**Question 1:** Copy the specific packet frame containing the intercepted password in ASCII format here. To do this, select the packet with the password, right click, and select print to file. In the window, make it output to a file such as wireshark.out to your home directory. Make sure the resulting output contains the packet header information as well as the password field. Copy the results of wireshark.out as your answer.

|  |
| --- |
| No. Time Source Destination Protocol Length Info  23 8.877673398 10.10.10.131 10.10.10.185 FTP 80 Request: PASS seng360  Frame 23: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface 0  Interface id: 0  Encapsulation type: Ethernet (1)  Arrival Time: Oct 5, 2016 14:13:40.604329754 PDT  [Time shift for this packet: 0.000000000 seconds]  Epoch Time: 1475702020.604329754 seconds  [Time delta from previous captured frame: 0.845655451 seconds]  [Time delta from previous displayed frame: 1.903550451 seconds]  [Time since reference or first frame: 8.877673398 seconds]  Frame Number: 23  Frame Length: 80 bytes (640 bits)  Capture Length: 80 bytes (640 bits)  [Frame is marked: False]  [Frame is ignored: False]  [Protocols in frame: eth:ip:tcp:ftp]  [Coloring Rule Name: TCP]  [Coloring Rule String: tcp]  Ethernet II, Src: Dell\_c3:bb:9a (d4:be:d9:c3:bb:9a), Dst: Dell\_c8:b7:09 (f8:b1:56:c8:b7:09)  Internet Protocol Version 4, Src: 10.10.10.131 (10.10.10.131), Dst: 10.10.10.185 (10.10.10.185)  Transmission Control Protocol, Src Port: 37936 (37936), Dst Port: ftp (21), Seq: 22, Ack: 55, Len: 14  File Transfer Protocol (FTP) |

**Question 2:** Investigate the traffic you have captured. Were you able to intercept the password?

Not in plain text, only as encrypted packets.

**Question 3:** What happened in the SFTP traffic? Describe how the secured communications channel was established.

An SSH key exchange was established and then FTP was used over the SSH tunnel using the shared encryption key. The data can only be viewed if the encryption can be broken.

**Question 4:** Since you are using a secure HTTPS connection, take a look at how it is secured. In Chrome, inspect the certificate. Who is verifying mitmproxy's website?

The certificate was issued by Amazon Server CA 1B on Tuesday April 12th, 2016 at 17:00.

**Pre-Question 5:** What's going on here? Can you detect the MITM attack on Wireshark? Can you still access the website?

There is no certificate issued other than the default issued by mitmproxy, this is because mitmproxy is the proxy service that we are routing all traffic through, if there was a MITM we should see a strange name here potentially. Yes, because the proxy service is on 127.0.0.1 (localhost), we can see a lot of connections going to localhost at port 8080 in order for it to then be re-routed. I can still access the website, although I may not want to...

**Question 5:** Suppose you ignored the untrusted certificate warning and logged in to the site. What are the potential consequences of this?

Assuming I was naive and ignored the certificate and just continued to the site, potentially all traffic that I send and receive from that website can be intercepted by a third party.

**Question 6:** Characterize/explain the MITM attack you performed. What things could you be looking for to detect a potential MITM attack on Wireshark?

I can look for a lot of connections going to an unknown IP address that is establishing a connection. I can also notice that the connection at some point is trying to be established using HTTP and not HTTPS.

**Question 7:** Try the above command by substituting https://website.com with <https://www.wikipedia.org/> and then on <https://mitmproxy.org/>. What were the results? Can you tell if either of them are using HSTS?

From Wikipedia, I received “Strict-Transport-Security: max-age=31536000; includeSubDomains; preload”. I can tell that Wikipedia is using HSTS due to the output from the grep. I received no output when running the command with mitmproxy.org, therefore I can assume that they are not using any HSTS.

**Question 8:** Are you able to access Wikipedia through the mitmproxy? Can you override/ignore the error? Why are you getting this type of behavior?

I only get an error page stating that the connection is not private. I cannot ignore the error as it states that wikipedia uses HSTS. It states that this is likely temporary and to try again later.

**Question 9:** Explain in your own words what HSTS is and what it does. How does this help to mitigate HTTPS MITM attacks?

It basically says that all incoming connections MUST be established using HTTPS and never HTTP. As HTTPS can only be established using a valid certificate, a MITM attack that does not use a certificate could only load HTTP and therefore could not load pages that use HSTS.