCP	54	[TCP Keep-Alive] 57292 → 80 [ACK] Seq=742 Ack=1407 Win=63920 Len=0
1520	25.069883092	72.21.91.29	10.0.2.15	TCP	60	[TCP Keep-Alive ACK] 80 → 57292 [ACK] Seq=1407 Ack=743 Win=65535 Len=0
1521	28.341688931	157.140.2.32	10.0.2.15	TCP	60	80 → 34456 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
1522	28.342281875	10.0.2.15	157.140.2.32	TCP	54	34456 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
1523	28.592419847	157.140.2.32	10.0.2.15	TCP	60	80 → 34474 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
1524	28.592467785	10.0.2.15	157.140.2.32	TCP	54	34474 → 80 [RST] Seq=1 Win=0 Len=0
1525	28.651227377	10.0.2.15	157.140.2.32	TCP	74	[TCP Retransmission] 34460 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3310145399 TSecr=0 WS=1024
1526	28.651873331	10.0.2.15	157.140.2.32	TCP	74	[TCP Retransmission] 34462 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3310145399 TSecr=0 WS=1024
1527	28.652099834	10.0.2.15	157.140.2.32	TCP	74	[TCP Retransmission] 34464 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3310145400 TSecr=0 WS=1024
1528	28.652479798	10.0.2.15	157.140.2.32	TCP	74	[TCP Retransmission] 34466 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3310145400 TSecr=0 WS=1024
1529	28.652729474	10.0.2.15	108.177.122.94	TCP	54	[TCP Keep-Alive] 33170 → 80 [ACK] Seq=1888 Ack=3509 Win=63791 Len=0
1530	28.653420406	108.177.122.94	10.0.2.15	TCP	60	[TCP Keep-Alive ACK] 80 → 33170 [ACK] Seq=3509 Ack=1889 Win=65535 Len=0
1531	29.739248455	10.0.2.15	157.140.2.32	TCP	74	[TCP Retransmission] 34486 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3310146487 TSecr=0 WS=1024
1532	29.938597978	10.0.2.15	157.140.2.32	TCP	74	[TCP Retransmission] 34490 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3310146686 TSecr=0 WS=1024
1533	29.938747845	10.0.2.15	157.140.2.32	TCP	74	[TCP Retransmission] 34492 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3310146686 TSecr=0 WS=1024
1534	29.938845921	10.0.2.15	157.140.2.32	TCP	74	[TCP Retransmission] 34496 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3310146686 TSecr=0 WS=1024

▸ Frame 1526: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0

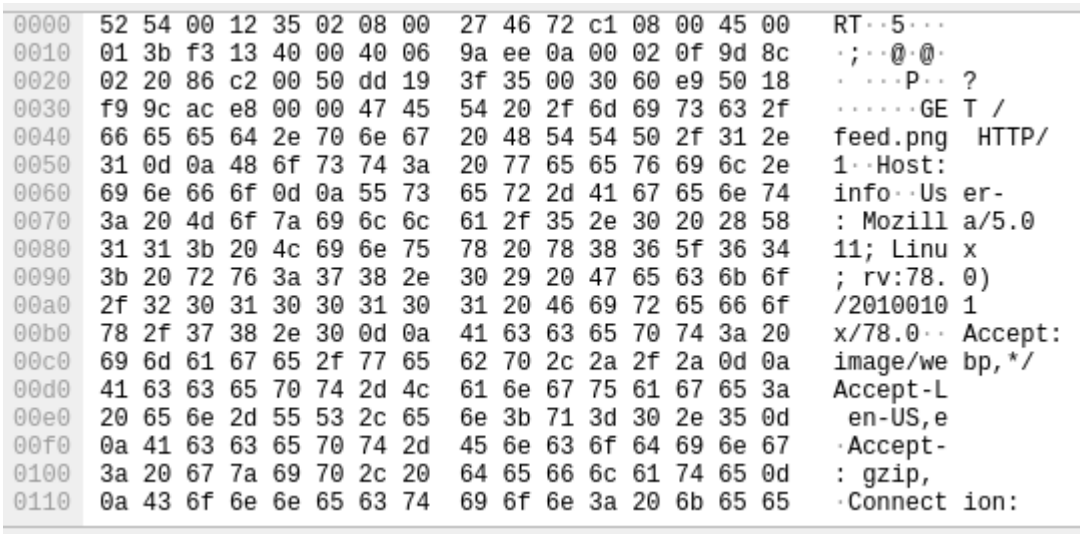
2.



No.	Time	Source	Destination	Protocol	Length	Info
1506	21.506780747	10.0.2.15	157.140.2.32	TCP	74	[TCP Retransmission] 34486 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3310138254 TSecr=0 WS=1024
1507	21.735103613	10.0.2.15	157.140.2.32	TCP	74	[TCP Retransmission] 34496 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3310138483 TSecr=0 WS=1024
1508	21.735285388	10.0.2.15	157.140.2.32	TCP	74	[TCP Retransmission] 34492 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3310138483 TSecr=0 WS=1024
1509	21.735615634	10.0.2.15	157.140.2.32	TCP	74	[TCP Retransmission] 34490 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3310138483 TSecr=0 WS=1024
1510	22.502941118	10.0.2.15	104.76.210.90	TCP	54	[TCP Keep-Alive] 42190 → 80 [ACK] Seq=370 Ack=889 Win=63936 Len=0
1511	22.503852065	104.76.210.90	10.0.2.15	TCP	60	[TCP Keep-Alive ACK] 80 → 42190 [ACK] Seq=889 Ack=371 Win=65535 Len=0
1512	22.763859706	10.0.2.15	13.249.112.123	TCP	54	[TCP Keep-Alive] 35100 → 443 [ACK] Seq=1325 Ack=5945 Win=63900 Len=0
1513	22.764383624	13.249.112.123	10.0.2.15	TCP	60	[TCP Keep-Alive ACK] 443 → 35100 [ACK] Seq=5945 Ack=1326 Win=65535 Len=0
1514	23.785816575	10.0.2.15	74.125.21.94	TCP	54	[TCP Keep-Alive] 48068 → 80 [ACK] Seq=377 Ack=702 Win=63791 Len=0
1515	23.786856047	74.125.21.94	10.0.2.15	TCP	60	[TCP Keep-Alive ACK] 80 → 48068 [ACK] Seq=702 Ack=378 Win=65535 Len=0
1516	24.554741267	10.0.2.15	104.20.150.16	TCP	54	[TCP Keep-Alive] 42290 → 80 [ACK] Seq=290 Ack=871 Win=63510 Len=0
1517	24.555329552	104.20.150.16	10.0.2.15	TCP	60	[TCP Keep-Alive ACK] 80 → 42290 [ACK] Seq=871 Ack=291 Win=65535 Len=0
1518	24.823272495	10.0.2.15	157.140.2.32	TCP	74	[TCP Retransmission] 34452 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3310141571 TSecr=0 WS=1024
1519	25.068506053	10.0.2.15	72.21.91.29	TCP	54	[TCP Keep-Alive] 57292 → 80 [ACK] Seq=742 Ack=1407 Win=63920 Len=0
1520	25.069883092	72.21.91.29	10.0.2.15	TCP	60	[TCP Keep-Alive ACK] 80 → 57292 [ACK] Seq=1407 Ack=743 Win=65535 Len=0
1521	28.341688931	157.140.2.32	10.0.2.15	TCP	60	80 → 34456 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
1522	28.342281875	10.0.2.15	157.140.2.32	TCP	54	34456 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
1523	28.592419847	157.140.2.32	10.0.2.15	TCP	60	80 → 34474 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
1524	28.592467785	10.0.2.15	157.140.2.32	TCP	54	34474 → 80 [RST] Seq=1 Win=0 Len=0
1525	28.651227377	10.0.2.15	157.140.2.32	TCP	74	[TCP Retransmission] 34460 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3310145399 TSecr=0 WS=1024
1526	28.651873331	10.0.2.15	157.140.2.32	TCP	74	[TCP Retransmission] 34462 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3310145399 TSecr=0 WS=1024
1527	28.652099834	10.0.2.15	157.140.2.32	TCP	74	[TCP Retransmission] 34464 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3310145400 TSecr=0 WS=1024
1528	28.652479798	10.0.2.15	157.140.2.32	TCP	74	[TCP Retransmission] 34466 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3310145400 TSecr=0 WS=1024
1529	28.652729474	10.0.2.15	108.177.122.94	TCP	54	[TCP Keep-Alive] 33170 → 80 [ACK] Seq=1888 Ack=3509 Win=63791 Len=0
1530	28.653420406	108.177.122.94	10.0.2.15	TCP	60	[TCP Keep-Alive ACK] 80 → 33170 [ACK] Seq=3509 Ack=1889 Win=65535 Len=0
1531	29.739248455	10.0.2.15	157.140.2.32	TCP	74	[TCP Retransmission] 34486 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3310146487 TSecr=0 WS=1024
1532	29.938597978	10.0.2.15	157.140.2.32	TCP	74	[TCP Retransmission] 34490 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3310146686 TSecr=0 WS=1024
1533	29.938747845	10.0.2.15	157.140.2.32	TCP	74	[TCP Retransmission] 34492 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3310146686 TSecr=0 WS=1024
1534	29.938845921	10.0.2.15	157.140.2.32	TCP	74	[TCP Retransmission] 34496 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3310146686 TSecr=0 WS=1024

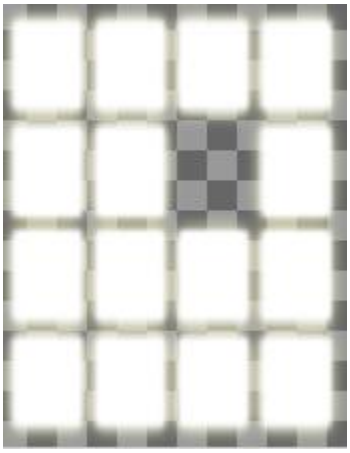
▸ Frame 1526: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0

3. The website is unencrypted because it uses http.



```
0000  52 54 00 12 35 02 08 00  27 46 72 c1 08 00 45 00   RT··5···  'Fr···E·
0010  01 3b f3 13 40 00 40 06  9a ee 0a 00 02 0f 9d 8c   ·;··@·@·  ········
0020  02 20 86 c2 00 50 dd 19  3f 35 00 30 60 e9 50 18   · ···P··  ?5·0`·P·
0030  f9 9c ac e8 00 00 47 45  54 20 2f 6d 69 73 63 2f   ······GE  T /misc/
0040  66 65 65 64 2e 70 6e 67  20 48 54 54 50 2f 31 2e   feed.png   HTTP/1.
0050  31 0d 0a 48 6f 73 74 3a  20 77 65 65 76 69 6c 2e   1··Host:  weevil.
0060  69 6e 66 6f 0d 0a 55 73  65 72 2d 41 67 65 6e 74   info··Us  er-Agent
0070  3a 20 4d 6f 7a 69 6c 6c  61 2f 35 2e 30 20 28 58   :  Mozill  a/5.0 (X
0080  31 31 3b 20 4c 69 6e 75  78 20 78 38 36 5f 36 34   11;  Linu  x x86_64
0090  3b 20 72 76 3a 37 38 2e  30 29 20 47 65 63 6b 6f   ;  rv:78.  0)  Gecko
00a0  2f 32 30 31 30 30 31 30  31 20 46 69 72 65 66 6f   /2010010  1  Firefo
00b0  78 2f 37 38 2e 30 0d 0a  41 63 63 65 70 74 3a 20   x/78.0··  Accept:
00c0  69 6d 61 67 65 2f 77 65  62 70 2c 2a 2f 2a 0d 0a   image/we  bp,*/*··
00d0  41 63 63 65 70 74 2d 4c  61 6e 67 75 61 67 65 3a   Accept-L  anguage:
00e0  20 65 6e 2d 55 53 2c 65  6e 3b 71 3d 30 2e 35 0d    en-US,e  n;q=0.5·
00f0  0a 41 63 63 65 70 74 2d  45 6e 63 6f 64 69 6e 67   ·Accept-  Encoding
0100  3a 20 67 7a 69 70 2c 20  64 65 66 6c 61 74 65 0d   :  gzip,  deflate·
0110  0a 43 6f 6e 6e 65 63 74  69 6f 6e 3a 20 6b 65 65   ·Connect  ion:  kee
```

6.



7. Anyone can see the traffic that goes to and from the website. If someone were to attempt to log in, then their information would be visible.

8. This site uses https. This means that the traffic is encrypted. Wireshark cannot display the pictures.