

SYNTHESIZE A SOLUTION TO A POTENTIAL REAL LIFE SCENARIO

Shay Friel
Computer Networks and Cybersecurity
Module Code: ACCB5000
Swansea, Wales
Sfriel.151758@student.uwtsd.ac.uk

TABLE OF CONTENTS

Introduction.....	1
Related Work.....	1
Discussion of the Case Study Investigation.....	5
- Johns Investigation Document Steps	5
- Johns Investigation Report.....	6
- Figures 1-8.....	7
Results/Findings.....	9
Conclusion.....	9
References.....	10

Abstract— Digital forensics has a crucial role in providing reliable computer analysis and digital evidence to serve legal purposes. Computer Forensic tools are used by professionals in the application of investigation and analysis techniques to collect and retain evidence from computer devices in a way that is applicable ready for demonstration in a court of law. This report analyses various Computer Forensic tools and categories the most frequent use tools by Computer Forensic professionals.

I. INTRODUCTION

In computer forensics the concept never changes, the method is partially change but the tools always change. Some tools are commercial while some are open source. The aim of computer forensics is to examine digital devices in a constructive way with the goal of identifying, preserving, recovering, analysing, and presenting the evidence in a court of

law. [1] The main objective of computer forensics is to perform crime investigations by using evidence from digital data to find who was responsible for that particular crime. For better research and investigation, developers have created many computer forensic tools. [2]

Digital forensic tools are designed for forensic investigators. These tools are also used for purposes of maintenance, data recovery, debugging and reverse engineering of computer systems in private settings. Digital forensics is used by both law enforcement and private sector investigators and is immediately becoming a consequential part of computer investigations around the world.

II. RELATED WORK

This section of related work includes conducted research and analysis of various computer forensic tools. These tools will be categorised by the most frequent used tools by computer forensics professionals.

SANS DFIR – SANS Digital Forensics and Incident Response is a computer forensics distribution that installs all necessary tools on Ubuntu to perform a detailed digital forensic and incident examination. [3] Developed by an international team of forensics experts, the SIFT Workstation is available to the digital forensics and incident response community as a public service.

Sift is a powerful open source tools that are freely available and can match any modern DFIR tool suite. [3] SANS DFIR produce thousands of free content rich resources for the digital forensics community, and these resources keep you up to date with the

latest in research and technology available to help you streamline your investigations. [3]

SANS supply training courses, which are extremely cutting edge and teach you the most up-to-date knowledge of how to detect and fight a criminal investigation. [3]

SIFT Workstation Overview – as mentioned above, the SIFT Workstation is a free open source incident response and forensics tools designed to perform detailed digital forensic examinations in a variety of settings. Rob Lee and his team created and continually update the SIFT Workstation. With over 100,000 downloads to date, the SIFT continues to be the most popular open-source incident-response and digital forensic offering next to commercial source solutions. [4]

FORENSIC TOOLKIT (FTK) – Forensic Toolkit (FTK) is a computer forensics software made by AccessData. This tool scans hard drives looking for various information. For example, it can locate deleted emails and scan a disk for text strings to use them as a password dictionary to crack encryption. [5] FTK uses distributed processing and is the only forensics solution to fully leverage multi-thread computers. FTK uses 100 percent of its hardware resources compared to other forensics tools who waste the potential of modern hardware solutions, this helps FTK investigators find relevant evidence faster. [5] FTK is database driven and is one shared case database. This means all teams use the same data which reduces the cost and complexity of creating multiple data sets. [5]

Some of FTK's capabilities to empower people are their third party integration with Belkasoft. This gives access to nearly 200 mobile parsers. FTK processes and indexes up front so you don't waste time waiting for searches to execute. The easy-to-use GUI provides a faster learning experience. Visualisation technology that displays your data in timelines, pie charts, cluster graphs, geolocation for example. This helps the user get a clearer picture of events. [5]

VOLATILITY FOUNDATION – The Volatility Foundation is an independent 501 non-profit organisation that maintains and promotes open source memory forensics with The Volatility Framework. The Volatility Framework is open source and written in Python. [6]

Volatility first released a version in 2007 and its goal was to research into advanced memory analysis and forensics. This changed when digital investigations had focused on finding the data found in volatile storage (RAM). [6] This provided a cross-platform, modular, and extensible platform to encourage further work into this area of research. [6]

Since that time, Volatility is supported by one of the largest and most active communities in the forensics industry. As a result, research built on top of Volatility has appeared at the top academic conferences and Volatility has been used on some of the most critical investigations of the past decade. It has become an indispensable digital investigation tool relied upon by law enforcement, military, and commercial investigators throughout the world. [7]

WIRESHARK – Wireshark is a free and open source packet analyzer used to capture, analyses, and filter packets. This allows a systems administrator to unveil any potential attacks. [8]

Wireshark is the world's foremost and widely-used network protocol analyzer. It lets you see what's happening on your network at a microscopic level and is the de facto standard across many commercial and non-profit enterprises, government agencies, and educational institutions. [9]

An example of Wireshark is that the tool can be used to filter specific mac addresses, IP addresses, and IP addresses with conditional TCP ports. [9]

AUTOPSY – THE SLEUTH KIT – Autopsy is a digital forensics platform and graphical interface to The Sleuth Kit and other digital forensics tools. It is used by law enforcement, military, and corporate examiners to investigate what happened on a computer. [10]

Autopsy was designed to be intuitive out of the box. It was designed to be an end-to-end platform with modules that come with it out of the box and others that are available from third parties. This digital forensic platform is extensible. It provides Timeline Analysis, advanced graphical event viewing interface. Hash filtering, Flag known bad files and ignore known good. Keyword search, indexed keyword search to find files that mention relevant terms. Data carving, recover deleted files from unallocated space using PhotoRec, and more. [10]

Autopsy runs background tasks in parallel using multiple cores and provides results to you as soon as they are found. It is very fast. Autopsy is also cost effective, it's free. [10]

The Sleuth Kit is an open source file and a library and collection of command line tools that allow you to investigate disk images. The plug-in framework allows you to incorporate additional modules to analyze file contents and build automated systems. [11]

The library can be incorporated into larger digital forensics tools and the command line tools can be directly used to find evidence. [11]

XPLICO – Xplico is a network forensics analysis tool, which is a software that reconstructs the contents of acquisitions performed with a packet sniffer. [12] Xplico is installed in the major distributions of digital forensics and penetration testing, such as Kali Linux, BackTrack, Security Onion, CERT-ToolKit, and more. Xplico allows concurrent access by multiple users, any user can manage one or more cases. Web Interface – The UI is a web user interface and its backend DB can be SQLite, MySQL or PostgreSQL. Xplico can also be used as a cloud network forensic analysis tool. [12]

Xpico isn't a network protocol analyzer. Xplico is an open source network forensic analysis tool. Its goal is to extract an internet traffic capture the applications data contained. [13] Some of Xplico key features are supported protocols such as HTTP, SIP, IMAP, TCP, UDP, IPv6 and more. Real time elaboration, IPv4 and IPv6 support, there is no size limit on data entry or the number of files entrance (only size limit is HD size). [13]

X-WAYS – An advanced computer examination and data recovery software. X-Ways Forensics is a powerful integrated computer forensics environment with numerous forensic features, rendering it a powerful disk analysis tool. X-Ways is a forensic edition of WinHex. [14] X-Ways is an advanced work environment for computer forensic examiners. It is based on the WinHex and disk editor and part of an efficient workflow model where computer forensic examiners share data and collaborate with investigators that use X-Ways investigator. [14]

Some of X-Ways features are disk editor, file editor, RAM editor. Other features such as data recovery, hard drive cleansing/disk wiping, unused space capturing, and disk catalog capturing. [14]

OXYGEN FORENSICS – Oxygen forensic detective is an advanced software to extract data from multiple sources. [15] Oxygen can be used to find passwords to encrypted backups and images, bypass screen lock

on popular Android OS devices, acquire location history and media files from drones. Oxygen detective features can also extract data from cloud services such as iCloud, Google, Microsoft, etc. The software is also capable of acquiring data from IoT devices and smartwatches and it offers import and analysis of call data records. [15]

Oxygen forensics was founded in 2000 as a PC-to-Mobile communication software company. [16] The team of mobile device experts have become unmatched in understanding mobile device communication protocols. Therefore, with all that knowledge, Oxygen created innovative techniques in Oxygen Forensic Detective which allows users to access much more critical information than competing forensic analysis tools. [16]

“We offer the most advanced forensic data examination tools for mobile and IoT devices, smartwatches, cloud services and drones. Our company delivers the universal forensic solution covering the widest range of mobile devices running iOS, Android, Windows Phone, BlackBerry and many others.” – Oxygen Forensics. [16]

CAINE – Computer Aided Investigative Environment. CAINE is an Italian GNU/Linux live distribution created as a digital forensics project. [17] CAINE offers a complete forensic environment that is organized to integrate existing software tools as software modules and to provide a friendly graphical interface. [17]

CAINE have three main design objectives, the first being an interoperable environment that supports the digital investigator during the four phases of the digital investigation. The second is a user-friendly graphical interface, and finally user-friendly tools. [17] CAINE is also an open source tool and everyone can take on the legacy of the previous developer.

CROWD STRIKE – CrowdStrike Falcon, is the CrowdStrike platform purpose-built to stop breaches via a unified set of cloud-delivered technologies that prevent all types of attacks – including malware and much more. [18]

CrowdStrike Falcon responds to attackers using ‘zero days’ and hard-to-detect methods such as credential theft and tools that are already part of the victims environment or operating system, such as ‘PowerShell’ by using a powerful yet lightweight solution that unifies next generation antivirus(NGAV), endpoint detection and

response(EDR), managed threat hunting capabilities and security hygiene. All contained in a tiny, single, lightweight sensor that is cloud-managed and delivered. [18]

Some of the detection capabilities CrowdStrike have for known threats are cloud-based antivirus and IOC detection. For unknown and zero-day threats, Falcon apply IOA detection, using machine learning techniques to build predictive models that can detect never-before-seen malicious activities with high accuracy. [18]

Falcon prevent stops known and unknown malware by using an array of complementary methods such as custom blocking, exploit blocking, indicators of attack prevention and as said above, machine learning. [18] Other protection Falcon provide is ransomware and it detects in-memory attacks by watching for suspicious processes and events and activities. [18]

EXIFTOOL – ExifTool is a command line application used as an open source software program for reading, writing, and manipulating image, audio, video and PDF metadata. ExifTool is platform independent and available as both Perl library and command line application. It is fast, powerful and supports a large range of file formats. [19] An example of ExifTool is it can be used for analysing the static properties of suspicious files in a host-based forensic investigation. [19]

ExifTool has many features like supporting a large number of different file formats, reads and writes EXIF, GPS, IPTC, XMP, JFIF and more. This tool Geotags images from GPS track log files, shifts date/time values to fix timestamps in images, creates text output file for each image file, and more. [20]

DSI USB WRITE BLOCKER – DSI USB Write Blocker is a software based write blocker that prevents write access to USB devices. This becomes important to an investigation when trying to prevent modifying the metadata or timestamps and invalidating the evidence. [19]

USB stick is the common device used by incident response team to collect and investigate any attack. How DSI USB Write Blocker works is the USB will include a number of tools required to run and analyse system artifact. It may also contain logs and reports that the user need to edit when they will connect back to their system. Once logs and metadata collected, the

user should make sure that there is no way to modify or change collected information. If you want to lock the USB device you can use DSI USB Blocker Utility. [21] This will help into converting the USB stick into read only mode so no change or modifications are allowed. [21]

PRO DISCOVER FORENSIC – Pro Discover Forensic is a powerful computer security tool that enables computer professionals to locate all of the data on a computer disk and at the same time protect evidence and create quality evidentiary reports for use in legal proceedings. [22] It is not possible to hide data from a Pro Discover Forensic because it reads the disk at the sector level. This tool can recover deleted files, access windows alternate data streams, examine slack space and dynamically allows a preview and image capture of the hardware protected area (HPA) of the disk utilizing its own pioneered technology. [22]

Key features of Pro Discover Forensic include creating a bit-stream copy of the disk to be analysed, including hidden HPA, to keep original evidence safe. A preview of all files, even if hidden or deleted, without altering data on disk, including metadata. [22] Pro Discover Forensic also feature examination and cross reference data at the file or cluster level to ensure nothing is hidden, and it utilizes Perl scripts to automate investigation tasks. [22]

ENCASE – EnCase is an open source forensics software and its use has made it one of the de-facto standard in forensics. [23] This software is commonly used by law enforcement and you have to purchase it. EnCase is available as a demo upon request but it is not for free.

This software is a windows only tool and is primarily used in collecting information from a computer system by employing checksums to aid in detect tampering to evidences. It can collect information from different types of devices and produce concise forensic reports. [23]

HELIX3 PRO – Helix3 Pro is a unique tool customised for computer forensics. This software was created to avoid touching the host computer in any way and it is forensically sound. [24] This tool works on Linux operating systems, MAC OS X and Windows. Helix3 Pro is a commercial tool, therefore it is not for free. There is a free version of this tool but it's outdated and not supported anymore. [24]

This tool focuses on forensics tools and incident response techniques. It is designed to be used by individuals who have an understanding of these techniques. Users can create forensic images of all internal devices and search for specific file types like document files, graphics files, etc. [24]

MALTEGO – Maltego is developed by Patreva and is a tool used for open source forensics and intelligence. [25] This tool is used to provide a library of transforms for the discovery of data from different open sources and visualise that data into a graph format which is suitable for data mining and link analysis. Maltego works on Windows, Linux and MAC operating systems.

This is a hacking tool which has two types of reconnaissance options, personal and infrastructural. Personal reconnaissance includes personal information such as email addresses, phone numbers, social networking profiles, etc. Infrastructural reconnaissance deals with the domains and covering DNS information such as name servers and mail exchangers. [25]

The prime focus of Maltego is to analyse real world relationships between data that is accessible through the internet which includes footprinting internet infrastructure and gathering data about people and organisations owning it. [25]

III. DISCUSSION OF THE CASE STUDY INVESTIGATION

Johns Investigation Document Steps -

A detective in a professional investigation service named John was given the task to investigate the items in the terrorist brief case. John is an incident handler, not a forensic investigator because he is only permitted to find evidence off a laptop and not do procedures such as finger prints of the terrorist or analyse the crime scene. John is to only analyse the evidence provided by Mr. Mark Wales and retrieve decrypted information off the terrorist's laptop. John was given a laptop bag along with the Dell Laptop which the terrorist had at the time of the confrontation with the police, photographs of the crime scene, and fingerprints that matched the terrorist. The computer was in standby mode, which helps conserve power when a computer is not in use without having to sacrifice the time it would take to turn the computer on and off. John took the photographs of the computer screen using his

Cannon Digital camera for evidence, a very high performance camera which features up to 24 megapixels resolution and 5 frames per second of continuous shooting. [26] John noticed that the operating system of the laptop was Microsoft Windows XP Professional Service Pack 2.

The forensic methods John would have used before preparing a chain-of-custody document and stored the original hard disk in a secure location would be to take another image/copy of the original disk. It is always best practice to take another image/copy because it helps with the integrity of the data. To maintain the integrity of the contents on the recovered disks, John took an MD5 hash and kept note of it. Taking an MD5 hash before and after the analysis will show that John hasn't manipulated the data in any way.

The chain of custody below includes information about where the recovered hard disk has been and who has had possession of the disk throughout the analysis of the investigation.

Chain of Custody

Date/Time	From:	To:	Location(s)
Date: 14/07/18	1568	4582	Heathrow Police Department
Time: 14:00pm	<i>M. Wales</i>	<i>John</i>	Analysis Room
Date: 20/07/18	4582	1568	Analysis Room
Time: 9:00am	<i>John</i>	<i>M. Wales</i>	Heathrow Police Department

John was asked to retrieve any Microsoft Word, Excel, PDF, Images files (jpeg, gif, bmp, tiff), video files (avi, mpeg, dat, mov), and audio files (mp3, wav, and rm) related to the case. Microsoft Outlook contacts, email messages, messenger chat history, and cache files were also required. John would retrieve these files by using the Forensic ToolKit (FTK). FTK is a computer software made by AccessData and it scans hard drives looking for various information. [5] This tool can locate deleted emails and scan a disk for text strings to use the, as a password dictionary to crack encryption. In this case, John will be using FTK to retrieve emails, images files, video files, and so on.

John Investigation Report -

First off, John added the evidence disks to FTK, and used the tool 'Verify Image Integrity' on the disks to check the MD5 hash hasn't changed so that the data hasn't been manipulated in any way. John then proceeded with an index search in order to refine his search results. Hit means the term repeated on any instances of file. As seen in figure 3, file shows the number of files with Excel association either name, content or extension. See figure 1 and 2 and 3. Note – All figures of images and videos have been retrieved by John from FTK and screen captured.

After index searching the requirements such as Excel, MS Word, and video files for example within the hard disks, John noticed a lot of related terrorist information, photos and videos. John discovered passport photos, 9/11 bombings, motivational speeches by leaders of various terrorist outfits, a 30-minute video of Heathrow International Airport and Mason International Airport at Fiji, information on passport arrest history and hundreds of information relating to a terrorist attack. See figure 4, 5 and 6.

John noted the incriminating list of videos and photos found in the evidence, including videos taken in a hotel room along with 6 other suspects, personal videos which showed the terrorist spending some light moments with his wife and two small kids, and also a video showing terrorists practicing at a terror camp. John documented all these suspicious images and videos for the chief of Heathrow Police Department and raised them as red flags for active terrorism. As seen in figure 6 and 8, there were photographs of Heathrow International Airport and Mason International Airport at Fiji. The terrorists had taken pictures of these two airports in detail, which John confirmed that this was a high intention of the terrorist group to which he was associated. Logos of a particular terrorist group were discovered and confirmed the terrorists association. There were documents related to 'How to make a chemical bomb', 'How to be a suicide bomber', 'How to prepare for Jihad' along with other materials which were also recovered. Excel sheets that John found had bank account names and the details of inflow of funds to the accounts. Inside the laptop bag there was a few documents and immigration visas which had made clear of the terrorists links with other terrorist organisations.

John finalised his document of findings and reported it back to Mark in the Heathrow Police Department. One particular document that caught Mark's eye was

'How to make a chemical bomb'. Mark then read the document and found that the article contained instructions from few people on how to spread terror at Mason International Airport, Fiji. Mark was more than assured about the involvement of how the accused in the crime.

John used two different types of software to get the list of contacts within the terrorists MS Outlook. These contact names were matched to the ones found in the earlier documents. The first software he used was Autopsy. This tool features timeline analysis that displays system events in a graphical interface to help identify activity. It has keyword search (which is important to this case) where text extraction and index searched modules enable you to find files that mention specific terms and regular expression patterns (John used specific terms such as passports, JPEG, rm videos, and so on). It also has other features which come in handy with this investigation like hash set filtering, file type detection, EXIF and most importantly registry analysis, where the software uses RegRipper to identify recently accessed documents and USB devices. [27]

FTK was the next software John used to get the list of contacts within the terrorists MS Outlook. John has already featured what FTK is capable of in 'Johns Investigation Documented Steps' above. Here are the advantages and disadvantages of using FTK for this investigation. [28]

Advantages:

- Can analyse data from several sources, including image files from other vendors
- FTK produces a case log file – supports options and advanced searching techniques
- Simple users' interface
- Fast searching
- EFS decryption
- Reporting
- Password dictionary creation
- E-mail display

Disadvantages:

- No progress bar
- No multi-tasking
- 2 million file limit
- No scripting support
- No PSD support and no AVI support

Figure 1 – ‘Verify Image Integrity’ to check the MD5 hash on every disk

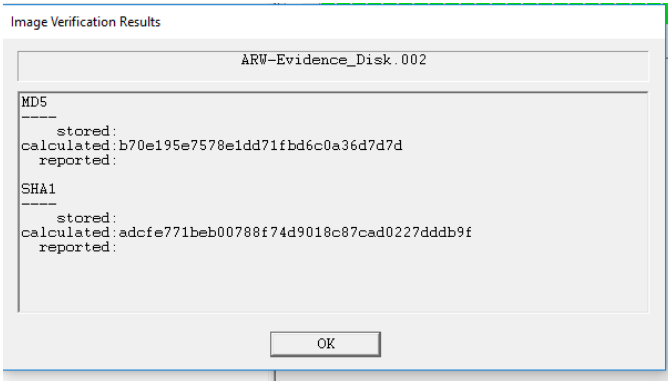


Figure 2 – Adding and analysing the evidence disks on FTK

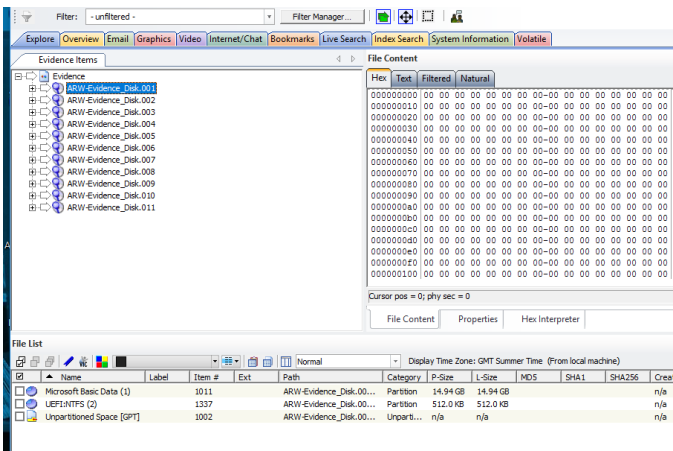


Figure 3 – Index search and hits on FTK software

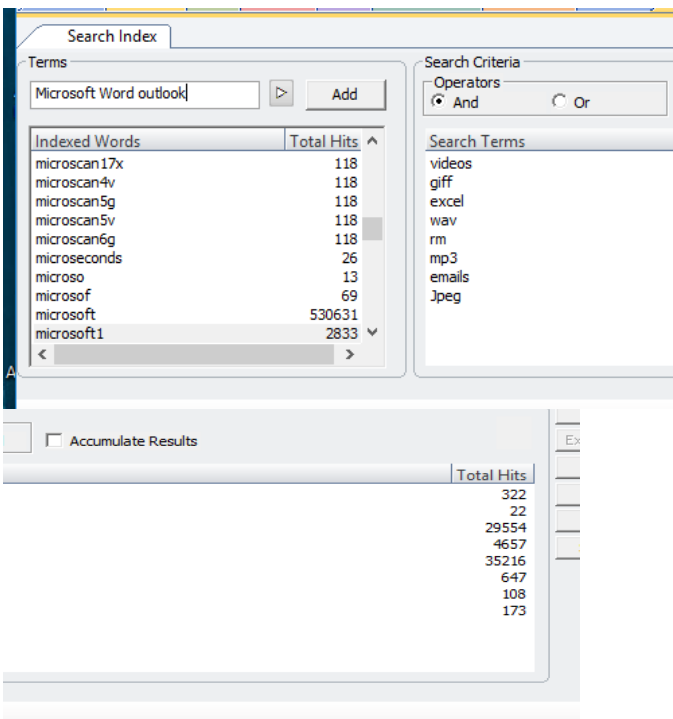


Figure 4 – Fake passport found – more leads to possible terrorist attack



Figure 5 – Information on passport arrest history – ‘On 8 June 1968, James Earl Ray, the man convicted of 4 April 1968 assassination of Martin Luther King Jr., was captured and arrested at Heathrow Airport International while attempting to leave the United Kingdom on a false Canadian passport.’

Terrorism and security incidents[[edit](#)]

- On 8 June 1968, James Earl Ray, the man convicted of 4 April 1968 assassination of Martin Luther King, Jr., was captured and arrested at Heathrow Airport while attempting to leave the United Kingdom on a false Canadian passport.^[12]

Figure 6 – Image of Heathrow International Airport

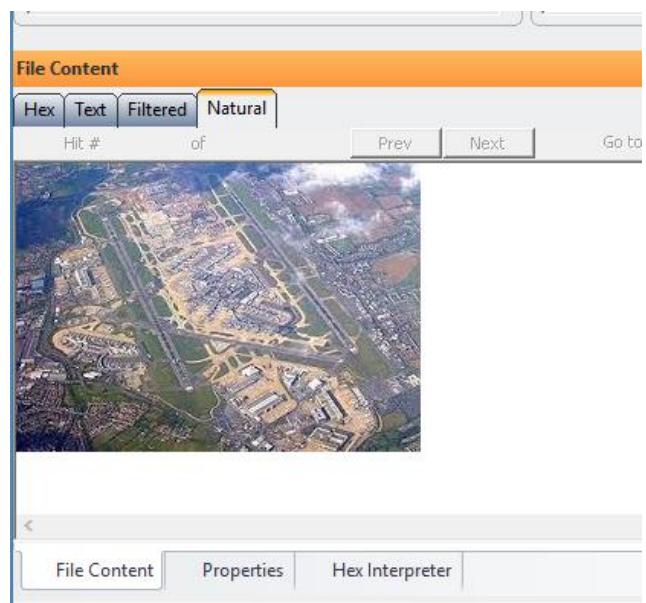


Figure 7 – Videos on speeches on terrorism, and Barack Obama speech on strategy against ISIS

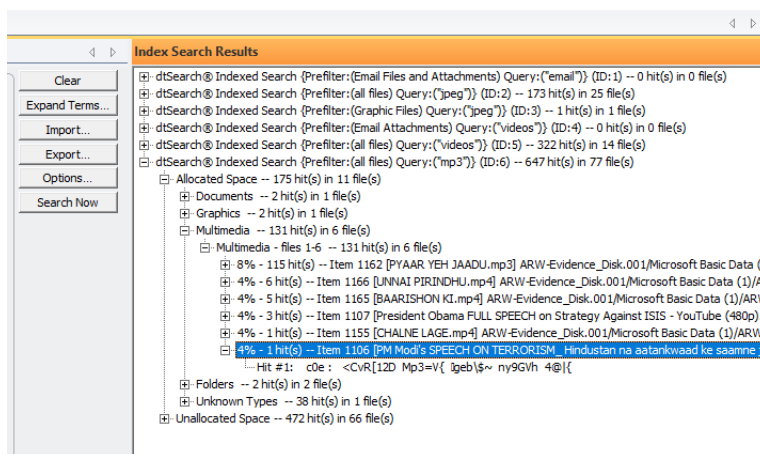


Figure 8 – Image of Mason International Airport



IV. RESULTS/FINDINGS

Throughout the investigation report, results retrieved from Investigator John have shown that there is a major possibility, in fact most certainly a terrorist group out in London trying to cause attacks on Heathrow International Airport. Findings such as fake passports, pictures of Heathrow International Airport and Mason International Airport in Fiji, President Obamas speech on strategies against ISIS, bank transactions from different countries, and videos of a terrorist camp prove that the terrorist is guilty. This evidence retrieved by John will now be processed by Heathrow Police Department and it is left in their hands and the hands of the law.

V. CONCLUSION

To conclude, task 1 was a very interesting to research and write about. Learning about the top 20 and most professional computer forensic tools in the world has given a much bigger picture into how extensive and considerable cybersecurity is to this day. Cyberattacks is one of the biggest and most dangerous threats to anyone and anything today, and cybersecurity is one of the fastest growing industries in the world, it's a pleasure to see how many people are attacking this problem and how much research and hard work goes into creating these computer forensic tools to help stop these crimes. These computer forensic tools are also used every day in police departments, investigator operations and the military. This states how important forensics tools are by getting used every day to keep the country safe.

If research on computer forensic tools was to be done again, a lot more research and time would go into explaining how these tools worked and how they are in use with the police and military. It is also recommended that more time is needed to research these tools because they're so interesting to learn about and most of them hand out free demos for the researcher to play around with and have a go.

To conclude on task 2, it was also very fun and interesting to finally use one of the computer forensic tools researched in the report. FTK is one of the simplest forensic tools to use because of its fast searching, EFS decryption, reporting, and so on. Analysing the evidence disk images was a good task to complete because whilst completing it, you learn a lot on the go. This was one of them tasks where

you learn more by doing the practical than by researching all about it.

If this task was to be completed again, the results and findings log would be in a lot more depth. An Excel spreadsheet could have been created with an evidence summary. This would have made it a lot easier for the reader to see a breakdown of the evidence retrieved off the Forensic Toolkit (FTK).

VI. REFERENCES

- [1] Introduction to Computer Forensics, varsonun, June 2018, Available:
<https://www.cybrary.it/0p3n/introduction-to-computer-forensics/>
- [2] Top Computer Forensic Tools, InfoSec, February 2019, Available:
<https://resources.infosecinstitute.com/computer-forensics-tools/#gref>
- [3] SANSDFIR, 2019, Available:
<https://digital-forensics.sans.org/>
- [4] SIFT Workstation, 2019, Available:
<https://digital-forensics.sans.org/community/downloads>
- [5] Forensics Toolkit, AccessData, 2019, Available:
<https://accessdata.com/products-services/forensic-toolkit-ftk>
- [6] Volatility Foundation, 2018, Available:
<https://www.volatilityfoundation.org/>
- [7] About Volatility, Volatility Foundation, 2018, Available:
<https://www.volatilityfoundation.org/about>
- [8] Wireshark, InfoSec Resources, 2019, Available:
<https://resources.infosecinstitute.com/wireshark-open-source-forensic-tool/#gref>
- [9] Wireshark, 2019, Available:
<https://www.wireshark.org/>
- [10] Autopsy, The Sleuth Kit, Brain Carrier, 2019, Available:
<https://www.sleuthkit.org/autopsy/>
- [11] The Sleuth Kit, Brain Carrier, 2019, Available:
<https://www.sleuthkit.org/sleuthkit/>
- [12] Xplico, Gianluca Costa & Andrea De Franceschi, 2018, Available:
<https://www.xplico.org/>
- [13] About Xplico, Gianluca Costa & Andrea De Franceschi, 2018, Available:
<https://www.xplico.org/about>
- [14] X-ways Forensics, X-ways software technology AG, Available:
<https://www.x-ways.net/winhex/forensics.html>
- [15] Oxygen Forensics, OxygenForensics.com, Available:
<https://www.oxygen-forensic.com/en/>
- [16] Oxygen Forensics, the company, Available:
<https://www.oxygen-forensic.com/en/company>
- [17] CAINE, Computer Aided Investigation Environment, 2019, Available:
<https://www.caine-live.net/>
- [18] CrowdStrike, 2019, Available:
<https://www.crowdstrike.com/endpoint-security-products/crowdstrike-falcon-faq/>
- [19] ExifTool, TechTalk, July 2018, Available:
<https://techtalk.gfi.com/top-20-free-digital-forensic-investigation-tools-for-sysadmins/>
- [20] ExifTool, Forum, Phil Harvey, 2019, Available:
<https://www.sno.phy.queensu.ca/~phil/exiftool/>
- [21] DSi USB Write Blocker, SecTechno, 2018, Available:
<http://www.sectechno.com/usb-write-blocker/>
- [22] ProDiscover Forensic, Infosec, 2019, Available:
<https://resources.infosecinstitute.com/7-best-computer-forensics-tools/#gref>
- [23] EnCase Forensic Tool, 2018, Available:
<https://www.guidancesoftware.com/encase-forensic>
- [24] Helix3 Pro, e-fence, 2014, Available:
<http://www.e-fense.com/helix3pro.php>
- [25] Maltego, Concise AC, 2019, Available:
<https://www.concise-courses.com/hacking-tools/forensics/>
- [26] Canon Camera Features, Specification and features, Canon, 2019, Available:
<https://www.canon.co.uk/cameras/eos-200d/specifications/>
- [27] The Sleuth Kit features, Autopsy, 2019, Brian Carrier, Available:
<https://www.sleuthkit.org/autopsy/features.php>

[28] Forensic Toolkit (FTK), amazonpaws.com,
Available:
[https://ad-
pdf.s3.amazonaws.com/ftk/FTK%206.1/FTK_UG.p
df](https://ad-pdf.s3.amazonaws.com/ftk/FTK%206.1/FTK_UG.pdf)