

Cyberpaths

- Network Traffic & Denial of Service Lab -

Lab Goals

1. Getting used to work with GENI
2. Learn how to connect to your GENI nodes using PuTTY
3. Obtain an experiential perspective of a DDoS attack
4. Learn how to save network traffic logs in a pcap file to read with Wireshark
5. Use Wireshark to generate a graph from your network traffic logs

Prerequisites

1. You will need basic command line knowledge to complete this lab. Codecademy has a great [tutorial](#) on this topic.
2. In this lab, you will implement a computer network attack, Denial of Service (DoS). This attack is designed to deprive services, such as web content, from legitimate users. From Wikipedia: "In computing, a denial-of-service attack is a cyber-attack where the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet." You can watch a [video](#) about this attack and [read more](#) about recent DDoS attacks using the Internet of Things interconnected devices.
3. To analyze the computer network traffic from this attack, we will use tool called [Wireshark](#). Here is a quick [video tutorial](#) for this tool, or you can watch the video below, made by College of Charleston undergrad Thomas Setzler.
4. Iperf is a tool that is used through command line to generate computer network traffic that resembles regular usage of a computer network. You can read more about this tool [here](#).
5. Hping3 is another computer networking tool that you will use. This tool, with the proper command line options, can generate a flood of computer network traffic that can overwhelm and take over networking resources. You can read more about this tool [here](#).

Setup

1. If your instructor has already provided you with a topology, you may move on to Part 1. Otherwise, complete the following instructions to set up your topology.
2. Create a new slice under the corresponding project
3. Click the "Add Resources" button located in the page of your newly created slice
4. Click the URL option

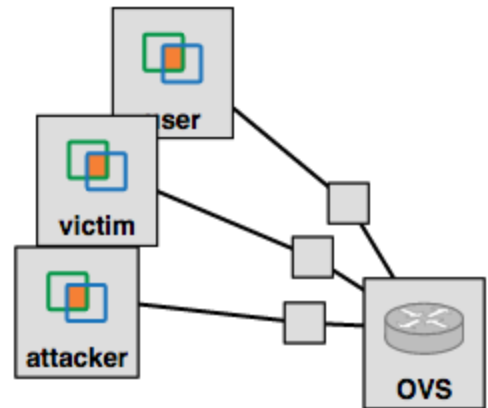
The screenshot shows a web interface for configuring an RSpec. On the left, there is a vertical orange sidebar with three sections: 'Choose RSpec', 'Save RSpec', and 'Editor Ops'. The main area on the right has a top row of radio buttons labeled 'Portal', 'File', 'URL', and 'Text Box'. The 'URL' radio button is selected, and a red arrow points to it. Below the radio buttons is a text input field labeled 'Select existing:'. Underneath that, it says 'This RSpec is valid.' Below the input field is a 'Download RSpec:' label followed by a 'Download' button. At the bottom, there is a row of buttons: 'Expand', 'Duplicate Nodes only', 'Auto IP', and 'Add Global Node'.

5. Paste on the input box the following link: <http://mountroudoux.people.cofc.edu/CyberPaths/files/denialOfServiceLevel1.txt>
6. Then click on the "Select" button

This screenshot shows the same RSpec configuration interface as the previous one, but with the 'URL' radio button now selected (indicated by a blue dot). The 'Load from URL:' label is followed by a 'Select' button and a text input field containing the URL 'http://mountroudoux'. Below this, it says 'This RSpec is valid and bound.' The 'Download RSpec:' label and 'Download' button are still present. The bottom row of buttons ('Expand', 'Duplicate Nodes only', 'Auto IP', 'Add Global Node') remains the same.

7. Your topology should now load and look like similar to this

Clemson InstaGENI



8. Now click on "Clemson InstaGENI" and select one of aggregates on the left that is available and then reserve the resources

X

Name

Site 1

Site

(any)

(any)

[Wisconsin InstaGENI](#)

✓

[CENIC InstaGENI](#)

✓

[Clemson InstaGENI](#)

✓

[Cornell InstaGENI](#)

✓

[GPO InstaGENI](#)

✓

[Illinois InstaGENI](#)

✓

[Kentucky InstaGENI](#)

✓

[Kentucky PKS2 InstaGENI](#)

✓

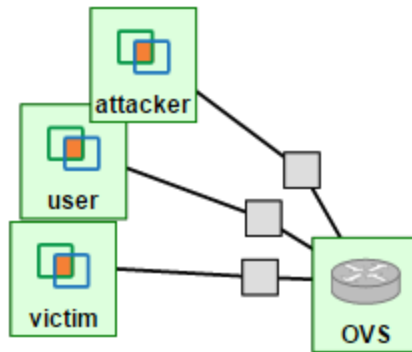
[Kentucky ProtoGENI](#)

✓

[MAX InstaGENI](#)

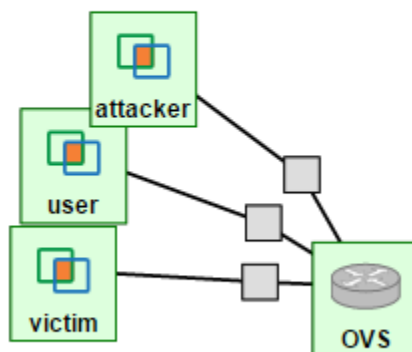
✓

9. Then wait some time until all your resources are ready, you can check the status of these by going to the page of your slice. If the background color of a given node is grey, it means that such node is not available yet; if it is green, it means that it is ready. Just like so:



Part 1: Retrieving your computer network topology, describing it and understanding it.

1. Log into the GENI Portal using your login credentials. Go to "Home", "Slices", and click on the slice that corresponds to your lab. Describe the names of the machines that you see in the topology and how they are connected.
2. Based on the names on each machine that is in your topology, describe what you think each machine will do. (You will need to make an educated guess.)



3. The OVS in your topology is going to play the role of a network switch. Describe in your own words what you think a network switch is and how it works

Part 2: SSHing/Logging into your nodes.

1. SSH stands for Secure Shell. SSH is a UNIX-based command interface and protocol for securely getting access to a remote computer. It is widely used by network administrators to control web servers and other kinds of servers remotely.
2. What is a network protocol and why do we need a protocol like SSH? (You may search for the answer but remember to include sources.)
3. Take a look at your topology. You should see four machines. These machines include "user", "victim", "attacker" and "OVS".
 - **"user"** machine: acts as a regular user on a network; like a user that browses the internet.
 - **"victim"** machine: acts as a victim of a Denial of Service (DoS) attack.
 - **"attacker"** machine: acts as a malicious user and creates and sends DoS attack to the victim.
4. On the GENI Portal, click on the machine in your topology called "user". You will need to open an SSH connection to this user node. If you do not know how to do this, follow the "HelloGENI" tutorial for [Windows users](#) or [Mac users](#).
5. Repeat the process and open ssh connection with all the nodes in your topology.

Part 3: Running your first experiment.

1. Go to the terminal that corresponds to the "user" machine. Type: ping victim and hit enter on your keyboard.

```
castillo@user: ~  
* Documentation: https://help.ubuntu.com/  
New release '14.04.1 LTS' available.  
Run 'do-release-upgrade' to upgrade to it.  
  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
castillo@user:~$ ping victim  
PING victim-link-1 (10.10.2.1) 56(84) bytes of data.  
64 bytes from victim-link-1 (10.10.2.1): icmp_req=1 ttl=63 time=1.16 ms  
64 bytes from victim-link-1 (10.10.2.1): icmp_req=2 ttl=63 time=0.708 ms  
64 bytes from victim-link-1 (10.10.2.1): icmp_req=3 ttl=63 time=0.770 ms  
64 bytes from victim-link-1 (10.10.2.1): icmp_req=4 ttl=63 time=0.779 ms  
^C  
--- victim-link-1 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3004ms  
rtt min/avg/max/mdev = 0.708/0.855/1.166/0.184 ms  
castillo@user:~$
```

2. Press both the Ctrl key and C key together. This will cancel the ping command as we do not want this to run forever. Copy three lines that were printed on the terminal after you pressed enter.
3. Go to the terminal that corresponds to the "victim" machine. Type: `sudo tcpdump -i eth1` and hit enter on your keyboard.
4. Go to the terminal that corresponds to the "user" machine. Type: `ping victim` and hit enter on your keyboard.
5. After a few seconds, press both the Ctrl key and C key together on both terminals.

```
castillo@victim: ~
12:21:54.613801 IP user-link-0 > victim-link-1: ICMP echo request, id 3243, seq 2, length 64
12:21:54.613837 IP victim-link-1 > user-link-0: ICMP echo reply, id 3243, seq 2, length 64
12:21:55.615444 IP user-link-0 > victim-link-1: ICMP echo request, id 3243, seq 3, length 64
12:21:55.615480 IP victim-link-1 > user-link-0: ICMP echo reply, id 3243, seq 3, length 64
12:21:56.617349 IP user-link-0 > victim-link-1: ICMP echo request, id 3243, seq 4, length 64
12:21:56.617380 IP victim-link-1 > user-link-0: ICMP echo reply, id 3243, seq 4, length 64
12:21:57.619036 IP user-link-0 > victim-link-1: ICMP echo request, id 3243, seq 5, length 64
12:21:57.619063 IP victim-link-1 > user-link-0: ICMP echo reply, id 3243, seq 5, length 64
12:21:58.620759 IP user-link-0 > victim-link-1: ICMP echo request, id 3243, seq 6, length 64
12:21:58.620834 IP victim-link-1 > user-link-0: ICMP echo reply, id 3243, seq 6, length 64
12:21:58.621175 ARP, Request who-has OVS-link-1 tell victim-link-1, length 28
12:21:58.621396 ARP, Reply OVS-link-1 is-at 02:b9:aa:f4:f9:0f (oui Unknown), length 28
```

6. Take a look at the terminal that corresponds to the "victim" machine. Copy the lines that were printed on the "victim" terminal. Do you think these lines have any relation to the command entered on the "user" machine terminal?
7. Take a look at the terminal that corresponds to the "user" machine. Copy the lines that were printed on the "user" terminal. What time units are used in the ping statistics?
8. What is RTT? (You may search the abbreviation but include sources.)
9. Do the ping statistics from 7 indicate a fast or slow network? (You may search network speeds for comparison but include sources.)
10. ***The ping command is a query, or a question, to another computer on a network. In this case the question is sent from the "user" machine to the "victim" machine to determine whether there is a connection.***

Part 4: Running an attack, observing user traffic, collecting and analyzing data.

1. Go to the terminal that corresponds to the "victim" machine. Type: `iperf -s` and hit enter on your keyboard.
2. Go to the terminal that corresponds to the "user" machine. Type: `iperf -c victim` and hit enter on your keyboard.


```
castillo@victim: ~  
castillo@victim:~$ iperf -s  
-----  
Server listening on TCP port 5001  
TCP window size: 85.3 KByte (default)  
-----  
[  4] local 10.10.2.1 port 5001 connected with 10.10.1.1 port 53627  
[ ID] Interval          Transfer      Bandwidth  
[  4]  0.0-10.1 sec    121 MBytes   100 Mbits/sec  
█
```

3. Iperf is software that tests the performance of a machine; how fast it serves network requests. The "victim" machine is running a server and the "user" machine is running a client with requests to the server on the "victim" machine.
4. Wait a few minutes then copy the lines that were printed on the "user" terminal.
5. Go to the terminal that corresponds to the "victim" machine and press both the Ctrl key and C key together.
6. Type: `ping ovs` and hit enter on your keyboard. Note the numbers and periods inside the parenthesis. There should be 4 numbers separated by 3 periods. For example, inside the parenthesis for me contains "10.10.2.2".

```
castillo@victim: ~  
castillo@victim:~$ iperf -s  
-----  
Server listening on TCP port 5001  
TCP window size: 85.3 KByte (default)  
-----  
[  4] local 10.10.2.1 port 5001 connected with 10.10.1.1 port 53627  
[ ID] Interval      Transfer    Bandwidth  
[  4]  0.0-10.1 sec  121 MBytes  100 Mbits/sec  
^C  
castillo@victim:~$ ping ovs  
PING OVS-link-1 (10.10.2.2) 56(84) bytes of data.  
64 bytes from OVS-link-1 (10.10.2.2): icmp_req=1 ttl=64 time=0.408 ms  
64 bytes from OVS-link-1 (10.10.2.2): icmp_req=2 ttl=64 time=0.469 ms  
64 bytes from OVS-link-1 (10.10.2.2): icmp_req=3 ttl=64 time=0.430 ms  
64 bytes from OVS-link-1 (10.10.2.2): icmp_req=4 ttl=64 time=0.446 ms  
64 bytes from OVS-link-1 (10.10.2.2): icmp_req=5 ttl=64 time=0.417 ms  
^C  
--- OVS-link-1 ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 4000ms  
rtt min/avg/max/mdev = 0.408/0.434/0.469/0.021 ms  
castillo@victim:~$
```

7. Go to the terminal that corresponds to the "OVS" machine. Type: `ifconfig` and hit enter.
8. Find the corresponding numbers from above in step 5 and remember the specific "eth" it is paired with. For example, after running `ifconfig`, I am looking for 10.10.2.2 and I see that it is located beside "eth2". The "eth" you see on your screen that corresponds to your specific number is what you will type. For example, I would use eth2. I would type: `sudo tcpdump -i eth2 -vv` and hit enter.

```
castillo@ovs: ~  
collisions:0 txqueuelen:1000  
RX bytes:100951 (100.9 KB) TX bytes:102106 (102.1 KB)  
  
eth1    Link encap:Ethernet  HWaddr 02:ab:50:5f:79:29  
        inet addr:10.10.1.2  Bcast:10.10.1.255  Mask:255.255.255.0  
        inet6 addr: fe80::ab:50ff:fe5f:7929/64 Scope:Link  
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
        RX packets:2097 errors:0 dropped:0 overruns:0 frame:0  
        TX packets:2109 errors:0 dropped:0 overruns:0 carrier:0  
        collisions:0 txqueuelen:1000  
        RX bytes:126593852 (126.5 MB) TX bytes:141614 (141.6 KB)  
  
eth2    Link encap:Ethernet  HWaddr 02:b9:aa:f4:f9:0f  
        inet addr:10.10.2.2  Bcast:10.10.2.255  Mask:255.255.255.0  
        inet6 addr: fe80::b9:aaff:fe4:f90f/64 Scope:Link  
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
        RX packets:2116 errors:0 dropped:0 overruns:0 frame:0  
        TX packets:2120 errors:0 dropped:0 overruns:0 carrier:0  
        collisions:0 txqueuelen:1000  
        RX bytes:110968 (110.9 KB) TX bytes:126627232 (126.6 MB)  
  
eth3    Link encap:Ethernet  HWaddr 02:54:6f:b3:c4:30  
        inet addr:10.10.3.2  Bcast:10.10.3.255  Mask:255.255.255.0  
        inet6 addr: fe80::54:6fff:feb3:c430/64 Scope:Link  
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
        RX packets:54 errors:0 dropped:0 overruns:0 frame:0  
        TX packets:64 errors:0 dropped:0 overruns:0 carrier:0  
        collisions:0 txqueuelen:1000  
        RX bytes:2952 (2.9 KB) TX bytes:6688 (6.6 KB)  
  
lo      Link encap:Local Loopback  
        inet addr:127.0.0.1  Mask:255.0.0.0  
        inet6 addr: ::1/128 Scope:Host  
        UP LOOPBACK RUNNING  MTU:65536  Metric:1  
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0  
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0  
        collisions:0 txqueuelen:0  
        RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)  
  
castillo@ovs:~$
```

9. Complete step 1 - 2 for a few seconds. What do you observe on the "OVS" machine? Where does this traffic come from?
10. Go to the terminal that corresponds to the "attacker" machine. Type: `sudo apt-get update` and hit enter on your keyboard. This command updates all the repositories in your machine and prepares it to install another tool. Then type `sudo apt-get install hping3` and hit enter on your keyboard. This command installs the tool "hping3". Finally, type: `sudo hping3 -S --flood victim` and hit enter on your keyboard. After a few seconds, press both the Ctrl key and C key together. What is happening in the

terminal that corresponds to the "OVS" machine?

```
castillo@ovs: ~
h 65160
12:30:09.557761 IP victim-link-1.5001 > user-link-0.53628: Flags [.] , ack 126170
057, win 32182, options [nop,nop,TS val 533412 ecr 794685], length 0
12:30:09.558921 IP user-link-0.53628 > victim-link-1.5001: Flags [P.] , seq 12630
0377:126365537, ack 1, win 913, options [nop,nop,TS val 794689 ecr 533407], leng
th 65160
12:30:09.562947 IP victim-link-1.5001 > user-link-0.53628: Flags [.] , ack 126235
217, win 32182, options [nop,nop,TS val 533414 ecr 794686], length 0
12:30:09.564106 IP user-link-0.53628 > victim-link-1.5001: Flags [.] , seq 126365
537:126430697, ack 1, win 913, options [nop,nop,TS val 794690 ecr 533409], lengt
h 65160
12:30:09.568144 IP victim-link-1.5001 > user-link-0.53628: Flags [.] , ack 126300
377, win 32182, options [nop,nop,TS val 533415 ecr 794688], length 0
12:30:09.569298 IP user-link-0.53628 > victim-link-1.5001: Flags [.] , seq 126430
697:126495857, ack 1, win 913, options [nop,nop,TS val 794691 ecr 533410], lengt
h 65160
12:30:09.573326 IP victim-link-1.5001 > user-link-0.53628: Flags [.] , ack 126365
537, win 32182, options [nop,nop,TS val 533416 ecr 794689], length 0
12:30:09.574491 IP user-link-0.53628 > victim-link-1.5001: Flags [.] , seq 126495
857:126561017, ack 1, win 913, options [nop,nop,TS val 794693 ecr 533411], lengt
h 65160
12:30:09.578523 IP victim-link-1.5001 > user-link-0.53628: Flags [.] , ack 126430
697, win 32182, options [nop,nop,TS val 533418 ecr 794690], length 0
12:30:09.579671 IP user-link-0.53628 > victim-link-1.5001: Flags [.] , seq 126561
017:126614593, ack 1, win 913, options [nop,nop,TS val 794693 ecr 533411], lengt
h 53576
12:30:09.583708 IP victim-link-1.5001 > user-link-0.53628: Flags [.] , ack 126495
857, win 32182, options [nop,nop,TS val 533419 ecr 794691], length 0
12:30:09.583886 IP user-link-0.53628 > victim-link-1.5001: Flags [FP.] , seq 1266
14593:126615577, ack 1, win 913, options [nop,nop,TS val 794693 ecr 533411], len
gth 984
12:30:09.588913 IP victim-link-1.5001 > user-link-0.53628: Flags [.] , ack 126561
017, win 32182, options [nop,nop,TS val 533420 ecr 794693], length 0
12:30:09.594078 IP victim-link-1.5001 > user-link-0.53628: Flags [.] , ack 126614
593, win 32182, options [nop,nop,TS val 533422 ecr 794693], length 0
12:30:09.602909 IP victim-link-1.5001 > user-link-0.53628: Flags [F.] , seq 1, ac
k 126615578, win 32182, options [nop,nop,TS val 533424 ecr 794693], length 0
12:30:09.603195 IP user-link-0.53628 > victim-link-1.5001: Flags [.] , ack 2, win
913, options [nop,nop,TS val 794705 ecr 533424], length 0
```

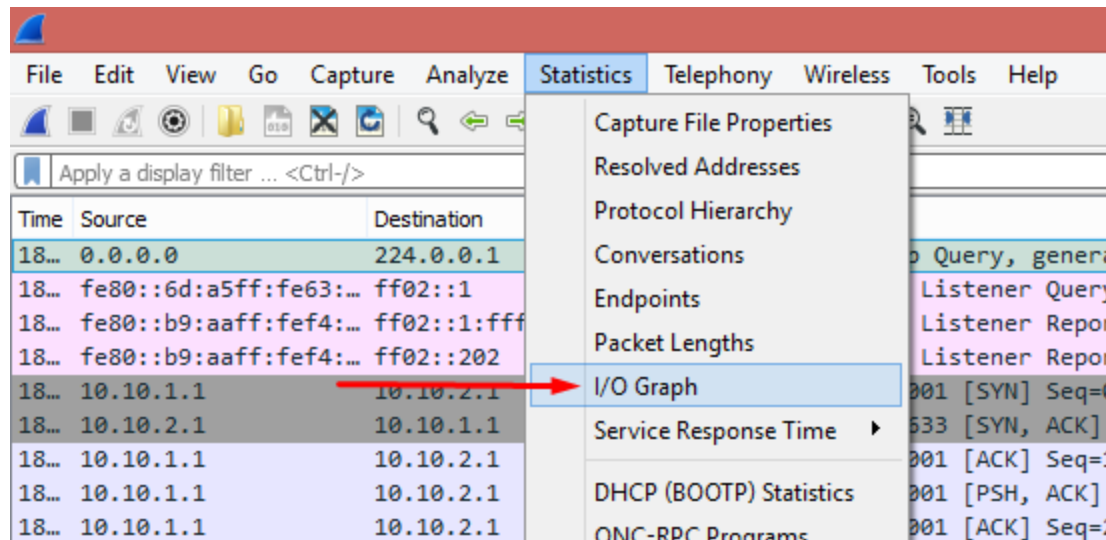
11. Does the traffic generated from the "attacker" machine look like it goes through at a faster pace than the traffic that you generated in task 3?
- The first part of the commands above, "sudo", makes you a root user. You are now the privileged user that is allowed to run anything you want on the machine.
 - The "tcpdump" command, calls a program that monitors the network traffic that is entering the "victim" machine. The ending part of the "tcpdump" command is the network interface that is being monitored.
 - The "hping3" command was used to run a flooding attack towards the "victim" machine. This attack is called a [Denial of Service \(DoS\) attack](#) and is designed to bring the network down by sending it useless traffic.

Part 5: Collecting Data from GENI machines.

1. We will now collect normal traffic and DoS traffic data and compare them. First, go to the terminal that corresponds to the "OVS" machine and press both the Ctrl key and C key together. Now in the "OVS" machine terminal, Type: `sudo tcpdump -i eth1 -s0 -w capture1.pcap` (where eth1 corresponds to the same "eth" you used in Task 4, Step 8) and hit enter on your keyboard. This command takes the tcpdump monitored traffic and writes it in a file called capture1.pcap.
2. Go to the terminal that corresponds to the "victim" machine and press both the Ctrl key and C key together. Now in the "victim" machine terminal, Type: `iperf -s` and hit enter on your keyboard. When you use `iperf -s` you are running an iperf server. Next you will run an iperf client on the "user" machine and generate some regular traffic
3. Go to the terminal that corresponds to the "user" machine. Type: `iperf -c victim` and hit enter on your keyboard.
4. Go to the terminal that corresponds to the "attacker" machine. Type: `sudo hping3 -S -flood victim` and hit enter on your keyboard. After 10 seconds, press both the Ctrl key and C key together on all your terminal windows.
5. Now we will analyze the information gathered after generating an attack.
 - If you are a windows user, drag and drop the capture file from your "OVS" machine to your computer using WinSCP. You can find instructions on [how to install and use WinSCP](#) in the embedded link.
 - If you are a Mac or Linux user, you may use sftp to transfer your files. Open a terminal on your local machine (Mac or Linux). You can find instructions on [how to install and use SFTP](#) in the embedded link.

Part 6: Analyzing the data.

1. Use Wireshark to view the statistics of your capture file. Write all the traffic statistics here.



2. Describe the I/O graph that is generated by your capture file. This is the graph of the traffic you ran in the previous task. Do you see at which time you started the flooding attack? Why is it very distinctive? Copy the graph.
3. Did the attack end at some point? What do you think happened at this point? (Refer back to Wireshark Installation & Usage Guide from Lab 0 if you need instruction on how to view the statistics and I/O graph of your capture file.)

Part 7: Repeatable experiments.

1. Repeat the experiments from task 3 at least four more times. You will need to change the name of the capture everytime (capture1.pcap, capture2.pcap, capture3.pcap, capture4.pcap, capture5.pcap).
2. Take the statistics of packet size and bandwidth from Wireshark from each pcap file and put these in an Excel spreadsheet. Calculate the average and standard deviation of this data and plot the data. Describe your observations of this data.