LAB 05

ĐIỀU TRA TRÊN THIẾT BỊ DI ĐỘNG

(Mobile Forensics)

Họ tên và MSSV: Trương Quang Long B2203727

Nhóm học phần: 01

- *Các sinh viên bị phát hiện sao chép bài của nhau sẽ nhận 0đ cho tất cả bài thực hành của môn này.*
- *Bài nộp phải ở dạng PDF, hình minh họa phải rõ ràng chi tiết.* Hình minh hoạ chỉ cần chụp ở nội dung thực hiện, không chụp toàn màn hình.

1. Phân tích hệ điều hành Android với Autopsy

1.1. Tải và cài đặt công cụ Autopsy trên máy tính cá nhân.

1.2. Tải tập tin `Lab05_01.zip`, giải nén được thư mục `Pixel 3`.

1.3. Trên công cụ Autopsy, chọn chức năng “New Case”. Nhập các thông tin cần thiết. Ở mục “Select Data Source Type” chọn “Logical Files”.

- Ở mục “Select Data Source” chỉ đường dẫn đến thư mục `Pixel 3` ở Câu 1.2.
- Ở mục “Configure Ingest Modules” xóa hết lựa chọn, chỉ chừa lại "Android Analyzer (aLEAPP)” và "Android Analyzer”.

1.4. Sau khi quá trình phân tích thành công, ở mục "Data Artifacts" sẽ hiển thị nhiều thông tin hữu ích như Phone calls, Messages, Web searches, …Tìm kiếm thông tin và trả lời các câu hỏi sau:

- Số điện thoại thực hiện cuộc gọi tới thiết bị lúc `2020-02-09 03:30:48 ICT`?
  Số điện thoại đã thực hiện cuộc gọi tới là +19195790479

- Số điện thoại của người tên “`Josh Hickman`”?
  Josh Hickman có số điện thoại là (919) 579-0479.

contacts2.db			0	Josh Hickman	(919) 579-0479
contacts2.db			0	Josh Hickman	(919) 579-0479

- Nội dung tin nhắn được gửi từ số điện thoại `+19842032223` lúc `2020-02-09 03:03:06 ICT`?
  Nội dung tin nhắn được gửi tới là Yep! Have to keep generating data.

2020-02-09 03:03:06 ICT	1	Incoming	+19842032223	…	Yep! Have to keep generating data.

- Địa chỉ website được truy cập vào lúc `2020-01-29 16:33:10 ICT`?
  Chụp hình minh họa các kết quả thực hiện trên.
  Người này đã truy cập vào trang web The CFReDS Project với địa chỉ là https://ww.cfreds.nist.gov/.

Date Accessed	URL	Title
2020-01-29 16:33:10 ICT	https://www.cfreds.nist.gov/	The CFReDS Project

2. Phân tích hệ điều hành iOS với Autopsy

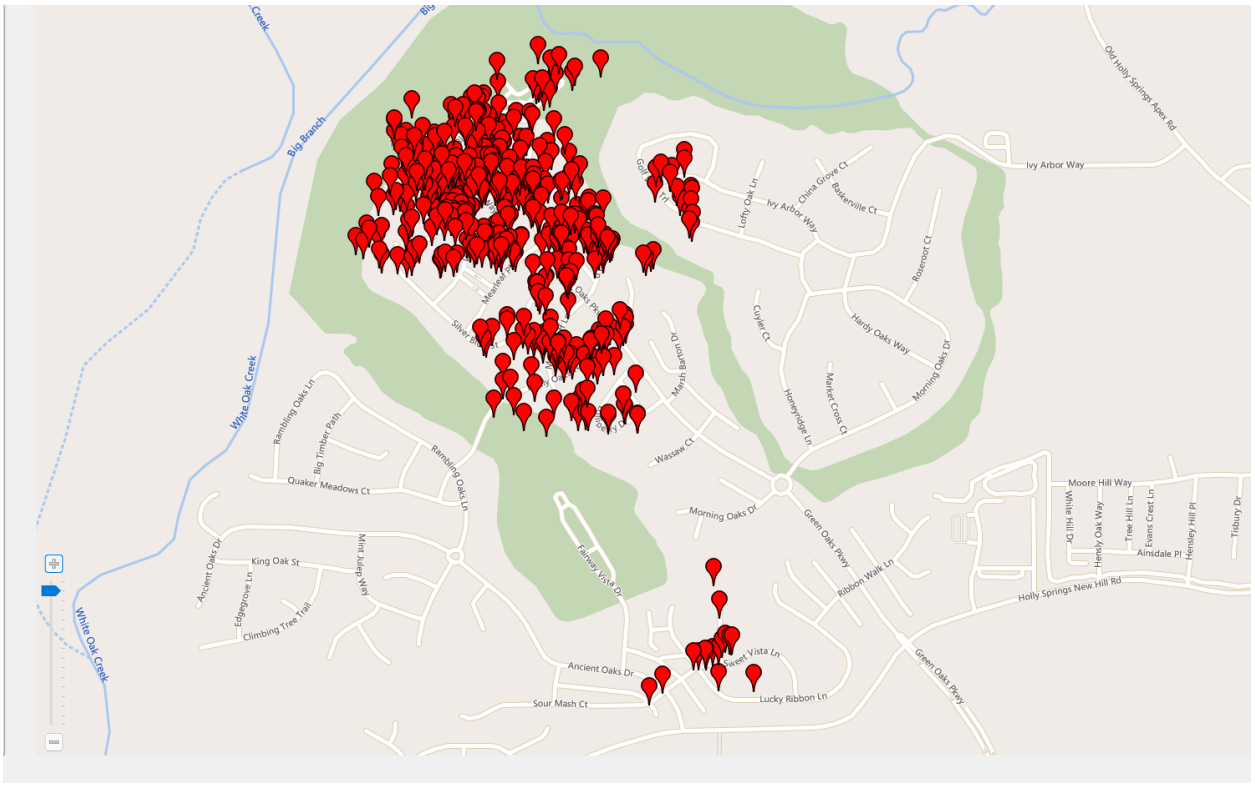
2.1. Tải tập tin `Lab05_02.zip`, giải nén được thư mục chứa dữ liệu `iOS 13.4.1 Extraction`.

2.2. Trên công cụ Autopsy, chọn chức năng “New Case”. Nhập các thông tin cần thiết. Ở mục “Select Data Source Type” chọn “Logical Files”.

- Ở mục “Select Data Source” chỉ đường dẫn đến thư mục `iOS 13.4.1 Extraction` ở Câu 2.1.
- Ở mục “Configure Ingest Modules” xóa hết lựa chọn, chỉ chừa lại "iOS Analyzer (iLEAPP)”.

2.3. Sau khi quá trình phân tích thành công, ở mục "Data Artifacts" sẽ hiển thị nhiều thông tin hữu ích như Phone calls, Messages, Web searches, …Tìm kiếm thông tin và trả lời các câu hỏi sau:
Chụp hình minh họa các kết quả thực hiện trên.

- Dựa vào GPS Last Know Location và chức năng Geolocation tìm các địa điểm mà chủ nhân điện thoại đã di chuyển đến?



- Tìm địa chỉ MAC của airpods của Josh?
  Địa chỉ MAC của airpods của Josh là 7C:04:D0:89:89:A0.

Source Name	S	C	O	Date/Time	MAC Address	Device Name
13-4-1.tar			0	2020-03-27 18:32:52 ICT	7C:04:D0:89:89:A0	Josh's AirPods
13-4-1.tar			0	2020-03-27 18:33:05 ICT	7C:04:D0:89:89:A0	Josh's AirPods
13-4-1.tar			0	2020-03-27 19:22:18 ICT	7C:04:D0:89:89:A0	Josh's AirPods
13-4-1.tar			0	2020-03-27 20:44:05 ICT	7C:04:D0:89:89:A0	Josh's AirPods

- Tên mạng Wi-Fi mà thiết bị đã kết nối vào?
  Tên mạng Wifi thiết bị đã kết nối là CcookiesDcastleR5 Guest.

Source Name	S	C	O	Name	Value	Data Source
13-4-1.tar				IPAddress	192.168.12.20	LogicalFileSet1
13-4-1.tar				LeaseLength	27423	LogicalFileSet1
13-4-1.tar				LeaseStartDate	2020-04-16 16:05:22	LogicalFileSet1
13-4-1.tar				RouterHardwareAddress	b'\xf8\xbb\xbf\x1e\xfa\xf1'	LogicalFileSet1
13-4-1.tar				RouterIPAddress	192.168.12.1	LogicalFileSet1
13-4-1.tar				SSID	CcookiesDcastleR5 Guest	LogicalFileSet1

3. **Hướng dẫn cài đặt Android Studio Simulator**
   Tham khảo, không cần thực hiện
4. **Hướng dẫn rooting Android Studio Simulator**

Tham khảo, không cần thực hiện

5. **Hướng dẫn thu thập dữ liệu trên Android Studio Simulator**
   Tham khảo, không cần thực hiện

--- Hết ---