**Splunk questions**

**Access log**

1.How many successful events occurred?

**status=200**

1. 34282
2. 37589
3. 28597
4. 31558

2.How many failed events occurred?

**status!=200**

1. 6482
2. 5250
3. 4724
4. 10415

3.Which day had the most successful events?

**status=200**

1. April 21, 2014
2. May 25, 2014
3. April 25, 2014
4. April 27, 2014

4.Which day had the most failed events?

**status!=200**

1. April 21, 2014
2. May 5, 2014
3. April 20, 2014
4. May 25, 2014

5.How many purchase attempts were made?

**action=purchase**

1. 5737
2. 6825
3. 4587
4. 5485

6.Which day had the most purchase attempts?

**action=purchase**

1. May 20, 2014
2. April 24, 2014
3. May 10, 2014
4. April 21, 2014

7.How many successful purchases were made?

**action=purchase status=200**

1. 5189
2. 6247
3. 5224
4. 4851

8.How many unsuccessful purchases were made?

**action=purchase status!=200**

1. 584
2. 513
3. 458
4. 685

9.Which log had the most successful events?

**status=200 | top limit=10 source**

1. www1/access.log
2. www1/secure.log
3. www2/access.log
4. www2/secure.log

10.Which log had the most failed events?

**status!=200 | top limit=10 source**

1. www3/access.log
2. www3/secure.log
3. www2/secure.log
4. www1/access.log

11.What IP address made the most purchases on Strategy games using Mozilla browser?

**action=purchase "categoryid=strategy" "Mozilla" | top limit=100 clientip**

1. 128.241.220.82
2. 182.236.164.11
3. 198.35.1.75
4. 71.192.86.205

12.How many POST requests were made from google.com on WC-SH-G04 item?

**post "google" "productid=wc-sh-g04"**

1. 25
2. 36
3. 29
4. 34

13.Which day was the third most successful day for Arcade games in sell?

**"categoryid=arcade" action=purchase**

1. April 28, 2014
2. April 24, 2014
3. April 26, 2014
4. April 30, 2014

14. For the www2/access.log how many events are there by using a Mozilla browser and a GET method request?

**source="\*www2/access.log" "mozilla" AND method=GET**

1. 7,758
2. 8,058
3. 7,669
4. 8,581

15.For the www1/access.log, in which day were the most strategy games sold?

**source="\*www1/access.log" "categoryid=strategy" action=purchase**

1. April 28, 2014
2. April 30, 2014
3. April 26, 2014
4. April 24, 2014

16. What is the number of accesses for POST from any IP address which starts with 198?

**post | regex \_raw="198\.\d{1,3}\.\d{1,3}\.\d{1,3}"**

1. 451
2. 401
3. 502
4. 536

17.How many simulation games were sold?  
**“categoryid=simulation”**

1. 1525
2. 1690
3. 1445
4. 2000

18**.** What is the number of accesses for GET from any IP address which starts with 81?

**get | regex \_raw="81\.\d{1,3}\.\d{1,3}\.\d{1,3}"**

1. 249
2. 276
3. 496
4. 369

**Secure log**

19.What is the most secure date in terms of fewer failed passwords?

**source="c:\buttercup.zip:.\buttercup/www1/secure.log" "failed" password**

1. April 24, 2014
2. May 21, 2014
3. April 19, 2014
4. May 24, 2014

20.How many failed password attempts were there?

**fail\* password**

1. 35754
2. 33253
3. 37845
4. 31241

21.How many errors have occurred using a Chrome browser?

**chrome AND error**

1. 98
2. 95
3. 89
4. 87

22. What is the first IP address that gave an incorrect password?

**fail\* password | reverse**

1. 118.142.68.222
2. 155.225.10.25
3. 125.2.3.98
4. 10.2.59.210

23. What status code has a signal.zip file?

**source="access.log" signals.zip**

1. 200
2. 400
3. **404**
4. 502

24. How many successful events are in www1/access.log and www1/secure.log together?

**Look for events!**

1. 48442
2. 45252
3. 40250
4. 50000

25. What is the percentage of numbers of “not found “status in access logs?

**source="buttercup.zip:.\\buttercup/www1/access.log" | top limit=10 status**

1. 1.56
2. 2.56
3. 10.5
4. 1.79

26. How many events have html documents with a 200 status code in access logs?

**source="buttercup.zip:.\\buttercup/www1/access.log" | regex \_raw="[a]+\.html" | top limit=10 status**

1. 34
2. 26
3. 15
4. 0

27. How many events occurred in access log launched from 87.194.216.51 and accessed the .uk domain?

**source="buttercup.zip:.\\buttercup/www1/access.log" clientip="87.194.216.51" | regex \_raw="[a-zA-Z\.]+\.(uk)"**

1. 25
2. 36
3. 0
4. 9

28. How many events occurred at 59th minute linked to access.log which has an IP address ending in x.x.124.50 (x is random)

**source="buttercup.zip:.\\buttercup/www1/access.log" | regex \_raw="[0-9]{2}\:59\:[0-9]{2}" | regex \_raw="\d{1,3}.\d{1,3}.124.50"**

1. 25
2. 16
3. 32
4. 0

29. What is the latest event in access log that occurred on Saturday at 17th min, including category.screen?

**source="buttercup.zip:.\\buttercup/www1/access.log" method=POST file="category.screen" date\_wday="saturday" date\_minute=17**

1. 10:17
2. 9:17
3. 8:17
4. 7:17

30. What is the host name that was accessed from port 2111 (secure log) at 2nd second?

**source="buttercup.zip:.\\buttercup/www1/secure.log" date\_second=2 2111**

1. LAPTOP-70H25MRC
2. LAPTOP-86H45MTG
3. LAPTOP-79H25TFD
4. None of the above