**CSC138-01 Lab1**

**303833894 Yunjeong Lee**

Task 4: Record your observation and answer the following questions.

1. List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window? Attach screen shots of your observation. What are these protocols used for?   
   텍스트, 전자제품, 스크린샷, 소프트웨어이(가) 표시된 사진

   자동 생성된 설명  
   There are DNS, TCP, and HTTP. First, DNS is used for translating human-readable domain names into IP addresses that are used by computers to communicate over a network. TCP is a core protocol of the Internet Protocol (IP). It provides reliable, ordered, and error-checked delivery of packets, making it suitable for applications. HTTP is the protocol used for transmitting web pages, images, videos, and other resources over the World Wide Web. It defines how messages are formatted and transmitted, as well as how web servers and browsers should respond to various commands.
2. On the display filter specification bar, type http and press enter. Attach screenshot of your result?   
   텍스트, 전자제품, 스크린샷, 소프트웨어이(가) 표시된 사진

   자동 생성된 설명
3. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time Display Format, then select Time-of-day.) You may see several get request and Ok messages, you can pick any and record your finding. Attach a screenshot. Answer: some milliseconds.  
   텍스트, 전자제품, 스크린샷, 소프트웨어이(가) 표시된 사진

   자동 생성된 설명  
   It took about 351.316876 milliseconds, from 20:00:52.814072185 to 20:00:53.165389061.
4. What is the Internet address of the www.neverssl.com? What is the Internet address of your computer? Attach a screenshot for each of the answers.  
   텍스트, 전자제품, 스크린샷, 소프트웨어이(가) 표시된 사진

   자동 생성된 설명  
   The Internet address of my computer is 192.168.239.128, which is the source of GET request. 텍스트, 전자제품, 스크린샷, 소프트웨어이(가) 표시된 사진

   자동 생성된 설명  
   The Internet address of the [www.neverssl.com](http://www.neverssl.com) is 34.223.124.45, which is the source of 200 OK response.
5. What HTTP status codes do you see in the “info” column? What is the purpose of status codes?  
   We can see 200 OK, 301 Moved Permanently in the “info” column. The purpose of status codes is to provide a concise way for the server to communicate the outcome of the client’s request. This helps the client understand what happened with the request, enabling appropriate actions to be taken, such as displaying a webpage, redirecting to a new location, or displaying an error message. It helps in debugging, troubleshooting, and understanding the current state of the communication between the client and the server. The HTTP status code 200 signifies a successful response from the server. It indicates that the request was received, understood, and accepted, and the server is returning the requested resource or confirming the success of the operation. The HTTP status code 301 indicates a permanent redirection. It informs the client that the requested resource has been permanently moved to a new URL. The client should use the new URL for all future requests to that resource.
6. Print the two HTTP messages (GET and OK) referred to in question 3 above. To do so, select Print from the Wireshark File command menu, and select the “Selected Packet Only” and “Print as displayed” radial buttons, and then click OK. Attach screenshots of the printed packets.  
   텍스트, 스크린샷, 문서, 폰트이(가) 표시된 사진

   자동 생성된 설명텍스트, 스크린샷, 문서, 폰트이(가) 표시된 사진

   자동 생성된 설명

Task 6: Answer questions on Tshark Task 5

1. How many packets can you see when you run the command mentioned in option ‘c’. What protocols did you observe in the displayed window? Attach a screenshot.  
   텍스트, 스크린샷, 폰트이(가) 표시된 사진

   자동 생성된 설명  
   There are 10 packets.  
   There are SNMP, TCT, HTTP protocols.
2. How many packets are sourced from host 192.168.1.102? (You can get your answer when you run command shown in point ‘d’)   
   텍스트, 스크린샷이(가) 표시된 사진

   자동 생성된 설명  
   There are 27 packets.
3. How many packets are destined to the host 134.241.6.82?  
   텍스트, 스크린샷, 폰트이(가) 표시된 사진

   자동 생성된 설명  
   There are 13 packets.
4. Attach screenshot of output from task 5.f.  
   텍스트, 스크린샷, 폰트이(가) 표시된 사진

   자동 생성된 설명