Download the 5 packet capture files and use Wireshark to analyze the file and answer the following questions and use different nmap scans types seen in the instructional video.

**Capture1.pcapng**

1. What type of scan is most-likely to have been run?   
   It looks like a ping sweep, based on the ICMP protocol all coming from 1 address
2. What is the exact syntax of the command?  
   nmap -sT 10.10.10.10/255
3. What is the result of the scan?  
   ACK response is returned by listening hosts
4. What are the machine types of vendors of machines seen in the scan?  
   The scanning device is a Gateway 2000 device – likely a PC or laptop. The target was a Cisco device, likely a router. Cisco makes other network machines as well.
5. What is the MAC address of the machine that is running nmap?   
   00:e0:b8:af:14:cb
6. What is the IPv4 address of the machine that is running nmap?  
   10.10.10.5
7. What is the IPv6 address of the machine that is running nmap? \*bonus question  
   fe8: :c14:ca44:6c33:171
8. List the four MAC addresses of devices on the network:  
   00:1b:2b:2f:b1:dc, 00:e0:b8:94:98:0b, 00:e0:b8:af:14:cb, 3.473040, 8:27:eb:1a:17:61

**capture2.pcapng:** This is an OS scan. Look at the file and answer the questions

1. What is the exact syntax of the command?  
   nmap -O 10.10.10.6
2. If this is between two machines on the local network, why are there packets from other hosts?  
   Because WireShark is monitoring the entire network
3. According to the capture file, what service(s) are responding on the target?  
   TCP
4. Which packet numbers are checking the Telnet service?   
   23

**capture3.pcapng**

1. What type of scan is most-likely to have been run?  
   Click here to enter text.
2. What is the major clue to the type of scan?   
   Click here to enter text.
3. What is the exact syntax of the command?   
   Click here to enter text.
4. According to the file, what port(s) are listening on the target?  
   Click here to enter text.

**capture4.pcapng**

1. What type of scan is most-likely to have been run?   
   SYN Scan
2. What is the major clue to the type of scan?   
   It completes the SYN with ports that ACK, and resubmits when it receives RST responses.
3. What is the exact syntax of the command?  
   nmap 10.10.10.4
4. What common service and port number is active on 2 of the devices, and which are the two?  
   DHCP/BOOTP on ports 67/68 Both used by 10.10.10.1 and 10.10.10.5

**capture5.pcapng:** This is a version scan. Look at the file and answer the questions

1. What is the exact syntax of the command?   
   nmap -sV 10.10.10.4
2. The target represents an Internet facing server, what service(s) are running on that server?   
   NBNS port 137, BROWSER port 138, UDP port 3456
3. What operating system is the target running?  
   Windows
4. What protocol is running that shows the OS of the target?   
   3389 RDP
5. What is the hostname of the target?   
   DHSCTE
6. What protocol is running that shows the hostname of the target?  
   Netbio
7. What is the hostname of the machine running nmap?  
   cte-tablet
8. What service is allowing the hostname of the machine running nmap to be seen?   
   DHCP