Electrical/Computer Engineering Design Project Proposal

Title: *Computer Forensic Investigation Tools*

Client: *Jacques Boucher(jjrboucher@gmail.com), Royal Canadian Mounted Police – Atlantic Region Integrated Technological Crime Unit*

Supervisor: *Dennis Peters*

Description

Computers seized from crime suspects can reveal significant evidence to assist in a criminal investigation, but finding and using this evidence is troublesome for two reasons:

1. *It requires deep knowledge of the particular techniques of the software and operating system used (e.g., where to look for cookies, history files, backups, deleted files etc.), and these particulars change with particular tools (e.g., IE vs Firefox vs Chrome), versions of tools or operating system and system or user settings.*
2. *Often it is the correlation of activities that helps build a case (e.g., web sites visited around the time that files were created/saved), so searching for evidence requires an effective presentation of system wide event histories.*

The proposal is to build a framework and suite of tools that can be used to do such forensic investigation. The tools must look for the timeline data and present it in a way that effectively helps in the investigation. The framework must allow ITCU staff to capture and modify the specifics of new OS and tool versions so that the tools can adapt to changing software and new knowledge.

Roles

This project is purely software, and can be expanded or contracted based on the number of students involved. Three or four Computer Engineering students would be ideal.