

Part III

Dataset :

Intrusion Detection Evaluation Dataset (CICIDS2017)

- ▶ CICIDS2017 dataset contains benign and the most up-to-date common attacks, which resembles the true real-world data (PCAPs).
- ▶ It also includes the results of the network traffic analysis using CICFlowMeter with labeled flows based on the time stamp, source and destination IPs, source and destination ports, protocols and attack (CSV files)
- ▶ The data: Thursday July 6, 2017, Morning

Dataset after cleaning

WorkingHours-Morning-WebAttacks.pcap.xlsx

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1	Flow ID	Source IP	Source Port	Destination IP	Destination Port	Protocol	Timestamp		Flow Duration	Label						
2	192.168.10.3-192.168.10.50-389-33898-6	Web server 16 Public	33898	192.168.10.3	389	6	6/7/2017 8:59		113095465	BENIGN						
3	192.168.10.3-192.168.10.50-389-33904-6	Web server 16 Public	33904	192.168.10.3	389	6	6/7/2017 8:59		113473706	BENIGN						
4	8.0.6.4-8.6.0.1-0-0-0	8.6.0.1	0	8.0.6.4	0	0	6/7/2017 8:59		119945515	BENIGN						
5	192.168.10.14-65.55.44.109-59135-443-6	Win 10, pro 32B	59135	192.168.44.109	443	6	6/7/2017 8:59		60261928	BENIGN						
6	192.168.10.3-192.168.10.14-53-59555-17	Win 10, pro 32B	59555	192.168.10.3	53	17	6/7/2017 8:59		269	BENIGN						
7	129.6.15.29-192.168.10.50-123-123-17	Web server 16 Public	123	129.6.15.29	123	17	6/7/2017 8:59		30352	BENIGN						
8	192.168.10.14-65.55.44.109-59135-443-6	65.55.44.109	443	192.168.10.14	59135	6	6/7/2017 9:00		48	BENIGN						
9	192.168.10.19-224.0.0.251-5353-5353-17	Ubuntu 14.4, 32B	5353	224.0.0.251	5353	17	6/7/2017 9:00		89501767	BENIGN						
10	192.168.10.1-192.168.10.3-53-60721-17	DNS+ DC Server	60721	192.168.10.1	53	17	6/7/2017 9:00		23527	BENIGN						
11	192.168.10.3-192.168.10.19-53-50535-17	Ubuntu 14.4, 32B	50535	192.168.10.3	53	17	6/7/2017 9:00		23978	BENIGN						
12	192.168.10.3-192.168.10.19-123-123-17	Ubuntu 14.4, 32B	123	192.168.10.3	123	17	6/7/2017 9:00		107015212	BENIGN						
13	192.168.10.255-192.168.10.19-138-138-17	Ubuntu 14.4, 32B	138	192.168.10.255	138	17	6/7/2017 9:00		75288199	BENIGN						
14	192.168.10.255-192.168.10.19-137-137-17	Ubuntu 14.4, 32B	137	192.168.10.255	137	17	6/7/2017 9:00		3378994	BENIGN						
15	192.168.10.19-192.168.10.50-137-137-17	Web server 16 Public	137	192.168.10.19	137	17	6/7/2017 9:00		3	BENIGN						
16	192.168.10.255-192.168.10.50-138-138-17	Web server 16 Public	138	192.168.10.255	138	17	6/7/2017 9:00		76354195	BENIGN						
17	192.168.10.1-192.168.10.3-53-62468-17	DNS+ DC Server	62468	192.168.10.1	53	17	6/7/2017 9:00		25117	BENIGN						
18	192.168.10.1-192.168.10.3-53-62174-17	DNS+ DC Server	62174	192.168.10.1	53	17	6/7/2017 9:00		25926	BENIGN						
19	192.168.10.3-192.168.10.19-53-1379-17	Ubuntu 14.4, 32B	1379	192.168.10.3	53	17	6/7/2017 9:00		25525	BENIGN						
20	192.168.10.3-192.168.10.19-53-55086-17	Ubuntu 14.4, 32B	55086	192.168.10.3	53	17	6/7/2017 9:00		171	BENIGN						
21	192.168.10.3-192.168.10.19-53-11737-17	Ubuntu 14.4, 32B	11737	192.168.10.3	53	17	6/7/2017 9:00		26386	BENIGN						
22	192.168.10.255-192.168.10.3-137-137-17	DNS+ DC Server	137	192.168.10.255	137	17	6/7/2017 9:00		1582026	BENIGN						
23	192.168.10.3-192.168.10.19-53-51849-17	Ubuntu 14.4, 32B	31849	192.168.10.3	53	17	6/7/2017 9:00		302	BENIGN						
24	192.168.10.3-192.168.10.19-53-40356-17	Ubuntu 14.4, 32B	40356	192.168.10.3	53	17	6/7/2017 9:00		257	BENIGN						
25	192.168.10.3-192.168.10.19-389-32791-6	Ubuntu 14.4, 32B	32791	192.168.10.3	389	6	6/7/2017 9:00		487	BENIGN						
26	192.168.10.3-192.168.10.19-88-41567-6	Ubuntu 14.4, 32B	41567	192.168.10.3	88	6	6/7/2017 9:00		1206	BENIGN						
27	192.168.10.3-192.168.10.19-389-32792-6	Ubuntu 14.4, 32B	32792	192.168.10.3	389	6	6/7/2017 9:00		27779	BENIGN						
28	192.168.10.3-192.168.10.19-88-41569-6	Ubuntu 14.4, 32B	41569	192.168.10.3	88	6	6/7/2017 9:00		1133	BENIGN						
29	192.168.10.3-192.168.10.19-389-32794-6	Ubuntu 14.4, 32B	32794	192.168.10.3	389	6	6/7/2017 9:00		118034439	BENIGN						
30	192.168.10.3-192.168.10.19-53-36981-17	Ubuntu 14.4, 32B	36981	192.168.10.3	53	17	6/7/2017 9:00		214	BENIGN						
31	192.168.10.3-192.168.10.19-53-25133-17	Ubuntu 14.4, 32B	25133	192.168.10.3	53	17	6/7/2017 9:00		190	BENIGN						
32	192.168.10.3-192.168.10.19-53-63701-17	Ubuntu 14.4, 32B	63701	192.168.10.3	53	17	6/7/2017 9:00		197	BENIGN						
33	192.168.10.3-192.168.10.19-53-41900-17	Ubuntu 14.4, 32B	41900	192.168.10.3	53	17	6/7/2017 9:00		210	BENIGN						
34	192.168.10.3-192.168.10.19-53-31375-17	Ubuntu 14.4, 32B	31375	192.168.10.3	53	17	6/7/2017 9:00		202	BENIGN						
35	192.168.10.3-192.168.10.19-53-39923-17	Ubuntu 14.4, 32B	39923	192.168.10.3	53	17	6/7/2017 9:00		350	BENIGN						
36	192.168.10.3-192.168.10.19-53-28357-17	Ubuntu 14.4, 32B	28357	192.168.10.3	53	17	6/7/2017 9:00		163	BENIGN						
37	192.168.10.3-192.168.10.19-53-49763-17	Ubuntu 14.4, 32B	49763	192.168.10.3	53	17	6/7/2017 9:00		191	BENIGN						
38	192.168.10.3-192.168.10.19-53-54131-17	Ubuntu 14.4, 32B	54131	192.168.10.3	53	17	6/7/2017 9:00		163	BENIGN						
39	192.168.10.3-192.168.10.19-53-6235-17	Ubuntu 14.4, 32B	6235	192.168.10.3	53	17	6/7/2017 9:00		203	BENIGN						
40	192.168.10.3-192.168.10.19-53-53306-17	Ubuntu 14.4, 32B	53306	192.168.10.3	53	17	6/7/2017 9:00		171	BENIGN						
41	192.168.10.3-192.168.10.19-53-26610-17	Ubuntu 14.4, 32B	26610	192.168.10.3	53	17	6/7/2017 9:00		167	BENIGN						
42	192.168.10.3-192.168.10.19-53-29080-17	Ubuntu 14.4, 32B	29080	192.168.10.3	53	17	6/7/2017 9:00		163	BENIGN						
43	192.168.10.3-192.168.10.19-53-2406-17	Ubuntu 14.4, 32B	23406	192.168.10.3	53	17	6/7/2017 9:00		162	BENIGN						

Logstash configuration file

```
下載項目 — ubuntu@ip-172-31-81-63: /usr/share/logstash/bin — ssh -i MyKeypair.pem ubuntu@ec2-3-82-193-119.compute-1.amazonaws.com —
GNU nano 2.5.3                                         File: /etc/logstash/conf.d/10-syslog.conf

input {
  file {
    path => ["/home/ubuntu/WorkingHours-Morning-WebAttacks.pcap_ISCX.csv"]    ##path of ur CSV file

    start_position => "beginning"
    since_db_path => "/dev/null"
  }
}
filter {
  csv {
    separator => ","
    columns => ["Flow ID","Source IP","Source Port","Destination IP","Destination Port","Protocol","Timestamp","Flow Duration", "Label"]
  }
  mutate {
    convert => {
      "Source Port" => "integer"
      "Destination Port" => "integer"
      "Flow Duration" => "integer"
    }
  }
}
output {
  elasticsearch {
    hosts => "http://localhost:9200"
    index => "test"
  }
  stdout{}
}
```

```
ubuntu@ip-172-31-81-63:/usr/share/logstash/bin$ sudo -u logstash /usr/share/logstash/bin/logstash --path.settings /etc/logstash -f /etc/logstash/conf.d/10-syslog.conf --config.test_and_exit
Sending Logstash logs to /var/log/logstash which is now configured via log4j2.properties
[2018-12-15T20:00:46,514][WARN ][logstash.config.source.multilocal] Ignoring the 'pipelines.yml' file because modules or command line options are specified
Configuration OK
[2018-12-15T20:00:56,406][INFO ][logstash.runner_] ] Using config.test_and_exit mode. Config Validation Result: OK. Exiting Logstash
```

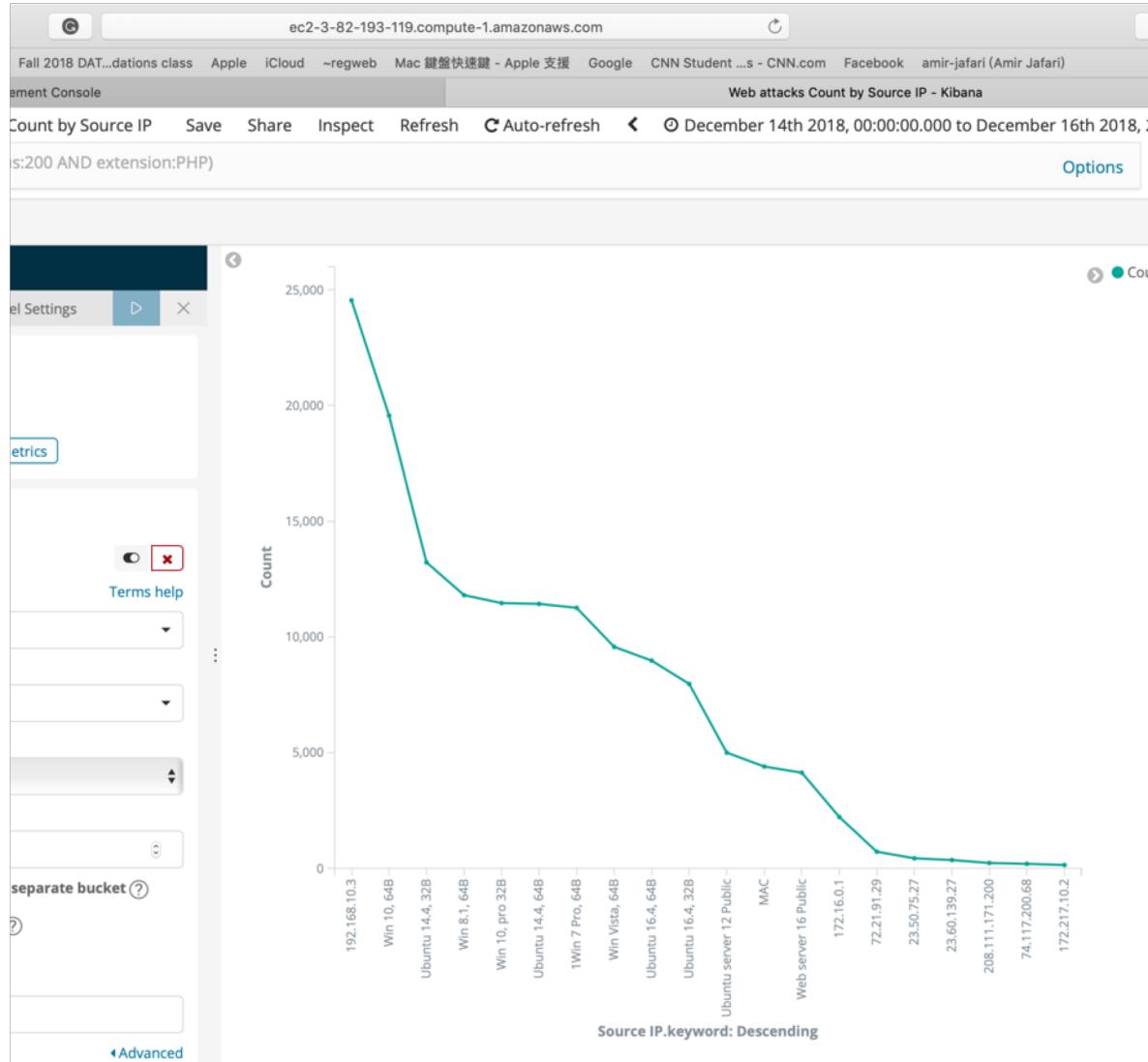
Kibana

The screenshot shows the Kibana Management interface. On the left, a sidebar menu lists various features: Discover, Visualize, Dashboard, Timelion, Canvas, Machine Learning, Infrastructure, Logs, APM, Dev Tools, Monitoring, and Management. The Management option is currently selected. At the bottom of the sidebar are two buttons: Default and Collapse.

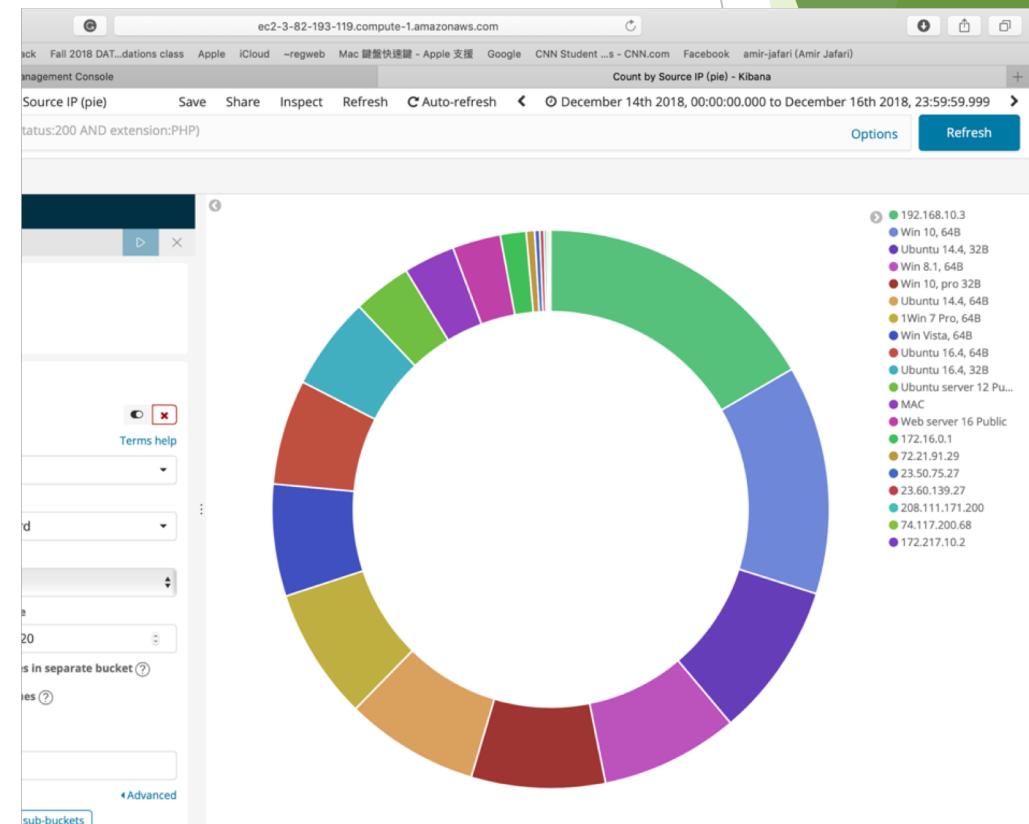
The main content area is titled "Management / Kibana" and shows the "Index Patterns" tab is active. Below the tabs are buttons for "Create index pattern" and "test*". A note indicates a "Time Filter field name: @timestamp". The page lists all fields in the "test*" index pattern, including their type, format, searchability, aggregability, and exclusion status. Fields listed include @timestamp, @version, @version.keyword, Destination IP, Destination IP.keyword, Destination Port, Flow Duration, Flow ID, Flow ID.keyword, and Label.

Name	Type	Format	Searchable	Aggregatable	Excluded
@timestamp	date		●	●	○
@version	string		●		○
@version.keyword	string		●	●	
Destination IP	string		●		○
Destination IP.keyword	string		●	●	○
Destination Port	number		●	●	○
Flow Duration	number		●	●	○
Flow ID	string		●		○
Flow ID.keyword	string		●	●	○
Label	string		●		○

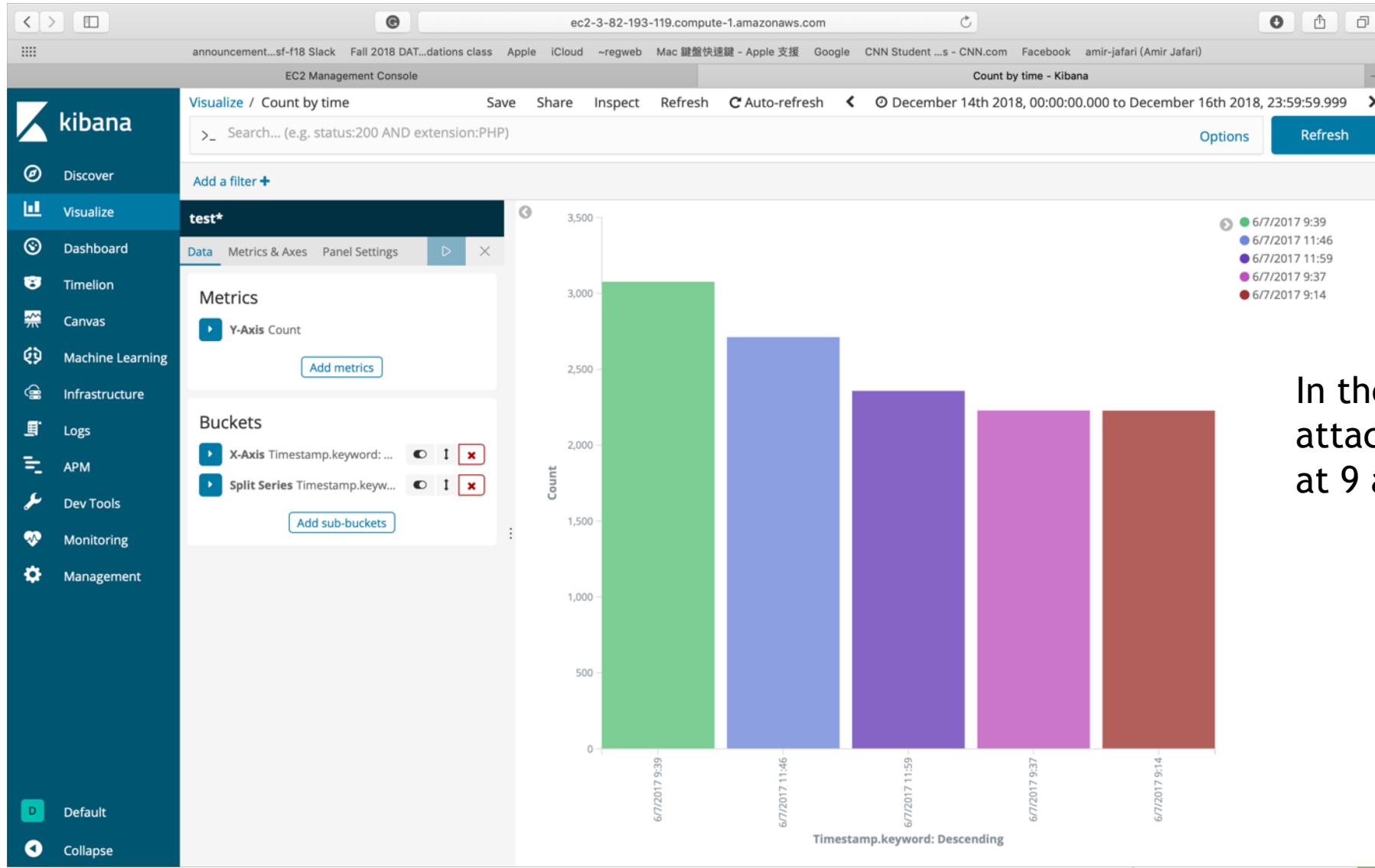
Web attacks Count by Source IP



The plots show that at IP 192.168.10.3 (DNS+ DC Server) get the most attacks.

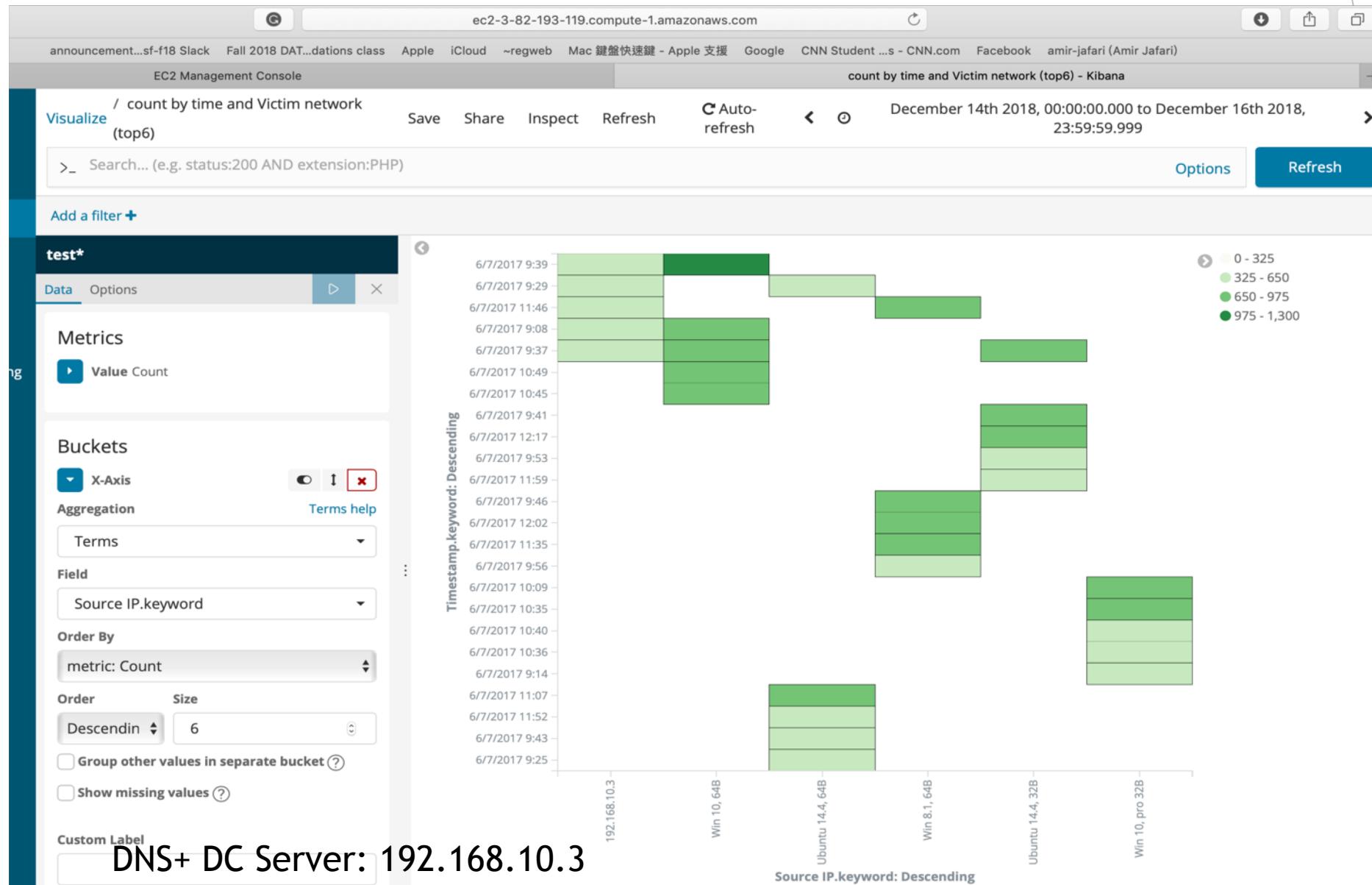


Web Attacks Count by Time (Top 5)



In the plot, the web attack happens more at 9 and 11 am

Count by time and Source IP (Top 6)



Count by Source IP and Destination IP

