[9144965]

Abstract

This is a digital forensic report on suspected terrorist John Jones computer to check for illegal activity

[Computer Forensics]

[Forensic Report on John Jones]



Table of contents

[Figures 1](#_Toc54799554)

[Forensic Report on John Jones 2](#_Toc54799555)

[Introduction 2](#_Toc54799556)

[Investigation 3](#_Toc54799557)

[Conclusion 19](#_Toc54799558)

[References 19](#_Toc54799559)

[Appendix 1: Photograps of the crimescene and computer 20](#_Toc54799560)

[Appendix 2: Chain of Custody Forms 20](#_Toc54799561)

[Appendix 3: Shows imaging and checksums of the suspects SSD. 24](#_Toc54799562)

[Appendix 4: Shows the suspects files and cloud storage accounts 25](#_Toc54799563)

[Appendix 5: Casenotes 37](#_Toc54799564)

[Appendix 6: Presentation 38](#_Toc54799565)

# Figures

[Figure 1: DFRWS Investigation Model 3](#_Toc54799541)

[Figure 2: The 4 ACPO Principles of Digital Evidence. 3](#_Toc54799542)

[Figure 3: A screenshot showing SAFE Block, blocking write ability to the suspects SSD. 4](#_Toc54799543)

[Figure 4: A screenshot of the FTK Imager Log.txt showing the results of John Jones SSD being imaged along with the MD5 and SHA1 checksums. 5](#_Toc54799544)

[Figure 5: Shows the image loaded into Autopsy and confirms the checksum is the same. 6](#_Toc54799545)

[Figure 6: A screenshot showing the users registry. It shows the windows version, current build and the install date. 7](#_Toc54799546)

[Figure 7: Shows the contents of 'Planning.docx' 10](#_Toc54799547)

[Figure 8: A snippet of 'The Cloudy Manifesto'. 11](#_Toc54799548)

[Figure 9: Shows the contents of 'Brother Chat.gdoc' 11](#_Toc54799549)

[Figure 10: Shows part of the contents of 000044.ldb. 12](#_Toc54799550)

[Figure 11: Shows a portion of the suspects browsing history. 15](#_Toc54799551)

[Figure 12: Suspect owns 2 SDCZ80 Flash drives 16](#_Toc54799552)

[Figure 13: Suspects accounts. 16](#_Toc54799553)

# Forensic Report on John Jones

Case No: 0001/2020

Date of investigation: 24/10/2020

Investigator: Steven Lovell

On behalf of: Scarborough Police

# Introduction

This is a digital forensic report on suspected terrorist John Jones computer to check for illegal activity. John Jones was reported to the police by his brother Jimmy Jones. Worried his brother was becoming radicalised after sharing files on Dropbox and fearing he may carry out a terrorist attack, Jimmy Jones reported his brother to the police. Following the Association of Chief Police Officers (ACPO) guidelines for handling forensic evidence (ACPO, 2012) and using the Digital Forensic Research Workshop (DFRWS) process (Palmer, 2001) to investigate the evidence, this report aims to answer the following questions. Who is the suspect, what were they planning, when was the attack planned for, where was the attack going to take place and how the attack was going to happen.

Figure 1: DFRWS Investigation Model

Graphical user interface, text, application, letter, email

Description automatically generated

Figure 2: The 4 ACPO Principles of Digital Evidence.

# Investigation

**Identification**

The suspect was reported to the police by his brother after sharing suspicious files on Dropbox. John Jones was arrested by the police and a court order was issued allowing the seizure of Mr Jones computer. Once an appointment was made with the aid of the police Mr Jones residence was searched. During the search a computer was found and the Solid-State Drive (SSD) storage device was removed.

**Preservation and Collection**

The tools used for this report are:

* Forensic CaseNotes v1.2.2010.6: Used to create secure notes that are timestamped and immutable.
* SAFE Block 1.3: Used to ensure that no data can be written to the suspects SSD.
* FTK Imager 4.3.1.1: A tool used to create an image of the suspects data.
* Autopsy 4.16.0: A digital forensics tool, used to analyse the data.

The first ACPO guideline states, when securing digital evidence, it is vital to make no changes to the users’ data. In order to accomplish this the suspects SSD is removed from the computer and transported to a secure forensics’ laboratory. For this case, Coventry University’s forensic laboratory was used. Once the data has been securely transported, SAFE Block 1.3 is used to make sure the suspects data is not accidently modified.

Graphical user interface, text, application, email

Description automatically generated

Figure 3: A screenshot showing SAFE Block, blocking write ability to the suspects SSD.

At this point FTK Imager 4.3.1.1 a tool designed to image the suspects SSD is used and a checksum is created of the image. See figure 4 for the log.

Text

Description automatically generated

Figure 4: A screenshot of the FTK Imager Log.txt showing the results of John Jones SSD being imaged along with the MD5 and SHA1 checksums.

This primary image is then copied. The original SSD is now removed from the laboratory and placed in a secure evidence locker and the primary image is also securely stored away. From this point on only a secondary copy will be analysed. This make sure that no data is accidently modified and ensures the protection of the original SSD. The folo

|  |  |
| --- | --- |
| Device | SSD |
| Make | Samsung |
| Model | 850 Evo Pro 512gb |
| Serial Number | S250NSAG505708H |
| Description | Suspects main storage device. |

Table 1: The suspects SSD make, model and serial number.

Table

Description automatically generated

Figure 5: Shows the image loaded into Autopsy and confirms the checksum is the same.

**Examination and Analysis**

The image was loaded into Autopsy which enabled forensic examination of the suspects data. The first objective was to get the suspects username and information on the operating system from the registry.

|  |  |
| --- | --- |
| User Account | Jcloudy |
| Operating System | Windows 10 Education |
| Windows Build | 16299 |
| Device Name | DESKTOP-PM6C56D |
| Install Date | 27/03/2018 @ 12:13pm |

Table 2: Shows the suspects username, operating system details and the install date.

Graphical user interface, application

Description automatically generated

Figure 6: A screenshot showing the users registry. It shows the windows version, current build and the install date.

The suspects brother mentioned a Dropbox file to the police. This made searching for cloud storage a high priority. The suspect had created accounts on four cloud storage platforms.

|  |  |
| --- | --- |
| **Cloud Storage Platform** | **Username** |
| Microsoft One Drive | jimcloudy@outlook.com |
| Google Drive | jimcloudy1@gmail.com |
| Dropbox | jimcloudy1@gmail.com |
| Amazon Web Service | jimcloudy1@gmail.com |

Table 3: Shows the suspects username across multiple cloud storage platforms.

The suspect John Jones was using the pseudonym of ‘Jim Cloudy’ as a counter measure to avoid detection. Across the four platforms there were four suspicious files as well as numerous images about gun control, these could also be found on the suspects desktop including a fifth suspicious file named ‘Cloudy thoughts (4apr).docx’. The suspicious files were identical across the cloud platforms and shared the same checksum.

**Suspicious files:**

* ***AIRPORT INFORMATION.docx***
  + Date Created: 30/03/2018
  + Shows the suspect planning a trip to Indonesia.
  + Comparing Ronald Reagan Washington National Airport to Washington Dulles International Airport.
  + The time to the airport from the Fairfax County Democratic Committee.
* ***Cloudy thoughts (4apr).docx:***
  + Date Created: 05/04/2018
  + Discusses a plan and being ‘killed at the site’. Mentions brother Paul which confirms the information received from the police.
* ***Operation 2nd Hand Smoke.pptx***
  + Date Created: 04/04/2018
  + A PowerPoint presentation the slides show:
    1. The title ‘OPERATION 2ND HAND SMOKE’.
    2. A town hall meeting event at the Whitfield library with senators Kaine and Warner about gun violence on 7/4/2018.
    3. A picture of Whitfield Library circled in red.
    4. A map of the area around Whitfield Library with multiple routes drawn on.
    5. A travel route from Whitfield Library to Dulles International Airport.
    6. Airplane ticket from Washington – Seoul and Seoul – Bali Indonesia.
    7. Shows the price of lodging at the ‘Sea Breeze Candidasa’ in Indonesia.
* ***Planning.docx*** 
  + Date Created: 30/03/2018
  + Shows the suspect planning to target a gun free zone near an airport with a Kel-Tec SUB 2000 with 1000 rounds of 9mm ammunition.
  + Suspect planned to escape to Indonesia or Vietnam two countries without extradition.
  + Suspect planned to upload a manifesto to the cloud and release it once he had escaped.

A picture containing text

Description automatically generated

Figure 7: Shows the contents of 'Planning.docx'

* ***The Cloudy Manifesto.docx***
  + Date Created: 02/04/2018
  + Ramblings about gun control filled with memes, talk of being a lonewolf and launching an attack on a gun free zone.

Graphical user interface, text, application, email

Description automatically generated

Figure 8: A snippet of 'The Cloudy Manifesto'.

Another file located on Google drive was called ‘Brother Chat.gdoc’. The suspect was using Google docs to chat with his brother to avoid being noticed by the police. The ‘Brother Chat.gdoc’ file contained a dead url.

Graphical user interface, text, application, email

Description automatically generated

Figure 9: Shows the contents of 'Brother Chat.gdoc'

By using Autopsy to search for the ‘doc\_id’ this led to ‘000044.ldb’ an indexed file of the Google doc. This file shows the suspect being paranoid and his brother being worried for him.

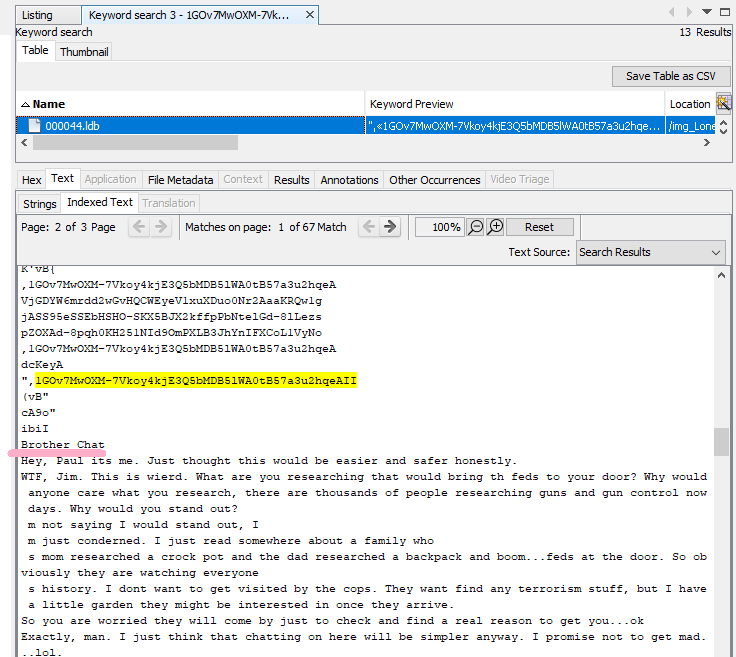


Figure 10: Shows part of the contents of 000044.ldb.

The next objective was to search the suspects browsing history. This can tell a lot about a person’s habits and mental state.

**28/03/2018**

* The suspect was researching how to upload files to different cloud storage platforms.
* Created Dropbox account
* The suspect was researching firearms.
  + Ruger 10-22 Rifle in .22 calibre
  + Kel-Tec SUB-2000 a folding carbine in 9mm
  + FN P90, a Belgian submachine gun in 5.7, a calibre infamously referred to as ‘cop killer’ by US officials after the 2009 Fort Hood shooting (Cole, Thomas, Ryan, & Esposito, 2009).
* Searching for local shooting ranges

**29/03/2018**

* Created a Google account
* Suspect researching how to buy an illegal firearm.

**30/03/2018**

* Looking for a Nokia 3310 dual sim phone commonly referred to as a ‘burner phone’.
* Searching for a map of gun free zones in Washington D.C.
* Looking for the location of Democratic offices and headquarters in D.C.
* ‘Airports near D.C.’
* ‘Police response times by zip code’
* ‘Which D.C. Airports has fewest delays’.
* Suspect researches ‘lone wolf’.
* Suspect searches ‘how to use google docs as chat’.
* Suspect visits right wing websites
  + The Blaze
  + Breitbart

**31/03/2018**

* Searches for ‘concealable tactical rifles’
* Visits gunbroker.com a marketplace for firearms and looks for a Kel-Tec 2000
* The suspect researches non extradition countries and information on which is cheaper Indonesia or Vietnam.
* Researches airports
* Suspect reads a Guardian article on the government tracking google searches at 21:00
* Suspect searches for ‘do the cops track web searches’ at 21:03 and goes quiet for 2 days.

**03/04/2018**

* Suspect looks for planes from Dulles to Bali
* Suspect searches for ‘upcoming anti-gun rally near me’.
* Researches cascade library.
  + Note: This is the library used by the senators for their upcoming discussion on gun violence

**04/04/2018**

* Searches for Velcro tear away clothes.
  + Note: This would enable the suspect to disguise themselves in the aftermath of the shooting.

**05/04/2018**

* More research on Bali, including gun control in Bali
* Suspect is researching gun control in the United Kingdom.
* Suspect is trying to create an overseas bank account and how to smuggle cash through customs.

**Table

Description automatically generated**

Figure 11: Shows a portion of the suspects browsing history.

In a forensic analysis of a storage device an investigator can find items that are out of the scope of their investigation. In this case there were 2 SanDisk SDCZ80 flash drives missing. The suspect also had 6 user accounts which should be seized.

**Table

Description automatically generated**

Figure 12: Suspect owns 2 SDCZ80 Flash drives

**Graphical user interface, text, application

Description automatically generated**

Figure 13: Suspects accounts.

**Presentation**

The browser history shows the suspect researching the attack from 28/03/2018 to 05/04/2018. As he becomes more radicalised, he becomes determined to launch an attack on the people he believes are trying to take away his guns.

The documents on the cloud services and the desktop show in detail how the suspect planned to launch the attack. From the target; a town hall discussion on gun violence, the gun; a Kel-Tec SUB 2000 with 1000 rounds of 9mm, to the suspects escape to Bali and the release of his manifesto. Each file tells a story and with metadata such as creation date helps to build a complete timeline. Showing when the suspect researched what part of the plan and when the suspect created his manifesto.

**Decision**

Two previous cases showing precedent for preparing mass killings are Kyle Davies and Mohiussunnath Chowdhury.

Mohiussunnath Chowdhury planned to launch a terrorist attack on the pride parade in London. He was charged under 2(1) of the terrorism act 2006 for publishing documents relating to terrorism as well as 5 (1) (a) of the Terrorism Act 2006 for preparing a terrorist attack (CPS, 2020).

Kyle Davies was planning a mass shooting and attempted to buy guns and ammo from the USA. He was charged under Section 1(1) of the Criminal Attempts Act 1981 for attempting to buy a gun and ammunition with the intent of committing a mass shooting (CPS, 2019).

The documents ‘Planning.docx’, ‘The Cloudy Manifesto.docx, and ‘Operation 2nd Hand Smoke.pptx’ along with the suspects browsing history show clear intent to buy a gun and launch a terrorist attack.

**Section 1(1) of the Criminal Attempts Act 1981 states:**

*“If, with intent to commit an offence to which this section applies, a person does an act which is more than merely preparatory to the commission of the offence, he is guilty of attempting to commit the offence.“*

The file ‘Planning.docx’ shows the suspects intent to buy a gun and ammo, this allows the suspect to be charged with conspiracy to buy a weapon and conspiracy to buy ammunition with the aim of committing murder.

**Section 5 (1) (a) of the Terrorism Act 2006 states:**

**Preparation of terrorist acts**

1. A person commits an offence if, with the intention of—
   1. committing acts of terrorism, or
   2. assisting another to commit such acts, he engages in any conduct in preparation for giving effect to his intention.

The files ‘Planning.docx’, ‘The Cloudy Manifesto.docx, and ‘Operation 2nd Hand Smoke.pptx’ show clear intent to launch a terrorist attack. This allows the suspect to be charged with an act of terrorism.

**Section 2(1) of the terrorism act 2006 states:**

**Dissemination of terrorist publications**

1. A person commits an offence if he engages in conduct falling within subsection (2) and, at the time he does so—
   1. he intends an effect of his conduct to be a direct or indirect encouragement or other inducement to the commission, preparation or instigation of acts of terrorism;

‘The Cloudy Manifesto.docx’ is a direct call to arms with the intent of starting a revolution. This would allow the suspect to be charged with disseminating terrorist materials.

**Professional Issues**

During the investigation ACPO principles 1,3 and 4 were used. No data was modified during the investigation and an audit log was created, this satisfies ACPO principles 1 and 3. There was no need to use principle 2, due to the creation of the primary backup copy. The author takes full responsibility for this report and all evidence within meets the requirements suitable for the courts, thus satisfying ACPO principle 4 (ACPO, 2012).

The forensic methodology created by DFRWS proved to be an effective method for gathering the evidence and ensuring its provenance will stand up in a court of law.

# Conclusion

In conclusion this report shows the principles and methodology used to catalogue the suspects attempt to launch a terrorist attack. Every step of the way, each piece of evidence has been catalogued and a chain of custody created. The checksums match between the original SSD and the copies showing no malfeasance has taken place, allowing the report to stand up to scrutiny. The report also recommends the suspect be charged with breaking both Section 1 of the Criminal Attempts Act 1981 and sections 2 and 5 of the Terrorism Act 2006.

# References

*ACPO*. (2012). Retrieved 10 23, 2020, from Association of Chief Police Officers: https://www.cps.gov.uk/legal/assets/uploads/files/ACPO\_guidelines\_computer\_evidence%5b1%5d.pdf

Cole, M., Thomas, P., Ryan, J., & Esposito, R. (2009, November 6). *ABC News*. Retrieved from ABC News Go: https://abcnews.go.com/Blotter/cop-killer-gun-thought-ft-hood-shooting/story?id=9019521

CPS. (2019, 9 13). *Teenager jailed for 19 years after researching mass shooting: CPS*. Retrieved from Crown Prosecution Service: https://www.cps.gov.uk/south-west/news/teenager-jailed-19-years-after-researching-mass-shooting

CPS. (2020, 7 9). *Terrorist given life for Pride attack plot: CPS*. Retrieved from Crown Prosecution Service: https://www.cps.gov.uk/cps/news/terrorist-given-life-pride-attack-plot

Palmer, G. (2001, August 7). *Papers & Presentations: DFRWS*. Retrieved from Digitalk Forensics Reserarch Workshop: https://dfrws.org/wp-content/uploads/2019/06/2001\_USA\_a\_road\_map\_for\_digital\_forensic\_research.pdf

Terrorism Act 2006

Criminal Attempts Act 1981

# Appendix 1: Photograps of the crimescene and computer

|  |  |
| --- | --- |
| Image | Description |
| A room filled with furniture and a table  Description automatically generated | A picture of the suspects computer and room before entry |
|  | A picture of the suspects computer, it also shows the entry to the room |

# Appendix 2: Chain of Custody Forms

|  |  |
| --- | --- |
| Image | Description |
| Table  Description automatically generated | Chain of custody form page 1 |
| Table, letter  Description automatically generated | Chain of custody form page 2 |
| Table  Description automatically generated | Chain of custody form page 3 |

# Appendix 3: Shows imaging and checksums of the suspects SSD.

|  |  |
| --- | --- |
| Image | Description |
| Graphical user interface, application, table  Description automatically generated | Shows the primary and secondary images of the suspects SSD |
|  | : Compares the checksum of E01 for both the primary and backup. Note: This is different from the image checksum as that’s a checksum of the entire image and this is only a checksum of the first of 9 files |

# Appendix 4: Shows the suspects files and cloud storage accounts

|  |  |
| --- | --- |
| Image | Description |
| Graphical user interface, application  Description automatically generated | Shows the suspects images on Dropbox |
| Text  Description automatically generated | Shows the upload log of the suspects Amazon Web Service account. |
| Table  Description automatically generated | Shows the Google Drive folder, including the ‘Brother Chat.gdoc’ file. |
| Graphical user interface, table  Description automatically generated | Shows the OneDrive folder with 4 of the suspicious files. |
| Graphical user interface, text, application  Description automatically generated | Shows the MD5 hash for the suspicious files across the cloud platforms. |
| Graphical user interface  Description automatically generated | Shows the dates the suspicious files were created. |
| Text, letter  Description automatically generated | Shows the contents of ’Cloudy Thoughts (4apr).docx’ |
| Graphical user interface, text, application  Description automatically generated | Shows the contents of ‘AIRPORT INFORMATION.docx’. |
| A picture containing text  Description automatically generated | Shows the contents of ‘Planning.docx’ |
| A picture containing graphical user interface, text, application  Description automatically generated | Shows the 7 slides of the ‘Operation 2nd Hand Smoke.pptx” presentation.  1st slide |
| Graphical user interface, text, application, website  Description automatically generated | 2nd Slide showing the target of the attack. |
| A car parked on the side of a building  Description automatically generated | 3rd Slide showing the location of the attack |
| Map  Description automatically generated | 4th Slide showing routes to the target |
| Graphical user interface, application, map  Description automatically generated | 5th Slide showing the suspects escape route to the airport |
| Graphical user interface, application  Description automatically generated | 6th Slide showing the suspects flight plan |
| Graphical user interface, application  Description automatically generated | 7th Slide showing the suspects planned lodging |
| Graphical user interface, text  Description automatically generated | ‘The Cloudy Manifesto.docx’ in its entirety.  Page 1 |
| Graphical user interface  Description automatically generated | Page2 |
| Text  Description automatically generated | Page 3 |
| Text  Description automatically generated | Page 4 |
| A picture containing text  Description automatically generated | Page 5 |
| A picture containing cat, sitting  Description automatically generated | Page 6 |
| Text, letter  Description automatically generated | Page 7 |

# Appendix 5: Casenotes

|  |  |
| --- | --- |
| Image | Description |
| Graphical user interface, text, email  Description automatically generated | Forensic Casenotes |

# Appendix 6: Presentation

<https://livecoventryac-my.sharepoint.com/:p:/g/personal/lovells3_cuscuni_coventry_ac_uk/ETWxxcp_90lCk_bClrpeALgBduJZXsUPcjPz4wXuv0Po-w?e=XoxWwr>