CIS 542: DIGITAL FORENSICS

PROJECT SUMMARY

Under the Guidance of:

Dr. Ashok Kumar Patel

Submitted by

Sai Alekhya Ravi (16)

Title: Demonstration of Autopsy's File System Analysis Features

Introductoion:

In an increasingly digital world, where every interaction leaves a trace, the landscape of forensics has exploded. Autopsy, an open-source digital forensics tool, is at the forefront of this development, offering advanced features tailored to the demands of modern forensic analysis. This report begins a comprehensive journey to explore the capabilities of file system dissection analysis, with a special focus on keyword searching, timeline analysis, and hash filtering.

Why Autopsy?

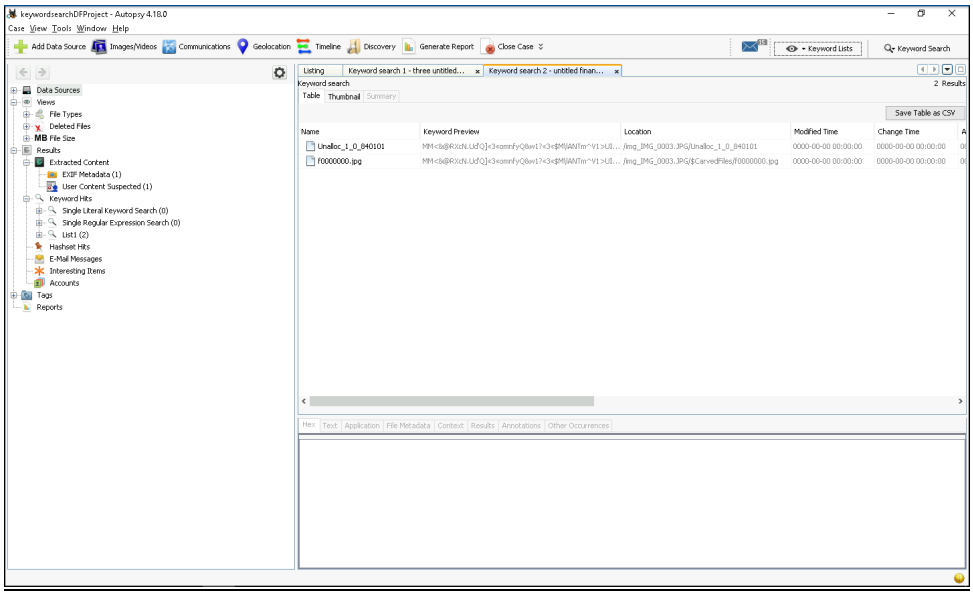
The decision to make dissection a central part of this project is based on versatility, accessibility and robust features. As an open-source platform, Autopsy breaks down proprietary software barriers and democratizes access to cutting-edge forensic techniques. Its intuitive user interface combined with a vibrant community of users and developers make it an invaluable tool for forensics, law enforcement and academic researchers. By illuminating the possibilities of autopsy, we aim to bridge the gap between theory and practice, empowering forensic professionals to navigate the complex stages of digital investigations with confidence and skill.

Understanding Features

Keyword Search:

At its core. , digital forensics is based on the ability to sift through vast amounts of data to find meaningful evidence. Autopsy's powerful keyword search gives investigators the tools to efficiently complete this daunting task. Dissection allows customizable search parameters, Boolean operators and regular expressions so researchers can tailor their search to specific criteria, improving the accuracy and relevance of search results. Autopsy's keyword search capabilities make critical evidence fast and the basis for thorough forensic analysis.

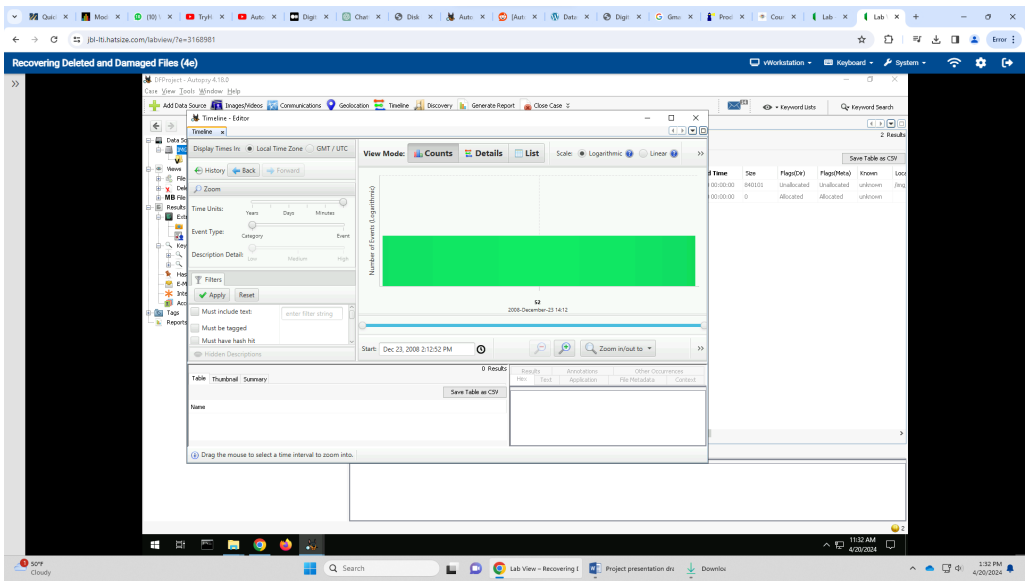
Screenshot:



Timeline Analysis:

In the field of digital investigations, time is not simply a linear progression, but a multifaceted dimension full of meaning. . The Dissection Timeline Analysis feature provides researchers with a comprehensive view of file activity over time, allowing visualization of patterns, correlations and anomalies. By combining the timestamps of file creation, modification, and access, Autopsy makes it easy to reconstruct events and helps researchers piece together the history of digital artifacts. Whether determining the chronology of a cyber attack, tracking the spread of illegal content or determining the provenance of digital evidence, autopsy timeline analysis capabilities provide valuable insight into the temporal aspects of forensic investigations.

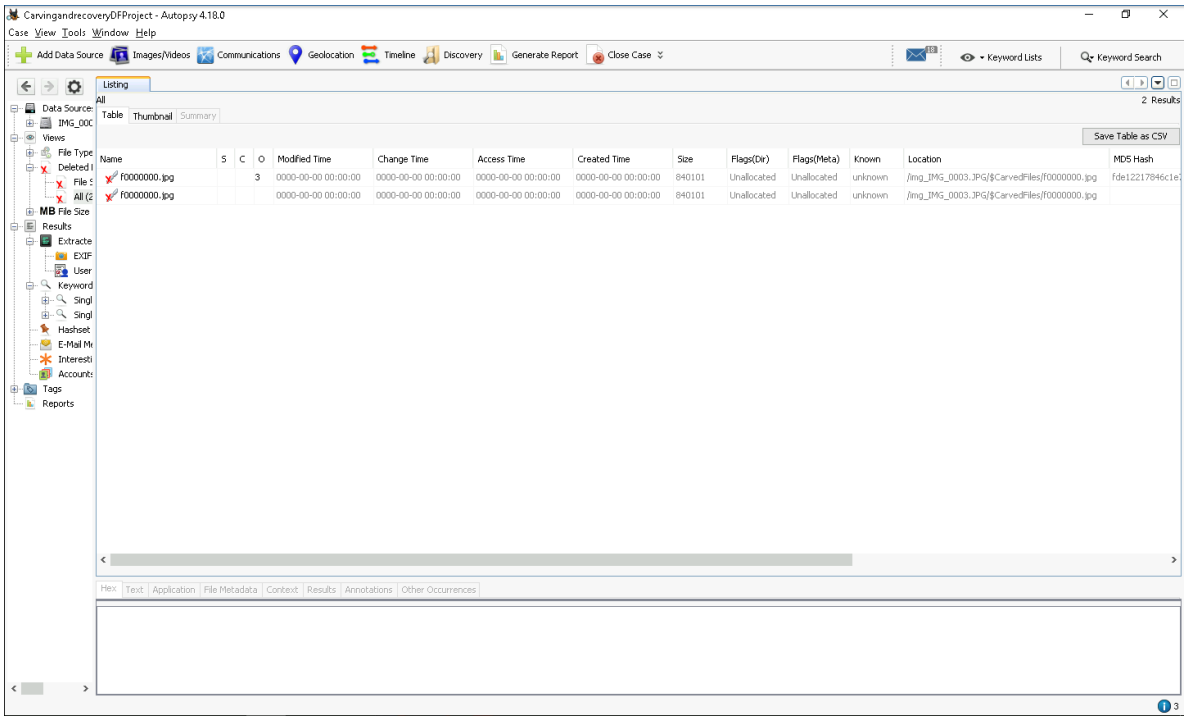
Screenshot:



Hash filtering:

Integrity and admissibility in digital evidence are the ability to ensure its authenticity and integrity. Autopsy hash filter capabilities provide researchers with a robust mechanism for this task. By generating hashes of files and comparing them to known hashes, dissection allows researchers to identify alterations, tampering or manipulation of digital objects. Whether verifying the integrity of forensic images, verifying the integrity of collected data, or detecting unauthorized changes to critical files, autopsy hash filtering functions are a cornerstone of forensic analysis and ensure the reliability and authenticity of digital evidence in court proceedings.

Screenshot:



Methodology:

The methodology used in this project involves a multifaceted approach that aims to provide a comprehensive understanding of the file system analysis capabilities of dissection. We use various datasets from the Digital Corpora repository - a well-known digital forensics repository - and use a combination of simulated scenarios and real case studies to illustrate the practical application of autopsy features. Through structured introductions, tutorials and practical exercises, we aim to provide practical knowledge and skills to both forensic practitioners and aspiring researchers. By promoting a deeper understanding of autopsy operations and workflows, we aim to equip forensic professionals with the tools and knowledge needed to skillfully and effectively navigate the complexities of digital investigations.

Conclusion:

In the ever-evolving landscape of digital forensics, the ability to use advanced tools and techniques is critical to investigative success. The analysis capabilities of the autopsy file system demonstrate innovation in advancing the field of forensic science. By providing a platform to explore and exploit these opportunities, this project aims to empower forensic professionals, improve the practice of forensic science and uphold the principles of justice in the digital age. As we continue to navigate the complexities of digital investigations, Autopsy is a beacon of innovation that guides us toward a future where truth, honesty, and accountability reign in the face of digital calamity.