Proposed Framework for Rootkits Analysis and Cyber Forensics for Cyber Security

Research Project Supervisor	• Dr. Mie Mie Su Thwin
	  • Associate Professor, UCSY
	  • Technical Supervisor, mmCERT

Members	• Ms. Cho Cho San • Mr. Tin Maung Maung • Mr. Naing Linn Htun

Presented by

Cho Cho San

Introduction

Cybercrimes are committed by using the technology and electronic devices (computers, mobile phones).

Computer forensics and android forensics are needed to search and analyze a vast amount of information quickly and efficiently.

The most salient artifact within cyber security is malicious software.

The use of rootkits and rootkit technologies in malware and cybercrime is increasing.

We propose a high-level framework of the overall solution delivery model to provide Forensics and Rootkits Analysis Framework.

Purposes

- To identify the exact nature and seriousness of the incident
- To collect information to get evidence from the crime scene
- To propose the Forensic Framework for Cyber Crime Investigation System
- To study the nature and complexity of rootkits
- To extract and categorize the dominant features of rootkits
- To propose the rootkits analysis framework
- To design and implement the Forensics and Rootkits Analysis Environment

Importance of Cyber Crime Investigation in Myanmar

As the ICT sector grows in Myanmar, services will evolve and risks will increase. e.g.

- online-banking,
- ecommerce,
- e-government
- email,
- social networking
- and online shopping, etc.

The use of smart-phone applications or web-applications for services is increasing, maintaining the availability, integrity of systems and confidentiality of information against attacks will become a central issue.

Proposed Framework for Cyber Security

I. Framework for Cyber Forensics

- Computer Forensics
- Android Forensics

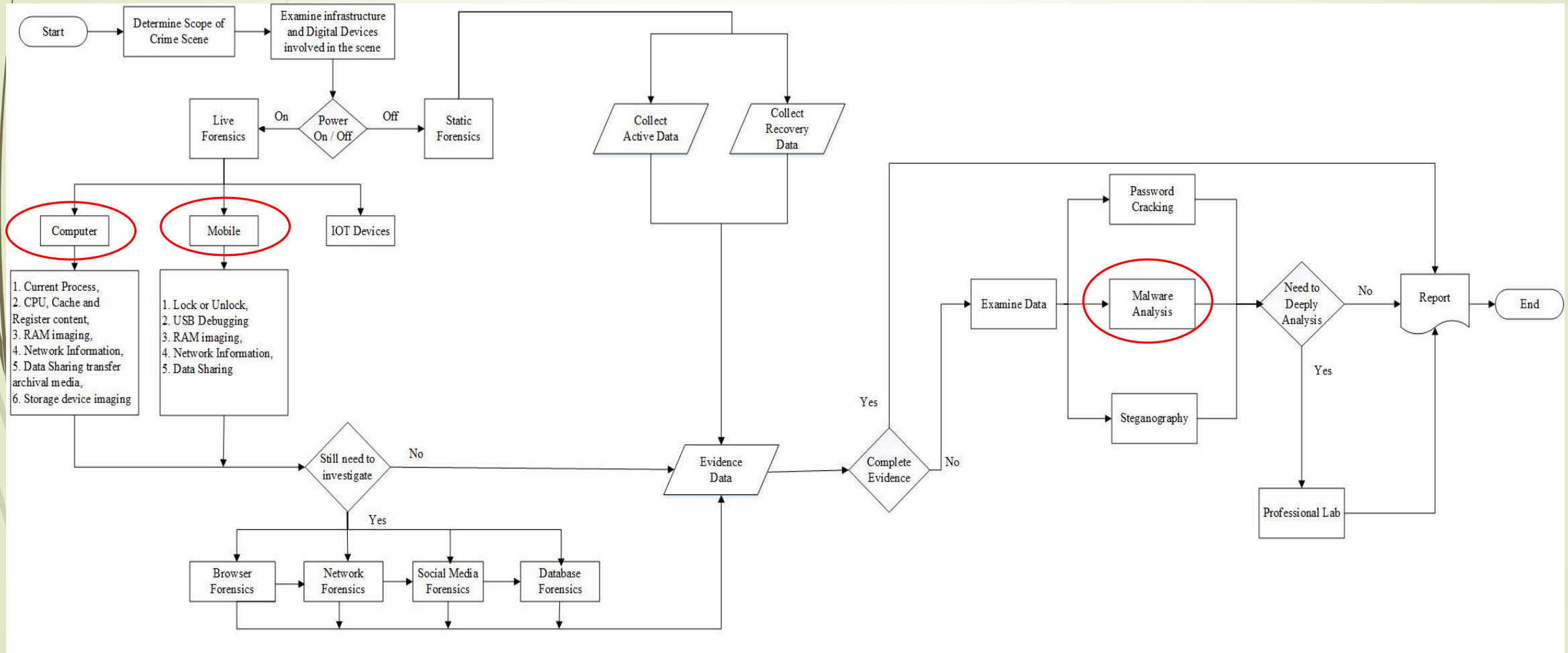

Figure1: High-level Framework for Cyber Forensics

II. Framework for Rootkits Analysis

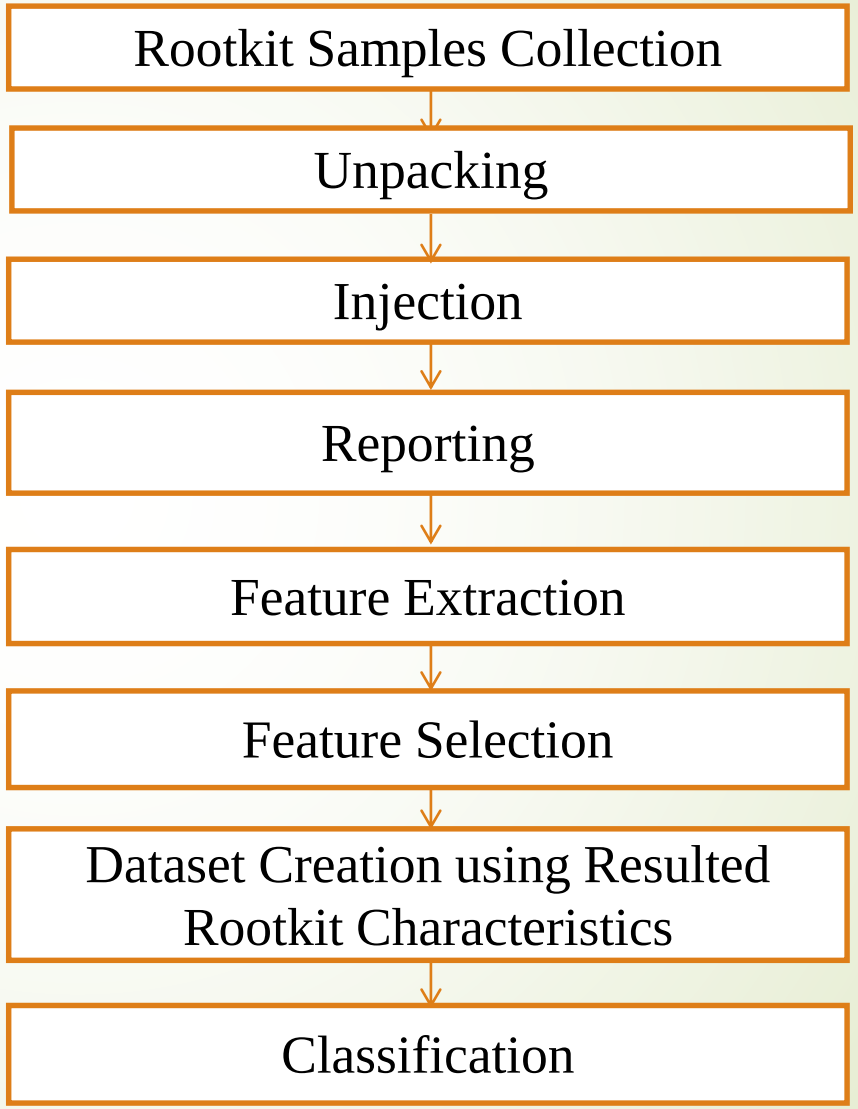

Figure2: Rootkits Analysis Procedure

Advantages

This framework has been developed to be a modular system.

It is very extensible when a new tool or module develops in it.

It could be plugged into the framework easily.

We have a list of points that need to be developed in the future

- To collect the evidence from the crime scene
- To examine and recover the information on victim's devices(computers or mobile phones)
- To extract the prominent features from rootkits execution
- To categorize the malicious samples with their variants

Conclusion

It provides the forensic suite framework, and detail rootkits analysis architecture.

The proposed system will provide the valuable dataset from the experiment of rootkits analysis.

This framework will support and cover to collect evidence information in different forensic fields.

We will use some freeware and ultimate tools, and our own tool in this framework.

We propose a high-level framework to provide Cyber Forensic and Rootkits Analysis, together with the specific benefits that will accrue to Cyber Security Research Lab in UCSY.

THANK YOU