Chapter 21
iPhone Forensics:
Recovering Investigative Evidence using Chip-off Method

Nilay R. Mistry
Institute of Forensic Science, Gandhinagar, India

Harshal Patel
Institute of Forensic Science, Gandhinagar, India

Binoj Koshy
Institute of Forensic Science, Gandhinagar, India

Dhaval Parekh
Institute of Forensic Science, Gandhinagar, India

Mohindersinh Dahiya
Institute of Forensic Science, Gandhinagar, India

Jaidip Kotak
Institute of Forensic Science, Gandhinagar, India

Chirag Chaudhary
Institute of Forensic Science, Gandhinagar, India

Komal Nayi
Institute of Forensic Science, Gandhinagar, India

Priyanka Badva
Institute of Forensic Science, Gandhinagar, India

ABSTRACT

Smartphone usage has increased in the recent past and has become an extension of the personal computer, so has the complexity of forensic investigation. Vital information on these devices makes them more critical especially when it is part of investigative evidences. The challenge here is the extraction of data, especially when the phone is logically or physically damaged. Chip-off is a niche technique, involving removal of Flash Memory chip with due sophistication, this then is subjected to direct extraction and analysis. Apple iPhones are robust and well locked; the study performed chip-off on model A1203 that revealed vital forensic evidences.

DOI: 10.4018/978-1-7998-3025-2.ch021

Copyright © 2020, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

INTRODUCTION

Penetration of Smart Phone into the environment has made the field of Digital Forensics a challenging task for experts in this field. The variance and models of these smart devices, which are otherwise extension of a PDA (Personal Digital Assistant), has poised indomitable challenge to forensic experts and investigators. The artifacts are extremely numerous and complex hence making the option more difficult then envisaged. The new advent of a branch namely "Mobile Phone Forensics" is a jargon, which is here to stay. Mobile phone forensics is even more challenging especially when miniaturization & chip integration are taking place at a faster pace is taking place as days passed by. The mushrooming of forensic tools with the increase in the number of Operating Systems, Models, variance, technology, hardware profiling, etc has also made the field more critical.

Experts are now resorting to Level-4 forensics, when it comes to handling investigative artifacts of such hand held smartphone devices. The level-4 digital forensics of smartphone entails chip-off and subsequent acquisition of artifacts from these devices. The less known level-4 digital forensics is also an enabler especially when the device is physically damaged or when the macro kernel is disintegrated from the hardware chip. This paper proposes to bring out the significance and the scope of chip-off as a digital forensic means to extract evidence when all other conventional forms of artefact extraction have not yielded desired output.

SMARTPHONE AND ITS TAXONOMY

Today Smartphone devices are widespread and they hold a number of types of information about the owner and their activities. As a result of the widespread adoption of these devices into every aspect of our lives they can be involved in almost any crime. The aim of digital forensics of Smartphone devices is to recover the digital evidence in a forensically sound manner so that the digital evidence can be forensically presentable and accepted in court. The digital forensic process consists of four phases, which are Preservation, Acquisition, Examination/Analysis and final Presentation. In this paper, we look at various types of smartphone formats and their associated digital evidence. The digital forensics process of the Smartphone devices is discussed and, this paper also contains recommended guidelines and procedures for how to perform the phases of the digital forensics process on Smartphone devices using the chip-off technique.

A smartphone contains much of the functionality of a desktop PC (Personal Computer), but it also includes radio communications capabilities that desktop PCs typically lack. Communication functionalities include GSM/CDMA (Global System for Mobiles / Code Division Multiple Access) radio, NFC (Near Field Communications), GPS (Global Positioning System), Wi-Fi and Bluetooth communication. The high mobility of these devices can be the most important factor in the shift from desktop/laptop computer to smartphones. Unlike laptops or desktop computers, a smartphone can easily fit in a pocket. It is a computer that is easy to use and small enough to be used almost anywhere. A user can browse the Internet, check email, use GPS navigation, and make online payments from personal bank accounts. Hence, a device this capable is also likely to contain personal user data.

There are various ways a user can protect his or her personal information on smartphones. Android and iOS (Operating System) phones can be set up by means of authentication login and password protected application access. Some phones include a data encryption method to protect sensitive data. Also,

15 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/iphone-forensics/252695

Related Content

Offender Mobility and Crime Pattern Formation from First Principles
P. Jeffrey Brantinghamand George Tita (2008). *Artificial Crime Analysis Systems: Using Computer Simulations and Geographic Information Systems (pp. 193-208).*
www.irma-international.org/chapter/offender-mobility-crime-pattern-formation/5264

A Prelude to Cybersecurity Challenges in the Metaverse
Shashwath Bhaskar, Aiesha Kuna, Akshaya Jayakumarand D. Lakshmi (2024). *Forecasting Cyber Crimes in the Age of the Metaverse (pp. 149-170).*
www.irma-international.org/chapter/a-prelude-to-cybersecurity-challenges-in-the-metaverse/334499

Watermark Embedding for Multiscale Error Diffused Halftone Images by Adopting Visual Cryptography
Yuanfang Guo, Oscar C. Auand Ketan Tang (2015). *International Journal of Digital Crime and Forensics (pp. 51-68).*
www.irma-international.org/article/watermark-embedding-for-multiscale-error-diffused-halftone-images-by-adopting-visual-cryptography/127342

Steganography in Thai Text
Natthawut Samphaiboonand Matthew N. Dailey (2010). *International Journal of Digital Crime and Forensics (pp. 43-64).*
www.irma-international.org/article/steganography-thai-text/46046

Web Bot Detection System Based on Divisive Clustering and K-Nearest Neighbor Using Biostatistics Features Set
Rizwan Ur Rahmanand Deepak Singh Tomar (2021). *International Journal of Digital Crime and Forensics (pp. 1-27).*
www.irma-international.org/article/web-bot-detection-system-based-on-divisive-clustering-and-k-nearest-neighbor-using-biostatistics-features-set/302136