Simplified and Inexpensive Mobile Digital Forensic Device

A Thesis Presented to

The Faculty of the Computer Science Department

California State University Channel Islands

In (Partial) Fulfillment

of the Requirements for the Degree

Masters of Science in Computer Science

by

Eric Elwood Gentry

Advisor: Michael Soltys

December 2018

APPROVED FOR MS IN COMPUTER SCIENCE

Advisor: Advisor Name **Date**

Name **Date**

Name **Date**

APPROVED FOR THE UNIVERITY

Name **Date**

Non-Exclusive Distribution License

In order for California State University Channel Islands (CSUCI) to reproduce, translate and distribute your submission worldwide through the CSUCI Institutional Repository, your agreement to the following terms is necessary. The author(s) retain any copyright currently on the item as well as the ability to submit the item to publishers or other repositories.

By signing and submitting this license, you (the author(s) or copyright owner) grants to CSUCI the nonexclusive right to reproduce, translate (as defined below), and/or distribute your submission (including the abstract) worldwide in print and electronic format and in any medium, including but not limited to audio or video.

You agree that CSUCI may, without changing the content, translate the submission to any medium or format for the purpose of preservation.

You also agree that CSUCI may keep more than one copy of this submission for purposes of security, backup and preservation.

You represent that the submission is your original work, and that you have the right to grant the rights contained in this license. You also represent that your submission does not, to the best of your knowledge, infringe upon anyone's copyright. You also represent and warrant that the submission contains no libelous or other unlawful matter and makes no improper invasion of the privacy of any other person.

If the submission contains material for which you do not hold copyright, you represent that you have obtained the unrestricted permission of the copyright owner to grant CSUCI the rights required by this license, and that such third party owned material is clearly identified and acknowledged within the text or content of the submission. You take full responsibility to obtain permission to use any material that is not your own. This permission must be granted to you before you sign this form.

IF THE SUBMISSION IS BASED UPON WORK THAT HAS BEEN SPONSORED OR SUPPORTED BY AN AGENCY OR ORGANIZATION OTHER THAN CSUCI, YOU REPRESENT THAT YOU HAVE FULFILLED ANY RIGHT OF REVIEW OR OTHER OBLIGATIONS REQUIRED BY SUCH CONTRACT OR AGREEMENT.

The CSUCI Institutional Repository will clearly identify your name(s) as the author(s) or owner(s) of the submission, and will not make any alteration, other than as allowed by this license, to your submission.

Title of Item

3 to 5 keywords or phrases to describe the item

Author(s) Name (Print)

Author(s) Signature Date

Simplified and Inexpensive Mobile Digital Forensic Device

Eric Elwood Gentry

May 7, 2018

Abstract

Contents

List of Figures

1 Introduction

2 Background

2.1 Review Material and Analysis

Testing the harmonised digital forensic investigation process model-using an Android mobile phone [8]

Forensic analysis of iPhone backups [9]

Forensic analysis of social networking applications on mobile devices [1]

A practical and robust approach to coping with large volumes of data submitted for digital forensic examination [10]

Jailbroken iPhone Forensics for the Investigations and Controversy to Digital Evidence [2]

Methods and tools of digital triage in forensic context: survey and future directions [6]

Current challenges and future research areas for digital forensic investigation [7]

A survey of digital forensic investigator decision processes and measurement of decisions based on enhanced preview [5]

Forensic examination of digital evidence: a guide for law enforcement [3]

Tiered forensic methodology model for Digital Field Triage by non-digital evidence specialists [4]

3 Conclusion and future work

Your work goes here

References

[1] Noora Al Mutawa, Ibrahim Baggili, and Andrew Marrington. Forensic analysis of social networking applications on mobile devices. *Digital Investigation*, 9:S24–S33, 2012.

[2] Ya-Ting Chang, Ke-Chun Teng, Yu-Cheng Tso, and Shiuh-Jeng Wang. Jailbroken iphone forensics for the investigations and controversy to digital evidence. *Journal of Computers*, 26(2), 2015.

[3] Sara V Hart, John Ashcroft, and Deborah J Daniels. Forensic examination of digital evidence: a guide for law enforcement. *National Institute of Justice NIJ-US, Washington DC, USA, Tech. Rep. NCJ*, 199408, 2004.

[4] Ben Hitchcock, Nhien-An Le-Khac, and Mark Scanlon. Tiered forensic methodology model for digital field triage by non-digital evidence specialists. *Digital Investigation*, 16:S75–S85, 2016.

[5] Joshua I James and Pavel Gladyshev. A survey of digital forensic investigator decision processes and measurement of decisions based on enhanced preview. *Digital Investigation*, 10(2):148–157, 2013.

[6] Vacius Jusas, Darius Birvinskas, and Elvar Gahramanov. Methods and tools of digital triage in forensic context: survey and future directions. *Symmetry*, 9(4):49, 2017.

[7] David Lillis, Brett Becker, Tadhg O'Sullivan, and Mark Scanlon. Current challenges and future research areas for digital forensic investigation. *arXiv preprint arXiv:1604.03850*, 2016.

[8] Stacey Omeleze and Hein S Venter. Testing the harmonised digital forensic investigation process model-using an android mobile phone. In *Information Security for South Africa, 2013*, pages 1–8. IEEE, 2013.

[9] B Satish. Forensic analysis of iphone backups. *Securitylearn. net*.

[10] Adrian Shaw and Alan Browne. A practical and robust approach to coping with large volumes of data submitted for digital forensic examination. *Digital Investigation*, 10(2):116–128, 2013.