Webtop

HTTP Traffic Aggregator and Analysis Tool

10/26/12

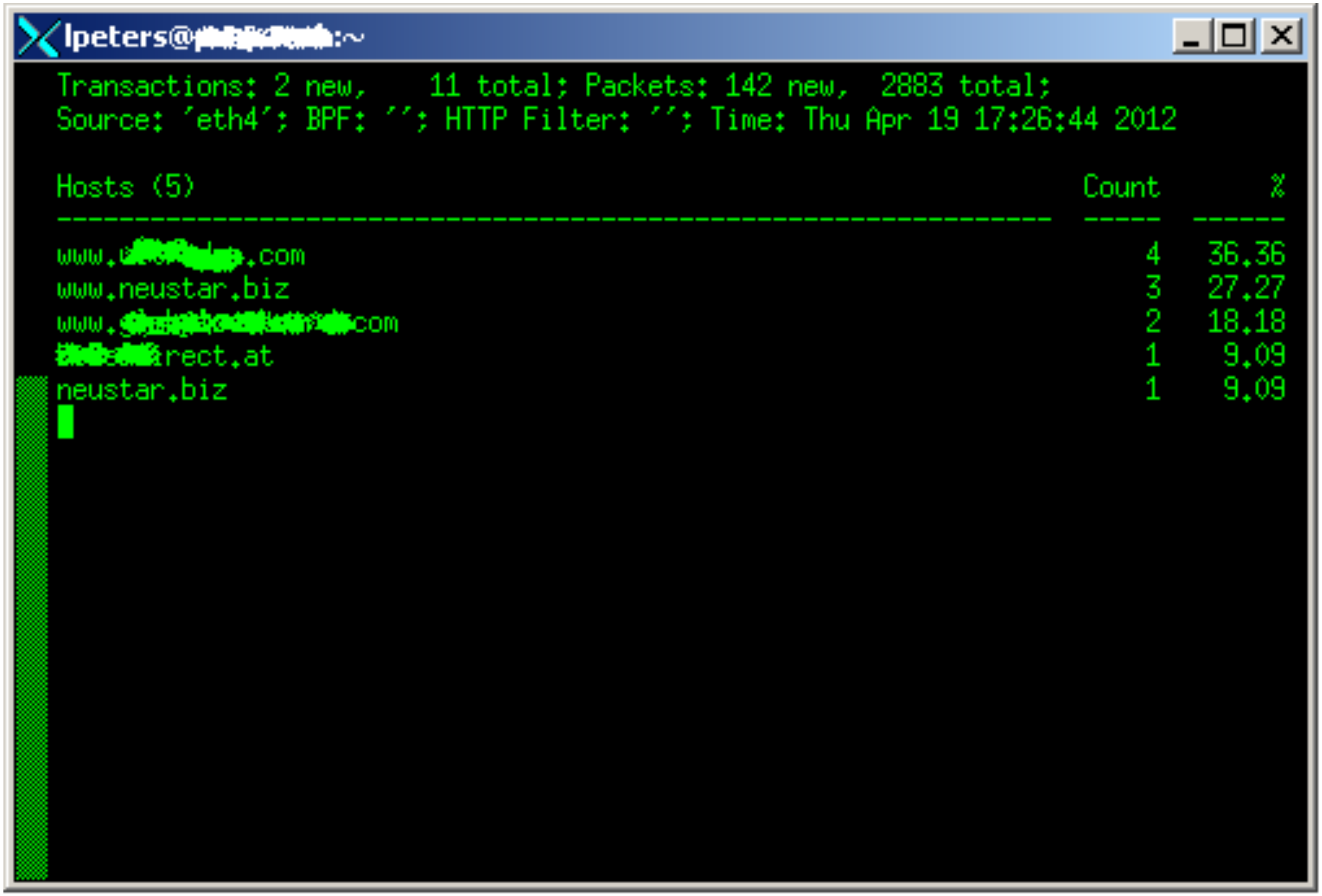
Les Peters

Senior Network & InfoSec Engineer / Neustar

The Problem

- Neustar launched an HTTP DDoS mitigation service, called SiteProtect, built on our experience of mitigation DNS attacks
- Dnstop used to analyze DNS traffic, but needed a similar tool for HTTP traffic, aggregating:
  - » GET/POST content
  - » Source/Destination IP address
  - » Various HTTP headers (Host, User-Agent, Accept-Language, Referer)
- Needed an easier solution than tcpdump fed to awk/grep/sed/etc…
- Webtop fulfills this need

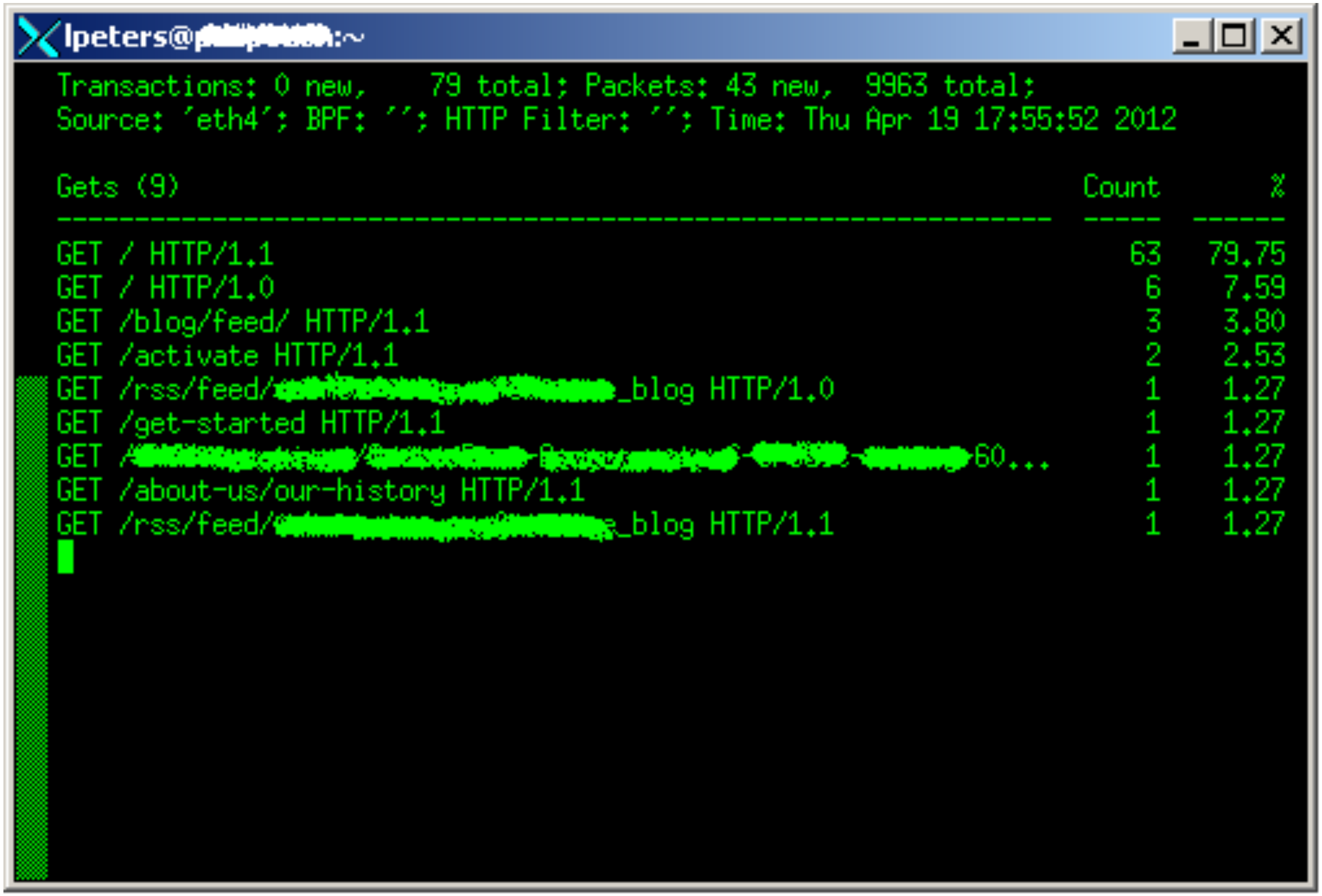
Webtop – Host



```
Transactions: 2 new,    11 total; Packets: 142 new,  2883 total;
Source: 'eth4'; BPF: ''; HTTP Filter: ''; Time: Thu Apr 19 17:26:44 2012

Hosts (5)                                                         Count       %
----------------------------------------------------------------  -----  ------
www.[redacted].com                                                    4   36.36
www.neustar.biz                                                       3   27.27
www.[redacted]com                                                     2   18.18
[redacted]rect.at                                                     1    9.09
neustar.biz                                                           1    9.09
```

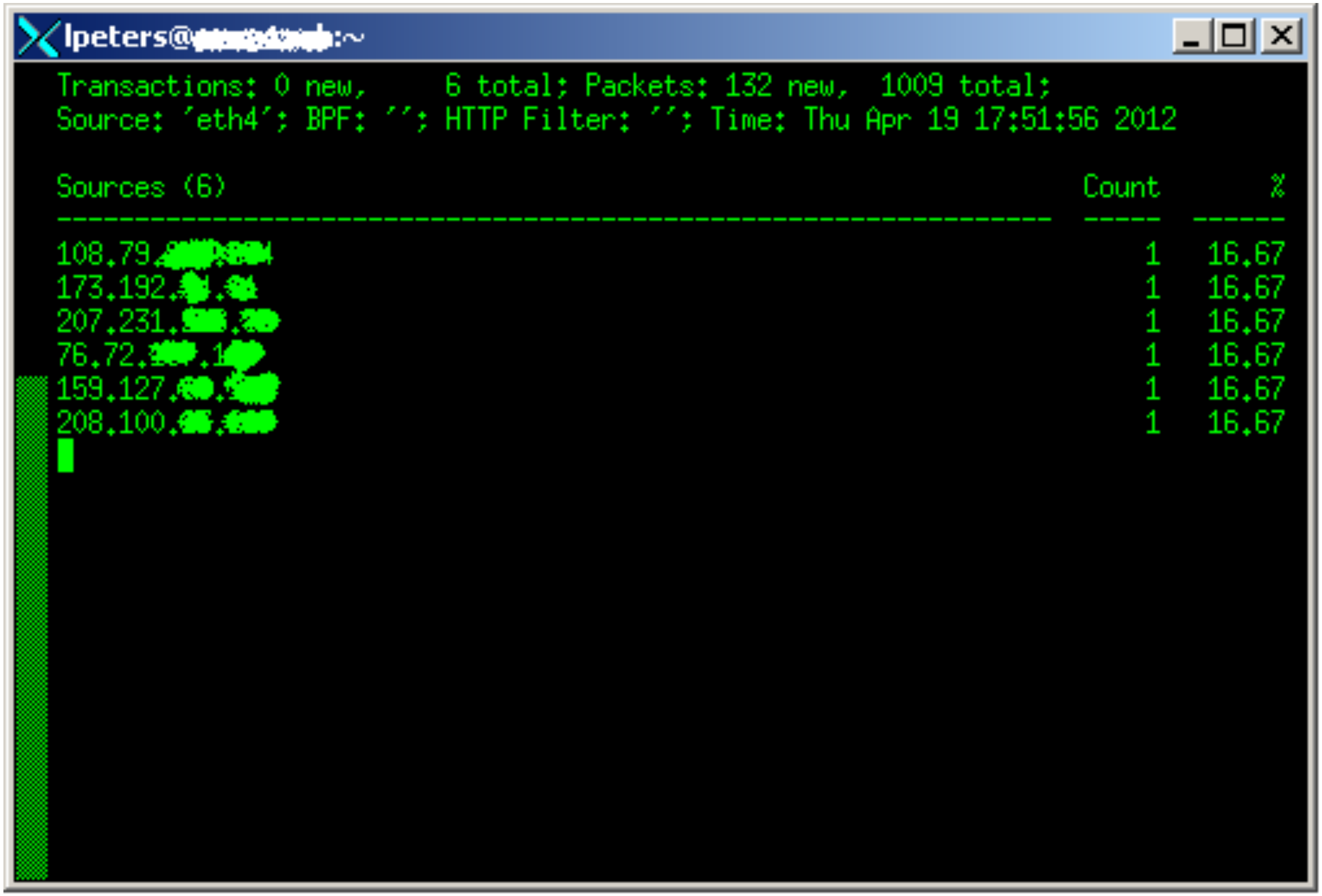
Webtop – GET/POST



```
Transactions: 0 new,    79 total; Packets: 43 new,  9963 total;
Source: 'eth4'; BPF: ''; HTTP Filter: ''; Time: Thu Apr 19 17:55:52 2012

Gets (9)                                                          Count       %
----------------------------------------------------------------  -----  ------
GET / HTTP/1.1                                                       63   79.75
GET / HTTP/1.0                                                        6    7.59
GET /blog/feed/ HTTP/1.1                                              3    3.80
GET /activate HTTP/1.1                                                2    2.53
GET /rss/feed/[redacted]_blog HTTP/1.0                                1    1.27
GET /get-started HTTP/1.1                                             1    1.27
GET /[redacted]60...                                                  1    1.27
GET /about-us/our-history HTTP/1.1                                    1    1.27
GET /rss/feed/[redacted]_blog HTTP/1.1                                1    1.27
```

Webtop – Source IP

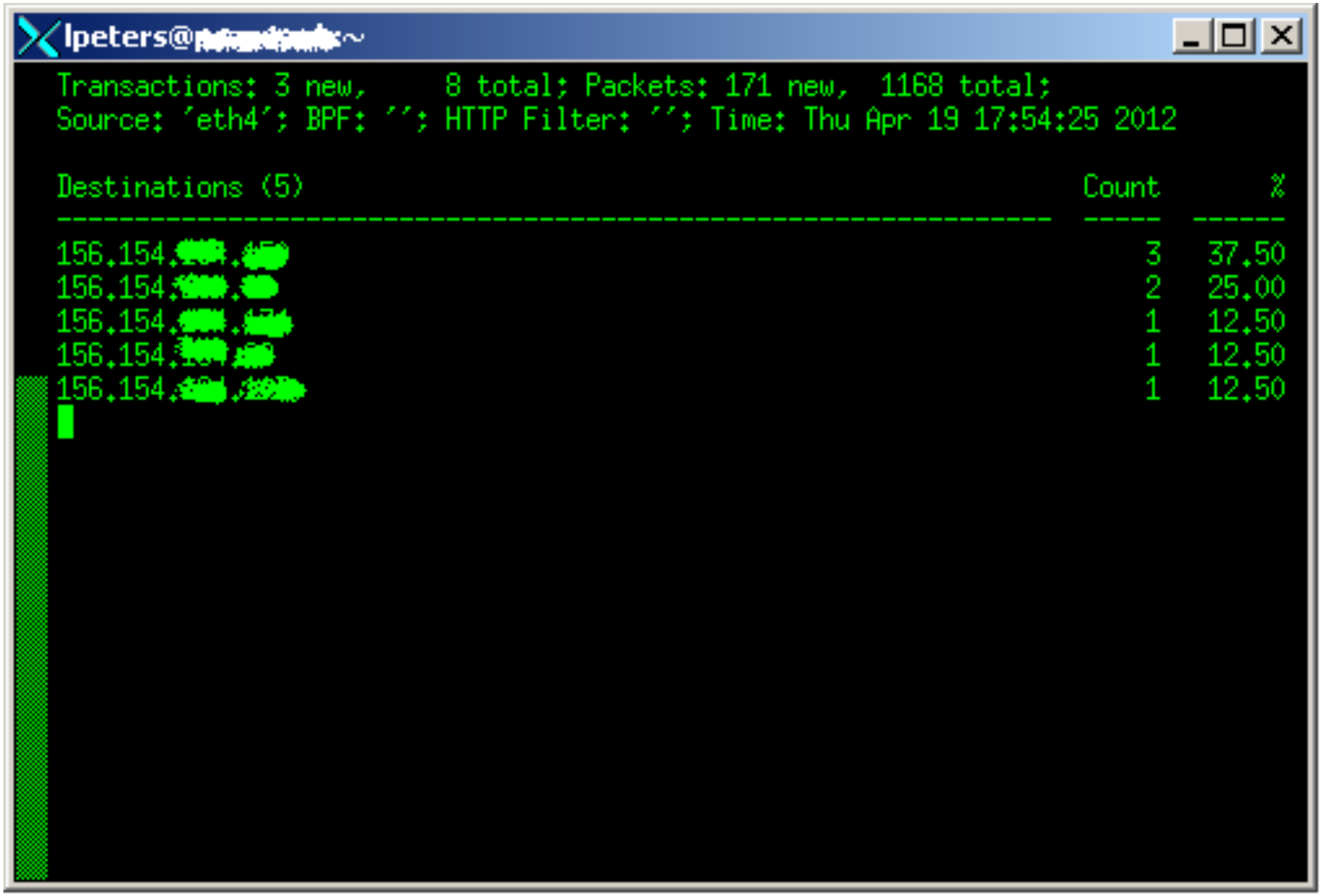


```
lpeters@[redacted]:~

Transactions: 0 new,     6 total; Packets: 132 new,  1009 total;
Source: 'eth4'; BPF: ''; HTTP Filter: ''; Time: Thu Apr 19 17:51:56 2012

Sources (6)                                                     Count      %
----------------------------------------------------------------  -----  ------
108.79.[redacted]                                                     1   16.67
173.192.[redacted].[redacted]                                         1   16.67
207.231.[redacted].[redacted]                                         1   16.67
76.72.[redacted].1[redacted]                                          1   16.67
159.127.[redacted].[redacted]                                         1   16.67
208.100.[redacted].[redacted]                                         1   16.67
```

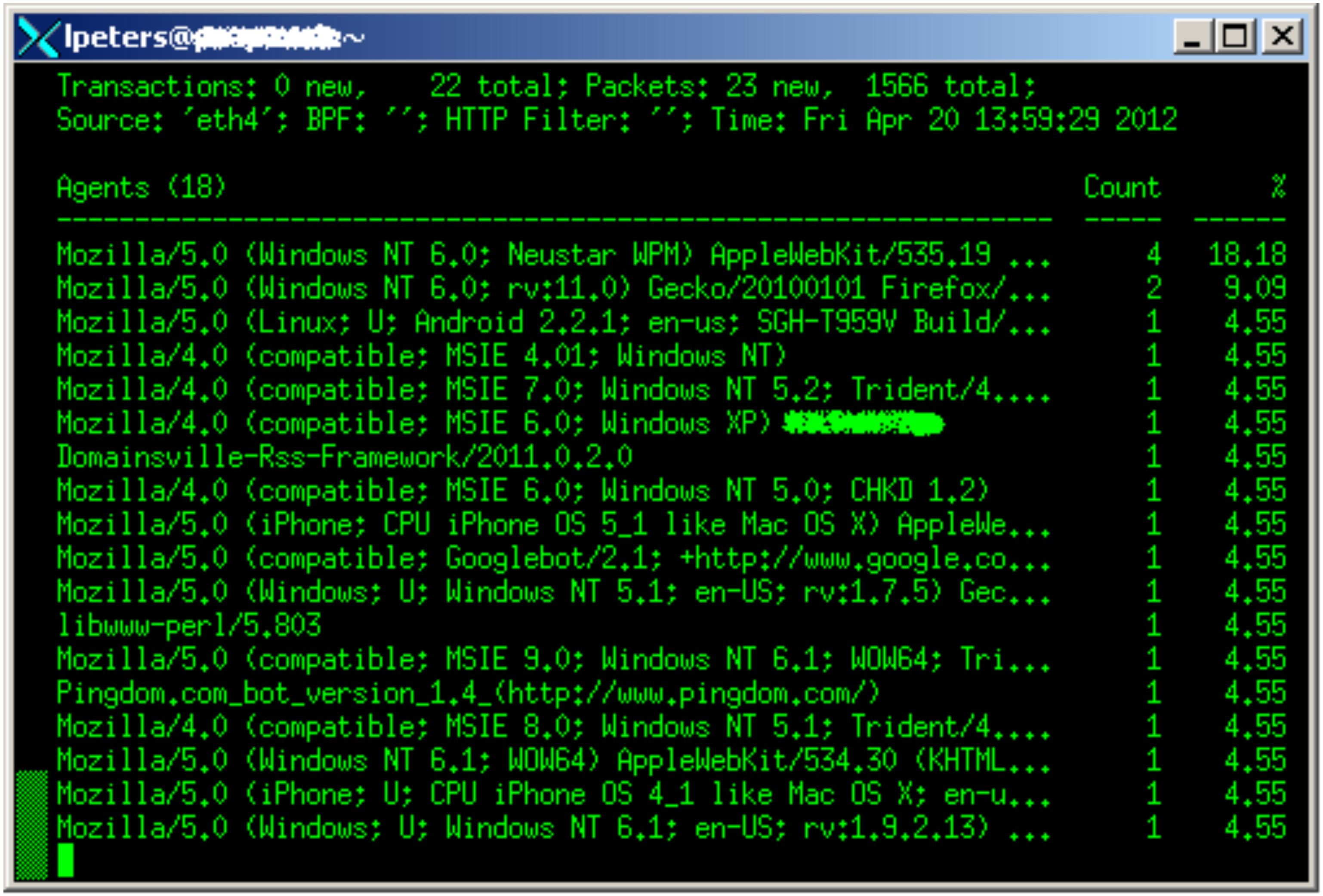
Webtop – Destination IP



```
Transactions: 3 new,     8 total; Packets: 171 new,  1168 total;
Source: 'eth4'; BPF: ''; HTTP Filter: ''; Time: Thu Apr 19 17:54:25 2012

Destinations (5)                                                  Count      %
----------------------------------------------------------------  -----  -------
156.154.[redacted].[redacted]                                         3    37.50
156.154.[redacted].[redacted]                                         2    25.00
156.154.[redacted].[redacted]                                         1    12.50
156.154.[redacted].[redacted]                                         1    12.50
156.154.[redacted].[redacted]                                         1    12.50
```

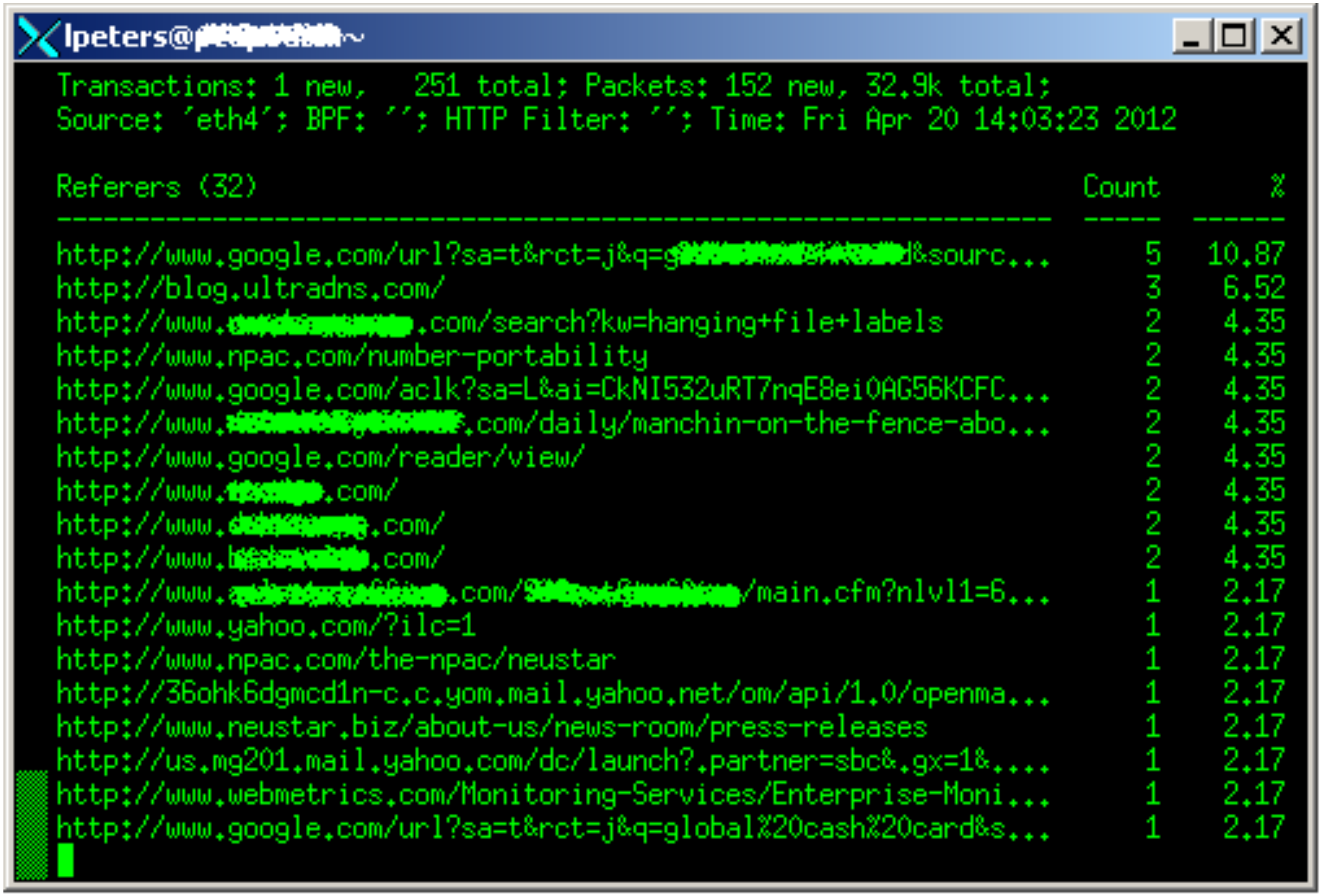
Webtop – User-Agent



```
Transactions: 0 new,    22 total; Packets: 23 new,  1566 total;
Source: 'eth4'; BPF: ''; HTTP Filter: ''; Time: Fri Apr 20 13:59:29 2012

Agents (18)                                                          Count       %
----------------------------------------------------------------    -----   ------
Mozilla/5.0 (Windows NT 6.0; Neustar WPM) AppleWebKit/535.19 ...        4    18.18
Mozilla/5.0 (Windows NT 6.0; rv:11.0) Gecko/20100101 Firefox/...        2     9.09
Mozilla/5.0 (Linux; U; Android 2.2.1; en-us; SGH-T959V Build/...        1     4.55
Mozilla/4.0 (compatible; MSIE 4.01; Windows NT)                         1     4.55
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.2; Trident/4....        1     4.55
Mozilla/4.0 (compatible; MSIE 6.0; Windows XP) [redacted]               1     4.55
Domainsville-Rss-Framework/2011.0.2.0                                   1     4.55
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; CHKD 1.2)            1     4.55
Mozilla/5.0 (iPhone; CPU iPhone OS 5_1 like Mac OS X) AppleWe...        1     4.55
Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.co...        1     4.55
Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.7.5) Gec...        1     4.55
libwww-perl/5.803                                                       1     4.55
Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Tri...        1     4.55
Pingdom.com_bot_version_1.4_(http://www.pingdom.com/)                   1     4.55
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4....        1     4.55
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/534.30 (KHTML...        1     4.55
Mozilla/5.0 (iPhone; U; CPU iPhone OS 4_1 like Mac OS X; en-u...        1     4.55
Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2.13) ...        1     4.55
```

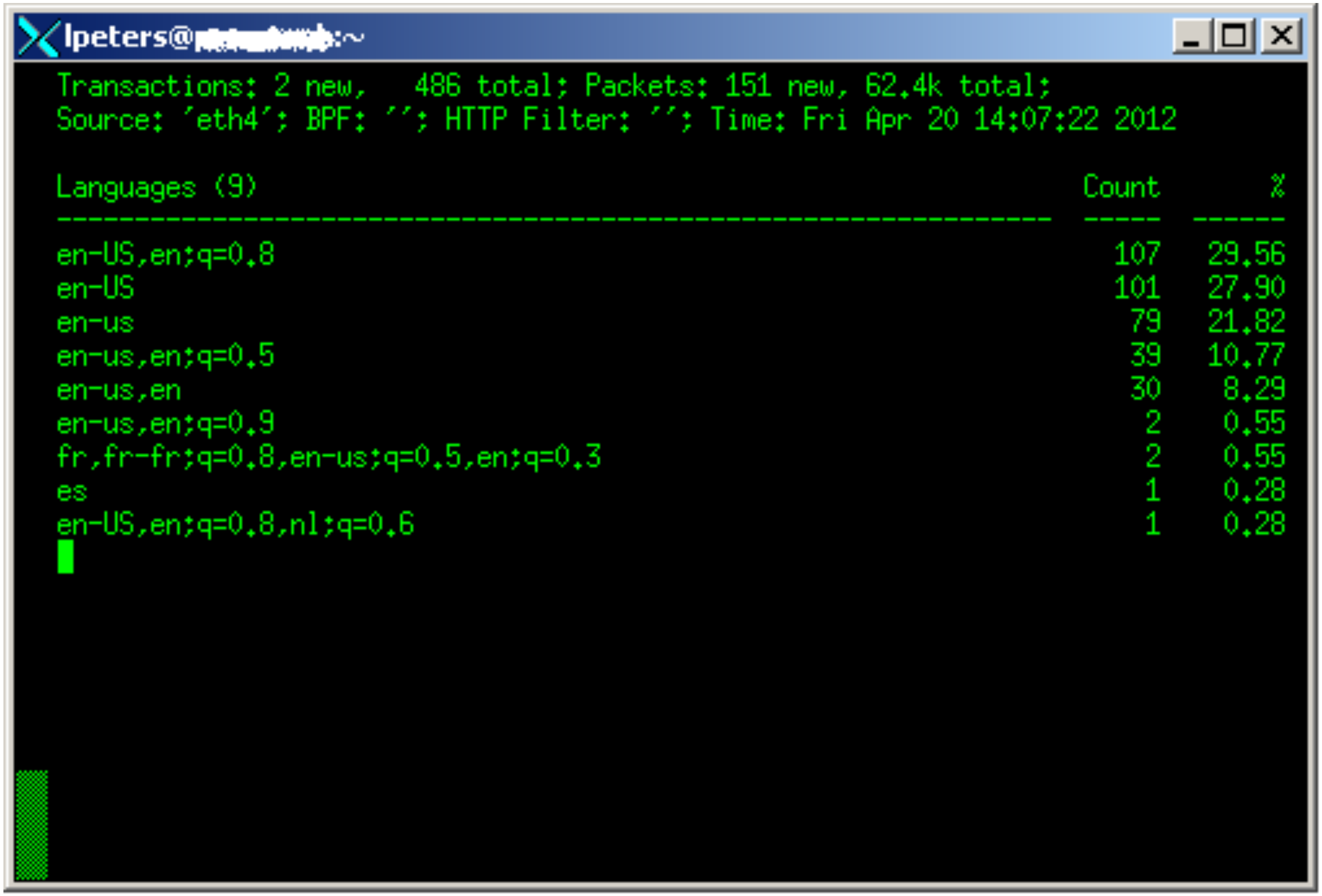
Webtop - Referer



```
Transactions: 1 new,   251 total; Packets: 152 new, 32.9k total;
Source: 'eth4'; BPF: ''; HTTP Filter: ''; Time: Fri Apr 20 14:03:23 2012

Referers (32)                                                     Count       %
----------------------------------------------------------------  -----  ------
http://www.google.com/url?sa=t&rct=j&q=[redacted]d&sourc...           5   10.87
http://blog.ultradns.com/                                             3    6.52
http://www.[redacted].com/search?kw=hanging+file+labels               2    4.35
http://www.npac.com/number-portability                                2    4.35
http://www.google.com/aclk?sa=L&ai=CkNI532uRT7nqE8ei0AG56KCFC...      2    4.35
http://www.[redacted].com/daily/manchin-on-the-fence-abo...           2    4.35
http://www.google.com/reader/view/                                    2    4.35
http://www.[redacted].com/                                            2    4.35
http://www.[redacted].com/                                            2    4.35
http://www.[redacted].com/                                            2    4.35
http://www.[redacted].com/[redacted]/main.cfm?nlvl1=6...              1    2.17
http://www.yahoo.com/?ilc=1                                           1    2.17
http://www.npac.com/the-npac/neustar                                  1    2.17
http://36ohk6dgmcd1n-c.c.yom.mail.yahoo.net/om/api/1.0/openma...      1    2.17
http://www.neustar.biz/about-us/news-room/press-releases              1    2.17
http://us.mg201.mail.yahoo.com/dc/launch?.partner=sbc&.gx=1&....      1    2.17
http://www.webmetrics.com/Monitoring-Services/Enterprise-Moni...      1    2.17
http://www.google.com/url?sa=t&rct=j&q=global%20cash%20card&s...      1    2.17
```

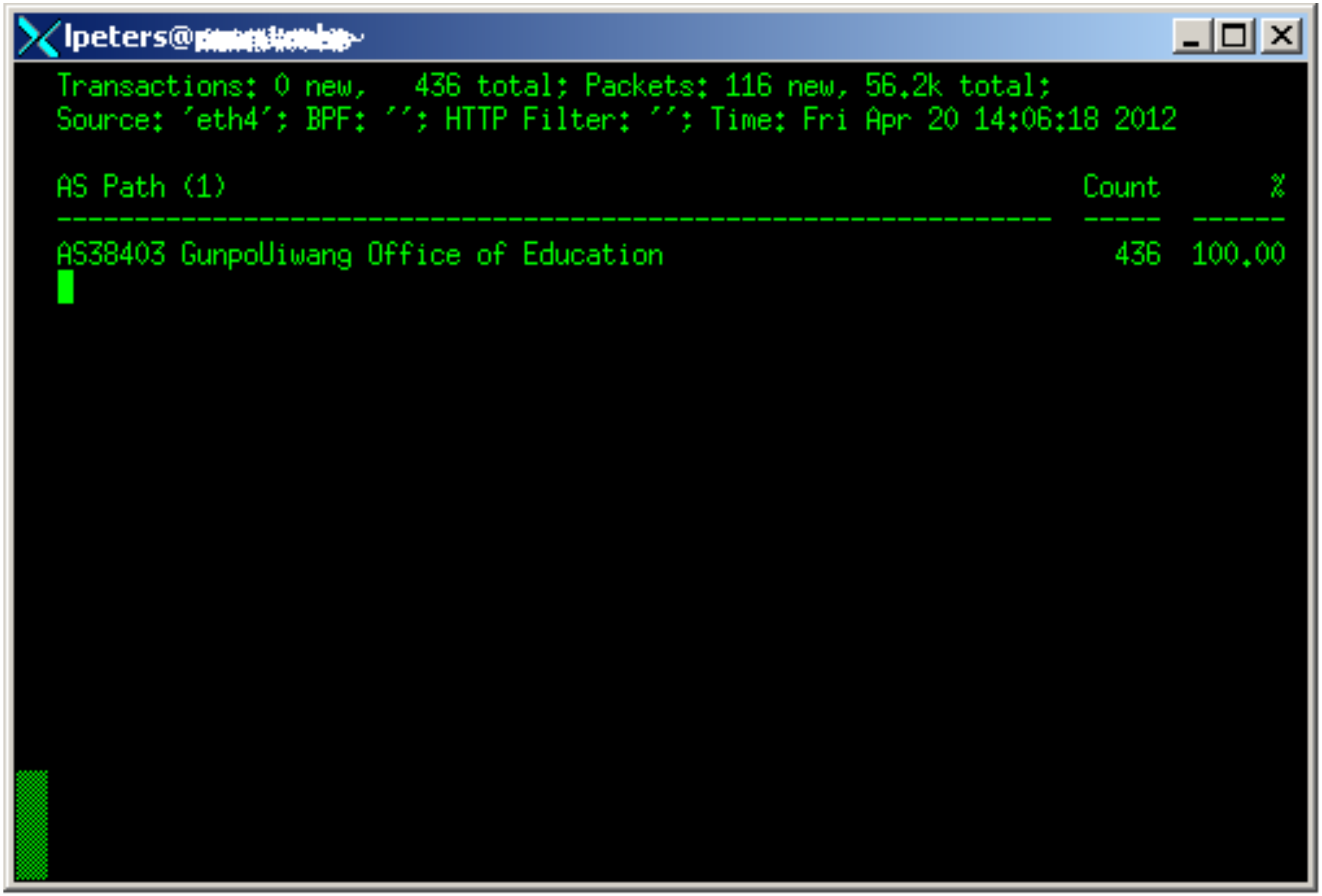
Webtop – Accept-Language



```
Transactions: 2 new,   486 total; Packets: 151 new, 62.4k total;
Source: 'eth4'; BPF: ''; HTTP Filter: ''; Time: Fri Apr 20 14:07:22 2012

Languages (9)                                                   Count       %
--------------------------------------------------------------- -----  ------
en-US,en;q=0.8                                                    107   29.56
en-US                                                             101   27.90
en-us                                                              79   21.82
en-us,en;q=0.5                                                     39   10.77
en-us,en                                                           30    8.29
en-us,en;q=0.9                                                      2    0.55
fr,fr-fr;q=0.8,en-us;q=0.5,en;q=0.3                                 2    0.55
es                                                                  1    0.28
en-US,en;q=0.8,nl;q=0.6                                             1    0.28
```

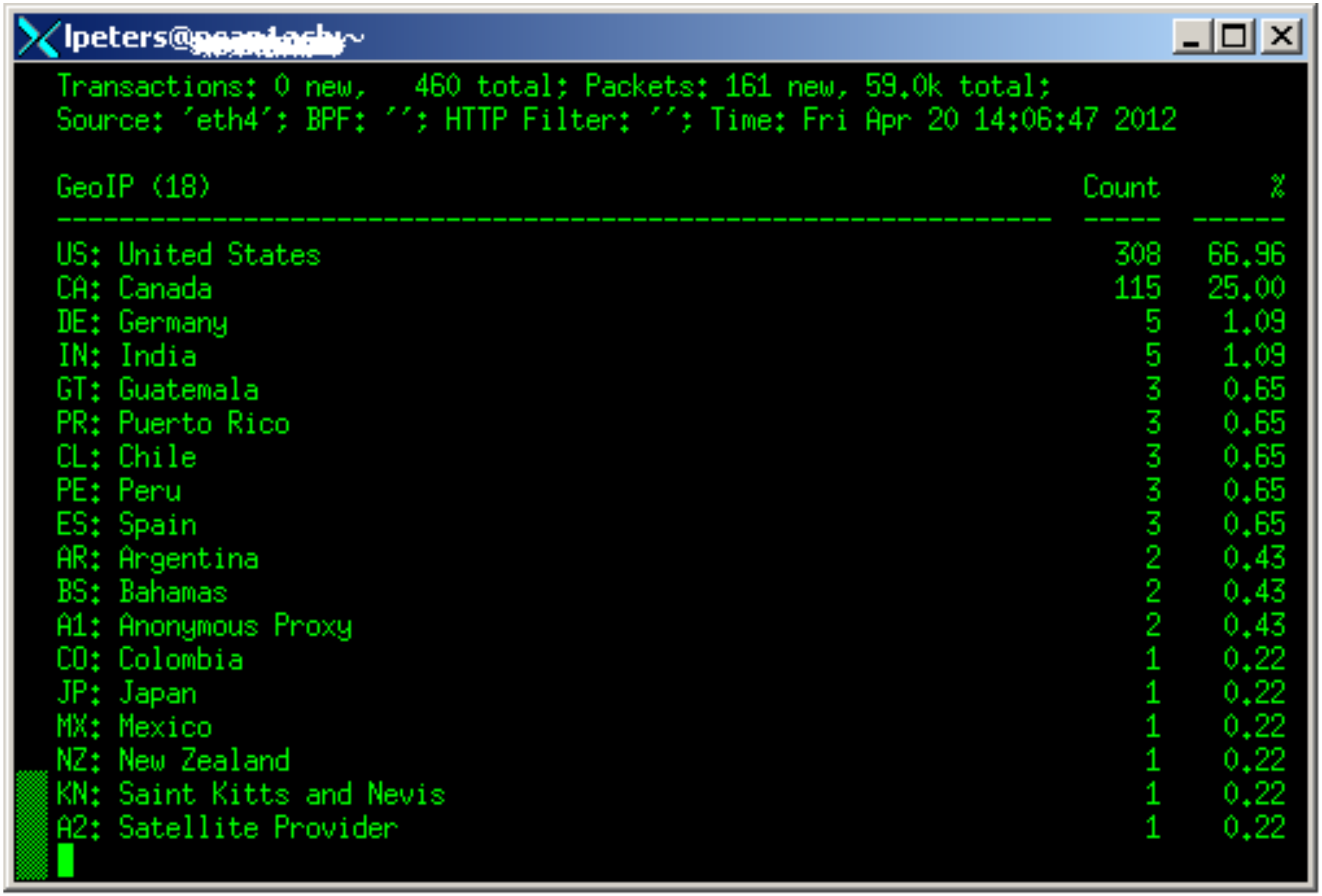
Webtop – AS Path



```
Transactions: 0 new,   436 total; Packets: 116 new, 56.2k total;
Source: 'eth4'; BPF: ''; HTTP Filter: ''; Time: Fri Apr 20 14:06:18 2012

AS Path (1)                                                        Count       %
------------------------------------------------------------------ -----  ------
AS38403 GunpoUiwang Office of Education                              436  100.00
```

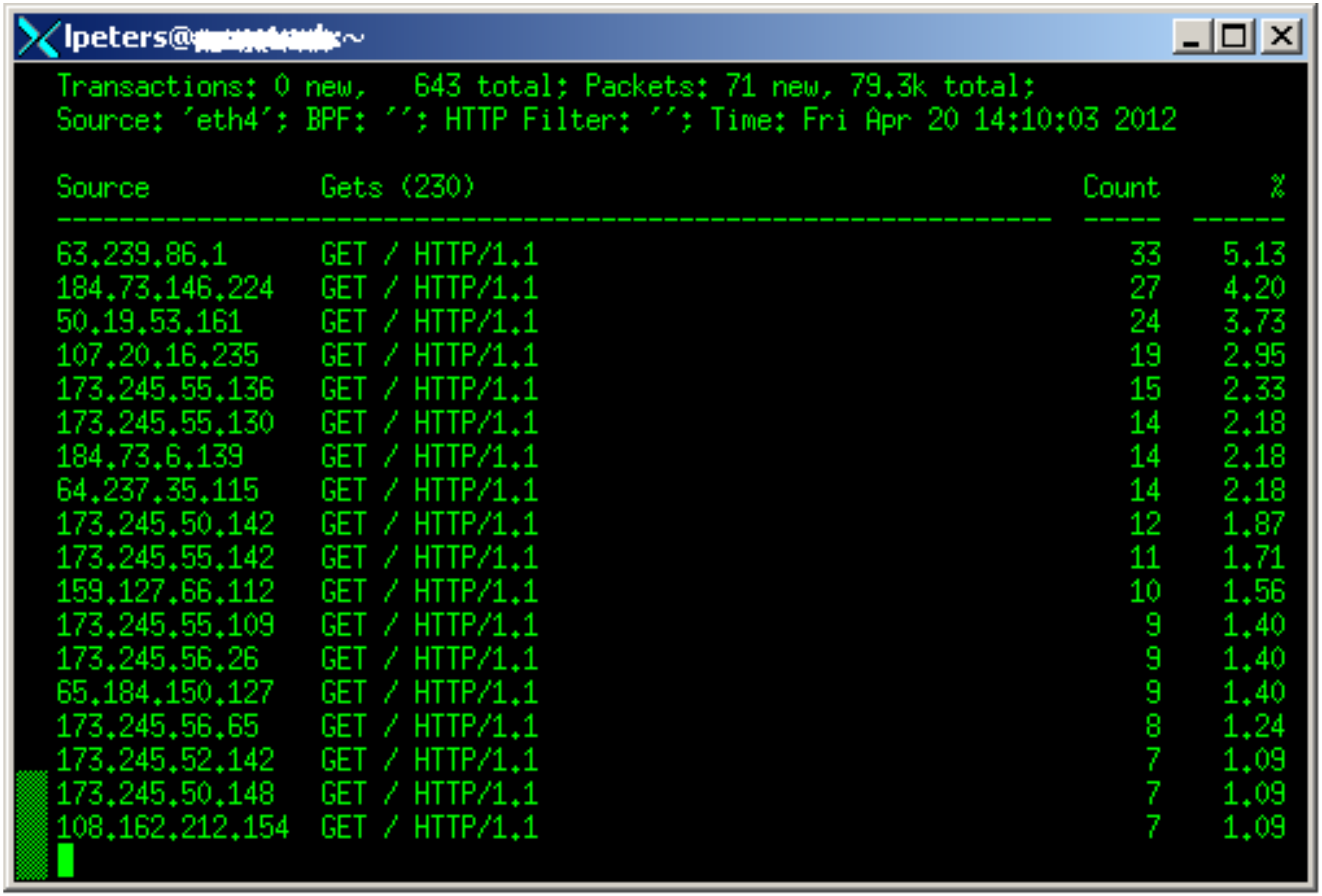
Webtop - GeoIP



```
Transactions: 0 new,   460 total; Packets: 161 new, 59.0k total;
Source: 'eth4'; BPF: ''; HTTP Filter: ''; Time: Fri Apr 20 14:06:47 2012

GeoIP (18)                                                         Count       %
----------------------------------------------------------------   -----  ------
US: United States                                                    308   66.96
CA: Canada                                                           115   25.00
DE: Germany                                                            5    1.09
IN: India                                                              5    1.09
GT: Guatemala                                                          3    0.65
PR: Puerto Rico                                                        3    0.65
CL: Chile                                                              3    0.65
PE: Peru                                                               3    0.65
ES: Spain                                                              3    0.65
AR: Argentina                                                          2    0.43
BS: Bahamas                                                            2    0.43
A1: Anonymous Proxy                                                    2    0.43
CO: Colombia                                                           1    0.22
JP: Japan                                                              1    0.22
MX: Mexico                                                             1    0.22
NZ: New Zealand                                                        1    0.22
KN: Saint Kitts and Nevis                                              1    0.22
A2: Satellite Provider                                                 1    0.22
```

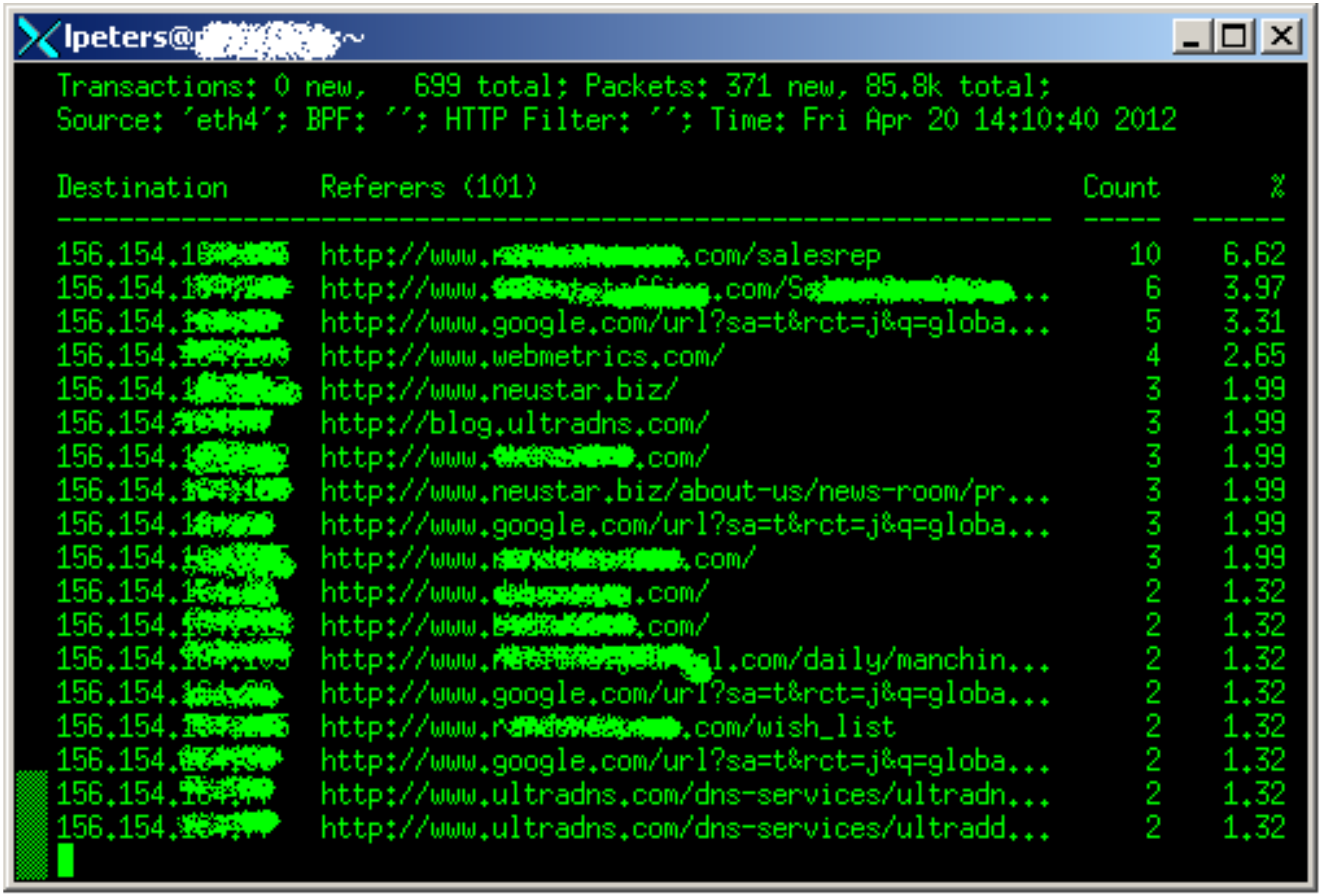
Webtop – GET/POST by Source IP



```
Transactions: 0 new,   643 total; Packets: 71 new, 79.3k total;
Source: 'eth4'; BPF: ''; HTTP Filter: ''; Time: Fri Apr 20 14:10:03 2012

Source           Gets (230)                                              Count      %
----------------------------------------------------------------------  -----  ------
63.239.86.1      GET / HTTP/1.1                                             33   5.13
184.73.146.224   GET / HTTP/1.1                                             27   4.20
50.19.53.161     GET / HTTP/1.1                                             24   3.73
107.20.16.235    GET / HTTP/1.1                                             19   2.95
173.245.55.136   GET / HTTP/1.1                                             15   2.33
173.245.55.130   GET / HTTP/1.1                                             14   2.18
184.73.6.139     GET / HTTP/1.1                                             14   2.18
64.237.35.115    GET / HTTP/1.1                                             14   2.18
173.245.50.142   GET / HTTP/1.1                                             12   1.87
173.245.55.142   GET / HTTP/1.1                                             11   1.71
159.127.66.112   GET / HTTP/1.1                                             10   1.56
173.245.55.109   GET / HTTP/1.1                                              9   1.40
173.245.56.26    GET / HTTP/1.1                                              9   1.40
65.184.150.127   GET / HTTP/1.1                                              9   1.40
173.245.56.65    GET / HTTP/1.1                                              8   1.24
173.245.52.142   GET / HTTP/1.1                                              7   1.09
173.245.50.148   GET / HTTP/1.1                                              7   1.09
108.162.212.154  GET / HTTP/1.1                                              7   1.09
```

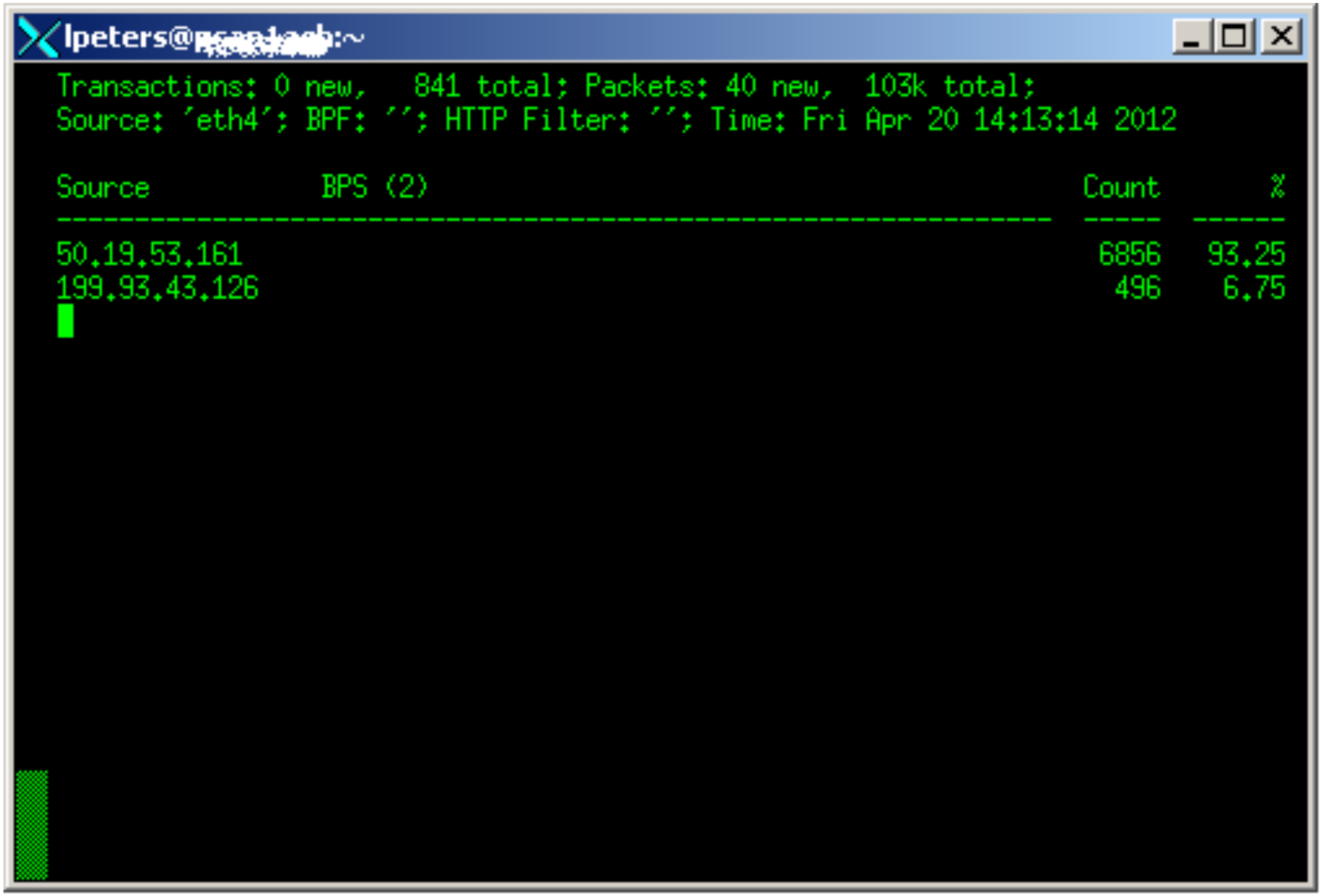
Webtop – Referer by Destination IP



```
Transactions: 0 new,   699 total; Packets: 371 new, 85.8k total;
Source: 'eth4'; BPF: ''; HTTP Filter: ''; Time: Fri Apr 20 14:10:40 2012

Destination       Referers (101)                                      Count       %
----------------------------------------------------------------      -----   ------
156.154.[redacted]   http://www.[redacted].com/salesrep                      10    6.62
156.154.[redacted]   http://www.[redacted].com/S[redacted]..                  6    3.97
156.154.[redacted]   http://www.google.com/url?sa=t&rct=j&q=globa...          5    3.31
156.154.[redacted]   http://www.webmetrics.com/                               4    2.65
156.154.[redacted]   http://www.neustar.biz/                                  3    1.99
156.154.[redacted]   http://blog.ultradns.com/                                3    1.99
156.154.[redacted]   http://www.[redacted].com/                               3    1.99
156.154.[redacted]   http://www.neustar.biz/about-us/news-room/pr...          3    1.99
156.154.[redacted]   http://www.google.com/url?sa=t&rct=j&q=globa...          3    1.99
156.154.[redacted]   http://www.[redacted].com/                               3    1.99
156.154.[redacted]   http://www.[redacted].com/                               2    1.32
156.154.[redacted]   http://www.[redacted].com/                               2    1.32
156.154.[redacted]   http://www.[redacted]l.com/daily/manchin...              2    1.32
156.154.[redacted]   http://www.google.com/url?sa=t&rct=j&q=globa...          2    1.32
156.154.[redacted]   http://www.[redacted].com/wish_list                      2    1.32
156.154.[redacted]   http://www.google.com/url?sa=t&rct=j&q=globa...          2    1.32
156.154.[redacted]   http://www.ultradns.com/dns-services/ultradn...          2    1.32
156.154.[redacted]   http://www.ultradns.com/dns-services/ultradd...          2    1.32
```

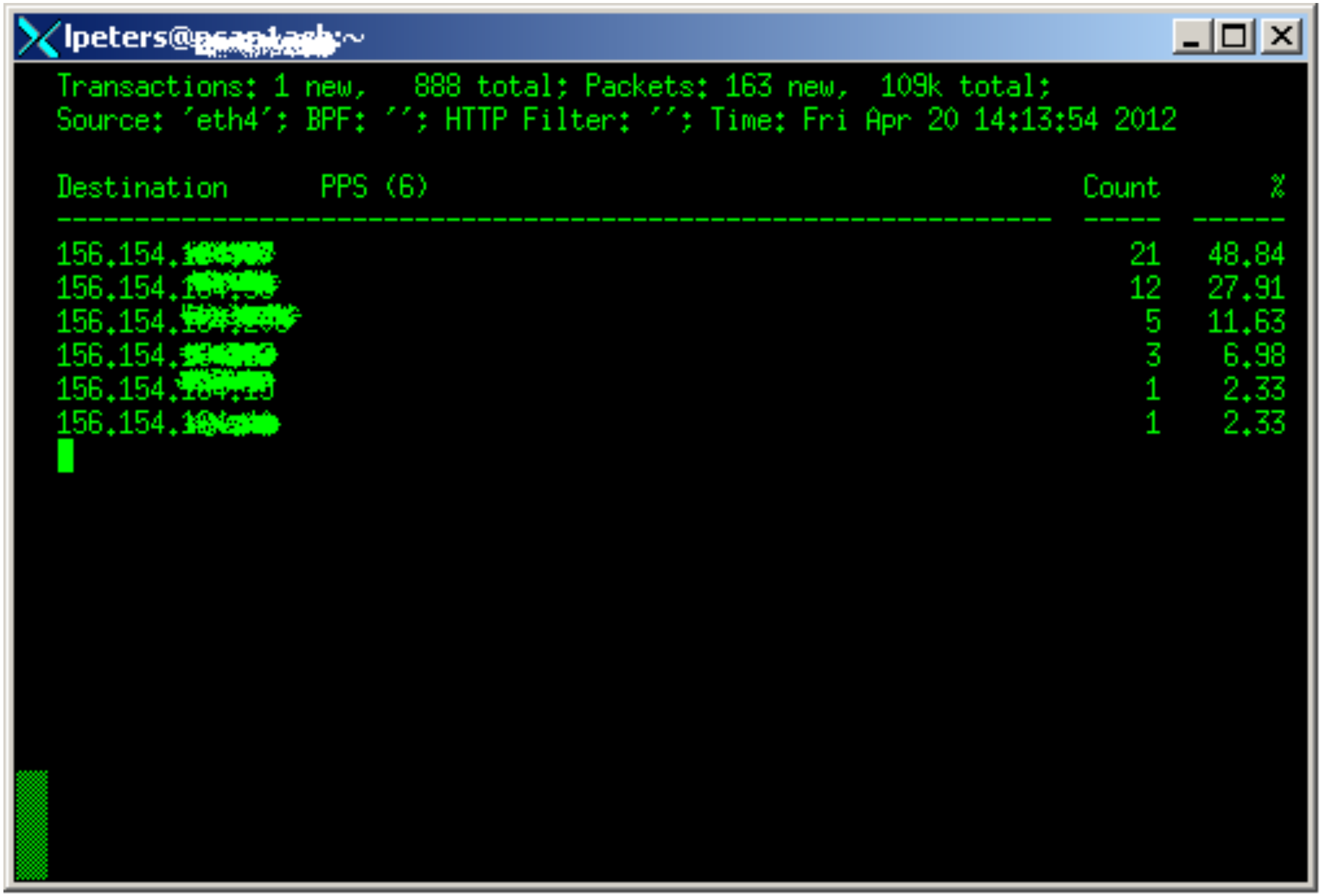
Webtop - BPS



```
Transactions: 0 new,   841 total; Packets: 40 new,  103k total;
Source: 'eth4'; BPF: ''; HTTP Filter: ''; Time: Fri Apr 20 14:13:14 2012

Source           BPS (2)                                            Count       %
---------------------------------------------------------------- ------  -------
50.19.53.161                                                         6856   93.25
199.93.43.126                                                         496    6.75
```

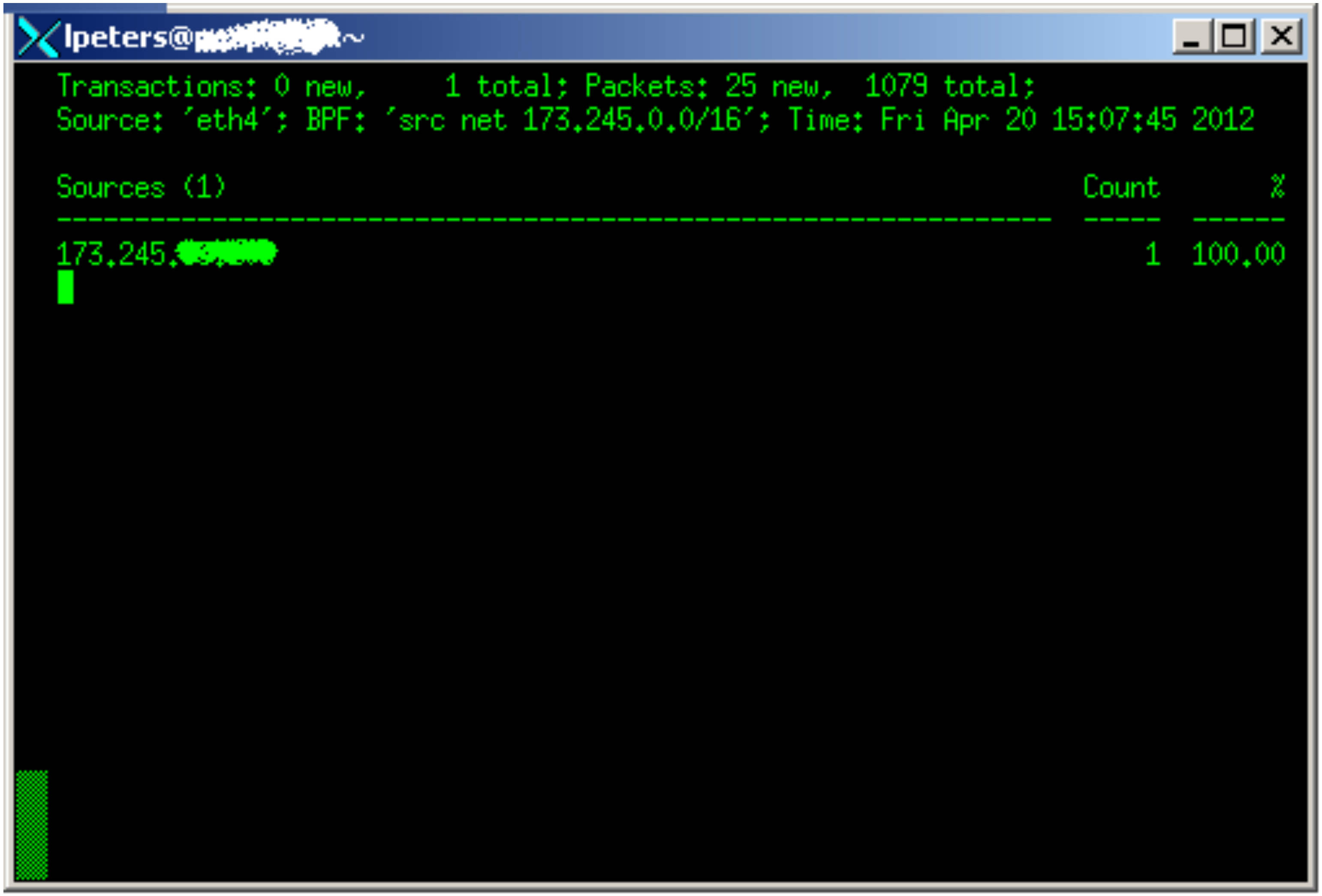
Webtop - PPS



```
Transactions: 1 new,   888 total; Packets: 163 new,  109k total;
Source: 'eth4'; BPF: ''; HTTP Filter: ''; Time: Fri Apr 20 14:13:54 2012

Destination      PPS (6)                                    Count       %
------------------------------------------------------------ -----  ------
156.154.[redacted]                                              21   48.84
156.154.[redacted]                                              12   27.91
156.154.[redacted]                                               5   11.63
156.154.[redacted]                                               3    6.98
156.154.[redacted]                                               1    2.33
156.154.[redacted]                                               1    2.33
```

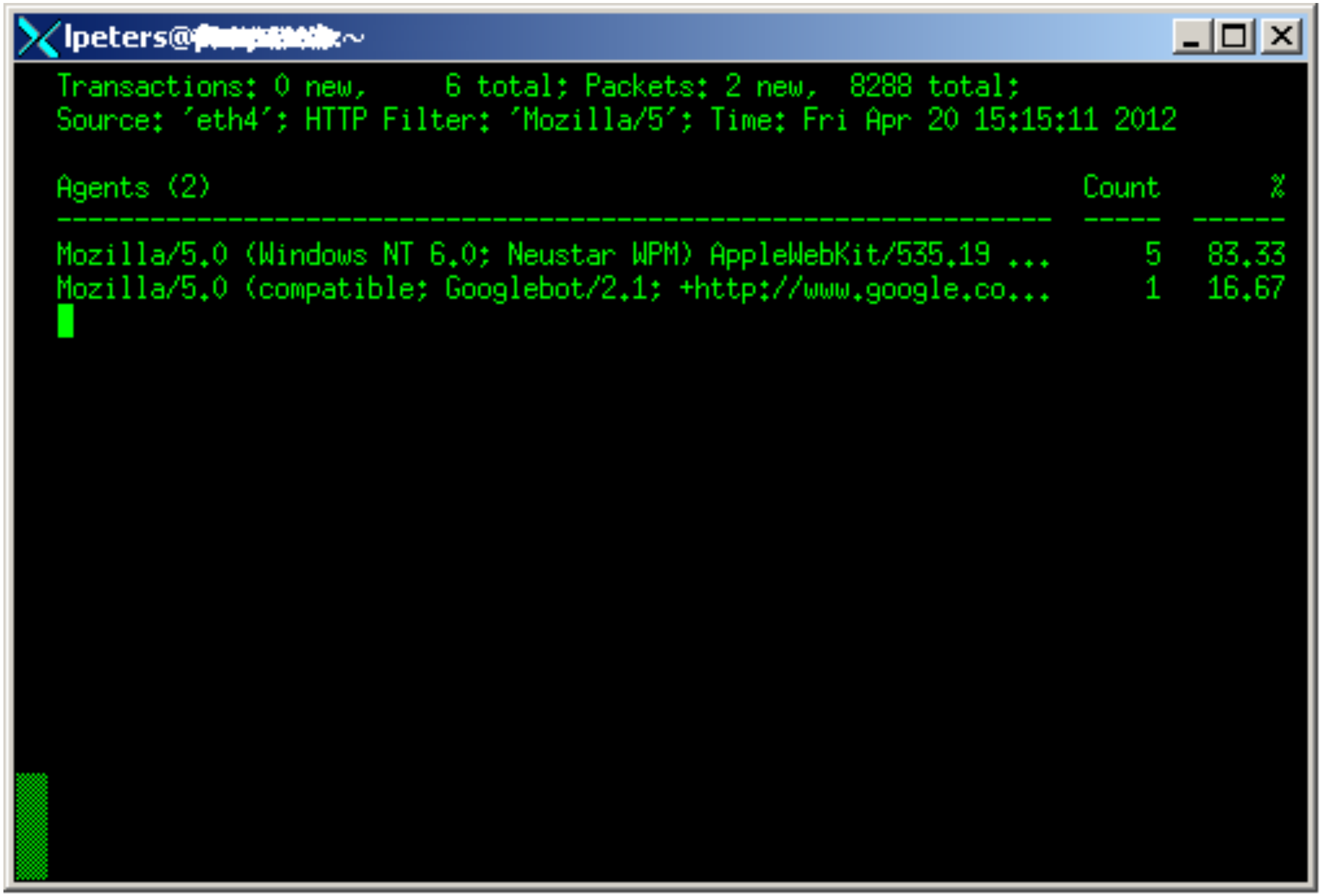
Webtop – Berkeley Packet Filter



```
Transactions: 0 new,     1 total; Packets: 25 new,  1079 total;
Source: 'eth4'; BPF: 'src net 173.245.0.0/16'; Time: Fri Apr 20 15:07:45 2012

Sources (1)                                                       Count       %
----------------------------------------------------------------  -----  ------
173.245.[redacted]                                                    1  100.00
```

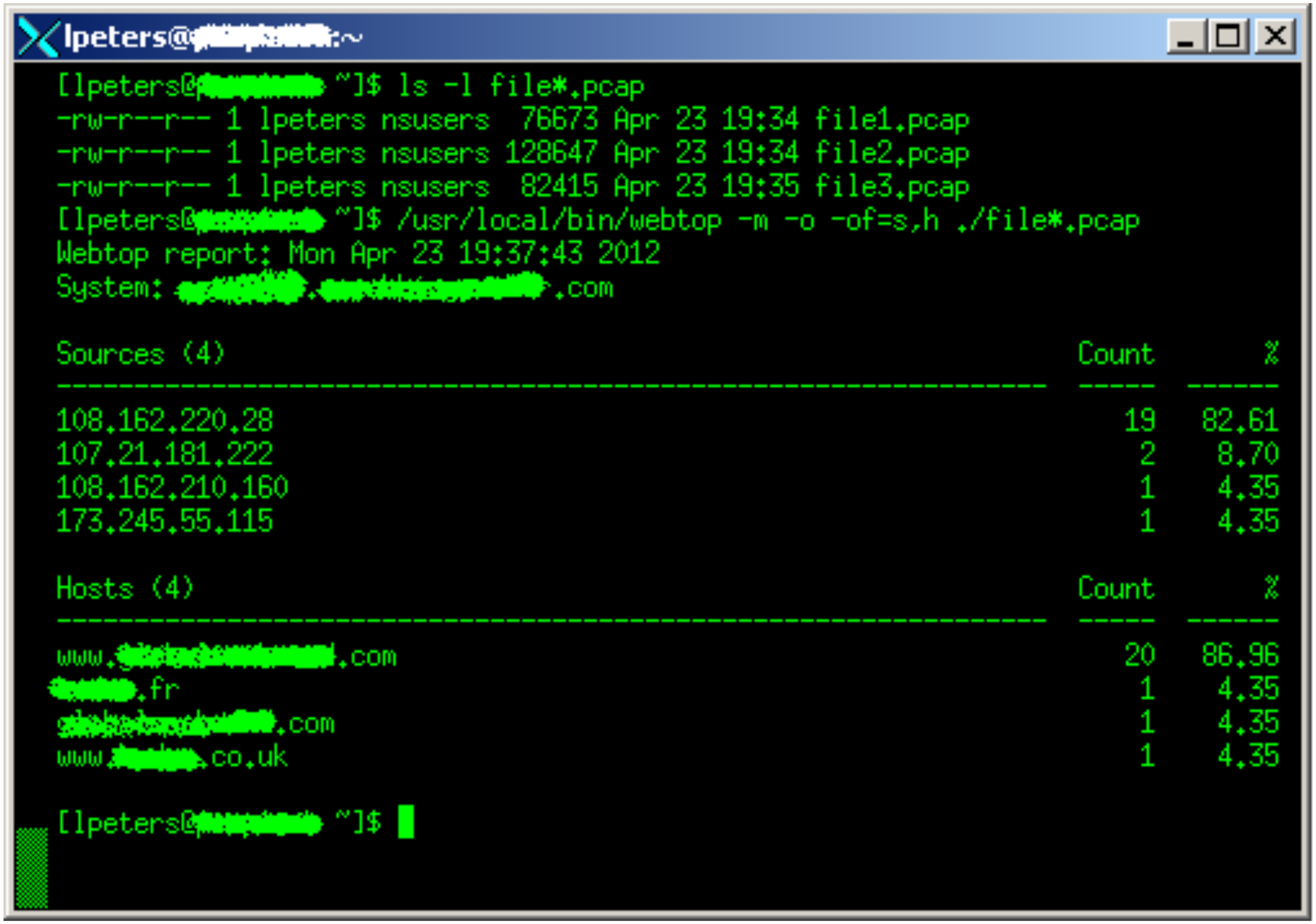
Webtop – HTTP Filter



```
Transactions: 0 new,     6 total; Packets: 2 new,  8288 total;
Source: 'eth4'; HTTP Filter: 'Mozilla/5'; Time: Fri Apr 20 15:15:11 2012

Agents (2)                                                        Count       %
----------------------------------------------------------------  -----  ------
Mozilla/5.0 (Windows NT 6.0; Neustar WPM) AppleWebKit/535.19 ...      5   83.33
Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.co...      1   16.67
```

Webtop – Multiple files



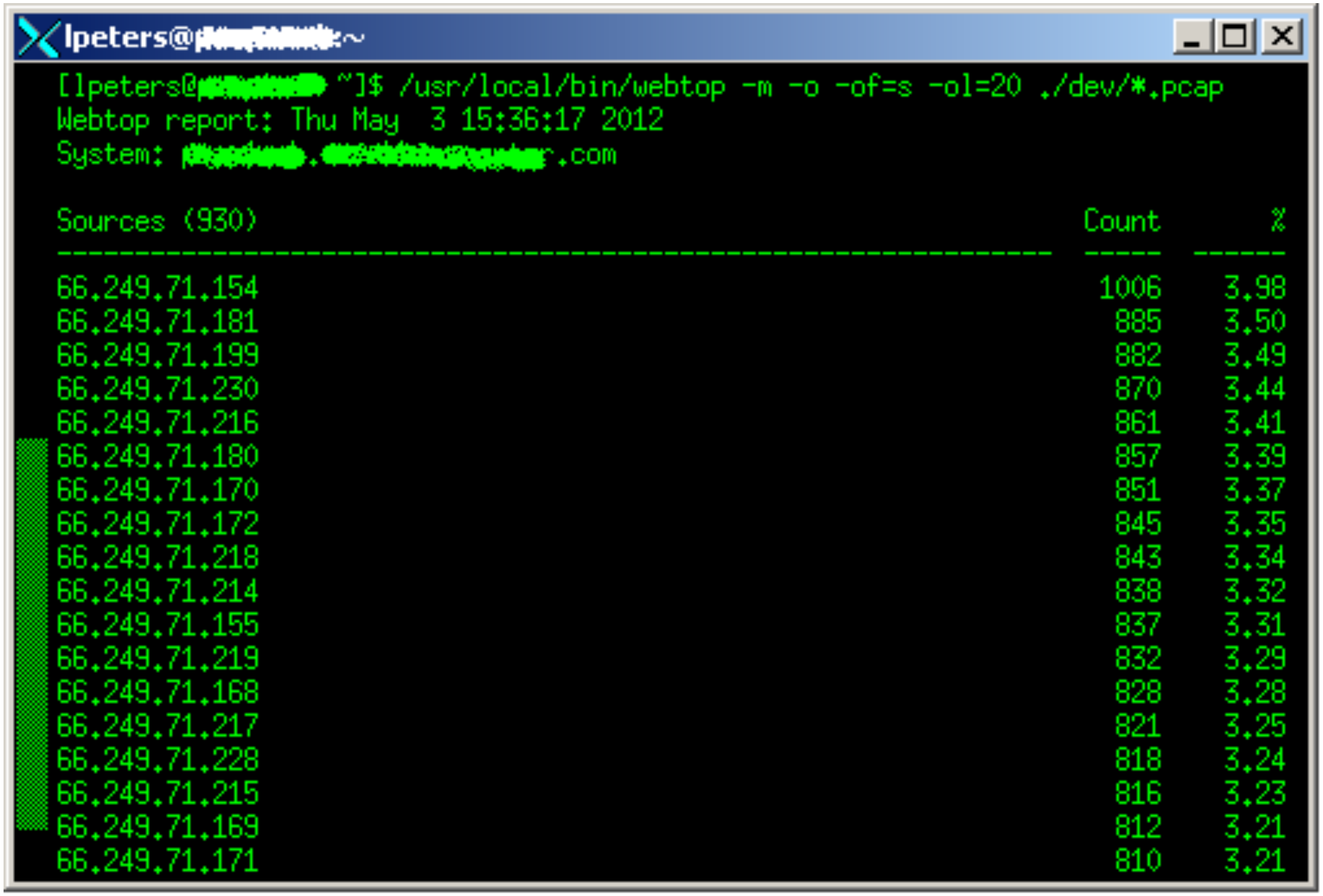
```
[lpeters@[redacted] ~]$ ls -l file*.pcap
-rw-r--r-- 1 lpeters nsusers  76673 Apr 23 19:34 file1.pcap
-rw-r--r-- 1 lpeters nsusers 128647 Apr 23 19:34 file2.pcap
-rw-r--r-- 1 lpeters nsusers  82415 Apr 23 19:35 file3.pcap
[lpeters@[redacted] ~]$ /usr/local/bin/webtop -m -o -of=s,h ./file*.pcap
Webtop report: Mon Apr 23 19:37:43 2012
System: [redacted].[redacted].com

Sources (4)                                                       Count      %
----------------------------------------------------------------  -----  ------
108.162.220.28                                                       19   82.61
107.21.181.222                                                        2    8.70
108.162.210.160                                                       1    4.35
173.245.55.115                                                        1    4.35

Hosts (4)                                                         Count      %
----------------------------------------------------------------  -----  ------
www.[redacted].com                                                   20   86.96
[redacted].fr                                                         1    4.35
[redacted].com                                                        1    4.35
www.[redacted].co.uk                                                  1    4.35

[lpeters@[redacted] ~]$
```

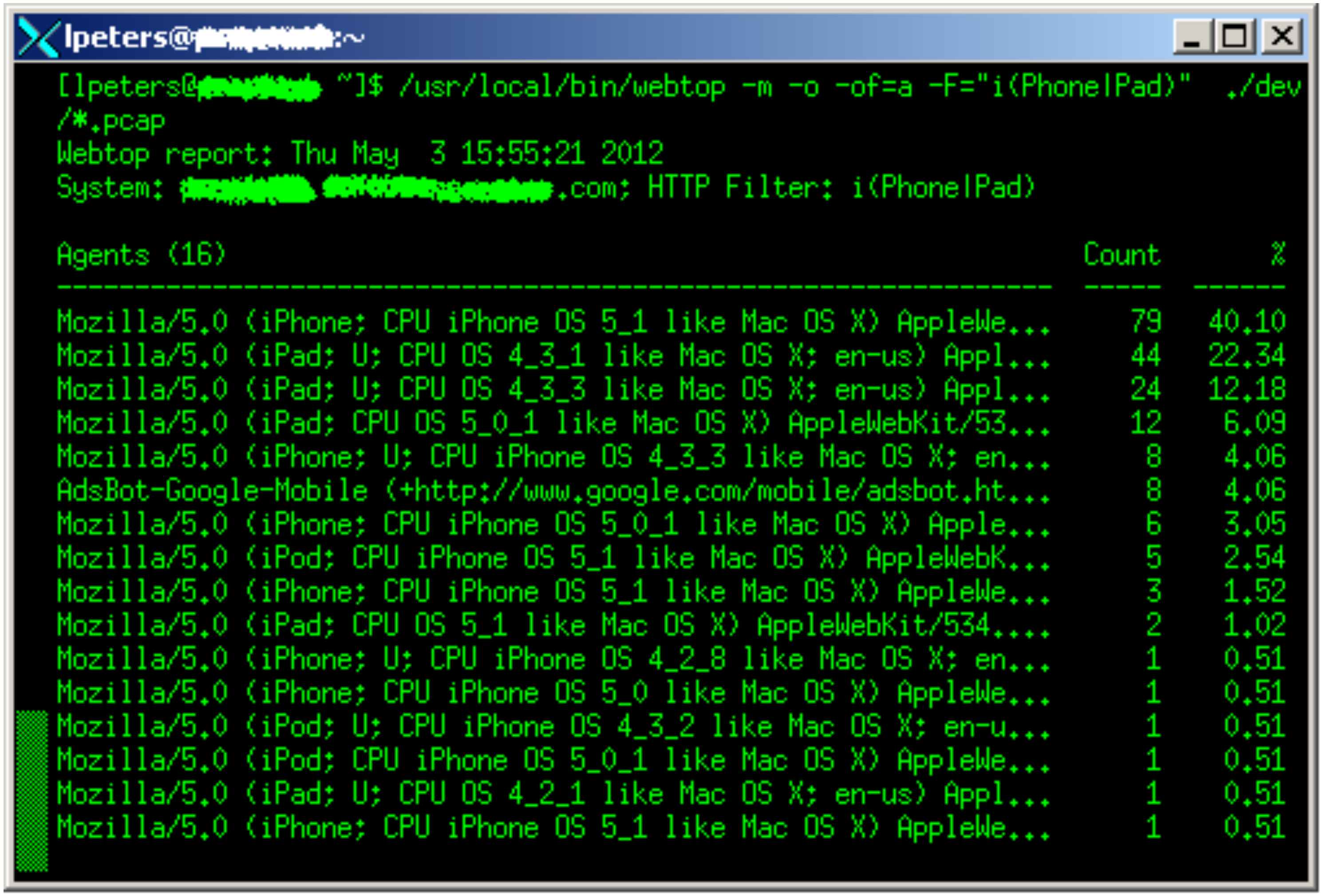
Webtop – Top Talkers



```
[lpeters@[redacted] ~]$ /usr/local/bin/webtop -m -o -of=s -ol=20 ./dev/*.pcap
Webtop report: Thu May  3 15:36:17 2012
System: [redacted].[redacted].com

Sources (930)                                                  Count      %
-------------------------------------------------------------  -----  ------
66.249.71.154                                                   1006    3.98
66.249.71.181                                                    885    3.50
66.249.71.199                                                    882    3.49
66.249.71.230                                                    870    3.44
66.249.71.216                                                    861    3.41
66.249.71.180                                                    857    3.39
66.249.71.170                                                    851    3.37
66.249.71.172                                                    845    3.35
66.249.71.218                                                    843    3.34
66.249.71.214                                                    838    3.32
66.249.71.155                                                    837    3.31
66.249.71.219                                                    832    3.29
66.249.71.168                                                    828    3.28
66.249.71.217                                                    821    3.25
66.249.71.228                                                    818    3.24
66.249.71.215                                                    816    3.23
66.249.71.169                                                    812    3.21
66.249.71.171                                                    810    3.21
```

Webtop – Apple User-Agents



```
[lpeters@[redacted] ~]$ /usr/local/bin/webtop -m -o -of=a -F="i(Phone|Pad)"  ./dev
/*.pcap
Webtop report: Thu May  3 15:55:21 2012
System: [redacted] [redacted].com; HTTP Filter: i(Phone|Pad)

Agents (16)                                                      Count      %
-------------------------------------------------------------    -----  ------
Mozilla/5.0 (iPhone; CPU iPhone OS 5_1 like Mac OS X) AppleWe...    79   40.10
Mozilla/5.0 (iPad; U; CPU OS 4_3_1 like Mac OS X; en-us) Appl...    44   22.34
Mozilla/5.0 (iPad; U; CPU OS 4_3_3 like Mac OS X; en-us) Appl...    24   12.18
Mozilla/5.0 (iPad; CPU OS 5_0_1 like Mac OS X) AppleWebKit/53...    12    6.09
Mozilla/5.0 (iPhone; U; CPU iPhone OS 4_3_3 like Mac OS X; en...     8    4.06
AdsBot-Google-Mobile (+http://www.google.com/mobile/adsbot.ht...     8    4.06
Mozilla/5.0 (iPhone; CPU iPhone OS 5_0_1 like Mac OS X) Apple...     6    3.05
Mozilla/5.0 (iPod; CPU iPhone OS 5_1 like Mac OS X) AppleWebK...     5    2.54
Mozilla/5.0 (iPhone; CPU iPhone OS 5_1 like Mac OS X) AppleWe...     3    1.52
Mozilla/5.0 (iPad; CPU OS 5_1 like Mac OS X) AppleWebKit/534....     2    1.02
Mozilla/5.0 (iPhone; U; CPU iPhone OS 4_2_8 like Mac OS X; en...     1    0.51
Mozilla/5.0 (iPhone; CPU iPhone OS 5_0 like Mac OS X) AppleWe...     1    0.51
Mozilla/5.0 (iPod; U; CPU iPhone OS 4_3_2 like Mac OS X; en-u...     1    0.51
Mozilla/5.0 (iPod; CPU iPhone OS 5_0_1 like Mac OS X) AppleWe...     1    0.51
Mozilla/5.0 (iPad; U; CPU OS 4_2_1 like Mac OS X; en-us) Appl...     1    0.51
Mozilla/5.0 (iPhone; CPU iPhone OS 5_1 like Mac OS X) AppleWe...     1    0.51
```

Webtop - Internals

100% Perl code

Extendible - just add

HTTP header regex
keyboard command
output format command

Location:
https://sourceforge.net/projects/neustarwebtop/

Thank you