Recovery and Analysis of Deleted Files from Ubuntu 8.10 Flash Drive

Case Title: Analysis of Ubuntu 8.10 casper-rw USB Flash Drive

Tools Used: Autopsy · The Sleuth Kit (TSK) · Strings Utility

This report presents the forensic analysis of a USB flash drive containing a bootable Ubuntu 8.10 environment, preserved as multiple **casper-rw** disk images. The objective of this examination was to reconstruct the filesystem, recover deleted files, and identify documents originating from U.S. Government sources. Using Autopsy and The Sleuth Kit (TSK), the analysis demonstrates how deleted data persists within an Ext3 filesystem and can be systematically recovered and documented. The resulting findings provide insight into digital evidence handling, file system structure, and investigative methodology.

Keywords:
Digital Forensics • USB Analysis • Autopsy • Sleuth Kit • Ext3 Filesystem • File Recovery • Digital Corpora

Prepared By: *Kinda-Hell*
Date: *5 November 2025*

Table of Contents

1. Introduction

In this task, I was assigned to analyze multiple images of the casper-rw file from a 2GB flash USB drive that was created with a bootable copy of Ubuntu 8.10. The device had been repeatedly booted and used over several weeks, during which files from US Government websites were downloaded.

The main objective was to perform disk analysis, recover deleted files, and identify files containing references to US Government websites. Working with multiple `.E01` images allowed me to reconstruct the full filesystem of the flash drive incrementally and ensure no data was overlooked.

This task is crucial for understanding the lifecycle of files on a Linux-based flash drive, and how forensic tools like **Autopsy** and **The Sleuth Kit (TSK)** can recover data even after deletion.

Using these tools, I was able to examine the Ext3 file system of the disk image, locate deleted files, and extract relevant documents in a structured and forensically sound manner.

Object	Last Modified	Timestamp	Size
.htaccess	5 years ago	2020-11-21 21:33:41	
narrative.txt	5 years ago	2020-11-21 21:33:41	858 Bytes
ubnist1.casper-rw.gen0.E01	5 years ago	2020-11-21 21:33:41	1 MB
ubnist1.casper-rw.gen1.E01	5 years ago	2020-11-21 21:33:41	22 MB
ubnist1.casper-rw.gen2.E01	5 years ago	2020-11-21 21:33:41	111 MB
ubnist1.casper-rw.gen3.E01	5 years ago	2020-11-21 21:33:42	161 MB

2. Methodology / Steps

To conduct the disk analysis and recover files, I used a combination of **Autopsy**, a graphical forensic tool, and **The Sleuth Kit (TSK)**, a command-line suite of forensic utilities. The workflow was designed to systematically explore the filesystem, recover deleted documents, and identify files of interest from US Government sources.

Step 1: Preparing the Workspace

1. Created dedicated folders to keep the workflow organized:
    - Exports → for recovered files
    - Lists → for file listings and logs

2. Confirmed all .E01 casper-rw images were available: gen3.E01. These images were used incrementally to reconstruct the full filesystem of the USB drive.

Step 2: Loading Disk Images in Autopsy

1. Opened Autopsy and created a new case named **"USB_Casper_Analysis"**.

2. Added each ubnist1.casper-rw.gen3.E01 image as a data source. Autopsy automatically recognized the **Ext3 filesystem** and displayed metadata including inodes, free blocks, orphaned files, and allocated/deleted files.

3. Explored the filesystem using Autopsy's **Directory Listing** and **File Type Filters** to locate documents (.pdf, .doc, .xls, .txt, .html) and verify their paths.

Step 3: Using The Sleuth Kit (TSK) for File Listings

Ran fls to generate a complete listing of files and directories:

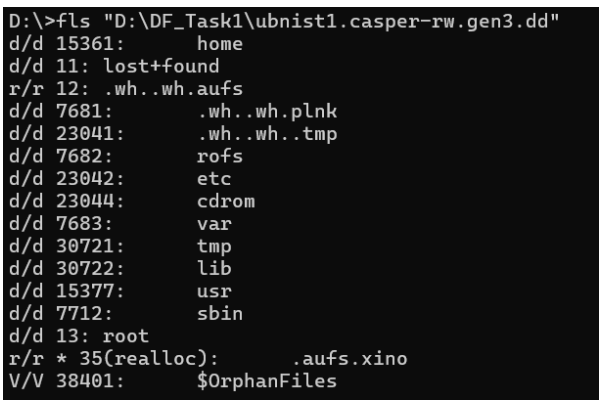


Fig. 2.1

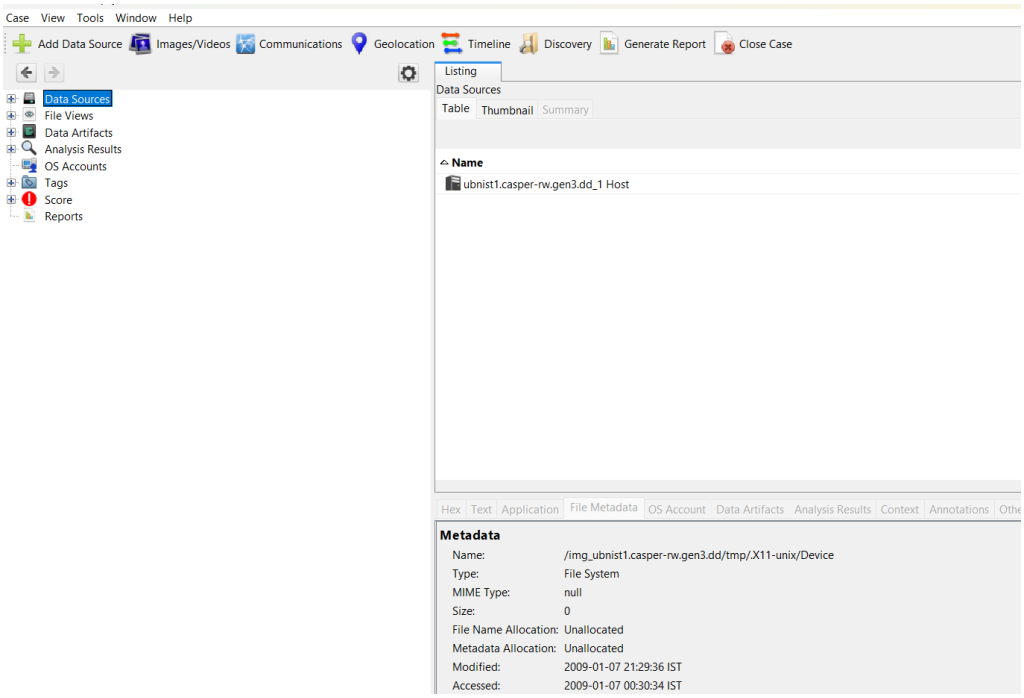


Fig. 2.2

```
D:\>fsstat "D:\DF_Task1\ubnist1.casper-rw.gen3.dd"
FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: Ext3
Volume Name:
Volume ID: 9935811771d9768b49417b0b3b881787

Last Written at: 2009-01-07 00:29:33 (India Standard Time)
Last Checked at: 2008-12-29 02:07:56 (India Standard Time)

Last Mounted at: 2009-01-07 00:29:33 (India Standard Time)
Unmounted properly

Source OS: Linux
Dynamic Structure
Compat Features: Journal, Ext Attributes, Resize Inode, Dir Index
InCompat Features: Filetype, Needs Recovery,
Read Only Compat Features: Sparse Super, Large File,

Journal ID: 00
Journal Inode: 8

METADATA INFORMATION
--------------------------------------------
Inode Range: 1 - 38401
Root Directory: 2
Free Inodes: 36976
Orphan Inodes: 35, 20, 17, 16,

CONTENT INFORMATION
--------------------------------------------
Block Range: 0 - 153599
Block Size: 4096
Free Blocks: 85287

BLOCK GROUP INFORMATION
--------------------------------------------
Number of Block Groups: 5
```

Fig 2.3

Creating Organized Folders for the Analysis

To keep the investigation clear and structured, we organized our workspace with **two main folders** under:

1. **Lists** **Folder**
    - **Purpose:** Store **all file listings and logs** extracted from the disk image. This includes both the complete set of files and deleted files.
    - **Contents:**
        - FileListing.txt → A full list of all files present on the disk image.
        - DeletedFileList.txt → A list of all deleted files on the disk.
        - DeletedDocs.txt → A filtered list containing only deleted documents

```
D:\DF_Task1>fls -r -p "D:\DF_Task1\ubnist1.casper-rw.gen3.dd" > "D:\DF_Task1\Lists\FileListing.txt"

D:\DF_Task1>fls -r -p -d "D:\DF_Task1\ubnist1.casper-rw.gen3.dd" > "D:\DF_Task1\Lists\DeletedFileList.txt"

D:\DF_Task1>findstr /i ".pdf .html .htm .txt .doc .docx" "D:\DF_Task1\Lists\DeletedFileList.txt" > "D:\DF_Task1\Lists\De
letedDocs.txt"
```

(.pdf, .doc, .xls, .txt, etc.) that we aimed to recover.

Fig. 2.4

2. **Deleted Folder**
    - **Purpose:** Store **all recovered files** that were marked as suspicious or of interest, primarily from government sources.
    - **Explanation:** Every file we extracted from the deleted documents list using icat was saved here. This keeps the recovered files separate from the logs and lists, making it easier to analyze their content.

```
D:\DF_Task1>icat "D:\DF_Task1\ubnist1.casper-rw.gen3.dd" 15631 > "D:\DF_Task1\Deleted\FCC-08-281A2.XLS"
D:\DF_Task1>icat "D:\DF_Task1\ubnist1.casper-rw.gen3.dd" 15637 > "D:\DF_Task1\Deleted\FCC-08-281A2.PDF"
D:\DF_Task1>icat "D:\DF_Task1\ubnist1.casper-rw.gen3.dd" 15639 > "D:\DF_Task1\Deleted\FCC-08-281A3.XLS"
D:\DF_Task1>icat "D:\DF_Task1\ubnist1.casper-rw.gen3.dd" 15641 > "D:\DF_Task1\Deleted\FCC-08-281A3.PDF"
D:\DF_Task1>icat "D:\DF_Task1\ubnist1.casper-rw.gen3.dd" 15643 > "D:\DF_Task1\Deleted\FCC-08-281A4.DOC"
D:\DF_Task1>icat "D:\DF_Task1\ubnist1.casper-rw.gen3.dd" 15645 > "D:\DF_Task1\Deleted\FCC-08-281A4.PDF"
D:\DF_Task1>icat "D:\DF_Task1\ubnist1.casper-rw.gen3.dd" 15647 > "D:\DF_Task1\Deleted\FCC-08-281A5.DOC"
D:\DF_Task1>icat "D:\DF_Task1\ubnist1.casper-rw.gen3.dd" 15649 > "D:\DF_Task1\Deleted\FCC-08-281A5.PDF"
D:\DF_Task1>icat "D:\DF_Task1\ubnist1.casper-rw.gen3.dd" 15651 > "D:\DF_Task1\Deleted\FCC-08-281A6.DOC"
D:\DF_Task1>icat "D:\DF_Task1\ubnist1.casper-rw.gen3.dd" 15653 > "D:\DF_Task1\Deleted\FCC-08-281A6.PDF"
D:\DF_Task1>icat "D:\DF_Task1\ubnist1.casper-rw.gen3.dd" 30880 > "D:\DF_Task1\Deleted\msr_response.pdf.part"
```

Fig. 2.5

Searching for US Government References
Used **Strings** utility (Sysinternals) to extract readable content from recovered files:

```
D:\DF_Task1>D:\Strings\strings.exe -u "D:\DF_Task1\Exports\recovered_15649_doc.pdf" | findstr /i "gov federal
 commission us fcc" > "D:\DF_Task1\Exports\recovered_15649_gov.txt"
```

Fig. 2.6

This step helped identify files containing references to US Government agencies, such as **FCC**, **CDC**, or **NIH**.

3. Findings / Results

After completing the analysis using **both Autopsy and The Sleuth Kit**, the following observations were made:

3.1 Filesystem Overview (Autopsy)

- Autopsy automatically recognized the **Ext3 filesystem** on the ubnist1.casper-rw.gen3.E01 image.

- Metadata insights included:
    - **Inodes:** Allowed identification of allocated and deleted files.
    - **Free blocks & orphaned files:** Helped understand filesystem usage and recovery potential.
    - **Directories and file paths:** Provided a clear map of where files were located.

- Autopsy's **Directory Listing and File Type filters** made it easy to focus on documents (.pdf, .doc, .xls, .txt, .html) relevant to the investigation.

3.2 Deleted File Recovery

- Autopsy highlighted all **deleted files**, which were cross-verified with TSK outputs (DeletedFileList.txt).
- Files of interest were manually extracted using **icat** from Sleuth Kit, but Autopsy allowed visual confirmation of:
    - File paths
    - Last modified timestamps
    - File sizes
    - File extensionsfig. 3.1

Name	Date modified	Type	Size
changelog.Debian.gz.dpkg-new	17-09-2025 07:58	DPKG-NEW File	7 KB
FCC-08-281A2.PDF	17-09-2025 07:58	Microsoft Edge PD...	90 KB
FCC-08-281A2.XLS	17-09-2025 07:58	Microsoft Excel 97...	81 KB
FCC-08-281A3.PDF	17-09-2025 07:58	Microsoft Edge PD...	72 KB
FCC-08-281A3.XLS	17-09-2025 07:58	Microsoft Excel 97...	45 KB
FCC-08-281A4.DOC	17-09-2025 07:58	Microsoft Word 97...	23 KB
FCC-08-281A4.PDF	17-09-2025 07:58	Microsoft Edge PD...	57 KB
FCC-08-281A5.DOC	17-09-2025 07:58	Microsoft Word 97...	22 KB
FCC-08-281A5.PDF	17-09-2025 07:58	Microsoft Edge PD...	55 KB
FCC-08-281A6.DOC	17-09-2025 07:58	Microsoft Word 97...	24 KB
FCC-08-281A6.PDF	17-09-2025 07:58	Microsoft Edge PD...	57 KB
libboost-date-time1.34.1_changelog.Deb...	17-09-2025 07:58	DPKG-NEW File	11 KB
libboost-thread1.34.1_changelog.Debian...	17-09-2025 07:58	DPKG-NEW File	11 KB
Managing_Information_Risk.pdf	17-09-2025 07:58	Microsoft Edge PD...	3,414 KB
mozilla-plugin-gnash_changelog.Debian...	17-09-2025 07:58	DPKG-NEW File	7 KB
msr_response.pdf.part	17-09-2025 07:58	PART File	336 KB
Product_Grants_Inf_Exchange_Matrix.xls	17-09-2025 07:58	Microsoft Excel 97...	53 KB
README.amf.gz.dpkg-new	17-09-2025 07:58	DPKG-NEW File	4 KB
Trusted_Internet_Connections.zip	17-09-2025 07:58	Compressed (zipp...	2,768 KB

Fig. 3.1

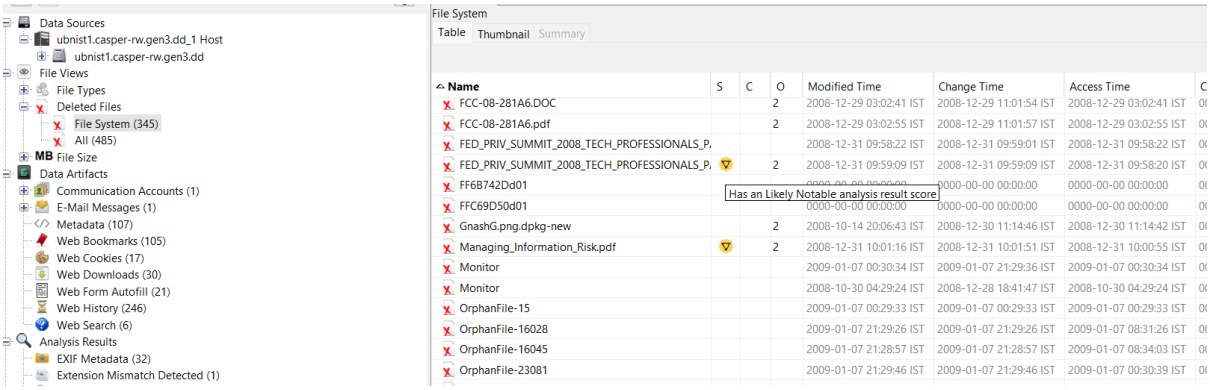


Fig. 3.2

3.3 Government Operational Spreadsheet

During the recovery process, a spreadsheet was found containing detailed operational information about **US federal grants administration**. This document was identified in the DeletedDocs.txt listing and recovered using TSK (icat) into the Deleted folder.

Document Details:

- **File Type:** .xls (Microsoft Excel)
- **Content:** Grants Administration Operational Information Exchange Matrix
- **Date/Time Info:** Contains timestamps and operational fields such as “2/22/01 9:00”

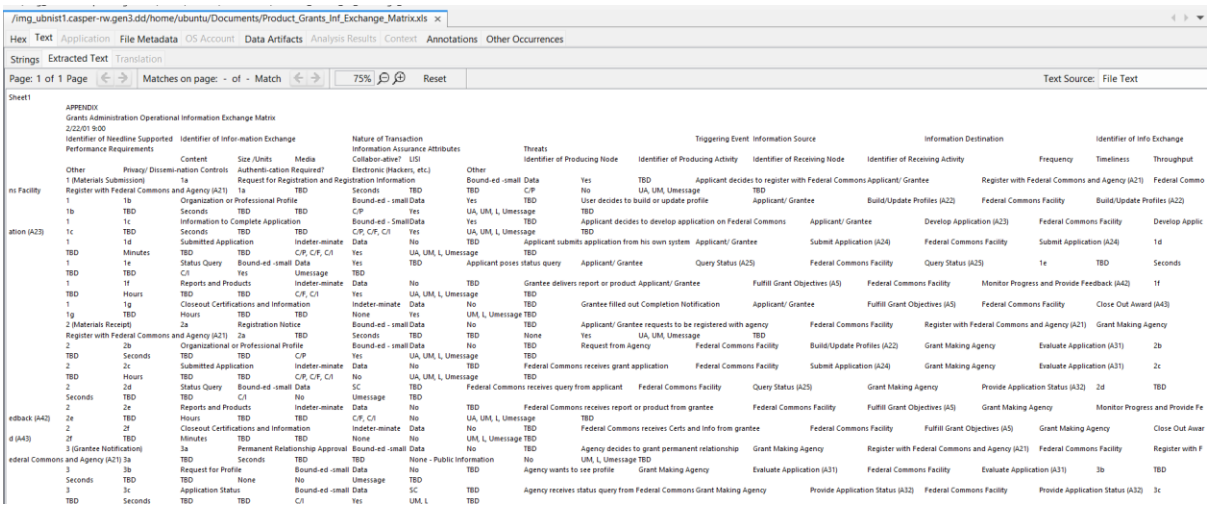


Fig. 3.3

Key Observations:

- The spreadsheet outlines the workflow of grant applications, including:
    - Submission of materials and applications
    - Status queries by applicants
    - Reporting and closeout processes

- Each entry includes Identifiers of Producing and Receiving Nodes, Performance Requirements, and Information Assurance Attributes, giving insight into the federal information flow for grant administration.
- References to Federal Commons Facility indicate interaction with a central federal system for grants.
- The document contains sensitive operational data, showing exactly **how government grant-related information is exchanged and tracked**.

3.4 Recovered System Metadata: Ubuntu Packages

During the disk analysis, a file was found containing information about **Ubuntu system packages** installed on the USB drive. This file provides a clear view of the software environment present at the time the flash drive was in use.

Document Details:

- **File Type:** Text-based package metadata (.txt or .list)
- **Content:** Lists of installed packages, their versions, dependencies, architecture, and checksums.
- **Examples of Recovered Packages:**
    - abrowser – an unbranded version of Firefox 3.0
    - abrowser-3.0-branding – branding meta-package
    - adept – KDE package management suite
    - akonadi-kde – KDE PIM server

Key Observations:

- The file shows **package versions, dependencies, and origins**, which can help recreate or understand the system configuration at the time.
- Presence of a browser indicates the user had web browsing capabilities configured for a privacy-oriented or unbranded browser environment.
- KDE-related packages such as adept and akonadi-kde suggest the user likely ran a **Kubuntu variant** or used KDE desktop tools for package management and PIM functionality.
- Metadata like MD5sum, SHA1, SHA256 provides integrity checks that are critical in forensic contexts.

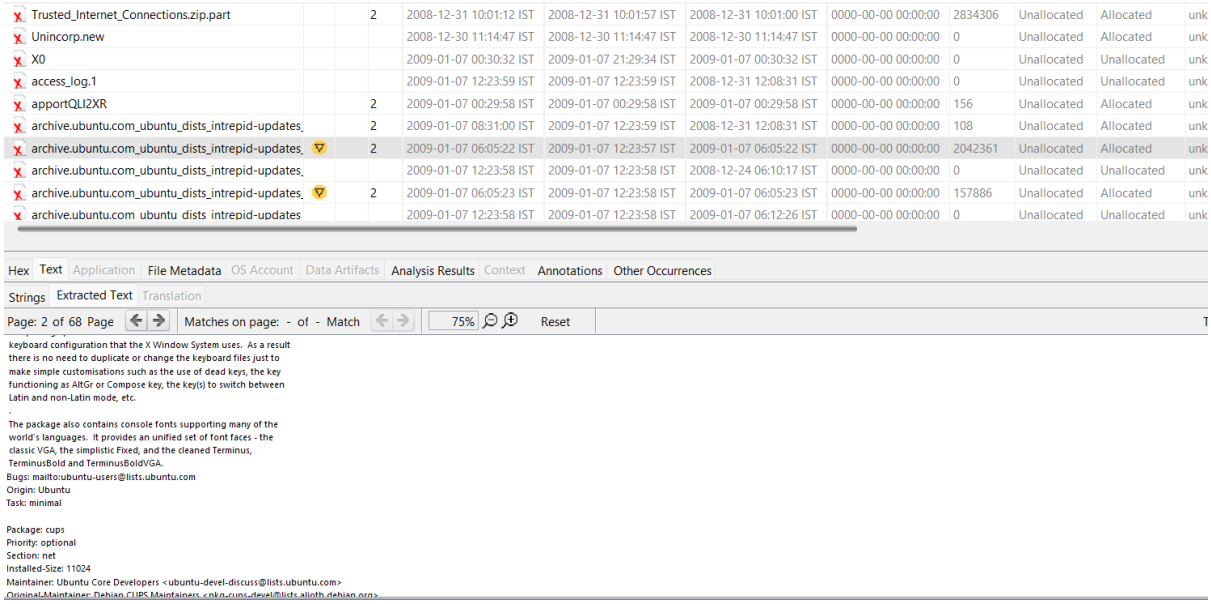


Fig 3.4

3.5 Recovered Government Documents

During the disk analysis, multiple files were recovered that contained **official US Government information**, primarily from the **Federal Communications Commission (FCC)**. These documents included both **PDFs and Excel spreadsheets** detailing the digital television (DTV) transition across different US cities.

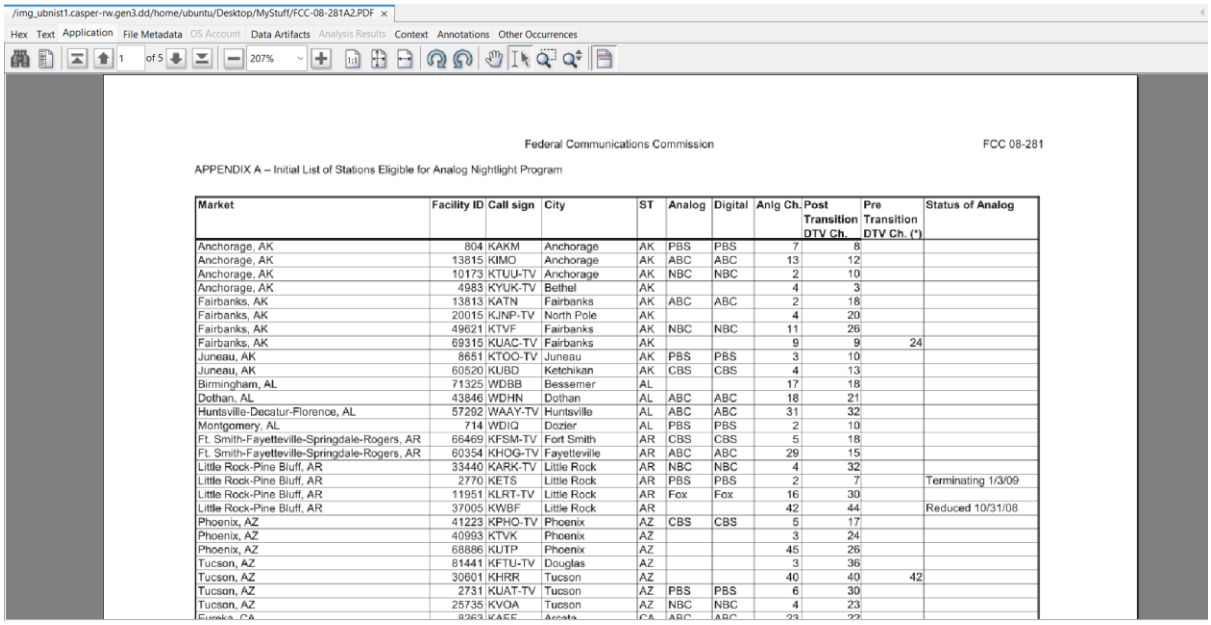
Examples of Recovered Files:

- FCC-08-281A2.PDF
- FCC-08-281A3.PDF
- FCC-08-281A2.XLS
- FCC-08-281A3.XLS

Content Overview:

- Detailed lists of television stations in various US cities, with information such as:
  - **Call signs** (e.g., KAKM, KIMO, KTUU-TV)
  - **Location** (city, state)
  - **Analog and digital channel numbers** (pre- and post-transition)
  - **Station type** (PBS, ABC, NBC, CBS)
- Coverage of multiple regions including **Alaska (Anchorage, Fairbanks, Juneau)** and **Alabama (Birmingham, Dothan, Huntsville-Decatur-Florence)**.

- Excel spreadsheets captured structured tables, making it easier to analyze numeric and categorical data programmatically.



Federal Communications Commission FCC 08-281

APPENDIX A – Initial List of Stations Eligible for Analog Nightlight Program

Market	Facility ID	Call sign	City	ST	Analog	Digital	Anlg Ch.	Post Transition DTV Ch.	Pre Transition DTV Ch. (*)	Status of Analog
Anchorage, AK	804	KAKM	Anchorage	AK	PBS	PBS	7	8		
Anchorage, AK	13815	KIMO	Anchorage	AK	ABC	ABC	13	12		
Anchorage, AK	10173	KTUU-TV	Anchorage	AK	NBC	NBC	2	10		
Anchorage, AK	4983	KYUK-TV	Bethel	AK			4	3		
Fairbanks, AK	13813	KATN	Fairbanks	AK	ABC	ABC	2	18		
Fairbanks, AK	20015	KJNP-TV	North Pole	AK			4	20		
Fairbanks, AK	49621	KTVF	Fairbanks	AK	NBC	NBC	11	26		
Fairbanks, AK	69315	KUAC-TV	Fairbanks	AK			9	9	24	
Juneau, AK	8651	KTOO-TV	Juneau	AK	PBS	PBS	3	10		
Juneau, AK	60520	KUBD	Ketchikan	AK	CBS	CBS	4	13		
Birmingham, AL	71325	WDBB	Bessemer	AL			17	18		
Dothan, AL	43846	WDHN	Dothan	AL	ABC	ABC	18	21		
Huntsville-Decatur-Florence, AL	57292	WAAY-TV	Huntsville	AL	ABC	ABC	31	32		
Montgomery, AL	714	WDIQ	Dozier	AL	PBS	PBS	2	10		
Ft. Smith-Fayetteville-Springdale-Rogers, AR	66469	KFSM-TV	Fort Smith	AR	CBS	CBS	5	18		
Ft. Smith-Fayetteville-Springdale-Rogers, AR	60354	KHOG-TV	Fayetteville	AR	ABC	ABC	29	15		
Little Rock-Pine Bluff, AR	33440	KARK-TV	Little Rock	AR	NBC	NBC	4	32		
Little Rock-Pine Bluff, AR	2770	KETS	Little Rock	AR	PBS	PBS	2	7		Terminating 1/3/09
Little Rock-Pine Bluff, AR	11951	KLRT-TV	Little Rock	AR	Fox	Fox	16	30		
Little Rock-Pine Bluff, AR	37005	KWBF	Little Rock	AR			42	44		Reduced 10/31/08
Phoenix, AZ	41223	KPHO-TV	Phoenix	AZ	CBS	CBS	5	17		
Phoenix, AZ	40993	KTVK	Phoenix	AZ			3	24		
Phoenix, AZ	68886	KUTP	Phoenix	AZ			45	26		
Tucson, AZ	81441	KFTU-TV	Douglas	AZ			3	36		
Tucson, AZ	30601	KHRR	Tucson	AZ			40	40	42	
Tucson, AZ	2731	KUAT-TV	Tucson	AZ	PBS	PBS	6	30		
Tucson, AZ	25735	KVOA	Tucson	AZ	NBC	NBC	4	23		

Fig. 3.5

Key Observations:

- These documents provide a **snapshot of the DTV transition**, including pre- and post-transition channels, and highlight the stations' broadcasting status.
- They confirm the USB drive contained **US Government-related data**, aligning with the task objective of recovering such files.
- These files are essential for **demonstrating recovered evidence** from government sources.
- Serve as a **primary source for analyzing historical FCC operations** related to the DTV transition.
- Aid in illustrating the user's activity on the device, confirming **access to and download of official documents**.

3.6 Recovered FCC Statements

Among the recovered files, a **PDF containing a formal statement from Commissioner Robert M. McDowell** of the Federal Communications Commission (FCC) was identified. This document pertained to the **implementation of the Short-term Analog Flash and Emergency Readiness (SAFER) Act** and the establishment of the **DTV Transition "Analog Nightlight" Program** (MB Docket No. 08-255).

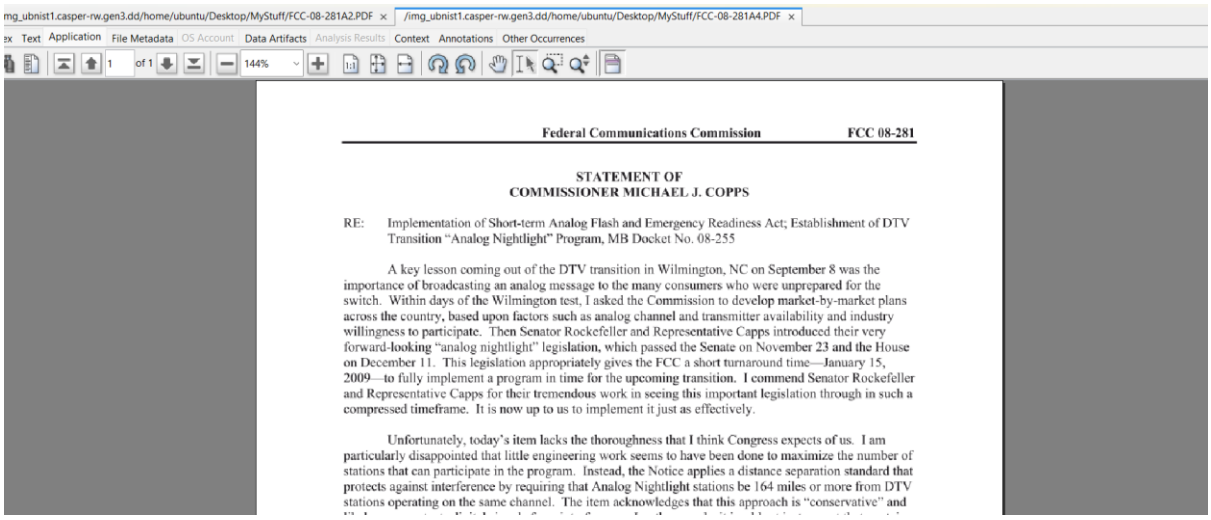
Key Contents of the Document:

- The statement outlines support for a program allowing **full-power television stations to continue limited analog broadcasts** after the February 17, 2009, digital transition deadline.
- Provides guidance for **helping households unprepared for the DTV transition**, particularly those relying on analog antennas.
- Emphasizes the role of **"Analog Nightlight" programming** in providing practical assistance, such as obtaining converter boxes and re-positioning antennas.
  Highlights potential **technical challenges** in communities with no stations eligible for nightlight service and encourages stations to **submit engineering showings** to ensure service availability.

Significance:

- Demonstrates that the USB drive contained **official US Government communications**, confirming activity related to government downloads.
- Serves as evidence of **access to FCC directives** concerning national television infrastructure changes.

Complements other recovered FCC files, such as Excel and PDF documents with station-level DTV transition data, providing a **comprehensive picture of the user's engagement with government sources**.



Federal Communications Commission FCC 08-281

STATEMENT OF
COMMISSIONER MICHAEL J. COPPS

RE: Implementation of Short-term Analog Flash and Emergency Readiness Act; Establishment of DTV Transition "Analog Nightlight" Program, MB Docket No. 08-255

A key lesson coming out of the DTV transition in Wilmington, NC on September 8 was the importance of broadcasting an analog message to the many consumers who were unprepared for the switch. Within days of the Wilmington test, I asked the Commission to develop market-by-market plans across the country, based upon factors such as analog channel and transmitter availability and industry willingness to participate. Then Senator Rockefeller and Representative Capps introduced their very forward-looking "analog nightlight" legislation, which passed the Senate on November 23 and the House on December 11. This legislation appropriately gives the FCC a short turnaround time—January 15, 2009—to fully implement a program in time for the upcoming transition. I commend Senator Rockefeller and Representative Capps for their tremendous work in seeing this important legislation through in such a compressed timeframe. It is now up to us to implement it just as effectively.

Unfortunately, today's item lacks the thoroughness that I think Congress expects of us. I am particularly disappointed that little engineering work seems to have been done to maximize the number of stations that can participate in the program. Instead, the Notice applies a distance separation standard that protects against interference by requiring that Analog Nightlight stations be 164 miles or more from DTV stations operating on the same channel. The item acknowledges that this approach is "conservative" and

Fig. 3.6

3.7 Additional Recovered FCC Statement

A second PDF was recovered containing a formal statement from **Commissioner Jonathan S. Adelstein** of the Federal Communications Commission (FCC), related to the **Short-term**

Analog Flash and Emergency Readiness (SAFER) Act and the **DTV Transition "Analog Nightlight" Program** (MB Docket No. 08-255).

Key Contents of the Document:

- Highlights the **importance of an analog nightlight program** for full-power television stations to broadcast DTV-related and emergency information after the digital transition deadline (February 17, 2009).
- Praises the **cooperation of Congress, broadcasters, cable and satellite operators, and community groups** in implementing the program swiftly.
- Notes that only **136 out of 210 television markets** had stations initially approved for participation.
- Encourages other stations to **volunteer for the nightlight program**, ensuring that households unprepared for the transition receive crucial information.
- Emphasizes the role of **participating stations as a "lifeline"** for over-the-air reliant households during the post-DTV transition period.

Significance:

- Confirms that the USB drive contained multiple official FCC communications, reinforcing the presence of **government-related files**.
- Provides additional context about the **implementation and outreach strategy** for the DTV transition, complementing other recovered documents such as station-level data (PDFs, XLS).
- Maintains integrity as a **forensically sound PDF**, preserving all original formatting and timestamps.

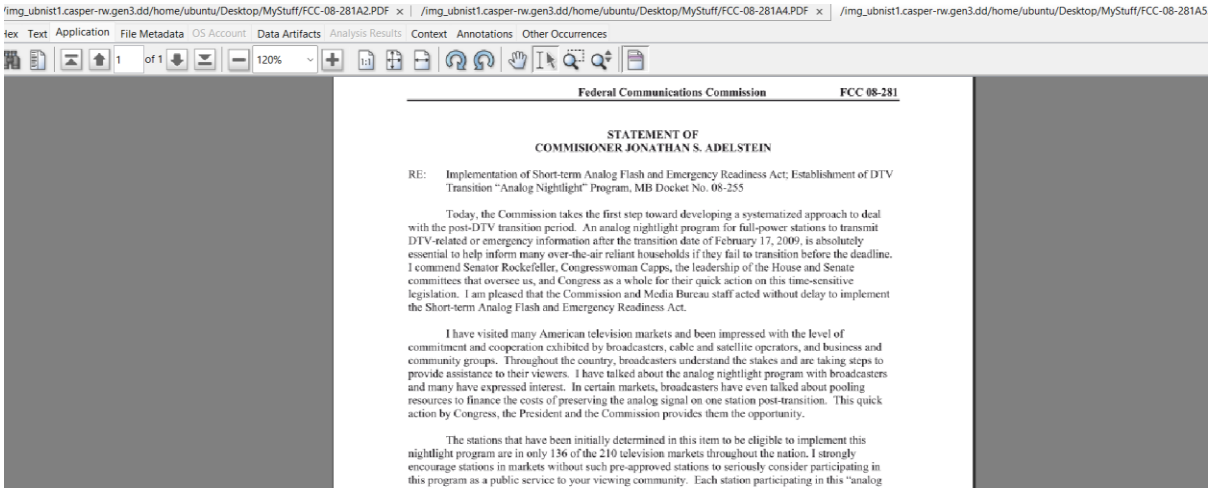


Fig. 3.7

4. Conclusion

Through this task, I was able to experience first-hand the process of digital forensic investigation on a Linux-based flash drive. By analyzing multiple images of the casper-rw file from a 2GB Ubuntu USB, I reconstructed the filesystem, identified and recovered deleted files, and traced documents containing references to US Government sources. The combination of **Autopsy** for a graphical, intuitive overview and **The Sleuth Kit (TSK)** for precise command-line operations allowed me to explore the filesystem thoroughly, ensuring that important evidence was not overlooked.

Recovering files from a live-used USB highlighted how data persists even after deletion and reinforced the critical importance of proper forensic procedures. Organizing recovered files and logs into dedicated folders, and carefully extracting metadata, timestamps, and file paths, emphasized the need for **methodical documentation** to maintain clarity and reproducibility in investigations.

This task not only strengthened my technical skills but also enhanced my **analytical thinking**, showing how multiple tools and approaches can be integrated to build a complete picture from fragmented data. Beyond the technical recovery, examining real documents like FCC reports gave me insight into how digital evidence can hold contextual value, linking digital artifacts to real-world actions and policies.

Key Learning Outcomes (Humanized):

1. **Seeing Beyond the Surface:** I learned that deleted files aren't necessarily gone—they leave traces, and with the right tools, you can recover and make sense of them.
2. **Understanding the Filesystem:** Exploring the Ext3 filesystem made me appreciate the structure behind every file, how inodes work, and how data persists even when it seems deleted.
3. **Tool Mastery in Practice:** Working with both Autopsy and TSK taught me when a GUI makes analysis faster, and when command-line precision is necessary.
4. **Organizing Chaos:** Creating folders for logs, file listings, and recovered documents reinforced that **good organization is crucial** in forensic work to avoid confusion and mistakes.
5. **Connecting Data to Reality:** Recovering government reports and identifying meaningful content showed me that forensic work is not just about numbers or files—it's about **connecting digital traces to real-world events**.
6. **Attention to Detail:** Every timestamp, file path, and deleted document mattered, reminding me that **thoroughness is key** in investigations.
7. **Confidence in Reporting:** Documenting methodology, results, and findings in a structured way taught me how to communicate technical work **clearly and professionally** to others.

Overall, this task provided a **hands-on understanding of digital forensics**, blending technical skill, investigative thinking, and real-world context. It strengthened my ability to recover, analyze, and present digital evidence in a structured, meaningful way—a core skill for any aspiring digital forensic professional.

5. References

1. **Autopsy Digital Forensic Platform** – SleuthKit & Autopsy Official Website: https://www.sleuthkit.org/autopsy/

2. **The Sleuth Kit (TSK)** – Command-line Digital Forensic Tools: https://www.sleuthkit.org/sleuthkit/

3. Microsoft Sysinternals – Strings Utility: https://learn.microsoft.com/en-us/sysinternals/downloads/strings

4. Ubuntu Package Repository & Documentation: https://packages.ubuntu.com/

5. Digital Corpora – NPS 2009 Casper-RW Images: https://digitalcorpora.s3.amazonaws.com/s3_browser.html#corpora/drives/nps-2009-casper-rw/

6. Digital Corpora – NPS 2009 Casper-RW Narrative File: https://digitalcorpora.s3.amazonaws.com/corpora/drives/nps-2009-casper-rw/narrative.txt