Bộ môn An toàn Thông tin – Khoa MMT&TT
Trường Đại học Công nghệ Thông tin (UIT)

BÁO CÁO BÀI TẬP

Môn học: Pháp chứng kỹ thuật số

Kỳ báo cáo: Buổi

Tên chủ đề: Android Forensics

GVHD: Lê Đức Thịnh

Ngày báo cáo: 24/5/2023

Nhóm:

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT334.N21.ANTN

STT	Họ và tên	MSSV	Email
1	Võ Anh Kiệt	20520605	20520605@gm.uit.edu.vn
2			
3			

2. NỘI DUNG THỰC HIỆN:[1]

STT	Công việc	Thực hiện	Thành viên thực hiện	Kết quả tự đánh giá
1	App		100%	
2	Device		100%	

[1] Ghi nội dung công việc, các kịch bản trong bài Thực hành,

BÁO CÁO CHI TIẾT

Application

1 Instagram Mobile Application Digital Forensics

Doi: 10.32604/csse.2021.014472

Mục tiêu: a plugin for our automated digital forensics framework to extract and preserve the evidence from the Android and the IOS-based mobile phone application, Instagram.

Không có github

Công cụ winhex

2 A Method of Android Application Forensics Based on Heap Memory Analysis

Doi: 10.1145/3207677.3277934

Mục tiêu: a new method of Android application forensics, based on the heap memory analysis. In this method, the heap memory data of an Android app, running on the virtual machine, is directly extracted, parsed and reconstructed.

Không github

Không tool

3 A Forensic Investigation of Android Mobile Applications

Doi: 10.1145/3291533.3291573

Mục tiêu: a forensic investigation to a set of Android mobile applications aiming at discovering sensitive information related to the owner of the mobile device.

Không github

Ngôn ngữ code: Java

4 The Android Forensics Automator (AnForA): A tool for the Automated Forensic Analysis of Android Applications

Doi: 10.1016/j.cose.2019.101650

Mục tiêu: the design, implementation, and evaluation of AnForA, a software tool that automates most of the activities that need to be carried out to forensically analyze Android applications, and that has been designed in such a way to yield various important properties, namely fidelity, artifact coverage, artifact precision, effectiveness, repeatability, and generality.

Không github

5 Network and device forensic analysis of Android social-messaging applications

Doi: 10.1016/j.diin.2015.05.009

Mục tiêu: We were able to reconstruct some or the entire message content from 16 of the 20 applications tested, which reflects poorly on the security and privacy measures employed by these applications but may be construed positively for evidence collection purposes by digital forensic practitioners.

Không github

6 Forensic investigation of OneDrive, Box, GoogleDrive and Dropbox applications on Android and iOS devices

Doi: 10.1080/00450618.2015.1110620

Mục tiêu: four popular cloud client apps, namely OneDrive, Box, GoogleDrive, and Dropbox, on both Android and iOS platforms (two of the most popular mobile operating systems). We identify artefacts of forensic interest, such as information generated during login, uploading, downloading, deletion, and the sharing of files. These findings may assist forensic examiners and practitioners in real-world examination of cloud client applications on Android and iOS platforms.

Không github

7 Forensic Analysis of Secure Ephemeral Messaging Applications on Android Platforms

Doi: 10.1007/978-3-319-51064-4_3

Mục tiêu: This paper forensically analyses two secure messaging applications, Wickr and Telegram, to recover artefacts from and then to compare them to reveal the differences between the applications. The artefacts were created on Android platforms by using the secure features of the applications, such as ephemeral messaging, the channel function and encrypted conversations.

Không github

8 Automated forensic analysis of mobile applications on Android devices

Doi: 10.1016/j.diin.2018.04.012

Mục tiêu: a fully automated tool, Fordroid for the forensic analysis of mobile applications on Android. Fordroid conducts inter-component static analysis on Android APKs and builds control flow and data dependency graphs. Furthermore, Fordroid identifies what and where information written in local storage with taint analysis. Data is located by traversing the graphs. This addresses several technique challenges, which include inter-component string propagation, string operations (e.g., append) and API invocations. Also, Fordroid identifies how the information is stored by parsing SQL commands, i.e., the structure of database tables. Finally, we selected 100 random Android applications consisting of 2841 components from four categories for evaluation.

9 Breaking into the vault: Privacy, security and forensic analysis of Android vault applications

Doi: 10.1016/j.cose.2017.07.011

Mục tiêu: Our results showed that 12/18 obfuscated their code and 5/18 applications used native libraries hindering the reverse engineering process of these applications

Không github

10 Map My Murder! A Digital Forensic Study of Mobile Health and Fitness Applications

Doi: 10.1145/3339252.3340515

Mục tiêu: Augmenting that with ongoing user activities, such as the user's walking paths, could potentially create exculpatory or inculpatory digital evidence. We conducted extensive manual analysis and explored forensic artifacts produced by (n = 13) popular Android mobile health and fitness applications.

Không github

Device

1 Forensic analysis of social networking applications on mobile devices

Doi: 10.1016/j.diin.2012.05.007

Mục tiêu: Potential evidence can be held on these devices and recovered with the right tools and examination methods. This paper focuses on conducting forensic analyses on three widely used social networking applications on smartphones: Facebook, Twitter, and MySpace. The tests were conducted on three popular smartphones: BlackBerrys, iPhones, and Android phones.

Không github

2 Forensic Analysis of Android Runtime (ART) Application Heap Objects in Emulated and Real Devices

Doi: 10.1007/978-3-319-93354-2_7

Mục tiêu: a new forensic technique for analyzing ART memory objects using a volatile memory data extraction. Considering the Android Open Source Project (AOSP) source code, a method and associated software tools were developed allowing the location, extraction and interpretation of arbitrary ART memory instances with the respective object classes and their data properties. The proposed technique and tools were validated both for emulated and real devices, illustrating the difficulties related to the forensics analysis for the target system due to its particular implementations by multiple manufacturers of mobile devices.

Không github

3 An Anti-forensics Method against Memory Acquiring for Android Devices

Doi: 10.1109/CSE-EUC.2017.45

Mục tiêu: presents an anti-forensics approach for Android devices which protects AES keys from being acquired by forensics tools. The keys are stored in the special memory space where the data will be covered when android reboots, thus attackers can not steal the privacy information.

4 Location Tracking Forensics on Mobile Devices

Doi: 10.1117/12.2003952

Mục tiêu: common procedures for securing and testing of mobile devices. Further there will be represented the specials in the investigation of each device. The different classes considered are GPS handhelds, mobile navigation devices and smartphones. It will be attempted, wherever possible, to read all data of the device. This is realized by the usage of current forensic software e.g. TomTology or Oxygen Forensic Suite. It is also attempted to use free software whenever possible.

5 Forensic investigation of OneDrive, Box, GoogleDrive and Dropbox applications on Android and iOS devices

Doi: 10.1080/00450618.2015.1110620

Mục tiêu: Consequently, mobile devices are an increasing important source of evidence in digital investigations. In this paper, we examine four popular cloud client apps, namely OneDrive, Box, GoogleDrive, and Dropbox, on both Android and iOS platforms (two of the most popular mobile operating systems). We identify artefacts of forensic interest, such as information generated during login, uploading, downloading, deletion, and the sharing of files. These findings may assist forensic examiners and practitioners in real-world examination of cloud client applications on Android and iOS platforms.

6 On the Efficacy of Using Android Debugging Bridge for Android Device Forensics

Mục tiêu: Evaluating a wide range of tools enables the selection of the appropriate tool for a given investigation. One method of evaluating forensic tools is to analyze the tools ability to detect mobile malware. Many commercial and open source forensic tools do not effectively find malware on a mobile device. This gap in capabilities requires a manual approach to extracting such data. This current study documents an experimental study to determine the efficacy of specific commercial tools in identifying malware on an Android phone

7 Mobile forensic reference set (MFReS) and mobile forensic investigation for android devices

Doi: 10.1007/s11227-017-2205-5

Mục tiêu: the mobile forensic reference set (MFReS), a mobile forensic investigation procedure and a tool for mobile forensics that we developed. The MFReS consists of repositories, databases, and services that can easily retrieve data from a database, which can be used to effectively classify meaningful data related to crime, among numerous data types in mobile devices.

8 Rapid differential forensic imaging of mobile devices

Doi: 10.1016/j.diin.2016.04.012

Mục tiêu: an automated differential forensic acquisition technique and algorithm that uses baseline datasets and hash comparisons to limit the amount of data sent from a mobile device to an acquisition endpoint.

9 Forensics of location data collected by Google Android mobile devices

Doi: 10.1117/12.909891

Mục tiêu: This paper deals with forensic investigation of stored location data collected by Android mobile devices. The main aspects of the study are the extraction and examination of the location data and the possibilities for additional use of the extracted data.

10 Towards a Forensic Analysis of Mobile Devices Using Android

Doi: 10.1007/978-3-319-73450-7_4

Mục tiêu: using a comparative method to allow us to formulate a forensic analysis to mobile devices with Android operating system; based on the chain of custody guidelines, compliance stages, and phases and to detect findings, nonconformities, locate vulnerabilities. Based

Lưu ý: Chỉ ghi Kịch bản thực hành được GVTH chỉ định phải làm báo cáo

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

(Xem trang kế tiếp)

Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này

YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hành theo hướng dẫn.
- Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
- Sinh viên báo cáo kết quả thực hiện và nộp bài.

Báo cáo:

- File .DOCX và .PDF. Tập trung vào nội dung, không mô tả lý thuyết.
- Nội dung trình bày bằng Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)– cỡ chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.
- Đặt tên theo định dạng: [Mã lớp]-SessionX_GroupY. (trong đó X là Thứ tự buổi Thực hành, Y là số thứ tự Nhóm Thực hành đã đăng ký với GVHD-TH).

  Ví dụ: [NT101.H11.1]-Session1_Group3.
- Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
- Không đặt tên đúng định dạng – yêu cầu, sẽ **KHÔNG** chấm điểm bài Lab.
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Đánh giá: Sinh viên hiểu và tự thực hiện được bài thực hành. Khuyến khích:

- Chuẩn bị tốt và đóng góp tích cực tại lớp.
- Có nội dung mở rộng, ứng dụng trong kịch bản phức tạp hơn, có đóng góp xây dựng bài thực hành.

Bài sao chép, trễ, ... sẽ được xử lý tùy mức độ vi phạm.

HẾT