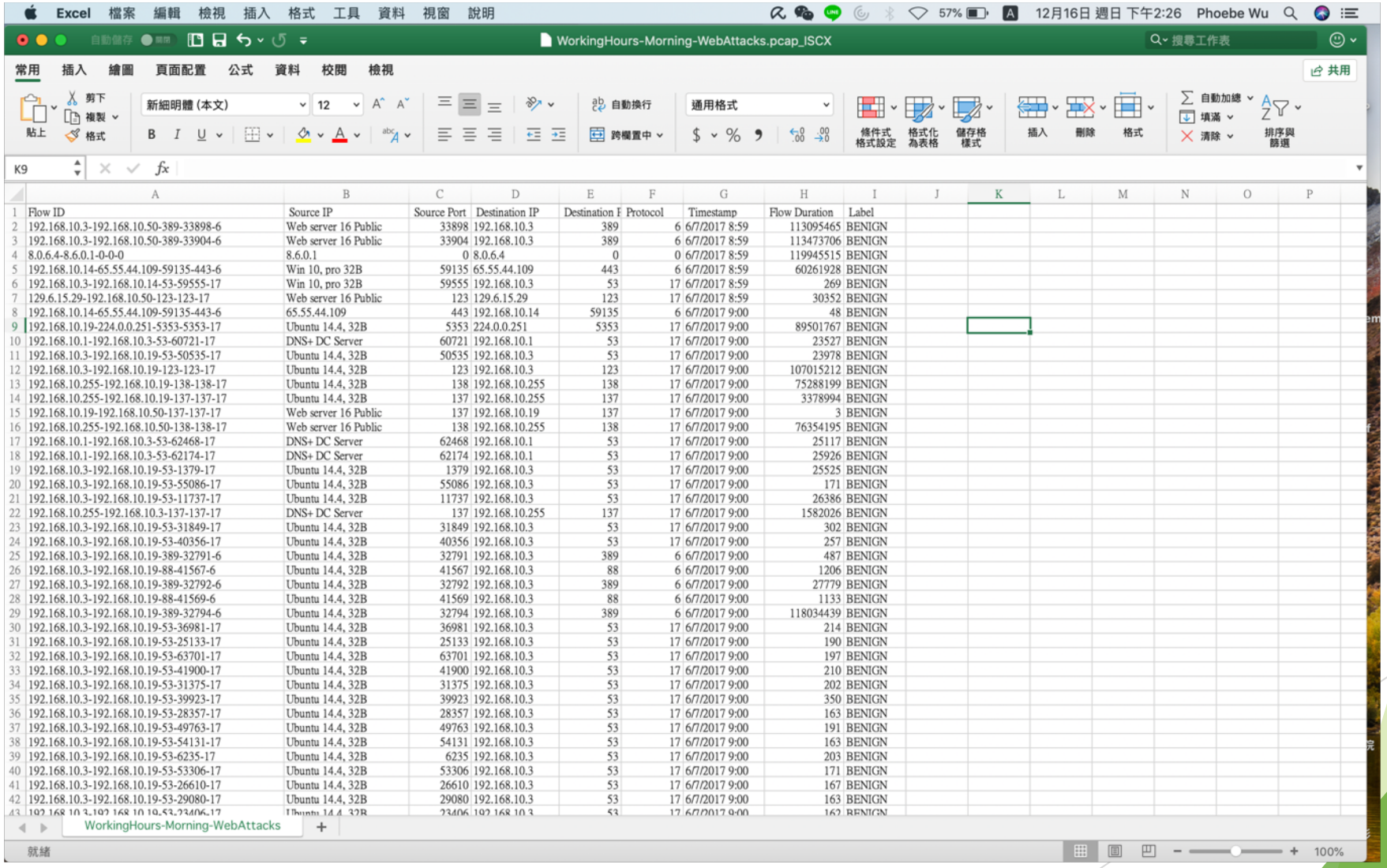
Part III

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



Flow ID	Source IP	Source Port	Destination IP	Destination F	Protocol	Timestamp	Flow Duration	Label
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
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
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
192.168.10.14-65.55.44.109-59135-443-6	Win 10, pro 32B	59135	65.55.44.109	443	6	6/7/2017 8:59	60261928	BENIGN
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
192.168.10.3-192.168.10.19-53-31849-17	Ubuntu 14.4, 32B	31849	192.168.10.3	53	17	6/7/2017 9:00	302	BENIGN
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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

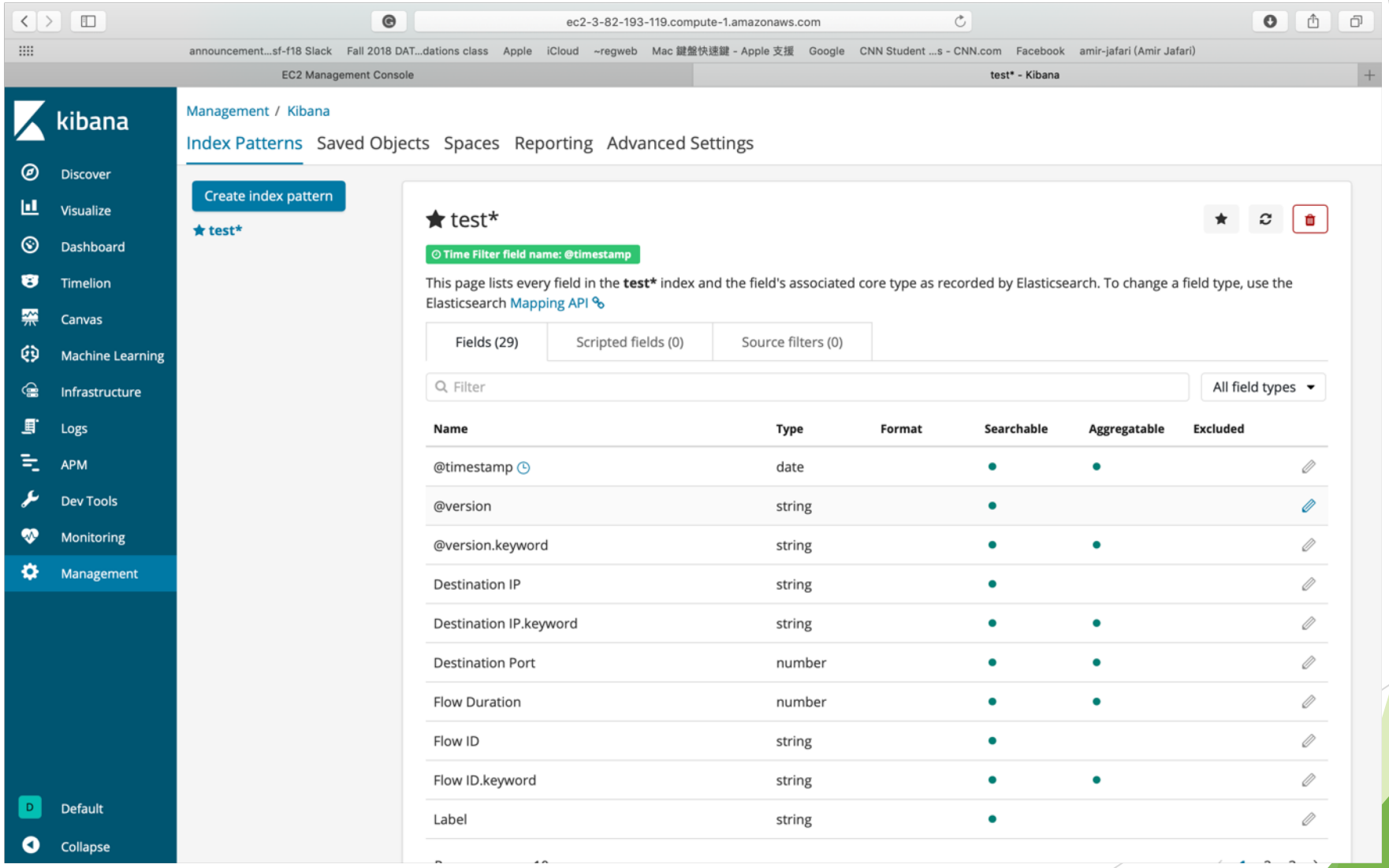
Logstash configuration file

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 –

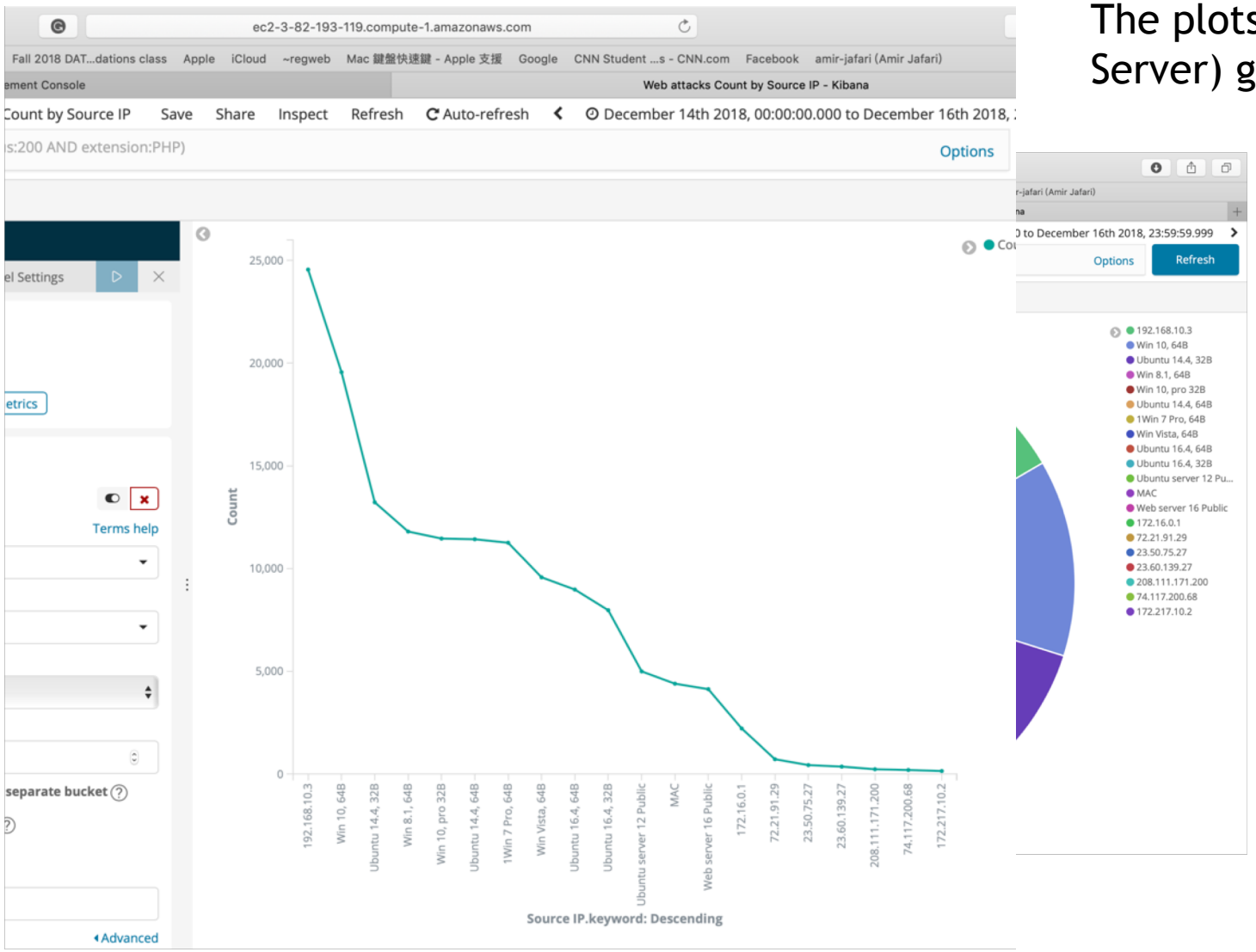
```
 GNU nano 2.5.3                          File: /etc/logstash/conf.d/10-syslog.conf

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

    start_position => "beginning"
    sincedb_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

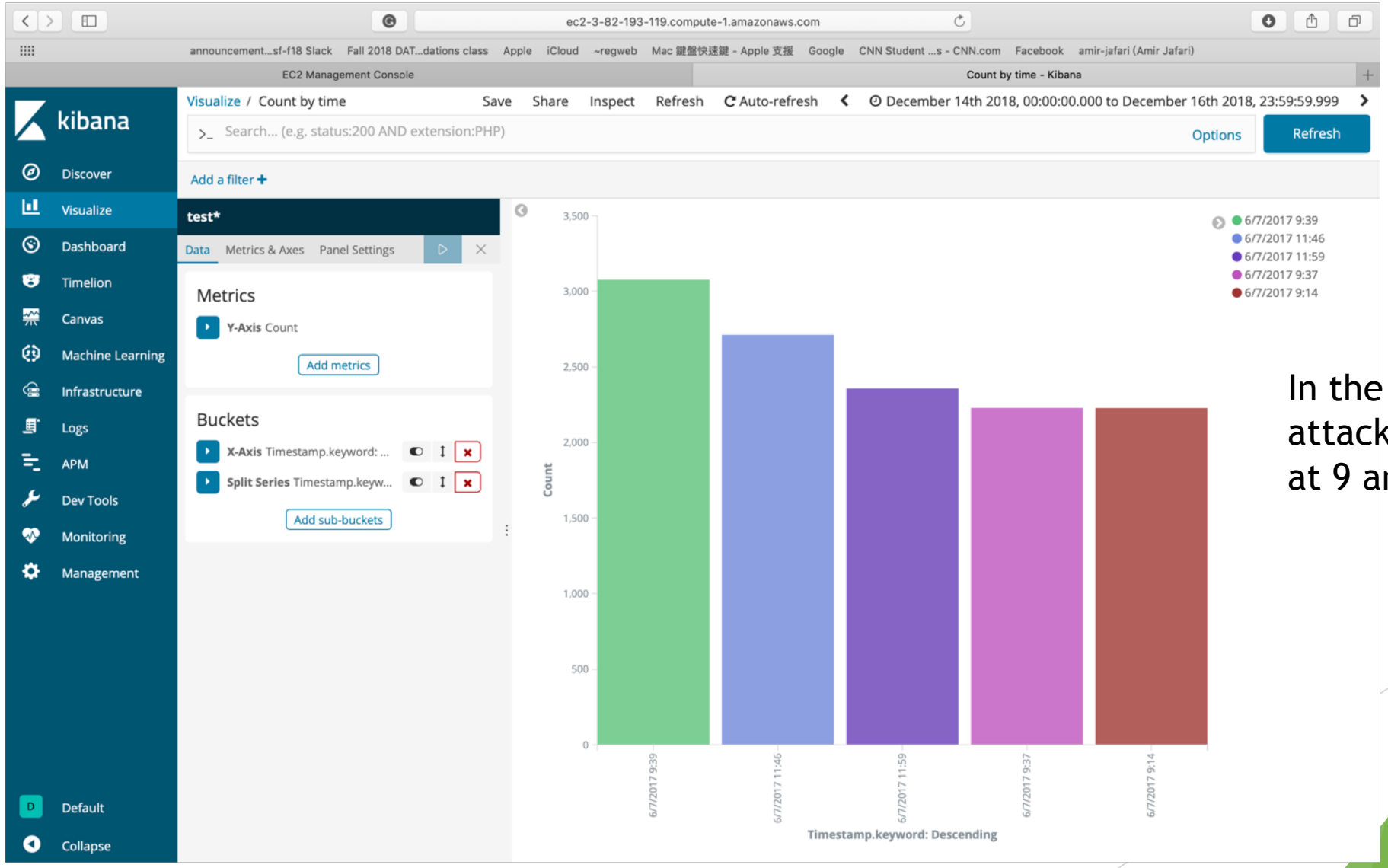

ec2-3-82-193-119.compute-1.amazonaws.com
announcement...sf-f18 Slack
Fall 2018 DAT...dations class
Apple
iCloud
~regweb
Mac 鍵盤快速鍵 - Apple 支援
Google
CNN Student ...s - CNN.com
Facebook
amir-jafari (Amir Jafari)
EC2 Management Console
test* - Kibana
kibana
Discover
Visualize
Dashboard
Timelion
Canvas
Machine Learning
Infrastructure
Logs
APM
Dev Tools
Monitoring
Management
Default
Collapse
Management / Kibana
Index Patterns
Saved Objects
Spaces
Reporting
Advanced Settings
Create index pattern
test*
test*
Time Filter field name: @timestamp
This page lists every field in the test* index and the field's associated core type as recorded by Elasticsearch. To change a field type, use the Elasticsearch Mapping API
Fields (29)
Scripted fields (0)
Source filters (0)
Filter
All field types
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



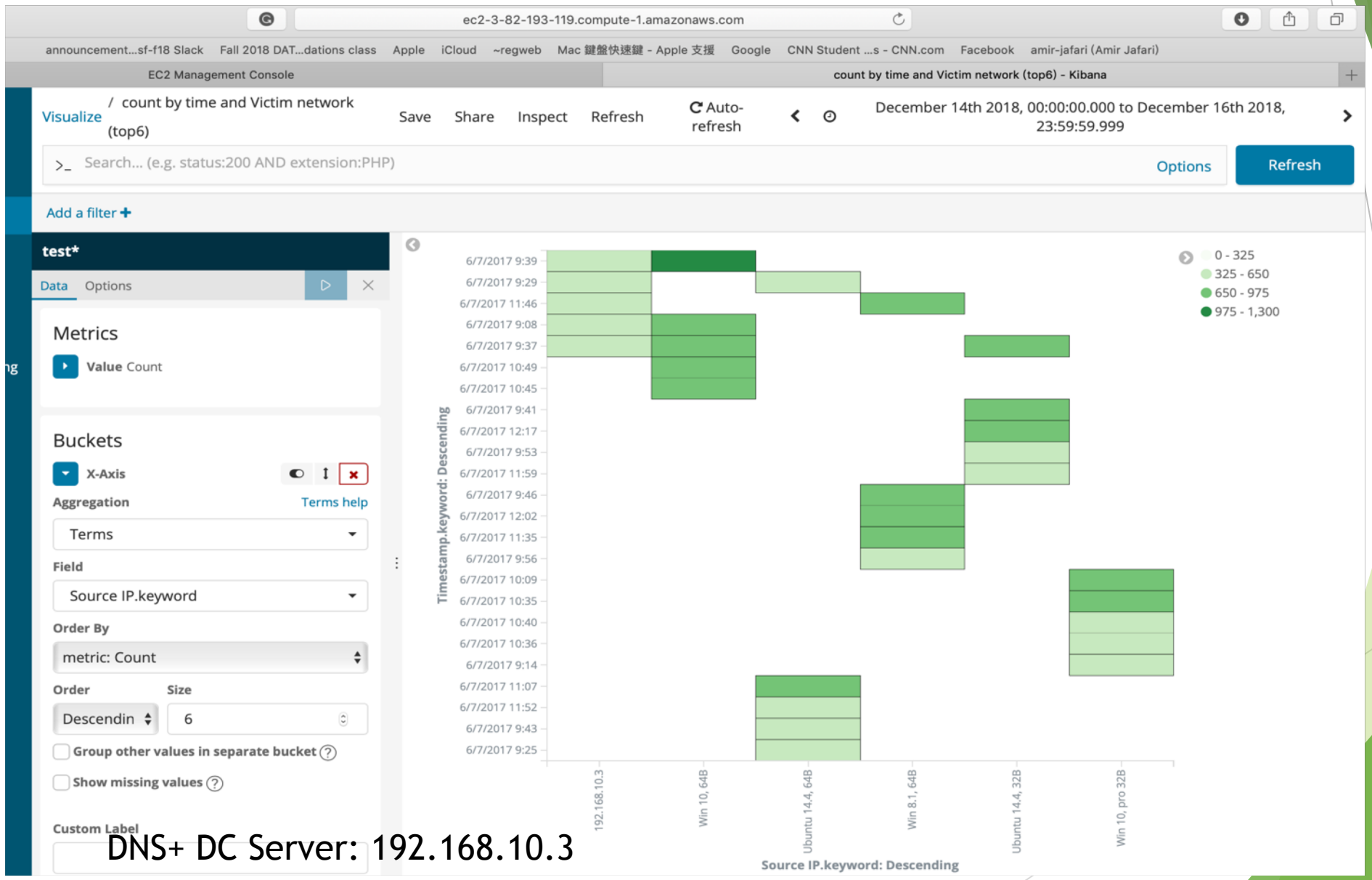
The plots show that at IP 192.168.10.3 (DNS+ DC Server) get the most attacks.

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)



DNS+ DC Server: 192.168.10.3

Count by Source IP and Destination IP