IT Capstone Project Understanding of Requirements

Polaris Sight : Live Forensics and Incident Response System

Supervisor

Name: Ernest Foo

Email: [e.foo@qut.edu.au](mailto:e.foo@qut.edu.au)

*The following is an initial understanding of requirements following the first meeting with the client (March 8th), in which we were briefed on the project, and then discussed the project aim, scope and other relevant details.*

The client explained that the idea for the project stems from his time working with a large government organisation who lamented a lack of live forensic analysis software. In particular, the ability to **assess an ongoing attack**, and to determine the **actions and aim of the hacker** as well as **the extent to which the system was compromised**. Learning what the hackers are doing also helps to protect against future attacks.

The system is to be deployed on critical infrastructure. It should be **scalable to a large network**, and this should be simulated through virtual machines. It should also be **suitable for small businesses**, and interpretable by a layman. The primary goal is **detection and analysis while maintaining forensic readiness**.

The client has recommended a set of tools including Google Rapid Response, Kibana and OSSEC. However, **other tools may be used** if they are open source and fulfil the requirements.