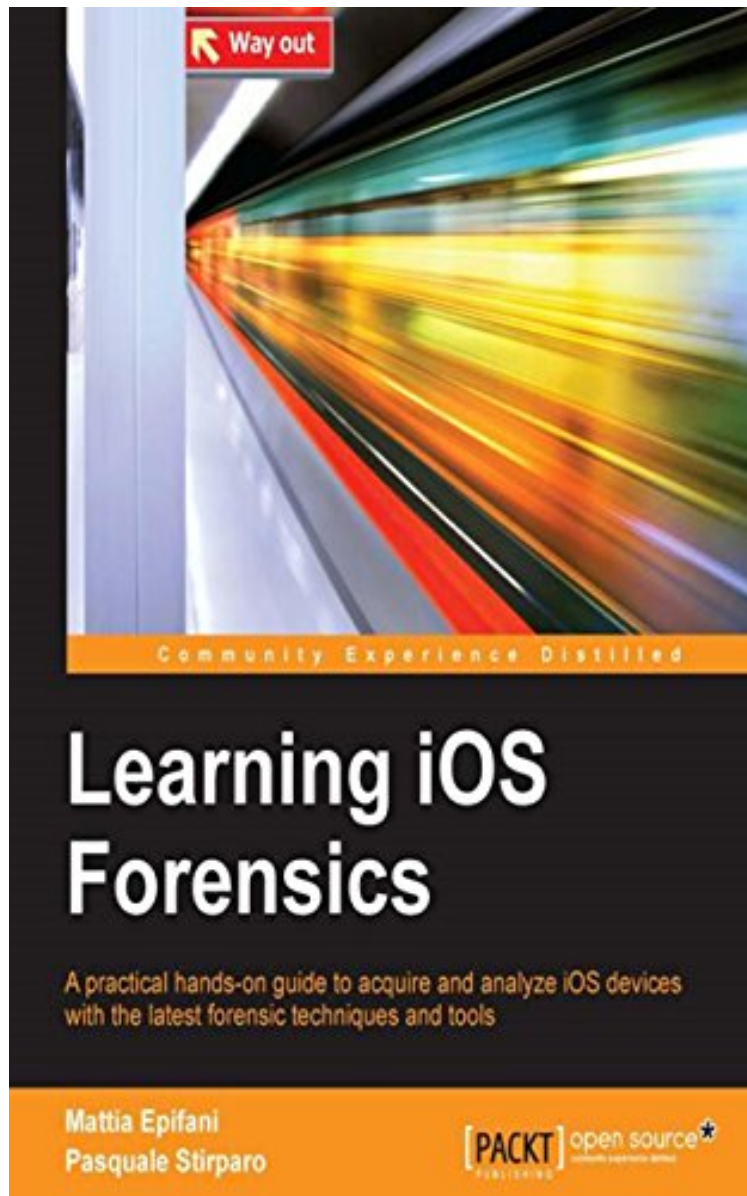


Learning iOS Forensics

Von Mattia Epifani, Pasquale Stirparo
*ePub | *DOC | audiobook | ebooks | Download PDF*



[Download](#)

[Read Online](#)

Produktinformation -Verkaufsrang: #438345 in eBooksVerffentlicht am: 2015-03-10Erscheinungsdatum: 2015-03-10File Name: B00UJRFGVW | File size: 28.Mb

Von Mattia Epifani, Pasquale Stirparo : Learning iOS Forensics before purchasing it in order to gage whether or not it would be worth my time, and all praised Learning iOS Forensics:

KundenrezensionenHilfreichste Kundenrezensionen0 von 0 Kunden fanden die folgende Rezension hilfreich. Nice bookVon TekDive2001This is a nice written book and gives a basic overview about iOS Forensics. It is a must have

for everyone who is involved in mobile forensics.

KurzbeschreibungA practical hands-on guide to acquire and analyze iOS devices with the latest forensic techniques and tools
About This BookPerform logical, physical, and file system acquisition along with jailbreaking the device
Get acquainted with various case studies on different forensic toolkits that can be used
A step-by-step approach with plenty of examples to get you familiarized with digital forensics in iOS
Who This Book Is ForIf you are a digital forensics examiner daily involved in the acquisition and analysis of mobile devices and want to have a complete overview of how to perform your work on iOS devices, this book is definitely for you.
What You Will LearnIdentify an iOS device among various models (iPhone, iPad, and iPod Touch) and verify the iOS version installed
Crack or bypass the passcode protection chosen by the user
Acquire detailed physical or logical info of an iOS device
Retrieve extra information from side channel data leaks
Recover information from a local backup and eventually crack the backup password
Download backup information stored on iCloud
Analyze the system, user, and third-party information from a device, backup, or iCloud
Examine malicious apps to identify the stolen data and credentials
In DetailMobile device forensics relates to the recovery of data from a mobile device. It has an impact on many different situations including criminal investigations and intelligence gathering. iOS devices, with their wide range of functionality and usability, have become one of the mobile market leaders. Millions of people often depend on iOS devices for storing sensitive information, leading to a rise in cybercrime. This has increased the need to successfully retrieve this information from these devices if stolen or lost.
Learning iOS Forensics will give you an insight into the forensics activities you can perform on iOS devices. You will begin with simple concepts such as identifying the specific iOS device and the operating system version and then move on to complex topics such as analyzing the different recognized techniques to acquire the content of the device. Throughout the journey, you will gain knowledge of the best way to extract most of the information by eventually bypassing the protection passcode. After that, you, the examiner, will be taken through steps to analyze the data. The book will give you an overview of how to analyze malicious applications created to steal user credentials and data.
KurzbeschreibungA practical hands-on guide to acquire and analyze iOS devices with the latest forensic techniques and tools
About This BookPerform logical, physical, and file system acquisition along with jailbreaking the device
Get acquainted with various case studies on different forensic toolkits that can be used
A step-by-step approach with plenty of examples to get you familiarized with digital forensics in iOS
Who This Book Is ForIf you are a digital forensics examiner daily involved in the acquisition and analysis of mobile devices and want to have a complete overview of how to perform your work on iOS devices, this book is definitely for you.
What You Will LearnIdentify an iOS device among various models (iPhone, iPad, and iPod Touch) and verify the iOS version installed
Crack or bypass the passcode protection chosen by the user
Acquire detailed physical or logical info of an iOS device
Retrieve extra information from side channel data leaks
Recover information from a local backup and eventually crack the backup password
Download backup information stored on iCloud
Analyze the system, user, and third-party information from a device, backup, or iCloud
Examine malicious apps to identify the stolen data and credentials
In DetailMobile device forensics relates to the recovery of data from a mobile device. It has an impact on many different situations including criminal investigations and intelligence gathering. iOS devices, with their wide range of functionality and usability, have become one of the mobile market leaders. Millions of people often depend on iOS devices for storing sensitive information, leading to a rise in cybercrime. This has increased the need to successfully retrieve this information from these devices if stolen or lost.
Learning iOS Forensics will give you an insight into the forensics activities you can perform on iOS devices. You will begin with simple concepts such as identifying the specific iOS device and the operating system version and then move on to complex topics such as analyzing the different recognized techniques to acquire the content of the device. Throughout the journey, you will gain knowledge of the best way to extract most of the information by eventually bypassing the protection passcode. After that, you, the examiner, will be taken through steps to analyze the data. The book will give you an overview of how to analyze malicious applications created to steal user credentials and data.
ber den Autor und weitere Mitwirkende
Mattia Epifani
Mattia Epifani (@mattiaep) is the CEO at Reality Net-System Solutions, an Italian consulting company involved in InfoSec and digital forensics. He works as a digital forensics analyst for judges, prosecutors, lawyers, and private companies. He is a court witness and digital forensics expert. He obtained a university degree in computer science in Genoa, Italy, and a postgraduate specialization course in computer forensics and digital investigations in Milan, Italy. Over the last few years, he obtained several certifications in digital forensics and ethical hacking (GCFA, GREM, GNFA, GCWN, GMOB, CIFI, CEH, CHFI, ACE, AME, ECCE, CCE, and MPSC) and attended several SANS classes (computer forensics and incident response, Windows memory forensics, mobile device security and ethical hacking, reverse engineering malware, smartphone forensics, Mac forensics, securing Windows, and network forensics analysis). He speaks regularly on digital forensics at different Italian and European universities (Genoa, Milano, Roma, Bolzano, Pescara, Salerno, Campobasso, Camerino, Pavia, Savona, Catania, Lugano, Como, and Modena e Reggio Emilia) and events (DFRWS, SANS European Digital Forensics Summit, Security Summit, IISFA Forum,

DEFT Conference, and DFA Open Day). He is a member of CLUSIT, DFA, IISFA, ONIF, and Tech and Law Center, and the author of various articles on scientific publications about digital forensics. More information is available on his LinkedIn profile (<http://www.linkedin.com/in/mattiaepifani>). Pasquale Stirparo Pasquale Stirparo (@pstirparo) is currently working as a cyber threat intelligence and incident response engineer at a Fortune 500 company. Prior to this, among other positions, Pasquale has also worked at the Joint Research Centre (JRC) of the European Commission as a digital forensics and mobile security researcher, with particular interest in the security and privacy issues related to mobile device communication protocols, mobile applications, mobile malware, and cybercrime. Since 2016, he has been appointed to the Advisory Group on Internet Security at the European Cyber Crime Center (EC3) of Europol and is an incident handler with the SANS Internet Storm Center (ISC). Pasquale has also been involved in the standardization of Digital Forensics as a contributor (the first in Italy) to the development of the standard ISO/IEC 27037: Guidelines for identification, collection and/or acquisition and preservation of digital evidence, for which he led the WG ISO27037 for the Italian National Body in 2010. He is the author of many scientific publications and has also been invited as a speaker at several national and international conferences and seminars on Digital Forensics and as a lecturer on the same subject for the Polytechnic of Milano (CEFRIEL) and the United Nations (UNICRI). Pasquale holds a Ph.D. in Computer Security from the Royal Institute of Technology (KTH) of Stockholm and a M.Sc. in Computer Engineering from the Polytechnic of Torino, and is certified with GCFA, GREM, OPST, OWSE, and ECCE. More information is available on his LinkedIn personal profile (<https://www.linkedin.com/in/pasqualestirparo>).