Introduction and Purpose

This project focused on developing a way to make forensic analysis easier for beginners, allowing automation and user intractability, with a clean organized output. Our project is a bash-based tool that uses a popular forensic analysis tool called Sleuth Kit as the backend. The reason this tool was created was due to the complexity of the many forensic tools that are in the industry. Though impressive, many services that are used in digital forensics are difficult for beginners, causing problems like slower investigations, inconsistencies, inorganization, and many inaccuracies. We aim to improve those adversities by writing a script that wraps Sleuth Kit into an interactable guide that walks beginners through what they want to do to certain disk images to gather their metadata for analysis.

Users of this tool do not need to have knowledge of Sleuth Kit to start gathering data off an image as the script uses simple message selection to point to a Sleuth Kit command that will work in the backend. Running our tool gives a selection page with a list of 10 options (Appendix 1A). The tool mentions that there is no loaded image and says to load it with option 1. Following loading an image, an output directory can be written by the user for organization. The other options range from listing all files, searching for deleted files, running complete analysis, and many more. Additionally, there is a help option with documentation discussing the workflow and use cases, details on the output and supported formats, and the requirements for running (Appendix 2A). Once the user is satisfied with their selection of outputs, they can quit the tool as each option saved metadata to a new file created where they selected previously.

Technical Implementation

The tool we've created was split into two parts developed using Python. The main part is the forensic engine toolkit with scripts deploying commands from Sleuth kit (Appendix 1B). The other is an interactive menu front-end script, developed to help the user gather the data they need from a disk image (Appendix 2B). Both scripts work together to automate commands and store the output in structured formats, eliminating the need for a user to manually enter Sleuth kit commands.

Backend

The main script is designed around a ForensicToolkit class containing many different operations from Sleuth Kit. Specifically, our tool touches on fsstat for filesystem analysis, fls for file enumeration, istat for detailed inode metadata, mmls for partition analysis, icat for file recovery, and fls –d for deleted files. Each operation is implemented as a standalone function, and the backend provides standardized return formats and error handling routines (Appendix 3B). This script is also responsible for generating structured files such as CSVs and JSON reports using standard Python libraries. Additionally, it timestamps all output files for organization and archival consistency.

Frontend

The front end consists of the menu script that manages user interaction through a guided menu-based system. It presents users with numbered options, performs input validation, and calls the corresponding ForensicToolkit methods. The menu provides options to load a disk image, configure output location, run individual Sleuth Kit modules, recover files, and generate a complete report (Appendix 2B). The frontend also includes a help & documentation system, built-in validation of file paths, and automated directory creation. A user can proceed through the entire workflow without manually learning Sleuth Kit commands or syntax.

HTML Version

Additionally, we’ve developed a version of our script specifically to dump all available selections on our options screen to an HTML report. This report contains summarized information of all categories in a simple, colorized format that's easy to read. The file contains totals on overall files, deleted files, partitions, and timeline entries. Detailed information about which deleted files can be recoverable is displayed along with reallocated files that were probably overwritten. It also contains a dump of the filesystem information, detailing the OS version with timeline dates and metadata summaries. Lastly, it has a list of files having a directory path structure with data like permissions and sizes (Appendix 4, 5 & 6B).

Tools and Dependencies

Using this tool requires a few dependencies, specifically the Sleuth kit suite, Python3 and its standard libraries, a readable disk image, and a usable Linux client. Wrapping these tools in Python scripts replicates the behavior of professional forensic workflows such as case output separations, artifact organization, and chain-of-custody style report exports.

Results

Our tool successfully automates the Sleuth Kit workflow and supports multiple forensic tasks that normally require extensive command-line knowledge. Testing was performed on an old free of use Ubuntu disk image, ubnist1.casper-rw.gen3.E01. and confirmed results such as full analysis pipeline through a single menu, modular data extraction for isolated traversal, deleted file recovery detection, CSV and JSON outputs are formatted in readable formats though still raw and basic. Each action produces its own output file with timestamps and uses file names that reflect what the command was used (Appendix 1 - 5C).

Limitations and Future Improvements

Some improvements we would like to see if the tool is continued in the future is integration with GUI using the generated JSON files to create an interactive web interface via JavaScript and HTML. Implementing an option for verbose output and keyword searching of files within the image. Additionally, hashing specific files or automatic hashing for checksums to be used for security purposes. These extensions will benefit even more beginners to learn and have an easy time analyzing data for forensic investigations.

Conclusion & Lessons Learned

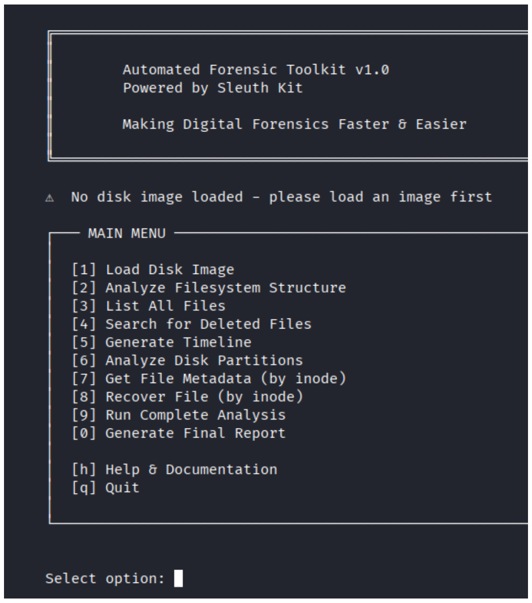
Reflecting on the hardships of building this tool, diverting from building our own forensic tool, into using a popular tool as a backend benefited our timeline and success of developing this tool. What didn't work with our tool was any decrypting methods on disk images. Thus, if any images were encrypted with a high entropy, our tool will not work to output any partitions or deleted files from the disk image.

With that being said, our automated forensic toolkit successfully met its primary objective of simplifying Sleuth Kit usage while preserving its investigative power. Through its automation, menu-driven workflows, and output organization, the tool provides a viable forensic analysis platform for students and beginner analysts. It combines commonly used Sleuth Kit commands into a single automated script, reducing errors, eliminating excessive manual terminal interaction, and thus accelerated forensic tasks.

The final version of this tool is able to generate structured reports, recover deleted files, enumerate filesystems, and produce timelines. It also maintains a clean user experience while supporting advanced operations with inode-based analysis.

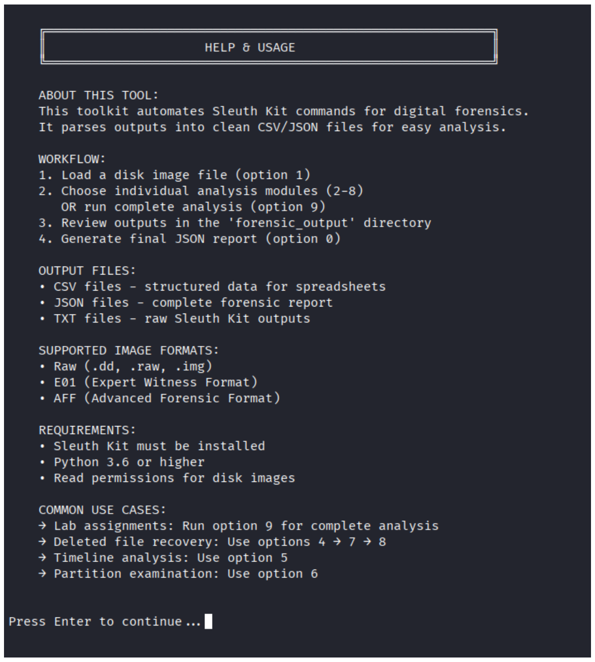
Appendix

A. Introduction and Purpose



```
        Automated Forensic Toolkit v1.0
        Powered by Sleuth Kit

        Making Digital Forensics Faster & Easier

⚠  No disk image loaded - please load an image first

┌─ MAIN MENU ─
│
│  [1] Load Disk Image
│  [2] Analyze Filesystem Structure
│  [3] List All Files
│  [4] Search for Deleted Files
│  [5] Generate Timeline
│  [6] Analyze Disk Partitions
│  [7] Get File Metadata (by inode)
│  [8] Recover File (by inode)
│  [9] Run Complete Analysis
│  [0] Generate Final Report
│
│  [h] Help & Documentation
│  [q] Quit
│
└─

Select option:
```

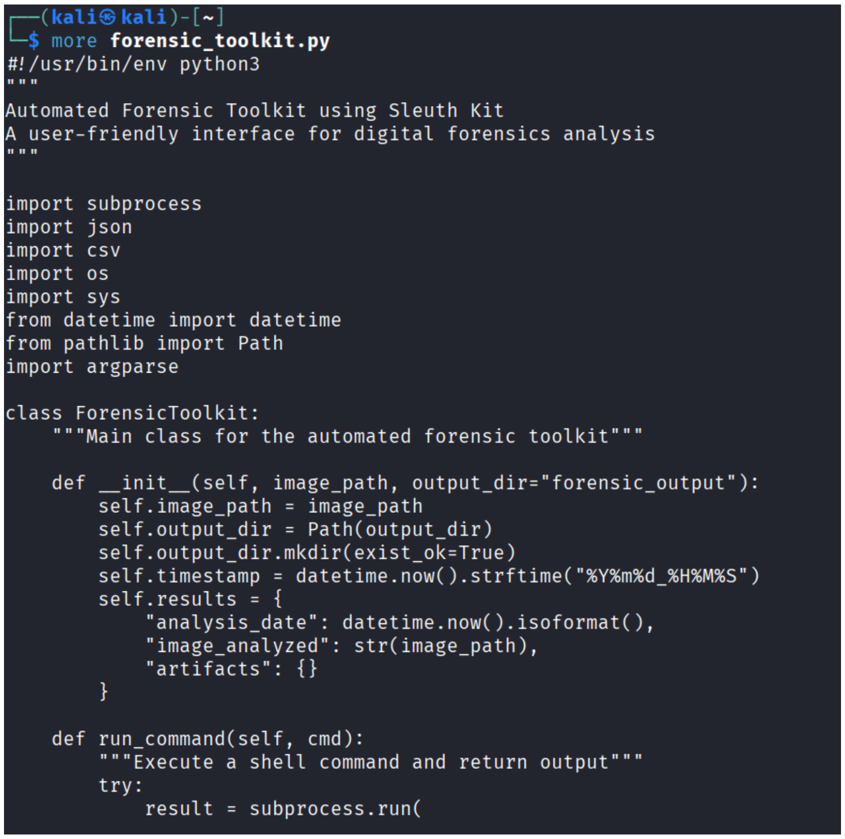
Figure 1. Tool landing page.



```
                    HELP & USAGE

ABOUT THIS TOOL:
This toolkit automates Sleuth Kit commands for digital forensics.
It parses outputs into clean CSV/JSON files for easy analysis.

WORKFLOW:
1. Load a disk image file (option 1)
2. Choose individual analysis modules (2-8)
   OR run complete analysis (option 9)
3. Review outputs in the 'forensic_output' directory
4. Generate final JSON report (option 0)

OUTPUT FILES:
• CSV files - structured data for spreadsheets
• JSON files - complete forensic report
• TXT files - raw Sleuth Kit outputs

SUPPORTED IMAGE FORMATS:
• Raw (.dd, .raw, .img)
• E01 (Expert Witness Format)
• AFF (Advanced Forensic Format)

REQUIREMENTS:
• Sleuth Kit must be installed
• Python 3.6 or higher
• Read permissions for disk images

COMMON USE CASES:
→ Lab assignments: Run option 9 for complete analysis
→ Deleted file recovery: Use options 4 → 7 → 8
→ Timeline analysis: Use option 5
→ Partition examination: Use option 6

Press Enter to continue...
```

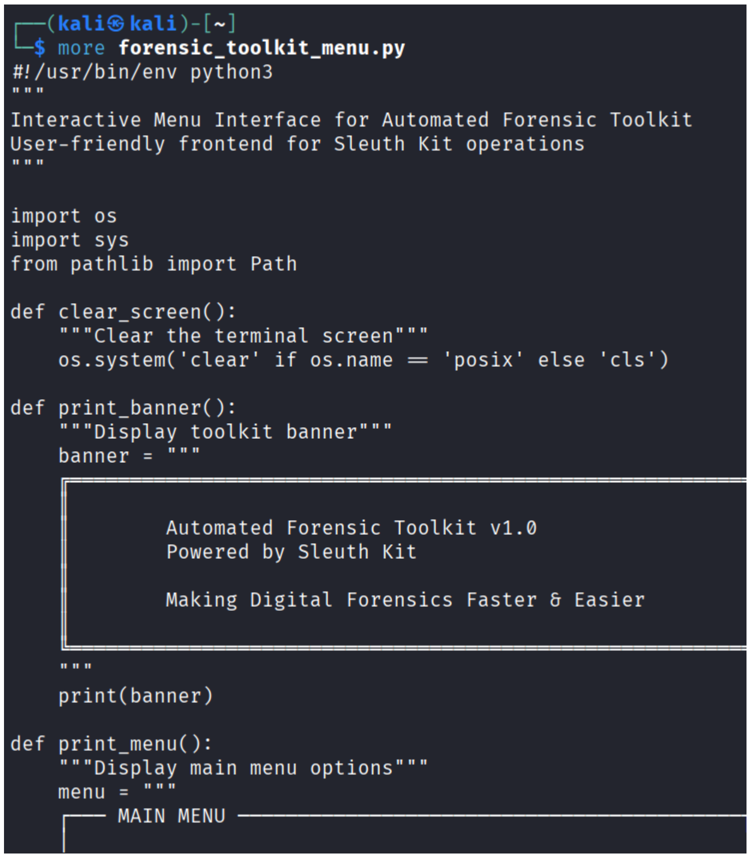
Figure 2. Help and Documentation option output.

B. Technical Integration



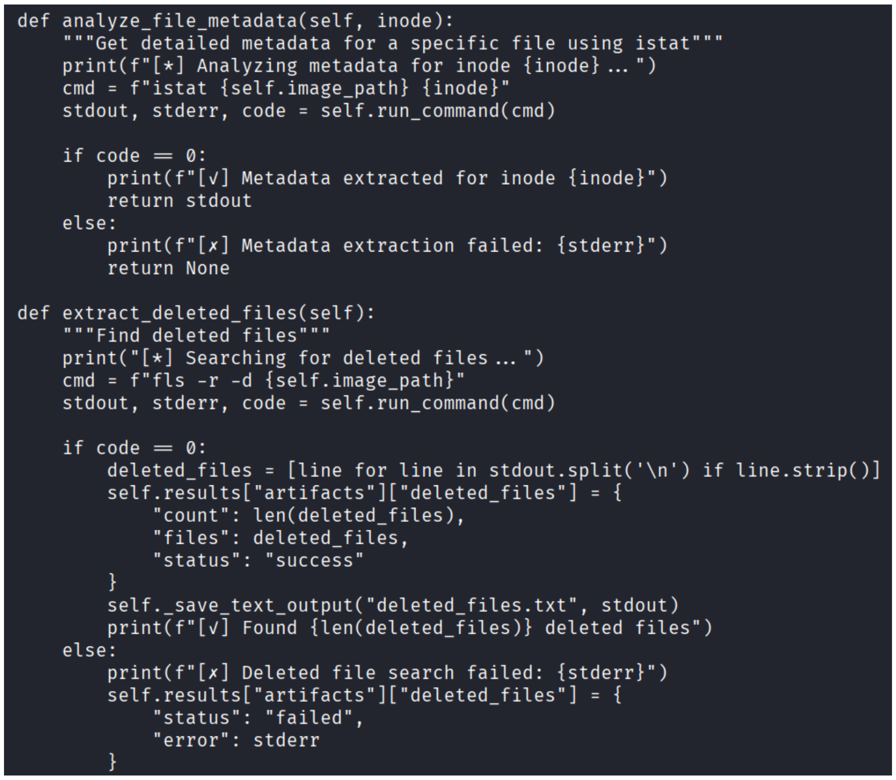
```
┌──(kali㉿kali)-[~]
└─$ more forensic_toolkit.py
#!/usr/bin/env python3
"""
Automated Forensic Toolkit using Sleuth Kit
A user-friendly interface for digital forensics analysis
"""

import subprocess
import json
import csv
import os
import sys
from datetime import datetime
from pathlib import Path
import argparse

class ForensicToolkit:
    """Main class for the automated forensic toolkit"""

    def __init__(self, image_path, output_dir="forensic_output"):
        self.image_path = image_path
        self.output_dir = Path(output_dir)
        self.output_dir.mkdir(exist_ok=True)
        self.timestamp = datetime.now().strftime("%Y%m%d_%H%M%S")
        self.results = {
            "analysis_date": datetime.now().isoformat(),
            "image_analyzed": str(image_path),
            "artifacts": {}
        }

    def run_command(self, cmd):
        """Execute a shell command and return output"""
        try:
            result = subprocess.run(
```

Figure 1. Code snippet of main forensic tool.



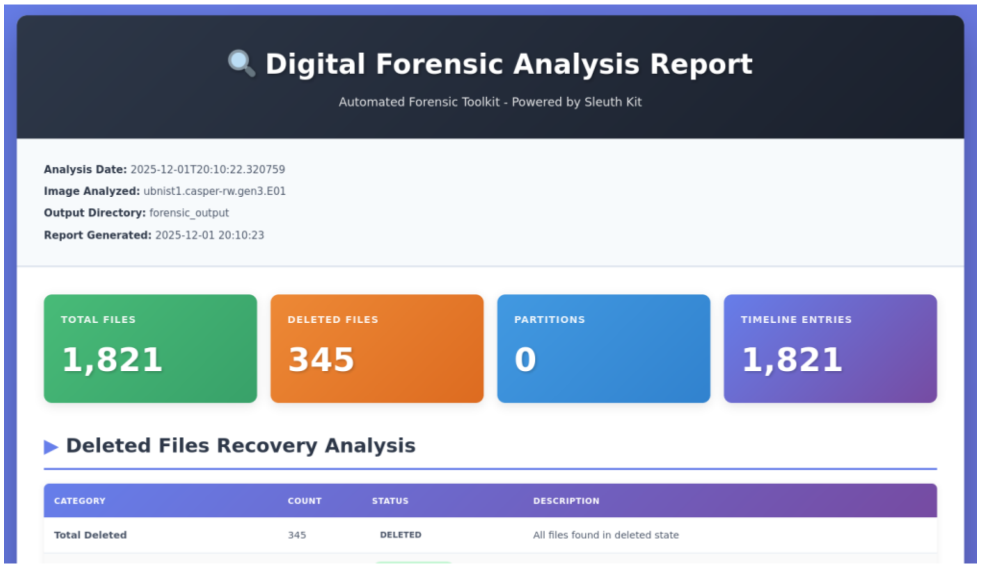
```
┌──(kali㉿kali)-[~]
└─$ more forensic_toolkit_menu.py
#!/usr/bin/env python3
"""
Interactive Menu Interface for Automated Forensic Toolkit
User-friendly frontend for Sleuth Kit operations
"""

import os
import sys
from pathlib import Path

def clear_screen():
    """Clear the terminal screen"""
    os.system('clear' if os.name == 'posix' else 'cls')

def print_banner():
    """Display toolkit banner"""
    banner = """
    ╔══════════════════════════════════════════════════════
    ║
    ║        Automated Forensic Toolkit v1.0
    ║        Powered by Sleuth Kit
    ║
    ║        Making Digital Forensics Faster & Easier
    ║
    ╚══════════════════════════════════════════════════════
    """
    print(banner)

def print_menu():
    """Display main menu options"""
    menu = """
    ┌──── MAIN MENU ───────────────────────────────────────
    │
```

Figure 2. *Code snippet of the forensic tool menu.*



```python
def analyze_file_metadata(self, inode):
    """Get detailed metadata for a specific file using istat"""
    print(f"[*] Analyzing metadata for inode {inode}...")
    cmd = f"istat {self.image_path} {inode}"
    stdout, stderr, code = self.run_command(cmd)

    if code == 0:
        print(f"[✓] Metadata extracted for inode {inode}")
        return stdout
    else:
        print(f"[✗] Metadata extraction failed: {stderr}")
        return None

def extract_deleted_files(self):
    """Find deleted files"""
    print("[*] Searching for deleted files...")
    cmd = f"fls -r -d {self.image_path}"
    stdout, stderr, code = self.run_command(cmd)

    if code == 0:
        deleted_files = [line for line in stdout.split('\n') if line.strip()]
        self.results["artifacts"]["deleted_files"] = {
            "count": len(deleted_files),
            "files": deleted_files,
            "status": "success"
        }
        self._save_text_output("deleted_files.txt", stdout)
        print(f"[✓] Found {len(deleted_files)} deleted files")
    else:
        print(f"[✗] Deleted file search failed: {stderr}")
        self.results["artifacts"]["deleted_files"] = {
            "status": "failed",
            "error": stderr
        }
```

Figure 3. Code example of two operations.



🔍 Digital Forensic Analysis Report

Automated Forensic Toolkit - Powered by Sleuth Kit

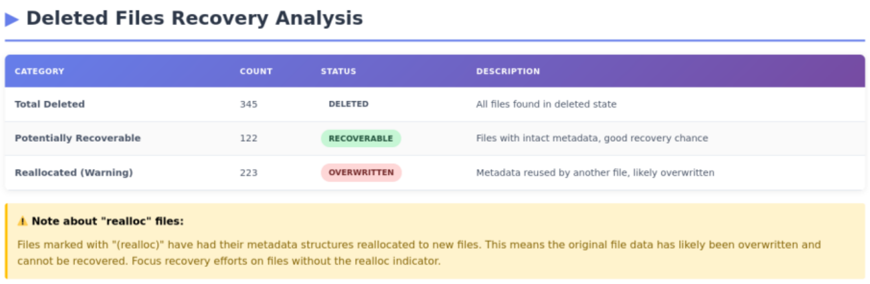
Analysis Date: 2025-12-01T20:10:22.320759
Image Analyzed: ubnist1.casper-rw.gen3.E01
Output Directory: forensic_output
Report Generated: 2025-12-01 20:10:23

TOTAL FILES	DELETED FILES	PARTITIONS	TIMELINE ENTRIES
1,821	345	0	1,821

▶ Deleted Files Recovery Analysis

CATEGORY	COUNT	STATUS	DESCRIPTION
Total Deleted	345	DELETED	All files found in deleted state

Figure 4. HTML output of script

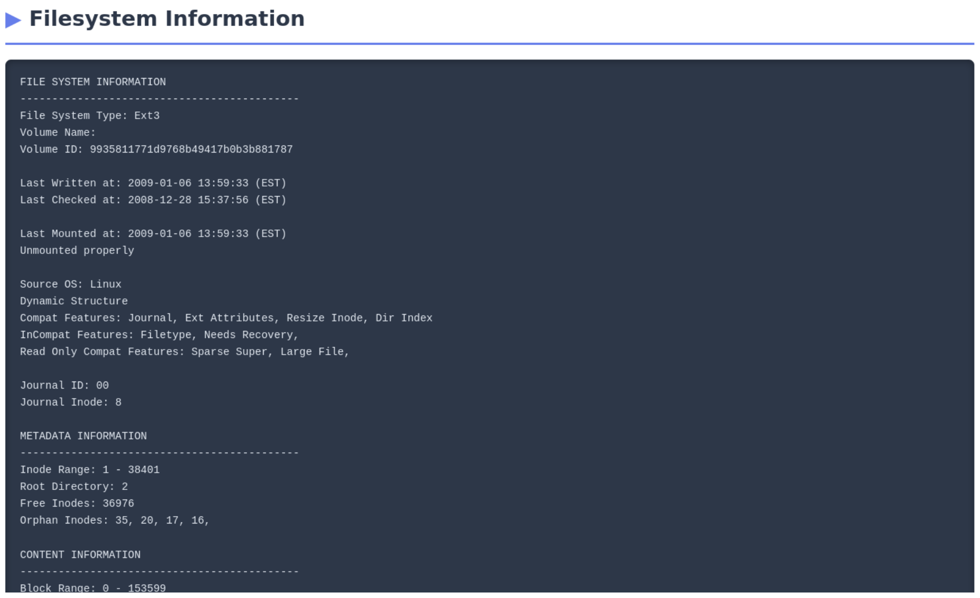


▶ **Deleted Files Recovery Analysis**

CATEGORY	COUNT	STATUS	DESCRIPTION
Total Deleted	345	DELETED	All files found in deleted state
Potentially Recoverable	122	RECOVERABLE	Files with intact metadata, good recovery chance
Reallocated (Warning)	223	OVERWRITTEN	Metadata reused by another file, likely overwritten

⚠ **Note about "realloc" files:**
Files marked with "(realloc)" have had their metadata structures reallocated to new files. This means the original file data has likely been overwritten and cannot be recovered. Focus recovery efforts on files without the realloc indicator.

Figure 5. Deleted section detailing what's recoverable.

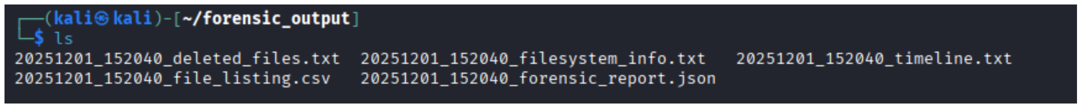


▶ **Filesystem Information**

```
FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: Ext3
Volume Name:
Volume ID: 9935811771d9768b49417b0b3b881787

Last Written at: 2009-01-06 13:59:33 (EST)
Last Checked at: 2008-12-28 15:37:56 (EST)

Last Mounted at: 2009-01-06 13:59:33 (EST)
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
```

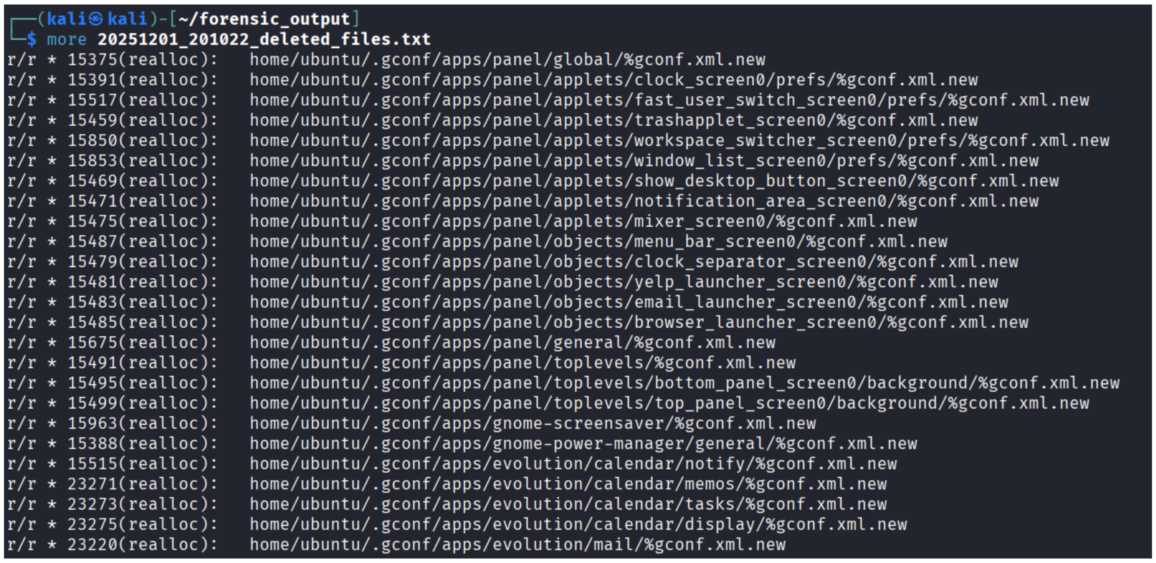
Figure 6. OS system information output on HTML.

C. Results



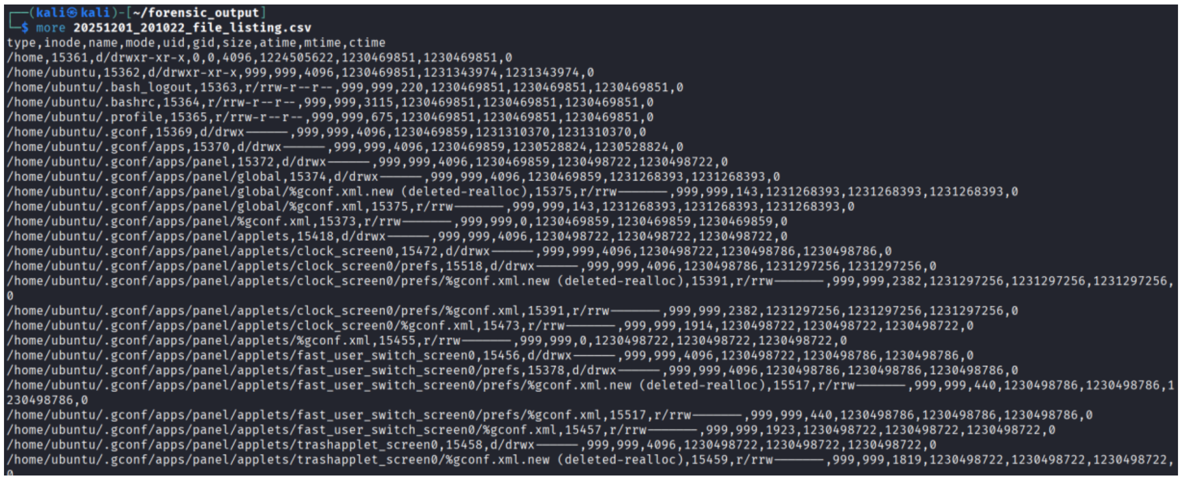
```
┌──(kali㉿kali)-[~/forensic_output]
└─$ ls
20251201_152040_deleted_files.txt  20251201_152040_filesystem_info.txt   20251201_152040_timeline.txt
20251201_152040_file_listing.csv   20251201_152040_forensic_report.json
```

Figure 1. Output in raw formats.



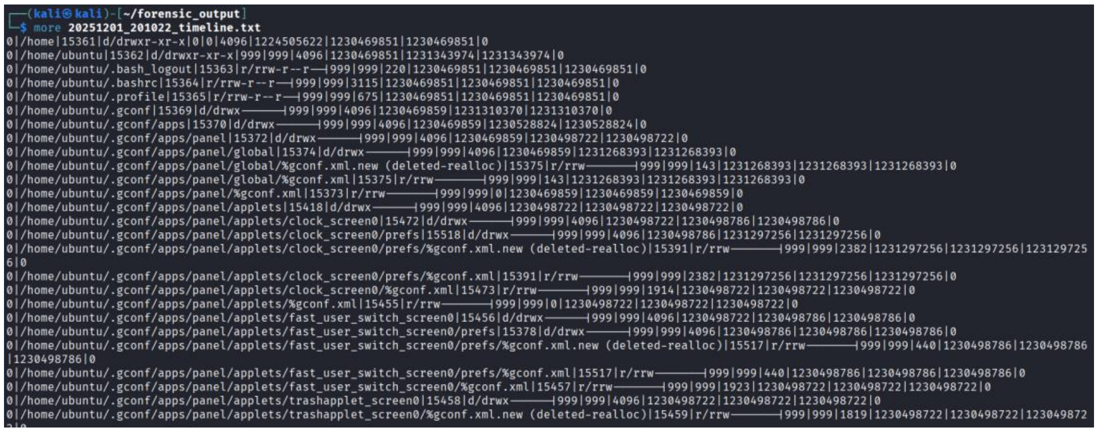
```
┌──(kali㉿kali)-[~/forensic_output]
└─$ more 20251201_201022_deleted_files.txt
r/r * 15375(realloc):   home/ubuntu/.gconf/apps/panel/global/%gconf.xml.new
r/r * 15391(realloc):   home/ubuntu/.gconf/apps/panel/applets/clock_screen0/prefs/%gconf.xml.new
r/r * 15517(realloc):   home/ubuntu/.gconf/apps/panel/applets/fast_user_switch_screen0/prefs/%gconf.xml.new
r/r * 15459(realloc):   home/ubuntu/.gconf/apps/panel/applets/trashapplet_screen0/%gconf.xml.new
r/r * 15850(realloc):   home/ubuntu/.gconf/apps/panel/applets/workspace_switcher_screen0/prefs/%gconf.xml.new
r/r * 15853(realloc):   home/ubuntu/.gconf/apps/panel/applets/window_list_screen0/prefs/%gconf.xml.new
r/r * 15469(realloc):   home/ubuntu/.gconf/apps/panel/applets/show_desktop_button_screen0/%gconf.xml.new
r/r * 15471(realloc):   home/ubuntu/.gconf/apps/panel/applets/notification_area_screen0/%gconf.xml.new
r/r * 15475(realloc):   home/ubuntu/.gconf/apps/panel/applets/mixer_screen0/%gconf.xml.new
r/r * 15487(realloc):   home/ubuntu/.gconf/apps/panel/objects/menu_bar_screen0/%gconf.xml.new
r/r * 15479(realloc):   home/ubuntu/.gconf/apps/panel/objects/clock_separator_screen0/%gconf.xml.new
r/r * 15481(realloc):   home/ubuntu/.gconf/apps/panel/objects/yelp_launcher_screen0/%gconf.xml.new
r/r * 15483(realloc):   home/ubuntu/.gconf/apps/panel/objects/email_launcher_screen0/%gconf.xml.new
r/r * 15485(realloc):   home/ubuntu/.gconf/apps/panel/objects/browser_launcher_screen0/%gconf.xml.new
r/r * 15675(realloc):   home/ubuntu/.gconf/apps/panel/general/%gconf.xml.new
r/r * 15491(realloc):   home/ubuntu/.gconf/apps/panel/toplevels/%gconf.xml.new
r/r * 15495(realloc):   home/ubuntu/.gconf/apps/panel/toplevels/bottom_panel_screen0/background/%gconf.xml.new
r/r * 15499(realloc):   home/ubuntu/.gconf/apps/panel/toplevels/top_panel_screen0/background/%gconf.xml.new
r/r * 15963(realloc):   home/ubuntu/.gconf/apps/gnome-screensaver/%gconf.xml.new
r/r * 15388(realloc):   home/ubuntu/.gconf/apps/gnome-power-manager/general/%gconf.xml.new
r/r * 15515(realloc):   home/ubuntu/.gconf/apps/evolution/calendar/notify/%gconf.xml.new
r/r * 23271(realloc):   home/ubuntu/.gconf/apps/evolution/calendar/memos/%gconf.xml.new
r/r * 23273(realloc):   home/ubuntu/.gconf/apps/evolution/calendar/tasks/%gconf.xml.new
r/r * 23275(realloc):   home/ubuntu/.gconf/apps/evolution/calendar/display/%gconf.xml.new
r/r * 23220(realloc):   home/ubuntu/.gconf/apps/evolution/mail/%gconf.xml.new
```

Figure 2. Deleted files output.



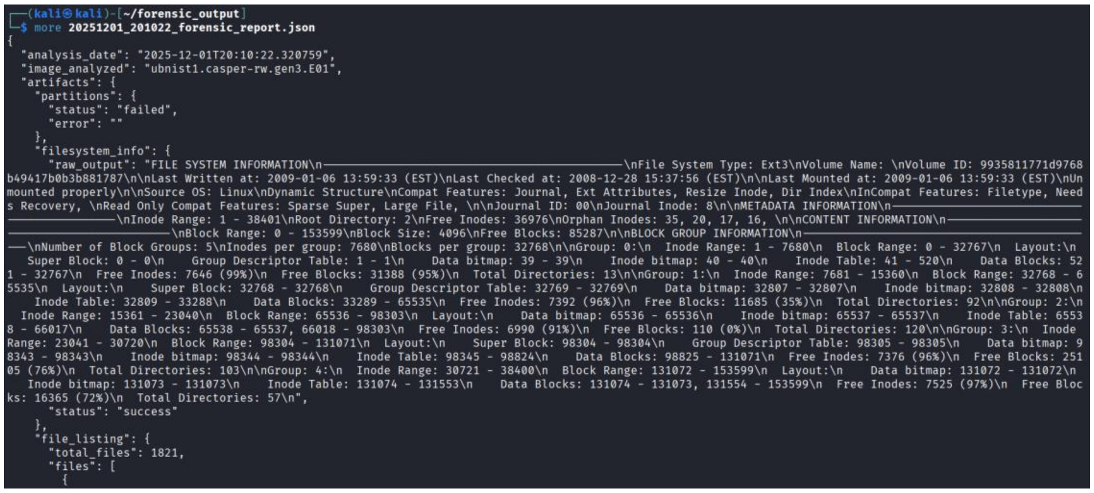
```
┌──(kali㉿kali)-[~/forensic_output]
└─$ more 20251201_201022_file_listing.csv
type,inode,name,mode,uid,gid,size,atime,mtime,ctime
/home,15361,d/drwxr-xr-x,0,0,4096,1224505622,1230469851,1230469851,0
/home/ubuntu,15362,d/drwxr-xr-x,999,999,4096,1230469851,1231343974,1231343974,0
/home/ubuntu/.bash_logout,15363,r/rrw-r--r--,999,999,220,1230469851,1230469851,1230469851,0
/home/ubuntu/.bashrc,15364,r/rrw-r--r--,999,999,3115,1230469851,1230469851,1230469851,0
/home/ubuntu/.profile,15365,r/rrw-r--r--,999,999,675,1230469851,1230469851,1230469851,0
/home/ubuntu/.gconf,15369,d/drwx------,999,999,4096,1230469859,1231310370,1231310370,0
/home/ubuntu/.gconf/apps,15370,d/drwx------,999,999,4096,1230469859,1230528824,1230528824,0
/home/ubuntu/.gconf/apps/panel,15372,d/drwx------,999,999,4096,1230469859,1230498722,1230498722,0
/home/ubuntu/.gconf/apps/panel/global,15374,d/drwx------,999,999,4096,1230469859,1231268393,1231268393,0
/home/ubuntu/.gconf/apps/panel/global/%gconf.xml.new (deleted-realloc),15375,r/rrw-------,999,999,143,1231268393,1231268393,1231268393,0
/home/ubuntu/.gconf/apps/panel/global/%gconf.xml,15375,r/rrw-------,999,999,143,1231268393,1231268393,1231268393,0
/home/ubuntu/.gconf/apps/panel/%gconf.xml,15373,r/rrw-------,999,999,0,1230469859,1230469859,1230469859,0
/home/ubuntu/.gconf/apps/panel/applets,15418,d/drwx------,999,999,4096,1230498722,1230498722,1230498722,0
/home/ubuntu/.gconf/apps/panel/applets/clock_screen0,15472,d/drwx------,999,999,4096,1230498722,1230498786,1230498786,0
/home/ubuntu/.gconf/apps/panel/applets/clock_screen0/prefs,15518,d/drwx------,999,999,4096,1230498786,1231297256,1231297256,0
/home/ubuntu/.gconf/apps/panel/applets/clock_screen0/prefs/%gconf.xml.new (deleted-realloc),15391,r/rrw-------,999,999,2382,1231297256,1231297256,1231297256,
0
/home/ubuntu/.gconf/apps/panel/applets/clock_screen0/prefs/%gconf.xml,15391,r/rrw-------,999,999,2382,1231297256,1231297256,1231297256,0
/home/ubuntu/.gconf/apps/panel/applets/clock_screen0/%gconf.xml,15473,r/rrw-------,999,999,1914,1230498722,1230498722,1230498722,0
/home/ubuntu/.gconf/apps/panel/applets/%gconf.xml,15455,r/rrw-------,999,999,0,1230498722,1230498722,1230498722,0
/home/ubuntu/.gconf/apps/panel/applets/fast_user_switch_screen0,15456,d/drwx------,999,999,4096,1230498722,1230498786,1230498786,0
/home/ubuntu/.gconf/apps/panel/applets/fast_user_switch_screen0/prefs,15378,d/drwx------,999,999,4096,1230498786,1230498786,1230498786,0
/home/ubuntu/.gconf/apps/panel/applets/fast_user_switch_screen0/prefs/%gconf.xml.new (deleted-realloc),15517,r/rrw-------,999,999,440,1230498786,1230498786,1
230498786,0
/home/ubuntu/.gconf/apps/panel/applets/fast_user_switch_screen0/prefs/%gconf.xml,15517,r/rrw-------,999,999,440,1230498786,1230498786,1230498786,0
/home/ubuntu/.gconf/apps/panel/applets/fast_user_switch_screen0/%gconf.xml,15457,r/rrw-------,999,999,1923,1230498722,1230498722,1230498722,0
/home/ubuntu/.gconf/apps/panel/applets/trashapplet_screen0,15458,d/drwx------,999,999,4096,1230498722,1230498722,1230498722,0
/home/ubuntu/.gconf/apps/panel/applets/trashapplet_screen0/%gconf.xml.new (deleted-realloc),15459,r/rrw-------,999,999,1819,1230498722,1230498722,1230498722,
```

Figure 3. File listing output.



```
┌──(kali㉿kali)-[~/forensic_output]
└─$ more 20251201_201022_timeline.txt
0|/home|15361|d/drwxr-xr-x|0|0|4096|1224505622|1230469851|1230469851|0
0|/home/ubuntu|15362|d/drwxr-xr-x|999|999|4096|1230469851|1231343974|1231343974|0
0|/home/ubuntu/.bash_logout|15363|r/rrw-r--r--|999|999|220|1230469851|1230469851|1230469851|0
0|/home/ubuntu/.bashrc|15364|r/rrw-r--r--|999|999|3115|1230469851|1230469851|1230469851|0
0|/home/ubuntu/.profile|15365|r/rrw-r--r--|999|999|675|1230469851|1230469851|1230469851|0
0|/home/ubuntu/.gconf|15369|d/drwx------|999|999|4096|1230469859|1231310370|1231310370|0
0|/home/ubuntu/.gconf/apps|15370|d/drwx------|999|999|4096|1230469859|1230528824|1230528824|0
0|/home/ubuntu/.gconf/apps/panel|15372|d/drwx------|999|999|4096|1230469859|1230498722|1230498722|0
0|/home/ubuntu/.gconf/apps/panel/global|15374|d/drwx------|999|999|4096|1230469859|1231268393|1231268393|0
0|/home/ubuntu/.gconf/apps/panel/global/%gconf.xml.new (deleted-realloc)|15375|r/rrw-------|999|999|143|1231268393|1231268393|1231268393|0
0|/home/ubuntu/.gconf/apps/panel/global/%gconf.xml|15375|r/rrw-------|999|999|143|1231268393|1231268393|1231268393|0
0|/home/ubuntu/.gconf/apps/panel/%gconf.xml|15373|r/rrw-------|999|999|0|1230469859|1230469859|1230469859|0
0|/home/ubuntu/.gconf/apps/panel/applets|15418|d/drwx------|999|999|4096|1230498722|1230498722|1230498722|0
0|/home/ubuntu/.gconf/apps/panel/applets/clock_screen0|15472|d/drwx------|999|999|4096|1230498722|1230498786|1230498786|0
0|/home/ubuntu/.gconf/apps/panel/applets/clock_screen0/prefs|15518|d/drwx------|999|999|4096|1230498786|1231297256|1231297256|0
0|/home/ubuntu/.gconf/apps/panel/applets/clock_screen0/prefs/%gconf.xml.new (deleted-realloc)|15391|r/rrw-------|999|999|2382|1231297256|1231297256|123129725
6|0
0|/home/ubuntu/.gconf/apps/panel/applets/clock_screen0/prefs/%gconf.xml|15391|r/rrw-------|999|999|2382|1231297256|1231297256|1231297256|0
0|/home/ubuntu/.gconf/apps/panel/applets/clock_screen0/%gconf.xml|15473|r/rrw-------|999|999|1914|1230498722|1230498722|1230498722|0
0|/home/ubuntu/.gconf/apps/panel/applets/%gconf.xml|15455|r/rrw-------|999|999|0|1230498722|1230498722|1230498722|0
0|/home/ubuntu/.gconf/apps/panel/applets/fast_user_switch_screen0|15456|d/drwx------|999|999|4096|1230498722|1230498786|1230498786|0
0|/home/ubuntu/.gconf/apps/panel/applets/fast_user_switch_screen0/prefs|15378|d/drwx------|999|999|4096|1230498786|1230498786|1230498786|0
0|/home/ubuntu/.gconf/apps/panel/applets/fast_user_switch_screen0/prefs/%gconf.xml.new (deleted-realloc)|15517|r/rrw-------|999|999|440|1230498786|1230498786
|1230498786|0
0|/home/ubuntu/.gconf/apps/panel/applets/fast_user_switch_screen0/prefs/%gconf.xml|15517|r/rrw-------|999|999|440|1230498786|1230498786|1230498786|0
0|/home/ubuntu/.gconf/apps/panel/applets/fast_user_switch_screen0/%gconf.xml|15457|r/rrw-------|999|999|1923|1230498722|1230498722|1230498722|0
0|/home/ubuntu/.gconf/apps/panel/applets/trashapplet_screen0|15458|d/drwx------|999|999|4096|1230498722|1230498722|1230498722|0
0|/home/ubuntu/.gconf/apps/panel/applets/trashapplet_screen0/%gconf.xml.new (deleted-realloc)|15459|r/rrw-------|999|999|1819|1230498722|1230498722|123049872
```

Figure 4. Timeline output.



```
┌──(kali㉿kali)-[~/forensic_output]
└─$ more 20251201_201022_forensic_report.json
{
  "analysis_date": "2025-12-01T20:10:22.320759",
  "image_analyzed": "ubnist1.casper-rw.gen3.E01",
  "artifacts": {
    "partitions": {
      "status": "failed",
      "error": ""
    },
    "filesystem_info": {
      "raw_output": "FILE SYSTEM INFORMATION\n────────────────────────────────────────────\nFile System Type: Ext3\nVolume Name: \nVolume ID: 9935811771d9768
b49417b0b3b881787\n\nLast Written at: 2009-01-06 13:59:33 (EST)\nLast Checked at: 2008-12-28 15:37:56 (EST)\n\nLast Mounted at: 2009-01-06 13:59:33 (EST)\nUn
mounted properly\n\nSource OS: Linux\nDynamic Structure\nCompat Features: Journal, Ext Attributes, Resize Inode, Dir Index\nInCompat Features: Filetype, Need
s Recovery, \nRead Only Compat Features: Sparse Super, Large File, \n\nJournal ID: 00\nJournal Inode: 8\n\nMETADATA INFORMATION\n──────────────────────────
────────────────\nInode Range: 1 - 38401\nRoot Directory: 2\nFree Inodes: 36976\nOrphan Inodes: 35, 20, 17, 16, \n\nCONTENT INFORMATION\n────────────────────
────────────────────────\nBlock Range: 0 - 153599\nBlock Size: 4096\nFree Blocks: 85287\n\nBLOCK GROUP INFORMATION\n──────────────────────────────────────
──\nNumber of Block Groups: 5\nInodes per group: 7680\nBlocks per group: 32768\n\nGroup: 0:\n  Inode Range: 1 - 7680\n  Block Range: 0 - 32767\n  Layout:\n
   Super Block: 0 - 0\n    Group Descriptor Table: 1 - 1\n    Data bitmap: 39 - 39\n    Inode bitmap: 40 - 40\n    Inode Table: 41 - 520\n    Data Blocks: 52
1 - 32767\n  Free Inodes: 7646 (99%)\n  Free Blocks: 31388 (95%)\n  Total Directories: 13\n\nGroup: 1:\n  Inode Range: 7681 - 15360\n  Block Range: 32768 - 6
5535\n  Layout:\n    Super Block: 32768 - 32768\n    Group Descriptor Table: 32769 - 32769\n    Data bitmap: 32807 - 32807\n    Inode bitmap: 32808 - 32808\n
    Inode Table: 32809 - 33288\n    Data Blocks: 33289 - 65535\n  Free Inodes: 7392 (96%)\n  Free Blocks: 11685 (35%)\n  Total Directories: 92\n\nGroup: 2:\n
  Inode Range: 15361 - 23040\n  Block Range: 65536 - 98303\n  Layout:\n    Data bitmap: 65536 - 65536\n    Inode bitmap: 65537 - 65537\n    Inode Table: 6553
8 - 66017\n    Data Blocks: 65538 - 65537, 66018 - 98303\n  Free Inodes: 6990 (91%)\n  Free Blocks: 110 (0%)\n  Total Directories: 120\n\nGroup: 3:\n  Inode
Range: 23041 - 30720\n  Block Range: 98304 - 131071\n  Layout:\n    Super Block: 98304 - 98304\n    Group Descriptor Table: 98305 - 98305\n    Data bitmap: 9
8343 - 98343\n    Inode bitmap: 98344 - 98344\n    Inode Table: 98345 - 98824\n    Data Blocks: 98825 - 131071\n  Free Inodes: 7376 (96%)\n  Free Blocks: 251
05 (76%)\n  Total Directories: 103\n\nGroup: 4:\n  Inode Range: 30721 - 38400\n  Block Range: 131072 - 153599\n  Layout:\n    Data bitmap: 131072 - 131072\n
   Inode bitmap: 131073 - 131073\n    Inode Table: 131074 - 131553\n    Data Blocks: 131074 - 131073, 131554 - 153599\n  Free Inodes: 7525 (97%)\n  Free Bloc
ks: 16365 (72%)\n  Total Directories: 57\n",
      "status": "success"
    },
    "file_listing": {
      "total_files": 1821,
      "files": [
        {
```

Figure 5. Report output.