I. ĐỀ CƯƠNG CHI TIẾT

Chương 1. Tổng quan về điều tra số

1.1. Khái niệm cơ bản

Điều tra máy tính

Điều tra máy tính là một phần của điều tra kỹ thuật số xử lý tội phạm trên các thiết bị điện toán như mạng, máy tính và phương tiện lưu trữ kỹ thuật số. Nó đề cập đến một tập hợp các thủ tục và kỹ thuật phương pháp để xác định, thu thập, bảo quản, trích xuất, giải thích, lập tài liệu và trình bày bằng chứng từ thiết bị máy tính sao cho bằng chứng được phát hiện có thể chấp nhận được trong quá trình tố tụng pháp lý và/hoặc hành chính tại tòa án.

Tóm lại, điều tra máy tính giải quyết quá trình tìm kiếm bằng chứng có thể chấp nhận được liên quan đến tội phạm kỹ thuật số để tìm ra thủ phạm và bắt đầu hành động pháp lý chống lại họ.

Mục tiêu

- Xác định, thu thập và lưu giữ bằng chứng về tội phạm mạng
- Theo dõi và truy tố thủ phạm trước tòa án
- Diễn giải, lập tài liệu và trình bày bằng chứng sao cho có thể chấp nhận được trong quá trình truy tố
- Ước tính tác động tiềm ẩn của hoạt động độc hại đối với nạn nhân và đánh giá ý định của thủ phạm
- Tìm lỗ hổng và sơ hở bảo mật giúp kẻ tấn công
- Hiểu các kỹ thuật và phương pháp được sử dụng bởi những kẻ tấn công để tránh bị truy tố và vượt qua chúng
- Khôi phục các tệp đã xóa, tệp ẩn và dữ liệu tạm thời có thể được sử dụng làm bằng chứng
- Thực hiện ứng phó sự cố (IR) để ngăn chặn tổn thất thêm về tài sản trí tuệ, tài chính và danh tiếng trong một cuộc tấn công
- Biết luật của các khu vực và khu vực khác nhau, vì tội phạm kỹ thuật số phổ biến và từ xa
- Biết quy trình xử lý nhiều nền tảng, loại dữ liệu và hệ điều hành
- Học cách xác định và sử dụng các công cụ thích hợp cho điều tra điều tra

Mục đích của điều tra máy tính

Sự gia tăng theo cấp số nhân về số lượng tội phạm mạng và các vụ kiện tụng dân sự liên quan đến các tổ chức lớn đã nhấn mạnh nhu cầu về điều tra máy tính. Việc các tổ chức sử dụng dịch vụ của cơ quan điều tra máy tính hoặc thuê một chuyên gia điều tra máy tính để giải quyết các vụ việc liên quan đến việc sử dụng máy tính và các công nghệ liên quan đã trở nên cần thiết. Những thiệt hại tài chính đáng kinh ngạc do tội phạm mạng gây ra cũng góp phần làm tăng sự quan tâm đến điều tra máy tính. Điều tra máy tính đóng một vai trò quan trọng trong việc theo dõi tội phạm mạng. Vai trò chính của điều tra máy tính như sau:

- Đảm bảo tính toàn vẹn tổng thể và sự tồn tại liên tục của hệ thống máy tính và cơ sở hạ tầng mạng của tổ chức
- Giúp tổ chức nắm bắt thông tin quan trọng nếu hệ thống máy tính hoặc mạng của họ bị xâm phạm. Bằng chứng điều tra cũng giúp truy tố thủ phạm của tội phạm mạng, nếu bị bắt.

- Trích xuất, xử lý và giải thích bằng chứng thực tế để chứng minh hành động của kẻ tấn công và tội lỗi hoặc sự vô tội của họ trước tòa
- Theo dõi hiệu quả thủ phạm/những kẻ khủng bố từ các nơi khác nhau trên thế giới. Những kẻ khủng bố sử dụng Internet làm phương tiện liên lạc có thể bị theo dõi và kế hoạch của chúng có thể bị phát hiện. Địa chỉ IP rất quan trọng để tìm ra vị trí địa lý của những kẻ khủng bố.
- Tiết kiệm tiền bạc và thời gian quý báu của tổ chức. Nhiều nhà quản lý phân bổ một phần lớn ngân sách CNTT của họ cho bảo mật mạng và máy tính.
- Theo dõi các trường hợp phức tạp như gửi thư rác email và các hoạt động bất chính khác, v.v.

1.2. Quy trình thực hiện điều tra số

- Ghi lại hiện trường vụ án

  Việc ghi lại hiện trường vụ án điện tử là cần thiết để duy trì hồ sơ về tất cả các quy trình điều tra pháp y được áp dụng để xác định, trích xuất, phân tích và bảo quản bằng chứng. Các chi tiết nên bao gồm vị trí của tội phạm, trạng thái của hệ thống, thiết bị mạng được kết nối, phương tiện lưu trữ, điện thoại thông minh, điện thoại di động, PDA, truy cập Internet và mạng,

  Tài liệu này sẽ giúp theo dõi số sê-ri hoặc số nhận dạng khác của thiết bị được mua. Lập tài liệu cũng bao gồm chụp ảnh, quay video, ghi chú và phác thảo hiện trường để tái tạo lại sau này. Điều tra viên cần ghi lại các quy trình và hoạt động đang chạy trên màn hình hiển thị.

  Các điểm cần xem xét trong khi ghi lại hiện trường vụ án điện tử là:
  - Tài liệu về hiện trường tội phạm điện tử là một quá trình liên tục trong suốt quá trình điều tra để tạo ra một bản ghi vĩnh viễn về hiện trường.
  - Điều cần thiết là ghi lại đúng trang web và trạng thái của máy tính, phương tiện lưu trữ kỹ thuật số và các thiết bị điện tử khác.
  - Ghi lại hiện trường vụ án, lưu ý vị trí của con chuột và vị trí của các yếu tố được tìm thấy gần hệ thống.
  - Tài liệu chi tiết về bất kỳ thành phần điện tử khó tìm nào có liên quan.
  - Ghi lại trạng thái của hệ thống máy tính, phương tiện lưu trữ kỹ thuật số, thiết bị điện tử và bằng chứng có thể dự đoán được, bao gồm cả trạng thái nguồn của máy tính.
  - Chụp ảnh màn hình của màn hình máy tính và viết ghi chú về những gì bạn đã thấy trên màn hình.
  - Tài liệu về hiện trường vụ án phải bao gồm các chi tiết toàn diện tại thời điểm điều tra.

  Chụp ảnh hiện trường

  Hiện trường vụ án là nguồn chính của bằng chứng vật lý và việc chụp ảnh nó sẽ cung cấp cho các nhà điều tra tài liệu tham khảo trực quan để sử dụng trong tương lai. Các hình ảnh cũng sẽ giúp các nhà điều tra tái tạo hiện trường khi được yêu cầu.

Phác thảo hiện trường

Một bản phác thảo truyền đạt mối quan hệ đo lường giữa hiện trường vụ án và bằng chứng được tìm thấy. Bản phác thảo giải thích dữ liệu trong ảnh và video được ghi lại. Bản phác thảo cũng có thể miêu tả vị trí của máy ảnh cũng như của nhiếp ảnh gia.

Những điểm cần nhớ khi phác thảo cảnh là:

Sau khi đảm bảo hiện trường, chuyên gia pháp y máy tính (CEP) phải chuẩn bị một bản phác thảo hiện trường vụ án.

Bản phác thảo này phải bao gồm tất cả các chi tiết về các đối tượng có mặt và các vị trí trộm cắp trong khu vực văn phòng.

Đối với các bức ảnh, các chuyên gia pháp y chuẩn bị nhiều bản phác thảo về toàn cảnh, cho đến từng mảnh bằng chứng nhỏ nhất.

Sau khi tạo một bản phác thảo cảnh chính xác, CFP nên phác thảo mặt trên của bàn máy tính, chỉ định các mẩu bằng chứng.

Danh sách kiểm tra ghi chú

Điều tra hiện trường vụ án máy tính đòi hỏi nỗ lực đáng kể. Nỗ lực điều tra thay đổi tùy theo tình huống và nếu không có danh sách kiểm tra thì không thể nhớ tất cả các phát hiện của cuộc điều tra tội phạm máy tính. Điều tra viên sử dụng danh sách kiểm tra để ghi lại những phát hiện của quy trình tìm kiếm, thu thập và bảo quản bằng chứng kỹ thuật số tại hiện trường vụ án.

- Tìm kiếm và thu giữ

Lập kế hoạch Khám xét và Thu giữ điều tra trong phần này điều tra viên cần thiết kế một quy trình chiến lược để tiến hành quy trình khám xét và thu giữ sau khi phân tích hiện trường vụ án. Điều này sẽ giúp họ phân phối nhiệm vụ giữa các thành viên trong nhóm để hoàn thành việc thu giữ và cho phép nhóm sử dụng thời gian và công cụ theo cách được xác định rõ ràng.

Tìm kiếm sự đồng ý

Sự đồng ý, trong điều tra pháp y máy tính, đề cập đến quá trình xin phép chính thức từ chủ sở hữu của tổ chức nạn nhân hoặc cá nhân sở hữu hệ thống mục tiêu để thực hiện điều tra kỹ lưỡng. Sự đồng ý bằng văn bản từ cơ quan có thẩm quyền là đủ để bắt đầu quá trình điều tra và tìm kiếm .

Tại thời điểm đồng ý, các điều tra viên nên sử dụng các biểu ngữ được viết đúng cách với các chính sách sử dụng phù hợp và được chủ sở hữu hiện trường hoặc thiết bị chứng cứ ký tên. Nếu bạn có một biểu ngữ được diễn đạt chính xác và chính sách sử dụng phù hợp thông báo cho người dùng về các hoạt động giám sát và cách sử dụng thông tin thu thập được từ các hoạt động giám sát, thì gánh nặng về sự đồng ý sẽ đủ trong phần lớn các trường hợp.

Có những trường hợp khi người dùng có mặt và phải đồng ý với tư cách là người dùng phần cứng. Quản trị viên hệ thống không bao giờ được phép thực hiện các hoạt động giám sát ngẫu nhiên và không có kế hoạch.

Sử dụng các biểu mẫu thích hợp cho khu vực tài phán và mang theo các tài liệu này trong túi xách để bảo vệ khỏi mọi tổn hại hoặc thiệt hại. Các hoạt động giám sát liên quan đến sự đồng ý phải là một phần của thủ tục được ghi chép đầy đủ trong sự đồng ý có được.

Lấy chữ ký nhân chứng

Nhân chứng là người có mặt trong khi ký một văn bản hoặc thỏa thuận và làm chứng rằng các bên được đề cập trong thỏa thuận đã tự nguyện ký vào đó. Tùy thuộc vào luật pháp trong khu vực tài phán, thỏa thuận hoặc hợp đồng cần có chữ ký của một hoặc hai nhân chứng.

Thông thường, một chữ ký của nhân chứng là đủ nếu nhà phân tích pháp y hoặc nhân viên thực thi pháp luật đang thực hiện việc thu giữ. Khi trường hợp yêu cầu hai chữ ký của nhân chứng, hãy tìm hướng dẫn để xác định người ký thứ hai.

Chữ ký của nhân chứng xác nhận rằng thông tin trong mẫu chấp thuận và các tài liệu bằng văn bản khác là chính xác và cũng đã được giải thích và hiểu bởi bên kia, và họ đã tự nguyện đồng ý.

Bất cứ ai ký tên với tư cách là nhân chứng đều phải hiểu rõ vai trò của mình và có thể phải cung cấp lời khai của nhân chứng hoặc tham dự phiên tòa.

Nhận lệnh khám xét và thu giữ

Cán bộ điều tra hoặc người ứng phó đầu tiên phải thực hiện quá trình điều tra một cách hợp pháp; nếu không, một tòa án của pháp luật sẽ từ chối bằng chứng thu thập được. Người phản hồi đầu tiên cần có lệnh khám xét để khám xét và thu giữ các thiết bị điện tử. Lệnh khám xét là văn bản cho phép của cơ quan có liên quan đề cập đến các thiết bị điện tử mà nhân viên điều tra hoặc người phản ứng đầu tiên có thể khám xét và thu giữ. Tòa án cũng có thể ban hành lệnh khám xét. Một thẩm phán có thể ban hành lệnh khám xét nếu người trả lời đầu tiên đã thuyết phục được thẩm phán về bằng chứng phạm tội.

Lệnh khám xét thiết bị điện tử tập trung vào các vấn đề sau: Lệnh khám xét thiết bị lưu trữ điện tử Lệnh khám xét thiết bị lưu trữ điện tử cho phép người phản ứng đầu tiên tìm kiếm và thu giữ các thành phần máy tính của nạn nhân như:

- Phần cứng
- Phần mềm
- Thiết bị lưu trư
- Tài liệu

Tìm kiếm không có lệnh

Toà án đã cho phép các điều tra viên tiến hành khám xét mà không cần lệnh, nhưng trong một số trường hợp nhất định, chẳng hạn như khi việc chậm trễ trong việc xin lệnh có thể dẫn đến việc tiêu hủy hoặc thao túng bằng chứng và cản trở quá trình điều tra. Các tuyên bố sau đây của các tòa án Hoa Kỳ khác nhau đã tạo tiền lệ cho việc khám xét mà không có lệnh:

“Khi việc tiêu hủy bằng chứng sắp xảy ra, việc thu giữ bằng chứng đó mà không có lệnh bắt giữ là hợp lý nếu có lý do hợp lý để tin rằng vật bị thu giữ là bằng chứng của hoạt động tội phạm.” Hoa Kỳ kiện David, 756 F. Supp. 1385, 1392 (D. Nev. 1991).

Các đại lý có thể khám xét một địa điểm hoặc đồ vật mà không cần lệnh hoặc nguyên nhân có thể xảy ra, nếu một người có thẩm quyền đã đồng ý. Schneckloth kiện Bustamonte, 412 U.S. 218, 219 (1973).

Tìm kiếm ban đầu của hiện trường

Khi đội pháp y đã đến hiện trường và dỡ bỏ thiết bị của họ, họ sẽ tiếp tục đến hiện trường vụ việc và cố gắng xác định bất kỳ bằng chứng nào. Thủ phạm có thể sử dụng chương trình tự hủy hoặc định dạng lại phương tiện lưu trữ khi nhóm đến. Để tính đến những khả năng như vậy, hãy kéo dây nguồn được kết nối với hệ thống xử lý trung tâm ngay lập tức.

Xác định, thu thập, dán nhãn, lưu giữ và bảo vệ tất cả bằng chứng kỹ thuật số tại hiện trường.

Cô lập hệ thống máy tính (máy trạm, độc lập hoặc máy chủ mạng) hoặc các dạng phương tiện khác để bằng chứng kỹ thuật số không bị mất.

Trong nhiều trường hợp, hệ thống máy tính thường xuyên tạo bản sao lưu. Mặc dù kẻ tấn công có thể xóa các tệp khỏi phương tiện lưu trữ chính nhưng những tệp này vẫn có thể tồn tại trên phương tiện lưu trữ dự phòng.

Bao gồm nhật ký tìm kiếm và thu giữ bằng chứng có chứa các mô tả ngắn gọn về tất cả các máy tính, thiết bị hoặc phương tiện được đặt trong quá trình tìm kiếm bằng chứng.

Ghi lại các địa điểm trên bản phác thảo hiện trường vụ án.

Chụp ảnh và phác thảo hiện trường vụ án, cùng với bản tường trình chi tiết về tất cả các bằng chứng máy tính.

Ghi lại mọi thứ tại hiện trường vụ án và vị trí tìm thấy bằng chứng.

Đóng gói và vận chuyển bằng chứng kỹ thuật số một cách an toàn.

Đối phó với máy tính đang bật

Bằng chứng điện tử có bản chất linh hoạt và dễ bị hỏng trong quá trình thu thập, bảo quản và phân tích. Do đó, hãy hành động thận trọng để ngăn ngừa thiệt hại.

- Nếu máy tính được BẬT và màn hình có thể xem được, hãy chụp ảnh màn hình và ghi lại các chương trình đang chạy, các tệp đang mở hoặc dữ liệu có giá trị chứng minh.
- Nếu máy tính đang BẬT và màn hình hiển thị trình bảo vệ màn hình, hãy di chuyển chuột từ từ mà không nhấn bất kỳ nút chuột nào, sau đó chụp ảnh màn hình và ghi lại các chương trình.
- Nếu một máy tính xách tay thức dậy, hãy ghi lại thời gian và ngày mà điều này xảy ra, chụp ảnh màn hình và ghi lại tất cả các chương trình đang chạy.
- Kéo dây nguồn từ phía sau máy tính ngay lập tức trong các trường hợp sau:
    - Có dấu hiệu trên màn hình cho biết dữ liệu đang bị ghi đè hoặc xóa
    - Các quy trình phá hủy được quan sát thấy đang chạy để xóa dữ liệu khỏi các thiết bị lưu trữ dữ liệu
    - o Màn hình máy tính hiển thị môi trường Microsoft Windows điển hình; trong trường hợp này, việc ngắt kết nối nguồn điện sẽ vẫn lưu giữ nhiều

thông tin có giá trị như thời gian đăng nhập lần cuối của người dùng, các tài liệu và lệnh được sử dụng gần đây, v.v.

- Không ngắt nguồn điện nếu:
  - Dữ liệu có giá trị chứng cứ hiển thị trên màn hình máy tính
  - Có các chương trình hoặc tệp đang hoạt động được sử dụng như phòng trò chuyện, tệp văn bản đang mở, tài liệu tài chính, tin nhắn nhanh, v.v.
    - Chụp ảnh và ghi lại toàn bộ thông tin trên màn hình
    - Thực hiện quy trình thu thập và bảo quản dữ liệu biến động
- Sau khi thu thập dữ liệu biến động, hãy rút phích cắm từ phía sau máy tính để ngắt kết nối nguồn điện.
- Trong trường hợp máy tính xách tay, hãy tháo pin và rút dây nguồn ra khỏi ổ cắm trên tường.
- Nếu không thể tháo pin ra, hãy nhấn công tắc nguồn trong 30 giây để tắt nguồn.

Xử lý máy tính bị tắt nguồn

- Tại thời điểm điều tra này, không thay đổi trạng thái của bất kỳ thiết bị hoặc thiết bị điện tử nào:
  - Nếu nó TẮT, hãy để nó TẮT
- Nếu một màn hình bị TẮT và màn hình trống:
  - BẬT màn hình, di chuyển chuột nhẹ, quan sát các thay đổi từ màn hình trống sang màn hình khác và lưu ý các thay đổi.
  - Chụp ảnh màn hình.
- Nếu màn hình được BẬT và màn hình trống:
  - Di chuyển chuột nhẹ
  - Nếu màn hình không thay đổi, không thực hiện bất kỳ thao tác gõ phím nào khác.
  - Chụp ảnh màn hình.

Xử lý máy tính nối mạng

Nếu máy tính của nạn nhân có kết nối Internet, người phản hồi đầu tiên phải tuân theo quy trình sau để bảo vệ bằng chứng:

- Rút cáp mạng ra khỏi bộ định tuyến và modem vì kết nối internet có thể khiến nó dễ bị tấn công hơn.
- Không sử dụng máy tính để tìm kiếm bằng chứng vì nó có thể thay đổi hoặc thay đổi tính toàn vẹn của bằng chứng hiện có.
- Chụp ảnh tất cả các thiết bị được kết nối với máy tính của nạn nhân, đặc biệt là bộ định tuyến và modem, đồng thời chụp ảnh máy tính từ các góc độ khác nhau. Nếu có bất kỳ thiết bị nào gần máy tính nạn nhân như máy in hoặc máy quét, hãy chụp ảnh các thiết bị đó.
- Nếu máy tính TẮT, hãy để nó TẮT.
- Nếu máy tính đang BẬT, hãy chụp ảnh màn hình.
- Nếu máy tính đang BẬT và màn hình trống, hãy di chuyển chuột từ từ và chụp ảnh màn hình.

- Rút phích cắm của tất cả các dây và thiết bị được kết nối với máy tính và dán nhãn cho chúng để nhận dạng sau này.
- Rút dây nguồn chính ra khỏi ổ cắm trên tường.
- Đóng gói bằng chứng điện tử đã thu thập đúng cách và đặt vào túi không có tĩnh điện.
- Để bằng chứng đã thu thập tránh xa nam châm, nhiệt độ cao, máy phát sóng vô tuyến và các yếu tố khác có thể làm hỏng tính toàn vẹn của chứng cứ.
- chứng cớ.
- Ghi lại tất cả các bước liên quan đến việc tìm kiếm và thu giữ máy tính của nạn nhân để điều tra sau này.

Xử lý tệp mở và tệp khởi động

Khi tội phạm máy tính xảy ra do phần mềm độc hại tấn công, phần mềm độc hại sẽ tạo ra một số tệp. Để chạy mã độc, phần mềm độc hại tạo một số tệp trong thư mục khởi động cho hệ điều hành Windows và trong thư mục tệp rc.local cho hệ điều hành Linux. Những người phản hồi đầu tiên có thể nhận được thông tin quan trọng từ các tệp này. Sử dụng lệnh Is cho hệ điều hành Linux.

Quy trình tắt hệ điều hành

Những người phản hồi đầu tiên phải đưa ra quyết định quan trọng tại thời điểm tắt hệ thống máy tính vì điều quan trọng là phải tắt hệ điều hành theo cách thích hợp để nó không làm hỏng tính toàn vẹn của tệp. Trong hầu hết các trường hợp, loại hệ điều hành là chìa khóa để đưa ra quyết định này. Các hệ điều hành khác nhau có quy trình tắt máy khác nhau. Một số hệ điều hành được tắt trực tiếp bằng cách rút dây nguồn ra khỏi ổ cắm trên tường mà không làm mất bất kỳ tệp nào. Tuy nhiên, đối với một số hệ điều hành, những người phản hồi đầu tiên phải tuân theo quy trình tắt máy được xác định trước; nếu không, dữ liệu có thể bị mất hoặc ổ đĩa cứng có thể bị hỏng.

Người phản hồi đầu tiên phải tuân theo các quy trình sau để tắt hệ điều hành:

Hệ điều hành Windows 7, Windows XP, Windows Vista, Windows Server 2008, Windows Server 2003:

- Chụp ảnh màn hình
- Nếu chương trình nào đang chạy, hãy giải thích ngắn gọn
- Rút dây nguồn ra khỏi ổ cắm trên tường

Hệ điều hành MAC OS X:

- Ghi lại thời gian từ thanh menu
- Nhấp vào Tắt máy đặc biệt
- Rút dây nguồn ra khỏi ổ cắm trên tường
- Bảo quản bằng chứng điện tử

Những điểm cần nhớ trong khi bảo quản bằng chứng điện tử là:

• Ghi lại các hành động và thay đổi mà bạn quan sát được trên màn hình, hệ thống, máy in hoặc các thiết bị điện tử khác.

• Xác minh rằng màn hình đang BẬT, TẮT hoặc ở chế độ ngủ.

• Tháo cáp nguồn, tùy thuộc vào trạng thái nguồn của máy tính, tức là BẬT, TẮT hoặc ở chế độ ngủ.
• Không BẬT máy tính nếu nó ở trạng thái TẮT.
• Chụp ảnh màn hình điều khiển nếu máy tính đang ở trạng thái BẬT.
• Kiểm tra các kết nối của modem điện thoại, cáp, ISDN và DSL.
• Rút phích cắm điện khỏi bộ định tuyến hoặc modem.
• Loại bỏ bất kỳ đĩa di động nào có sẵn tại hiện trường để bảo vệ bằng chứng tiềm năng
Giữ băng trên các khe ổ đĩa và đầu nối nguồn.
• Chụp ảnh các kết nối giữa hệ thống máy tính và các dây cáp liên quan và dán nhãn riêng cho chúng.
• Dán nhãn mọi đầu nối và cáp được kết nối với các thiết bị ngoại vi.

- Bảo quản bằng chứng
  Việc xử lý và bảo quản bằng chứng là một số khía cạnh quan trọng nhất của điều tra pháp y kỹ thuật số. Các điều tra viên nên thực hiện tất cả các bước cần thiết để đảm bảo rằng bằng chứng vẫn ở nguyên trạng, chính xác như được tìm thấy tại hiện trường vụ án.
  Tại thời điểm chuyển giao chứng cứ, cả bên gửi và bên nhận cần cung cấp thông tin về ngày giờ chuyển giao trong hồ sơ chuỗi hành trình sản phẩm.
  Những điều sau đây được yêu cầu để bảo vệ bằng chứng và ghi lại bằng chứng trong khi thu thập và vận chuyển:
    - Nhật ký của dự án để ghi lại các quan sát liên quan đến bằng chứng
    - Một thẻ để xác định duy nhất bất kỳ bằng chứng nào
    - Hồ sơ chuỗi hành trình sản phẩm
- Thu thập dữ liệu
  Thu thập dữ liệu
  Thu thập dữ liệu là việc sử dụng các phương pháp đã được thiết lập để trích xuất Thông tin lưu trữ điện tử (ESI) từ một máy tính hoặc phương tiện lưu trữ bị nghi ngờ nhằm hiểu rõ hơn về tội phạm hoặc sự cố. Thu thập dữ liệu pháp y là một quá trình chụp ảnh hoặc thu thập thông tin từ các phương tiện khác nhau theo các tiêu chuẩn nhất định để phân tích giá trị pháp y của nó. Sau đó, các nhà điều tra có thể xử lý pháp y và kiểm tra dữ liệu đã thu thập để trích xuất thông tin liên quan đến bất kỳ trường hợp hoặc sự cố cụ thể nào đồng thời bảo vệ tính toàn vẹn của dữ liệu. Đây là một trong những bước quan trọng nhất của pháp y kỹ thuật số vì bất kỳ việc thu thập không đúng cách nào cũng có thể làm thay đổi dữ liệu trong phương tiện bằng chứng và khiến dữ liệu đó không được chấp nhận trước tòa án.
  Các nhà điều tra pháp y sẽ có thể xác minh tính chính xác của dữ liệu thu được và toàn bộ quy trình phải được chấp nhận và tái sản xuất tại tòa án.
  Trước khi thu thập dữ liệu, điều tra viên cần đảm bảo rằng thiết bị lưu trữ của họ sạch sẽ về mặt pháp lý và sau đó bắt đầu bảo vệ ghi để bảo mật và bảo vệ bằng chứng gốc.
  Bằng chứng gốc KHÔNG BAO GIỜ được sử dụng để phân tích.
  Sao chép dữ liệu (Hình ảnh)
  Hãy nhớ những điểm sau trong khi sao chép dữ liệu:
    - Tạo một bản sao của dữ liệu đã thu thập để giữ nguyên bản gốc.

- Dữ liệu phải được sao chép từng chút một để thể hiện cùng một dữ liệu gốc.
- Tính toán giá trị băm của dữ liệu gốc và hình ảnh pháp y được tạo, sau đó kiểm tra xem kết quả có trùng khớp hay không để xác minh tính toàn vẹn của nó.
- Khi một bản sao của dữ liệu gốc được tạo và xác minh, điều tra viên có thể sử dụng bản sao đó để xử lý thêm.
- Sử dụng các công cụ phần cứng hoặc phần mềm theo tiêu chuẩn ngành hoặc được cấp phép để sao chép dữ liệu.

- Phân tích dữ liệu

  Phân tích dữ liệu đề cập đến quá trình kiểm tra, xác định, tách, chuyển đổi và mô hình hóa dữ liệu để cô lập thông tin hữu ích. Trong điều tra pháp y, phân tích dữ liệu giúp thu thập và kiểm tra dữ liệu để tìm ra mối liên quan của nó với vụ việc nhằm gửi kết quả cho cơ quan có thẩm quyền để kết luận và ra quyết định.

  Điều tra viên phải phân tích kỹ lưỡng các dữ liệu thu được để đưa ra kết luận liên quan đến vụ án. Ở đây, các kỹ thuật phân tích dữ liệu phụ thuộc vào phạm vi của trường hợp hoặc yêu cầu của khách hàng và loại bằng chứng.

  Giai đoạn này bao gồm những điều sau đây:
  - Phân tích nội dung tệp để sử dụng dữ liệu
  - Phân tích ngày và thời gian tạo và sửa đổi tệp
  - Tìm người dùng được liên kết với việc tạo tệp, truy cập và sửa đổi tệp
  - Xác định vị trí lưu trữ vật lý của tệp
  - Tạo dòng thời gian
  - Xác định nguyên nhân gốc rễ của vụ việc

  Xác định và phân loại dữ liệu theo thứ tự liên quan đến vụ án, sao cho dữ liệu phù hợp nhất đóng vai trò là bằng chứng quan trọng nhất đối với vụ án.

- Phân tích trường hợp

  Phân tích trường hợp

  Trong giai đoạn này, điều tra viên đánh giá tác động của sự cố đối với tổ chức, lý do và nguồn gốc của sự cố, các bước cần thiết để giải quyết sự cố, nhóm điều tra cần thiết để xử lý vụ việc, thủ tục điều tra và kết quả có thể có của quy trình pháp y. Phân tích trường hợp rất quan trọng để thực hiện một kế hoạch phù hợp trong việc xử lý trường hợp và đạt được kết quả mong muốn. Phân tích trường hợp có thể giúp các điều tra viên xác định các hành động trong tương lai, chẳng hạn như sau:
  - Kiểm tra xem có khả năng thực hiện theo các phương pháp điều tra khác để xác định vị trí lưu trữ từ xa, kiểm tra nhật ký dịch vụ mạng để tìm bất kỳ thông tin nào có giá trị chứng cứ, thu thập bằng chứng cụ thể theo từng trường hợp từ phương tiện truyền thông xã hội, gửi yêu cầu bảo quản đến dịch vụ Internet nhà cung cấp (ISP) hoặc nhận email.
  - Xác định mức độ liên quan của các yếu tố mạng khác nhau với hiện trường vụ án như thẻ tín dụng, giấy tờ séc, máy quét và máy ảnh.
  - Xem xét sự liên quan của các thành phần ngoại vi đối với cuộc điều tra; chẳng hạn, trong các trường hợp giả mạo hoặc gian lận, hãy xem xét các thiết bị không phải máy

tính như máy ép, giấy kiểm tra, máy quét và máy in hoặc trong các hoạt động bất chính khác, hãy xem xét máy ảnh kỹ thuật số.

- Báo cáo

  Viết báo cáo điều tra

  Viết báo cáo là một giai đoạn quan trọng trong quá trình điều tra pháp y, vì nó tóm tắt toàn bộ cuộc điều tra thành một báo cáo có thể đọc được để trình bày trước tòa án. Dựa trên tính chính xác và chắc chắn của báo cáo này, tòa án sẽ truy tố các nghi phạm. Báo cáo phải rõ ràng, ngắn gọn và được viết cho đối tượng thích hợp. Báo cáo phải bằng ngôn ngữ địa phương nếu cần thiết và không có bất kỳ biệt ngữ nào. Nó chỉ nên bao gồm các dữ liệu liên quan đến vụ án và bằng chứng. Mỗi tuyên bố nên có một tài liệu hoặc bằng chứng hỗ trợ.

  Báo cáo cũng nên đưa ra một tài khoản chi tiết về các sự cố bằng cách nhấn mạnh sự khác biệt trong lời khai của các nhân chứng. Nó phải là một tài liệu được viết tốt tập trung vào các tình huống của vụ việc, lời khai của các nhân chứng, ảnh chụp hiện trường vụ án, tài liệu tham khảo dẫn đến bằng chứng, bản vẽ sơ đồ của hệ thống máy tính và báo cáo phân tích pháp y mạng. Kết luận của báo cáo điều tra phải dựa trên sự thật chứ không phải ý kiến của điều tra viên. Một điều tra viên nên soạn thảo tài liệu bằng cách xem xét rằng nhóm bào chữa cũng sẽ xem xét kỹ lưỡng nó.

- Làm chứng với tư cách là Chuyên gia Nhân chứng

  Làm chứng tại Tòa án

  Một nhân chứng chuyên gia phải xem xét các yếu tố nhất định trong khi làm chứng tại tòa án. Họ nên thu thập đầy đủ thông tin về các thủ tục tiêu chuẩn trong quá trình xét xử và không bao giờ được chất vấn luật sư của mình về vấn đề này. Trước khi nhân chứng là chuyên gia làm chứng trước tòa, trước tiên, luật sư giới thiệu họ với tòa với sự tôn trọng cao và tiết lộ thông tin xác thực cũng như thành tích của chuyên gia để tạo uy tín với bồi thẩm đoàn. Tuy nhiên, luật sư đối lập có thể cố gắng thách thức hoặc đặt câu hỏi về uy tín của chuyên gia bằng cách tiết lộ thêm những thất bại trong quá khứ của chuyên gia liên quan đến vụ việc, nếu có.

  Luật sư hướng dẫn nhân chứng chuyên môn thông qua bằng chứng và giải thích vai trò của nhân chứng chuyên môn liên quan đến bằng chứng sao cho bồi thẩm đoàn, khán giả và luật sư đối lập có thể hiểu được. Một cuộc kiểm tra chéo của luật sư đối lập diễn ra sau đó, người này sau đó đặt câu hỏi cho nhân chứng chuyên gia về mô tả của họ về bằng chứng và các phương pháp họ đã tuân theo trong khi thu thập và phân tích bằng chứng.

1.3. Các loại hình điều tra số phổ biến

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) là 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 bản ghi (Register).

Điều tra bộ nhớ (Memory Forensics) là 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. Để xác định các hành vi đã xảy ra trong hệ thống, người ta thường 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.

Điều tra phương tiện lưu trữ (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.

Điều tra mạng (network forensic) là một nhánh của khoa học điều tra số liên quan đến việc giám sát và phân tích lưu lượng mạng máy tính nhằm phục vụ cho việc thu thập thông tin, chứng cứ pháp lý hay phát hiện các xâm nhập vào hệ thống máy tính này. Điều tra mạng có thể được thực hiện như một cuộc điều tra độc lập hoặc kết hợp với việc điều tra máy tính (computer forensics) – thường được sử dụng để phát hiện mối liên kết giữa các thiết bị kỹ thuật số hay tái tạo lại quy trình phạm tội.

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.

Điều tra thiết bị di động (Mobile device Forensics) 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.

1.4. Các nguyên tắc khi thực hiện điều tra

- Tính chính xác: Cung cấp thông tin chính xác và đáng tin cậy. Đảm bảo rằng dữ liệu được thu thập và xử lý một cách chính xác để tránh sai sót và nhầm lẫn.
- Quyền riêng tư: Bảo vệ quyền riêng tư của người tham gia. Đảm bảo rằng thông tin cá nhân không bị tiết lộ cho bất kỳ ai ngoại trừ những người có quyền truy cập.
- Đảm bảo an toàn thông tin: Bảo vệ dữ liệu và thông tin được thu thập khỏi sự truy cập trái phép, mất mát hoặc hủy hoại bằng cách sử dụng các biện pháp bảo mật phù hợp.
- Tự nguyện tham gia: Người tham gia cuộc điều tra số nên tham gia tự nguyện và có quyền từ chối tham gia hoặc rút lui bất cứ lúc nào mà không bị bất kỳ hình phạt hay hậu quả tiêu cực nào.

- Trung thực và minh bạch: Tạo điều kiện cho người tham gia thể hiện ý kiến và thông tin một cách trung thực và minh bạch. Cung cấp cho họ thông tin cần thiết về mục đích, phạm vi và phương pháp của cuộc điều tra.
- Bảo mật dữ liệu: Đảm bảo an toàn dữ liệu thu thập được trong suốt quá trình cuộc điều tra. Sử dụng các biện pháp bảo mật phù hợp để bảo vệ dữ liệu khỏi sự truy cập trái phép hoặc lạm dụng.
- Sự đa dạng và đại diện: Đảm bảo một mẫu đa dạng và đại diện của người tham gia trong cuộc điều tra để đảm bảo tính đại diện và khảo sát toàn diện.
- Tôn trọng và công bằng: Tôn trọng và đối xử công bằng với tất cả các người tham gia cuộc điều tra, không phân biệt đối xử dựa trên dân tộc, tôn giáo, giới tính, tuổi tác hoặc bất kỳ yếu tố nào khác.
- Phân tích và báo cáo chính xác: Phân tích dữ liệu thu thập được một cách chính xác và tổ chức thông tin thành báo cáo một cách minh bạch, cung cấp kết quả và phân tích rõ ràng.
- Tuân thủ quy định pháp luật: Thực hiện cuộc điều tra số theo các quy định và quyền hạn pháp lý liên quan, bao gồm việc bảo vệ quyền riêng tư và bảo mật thông tin cá nhân.

1.5. Kỹ thuật phòng chống anti-forensics

1. Mã hóa

Một trong những kỹ thuật chống pháp y phổ biến là mã hóa, là nghệ thuật nhúng thông tin bí mật và nhạy cảm vào bản mã (văn bản bị cắt xén). Các thuật toán mã hóa hiện đại được sử dụng để ngăn những con mắt không mong muốn truy cập vào văn bản, hình ảnh hoặc mã được che giấu. Những kẻ tấn công sử dụng mã hóa toàn bộ khối lượng và một tệp chính để che giấu các chiến dịch hoặc mã độc hại của chúng. Một khóa bí mật được sử dụng để niêm phong thông tin, sau đó được giải mã — giải mã bản mã trở lại văn bản thuần túy tại điểm đích.

Các nhà phân tích pháp y không thể giải mã các tệp độc hại nếu không có khóa bí mật được xác thực. Các tệp độc hại được mã hóa không được phát hiện trong nhiều công cụ và kỹ thuật sàng lọc bảo mật.

2. Trình đóng gói chương trình

Trình đóng gói chương trình chỉ là một trong nhiều kỹ thuật chống điều tra mà kẻ tấn công sử dụng để ẩn dữ liệu của họ khỏi bất kỳ phương pháp quét hoặc phát hiện nào. Giống như mật mã, các trình đóng gói trước tiên nén/mã hóa các tệp dữ liệu và các mã tệp thực thi khác. Các trình đóng gói chương trình ban đầu được sử dụng để nén kích thước của tệp và chương trình. Tuy nhiên, tin tặc bắt đầu sử dụng các trình đóng gói để ẩn tệp hoặc chương trình bị nhiễm nhằm xâm phạm bảo mật bằng cách tránh bị phát hiện thông qua các công cụ chống phần mềm độc hại hoặc phân tích bảo mật.

Một số trình đóng gói được sử dụng cho mục đích xấu là UPX, The Enigma Protector, MPRESS, v.v.

3. Ghi đè dữ liệu

Những kẻ tấn công sử dụng các chương trình ghi đè để phá vỡ các cuộc điều tra pháp y và giảm thiểu dấu vết kỹ thuật số. Còn được gọi là làm sạch dữ liệu hoặc xóa dữ liệu, xóa dữ liệu một cách an toàn là thủ thuật cũ mà những kẻ tấn công sử dụng. Ngày nay, nhiều công cụ có sẵn để ghi đè lên văn bản, siêu dữ liệu hoặc toàn bộ phương tiện quan trọng trên hệ thống lưu trữ, điều này cản trở nhiệm vụ của các nhà phân tích pháp y trong giai đoạn khôi phục. Kỹ thuật ghi đè dữ liệu gốc này giảm thiểu dấu chân kỹ thuật số của kẻ tấn công về dữ liệu sai và bị thay đổi. Dữ liệu ghi đè bao gồm:

Ghi đè tất cả dữ liệu gốc
Ghi đè lên các tập tin cá nhân
Ghi đè các tệp đã xóa trước đó và làm việc trên các tệp đó cho đến khi không còn dung lượng trống
4. Định tuyến hành tây
Định tuyến hành tây là một kỹ thuật được sử dụng để giao tiếp ẩn danh qua mạng nơi các thông báo được mã hóa theo cách phân lớp. Mã hóa lớp giống như một củ hành tây, do đó có tên này. Onion Router hoặc TOR được sử dụng để truy cập web ẩn danh, cung cấp cho tin tặc một tùy chọn tuyệt vời để truy cập web tối, ẩn dấu chân của chúng và khởi chạy các cuộc tấn công mạng. Onion Routing cho phép tin tặc che giấu các hoạt động internet, địa chỉ IP và việc sử dụng mạng của chúng.

Dữ liệu được truyền qua định tuyến củ hành đi qua nhiều nút mạng, mỗi nút được mã hóa theo lớp. Dữ liệu đến đích khi lớp mã hóa cuối cùng được chuyển qua. Các nhà điều tra pháp y sẽ đột phá thành công từng lớp từ nút đích đến nút thoát để xác định kẻ tấn công. Định tuyến Onion gây khó khăn cho các nhà điều tra pháp y trong việc theo dõi cuộc tấn công trở lại kẻ tấn công và tăng thời gian phân tích bảo mật.

5. Bí mật
Steganography là quá trình ẩn các tin nhắn hoặc thông tin bí mật trong tệp âm thanh, hình ảnh, video hoặc văn bản theo cách không đáng ngờ. Các kỹ thuật giấu tin thường được kết hợp với mã hóa để cung cấp thêm một lớp bảo mật. Dữ liệu bí mật được trích xuất bởi người được xác thực có quyền truy cập vào đích bằng cách sử dụng công cụ ghi mật mã để giải mã thông báo ẩn.

Tin tặc đã và đang sử dụng kỹ thuật ghi mật mã để ẩn mã và tệp độc hại trong các tệp hợp pháp nhằm vượt qua bảo mật và làm xáo trộn dấu vết của chúng. Kỹ thuật chống pháp y này cho phép kẻ tấn công tiến hành các hoạt động độc hại mà không bị phát hiện thông qua các công cụ phát hiện mối đe dọa và các tham số bảo mật khác. Tin tặc đã được biết là che giấu các tải trọng độc hại bí mật hoặc tin nhắn đáng ngờ bằng mực vô hình trong hình ảnh của những người nổi tiếng, bài báo, quảng cáo, v.v.

6. Thay đổi dấu thời gian
Các nhà điều tra pháp y có thể xác định chính xác hoặc theo dõi kẻ tấn công bằng cách tìm ra vị trí và thời gian của cuộc tấn công. Do đó, những kẻ tấn công sử dụng các kỹ thuật chống điều tra như

thay đổi dấu thời gian để ẩn hoặc loại bỏ nhật ký, xác định vị trí hoặc thời gian tấn công của kẻ tấn công. Việc thay đổi dấu thời gian có thể xóa các mục nhập hoặc ghi đè lên nhật ký mục nhập, khiến điều tra viên khó xác định thông tin thực tế để làm bằng chứng.

Kẻ tấn công thậm chí có thể sửa đổi dấu thời gian của tệp hoặc chương trình như một phương pháp bổ sung để thoát khỏi cuộc điều tra. Họ thay đổi dấu thời gian trên máy chủ để vượt qua an ninh mạng, khởi động một cuộc tấn công và xóa bằng chứng mà không cần đăng nhập vào máy chủ.

Những thách thức mà các công cụ chống pháp y đưa ra đối với cuộc điều tra pháp y kỹ thuật số là đáng báo động. Các doanh nghiệp đang chuyển đổi sang khuôn khổ làm việc từ xa và áp dụng các phương pháp kỹ thuật số tinh vi. Tương tự như vậy, các tác nhân độc hại sử dụng các công cụ và kỹ thuật chống điều tra để khởi chạy các chiến dịch phần mềm độc hại đang phát triển và ngày càng phức tạp. Họ cũng có thể mã hóa các giao thức mạng để thực hiện hành vi trộm cắp danh tính hoặc các tệp bị hỏng. Do đó, các tổ chức phải thực hiện các chiến lược biện pháp đối phó để phát hiện, báo cáo và hạn chế việc sử dụng các kỹ thuật chống pháp y. Tuy nhiên, chỉ một nhóm chuyên gia pháp y kỹ thuật số đủ tiêu chuẩn được đào tạo trong lĩnh vực này mới có thể thực hiện các nhiệm vụ này. Vì vậy, nếu bạn tiếp tục sự nghiệp của mình trong lĩnh vực này, bạn cần đạt được kiến thức và chứng chỉ trong một chương trình đáng tin cậy.

1.6. Luật pháp trong điều tra số

Đạo luật Gramm-Leach-Bliley (GLBA)

Được ban hành vào năm 1999, Đạo luật Gramm-Leach-Bliley (GLBA) yêu cầu các tổ chức tài chính - các công ty cung cấp cho người tiêu dùng các sản phẩm hoặc dịch vụ tài chính như khoản vay, tư vấn tài chính hoặc đầu tư hoặc bảo hiểm - phải giải thích các hoạt động chia sẻ thông tin của họ cho khách hàng và để bảo vệ dữ liệu nhạy cảm. Mục tiêu của GLBA là tạo điều kiện thuận lợi cho việc chuyển giao thông tin tài chính giữa các tổ chức và ngân hàng đồng thời làm cho các quyền của cá nhân thông qua các yêu cầu bảo mật trở nên cụ thể hơn.

Các điều khoản của giới hạn GLBA khi một "tổ chức tài chính" có thể tiết lộ "thông tin cá nhân không công khai" của người tiêu dùng cho các bên thứ ba không liên kết. Luật áp dụng cho nhiều tổ chức tài chính, bao gồm nhiều công ty không được coi là tổ chức tài chính theo truyền thống vì họ tham gia vào một số "hoạt động tài chính". Theo Quy tắc Bảo mật, chỉ một tổ chức "tham gia đáng kể" vào các hoạt động tài chính mới được coi là một tổ chức tài chính.

Các tổ chức tài chính nên thông báo cho khách hàng của họ về các hoạt động chia sẻ thông tin của họ và cho người tiêu dùng biết về quyền "không tham gia" nếu họ không muốn thông tin của mình được chia sẻ với một số bên thứ ba không liên kết. Ngoài ra, bất kỳ thực thể nào nhận thông tin tài chính của người tiêu dùng từ một tổ chức tài chính có thể bị hạn chế trong việc sử dụng lại và tiết lộ lại thông tin đó. Nó giúp giải quyết các sự cố truy cập trái phép vào thông tin nhạy cảm của khách hàng do tổ chức tài chính lưu giữ theo cách có thể dẫn đến "tổn hại hoặc bất tiện đáng kể cho bất kỳ khách hàng nào".

Đạo luật hiện đại hóa an ninh thông tin liên bang năm 2014 (FISMA)

FISMA được giới thiệu như một sửa đổi đối với Đạo luật quản lý bảo mật thông tin liên bang năm 2002, được triển khai để cung cấp khuôn khổ cho các hệ thống thông tin liên bang nhằm

kiểm soát bảo mật thông tin hiệu quả hơn. FISMA 2014 đã thực hiện một số sửa đổi đối với các điều khoản hiện có của FISMA 2002 nhằm hiện đại hóa các biện pháp bảo mật mà các cơ quan liên bang tuân theo để giải quyết các mối lo ngại về bảo mật đang gia tăng. Những thay đổi này dẫn đến ít báo cáo tổng thể hơn, tăng cường sử dụng giám sát liên tục trong các hệ thống, tăng cường tập trung vào các cơ quan để tuân thủ và khuyến khích báo cáo tập trung hơn vào các vấn đề do sự cố bảo mật gây ra.

FISMA 2014 yêu cầu Văn phòng Quản lý tại (OMB) sửa đổi/sửa đổi A-130 để loại bỏ việc báo cáo không hiệu quả và lãng phí, đồng thời phản ánh những thay đổi về luật và những tiến bộ trong A-130 cập nhật vòng đời thông tin và các yêu cầu dưới dạng các bài tập tuân thủ các yếu tố quan trọng của chương trình dựa trên rủi ro toàn diện, chiến lược và liên tục tại các cơ quan liên bang.

Đạo luật Trách nhiệm Giải trình và Cung cấp Bảo hiểm Y tế năm 1996 (HIPAA)

Quy tắc về quyền riêng tư của HIPAA cung cấp các biện pháp bảo vệ của liên bang đối với thông tin sức khỏe có thể nhận dạng cá nhân do các thực thể được bảo hiểm và các đối tác kinh doanh của họ nắm giữ, đồng thời cung cấp cho bệnh nhân một loạt các quyền đối với thông tin đó. Quy tắc Quyền riêng tư cũng cho phép tiết lộ thông tin sức khỏe cần thiết để chăm sóc bệnh nhân và các mục đích quan trọng khác. Quy tắc bảo mật HIPAA chỉ định một loạt các biện pháp bảo vệ hành chính, vật lý và kỹ thuật cho các thực thể được bảo vệ và các đối tác kinh doanh của họ sử dụng để đảm bảo tính bảo mật, tính toàn vẹn và tính sẵn có của thông tin sức khỏe điện tử được bảo vệ.

Văn phòng Dân quyền đã triển khai Quy chế và Quy tắc Đơn giản hóa Hành chính của HIPAA, như được thảo luận dưới đây:

- Tiêu chuẩn Bộ mã và Giao dịch điện tử

  Giao dịch là trao đổi điện tử liên quan đến việc chuyển thông tin giữa hai bên cho các mục đích cụ thể. HIPAA đặt tên cho một số loại tổ chức nhất định là các thực thể được bảo hiểm, bao gồm các chương trình sức khỏe, trung tâm thanh toán bù trừ chăm sóc sức khỏe và một số nhà cung cấp dịch vụ chăm sóc sức khỏe. Trong các quy định của HIPAA, Bộ trưởng Bộ Y tế và Dịch vụ Nhân sinh (HHS) đã thông qua một số giao dịch tiêu chuẩn nhất định cho Trao đổi Dữ liệu Điện tử (EDI) về dữ liệu chăm sóc sức khỏe.
- Quy tắc về quyền riêng tư

  Quy tắc về quyền riêng tư của HIPAA thiết lập các tiêu chuẩn quốc gia để bảo vệ hồ sơ y tế của cá nhân và thông tin sức khỏe cá nhân khác, đồng thời áp dụng cho các chương trình bảo hiểm sức khỏe, trung tâm thanh toán bù trừ chăm sóc sức khỏe và những nhà cung cấp dịch vụ chăm sóc sức khỏe thực hiện một số giao dịch chăm sóc sức khỏe bằng điện tử. Quy tắc yêu cầu các biện pháp bảo vệ thích hợp để bảo vệ quyền riêng tư của thông tin sức khỏe cá nhân và đặt ra các giới hạn và điều kiện đối với việc sử dụng và tiết lộ thông tin đó mà không có sự cho phép của bệnh nhân. Quy tắc cũng trao cho bệnh nhân các quyền đối với thông tin sức khỏe của họ, bao gồm quyền kiểm tra và nhận bản sao hồ sơ sức khỏe của họ cũng như yêu cầu chỉnh sửa.
- Quy tắc bảo mật

  Quy tắc bảo mật HIPAA thiết lập các tiêu chuẩn quốc gia để bảo vệ thông tin sức khỏe cá nhân điện tử của các cá nhân được tạo, nhận, sử dụng hoặc duy trì bởi một thực thể được bảo hiểm.

Quy tắc Bảo mật yêu cầu các biện pháp bảo vệ hành chính, vật lý và kỹ thuật phù hợp để đảm bảo tính bảo mật, tính toàn vẹn và an ninh của thông tin sức khỏe được bảo vệ bằng điện tử.

- Tiêu chuẩn định danh nhà tuyển dụng
  Đạo luật về trách nhiệm giải trình và cung cấp thông tin bảo hiểm y tế năm 1996 (HIPAA) yêu cầu người sử dụng lao động phải có số quốc gia tiêu chuẩn để xác định họ trên các giao dịch tiêu chuẩn.
- Tiêu chuẩn định danh nhà cung cấp quốc gia
  Mã định danh Nhà cung cấp Quốc gia (NPI) là một Tiêu chuẩn Đơn giản hóa Hành chính của HIPAA. NPI là mã số nhận dạng duy nhất dành cho các nhà cung cấp dịch vụ chăm sóc sức khỏe được bảo hiểm. Các nhà cung cấp dịch vụ chăm sóc sức khỏe được bảo hiểm và tất cả các chương trình bảo hiểm y tế và trung tâm thanh toán bù trừ chăm sóc sức khỏe phải sử dụng NPI trong các giao dịch hành chính và tài chính được thông qua theo HIPAA. NPI là một mã định danh số mười vị trí, không có thông tin tình báo (số có mười chữ số). Điều này có nghĩa là các con số không mang thông tin khác về các nhà cung cấp dịch vụ chăm sóc sức khỏe, chẳng hạn như tiểu bang nơi họ sinh sống hoặc chuyên môn y tế của họ.
- Quy tắc thực thi
  Quy tắc Thực thi HIPAA bao gồm các điều khoản liên quan đến việc tuân thủ và điều tra, việc áp dụng hình phạt tiền dân sự đối với hành vi vi phạm Quy tắc Đơn giản hóa Hành chính của HIPAA và thủ tục điều trần.

Đạo luật bảo mật thông tin liên lạc điện tử

Đạo luật bảo mật thông tin liên lạc điện tử và Đạo luật thông tin liên lạc điện tử dây được lưu trữ thường được gọi chung là Đạo luật bảo mật thông tin liên lạc điện tử (ECPA) năm 1986, theo 18 U.S.C. §§ 2510-2523. ECPA đã cập nhật Đạo luật Nghe lén Liên bang năm 1968, đề cập đến việc chặn các cuộc hội thoại bằng đường dây điện thoại "cứng" nhưng không áp dụng cho việc chặn máy tính và các phương tiện liên lạc kỹ thuật số và điện tử khác. ECPA, như đã sửa đổi, bảo vệ các thông tin liên lạc bằng dây, bằng miệng và điện tử, trong khi các thông tin liên lạc đó đang được thực hiện, đang chuyển tiếp và được lưu trữ trên máy tính. Đạo luật áp dụng cho email, cuộc trò chuyện qua điện thoại và dữ liệu được lưu trữ bằng điện tử.

ECPA có ba tiêu đề, được thảo luận dưới đây:

Tiêu đề I

Thường được gọi là Đạo luật Nghe lén, Tiêu đề I nghiêm cấm hành vi cố ý, thực tế hoặc cố gắng chặn, sử dụng, tiết lộ hoặc "mua [tinh thần] [của] bất kỳ người nào khác để chặn hoặc cố gắng chặn bất kỳ thông tin liên lạc qua đường dây, bằng miệng hoặc điện tử nào ." Tiêu đề I cũng cấm sử dụng các thông tin liên lạc thu được bất hợp pháp làm bằng chứng.

Ngoại lệ: Tiêu đề I đưa ra các ngoại lệ đối với các nhà khai thác và nhà cung cấp dịch vụ đối với các mục đích sử dụng "trong quá trình làm việc bình thường của anh ta khi tham gia vào bất kỳ hoạt động nào là sự cố cần thiết đối với việc thực hiện dịch vụ của anh ta" và đối với "những người được pháp luật ủy quyền để chặn đường dây, lời nói , hoặc liên lạc điện tử hoặc để tiến hành giám sát điện tử, như được định nghĩa trong phần 101 của Đạo luật giám sát tình báo nước ngoài (FISA) năm 1978." Nó cung cấp các thủ tục cho các quan chức chính phủ liên bang, Tiểu bang và các cơ quan

chính phủ khác để xin phép tư pháp nhằm chặn các thông tin liên lạc đó và cũng quy định việc sử dụng và tiết lộ thông tin thu được thông qua hoạt động nghe lén được ủy quyền.

Tiêu đề II

Còn được gọi là Đạo luật Truyền thông được Lưu trữ (SCA), Tiêu đề II bảo vệ quyền riêng tư của các tệp được lưu trữ bởi nhà cung cấp dịch vụ và hồ sơ do nhà cung cấp dịch vụ lưu giữ về người đăng ký, chẳng hạn như tên người đăng ký, hồ sơ thanh toán hoặc địa chỉ IP.

Tiêu đề III

Tiêu đề III đề cập đến các thiết bị theo dõi và theo dõi bút đăng ký và yêu cầu các cơ quan chính phủ phải có lệnh của tòa án cho phép cài đặt và sử dụng bút đăng ký (một thiết bị ghi lại các số đã quay và thông tin liên quan đến các cuộc gọi đi hoặc liên lạc được thực hiện bởi đối tượng) và/hoặc bẫy và theo dõi (một thiết bị ghi lại các số và thông tin liên quan mà từ đó các cuộc gọi đến và thông tin liên lạc đến đối tượng được bắt nguồn).

Quy định chung về bảo vệ dữ liệu (GDPR)

GDPR của EU đã thay thế Chỉ thị bảo vệ dữ liệu 95/46/EC và được thiết kế để hài hòa các luật về quyền riêng tư dữ liệu trên khắp châu Âu, nhằm bảo vệ và trao quyền cho tất cả công dân EU về quyền riêng tư dữ liệu, đồng thời định hình lại cách các tổ chức trong khu vực tiếp cận quyền riêng tư dữ liệu.

Điều 32: Các biện pháp kỹ thuật và tổ chức cần đảm bảo các nội dung sau:

- Bí danh và mã hóa dữ liệu cá nhân
- Khả năng đảm bảo tính bảo mật, tính toàn vẹn, tính sẵn sàng và khả năng phục hồi liên tục của các hệ thống và dịch vụ xử lý
- Khả năng khôi phục tính khả dụng và quyền truy cập vào dữ liệu cá nhân một cách kịp thời trong trường hợp xảy ra sự cố vật lý hoặc kỹ thuật
- Một quy trình thường xuyên kiểm tra, đánh giá và đánh giá hiệu quả của các biện pháp kỹ thuật và tổ chức để đảm bảo an toàn cho quá trình xử lý.

Điều 33(1):

"Trong trường hợp vi phạm dữ liệu cá nhân, bộ điều khiển sẽ không chậm trễ quá mức và, nếu khả thi, không quá 72 giờ sau khi biết về nó, thông báo vi phạm dữ liệu cá nhân cho cơ quan giám sát có thẩm quyền theo Điều 55, trừ khi việc vi phạm dữ liệu cá nhân không có khả năng dẫn đến rủi ro đối với quyền và tự do của thể nhân. Trường hợp không thông báo cho cơ quan giám sát trong vòng 72 giờ thì phải kèm theo lý do chậm trễ."

Đạo luật bảo vệ dữ liệu năm 2018

Đạo luật bảo vệ dữ liệu, được ban hành vào năm 2018, đưa ra các điều khoản về quy định xử lý thông tin liên quan đến các cá nhân, liên quan đến các chức năng của Ủy viên thông tin theo một số quy định liên quan đến thông tin, đối với quy tắc thực hành tiếp thị trực tiếp và cho các mục đích liên quan. Nó bảo vệ dữ liệu cá nhân theo cách sau:

"(1) GDPR, GDPR được áp dụng và Đạo luật này bảo vệ các cá nhân liên quan đến việc xử lý dữ liệu cá nhân, đặc biệt là bởi:

- yêu cầu dữ liệu cá nhân được xử lý hợp pháp và công bằng theo sự đồng ý của chủ thể dữ liệu hoặc cơ sở cụ thể khác;

- trao quyền cho chủ thể dữ liệu để lấy thông tin về việc xử lý dữ liệu cá nhân và yêu cầu chỉnh sửa dữ liệu cá nhân không chính xác; Và
- trao các chức năng cho Ủy viên, trao cho người giữ chức vụ đó trách nhiệm giám sát và thực thi các điều khoản của họ.

(2) Khi thực hiện các chức năng theo GDPR, GDPR được áp dụng và Đạo luật này, Ủy viên phải lưu ý đến tầm quan trọng của việc đảm bảo mức độ bảo vệ phù hợp cho dữ liệu cá nhân, có tính đến lợi ích của chủ thể dữ liệu, bên kiểm soát và những vấn đề khác và những vấn đề liên quan đến lợi ích chung của công chúng."

Tiêu chuẩn bảo mật dữ liệu ngành thẻ thanh toán (PCI DSS)

PCI DSS là một tiêu chuẩn bảo mật thông tin độc quyền dành cho các tổ chức xử lý thông tin chủ thẻ đối với thẻ ghi nợ, tín dụng, trả trước, ví điện tử, ATM và thẻ POS chính. PCI DSS áp dụng cho các tổ chức "lưu trữ, xử lý hoặc truyền dữ liệu chủ thẻ" cho thẻ tín dụng. Một trong những yêu cầu của nó là "theo dõi...tất cả quyền truy cập vào tài nguyên mạng và dữ liệu chủ thẻ."

Đạo luật Sarbanes-Oxley (SOX) năm 2002

Đạo luật Sarbanes-Oxley năm 2002 (SOX) là một đạo luật được Quốc hội Hoa Kỳ thông qua vào năm 2002 để bảo vệ các nhà đầu tư khỏi khả năng các hoạt động kế toán gian lận của các tập đoàn. Mặc dù SOX áp dụng chủ yếu cho các hoạt động tài chính và kế toán, nhưng nó cũng bao gồm các chức năng công nghệ thông tin (CNTT) hỗ trợ các hoạt động này. SOX có thể được hỗ trợ bằng cách xem xét nhật ký thường xuyên để tìm kiếm các dấu hiệu vi phạm bảo mật, bao gồm khai thác, cũng như lưu giữ nhật ký và hồ sơ đánh giá nhật ký để kiểm toán viên xem xét trong tương lai.

Câu hỏi và bài tập

Chương 2. Thu thập và sao lưu dữ liệu

2.1. Khái niệm cơ bản

Hiểu về thu thập dữ liệu

Thu thập dữ liệu pháp y là một quá trình chụp ảnh hoặc thu thập thông tin bằng các phương pháp đã được thiết lập từ các phương tiện khác nhau theo các tiêu chuẩn nhất định cho giá trị pháp y của chúng. Thông tin này sau đó có thể được phân tích để hiểu rõ hơn về tội phạm hoặc sự cố. Với sự tiến bộ của công nghệ, quá trình thu thập dữ liệu ngày càng trở nên chính xác, đơn giản và linh hoạt. Tuy nhiên, các điều tra viên cần đảm bảo rằng phương pháp mua lại được sử dụng là hợp lý về mặt pháp lý. Cụ thể, phương pháp mua lại được áp dụng phải được kiểm chứng và lặp lại. Điều này giúp tăng cường khả năng chấp nhận dữ liệu hoặc bằng chứng thu được trước tòa án. Một yếu tố cơ bản cần xem xét trong việc thu thập dữ liệu pháp y là thời gian. Mặc dù dữ liệu trong một số nguồn như ổ cứng vẫn không thay đổi và có thể được thu thập ngay cả sau khi hệ thống tắt, nhưng dữ liệu trong một số nguồn như RAM rất dễ bay hơi và động, do đó phải được thu thập trong thời gian thực. Từ quan điểm này, việc thu thập dữ liệu có thể được phân loại thành thu thập dữ liệu trực tiếp hoặc thu thập dữ liệu chết.

Trong thu thập dữ liệu trực tiếp, dữ liệu được thu thập từ máy tính đã được bật nguồn (bị khóa hoặc ở chế độ ngủ). Điều này cho phép thu thập dữ liệu dễ bay hơi dễ vỡ và bị mất khi hệ thống mất điện hoặc bị tắt. Dữ liệu như vậy nằm trong sổ đăng ký, bộ đệm và RAM. Hơn nữa, dữ liệu dễ bay hơi chẳng hạn như dữ liệu trong RAM là động và thay đổi nhanh chóng, do đó phải được thu thập trong thời gian thực.

Trong quá trình thu thập dữ liệu chết hoặc tĩnh, dữ liệu cố định vẫn không bị thay đổi trong hệ thống ngay cả sau khi tắt máy được thu thập. Các nhà điều tra có thể khôi phục dữ liệu đó từ ổ cứng cũng như từ dung lượng trống, tệp hoán đổi và dung lượng ổ đĩa chưa phân bổ. Các nguồn dữ liệu cố định khác bao gồm CD-ROM, ổ USB, điện thoại thông minh và PDA.

Thu thập trực tiếp

Quá trình thu thập dữ liệu trực tiếp liên quan đến việc thu thập dữ liệu dễ bay hơi từ các thiết bị khi chúng đang hoạt động hoặc được bật nguồn. Thông tin dễ bay hơi, như có trong nội dung của RAM, bộ đệm, DLL, v.v. là động và có khả năng là thông tin cuối cùng nếu thiết bị được điều tra bị tắt. Do đó, nó phải được mua trong thời gian thực. Kiểm tra thông tin dễ bay hơi hỗ trợ xác định dòng thời gian hợp lý của bảo mật và người dùng có khả năng chịu trách nhiệm về thông tin đó.

Sau đó, quá trình thu thập trực tiếp có thể được theo sau bằng quá trình thu thập tĩnh/chết, trong đó điều tra viên tắt máy nghi ngờ, tháo đĩa cứng và sau đó thu được hình ảnh pháp y của nó.

Thu thập dữ liệu trực tiếp có thể giúp các nhà điều tra thu thập thông tin ngay cả khi dữ liệu có giá trị chứng cứ được lưu trữ trên đám mây bằng dịch vụ như Dropbox hoặc Google Drive.

Các nhà điều tra cũng có thể thu thập dữ liệu từ các thùng chứa hoặc đĩa không được mã hóa đang mở trên hệ thống và được mã hóa tự động khi hệ thống tắt. Nếu nghi phạm đã cố gắng ghi đè dữ liệu lên đĩa cứng vật lý để tránh bị phát hiện, thì có khả năng các nhà điều tra có thể tìm thấy dấu vết của dữ liệu bị ghi đè đó bằng cách kiểm tra nội dung RAM.

Tùy thuộc vào nguồn mà chúng được lấy, dữ liệu dễ bay hơi có hai loại:

- Dữ liệu hệ thống

  Thông tin hệ thống là thông tin liên quan đến một hệ thống, có thể dùng làm bằng chứng trong một sự cố bảo mật. Thông tin này bao gồm cấu hình hiện tại và trạng thái hoạt động của máy tính nghi ngờ. Thông tin hệ thống dễ thay đổi bao gồm hồ sơ hệ thống (chi tiết về cấu hình), hoạt động đăng nhập, ngày và giờ hệ thống hiện tại, lịch sử lệnh, thời gian hoạt động của hệ thống hiện tại, các quy trình đang chạy, tệp đang mở, tệp khởi động, dữ liệu khay nhớ tạm, người dùng đã đăng nhập, DLLS và thư viện dùng chung. Thông tin hệ thống cũng bao gồm dữ liệu quan trọng được lưu trữ trong khoảng trống của ổ đĩa cứng.

- Dữ liệu mạng

  Thông tin mạng là thông tin liên quan đến mạng được lưu trữ trong hệ thống nghi ngờ và các thiết bị mạng được kết nối. Thông tin mạng không ổn định bao gồm các kết nối và cổng đang mở, thông tin định tuyến và cấu hình, bộ đệm ARP, các tệp được chia sẻ và các dịch vụ được truy cập.

Thu thập chết

Dữ liệu tĩnh đề cập đến dữ liệu không biến đổi, không thay đổi trạng thái ngay cả sau khi hệ thống bị tắt.

Thu thập chết đề cập đến quá trình trích xuất và thu thập những dữ liệu này theo cách không thay đổi từ phương tiện lưu trữ. Các nguồn dữ liệu cố định bao gồm ổ cứng, DVD-ROM, ổ USB, flashcard, điện thoại thông minh và ổ cứng ngoài. Loại dữ liệu này tồn tại dưới dạng email, tài liệu xử lý văn bản, hoạt động web, bảng tính, dung lượng trống, tệp hoán đổi, dung lượng ổ đĩa chưa phân bổ và các tệp đã xóa khác nhau. Các nhà điều tra có thể lặp lại quy trình thu nhận xác chết trên bằng chứng đĩa được bảo quản tốt.

Dữ liệu tĩnh được khôi phục từ ổ cứng bao gồm:

- Tệp tạm thời (tạm thời)
- Đăng ký hệ thống
- Nhật ký sự kiện/hệ thống
- lĩnh vực khởi động
- Bộ nhớ cache của trình duyệt web
- Cookies
- Các tệp ẩn

2.2. Xác định dữ liệu

Xác định định dạng thu thập dữ liệu

Định dạng thô

Định dạng thô đề cập đến một bản sao từng bit của ổ đĩa nghi ngờ. Hình ảnh ở định dạng này thường thu được bằng cách sử dụng lệnh dd.

Thuận lợi

- Hiệu suất tìm kiếm bằng chứng thường cao hơn
- Được hỗ trợ bởi hầu hết các công cụ pháp y bao gồm các công cụ phần mềm miễn phí như dd, dc3dd và dcfldd

Nhược điểm

- Không bao gồm bất kỳ siêu dữ liệu nào
- Không hỗ trợ nén hình ảnh, dẫn đến cùng kích thước với phương tiện đáng ngờ

Định dạng độc quyền

Định dạng độc quyền đề cập đến các công cụ hỗ trợ các định dạng tệp hình ảnh khác nhau. đào tạo thương mại khác nhau

Thuận lợi

- Hỗ trợ nén các tập tin hình ảnh
- Hỗ trợ các tệp hình ảnh được phân đoạn
- Các tệp hình ảnh có thể bao gồm siêu dữ liệu

Nhược điểm

- Tốn nhiều thời gian tìm kiếm bằng chứng hơn định dạng thô
- Định dạng tệp hình ảnh do công cụ tạo ra có thể không được (các) công cụ khác hỗ trợ

Định dạng pháp y nâng cao (AFF)

AFF là định dạng thu thập dữ liệu nguồn mở lưu trữ hình ảnh đĩa và siêu dữ liệu liên quan. Mục tiêu đằng sau sự phát triển của định dạng là tạo ra một định dạng hình ảnh đĩa mở cung cấp cho người dùng một giải pháp thay thế để không bị khóa trong một định dạng độc quyền.

AFF và AFFv3 hỗ trợ các phần mở rộng tệp như .afm cho siêu dữ liệu và .afd cho tệp hình ảnh. Không có giới hạn triển khai nào do AFF áp đặt đối với điều tra viên pháp y, vì đây là một định dạng mã nguồn mở.

AFF có thiết kế đơn giản và tương thích để chạy trong nhiều môi trường máy tính. Nó cung cấp tùy chọn để nén các tệp hình ảnh và phân bổ không gian để ghi siêu dữ liệu của tệp hình ảnh hoặc tệp được phân đoạn

AFF hỗ trợ hai thuật toán nén sau:

- Zlib, nhanh hơn nhưng kém hiệu quả hơn
- LZMA, chậm hơn nhưng hiệu quả hơn

Hình ảnh đĩa thực tế trong AFF là một tệp duy nhất, bao gồm các phân đoạn có dữ liệu ổ đĩa và siêu dữ liệu. Nội dung tệp AFF có thể được nén và giải nén. AFFv3 hỗ trợ các phần mở rộng tệp AFF, AFD và AFM.

Khung pháp lý nâng cao 4 (AFF4)

Michael Cohen, Simson Garfinkel và Bradly Schatz đã tạo Advanced Forensic Framework 4 (AFF4) dưới dạng phiên bản được thiết kế lại và cải tiến của định dạng AFF, được thiết kế để hỗ trợ phương tiện lưu trữ có dung lượng lớn. Những người sáng tạo gọi thiết kế của nó là hướng đối tượng vì định dạng này bao gồm các đối tượng chung với hành vi có thể truy cập từ bên ngoài. Những đối tượng này có thể được giải quyết bằng tên của chúng trong vũ trụ AFF4.

Định dạng này có thể hỗ trợ một số lượng lớn hình ảnh và cung cấp nhiều lựa chọn định dạng vùng chứa chẳng hạn như Zip và Zip64 cho các tệp nhị phân và các thư mục đơn giản. Nó cũng hỗ trợ lưu trữ từ mạng và việc sử dụng WebDAV (phần mở rộng của giao thức HTTP) cho phép chụp ảnh trực tiếp đến một máy chủ HTTP trung tâm.

Định dạng này cũng hỗ trợ các bản đồ, là các phép biến đổi dữ liệu không sao chép. Các phép biến đổi không sao chép giúp CPU không phải thực hiện nhiệm vụ sao chép dữ liệu từ vùng bộ nhớ này sang vùng bộ nhớ khác, do đó tăng hiệu quả của nó.

Ví dụ: không lưu trữ bản sao mới của tệp chạm khắc (tệp đang được trích xuất), chỉ có thể lưu trữ bản đồ của các khối được phân bổ cho tệp này. AFF4 hỗ trợ ký hình ảnh và mật mã. Định dạng này cũng cung cấp độ trong suốt của hình ảnh cho khách hàng.

Thiết kế AFF4 áp dụng sơ đồ các số nhận dạng duy nhất trên toàn cầu để xác định và tham khảo tất cả các bằng chứng. Các loại đối tượng AFF4 cơ bản bao gồm:

- Tập: Chúng lưu trữ các phân đoạn là các khối dữ liệu không thể chia nhỏ
- Luồng: Đây là những đối tượng dữ liệu có thể giúp đọc hoặc viết, ví dụ: phân đoạn, hình ảnh và bản đồ
- Đồ thị: Tập hợp các câu lệnh RDF

2.3. Các phương pháp thu thập dữ liệu

Tệp chuyển từ đĩa sang ảnh: Tệp chuyển từ đĩa sang ảnh đề cập đến quá trình tạo một ảnh hoặc bản sao hoàn chỉnh của đĩa hoặc thiết bị lưu trữ và lưu nó dưới dạng một tệp duy nhất. Tệp hình ảnh này chứa một bản sao chính xác của đĩa gốc, bao gồm hệ thống tệp, cấu trúc phân vùng và tất cả dữ liệu được lưu trữ trên đĩa. Nó ghi lại toàn bộ nội dung của đĩa, bao gồm cả các khu vực được sử dụng và không sử dụng. Ảnh đĩa thường được sử dụng cho mục đích sao lưu, sao chép hoặc pháp y.

Sao chép từ đĩa sang đĩa: Sao chép từ đĩa sang đĩa liên quan đến việc sao chép trực tiếp dữ liệu từ đĩa này sang đĩa khác. Quá trình này tạo ra một bản sao giống hệt của đĩa nguồn, bao gồm tất cả các tệp, thư mục và cấu trúc hệ thống tệp. Nó có thể được sử dụng để di chuyển dữ liệu từ đĩa này sang đĩa khác, thực hiện sao lưu hoặc tạo các bản sao dự phòng của dữ liệu quan trọng. Sao chép từ đĩa sang đĩa có thể được thực hiện bằng nhiều công cụ phần mềm khác nhau hoặc thông qua các tiện ích tích hợp sẵn của hệ điều hành.

Tệp logic từ đĩa sang đĩa hoặc tệp từ đĩa sang dữ liệu: Sao chép tệp logic từ đĩa sang đĩa hoặc đĩa sang dữ liệu đề cập đến quá trình sao chép có chọn lọc các tệp hoặc thư mục cụ thể từ đĩa này sang đĩa khác. Không giống như sao chép toàn bộ từ đĩa này sang đĩa khác, phương pháp này cho phép bạn chọn dữ liệu cụ thể sẽ được truyền thay vì sao chép toàn bộ đĩa. Nó có thể hữu ích khi bạn chỉ cần chuyển các tệp hoặc thư mục cụ thể sang một ổ đĩa khác hoặc khi bạn muốn tạo một bản sao lưu dữ liệu quan trọng mà không cần sao chép toàn bộ ổ đĩa.

Sao chép dữ liệu thưa thớt: Sao chép dữ liệu thưa đề cập đến phương pháp sao chép tệp hoặc thư mục trong khi tối ưu hóa không gian lưu trữ bằng cách chỉ sao chép dữ liệu thực thay vì phân bổ không gian cho các phần trống hoặc không sử dụng. Nó đặc biệt hữu ích khi xử lý các tệp lớn hoặc ảnh đĩa chứa không gian trống đáng kể hoặc các vùng không có dữ liệu có ý nghĩa. Các kỹ thuật sao chép dữ liệu thưa thớt xác định các vùng trống hoặc thưa thớt và loại trừ chúng khỏi quy trình sao chép, giúp sử dụng đĩa hiệu quả hơn và giảm yêu cầu lưu trữ.

2.4. Lưu trữ dữ liệu

2.5. Thiết bị điều tra

Câu hỏi ôn tập

Chương 3. Điều tra trên Windows

3.1. Khái niệm cơ bản

Windows forensics đề cập đến việc điều tra tội phạm mạng liên quan đến máy Windows. Nó liên quan đến việc thu thập bằng chứng từ máy Windows để có thể xác định (những) thủ phạm của tội phạm mạng và truy tố Windows là một trong những hệ điều hành được sử dụng rộng rãi nhất; do đó, khả năng máy Windows gặp sự cố là rất cao. Vì vậy, các điều tra viên phải hiểu thấu đáo về các thành phần khác nhau của HĐH Windows, chẳng hạn như hệ thống tệp, sổ đăng ký, tệp hệ thống và nhật ký sự kiện, nơi họ có thể tìm thấy dữ liệu có giá trị bằng chứng.

3.2. Thu thập dữ liệu khả biến

Thu thập thông tin dễ bay hơi

Như đã đề cập trước đó, thông tin dễ bay hơi đề cập đến dữ liệu được lưu trữ trong sổ đăng ký, bộ đệm và RAM của thiết bị kỹ thuật số. Thông tin này thường bị mất hoặc bị xóa bất cứ khi nào hệ thống bị tắt hoặc khởi động lại. Thông tin dễ bay hơi có bản chất động và thay đổi theo thời gian; vì vậy, các nhà điều tra sẽ có thể thu thập dữ liệu trong thời gian thực.

Dữ liệu dễ bay hơi tồn tại trong bộ nhớ vật lý hoặc RAM và bao gồm thông tin quy trình, ánh xạ quy trình tới cổng, bộ nhớ quy trình, kết nối mạng, nội dung khay nhớ tạm, trạng thái của hệ thống, v.v. Các nhà điều tra phải thu thập dữ liệu này trong quá trình thu thập dữ liệu trực tiếp. Ngoài ra, họ nên tuân theo Nguyên tắc trao đổi của Locard và thu thập nội dung của RAM ngay khi bắt đầu điều tra để giảm thiểu tác động của các bước tiếp theo đối với tính toàn vẹn của nội dung trong RAM.

Các nhà điều tra cần nhận thức rõ thực tế rằng các công cụ họ đang chạy để thu thập thông tin không ổn định khác có thể sửa đổi nội dung của bộ nhớ. Dựa trên thông tin không ổn định được thu thập, các nhà điều tra có thể xác định (những) người dùng đã đăng nhập, dòng thời gian xảy ra sự cố bảo mật, các chương trình và thư viện liên quan, các tệp được truy cập và chia sẻ trong một cuộc tấn

công đáng ngờ, cũng như các chi tiết khác như thông tin mạng, mở tệp, ánh xạ quy trình tới cổng, ổ đĩa được ánh xạ, lịch sử lệnh, thông tin quy trình, chia sẻ, nội dung khay nhớ tạm, v.v.

Thu thập thời gian hệ thống

Thu thập người dùng đã đăng nhập

Thu thập tệp mở: lệnh net file

Thu thập tệp mở: Sử dụng NetworkOpenedFiles

Thu thập thông tin mạng

Thu thập trạng thái mạng

Thu thập thông tin về kết nối mạng

Thu thập Thông tin tiến trình

Thu thập tiến trình với cổng tương ứng

Thu thập lịch sử lệnh và thông tin tài nguyên được chia sẻ cục bộ

3.3. Thu thập dữ liệu bất biến

Thu thập thông tin không bay hơi

Dữ liệu cố định không thay đổi khi hệ thống tắt hoặc mất điện. Một số ví dụ về dữ liệu cố định bao gồm email, tài liệu soạn thảo văn bản, bảng tính và các tệp "đã xóa" khác nhau.

Điều tra viên có thể quyết định thông tin nào cần được trích xuất từ sổ đăng ký hoặc thông tin nào về (hoặc từ) tệp sẽ được thu thập để phân tích bổ sung. Cũng có khả năng kẻ tấn công có thể chủ động đăng nhập vào hệ thống và truy cập dữ liệu. Trong những trường hợp như vậy, điều tra viên thậm chí có thể quyết định theo dõi kẻ tấn công. Điều quan trọng là điều tra viên phải giữ nguyên một số thông tin quan trọng mà không có bất kỳ sửa đổi hoặc xóa nào. Sau khi người dùng khởi động hệ thống, một số dữ liệu có thể được sửa đổi, chẳng hạn như các ổ đĩa được ánh xạ tới hoặc từ hệ thống, các dịch vụ đã khởi động hoặc các ứng dụng được cài đặt. Những sửa đổi này có thể không liên tục trong quá trình khởi động lại và do đó, điều tra viên nên ghi lại và ghi lại chúng.

Dữ liệu cố định thường nằm trong ổ cứng; nó cũng tồn tại trong các tệp hoán đổi, không gian chùng và không gian ổ đĩa chưa phân bổ. Các nguồn dữ liệu cố định khác bao gồm CD-ROM, ổ lưu trữ USB và điện thoại thông minh.

- Kiểm tra hệ thống tập tin
- Tệp cơ sở dữ liệu ESE
- Phân tích chỉ mục tìm kiếm Windows
- Bộ nhớ cache của trình duyệt web
- Phát hiện các thiết bị được kết nối bên ngoài với hệ thống
- Những file không sử dụng đến dung lượng
- Cookies
- File tạm thời

3.4. Phân tích Cache, Cookie và History

- Phân tích bộ đệm:

  Khi bạn duyệt internet, các trình duyệt web thường lưu trữ các bản sao tạm thời của các trang web, hình ảnh và các tài nguyên khác trong bộ đệm ẩn. Bộ đệm này được sử dụng để cải thiện trải nghiệm duyệt web bằng cách cho phép truy cập nhanh hơn vào các trang web đã truy cập trước đó. Trong pháp y kỹ thuật số, việc phân tích bộ đệm có thể cung cấp thông

tin có giá trị về các hoạt động trực tuyến của người dùng. Điều này có thể bao gồm bằng chứng về các trang web đã truy cập, tệp đã tải xuống, hình ảnh đã xem và thậm chí cả các tương tác của người dùng, chẳng hạn như gửi biểu mẫu.

Phân tích bộ đệm liên quan đến việc kiểm tra các tệp và thư mục bộ đệm được lưu trữ trên máy tính hoặc trong các thư mục dữ liệu của trình duyệt web. Việc phân tích có thể được thực hiện bằng cách sử dụng các công cụ pháp y chuyên dụng hoặc bằng cách kiểm tra thủ công các tệp bộ đệm. Thông tin được trích xuất có thể được sử dụng để xây dựng lại lịch sử duyệt web của người dùng, xác định các trang web đã truy cập và có khả năng khôi phục nội dung web đã bị xóa hoặc bị che khuất.

- Phân tích cookie:
- Cookie là các tệp văn bản nhỏ mà các trang web lưu trữ trên máy tính của người dùng để ghi nhớ một số thông tin nhất định về các tương tác của người dùng. Những cookie này có thể chứa dữ liệu như thông tin đăng nhập, số nhận dạng phiên, tùy chọn và thông tin theo dõi. Trong pháp y kỹ thuật số, việc phân tích cookie có thể cung cấp thông tin chi tiết về các hoạt động trực tuyến của người dùng, bao gồm các trang web đã truy cập, chi tiết đăng nhập và dấu thời gian.

  Phân tích cookie thường liên quan đến việc kiểm tra các tệp cookie được lưu trữ trên máy tính hoặc trong thư mục dữ liệu của trình duyệt web. Tương tự như phân tích bộ đệm, các công cụ pháp y chuyên dụng hoặc kiểm tra thủ công có thể được sử dụng cho mục đích này. Bằng cách phân tích cookie, các nhà điều tra pháp y có thể phát hiện ra bằng chứng có giá trị liên quan đến hành vi trực tuyến của người dùng và tương tác với các trang web cụ thể.
- Phân tích lịch sử:

  Các trình duyệt web duy trì lịch sử duyệt web ghi lại các trang web mà người dùng đã truy cập. Thông tin lịch sử thường bao gồm các URL, dấu thời gian, tiêu đề trang và đôi khi là số lượt truy cập. Các nhà điều tra pháp y kỹ thuật số có thể phân tích lịch sử duyệt web để thiết lập dòng thời gian cho các hoạt động trực tuyến của người dùng và xác định các mẫu quan tâm.

  Phân tích lịch sử có thể được thực hiện bằng cách kiểm tra cơ sở dữ liệu lịch sử của trình duyệt hoặc bằng cách xem lại các tệp lịch sử được lưu trữ trên máy tính. Các công cụ pháp y chuyên dụng thường cung cấp các cách hiệu quả để trích xuất và phân tích thông tin này. Bằng cách phân tích lịch sử duyệt web, các nhà điều tra có thể phát hiện ra bằng chứng có giá trị như các trang web đã truy cập, tần suất truy cập và các mục có khả năng bị xóa hoặc sửa đổi.

Một số tool:

MZCacheView, MZCookieView, MZHistoryView, ChromeCacheView, ChromeCookieView, Chrome HistoryView,…

3.5. Phân thích Windows registry

Phân tích pháp y sổ đăng ký Windows giúp điều tra viên trích xuất các tạo phẩm pháp y như tài khoản người dùng, tệp được truy cập gần đây, hoạt động USB, chương trình chạy lần cuối và ứng dụng đã cài đặt.

Điều tra viên có thể kiểm tra sổ đăng ký Windows theo hai phương pháp sau:

- Phân tích tĩnh: Trong phương pháp này, các điều tra viên nên kiểm tra các tệp đăng ký có trong tệp bằng chứng thu được.
  Các tệp này nằm trong thư mục C:\Windows\System32\config.
- Phân tích trực tiếp: Trong phương pháp này, các điều tra viên sử dụng trình chỉnh sửa sổ đăng ký tích hợp sẵn để kiểm tra sổ đăng ký và các công cụ như FTK Imager để chụp các tệp đăng ký từ hệ thống trực tiếp để phân tích pháp y.

Để chụp các tệp đăng ký Windows trên hệ thống Live bằng FTK Imager:

- Mở FTK Imager và duyệt File>Obtain Protected Files
- Chọn Khôi phục mật khẩu và tất cả các tệp đăng ký (như trong ảnh chụp màn hình bên dưới) và cung cấp thư mục đích để giải nén các tệp
- Các tệp được hiển thị trong hình bên dưới là các khóa phụ của HKEY_LOCAL_MACHINE đã được xuất bằng FTK Imager từ một máy nghi ngờ trực tiếp

Các khóa con được trích xuất của HKEY_LOCAL_MACHINE chứa thông tin sau:

- SAM (Trình quản lý tài khoản bảo mật): Khóa con này lưu trữ thông tin về người dùng, tài khoản quản trị viên, tài khoản khách, hàm băm mật mã của mọi mật khẩu người dùng, v.v.
- Bảo mật: Khóa con này lưu trữ thông tin về chính sách bảo mật người dùng hiện tại
- Phần mềm: Khóa con này chứa thông tin về các ứng dụng phần mềm được cài đặt và cài đặt cấu hình của chúng trên hệ thống
- Hệ thống: Khóa con này lưu trữ thông tin về cài đặt cấu hình của trình điều khiển và dịch vụ phần cứng
- Mặc định: Khóa con này lưu trữ thông tin về cài đặt người dùng mặc định. Tuy nhiên, tệp NTUSER.dat liên quan đến người dùng hiện đang đăng nhập sẽ ghi đè cài đặt người dùng mặc định.

3.6. Phân tích tập tin Windows

Điểm khôi phục hệ thống (Tệp Change.log.x)

Các tệp ứng dụng và hệ thống chính được theo dõi liên tục để khôi phục hệ thống về trạng thái cụ thể. Thay đổi tập tin được ghi lại trong các thư mục. Các thay đổi đối với tệp được giám sát được phát hiện bởi trình điều khiển hệ thống tệp điểm khôi phục, tên tệp gốc được nhập vào tệp change.log cùng với số thứ tự, loại thay đổi đã xảy ra, v.v. Tệp được giám sát được giữ nguyên và sao chép vào thư mục điểm khôi phục và được đổi tên ở định dạng Axxxxxxx.ext, trong đó x đại diện cho số thứ tự và .ext là phần mở rộng ban đầu của tệp. Tệp change.log đầu tiên được thêm vào một số thứ tự và tệp change.log mới được tạo khi hệ thống được khởi động lại.

Các tệp tìm nạp trước

Các tệp tìm nạp trước lưu trữ thông tin về các ứng dụng đã được chạy trên hệ thống. Các tệp tìm nạp trước có thể đóng vai trò là nguồn bằng chứng pháp y có giá trị cho các nhà điều tra vì ngay cả khi các ứng dụng chạy trên hệ thống sau đó bị xóa hoặc gỡ cài đặt, thì các tệp tìm nạp trước liên quan đến các ứng dụng đó vẫn nằm trong thư mục tìm nạp trước tại C:\Windows\Prefetch .

Giá trị DWORD ở độ lệch 144 trong tệp tương ứng với số lần ứng dụng được khởi chạy. Giá trị DWORD ở độ lệch 120 trong tệp tương ứng với lần chạy ứng dụng cuối cùng, giá trị này được lưu

trữ ở định dạng UTC. Thông tin từ tệp .pf có thể tương quan với thông tin sổ đăng ký hoặc Nhật ký sự kiện để xác định ai đã đăng nhập vào hệ thống, ai đang chạy ứng dụng nào, v.v.

Tệp hình ảnh

Siêu dữ liệu có trong tệp hình ảnh JPEG phụ thuộc phần lớn vào ứng dụng đã tạo hoặc sửa đổi nó. Ví dụ: máy ảnh kỹ thuật số nhúng thông tin Định dạng tệp hình ảnh có thể trao đổi (EXIF) vào hình ảnh, có thể bao gồm kiểu máy và nhà sản xuất máy ảnh, thậm chí lưu trữ hình thu nhỏ hoặc thông tin âm thanh.

Bạn có thể sử dụng các công cụ như Exiv2, IrfanView và mô-đun Image::MetaData::JPEG Perl để xem, truy xuất và trong một số trường hợp sửa đổi siêu dữ liệu được nhúng trong các tệp hình ảnh JPEG. Các công cụ như ExifReader, Thư viện EXIF và ExifTool hiển thị dữ liệu EXIF được tìm thấy trong ảnh JPEG.

3.7. Điều tra bộ nhớ máy tính

Điều tra bộ nhớ: Phương pháp thu nhận

Góc độ điều tra mà bạn thực hiện trong giai đoạn mua lại này sẽ phụ thuộc chủ yếu vào tình huống mà bạn gặp phải và các yêu cầu của trường hợp. Điều này phụ thuộc phần lớn vào hệ điều hành mà máy chủ lưu trữ của bạn đang chạy hoặc vấn đề nhận thấy là gì cần được điều tra tại thời điểm xảy ra sự cố. Cách bạn chụp ảnh cũng phụ thuộc vào những gì bạn đang cố gắng thiết lập thông qua quá trình điều tra của mình và những gì bạn đang cố gắng chứng minh hoặc bác bỏ.

Nói chung, cuộc điều tra của bạn sẽ tập trung vào các hoạt động của người dùng trên hệ thống hoặc bằng chứng chứng minh rằng hệ thống được đề cập đã bị xâm phạm. Đôi khi, ngay cả các khóa mã hóa và mật khẩu cũng có thể bị phát hiện nếu chúng là một phần của các yêu cầu chứng cứ trong trường hợp của bạn. Phải có sự hiểu biết rõ ràng về những gì cần được thiết lập trên hệ thống mục tiêu và cách nó có thể giúp thúc đẩy quá trình điều tra của bạn.

Các nhà điều tra pháp y có tay nghề cao và có thể xác định hoạt động trên một hệ thống không nên có, cho phép họ chứng minh rằng một hệ thống đã bị xâm phạm. Nó cho phép họ xác định rootkit và phần mềm độc hại, tìm các quy trình bất thường và tiết lộ thông tin liên lạc bí mật, có thể làm sáng tỏ những gì đang xảy ra trong hệ thống mục tiêu.

Dưới đây là một số ví dụ về các định dạng thu nhận được sử dụng trong điều tra bộ nhớ. Có nhiều loại thu nhận bộ nhớ khác nhau, nhưng đây là năm trong số các phương pháp và định dạng phổ biến nhất được sử dụng ngày nay:

Định dạng RAW – Được trích xuất từ môi trường trực tiếp
Crash Dump – Thông tin được hệ điều hành thu thập
Tệp ngủ đông – Ảnh chụp nhanh đã lưu mà hệ điều hành của bạn có thể quay lại sau khi ngủ đông
Tệp trang – Đây là tệp lưu trữ thông tin tương tự được lưu trữ trong RAM hệ thống của bạn
Ảnh chụp nhanh VMWare – Đây là ảnh chụp nhanh của một máy ảo, giúp lưu trạng thái của nó như tại thời điểm chính xác mà ảnh chụp nhanh được tạo

Khi bạn đã có được dữ liệu của mình, bạn có thể bắt đầu quá trình kiểm tra hệ thống và mọi hoạt động đáng ngờ sau đó sẽ được phát hiện khi bạn tiếp tục. Khắc dữ liệu là một cách tiếp cận thường được sử dụng và tùy thuộc vào kết quả mong muốn của trường hợp cụ thể của bạn, có nhiều cách tiếp cận khác cũng có thể được xem xét. Dưới đây là danh sách một số công cụ thường được sử dụng trong lĩnh vực này cho phép sử dụng các phương pháp khác nhau này.

Một số tool:

- Volatility Suite: Đây là bộ chương trình mã nguồn mở để phân tích RAM và có hỗ trợ cho các hệ điều hành Windows, Linux và Mac. Nó có thể phân tích các kết xuất RAW, Crash, VMWare và Virtualbox mà không gặp vấn đề gì.
- Rekall: Đây là giải pháp toàn diện dành cho người ứng phó sự cố và điều tra viên, đồng thời có cả công cụ thu thập và phân tích. Nó có thể được coi là một bộ khung pháp y hơn là một ứng dụng đơn lẻ.
- Helix ISO: Đây là một đĩa CD trực tiếp có thể khởi động cũng như một ứng dụng độc lập giúp bạn dễ dàng ghi lại kết xuất bộ nhớ hoặc hình ảnh bộ nhớ của hệ thống. Có một số rủi ro liên quan đến việc chạy ứng dụng này trực tiếp trên hệ thống đích, cụ thể là dấu chân mua lại, vì vậy hãy đảm bảo rằng nó phù hợp với yêu cầu của bạn.
- Belkasoft RAM Capturer: Đây là một công cụ pháp y khác cho phép ghi lại phần không ổn định của bộ nhớ hệ thống vào một tệp. Những người phản hồi đầu tiên sẽ thấy rằng chức năng và nhiều loại công cụ có sẵn trong gói phần mềm này sẽ cho phép cuộc điều tra của họ bắt đầu nhanh nhất có thể.
- Process Hacker: Đây là một ứng dụng giám sát tiến trình mã nguồn mở rất hữu ích để chạy trong khi máy mục tiêu đang được sử dụng. Nó sẽ giúp điều tra viên hiểu rõ hơn về những gì hiện đang ảnh hưởng đến hệ thống trước khi chụp nhanh bộ nhớ và có thể giúp phát hiện ra bất kỳ quy trình độc hại nào hoặc thậm chí giúp xác định quy trình nào đã bị chấm dứt trong một khoảng thời gian nhất định. thời gian.

Câu hỏi và bài tập

Chương 4. Điều tra trên Linux

4.1. Khái niệm cơ bản

Giới thiệu về pháp y Linux

Linux là một hệ điều hành nguồn mở được sử dụng rộng rãi trong các tổ chức. Với sự gia tăng của tội phạm mạng, điều quan trọng đối với các nhà điều tra pháp y là phải được trang bị đầy đủ kiến thức về thu thập các hiện vật từ các máy Linux theo cách hợp pháp về mặt pháp y.

Điều tra Linux liên quan đến việc sử dụng các lệnh/công cụ khác nhau để truy xuất, kiểm tra và phân tích các hiện vật có giá trị liên quan đến các sự cố tội phạm mạng liên quan đến máy Linux.

Mặt khác, việc sử dụng máy trạm điều tra Linux đóng vai trò là nền tảng rất hiệu quả để điều tra các sự cố bảo mật liên quan đến hệ thống Linux vì chúng cung cấp hỗ trợ rộng rãi cho một số hệ thống tệp và dễ dàng truy cập vào các công cụ điều tra kỹ thuật số tiên tiến.

4.2. Các lệnh Shell

Thu thập tên máy chủ, ngày và giờ

Hostname, date, uptime

Thu thập thông tin mạng

netstat -i, ip addr show, ifconfig
Xem bảng định tuyến mạng
Ip r, netstat -rn
Thu thập thông tin các cổng mở
Nmap -sT localhost, -sU
Tìm các chương trình/tiến trình được liên kết với một cổng
Netstat -tulpn, lsof -I -p -n | grep LISTEN
Thu thập dữ liệu trên các tệp mở
Lsof

4.3. Linix Log Files

Tệp nhật ký Linux

Tệp nhật ký là bản ghi của tất cả các hoạt động được thực hiện trên một hệ thống. Tệp nhật ký Linux lưu trữ thông tin về nhân của hệ thống và các dịch vụ đang chạy trong hệ thống. Trong môi trường Linux, các tệp nhật ký khác nhau chứa các loại thông tin khác nhau. Điều này giúp các nhà điều tra phân tích các vấn đề khác nhau trong một sự cố an ninh. Hiểu nội dung của các tệp nhật ký khác nhau có thể giúp các nhà điều tra pháp y xác định bằng chứng tiềm ẩn trên hệ thống trong các sự cố bảo mật.

Trên đây là một số địa chỉ tệp nhật ký Linux có thể hữu ích cho các nhà điều tra khi tiến hành kiểm tra pháp y đối với máy Linux.

Thu thập thông tin tệp lịch sử người dùng và xem các tệp và thư mục ẩn

Nếu bash shell có sẵn trên hệ thống Linux, mọi lệnh do người dùng chạy sẽ được lưu trữ trong một tệp ẩn có tên .bash_history, tệp này được lưu trong thư mục chính của mỗi người dùng.

Điều tra viên có thể sử dụng lệnh history để xem các lệnh đã chạy trước đó trên hệ thống như được lưu trữ trong tệp bash_history.

Điều tra viên cũng có thể xem các tệp và thư mục ẩn bằng cách chạy lệnh ls -al. Các hình sau đây cho thấy việc thực thi các lệnh history và ls -al tương ứng.

Thu thập thông tin đáng ngờ

rkhunter --check --rwo
chrootkit

Phân tích chữ ký tệp

Xxd - <File_name.ext> | head

4.4. Hệ thống cây thư mục

Trong pháp y kỹ thuật số, việc phân tích hệ thống Linux thường liên quan đến việc kiểm tra hệ thống tệp và cấu trúc thư mục của nó, thường được gọi là cây thư mục hoặc cây thư mục. Dưới đây là tổng quan ngắn gọn về cấu trúc thư mục điển hình trong Linux:

Root ("/"): Thư mục gốc là thư mục cấp cao nhất trong hệ thống phân cấp hệ thống tệp Linux. Tất cả các thư mục và tệp khác được đặt trong thư mục gốc.

Các tệp nhị phân ("/bin" và "/sbin"): Các thư mục này chứa các tệp nhị phân và chương trình thực thi thiết yếu. Thư mục "/bin" thường chứa các tệp nhị phân người dùng phổ biến, trong khi thư mục "/sbin" chứa các tệp nhị phân hệ thống được sử dụng cho các tác vụ quản trị.

Cấu hình hệ thống ("/etc"): Thư mục "/etc" lưu trữ các tệp cấu hình hệ thống. Điều này bao gồm cấu hình mạng, thông tin tài khoản người dùng, tập lệnh khởi động, v.v.

Thư mục chính của người dùng ("/home"): Mỗi người dùng trên hệ thống Linux thường có một thư mục chuyên dụng trong "/home" đóng vai trò là thư mục chính của họ. Các tệp và cấu hình dành riêng cho người dùng được lưu trữ tại đây.

Tệp tạm thời ("/tmp"): Thư mục "/tmp" được sử dụng để lưu trữ tệp tạm thời. Nó chứa các tệp được tạo bằng cách chạy các quy trình hoặc tập lệnh và nội dung của nó thường bị xóa khi khởi động lại hệ thống.

Thư viện ("/lib" và "/lib64"): Các thư mục này chứa các thư viện được chia sẻ theo yêu cầu của các chương trình và tệp nhị phân khác nhau trong hệ thống. Thư mục "/lib" được sử dụng cho các thư viện 32 bit, trong khi "/lib64" chứa các thư viện 64 bit.

Tệp thiết bị ("/dev"): Thư mục "/dev" chứa các tệp thiết bị đại diện cho các thiết bị vật lý và logic trên hệ thống, chẳng hạn như ổ cứng, phân vùng, thiết bị đầu cuối và thiết bị đầu vào/đầu ra.

Tệp hạt nhân ("/boot"): Thư mục "/boot" lưu trữ các tệp cần thiết để khởi động hệ thống Linux, bao gồm ảnh hạt nhân, cấu hình bộ tải khởi động và đĩa RAM ban đầu (initrd).

Nhật ký hệ thống ("/var/log"): Tệp nhật ký hệ thống được lưu trữ trong thư mục "/var/log". Các nhật ký này chứa thông tin về các sự kiện, dịch vụ và quy trình hệ thống khác nhau, có thể hữu ích trong điều tra pháp y.

Tệp cấu hình ("/etc/sysconfig" và "/etc/default"): Những thư mục này chứa các tệp cấu hình dành riêng cho một số dịch vụ hệ thống và daemon.

Tệp ứng dụng ("/ usr"): Thư mục "/ usr" chứa các ứng dụng do người dùng cài đặt và các tệp liên quan của chúng, bao gồm tệp nhị phân, thư viện, tài liệu và tài nguyên được chia sẻ.

Tệp cấu hình ("/etc/opt"): Thư mục này lưu trữ các tệp cấu hình cho các gói phần mềm tùy chọn được cài đặt trên hệ thống.

Điều quan trọng cần lưu ý là cấu trúc thư mục thực tế có thể khác nhau tùy thuộc vào bản phân phối Linux và thiết lập cụ thể của hệ thống được phân tích. Ngoài ra, có thể có các thư mục và tệp bổ sung tùy thuộc vào phần mềm đã cài đặt, cấu hình người dùng và thực tiễn quản trị hệ thống.

4.5. Hệ thống tập tin Linux

Sleuth Kit (TSK) cho phép bạn điều tra ảnh đĩa. Chức năng cốt lõi của nó cho phép bạn phân tích khối lượng và dữ liệu hệ thống tệp. Khung trình cắm cho phép bạn kết hợp các mô-đun bổ sung để phân tích nội dung tệp và xây dựng hệ thống tự động. Phần này sẽ khám phá các lệnh TSK có thể giúp điều tra để xem và kiểm tra các hệ thống tệp.

Lênh: fsstat -t raw Evidence.dd

fls -I <image_type> <imgfile_name>

istat -f <fstype> -I <imgtype> <imgfile_name> <inode_number>

Câu hỏi và bài tập

Tài liệu tham khảo: **CHFIv10**