CERIAS

The Center for Education and Research in Information Assurance and Security

Leveraging Memory Forensics to Decrypt iOS Backups

Colin Cowie and Marcus Thompson
Department of Computer and Information Technology

Abstract

This research focuses on the analysis of random access memory of a personal computer to discover digital artifacts from previously connected iOS device. This study aimed to locate information including AppleID credentials, encrypted backup passwords, sensitive device information and more. For some iOS artifacts, it was possible to locate them in memory as well create techniques to locate them without knowing their value beforehand. Therefore, this is a step towards using memory forensics for discover mobile investigations.

Problem Overview

The amount of iOS devices globally has been increasing. Mobile forensics often has limitations in obtaining evidence due to the rapid changes in technology and the advancement of mobile software and operating systems (Mahalik, 2016). Law enforcement and forensics examiners often struggle to obtain digital evidence from mobile devices (Mahalik, 2016). When iOS device users backup their phone to a computer, a repository of important information is stored on the computer. Depending on the device, the best information may be found within the iOS backup (Mahalik, 2016). In some cases, traditional computer forensics play an important role for analyzing a mobile device. Techniques that could provide evidence about iOS devices from the memory of a personal computer have the potential to significantly assist law enforcement and forensics examiners aiming to retrieve iOS artifacts. The law enforcement community needs up to date methods and techniques to assist mobile device investigations.

References

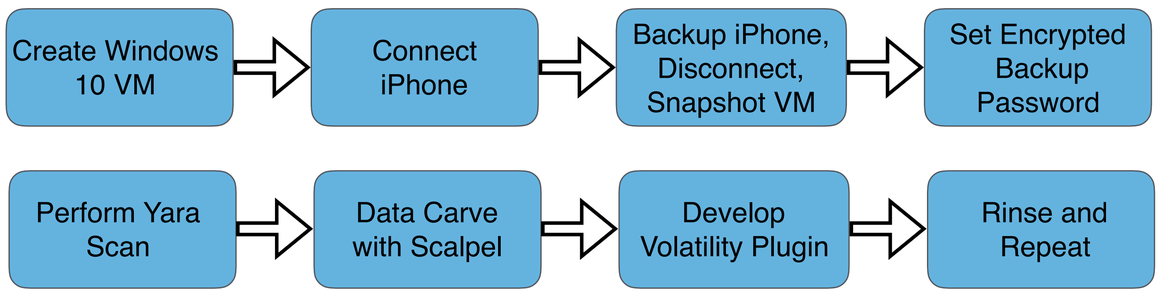
IDC (2016). *Smartphone OS Market Share*. Retrieved October 6, 2017, from http://www.idc.com/promo/smartphone-market-share/os

Mahalik, H. (2016). *Practical mobile forensics: A hands-on guide to mastering mobile forensics for the iOS, Android, and the Windows Phone platforms Second Edition*. Birmingham: Packt Publishing.

Case, A., Ligh, M. H., Levy, J., & Walters, A. (2014). *The art of memory forensics: detecting malware and threats in Windows, Linux, and Mac memory.* Indianapolis, IN: Wiley.

Methodology

The procedures were divided into two general phases: acquisition and analysis. Each phase contained four steps. The first step in the acquisition phase consisted of setting up the environment used in this research. During phase one steps two and three, an iPhone 7 was connected to a Windows 10 machine, iCloud was signed in, and an encrypted iTunes backup was created. Once the backup was completed, the device was disconnected and the Windows 10 computer's memory was captured. Phase two consisted of analyzing the memory capture for the specified iOS artifacts. In phase two step one, the memory capture was analyzed with the Volatility Framework Yarascan plugin. In step two Scalpel was used to attempt to extract the artifacts found from the Yarascan. For the artifacts that were found, the Volatility library was used to attempt to locate them without previously knowing its value. If any of the the artifacts were not able to be found within the memory capture, then a negative hypothesis for that artifact was recorded.



Results

Through the use of Volatility, Yara scans and Scalpel eight of the ten specified artifacts were located. The results are shown below.

Artifact	Found	Process
AppleID Login	TRUE	iCloudDrive.exe
AppleID Password	FALSE	N/A
Device Name	TRUE	AppleMobileDevice.exe iTunes.exe
iOS Backup Location	TRUE	AppleMobileDevice.exe iTunes.exe
iOS Backup Encryption Status	TRUE	iTunes.exe
iOS Backup Password	TRUE	iTunes.exe
International Mobile Equipment Identity (IMEI)	TRUE	AppleMobileDevice.exe iTunes.exe
Device Model	TRUE	AppleMobileDevice.exe iTunes.exe
Serial Numer	TRUE	AppleMobileDevice.exe iTunes.exe
Device PIN Number	FALSE	N/A