
# Peel Back the Layers of Your Network in Minutes

Doug Burks

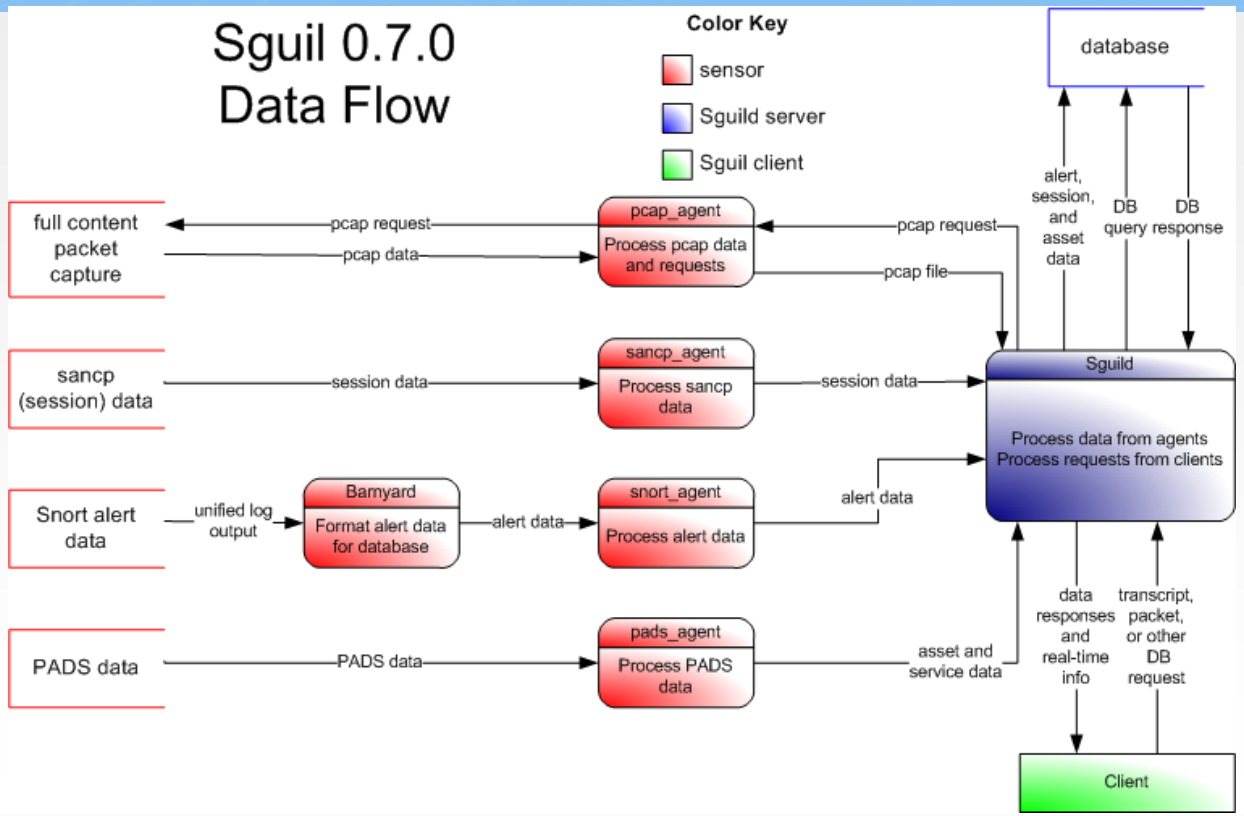
# What is Security Onion?

Security Onion is a Linux distro for IDS (Intrusion Detection) and NSM (Network Security Monitoring). It's based on Ubuntu and contains Snort, Suricata, Bro, Sguil, Squert, Snorby, ELSA, Xplico, NetworkMiner, and many other security tools. The easy-to-use Setup wizard allows you to build an army of distributed sensors for your enterprise in minutes!

# IDS is sub-optimal; need NSM (multiple data types)

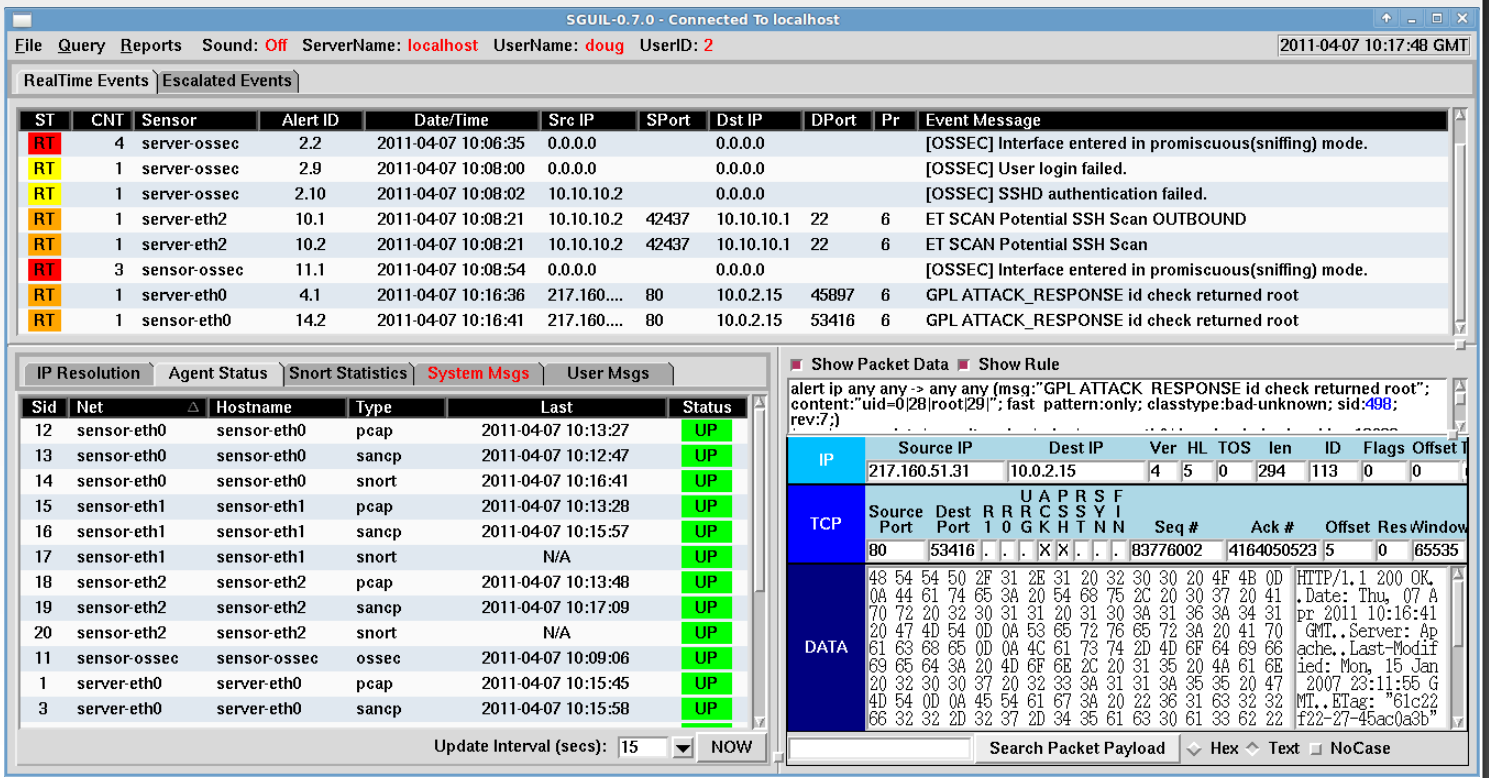
# Sguil is the defacto reference implementation of NSM

# Lots of pieces in the Sguil jigsaw puzzle

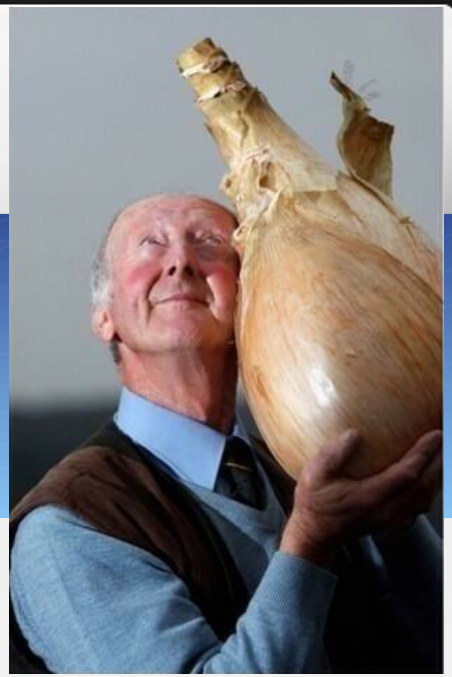



http://nsmwiki.org/images/e/ea/Sguil-0.7.dfd.png

# Security Onion:
# Next, Next, Finish for NSM

# Big Onions

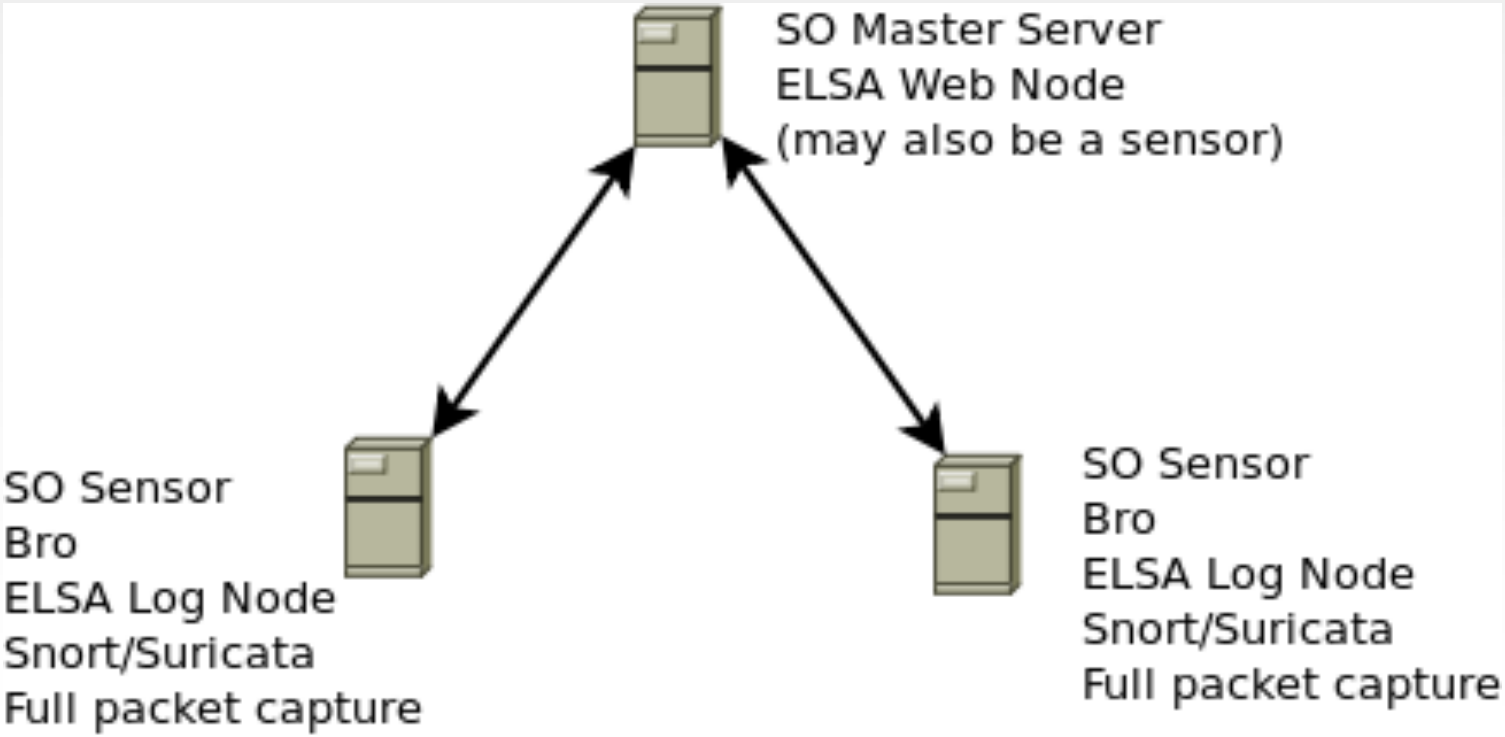


- Use our ISO image (based on Xubuntu 12.04 **64-bit**)
  OR
  Start with your preferred flavor of Ubuntu 12.04 (Ubuntu, Kubuntu, Lubuntu, Xubuntu, or **Ubuntu Server**) 32-bit or **64-bit**, add our PPA and install our packages
- High performance:
  - Snort/Suricata/Bro running on **PF_RING**
  - Netsniff-ng uses **zero-copy** for high-speed full-packet capture
- ELSA (like a free version of Splunk) – **distributed** database with central web interface

# Data Types

- Alert data
  - NIDS alerts from Snort/Suricata
  - HIDS alerts from OSSEC
- Asset data from Bro and PRADS
- Session data from Argus, Bro, and PRADS
- Transaction data – http/ftp/dns/ssl/other logs from Bro
- Full content data from netsniff-ng

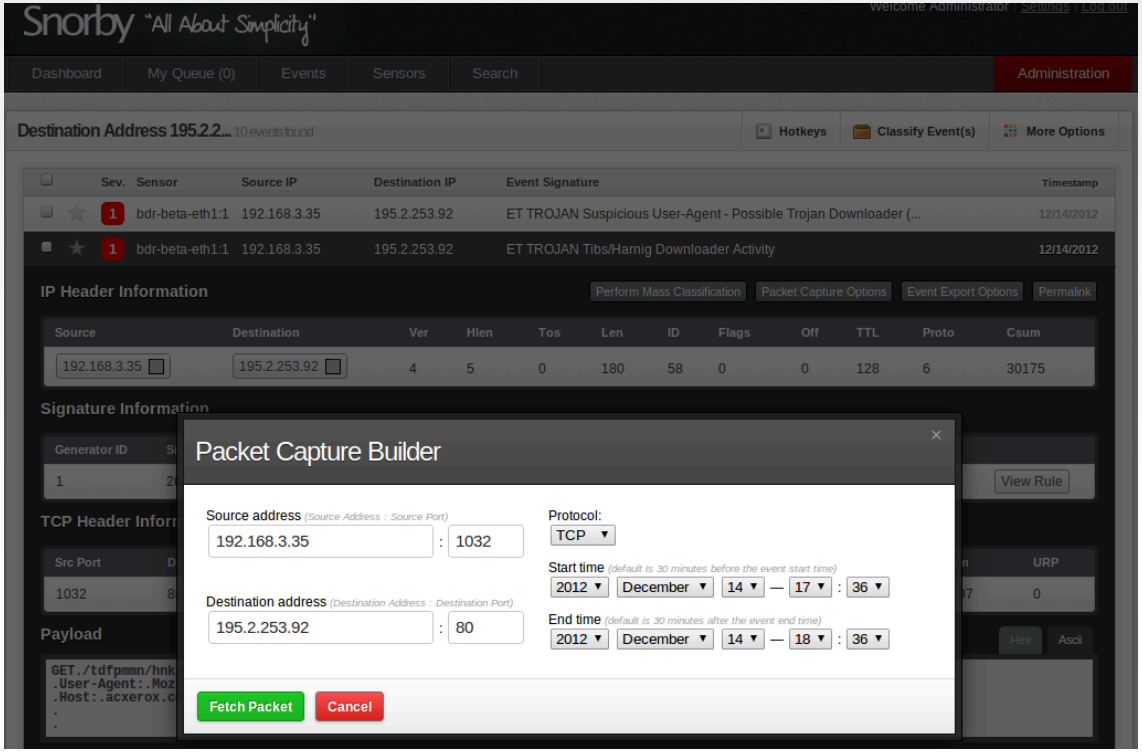
# Distributed Deployment



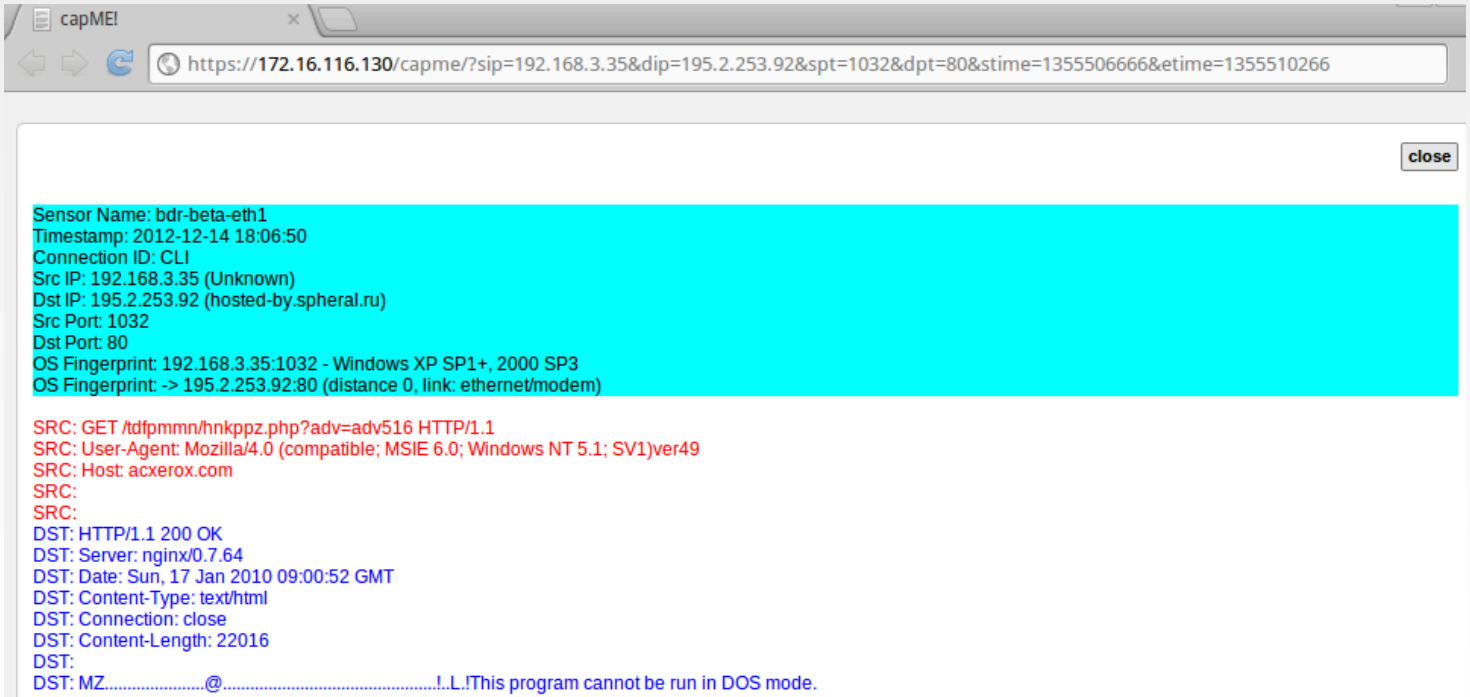
# Snorby


Snorby "All About Simplicity"
Welcome Dustin Webber | Settings | Log out
Dashboard
My Queue (8)
Events
Sensors
Search
Administration
Dashboard
More Options
TODAY YESTERDAY THIS WEEK THIS MONTH THIS QUARTER THIS YEAR
Last Updated: 11/28/10 5:00:00 PM
58
HIGH SEVERITY
58 / 2268
64
MEDIUM SEVERITY
64 / 2268
2146
LOW SEVERITY
2146 / 2268
Sensors
Severities
Protocols
Signatures
Sources
Destinations
Event Count vs Time By Sensor
Snorby.org
Home Sensor
Event Count
Hour of Day
Highcharts v2.1 Beta
TOP 5 SENSOR
Snorby.org 3120
Home Sensor 494
TOP 5 ACTIVE USERS
Dustin Webber 8
Administrator 0
LAST 5 UNIQUE EVENTS
(http_inspect) CHUNK S... 2
Bad segment, adjusted ... 8
(http_inspect) OVERSIZ... 2
ET WORM Potential MySQ... 4
TCP Timestamp is outsi... 6
ANALYST CLASSIFIED EVENTS
False Positive 418
Unauthorized Root Access 0
Unauthorized User Access 0
Attempted Unauthorized... 0
Denial of Service Attack 0
Policy Violation 0
Reconnaissance 0
Virus Infection 0
Snorby 2.0.0 - http://www.snorby.org © 2010 Dustin Willis Webber

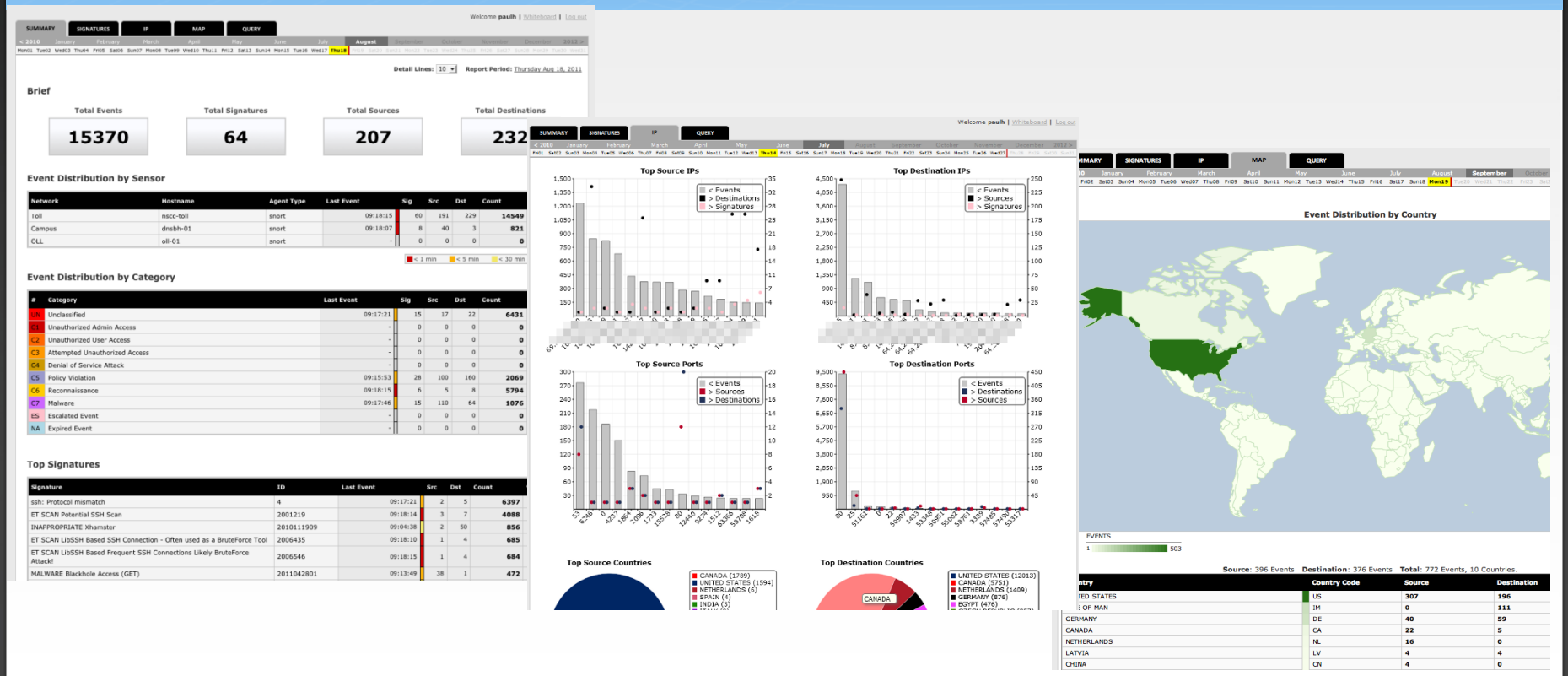
# Pivot to pcap from Snorby



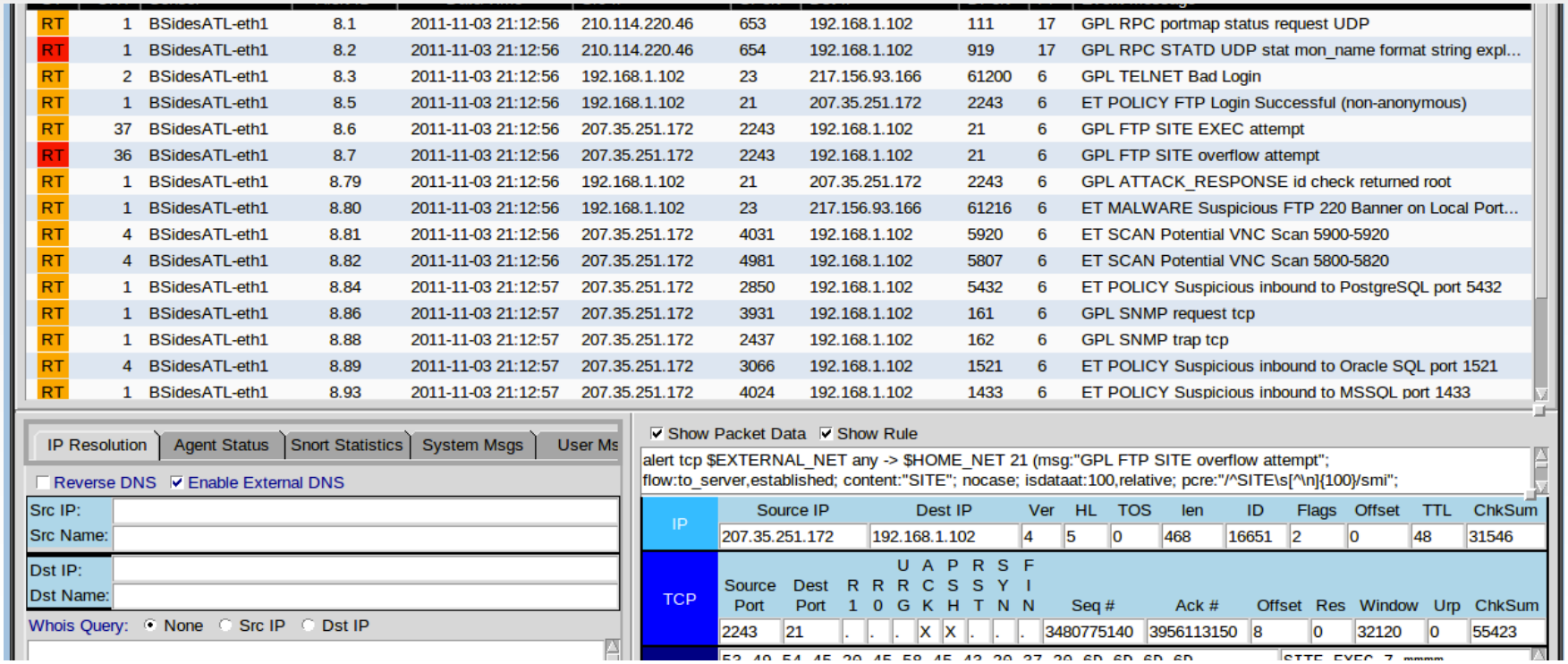
# CapME


capME!
https://172.16.116.130/capme/?sip=192.168.3.35&dip=195.2.253.92&spt=1032&dpt=80&stime=1355506666&etime=1355510266
close
Sensor Name: bdr-beta-eth1
Timestamp: 2012-12-14 18:06:50
Connection ID: CLI
Src IP: 192.168.3.35 (Unknown)
Dst IP: 195.2.253.92 (hosted-by.spheral.ru)
Src Port: 1032
Dst Port: 80
OS Fingerprint: 192.168.3.35:1032 - Windows XP SP1+, 2000 SP3
OS Fingerprint: -> 195.2.253.92:80 (distance 0, link: ethernet/modem)
SRC: GET /tdfpmmn/hnkppz.php?adv=adv516 HTTP/1.1
SRC: User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)ver49
SRC: Host: acxerox.com
SRC:
SRC:
DST: HTTP/1.1 200 OK
DST: Server: nginx/0.7.64
DST: Date: Sun, 17 Jan 2010 09:00:52 GMT
DST: Content-Type: text/html
DST: Connection: close
DST: Content-Length: 22016
DST:
DST: MZ.....@.....!..L.!This program cannot be run in DOS mode.

# Squert web interface



# Sguil client



| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| RT | 1 | BSidesATL-eth1 | 8.1 | 2011-11-03 21:12:56 | 210.114.220.46 | 653 | 192.168.1.102 | 111 | 17 | GPL RPC portmap status request UDP |
| RT | 1 | BSidesATL-eth1 | 8.2 | 2011-11-03 21:12:56 | 210.114.220.46 | 654 | 192.168.1.102 | 919 | 17 | GPL RPC STATD UDP stat mon_name format string expl... |
| RT | 2 | BSidesATL-eth1 | 8.3 | 2011-11-03 21:12:56 | 192.168.1.102 | 23 | 217.156.93.166 | 61200 | 6 | GPL TELNET Bad Login |
| RT | 1 | BSidesATL-eth1 | 8.5 | 2011-11-03 21:12:56 | 192.168.1.102 | 21 | 207.35.251.172 | 2243 | 6 | ET POLICY FTP Login Successful (non-anonymous) |
| RT | 37 | BSidesATL-eth1 | 8.6 | 2011-11-03 21:12:56 | 207.35.251.172 | 2243 | 192.168.1.102 | 21 | 6 | GPL FTP SITE EXEC attempt |
| RT | 36 | BSidesATL-eth1 | 8.7 | 2011-11-03 21:12:56 | 207.35.251.172 | 2243 | 192.168.1.102 | 21 | 6 | GPL FTP SITE overflow attempt |
| RT | 1 | BSidesATL-eth1 | 8.79 | 2011-11-03 21:12:56 | 192.168.1.102 | 21 | 207.35.251.172 | 2243 | 6 | GPL ATTACK_RESPONSE id check returned root |
| RT | 1 | BSidesATL-eth1 | 8.80 | 2011-11-03 21:12:56 | 192.168.1.102 | 23 | 217.156.93.166 | 61216 | 6 | ET MALWARE Suspicious FTP 220 Banner on Local Port... |
| RT | 4 | BSidesATL-eth1 | 8.81 | 2011-11-03 21:12:56 | 207.35.251.172 | 4031 | 192.168.1.102 | 5920 | 6 | ET SCAN Potential VNC Scan 5900-5920 |
| RT | 4 | BSidesATL-eth1 | 8.82 | 2011-11-03 21:12:56 | 207.35.251.172 | 4981 | 192.168.1.102 | 5807 | 6 | ET SCAN Potential VNC Scan 5800-5820 |
| RT | 1 | BSidesATL-eth1 | 8.84 | 2011-11-03 21:12:57 | 207.35.251.172 | 2850 | 192.168.1.102 | 5432 | 6 | ET POLICY Suspicious inbound to PostgreSQL port 5432 |
| RT | 1 | BSidesATL-eth1 | 8.86 | 2011-11-03 21:12:57 | 207.35.251.172 | 3931 | 192.168.1.102 | 161 | 6 | GPL SNMP request tcp |
| RT | 1 | BSidesATL-eth1 | 8.88 | 2011-11-03 21:12:57 | 207.35.251.172 | 2437 | 192.168.1.102 | 162 | 6 | GPL SNMP trap tcp |
| RT | 4 | BSidesATL-eth1 | 8.89 | 2011-11-03 21:12:57 | 207.35.251.172 | 3066 | 192.168.1.102 | 1521 | 6 | ET POLICY Suspicious inbound to Oracle SQL port 1521 |
| RT | 1 | BSidesATL-eth1 | 8.93 | 2011-11-03 21:12:57 | 207.35.251.172 | 4024 | 192.168.1.102 | 1433 | 6 | ET POLICY Suspicious inbound to MSSQL port 1433 |

IP Resolution | Agent Status | Snort Statistics | System Msgs | User Ms

Reverse DNS | Enable External DNS

Src IP:
Src Name:
Dst IP:
Dst Name:

Whois Query: None | Src IP | Dst IP

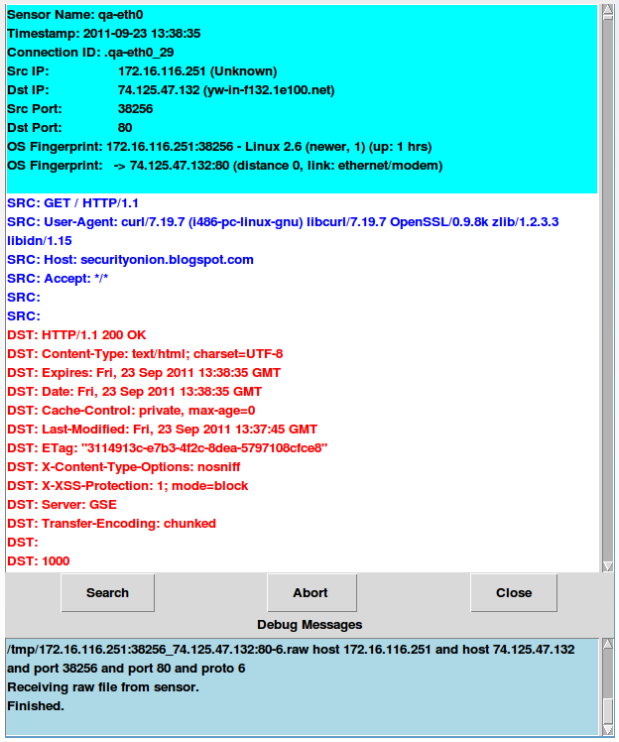
Show Packet Data | Show Rule

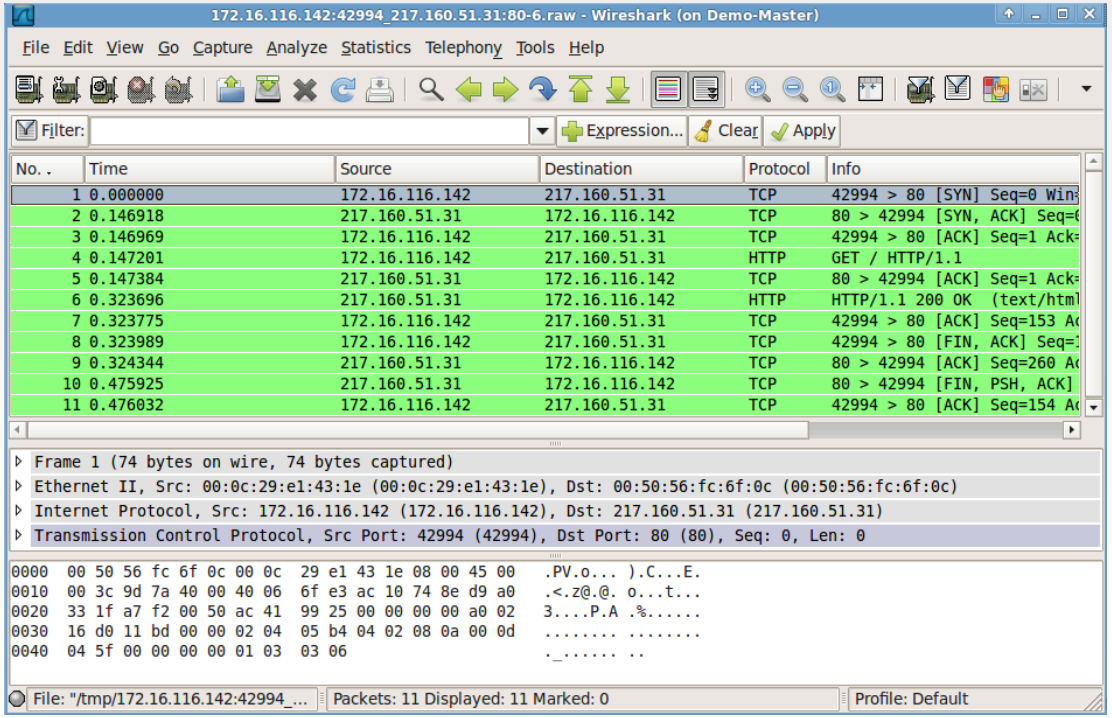
```
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"GPL FTP SITE overflow attempt";
flow:to_server,established; content:"SITE"; nocase; isdataat:100,relative; pcre:"/^SITE\s[^\n]{100}/smi";
```

| IP | Source IP | Dest IP | Ver | HL | TOS | len | ID | Flags | Offset | TTL | ChkSum |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | 207.35.251.172 | 192.168.1.102 | 4 | 5 | 0 | 468 | 16651 | 2 | 0 | 48 | 31546 |

| TCP | Source Port | Dest Port | R 1 | R 0 | URG | ACK | PSH | RST | SYN | FIN | Seq # | Ack # | Offset | Res | Window | Urp | ChkSum |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 2243 | 21 | . | . | . | X | X | . | . | . | 3480775140 | 3956113150 | 8 | 0 | 32120 | 0 | 55423 |

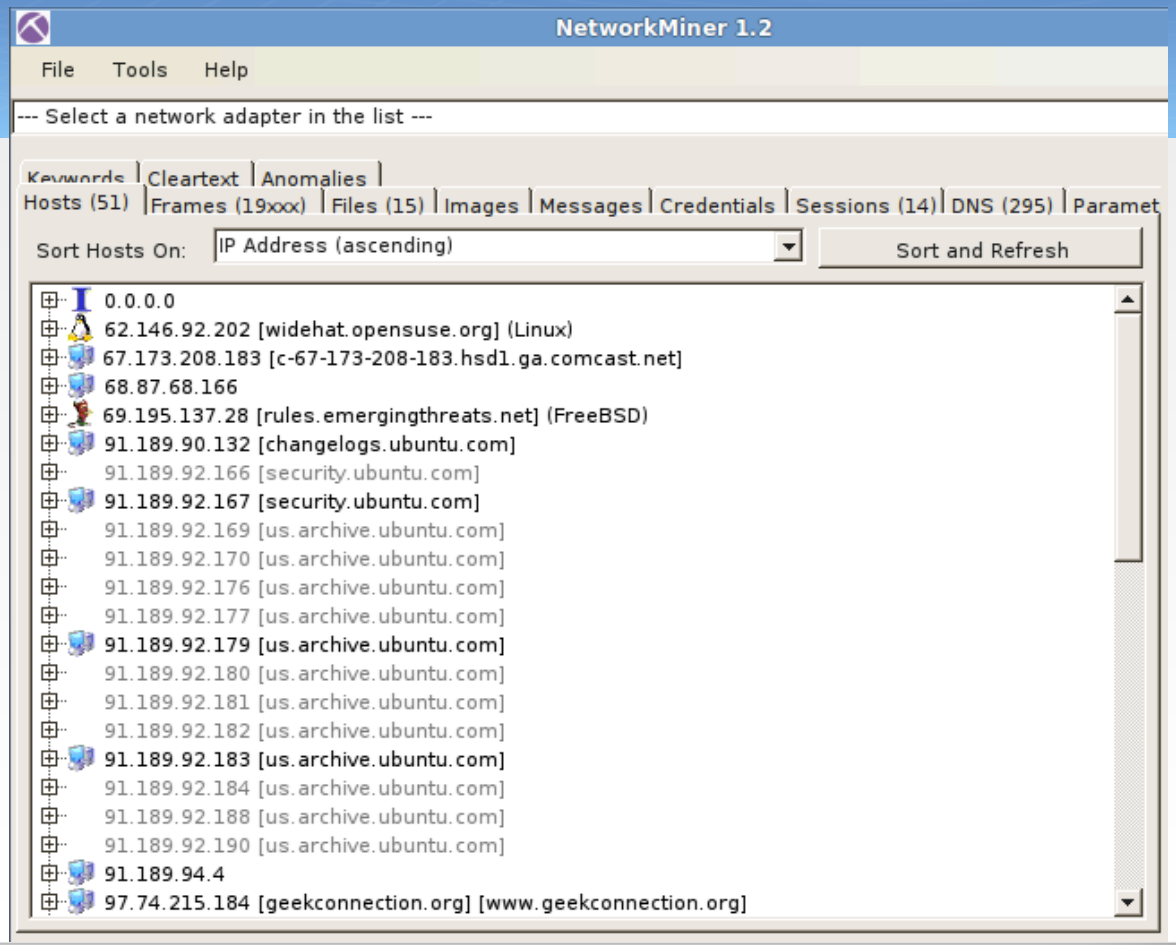
# Pivot to pcap from Sguil



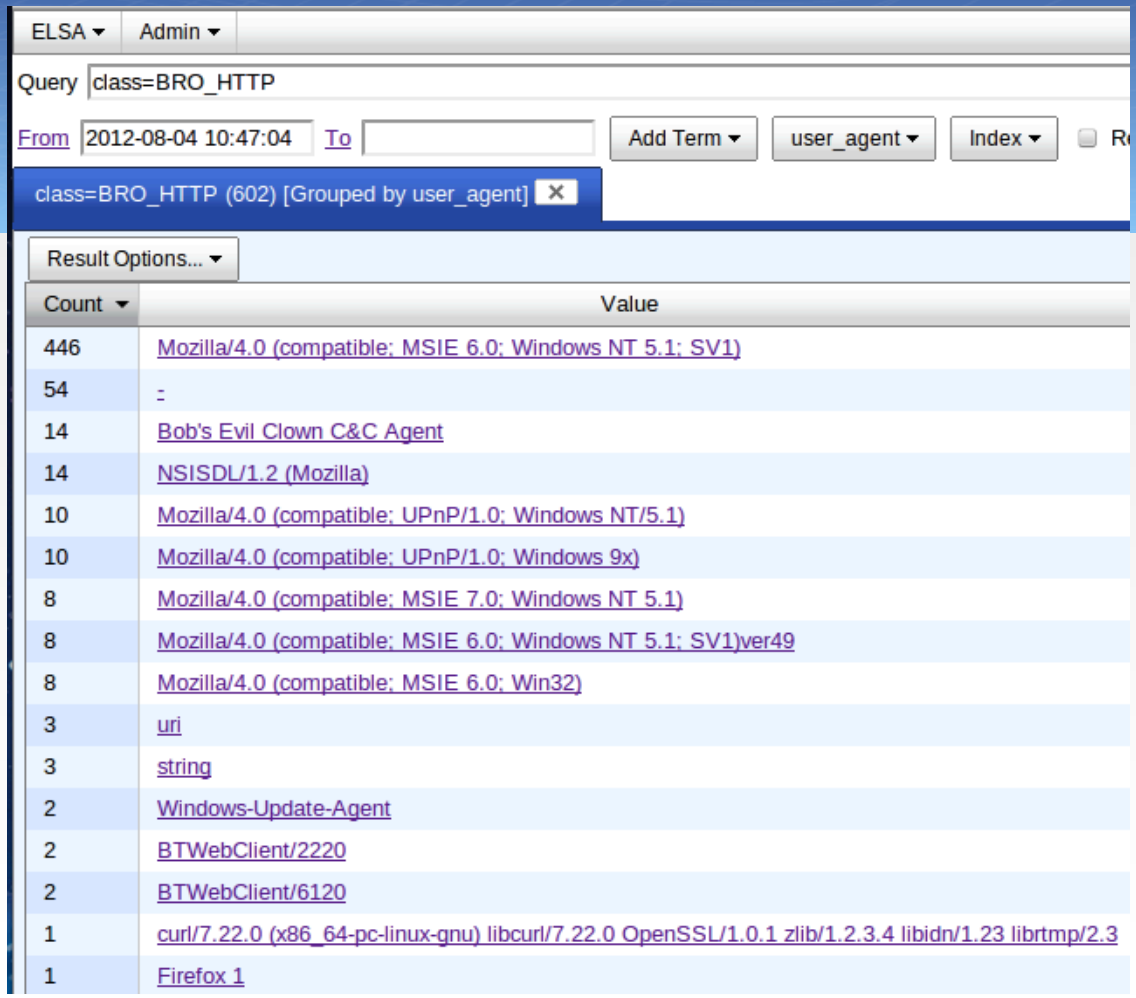



# NetworkMiner

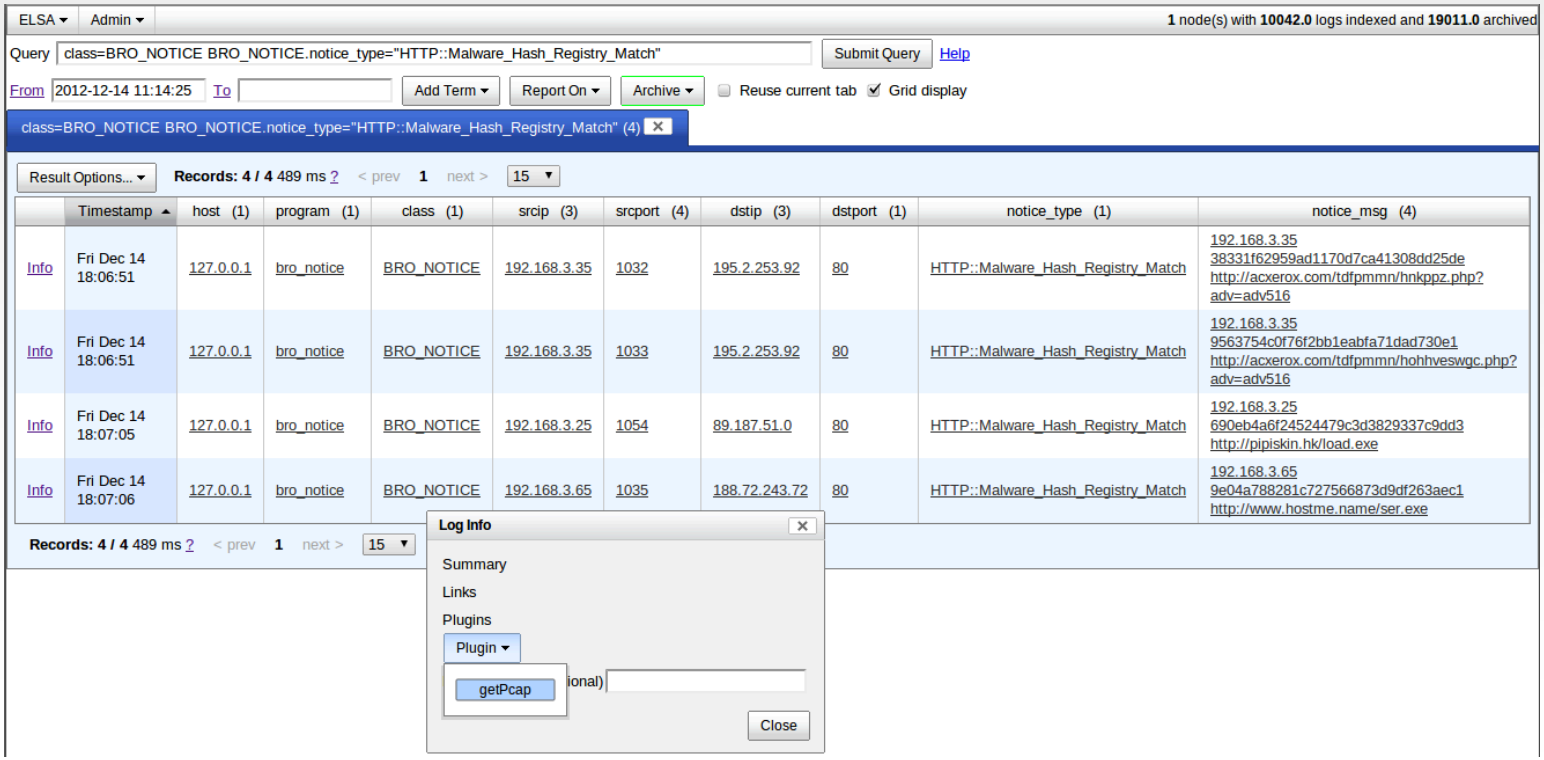
There’s gold in them thar PCAPs!



# ELSA

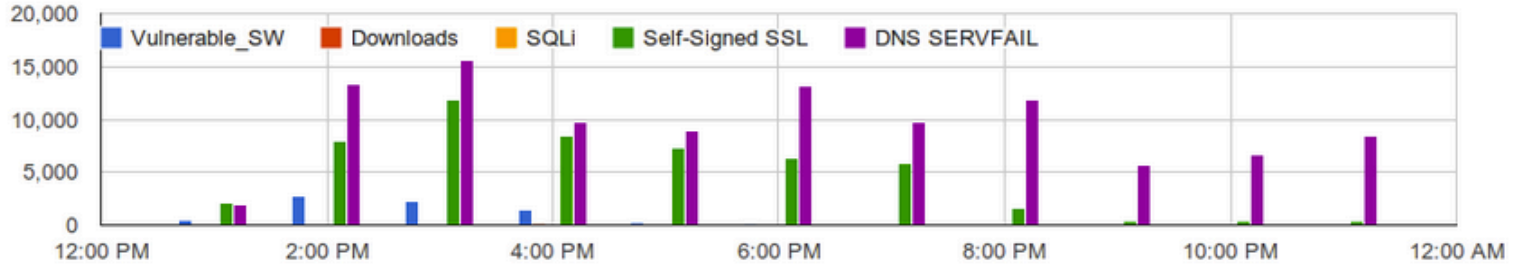

ELSA
Admin
Query class=BRO_HTTP
From 2012-08-04 10:47:04
To
Add Term
user_agent
Index
class=BRO_HTTP (602) [Grouped by user_agent]
Result Options...
Count
Value
446 Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
54 -
14 Bob's Evil Clown C&C Agent
14 NSISDL/1.2 (Mozilla)
10 Mozilla/4.0 (compatible; UPnP/1.0; Windows NT/5.1)
10 Mozilla/4.0 (compatible; UPnP/1.0; Windows 9x)
8 Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)
8 Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)ver49
8 Mozilla/4.0 (compatible; MSIE 6.0; Win32)
3 uri
3 string
2 Windows-Update-Agent
2 BTWebClient/2220
2 BTWebClient/6120
1 curl/7.22.0 (x86_64-pc-linux-gnu) libcurl/7.22.0 OpenSSL/1.0.1 zlib/1.2.3.4 libidn/1.23 librtmp/2.3
1 Firefox 1

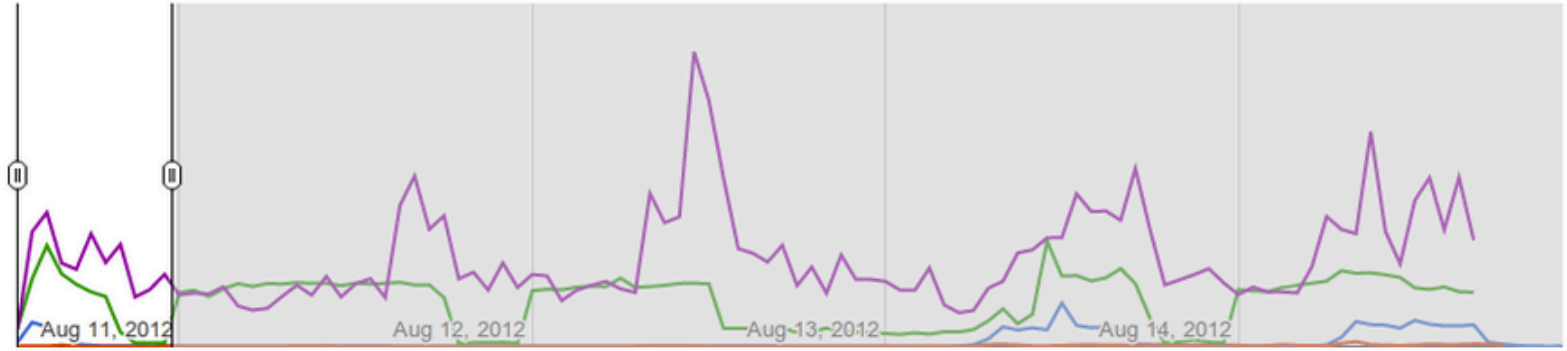
# Pivot to pcap from ELSA



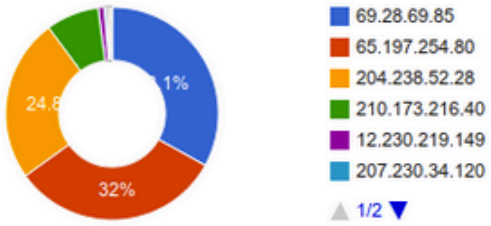
# Bro IDS

## Bro Events




**Self-Signed SSL Destinations**

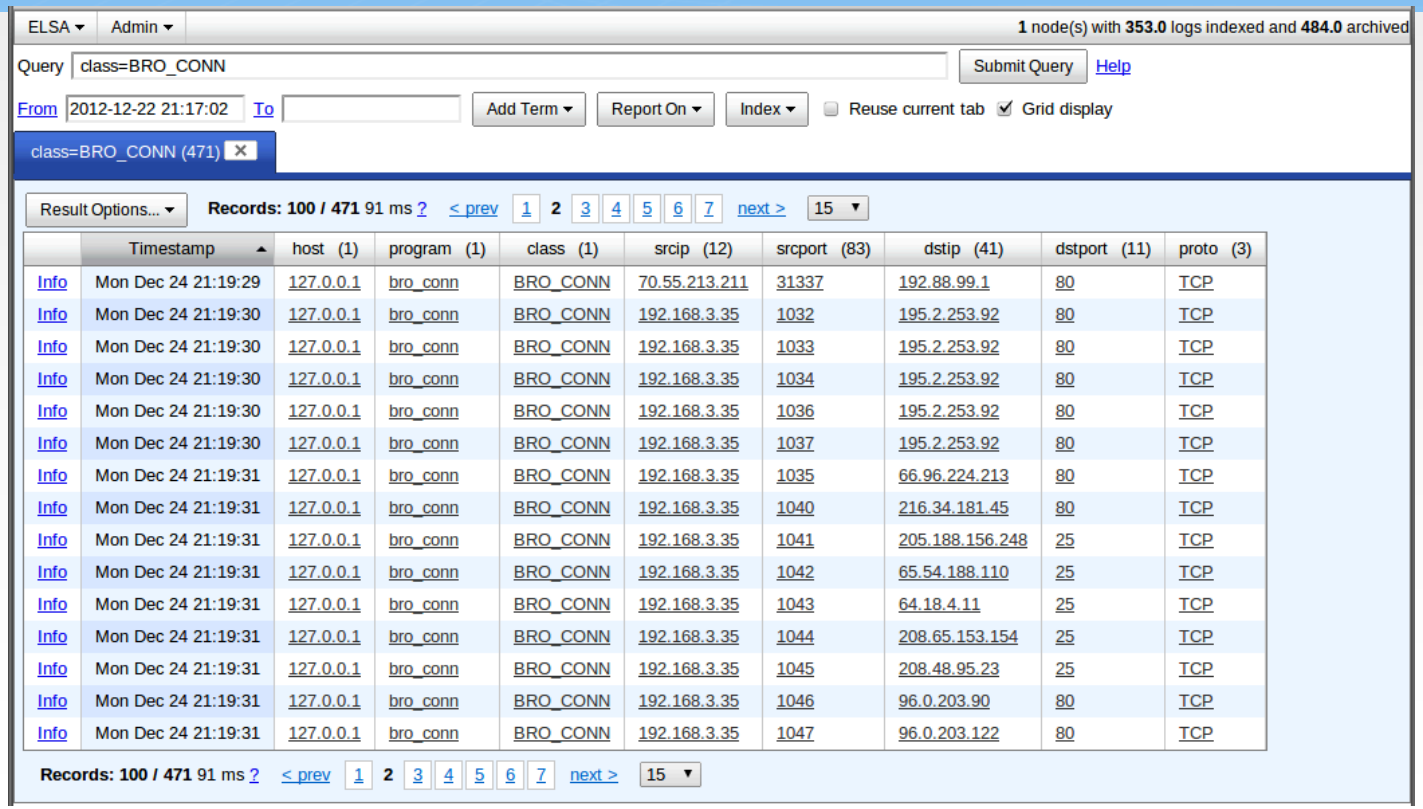



- 69.28.69.85
- 65.197.254.80
- 204.238.52.28
- 210.173.216.40
- 12.230.219.149
- 207.230.34.120

1/2

| subject |
| --- |
| emailAddress=admin@wiredsolar.net,CN=secure.wiredsolar.net,OU=IT,O=Wired Solar,L=Flagler,ST=Florida,C=US |
| CN=rsip.monitoredsecurity.com,OU=IT Security,O=Symantec Corporation,L=Northern |
| emailAddress=dhoover@centonline.com,CN=Dean Hoover,OU=Network Admin,O=Ce Berlin,ST=Wisconsin,C=US |
| ST=Tokyo,OU=Remote Service,O=RICOH COMPANY\,LTD.,L=Aoyama,C=JP,CN=G |
| CN=mcs1hkg.live.citrixonline.com,OU=Operations,O=Citrix Online LLC,L=Fort Lauder |
| C=CA |
| C=US,CN=mail.tytix.com |
| CN=TrustedSourceServer_IMQA01 |

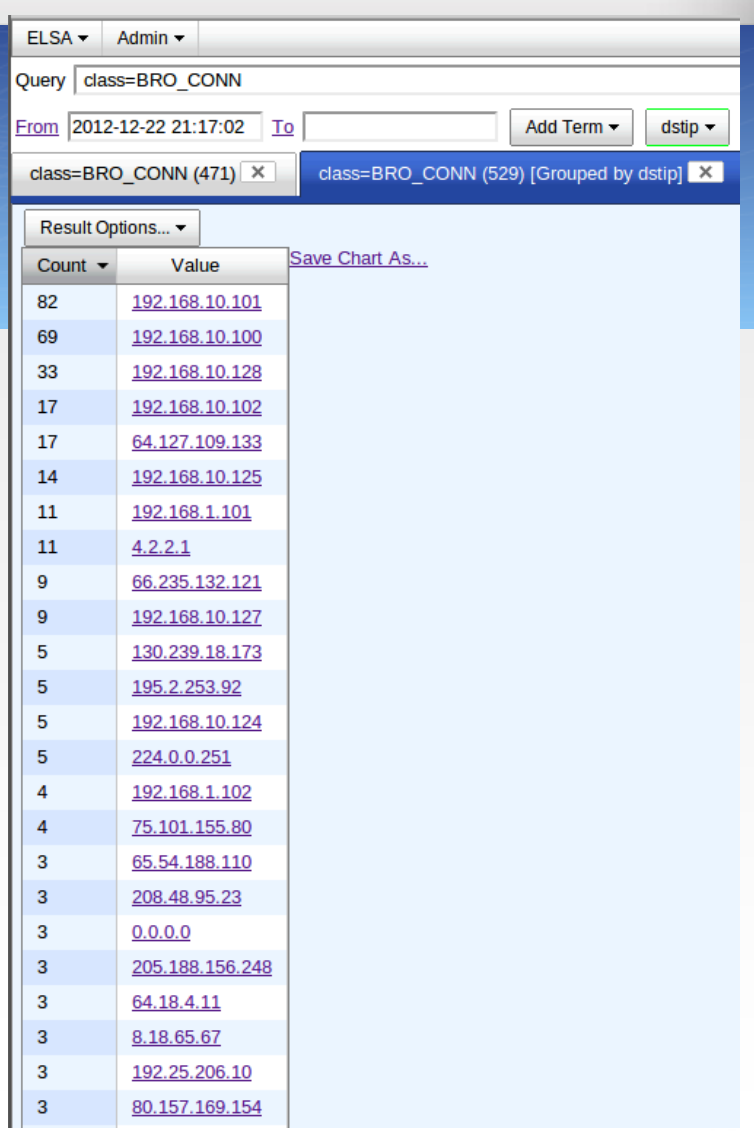
# Bro Flow



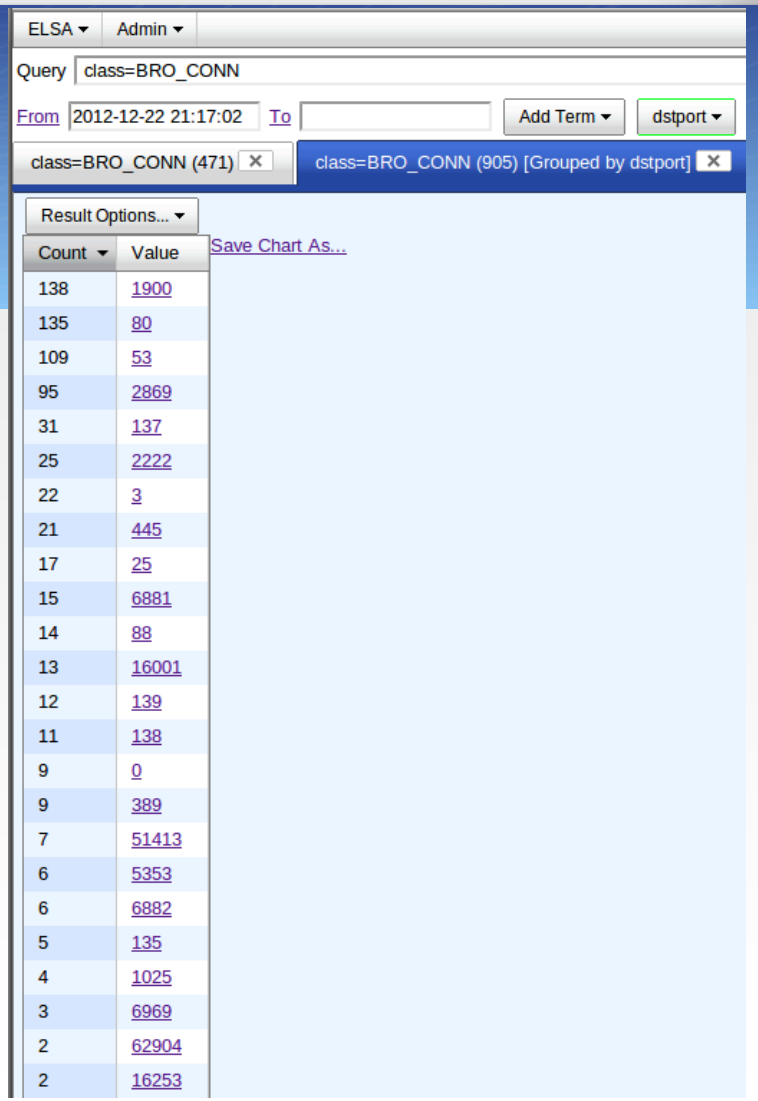

| | Timestamp | host (1) | program (1) | class (1) | srcip (12) | srcport (83) | dstip (41) | dstport (11) | proto (3) |
|---|---|---|---|---|---|---|---|---|---|
| Info | Mon Dec 24 21:19:29 | 127.0.0.1 | bro_conn | BRO_CONN | 70.55.213.211 | 31337 | 192.88.99.1 | 80 | TCP |
| Info | Mon Dec 24 21:19:30 | 127.0.0.1 | bro_conn | BRO_CONN | 192.168.3.35 | 1032 | 195.2.253.92 | 80 | TCP |
| Info | Mon Dec 24 21:19:30 | 127.0.0.1 | bro_conn | BRO_CONN | 192.168.3.35 | 1033 | 195.2.253.92 | 80 | TCP |
| Info | Mon Dec 24 21:19:30 | 127.0.0.1 | bro_conn | BRO_CONN | 192.168.3.35 | 1034 | 195.2.253.92 | 80 | TCP |
| Info | Mon Dec 24 21:19:30 | 127.0.0.1 | bro_conn | BRO_CONN | 192.168.3.35 | 1036 | 195.2.253.92 | 80 | TCP |
| Info | Mon Dec 24 21:19:30 | 127.0.0.1 | bro_conn | BRO_CONN | 192.168.3.35 | 1037 | 195.2.253.92 | 80 | TCP |
| Info | Mon Dec 24 21:19:31 | 127.0.0.1 | bro_conn | BRO_CONN | 192.168.3.35 | 1035 | 66.96.224.213 | 80 | TCP |
| Info | Mon Dec 24 21:19:31 | 127.0.0.1 | bro_conn | BRO_CONN | 192.168.3.35 | 1040 | 216.34.181.45 | 80 | TCP |
| Info | Mon Dec 24 21:19:31 | 127.0.0.1 | bro_conn | BRO_CONN | 192.168.3.35 | 1041 | 205.188.156.248 | 25 | TCP |
| Info | Mon Dec 24 21:19:31 | 127.0.0.1 | bro_conn | BRO_CONN | 192.168.3.35 | 1042 | 65.54.188.110 | 25 | TCP |
| Info | Mon Dec 24 21:19:31 | 127.0.0.1 | bro_conn | BRO_CONN | 192.168.3.35 | 1043 | 64.18.4.11 | 25 | TCP |
| Info | Mon Dec 24 21:19:31 | 127.0.0.1 | bro_conn | BRO_CONN | 192.168.3.35 | 1044 | 208.65.153.154 | 25 | TCP |
| Info | Mon Dec 24 21:19:31 | 127.0.0.1 | bro_conn | BRO_CONN | 192.168.3.35 | 1045 | 208.48.95.23 | 25 | TCP |
| Info | Mon Dec 24 21:19:31 | 127.0.0.1 | bro_conn | BRO_CONN | 192.168.3.35 | 1046 | 96.0.203.90 | 80 | TCP |
| Info | Mon Dec 24 21:19:31 | 127.0.0.1 | bro_conn | BRO_CONN | 192.168.3.35 | 1047 | 96.0.203.122 | 80 | TCP |

Records: 100 / 471 91 ms ? < prev 1 2 3 4 5 6 7 next > 15

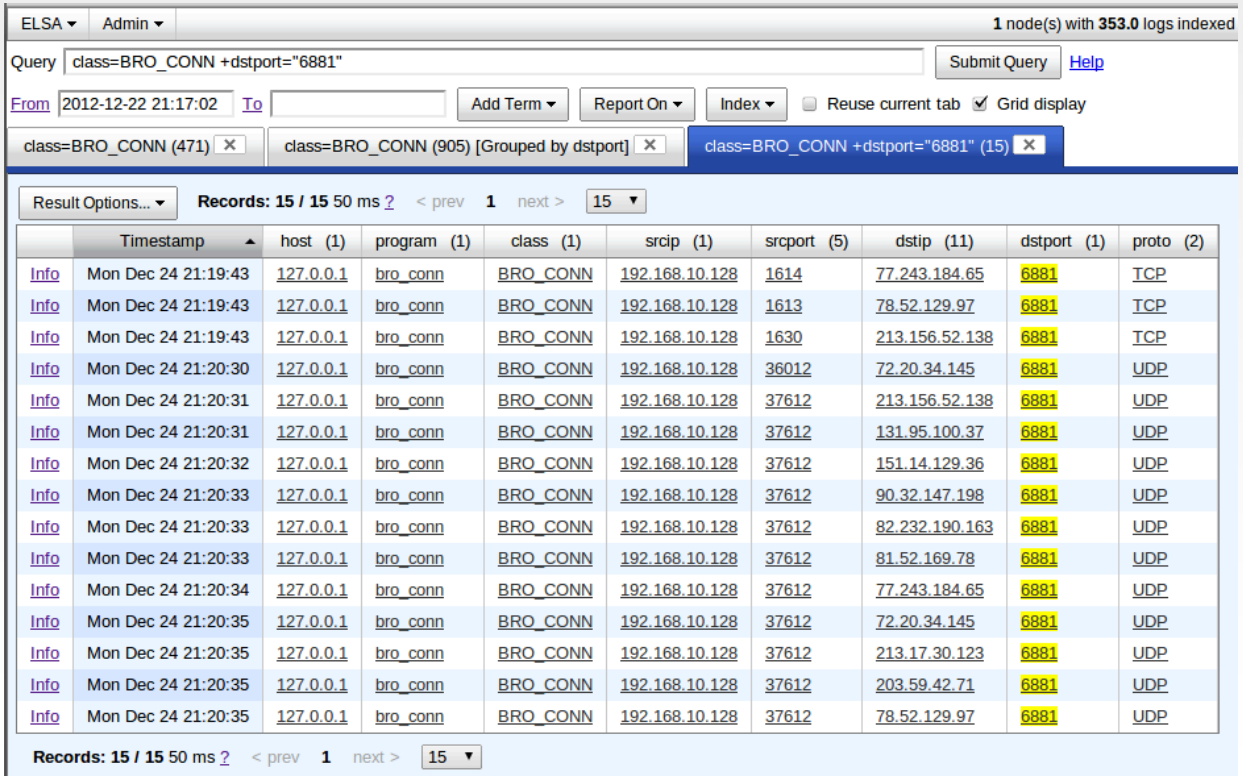
# Popular Dst IPs



# Popular Dst Ports



# Drilling into an interesting Dst Port




| | Timestamp | host (1) | program (1) | class (1) | srcip (1) | srcport (5) | dstip (11) | dstport (1) | proto (2) |
|---|---|---|---|---|---|---|---|---|---|
| Info | Mon Dec 24 21:19:43 | 127.0.0.1 | bro_conn | BRO_CONN | 192.168.10.128 | 1614 | 77.243.184.65 | 6881 | TCP |
| Info | Mon Dec 24 21:19:43 | 127.0.0.1 | bro_conn | BRO_CONN | 192.168.10.128 | 1613 | 78.52.129.97 | 6881 | TCP |
| Info | Mon Dec 24 21:19:43 | 127.0.0.1 | bro_conn | BRO_CONN | 192.168.10.128 | 1630 | 213.156.52.138 | 6881 | TCP |
| Info | Mon Dec 24 21:20:30 | 127.0.0.1 | bro_conn | BRO_CONN | 192.168.10.128 | 36012 | 72.20.34.145 | 6881 | UDP |
| Info | Mon Dec 24 21:20:31 | 127.0.0.1 | bro_conn | BRO_CONN | 192.168.10.128 | 37612 | 213.156.52.138 | 6881 | UDP |
| Info | Mon Dec 24 21:20:31 | 127.0.0.1 | bro_conn | BRO_CONN | 192.168.10.128 | 37612 | 131.95.100.37 | 6881 | UDP |
| Info | Mon Dec 24 21:20:32 | 127.0.0.1 | bro_conn | BRO_CONN | 192.168.10.128 | 37612 | 151.14.129.36 | 6881 | UDP |
| Info | Mon Dec 24 21:20:33 | 127.0.0.1 | bro_conn | BRO_CONN | 192.168.10.128 | 37612 | 90.32.147.198 | 6881 | UDP |
| Info | Mon Dec 24 21:20:33 | 127.0.0.1 | bro_conn | BRO_CONN | 192.168.10.128 | 37612 | 82.232.190.163 | 6881 | UDP |
| Info | Mon Dec 24 21:20:33 | 127.0.0.1 | bro_conn | BRO_CONN | 192.168.10.128 | 37612 | 81.52.169.78 | 6881 | UDP |
| Info | Mon Dec 24 21:20:34 | 127.0.0.1 | bro_conn | BRO_CONN | 192.168.10.128 | 37612 | 77.243.184.65 | 6881 | UDP |
| Info | Mon Dec 24 21:20:35 | 127.0.0.1 | bro_conn | BRO_CONN | 192.168.10.128 | 37612 | 72.20.34.145 | 6881 | UDP |
| Info | Mon Dec 24 21:20:35 | 127.0.0.1 | bro_conn | BRO_CONN | 192.168.10.128 | 37612 | 213.17.30.123 | 6881 | UDP |
| Info | Mon Dec 24 21:20:35 | 127.0.0.1 | bro_conn | BRO_CONN | 192.168.10.128 | 37612 | 203.59.42.71 | 6881 | UDP |
| Info | Mon Dec 24 21:20:35 | 127.0.0.1 | bro_conn | BRO_CONN | 192.168.10.128 | 37612 | 78.52.129.97 | 6881 | UDP |

# What is that Dst Port? Pivot 2 Pcap!

# 2013: The Metrics

- Security Onion 10.04
  37,521
- Security Onion 12.04 (released 12/31/2012)
  34,290 from SourceForge
- Security Onion 12.04.1 (released 6/10/2013)
  6,380 from Sourceforge
- Security Onion 12.04.2 (released 7/25/2013)
  737 from Sourceforge
- ??? From BitTorrent
  ??? Ubuntu/Kubuntu/Lubuntu + Security Onion PPA

# Where do we go now?

## http://securityonion.blogspot.com

Updates are announced here and it also has the following links:

- Download/Install
- FAQ
- Mailing Lists
- IRC #securityonion on irc.freenode.net
- @securityonion