1. Which web browser and version did you use?

Firefox, 112.0.1

2. Which operating system and version did you use?  
 windows 10 Version 10.0.19045 Build 19045

3. What TLS version is being used by your browser? What is the destination port?  
TLSv1.3, destination port 443

4. How many Cipher Suites were offered by your client? List the text name of the first Cipher  
Suite offered.

17, Cipher Suite: TLS\_AES\_128\_GCM\_SHA256 (0x1301)

5. Find the first TLS message sent from the server back to your browser. What kind of message is it? Which version of TLS is used here?

1.3, change cipher spec application data

6. Which Cipher Suite was accepted by the server? (Hint: multiple TLS records may be  
contained within a single IP packet.)

Cipher Suite: TLS\_AES\_128\_GCM\_SHA256 (0x1301)

7. What digital signature algorithm was used to sign that certificate? (You’ll need to “drill down” to find the answer. Refer to the lecture 27 slides titled “A Public Key Certificate (Excerpts)”).

RSA

8. What organization (certification authority) issued the certificate and signed it?

Entrust

9. Take a look at the URL in your browser. What type of certificate was provided by the server (DV, OV or EV)? (If you can’t figure this out by looking at the URL, review the lecture 26 slide titled “Types of Public Key Certificates”.)  
Ev as it has a padlock

10. Look further down into the certificate and locate subjectPublicKeyInfo. What algorithm was used to generate the Utah Retirement Systems public key? (Hint: be careful to select the correct algorithm. There are several algorithms used in different parts of the certificate.

PKCS #1 RSA Encryption

11. What numbers does that string contain? Use that string of numbers as a Google search  
argument. What do you get from the search?

1.3.6.1.4.1.11129.2.4.2, this leads to finding the reference for the OID

12. What is the ASN.1 data type of that numeric string? If necessary, check the lecture 15 slide  
titled “ASN.1/BER Universal Object Types”. Confirm your answer result by selecting the  
Algorithm ID field in the Packet Details pane and then checking the hex value two bytes  
before the beginning of the string in the Packet Bytes pane below.

unsigned int

13. In the Packet List pane, locate the first packet that contains TLS Application Data (identified  
as such in the Wireshark “Info” column). Highlight the Encrypted Application Data field in the  
Packet Details pane below. You’ll observe that (surprise!) you cannot read the data in the  
Packet Bytes pane at the bottom. What does this tell you about the “protocol stack”  
relationship between TLS and Npcap (or libcap)?

Npcap does not have access to the data of TLSGraphical user interface, text, application

Description automatically generated