**HW 1**

**PART 1: WireShark**

1. Identify the IP address of each host that communicated on the network during this time. What are their associated HW/Ethernet addresses?  
   *10.1.1.101 00:04:e2:22:5a:03  
   209.225.0.6 00:05:5d:6f:d7:c1  
   209.223.11.237 00:05:5d:6f:d7:c1*

*10.1.1.1 00:c0:df:20:6c:df*

1. How many unique TCP sessions were used during this time?   
   *19*
2. Use the Display Filter bar to query for specific packet features.  
   Provide the syntax needed to perform the following queries:
   1. Identify all packets with a source IP address of 10.1.1.1   
      *ip.src == 10.1.1.1*
   2. Identify all packets with an IP of 10.1.1.1 and a TCP port of 3189   
      *ip.src == 10.1.1.1 and tcp.port == 3189*
3. View the TCP stream associated with the IP address 10.1.1.1 and TCP port 3189 number (use “Follow TCP Stream”). What type of information was requested/sent?   
   *HTTP GET request was sent to the http://10.1.1.1/… and a JPEG JFIF image was returned along with a 200 OK status.*
4. 5. Is it ethical to run Wireshark on a network where you don’t have previous authorization to do so? Explain your answer.   
   *Not only is it unethical, it can also be illegal. One can obtain data to analyze network traffic, but should not be used on networks in which explicit permission to monitor has not been given.***PART 2: Mininet**
5. The following command can be used to test the reachability of each host. How many messages were sent?   
   $ pingall   
   *56/56*
6. The following command can be used to test the performance between hosts. What does the iperf tool to and what does it tell you?   
   $ iperf h2 h4   
   *Tests TCP bandwidth between 2 hosts; here, 43.1 Gbps up/43.1 Gbps down*
7. Use the following command to get the IP addresses for the following hosts: h1, s1. What are the addresses?   
   $ <host> ifconfig -a   
   *H1-ipv4 10.0.0.1  
   H1-ipv6 fe80::94dd:16ff:fea9:9b05  
   S1\_eth1 fe80::74ab:b7ff:fece:8c15  
   S1\_eth2 fe80::c8c0:e5ff:fec7:f757*
8. Draw the topology for this network, including all hosts and switches (you can ignore any “controllers” for now). The following command should be helpful:   
   $ net   
    *S1  
    -----------------------------------  
    | |  
    S2 S5  
    ------------------ -----------------  
    | | | |  
    S3 S4 S6 S7  
    --------- --------- --------- ---------   
    | | | | | | | |  
    H1 H2 H3 H4 H5 H6 H7 H8*
9. Run the following commands. The first starts wireshark on h1 (you’ll have to then choose the appropriate network interface), the second creates a simple web server on h2, while the third creates a simple web requests between h1 and h2. Identify how many messages are associated with this connection, and what are their associated protocols.   
   $ h1 wireshark &   
   $ h2 python -m SimpleHTTPServer 80 &   
   $ h1 wget h2 &  
   *11 total messages: 9 TCP, 2 HTTP*