CARDIFF UNIVERSITY SCHOOL OF COMPUTER SCIENCE AND INFORMATICS

CM3202 One Semester Project: 40 Credits
Author: Benjamin Ajax-Lewis
Supervisor: Michael Daley
Moderator: Alun Preece

Initial Plan

"An Overview of Digital Forensics Standards"

1.Project Description

The problem that I will be aiming to solve is Digital Forensic Standards because currently there aren't any formal standards that everyone has adopted to tackle Digital forensic investigations. One of the main international standards that has been published is the ISO/IEC 27037 (ISO/IEC 27037:2012) that covers the identification, acquisition and preservation of digital evidence, that ISO alongside ISO 17025 (ISO/IEC 17025:2005)which looks at verifying and backing up procedures with scientific evidence , but currently no government has enforced the use of these standards so every country is still using the guidelines that they have individually drawn up; therefore in the United Kingdom we use the ACPO Good Practice Guidelines (ACPO Good Practice Guide for Digital Evidence)for managing digital evidence, but these guidelines are becoming difficult to follow with the introduction and advancement of mobile forensics and wearable technologies which in current practice contradicts some of the principles outlined in the guide. My target will be to collect guidelines currently enforced in the developed countries/unions in Europe, America and Asia, and look at how different investigations are undertaken in these countries to produce a global standard set of procedures to follow at every stage of an investigation, I will look at the ISO' as a point of reference to build these procedures from. Another aim for this project will be to collect and perform tests on the many forensic tools that get used in these different countries to prove that the features in these applications are analyzing the data correctly and extracting the evidence in efficient manner, from these tests I intend to build a list of recommended tools for certain situations and attach them with the procedures that I will finalize in my report. By undertaking these tests my aim will be to help prove that these trusted tools work correctly, and to a high standard, and with my results you would be able to prove that these tools work in a court of law.

2.Project Aims and Objectives

Primary Aims and Objectives:

Adapt Current Government Guidelines – I want to look at the many police forces that govern each country and analyze their approach to a crime scene and what guidelines they currently must adhere to so that I can gain an understanding of the similarities and differences in these countries.

Collection of Reliable Tools – there are many forensic tools that are currently used and more being developed as technology advances and changes with each new iteration; my aim will be to produce a list of recommended tools that I have tested to give a viable option of what tools can be trusted without being too strict on their use as you can't plan for every situation and the advancement of technology is rapid.

Produce individual Procedures for each facet of an investigation: these include the verification that a crime has been committed, correct procedure of how to collect this evidence, efficient analysis of the evidence collected and storage of the findings collected in this investigation.

Secondary Aims and Objectives:

Create different procedures on how to handle different kinds of hardware – I want to be able to make the collection of data to be as efficient as possible and with the growing

number of devices that each individual person has this means that you must collect most of the items that a suspect owns because everything has some form of data stored on it.

2.1 Project Constraints

The main constraint to this project will be the amount of hands on information I can obtain from people working in the field of digital forensics to be able to make good procedures that assist in the way that they do their jobs rather than restrict them.

2.2 Project Deliverables

By the end of this project the main deliverables I want to produce will be, clearly outlined procedures with documentation and diagrams on how to identify, collect and store information on a digital forensic investigation and a list of recommended tools and how best to use them in each stage of the investigation along with guidelines on how to handle new hardware technologies.

3. Work Plan

Week 1: 23/1/17 – 29/1/17 –

- Work on Initial Plan
- Collecting and Reading Resources
- Deliverable: Initial Plan Due 30/1/17

Week 2: 30/1/17 – 5/2/17 –

- Collect Resources and Research police guidelines and procedures in the UK and Europe:
    - Write up notes on similarities and Differences in the laws and procedures
- Collect Resource material on digital forensic law in other countries
    - America, Asia etc.
- Collect research on handling current and future physical hardware
- Collect publicly available cases to use for Scenarios later
- Add resource information to bibliography file as you collect it

Week 3: 6/2/17 – 12/2/17 –

- Research and assess guidelines and procedures in America and Asia:
    - Look at the differences between the digital forensic laws in each country and compare with the research collected in the previous week
- Continue research on handling current and future physical hardware
- Continue collecting publicly available cases to use for Scenarios later
- Collect list of preferable tools that are being used across the world
    - How they are used?
    - Who is providing them?
    - What environment has it been developed for?
- Assess Gantt Chart and make adjustment's if needed

Week 4: 13/2/17 – 19/2/17 –

- Write up a couple procedures of verification that a crime has been committed
    - Apply different crime scenarios to these procedures to test which one is the most versatile
- Draw up rough diagram of the final selected verification procedure
- Starting writing up procedure for handling physical hardware

Week 5: 20/2/17 – 26/2/17 –

- Write up procedures on how best to collect data from the crime scene
    - write procedures for a live acquisition and for a system that's switched off
    - Apply different scenarios to these procedures to test which one is the most versatile
    - Make note of frequently used tools used in the acquisition of data
    - Include procedures on how to deal with current and future hardware
- Draw up rough diagrams on the final acquisition procedures that get chosen
- Assess Gantt Chart for any changes

Week 6: 27/2/17 – 5/3/17 –

- Write up a couple procedures of analyzing the data that is collected
    - Make note of currently used tools for analysis of the data

Week 7: 6/3/17 – 12/3/17 –

- Continue Assessment of analysis procedures
    - Applying currently used methodologies to improve efficiency on searching the data
- Draw up diagrams on the final analysis procedure that is chosen
- Assess Gantt chart for adjustments

Week 8: 13/3/17 – 19/3/17 –

- Write up a couple procedures on how the data and information is stored
- Deliverable: Design and main implementation of the report
- Have Supervisor Milestone meeting to assess the procedures that I've drawn up in this section

Week 9: 20/3/17 – 26/3/17 –

- Apply any adjustments or changes needed from supervisor meeting on the procedures
- Collect tools for acquisition and analysis of data
- Write up test plans for each frequently used tool
    - Using same fixed set of data to make it easier to compare
    - Outlining good features and bad features for how the tool is used
- Adjust Gantt chart if needed

Week 10: 27/3/17 – 2/4/17 –

- Continue testing of tools

    - Take screenshots
    - Write up documentation of findings
- Deliverable: List of Recommended tools and Tests

Week 11: 3/4/17 – 9/4/17 –

- Start drawing up the structure of the final report
    - get together final chosen procedures and diagrams
    - Draw up final list of recommended tools
- Have Supervisor Milestone meeting to review current findings and to go over the structure of the final report

Easter Weeks

Easter Week 1: 10/4/17 – 16/4/17-

- make any changes to current structure from supervisor meeting
- Write final Report
    - Evaluate procedures chosen

Easter Week 2: 17/4/17 – 23/4/17-

- Write final Report
    - write up future additions to the standard
    - Reflection of how the project was structured

Easter Week 3: 24/4/17 – 30/4/17-

- Reference checking and finish bibliography

Week 12: 1/5/17 – 5/5/17 –

- Grammar and spell checking
- Finish off final report and submit
- Deliverable: Final Report due 5/5/17

Gantt Chart

Gantt Chart					Weeks														
ID	Task	Start Date	End Date	Duration (weeks)	1	2	3	4	5	6	7	8	9	10	11	EW 1	EW 2	EW 3	12
1	Research and background Section	23/01/2017	12/02/2017	3															
1.1	Complete Work Plan	23/01/2017	29/01/2017	1															
1.2	Research police guidelines and procdures in the UK and Europe	30/01/2017	05/02/2017	1															
1.3	Collect research on current and future hardware	30/01/2017	05/02/2017	1															
1.4	Research guidelines from America and Asia	06/02/2017	12/02/2017	1															
1.5	Collect list of perferable tools	06/02/2017	12/02/2017	1															
2	Approach and Implementation	13/02/2017	19/03/2017	5															
2.2	Write Procedure for Verfication of Forensic crime	13/02/2017	19/02/2017	1															
2.3	Write Procedure for Collection of Forensic data	20/02/2017	26/02/2017	1															
2.4	Write Procedure for Analysis of Forensic data	27/02/2017	12/03/2017	2															
2.5	Continue Procedure for Analysis of Forensic data	06/03/2017	12/03/2017	2															
2.6	Write Procedure for Storage of Forensic information	13/03/2017	19/03/2017	1															
2.7	Supervisor Milestone Meeting	13/03/2017	19/03/2017	1															
3	Testing	20/03/2017	02/04/2017	2															
3.1	Collect Tools and Write test plans	20/03/2017	26/03/2017	1															
3.2	Test Tools and write up documentation	27/03/2017	02/04/2017	1															
4	Final Report Deliverable	03/04/2017	05/05/2017	5															
4.1	Supervisor Milestone Meeting	03/04/2017	09/04/2017	1															
4.2	Draw up final report structure	03/04/2017	09/04/2017	1															
4.3	Evaluate Chosen Procedures	10/04/2017	16/04/2017	1															
4.4	Write up future additions to the standard and Reflection of the project structure	17/04/2017	23/04/2017	1															
4.5	Reference Checking and Finish bibliography	24/04/2017	30/04/2017	1															
4.6	Grammar, spell checking and finish final report	01/05/2017	05/05/2017	1															
5	Continuous Tasks	26/01/2017	04/05/2017	15															
5.1	Review Gantt Chart	06/02/2017	23/04/2017	11															
5.2	Meetings with supervisor	26/01/2017	04/05/2017	15															

Key	Colour/symbols
Completed Tasks	
Weekly Scale	
Provisional Task Targets	
Milestone	

References

ISO/IEC 27037:2012 — Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence[online]. Available at: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44381 [Accessed: 30 January 2017].

ACPO Good Practice Guide for Digital Evidence - Available at: http://library.college.police.uk/docs/acpo/digital-evidence-2012.pdf [Accessed: 30 January 2017].

ISO/IEC 17025:2005 – General requirements for the competence of testing and calibration laboratories [online] Available at: http://www.iso.org/iso/catalogue_detail?csnumber=39883 [Accessed: 30 January 2017]