Visualizing PHPIDS Log Files for Better Understanding of Web Server Attacks

Abdullah Alqahtani
King Saud University, Saudi Arabia

Introduction

- PHPIDS
- Log visualization

Contributions

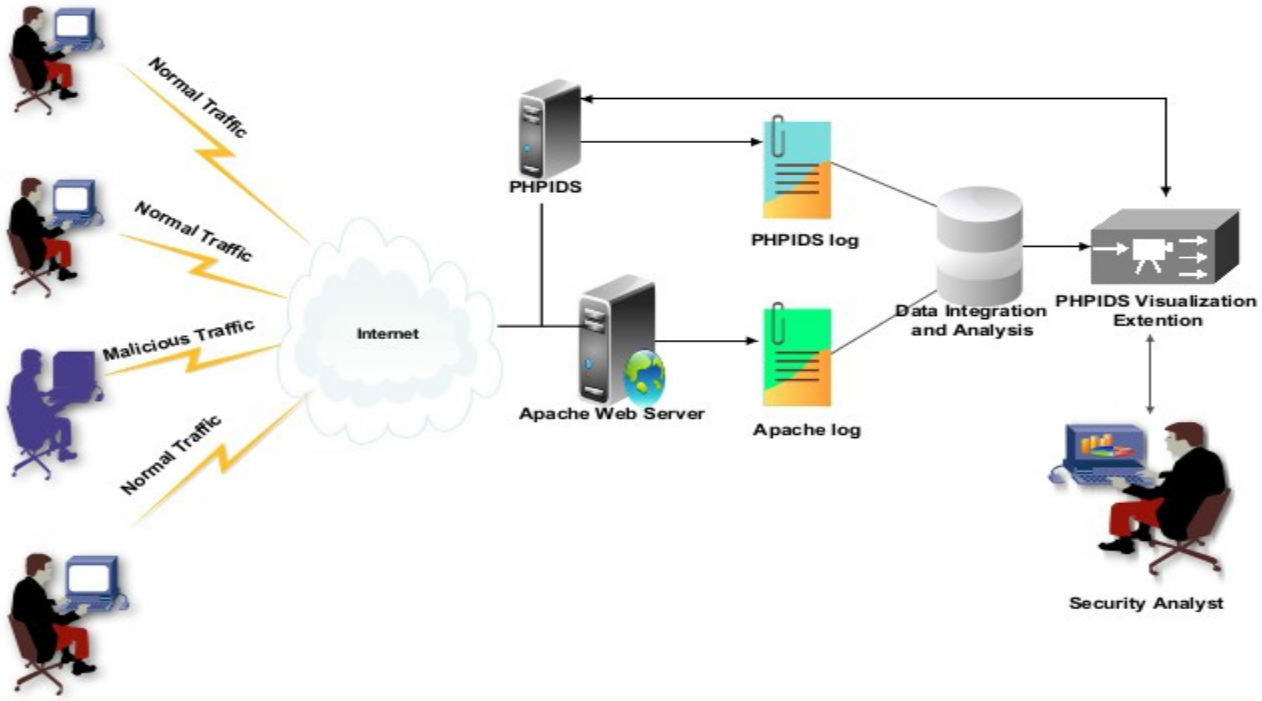
- Analysis and correlation of PHPIDS and web server logs
- PHPIDS visualization extension
- Experimentation on real-world datasets

Datasets and methodology

- Datasets
- Prefuse toolkit
- Exploring various data visualization

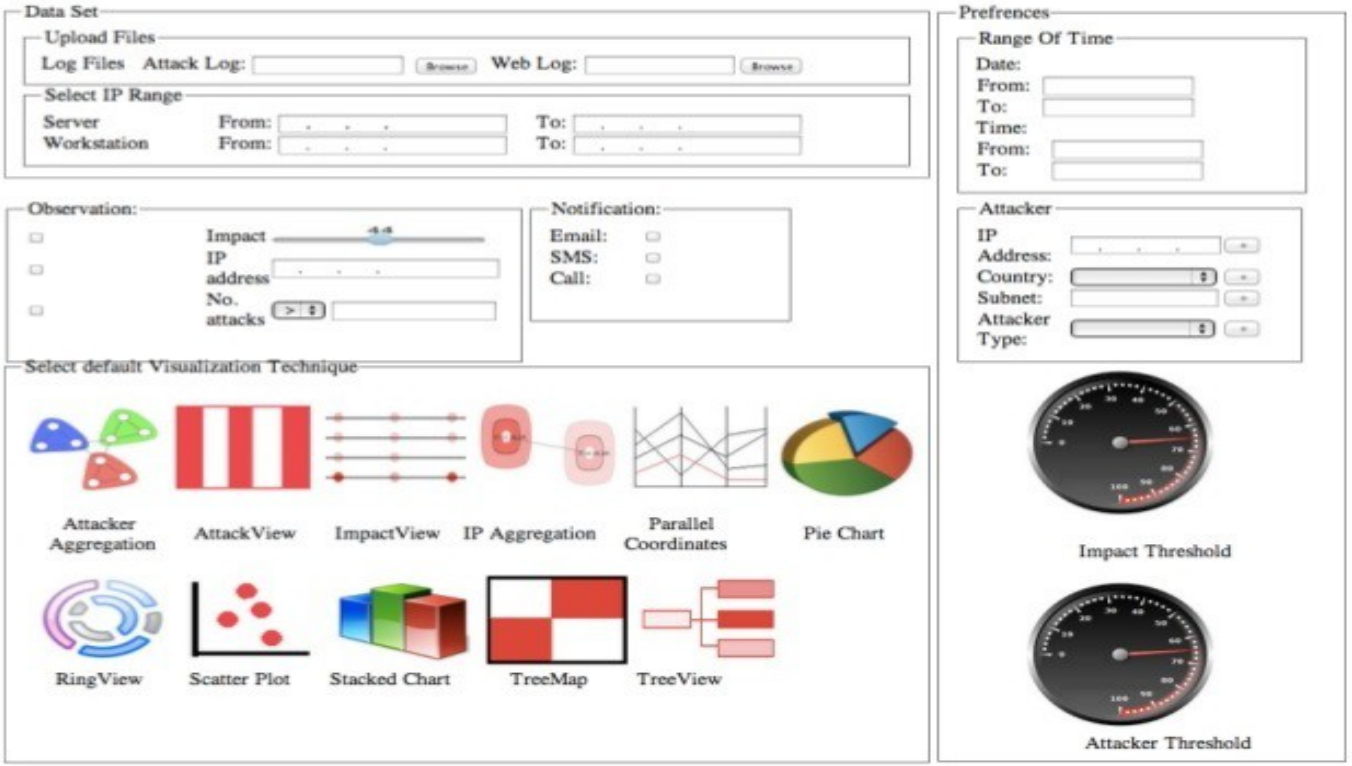
PHPIDS Visualization Extension

- System Design

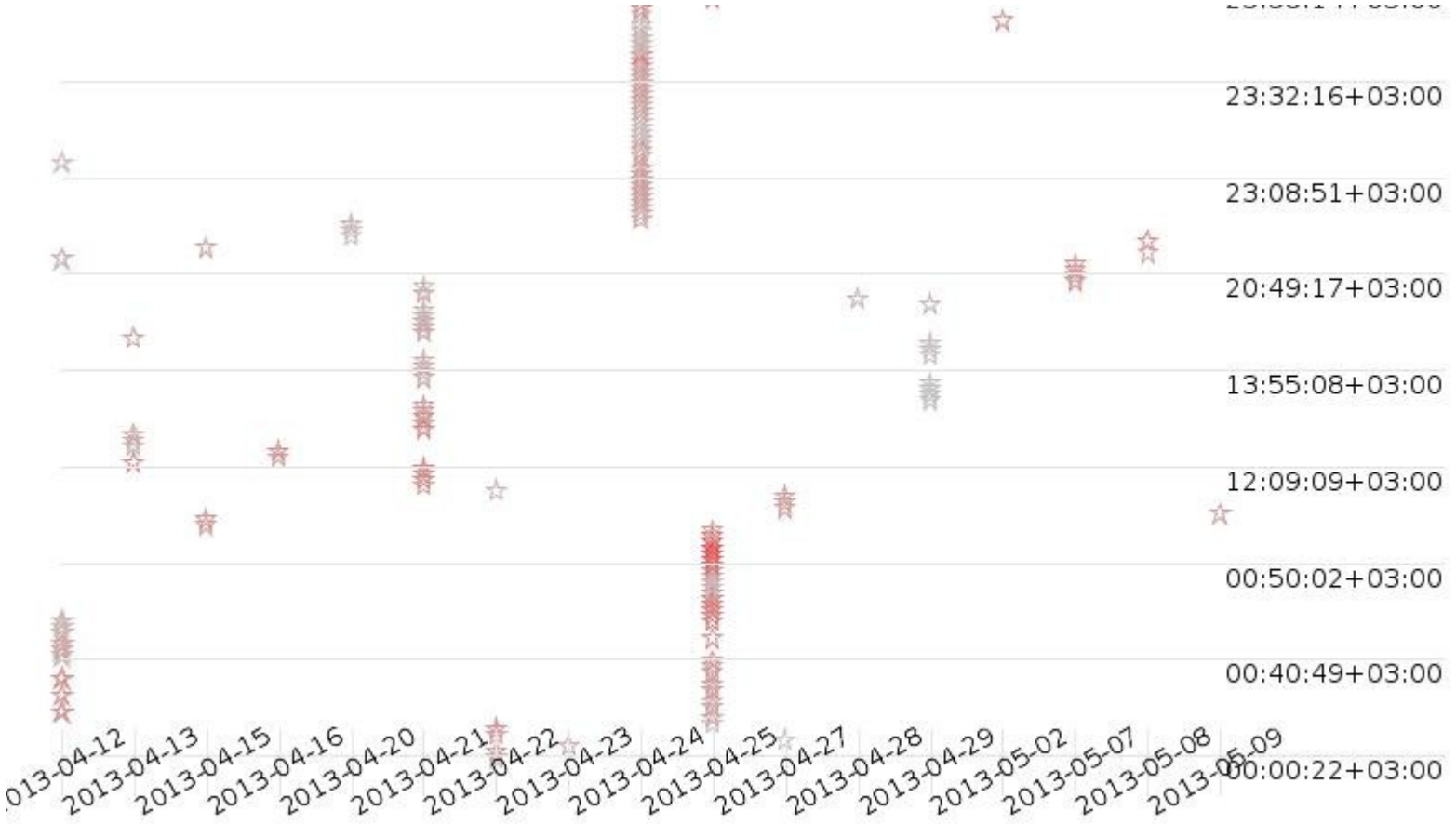


PHPIDS Visualization Extension

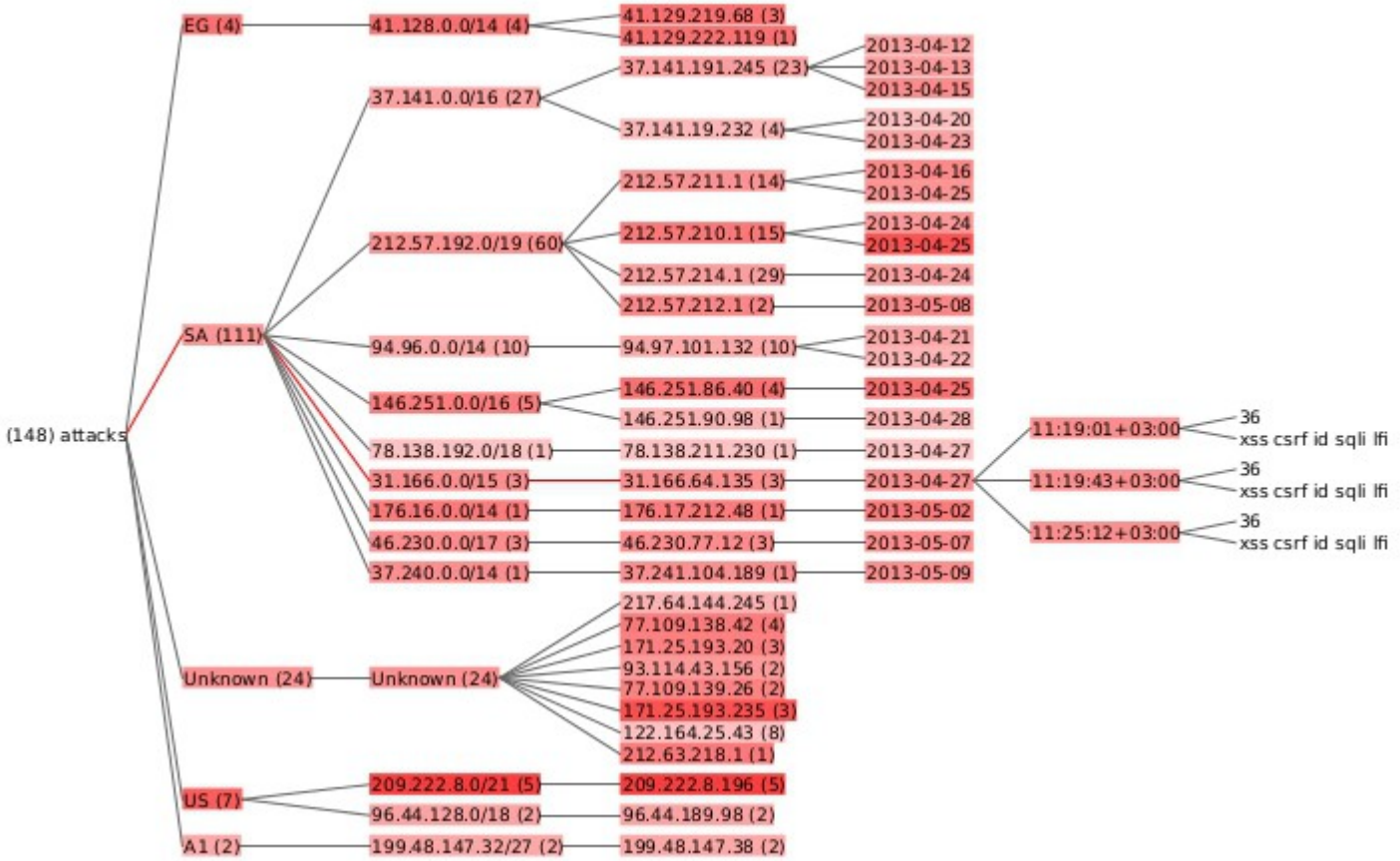
- Control console



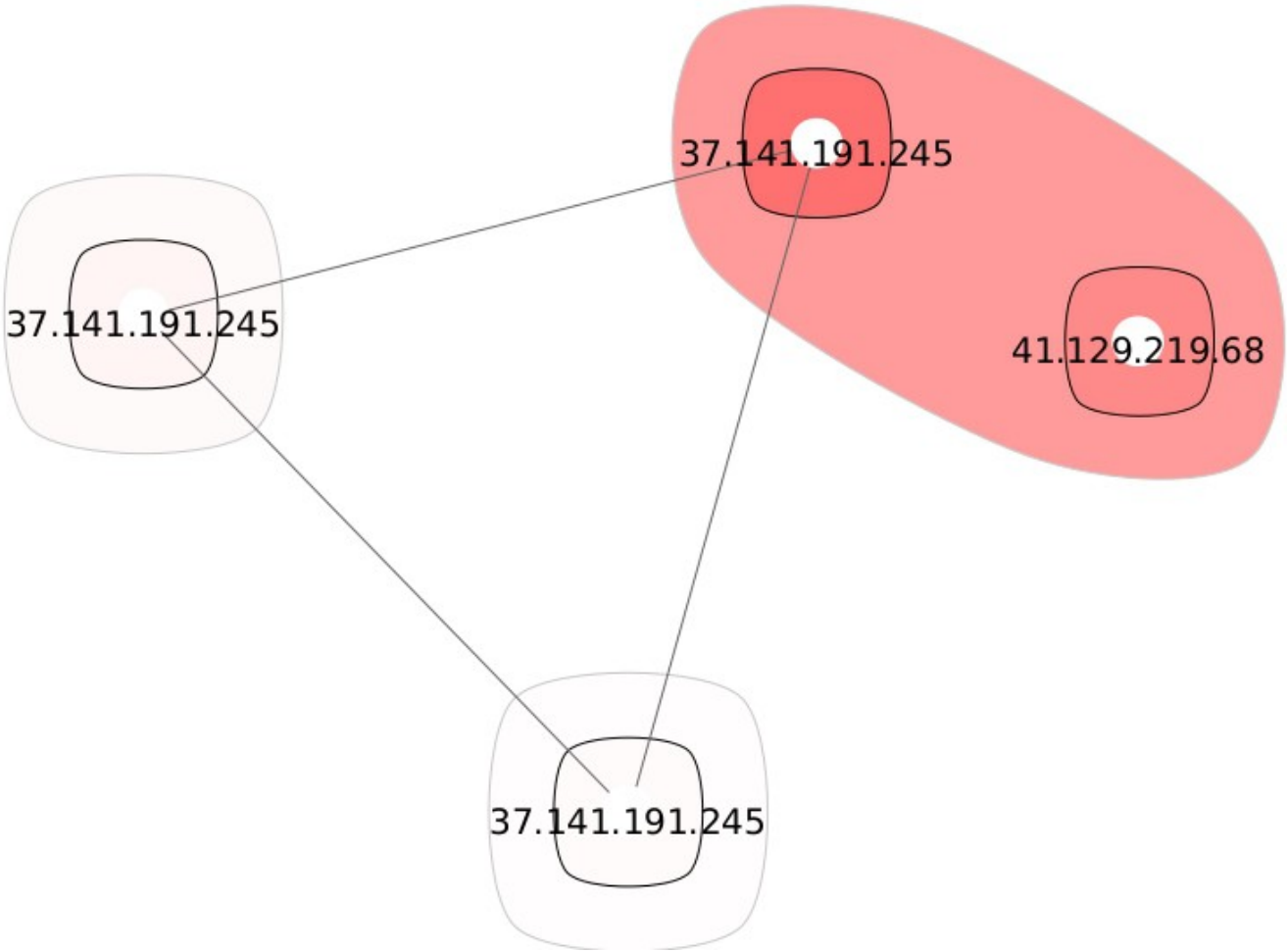
Scatter Plot



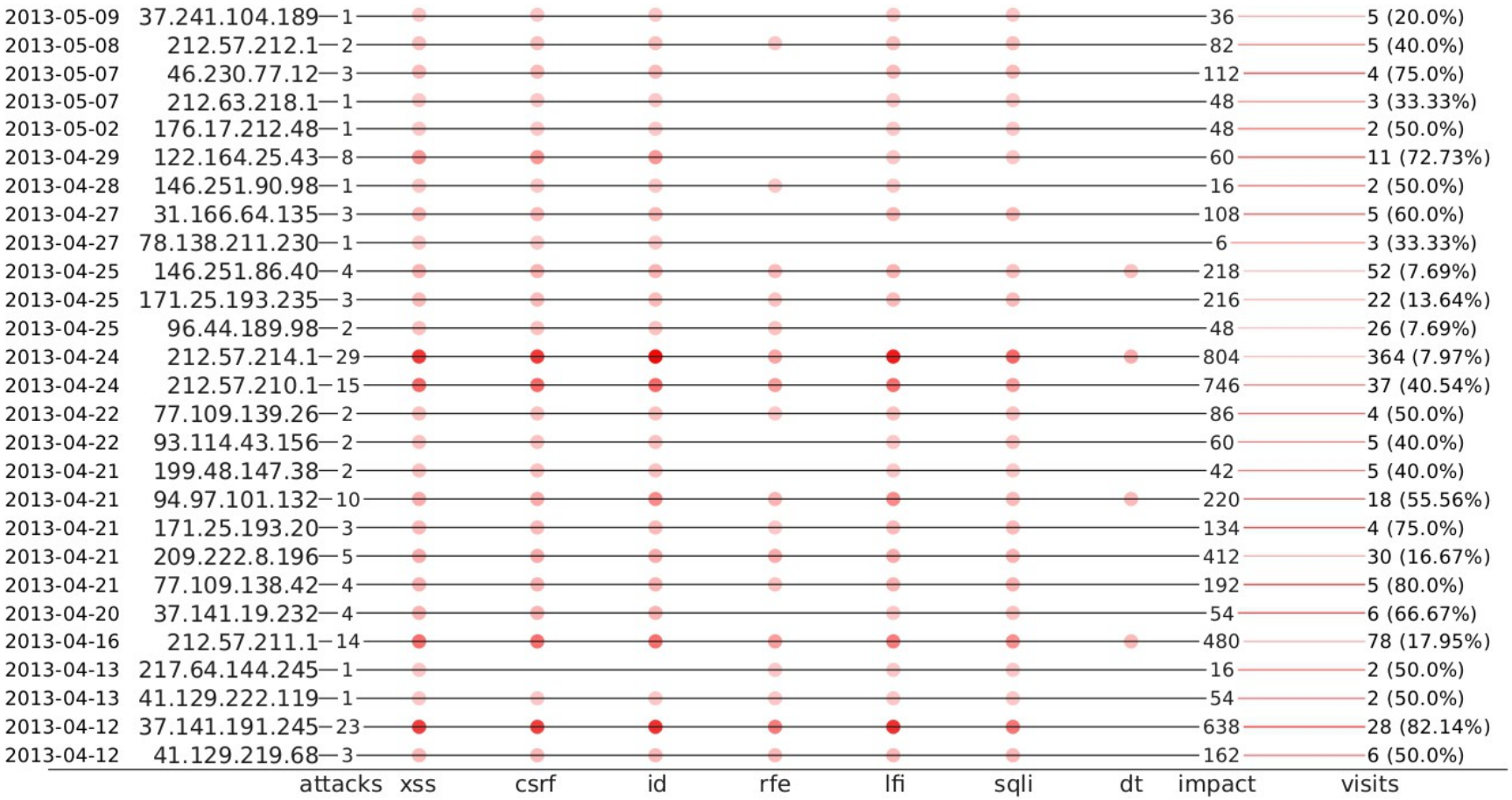
TreeView


(148) attacks
EG (4)
41.128.0.0/14 (4)
41.129.219.68 (3)
41.129.222.119 (1)
SA (111)
37.141.0.0/16 (27)
37.141.191.245 (23)
2013-04-12
2013-04-13
2013-04-15
37.141.19.232 (4)
2013-04-20
2013-04-23
212.57.192.0/19 (60)
212.57.211.1 (14)
2013-04-16
2013-04-25
212.57.210.1 (15)
2013-04-24
2013-04-25
212.57.214.1 (29)
2013-04-24
212.57.212.1 (2)
2013-05-08
94.96.0.0/14 (10)
94.97.101.132 (10)
2013-04-21
2013-04-22
146.251.0.0/16 (5)
146.251.86.40 (4)
2013-04-25
146.251.90.98 (1)
2013-04-28
78.138.192.0/18 (1)
78.138.211.230 (1)
2013-04-27
31.166.0.0/15 (3)
31.166.64.135 (3)
2013-04-27
11:19:01+03:00
36
xss csrf id sqli lfi
11:19:43+03:00
36
xss csrf id sqli lfi
11:25:12+03:00
36
xss csrf id sqli lfi
176.16.0.0/14 (1)
176.17.212.48 (1)
2013-05-02
46.230.0.0/17 (3)
46.230.77.12 (3)
2013-05-07
37.240.0.0/14 (1)
37.241.104.189 (1)
2013-05-09
Unknown (24)
Unknown (24)
217.64.144.245 (1)
77.109.138.42 (4)
171.25.193.20 (3)
93.114.43.156 (2)
77.109.139.26 (2)
171.25.193.235 (3)
122.164.25.43 (8)
212.63.218.1 (1)
US (7)
209.222.8.0/21 (5)
209.222.8.196 (5)
96.44.128.0/18 (2)
96.44.189.98 (2)
A1 (2)
199.48.147.32/27 (2)
199.48.147.38 (2)

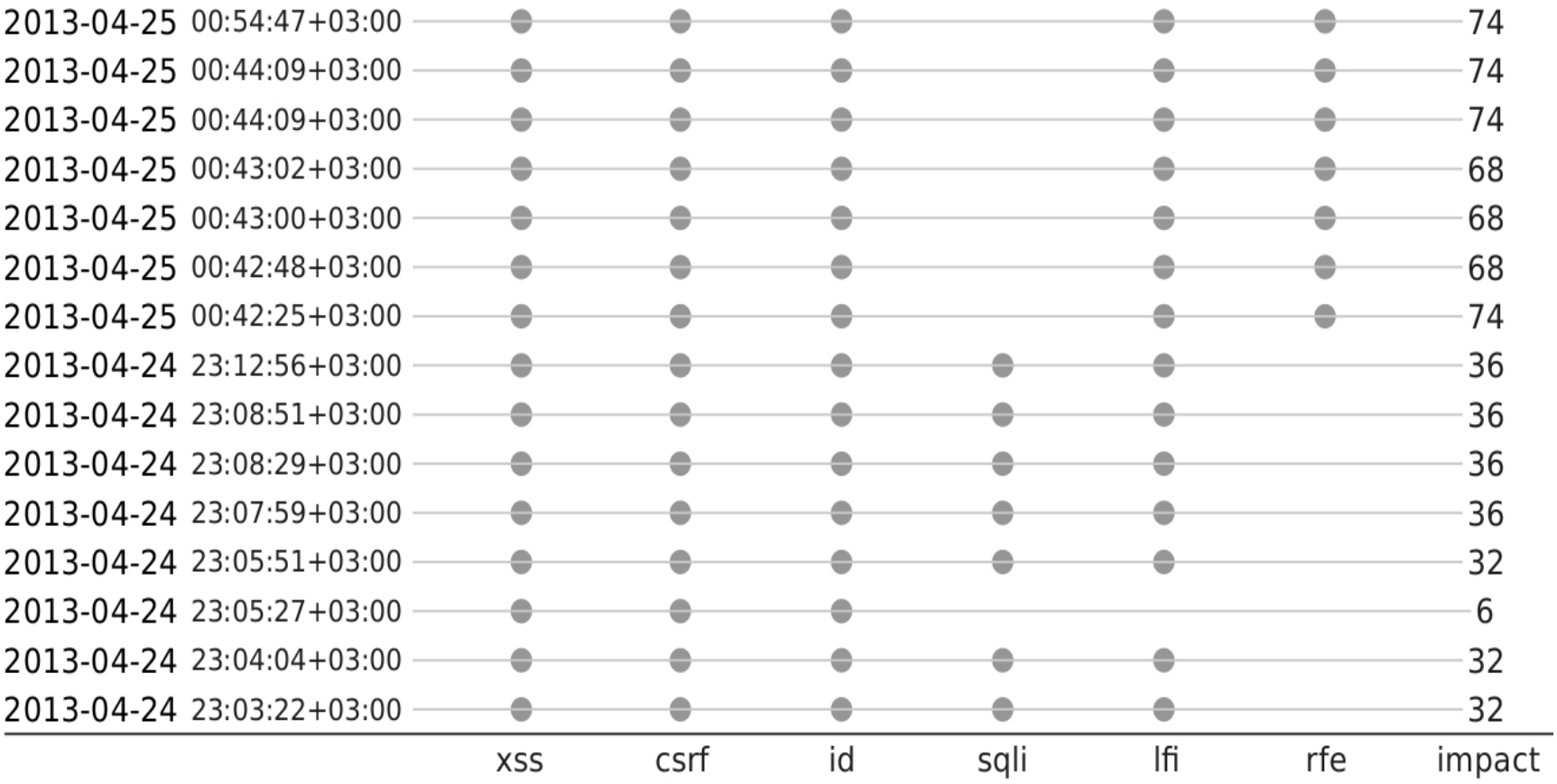
IP Address Aggregator



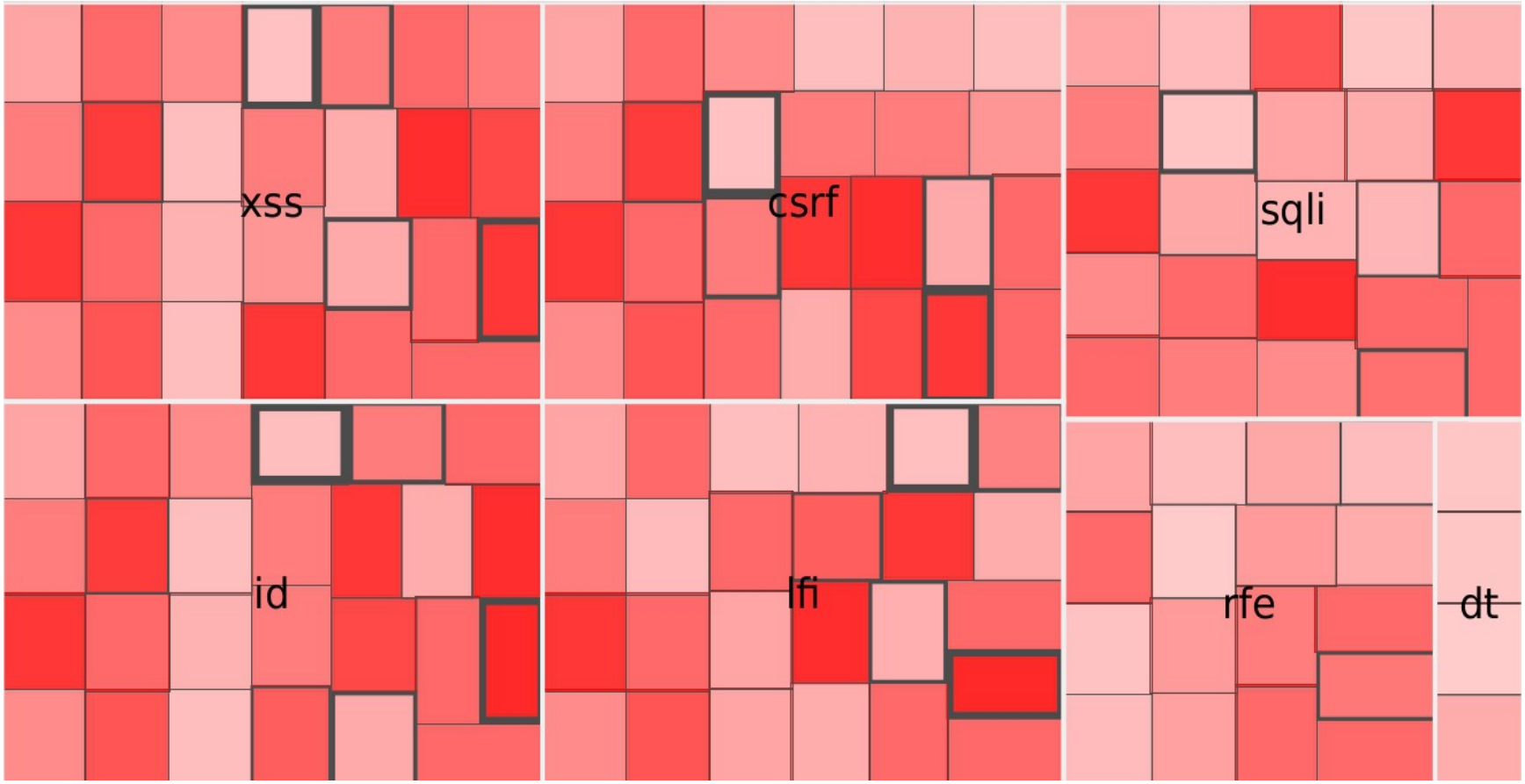
Attack Frequency View



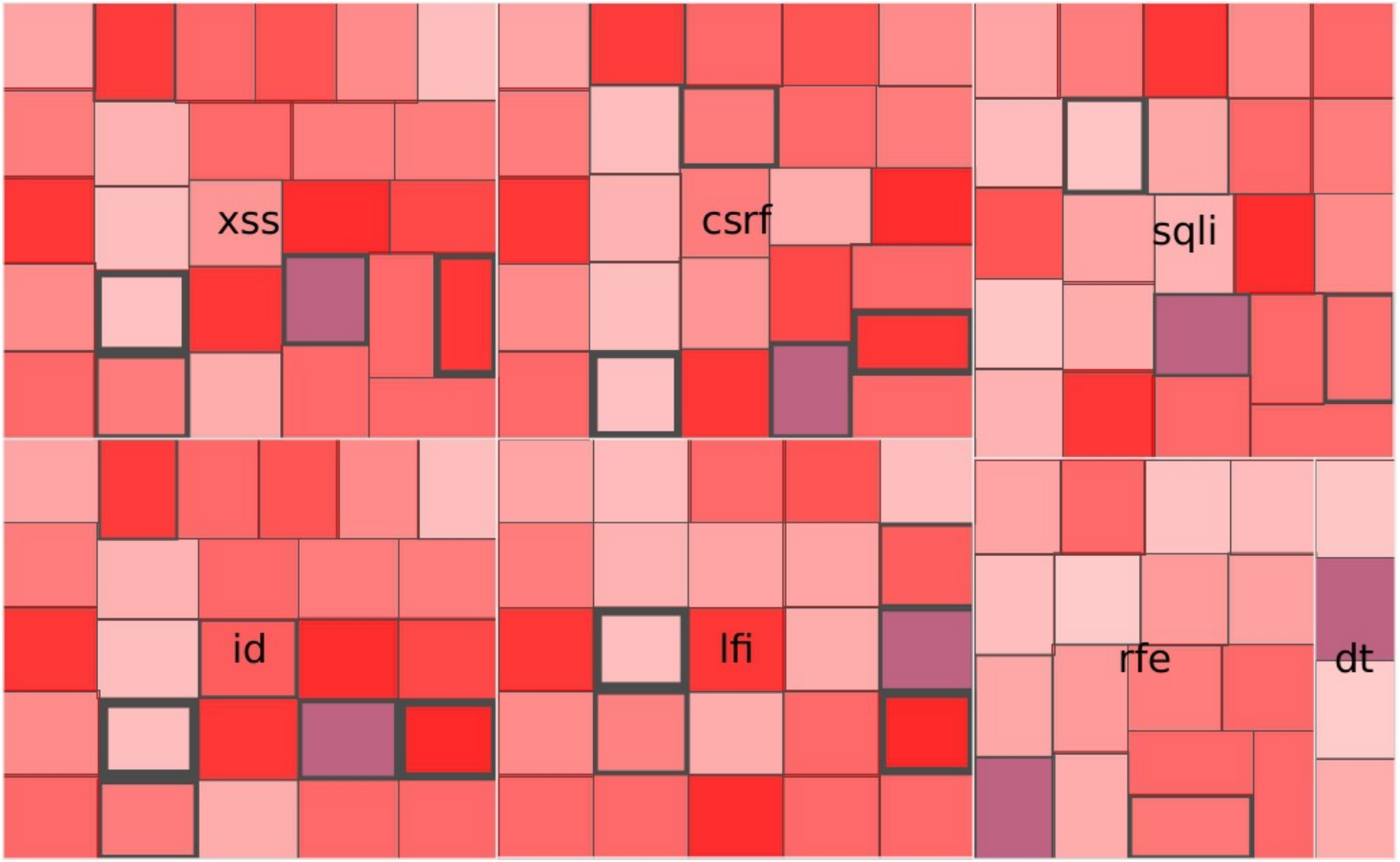
Attack Frequency View



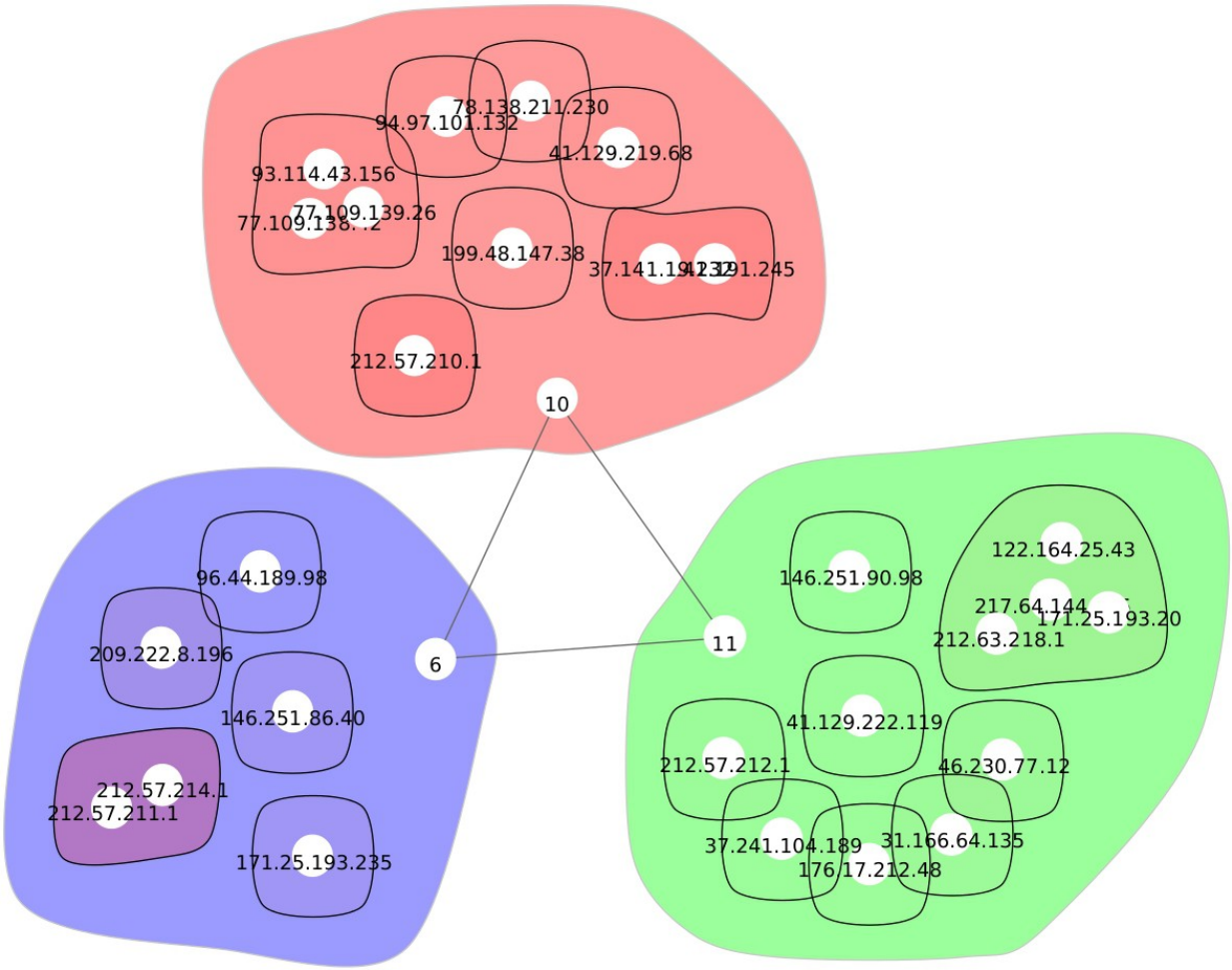
TreeMap



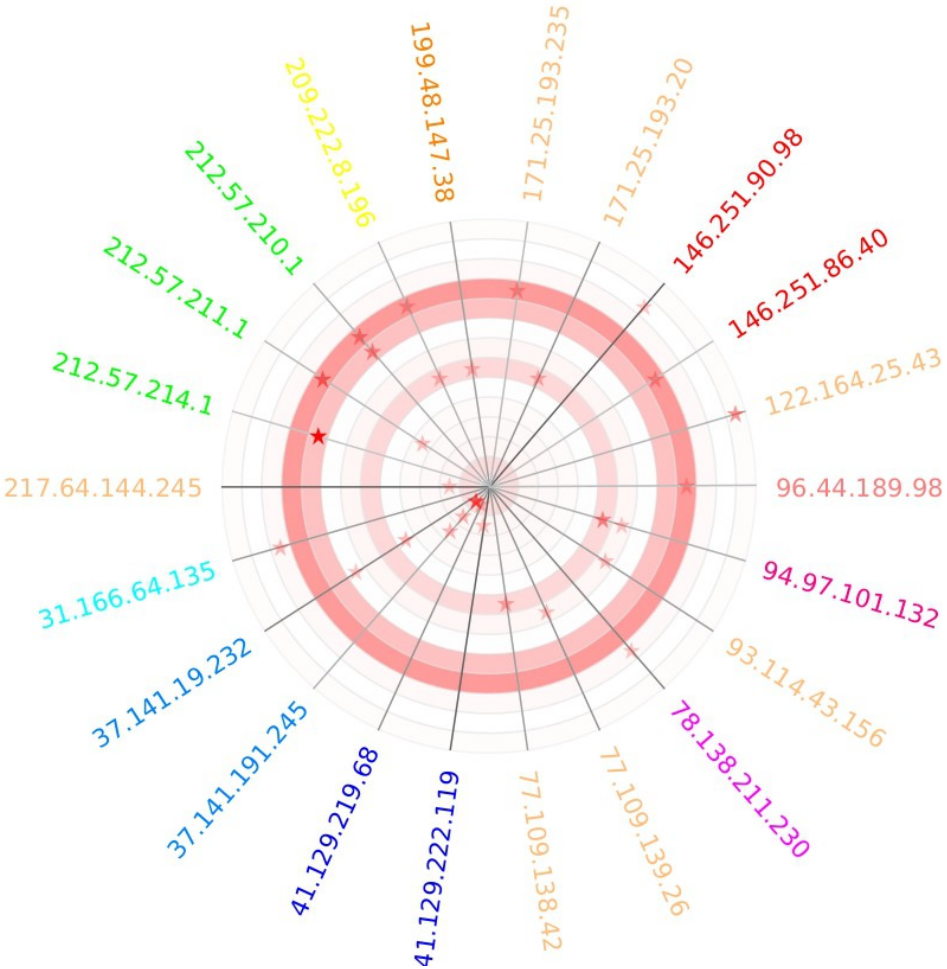
TreeMap



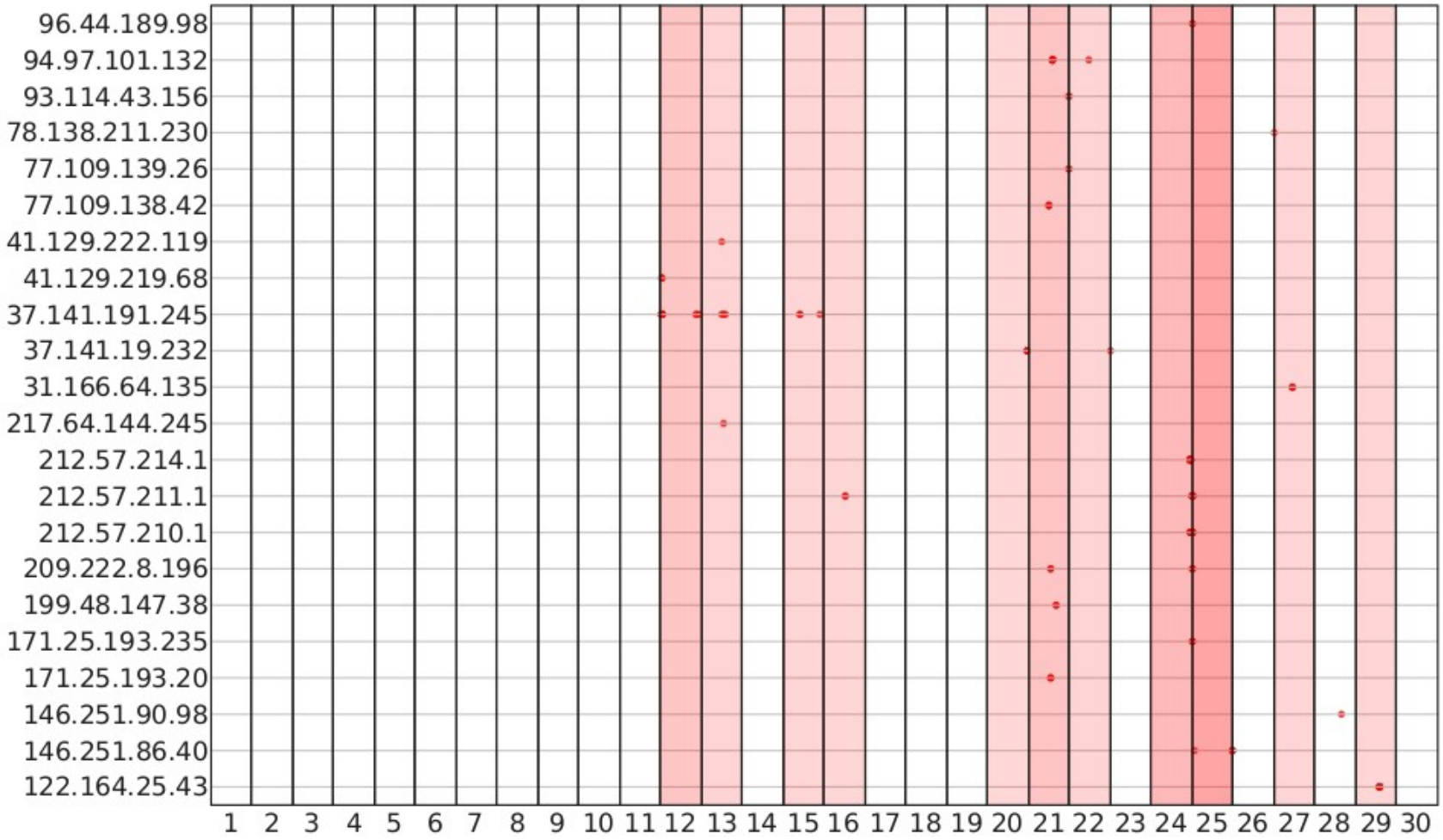
Attacker Aggregation



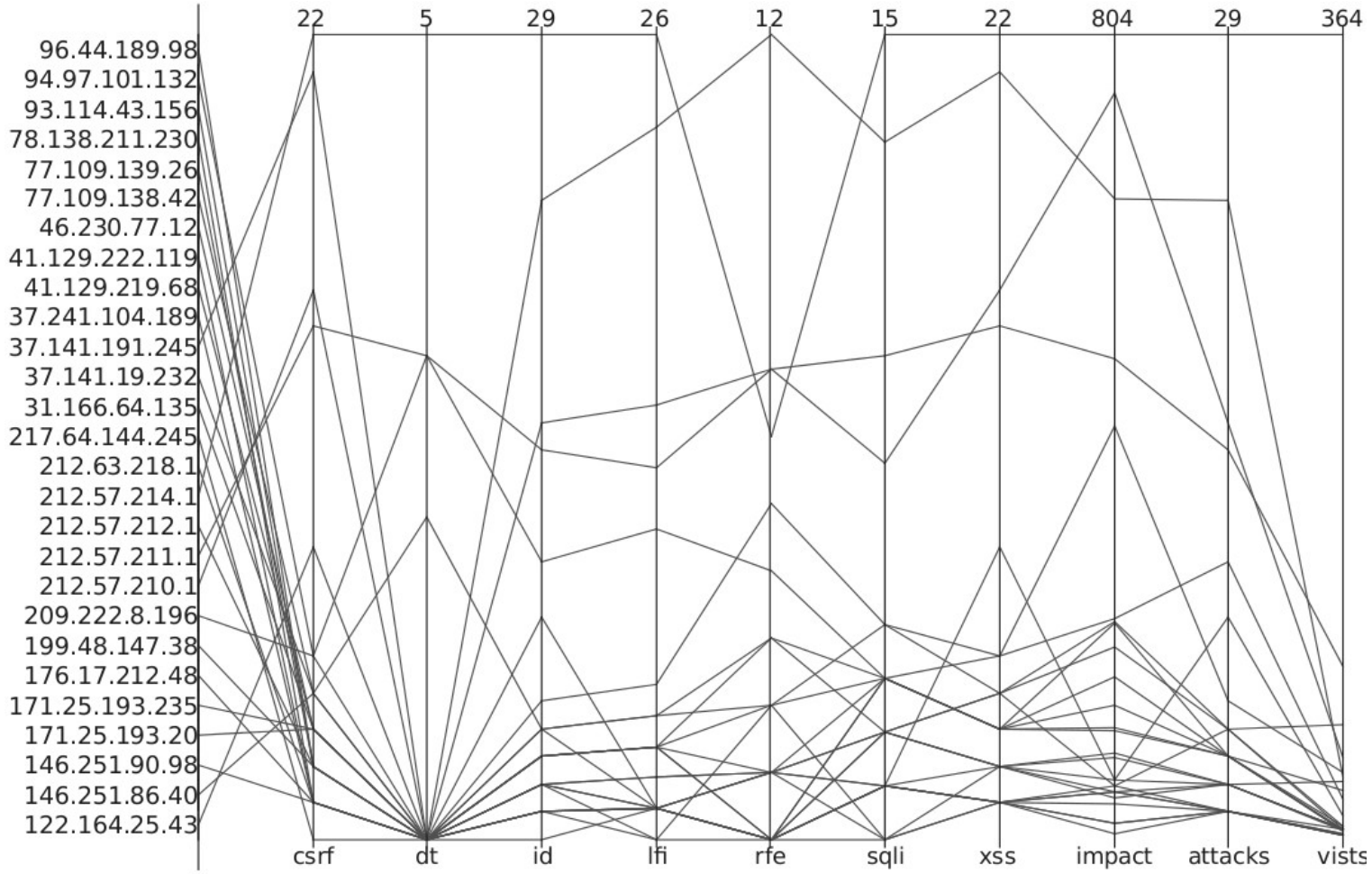
RingView


199.48.147.38
171.25.193.235
171.25.193.20
146.251.90.98
146.251.86.40
122.164.25.43
96.44.189.98
94.97.101.132
93.114.43.156
78.138.211.230
77.109.139.26
77.109.138.42
41.129.222.119
41.129.219.68
37.141.191.245
37.141.19.232
31.166.64.135
217.64.144.245
212.57.214.1
212.57.211.1
212.57.210.1
209.222.8.196

BarView


96.44.189.98
94.97.101.132
93.114.43.156
78.138.211.230
77.109.139.26
77.109.138.42
41.129.222.119
41.129.219.68
37.141.191.245
37.141.19.232
31.166.64.135
217.64.144.245
212.57.214.1
212.57.211.1
212.57.210.1
209.222.8.196
199.48.147.38
171.25.193.235
171.25.193.20
146.251.90.98
146.251.86.40
122.164.25.43
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30

Parallel Coordinates



Limitations and future work

- Different visual representations
- Cluttered plots
- Correlating other logs
- Experimenting on large logs
- Gathering feedback from administrators in the field

Conclusion

- PHPIDS visualization extension
- Analyzing and correlating PHPIDS and Apache web server log
- Using real-world PHPIDS and Apache log files
- Data visualization feature

Questions