



Security@onion

Peel Back the Layers of Your Network in Minutes

Doug Burks

```
tcpdump -nnAi eth1 -s0 | grep -A5 "Doug Burks"
```

About Doug Burks:

- Christian, husband, father
- Corporate Incident Handler for Mandiant
- SANS GSE and Community Instructor
- President of Greater Augusta ISSA
- Founder and lead developer of Security Onion



What is Security Onion?

Security Onion is a FREE Linux distro for:

- intrusion detection
- network security monitoring
- log management

What data does it give me?

- Flow data from Argus, Bro, and PRADS
- Alert data
 - NIDS alerts from Snort/Suricata
 - HIDS alerts from OSSEC
- Syslog data received by syslog-ng or sniffed by Bro
- Asset data from Bro and PRADS
- Transaction data – http/ftp/dns/ssl/other logs from Bro
- Full content data from netsniff-ng

Does it scale?

- Big Onions – 64-bit
- Big Traffic – PF_RING
- Big Data – ELSA



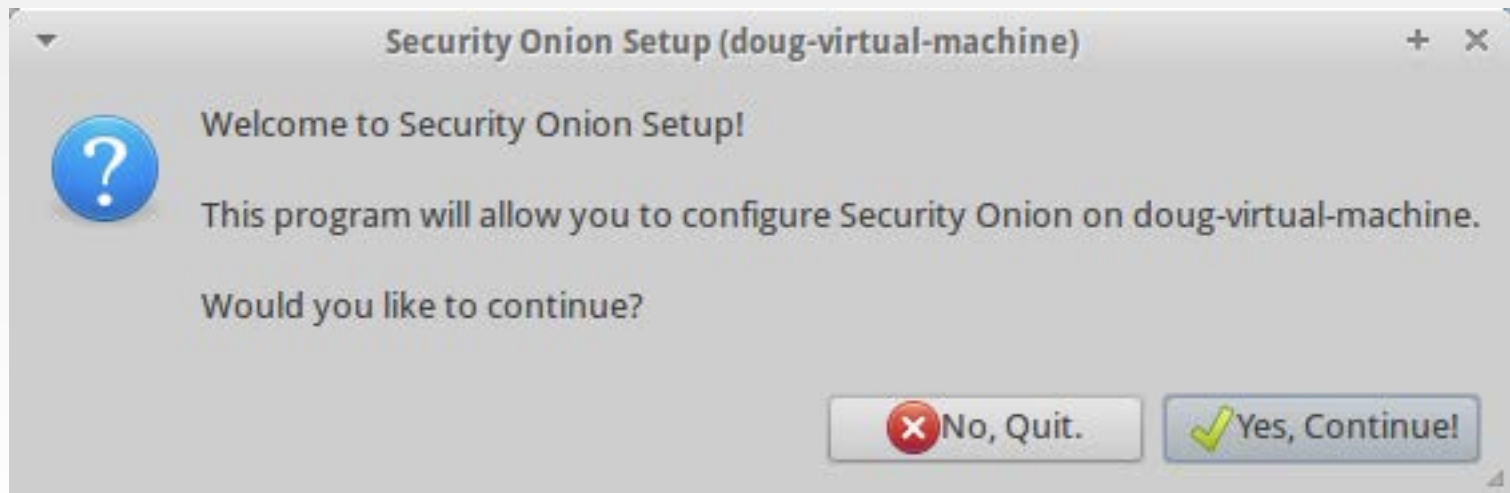
How many Security Onion users are there?

- Over **100,000** ISO downloads from Sourceforge!
 - Security Onion 10.04 ISO (based on Ubuntu 10.04) - 37,777
 - Security Onion 12.04 ISO (released 12/31/2012) - 34,573
 - Security Onion 12.04.1 ISO (released 6/10/2013) - 7,511
 - Security Onion 12.04.2 ISO (released 7/25/2013) - 6,396
 - Security Onion 12.04.3 ISO (released 9/14/2013) - 15,824
- ??? From BitTorrent
- ??? Ubuntu/Kubuntu/Lubuntu + Security Onion PPA

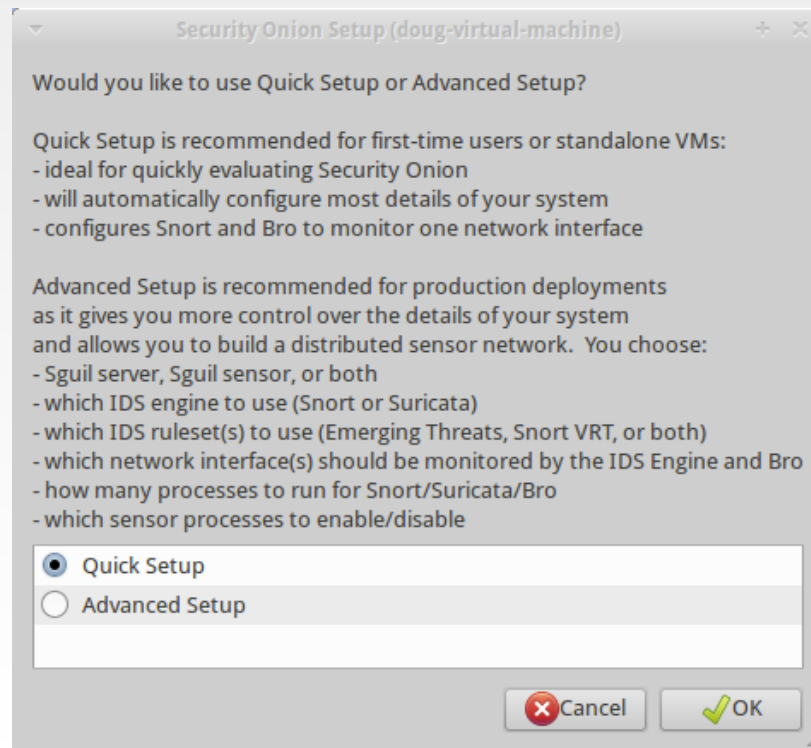
What has changed since last FloCon?

- Updated just about every piece of software, including:
Snort, Suricata, Bro, PF_RING, PRADS, ELSA, Snorby, Squert, CapMe, NetworkMiner
- Fixed lots o' bugs!
- Moved to a standard argus.conf to allow more Argus customization
- Added more knobs for tuning:
 - Enable/disable sensor processes
 - Adjustable netsniff-ng (full packet capture) settings
 - Adjustable log purge threshold
- Added OnionSalt to manage lots o' onions

What does it look like?



Answer a few simple questions...



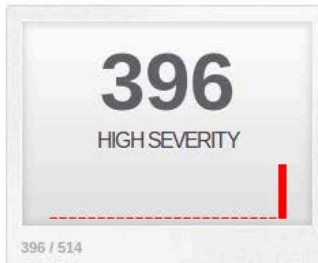
Snorby

Dashboard

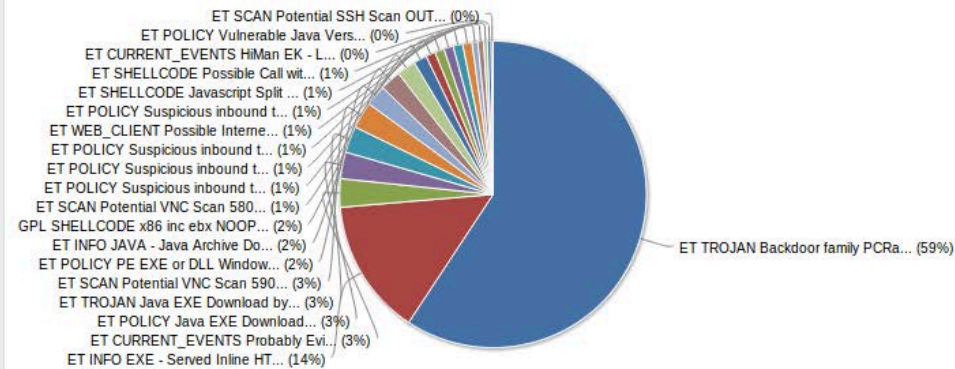
More Options

LAST 24 TODAY YESTERDAY THIS WEEK THIS MONTH THIS QUARTER THIS YEAR

Updated: 01/11/14 04:47 PM UTC



Sensors Severities Protocols Signatures Sources Destinations



TOP 5 SENSOR

doug-virtual-machine-eth1:1 514

TOP 5 ACTIVE USERS

Administrator 0

LAST 5 UNIQUE EVENTS

ET POLICY PE EXE or DLL W... 11

GPL SHELLCODE x86 inc ebx... 10

ET SHELLCODE Possible Cal... 3

ET INFO Executable Downlo... 1

ET POLICY SUSPICIOUS *.do... 1

ANALYST CLASSIFIED EVENTS

Unauthorized Root Access 0

Unauthorized User Access 0

Attempted Unauthorized... 0

Denial of Service Attack 0

Policy Violation 0

Reconnaissance 0

Virus Infection 0

False Positive 0

Pivot to pcap from Snorby

The screenshot displays the Snorby web interface. At the top, it says "Sponsored by threat stack" and "Welcome Administrator | Settings | Log out". The navigation menu includes Dashboard, My Queue (0), Events, Sensors, Search, and Administration. The main content area is titled "Listing Sessions (62 unique unclassified sessions)". Below this is a table with columns: Sev., Sensor, Source IP, Destination IP, Event Signature, Timestamp, and Sessions. Two sessions are visible:

Sev.	Sensor	Source IP	Destination IP	Event Signature	Timestamp	Sessions
1	doug-virtual-	172.16.150.20	66.32.119.38	ET INFO Executable Download from dotted-quad Host	4:16 PM	1
2	doug-virtual-	172.16.150.20	66.32.119.38	ET POLICY SUSPICIOUS *.doc.exe in HTTP URL	4:16 PM	1

Below the table, there are several tabs: "View All Sessions", "Perform Mass Classification", "Packet Capture Options", "Event Export Options", and "Permalink". A "Packet Capture Builder" dialog box is open, showing the following fields:

- Source address (Source Address : Source Port): 172.16.150.20 : 1294
- Destination address (Destination Address : Destination Port): 66.32.119.38 : 80
- Protocol: TCP
- Start time (default is 30 minutes before the event start time): 2014 January 11 15 : 46
- End time (default is 30 minutes after the event end time): 2014 January 11 16 : 46

At the bottom of the dialog box, there are two buttons: "Fetch Packet" (green) and "Cancel" (red).

CapME

close

[172.16.150.20:1294_66.32.119.38:80-6-1456675353.pcap](#)

Sensor Name: doug-virtual-machine-eth1
Timestamp: 2014-01-11 16:16:39
Connection ID: CLI
Src IP: 172.16.150.20 (Unknown)
Dst IP: 66.32.119.38 (static-66-32-119-38.earthlinkbusiness.net)
Src Port: 1294
Dst Port: 80
OS Fingerprint: 172.16.150.20:1294 - Windows 2000 SP2+, XP SP1+ (seldom 98)
OS Fingerprint -> 66.32.119.38:80 (distance 0, link: ethernet/modem)

SRC: GET /tigers/BrandonInge/Diagnostics/swing-mechanics.doc.exe HTTP/1.1
SRC: Accept: image/gif, image/x-bitmap, image/jpeg, application/x-shockwave-flash, */*
SRC: Accept-Language: en-us
SRC: Accept-Encoding: gzip, deflate
SRC: User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
SRC: Host: 66.32.119.38
SRC: Connection: Keep-Alive
SRC:
SRC:
DST: HTTP/1.1 200 OK
DST: Date: Fri, 27 Apr 2012 17:40:31 GMT
DST: Server: Apache/2.2.16 (Ubuntu)
DST: Last-Modified: Sat, 14 Apr 2012 09:34:10 GMT
DST: ETag: "42d3b-2000-4bda04a8ed053"
DST: Accept-Ranges: bytes
DST: Content-Length: 8192
DST: Keep-Alive: timeout=15, max=100
DST: Connection: Keep-Alive
DST: Content-Type: application/x-msdos-program
DST:
DST: MZ.....@.....!L!This program cannot be run in DOS mode.
DST:
DST: \$......n...n.wq...n..N..n..Rich.n.....PE.L.....G.....<.....(
.....text...h.....data...-...data...@.....L.....@...j.....%..@.D.....Z.....L.....ExitProcess.kernel32.dll.....


Squert web interface

Events Welcome doug | Logout

Timeline: 2014-01-11 00:00:00 until 2014-01-11 23:59:59 (+00:00) Filtered by Object: NO Filtered by Sensor: NO Status: Squert/loaded

Iscale
 Event Grouping: on
 Event Queue Only: on
 Map: on
Event Summary
 Queued Events: 565
 Total Events: 796
 Total Signatures: 35
 Total Sources: -
 Total Destinations: -
Event Count by Priority
 High: 396 (50.2%)
 Medium: 46 (5.8%)
 Low: 72 (9.0%)
 Other: 50 (6.2%)
Event Count by Classification
 Admin Access: -
 User Access: -
 Attempted Access: -
 Denial of Service: -
 Policy Violation: -
 Reconnaissance: -
 Malware: -
 No Action Req'd: 191 (23.9%)
 Escalated Event: -
History
 172.16.150.20 66.32.119.38

Countries as sources: 2 with 72 events Countries as destinations: 5 with 447 events Total countries: 5



1 1 1 16:16:39 ET POLICY SUSPICIOUS *.doc.exe in HTTP URL 2013475 6 0.132%

alertr tcp \$HOME_NET any -> \$EXTERNAL_NET \$HTTP_PORTS (msg:"ET POLICY SUSPICIOUS *.doc.exe in HTTP URL"; flow:to_server,established; content:".doc.exe"; http_url; nocase; classtype:bad-unknown; sid:2013475; rev:1)

file: downloaded.rules:10836
categorize 0 event(s)

QUEUE	ACTIVITY	LAST EVENT	SOURCE	COUNTRY	DESTINATION	COUNTRY
1		2014-01-11 16:16:39	172.16.150.20	RFC1918 (us)	66.32.119.38	UNITED STATES (us)

ST	TIMESTAMP	EVENT ID	SOURCE	PORT	DESTINATION	PORT	SIGNATURE
RT	2014-01-11 16:16:39	3.512	172.16.150.20	1294	66.32.119.38	80	ET POLICY SUSPICIOUS *.doc.exe in HTTP URL

Sensor Name: doug-virtual-machine-eth1-1
Timestamp: 2014-01-11 16:16:39
Connection ID: CLI
Src IP: 172.16.150.20 (Unknown)
Dst IP: 66.32.119.38 (static-66-32-119-38.earthlinkbusiness.net)
Src Port: 1294
Dst Port: 80
OS Fingerprint: 172.16.150.20:1294 - Windows 2000 SP2+; XP SP1+ (seldom 98)
OS Fingerprint: -> 66.32.119.38:80 (distance 0, link: ethernet/modem)

```

SRC: GET /ligers/BrandenInge/Diagnostics/swing-mechanics.doc.exe HTTP/1.1
SRC: Accept: image/gif, image/x-bitmap, image/jpeg, application/x-shockwave-flash, */
SRC: Accept-Language: en-us
SRC: Accept-Encoding: gzip, deflate
SRC: User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
SRC: Host: 66.32.119.38
SRC: Connection: Keep-Alive
SRC:
DST: HTTP/1.1 200 OK
DST: Date: Fri, 27 Apr 2012 17:40:31 GMT
DST: Server: Apache/2.2.16 (Ubuntu)
DST: Last-Modified: Sat, 14 Apr 2012 09:34:10 GMT
DST: ETag: "42d3b-2000-4bda048ed053"
DST: Accept-Ranges: bytes
DST: Content-Length: 8192
DST: Keep-Alive: timeout=15, max=100
DST: Connection: Keep-Alive
DST: Content-Type: application/x-msdos-program
DST:
DST: MZ.....@.....!L!This program cannot be run in DOS mode.
DST:
DST: .....n..n..n..wq..n..n..Richn.....PE.L.....G.....@.....<.....(.....
.....ext..h..n..n..n..Richn.....PE.L.....G.....@.....L.....@..j..%..@..D..Z.....L.....ExitProcess.kernde32.dll
  
```

QUEUE	SC	DC	ACTIVITY	LAST EVENT	SIGNATURE
11	7	1	1	16:18:50	[OSSEC] Integrity checksum changed again (2nd time)
21	5	11	17	16:16:40	PADS New Asset - unknown @https
11	5	6	6	16:16:39	ET POLICY PE EXE or DLL Windows file download
3	2	2	2	16:18:39	ET SHELLOCODE Possible Call with No Offset TCP Shellcode
1	1	1	1	16:16:39	ET POLICY SUSPICIOUS *.doc.exe in HTTP URL
1	1	1	1	16:16:39	ET INFO Executable Download from dotted-quad Host
10	5	6	6	16:16:39	GPL SHELLOCODE x86 exe etex NOOP
3	2	2	2	16:16:38	ET SHELLOCODE Possible Call with No Offset TCP Shellcode

Sguil client

RT	11	doug-...	3.431	2014-01-11 16:16:36	59.53.91.102	80	192.168.23.129	1064	6	ET INFO JAVA - Java Archive Download By Vulnerable Client
RT	2	doug-...	3.442	2014-01-11 16:16:36	59.53.91.102	80	192.168.23.129	1066	6	ET POLICY PE EXE or DLL Windows file download
RT	27	doug-...	3.444	2014-01-11 16:16:36	59.53.91.102	80	192.168.23.129	1067	6	ET INFO EXE - Served Inline HTTP
RT	14	doug-...	3.458	2014-01-11 16:16:36	59.53.91.102	80	192.168.23.129	1067	6	ET POLICY Java EXE Download
RT	14	doug-...	3.472	2014-01-11 16:16:36	59.53.91.102	80	192.168.23.129	1067	6	ET TROJAN Java EXE Download by Vulnerable Version - Likely Driveby
RT	1	doug-...	3.499	2014-01-11 16:16:37	192.168.23.129	1069	212.252.32.20	80	6	ET USER_AGENTS Suspicious User Agent (Microsoft Internet Explorer)
RT	1	doug-...	3.500	2014-01-11 16:16:37	192.168.23.129	1069	212.252.32.20	80	6	ET TROJAN SpyEye Bot Checkin
RT	1	doug-...	3.501	2014-01-11 16:16:37	192.168.23.129	1069	212.252.32.20	80	6	ET TROJAN SpyEye C&C Check-in URI
RT	1	doug-...	3.502	2014-01-11 16:16:37	192.168.23.129	1069	212.252.32.20	80	6	ET TROJAN Banker PWS/Infostealer HTTP GET Checkin
RT	2	doug-...	3.503	2014-01-11 16:16:37	10.10.10.10	4444	10.10.10.70	1036	6	ET POLICY PE EXE or DLL Windows file download
RT	4	doug-...	3.504	2014-01-11 16:16:37	10.10.10.10	4444	10.10.10.70	1036	6	ET SHELLCODE Possible Call with No Offset TCP Shellcode
RT	2	doug-...	3.505	2014-01-11 16:16:37	10.10.10.10	4444	10.10.10.70	1036	6	GPL SHELLCODE x86 inc ebx NOOP
RT	1	doug-...	3.511	2014-01-11 16:16:39	172.16.150.20	1294	66.32.119.38	80	6	ET INFO Executable Download from dotted-quad Host
RT	1	doug-...	3.512	2014-01-11 16:16:39	172.16.150.20	1294	66.32.119.38	80	6	ET POLICY SUSPICIOUS *.doc.exe in HTTP URL
RT	1	doug-...	3.513	2014-01-11 16:16:39	66.32.119.38	80	172.16.150.20	1294	6	ET POLICY PE EXE or DLL Windows file download
RT	1	doug-...	3.514	2014-01-11 16:16:39	66.32.119.38	80	172.16.150.20	1294	6	ET SHELLCODE Possible Call with No Offset TCP Shellcode

IP Resolution
Agent Status
Snort Statistics
System Msgs
User Msgs

Reverse DNS
 Enable External DNS

Src IP: 172.16.150.20

Src Name: Unknown

Dst IP: 66.32.119.38

Dst Name: static-66-32-119-38.earthlinkbusiness.net

Whois Query: None Src IP Dst IP

#

NetRange: 66.32.0.0 - 66.32.255.255

CIDR: 66.32.0.0/16

OriginAS:

Show Packet Data Show Rule


```

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET POLICY SUSPICIOUS *.doc.exe in HTTP URL"; flow:to_server,established; content:".doc.exe"; http_uri; nocase; classtype:bad-unknown; sid:2013475; rev:1;)
/nsm/server_data/securityonion/rules/doug-virtual-machine-eth1-1/downloaded.rules: Line 10836
        
```

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
	172.16.150.20	66.32.119.38	4	5	0	378	8716	2	0	128	56326

TCP	Source Port	Dest Port	R	R	C	S	S	Y	I	Seq #	Ack #	Offset	Res	Window	Urp	ChkSum
	1294	80	.	.	X	X	.	.	.	2574696136	968806116	5	0	17520	0	31695

47 45 54 20 2F 74 69 67 65 72 73 2F 42 72 61 6E	GET /tigers/Bran donInge/Diagnost ics/swing-mechan
64 6F 6E 49 6E 67 65 2F 44 69 61 67 6E 6F 73 74	
69 63 73 2F 73 77 69 6F 67 2D 6D 65 63 68 61 6F	

Pivot to pcap from Sguil

doug-virtual-machine-eth1-1_512

File

Sensor Name: doug-virtual-machine-eth1-1
Timestamp: 2014-01-11 16:16:39
Connection ID: .doug-virtual-machine-eth1-1_512
Src IP: 172.16.150.20 (Unknown)
Dst IP: 66.32.119.38 (static-66-32-119-38.earthlinkbusiness.net)
Src Port: 1294
Dst Port: 80
OS Fingerprint: 172.16.150.20:1294 - Windows 2000 SP2+, XP SP1+ (seldom 98)
OS Fingerprint: -> 66.32.119.38:80 (distance 0, link: ethernet/modem)

SRC: GET /tigers/BrandonInge/Diagnostics/swing-mechanics.doc.exe HTTP/1.1
SRC: Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, */*
SRC: Accept-Language: en-us
SRC: Accept-Encoding: gzip, deflate
SRC: User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
SRC: Host: 66.32.119.38
SRC: Connection: Keep-Alive
SRC:
DST: HTTP/1.1 200 OK
DST: Date: Fri, 27 Apr 2012 17:40:31 GMT
DST: Server: Apache/2.2.16 (Ubuntu)
DST: Last-Modified: Sat, 14 Apr 2012 09:34:10 GMT
DST: ETag: "42d3b-2000-4bda04a8ed053"
DST: Accept-Ranges: bytes
DST: Content-Length: 8192
DST: Keep-Alive: timeout=15, max=100
DST: Connection: Keep-Alive
DST: Content-Type: application/x-msdos-program

Search Abort Close

Debug Messages

Using archived data:
/nsm/server_data/securityonion/archive/2014-01-11/doug-virtual-machine-eth1-1/172.16.150.20:1294_66.32.119.38:80-6.raw
Finished.

172.16.150.20:1294_66.32.119.38:80-6.raw [Wireshark 1.6.7]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.16.150.20	66.32.119.38	TCP	62	1294 > 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
2	0.000272	66.32.119.38	172.16.150.20	TCP	62	80 > 1294 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
3	0.000412	172.16.150.20	66.32.119.38	TCP	60	1294 > 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
4	0.000923	172.16.150.20	66.32.119.38	HTTP	392	GET /tigers/BrandonInge/Diagnostics/swing-mechanics.doc.exe HTTP/1.1
5	0.001160	66.32.119.38	172.16.150.20	TCP	54	80 > 1294 [ACK] Seq=1 Ack=339 Win=6432 Len=0
6	0.002683	66.32.119.38	172.16.150.20	TCP	1514	[TCP segment of a reassembled PDU]
7	0.003868	66.32.119.38	172.16.150.20	TCP	1514	[TCP segment of a reassembled PDU]
8	0.005282	66.32.119.38	172.16.150.20	TCP	1514	[TCP segment of a reassembled PDU]
9	0.005378	172.16.150.20	66.32.119.38	TCP	60	1294 > 80 [ACK] Seq=339 Ack=2921 Win=17520 Len=0
10	0.005461	172.16.150.20	66.32.119.38	TCP	60	1294 > 80 [ACK] Seq=339 Ack=4381 Win=17520 Len=0
11	0.006818	66.32.119.38	172.16.150.20	TCP	1514	[TCP segment of a reassembled PDU]
12	0.008442	66.32.119.38	172.16.150.20	TCP	1514	[TCP segment of a reassembled PDU]
13	0.009597	66.32.119.38	172.16.150.20	HTTP	1258	HTTP/1.1 200 OK (application/x-msdos-program)

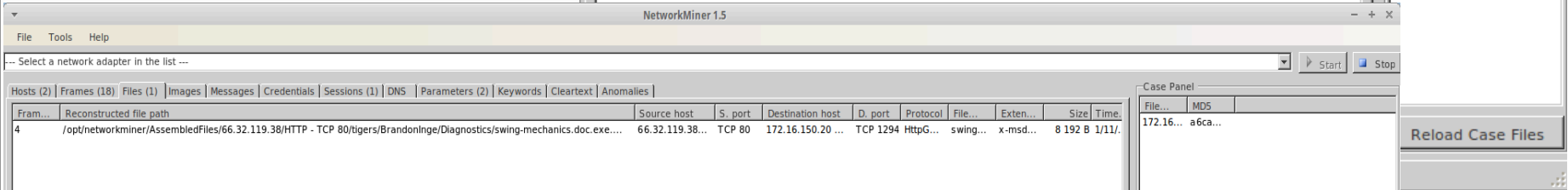
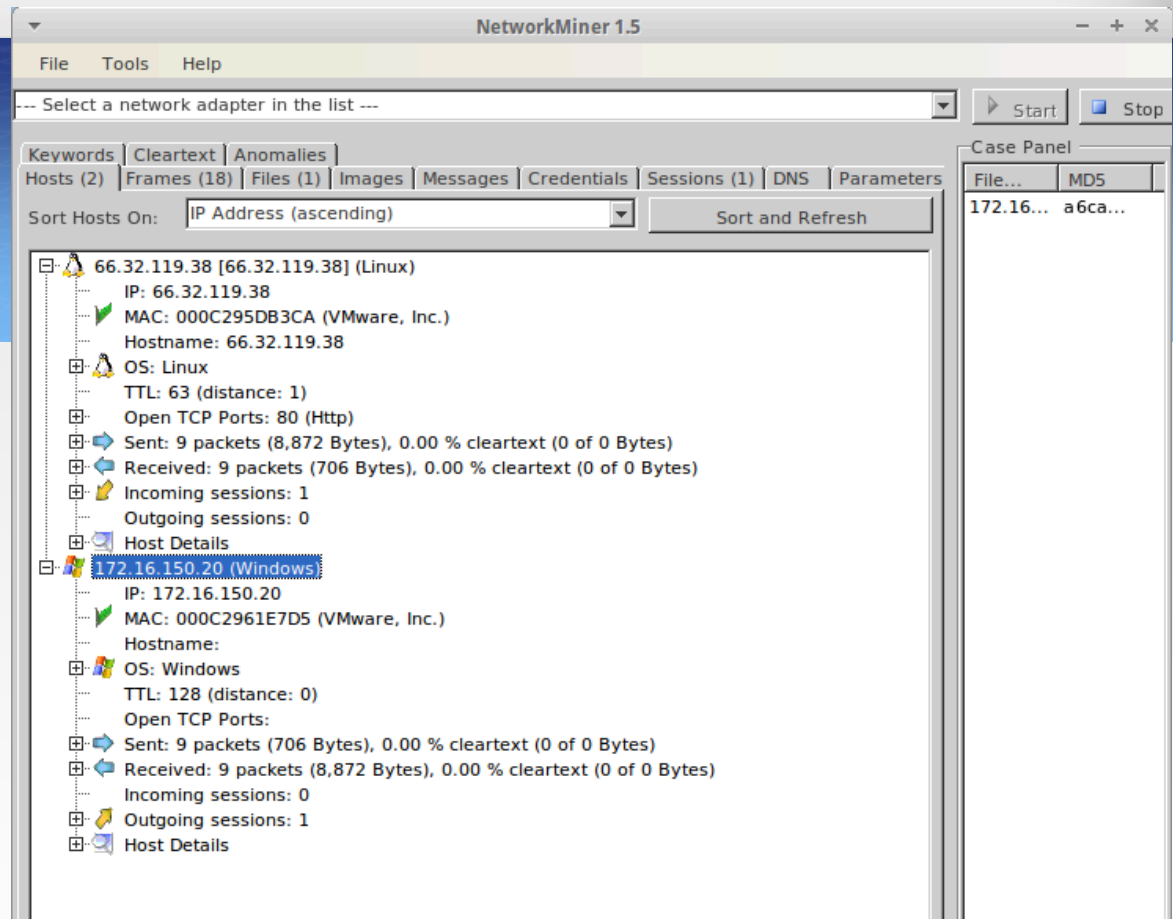
▶ Frame 4: 392 bytes on wire (3136 bits), 392 bytes captured (3136 bits)
▶ Ethernet II, Src: 00:0c:29:61:e7:d5 (00:0c:29:61:e7:d5), Dst: 00:0c:29:5d:b3:ca (00:0c:29:5d:b3:ca)
▶ Internet Protocol Version 4, Src: 172.16.150.20 (172.16.150.20), Dst: 66.32.119.38 (66.32.119.38)
▶ Transmission Control Protocol, Src Port: 1294 (1294), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 338
▶ Hypertext Transfer Protocol

```
0000 00 0c 29 5d b3 ca 00 0c 29 61 e7 d5 08 00 45 00  ..)....)a....E.
0010 01 7a 22 0c 40 00 80 06 dc 06 ac 10 96 14 42 20  .z".@... ..B
0020 77 26 05 0e 00 50 99 76 be c8 39 be ce e4 50 18  w&...P.v...9...P.
0030 44 70 7b cf 00 00 47 45 54 20 2f 74 69 67 65 72  Dp{...GE T /tiger
0040 73 2f 42 72 61 6e 64 6f 6e 49 6e 67 65 2f 44 69  s/Brando nInge/Di
0050 61 67 6e 6f 73 74 69 63 73 2f 73 77 69 6e 67 2d  agnostic s/swing-
0060 6d 65 63 68 61 6e 69 63 73 2e 64 6f 63 2e 65 78  mechanic s.doc.ex
0070 65 20 48 54 54 50 2f 31 2e 31 0d 0a 41 63 63 65  e HTTP/1 .1..Acce
0080 70 74 3a 20 69 6d 61 67 65 2f 67 69 6e 2c 20 69  pt: imag e/gif, i
0090 6d 61 67 65 2f 78 2d 78 62 69 74 6d 61 70 2c 20  mage/x-x bitmap,
```

File: *tmp/172.16.150.20:1294_66.32.119.38:80-6.raw Packets: 18 Displayed: 18 Marked: 0 Load time: 0:00:00 Profile: Default

NetworkMiner

There's gold in them
thar PCAPs!



ELSA

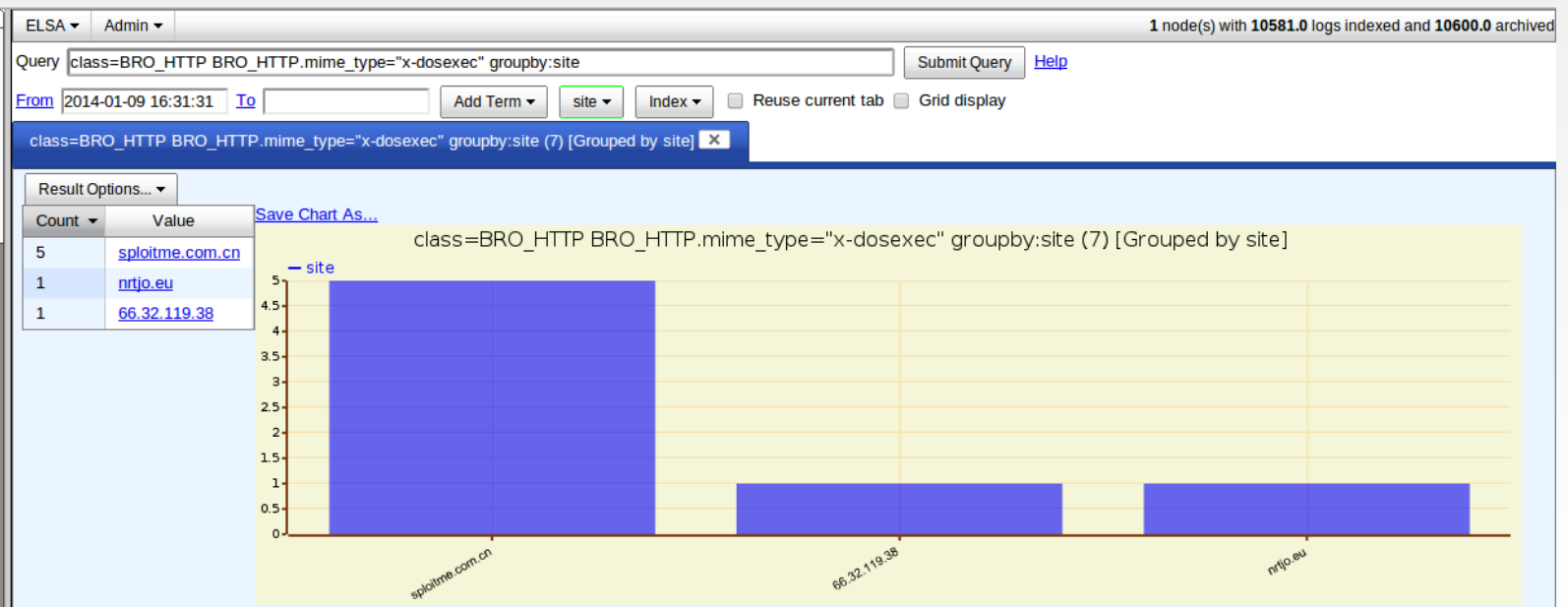
[Top requests](#)
[Top Responses](#)
[Top nxdomain](#)

Files
[MIME Types](#)
[Sources](#)

FTP
[Top SRC IPs](#)
[Top DST IPs](#)
[Top DST Ports](#)
[Top MIME Types](#)
[Top arg](#)

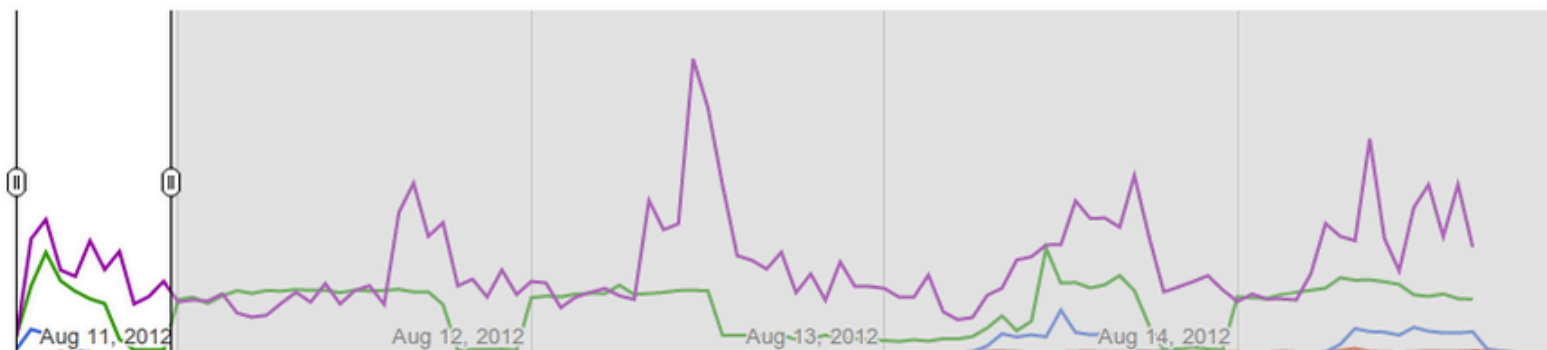
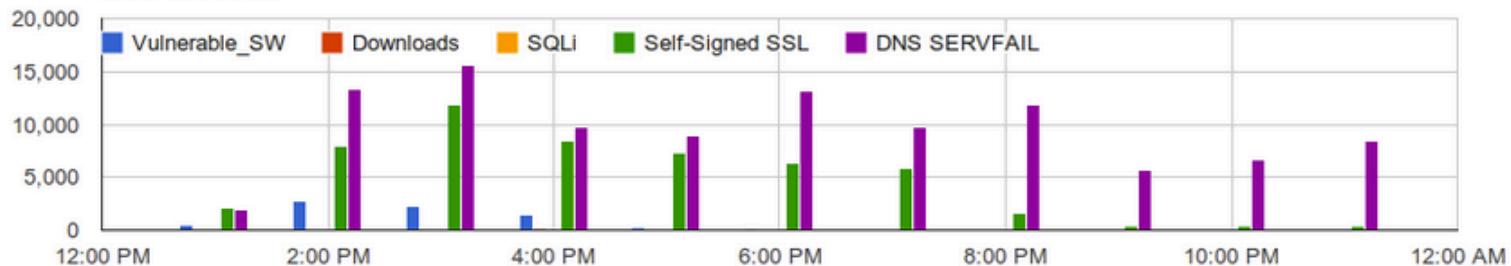
Host Logs
[OSSEC Alerts](#)
[All OSSEC Logs](#)
[Syslog-NG](#)
[Syslog Detected by Bro](#)

HTTP
[Top SRC IPs](#)
[Top DST IPs](#)
[Top DST Ports](#)
[Top MIME Types](#)
[Top User Agents](#)
[Top Sites](#)
[Sites hosting EXEs](#)
[Sites hosting RARs](#)

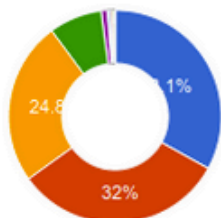


Bro IDS

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

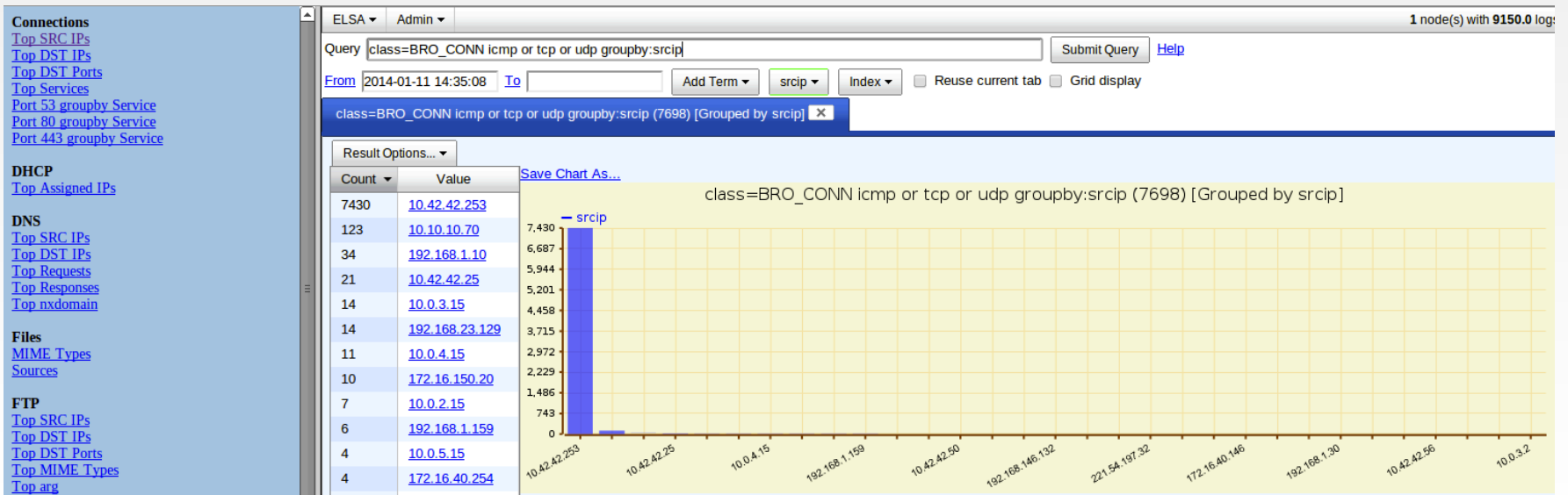
```

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,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
    
```

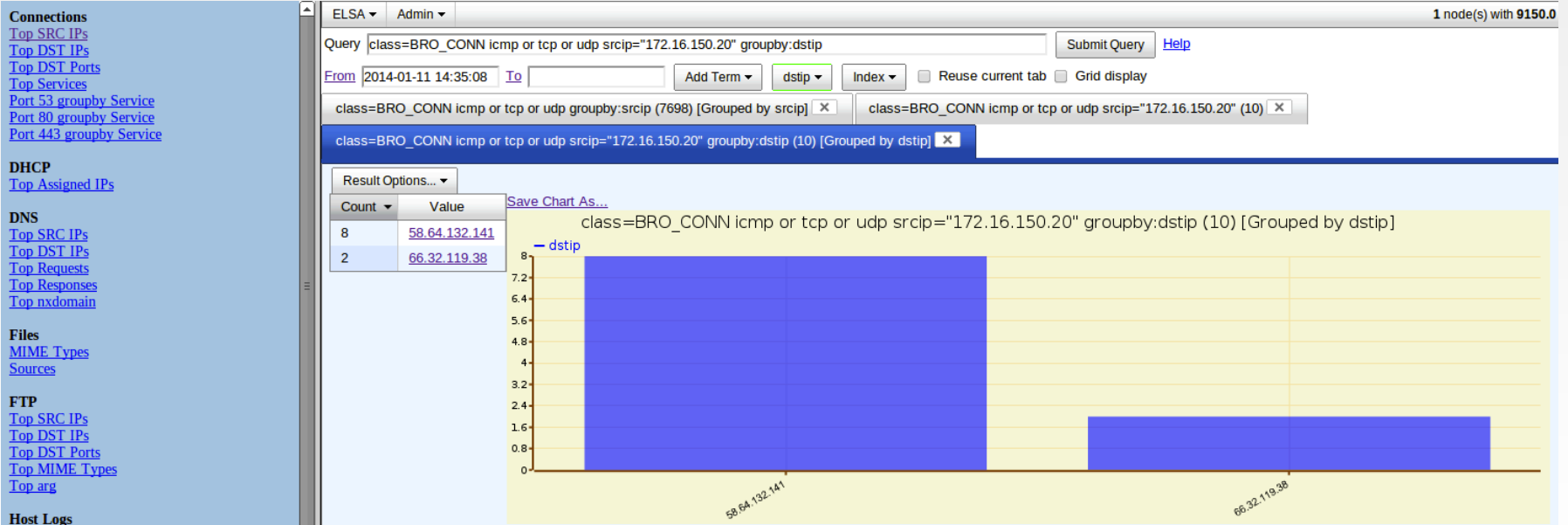
Case Study

- Was an EXE downloaded?
- Was it executed?
- Was the computer compromised?
- Was there any data exfil?

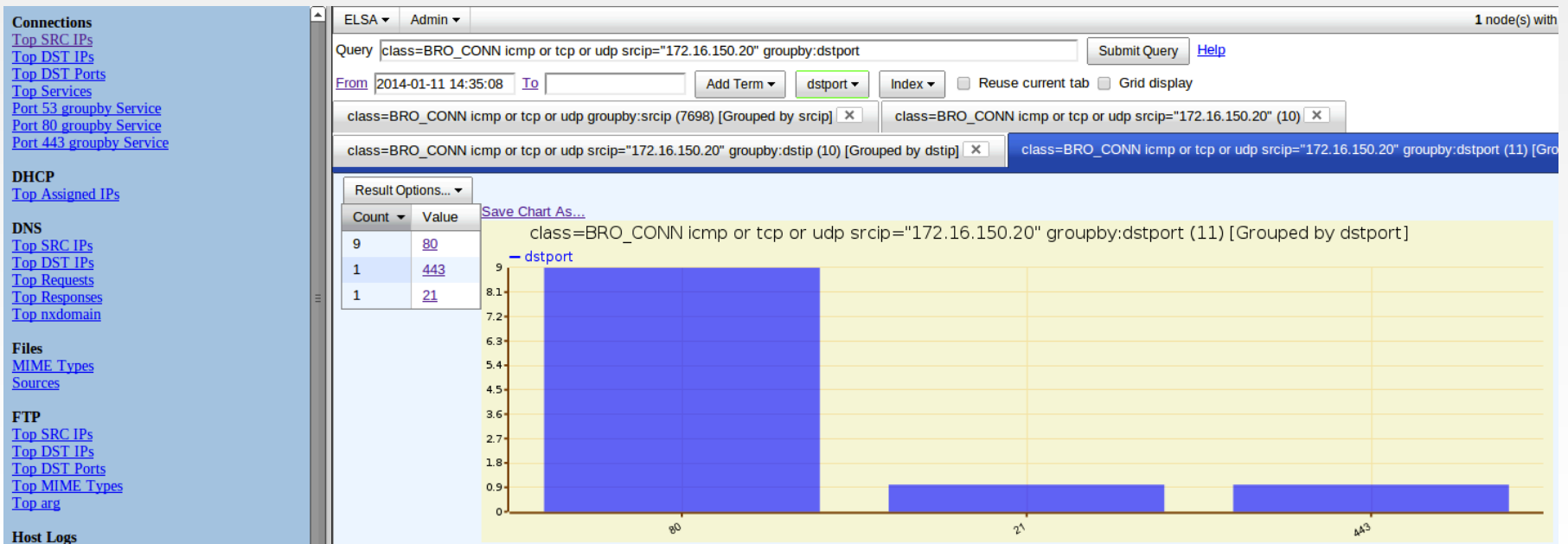
Bro Flow



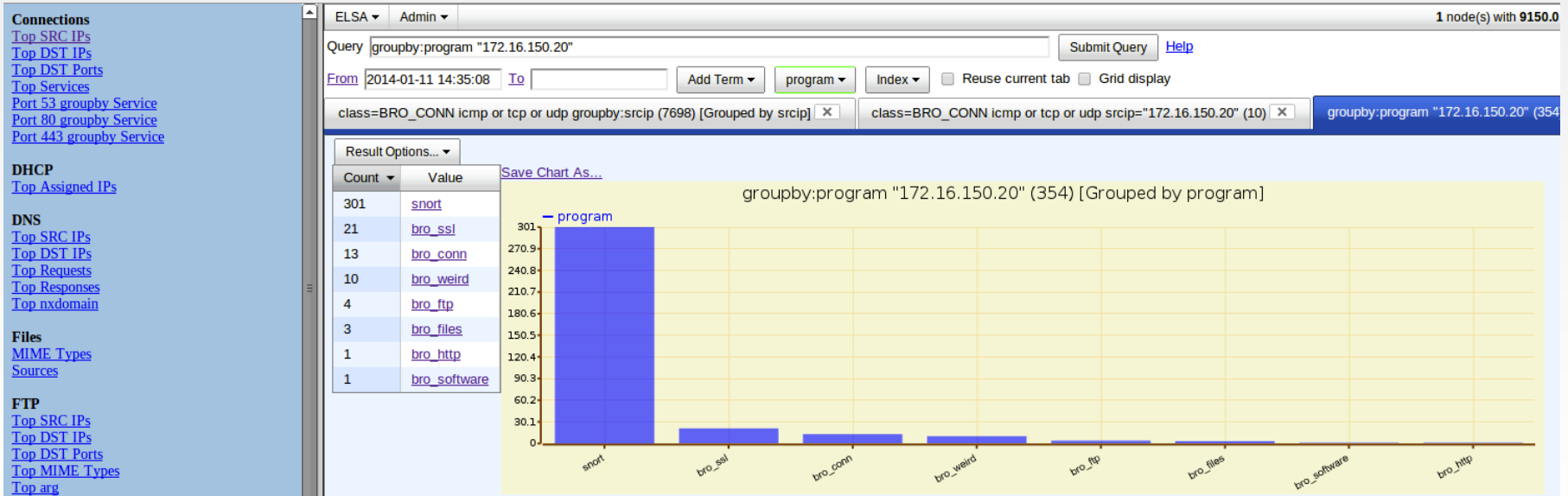
Who did this IP talk to?



And over what ports?



What all do we know about the source?



Found an EXE

Connections
[Top SRC IPs](#)
[Top DST IPs](#)
[Top DST Ports](#)
[Top Services](#)
[Port 53 groupby Service](#)
[Port 80 groupby Service](#)
[Port 443 groupby Service](#)

DHCP
[Top Assigned IPs](#)

DNS
[Top SRC IPs](#)
[Top DST IPs](#)
[Top Requests](#)
[Top Responses](#)
[Top nxdomain](#)

Files
[MIME Types](#)
[Sources](#)

ELSA Admin 1 node(s) with 9150.0 k

Query "172.16.150.20" program="bro_http" [Help](#)

From 2014-01-11 14:35:08 To Reuse current tab Grid display

class=BRO_CONN icmp or tcp or udp groupby:srcip (7698) [Grouped by srcip] class=BRO_CONN icmp or tcp or udp srcip="172.16.150.20" (10) groupby:program "172.16.150.20" (354)

"172.16.150.20" program="bro_http" (1)

Field Summary
host(1) program(1) class(1) srcip(1) srcport(1) dstip(1) dstport(1) status_code(1) content_length(1) method(1) site(1) uri(1) referer(1) user_agent(1) mime_type(1)

Records: 1 / 1 97 ms ? << first < prev 1 next > last >> 15 ▾

	Timestamp	Fields
Info	Mon Jan 13 14:32:59	1389623578.149097 CevVRm1BRMlcQQYHTd 172.16.150.20 1294 66.32.119.38 80 1 GET 66.32.119.38 tigers/BrandonInge/Diagnostics/swing-mechanics.doc.exe - Mozilla 6.0; Windows NT 5.1; SV1 0 8192 200 OK - - (empty) - - - F5wbvP2Ht50aZITeq4 application/x-dosexec host=127.0.0.1 program=bro_http class=BRO_HTTP srcip=172.16.150.20 srcport=1294 dstip=66.32.119.38 dstport=80 status_code=200 content_length=8192 method=GET site=/ uri=/tigers/BrandonInge/Diagnostics/swing-mechanics.doc.exe referer=; user_agent=Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) mime_type=application/x-dosexec

Records: 1 / 1 97 ms ? << first < prev 1 next > last >> 15 ▾

IP address in EXE

```
doug@doug-virtual-machine:~$ strings /nsm/bro/extracted/*F5wbvP2Ht50aZITeq4*
ExitProcess
kernel32.dll
ws2_32
cks=u
ttp=
cks=
CONNECT %s:%i HTTP/1.0
QSRW
?503
200
thj@h
VSWRQ
YZ_[^
s f5
YZ_[^
QVlM
6I*h<8
^-m-m<|<|<|M
o/o/
advapi32
ntdll
user32
1+KY
#%li
}>*K
QQVP
advpack
StubPath
SOFTWARE\Classes\http\shell\open\commandV
Software\Microsoft\Active Setup\Installed Components\
tigers
221.54.197.32
tigers
svchostsA
explorer.exe
)!VoqA.I4-
svchosts.exe
SOFTWARE\Microsoft\Windows\CurrentVersion\Run
explorer.exe
QPRRQ
VSWRQ
W1jD
YZ_[^
SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
AppData
V%X_
```


Interesting FTP Activity

ELSA Admin 1 node(s) with 9150.0 logs indexed and 9155.0 archi

Query "172.16.150.20" program="bro_ftp" Submit Query Help

From 2014-01-11 14:35:08 To Add Term Report On Index Reuse current tab Grid display

class=BRO_CONN icmp or tcp or udp groupby:srcip (7698) [Grouped by srcip] X class=BRO_CONN icmp or tcp or udp srcip="172.16.150.20" (10) X groupby:program "172.16.150.20" (354) [Grouped by program] X

"172.16.150.20" program="bro_ftp" (4) X

Result Options... Field Summary
host(1) program(1) class(1) srcip(1) srcport(1) dstip(1) dstport(1) file_size(2) command(2) arg(4) mime_type(2) reply_msg(2)

Records: 4 / 4 493 ms 2 << first < prev 1 next > last >> 15

	Timestamp	Fields
Info	Mon Jan 13 14:33:04	1389623579.149410 CWJaTi4VKHixVWNGF6 172.16.150.20 1367 66.32.119.38 21 jack <hidden> PORT 172.16.150.20,5.89 1 200 PORT command successful. Consider using PASV. f 66.32.119.38 172.16.150.20 1369 - host=127.0.0.1 program=bro_ftp class=BRO_FTP srcip=172.16.150.20 srcport=1367 dstip=66.32.119.38 dstport=21 file_size=200 command=PORT arg=172.16.150.20 5.89 mime_type=- reply_msg=F
Info	Mon Jan 13 14:33:04	1389623579.149675 CWJaTi4VKHixVWNGF6 172.16.150.20 1367 66.32.119.38 21 jack <hidden> STOR ftp://66.32.119.38/.1.txt application/x-rar 226 Transfer complete. 1 1 FF2CIPXmfrisagya host=127.0.0.1 program=bro_ftp class=BRO_FTP srcip=172.16.150.20 srcport=1367 dstip=66.32.119.38 dstport=21 file_size=226 command=STOR arg=ftp://66.32.119.38/.1.txt mime_type=application/x-rar reply_msg=-
Info	Mon Jan 13 14:33:04	1389623579.208483 CWJaTi4VKHixVWNGF6 172.16.150.20 1367 66.32.119.38 21 jack <hidden> PORT 172.16.150.20,5.90 1 200 PORT command successful. Consider using PASV. f 66.32.119.38 172.16.150.20 1370 FF2CIPXmfrisagya host=127.0.0.1 program=bro_ftp class=BRO_FTP srcip=172.16.150.20 srcport=1367 dstip=66.32.119.38 dstport=21 file_size=200 command=PORT arg=172.16.150.20 5.90 mime_type=- reply_msg=F
Info	Mon Jan 13 14:33:04	1389623579.208781 CWJaTi4VKHixVWNGF6 172.16.150.20 1367 66.32.119.38 21 jack <hidden> STOR ftp://66.32.119.38/.2.txt 1 226 Transfer complete. 1 1 FF2CIPXmfrisagya host=127.0.0.1 program=bro_ftp class=BRO_FTP srcip=172.16.150.20 srcport=1367 dstip=66.32.119.38 dstport=21 file_size=226 command=STOR arg=ftp://66.32.119.38/.2.txt mime_type=- reply_msg=-

Records: 4 / 4 493 ms 2 << first < prev 1 next > last >> 15

Host Logs OSSEC Alerts

Interesting FTP Activity

[172.16.150.20:1367_66.32.119.38:21-6-382759083.pcap](#)

```
Sensor Name: doug-virtual-machine-eth1
Timestamp: 2014-01-11 16:16:40
Connection ID: CLI
Src IP: 172.16.150.20 (Unknown)
Dst IP: 66.32.119.38 (static-66-32-119-38.earthlinkbusiness.net)
Src Port: 1367
Dst Port: 21
OS Fingerprint: 172.16.150.20:1367 - Windows 2000 SP2+ XP SP1+ (seldom 98)
OS Fingerprint -> 66.32.119.38:21 (distance 0, link: ethernet/modem)
```

```
DST: 220 (vsFTPd 2.3.0)
DST:
SRC: USER jack
SRC:
DST: 331 Please specify the password.
DST:
SRC: PASS 2awes0me
SRC:
DST: 230 Login successful.
DST:
SRC: TYPE I
SRC:
DST: 200 Switching to Binary mode.
DST:
SRC: PORT 172.16.150.20,5.89
SRC:
DST: 200 PORT command successful. Consider using PASV.
DST:
SRC: STOR 1.txt
SRC:
DST: 150 Ok to send data.
DST:
DST: 226 Transfer complete.
DST:
SRC: TYPE A
SRC:
DST: 200 Switching to ASCII mode.
DST:
SRC: PORT 172.16.150.20,5.90
SRC:
DST: 200 PORT command successful. Consider using PASV.
DST:
SRC: STOR 2.txt
SRC:
DST: 150 Ok to send data.
DST:
DST: 226 Transfer complete.
DST:
SRC: QUIT
SRC:
DST: 221 Goodbye.
DST:
DEBUG: Using archived data: /nsm/server_data/securityonion/archive/2014-01-11/doug-virtual-machine-eth1/172.16.150.20:1367_66.32.119.38:21-6-382759083.pcap
QUERY: SELECT sid FROM sensor WHERE hostname='doug-virtual-machine-eth1' AND agent_type='pcap' LIMIT 1
172.16.150.20:1367_66.32.119.38:21-6-382759083.pcap
```

close

[172.16.150.20:1370_66.32.119.38:20-6-1492986788.pcap](#)

```
Sensor Name: doug-virtual-machine-eth1
Timestamp: 2014-01-11 16:16:40
Connection ID: CLI
Src IP: 172.16.150.20 (Unknown)
Dst IP: 66.32.119.38 (static-66-32-119-38.earthlinkbusiness.net)
Src Port: 1370
Dst Port: 20
OS Fingerprint: 66.32.119.38:20 - UNKNOWN [S4:63:1:60:M1460.S,T,N,W4:..??] (up: 71 hrs)
OS Fingerprint -> 172.16.150.20:1370 (link: ethernet/modem)
```

```
SRC: gsecdump v0.7 by Johannes Gumbel (johannes.gumbel@truesec.se)
SRC:
SRC: usage: gsecdump [options]
SRC:
SRC:
SRC: options:
SRC: -a [--dump_all] dump all secrets
SRC: -s [--dump_hashes] dump hashes from SAM/AD
SRC: -l [--dump_lsa] dump lsa secrets
SRC: -u [--dump_usedhashes] dump hashes from active logon sessions
SRC: -w [--dump_wireless] dump microsoft wireless connections
SRC: -h [--help] show help
SRC: -S [--system] run as localsystem
SRC:
```

```
DEBUG: Raw data request sent to doug-virtual-machine-eth1.
DEBUG: Making a list of local log files.
DEBUG: Looking in /nsm/sensor_data/doug-virtual-machine-eth1/dailylogs/2014-01-11.
DEBUG: Making a list of local log files in /nsm/sensor_data/doug-virtual-machine-eth1/dailylogs/2014-01-11.
DEBUG: Available log files:
DEBUG: 1389456708
DEBUG: Creating unique data file: /usr/sbin/tcpdump -r /nsm/sensor_data/doug-virtual-machine-eth1/dailylogs/2014-01-11/snort.log.1389456708 -w /tmp/172.16.150.20:1370_66.32.119.38:20-6.raw (ip and host 66.32.119.38 and host 172.16.150.20 and port 20 and port 1370 and proto 6) or (vlan and host 66.32.119.38 and host 172.16.150.20 and port 20 and port 1370 and proto 6)
DEBUG: Receiving raw file from sensor.
QUERY: SELECT sid FROM sensor WHERE hostname='doug-virtual-machine-eth1' AND agent_type='pcap' LIMIT 1
172.16.150.20:1370_66.32.119.38:20-6-1492986788.pcap
```

close

Interesting FTP Activity - RAR

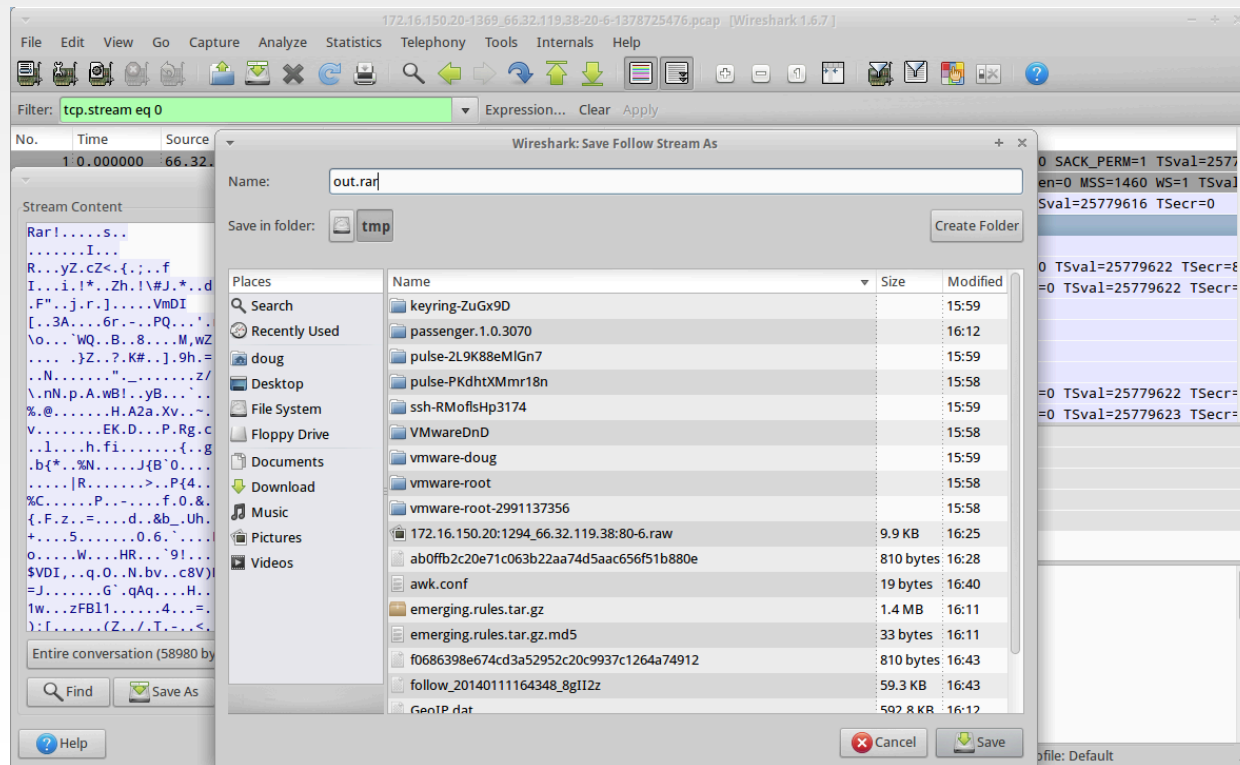
close

[172.16.150.20:1369_66.32.119.38:20-6-1378725476.pcap](#)

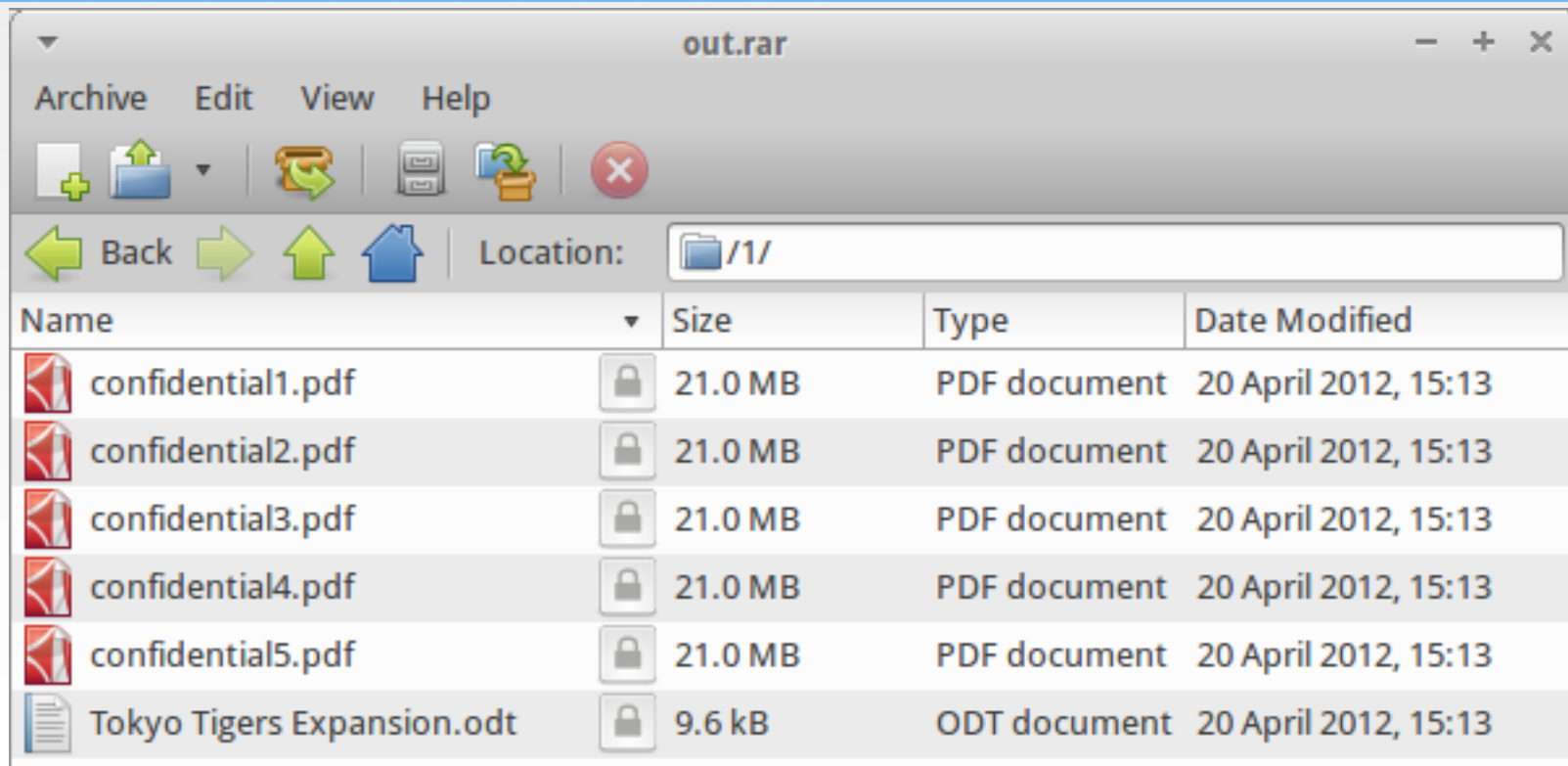
Sensor Name: doug-virtual-machine-eth1
Timestamp: 2014-01-11 16:16:40
Connection ID: CLI
Src IP: 172.16.150.20 (Unknown)
Dst IP: 66.32.119.38 (static-66-32-119-38.earthlinkbusiness.net)
Src Port: 1369
Dst Port: 20
OS Fingerprint: 66.32.119.38:20 - UNKNOWN [S4:63:1:60:M1460,S,T,N,W4::?:?] (up: 71 hrs)
OS Fingerprint -> 172.16.150.20:1369 (link: ethernet/modem)

```
SRC: Rar!....s..
SRC: .....l...
SRC: R...yZ.cZ<{;...f
SRC: l...i!*.Zh.!#J*.d.1...f_.....5.;0...K..
SRC: .F'.j.r.]....VmDl[.3A...6r-.PQ...'r.N...-DR.N..AW8*U...j.?z.<.d.mNrLIA..ZG.C...i.Ii.Q\o...'WQ..B.8...M,wZ_..X'...e]wG...m....d"q.....G..V.T
SRC: ....jZ..?.K#.].9h.=.QuP.
SRC: .N.....": .....z/.B.g...0...v.....3...s.1.-\nN.p.A.wB!.yB...`&X.....".L|j..ZJ].%.@.....H.A2a.Xv.~.....<.-.SV.K..Wq/... J..&....z.....'a...= ;G=v.....EK.D...P.Rg.c..3..j.l...
```


Extract the RAR



What's in the RAR?



The screenshot shows a RAR archive viewer window titled "out.rar". The window has a menu bar with "Archive", "Edit", "View", and "Help". Below the menu bar is a toolbar with icons for adding files, folders, and deleting. The location bar shows the path "/1/". The main area displays a list of files with columns for Name, Size, Type, and Date Modified.

Name	Size	Type	Date Modified
confidential1.pdf	21.0 MB	PDF document	20 April 2012, 15:13
confidential2.pdf	21.0 MB	PDF document	20 April 2012, 15:13
confidential3.pdf	21.0 MB	PDF document	20 April 2012, 15:13
confidential4.pdf	21.0 MB	PDF document	20 April 2012, 15:13
confidential5.pdf	21.0 MB	PDF document	20 April 2012, 15:13
Tokyo Tigers Expansion.odt	9.6 kB	ODT document	20 April 2012, 15:13

Future of Security Onion

- More documentation
 - Best practices
 - Tuning
- Web interface for administration
- More/better integration with Argus?
- Add Silk?
- Others?

Where do we go now?

<http://securityonion.net>

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

- Download/Install
- FAQ
- Mailing Lists
- IRC #securityonion on irc.freenode.net
- @securityonion
- Security Onion classes throughout 2014!