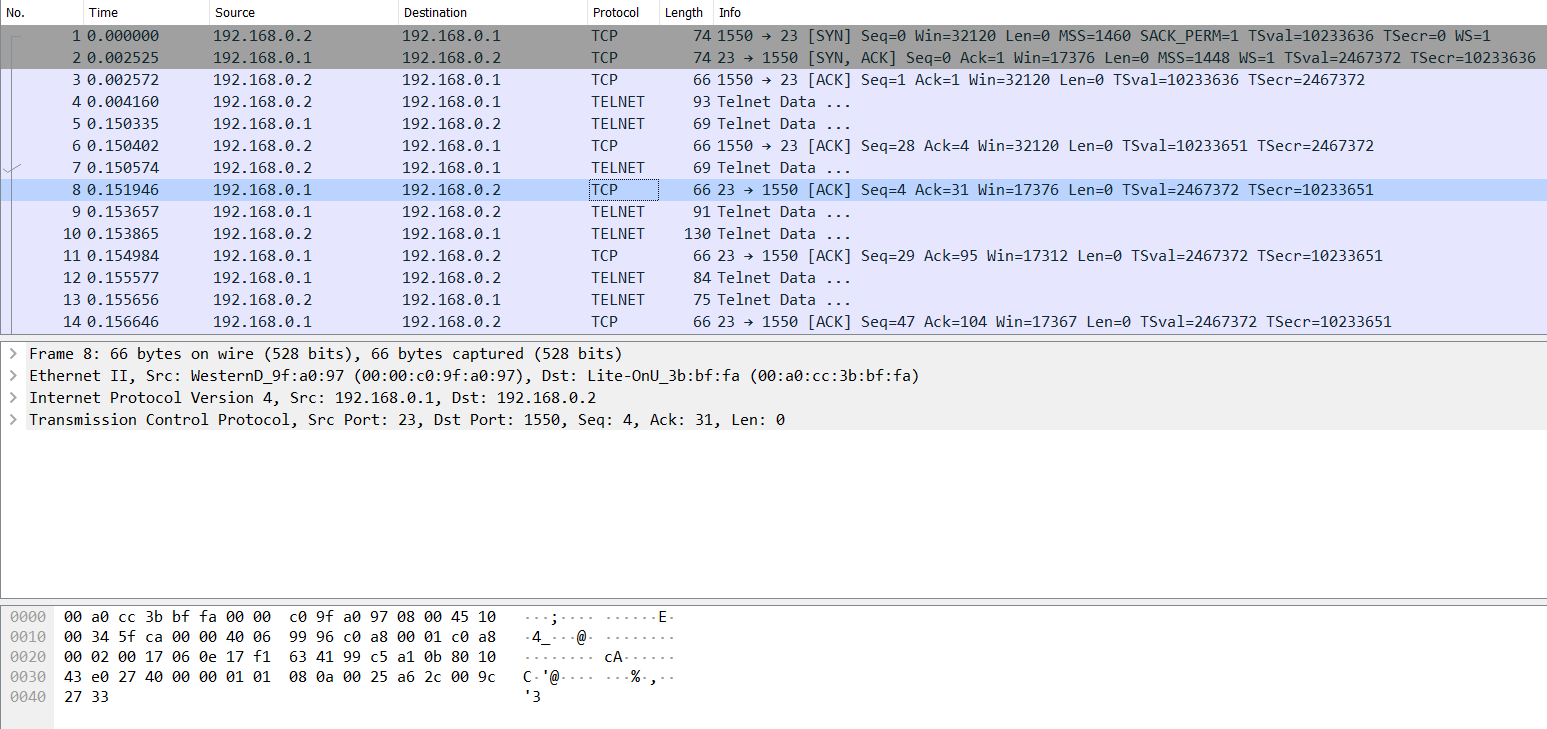
Austin Brown

CPE 434-01

3/16/2021

Lab 10

**Subtask 1**



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.



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

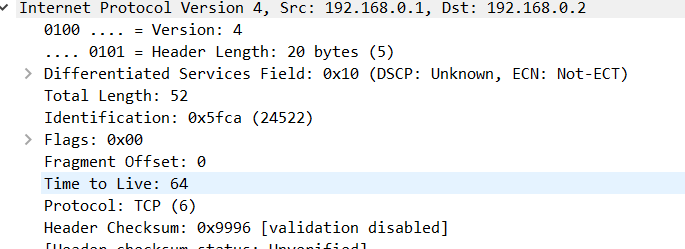


The total transmission time is 39.571274 seconds.

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

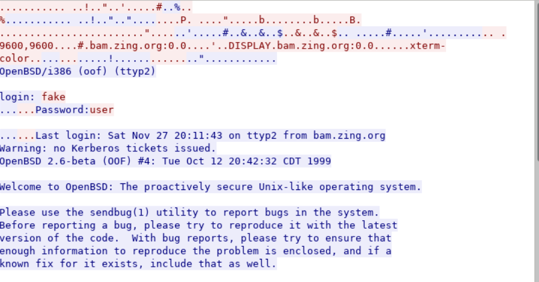
**Subtask 2**

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

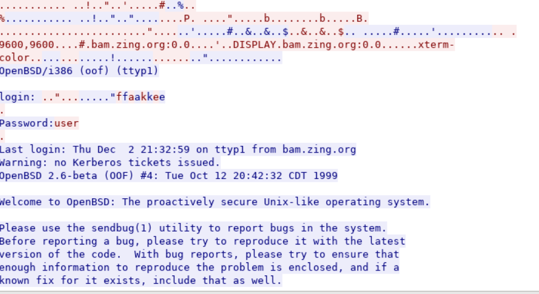


7. The time to live is how long until the frame is discarded. It is 64 as per the last screenshot.

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



9.



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

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

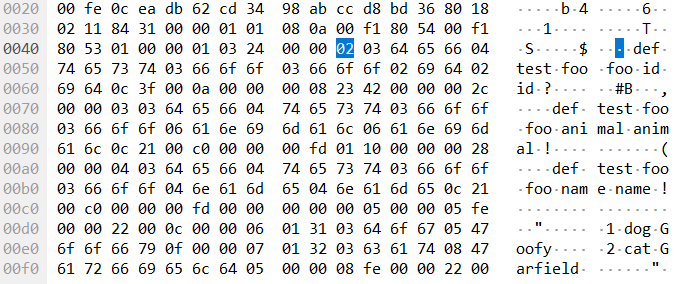
11. UTFP is an encrypted file transfer protocol. It can send to multiple receivers at once. The sender is uftp\_v3\_transfer.pcapng. It has an ip of 10.0.0.1. The receiving group has an ip of 230.4.4.1.

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.

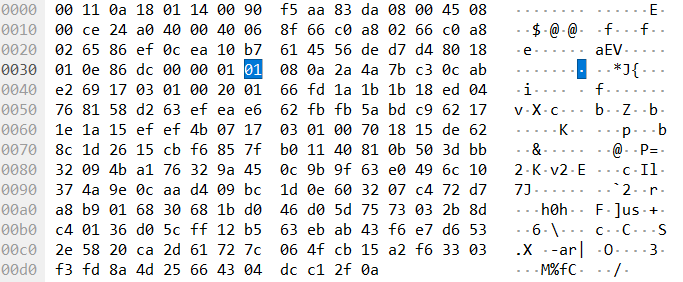
**Subtask 3**

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

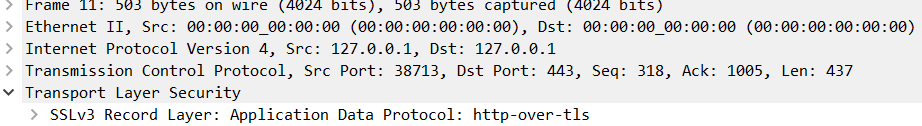
13. This file is not encrypted. I can read data in packet 34.



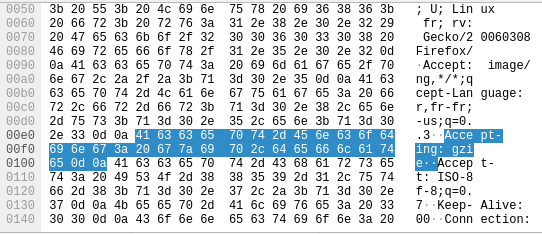
14. This file is encrypted. The file is unreadable.



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



16. The decryption of the file is below.



1. The image is requested in frame 31.

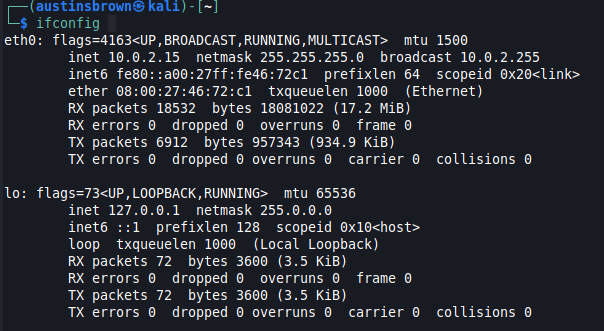
2. It responds with 200.

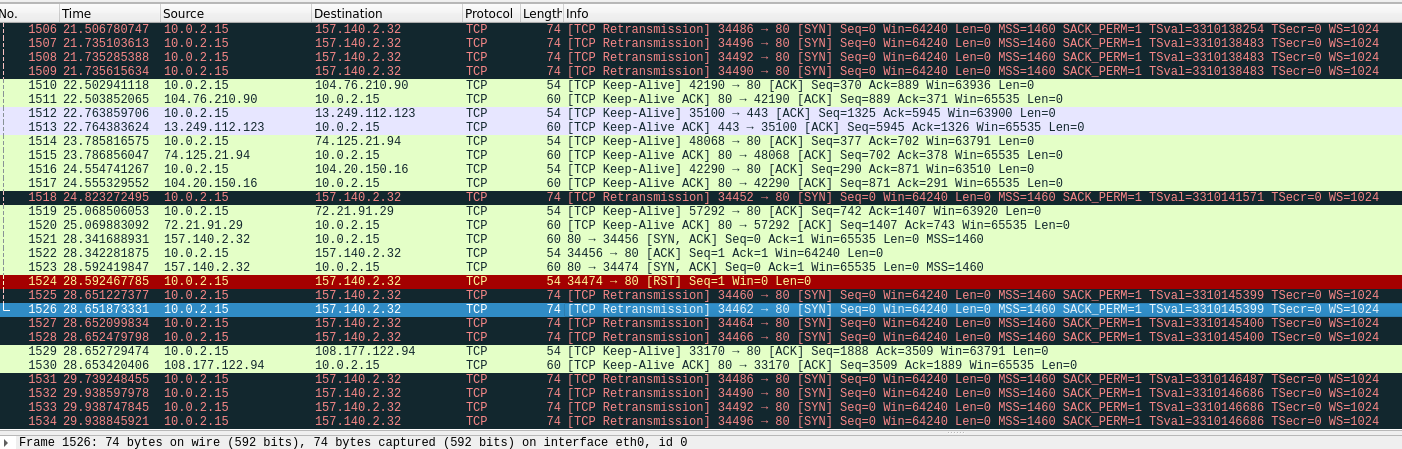
3.



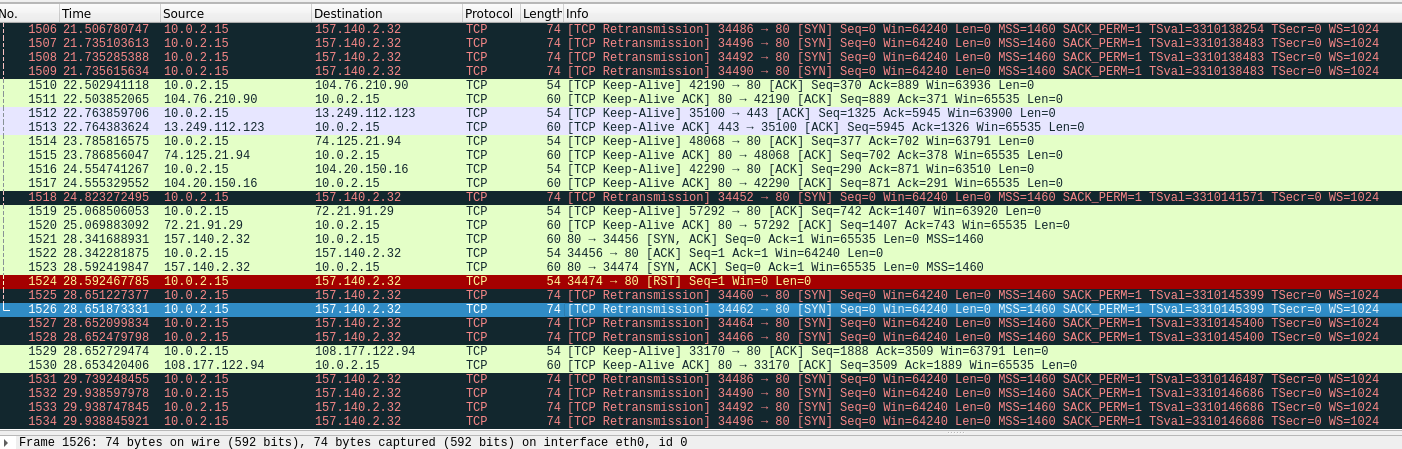
**Subtask 4**

18.

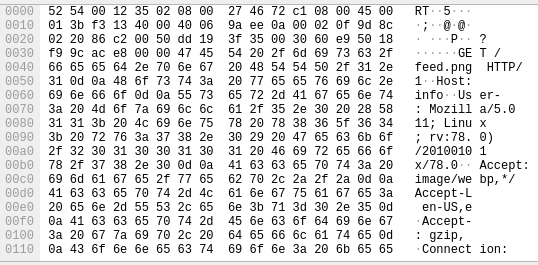




2.

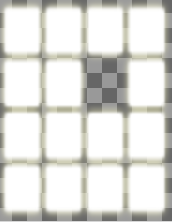


3. The website is unencrypted because it uses http.



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.