

Intro

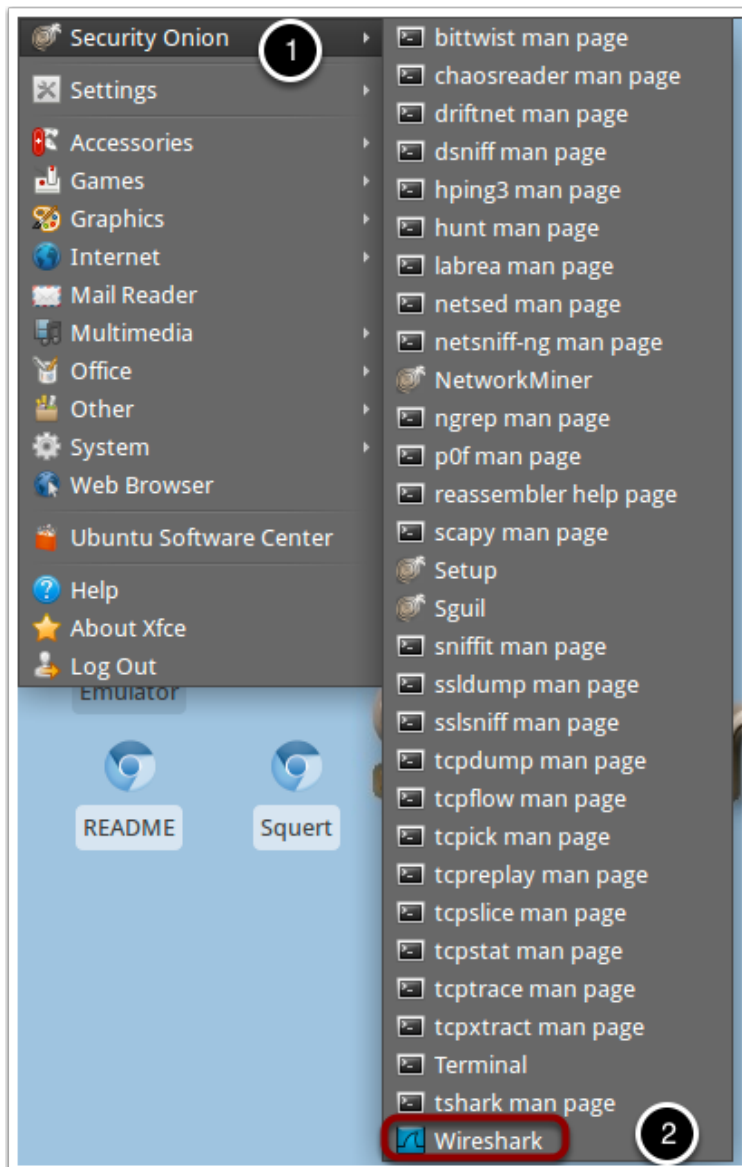
Security Onion has a variety of traffic analysis tools. In this lab you will be introduced to these tools and complete your own analysis of a traffic capture (pcap) file.

Note on questions: The submission requirements for the lab are on the last page. During the lab you will be asked several questions. You are encouraged to consider these questions but you don't have to submit a response. The Professor may bring these up in class or during online sessions.

Wireshark

Wireshark is a network traffic capture and analysis tool with a nice visual interface.

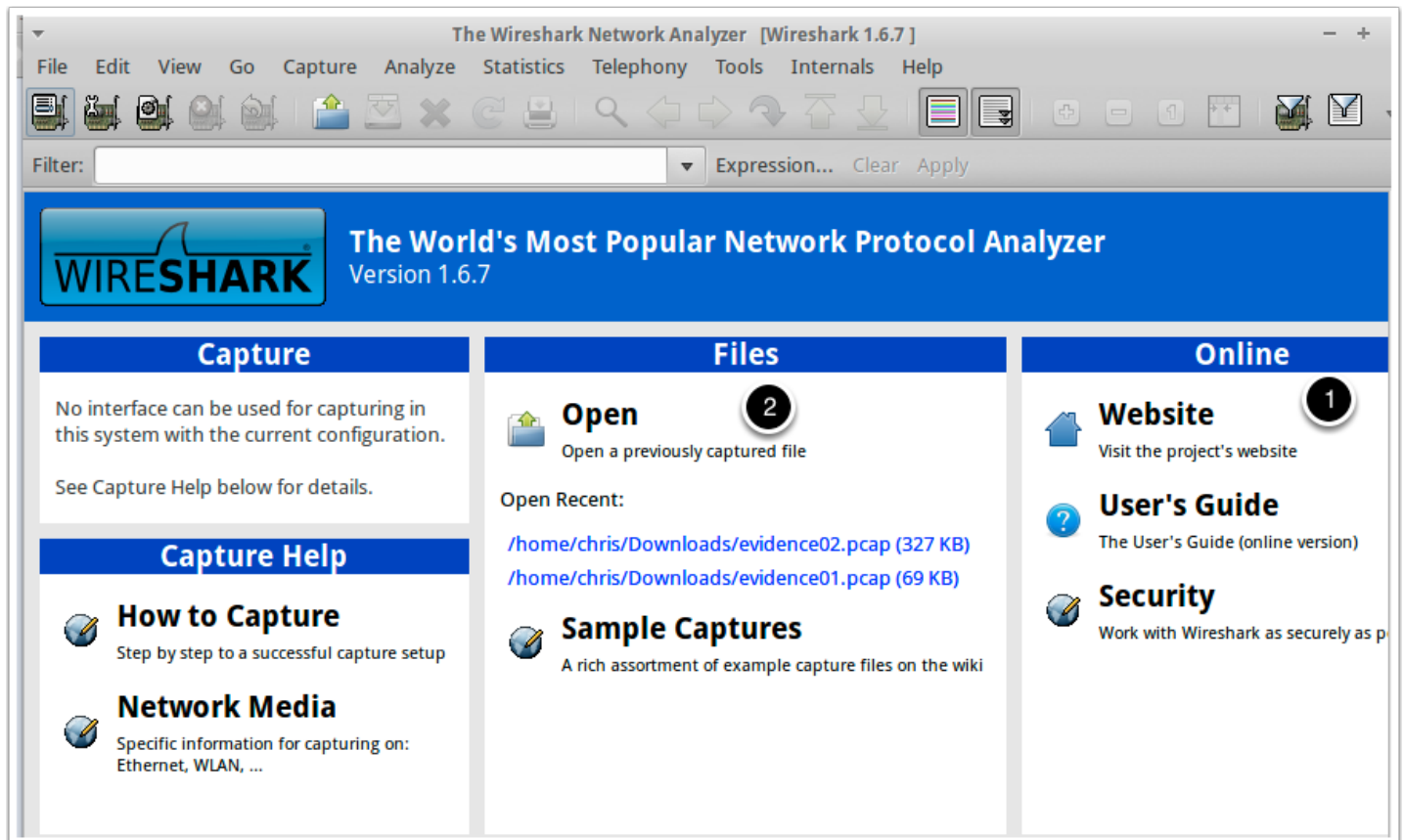
1. Click on the Security Onion menu in the top left corner.
2. Note the large number of tools.
3. Select Wireshark (Note: Wireshark is also available from the Internet menu item).



Wireshark

This is the opening screen for Wireshark.

1. This is where you can find help online.
2. This is where you open pcap files.

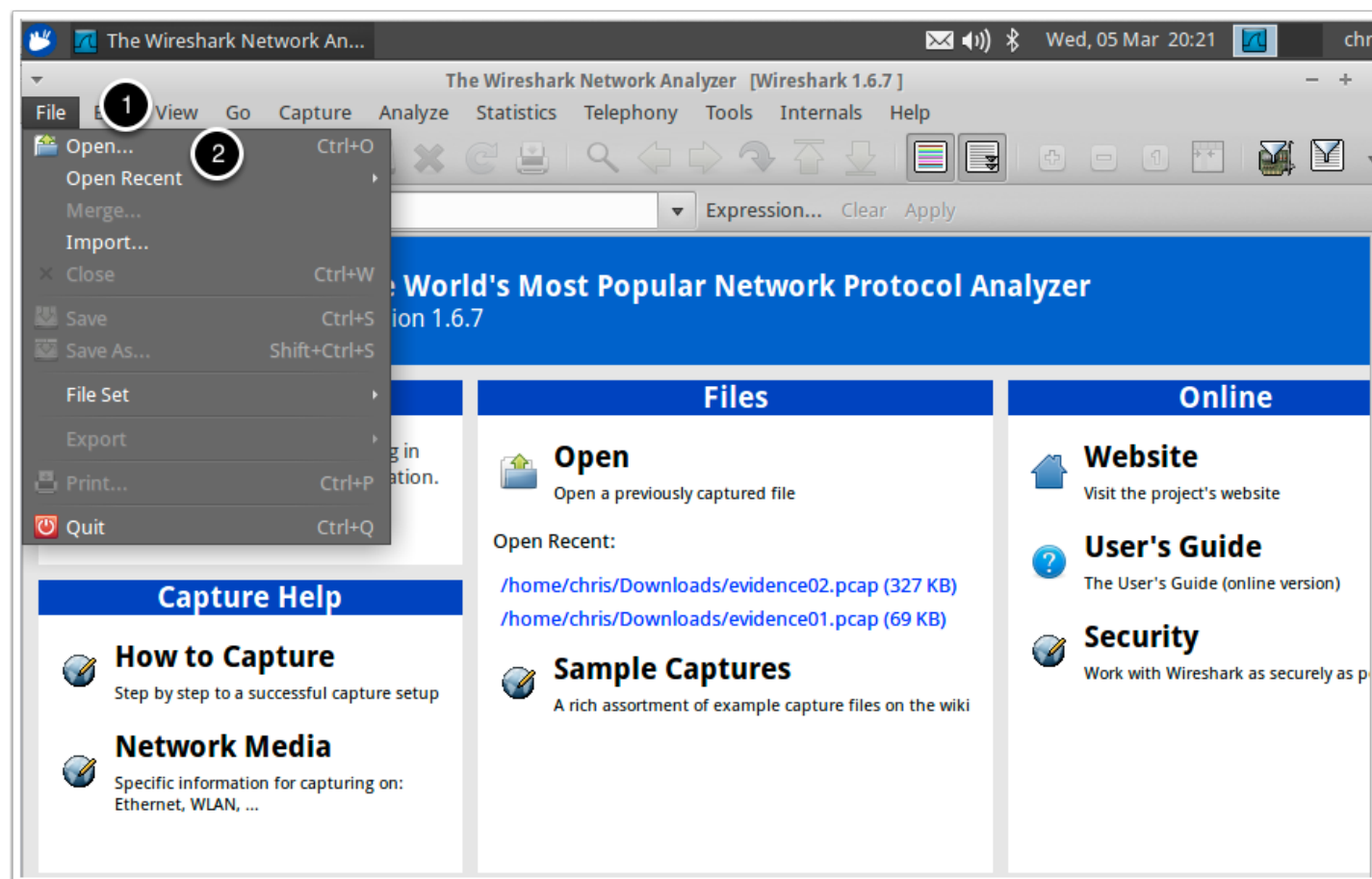


Open pcap file

To see the power of Wireshark, we'll open a pcap file from a Network Forensics contest. You can read about the scenario at this link: <http://forensicscontest.com/2009/09/25/puzzle-1-anns-bad-aim>. This first scenario is a demo, at the end of the lab you will be asked to complete another scenario using the tools we discuss.

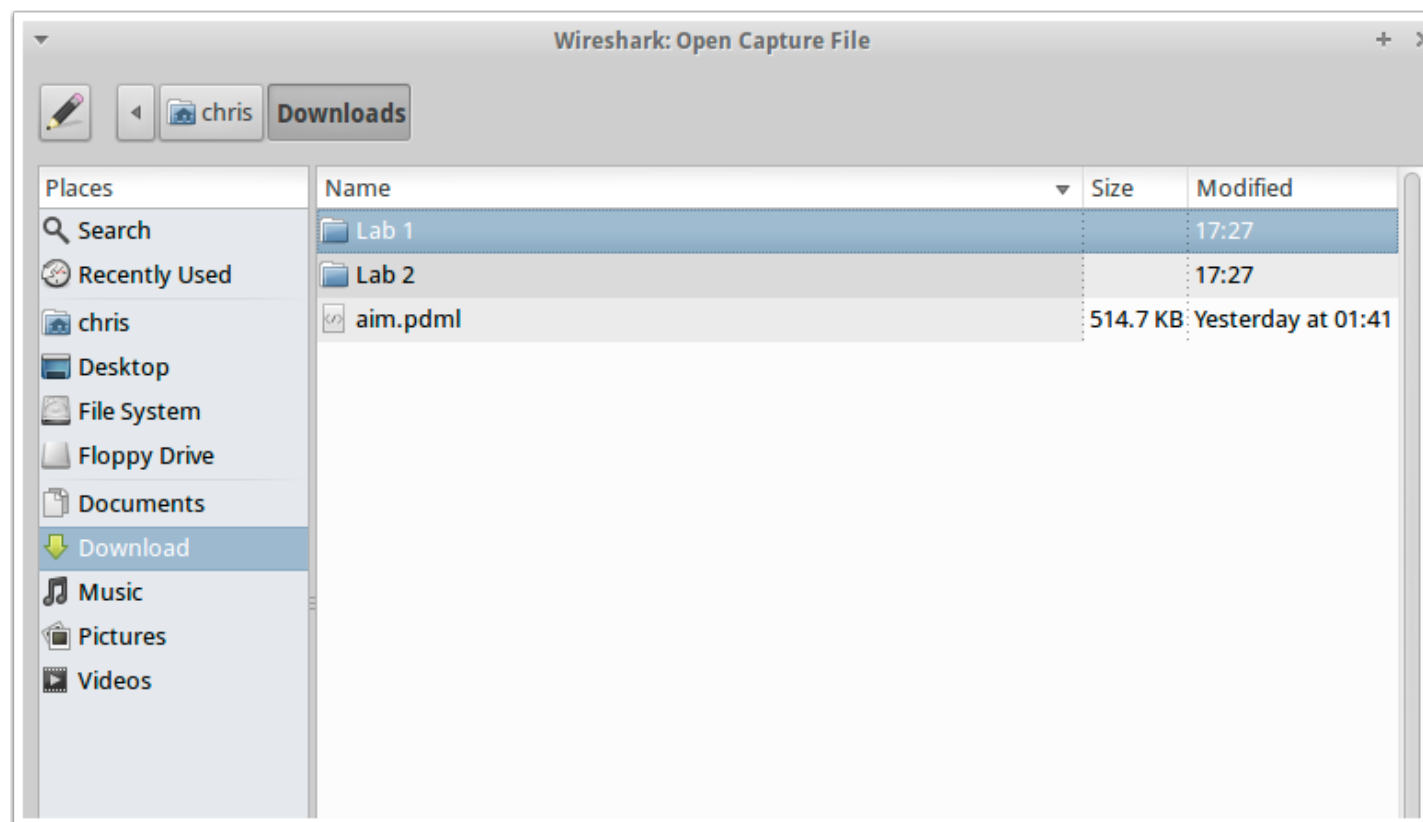
To open a pcap file:

1. Click file
2. Click Open



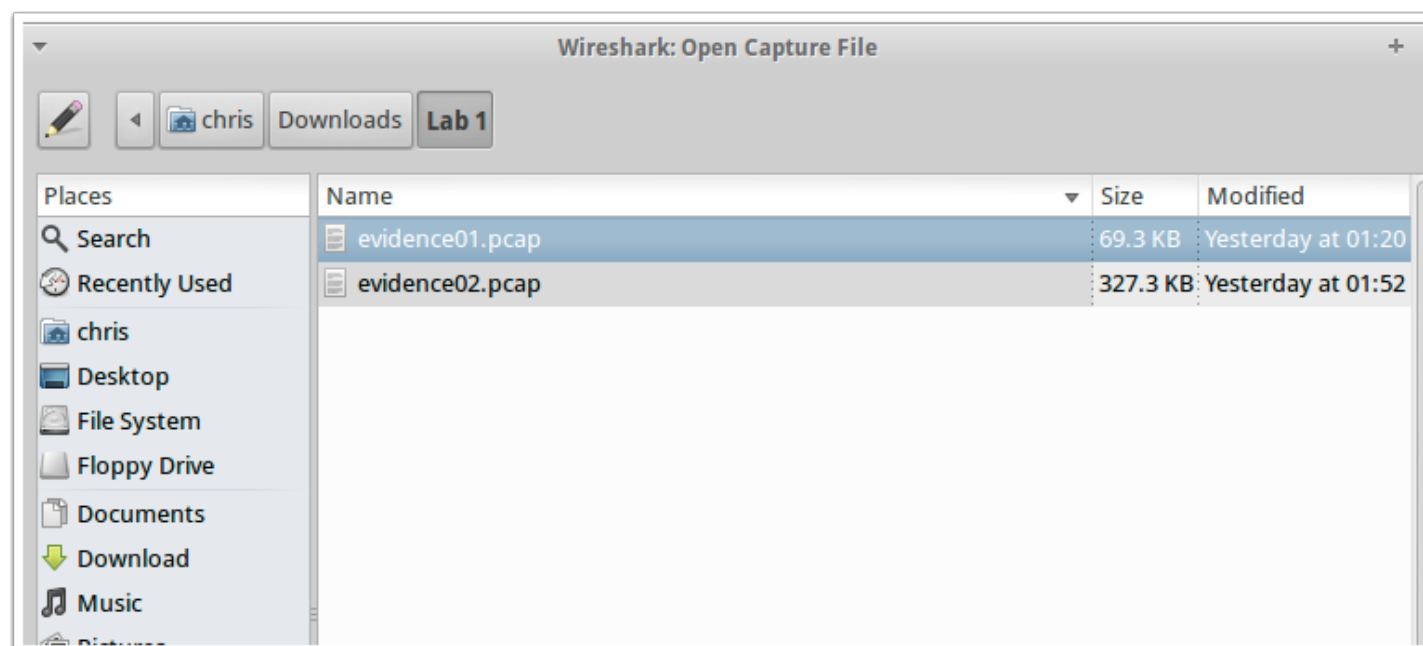
Open PCAP File

Go to the Download/Lab 1 Directory



Open PCAP file

Select evidence01.pcap file and click open



Traffic Capture

Notice the 7 columns on the main screen. You can sort each column by selecting it. This feature is useful when you are conducting your initial assessment of an incident.

Sort by source IP and see if you can find the IP of interest.

Wireshark 1.6.7 interface showing a packet capture of evidence01.pcap. The packet list shows 12 packets. Packet 3 is selected, showing details of a TCP ACK segment. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.2	192.168.1.30	TCP	66	55488 > ssh [ACK] Seq=1 Ack=1 Win=1002 Len=0 TS=
2	0.000004	192.168.1.30	192.168.1.2	SSH	114	Encrypted response packet len=48
3	0.003178	192.168.1.2	192.168.1.30	TCP	66	[TCP ACKed lost segment] 55488 > ssh [ACK] Seq=
4	0.003184	192.168.1.30	192.168.1.2	SSH	178	[TCP Retransmission] Encrypted response packet
5	0.918234	Vmware_b0:8d:62	Dell_4d:4f:ae	ARP	60	who has 192.168.1.159? Tell 192.168.1.10
6	0.918240	Dell_4d:4f:ae	Vmware_b0:8d:62	ARP	60	192.168.1.159 is at 00:21:70:4d:4f:ae
7	3.185626	192.168.1.30	192.168.1.10	NTP	90	NTP Version 4, client
8	3.186114	192.168.1.10	192.168.1.30	NTP	90	NTP Version 4, server
9	4.680216	192.168.1.10	192.168.1.255	NTP	90	NTP Version 4, broadcast
10	8.181469	Vmware_69:e6:2b	Vmware_b0:8d:62	ARP	60	who has 192.168.1.10? Tell 192.168.1.30
11	8.181738	Vmware_b0:8d:62	Vmware_69:e6:2b	ARP	60	192.168.1.10 is at 00:0c:29:b0:8d:62
12	11.909351	Vmware_c0:00:02	Broadcast	ARP	60	who has 192.168.1.157? Tell 192.168.1.2

Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)

Ethernet II, Src: Vmware_c0:00:02 (00:50:56:c0:00:02), Dst: Vmware_69:e6:2b (00:0c:29:69:e6:2b)

Internet Protocol Version 4, Src: 192.168.1.2 (192.168.1.2), Dst: 192.168.1.30 (192.168.1.30)

Transmission Control Protocol, Src Port: 55488 (55488), Dst Port: ssh (22), Seq: 1, Ack: 1, Len: 0

```

0000  00 0c 29 69 e6 2b 00 50 56 c0 00 02 08 00 45 10  ..)i.+P V....E.
0010  00 34 d3 a8 40 00 40 06 e3 9a c0 a8 01 02 c0 a8  .4..@.@. ....
0020  01 1e d8 c0 00 16 33 09 5e a5 5a 1e 27 43 80 10  .....3. ^.Z.'C..
0030  03 ea 48 54 00 00 01 01 08 0a 1d c1 35 0c 0b 0e  ..HT.... ..5...
  
```

Sorted by IP

Your screen should look like this

Wireshark 1.6.7 interface showing a packet capture sorted by IP. The packet list shows several SSL and TCP packets, with two SSDP packets highlighted in green. The packet details pane shows the structure of the first packet (Frame 1), including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
23	18.870898	192.168.1.158	64.12.24.50	SSL	60	Continuation Data
25	33.914966	192.168.1.158	64.12.24.50	SSL	243	Continuation Data
27	34.006599	192.168.1.158	64.12.24.50	SSL	94	Continuation Data
32	34.026804	192.168.1.158	64.12.24.50	TCP	60	51128 > https [ACK] Seq=236 Ack=210 Win=
33	34.026809	192.168.1.158	64.12.24.50	TCP	60	51128 > https [ACK] Seq=236 Ack=248 Win=
90	56.425051	192.168.1.158	239.255.255.250	SSDP	174	M-SEARCH * HTTP/1.1
91	57.427165	192.168.1.158	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
92	58.458768	192.168.1.158	64.12.24.50	SSL	182	Continuation Data
96	58.569716	192.168.1.158	64.12.24.50	TCP	60	51128 > https [ACK] Seq=364 Ack=457 Win=
98	58.574447	192.168.1.158	64.12.24.50	TCP	60	51128 > https [ACK] Seq=364 Ack=495 Win=
110	61.052930	192.168.1.158	192.168.1.159	TCP	62	aol > cspmlockmgr [SYN, ACK] Seq=0 Ack=1
112	61.054884	192.168.1.158	192.168.1.159	TCP	310	aol > cspmlockmgr [PSH, ACK] Seq=1 Ack=1

► Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)

► Ethernet II, Src: Vmware_c0:00:02 (00:50:56:c0:00:02), Dst: Vmware_69:e6:2b (00:0c:29:69:e6:2b)

► Internet Protocol Version 4, Src: 192.168.1.2 (192.168.1.2), Dst: 192.168.1.30 (192.168.1.30)

► Transmission Control Protocol, Src Port: 55488 (55488), Dst Port: ssh (22), Seq: 1, Ack: 1, Len: 0

```

0000  00 0c 29 69 e6 2b 00 50 56 c0 00 02 08 00 45 10  ..)i.+P V.....E.
0010  00 34 d3 a8 40 00 40 06 e3 9a c0 a8 01 02 c0 a8  .4..@.@. ....
0020  01 1e d8 c0 00 16 33 09 5e a5 5a 1e 27 43 80 10  .....3. ^.Z.'C..
0030  03 ea 48 54 00 00 01 01 08 0a 1d c1 35 0c 0b 0e  ..HT.... ....5...
  
```

Follow TCP stream

1. Right click the first entry for 192.168.1.158

2. Select Follow TCP Stream.

This will show the tcp stream for that connection.

The image shows a Wireshark packet capture interface. The packet list pane on the left shows several packets. Packet 239 is selected, and a context menu is open over it. The menu options include: Mark Packet (toggle), Ignore Packet (toggle), Set Time Reference (toggle), Manually Resolve Address, Apply as Filter, Prepare a Filter, Conversation Filter, Colorize Conversation, Sctp, Follow TCP Stream (highlighted with a red circle and the number 2), Follow UDP Stream, Follow SSL Stream, Copy, Decode As..., Print..., and Show Packet in New Window. The packet details pane on the right shows the structure of the selected packet: Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The packet bytes pane at the bottom shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
131	61.811479	192.168.1.157	192.168.1.255	NBNS	110	Registration NB SANS<1e>
152	63.625917	192.168.1.157	192.168.1.255	NBNS	110	Registration NB HERBIVORE<20>
153	63.627865	192.168.1.157	192.168.1.255	NBNS	110	Registration NB HERBIVORE<03>
154	63.629367	192.168.1.157	192.168.1.255	NBNS	110	Registration NB HERBIVORE<00>
155	63.631162	192.168.1.157	192.168.1.255	NBNS	110	Registration NB SANS<00>
156	63.632793	192.168.1.157	192.168.1.255	NBNS	110	Registration NB SANS<1e>
209	90.000408	192.168.1.157	192.168.1.255	NBNS	92	Name query NB SANS<1d>
221	92.007474	192.168.1.157	192.168.1.255	NBNS	92	Name query NB SANS<1d>
222	92.008941	192.168.1.157	192.168.1.255	NBNS	92	Name query NB SANS<1d>
239	94.250094	192.168.1.157	192.168.1.255	NBNS	92	Name query NB SANS<1d>
243	18.870898	192.168.1.157	192.168.1.255	SSL	60	Continuation Data
253	33.914966	192.168.1.157	192.168.1.255	SSL	243	Continuation Data
273	34.006500	192.168.1.157	192.168.1.255	SSL	64	Continuation Data

Context Menu Options:

- Mark Packet (toggle)
- Ignore Packet (toggle)
- Set Time Reference (toggle)
- Manually Resolve Address
- Apply as Filter
- Prepare a Filter
- Conversation Filter
- Colorize Conversation
- Sctp
- Follow TCP Stream
- Follow UDP Stream
- Follow SSL Stream
- Copy
- Decode As...
- Print...
- Show Packet in New Window

Packet Details:

- Frame 23: 60 bytes captured (480 bits) on interface 0
- Ethernet II, Src: Vmware_b0:8d:62 (00:0c:29:b0:8d:62), Dst: Vmware_b0:8d:62 (00:0c:29:b0:8d:62)
- Internet Protocol Version 4, Src: 192.168.1.157, Dst: 192.168.1.255
- Transmission Control Protocol, Src Port: 51128, Dst Port: https (443), Seq: 1, Ack: 1, Len: 6

Packet Bytes:

```

0000  00 0c 29 b0 8d 62 00 00 00 00 00 00 00 00 00 00  ..).b...yE...E.
0010  00 2e ab 3b 00 00 00 00 00 00 00 00 00 00 00 00  ...;@.u.....@.
0020  18 32 c7 b8 00 00 00 00 00 00 00 00 00 00 00 00  .2....3k.....P.
0030  f5 3c 3d 39 00 00 2a 05 00 60 00 00 00 00 00 00  .<=9..*.
  
```


TCP Stream

This is an example of the TCP stream. Do you see any answers to the problem?

1. Possible IM user name
2. Possible IM comment
3. Possible file name

As you scroll through the capture you'll notice some SSL traffic. Any idea why you can read the IM?

Follow TCP Stream

Stream Content

```
*...*.a.....E4628778... Sec558user1.....Here's the secret
recipe... I just downloaded it from the file server. Just copy to a thumb drive and
you're good to go &gt;:-)....*.b.".....F.....Sec558user1...*.V.....
...*.A.....E.....P.....p...p.....P.....p...
p.&.'.....U4.....|.....h.....p...@.&.'.....
...|.....h.....p...@.&.'*.V.....E4628778...Sec558user1*..c.z.....G71746
47...Sec558user1...R...7174647..F.CL..."DEST.....F.
.....'.recipe.docx.'.V.....
...*.c.....p...p..._w.....P.....p...
p.&a.....U.....|.....h.....p...@.&a.....
...|.....h.....p...@.&a.*.V.....G7174647...Sec558user1*.V..
{.....*.7174647...Sec558user1.....J.H.....+.1n....
+...O.....J.....7174647..F.CL..."DEST.....*.V..".....*.1.....Sec55
8user1..*.V.....*.y..N...w...Sec558user1.....J.H.....+.1n....
+...O.....J.....a.....X...<HTML><BODY><FONT FACE="Arial" SIZE=2
COLOR=#000000>thanks dude</FONT></BODY></HTML>.
.....+.1n....+.O.....*.V..".....*.Sec558user1..*.V.....
+.Q....L....Sec558user1.....J.H.....+.1n....
+...O.....J.....s.....j...<HTML><BODY><FONT FACE="Arial" SIZE=2
COLOR=#000000>can't wait to sell it on ebay</FONT></BODY></HTML>.
.....+.1n....+.O.....*.V..".....+
.....Sec558user1..*.V..".....
+.....Sec558user1..*..d..".....H.....Sec558user1..*..e.J.....I50884
```

Entire conversation (2023 bytes)

Find Save As Print ASCII EBCDIC Hex Dump C Arrays Raw

Help Filter Out This Stream Close

TCP Stream

1. You can see the type of file transfer here (This is a different stream)
Click through the traffic and look at some of the other streams.

Follow TCP Stream

Stream Content

```

OFT2...d...Cool
FileXfe
r...
recipe.docx...OFT2...717464
7...d...Cool
FileXfe
r...
recipe.docx...PK...!|..
=.....[Content_Types].xml ...
(.....
Ik.0.....k...PJ..C.c.h
...8...4...}.NbJ..6.b.f....H....d.!*gs..z,..+]..$g....
%...-v.r.....`.....1gSD..y.S0"f...?..F ...
{!...m.w.....S.....JHF"..0...,3.Fs.`F.....uum g.
{..@.....N]U)...3C.Y..y.PA.....<A%f...%Y[...@...m.....w)t..qv(...%o.....$.Hs7:k.F
(.M....+
....Xs...g.....l}.'_B.R.;.q.u@.....~..Hw.x.=..4.....pv.
{3o.'M,...b...w.i.O..0..E}}`.x...?.....PK.....!.....N....._rels/.rels ...
(.....
J.A.....a.}7.
"...H.w".....w......P.^....O.....;<..aY....`G.kxm...PY.[...g
G..ino./<...<.1.....A$>"f3..\...T...I.S.....W.....Y
  
```

Entire conversation (12776 bytes)

Find Save As Print ASCII EBCDIC Hex Dump C Arrays ☒ Raw

Help Filter Out This Stream Close

Filters

Instead of sorting we could have filtered the traffic for the IP address of interest.

1. Filter for IP address

See the Wireshark manual for filter syntax, you can get very robust with filters. Keep this in mind if you need to find specific traffic like SMTP or DNS

Wireshark 1.6.7 interface showing a packet capture filter for IP address 192.168.1.159. The packet list shows a DNS response and several TCP connections to cspmlockmgr. The packet details pane shows the structure of frame 226, including Ethernet II, IP, and DNS. The packet bytes pane shows the raw hex and ASCII data.

No.	Time	Source	Destination	Protocol	Length	Info
226	93.347300	10.1.1.20	192.168.1.159	DNS	465	Standard query response CNAME glb-at.atwola.adt
110	61.052930	192.168.1.158	192.168.1.159	TCP	62	ao1 > cspmlockmgr [SYN, ACK] Seq=0 Ack=1 Win=58
112	61.054884	192.168.1.158	192.168.1.159	TCP	310	ao1 > cspmlockmgr [PSH, ACK] Seq=1 Ack=1 Win=58
118	61.155760	192.168.1.158	192.168.1.159	TCP	60	ao1 > cspmlockmgr [ACK] Seq=257 Ack=257 Win=643
119	61.270615	192.168.1.158	192.168.1.159	TCP	1514	ao1 > cspmlockmgr [ACK] Seq=257 Ack=257 Win=643
120	61.270620	192.168.1.158	192.168.1.159	TCP	1514	ao1 > cspmlockmgr [ACK] Seq=1717 Ack=257 Win=64
122	61.270628	192.168.1.158	192.168.1.159	TCP	1230	ao1 > cspmlockmgr [PSH, ACK] Seq=3177 Ack=257 W
123	61.270632	192.168.1.158	192.168.1.159	TCP	1514	ao1 > cspmlockmgr [ACK] Seq=4353 Ack=257 Win=64
124	61.270635	192.168.1.158	192.168.1.159	TCP	1514	ao1 > cspmlockmgr [ACK] Seq=5813 Ack=257 Win=64
126	61.270641	192.168.1.158	192.168.1.159	TCP	1514	ao1 > cspmlockmgr [ACK] Seq=7273 Ack=257 Win=64
127	61.270644	192.168.1.158	192.168.1.159	TCP	1514	ao1 > cspmlockmgr [ACK] Seq=8733 Ack=257 Win=64
128	61.270647	192.168.1.158	192.168.1.159	TCP	358	ao1 > cspmlockmgr [PSH, ACK] Seq=10193 Ack=257

Frame 226: 465 bytes on wire (3720 bits), 465 bytes captured (3720 bits)

- Ethernet II, Src: Vmware_b0:8d:62 (00:0c:29:b0:8d:62), Dst: Dell_4d:4f:ae (00:21:70:4d:4f:ae)
- Internet Protocol Version 4, Src: 10.1.1.20 (10.1.1.20), Dst: 192.168.1.159 (192.168.1.159)
- User Datagram Protocol, Src Port: domain (53), Dst Port: cardax (1072)
- Domain Name System (response)

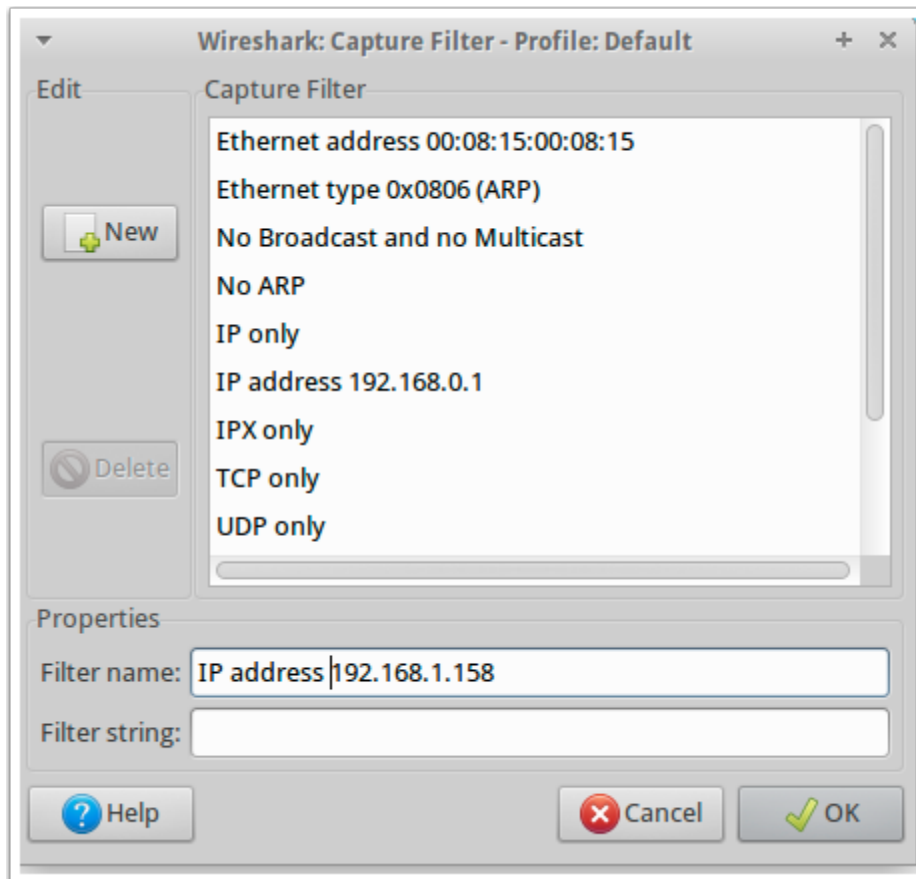
```

0000  00 21 70 4d 4f ae 00 0c 29 b0 8d 62 08 00 45 00  .!pMO... )..b..E.
0010  01 c3 00 00 40 00 3f 11 6c ce 0a 01 01 14 c0 a8  ....@.? l.....
0020  01 9f 00 35 04 30 01 af d4 ab d5 bd 81 80 00 01  ...5.0.. ....
0030  00 03 00 06 00 08 02 61 74 06 61 74 77 6f 6c 61  .....a t.atwola
0040  03 63 6f 6d 00 00 01 00 01 c0 0c 00 05 00 01 00  .com.... ....
0050  00 03 6f 00 19 06 67 6c 62 2d 61 74 06 61 74 77  ..o...gl b-at.atw
0060  6f 6c 61 08 61 64 74 65 63 68 75 73 c0 16 c0 2b  ola.adte chus...+
0070  00 01 00 01 00 00 00 21 00 04 40 ec 44 f6 c0 2b  ....! ..@.D...+
0080  00 01 00 01 00 00 00 21 00 04 40 ec 44 f5 c0 39  ....! ..@.D...9
0090  00 02 00 01 00 01 38 b8 00 14 05 70 64 6e 73 34  ....8. ...pdns4
  
```

File: "/home/chris/Downloads/evidenc... Packets: 240 Displayed: 135 Marked: 0 Load time: 0:00.003 Profile: Default

Capture Filters

Although we won't use it in this class, you can also set filters for traffic capture for IP address or type of traffic. This can help reduce the extra information you collect.



Close Wireshark

Close Wireshark prior to opening Network Miner

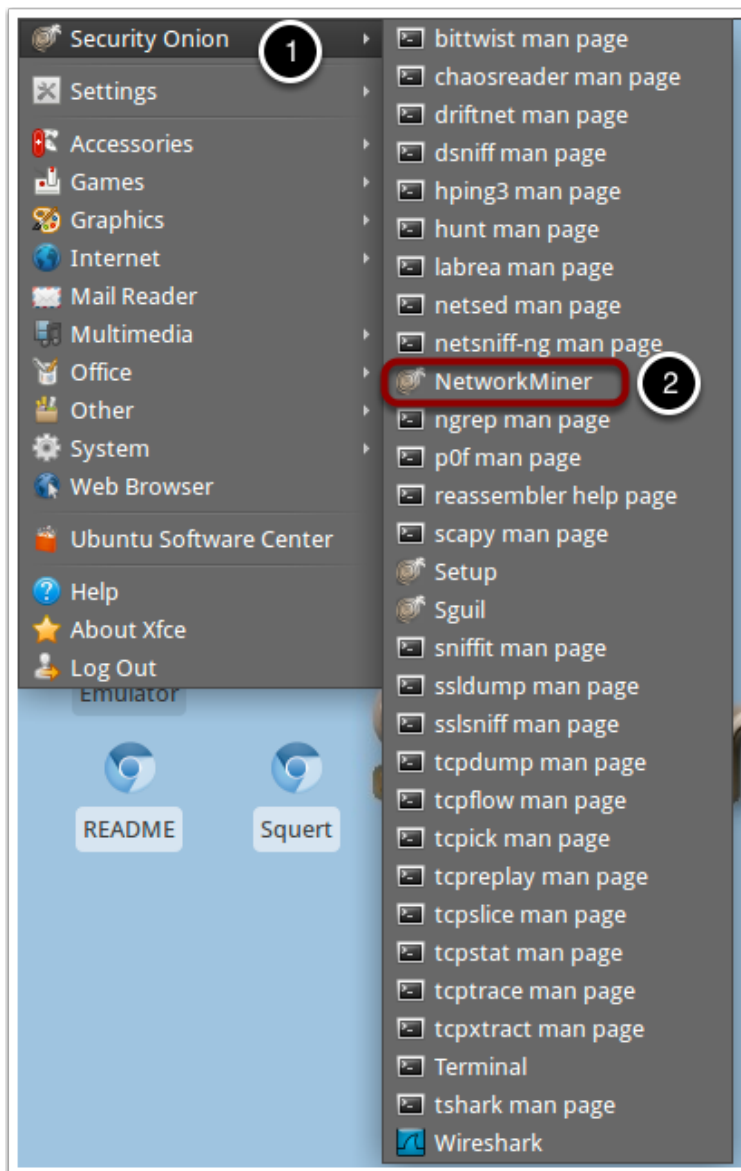
Network Miner

Network Miner is another great open source network analysis tool.

1. Go to the Security Onion menu

2. Click on Network Miner

****Note:** Sometimes it takes several minutes for Network Miner to open. Make sure all other programs are closed before starting Network Miner.**

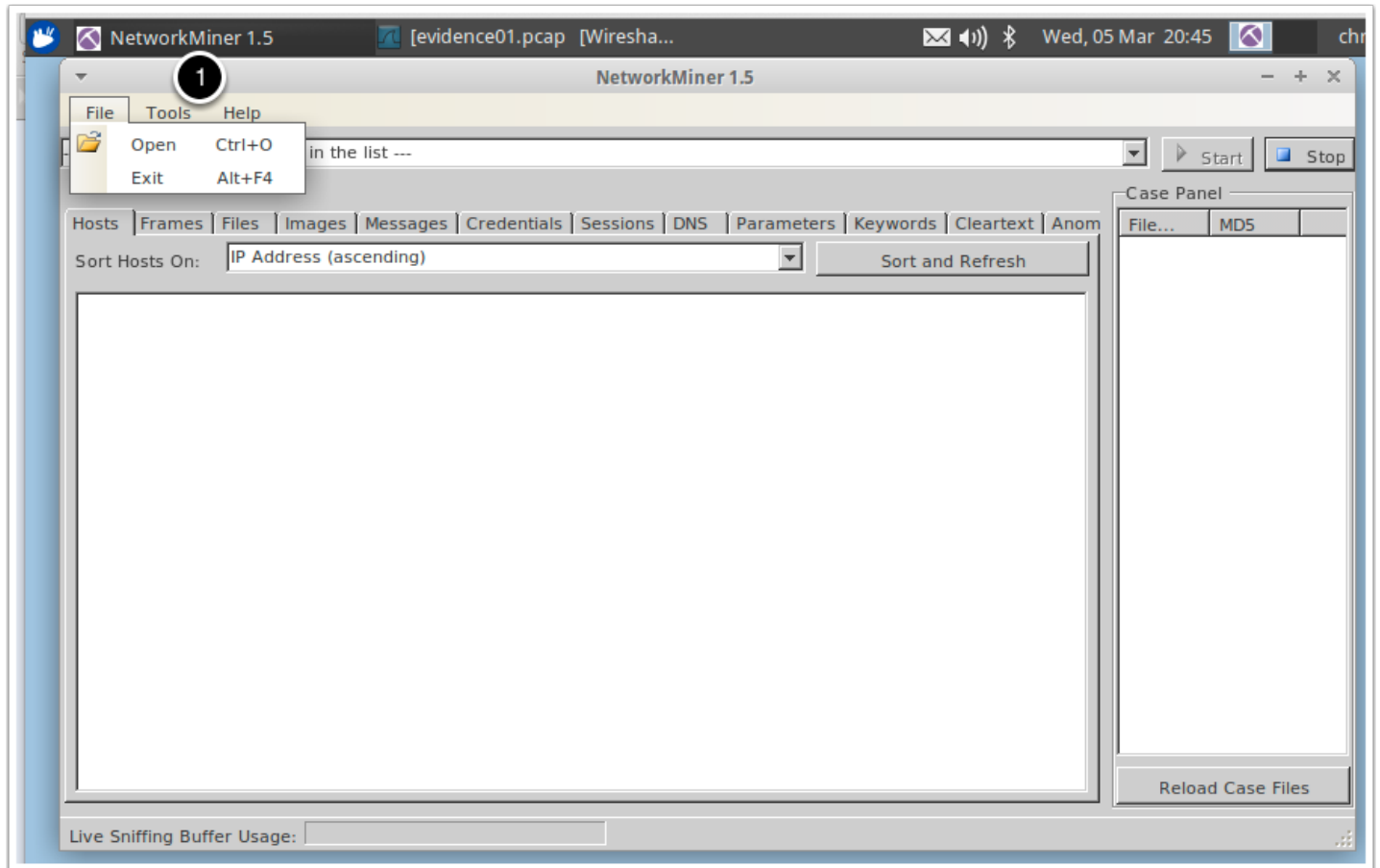


Network Miner

Open the same pcap file

1. Click File > Open

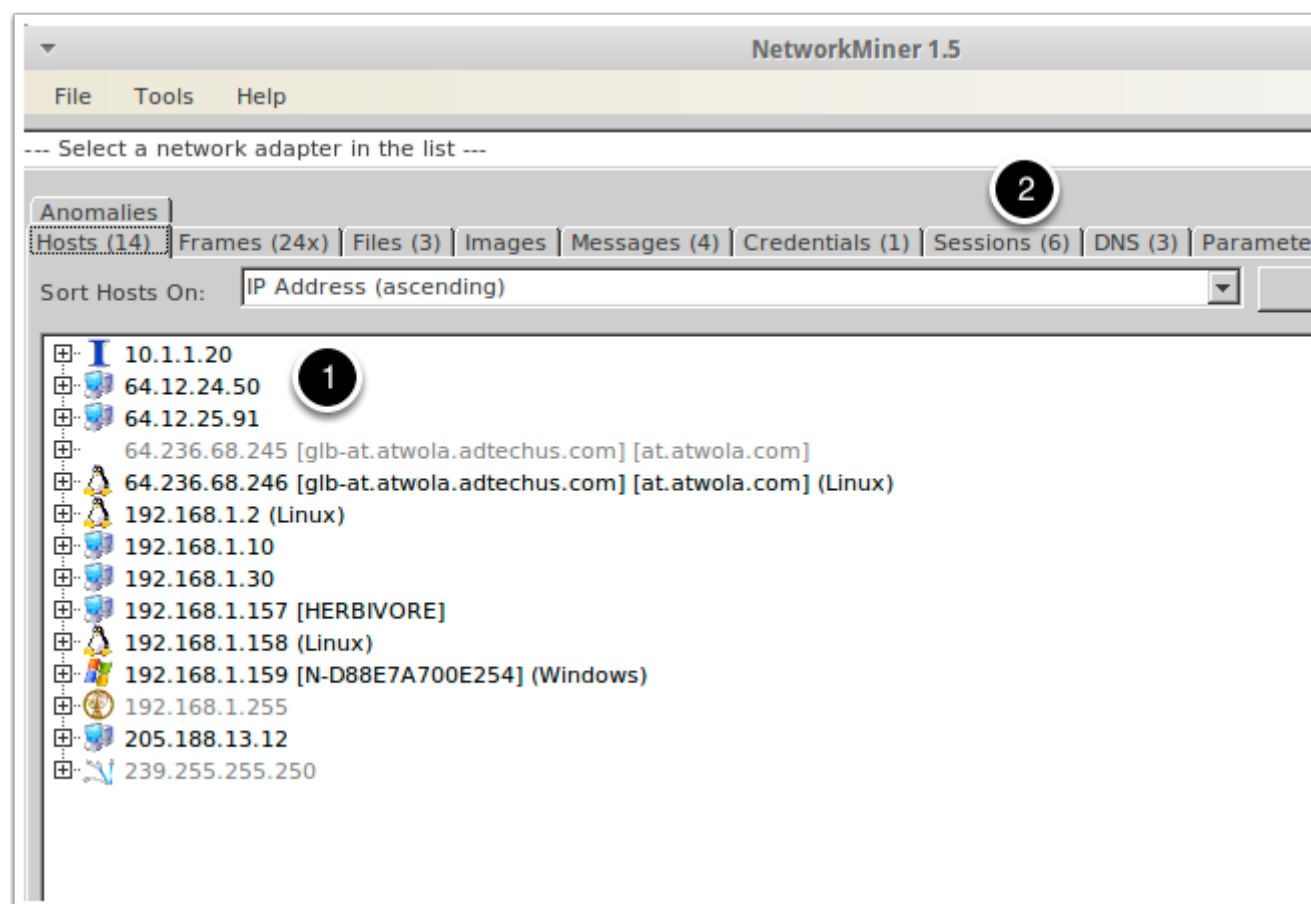
File is /Downloads/Lab 1/evidence01.pcap (same as previous exercise)



Network Miner

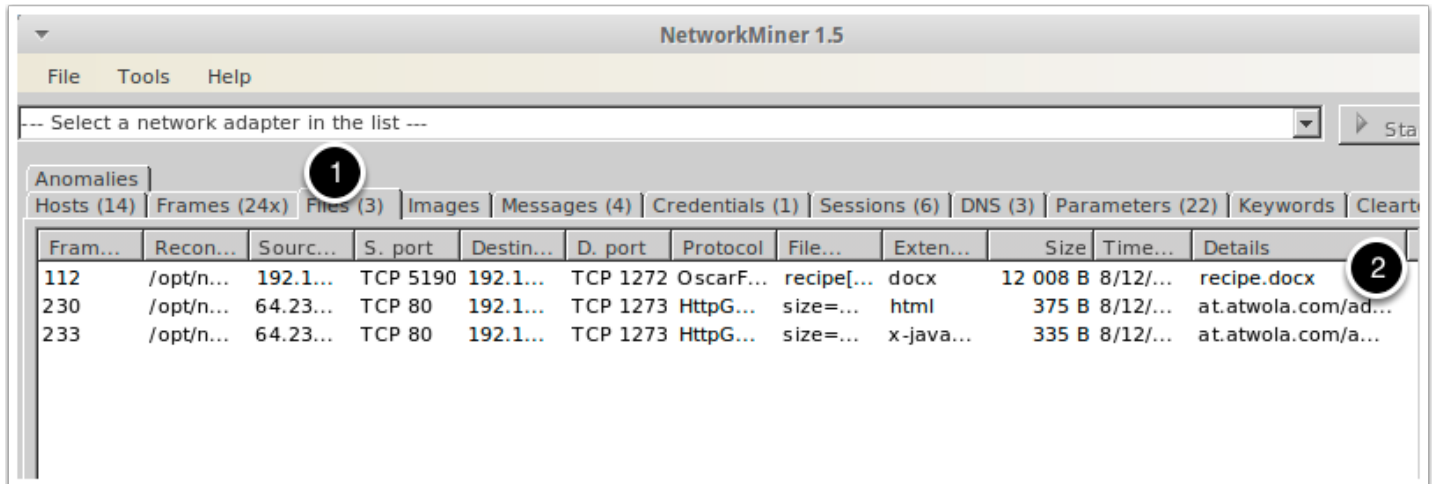
As you can see Network Miner parses the pcap file for you. You can see the different IP addresses from the capture.

1. Click on the + sign to see more information about each capture
2. Note the other information on the tabs along the top. Network Miner will extract files, messages, and credentials from the capture.



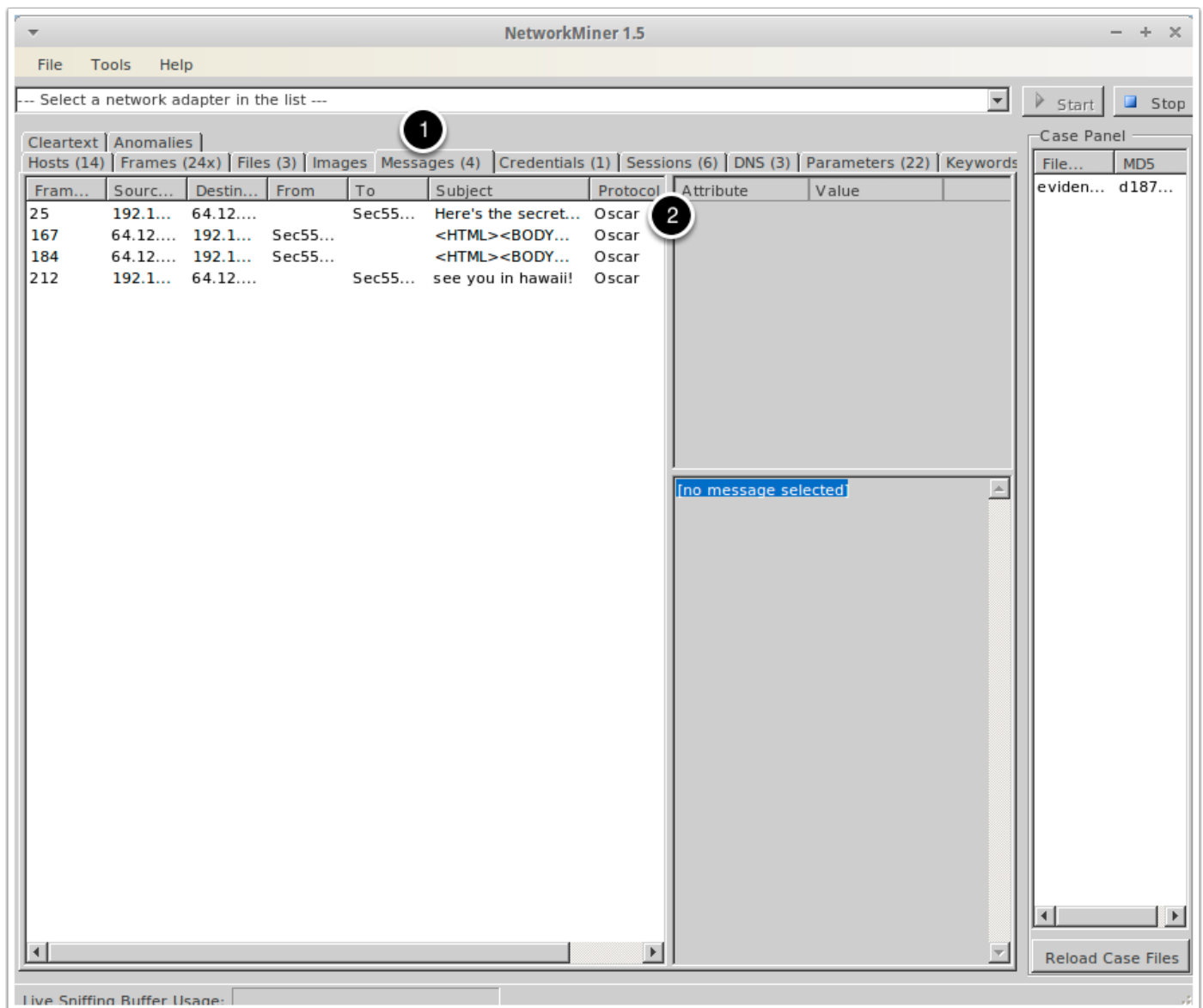
Network Miner File Extraction

1. Click on the File tab
2. Note the file of interest. You can open this file with Word or OpenOffice



Messages

1. Click the Messages tab
2. Network Miner extracted the messages for you.
3. Explore the other tabs and connections



Close Network Miner

Close Network Miner prior to opening Sguil

Sguil and Snorby

Next we'll take a look at using Sguil and Snorby. In a business environment you would configure security onion to capture and monitor all traffic. For our lab, we'll replay pcap files to the sensor can detect the traffic.

First double click on the Sguil icon

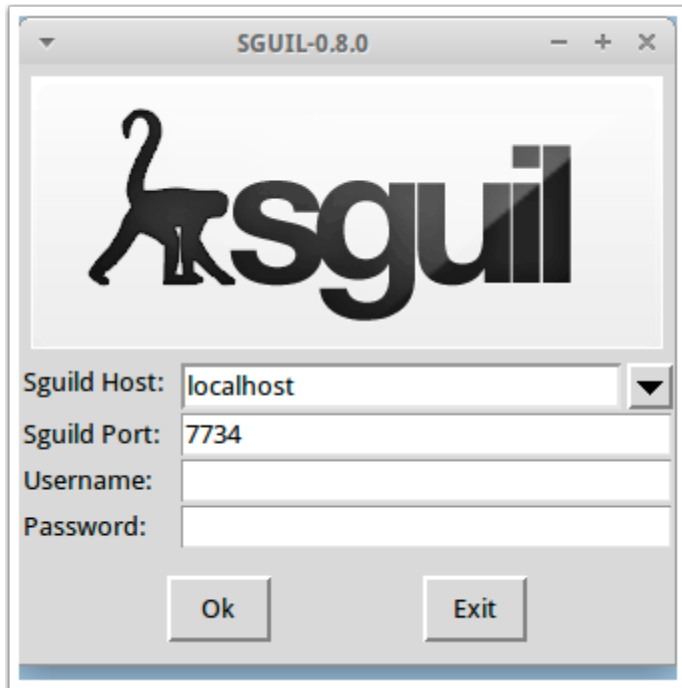


Sguil Login

Enter your username and password:

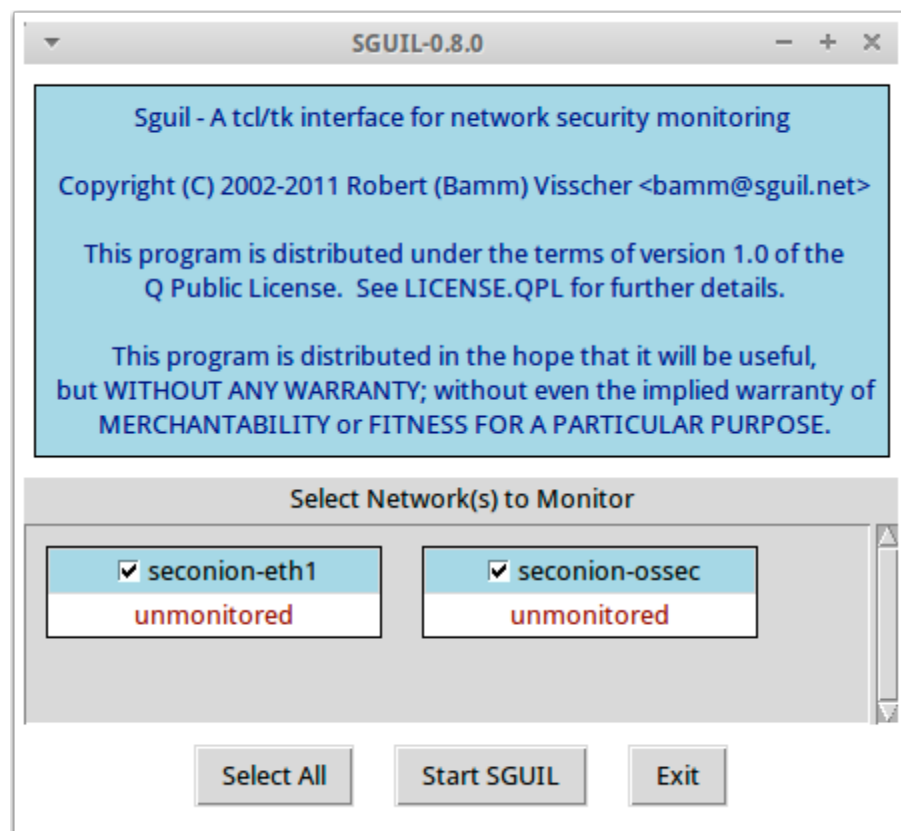
User: student

Password: password



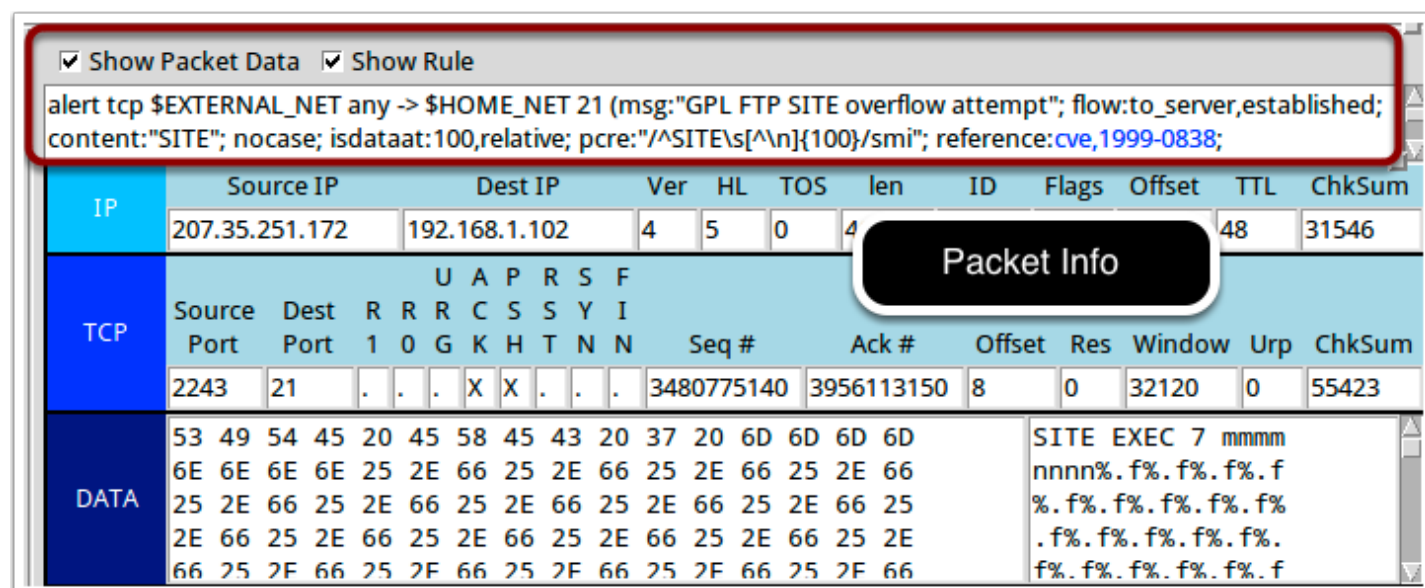
Start Sguil

Check both boxes and start Squil



Sguil Alert Information

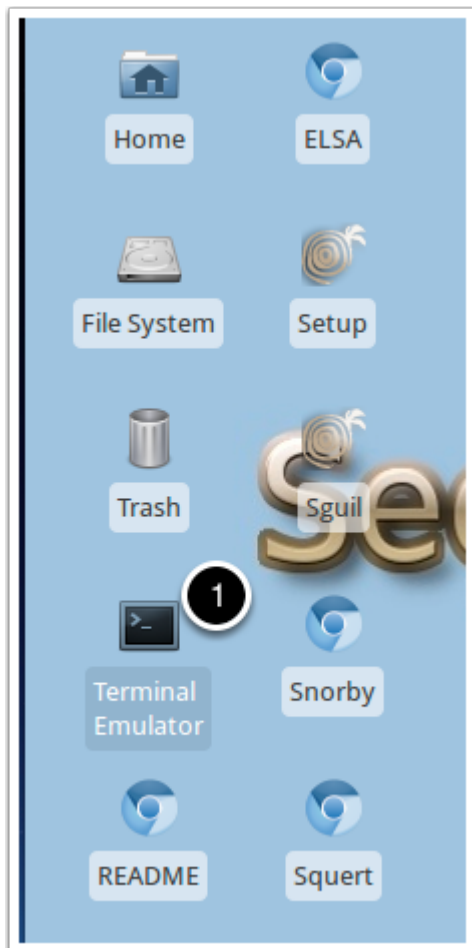
When you click on an alert and select Show Packet Data and Show Rule, you will see packet info on what triggered the alert and the alert that was triggered. This may help you determine false positives or research what the alert means.



Using tcpreplay

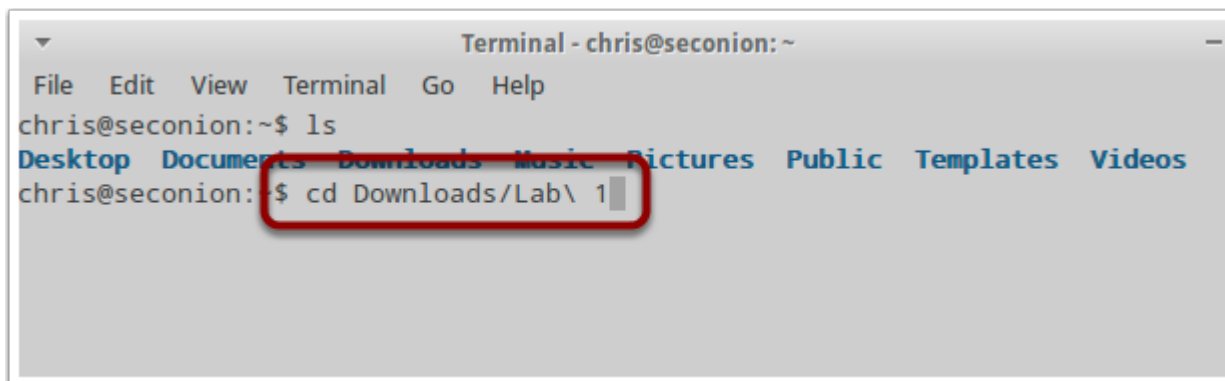
tcpreplay allows you to play packets on an interface.

1. Open a terminal window
2. Sguil should be running when completing the next steps



tcpreplay

change directories to Downloads/Lab 1

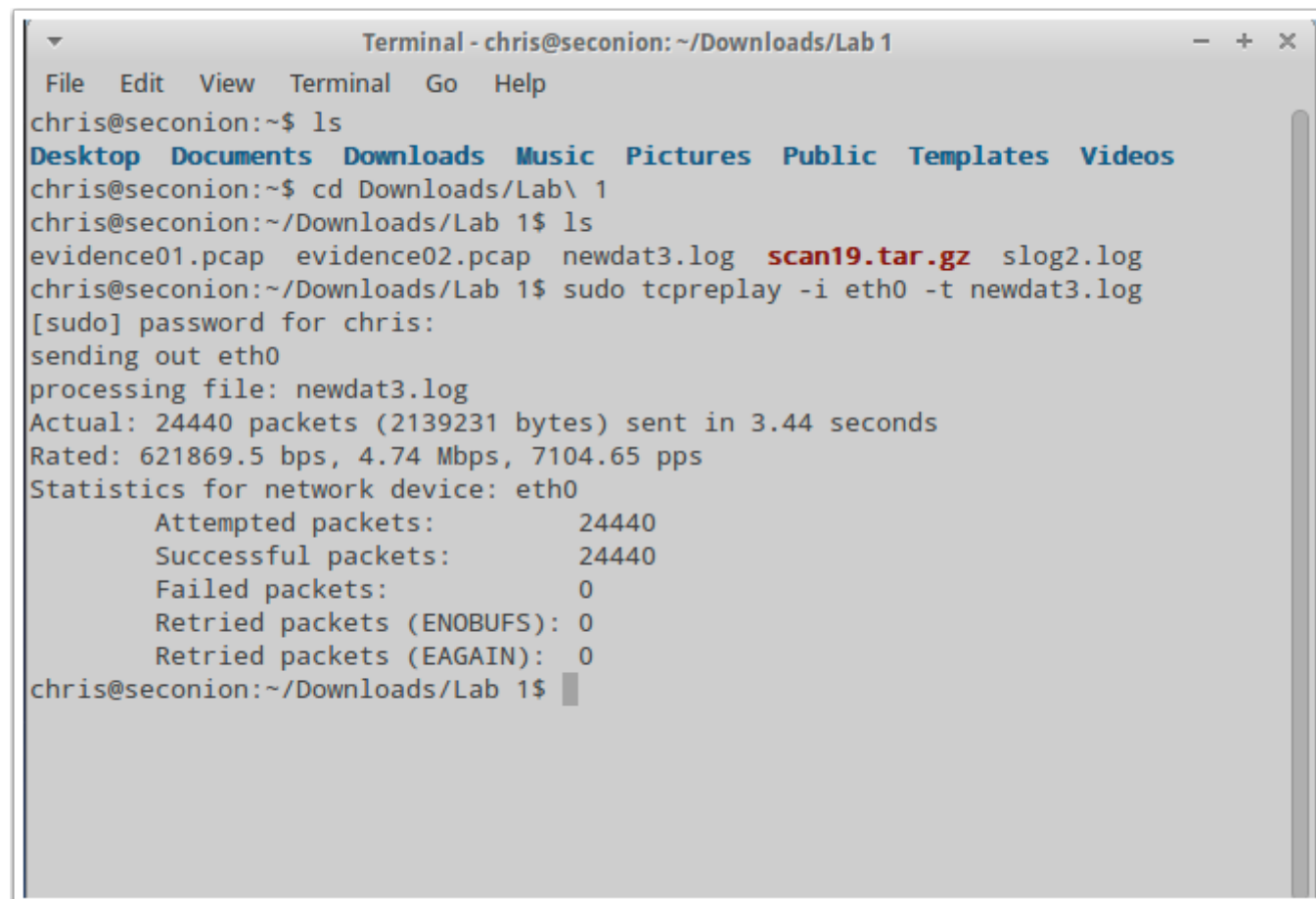


Play the file

Run the command: `sudo tcpreplay -i eth1 -t newdat3.log`

****Make sure you play it over eth1**

You should see a similar output. You will need to enter the student password.



```
Terminal - chris@seconion: ~/Downloads/Lab 1
File Edit View Terminal Go Help
chris@seconion:~$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos
chris@seconion:~$ cd Downloads/Lab\ 1
chris@seconion:~/Downloads/Lab 1$ ls
evidence01.pcap evidence02.pcap newdat3.log scan19.tar.gz slog2.log
chris@seconion:~/Downloads/Lab 1$ sudo tcpreplay -i eth0 -t newdat3.log
[sudo] password for chris:
sending out eth0
processing file: newdat3.log
Actual: 24440 packets (2139231 bytes) sent in 3.44 seconds
Rated: 621869.5 bps, 4.74 Mbps, 7104.65 pps
Statistics for network device: eth0
    Attempted packets:      24440
    Successful packets:     24440
    Failed packets:         0
    Retried packets (ENOBUFS): 0
    Retried packets (EAGAIN): 0
chris@seconion:~/Downloads/Lab 1$
```

Sguil

Now switchback to Sguil. You should see a variety of alert as depicted below.

File Query Reports Sound: Off ServerName: localhost UserName: chris UserID: 2 2014-03-07 18:41:54 GM

RealTime Events Escalated Events

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	seconion-...	3.1	2014-03-07 18:39:51	210.114.220.46	653	192.168.1.102	111	17	GPL RPC portmap status r...
RT	1	seconion-...	3.2	2014-03-07 18:39:51	210.114.220.46	654	192.168.1.102	919	17	GPL RPC STATD UDP stat ...
RT	2	seconion-...	3.3	2014-03-07 18:39:51	192.168.1.102	23	217.156.93.166	61200	6	GPL TELNET Bad Login
RT	1	seconion-...	3.5	2014-03-07 18:39:51	192.168.1.102	21	207.35.251.172	2243	6	ET POLICY FTP Login Succ...
RT	37	seconion-...	3.6	2014-03-07 18:39:51	207.35.251.172	2243	192.168.1.102	21	6	GPL FTP SITE EXEC attempt
RT	36	seconion-...	3.7	2014-03-07 18:39:51	207.35.251.172	2243	192.168.1.102	21	6	GPL FTP SITE overflow atte...
RT	1	seconion-...	3.79	2014-03-07 18:39:51	192.168.1.102	21	207.35.251.172	2243	6	GPL ATTACK_RESPONSE id ...
RT	1	seconion-...	3.80	2014-03-07 18:39:51	192.168.1.102	23	217.156.93.166	61216	6	ET MALWARE Suspicious F...
RT	4	seconion-...	3.81	2014-03-07 18:39:52	207.35.251.172	4031	192.168.1.102	5920	6	ET SCAN Potential VNC Sca...
RT	4	seconion-...	3.82	2014-03-07 18:39:52	207.35.251.172	4981	192.168.1.102	5807	6	ET SCAN Potential VNC Sca...

IP Resolution Agent Status Snort Statistics System Msg

☐ Reverse DNS ☒ Enable External DNS

Src IP:

Src Name:

Dst IP:

☒ Display Detected Banner

50 52 41 44 53 20 53 45 52 56 45 52 PRADS SE RVER

Sguil

Find the GPL FTP SITE overflow attempt alert

1. Right click in the alert ID section and select Transcript

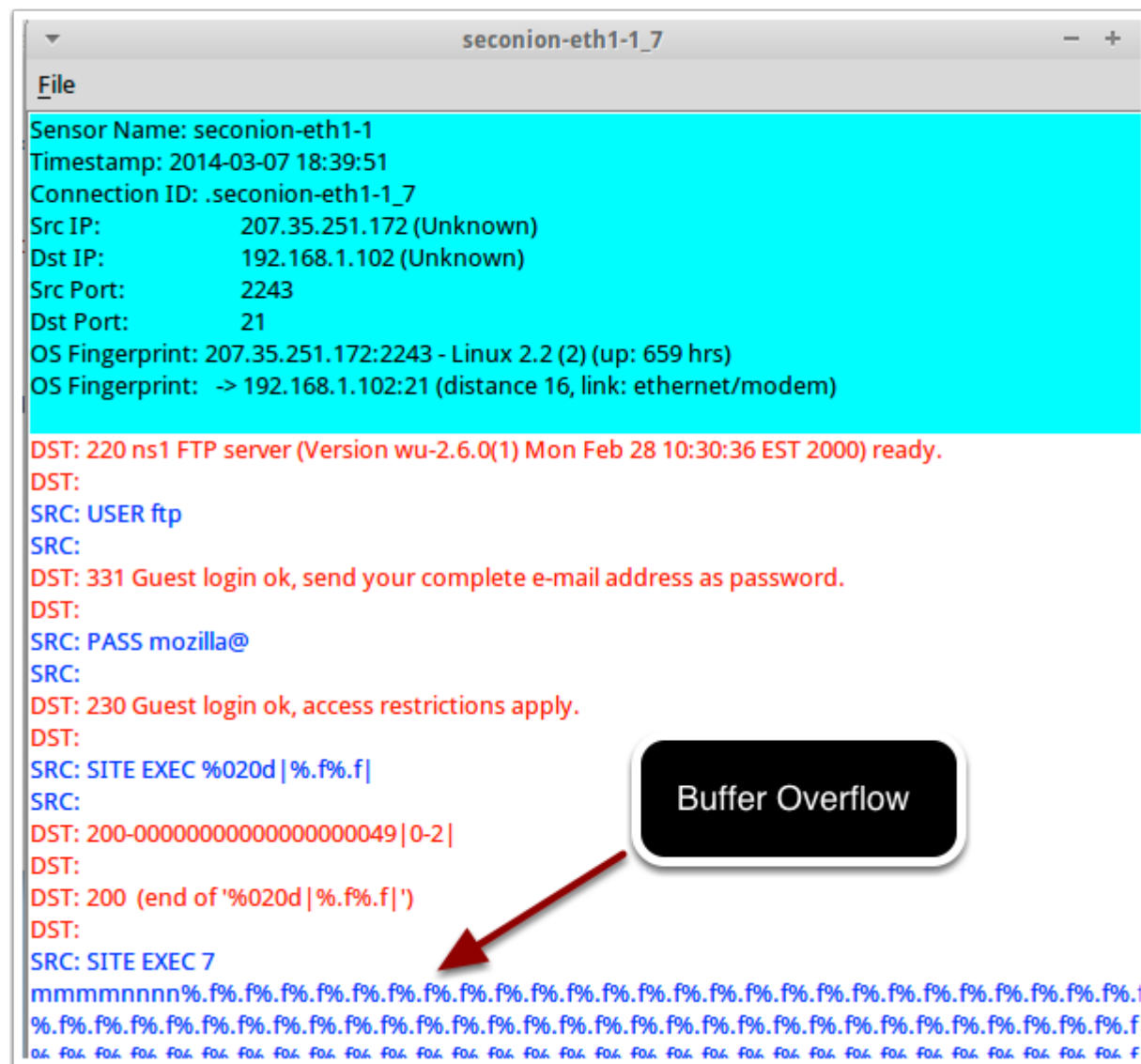
File Query Reports Sound: Off ServerName: localhost UserName: chris UserID: 2 2014-03-07 18:45:25 GM

RealTime Events Escalated Events

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	seconion-...	3.1	2014-03-07 18:39:51	210.114.220.46	653	192.168.1.102	111	17	GPL RPC portmap status r...
RT	1	seconion-...	3.2	2014-03-07 18:39:51	210.114.220.46	654	192.168.1.102	919	17	GPL RPC STATD UDP stat ...
RT	2	seconion-...	3.3	2014-03-07 18:39:51	192.168.1.102	23	217.156.93.166	61200	6	GPL TELNET Bad Login
RT	1	seconion-...	3.5	2014-03-07 18:39:51	192.168.1.102	21	207.35.251.172	2243	6	ET POLICY FTP Login Succ...
RT	37	seconion-...	3.6	2014-03-07 18:39:51	207.35.251.172	2243	192.168.1.102	21	6	GPL FTP SITE EXEC attempt
RT	36	seconion-...	3.7	2014-03-07 18:39:51	207.35.251.172	2243	192.168.1.102	21	6	GPL FTP SITE overflow atte...
RT	1	seconion-...	3.79	2014-03-07 18:39:51	192.168.1.102	21	207.35.251.172	2243	6	GPL ATTACK_RESPONSE id ...
RT	1	seconion-...	3.80	2014-03-07 18:39:51	192.168.1.102	23	217.156.93.166	61216	6	ET MALWARE Suspicious F...
RT	4	seconion-...	3.81	2014-03-07 18:39:52	207.35.251.172	4031	192.168.1.102	5920	6	ET SCAN Potential VNC Sca...
RT	4	seconion-...	3.82	2014-03-07 18:39:52	207.35.251.172	4981	192.168.1.102	5807	6	ET SCAN Potential VNC Sca...

Sguil Transcript

This shows the entire packet trace from the alert. You can see the successful buffer overflow and the attacker running the cat command on the paswd file. Why did the attacker run the cat command?



Attacker Commands

This is an example of the attacker running the cat command. Look at the other commands the attacker runs. Think about why the attacker does this. This might be handy for you in CYB 608. Explore the other alerts and see what you can learn.

```
SRC: cat passwd-  
SRC:  
DST: root:x:0:0:root:/root:/bin/bash  
DST: bin:x:1:1:bin:/bin:  
DST: daemon:x:2:2:daemon:/sbin:  
DST: adm:x:3:4:adm:/var/adm:  
DST: lp:x:4:7:lp:/var/spool/lpd:  
DST: sync:x:5:0:sync:/sbin:/bin/sync  
DST: shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown  
DST: halt:x:7:0:halt:/sbin:/sbin/halt  
DST: mail:x:8:12:mail:/var/spool/mail:  
DST: news:x:9:13:news:/var/spool/news:  
DST: uucp:x:10:14:uucp:/var/spool/uucp:  
DST: operator:x:11:0:operator:/root:  
DST: games:x:12:100:games:/usr/games:  
DST: gopher:x:13:30:gopher:/usr/lib/gopher-data:  
DST: ftp:x:14:50:FTP User:/home/ftp:  
DST: nobody:x:99:99:Nobody:/:  
DST: xf  
DST: s:x:43:43:X Font Server:/etc/X11/fs:/bin/false  
DST: named:x:25:25:Named:/var/named:/bin/false  
DST: postgres:x:26:26:PostgreSQL Server:/var/lib/pgsql:/bin/bash  
DST: john:x:500:500:John:/home/john:/bin/bash  
DST: dns:x:0:0:/bin:/bin/bash  
DST:
```

Close Sguil and the Terminal Window

Close Sguil and the Terminal Window

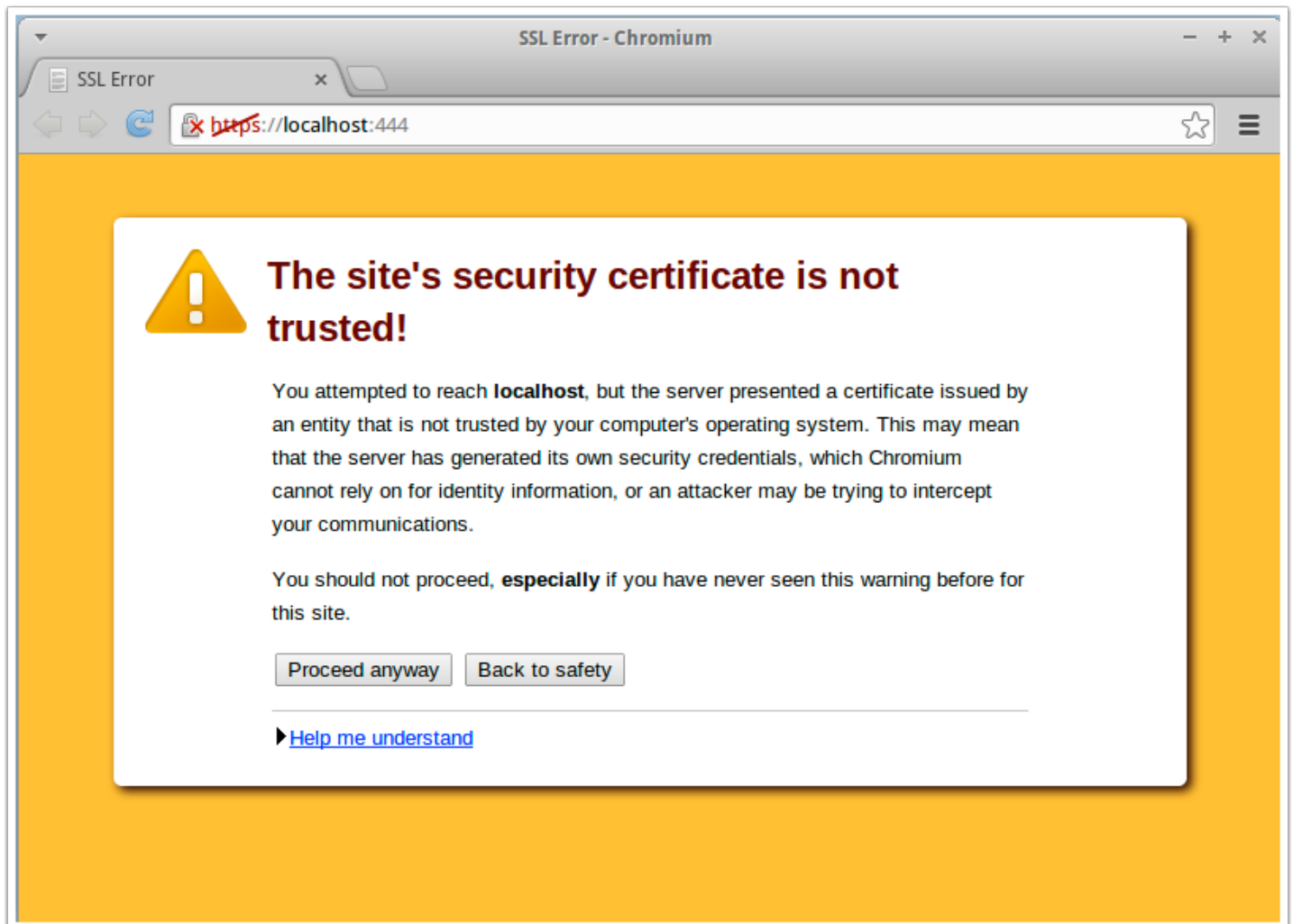
Using Snorby

Double click on the Snorby icon



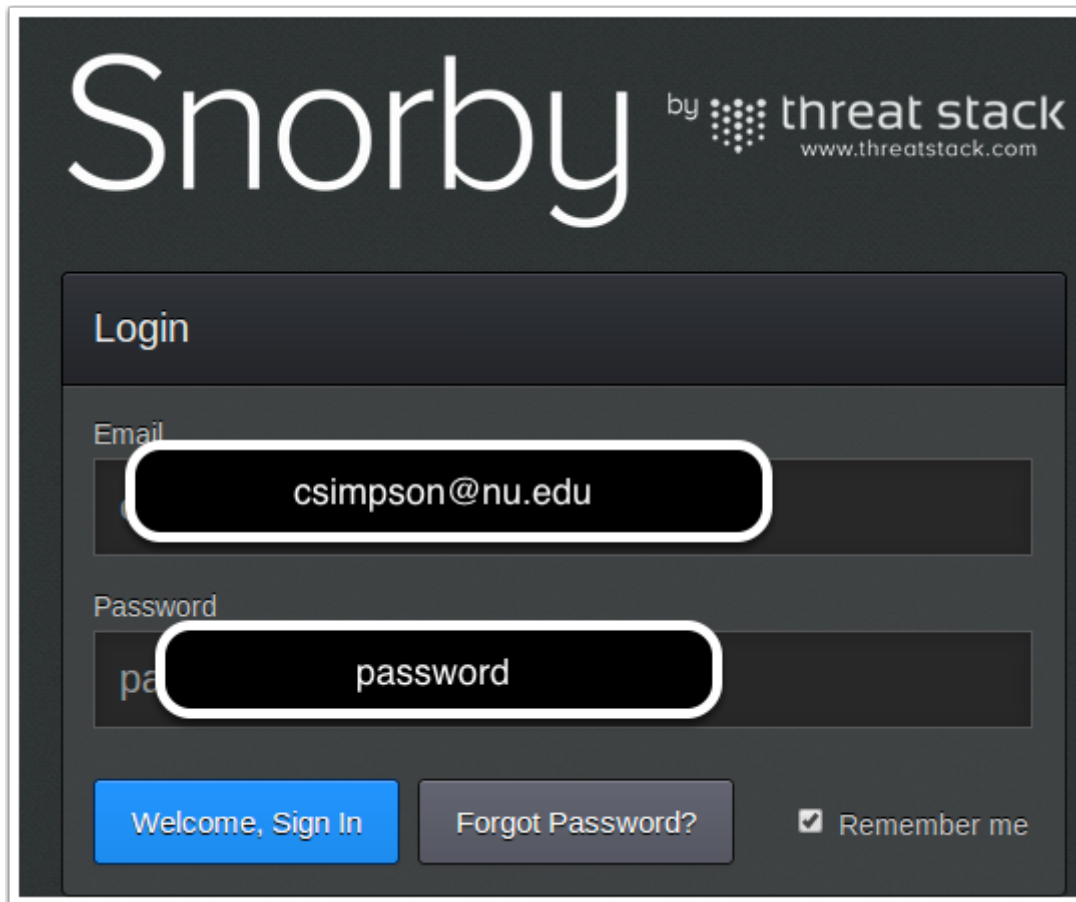
Using Snorby

Click Proceed anyway



Using Snorby

1. Login to Snorby



The image shows the Snorby login interface. At the top, the word "Snorby" is displayed in a large, white, sans-serif font. To its right, the text "by threat stack" is shown, with a small logo of a grid of dots between "by" and "threat stack". Below this, the website "www.threatstack.com" is listed. The main login area is a dark gray box with a "Login" header. It contains two input fields: "Email" and "Password". The "Email" field contains the text "csimpson@nu.edu" and the "Password" field contains the text "password". Both fields are highlighted with a white border. Below the input fields, there are three buttons: a blue "Welcome, Sign In" button, a gray "Forgot Password?" button, and a checkbox labeled "Remember me".

Snorby by threat stack
www.threatstack.com

Login

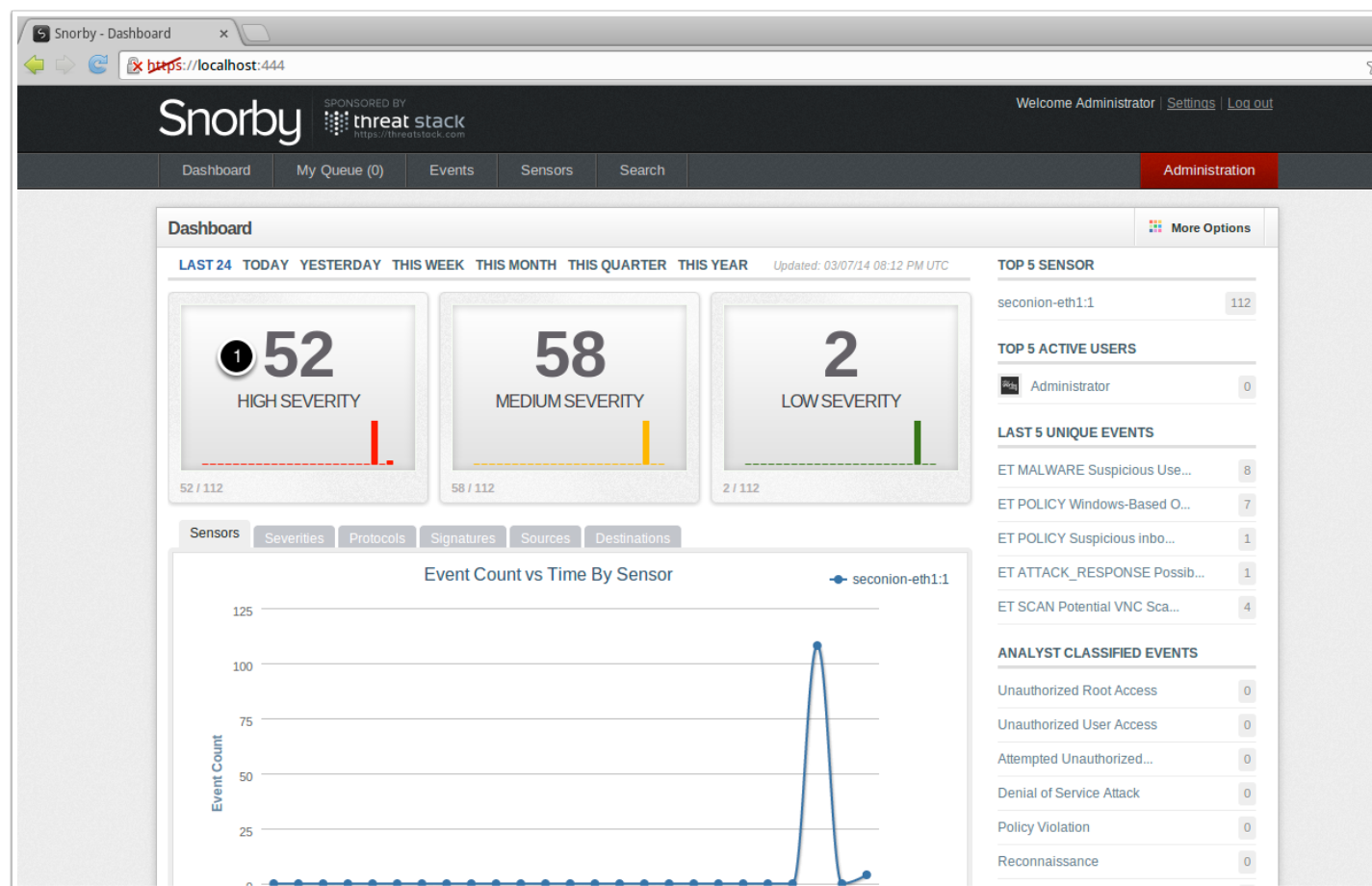
Email
csimpson@nu.edu

Password
password

Welcome, Sign In Forgot Password? ☒ Remember me

Snorby Opening Screen

1. Click on High Severity to see specific alerts



Snorby Alerts

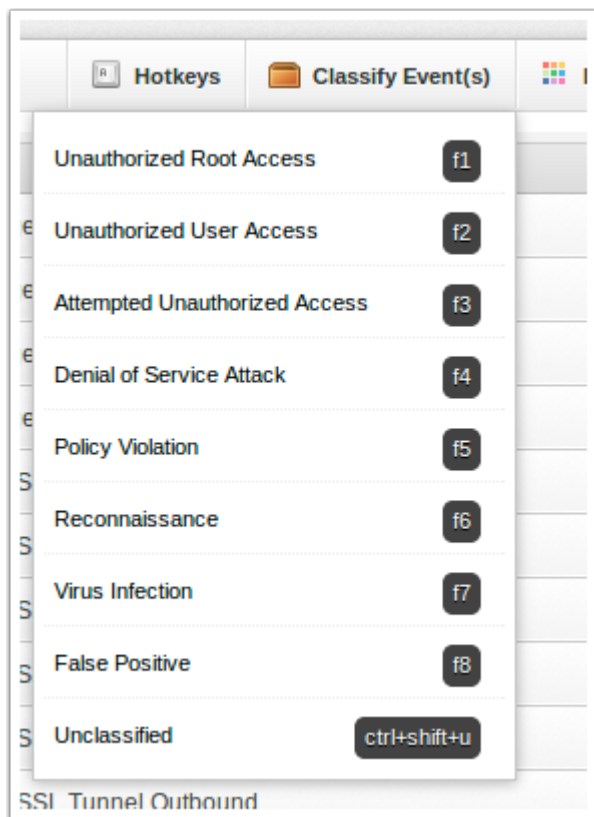
1. Click on one of the GPL FTP SITE overflow attempt alerts

Notice how the information is similar to Sguil alert, You can see the payload and packet information. Snorby is good for coordinating a team. Notice how you can export event information (including email and perform classification

[illegible]

Snorby Classifying Events

Snorby also allows you to classify events. This is great for a team environment.



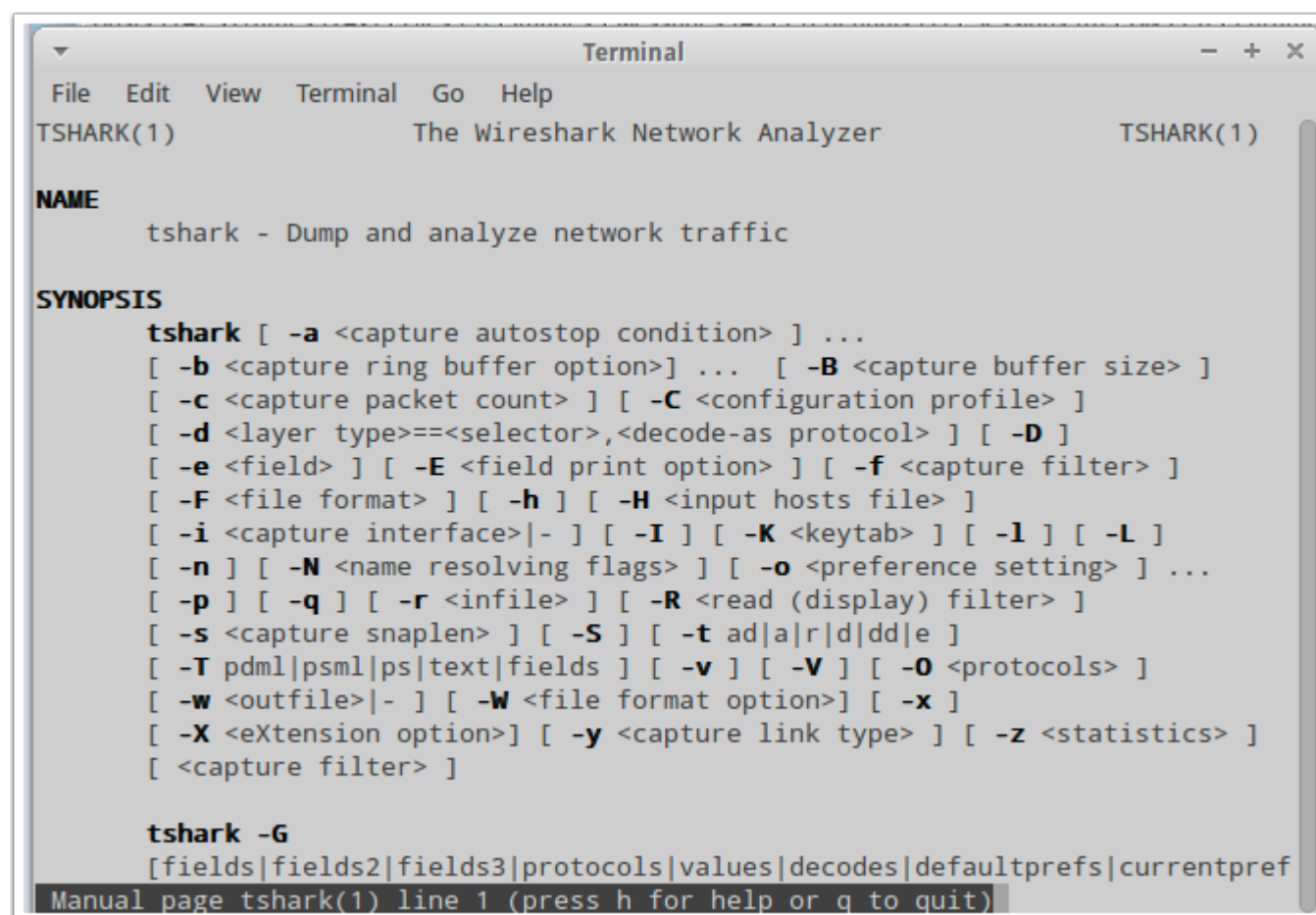
Next Steps

In this lab we have focussed on tools with graphical user interfaces. As you gain additional skills you should learn command line tools like tshark discussed on the next page.

tshark

tshark is a command line network analysis tool that allows for more granular control of pcap data. Review how other people solved this contest to see the power of the command line tool and scripting: <http://forensicscontest.com/contest01/Finalists/>

If you plan on working as a Network Intrusion Analyst you should learn the command line and scripting tools.



```

Terminal
File Edit View Terminal Go Help
TSHARK(1) The Wireshark Network Analyzer TSHARK(1)

NAME
    tshark - Dump and analyze network traffic

SYNOPSIS
    tshark [ -a <capture autostop condition> ] ...
    [ -b <capture ring buffer option> ] ... [ -B <capture buffer size> ]
    [ -c <capture packet count> ] [ -C <configuration profile> ]
    [ -d <layer type>==<selector>,<decode-as protocol> ] [ -D ]
    [ -e <field> ] [ -E <field print option> ] [ -f <capture filter> ]
    [ -F <file format> ] [ -h ] [ -H <input hosts file> ]
    [ -i <capture interface>|- ] [ -I ] [ -K <keytab> ] [ -l ] [ -L ]
    [ -n ] [ -N <name resolving flags> ] [ -o <preference setting> ] ...
    [ -p ] [ -q ] [ -r <infile> ] [ -R <read (display) filter> ]
    [ -s <capture snaplen> ] [ -S ] [ -t ad|a|r|d|dd|e ]
    [ -T pdml|psml|ps|text|fields ] [ -v ] [ -V ] [ -O <protocols> ]
    [ -w <outfile>|- ] [ -W <file format option> ] [ -x ]
    [ -X <eXtension option> ] [ -y <capture link type> ] [ -z <statistics> ]
    [ <capture filter> ]

    tshark -G
    [fields|fields2|fields3|protocols|values|decodes|defaultprefs|currentpref
Manual page tshark(1) line 1 (press h for help or q to quit)

```


Your turn ****Lab Submission Requirements****

Now that you know a little about the tools see if you can solve a scenario. Go to this website and read the scenario:

<http://forensicscontest.com/2009/10/10/puzzle-2-ann-skips-bail>

Using the tools we discussed to analyse the pcap file located in this directory: Student/Downloads/Lab 1/evidence02.pcap try to answer these questions. Each answer should include an explanation on how you found the answer and a screenshot of where you found it. The answer should be written as if you were providing an official response to your boss.

1. What is Ann's email address? (4 points)
2. What is Ann's email password? (4 points)
3. What is Ann's secret lover's email address? (4 points)
4. What two items did Ann tell her secret lover to bring? (4 points)
5. What is the NAME of the attachment Ann sent to her secret lover? (4 points)
6. In what CITY and COUNTRY is their rendez-vous point? (4 points)

Total: 24 Points

The analysis will be worth 16 points and evaluated on the following criteria:

- a. Clearly explained how the answer was determined
- b. Conclusion supported with clear and easy to read screenshots
- c. Written in your own words
- d. Use of different tools to conduct the analysis and validate results



Total Points for lab: 40

Note: Network Miner, Wireshark, and Sguil are probably the best tools for this exercise. You are encouraged to try the command line tool and see if you can develop your own scripts.

1. Submit the assignment to the correct dropbox. Your report should include screenshots.
2. Try not to use the answers on the website, the best way to learn is by using the tools yourself. You may want to use Wireshark first to get a good overview and then move to Network Miner. You are also encouraged to use the command line tools.

Oct
10
2009

Puzzle #2: Ann Skips Bail

 Contest, Puzzle #2 Add comments

After being released on bail, Ann Dercover disappears! Fortunately, investigators were carefully monitoring her network activity before she skipped town.

"We believe Ann may have communicated with her secret lover, Mr. X, before she left," says the police chief. "The **packet capture** may contain clues to her whereabouts."

You are the forensic investigator. Your mission is to figure out what Ann emailed, where she went, and recover evidence including:

1. What is Ann's email address?
2. What is Ann's email password?
3. What is Ann's secret lover's email address?
4. What two items did Ann tell her secret lover to bring?
5. What is the NAME of the attachment Ann sent to her secret lover?
6. What is the MD5sum of the attachment Ann sent to her secret lover?
7. In what CITY and COUNTRY is their rendez-vous point?
8. What is the MD5sum of the image embedded in the document?