

Week	Date	Teaching	Attended
9	Mar 2013	Lab 9: Network Forensics	
<p>Aim: The aim of this lab is to further investigate network-based forensic investigations, including network evidence capture and analysis using TShark, Wireshark and NetWitness tools.</p> <p>Time to complete: 4 hours (Two supervised hours in the lab, and two additional hours, unsupervised).</p> <p>Activities:</p> <ul style="list-style-type: none"> • Complete Lab 9: Network Forensics http://www.dcs.napier.ac.uk/~cs342/CSN10102/Lab9.pdf <p>Learning activities: At the end of these activities, you should understand:</p> <ul style="list-style-type: none"> • How to capture network-based evidence. • How to analyse network packet captures using various methods. • How to analyse files for their endpoints, and protocols over time. • How to investigate sessions and reconstruct data. <p>Reflective statements (end-of-exercise): What might be the problems in collecting network-based evidence in a proactive manor? Why might specifying a maximum size of capture files be important? How would you go about analysing a very large network evidence trace file? Which tools would be best for network-based digital evidence analysis on a Windows system?</p>			

Lab 9: Network Forensics

Rich Macfarlane 2013

9.1 Details

Aim: The aim of this lab is to investigate network-based digital investigation, including gathering and analysis of network-based evidence.

9.2 Activities – Network Forensics

Many different methodologies exist for forensic investigations in general, and network-based digital investigations have specific techniques. A very simplified process is shown below, and this lab will look at the basic steps of Collecting and then Analysing evidence in a network-based digital investigation.

Network Forensic Steps:

1. Gathering Network-based Evidence
2. Analysis of Network-based Evidence
3. Reporting

■ Gathering Network-based Evidence

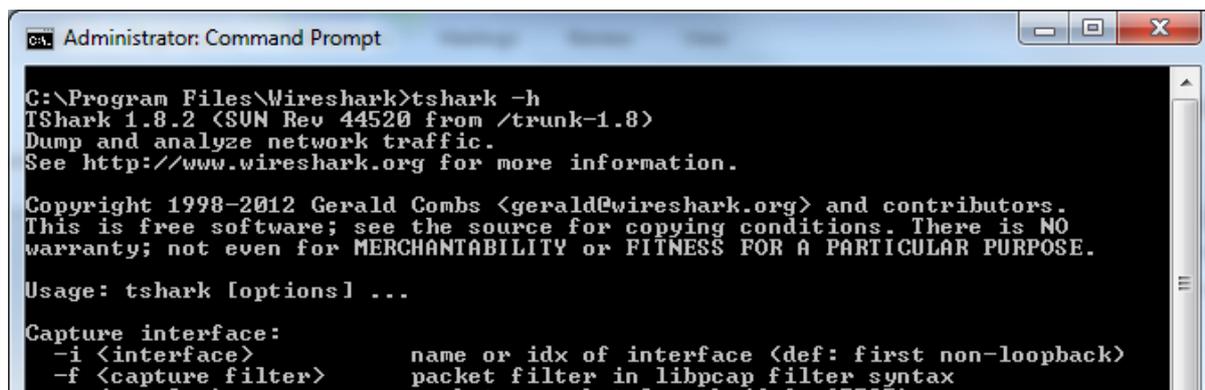
Many different types of network-based digital evidence can be gathered by organisations. There are many tools which can be used to help collect and collate this evidence. This section of the lab introduces some of the tools and techniques for network-based evidence gathering.

TShark

TShark is a command line packet capture and analysis tool. It can capture packets live from a network interface, or read packets from a saved pcap capture file.

If you have Wireshark installed on your system, change to the Wireshark directory, and use the following to check the Dumpcap options:

```
tshark -h
```



```
Administrator: Command Prompt
C:\Program Files\Wireshark>tshark -h
TShark 1.8.2 (SUN Rev 44520 from /trunk-1.8)
Dump and analyze network traffic.
See http://www.wireshark.org for more information.

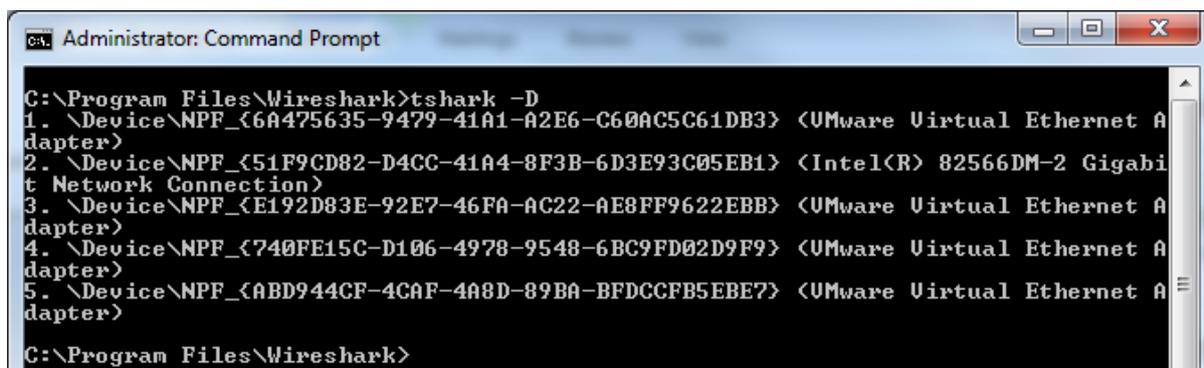
Copyright 1998-2012 Gerald Combs <gerald@wireshark.org> and contributors.
This is free software; see the source for copying conditions. There is NO
warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

Usage: tshark [options] ...

Capture interface:
-i <interface>          name or idx of interface (def: first non-loopback)
-f <capture filter>    packet filter in libpcap filter syntax
-p <packet length>     packet packet length (def: 65535)
```

Check the interfaces available via Dumpcap:

```
tshark -D
```



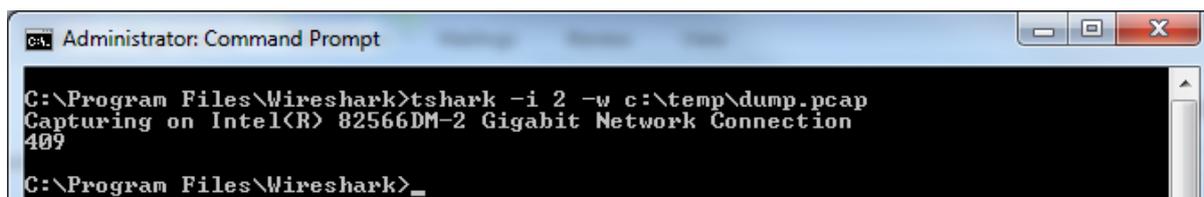
```
Administrator: Command Prompt
C:\Program Files\Wireshark>tshark -D
1. \Device\NPF_{6A475635-9479-41A1-A2E6-C60AC5C61DB3} <UMware Virtual Ethernet A
dapter>
2. \Device\NPF_{51F9CD82-D4CC-41A4-8F3B-6D3E93C05EB1} <Intel(R) 82566DM-2 Gigabi
t Network Connection>
3. \Device\NPF_{E192D83E-92E7-46FA-AC22-AE8FF9622EBB} <UMware Virtual Ethernet A
dapter>
4. \Device\NPF_{740FE15C-D106-4978-9548-6BC9FD02D9F9} <UMware Virtual Ethernet A
dapter>
5. \Device\NPF_{ABD944CF-4CAF-4A8D-89BA-BFDCCFB5EBE7} <UMware Virtual Ethernet A
dapter>
C:\Program Files\Wireshark>
```

Capture some packets from your Ethernet interface, and dump to a file, with a command similar to the following:

```
tshark -i 2 -w c:\temp\dump.pcap
```

Create some traffic using a web browser.

Use CTRL+C to stop the capture.



```
Administrator: Command Prompt
C:\Program Files\Wireshark>tshark -i 2 -w c:\temp\dump.pcap
Capturing on Intel(R) 82566DM-2 Gigabit Network Connection
409
C:\Program Files\Wireshark>_
```

View the details of the capture file in Wireshark using:

```
start wireshark c:\temp\dump.pcap
```

Questions

Q: Did you successfully save your capture to disc, and view in Wireshark?

YES/NO

TShark differs from TCPDump and Wireshark in that it allows advanced specification of when to stop collecting the traffic.

Try using the `-c` argument to only capture 1000 packets.

Questions

Q: What is the command?

Q: Did you successfully save your capture to disc?

YES/NO

Start Wireshark with the capture and scroll down to the bottom of the capture.

Questions

Q: What is the packet number of the last packet?

TShark can also be set up to stop collecting packets based on time and filesize using the `-a` argument.

Try using the `-a` command to capture packets for only 60 seconds:

```
tshark -i 2 -w c:\temp\dump.pcap -a duration:60
```

Create some web traffic before the trace stops.

Questions

Q: How many packets were captured?

List the details of the dump file:

```
dir c:\temp\dump.pcap
```

Questions

Q: What is the size of the file?

Q: What would the size of the file be if you captured this type of traffic for an entire day?

(*60=1hr, *24=1day ... /1000,000,000=GB)

Sometimes capture files of a certain size would be sought after. Files which can be analysed without too much overhead can be more efficient to work with.

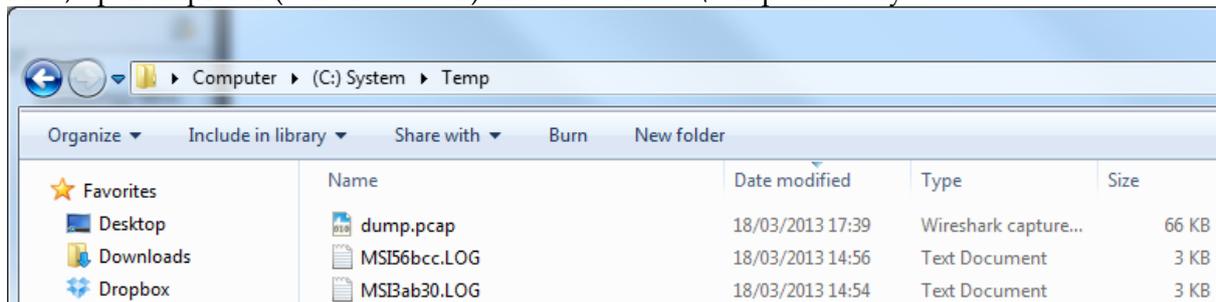
Try using the `-a` command to stop the capture after a file reaches a size of 64 kilobytes:

Questions

Q: What is the tshark command?

Multiple files of a certain size can be saved off using TShark, but care must be taken as captures can quickly fill up your disk!

First, open Explorer (WINDOWS+E) and view the C:\temp directory.



Multiples files can be generated using the -b argument – try creating multiple files of 64Kb.

```
tshark -i 2 -w c:\temp\dump.pcap -b filesize:64
```

Questions

Q. Can you see the files being created?

Use CTRL+C to stop the tshark capture (before it fills up your HDD). Delete the time stamped dump files.

Questions

Q. What is the problem with this method?

A Gigabyte of data per machine would not be unusual per machine per day. Depending on the organisation and use for the network forensic captures, several days worth of data might need to be stored per machine.

Typically at least several days worth of data would need to be stored. To do this data would need to be overwritten after a period of time or when a number of files get to a certain size.

TShark has functionality to overwrite captures; using the -b arguments a ring buffer can be set up. This saves the capture in multiple files and starts overwriting the first file (in the ring buffer) once the last file is full.

This time create a ring buffer of dump files -b argument twice; once to create a new dump file every 3 seconds and secondly to use multiple files in the ring buffer.

```
tshark -i 2 -w c:\temp\dump.pcap -b duration:3 -b files:5
```

Questions

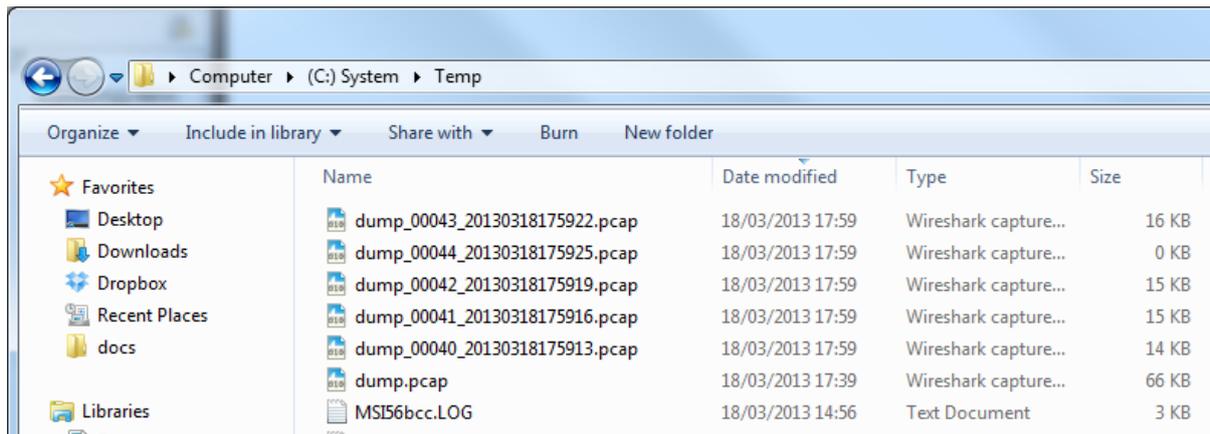
Q. Was the ring buffer capture successful?

YES/NO

Q. How many files are being used in the ring buffer?

Q. When is the capture complete?

```
C:\Program Files\Wireshark>tshark -i 2 -w c:\temp\dump.pcap -b duration:3 -b files:5
Capturing on Intel(R) 82566DM-2 Gigabit Network Connection
4828
```



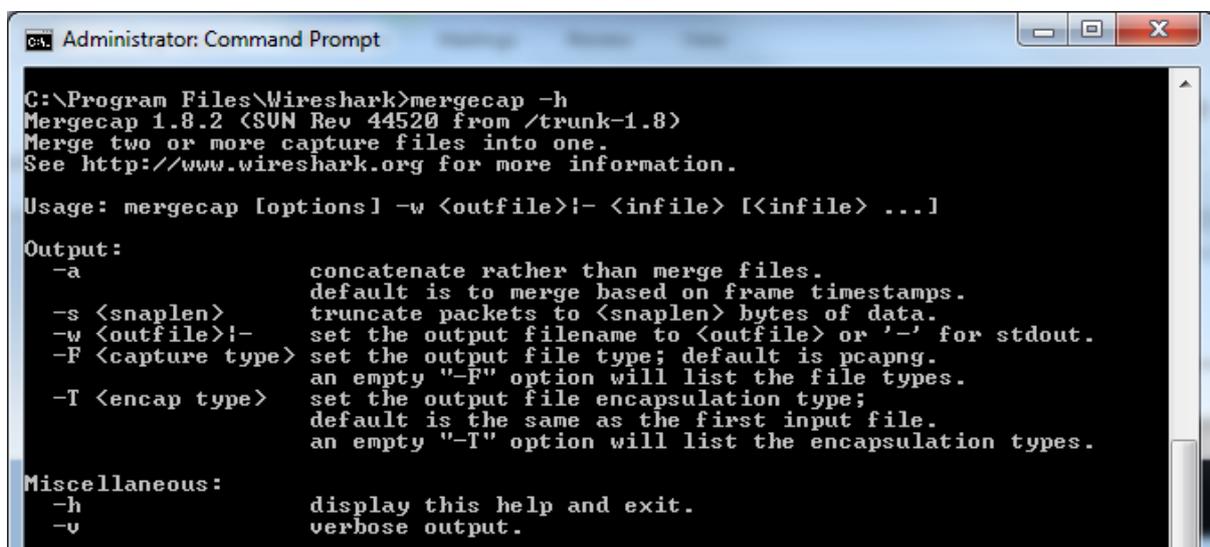
This type of capture can be used to continually collect possible evidence, for later analysis.

Mergecap

Mergecap is a packet capture merge tool. It can combine multiple captures into a new pcap capture file. It can manipulate libpcap format capture files, including files created using Wireshark, TShark and TCPDump.

Use the `-h` flag to check the options:

```
mergecap -h
```



We can try to merge our ring buffer files together into a single capture. Before we merge open one of the ringz buffer files in Wireshark.

Questions

Q: What is the total number of packets in the capture?

Q: What is the size of the file?

Use mergecap to create a single capture file from our ring buffer files:

```
mergcap -w c:\temp\mergedump.pcap c:\temp\dump_*.pcap -a
```

Open the new capture file in Wireshark.

Questions

Q: What is the total number of packets in the capture?

Q: What is the size of the new file?

Analysis of Network Forensic Evidence

Many different methodologies exist for network-based evidence analysis, and many tools can be used. This section of the lab introduces some of the types of network-based evidence analysis and some of the well known tools.

Analysis of Entire Evidence (Full Content Data)

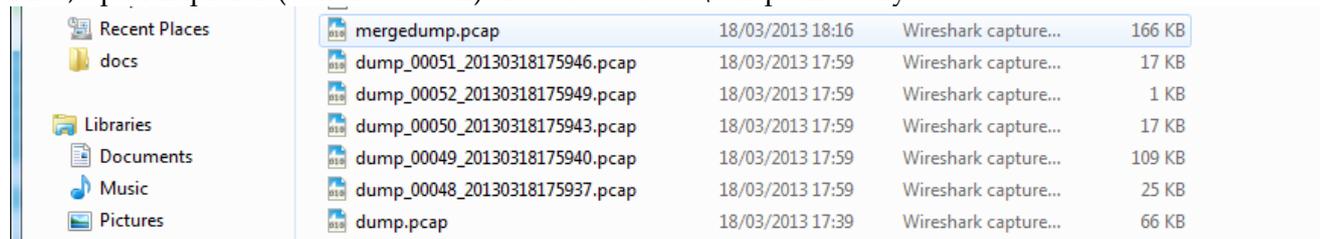
Full content data is the type of data we collected in the previous section. All packets, with full content of every packet. This gives the analyst access to all of the network-based evidence, which can be overwhelming. It can however allow the analysis of the entire traffic which can be used to derive statistics, and to drill right down to details of specific packets, and to follow an attacker via his actions through the entire network.

As we have seen in the previous section, the downside to this type of data is that it can take up a huge amount of storage, and as we will see it can also take large amounts of time to analyse.

Wireshark

Wireshark is one of the most popular network traffic analysis tools. It runs on many platforms, is free, and is used extensively in industry and for education.

First, open Explorer (WINDOWS+E) and view the C:\temp directory.



Open two of the ring buffer dump files which should contain contiguous chronological data. The 2nd number in the file name is the time stamp and so in the above example, the files ending in 785937 and 75940 should be contiguous.

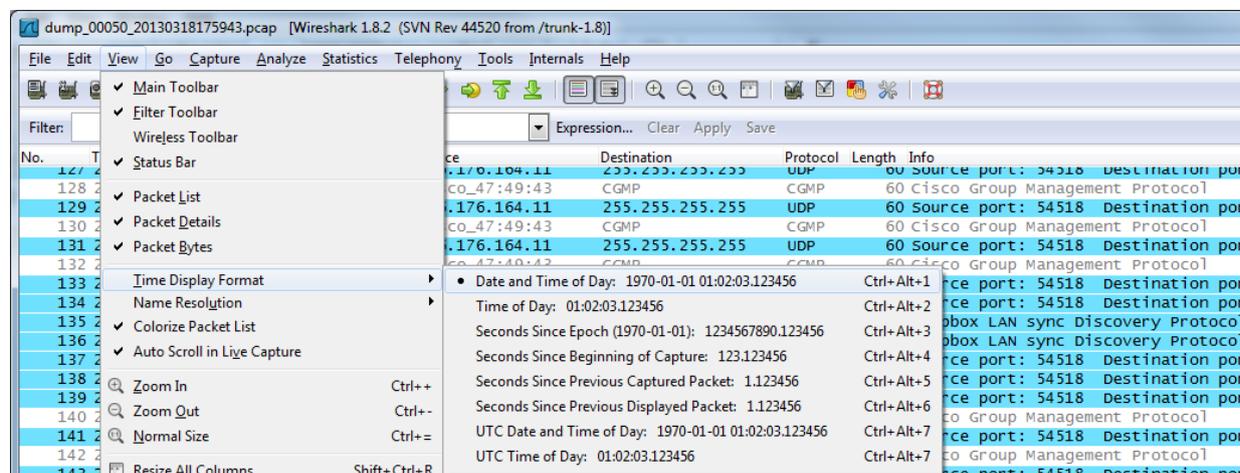
Date and Time

When analysing network evidence it is sometimes important to focus on the timings of incidents. The Time column in Wireshark is derived from the timestamp from libpcap at capture time, but can be displayed in various ways.

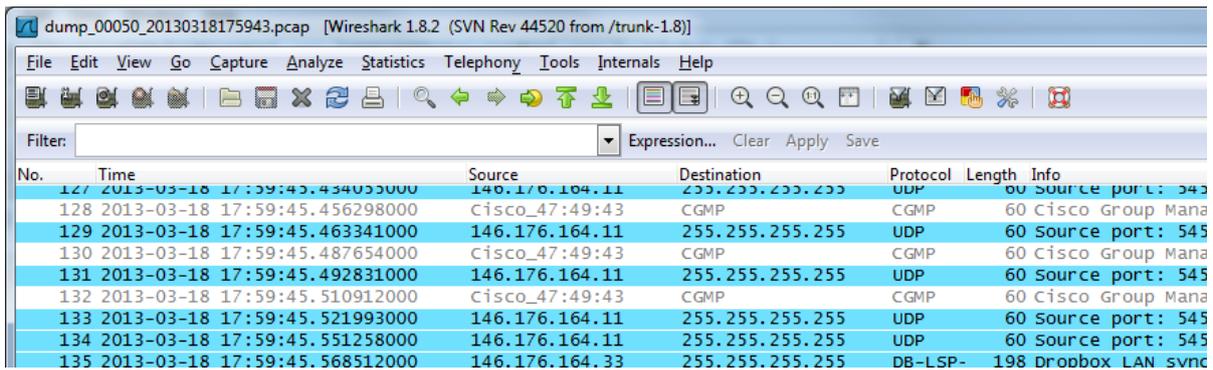
For the open captures, us select the **View>Time Display Format** menu and review the options.

Questions

Q: What is the Time format current being displayed in the Time column?



We cannot compare packets in the 2 different captures using this relative time format. Set the Time column to **Date and Time of Day** for your 2 open captures.



Scroll to the end of the earlier capture, and the beginning of the later capture file.

Questions

Q: Can you see the time and packets where the capture files meet?

Now open the mergedump.pcap capture file and change the time format to the same.

Questions

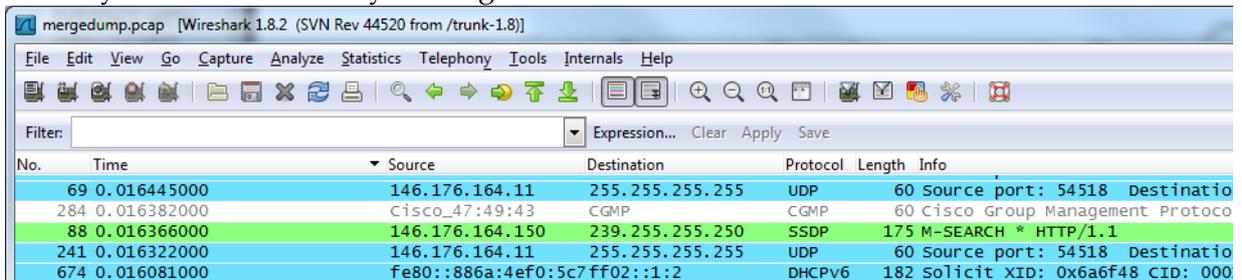
Q: From the Time column, can you identify the packet number of the last packet in the earlier trace file, and the first in the later trace file?

This time format is useful if you want to find day/time of specific incidents. Close the 2 ring buffer trace files.

Questions

Q: Can you tell easily if there are any large delays between packets in the mergedump trace?

Set the Time column to **Seconds Since Previous Displayed** for the mergedump capture, and order by the Time column by clicking the column header.



Questions

Q. Can you easily identify the 3 packets with the largest delays?

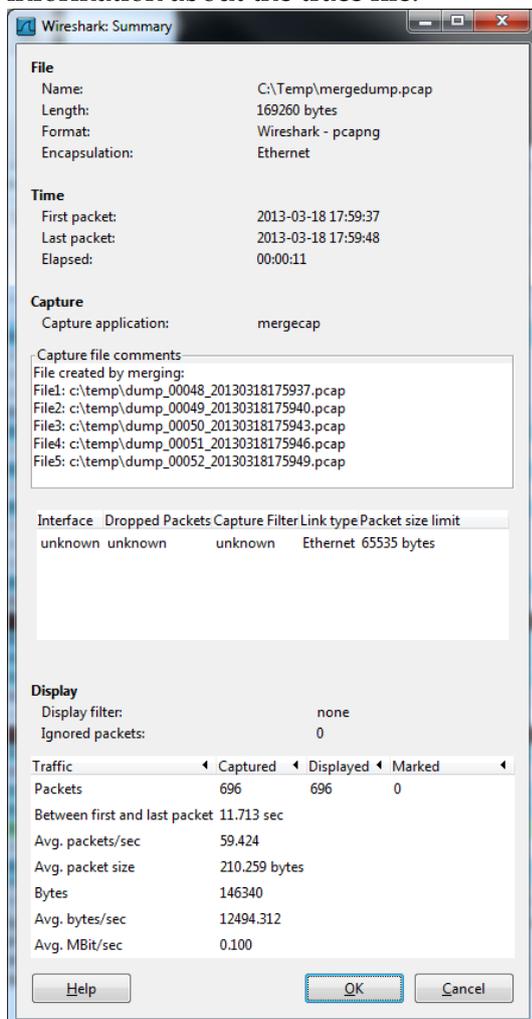
Order by the packet number column to return the trace into chronological order.

Techniques such as this can be useful when trying to identify time gaps leading up to an incident, or machines being particularly overloaded which may signify an attack.

Analysis of Statistics

Full content data can be used to generate network statistics, which can be useful in the early part of the analysis phase, to identify machines and network traffic types involved in any incident.

Select the **Statistics->Summary** menu option, and you should be shown a summary of basic information about the trace file.



This can also be used to get summary information on sections of a trace. Add a display filter of **http** and generate the summary statistics again.

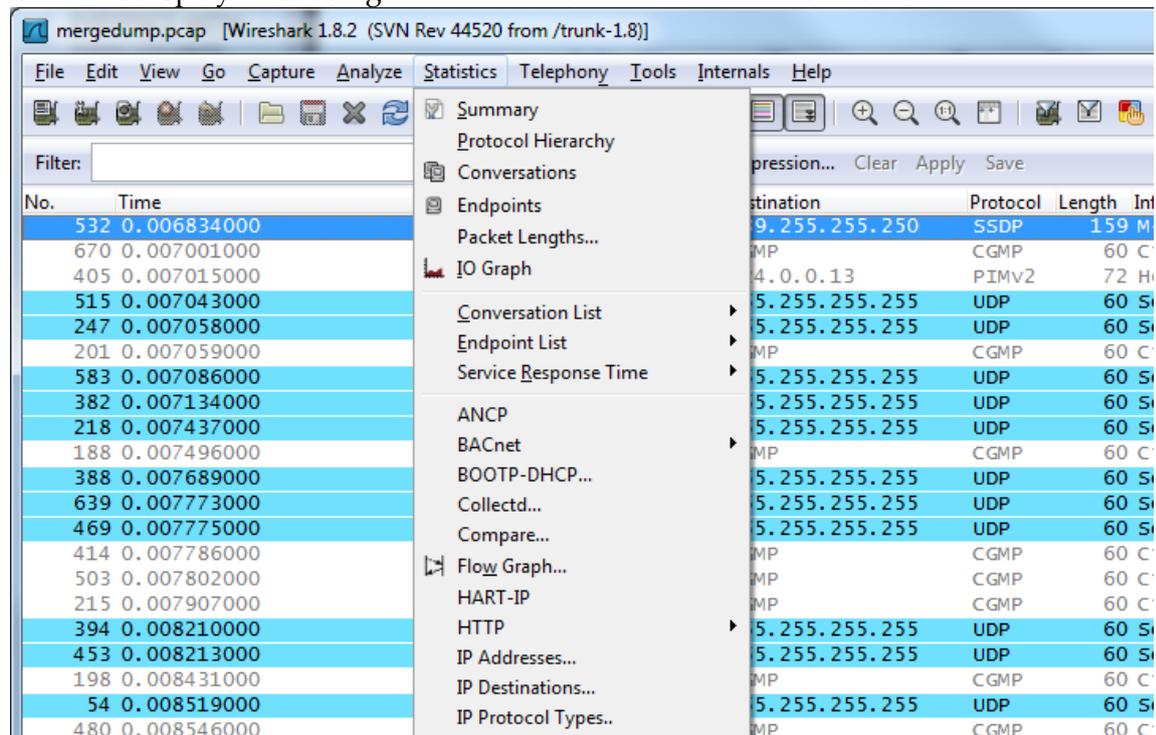
Questions

Q. How many seconds between the 1st and last packets?

This could be used to compare various dump files/protocols/sessions and spot unusually slow processes. It is not unusual for baseline traffic statistics to be stored for this type of comparison, which can identify unusual behaviour/incidents.

Wireshark can produce statistics for a number of different network behaviours and traffic types.

Clear the display filter using the clear button and review the statistics menu.



Close this trace and download the following large network-based evidence capture file, and unpack to the c:\temp directory.



Network Evidence Capture File:

http://www.dcs.napier.ac.uk/~cs342/CSN10102/netfor_capture.zip

Open the capture in Wireshark, and change the Time format to **Time of Day**.

No.	Time	Source	Destination	Protocol	Length	Info
1	13:30:39.582441	192.168.75.1	192.168.75.255	BROWSEFF	216	Get Backup List Request
2	13:30:39.587483	Vmware_Of:71:a3	Broadcast	ARP	42	who has 192.168.75.2? Tell 192.168.75.132
3	13:30:39.594271	Vmware_f5:2e:f3	Vmware_Of:71:a3	ARP	60	192.168.75.2 is at 00:50:56:f5:2e:f3
4	13:30:39.595288	192.168.75.132	192.168.75.2	NBNS	92	Name query NB BILLS<00>
5	13:30:40.614606	192.168.75.1	192.168.75.255	BROWSEFF	216	Get Backup List Request
6	13:30:41.085781	192.168.75.132	192.168.75.2	NBNS	92	Name query NB BILLS<00>
7	13:30:41.634893	192.168.75.1	192.168.75.255	BROWSEFF	216	Get Backup List Request
8	13:30:42.586753	192.168.75.132	192.168.75.2	NBNS	92	Name query NB BILLS<00>
9	13:30:42.655873	192.168.75.1	192.168.75.255	BROWSEFF	225	Browser Election Request
10	13:30:42.679032	Vmware_a7:56:72	Broadcast	ARP	60	who has 192.168.75.2? Tell 192.168.75.146
11	13:30:42.932606	Vmware_f5:2e:f3	Vmware_a7:56:72	ARP	60	192.168.75.2 is at 00:50:56:f5:2e:f3

Questions

Q: What are the start and end times of the trace?

Q: Get summary statistics and check if this matches the start and end packet times?

Statistics on Protocols and Applications

Use the Statistics>Protocol Hierarchy menu option to examine the traffic type within the evidence trace file.

Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100.00 %	18995	100.00 %	9274979	0.027	0	0	0.000
Ethernet	100.00 %	18995	100.00 %	9274979	0.027	0	0	0.000
Internet Protocol Version 4	99.25 %	18853	99.92 %	9267215	0.027	0	0	0.000
User Datagram Protocol	3.77 %	716	1.42 %	131762	0.000	0	0	0.000
NetBIOS Datagram Service	0.31 %	59	0.15 %	13489	0.000	0	0	0.000
SMB (Server Message Block Protocol)	0.31 %	59	0.15 %	13489	0.000	0	0	0.000
SMB MailSlot Protocol	0.31 %	59	0.15 %	13489	0.000	0	0	0.000
Microsoft Windows Browser Protocol	0.31 %	58	0.14 %	13219	0.000	58	13219	0.000
Data	0.01 %	1	0.00 %	270	0.000	1	270	0.000
NetBIOS Name Service	0.25 %	48	0.06 %	5541	0.000	48	5541	0.000
Domain Name Service	2.61 %	496	0.83 %	76929	0.000	496	76929	0.000
Bootstrap Protocol	0.14 %	26	0.10 %	8892	0.000	26	8892	0.000
Hypertext Transfer Protocol	0.44 %	84	0.29 %	26733	0.000	84	26733	0.000
Data	0.02 %	3	0.00 %	178	0.000	3	178	0.000
Transmission Control Protocol	95.02 %	18049	98.41 %	9127237	0.027	8339	3169913	0.009
Hypertext Transfer Protocol	2.42 %	459	3.10 %	287858	0.001	290	162722	0.000
Line-based text data	0.65 %	124	1.01 %	94137	0.000	124	94137	0.000
CompuServe GIF	0.08 %	15	0.09 %	8047	0.000	15	8047	0.000
Portable Network Graphics	0.02 %	3	0.04 %	3793	0.000	3	3793	0.000
eXtensible Markup Language	0.01 %	1	0.01 %	1340	0.000	1	1340	0.000

Questions

Q: What percentage of packets are web browsing packets?

Q: Which protocols can be seen which would encryption traffic?

Q: Approx. what percentage of packets are encrypted?

Q: Which application protocol shows a higher than might be expected amount of traffic?

Display filters can be used to remove traffic we may not be interested in. Try the display filter !udp and generate the protocol statistics again.

Endpoints

Use the Statistics>Endpoints menu option to examine the session endpoints within the evidence trace file.

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
Vmware_c0:00:08	12 318	5 830 706	8 894	5 566 721	3 424	263 985
Broadcast	114	14 959	0	0	114	14 959
Vmware_0f:71:a3	14 244	6 130 861	4 330	492 329	9 914	5 638 532
Vmware_f5:2e:f3	4 612	3 108 841	2 792	2 878 241	1 820	230 600
Vmware_a7:56:72	1 225	367 218	618	79 324	607	287 894
Vmware_34:f9:01	803	368 893	359	77 373	444	291 520
Vmware_f5:23:c8	39	9 672	26	5 226	13	4 446
IPv4mcast_7f:ff:fa	84	26 733	0	0	84	26 733
IPv4mcast_00:00:fc	10	640	0	0	10	640
Vmware_6b:0e:96	4 536	2 691 093	1 976	175 765	2 560	2 515 328
IPv4mcast_00:00:fb	2	164	0	0	2	164
IPv4mcast_00:01:18	3	178	0	0	3	178

Questions

Q: What type of addresses are shown by default?

Change to network addresses, by selecting the IPv4 tab.

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Latitude	Longitude
192.168.75.1	12 278	5 828 666	8 874	5 565 521	3 404	263 145	-	-
192.168.75.255	56	11 641	0	0	56	11 641	-	-
192.168.75.132	14 195	6 129 397	4 300	492 005	9 895	5 637 392	-	-
192.168.75.2	493	76 953	241	56 993	252	19 960	-	-
192.168.75.146	1 203	365 952	607	78 664	596	287 288	-	-
66.102.9.147	139	88 651	84	77 231	55	11 420	-	-
209.85.229.139	9	1 405	4	520	5	885	-	-
192.168.0.3	20	3 662	10	1 992	10	1 670	-	-
64.4.52.169	18	3 131	8	1 150	10	1 981	-	-

This shows the IP Addresses of each end of a network session/conversation.

Order by total Packets, by clicking on the Packets column, then by Tx Packets and Tx Bytes to see which endpoint transmitted the most packets and data, and by Rx Packets and Rx Bytes to see which endpoint received the most packets and data.

Questions

Q: Which IP Address was involved with the most packets?

Q: Which IP Address transmitted the most packets?

Q: Which IP Address received the most data?

Q: Which IP subnet are these machines on?

This endpoint analysis can be used to produce a network map of the IP Addresses involved from the evidence trace.

Questions

Q: Can you list the IP Addresses of the machines on the local subnet?

Endpoint and Protocol analysis can be used together. Try adding a display filter for the IP Address which was involved with the most traffic and then generating protocol statistics (filter ip.addr==ipAddress)

Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End	Packets	End Bytes
Frame	100.00 %	14183	100.00 %	6127957	0.018		0	0
Ethernet	100.00 %	14183	100.00 %	6127957	0.018		0	0
Internet Protocol Version 4	100.00 %	14183	100.00 %	6127957	0.018		0	0
User Datagram Protocol	0.80 %	114	0.31 %	18888	0.000		0	0
NetBIOS Name Service	0.34 %	48	0.09 %	5541	0.000		48	5541
Domain Name Service	0.13 %	18	0.03 %	1846	0.000		18	1846
NetBIOS Datagram Service	0.29 %	41	0.15 %	9391	0.000		0	0
SMB (Server Message Block Protocol)	0.29 %	41	0.15 %	9391	0.000		0	0
SMB MailSlot Protocol	0.29 %	41	0.15 %	9391	0.000		0	0

Questions

Q: What is the percentage of FTP traffic for this host?

Other menu items Statistics>IP Addresses/IP Destinations can also be useful for host identification/analysis.

Analysis of Protocol and Session Data

Once Protocols and hosts involved have been identified, protocol and specific session data can be analysed.

Having identified that the FTP protocol data is unusually large for the evidence trace, we can concentrate on this. Use a display filter to pull out the ftp data.

No.	Time	Source	Destination	Protocol	Length	Info
3659	13:40:43.956588	192.168.75.132	192.168.75.1	FTP	93	Response: 220 Microsoft FTP Service
3661	13:40:49.892660	192.168.75.1	192.168.75.132	FTP	68	Request:
3662	13:40:49.892881	192.168.75.132	192.168.75.1	FTP	98	Response: 500 '': command not understood
3664	13:40:51.046888	192.168.75.1	192.168.75.132	FTP	68	Request:
3665	13:40:51.047253	192.168.75.132	192.168.75.1	FTP	98	Response: 500 '': command not understood
3667	13:40:51.599505	192.168.75.1	192.168.75.132	FTP	68	Request:
3668	13:40:51.599693	192.168.75.132	192.168.75.1	FTP	98	Response: 500 '': command not understood
3670	13:40:51.797915	192.168.75.1	192.168.75.132	FTP	68	Request:
3671	13:40:51.798182	192.168.75.132	192.168.75.1	FTP	98	Response: 500 '': command not understood
3672	13:40:51.970340	192.168.75.1	192.168.75.132	FTP	68	Request:
3673	13:40:51.970499	192.168.75.132	192.168.75.1	FTP	98	Response: 500 '': command not understood
3682	13:41:12.028617	192.168.75.132	192.168.75.1	FTP	93	Response: 220 Microsoft FTP Service
3683	13:41:12.034430	192.168.75.1	192.168.75.132	FTP	86	Request: USER Administrator
3684	13:41:12.034637	192.168.75.132	192.168.75.1	FTP	108	Response: 331 Password required for Administrator.
3685	13:41:12.039589	192.168.75.1	192.168.75.132	FTP	77	Request: PASS test
3686	13:41:12.162470	192.168.75.132	192.168.75.1	FTP	105	Response: 530 User Administrator cannot log in.
3797	13:42:06.556873	192.168.75.132	192.168.75.1	FTP	93	Response: 220 Microsoft FTP Service
3798	13:42:06.570677	192.168.75.1	192.168.75.132	FTP	86	Request: USER Administrator
3799	13:42:06.570878	192.168.75.132	192.168.75.1	FTP	108	Response: 331 Password required for Administrator.
3800	13:42:06.572315	192.168.75.1	192.168.75.132	FTP	77	Request: PASS fred

Display filters can then be used to pull out traffic relating to specific types of traffic. Try the display filter to highlight all traffic with an FTP command in:

```
ftp.request.command
```

Questions

Q: What is the IP Address of the server?

Q: Which hosts are using the FTP service?

To highlight the hosts attempting to login with the USER command, try the following filter:

```
ftp.request.command=="USER"
```

Questions

Q: What is the IP Address of the host trying to log in many times?

To highlight the hosts attempting to transfer files to the FTP server:

```
ftp.request.command=="STOR"
```

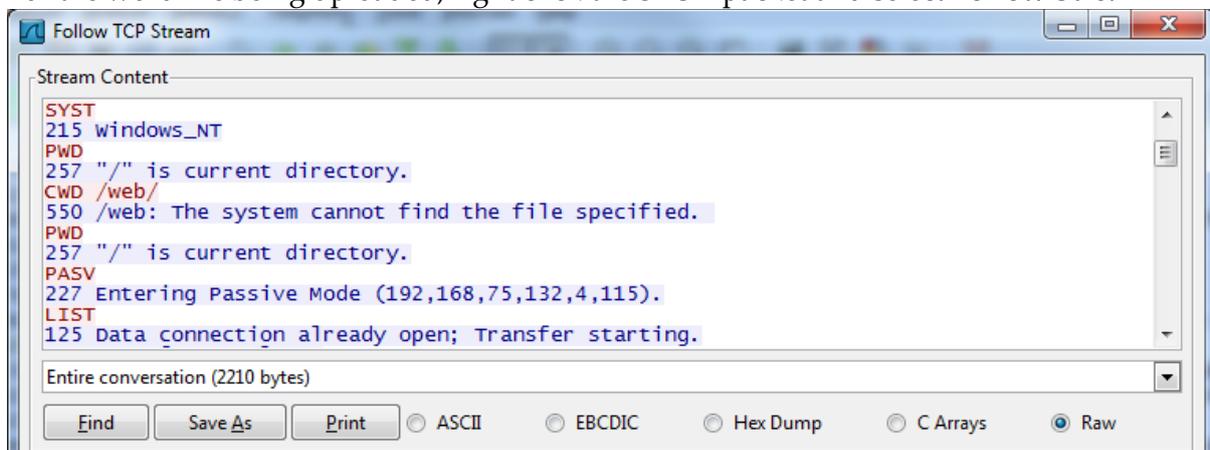
Questions

Q: What is the IP Address of the host uploading files?

Q: Can you list some of the files?

To focus in on a certain session/conversation, we can use Wiresharks conversation Stream rebuilding functionality.

For the word file being uploaded, right click the STOR packet and select **Follow Stream**



Questions

Q: Which directory is created in this session?

Q: Which text files are uploaded to the FTP server in this session?

NetWitness Investigator

NetWitness Investigator is free to use. Download the file, install and sign up for a free account.



NetWitness free can be found at:

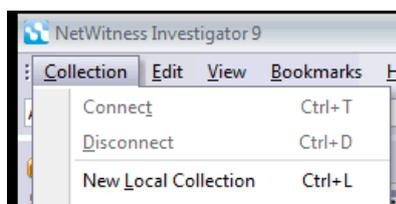
<http://www.emc.com/security/rsa-netwitness.htm#!freeware>

NetWitness is an analysis tool that allows for easy, rapid, investigation of voluminous amounts of network traffic. By importing a network capture file in a .pcap, or other recognised format, into a 'Collection', an investigator can view the main characteristics of the data in the capture file. The tool takes the packets in the capture and reassembles session streams for services and hosts, even for connectionless protocols.

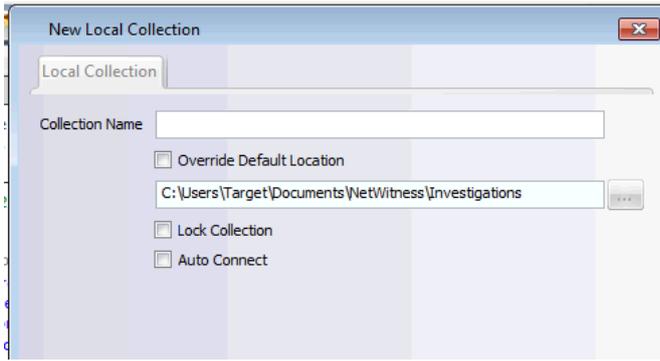
Run NetWitness:



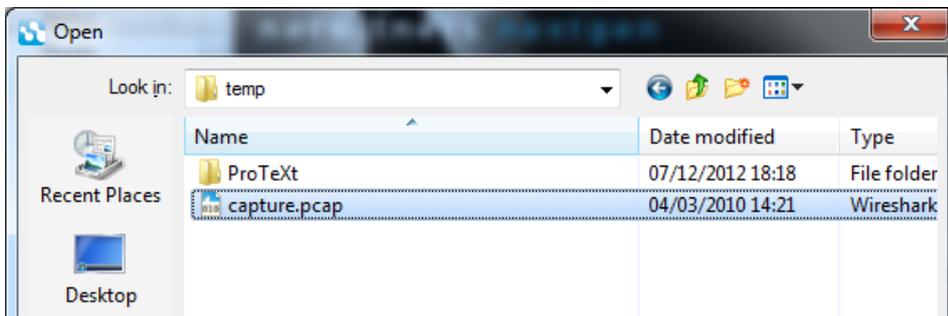
To create a new Collection, select **Collection>New Local Collection**



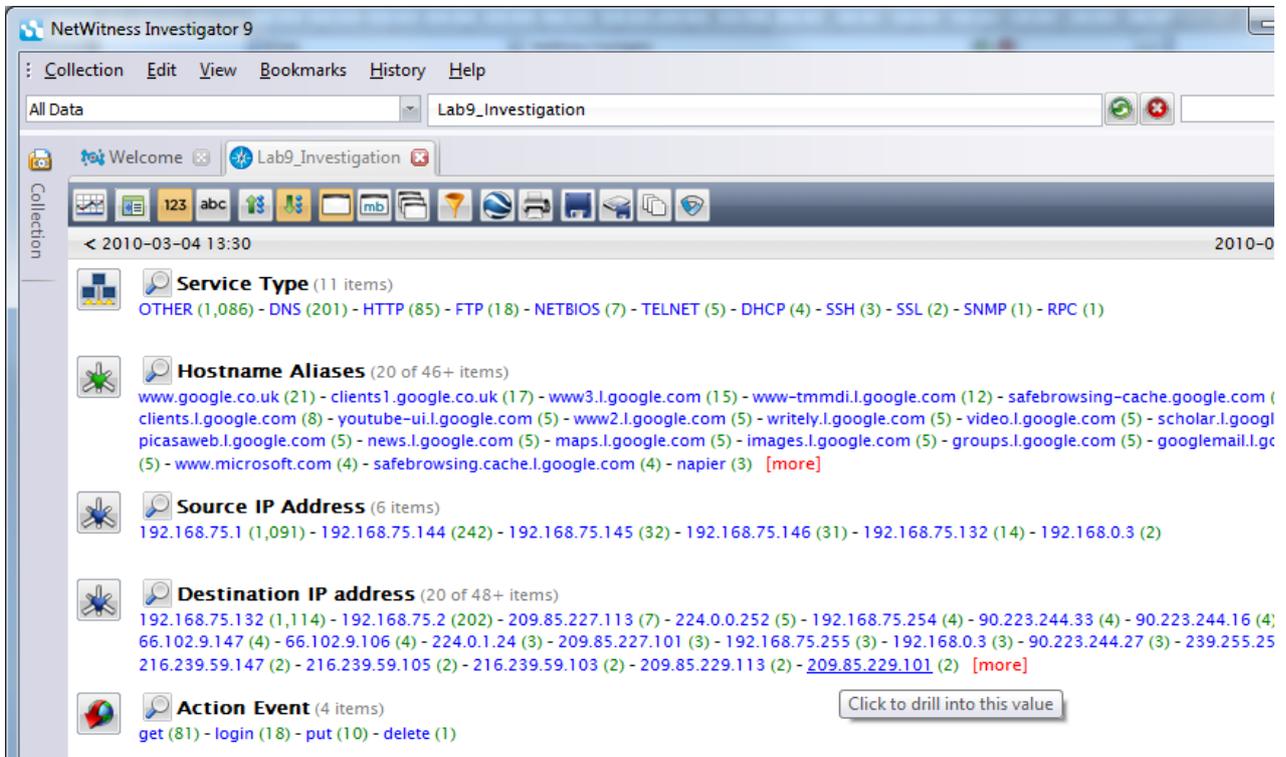
In the New Local Collection Dialog Box, type the name of the Collection, such as Lab9 Investigation and hit OK.



To analyse network data, it must be imported into a collection. To import your pcap file , double click on the new collection, until it states it is **Ready**. Then select **Collection>Import Packets** and add the capture file



Double click the collection and the details of the capture file are shown

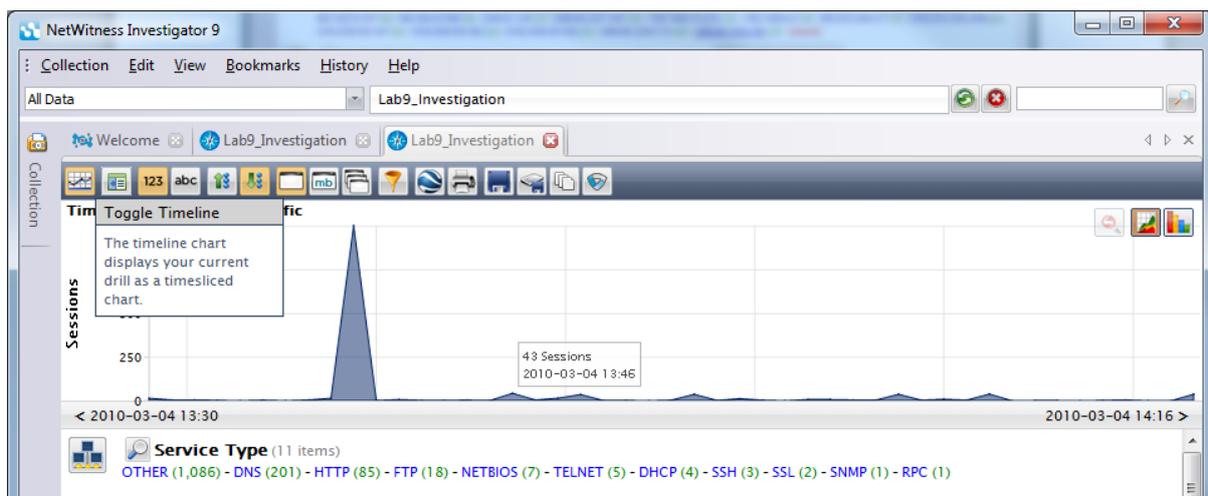


The navigation/breadcrumb bar is at the top. This allows you to understand the context of the data you are currently looking.

Note that each protocol name/data type is a hyperlink that can be clicked in order to further drill-down into the data.

Timeline

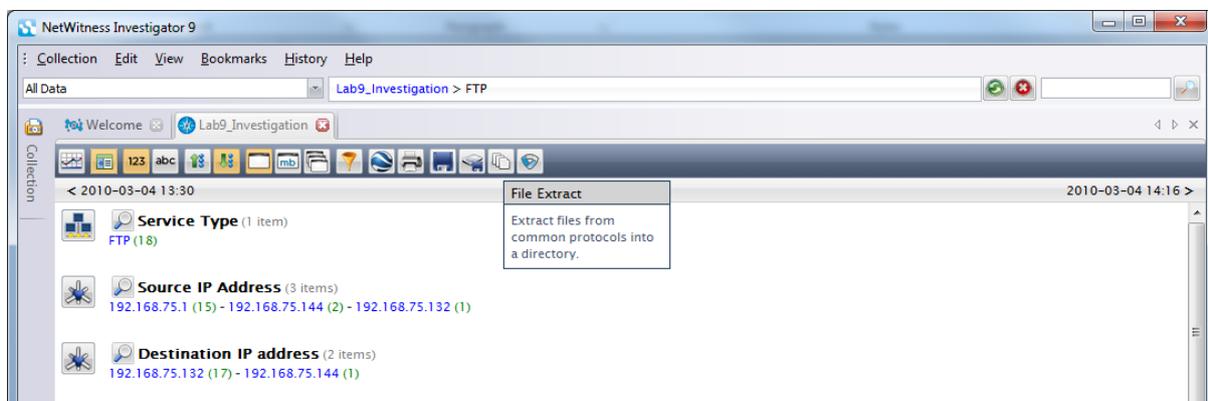
To create a timeline of activity for the entire trace, click the Toggle Timeline button, on the far left of the button toolbar.



Questions

Q. At what time do the sessions spike?

Protocols and sessions can be drilled into. Click on the FTP protocol and the details of all FTP sessions can be seen.



Questions

Q. Which FTP user has been used?

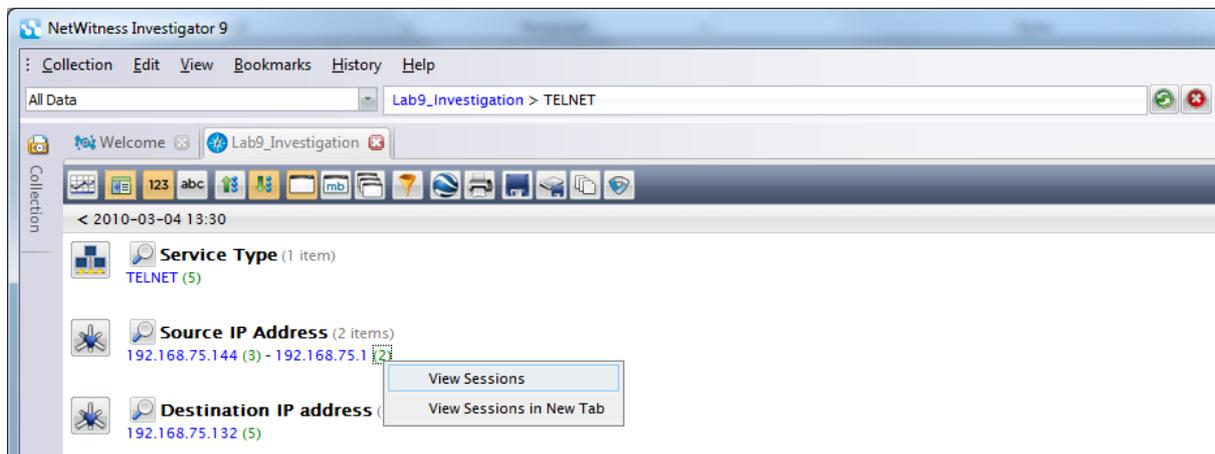
Go back to the main trace and select the Telnet sessions.

Questions

Q. From the details, which 3 IP Addresses are involved in Telnet?

Q. Which user accounts have been used?

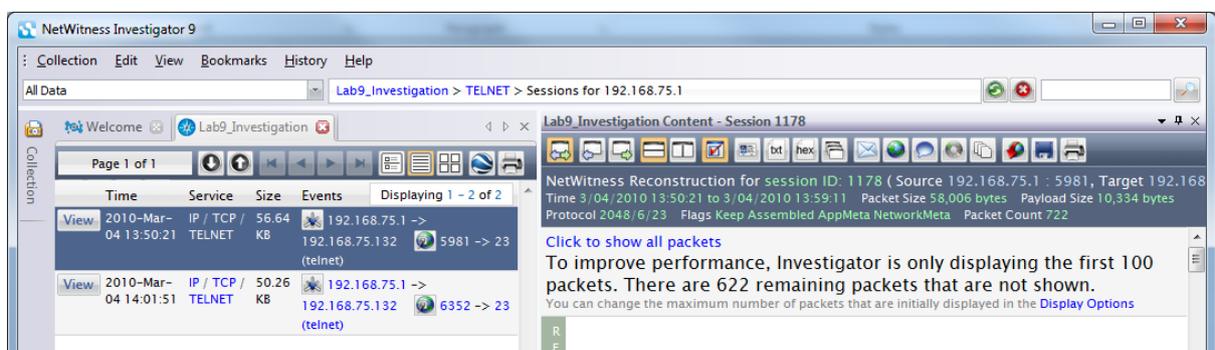
To drill down further, Right click the session number for the 192.168.75.1 host and select View Sessions.



Questions

Q. What are the times of the FTP sessions?

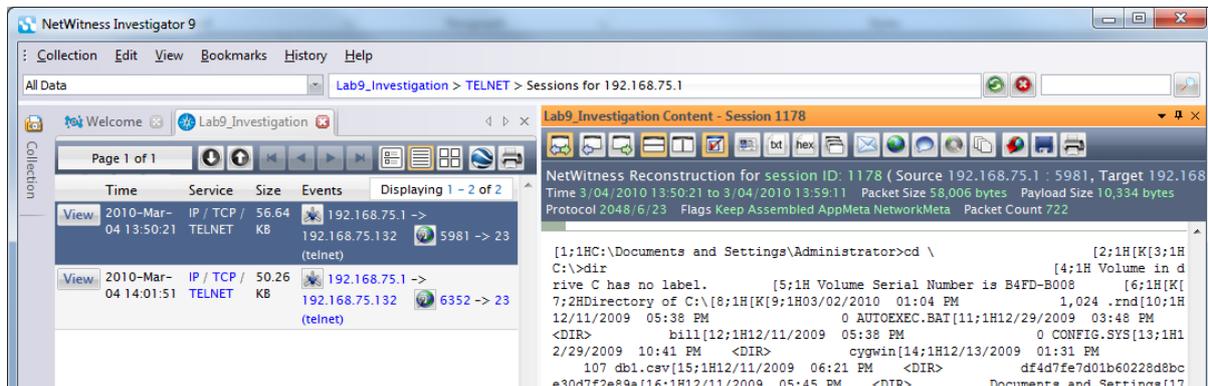
Click the 1st session and the details and content of the session should be shown:



Scroll down to see the content.

Questions

Q. Can you find the directory listing, and can you list some of the directories?



NetWitness can view details on sessions in various formats, reconstructing web pages, images and emails. The view buttons at the top of the session details pane can be used.

Extracting and Rebuilding File Content from Evidence Files

In NetWitness, create a new collection, and download and add the following evidence trace to the collection.

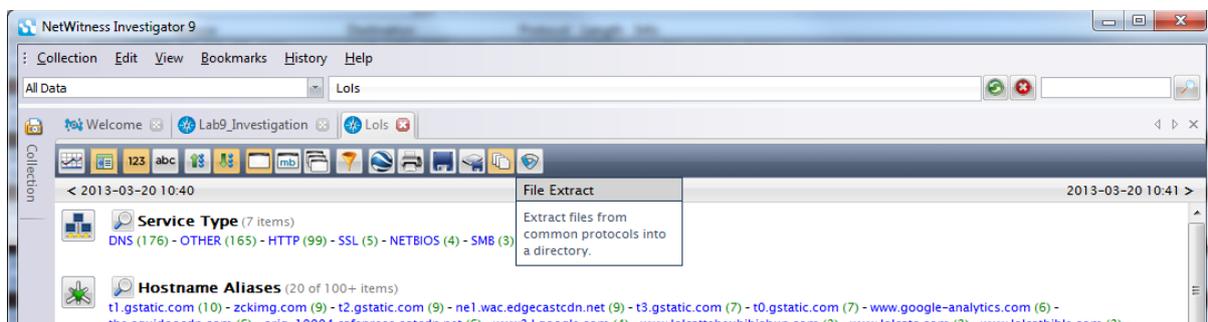


The Evidence Trace is at:

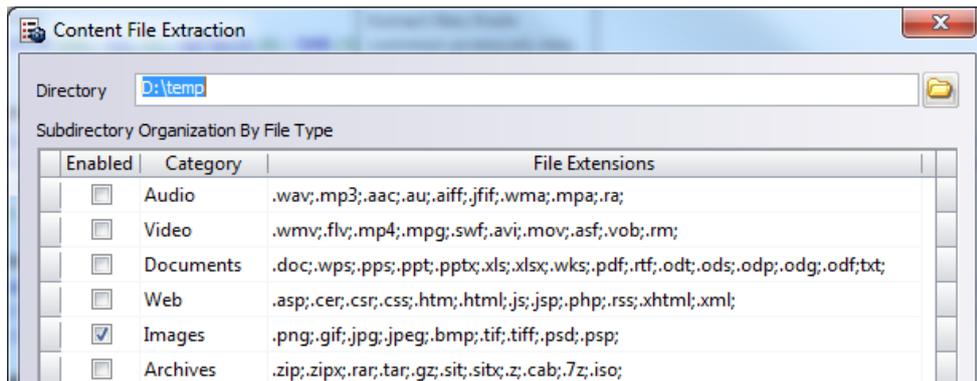
http://www.dcs.napier.ac.uk/~cs342/CSN10102/evidence_lol.pcap

Explore the trace briefly.

Now extract and rebuild image files from the trace using the File Extract button:



Click the images button and save to your c:\temp drive:

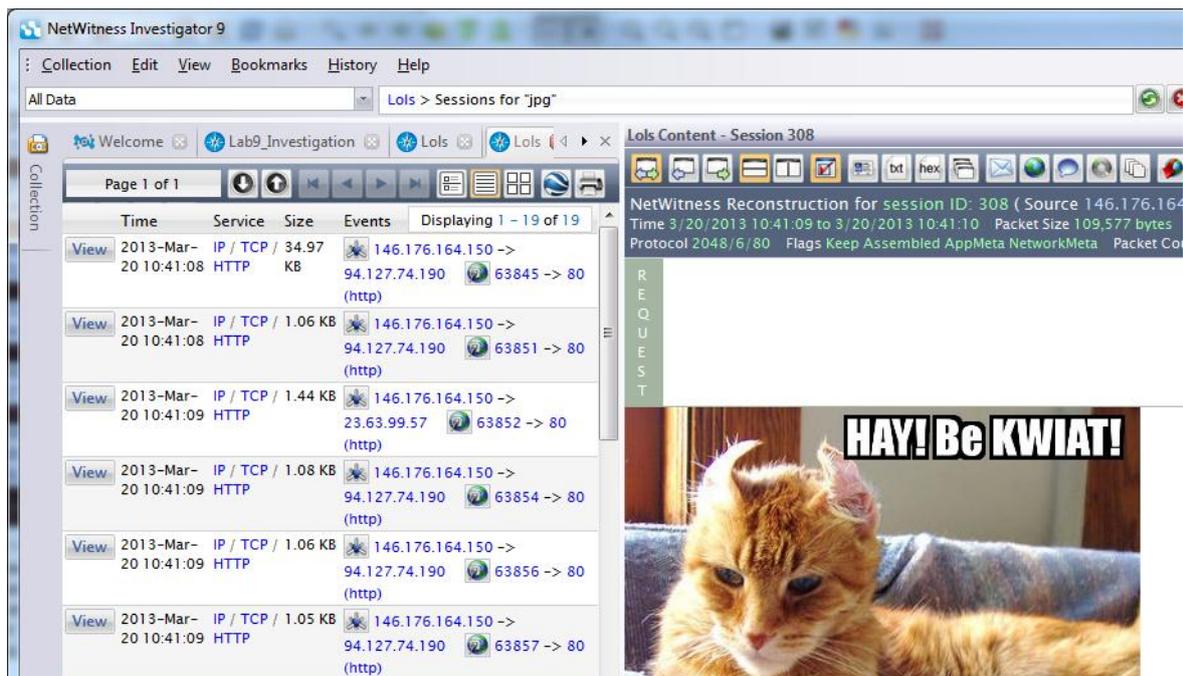


Open Explorer and investigate the evidence image files recovered.

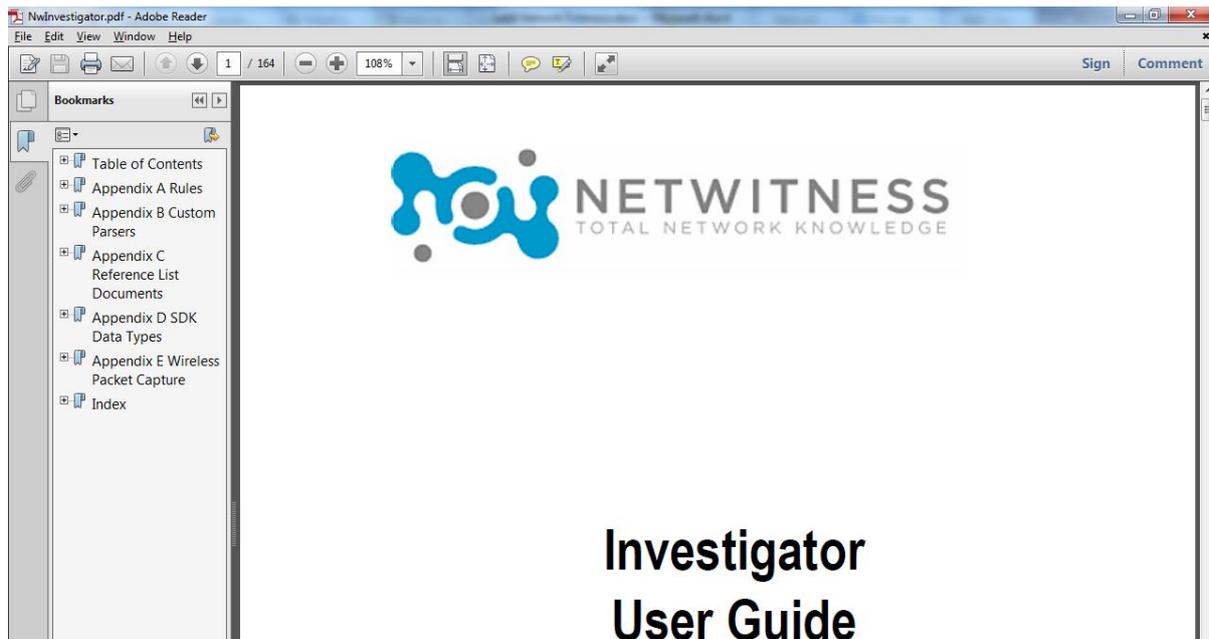
Questions

Q. What type of image files have been found?

Explore the HTTP sessions, and the image type sessions, of the trace and try to view each image file individually:

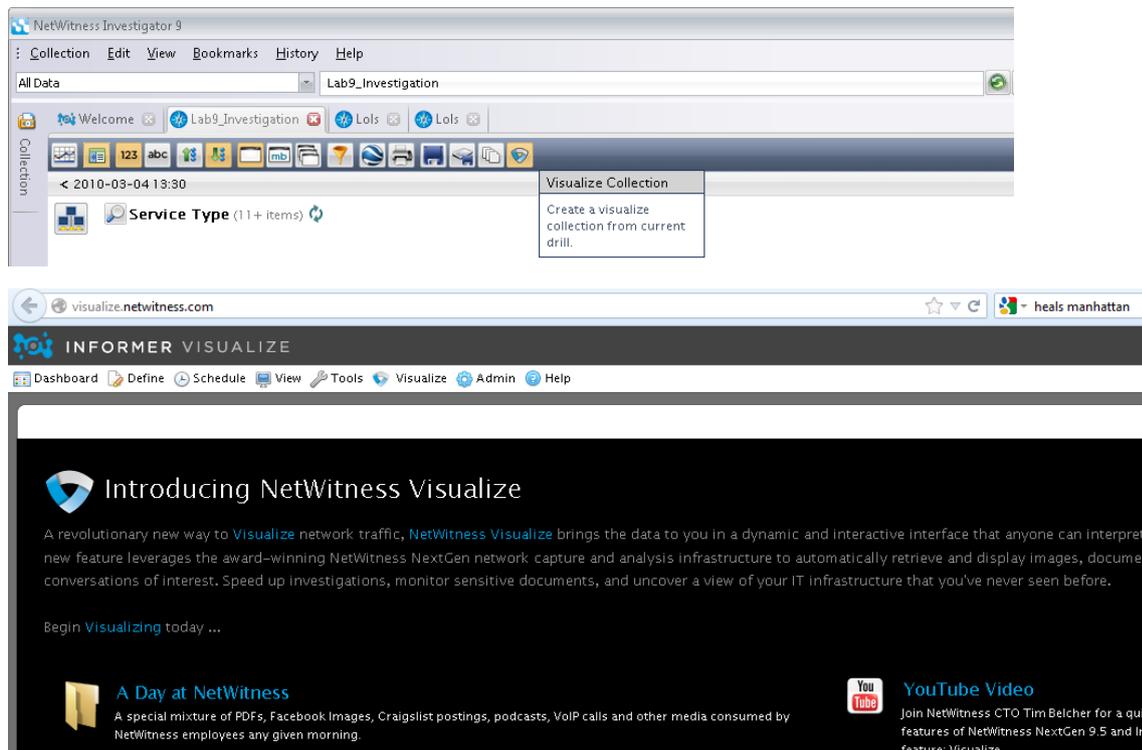


For more detailed information on Netwitness refer to the manual, which can be accessed from Help>Documentation menu option, as shown below:



Netwitness Visualize

Netwitness Visualize is a brand new web-based visualisation tool for network trace analysis. It allows the analysis of completely visualised network trace. If you click the **Visualise Collection** button, it will take you to the web site.



The YouTube video gives an overview of the visualisation tool, and the **A Day at Netwitness** and **Personnel Investigation** links let you try out the tool.

