**MSc projects: Dr Suleiman Yerima**

**1 Lightweight proactive detection of malicious mobile malware**

The aim of the project is to explore, investigate and develop an automated system to detect the presence of malicious code within a mobile application. The project will develop and evaluate a technique that will utilize static structural properties of an app to proactively detect malicious code within the app. The system will be evaluated on real mobile malware samples.

Objectives:

* Review existing techniques for mobile malware detection
* Determine the types of app/code properties that could be used to characterize apps for risk analysis
* Utilize these app and code properties to build a system that can classify apps as benign or suspicious.
* Evaluate the system on real world malicious apps from various repositories.

**2 Disk image anti-forensic detection and remediation**

Anti-forensics measures are taken by criminals in order to hide data and frustrate recovery efforts by forensic tools. Disk obfuscation allows for whole partitions or sections of drives to be hidden from forensic software. The aim of the project is to develop techniques that can detect hidden partitions of various types from obfuscated disk drive images. These techniques will then be used to create a forensics image scanning triage tool. The main objective of the developed techniques will be to reduce false positives and complement the data recovery capabilities of existing forensic software.

Objectives:

* Review data hiding and obfuscation approaches on disk images and understand how they are applied
* Research and understand the shortcomings of existing forensic tools with regards to detection of various disk image obfuscation techniques.
* Develop techniques to detect hidden sections/partitions of various types.
* Create a forensic scanning triage tool from the detection techniques
* Evaluate the effectiveness of the created tool on various obfuscated forensic images and compare these to capabilities of existing forensic software.

**3 Message carving from volatile memory on mobile devices**

The rapid rise in data and information storage and transfer on varieties of mobile devices nowadays is of great concern to the forensic community. Android is fast becoming the OS of choice for hand-held mobile devices, hence the need to develop better forensics techniques for data recovery. This project aims to analyze the volatile memory of Android devices and develop techniques for message carving from volatile memory. It would design a method that will integrate volatile memory acquisition and message carving to recover both deleted and undeleted email and chat messages from Android devices.