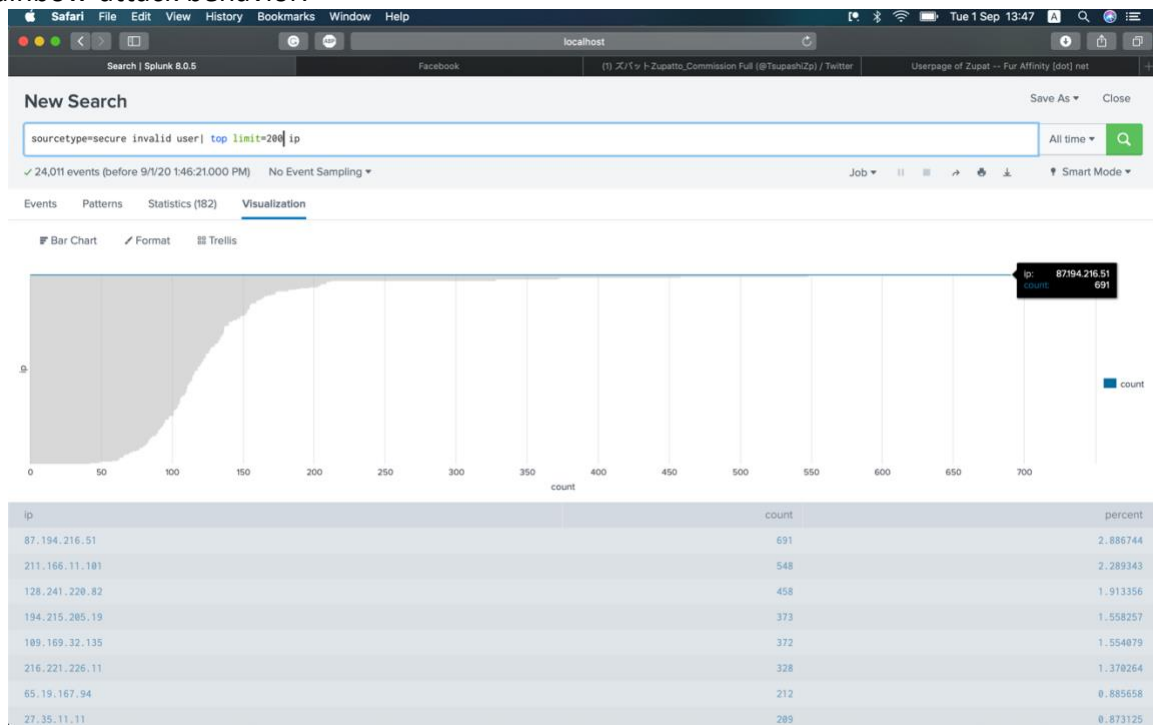


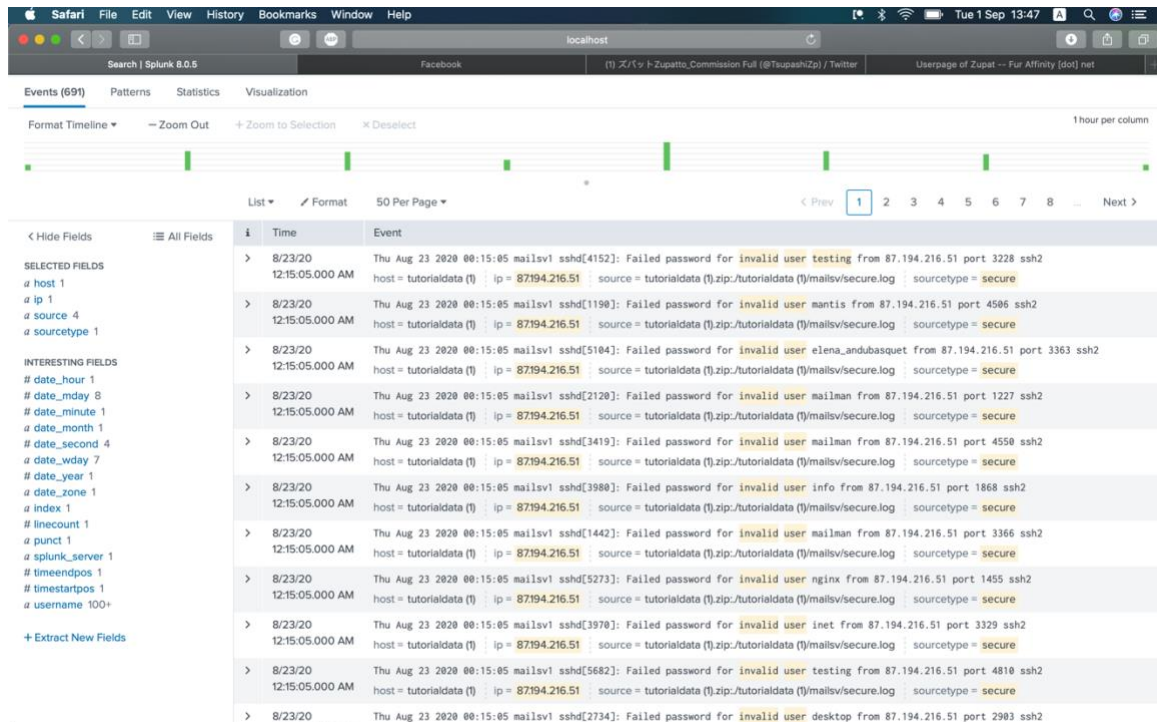
## Activity-IV Log Analysis

Q1 - How many hackers are trying to get access to our servers? And how many attempts are there?

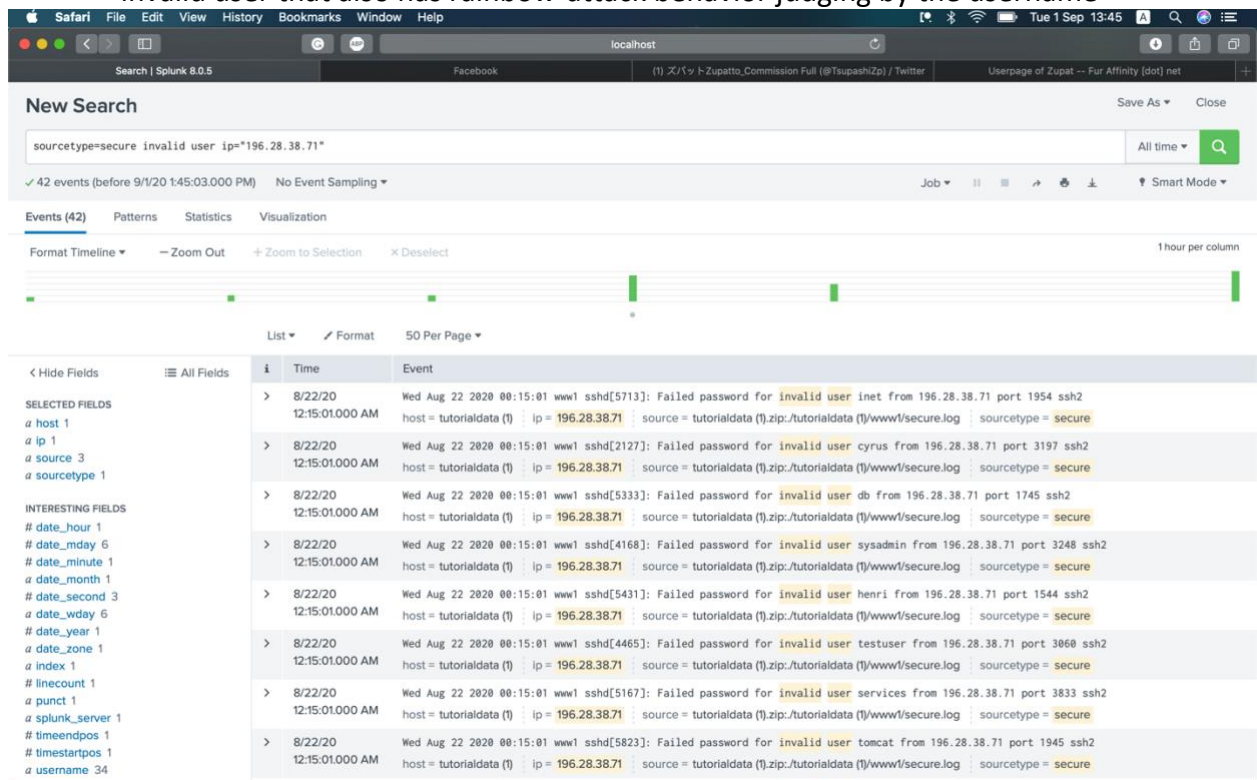
Query for “invalid user” attempts showed a lot of IP that is trying to rainbow-attack the servers. There are total of **182 different ips with 24011 attempts** trying to log in with rainbow-attack behavior.



The picture below shows attempts from 87.194.216.51 which has the most attempt with invalid user, also has rainbow-attack behavior judging by the username



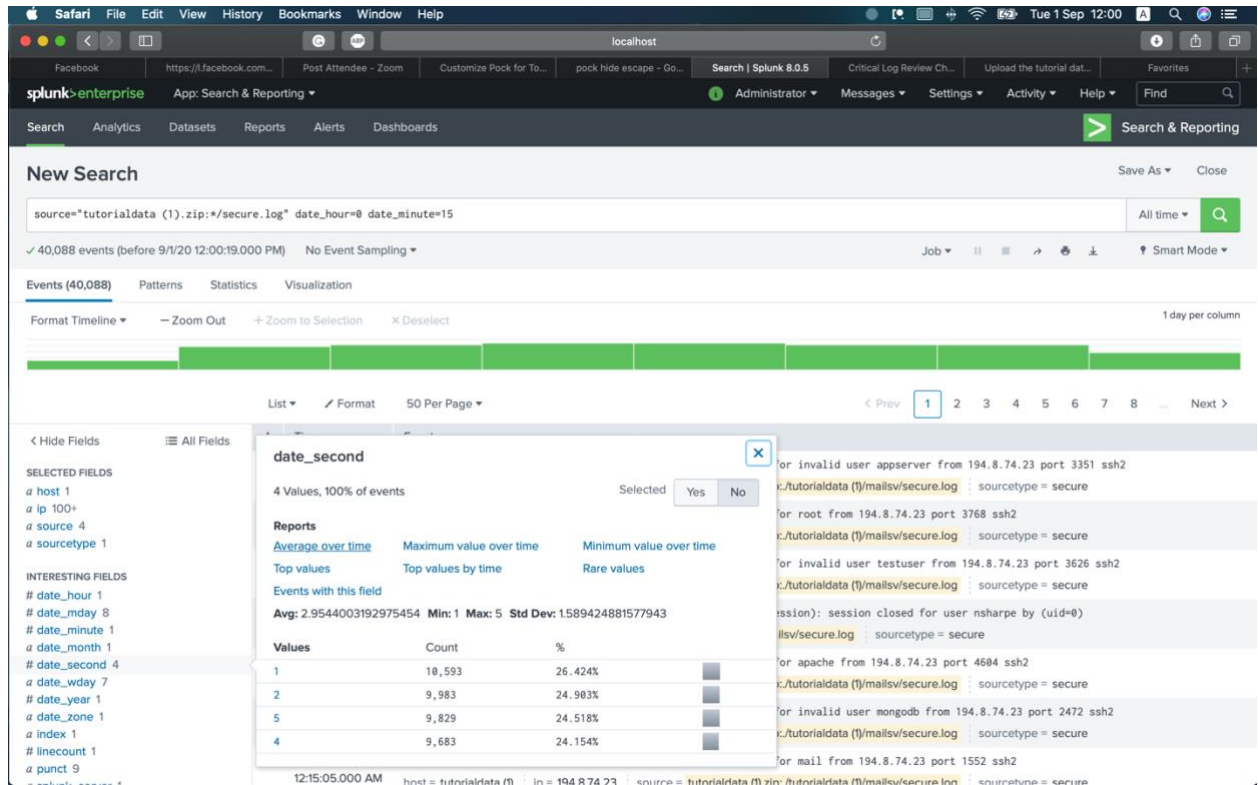
The picture below shows attempts from 196.28.38.71 which has the least attempt with invalid user that also has rainbow-attack behavior judging by the username



So it is safe to conclude that there are total of 182 hackers and 24011 attempts

Q2

12:15 AM seems to be the most favorable time (almost the only time) that the hackers favor the most



Q3

www1 seems to have most attempts (10593 attempts).

**Splunk Enterprise** App: Search & Reporting

**New Search** Save As Close

source="tutorialdata (1).zip:\*/secure.log" All time Q

✓ 40,088 events (before 9/1/20 12:01:03.000 PM) No Event Sampling

Events (40,088) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 day per column

**source** 4 Values, 100% of events Selected Yes No

**Reports** Top values Top values by time Rare values

**Values**

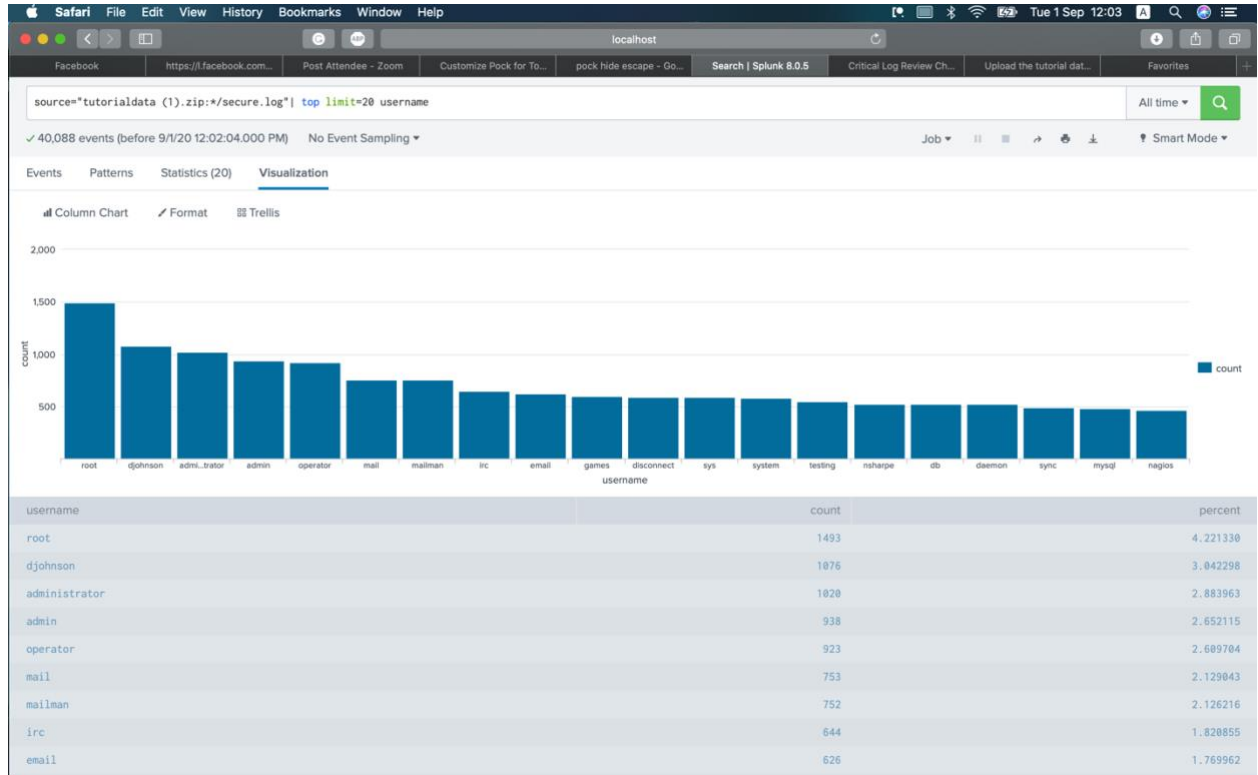
Values	Count	%
tutorialdata (1).zip:./tutorialdata (1)/www1/secure.log	10,593	26.424%
tutorialdata (1).zip:./tutorialdata (1)/www3/secure.log	9,983	24.903%
tutorialdata (1).zip:./tutorialdata (1)/mailsv/secure.log	9,829	24.518%
tutorialdata (1).zip:./tutorialdata (1)/www2/secure.log	9,683	24.154%

**INTERESTING FIELDS**

- # date\_hour 1
- # date\_mday 8
- # date\_minute 1
- # date\_month 1
- # date\_second 4
- # date\_wday 7
- # date\_year 1
- # date\_zone 1
- # index 1
- # linecount 1
- # punct 9

for invalid user appserver from 194.8.74.23 port 3351 ssh2  
 tutorialdata (1)/mailsv/secure.log : sourcetype = secure  
 for root from 194.8.74.23 port 3768 ssh2  
 tutorialdata (1)/mailsv/secure.log : sourcetype = secure  
 for invalid user testuser from 194.8.74.23 port 3626 ssh2  
 tutorialdata (1)/mailsv/secure.log : sourcetype = secure  
 session): session closed for user nsharpe by (uid=0)  
 tutorialdata (1)/mailsv/secure.log : sourcetype = secure  
 for apache from 194.8.74.23 port 4604 ssh2  
 tutorialdata (1)/mailsv/secure.log : sourcetype = secure  
 Thu Aug 23 2020 00:15:05 mailsv sshd[3760]: Failed password for invalid user mongodb from 194.8.74.23 port 2472 ssh2  
 host = tutorialdata (1) ip = 194.8.74.23 source = tutorialdata (1).zip:./tutorialdata (1)/mailsv/secure.log : sourcetype = secure  
 Thu Aug 23 2020 00:15:05 mailsv sshd[4998]: Failed password for mail from 194.8.74.23 port 1552 ssh2  
 host = tutorialdata (1) ip = 194.8.74.23 source = tutorialdata (1).zip:./tutorialdata (1)/mailsv/secure.log : sourcetype = secure

Q4

Most popular account would be **root** (1493 attempts).

Q5

**Password.pdf** (which does not exist in the web service, as all status code are 404)

**Safari** File Edit View History Bookmarks Window Help

localhost

Facebook | https://l.facebook.com... | Post Attendee - Zoom | Customize Pock for To... | pock hide escape - Go... | Search | Splunk 8.0.5 | Critical Log Review Ch... | Upload the tutorial dat... | Favorites

**splunk>enterprise** App: Search & Reporting Administrator Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

### New Search

source="tutorialdata (1).zip:/access.log" top limit=20 file All time

✓ 39,532 events (before 9/1/20 12:04:29.000 PM) No Event Sampling Job Visualization

Events Patterns Statistics (14) Visualization

Bar Chart Format Trellis

file	count	percent
cart.do	12653	32.006982
product.screen	9932	25.123950
category.screen	6885	17.416270
oldlink	6871	17.380856
success.do	2154	5.448750

**Safari** File Edit View History Bookmarks Window Help

localhost

Facebook | https://l.facebook.com... | Post Attendee - Zoom | Customize Pock for To... | pock hide escape - Go... | Search | Splunk 8.0.5 | Critical Log Review Ch... | Upload the tutorial dat... | Favorites

**splunk>enterprise** App: Search & Reporting Administrator Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

### New Search

source="tutorialdata (1).zip:/access.log" file="passwords.pdf" All time

✓ 68 events (before 9/1/20 12:04:33.000 PM) No Event Sampling Job Visualization

Events (68) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 hour per column

List Format 50 Per Page Prev 1 2 Next

< Hide Fields All Fields

SELECTED FIELDS

- a host 1
- a source 3
- a sourcetype 1

INTERESTING FIELDS

- a action 5
- # bytes 66
- a clientip 54
- # date\_hour 22
- # date\_mday 8
- # date\_minute 46
- # date\_month 1
- # date\_second 44
- # date\_wday 7
- # date\_year 1
- a file 1

i	Time	Event
>	8/23/20 2:54:08.000 PM	175.44.1.172 - - [23/Aug/2020:14:54:08] "POST /passwords.pdf?JSESSIONID=SD10SL2FF3ADFF51999 HTTP 1.1" 404 2388 "http://www.buttercupgames.com/oldlink?itemId=EST-6" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; MS-RTC LM 8; InfoPath.2)" 1 02 host = tutorialdata (t)   source = tutorialdata (t).zip:/tutorialdata (t)/www1/access.log   sourcetype = access_combined_wcookie
>	8/23/20 12:38:50.000 PM	198.35.1.10 - - [23/Aug/2020:12:38:50] "POST /passwords.pdf?JSESSIONID=SD9SL3FF3ADFF51356 HTTP 1.1" 404 446 "http://www.buttercupgames.com/product.screen?productId=SF-BVS-G01" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; BOIE9;ENUS)" 542 host = tutorialdata (t)   source = tutorialdata (t).zip:/tutorialdata (t)/www2/access.log   sourcetype = access_combined_wcookie
>	8/23/20 12:07:15.000 PM	59.36.99.70 - - [23/Aug/2020:12:07:15] "GET /passwords.pdf?JSESSIONID=SD3SL5FF4ADFF51205 HTTP 1.1" 404 2152 "http://www.buttercupgames.com/oldlink?itemId=EST-26" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 162 host = tutorialdata (t)   source = tutorialdata (t).zip:/tutorialdata (t)/www1/access.log   sourcetype = access_combined_wcookie
>	8/23/20 7:51:55.000 AM	198.35.3.23 - - [23/Aug/2020:07:51:55] "GET /passwords.pdf?JSESSIONID=SD1SL6FF4ADFF50222 HTTP 1.1" 404 2272 "http://www.buttercupgames.com/cart.do?action=view&itemId=EST-7" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.2; .NET CLR 1.1.4322; InfoPath.1; MS-RTC LM 8)" 355 host = tutorialdata (t)   source = tutorialdata (t).zip:/tutorialdata (t)/www1/access.log   sourcetype = access_combined_wcookie
>	8/23/20 2:19:36.000 AM	178.162.239.192 - - [23/Aug/2020:02:19:36] "GET /passwords.pdf?JSESSIONID=SD10SL7FF10ADFF48635 HTTP 1.1" 404 3741 "http://www.buttercupgames.com/category.screen?categoryId=NULL" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_6_8) AppleWebKit/534.55.3 (KHTML, like Gecko) Version/5.1.5 Safari/534.55.3" 681



The screenshot shows a Splunk search interface with a list of events and a summary report for the 'status' field.

**Search Results (List View):**

Time	Event
8/23/20 7:51:55.000 AM	198.35.3.23 - - [23/Aug/2020:07:51:55] "GET /passwords.pdf?JSESSIONID=SD1SL6FF4ADFF50222 HTTP 1.1" 404 2272 "http://www.buttercupgames.com/cart.do?action=view&itemId=EST-7" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.2; .NET CLR 1.1.4322; InfoPath.1; MS-RTC LM 8)" 355
8/23/20 2:19:36.000 AM	178.162.239.192 - - [23/Aug/2020:02:19:36] "GET /passwords.pdf?JSESSIONID=SD18SL7FF10ADFF48635 HTTP 1.1" 404 3741 "http://www.buttercupgames.com/category.screen?categoryId=NULL" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_6_8) AppleWebKit/534.55.3 (KHTML, like Gecko) Version/5.1.5 Safari/534.55.3" 601
8/22/20 10:45:49.000 AM	69.72.161.186 - - [22/Aug/2020:10:45:49] "POST /passwords.pdf?JSESSIONID=SD0SL9FF2ADFF44039 HTTP 1.1" 404 3756 "http://www.buttercupgames.com/product.screen?productId=SF-BVS-G01" "Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_6_3; en-US) AppleWebKit/533.4 (KHTML, like Gecko) Chrome/5.0.375.38 Safari/533.4" 538
8/22/20 9:03:24.000 AM	99.61.68.230 - - [22/Aug/2020:09:03:24] "POST /passwords.pdf?JSESSIONID=SD5SL8FF7ADFF43135 HTTP 1.1" 404 3946 "http://www.buttercupgames.com/product.screen?productId=SF-BVS-G01" "Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1055.1" 458

**Summary Report (Status):**

1 Value, 100% of events

Values	Count	%
404	68	100%

Q6

Password.pdf (reasoning in Q5 above)