Học viện Kỹ thuật Quân sự

Báo cáo tiến độ đợt 2

**Đề tài: Điều tra số trên thiết bị di động**

GVHD: TS.Hoàng Tuấn Hảo

Học viên: Đoàn Ngọc Minh Thư

Lớp: CHHTTT – K27A

Mục lục

[Đặt vấn đề 4](#_Toc471925607)

[Chương I. Tổng quan 5](#_Toc471925608)

[I. Điều tra số 5](#_Toc471925609)

[1. Khái niệm 5](#_Toc471925610)

[2. Mục đích và ứng dụng 5](#_Toc471925611)

[2.1 Mục đích 5](#_Toc471925612)

[2.2 Khi nào thì thực sự cần thiết thực hiện một cuộc điều tra số? 5](#_Toc471925613)

[II. Bằng chứng số 5](#_Toc471925614)

[1. Khái niệm 5](#_Toc471925615)

[2. Đặc tính của bằng chứng số 6](#_Toc471925616)

[3. Vị trí có thể tìm thấy bằng chứng số 6](#_Toc471925617)

[II. Phân loại các loại hình điều tra số 9](#_Toc471925618)

[1. Điều tra bản ghi (Registry Forensics) 9](#_Toc471925619)

[2. Điều tra ổ đĩa (Disk Forensics) 10](#_Toc471925620)

[3. Điều tra ứng dụng (Application Forensics) 10](#_Toc471925621)

[4. Điều tra bộ nhớ (Memory Forensics) 11](#_Toc471925622)

[5. Điều tra số trên thiết bị di động (Mobile forensics) 12](#_Toc471925623)

[6. Điều tra mạng (Network Forensics) 12](#_Toc471925624)

[III. Quy trình điều tra số 13](#_Toc471925625)

[IV. Điều tra viên 13](#_Toc471925626)

[1. Khái niệm 13](#_Toc471925627)

[2. Bốn quy tắc đạo đức của điều tra viên (ĐTV) 14](#_Toc471925628)

[2.1 Tránh những điều có hại 14](#_Toc471925629)

[2.2 Không phát tán những thông tin nguy hiểm 14](#_Toc471925630)

[2.3 Sử dụng có chừng mực 14](#_Toc471925631)

[2.4 Luôn giữ bí mật 14](#_Toc471925632)

[Chương 2. Điều tra số trên thiết bị di động (Mobile device Forensics) 15](#_Toc471925633)

[1. Giới thiệu 15](#_Toc471925634)

[2. Các phương pháp kỹ thuật khai thác thông tin dữ liệu trên smartphone 15](#_Toc471925635)

[2.1. Các thông tin lưu trữ trên điện thoại di động 15](#_Toc471925636)

[2.1.1. Thông tin lưu trữ trên SIM: 15](#_Toc471925637)

[2.1.2. Thông tin lưu trữ trên Phone Memory 15](#_Toc471925638)

[2.1.3. Các thông tin lưu trữ trên thẻ nhớ ngoài 15](#_Toc471925639)

[2.2. Tổng quan về kỹ thuật khai thác dữ liệu trên điện thoại di động 16](#_Toc471925640)

[2.3. Kỹ thuật khai thác dữ liệu trên bộ nhớ trong của smartphone 16](#_Toc471925641)

[2.3.1 Kỹ thuật khai thác vật lý 16](#_Toc471925642)

[2.3.2 Kỹ thuật khai thác logic 17](#_Toc471925643)

[2.4 Kỹ thuật khai thác dữ liệu trên SIM 17](#_Toc471925644)

[2.4.1 Kết nối SIM với máy tính thông qua đầu đọc SIM 17](#_Toc471925645)

[Chương 3. Tính năng kỹ thuật, hình thức tổ chức và các chức năng của hệ điều hành Android và SIM 19](#_Toc471925646)

[I. Hệ điều hành Android 19](#_Toc471925647)

[1. Tổng quan 19](#_Toc471925648)

[2. Kiến trúc cơ bản của hệ điều hành Android 19](#_Toc471925649)

[3. Các phiên bản của hệ điều hành Android 20](#_Toc471925650)

[II. SIM 20](#_Toc471925651)

[1. Cấu trúc SIM 20](#_Toc471925652)

[2. Cấu tạo thẻ SIM 21](#_Toc471925653)

[3. Sơ đồ cấu trúc Data trong SIM 21](#_Toc471925654)

[4. Cấu trúc các File 22](#_Toc471925655)

[Chương 4: Xây dựng kịch bản thực tế 23](#_Toc471925656)

[1. Kịch bản thực tế 23](#_Toc471925657)

[2. Hướng giải quyết 23](#_Toc471925658)

[2.1 Thu giữ và bảo quản thiết bị 23](#_Toc471925659)

[2.2 Thu thập dữ liệu trên điện thoại 23](#_Toc471925660)

[3. Xây dựng, phát triển phần mềm thu thập, khai thác dữ liệu từ SIM và bộ nhớ trong của smartphone trên các hệ điều hành Android 24](#_Toc471925661)

# Đặt vấn đề

Với sự phát triển không ngừng của khoa học công nghệ, điện thoại di động đặc biệt là điện thoại di động thông minh đã trở nên rất thân thuộc trong cuộc sống hàng ngày của mỗi chúng ta. Điện thoại di động thông minh trở thành phương tiện giao tiếp trực tiếp. Với một chiếc di động nhỏ gọn chúng ta không những có thể sử dụng để nghe, gọi và nhắn tin mà nó có thể hỗ trợ nhiều dịch vụ tiện ích phục vụ cho việc giải trí, ứng dụng văn phòng như chơi game, nghe nhạc, xem phim, word, excel, tiếp nhận và gửi email…

Với nhiều chức năng tiện ích như vậy, việc sử dụng chiếc điện thoại di động thông minh làm phương tiện để thực hiện các hành vi vi phạm phát luật trong đó có nhiều vụ án liên quan đến việc các đối tượng sử dụng điện thoại để lưu thông tin cá nhân, liên lạc với nhau, trao đổi tin nhắn, truy cập mạng xã hội, các trang web bất hợp pháp…

Từ giả thiết đặt ra, việc khai thác các thông tin từ thiết bị di động của đối tượng, trinh sát đã tìm, xác định được đối tượng, thu thập được nhiều thông tin hữu ích để phục vụ việc điều tra. Qua việc khai thác các thông tin lấy được từ thiết bị di động, ta có thể tìm được nhiều chứng cứ quan trọng. Vì thế việc sử dụng các công cụ phần mềm giám định theo đúng quy trình khai thác dữ liệu thích hợp để tránh mất mát, thay đổi thông tin trên thiết bị gốc, nhưng thông tin này sẽ phục vụ cho việc phòng chống tội phạm công nghệ cao.

Đề tài luận văn Thạc sĩ của em ‘Điều tra số trên thiết bị di động’ sẽ phần nào đưa ra được định hướng sử dụng công cụ phần mềm để giải quyết vấn đề khai thác thông tin trên thiết bị di động.

# Chương I. Tổng quan

## Điều tra số

### Khái niệm

Digital Forensics (điều tra số) là một nhánh của ngành khoa học điều tra đề cập đến việc sử dụng các phương pháp, công cụ kỹ thuật khoa học đã được chứng minh để thu thập, bảo quản, phân tích, lập báo cáo và trình bày lại những thông tin thực tế từ các nguồn dữ liệu số với mục đích tạo điều kiện hoặc thúc đẩy việc tái hiện lại các sự kiện nhằm tìm ra hành vi phạm tội hay hỗ trợ cho việc dự đoán các hoạt động trái phép như cố ý xâm nhập, tấn công hoặc gây gián đoạn quá trình làm việc của hệ thống.

### 2. Mục đích và ứng dụng

#### 2.1 Mục đích

Mục đích quan trọng nhất của điều tra số là thu thập, phân tích và tìm ra chứng cứ thuyết phục về một vấn đề cần sáng tỏ. Điều tra số có những ứng dụng quan trọng trong khoa học điều tra cụ thể:

* Về mặt kỹ thuật thì điều tra số giúp xác định những gì đang xảy ra làm ảnh hưởng tới hệ thống đồng thời qua đó phát hiện các nguyên nhân hệ thống bị xâm nhập, các hành vi, nguồn gốc của các vi phạm xảy ra đối với hệ thống.
* Về mặt pháp lý thì điều tra số giúp cho cơ quan điều tra khi tố giác tội phạm công nghệ cao có được những chứng cứ số thuyết phục để áp dụng các chế tài xử phạt với các hành vi phạm pháp.

#### 2.2 Khi nào thì thực sự cần thiết thực hiện một cuộc điều tra số?

- Khi hệ thống bị tấn công mà chưa xác định được nguyên nhân.

- Khi cần thiết khôi phục dữ liệu trên thiết bị, hệ thống đã bị xóa đi

- Hiểu rõ cách làm việc của hệ thống

- Khi thực hiện điều tra tội phạm có liên quan đến công nghệ cao

- Điều tra sự gian lận trong tổ chức

- Điều tra các hoạt động gián điệp công nghiệp

- Điều tra số trên thiết bị di động là khoa học về phục hồi bằng chứng kỹ thuật số từ một thiết bị di động theo

## II. Bằng chứng số

### Khái niệm

Digital Evidence (bằng chứng số), hay còn gọi là bằng chứng điện tử (Electronic Evidence), là mọi thông tin có giá trị pháp lý được lưu trữ, được truyền dẫn trong dạng thức số và có giá trị pháp lý trước tòa. Trước khi chấp nhận bằng chứng số, quan tòa phải xác định được là nó có liên quan đến vụ án đang xem xét, cho dù tính xác thực của nó đã được kiểm chứng.

Có thể hiểu về bằng chứng số một cách ngắn gọn như sau: Bằng chứng số là các bằng chứng ở dạng thức số, nó được khôi phục, hay được tìm thấy, trong các thiết bị số – thường là các thiết bị liên quan với máy tính.

Dữ liệu nhận được từ các ổ đĩa trên máy tính hoặc từ các thiết bị lưu trữ khác chưa thể là bằng chứng (số). Để có được bằng chứng, điều tra viên phải thực hiện quá trình khảo sát và phân tích dữ liệu ban đầu. Nếu tìm được dữ liệu họ phải “ráp” chúng lại với nhau để đưa ra được bằng chứng.

### Đặc tính của bằng chứng số

Admissible (thừa nhận): Phải được quan tòa thừa nhận. Tức là, bằng chứng có thể được sử dụng trước tòa và những nơi khác

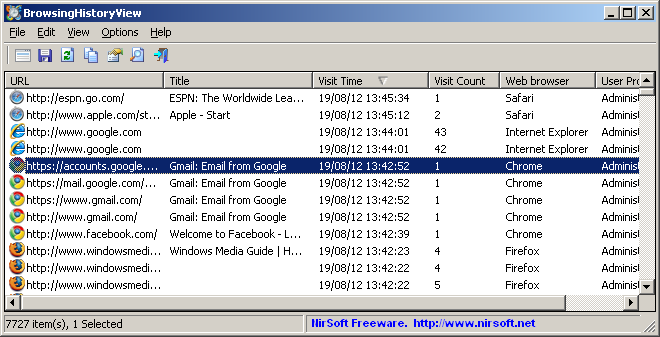
Authentic (xác thực): Phải đảm bảo tính xác thực. Tức là, bằng chứng được đưa ra có quan hệ với các tình huống có liên quan.

Reliable (tin cậy): Làm cho quan tòa hoàn toàn tin cậy vào tính xác thực và tính chính xác của bằng chứng.

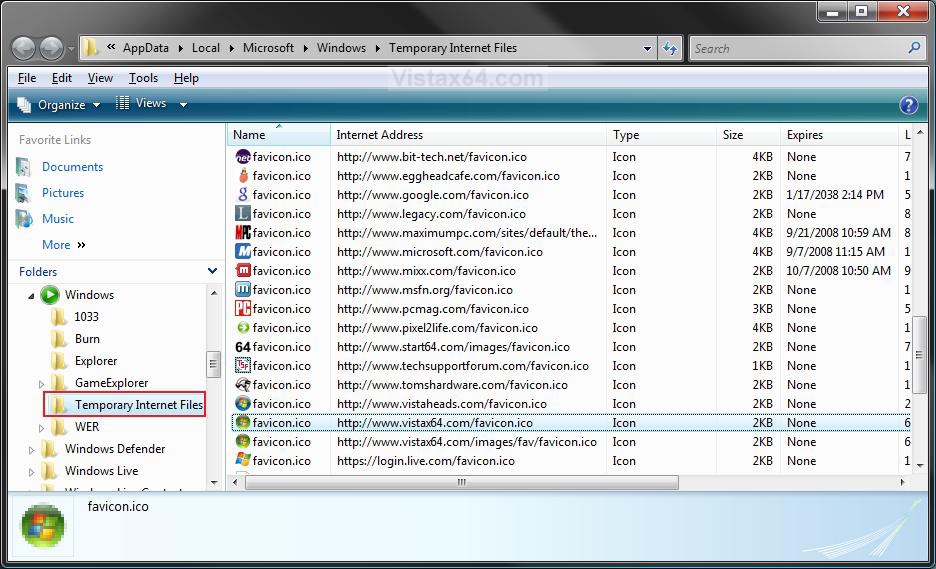
Believable (đáng tin): Bằng chứng phải rõ ràng, dễ hiểu và đáng tin với quan tòa.

### Vị trí có thể tìm thấy bằng chứng số

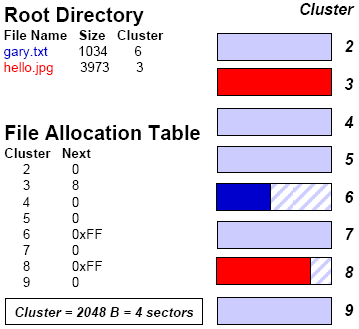
Internet History Files (trong các tập tin lịch sử truy cập internet)



Temporary Internet Files (trong các tập tin tạm sinh ra từ truy cập internet)



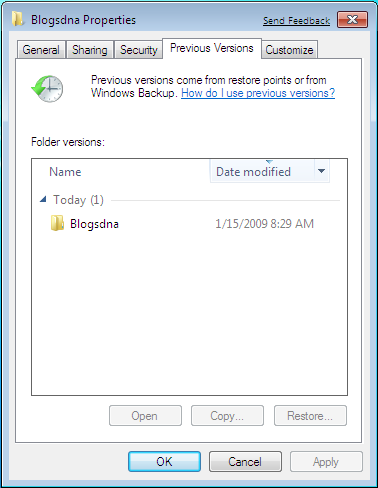
Slack/Unallocated Space (tại không gian (đĩa) chưa cấp phát/thuộc slack của tập tin)



File Settings, folder structure, file names (nơi lưu trữ các thiết lập tập tin, cấu trúc thư mục, tên tập tin)



File Storage Dates (nơi lưu trữ ngày lưu trữ tập tin)



Software/Hardware added (ẩn/nhúng trong phần mềm/phần cứng bổ sung)



Sharing Files (trong các tập tin chia sẻ)



E-mails (ẩn trong các e-mail)



## Phân loại các loại hình điều tra số

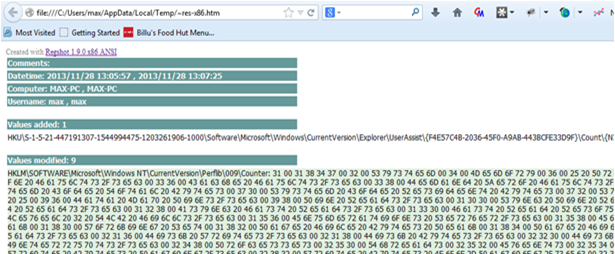
Với nhiều loại hình điều tra số như: điều tra Internet, điều tra điện tử, điều tra mạng, điều tra ứng dụng... có các cách phân chia khác nhau, nhưng về cơ bản điều tra số được chia thành 3 loại hình chính là điều tra máy tính, điều tra mạng và điều tra thiết bị di động.

Điều tra máy tính (Computer Forensics) là một nhánh của khoa học điều tra số liên quan đến việc phân tích các bằng chứng pháp lý được tìm thấy trong máy tính và các phương tiện lưu trữ kỹ thuật số như:

### Điều tra bản ghi (Registry Forensics)

Đây là loại hình điều tra liên quan đến việc trích xuất thông tin và ngữ cảnh từ một nguồn dữ liệu chưa được khai thác qua đó biết được những thay đổi (chỉnh sửa, thêm bớt…) dữ liệu trong Register.

Công cụ thường dùng: MuiCache View, Process Monitor, Regshot, USBDeview

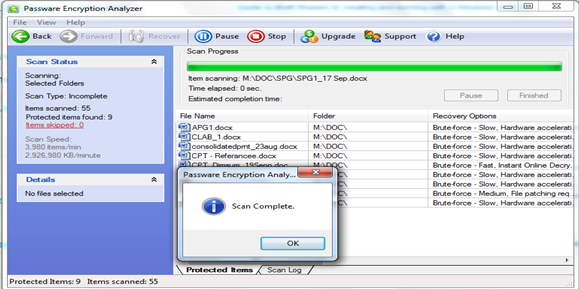


Sử dụng Regsshot quan sát sự thay đổi trong Registry

### Điều tra ổ đĩa (Disk Forensics)

Là việc thu thập, phân tích dữ liệu được lưu trữ trên phương tiện lưu trữ vật lý, nhằm trích xuất dữ liệu ẩn, khôi phục các tập tin bị xóa, qua đó xác định người đã tạo ra những thay đổi dữ liệu trên thiết bị được phân tích.

Công cụ thường dùng: ADS Locator, Disk Investigator, Passware Encryption Analyzer, Disk Detector, Sleuth Kit, FTK

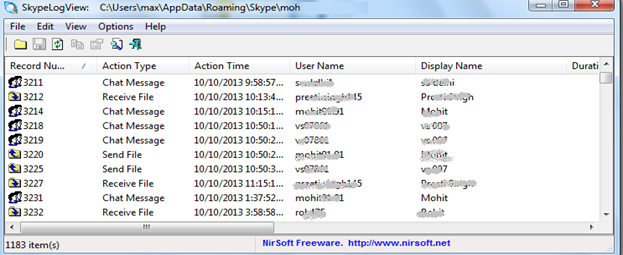


Passware Encryption Analyzer xác định những file được bảo vệ bởi mật khẩu

### Điều tra ứng dụng (Application Forensics)

Là loại hình điều tra phân tích các ứng dụng chạy trên hệ thống như Email, dữ liệu trình duyệt, skype, yahoo… Qua đó trích xuất các bản ghi được lưu trữ trên các ứng dụng phục vụ cho việc điều tra tìm kiếm chứng cứ.

Công cụ thường dùng: ChromeCacheView, MozillaCookiesView, MyLastSearch, PasswordFox, SkypeLogView

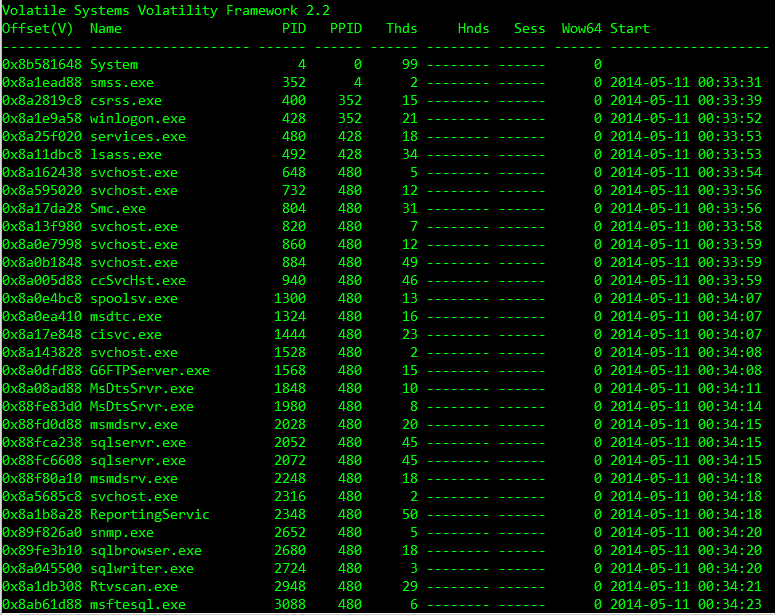


Sử dụng skypelogview xem dữ liệu được trao đổi qua đường truyền

### Điều tra bộ nhớ (Memory Forensics)

Là phương thức điều tra máy tính bằng việc ghi lại bộ nhớ khả biến (bộ nhớ RAM) của hệ thống sau đó tiến hành phân tích làm rõ các hành vi đã xảy ra trên hệ thống. Cụ thể hơn, đó là cố gắng sử dụng kiến trúc quản lý bộ nhớ trong máy tính để ánh xạ, trích xuất các tập tin đang thực thi và cư trú trong bộ nhớ. Những tập tin thực thi có thể được sử dụng để chứng minh rằng hành vi của tội phạm đã xảy ra hoặc để theo dõi nó đã diễn ra như thế nào

Công cụ sử dụng: Dumpit, Strings, The Sleuthkit, Win32dd, Foremost, Volatility, Mandiant Redline, DFF.

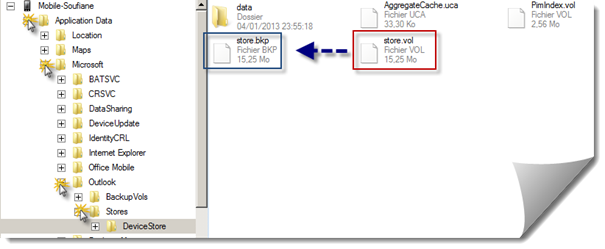


Sử dụng Volatility liệt kê các tiến trình đang chạy trên hệ thống

### Điều tra số trên thiết bị di động (Mobile forensics)

Là loại hình điều tra được thực hiện trên các thiết bị di động, thiết bị PDA, GPS, máy tính bảng, nhằm thu thập dữ liệu, các chứng cứ kỹ thuật số.

Công cụ thường dùng: WPDeviceManager, PwnageTool,OXYGEN, Apktool, IPhone Analyzer, wireshark



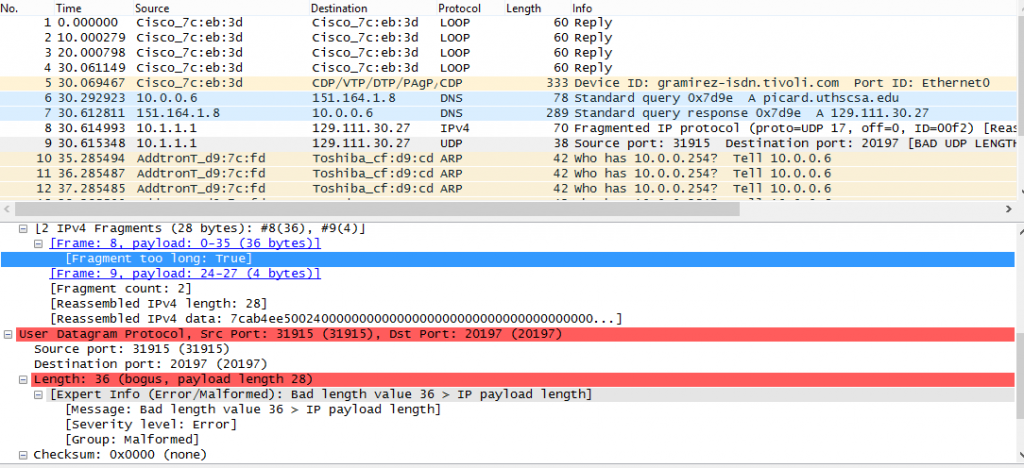
Sử dụng WPDeviceManager để trích xuất SMS

### Điều tra mạng (Network Forensics)

Liên quan đến việc theo dõi, giám sát, phân tích lưu lượng mạng máy tính nhằm phục vụ cho việc thu thập thông tin, sự kiện liên quan, tìm kiếm chứng cứ pháp lý, mục đích là phát hiện sự bất thường, các dấu hiệu xâm nhập trên môi trường mạng.

Công cụ sử dụng: Wireshark, Tcpdump, Networkminer, Wildpackets, bro ids, Xplico, Snort

Điều tra mạng bao gồm việc chặn bắt, ghi âm và phân tích các sự kiện mạng để khám phá nguồn gốc của các cuộc tấn công hoặc sự cố của một vấn đề nào đó. Không giống các loại hình điều tra số khác, điều tra mạng xử lý những thông tin dễ thay đổi và biến động. Lưu lượng mạng được truyền đi và không được lưu lại, do đó việc điều tra mạng thường phải rất linh hoạt, chủ động.



Sử dụng Wireshark phân tích tấn công Teadrop

## Quy trình điều tra số

Một cuộc điều tra số thường bao gồm 4 gian đoạn: Chuẩn bị (Preparation), tiếp nhận dữ liệu hay còn gọi là ảnh hóa tang vật (Acquisition), phân tích (analysis) và lập báo cáo (Reporting)



Preparation: Bước này thực hiện việc mô tả lại thông tin hệ thống, những gì đã xảy ra, các dấu hiệu, để xác định phạm vi điều tra, mục đích cũng như các tài nguyên cần thiết sẽ sử dụng trong suốt quá trình điều tra.

Acquisition: Đây là bước tạo ra một bản sao chính xác các sector hay còn gọi là nhân bản điều tra các phương tiện truyền thông, xác định rõ các nguồn chứng cứ sau đó thu thập và bảo vệ tính toàn vẹn của chứng cứ bằng việc sử dụng hàm băm mật mã.

Analysis: Đây là giai đoạn các chuyên gia sử dụng các phương pháp nghiệp vụ, các kỹ thuật cũng như công cụ khác nhau để trích xuất, thu thập và phân tích các bằng chứng thu được.

Reporting: Sau khi thu thập được những chứng cứ có giá trị và có tính thuyết phục thì tất cả phải được tài liệu hóa lại rõ ràng, chi tiết và báo cáo lại cho bộ phận có trách nhiệm xử lý chứng cứ thu được.

## Điều tra viên

### Khái niệm

Những người làm công việc Forensics thường phải có kinh nghiệm và kiến thức khá rộng về khoa học máy tính, mạng, bảo mật. Trong những trường hợp cần kiến thức chuyên sâu, sẽ có nhiều người cùng tham gia để giải quyết. Ở các doanh nghiệp lớn, những người làm An toàn vận hành(Security Operator) sẽ đảm nhận công việc này.

### Bốn quy tắc đạo đức của điều tra viên (ĐTV)

#### 2.1 Tránh những điều có hại

Trong công việc của mình, người ĐTV cần phải tránh việc gây hại cho đối tượng được bảo vệ, trừ trường hợp việc gây hại là cần thiết để ngăn chặn một thiệt hại lớn hơn. Cần tránh gây hại cho những bên không liên quan, cho dù việc gây hại đó giúp tránh được thiệt hại cho đối tượng được bảo vệ.

#### 2.2 Không phát tán những thông tin nguy hiểm

Người làm ĐTV không được cung cấp cho bất kỳ ai thông tin về các điểm yếu mà có thể bị khai thác (ngoại trừ việc cung cấp thông tin cho chủ sở hữu hoặc nhà phát triển hệ thống chứa điểm yếu nhằm mục đích loại trừ điểm yếu đó). Không được cung cấp cho bất kỳ ai những chương trình độc hại hoặc chương trình đa mục đích, nếu như có căn cứ để cho rằng người được cung cấp sẽ sử dụng chương trình một cách ác ý.

#### 2.3 Sử dụng có chừng mực

Khi có được quyền truy cập tới hệ thống hoặc thông tin về hệ thống, người làm ĐTV chỉ được sử dụng quyền truy cập/thông tin đó để thực hiện việc tìm bằng chứng số, bảo vệ, ngăn chặn các mối nguy hại và tăng cường mức an toàn, mà không được sử dụng quyền truy cập/thông tin đó cho bất kỳ mục đích nào khác, kể cả mục đích vô hại. Khi thực hiện xong nhiệm vụ, quyền truy cập cần được đóng lại, còn thông tin thì cần phải được xóa bỏ.

#### 2.4 Luôn giữ bí mật

Người làm ĐTV cần phải giữ bí mật mọi thông tin được tiếp cận trong quá trình cung cấp dịch vụ bảo vệ, nếu thông tin đó là bí mật thương mại, bí mật đời tư, bí mật nghề nghiệp hay bất kỳ dạng thông tin mật

# Chương 2. Điều tra số trên thiết bị di động (Mobile device Forensics)

## Giới thiệu

Điều tra thiết bị di động là một nhánh của khoa học điều tra số liên quan đến việc thu hồi bằng chứng kỹ thuật số hoặc dữ liệu từ các thiết bị di động. Thiết bị di động ở đây không chỉ đề cập đến điện thoại di động mà còn là bất kỳ thiết bị kỹ thuật số nào có bộ nhớ trong và khả năng giao tiếp, bao gồm các thiết bị PDA, GPS và máy tính bảng.

Việc sử dụng điện thoại với mục đích phạm tội đã phát triển mạnh trong những năm gần đây, nhưng các nghiên cứu điều tra về thiết bị di động là một lĩnh vực tương đối mới. Sự gia tăng các loại hình điện thoại di động trên thị trường (đặc biệt là điện thoại thông minh) đòi hỏi nhu cầu giám định về tính an toàn của các thiết bị này mà không thể đáp ứng bằng các kỹ thuật điều tra máy tính hiện tại.

## 2. Các phương pháp kỹ thuật khai thác thông tin dữ liệu trên smartphone

### 2.1. Các thông tin lưu trữ trên điện thoại di động

Điện thoại di động có thể lưu trữ các thông tin ở nhiều nơi khác nhau: Thẻ SIM, bộ nhớ trong, thẻ nhớ ngoài (đối với những loại máy có khe cắm thẻ nhớ)

#### 2.1.1. Thông tin lưu trữ trên SIM:

Thẻ SIM là một loại thẻ thông minh được dùng trong các loại máy sử dụng mạng GSM, nó cho phép người sử dụng kết nối tới mạng và xác định tính duy nhất của thuê bao trong mạng. Thẻ SIM chứa các thông tin bao gồm thông tin về thuê bao di đông, và một số thông tin cá nhân khác, như: Các tin nhắn SMS đã nhận và đã gửi, nhật ký điện thoại, danh bạ điện thoại, số Se-ri, thông tin về trạng thái của SIM, số nhận dạng thuê bao di động quốc tế IMSI, mã dịch vụ (cho mạng GSM), các thuật toán nhận thực và bảo mật A3, A8, A5, khoá nhận thực thuê bao riêng Ki, Số điện thoại di động quốc tế MSISDN, các khoá cho quá trình cá nhân hoá SIM, thông tin về vị trí hiện tại, mã số nhận dạng cá nhân PIN, mã số mở khóa cá nhân PUK

#### 2.1.2. Thông tin lưu trữ trên Phone Memory

Từ cuối những năm 1990, các nhà sản xuất đã tích hợp thêm bộ nhớ vào trong các điện thoại di động để chúng có thể lưu trữ được nhiều thông tin hơn. Ngoài việc lưu trữ trên SIM, dữ liệu còn được lưu trữ trên bộ nhớ trong của điện thoại di động.

#### 2.1.3. Các thông tin lưu trữ trên thẻ nhớ ngoài

Do nhu cầu của người sử dụng điện thoại đòi hỏi chiếc điện thoại phải làm được chức năng như một chiếc máy tính nên khả năng lưu trữ dữ liệu của điện thoại cũng được mở rộng.

Nhiều loại điện thoại cho phép hỗ trợ thẻ nhớ ngoài, thẻ nhớ ngoài giúp mở rộng khả năng lưu trữ trên điện thoại, nó cho phép người sử dụng có thể lưu trư được nhiều thông tin hơn so với khả năng của bộ nhớ được tích hợp trong điện thoại. Thẻ nhớ là một thiết bị lưu trữ bất biến, khi tháo thẻ nhớ ra khỏi thiết bị thì dữ liệu cũng không bị mất đi.

### 2.2. Tổng quan về kỹ thuật khai thác dữ liệu trên điện thoại di động

Khai thác dữ liệu trên điện thoại di động hiện nay là một vấn đề khá mới mẻ trong lĩnh vực điều tra tội phạm, nhưng nó đang dần dần chứng tỏ vai trò của mình trong việc giải quyết các vụ án. Khai thác dữ liệu từ điện thoại di động giúp cho các nhà điều tra có thể tìm được nhiều chứng cứ mà các cách điều tra thông thường không thể có được. Khai thác dữ liệu trên điện thoại di động nhằm mục đích:

− Trích xuất toàn bộ và không làm thay đổi các thông tin trên điện thoại di động

− Phân tích các thông tin đã trích xuất và tìm ra các chứng cứ liên quan tới vụ án.

− Cung cấp cho điều tra viên những thông tin có độ tin cậy cao có thể được sử dụng để làm bằng chứng tại tòa án.

Khai thác dữ liệu trên điện thoại di động là một bài toán khó và khá mới mẻ. Để giải quyết được bài toán này đòi hỏi cán bộ điều tra phải có kiến thức nhất định về thiết bị cần khai thác và các công cụ khai thác, đối với mỗi loại thiết bị phải tìm được phương pháp khai thác có hiệu quả nhất. Việc khai thác cũng phải được thực hiện theo đúng quy trình tránh làm mất dữ liệu và đảm bảo giá trị pháp lý của các dữ liệu khai thác được.

### 2.3. Kỹ thuật khai thác dữ liệu trên bộ nhớ trong của smartphone

#### 2.3.1 Kỹ thuật khai thác vật lý

Kỹ thuật khai thác vật lý là kỹ thuật dữ liệu được khai thác bằng phương pháp đọc trực tiếp bộ nhớ

Ưu điểm:

Toàn bộ dữ liệu được khai thác.

Áp dụng phương pháp này cho trường hợp điện thoại bị hỏng hoặc thiết bị không có giao diện.

Nhược điểm:

- Khó thực hiện, rất khó để phân tích dữ liệu,

- Phần mềm khai thác dữ liệu đắt, cần thiết bị phần cứng riêng biệt để khai thác dữ liệu.

- Không an toàn cho dữ liệu đang hoạt động. Thành công của phương pháp này phụ thuộc vào kinh nghiệm điều tra của kỹ thuật viên, một thao tác không chính xác trong kỹ thuật điều tra có thể phá hủy toàn bộ thiết bị và dữ liệu trong thiết bị điện thoại di động.

#### 2.3.2 Kỹ thuật khai thác logic

Phương pháp logic là các a bit-by-bit copy trên các đối tương lưu trữ logic như là: thư mục, file, mà nằm trong bộ nhớ logic ( ví dụ đó là một phân vùng hệ thống file)

Ưu điểm:

Dễ dàng thực hiện, dễ phân tích, an toàn với dữ liệu đang hoạt động.

Phần mềm sử dụng khai thác dữ liệu giá cả phải chăng, không cần đến thiết bị phần cứng chuyên dụng.

Nhược điểm:

Việc thiết lập kết nối dữ liệu có thể làm thay đổi dữ liệu.

Một số dữ liệu được khai thác, những dữ liệu đã bị xóa vẫn còn trong hệ thống, có thể bị xóa không thể khôi phục được.

Một số trường hợp không thể áp dụng phương pháp này đó là: Khi điện thoại hỏng

không thể sửa chữa, hoặc khi các thiết bị không có giao diện.

Thông qua các thiết bị như: cổng hồng ngoại, Bluetooth, cáp kết nối giúp chúng ta kết nối điện thoại di động với máy tính. Từ đó, chúng ta có thể khai thác được các thông tin lưu trong điện thoại di động. Kết hợp sử dụng các phần mềm hỗ trợ khai thác thông tin trên điện thoại di động, chúng ta có thể thu thập được thông tin cần thiết cho quá trình điều tra, phục vụ công tác điều tra tội phạm công nghệ cao.

### 2.4 Kỹ thuật khai thác dữ liệu trên SIM

#### 2.4.1 Kết nối SIM với máy tính thông qua đầu đọc SIM

Như chúng ta đã biết, SIM điện thoại thường chứa nhiều thông tin quan trọng như các tin nhắn SMS, danh bạ…Việc khai thác những thông tin này có thể được tiến hành ngay trên điện thoại tuy nhiên cách này không hiệu quả và không phục hồi lại được những thông tin đã bị xóa. Để khai thác được toàn bộ các thông tin trên SIM, ta kết nối SIM trực tiếp với máy tính qua một đầu đọc thẻ SIM.

Các bước kết nối:

− Lắp SIM vào khe cắm SIM trên thiết bị

− Gắn thiết bị vào máy tính qua cổng USB

− Chạy phần mềm nhận dạng thiết bị đã cài đặt trên máy tính để kiểm tra kết nối.

− Nhập mã PIN (nếu SIM được bảo vệ bằng mã PIN)

− Nhấn Connect để kết nối SIM với máy tính

# Chương 3. Tính năng kỹ thuật, hình thức tổ chức và các chức năng của hệ điều hành Android và SIM

## Hệ điều hành Android

### Tổng quan

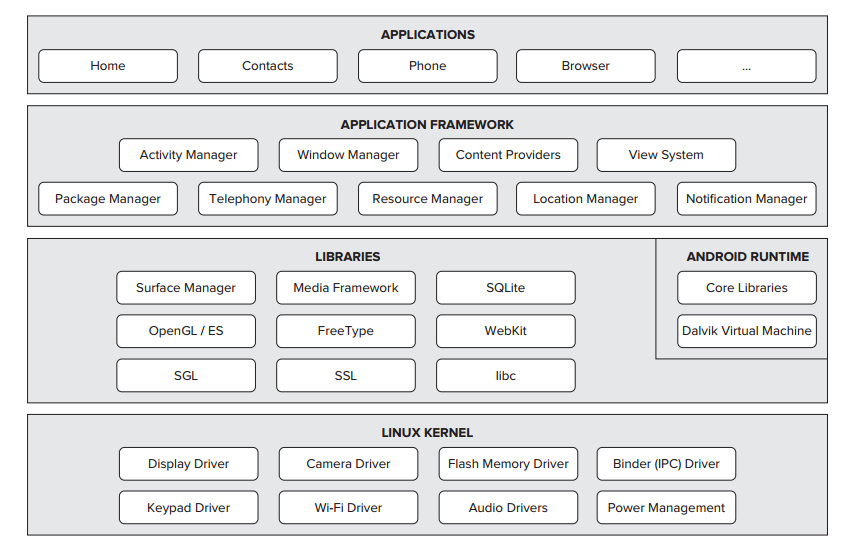
Android là một hệ điều hành dựa trên nền tảng Linux được thiết kế dành cho các thiết bị di động có màn hình cảm ứng như điện thoại thông minh và máy tính bảng. Ban đầu, Android được phát triển bởi Tổng công ty Android, với sự hỗ trợ tài chính từ Google và sau này được chính Google mua lại vào năm 2005. Android ra mắt vào năm 2007 cùng với tuyên bố thành lập Liên minh thiết bị cầm tay mở: một hiệp hội gồm các công ty phần cứng, phần mềm, và viễn thông với mục tiêu đẩy mạnh các tiêu chuẩn mở cho các thiết bị di động.

Android có mã nguồn mở và Google phát hành mã nguồn theo Giấy phép Apache. Chính mã nguồn mở cùng với một giấy phép không có nhiều ràng buộc đã cho phép các nhà phát triển thiết bị, mạng di động và các lập trình viên nhiệt huyết được điều chỉnh và phân phối Android một cách tự do. Ngoài ra, Android còn có một cộng đồng lập trình viên đông đảo chuyên viết các ứng dụng để mở rộng chức năng của thiết bị, bằng một loại ngôn ngữ lập trình Java có sửa đổi.

### Kiến trúc cơ bản của hệ điều hành Android

Android gồm 5 phần chính sau được chứa trong 4 lớp:

* + Nhân Linux: Đây là nhân nền tảng mà hệ điều hành Android dựa vào nó để phát triển. Đâu là lớp chứa tất cả các thiết bị giao tiếp ở mức thấp dùng để điều khiển các phần cứng khác trên thiết bị Android.
  + Thư viện: Chứa tất cả các mã cái mà cung cấp cấp những tính năng chính của hệ điều hành Android, đôi với ví dụ này thì SQLite là thư viện cung cấp việc hộ trợ làm việc với database dùng để chứa dữ liệu. Hoặc Webkit là thư viện cung cấp những tính năng cho trình duyệt Web.
  + Android runtime: Là tầng cùng với lớp thư viện Android runtime cung cấp một tập các thư viện cốt lỗi để cho phép các lập trình viên phát triển viết ứng dụng bằng việc sử dụng ngôn ngữ lập trình Java. Android Runtime bao gốm máy ảo Dalvik(ở các version < 4.4, hiện tài là phiên bản máy ảo ART được cho là mạnh mẽ hơn trong việc xử lý biên dịch). Là cái để điều khiển mọi hoạt động của ứng dụng Android chạy trên nó(máy ảo Dalvik sẽ biên dịch ứng dụng để nó có thể chạy(thực thi) được , tương tự như các ứng dụng được biên dịch trên máy ảo Java vậy). Ngoài ra máy ảo còn giúp tối ưu năng lượng pin cũng như CPU của thiết bị Android
  + Android framework: Là phần thể hiện các khả năng khác nhau của Android(kết nối, thông báo, truy xuất dữ liệu) cho nhà phát triển ứng dụng, chúng có thể được tạo ra để sử dụng trong các ứng dụng của họ.
  + Application: Tầng ứng dụng là tầng bạn có thể tìm thấy chuyển các thiết bị Android như Contact, trình duyệt…Và mọi ứng dụng bạn viết đều nằm trên tầng này.



### Các phiên bản của hệ điều hành Android

Từ lúc ra đời, hệ điều hành Android đã trải qua nhiều phiên bản với nhiều sự cải tiến rõ rệt từ các phiên bản của Android. Hiện tại Android mới nhất phiên bản 6.0 Marshmallow

## SIM

### Cấu trúc SIM

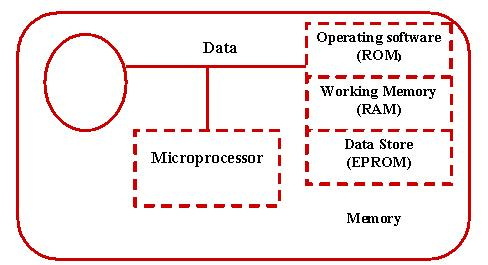
Thẻ SIM (hay còn gọi là Module nhận dạng thuê bao) là một loại thẻ thông minh được dùng trong các điện thoại di động sử dụng mạng GSM (Global System for Mobile communication – Hệ thống thông tin di động toàn cầu) Các chức năng chính của thẻ SIM bao gồm:

+ Cung cấp chức năng xác thực thuê bao cho phép người sử dụng truy cập vào các dịch vụ đã đăng ký, bảo mật cho các thuê bao trong mạng.

+ Lưu trữ các thông tin cá nhân.

+ Cung cấp các dịch vụ phi thoại khác…

1. Cấu tạo thẻ SIM: Cấu tạo tổng quát của thẻ SIM được mô tả trong hình vẽ sau:

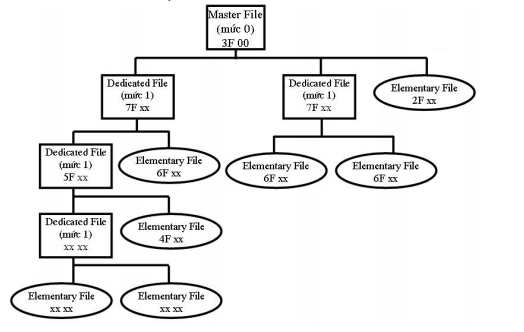


Cấu tạo thẻ SIM

SIM có kích thước nhỏ tương đương một con tem bưu chính (chiều dài là 25 mm, chiều rộng là 15 mm, và độ dày là 0,76 mm). Bộ nhớ của SIM có dung lượng từ 16 KB đến 128 KB. Tại lõi của nó chứa một bộ vi xử lý, bộ nhớ chỉ đọc (EPROM) có khả năng lập trình và xóa bằng tín hiệu điện, nó cũng bao gồm bộ nhớ truy cập ngẫu nhiên (RAM) cho việc thực hiện các chương trình và bộ nhớ chỉ đọc (ROM) cho hệ điều hành, xác thực người sử dụng, các thuật toán mã hóa dữ liệu và các ứng dụng khác.

### Sơ đồ cấu trúc Data trong SIM

Sơ đồ cấu trúc dữ liệu:



Sơ đồ cấu trúc file trên thẻ SIM

Kiểu File: Có 3 kiểu file sau:

+ MF: Master File file chủ.

+ DF: Dedicated File file dành riêng.

+ EF: Elementary File file thành phần.

Theo như hình vẽ trên MF là các file DF uỷ nhiệm được phân bố tại phần đầu của tổ chức logic bộ nhớ và được phân ở mức 0. Các DF khác tương ứng được phân chia ở mức 1,2,3. Cấu trúc phân cấp logic này được dành riêng cho môi trường đa ứng dụng và cho mục đích quản trị.

### Cấu trúc các File

Mỗi file được gán một mã nhận dạng duy nhất 2 byte mà được sử dụng bởi hệ điều hành lựa chọn file:

+ Byte thứ nhất của file nhận dạng được gọi là nhận dạng hệ thống.

+ Byte thứ hai nhận dạng file nguồn của nó.

# Chương 4: Xây dựng kịch bản thực tế

## Kịch bản thực tế

Đối tượng bị tình nghi có mục đích gây rối, đánh bom HVKTQS, đối tượng sử dụng điện thoại Android để liên lạc với đồng bọn. Đối tượng tình nghi bị bắt và thu giữ điện thoại của đối tượng.

## Hướng giải quyết

Đối với mỗi loại điện thoại sẽ có những phương pháp khai thác khác, thu thập dữ liệu khác nhau. Tuy nhiên, để đảm bảo giá trị pháp lý của những thông tin thu được và không bị mất mát thông tin thì bất kỳ quá trình khai thác nào cũng phải trải qua 4 giai đoạn sau:

### 2.1 Thu giữ và bảo quản thiết bị

Trên điện thoại di động có những thông tin bất biến nhưng cũng có những thông tin dễ bị thay đổi hoặc biến mất. Quá trình này bao gồm các công việc: thu giữ, đóng gói, vận chuyển và lưu trữ. Việc thu giữ và bảo quản đúng quy trình sẽ đảm bảo cho quá trình khai thác dữ liệu tiến hành thuận lợi và đạt hiệu quả cao.

### 2.2 Thu thập dữ liệu trên điện thoại

Thu thập dữ liệu là việc khai thác tất cả những thông tin có trên điện thoại, bao gồm cả những thông tin đang lưu trên máy và những thông tin đã xóa nhằm tạo điều kiện cho quá trình khai thác thông tin. SIM điện thoại cũng là một thiết bị lưu trữ nhiều thông tin. Trên SIM thường lưu những tin nhắn SMS, danh bạ… Vì vậy, trong quá trình khai thác dữ liệu, khai thác SIM cũng là một khâu quan trọng. Việc khai thác dữ liệu trên SIM có thể được tiến hành trực tiếp thông qua điện thoại hoặc kết nối với máy tính bằng một đầu đọc thẻ SIM Đối với mỗi loại điện thoại sẽ có một phương pháp khai thác dữ liệu khác nhau, tùy thuộc vào từng loại điện thoại thu được mà cán bộ kỹ thuật sẽ quyết định nên khai thác theo phương pháp nào. Tuy nhiên để khai thác một cách có hiệu quả thì các phương pháp đều phải tuân theo trình tự sau:

Bước1: Tiến hành thu giữ điện thoại theo đúng quy trình để tránh làm mất thông tin trên điện thoại và đảm bảo đúng thủ tục pháp lý.

Bước 2: Khi ở trạng thái tiết kiệm năng lượng điện thoại giống như đang tắt, nhưng trên thực tế điện thoại đang bật. Để kiểm tra trạng thái của điện thoại có thể ấn một nút bất kỳ trên điện thoại

Bước 3: Kiểm tra xem điện thoại có dùng SIM không. Nếu điện thoại dùng SIM thì chuyển sang quy trình khai thác SIM. Nếu điện thoại sử dụng công nghệ CDMA thì việc khai thác dữ liệu chỉ tiến hành trên máy điện thoại.

Bước 4: Bật nguồn lên và tiến hành các bước tiếp theo để khai thác thông tin trên điện thoại

Bước 5: Kiểm tra các đặc điểm của điện thoại, nắm rõ các đặc điểm kỹ thuật để có thể đưa ra phương pháp thu thập dữ liệu hợp lý. Bước này đòi hỏi cán bộ kỹ thuật phải có kiến thức, am hiểu về các loại điện thoại và đặc điểm của chúng.

Bước 6: Lập kế hoạch khai thác

Bước 7: Kiểm tra xem loại điện thoại đó có hỗ trợ kết nối với máy tính không? Có thể sử dụng công cụ khai thác dữ liệu nào?

Bước 8: Sử dụng các công cụ để thu thập, khai thác và phục hồi dữ liệu trên điện thoại. Tùy thuộc vào dữ liệu cần khai thác mà chọn công cụ khai thác hợp lý để đạt được hiệu quả cao nhất

Bước 9: Sử dụng các phương pháp khai thác dữ liệu thực hiện quá trình khai thác dữ liệu trên điện thoại di động.

Bước 10: Sau khi khai thác hết các thông tin trên máy thì tắt nguồn và tháo SIM ra khỏi máy để chuyển sang qui trình khai thác SIM Khai thác SIM: SIM điện thoại cũng là một thiết bị lưu trữ nhiều thông tin. Trên SIM thường lưu những tin nhắn, danh bạ điện thoại. Vì vậy, trong quá trình khai thác dữ liệu, khai thác SIM cũng là một khâu quan trọng. Để khai thác triệt để các thông tin trên SIM (kể cả những thông tin đã bị xóa), kết nối SIM với máy tính thông qua một đầu đọc SIM và sử dụng các phần mềm được cài trên máy tính.

Quá trình khai thác SIM có thể được khái quát bằng sơ đồ sau:

Kiểm tra và phân tích dữ liệu Quá trình khai thác dữ liệu trên điện thoại sẽ đưa ra tất cả những thông tin lưu trên điện thoại, trong đó có những thông tin có liên quan và không liên quan đến vụ án. Giai đoạn kiểm tra và phân tích chứng cứ sẽ sàng lọc tìm ra những thông tin có liên quan đến vụ án.

1.3 Báo cáo

Sau khi kiểm tra và phân tích các chứng cứ đã thu thập được, kết quả được tổng hợp lại dùng làm căn cứ để phục vụ cho quá trình điều tra vụ án hoặc được dùng làm bằng chứng tại tòa án.

## Xây dựng, phát triển phần mềm thu thập, khai thác dữ liệu từ SIM và bộ nhớ trong của smartphone trên các hệ điều hành Android