Lab 7: VPNs

15 points

**Due: Before class on 4/13/2022**

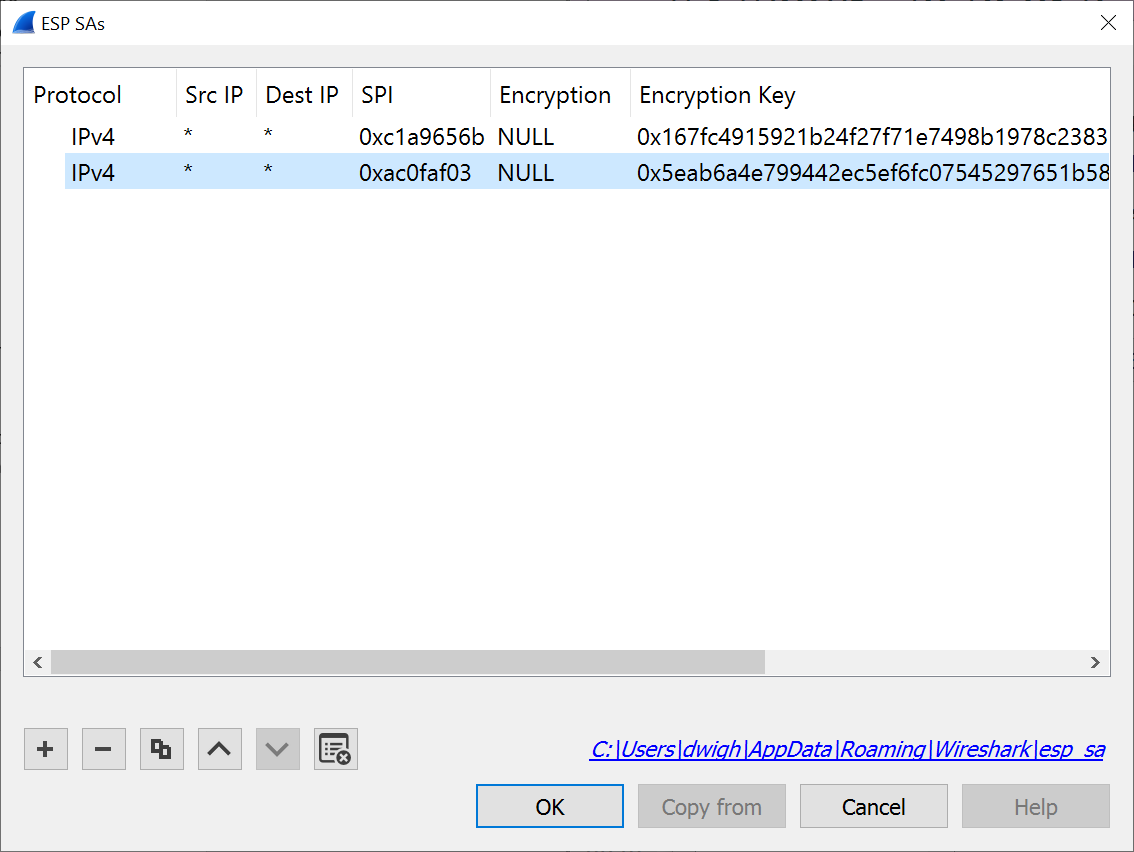
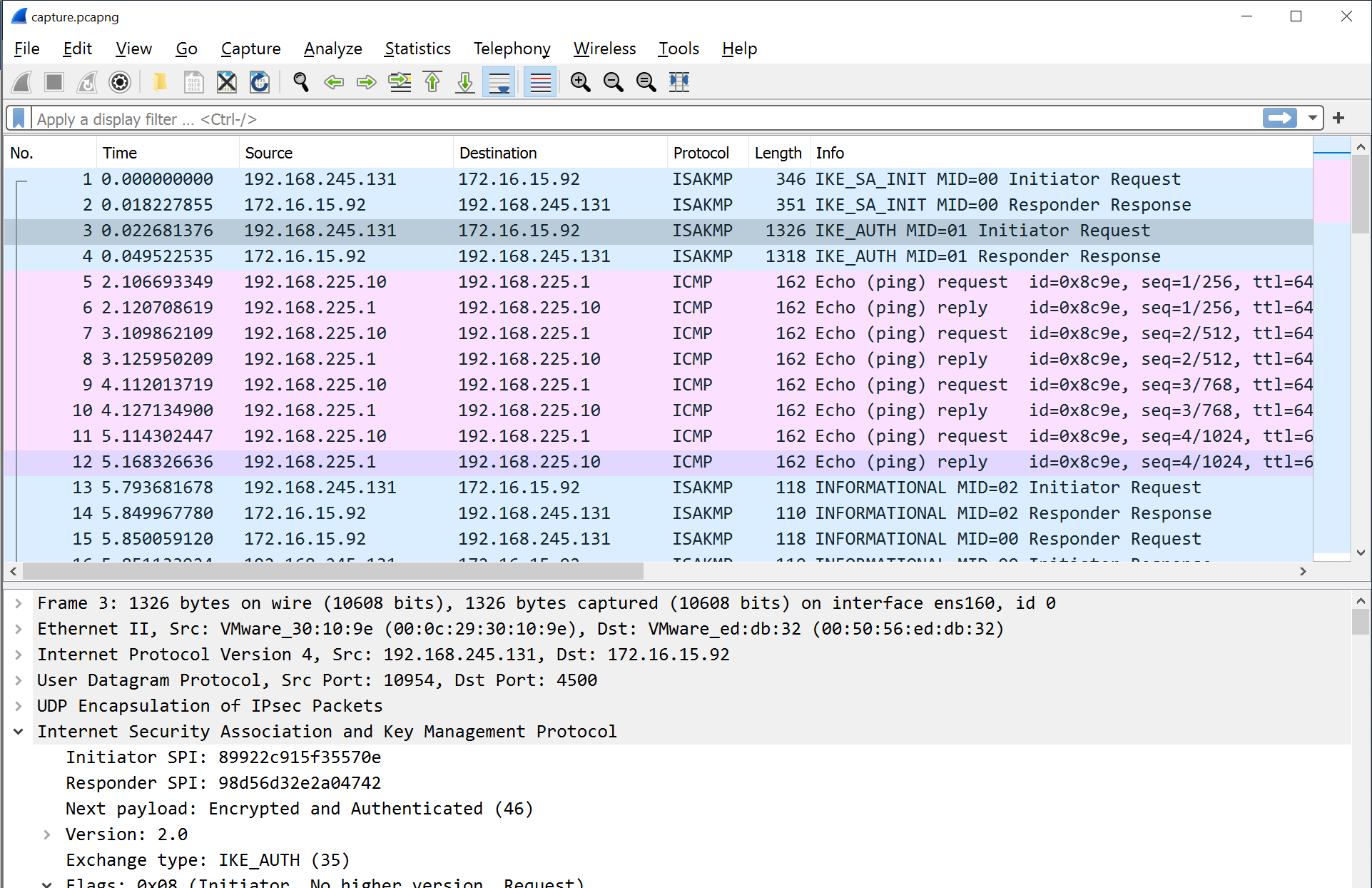
**Objectives of this lab:**

1. Interpret an IPSec VPN session using a pcap file
2. Research aspects of VPN technology

# PCAP file

For the following questions open the file **ipsec.pcapng** from the D2L lab.

The PCAP file contains the traffic of several IPSec sessions being created. As discussed in class, in order to establish a tunnel both sides need to establish a Security Associataion (SA), or the shared attributes that will be used to generate the tunnels.

1. The first step in establishing the IKE phase 1 tunnel is for the sender/initiator to send a **proposal** to the receiver that includes the parameters that they would like to use. The proposal parameters can be found in packet 1 (the IKE\_SA\_INIT Initiator Request packet). Expand the details for the ISAKMP protocol and look under the Payload headers for Security Association > Prposal > Transform (you should find 3). What are the 3 parameters the initiator specifies? [3 points]  
   1. **Encryption Algorithm: AES-GCM with 16 octet ICV**
   2. **Pseudo-random Function: PRF\_HMAC\_sha2\_256**
   3. **Diffie-Hellman Group (include the number in parentheses): 256bit random ECP group**
2. The second step is for the receiver to decide what parameters to use. The initiator may send multiple options and the receiver can choose which they prefer. [1 point]  
   1. **Are the parameters sent back by the responder the same as your answers in question #1? If not, what parameters did the responder choose? Yes they are the same**
3. Now that we have the parameters for the IKE phase 1 tunnel we can create the IKE phase 2 tunnel. As part of the IKE phase 2 tunnel (labelled IKE\_AUTH in Wireshark) the initiator and responder validate the authenticity of the other side (to confirm they are allowed to create this tunnel). But we can’t actually see that traffic because it’s now been encrypted inside the IKE phase 1 tunnel. If we know the encryption keys and the algorithm we can have Wireshark decrypt this traffic for us. In Wireshark go to Edit > Preferences, click the dropdown arrow next to Protocols, then scroll down and click ESP. Check the box next to “Attempt to detect/decode encrypted ESP payloads”, if it’s unchecked. Click the “Edit” button next to ESP SAs, you should see a window that looks like the following:  
     
     
     
   Click the **+** icon in the lower left and add the following 2 entries:  
     
   Protocol: IPv4  
   Src IP: \*  
   Dest IP: \*  
   SPI: 0xc1a9656b  
   Encryption: [your answer from 1a]  
   Encryption Key: 0x167fc4915921b24f27f71e7498b1978c238398d6  
   Authentication: NULL  
     
   Protocol: IPv4  
   Src IP: \*  
   Dest IP: \*  
   SPI: 0xac0faf03  
   Encryption: [your answer from 1a]  
   Encryption Key: 0x5eab6a4e799442ec5ef6fc07545297651b5832fc  
   Authentication: NULL
4. After clicking OK, scroll to ISAKMP in the Protocol list and select it. Click the “Edit” button next to “IKEv2 Decryption Table”. Click the **+** icon in the lower left and add the following entry:  
     
   Initiator’s SPI: 89922c915f35570e  
   Responder’s SPI: 98d56d32e2a04742  
   SK\_ei: f49c0d53899c8aef4435e2850619825dacc1c8b4bfd636f7175032cfbe4c57db8b7b260f  
   SK\_er: 42e53af4eabccaabf10ad37da3b980edc5af5a4c742fd47a29b4341f7847caf92ccacf3d  
   Encryption algorithm: [your answer from 1a]  
   Integrity algorithm: NONE  
     
   Click “OK” to close the decryption table. Click “OK” again to close the Preferences window. You should see your Wireshark list update and the list of entries should look a little different.  
     
   
5. Selecting the 3rd packet (labelled IKE\_AUTH Initiator Request) you should now have a new dropdown in the Details section called “Decrypted Data”. As we discussed in class there are 2 main methods of authentication. **Does this session use a pre-shared key or a certificate to authenticate?** [1 point]

Certificate

1. The sender also includes the range of IP addresses that should be allowed to send traffic through the tunnel in a section called “Traffic Selector”. **What is the allowed IP address range sent?** (Hint: There are 2 ranges in the traffic, I’m looking for the one that begins 192.168.) [1 point]

192.168.225.0 – 192.168.225.255

1. As part of the response (in the packet labelled IDE\_AUTH Responder Response) there are a number of configuration attributes aptly included in a section called “Payload: Configuration”. **What is the IP address and subnet mask returned?** (Hint: There are several IP sections, you’re looking for one that isn’t 0.0.0.0) [2 points]

192.168.225.10

255.255.255.0

1. After the tunnel is established traffic is sent over the tunnel. **What type of traffic is sent over the tunnel, what is the source IP address, and what is the destination IP address?** (Hint: it should be the only traffic in the capture that isn’t ISAKMP or ESP in the protocol column, it will only show up after you’ve decrypted the traffic.) [3 points]

Source address: 172.16.15.92

Destination: 192.168.245.131

Type of traffic: UDP

1. IPSec uses an authenticated hash to ensure that data sent over the connection hasn’t been modified. Previously we learned about checksums which are used in TCP and UDP. **Why is a hash better than a checksum for ensuring data hasn’t been modified?** [1 point]

It’s much harder to create a file with a given encrypted hash

1. **What is the difference between hashing and encryption?** [1 point]

Hashing maps data to a fixed length integer or whatever. A hash couldn’t be turned back into the original data.

Encryption uses a key to obfuscate data with the intent decrypting it later back to the original data.

1. There are several places in the capture where a *nonce* is passed back as a parameter. **What is a nonce and what is it used for?** (There are multiple uses for a nonce, you can provide any use, not just its use in IPSec). [2 points]  
   A number used once typically based on time to ensure that a value isn’t used more than once