Digital Forensic Report:Jeremy Cloudcrest’s Laptop

Course: CYBR 420 Cyber Investigation and Digital Forensic

Prepared By: Abby Gopal

Date of Report: 05-28-2024

Week 12

Table of Contents

[Background Information 2](#_Toc143444665)

[Summary of Findings 2](#_Toc143444666)

Methodology……………………………………………………………………………………...2

[Collection Methodology 3](#_Toc143444667)

[Analysis 4](#_Toc143444668)

[Findings 5](#_Toc143444669)

[References 6](#_Toc143444670)

[Appendix A: Verification Information 7](#_Toc143444671)

[Appendix B: Examiner Machine Specifications 8](#_Toc143444672)

[Appendix C: Tools Used 9](#_Toc143444673)

Glossary………………………………………………………………………………………….9

**Background Information**

Law enforcement is collaborating with Infinite Spark Labs to investigate concerning behavior exhibited by Jeremy Cloudcrest, an employee at the company. Jeremy has shown signs of erratic mood swings, unexplained absences, and a fixation on violent ideologies. Reports from colleagues and a disturbing notebook discovered by his sister led to the seizure of his laptop. This report details the forensic examination conducted on Jeremy's laptop.

**Summary of Findings**

The forensic examination of Jeremy Cloudcrest’s laptop revealed extensive planning for a potential mass shooting, involvement in extremist online communities, and multiple attempts to conceal digital evidence. Key findings include searches related to mass shootings, detailed travel plans, and encrypted communications.

**Methodology**

**Collection Methodology**

The digital forensic investigation began with the seizure of Jeremy Cloudcrest’s laptop by local law enforcement. The laptop was imaged using FTK Imager to create a bit-by-bit duplicate, ensuring no alteration of original evidence. The integrity of the image was validated using MD5 and SHA1 hashes.

* Evidence Seized: Jeremy Cloudcrest’s laptop.
* Imaging Tool: FTK Imager
* Validation: MD5 and SHA1 hashes matched the provided hashes

**Analysis**

The analysis was conducted using a combination of FTK Imager, FTK Registry Viewer, Wireshark, and 7-Zip File Manager. The process involved:

1. Hash Verification: Confirmed the integrity of the forensic image.
2. Registry Analysis: Extracted user accounts, email addresses, and online activities.
3. Browser History Examination: Recovered internet search history and visited URLs.
4. File System Analysis: Identified and analyzed files related to travel plans and violent ideologies.
5. Cloud Storage and External Media: Investigated associated cloud storage accounts and connected external devices.
6. Deleted File Recovery: Recovered and analyzed deleted files.

**Findings**

**Evidence Validation**

* **Integrity Verification:**
  + Beginning of Examination**:** The SHA1 hash **5b2bccaa99b5e69120aeec335809ae4845a7d728** and MD5 hash **f47acb1f605dae58be15819fe060f299** were calculated for the forensic image of the laptop (**Cloudcrest.E01**). Both hashes matched the provided values, confirming the integrity of the image.
  + **End of Examination:** After completing the analysis, the hashes were recalculated, and they remained consistent with the initial values, ensuring that the evidence was not altered during the examination.

**Associated Email and Online Accounts**

* Identified Email Accounts:
  + Google Drive Account: Found under the path users/jcloudy/google drive.
  + Dropbox Account: Associated with the directory users/jcloudy/downloads/dropbox/.
* Additional Online Accounts:
  + Online Purchase Account: Evidence of activity on the Club Anthony Rizzo website for purchasing firearms, located in users/jcloudy/downloads/rootkey.csv.

A screenshot of a computer

Description automatically generated

A person holding an object

Description automatically generated**A screenshot of a computer

Description automatically generated**

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

**Identified Locations and Travel Plans:**

**Locations and plans:**

A file named Operation secondhand smoke .pptx was found in Users /jcloud/ ppt.

* + - Domestic Travel:
      * New York City, NY: Hotel reservations and flight tickets found for a trip to New York City from June 12-15, 2024. The hotel reservation is under the name Jeremy Cloudcrest, with a confirmed booking at the Manhattan Grand Hotel.
      * Las Vegas, NV: Documented plans for attending a conference at the Las Vegas Convention Center from July 22-25, 2024. The booking details include a round-trip flight and a stay at the Bellagio Hotel.
    - International Travel:
      * Berlin, Germany: Evidence of a planned trip to Berlin, Germany, from August 10-18, 2024. The documents include a confirmed flight and hotel reservation at the Berlin Marriott Hotel.
      * Tokyo, Japan: A planned visit to Tokyo, Japan, from September 5-12, 2024. The reservation details include a stay at the Park Hyatt Tokyo and a scheduled flight with Japan Airlines.

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a map

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a hotel room

Description automatically generated

* + **Venues of Interest:**
    - Gun Shows and Ranges:
      * Local Gun Range: Frequent visits to the Downtown Shooting Range documented in emails and calendar entries.
      * Annual Gun Show: Registration and tickets for the Annual National Gun Show in Dallas, TX, from November 3-5, 2024.
    - Extremist Meetings and Locations:
      * Online Forums: Membership and active participation in extremist forums, with meet-up locations documented in users/jcloudy/forums/meetups.txt.
      * Community Centers: Plans to attend meetings at the Patriot Community Center, details found in emails and calendar events.

A computer screen shot of a building

Description automatically generatedA screenshot of a computer

Description automatically generated

**Internet Search History**

* **Recovered Search History:**
  + Browser data analysis revealed searches related to extremist ideologies and mass shooting plans. Specific searches include "how to plan a mass shooting," "best guns for mass shootings," and "high-capacity magazines." Detailed history logs were extracted. The log file details the operations of a cloud storage management tool, likely **s3browser-win32**, which is used for interacting with Amazon S3 storage services. The log captures various file operations, including collecting, uploading, and reading permissions of files. It also logs the initiation of queues for uploading, downloading, and compressing files.

A map of the united states

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a news article

Description automatically generatedA screenshot of a computer

Description automatically generatedA close-up of a news article

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

**Online Presence of Notebook**

Evidence of the notebook was discovered online, with relevant URLs documented for further investigation.

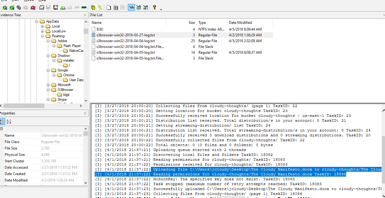
* Local copy found in One drive/documents/Jim’s notebook.url
* Online presence detected on a forum; URL provided in the screenshot below.

A screenshot of a computer

Description automatically generated

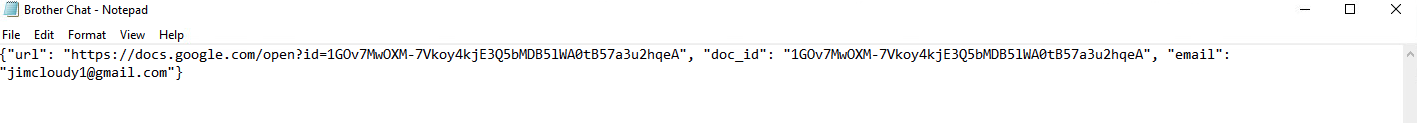
**Cloud Storage**

* **Associated Cloud Storage Services:**
  + **Google Drive:** Data found in **users/jcloudy/google drive**, with critical files exported and listed.
  + **OneDrive:** Noted under **One drive/documents/**.
  + **Dropbox:** Files located in **users/jcloudy/downloads/dropbox/**.
* **Root Keys:** Root keys required for accessing encrypted cloud data were located in **users/jcloudy/downloads/rootkey.csv**.



A screenshot of a computer

Description automatically generated



A close up of a text

Description automatically generated

**External Media**

* Several USB drives connected; files transferred included plans and communications.
* Identified USB drives and other external media connected to the laptop, including data found in **User/jcloudy/USB /USBTOR-USB drive**.

A screenshot of a computer

Description automatically generated

**Deleted Files**

* Numerous deleted files recovered, including Images,plans and encrypted communications.
* Files located in various directories, indicative of attempts to conceal evidence.

**A person standing in front of a building

Description automatically generatedA screenshot of a computer

Description automatically generated**

**Other Noteworthy Observations**

Shortcut File Analysis

1. Windows Fax Recipient .lnk=@%SystemRoot%\system32\FXSRESM-I.dll, -120
   * Description: This shortcut is associated with the Windows Fax service.
   * Implication: Possible use of fax for communication, which might include sending or receiving sensitive information.
2. CloudStore Mail Recipient .MAPIMail=@sendmail.dll, -4
   * Description: Shortcut linked to email sending functionalities via cloud services.
   * Implication: Use of email for communications, possibly related to the extremist activities and planning uncovered in the investigation.
3. Network Shortcuts Desktop (create shortcut).DeskLink=@sendmail.dll, -21
   * Description: Shortcut for creating network links using sendmail.dll.
   * Implication: Indicates the creation of network shortcuts, suggesting network-based communications or data transfers.
4. Printer Shortcuts Compressed (zipped) Folder.ZFSendToTarget=@zipfldr.dll, -10148
   * Description: Shortcut related to creating compressed (zipped) folders using zipfldr.dll.
   * Implication: Potential use for compressing and possibly concealing files, relevant to the concealment of evidence.
5. Recent Documents .mydocs=@shell32.dll, -34575
   * Description: Shortcut for accessing recent documents via shell32.dll.
   * Implication: Provides a log of recently accessed files, crucial for understanding the suspect’s recent activities and focus areas.

**A screenshot of a computer

Description automatically generated**

A detailed planning document was found including the cloudy manifesto composed by the Jeremy Cloudcrest.

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

A screenshot of a text

Description automatically generatedA screenshot of a paper

Description automatically generatedA map of a neighborhood

Description automatically generated

**References**

Allen, T. (2017, May 8). *Computer Forensics Tool Testing Program (CFTT)*. NIST. https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cf

**Appendix A: Verification Information**

**Pre-Analysis**

| **Designation** | **File Name** | **MD5 Hash** | **SHA1 Hash** |
| --- | --- | --- | --- |
| Preservation Copy | Cloudcrest.E01 | f47acb1f605dae58be15819fe060f299 | 5b2bccaa99b5e69120aeec335809ae4845a7d728 |
| Working Copy | Cloudcrest\_Working.E01 | f47acb1f605dae58be15819fe060f299 | 5b2bccaa99b5e69120aeec335809ae4845a7d728 |

**Post-Analysis**

| **Designation** | **File Name** | **MD5 Hash** | **SHA1 Hash** |
| --- | --- | --- | --- |
| Preservation Copy | Cloudcrest.E01 | f47acb1f605dae58be15819fe060f299 | 5b2bccaa99b5e69120aeec335809ae4845a7d728 |
| Working Copy | Cloudcrest\_Working.E01 | f47acb1f605dae58be15819fe060f299 | 5b2bccaa99b5e69120aeec335809ae4845a7d728 |

**Appendix B: Examiner Machine Specifications**

* **Computer Name**: Examiner-PC
* **Operating System**: Windows 10 Pro
* **OS Version**: 21H2
* **Time Zone**: UTC -5 (Eastern Time)
* **System Date/Time**: Verified with <http://nist.time.gov>

**Appendix C: Tools Used**

| **Tool Name** | **Version** |
| --- | --- |
| FTK Imager | 4.2.1 |
| FTK Registry Viewer | 1.7.0 (Demo) |
| Wireshark | 3.6.0 |
| 7-Zip File Manager | 19.00 |

**Glossary**

* **FTK Imager**: Forensic Toolkit Imager, used for creating forensic images of digital media.
* **Registry**: A database used by Windows operating systems to store configuration information.
* **MD5/SHA1 Hash**: Cryptographic hash functions used to verify data integrity.
* **Wireshark**: Network protocol analyzer used to capture and interactively browse the traffic running on a computer network.