The Security Onion

Chris Krieger

Security Onion 101

Security Onion is a network security monitoring (NSM) system that provides full-context and forensic visibility into the traffic it monitors

Designed to make deploying complex open source tools simple via a single package (Snort, Suricata, Sguil, Snorby etc.)

Peeling the Onion

Contains a boatload of security tools

Easy setup wizard … even a Windows Admin can do it!

Has the ability to pivot from one tool to the next to seamlessly

- One of the most effective collection of network security tools available in a single package

Behind the Onion

Created by Doug Burks

Grew out of a SANS Gold Paper

He wanted to make NSM easier to deploy

Before the Onion

Get an alert (firewall, user, etc.)

Look for the alert in some SIEM tool

Try to correlate with other events in SIEM

Oh crap … We didn’t add that server to the SIEM yet – my bad

With NSM & SO

We can take an IDS alert -->

alert ip $EXTERNAL_NET $SHELLCODE_PORTS -> $HOME_NET any (msg:"GPL SHELLCODE x86 inc ebx NOOP";content:"CCCCCCCCCCCCCCCCCCCCCCCCCC"; fast_pattern:only; classtype: shellcode-detect; sid:2101390; rev:7;)

And turn it into something useful:

- Full traffic packet captures
- ASCII transcripts of traffic
- Ability to carve files (or malware) for later analysis
- Build our own alerts

Onion Layers

Over 60 custom tools

- Snort – Signature based IDS
- Sguil – Security analyst console
- Squert -View HIDS/NIDS alerts and HTTP logs
- Snorby -View and annotate IDS alerts
- ELSA - Search logs (IDS, Bro and syslog)
- Bro - Powerful network analysis framework with highly detailed logs
- OSSEC - Monitors local logs, file integrity & rootkits

Onion Links

Project Home

http://code.google.com/p/security-onion/

Blog

http://securityonion.blogspot.com

Mailing Lists

http://code.google.com/p/security-onion/wiki/MailingLists

Google Group

https://groups.google.com/forum/?fromgroups#!forum/security-onion

Wiki

http://code.google.com/p/security-onion/w/list

Installing the Onion

Download the ISO from the SO website.

Write/Burn to media

- Do *not* download updates while installing
- Do *not* Install this third-party software
- Create Username & Password
  - Just make sure you remember them.

VMTools/Virtualbox on the Onion

Tools adds features to the VM and helps manage memory better

Updating the Onion

SO has a customized update script

- # sudo soup

Wireshark

The default version of Wireshark (WS) in SO needs updating

Download WS source code from WS's website in SO

tar xaf wireshark-<version..tar.bz2

cd wireshark-<version>

sudo apt-get install build-essential qt4-dev-tools libgtk-3-dev libpcap-dev

sudo ./configure

sudo make

sudo make install

sudo ldconfig

Setup the Onion

SO has a Customized Configuration script

- Configuring SO Software
  - Configuration of network
  - Install NSM Software Components
  - Configure storage settings
  - Finalize configuration

SO tool highlights

- SO Data presentation tools
  - Packet Analysis Tools
  - NSM consoles
- SO Data collection tools
- SO Data delivery tools

tcpdump

- Command line tool
  - Available, but does not run by default
- Many uses, capture’s live traffic
- Replays already captured traffic
- Can use BPF filters to only capture protocol
  - host, ip, port, etc.
- Available for almost all Linux distributions.

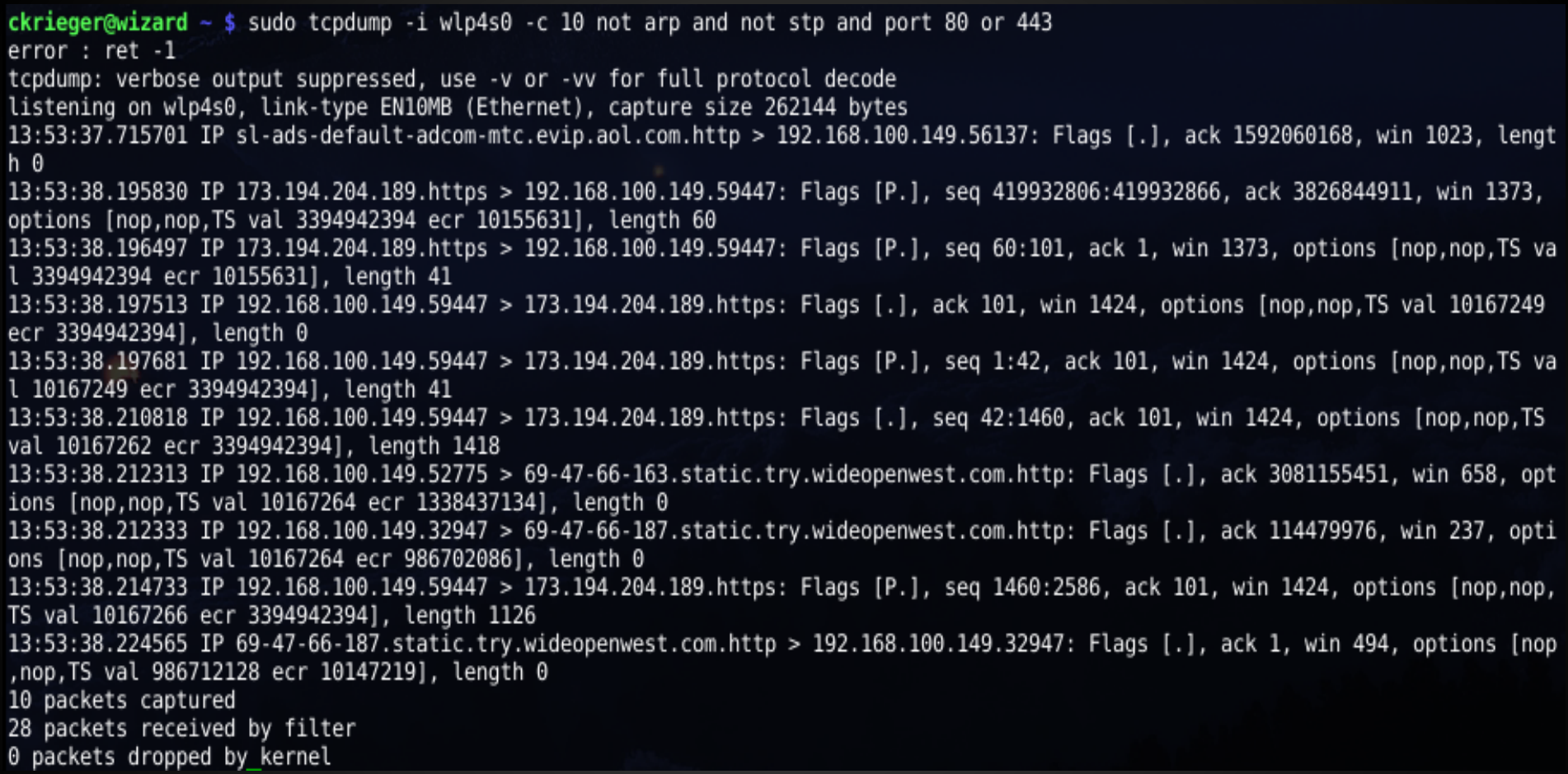
tcpdump switches

- -n doesn’t resolve IP’s to hosts
- -i specific ethernet adapter
- -c count of packets to capture
- -s specify bytes to capture
- -w <filename> write packets to file
- -r <filename> read packets from filename

** man tcpdump for more details

tcpdump filters

- icmp (only capture icmp traffic)
- port <port #>(only capture specific port)
- tcp (only capture tcp traffic)
- host <host, IP, or net> traffic related to host
- src <host, IP, or net> only capture src traffic
- dst <host, IP, or net> only capture dst traffic
- NOT <any above> to remove

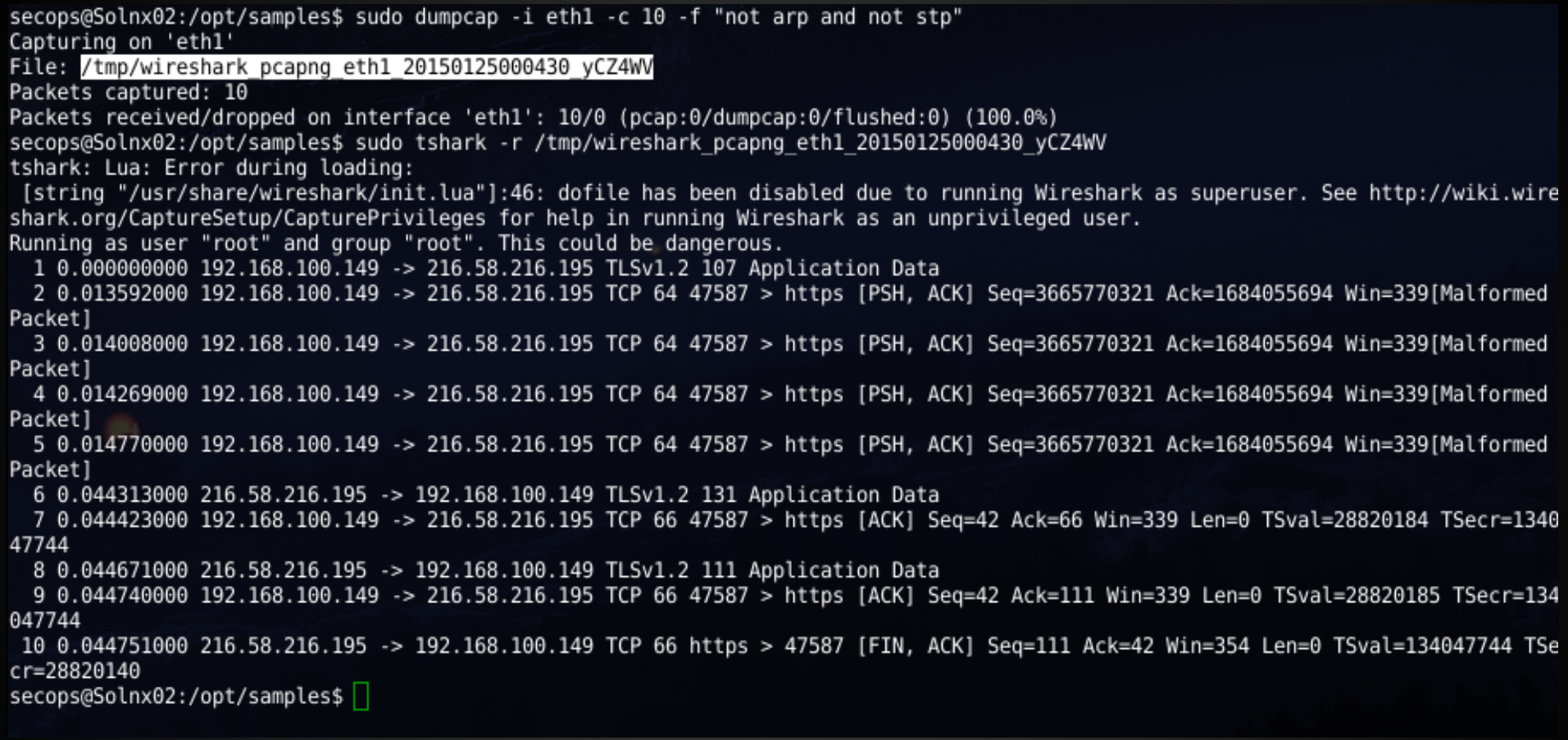


tcpdump in action

dumpcap and tshark

- Part of Wireshark's installation
- dumpcap works similar to tcpdump
  - However, dumps traffic without reading it
- dumpcap uses BPF filters, just like tcpdump
- tshark can use Wireshark Display filters

** man <command> gives more details



dumpcap and tshark in action

Argus

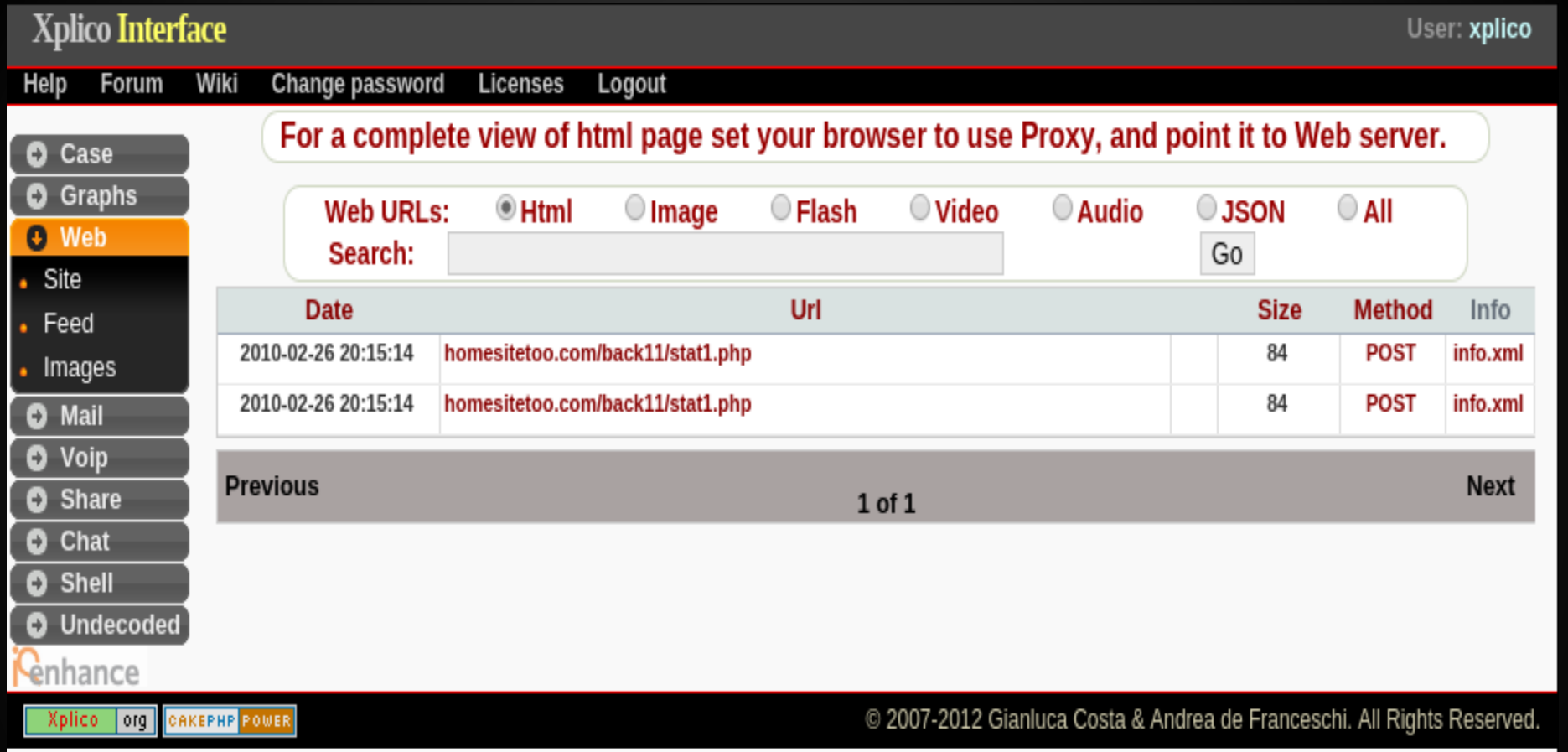
- Generates and analyzes Session data
- Saves data in binary
  - Only readable by Argus
- Session data much smaller than full packets
- There are several SO tools that capture session data

```
secops@Solnx02:~$ ra -n -r /nsm/sensor_data/Solnx02-eth1/argus/2015-01-24.log -N 30
        StartTime      Flgs  Proto           SrcAddr  Sport   Dir           DstAddr  Dport  TotPkts   TotBytes State
   23:20:00.065622  e          udp    192.168.100.10.63038     ->      233.89.188.1.10001        1         60   INT
   23:20:00.065986  e          udp    192.168.100.10.63038     ->  255.255.255.255.10001       10        871   INT
   23:20:00.351122  e          arp    192.168.100.149          who   192.168.100.230             9        568   CON
   23:20:00.577979  *          llc  00:14:69:16:bb:49.170       ->  01:00:0c:cc:cc:cd.170      14        908   INT
   23:20:00.578818  e          arp    192.168.100.200          who    192.168.100.19            12        764   INT
   23:20:00.783350  e          arp     192.168.100.15          who    192.168.100.19            69       4913   INT
   23:20:00.885565  e          arp    192.168.100.138          who   192.168.100.254            82       5240   INT
   23:20:01.806091  e          arp     192.168.100.51          who   192.168.100.254             4        252   INT
   23:20:05.663844  e          udp    192.168.100.149.39904    <->     192.168.100.2.53          2        576   CON
   23:20:05.665277  e          udp    192.168.100.149.38996    <->     192.168.100.2.53          2        552   CON
   23:20:05.666853  e *        tcp    192.168.100.149.53350     ->   141.101.114.190.80       10170    8952675   CON
   23:20:05.800225  e          arp     192.168.100.15          who    192.168.100.19             2        124   INT
   23:20:06.721243  *          llc  00:14:69:16:bb:49.170       ->  01:00:0c:cc:cc:cd.170      12        780   REQ
   23:20:07.031672  e          arp    192.168.100.138          who   192.168.100.254             9        564   INT
   23:20:07.540879  e          arp     192.168.100.10          who    192.168.100.70             4        252   INT
   23:20:10.037811  e          tcp     173.194.68.189.443      <?>   192.168.100.149.57883      2        192   CON
   23:20:10.675006  e d        tcp    192.168.100.149.53350     ->   141.101.114.190.80        4141    3772271   FIN
   23:20:11.116802  e d        tcp      74.125.29.189.443      <?>   192.168.100.149.45397      14       4831   CON
   23:20:12.764684  *          llc  00:14:69:16:bb:49.170       ->  01:00:0c:cc:cc:cd.170      24       1548   REQ
   23:20:13.173594  e          arp    192.168.100.138          who   192.168.100.254            24       1524   INT
   23:20:13.377028  e          udp    192.168.100.149.59753    <->     192.168.100.2.53          8        960   CON
   23:20:13.382383  e          udp    192.168.100.149.48416    <->     192.168.100.2.53          2        552   CON
   23:20:13.384236  e d        tcp    192.168.100.149.36953     ->   141.101.115.190.80         558     471383   FIN
   23:20:15.016296  e          arp     192.168.100.17          who    192.168.100.19            35       2216   INT
   23:20:15.535128  e          udp    192.168.100.149.54471    <->     192.168.100.2.53          5       1083   CON
   23:20:15.821214  e s        tcp    192.168.100.149.59464     ->      196.216.2.9.21          62       4768   FIN
   23:20:17.476544  e          tcp    192.168.100.149.44360     ->      196.216.2.9.33300       13        938   FIN
   23:20:18.379222  e          arp      192.168.100.2          who   192.168.100.149             6        376   CON
   23:20:18.497564  e          arp     192.168.100.20          who    192.168.100.19            18       1132   INT
   23:20:18.580823  e          udp    192.168.100.149.55761    <->     192.168.100.2.53          2        609   CON
secops@Solnx02:~$
```

argus in action

xplico

- Similar to Networkminer, except using a web interface
- Load a pcap file in and it analyses and spits out contents
- Also able to sniff traffic off the wire
  - Powerful analysis tool



xplico interface

NSM - Centric look at Network Traffic

- Tools are designed to help paint the bigger picture of overall communication
- Help with analysis to review many forms of data
- Help create an auditable analysis workflow

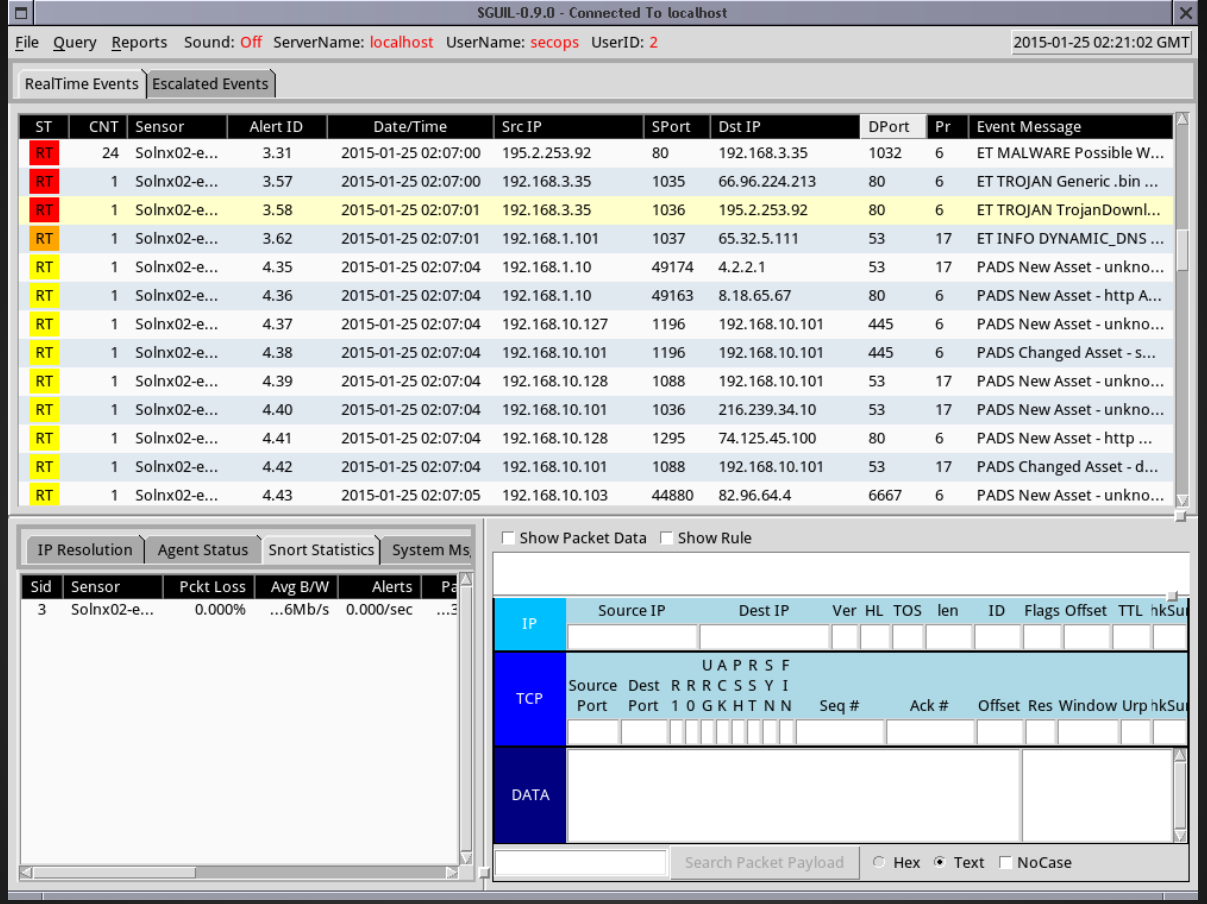
Sguil

- A Client / server application
- Collects data with deployed agents
- *Only a live tool*
- Key functions
  - Aggregates similar alert data
  - Processes metadata and makes it easy to find
  - Allows for queries and review of alert data
  - Allows for classification and pivot of events

Sguil alerts

- Incorporates 4 types of event data
  - IDS engine data like snort
  - Host based IDS like OSSEC
  - Network profile data from prads
  - Http transaction data from bro
- The interface takes some getting used to
  - NSM book does a decent job explaining it

*We'll explore these other tools later in the course



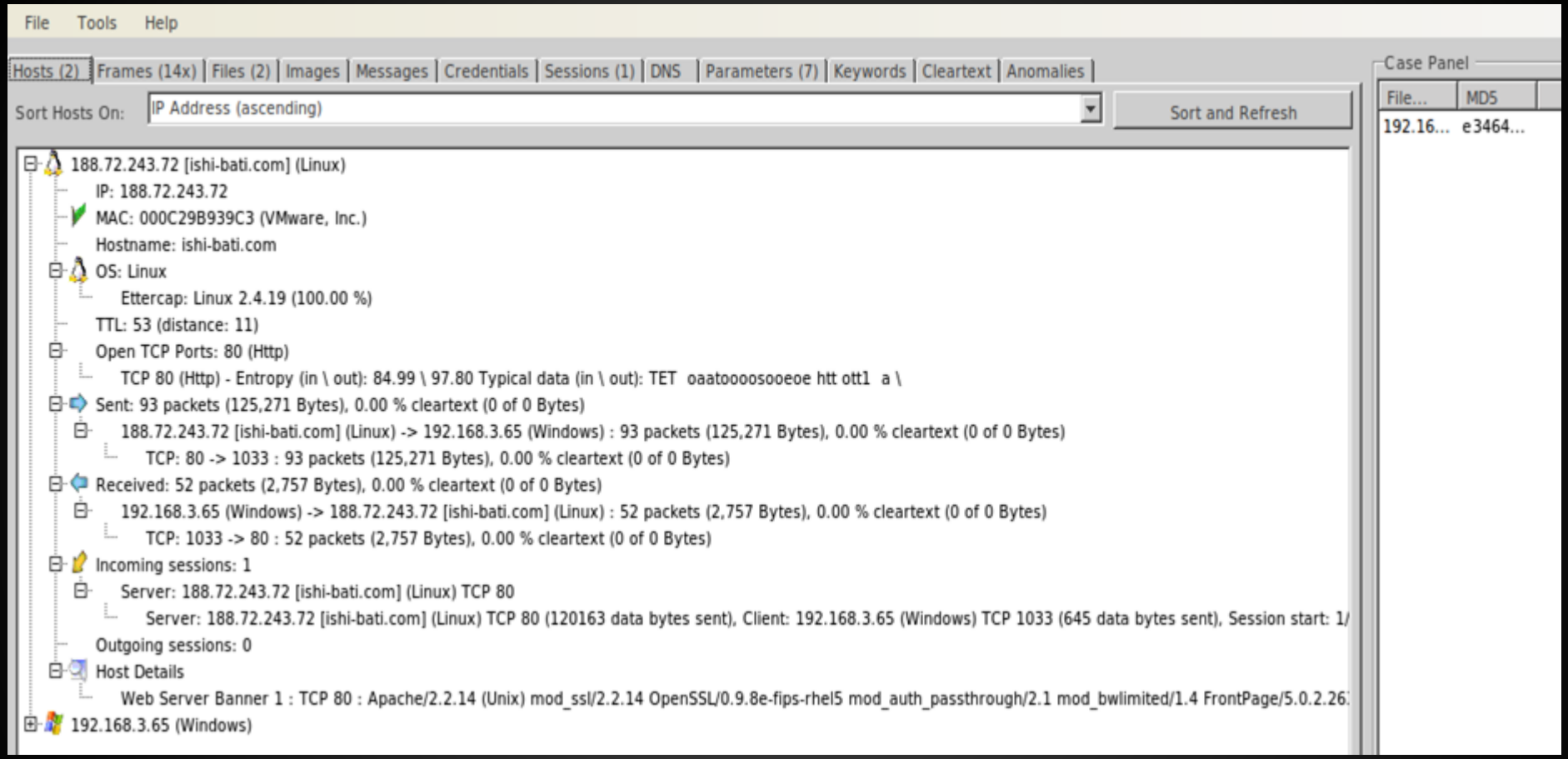
sguil main screen

Network Miner

Windows App, running under Mono in SO

Extracts & organizes host and content data

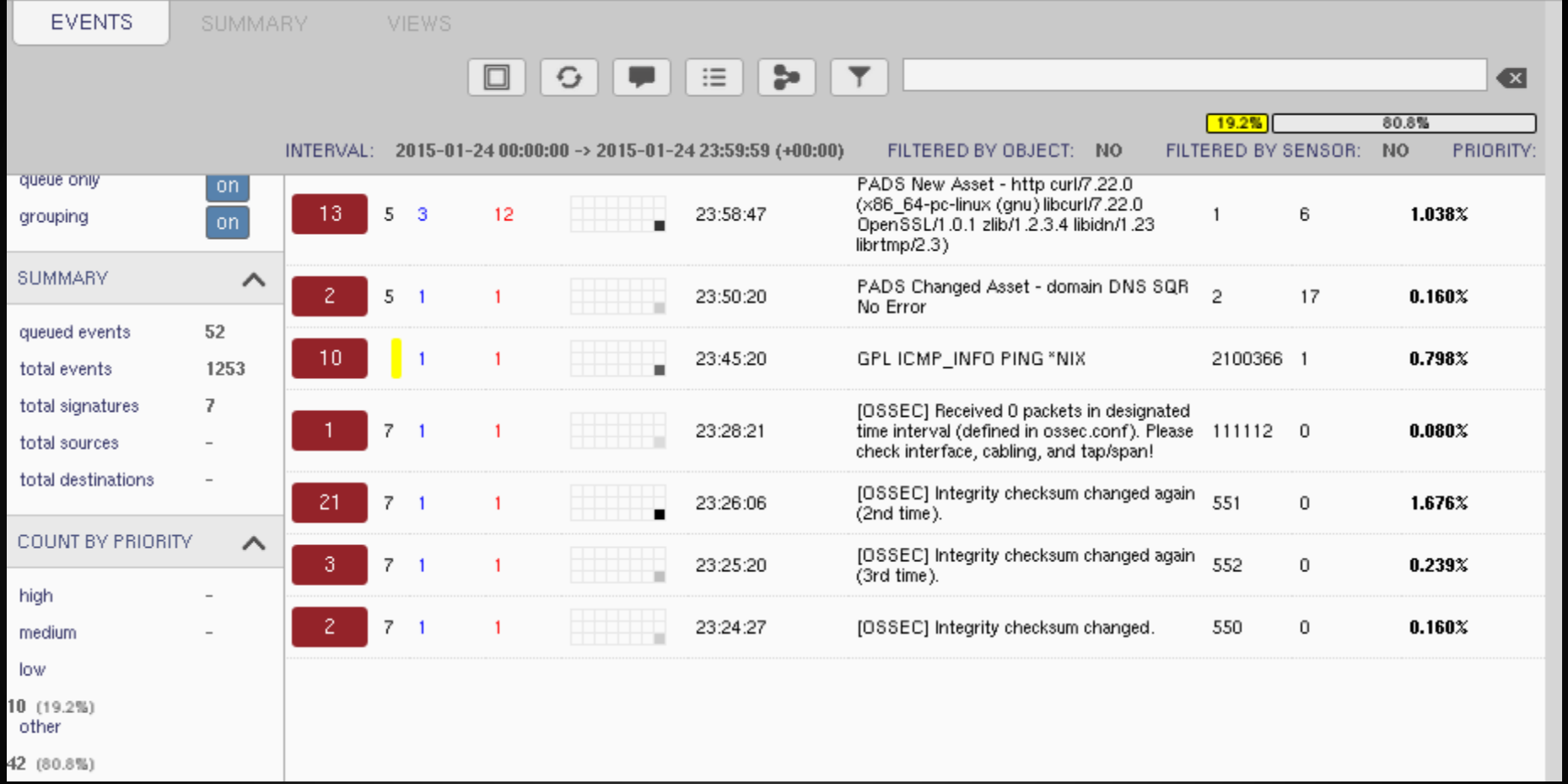
- Provides good overview of network-based artifacts
- Parsing traces might take time



Network Miner in action

Squert

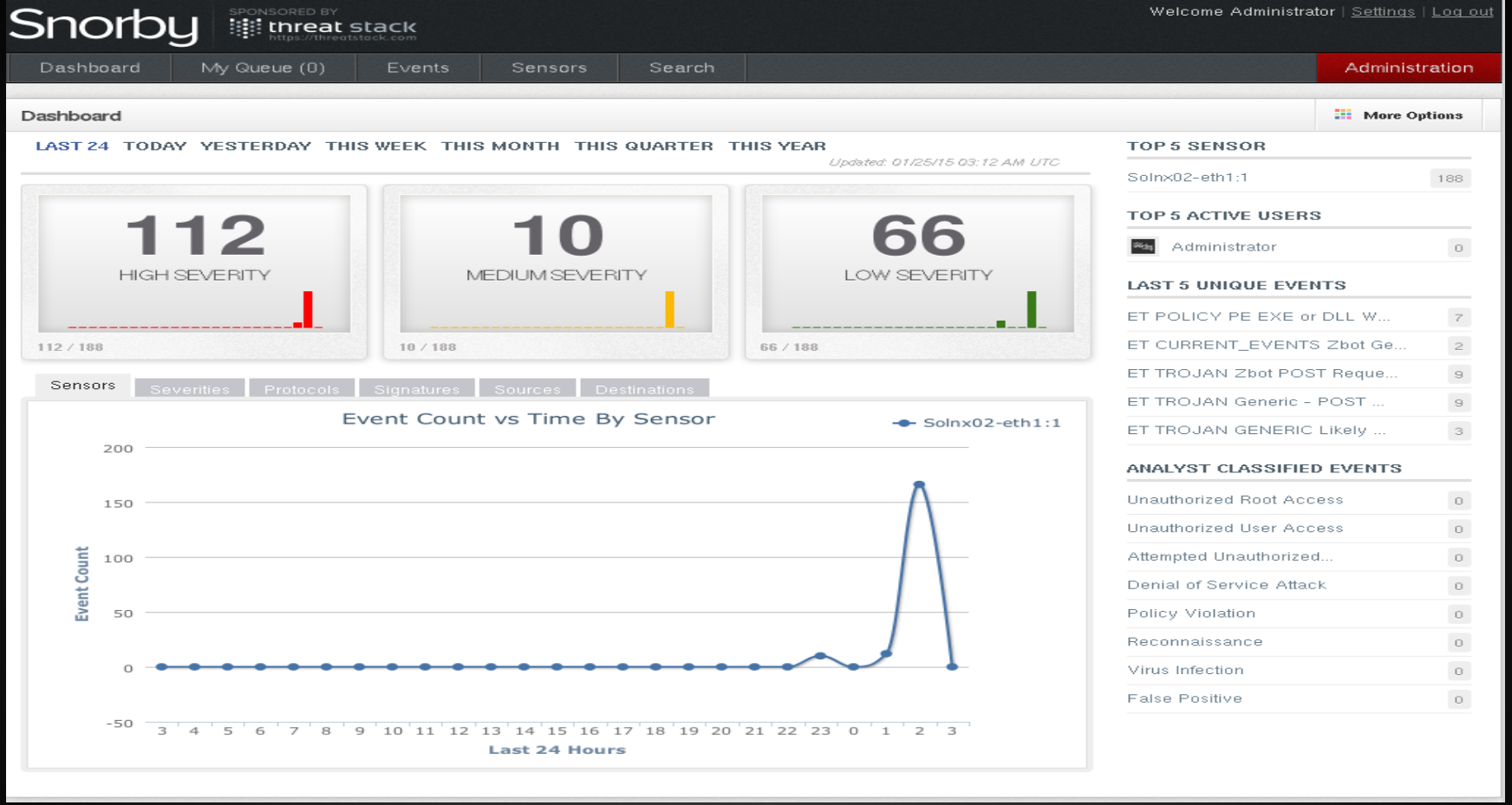
- Web front-end for Sguil database
- Adds additional features like visualizations and supporting information to events



squert main screen

Snorby

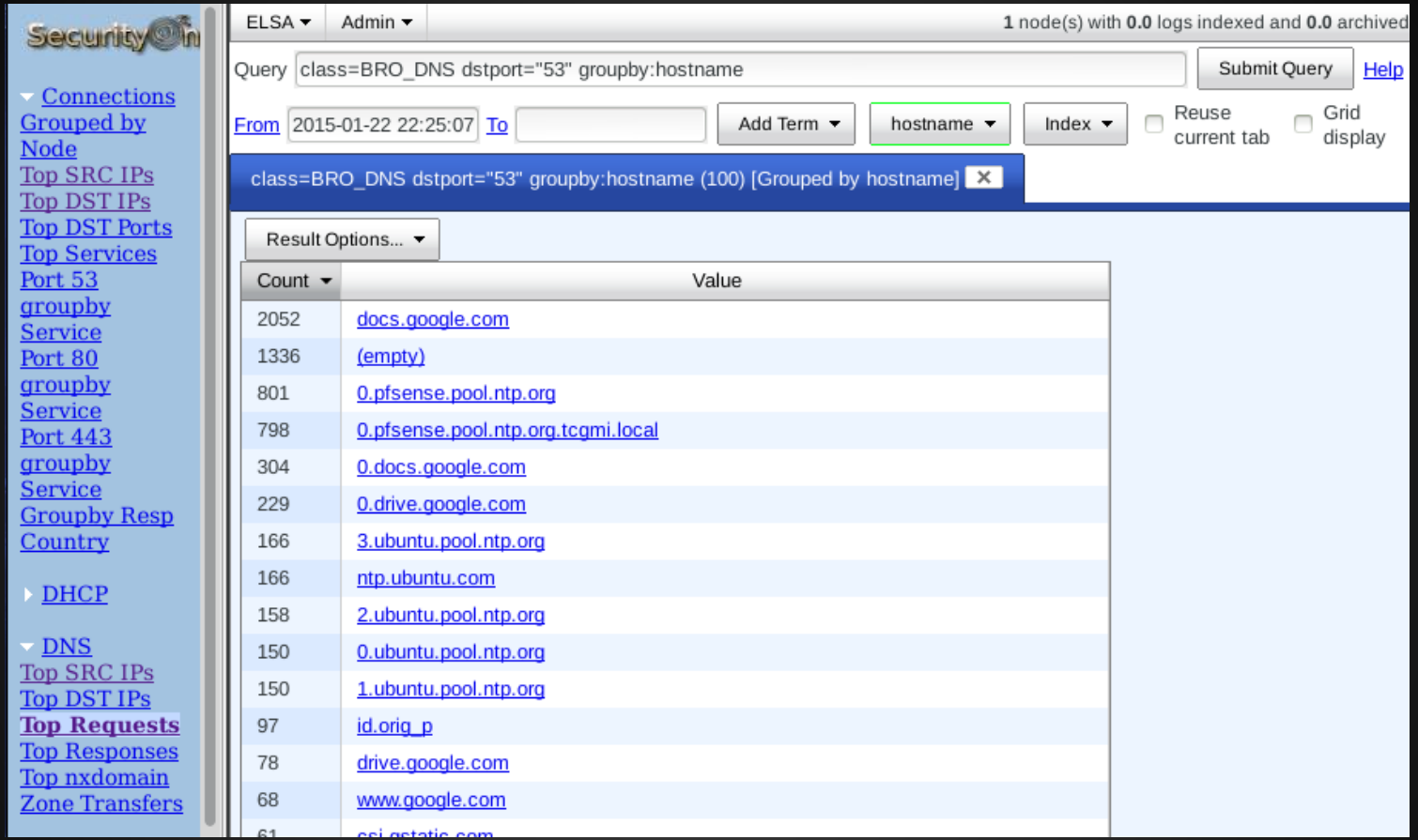
- Web front-end mostly for IDS data (snort)
- Allows for transcript creation
- Allows for classification of data
- Allows for pulling of full packet captures



snorby main screen

ELSA

- Web frontend for logs, includes bro logs
- Uses syslog-ng to collect remote events
- Uses mysql to store and query events
- If installed, then just double-click on the link
- Rapidly becoming one of my favorites
  - https://<host or IP>:3154
  - Accept SSL cert
- SO side panel has some pre-built queries



Elsa SO interface

Getting pcap data into SO

- Using tcpreplay
  - sudo tcpreplay -i eth1 -t example.pcap
- Allows you to run pcap files through all of the live action tools in SO.
- Only catch is, the timestamps on the packets are now system time.

Live Action of SO

Questions

http://blog.securityonion.net/p/securityonion.html