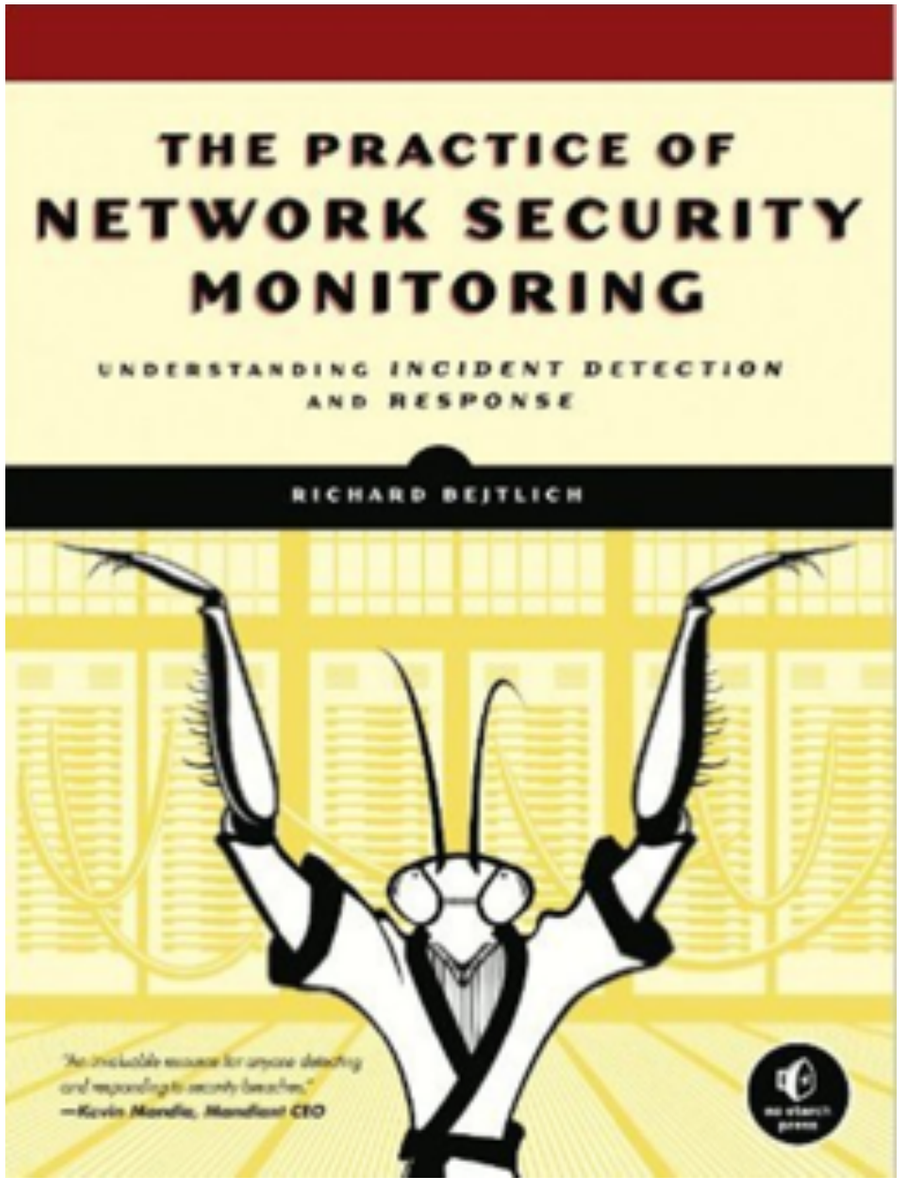
CNIT 50:
Network Security Monitoring

7 Graphical Packet Analysis Tools



Topics

- **Using Wireshark**
- **Using Xplico**
- **Examining Content with NetworkMiner**

Wireshark

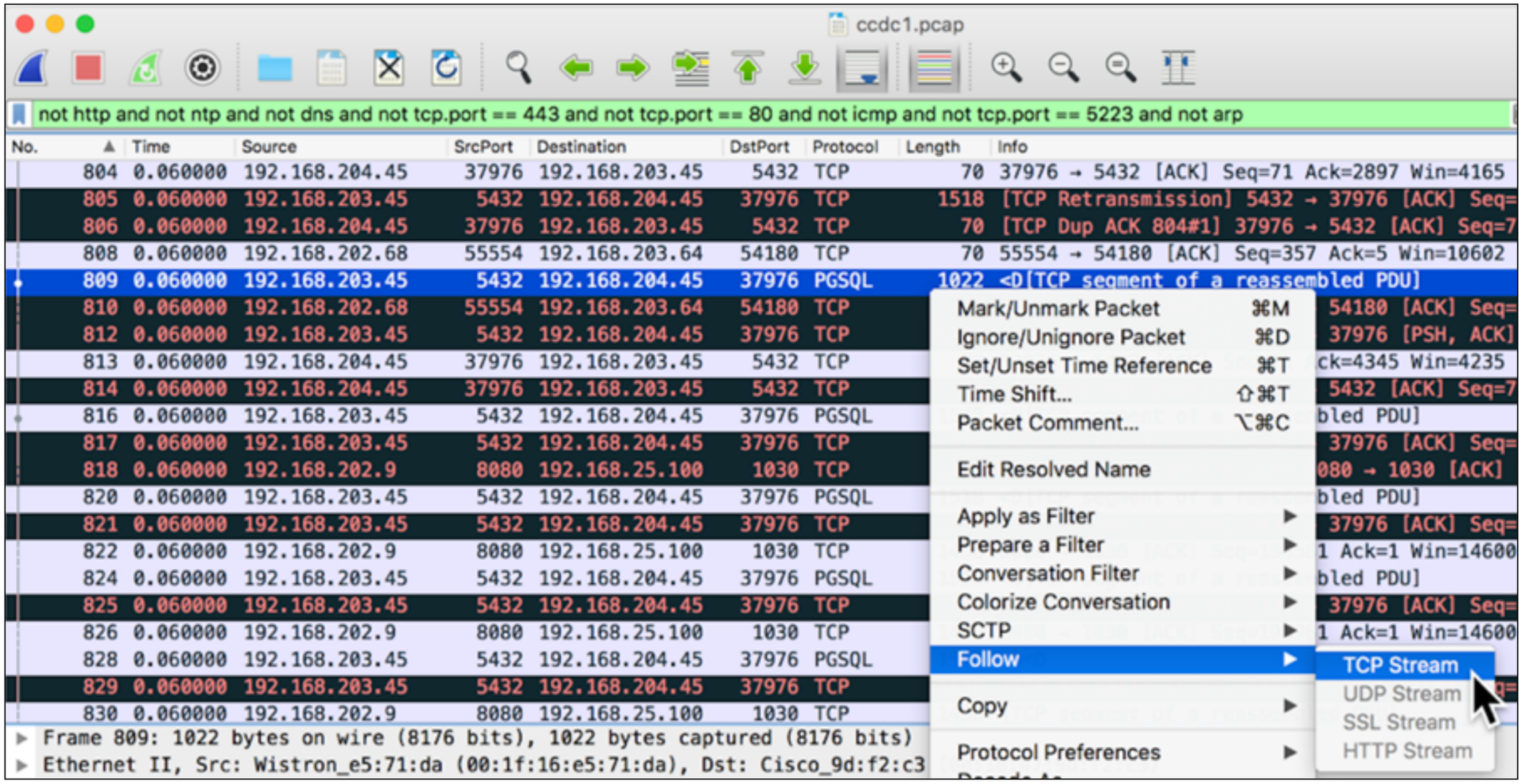
Wireshark Limitations

- Slow for processing large data sets
- Best to first locate traffic of interest with another tool such as session data
- And use Wireshark on that limited data

Useful Wireshark Features

- Viewing lower-level Protocol Features in Detail
- Omitting Traffic to See Remnants
- Following Streams
- Setting the Protocol Decode Method with Decode As
- Following Other Streams

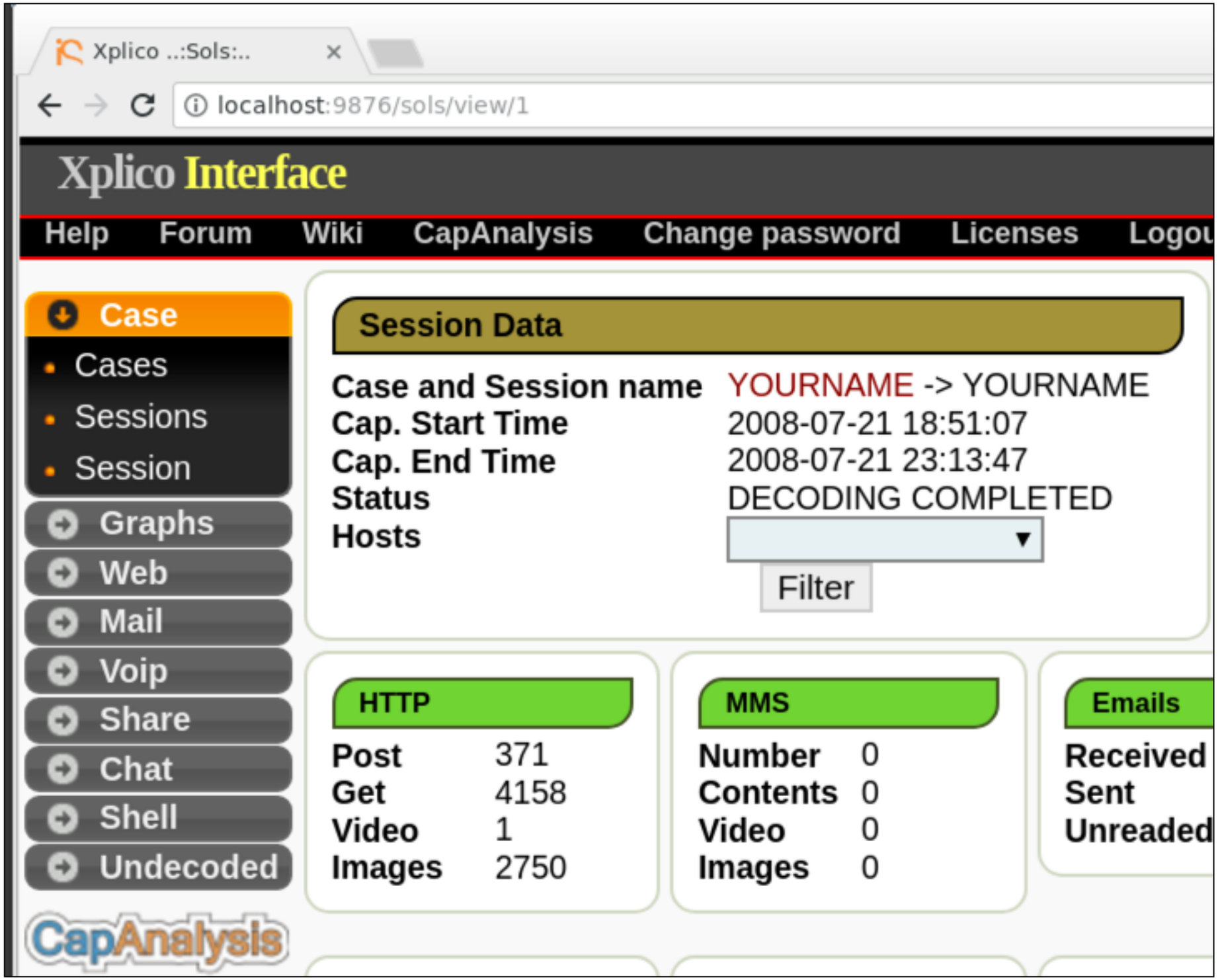
Project 2


ccdc1.pcap
not http and not ntp and not dns and not tcp.port == 443 and not tcp.port == 80 and not icmp and not tcp.port == 5223 and not arp
No. Time Source SrcPort Destination DstPort Protocol Length Info
804 0.060000 192.168.204.45 37976 192.168.203.45 5432 TCP 70 37976 → 5432 [ACK] Seq=71 Ack=2897 Win=4165
805 0.060000 192.168.203.45 5432 192.168.204.45 37976 TCP 1518 [TCP Retransmission] 5432 → 37976 [ACK] Seq=
806 0.060000 192.168.204.45 37976 192.168.203.45 5432 TCP 70 [TCP Dup ACK 804#1] 37976 → 5432 [ACK] Seq=7
808 0.060000 192.168.202.68 55554 192.168.203.64 54180 TCP 70 55554 → 54180 [ACK] Seq=357 Ack=5 Win=10602
809 0.060000 192.168.203.45 5432 192.168.204.45 37976 PGSQL 1022 <D[TCP segment of a reassembled PDU]
810 0.060000 192.168.202.68 55554 192.168.203.64 54180 TCP
812 0.060000 192.168.203.45 5432 192.168.204.45 37976 TCP
813 0.060000 192.168.204.45 37976 192.168.203.45 5432 TCP
814 0.060000 192.168.204.45 37976 192.168.203.45 5432 TCP
816 0.060000 192.168.203.45 5432 192.168.204.45 37976 PGSQL
817 0.060000 192.168.203.45 5432 192.168.204.45 37976 TCP
818 0.060000 192.168.202.9 8080 192.168.25.100 1030 TCP
820 0.060000 192.168.203.45 5432 192.168.204.45 37976 PGSQL
821 0.060000 192.168.203.45 5432 192.168.204.45 37976 TCP
822 0.060000 192.168.202.9 8080 192.168.25.100 1030 TCP
824 0.060000 192.168.203.45 5432 192.168.204.45 37976 PGSQL
825 0.060000 192.168.203.45 5432 192.168.204.45 37976 TCP
826 0.060000 192.168.202.9 8080 192.168.25.100 1030 TCP
828 0.060000 192.168.203.45 5432 192.168.204.45 37976 PGSQL
829 0.060000 192.168.203.45 5432 192.168.204.45 37976 TCP
830 0.060000 192.168.202.9 8080 192.168.25.100 1030 TCP
Frame 809: 1022 bytes on wire (8176 bits), 1022 bytes captured (8176 bits)
Ethernet II, Src: Wistron_e5:71:da (00:1f:16:e5:71:da), Dst: Cisco_9d:f2:c3
Mark/Unmark Packet ⌘M
Ignore/Unignore Packet ⌘D
Set/Unset Time Reference ⌘T
Time Shift... ⇧⌘T
Packet Comment... ⌥⌘C
Edit Resolved Name
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
TCP Stream
UDP Stream
SSL Stream
HTTP Stream

Xplico

Using Xplico

- Not intended for live capture, although that is possible
- Better for analyzing saved PCAPs
- Managed via a Web browser
  - By default, SO only allows access from localhost


Xplico ..:Sols:..
localhost:9876/sols/view/1
Xplico Interface
Help
Forum
Wiki
CapAnalysis
Change password
Licenses
Logou
Case
Cases
Sessions
Session
Graphs
Web
Mail
Voip
Share
Chat
Shell
Undecoded
CapAnalysis
Session Data
Case and Session name YOURNAME -> YOURNAME
Cap. Start Time 2008-07-21 18:51:07
Cap. End Time 2008-07-21 23:13:47
Status DECODING COMPLETED
Hosts
Filter
HTTP
Post 371
Get 4158
Video 1
Images 2750
MMS
Number 0
Contents 0
Video 0
Images 0
Emails
Received
Sent
Unreaded

Xplico ..:Webs:...

localhost:9876/webs/index

Xplico Interface

User: xplico

Help Forum Wiki CapAnalysis Change password Licenses Logout

- Case
- Graphs
- Web
  - Site
  - Feed
  - Images
- Mail
- Voip
- Share
- Chat

For a complete view of html page set your browser to use Proxy, and point it to Web server.

Web URLs: Html Image Flash Video Audio JSON All

Search: Go

Date	Url	Size	Method	Info
2008-07-21 23:11:34	www.google.com/firefox?client=firefox-a&rls=org.mozilla:en-U	2756	GET	info.xml
2008-07-21 23:11:32	en-us.start2.mozilla.com/firefox?client=firefox-a&rls=org.mozil	278	GET	info.xml
2008-07-21 23:11:32	track.sellathon.com/track2.php?S10=230272271621&S01=1216	493	GET	info.xml

Xplico ..:Webs:..

localhost:9876/webs

Xplico Interface

User: xplico

Help Forum Wiki CapAnalysis Change password Licenses Logout

- Case
- Graphs
- Web
  - Site
  - Feed
  - Images
- Mail
- Voip
- Share
- Chat

For a complete view of html page set your browser to use Proxy, and point it to Web server.

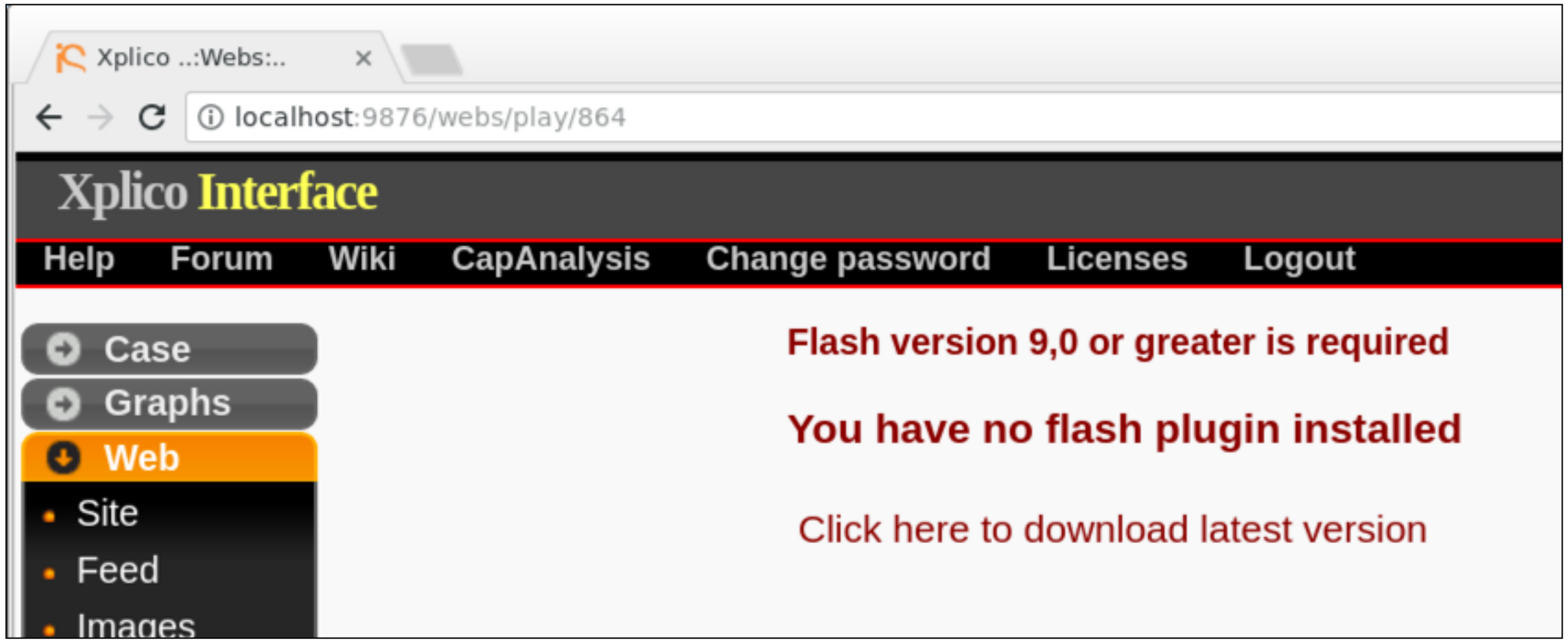
Web URLs: Html Image Flash Video Audio JSON All

Search: Go

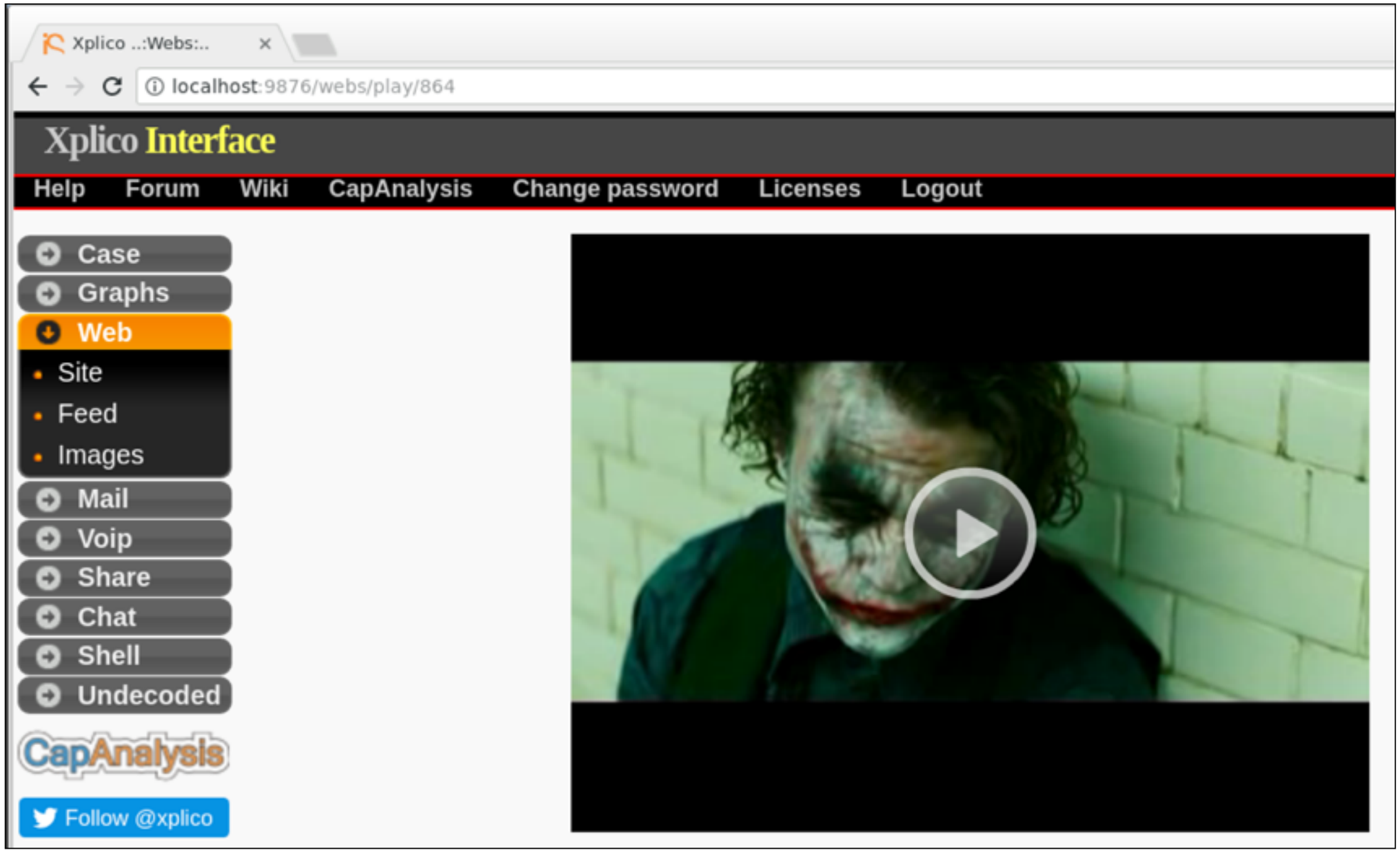
Date	Url	Size	Method	Info
2008-07-21 21:47:30	v6.cache.googlevideo.com/get_video?video_id=WaIR9dAZRR0&	4632715	GET	info.xml

Previous 1 of 1 Next

Flash Often Fails



Reconstructed from Packets



Xplico ..:Webs:..

localhost:9876/webs/images/page:2

Xplico Interface

Help | Forum | Wiki | CapAnalysis | Change password | Licenses | Logou

- Case
- Graphs
- Web
  - Site
  - Feed
  - Images
- Mail
- Voip
- Share
- Chat
- Shell
- Undecoded

CapAnalysis

Follow @xplico

Search:

pics.ebaystatic.com Image or Page	pics.ebaystatic.com Image or Page
pics.ebaystatic.com Image or Page	pics.ebaystatic.com Image or Page
thumbs3.ebaystatic.com Image or Page	thumbs3.ebaystatic.com Image or Page

Previous

1 | 2 | 3 | 4 |

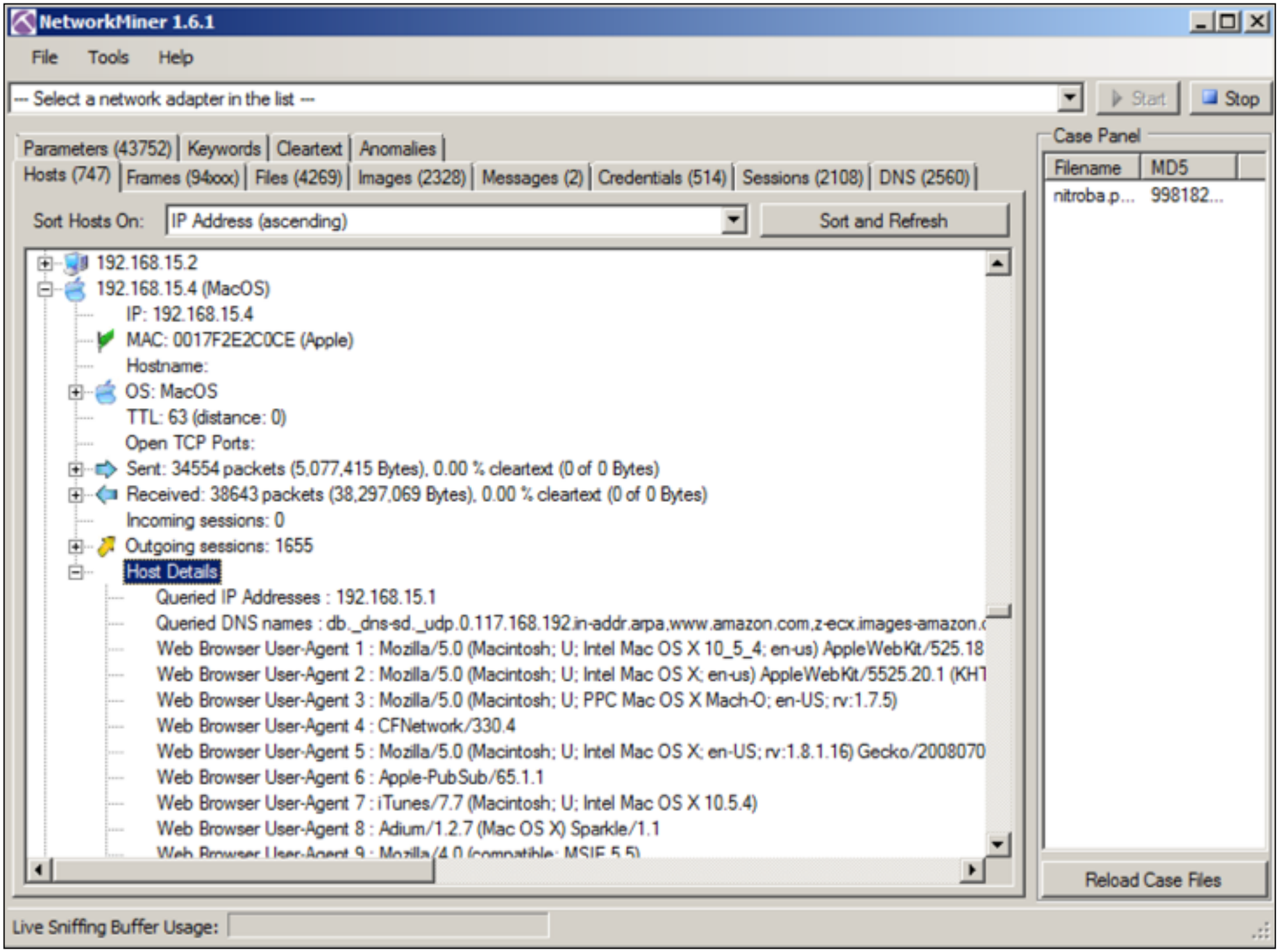
NetworkMiner

Windows Only!

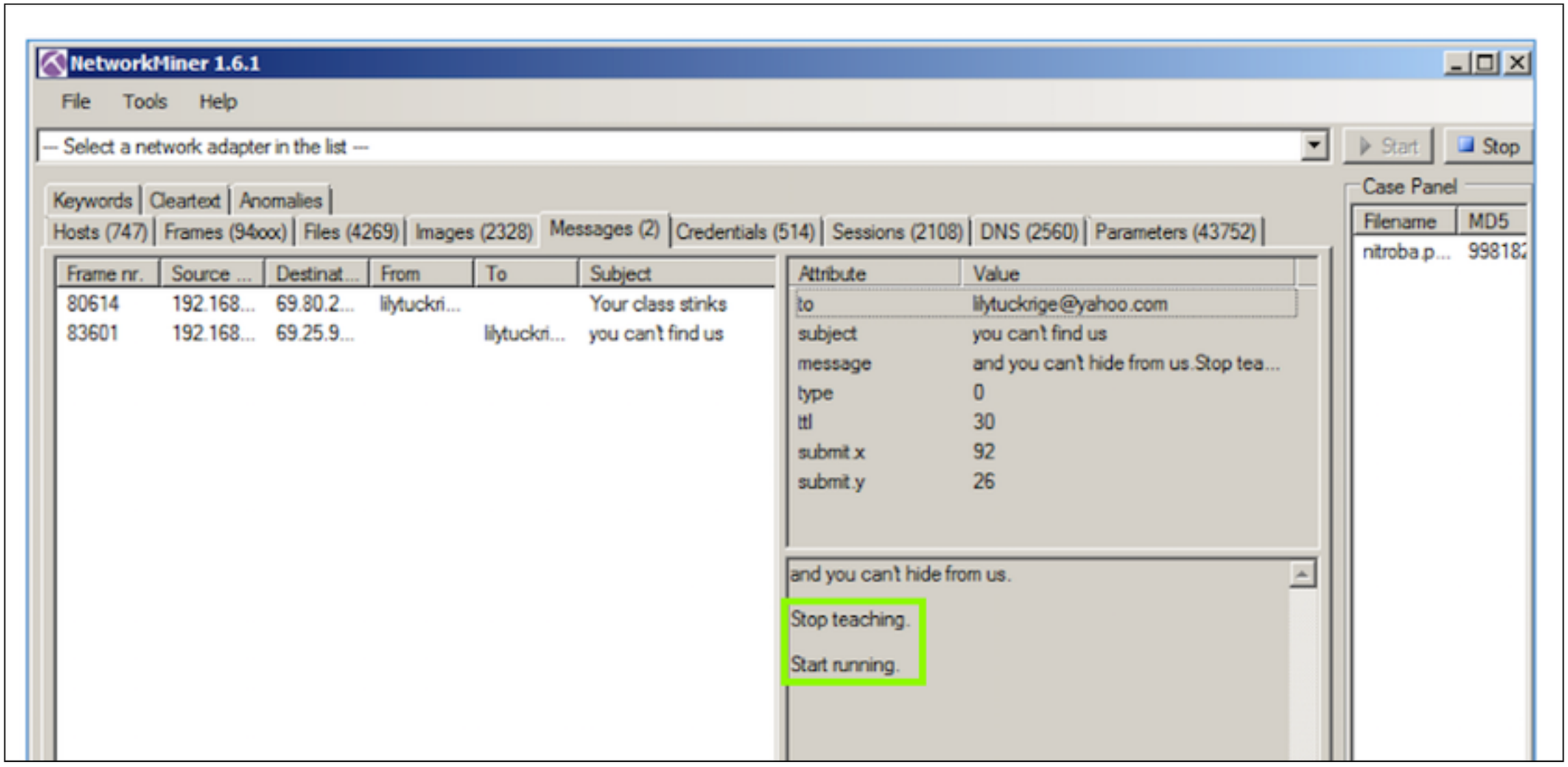
- On Linux: takes more than two hours to load the **nitroba.pcap** file, which is only 55 MB

- On Windows: < 5 min.

Hosts

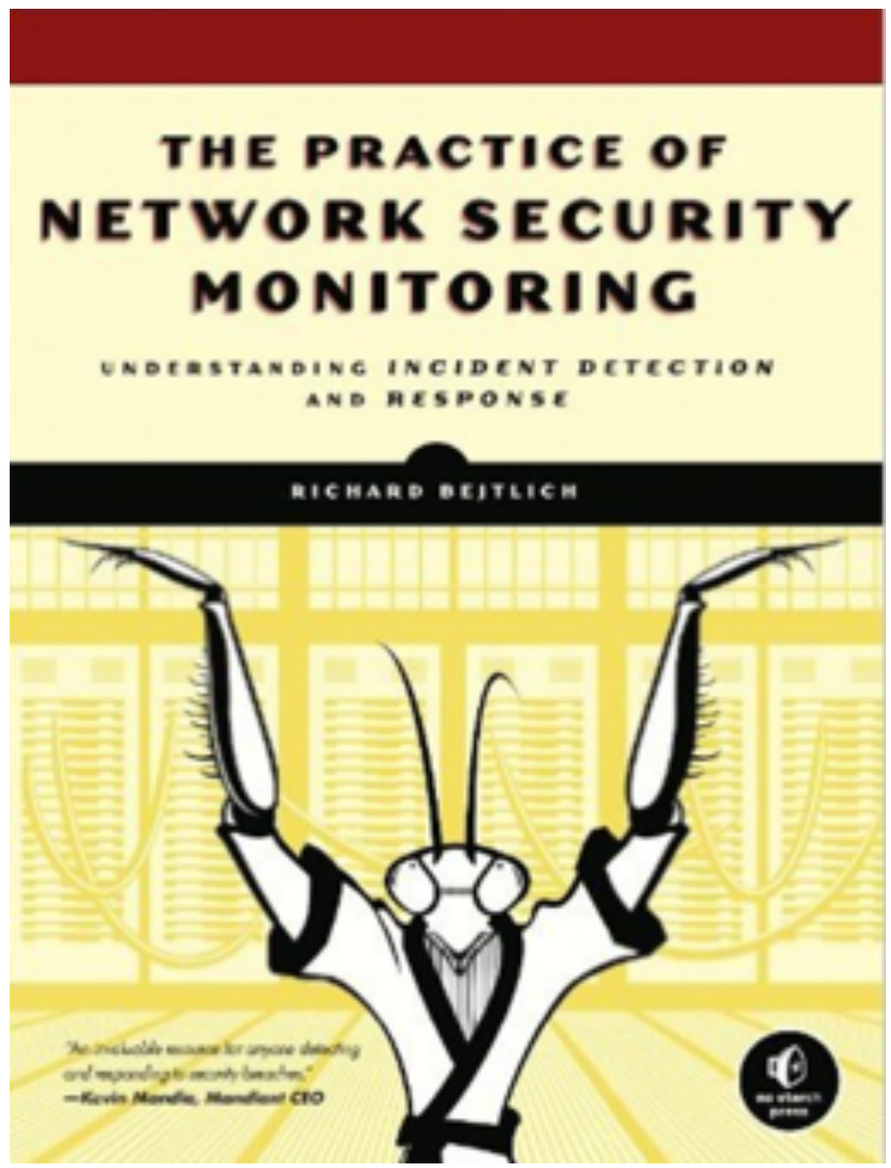

NetworkMiner 1.6.1
File
Tools
Help
--- Select a network adapter in the list ---
Start
Stop
Case Panel
Filename
MD5
nitroba.p...
998182...
Parameters (43752)
Keywords
Cleartext
Anomalies
Hosts (747)
Frames (94xxx)
Files (4269)
Images (2328)
Messages (2)
Credentials (514)
Sessions (2108)
DNS (2560)
Sort Hosts On:
IP Address (ascending)
Sort and Refresh
192.168.15.2
192.168.15.4 (MacOS)
IP: 192.168.15.4
MAC: 0017F2E2C0CE (Apple)
Hostname:
OS: MacOS
TTL: 63 (distance: 0)
Open TCP Ports:
Sent: 34554 packets (5,077,415 Bytes), 0.00 % cleartext (0 of 0 Bytes)
Received: 38643 packets (38,297,069 Bytes), 0.00 % cleartext (0 of 0 Bytes)
Incoming sessions: 0
Outgoing sessions: 1655
Host Details
Queried IP Addresses : 192.168.15.1
Queried DNS names : db._dns-sd._udp.0.117.168.192.in-addr.arpa,www.amazon.com,z-ecx.images-amazon.c
Web Browser User-Agent 1 : Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_5_4; en-us) AppleWebKit/525.18
Web Browser User-Agent 2 : Mozilla/5.0 (Macintosh; U; Intel Mac OS X; en-us) AppleWebKit/5525.20.1 (KHT
Web Browser User-Agent 3 : Mozilla/5.0 (Macintosh; U; PPC Mac OS X Mach-O; en-US; rv:1.7.5)
Web Browser User-Agent 4 : CFNetwork/330.4
Web Browser User-Agent 5 : Mozilla/5.0 (Macintosh; U; Intel Mac OS X; en-US; rv:1.8.1.16) Gecko/2008070
Web Browser User-Agent 6 : Apple-PubSub/65.1.1
Web Browser User-Agent 7 : iTunes/7.7 (Macintosh; U; Intel Mac OS X 10.5.4)
Web Browser User-Agent 8 : Adium/1.2.7 (Mac OS X) Sparkle/1.1
Reload Case Files
Live Sniffing Buffer Usage:

Messages


NetworkMiner 1.6.1
File
Tools
Help
-- Select a network adapter in the list --
Start
Stop
Case Panel
Filename
MD5
nitroba.p...
Keywords
Cleartext
Anomalies
Hosts (747)
Frames (94xxx)
Files (4269)
Images (2328)
Messages (2)
Credentials (514)
Sessions (2108)
DNS (2560)
Parameters (43752)
Frame nr.
Source ...
Destinat...
From
To
Subject
80614
192.168...
69.80.2...
lilytuckri...
Your class stinks
83601
192.168...
69.25.9...
lilytuckri...
you can't find us
Attribute
Value
to
lilytuckrige@yahoo.com
subject
you can't find us
message
and you can't hide from us.Stop tea...
type
0
ttl
30
submit.x
92
submit.y
26
and you can't hide from us.
Stop teaching.
Start running.

CNIT 50:
Network Security Monitoring

8 NSM Consoles



Topics

- **An NSM-centric Look at Network Traffic**
- **Using Sguil**
- **Using Squert**
- **Using Snorby (Removed from SO)**
- **Using ELSA**

Sguil

Sguil's Six Key Functions

Sguil enables six key functions helpful to NSM analysts:

- Sguil performs simple aggregation of similar alert data records.
- Sguil makes certain types of metadata, and related data, readily available.
- Sguil allows queries and review of alert data.
- Sguil permits queries and review of session data.
- Sguil provides a right-click menu that lets you pivot, or move from either of those two categories of data to full content data, rendered as text in a *transcript*, in a protocol analyzer like Wireshark, or in a network forensic tool like NM.
- Sguil exposes features so analysts can count and classify events, thereby enabling escalation and other incident response decisions.

Events

SGUIL-0.9.0 - Connected To localhost

File Query Reports Sound: Off ServerName: localhost UserName: sguil UserID: 2 2017-10-30 19:13:46 GMT

RealTime Events | Escalated Events

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	60	so-virtual...	3.477	2017-10-09 19:39:11	95.211.224.12	123	172.16.1.196	123	17	ET TOR Known Tor Relay/Router (Not Exit) Node UDP Traf...
RT	11	so-virtual...	3.543	2017-10-10 00:45:02	172.16.1.195		172.16.1.1		1	GPL ICMP_INFO PING *NIX
RT	2	so-virtual...	3.565	2017-10-30 19:12:42	172.16.1.1	43723	172.16.1.196	3306	6	ET POLICY Suspicious inbound to mySQL port 3306
RT	1	so-virtual...	3.567	2017-10-30 19:12:42	172.16.1.1	43723	172.16.1.196	5906	6	ET SCAN Potential VNC Scan 5900-5920
RT	2	so-virtual...	3.568	2017-10-30 19:12:43	172.16.1.1	43723	172.16.1.196	5432	6	ET POLICY Suspicious inbound to PostgreSQL port 5432
RT	1	so-virtual...	3.570	2017-10-30 19:12:43	172.16.1.1	43723	172.16.1.196	5801	6	ET SCAN Potential VNC Scan 5800-5820
RT	2	so-virtual...	3.571	2017-10-30 19:12:44	172.16.1.1	43723	172.16.1.196	1433	6	ET POLICY Suspicious inbound to MSSQL port 1433
RT	2	so-virtual...	3.572	2017-10-30 19:12:44	172.16.1.1	43723	172.16.1.196	1521	6	ET POLICY Suspicious inbound to Oracle SQL port 1521
RT	1	so-virtual...	1.363	2017-10-31 02:12:46	172.16.1.1		0.0.0.0			[OSSEC] SSH insecure connection attempt (scan).
RT	14	so-virtual...	3.575	2017-10-30 19:13:01	172.16.1.1	45878	172.16.1.196	22	6	ET SCAN Potential SSH Scan OUTBOUND
RT	1	so-virtual...	3.576	2017-10-30 19:13:01	172.16.1.1	45878	172.16.1.196	22	6	ET SCAN Potential SSH Scan
RT	4	so-virtual...	3.578	2017-10-30 19:13:02	172.16.1.1	45900	172.16.1.196	32004	17	GPL SHELLCODE x86 inc ebx NOOP
RT	4	so-virtual...	3.579	2017-10-30 19:13:02	172.16.1.1	45900	172.16.1.196	32004	17	ET SCAN NMAP OS Detection Probe

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

Reverse DNS Enable External DNS

Src IP: 172.16.1.1
Src Name: Unknown
Dst IP: 172.16.1.196
Dst Name: Unknown

Whois Query: None Src IP Dst IP

Show Packet Data Show Rule

alert tcp $EXTERNAL_NET any -> $HOME_NET 5900:5920 (msg:"ET SCAN Potential VNC Scan 5900-5920"; flags:S,12; threshold: type both, track by_src, count 5, seconds 60; reference:url,doc.emergingthreats.net/2002911;

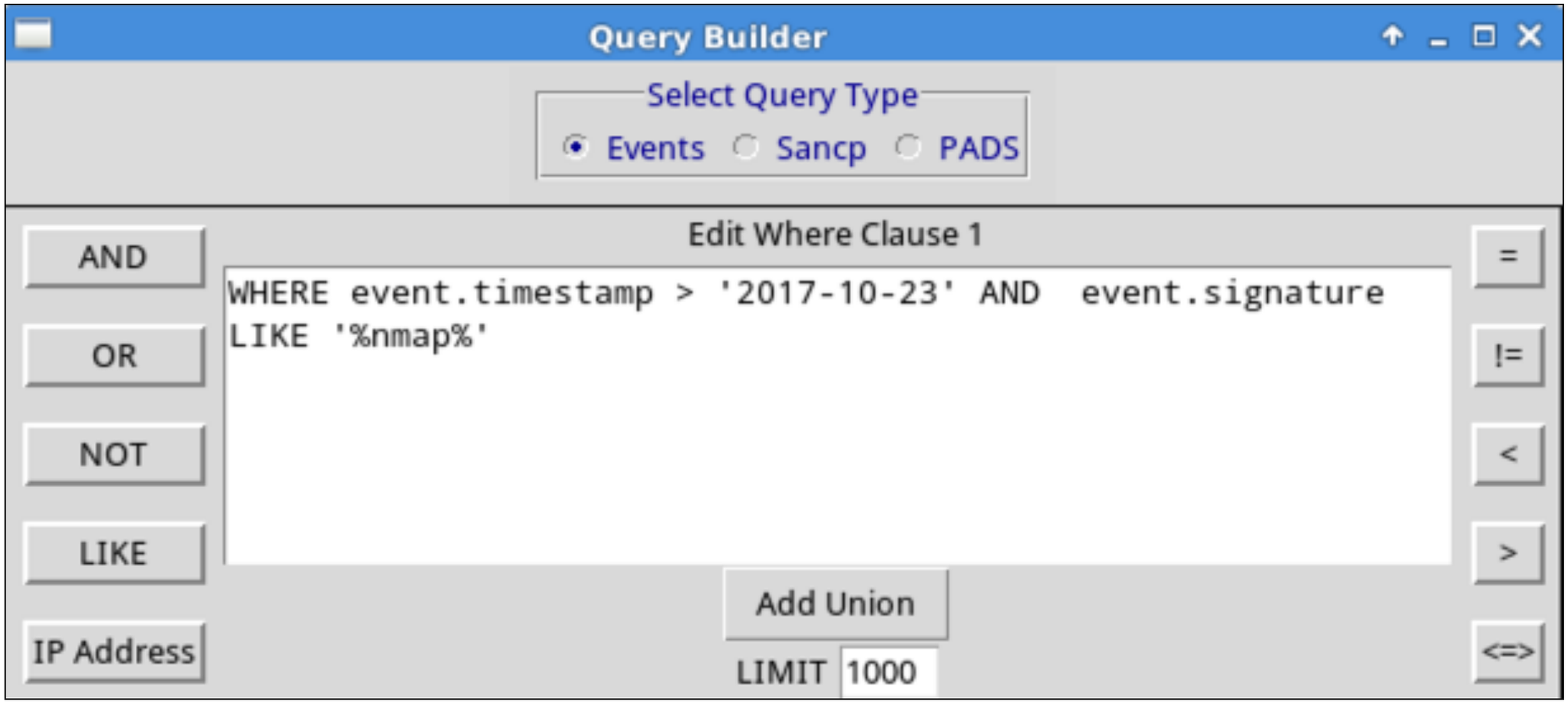
	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
IP	172.16.1.1	172.16.1.196	4	5	0	44	16503	0	0	53	60015

	Source Port	Dest Port	R 1	R 0	URG	ACK	PSH	RST	SYN	FIN	Seq #	Ack #	Offset	Res	Window	Urp	ChkSum
TCP	43723	5906	.	.	.	.	.	.	X	.	776718384	0	6	0	1024	0	32999

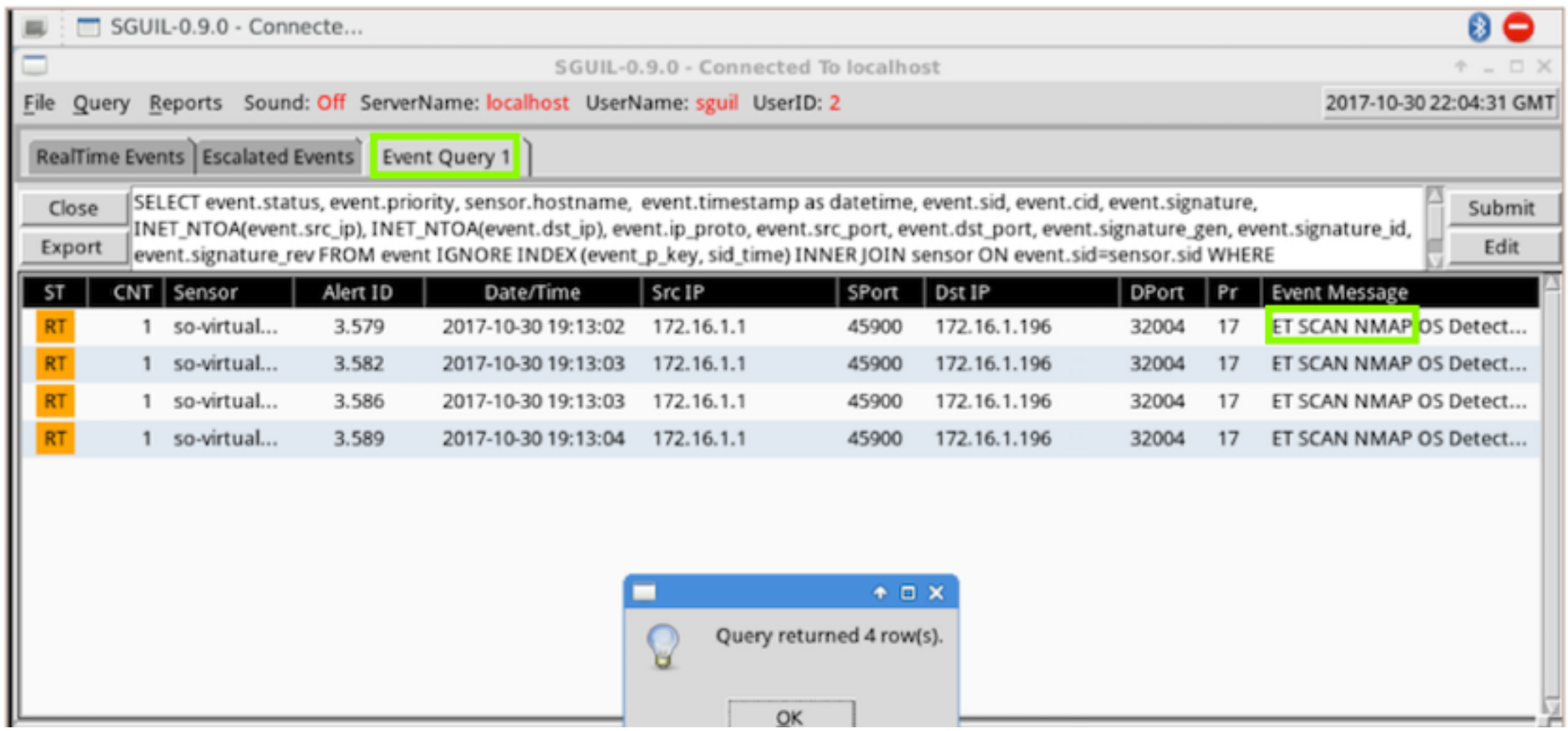
DATA: None . | None .

Search Packet Payload Hex Text NoCase

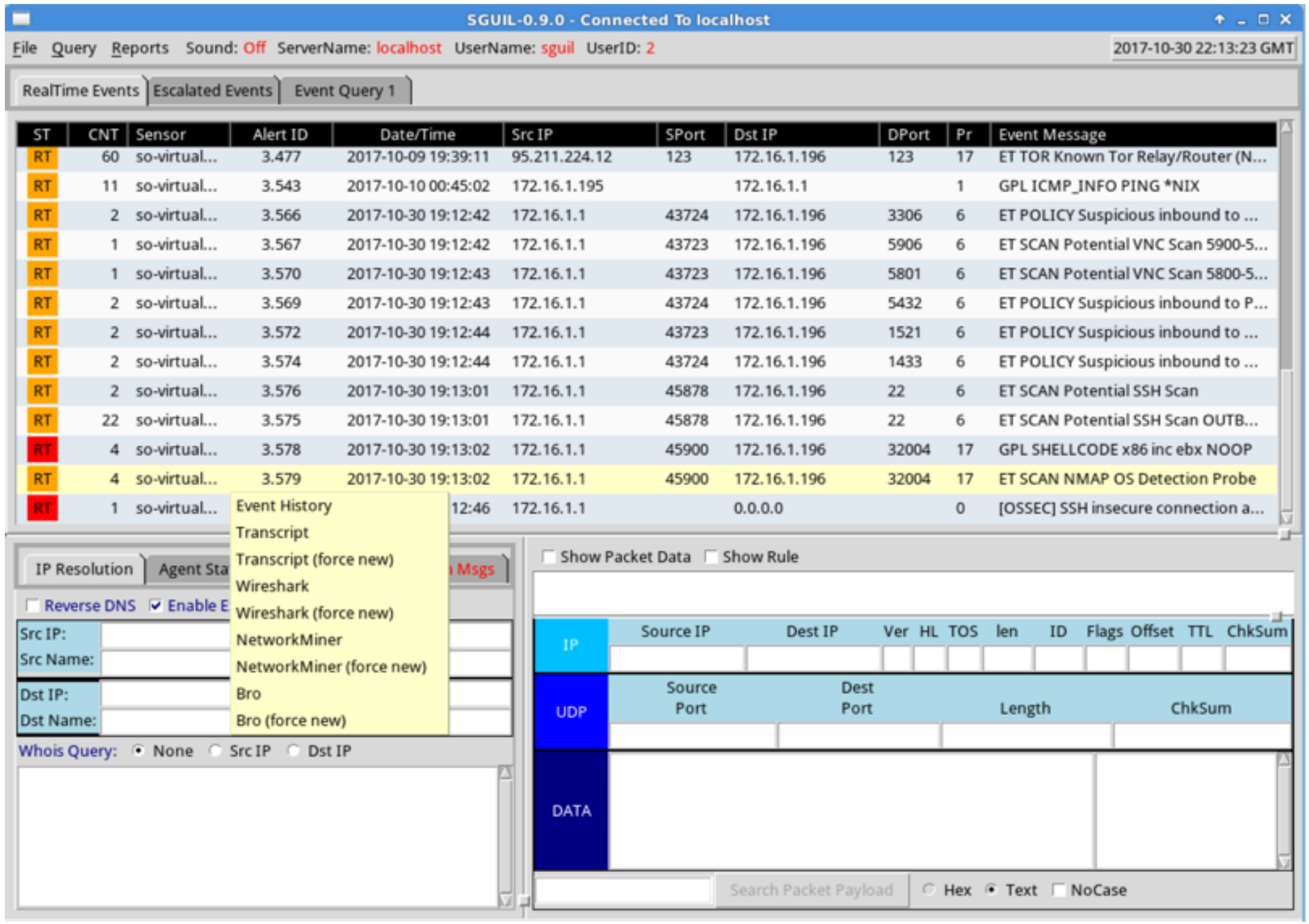
Query


Query Builder
Select Query Type
Events
Sancp
PADS
Edit Where Clause 1
AND
OR
NOT
LIKE
IP Address
WHERE event.timestamp > '2017-10-23' AND event.signature
LIKE '%nmap%'
=
!=
<
>
<=>
Add Union
LIMIT
1000

Like Splunk


SGUIL-0.9.0 - Connecte...
SGUIL-0.9.0 - Connected To localhost
File Query Reports Sound: Off ServerName: localhost UserName: sguil UserID: 2
2017-10-30 22:04:31 GMT
RealTime Events
Escalated Events
Event Query 1
Close
Export
SELECT event.status, event.priority, sensor.hostname, event.timestamp as datetime, event.sid, event.cid, event.signature, INET_NTOA(event.src_ip), INET_NTOA(event.dst_ip), event.ip_proto, event.src_port, event.dst_port, event.signature_gen, event.signature_id, event.signature_rev FROM event IGNORE INDEX (event_p_key, sid_time) INNER JOIN sensor ON event.sid=sensor.sid WHERE
Submit
Edit
ST CNT Sensor Alert ID Date/Time Src IP SPort Dst IP DPort Pr Event Message
RT 1 so-virtual... 3.579 2017-10-30 19:13:02 172.16.1.1 45900 172.16.1.196 32004 17 ET SCAN NMAP OS Detect...
RT 1 so-virtual... 3.582 2017-10-30 19:13:03 172.16.1.1 45900 172.16.1.196 32004 17 ET SCAN NMAP OS Detect...
RT 1 so-virtual... 3.586 2017-10-30 19:13:03 172.16.1.1 45900 172.16.1.196 32004 17 ET SCAN NMAP OS Detect...
RT 1 so-virtual... 3.589 2017-10-30 19:13:04 172.16.1.1 45900 172.16.1.196 32004 17 ET SCAN NMAP OS Detect...
Query returned 4 row(s).
OK

Pivot to Full Content Data

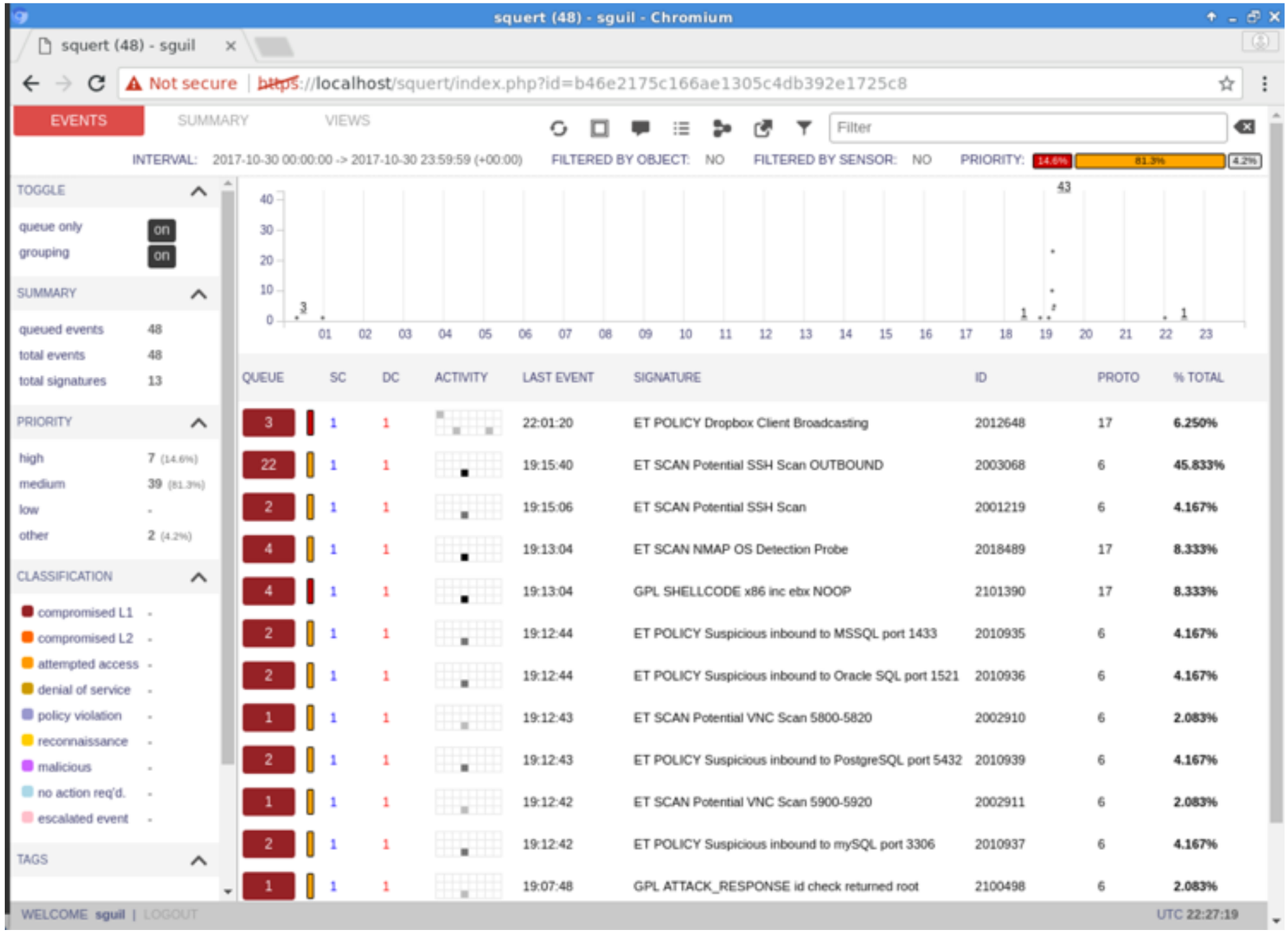


Squert

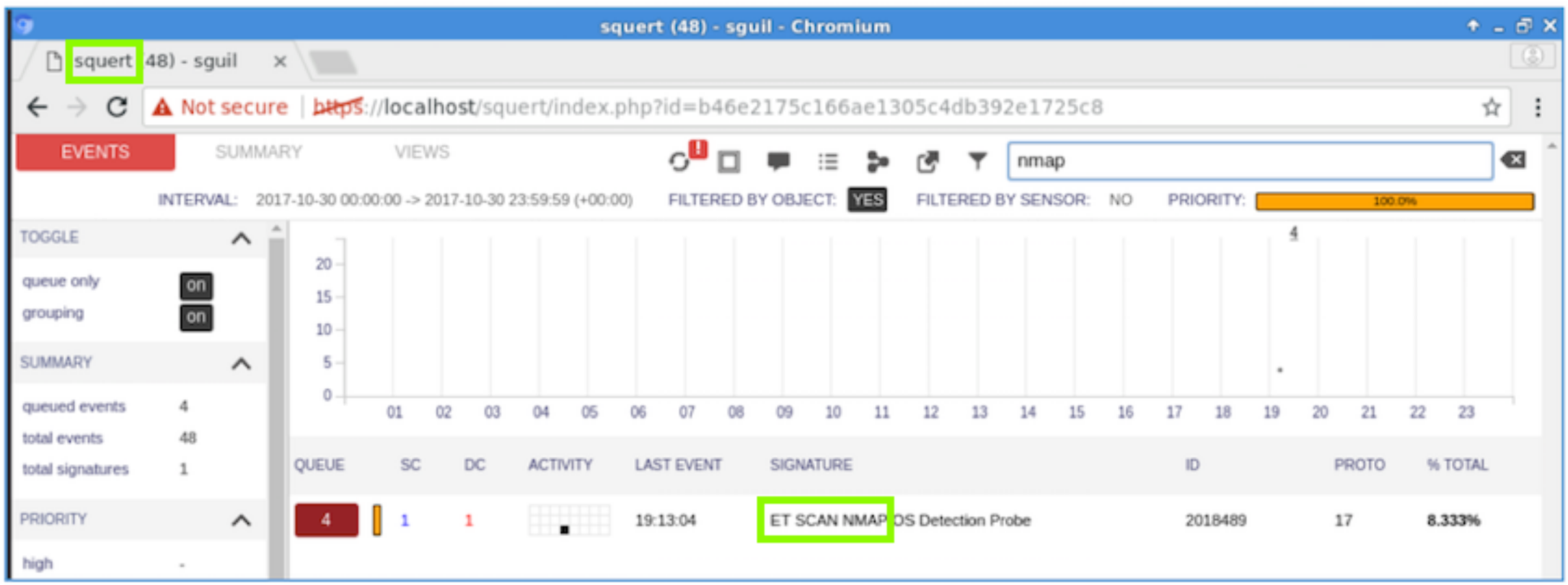
Squert

- Open-source web interface for NSM data
- Written to provide access to Sguil databases via a Web browser
- Adds visualizations and supporting information

Events


squert (48) - sguil - Chromium
squert (48) - sguil
Not secure
https://localhost/squert/index.php?id=b46e2175c166ae1305c4db392e1725c8
EVENTS
SUMMARY
VIEWS
Filter
INTERVAL: 2017-10-30 00:00:00 -> 2017-10-30 23:59:59 (+00:00)
FILTERED BY OBJECT: NO
FILTERED BY SENSOR: NO
PRIORITY:
TOGGLE
queue only on
grouping on
SUMMARY
queued events 48
total events 48
total signatures 13
PRIORITY
high 7 (14.6%)
medium 39 (81.3%)
low -
other 2 (4.2%)
CLASSIFICATION
compromised L1 -
compromised L2 -
attempted access -
denial of service -
policy violation -
reconnaissance -
malicious -
no action req'd. -
escalated event -
TAGS
QUEUE SC DC ACTIVITY LAST EVENT SIGNATURE ID PROTO % TOTAL
3 1 1 22:01:20 ET POLICY Dropbox Client Broadcasting 2012648 17 6.250%
22 1 1 19:15:40 ET SCAN Potential SSH Scan OUTBOUND 2003068 6 45.833%
2 1 1 19:15:06 ET SCAN Potential SSH Scan 2001219 6 4.167%
4 1 1 19:13:04 ET SCAN NMAP OS Detection Probe 2018489 17 8.333%
4 1 1 19:13:04 GPL SHELLCODE x86 inc ebx NOOP 2101390 17 8.333%
2 1 1 19:12:44 ET POLICY Suspicious inbound to MSSQL port 1433 2010935 6 4.167%
2 1 1 19:12:44 ET POLICY Suspicious inbound to Oracle SQL port 1521 2010936 6 4.167%
1 1 1 19:12:43 ET SCAN Potential VNC Scan 5800-5820 2002910 6 2.083%
2 1 1 19:12:43 ET POLICY Suspicious inbound to PostgreSQL port 5432 2010939 6 4.167%
1 1 1 19:12:42 ET SCAN Potential VNC Scan 5900-5920 2002911 6 2.083%
2 1 1 19:12:42 ET POLICY Suspicious inbound to mySQL port 3306 2010937 6 4.167%
1 1 1 19:07:48 GPL ATTACK_RESPONSE id check returned root 2100498 6 2.083%
WELCOME sguil | LOGOUT
UTC 22:27:19

Search


squert (48) - sguil - Chromium
squert (48) - sguil
Not secure
https://localhost/squert/index.php?id=b46e2175c166ae1305c4db392e1725c8
EVENTS
SUMMARY
VIEWS
nmap
INTERVAL: 2017-10-30 00:00:00 -> 2017-10-30 23:59:59 (+00:00)
FILTERED BY OBJECT: YES
FILTERED BY SENSOR: NO
PRIORITY:
100.0%
TOGGLE
queue only on
grouping on
SUMMARY
queued events 4
total events 48
total signatures 1
PRIORITY
high -
QUEUE
SC
DC
ACTIVITY
LAST EVENT
SIGNATURE
ID
PROTO
% TOTAL
4
1
1
19:13:04
ET SCAN NMAP OS Detection Probe
2018489
17
8.333%

Snorby

Removed from SO

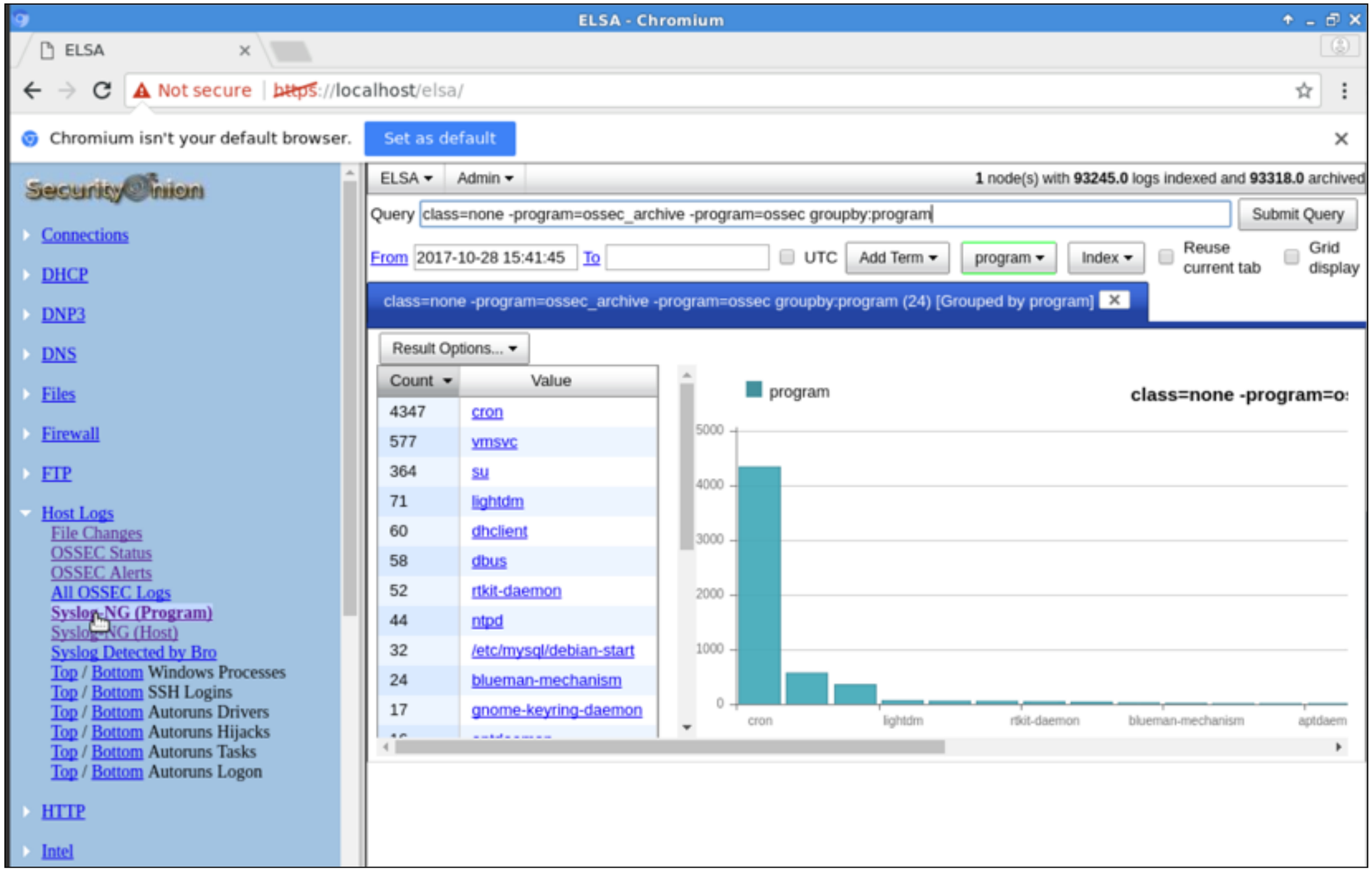
- Newer open-source Web interface for NSM data
- Abandoned by its developers and removed from SO

ELSA

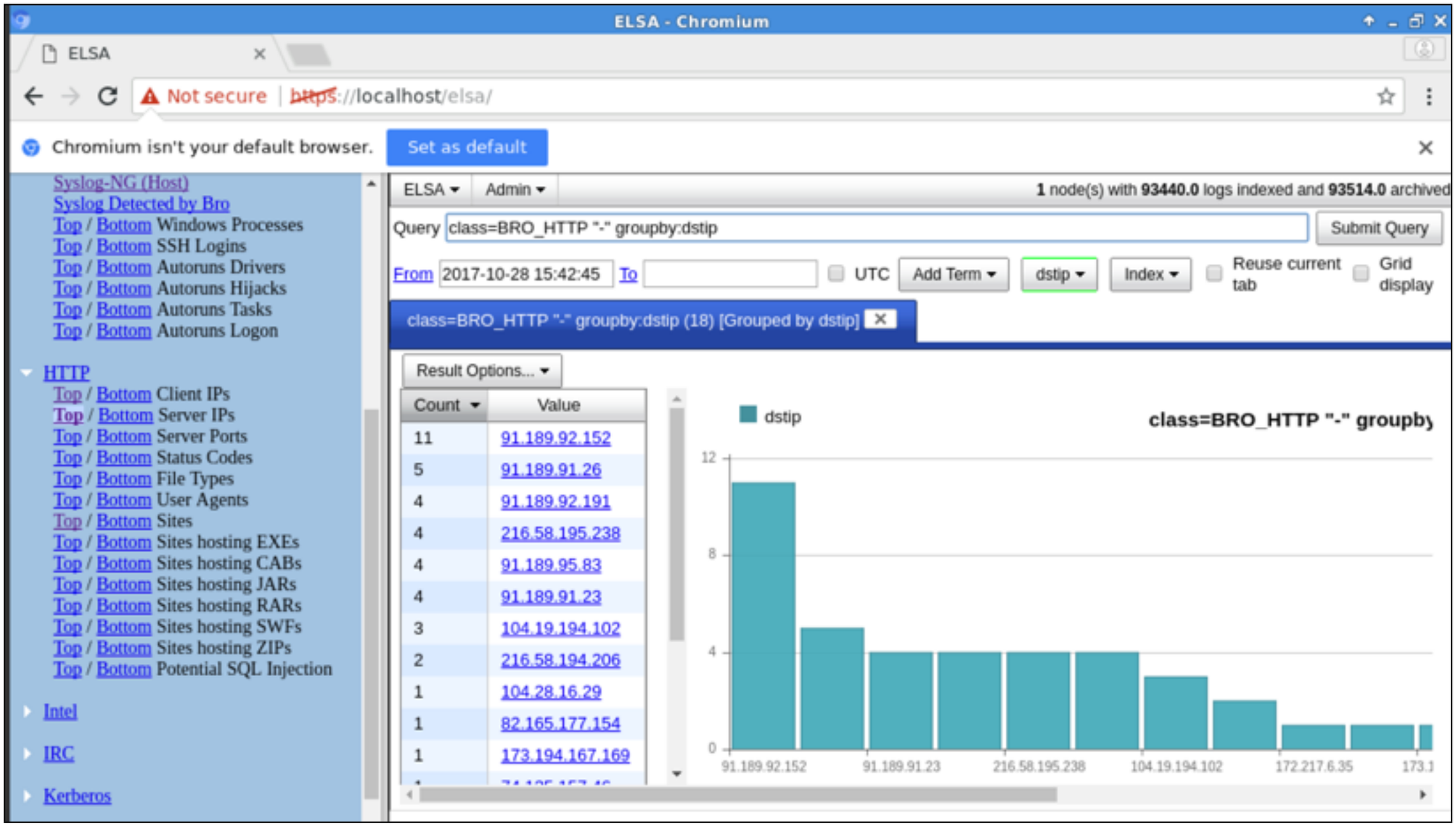
ELSA: Enterprise Log Search and Archive

- Lets you search logs for strings like Splunk
- Fully asynchronous web-based query interface
- Closely tied to Bro

Programs


ELSA - Chromium
ELSA
Not secure
https://localhost/elsa/
Chromium isn't your default browser.
Set as default
Security Onion
Connections
DHCP
DNP3
DNS
Files
Firewall
FTP
Host Logs
File Changes
OSSEC Status
OSSEC Alerts
All OSSEC Logs
Syslog-NG (Program)
Syslog-NG (Host)
Syslog Detected by Bro
Top / Bottom Windows Processes
Top / Bottom SSH Logins
Top / Bottom Autoruns Drivers
Top / Bottom Autoruns Hijacks
Top / Bottom Autoruns Tasks
Top / Bottom Autoruns Logon
HTTP
Intel
ELSA
Admin
1 node(s) with 93245.0 logs indexed and 93318.0 archived
Query class=none -program=ossec_archive -program=ossec groupby:program
Submit Query
From 2017-10-28 15:41:45
To
UTC
Add Term
program
Index
Reuse current tab
Grid display
class=none -program=ossec_archive -program=ossec groupby:program (24) [Grouped by program]
Result Options...
Count
Value
4347 cron
577 vmsvc
364 su
71 lightdm
60 dhclient
58 dbus
52 rtkit-daemon
44 ntpd
32 /etc/mysql/debian-start
24 blueman-mechanism
17 gnome-keyring-daemon
program
class=none -program=o
5000
4000
3000
2000
1000
0
cron
lightdm
rtkit-daemon
blueman-mechanism
aptdaem

Visited IPs


ELSA - Chromium
ELSA
Not secure
https://localhost/elsa/
Chromium isn't your default browser.
Set as default
Syslog-NG (Host)
Syslog Detected by Bro
Top / Bottom Windows Processes
Top / Bottom SSH Logins
Top / Bottom Autoruns Drivers
Top / Bottom Autoruns Hijacks
Top / Bottom Autoruns Tasks
Top / Bottom Autoruns Logon
HTTP
Top / Bottom Client IPs
Top / Bottom Server IPs
Top / Bottom Server Ports
Top / Bottom Status Codes
Top / Bottom File Types
Top / Bottom User Agents
Top / Bottom Sites
Top / Bottom Sites hosting EXEs
Top / Bottom Sites hosting CABs
Top / Bottom Sites hosting JARs
Top / Bottom Sites hosting RARs
Top / Bottom Sites hosting SWFs
Top / Bottom Sites hosting ZIPs
Top / Bottom Potential SQL Injection
Intel
IRC
Kerberos
ELSA
Admin
1 node(s) with 93440.0 logs indexed and 93514.0 archived
Query class=BRO_HTTP "-" groupby:dstip
Submit Query
From 2017-10-28 15:42:45
To
UTC
Add Term
dstip
Index
Reuse current tab
Grid display
class=BRO_HTTP "-" groupby:dstip (18) [Grouped by dstip]
Result Options...
Count
Value
11 91.189.92.152
5 91.189.91.26
4 91.189.92.191
4 216.58.195.238
4 91.189.95.83
4 91.189.91.23
3 104.19.194.102
2 216.58.194.206
1 104.28.16.29
1 82.165.177.154
1 173.194.167.169
dstip
class=BRO_HTTP "-" groupby
12
8
4
0
91.189.92.152
91.189.91.23
216.58.195.238
104.19.194.102
172.217.6.35

Search

ELSA - Chromium

ELSA

Not secure | https://localhost/elsa/

Chromium isn't your default browser. Set as default

Security Onion

- Connections
- DHCP
- DNP3
- DNS
- Files
- Firewall
- FTP
- Host Logs
- HTTP
- Intel
- IRC
- Kerberos
- Modbus
- MySQL
- Notice
- PE
- RADIUS
- RDP
- RFB

ELSA | Admin | 1 node(s) with 92887.0 logs indexed and 92956.0 archived

Query nmap | Submit Query

From 2017-10-28 15:37:42 To | UTC | Add Term | Report On | Index | Reuse current tab | Grid display

nmap (4)

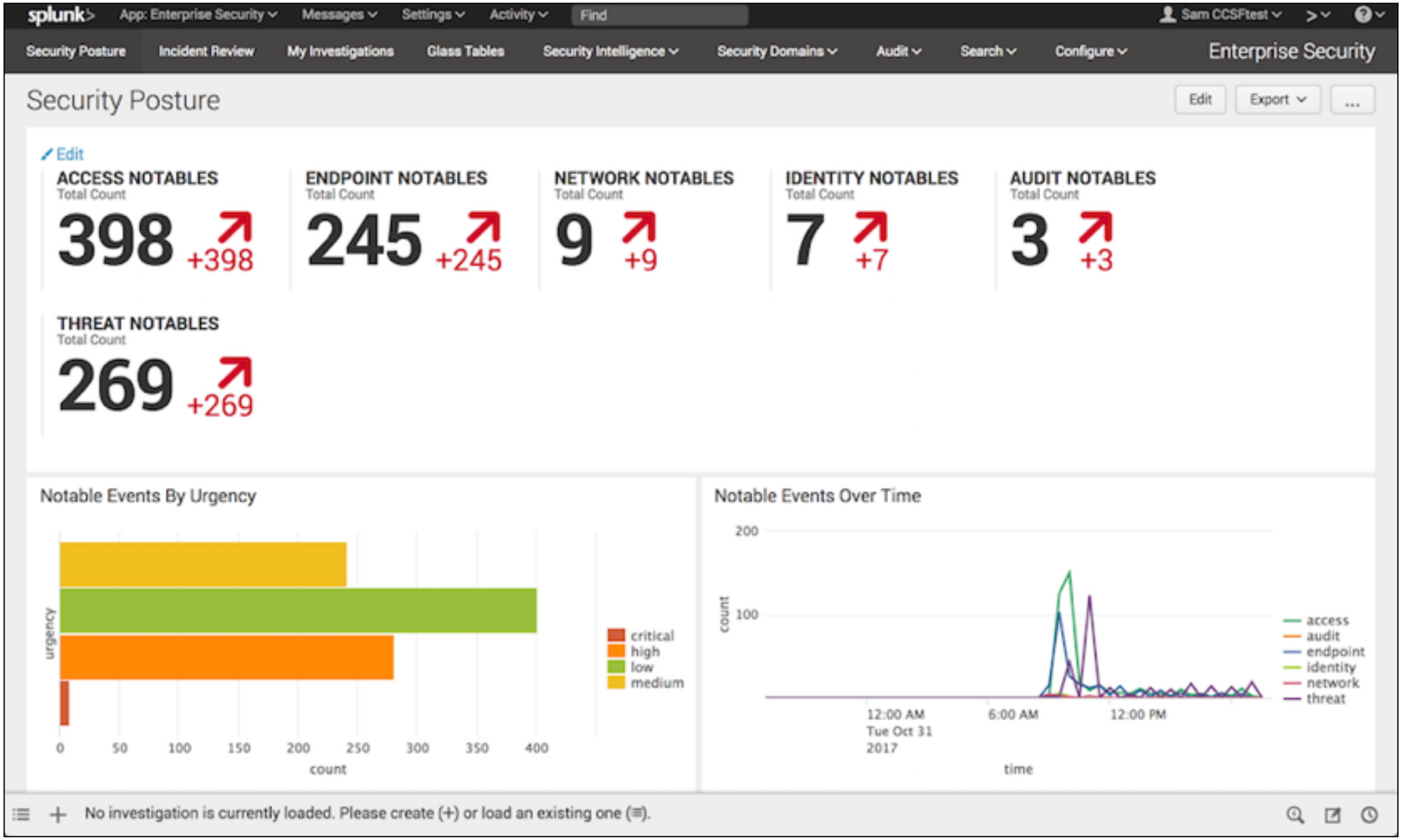
Result Options... | Field Summary host(1) program(1) class(1) sig_priority(1) proto(1) srcip(1) srcport(1) dstip(1) dstport(1) sig_sid(1) sig_msg(1) sig_classification(1) interface(1)

Records: 4 / 4 50 ms ? << first < prev 1 next > last >> 15

	Timestamp	Fields
Info	Mon Oct 30 12:13:03	[1:2018489:3] ET SCAN NMAP OS Detection Probe [Classification: Attempted Information Leak] [Priority: 2]: <so-virtual-machine-eth0-1> {UDP} 172.16.1.1:45900 -> 172.16.1.196:32004 host=127.0.0.1 program=snort class=SNORT sig_priority=2 proto=UDP srcip=172.16.1.1 srcport=45900 dstip=172.16.1.196 dstport=32004 sig_sid=1:2018489:3 sig_msg=ET SCAN NMAP OS Detection Probe sig_classification=Attempted Information Leak interface=so-virtual-machine-eth0-1
Info	Mon Oct 30 12:13:03	[1:2018489:3] ET SCAN NMAP OS Detection Probe [Classification: Attempted Information Leak] [Priority: 2]: <so-virtual-machine-eth0-1> {UDP} 172.16.1.1:45900 -> 172.16.1.196:32004 host=127.0.0.1 program=snort class=SNORT sig_priority=2 proto=UDP srcip=172.16.1.1 srcport=45900 dstip=172.16.1.196 dstport=32004 sig_sid=1:2018489:3 sig_msg=ET SCAN NMAP OS Detection Probe sig_classification=Attempted Information Leak interface=so-virtual-machine-eth0-1
Info	Mon Oct 30 12:13:04	[1:2018489:3] ET SCAN NMAP OS Detection Probe [Classification: Attempted Information Leak] [Priority: 2]: <so-virtual-machine-eth0-1> {UDP} 172.16.1.1:45900 -> 172.16.1.196:32004 host=127.0.0.1 program=snort class=SNORT sig_priority=2 proto=UDP srcip=172.16.1.1 srcport=45900 dstip=172.16.1.196 dstport=32004 sig_sid=1:2018489:3 sig_msg=ET SCAN NMAP OS Detection Probe sig_classification=Attempted Information Leak interface=so-virtual-machine-eth0-1
Info	Mon Oct 30 12:13:04	[1:2018489:3] ET SCAN NMAP OS Detection Probe [Classification: Attempted Information Leak] [Priority: 2]: <so-virtual-machine-eth0-1> {UDP} 172.16.1.1:45900 -> 172.16.1.196:32004 host=127.0.0.1 program=snort class=SNORT sig_priority=2 proto=UDP srcip=172.16.1.1 srcport=45900 dstip=172.16.1.196 dstport=32004 sig_sid=1:2018489:3 sig_msg=ET SCAN NMAP OS Detection Probe sig_classification=Attempted Information Leak interface=so-virtual-machine-eth0-1

Records: 4 / 4 50 ms ? << first < prev 1 next > last >> 15

Splunk Enterprise Security



Splunk Cost

Index Volume	Perpetual License (per GB)	Annual Term License (per GB)	Volume Purchase Discount
1 GB/Day	$4,500	$1,800	0%
10 GB/Day	$2,500	$1,000	44%
50 GB/Day	$1,900	$760	58%
100 GB/Day	$1,500	$600	67%
>100 GB/Day	Contact sales for custom pricing with additional volume discounts		