### **Forensic Investigator Tool**

### SOHAIB KHAN 2022551

### **CYBER SECURITY**

**DIGITAL FORENSICS PROJECT  
  
Week 9**

**Week 9: Research and System Design**

**Research**

The first stage required me to carry out extensive research about essential core principles and technological aspects for constructing the Forensic Investigator Tool system. I aimed to gain full comprehension of current digital forensics solutions alongside tools while understanding how to bring them into my project. I started by researching several key areas:**The standard evaluation encompassed techniques for evidence collection while also assessing analytical methods for documentation purposes. I studied essential aspects relating to file integrity checks and suspicious file detection as well as log inspection and disk data analysis since these features would serve as basic elements of my tool.This investigation evaluated the three important forensic tools consisting of Autopsy and FTK Imager and Sleuth Kit. The review process of analytical tools gave me insight into standard operations but identified areas which my tool needed to overcome. The two analysis libraries I examined included the hashlib component for verifying file integrity as well as the pytsk3 library to analyze disk images.The practice of security incident handling focused on my investigation of system-generated records used to detect unauthorized access violations and brute force attacks through their analysis in the field of security incident handling. Log formats including syslog and Windows Event Logs represented my main analysis area as I used pattern recognition to discover abnormal behaviors in time.File Integrity Checking demanded that I gain knowledge about the MD5 and SHA-1 and SHA-256 file hashing algorithms. Jurors learned about the advantages and disadvantages of law enforcement algorithms used to verify forensic investigation files.My work involved both analysis of EXIF metadata in images and extraction of metadata from PDFs and Microsoft Office file platforms. I learned from this research about the way metadata reveals important timestamps and file creation and modification dates and authorship information that forensic investigators require.I researched how to generate detailed forensic reports because the Forensic Investigator Tool demands proper report creation. ReportLab became my selection due to its capability to produce PDF reports with flexible formats and professional presentation options.**

**System Design**

The completion of research marked a starting point for my system architecture design of the Forensic Investigator Tool. The design solution targets the development of an efficient multi-purpose system that combines scalability with user-friendliness for managing multiple forensic operations.

* The system uses High-Level Architecture through separate modular implementations for features such as file integrity checking and suspicious file detection and log file analysis and so on. The tool enables effortless extension and tool upkeep because new forensic techniques can easily be integrated.
* Tcl/Tk Library through Tkinter creates the User Interface (UI) which contains a straightforward and easy-to-use Graphical User Interface (GUI). The user interface includes specific fields which enable users to pick their files and directories while buttons trigger each analytical feature clearly.
* The core forensic analysis operations are handled by the backend section of the system. Every analysis capability resides within its own separate module in the system design. I built the analysis functions through Python library implementations which include pytsk3, python-magic, hashlib and other modules. The system contains individual modules which accomplish individual processes such as timeline generation and file integrity checking and suspicious file detection plus additional functions.
* I decided to establish a small database or storage platform which would maintain records of analyzed artifact data and their evaluation results. CSV files combined with a lightweight SQLite database will be used for data storage to let users access past analysis results and maintain records through time.

****The tool contains these distinct program modules for operation:****

1. **File Integrity Checker analyzes files in stated directories by comparing their cryptographic hashes with predefined data for identification of unauthorized file changes.**
2. **The Log File Analysis module performs scanning operations on logs to detect illegal access attempts followed by unauthorized login activities.**
3. **The metadata extraction system in this module obtains metadata information from different file types including images and documents and audio files to extract timestamp and author data.**
4. **The system employs Disk Image Analysis to examine .img file disks for deleted data while reconstructing file system organization.**
5. **This application includes a module which enables automatic artifact collection and storage of forensic evidence such as logs and images as well as documents.**
6. **The module enables the application to create extensive PDF reports which merge analytical summaries retrieved from different analysis modules.**
7. **All user interface design elements follow a friendly approach alongside efficiency.**

****Operations:****

* **The system uses a solitary user interface containing buttons to access all forensic examination operations.**
* **The application includes input elements which allow users to choose analysis files or directories.**
* **The user interface displays both status messages through real-time alerts and pop-up messages to show analytical outcomes along with any occurring errors.**
* **Technology Stack:**
* **Tkinter serves as the underlying technology to build the GUI since it enables users to operate through an approachable interface.**
* **The primary selection of Python 3 occurs because it offers convenient usage and includes digital forensics libraries.**
* **pytsk3 and python-magic for disk image and file type analysis.**
* **The tool employs hashlib to check file integrity through hash algorithms.**
* **The software employs ReportLab for creating professional and customizable PDF reports.**
* **The analysis results benefit from the efficient management using pandas along with the ability to organize data through pandas.**
* **The architecture design of the system received clarity through various UML diagrams which I developed.**
* **The system design structure with interaction details between modules appears in the Class Diagrams.**
* **The Activity Diagrams demonstrate how users operate with the tool in addition to presenting data pathway behavior within the system.**

**Refinements**

* **My work on error handling involved making the tool show precise understandable error alerts to users when analysis-related problems occur.**
* **The tool receives enhanced file path validation which guarantees proper file and directory entry from users thus minimizing system errors and improving the user experience.**
* **During this stage I finalized how the project would take shape and became both technologically reliable and convenient for users to work with. In the future I will deploy these design solutions into the tool's operations while conducting continued testing of every module.**