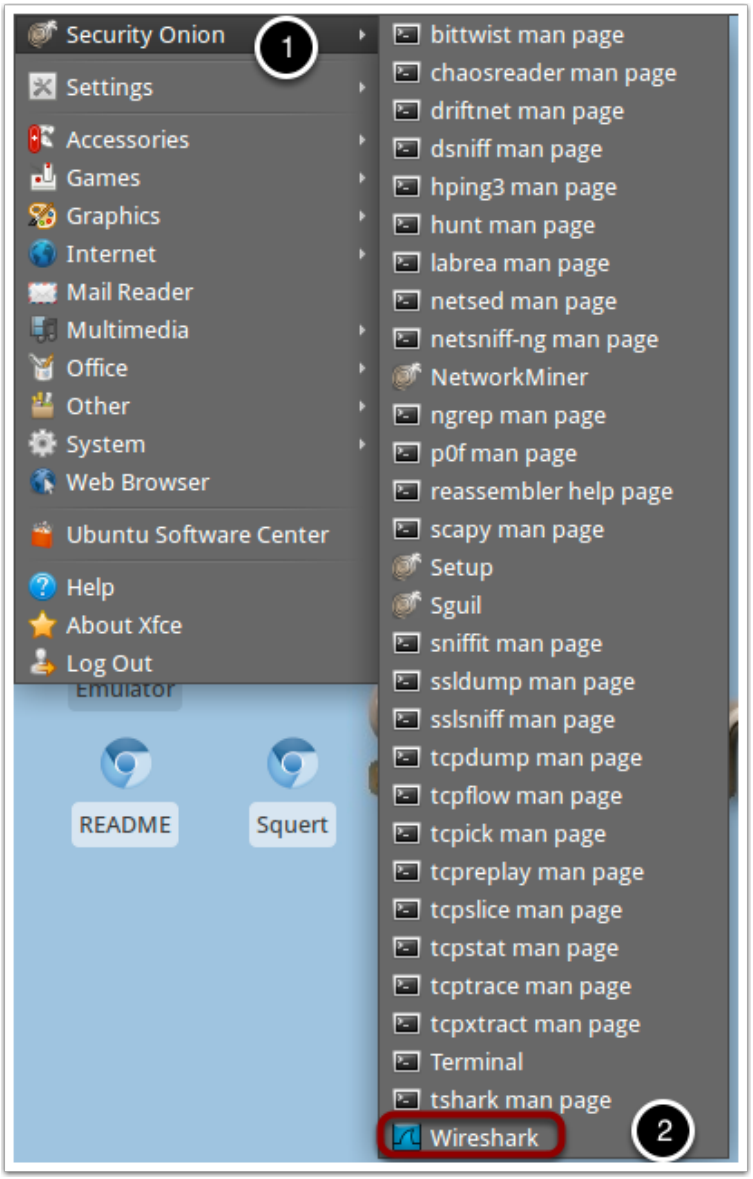
CYB 606 Lab 1 - Intro to Security Onion

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.

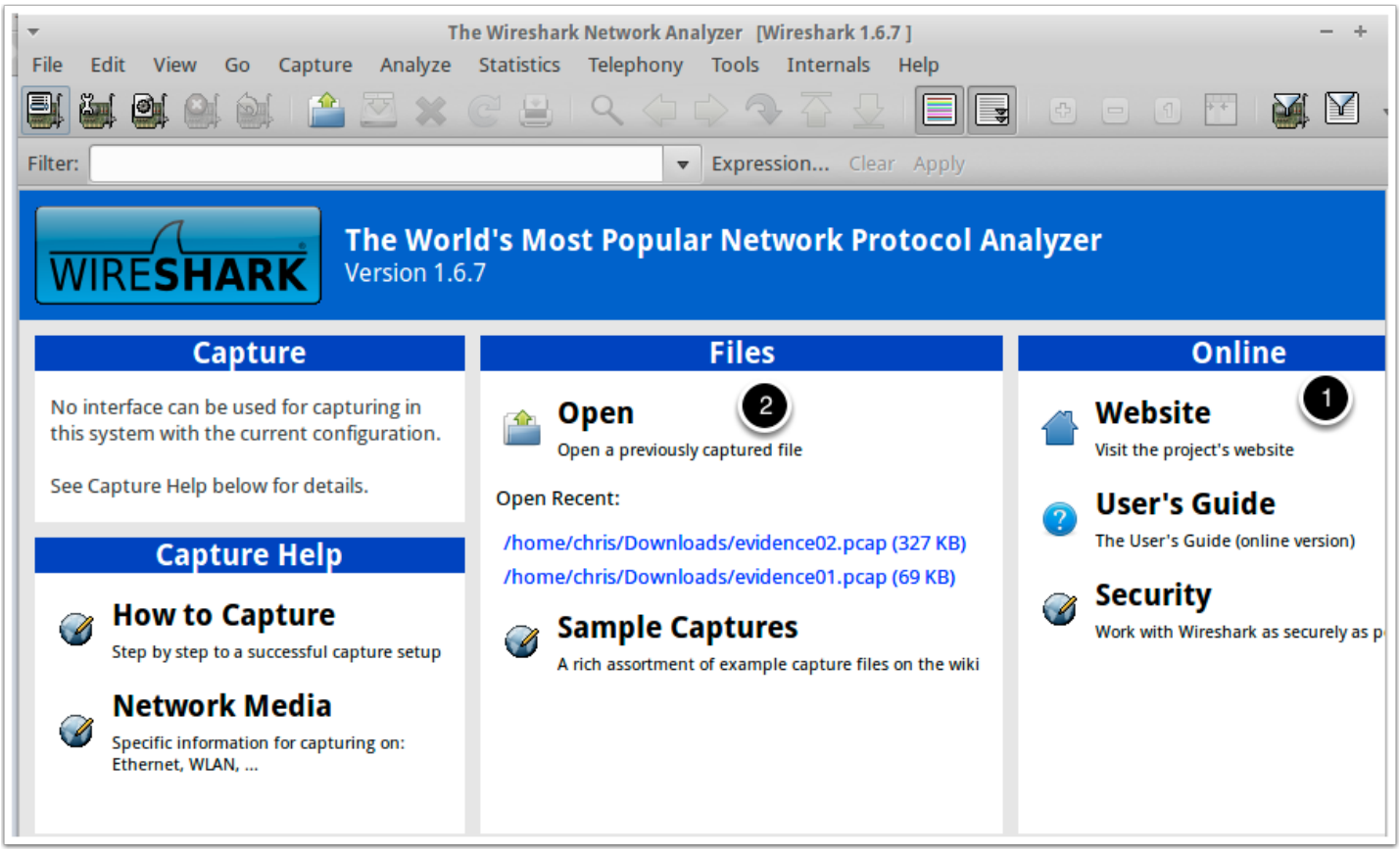
Wireshark

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.



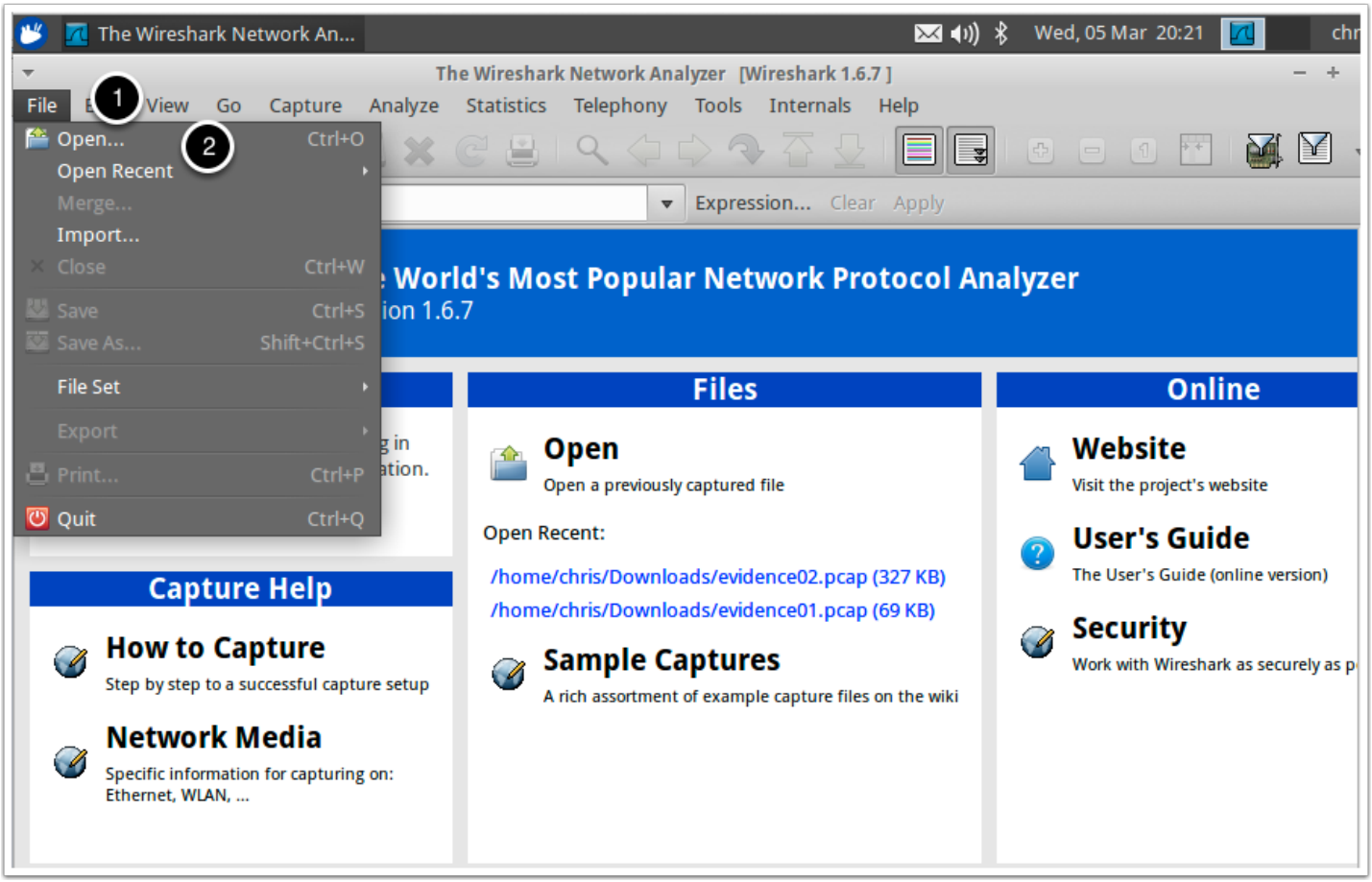
Wireshark

This is the opening screen for Wireshark.
1.This is where you can find help online.
2. This is where you open pcap files.



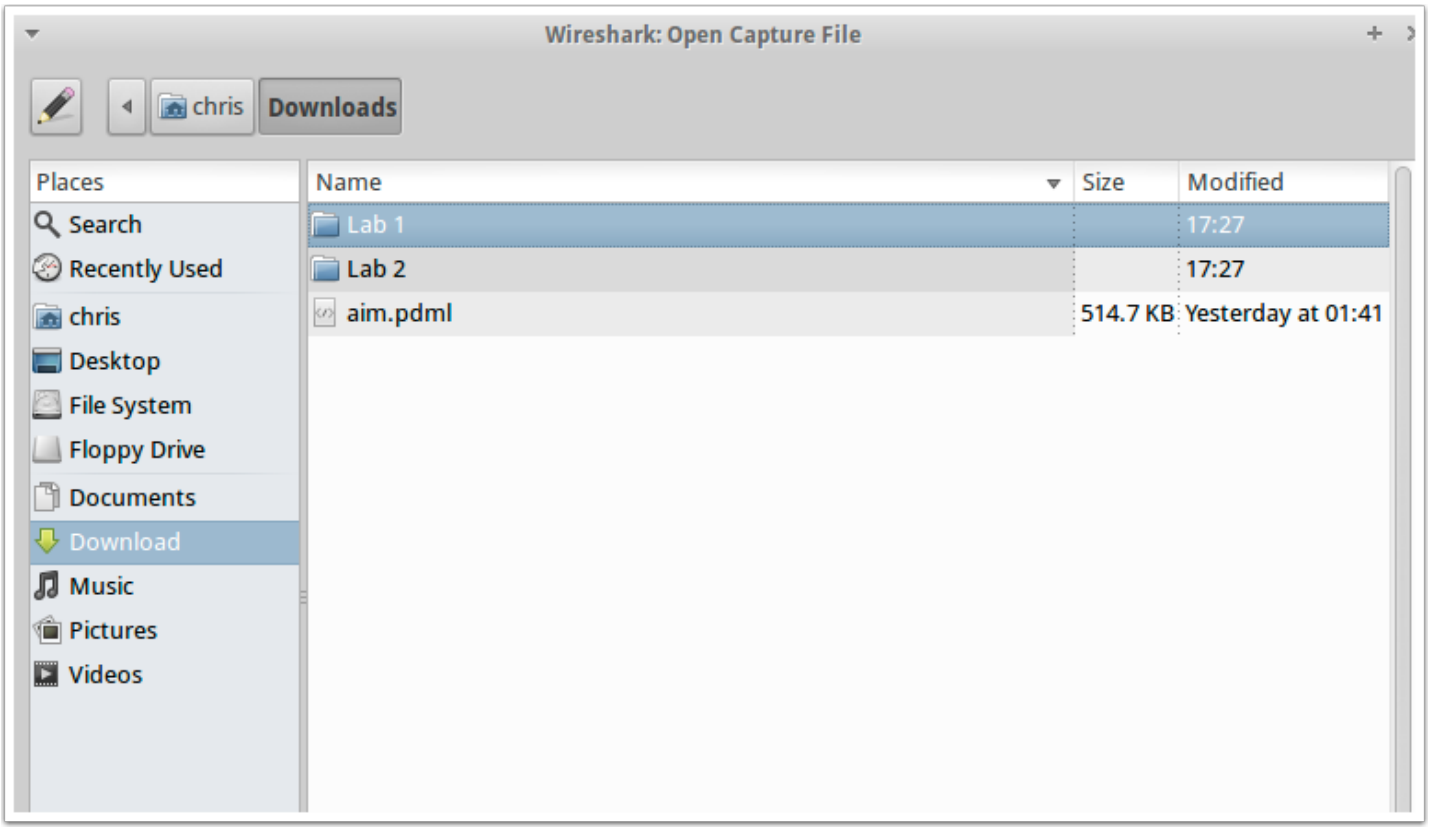
Open pcap file

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



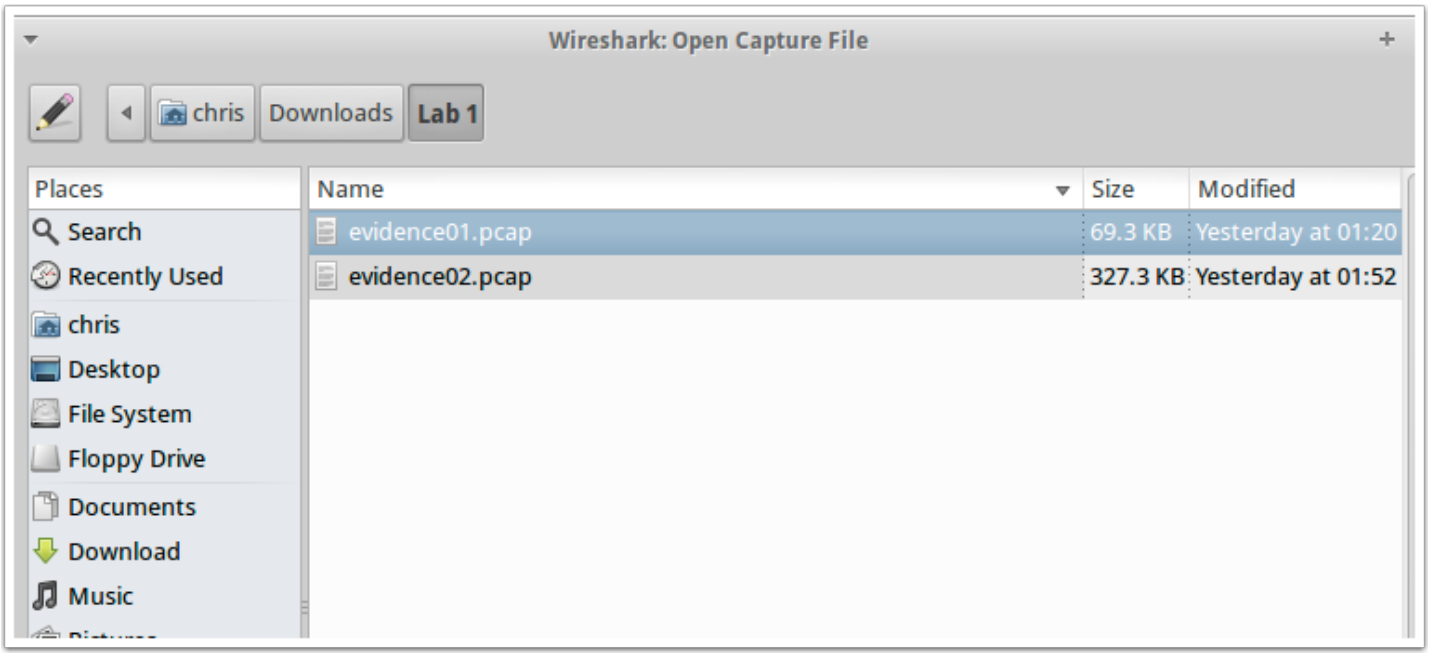
Open PCAP File

Go to the Download/Lab 1 Directory



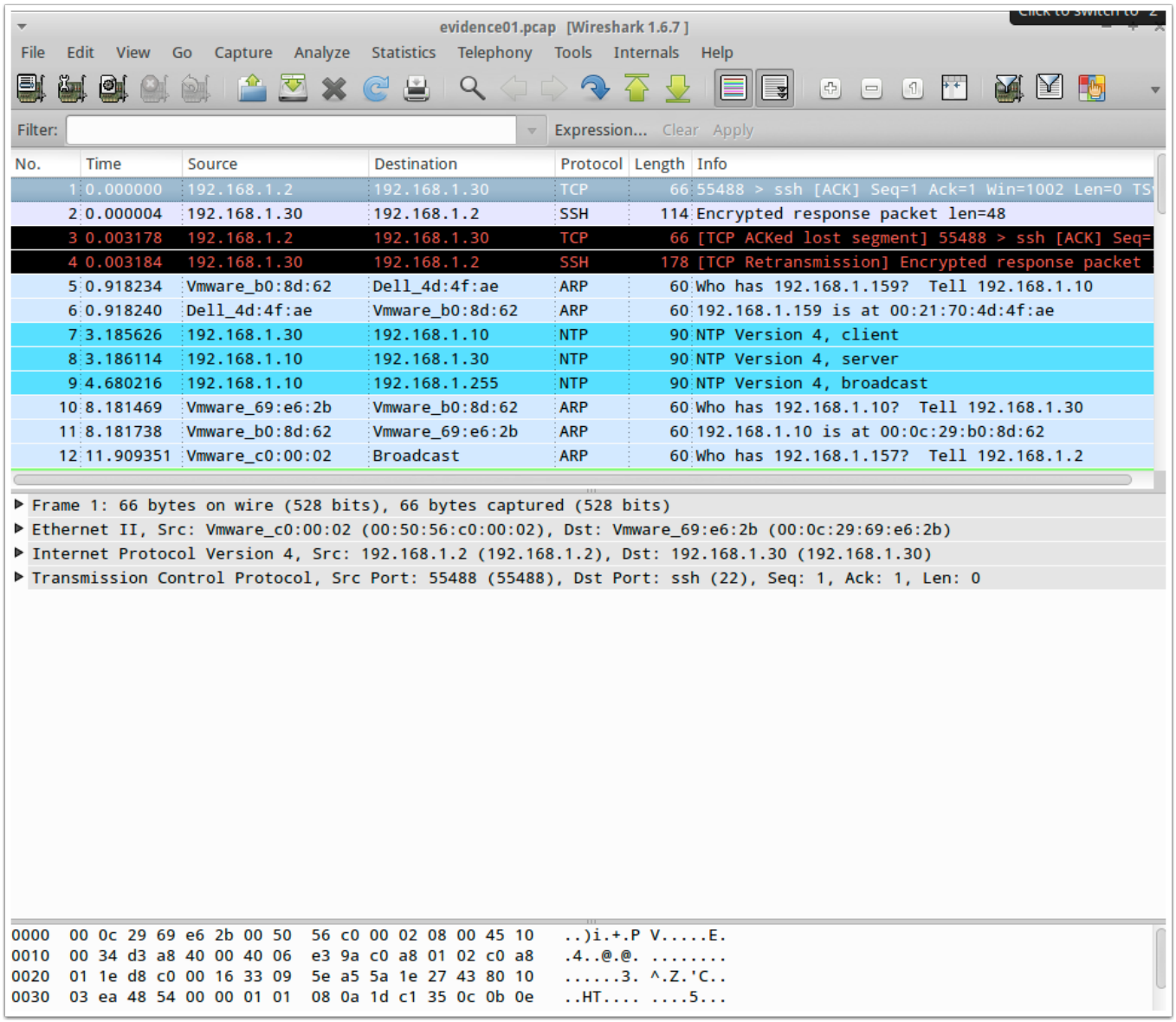
Open PCAP file

Select evidence01.pcap file and click open



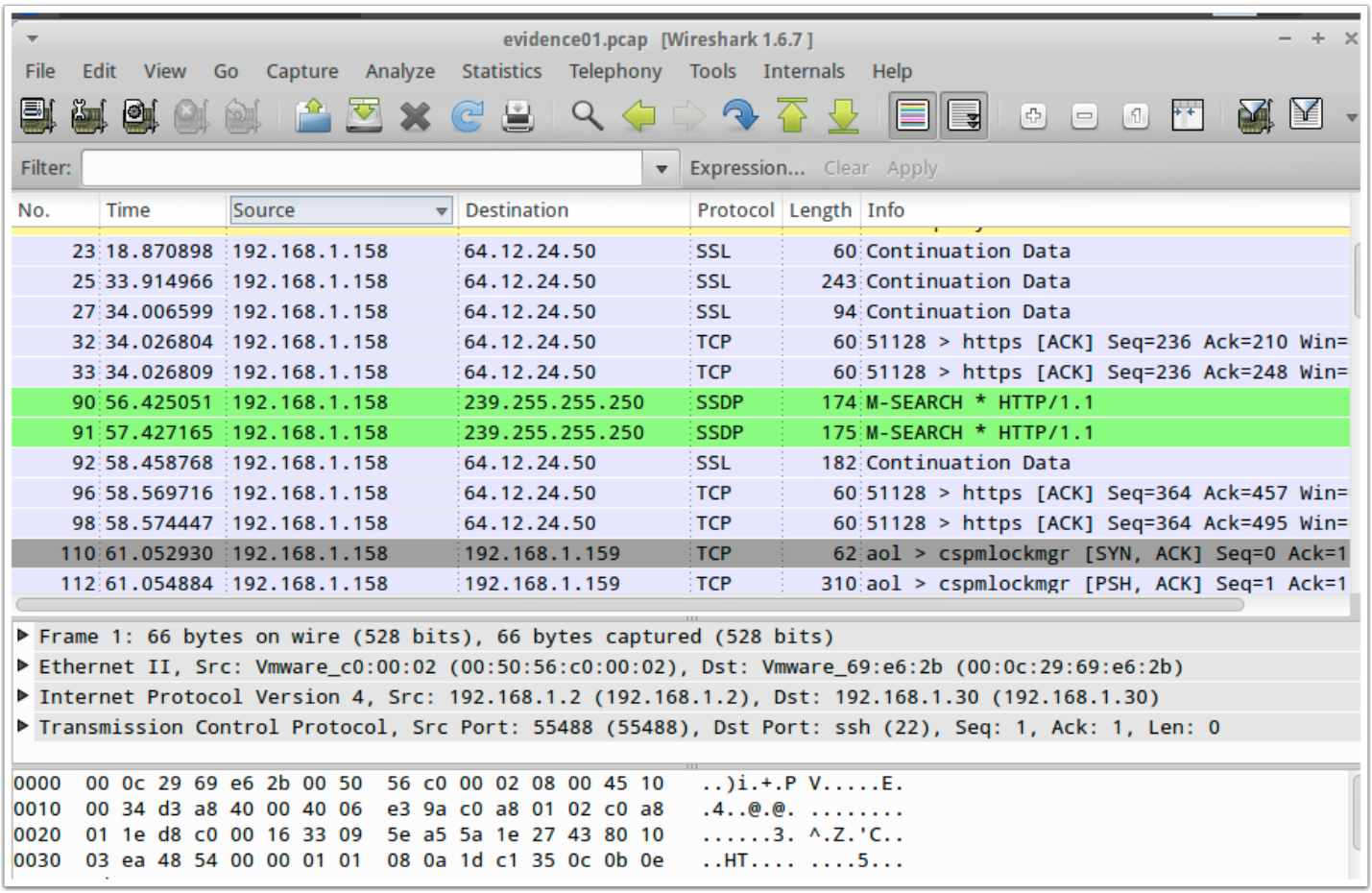
Traffic Capture

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.



Sorted by IP

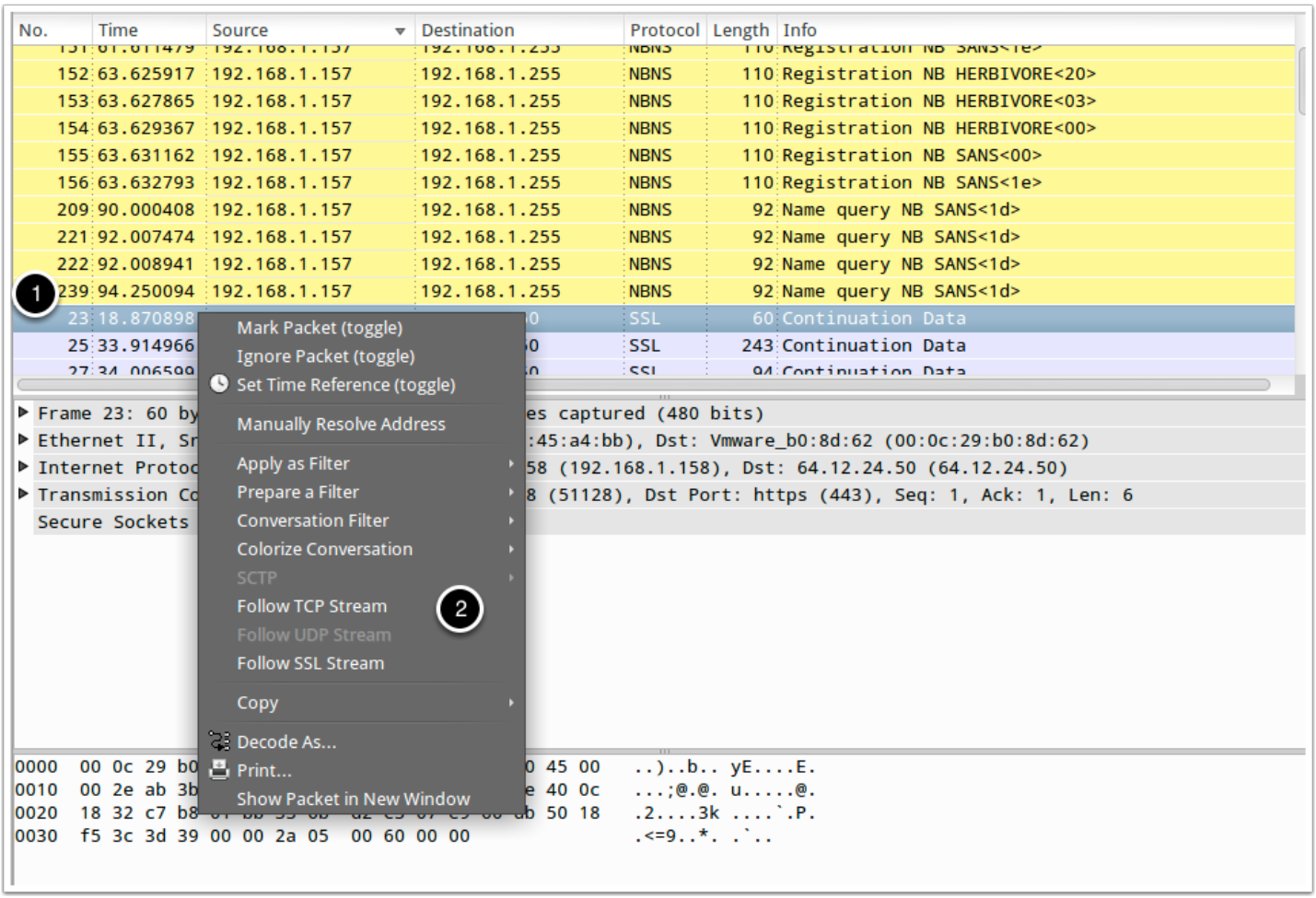
Your screen should look like this



Follow TCP stream

1. Right click the first entry for 192.168.1.158
2. Select Follow TCP Stream.

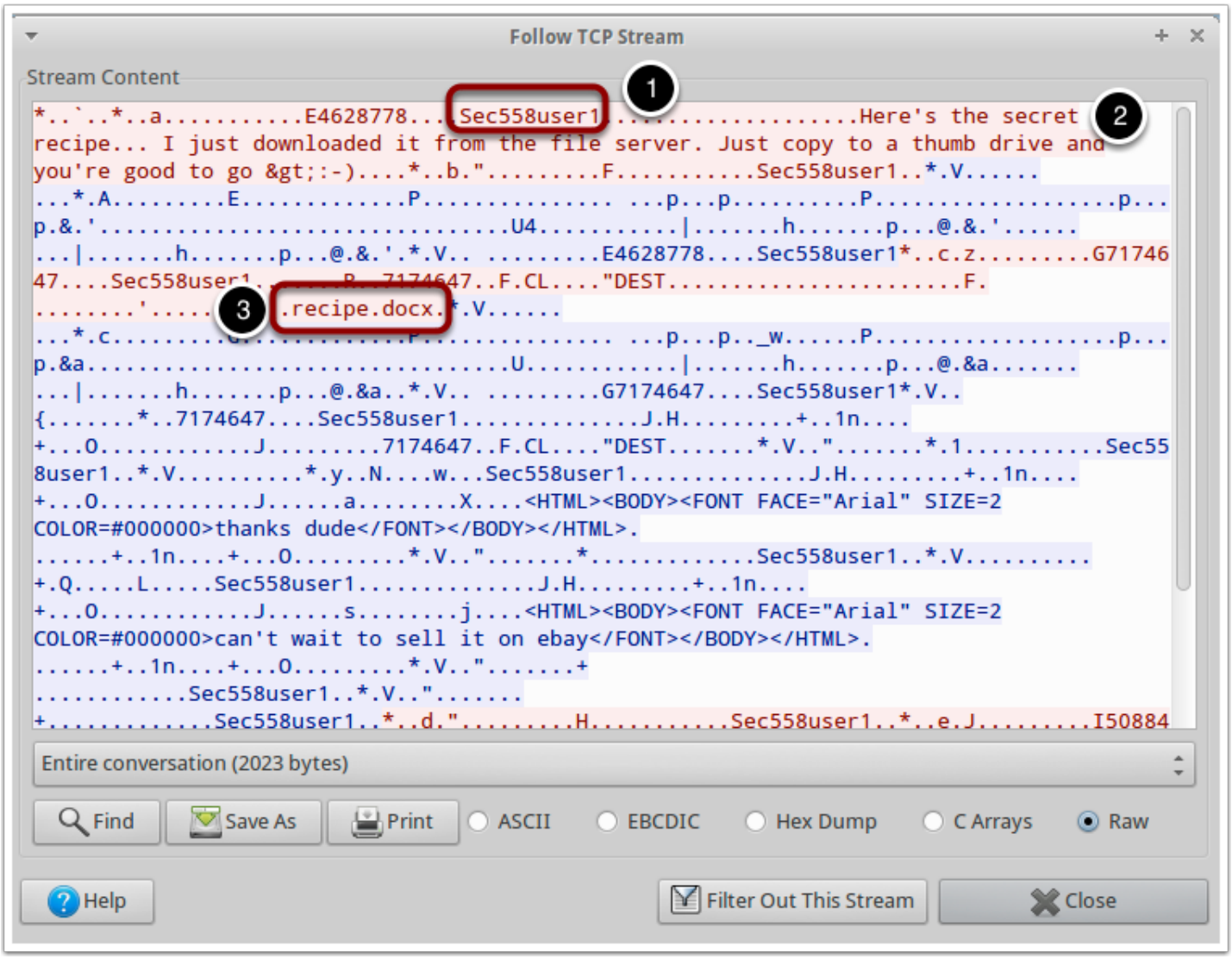
This will show the tcp stream for that connection.



TCP Stream

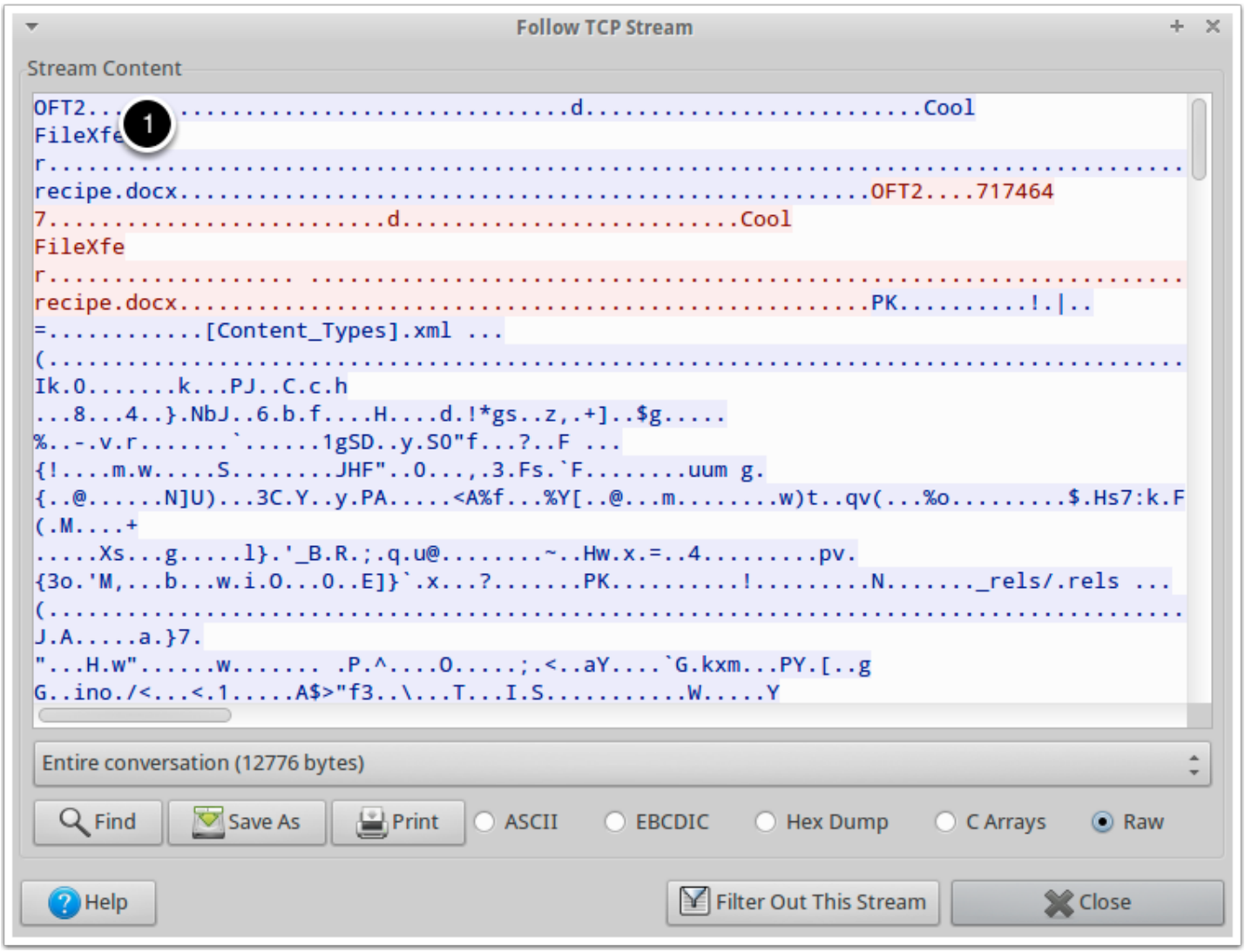
This is an example of the TCP stream. Do you see any answers to the problem?
1. Possible IM user name
2. Possible IM comment
3. Possible file name

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



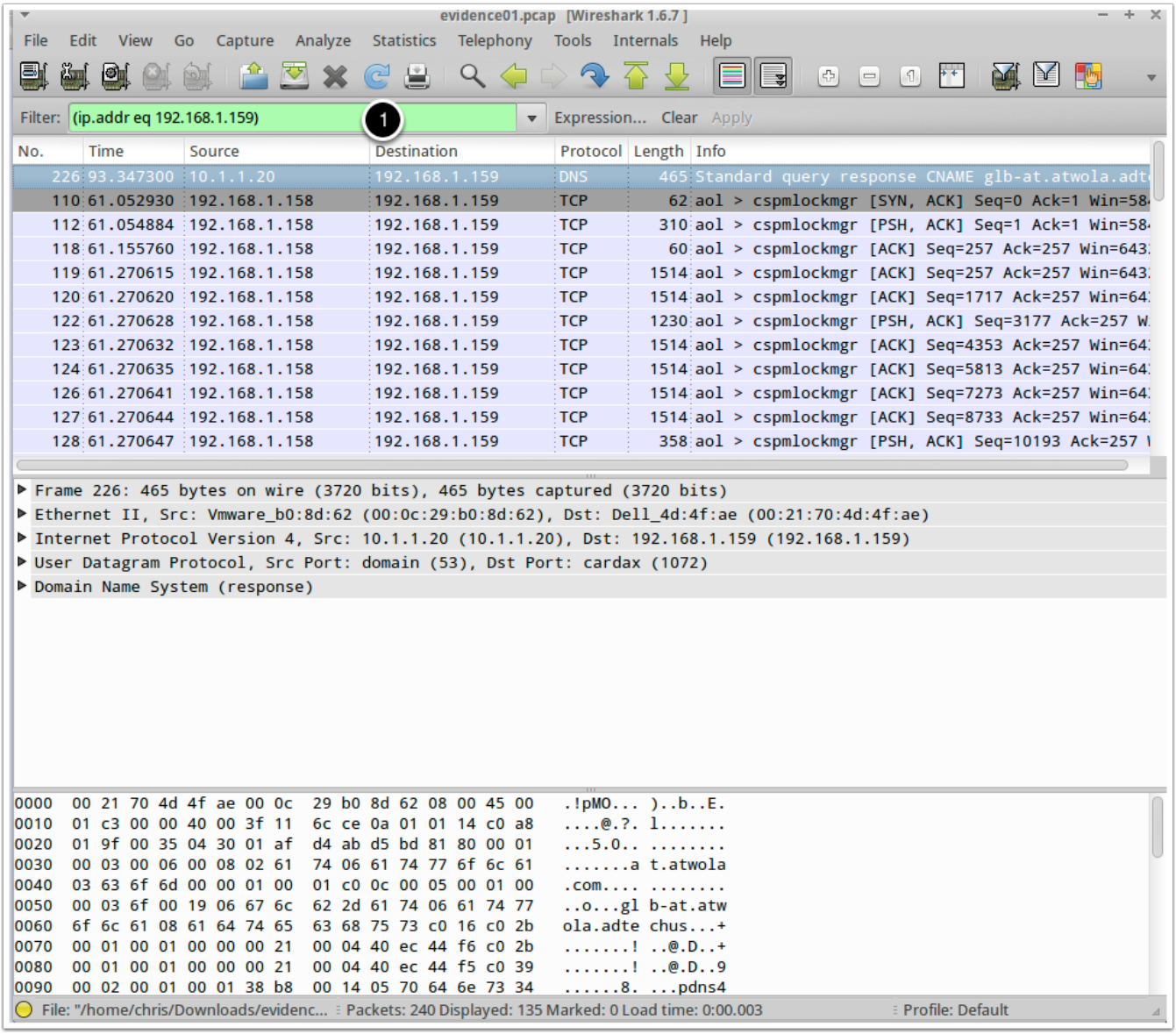
TCP Stream

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.



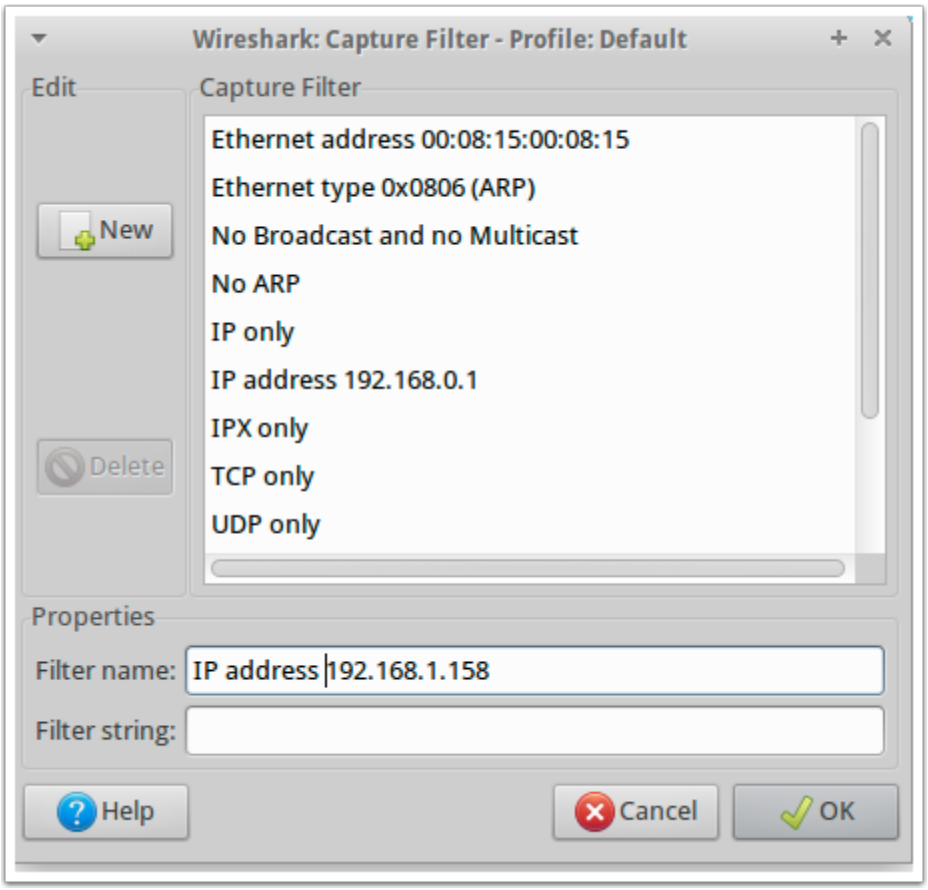
Filters

Instead of sorting we could chave 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



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.

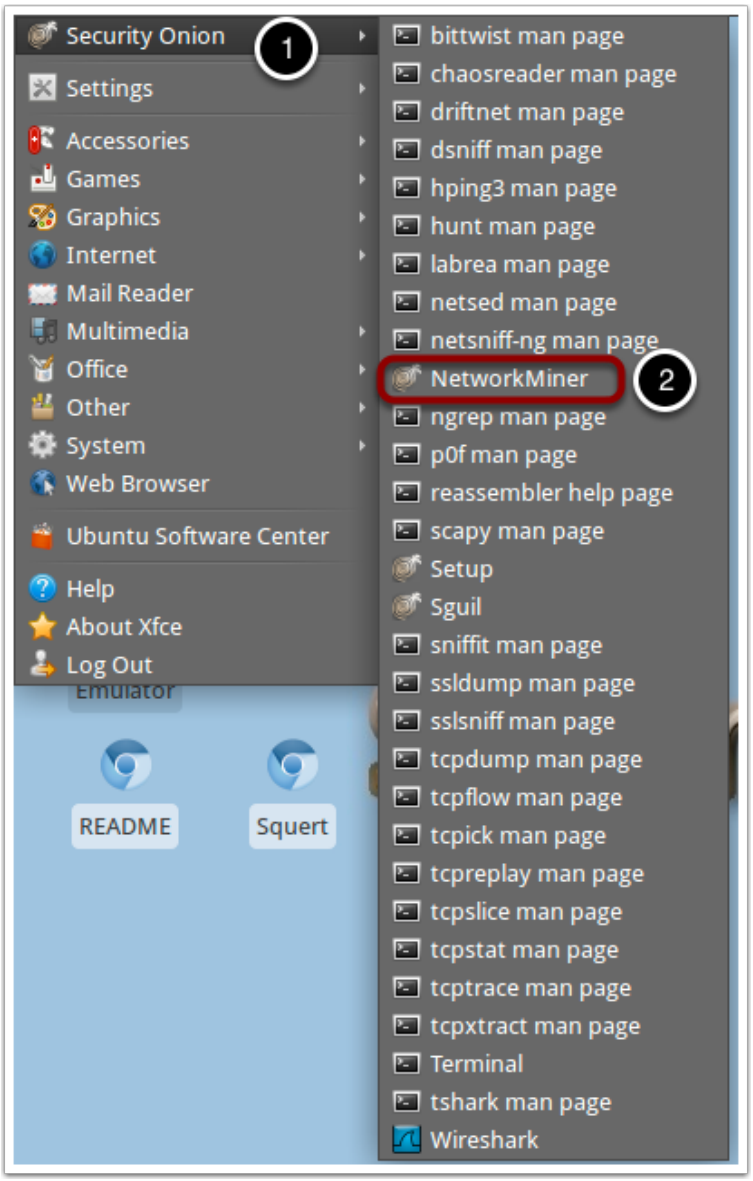


Close Wireshark

Close Wireshark prior to opening Network Miner

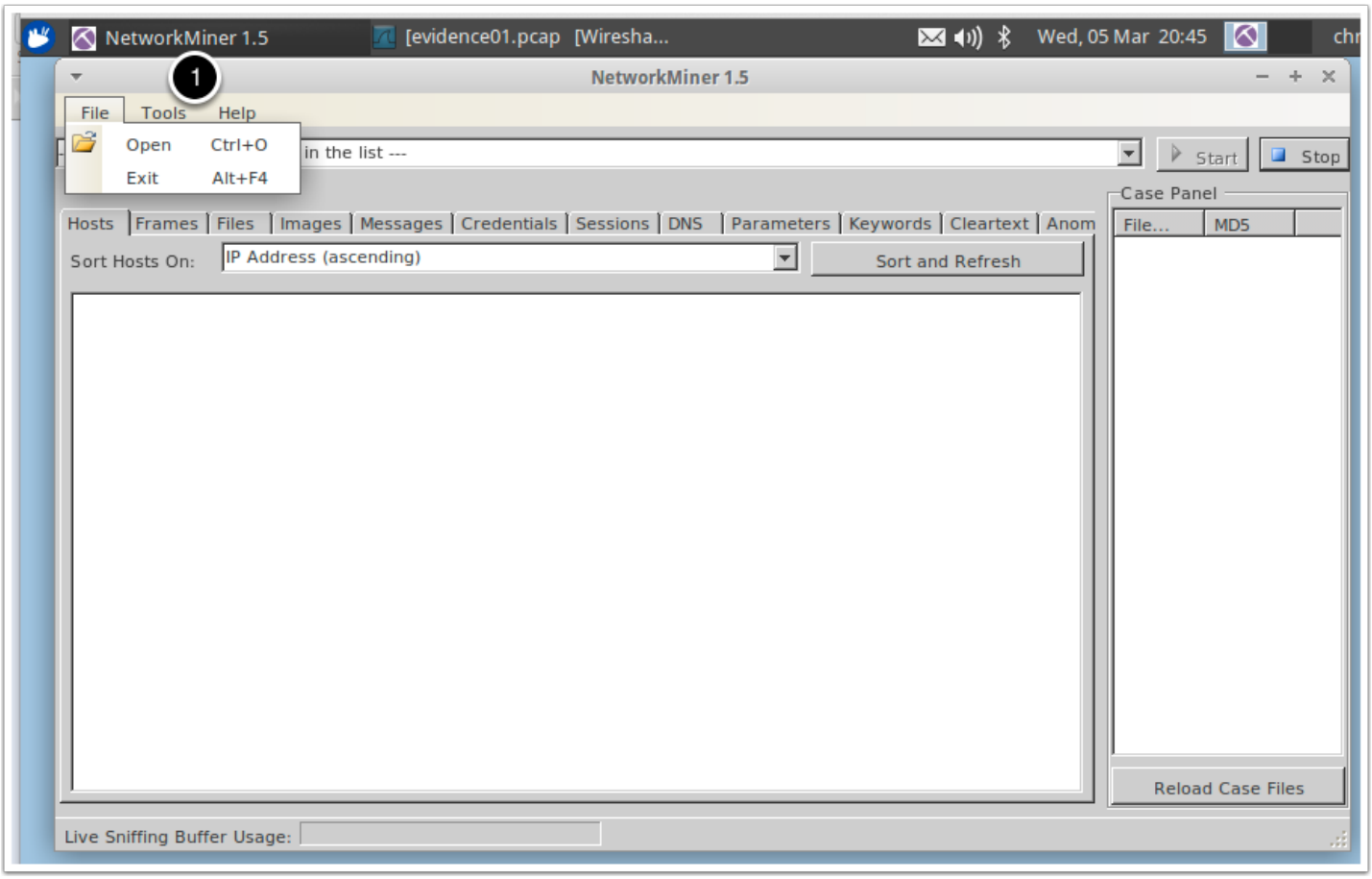
Network Miner

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.



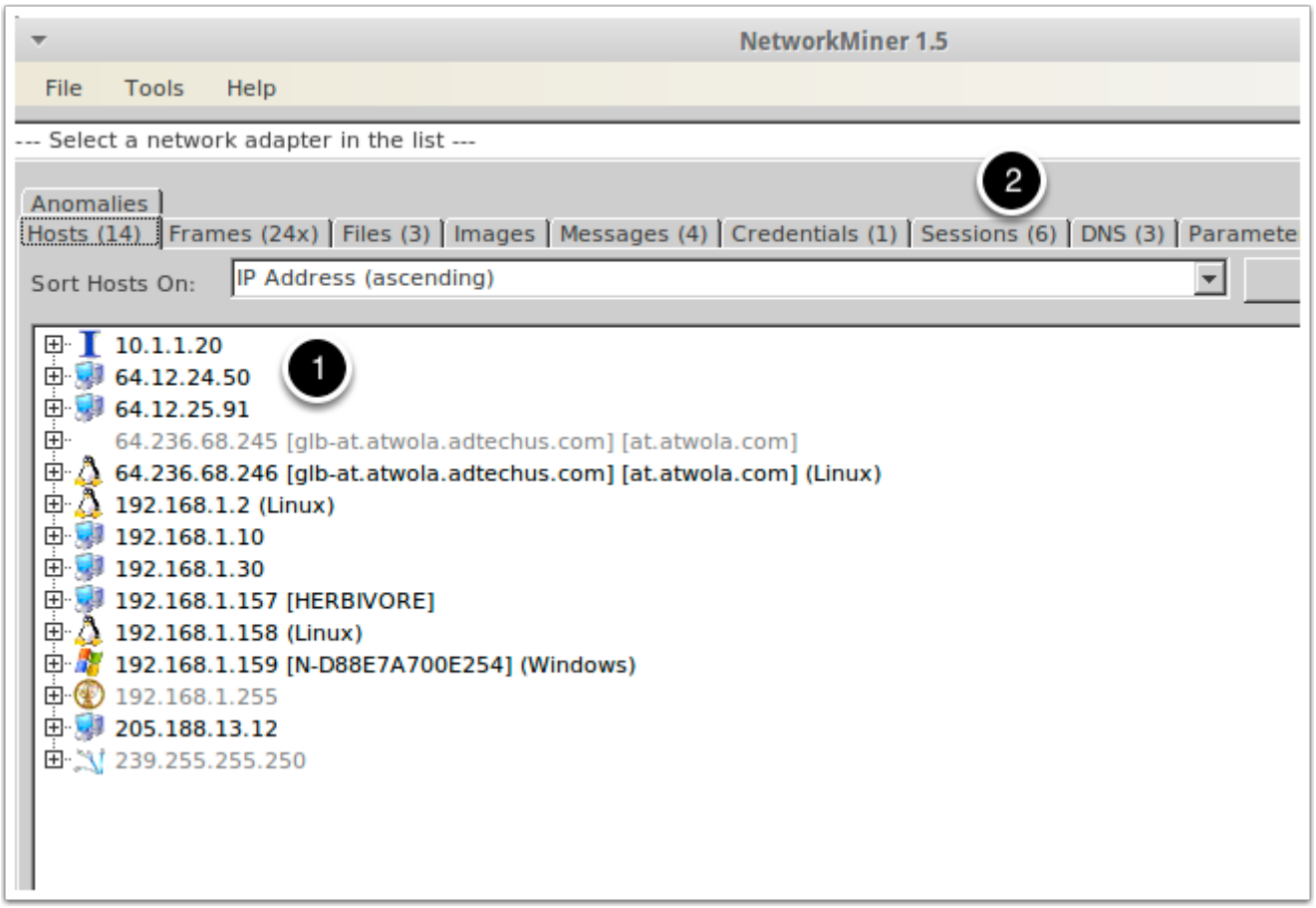
Network Miner

Open the same pcap file
1. Click File > Open
File is /Downloads/Lab 1/evidence01.pcap (same as previous exercise)



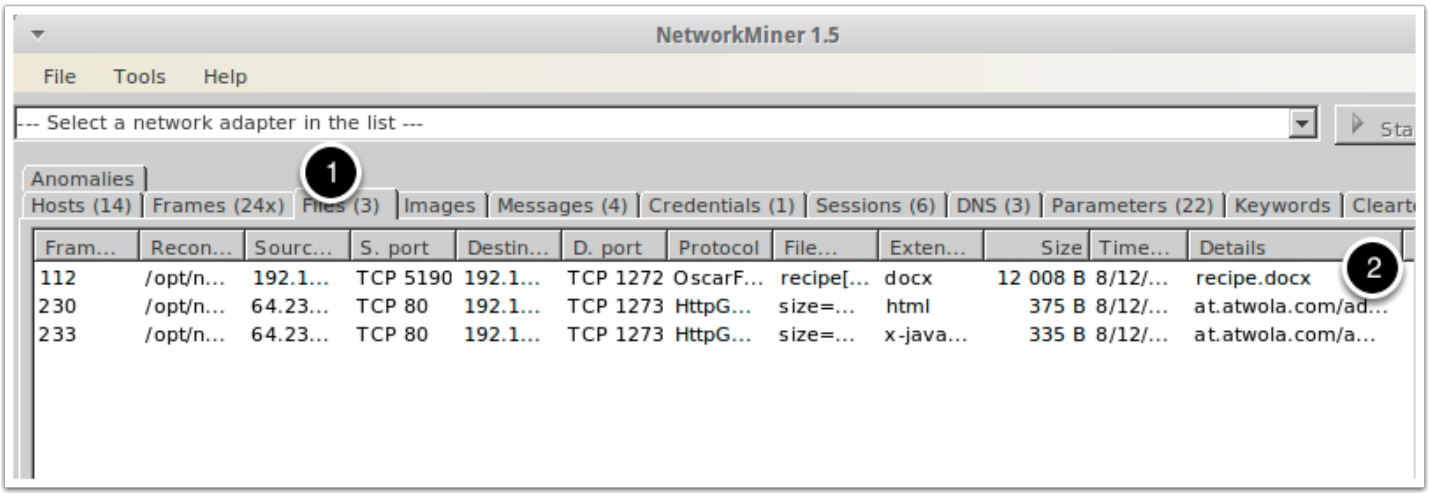
Network Miner

As you can see Network Miner parses the pcap file for you. You can see the different IP adresses 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.



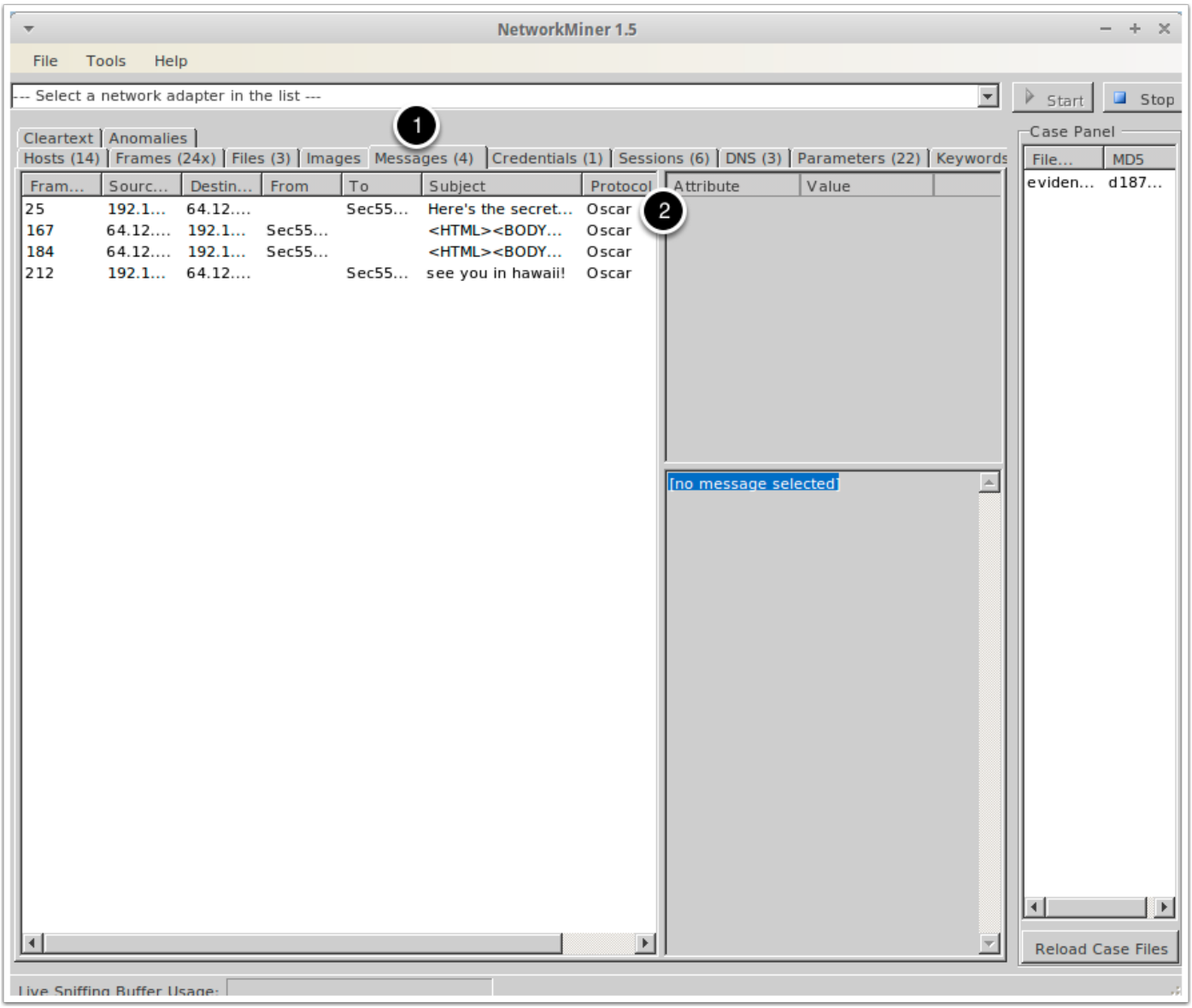
Network Miner File Extraction

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

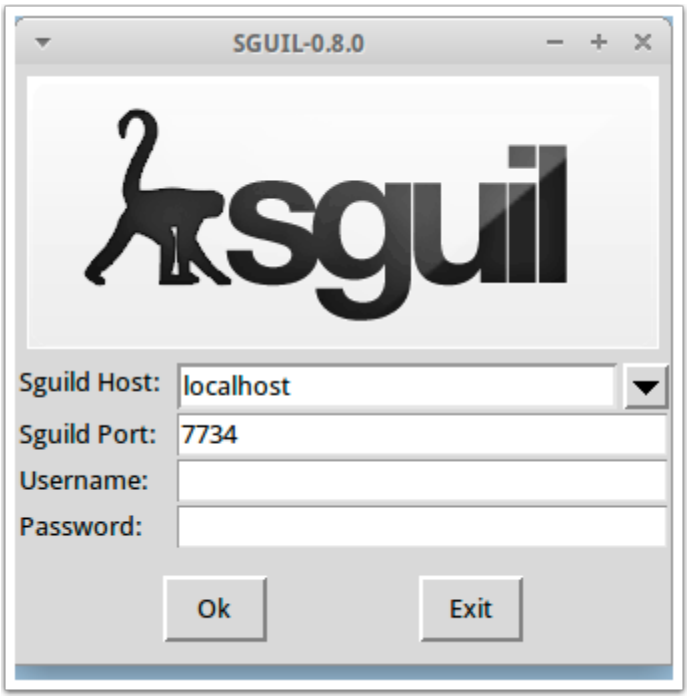
Close Network Miner prior to opening Sguil

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.
Firs double click on the Sguil icon

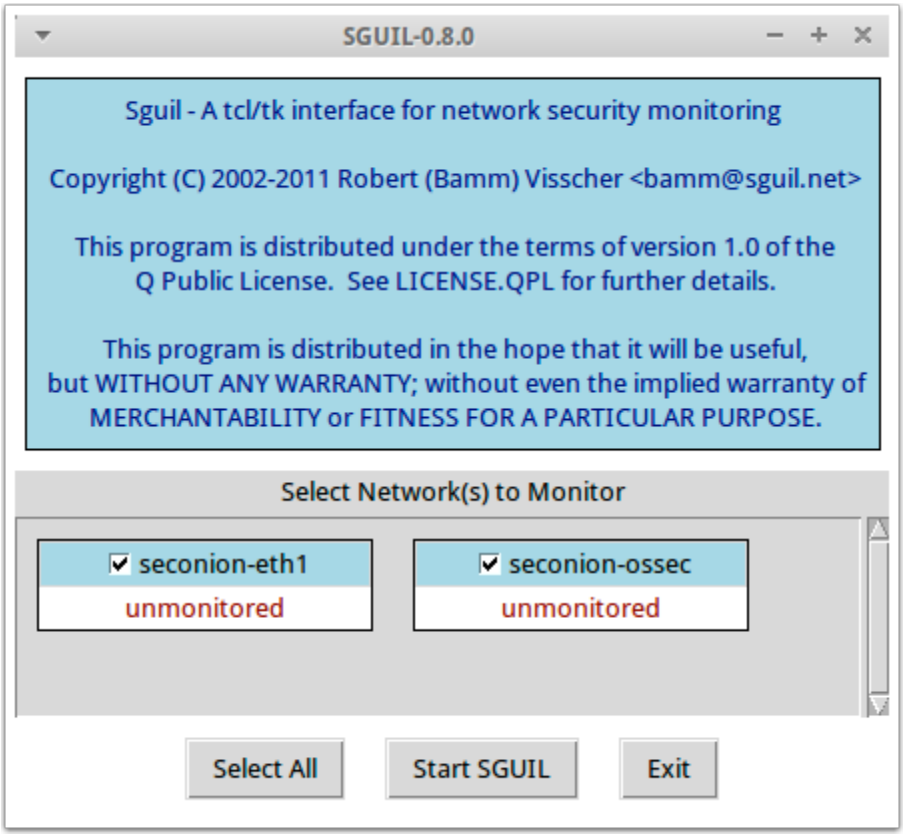
Sguil Login

Enter your username and password:
User: student
Password: password



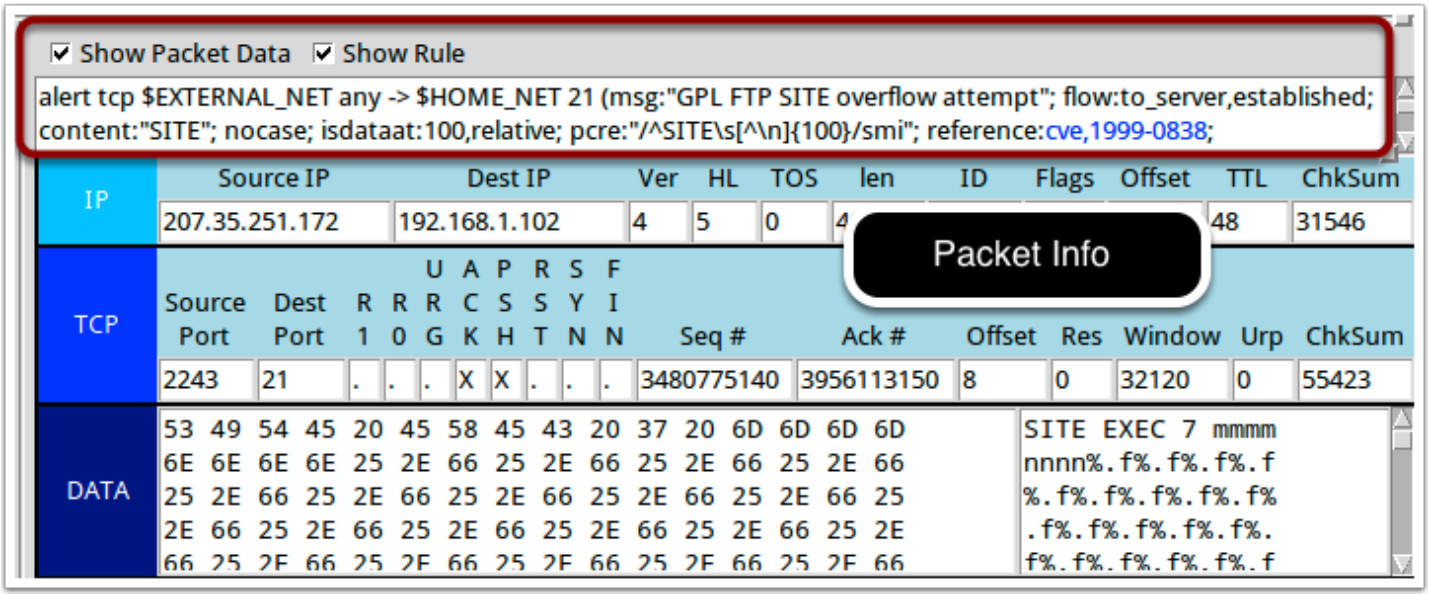
Start Sguil

Check both boxes and start Sguil



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.

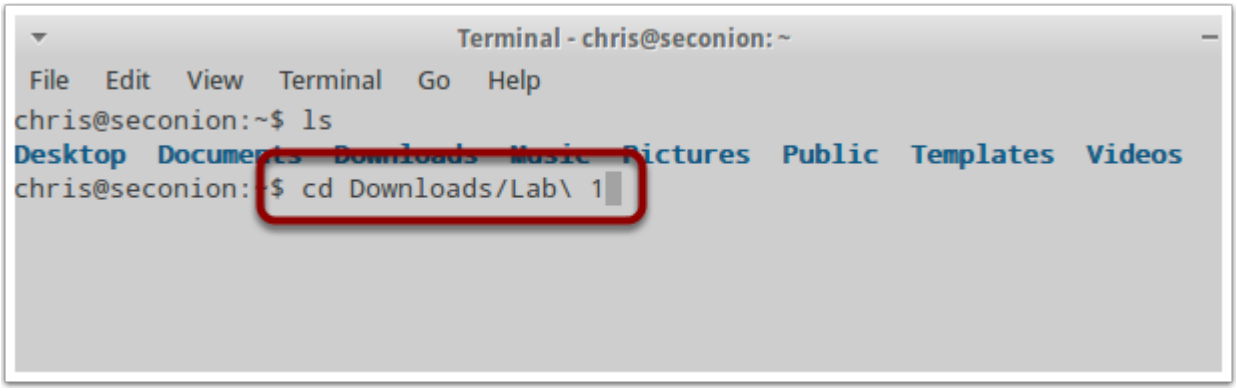


Using tcpreplay

tcpreplay allows you to play packtes on an interface.
1. Open a terminal window
2. Sguil should be running when completing the next steps

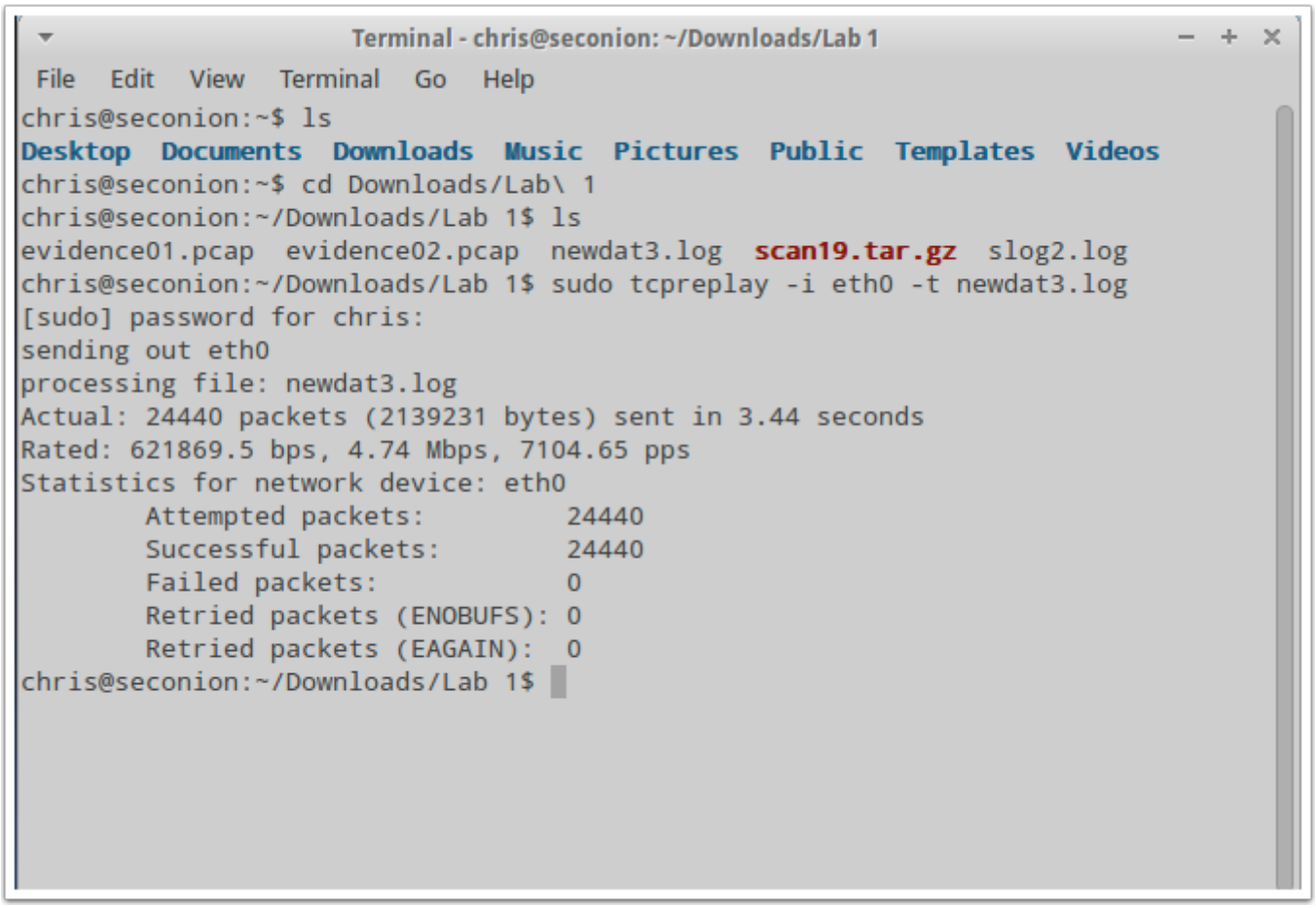
tcpreplay

change directories to Downloads/Lab 1



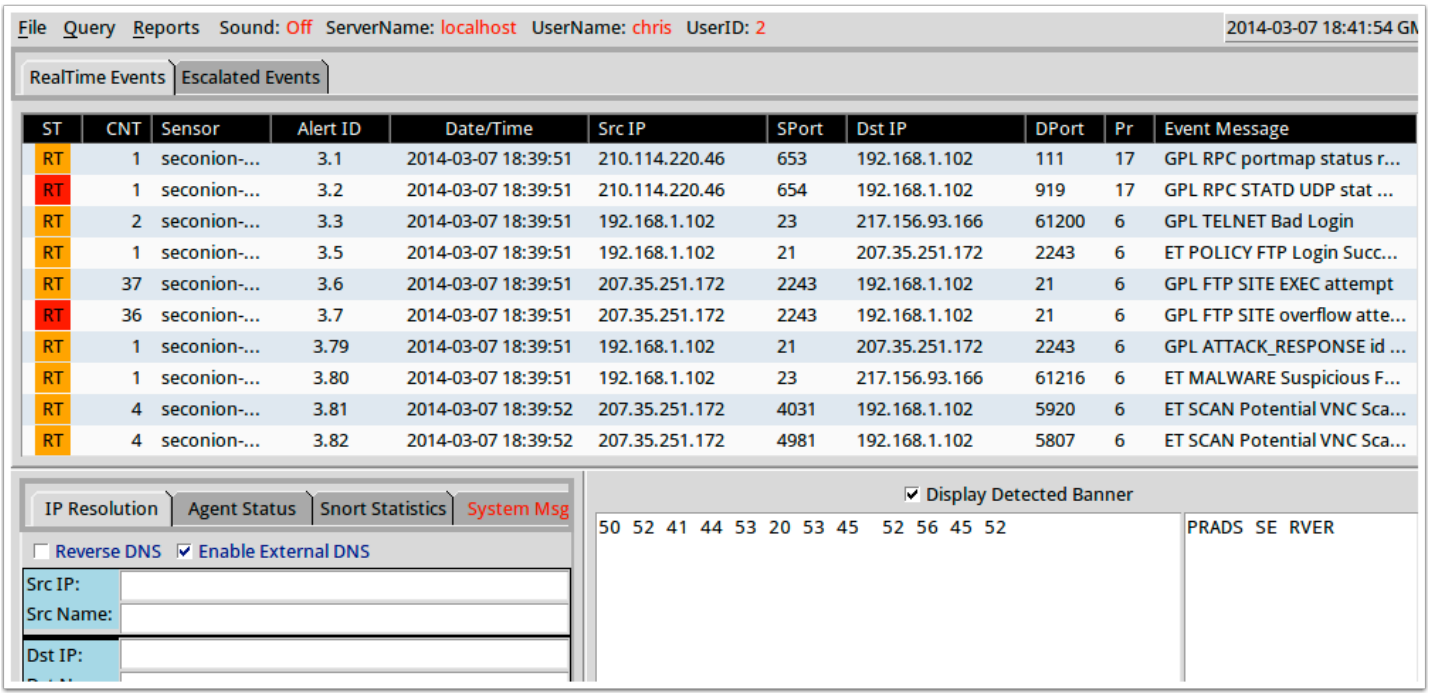
Play the file

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.



Sguil

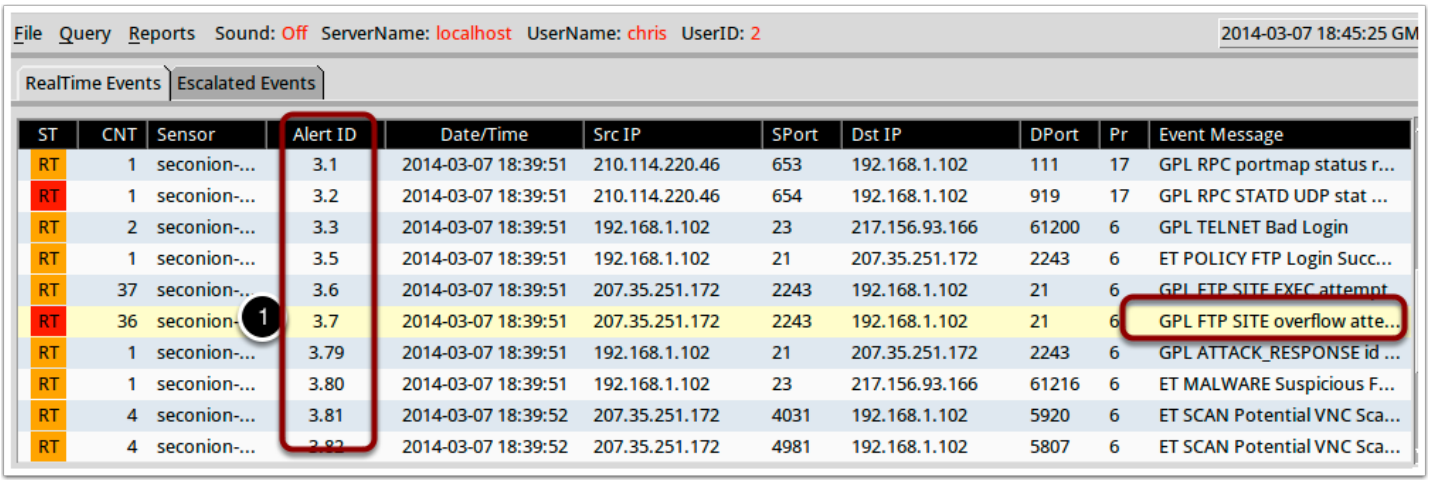
Now switchback to Sguil. You should see a variety of alert as depicted below.



Sguil

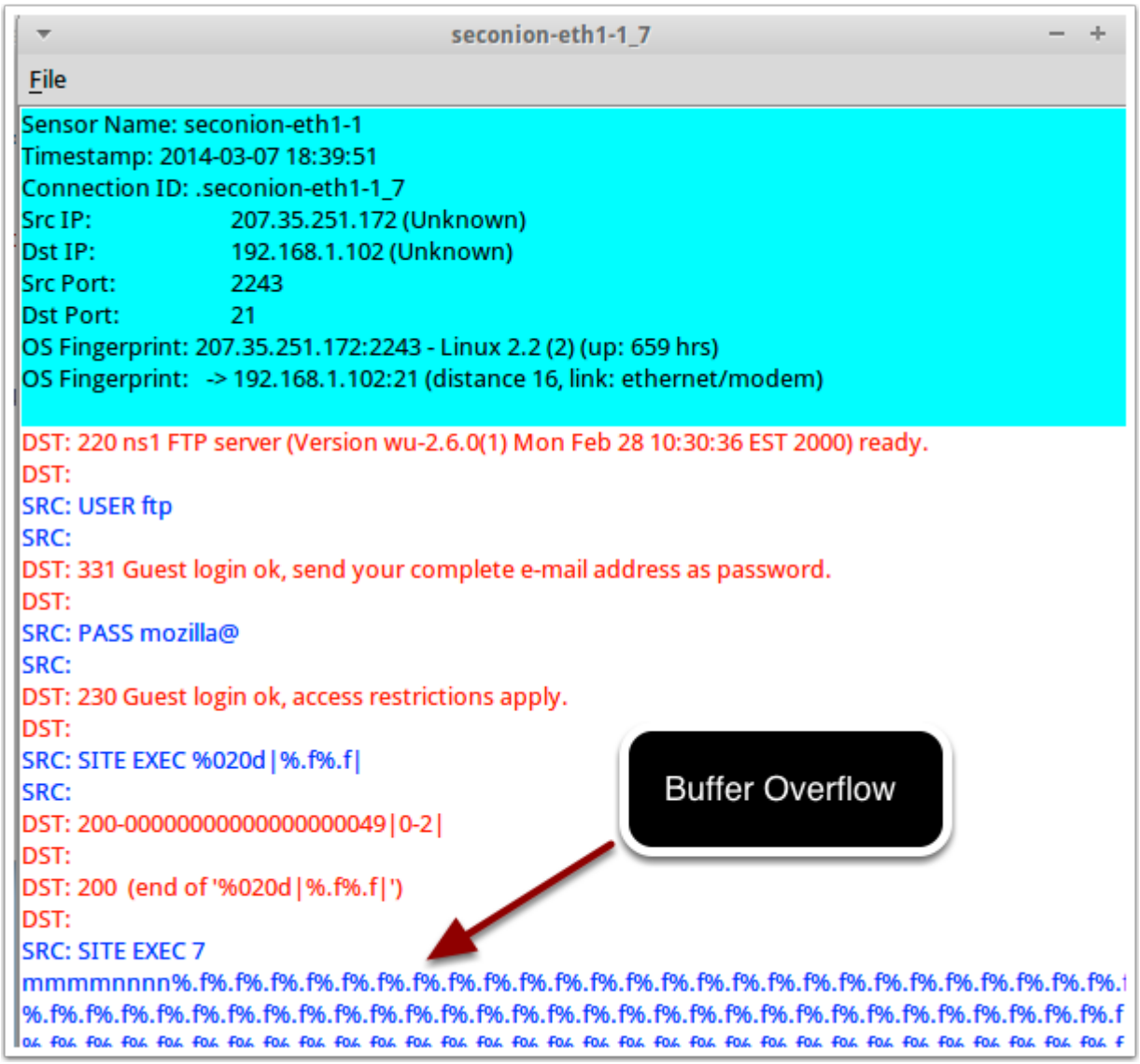
Find the GPL FTP SITE overflow attempt alert

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



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?



```
Sensor Name: seconion-eth1-1
Timestamp: 2014-03-07 18:39:51
Connection ID: .seconion-eth1-1_7
Src IP:             207.35.251.172 (Unknown)
Dst IP:             192.168.1.102 (Unknown)
Src Port:           2243
Dst Port:           21
OS Fingerprint: 207.35.251.172:2243 - Linux 2.2 (2) (up: 659 hrs)
OS Fingerprint:   -> 192.168.1.102:21 (distance 16, link: ethernet/modem)

DST: 220 ns1 FTP server (Version wu-2.6.0(1) Mon Feb 28 10:30:36 EST 2000) ready.
DST:
SRC: USER ftp
SRC:
DST: 331 Guest login ok, send your complete e-mail address as password.
DST:
SRC: PASS mozilla@
SRC:
DST: 230 Guest login ok, access restrictions apply.
DST:
SRC: SITE EXEC %020d|%.f%.f|
SRC:
DST: 200-00000000000000000049|0-2|
DST:
DST: 200  (end of '%020d|%.f%.f|')
DST:
SRC: SITE EXEC 7
mmmmnnnn%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.
%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f
```

Buffer Overflow

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

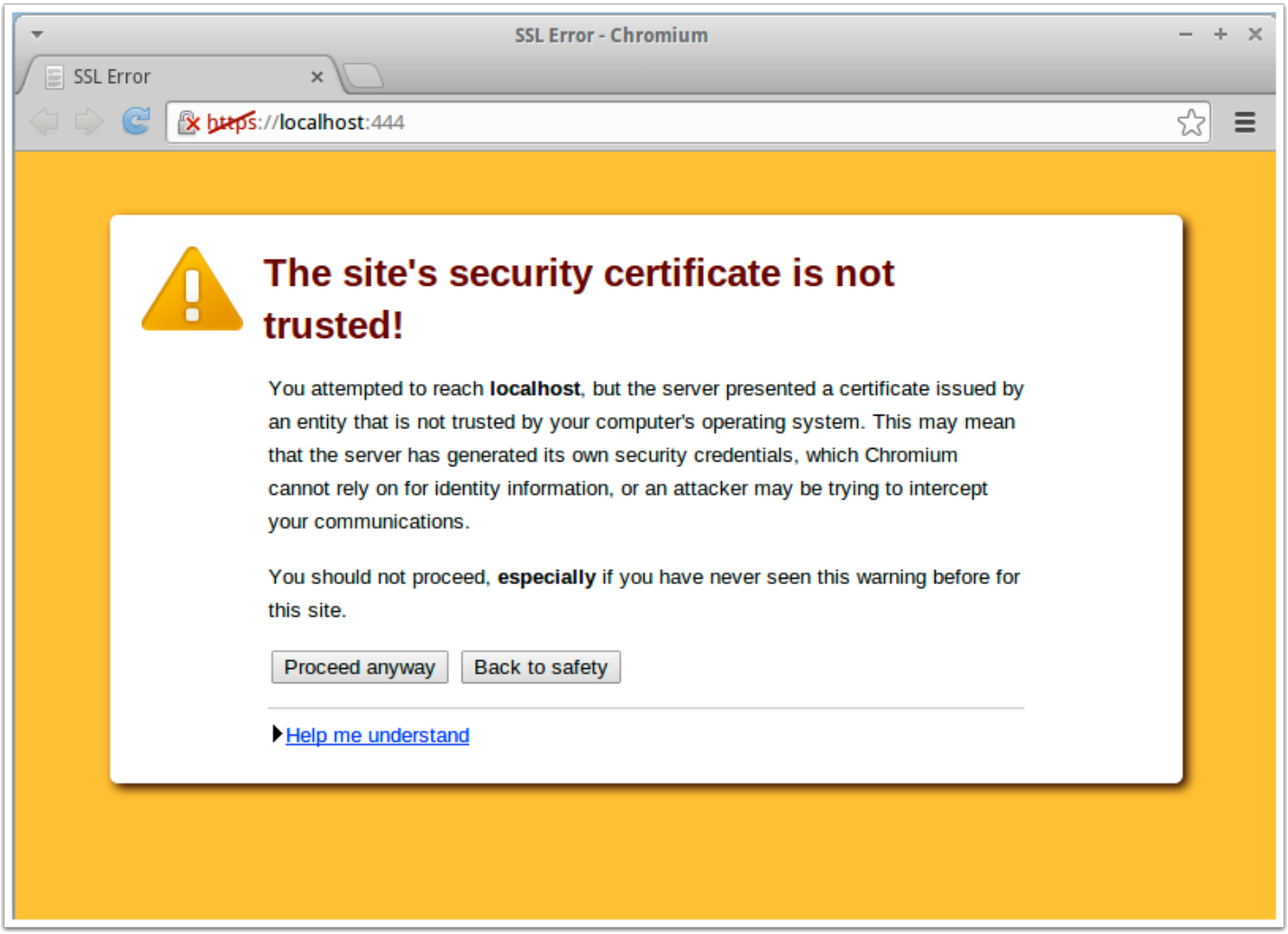
Close Sguil and the Terminal Window

Using Snorby

Double click on the Snorby icon

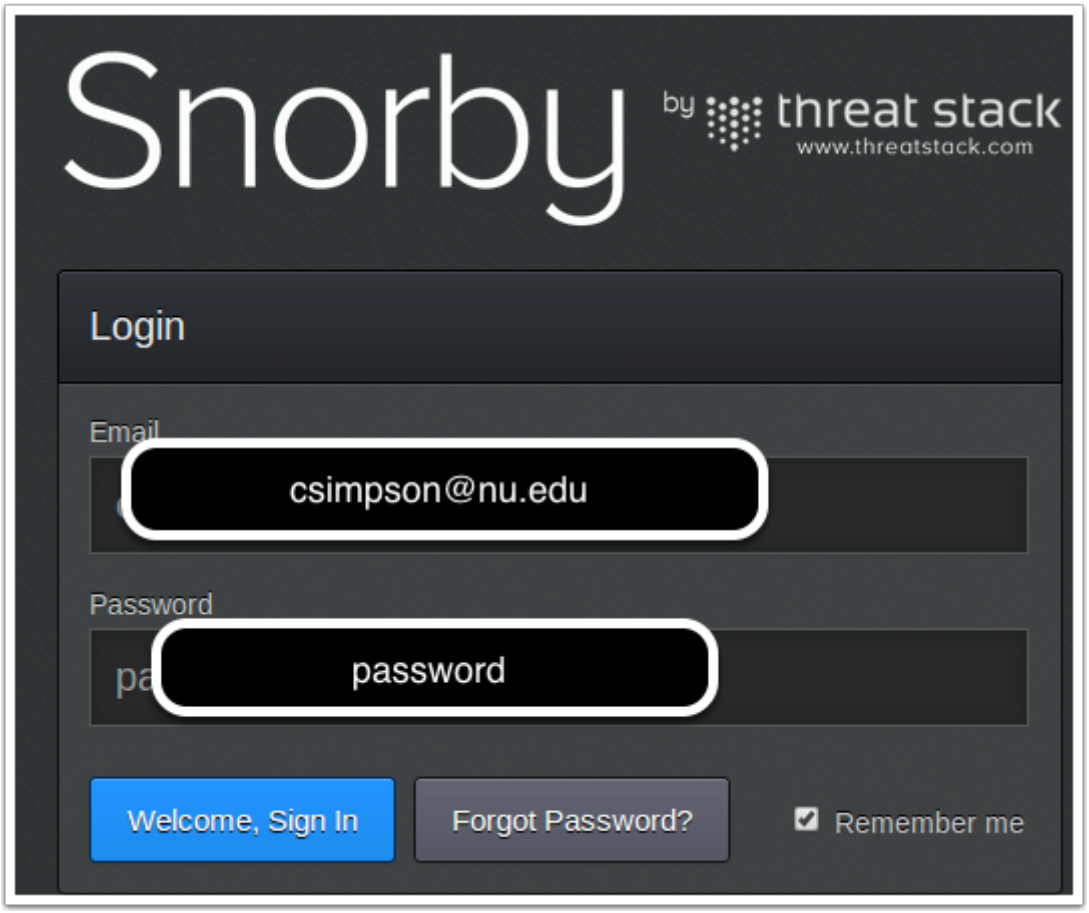
Using Snorby

Click Proceed anyway



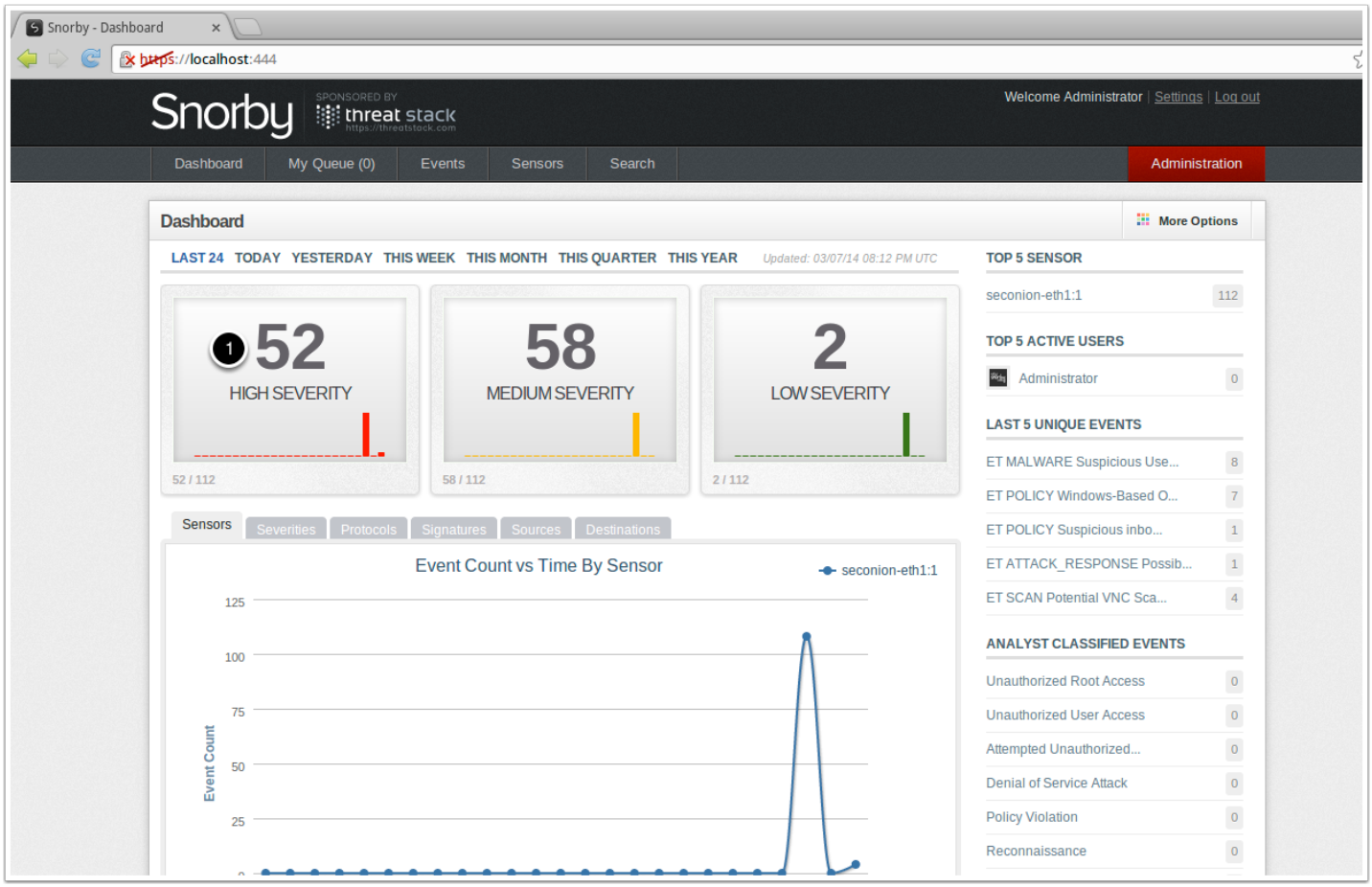
Using Snorby

1. Login to Snorby



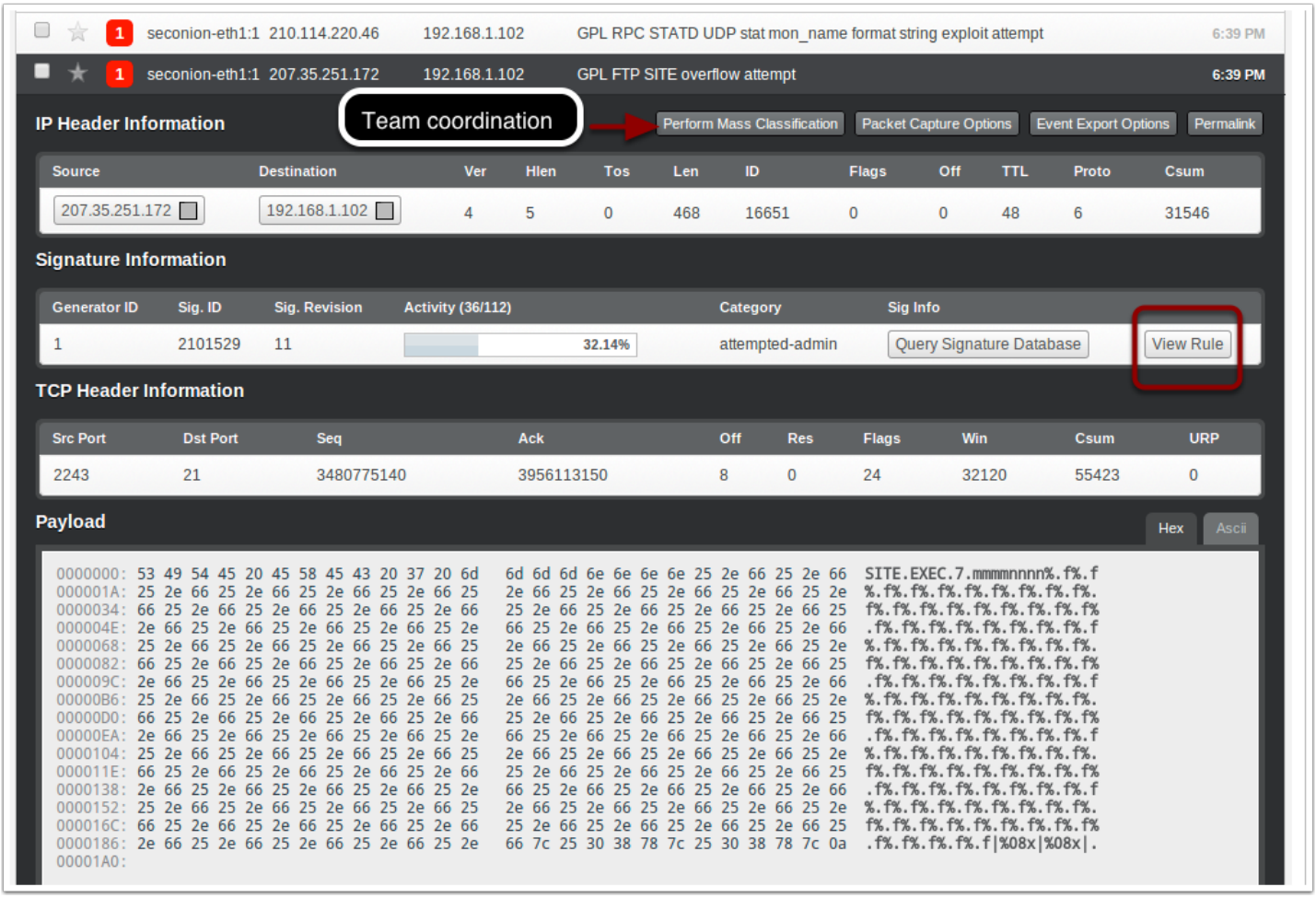
Snorby Opening Screen

1. Click on High Severity to see specific alerts



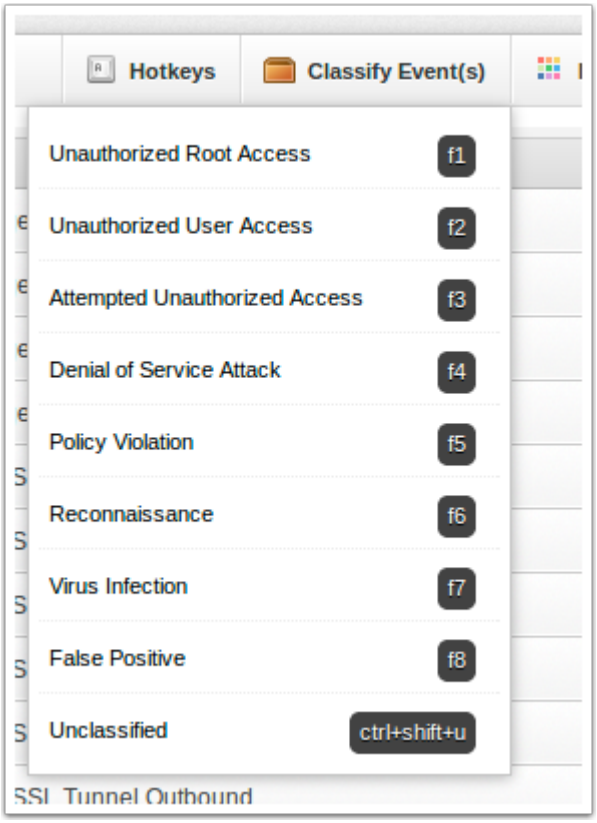
Snorby Alerts

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 ca export event information (including email and perform classification



Snorby Classifying Events

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

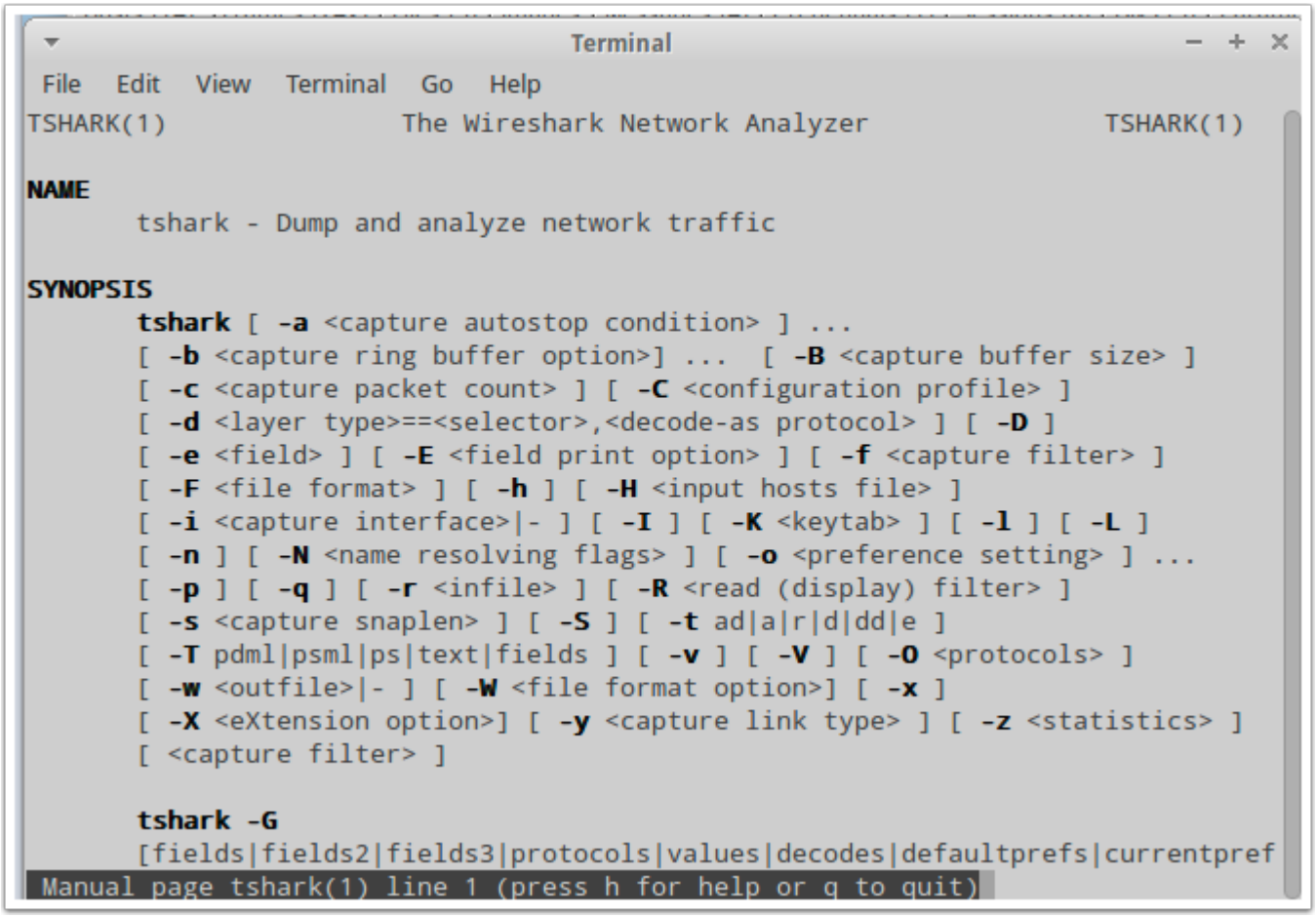


Next Steps

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 en 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?