**Project Synopsis Format**

1. **Title of the project**: User/owner trail identification using Android Forensics.
2. **Area of the Project**: Mobile device forensics, Android forensics, Forensic data acquisition, Mobile database forensics.
3. **Project Team Members Details**:

* Kanchan Chowdhari, [kanchan.chowdhari@cumminscollege.in](mailto:kanchan.chowdhari@cumminscollege.in), 7350883625
* Garima Chhaparwal, [garima.chhaparwal@cumminscollege.in](mailto:garima.chhaparwal@cumminscollege.in), 9970171182
* Khushboo Sharma, [khushboo@cumminscollege.in](mailto:khushboo@cumminscollege.in), 8237337041
* Mudita Sharma, [mudita.sharma@cumminscollege.in](mailto:mudita.sharma@cumminscollege.in) , 9762271751

1. **Sponsoring Company Details**: In-house.
2. **Details of the Internal Guide**: Mrs. Soudamini Patil, 8446608042
3. **Motivation of the Project:** In digital forensics, one of the primary objectives of forensic data collection is identification, analysis, interpretation of collected evidences. However many a times it is observed that when a stray mobile device is seized, the common man does not have expertise to identify the owner of the device. Hence there is a need of an easy mechanism for a common man to get the traces of the owner/user of the mobile device.

This synopsis proposes a development of guided software that can help/aid in identification of owner/user of an android device. This project proposes owner trail identification on mobile devices by analyzing SIM cards, device memory, SD card. The software is proposed to collect a set of user activities and analyze them inferring intelligent races of owner/user of mobile device.

1. **Scope of the project and what is not in the scope**: The proposed project considers only the Android mobile devices. The data analysis is limited to collection of information from calls, messages, contacts, pictures, videos, updates, chat logs, documents and various applications.

The usage of some of the existing mobile forensic tools in this project is permitted.

The development platform is Android operating system ecosystem.

1. **External Interfaces/Tools/ Libraries planning to use**: Android Studio, Existing mobile forensic tools (dd, Sleuth kit,etc), R Scripting, Qt creator
2. **Module-wise description**:
   * Acquisition-In this module, acquiring of user logs such as calls, messages, contacts, pictures, videos, updates, chat logs, network logs, disk image, documents and various applications would be done.
   * Encryption and decryption- This module is required to ensure mobile security and data integrity.
   * Mining- User trails can be identified by performing data mining operations on acquired data.
3. **Hardware and Software Requirements** :

Android OS, v4.0 (Ice Cream Sandwich), Ubuntu Tested on Ubuntu® 12.04, 64-bit distribution 2 GB RAM minimum, 8 GB RAM recommended 2 GB of available disk space minimum, 4 GB Recommended (500 MB for IDE + 1.5 GB for Android SDK and emulator system image)

1. **Any Limitations**- The proposed project considers only the Android mobile devices and Ubuntu Operating System.
2. **Any Future Enhancement** (Minimum Guaranteed, Desirable etc.): The developed technique can be extended for different mobile platforms and different operating systems.
3. **Study curve** (Tools, Technologies, Related theoretical background etc.):

* Existing relevant Forensic tools (dd, etc), Android studio, Android debug Bridge.
* Android architecture and file organization.
* Linux commands.
* Data extraction of underlying hardware of a mobile device.
* R programming, shell scripting.