BAN CƠ YẾU CHÍNH PHỦ

HỌC VIỆN KỸ THUẬT MẬT MÃ

PHÒNG CHỐNG VÀ ĐIỀU TRA TỘI PHẠM

HƯỚNG DẪN CHO NGƯỜI ĐIỀU TRA KỸ THUẬT SỐ

QUẢN LÝ VỤ ÁN KỸ THUẬT SỐ & THỦ TỤC PHÂN TÍCH PHÒNG GIÁM ĐỊNH

Người hướng dẫn: **GV. Lại Minh Tuấn**

Sinh viên thực hiện:

1. **Lưu Thị Minh Huệ**
2. **Đỗ Thị Lan Anh**
3. **Phạm Thị Bình**

Hà Nội, 2019

MỤC LỤC

DANH MỤC TỪ VIẾT TẮT

Từ viết tắt	Chú giải tiếng Anh	Chú giải tiếng Việt
AFF	Advanced Forensic Format	Định dạng điều tra nâng cao
DF	Digital Forensic	Điều tra kỹ thuật số
DFL	Digital Forensics Laboratory	Phòng điều tra kỹ thuật số
EWF	Expert Witness Format	Định dạng nhân chứng chuyên gia
HPA	Host Protected Area	Khu vực bảo vệ máy chủ
IDEN	Integrated Digital Enhanced Network	Mạng tích hợp kỹ thuật số
IMEI	International Mobile Equipment Identity Number	Số nhận dạng thiết bị di động quốc tế
MEID	Mobile Equipment Identity Number	Số nhận dạng thiết bị di động
PDP	Personal Development Portfolio	Danh mục đầu tư phát triển cá nhân
RAM	Random Access Memory	Bộ nhớ truy cập ngẫu nhiên
SIM	Subscriber Identity Module	Module nhận dạng thuê bao
SWGDE	Scientific Working Group on Electronic evidence	Nhóm công tác khoa học về bằng chứng điện tử

DANH MỤC BẢNG

DANH MỤC HÌNH ẢNH

CHƯƠNG 4. QUẢN LÝ VỤ ÁN KỸ THUẬT SỐ

DFL phải thiết lập một quy trình thủ tục quản lý các vụ án cụ thể trước khi bắt đầu tiếp nhận. Thông thường có bảy bước trong quy trình xử lý một vụ án, được minh họa trong hình dưới đây và giải thích thêm trong các phần tiếp theo. Trước khi tiến hành một vụ án, DFL phải đảm bảo rằng vụ án đang tuân theo và tuân thủ pháp luật liên quan. Người quản lý hoặc người kiểm tra phải đảm bảo quyền hạn hợp pháp để xử lý những bằng chứng tồn tại thông qua các lệnh hoặc văn bản chính thức. Mục đích của việc tiến hành công việc DF là sử dụng bằng chứng để chứng minh hoặc bác bỏ các sự kiện đang tranh chấp, do đó phải thu được bằng chứng điện tử tuân thủ luật pháp. Khi kết thúc công việc DF, phải đảm bảo rằng bằng chứng điện tử được chấp nhận và báo cáo pháp y được chấp nhận tại tòa án.

Hình 4.Thủ tục xử lý trường hợp

4.1 Tiếp nhận yêu cầu

DFL bắt đầu khi nhận được yêu cầu chính thức từ bên yêu cầu. Yêu cầu chính thức này có thể ở dạng thư, e-mail hoặc fax. Thông tin được cung cấp trong yêu cầu chính thức bao gồm mô tả về tội phạm liên quan, hành vi liên quan, chi tiết bằng chứng điện tử, mục tiêu vụ án và có thể là lệnh bắt giữ. Người quản lý phòng thí nghiệm hoặc nhân viên được chỉ định sau đó sẽ xem xét yêu cầu và xác định xem vụ án đó có khả thi hay không, dựa trên các tiêu chí sau:

a. Trường hợp vụ án nằm trong phạm vi của điều tra kỹ thuật số, tức là bằng chứng là điện tử
b. Phương pháp và công cụ có sẵn
c. Nhân viên sẵn sàng để tiến hành vụ án
d. Yêu cầu pháp lý được đáp ứng

Sau đó DFL sẽ chính thức trả lời yêu cầu về việc có thể chấp nhận vụ án đó hay không. Nếu quyết định chấp nhận, DFL sẽ cung cấp ngày gửi bằng chứng điện tử từ bên yêu cầu.

4.2 Đăng ký một vụ án

Khi DFL quyết định rằng vụ án đó là khả thi, Bên yêu cầu sẽ đến DFL với bằng chứng điện tử. DFL tạo một số vụ án đang tiến hành duy nhất cho vụ án đó và điền vào mẫu đăng ký vụ án.

Dựa trên thông tin đó, Người kiểm sát có thể lập kế hoạch cho các phương pháp và công cụ được sử dụng để xử lý bằng chứng.

Cả hai bên, nhân viên Bên yêu cầu và nhân viên DFL đều phải ký vào mẫu đơn. Công việc hiện đã chính thức bắt đầu. DFL sau đó sẽ tạo một thư mục trong phương tiện lưu trữ để lưu trữ tất cả dữ liệu logic liên quan đến vụ án.

4.3 Đăng ký một vật chứng

Khi nhận được bằng chứng điện tử (tang vật), điều quan trọng là tang vật phải được niêm phong trước khi quyền tạm giữ được chuyển sang DFL. Để loại bỏ mọi nghi ngờ hợp lý về tính toàn vẹn của bằng chứng, cả bên yêu cầu và người kiểm tra phải chứng minh rằng không ai khác có được quyền truy cập bằng chứng trong quá trình chuyển từ bên này sang bên kia. Thực thi này là mới mẻ và tốn kém đối với một số cơ quan, tuy nhiên DFL sẽ cung cấp kiến thức một cách liên tục và cung cấp thời gian biểu vững chắc để bắt đầu thực hành quy trình này với các cơ quan. Một mẫu của mẫu đăng ký tang vật có sẵn tại phụ lục D: Mẫu đăng ký tang vật.

Mỗi mảnh bằng chứng điện tử được gửi phải được đăng ký và gán một nhãn tang vật duy nhất được ghi lại với các chi tiết tang vật trong mẫu đăng ký. Việc đăng ký này bao gồm mỗi mục con vật chứng, như thẻ sim và thẻ nhớ. Các nhãn phải có thể theo dõi các mục con đến mục cha.

Ví dụ: nếu điện thoại di động được gắn nhãn là 20190105 (2) -MP01, thì thẻ sim có thể được gắn nhãn là 20190105 (2) -MP01-SIM01. Điều quan trọng cần lưu ý là bất kỳ khiếm khuyết nào trên tang vật phải được ghi lại trong mẫu đăng ký tang vật. Điều này là để bảo vệ DFL khỏi mọi khiếu nại tiêu cực trong tương lai. Bất kỳ hình thức tài liệu bản mềm liên quan đến tang vật phải được tải lên thư mục vụ án.

Bây giờ chuỗi hành trình của các vật chứng đã bắt đầu, và mẫu đăng ký phải được điền bởi các nhân viên tiếp nhận tang vật.

4.4 Chụp ảnh tang vật

Một bức ảnh của tang vật được chụp vì những lý do sau: để ghi lại trạng thái của tang vật và để xác định hiệu quả tang vật trong tương lai. Chụp ảnh tổng quan của tang

vật cũng như góc nhìn cận cảnh. Nếu màn hình đang hoạt động, chụp ảnh màn hình cũng hiển thị. Các hình ảnh sau đó nên được tải lên thư mục vụ án. Nên chụp ảnh tang vật trước khi trả lại cho bên yêu cầu để tham khảo trong tương lai về tình trạng của nó.

4.5 Tiến hành phân tích

Việc phân tích phải được tiến hành theo mô hình phân tích DFL. Trong quá trình, người kiểm tra phải duy trì liên lạc với bên yêu cầu và thông báo bất kỳ sai lệch hoặc giới hạn nào có thể phát sinh trong quá trình kiểm tra. Một số người kiểm tra có nhiều năm kiến thức về điều tra kỹ thuật số và do đó họ có thể phân bổ dữ liệu chính xác khi có thông tin liên lạc hiệu quả giữa người kiểm tra và bên yêu cầu.

4.6 Trả lại tang vật

Sau khi hoàn thành phân tích, DFL liên hệ với bên yêu cầu để lấy bằng chứng. Thực tế hầu hết trong DFL là trả lại tang vật cùng với báo cáo điều tra cho bên yêu cầu để tiết kiệm thời gian đi lại. Trước khi trả lại tang vật, DFL phải niêm phong nó. Con dấu phải có của nhân viên ban đầu, nhãn hiệu tang vật và ngày, thời gian được niêm phong. Một ví dụ về niêm phong tang vật có sẵn tại phụ lục E: Mẫu niêm phong vật chứng

4.7 Kết thúc vụ án

Quá trình sau đó hoàn tất và DFL có thể đóng hồ sơ. Để kết thúc vụ kiện, cả hai bên phải đồng ý rằng công việc đã hoàn thành và báo cáo đã được gửi cho bên yêu cầu. Điều này có thể được thực hiện bằng cách ký vào một mẫu đơn. Một ví dụ có sẵn tại phụ lục D: Mẫu đăng ký tang vật, trong đó bằng cách ký vào phần hoàn trả tang vật, cả hai bên đồng ý rằng công việc hiện đã hoàn tất.

Sau khi hoàn thành vụ án, giai đoạn phía trước liên quan đến người kiểm tra xuất hiện tại tòa án để cung cấp lời khai của chuyên gia về kết quả điều tra của vụ án nếu được yêu cầu. Bên yêu cầu thông báo cho người kiểm tra khi cần đến tòa án.

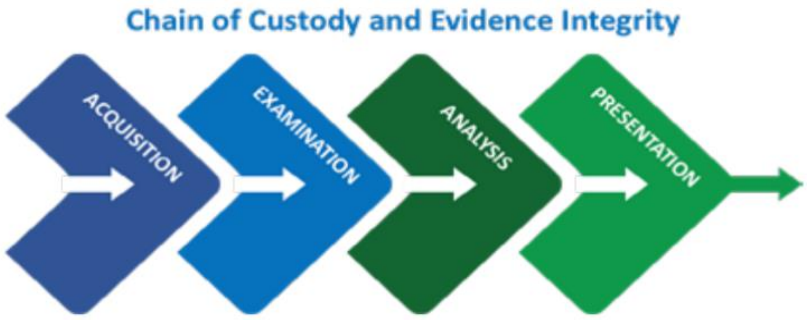
CHƯƠNG 5. THỦ TỤC PHÂN TÍCH PHÒNG GIÁM ĐỊNH

Chương này bao gồm các thủ tục để tiến hành phân tích về bằng chứng điện tử tại DFL. Một mô hình quy trình tổng thể, theo thời gian được trình bày để cung cấp một cái nhìn tổng quan hơn về các quy trình chính.

Thông thường có bốn giai đoạn liên quan đến phân tích bằng chứng điện tử trong DFL: thu nhận, kiểm tra, phân tích và trình bày. Trong suốt quá trình, chuỗi lưu giữ bằng chứng phải luôn được cập nhật bất cứ khi nào nó thay đổi và tính toàn vẹn của nó phải được bảo đảm mọi lúc. Các giai đoạn kiểm tra và phân tích có thể được lặp lại cho đến khi công việc đáp ứng yêu cầu vụ án.

Ta thường hiểu rằng tiến hành công việc DF trong DFL đòi hỏi bốn giai đoạn này, tuy nhiên không phải tất cả các vụ án sẽ yêu cầu tất cả các giai đoạn. Trong một số trường hợp nhất định, giai đoạn thu nhận có thể được bỏ qua để tiến hành xử lý ngay trong giai đoạn kiểm tra. Một ví dụ về trường hợp như vậy là khi có các bộ dữ liệu lớn, trong đó tiến hành thu thập trên mỗi mục bằng chứng có thể không khả thi.

Hình dưới đây cho thấy mô hình phân tích phòng thí nghiệm:



Hình 5. Mô hình phân tích phòng thí nghiệm điều tra kỹ thuật số

5.1 Thu thập

5.1.1 Tổng quan

Thu nhận hay được biết đến nhiều hơn, thu thập dữ liệu, là quá trình tạo ra một bản sao điều tra của bằng chứng điện tử (tang vật) như đĩa cứng, ổ đĩa Thumb hoặc máy chủ ở dạng tệp hình ảnh hoặc tệp. Tệp hình ảnh hoặc tệp sau đó sẽ được sử dụng cho giai đoạn tiếp theo của quá trình phân tích bằng chứng. Việc thu thập được thực hiện để bảo vệ tính toàn vẹn của bằng chứng điện tử. Đó là tạo ra một bản sao dữ liệu giống hệt nhau mà không thay đổi nội dung của bằng chứng điện tử dưới bất kỳ hình thức nào.

Bằng chứng điện tử cần phải được thu thập theo cách thức điều tra. Dữ liệu thường được lấy bằng cách thu thập dữ liệu dễ bay hơi từ máy tính đang chạy trong khi tìm kiếm hoặc bằng cách lấy phương tiện lưu trữ từ máy tính bị tịch thu hoặc ở bất kỳ giai đoạn nào khác trong quá trình điều tra. Bản chất vô hình của dữ liệu và thông tin được lưu trữ ở dạng điện tử giúp dễ dàng thao tác và dễ bị thay đổi hơn so với các dạng bằng chứng truyền thống. Do đó, điều quan trọng là phải có một quy trình thu thập được xác định và thử nghiệm.

Khi một tệp hình ảnh đã được tạo, cả giá trị băm của vật chứng và tệp hình ảnh phải được ghi lại. Hàm băm được sử dụng để chứng minh rằng tệp hình ảnh hoàn toàn giống với nội dung của vật chứng. Có rất nhiều thuật toán băm được sử dụng trong DF, chẳng hạn như Sha-256. Hầu hết các phần mềm và phần cứng điều tra đều cung cấp tính năng tạo hàm băm.

Kiểm tra và phân tích phải được thực hiện trên một bản sao điều tra của bằng chứng ban đầu, trừ khi hoàn cảnh cản trở người kiểm tra làm như vậy. Điều này rất quan trọng để bảo vệ tính toàn vẹn của bằng chứng. Bản sao kiểm tra của bằng chứng điện tử phải được lưu trữ trên phương tiện lưu trữ khác, không bao giờ được đưa vào bằng chứng. Bản sao pháp y phải được dán nhãn rõ ràng để đảm bảo nó không bị nhầm lẫn với các bằng chứng ban đầu hoặc với các bản sao điều tra từ các vụ án khác. Do đó, DFL phải chuẩn bị một số phương tiện lưu trữ trước khi nhận các vụ án.

Tài liệu này giải thích quá trình tiến hành kiểm tra và phân tích DF trên hai loại thiết bị:

(I) Máy tính

(II) Thiết bị di động

5.1.2 Máy tính

5.1.2.1 Các loại thu thập dữ liệu

Có hai cấp độ thu thập dữ liệu: thu thập dữ liệu vật lý và thu thập dữ liệu logic. Mặc dù thu thập dữ liệu vật lý bao gồm tất cả dữ liệu thô, một bản sao logic thường chỉ bao gồm một tập hợp con được phân bổ của những dữ liệu đó.

Thu thập dữ liệu vật lý, ở cấp toàn bộ đĩa, sao chép tất cả dữ liệu chứa trên đĩa, bao gồm sơ đồ phân vùng, khu vực được phân vùng và khu vực không được phân vùng. Thu thập dữ liệu logic trên cấp độ đĩa chỉ sao chép một khu vực được phân chia hợp lý.

Người kiểm tra thường chọn thu thập dữ liệu vật lý của toàn bộ đĩa vì nó bao gồm các tệp bị xóa và các cụm chưa được phân bổ. Tuy nhiên, khi xử lý mã hóa, việc thu thập dữ liệu logic của dữ liệu đã được mở khóa được ưu tiên hơn so với việc thu thập vật lý dữ liệu được mã hóa. Trong trường hợp này, việc thu hồi vật lý vẫn được khuyến nghị nếu phần mềm kiểm tra hỗ trợ việc gắn hình ảnh được mã hóa.

Để tạo một bản sao, người kiểm tra trước tiên cần chọn trạng thái của vật chứng. Nếu hệ thống hoạt động và chạy, người kiểm tra có thể cần chọn mua lại trực tiếp.

Tuy nhiên, nếu hệ thống bị tắt nguồn, người kiểm tra có thể chọn tiến hành thu thập gians tiếp. Sự khác biệt giữa các phương thức thu thập này được mô tả trong bảng sau.

	Thu thập gián tiếp	Thu thập trực tiếp
Khái niệm	Thu thập gián tiếp được thực hiện trên một hệ thống chết. Một hệ thống chết là một hệ thống không còn chạy; tắt hoàn toàn, không có điện. Khi hệ thống chết, dữ liệu dễ bay hơi trong các vùng lưu trữ tạm thời như bộ nhớ RAM, các tiến trình đang chạy, bộ đệm hoặc các hộp thoại ứng dụng đang hoạt động trên máy tính sẽ không còn khả dụng.	Thu thập trực tiếp được thực hiện trên một hệ thống sống. Một hệ sống là một hệ thống đang hoạt động và hoạt động trong đó thông tin có thể bị thay đổi khi dữ liệu liên tục được xử lý. Bởi vì giá trị bằng chứng phong phú có thể được phát hiện trong một hệ thống sống, tắt nó đi có thể làm mất dữ liệu dễ bay hơi, chẳng hạn như dữ liệu được lưu trữ trên cloud, dữ liệu được mã hóa, quy trình chạy, hệ thống tệp được kết nối và gắn kết mạng.
Phương thức	Quá trình tiến hành thu thập gián tiếp rất đơn giản vì nó thường được thực hiện tự động bằng thiết bị điều tra. Đĩa cứng trước tiên phải được lấy ra khỏi máy tính trước khi kết nối nó với thiết bị, nếu có thể. Trong một số trường hợp, máy tính netbook hoặc thiết bị có bộ lưu trữ ổ đĩa trạng thái hàn có thể được trích xuất khi thu hồi. Các	Dữ liệu trên một hệ thống có mức độ biến động khác nhau. Những dữ liệu này sẽ bị mất nếu hệ thống bị tắt hoặc khởi động lại. Bất cứ khi nào người kiểm tra có được dữ liệu sống, việc thu thập từ dữ liệu dễ bay hơi nhất đến ít biến động nhất là điều hợp lý. Mức độ biến động điển hình, từ biến động nhiều nhất đến biến động ít nhất như sau:

	phương pháp khác để thực hiện trích xuất trong các trường hợp như vậy, như khởi động hệ thống bằng CD / USB trực tiếp, cần được xem xét.	▪ Bộ nhớ ▪ Hoán đổi tập tin ▪ Quy trình mạng ▪ Quy trình hệ thống ▪ Thông tin file hệ thống
Bối cảnh	Việc thu thập gián tiếp được thực hiện khi: ▪ Hệ thống bị tắt ▪ Dữ liệu đã xóa quan trọng hơn dữ liệu dễ bay hơi	Thu thập trực tiếp được thực hiện khi: ▪ Hệ thống rất quan trọng và không thể ngừng hoạt động ▪ Dữ liệu dễ bay hơi quan trọng hơn dữ liệu bị xóa

Bảng 6. Phương pháp thu hồi mới - Thu hồi gián tiếp và Thu hồi trực tiếp

Sau đó, người kiểm tra cần chọn sao chép bản trình bày hoặc tạo một hình ảnh. Bản sao sao chép dữ liệu từng bit một từ phương tiện lưu trữ sang phương tiện lưu trữ khác. Mặt khác, hình ảnh sao chép dữ liệu từng bit một từ một phương tiện lưu trữ vào một tệp hình ảnh. Tập tin này sau đó có thể được lưu trữ trên một phương tiện khác.

Kỹ thuật thứ hai được sử dụng phổ biến hơn vì tệp hình ảnh sau đó có thể được đọc bởi hầu hết các phần mềm kiểm tra để xử lý phân tích điều tra. Nhân bản thường được sử dụng cho mục đích mô phỏng. Trước khi có thể được thực hiện, người kiểm tra phải đảm bảo rằng tang vật bị chặn viết; một phương pháp chỉ cho phép đọc và ngăn chặn bất kỳ cách viết nào trên tang vật.

5.1.2.2 Trình chặn ghi

Trình chặn ghi là một thiết bị cho phép thu thập dữ liệu từ đĩa cứng mà không cần sửa đổi dữ liệu đĩa. Thiết bị cho phép lệnh đọc, nhưng không cho phép các lệnh ghi được thực thi trên đĩa cứng. Hầu hết các công cụ hình ảnh đều có trình chặn ghi tích hợp mà người kiểm tra có thể sử dụng trong khi chụp ảnh đĩa cứng. Mặc dù chặn ghi cũng có thể đạt được bằng các công cụ phần mềm hoặc thay đổi trong Windows registry, các giải pháp phần cứng sẽ được ưu tiên trong các DFL.

5.1.2.3 Công cụ hình ảnh

Hình ảnh của một phương tiện lưu trữ có thể được thực hiện bằng phần mềm điều tra hoặc phần cứng. Có những sản phẩm miễn phí, cũng như thương mại, có sẵn có thể hỗ trợ trong quá trình này. Khi mua một công cụ, tiêu chí quan trọng nhất cần

tìm là tốc độ tiến hành hình ảnh và độ tin cậy. Phần mềm hình ảnh có thể bao gồm các tính năng như:

- Nhận diện các khu vực ẩn
- Chụp ảnh đồng thời nhiều thiết bị
- Hình ảnh đến nhiều điểm cùng một lúc
- Hàng đợi hình ảnh
- Xác minh băm với các thuật toán băm phổ biến
- Xác minh băm ở các giai đoạn khác nhau của quá trình hình ảnh
- Hỗ trợ các định dạng hình ảnh điều tra phổ biến nhất
- Tạo ra hình ảnh được mã hóa và nén
- Tiếp tục quá trình thu thập bị gián đoạn
- Khả năng chịu lỗi phần cứng

Người kiểm tra phải luôn cảnh giác với khả năng của các kỹ thuật chống điều tra. Các khu vực ẩn như khu vực được bảo vệ máy chủ (HPAs) hoặc lớp phủ cấu hình thiết bị (DCO), chỉ có thể truy cập thông qua các lệnh ATA đặc biệt, chỉ có thể được phát hiện bởi một số giải pháp phần mềm hình ảnh có sẵn.

5.1.2.4 Định dạng hình ảnh

Có một số định dạng tệp hình ảnh phổ biến, cụ thể là raw hoặc dd. Các định dạng này lưu trữ tất cả dữ liệu từ phương tiện ban đầu trong một tệp thô. Các định dạng khác bao gồm định dạng nhân chứng chuyên nghiệp (EWF) và định dạng điều tra nâng cao (AFF). Chúng chứa các tính năng như:

- Nén dữ liệu
- Mã hóa dữ liệu
- Kiểm tra lỗi
- Trường hợp siêu dữ liệu
- Tổng băm
- Chia hình ảnh thành khối

Hơn nữa, các giải pháp phần mềm điều tra khác nhau đi kèm với các định dạng hình ảnh độc quyền của riêng chúng với các tính năng tương tự. Khi chọn định dạng hình ảnh, luôn chọn một định dạng được hỗ trợ bởi hầu hết các giải pháp phần mềm điều tra. Một số DFL sử dụng phần mềm điều tra khác nhau và do đó, có khả năng tệp hình ảnh có thể không được mở nếu người điều tra chọn định dạng tệp hình ảnh duy nhất.

5.1.2.5 Luồng quy trình

Quá trình chung để tiến hành thu thập dữ liệu được minh họa trong hình sau:

Hình 6. Quy trình thu thập dữ liệu trên máy tính

A. Xác định phương tiện lưu trữ

Người giám định phải chuẩn bị một phương tiện lưu trữ tương thích, với kích thước dữ liệu đủ trước khi bàn giao. Nếu cuộc điều tra lớn, người kiểm tra có thể cần chuẩn bị một số phương tiện lưu trữ để lưu trữ tệp hình ảnh.

B. Hình ảnh tang vật

Để thu thập hình ảnh tang vật, đầu tiên kết nối nó với một trình chặn viết để đảm bảo tang vật không thể bị ghi, do đó bảo vệ tính toàn vẹn của nó. Hầu hết các công cụ pháp y cung cấp tính năng này. Các tập tin hình ảnh sau đó được lưu trữ trong phương tiện lưu trữ chuẩn bị. Để bảo vệ phương tiện lưu trữ và tệp hình ảnh, hãy sử dụng định dạng ghi nhãn tiêu chuẩn bằng cách băm tất cả các bằng chứng thu được với SHA256.

Người kiểm tra cần lưu ý rằng sử dụng kỹ thuật chặn ghi có sẵn không ngăn được các thay đổi đối với dữ liệu trên ổ đĩa trạng thái rắn hoặc phương tiện flash, bao gồm chip điều khiển. Ngay khi bộ điều khiển được gắn vào nguồn điện, nó sẽ bắt đầu sắp xếp lại dữ liệu trên các chip flash. Các tác vụ như cân bằng hao mòn, khuếch đại ghi và thu gom rác được thực hiện bởi bộ điều khiển ngay cả khi nó được gắn vào thiết bị chặn ghi. Tại thời điểm này, chỉ có một cách sử dụng nhiều tài nguyên để tạo ra một bản sao điều tra thực sự của phương tiện flash. Điều này được thực hiện bằng cách mở rộng (các) chip từ bảng mạch và sau đó lắp lại dữ liệu theo cách chính xác nếu có thể.

C. Xác minh tập tin tang vật và hình ảnh

Sau khi tệp hình ảnh được tạo người kiểm tra cần kiểm tra xem nó có thể chạy bằng phần mềm điều tra hay không và các giá trị băm của cả vật chứng và tệp hình ảnh có khớp với nhau không.

D. Tài liệu "Tất cả các hành động"

Bước cuối cùng trong việc kiểm tra và phân tích máy tính là ghi lại quá trình, các công cụ được sử dụng, các giá trị băm, ngày và giờ, cũng như các chữ cái đầu của người kiểm tra trong các trường hợp ghi chú hoặc bảng tính có sẵn tại phụ lục F: bảng tính thu thập dữ liệu.

5.1.3 Thiết bị di động

Phần tiếp theo sẽ cung cấp chi tiết phương pháp khai thác dữ liệu trên thiết bị di động.

5.1.3.1 Các loại khai thác dữ liệu

Trước khi bắt đầu công việc DF, người kiểm tra phải xem xét các giấy tờ vụ án thu được từ bên yêu cầu để xác định các loại dữ liệu được yêu cầu từ tang vật. Điều này có thể giúp người kiểm tra quyết định phương pháp trích xuất tốt nhất cho vụ án. Cần nỗ lực thực hiện để thu thập tất cả mật mã, mật khẩu hoặc mẫu của tang vật, trước khi tiến hành công việc. Sử dụng phương pháp thủ công, ví dụ, yêu cầu điện thoại phải được mở khóa. Hầu như tất cả các phương pháp trích xuất đều yêu cầu điện thoại phải được mở khóa. Do đó, luôn luôn cần thiết để cố gắng lấy mã mở khóa tại thời điểm bị tịch thu.

Có năm mức trích xuất dữ liệu khác nhau cho các thiết bị di động, được mô tả từ cấp độ mà hầu hết dữ liệu có thể được trích xuất đến mức có thể trích xuất ít nhất. Bất kể phương pháp nào được sử dụng, sau khi thông tin được trích xuất từ thiết bị (đã lắp SIM và MicroSD), thẻ SIM và Micro SD phải được phân tích riêng.

A. Khai thác vật lý

Một trích xuất vật lý là việc thu thập dữ liệu nhị phân thô từ bộ lưu trữ phương tiện của thiết bị. Những dữ liệu thô này sau đó cần được phân tích và xử lý ở giai đoạn sau bằng phần mềm điều tra. Phương pháp này thường cho phép người kiểm tra truy cập dữ liệu trực tiếp và bị xóa, các tệp hệ điều hành và các khu vực của thiết bị mà người dùng thường không thể truy cập.

B. Kết xuất hệ thống tệp (FSD)

Kết xuất hệ thống tệp (FSD) là sự kết hợp giữa khai thác vật lý và khai thác logic. FSD lấy hệ thống tập tin của thiết bị và diễn tả dữ liệu trong giai đoạn xử lý. Điều này cho phép người kiểm tra truy xuất, ví dụ, cơ sở dữ liệu chứa các thông báo đã xóa có thể không khả dụng khi trích xuất logic và có thể không truy cập được trong quá trình trích xuất vật lý. Tuy nhiên, một hạn chế của FSD là nó không truy xuất tất cả dữ liệu đã bị xóa theo cách mà một trích xuất vật lý có thể thực hiện.

C. Khai thác logic

Khai thác logic bao gồm nhận thông tin từ thiết bị di động và cho phép thiết bị trình bày dữ liệu để phân tích. Điều này thường tương đương với việc truy cập dữ liệu trên chính thiết bị. Phương pháp này làm cho dữ liệu trực tiếp có sẵn cho người kiểm tra. Hầu hết các phần mềm điều tra thiết bị di động cung cấp loại tính năng này.

D. Cách sử dụng

Một hạn chế của phần mềm điều tra là đôi khi nó không hỗ trợ kiểu máy của một số thiết bị di động duy nhất hoặc các mẫu mới ra mắt gần đây. Trong trường hợp này, người kiểm tra thường chấp nhận sử dụng phương pháp thủ công. Phương pháp này truy cập vào thiết bị và bản ghi dữ liệu được hiển thị trên màn hình bằng hình ảnh hoặc video hoặc bằng cách sao chép dữ liệu của thiết bị. Dành cho các thiết bị Android, người kiểm tra có thể xem xét thực hiện chụp màn hình bằng các công cụ phần mềm. Phương pháp này có thể yêu cầu điện thoại được kết nối thông qua lệnh ADB với chế độ nhà phát triển được bật.

E. JTAG / Chip-Off / Rooting / Jail Breaking

Đối với các thiết bị di động bị hỏng hoặc bị khóa bằng mật khẩu, phương pháp JTAG và Chip-Off có thể được sử dụng để trích xuất dữ liệu. Trích xuất JTAG đòi hỏi kỹ năng kỹ thuật cao. Sử dụng phương pháp này, người kiểm tra sẽ có thể truy xuất dữ liệu nhị phân thô từ bộ lưu trữ phương tiện của thiết bị.

Chip-Off cũng cho phép trích xuất dữ liệu nhị phân thô từ bộ lưu trữ của thiết bị, nhưng nó yêu cầu loại bỏ vĩnh viễn chip nhớ của thiết bị khỏi bảng nhớ. Khi người kiểm tra tiến hành Chip-Off, thiết bị sẽ bị hỏng và không thể sử dụng được nữa. Trên hết, những việc sử dụng Chip-Off cho thiết bị di động phải được kiểm

duyệt. Các thiết bị gần đây lưu trữ dữ liệu được mã hóa trên chip nhớ của họ. Các thiết bị hoạt động trên phiên bản Android 7.0 trở đi được mã hóa theo mặc định. Tắt chip vẫn sẽ tồn tại đối với các thiết bị IOT khác thường lưu trữ dữ liệu ở dạng văn bản rõ ràng.

Một phương pháp khác, ít tổn hại hơn, có thể được sử dụng với một số thiết bị di động là “Rooting” hoặc“Jail Breaking”. Quá trình này bao gồm việc tận dụng các tính năng của hệ điều hành để nâng cao quyền và đặc quyền của người dùng đang chạy (tương tự như quá trình giành quyền truy cập Root trong Linux). Quá trình này không thể được coi là một kỹ thuật điều tra vì nó liên quan đến việc sửa đổi các tệp hệ thống và có khả năng làm hỏng thiết bị và do đó nó nên nằm trong danh sách các kỹ thuật ít được sử dụng.

Thứ tự trích xuất là quan trọng. Người kiểm tra nên cố gắng tiến hành phương pháp kiểm tra ít phá hủy nhất nhưng mang lại nhiều dữ liệu nhất. Điều này cho phép người kiểm tra nắm bắt các khu vực có thể bị hư hỏng hoặc bị ghi đè ở các giai đoạn sau. Các phương pháp trích xuất như JTAG và Chip-Off chỉ nên được coi là biện pháp cuối cùng, đặc biệt là với Chip-Off, vì quá trình này có thể bị phá hủy và không thể phục hồi.

5.1.3.2. Công cụ khai thác

Phân tích thiết bị di động thường yêu cầu sử dụng phần mềm chuyên dụng, cáp nguồn và cáp dữ liệu. Các kỹ thuật kiểm tra cao hơn, như JTAG hoặc Chip-Off, yêu cầu thêm các công cụ khác.

Chúng bao gồm thiết bị hàn và đồ chuyên dụng để đọc dữ liệu thô từ chip nhớ của thiết bị

5.1.3.3. Định dạng file trích xuất

Do yêu cầu sử dụng các công cụ chuyên dụng để trích xuất dữ liệu, dữ liệu điện thoại di động thường được trích xuất ở định dạng độc quyền. Các định dạng này thường có thể được chuyển giữa các công cụ khác nhau để tận dụng điểm mạnh của các khả năng giải mã khác nhau. Các định dạng không độc quyền khác bao gồm tệp rác và tệp thô.

5.1.3.4. Quy trình

A. Xác định vật chứng và phương tiện lưu trữ

Người kiểm tra tiến hành kiểm tra trong tay, trước khi tiến hành quy trình tiếp theo. Nhãn của vật chứng phải được dán ở mặt trong của thiết bị di động hoặc được in ở mặt sau của thiết bị. Nhãn phải bao gồm số nhận dạng thiết bị di động quốc tế (IMEI), số nhận dạng thiết bị (MEID) hoặc số Serial . Những dữ liệu này xác định duy nhất cho thiết bị và được sử dụng để gửi yêu cầu cho hồ sơ thanh toán hoặc để tiến hành phân tích trang mạng thiết bị di động trong các giai đoạn sau của cuộc điều tra. Việc tạo, mô hình và IMEI / MEID, cũng có thể được sử dụng để xác định mức độ hỗ trợ từ phần mềm kiểm tra.

Tiếp theo, một phương tiện lưu trữ nên được chuẩn bị để lưu trữ dữ liệu trích xuất. Nếu yêu cầu có thẻ SIM, cần chuẩn bị thẻ SIM sạch, trống.

B. Cách ly vật chứng tới mạng

Khi tiến hành trích xuất thiết bị di động, thiết bị cần được bật. Để ngăn chặn mọi nỗ lực kết nối với mạng và sau đó có nguy cơ thay đổi dữ liệu, vật chứng cần phải được cách ly khỏi mạng. Ở một số quốc gia, một số mạng công cộng có sẵn ở mọi nơi và bằng chứng phải được cấu hình để kết nối chúng theo mặc định.

Tùy thuộc vào chi phí, sự cô lập có thể đạt được thông qua các hình thức khác nhau như:

Phương pháp cách ly mạng	
Nhân bản SIM / IDEN card	Thẻ SIM / IDEN xuất hiện trong vật chứng dưới dạng thẻ gốc nhưng thiếu khả năng kết nối với mạng di động. Một thẻ SIM / IDEN xác định thuê bao và tạo kết nối vào mạng Một số công cụ pháp y cung cấp chức năng nhân bản thẻ SIM / IDEN. Điện thoại di động mới nhất có thể được cung cấp không có thẻ SIM và không có tác động đến dữ liệu lưu trữ trong điện thoại
Phòng chắn mạng	Một phòng thí nghiệm được lắp đặt với tấm chắn Faraday để ngăn chặn tín hiệu mạng. Tuy nhiên đây là một giải pháp rất tốn kém và việc sử dụng các hộp Faraday nhỏ hơn có thể được coi là một giải pháp thay thế hiệu quả
Thiết bị gây nhiễu không dây	Thiết bị này chặn tín hiệu mạng đến. Trong một số

	quyền lực pháp lý, việc sử dụng này là bất hợp pháp, như đã nêu trong Mục 3.2.2
Phương pháp thủ công	Đây là phương pháp cấu hình để dàng và chi phí rẻ nhất. Tuy nhiên, nó cần người kiểm tra truy cập vào thiết bị. Điều này đặt ra một số rủi ro thay đổi dữ liệu. Nó được thực hiện bằng cách đặt thiết bị di động ở chế độ 'Flight Mode' và tắt WiFi, Bluetooth và bất kỳ kết nối mạng nào khác.

Bảng 7: Phương pháp cách ly mạng

C. Trích xuất dữ liệu liên quan

Do một số kỹ thuật trích xuất cụ thể, chẳng hạn như trích xuất bộ tải khởi động iOS và root cuả thiết bị Android, không phải lúc nào cũng có thể thực hiện chặn ghi vào thiết bị di động. Nếu có thể, việc chặn ghi nên được bổ sung, ví dụ như trên thẻ nhớ. Tuy nhiên, có thể thừa nhận rằng phương pháp chặn ghi không phải lúc nào cũng có thể thực hiện hoặc không thực tế đối với thiết bị di động. Vì lý do này, người kiểm tra điều bắt buộc phải nhận thức đầy đủ về hậu quả hành động của họ khi xử lý các thiết bị di động và có thể giải thích và biện minh cho những hành động này. Thiết bị di động được trình bày với ba phương tiện riêng biệt yêu cầu xử lý riêng các kỹ thuật, như trong bảng sau:

Phương tiện	Mô tả
SIM/IDEN card	Yêu cầu các công cụ điều tra thiết bị di động. Phương pháp để trích xuất dữ liệu là trích xuất logic. Khai thác vật lý là không thể cho thiết bị này. Cách tốt nhất là gỡ bỏ thẻ SIM / IDEN khỏi thiết bị trong quá trình làm việc. Tuy nhiên, một số thiết bị yêu cầu thẻ phải nằm bên trong các thiết bị khi chúng được bật. Người kiểm tra có thể nhân bản SIM / IDEN để khắc phục điều này.
Memory Cards	Có thể được kiểm tra như một đĩa cứng máy tính. Cả logic và khai thác vật lý có thể được tiến hành trên các thẻ này, miễn là công cụ điều tra hỗ trợ tính năng này. Người kiểm tra phải vào thẻ, trích xuất dữ liệu và sau đó đặt lại vào thiết bị trước khi bật

	nó lên. Một số thiết bị lưu trữ dữ liệu trong thẻ nhớ và nếu thấy rằng thẻ không có sẵn, nó có thể là nguyên nhân gây mất dữ liệu từ thiết bị di động. Nếu thời gian và tài nguyên cho phép, thẻ nhớ nên được nhân bản và chèn bản sao đó vào thiết bị cầm tay.
Internal Memory	Đòi hỏi các công cụ điều tra thiết bị di động. Một số thiết bị được hỗ trợ bởi các công cụ điều tra để trích xuất vật lý bộ tải khởi động. Điều này thường có thể được thực hiện mà không cần thẻ SIM / IDEN. Các công cụ điều tra sẽ khởi động thiết bị theo một cách cụ thể và tiến hành trích xuất vật lý mà không thực hiện bất kỳ thay đổi hoặc biến đổi nào đối với dữ liệu người dùng trên thiết bị. Phương pháp này có khả năng phục hồi mã khóa thiết bị, cho phép người kiểm tra có quyền truy cập đầy đủ vào thiết bị, sau khi được bật.

Bảng 8: Phương tiện lưu trữ thiết bị di động

Quá trình trích xuất sẽ thay đổi tùy thuộc vào công cụ trích xuất được chọn. Hầu hết các công cụ điều tra đều có hướng dẫn giải thích quy trình phải tuân theo để trích xuất thành công. Trong một số trường hợp, kiểm tra và phân tích thiết bị di động yêu cầu sửa đổi các file hệ thống hoặc hệ điều hành để trích xuất dữ liệu. Ở một mức độ nào đó, cần phải tải lên hoặc cài đặt các ứng dụng cho thiết bị di động. Quá trình này có thể khiến một số dữ liệu bị mất không thể phục hồi, tuy nhiên nó chỉ ảnh hưởng đến các tệp hệ thống có ít giá trị chứng minh.

Kiến thức về những gì bị thay đổi bởi bất kỳ quy trình nào trong số này có thể đạt được bằng cách nắm giữ các chứng chỉ đào tạo phù hợp, chẳng hạn như đào tạo được cung cấp bởi các nhà sản xuất phần mềm điều tra di động hoặc kinh nghiệm thực tế liên quan đến thử nghiệm trích xuất thiết bị di động.

Một nguồn tốt khác cho bằng chứng điều tra là tập tin sao lưu thiết bị di động. Một số người dùng và thiết bị sẽ tạo bản sao lưu trên các thiết bị khác, chẳng hạn như trong máy tính hoặc trên cloud. Các bản sao lưu này có thể hỗ trợ quá trình thu thập bằng chứng và cũng có thể được sử dụng để có quyền truy cập vào thiết bị bị khóa mật mã. Cũng có thể phân tích một số bản sao lưu như thể chúng là một thiết bị vật lý.

D. Xác minh chứng cứ và dữ liệu được trích xuất

Khi dữ liệu đã được trích xuất, người kiểm tra phải xác minh dữ liệu dựa trên dữ liệu được hiển thị trên thiết bị chứng cứ. Thông tin như ngày và giờ phải được kiểm tra bởi người kiểm tra, vì đôi khi nó được chuyển đổi sang định dạng ngày / giờ khác trong quá trình trích xuất.

E. Tài liệu tất cả các hành động

Bước cuối cùng trong việc kiểm tra và phân tích một thiết bị di động là ghi lại quá trình, các công cụ được sử dụng, ngày và thời gian và tên viết tắt của người kiểm tra trong các trường ghi chú

5.2 Kiểm tra

5.2.1 Tổng quát

Kiểm tra bằng chứng gốc nên tránh, nếu có thể. Người kiểm tra phải luôn luôn làm việc trên bản sao (file hình ảnh) của bằng chứng. Nếu điều này là không thể tránh khỏi, quyền truy cập vào dữ liệu phải được bảo vệ bằng cách sử dụng trình chặn ghi. Trong một số trường hợp nhất định, người kiemr tra cần sử dụng một môi trường biệt lập hoặc môi trường được thiết lập sẵn để tiến hành kiểm tra. Ví dụ: tiến hành mô phỏng trên hệ thống cơ sở dữ liệu hoặc phần mềm chơi trò chơi. Để đạt được điều này, người kiểm tra có thể sử dụng công nghệ ảo hóa. Khi kiểm tra hoàn tất, người kiểm tra có thể hoàn nguyên máy trạm về trạng thái trước đó bằng hình ảnh đã biết hoặc sử dụng một tính năng được cung cấp bởi hệ điều hành.

5.2.2 Triage

Triage là quá trình ưu tiên các trường hợp, chứng cứ hoặc dữ liệu cho các quá trình phân tích, theo mức độ phù hợp của chúng với vụ việc. Dựa trên kết quả của việc phân loại, các trường hợp, chứng cứ hoặc dữ liệu sẽ được phân tích tùy thuộc vào trình tự ưu tiên của chúng từ quan trọng nhất đến ít quan trọng nhất. Có thể một số có thể không được phân tích ở tất cả do không liên quan đến vụ án đang được điều tra. Việc xử lý được tiến hành để giải quyết các tình huống như:

- Một số lượng lớn chứng cứ hoặc dữ liệu cần được phân tích trong một khung thời gian ngắn;
- Các chứng cứ không thể được lưu trữ lâu hơn do các vấn đề pháp lý;
- Đây là trường hợp ưu tiên cao và cần phải tạo ra kết quả ngay lập tức, tức là trong trường hợp có thể gây tổn hại cơ thể hoặc tử vong.

Trong qua trình xử lý Triage cung cấp một số lợi thế, cũng có những nhược điểm cần được giải quyết. Một triage không thể thay thế một cuộc kiểm tra đầy đủ. Việc xử lý được tiến hành bằng cách xử lý tự động, điều này được cung cấp bởi phần mềm điều tra hoặc bằng cách chạy mã tự viết cho các chứng cứ hoặc dữ liệu. Có một rủi ro là việc xử lý tự động này chỉ kiểm tra các tập hợp con của dữ liệu và một số dữ liệu quan trọng có thể bị bỏ qua. Rủi ro này cần được giải thích cho điều tra viên, công tố viên hoặc thẩm phán và dựa trên thông tin đó họ có thể cần quyết định ủng hộ hoặc chống lại quá trình xử lý cho trường hợp cụ thể đó. Tuy nhiên, triage vẫn là một phương pháp hợp lệ để đối phó với một tình huống không thể giải quyết bằng bất kỳ cách nào khác.

Có rất nhiều phần mềm trên thị trường cung cấp các chức năng phân loại, một số là thương mại và một số là nguồn mở. Việc phân loại có thể được tiến hành bằng cách chạy phần mềm trong khi thiết bị vẫn còn hoạt động hoặc bằng cách khởi động thiết bị bằng phương tiện có thể khởi động điều tra. Người kiểm tra sau đó nhập từ khóa và cho phép hệ thống chạy, trước khi chọn các tệp có liên quan và lưu trữ chúng trong phương tiện lưu trữ di động. Bằng cách này, nhiều thiết bị có thể được xử lý cùng một lúc, thậm chí qua đêm hoặc trong những ngày cuối tuần.

Sau khi tiến hành phân loại và người kiểm tra quyết định rằng tang vật có liên quan đến cuộc điều tra, người kiểm tra có thể tiến hành quy trình tiếp theo được mô tả trong tài liệu này và sử dụng các phương pháp tinh vi hơn để thu thập thêm dữ liệu từ máy tính.

5.2.3 Phương pháp kiểm tra máy tính

Có nhiều phương pháp và kỹ thuật để kiểm tra một máy tính. Một số yêu cầu kỹ năng chuyên sâu trong khi những người khác yêu cầu kỹ năng tối thiểu, chẳng hạn như tiến hành một quy trình tự động. Một số phần mềm điều tra có thể được người kiểm tra sử dụng. Tùy thuộc vào khả năng của phần mềm, một số có thể khôi phục mật khẩu, tương quan dữ liệu giữa bằng chứng điện tử và tiến hành tìm kiếm từ khóa. Luồng quy trình để tiến hành kiểm tra trên máy tính có sẵn tại phụ lục H: Biểu đồ quy trình kiểm tra máy tính. Biểu đồ luồng được giải thích trong phần sau.

5.2.3.1 Kiểm tra trên "Dead System"

Một "Dead System" là một hệ thống không chạy, đã tắt. Khi hệ thống bị "dead", dữ liệu dễ bị mất trong các vùng lưu trữ tạm thời như bộ nhớ RAM, các tiến trình đang chạy, bộ đệm hoặc các hộp thoại ứng dụng đang hoạt động trên máy tính sẽ không còn khả dụng. Việc kiểm tra một hệ thống đã "dead", phải xem xét các dữ liệu sau:

- Các file đang hoạt động, các file đã bị xóa, file slack, phân vùng slack , disk slack, and shadow files
- File hệ điều hành, file registry, file metadata, encrypted files, log files and database files
- Lịch sử duyệt web, e-mail, phương tiện truyền thông xã hội và chia sẻ tệp ngang hàng

5.2.3.2 Kiểm tra trên "Live System"

Một "Live System" là một hệ thống đang bật và hoạt động, nơi các ứng dụng có thể đang chạy và có thể được cập nhật khi dữ liệu liên tục được xử lý. Do các bằng chứng có giá trị có thể được phát hiện trong một hệ thống đang hoạt động, việc tắt nó có thể gây mất dữ liệu dễ mất như dữ liệu được lưu trữ trên cloud, dữ liệu được mã hóa, tiến trình đang chạy, kết nối mạng và hệ thống file được gắn.

Kiểm tra một hệ thống đang hoạt động nên xem xét các dữ liệu sau:

- Bộ nhớ truy cập ngẫu nhiên (RAM)
- Các tiến trình đang chạy
- Kết nối mạng
- Cài đặt hệ thống
- Phương tiện lưu trữ
- Dịch vụ cloud

Tùy thuộc vào yêu cầu trường hợp, việc kiểm tra hệ thống đang hoạt động có thể được tiến hành trên bất kỳ dữ liệu nào ở trên.

5.2.3.3 Xử lý tự động

Xử lý tự động thường được tiến hành bằng cách sử dụng các tính năng có sẵn trên phần mềm điều tra. Phạm vi xử lý tự động thường được người kiểm tra đặt ra khi bắt đầu kiểm tra. Phạm vi này có thể được lặp lại cho các trường hợp khác trong phạm vi điều tra tương tự.

Một ví dụ là chạy so sánh băm trên hình ảnh trong trường hợp khiêu dâm trẻ em. Các hoạt động và trình tự phổ biến để xử lý tự động là:

i. Khai thác dữ liệu người dùng và hệ điều hành
ii. Gắn các mục chứa như ZIP, RAR và mục chứa được mã hóa.
iii. Trích xuất và phân tích các thông tin như hộp thư và lịch sử Internet

iv. Phân tích chữ ký
v. Khôi phục các tập tin và thư mục đã xóa
vi. Khôi phục phân vùng đã xóa
vii. Khắc phục một số loại tệp
viii. Tùy thuộc vào trường hợp yêu cầu, các phương pháp phân tích này có thể được sử dụng:

- Tìm kiếm từ khóa
- Nhận dạng ký tự quang học (OCR) của file PDF
- Tạo hình thu nhỏ để xem dễ dàng
- Trích xuất hình ảnh từ video
- Phát hiện tông màu cho video
- So sánh băm

ix. Xử lý nhật ký hệ điều hành (ví dụ: windows event log)

Bước này giúp tiết kiệm thời gian vì nó có thể chạy qua đêm hoặc cuối tuần với sự giám sát tối thiểu, mặc dù nó sử dụng khả năng tính toán cao.

5.2.3.4 Phục hồi dữ liệu

Phục hồi dữ liệu liên quan đến việc khôi phục dữ liệu trên phương tiện lưu trữ đã bị xóa, bị hỏng, bị ẩn hoặc bị mất. Trong một số trường hợp, phương tiện lưu trữ bị hỏng hoặc được định dạng, khiến dữ liệu không thể truy cập được. Do đó, phục hồi dữ liệu cũng liên quan đến quá trình sửa chữa phương tiện lưu trữ để dữ liệu có thể được trích xuất từ phương tiện truyền thông.

Có hai loại phục hồi dữ liệu - phục hồi logic và phục hồi vật lý.

Phục hồi logic được tiến hành khi phương tiện lưu trữ có thể truy cập được, nhưng dữ liệu được định dạng, bị hỏng, bị ẩn hoặc bị mất. Quá trình phục hồi thường được tiến hành bằng phần mềm điều tra.

Phục hồi vật lý được tiến hành khi phương tiện lưu trữ không thể truy cập do lỗi cơ học hoặc lỗi điện tử. Quá trình phục hồi đòi hỏi một số kỹ năng nâng cao. Trong một số trường hợp, cần có một phòng đặc biệt để tiến hành phục hồi vật lý, ví dụ thay thế một đầu trong đĩa cứng đòi hỏi nó phải được tiến hành trong phòng 100 lớp. Trong các

trường hợp khác, thiết bị đặc biệt là cần thiết để phục hồi dữ liệu. Ví dụ, cần có máy hàn khi thay thế cáp trong ổ USB.

Không phải tất cả các DFL đều có thể có một cơ sở phục hồi vật lý vì chi phí cao và người kiểm tra phải có tay nghề cao để thực hiện các nhiệm vụ. Tuy nhiên, có một cơ sở phục hồi logic là đủ cho DFL. Hầu hết các phần mềm phân tích điều tra đều đi kèm với tính năng khôi phục logic, vì vậy người kiểm tra có thể sử dụng hoặc nâng cấp để thêm tính năng được cung cấp để tiết kiệm chi phí.

5.2.3.5 Lọc

Áp dụng các bộ lọc cho một file hình ảnh trước khi nó được phân tích có thể giúp giảm lượng dữ liệu mà người kiểm tra phải xem và phân tích. Các kỹ thuật lọc phổ biến sử dụng các bộ băm để lọc các hệ điều hành hoặc file chương trình đã biết (whitelisting) hoặc để tìm kiếm cụ thể các kết quả băm trong cơ sở dữ liệu của các tài liệu bất hợp pháp đã biết (blacklisting).

Lọc cũng có thể được áp dụng khi chỉ một số loại phát hiện nhất định có liên quan đến vụ án. Các file có thể được lọc bằng phân tích chữ ký - theo kích thước, ngày, chủ sở hữu và nhiều chi tiết khác nằm trong siêu dữ liệu. Tính năng lọc này được cung cấp trong hầu hết các phần mềm điều tra thương mại.

5.2.4 Phương pháp kiểm tra thiết bị di động

Thiết bị di động đặt ra một thách thức cho người kiểm tra vì sự đa dạng của hệ điều hành, thương hiệu và kiểu máy, sự phong phú của dữ liệu và sự đa dạng của các loại dữ liệu được lưu trữ trong thiết bị là quá lớn.

Dưới đây mô tả các phương pháp chung phổ biến được tiến hành trên thiết bị di động.

5.2.4.1 Xử lý tự động

Việc xử lý các thiết bị di động thường đòi hỏi một cách tiếp cận khác với máy tính do phần cứng và phần mềm được sử dụng giữa các thiết bị rất khác nhau. Các ứng dụng được cập nhật với tần suất lớn hơn nhiều. Vì lý do này, các công cụ điều tra chuyên dụng sẽ tự động xử lý nhiều dữ liệu, tuy nhiên việc xác minh thủ công thường là cần thiết. Một số công cụ có sẵn sử dụng một hình thức xử lý “fuzzy processing”, có nghĩa là, xử lý được thực hiện theo cách tận dụng logic và các kết quả không được chặt chẽ.

5.2.4.2 Lọc

Lọc dữ liệu di động thường được thực hiện ở mức độ loại dữ liệu. Dữ liệu được lọc bởi các công cụ trong quá trình xử lý thành các nhóm như dữ liệu truyền thông và file phương tiện. Các nhóm này sau đó được chia tiếp; ví dụ dữ liệu liên lạc có thể được chia thành các bản ghi cuộc gọi và tin nhắn. Mức lọc được đưa ra cho nhà phân tích phụ thuộc vào công cụ được sử dụng, tuy nhiên, bộ lọc này cho phép các nhà phân tích nhanh chóng xem xét các loại dữ liệu chính. Chúng có thể bao gồm tin nhắn SMS đã gửi và nhận và hồ sơ cuộc gọi để thiết lập liên lạc giữa các nghi phạm.

5.3 Phân tích

Trong giai đoạn phân tích, người kiểm tra tìm kiếm bằng chứng điện tử trên hình ảnh. Điều này có thể rất tốn thời gian và có thể đòi hỏi nhiều kiến thức chuyên môn để giải thích các dấu vết từ nhiều file hệ thống, hệ điều hành và ứng dụng. Nhiều yếu tố khác nhau có ảnh hưởng đến thời gian và khối lượng công việc cần thiết cho giai đoạn phân tích. Các yếu tố này bao gồm lượng phương tiện lưu trữ được phân tích, kích thước của phương tiện lưu trữ, độ phức tạp của file hệ thống được sử dụng, mức độ sử dụng của hệ điều hành, độ tinh vi của người dùng, độ phức tạp của phần mềm và các kỹ thuật được sử dụng bởi người dùng máy tính, v.v.

5.3.1 Phân tích máy tính

5.3.1.1 Danh mục dấu vết kỹ thuật số

Giống như một tên tội phạm để lại dấu vết vật lý ở hiện trường vụ án, tên tội phạm sử dụng bằng máy tính sẽ để lại dấu vết tại hiện trường vụ án. Một số dấu vết này có thể được khám phá, một số trong số chúng có thể được cấu hình để người kiểm tra không thể khám phá được. Bảng sau liệt kê một số ví dụ về các dấu vết và cấu hình có thể khám phá để tránh các dấu vết có thể phát hiện được.

Dấu vết có thể phát hiện	Dấu vết không thể phát hiện được
Được lưu trữ trên máy tính theo mặc định. Xác suất tìm thấy dấu vết như vậy là rất cao, ngay cả khi nghi phạm cố gắng che dấu vết của mình. Một số dấu vết có thể khám phá: • Slack space • Unallocated space	Có thể được cấu hình không được lưu trữ trên máy tính. Ví dụ: trình duyệt web nơi người dùng có thể vô hiệu hóa hoặc xóa lịch sử tải xuống. Một số dấu vết không thể phát hiện: • Thumb caches

• MFT entries • RAM	• Most recently used lists • Log files • Browser histories • Browser caches • Most used programs • Form data • Pagefile.sys • Hiberfil.sys • Volume shadow copies • Download history

Bảng 9. Dấu vết có thể phát hiện và không thể phát hiện từ máy tính

5.3.1.2 Quy trình cho các dấu vết khác nhau

Dữ liệu và thông tin cần được trích xuất từ máy tính tùy thuộc vào loại trường hợp. Ví dụ: trong trường hợp liên quan đến gian lận, dữ liệu / thông tin thường được trích xuất từ máy tính ở dạng bảng tính, e-mail và tài liệu văn phòng. Trong trường hợp lạm dụng trẻ em, dữ liệu / thông tin liên quan có thể có thể là hình ảnh, video và tin nhắn liên lạc.

Quá trình phân tích các loại vật chứng khác nhau được minh họa tại Phụ lục I: Quy trình phân tích các vật chứng. Các phần sau đây giải thích chi tiết các loại dữ liệu có thể được trích xuất từ máy tính.

A. Email

Phân tích e-mail, thường liên quan đến các ứng dụng thư khách như Outlook, Thunderbird và Mail cũng như các tài khoản webmail. Các ứng dụng thư khác nhau sẽ tạo ra các loại vật chứng khác nhau. Ví dụ: Outlook lưu trữ dữ liệu bằng chứng trong các tệp thư mục cá nhân như các tệp PST, OST và PAB. Thunderbird lưu trữ tin nhắn trong các tập tin hộp thư đến. Thông thường, phần mềm điều tra có khả năng phân tích các tệp này, tuy nhiên chúng không nhất thiết phải trích xuất tất cả các tin nhắn. Một số phần mềm điều tra không thể truy xuất các tin nhắn đã xóa từ các tệp thư mục cá nhân, vì vậy phương pháp khôi phục dữ liệu có thể cần thiết trong trường hợp này.

B. Tài liệu (Trình xử lý Word, Bảng tính, bản trình bày)

Phân tích các tài liệu văn phòng thường bắt đầu bằng phân tích chữ ký file và được theo sau bằng cách lọc các file liên quan. Phân tích chữ ký file so sánh tiêu đề file với phần mở rộng của nó để đảm bảo nó được khớp. Nếu nó không khớp, có thể có tiêu đề hoặc phần mở rộng tài liệu đang được sửa đổi để ẩn nội dung. Lọc các tập tin liên quan đến việc sử dụng một tìm kiếm từ khóa. Hầu hết các phần mềm điều tra có thể thực hiện cả hai nhiệm vụ tự động.

Khi gười kiểm tra đã phát hiện ra các tài liệu liên quan, điều này có lợi cho việc phân tích nội dung. Điều này là để đảm bảo rằng tài liệu trích xuất thực sự có liên quan đến vụ án đang được điều tra. Khi người yêu cầu đã xác nhận các tài liệu, người kiểm tra có thể tiến hành phân tích sâu hơn về tài liệu, siêu tài liệu, nhà sản xuất tài liệu và xác định xem nó đã được gửi hoặc nhận trên máy tính chưa.

C. Hình ảnh và video

Để tiến hành phân tích trên hình ảnh và video, trước tiên, người kiểm tra cần có một ý tưởng rõ ràng về những gì cần tìm kiếm từ người yêu cầu. Nếu liên quan đến việc tìm kiếm các bức ảnh giống hệt nhau, thì người yêu cầu cần cung cấp cho người kiểm tra những bức ảnh cần thiết. Nếu nó liên quan đến các file với các hàm băm đã biết, thì người yêu cầu có thể cần cung cấp cho người kiểm tra hoặc người kiểm tra có thể sử dụng danh sách các giá trị băm từ cơ sở dữ liệu đã biết. Nếu nó liên quan đến một phần nhất định của video, thì người yêu cầu cần nêu các tính năng độc đáo của video. Ví dụ: để trích xuất tất cả hình ảnh từ video có xe máy.

Phân tích hình ảnh thường bắt đầu với phân tích chữ ký. Sau đó người kiểm tra có thể chọn lọc các hình ảnh trong bộ sưu tập bằng cách sử dụng chế độ xem hình thu nhỏ.

Trường hợp yêu cầu tìm kiếm một tập hợp các hình ảnh đã biết - ví dụ trong trường hợp lạm dụng trẻ em hoặc bản thiết kế bị đánh cắp - một phép so sánh băm có thể được sử dụng để thực hiện nhiệm vụ này. Một số phần mềm điều tra cung cấp một tính năng phát hiện hình ảnh tương tự, người kiểm tra có thể sử dụng tính năng này bằng cách cung cấp hình ảnh cần thiết cho phần mềm.

Để phân tích video, một số phần mềm cung cấp tính năng trích xuất ảnh tĩnh từ video. Ví dụ hình ảnh Y, trong mỗi X giây / phút. Những hình ảnh được trích xuất sau đó cũng có thể được xem trong một bộ sưu tập. Điều này cho phép xem trước các tập tin video hiệu quả hơn nhiều.

Trong trường hợp vị trí hoặc chi tiết sản xuất của các tệp hình ảnh và video là quan trọng, người liểm tra nên xem xét trích xuất siêu dữ liệu của các tệp đó. Siêu dữ liệu là tập hợp dữ liệu mô tả và cung cấp thông tin về các dữ liệu khác, ví dụ tọa độ GPS nơi ảnh được chụp, ngày và giờ tạo cũng như thiết bị được sử dụng để chụp ảnh. Một số vật chứng có thể có hàng ngàn hình ảnh và video và nười kiểm tra là không thể sàng lọc và định vị một tập tin video hoặc hình ảnh cụ thể. Cách tốt nhất để làm điều này là trích xuất tất cả các hình ảnh và sau đó chuyển chúng cho người yêu cầu. Nhiệm vụ đơn giản là xem nội dung của hình ảnh / video không yêu cầu bất kỳ chuyên môn điều tra kỹ thuật số nào và do đó người yêu cầu có thể thực hiện được. Khi các hình ảnh / video liên quan đã được xác định, người kiểm tra có thể tiến hành phân tích thêm để trích xuất dữ liệu có ý nghĩa hơn, chẳng hạn như tọa độ GPS và dữ liệu tạo hoặc sửa đổi.

D. Trình duyệt Internet

Các trình duyệt Internet có giá trị bằng chứng trong nhiều trường hợp. Chúng thường chứa các thành phần sau:

- Lịch sử truy cập trang web
- Bộ nhớ cache cục bộ / tập tin internet tạm thời
- Dấu trang / mục yêu thích
- Thông tin phiên
- Cookies
- Tên người dùng và mật khẩu đã lưu
- Tìm kiếm từ khóa Internet

Phân tích các thành phần của trình duyệt có thể quan trọng để đề xuất mục đích hoặc ý định, một ví dụ là các từ khóa được sử dụng trong các công cụ tìm kiếm có thể chứng minh ý định. Các trình duyệt phổ biến bao gồm Google Chrome, Microsoft Internet Explorer / Edge, Mozilla Firefox và Apple Safari. Tất cả đều lưu trữ dữ liệu trong thư mục “Home”của người dùng. Ngoại trừ các

trình duyệt của Microsoft, tất cả các trình duyệt khác đều sử dụng cơ sở dữ liệu SQLite để lưu trữ các thành phần đã nêu ở trên.

Hầu hết các phần mềm điều tra phân tích internet đều cung cấp phân tích trình duyệt. Tuy nhiên, do công nghệ phát triển trong đó một số trình duyệt thường xuyên được cập nhật, một số phần mềm điều tra có thể mất một thời gian để cập nhật cơ sở dữ liệu của nó. Do đó, điều quan trọng là người kiểm tra phải hiểu cấu trúc cơ bản của trình duyệt internet. Vì hầu hết các trình duyệt ngày nay hoạt động trên cơ sở dữ liệu SQLite, người kiểm tra có thể xem xét phân tích thủ công bằng cách sử dụng các trình duyệt cơ sở dữ liệu SQLite, có thể tải xuống miễn phí.

Điều này không chỉ cho phép người kiểm tra độc lập với một phần mềm cụ thể mà còn cho phép họ kiểm tra chéo kết quả của phần mềm với các trình duyệt cơ sở dữ liệu SQLite.

E. Phần mềm

Bất cứ khi nào có một phần mềm nhất định cần phải được phân tích, phần lớn quá trình liên quan đến việc trích xuất và tìm hiểu về các thành phần của phần mềm đó. Ví dụ về các phần mềm như vậy bao gồm phần mềm giao tiếp (Whatsapp và Skype), phần mềm steganography (ví dụ: OpenStego), két mật khẩu (ví dụ: KeePass), phần mềm chia sẻ tệp (ví dụ: uTorrent) và phần mềm tiền điện tử.

Mặc dù không có quy trình chuẩn nào về cách phân tích tất cả các dữ liệu phần mềm do tính đa dạng của chúng, nhưng việc phân tích thường được thực hiện bằng cách tiến hành thu thập thông tin trên các nguồn xác thực và đáng tin cậy trên các phần mềm. Những phát hiện sau đó có thể được xác minh bằng cách tiến hành một bản mô phỏng.

F. Hoạt động người dùng

Hệ điều hành theo dõi hoạt động của người dùng ở nhiều nơi khác nhau, Ví dụ như:

- Thời gian bật và tắt nguồn
- Cài đặt phần mềm
- Danh sách tập tin được sử dụng gần đây nhất

- Sử dụng thiết bị
- Đăng nhập người dùng
- Kết nối Wi-Fi
- Các chương trình ưu tiên
- Thiết lập môi trường người dùng
- Tập tin thường xuyên truy cập

Phân tích hoạt động người dùng giúp hiểu rõ hơn về hành vi của người dùng và thậm chí có thể chứng minh các hoạt động để làm chứng cứ. Tùy thuộc vào hệ điều hành, các chứng cứ được lưu trữ ở nhiều vị trí khác nhau. Trong Microsoft Windows, hầu hết các dữ liệu được lưu trữ trong Register, Event Logs và Jump list.

Trên các hệ thống OS X, các chứng cứ được lưu trữ trong Library và các thư mục nhật ký, trong khi trên các hệ thống Linux, hầu hết dữ liệu sẽ được lưu trữ trong home folder của người dùng hoặc các thư mục "/ etc" hoặc "/ var".

G. Tệp tin nhật ký

Phân tích các tệp tin nhật ký là rất cần thiết, đặc biệt trong các trường hợp tấn công chống lại hệ thống. Examiner nên trích xuất không chỉ các tệp nhật ký được chỉ định mà cả dấu vết của các tệp nhật ký đã xóa hoặc chưa phân bổ. Phần mềm chuyên dụng được cũng cấp sẵn sàng cho việc phân tích tệp nhật ký. Cơ sở của hoạt động phân tích như vậy là tìm kiếm các từ khóa cụ thể, các mẫu bất thường hoặc tìm kiếm các bản ghi nằm trong khung thời gian đặt trước.

H. Mã hóa

Hầu hết các hệ điều hành phổ biến hiện nay đều cung cấp các phương tiện mã hóa tích hợp. Người dùng dễ dàng kích hoạt mã hóa toàn bộ cho ổ đĩa hệ thống. Lưu ý rằng mật khẩu hoặc khóa mã hóa được thu thập tại hiện trường vụ án bằng cách sử dụng biện pháp thu thập dữ liệu trực tiếp trước khi truy tố sẽ được chuyển đến DFL.

Mã hóa cũng có thể hữu ích để trích xuất các mật khẩu khác (ví dụ: mật khẩu trình duyệt) từ đĩa nếu có thể. Những mật khẩu và hoán vị của chúng có thể được

sử dụng để tạo ra một từ điển giúp tiến hành một cuộc tấn công bằng cách sử dụng các kỹ thuật bẻ khóa mật khẩu chuyên dụng.

Ngoài ra, các hoạt động thực thi pháp luật truyền thống như thu thập bằng chứng vật lý, bao gồm cả mật khẩu bằng văn bản, khóa hoặc chuỗi khôi phục nên được tiến hành trong công tác tìm kiếm mật mã.

I. Không gian chưa phân bổ

Các khu vực chưa được phân bổ có thể chứa tất cả các loại bằng chứng được đề cập ở trên. Tìm kiếm và trích xuất các loại tệp nhất định trong các khu vực chưa được phân bổ có thể được tự động bằng cách sử dụng phần mềm khắc. Người kiểm tra nên chỉ định loại tệp nào họ đang tìm kiếm vì khắc dữ liệu là một công việc rất tốn thời gian. Khắc dữ liệu không hoạt động tốt trên các tệp bị phân mảnh. Hầu hết dữ liệu thời gian được tìm thấy trong các khu vực chưa được phân bổ không thể được liên kết với một người dùng nhất định, dấu thời gian hoặc thậm chí là một vị trí nào đó trong thư mục.

J. Lưu trữ từ xa và lưu trữ cloud

Khi người kiểm tra phát hiện ra dấu vết của dịch vụ cloud trong máy tính, nó có thể chỉ ra một trong những điều sau đây:

- Dữ liệu được lưu trữ cục bộ trên máy tính và từ xa trên đám mây; hoặc
- Dữ liệu được lưu trữ đầy đủ trên đám mây. Máy tính có thể không chứa bất kỳ dữ liệu nào cả.

Trên thực tế, dữ liệu được lưu trữ từ xa có thể không chỉ được lưu trữ trên một máy chủ mà còn có thể được lưu trữ trên nhiều máy chủ khác nhau trong cloud. Hầu hết thời gian, ngay cả nhà cung cấp dịch vụ cloud cũng không thể biết máy chủ cụ thể, trung tâm dữ liệu hoặc quốc gia nào được lưu trữ một số phần nhất định của dữ liệu.

Người kiểm tra thậm chí có thể tìm thấy các tình huống trong đó không thể lấy một byte dữ liệu nào từ máy tính của công ty vì chúng chỉ là máy tính khách không có bất kỳ phương tiện lưu trữ nào, mà chúng sử dụng tài nguyên của máy ảo trong cloud.

Mặc dù về mặt kỹ thuật, thật dễ dàng để tạo một bản sao của máy ảo nằm trong cloud, nhưng vẫn có một số vấn đề pháp lý cần được xem xét. Tùy thuộc vào luật pháp hiện hành, việc xác định và có được ủy quyền pháp lý phù hợp để chặn bắt lấy được dữ liệu đó có thể là không dễ dàng. Nó cũng có thể là thách

thức do cần đảm bảo rằng dữ liệu đã được thu thập tuân thủ các thủ tục pháp lý tại quốc gia đó.

Một nhược điểm khác là khả năng dữ liệu có thể phục hồi được là rất ít. Thật vậy, nếu một nghi phạm tạo ra một máy ảo tạm thời để thực hiện tội ác của mình và sau đó xóa máy đó, có thể không có bằng chứng nào được phục hồi.

Khả năng có được và phân tích dữ liệu được lưu trữ từ xa phụ thuộc vào luật pháp và quyền hạn pháp lý. Trong một số khu vực pháp lý hoặc trong một số trường hợp, người kiểm tra được phép kết nối với bộ lưu trữ từ xa bằng thông tin xác thực của nghi phạm từ máy tính để lấy dữ liệu. Các khu vực pháp lý khác có thể không chấp nhận việc mua lại như vậy. Trong những trường hợp này, các kênh chính thức có thể được sử dụng để yêu cầu duy trì và truy cập dữ liệu từ nhà cung cấp.

K. Bộ nhớ máy tính (RAM)

Nếu bộ nhớ máy tính đã được trích xuất trong khi máy tính bị tịch thu vẫn đang chạy, kết xuất bộ nhớ có thể được phân tích trong DFL.

Hiểu biết về cấu trúc bộ nhớ của các hệ điều hành khác nhau là cần thiết vì việc phân tích kết xuất bộ nhớ đòi hỏi các kỹ năng kỹ thuật và kỹ năng rất cao, do đó, chỉ có một người kiểm tra có trình độ mới thực hiện được công việc. Phần mềm đặc biệt là cần thiết để phân tích kết xuất bộ nhớ, ví dụ như Volatility và Rekall, được công khai miễn phí trên Internet.

Các dữ liệu điển hình có thể được trích xuất từ các bãi chứa bộ nhớ bao gồm:

- Các tiến trình đang chạy, kể cả bộ nhớ của chúng
- Thông tin quy trình (ví dụ: xử lý)
- Khóa mã hóa
- Các tệp đã mở
- Tên người dùng, mật khẩu
- Tài liệu chưa được lưu

5.3.1.3 Ảo hóa

Một bức tranh đáng giá cả ngàn lời nói - điều này đặc biệt đúng với ảo hóa. Sử dụng ảo hóa, người kiểm tra có thể xem môi trường hệ điều hành của một vụ án giống như nghi phạm đã thấy. Tìm kiếm bằng chứng từ bên trong một máy ảo đôi khi có thể nhanh hơn và dễ dàng hơn so với việc gắn lại các dấu vết dữ liệu từ tệp hình ảnh. Một ví dụ là xem phần mềm chơi game giả.

Khi gắn hình ảnh, nó phải được gắn với các tham số được bảo vệ ghi hoặc chỉ đọc với bộ đệm ghi, cho phép hệ điều hành ảo ghi tệp nhật ký, mà không ảnh hưởng đến tính toàn vẹn của tệp hình ảnh.

Một số hệ điều hành từ chối bắt đầu trong môi trường ảo. Điều này thường có thể được giải quyết bằng cách thay thế một số trình điều khiển bằng cách định cấu hình cài đặt hệ thống, sử dụng phần mềm như OpenGates và OpenJobs. Nếu hệ điều hành ảo yêu cầu nhập mật khẩu, Examiner cần phải bẻ khóa mật khẩu hoặc xóa nó.

5.3.1.4 Quy trình xử lý dữ liệu hàng loạt

Một số trường hợp liên quan đến rất nhiều máy tính với khối lượng dữ liệu lớn. Để thực hiện điều tra, một chiến lược cần phải được thực hiện để xúc tiến công việc. Một cách để làm điều này là tách nhiệm vụ phân tích pháp lý khỏi nhiệm vụ phân tích nội dung. Người kiểm tra tập trung vào các nhiệm vụ phân tích pháp lý như phục hồi, phân tích cú pháp, lắp đặt và xử lý tang vật, trong khi điều tra viên có kinh nghiệm sẽ thực hiện phân tích nội dung.

Một quy trình thích hợp để xử lý và xem các tệp được trích xuất có thể cần được phát triển và triển khai giữa người kiểm tra và người điều tra để đảm bảo quá trình hoạt động trơn tru.

Một phương pháp khác để xử lý dữ liệu hàng loạt là bằng cách tiến hành xử lý, được giải thích trong phần 5.2.2 trong tài liệu này.

5.3.1.5 Hỗ trợ trực quan

Để hỗ trợ các hiểu biết về dữ liệu và luồng phức tạp, hỗ trợ trực quan có thể hữu ích. Một số ví dụ về các công cụ hỗ trợ như vậy là:

Dòng thời gian (Timelines)	Chúng có thể được sử dụng để hiển thị hành vi người dùng; khi nghi phạm đăng nhập hoặc kết nối với một phương tiện nhất định, khi anh ta kết nối với một bộ định tuyến không dây hoặc khi anh ta xem một trang web cụ thể.
Sơ đồ mối quan hệ	Đưa ra câu trả lời cho các câu hỏi như: Ai đã gặp ai; tại thời điểm nào; dùng phương tiện nào? Thông tin nào đã được gửi / nhận? Ai biết ai? Ai là nghi phạm chính phối hợp với người khác?

Sơ đồ dòng tiền	Giúp hiểu được tại thời điểm nào một số tiền đã được gửi, qua kênh nào và bởi cá nhân nào.
Sơ đồ truyền thông	Tương tự như một sơ đồ mối quan hệ, nhưng những điều này không nhất thiết liên quan đến con người. Nó có thể hiển thị tần suất một địa chỉ IP nhất định tấn công một số máy chủ từ các quốc gia khác nhau.

Bảng 10. Phương pháp hỗ trợ thị giác

Biểu diễn đồ họa giúp dễ hiểu hơn về mối tương quan giữa các dữ liệu. Chúng cũng cho phép điều tra viên tìm các mối quan hệ mới không được ghi nhận trước đây. Thông thường, cơ sở cho các sơ đồ như vậy là các dữ liệu thô được lưu trữ một cách có cấu trúc, ví dụ ở định dạng CSV, TSV hoặc XML. Những tập tin này được tải vào phần mềm phân tích.

Ví dụ, trên Linux, các lệnh đơn giản như awk, sort và uniq được sử dụng cùng với Graphviz hoặc dấu chấm, có thể giúp vẽ biểu diễn đồ họa.

5.3.2 Phân tích các thiết bị di động

Thiết bị di động chứa các bản ghi và nhật ký liên lạc, cùng với thời gian và ngày của các liên lạc cụ thể. Ngoài ra, thiết bị di động cũng có thể chứa các tệp phương tiện và vị trí GPS.

5.3.2.1 Danh mục dấu vết kỹ thuật số

Dấu vết kỹ thuật số được tìm thấy trên thiết bị di động có thể được chia thành ba nhóm đặc biệt: dữ liệu truyền thông, tệp phương tiện và dữ liệu khác. Dữ liệu truyền thông có thể bao gồm các bản ghi cuộc gọi, tin nhắn SMS và các tin nhắn dịch vụ khác. Các tệp phương tiện, như với máy tính, có thể chứa thông tin vượt quá những gì được mô tả bởi tệp. Ví dụ, siêu dữ liệu trên các tệp phương tiện được chụp trong điện thoại di động có khả năng chứa thẻ địa lý hoặc dữ liệu nhận dạng và vị trí hữu ích khác được nhúng trong chính tệp

5.3.2.2 Quy trình cho các dấu vết khác nhau

Các phần sau đây giải thích các loại dữ liệu có thể được trích xuất từ thiết bị di động.

A. Lịch sử cuộc gọi

Lịch sử cuộc gọi cung cấp cái nhìn sâu sắc về hoạt động cuộc gọi của chủ sở hữu trước khi mua thiết bị Điện thoại thông minh. Điều tra viên có thể thấy các cuộc gọi đến, đi và cuộc gọi nhỡ bao gồm cả thời gian và thời lượng. Điều này có thể giúp điều tra viên pháp y đưa ra kết luận gián tiếp về các hoạt động bị nghi ngờ, do đó hỗ trợ DFL đẩy nhanh quá trình phân tích bằng cách đưa ra yêu cầu vụ án một cách ngắn gọn và rõ ràng.

B. Danh sách liên hệ

Danh sách liên hệ không chỉ cung cấp tên liên lạc, mà còn cung cấp cả số nhà, số điện thoại di động và số dành cho công việc. Các loại thông tin khác như tiêu đề liên hệ, công ty, địa chỉ và e-mail liên quan cũng có thể được trích xuất từ danh sách liên lạc. Một số thiết bị điện thoại thông minh lưu trữ cả hình ảnh của một số liên lạc trong danh sách liên lạc, có thể giúp xác định một cá nhân nào đó. Thông tin được lưu trữ trong danh sách liên lạc cung cấp cho điều tra viên các mối quan hệ xã hội và công việc của chủ sở hữu thiết bị điện thoại thông minh. Bên cạnh đó, nhiều người lưu trữ các loại thông tin tài khoản khác nhau và mật khẩu trong danh sách liên lạc

C. E-mail và tin nhắn

Không giống như lịch sử cuộc gọi và danh sách liên lạc, nơi cung cấp thông tin gián tiếp, tin nhắn văn bản và e-mail cung cấp thông tin rõ ràng có thể được sử dụng làm bằng chứng trước tòa. Điều này là do chúng chứa văn bản chính xác hoạt động gửi và nhận thông tin củangười dùng thiết bị.

D. Tệp tin đa phương tiện (video, audio, hình ảnh)

Các file phương tiện như hình ảnh, video và âm thanh có thể được sử dụng làm bằng chứng kỹ thuật số hữu ích tại tòa án. Nhiều thiết bị điện thoại thông minh như iPhone nhúng tọa độ GPS của vị trí vào siêu dữ liệu được gọi là Định dạng tệp có thể trao đổi (EXIF) của hình ảnh. Các thông tin khác được nhúng trong dữ liệu EXIF có thể bao gồm thương hiệu điện thoại thông minh, ngày và giờ chụp ảnh, cũng như phần mềm được sử dụng để sửa đổi hình ảnh (nếu có). Điều này cung cấp cho điều tra viên cái nhìn sâu sắc hơn về các hoạt động của chủ sở hữu điện thoại thông minh.

E. Lịch sử duyệt web và từ khóa tìm kiếm

Lịch sử duyệt web và từ khóa tìm kiếm được thực hiện trong thiết bị điện thoại thông minh cung cấp cho điều tra viên hiểu biết chung về các hoạt động

trên Internet của chủ sở hữu. Điều tra viên sẽ khám phá các loại trang web mà chủ sở hữu đã truy cập và trong một chừng mực nào đó, như các trang web yêu thích của người dùng.

F. Nhật ký trò chuyện và các ứng dụng nhắn tin

G. Nhật ký trò chuyện và Ứng dụng nhắn tin

Có một số ứng dụng trò chuyện và ứng dụng nhắn tin có sẵn. Ví dụ bao gồm Whatsapp, Telegram, Skype, Line, Weebo, WeChat, QQ, Windows Live Messenger, Google Talk và BlackBerry Messenger. Người dùng các ứng dụng này thường chọn lưu nhật ký trò chuyện. Nhật ký trò chuyện có thể được sử dụng làm bằng chứng kỹ thuật số tại tòa án về những gì chủ sở hữu đã truyền đạt cho người khác. Một số nhật ký trò chuyện được sao lưu trên cloud hoặc bộ nhớ cục bộ như máy tính, do đó, phân tích máy tính có thể rất hữu ích để thu được nhiều dữ liệu hơn.

Ứng dụng nhắn tin cũng có thể cung cấp dịch vụ VoIP (Thoại qua IP). Điều này cho phép chủ sở hữu điện thoại thông minh giao tiếp với nhiều người bằng giao thức IP mà không để lại một bản ghi trong lịch sử cuộc gọi của thiết bị. Nghi phạm có thể sử dụng phần mềm này để liên lạc với đồng phạm hoặc kể cả với nạn nhân. Ví dụ, trong các vụ lạm dụng trẻ em, tên tội phạm có thể liên lạc với trẻ bằng các ứng dụng nhắn tin này.

H. Tài khoản mạng xã hội

Các tài khoản mạng xã hội, chẳng hạn như Instagram, Facebook, Twitter và Tumblr lưu thông tin đăng nhập của người dùng trong chính thiết bị của họ. Bằng cách lưu trữ thông tin đăng nhập cục bộ, người dùng không phải đăng nhập mỗi lần họ muốn truy cập các trang web này. Các thông tin đăng nhập này có giá trị đối với người kiểm tra, vì chúng có thể được sử dụng để có quyền truy cập vào tài khoản phương tiện truyền thông xã hội bị nghi ngờ, cho phép trích xuất dữ liệu từ thiết bị.

Rất nhiều dữ liệu được lưu trữ trong các tài khoản mạng xã hội, danh sách liên lạc, tin nhắn giữa các cá nhân và nhóm, hình ảnh, video, hoạt động của người dung, danh sách này có thể xem là vô tận. Người kiểm tra cần yêu cầu được cung cấp một trường hợp rõ ràng để trích xuất dữ liệu chính xác và trình bày kết quả phân tích đầy đủ và chính xác trong các báo cáo pháp lý.

I. Lịch và Ghi chú

Lịch đưa ra các hoạt động theo kế hoạch trong quá khứ, hiện tại và tương lai của chủ sở hữu điện thoại thông minh. Lịch có thể được sử dụng để liên kết chủ sở hữu của điện thoại thông minh với các địa điểm và thời gian cụ thể để tìm kiếm các nhân chứng có thể. Chủ sở hữu của điện thoại thông minh cũng có thể đã lưu các ghi chú có thông tin có giá trị có thể được trình bày làm bằng chứng trước tòa.

J. Kết nối (Mạng điện thoại, Wifi, Bluetooth)

Những kết nối này sẽ cung cấp cho điều tra viên một cái nhìn tổng quan về các hoạt động mạng được thực hiện bởi thiết bị điện thoại thông minh chủ sở hữu. Mạng di động sẽ đưa ra hình ảnh về quốc gia hoặc khu vực mà chủ sở hữu đã chuyển vùng. Wi-Fi sẽ đưa ra hình ảnh về Mạng cục bộ (LAN) mà điện thoại thông minh đã kết nối. Kết nối Bluetooth sẽ cung cấp cho Điều tra viên thông tin về danh tính của các thiết bị được kết nối với chủ sở hữu của điện thoại thông minh.

K. Bản đồ (Vị trí, trợ giúp, favorites)

Điều này sẽ cung cấp cho Điều tra viên một cái nhìn theo phương diện địa lý về các hoạt động của chủ sở hữu, có thể được sử dụng làm bằng chứng tiềm năng tại tòa án. Các tọa độ GPS khi người dùng chuyển động cũng có thể được ghi lại và phân tích, chẳng hạn như trong trường hợp các ứng dụng cung cấp chỉ đường được sử dụng. Chúng bao gồm Google Maps, Bings Maps và Apple Maps.

L. Phần mềm (xử lý Tài liệu, PDF, …)

Hầu hết các điện thoại thông minh cung cấp tính năng tạo và chỉnh sửa tài liệu. Phần mềm xử lý tài liệu, như Word To Go và Sheet To Go, có thể chứa bằng chứng tiềm năng liên quan đến vụ án.

5.4 Trình bày

Giai đoạn trình bày đòi hỏi phải kết hợp các chứng cứ theo một cách có thể trình bày được và dễ hiểu cho các bên liên quan. Khi giai đoạn phân tích được hoàn thành, người kiểm tra cần đưa những phát hiện và kết quả vào một báo cáo điều tra. Người kiểm tra nên minh họa và dịch các bối cảnh kỹ thuật phức tạp thành các sự kiện mà các thẩm phán, công tố viên và các bên liên quan khác có thể dễ dàng hiểu được. Họ cũng

có thể được yêu cầu giải thích những chứ cứ đó, và bày tỏ ý kiến về ý nghĩa của chúng. Trong một số trường hợp khi một số lượng lớn các chứng cứ được phân tích, sẽ rất khó để người kiểm tra trình bày kết quả cho đội điều tra. Nên sử dụng một phần mềm phân tích, để tạo điều kiện phù hợp với bằng chứng kỹ thuật số với dữ liệu khác từ các cuộc điều tra. Loại công cụ này cũng có thể được sử dụng để lập chỉ mục và tìm kiếm tất cả các bằng chứng, cung cấp cho nhóm điều tra một cái nhìn tổng quan về vụ án.

5.4.1 Quyền chấp nhận chứng cứ điện tử

Nói chung, người kiểm tra cần xem xét các tiêu chí sau khi đánh giá bằng chứng điện tử:

Tính xác thực	Bằng chứng phải dựa theo sự thật theo cách không thể tranh cãi và là đại diện cho trạng thái ban đầu của nó.
Hoàn thành	Việc phân tích, hoặc bất kỳ ý kiến dựa trên bằng chứng phải nói lên toàn bộ sự việc và không được điều chỉnh để phù hợp hơn hoặc theo quan điểm cá nhân.
Độ tin cậy	Cách thu thập bằng chứng và công việc xử lý sau đó không có gì gây nghi ngờ về tính xác thực hoặc tính tin cậy của nó.
Tính thuyết phục	Bằng chứng phải có sức thuyết phục đối với các sự việc mà nó thể hiện và phải có khả năng thuyết phục các bên liên quan về sự thật trước tòa.
Tương xứng	Các phương pháp được sử dụng để thu thập bằng chứng phải công bằng và tương xứng với lợi ích của công lý: định kiến (nghĩa là mức độ xâm nhập hoặc ép buộc) gây ra đối với quyền của bất kỳ bên nào không nên vượt quá giá trị bằng chứng của chứng cứ (nghĩa là giá trị làm bằng chứng).

Bảng 11. Tiêu chí chung cho sự chấp nhận chứng cứ điện tử

5.4.2 Viết báo cáo

Một báo cáo điều tra phải được viết bằng ngôn ngữ rõ ràng và dễ hiểu. Kết quả phải được tóm tắt chính xác và nó cũng phải cung cấp câu trả lời ngắn gọn cho yêu cầu trường hợp, được cung cấp bởi người yêu cầu.

Chúng tôi đề nghị rằng tất cả các chi tiết kỹ thuật được liệt kê trong phần phụ lục, thay vì đưa vào với nội dung chính. Điều này là để tạo điều kiện thuận lợi khi đọc báo cáo. Người kiểm tra cũng không được cung cấp một tuyên bố không thể chứng minh được. Ví dụ: "Nghi phạm đã thay đổi Tập tin A. Một câu thích hợp sẽ là Tập tin A được tìm thấy trong Máy tính B đã bị thay đổi"

Do sự phức tạp của vụ án, đôi khi rất khó để người kiểm tra thể hiện một số thông tin trong báo cáo. Việc sử dụng các phương tiện trực quan và biểu diễn trực quan như hoạt hình, slide, hình ảnh và trình diễn trực tiếp là những phương pháp tốt để tạo việc báo cáo dễ hiểu hơn.

5.4.3 Nhân chứng chuyên gia

Trong một số khu vực pháp lý, một báo cáo điều tra được đệ trình là đủ, thay cho người kiểm tra tham dự phiên tòa. Tuy nhiên, trong các khu vực pháp lý khác, người kiểm tra được yêu cầu tham dự phiên tòa và trình bày lời khai chuyên môn của mình liên quan đến vụ án.

Một nhân chứng chuyên gia là một người mà nhờ vào giáo dục, đào tạo, kỹ năng hoặc kinh nghiệm, có chuyên môn và kiến thức chuyên ngành vượt xa người bình thường. Kiến thức của nhân chứng này là đủ để những người khác có thể chính thức và hợp pháp dựa trên ý kiến chuyên môn (khoa học, kỹ thuật hoặc chuyên môn khác) của người đó về bằng chứng, hoặc thực tế trong phạm vi chuyên môn của người đó, được gọi là ý kiến chuyên gia.

Trong một số khu vực pháp lý, chuyên gia được quyết định trong từng trường hợp bởi thẩm phán xét xử và người đó chỉ là một chuyên gia trong vụ án đó. Trong các khu vực pháp lý khác, tư cách chuyên gia được chỉ định bởi tổ chức pháp lý và người chịu trách nhiệm cho bất kỳ trường hợp nào trong chuyên môn của mình.

Các quyền và nghĩa vụ của một nhân chứng chuyên gia là khác nhau giữa các quốc gia. Điều quan trọng là người kiểm tra phải làm quen với luật pháp, thủ tục tòa án, vai trò của họ và quyền và nghĩa vụ của họ trong vai trò đó.