Network Capture Visualisation

Integrated Design Project 3

Euan McKerrow S1223475

Khalid Zeari S1312249

Nabeel Nabi S1222196

Tamar Everson S1226265

Published, April 28th 2015

Content Page

Abstract: There have been many tools which have been created for visually analysing network traffic, these have been created to show visually the packets and the data about live PCAP files and captured PCAP files. These tools have made it easier for an analyst to view the data instead of reading it, because it is easier for them to comprehend the information. The tools created can do more that just display the information they can allow the analyst to filter certain packets so that the visual representation isn't overwhelming.

Keywords: PCAP, Network visualisation, unusual traffic detection.

1 Introduction

There has been a growing interest in the visualisation of PCAP files and the security of a network. Trying to detect malicious activity within a network is a difficult problem to face, made more difficult by large scale databases and very limited function of analysis tools. Even on a small network analysing packets manually is inefficient and time consuming. (Sven Krasser', Member, IEEE; Gregory Conti, 2005)Real-Time and Forensic Network Data Analysis

Using Animated and Coordinated Visualization.Current machine processing techniques, while they are quite fast, they still suffer from a unpleasant percentage of false positive and false negative alert. The world wide web has become one of the nation's critical infrastructures, there is a large amount of data being transmitted everyday over a standard network making it very difficult to notice any malicious activity. There are many ways to display PCAP files; typically, we analyse data with written reports, command scripts, or simple bar graphs and pie charts. However there is ways of displaying those files visually, using programs and tools, with the intention to test which programs exceeds in cost, packet visualisation, malformed packet identification, malicious packet detection, filters, blacklist packets for flags, and unusual packet detection. Using visual representation instead of textual representation can help in carrying out analysis on the data. Looking at the data it takes humans less time to understand specific information or patterns in an image rather than in text. Life form over time have become more advanced and knowledgeable in recognising complex patterns better than computers.(Mansour Alsaleh, David Barrera, P.C. van Oorschot 2008) Improving Security Visualization with Exposure Map Filtering Most importantly advanced visualization tools make it easier for humans to detect threats. To accommodate for both manual and automated visualisation techniques we have PCAP visualisation techniques to bring human life into the investigative cycle. (Mehmet Celenk, Member, IEEE, Thomas Conley, John Willis, Student Member, IEEE, and James Graham, Student Member, IEEE 2010) Predictive Network Anomaly Detection and Visualization. Research has been done in the past for many years for PCAP files to be used to create an alert system. In our research we will be reviewing these software and tools, to observe what information can be obtained from the tools and compare them to each other. The information that we would like to know from each software is how well they can handle a trojan attack, worm attack what information it can give from the packets. By comparing the tools that we are looking at we will be able to pick out the one that we find most useful and user friendly, which all other tools should follow as an example. We will also be looking to develop a preferred solution program, which will address the issues of the programs already tested on the market.

2 Literature Review

In this literature review, we aim to research into specific areas so later in our report we can bring the areas together, and create our own intake and interruption of the results from our experiment. The areas we look to cover is: network comparison tool paper, searching for papers that compare network monitoring tools, to find a best possible solution to carry out and display the results of our own experiment; intrusion detection papers, papers that research into patterns of attacks and the how they appear mixed-in with 'normal' and legitimate network traffic; visualisation development papers, looking into the benefits of visualizing a tool and what type of visualisation is the best to use; and finally research papers on specific tools we are going to aim to use in our research paper,

looking at their design and underlined key features of the tool.

The first area we are looking at in the literature review is network tools and how the tools stand out in comparison with one another.

2.1 Network Comparison tools:

The first paper researches the use of four network tools: Wireshark, Tcpdump, EtherApe and Caspa. Looking at functions each tool can carry out and how they work like, what Operating System they work on. (Suri, Batra. 2012) *Comparative Study of Network Monitoring Tools.* Suri and Batra (2012) examined and defined the key feature of the following network tools: Wireshark, Tcpdump, EtherApe and Caspa. They found Wireshark had the best cross-platform working on Mac OS X, Windows, Solaris, and BSD, then Tcpdump and EtherApe was next best working on Unix based operating system and then finally Caspa only working on some Linux based Operating Systems. They also underlined each tools defining features starting with Wireshark. Wireshark can capture data live "from the wire", meaning it can capture packets in real-time as they go through the network. Wireshark also has the capabilities to read from already logged PCAP files. They also found Wireshark has the capability to capture VoIP packets, which none of the other tools can do and the tool is split into three panels: the transmission overview, packet details and a panel for showing raw hex. Next they researched into Tcpdump which is a command-line based tool and found the tool picked up all packets, even the ones without an address. As Tcpdump is command-line based they are a lot of different options that the user can use, making the tool very effective if the user knows what they are doing. EtherApe was the next tool researched finding the tool have the benefit of a well thought-through visual design, with colour coordination. EtherApe also has a filter feature like the rest of the tools used except Tcpdump. Finally they looked at Caspa, Caspa was found to be easy to use, and deals better with real-time packets. Caspa was ideal for looking at LAN and WLAN networks.

From Suri and Batra's paper, Wireshark was found to Wireshark worked best, working on different Operating Systems and EtherApe and Caspa were found to visualise the data the best and most efficient.

In this paper, Suri and Batra demonstrated the benefits and defining feature of the four tools.

The next research paper is the similar to the Suri and Batra's research paper only looking at three of the tools. (Gandhi, Suri, Golyan, Saxena and Saxen. 2014) *Packet Sniffer - A Comparative Study.* Gandhi, Suri, Golyan, Saxena and Saxen (2014) researched key features of the following network tools: Wireshark, Tcpdump, Colasoft Caspa. They stated similar to Suri and Batra (2012) paper that Wireshark had the best cross-platform as it is able to use on Windows and Unix based Operating System, whereas Tcpdump is only Unix based and Caspa is only Windows based. It was tested that Wireshark uses the most disk usage and Tcpdump the least by quite a bit. Caspa is the only tool that costs money ($999) as the other two are free. Wireshark can deal with the most protocols with over 1000, then Caspa at 300 protocol, and lastly Tcpdump only deals with the TCP and IP packet protocols. Caspa is the only tool that can put alarms on traffic and protocols, however both Wireshark and Caspa can identify packets with forged data.

Again in this paper, the benefits of each tools is underlined, creating a ranking system based on capabilities. In this paper, the results were placed in a results table making the comparison of tools easy to read for the reader, and is a good, efficient way of displays the results.

The next section and area of interest is intrusion detection.

2.2 Intrusion Detection:

This paper looks how to develop a tool for intrusion detection visually. (Alaa El-Din Riad, Ibrahim Elhenawy, Ahmed Hassan and Nancy Awadallah. 2011) *Data visualisation Technique Framework for Intrusion Detection.* El-Din Riad, Elhenawy, Hassan and Awadallah, researched into the ways intrusion detection can be improved, and found that for the best results and would be more beneficial to capture in real-time. In this paper, they proposed to develop the tool called Snort, making it more visual and better at detecting intrusion. They suggested to implement this by using CSS & PHP. The paper also stated to make this work with Snort, it would

require five elements: a packet decoder, a preprocessor, a detection engine, a logging and alerting system and output modules. This also requires the identification of attack signatures that are in common with specific attacks and the patterns they create within a network.

In this paper, they looked at the requirements for an intrusion detection tool and planned what would be needed.

The next paper is similar, and takes a more mathematical approach looking probabilities of false positives and false negatives. (Li. 2004), *An approach to reliably identifying signs of DDOS flood attacks based on LRD traffic pattern recognition.*

Li looked to identify the patterns of the DDOS (distributed denial-of-service) attack with network traffic. In this paper, Li begins to states a required approach of creating a system with a high identification probability, while finding the balance of a low false alarm probability. In turn, this will be able to return any abnormal behaviour using the probabilities calculated by Li in this paper. As the technology advances at a rapid speed the research will soon or already be out of date requiring further research.

The next section looks at what are the best methods of visualising a tool and the benefits of visualisation.

2.3 Visualisation Development:

(Salova, Heinonen. 2011), *A Visualization and Modeling Tool for Security Metrics and Measurements Management.*

This research looks at the development of a tool called Metrics Visualization System (MVS), MVS is graphical security model environment. To measure the security threat confidence level, MVS using a metric range 0 to 1. 0 being definitely no threats detected and 1 conveying there is definitely a threat or threat to security. The tools also manages security metrics. Using visualisation with this tool increases the meaningfulness of the metrics in the context of security assurance, making it more user friendly.

Visualisation of a tool makes it more user-friendly, easier to use and sometimes easier to understand raw data.

The next section looks at papers that focus in on specific tools, we picked tools we may want to research in more depth in our paper.

2.4 Specific Tools:

Wireshark

(McRee. 2006), *Security Analysis with Wireshark.*

In this paper, McRee looks at defining feature within Wireshark, finding one of the most important feature of Wireshark, is how Wireshark colour coordinates everything, making the tool more user friendly, which can also be customised to suit the user. This paper also determines how an attack can be detected by using Wireshark, using the 'follow TCP Stream' feature, done by right clicking on a specific packet. The attack is detected by an unauthorised, unknown requests to a website show by the packets. If the website found, is searched on Google, it is found to be a sdBot, which is from the family of worms, that propagates through removable drives.

In our paper we look to research this intrusion detection through Wireshark, but from this paper it looks like the user is required to have vast knowledge and know what they are looking for.

RUMINT

(Conti, Grizzard, Ahamad and Owen. 2005) *Visual exploration of malicious network objects using semantic zoom, interactive encoding and dynamic queries.*

This paper looks at all the features of RUMINT and how the tool visualises the data. Conti and co claim the overall design is to intake a large volume of packets analysing them rapidly helping to search and find packet spikes, and carry out comparisons of packets. RUMINT does not just view a wide overview of packets it also can narrow in and pick out specific packets of interest.

In this paper, they also carried out an experiment to show difference between packets containing a threat or attack and legitimate packet traffic. Firstly they have to set up a control and find what is normal and legitimate packet traffic. Then mixed in the attack to see if it stand out in the traffic.

EtherApe

(Pallavi Asrodia and Hemlata Patel. 2012) *Analysis of Various Packet Sniffing Tools for Network Monitoring and Analysis.*

This researches into a number of network monitoring tools, but the one we

would like to research into is there take on the network monitoring tool, EtherApe. According to this paper EtherApe visualises the network, by colouring coordinating each protocol and drawing lines from IP address to IP address, and grow and reduce in size, when there is a spike or reduction in packets going from a specific source IP address to a specific IP address. Also EtherApe can handle a variety of different medias and encapsulation types and can read traffic from PCAP files (which we are looking to do in our paper) and live from a network.

The paper concludes that it is possible for network tools to detect an intrusion within the network, this is not just specific to EtherApe, but other similar network tools.

NetworkMiner

(Erik Hjelmvik. 2008) *Passive Network Security Analysis with NetworkMiner.* In this paper, Hjelmvik tries to demonstrate the strength of NetworkMiner and starts with NetworkMiner analysis of a PCAP file within the host tab, demonstrating how each host is identified within the traffic and each host a node that can be expanded showing details of server banners, open port and domain names. Also within this paper, within Hjelmvik's experiment they investigate if it is possible to identify rogue hosts, and concluded that it is, and prove why the host tab is a very useful feature. The next feature the paper talks about is the file tab and how NetworkMiner reassembles transferred files. Another feature that is mentioned within this paper is the keywords search which is not limited to protocol and can search all traffic.

This paper shows that NetworkMiner is not just any original network tool and can be used for multiple functions as it is not just limited to network sniffing.

3 Methods Section

Hypothesis: *Visualisation of PCAP files can be used to help attack discovery, better than viewing it through text.*

3.1 Design

In this paper, we look to compare different network tools that accept an importation of PCAP (Packet CAPture) files and how the tool visualises data and if and how the tool identifies intrusion detection. From the literature review we tried to research the how these points are looked at individually and tried to design an experiment to incorporate all this features in one paper.

We looked into the following tools: RUMINT**,** Wireshark and Etherape. We looked into the tools, and what features of the tool set, them aside from the rest, making them unique. We also looked at feature that let the down. The key elements we looked into were packet visualisation, how the tool looked when representing different types of data and information, like IP addresses, Port numbers, packets, protocol types. Other key elements we addressed were malformed packet identification and malicious packet detection, analysing how useful the information is that is displayed. Filter packets types, blacklist packets for flags and unusual packet detection were analysed within each tool.

3.2 Apparatus & Software

RUMINT:

RUMINT is used to capture live packets in real-time or can be imported from a PCAP dataset file. RUMINT is known for it design, being able to view data in seven different windows: a byte frequency window, a parallel coordinate plot, a scatter plot, a text rainfall, binary rainfall, a combined visualisation window, a detail view and most important the control panel. The control panel can be used to run through the packets and displays the packet number. The panel is able to stop and rewound at anytime so specific packets can be examined and analysed.

WireShark:

Wireshark (formerly called Ethereal) is one of the most popular network analysing tools, that allows the user to view all visible traffic on an specific interface or a pre-saved PCAP file. The tool was created by Gerald Combs and released in 1998. Wireshark's graphical interface has

three main panels: a packets overview, listing all the packets from the live capture or PCAP file; a packet detail panel, that shows information about a selected packet from the live feed or PCAP file and the third panel is a hex data panel, used to view the hex data of a selected packet and its raw data.

EtherApe:

EtherApe is a free tool that presents PCAP data in a graph. It is modelled after Etherman and features multiple modes including TCP and IP (EtherApe, no date). EtherApe is built for *nix operating systems, and features 64th on SecTools' (No Date) top 125 Network Security Tools list. The tool was created by Juan Toledo and released in 2000 (EtherApe, No Date).

NetworkMiner:

NetworkMiner is a Network Forensic Analysis Tool (NFAT), which sniffs traffic and takes information of saved traffic from PCAP files. NetworkMiner has a number of tabs dividing the information neatly. NetworkMiner extracts files, images and others objects from the network traffic. (No author. 2012) *Brief overview of 4 NFATs.*

3.3 Procedure

To test our collected software in our experiment we decided to use an exist PCAP files that we know previously it contains some suspect traffic which could broke out into two main PCAP files. The first file is called *'korgo.pcap'* variant as the culprit. Korgo, is knowing as Padobot, which is an old worm that exploited a Microsoft windows LSASS vulnerability in 2004. According to F-Secure, the worm contacts remote computers on TCP port 445, exploits the Microsoft windows LSASS vulnerability, and it copy its files into the remote system.

The second PCAP file that we have used for our experiment is called '*Kraken.pcap'* which was found on an OpenPacket website, listed in the Malicious category. Here is an MD5 hash value of the binary that generated the traffic '*traffic12b0c78f05f33fe25e08addc60bd9b7c.pcap*'. Kraken is a spam bot, this particular variant made use of TCP/UDP port number 447 for command control.

The two mentioned PCAP files were used in all the tools that we have used in our research Wireshark, RUMINT, EtherApe, and NetworkMiner. We tried to get different tools that analysis the PCAP files from completely different approach to any patterns in the different time of attacks and how they are displayed.

Our main aim in the result section was to see how the tools is going to handle the PCAP files specially the way they indicate the suspect traffic. Since we have have graphical based software and detailed view software.

4 Results

4.1 RUMINT

(Gregory Conti, Julian Grizzard, Mustaque Ahamad and Henry Owen, 2005) Visual Exploration of Malicious Network Objects Using Semantic Zoom, Interactive Encoding and Dynamic Queries.

One of the tools which has been recommended for data visualisation is RUMINT. RUMINT is a tool which is free to download off the internet and available for a Microsoft Windows Operating System. It lets a user compare a large amount of packets with header and payload fields using seven different windows.

After extend research into packet capturing tools, the first tool we researched was RUMINT. Collective, we came to the conclusion that it is a very useful tool when everything can be understood, as shown in the figure 4.1.1. Figure 4.1.1 is the research we carried out, which is of a PCAP file we have analysed, which contains a worm within the captured packet traffic. RUMINT adds a new window for each feature as shown in figure 4.1.1. The top left of the screen is showing the byte frequency window. The byte frequency window view shows all bytes (0 - 255) plotted along the horizontal axis. As each of the packets is plotted, pixels are illuminated according to the byte relative to each packet. Window (D) shows the text rainfall displaying the printable ASCII characters by using UNIX strings-like functionality of the PCAP file. The detail view window, window (E), displays the details of a specific packet in hexadecimal and ASCII. The first packet in the capture is shown in figures 4.1.1 and 4.1.2, as indicated by the main control panel in the centre of the screen. Window G of the Figure 4.1.1 shows the binary rainfall which plots the raw binary and a text rainfall view.

In the Parallel coordinate plot window (Window B), a comparison of the header fields from the PCAP file takes place. On the remaining two windows: scatter plot (C) and combined visualisation (F), it shows what machines were infected with the worm. It only shows one output because only one ethertype was infected which was 0x800. The other window (F) shows the source IP address affecting the TCP destination port.

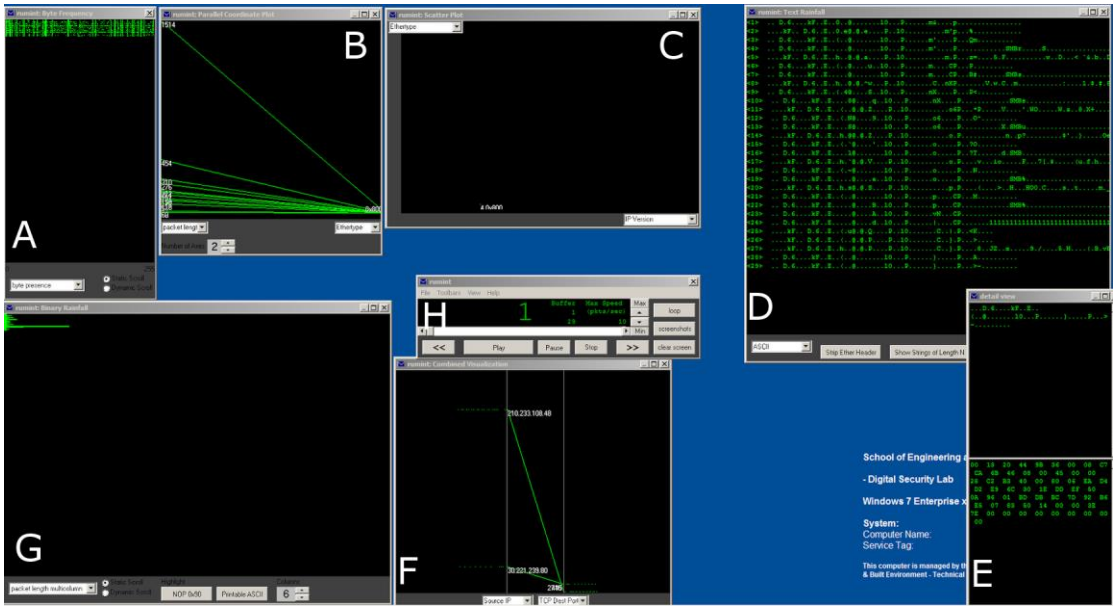

Figure 4.1.1

Another way Rumint network analysis tool was tested is by using a PCAP file which contained the traffic of a Trojan as shown in the figure below. We compared it to the result from the PCAP file it shows a lot more of the information such as the colour orange which represents network layer protocol headers. With this result everything was kept the same when carrying out the two experiments so that the results would be valid and not favouring the tool in any matter.

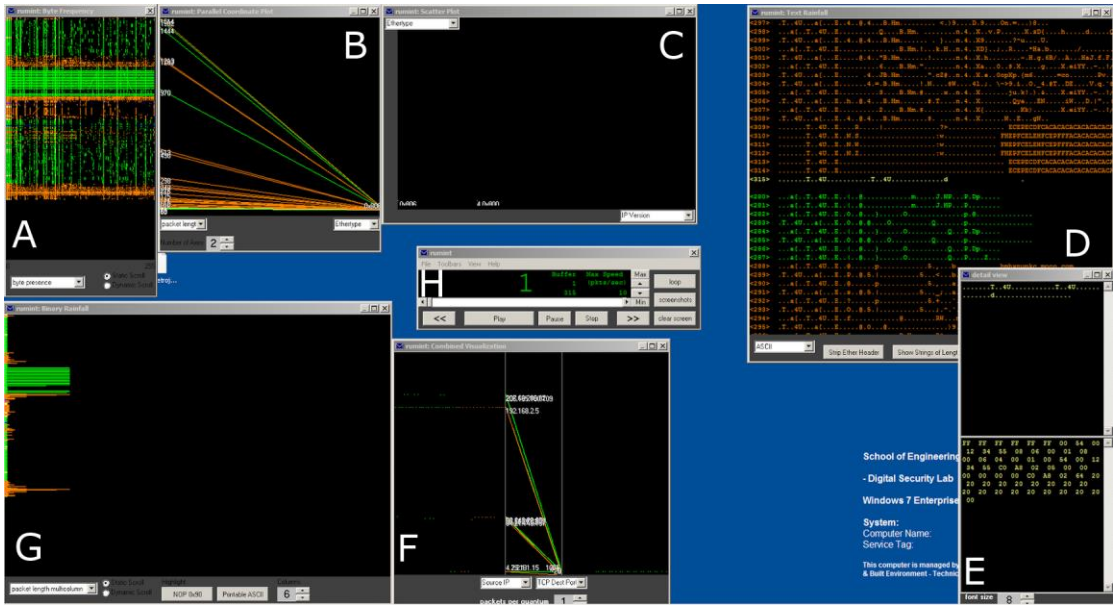

Figure 4.1.2

When carrying out the two experiments we noticed that although a lot of the information that is needed is shown from the results given by RUMINT, the results don't seem to be as user friendly to anyone who isn't an analyst. The tool also

never provided a closer look at the binary frequency rainfall screen, which would be very handy to look at. Lastly the tool didn't allow a user to toggle between the windows, because when this is attempted the results shown disappeared.

4.2 Wireshark

According to Suri and Batra (2010), Wireshark is the most used network monitoring tool in the world. It has both a graphical interface and can also be run through the command line, making it a flexible tool for use on both local and remote networks. Wireshark supports in excess of 770 protocols (Kaur I and Kaur H 2014) and is widely used for network analysis and troubleshooting. It has tools for capturing, viewing and analysing packets.

As can be seen in figure 4.2.1, Wireshark highlights different packet types, making it easy to identify them. Wireshark also provides an option to follow the TCP or UDP stream, allowing a network analyst to easily follow the communications between two hosts (Figure 4.2.2).

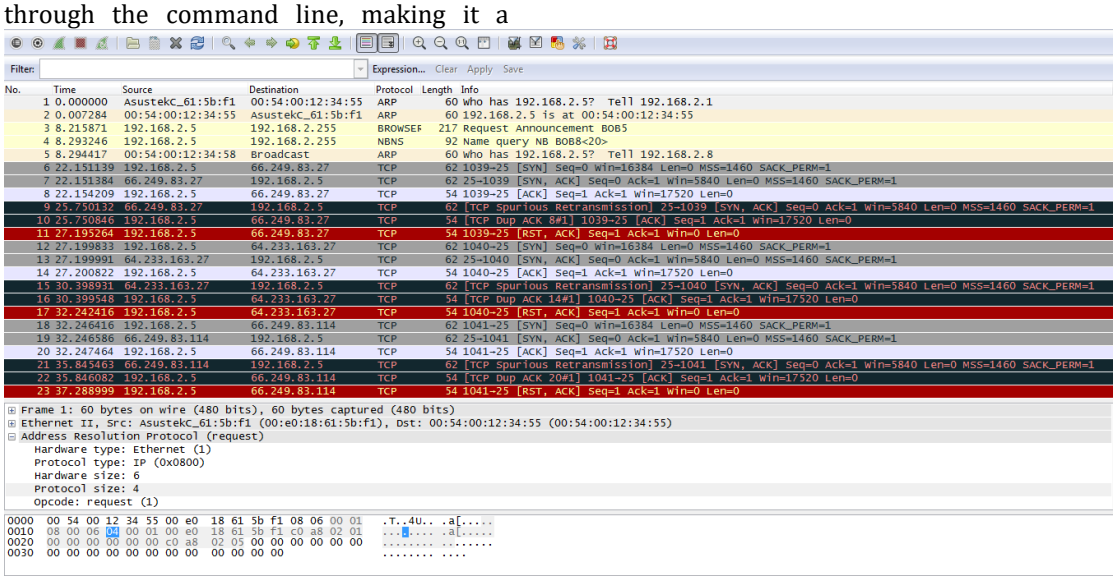

Figure 4.2.1

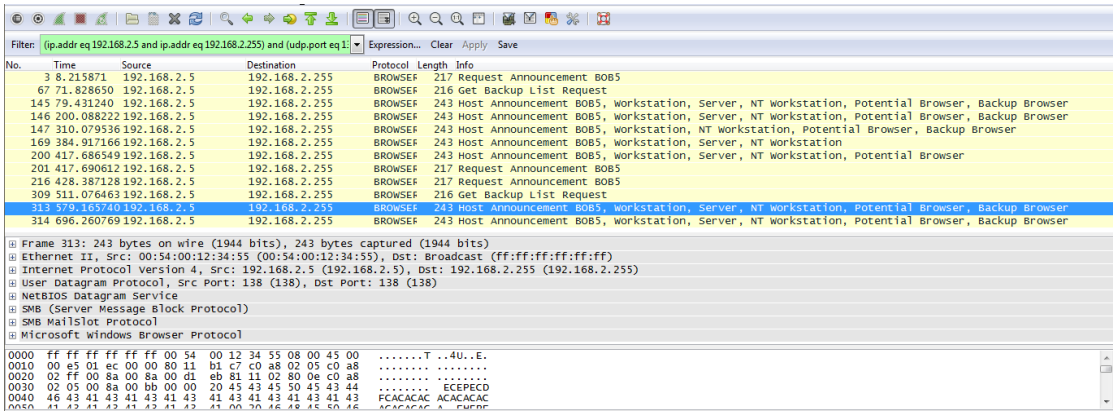

Figure 4.2.2

In our investigation, Wireshark presented the packet data in a visually easy to follow format, providing a number of tools to assist with the filtering of the packets. However, we felt that it didn't present the data effectively in a way to aid attack discovery.

Some of the other tools that we have investigated for this paper show graphical representations of the traffic across the network. This can help detect anomalies in the traffic such as an abnormal amount or type of traffic to a specific host. This is one area in which we feel that Wireshark lacks the ability to be the sole

PCAP analyser in use when investigating attacks, as whilst the data is colour coded, it is not possible to view the events in a graph. This makes it hard to use Wireshark to detect network problems.

Wireshark does, however, provide a plethora of data about each packet. With its tri-windowed display and ability to follow a stream, it makes it easy to identify who is requesting information from who, and who is responding to requests (Murphy B 2013).

Viewing the PCAP data from our sample captures in Wireshark, it was not instantly obvious that there were malicious packets, like in some of the other programs we analysed. We feel that if Wireshark were to introduce graphical features to help better visualise the data, it would be a far more capable program for identifying malicious network activity.

4.3 EtherApe

The third tool that we investigated is EtherApe. EtherApe is also a free tool available for *nix based systems. It presents a graphical map of all network traffic seen captured (Ferrill 2010). The tool allows users to both capture live data across a network and to analyse existing PCAP files.

EtherApe allows the user to view the protocols of packets as well as nodes that have sent or received data. The produced graph (as shown in Figure 4.3.1) shows the hosts on the network as nodes and the connections between the hosts as edges. Each element is colour coded to help visualise the protocols in use across the network. The edges and nodes adjust size to indicate the volume of data (Suri and Batra 2012).

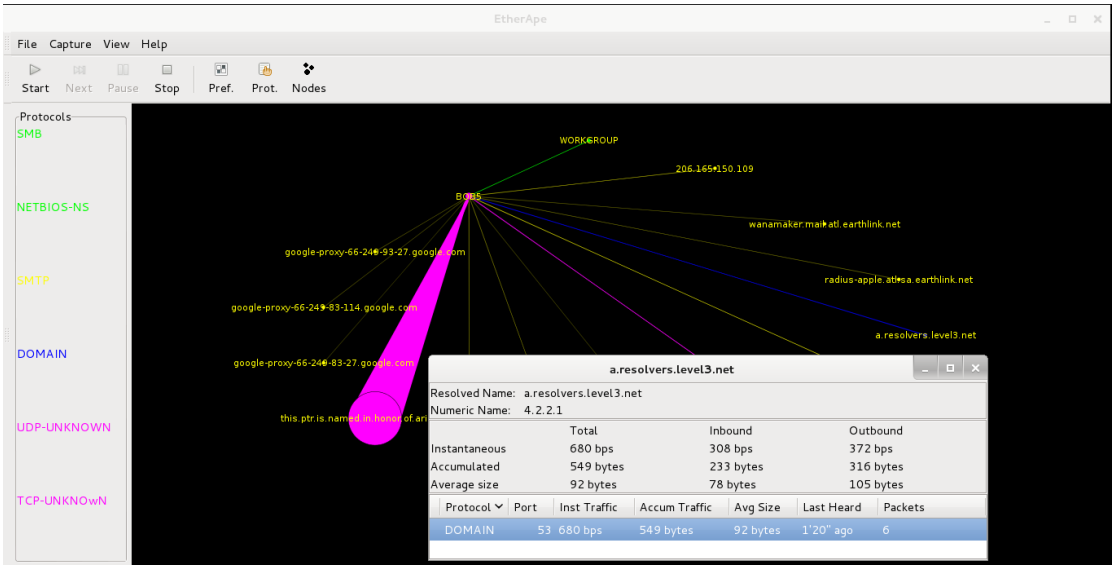

Figure 4.3.1

Having investigated EtherApe with our sample PCAP data, it is very effective at clearly visualising what hosts have communicated with one another. By clicking on a graph edge, data is provided about the protocol and port used for the data transfer. However, unless the person analysing the data is familiar with hosts that contain malware or unwanted content, it will be tricky for them to identify potentially unwanted traffic.

One good use for EtherApe in visualising PCAP data is the ability to see if one host has a significantly larger amount of traffic than other hosts on the network. If it is noticed that one host has an abnormal volume of traffic, it could be indicative of a breach or other malicious activity that should be investigated further.

EtherApe is a good tool for examining the growing web of connections over time, and determining which hosts within a network communicate with each other. However, in relation to an attack such as a worm on a network, it would not be immediately obvious that the attack is taking place.

4.4Network Miner

(Russ McRee. 2008) NetworkMiner is a Network Forensics Tool (NFAT) which has significant features that makes such a piece of art of it. It is windows based software which can be used as a passive network sniffer/ packet capturing tool in order to detect the operating systems, hostnames, sessions, DNS, Images, Messages, Credentials, and open ports of network hosts through packet sniffing or by parsing a PCAP file. What we really find is fascinating about NetworkMiner is that it can extract transmitted files from network traffic into different categories in such easy and organized way for network administrators to view. Network Miner's display focuses on the hosts and their attribute unlike Wireshark which displays only raw packets.

The purpose of NM is to collect data such as (forensics evidence) about hosts on the network instead of collecting data regarding the traffic on the network.

NetworkMiner in Action

(Carvey, Harlan A. 2014) Here a demonstration of Network Miner. I'll use some malicious PCAP files which we have downloaded from the internet with prior permission from the website holder of the PCAP files.

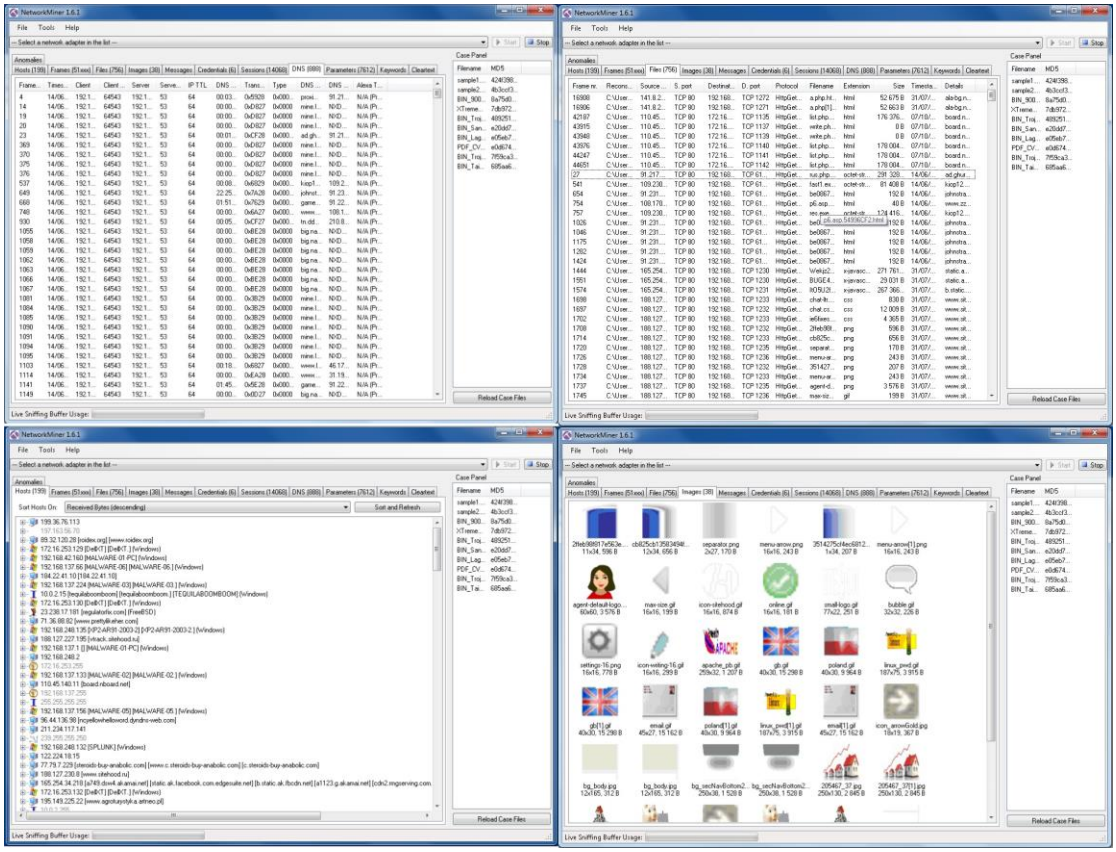

Figure 4.4.1

Once you load the PCAP files into the NetworkMiner, it parses the file and presents several tabs with various aspects of the traffic and its contents. These include:

The detected hosts, including their DNS names and their IP addresses as well as the ports that used during the capturing period.

- As part of the observed session HTTP parameters sent to web servers.
- Messages and websites content displayed as a clear-text, ASCII contents extracted from the network streams, including a separate tab for any captured credentials
- Any files exchanged between hosts during the monitored period

(Chris Sanders. 2011) Network Miner has the ability to carve out any files found in the network stream, saving them into a local folder. It's advisable that to use a dedicated laboratory system when using the tool in this capacity is that the files might be malicious and your device may get infected if you don't handle them probably.

To view any of the extracted files, you have to right-click on the file of interest in the NetworkMiner's Files tab, then you select open folder.

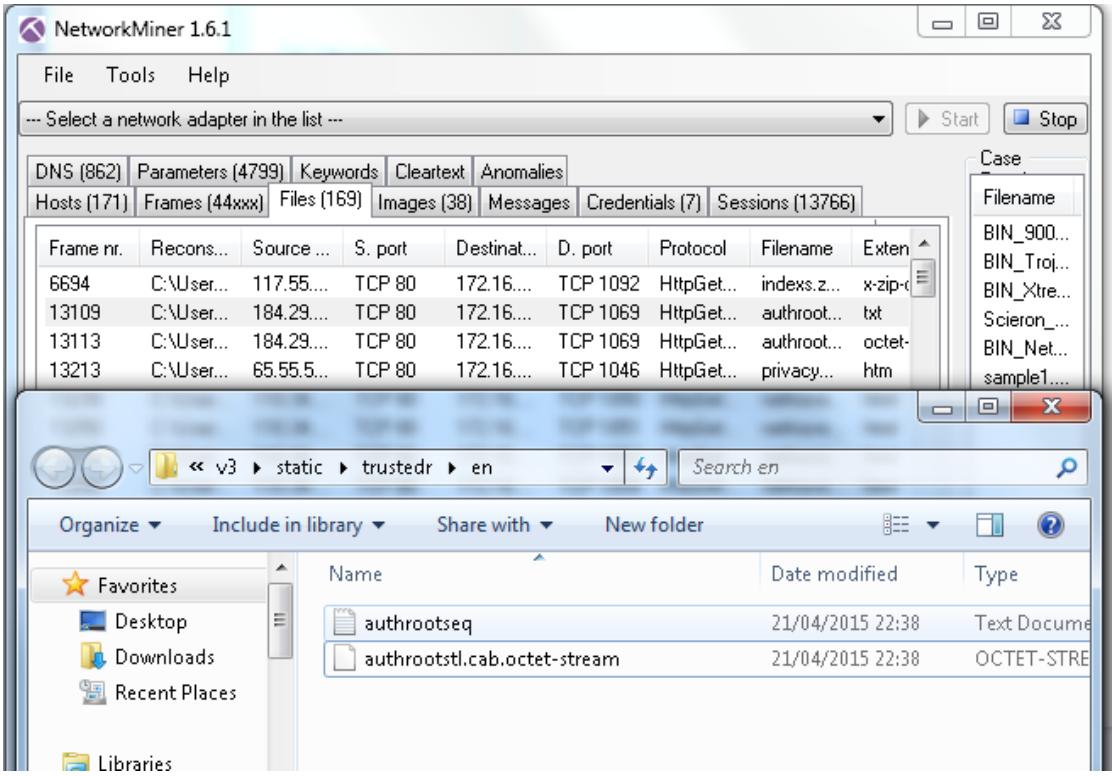

Figure 4.4.2

NetworkMiner is one of the certain tools that every incident responder should always have in his toolkit. It's an excellent option as a tool for attack investigation, and it can be used to conduct behaviour analysis of a compromised machine and potential vicious host or malicious users.

4.5 Comparison

Viewing the tools at a glance it seems as if EtherApe is the best to view if you are not a network analyst. But the tool which had the most detail was NetworkMiner we think this because it was easy to understand, everything was categorised into their own pages and they were in their own columns.

Looking at wireshark it provided the basic information needed to analyse a PCAP file but it at the same time it gave a lot of information which was not needed for analysis it was partially graphical by using different colour for their each packet. Lastly RUMINT gave a lot of detailed information but it would only be valid if it was being viewed by a network analyst, the information and symbols was coloured

differently to show the different information from the packets such as a header being orange.

4.6 Our tool (ENVA)

ENVA is a PCAP visualisation tool, that is currently under development, coded in Python using the Tkinter module library, an in-built GUI for Python. ENVA has three main components: down the left hand side of the main application window is the packets represented as button. When a specific packet (button) is clicked, the corresponding packet details will appear, as shown in figure 4.6.1. Each protocol is colour coded for each packet, for example packets using the ARP protocol are displayed in red, grey for TCP, dark blue for UDP, and light blue for IGMP.

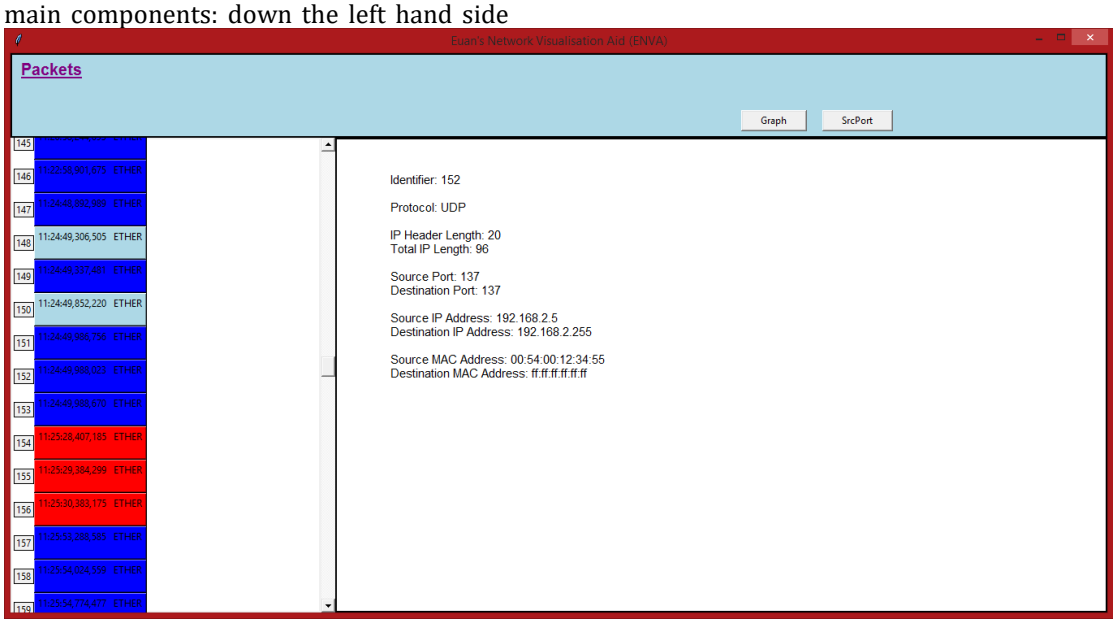

Figure 4.6.1

The remaining two components are shown when the user clicks the 'Graph' and 'SrcPort' button. The 'Graph' button displays all the packets and their corresponding times as a graph, so any spike in the traffic can be identified, showing the time as well. The 'SrcPort' button displays the source ports of every packet down the left hand side of that window and the source IP addresses down the right hand side. Each line represents a packet from the source port to source IP address of that specific packet. This feature can show any port communications as shown in figure 4.6.2. Figure 4.6.2 shows address 192.168.5.2 has come into contact with every port used within the traffic, maybe highlighting malicous or unusual behaviour. Both 'Graph' and 'SrcPort' are shown in their own windows, similar to RUMINT.

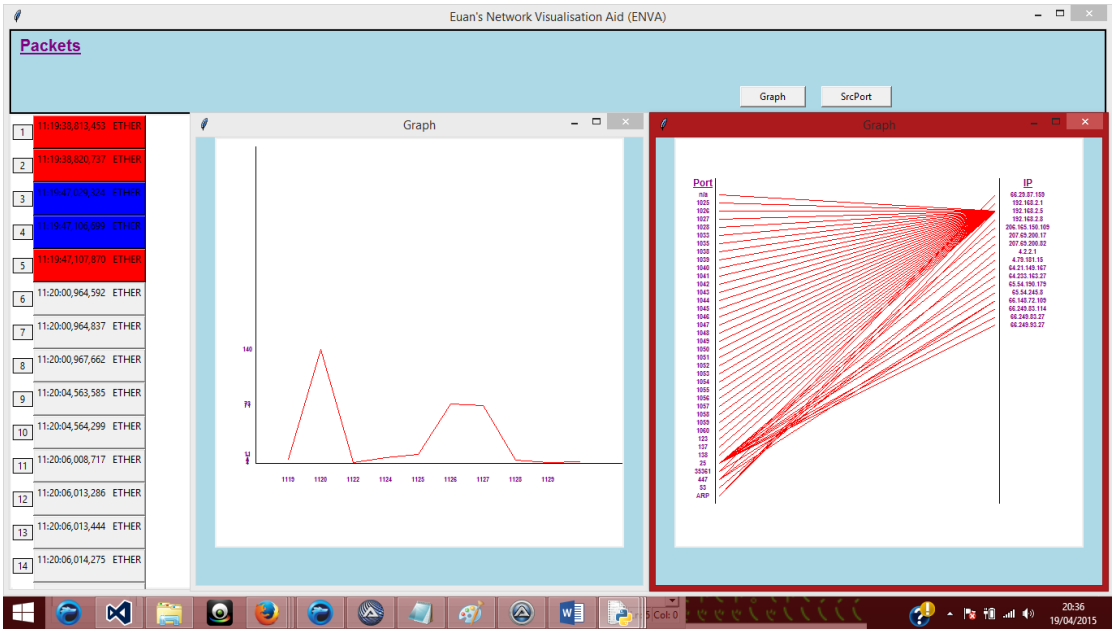

Figure 4.6.2

5 Final Discussion & Conclusions

5.1 Final Discussion

Our study has compared a variety a of PCAP analyst tools with the ultimate goal of developing our own PCAP analysing tool and visualisation of the detection of an attack. We found out that some tools are better than others as discussed in our comparison (section 4.5). We liked aspects of all the tools that we researched and put this research together to develop our own tool, that we believe can be further developed to become a leading PCAP analysing tool in the market. We feel we achieved our initial goals, which was evaluating the network visualisation tools and to develop our own tool. We have found that the tools we researched displayed and conveyed the information of packets better when it was visualised, rather than text based. Looking our results we believe we have proved our hypothesis is true of: *Visualisation of PCAP files can be used to help attack discovery, better than viewing it through text.* We research we carried out showed that other research papers agreed with research.

5.2 Project critique

There were a number of tools which we wanted to investigate as part of this project, but we ran across technical difficulties. Some of the tools were also outdated, meaning that they wouldn't run on our systems. Due to the time constraints with the project, we were unable to get these work. Given more time, we would have made these tools work, as some of them (especially TNV) looked like very good programs. We discounted them for this paper due to the difficulties in getting them work, but would like to go back given more time to do so.

Overall, we feel that the research was conducted in a fair and unbiased manner, allowing us to find the best aspects of each program in order to develop ENVA.

5.3 Further work

We have built the foundations of a strong PCAP visualisation tool after comparing the features in a number of existing tools. We plan to continue reviewing PCAP visualisation tools and further developing our tool, ENVA. Future additions to our tool would include adding the destination IP and change the colouring of the graphs to make them clearer.

We plan to implement a system to automatically flag suspicious behaviour to help aid attack discovery and investigation. We are also open to suggestions on further

work that we should pursue on the topic, and suggestions on how to improve our PCAP visualisation tool.

We would also like to investigate the tools that we were unable to analyse as part of this paper, notably TNV.

5.4 Conclusions

We have researched into four different Packet Capture visualisation tools in order to identify the strengths and weaknesses of each. The tools investigated include RUMINT, Wireshark, EtherApe, and NetworkMiner. By finding this data, we have been able to develop our own PCAP visualisation tool, ENVA, to attempt to combine the best features of each. We hope that by researching these tools and developing ENVA, we will be able to better help network security professionals keep track of the data passing across their networks in order to easily identify threats and issues within their network. We intend to further develop ENVA to support more protocols, and build more features into it after identifying features from other PCAP visualisation tools that we feel will be beneficial to the security community.

References:

Shrutika Suri, Vandna Batra. 2012, *Comparative Study of Network Monitoring Tools.* International Journal of Innovative Technology and Exploring Engineering (IJITEE) (ISSN: 2278-3075, Volume-1, Issue-3) [online], Available at: http://www.ijitee.org/attachments/File/v1i3/C0210071312.pdf [Accessed 14 April 2015].

Dr. Charu Gandhi, Gaurav Suri, Rishi P. Golyan, Pupul Saxen, Bhavya K. Saxena. 2014, *Packet Sniffer - A Comparative Study.* International Journal of Computer Networks and Communications Security (ISSN: 2308-9830, VOL. 2, NO. 5, MAY 2014, 179–187) [online], Available at: http://www.ijcncs.org/published/volume2/issue5/p6_2-5.pdf [Accessed 14 April 2015].

Alaa El-Din Riad, Ibrahim Elhenawy, Ahmed Hassan and Nancy Awadallah. 2011, *Data visualisation Technique Framework for Intrusion Detection*. IJCSI International Journal of Computer Science Issues (ISSN (Online): 1694-0814 Vol. 8, Issue 5, No 1, September 2011. Available at: http://ijcsi.org/papers/IJCSI-8-5-1-440-443.pdf [Accessed 14 April 2015].

Ming Li. 2004, *An approach to reliably identifying signs of DDOS flood attacks based on LRD traffic pattern recognition.* Elsevier Computers & Security, (April 2004) [online]. Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.332.8593&rep=rep1&type=pdf [Accessed 15 April 2015].

Reijo M. Savola, Petri Heinonen. 2011, *A Visualization and Modeling Tool for Security Metrics and Measurements Management.* (2011) [online]. Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.232.1151&rep=rep1&type=pdf

Russ McRee. 2006, *Security Analysis with Wireshark.*(2006) [online]. Available at: http://holisticinfosec.org/toolsmith/pdf/november2006.pdf

EtherApe. No Date, *EtherApe* [online]. Available at http://etherape.sourceforge.net/ [Accessed 20 April 2015].

SecTools. No Date, *SecTools* [online]. Available at http://sectools.org/?page=3 [Accessed 21 April 2015].

Kaur I, Kaur H. 2014, *Analysing Various Packet Sniffing Tools.* International Journal of Electrical Electronics & Computer Science Engineering (IJITEE) (ISSN: 2348-2273, Volume-1, Issue-5) [online], Available at http://www.ijeecse.com/V1N5-014.pdf [Accessed 20 April 2015].

Murphy B, 2013, *Network Penetration Testing and Research* [online], NASA. John F. Kennedy Space Center. Available at http://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20140002617.pdf [Accessed 20 April 2015]

Ferrill, P. 2010, *Linux Planet.* [online] Available from: http://www.linuxplanet.com/linuxplanet/tutorials/7215/1 [Accessed 19 April 2015].

Gregory Conti, Julian Grizzard, Mustaque Ahamad and Henry Owen. 2005, *Visual exploration of malicious network objects using semantic zoom, interactive encoding and dynamic queries.* (2005) [online]. Available at: http://www.rumint.org/gregconti/publications/20050813_VizSec_BinaryRainfall.pdf [Accessed 19 April 2015].

No author. 2012, *Brief overview of 4 NFATs.* (January 2012). Available at: http://gutterchurl.blogspot.co.uk/2012/01/brief-overview-of-4-nfats.html

Pallavi Asrodia and Hemlata Patel. 2012, *Analysis of Various Packet Sniffing Tools for Network Monitoring and Analysis.* International Journal of Electrical, Electronics and Computer Engineering. ISSN No. (Online) : 2277-2626 (May 2012). Available at: http://www.researchtrend.net/pdf/13%20PALLAVI.pdf [Accessed 19 April 2015].

Erik Hjelmvik. 2008, *Passive Network Security Analysis with NetworkMiner.* Forensics Focus. [online]. Available at: http://www.forensicfocus.com/passive-network-security-analysis-networkminer [Accessed 21 April 2015].

Sam Abbott-McCune, A.J. Newtson, Robert Ross, Ralph Ware, and Gregory Conti. 2008, *Malware* INSECURE (magazine 15) [online], Available at: http://www.net-

security.org/dl/insecure/INSECURE-Mag-15.pdf
[Accessed 13 April 2015].

Angela Orebaugh, Gilbert Ramirez, Josh Burke, Greg Morris, Larry Pesce, and Joshua Wright. 2007, *Wireshark & Ethereal Network Protocol Analyzer Toolkit*, 1st Edition, Rockland, Massachusetts.
https://books.google.co.uk/books?hl=en&lr=&id=-AdTE9S3kigC&oi=fnd&pg=PA1&dq=wireshark&ots=Y7w2yXQMqS&sig=Gs4rYWS6HSnp_whMytseiHyh2Dc#v=onepage&q=wireshark&f=false
[Accessed 20 April 2015].

Russ McRee. 2008, *Expanding Response: Deeper Analysis for Incident Handlers.* [online], Available at: http://www.sans.org/reading-room/whitepapers/incident/expanding-response-deeper-analysis-for-incident-handlers-32904
[Accessed 22 April 2015].

Carvey, Harlan A. 2014, *Windows Forensic Analysis Toolkit.* Available at:
http://www.sciencedirect.com/science/article/pii/B9780124171572000102?np=y
[Accessed 22 April 2015].

Chris Sanders. 2011, *Practical Packet Analysis, 2nd Edition.* Available at:
http://www.nostarch.com/packet2.htm
[Accessed 22 April 2015].

Bibliography:

Malware
http://www.net-security.org/dl/insecure/INSECURE-Mag-15.pdf Insecure Magazine, February 2008

PCAP files comparison: web sites
http://147.228.94.30/images/PDF/Rocnik2012/Cislo5_2012/r6c5c5.pdf Electroscope, 2012

PCAP comparison: wireshark, tcpdumps, etherape, caspa (Y)
http://www.ijitee.org/attachments/File/v1i3/C0210071312.pdf International Journal of Innovative Technology and Exploring Engineering (IJITEE), August 2012

packet sniffers
http://www.ijcit.com/archives/volume2/issue1/Paper020110.pdf International Journal of Computer and Information Technology, January 2013

File Carving from PCAP
http://www.ijsart.com/pdf_up/108ijsart_150101023.pdf International Journal for Science And Research In Technology (IJSART), February 2015

winPCap
http://www.ijarcsse.com/docs/papers/11_November2012/Volume_2_issue_11_November2012/V2I11-0142.pdf International Journal of Advanced Research in Computer Science and Software Engineering, November 2012

packet sniffer
http://www.ijcncs.org/published/volume2/issue5/p6_2-5.pdf Attack Detection Methods for All-Optical Networks, No Date

evaluate performance of Microsoft NetMon, LibPCAP, PCAPng
http://www.researchgate.net/publication/260745050_Extended_Comparison_Study_on_Merging_PCAP_Files ElectroScope, October 2012

intentionally attacks on network detection
https://www.isoc.org/isoc/conferences/ndss/98/medard.pdf Attack Detection Methods for All-Optical Networks, No Date

scalable attack detection
http://cseweb.ucsd.edu/~varghese/PAPERS/p103-kompella.pdf On Scalable Attack Detection in the Network, No Date

passive visualisation of attack detection
http://dl.acm.org/citation.cfm?id=1029216 Passive visual fingerprinting of network attack tools**,** October 2004

Data visualisation Technique Framework for Intrusion Detection (snort) (Y)
http://ijcsi.org/papers/IJCSI-8-5-1-440-443.pdf IJCSI International Journal of Computer Science, September 2011

visualising network data for intrusion detection
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.106.5388&rep=rep1&type=pdf Visualizing Network Data for Intrusion Detection, June 2002

detecting dns-tunnels through n-gram visualisation and quantitative analysis
http://arxiv.org/ftp/arxiv/papers/1004/1004.4359.pdf NgViz: Detecting DNS Tunnels through N-Gram Visualization and Quantitative Analysis, No Date

Visualisation for computer security
http://web.ornl.gov/~ojg/goodall-vizsec07.pdf Introduction to Visualization for Computer Security, No Date

Visualisation System for Network Security Situational Awareness
http://trust.csu.edu.cn/conference/css2013/css13-3-111.pdf NetSecRadar: A Visualization System for Network Security Situational Awareness, No Date

DDOS detection
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.332.8593&rep=rep1&type=pdf An approach to reliably identifying signs of DDOS flood attacks based on LRD traffic pattern recognition, January 2004

Booz Allen Cyber Security Solutions
http://www.boozallen.com/media/file/CSN_Brochure.pdf Booz Allen Cyber Solutions Network, 2012

ten strategies of a world class cyber security operations center
https://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-

ops-center.pdf Ten Strategies of a World-Class Cybersecurity Operations Center, 2014

Advance Network Defense Research
http://www.rand.org/content/dam/rand/pubs/conf_proceedings/2005/CF159.pdf Advanced Network Defense Research, August 2000

tools for visualising IDS output (using my files)
http://www.cs.umd.edu/projects/netgrok/files/linux-mag-security_visualization_tools.pdf Spot intruders with these easy security visualization tools, September 2009

network attack visualisation
https://www.defcon.org/images/defcon-12/dc-12-presentations/Conti/dc-12-conti.pdf
Network Attack Visualization, No Date

malwarevis: entity based visualisation of malware network traces
http://www.cc.gatech.edu/~wzhuo3/pdf/malwarevis_vizsec_2012.pdf MalwareVis: Entity-based Visualization of Malware Network Traces , No Date

forensics visualisation with open source tools
http://simson.net/ref/2013/2013-11-05_VizSec.pdf Forensics Visualizations with Open Source Tools, November 2013

Visualisation and data collection
https://www.nsnam.org/tutorials/consortium13/visualization-tutorial.pdf NS-3 Advanced Tutorial: Visualization and Data Collection, March 2013

Davix visualisation workshop
http://www.secviz.org/files/DefCon2008_DAVIX.pdf DAVIX Visualization Workshop, 2008

interactive network anti-traffic visualisation
http://inav.scaparra.com/docs/whitePapers/INAV.pdf INTERACTIVE NETWORK ACTIVE-TRAFFIC VISUALIZATION, No Date

a visualisation tool for multi-scale networks
http://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=15&ved=0CEAQFjAEOAo&url=http%3A%2F%2Fwww.researchgate.net%2Fprofile%2FRomain_Fontugne%2Fpublication%2F220383974_A_Visualization_Tool_for_Exploring_Multi-scale_Network_Traffic_Anomalies%2Flinks%2F00b4953b127d5ac675000000.pdf&ei=WdUsVfqKM9LeaKahgLgI&usg=AFQjCNHDD_B32FDuc_CBoctE-8-mAaLlQQ&sig2=9U_h8SBQPVgucAkXxcOxlg A Visualization Tool for Exploring Multi-scale Network Traffic Anomalies, April 2011

visualisation for Rumint network data
http://www.rumint.org/gregconti/publications/20050423_IAW_Abdullah%28final%29.pdf
Visualizing Network Data for Intrusion Detection, June 2002

WiPal and WScout, Two Hands-on Tools for Wireless Packet Traces Manipulation and Visualization
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.218.5945&rep=rep1&type=pdf
Demo: WiPal and WScout, Two Hands-on Tools for Wireless Packet Traces Manipulation and Visualization, No Date

Real-time network visualisation
http://worldcomp-proceedings.com/proc/p2013/SAM9736.pdf
Simplified Network Traffic Visualization for Real-Time Security Analysis, No Date.

network analysis visualisation
https://www.cs.ubc.ca/~spark343/NAV.pdf
NAV - Network Analysis Visualisation, No Date.

designing visualisation capabilities for IDS Challenges
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.302.2949&rep=rep1&type=pdf
Designing Visualization Capabilities for IDS Challenges, No Date

integrite visualisation for network detection
http://scholar.google.co.uk/scholar_url?url=https%3A%2F%2Fsvn.labri.fr%2Fvisu%2FInfoVis_2011%2FVisWeek2011_proceedings%2Fvast%2Fchallenge%2Flamagna.pdf&hl=en&sa=T&oi=gga&ct=gga&cd=1&ei=B9gsVZihIMrI0QGqiYC4Dw&scisig=AAGBfm0et-vGXn6XAZzorAfOS5yGSsecQw&nossl=1&ws=1366x657
An Integrated Visualization on Network Events VAST 2011 Mini Challenge #2 Award: "Outstanding Integrated Overview Display", No Date.

network visualisation tool for network forensics using IDS cyberViZ
http://dspace.sliit.lk/bitstream/123456789/212/1/Page%2058-61.pdf
Visualization Tool for Network Forensics Analysis Using an Intrusion Detection System CyberViZ, Dec 2009.

Data capture architecture for honeynets
ftp://ftp.ie.freshrpms.net/pub/www.honeynet.org/papers/individual/model.pdf
Data Capture Architecture for Honeynets, No Date.

network visualisation tool for network forensics using IDS cyberViZ
http://www.cyberviz.webs.com/docs/CyberViZ%20SRS%20.PDF
Visualization tool for network forensics analysis using an Intrusion Detection System (CyberViZ), no date

visualisation of network to detect malicious network activity
http://www.diva-portal.org/smash/get/diva2:347722/FULLTEXT01.pdf
Visualization of Network Traffic to Detect Malicious Network Activity, no date

security visualisation
https://holisticinfosec.org/toolsmith/pdf/june2008.pdf
Security Visualization: What you don't see can hurt you, June 2008

network traffic threat detection
http://iiste.org/Journals/index.php/NCS/article/viewFile/19726/20232
Network Traffic Threat Detection and Reporting System Validation through UML
passive network fingerprinting, no date

http://scholar.google.co.uk/scholar_url?url=http%3A%2F%2Fwww.dtic.mil%2Fcgi-bin%2FGetTRDoc%3FAD%3DADA509167%26amp%hl=en&sa=T&oi=gga&ct=gga&cd=7&ei=DdssVbXoLMSr0QHAw4GIBw&scisig=AAGBfm1CIz6tkFd8jLvQ62EN12y8CwCToQ&nossl=1&ws=1366x657
visualising network resource usage (netgrok)
http://babu.cs.umd.edu/~cdunne/hcil/pubs/Blue08VisualizingReal-TimeNetwork.pdf
Visualizing Real-Time Network Resource Usage, no date

network attacks: taxonomy, tools and systems
http://cs.uccs.edu/~jkalita/papers/2014/HoqueNetworkAttacksJCNA2014.pdf
Journal of Network and Computer Applications, 2013

tracking of compromised hosts (afterglow)
http://bmeindia.org/paper/BEATs2010_355.pdf
Tracking Of Compromised Hosts Using Log Visualization System, no date

accessing outbound traffic to uncover advanced persistent threat
https://www.sans.edu/student-files/projects/JWP-Binde-McRee-OConnor.pdf
Assessing Outbound Traffic to Uncover Advanced Persistent Threat, no date

identifying network protocols in computer networks using vetrex profiles
https://wakespace.lib.wfu.edu/bitstream/handle/10339/14755/eddie_thesis_final.pdf?sequence=1

snort IDS and IPS toolkit [book]
https://books.google.co.uk/books?hl=en&lr=&id=ZI1sfn4eJ8oC&oi=fnd&pg=PP2&dq=afterglow+pcap&ots=NfNlZvttYi&sig=L7qw7O7ylCoteymTzl2Jak4B2bM#v=onepage&q=afterglow%20pcap&f=false

attack simulation and threat modelling
https://docs.google.com/document/d/1kVoIUoMb59TksS2HHxWkHhDQEx-D-fMU7ClmHcy_sbo/edit

graphical user interface for Intrusion Detection in telecommunications network
http://future-internet.fi/publications/zahariev2011.pdf
Graphical User Interface for Intrusion Detection in Telecommunications Networks march 2011

visualisation of PRADS output data using open source visualisation tools
https://www.duo.uio.no/bitstream/handle/10852/42155/1/Desta-Dawit-Master.pdf
Visualization of PRADS Output Data Using Open-source Visualization Tools For Improved Log Analysis, no date

applied network security monitoring [book]
https://books.google.co.uk/books?hl=en&lr=&id=TTIDAQAAQBAJ&oi=fnd&pg=PP1&dq=afterglow+pcap&ots=Uv0OK4zM3W&sig=-zRoscAoFBoLL0SfDrSfIPEPT3g#v=onepage&q=afterglow%20pcap&f=false Applied network security monitoring, no date

security analysis with wireshark
http://holisticinfosec.org/toolsmith/pdf/november2006.pdf

Security Analysis with Wireshark, november 2006

evaluating IDS and IPS using tomahawk and wireshark
http://worldcomp-proceedings.com/proc/p2012/SAM9784.pdf
Evaluating Intrusion Detection and Prevention Systems Using Tomahawk and Wireshark, no date

analysis of a man-in-the-middle experiment with wireshark
http://www.lidi.info.unlp.edu.ar/WorldComp2011-Mirror/SAM4991.pdf
Analysis of a Man-in-the-Middle Experiment with Wireshark, no date

A visual querying system for network monitoring and anomaly detection
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.227.7802&rep=rep1&type=pdf TVi: A Visual Querying System for Network Monitoring and Anomaly Detection, no date

metric visualisation security
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.232.1151&rep=rep1&type=pdf A Visualization and Modeling Tool for Security Metrics and Measurements Management, no date

real-time and forensic network data analysis. Using animated and coordinated visualisation
http://juliangrizzard.com/pubs/2005_krasser_iaw.pdf
Real-Time and Forensic Network Data Analysis Using Animated and Coordinated Visualization, no date

User requirements and design of visualisation for intrusion detection analysis
http://web.ornl.gov/~ojg/goodall-iaw05.pdf

User Requirements and Design of a Visualization for Intrusion Detection Analysis
an overview visualisation for network analysis
https://projects.cs.dal.ca/flovis/files/VizSec-2009.pdf OverFlow: An Overview Visualization for Network Analysis, no date

Identifying and investigating intrusive scanning patterns by visualising network
http://icsa.cs.up.ac.za/issa/2006/Proceedings/Full/50_Paper.pdf
IDENTIFYING AND INVESTIGATING INTRUSIVE SCANNING PATTERNS BY VISUALIZING NETWORK TELESCOPE TRAFFIC IN A 3-D SCATTER-PLOT, no date

security visualisation tools and ipv6 addresses
https://www.ccsl.carleton.ca/paper-archive/barrera-vizsec-09.pdf Security Visualization Tools and IPv6 Addresses∗, no date
visualisation of power-law network topologies
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.124.4700&rep=rep1&type=pdf
Visualisation of Power-Law Network Topologies, no date

visualisation of network data provenance
http://d2i.indiana.edu/sites/default/files/pid2542375.pdf
Visualization of Network Data Provenance, no date

SpiralView: Towards Security Policies Assessment through Visual Correlation of Network Resources with Evolution of Alarms
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.139.4387&rep=rep1&type=pdf
SpiralView: Towards Security Policies Assessment through Visual Correlation of Network Resources with Evolution of Alarms, no date

Analysis of Various Packet Sniffing Tools for Network Monitoring and Analysis.
http://www.researchtrend.net/pdf/13%20PALLAVI.pdf analysis of various packet sniffing tools for network monitoring and analysis, may 2012

Wireshark and Ethereal Network Analyzer Tool
https://books.google.co.uk/books?hl=en&lr=&id=-AdTE9S3kigC&oi=fnd&pg=PA1&dq=wireshark&ots=Y7w2yXQMqS&sig=Gs4rYWS6HSnp_whMytseiHyh2Dc#v=onepage&q=wireshark&f=false
Wireshark and Ethereal, 2007

Passive Network Security Analysis with NetworkMiner
http://www.forensicfocus.com/passive-network-security-analysis-networkminer
Forensic Focus, no date

A brief overview of 4 nfats tools
http://gutterchurl.blogspot.co.uk/2012/01/brief-overview-of-4-nfats.html don't blink, January 2012