Certainly! Below is an implementation plan that will help you develop a fully integrated digital forensics application for Windows. The plan is divided into stages, each with specific tasks and deliverables to ensure steady progress.

**Implementation Plan**

**Stage 1: Project Planning and Setup**

**Duration: 1 Week**

1. **Define Project Scope**:
   * Clarify objectives and deliverables.
   * Identify key features and functionalities.
2. **Set Up Development Environment**:
   * Install necessary software and tools (Python, IDE, version control).
   * Configure project repository (GitHub/GitLab).
3. **Literature Review**:
   * Research existing digital forensics tools and methodologies.
   * Document findings and identify gaps to address.

**Stage 2: Data Collection Module**

**Duration: 3 Weeks**

1. **File System Analysis**:
   * Develop scripts to gather file metadata (creation date, size, permissions).
   * Implement file hashing for integrity checks (SHA-256, MD5).
2. **Registry Analysis**:
   * Create functions to extract relevant Windows Registry keys and values.
   * Identify critical registry paths for analysis.
3. **Network Activity Monitoring**:
   * Implement monitoring of network connections and data transfer.
   * Log active connections and open ports.
4. **Process and Memory Analysis**:
   * Develop tools to capture running processes and memory dumps.
   * Gather process details (PID, command line arguments).

**Deliverable**: A module that collects and stores data from the file system, registry, network, and processes.

**Stage 3: Data Storage and Management**

**Duration: 2 Weeks**

1. **Database Design**:
   * Design schema for SQLite database to store collected forensic data.
   * Create tables for file metadata, registry data, network logs, and process information.
2. **Data Ingestion**:
   * Implement functions to store collected data in the database.
   * Ensure efficient data handling and storage.
3. **Data Retrieval**:
   * Develop queries to retrieve and display data for analysis.
   * Optimize data access for performance.

**Deliverable**: A database system to store and manage forensic data with efficient data retrieval mechanisms.

**Stage 4: Data Analysis Module**

**Duration: 3 Weeks**

1. **File and Registry Analysis**:
   * Implement methods to analyze file and registry data for anomalies.
   * Develop criteria for identifying suspicious files and registry changes.
2. **Network and Process Analysis**:
   * Create algorithms to detect unusual network activity and processes.
   * Implement heuristic checks for common signs of malware.
3. **Artifact Correlation**:
   * Develop logic to correlate data from different sources (e.g., file access times with network activity).
   * Identify patterns indicative of compromise.

**Deliverable**: A module that analyzes collected data and identifies potential security incidents.

**Stage 5: Reporting Module**

**Duration: 2 Weeks**

1. **Report Generation**:
   * Design templates for forensic reports (summary, detailed).
   * Implement functions to populate reports with analyzed data.
2. **Export Functionality**:
   * Enable export of reports in various formats (PDF, Excel).
   * Ensure reports include all relevant details and findings.
3. **User Interface for Reporting**:
   * Create a simple UI to view and generate reports.
   * Provide options to customize report contents.

**Deliverable**: A reporting module that generates comprehensive forensic reports.

**Stage 6: Integration and Testing**

**Duration: 2 Weeks**

1. **Module Integration**:
   * Integrate data collection, storage, analysis, and reporting modules.
   * Ensure smooth data flow and interaction between modules.
2. **Testing**:
   * Perform unit testing on individual modules.
   * Conduct integration testing to ensure overall system functionality.
   * Debug and fix issues identified during testing.
3. **User Testing**:
   * Test the application with end-users to gather feedback.
   * Make necessary adjustments based on user feedback.

**Deliverable**: A fully integrated and tested digital forensics application.

**Stage 7: Documentation and Final Review**

**Duration: 1 Week**

1. **Documentation**:
   * Prepare detailed documentation for the project, including user guide and technical manual.
   * Document installation, configuration, and usage instructions.
2. **Final Review**:
   * Review the entire project for completeness.
   * Ensure all objectives and requirements are met.
3. **Presentation Preparation**:
   * Create a presentation summarizing the project.
   * Highlight key features, methodologies, and findings.

**Deliverable**: Complete project documentation and a presentation ready for submission.

**Starting Point**

**Week 1: Project Setup and Planning**

1. **Define Objectives**: Clearly outline what your project aims to achieve.
2. **Set Up Environment**: Install Python, an IDE (like PyCharm or VS Code), and set up a version control system (Git).
3. **Initial Research**: Conduct a literature review on digital forensics tools and techniques.
4. **Plan Milestones**: Break down the project into smaller tasks with deadlines.