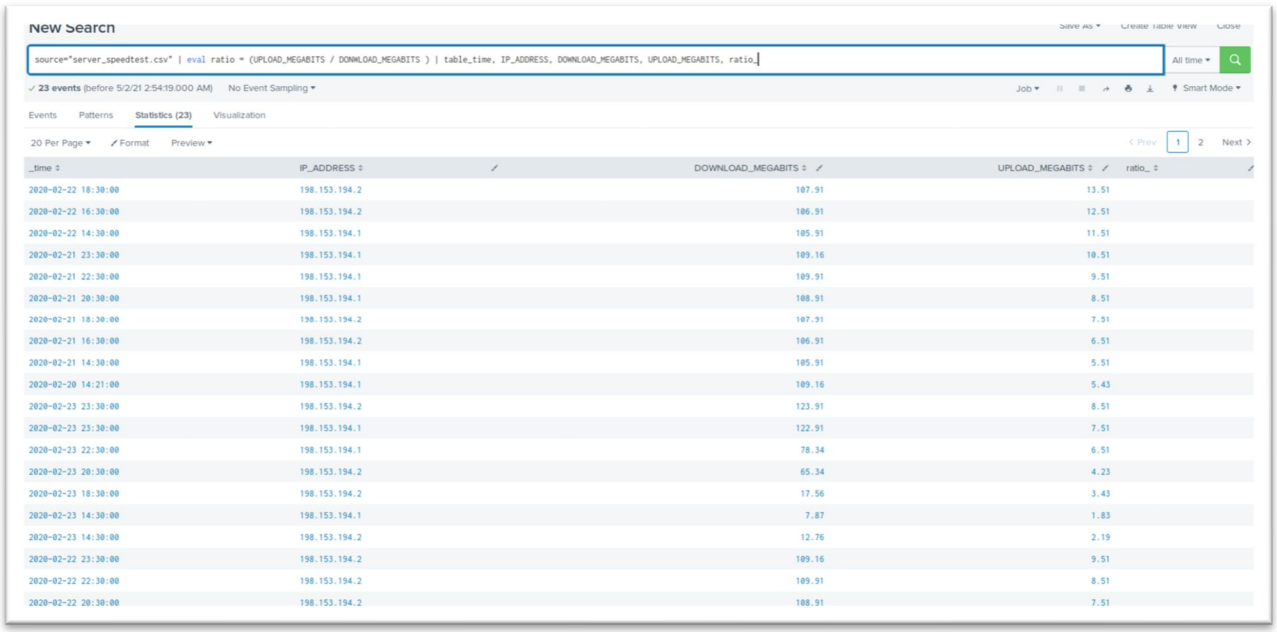
SIEM – Splunk Log Analysis

The Need for Speed:

1) Based on the report created, what is the approximate date and time of the attack?

02/23/2020 @ 14:30



New Search

source="server_speedtest.csv" | eval ratio = (UPLOAD_MEGABITS / DOWNLOAD_MEGABITS) | table_time, IP_ADDRESS, DOWNLOAD_MEGABITS, UPLOAD_MEGABITS, ratio_

All time

✓ 23 events (before 5/2/21 2:54:19.000 AM) No Event Sampling

Job Smart Mode

Events Patterns Statistics (23) Visualization

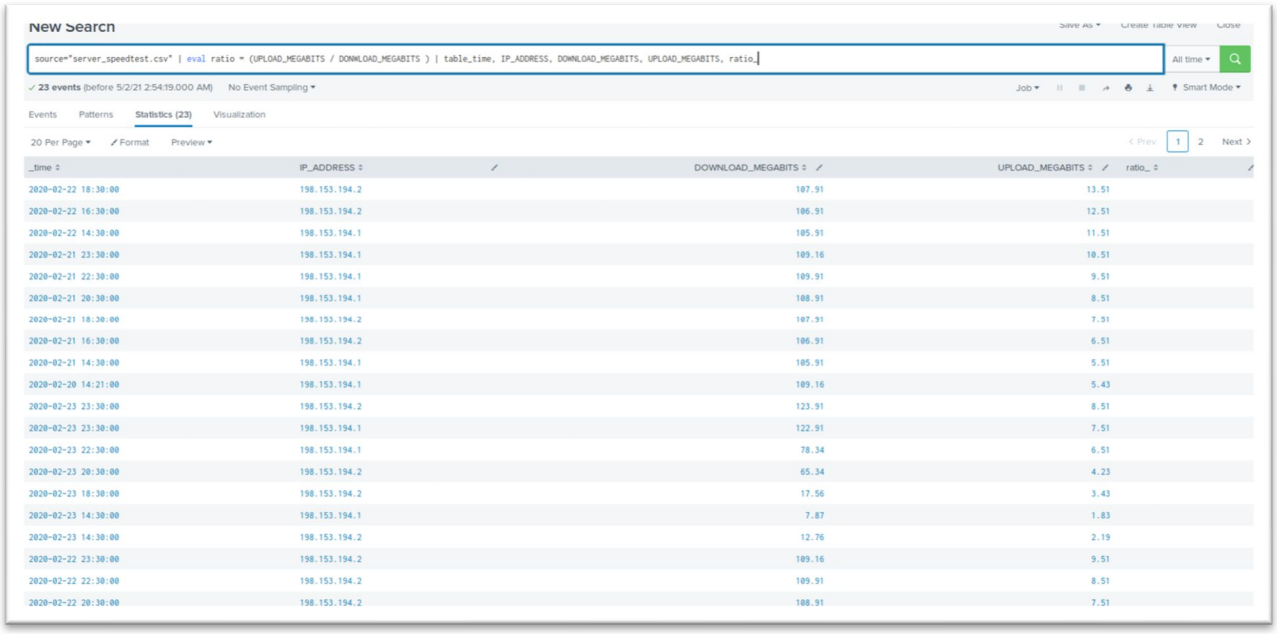
20 Per Page Format Preview

< Prev 1 2 Next >

_time	IP_ADDRESS	DOWNLOAD_MEGABITS	UPLOAD_MEGABITS	ratio_
2020-02-22 18:30:00	198.153.194.2	107.91	13.51	
2020-02-22 16:30:00	198.153.194.2	106.91	12.51	
2020-02-22 14:30:00	198.153.194.1	105.91	11.51	
2020-02-21 23:30:00	198.153.194.1	109.16	10.51	
2020-02-21 22:30:00	198.153.194.1	109.91	9.51	
2020-02-21 20:30:00	198.153.194.1	108.91	8.51	
2020-02-21 18:30:00	198.153.194.2	107.91	7.51	
2020-02-21 16:30:00	198.153.194.2	106.91	6.51	
2020-02-21 14:30:00	198.153.194.1	105.91	5.51	
2020-02-20 14:21:00	198.153.194.1	109.16	5.43	
2020-02-23 23:30:00	198.153.194.2	123.91	8.51	
2020-02-23 23:30:00	198.153.194.1	122.91	7.51	
2020-02-23 22:30:00	198.153.194.1	78.34	6.51	
2020-02-23 20:30:00	198.153.194.2	65.34	4.23	
2020-02-23 18:30:00	198.153.194.2	17.56	3.43	
2020-02-23 14:30:00	198.153.194.1	7.87	1.83	
2020-02-23 14:30:00	198.153.194.2	12.76	2.19	
2020-02-22 23:30:00	198.153.194.2	109.16	9.51	
2020-02-22 22:30:00	198.153.194.2	109.91	8.51	
2020-02-22 20:30:00	198.153.194.2	108.91	7.51	

2) How long did it take your systems to recover?

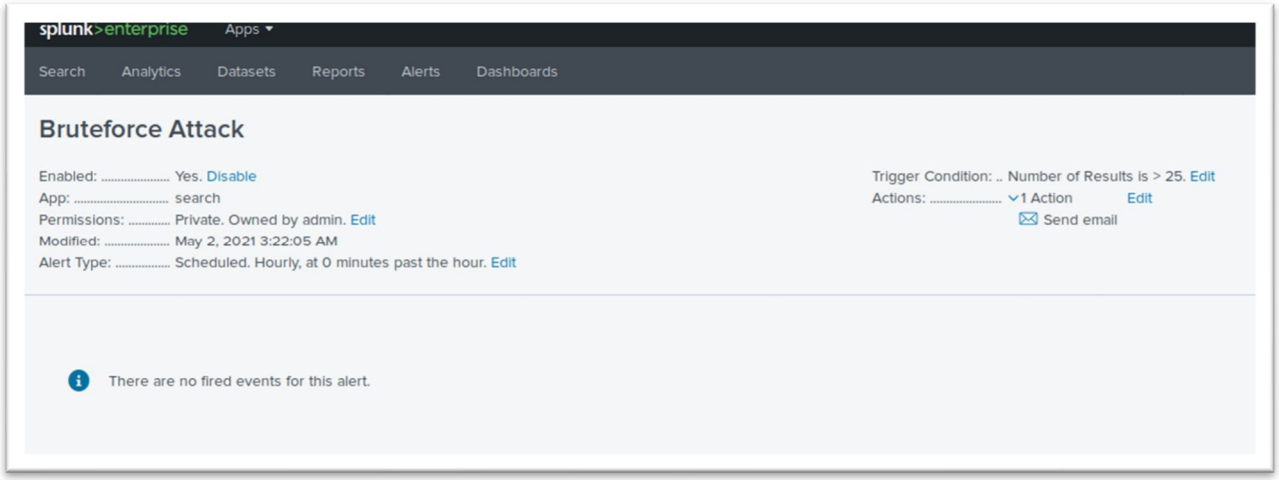
9 hours at 23:30

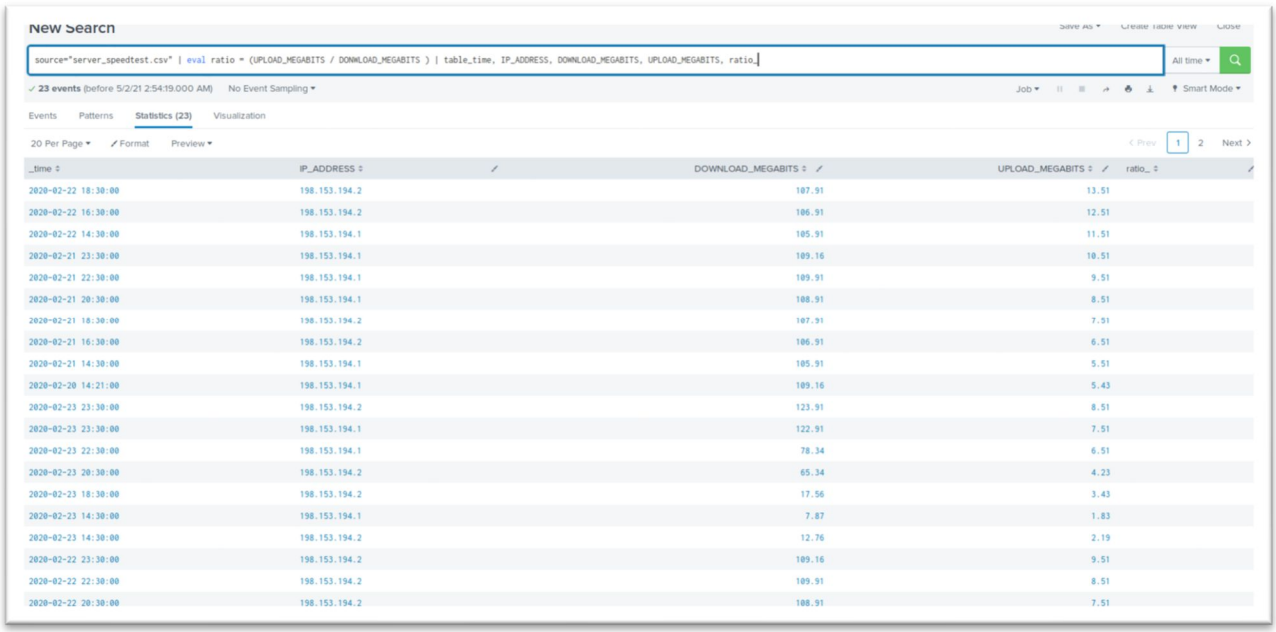


Drawing the (base)line:

1) When did the brute force attack occur?

Since there were 23 suspicious events that occurred at 4AM on 2/21/2020, attack probably happened then.





_time	IP_ADDRESS	DOWNLOAD_MEGABITS	UPLOAD_MEGABITS	ratio_
2020-02-22 18:30:00	198.153.194.2	107.91	13.51	
2020-02-22 16:30:00	198.153.194.2	106.91	12.51	
2020-02-22 14:30:00	198.153.194.1	105.91	11.51	
2020-02-21 23:30:00	198.153.194.1	109.16	10.51	
2020-02-21 22:30:00	198.153.194.1	109.91	9.51	
2020-02-21 20:30:00	198.153.194.1	108.91	8.51	
2020-02-21 18:30:00	198.153.194.2	107.91	7.51	
2020-02-21 16:30:00	198.153.194.2	106.91	6.51	
2020-02-21 14:30:00	198.153.194.1	105.91	5.51	
2020-02-20 14:21:00	198.153.194.1	109.16	5.43	
2020-02-23 23:30:00	198.153.194.2	123.91	8.51	
2020-02-23 23:30:00	198.153.194.1	122.91	7.51	
2020-02-23 22:30:00	198.153.194.1	78.34	6.51	
2020-02-23 20:30:00	198.153.194.2	65.34	4.23	
2020-02-23 18:30:00	198.153.194.2	17.56	3.43	
2020-02-23 14:30:00	198.153.194.1	7.87	1.83	
2020-02-23 14:30:00	198.153.194.2	12.76	2.19	
2020-02-22 23:30:00	198.153.194.2	109.16	9.51	
2020-02-22 22:30:00	198.153.194.2	109.91	8.51	
2020-02-22 20:30:00	198.153.194.2	108.91	7.51	