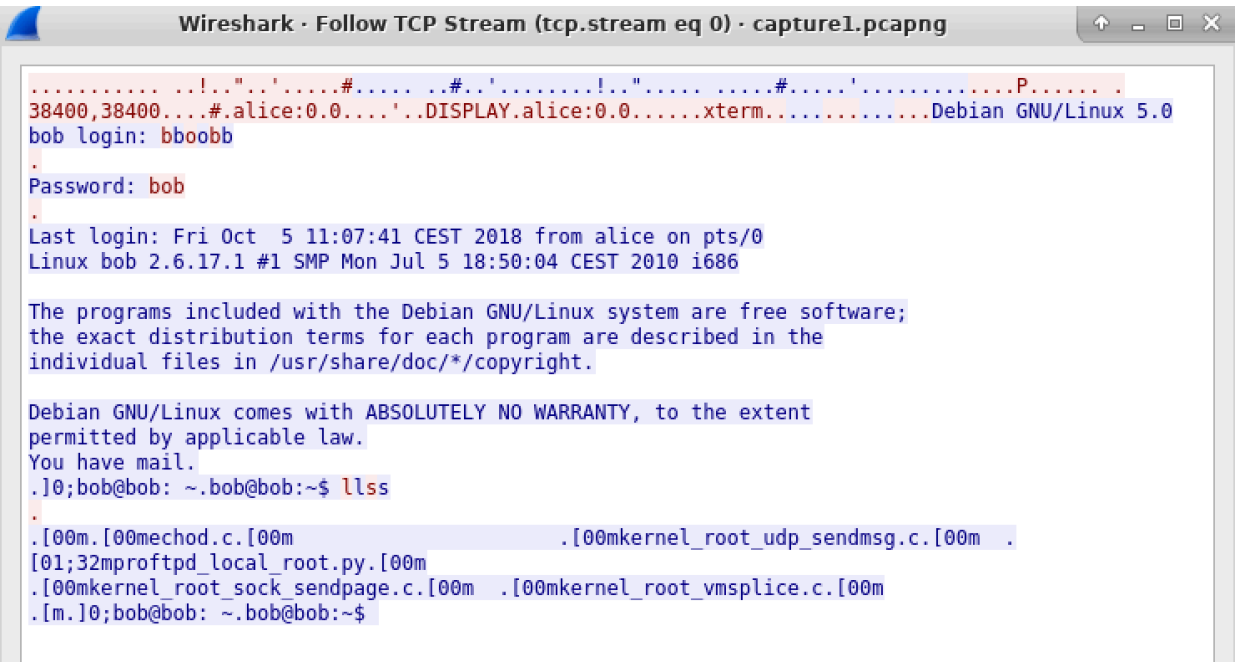
Assignment 2

Part A

When inspecting the packets in wireshark, we find a packet which has Telnet: `Data: Password:`. The next packet would then consist of the password, and through wireshark we analyze the packet and follows the TCP stream. From this we get the login credentials.



Part B

Since TLS uses synchronized encryption, with a private key obtained through a key sharing algorithm, for instance Diffie-Helman, it's not possible to decrypt the traffic.

Part C

When expecting the results from the keylog, we find a HTTP-POST-request, which contains Alice's log-in credentials. Since these are not encrypted on the client side, Mallory can read these as plain-text.

```
mallory [Running]
Applications   *eth0   Terminal - mallory...   Terminal - mallory...   13:16
Terminal - mallory@mallory: ~
File  Edit  View  Terminal  Tabs  Help
Flow Details
2018-10-08 13:15:22 POST https://bob/index.php?option=com_user&task=login
                         ← 301 Moved Permanently text/html 20b 185ms
        Request                Response                Detail
Accept-Encoding:  gzip,deflate
Accept-Charset:   ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive:       115
Connection:       keep-alive
Referer:          https://bob/index.php?option=com_content&view=frontpage
Cookie:           ca835771a6589ed0ff94355cd5a5841f=db9fad7c6cc4460c19374658b4c
                  edd5e
Content-Type:     application/x-www-form-urlencoded
Content-Length:   172
URLEncoded form                                                    [m:auto]
username:                       alice
passwd:                         alice123
remember:                       yes
Login:                          Login
op2:                            login
return:
aW5kZXgucGhwP29wdGlvbj1jb21fY29udGVudCZ2aWV3PWZyb250cGFnZQ==
881bebd3ef599139f4ca9afc8a04506e:1
⇩  [43/44]                                                         [*:8080]
```