**Project Proposal: Introduction**

**1.1 Introduction**

**Scope**

This project is focused on enhancing digital forensic investigations by addressing the inherent complexities of analyzing fragmented user activity data within the Windows Registry. The scope encompasses the design and development of a specialized digital forensic analysis tool. This tool will concentrate on the automated extraction, sophisticated correlation, and integrated presentation of diverse registry artifacts pertaining to user activity. Key artifact types to be investigated and correlated include:

* **Last Logon Timestamps:** Identifying and reconciling various "last logon" and "last activity" timestamps from multiple registry locations (e.g., SAM hive, Winlogon keys, UserAssist entries) to derive a most likely accurate timeline.
* **USB Device Connection History:** Extracting and linking records of connected USB devices to specific user profiles and activity sessions.
* **Program Execution History:** Analyzing registry-based evidence of application launches (e.g., ShimCache, AmCache.hve) to build a comprehensive picture of software usage.
* **Folder Access History (Shellbags):** Recovering and correlating data on accessed folders, including local, removable, and network shares, to understand user navigation patterns.
* **Email Activity Referencing:** Leveraging existing email artifact processing capabilities of forensic platforms to link relevant email communications to user activity profiles.

The solution aims to provide a cohesive, context-rich view of user actions directly within its interface, thereby reducing manual analysis overhead and improving the depth of investigative insights. This custom analytical solution is envisioned to be implemented as a dedicated application, with potential approaches including development as a module for an existing forensic platform or as a standalone Python-based tool.

**Aim**

The overarching aim of this project is to develop a specialized digital forensic application capable of performing advanced, automated correlation of Windows Registry data and related user activity artifacts. This will enable investigators to gain a more comprehensive, accurate, and actionable understanding of a user's digital footprint, ultimately enhancing the efficiency and effectiveness of digital forensic investigations.

**Objectives**

To achieve the stated aim, the project will pursue the following specific objectives:

1. **Automated Registry Artifact Extraction:** To implement robust mechanisms for the automated extraction of critical user activity-related data from various Windows Registry hives (SAM, SOFTWARE, SYSTEM, NTUSER.DAT, AmCache.hve).
2. **Refined Last Logon Correlation:** To develop and apply sophisticated correlation algorithms to reconcile and present a "most likely" accurate last logon timestamp by integrating data from multiple, potentially conflicting, registry sources.
3. **Contextual User Profile Generation:** To generate enriched user activity profiles by automatically linking extracted logon events with associated USB device connections, program executions, and folder access histories.
4. **Integrated Email Activity Referencing:** To incorporate references to relevant email communications into user activity profiles by querying and utilizing email artifacts already processed by a forensic analysis environment.
5. **Heuristic-Based Suspicious Activity Flagging:** To implement basic heuristic rules for flagging potentially suspicious characteristics within the extracted user activity data (e.g., unusual program executions, specific keywords in email references), to draw investigator attention to anomalies.
6. **Integrated Findings Presentation:** To ensure that all extracted, correlated, and flagged user activity data is presented clearly and cohesively within the application's interface, facilitating intuitive analysis and interpretation by forensic examiners.