**Tổng kết**

**Chương 1**

Trong chương này, chúng ta đã xem xét khoa học pháp y, đặc biệt là pháp y kỹ thuật số, là gì và không. Khoa học pháp y không phải là những bộ phim truyền hình giải quyết tội phạm có nhịp độ nhanh mà chúng ta xem trên truyền hình, mà là một phương pháp thu thập, điều tra và phân tích khoa học được sử dụng để giải quyết một số loại vấn đề pháp lý. Pháp y kỹ thuật số không chỉ giới hạn ở máy tính. Nó bao gồm bất kỳ loại thiết bị điện tử nào có thể lưu trữ dữ liệu. Những thiết bị này bao gồm điện thoại di động, máy tính bảng và đơn vị GPS chỉ để gọi tên một số thiết bị.

Pháp y kỹ thuật số có thể áp dụng tốt ngoài điều tra tội phạm. Nó được sử dụng thường xuyên trong các vụ kiện dân sự, các vấn đề tình báo quốc gia và quân sự cũng như khu vực tư nhân.

Điểm lưu ý:

1. Định nghĩa của các loại hình điều tra: Hình sự, Dân sự, Quản trị viên điều tra mạng
2. Định nghĩa khoa học pháp y kỹ thuật số

**Chương 2**

Trong Chương 2, chúng ta đã xem xét kỹ hơn cách máy tính lưu trữ dữ liệu ở các dạng khác nhau bao gồm từ tính, quang học, flash và các dạng khác. Mỗi phương pháp lưu trữ này là khác nhau và những khác biệt đó có ý nghĩa pháp lý. Máy tính hoạt động với cả bộ nhớ và bộ lưu trữ. Mặc dù chúng nghe có vẻ giống nhau, nhưng mục đích dự định của chúng lại khác nhau rõ ràng. Bộ nhớ lưu giữ dữ liệu mà máy tính đang hoạt động tích cực vào lúc này. Nó dễ bay hơi, có nghĩa là nó giữ dữ liệu miễn là nó có sức mạnh. Khi nguồn điện bị ngắt, dữ liệu bắt đầu biến mất. RAM trong máy tính của bạn được sử dụng cho bộ nhớ.

Ngược lại, lưu trữ được sử dụng để lưu trữ lâu dài dữ liệu. Lưu trữ được coi là bất biến vì dữ liệu vẫn còn ngay cả khi thiết bị mất nguồn. Ổ cứng của bạn là một ví dụ về lưu trữ.

Hệ thống tệp của máy tính là trọng tâm của cách nó lưu và truy xuất dữ liệu. Hệ thống tệp theo dõi các phần dữ liệu khác nhau phải được tìm thấy và hoàn nguyên để mở tệp. Ngày nay, có nhiều hệ thống tệp được sử dụng, mỗi hệ thống có cách hoạt động riêng.

Điểm lưu ý:

1. Định nghĩa của bộ nhớ tạm thời (ví dụ RAM, CPU)
2. Định nghĩa của bộ nhớ lưu trữ lâu dài (ví dụ HDD, SSD)
3. Ảnh hưởng của việc tắt/mở nguồn điện

**Chương 4**

Như chúng ta đã thảo luận trong chương này, bước đầu tiên trong quá trình thu thập là bảo mật cả hiện trường và bằng chứng. Nếu thiết bị chứa bằng chứng là điện thoại di động, bạn sẽ cần phải cách ly điện thoại khỏi tín hiệu mạng để ngăn bằng chứng bị phá hủy.

Các bức ảnh là một cách tuyệt vời để ghi lại bằng chứng và hiện trường. Bạn sẽ chụp toàn bộ khung cảnh (ví dụ: toàn bộ căn phòng, không chỉ máy tính trên bàn làm việc). Bạn phải đảm bảo rằng chuỗi hành trình được ghi chép đầy đủ và bằng chứng được đánh dấu thích hợp.

Bảo quản bằng chứng là rất quan trọng. Chụp ảnh pháp y hoặc nhân bản giúp loại bỏ nhu cầu kiểm tra bằng chứng ban đầu. Việc xem xét bản gốc có thể dẫn đến việc loại trừ bằng chứng.

Sao chép thiết bị sẽ tạo ra một bản sao chính xác từng chút một của bằng chứng gốc. Giá trị băm được sử dụng để xác minh rằng bằng chứng được sao chép giống với bản gốc. Các giá trị băm này, chẳng hạn như MD5 hoặc SHA1, thường được ví như “DNA kỹ thuật số” hoặc “Vân tay kỹ thuật số”. Báo cáo cuối cùng phải bao gồm chi tiết về hiện trường, quá trình thu thập, phân tích và kết luận nào, nếu có, đã đạt được. Điều quan trọng là báo cáo cuối cùng phải dễ hiểu đối với khán giả không chuyên về kỹ thuật.

Điểm lưu ý:

1. Quy trình thu thập bằng chứng: Chụp ảnh hiện trường -> tạo bản sao -> bảo quản bằng chứng -> Xác minh bằng giá trị băm -> phân tích tại phòng thí nghiệm -> báo cáo cuối (chi tiết hiện trường, quá trình thu thập, và thách thức đối với dữ liệu thu thập được như nguồn thu thập, tình trạng bằng chứng)
2. Điều quan trọng là báo cáo cuối cùng phải dễ hiểu đối với dân không chuyên về kỹ thuật
3. Giá trị băm là gì? ảnh hưởng của giá trị băm?

**Chương 5**

Máy tính ghi lại một lượng lớn thông tin mà đại đa số người dùng không biết. Các hiện vật này có nhiều dạng và có thể tìm thấy trên toàn hệ thống. Ví dụ: có thể xác định các thiết bị lưu trữ bên ngoài, như ổ USB, đã được gắn vào hệ thống. Các mục được chuyển đến Thùng rác của Windows có thể cho chúng tôi biết khi nào chúng bị xóa và theo tài khoản nào.

Ngay cả khi tệp đã bị xóa hoặc bị ghi đè, các bản sao của tệp vẫn có thể tồn tại trên ổ đĩa ở nhiều dạng. Các bản sao thường bị bỏ qua này được tạo ra bởi lệnh in và chức năng ngủ đông cũng như các điểm khôi phục. Các tệp này cũng có thể được tìm thấy trong không gian hoán đổi, một phần cụ thể của ổ cứng được sử dụng khi hệ thống hết RAM.

Một điểm rút ra chính từ chương này là bằng chứng có giá trị về các tệp, hành động hoặc sự kiện cụ thể có thể được ghi lại ở nhiều vị trí. Như vậy, thực sự loại bỏ nó có thể là một quá trình kỹ thuật cao ngoài tầm với của hầu hết những kẻ gian.

Ngay cả việc xóa dữ liệu và chống phân mảnh ổ cứng của bạn cũng không thoát khỏi nó. Máy tính lưu trữ dữ liệu theo cách cho phép khắc các đoạn tệp cũ hơn để phân tích thêm. Các tệp một phần được xóa khỏi không gian chùng chỉ có thể chứa đủ thông tin để trở thành một bằng chứng hữu ích.

Hệ thống và các ứng dụng chúng tôi sử dụng tạo ra dữ liệu về dữ liệu. Thông tin này, được gọi là siêu dữ liệu, có thể cho chúng tôi biết khi nào tệp được tạo, truy cập, sửa đổi và xóa. Biết phần mềm nào đã được cài đặt và chạy có thể liên quan đến một cuộc điều tra. Ví dụ, phần mềm xóa ổ đĩa có thể được quan tâm đặc biệt. Windows Registry và Windows Explorer là nguồn cung cấp thông tin thông dụng.

Điểm lưu ý:

1. Định nghĩa Windows Registry
2. Định nghĩa Windows Explorer
3. Bằng chứng có giá trị về các tệp, hành động hoặc sự kiện cụ thể có thể được ghi lại ở nhiều vị trí. Ngay cả việc xóa dữ liệu và chống phân mảnh ổ cứng của bạn cũng không thoát khỏi nó.
4. Hành động thực sự của máy tính khi ta xóa 1 tệp vào Recycle Bin

**Chương 6**

Các công cụ và kỹ thuật chống pháp y có thể có tác động đáng kể đến việc kiểm tra pháp y đối với máy tính. Để làm thất vọng các giám khảo, các đối tượng thường cố gắng che giấu dữ liệu buộc tội theo một cách nào đó hoặc cố gắng phá hủy nó hoàn toàn. Mã hóa là một trong những hình thức ẩn dữ liệu phổ biến nhất và tiềm năng nhất. Mã hóa mạnh mẽ có sẵn miễn phí trên Internet và được bao gồm trong một số phiên bản của cả hệ điều hành Microsoft và Apple. Những công cụ này có thể làm cho việc khôi phục dữ liệu đã mã hóa trên thực tế là không thể.

Nếu gặp phải sự cố mã hóa, nó có thể bị tấn công theo nhiều cách khác nhau. Trong một cuộc tấn công bạo lực, mọi mật khẩu có thể được thử cho đến khi tìm thấy mật khẩu phù hợp. Đây là cuộc tấn công chậm nhất và ít được mong đợi nhất trong số các cuộc tấn công. Tăng sức mạnh xử lý được sử dụng trong một cuộc tấn công có thể giảm thời gian cần thiết để phá vỡ mật khẩu. Một số ứng dụng được bảo vệ bằng mật khẩu có các lỗ hổng có thể bị khai thác. Những lỗ hổng này có thể cho phép chúng tôi đặt lại mật khẩu theo một trong những lựa chọn của chúng tôi.

Từ điển có thể được tạo và sử dụng để phá mật khẩu. Chúng có thể bao gồm từ điển tiêu chuẩn đến từ điển tùy chỉnh dựa trên thông tin cụ thể cho mục tiêu. Tên vật nuôi, sở thích, mối quan tâm và ngày sinh chỉ là một số chi tiết có thể tạo ra một từ điển tùy chỉnh.

Tin nhắn hoặc dữ liệu có thể bị ẩn trong các tệp khác. Trong một quá trình được gọi là steganography, các tệp (được gọi là tải trọng) được chèn vào các tệp khác như ảnh hoặc phim (được gọi là tệp mạng). Steganography có thể rất khó phát hiện. Nếu nó được phát hiện, nó cũng có thể chứng tỏ khó trích xuất tin nhắn từ tệp nhà cung cấp dịch vụ.

Đối tượng có thể chọn hủy dữ liệu bằng một công cụ xóa ổ đĩa có bán trên thị trường. Hiệu quả của những công cụ này thường không đạt. Dữ liệu vẫn có thể được phục hồi ngay cả khi công cụ đã được sử dụng. Ngay cả khi dữ liệu đã được xóa thành công, phần mềm có thể để lại dấu hiệu cho thấy việc sử dụng chúng. Bằng chứng về việc sử dụng chúng cũng có thể là bằng chứng mạnh mẽ.

Điểm lưu ý:

1. Tấn công tài liệu được mã hóa (bằng mật khẩu/Brute Force – Dictionary Attacks – Rainbow Table)
2. Steganography, các tệp (được gọi là tải trọng) được chèn vào các tệp khác như ảnh hoặc phim
3. Phần mềm chống lại điều tra số (mã hóa, xóa dữ liệu) có thể để lại dấu hiệu cho thấy việc sử dụng chúng. Bằng chứng về việc sử dụng chúng cũng có thể là bằng chứng mạnh mẽ

**Chương 8**

Internet hoạt động phần lớn nhờ vào hai giao thức, cụ thể là HTTP và TCP / IP. Một công nghệ rất phổ biến khác được sử dụng rộng rãi là HTML hoặc Ngôn ngữ đánh dấu siêu văn bản. HTML là một trong những ngôn ngữ chính được sử dụng để xây dựng các trang web. Trong pháp y kỹ thuật số, bằng chứng có thể được tìm thấy trong mã này, vì vậy nó được coi là người kiểm tra chúng tôi có thể điều hướng thông qua nó để tìm bất kỳ bằng chứng hiện có nào.

Chúng tôi cũng đã xem xét cách các trang web được tìm thấy và gửi đến các trình duyệt bằng cách sử dụng Bộ định vị tài nguyên thống nhất (URL) và Máy chủ tên miền (DNS).

Mạng ngang hàng (P2P) có thể được sử dụng để chia sẻ không chỉ nhạc và phim vi phạm bản quyền mà còn cả nội dung lậu.

Chương 8 cũng xem xét một số hiện vật được tạo ra từ việc sử dụng Internet và e-mail. Điều này bao gồm những thứ như bản ghi INDEX.DAT, Tệp Internet Tạm thời (TIF), tệp NTUSER.DAT, cookie và tiêu đề e-mail. Việc truy tìm nguồn gốc của một e-mail không phải là việc dễ dàng vì thông tin nhận dạng có thể bị giả mạo hoặc xóa bỏ.

Ứng dụng khách trò chuyện và nhật ký liên quan của họ rất đáng được kiểm tra nếu được tìm thấy trên máy tính. Hãy nhớ rằng, ghi nhật ký có thể không được bật theo mặc định.

Internet Relay Chat (IRC) và ICQ là hai phương thức giao tiếp Internet không thể bỏ qua. Đây là hai trong số những cách phổ biến nhất để bọn tội phạm (và những kẻ khác liên quan đến giao tiếp riêng tư) giúp che dấu vết của chúng.

Mạng xã hội ngày nay được sử dụng rộng rãi trên toàn thế giới bởi một lượng lớn người. Bằng chứng mạng xã hội có thể được tìm thấy cục bộ và từ xa trên mạng của nhà cung cấp.

Điểm lưu ý:

1. Các trang web được tìm thấy và gửi đến các trình duyệt bằng cách sử dụng Bộ định vị tài nguyên thống nhất (URL) và Máy chủ tên miền (DNS).
2. Mạng ngang hàng (P2P) có thể được sử dụng để chia sẻ không chỉ nhạc và phim vi phạm bản quyền mà còn cả nội dung lậu.
3. Thu thập bằng chứng thông qua bản ghi lịch sử trình duyệt web, INDEX.DAT, Tệp Internet Tạm thời (TIF), tệp NTUSER.DAT, cookie và tiêu đề e-mail.
4. IRC (hệ thống dành cho diễn đàn, nhóm trao đổi), ICQ (Yahoo), IM (Facebook)

**Chương 9**

An ninh mạng phải là một mối quan tâm lớn đối với tất cả chúng ta. Mạng và PC của chúng tôi gần như đang bị tấn công liên tục từ các tin tặc đơn độc, tội phạm có tổ chức và nước ngoài. Tội phạm mạng, chiến tranh mạng và khủng bố mạng là những vấn đề lớn đe dọa không chỉ các quốc gia và công ty của chúng ta, mà còn cả máy tính cá nhân của chúng ta. Từ quan điểm pháp y, mạng đại diện cho một thách thức lớn hơn nhiều. Chúng rất khác nhau về kích thước và độ phức tạp. Có một số công cụ giúp chúng tôi bảo vệ cơ sở hạ tầng mạng quan trọng của mình, bao gồm tường lửa và hệ thống phát hiện xâm nhập. Các tổ chức thông minh lên kế hoạch trước cho các vi phạm bảo mật, cho phép họ phản ứng hiệu quả và hiệu quả, giảm thiểu thiệt hại và tăng khả năng họ có thể xác định (các) thủ phạm.

Điểm lưu ý:

1. Tường lửa và hệ thống phát hiện xâm nhập giúp phòng thí nghiệm, điều tra viên bảo vệ dữ liệu không gian mạng
2. Điều tra bằng chứng có trên tường lửa (nhật ký, ví dụ Windows Defender/AV báo cáo khi có phân mềm nguy hại được cài đặt/chạy trên thiết bị máy)
3. Điều tra bằng chứng có trên hệ thống phát hiện xâm nhập (nhật ký, ví dụ SIEM/SOAR báo cáo và xử lý khi tin tặc tấn công thông qua không gian mạng)

https://manytools.org/hacker-tools/steganography-encode-text-into-image/go/