

# CSCI 353 Assignment 2. Part 1.

## Sample log file output from Test Files

I used the following three pcap files to generate the output in a log file.

- 1) tcp-twoIP-200.pcap
- 2) tcp-multipleIP-97.pcap
- 3) udp-multipleIP-6.pcap

## Two Columns:

Using Sample file: tcp-twoIP-200.pcap  
(single src/two dst)

**With “-s -p”**

Verbosely, you could print out the details in the command line as follows for debugging purpose:

```
10.1.1.2          1
10.1.1.2          2
10.1.1.2          3
...
```

However, the **final log file output** should be below:

```
10.1.1.2      200
```

Similarly,

**With “-d -b”,**

You can verbosely print out the information in the command as follows:

```
10.1.2.2          60
10.1.2.2          112
10.1.2.3          60
10.1.2.3          112
10.1.2.3          1612
...
```

However, the **Final log file output** is below:

<b>10.1.2.2</b>	<b>112</b>
<b>10.1.2.3</b>	<b>294112</b>

Using Sample file: tcp-multipleIP-97.pcap(single src/multiple dst)

**With “-s -p”**

You can verbosely print out the information in the command as follows:

192.216.124.1	1
192.216.124.1	2
192.216.124.1	3
...	

However, the **Final log file output** is below:

<b>192.216.124.1</b>	<b>97</b>
----------------------	-----------

**With “-d -p”**

You can verbosely print out the information in the command as follows:

131.119.28.149	1
131.119.28.149	2
131.119.28.149	3
...	

However, the **Final log file output** is below:

<b>128.54.173.23</b>	<b>3</b>
<b>131.119.28.149</b>	<b>49</b>
<b>141.163.38.200</b>	<b>23</b>
<b>192.216.124.22</b>	<b>10</b>
<b>192.216.124.37</b>	<b>6</b>
<b>206.50.182.5</b>	<b>6</b>

Using Sample file: udp-multipleIP-6.pcap (single src/multiple dst)

**With “-s -p”**

**Final log file output:**

192.216.124.1	6
---------------	---

**With “-d -p”**

**Final log file output:**

157.22.226.1	3
169.199.29.5	1
204.75.161.14	2

## **Three Columns:**

Using Sample file: tcp-oneIP-200.pcap

**With “-s -p -b”**

10.1.1.2	1	60
10.1.1.2	2	112
10.1.1.2	3	172
...		

**Final log file output:**

10.1.1.2	200	294224
----------	-----	--------

**With “-d -p -b”**

**Final log file output:**

10.1.2.2	2	112
10.1.2.3	198	294112

**With “-s -d -p”**

**Final log file output:**

10.1.1.2	10.1.2.2	2
10.1.1.2	10.1.2.3	198

Using Sample file: tcp-multipleIP-97.pcap

**With “-s -p -b”**

You can verbosely print out the information in the command as follows:

192.216.124.1	1	45
192.216.124.1	2	90
192.216.124.1	3	130
...		

**Final log file output:**

192.216.124.1	97	18109
---------------	----	-------

**With “-d -p -b”**

You can verbosely print out the information in the command as follows:

131.119.28.149	1	45
131.119.28.149	2	90
131.119.28.149	3	130
...		
141.163.38.200	1	552
141.163.38.200	2	1104
141.163.38.200	3	1656
...		

However, **Final log file output** should be:

128.54.173.23	3	190
131.119.28.149	49	2110
141.163.38.200	23	12696
192.216.124.22	10	599
192.216.124.37	6	2168
206.50.182.5	6	843

**With “-s -d -p”**

**Final log file output** should be:

192.216.124.1	128.54.173.23	3	
192.216.124.1	131.119.28.149	49	
192.216.124.1	141.163.38.200	23	
192.216.124.1	192.216.124.22	10	
192.216.124.1	192.216.124.37	6	
192.216.124.1	206.50.182.5	6	

Using Sample file: udp-multipleIP-6.pcap (single src/multiple dst)

**With “-s -p -b”**

**Final log file output** should be:

192.216.124.1	6	628	
---------------	---	-----	--

**With “-d -p -b”**

**Final log file output** should be:

157.22.226.1	3	177	
169.199.29.5	1	333	
204.75.161.14	2	118	

## **Four Columns:**

Using Sample file: tcp-oneIP-200.pcap

**With “-s -d -p -b”**

**Final log file output** should be:

10.1.1.2	10.1.2.2	2	112
10.1.1.2	10.1.2.3	198	294112

Using Sample file: tcp-multipleIP-97.pcap

**With “-s -d -p -b”**

**Final log file output should be:**

192.216.124.1	128.54.173.23	3	190
192.216.124.1	131.119.28.149	49	2110
192.216.124.1	141.163.38.200	23	12696
192.216.124.1	192.216.124.22	10	599
192.216.124.1	192.216.124.37	6	2168
192.216.124.1	206.50.182.5	6	843

Using Sample file: udp-multipleIP-6.pcap (single src/multiple dst)

**With “-s -d -p -b”**

**Final log file output should be:**

192.216.124.1	157.22.226.1	3	177
192.216.124.1	169.199.29.5	1	333
192.216.124.1	204.75.161.14	2	118