COMP3000 - Computing Project

2020/2021

Pi4 In-Field Forensic Investigation.

Links

Source code: *https://github.com/Jiskey/Raspberry-Pi4-Forensics*

Backlog: *https://tasks.office.com/live.plymouth.ac.uk/en-US/Home/Planner/#/plantaskboard?groupId=70a71d6e-2599-47e9-81f9-b53f5b6fb5ae&planId=8I6GnC5uDEeY2jvOWbVVOJYAFUcw*

Project Vision

In the ever-evolving world of cyber space and the technologies it includes, also increases the need for cyber professionals to perform tasks to keep a company safe from either a cyber-attack or legal repercussions. One of these tasks would be the process of forensic triaging, the process of collecting and analysing data collected from a suspect host for investigation purposes. Traditionally, forensic investigators Identify possible locations where the evidence could be found then collect the data, preserving its integrity, before analysing the data back at a lab. The hardware required to perform this task inline with good forensic practise such as; write blockers and forensic imagers, are both complicated and expensive. Furthermore, analysing the data can take a lot of time when transferring from scene too lab. With high-powered single-board computers getting more affordable and open source software such as Kali Linux and its packages being easily accessible, there is a possibility for this process to become both more accessible and affordable to Cyber Professionals, Small business and IT enthusiasts alike.

Raspberry Pi is one of the many single-board computers available to everyone. With the Pi 4 having up to 8GB's of ram and a 1.5ghz processor, these can be used as mini computers to both collect and analyse the data collected from the scene, at the scene, eliminating the need to perform analysis back at a lab. Kali Linux OS includes many free and open-source software to allow for forensic investigation and can be installed on the Pi. Using these tools alongside coding languages such as python to collect and analyse data in the field, the price of this device compared to other forensic imagers drops drastically and allows Individuals a cheaper and simpler entry into forensic investigation.

The tools and capabilities included in Kali Linux combined with the flexibility and affordability of single-board computers allows for simple acquisition and analysis of data. introducing users and companies to the process of forensic triaging, who may not be able to before, eliminating the need for a lab and decreasing the time it traditionally takes.

Risk Plan

ID	Category	Description	Severity (1-5)	Likelihood (%)	Rating (1-5)	Approach	Response
1 - B1	Budget	Damaged hardware and replacements are needed.	High - 5	10%	0.5	Risk Avoidance	Single-board computer will require a form of passive/active cooling to prevent overheating. Protective housing will be required to protect the unit for transportation
2 - B2	Budget	Required hardware Is too expensive or unaffordable	Low - 1	10%	0.1	Acceptance	Project Idea is about cost saving. Optional hardware like write blockers are expensive.
3 - S1	Scope	The scope of the project and what it involves becomes too small or large	Medium - 3	20%	0.6	Mitigation	Ensure Adequate time and planning is made throughout the project.
4 - S2	Scope	A specific task taking more time than necessary.	Medium-High - 4	50%	2	Risk Avoidance	Follow planning
5 - S3	Scope	Task requirements changing and task redo's	Medium-High - 4	40%	1.6	Acceptance	Accept and complete the new task
6 - HR1	Human Recourses	The person is unwell or injured and cannot complete tasks.	High - 5	50%	2.5	Mitigation	The chances are low however are more likely due to the pandemic.
7 - HR2	Human Recourses	Additional knowledge required to complete a specific Task.	Low - 1	80%	0.8	Risk Avoidance	Ensure appropriate planning and time is given to the task.
8 - P1	Programme	Uncompleted tasks requiring extra time based on sprints.	Medium-Low - 2	60%	1.2	Acceptance	Take the extra time needed and adjust planning appropriately
9 - P2	Programme	"Clogging" of schedule. Schedule changes due to unexpected problems and changes.	Medium-High - 4	20%	0.8	Mitigation	Insure most/all tasks are complete on time and complete already assigned tasks before starting another.
10 - T1	Technical	Hardware Failures.	High - 5	10%	0.5	Acceptance	N/A
11 - T2	Technical	Software Failures. Task completion time could Increase greatly with	Medium-Low - 2	50%	1	Acceptance	With limited recourses on a single-board computer, this is likely to increase time

		limited hardware resources.					and may crash the software after long run times.
12 - T3	Technical	A Specific Task Requiring Additional hardware / software to complete.	Medium-Low - 2	20%	0.4	Acceptance	Look for "work-arounds" and other possible solutions
13 - T4	Technical	Software Requirements, hardware can't run specific software.	Low - 1	10%	0.1	Acceptance	N/A
14 - T5	Technical	Test Environment damaged and/or unusable.	Medium - 3	40%	1.2	Mitigation	Ensure methods are in place so that the VM's and Data storage will not be damaged. Allow for quick and easy rebuilding of test assets.
15 - T6	Technical	File Format incompatibilities.	Medium-Low - 2	50%	1	Risk Avoidance	Ensure correct data formats are collected and ensure multiple applications are available
16 - T7	Technical	Uncontrolled Accidental Malware Infection	High - 5	20%	1	Risk Avoidance	Infection will take place in a safe environment and following strict tools and guidance.
17 - T8	Technical	Software Incompatibilities	Low - 1	10%	0.1	Acceptance	N/A
18 - Q1	Quality	Data integrity is damaged / compromised.	Medium - 3	60%	1.8	Mitigation	Collect data with the appropriate tools and methods and check if data has been altered on a regular basis.
19 - Q2	Quality	Data and hardware, Loss / Damage / Theft.	High - 5	10%	0.5	Risk Avoidance	Keep things safe by keeping them with your person and being careful not to damage anything.
20 - Q3	Quality	Loss of recorded data / results	High - 5	10%	0.5	Risk Avoidance	Using online data storage means to store the data collected (GitHub, Google Drive, etc)
21 – Q4	Quality	Copyright Infringement	Low - 1	20%	0.2		For education purposes but using Images from Online and other forms of media, copyright will be

							considered and everything sourced
22 – Q5	Quality	Regulatory Incompliance	Medium-Low - 2	20%	0.4		For education purposes, but compliance will be followed unless unintentional.

Legend	
Risk Categories	
Category	**Description**
Budget - B	Risks relating to funding of the project. Is the project financially adequate and will more costs be included if something happened to something or someone?
Scope - S	Risks relating to the overall scope of the project. Is the project able to be completed in time?
Human Recourses - HR	Risks relating to the persons involved in the project. Will any of the individuals be affected for whatever reason and Is there much additional work to be completed by the individual.
Programme - P	Risks relating to the programme scheduling. Will more research be required to complete a specific task
Technical - T	Risks Relating to the technical aspects of the project. Will there be any problems relating to any software and hardware in the project?
Quality - Q	Risks Relating to the quality of the project. Is the quality of environments and results to an adequate standard and follows ethical and legal issues? Has any work been damaged / lost or stolen?
Risk Approaches	
Approach	**Description**
Risk Avoidance	Eliminating the threat of the risk by eliminating its cause. Risks in this category usually point to a single point of failure.
Mitigation	Reducing the consequences of the risk and controlling its impact or reducing the chance of the risk occurring. Risks in this category usually have multiple points of failure.
Acceptance	Accepting the risk and its Impact. Risks In this category means that the user has no control of what happens after it occurs or its impact and its fix is more effective than implementing mitigation methods.

Keywords

Raspberry Pi, Pi, Pi4, Forensics, Triage, Forensic Investigation, Imaging, Acquisition, File Analysis, Linux, Kali, Kali Linux, Windows, Virtual Machine, Registry Analysis, Page-File Analysis, Carving, Forensic Cases, Hashes, Memory Forensics, Network Forensics, Python, Programming.