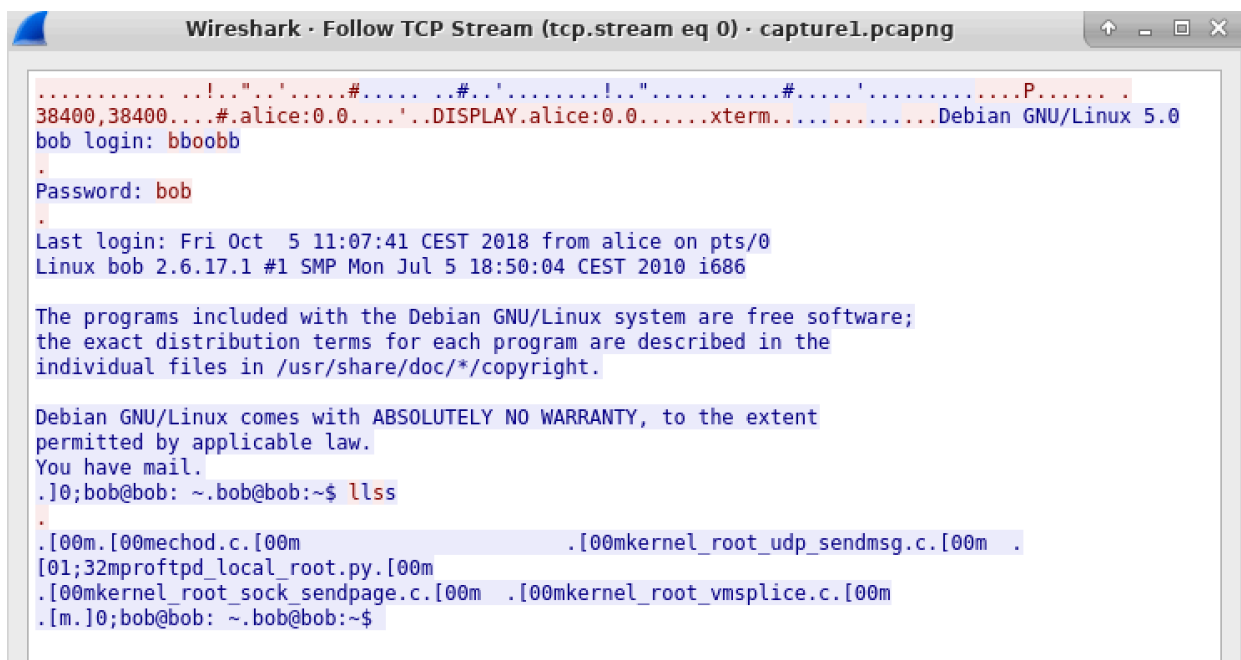


Assignment 2

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 follow the TCP stream. From this we get the login credentials.

A screenshot of the Wireshark 'Follow TCP Stream' window. The title bar reads 'Wireshark · Follow TCP Stream (tcp.stream eq 0) · capture1.pcapng'. The main content area displays a Telnet session transcript. At the top, there's a line of hex and ASCII characters. Below that, the text '38400,38400...#.alice:0.0...'.DISPLAY.alice:0.0.....xterm.....Debian GNU/Linux 5.0' is shown. This is followed by 'bob login: bboobb', 'Password: bob', and 'Last login: Fri Oct 5 11:07:41 CEST 2018 from alice on pts/0'. Then, 'Linux bob 2.6.17.1 #1 SMP Mon Jul 5 18:50:04 CEST 2010 i686' is displayed. A block of text follows: 'The programs included with the Debian GNU/Linux system are free software; the exact distribution terms for each program are described in the individual files in /usr/share/doc/*/copyright.' Below this is 'Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law.' and 'You have mail.'. The prompt '.]0;bob@bob: ~/.bob@bob:~\$' is shown, followed by the command 'llss'. The bottom of the window shows a list of loaded modules: '.[00m.[00mchod.c.[00m .[00mkernel_root_udp_sendmsg.c.[00m .[01;32mproftpd_local_root.py.[00m .[00mkernel_root_sock_sendpage.c.[00m .[00mkernel_root_vmsplice.c.[00m .[m.]0;bob@bob: ~/.bob@bob:~\$'.

```
.....!..".'.....#.....#..'.....!.."......#.....'.....P.....  
38400,38400...#.alice:0.0...'.DISPLAY.alice:0.0.....xterm.....Debian GNU/Linux 5.0  
bob login: bboobb  
Password: bob  
Last login: Fri Oct 5 11:07:41 CEST 2018 from alice on pts/0  
Linux bob 2.6.17.1 #1 SMP Mon Jul 5 18:50:04 CEST 2010 i686  
  
The programs included with the Debian GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
You have mail.  
.]0;bob@bob: ~/.bob@bob:~$ llss  
.  
.[00m.[00mchod.c.[00m .[00mkernel_root_udp_sendmsg.c.[00m .  
[01;32mproftpd_local_root.py.[00m  
.[00mkernel_root_sock_sendpage.c.[00m .[00mkernel_root_vmsplice.c.[00m  
.[m.]0;bob@bob: ~/.bob@bob:~$
```

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=db9fad7c6cc4460c19374658b4cedd5e
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]
```