Analysis of NetFlow Capture 1:

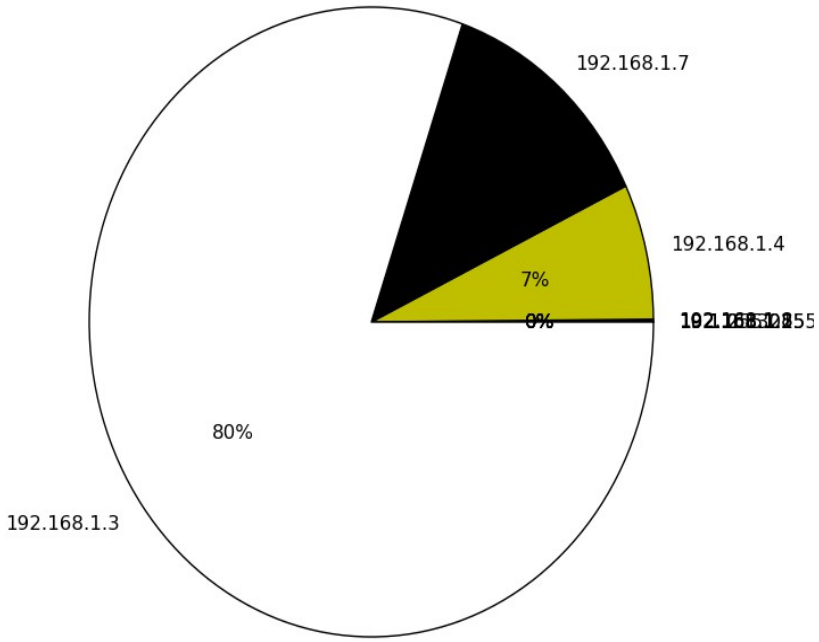
Upon initial review of the remote sites graph, we have determined that the network was utilized the most by streaming music from Pandora, taking up about 78% of the data consumed among the top 10 remote sites. Akamai technologies accounted for roughly 8% of data consumed. Other sites among the top 10 include Google search engine, Google DNS, Edgecast networks, and Level 3 Communications, who together consumed about 14% of data out of the top 10.

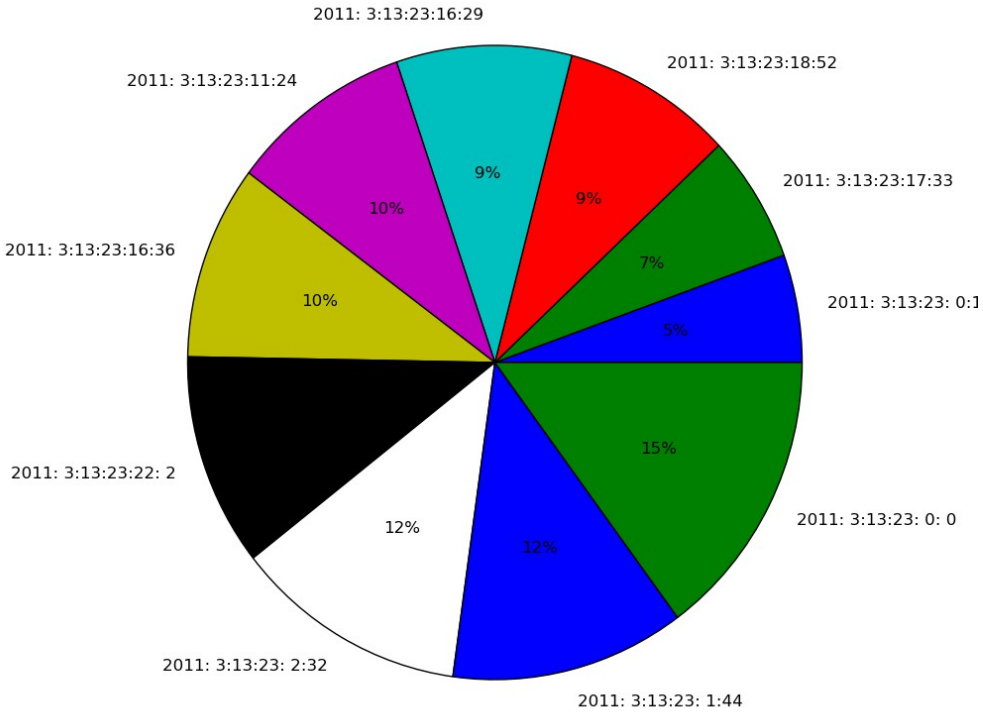
We have also found that the host/user at IP 192.168.1.3 single-handedly consumed about 80% of the web traffic shared among the top 10. There is a strong correlation between this users data consumption and excessive amount of Pandora traffic on the network.

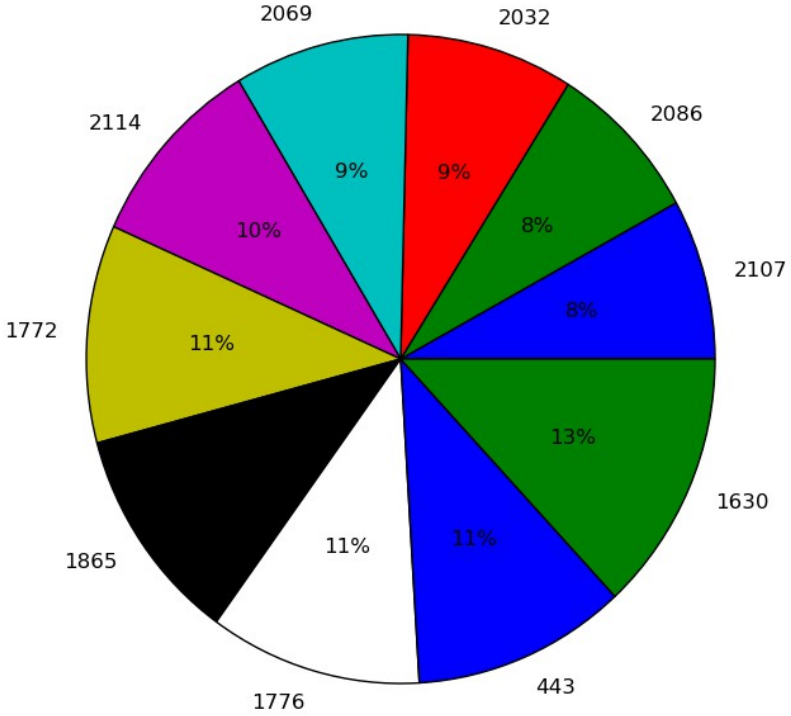
Most of the port usage was related to TCP and https, but there was a noticeably high octet count on the Federal Emergency System port, indicating a possible emergency alert being broadcast during the sample time.

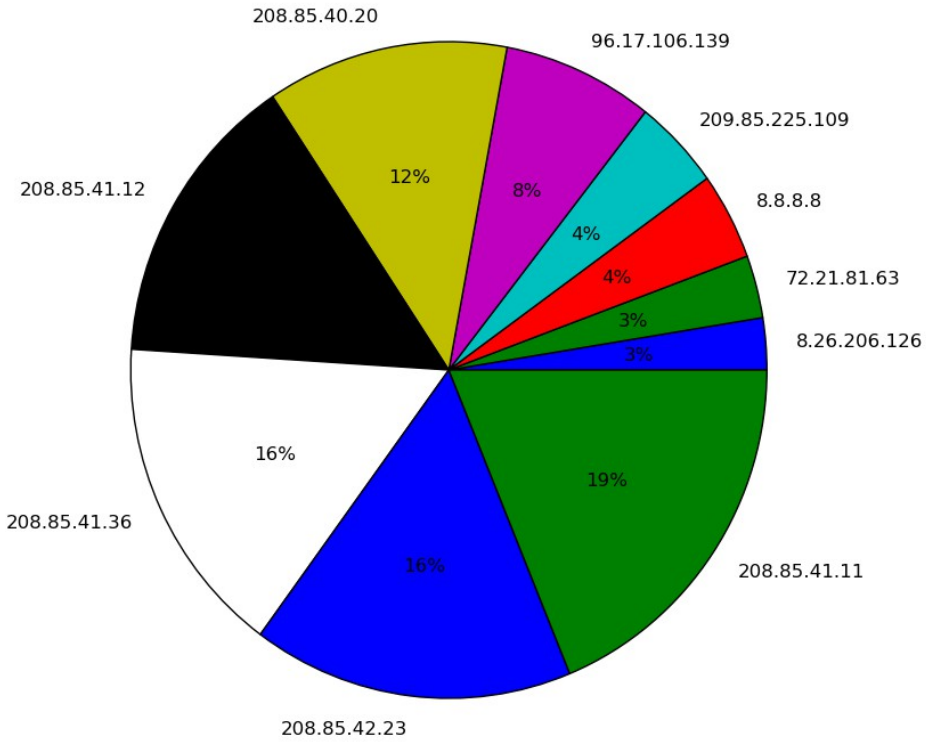
It is also interesting to note that the peak in network traffic occurred at exactly midnight, which may have something to do with network related CRON jobs, system updates, etc.

Below are four graphs that we drew these conclusions from. The first graph shows the top data consuming internal hosts. Figure 2 shows the peak network traffic times, and figure 3 shows the top consuming ports. Figure 4 shows the top 10 remote sites by total traffic.


192.168.1.7
192.168.1.4
7%
0%
80%
192.168.1.3


2011: 3:13:23:16:29
2011: 3:13:23:18:52
2011: 3:13:23:11:24
2011: 3:13:23:17:33
2011: 3:13:23:16:36
2011: 3:13:23: 0:1
2011: 3:13:23:22: 2
2011: 3:13:23: 0: 0
2011: 3:13:23: 2:32
2011: 3:13:23: 1:44
9%
9%
10%
7%
10%
5%
15%
12%
12%


2069
2032
2086
2107
1630
443
1776
1865
1772
2114
9%
9%
8%
8%
13%
11%
11%
11%
10%



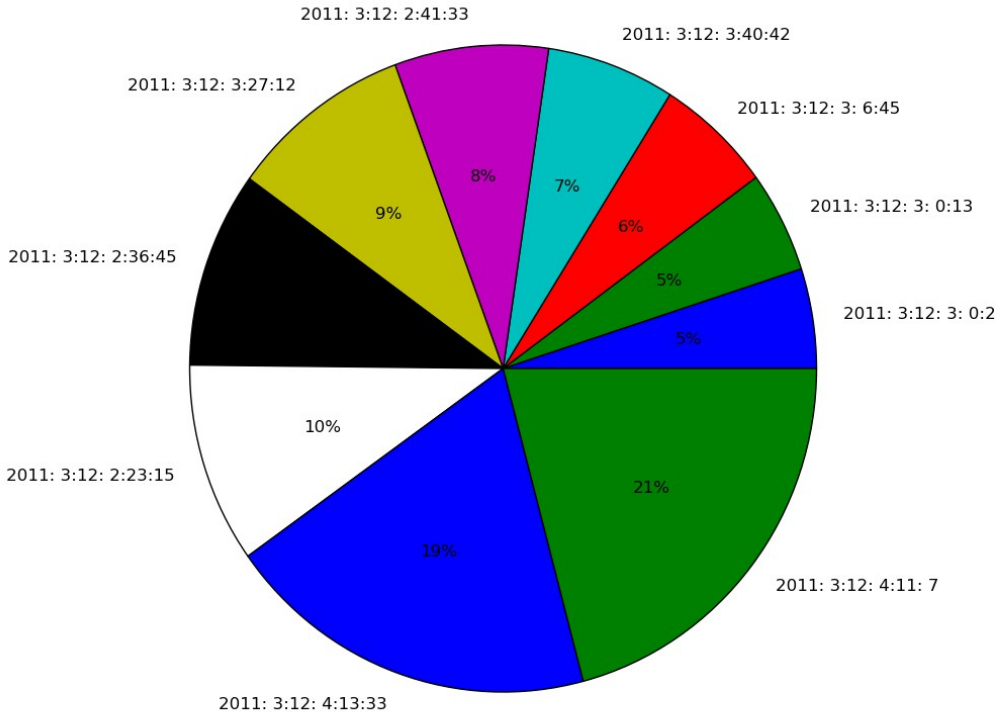
Analysis of NetFlow Capture 2:

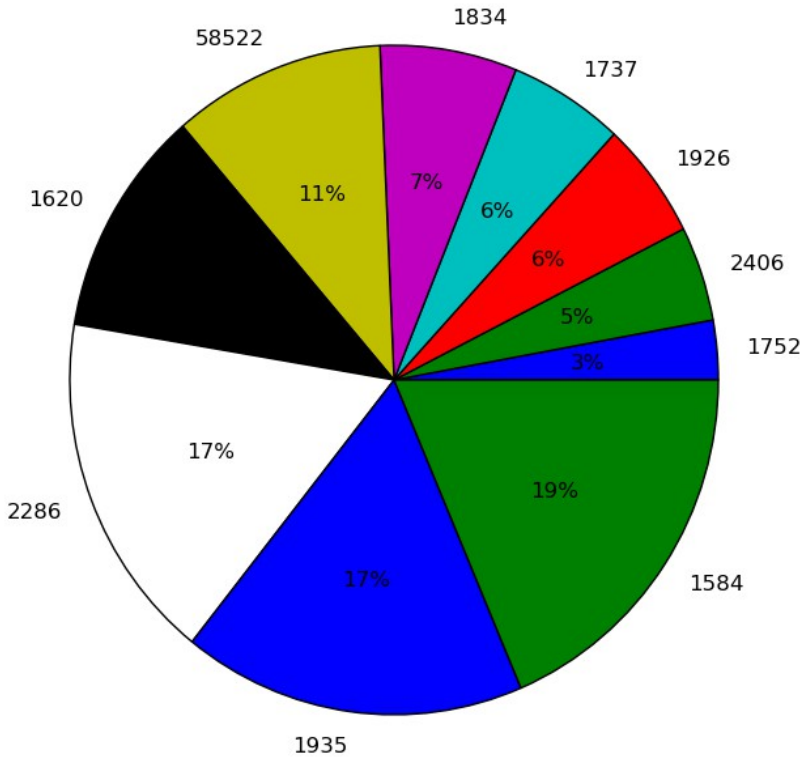
Upon initial review of the remote sites graph, we have determined that the network was utilized the most by a Content Distribution Network shared by Google and Level 3 Communications. 32% of the top 10 network traffic was a Google content hosting server, and Level 3 servers accounted for another 50%. Since the two together combined for over 80% of top 10 network traffic, it's fair to assume that the network event involved some sort of large media content distribution from Google, with Level 3 hosting remote sites for redundancy and performance. Additionally, upon reviewing the top 10 consuming ports, we found that nearly 20% of the traffic was accounted for on a port that is reserved for streaming flash media service.

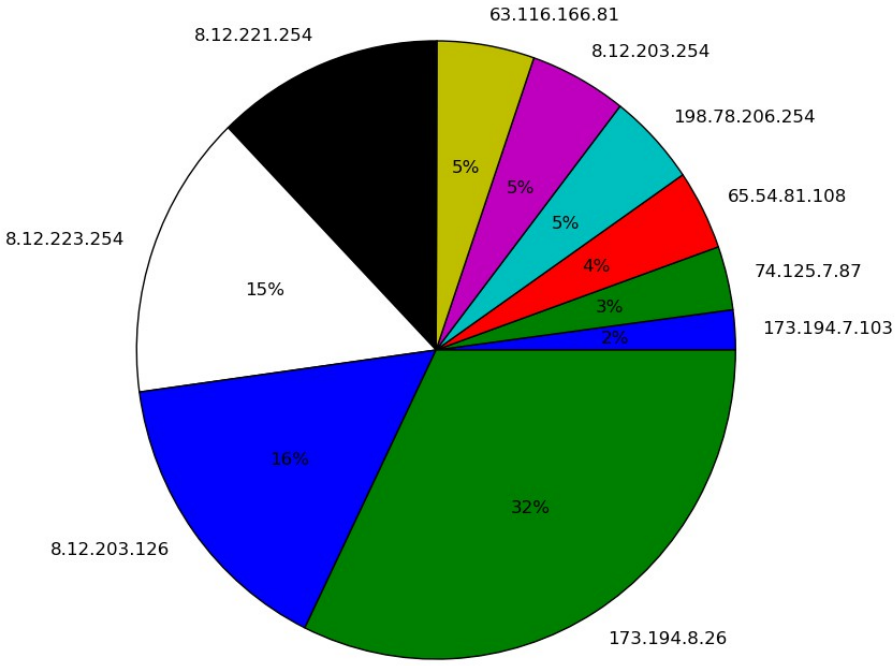
We have also found that the users on IP's 192.168.1.5 and 192.168.1.4 accounted for about 79% of the network usage among the top 8 internal hosts. There is a strong correlation between their network consumption and the sheer volume of the Google/Level 3 CDN.

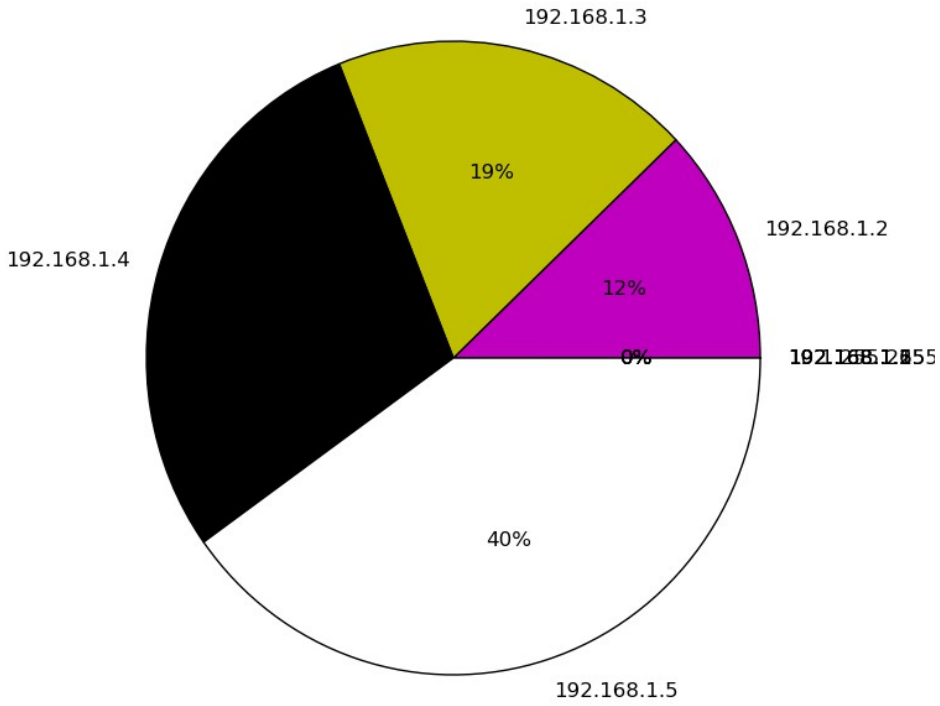
The top consuming ports were TCP/UDP ports, which makes sense given the nature of the network traffic. Around 11 in the morning is when network traffic peaked, so it's possible that the event/stream started at this time.

Below are the four graphs that we drew these conclusions from. Figure 1 shows the peak network traffic times. Figure 2 shows the the top 10 ports by data used, and figure 3 shows the top 10 remote sites by traffic. Figure 4 shows the highest consuming hosts.


2011: 3:12: 2:41:33
2011: 3:12: 3:40:42
2011: 3:12: 3:27:12
2011: 3:12: 3: 6:45
8%
7%
9%
6%
2011: 3:12: 3: 0:13
2011: 3:12: 2:36:45
5%
2011: 3:12: 3: 0:2
5%
10%
2011: 3:12: 2:23:15
21%
19%
2011: 3:12: 4:11: 7
2011: 3:12: 4:13:33


1834
58522
1737
1926
1620
11%
7%
6%
6%
2406
5%
1752
3%
17%
19%
2286
17%
1584
1935


63.116.166.81
8.12.221.254
8.12.203.254
198.78.206.254
65.54.81.108
8.12.223.254
74.125.7.87
173.194.7.103
8.12.203.126
173.194.8.26
5%
5%
5%
4%
3%
2%
15%
16%
32%


192.168.1.3
19%
192.168.1.2
192.168.1.4
12%
0%
40%
192.168.1.5