Insight: An Application of Information Visualisation Techniques to Digital Forensics Investigations

Gavin Hales, Ian Ferguson, and Jacqueline Archibald

School of Design and Informatics, Abertay University, UK

ABSTRACT

As digital devices are becoming ever more ubiquitous in our day to day lives, more of our personal information and behavioural patterns are recorded on these devices. The volume of data held on these devices is substantial, and people investigating these datasets are facing growing backlog as a result. This is worsened by the fact that many software tools used in this area are text based and do not lend themselves to rapid processing by humans.

This body of work looks at several case studies in which these datasets were visualised in attempt to expedite processing by humans. A number of different 2D and 3D visualisation methods were trialled, and the results from these case studies fed into the design of a final tool which was tested with the assistance of a group of individuals studying Digital Forensics.

The results of this research show some encouraging results which indicate visualisation may assist analysis in some aspects, and indicates useful paths for future work.

Keyword: digital forensics, information visualisation, computer security, usable security

1 INTRODUCTION

Significant problems are being faced by those in investigative roles, such as law enforcement, who deal with digital devices; as the volume of data these investigators are required to analyse is constantly increasing. The tools used to investigate these datasets are adapting in their ability to capture and process the data from devices, for example, creating evidentially sound duplicates. However, these tools tend to lag behind in their ability to display the acquired data in a way which lends itself to rapid analysis by humans. The tools typically display information in a textual format; however, it is well established that humans excel at the rapid processing of visual data, and do not do so well at processing the same data presented in a textual format.

This body of research examines the application of various information visualisation techniques to digital forensic datasets, and the impact on usability and investigative effectiveness from the application of such techniques. As a digital forensic investigator, the aim is often to discover evidence within the dataset which proves or disproves the guilt of a suspect involved in a criminal act. Not only this, but the frequently personal nature of the datasets taken from devices is often useful in building a narrative of user behaviour and intentions. From a situational awareness perspective, it is important that the investigator is aware of the information presented to them by the device and how it fits into the case they are dealing with. It is hoped that the visualisation of this information can aid their comprehension and allow them to form an understanding of how the device dataset impacts on the case in terms of providing evidence of guilt, and suspect motives.

This paper will discuss a number of case studies in which pilot visualisations were created to visualise a digital forensic dataset; and the ways in which the outcomes of these case study visualisations were used to feed into the design of a final prototype tool called “Insight”. This tool was then tested with a group of qualified participants to examine whether there are any significant advantages to displaying digital forensic datasets to the investigator in a visual format, specifically whether there are any gains to investigative effectiveness. The participants were asked to complete 6 tasks which required them to explore the dataset using the tool they were allocated to find the answer. This mock investigation was timed in order to provide a metric to assess investigative efficiency, and the accuracy of the answers given by the participants was quantified using a simple correct / incorrect grading system. Each task was also followed by a Likert scale which asked the participant to feedback how easy they found the task to

complete using the tool they were given. This was used to gauge the overall user experience when using the tool.

2 BACKGROUND

Computers initially began as an expensive piece of technology which would only be owned by companies. This has rapidly changed over the years to a point where personal digital devices are ubiquitous in developed economies. It is very common for a single person to own multiple digital devices of various descriptions, and in fact, most households will also have a multitude of devices to serve various purposes ranging from entertainment to home security. Casey (2010) observed that this has led to accumulation of "digital dust"; that is, the accumulation of digital evidence in places which would not necessarily be expected. This transforms them into excellent sources of information and evidence to be utilised in digital forensics investigations. The issue which arises from this is the volume of data to be processed from all of these devices becomes so large that it becomes troublesome to analyse in a timely manner. Roussev et al (2013) identified that between 2003 and 2011 the volume of data a law enforcement digital forensic investigator was required to deal with, per case on average, increased by 6.65x, from 84GB to 559GB. Lillis et al (2016) recognise that backlogs faced by law enforcement in digital forensics investigations are often around 2 years and in some cases even up to 4 years. This has even meant that in severe cases some prosecutions have been dismissed by courts due to the delay. Garfinkel (2010) has argued that we are in fact nearing the end of the "Golden Age of Digital Forensics" due to the increasing difficulties faced in processing data. In the taxonomy of issues faced in the field of digital forensics produced by Karie and Venter (2015), "vast volumes of data" is one of the significant challenges faced, along with "emerging technologies and devices", which is demonstrated through the increasing move towards devices such as smart TVs and voice controlled assistants such as the Amazon Echo.

A number of attempts to reduce this backlog have been made by targeting different stages of the investigative process. The acquisition stage has been expedited somewhat with the creation of newer drive interfaces with higher transfer rates, and with research utilising the massive parallel processing ability of graphics cards to carve files from disk images (Bayne, Ferguson, Sampson, & Isaacs, 2016). The analysis phase has also been targeted in some different ways. Much of the research in this area aims to reduce the amount of data the investigator is required to examine via triage techniques, or by filtering the data in some way so as to give the investigator an indication of where to focus their searches. Gladyshev and James (2017)

implemented decision theoretic carving (DECA) which fulfils both a filtering and a triage role. This work is designed to allow an investigator to rapidly retrieve JPEG images from the disk. In doing so, they are quickly given an indication as to whether the disk is likely to contain images which would be considered as contraband, and then investigate this further if necessary. The authors point out this is very useful in a situation such as when a parole officer needs to check an offender's computer. In such a scenario, a full digital forensics investigation would not be feasible because of the amount of time it would take, and would add to the already unacceptable backlogs faced by law enforcement.

This research looks to focus on the analysis stage of the investigation, and specifically how tool support can be improved to support a full investigation through the utilisation of information visualisation techniques. It is expected at this stage that the dataset will have been subject to triage already and may have indicated some content which warranted further investigation. The tools used at this stage of a full investigation such as Encase and Autopsy are often referred to as "push-button" tools which analyse a dataset automatically and retrieve substantial amounts of data which would be useful to an investigation. However, at the time of writing, these tools tend to display the information to the investigator in a textual, tabular format, with some filtering functionality. The end user must then explore the data to find evidence relevant to the case. It is this exploratory aspect which is of interest, and which information visualisation techniques may be able to assist.

Visualisation of data has been shown to be an effective way to explore a dataset for a long time. Scottish engineer William Playfair (1796) was one of the pioneers of information visualisation with his use of bar and line graphs to depict economic data in a more accessible format to the reader. An excellent historical example of the value of exploratory information visualisation was that of John Snow (1855) who created a diagram which overlaid confirmed cases of cholera infection onto a street map of Soho in London (Figure 1). It was through this visualisation of the data that the data could be seen from a perspective which allowed exploration of the data in a different way than would have been possible had the data been displayed in a solely textual format. Through this visualisation it could be seen that cases of infection were clustered around a water pump. From this, it was realised that cholera was a waterborne disease.

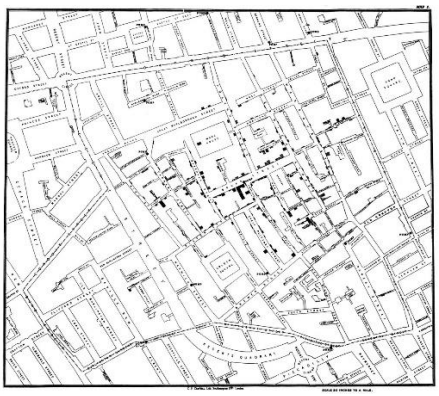

Figure 1 - Map of cholera infection in London (1854)

In many areas of computer security, information visualisation techniques have also been applied successfully. One of the most prominent of these is the area of network security and situational awareness. Typically, network security appliances such as firewalls and intrusion detection systems generate a significant amount of logging data in text format. The velocity of this data in a large network also tends to be very high. For a human to manually parse this information and maintain awareness of the security state of the network is entirely unrealistic. It would be extremely difficult for an analyst to maintain awareness of the hierarchy of the network and the typical activity which takes place across it; and to spot any anomalies in this. The application of information visualisation techniques to this data is invaluable. One such example of this is the tool Snorby (Sanders & Smith, 2014) which takes data from the Snort IDS and presents it as an easy to understand dashboard to the end user. In doing this, the end user can easily spot any high priority intrusion events on the network, maintain an effective awareness of the security of their network, and quickly take appropriate action. It is reasoned that as this application of information visualisation has been successful in this area of computer security, that digital forensics may benefit from its application as well.

3 METHODOLOGY

Introduction

As this research aimed to apply information visualisation techniques to digital forensics datasets, it was important to methodologically find a visualisation which was “best-fit” for the data and which would likely be of most use to the investigator. To do this, an iterative approach was taken which would examine different ways to apply these techniques to the data as a small case study. The strengths and the weaknesses of the prototype

visualisation tool would be examined by the authors, and used to inform the design of the next case study tool. No additional participants were utilised in the early case study stages of this research. Once a stage had been reached where a number of case studies had been performed and a satisfactory level of knowledge regarding what may be the best format to use had been gained, a final prototype tool was created. This tool was named "Insight" and was refined with the input of a focus group consisting of students with a background in computer security. The tool was then used in a final experiment involving Digital Forensics students who possessed the baseline level of knowledge required to complete a small-scale investigation, with the aim to discover whether there were any effects on investigative efficiency, accuracy, or user experience.

One of the issues when conducting digital forensics datasets is the lack of availability of realistic datasets. This is due to the fact that they will often contain a large amount of copyrighted, personal, or even illegal data. In order to work around this issue, two datasets were used in this research; the primary dataset is a Windows XP disk image created by one of the authors, Ferguson, as a teaching tool. This image is around 5GB in size and depicts around 2 weeks' worth of frequent device usage in which the user deals with images and information of birds. This is used to simulate a criminal case involving the trade of contraband images without the use of illegal material. The small size of the disk image allows an investigation to be completed in a reasonable amount of time. This is essential for testing as it allows participants to explore most of the information in one sitting, allowing for relatively tightly controlled experiments. There are 368 events in this dataset when processed. The secondary dataset used was a 500GB disk image with several years usage taken from the personal laptop of one of the researchers. This dataset was used solely to test the visualisation with realistic scale datasets to ensure information was not obscured, performance was acceptable etc. Due to the personal nature of this data, no results from its use were made publicly available, but were used to inform the design of each case study. There were 23,112 events in this dataset when processed.

The datasets were first pre-processed using the Autopsy 3 software to derive a dataset which was more readily usable when creating a visualisation tool. Autopsy extracts information such as filesystem information, web browser histories, emails, EXIF data etc. and deposits this into an SQLite database. The reason for using this pre-processed dataset as opposed to the raw disk image is that this would add a significant amount of unnecessary work to the research. Autopsy and related tools are very effective at extracting usable data from a disk image, but this research seeks to improve on the way this information is then displayed to the end user.

Case Studies

Case Study 1 – Pysight

The first of the case studies looked to build on the limited timeline visualisation included in the Autopsy software. This timeline simply displays the total number of events that had occurred in a day, in a bar chart format. This case study examined whether this timeline could be split out into a 3D cube, in which distinct types of events were shown on different "layers" along the z axis. Individual dates were marked along the x-axis, and the time of day increased along the y axis, with midnight marked at the top and 23:59 marked along the bottom. This layout was designed for the viewer to read from top to bottom, left to right. The motive behind this was that it was hoped repetitive user behaviours at similar times of day would create a pattern along the cube. This could be correlated with different types of event along the z axis.

This case study was of limited success as it immediately showed that the stacking of events in layers significantly obscured what the user could see. Allowing the user to rotate the cube partially solved this issue, however, it then introduced the problem of the end user losing track of the correct orientation of the cube, rendering it useless.

Case Study 2 – Hyperbolic Visualisation of File Systems

The second case study aimed to look at the value of the file system data presented by Autopsy, and examine the use of a visualisation built using hyperbolic space as opposed to Cartesian space (Hales, Ferguson, & Archibald, 2013). This visualisation utilised the Walrus hyperbolic graph visualisation tool (Hughes, Hyun, & Liberles, 2004). It was hoped that a hyperbolic graph be built showing the directory structure from the disk and other useful information could be overlaid onto this. Figure 2 shows a visualisation of the file system from clean installation of the Windows 7 operating system. The varying colour of the nodes represents the file creation timestamp.

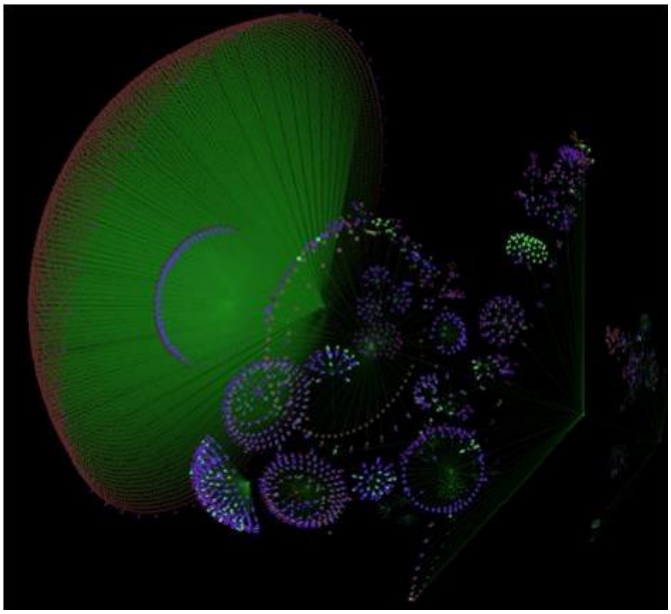

Figure 2 – Hyperbolic graph of a Windows 7 installation using Walrus

This visualisation showed some positive results in that patterns could be recognised between different OS versions, and information such as directory creation times could show old and new branches of the file system. For example, in Figure 2 the large cluster of burgundy colour nodes can easily be recognised by the end user as subdirectories of the WinSxS folder. However, this was of limited use to an investigation, and as the visualisation again allowed the user to rotate and re-centre the graph in 3D, the user could quickly lose their ability to recognise patterns and keep their bearing. As this had been a repeated problem with 3D visualisations, it was decided at this stage that the next case study would look at 2D visualisations, and that file system information would not be the focus as it provided little value when trying to discover narratives of user behaviour.

Case Study 3 – Insight.js

The final case study took the lessons learned from the previous case studies and moved to a 2D visualisation as a result. In this instance, the timeline format of displaying information seemed like the best fit for the data, and so a 2D timeline was built to run in web browser using available JavaScript libraries. Several types of event were placed on the timeline using different colours, and this would allow the end user to quickly see a chain of events regardless of their type. For example, “the user took a photo (as indicated by

EXIF data) and then shortly after, uploaded this to a photo sharing site (as indicated by web browsing history).

Although the format of this visualisation seemed promising, and followed the Visual Information Seeking Mantra proposed by Shneiderman (1996) of "overview first, zoom and filter, details on demand", the performance of the tool was poor. As the datasets in digital forensics investigations are generally large, this did not work well when loaded into a web browser. Frequently, script timeouts were triggered, and the tool was terminated by the browser.

Final Tool – Insight

The final version of the prototype tool built on the last case study, having discovered that a timeline visualisation provided an intuitive way to display different data types to the end user and to allow them to explore it in a familiar way. The final tool took into account the problems that had been found with the web version of the tool and moved to the .NET platform to run as a Windows desktop application (Figure 3).

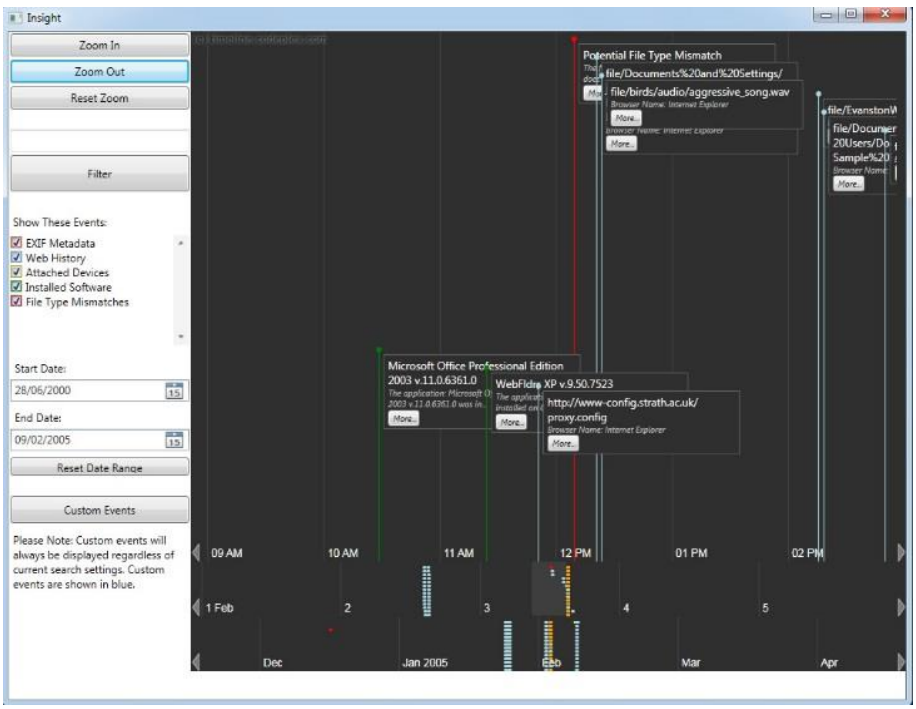

Figure 3 – Insight visualisation software

This final version of the tool also expanded the ability of the user to search and filter the data by type, for example, web browsing history or installation of software; added 2 smaller timelines below the primary timeline with different time scales, allowing the user to move through different time frames more effectively; and also gave the user the ability to add custom events to the timeline. The reason for this is that the first 2 case studies showed how important it is for the user to have landmarks when exploring a large visual dataset. This feature allows them to add their own landmarks, and to add additional external information they may be in possession of but may not necessarily be reflected in the dataset. For example, if the suspect was not in possession of the device for a period of time. A detail window was also added which would allow the user to see much more information about the event, a feature which had been missing from the web case study tool (Figure 4).

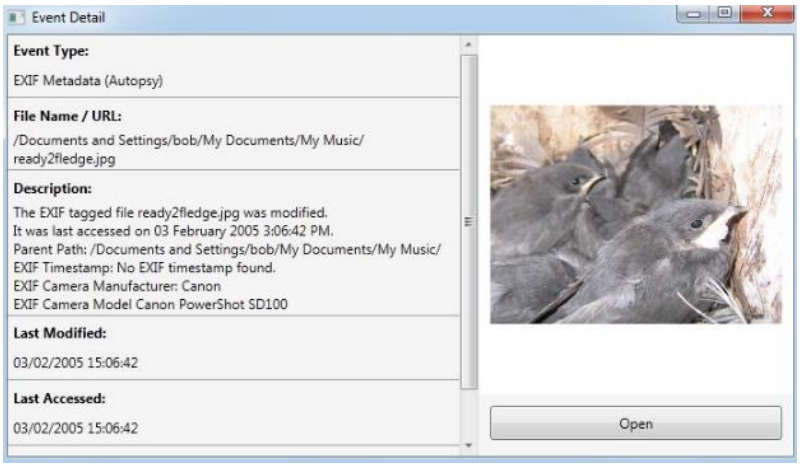

Figure 4 – Event Detail Window

Once this tool had been built, it was tested with a small pilot group of students with backgrounds in computer security (n=5). From this group, qualitative feedback was gathered regarding the usability of the tool which highlighted any missing features and major flaws, for example, cases in which the application would frequently crash, and the fact that a number of events from the Windows base install had dates from the year 1980 which led to an unnecessary extension of the timeline and excessive scrolling for the end user. These were then fixed, and the final tool prepared for test with a full participant group. The tool was also tested with the secondary dataset of 23,112 events and performed well, loading and scrolling along the timeline in an acceptable time.

The final experiment was conducted with a group of Digital Forensics students (n=29) who possessed the baseline knowledge required to complete a digital forensics investigation. Autopsy 3 was used as the control tool in this experiment to allow for a comparison to traditional text based digital forensics tools. The participants taking part in this experiment had no previous experience in using either the Autopsy 3 or prototype Insight software, as they had reached a point in their education in which they had been exposed to mostly command line digital forensics tools such as Scalpel, along with the methodologies for completing a digital forensic investigation.

All of the participants were given a set of 6 tasks to answer which required them to find different pieces of evidence in the primary dataset. Some of these tasks were broken down into smaller sub-questions relating to the same event to aid clarity for the participant. For example, one of the tasks required the participant to find the model of camera used to take a large number of the images in the dataset, while another required that they identify where the user had been on a particular day (identified by the presence of a Wi-Fi captive portal login page). The tasks presented to the participants are shown in Table 1. To complete these tasks, participants were randomly allocated either the Autopsy or Insight software to use. 15 participants were allocated the Insight software and 14 allocated the Autopsy software. Each participant was given a virtual machine with the software and dataset preinstalled, and timer software installed to time how long they took to complete the investigation. The participants were instructed to only use the software they had been assigned, and to withhold discussions about the experiment with others until everyone had completed the investigation. The investigation was designed to be completed in one sitting so as to prevent external factors from influencing the results.

Task 1 – Firefox	
1.1	The suspect installed Firefox on their PC. Find the date and time of installation.
1.2	The suspect initially tried to download the Firefox installer from a non-Mozilla website. Which website was this?
Task 2 – Avian Images	
2.1	The suspect is known to own a Canon EOS-1D camera. Find a photo of a bird taken with this model of camera. What is the filename and path?
2.2	When was this image last accessed?

Task 3 – Anti-Forensics	
3.1	The suspect has attempted to hide a ZIP file full of bird images. What is the filename and path?
3.2	List the filenames of two of the images inside this ZIP file.
Task 4 – EXIF Metadata	
4.1	A large number of the photos on the suspects device were taken using the same camera, what make and model? *Note (not given to participants): This is not related to Task 2. Very few images were taken with the camera model in Task 2.*
Task 5 – University	
5.1	The suspect took their device to a university at some point. Which university?
5.2	How do you know this?
5.3	On what date did they take it to the university?
Task 6 – Suspicious Event	
6.1	On 2nd Feb 2005 at 4:32pm, the suspect did something on their device which could be considered to be suspicious. What did they do?

Table 1 – Tasks presented to participants

As part of each task, the participants were asked to rate on a Likert scale how easy they found the task to complete, on a scale of 1 – Very Difficult to 5 – Very Easy. They were also given an opportunity to provide open-ended feedback after each task, and at the end of the experiment to comment on the tool they used in general. This metric was used to assess the user experience of using the visualisation method in comparison to the traditional text based tool.

The accuracy of the participant's response to each task was also assessed. This was measured as a simple correct / incorrect grading for each task based on whether their answer matched the known evidence in the dataset. It was important to measure this metric to ensure that any other differences which were found from the use of the visualisation software were not counterbalanced by a significantly lower accuracy rate. Such a situation in a law enforcement context would not be acceptable as this could have a serious impact on the outcome of a case. In cases where the task was broken

into a few sub-questions, each of the sub-questions had to be correct for the entire task to be considered correct. This is due to the fact that all of the sub-questions relate to the same event in the dataset and are tightly linked to a fragment of user behaviour.

4 RESULTS

The results of this research showed that when comparing the time taken to complete the task, a metric to reflect investigative efficiency, there was no statistically significant difference between the groups (Table 2), (unpaired t-test, $\alpha = 0.05$). In this context we cannot conclude that the use of visualisation techniques leads to gains in investigative efficiency.

	Autopsy	Insight
Min	00:37:14	00:23:15
Mean	01:05:22	00:56:12
Max	02:22:08	02:02:38
	p-Value	0.4382

Table 2 – Participant Completion Times

When looking at the accuracy of participant responses (n-1 Chi-Squared, $\alpha = 0.05$), it was found that in 5 of the 6 tasks showed no significant differences in levels of accuracy (Table 3). However, one of the tasks showed a significant difference with a p-value of 0.0004598. This question showed that the accuracy rate was significantly better amongst the group using the Insight tool. This allows us to conclude that in some cases, evidence is more obtainable when the dataset is presented in a visual format.

	Task 1	Task 2	Task 3	Task 4	Task 5	Task 6
Insight	80.00%	100.00%	46.67%	100.00%	80.00%	80.00%
Autopsy	54.55%	90.91%	72.73%	100.00%	9.09%	72.73%
p-Value	0.1730799	0.4230769	0.1925642	1	0.0004598	0.6698151

Table 3 – Accuracy of participant responses

3 participants were unable to fully complete the investigation, or the timing mechanism failed during the experiment. For these participants, their results have not been considered when calculating efficiency or accuracy metrics. Their results were included when calculating Likert scale results, as this data was available.

Finally, the Likert scale results were analysed to assess for any significant differences in the participant's experience of using each tool (Mann-Whitney U test, $\alpha = 0.05$). It could be seen that in 2 of the 6 tasks, there were significant differences. In both tasks, participants from the Insight test

group reported generally that the task was easy to solve, in comparison to the Autopsy group in which very few people reported finding the task easy (Figure 5). These results allow us to conclude that when dealing with certain tasks in an investigation, the visualisation of information provides a more intuitive way for the end user to explore the information available to them. This is reinforced by the fact that one of the two tasks which showed a significant positive difference in terms of user experience when using visualisation also showed a significant positive difference in terms of accuracy.

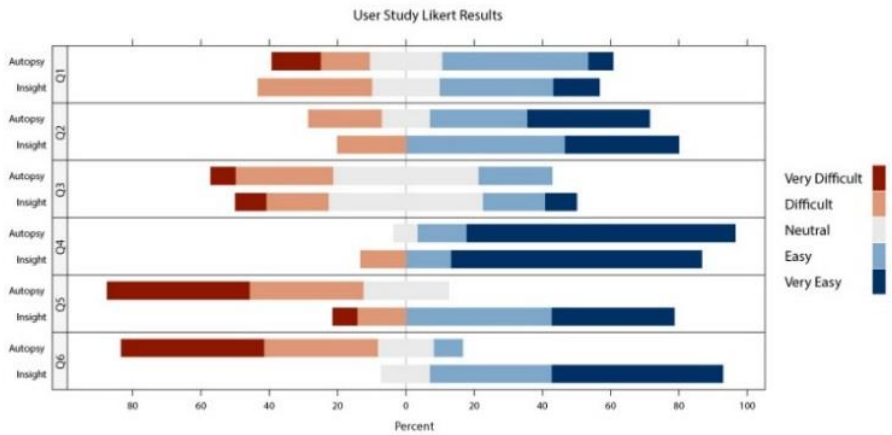

Figure 5 – Participant Task Feedback

5 CONCLUSION

The results from this body of research have shown that when information visualisation in the form of a 2D timeline is used to complete a digital forensics investigation, it cannot be said that it provides benefits in terms of an increase in investigative efficiency. As such, it cannot definitively be said at this stage that application of visualisation techniques in this format is a solution to the increasing backlogs faced by investigators. However, it is recognised that for the purposes of this research, the length of the investigation was much shorter than would normally be encountered by a digital forensics investigation in a realistic scenario. This is difficult to address due to the lack of availability of real datasets and available qualified participants to form an acceptable sample size.

It is however, interesting to note that it was discovered that in parts of the investigation, it was shown that the use of a visualisation tool resulted in

more accurate responses and an improved user experience. This is encouraging when combined with the fact that there was no significant difference in investigative efficiency, as this means that these benefits are present and do not have a negative impact on the time taken to complete an investigation. It is conjectured that if these benefits were present in a real investigation and were used to compliment, rather than replace, existing tools, gains in investigative efficiency may become evident.

As situational awareness can be defined as "the state of being aware of circumstances that exist around us, especially those that are particularly relevant to us and which we are interested about" (Onwubiko & Owens, 2011). We can say that this visualisation tool can improve the situational awareness of the investigator as it allows them to become aware of the behaviours of the device owner, and how this information relates to the case they are investigating, shown by the improved user experience and slight accuracy increase provided by the tool.

6 FUTURE WORK

As an outcome of this research it was recognised that it would have been useful to tightly classify the type of questions the participants were being asked to answer, to establish whether certain tasks or data types benefitted more heavily from visualisation than others. Given a larger sample size, a similar experiment could be conducted in which these differences between types of tasks in an investigation are examined.

The issues faced in the creation of a 3D visualisation in the case study stage of this research have raised several interesting ideas amongst the authors for further paths in which this could be explored. The early stages of research are being carried out to examine ways in which modern 3D techniques and technologies can be used to overcome some of the issues faced in this body of research. Modern game engines, such as Unity and Unreal, are being explored in this research. There is also a potential to explore a "story-telling" aspect of this field, in which the evidence is presented to end users in a visual way. This may be of use in the presentation phase of an investigation to allow non-technical users to explore a narrative of user behaviour. This research would also allow a cross-disciplinary approach to

be taken which draws together researchers in cyber security, computer games and computer arts.

As Virtual Reality technology is becoming more accessible, in forms such as the HTC Vive, future work may look to explore how digital forensics datasets could be explored in such an environment. In using such a technology, the user has the ability to walk around in the data and will naturally have a few landmarks such as their own position in 3D space, the direction their body is facing in relation to the environment etc. As many uses of VR visualisation tend to utilise existing visualisation methods and reuse these VR, it would be of interest to create an entirely new way to visualise to data which makes full use of the opportunities provided by VR hardware to display digital forensic data.

There are also opportunities to utilise AI and machine learning in this area. Specifically, this could be used to effectively triage a dataset or to prioritise the display of information to a user when combined with information visualisation techniques. It is conjectured that machine learning could potentially be utilised to recognise common patterns of user behaviour which may be associated with criminal activity. This may become very useful if analysing large datasets from social media, in which AI could be used to learn communication patterns between people, and interaction patterns which could be indicative of organised criminal behaviour.

6 REFERENCES

Bayne, E., Ferguson, R. I., Sampson, A., & Isaacs, J. (2016). Using multiple GPUs to accelerate string searching for digital forensic analysis. *11th International Conference on Systematic Approaches to Digital Forensic Engineering (SADFE 2016).*

Casey, E. (2010). Digital dust: Evidence in every nook and cranny. *Digital Investigation, 6*(3), 93-94. doi:10.1016/j.diin.2010.02.002

Garfinkel, S. (2010). Digital forensics research: The next 10 years. *Digital Investigation, 7*, 864-873.

Gladyshev, P., & James, J. I. (2017). Decision-theoretic file carving. *Digital Investigation, 22*, 46-61.

Hales, G., Ferguson, I., & Archibald, J. (2013). On the use of hyperbolic visualization to assist digital forensic analysis. *Cyberforensics Perspectives: Proceedings of the 3rd International Conference on Cybercrime, Security and Digital Forensics (Cyberforensics 2013).* Glasgow.

Hughes, T., Hyun, Y., & Liberles, D. (2004). Visualising very large phylogenetic trees in three dimensional hyperbolic space. *BMC Bioinformatics, 5*(1), 1-6.

Karie, N., & Venter, H. (2015). Taxonomy of Challenges for Digital Forensics. *Journal of Forensic Sciences*, 885-893.

Lillis, D., Becker, B., O'Sullivan, T., & Scanlon, M. (2016). Current Challenges and Future Research Areas for Digital Forensic Investigation. *The 11th ADFSL Conference on Digital Forensics, Security and Law (CDFSL 2016).* Daytona Beach, Florida, USA.

Onwubiko, C. & Owens T.J. (2011). Review of Situational Awareness for Computer Network Defense. In C. Onwubiko and T.J. Owens (Eds.) Situational Awareness in Computer Network Defense: Principles, Methods and Applications

Playfair, W. (1796). *The Commercial and Political Atlas: Representing, by Means of Stained Copper-Plate Charts, the Progress of the Commerce, Revenues, Expenditure and Debts of England during the Whole of the Eighteenth Century.*

Roussev, V., Quates, C., & Martell, R. (2013). Real-time digital forensics and triage. *Digital Investigation, 10*(2), 158-167. doi:10.1016/j.diin.2013.02.001

Sanders, C., & Smith, J. (2014). Signature-Based Detection with Snort and Suricata. In *Applied Network Security Monitoring* (pp. 203-254). Boston: Syngress.

Shneiderman, B. (1996). The Eyes Have It: A Task by Data Type Taxonomy for Information Visualizations. *Proceedings of the 1996 IEEE Symposium on Visual Languages*, (pp. 336-343).

Snow, J. (1855). *On the Mode of Communication of Cholera.* John Churchill. Retrieved from http://books.google.co.uk/books?id=-N0_AAAAcAAJ

BIOGRAPHICAL NOTES

Dr Gavin Hales is a Lecturer in the Division of Cyber Security at Abertay University. Gavin completed his PhD in the area of Digital Forensics and Information Visualisation at Abertay University in 2016; this PhD was funded by a SICSA Prize Studentship with a value of around £54k.

Gavin teaches on a number of undergraduate modules, including Introduction to Security, Enterprise Systems Engineering, Software Design; he also supervises both undergraduate and postgraduate students during their final projects.

As an early-career researcher, his research interests lie in Digital Forensics, Secure Software Development and Internet of Things Security.

Dr Ian Ferguson gained his PhD in Software Engineering from the University of Sunderland in 1998. His work on engineering mobile agent environments led to an interest in mobile computing and context aware systems.

Between 2000 and 2010 at the University of Strathclyde, in the Pervasive and Ubiquitous Computing Group of Smartlab, he successfully supervised 5 PhDs on networks of distributed mobile agents. These experiences led to an interest in digital forensic readiness and funded projects looking at security issues in public access networks. Other funded research included a £30K Microsoft project looking at agent mobility.

At Abertay University (where he leads the Security Research Group) his work concentrates on the application of software tools to cybersecurity particularly the use of data-visualisation techniques to aid security incident awareness and digital forensic investigation. This has resulted in 3 successful PhDs and 3 current supervisions. Funded research includes two SICSA funded PhDs (£72K), two R-LINCS PhD studentships (£72K) in cybersecurity, and a SIPR award of £50K to perform a review of the international policing response to cybercrime.

Dr Jaqueline Archibald is a Lecturer in Computing at Abertay University. She has a PhD in Natural Language Processing and MSc in Information Technology from Aston University and MA (Hons) in Russian Language and Literature from University of Glasgow.

Her main teaching interests are in aspects of User Interfaces, Usability, Affective Computing and Cybersecurity. Dr Archibald's research focus is primarily in Cybersecurity, specifically Usable Security.

Previously she has researched and published in area of Women in Computing, Natural Language Processing and Intelligent systems. She has successfully supervised 6 PhDs, 2 MPhils and 2 MbR (with industry partners). She has also examined 5 PhDs. Dr Archibald has over 30 publications ranging from conference proceedings, journal articles and book editorials.

REFERENCE

Reference to this paper should be made as follows: Hales, G., Ferguson, I. & Archibald, J. (2017). Insight: An Application of Information Visualisation Techniques to Digital Forensics Investigations. *International Journal on Cyber Situational Awareness,* Vol. 2. No. 1, pp100-118.