A logo for a university

Description automatically generated

**Department of Computer and Information Sciences**

**Networks and Cyber Security BSc (Hons)**

**KV5041 : Digital Forensics Incident Response**

**Investigation Report**

**Mohammad Sohaib**

**W23017751**

**Word count** **3696**

Table of Contents

[1.Introduction 2](#_Toc198232908)

[2. Forensic Examination 2](#_Toc198232909)

[1. Tools 2](#_Toc198232910)

[1.1 Exterro FTK Imager 4.7.3.81: 3](#_Toc198232911)

[1.2 Autopsy 4.22.1: 3](#_Toc198232912)

[1.3 Access Data Registry Viewer: 3](#_Toc198232913)

[1.4 Event Log Explorer: 3](#_Toc198232914)

[1.5 Volatility Workbench 2.1 and 3.0: 3](#_Toc198232915)

[1.6 ChromeCacheView (NirSoft): 3](#_Toc198232916)

[2. Evidence 3](#_Toc198232917)

[2.1 Planning.docx: 4](#_Toc198232918)

[2.2 Operation 2nd Hand Smoke.pptx: 4](#_Toc198232919)

[2.3 Airport Information.docx 4](#_Toc198232920)

[2.4 Cloudy thoughts (4apr).docx 5](#_Toc198232921)

[2.5 The Cloudy Manifesto.docx 5](#_Toc198232922)

[2.6 Brother chat.gdoc 5](#_Toc198232923)

[2.7 RAM Evidence and Volatility Artifacts 5](#_Toc198232924)

[3. Analysis 6](#_Toc198232925)

[3.1 Document content and metadata 6](#_Toc198232926)

[3.2 Browser Activity and Search History 7](#_Toc198232927)

[3.3 Registry and System Usage 7](#_Toc198232928)

[3.4 RAM Forensics and Live Artifacts 7](#_Toc198232929)

[3.5 Processes 8](#_Toc198232930)

[3.6 Network Activity 8](#_Toc198232931)

[3.7 Timeline Correlation and Behaviour 8](#_Toc198232932)

[3.8 Psychological Indicators 8](#_Toc198232933)

[4. Findings 8](#_Toc198232934)

[4.1 Evidence of Operational Planning 8](#_Toc198232935)

[4.2 Indicators of Motive and Ideological Justification 9](#_Toc198232936)

[4.3 Technical Complexity and Awareness 9](#_Toc198232937)

[4.4 Browser history 10](#_Toc198232938)

[4.5 RAM Analysis Confirms Session Activity 10](#_Toc198232939)

[4.6 Link Between Identity and System Usage 10](#_Toc198232940)

[4.7 Other related data 10](#_Toc198232941)

[4.8 Synced Cloud Content 11](#_Toc198232942)

[4.9 User and system information: 12](#_Toc198232943)

[3. Conclusions 12](#_Toc198232944)

[Appendix A – Supporting Screenshots 13](#_Toc198232945)

# 1.Introduction

This forensic investigation report has been compiled as part of an incident response assessment to determine the digital behaviour, intent and potential criminal planning of the suspect identified as Jim Cloudy. The investigation involved a detailed forensic examination of both a disk image (LoneWolf.E01) and a RAM memory dump acquired from the suspect's workstation. The primary goal is to assess whether the user demonstrated knowledge, motive, and intent relating to any potentially harmful activity, particularly those posing a threat to public safety.

The forensic process followed industry best practices and used a range of tools, including Autopsy, FTK Imager, Registry Viewer, Volatility Workbench, and browser analysis utilities such as ChromeCacheView. These tools enabled the identification, extraction, and analysis of files and metadata from the suspect’s computer. Particular attention was paid to document contents, browser history, registry entries, command-line activity, and volatile memory artifacts that could indicate planning or ideologically motivated behaviour.

From the disk image, several files were recovered containing concerning content including The Cloudy Manifesto, Planning.docx, Cloudy Thoughts (4apr), and Operation 2nd Hand Smoke.pptx. These documents featured ideologically charged narratives, tactical planning notes, reconnaissance data, and references to public locations such as airports. Combined with browser search activity and synced cloud storage artifacts, these findings contribute to a behavioural profile of the suspect and help assess their psychological state and level of preparation.

RAM analysis using Volatility further revealed running processes, active sessions, and network connections. This volatile data provides insight into the system’s state at the time of acquisition and may reveal any attempted anti-forensic techniques.

This report is organised into key sections: the tools and methodology used during the investigation, a catalogue of recovered evidence (including metadata and hash values), a behavioural and content analysis of the findings, and a final set of conclusions to assess the suspect’s intent and capability to carry out a harmful act.

Through this comprehensive forensic investigation, the aim is to present a factual, unbiased account of the suspect’s digital footprint and determine whether indicators of intent or planning can be established based on the recovered data.

# 2. Forensic Examination

## Tools

A range of digital forensic tools were used throughout the investigation to analyse the disk image and RAM image that were provided by the Northumbria university. These tools helped extract, analyse, and interpret data relevant to confirming user activity, system behaviour, and potential intent or motive behind any suspicious actions. Each tool served a specific role in examining several aspects of the suspect’s system, both volatile and non-volatile data.

### 1.1 Exterro FTK Imager 4.7.3.81:

FTK Imager was used at the beginning of the investigation, not to create a forensic image but to verify the disk image file named LoneWolf.E01 and the RAM image that were already provided. I used FTK Imager to browse through the content of the disk image and to extract certain files of interest. It allowed for quick viewing of file structures and metadata, which helped identify documents, logs, and cloud-sync paths that required deeper analysis.

### 1.2 Autopsy 4.22.1:

Autopsy, an open-source digital forensics platform, was used to conduct a more detailed investigation of the disk image. It enabled the recovery and viewing of deleted files, examining of browser history, file system examination, and timeline analysis. Through Autopsy, I found multiple documents with suspicious titles and contents stored in the suspect's Desktop and other directories. The keyword search and metadata analysis features helped uncover sensitive documents such as: The Cloudy Manifesto, Planning.docx, AIRPORT INFORMATION.docx, Cloudy thoughts.docx and user personal information.

### 1.3 Access Data Registry Viewer:

Registry Viewer was used to analyse the Windows Registry hives extracted from the disk image. This tool helped locate key user information such as the username jcloudy, evidence of connected external devices, and traces of program execution. It also helped verify last login times and supported the establishment of a timeline of user activity.

### 1.4 Event Log Explorer:

Was another tool used to examine Windows Event Logs for system-level information such as shutdowns, logins, service executions, and installed applications or drivers. This helped build a clearer picture of when specific events occurred and validated data from other sources.

### 1.5 Volatility Workbench 2.1 and 3.0:

For memory analysis, I used both Volatility Workbench 2.6.1 and Volatility 3.0. Since Volatility 2.6.1 encountered some compatibility issues, I switched to Volatility 3, which collaborated successfully with the RAM image. These tools allowed for in-depth memory analysis, including retrieving active and terminated processes, network connections, and command history. The plugins used included pslist, pstree, cmdscan, malfind, filescan, and netscan, which revealed the presence of multiple cloud-sync applications.

### 1.6 ChromeCacheView (NirSoft):

Lastly, ChromeCacheView was used to extract browser cache data from Chrome, including visited websites, autofill data, and potential URL indicators related to planning or reconnaissance Although I had no prior experience with this tool, I followed online guidance to use it effectively and it was useful in identifying web-based behaviour that matched findings from memory and disk analysis.

## Evidence

Evidence extracted and analysed from following devices:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Item** | **Description** | **MD5** | **SHA1** | **Size** | **Time zone** |
| RAM memory dump image | Memory dump image from suspect device | 694d1b7c761b50f f5145e0fed4f4f411 | 072d118d528d6f17772e f3e5042a0c37906defc9 | 17.96 Gb | Europe/London |
| Hard Drive | Disk image of Dell Latitude E6430 ATG | 7af48fa65519e8424 6b1729e5b68f140 | 694e26624d1ea029eb5 0d793b198edf85be4b4fc | 512.11 Gb | Europe/London |

During the forensic analysis of the disk image LoneWolf.E01 and the RAM dump, multiple critical artifacts were recovered. These artifacts helped establish the user's identity, timeline of events, and psychological state, and contributed to a strong narrative of intent and planning. The files recovered range from planning documents and manifestos to cached browser history and application remnants in memory. Below is a breakdown of the most significant pieces of evidence.

### 2.1 Planning.docx:

Location: /Users/jcloudy/Desktop/Planning.docx (Dates differ on other paths documents found)  
Created: 2018-03-30 03:16:48 BST  
Modified: 2018-04-04 06:30:49  
Accessed: 2018-04-04 06:30:49  
Changed: 2018-04-04 06:30:49  
MD5: 4ef414e469b7830faa2db429fe1321ee  
Description: This document lays out specific operational details, including target selection, timing considerations, and logistics such as equipment. It states a tactical plan and directly indicates the author was not simply wandering but actively planning a real-world action.

### 2.2 Operation 2nd Hand Smoke.pptx:

Location: /Users/jcloudy/Desktop/Operation 2nd Hand Smoke.pptx (Dates differ on other paths documents found)  
Created: 2018-03-30 15:11:34  
Modified: 2018-04-04 06:11:27  
Accessed: 2018-04-06 06:11:27  
Changed: 2018-04-06 06:11:53  
MD5: abecb19cba0566f27067c403ecfb3bd2  
SHA-256: df7417d3cb0edc3ea0e81a6f1d1d045fa7292adbd54b30020aa04a8d3e9a0a82  
Description: This PowerPoint presentation is titled with a codename suggestive of a covert operation. The slides discuss themes of social revolution and passive resistance but combined with radical rhetoric. It may have been intended for ideological propagation or group motivation.

### 2.3 Airport Information.docx

Location: /Users/jcloudy/Desktop/AIRPORT INFORMATION.docx (Dates differ on other paths documents found)  
Created: 2018-03-30 03:29:57 BST  
Modified: 2018-04-04 05:59:32  
Accessed: 2018-04-04 05:59:32  
Changed: 2018-04-04 05:59:40  
MD5: 297eec248647f33f887d72328ab56f3c  
Description: This document details airport distance and timetables for flights. It includes visual references and schedules, suggesting physical reconnaissance or elementary research. The presence of this file complements operational documents and suggests tactical awareness.

### 2.4 Cloudy thoughts (4apr).docx

Location: /Users/jcloudy/Desktop/Cloudy thoughts (4apr).docx (Dates differ on other paths documents found)  
Created: 2018-04-04 17:02:30  
Modified: 2018-04-06 08:20:20  
Accessed: 2018-04-06 08:20:20  
Changed: 2018-04-06 08:20:42  
MD5: d9dfd7b28cb26724a9c1e3b7f929bcb6  
Description: This document appears to be a personal journal entry expressing existential despair and dislike toward society. While not a direct plan, it offers context and emotional insight into the author’s mindset, showing increasing emotional instability, radical thinking, and suicidal action.

### 2.5 The Cloudy Manifesto.docx

Location: /Users/jcloudy/Desktop/The Cloudy Manifesto.docx (Dates differ on other paths documents found)  
Created: 2018-03-31 21:19:54  
Modified: 2018-04-02 02:35:27  
Accessed: 2018-04-02 02:35:27  
Changed: 2018-04-02 02:35:39  
MD5: 14c07920ddc81fbd489e61d60e5c9f28  
Description: The manifesto is a psychological and ideological justification of violence, outlining the author’s philosophical beliefs, perceived injustices, and moral reasoning for potential acts of retaliation. It is heavily personalized and includes emotionally charged language indicating internal conflict and radicalization.

### 2.6 Brother chat.gdoc

Location: /Users/jcloudy/Google Drive/Brother Chat.gdoc   
Created: 2018-03-31 21:09:54  
Modified: 2018-04-06 08:20:00  
Accessed: 2018-04-06 08:20:00  
Changed: 2018-04-06 08:21:28  
MD5: 9eb42bf9159828639cc2f30214050e0f  
Description: Although this file is a shortcut to a Google Drive document, metadata and filename suggest it was used for communication possibly with his brother. While its contents could not be directly reviewed, it strongly implies off-device communication.

### 2.7 RAM Evidence and Volatility Artifacts

Memory analysis using Volatility 2.6.1 and Volatility 3.0 Workbench recovered several relevant processes, including:

* Running instances of Chrome with active sessions.
* Residual memory strings pointing to the names of the planning documents listed above.
* Network connections through netscan indicating usage of remote collaboration tools.

**RAM Data:**

|  |  |  |  |
| --- | --- | --- | --- |
| Artifact/Program | Evidence from Disk | Evidence from RAM | Notes |
| Drop Box | Detected as an installed and active service | Found via PsList, NetScan and other commands | Presence in both disk and Ram, consistent usage |
| Box Sync | Detected as an installed and active service | Found through PsList, NetScan and other commands | Presence in both disk and RAM, consistent usage |
| Google Drive Sync | Found in registry and file paths | Running process googledrivesync.exe | Presence in both |
| FTK Imager | Found in event log explorer | Found via PsList command | Matched in both disk and RAM but seen some error during running. |
| Chrome.exe | Found in installed path | Multiple active chrome processes | Matched and active usage in both disk and RAM |
| DbxSvc (Dropbox helper) | Detected as an installed and active service | Running processes | Present in both disk and RAM |
| Malicious Indicators | None seen in disk | Might be some but not serious | Only found in RAM |
| Network Connections | Basin information | Highly active connections found via NetScan command | Found detailed in RAM |
| Planning.docx | Presence in multiple path | Found via FileScan command | Presence in disk and RAM |
| Airport information.docx | Presence in multiple path | Found via FileScan command | Presence in disk and RAM |
| Cloudy thoughts(4apr).docx | Presence in multiple path | Found via FileScan command | Presence in disk and RAM |
| Operation 2nd hand smoke.pptx | Presence in multiple path | Found via FileScan command | Presence in disk and RAM |
| Skype | None found | Found via PsList | Only found in RAM |
| One Drive | Installed and used service | Found in ram | Available in both disk and RAM |

These findings confirm that many of the documents were not only stored on disk but were also in active use during the memory capture and those documents was found in many cloud storage services.

## Analysis

The forensic analysis focused on linking together multiple digital traces found across the disk and RAM images. The main objective was to determine whether the suspect, Jim Cloudy, revealed intent, planned a specific operation, or acted with motive. Evidence was analysed in context to behaviour, system usage, and psychological state.

### 3.1 Document content and metadata

Five key documents retrieved from the disk provide foundational insight into the suspect’s thought process and operational planning.

* The Cloudy Manifesto.docx and Cloudy thoughts (4apr).docx reflect the psychological and ideological condition of the suspect. Content analysis showed elements of anger, justification for extreme actions, and underlying rational frustration with societal norms. The manifesto mirrored similar structures to real-world radical documents, indicating a belief in the legitimacy and necessity of his planned actions.
* Planning.docx contained operational outlines, resource lists, and contingency arrangements. The structured tone and language used signified calculated decision-making rather than impulsive thoughts. Details such as locations, required items, and alternative strategies pointed toward the intent to conduct an action in public spaces.
* AIRPORT INFORMATION.docx showed reconnaissance data on terminals and layouts for US airports. Cross-referencing timestamps and other documents suggested that the suspect considered this location because it is closer to the operation area.
* Operation 2nd Hand Smoke.pptx stood out as a visual representation of an action plan, with coded naming and slide content resembling strategic objectives, target, and escape route.

Each document's metadata was carefully reviewed. All were modified and accessed on April 4-6 of 2018, suggesting a conclusion of planning. The matching access and modified dates on these files indicate they were reviewed or edited in a single session, within hours of each other.

### 3.2 Browser Activity and Search History

Using ChromeCacheView, Autopsy, and event logs, browsing data was retrieved that back up the documents' contents. Autopsy revealed visited URLs and autofill entries indicating:

* Searches related to airport maps, security layout, flight schedules, Ammunition, weapons, and escape route.
* Keywords linked to ideological phrases, radical publications, and protest terminology.
* Google queries involving weapon parts and terminology related to operation 2nd hand smoke.

Furthermore, the browser autofill database stored a previously entered email address (jcloudy@outlook.com), along with aliases found in document metadata, directly linking system activity to the suspect.

### 3.3 Registry and System Usage

Registry Viewer was used to analyse NTUSER.DAT and SOFTWARE hives. These revealed:

* Last login user as Jim Cloudy, which matched the document authorship and username on the system.
* Most Recently Used lists included paths to the planning and manifesto files.
* User Assist entries confirmed execution of Microsoft Word, PowerPoint, and Google Drive, consistent with observed documents.

These findings further established continuity between the suspect’s user profile, document creation, and browsing behaviour.

### 3.4 RAM Forensics and Live Artifacts

Analysis of the RAM image was performed using Volatility Workbench 2.6.1 and Volatility 3, allowing for process, command line and network session inspection.

### 3.5 Processes

Using commands like pslist, pstree, and cmdscan revealed multiple processes were active at the time of memory capture:

* chrome.exe appeared multiple times, correlating with the recovered browser data.
* WINWORD.EXE and POWERPNT.EXE processes confirmed live editing of documents such as “Cloudy Manifesto” and “Operation 2nd Hand Smoke.”
* Communication activity such as Skype might proves the connection to the brother chat.gdoc.

### 3.6 Network Activity

The netscan plugin revealed several established connections from chrome.exe to cloud storage services like Dropbox and Google Drive. The timing of these connections aligns closely with file modification timestamps, suggesting document synchronization or sharing activity. Furthermore, placeholder .gdoc files were found on disk (e.g., Brother Chat.gdoc), indicating active use of Google Drive for off-device storage or collaboration.

### 3.7 Timeline Correlation and Behaviour

Combining timestamps from the file system, RAM data, and network logs enabled the reconstruction of the suspect’s recent session on the system:

* Between April 4–6, 2018, the suspect created or modified all major planning documents.
* Chrome sessions occurred simultaneously, with tab activity focused on logistics, ideology, and social issues.
* Google Drive sync activity overlapped with the editing sessions, supporting the theory of external collaboration or cloud backup.

### 3.8 Psychological Indicators

The combination of emotional tone, philosophical content, and operational detail suggests a complex mindset. Unlike natural outbursts, the structured nature of the writing, references to historical figures, and careful word choice in The Cloudy Manifesto point to ideological motivation rather than emotional instability. The use of code words and symbolic names (e.g., 2nd Hand Smoke) further reveals an effort to use vague or symbolic terms to keep plans hidden a characteristic of intentional ideological operations.

## Findings

The forensic investigation presents a cohesive overview of the suspect’s activities, mindset, and planning behaviour. Evidence from disk analysis, browser history, system logs and memory forensics all contributed to the findings outlined below.

### 4.1 Evidence of Operational Planning

The suspect’s computer contained multiple documents that outlined planning for an event of potentially dangerous or criminal nature. These included:

* Planning.docx contained strategic outlines, suggesting preparation for a coordinated action involving the public. It detailed what equipment would be needed, timing considerations, and references to specific locations, meaning more than accidental writing.
* Operation 2nd Hand Smoke.pptx further supported this by presenting a formalized action plan with codewords, symbolic terminology, and visual components, indicating a serious level of preparation.
* AIRPORT INFORMATION.docx provided technical details about terminal layouts, travel flow, and logistics common elements in operational reconnaissance. The correlation with other planning files point out its strategic value.

This collection of documents which are consistent in tone, writing metadata and creation timeline strongly suggests that the suspect was actively planning and refining a real-world operation.

### 4.2 Indicators of Motive and Ideological Justification

The investigation uncovered files that help conclude the suspect’s motive and ideological stance:

* The Cloudy Manifesto.docx laid out a philosophical and personal worldview, expressing deep dissatisfaction with societal structures. It included suggestions to historical movements and justified radical actions as a response to identified injustice.
* Cloudy thoughts (4apr).docx, resembling a diary entry or personal log, revealed emotional instability, disappointment, and recurring themes of grievance. The combination of emotional content and calls for action suggested a transition from passive dissatisfaction to active planning.

These documents are critical in establishing motive. The psychological and ideological content matches typical indicators found in threat modelling or behavioural threat assessments particularly in lone-actor threat scenarios such as lone wolf.

### 4.3 Technical Complexity and Awareness

The suspect understood technical tools and took some steps to protect their digital activities. Several indicators support this:

* Use of Cloud Services: Google Drive activity was present on the machine, and Chrome sessions showed syncs with Google Docs. A .gdoc file (Brother Chat.gdoc) existed as a placeholder, indicating that some discussions or collaboration occurred online and off-device. This would reduce the risk of forensic recovery unless cloud credentials are obtained separately.
* Use of Word and PowerPoint: The suspect favoured Microsoft Office tools for documentation. These tools store significant metadata, and their consistent use suggests a preference for local document manipulation with potential export/sharing to cloud locations.

While no encryption or data wiping tools were found, the structuring and categorization of data (naming, folder locations, timestamps) suggest some operational awareness.

### 4.4 Browser history

Browser activity confirmed the suspect conducted extensive online research in line with the planning documents. Recovered history showed:

* Searches for airport terminal maps, security patrol timings, passenger flow, flight delays, safest destination, weather forecast and carrying cash.
* Access to logistical websites, including transit schedules and airport databases.
* Queries about philosophical movements, revolutionary acts, and references to past Lone Attack.

The browsing data's alignment with document content further substantiates that the suspect's writing was not purely theoretical it was informed by real data gathered through active reconnaissance.

### 4.5 RAM Analysis Confirms Session Activity

Memory analysis via Volatility plugins showed that:

* WINWORD.EXE and POWERPNT.EXE processes were active, confirming that the suspect had been editing documents during or shortly before the RAM image was taken.
* Filescan command-line activity matched access to folders where the planning documents resided.
* netscan results identified active sessions with Google Drive, substantiating cloud synchronization during this period.

RAM analysis confirmed not only what the suspect had done but when it was done namely, the activities occurred within a close period to when the memory was acquired.

### 4.6 Link Between Identity and System Usage

Every stage of the investigation consistently linked digital activity back to the user, Jim Cloudy:

* Username “jcloudy” was rooted in the user profile path.
* All documents listed “Jim Cloudy” as the author.
* Registry hive data confirmed login activity for the same user.
* Email autofill entries and Chrome profile information also referenced the same identity.

This clearly establishes both system ownership and user responsibility, with the case scenario confirming the device was given to the suspect by his brother.

### 4.7 Other related data

Additional artifacts relevant to the case are worth noting:

* Web Data File  
  Located at:  
  user/jcloudy/AppData/Local/Google/Chrome/User Data/Default/Web Data  
  This file contains personal information linked to Jim Cloudy, including a phone number (7038727612) and email address (jimcloudy1@gmail.com), further supporting user attribution.
* Rootkey.csv File  
  Located at:  
  user/jcloudy/Downloads/rootkey.csv  
  This file contains credentials related to Amazon Web Services (AWS), specifically:

AWS Access Key=AKIAJQCL74OG6U6JRXKQ

AWS Secret Key=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

The presence of these keys suggests potential access to cloud-hosted resources or services, which needs further investigation. (as shown in Figure A8 of Appendix A).

### 4.8 Synced Cloud Content

Several files were synchronised to cloud storage services, indicating potential off-device access or backup. This behaviour supports the notion that the suspect may have intended to preserve, share, or remotely access key documents.

Files identified as synchronised to the cloud include:

* The Cloudy Manifesto.docx
* Cloudy thoughts.docx
* Operation 2nd Hand Smoke.pptx
* Planning.docx
* AIRPORT INFORMATION.docx
* DeathToll.jpg
* DemLogic.jpg
* HoldMyTidePod.jpg
* Huckleberry.png
* MyTiredHead.jpg
* Sheep.jpg
* RedGuns.jpg
* CubaDearmed.jpg
* DarkWolf.png
* BladeofGrass.jpg

These items reflect a mix of operational documents and ideologically suggestive images. Their presence in cloud storage strengthens the link between the suspect and digital planning activities.

### 4.9 User and system information:

During forensic analysis of the disk image LoneWolf.E01, system metadata was extracted from the Recent Activity artifacts. The system was identified as a Windows 10 Education edition running on an AMD64 architecture. The machine name is DESKTOP-PM6C56D, with its system root located at C:\Windows and temporary files stored in %SystemRoot%\TEMP. The Windows Product ID was recorded as 00328-00089-23637-AA141. The primary user of the system was identified as "Windows User". This foundational system and user data helped establish the environment in which the suspect operated and provided a basis for correlating other user-specific evidence. (As shown in Figure A10 Appendix A).

User information: following information extracted from keyword search hits chrome web data.

* Name = Jim Cloudy
* email address = [jimcloudy1@gmail.com](mailto:jimcloudy1@gmail.com)
* email address = [jcloudy@outlook.com](mailto:jcloudy@outlook.com)
* user phone number = 7038727612

(As shown in Figure A5 of Appendix A).

# 3. Conclusions

The digital forensic examination of Jim Cloudy’s disk and memory images produced strong, comprehensive evidence pointing toward the active planning of a potential attack. Using industry-standard tools such as Autopsy, Volatility Workbench, FTK Imager, ChromeCacheView, and Registry Viewer, this investigation successfully reconstructed user behaviour, document authorship, and online activity in detail.

The disk analysis revealed a concerning collection of documents notably Planning.docx, Operation 2nd Hand Smoke.pptx, and AIRPORT INFORMATION.docx each containing operational details, logistical notes, and reconnaissance data. These files reflect a clear progression from abstract ideation to structured planning, with timestamp metadata confirming recent and planned activity.

Supporting documents like The Cloudy Manifesto.docx and Cloudy thoughts (4apr).docx revealed the suspect’s ideological stance and psychological state. Their content matched known patterns in behavioural threat assessments, highlighting themes of dissatisfaction, justification, and readiness to act.

The forensic timeline confirms that this activity occurred shortly before image capture, reinforcing the relevance of the evidence. Metadata, registry entries, and browser autofill all consistently tied the actions to the user account “jcloudy,” leaving little doubt about user attribution.

Although no traditional malware or exploit code was identified, this is consistent with the behavioural profile of a Lone Actor focused on planning and ideology rather than technical cyber-offensive skills.

In conclusion, the evidence supports that Jim Cloudy engaged in intentional, ideologically driven planning. The digital artifacts demonstrate motive, reconnaissance, operational preparation, and active system usage meeting the investigative goal of establishing both intent and capability. This case highlights the value of digital forensics in uncovering both technical actions and the underlying psychology behind them.

# Appendix A – Supporting Screenshots

A screenshot of a computer

AI-generated content may be incorrect.

Figure A1 – Metadata for AIRPORT INFORMATION.docx showing timestamps and hash.

A screenshot of a computer program

AI-generated content may be incorrect.

Figure A2 – Metadata for Operation 2nd Hand Smoke.pptx confirming active session.

A screenshot of a computer program

AI-generated content may be incorrect.

Figure A3 – Metadata for Planning.docx confirming coordinated planning.

A screenshot of a computer

AI-generated content may be incorrect.

Figure A4 – Extracted Chrome data showing suspect’s phone, email, and search terms.

A screenshot of a computer

AI-generated content may be incorrect.

Figure A5 – Chrome Web Data file metadata supporting user identity linkage.

A screenshot of a computer

AI-generated content may be incorrect.

Figure A6 – Windows Event Log showing SSD activity and timestamps.

A screenshot of a computer

AI-generated content may be incorrect.

Figure A7 – Metadata for rootkey.csv containing AWS credential information.

A screenshot of a computer

AI-generated content may be incorrect.

Figure A8 – Extracted AWS credentials showing potential cloud service access.

A screenshot of a computer

AI-generated content may be incorrect.

Figure A9 – USB device metadata from SYSTEM hive showing external device usage.

A screenshot of a computer

AI-generated content may be incorrect.

Figure A10 – System information showing Windows user and machine identity.