Lời nói đầu

Giáo trình cơ bản điều tra số (khoa học pháp y) được biên dịch, tóm tắt, trình bày dựa trên cuốn sách “The Basics of Digital Forensics” được viết bởi John Sammon. Cuốn sách này là một trong những cuốn sách được đề cử hàng đầu bởi rất nhiều trường đại học, cao học, và điều tra viên danh tiếng khi bạn muốn tìm hiểu cơ bản về điều tra số. Tuy nhiên, do cuốn sách này được viết dựa trên tư pháp, môi trượng tại Hoa Kỳ, nên một số điều luật, hành động tư pháp, sự kiện sẽ chỉ mang tính chất tham khảo. Ngoài ra, cuối các chương đều được tổng kết kiến thức từ cuốn sách này và những kiến thức mới theo thời gian nhằm liên tục làm mới giáo trình.

Pháp y kỹ thuật số được sử dụng để giữ cho chúng ta an toàn, đảm bảo công lý được thực hiện và các nguồn lực của công ty và cá nhân không bị lạm dụng. Giáo trình này là bước đầu tiên của bạn vào thế giới pháp y kỹ thuật số. Chào mừng!

Pháp y kỹ thuật số được sử dụng rất nhiều trong đời sống, không chỉ trong việc bắt những kẻ trộm danh tính và những kẻ săn mồi trên Internet. Ví dụ, nó đang được sử dụng trên chiến trường Afghanistan để thu thập thông tin tình báo. Việc khai thác nhanh chóng các thông tin thu được từ điện thoại di động và các thiết bị khác giúp quân đội xác định và loại bỏ những kẻ khủng bố và quân nổi dậy.

Nó được sử dụng trong thế giới hàng tỷ đô la của các vụ kiện dân sự. Đã qua rồi cái thời mà các bên đối lập trao đổi những hộp giấy ghi nhớ, thư từ và báo cáo như một phần của quá trình kiện tụng. Ngày nay, những tài liệu đó được viết bằng 1s và 0s chứ không phải bằng mực. Chúng được lưu trữ gấp nhiều lần trên ổ cứng và băng dự phòng hơn là trong tủ đựng hồ sơ.

Pháp y kỹ thuật số giúp kiểm soát và chống lại sự gia tăng của tội phạm mạng. Những kẻ trộm danh tính, những kẻ lừa đảo và những tên tội phạm “thế hệ cũ” đều đang sử dụng và tận dụng công nghệ để tạo điều kiện cho các hoạt động bất hợp pháp của chúng.

Cuối cùng, điều tra số được sử dụng ở nơi làm việc để giúp bảo vệ cả các công ty và tổ chức chính phủ khỏi việc lạm dụng hệ thống máy tính của họ.

Mục lục

[**A. Đối tượng độc giả của giáo trình 9**](#_Toc117846331)

[**B. Cấu trúc của giáo trình này 10**](#_Toc117846332)

[Chương 1 - Giới thiệu 10](#_Toc117846333)

[Chương 2 - Các khái niệm kỹ thuật chính 10](#_Toc117846334)

[Chương 3 - Phòng thí nghiệm và Công cụ 10](#_Toc117846335)

[Chương 4 - Thu thập bằng chứng 11](#_Toc117846336)

[Chương 5 - Phần mềm Hệ thống Windows 11](#_Toc117846337)

[Chương 6 – Kỹ thuật chống lại điều tra số 11](#_Toc117846338)

[Chương 8 - Internet và E-Mail 11](#_Toc117846339)

[Chương 9 - Pháp y mạng 11](#_Toc117846340)

[Chương 10 - Pháp y thiết bị di động 12](#_Toc117846341)

[Chương 11 - Nhìn về phía trước: Thử thách và Mối quan tâm 12](#_Toc117846342)

[I. Chương 1: Giới thiệu 12](#_Toc117846343)

[1. Giới thiệu 13](#_Toc117846344)

[2. Khoa học pháp y là gì? 14](#_Toc117846345)

[3. Pháp y kỹ thuật số là gì? 14](#_Toc117846346)

[4. Sử dụng pháp y kỹ thuật số 15](#_Toc117846347)

[4.1 Điều tra hình sự 15](#_Toc117846348)

[4.2 Tố tụng dân sự 16](#_Toc117846349)

[4.3 Sự thông minh 17](#_Toc117846350)

[4.4 Các vấn đề quản trị 18](#_Toc117846351)

[5. Nguyên tắc trao đổi của Locard 19](#_Toc117846352)

[6. Phương pháp khoa học 20](#_Toc117846353)

[7. Tổ chức ghi chú 20](#_Toc117846354)

[7.1 Nhóm công tác khoa học về bằng chứng kỹ thuật số 20](#_Toc117846355)

[7.2 Viện hàn lâm khoa học pháp y Hoa Kỳ 21](#_Toc117846356)

[7.3 Hội đồng Giám đốc Phòng thí nghiệm điều tra tội phạm Hoa Kỳ / Ban Công nhận Phòng thí nghiệm 21](#_Toc117846357)

[7.4 Viện Tiêu chuẩn và Công nghệ Quốc gia (NIST) 22](#_Toc117846358)

[7.5 Hiệp hội Vật liệu và Thử nghiệm Hoa Kỳ (ASTM) 22](#_Toc117846359)

[8. Vai trò của Giám định viên pháp y trong hệ thống tư pháp 22](#_Toc117846360)

[8.1 Hiệu ứng CSI 23](#_Toc117846361)

[9. Bản tóm tắt 23](#_Toc117846362)

[10. Tổng kết và kiến thức thêm chương 1 24](#_Toc117846363)

[II. Chương 2: Các khái niệm kỹ thuật chính 28](#_Toc117846364)

[1. Giới thiệu 28](#_Toc117846365)

[2. Lược đồ bit, byte và đánh số 29](#_Toc117846366)

[2.1 Hệ thập lục phân 29](#_Toc117846367)

[2.2 Nhị phân thành văn bản: ASCII và Unicode 30](#_Toc117846368)

[3. Phần mở rộng Tệp và Chữ ký Tệp 30](#_Toc117846369)

[4. Lưu trữ và bộ nhớ 32](#_Toc117846370)

[4.1 Đĩa từ tính 32](#_Toc117846371)

[4.2 Bộ nhớ flash 33](#_Toc117846372)

[4.3 Lưu trữ quang học 34](#_Toc117846373)

[4.4 Bộ nhớ lưu trữ so với tạm thời 34](#_Toc117846374)

[5. Môi trường máy tính 35](#_Toc117846375)

[5.1 Điện toán đám mây 35](#_Toc117846376)

[6. Loại dữ liệu 36](#_Toc117846377)

[6.1 Dữ liệu hoạt động 36](#_Toc117846378)

[6.2 Dữ liệu tiềm ẩn 37](#_Toc117846379)

[6.3 Dữ liệu lưu trữ 37](#_Toc117846380)

[7. Hệ thống tệp 37](#_Toc117846381)

[8. Không gian được phân bổ và chưa được phân bổ 38](#_Toc117846382)

[8.1 Độ bền dữ liệu 38](#_Toc117846383)

[9. Cách ổ cứng từ tính lưu trữ dữ liệu 39](#_Toc117846384)

[9.1 Tệp Trang (hoặc Hoán đổi Không gian) 42](#_Toc117846385)

[10. Chức năng máy tính cơ bản — Kết hợp tất cả lại với nhau 43](#_Toc117846386)

[11. Bản tóm tắt 44](#_Toc117846387)

[12. Tổng kết và kiến thức thêm chương 2 45](#_Toc117846388)

[III. Chương 3: Phòng thí nghiệm và Công cụ 50](#_Toc117846389)

[1. Giới thiệu 50](#_Toc117846390)

[2. Phòng thí nghiệm pháp y 50](#_Toc117846391)

[2.1 Phòng thí nghiệm ảo 51](#_Toc117846392)

[2.2 Bảo mật phòng thí nghiệm 52](#_Toc117846393)

[2.3 Lưu trữ bằng chứng 53](#_Toc117846394)

[3. Chính sách và thủ tục 53](#_Toc117846395)

[4. Đảm bảo chất lượng 53](#_Toc117846396)

[4.1 Xác thực công cụ 55](#_Toc117846397)

[4.2 Tài liệu 55](#_Toc117846398)

[5. Công cụ pháp y kỹ thuật số 58](#_Toc117846399)

[5.1 Lựa chọn công cụ 58](#_Toc117846400)

[5.2 Phần cứng 59](#_Toc117846401)

[5.3 Phần mềm 61](#_Toc117846402)

[6. Sự công nhận 64](#_Toc117846403)

[6.1 Hiệp hội Vật liệu và Thử nghiệm Hoa Kỳ (ASTM) 65](#_Toc117846404)

[6.2 Công nhận so với chứng nhận 66](#_Toc117846405)

[7. Bản tóm tắt 66](#_Toc117846406)

[8. Tổng kết và kiến thức thêm chương 3 67](#_Toc117846407)

[IV. Chương 4: Thu thập bằng chứng 71](#_Toc117846408)

[1. Giới thiệu 71](#_Toc117846409)

[2. Hiện trường vụ án và thu thập bằng chứng 72](#_Toc117846410)

[2.1 Phương tiện có thể tháo rời 72](#_Toc117846411)

[2.2 Điện thoại di động 73](#_Toc117846412)

[2.2.1 Thứ tự biến động 75](#_Toc117846413)

[4. Ghi lại hiện trường, quá trình 75](#_Toc117846414)

[4.1 Nhiếp ảnh 76](#_Toc117846415)

[4.2 Ghi chú 77](#_Toc117846416)

[5. Chuỗi hành trình 78](#_Toc117846417)

[5.1 Đánh dấu bằng chứng 78](#_Toc117846418)

[6. Sao y 79](#_Toc117846419)

[6.1 Mục đích của sao y 80](#_Toc117846420)

[6.2 Quá trình sao y 81](#_Toc117846421)

[6.3 Phương tiện sạch về mặt pháp lý 81](#_Toc117846422)

[6.4 Định dạng hình ảnh pháp y 82](#_Toc117846423)

[6.5 Rủi ro và thách thức 82](#_Toc117846424)

[6.6 Giá trị trong eDiscovery 82](#_Toc117846425)

[7. Hệ thống sống và hệ thống chết 83](#_Toc117846426)

[7.1 Mối quan tâm về chuyển đổi trực tiếp 83](#_Toc117846427)

[7.2 Lợi thế của Bộ sưu tập Trực tiếp 84](#_Toc117846428)

[7.3 Nguyên tắc thu thập trực tiếp 85](#_Toc117846429)

[7.4 Tiến hành và ghi lại một bộ sưu tập trực tiếp 85](#_Toc117846430)

[8. Băm 86](#_Toc117846431)

[8.1 Các loại thuật toán băm 86](#_Toc117846432)

[8.2 Ví dụ về băm 86](#_Toc117846433)

[8.3 Sử dụng băm 87](#_Toc117846434)

[9. Bản báo cáo cuối 88](#_Toc117846435)

[10. Bản tóm tắt 88](#_Toc117846436)

[11. Tổng kết và kiến thức thêm chương 4 89](#_Toc117846437)

[V. Chương 5: Phần mềm Hệ thống Windows 95](#_Toc117846438)

[Thông tin trong Chương này: 95](#_Toc117846439)

[1. Giới thiệu 95](#_Toc117846440)

[2. Dữ liệu đã xóa 96](#_Toc117846441)

[3. Tệp ngủ đông (Hiberfile.Sys) 96](#_Toc117846442)

[3.1 Ngủ 97](#_Toc117846443)

[3.2 Ngủ đông 97](#_Toc117846444)

[3.3 Ngủ lai 97](#_Toc117846445)

[4. Windows Registry 97](#_Toc117846446)

[4.1 Cấu trúc sổ đăng ký 98](#_Toc117846447)

[4.1.3 Ghi lại 99](#_Toc117846448)

[4.2 Ổ đĩa bên ngoài 100](#_Toc117846449)

[5. In Spooling 100](#_Toc117846450)

[6. Thùng rác 101](#_Toc117846451)

[7. Metadata 103](#_Toc117846452)

[7.1 Xóa siêu dữ liệu 105](#_Toc117846453)

[8. Bộ nhớ cache hình thu nhỏ 107](#_Toc117846454)

[9. Được sử dụng gần đây nhất (MRU) 107](#_Toc117846455)

[10. Điểm khôi phục và sao chép bóng (shadow copy) 108](#_Toc117846456)

[10.1 Điểm khôi phục 108](#_Toc117846457)

[10.2 Bản sao bóng 109](#_Toc117846458)

[11. Liên kết tệp 110](#_Toc117846459)

[11.1 Các chương trình đã cài đặt 110](#_Toc117846460)

[12. Bản tóm tắt 111](#_Toc117846461)

[13. Tổng kết và kiến thức thêm chương 5 111](#_Toc117846462)

[VI. Chương 6: Kỹ thuật chống lại điều tra số 115](#_Toc117846463)

[1. Giới thiệu 115](#_Toc117846464)

[2. Ẩn dữ liệu 117](#_Toc117846465)

[2.1 Mã hóa 117](#_Toc117846466)

[2.2 Mã hóa là gì? 118](#_Toc117846467)

[2.3 Mã hóa sớm 118](#_Toc117846468)

[2.4 Các thuật toán 120](#_Toc117846469)

[2.5 Không gian chính 121](#_Toc117846470)

[2.6 Một số kiểu mã hóa phổ biến 121](#_Toc117846471)

[2.7 Phá mật khẩu 123](#_Toc117846472)

[3. Tấn công mật khẩu 124](#_Toc117846473)

[3.1 Tấn công Bruteforce 124](#_Toc117846474)

[3.2 Đặt lại mật khẩu 125](#_Toc117846475)

[3.3 Tấn công từ điển 125](#_Toc117846476)

[4. Steganography 128](#_Toc117846477)

[5. Phá hủy dữ liệu 129](#_Toc117846478)

[5.1 Drive Wiping 129](#_Toc117846479)

[6. Bản tóm tắt 136](#_Toc117846480)

[7. Tổng kết và kiến thức thêm chương 6 136](#_Toc117846481)

[VII. Chương7:Tư pháp quyền riêng tư (Tham khảo Hoa Kỳ và thế giới) 142](#_Toc117846482)

[1. Giới thiệu 142](#_Toc117846483)

[2. Tu chính án thứ tư 143](#_Toc117846484)

[3. Luật hình sự — Tìm kiếm mà không cần lệnh khám xét 143](#_Toc117846485)

[3.1 Kỳ vọng hợp lý về quyền riêng tư 143](#_Toc117846486)

[3.2 Tìm kiếm Riêng tư 144](#_Toc117846487)

[3.3 E-mail 144](#_Toc117846488)

[3.4 Đạo luật về quyền riêng tư của truyền thông điện tử (ECPA) 145](#_Toc117846489)

[3.5 Các ngoại lệ đối với Yêu cầu Lệnh khám xet Tìm kiếm 145](#_Toc117846490)

[4. Quyền tìm kiếm bằng chứng 148](#_Toc117846491)

[4.1 Nắm bắt phần cứng hay chỉ thông tin? 148](#_Toc117846492)

[4.2 Tính đặc biệt 148](#_Toc117846493)

[4.3 Thiết lập nhu cầu phân tích ngoài địa điểm 149](#_Toc117846494)

[4.4 Luật truyền thông được lưu trữ 149](#_Toc117846495)

[5. Khám phá điện tử (eDiscovery) 150](#_Toc117846496)

[5.1 Nhiệm vụ bảo tồn 151](#_Toc117846497)

[5.2 Tìm kiếm Riêng tư trong Nơi làm việc 152](#_Toc117846498)

[6. Bằng chứng chuyên môn 153](#_Toc117846499)

[7. Bản tóm tắt 154](#_Toc117846500)

[8. Tổng kết và kiến thức thêm chương 7 155](#_Toc117846501)

[VIII. Chương8: Internet và E-Mail 157](#_Toc117846502)

[1. Giới thiệu 157](#_Toc117846503)

[2. Tổng quan về Internet 157](#_Toc117846504)

[2.1 Peer-to-Peer (P2P) 159](#_Toc117846505)

[2.2 Tệp INDEX.DAT 160](#_Toc117846506)

[3. Trình duyệt web — Internet Explorer 160](#_Toc117846507)

[3.1 Cookie 160](#_Toc117846508)

[3.2 Tệp Internet tạm thời, hay còn gọi là bộ nhớ cache web 161](#_Toc117846509)

[3.3 Lịch sử trình duyệt Internet 162](#_Toc117846510)

[3.4 Phần mềm Internet Explorer trong Sổ đăng ký 163](#_Toc117846511)

[3.5 Ứng dụng trò chuyện 164](#_Toc117846512)

[3.6 Trò chuyện chuyển tiếp Internet (IRC) 166](#_Toc117846513)

[3.7 ICQ "Tôi tìm kiếm bạn" 166](#_Toc117846514)

[4. E-mail 167](#_Toc117846515)

[4.1 Truy cập E-mail 167](#_Toc117846516)

[4.2 Giao thức e-mail 167](#_Toc117846517)

[4.3 E-mail làm bằng chứng 167](#_Toc117846518)

[4.4 E-mail — Bao quát Đường mòn 168](#_Toc117846519)

[4.5 Truy tìm E-mail 169](#_Toc117846520)

[4.6 Đọc tiêu đề e-mail 169](#_Toc117846521)

[5. Các trang web mạng xã hội 171](#_Toc117846522)

[6. Bản tóm tắt 172](#_Toc117846523)

[7. Tổng kết và kiến thức thêm chương 8 173](#_Toc117846524)

[E-mail 173](#_Toc117846525)

[Internet/browser 175](#_Toc117846526)

[Database 181](#_Toc117846527)

[IX. Chương 9: Pháp y mạng 185](#_Toc117846528)

[1. Giới thiệu 185](#_Toc117846529)

[1.1 Kỹ thuật xã hội 186](#_Toc117846530)

[2. Các nguyên tắc cơ bản về mạng 187](#_Toc117846531)

[2.1 Các loại mạng 187](#_Toc117846532)

[3. Công cụ bảo mật mạng 189](#_Toc117846533)

[4. Tấn công mạng 190](#_Toc117846534)

[5. Ứng phó sự cố 192](#_Toc117846535)

[6. Điều tra và Bằng chứng Mạng 193](#_Toc117846536)

[6.1 Tệp nhật ký 194](#_Toc117846537)

[6.2 Công cụ điều tra mạng 195](#_Toc117846538)

[6.3 Thách thức điều tra mạng 196](#_Toc117846539)

[7. Bản tóm tắt 196](#_Toc117846540)

[8. Tổng kết và kiến thức thêm chương 9 197](#_Toc117846541)

[X. Chương 10: Pháp y thiết bị di động 200](#_Toc117846542)

[1. Giới thiệu 201](#_Toc117846543)

[2. Mạng di động 201](#_Toc117846544)

[2.1 Các thành phần mạng di động 203](#_Toc117846545)

[2.2 Các loại mạng di động 204](#_Toc117846546)

[3. Các hệ điều hành 205](#_Toc117846547)

[4. Bằng chứng điện thoại di động 206](#_Toc117846548)

[4.1 Bản ghi chi tiết cuộc gọi 207](#_Toc117846549)

[4.2 Thu thập và Xử lý Bằng chứng Điện thoại Di động 209](#_Toc117846550)

[4.3 Mô-đun nhận dạng người đăng ký 211](#_Toc117846551)

[4.4 Mua lại điện thoại di động: Vật lý và logic 212](#_Toc117846552)

[5. Công cụ pháp y trên điện thoại di động 212](#_Toc117846553)

[6. Hệ thống định vị toàn cầu (GPS) 214](#_Toc117846554)

[7. Bản tóm tắt 218](#_Toc117846555)

[8. Tổng kết và kiến thức thêm chương 10 219](#_Toc117846556)

[XI. Chương 11:Nhìn về phía trước 227](#_Toc117846557)

[Thông tin trong Chương này: 227](#_Toc117846558)

[1. Giới thiệu 227](#_Toc117846559)

[2. Tiêu chuẩn và Kiểm soát 228](#_Toc117846560)

[3. Cloud Forensics (Tìm kiếm / Xác định Bằng chứng Tiềm năng được Lưu trữ Trong Đám mây) 229](#_Toc117846561)

[3.1 Điện toán đám mây là gì? 229](#_Toc117846562)

[3.2 Lợi ích của đám mây 230](#_Toc117846563)

[3.3 Các quan ngại về pháp lý và pháp lý trên đám mây 230](#_Toc117846564)

[4. Ổ cứng thể rắn (SSD) 232](#_Toc117846565)

[4.1 Cách các ổ đĩa thể rắn lưu trữ dữ liệu 232](#_Toc117846566)

[4.2 Vấn đề: Bỏ Thùng rác 233](#_Toc117846567)

[5. Tốc độ thay đổi 233](#_Toc117846568)

[6. Bản tóm tắt 236](#_Toc117846569)

[7. Tổng kết và kiến thức thêm chương 11 237](#_Toc117846570)

## Đối tượng độc giả của giáo trình

Như tiêu đề cho thấy, đây là một giáo trình dành cho người mới bắt đầu. Giả định duy nhất là bạn có hiểu biết cơ bản hoặc quen thuộc về máy tính và các thiết bị kỹ thuật số khác. Nếu bạn có hiểu biết vừa phải hoặc nâng cao về pháp y kỹ thuật số, giáo trình này có thể không dành cho bạn. Là một phần của “Những điều cơ bản”, giáo trình này được viết như một lời giới thiệu rộng rãi về chủ đề này hơn là một bài tổng hợp. Giáo trình đã cố gắng sử dụng càng nhiều “thuật ngữ đơn giản” càng tốt, làm cho nó (hy vọng) dễ đọc hơn.

Tôi muốn nhấn mạnh rằng đây là một giáo trình giới thiệu bị giới hạn về độ dài một cách có chủ ý. Có rất nhiều chương, kỹ thuật không được bao quát quá sâu hoặc thậm chí không thể bao quát được toàn bộ kỹ thuật. Mỗi chương là một tiêu đề riêng. Có rất nhiều cuốn sách tuyệt vời có thể giúp bạn hiểu thêm về những tiêu đề được nhắc đến trong giáo trình này. Tôi chân thành hy vọng bạn không dừng lại ở đây.

## Cấu trúc của giáo trình này

Giáo trình này được sắp xếp một cách khá đơn giản. Mỗi chương bao gồm một loại công nghệ cụ thể và bắt đầu với phần giải thích cơ bản về công nghệ có liên quan. Đây là một điều cần thiết để thực sự hiểu các tài liệu pháp y sau đó.

Để giúp củng cố tài liệu, giáo trình cũng bao gồm các câu chuyện từ thực địa, các ví dụ trường hợp, Q và A với các chuyên viên cũng như các chuyên gia về pháp y điện thoại di động.

### [Chương 1](#Top_of_CHP001_html) - Giới thiệu

Pháp y kỹ thuật số chính xác là gì? [Chương 1](#Top_of_CHP001_html) tìm cách định nghĩa pháp y kỹ thuật số. Vai trò của pháp y kỹ thuật số từ chiến trường đến phòng họp cho đến phòng xử án, pháp y kỹ thuật số ngày càng đóng một vai trò lớn hơn.

### [Chương 2](#Top_of_CHP002_html) - Các khái niệm kỹ thuật chính

Hiểu cách máy tính tạo và lưu trữ thông tin kỹ thuật số là điều kiện tiên quyết để nghiên cứu pháp y kỹ thuật số. Chính sự hiểu biết này cho phép ta trả lời những câu hỏi như "DỮ liệu đó được tạo ra như thế nào?" và "Đó là do chính máy tính tạo ra hay là kết quả của một số hành động của người dùng?" Chúng ta sẽ xem xét hệ nhị phân, cách dữ liệu được lưu trữ, phương tiện lưu trữ và hơn thế nữa.

### [Chương 3](#Top_of_CHP003_html) - Phòng thí nghiệm và Công cụ

Trong “Phòng thí nghiệm và Công cụ”, chúng ta xem xét môi trường pháp y kỹ thuật số cũng như phần cứng và phần mềm được sử dụng thường xuyên. Chúng ta cũng sẽ điều tra các tiêu chuẩn được sử dụng để công nhận các phòng thí nghiệm và xác nhận các công cụ. Những tiêu chuẩn đó được khám phá cùng với đảm bảo chất lượng, đây là nền tảng của bất kỳ hoạt động pháp y nào. Đảm bảo chất lượng nhằm đảm bảo rằng các kết quả do giám định pháp y tạo ra là chính xác.

### [Chương 4](#Top_of_CHP004_html) - Thu thập bằng chứng

Cách xử lý bằng chứng kỹ thuật số sẽ đóng một vai trò quan trọng trong việc đưa bằng chứng đó ra tòa. [Chương 4](#Top_of_CHP004_html) bao gồm các thực tiễn cơ bản về mặt pháp lý mà bạn có thể sử dụng để thu thập bằng chứng và thiết lập chuỗi hành trình lưu ký.

### [Chương 5](#Top_of_CHP005_html) - Phần mềm Hệ thống Windows

Gần như chắc chắn là bạn có (đã từng dùng) một máy tính chạy Windows trên bàn làm việc, trong cặp hoặc cả hai. Đó là một thế giới Windows. Với hơn 90% thị phần, nó thể hiện rõ ràng phần lớn công việc của chúng ta nằm ở [Chương 5](#Top_of_CHP005_html)  ;xem xét nhiều tạo tác Windows phổ biến và cách chúng được tạo ra.

### [Chương 6](#Top_of_CHP006_html) – Kỹ thuật chống lại điều tra số

Pháp y kỹ thuật số không còn là bí mật mà nó từng có. Khôi phục bằng chứng kỹ thuật số, các tệp đã xóa và những thứ tương tự hiện rất phổ biến. Bây giờ chúng ta xem xét các công cụ và kỹ thuật được sử dụng để ẩn, che dấu và phá hủy dữ liệu. Chúng được xem xét trong [Chương 6](#Top_of_CHP006_html) .

[Chương 7](#Top_of_CHP007_html) - Pháp lý

Mặc dù là một khoa học "pháp y", các khía cạnh pháp lý của pháp y kỹ thuật số không thể tách rời khỏi kỹ thuật. Trong tất cả các ứng dụng quân sự / tình báo, trừ một số ứng dụng quân sự / tình báo, cơ quan pháp lý để khám xét là điều kiện tiên quyết để điều tra pháp y kỹ thuật số. [Chương 7](#Top_of_CHP007_html) xem xét luật hiện nay về bảo vệ quyền riêng, cũng như các kỳ vọng hợp lý về quyền riêng tư, tìm kiếm riêng tư, tìm kiếm có và không có giấy khám xét, và các đạo luật truyền thông.

### [Chương 8](#Top_of_CHP008_html) - Internet và E-Mail

Mạng xã hội, e-mail, nhật ký trò chuyện và lịch sử Internet đại diện cho một số bằng chứng tốt nhất mà chúng ta có thể tìm thấy trên máy tính. Công nghệ này hoạt động như thế nào? Bằng chứng này nằm ở đâu? Đây chỉ là một số câu hỏi mà chúng ta tìm hiểu trong [Chương 8](#Top_of_CHP008_html) .

### [Chương 9](#Top_of_CHP009_html) - Pháp y mạng

Chúng ta có thể tìm thấy một hệ thống mạng máy tính ở hầu hết mọi nơi, từ các mạng gia đình nhỏ đến các mạng công ty lớn. Giống như máy tính và điện thoại di động, trước tiên chúng ta phải hiểu cách thức hoạt động của mọi thứ. [Chương 9](#Top_of_CHP009_html) bắt đầu với những điều cơ bản về mạng. Tiếp theo, chúng ta bắt đầu xem xét cách thức các mạng bị tấn công và vai trò của pháp y kỹ thuật số không chỉ đối với phản ứng mà còn cách thức truy tìm thủ phạm.

### [Chương 10](#Top_of_CHP010_html) - Pháp y thiết bị di động

Các thiết bị di động quy mô nhỏ như điện thoại di động và thiết bị GPS có ở khắp mọi nơi. Các thiết bị này ở nhiều khía cạnh là máy tính bỏ túi. Chúng có một tiềm năng rất lớn để lưu trữ bằng chứng. Pháp y kỹ thuật số phải thành thạo với các thiết bị này như máy tính để bàn. Chúng ta sẽ tìm hiểu công nghệ cơ bản cung cấp năng lượng cho điện thoại di động và thiết bị GPS cũng như bằng chứng tiềm năng mà chúng có thể chứa đựng.

### [Chương 11](#Top_of_CHP011_html) - Nhìn về phía trước: Thử thách và Mối quan tâm

Có hai công nghệ “thay đổi cuộc chơi” đối với chúng ta sẽ có tác động rất lớn đến không chỉ khía cạnh kỹ thuật của pháp y kỹ thuật số mà còn cả mảng pháp lý.

Điện toán đám mây tạo ra một rào cản lớn khác. Trong đám mây, dữ liệu được lưu trữ trong một môi trường ảo phức tạp có thể được đặt ở bất kỳ đâu trên thế giới. Điều này tạo ra hai vấn đề; từ quan điểm kỹ thuật, có sự thiếu hụt đáng báo động của các công cụ pháp y hoạt động trong môi trường này. Các tệp đã xóa cũng gần như không thể khôi phục được. Về mặt pháp lý, đó là một cơn ác mộng. Với việc dữ liệu có khả năng nằm rải rác trên toàn cầu, các thủ tục pháp lý và tiêu chuẩn rất khác nhau. Mặc dù các bước đang được thực hiện để giảm thiểu tình trạng khó xử pháp lý này, tình hình vẫn tiếp diễn cho đến ngày nay.

Ở giai đoạn sơ khai, cộng đồng pháp y kỹ thuật số vẫn còn nhiều việc phải làm liên quan đến cách thức hoạt động kinh doanh của mình, đặc biệt là liên quan đến các lĩnh vực truyền

# 

# Chương 1: Giới thiệu

**Thông tin trong Chương này:**

Khoa học pháp y là gì?



Pháp y kỹ thuật số là gì?



Sử dụng pháp y kỹ thuật số



Vai trò của Giám định viên pháp y trong hệ thống tư pháp



## Giới thiệu

Máy tính của bạn sẽ phản bội bạn. Đây là một bài học mà nhiều CEO, tội phạm, chính trị gia và những người dân bình thường đã học được một cách khó khăn. Bạn đang để lại một con đường mòn, mặc dù là một con đường kỹ thuật số; dù sao thì đó cũng là một con đường mòn. Giống như một lớp tuyết mới bao phủ, các số 1 và 0 này ghi lại “dấu chân” của chúng ta khi chúng ta đi về cuộc sống hàng ngày của mình.

Hồ sơ điện thoại di động, giao dịch ATM, tìm kiếm trên web, e-mail và tin nhắn văn bản là một số dấu ấn mà chúng ta để lại. Với tư cách là một xã hội, việc chúng ta sử dụng nhiều công nghệ có nghĩa là chúng ta đang chết chìm trong thông tin được lưu trữ điện tử. Tuy nhiên thủy triều vẫn tiếp tục cuốn vào. Bạn không tin? Điều tra những con số này từ công ty nghiên cứu IDC:

Vũ trụ kỹ thuật số (tất cả thông tin kỹ thuật số trên thế giới) sẽ đạt 1,2 triệu petabyte vào năm 2010. Con số này tăng 62% so với năm 2009.



Nếu bạn không thể xoay sở với một petabyte, có thể điều này sẽ giúp ích:

“Một petabyte tương đương với: 20 triệu, tủ đựng hồ sơ 4 ngăn chứa đầy văn bản hoặc video HD-TV 13,3 năm”.

( Mozy, 2009 )

Tác động của sự phụ thuộc vào kỹ thuật số ngày càng tăng của chúng ta đang được phản ánh qua nhiều lĩnh vực, một trong số những lĩnh vực đó là hệ thống pháp luật. Mỗi ngày, bằng chứng kỹ thuật số đang tìm đường đến các tòa án trên thế giới. Đây chắc chắn không phải là vụ kiện tụng của thời bố bạn. Đã qua rồi cái thời mà hồ sơ chỉ là giấy tờ nghiêm ngặt. Hình thức bằng chứng mới này đưa ra một số thách thức rất lớn đối với hệ thống pháp luật của chúng ta. Bằng chứng kỹ thuật số khác đáng kể so với tài liệu giấy và không thể được xử lý theo cách tương tự. Do đó, thay đổi là điều không thể tránh khỏi. Nhưng hệ thống pháp luật không có lợi. Trên thực tế, nó nhanh nhẹn như tàu Titanic. Bây giờ nó đang vật lộn để bắt kịp với tốc độ chóng mặt của công nghệ.

Các thủ tục tố tụng hình sự, dân sự và hành chính thường tập trung vào bằng chứng kỹ thuật số, vốn là ngoại lệ đối với nhiều người chơi chính, bao gồm luật sư và thẩm phán. Tất cả chúng ta đều biết những người không điều tra e-mail của riêng họ hoặc thậm chí không biết cách lướt Internet. Một số luật sư, thẩm phán, doanh nhân và cảnh sát cũng phù hợp với danh mục đó. Thật không may cho những người đó, sự ngu dốt hạnh phúc này không còn là một lựa chọn.

Xã hội tuân thủ pháp luật đi đến đâu, kẻ xấu sẽ ở rất gần phía sau (nếu không muốn nói là đi trước một chút). Họ đã tham gia với chúng ta trên máy tính xách tay, điện thoại di động, iPad và Internet. Tội phạm sẽ luôn theo dõi đồng tiền và tận dụng bất kỳ công cụ nào, bao gồm cả công nghệ, có thể hỗ trợ cho việc thực hiện tội ác của chúng.

Mặc dù khoa học pháp y đã ra đời nhiều năm nhưng pháp y kỹ thuật số vẫn còn sơ khai. Nó vẫn đang tìm thấy vị trí của mình trong số các ngành pháp y khác được thành lập hơn, chẳng hạn như DNA và chất độc học. Như một kỷ luật, nó là nơi DNA đã ở nhiều năm trước. Các tiêu chuẩn và thực hành tốt nhất vẫn đang được phát triển.

Pháp y kỹ thuật số không thể được thực hiện nếu không chui vào gầm và làm bẩn bàn tay của bạn, có thể nói như vậy. Tất cả bắt đầu với số 1 và số 0. Ngôn ngữ nhị phân này không chỉ làm nền tảng cho chức năng của máy tính mà còn cả cách nó lưu trữ dữ liệu. Chúng ta cần hiểu cách chuyển đổi số 1 và số 0 này thành văn bản, hình ảnh và video mà chúng ta thường sử dụng và sản xuất trên máy tính của mình.

## Khoa học pháp y là gì?

Hãy bắt đầu bằng cách điều tra xem nó không phải là gì. Đó chắc chắn không phải là Humvees, kính râm và những bộ quần áo đắt tiền. Nó không được hoàn thành mà không cần nhiều thủ tục giấy tờ, và nó không bao giờ gói gọn trong sáu mươi phút (có hoặc không có quảng cáo). Bây giờ chúng ta biết nó không phải là gì, hãy xem nó là gì. Nói một cách đơn giản, pháp y là ứng dụng của khoa học để giải quyết một vấn đề pháp lý. Trong pháp y, luật pháp và khoa học mãi mãi được tích hợp. Không thể áp dụng mà không tỏ lòng tôn kính đối với người kia. Bằng chứng khoa học tốt nhất trên thế giới là vô giá trị nếu nó không được chấp nhận trước tòa án pháp luật.

## Pháp y kỹ thuật số là gì?

Có nhiều cách để xác định pháp y kỹ thuật số. Trong Tạp chí Pháp y , Ken Zatyko đã định nghĩa pháp y kỹ thuật số theo cách này:

“Việc áp dụng khoa học máy tính và các quy trình điều tra cho mục đích pháp lý liên quan đến việc phân tích bằng chứng kỹ thuật số sau khi có thẩm quyền tìm kiếm thích hợp, chuỗi hành trình, xác nhận bằng toán học, sử dụng các công cụ đã được xác thực, khả năng lặp lại, báo cáo và có thể có trình bày của chuyên gia.”

( Zatyko, 2007 )

Pháp y kỹ thuật số bao gồm nhiều thứ không chỉ là máy tính xách tay và máy tính để bàn. Các thiết bị di động, mạng và hệ thống “đám mây” nằm trong phạm vi ngành học. Nó cũng bao gồm phân tích hình ảnh, video và âm thanh (ở cả định dạng tương tự và kỹ thuật số). Trọng tâm của loại phân tích này nói chung là tính xác thực, so sánh và nâng cao.

## Sử dụng pháp y kỹ thuật số

Từ một góc nhìn đơn giản, Pháp y kỹ thuật số (Điều tra số) là một chuỗi hành động nhằm xác định, thu thập, bảo toàn, phân tích, giải thích, và ghi hồ sơ các bằng chứng số có giá trị trên các đối tượng thiết bị, ứng dụng, hệ thống bị điều tra. Mục tiêu của điều tra số là sử dụng các bằng chứng đã thu thập được để phục vụ cho mục đích xử lý sự cố hệ thống, ATTT.

### 4.1 Điều tra hình sự

Khi bạn đề cập đến pháp y kỹ thuật số trong bối cảnh điều tra tội phạm mạng, mọi người có xu hướng nghĩ đến đầu tiên là lừa đảo và đánh cắp danh tính. Mặc dù những cuộc điều tra đó chắc chắn tập trung vào bằng chứng kỹ thuật số, nhưng chúng không phải là hai trường hợp duy nhất. Trong thế giới kỹ thuật số ngày nay, bằng chứng điện tử có thể được tìm thấy trong hầu hết mọi cuộc điều tra tội phạm được tiến hành. Giết người, tấn công tình dục, cướp và trộm chỉ là một vài trong số rất nhiều ví dụ về tội phạm “tương tự” có thể để lại bằng chứng kỹ thuật số.

Một trong những cuộc đấu tranh lớn trong việc thực thi pháp luật là thay đổi mô hình của cảnh sát và khiến họ suy nghĩ và tìm kiếm bằng chứng kỹ thuật số. Các thiết bị kỹ thuật số hàng ngày như điện thoại di động và máy chơi game có thể chứa một kho tàng bằng chứng. Thật không may, không một bằng chứng nào trong số đó sẽ được đưa vào phòng xử án nếu nó không được công nhận và thu thập lần đầu. Khi thời gian trôi qua và các cơ quan thực thi pháp luật của chúng ta được bổ sung và thay đổi theo nhu cầu, điều này sẽ ngày càng trở nên ít vấn đề hơn.

#### 4.1.1 Trói buộc. Tra tấn. Giết chết.

Trường hợp của Dennis Rader, được biết đến với biệt danh kẻ giết người BTK, là một ví dụ tuyệt vời về vai trò quan trọng của pháp y kỹ thuật số trong một cuộc điều tra tội phạm. Vụ án này đã thu hút sự chú ý của toàn quốc và nhờ pháp y kỹ thuật số, đã được giải quyết ba mươi năm sau. Đối với tất cả những người biết anh ta trước khi bị bắt, Dennis Rader là một người đàn ông của gia đình, thành viên nhà thờ và công chức tận tụy. Những gì họ không biết là anh ta cũng là một kẻ giết người hàng loạt hoàn hảo. Dennis Rader, được biết đến với biệt danh Bind, Torture, Kill (BTK), đã sát hại 10 người ở Kansas từ năm 1974 đến năm 1991. Rader đã cố gắng tránh bị bắt trong hơn ba mươi năm cho đến khi công nghệ phản bội anh ta.

Sau nhiều năm im lặng, Rader đã gửi một lá thư đến tờ báo Wichita Eagle tuyên bố rằng anh ta phải chịu trách nhiệm về vụ giết hại một người mẹ trẻ vào năm 1986. Bức thư được Eagle nhận được vào ngày 19 tháng 3 năm 2004. Sau khi trao đổi với Đơn vị Phân tích Hành vi của FBI, cảnh sát quyết định cố gắng liên lạc với BTK thông qua các phương tiện truyền thông.

Vào tháng 1 năm 2005, Rader để lại một mảnh giấy cho cảnh sát, giấu trong một hộp ngũ cốc, ở phía sau xe bán tải của một nhân viên Home Depot. Trong ghi chú, anh ấy nói:

“Tôi có thể giao tiếp với Floppy và không bị theo dõi trên máy tính không. Hãy trung thực. Trong Mục Linh tinh, 494, (Rex, sẽ ổn thôi), hãy chạy nó trong vài ngày nếu tôi ở ngoài thành phố, v.v. Tôi sẽ thử một đĩa mềm để chạy thử một thời gian trong tương lai gần - tháng Hai hoặc tháng Ba. "

Cảnh sát đã làm điều duy nhất họ có thể. Họ đã nói dối. Theo chỉ dẫn, họ đã phản hồi (thông qua một quảng cáo ở Eagle ) vào ngày 28 tháng 1. Quảng cáo có nội dung "Rex, sẽ ổn thôi, Liên hệ với tôi PO Box đầu tiên bốn số tham chiếu tại 67202."

Vào ngày 16 tháng 2, một phong bì manila đã đến KSAS, chi nhánh của Fox ở Wichita. Bên trong là một đĩa mềm màu tím của BTK. Đĩa chứa một tệp có tên “Test A.rtf.” (Phần mở rộng .rtf là viết tắt của “Rich Text File”). Một cuộc khám nghiệm pháp y số hồ sơ được bắt đầu. Siêu dữ liệu của tệp (dữ liệu về dữ liệu) đã cung cấp cho các nhà điều tra những dữ liệu tiềm năng mà họ đã chờ đợi hơn ba mươi năm. Ngoài “Ngày được tạo” (Thứ Năm, ngày 10 tháng 2 năm 2005 6:05:34 CH) và “Ngày được sửa đổi” (Thứ Hai, ngày 14 tháng 2 năm 2005 2:47:44 CH) là “Tiêu đề” (Nhà thờ Chúa Kitô Lutheran ) và “Được lưu lần cuối bởi:” (Dennis).

Với thông tin này, các nhà điều tra nhanh chóng đăng nhập vào trang web của Nhà thờ Christ Lutheran. Ở đó, họ phát hiện ra rằng Dennis Rader là chủ tịch Hội đồng giáo đoàn của nhà thờ. Thòng lọng đã thắt lại, nhưng nó không đủ chặt. Các nhà điều tra đã chuyển sang DNA để làm cho vụ án trở nên kín đáo. Các thám tử tiếp tục lấy một mẫu DNA từ con gái của Rader và so sánh nó với DNA từ BTK. Kết quả đã chứng minh BTK chính là cha của cô. Vào ngày 25 tháng 2, ba ngày sau khi mẫu DNA đến phòng thí nghiệm, Rader bị bắt giữ, đóng lại số phận của BTK. Anh ta hiện đang thụ án mười bản án chung thân liên tiếp (Witchita Eagle ).

### 4.2 Tố tụng dân sự

Việc sử dụng pháp y kỹ thuật số trong các vụ án dân sự là một doanh nghiệp lớn. Vào năm 2011, tổng giá trị ước tính của thị trường khám phá điện tử là ở đâu đó về phía bắc là 780 triệu đô la (Global EDD Group). Là một phần của quy trình được gọi là Khám phá điện tử (eDiscovery) , pháp y kỹ thuật số đã trở thành một thành phần chính của các vụ kiện tụng dân sự trị giá hàng triệu đô la. eDiscovery “đề cập đến bất kỳ quá trình nào trong đó dữ liệu điện tử được tìm kiếm, định vị, bảo mật và tìm kiếm với mục đích sử dụng nó làm bằng chứng trong một vụ án dân sự hoặc hình sự” (TechTarget, 2005).

Trong một vụ án dân sự, cả hai bên thường có quyền xem xét các bằng chứng sẽ được sử dụng để chống lại họ trước khi xét xử. Quy trình pháp lý này được gọi là “khám phá”. Trước đây, khám phá phần lớn là một bài tập trên giấy, với mỗi bên trao đổi báo cáo, thư từ và bản ghi nhớ; tuy nhiên, sự ra đời của pháp y kỹ thuật số và khám phá điện tử đã thay đổi rất nhiều thực tiễn này.

Sự gia tăng của máy tính đã khiến cho phương pháp này gần như tuyệt chủng. Ngày nay, các bên không còn nói về tủ đựng hồ sơ, sổ cái, và các bản ghi nhớ; họ nói về ổ cứng, bảng tính và các loại tệp. Một số vật liệu làm từ giấy có thể phát huy tác dụng, nhưng đó là ngoại lệ hơn là quy luật. Nhìn thấy bối cảnh chứng cứ thay đổi nhanh chóng, các tòa án đã bắt đầu sửa đổi các quy tắc về chứng cứ. Các quy tắc về bằng chứng, có thể là quy tắc của tiểu bang hoặc liên bang, chi phối cách bằng chứng kỹ thuật số có thể được thừa nhận trong quá trình tranh tụng dân sự. Các Quy tắc Liên bang về Thủ tục Dân sự2 đã được thay đổi vào tháng 12 năm 2006 để giải quyết cụ thể cách thức xử lý thông tin được lưu trữ điện tử trong những trường hợp này.

Bằng chứng kỹ thuật số có thể nhanh chóng trở thành tâm điểm của một vụ án, bất kể nó được sử dụng trong thủ tục pháp lý nào.

### 4.3 Sự thông minh

Những kẻ khủng bố và các chính phủ nước ngoài, mục tiêu của các cơ quan tình báo của chúng ta, cũng đã tham gia vào thời đại kỹ thuật số. Những kẻ khủng bố đã và đang sử dụng công nghệ thông tin để liên lạc, tuyển dụng và lên kế hoạch cho các cuộc tấn công. Tại Iraq và Afghanistan, các lực lượng vũ trang của chúng ta đang khai thác thông tin tình báo thu thập được từ các thiết bị kỹ thuật số được đưa thẳng từ chiến trường. Quá trình này được gọi là DOMEX ( Khai thác tài liệu và phương tiện) . DOMEX đang trả cổ tức lớn, cung cấp thông tin tình báo có thể hành động để hỗ trợ binh lính trên bộ (Quân đội Hoa Kỳ).

#### 4.3.1 Moussaoui

Có nhiều tài liệu cho rằng những kẻ không tặc ngày 9-11 đã tìm kiếm và được huấn luyện bay để tạo điều kiện cho vụ tấn công khủng bố chết người nhất từ trước đến nay trên đất Mỹ. Pháp y kỹ thuật số đã đóng một vai trò trong việc điều tra khía cạnh này của cuộc tấn công.

Vào ngày 16 tháng 8 năm 2001, Zacarias Moussaoui bị đặc vụ INS ở Eagan, Minnesota bắt giữ vì ở quá hạn visa. Các nhân viên cũng thu giữ một máy tính xách tay và đĩa mềm. Sau khi có lệnh khám xét, FBI đã khám xét hai mục này vào ngày 11 tháng 9 năm 2001. Trong quá trình phân tích, họ tìm thấy bằng chứng về tài khoản Hotmail ( pilotz123@hotmail.com ) được Moussaoui sử dụng. Anh đã sử dụng tài khoản này để gửi e-mail cho trường bay cũng như các tổ chức hàng không khác.

Đối với những người không quen thuộc với tài khoản Hotmail, đây là một dịch vụ e-mail miễn phí do Microsoft cung cấp, tương tự như Gmail và Yahoo !. Chúng khá dễ lấy và chỉ yêu cầu thông tin cơ bản về người đăng ký. Thông tin này về cơ bản là vô nghĩa, vì không có thông tin nào được xác minh. Trong quá trình điều tra e-mail của Moussaoui, các đặc vụ cũng có thể phân tích nhật ký kết nối giao thức Internet. Một trong những địa chỉ IP được xác định đã được gán cho “PC11” trong phòng máy tính tại Đại học Oklahoma.

Cuộc điều tra tiếp tục cho thấy Moussaoui và phần còn lại của mười chín tên không tặc đã sử dụng rộng rãi máy tính tại nhiều địa điểm cửa hàng của Kinko ở các thành phố khác. Các đặc vụ đến Kinko's ở Eagan với hy vọng tìm ra bằng chứng. Họ rất thất vọng khi biết rằng Kinko cụ thể này thực hiện hành vi xóa ổ đĩa trên máy tính thuê của họ hàng ngày. Bây giờ bốn mươi bốn ngày sau chuyến thăm của Moussaoui, các đặc vụ cảm thấy khả năng thu hồi bất kỳ bằng chứng nào sẽ là giữa mảnh và không. Họ không thèm điều tra máy tính của Kinko. Cửa hàng Eagan không đơn độc. Các địa điểm khác cũng thực hiện thói quen xóa hoặc định dạng lại các máy tính cho thuê. Việc này được thực hiện định kỳ, một số sớm nhất là 24 giờ, một số khác kéo dài đến ba mươi ngày. Các ổ đĩa được xóa để cải thiện hiệu suất và độ tin cậy của máy tính cũng như để bảo vệ quyền riêng tư của khách hàng ( [Lawler, 2002](#10__Saferstein_R__Criminalistics) ).

### 4.4 Các vấn đề quản trị

Bằng chứng kỹ thuật số cũng có thể có giá trị đối với các vụ việc khác ngoài kiện tụng và các vấn đề liên quan đến an ninh quốc gia. Các hành vi vi phạm chính sách và thủ tục thường liên quan đến một số loại thông tin được lưu trữ điện tử, chẳng hạn như một nhân viên điều hành một công việc kinh doanh cá nhân, sử dụng máy tính của công ty trong thời gian làm việc của công ty. Điều đó có thể không cấu thành vi phạm pháp luật, nhưng nó có thể yêu cầu công ty tiến hành điều tra.

#### 4.4.1 Ủy ban Chứng khoán và Giao dịch (SEC)

Vào năm 2008, trong khi nền kinh tế đang trong giai đoạn bắt đầu của vòng xoáy đi xuống lịch sử, thì Ủy ban Chứng khoán và Giao dịch (SEC) lẽ ra phải kiểm soát Phố Wall. Thay vào đó, nhiều người trong số họ đã dành hàng giờ trong ngày để xem nội dung khiêu dâm. Pháp y máy tính đóng vai trò quan trọng trong cuộc điều tra hành chính này.

Vào tháng 8 năm 2007, Văn phòng Tổng thanh tra của SEC (OIG) chính thức mở cuộc điều tra về khả năng sử dụng sai máy tính của chính phủ. OIG đã được cảnh báo về một vấn đề tiềm ẩn sau khi nhật ký tường lửa xác định một số người dùng đã bị từ chối truy cập vì nội dung “đen”trên Internet. Tường lửa SEC đã được định cấu hình để chặn và ghi lại loại lưu lượng này. Các nhật ký cho thấy nhân viên này đã cố gắng truy cập các trang web như [www.thefetishvault.com](http://www.thefetishvault.com) , [www.bondagetemple.com](http://www.bondagetemple.com) , [www.rape-cartoons.com](http://www.rape-cartoons.com) và [www.pornobaron.com](http://www.pornobaron.com) .

Vào ngày 5 tháng 9 năm 2007, OIG đã thông báo cho Giám đốc khu vực rằng một trong những nhân viên của ông là trọng tâm của cuộc điều tra liên quan đến việc sử dụng sai máy tính của chính phủ họ. Vào ngày 19 tháng 9, chính nhân viên này đã báo cáo rằng ổ cứng máy tính xách tay của cô đột nhiên bị hỏng. Cô đã được cấp một ổ đĩa thay thế và trở lại làm việc. Một phân tích pháp y về ổ cứng của cô ấy đã tìm thấy 592 hình ảnh “đen”(trong các tệp Internet tạm thời của cô ấy) cùng với bằng chứng cho thấy cô ấy đã cố gắng vượt qua các bộ lọc Internet của SEC.

Phạm vi của cuộc điều tra này cuối cùng đã mở rộng đáng kể, xác định thêm một số nhân viên hoặc nhà thầu đang xem nội dung “đen”trên máy tính chính phủ của họ khi đang làm việc.

Sau khi điều tra thêm, OIG nhận thấy rằng:

Một Kế toán Nhân viên Khu vực đã nhận được hơn 16 nghìn từ chối truy cập vào các trang web “đen”trong một tháng.



Một cố vấn cấp cao của Bộ phận thực thi đã truy cập nội dung “đen”từ máy tính xách tay của SEC trong nhiều trường hợp. Ổ cứng của anh ta chứa 775 hình ảnh khiêu dâm.



Một Luật sư Cấp cao tại Trụ sở chính đã tải xuống quá nhiều nội dung “đen”đến mức anh ta hết dung lượng đĩa theo đúng nghĩa đen.



Báo cáo tiếp tục liệt kê các chính sách cấm các hành vi này. Nó nói một phần:

“SECR 24-4.3 TK IIIC, quy định rằng việc sử dụng hoặc sử dụng cá nhân không thích hợp thiết bị văn phòng của chính phủ bao gồm việc tạo, tải xuống, xem, lưu trữ, sao chép hoặc truyền tải các tài liệu liên quan đến cờ bạc, vũ khí, hoạt động khủng bố và bất kỳ các hoạt động bất hợp pháp khác hoặc các hoạt động bị cấm khác vv 'id tại 3. Bản ghi nhớ dành cho nhân viên SEC đi kèm với SECR 24-4.3 nêu rõ rằng nhân viên bị cấm “truy cập tài liệu liên quan đến các hoạt động bất hợp pháp hoặc bị cấm, bao gồm cả tài liệu khiêu dâm.”

Cuối cùng, vì đây không được coi là tội phạm, nên toàn bộ vấn đề đã được chuyển đến cơ quan quản lý của SEC để xử lý (Ủy ban Chứng khoán và Giao dịch Hoa Kỳ).

## Nguyên tắc trao đổi của Locard

Nguyên tắc trao đổi của Locard nói rằng trong thế giới vật chất, khi hung thủ đi vào hoặc rời khỏi hiện trường vụ án, họ sẽ để lại thứ gì đó và mang theo thứ gì đó bên mình. Ví dụ bao gồm DNA, bản in tiềm ẩn, tóc và sợi ( [Saferstein, 2006](#10__Saferstein_R__Criminalistics) ).

Điều này cũng đúng trong pháp y kỹ thuật số. Các khóa sổ đăng ký và tệp nhật ký có thể đóng vai trò là kỹ thuật số tương đương với tóc và sợi ( [Carvey, 2005](#5__Carvey__H___2005__January_27) ). Giống như DNA, khả năng phát hiện và phân tích những hiện vật này của chúng ta chủ yếu dựa vào công nghệ sẵn có vào thời điểm đó. Nhìn vào nhiều trường hợp lạnh đang được giải quyết là kết quả của những tiến bộ quan trọng trong khoa học DNA. Xem một thiết bị hoặc sự cố qua “lăng kính” của nguyên lý Locard có thể rất hữu ích trong việc xác định vị trí và giải thích không chỉ bằng chứng vật lý mà còn cả bằng chứng kỹ thuật số.

## Phương pháp khoa học

Là một ngành học mới nổi trong khoa học pháp y, pháp y kỹ thuật số đang phải trải qua một số khó khăn ngày càng tăng. Cho đến ngày nay, pháp y kỹ thuật số thiếu nền tảng rộng lớn và hồ sơ theo dõi lâu dài do DNA pháp y thiết lập. Hiện nay, DNA được nhiều người coi là “tiêu chuẩn vàng” của khoa học pháp y. Pháp y kỹ thuật số chỉ đơn giản là thiếu nhiều năm phát triển, thử nghiệm, tinh chỉnh và những thách thức pháp lý mà DNA đã phải trải qua kể từ khi thành lập.

Lập kế hoạch cho khóa học về phía trước là một số tổ chức được xem xét để thiết lập các giao thức, tiêu chuẩn và thủ tục sẽ thúc đẩy pháp y kỹ thuật số đi trước. Các phần sau cung cấp thêm thông tin về các tổ chức quan trọng này.

## Tổ chức ghi chú

Có một số tổ chức đóng góp đáng kể vào lĩnh vực pháp y kỹ thuật số năm này qua năm khác. Các tổ chức này không chỉ đặt ra các tiêu chuẩn và thiết lập các phương pháp hay nhất mà còn cung cấp khả năng lãnh đạo. Người giám định nên quen thuộc với các thực thể này, vai trò của họ và những đóng góp mà họ thực hiện. Là các chuyên gia, chúng ta có trách nhiệm tham gia vào một hoặc nhiều tổ chức này.

### 7.1 Nhóm công tác khoa học về bằng chứng kỹ thuật số

<http://www.swgde.org/>

Các tiêu chuẩn và kỹ thuật là một phần thiết yếu của khoa học pháp y hợp lệ và chính xác. Chúng là nền tảng của nó, cốt lõi của nó. Cùng với các cơ quan liên bang khác, FBI đã hỗ trợ sự hình thành và nỗ lực của một loạt các Nhóm Công tác Khoa học (SWG) và Nhóm Công tác Kỹ thuật (TWG) (Cục Điều tra Liên bang). Các nhóm hợp tác này thu hút các thành viên của họ từ “pháp y, công nghiệp, thương mại, học thuật và trong một số trường hợp là các cộng đồng quốc tế” (Cục Điều tra Liên bang). Một số ví dụ bao gồm Nhóm Công tác Khoa học về Phương pháp Phân tích DNA (SWGDAM) và Nhóm Công tác Khoa học về Súng và Dấu công cụ (SWGGUN). Bằng chứng kỹ thuật số hiện đã tham gia cùng với sự hình thành của SWGDE.

Được thành lập vào năm 1998, Nhóm Công tác Khoa học về Bằng chứng Kỹ thuật số (SWGDE ) được tạo thành từ “cơ quan chính phủ liên bang, cơ quan thực thi pháp luật tiểu bang hoặc địa phương liên quan đến nghề pháp y kỹ thuật số và đa phương tiện” (Nhóm Công tác Khoa học về Bằng chứng Kỹ thuật số).

Sứ mệnh của SWGDE như sau: “Tập hợp các tổ chức tích cực tham gia vào lĩnh vực bằng chứng kỹ thuật số và đa phương tiện để thúc đẩy giao tiếp và hợp tác cũng như đảm bảo chất lượng và tính nhất quán trong cộng đồng pháp y” (Nhóm làm việc khoa học về bằng chứng kỹ thuật số).

### 7.2 Viện hàn lâm khoa học pháp y Hoa Kỳ

<http://www.aafs.org/>

Viện Khoa học Pháp y Hoa Kỳ (AAFS) được coi là tổ chức pháp y hàng đầu trên thế giới. Các thành viên của Học viện làm việc cho Viện Tiêu chuẩn và Công nghệ Quốc gia (NIST) và Học viện Khoa học Quốc gia (NAS). Giám đốc của hầu hết các phòng thí nghiệm điều tra tội phạm liên bang là thành viên của AAFS. Các thành viên của AAFS cũng hoạt động tích cực trong các Nhóm Công tác Khoa học khác nhau bao gồm cả SWGDE. Học viện đóng một vai trò quan trọng trong việc phát triển các tiêu chuẩn thực hành đồng thuận cho cộng đồng pháp y.

Ủy ban Công nhận Chương trình Giáo dục Khoa học Pháp y (FEPAC) là một thành lập của AAFS để đảm bảo chất lượng giáo dục khoa học pháp y và nền tảng cho các nhà khoa học pháp y trong tương lai.

AAFS có khoảng sáu nghìn thành viên và được chia thành “mười một phần bao gồm doanh nghiệp pháp y.” Học viện bao gồm “bác sĩ, luật sư, nha sĩ, nhà chất độc học, nhà nhân chủng học vật lý, người điều tra tài liệu, bác sĩ tâm thần, nhà vật lý, kỹ sư, nhà tội phạm học, nhà giáo dục, chuyên gia bằng chứng kỹ thuật số và những người khác” (Học viện Khoa học Pháp y Hoa Kỳ).

Phần Khoa học Đa phương tiện & Kỹ thuật số đại diện cho pháp y kỹ thuật số. Tính đến ngày 3 tháng 11 năm 2010, mục Bằng chứng kỹ thuật số đã có 103 thành viên. Bất chấp tên gọi, phạm vi hoạt động của AAFS thực sự mang tính toàn cầu, đại diện cho hơn 60 quốc gia trên thế giới (Viện Khoa học Pháp y Hoa Kỳ).

### 7.3 Hội đồng Giám đốc Phòng thí nghiệm điều tra tội phạm Hoa Kỳ / Ban Công nhận Phòng thí nghiệm

<http://www.ascld-lab.org/index.htm>

ASCLD / LAB (phát âm là phòng thí nghiệm có vỏ bọc). ASCLD là đối với các phòng thí nghiệm pháp y, những gì Underwriters Labs là đối với các sản phẩm gia dụng. ASCLD / LAB là “cơ quan kiểm định phòng thí nghiệm pháp y / tội phạm lâu đời nhất và nổi tiếng nhất trên thế giới.” Các phòng thí nghiệm được ASCLD / LAB công nhận là “tiêu chuẩn vàng” trong thế giới pháp y. Phòng thí nghiệm chỉ được công nhận sau khi đáp ứng thành công tất cả các tiêu chuẩn và yêu cầu được quy định trong sổ tay công nhận ASCLD / LAB. Các yêu cầu và tiêu chuẩn này bao gồm mọi khía cạnh hoạt động của phòng thí nghiệm và phải được tuân thủ nghiêm ngặt. Việc tuân thủ các tiêu chuẩn này phải được lập thành văn bản kỹ lưỡng và đầy đủ (Hội đồng Giám đốc Phòng thí nghiệm điều tra tội phạm Hoa Kỳ / Ban Công nhận Phòng thí nghiệm).

### 7.4 Viện Tiêu chuẩn và Công nghệ Quốc gia (NIST)

<http://www.nist.gov/itl/ssd/computerforensics.cfm>

Viện Tiêu chuẩn và Công nghệ Quốc gia ( NIST) được thành lập vào năm 1901 và là một bộ phận của Bộ Thương mại Hoa Kỳ. Đây là phòng thí nghiệm nghiên cứu khoa học vật lý đầu tiên của liên bang. Một số lĩnh vực trọng tâm của NIST bao gồm khoa học sinh học và sức khỏe, hóa học, vật lý, toán học, chất lượng và công nghệ thông tin (Viện Tiêu chuẩn và Công nghệ Quốc gia).

NIST tham gia rất nhiều vào pháp y kỹ thuật số. Một số chương trình và dự án bao gồm:

National Initiative Cyber Security Education (NICE) —Một chương trình giáo dục an ninh mạng quốc gia giảng dạy các thực hành an ninh mạng hợp lý sẽ cải thiện an ninh của đất nước.



Thư viện Tài liệu Tham khảo Phần mềm Quốc gia — Một tập hợp các chữ ký tệp phần mềm đã biết có thể được người điều tra sử dụng để nhanh chóng loại trừ các tệp không có giá trị điều tra. Điều này sẽ bao gồm những thứ như tệp hệ điều hành. Điều này thực sự có thể làm giảm thời gian dành cho việc điều tra.



Điều tra Công cụ Pháp y trên Máy tính — Dự định phát triển các phương pháp và tiêu chuẩn điều tra cho phần cứng và phần mềm pháp y.



(Viện Tiêu chuẩn và Công nghệ)

### 7.5 Hiệp hội Vật liệu và Thử nghiệm Hoa Kỳ (ASTM)

<http://www.astm.org/Standards/E2763.htm>

Một nhân tố chính khác trong việc phát triển các tiêu chuẩn là ASTM . ASTM là một tổ chức toàn cầu đã phát triển khoảng mười hai nghìn tiêu chuẩn được sử dụng để “cải thiện chất lượng sản phẩm, nâng cao tính an toàn, tạo thuận lợi cho việc tiếp cận thị trường và thương mại, cũng như xây dựng niềm tin của người tiêu dùng.” ASTM, được thành lập vào năm 1898, bao gồm khoảng 30.000 thành viên được chia thành 141 ủy ban. Ủy ban Khoa học Pháp y, được gọi là E30, được chia thành nhiều tiểu ban. Tiểu ban Bằng chứng Đa phương tiện và Kỹ thuật số được gọi là E30.12 (ASTM).

## Vai trò của Giám định viên pháp y trong hệ thống tư pháp

Người hành nghề pháp y kỹ thuật số thường đóng vai trò của một chuyên gia chứng kiến. Điều gì khiến họ khác với những nhân chứng khác? Các nhân chứng khác chỉ có thể làm chứng cho những gì họ đã làm hoặc nhìn thấy. Chúng thường bị giới hạn trong những lĩnh vực đó và không được phép đưa ra ý kiến. Ngược lại, các chuyên gia có thể và thường đưa ra ý kiến của họ. Điều gì khiến ai đó trở thành “chuyên gia”? Theo nghĩa pháp lý, đó là người có thể hỗ trợ thẩm phán hoặc bồi thẩm đoàn hiểu và giải thích bằng chứng mà họ có thể không quen thuộc. Để được coi là một chuyên gia trong tòa án luật, một người không nhất thiết phải có bằng cấp cao. Một chuyên gia chỉ đơn giản là phải biết nhiều hơn về một chủ đề cụ thể hơn một người bình thường. Theo định nghĩa pháp lý, một bác sĩ, nhà khoa học, thợ làm bánh hoặc người thu gom rác có thể đủ tiêu chuẩn làm nhân chứng chuyên môn trước tòa án pháp luật. Các cá nhân được tòa án đủ điều kiện làm chuyên gia dựa trên quá trình đào tạo, kinh nghiệm, giáo dục của họ, v.v. (Saferstein, 2011).

Điều gì ngăn cách một chuyên gia đủ điều kiện với một chuyên gia thực sự hiệu quả? Đó là khả năng giao tiếp của họ với thẩm phán và bồi thẩm đoàn. Họ phải là những giáo viên hiệu quả. Đại đa số xã hội thiếu hiểu biết về kỹ thuật để nắm bắt đầy đủ loại chứng thực này mà không có ít nhất một số lời giải thích. Giám định pháp y kỹ thuật số phải thực hiện nhiệm vụ của mình mà không thiên vị. Cuối cùng, một giám định viên pháp y kỹ thuật số phải đến nơi mà bằng chứng đưa họ đến mà không có bất kỳ định kiến nào.

### 8.1 Hiệu ứng CSI

Có vẻ như tất cả mọi người đều đã xem hoặc đã xem một hoặc nhiều phiên bản của loạt phim truyền hình nổi tiếng CSI . Những điều này cho thấy và những điều khác giống như nó có xu hướng thuyết phục các bồi thẩm rằng một số hình thức khoa học pháp y có thể giải quyết bất kỳ trường hợp nào. Nói cách khác, bây giờ họ mong đợi điều đó. Những kỳ vọng không hợp lý này có thể dẫn đến các phán quyết không chính xác. Bồi thẩm đoàn có thể tha bổng một bị cáo có tội đơn giản vì không có bằng chứng khoa học nào được đưa ra, giả định rằng nếu bị cáo có tội, sẽ có một số loại bằng chứng khoa học để chứng minh điều đó (Saferstein, 2011).

## Bản tóm tắt

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.

Có nhiều tổ chức giúp thiết lập các tiêu chuẩn và thực tiễn tốt nhất được sử dụng trong pháp y kỹ thuật số. Các tổ chức này bao gồm Viện Hàn lâm Khoa học Pháp y Hoa Kỳ, Nhóm Công tác Khoa học về Bằng chứng Kỹ thuật số và ASTM.

Là một người hành nghề, kỹ năng giao tiếp là vô cùng quan trọng. Bạn sẽ dành một lượng thời gian đáng kể để giải thích những phát hiện của mình cho các sĩ quan cảnh sát, luật sư và khách hàng. Quan trọng nhất, bạn phải có khả năng giải thích những điều này với thẩm phán và bồi thẩm đoàn. Tất cả các bên liên quan này phải có khả năng hiểu các phương pháp và phát hiện của bạn. Giống như tất cả các bằng chứng khoa học, bằng chứng kỹ thuật số có thể khá khó hiểu và choáng ngợp. Với những lời khai như thế này, rất dễ mất lòng người. Việc mất thẩm phán hoặc bồi thẩm đoàn trong một phiên tòa có thể gây ra những hậu quả tai hại như bị bỏ qua hoặc hiểu lầm những phát hiện của bạn.

## Tổng kết và kiến thức thêm chương 1

1. **Định nghĩa digital forensics và hiểu về mục đích của nó**

Điều tra số đươc định nghĩa là một chuỗi hành động nhằm xác định, thu thập, bảo toàn, phân tích, giải thích, và ghi hồ sơ các bằng chứng số có giá trị trên các đối tượng thiết bị, ứng dụng, hệ thống bị điều tra. Mục tiêu của điều tra số là sử dụng các bằng chứng đã thu thập được để phục vụ cho mục đích xử lý sự cố hệ thống, ATTT.

1. **Hiểu và phân biệt được tội phạm mạng (cyber crime)**

Tội phạm mạng là thuật ngữ được định nghĩa cho mọi hoạt động sai phạm liên quan đến thiết bị điện từ, mạng, hệ thống, và ứng dụng. Các hoạt động này được phân loại thành hai loại dựa trên hướng xâm nhập: tấn công nội bộ (internal attacks) và tấn công từ bên ngoài (external attacks)

1. **Hiểu được các khó khăn trong việc điều tra số**

Các cuộc tấn công mạng gây rất nhiều khó khăn cho cuộc điều tra số do khả năng thay đổi nhanh chóng của các bằng chứng, hệ thống nhằm xóa dấu vết. Ngoài ra, các cuộc điều tra số còn bị ảnh hưởng rất nhiều từ yếu tố địa lý, quốc gia.

1. **Hiểu được các loại hình điều tra số khác nhau**

Thông thường có ba loại hình điều tra số là điều tra số dân sự (civil forensics), điều tra số tội phạm/hình sự (criminal forensics), và điều tra số hệ thống cho mục đích quản trị (administrative forensics).

1. **Hiểu được luật về bằng chứng số**

Bằng chứng số là các bằng chứng được lưu trữ theo dạng điện tử. Có hai loại bằng chứng chính là bằng chứng bị thay đổi và bằng chứng được công nhận

1. **Hiểu được vai trò của điều tra số cho quá trình xử lý sự cố ATTT**

Điều tra số một cách có hệ thống, quy trình và chính xác có thể giảm thiểu rủi ro cho hệ thống, giảm chi phí yêu cầu cho cuộc điều tra số, cũng như đẩy nhanh quá trình quyết định, xử lý ATTT.

1. **Hiểu được vai trò của nhân viên điều tra số và trách nhiệm của họ**

Thông thường, tại Việt Nam, các nhân viên điều tra số sẽ được sắp xếp làm việc trực tiếp với đội xử lý sự cố ATTT. Các nhân viên điều tra số có trách nhiệm đảm bảo bằng chứng được công nhận; cũng như thực hiện các thủ tục, thông báo cho các cơ quan chức năng hoặc đối tượng liên quan để đảm bảo cuộc điều tra số không sai luật, quy trình của tổ chức.

1. **Các hành động được quy ước trong điều tra số**

**Nhân viên điều tra số cần:**

\_ Thực hiện điều tra số theo quy trình

\_ Đảm bảo tính chính xác trong thực hiện các bước

\_ Đảm bảo tính trung thực trong quá trình thực hiện

\_ Đảm bảo chỉ thực hiện điều tra trong phạm vi được cho phép

\_ Đảm bảo bảo toàn thông tin vật chứng

\_ Làm theo luật lệ của doanh nghiệp, cơ quan chức năng về điều tra số

\_ Đảm bảo điều tra lại bằng chứng trước khi sử dụng bằng chứng đó

**Nhân viên điều tra số không nên:**

\_ Bỏ qua thông tin có thể được xem là bằng chứng

\_ Công bố thông tin bằng chứng khi chưa thực hiện xong quá trình điều tra

\_ Cố gắng làm việc quá kinh nghiệm, kĩ năng của mình

\_ Thay đổi bất kì chi tiết trên vật chứng đang được điều tra

\_ Điều tra số trực tiếp trên vật chứng

Tài liệu tham khảo

1. Viện hàn lâm khoa học pháp y Hoa Kỳ. (nd). Giới thiệu về AAFS . Truy cập ngày 4 tháng 2 năm 2011, từ: <http://www.aafs.org/about-aafs>.

2. ASTM. (nd). GIỚI THIỆU: ASTM . Truy cập ngày 23 tháng 2 năm 2011, từ: <http://www.astm.org/ABOUT/aboutASTM.html>.

3. ASTM. (nd). E30 . Truy cập ngày 23 tháng 2 năm 2011, từ: <http://www.astm.org/COMMIT/SUBCOMMIT/E30.htm>.

4. ASTM. (nd). Tổng quan: GIỚI THIỆU: ASTM . Truy cập ngày 23 tháng 2 năm 2011, từ: <http://www.astm.org/ABOUT/overview.html>.

5. Carvey, H. (2005, ngày 27 tháng 1). Nguyên tắc trao đổi của Locard trong thế giới kỹ thuật số: Ứng phó sự cố của Windows . Được truy cập ngày 23 tháng 2 năm 2011, từ: <http://windowsir.blogspot.com/2005/01/locards-exchange-principle-in-digital.html>.

6. Cục Điều tra Liên bang. (nd). Các Nhóm Công tác Khoa học: Cục Điều tra Liên bang . Truy cập ngày 19 tháng 2 năm 2011, từ: <http://www.fbi.gov/about-us/lab/swgs>.

7. Lawler, BA (2002, ngày 4 tháng 9). Phản hồi của Chính phủ đối với Lệnh của Tòa án về Bằng chứng Máy tính và Email . Được truy cập ngày 13 tháng 9 năm 2011, từ [FindLaw.com](http://FindLaw.com) : [news.findlaw.com/hdocs/docs/moussaoui/usmouss90402grsp.pdf](http://news.findlaw.com/hdocs/docs/moussaoui/usmouss90402grsp.pdf) .

8. McKendrick, J. (2010, ngày 12 tháng 5). Kích thước của Vũ trụ dữ liệu: 1,2 Zettabyte và đang phát triển nhanh chóng: ZDNet . Được truy cập ngày 23 tháng 2 năm 2011, từ: <http://www.zdnet.com/blog/service-oriented/size-of-the-data-universe-12-zettabytes-and-growing-fast/4750>.

9. Phòng thí nghiệm Pháp y Máy tính Khu vực. (nd). RCFL: Phòng thí nghiệm Pháp y Máy tính Khu vực . Truy cập ngày 4 tháng 2 năm 2011, từ: <http://www.rcfl.gov/>.

10. Saferstein R. Tội phạm học: Giới thiệu về Phiên bản Cao đẳng Khoa học Pháp y Upper Saddle River, New Jersey: Prentice Hall; Năm 2006.

11. Nhóm Công tác Khoa học về Bằng chứng Kỹ thuật số. (nd). Nhóm làm việc khoa học về bằng chứng kỹ thuật số — Về chúng ta . Truy cập ngày 4 tháng 2 năm 2011, từ: <http://www.swgde.org>.

12. Stuart, J., Nordby, JJ, & Bell, S. (2009). Khoa học pháp y: Giới thiệu về các kỹ thuật điều tra và khoa học ngày 20 tháng 2 năm 2009 (xuất bản lần thứ 3). Boca Raton, FL: CRC Press.

13. Quân đội Hoa Kỳ. (nd). Khai thác Tài liệu và Phương tiện (DOMEX): Tuyên bố Tư thế Quân đội 2010 . Được truy cập ngày 23 tháng 2 năm 2011, từ: <https://secureweb2.hqda.pentagon.mil/vdas_armyposturestatement/2010/information_papers/Document_and_Media_Exploitation_%28DOMEX%29.asp>.

14. Bộ Tư pháp Hoa Kỳ. Báo cáo Thường niên RCFL cho Năm Tài chính 2009 Washington, DC: Bộ Tư pháp Hoa Kỳ; Năm 2009.

15. Zatyko, K. (nd). CHÚ THÍCH: Định nghĩa pháp y kỹ thuật số . Truy cập ngày 19 tháng 2 năm 2011, từ:

# Chương 2: Các khái niệm kỹ thuật chính

**Thông tin trong Chương này:**

Vận hành máy tính cơ bản



Bit & byte



Phần mở rộng Tệp và Chữ ký Tệp



Cách máy tính lưu trữ dữ liệu



Bộ nhớ truy cập tạm thời



Sự biến động của dữ liệu



Sự khác biệt giữa các môi trường máy tính



Dữ liệu hoạt động, tiềm ẩn và lưu trữ



Sự khác biệt giữa không gian được phân bổ và không được phân bổ



Hệ thống tệp máy tính



Biết cách và nơi dữ liệu được tạo và lưu trữ là điều cần thiết trong pháp y kỹ thuật số. Chương 2 sẽ xem xét kỹ phần cứng và các quy trình quan trọng liên quan đến các chức năng tính toán cơ bản này. Các chủ đề được đề cập bao gồm bit, byte, hình dạng ổ đĩa, ổ cứng từ tính, v.v. Các môi trường máy tính khác nhau được điều tra, bao gồm cả mạng và đám mây.

Bit, Byte, Binary, Hexadecimal, ASCII, Unicode, Bộ nhớ truy cập ngẫu nhiên, Bộ nhớ, Bộ nhớ, Bộ nhớ từ, Bộ nhớ quang, Bộ nhớ flash, Ổ đĩa thể rắn, Bộ nhớ tạm thời, Bộ nhớ lưu trữ, Đám mây, Dữ liệu đang hoạt động, Dữ liệu tiềm ẩn, Lưu trữ Dữ liệu, Chữ ký tệp, Tiêu đề tệp, Hệ thống tệp, Bảng phân bổ tệp, Hệ thống tệp công nghệ mới, Hệ thống tệp phân cấp Plus, Không gian được phân bổ, Không gian chưa phân bổ, Khu vực được bảo vệ trên máy chủ lưu trữ, Dữ liệu kế thừa, Không gian trượt, Không gian hoán đổi, Cơ sở hạ tầng như một dịch vụ (IaaS ), Nền tảng như một dịch vụ (PaaS), Phần mềm như một dịch vụ (SaaS)

## Giới thiệu

Kiến thức sâu sắc về hoạt động bên trong của máy tính là rất quan trọng đối với người hành nghề pháp y kỹ thuật số. Chính kiến thức này cho phép chúng ta điều tra kỹ lưỡng bằng chứng và đưa ra ý kiến chính xác. Nói một cách đơn giản, chúng ta không thể làm công việc của mình mà không có nó. Không phải tất cả các quy trình và phần cứng đều có giá trị giống nhau về mặt trước. Bộ nhớ và lưu trữ đóng một vai trò quan trọng trong hầu hết các cuộc điều tra. Ngược lại, bộ xử lý hoặc CPU đóng vai trò rất ít nếu có. Chương này xem xét một số chi tiết kỹ thuật của máy tính cơ bản. Trọng tâm của nó sẽ là các lĩnh vực chính ảnh hưởng đến một cuộc điều tra. Không có gì thay thế cho sự thành thạo của vật liệu này. Trách nhiệm của chúng ta với tư cách là một nhân chứng chuyên môn bao gồm giải thích các vấn đề kỹ thuật theo cách mà một người bình thường có thể hiểu được.

## Lược đồ bit, byte và đánh số

Đối với máy tính, mọi thứ khá đen và trắng. Đó là tất cả về số 1 và số 0. Máy tính sử dụng một ngôn ngữ gọi là nhị phân . Trong hệ nhị phân, chỉ có hai kết quả có thể xảy ra: 1 hoặc 0. Mỗi 1 hoặc 0 được gọi là một bit. Theo thuật ngữ toán học, hệ nhị phân được phân loại là hệ thống đánh số cơ số 2. Để so sánh, chúng ta sử dụng hệ thống số 10 cơ số được gọi là hệ thập phân . Số thập phân sử dụng các chữ số 0-9. Để tăng tốc độ mọi thứ, máy tính làm việc với các bộ sưu tập bit lớn hơn. Những phần dữ liệu lớn hơn này được gọi là byte . Một byte được tạo thành từ tám bit. Nó có dạng như sau: 01101001.

Làm thế nào để byte liên quan đến các chữ cái và số? Mỗi chữ cái, số, khoảng trắng và ký tự đặc biệt được thể hiện bằng một byte duy nhất. Ví dụ: sử dụng bộ ký tự ASCII 01000001 đại diện cho chữ hoa “A” trong khi chữ thường “a” là 01100001.

Hãy làm một thử nghiệm nhỏ để bạn có thể thấy điều này đang hoạt động. Mở tài liệu văn bản mới (sử dụng trình soạn thảo văn bản thuần túy, không phải ứng dụng xử lý văn bản như MS Word) trên máy tính của bạn và nhập cụm từ “Pháp y kỹ thuật số của Đại học Marshall”. Bây giờ, hãy đếm tất cả các chữ cái và khoảng trắng. Tiếp theo, lưu và đóng tệp văn bản mới vào màn hình của bạn. Nhấp chuột phải vào tệp và chọn thuộc tính. Kích thước tệp là bao nhiêu? Nó phải là 26 byte, cũng là số lượng chính xác của các chữ cái và khoảng trắng.

Để có một góc nhìn rộng hơn, hãy xem xét tất cả các hệ nhị phân cần thiết để đại diện cho cụm từ mẫu của chúng ta “Pháp y kỹ thuật số của Đại học Marshall”:

0100110101100001011100100111001101101000011000010110   
1100011011000010000001010101011011100110100101110110011001010111001001110011011010010111010001111001000000100010001101001011001000000101010101101110011010010111011001100101011100100111001101101001011101000111100100100000010001000110100101100111011010010111010001110111011100111011101110011101110111001110111011100111011101110111011100

Thoạt nhìn, nó hơi khó đọc, không nghi ngờ gì. May mắn thay, có một cách viết tắt mà chúng ta có thể sử dụng để làm cho nó dễ đọc hơn. Tốc ký này được gọi là hệ thập lục phân .

### 2.1 Hệ thập lục phân

Hệ thập lục phân, hoặc hệ thập lục phân, là một hệ cơ số 16, là một cách thích hợp để biểu thị số nhị phân. Hex được thể hiện bằng cách sử dụng các chữ số 0-9 và các chữ cái A-F. Chữ hoa “M” được biểu thị dưới dạng 4D trong hệ thập lục phân. Chữ thường “a” là 61. Khá thường xuyên, bạn sẽ thấy một số thập lục phân được biểu thị bằng tiền tố 0x. Tiền tố này hoặc hậu tố “h” được sử dụng để chỉ định hoặc xác định nó là số thập lục phân hoặc cơ số 16. Đây là cụm từ tương tự (Pháp y kỹ thuật số của Đại học Marshall) được thể hiện bằng hệ thập lục phân:

4d 61 72 73 68 61 6D 6C 20 55 6E 69 76 65 72 73 69 74 79

20 44 69 67 69 74 61 6D 20 46 6F 72 65 6E 73 69 63 73

Nếu bạn nhìn kỹ hơn, bạn sẽ thấy số “20” được lặp lại trong suốt chuỗi. Số “20” trong hệ thập lục phân đại diện cho một khoảng trắng.

### 2.2 Nhị phân thành văn bản: ASCII và Unicode

Vậy làm thế nào để các số 1 và 0 này kết thúc là As và B? Máy tính sử dụng các lược đồ mã hóa để chuyển đổi hệ nhị phân thành thứ mà con người có thể đọc được. Có hai lược đồ mã hóa mà chúng ta cần quan tâm, ASCII và Unicode . ASCII, Mã tiêu chuẩn Hoa Kỳ để trao đổi thông tin, là sơ đồ mã hóa được sử dụng cho ngôn ngữ tiếng Anh. ASCII định nghĩa 128 ký tự, trong đó chỉ 94 ký tự thực sự có thể in được. Phần còn lại là các ký tự điều khiển được sử dụng để tạo khoảng cách và xử lý. Ngược lại, Unicode được dùng để đại diện cho tất cả các ngôn ngữ trên thế giới và bao gồm hàng nghìn ký tự ( [Unicode Inc., 2010](#9__Unicode_Inc___2010__September) ).

Vì vậy, điều này có liên quan như thế nào đến pháp y kỹ thuật số? Trong nhiều trường hợp, giám định viên phải xem dữ liệu ở cấp độ “bit” và “byte” để tìm, trích xuất và giải thích bằng chứng. Điều này được thể hiện rõ ràng nhất trong một quá trình được gọi là khắc tệp . Việc khắc tệp được thực hiện để xác định vị trí và khai thác tệp từ các đốm dữ liệu vô định hình, chẳng hạn như không gian chưa được phân bổ (còn được gọi là không gian trống của ổ đĩa). Bước đầu tiên trong quá trình khắc tệp là xác định tệp tiềm năng. Thông thường, tệp được xác định bởi tiêu đề, nếu nó có một. Sau khi tìm thấy chân trang, tệp có thể được trích xuất thông qua một bản sao đơn giản và dán miễn là nó liên tục. Tệp bị phân mảnh khó khôi phục hơn nhiều ( [Casey, 2011](#2__Casey_E__Digital_Evidence_and) ). Có khả năng giải thích hệ nhị phân và hex giúp cho việc khắc tệp có thể thực hiện được.

## Phần mở rộng Tệp và Chữ ký Tệp

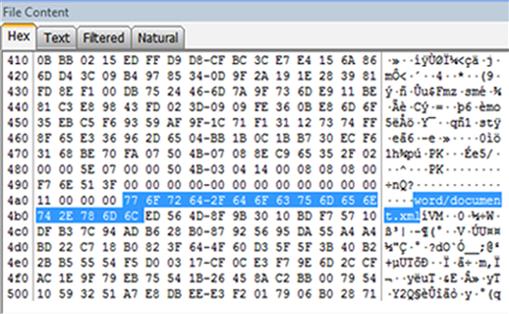
Về cơ bản, tệp là chuỗi hoặc chuỗi các bit và byte. Việc xác định tệp có thể được thực hiện theo một số cách khác nhau. Phần mở rộng tệp là phổ biến nhất. Là người dùng, chúng ta thường xác định loại tệp bằng phần mở rộng tệp, nếu hệ thống được định cấu hình. Hệ điều hành có thể được đặt sao cho phần mở rộng tệp bị ẩn. Phần mở rộng tệp là các hậu tố được thêm vào cuối tên tệp máy tính, cho biết định dạng của nó. Ví dụ sẽ bao gồm .docx và .pptx (tương ứng cho các phiên bản Microsoft Word và PowerPoint mới nhất).

Đối với mục đích của chúng ta, phần mở rộng tệp không phải là cách đáng tin cậy nhất để xác định nó. Phần mở rộng của tệp rất dễ thay đổi, chỉ cần một cú nhấp chuột và một vài lần nhấn phím. Bạn có thể thử điều này cho mình. Trong Windows, chỉ cần nhấp chuột phải vào tên tệp và đổi tên nó, thay đổi phần mở rộng. Giả sử chúng ta thay đổi phần mở rộng của tệp Word thành phần mở rộng của một hình ảnh, ví dụ: JPEG. Điều này dễ dàng hoàn thành. Trên máy Windows, chỉ cần nhấp, tạm dừng nhẹ, nhấp lại. Trên máy Mac, nhấp vào + Quay lại. Điều gì xảy ra khi chúng ta cố gắng mở tệp đó? Không. Nó sẽ không mở. Thay đổi nó trở lại và nó sẽ mở ra ngay lập tức.

Một số người sẽ cố gắng tận dụng khả năng này để thay đổi phần mở rộng tệp như một cách để che giấu dữ liệu, ẩn chúng trong tầm nhìn rõ ràng. Về mặt pháp lý, cách làm này không hiệu quả lắm. Các công cụ pháp y xác định tệp dựa trên tiêu đề, không phải phần mở rộng tệp. Nhiều công cụ thậm chí sẽ tách những tệp có tiêu đề không khớp với phần mở rộng, khiến chúng dễ dàng bị phát hiện. So sánh này thường được gọi là phân tích chữ ký tệp . [Hình 2.1](#F0010_2) và [2.2](#F0015) minh họa điều gì sẽ xảy ra khi phần mở rộng tệp được thay đổi.



Hình 2.1 Ở đây chúng ta đã thay đổi phần mở rộng tệp trên “Smoking Gun.docx” thành .mp3. Lưu ý rằng biểu tượng đã thay đổi. Đồ họa của Jonathan Sisson.



Hình 2.2 Đây là khung nhìn thập lục phân của “Smoking Gun.mp3.” Lưu ý rằng tiêu đề tệp được đánh dấu cho thấy đây thực sự là tài liệu Word. Đồ họa của Jonathan Sisson.

## Lưu trữ và bộ nhớ

Dữ liệu được lưu trữ và ghi ở đâu và như thế nào là một trong những khái niệm cơ bản chính cần phải học. Có nhiều hơn một cách để ghi dữ liệu. Ngày nay, dữ liệu thường được tạo ra theo ba cách khác nhau: điện từ học , bóng bán dẫn điện cực nhỏ (đèn flash) và ánh sáng phản xạ (CD, DVD, v.v.). Các vị trí lưu trữ bên trong máy tính phục vụ các mục đích khác nhau. Một số là ngắn hạn, được sử dụng để tạm thời giữ dữ liệu mà máy tính đang sử dụng tại thời điểm này. Loại còn lại là để lưu giữ lâu dài và lâu dài hơn.

### 4.1 Đĩa từ tính

Hầu hết các ổ đĩa trong máy tính ngày nay đều đọc và ghi dữ liệu từ tính. Chúng sẽ làm cho từng hạt có từ tính hoặc không từ hóa. Nếu hạt được từ hóa, nó được đọc là 1. Nếu không, nó được đọc là 0. Bản thân các ổ đĩa thường được tạo thành từ các đĩa nhôm phủ một vật liệu từ tính. Các đĩa này quay với tốc độ rất cao. Các đĩa quay trong vùng lân cận từ 7.000 vòng / phút đến 15.000 vòng / phút. Tốc độ thậm chí có thể lớn hơn đối với các ổ đĩa cao cấp. Các ổ đĩa hạng nặng này thường được tìm thấy trong các máy chủ hoặc máy trạm chuyên nghiệp. Từ quan điểm pháp lý, tốc độ ổ đĩa nhanh hơn có thể dẫn đến việc mua lại nhanh hơn.

Chúng ta hãy xem xét các bộ phận chính của một ổ cứng tiêu chuẩn. Các đĩa xoay quanh một thanh nhỏ gọi là trục xoay. Dữ liệu được ghi vật lý vào đĩa bằng cách sử dụng một đầu đọc / ghi gắn với một bộ truyền động, được cung cấp bởi chính bộ truyền động. Cánh tay truyền động di chuyển đầu trên (các) đĩa, đọc và ghi dữ liệu. Đầu đọc / ghi nổi trên một lớp đệm không khí. Đầu đọc / ghi, như tên gọi của nó, hầu như không nổi lên trên bề mặt đĩa, ở độ cao nhỏ hơn đường kính của sợi tóc người. Những thiết bị này thực sự khá tuyệt vời. [Hình 2.3](#F0020) cho chúng ta thấy bên trong của một ổ đĩa từ điển hình. Chúng ta có thể thấy rõ các đĩa, cánh tay truyền động và đầu đọc / ghi.



Hình 2.3 Bên trong một ổ đĩa từ điển hình.

### 4.2 Bộ nhớ flash

Bộ nhớ flash được sử dụng trong nhiều loại thiết bị. Ổ đĩa ngón tay cái và thẻ nhớ cung cấp khả năng lưu trữ đáng tin cậy trong một gói rất di động, cho phép chúng ta chụp nhiều ảnh hơn và mang theo các tệp của mình trên đường. Không giống như các loại bộ nhớ khác, bộ nhớ flash lưu giữ dữ liệu của chúng ta ngay cả khi không có điện. Đèn flash được tạo thành từ các bóng bán dẫn . Mỗi bóng bán dẫn đều mang điện hoặc không. Khi bóng bán dẫn được sạc, nó được đọc là "1"; mà không tính phí, nó được đọc là "0"

Ổ cứng dựa trên flash đang ngày càng trở nên phổ biến hơn. Không giống như ổ đĩa từ tính, ổ đĩa flash ở trạng thái rắn, có nghĩa là chúng không có bộ phận chuyển động. Chúng thường được gọi là SSD hoặc “Ổ cứng thể rắn”. Chúng cung cấp một số lợi thế đáng kể bao gồm tăng tốc độ, ít nhạy cảm hơn và tiêu thụ điện năng thấp hơn.

SSD sẽ đóng một vai trò quan trọng trong tính toán và pháp y kỹ thuật số trong tương lai. Mặc dù các thiết bị này cung cấp hiệu suất được cải thiện, nhưng chúng cũng là một thách thức lớn đối với pháp y kỹ thuật số. Chúng ta sẽ xem xét sâu hơn thách thức quan trọng mà SSD đưa ra trong [Chương 11](#Top_of_CHP011_html) .

### 4.3 Lưu trữ quang học

Phương tiện quang học đọc và ghi dữ liệu bằng cách sử dụng đèn laser cùng với vật liệu phản chiếu được tích hợp vào đĩa quang. Đĩa quang được làm bằng đế polycarbonate được bao phủ bởi một lớp nhôm mỏng. Đĩa sau đó được phủ một lớp vật liệu acrylic trong để bảo vệ. Trong quá trình sản xuất, bề mặt đĩa được dập nổi những vết sần nhỏ li ti. Chuỗi va chạm này tạo thành một đường xoắn ốc dài, duy nhất. Một tia laser chiếu một chùm ánh sáng tập trung cao vào đường đua. Ánh sáng được phản chiếu khác với những chỗ lồi lõm và khoảng không ở giữa, được gọi là “ vùng đất ”. Sự thay đổi trong hệ số phản xạ này được hệ thống đọc là hệ nhị phân (Brain). Các loại phương tiện lưu trữ quang phổ biến nhất bao gồm CD, DVD và Blu-ray (Brain).

### 4.4 Bộ nhớ lưu trữ so với tạm thời

Bộ nhớ lưu trữ và bộ nhớ tạm thời là hai thuật ngữ có phần đồng nghĩa khi nói đến máy tính. Cả hai đều đề cập đến những nơi nội bộ, nơi dữ liệu được lưu giữ. Bộ nhớ được sử dụng để lưu trữ ngắn hạn, trong khi lưu trữ lâu dài hơn. Bất kể bạn gọi nó là gì, có một sự khác biệt đáng kể giữa hai điều này, đặc biệt là từ góc độ pháp y. Sự khác biệt đó nằm ở sự biến động của dữ liệu. Dữ liệu trong RAM chỉ tồn tại khi nguồn điện được cung cấp. Khi nguồn điện được rút ra (tức là máy đã tắt), dữ liệu bắt đầu biến mất; hành vi này làm cho loại bộ nhớ này dễ thay đổi. Ngược lại, các tệp được lưu trên ổ cứng của bạn vẫn còn ngay cả sau khi máy tính bị tắt nguồn, khiến nó không dễ bị thay đổi ( [Cooper, 2004](#4__Cooper__B___2004__August___Wh) ).

RAM lưu trữ tất cả dữ liệu hiện đang được Bộ xử lý trung tâm (CPU) làm việc. Dữ liệu được đưa từ RAM đến CPU, nơi chúng được thực thi. Theo truyền thống, phân tích pháp y của một máy tính tập trung vào ổ cứng, vì nhiều bằng chứng có thể được tìm thấy ở đó. Ngày nay, chúng ta nhận thấy điều đó không phải lúc nào cũng vậy. Ví dụ, một số ứng dụng nhắn tin nhanh không ghi vào ổ cứng trừ khi tính năng ghi nhật ký được bật. AOL Instant Messenger và MSN thuộc loại đó. Vì vậy, nếu việc ghi nhật ký bị tắt (theo mặc định), bằng chứng duy nhất sẽ được tìm thấy trong RAM khi máy đang chạy.

## Môi trường máy tính

Không phải tất cả các “môi trường” máy tính đều được tạo ra như nhau. Có sự khác biệt đáng kể giữa chúng. Chúng ta có thể gặp các máy tính riêng lẻ, các mạng có kích thước khác nhau, hoặc các hệ thống phức tạp hơn. Những chênh lệch này sẽ có tác động đáng kể đến quá trình thu thập của bạn, nơi bạn tìm kiếm dữ liệu, các công cụ bạn sẽ sử dụng và mức độ phức tạp cần thiết. Việc làm rõ chính xác về môi trường là hữu ích cần có ngay từ khi bắt đầu điều tra, ngay cả trước khi bạn phản hồi một hiện trường. Môi trường có thể được chia thành bốn loại: độc lập, nối mạng, máy tính lớn và đám mây.

Máy tính độc lập là máy tính không được kết nối với máy tính khác. Đây là những thứ dễ xử lý và điều tra nhất. Các vị trí có thể có bằng chứng được giới hạn hợp lý. Hệ thống độc lập thường được bắt gặp trong các khu dân cư như căn hộ và nhà ở.

Một máy tính nối mạng được kết nối với ít nhất một máy tính khác và có thể là nhiều máy tính khác. Điều này làm tăng sự phức tạp cũng như những nơi mà bằng chứng có thể được tìm thấy. Giờ đây, chúng ta có thể thấy các tệp và hiện vật thường được tìm thấy trên máy cục bộ được lan truyền đến các máy chủ hoặc các máy khác. Môi trường này đưa nhiều biến vào phương trình. Mặc dù mạng được tìm thấy phổ biến hơn trong môi trường kinh doanh, nhưng chúng ngày càng được tìm thấy nhiều hơn trong các gia đình.

Không giống như một máy độc lập, một hệ thống máy tính lớn tập trung toàn bộ sức mạnh tính toán vào một vị trí. Tất cả các bộ xử lý, bộ nhớ và ứng dụng đều có thể được định vị và điều khiển từ một vị trí duy nhất.

### 5.1 Điện toán đám mây

Có thể bạn không quen với thuật ngữ “ điện toán đám mây ”, nhưng nếu bạn sử dụng Gmail, Facebook hoặc Twitter, bạn đã sử dụng nó. Điện toán đám mây đang là một chủ đề nóng những ngày này, thu hút được nhiều sự quan tâm của cả cộng đồng CNTT và doanh nghiệp. Mô hình máy tính “mới” này rất giống với các hệ thống máy tính lớn cũ. Giống như máy tính lớn, tài nguyên máy tính được chuyển từ máy cục bộ đến một số nơi tập trung khác.

Mô hình đám mây trình bày một số tính năng rất thú vị khiến nó trở nên hấp dẫn đối với các doanh nghiệp, đặc biệt là từ góc độ chi phí. Đám mây cung cấp phần mềm cùng với cơ sở hạ tầng và nền tảng điện toán trên mô hình trả tiền cho mỗi lần sử dụng. Điều này mang lại cho các công ty sự xa xỉ khi chỉ trả tiền cho những gì họ sử dụng. Những người khổng lồ về công nghệ như Microsoft, Google và Amazon chỉ là ba trong số các công ty đang nhảy vào cuộc đua cung cấp dịch vụ đám mây. Các dịch vụ đám mây bao gồm Cơ sở hạ tầng như một dịch vụ (IaaS), Nền tảng như một dịch vụ (PaaS) và Phần mềm như một dịch vụ (SaaS) . Tất cả những thứ này đều được cung cấp qua Internet. Trong đám mây, khách hàng chỉ trả tiền cho các tài nguyên mà họ thực sự sử dụng, giống như cách chúng ta thanh toán cho nước và điện của mình.

#### IaaS

Với IaaS, các tổ chức thuê ngoài nhu cầu phần cứng của họ cho một nhà cung cấp dịch vụ. Điều này sẽ bao gồm các nhu cầu phần cứng hàng ngày như máy chủ, bộ nhớ và những thứ tương tự. Các chi phí liên quan để chạy và bảo trì phần cứng do nhà cung cấp thanh toán.

#### PaaS

Các lập trình viên phát triển phần mềm của họ để hoạt động trong các môi trường máy tính cụ thể (hệ điều hành, dịch vụ, v.v.). PaaS cung cấp cho các nhà phát triển khả năng thuê môi trường (phần cứng, hệ điều hành, lưu trữ, máy chủ, v.v.) trên cơ sở “khi cần thiết”. PaaS cung cấp tính linh hoạt tuyệt vời trong đó hệ điều hành có thể được sửa đổi hoặc nâng cấp thường xuyên.

#### SaaS

Trên đám mây, SaaS cung cấp các ứng dụng theo yêu cầu cho khách hàng qua Internet. Các ứng dụng này được lưu trữ và duy trì bởi nhà cung cấp dịch vụ.

Đám mây đại diện cho một thách thức lớn đối với cộng đồng pháp y kỹ thuật số, từ cả quan điểm kỹ thuật và pháp lý. Về mặt kỹ thuật, đám mây thể hiện một môi trường ảo hóa rất phức tạp, gây khó chịu nếu không muốn nói là phủ nhận hoàn toàn nhiều quy trình pháp y thông thường. Về mặt pháp lý, nó có thể là một cơn ác mộng về mặt pháp lý. Trong đám mây, dữ liệu không có giới hạn. Theo nghĩa đen, bằng chứng có thể là ở tiểu bang tiếp theo hoặc một quốc gia xa lạ cách nửa vòng trái đất. Chúng ta sẽ xem xét kỹ hơn đám mây và tác động của nó đối với pháp y trong [Chương 11](#Top_of_CHP011_html) .

## Loại dữ liệu

Dữ liệu có thể được gộp thành ba danh mục lớn: hoạt động, tiềm ẩn và lưu trữ. Xem xét dữ liệu theo cách này giúp làm rõ vị trí của chúng, cách chúng được hệ thống tệp tính đến, cách người dùng có thể truy cập chúng, v.v. Nó cũng giúp thu hẹp chi phí và nỗ lực cần thiết để khôi phục dữ liệu được đề cập.

### 6.1 Dữ liệu hoạt động

Dữ liệu hoạt động là dữ liệu mà chúng ta sử dụng hàng ngày trên máy tính của mình. Hệ điều hành "nhìn thấy" và theo dõi các tệp này. Bạn có thể định vị các tệp này bằng Windows Explorer. Đây là các tệp nằm trong không gian được cấp phát của ổ đĩa. Những dữ liệu này có thể được thu thập bằng các kỹ thuật sao y pháp y tiêu chuẩn.

### 6.2 Dữ liệu tiềm ẩn

Dữ liệu đã bị xóa hoặc bị ghi đè một phần được phân loại là tiềm ẩn . Những tệp này không còn được theo dõi bởi hệ điều hành và do đó "ẩn" đối với người dùng bình thường. Hãy tìm kiếm một trong những tệp này bằng Windows Explorer và bạn sẽ không tìm thấy nó. Cần có một luồng bit hoặc hình ảnh pháp y để thu thập những dữ liệu này.

### 6.3 Dữ liệu lưu trữ

Dữ liệu lưu trữ hoặc bản sao lưu có thể có nhiều dạng. Ổ cứng gắn ngoài, DVD và băng sao lưu chỉ là một vài ví dụ. Việc thu thập dữ liệu lưu trữ có thể từ đơn giản đến cực kỳ phức tạp. Loại và tuổi của phương tiện sao lưu là những yếu tố chính trong việc xác định mức độ phức tạp của quy trình.

Băng dự phòng có thể gây ra một số thách thức rất lớn, đặc biệt nếu chúng được làm bằng phần mềm hoặc phần cứng không còn được sản xuất. Băng được tạo ra bằng cách sử dụng các phần cứng và phần mềm cụ thể. Những công cụ tương tự này sẽ cần thiết để khôi phục dữ liệu thành một dạng có thể hiểu và thao tác được. Nơi mà nó thực sự thú vị là khi phần cứng và phần mềm không còn được sản xuất nữa. Đó có thể là phiên bản cũ của phần mềm không còn khả dụng hoặc công ty không còn kinh doanh. Đây được gọi là dữ liệu kế thừa . Bạn sẽ làm gì nếu bạn không còn và không thể truy cập vào các công cụ cần thiết để khôi phục dữ liệu? Đôi khi eBay có thể tiết kiệm trong ngày.

## Hệ thống tệp

Với tất cả hàng triệu hoặc hàng tỷ tệp trôi nổi bên trong máy tính của chúng ta, phải có một số cách để giữ cho mọi thứ gọn gàng và ngăn nắp. Chức năng không thể thiếu này là trách nhiệm của hệ thống tệp . Hệ thống tệp theo dõi dung lượng trống của ổ đĩa cũng như vị trí của mỗi tệp. Không gian trống, còn được gọi là không gian chưa được phân bổ, trống hoặc tệp trước đó chiếm vị trí đó đã bị xóa.

Có nhiều loại hệ thống tệp khác nhau. Một số phổ biến nhất mà giám định viên pháp y gặp phải bao gồm FAT, NTFS và HFS +. Chúng ta hãy xem xét kỹ hơn:

Bảng phân bổ tệp (FAT) là bảng cũ nhất trong hệ thống tệp chung. Nó có bốn hương vị: FAT12, FAT16, FAT32 và FATX. Mặc dù không được sử dụng trong các hệ điều hành mới nhất, nó thường có thể được tìm thấy trong các phương tiện flash và những thứ tương tự.

Hệ thống Tệp Công nghệ Mới (NTFS) là hệ thống hiện đang được Windows 7, Vista, XP và Windows Server sử dụng. Nó mạnh hơn nhiều so với FAT và có khả năng thực hiện nhiều chức năng hơn. Ví dụ: “NTFS có thể tự động khôi phục một số lỗi liên quan đến đĩa mà FAT32 không làm được”, nó hỗ trợ tốt hơn cho các ổ cứng lớn hơn và bảo mật tốt hơn thông qua quyền và mã hóa (Microsoft Corporation).

Hệ thống tệp phân cấp (HFS +) và họ hàng của nó là HFS và HFSX được sử dụng trong các sản phẩm của Apple. HFS + là phiên bản kế thừa được nâng cấp cho HFS. Phiên bản mới hơn này cung cấp một số cải tiến bao gồm cải thiện việc sử dụng không gian đĩa, khả năng tương thích đa nền tảng và tên tệp thân thiện với quốc tế ( [Apple, Inc., 2004](#1__Apple__Inc___2004__March_5) ).

## Không gian được phân bổ và chưa được phân bổ

Trước khi chúng ta đi xa hơn, đã đến lúc chúng ta nói về cách máy tính xem dung lượng trên ổ cứng. Nói chung, hệ thống tệp phân loại tất cả dung lượng trên ổ cứng theo một trong hai cách. Không gian được phân bổ hoặc không được phân bổ (có một vài trường hợp ngoại lệ; xem thanh bên trên Khu vực được Bảo vệ Máy chủ). Nói cách khác, hoặc không gian đang được sử dụng hoặc không. Windows không thể xem dữ liệu trong không gian chưa được phân bổ này. Đối với Hệ điều hành, các tệp nằm trong không gian chưa được phân bổ về cơ bản là vô hình. Tuy nhiên, điều quan trọng là phải hiểu rằng “không được sử dụng” không phải lúc nào cũng có nghĩa là “trống rỗng”.

Nâng cao hơn

Vùng được Bảo vệ Máy chủ (HPA) và Lớp phủ Cấu hình Thiết bị (DCO)

Vùng được bảo vệ trên máy chủ (HPA) và Lớp phủ cấu hình thiết bị (DCO) đề cập đến các vùng ẩn trên ổ cứng thường khó phát hiện. Các khu vực này được tạo ra bởi các nhà sản xuất mà người dùng cuối có thể “truy cập, sửa đổi và viết cho người dùng cuối bằng cách sử dụng các công cụ nguồn mở cụ thể và có sẵn miễn phí, cho phép dữ liệu được lưu trữ và / hoặc ẩn trong các khu vực này” ( [Gupta, Hoeschele, & Rogers, Năm 2006](#6__Gupta_MR__Hoeschele_MD__Roger) ). HPA có thể chứa các công cụ chẩn đoán, hệ điều hành cho mục đích khôi phục, v.v. Hiếm khi HPA được các nghi phạm sử dụng để che giấu dữ liệu.

### 8.1 Độ bền dữ liệu

Giống như một nhà tiếp thị qua điện thoại, dữ liệu trên ổ cứng khá bền bỉ. Không dễ dàng để thoát khỏi như bạn nghĩ. Các tệp đã xóa sẽ ở đó cho đến khi chúng được ghi đè bằng nhiều dữ liệu hơn. Bạn có thể tự hỏi mình, "Vậy điều đó mất bao lâu?" Câu trả lời là, nó phụ thuộc (nhân tiện, là một trong những câu trả lời phổ biến nhất trong pháp y kỹ thuật số). Với dung lượng lưu trữ khổng lồ có sẵn trên các ổ đĩa cứng ngày nay, một tập tin có cơ hội tốt để không bao giờ bị ghi đè. Hình ảnh bữa tiệc độc thân (hoặc cử nhân) của bạn có thể vẫn còn trong ổ cứng của bạn trong một thời gian dài. Chỉ cần ghi nhớ điều đó trước khi bạn ứng cử vào văn phòng công.

Hãy nhớ rằng, công việc của hệ thống tệp là theo dõi tất cả các tệp và dung lượng lưu trữ. Hệ thống tệp giữ cho mọi thứ tốt đẹp và có trật tự. Hãy nghĩ về hệ thống tệp như một chỉ mục ở phía sau một cuốn sách. Khi tra cứu một chủ đề cụ thể, chúng ta lướt qua chỉ mục cho đến khi chúng ta tìm thấy thuật ngữ mà chúng ta đang tìm kiếm. Chỉ mục hữu ích của chúng ta sau đó cung cấp cho chúng ta số trang và chúng ta bắt đầu. Hệ thống tệp về cơ bản hoạt động theo cùng một cách. Sử dụng lại phép tương tự về cuốn sách, việc xóa tệp sẽ giống như việc xóa mục nhập khỏi mục lục của cuốn sách. Mặc dù chủ đề của chúng ta không còn được tham chiếu trong chỉ mục, trang và tất cả nội dung của nó vẫn còn trong sách, nguyên vẹn và không bị đụng chạm.

Bạn có thể ngạc nhiên khi biết rằng khi bạn lưu tệp của mình, nó không nhất thiết phải được lưu trữ ở một nơi. Trên thực tế, bảng tính của bạn có thể nằm rải rác trên (các) đĩa cứng của bạn. Lạ nhỉ? Bạn sẽ nghĩ có trật tự như máy tính, điều đó sẽ không xảy ra.

Công việc của hệ thống tệp là theo dõi các cụm riêng biệt này để chúng có thể được tập hợp lại vào lần tiếp theo bạn mở tệp đó. Bạn đã bao giờ "chống phân mảnh" ổ cứng của mình chưa? Nếu bạn có, bạn chỉ đơn giản là di chuyển những mảnh khác nhau này lại gần nhau nhất có thể. Di chuyển chúng gần nhau hơn giúp tăng tốc mọi thứ cho máy tính của bạn. Chúng càng gần nhau, chúng có thể được tập hợp lại với nhau và cung cấp cho bạn càng nhanh. Một số cá nhân quanh co có thể cố gắng phá hủy dữ liệu bằng cách sử dụng quy trình chống phân mảnh. Trong [Chương 6](#Top_of_CHP006_html) , chúng ta sẽ xem điều đó có thể hiệu quả hoặc không hiệu quả như thế nào.

Các tệp bị ghi đè thường được coi là không thể khôi phục được. Nhưng tất cả không mất đi (pardon the chơi chữ). Giống như nhiều quy tắc trong cuộc sống, có những ngoại lệ và đây là một trong số đó. Có thể tệp mới được gán cho không gian đó sẽ không cần tất cả. Nếu đúng như vậy, tệp gốc chỉ bị ghi đè một phần . Phần còn lại có thể được phục hồi và có thể chứa thông tin chúng ta có thể sử dụng. Không gian còn lại này được gọi là không gian chùng . Trước khi xem xét kỹ hơn một chút về không gian chùng, chúng ta sẽ phải tìm hiểu kỹ hơn một chút về kỹ thuật. Vì vậy, hãy bắt đầu "mọt sách" của bạn và làm theo.

## Cách ổ cứng từ tính lưu trữ dữ liệu

Chúng ta cần hiểu cách máy tính lưu trữ các tệp của bạn. Máy tính lưu trữ dữ liệu của bạn trong các không gian xác định được gọi là các cung . Hãy coi các sector là vùng chứa nhỏ nhất mà máy tính có thể sử dụng để lưu trữ thông tin. Mỗi sector chứa tối đa 512 byte dữ liệu như minh họa trong [Hình 2.4](#F0025) . Nó có thể chứa ít hơn, nhưng nó không thể chứa nhiều hơn.



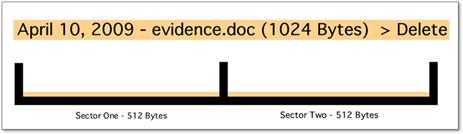
Hình 2.4 Một lĩnh vực.

Trong khi sector là vùng chứa nhỏ nhất, hệ điều hành của máy tính chỉ lưu trữ dữ liệu dưới dạng các cluster. Giả sử chúng ta lưu kế hoạch tội phạm tổng thể của mình vào ổ cứng. Chúng ta sẽ gọi nó là "bằng chứng." Nó chỉ xảy ra với kích thước 1024 byte (thuận tiện, phải không?). Máy tính của chúng ta sẽ gán tệp đó thành hai sector riêng biệt, như trong [Hình 2.5](#F0030) .



Hình 2.5 Hai cung có một tệp được gọi là bằng chứng.doc.

Sau khi xem Abby và McGee thực hiện phép thuật của họ trên NCIS , chúng ta bắt đầu có suy nghĩ thứ hai. Chúng ta quyết định tốt hơn là không nên có tệp đó trên máy tính của mình. Vì vậy, chúng ta nhấn phím xóa, gửi tệp vào thùng rác. Với một nụ cười ranh mãnh, chúng ta dọn sạch thùng rác, nội dung mà chúng ta biết rằng bằng chứng.doc hiện đang nằm trong quên lãng của kỹ thuật số. [Hình 2.6](#F0035) mô tả hai cung của chúng ta sau khi thùng rác đã được dọn sạch.



Hình 2.6 Tệp đã xóa, “bằng chứng.doc.” Lưu ý rằng nó vẫn chiếm hai cung ban đầu.

Hai ngày sau, chúng ta lưu một tệp khác vào ổ đĩa của mình. Chúng ta sẽ gọi cái này là “new.doc”. Nó chỉ có 780 byte. Có bao nhiêu lĩnh vực sẽ được chỉ định cho tài liệu mới này? Hai bạn nói? Xuất sắc! Bạn nói đúng. Hãy nhớ rằng khu vực 512 byte là “nhóm” nhỏ nhất mà máy tính có thể lưu trữ dữ liệu. Tệp này có kích thước 780 byte nên nó lớn hơn một khu vực nhưng sẽ không đầy một giây. (Xem [Hình 2.7](#F0040) .)



Hình 2.7 “New.doc” được lưu trên “Evidence.doc”, ghi đè phần lớn tệp gốc. Các tệp bị ghi đè sẽ không thể khôi phục được.

Máy tính của chúng ta, chỉ hoạt động theo ý mình, quyết định đặt tệp mới này vào cùng hai lĩnh vực ban đầu bị chiếm bởi tệp đầu tiên của chúng ta, Evidence.doc. 780 byte đầu tiên của tệp gốc của chúng ta đã bị ghi đè. Một số phép toán nhanh cho chúng ta biết rằng 244 byte trong tệp gốc của chúng ta vẫn còn ở đó. 244 byte còn lại đó bao gồm không gian chùng. Không gian chùng, được mô tả trong [Hình 2.8](#F0045) là sự khác biệt giữa không gian được gán và không gian thực sự được sử dụng.



Hình 2.8 Lưu ý không gian chùng. Đoạn dữ liệu này có thể được phục hồi.

Ngoài không gian chùng, chúng ta có thể khôi phục các phân đoạn của tệp trước đó. Nó có thể không hữu ích. Nhưng sau đó một lần nữa, nó chỉ có thể. Nó có thể là một phần của bảng tính, e-mail hoặc hình ảnh buộc tội. Những đoạn này có thể chứa vừa đủ một e-mail để xác định người gửi hoặc địa chỉ IP của người gửi. Một phần hình ảnh của nạn nhân có thể liên kết họ với nghi phạm. Người dùng hoặc hệ điều hành không thể truy cập không gian Slack. Do đó, bằng chứng này tồn tại mà nghi phạm không thể biết được.

Tài nguyên bổ sung

Cách hoạt động của ổ cứng

Scott Moulton, từ [MyHardDriveDied.com](http://MyHardDriveDied.com) , có một số bài thuyết trình tuyệt vời về ổ đĩa từ tính và thể rắn. Cách giao hàng của anh ấy không nhàm chán hay quá kỹ thuật. Hình ảnh rất nổi bật. Trang web của anh ấy có video về các bài thuyết trình của anh ấy. Chúng rất xứng đáng với thời gian.

<http://myharddrivedied.com/presentations-resources>

### 9.1 Tệp Trang (hoặc Hoán đổi Không gian)

Ổ cứng được sử dụng để lưu trữ dữ liệu và ứng dụng của bạn khi chúng không được sử dụng. Nói một cách tương đối, đây là thành phần chậm nhất trong ba thành phần mà chúng ta đang thảo luận. Ổ cứng là một điểm “chậm chạp”, nó không thể bắt kịp với tốc độ chóng mặt của CPU. Vì vậy, tất cả dữ liệu và hướng dẫn phải được cấp cho CPU từ RAM. Nếu không, có thể dễ dàng hơn khi sử dụng một tấm bia đá và một cái đục. Được rồi, có thể không, nhưng bạn có ý tưởng.

Rất ít người có thể sử dụng máy tính của họ và chỉ mở một ứng dụng. Nó giống như quảng cáo khoai tây chiên của Lay từ vài năm trước. Bạn không thể mở chỉ một cái. Giả sử bạn đã thiết lập và chạy Word, Outlook và Firefox. Bên trong Firefox, bạn có ba tab riêng biệt đang mở. Nếu bạn tiếp tục mở các ứng dụng hoặc sử dụng các chương trình như Adobe Photoshop cần nhiều bộ nhớ của máy tính, cuối cùng bạn sẽ thấy máy tính của mình chậm lại. Bạn cũng có thể nghe thấy ổ cứng của mình bắt đầu quay. Tại thời điểm này, bạn sẽ bắt đầu sử dụng bộ nhớ ảo của máy tính.

Bộ nhớ ảo này được gọi là tệp trang hoặc không gian hoán đổi. Tệp trang không phải là một chức năng được sử dụng một cách nhất quán. Tệp trang được sử dụng khi chúng ta đã sử dụng hết bộ nhớ chính của máy tính. Bộ nhớ chính được gọi là RAM. RAM là viết tắt của Random Access Memory (Bộ nhớ truy cập ngẫu nhiên). RAM lưu giữ mọi thứ mà máy tính của bạn đang hoạt động tại thời điểm này. Tất cả dữ liệu và hướng dẫn (chương trình, v.v.) phải chuyển từ bộ nhớ chính sang CPU, nơi chúng được xử lý. Mỗi máy tính đều có một dung lượng RAM nhất định. Nó không phải là nguồn cung cấp vô tận và cuối cùng có thể cạn kiệt. Khi hết RAM, máy tính sẽ phải bắt đầu di chuyển một số thứ xung quanh. Để giảm bớt tình trạng này, máy tính sẽ hoán đổi dữ liệu trong và ngoài RAM, ghi dữ liệu vào tệp trang để giải phóng dung lượng trong RAM ( [Casey, 2009](#3__Casey_E__Handbook_of_Digital) ). Điều tuyệt vời về tệp trang là nó có thể chứa các tệp và các đoạn tệp không còn tồn tại ở bất kỳ nơi nào khác trên ổ đĩa. Ngay cả những nghi phạm thành công trong việc xóa và ghi đè các tệp của họ cũng sẽ bỏ qua không gian hoán đổi, để lại bằng chứng này cho việc khôi phục sau này.

Vì vậy, những gì trong đó cho chúng ta? Nó có thể là rất nhiều. Hãy kết nối tất cả các dấu chấm và bạn sẽ thấy:

1 . Dữ liệu sẽ ở trên ổ cứng cho đến khi chúng bị ghi đè.

2 . Tệp trang không được sử dụng nhất quán, vì vậy một số dữ liệu có thể tồn tại ở đó một thời gian.

3 . Tệp trang sẽ chứa dữ liệu tại một điểm trong RAM. Đó có thể là bất cứ điều gì. Chúng ta thậm chí có thể tìm thấy mật khẩu được viết rõ ràng.

## Chức năng máy tính cơ bản — Kết hợp tất cả lại với nhau

Chúng ta hãy cùng xem xét những gì đang diễn ra "bên dưới" máy tính của chúng ta khi chúng ta tìm hiểu về một số tác vụ phổ biến. Dữ liệu mẫu của chúng ta, chẳng hạn như tài liệu Word, bắt đầu trên ổ cứng nơi chúng ta đã lưu nó vào ngày hôm trước. Tệp của chúng ta được lưu trữ trên ổ cứng dưới dạng một dãy số 1 và 0. Thông thường, các tệp sẽ có cấu trúc hoặc định dạng cụ thể. Phần đầu của tệp được gọi là “ tiêu đề ”. Phần cuối của tệp được gọi là “ chân trang ”. Tất cả các byte ở giữa đại diện cho phần còn lại của tệp. Về mặt kỹ thuật, tiêu đề tệp được coi là một dạng siêu dữ liệu (“dữ liệu về dữ liệu”). Tiêu đề, giống như phần mở rộng, được sử dụng để xác định loại tệp. Tuy nhiên, không giống như tiện ích mở rộng, tiêu đề khó thay đổi hơn nhiều và hầu hết người dùng thường không thể truy cập được.

Khi tệp được lưu hoặc ghi vào ổ cứng, nó không nhất thiết phải được lưu vào các cụm liền kề như người ta có thể mong đợi. Các phần riêng biệt này của tệp có thể nằm trên các mặt khác nhau của đĩa hoặc trên các đĩa khác nhau hoàn toàn. Khi chúng ta nhấp đúp vào tệp để mở, máy tính sẽ lấy vị trí của tất cả các cung được phân bổ cho tệp từ hệ thống tệp và tạo lại tệp của bạn.

Để làm việc trên tệp, nó phải được tải vào bộ nhớ chính của máy tính, còn được gọi là RAM. Từ đây, tệp được đưa vào bộ xử lý trung tâm (CPU) khi chúng ta đang làm việc với nó.

Tủ hồ sơ, bàn làm việc và người làm việc được sử dụng như một phép tương tự phổ biến để giúp giải thích quá trình này. Tủ hồ sơ tượng trưng cho ổ cứng. Bàn làm việc đại diện cho RAM. Cuối cùng, nhân viên tại bàn làm việc đại diện cho CPU. Tủ hồ sơ, giống như ổ cứng, lưu trữ các tệp của chúng ta khi chúng ta không sử dụng chúng. Cũng giống như trong thế giới thực, chúng ta không thể làm việc trên bất kỳ tài liệu nào của mình từ tủ hồ sơ cho đến khi chuyển chúng đến bàn làm việc. Nhân viên (CPU) không thể làm việc trên các tài liệu của chúng ta cho đến khi chúng được chuyển từ tủ hồ sơ sang bàn làm việc.

## Bản tóm tắt

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.

Không phải tất cả các môi trường máy tính đều giống nhau. Một số tương đối đơn giản, một số khác phức tạp hơn nhiều. Máy tính độc lập, mạng và đám mây được đề cập trong chương này.

Là giám định viên pháp y, chúng ta phải có quyền chỉ huy tài liệu này để chúng ta có thể giải thích nó cho người bình thường. Chính những “người bình thường” này tạo nên bồi thẩm đoàn của chúng ta.

## Tổng kết và kiến thức thêm chương 2

1. **Phân biệt và mô tả các loại hình đĩa cứng và tính chất của chúng**

Có hai loại hình ổ đĩa chính là

Hard Disk Drive (HDD)

đĩa cứng HDD được định nghĩa là thiết bị lưu trữ thông tin dài hạn được sử dụng trong bất kỳ thiết bị máy tính diện tử. Chức năng chính của ổ đĩa này là thu thập, lưu trữ thông tin cũng như chuyển thông tin từ ổ đĩa này sang ổ đĩa khác.

Solid State Drive (SSD)

đĩa cứng SDD được định nghĩa là thiết bị lưu trữ thông tin ở thể solid, có cùng chức năng với ổ đĩa HDD. Tuy nhiên ổ đĩa SDD sử dụng các vi mạch bán dẫn nhằm lưu trữ thông tin thay vì các yếu tố cơ học như HDD.

đĩa cứng SDD có chức năng:

NAND-based flash memory: Tức là các thông tin lưu trữ vẫn được lưu giữ kể cả khi mất điện

Volatile RAM: Với khả năng lưu trữ liên tục, người dùng có khả năng truy cập thông tin nhanh hơn so với ổ cứng HDD

1. **Hiểu được cấu trúc vật lý và cấu trúc vận hành của đĩa cứng**

Cấu trúc vật lý đĩa cứng:



Khả năng vận hành của đĩa cứng:

Khả năng vận hành của đĩa cứng phụ thuộc vào các tệp tin hệ thống và phần mềm được sử dụng để kiểm soát truy cập vào nơi lưu trữ trên đĩa cứng. Ngoài ra, khả năng vận hành này sẽ bị ảnh hưởng bởi một số yếu tố khác giữa đĩa cứng và thiết bị như khả năng tương thích, khả năng mở rộng, hệ điều hành của thiết bị, …

1. **Hiểu được quá trình khởi động Windows, Mac, và Linux**

Windows (UEFI):

Khởi động phần cứng: chạy các firmware và kết nối các phần cứng cơ bản khác như bàn phím, con chuột

Khởi động dịch vụ liên quan UEFI: khởi động ổ đĩa EFI -> Chạy Boot Loader -> Chạy các kernel cơ bản -> Khởi động toàn bộ Hệ điểu hành -> Chuyển sang giao diện người dùng

MAC:

Khởi động cùng lúc cả hai thành phần là phần dịch vụ và phần ổ đĩa

Chạy mã khởi động (Boot Code) -> Trong trường hợp có lỗi thì từ chối, trong trường hợp không có lỗi thì bắt đầu khởi động hệ điều hành -> Chuyển sang giao diện người dùng

Linux:

Khởi động BIOS -> Xác nhận không bị lỗi -> Tìm kiếm Master Boot Record (MBR) -> Bắt đầu chạy boot loader -> Song song điều tra hệ điều hành cũng như kernel -> khi được chấp thuận sẽ tạo root và bắt đầu chuyển sang giao diện cho phép nhập thông tin

1. **Biết được các tệp tin hệ thống được sử dụng trong các hệ điều hành Windows, Mac, và Linux**

Windows: FAT 12, FAT 16, FAT 32, NTFS, EFS

Linux: FHS, EXT, EXT2, EXT 3, EXT 4

Mac OS X: HFS, HFS +, CDFS, VFS, UDF

1. **Sự khác biệt giữa các RAID (Redundant Arrays of Inexpensive Disks) lưu trữ**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RAID 0 | RAID 1 | RAID 2 | RAID 3 | RAID 5 | RAID 10 |
| Dữ liệu được phân chia giữa các đĩa cứng | Dữ liệu được phân chia giữa 2 ổ đĩa chính và 2 ổ đĩa dự phòng | Đối với Raid 2, dung lượng lưu trữ cũng như thời gian cần thiết truy cập sẽ cao hơn RAID 1 | Sử dụng kĩ thuật lưu trữ gọi là chia tách dữ liệu (data stripping) và ổ đĩa biệt lập (dedicated parity) | Dữ liệu về trạng thái, thông tin ổ đĩa sẽ được chia đều cho các ổ đĩa được sử dụng | Là sự kết hợp giữa RAID 0 và 1. |
| Trong trường hợp đĩa cứng hỏng, sẽ không thể hồi phục lại được | Trong trường hợp đĩa cứng hỏng, có thể hồi phục dữ liệu từ ổ dự phòng | Đặc biệt rằng đối với loại RAID 2, khi thông tin được ghi lại thành công, sự kiện này sẽ được ghi lại trong nhật ký | Đối với RAID 3, thông tin khi bị mất đi sẽ có thể hồi phục cũng như hồi phục lại trạng thái ổ đĩa | Quá trình ghi, lưu trữ thông tin rất chậm so với các loại khác | So sánh với các loại hình RAID khác, quá trình hồi phục dữ liệu cũng như xử lý công việc lưu trữ của RAID 10 sẽ tốt hơn |
| Cần ít nhất 2 ổ đĩa | Cần có ổ đĩa dự phòng và đảm bảo dữ liệu giữa ổ chính và dự phòng là giống nhau | Khi so sánh với RAID 0 và 1, RAID 2 có thể đảm bảo tính chính xác của thông tin nhưng lại chậm hơn RAID 0 khi lưu trữ dữ liệu | Cần ít nhất 3 ổ đĩa | Cần ít nhất 3 ổ đĩa | Cần ít nhất 4 ổ đĩa |

NGƯỜI GIỚI THIỆU

1. Apple, Inc. (2004, ngày 5 tháng 3). Ghi chú kỹ thuật Định dạng âm lượng TN1150 HFS Plus . Được truy cập ngày 10 tháng 8 năm 2011, từ: <http://developer.apple.com/library/mac/#technotes/tn/tn1150.html>.

2. Casey E. Bằng chứng Kỹ thuật số và Tội phạm Máy tính: Khoa học Pháp y, Máy tính và Internet Waltham, MA: Báo chí Học thuật; 2011.

3. Casey E. Sổ tay Điều tra và Pháp y Kỹ thuật số Burlington, MA: Academic Press; Năm 2009.

4. Cooper, B. (2004, tháng 8). Sự khác biệt giữa bộ nhớ và bộ nhớ là gì? Được truy cập ngày 10 tháng 8 năm 2011, từ: <http://searchstorage.techtarget.com/answer/What-is-the-difference-between-memory-and-storage>.

5. Dale N. Computer Science Illuminated Edition 4 Sudbury, MA: Jones và Bartlett; Năm 2009.

6. Gupta MR, Hoeschele MD, Rogers MK. Vùng đĩa ẩn: HPA và DCO. Tạp chí Quốc tế về Bằng chứng Kỹ thuật số . Năm 2006; 5.

7. Tập đoàn Microsoft. (nd). So sánh hệ thống tệp NTFS và FAT . Được truy cập ngày 10 tháng 8 năm 2011, từ: <http://windows.microsoft.com/en-US/windows-vista/Comparing-NTFS-and-FAT-file-systems>.

8. [SearchStorage.com](http://SearchStorage.com) . (2000, tháng 12). Phương tiện quang học . Truy cập ngày 10 tháng 8 năm 2011, từ: <http://searchstorage.techtarget.com/definition/optical-media>.

9. Unicode Inc. (2010, ngày 17 tháng 9). Unicode là gì? Truy cập ngày 10 tháng 8 năm 2011, từ:

# Chương 3: Phòng thí nghiệm và Công cụ

**Thông tin trong Chương này:**

Vai trò và Tổ chức của Phòng thí nghiệm Pháp y



Mục đích của các Chính sách & Thủ tục trong Phòng thí nghiệm Pháp y



Vai trò của đảm bảo chất lượng trong pháp y



Phần cứng và phần mềm pháp y kỹ thuật số



Công nhận so với chứng nhận



Các phòng thí nghiệm và công cụ pháp y đóng vai trò quan trọng trong sự thành công của bất kỳ cuộc điều tra pháp y kỹ thuật số nào. Công nhận phòng thí nghiệm là một cơ chế được thực hiện để đảm bảo rằng các kết quả đáng tin cậy và chính xác thu được từ bất kỳ phân tích nào. Các công cụ pháp y có nhiều loại bao gồm phần cứng, phần mềm, thương mại và mã nguồn mở.

Hiệp hội Giám đốc Phòng thí nghiệm điều tra tội phạm Hoa Kỳ / Ban Công nhận Phòng thí nghiệm (ASCLD / LAB), Phòng thí nghiệm Pháp y Máy tính Khu vực (RCFL), Quy trình Hoạt động Tiêu chuẩn, Đảm bảo Chất lượng (QA), Khối Viết, Công nhận, Chứng nhận, Báo cáo cuối cùng của Người giám định

## Giới thiệu

Trong chương này, chúng ta sẽ khám phá các kiểu thiết lập phòng thí nghiệm khác nhau cũng như các công cụ phần cứng và phần mềm được sử dụng phổ biến. Chúng ta cũng sẽ xem xét Quy trình hoạt động tiêu chuẩn và Đảm bảo chất lượng, hai thành phần quan trọng của một phòng thí nghiệm pháp y kỹ thuật số hiệu quả. Đạt được và duy trì việc công nhận phòng thí nghiệm, mặc dù tốn thời gian và tốn kém, nhưng cải thiện đáng kể hiệu suất của phòng thí nghiệm và chất lượng của các phát hiện của nó. Chứng nhận giám định đảm bảo rằng kỹ năng của các phòng thí nghiệm đáp ứng mức tối thiểu. Vào cuối ngày, các yếu tố này kết hợp với nhau để đảm bảo rằng chỉ những kết quả hợp lệ và đáng tin cậy mới được tạo ra và công lý được thực thi.

## Phòng thí nghiệm pháp y

Các phòng thí nghiệm pháp y nằm rải rác trên khắp Hoa Kỳ và tuân thủ chặt chẽ các khu vực pháp lý của cơ quan thực thi pháp luật (địa phương, hạt, tiểu bang và liên bang) ( [James & Nordby, 2009](#11__James_S__Nordby_JJ__Forensic) ). Phần lớn các cơ sở này được điều hành bởi một cơ quan thực thi pháp luật. Phòng thí nghiệm điều tra tội phạm của FBI ở Quantico, Virginia, được đánh giá là phòng thí nghiệm lớn nhất trên thế giới ( [Saferstein, 2006](#15__Saferstein_R__Criminalistics) ).

Không phải tất cả các cuộc giám định pháp y trên máy tính đều được tiến hành trong nơi được coi là bối cảnh phòng thí nghiệm truyền thống. Nhiều cơ quan tiến hành chúng tại địa phương tại bộ phận của họ nếu họ có sẵn thiết bị cần thiết và nhân viên được đào tạo.

Pháp y kỹ thuật số không hề rẻ, vì vậy không phải cơ quan nào cũng có đủ khả năng để đào tạo và trang bị cho các giám định viên của riêng họ. Một cách để đáp ứng nhu cầu ngày càng tăng này là chương trình Phòng thí nghiệm Pháp y Máy tính Khu vực (RCFL) do FBI bắt đầu. Chương trình RCFL có mười sáu cơ sở trên khắp Hoa Kỳ. Họ cung cấp các dịch vụ pháp y kỹ thuật số và đào tạo cho tất cả các cấp thực thi pháp luật. Mỗi RCFL được biên chế và quản lý bởi sự hợp tác của các cơ quan thực thi pháp luật địa phương, tiểu bang và liên bang.

Chương trình RCFL là một thành công lớn và tạo ra một vết nứt đáng kể trong việc tồn đọng các cuộc giám định pháp y kỹ thuật số trên toàn quốc. Trong năm tài chính 2010, RCFLs trên toàn quốc đã thực hiện 6.564 cuộc giám định pháp y và xử lý một con số khổng lồ 3.086 terabyte dữ liệu. Để đặt điều đó trong bối cảnh, Báo cáo thường niên năm 2010 giải thích theo cách này; “Một terabyte tương đương với 1.024 gigabyte hoặc khoảng 1.000 bản sao của Bách khoa toàn thư Britannica.” Làm toán, đó là khoảng 3.086.000 bách khoa toàn thư. RCFL xử lý nhiều loại thiết bị kỹ thuật số và phương tiện bao gồm điện thoại thông minh, ổ cứng, thiết bị GPS (Hệ thống Định vị Toàn cầu) và ổ đĩa flash. Năm 2010, các giám định viên RCFL đã giúp kết tội những kẻ hiếp dâm, khủng bố và các chính trị gia quanh co ( [Cục Điều tra Liên bang, 2010](#10__Federal_Bureau_of_Investigat) ).

### 2.1 Phòng thí nghiệm ảo

Phòng thí nghiệm kỹ thuật số không cần phải giới hạn ở một vị trí duy nhất. Công nghệ ngày nay làm cho nó có thể chạy một phòng thí nghiệm "ảo" với các giám định viên và kho lưu trữ bằng chứng trung tâm nằm ở các vị trí địa lý riêng biệt. Sự sắp xếp này có một số lợi thế bao gồm tiết kiệm chi phí, tiếp cận nhiều tài nguyên hơn (ví dụ: công cụ và bộ nhớ), tiếp cận với chuyên môn đa dạng và cao hơn, và giảm sự trùng lặp tài nguyên không cần thiết (Craiger).

Sự sắp xếp ảo này cho phép truy cập dựa trên vai trò riêng biệt. Ví dụ, quyền truy cập đầy đủ có thể được cấp cho giám định viên và quản lý phòng thí nghiệm. Các công tố viên, điều tra viên và luật sư bào chữa sẽ bị hạn chế quyền truy cập. Quyền truy cập hạn chế này sẽ hạn chế những gì những người đó có thể nhìn thấy và những gì họ có thể làm (chỉ đọc, v.v.) ( [Whitcomb](#17__Whitcomb__C__A___n_d____Virt) ).

Có một số lo ngại đáng kể với cách tiếp cận này:

1 . Bảo mật — Bảo mật của hệ thống phải đủ mạnh để duy trì mức độ toàn vẹn bằng chứng theo yêu cầu của tòa án. Nếu không, có thể có những hậu quả thảm khốc, chẳng hạn như không thể chấp nhận được bằng chứng từ nhiều trường hợp.

2 . Hiệu suất —Để kế hoạch này hoạt động, kết nối phải vừa nhanh vừa đáng tin cậy. Không có kết nối hoặc kết nối chậm sẽ nhanh chóng ảnh hưởng đến khả năng hoạt động của tổ chức.

3 . Chi phí —Chi phí khởi động nói riêng là đáng kể và có khả năng vượt quá khả năng chi trả của nhiều đại lý ( [Whitcomb](#17__Whitcomb__C__A___n_d____Virt) ).

### 2.2 Bảo mật phòng thí nghiệm

Bảo mật phòng thí nghiệm luôn là mối quan tâm lớn. Việc tiếp cận các bằng chứng và phương tiện phải được quản lý chặt chẽ. Bảo mật nghiêm ngặt đóng một vai trò quan trọng trong việc duy trì tính toàn vẹn của bằng chứng kỹ thuật số đi qua phòng thí nghiệm. Chỉ những nhân viên được ủy quyền, đã được điều tra kỹ lưỡng mới được phép tiếp cận các khu vực quan trọng như trạm điều tra và lưu trữ bằng chứng. Các cá nhân không được phép thường bị cấm sử dụng cửa ra vào và các rào cản vật lý khác cùng với các biện pháp kiểm soát truy cập như chìa khóa, thẻ quẹt và mã truy cập. Các giải pháp kỹ thuật số như thẻ quẹt và mã truy cập mang lại lợi thế hơn so với các phương pháp cũ hơn như chìa khóa. Các phương tiện điện tử cung cấp một lộ trình đánh giá được tạo sẵn có thể được sử dụng để hỗ trợ chuỗi hành trình sản phẩm. An ninh được tăng cường hơn nữa với hệ thống báo động và những thứ tương tự.

Truy cập trái phép không phải là mối đe dọa duy nhất đối với bằng chứng. Rủi ro hỏa hoạn, lũ lụt và các thiên tai khác cũng phải được giải quyết.

Chuỗi hành trình sản phẩm vẫn tiếp tục tại phòng thí nghiệm, cũng như các thủ tục giấy tờ. Trong phòng thí nghiệm, bằng chứng phải được ký tên vào và ra khỏi khu vực lưu trữ bằng chứng để điều tra và tòa án. Nhật ký này phải được hoàn thành mỗi và mỗi khi chứng cứ được loại bỏ hoặc trả lại phòng chứng cứ hoặc kho tiền. Quá trình điều tra và nhận phòng này có thể được thực hiện theo cách cổ điển với bút và giấy hoặc điện tử với máy quét và mã vạch.

Cũng giống như ngoài thực địa, việc truy cập mạng để lấy bằng chứng trong phòng thí nghiệm cũng là một vấn đề cần quan tâm. Điều này đúng với cả Internet và máy tính của phòng thí nghiệm. Thực tiễn tốt nhất cho chúng ta biết rằng máy được sử dụng để thực hiện điều tra không được kết nối với Internet. Việc xóa kết nối này sẽ xóa lập luận rằng bằng chứng đã bị ai đó hoặc thứ gì đó xâm nhập bằng cách nào đó (ví dụ: phần mềm độc hại) qua Internet. Các phòng thí nghiệm ảo sẽ cần có khả năng trình bày rõ cách duy trì tính toàn vẹn của bằng chứng, dựa trên bản chất hoạt động của chúng.

Phần mềm độc hại (vi rút, sâu, v.v.) có thể ẩn náu trên bất kỳ ổ đĩa bằng chứng nào được đưa đến để điều tra. Việc kết nối nó với mạng nội bộ theo một cách nào đó gây ra rủi ro lớn cho không chỉ máy tính của phòng thí nghiệm mà còn cả bằng chứng từ các trường hợp khác. Để giảm thiểu rủi ro, các ổ đĩa này nên được quét vi-rút bằng ít nhất một công cụ chống vi-rút trước khi điều tra.

### 2.3 Lưu trữ bằng chứng

Khi bằng chứng không được điều tra tích cực, nó phải được lưu trữ ở một vị trí an toàn với khả năng tiếp cận hạn chế. Một trong những giải pháp tốt nhất là an toàn dữ liệu. Những chiếc két này có nhiều kích cỡ và được thiết kế đặc biệt để bảo vệ bằng chứng kỹ thuật số khỏi trộm cắp và hỏa hoạn. Một số loại phương tiện kỹ thuật số rất dễ bị tác động bởi nhiệt (ví dụ như băng keo). Một an toàn dữ liệu có thể giữ cho phương tiện ở nhiệt độ chấp nhận được đủ lâu (hy vọng) để đám cháy được dập tắt.

Các vị trí lưu trữ bằng chứng phải được khóa mọi lúc khi không được sử dụng tích cực. Một nhật ký hoặc dấu vết điều tra cũng nên được duy trì chi tiết những ai đã nhập, khi nào họ nhập và những gì họ đã xóa hoặc trả lại.

Việc truy cập vào kho lưu trữ bằng chứng và các khu vực nhạy cảm khác có thể được kiểm soát bằng nhiều phương tiện khác nhau bao gồm cả mã thông hành và thẻ khóa. Điều khiển điện tử có một số lợi thế khác biệt so với phím. Một lợi thế đáng kể là khả năng ghi nhật ký mỗi khi một cá nhân truy cập vào một khu vực hạn chế. Quá trình đánh giá này có thể rất hữu ích trong việc giám sát và xác minh chuỗi hành trình sản phẩm.

## Chính sách và thủ tục

Cách phòng thí nghiệm xử lý bằng chứng, tiến hành điều tra, lưu giữ hồ sơ và đảm bảo an toàn cho cơ sở của mình không nên để xảy ra tình huống ngẫu nhiên hoặc ý tưởng bất chợt của bất kỳ cá nhân nào. Các nhiệm vụ này cần được điều chỉnh bởi các chính sách và Quy trình hoạt động chuẩn (SOP) . SOP là tài liệu trình bày chi tiết, cùng với những thứ khác, cách thức thực hiện các cuộc giám định pháp y thông thường. Nghệ thuật viết SOP nằm ở chỗ tìm được sự cân bằng phù hợp giữa việc quá hẹp hoặc quá rộng. Nếu quá cụ thể, SOP sẽ thiếu tính linh hoạt cần thiết để giải quyết bất kỳ điều kiện bất thường nào có thể phát sinh. Trong pháp y kỹ thuật số, những tình huống này xảy ra thường xuyên hơn chúng ta mong muốn. Nếu quá rộng, chúng có thể không hiệu quả trong việc giữ cho mọi thứ nhất quán và đảm bảo tính toàn vẹn của bằng chứng.

Có những nguy hiểm cố hữu khi không tuân theo các chính sách và SOP của tổ chức bạn. Điều kỳ lạ là các câu hỏi về chính sách và SOP của tổ chức bạn sẽ được đưa ra trong quá trình thẩm tra chéo nếu vụ việc được đưa ra tòa.

## Đảm bảo chất lượng

Vào đầu những năm 1980, Ford Motor Company đã nói với chúng ta rằng “Chất lượng là Công việc 1”. Bạn có thể không tin điều đó ngày nay đối với Ford, nhưng điều đó chắc chắn là đúng đối với khoa học pháp y.

Đảm bảo chất lượng (QA) là một nguyên tắc cơ bản làm nền tảng cho mọi ngành học trong khoa học pháp y. Như vậy, mọi phòng thí nghiệm nên có một chương trình QA. Đảm bảo chất lượng được định nghĩa là “một hệ thống tài liệu đầy đủ về các giao thức được sử dụng để đảm bảo tính chính xác và độ tin cậy của các kết quả phân tích” ( [James & Nordby, 2009](#11__James_S__Nordby_JJ__Forensic) ). Một chương trình QA tốt sẽ bao gồm nhiều chủ đề bao gồm đánh giá đồng cấp các báo cáo, xử lý bằng chứng, tài liệu tình huống, đào tạo nhân viên phòng thí nghiệm, v.v. ( [James & Nordby, 2009](#11__James_S__Nordby_JJ__Forensic) ).

Quá trình xem xét có thể được chia thành hai loại rời rạc: xem xét kỹ thuật và xem xét hành chính.

Việc xem xét kỹ thuật, được thực hiện bởi một giám định viên riêng biệt, tập trung vào các kết quả và kết luận. Câu hỏi trọng tâm trong đánh giá kỹ thuật là "Các kết quả được báo cáo bởi người giám định ban đầu có được hỗ trợ bởi bằng chứng trong trường hợp không?"



Ngược lại, trọng tâm của việc xem xét hành chính là đảm bảo rằng tất cả các thủ tục giấy tờ đều có mặt và đã được hoàn thành một cách chính xác.



Năng lực của điều tra viên phải được xác nhận và ghi lại một cách thường xuyên. Trong cộng đồng pháp y, điều này được gọi là thử nghiệm thành thạo. Trong bài điều tra trình độ, điều tra viên phải chứng minh năng lực của mình bằng các bằng chứng giả. Có bốn loại bài điều tra trình độ:

1 . Thử nghiệm mở — (các) nhà phân tích và nhân viên hỗ trợ kỹ thuật biết rằng họ đang được thử nghiệm.

2 . Thử nghiệm mù — (các) nhà phân tích và nhân viên hỗ trợ kỹ thuật không biết họ đang được thử nghiệm.

3 . Thử nghiệm nội bộ — do chính cơ quan thực hiện.

4 . Điều tra bên ngoài — do một cơ quan độc lập với cơ quan được điều tra tiến hành. (Các Nhóm Công tác Khoa học về Công nghệ Hình ảnh và Bằng chứng Kỹ thuật số, 2011).

Các thử nghiệm này có thể được tiến hành trong nhà, với các nhân viên phòng thí nghiệm khác. Những kết quả này phải được lập thành văn bản vì tại một số điểm, kỹ năng và khả năng của nhà phân tích có thể bị nghi ngờ trong quá trình tố tụng tại tòa án. Tài liệu này sẽ rất quan trọng nếu điều đó xảy ra.

Trường hợp của Glen Woodall, mặc dù liên quan đến DNA, là một ví dụ mạnh mẽ về nhu cầu đảm bảo chất lượng. Vào ngày 8 tháng 7 năm 1997, Glen Woodall bị bồi thẩm đoàn Quận Cabell, Tây Virginia kết tội tấn công tình dục dã man hai phụ nữ. Anh ta bị kết án tổng hợp hai án chung thân với mức án bổ sung từ 203 đến 335 năm tù (Sáng kiến DNA). Việc bắt giữ và kết tội Woodall đã mang lại sự khép kín rất cần thiết cho cả các nạn nhân và sự bình yên cho cả cộng đồng nói chung. Thật không may cho các nạn nhân và cộng đồng, việc cứu trợ không kéo dài lâu.

Nhà khoa học pháp y trong trường hợp này là nhà huyết thanh học Fred Zain của Cảnh sát bang West Virginia. Sau một cuộc điều tra về công việc của Zain ở cả Tây Virginia và Texas, anh ta bị buộc tội khai man và giả mạo bằng chứng ( [Chan, 1994](#9__Chan__S___1994__August_21___S) ). Trong quá trình điều tra, người ta thấy rằng Woodall vô tội và anh ta cũng là nạn nhân. Sau khi thụ án bốn năm trong nhà tù ở Tây Virginia, Woodall được trả tự do và thưởng 1 triệu đô la từ tiểu bang cho việc bỏ tù oan sai của mình.

Những gì ban hội thẩm tìm thấy là cực kỳ đáng lo ngại. Họ phát hiện ra rằng Zain đã “bịa đặt hoặc thay đổi bằng chứng và nói dối về bằng cấp học vấn khi tuyên thệ.” Đó không phải là tất cả. Ban hội thẩm cũng phát hiện ra rằng những người giám sát của anh ấy cũng có thể bịp bợm, bỏ qua hoặc che giấu những lời phàn nàn về màn trình diễn của anh ấy ( [Chan, 1994](#9__Chan__S___1994__August_21___S) ).

Vào năm 2011, hai mươi bốn năm sau, nghi phạm thực sự bị bắt và cuối cùng bị kết án về những tội ác mà Woodall ban đầu bị kết tội. Vào ngày 1 tháng 4, Donald Good bị kết án hơn hai trăm năm tù ( [WSAZ, 2011](#18__WSAZ___2011__April_1___UPDAT) ). Những trường hợp như chiếc búa này cho thấy nhu cầu về các chương trình đảm bảo chất lượng hiệu quả trong tất cả các ngành khoa học pháp y.

### 4.1 Xác thực công cụ

Các công cụ của chúng ta, dù là phần cứng hay phần mềm, đều phải hoạt động như được thiết kế. Mỗi và mọi công cụ phải được xác thực trước khi sử dụng trong trường hợp thực tế. Quy trình xác thực chứng minh rõ ràng rằng công cụ đang hoạt động bình thường, đáng tin cậy và mang lại kết quả chính xác. Chúng ta không thể đơn giản chấp nhận lời của nhà sản xuất cho nó; giả định không được phép.

Quy trình xác nhận là một trong những quy trình phải được cam kết trên giấy tờ. Làm theo cách khác sẽ đặt bất kỳ bằng chứng nào được tìm thấy trong nguy cơ thực sự bị loại trừ.

### 4.2 Tài liệu

Không thể phóng đại tầm quan trọng của tài liệu đầy đủ và chính xác. Câu nói cổ "nếu bạn không viết nó ra, nó đã không xảy ra" thực sự là những từ để sống trong ngành công nghiệp này. Có nhiều loại tài liệu và báo cáo khác nhau được sử dụng trong toàn bộ quy trình pháp y. Những điều này nên được viết trong SOP của phòng thí nghiệm hoặc cơ quan và sổ tay chính sách. Biểu mẫu đệ trình, hồ sơ chuỗi hành trình, ghi chú của điều tra viên và báo cáo cuối cùng của điều tra viên là mấu chốt của tài liệu bắt buộc.

Thông thường, tất cả các thủ tục giấy tờ liên quan đến một vụ án cụ thể được thu thập thành một hồ sơ vụ án. Hồ sơ vụ án sẽ chứa tất cả các tài liệu liên quan đến vụ án, bao gồm cả giấy tờ do người giám định và những người khác tạo ra. Thông thường, chúng bao gồm các biểu mẫu đệ trình vụ án, yêu cầu hỗ trợ, ghi chú của giám định viên, báo cáo hiện trường vụ án, bản tường trình vụ án, bản sao của cơ quan khám xét, chuỗi hành trình tạm giữ, v.v. ( [Viện Tư pháp Quốc gia, 2004](#12__National_Institute_of_Justic) ).

#### 4.2.1 Các hình thức

Các biểu mẫu in sẵn được sử dụng rộng rãi trong cả hiện trường và phòng thí nghiệm. Họ giúp hướng dẫn nhân viên trong suốt quá trình và đảm bảo rằng chất lượng cao được duy trì. Các biểu mẫu đảm bảo tất cả các thông tin cần thiết được nắm bắt một cách thống nhất. Thông thường, các biểu mẫu được sử dụng để mô tả chi tiết bằng chứng (kiểu dáng, kiểu máy, số sê-ri, v.v.), ghi lại chuỗi hành trình, yêu cầu điều tra, v.v.

#### 4.2.2 Ghi chú của Điều tra viên

Ghi chú của điều tra viên bao gồm hầu hết, nếu không phải tất cả, các hành động và quan sát của điều tra viên cùng với ngày tháng tương ứng. Chúng phải đủ chi tiết để cho phép một điều tra viên khác sao chép quy trình được sử dụng trong quá trình điều tra. Những điều thường được ghi lại ở đây bao gồm:

Thảo luận với những người chơi chính bao gồm cả công tố viên và điều tra viên.



Các điểm bất thường được tìm thấy và các hành động liên quan được thực hiện.



Hệ điều hành, phiên bản và trạng thái bản vá.



Mật khẩu.



Mọi thay đổi đối với hệ thống bởi nhân viên phòng thí nghiệm và cơ quan thực thi pháp luật. ( [Viện Tư pháp Quốc gia, 2004](#12__National_Institute_of_Justic) )



Nếu bạn đã từng làm việc trong hệ thống pháp luật, thì bạn biết rằng bánh xe công lý có thể quay rất chậm. Điều này áp dụng cho cả vụ án hình sự và dân sự. Có thể mất vài tháng hoặc thậm chí nhiều năm trước khi một vụ án được đưa ra xét xử. Vào thời điểm bạn phải làm chứng, bạn chỉ có thể nhớ lại một vài dữ kiện, nếu có, của vụ án. Tài liệu về trường hợp và đặc biệt là các ghi chú của bạn, sẽ chứng minh một công cụ tuyệt vời để làm mới hồi ức của bạn.

#### 4.3.3 Báo cáo cuối cùng của Điều tra viên

Báo cáo cuối cùng của giám định viên là tài liệu chính thức được gửi cho các công tố viên, điều tra viên, luật sư đối lập, v.v. vào lúc hoặc gần khi kết thúc một cuộc điều tra. Các báo cáo này thường bao gồm:

Danh tính của cơ quan báo cáo.



Mã số hồ sơ / số hồ sơ.



Danh tính của người trình và người điều tra vụ án.



Ngày nhận và báo cáo



Mô tả chi tiết về các mục bằng chứng được gửi bao gồm số sê-ri, kiểu dáng, kiểu máy, v.v.



Danh tính của người giám định.



Mô tả các bước thực hiện trong quá trình khám bệnh.



Kết quả và kết luận. ( [Viện Tư pháp Quốc gia, 2004](#12__National_Institute_of_Justic) )



Khi soạn thảo báo cáo của người thẩm định cuối cùng, điều quan trọng là phải tính đến đối tượng dự kiến, chủ yếu là giáo dân. Các luật sư, điều tra viên, thẩm phán và khách hàng rất có thể sẽ có ít hoặc không có kiến thức kỹ thuật. Tất cả các báo cáo này thường chứa đầy những biệt ngữ kỹ thuật và các chi tiết chỉ nhằm mục đích gây thất vọng và gây nhầm lẫn cho phần lớn khán giả dự định của nó. Các báo cáo này phải dễ hiểu đối với đối tượng không phải là kỹ thuật viên. Các biệt ngữ và từ viết tắt phải được giữ ở mức tối thiểu tuyệt đối.

Hai phần chính trong báo cáo của giám định viên là phần tóm tắt và chi tiết của các phát hiện. Phần tóm tắt là một mô tả ngắn gọn về kết quả của cuộc điều tra. Người dùng cuối trong các báo cáo của chúng ta nhận thấy tính năng này hữu ích, đặc biệt là đối với lượng tải tiền khổng lồ và lượng thông tin mà họ thường xử lý. Các phát hiện ở đây cần được hỗ trợ và giải thích trong các kết quả chi tiết.

Các phát hiện chi tiết cung cấp nội dung của báo cáo. Họ cung cấp các chi tiết của cuộc điều tra, các bước thực hiện, kết quả, v.v. Thông thường, bạn có thể tìm thấy các chi tiết liên quan đến:

Các tệp liên quan trực tiếp đến yêu cầu.



Các tệp hỗ trợ các phát hiện.



Email, bộ nhớ cache web, nhật ký trò chuyện, v.v.



Tìm kiếm từ khóa.



Bằng chứng về quyền sở hữu của thiết bị. ( [Viện Tư pháp Quốc gia, 2004](#12__National_Institute_of_Justic) )



Bảng chú giải thuật ngữ là một bổ sung hữu ích cho báo cáo của điều tra viên. Bất cứ điều gì chúng ta có thể làm để giúp khán giả của chúng ta vượt qua mọi biệt ngữ xa lạ và từ viết tắt luôn là điều tốt. Truyền đạt những phát hiện của chúng ta theo cách có thể hiểu là trách nhiệm của chúng ta với tư cách là các chuyên gia pháp y.

## Công cụ pháp y kỹ thuật số

Các công cụ pháp y kỹ thuật số giúp công việc của chúng ta hiệu quả hơn nhiều hoặc thậm chí có thể. Có các công cụ cho các mục đích cụ thể cũng như các công cụ có chức năng rộng hơn. Chúng có thể ở dạng cả phần cứng hoặc phần mềm. Chúng có thể là các công cụ thương mại phải mua hoặc có thể là mã nguồn mở được cung cấp miễn phí. Có những lợi thế và bất lợi cho tất cả. Hãy nhớ rằng, không có công cụ duy nhất nào làm được mọi thứ hoặc làm mọi thứ cực kỳ tốt. Do đó, bạn nên chuẩn bị sẵn nhiều công cụ. Sử dụng nhiều công cụ cũng là một cách tuyệt vời để xác nhận những phát hiện của bạn. Kết quả giống nhau, với hai công cụ khác nhau, làm tăng đáng kể độ tin cậy của bằng chứng.

### 5.1 Lựa chọn công cụ

Thị trường công cụ pháp y kỹ thuật số tự hào có một số lượng lớn các sản phẩm, với nhiều sản phẩm được tung ra liên tục. Làm thế nào để người giám định biết công cụ nào đáng tin cậy và công cụ nào không? Làm thế nào để các công cụ này được xác nhận? Viện Tiêu chuẩn và Công nghệ Quốc gia (NIST) và Viện Tư pháp Quốc gia (NIJ) đã đạt được một bước tiến lớn trong việc giúp trả lời những câu hỏi này và những câu hỏi khác.

NIST đã khởi động Dự án Điều tra Công cụ Pháp y Máy tính (CFTT), thiết lập “phương pháp luận để điều tra các công cụ phần mềm pháp y máy tính bằng cách phát triển các đặc điểm kỹ thuật chung của công cụ, quy trình điều tra, tiêu chí điều tra, bộ điều tra và phần cứng điều tra” (Viện Tiêu chuẩn Quốc gia và Công nghệ).

Hãy khám phá xem nó trông như thế nào. Đây là đoạn trích từ thử nghiệm NIST của thiết bị chặn ghi phần cứng thương hiệu Tableau (HWB ), tóm tắt một số tiêu chí và kết quả thử nghiệm:

“Thiết bị HWB sẽ không truyền lệnh đến thiết bị lưu trữ được bảo vệ để sửa đổi dữ liệu trên thiết bị lưu trữ.”

“Đối với tất cả các trường hợp thử nghiệm được chạy, thiết bị luôn chặn bất kỳ lệnh nào đã thay đổi dữ liệu người dùng hoặc hệ điều hành được lưu trữ trên ổ đĩa được bảo vệ.”

“Một thiết bị HWB sẽ trả về dữ liệu được yêu cầu bởi một hoạt động đọc.”

“Đối với tất cả các trường hợp thử nghiệm được chạy, thiết bị luôn cho phép các lệnh đọc ổ đĩa được bảo vệ.” ( [Viện Tư pháp Quốc gia, 2009](#13__National_Institute_of_Justic) )

Mỗi công cụ, dù là phần cứng hay phần mềm, đều phải được xác thực trước khi sử dụng trên casework cũng như bất cứ khi nào nó được sửa đổi hoặc cập nhật. Ví dụ: giống như phần mềm khác mà bạn quen thuộc, phần mềm pháp y của chúng ta được cập nhật thường xuyên. Sau mỗi lần cập nhật, công cụ phải được xác thực lại. Việc xác nhận cũng tỏ ra hữu ích trước tòa, hỗ trợ tính hợp lệ của các kết quả của công cụ.

### 5.2 Phần cứng

Có rất nhiều công cụ phần cứng được thiết kế và xây dựng đặc biệt cho pháp y kỹ thuật số. Một số công cụ này bao gồm thiết bị sao y, thiết bị thu nhận điện thoại di động, trình chặn ghi, thiết bị lưu trữ di động, bộ điều hợp, cáp, v.v.

Như bạn có thể mong đợi, pháp y kỹ thuật số phụ thuộc nhiều vào nhiều loại phần cứng như PC, máy chủ, bộ chặn ghi, bộ dụng cụ điện thoại di động, cáp, v.v. [Hình 3.1](#F0010_3) cho thấy một máy trạm pháp y kỹ thuật số được trang bị tốt.



Hình 3.1 Một trong các máy trạm trong Phòng thí nghiệm Pháp y Kỹ thuật số của Cảnh sát Bang West Virginia đặt tại Trung tâm Khoa học Pháp y của Đại học Marshall. (Được phép của Cpl. Bob Boggs).

Máy tính là xương sống của bất kỳ phòng thí nghiệm pháp y kỹ thuật số nào. Vì vậy, là một giám định viên, bạn sẽ cần một máy trạm máy tính tốt nhất mà bạn có thể mua được. Các kỳ thi pháp y kỹ thuật số đòi hỏi khá nhiều khả năng tính toán. Những công việc này có thể đánh thuế ngay cả những hệ thống tốt nhất và đè bẹp những hệ thống không đo lường được. Một máy thi tốt có nhiều bộ vi xử lý đa lõi, càng nhiều RAM càng tốt (càng nhiều càng tốt) và ổ cứng lớn, nhanh. Các nhà sản xuất phần mềm pháp y cung cấp danh sách chi tiết các yêu cầu phần cứng tối thiểu và được đề xuất. Bạn tự chịu rủi ro khi đi lạc dưới mức tối thiểu. Để hiểu rõ hơn, hãy xem các yêu cầu hệ thống tối thiểu và được đề xuất (tính đến thời điểm báo chí) đối với Bộ công cụ pháp y của AccessData (FTK).

FTK của AccessData bao gồm bốn thành phần và hoặc ứng dụng riêng biệt. Họ đang:

1 . Cơ sở dữ liệu Oracle

2 . Giao diện người dùng FTK Client (UI)

3 . Công cụ xử lý phía máy khách

4 . Công cụ xử lý phân tán

Mức tối thiểu và thông số kỹ thuật được đề xuất sẽ thay đổi theo từng thành phần, nhưng đủ để nói rằng bạn không bao giờ có thể có quá nhiều RAM hoặc sức mạnh tính toán. Ví dụ, trên một máy chạy cơ sở dữ liệu Oracle, giao diện người dùng FTK và công cụ xử lý chính, AccessData đề xuất các yêu cầu được hiển thị trong [Bảng 3.1](#Top_of_CHP003_html) .

Bảng 3.1. Yêu cầu cơ bản được đề xuất ( [AccessData Group, LLC, 2011](#2__AccessData_Group__LLC___2011) )

|  |  |  |
| --- | --- | --- |
|  | Tối thiểu | Khuyến khích |
| Bộ xử lý | Intel ® i7 hoặc AMD tương đương | Intel ® i9 Dual Quad Core Xeon, i7 Nehalem hoặc AMD tương đương |
| ĐẬP | 12GB (DDR3) 8GB (DDR2) | 12GB (DDR3) 8GB (DDR2) |
| Hệ điều hành | Vista, 2008, Windows 7 (64 bit) | Vista, 2008, Windows 7 (64 bit) |

Một số thành phần có thể được cài đặt trên các máy riêng biệt. Các yêu cầu tối thiểu và được đề xuất sẽ thay đổi tùy thuộc vào cấu hình được sử dụng.

Người điều tra thường xuyên sàng lọc một lượng lớn dữ liệu. Do đó, các phòng thí nghiệm pháp y kỹ thuật số cần có khả năng lưu trữ một lượng lớn dữ liệu. Khi duyệt các PC được rao bán trên [bestbuy.com](http://bestbuy.com) , phần lớn chúng có dung lượng ổ cứng từ 500 GB đến 699 GB. Ổ đĩa multiterabyte cũng có sẵn. Với những con số như thế này và số thùng ngày càng tăng, thật dễ dàng nhận thấy rằng việc lưu trữ là một mối quan tâm lớn.

Pháp y kỹ thuật số không còn là nỗ lực “trung tâm của PC” nữa. Các thiết bị quy mô nhỏ như điện thoại di động và thiết bị GPS đang đổ vào các phòng thí nghiệm trên khắp đất nước. Các thiết bị này yêu cầu phần cứng khác với phần cứng được sử dụng trên máy tính xách tay và máy tính để bàn. Cellebrite's UFED hỗ trợ hơn ba nghìn điện thoại (Cellebrite Mobile Synchronization LTD). Paraben Corporation, một đối thủ cạnh tranh của Cellebrite, tự hào hỗ trợ hơn bốn nghìn điện thoại, PDA và thiết bị GPS (Paraben Corporation). Khi xử lý điện thoại di động, việc trang bị cáp thích hợp là rất quan trọng. Không giống như PC, thiết bị di động thiếu nhiều tiêu chuẩn liên quan đến đầu nối và cáp. Các phòng thí nghiệm cần có sẵn nhiều loại cáp để đối phó với vô số thiết bị cầm tay đi qua cửa. May mắn thay, các nhà sản xuất phần cứng pháp y điện thoại di động cung cấp nhiều loại cáp cần thiết.

Một số công ty sản xuất thiết bị sao chép phần cứng. Nếu bạn nhớ lại, bản sao pháp y là bản sao “dòng bit” của một phần phương tiện cụ thể như ổ cứng. Những công cụ này thực sự có thể tăng tốc quá trình, sao chép nhiều ổ đĩa cùng một lúc. Chúng cũng có thể cung cấp tính năng bảo vệ ghi, xác thực băm, xóa ổ đĩa, theo dõi điều tra và hơn thế nữa.

#### 5.2.1 Thiết bị khác

Phần cứng và phần mềm mà chúng ta đã thảo luận trước đó không phải là thiết bị duy nhất cần thiết. Bộ dụng cụ hiện trường vụ án rất hữu ích bên ngoài phòng thí nghiệm. Những bộ dụng cụ này được tải sẵn tất cả các vật dụng mà người giám định cần trong hiện trường để thu thập bằng chứng kỹ thuật số. Bộ dụng cụ chứa các vật dụng tiêu chuẩn như bút, máy ảnh kỹ thuật số, phương tiện lưu trữ sạch sẽ, túi đựng bằng chứng, băng bằng chứng, biểu mẫu báo cáo, bút đánh dấu vĩnh viễn và những thứ tương tự.

### 5.3 Phần mềm

Hiện nay trên thị trường có rất nhiều sản phẩm phần mềm pháp y kỹ thuật số. Một số là các công cụ chung phục vụ nhiều chức năng khác nhau. Những người khác tập trung hơn, phục vụ một mục đích khá hạn chế. Các ứng dụng này có xu hướng tập trung vào một loại bằng chứng rất cụ thể, chẳng hạn như e-mail hoặc Internet.

Khi lựa chọn phần mềm, cần phải lựa chọn giữa việc sử dụng các công cụ mã nguồn mở hoặc một sản phẩm được sản xuất thương mại. Có những lợi thế và bất lợi cho cả hai. Các yếu tố như chi phí, chức năng, khả năng và hỗ trợ là một số tiêu chí có thể được sử dụng để đưa ra quyết định này.

Tài nguyên bổ sung

Công cụ nguồn mở

Cuốn sách của Cory Altheide và Harlan Carvey's Digital Forensics With Open Source Tools là một tài liệu tham khảo tuyệt vời cho những người thực hành sử dụng các ứng dụng này.

Một trong những công cụ nguồn mở phổ biến hơn là SIFT, hoặc Bộ công cụ pháp y điều tra SANS. SIFT Workstation là một công cụ mã nguồn mở, miễn phí, mạnh mẽ. Nó được xây dựng trên hệ điều hành Linux Ubuntu. Công cụ này có khả năng khắc tệp cũng như phân tích hệ thống tệp, lịch sử web, thùng rác và hơn thế nữa. Nó cũng có thể phân tích lưu lượng mạng và bộ nhớ dễ bay hơi. Nó cũng có thể tạo ra một dòng thời gian, có thể vô cùng hữu ích trong quá trình điều tra. SIFT hỗ trợ các hệ thống tệp sau:

Windows (MSDOS, FAT, VFAT, NTFS)



MAC (HFS)



Solaris (UFS)



Linux (EXT2 / 3/4)



(Viện SANS)

Đối với các công cụ thương mại, hai trong số các công cụ phần mềm phổ biến nhất là Bộ công cụ pháp y (FTK ® ) từ AccessData và EnCase ® từ Phần mềm Hướng dẫn. Cả hai đều xuất sắc và có thể làm cho các kỳ thi trở nên dễ dàng và hiệu quả hơn. Các ứng dụng này có các khả năng giống như “con dao Quân đội Thụy Sĩ”. Họ thực hiện vô số tác vụ, bao gồm:

Đang tìm kiếm



Phân tích e-mail



Sắp xếp



Báo cáo



Bẻ khóa mật khẩu



Các công cụ tìm kiếm trong các sản phẩm này đặc biệt mạnh mẽ và cung cấp cho người điều tra khả năng đi sâu vào tìm kiếm chính xác thông tin họ đang tìm kiếm. Dưới đây là danh sách nhanh một số thông tin có thể được tìm kiếm:

Địa chỉ e-mail



Tên



Số điện thoại



Từ khóa



Địa chỉ web



Loại tập tin



Phạm vi ngày



Những công cụ này có thể hữu ích nhưng chúng có một số hạn chế. Thực tế là không có công cụ duy nhất nào làm được tất cả. Vì lý do đó, ngân sách cho phép, các phòng thí nghiệm cần phải có sẵn nhiều công cụ khác nhau.

Ngày càng có nhiều công cụ đặc biệt được tung ra thị trường. Các công cụ này tập trung vào một khía cạnh của bằng chứng kỹ thuật số như e-mail hoặc bằng chứng dựa trên web. Những điều này có thể mang lại một số khả năng bổ sung cho bảng mà một số công cụ đa năng không có.

Báo động!

Sự phụ thuộc vào các công cụ

Các công cụ pháp y dựa trên GUI có thể trở thành một chiếc nạng. Các công cụ “nút bấm” có thể làm cho kỳ thi hiệu quả hơn nhiều, nhưng chúng không làm cho điều tra viên bớt trách nhiệm hiểu những gì đang diễn ra bên dưới bề mặt. Người giám định không chỉ cần hiểu công cụ đang làm gì, mà còn cả cách tạo tác được đề cập đến để bắt đầu.

Một số công cụ pháp y mà giám định viên có thể sử dụng được liệt kê trong [Bảng 3.2](#Top_of_CHP003_html) . Nhiều công ty trong số này cung cấp các video hướng dẫn hoặc trình diễn sản phẩm của họ. Đây có thể là một nguồn thông tin bổ sung tuyệt vời. Chúng thường có sẵn từ trang web của họ hoặc trên YouTube. Điều này không có nghĩa là một sự chứng thực của một công cụ cụ thể. Đây chỉ là một mẫu đại diện của nhiều công cụ có sẵn.

Bảng 3.2. Một số công cụ phần cứng và phần mềm có thể được tìm thấy trong phòng thí nghiệm pháp y kỹ thuật số

|  |  |  |
| --- | --- | --- |
| Dụng cụ | Sử dụng | URL |
| bộ công cụ pháp y  , LLC | Công cụ đa năng (thu thập, xác minh, tìm kiếm, báo cáo, xóa, v.v.) | <http://accessdata.com> |
| EnCase  , Inc. | Công cụ đa năng (thu thập, xác minh, tìm kiếm, báo cáo, xóa, v.v.) | <http://www.guidancesoftware.com> |
| SMART & SMART cho  Dữ liệu ASR Linux, Thu thập và Phân tích Dữ liệu, LLC | Công cụ đa năng (thu thập, xác minh, tìm kiếm, báo cáo, xóa, v.v.) | <http://www.asrdata.com/forensic-software/> |
| X-Ways Forensics  Công nghệ phần mềm X-Ways AG | Công cụ đa năng (thu thập, xác minh, tìm kiếm, báo cáo, xóa, v.v.) | <http://www.x-ways.net/forensics/> |
| Helix3 Pro  e-fense, Inc. | Công cụ đa năng (thu thập, xác minh, tìm kiếm, báo cáo, xóa, v.v.) | <http://www.e-fense.com/products.php> |
| Softblock, Macquisition, Blacklight  BlackBag Technologies, Inc. | Nhiều công cụ pháp y Macintosh | <https://www.blackbagtech.com/forensics.html> |
| Mac Marshall  Architecture Technology Corporation | Nhiều công cụ pháp y Macintosh | <http://www.macmarshal.com/> |
| Raptor  Forward Discovery, Inc. | Công cụ thu thập và xem trước dựa trên Linux | [http://www.nticdiscovery.com/Raptor](http://www.forwarddiscovery.com/Raptor) |
| Dossier  Logicube, Inc. | Mua lại phần cứng | <http://www.logicube.com/> |
| Công cụ phần cứng pháp y  Tableau | Viết chặn, cầu nối, lưu trữ, mua lại | <http://www.tableau.com/> |
| Wiebetech | Bộ chặn lưu trữ, ghi, v.v. | <http://www.wiebetech.com/home.php> |

## Sự công nhận

Công nhận là sự xác nhận các chính sách và thủ tục của phòng thí nghiệm điều tra tội phạm, cách nó hoạt động, nếu bạn muốn ( [James & Nordby, 2009](#11__James_S__Nordby_JJ__Forensic) ). Hiệp hội Giám đốc Phòng thí nghiệm điều tra tội phạm Hoa Kỳ / Ban Công nhận Phòng thí nghiệm (ASCLD / LAB) được công nhận là tổ chức hàng đầu thế giới về công nhận các phòng thí nghiệm pháp y. Bất chấp tên gọi, ASCLD / LAB cấp chứng nhận cho các phòng thí nghiệm ở cả trong và ngoài Hoa Kỳ, điều mà nó đã được thực hiện từ năm 1982 (Barbara).

Có trụ sở tại Garner, North Carolina, ASCLD / LAB đã công nhận tổng cộng 385 phòng thí nghiệm điều tra tội phạm, 17 trong số đó nằm ngoài Hoa Kỳ (Hội đồng Giám đốc Phòng thí nghiệm điều tra tội phạm Hoa Kỳ / Ban Công nhận Phòng thí nghiệm).

Theo ASCLD / LAB, họ có bốn mục tiêu. Họ phải:

1 . nâng cao chất lượng các dịch vụ xét nghiệm cung cấp cho hệ thống tư pháp hình sự.

2 . phát triển và duy trì các tiêu chí mà phòng thí nghiệm có thể sử dụng để đánh giá mức độ hoạt động của phòng thí nghiệm và để củng cố hoạt động của phòng thí nghiệm.

3 . cung cấp một hệ thống độc lập, công bằng và khách quan mà qua đó các phòng thí nghiệm có thể hưởng lợi từ việc đánh giá tổng thể hoạt động.

4 . cung cấp cho công chúng và người sử dụng dịch vụ phòng thí nghiệm một phương tiện để xác định những phòng thí nghiệm đã chứng minh rằng họ đáp ứng các tiêu chuẩn đã được thiết lập (Hiệp hội Giám đốc Phòng thí nghiệm điều tra tội phạm Hoa Kỳ / Ban Công nhận Phòng thí nghiệm).

Hãy coi ASCLD / LAB là “Con dấu phê duyệt của dịch vụ quản lý tốt” cho khoa học pháp y. Việc kiếm được và duy trì chứng nhận ASCLD / LAB không phải là việc dễ dàng. Nó đòi hỏi một lượng lớn thời gian, kế hoạch, tài liệu và tiền bạc. Không có gì được coi là đương nhiên. Mọi tiêu chuẩn được đáp ứng phải được sao lưu với tài liệu chi tiết, phong phú.

ASCLD / LAB cung cấp hai chương trình công nhận. Thứ nhất là chương trình kế thừa và thứ hai là chương trình quốc tế. Chương trình kế thừa là chương trình đầu tiên do ASCLD / LAB thiết lập. Như bạn có thể mong đợi, có sự khác biệt giữa hai chương trình cũng như một số điểm chung. Một sự khác biệt chính là số lượng các tiêu chí phải được đáp ứng trong mỗi chương trình. Chương trình quốc tế có nhiều tiêu chuẩn cần đáp ứng hơn nhiều so với chương trình kế thừa. Các phòng thí nghiệm đang tìm kiếm sự công nhận theo chương trình quốc tế phải đáp ứng các yêu cầu liên quan để chứng minh sự phù hợp với các yêu cầu áp dụng của cả ISO / IEC 17025: 1999 (E) Yêu cầu chung về năng lực của các phòng thử nghiệm và hiệu chuẩn và ASCLD / LAB-International Yêu cầu bổ sung đối với việc công nhận các phòng thí nghiệm điều tra và hiệu chuẩn khoa học pháp y.

Mặc dù công nhận là rất mong muốn, nhưng nó không phải là bắt buộc. Các phòng thí nghiệm không được công nhận có thể xử lý thành công bằng chứng. Thực tế là có được và duy trì một phòng thí nghiệm pháp y được công nhận là một đề xuất tốn nhiều tiền mặt và công sức. Loại cam kết về nhân sự và kinh phí cần thiết rất khó để đảm bảo và thành thật mà nói không phải là một lựa chọn cho tất cả mọi người.

### 6.1 Hiệp hội Vật liệu và Thử nghiệm Hoa Kỳ (ASTM)

Ngoài ASCLD / LAB, ASTM International cũng cung cấp các tiêu chuẩn cho các lĩnh vực khác nhau trong khoa học pháp y, bao gồm cả pháp y kỹ thuật số. ASTM International trước đây được gọi là Hiệp hội Vật liệu và Thử nghiệm Hoa Kỳ . Nó được thành lập vào năm 1898 bởi các kỹ sư và nhà hóa học của Đường sắt Pennsylvania. Các tiêu chuẩn được phát triển bởi các chuyên gia chủ đề là thành viên của ASTM (ASTM quốc tế).

### 6.2 Công nhận so với chứng nhận

Các điều khoản này có vẻ có thể thay thế cho nhau; tuy nhiên, trong bối cảnh của một phòng thí nghiệm pháp y, chúng không như vậy. Như đã mô tả trước đó, công nhận đề cập đến phòng thí nghiệm, trong khi chứng nhận liên quan đến cá nhân người điều tra. Chứng chỉ thường yêu cầu một giám định viên phải vượt qua (các) bài điều tra viết hoặc thực hành.

Nhóm Công tác Khoa học về Bằng chứng Kỹ thuật số (SWGDE) đã ban hành một bài báo đề cập đến việc cấp chứng chỉ hành nghề pháp y kỹ thuật số. SWGDE khẳng định rằng bất kỳ chứng nhận pháp y kỹ thuật số nào đều phải đáp ứng các năng lực cốt lõi sau, ở mức tối thiểu:

1 . Các thủ tục trước khi khám và các vấn đề pháp lý

2 . Đánh giá và phân tích phương tiện

3 . Phục hồi dữ liệu

4 . Phân tích cụ thể dữ liệu đã phục hồi

5 . Tài liệu và báo cáo

6 . Trình bày kết quả ( [Nhóm công tác khoa học về bằng chứng kỹ thuật số, 2010](#16__Scientific_Working_Group_on) )

## Bản tóm tắt

Phòng thí nghiệm pháp y đóng một vai trò quan trọng trong hệ thống tư pháp của chúng ta. Bằng chứng pháp y được trình bày tốt có thể rất, rất thuyết phục đối với bồi thẩm đoàn. Nhiều, rất nhiều trường hợp tự bật bằng chứng pháp y hoặc thiếu bằng chứng pháp y. Phòng thí nghiệm pháp y do đó đóng một vai trò quan trọng trong việc tìm kiếm công lý.

Chất lượng phải được ưu tiên trong mọi phòng thí nghiệm pháp y và mọi chuyên gia pháp y. Pháp y kỹ thuật số không có gì khác biệt. Chất lượng đạt được thông qua việc tuân thủ nghiêm ngặt các tiêu chuẩn chất lượng đã thiết lập như một phần của chương trình đảm bảo chất lượng tổng thể. Công nhận phòng thí nghiệm pháp y kỹ thuật số là một cách để đảm bảo tuân thủ các tiêu chuẩn này. Tổ chức hàng đầu thế giới được công nhận về công nhận các phòng thí nghiệm pháp y là ASCLD / LAB. Tiêu chuẩn cho pháp y kỹ thuật số được soạn thảo bởi ASTM.

Công nhận và chứng nhận không đồng nghĩa với nhau. Sự khác biệt cơ bản là sự công nhận liên quan đến phòng thí nghiệm vật lý, nơi chứng nhận áp dụng cho nhân viên thực hiện các cuộc điều tra. Không chỉ các giám định viên phải được điều tra để chứng minh rằng họ “hoạt động bình thường”, mà các công cụ của họ cũng vậy. Chỉ những công cụ đã được điều tra và chứng minh là đáng tin cậy mới được sử dụng khi xử lý một trường hợp. Quy trình điều tra này được gọi là xác nhận.

Người hành nghề pháp y kỹ thuật số sử dụng cả phần mềm và công cụ phần cứng trong công việc của họ. Không có một công cụ duy nhất nào làm tốt mọi thứ hoặc làm tốt điều đó. Hầu hết các phòng thí nghiệm sẽ có nhiều loại công cụ khác nhau để cung cấp cho họ khả năng rộng lớn mà họ cần với hàng loạt công nghệ mà họ thấy đang sẵn sàng để phân tích.

## Tổng kết và kiến thức thêm chương 3

1. **Mô tả được chức năng và khi nào áp dụng công cụ để phân tích tệp tin hệ thống**

**Hex Editor** (công cụ đọc mã hex)

**Chức năng**: Phân tích file thông qua mã hex của tệp tin

**Áp dụng khi**: Tội phạm mạng thay đổi files extension (.doc; .jpg) nhằm che dấu hình ảnh, thông tin

Mã hex của một số files extension

.JPEG: bắt đầu với ff d8 ff

.BMP: bắt đầu với 42 4d

.GIF: Bắt đầu với 47 49 46 39

Và một số thông tin khác dựa theo bài thuyết trình

**The Sleth Kit**

Là một thư viện lệnh bao gồm các lệnh nhằm hỗ trợ cho việc điều tra dữ liệu ổ đĩa và thông tin từ hệ thống

Có 2 công cụ điều tra chính trong bộ thư viện này là

* Công cụ điều tra tệp tin hệ thống

Chức năng: Thu thập, tìm kiếm thông tin liên quan đến hệ điều hành và bản sao phần mềm của ổ đĩa vật lý (disk image)

Áp dụng khi: Điều tra bằng chứng có liên quan đến OS hoặc disk image

* Công cụ điều tra dữ liệu ổ đĩa

Chức năng: Điều tra các thông tin liên quan đến ổ đĩa và các phần cứng khác

Áp dụng khi: Điều tra bằng chứng có liên quan đến ổ đĩa và phần cứng tách rời (Media)

1. **Hiểu được yêu cầu cần thiết để thực hiện một cuộc điều tra số**

Thông thường, để thực hiện một cuộc điều tra số, đối tượng yêu cầu cần đảm bảo có đầy đủ công cụ, thiết bị, cũng như kĩ năng để thực hiện một cuộc điều tra. Điều này đúng với mọi loại hình điều tra số, kể cả khi quản trị viên điều tra hệ thống. Trong trường hợp công ty điều tra số nhân sự cần phải đảm bảo có được sự chấp thuận của bên bị điều tra hoặc chỉ điều tra trên vật chứng được sở hữu bởi công ty.

1. **Các công cụ điều tra số thường được sử dụng nhằm phục vụ điều tra vật chứng**

* Linux: Linux có lệnh dd và dcfldd để sao y thông tin từ ổ đĩa.
* Windows: AccessData FTK Imager (Thuộc Sleath Tool Kit)
* RAID: X-Ways Forensics
* Remote Data Acquisition: F-Response
* **UltraKit (công cụ bảo vệ vật lý)** – đây là bộ công cụ để bảo vệ cho vật lý của các vật chứng
* **Forensic Falcon (công cụ thu thập thông tin tại chỗ**)– đây là thiết bị có khả năng sao y, xác mình, xem xet, điều tra và cho phép điều tra viên sao y lại thông tin hệ thống cũng như kết nối từ xa
* **EnCase Forensic (công cụ thu thập, điều tra, phân tích thông tin)–** Phần mềm này có thể thu thập dữ liệu từ nhiều nguồn khác nhau, hỗ trợ chỉ định các thông số có giá trị sau khi phân tích ổ đĩa, hỗ trợ trong việc xuất báo cáo về các thông tin thu thập được, đảm bảo được tính an toàn của công cụ thu thập do được tin tưởng bởi các chuyên gia, tổ chức điều tra số.

Tài liệu tham khảo

1. Giới thiệu: Hiệp hội Giám đốc Phòng thí nghiệm điều tra tội phạm Hoa Kỳ / Ban Công nhận Phòng thí nghiệm . (nd). Truy cập ngày 4 tháng 6 năm 2011, từ: <http://www.ascld-lab.org/about_us/aboutoverview.html>.

2. Nhóm AccessData, LLC. (2011, tháng 2). Tải xuống: AccessData . Được truy cập ngày 24 tháng 8 năm 2011, từ: [http://accessdata.com/downloads/media/FTK\_3x\_System\_Specilities\_Guide.pdf](http://accessdata.com/downloads/media/FTK_3x_System_Specifications_Guide.pdf) .

3. Hội đồng Giám đốc Phòng thí nghiệm điều tra tội phạm Hoa Kỳ / Ban Công nhận Phòng thí nghiệm. (nd). Bạn có biết: Hiệp hội Giám đốc Phòng thí nghiệm điều tra tội phạm Hoa Kỳ / Ban Công nhận Phòng thí nghiệm . Truy cập ngày 4 tháng 6 năm 2011, từ: <http://www.ascld-lab.org/largest_accreditation.html>.

4. Hội đồng Giám đốc Phòng thí nghiệm điều tra tội phạm Hoa Kỳ / Ban Công nhận Phòng thí nghiệm. (nd). Mục tiêu: Hiệp hội Giám đốc Phòng thí nghiệm điều tra tội phạm Hoa Kỳ / Ban Công nhận Phòng thí nghiệm . Truy cập ngày 4 tháng 6 năm 2011, từ: <http://www.ascld-lab.org/about_us/objectives.html>.

5. Barbara, JJ (nd). Chứng nhận bằng chứng kỹ thuật số . Được truy cập ngày 25 tháng 8 năm 2011, từ: <http://www.forensicmag.com/article/digital-evidence-accreditation?page=0,3>.

6. Barbara, JJ (nd). Công nhận bằng chứng kỹ thuật số: Tạp chí pháp y . Truy cập ngày 4 tháng 6 năm 2011, từ: <http://www.forensicmag.com/article/digital-evidence-accreditation>.

7. Brunty, J. (2011, ngày 2 tháng 3). Xác thực các công cụ và phần mềm pháp y: Hướng dẫn nhanh cho Giám định viên pháp y kỹ thuật số . Được truy cập ngày 24 tháng 8 năm 2011, từ: <http://www.dfinews.com/article/validation-forensic-tools-and-software-quick-guide-digital-forensic-examiner?page=0,2>.

8. Người vận chuyển, BB (2002, tháng 10). Bài báo: [Digital-evidence.org](http://Digital-evidence.org) . Truy cập ngày 24 tháng 8 năm 2011, từ: <http://www.digital-evidence.org/papers/opensrc_legal.pdf>.

9. Chan, S. (1994, ngày 21 tháng 8). Điểm của Niềm tin Được đánh giá là Nhà hóa học Đối mặt với Những lời buộc tội tổn thương . Lấy từ [LATimes.com](http://www.LATimes.com) : <http://articles.latimes.com/1994-08-21/news/mn-29449_1_lab-tests-fred-zain-double-murder>(Truy cập 21.08.94).

10. Cục Điều tra Liên bang. Phòng thí nghiệm Pháp y Máy tính Khu vực Báo cáo Thường niên Năm Tài chính 2010 Washington, DC: Bộ Tư pháp Hoa Kỳ; Năm 2010.

11. James S, Nordby JJ. Khoa học pháp y: Giới thiệu về các kỹ thuật điều tra và khoa học Ấn bản thứ ba Boca Raton, FL: CRC Press; Năm 2009.

12. Viện Tư pháp Quốc gia. Điều tra pháp y đối với bằng chứng kỹ thuật số: Hướng dẫn thực thi pháp luật Washington, DC: Bộ Tư pháp Hoa Kỳ; Năm 2004.

13. Viện Tư pháp Quốc gia. Kết quả điều tra thiết bị khối ghi phần cứng: Cầu SCSI của pháp y T4 (Giao diện FireWire) Washington, DC: Viện Tư pháp Quốc gia; Năm 2009; Bộ Tư pháp Hoa Kỳ, Văn phòng các Chương trình Tư pháp.

14. Viện Tiêu chuẩn và Công nghệ Quốc gia. (nd). Trang web của Dự án Điều tra Công cụ Pháp y Máy tính: Viện Tiêu chuẩn và Công nghệ Quốc gia . Truy cập ngày 6 tháng 6 năm 2011, từ: <http://www.cftt.nist.gov/index.html>.

15. Saferstein R. Tội phạm học: Giới thiệu về Khoa học Pháp y (Phiên bản Cao đẳng) Lần xuất bản thứ 9. Upper Saddle River, NJ: Prentice Hall; Năm 2006.

16. Nhóm Công tác Khoa học về Bằng chứng Kỹ thuật số. (2010, ngày 15 tháng 5). Yêu cầu tối thiểu để đảm bảo chất lượng trong xử lý bằng chứng kỹ thuật số và đa phương tiện . Truy cập ngày 24 tháng 8 năm 2011, từ: <http://www.swgde.org/documents/current-documents/>.

17. Whitcomb, CA (nd). Phòng thí nghiệm pháp y kỹ thuật số ảo . Largo, FL: Trung tâm Khoa học Pháp y Quốc gia.

18. WSAZ. (2011, ngày 1 tháng 4). CẬP NHẬT: Donald Good nhận được hai bản án cuộc đời trong vụ án hiếp dâm trung tâm mua sắm . Lấy từ [WSAZ.com](http://www.WSAZ.com) : <http://www.wsaz.com/news/headlines/UPDATE_Judge_OHanlon_Will_Preside_Over_Huntington_Mall_Rape_Case.html>(Truy cập

# Chương 4: Thu thập bằng chứng

**Thông tin trong Chương này:**

Giới thiệu về hiện trường tội phạm



Ghi lại hiện trường và bằng chứng



Thiết lập và Duy trì Quy trình Giám sát Nguồn gốc



Sao y pháp y bằng chứng



Xử lý hệ thống sống và hệ thống chết



Sử dụng băm để xác minh tính toàn vẹn của bằng chứng



Soạn thảo Báo cáo cuối cùng của Điều tra viên



Các vụ kiện có thể thắng hoặc thua dựa trên cách thu thập bằng chứng kỹ thuật số. Bằng chứng kỹ thuật số rất mong manh và phải được xử lý cẩn thận. Chúng ta sẽ khám phá cách thu thập bằng chứng đúng cách từ các thiết bị khác nhau để người giám định có cơ hội trình bày bằng chứng khó tìm thấy của họ bên ngoài phòng thí nghiệm.

Quy trình giám sát nguồn gốc, Hệ thống sống, Hệ thống chết, Bộ nhớ biến động, Thứ tự biến động, Hàm băm, Thuật toán, Faraday

## Giới thiệu

Bằng chứng mà bạn phát hiện sẽ không bao giờ đến được với bồi thẩm đoàn trừ khi nó được thu thập và tính toán đúng cách để bắt đầu tại hiện trường. Quan trọng là bạn sẽ không bao giờ thấy nó được thực hiện ngay trên các chương trình cảnh sát trên TV. Không có gì giết chết sự phấn khích nhanh hơn ba giờ làm thủ tục giấy tờ đảm bảo. Trong thế giới thực, ba giờ làm thủ tục giấy tờ đảm bảo đó sẽ đưa bằng chứng của bạn ra tòa. Tất cả bắt đầu tại hiện trường vụ án. Chỉ cần xác định bằng chứng là có thể khó khăn. Đặc biệt là với thẻ nhớ cỡ con tem (hoặc nhỏ hơn) và những thứ tương tự. Chúng có thể được giấu ở một số lượng gần như vô hạn.

Tại hiện trường, các giám định có thể phải đối mặt với nhiều thiết bị và phương tiện lưu trữ. Họ có thể tìm thấy một hoặc nhiều máy tính đang chạy và các thiết bị không dây như điện thoại di động. Cùng nhau, họ đưa ra một số thử thách độc đáo cho điều tra viên.

Các hành động trong quá trình thu thập phải được ghi chép đầy đủ. Ghi chú, ảnh, video và bản phác thảo ghi lại hành động của chúng ta và làm mới hồi ức của chúng ta. Vì bằng chứng kỹ thuật số rất dễ bay hơi, nên việc bảo quản là điều tối quan trọng. Nếu có thể, một hình ảnh pháp y hoặc bản sao được tạo ra từ phương tiện nghi ngờ. Kỳ thi được tiến hành trên bản sao (là một bit chính xác cho bản sao bit) chứ không phải là bản gốc.

## Hiện trường vụ án và thu thập bằng chứng

Từ quan điểm thực tế, không phải tất cả các cảnh liên quan đến bằng chứng kỹ thuật số đều được tạo ra hoặc đối xử bình đẳng. Bằng chứng kỹ thuật số đã và đang là trọng tâm của tố tụng hình sự, dân sự và nội bộ doanh nghiệp. Có sự khác biệt rõ ràng về cách hiện trường và bằng chứng có thể được xử lý và ghi lại cho các thủ tục tố tụng này. Một số trường hợp, chẳng hạn như một vụ giết người, sẽ yêu cầu tài liệu cẩn thận. Những trường hợp khác, như một tranh chấp dân sự, sẽ yêu cầu ít một tài liệu hơn. Mặc dù thừa nhận những khác biệt nhỏ này, nhưng có một số nguyên tắc và giao thức cốt lõi nhất định sẽ vẫn nhất quán.

Sau khi hiện trường được coi là an toàn, công việc đầu tiên tại hiện trường vụ án kỹ thuật số, hoặc bất kỳ công việc nào khác, là lệnh khám xet tính toàn vẹn của vật chứng. Hiện trường và bằng chứng của nó phải được bảo vệ khỏi các tác động vô tình hoặc cố ý. Việc bảo mật một hiện trường tội phạm truyền thống đòi hỏi phải hạn chế khả năng tiếp cận vật lý của những người không có lý do chính đáng để ở đó. Những người hàng xóm, giới truyền thông và cảnh sát giám sát là những kẻ đột nhập hiện trường vụ án điển hình. Bảo vệ một hiện trường truyền thống được thực hiện bằng cách xâu chuỗi băng ghi âm hiện trường vụ án, lính canh hoặc đơn giản là yêu cầu mọi người rời đi.

Ngược lại, đối với bằng chứng kỹ thuật số cho thấy một khía cạnh tiếp cận hoàn toàn mới. Hầu hết các máy tính và thiết bị kỹ thuật số đều được kết nối với Internet, mạng di động hoặc các loại mạng khác. Chính kết nối này cho phép truy cập từ xa và khiến bằng chứng gặp rủi ro. Máy tính và thiết bị không dây phải được đặt ở chế độ không truy cập được ngay khi bạn chắc chắn rằng không có dữ liệu dễ bay hơi nào bị mất ( [Hiệp hội Cảnh sát trưởng, 2011](#6__Association_of_Chief_Police_O) ). Đối với máy tính, có thể là vấn đề tháo cáp Ethernet hoặc rút modem hoặc bộ định tuyến không dây. Với các thiết bị không dây như điện thoại di động, chúng ta phải thực hiện các bước để cách ly điện thoại khỏi các tín hiệu mạng.

### 2.1 Phương tiện có thể tháo rời

Nếu được pháp luật cho phép (chẳng hạn như có giấy đảm bảo), chúng ta sẽ tìm kiếm bất kỳ nơi nào có thể chứa một phần phương tiện lưu trữ. Xem xét thẻ nhớ “cỡ con tem” ngày nay, mảnh bằng chứng này có thể được giấu ở hầu hết mọi nơi chẳng hạn như trong sách, ví, băng đô, v.v.

Mặc dù có kích thước nhỏ, thẻ nhớ có thể chứa rất nhiều bằng chứng tiềm ẩn như nội dung “đen” hoặc số thẻ tín dụng bị đánh cắp.. Điều tra nhanh [Amazon.com](http://Amazon.com) cho thấy rằng bạn có thể mua thẻ nhớ 64 gigabyte với giá khoảng 120 đô la. Gigabyte (GB) khá trừu tượng đối với hầu hết chúng ta. Thay vì sử dụng một đơn vị lưu trữ dữ liệu tiêu chuẩn, chúng ta sẽ sử dụng một ví dụ ít thông thường hơn nhưng dễ liên quan hơn.

Chúng ta sẽ chuyển đổi thẻ nhớ 64 GB thành đơn vị đo lường của riêng mình, mà chúng ta sẽ gọi là “Potters” — chính xác làHarry là “Potters”. Hình dung một bộ gồm tất cả bảy cuốn sách trong bộ truyện Harry Potter. Theo con số thô, mỗi GB chứa khoảng 109 bộ hoàn chỉnh. Với một số phép toán đơn giản, chúng ta thấy rằng thẻ nhớ 64 GB của chúng ta có thể chứa khoảng bảy nghìn bộ sách hoàn chỉnh trên một thứ có kích thước bằng một con tem bưu chính! Hãy nghĩ về số lượng bằng chứng có thể được lấy ra chỉ từ một thẻ nhớ.

#### 2.1.1 Phương tiện lưu trữ có thể tháo rời

Phương tiện lưu trữ có thể tháo rời bao gồm những thứ như DVD, ổ cứng ngoài, ổ cứng và thẻ nhớ.

Chúng ta không chỉ quan tâm đến các thiết bị và phương tiện lưu trữ tại hiện trường; khu vực xung quanh và các mặt hàng cũng đáng xem. Ví dụ, sách và sách hướng dẫn có thể cung cấp cho các nhà điều tra manh mối về trình độ kỹ năng của mục tiêu và loại công nghệ mà họ có thể chống lại. Có lẽ phần thưởng lớn nhất là một cảnh báo về khả năng sử dụng mã hóa. Bao bì bỏ vào thùng rác cũng có thể hữu ích. Bất kỳ giám định viên pháp y nào cũng sẽ nói với bạn rằng việc tránh mã hóa chắc chắn đáng gặp rắc rối.

### 2.2 Điện thoại di động

Ngày nay hầu như mọi người đều có điện thoại di động. Như vậy, chúng thường chứa một số bằng chứng rất có giá trị. Tin nhắn văn bản, e-mail, nhật ký cuộc gọi và danh bạ là những ví dụ về những gì bạn có thể khôi phục. Những vật phẩm này có thể được sử dụng để thể hiện ý định, xác định người cuối cùng tiếp xúc với nạn nhân vụ giết người, thiết lập alibis, xác định vị trí gần đúng và hơn thế nữa.

Cũng như các thiết bị điện tử khác, nhiệm vụ đầu tiên của chúng ta là không thực hiện thay đổi nào đối với thiết bị hoặc phương tiện lưu trữ của nó. Vì vậy, nên tránh tương tác với điện thoại trừ khi thực sự cần thiết. Điện thoại di động đặc biệt dễ bị tổn thương vì chúng có thể bị xóa bởi nhà cung cấp dịch vụ di động hoặc thậm chí bởi chính chủ sở hữu. Chức năng này nhằm bảo vệ dữ liệu của bạn nếu bạn bị mất điện thoại hoặc bị đánh cắp. Ứng dụng “Tìm điện thoại của tôi” của Apple là một ví dụ đáng chú ý. Chúng ta phải giải quyết mối lo ngại này bằng cách cách ly hoặc che chắn điện thoại càng sớm càng tốt.

Bạn có một số tùy chọn để hoàn thành việc này:

Tắt điện thoại. Mối quan tâm với cách tiếp cận này cũng giống như PC. Điện thoại có thể được bảo vệ bằng mật khẩu. Sau khi tắt nguồn, có thể cần mã để truy cập điện thoại. Nếu có thể, tốt nhất là bạn nên cách ly điện thoại trong túi Faraday hoặc hộp đốt và để nó bật nguồn. Sau đó, nó có thể được vận chuyển đến phòng thí nghiệm để điều tra trong một căn phòng được che chắn, v.v.



Đặt điện thoại trong các hộp đựng đặc biệt để che chắn điện thoại khỏi các tín hiệu không dây. Thùng sơn rỗng và túi Faraday là hai trong số những lựa chọn tiêu biểu hơn cả. Cả hai mục này đều có hiệu quả trong việc bảo vệ điện thoại khỏi các tín hiệu di động. (Xem [Hình 4.1](#F0010_4) .)



Hình 4.1 Một túi Faraday và điện thoại di động.

Báo động!

Bảo vệ điện thoại di động khỏi tín hiệu mạng

Điều cần thiết là phải cách ly điện thoại di động đang hoạt động khỏi mạng. Nếu không, nó có thể nhận cuộc gọi, tin nhắn văn bản hoặc thậm chí lệnh xóa tất cả dữ liệu. Túi Faraday là một cách để ngăn tín hiệu mạng đến điện thoại. Túi Faraday được làm bằng “một số loại vật liệu dẫn điện hoặc lưới” có tác dụng đẩy lùi các tín hiệu này. Chức năng của chiếc túi dựa trên công trình nghiên cứu của Michael Faraday, một nhà khoa học người Anh chuyên về điện từ học (Tập đoàn Microsoft).

Báo động!

Quyền lực

Quyền lực là mối quan tâm bất cứ khi nào bạn thu giữ điện thoại di động. Nếu điện thoại đang bật, nó sẽ liên tục cố gắng kết nối với một tháp, làm tiêu hao pin. Nếu điện thoại đang tắt, bạn cũng nên thu giữ cáp nguồn. Nhân viên phòng thí nghiệm rất có thể cần phải sạc lại thiết bị để hoàn thành bài điều tra của họ.

Không loại bỏ kết nối với các thiết bị này không chỉ có nguy cơ phá hủy bằng chứng; nó cũng có thể gây ra những lo ngại nghiêm trọng về tính toàn vẹn của nó. Một luật sư có thẩm quyền có thể lập luận thành công rằng bằng chứng này là không đáng tin cậy và cần được loại trừ.

Sau khi đảm bảo bằng chứng, một cuộc khảo sát hiện trường sẽ cho các nhà điều tra cảm nhận chính xác về những gì phía trước. Một số câu hỏi cần được trả lời:

Có những loại thiết bị nào?



Chúng ta đang xử lý bao nhiêu thiết bị?



Có thiết bị nào đang chạy không?



Những công cụ nào sẽ cần thiết?



Chúng ta có đủ kiến thức chuyên môn cần thiết trong tay không?



Một khi những câu hỏi này được trả lời, công việc thực sự bắt đầu.

### 2.2.1 Thứ tự biến động

Bạn nên ưu tiên các bằng chứng cần thu thập. Nói chung, chúng ta muốn bắt đầu với những bằng chứng dễ bay hơi nhất trước. Theo cách nói của máy tính, đây được gọi là thứ tự biến động . Danh sách giảm dần này hoạt động từ bộ nhớ dễ bay hơi nhất (RAM) đến ít biến động nhất (dữ liệu lưu trữ). Thứ tự biến động là:

1 . CPU, bộ nhớ đệm và đăng ký nội dung

2 . Bảng định tuyến, bộ nhớ cache ARP, bảng quá trình, thống kê hạt nhân

3 . Kỉ niệm

4 . Hệ thống tệp tạm thời / không gian hoán đổi

5 . Dữ liệu trên đĩa cứng

6 . Dữ liệu được ghi từ xa

7 . Dữ liệu có trên phương tiện lưu trữ ( [Henry, 2009](#23__Henry__P___2009__September_1) )

## Ghi lại hiện trường, quá trình

Có một câu nói cổ xưa đã được thử nghiệm và đúng trong thực thi pháp luật: "Nếu bạn không viết nó ra, điều đó đã không xảy ra." Đây thực sự là những lời của sự khôn ngoan. Bất kể tình huống nào, bất kỳ thời điểm nào bằng chứng được thu thập, tài liệu là một phần cực kỳ quan trọng của quy trình. Có một số loại tài liệu khác nhau. Phổ biến nhất về pháp y kỹ thuật số là hình ảnh và ghi chú bằng văn bản; video cũng là một lựa chọn để ghi lại bằng chứng.

Quá trình lập hồ sơ này bắt đầu vào thời điểm các nhà điều tra đến hiện trường. Thông thường, chúng ta bắt đầu bằng cách ghi lại ngày và giờ chúng ta đến cùng với tất cả những người có mặt tại hiện trường. Phần còn lại của ghi chú của chúng ta bao gồm mô tả chi tiết về bằng chứng chúng ta thu thập, vị trí của nó, tên của người đã phát hiện và thu thập nó, cũng như cách thức thu thập nó. Bạn cũng nên lưu ý tình trạng của món đồ, đặc biệt là nếu có hư hỏng có thể nhìn thấy được.

Mô tả chính xác và chính xác các bằng chứng là rất quan trọng. Một phần bằng chứng kỹ thuật số được mô tả theo loại, kiểu dáng, kiểu máy, số sê-ri hoặc các mô tả tương tự khác. Điều quan trọng cần lưu ý là một thiết bị đang bật hay tắt hoặc nếu nó được kết nối với các thiết bị khác (chẳng hạn như máy in) hoặc mạng (như Internet). Hầu như mọi thứ chúng ta thấy, tìm thấy và làm đều phải được ghi lại.

Trong khi chúng ta đang nói về các kết nối ngoại vi, bạn nên dán nhãn cho từng kết nối để toàn bộ hệ thống có thể được tái tạo trong phòng thí nghiệm nếu điều đó trở nên cần thiết.

Sau khi hiện trường và bằng chứng được bảo mật, sự chú ý của chúng ta có thể chuyển sang tài liệu cũng như xác định và thu thập các nguồn bằng chứng tiềm năng. Trước khi hoàn thành mọi việc, bạn nên đi dạo để khảo sát hiện trường, xác định loại và số lượng thiết bị cũng như tài nguyên sẽ cần.

### 4.1 Nhiếp ảnh

Tiếp theo, toàn bộ cảnh nên được chụp ảnh. Nên chụp ảnh hiện trường trước khi có bất cứ điều gì bị xáo trộn, kể cả bằng chứng. Thật hữu ích khi coi những bức ảnh như một câu chuyện kể. Hãy nhớ rằng, tại một số thời điểm, bạn có thể phải dẫn thẩm phán hoặc bồi thẩm đoàn đi qua cảnh này hàng tuần, hàng tháng hoặc thậm chí nhiều năm sau đó.

Bắt đầu với một góc nhìn rộng, có thể là bên ngoài của ngôi nhà hoặc văn phòng đang được điều tra. Sau khi chụp ảnh toàn cảnh, chúng ta có thể tập trung vào từng phần bằng chứng riêng lẻ. Ảnh tầm xa, trung bình và gần hiển thị mặt hàng trong bối cảnh xung quanh nó. Các bức ảnh của mỗi mặt hàng phải hiển thị rõ ràng tình trạng của mặt hàng khi nó được tìm thấy. Chúng ta cần đặc biệt chú ý và nắm bắt những thông tin nhận dạng như số sê-ri, hư hỏng và kết nối. Ví dụ về kết nối có thể bao gồm mạng và thiết bị ngoại vi như máy in và máy quét. Điều rất quan trọng cần lưu ý là đây có thể là cơ hội duy nhất mà chúng ta có được để chụp cảnh. Vì vậy, khi nghi ngờ, hãy bắn nhiều hơn, không ít hơn.

Bạn có thể đã từng xem những bức ảnh có cả vật chứng và thước đo của một loại nào đó. Điều này được thực hiện để cung cấp một số quan điểm cho mặt hàng. Nó cho chúng ta một ý tưởng về kích thước của phần bằng chứng cụ thể đó. Hãy nhớ rằng, chúng ta muốn ghi lại cảnh trước khi nó bị xáo trộn hoặc thay đổi theo bất kỳ cách nào để chèn bất kỳ thứ gì vào cảnh bằng vật phẩm đó (như thước kẻ) có thể đủ điều kiện là thay đổi. Nếu cần thể hiện kích thước của mảnh bằng chứng, bạn nên chụp một bức ảnh không có thước trước, sau đó chụp một tấm bằng thước.

Các bức ảnh được sử dụng để mô tả hiện trường và bằng chứng chính xác như những gì chúng ta tìm thấy để giúp bổ sung các ghi chú của chúng ta. Họ không thay thế chúng. Ghi chú ghi lại những quan sát cá nhân của chúng ta sẽ không được ghi lại trong ảnh. Chúng được sử dụng để làm mới hồi ức của chúng ta khi chúng ta ra tòa. Hình ảnh là một sự hỗ trợ tuyệt vời để giúp chúng ta kể câu chuyện của mình với điều tra viên và bồi thẩm đoàn. Chúng thực sự đáng giá một ngàn lời nói.



Hình 4.2 Các loại cáp được đánh dấu từ mặt sau của PC. Nhãn được đặt trên cả hai đầu của cáp để giúp ghi lại cách những gì được kết nối với PC tại thời điểm nó được thu thập.

### 4.2 Ghi chú

Khi chúng ta chụp ảnh bằng chứng, chúng ta cũng sẽ ghi chú chi tiết các hành động của chúng ta cùng với bất kỳ bằng chứng tiềm năng nào mà chúng ta tìm thấy. Không có tiêu chuẩn thiết lập cho việc ghi chú. Nó thực sự phụ thuộc vào cá nhân về cách họ muốn ghi lại mọi thứ. Trình tự thời gian là một phương pháp phổ biến. Bạn sẽ muốn ghi lại những điều như thời gian bạn đến, ai có mặt tại hiện trường, ai đã thực hiện hành động gì, ai đã tìm thấy và thu thập mảnh bằng chứng nào, v.v.

Đừng bao giờ để ý đến sự thật rằng bạn sẽ dựa vào những bức ảnh, ghi chú và báo cáo này vài tháng hoặc nhiều năm sau khi bạn chuẩn bị ra tòa. Với suy nghĩ đó, bạn sẽ muốn có nhiều chi tiết hơn là ít hơn. Ký ức mờ dần, các trường hợp chạy cùng nhau và các chi tiết bị mờ. Chúng cũng phải rõ ràng vì lý do tương tự. Nếu chi phí là một vấn đề đáng lo ngại, hãy nhớ rằng ảnh kỹ thuật số rất rẻ. Bạn có thể phù hợp với rất nhiều ảnh trên thẻ nhớ hiện nay.

Những gì bạn viết trong những ghi chú đó quan trọng đối với những người khác có liên quan đến vụ án, đặc biệt nếu họ cuối cùng bị chuyển sang tay phe đối lập. Theo các yêu cầu pháp lý nhất định, ghi chú của bạn có thể được phát hiện và cung cấp cho phía đối phương. Điều này có thể xảy ra nếu bạn mang theo ghi chú của mình đến quầy nhân chứng. Với ý nghĩ đó, điều quan trọng là không đưa ra kết luận hoặc suy đoán dựa trên những quan sát ban đầu của bạn. Bạn rất có thể kết thúc bằng việc ăn những lời đó và thua kiện. Tốt nhất hãy giữ cho những ghi chú đó tập trung vào những gì bạn làm và quan sát tại hiện trường. Lưu các diễn giải và kết luận cho đến sau khi phân tích là một cách tiếp cận tốt hơn nhiều.

## Chuỗi hành trình

Trước khi một phần bằng chứng được đưa ra trước bồi thẩm đoàn, trước tiên nó phải đáp ứng một loạt các yêu cầu pháp lý nghiêm ngặt. Một trong số đó là chuỗi hành trình được ghi chép đầy đủ. Một máy tính được lấy làm bằng chứng khiến nhiều người dừng lại trên đường xét xử. Nó được thu thập, đăng nhập tại phòng thí nghiệm, lưu trữ, điều tra để phân tích, đăng nhập lại để lưu trữ, v.v. Mỗi điểm dừng này phải được ghi lại, theo dõi mỗi khi vật chứng thay đổi chủ sở hữu hoặc địa điểm. Nếu không có kế toán chi tiết này, bằng chứng sẽ được coi là không đáng tin cậy và không thể chấp nhận được. Đó là dấu vết chi tiết tạo nên chuỗi hành trình sản phẩm.

### 5.1 Đánh dấu bằng chứng

“Mắt xích” đầu tiên trong chuỗi hành trình trong mọi trường hợp là người thu thập bằng chứng. Các vụ việc dân sự có thể khác một chút ở chỗ nhân viên CNTT hoặc những người khác có thể phân biệt được đâu là mắt xích đầu tiên. Bằng chứng được đánh dấu khi nó được thu thập. Thông thường, các mục bằng chứng được đánh dấu bằng tên viết tắt, ngày tháng và có thể là số trường hợp. Các điểm đánh dấu vĩnh viễn là tốt nhất để đảm bảo các dấu hiệu không bị nhòe hoặc bị xóa hoàn toàn. Ngoài việc ghi lại chuỗi hành trình sản phẩm, những dấu này giúp xác thực mặt hàng nếu nó được đưa ra tòa. Người đã thu thập vật phẩm có thể được yêu cầu xác định nó từ quầy nhân chứng. Điều cần chứng minh là vật phẩm được trình bày là vật phẩm đã được thu thập. Những dấu hiệu này làm cho việc xác định này trở thành một điều gần như chắc chắn. (Xem [Hình 4.3](#F0020_1) .)



Hình 4.3 Một mảnh bằng chứng được đánh dấu, được niêm phong trong túi đựng bằng chứng. (Ảnh do Đại học Marshall cung cấp.)

Các đồ vật đủ nhỏ thường được niêm phong trong túi bằng băng dính bằng chứng chống giả mạo. Con dấu sau đó được ký tắt và ghi ngày tháng. Túi thường được làm bằng giấy, nhựa hoặc vật liệu chống tĩnh điện đặc biệt. Túi vật liệu chống tĩnh điện được sử dụng cho các thiết bị điện tử vì vật liệu này giúp bảo vệ các thiết bị điện tử nhạy cảm được tìm thấy trên ổ cứng khỏi bị hỏng do tĩnh điện.

## Sao y

Bản sao pháp y là một bản sao chính xác, từng chút một của ổ cứng. Nó còn được gọi là hình ảnh dòng bit. Nói cách khác, mỗi bit (1 hoặc 0) được sao chép trên một phần phương tiện riêng biệt, sạch sẽ, chẳng hạn như ổ cứng. Tại sao lại đi đến tất cả những rắc rối đó? Tại sao không chỉ sao chép và dán các tệp? Những lý do là đáng kể. Đầu tiên, việc sao chép và dán chỉ nhận được dữ liệu đang hoạt động. Đó là, dữ liệu mà người dùng có thể truy cập được. Đây là các tệp và thư mục mà người dùng tương tác, chẳng hạn như tài liệu Microsoft Word. Thứ hai, nó KHÔNG lấy dữ liệu trong không gian chưa được phân bổ, bao gồm các tệp bị xóa và ghi đè một phần. Thứ ba, nó không nắm bắt dữ liệu hệ thống tệp. Tất cả những điều này sẽ dẫn đến một cuộc khám nghiệm pháp y không hiệu quả và không đầy đủ.

Chúng ta sẽ muốn tạo bản sao pháp y cho (các) ổ cứng của nghi phạm ngay khi có thể. Sao chép một ổ đĩa có thể là một quá trình khá tốn thời gian và vì lý do đó, việc sao y trong phòng thí nghiệm thường hợp lý hơn so với tại hiện trường. Sao y trong phòng thí nghiệm giúp loại bỏ sự cần thiết phải có mặt tại hiện trường trong thời gian có thể là hàng giờ đồng hồ. Nó cũng cung cấp một môi trường ổn định hơn nhiều, cho phép chúng ta kiểm soát quá trình tốt hơn.

Trước khi đưa máy tính ra khỏi cơ sở, chúng ta phải có thẩm quyền hợp pháp để làm điều đó. Trong trường hợp hình sự, yêu cầu này và lý do đằng sau nó phải là một phần của đơn xin lệnh khám xét. Trong các vụ án dân sự, điều khoản này có thể do các bên thương lượng hoặc do thẩm phán ra lệnh.

Mặc dù việc đưa phần cứng trở lại phòng thí nghiệm là việc làm thường xuyên trong các vụ án hình sự, nhưng việc sao y có thể phải được thực hiện tại hiện trường trong một vụ án dân sự. Hầu hết các vụ án dân sự với bằng chứng kỹ thuật số tập trung vào máy tính doanh nghiệp. Một máy tính kinh doanh ngồi trong phòng thí nghiệm không tạo ra bất kỳ doanh thu nào, điều này có xu hướng khiến những người kinh doanh trở nên cáu kỉnh một cách dễ hiểu. Nếu ổ cứng trong máy tính doanh nghiệp không thể thay thế được, thì máy thường được sao y và đưa vào phục vụ ngay.

### 6.1 Mục đích của sao y

Chúng ta đã biết từ các chương trước rằng bằng chứng kỹ thuật số rất dễ bay hơi. Do đó, bạn không bao giờ muốn tiến hành điều tra bằng chứng ban đầu trừ khi có những tình huống cấp bách hoặc không còn lựa chọn nào khác. Các hoàn cảnh cấp bách có thể bao gồm các tình huống mà một đứa trẻ bị mất tích. Đôi khi không có công cụ hoặc kỹ thuật nào có sẵn để giải quyết vấn đề trong tầm tay.

Việc điều tra bản sao cho chúng ta cơ hội tìm thấy một "kẻ xấu" nếu có vấn đề gì xảy ra. Nếu có thể, ổ đĩa gốc nên được bảo quản ở một nơi an toàn và chỉ được mang ra ngoài để hình dung lại nếu cần.

Ổ cứng dễ bị hỏng. Có hai bản sao cho bạn một bản để điều tra và một bản để quay lại. Lý tưởng nhất là tất cả các bài điều tra được thực hiện trên một bản sao trái ngược với bản gốc.

Đôi khi, đó không phải là một tùy chọn, đặc biệt là trong môi trường kinh doanh khi máy và ổ đĩa phải được đưa trở lại hoạt động. Dưới con mắt của tòa án, một bản sao pháp y được xác thực đúng đắn sẽ tốt như bản gốc.

### 6.2 Quá trình sao y

Sao chép ổ cứng phải là một quá trình khá đơn giản, ít nhất là trên lý thuyết. Thông thường, bạn sẽ sao chép ổ cứng này sang ổ cứng khác. Ổ của nghi phạm được gọi là ổ nguồn và ổ mà bạn đang sao y được gọi là ổ đích. Ổ đĩa đích ít nhất phải lớn (nếu không lớn hơn một chút) so với ổ đĩa nguồn của chúng ta. Mặc dù không phải lúc nào cũng có thể thực hiện được, nhưng việc biết trước kích thước của nguồn là khá hữu ích. Mang đúng kích thước ổ sẽ tiết kiệm được nhiều thời gian và nặng hơn.

Ổ đĩa chúng ta muốn sao chép (nguồn) thường được lấy ra khỏi máy tính. Sau đó, nó được kết nối qua cáp với một thiết bị sao y nào đó hoặc với một máy tính khác. Điều quan trọng là phải có một số loại chặn ghi trước khi bắt đầu quá trình. Khối ghi là một phần cứng hoặc phần mềm quan trọng được sử dụng để bảo vệ bằng chứng gốc trong quá trình sao y. Khối ghi phần cứng được đặt giữa thiết bị sao chép (PC, máy tính xách tay hoặc phần cứng độc lập) và nguồn. Khối ghi ngăn không cho bất kỳ dữ liệu nào được ghi vào ổ đĩa bằng chứng ban đầu. Sử dụng loại thiết bị này giúp loại bỏ khả năng vô tình làm tổn hại đến bằng chứng. Hãy nhớ rằng, thiết bị chặn ghi phần cứng nằm giữa ổ nguồn và nền tảng sao chép.

Có một công việc chuẩn bị nhỏ liên quan đến việc tạo ra một bản sao. Ổ đĩa đích phải được làm sạch trước khi sao chép ổ đĩa của kẻ tình nghi vào nó. Hầu hết nếu không phải tất cả các công cụ hình ảnh pháp y sẽ tạo ra một số loại vệt giấy, chứng tỏ rằng quá trình làm sạch đã diễn ra. Giấy tờ này trở thành một phần của hồ sơ vụ án.

Sau khi các kết nối được thực hiện, quá trình được bắt đầu bằng cách nhấn một vài nút hoặc nhấp chuột. Khi hoàn tất, một báo cáo ngắn sẽ được tạo bởi công cụ cho biết liệu quá trình sao y có thành công hay không. Sao chép thành công khi các giá trị băm (nghĩ là "dấu vân tay kỹ thuật số") cho nguồn và bản sao khớp nhau. Chúng ta sẽ tìm hiểu sâu hơn về các giá trị băm chỉ sau một chút.

### 6.3 Phương tiện sạch về mặt pháp lý

Một ổ đĩa sạch về mặt thực tế là một ổ đĩa có thể được chứng minh là không có bất kỳ dữ liệu nào tại thời điểm tạo bản sao. Vô trùng là một cách nhìn khác về nó. Điều quan trọng là phải chứng minh ổ đĩa sạch vì dữ liệu đi kèm là dữ liệu không được phép. Các ổ đĩa có thể được làm sạch bằng các thiết bị tương tự được sử dụng để tạo bản sao. Quá trình dọn dẹp ghi đè lên toàn bộ ổ cứng bằng một mẫu dữ liệu cụ thể như 1111111111111 ( [Casey, 2011](#15__Casey_E__Digital_Evidence_an) ).

### 6.4 Định dạng hình ảnh pháp y

Kết quả cuối cùng của quá trình sao y là một hình ảnh pháp y của ổ cứng nguồn. Bản sao đã hoàn thành của chúng ta có thể có một số định dạng khác nhau. Phần mở rộng tệp là chỉ báo dễ thấy nhất về định dạng tệp. Một số định dạng hình ảnh pháp y phổ biến nhất bao gồm:

EnCase (Phần mở rộng .E01)



Dd thô (Phần mở rộng .001)



Hình ảnh nội dung tùy chỉnh AccessData (Phần mở rộng .AD1)



Có sự khác biệt trong các định dạng, nhưng về mặt bản chất, chúng đều rất hợp lý. Một số, như DD, là mã nguồn mở, trong khi một số khác, như AD1, là độc quyền. Việc chọn một định dạng này so với định dạng khác có thể chỉ đơn giản là một vấn đề ưu tiên. Hầu hết các công cụ giám định pháp y sẽ đọc và ghi nhiều định dạng hình ảnh.

Ngoài âm thanh rõ ràng, điều quan trọng khác là các công cụ được sử dụng có thể đọc được hình ảnh. Tài liệu kèm theo công cụ phải cung cấp thông tin này. Khả năng tương thích là một mối quan tâm. Điều này đặc biệt đúng khi trao đổi tệp hình ảnh giữa các điều tra viên.

### 6.5 Rủi ro và thách thức

Rủi ro lớn nhất trong quá trình sao y là bằng văn bản tới nguồn hoặc ổ đĩa bằng chứng. Bất kỳ văn bản nào đối với bằng chứng sẽ làm tổn hại đến tính toàn vẹn của nó và gây nguy hiểm cho khả năng chấp nhận của nó. Chuẩn bị sẵn một thiết bị hoặc phần mềm chặn ghi đang hoạt động sẽ giúp điều này không xảy ra. Sao y đúng cách sẽ khá nhàm chán. Bất cứ lúc nào nó trở nên thú vị, bạn sẽ gặp vấn đề. Điều gì có thể làm tăng adrenaline? Các thành phần xấu và ổ đĩa bị hỏng hoặc trục trặc là điều cần lưu ý. Khu vực khởi động bị hỏng hoặc động cơ bị lỗi cũng có thể tạo ra các biến chứng.

### 6.6 Giá trị trong eDiscovery

Hội nghị Sedona, tổ chức tư vấn hàng đầu về khám phá điện tử, định nghĩa Khám phá điện tử là: “Quá trình xác định, bảo quản, thu thập, chuẩn bị, xem xét và sản xuất thông tin được lưu trữ điện tử (“ ESI ”) trong bối cảnh của quy trình pháp lý” ( [Sedona Hội nghị, 2010](#40__Sedona_Conference___2010__Se) ).

Sao y pháp y cung cấp một số giá trị bổ sung trong quy trình Khám phá điện tử. Bảo quản dữ liệu có liên quan tiềm năng là điều tối quan trọng trong khám phá điện tử. Các bên không bảo quản bằng chứng có thể phải đối mặt với một số hình phạt rất nghiêm khắc. Sao y pháp y là một tùy chọn có sẵn để bảo quản một số loại phương tiện như ổ cứng và phương tiện di động như ổ đĩa flash. Nó đóng vai trò là “tiêu chuẩn vàng” của việc bảo quản dữ liệu trong đó nó lưu giữ tất cả dữ liệu trên một phần phương tiện, không chỉ dữ liệu đang hoạt động. Mặt trái của việc sao y là nó có thể tốn kém và không thực tế trong mọi tình huống.

Báo động!

Các biện pháp trừng phạt trong Khám phá Điện tử

Lấy trường hợp của EI du Pont de Nemours kiện Kolon Industries (2011) . Trong trường hợp này, bồi thẩm đoàn đã trao 919 triệu đô la cho DuPont trong một phán quyết hấp dẫn. Trước đó trong vụ án, tòa án xác định rằng Kolon đã phá hủy các thư điện tử và các dữ liệu có khả năng liên quan khác kết nối nó với hành vi trộm cắp bí mật thương mại. Kết quả của việc xác định đó, thẩm phán đã hướng dẫn bồi thẩm đoàn rằng Kolon (cả giám đốc điều hành và nhân viên) đã xóa bằng chứng quan trọng mặc dù họ có nhiệm vụ bảo quản nó. Sự đau khổ của Kolon có thể không kết thúc ở đó. DuPont có kế hoạch yêu cầu 50 triệu đô la tiền bồi thường thiệt hại cộng với 30 triệu đô la nữa cho phí luật sư (Favro, 2011).

## Hệ thống sống và hệ thống chết

Cho đến nay, chúng ta đã nói về máy "chết" hoặc tắt nguồn. Điều gì xảy ra khi chúng ta bắt gặp một máy tính đang chạy? Hiện tại vẫn chưa có sự thống nhất về câu trả lời. Một cuộc tranh luận ngày càng tăng trong cộng đồng pháp y kỹ thuật số về cách xử lý một máy "sống" hoặc đang chạy. Giải pháp "truyền thống" chỉ đơn giản là kéo phích cắm, ngay lập tức loại bỏ nguồn điện cho máy tính. Ngày nay, cách tiếp cận đó đang thu hút những suy nghĩ thứ hai. Có những lý do thuyết phục để không sử dụng nguồn trên máy tính đang chạy. Tiếp theo, chúng ta sẽ xem xét lý do của cả hai và chống lại phương pháp gây tranh cãi này.

### 7.1 Mối quan tâm về chuyển đổi trực tiếp

Mặt tích cực, việc kéo phích cắm giúp loại bỏ nhu cầu tương tác với máy đang chạy. Tương tác với một máy tính đang chạy, theo bất kỳ cách nào, đều gây ra các thay đổi đối với hệ thống. Bất kỳ thay đổi nào đối với một phần bằng chứng đều không tốt và có thể gây ra các vấn đề lớn từ quan điểm pháp lý. Những thay đổi này có thể khiến tính toàn vẹn của bằng chứng bị nghi ngờ. Ngay cả khi máy chỉ được bật nguồn, mọi thứ vẫn đang thay đổi. Khi một người tương tác với một máy đang chạy, thậm chí nhiều thứ đang thay đổi. Biết rằng thay đổi đó là giả mạo pháp y; thật dễ dàng để hiểu tại sao kéo phích cắm là một lựa chọn hấp dẫn. Lưu ý nhỏ, những thay đổi này có thể không ảnh hưởng đến các hiện vật liên quan đến vụ án. Nhưng dù sao thì hệ thống cũng đang thay đổi.

Bây giờ chúng ta đang bắt đầu phỏng đoán thứ hai về cách tiếp cận này, nhận ra rằng việc kéo phích cắm có một số nhược điểm đáng kể.

Đối với người mới bắt đầu, việc kéo mạnh phích cắm có nghĩa là bất kỳ bằng chứng nào trong RAM sẽ bị đe dọa phá hủy thực sự. Dữ liệu trong RAM bắt đầu tiêu tan hoặc mờ dần khi nguồn điện bị ngắt. Có một kỹ thuật có thể được sử dụng để lưu giữ dữ liệu trong bộ nhớ sau khi tắt nguồn, nhưng nó vẫn chưa được áp dụng rộng rãi. (Xem thanh bên.)

Nâng cao hơn

Lưu trữ bằng chứng trong RAM

Nhiều người cho rằng dữ liệu trong RAM sẽ biến mất khi tắt nguồn. Điều đó thực sự không đúng. Nghiên cứu của Đại học Princeton đã chỉ ra rằng dữ liệu trong RAM mờ dần thay vì biến mất. Quá trình tản nhiệt này có thể bị làm chậm hơn nữa nếu RAM được làm mát đến –58 độ F (–50 độ C). Việc làm mát này sẽ giúp điều tra viên có thêm thời gian để thu thập dữ liệu dễ bay hơi này. Để xem kỹ thuật này hoạt động, hãy xem video tại đây: <http://www.youtube.com/watch?v=JDaicPIgn9U>.

Thứ hai, là mã hóa. Hệ thống hoặc các tệp có thể không được mã hóa khi máy được bật nguồn. Việc kéo phích cắm đột ngột có thể đưa phích cắm trở về trạng thái được mã hóa, có khả năng khiến bằng chứng đó ngoài tầm với. Tránh mã hóa là một ý kiến hay.

Thứ ba, việc mất điện đột ngột có thể làm hỏng dữ liệu, khiến chúng không thể đọc được. Thứ tư, một số bằng chứng có thể không được ghi lại trên ổ đĩa trừ khi và cho đến khi máy tính được tắt đúng cách.

Giải pháp cũ của trường học là kéo phích cắm không phải là lựa chọn duy nhất trên bàn những ngày này. Hiện nay có các công cụ và kỹ thuật sẽ ghi lại bộ nhớ dễ bay hơi từ một máy trực tiếp theo một cách thức rõ ràng hoặc sao y ra ảnh chụp thiết bị. Với những tiến bộ này, đã đến lúc bắt đầu nhận ra những lợi thế của thu thập trực tiếp.

### 7.2 Lợi thế của Bộ sưu tập Trực tiếp

Cho đến gần đây, kéo phích cắm là lựa chọn thực sự duy nhất. Ghi lại dữ liệu trong bộ nhớ chính (RAM) của máy tính đang chạy không phải là một lựa chọn thực tế. Các giải pháp tiềm năng đã tồn tại không thực tế để sử dụng trên thực địa. Ngược lại, các điều tra viên ngày nay thực sự có một số lựa chọn thay thế hợp lý. Có một số công cụ thương mại và mã nguồn mở có thể được sử dụng để thu thập những dữ liệu dễ bay hơi này. Không giống như các phương pháp tiếp cận phòng thí nghiệm cũ hơn, những công cụ này rất đơn giản để sử dụng — trên thực tế, đơn giản đến mức chúng đang được tiếp thị cho những người không có kỹ thuật như hầu hết những người phản hồi đầu tiên. Những người phản ứng đầu tiên có thể bao gồm các sĩ quan tuần tra và nhân viên CNTT trong số những người khác. Mặc dù các công cụ này đơn giản hóa quy trình, nhưng chúng vẫn yêu cầu đào tạo để sử dụng đúng cách.

### 7.3 Nguyên tắc thu thập trực tiếp

Thực hiện một bộ sưu tập trực tiếp không phải là một nhiệm vụ thô sơ. Sau đây là một ví dụ về một cách tiếp cận.

Sau khi bắt gặp một máy tính đang chạy tại hiện trường, một số câu hỏi sẽ cần được trả lời ngay từ đầu. Bằng chứng tiềm năng cần được thu hồi có thực sự xứng đáng với thời gian và công sức không? Trong một số trường hợp, câu trả lời có thể là “không”. Trong các trường hợp liên quan đến phần mềm độc hại, RAM là cực kỳ quan trọng. Trong những trường hợp khác, chẳng hạn như sở hữu rõ ràng nội dung “đen”, RAM có thể sẽ có rất ít giá trị. Thứ hai, các nguồn lực cần thiết có sẵn không? Để nắm bắt thành công bằng chứng trong bộ nhớ sẽ cần một số công cụ và đào tạo chuyên biệt. Nếu không có những thành phần quan trọng này, tốt nhất là bạn nên bắt đầu và chỉ cần kéo phích cắm. Rủi ro làm ảnh hưởng đến bằng chứng có thể đơn giản là quá lớn. Điều quan trọng là có thể nhận ra khi nào bạn đang ở trong đầu và khi nào bạn nên kêu cứu.

Khi tương tác với một máy trực tiếp, tốt nhất bạn nên luôn chọn cách tiếp cận ít xâm lấn nhất có thể. Điều này sẽ yêu cầu suy nghĩ trước khi bạn nhấp vào. Sự vội vàng không phải là người bạn của bạn trong tình huống này. Như đã đề cập trước đó, chúng ta muốn thu thập những thông tin bất ổn nhất trước tiên.

Báo động!

Bằng chứng trong RAM

Bộ nhớ dễ bay hơi (RAM) của máy tính có thể chứa một số bằng chứng rất có giá trị, bao gồm các quy trình đang chạy, lệnh bảng điều khiển được thực thi, mật khẩu ở dạng văn bản rõ ràng, dữ liệu không được mã hóa, tin nhắn tức thì, địa chỉ Giao thức Internet và (các) con ngựa thành Troy ( [Shipley & Reeve, 2006](#43__Shipley_TG__Reeve_HR__Collec) ) .

### 7.4 Tiến hành và ghi lại một bộ sưu tập trực tiếp

Bây giờ đến phần khó khăn. Đã đến lúc phải tập trung. Khi bạn bắt đầu, bạn nên làm việc không bị gián đoạn cho đến khi quá trình hoàn tất. Làm khác đi chỉ mời những sai lầm. Trước khi bắt đầu, hãy thu thập mọi thứ bạn cần: biểu mẫu báo cáo, bút, công cụ ghi lại bộ nhớ, v.v. Mọi tương tác với máy tính sẽ cần được lưu ý. Bạn có thể sử dụng cách tiếp cận hành động / phản hồi (“Tôi đã làm điều này… Máy tính đã làm điều đó.”).

Nếu màn hình không hiển thị, bạn có thể di chuyển chuột một chút để đánh thức màn hình. Nếu điều đó không hiển thị màn hình, nhấn một phím duy nhất sẽ giải quyết được vấn đề. Tất nhiên, bạn nên ghi lại khóa nào đã bị bỏ quên trong ghi chú của mình. Bây giờ bạn có thể nhìn thấy màn hình nền, điều đầu tiên cần lưu ý là ngày và giờ khi nó xuất hiện trên máy tính. Tiếp theo, ghi lại các biểu tượng và ứng dụng đang chạy. Bạn không muốn dừng lại ở đó. Ghi lại các quy trình đang chạy có thể giúp xác định bất kỳ phần mềm độc hại nào đang cư trú trên máy tính. Các quy trình đang chạy có thể được ghi lại bằng cách truy cập trình quản lý tác vụ. Tại sao điều đó lại quan trọng? Một trong những biện pháp bảo vệ phổ biến hơn, đặc biệt là trong các trường hợp “đen”, là tuyên bố rằng các hình ảnh lậu đã được gửi bởi một bên thứ ba không xác định bằng con đường Trojan.

Bây giờ đã đến lúc sử dụng một công cụ thu thập bộ nhớ đã được xác thực để thu thập bằng chứng bất ổn đó trong RAM. Sau khi bước này hoàn tất, quá trình kết thúc với việc tắt máy đúng cách. Việc tắt máy thích hợp cho phép bất kỳ ứng dụng nào đang chạy có cơ hội ghi bất kỳ hiện vật nào vào đĩa, cho phép chúng ta khôi phục chúng sau này.

## Băm

Làm sao chúng ta biết bản sao của mình là bản sao chính xác của ổ đĩa bằng chứng? Câu trả lời có dạng giá trị băm. Hàm băm là một giá trị duy nhất được tạo bởi thuật toán băm mật mã . Giá trị băm (hàm) được sử dụng theo nhiều cách khác nhau bao gồm cả mật mã và tính toàn vẹn của bằng chứng. Giá trị băm thường được gọi là “dấu vân tay kỹ thuật số” hoặc “DNA kỹ thuật số”. Bất kỳ thay đổi nào đối với ổ cứng, dù chỉ một bit, sẽ dẫn đến một giá trị băm hoàn toàn khác. Do đó, mọi sự giả mạo hoặc thao túng bằng chứng đều có thể dễ dàng phát hiện được.

### 8.1 Các loại thuật toán băm

Có nhiều loại thuật toán băm. Thuật toán kỳ hạn có thể gây ra nỗi sợ hãi trong trái tim của những người bị thách thức về mặt toán học. Đừng bao giờ sợ hãi. Chúng ta sẽ không tham gia vào bất kỳ môn toán cấp cao nào ở đây, nhưng chúng ta sẽ cảm thấy thoải mái với một số khái niệm và thuật ngữ cơ bản. Các hàm băm phổ biến nhất được sử dụng trong pháp y kỹ thuật số là Thông báo số 5 (MD5) và Thuật toán băm an toàn (SHA) 1 và 2.

### 8.2 Ví dụ về băm

Hãy băm một cụm từ ngắn gọn để chứng minh điều gì xảy ra chỉ với một thay đổi nhỏ. Xin gửi lời xin lỗi trước mọi người hâm mộ Baltimore hoặc Cleveland. Đối với bài tập này, chúng ta sẽ sử dụng SHA1.

Cụm từ - Go Steelers!

SHA1 - c924 4cac 47b3 4335 5aed 06f3 cc85 ea82 885f 9f3e

Bây giờ chúng ta hãy thực hiện một thay đổi nhỏ, thay đổi chữ “S” từ chữ hoa thành chữ thường. Khi chúng ta rehash, chúng ta nhận được điều này:

Cụm từ - Đi luyện thép!

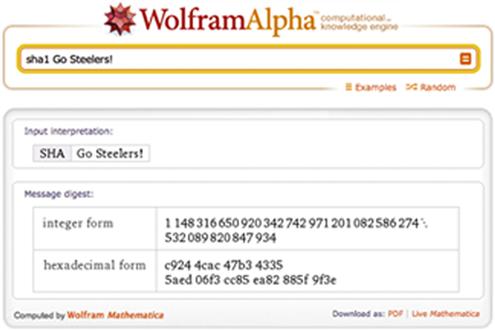
SHA 1 - 1a10 ffd1 db12 c88f 88e6 b070 561f 6124 f632 26ec

Lưu ý sự thay đổi mạnh mẽ trong các giá trị băm kết quả. Ở đây chúng được xếp chồng lên nhau để dễ so sánh hơn:

c924 4cac 47b3 4335 5aed 06f3 cc85 ea82 885f 9f3e

1a10 ffd1 db12 c88f 88e6 b070 561f 6124 f632 26ec

Như bạn có thể thấy, những thay đổi nhỏ tạo ra sự khác biệt lớn. Nếu bạn muốn tự mình thử điều này, rất dễ thực hiện. Truy cập <http://www.wolframalpha.com>và nhập hàm băm bạn muốn sử dụng (MD5, SHA1, v.v.), theo sau là dấu cách và sau đó là cụm từ Go Steelers! (Xem [Hình 4.4](#F0025_1) .)



Hình 4.4 Kết quả WolframAlpha.

### 8.3 Sử dụng băm

Giá trị băm có thể được sử dụng trong suốt quá trình pháp y kỹ thuật số. Chúng có thể được sử dụng sau quá trình sao y để xác minh rằng bản sao thực sự là một bản sao chính xác. Chúng cũng có thể được sử dụng như một điều tra tính toàn vẹn tại bất kỳ thời điểm nào cần thiết. Người giám định thường phải trao đổi hình ảnh pháp y với người giám định ở phía đối diện. Giá trị băm được gửi cùng với hình ảnh để có thể so sánh với giá trị ban đầu. So sánh này xác minh rằng hình ảnh là một chút bản sao của bản gốc.

Các giá trị băm có liên quan đã được tạo và ghi lại trong toàn bộ trường hợp cần được lưu giữ và đưa vào báo cáo cuối cùng. Những dấu vân tay kỹ thuật số này rất quan trọng để chứng minh tính toàn vẹn của bằng chứng và cuối cùng là đưa chúng ra trước bồi thẩm đoàn.

## Bản báo cáo cuối

Khi kết thúc phân tích, giám định viên sẽ tạo ra một báo cáo cuối cùng nêu chi tiết những gì đã được thực hiện, những gì đã được tìm thấy và những phát hiện của họ. Lý tưởng nhất là các báo cáo cuối cùng cần được soạn thảo với đối tượng mong muốn. Trên thực tế, có quá nhiều báo cáo cuối cùng được đọc giống như hướng dẫn sử dụng của chủ sở hữu cho tàu con thoi. Những báo cáo này không chỉ khó đọc mà còn có thể cực kỳ đáng sợ.

Bởi vì chúng thường chứa đầy biệt ngữ và mã, những báo cáo này không hữu ích lắm đối với những người đọc không am hiểu kỹ thuật như thẩm phán, luật sư và bồi thẩm đoàn. Điều quan trọng cần nhớ là những người này phải có khả năng hiểu được thông tin có trong báo cáo của bạn. Ngay cả những bằng chứng tốt nhất, thuyết phục nhất cũng có thể bị bỏ qua nếu bồi thẩm đoàn không thể hiểu được.

Các công cụ pháp y chính, chẳng hạn như EnCase và FTK, có các tính năng báo cáo rất mạnh mẽ, tạo ra khá nhiều thông tin có thể tùy chỉnh. Tuy nhiên, các báo cáo này hữu ích như vậy, chúng chỉ là không đủ để tự đứng vững. Chúng khó hiểu đối với hầu hết người đọc không am hiểu kỹ thuật. Thông tin này nên được đưa vào báo cáo cuối cùng, nhưng chúng không được coi là phần tài liệu duy nhất cho toàn bộ cuộc điều tra.

Các báo cáo tốt nhất sẽ bao gồm nhiều thứ hơn so với báo cáo tiêu chuẩn được tạo bằng công cụ đơn thuần. Báo cáo cuối cùng phải bao gồm tường thuật chi tiết về tất cả các hành động được thực hiện bởi người giám định, bắt đầu tại hiện trường nếu họ có mặt. Việc điều tra phải được lập thành văn bản với đầy đủ chi tiết để quy trình này có thể được sao y bởi một điều tra viên khác.

Một báo cáo pháp y kỹ thuật số được viết bằng tiếng Anh đơn giản được đánh giá cao và hiệu quả hơn nhiều (tôi có thể nhận được "Amen" từ các luật sư ở đó không?).

## Bản tóm tắt

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 sao y giúp loại bỏ nhu cầu điều 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”. Chúng ta đã thảo luận về sự khác biệt giữa mua lại còn sống và đã chết cũng như lợi ích và thách thức của từng loại. 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.

## Tổng kết và kiến thức thêm chương 4

1. **Hiểu vai trò của thu thập thông tin từ phần cứng**

Thu thập thông tin là phương pháp để thu thập những thông tin số (ESI) từ vật chứng như thiết bị điện tử, thiết bị lưu trữ để có thể nhìn rõ hơn vào hiện trường, sự cố.

1. **Hiểu vai trò của thu thập dữ liệu sống từ phần cứng**

Thu thập dữ liệu sống là thu thập những thông tin có khả năng bị thay đổi nhanh chóng theo thời gian như RAM, Cache, hoặc các cấu hình. Khi thu thập dữ liệu sống, ta cần đảm bảo thu thập từ những thông tin có khả năng bị thay đổi nhanh chóng nhất rồi mới thu thập các thông tin khác.

1. **Hiểu vai trò của thu thập thông số phần cứng**

Thu thập các thông số phần cứng được định nghĩa là thu thập thông tin từ ổ đĩa, USB, DVD, là những thiết bị mà có khả năng lưu trữ thông tin kể cả khi thay đổi trạng thái.

1. **Nhớ được quy trình thu thập, điều tra và sao y dữ liệu**
2. Dán nhãn Chain of Custody
3. Sử dụng cộng cụ bảo vệ các vật chứng
4. Đảm bảo an toàn cho các thiết bị lưu trữ thông tin
5. Xác định các dạng dữ liệu sẽ được kiếm thấy
6. Xác định phương pháp thu thập tốt nhất
7. Xác định công cụ để thu thập dữ liệu
8. Thu thập và bảo quản dữ liệu
9. Lập kế hoạch cho các trường hợp (phân tích dữ liệu hoặc cần thu thập thêm bằng chứng)
10. Điều tra lại quá trình thu thập thông tin
11. **Hiểu được phương pháp xử lý để không ảnh hưởng thiết bị**

Trong quá trình thu thập thông tin, điều tra viên cần:

1. Sử dụng sai phương pháp, công cụ để thu thập thông tin
2. Sử dụng các đường truyền, dây cáp không an toàn hoặc không phù hợp
3. Điều tra khi không đủ thông tin
4. Kết nối nhằm với các thiết bị, hệ thống, mạng.
5. **Hiểu được các phương pháp thu thập thông tin và chọn đúng công cụ thu thập**

Phương pháp thu thập thông tin:

1. UltraKit (công cụ bảo vệ vật lý) – đây là bộ công cụ để bảo vệ cho vật lý của các vật chứng
2. Forensic Falcon (công cụ thu thập thông tin tại chỗ)– đây là thiết bị có khả năng sao y, xác mình, xem xet, điều tra và cho phép điều tra viên sao y lại thông tin hệ thống cũng như kết nối từ xa
3. EnCase Forensic (công cụ thu thập, điều tra, phân tích thông tin)– Phần mềm này có thể thu thập dữ liệu từ nhiều nguồn khác nhau, hỗ trợ chỉ định các thông số có giá trị sau khi phân tích ổ đĩa, hỗ trợ trong việc xuất báo cáo về các thông tin thu thập được, đảm bảo được tính an toàn của công cụ thu thập do được tin tưởng bởi các chuyên gia, tổ chức điều tra số.

Khi chọn công cụ, cần phải đảm bảo:

1. Công cụ này không thay đổi thông tin dữ liệu
2. Công cụ này có thể hiển thị rõ ràng trạng thái, câu lệnh, lỗi trong quá trình sử dụng
3. Công cụ này phải báo cáo cho người dùng về dung lượng giữa các ổ đĩa

Các kết quả từ công cụ này phải chính xác, được ghi lại và có thể xem lại

1. **Công cụ sao y, thu thập thông tin trên vật chứng**

Linux: Linux có lệnh dd và dcfldd để sao y thông tin từ ổ đĩa.

Windows: AccessData FTK Imager (Thuộc Sleath Tool Kit)

RAID: X-Ways Forensics

Remote Data Acquisition: F-Response

1. **Đảm bảo quá trình thu thập thông tin tốt nhất**
2. Tắt mọi kết nối tới vật chứng ngoài những thiết bị được gắn nhãn
3. Chụp lại mọi thông tin
4. Bảo toàn vật chứng ở nơi an toàn
5. Đảm bảo an toàn vật lý cho các vật chứng
6. Đảm bảo các vật chứng tránh xa khỏi các thiết bị có khả năng phát sóng hoặc nam châm
7. Đảm bảo mọi người trong hiện trường phải được định danh và cho phép
8. Đảm bảo không bao giờ điều tra trực tiếp trên vật chứng

Tài liệu tham khảo

1. Giới thiệu: Hiệp hội Giám đốc Phòng thí nghiệm điều tra tội phạm Hoa Kỳ / Ban Công nhận Phòng thí nghiệm . (nd). Truy cập ngày 4 tháng 6 năm 2011, từ: <http://www.ascld-lab.org/about_us/aboutoverview.html>.

2. Nhóm AccessData, LLC. (2011, tháng 2). Tải xuống: AccessData . Được truy cập ngày 24 tháng 8 năm 2011, từ: [http://accessdata.com/downloads/media/FTK\_3x\_System\_Specilities\_Guide.pdf](http://accessdata.com/downloads/media/FTK_3x_System_Specifications_Guide.pdf) .

3. Hội đồng Giám đốc Phòng thí nghiệm Phòng thí nghiệm điều tra tội phạm Hoa Kỳ. (nd). ASCLD / LAB Các Nguyên tắc Hướng dẫn về Trách nhiệm Nghề nghiệp cho Phòng thí nghiệm Crome và Các nhà khoa học Pháp y . Truy cập ngày 3 tháng 9 năm 2011, từ: <http://www.ascld-lab.org/about_us/guidingprinciples.html>.

4. Hội đồng Giám đốc Phòng thí nghiệm điều tra tội phạm Hoa Kỳ / Ban Công nhận Phòng thí nghiệm. (nd). Bạn có biết: Hiệp hội Giám đốc Phòng thí nghiệm điều tra tội phạm Hoa Kỳ / Ban Công nhận Phòng thí nghiệm . Truy cập ngày 4 tháng 6 năm 2011, từ: <http://www.ascld-lab.org/largest_accreditation.html>.

5. Hội đồng Giám đốc Phòng thí nghiệm điều tra tội phạm Hoa Kỳ / Ban Công nhận Phòng thí nghiệm. (nd). Mục tiêu: Hiệp hội Giám đốc Phòng thí nghiệm điều tra tội phạm Hoa Kỳ / Ban Công nhận Phòng thí nghiệm . Truy cập ngày 4 tháng 6 năm 2011, từ: <http://www.ascld-lab.org/about_us/objectives.html>.

6. Hiệp hội các sĩ quan cảnh sát trưởng. Hướng dẫn Thực hành Tốt về Bằng chứng Điện tử Dựa trên Máy tính Cambridge, MA: 7Safe; 2011.

7. ASTM quốc tế. (nd). Tổng quan về ASTM . Truy cập ngày 1 tháng 10 năm 2011, từ: <http://www.astm.org/ABOUT/overview.html>.

8. Barbara, JJ (nd). Chứng nhận bằng chứng kỹ thuật số . Được truy cập ngày 25 tháng 8 năm 2011, từ: <http://www.forensicmag.com/article/digital-evidence-accreditation?page=0,3>.

9. Barbara, JJ (nd). Công nhận bằng chứng kỹ thuật số: Tạp chí pháp y . Truy cập ngày 4 tháng 6 năm 2011, từ: <http://www.forensicmag.com/article/digital-evidence-accreditation>.

10. Barbara, JJ (nd). Thử nghiệm một máy tính . Được truy cập ngày 14 tháng 6 năm 2011, từ: <http://www.forensicmag.com/article/triage-computer>.

11. Brunty, J. (2011, ngày 2 tháng 3). Xác thực các công cụ và phần mềm pháp y: Hướng dẫn nhanh cho Giám định viên pháp y kỹ thuật số . Được truy cập ngày 24 tháng 8 năm 2011, từ: <http://www.dfinews.com/article/validation-forensic-tools-and-software-quick-guide-digital-forensic-examiner?page=0,2>.

12. Người vận chuyển, BB (2002, tháng 10). Bài báo: Digital-evidence.org . Truy cập ngày 24 tháng 8 năm 2011, từ: <http://www.digital-evidence.org/papers/opensrc_legal.pdf>.

13. Carvey H. Bộ công cụ DVD Phân tích Pháp y Windows phiên bản thứ 2. Burlington, MA: Syngress; Năm 2009.

14. Casey E. Sổ tay Điều tra và Pháp y Kỹ thuật số Burlington, MA: Academic Press; Năm 2009.

15. Casey E. Bằng chứng Kỹ thuật số và Tội phạm Máy tính, xuất bản lần thứ 3: Khoa học Pháp y, Máy tính và Internet Waltham, MA: Academic Press; 2011.

16. Cellebrite Mobile Synchronization LTD. (nd). UFED Physical Pro . Được truy cập ngày 2 tháng 10 năm 2011, từ: <http://www.cellebrite.com/forensic-products/forensic-products/ufed-physical-pro.html>.

17. Chan, S. (1994, ngày 21 tháng 8). Điểm số của Niềm tin Được đánh giá là Nhà hóa học Đối mặt với Những cáo buộc về Tổn thương: Pháp y . Truy cập ngày 27 tháng 9 năm 2011, từ: <http://articles.latimes.com/1994-08-21/news/mn-29449_1_lab-tests-fred-zain-double-murder>.

18. Craiger, PJ (nd). Phòng thí nghiệm bằng chứng kỹ thuật số ảo . Truy cập ngày 16 tháng 9 năm 2011, từ: <http://www.ncfs.org/VDEL.Craiger.Report.NIJ.final.pdf>.

19. Sáng kiến DNA, The. (nd). Glen Woodall (Huntington, Tây Virginia) . Truy cập ngày 27 tháng 9 năm 2011, từ: <http://www.dna.gov/postconviction/convicted_exonerated/woodall>.

20. Hội đồng EC. Pháp y Máy tính: Quy trình Điều tra và Ứng phó Clifton Park, NY: Cengage Learning; Năm 2009.

21. Favro, P. (2011, ngày 15 tháng 9) Tin tức mới nhất: Bản án trị giá 919 triệu đô la cho DuPont trong Vụ án trộm cắp bí mật thương mại và trừng phạt eDiscovery . Blog E-Discovery: <http://www.clearwellsystems.com/e-discovery-blog/>.

22. Cục Điều tra Liên bang. Phòng thí nghiệm Pháp y Máy tính Khu vực Báo cáo Thường niên Năm Tài chính 2010 Washington, DC: Bộ Tư pháp Hoa Kỳ; Năm 2010.

23. Henry, P. (2009, ngày 12 tháng 9). Các phương pháp hay nhất trong việc thu thập bằng chứng kỹ thuật số . Truy cập ngày 15 tháng 10 năm 2011, từ: <http://computer-forensics.sans.org/blog/2009/09/12/best-practices-in-digital-evidence-collection/>.

24. James S, Nordby JJ. Khoa học pháp y: Giới thiệu về các kỹ thuật điều tra và khoa học xuất bản lần thứ 3. Boca Raton, FL: CRC Press; Năm 2009.

25. Tập đoàn Microsoft. (nd). Encarta: Michael Faraday . Truy cập ngày 13 tháng 6 năm 2011, từ: <http://www.webcitation.org/5kwc3quLs>.

26. Viện Tư pháp Quốc gia. (nd). Lưu đồ thu thập bằng chứng kỹ thuật số: Viện Tư pháp Quốc gia . Truy cập ngày 14 tháng 6 năm 2011, từ: <http://www.nij.gov/publications/ecrime-guide-219941/ch5-evidence-collection/collecting-digital-evidence-flowchart.htm>.

27. Viện Tư pháp Quốc gia. (nd). Bằng chứng kỹ thuật số và Pháp y: Viện Tư pháp Quốc gia . Truy cập ngày 14 tháng 6 năm 2011, từ: <http://www.nij.gov/nij/topics/forensics/evidence/digital/welcome.htm>.

28. Viện Tư pháp Quốc gia. Điều tra pháp y về bằng chứng kỹ thuật số: Hướng dẫn thực thi pháp luật Washington, DC: Văn phòng Bộ Tư pháp Hoa Kỳ về các Chương trình Tư pháp; Năm 2004.

29. Viện Tư pháp Quốc gia. Điều tra hiện trường tội phạm điện tử: Hướng dẫn cho người trả lời đầu tiên xuất bản lần thứ 2. Washington, DC: Bộ Tư pháp Hoa Kỳ; Năm 2008.

30. Viện Tư pháp Quốc gia. Điều tra hiện trường tội phạm điện tử: Tài liệu tham khảo hiện trường cho người trả lời đầu tiên Washington, DC: Bộ Tư pháp Hoa Kỳ; Năm 2009a ;.

31. Viện Tư pháp Quốc gia. Kết quả điều tra thiết bị khối ghi phần cứng: Cầu SCSI của pháp y T4 (Giao diện FireWire) Washington, DC: Viện Tư pháp Quốc gia; Năm 2009b; Bộ Tư pháp Hoa Kỳ, Văn phòng các Chương trình Tư pháp.

32. Viện Tiêu chuẩn & Công nghệ Quốc gia. (nd). Tổng quan về Dự án CFTT . Truy cập ngày 30 tháng 9 năm 2011, from.gov: <http://www.cftt.nist.gov/project_overview.htm>.

33. Viện Tiêu chuẩn và Công nghệ Quốc gia. (nd). Trang web của Dự án Điều tra Công cụ Pháp y Máy tính: Viện Tiêu chuẩn và Công nghệ Quốc gia . Truy cập ngày 6 tháng 6 năm 2011, từ: <http://www.cftt.nist.gov/index.html>.

34. Tổng công ty Paraben. (nd). Thu giữ thiết bị v4.5 . Truy cập ngày 2 tháng 10 năm 2011, từ: <http://www.paraben.com/device-seizure.html>.

35. Phillip A, Cowen D, Davis C. Hacking Exposed Computer Forensics: Computer Forensics Secrets & Solutions New York: McGraw-Hill; Năm 2009.

36. Trung tâm Chính sách Công nghệ Thông tin của Đại học Princeton. (2008, ngày 21 tháng 2). Chúng ta không nên nhớ: Các cuộc tấn công khởi động nguội vào các phím mã hóa . Được truy cập ngày 19 tháng 10 năm 2011, từ: <http://www.youtube.com/watch?v=JDaicPIgn9U>.

37. Saferstein R. Tội phạm học: Giới thiệu về Khoa học Pháp y (Phiên bản Cao đẳng) Lần xuất bản thứ 9. Upper Saddle River, NJ: Prentice Hall; Năm 2006.

38. Nhóm Công tác Khoa học về Bằng chứng Kỹ thuật số. (2009, ngày 15 tháng 1). Hướng dẫn Đề xuất của SWGDE cho Điều tra Xác thực v1.1 . Truy cập ngày 19 tháng 9 năm 2011, từ: <http://www.swgde.org/documents/current-documents/>.

39. Nhóm Công tác Khoa học về Bằng chứng Kỹ thuật số. (2010a, ngày 15 tháng 5). Yêu cầu tối thiểu để đảm bảo chất lượng trong xử lý bằng chứng kỹ thuật số và đa phương tiện . Truy cập ngày 24 tháng 8 năm 2011, từ: <http://www.swgde.org/documents/current-documents/>.

40. Hội nghị Sedona. (2010, tháng 9). Thuật ngữ Hội nghị Sedona: Khám phá điện tử & Quản lý thông tin kỹ thuật số (xuất bản lần thứ 3). Truy cập ngày 21 tháng 10 năm 2011, từ: <http://www.thesedonaconference.org/publications_html>.

41. Shipley, TG (nd). Thu thập bằng chứng từ Internet: Phần 1 . Truy cập ngày 14 tháng 6 năm 2011, từ: <http://www.dfinews.com/article/collection-evidence-internet-part-1?page=0,1>.

42. Shipley, TG (nd). Thu thập bằng chứng từ Internet: Phần 2 . Truy cập ngày 14 tháng 6 năm 2011, từ: <http://www.dfinews.com/article/collection-evidence-internet-part-2>.

43. Shipley TG, Reeve HR. Thu thập Bằng chứng từ Máy tính Đang chạy: Sơ yếu về Kỹ thuật và Pháp lý cho Cộng đồng Tư pháp Sacramento, CA: Search Group, Incorporated; Năm 2006.

44. Warrington, D. (nd). Cảnh Tội ác 101: Xác định vị trí và lập hồ sơ bằng chứng . Truy cập ngày 14 tháng 6 năm 2011, từ: <http://www.forensicmag.com/article/crime-scene-101-locating-and-documenting-evidence>.

45. Whitcomb, C. (nd). Phòng thí nghiệm pháp y kỹ thuật số ảo . Truy cập ngày 28 tháng 9 năm 2011, từ: <http://www.ascld.org/files/digital%20VDEL%20Craiger%20ASCLD%20cmw.pdf>.

46. WSAZ. (2011, ngày 1 tháng 4). CẬP NHẬT: Donald Good nhận được hai bản án cuộc đời trong vụ án hiếp dâm trung tâm mua sắm .

# Chương 5: Phần mềm Hệ thống Windows

### Thông tin trong Chương này:

Tìm dữ liệu đã xóa



Tệp ngủ đông



Điều tra Sổ đăng ký Windows



In bằng chứng Spooling



Hoạt động thùng rác



Siêu dữ liệu: Nó là gì và nó được sử dụng như thế nào



Hình ảnh thu nhỏ làm bằng chứng



Các danh sách được sử dụng gần đây nhất: Cách chúng được tạo ra và giá trị pháp lý của chúng



Làm việc với Điểm Khôi phục và Bản sao Bóng tối



Điều tra tìm nạp trước và liên kết tệp



Microsoft Windows là hệ điều hành được sử dụng rộng rãi nhất trên thế giới. Do đó, những người giám định pháp y kỹ thuật số phải hiểu về cách tạo ra những hiện vật này và cách chúng có thể được sử dụng để theo dõi hoạt động của người dùng. Chương này bao gồm dữ liệu đã xóa và các phần mềm tạo tác như điểm khôi phục, siêu dữ liệu, thùng rác, v.v.

Dữ liệu đã xóa, Hiberfile.sys, Registry, Print Spooling, Recycle BIN, Metadata, Thumbnail Cache, Tệp được sử dụng gần đây nhất (MRU), Điểm khôi phục và Shadow Copy, Liên kết tệp

## Giới thiệu

Nhiều người cho rằng đôi mắt là cửa sổ tâm hồn, nhưng đối với giám định pháp y, Windows có thể là “linh hồn” của máy tính. Khả năng cao là các điều tra viên sẽ gặp phải hệ điều hành Windows nhiều lần hơn là không khi tiến hành điều tra. Tin tốt cho chúng ta là chúng ta có thể sử dụng chính Windows như một công cụ để khôi phục dữ liệu và theo dõi dấu chân người dùng để lại. Do đó, điều tra viên bắt buộc phải có hiểu biết sâu rộng về hệ điều hành Windows và tất cả các chức năng của nó.

Yêu hay ghét nó, đó là một thế giới Windows. Với khoảng 90% ( [Brodkin, 2011](#2__Brodkin__J___n_d____Windows_o) ) thị phần máy tính để bàn, giám định viên pháp y sẽ phải đối mặt với máy chạy Windows phần lớn thời gian. Làm quen với Windows là một điều cần thiết tuyệt đối trong dòng công việc này. Trong quá trình sử dụng Windows và vô số ứng dụng tương thích của nó, người dùng sẽ để lại các hiện vật hoặc dấu chân rải rác khắp máy. Như bạn có thể tưởng tượng, điều này khá hữu ích từ góc độ điều tra. Những hiện vật này thường được đặt ở những nơi xa lạ hoặc “khó tiếp cận”. Ngay cả một cá nhân hiểu biết, cố gắng che giấu dấu vết của họ, có thể bỏ lỡ một số kho báu pháp y bị chôn vùi này.

Thách thức của pháp y là xác định, bảo quản, thu thập và giải thích bằng chứng này một cách chính xác. Trong chương này, chúng ta sẽ xem xét kỹ hơn nhiều hiện vật này, mục đích của chúng và ý nghĩa pháp lý của chúng.

## Dữ liệu đã xóa

Đối với người dùng bình thường, nhấn phím xóa mang lại cảm giác an toàn thỏa mãn. Chỉ với một cú nhấp chuột, chúng ta nghĩ rằng dữ liệu của chúng ta sẽ vĩnh viễn bị xóa sổ, không bao giờ có thể nhìn thấy ánh sáng ban ngày. Nghĩ lại. Chúng ta đã biết từ [Chương 2](#Top_of_CHP002_html) rằng, trái ngược với những gì nhiều người tin tưởng, việc nhấn phím xóa không ảnh hưởng gì đến bản thân dữ liệu. Tệp đã không đi đâu cả. “Xóa” một tệp chỉ cho máy tính biết rằng không gian bị chiếm bởi tệp đó khả dụng nếu máy tính cần. Dữ liệu đã xóa sẽ vẫn còn cho đến khi một tệp khác được ghi lên nó. Quá trình này có thể mất khá nhiều thời gian, nếu nó được thực hiện xong.

Nâng cao hơn

Khắc tệp

Không gian chưa được phân bổ trên ổ cứng có thể chứa bằng chứng có giá trị. Trích xuất dữ liệu này không phải là nhiệm vụ đơn giản. Quá trình này được gọi là khắc tệp và có thể được thực hiện thủ công hoặc với sự trợ giúp của công cụ. Như bạn có thể tưởng tượng, các công cụ có thể tăng tốc quá trình lên rất nhiều. Các tệp được xác định trong không gian chưa được phân bổ bởi một số đặc điểm duy nhất. Đầu trang và chân trang của tệp là những ví dụ phổ biến về các đặc điểm hoặc chữ ký này. Đầu trang và chân trang có thể được sử dụng để xác định tệp cũng như đánh dấu phần đầu và phần cuối của tệp.

Không gian được phân bổ đề cập đến dữ liệu mà máy tính đang sử dụng và luôn bật các tab. Đây là tất cả các tệp mà chúng ta có thể xem và mở trong Windows. Hệ thống tệp của máy tính giám sát các tệp này và ghi lại nhiều thông tin về chúng. Ví dụ: hệ thống tệp theo dõi và ghi lại ngày và giờ một tệp cụ thể được sửa đổi, truy cập và tạo lần cuối. Chúng ta sẽ xem lại loại thông tin này khi chúng ta nói về siêu dữ liệu ở phần sau của chương này.

## Tệp ngủ đông (Hiberfile.Sys)

Máy tính đôi khi cần được nghỉ ngơi và có thể ngủ trưa giống như chúng ta. Thông qua quá trình “cybernap” này, nhiều bằng chứng tiềm năng hơn có thể được tạo ra, tùy thuộc vào mức độ “sâu” của PC đi vào trạng thái ngủ. Các chế độ “ngủ sâu” như ngủ đông và ngủ lai lưu dữ liệu vào ổ cứng thay vì chỉ giữ nó trong RAM (như “ngủ”). Như chúng ta đã biết, dữ liệu được ghi vào ổ đĩa sẽ bền hơn và có thể được phục hồi. Có thể các tệp bị nghi phạm xóa vẫn có thể được tìm thấy ở đây. Làm sao? Giả sử rằng nghi phạm đang làm việc với một tài liệu buộc tội vào thứ Hai. Cô ấy phải bước ra xa một lúc để gọi điện thoại. Cô đặt máy tính xách tay vào chế độ ngủ đông , điều này khiến máy tính lưu mọi thứ cô đang làm vào ổ cứng. Khi cô ấy quay lại 45 phút sau và mang máy tính xách tay trở lại, mọi thứ vẫn y như rằng cô ấy đã để nó, kể cả tài liệu buộc tội. Nói chung, một máy tính có thể chuyển sang ba chế độ hoặc trạng thái khác nhau khi nó ở chế độ ngủ. Các chế độ đó là: ngủ, ngủ đông và ngủ lai. (Tập đoàn Microsoft). Các chế độ khác nhau nhằm tiết kiệm năng lượng và có thể khác nhau giữa các máy tính xách tay với máy tính để bàn.

### 3.1 Ngủ

Chế độ nghỉ nhằm mục đích tiết kiệm năng lượng nhưng cũng nhằm mục đích đưa máy tính trở lại hoạt động nhanh nhất có thể. Microsoft so sánh trạng thái này với trạng thái “tạm dừng đầu đĩa DVD” (Microsoft Corporation; TechTarget). Tại đây, một lượng điện năng nhỏ liên tục được cấp vào RAM, giữ nguyên các dữ liệu đó. Hãy nhớ rằng RAM được coi là bộ nhớ dễ bay hơi, có nghĩa là dữ liệu sẽ biến mất khi nguồn điện bị ngắt. Về cơ bản, chế độ ngủ không có tác dụng gì nhiều đối với chúng ta vì tất cả dữ liệu vẫn còn trong RAM.

### 3.2 Ngủ đông

Ngủ đông (Hibernation) cũng là một chế độ tiết kiệm năng lượng nhưng dành cho máy tính xách tay hơn là máy tính để bàn. Tại đây, chúng ta bắt đầu thấy một số lợi ích điều tra tiềm năng. Ở chế độ này, tất cả dữ liệu trong RAM đều được ghi vào ổ cứng, như chúng ta đã biết, khó bị xóa hơn nhiều.

### 3.3 Ngủ lai

Như tên của nó, chế độ ngủ lai là sự pha trộn của hai chế độ trước đó và chủ yếu dành cho máy tính để bàn. Nó giữ một lượng điện năng tối thiểu được áp dụng cho RAM của bạn (bảo quản dữ liệu và ứng dụng của bạn) và ghi dữ liệu vào đĩa.

Giống như tệp trang, những kẻ tình nghi muốn phá hủy bằng chứng có thể bỏ qua các tệp ngủ đông này. Những kẻ ấu dâm hoặc kẻ gian của công ty thường cố gắng tránh bị phát hiện bằng cách xóa hoặc hủy bằng chứng trên ổ cứng của họ khi cuộc điều tra kết thúc. Những tệp ngủ đông này, không được biết đối với hầu hết người dùng, thường bị bỏ lỡ trong những phút cuối cùng "xóa-a-thons."

## Windows Registry

Windows Registry đóng một vai trò quan trọng trong hoạt động của PC. TechNet của Microsoft định nghĩa sổ đăng ký “chỉ đơn giản là một cơ sở dữ liệu cho các tệp cấu hình”. Bạn cũng có thể mô tả nó như là hệ thống thần kinh trung ương của máy tính. Trong bối cảnh đó, bạn có thể thấy sổ đăng ký quan trọng như thế nào đối với máy tính Windows.

Cơ quan đăng ký theo dõi cấu hình và sở thích của người dùng và hệ thống, đây không phải là nhiệm vụ đơn giản. Từ quan điểm pháp y, nó có thể cung cấp rất nhiều bằng chứng tiềm năng. Nhiều hiện vật mà chúng ta tìm kiếm được lưu giữ trong sổ đăng ký. Một số bằng chứng tiềm năng có thể bao gồm các cụm từ tìm kiếm, chương trình đã được chạy hoặc cài đặt, địa chỉ web, tệp mới được mở gần đây, v.v.

### 4.1 Cấu trúc sổ đăng ký

Sổ đăng ký được thiết lập theo cấu trúc cây tương tự như các thư mục, thư mục và tệp bạn đã quen làm việc trong Windows. Sổ đăng ký được chia thành bốn cấp hoặc cấp.

Điều tra sổ đăng ký là việc được thực hiện trong hầu hết các cuộc khám nghiệm pháp y. Nhìn vào sổ đăng ký yêu cầu một công cụ có thể dịch thông tin này thành một thứ mà chúng ta có thể hiểu được. Hai trong số các công cụ pháp y đa năng chính, EnCase và FTK, làm được điều đó.

Là một kho lưu trữ quan trọng của thông tin hệ thống quan trọng, sổ đăng ký có thể chứa khá nhiều bằng chứng. Như một phần thưởng bổ sung, Cơ quan đăng ký cũng có thể giữ thông tin chúng ta cần để phá vỡ bất kỳ tệp được mã hóa nào mà chúng ta tìm thấy.

#### 4.1.1 Từ các tập tin trường hợp: Windows Registry

Cơ quan đăng ký Windows đã giúp các quan chức thực thi pháp luật ở Houston, Texas phá một trường hợp thẻ tín dụng. Trong trường hợp này, số thẻ tín dụng bị đánh cắp của nghi phạm đã được sử dụng để mua các mặt hàng từ Internet. Hai nghi phạm trong vụ án này, một cặp vợ chồng, đã bị bắt sau một vụ đánh rơi hàng hóa được đặt mua từ Internet có kiểm soát. Điều tra thông tin Nhà cung cấp hệ thống lưu trữ được bảo vệ, đăng ký và NTUSER.DAT của máy tính, tìm thấy danh sách nhiều tên, địa chỉ và số thẻ tín dụng khác được sử dụng trực tuyến để mua hàng. Sau khi điều tra thêm, các nhà điều tra phát hiện ra rằng những thứ này cũng đang được sử dụng bất hợp pháp mà không có sự đồng ý của chủ sở hữu.

Thông tin được khôi phục từ sổ đăng ký là đủ để có được lệnh khám xét bổ sung. Các cuộc khám xét bổ sung này đã bắt giữ 22 cá nhân và dẫn đến việc thu hồi hơn 100.000 đô la hàng hóa đã mua bất hợp pháp. Cuối cùng, tất cả các nghi phạm đều nhận tội danh có tổ chức và bị kết án tù.

#### 4.1.2 Từ tệp trường hợp: Windows Registry và USBStor

Tại một thị trấn nhỏ ngoại ô Austin, Texas, khách tại một khách sạn địa phương đã gọi điện cho cảnh sát sau khi quan sát thấy một cá nhân tại khách sạn đang khỏa thân chuyển vùng và có vẻ hơi say. Khi cảnh sát đến, họ tìm thấy cá nhân và xác định anh ta đang ở tại khách sạn. Họ cùng anh trở về phòng và ngạc nhiên trước những gì họ tìm thấy. Khi cánh cửa mở ra, họ phát hiện ra một cá nhân khác trong phòng và một bức ảnh “đen”được chiếu trên tường. Máy chiếu được gắn vào máy tính xách tay. Hai ổ cứng gắn ngoài được tìm thấy nằm cạnh máy tính xách tay. Người cư ngụ bất ngờ nói rằng chiếc máy tính xách tay là của anh ta nhưng hai ổ đĩa ngoài thuộc về những người đàn ông khác và chưa bao giờ được kết nối với máy tính xách tay của anh ta. Tất cả các thiết bị đã được thu giữ và gửi đi giám định. Bản sao của pháp y được tạo ra từ máy tính xách tay và cả hai ổ đĩa ngoài. Điều tra ban đầu các ổ đĩa bên ngoài đã tìm thấy cả hình ảnh tĩnh và phim khiêu dâm.

Tiếp theo, những người giám định muốn xác định xem một trong hai ổ đĩa đó đã từng được kết nối với máy tính xách tay hay chưa. Tệp đăng ký hệ thống của máy tính xách tay đã được tìm kiếm các mục nhập trong khóa USBStor. Danh sách ổ cứng gắn ngoài đã được phát hiện cùng với số sê-ri phần cứng từ cả hai ổ cứng ngoài.

Tiếp theo, các điều tra viên tìm cách xác nhận kết quả của họ. Sử dụng hệ thống máy tính phòng thí nghiệm có cài đặt Windows sạch sẽ, họ kết nối ổ đĩa ngoài của các bị cáo với hệ thống phòng thí nghiệm. Một trình chặn ghi được kết nối giữa các ổ đĩa và hệ thống để ngăn chặn bất kỳ thay đổi hoặc sửa đổi nào đối với các bản sao của các ổ đĩa ngoài.

Tệp đăng ký hệ thống của máy tính trong phòng thí nghiệm sau đó đã được điều tra và các khóa USBStor hiển thị danh sách ổ cứng ngoài giống như của nghi phạm với số sê-ri phần cứng khớp. Những kết quả này đã chứng minh rằng ổ cứng gắn ngoài của nghi phạm trên thực tế đã được kết nối với máy tính xách tay cùng một lúc. Nghi phạm cuối cùng bị kết tội tàng trữ hình ảnh “đen”.

### 4.1.3 Ghi lại

Pháp y kỹ thuật số có thể được sử dụng để trả lời nhiều câu hỏi, chẳng hạn như, những thuật ngữ nào đã được tìm kiếm bằng Google? Chúng ta có thể tìm thấy điều đó. Bob có gõ những điều khoản đó không? Houston, chúng ta có sự cố rồi. Thật không may, chúng ta hiếm khi có thể đặt ngón tay dính của ai đó lên bàn phím khi một tác phẩm cụ thể được tạo ra. Chúng ta có thể cần khám phá các bằng chứng khác để kết nối các dấu chấm đó.

Theo dõi một cái gì đó trở lại một tài khoản người dùng cụ thể hoặc xác định chủ sở hữu đã đăng ký của hệ thống là một nhiệm vụ dễ dàng hơn nhiều. Một PC có thể có nhiều tài khoản người dùng được thiết lập trên máy. Theo nghĩa kỹ thuật, tài khoản người dùng thiết lập những gì người dùng cụ thể đó có thể và không thể làm trên máy tính (Tập đoàn Microsoft). Theo mặc định, PC sẽ thiết lập hai tài khoản, tài khoản quản trị viên và tài khoản khách. Các tài khoản khác có thể được tạo, nhưng chúng không bắt buộc. Người quản trị có tất cả các quyền và đặc quyền trên máy. Họ có thể làm bất cứ điều gì. Tài khoản khách (không yêu cầu bất kỳ thông tin đăng nhập nào) thường có ít quyền hạn hơn.

Ví dụ: một PC gia đình có thể có các tài khoản riêng cho mẹ, bố và từng đứa trẻ. Mỗi tài khoản này có thể được bảo vệ bằng mật khẩu.

Mỗi tài khoản trên máy được gán một số duy nhất được gọi là số nhận dạng bảo mật hoặc SID. Nhiều hành động trên máy tính được liên kết và theo dõi bởi một SID cụ thể. Thông qua SID mà chúng ta có thể liên kết tài khoản với một số hành động hoặc sự kiện cụ thể.

### 4.2 Ổ đĩa bên ngoài

Thông tin có giá trị, đôi khi giá trị đáng kể. Họ không giữ công thức cho Coke dưới sự khóa chặt và chìa khóa cho nụ cười. Trộm cắp tài sản trí tuệ là một mối quan tâm lớn. Một cách mà những tên trộm có thể dễ dàng tuồn dữ liệu ra khỏi tổ chức là thông qua một trong những thiết bị lưu trữ bên ngoài này, chẳng hạn như ổ USB. Do đó, các điều tra viên thường được yêu cầu xác định xem có bất kỳ thiết bị nào như vậy được gắn vào máy tính hay không.

Các thiết bị này có thể có nhiều dạng khác nhau như ổ USB hoặc ổ cứng gắn ngoài. Ngoài việc đánh cắp thông tin, các thiết bị này cũng có thể được sử dụng để tiêm vi rút hoặc lưu trữ nội dung “đen”. Việc một thiết bị như vậy có được đính kèm hay không có thể được xác định bởi dữ liệu có trong sổ đăng ký. Cơ quan đăng ký ghi lại loại thông tin này với một lượng chi tiết đáng kể. Nó cho chúng ta biết cả nhà cung cấp và số sê-ri của thiết bị.

## In Spooling

Trong một số cuộc điều tra, hoạt động in ấn của nghi phạm có thể có liên quan. Như bạn có thể mong đợi, việc in ấn cũng có thể để lại một số dấu vết cho chúng ta theo dõi. Bạn có thể nhận thấy rằng có một chút chậm trễ sau khi bạn nhấp vào In. Sự chậm trễ này là một dấu hiệu của một quá trình được gọi là spooling . Về cơ bản, bộ đệm tạm thời lưu trữ lệnh in cho đến khi nó có thể được in vào thời điểm thuận tiện hơn cho máy in (TechTarget). Trong quy trình ghép nối này, Windows sẽ tạo một cặp tệp bổ sung. Một là Tệp Meta Nâng cao (EMF), là hình ảnh của tài liệu sẽ được in. Cái còn lại là tệp cuộn chứa thông tin về chính lệnh in.

Có một trong số mỗi cho mỗi lệnh in. Chúng ta có thể khôi phục loại thông tin nào từ tệp cuộn? Tệp cuộn (.spl) cho chúng ta biết những thứ như tên máy in, tên máy tính cũng như tài khoản người dùng đã gửi lệnh đến máy in. Một trong hai hoặc cả hai tệp này có thể có giá trị chứng minh. Vấn đề là chúng không gắn bó lâu dài. Trên thực tế, chúng thường tự động bị xóa sau khi lệnh in kết thúc. Tuy nhiên, có một vài trường hợp ngoại lệ.

Ngoại lệ đầu tiên xảy ra nếu có một số loại sự cố và tài liệu không được in. Thứ hai là máy tính đang bắt đầu lệnh in có thể được thiết lập để giữ lại một bản sao. Một số công ty có thể thấy thiết lập này hấp dẫn nếu họ có lý do nào đó để bám vào một bản sao.

Các tệp Spool và EMF có thể được sử dụng để kết nối trực tiếp các mục tiêu với tội ác của chúng. Bản sao của các bức thư tống tiền, hợp đồng giả mạo, danh sách khách hàng bị đánh cắp và bản đồ đến các địa điểm bán xác chỉ là một vài mẩu vàng làm bằng chứng có khả năng được khai thác từ máy tính của họ.

## Thùng rác

“Thùng rác” đã là một sự hiện diện quen thuộc trên máy tính để bàn của chúng ta bắt đầu từ các hệ thống Macintosh đời đầu. Đó thực sự là một ý tưởng hay, đặc biệt là từ quan điểm của người dùng bình thường. Người dùng có thể không hiểu các sector và byte, nhưng hầu hết mọi người đều “nhận” được thùng rác. Tuy nhiên, đôi khi, thùng rác “lấy” chúng. Điều này đặc biệt đúng khi họ dựa vào thùng rác để xóa bằng chứng của họ. Họ cho rằng dữ liệu buộc tội của họ đã biến mất trong một "Tam giác quỷ Bermuda" kỹ thuật số, không bao giờ còn nhìn thấy ánh sáng ban ngày. Không giống như Amelia Earhart, điều đó chắc chắn không phải vậy. Bằng cách sử dụng các công cụ pháp y như Bộ công cụ pháp y và EnCase, chúng ta khá thường xuyên có thể đưa các tệp đó trở lại trong tình trạng bạc hà.

Báo động!

Chức năng thùng rác

Đây là một câu hỏi nhanh. Một tập tin được di chuyển đến đâu khi nó bị xóa? Tôi cá là một số bạn đã nói thùng rác. Điều đó sẽ có ý nghĩa nhất. Ý tôi là, đó là nơi chúng ta đặt các tệp không mong muốn, phải không? Nhưng nó cũng sẽ sai. Khi bạn xóa một tệp, tệp đó sẽ được chuyển đến ... đợi nó ... ở đâu cả. Bản thân tệp vẫn ở chính xác vị trí của nó. Người ta thường quan niệm rằng khi bị xóa, tệp sẽ thực sự được chọn và chuyển vào thùng rác . Không phải vậy đâu.

Các tệp không mong muốn có thể được chuyển vào thùng rác theo một số cách khác nhau. Chúng có thể được di chuyển từ một mục menu hoặc bằng cách kéo và thả tệp vào thùng rác. Cuối cùng, bạn có thể nhấp chuột phải vào một mục và chọn Xóa. Lợi ích của việc đưa các tệp vào thùng rác là chúng ta có thể tìm hiểu nó và kéo các tệp của mình ra ngoài. Tôi đã làm việc ở những nơi mà đào bới thùng rác văn phòng là một công việc khá nguy hiểm. May mắn thay, mọi thứ gần như không phức tạp trên máy tính của chúng ta. Miễn là các tệp của chúng ta vẫn còn "trong hộp", chúng ta có thể lấy lại chúng. Tuy nhiên, việc dọn sạch thùng rác (tức là “đổ rác”) khiến người dùng bình thường không thể khôi phục được.

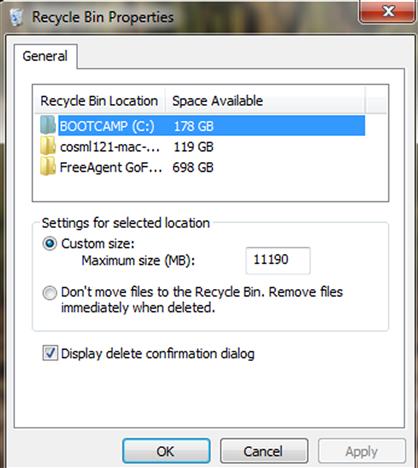
Không phải mọi thứ đã xóa đều đi qua thùng rác. Người dùng thực sự có thể bỏ qua thùng rác hoàn toàn. Bỏ qua có thể được thực hiện theo một số cách. Đầu tiên, nếu bạn nhấn Shift + Delete, tệp sẽ chuyển thẳng đến không gian chưa được phân bổ mà không bao giờ đi qua thùng rác. Bạn cũng có thể định cấu hình máy của mình để hoàn toàn bỏ qua thùng rác. Các tệp đã xóa của bạn thậm chí sẽ không quét các mặt của thùng rác.

Thùng rác rõ ràng là một trong những nơi đầu tiên mà người giám định tìm kiếm bằng chứng tiềm năng. Bản năng đầu tiên mà nghi phạm có là loại bỏ bất kỳ và mọi tệp buộc tội trên máy tính của họ. Không hiểu hết cách thức hoạt động của máy tính, họ đặt trọn niềm tin vào thùng rác. Bây giờ bạn biết đó là một bước đi tồi tệ. Thật may mắn cho chúng ta, nhiều người vẫn không nhận ra niềm tin của họ đã đặt sai chỗ như thế nào. Do đó, thùng rác là một nơi tuyệt vời để tìm kiếm tất cả các loại tệp có khả năng buộc tội.

Nâng cao hơn

Bỏ qua thùng rác

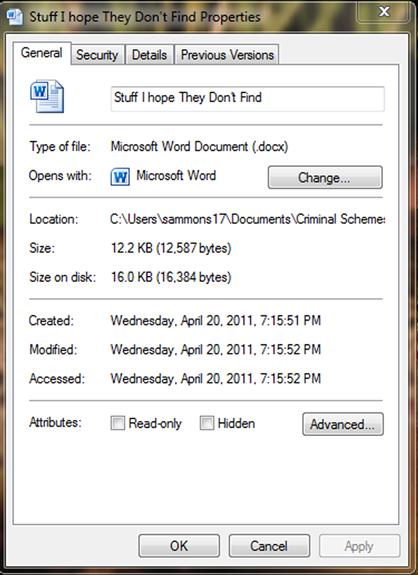
Nếu người điều tra nghi ngờ rằng hệ thống đã được thiết lập để vượt qua thùng rác, điều đầu tiên họ sẽ điều tra là sổ đăng ký. Giá trị “NukeOnDelete” sẽ được đặt thành “1” cho biết rằng chức năng này đã được bật. (Xem [Hình 5.1](#F0010_5) .)



Hình 5.1 Tùy chọn bỏ qua thùng rác.

## Metadata

Siêu dữ liệu thường được định nghĩa là dữ liệu về dữ liệu. Tỷ lệ cược là bạn đã gặp siêu dữ liệu tại một số điểm. Bạn có thể không biết đó là những gì bạn đang nhìn. Có hai loại siêu dữ liệu nếu bạn muốn: ứng dụng và hệ thống tệp. Hãy nhớ rằng hệ thống tệp theo dõi các tệp và thư mục của chúng ta cũng như một số thông tin về chúng. Siêu dữ liệu hệ thống tệp bao gồm ngày và giờ một tệp hoặc thư mục được tạo, truy cập hoặc sửa đổi. Nếu bạn nhấp chuột phải vào một tệp và chọn “Thuộc tính”, bạn có thể thấy các dấu ngày / giờ này như trong [Hình 5.2](#F0015_2) .



Hình 5.2 Thông tin siêu dữ liệu được hiển thị sau khi nhấp chuột phải vào tệp và chọn “Thuộc tính”. Lưu ý ngày và giờ được tạo, sửa đổi và truy cập.

Mặc dù thông tin này có thể chứng minh khá có giá trị đối với một cuộc điều tra, nhưng chúng ta phải lưu ý rằng tất cả các dấu ngày / giờ này có thể không giống như chúng có vẻ. Một vấn đề là đồng hồ của hệ thống có thể được thay đổi bởi người dùng. Sự khác biệt về múi giờ cũng có thể gây ra một số vấn đề. Hãy xem xét kỹ hơn một chút về các tem ngày / giờ được tạo, truy cập và sửa đổi.

Đã tạo — Dấu ngày / giờ được tạo thường cho biết thời điểm tệp hoặc thư mục được tạo trên một phần phương tiện cụ thể, chẳng hạn như ổ cứng ( [Casey, 2009](#3__Casey_E__Handbook_of_Digital_1) ). Làm thế nào tệp đến đó tạo ra sự khác biệt. Nói chung, một tệp có thể được lưu, sao chép, cắt và dán hoặc kéo và thả.

Đã sửa đổi —Ngày và giờ sửa đổi được đặt khi một tệp được thay đổi theo bất kỳ cách nào và sau đó được lưu ( [Casey, 2009](#3__Casey_E__Handbook_of_Digital_1) ).

Đã truy cập — Dấu ngày / giờ này được cập nhật bất cứ khi nào tệp được hệ thống tệp truy cập. Đã truy cập không có nghĩa là giống như đã mở. Bạn có thể hỏi làm thế nào một tệp có thể được truy cập mà không cần mở, và đó là một câu hỏi hay. Bạn thấy đấy, bản thân máy tính có thể tương tác với các tệp. Quét chống vi-rút và các sự kiện đặt trước khác chỉ là hai ví dụ về tương tác tự động này.

Báo động!

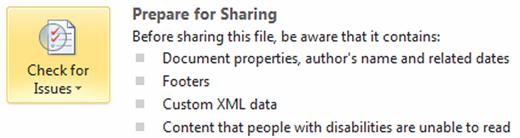
Dấu ngày và giờ

Dấu ngày và giờ của hệ thống KHÔNG nên được lấy đơn giản theo mệnh giá. Các cài đặt này có thể truy cập dễ dàng và có thể dễ dàng thay đổi. Việc xác định mốc thời gian chính xác có thể phức tạp hơn nữa nếu trường hợp liên quan đến nhiều hơn một múi giờ. Chỉ vì siêu dữ liệu nói rằng một tệp được tạo vào một ngày và giờ nhất định không nhất thiết phải làm cho nó như vậy.

Bản thân các ứng dụng cũng có thể tạo và lưu trữ siêu dữ liệu. Giống như hệ thống tệp, chúng có thể theo dõi ngày và giờ được tạo, truy cập và sửa đổi. Nhưng nó không dừng lại ở đó. Họ cũng có thể theo dõi nhiều thuộc tính dành riêng cho ứng dụng. Ví dụ có thể bao gồm tên của tác giả, tên của công ty hoặc tổ chức và tên máy tính, chỉ để đặt tên cho một vài ( [Casey, 2009](#3__Casey_E__Handbook_of_Digital_1) ).

### 7.1 Xóa siêu dữ liệu

Mặc dù siêu dữ liệu từng là một trong những bí mật được giữ kín nhất của chúng ta, nhưng nó không còn nữa. Những tên tội phạm không phải là những người duy nhất chú ý. Các tập đoàn, công ty luật và công dân tư nhân chỉ là một số người quan tâm đến siêu dữ liệu và thông tin có trong đó. Những mối quan tâm chính đáng này đang được giải quyết bằng cách thực sự xóa siêu dữ liệu trước khi chia sẻ những tệp đó với những người khác. Nhiều công cụ tồn tại chỉ cho mục đích đó. Ví dụ: các công ty luật thường xuyên xóa siêu dữ liệu khỏi tất cả các tài liệu gửi đi của họ, như những tài liệu được truyền qua e-mail. Đối với cá nhân quan tâm đến quyền riêng tư, các phiên bản mới hơn của Microsoft Word có khả năng phát hiện và loại bỏ siêu dữ liệu. (Xem [Hình 5.3](#F0020_2) và [5.4](#F0025_2) .)



Hình 5.3 Mục menu để chọn lọc bên trong Microsoft Word 2010.



Hình 5.4 Tùy chọn quét siêu dữ liệu trong Microsoft Word 2010.

Siêu dữ liệu đã khôi phục có thể được sử dụng để bác bỏ các tuyên bố của người nghi ngờ rằng họ không biết về sự tồn tại của tệp. Thật khó để khẳng định rằng bạn không biết nó đã ở đó khi bạn không chỉ mở tệp mà còn thay đổi hoặc xóa tệp. Những ngày và giờ này cũng có thể được sử dụng để xây dựng các mốc thời gian trong một trường hợp.

#### 7.1.1 Từ tệp trường hợp: Siêu dữ liệu

Siêu dữ liệu có thể giúp các nhà điều tra xác định tất cả các nghi phạm trong một vụ án và thu hồi thêm bằng chứng. Lấy trường hợp này từ Houston, Texas liên quan đến việc sản xuất thẻ tín dụng giả mạo. Các nghi phạm trong trường hợp này đã sử dụng thông tin thẻ “đọc lướt” trong quá trình sản xuất thẻ của họ. Thẻ tín dụng “đọc lướt” là khi kẻ trộm lấy dữ liệu từ dải từ tính ở mặt sau của thẻ tín dụng và thẻ ghi nợ. Điều này thường xảy ra trong một giao dịch hợp pháp, chẳng hạn như khi bạn sử dụng thẻ của mình để thanh toán bữa tối.

Sau khi xác định được nghi phạm chính của họ, cảnh sát đã bắt anh ta và khám xét máy tính của anh ta. Cuối cùng, việc tìm kiếm máy tính thật đáng thất vọng. Cuộc tìm kiếm chỉ tìm thấy một tài liệu Microsoft Word có chứa thông tin “đã đọc lướt qua”. Hơn nữa, khám xét nơi ở không tìm thấy phần cứng skimmer và cũng không có phần mềm đọc lướt trên máy tính. Không hẳn là kho báu mà họ hy vọng sẽ tìm thấy.

Kỳ thi không dừng lại ở đó. Điều tra thêm tài liệu Word nhấn phải trả tiền. Đánh giá siêu dữ liệu cho thấy tác giả của tài liệu, một phụ nữ. Điều tra sâu hơn cho thấy cô là bạn gái của nghi phạm và cô làm hầu bàn ở một thị trấn lân cận. Thông tin này cung cấp cho các nhà điều tra nguyên nhân có thể xảy ra để có được lệnh khám xét căn hộ của cô lần thứ hai. Trong lần tìm kiếm thứ hai, skimmer (phần cứng được sử dụng để trích xuất dữ liệu từ dải từ) đã được phục hồi. Việc điều tra máy tính không chỉ tìm thấy phần mềm đọc lướt mà còn có thêm danh sách thẻ ghi nợ và các thông tin liên quan. May mắn thay, thông tin này đã được thu giữ trước khi nó có thể được sử dụng. Cả hai nghi phạm cuối cùng đều bị kết tội.

## Bộ nhớ cache hình thu nhỏ

Để giúp bạn duyệt ảnh trên máy tính dễ dàng hơn, Windows tạo các phiên bản ảnh nhỏ hơn gọi là ảnh thu nhỏ . Hình thu nhỏ chỉ là phiên bản thu nhỏ của các bản sao lớn hơn của chúng. Những hình thu nhỏ này được tạo tự động bởi Windows khi người dùng chọn chế độ xem “Hình thu nhỏ” khi sử dụng Windows Explorer. Windows tạo ra một số loại tệp hình thu nhỏ khác nhau, tùy thuộc vào phiên bản đang được sử dụng. Windows XP tạo một tệp có tên thumbs.db. Microsoft Vista và Windows 7 tạo một tệp tương tự có tên là thumbcache. db.

Hầu hết người dùng hoàn toàn không biết rằng các tệp này thậm chí còn tồn tại. Điều thú vị về những tệp này là chúng vẫn còn ngay cả sau khi hình ảnh gốc đã bị xóa. Ngay cả khi chúng ta không khôi phục được hình ảnh ban đầu, hình thu nhỏ có thể là bằng chứng tốt nhất tiếp theo. Sự tồn tại đơn thuần của chúng cho chúng ta biết rằng những bức ảnh đó tồn tại tại một điểm trên hệ thống.

## Được sử dụng gần đây nhất (MRU)

Windows cố gắng làm cho cuộc sống của chúng ta, ít nhất là trên máy tính của chúng ta, trở nên dễ chịu nhất có thể. Không phải lúc nào họ cũng thành công, nhưng trái tim của họ đã đặt đúng chỗ. Danh sách được sử dụng gần đây nhất (MRU) là một trong những ví dụ về việc Microsoft nghĩ đến chúng ta. MRU là các liên kết đóng vai trò là lối tắt đến các ứng dụng hoặc tệp đã được sử dụng gần đây. Bạn có thể thấy những điều này đang hoạt động bằng cách nhấp vào nút Bắt đầu của Windows thông qua menu tệp trên nhiều ứng dụng. (Xem [Hình 5.5](#F0030_1) .)



Hình 5.5 Ví dụ về MRU trong Microsoft Word 2010.

## Điểm khôi phục và sao chép bóng (shadow copy)

Bạn có bao giờ ước mình có thể quay ngược thời gian không? Chúng ta vẫn chưa ở đó, nhưng may mắn cho chúng ta là Windows. Có thể đến một lúc nào đó, việc máy tính của chúng ta trở lại thời điểm trước đó dễ dàng hơn (hoặc cần thiết) khi mọi thứ đang hoạt động tốt. Trong Windows, chúng được gọi là điểm khôi phục (RP) và chúng đóng vai trò như cỗ máy du hành thời gian cho máy tính của chúng ta.

### 10.1 Điểm khôi phục

Điểm khôi phục là ảnh chụp nhanh các cài đặt và cấu hình hệ thống chính tại một thời điểm cụ thể (Tập đoàn Microsoft). Những ảnh chụp nhanh này có thể được sử dụng để đưa hệ thống trở lại trạng thái hoạt động. Điểm khôi phục được tạo theo nhiều cách khác nhau. Chúng có thể được hệ thống tạo tự động trước các sự kiện lớn của hệ thống, chẳng hạn như cài đặt phần mềm. Chúng có thể được lên lịch định kỳ, chẳng hạn như hàng tuần. Cuối cùng, người dùng có thể tạo chúng theo cách thủ công. Tính năng điểm khôi phục được bật theo mặc định và một ảnh chụp nhanh được tạo tự động mỗi ngày.

Trước khi bắt đầu tìm kiếm các điểm khôi phục, bạn nên biết rằng Microsoft đã thực hiện các bước để giữ chúng khỏi con mắt tò mò của bạn. Chúng thường bị ẩn khỏi người dùng.

Các RP này có siêu dữ liệu (dữ liệu về dữ liệu) được liên kết với chúng. Thông tin này có thể có giá trị trong việc xác định thời điểm mà ảnh chụp nhanh này được chụp. Nếu RP chứa bằng chứng, điều này có thể cho chúng ta biết chính xác thời điểm dữ liệu đó tồn tại trên hệ thống được đề cập.

Đào qua các điểm khôi phục có thể phát hiện ra những viên ngọc bằng chứng không tồn tại ở bất kỳ nơi nào khác. Đối với những người bình thường cố gắng che giấu thông tin với các nhà điều tra, các điểm khôi phục có thể không phải là nơi đầu tiên họ bắt đầu tiêu hủy bằng chứng. Rõ ràng, điều đó có lợi cho chúng ta.

#### 10.1.1 Từ các tập tin trường hợp: Lịch sử Internet & Điểm khôi phục

Một bị cáo bị buộc tội sở hữu nội dung “đen” khai rằng anh ta đã truy cập trang web được đề cập chỉ trong một lần truy cập và đó chỉ là tình cờ. Để bác bỏ tuyên bố này, các điều tra viên đã quay sang các điểm khôi phục trong hai tháng trước đó. Việc điều tra từng tệp đăng ký được tìm thấy trong các điểm khôi phục khác nhau đã kể một câu chuyện khác nhau đáng kể. Bằng chứng cho thấy không chỉ có nhiều trang web “đen” đã được truy cập, mà các URL đã được nhập trực tiếp vào thanh địa chỉ của trình duyệt, hủy bỏ tuyên bố của anh ta rằng trang web đã được truy cập một cách tình cờ. Đối chất với chứng cứ mới này, bị cáo nhanh chóng nhận tội.

### 10.2 Bản sao bóng

Các bản sao bóng cung cấp dữ liệu nguồn cho các điểm khôi phục. Giống như điểm khôi phục, các tệp bóng là một tạo tác khác rất có thể đáng để xem xét. Chúng ta có thể sử dụng chúng để chứng minh cách một tệp cụ thể đã được thay đổi theo thời gian. Họ cũng có thể giữ các bản sao của các tệp đã bị xóa ( [Larson, 2010](#5__Larson__T___2010__July_8___Wi) ).

#### 10.2.1 Từ Hồ sơ Vụ án: Điểm khôi phục, Bản sao bóng tối và Chống pháp y

Các sĩ quan từ Đơn vị Không gian mạng của Texas OAG (Văn phòng hoặc Bộ trưởng Tư pháp), đáp ứng lời khuyên, đã tống đạt lệnh khám xét nơi ở của nghi phạm. Đơn vị Không gian mạng của OAG đã nhận được lệnh khám xét sau khi họ được cảnh báo rằng nghi phạm đang tải nội dung “đen” lên Internet. Khi các sĩ quan tống đạt lệnh khám xét, họ thấy ngôi nhà không có người ở. Các nhân viên đã gọi cho nghi phạm để thông báo cho anh ta biết họ đang ở trong nhà của anh ta và anh ta nên về nhà ngay lập tức và gặp họ. Khi nghi phạm đến nơi, các cảnh sát đã phỏng vấn nghi phạm và khám xét xe của anh ta. Bên trong xe có một máy tính xách tay.

Tất cả các vật phẩm bị thu giữ đã được đưa đến văn phòng OAG để giám định pháp y. Trong quá trình điều tra máy tính xách tay của nghi phạm, một phát hiện đáng báo động đã được thực hiện. Có vẻ như nghi phạm, trên đường lái xe về nhà để gặp các sĩ quan, đã sử dụng một công cụ xóa để xóa không chỉ các hình ảnh buộc tội mà còn cả lịch sử Internet khỏi máy tính xách tay của anh ta. Trong khi điều tra ban đầu không tìm thấy nội dung “đen” nào trên máy tính xách tay, các bằng chứng thuyết phục khác đã được thu hồi.

Ví dụ: người điều tra có thể khôi phục nhật ký từ chính chương trình xóa cho thấy rằng nó thực sự đã được chạy. Đó không phải là tất cả. Vì hệ điều hành là Windows Vista, điều tra viên quyết định điều tra các bản sao bóng được tìm thấy trên máy. Hãy nhớ rằng, các Bản sao Bóng tối này (hoặc Điểm Khôi phục Hệ thống) về cơ bản là những bức ảnh chụp nhanh dữ liệu tại một thời điểm nhất định.

Tiếp theo, hình ảnh pháp y (bản sao) của máy tính xách tay của nghi phạm được tải vào một môi trường ảo. Điều này cho phép người giám định nhìn thấy hệ thống máy tính như những gì nghi phạm đã nhìn thấy. Giám định viên đã xuất ra các điểm khôi phục từ máy tính xách tay của nghi phạm, sau đó nhập các tệp đó vào công cụ pháp y của mình. Quá trình này cho phép người giám định sử dụng các công cụ của mình để trích xuất hình ảnh và các thông tin khác từ các điểm khôi phục hệ thống của nghi phạm. Thủ tục này đánh trả tiền bẩn. Hơn 3000 hình ảnh “đen” đã được thu hồi. Ngoài ra, các tệp nhật ký đã được tìm thấy hiển thị các tìm kiếm và tải xuống các tệp đó. Khi tất cả những gì đã nói và làm, nghi phạm nhận tội và hiện đang thụ án 10 năm trong nhà tù ở bang Texas.

## Liên kết tệp

Tất cả chúng ta đều thích các phím tắt. Chúng giúp chúng ta tránh việc xây dựng đường và tránh tắc đường. Chúng giúp chúng ta tiết kiệm thời gian và làm cho chuyến đi của chúng ta dễ dàng hơn, ít nhất là trên lý thuyết. Microsoft Windows cũng thích các phím tắt. Nó thích họ rất nhiều.

Các tệp liên kết chỉ đơn giản là các phím tắt. Chúng trỏ đến các tệp khác. Các tệp liên kết có thể được tạo bởi chúng ta hoặc thường xuyên hơn bởi máy tính. Bạn có thể đã tạo một lối tắt trên màn hình đến chương trình hoặc thư mục yêu thích của mình. Máy tính tự tạo ra chúng ở một số nơi khác nhau. Bạn có thể đã xem và sử dụng các tệp liên kết này trước đây. Lấy ví dụ như Microsoft Word. Nếu bạn nhìn dưới menu Tệp, bạn sẽ thấy một tùy chọn có tên là “gần đây”. Các mục trong danh sách đó là các tệp liên kết hoặc phím tắt do máy tính tạo ra.

Các tệp liên kết có dấu ngày và thời gian của riêng chúng hiển thị khi chúng được tạo và sử dụng lần cuối. Sự tồn tại của một tệp liên kết có thể quan trọng. Nó có thể được sử dụng để cho thấy rằng ai đó đã thực sự mở tệp được đề cập. Nó cũng có thể được sử dụng để bác bỏ khẳng định rằng một tệp hoặc thư mục chưa bao giờ tồn tại. Các tệp liên kết cũng có thể chứa đường dẫn tệp đầy đủ, ngay cả khi thiết bị lưu trữ không còn được kết nối, chẳng hạn như ổ USB.

### 11.1 Các chương trình đã cài đặt

Phần mềm được hoặc đã được cài đặt trên máy tính được hỏi cũng có thể được quan tâm. Điều này đặc biệt đúng nếu ứng dụng tương tự hiện đã bị xóa sau một số thời điểm có liên quan (tức là khi nghi phạm biết về một cuộc điều tra tiềm năng). Có nhiều vị trí trên ổ đĩa để tìm kiếm những hiện vật này. Thư mục chương trình là một nơi tuyệt vời để bắt đầu. Các tệp liên kết và tìm nạp trước là hai vị trí khác cũng có thể mang lại kết quả.

## Bản tóm tắt

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 ta 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. Ghi công là một thách thức lớn trong pháp y kỹ thuật số. Nói một cách chắc chắn tuyệt đối rằng một cá nhân cụ thể chịu trách nhiệm về một hiện vật nhất định thường là không thể. Xác định tài khoản thường là cách tốt nhất có thể được thực hiện.

Hệ thống và các ứng dụng chúng ta sử dụng tạo ra dữ liệu về dữ liệu. Thông tin này, được gọi là siêu dữ liệu, có thể cho chúng ta 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 chức năng tìm nạp trước là hai nguồn cung cấp thông tin có thể có liên quan này.

## Tổng kết và kiến thức thêm chương 5

1. **Hiểu được cách thu thập và điều tra dữ liệu trên thiết bị Windows**

Quá trình thu thập dữ liệu trên thiết bị Windows

Thu thập thông tin tạm thời -> Thu thập thông tin được lưu trữ -> Phân tích bộ nhớ Windows -> Phân tích cấu hình Windows -> Phân tích cache, cookie, và lịch sử trình duyệt -> phân tích tệp tin hệ thống -> phân tích mảnh thông tin -> phân tích nhật ký sự kiện

1. Thu thập thông tin tạm thời
2. Thu thập thông tin được lưu trữ
3. **Phân tích bộ nhớ, cấu hình windows**
4. Phân tích bộ nhớ

Mục đích: Thu thập các thông tin sống

Phương pháp phân tích bộ nhớ:

Thông qua phương pháp phân tích VHD

Thông qua phương pháp Memory Dump

Công cụ phân tích bộ nhớ:

Bin text, Handle

1. Phân tích cấu hình windows

Mục đích: Xem những thay đổi liên quan đến hệ điều hành cũng như thời gian xảy ra sự cố

Phương pháp phân tích cấu hình windows:

Thông qua phương pháp xem nhật ký sự kiện

Công cụ phân tích cấu hình windows:

ProDiscover

1. **Phân tích tệp tin Windows**

Mục đích: Thu thập thông tin được tạo, cấu hình từ hệ điều hành Windows

Phương pháp:

1. Nhật ký ghi lại thông tin khôi phục hệ thống
2. Prefetch directory
3. Lối tắt
4. Tệp hình ảnh
5. Siêu dữ liệu metadata – Công cụ Metashield Analyzer
6. **Phân tích nhật ký và nhật ký sự kiện trên Windows**

Mục đích: điều tra toàn bộ sự kiện xảy ra trên thiết bị

Phương pháp: Thu thập tất cả nhật ký được ghi lại trong tệp tin nhật ký

Công cụ: OS Forensics

1. **Kiểm tra cache, cookies, và thông tin trên trình duyệt**

Mục đích: Thu thập các bằng chứng liên quan đến trình duyệt, hoạt động duyệt web

* Phân tích trình duyệt Firefox:

Thông thường các thông tin này được lưu trong tệp tin trình duyệt. Đối với Cache sẽ được lưu vào mục Local, nhưng với Cookies và Lịch sử sẽ được lưu vào mục Roaming.

Công cụ phân tích: MZCacheView; MZCookiesView; và MZHistoryView

* Phân tích Chrome

Đối với Chrome, các tệp tin đều được lưu trong mục Local, tuy nhiên dữ liệu cache sẽ được chrome lưu trữ dười mục cache

Công cụ phân tích: ChromeCacheView, ChromeCookiesView, ChromeHistoryView

* Phân tích Edge

Đối với Edge, các tệp này đều được lưu trong mục local, tuy nhiên dữ liệu cache và lịch sử được lưu dưới mục Microsoft, Cookies thì lại được lưu dưới mục Packages

Công cụ phân tích: IECacheView, IECookiesView, BrowsingHistoryView

1. **Biết được các lệnh để truy cập nhật ký trên Linux**

Các lệnh tiêu biểu: stat, history, ps, su, sudo

1. **Hiểu được cách thu thập và điều tra dữ liệu trên thiết bị Linux**

Các lệnh tiêu biểu: netstat, ifconfig –a, arp, ls

Tài liệu tham khảo

1. Bard, J. (nd). Sổ đăng ký Windows . Truy cập ngày 2 tháng 5 năm 2011, từ: <http://technet.microsoft.com/en-us/library/cc751049.aspx>.

2. Brodkin, J. (nd). Windows sắp giảm xuống dưới 90% thị phần . Truy cập ngày 2 tháng 5 năm 2011, từ: <http://www.networkworld.com/news/2011/011311-windows-on-verge-of-dropping.html>.

3. Casey E. Sổ tay Điều tra và Pháp y Kỹ thuật số Burlington, MA: Academic Press; Năm 2009.

4. Gupta MR, Hoeschele MD, Rogers MK. Vùng đĩa ẩn: HPA và DCO. Tạp chí Quốc tế về Bằng chứng Kỹ thuật số 2006;: 1–8.

5. Larson, T. (2010, ngày 8 tháng 7). Windows 7: Các sự kiện hiện tại trong thế giới của Windows Forensics . Truy cập ngày 3 tháng 5 năm 2011, từ: <http://computer-forensics.sans.org/summit-archives/2010/files/12-larson-windows7-foreniscs.pdf>.

6. Tập đoàn Microsoft. (nd). Cách Thùng rác Lưu trữ Tệp . Truy cập ngày 2 tháng 5 năm 2011, từ: <http://support.microsoft.com/kb/136517>.

7. Tập đoàn Microsoft. (nd). Ngủ và Ngủ đông: Các câu hỏi thường gặp . Được truy cập ngày 2 tháng 5 năm 2011, từ: <http://windows.microsoft.com/en-US/windows7/Sleep-and-hibernation-frequently-asked-questions>.

8. Tập đoàn Microsoft. (nd). Khôi phục hệ thống: Các câu hỏi thường gặp . Được truy cập ngày 2 tháng 5 năm 2011, từ: <http://windows.microsoft.com/en-US/windows-vista/System-Restore-frequently-asked-questions>.

9. Tập đoàn Microsoft. (nd). Tổng quan về Tài khoản Người dùng: Tập đoàn Microsoft . Được truy cập ngày 2 tháng 5 năm 2011, từ: <http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/usercpl_overview.mspx?mfr=true>.

10. Phillip A, Cowen D, Davis C. Hacking Exposed Computer Forensics: Computer Forensics Secrets & Solutions New York: McGraw-Hill; Năm 2009.

11. TechTarget. (nd). Spool: [Whatis.com](http://Whatis.com) . Được truy cập ngày 2 tháng 5 năm 2011, từ: <http://whatis.techtarget.com/definition/0,,sid9_gci214229,00.html>.

# Chương 6: Kỹ thuật chống lại điều tra số

**Thông tin trong Chương này:**

Giới thiệu công nghệ mã hóa và mối đe dọa mà nó đặt ra



Các cuộc tấn công được sử dụng để phá vỡ mã hóa



Các kỹ thuật được sử dụng để ẩn và phá hủy dữ liệu



Những câu chuyện thành công của pháp y kỹ thuật số đang được biết đến rộng rãi. Do đó, tội phạm rất quan tâm trong việc cản trở các loại hình điều tra này. Một số kỹ thuật này rất hiệu quả, chúng có thể khiến việc khôi phục thông tin hầu như không thể. Đây là mối quan tâm nghiêm trọng đặc biệt là trong bối cảnh an toàn công cộng. Để chống lại các kỹ thuật chống lâm sàng này, các giám định viên phải làm quen với các cách khác nhau để che giấu và phá hủy dữ liệu. Họ cũng phải nắm vững các công cụ và phương pháp theo ý mình để vượt qua các nỗ lực chống pháp y.

Thuật toán, Mã hóa, Làm xáo trộn, Không gian khóa, Bẻ khóa mật khẩu, Xóa, Ghi mật mã, Tệp mang, Tải trọng, Hệ thống tệp mã hóa (EFS), FileVault, Tấn công Brute Force, Mã hóa đối xứng, Mã hóa không đối xứng, Mô-đun nền tảng đáng tin cậy (TPM), , Tấn công từ điển, Văn bản mật mã

## Giới thiệu

Các cuộc điều tra máy tính và kết quả bằng chứng xuất hiện thường xuyên trong các blog cảnh sát trên khắp đất nước. Để chống lại những tiến bộ pháp y tương đối mới này, các công cụ và kỹ thuật chống pháp y đang được cắt xén với số lượng đáng kể. Chúng đang được sử dụng bởi tội phạm, khủng bố và các giám đốc điều hành công ty. Vào tháng 2 năm 2011, Valerie Caproni, Tổng cố vấn của FBI, đã phát biểu trước Tiểu ban Hạ viện về Tội phạm, Khủng bố và An ninh Nội địa. Liên quan đến mã hóa và mối đe dọa mà nó đại diện, cô nói với tiểu ban, "Khi khoảng cách giữa thẩm quyền và năng lực ngày càng rộng, chính phủ ngày càng không thể thu thập bằng chứng có giá trị trong các trường hợp từ bóc lột trẻ em và nội dung “đen”đến tội phạm có tổ chức và buôn bán ma túy cho đến khủng bố và gián điệp - tin rằng một tòa án đã ủy quyền cho chính phủ thu thập. Khoảng cách này gây ra mối đe dọa ngày càng tăng đối với an toàn công cộng ”( [Caproni, 2011](#7__Caproni_V__Going_Dark__Lawful) ).

Có nhiều định nghĩa cho thuật ngữ chống lại điều tra số . John Barbara định nghĩa nó theo cách này “một cách tiếp cận để thao túng, xóa hoặc làm xáo trộn dữ liệu kỹ thuật số hoặc làm cho việc điều tra dữ liệu đó trở nên khó khăn, tốn thời gian hoặc hầu như không thể” ( [Barbara, 2008](#4__Barbara__J___2008__December_0) ).

Thậm chí có một trang web dành riêng cho chủ đề này, và chúng không hề tinh tế chút nào về mục tiêu của chúng. [Anti-Forensics.com](http://Anti-Forensics.com) là một “cộng đồng dành riêng cho việc nghiên cứu và chia sẻ các phương pháp, công cụ và thông tin có thể được sử dụng để làm nản lòng các cuộc điều tra pháp y máy tính và giám định pháp y”. Nó tiếp tục mô tả mục đích của trang web, nói rằng, "Mục tiêu chính của một số phần mềm chống pháp y và trọng tâm của [Anti-Forensics.com](http://Anti-Forensics.com) , là làm cho việc phân tích và điều tra bằng chứng kỹ thuật số trở nên khó khăn, khó hiểu và tốn nhiều thời gian. tiêu thụ càng nhiều càng tốt ”( [Anti-Forensics.com là](http://Anti-Forensics.com) gì?).

Việc sử dụng các kỹ thuật chống lâm tặc không chỉ giới hạn ở những kẻ khủng bố và ấu dâm. Các giám đốc điều hành công ty cũng đã đưa chúng vào sử dụng, sử dụng các công cụ và kỹ thuật này để ẩn hoặc hủy các thư điện tử buộc tội, hồ sơ tài chính, v.v. Ngay cả các ứng dụng hàng ngày như trình duyệt web cũng có các tính năng có thể được sử dụng để cản trở việc khám nghiệm pháp y — chẳng hạn như xóa lịch sử Internet. Hầu hết các trình duyệt mới hơn đều có chế độ “duyệt web riêng tư” không ghi lại những thứ như các trang web đã truy cập và tìm kiếm. Trong phiên bản Firefox mới nhất, việc chạy ở chế độ riêng tư sẽ không còn lưu các trang đã truy cập, các mục nhập biểu mẫu và thanh tìm kiếm, mật khẩu, mục danh sách tải xuống, cookie và tệp bộ đệm web ( [Mozilla Foundation, 2011](#26__Mozilla_Foundation___n_d) ). Xem [Hình 6.1](#F0010_6) .



Hình 6.1 Tùy chọn menu “Bắt đầu duyệt web riêng tư” trong Firefox 6.0. Cũng lưu ý tùy chọn “Xóa lịch sử gần đây”.

Trong chương này, chúng ta sẽ xem xét một số kỹ thuật được sử dụng để che giấu hoặc tiêu hủy bằng chứng kỹ thuật số. Như bạn sẽ thấy, một số kỹ thuật này có hiệu quả cao khi được sử dụng đúng cách. Các kỹ thuật khác ít hoặc không ảnh hưởng đến việc khám nghiệm pháp y. Ngay cả khi sử dụng một trong những công cụ xóa ổ đĩa có sẵn trên thị trường cũng không đảm bảo rằng dữ liệu sẽ thực sự biến mất.

Từ góc độ điều tra, điều quan trọng là phải biết rằng có những cách sử dụng hợp pháp các công cụ và kỹ thuật chống lâm nghiệp này. Do đó, việc chứng minh ý định là rất quan trọng. Những kẻ tình nghi có thể khẳng định rằng ứng dụng xóa chỉ được sử dụng để bảo vệ quyền riêng tư của họ hoặc họ đã sử dụng tiện ích chống phân mảnh để cải thiện hiệu suất. Điều đó là khả thi. Tuy nhiên, sự phòng thủ đó sẽ khó nuốt trôi hơn một chút nếu công cụ chỉ được sử dụng một lần và đó là ba giờ sau khi mục tiêu biết về cuộc điều tra.

## Ẩn dữ liệu

Kỹ thuật ẩn bao gồm từ đơn giản đến rất phức tạp. Thay đổi tên tệp và phần mở rộng, chôn tệp sâu trong các thư mục dường như không liên quan, ẩn tệp trong tệp và mã hóa là một số kỹ thuật ẩn phổ biến nhất. Đây là hai kỹ thuật cuối cùng có thể khiến các học viên pháp y kỹ thuật số mất ngủ vào ban đêm.

### 2.1 Mã hóa

Tất cả chúng ta có những bí mật. Các công ty, chính phủ và cá nhân chia sẻ sự thật phổ quát này. Công thức chế biến gà rán của Đại tá, số tài khoản ngân hàng của chúng ta và kế hoạch chiến tranh của Quân đội chỉ là một vài ví dụ về thông tin cần được giữ kín. Trước khi thế giới của chúng ta trở thành một thế giới có dây như vậy, việc giữ an toàn cho vật liệu này, theo nhiều khía cạnh, ít phức tạp hơn rất nhiều.

Việc sử dụng hợp pháp mã hóa đã cho phép chúng ta tận hưởng nhiều dịch vụ Internet mà hiện nay chúng ta coi đó là điều hiển nhiên. Ví dụ: mã hóa được sử dụng trong thương mại điện tử cho phép chúng ta mua những cuốn sách yêu thích và đặt chỗ cho kỳ nghỉ hè của chúng ta. Nó giữ cho các doanh nghiệp của chúng ta hoạt động và đất nước của chúng ta an toàn. Tuy nhiên, những tiện nghi hiện đại này không phải là không có. Tiền mã hóa là một con dao hai lưỡi với những hậu quả nghiêm trọng khi được sử dụng bởi tội phạm, khủng bố, các quốc gia không thân thiện và cả những CEO quanh co.

Ngày nay, chúng ta có ít quyền kiểm soát trực tiếp hơn đối với những bí mật này khi chúng di chuyển qua Internet hoặc bay qua không trung trên mạng không dây. Đó là mã hóa cung cấp cho chúng ta cả cơ chế và sự tự tin để lưu trữ và truyền tải thông tin kỹ thuật số nhạy cảm nhất của chúng ta. Tuy nhiên, trong cuốn sách này, trọng tâm là mặt tối của công nghệ này và mối đe dọa mà nó gây ra. Giá trị của nó chắc chắn không bị mất vào tay nhiều người có ý đồ xấu. Lấy ví dụ những kẻ khủng bố; mặc dù lối sống dường như công nghệ thấp của họ, họ đang nắm bắt công nghệ bao gồm cả mã hóa.

“Ở mức độ lớn hơn và lớn hơn, các nhóm khủng bố, bao gồm cả Hezbollah, Hamas và nhóm al Qaida của bin Laden, đang sử dụng các tệp tin, e-mail và mã hóa được máy tính hóa để hỗ trợ các hoạt động của chúng” - Giám đốc CIA George Tenet viết hồi tháng 3 năm ngoái. Ủy ban Đối ngoại Thượng viện. Ramzi Yousef, kiến trúc sư của vụ đánh bom Trung tâm Thương mại Thế giới năm 1993, là một trong những kẻ khủng bố đưa tiền mã hóa vào sử dụng. Yousef đã lưu kế hoạch chi tiết để tiêu diệt các máy bay của Mỹ được mã hóa trên máy tính xách tay của mình ( [Dick, 2001](#11__Dick__Ronald_L__Issue_of_Int) ). Nếu được thực hiện đúng cách, mã hóa có thể giữ chân người điều tra cho đến khi địa ngục đóng băng, theo đúng nghĩa đen.

### 2.2 Mã hóa là gì?

Mã hóa là việc chuyển đổi dữ liệu thành một dạng, được gọi là văn bản mật mã , mà những người không có thẩm quyền không thể dễ dàng hiểu được ( [Bauchie, Hazen, Lund, Oakley, & Rundatz, 2000](#5__Bauchie_R__Hazen_F__Lund_J__O) ). Mã hóa bắt đầu bằng văn bản thuần túy. Văn bản thuần túy là tin nhắn gốc, không được mã hóa. Tin nhắn văn bản thuần túy rõ ràng và có thể được đọc bởi bất kỳ ai. Sau đó, một thuật toán mật mã được áp dụng cho văn bản thuần túy, tạo ra văn bản mật mã. Văn bản mật mã về cơ bản là một phiên bản xáo trộn của văn bản thuần túy khó hiểu. Thuật toán là phương pháp được sử dụng để mã hóa thông điệp. Chìa khóa là dữ liệu được sử dụng để mã hóa và giải mã thông tin. Mật khẩu hoặc cụm mật khẩu thường được sử dụng làm chìa khóa.

### 2.3 Mã hóa sớm

Bản thân mã hóa không phải là sản phẩm phụ của công nghệ máy tính. Nó đã tồn tại hàng ngàn năm dưới dạng này hay dạng khác. Một trong những sơ đồ mã hóa sớm nhất và nổi tiếng nhất là Mật mã Caesar. Caesar Cipher là một công cụ chuyển đổi mật mã và mã hóa dữ liệu bằng cách thay thế các ký tự gốc bằng số ký tự “x” phía trước trong bảng chữ cái. Ví dụ: sử dụng Mật mã Caesar và khóa năm, chữ “A” sẽ trở thành chữ “F”. [Bảng 6.1](#Top_of_CHP006_html) cho thấy toàn bộ bảng chữ cái cả dưới dạng văn bản thuần túy và văn bản mật mã sau khi áp dụng cùng một mật mã. Lưu ý rằng mỗi chữ cái đã được dịch chuyển năm khoảng trắng so với vị trí ban đầu của nó.

Bảng 6.1. Bảng chữ cái với mã hóa đơn giản (Caesar Cipher). Chìa khóa trong ví dụ này là Năm

|  |  |
| --- | --- |
| Văn bản thô | ABCDEFGHIJKLMNOPQRSTU VWXYZ |
| Văn bản mật mã | FGHIJKLMNOPQRSTUVWXYZ ABCDE |

Bây giờ chúng ta hãy mã hóa “pháp y” bằng Caesar Cipher với khóa là tám. [Bảng 6.2](#T0015) cho chúng ta thấy sự chuyển đổi văn bản thuần túy sang văn bản mật mã.

Bảng 6.2. Hiển thị chuyển đổi từng chữ cái bằng cách sử dụng mật mã Caesar và khóa 8

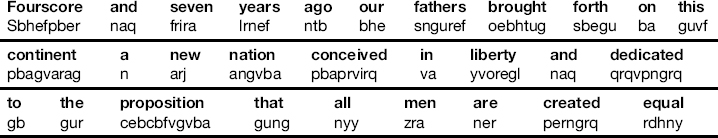


Quy trình đơn giản này vẫn được sử dụng cho đến ngày nay. Nó thường được sử dụng để làm xáo trộn mã máy tính. Thoạt nhìn, có vẻ như các thuật ngữ mã hóa và obfuscate có thể hoán đổi cho nhau. Chúng giống nhau đến mức đôi khi bị nhầm lẫn, nhưng sự khác biệt đủ đáng kể để làm rõ. Cả hai đều nhằm mục đích làm cho mọi thứ khó hiểu hơn. Tuy nhiên, Obfuscation được sử dụng để bảo vệ mã máy tính, thay vì chính dữ liệu ( [Tyma, 2003](#37__Tyma_P__Encryption__Hashing) ). Obfuscation cũng bảo vệ mã khỏi kỹ thuật đảo ngược. Không thể sử dụng mã hóa theo cách này vì nó sẽ hiển thị mã hoàn toàn không thể đọc được đối với máy tính.

ROT13 là phiên bản hiện đại của Mật mã Caesar đang được sử dụng ngày nay để giải mã. Trong ROT13, các chữ cái được dịch chuyển 13 vị trí. Trong lược đồ này, chữ “A” trở thành chữ “N”, v.v. [Bảng 6.3](#T0020) cho thấy một đoạn trích từ Địa chỉ Gettysburg của Lincoln sau khi ROT13 đã được áp dụng.

Bảng 6.3. Việc mở địa chỉ Gettysburg của Lincoln được mã hóa bằng ROT13

‘



### 2.4 Các thuật toán

Đối với những thách thức về mặt toán học, như bản thân tôi, chỉ cần thuật toán từ ngữ cũng có thể gây ra một số lo lắng. Các thuật toán chúng ta sử dụng để gửi số thẻ tín dụng của mình trên Internet phức tạp hơn theo cấp số nhân so với mật mã mà Julius sử dụng ở Rome. Mặc dù các thuật toán phức tạp và nằm ngoài phạm vi của cuốn sách này, chúng ta vẫn có thể nắm được cách sử dụng và chức năng cơ bản của chúng. Nói một cách đơn giản, thuật toán chỉ là một tập hợp các hướng dẫn được sử dụng để hoàn thành một nhiệm vụ nhất định. Ví dụ, chúng ta có thể tạo một thuật toán để gửi e-mail về một cuộc họp sắp tới.

1 . Đến văn phòng.

2 . Bật máy tính

3 . Mở Microsoft Outlook

4 . Nhấp vào “Email mới”

5 . Điền thông tin "Tới"

6 . Nhập “Cuộc họp” vào dòng chủ đề

7 . Nhập nội dung thư

8 . Nhấn gửi

Về cơ bản, có hai loại thuật toán mã hóa: đối xứng và không đối xứng. Mã hóa đối xứng sử dụng cùng một khóa để mã hóa và giải mã dữ liệu. Ngược lại, mã hóa không đối xứng sử dụng hai khóa riêng biệt và khác biệt.

Ngày nay có rất nhiều thuật toán mã hóa đang được sử dụng phục vụ nhiều mục đích khác nhau. Bạn có thể đã nghe nói về một số trong số họ. AES, TripleDES, Blowfish và RSA chỉ là một số ít.

#### 2.4.1 Thuật toán: Không có gì bí mật

Nó có thể gây ngạc nhiên, nhưng bản thân các thuật toán đã mở và được công bố tốt. Tại sao trên thế giới họ sẽ đưa thông tin này ra khỏi đó? Nó chắc chắn có vẻ phản trực giác. Tin hay không thì tùy, câu trả lời là bảo mật. Thực tiễn tốt nhất trong mật mã nói rằng tính bảo mật của các thuật toán nên “độc lập với tính bí mật của chúng” ( [Schneier, 2002](#29__Schneier_B__Crypto_Gram_News) ).

Nguyên tắc mật mã cơ bản này đã có từ khá lâu. Vào năm 1883, Auguste Kerckhoffs, một nhà ngôn ngữ học và mật mã học người Hà Lan, đã nói rằng trong bất kỳ hệ thống mật mã thực sự hiệu quả nào, chìa khóa phải là bí mật duy nhất. Bất kỳ hệ thống nào dựa vào tính bí mật của thuật toán đều kém an toàn hơn ( [Schneier, 2002](#29__Schneier_B__Crypto_Gram_News) ).

“Bài học số 1 mà tôi đã học được từ công việc của mình tại AccessData là 'bạn không thể tin tưởng vào tiền điện tử nguồn đóng.' Bạn không biết liệu nó có an toàn hay không, ”Nephi Allred, một nhà phân tích mật mã của AccessData cho biết. “Tôi đã thiết kế ngược rất nhiều ứng dụng trong thời của mình: một số tốt, một số xấu. Mặc dù có một số ứng dụng mã nguồn đóng tốt và một số ứng dụng mã nguồn mở xấu (thực tế là rất ít), các ứng dụng tốt nhất luôn là mã nguồn mở và tệ nhất luôn là mã nguồn đóng. Cá nhân tôi, tôi sẽ không bao giờ tin tưởng dữ liệu của mình vào một ứng dụng mã nguồn đóng ”, Allred nói.

### 2.5 Không gian chính

Không gian khóa là một số liệu thường được thảo luận khi nói về sức mạnh của một lược đồ mã hóa cụ thể. Không gian khóa hoặc độ dài khóa có ảnh hưởng trực tiếp đến khả năng phá vỡ mã hóa của chúng ta, đặc biệt là với một cuộc Bruteforce. Một cuộc tấn công brute force cố gắng phá mật khẩu bằng cách thử mọi tổ hợp phím có thể có cho đến khi tìm thấy đúng.

Đây là lúc điều này trở nên đặc biệt khó khăn khi bạn xem xét tất cả các hoán vị khóa có thể có và mất bao lâu để "đoán" mật khẩu. Một lược đồ mã hóa với khóa 128 bit sẽ có khoảng 340.282.366.920, 938.000.000.000.000.000.000.000.000.000.000 tổ hợp khóa khả thi. Máy tính sẽ mất bao lâu để đoán mật khẩu? Nghiền một số con số thô sẽ cho chúng ta một ý tưởng. Sử dụng một máy tính, đoán 500.000 mật khẩu mỗi giây sẽ phá vỡ khóa đó trong khoảng 21.580.566.141.612.000.000.000.000.000.000 năm. Hãy nâng số lượng máy tính đoán mật khẩu lên con số 1000. Điều đó đưa chúng ta đến thời gian chờ "dễ quản lý" hơn nhiều chỉ là 21.580, 566.11612.000.000.000.000.000.000 năm. Hãy nhớ những con số này đại diện cho các ước tính thô; sự thật là chúng có thể cao hơn nhiều tùy thuộc vào thuật toán được sử dụng. Các chương trình mã hóa phức tạp như Pretty Good Privacy (PGP) có thể giảm hoàn toàn số lần thử mỗi giây xuống chỉ còn vài trăm ( [Schneier, 2007](#30__Schneier_B__Secure_Passwords) ).

### 2.6 Một số kiểu mã hóa phổ biến

Với mối quan tâm lớn về quyền riêng tư như vậy, các công cụ mã hóa hiện đã được đưa vào một số phiên bản của hệ điều hành mới hơn bao gồm Windows 7 và Apple OS X. Các công cụ này lần lượt là BitLocker và FileVault . Các lược đồ mã hóa này có thể được áp dụng một cách chọn lọc, chỉ mã hóa một số tệp hoặc thư mục nhất định. Chúng cũng có thể được sử dụng để mã hóa toàn bộ ổ đĩa. Đây được gọi là mã hóa toàn bộ hoặc toàn bộ đĩa.

Mã hóa toàn bộ đĩa (FDE) có một số ưu điểm đáng chú ý. Chúng ta đã biết từ các chương trước rằng hệ điều hành trong quá trình hoạt động bình thường của chúng sẽ để lại các hiện vật nằm rải rác trên ổ đĩa. Lấy không gian hoán đổi chẳng hạn. Mặc dù chúng ta mã hóa toàn bộ thư mục chứa các tệp nhạy cảm của chúng ta, phần còn lại (hoặc toàn bộ tệp) có thể nằm trong không gian hoán đổi. Mã hóa toàn bộ đĩa sẽ xử lý những “rò rỉ” dữ liệu này. Thuật ngữ mã hóa toàn bộ ổ đĩa hơi gây hiểu nhầm. Nó không thực sự mã hóa toàn bộ đĩa. Để chạy BitLocker, phải có hai phân vùng (phần) trên ổ cứng: một phân vùng được gọi là “ổ đĩa hệ điều hành” và phân vùng còn lại chứa các tệp để khởi động máy, các công cụ hệ thống, v.v. Khối lượng hệ điều hành chứa mọi thứ khác bao gồm phần lớn các mục mà chúng ta quan tâm nhất ( [Microsoft Corporation, 2009](#25__Microsoft_Corporation__Windo) ).

Như họ nói, không có bữa trưa miễn phí. FDE cũng có một số nhược điểm. Hiệu suất có thể sẽ bị ảnh hưởng vì dữ liệu đang được mã hóa và giải mã. Việc mã hóa / giải mã này được thực hiện “nhanh chóng”, nghĩa là nó xảy ra ngay trước khi dữ liệu được lưu hoặc tải vào RAM. Mật khẩu và chìa khóa là một mối quan tâm khác. Việc khôi phục dữ liệu của bạn phụ thuộc vào việc có xác thực thích hợp. Nếu bạn bị mất hoặc quên mật khẩu, bạn sẽ rất có thể không bao giờ lấy lại được dữ liệu của mình. Mã hóa cắt giảm cả hai cách.

#### 2.6.1 Hệ thống tệp mã hóa (EFS)

Hệ thống tệp mã hóa (EFS) được sử dụng để mã hóa tệp và thư mục. EFS rất dễ sử dụng, chỉ sử dụng hộp kiểm trong thuộc tính của tệp. Nó “không được hỗ trợ đầy đủ trên Windows 7 Starter, Windows 7 Home Basic và Windows 7 Home Premium” (Microsoft Corporation). EFS sử dụng tên người dùng và mật khẩu Windows như một phần của thuật toán mã hóa. EFS là một tính năng của Hệ thống Tệp Công nghệ Mới (NTFS), không phải của hệ điều hành Windows (Microsoft Corporation).

#### 2.6.2 Bitlocker

Không giống như EFS, BitLocker có thể được sử dụng để mã hóa toàn bộ ổ cứng, trong khi BitLocker To Go được sử dụng để mã hóa phương tiện di động như ổ USB (Tập đoàn Microsoft). BitLocker không có sẵn trong tất cả các phiên bản Windows. Hiện tại, nó chỉ có sẵn trên hệ thống Windows 7 Ultimate (Microsoft Corporation). BitLocker thường không hoạt động một mình. Nó thường hoạt động cùng với một phần cứng được gọi là Mô-đun nền tảng đáng tin cậy (TPM) . TPM là một vi mạch trên bo mạch chủ của máy tính xách tay hoặc PC nhằm cung cấp các chức năng mật mã (Tập đoàn Microsoft). TPM tạo và mã hóa các khóa mà chỉ TPM mới có thể giải mã được. Nếu được định cấu hình để hoạt động mà không cần TPM, thì các khóa cần thiết sẽ được lưu trữ trên ổ USB.

Mã hóa BitLocker khá cứng nhắc, khiến việc giải mã trở nên nghi ngờ nếu không có chìa khóa.

Gặp phải một máy BitLockered đang chạy mang lại cho người điều tra một cơ hội tuyệt vời để khôi phục dữ liệu mà không cần phải đánh bại mã hóa BitLocker. Các tệp được lưu trữ trong vùng được bảo vệ bằng BitLocker của ổ cứng sẽ được giải mã khi chúng được hệ thống yêu cầu ( [Microsoft Corporation, 2009](#25__Microsoft_Corporation__Windo) ). Bất cứ lúc nào bạn có thể tránh sử dụng mã hóa là một điều tốt.

Khi xử lý một máy tính đang chạy, việc nhận ra sự hiện diện của BitLocker có thể tạo ra tất cả sự khác biệt trong một trường hợp. Máy BitLockered đang chạy đó rất có thể đại diện cho cơ hội duy nhất mà bạn có để khôi phục bất kỳ bằng chứng nào từ máy tính đó.

#### 2.6.3 Apple Filevault

Phiên bản OS X mới nhất của Apple, Lion, đi kèm với FileVault 2. FileVault2 sử dụng mã hóa AES 128 bit. Với FileVault 2, bạn có thể mã hóa nội dung của toàn bộ ổ đĩa của mình. Apple cho phép khách hàng có cơ hội lưu trữ khóa khôi phục bên mình. Mật khẩu được lưu trữ với Apple có thể được truy xuất với cơ quan tìm kiếm pháp lý thích hợp ( [Apple, Inc., 2011](#2__Apple__Inc__OS_X_Lion__About) ).

#### 2.6.4 Truecrypt

TrueCrypt là một phần mềm mã nguồn mở miễn phí cung cấp chức năng mã hóa nhanh chóng. Trong mã hóa nhanh, dữ liệu sẽ tự động được mã hóa và giải mã khi chúng được lưu và mở. Tất cả những điều này được thực hiện ở hậu trường mà không có bất kỳ sự tham gia nào của người dùng. TrueCrypt cũng có khả năng cung cấp mã hóa toàn bộ ổ đĩa. Điều này bao gồm tên tệp, tên thư mục, cũng như nội dung của mọi tệp. Nó cũng bao gồm những tệp có thể chứa dữ liệu nhạy cảm mà hệ thống tự tạo ra. Những tệp này bao gồm những thứ như tệp nhật ký, tệp hoán đổi và mục đăng ký. Việc giải mã yêu cầu mật khẩu chính xác và (các) tệp khóa. TrueCrypt hỗ trợ các hệ điều hành Windows, Mac và Linux ( [Hiệp hội các nhà phát triển TrueCrypt, 2011](#35__TrueCrypt_Developers_Associa) ). TrueCrypt có thể sử dụng nhiều thuật toán mã hóa bao gồm AES, Serpent, Twofish hoặc một số kết hợp của ba thuật toán này. Không gian khóa là 256 bit.

### 2.7 Phá mật khẩu

Việc phá mật khẩu, hoặc phá mật mã, rất khó khăn, hoặc gần như không thể trong thực tế. Để mang đến cho chúng ta cơ hội thành công tốt nhất, chúng ta cần sử dụng bất kỳ lợi thế nào mà chúng ta có thể có được. Có nhiều cách để phá mật khẩu; một số là kỹ thuật, một số thì không. Đôi khi nó đơn giản như hỏi. Các tùy chọn bao gồm tấn công Bruteforce , tấn công từ điển và đặt lại mật khẩu. Tất cả chúng đều có thể mang lại kết quả tích cực. Chúng ta sẽ tìm hiểu kỹ hơn về những cuộc tấn công này trong phần sắp tới.

Tin tốt là nó không phải là tất cả đều u ám và diệt vong. Trong hầu hết các trường hợp, chúng ta vẫn đang giao dịch với mọi người và họ đại diện cho điểm yếu nhất trong toàn bộ quá trình này. Con người có thể vừa lười biếng vừa bất cẩn, tạo cơ hội cho chúng ta bẻ khóa mã hóa. Có quá nhiều người sử dụng mật khẩu đơn giản dễ bị phá vỡ. Một số tốt nhất bao gồm “mật khẩu”, “letmein” hoặc “123.” ngày càng phổ biến. Ngày sinh, tên thú cưng, hoặc tên của đội thể thao yêu thích của chúng ta cũng được sử dụng thường xuyên. Việc ghi nhớ các mật khẩu dài ngẫu nhiên không phải là điều dễ dàng hoặc thuận tiện đối với đa số chúng ta. Ngay cả khi một mật khẩu mạnh được sử dụng, đôi khi nó được ghi vào một ghi chú Post-It và được dán vào màn hình. Hơn nữa, các khóa mã hóa có thể không được bảo mật và có thể bị xâm phạm.

Con người, là những sinh vật có thói quen, khá thường xuyên sử dụng lại ít nhất một phần mật khẩu của họ. Chúng ta có thể khai thác hành vi này để có lợi cho mình. Nếu chúng ta có thể lấy một mật khẩu, nhiều lần chúng ta có thể lấy được tất cả. “Đôi khi nếu chúng ta có thể truy cập và tìm thấy một trong hai mật khẩu đó, hoặc hai hoặc ba mật khẩu, tôi có thể bắt đầu phát hiện ra rằng trong mỗi mật khẩu, bạn sử dụng số 3,” Stuart Van Buren, một nhân viên Sở Mật vụ Hoa Kỳ ( [Homeland Security Newswire, 2011](#15__Homeland_Security_Newswire) ).

Điều gì đủ điều kiện chính xác là một mật khẩu mạnh? Theo Microsoft, một mật khẩu mạnh sử dụng nhiều chữ cái, số, dấu chấm câu và ký hiệu và có độ dài tối thiểu là mười bốn ký tự (Tập đoàn Microsoft).

Điều tra viên có thể gặp may và tìm thấy mật khẩu trong không gian hoán đổi trên ổ cứng. Việc nắm bắt RAM của máy đang chạy cũng có thể giúp phá mật khẩu. Có thể bạn đã nhập mật khẩu trên một trang web vào lúc này hay lúc khác. Khi bạn nhập mật khẩu của mình, các dấu chấm xuất hiện, che giấu văn bản khi bạn nhập. Điều bạn có thể không nhận ra là mật khẩu thực được ghi trong RAM. Không lấy được RAM từ một máy đang chạy thực sự có thể là một cơ hội bị bỏ lỡ.

Khi có nhu cầu, chúng ta có sẵn các công cụ đặc biệt có thể phá mật khẩu thông qua nhiều cuộc tấn công khác nhau. Những công cụ này có thể phá vỡ một số mật khẩu đơn giản trong vòng chưa đầy một giây. Một trong những công cụ hàng đầu thuộc loại này là Bộ công cụ khôi phục mật khẩu (PRTK) của AccessData, công ty phần mềm pháp y máy tính có trụ sở tại Utah. Các công cụ khác bao gồm John the Ripper và Cain and Abel.

## Tấn công mật khẩu

Mật khẩu có thể bị tấn công và phá vỡ theo nhiều cách, nhưng tránh mã hóa luôn tốt hơn là phải tấn công mật khẩu. Có những công cụ và kỹ thuật chúng ta có thể sử dụng để tăng cơ hội thành công. Một điều có lợi cho chúng ta là tính dễ bị tổn thương mà con người gây ra. Các chuỗi chữ cái, số và ký tự ngẫu nhiên dài tạo nên mật khẩu tuyệt vời. Thật không may, chúng cũng khó để mọi người nhớ đến. Do đó, hầu hết các mật khẩu đều dựa trên các từ thực tế, các mẫu có thể nhận dạng được hoặc cả hai.

### 3.1 Tấn công Bruteforce

Một cuộc tấn công Bruteforce chỉ là những gì nó nghe có vẻ như vậy. Chúng ta đang sử dụng nhiều khả năng tính toán nhất có thể để đoán đúng mật khẩu. Chúng ta có thể ném càng nhiều máy tính (hay chính xác hơn là các đơn vị xử lý trung tâm) thì chúng ta có thể phá vỡ nó càng nhanh. Như bạn sẽ thấy, “nhanh hơn” là một thuật ngữ tương đối khi nói đến việc phá mật khẩu. Các sản phẩm hiện có sẵn để khai thác các máy tính không hoạt động và sử dụng chúng với tệp, thư mục hoặc ổ đĩa được mã hóa. Đây được gọi là một cuộc tấn công phân tán vì gánh nặng tính toán được lan truyền giữa nhiều máy tính. Một số cơ quan đang trở nên khá sáng tạo trong việc phá vỡ mã hóa.

Các nhân viên pháp y kỹ thuật số của Trung tâm Tội phạm Mạng Thực thi Di trú và Hải quan Hoa Kỳ đang sử dụng máy chơi game Sony PS3 nối mạng để tấn công mật khẩu. Cách tiếp cận này tận dụng sức mạnh của các thiết bị này cũng như hiệu quả chi phí của chúng. Claude E. Davenport, một đại lý tại Trung tâm Tội phạm Mạng Thực thi Di trú và Hải quan Hoa Kỳ cho biết: “Kẻ xấu đang mã hóa nội dung của họ, vì vậy chúng ta cần một phương pháp hack vào đó để cố gắng phá mật khẩu. “Playstation 3 - thành phần xử lý của nó - hoàn hảo cho các cuộc tấn công thư viện quy mô lớn” ( [Wawro, 2009](#40__Wawro_A__US_Government_Using) ).

### 3.2 Đặt lại mật khẩu

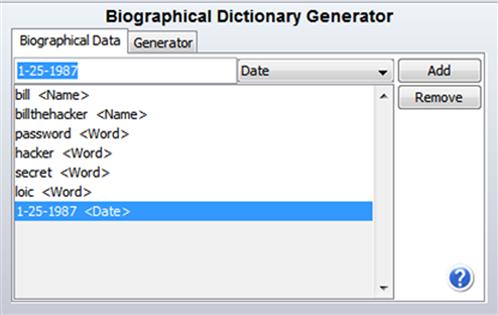
Đôi khi chúng ta sẽ theo đuổi phần mềm hơn là mật khẩu. Một số ứng dụng có lỗ hổng có thể bị khai thác để chỉ cần đặt lại mật khẩu, cung cấp cho chúng ta quyền truy cập mà chúng ta cần. Thật không may, việc đặt lại mật khẩu không có hiệu quả rộng rãi, chỉ hoạt động trên một số lượng tương đối nhỏ các ứng dụng. Trong những trường hợp cần thiết phải bỏ qua mật khẩu hệ thống Windows, đĩa CD khởi động được có thể hoàn thành công việc. Họ thực hiện điều này bằng cách ghi đè dữ liệu trong Trình quản lý tài khoản bảo mật, gọi tắt là SAM. Công cụ Khôi phục Hệ thống của Elcomsoft là một trong nhiều sản phẩm đáp ứng nhu cầu này (Elcomsoft Co. Ltd.).

### 3.3 Tấn công từ điển

Tấn công từ điển chính xác hơn, sử dụng các từ và cụm từ có thể được thu thập từ nhiều nguồn. Ví dụ, một ứng dụng pháp y có thể tạo chỉ mục của tất cả các từ được tìm thấy trên ổ cứng của nghi phạm. Những từ này sẽ đến từ cả không gian được phân bổ và không được phân bổ. Các nguồn từ điển khác có thể là các thuật ngữ thường được sử dụng trong một số giới tội phạm nhất định như nội dung “đen” hoặc buôn bán ma tuý. Từ điển cũng có thể chứa các từ từ các nguồn cụ thể như các trang web.

Thông tin tình báo, thông tin cơ bản về kẻ tình nghi hoặc mục tiêu của chúng ta, thực sự có thể làm tăng cơ hội thành công của chúng ta. Thông tin này có thể được sử dụng để xây dựng một từ điển các mật khẩu tiềm năng. Thu thập thông tin này bắt đầu tại hiện trường. Chúng ta không chỉ quan tâm đến các thiết bị kỹ thuật số mà còn là ảnh, sách, v.v. Chúng ta muốn biết tên của trẻ em và vật nuôi trong đối tượng của chúng ta. Chúng ta muốn biết sở thích và đam mê của họ. Các điều khoản và từ ngữ liên quan đến những lợi ích này có thể cung cấp manh mối cho mật khẩu của nghi phạm. Ví dụ: nếu nghi phạm là một fan cuồng của Chúa tể những chiếc nhẫn (LOTR), chúng ta có thể sử dụng một công cụ sẽ lập chỉ mục (ghi lại nội dung) của một trang web dành cho LOTR. Công cụ sẽ lấy tên và địa điểm như Aragorn và Rivendell. Sau đó, những thuật ngữ này có thể được sử dụng để tạo từ điển tùy chỉnh có thể giúp mở khóa mật khẩu.

Hãy xem việc tạo một từ điển tùy chỉnh dựa trên thông tin tiểu sử về nghi phạm của chúng ta, Bill Thehacker. Chúng ta sẽ sử dụng Bộ công cụ khôi phục mật khẩu của AccessData. Chúng ta nhập tổng cộng bảy bit thông tin bao gồm tên, ngày sinh và một số từ khóa liên quan đến Bill. (Xem [Hình 6.2](#F0015_3) .)

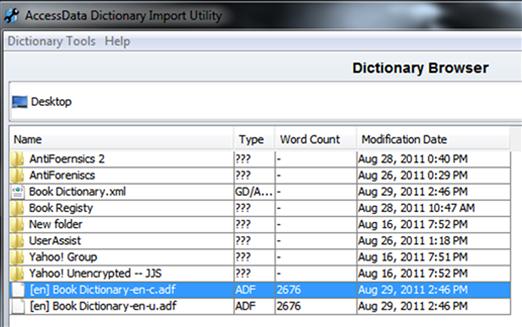


Hình 6.2 Trình tạo từ điển tiểu sử trong PRTK.

Từ bảy từ trong [Hình 6.2](#F0015_3) , công cụ sau đó tạo ra hơn 26 trăm hoán vị, một mẫu trong số đó được thể hiện trong [Bảng 6.4](#Top_of_CHP006_html) . Lưu ý sự kết hợp của các thuật ngữ với vô số tiền tố và hậu tố.

Bảng 6.4. Lấy mẫu của hơn 26 trăm từ khóa được tạo từ danh sách bảy từ khóa ban đầu của chúng ta

|  |  |  |
| --- | --- | --- |
| 1  2519871251987billbillbill billbill-billbill\_billbillb  bill  -bbill\_bbillbillthehackerbill billthehackerbill-billthehackerbill\_billthehackerbillbbill bbill-bbill\_b | b25billthehacker  billthehacker251bbillthehacker125bb251billthehackerb125billthehacker25billthehacker1b25b1billthehacker1billthehacker25b1b25billthehacker  billthehacker1b25  b1billthehacker25billthehacker25b1b25billthehacker1billthehacker25billbill25billthehackerbillthehacker251billbillthehacker125billbill251billthehackerbill125billthehacker25billthehacker1bill25bill1billthehacker | 251987secret  251987  secretecret1987h1987secretsecret198725hsecret251987hh198725secreth251987secret1987secret25h 1987h25secret  25secret1987h25h1987secretsecret25h1987h25secret1987ecretecret1987h |



Hình 6.3 Số lượng từ cuối cùng được tạo ra bởi bảy mục nhập gốc của chúng ta.

Tài nguyên bổ sung

Mã hóa

Bruce Schneier là một tác giả và nhà mật mã học có uy tín, người thường xuyên xuất bản về các vấn đề liên quan đến mã hóa và bảo mật. Ông là tác giả của một số cuốn sách cũng như Thuật toán mã hóa Blowfish. Cuốn sách của anh ấy Bí mật & Dối trá: An ninh kỹ thuật số trong một thế giới có mạng vừa hấp dẫn vừa rất dễ đọc. Anh ấy cũng xuất bản một blog và Bản tin Crypto-Gram. Bạn nên ghé thăm trang web của anh ấy, <http://www.schneier.com/>.

## Steganography

Steganography , hay viết tắt là stego, là một cách khác và rất hiệu quả để che giấu dữ liệu. Từ steganography bắt nguồn từ tiếng Hy Lạp “Stegos” có nghĩa là bao phủ và “Graphie” có nghĩa là viết. Nguồn gốc chính xác của nó tương đương với chữ viết được che phủ. [SearchSecurity.com](http://SearchSecurity.com) định nghĩa steganography là “việc che giấu một thông điệp bí mật trong một tin nhắn thông thường và trích xuất nó tại đích của nó” ( [TechTarget, 2000](#34__TechTarget__Steganography_20) ).

Có hai tệp tạo thành tệp stego đã hoàn thành. Tệp chứa thông điệp bí mật được gọi là tệp mang . Tệp mang có thể là tệp hình ảnh, tệp video, tệp âm thanh và tài liệu xử lý văn bản, chỉ để đặt tên cho một số tệp. Tài liệu bí mật được nhúng được gọi là tải trọng . Khái niệm cơ bản đằng sau steganography khá đơn giản. Hãy bắt đầu với các tệp của nhà cung cấp dịch vụ. Các loại tệp này được sử dụng vì chúng có lượng dữ liệu dư thừa đáng kể, còn được gọi là “nhiễu”. Dữ liệu thừa được thay thế bằng dữ liệu soạn tin ẩn. Tệp tải trọng không nhất thiết phải dựa trên văn bản. Một tệp hình ảnh có thể được chèn vào một tệp hình ảnh khác. Có thể có nhiều biến thể hoặc kết hợp.

Các ứng dụng Steganography có sẵn rộng rãi trên Internet và nhiều ứng dụng miễn phí. Backbone Security, một công ty sản xuất một trong những công cụ phát hiện steg phổ biến hơn, đã lập danh mục hơn 960 ứng dụng steganography riêng biệt có sẵn để tải xuống trên internet ( [Backbone Security.com, 2011](#3__Backbone_Security_com__Backbo) ).

Điều gì làm cho stego trở thành mối quan tâm như vậy? Đầu tiên, nó rất khó phát hiện. Thứ hai, sau khi phát hiện ra, rất khó, nếu không muốn nói là không thể, để giải nén tải trọng mà không biết ứng dụng steg và mật khẩu được sử dụng để tạo nó.

Trước khi chết dưới tay của Seal Team Six, Osama Bin Laden và các đồng nghiệp của hắn đã sử dụng rộng rãi kỹ thuật đọc mật mã để giao tiếp. Các tệp Stego đã được đăng trong các phòng trò chuyện thể thao và các bảng thông báo “đen”( [Kelley, 2005](#17__Kelley_J__Terrorist_Instruct) ).

Việc phát hiện việc sử dụng steganography khá khó khăn. Một trong những công cụ phổ biến nhất là Stego Suite ™ từ Trung tâm Nghiên cứu và Phân tích Steganography (SARC). Phiên bản hiện tại xác định hơn năm trăm ứng dụng steganography đã biết và có khả năng bẻ khóa và trích xuất tải trọng từ các tệp của nhà cung cấp (Wetstone Technologies, Inc.).

Vào tháng 6 năm 2010, FBI đã bắt giữ mười điệp viên Nga đã ở Hoa Kỳ trong khoảng một thập kỷ. Những điệp viên này đã sử dụng rộng rãi kỹ thuật in mật mã khi họ chuyển các thông điệp bí mật cho SVR, cơ quan tình báo Nga ( [CBS News, 2010](#10__CBS_News__FBI__10_Russian_Sp) ). Một đơn khiếu nại hình sự trong trường hợp này, được nộp tại Quận phía Nam của New York, đã cung cấp một số thông tin chi tiết về việc sử dụng kỹ thuật in mật mã của người Nga. Trong đơn khiếu nại, Đặc vụ Maria Ricci nói một phần:

“Ngoài ra, và trong số những thứ khác, một số Thông điệp Điện tử của Kẻ âm mưu Boston xuất hiện trực tiếp liên quan đến việc liên lạc bằng phương tiện mật mã. Ví dụ, một tin nhắn, ngày 15 tháng 12 năm 2004, thảo luận về quá trình 'giải mã [ing]' các tin nhắn được nhúng trong hình ảnh; một thông báo khác, ngày 22 tháng 2 năm 2005, thảo luận về dữ liệu 'decypher [ing] [sic]' được nhúng trong hình ảnh. Tương tự, vào hoặc khoảng ngày 3 tháng 10 năm 2004, các nhân viên thực thi pháp luật, hành động theo lệnh tư pháp, đã chặn liên lạc bằng âm thanh diễn ra bên trong ngôi nhà ở Boston. Tracey Lee Ann Foley, bị cáo, đã được nghe nói với Donald Howard Heathfield, bị cáo: 'Chúng ta có thể đính kèm hai tệp có chứa tin nhắn hay không? Hãy nói bốn bức tranh…. ' Dựa trên quá trình đào tạo, kinh nghiệm và sự tham gia của tôi trong cuộc điều tra này, tôi tin rằng đây là một tham chiếu đến việc truyền tải thông điệp bằng phương pháp in mật mã — đặt 'tệp chứa thông báo' trong 'ảnh'. Vào hoặc khoảng ngày 7 tháng 3 năm 2010, các nhân viên thực thi pháp luật, hành động theo lệnh tư pháp, đã chặn liên lạc bằng âm thanh diễn ra bên trong ngôi nhà ở Boston. Ví dụ cuối cùng, trong hoặc khoảng tháng 3 năm 2010, Foley và Heathfield đã được nghe thảo luận về việc Foley sử dụng kỹ thuật in mật mã và lịch trình liên lạc của cô ấy với Trung tâm Moscow ”

( [Hợp chủng quốc Hoa Kỳ kiện Christopher R. Metsos , 2010](#38__United_States_of_America_v) )

## Phá hủy dữ liệu

Đôi khi, việc ẩn dữ liệu là không đủ và thay vào đó, thủ phạm cố gắng phá hủy dữ liệu. Trên thực tế, việc phá hủy dữ liệu phức tạp hơn một chút so với suy nghĩ của nhiều người. Người chưa khởi tạo có thể chỉ cần nhấn phím xóa, giả sử rằng dữ liệu không còn tồn tại. Như chúng ta đã thấy, cách tiếp cận này không hiệu quả vì dữ liệu “đã xóa” vẫn còn trên phương tiện và dễ dàng được khôi phục. Ngược lại, nhiều công cụ xóa ổ đĩa có thể rất hiệu quả. Việc sử dụng các tiện ích như thế này có thể để lại dấu hiệu rõ ràng về việc sử dụng chúng, cung cấp bằng chứng đáng kể ngay cả khi không có dữ liệu gốc được đề cập.

Việc phá hủy dữ liệu có thể được thực hiện hoặc cố gắng theo một số cách. Một số người trong số họ tốt hơn những người khác. Phần mềm xóa ổ đĩa có sẵn trên thị trường và có thể hiệu quả trong việc tiêu hủy bằng chứng tiềm năng. Phần lớn hiệu quả của nó phụ thuộc vào chất lượng của phần mềm, cách nó được sử dụng và số lượng "khăn lau" được thực hiện. Việc chống phân mảnh hoặc định dạng lại ổ đĩa thường được cố gắng, nhưng thường mang lại kết quả hạn chế.

### 5.1 Drive Wiping

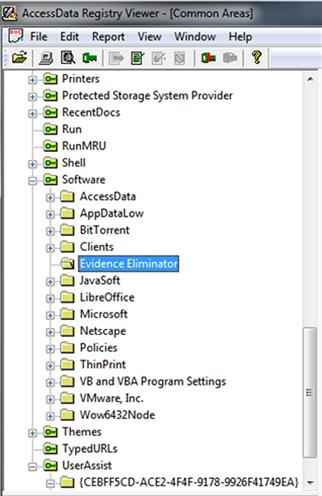
Tiện ích xóa ổ đĩa được sử dụng để ghi đè dữ liệu trên ổ cứng theo cách khiến chúng không thể khôi phục được. Hầu hết các ứng dụng này được quảng bá và / hoặc nhằm mục đích giữ bí mật thông tin cá nhân hoặc công ty. Quả thật cả hai đều là những nguyên nhân cao cả. Thật không may, những tiện ích tương tự này có thể được sử dụng cho các mục đích khác, ít danh dự hơn. Ví dụ về các công cụ này bao gồm “Darik's Boot và Nuke,” “DiskWipe”, “CBL Data Shredder”, “Webroot Window Washer” và “Evidence E Remo”.

Sử dụng những công cụ này không phải là một mệnh đề “tất cả hoặc không”. Chúng có thể hơi phẫu thuật trong ứng dụng của chúng, chỉ xóa các tệp được chỉ định trong khi để các tệp khác không bị ảnh hưởng. Ví dụ: các tệp hệ điều hành có thể được giữ nguyên. Chúng có thể nhắm mục tiêu các tệp và thư mục cụ thể cũng như các giá trị hệ thống có khả năng buộc tội như những giá trị được tìm thấy trong Windows Registry.

Những công cụ này có mục đích sử dụng hợp pháp và có sẵn tại nhiều cửa hàng công nghệ như Best Buy. Quyền riêng tư là mối quan tâm chính của mọi người và các tiện ích xóa có thể giúp ích. Nếu chúng ta muốn tặng máy tính cũ của mình, chúng ta chắc chắn không muốn các e-mail và thông tin cá nhân khác của chúng ta đi cùng với nó cho Goodwill.

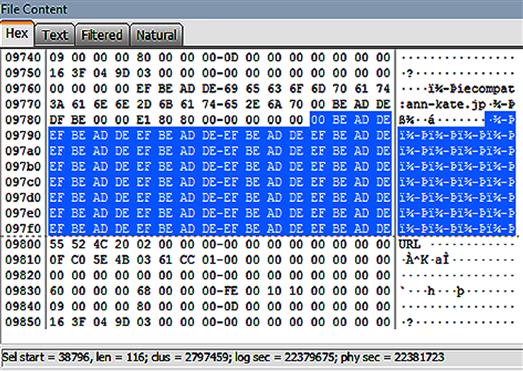
Việc sử dụng các công cụ này không có gì đảm bảo rằng dữ liệu không thể được khôi phục. Thành công phụ thuộc phần lớn vào chất lượng của công cụ và kỹ năng của người dùng.

Từ góc độ chứng minh hoặc điều tra, sự hiện diện hoặc sử dụng các ứng dụng này có thể là điều tốt nhất tiếp theo đối với bằng chứng ban đầu. Những kẻ tình nghi có thể khó giải thích tại sao phần mềm “Trình loại bỏ Chứng cứ” lại được cài đặt và chạy trên máy tính của họ vào ngày trước khi máy tính của họ được khám xét. [Hình 6.4](#F0025_3) cho thấy mục nhập cho “Trình loại bỏ bằng chứng” trong khóa phần mềm trong Windows Registry. Đây là chỉ báo cho biết phần mềm này đã được cài đặt trên máy.



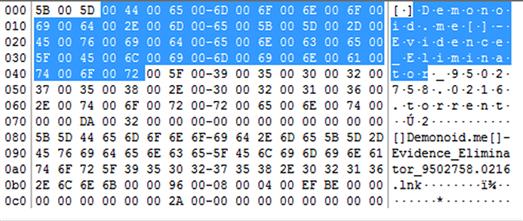
Hình 6.4 Lưu ý sự hiện diện của “Trình loại bỏ bằng chứng” trong khóa phần mềm Windows Registry.

Việc xóa các tiện ích có thể để lại dấu hiệu rõ ràng về việc sử dụng chúng. Khi nhìn vào ổ đĩa ở mức bit, có thể thấy một mẫu dữ liệu lặp lại khác biệt. Điều này hoàn toàn khác với những gì thường thấy trên ổ cứng khi sử dụng hàng ngày. (Xem [Hình 6.5](#F0030_2) .)



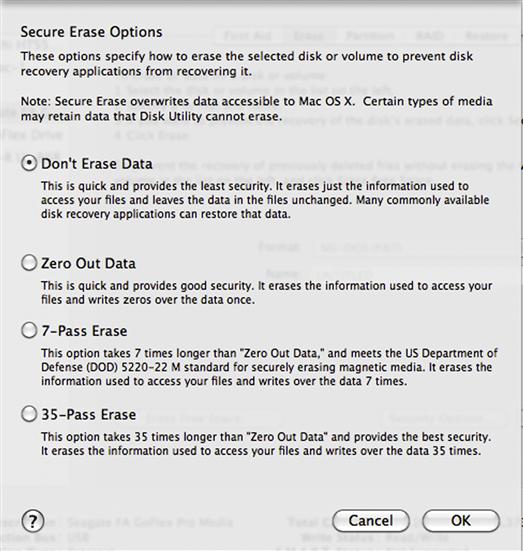
Hình 6.5 Lưu ý mô hình lặp lại riêng biệt của các số thập lục phân. Mẫu này không bình thường và có thể là dấu hiệu cho thấy một tiện ích lau đã được sử dụng.

Bằng chứng về việc sử dụng chúng có thể được tìm thấy ở những nơi khác trên ổ đĩa. [Hình 6.6](#F0035_1) cho thấy các dấu hiệu của Trình loại bỏ bằng chứng đang được mở trên máy đó.



Hình 6.6 Cho thấy các dấu hiệu trong MRU rằng Chương trình Loại bỏ Bằng chứng đã được mở trên máy này.

Một số hệ điều hành, chẳng hạn như Apple OSX Lion, được cài đặt tiện ích xóa ổ đĩa. Được gọi là Xóa bảo mật, tiện ích này cung cấp nhiều tùy chọn để hủy dữ liệu. (Xem [Hình 6.7](#F0040_1) .)



Hình 6.7 Các tùy chọn Xóa An toàn từ Apple OS X. Lưu ý đến dãy tùy chọn, đặc biệt là số lần truyền dữ liệu.

Nâng cao hơn

Chống phân mảnh như Kỹ thuật Chống Phân mảnh

Chống phân mảnh hay “Chống phân mảnh” như thường được gọi là thường được thực hiện để cải thiện hiệu suất máy tính. Chống phân mảnh là quá trình di chuyển các cụm càng gần nhau càng tốt để tăng tốc hệ thống. Quy trình này liên quan đến việc di chuyển dữ liệu từ vị trí này trên ổ đĩa sang vị trí khác. Do đó, dữ liệu có thể bị ghi đè trong quá trình này. Những dữ liệu bị ghi đè (bị phá hủy) này có thể có một số giá trị bằng chứng.

Quá trình chống phân mảnh có thể xảy ra theo ba cách; nó có thể do người dùng lập lịch, do người dùng khởi tạo thủ công hoặc được thực hiện tự động bởi hệ điều hành ( [Casey, 2009](#8__Casey_E__Handbook_of_Digital) ).

Có một số cách khác nhau mà bạn có thể thử để xác định xem ổ đĩa đã được chống phân mảnh gần đây hay chưa. Một cách là khởi động hình ảnh ổ đĩa trong Windows và xem số lượng tệp bị phân mảnh. Các ổ đĩa được sử dụng thường xuyên thường cho thấy một lượng lớn tệp bị phân mảnh. Các ổ đĩa hiển thị khác, không có lời giải thích hợp lý, sẽ bị nghi ngờ.

Hỏi & Đáp Với Nephi Allred, Nhà phân tích mật mã với AccessData, Nhà sản xuất Bộ công cụ khôi phục mật khẩu (PRTK)

Bây giờ, rõ ràng là mã hóa là một mối quan tâm lớn đối với cộng đồng pháp y kỹ thuật số. Như vậy, chúng ta phải chuẩn bị để đối phó với dữ liệu được mã hóa. Các công cụ giải mã là một trong những vũ khí mà chúng ta có thể mang theo để chiến đấu. Một trong những công cụ giải mã hàng đầu trên thị trường là Bộ công cụ khôi phục mật khẩu (PRTK) từ AccessData. Trong phần Hỏi & Đáp bên dưới, chúng ta sẽ xem xét kỹ hơn bên trong PRTK và mã hóa mà nó nhằm mục đích phá vỡ. PRTK được sử dụng rộng rãi trên toàn thế giới bởi các cơ quan thực thi pháp luật, cơ quan tình báo và các tập đoàn tư nhân như các tổ chức tài chính lớn. Người dùng Hoa Kỳ bao gồm FBI, CIA và Mật vụ, chỉ để nêu tên một số.

[Q] PRTK đoán bao nhiêu mật khẩu mỗi giây trên một máy "tiêu chuẩn"?

[A] Allred: Chúng ta nhận được câu hỏi này rất nhiều. Không thể trả lời đúng như hiện tượng của nó bởi vì bản thân câu hỏi đã có một giả định ngầm, điều này là sai. Cụ thể: tất cả các lược đồ mật khẩu không giống nhau. Nó hơi giống như hỏi động vật có thể đi nhanh như thế nào. Con vật nào? Mỗi chương trình hoặc ứng dụng hoặc hệ thống khác sử dụng mật khẩu đều thực hiện theo cách khác nhau. Cách họ làm điều đó tạo nên sự khác biệt trên thế giới về mức độ tính toán cần thiết để điều tra mật khẩu.  Ví dụ: một máy “thông thường” có thể đoán hai triệu mật khẩu mỗi giây cố gắng bẻ khóa tệp Office 97, trong khi máy tương tự có thể chỉ đoán năm trăm mật khẩu mỗi giây bẻ khóa tệp Office 2010.   
Và tất nhiên câu trả lời cũng phụ thuộc vào ý bạn muốn nói về một cỗ máy “điển hình” (và điều đó cũng thay đổi theo thời gian).

[Q] PRTK đoán mật khẩu theo thứ tự nhất định để cải thiện tốc độ và hiệu quả. Bạn có thể nói một chút về cách thức hoạt động và tại sao nó lại quan trọng không?

[A] Allred: Không phải tất cả các mật khẩu đều được tạo như nhau. Trong không gian của tất cả các mật khẩu có thể có, một số có nhiều khả năng được con người sử dụng hơn những mật khẩu khác. (Ví dụ: “Br1tn3y” có nhiều khả năng được sử dụng hơn “H \* i3} -aV.K = TyG7”). Vì vậy, nếu bạn đang cố gắng đoán mật khẩu, trung bình bạn sẽ nhanh hơn và thành công hơn nếu bạn đoán được nhiều mật khẩu có khả năng xảy ra hơn.

Tất nhiên mật khẩu nào có khả năng xảy ra cao hơn không phải lúc nào cũng dễ xác định, và chắc chắn là khác nhau ở mỗi người. PRTK xác định thứ tự mặc định của mật khẩu mà chúng ta đã cố gắng tạo ra hiệu quả nhất có thể, dựa trên những gì đã biết về cách mọi người có xu hướng chọn mật khẩu. Nhưng một điều tra viên thường có kiến thức cụ thể về kẻ tình nghi và có thể sử dụng kiến thức đó để làm cho việc đặt hàng mật khẩu phù hợp hơn với cá nhân đó. Đây là lý do tại sao PRTK cung cấp cho người dùng rất nhiều tùy chỉnh không gian mật khẩu. Ví dụ: thay vì chọn mặc định, bạn có thể chỉ định rằng công việc trước tiên hãy thử tất cả các mật khẩu trong từ điển (có thể tùy chỉnh), sau đó tất cả các từ đó theo thứ tự ngược lại, sau đó tất cả các từ đó với “123”, “4eva "Hoặc" asdf "được thêm vào. Và nhiều hơn nữa.

[Q] Tôi biết rằng PRTK cũng dựa trên các mẫu mật khẩu được xác định (gốc và phần phụ). Những cái đó dựa trên cái gì và nó hoạt động như thế nào?

[A] Allred: Dựa trên các danh sách mật khẩu khác nhau mà chúng ta đã có được trong nhiều năm (một số từ khách hàng của chúng ta, một số khác có sẵn miễn phí), chúng ta đã cố gắng tạo ra các “quy tắc” mật khẩu để tạo ra các mật khẩu mà mọi người thực sự sử dụng trong cuộc sống thực . Tại thời điểm này, đây vẫn là một nghệ thuật hơn là một khoa học. Có nghĩa là, không có phân tích thống kê sâu nào đang diễn ra - hầu hết chúng ta nhắm vào danh sách và tìm kiếm các mẫu. Ví dụ: rất nhiều mật khẩu dường như kết thúc bằng “1”. Vì vậy, một trong những quy tắc mật khẩu của chúng ta là “Từ điển theo sau là các hậu tố phổ biến” (và “1” là một trong những hậu tố phổ biến đó).

[Q] Bạn có biết PRTK hiệu quả như thế nào trong việc phá mật khẩu không?

[A] Allred: Một lần nữa, điều này rất khác nhau đối với các loại tệp và nghi phạm. Tôi không có bất kỳ số nào cho bạn, rất tiếc. Bạn có thể nên nói chuyện với những người sử dụng PRTK (hoặc DNA) trong các trường hợp thực tế.   
Cần lưu ý rằng không phải tất cả các cuộc tấn công mà PRTK thực hiện đều là các cuộc tấn công đoán mật khẩu. Một số hệ thống tiền điện tử có các lỗ hổng cho phép mật khẩu của họ được khôi phục ngay lập tức mà không liên quan đến "phỏng đoán". Ví dụ, PRTK có thể khôi phục ngay mật khẩu chính trên trình quản lý mật khẩu “Whisper32”. Điều này không phải là hiếm trong các ứng dụng một thập kỷ trước, nhưng ngày nay nó trở nên hiếm hơn nhiều khi các nhà phát triển phần mềm trở nên hiểu biết hơn về tiền điện tử.

[Q] Có điều gì làm chậm quá trình giải mã không? Bạn có thể nói về điều đó và tại sao lại như vậy?

[A] Allred: Vâng, có. Ngày nay, hầu hết các nhà phát triển ứng dụng sử dụng mật khẩu đều biết đến các công cụ như PRTK và họ sẽ sử dụng các biện pháp để làm chậm các cuộc tấn công đoán mật khẩu. Như tôi đã giải thích ở phần 1, tốc độ chúng ta có thể đoán mật khẩu phụ thuộc vào cách ứng dụng sử dụng mật khẩu.   
Một ứng dụng có thể cố tình chọn một phương pháp chuyển mật khẩu thành khóa rất chậm. Chẳng hạn, nó có thể băm mật khẩu mười nghìn lần thay vì chỉ một, trong khi chuyển mật khẩu thành khóa. (Đây là một sự đơn giản hóa, nhưng bạn có được ý tưởng). Điều này buộc công cụ đoán mật khẩu cũng phải băm mật khẩu mười nghìn lần cho mỗi lần đoán mật khẩu, dẫn đến ít mật khẩu hơn mỗi giây.

[Q] Mã hóa thay đổi như thế nào? Bạn thấy “điều lớn” tiếp theo trong mật mã là gì? Bạn thấy những thách thức nào ở phía trước?

[A] Allred: Mật mã học là một chủ đề lớn, và tôi hầu như không phải là chuyên gia trong bất kỳ khía cạnh nào của nghiên cứu mới. Nhưng trong lĩnh vực mã hóa dựa trên mật khẩu, mọi thứ đang thay đổi.   
Đó không hẳn là một cái nhìn sâu sắc mới, nhưng mọi người ngày càng nhận ra rằng mật khẩu như một thiết bị bảo mật thường không đủ. Những gì chúng ta sẽ sử dụng thay vì chúng (hoặc, nhiều khả năng hơn, ngoài chúng) vẫn chưa hoàn toàn rõ ràng, nhưng các nhà cung cấp mã hóa đang thử những điều mới.   
Ví dụ: một số ứng dụng, như TrueCrypt, cho phép người dùng nâng cao mật khẩu của họ bằng “tệp khóa”. Tệp khóa có thể là bất kỳ tệp nào và nó được sử dụng để xáo trộn mật khẩu trước khi sử dụng. Điều này có nghĩa là để thực hiện một cuộc tấn công đoán mật khẩu thành công, PRTK cần phải sử dụng bất kỳ và tất cả các tệp chính. Điều tra viên có thể không dễ dàng tìm ra những tệp chính nào đã được sử dụng, nếu có.

## 6. Bản tóm tắt

Các công cụ và kỹ thuật chống pháp y có thể có tác động đáng kể đến việc điều tra pháp y đối với máy tính. Để làm thất vọng các điều tra viên, 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 mã hóa, nó có thể bị tấn công theo nhiều cách khác nhau. Trong một cuộc Bruteforce, 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 ta đặt lại mật khẩu theo một trong những lựa chọn của chúng ta.

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 là xa vời. Dữ liệu phân biệt đối xử 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.

## 7. Tổng kết và kiến thức thêm chương 6

1. **Định nghĩa kỹ thuật chống lại điều tra số và mục tiêu của các kỹ thuật này**

Kỹ thuật chống lại điều tra số là một chuỗi hành động, phương pháp để che giấu, thay đổi, mã hóa thông tin nhằm giảm thiểu các bằng chứng số liên quan đến sự kiện

Mục tiêu chống lại điêu tra số:

\_ Gây gián đoạn, chống lại quá trình thu thập thông tin

\_ Yêu cầu cao trình độ, kỹ thuật để thu thập thông tin

\_ Che dấu các dấu vết thu thập

\_ Gây ảnh hưởng đến tính chính xác của bản báo cáo, bằng chứng

1. **Hiểu được các phương pháp chống lại điều tra số**
2. Xóa tệp tin
3. Bảo vệ tệp tin bằng mật khảu
4. Dấu tệp tin
5. Trail Obfuscation (Nhiễu loạn thông tin)
6. Artfact Wiping (xóa mảnh)
7. Overwriting Data (ghi đè thông tin)
8. Mã hóa
9. Mã hóa mạng
10. Program Packers
11. Rootkits
12. **Công cụ khôi phục dữ liệu bị xóa, lỗi**

Recover My Files (Khôi phục tệp tin, vùng lưu trữ bị xóa) dành cho Windows

Mac Data Recovery (Khôi phục tệp tin, vùng lưu trữ bị xóa) dành cho MAC OSX

TestDisk (Khôi phục tệp tin, vùng lưu trữ bị xóa) dành cho Linux

1. **Các phương pháp chống lại điều tra số môi trường vật lý, lưu trữ offline như trail obfuscation, artifact wiping, data/metadata overwriting, and encryption**
2. Trail obfuscation:

\_ Mục tiêu: Gây nhiễu loạn thông tin và quá trình điều tra

\_ Kỹ thuật: Xóa logs, Spoofing, Giả thông tin, Tài khoản giả, lệnh từ Trojan, VPN và SSH tunneling

1. Artifact wiping:

* Mục tiêu: Xóa toàn bộ dữ liệu kể cả các tệp tin hệ thống
* Kỹ thuật: Chình sửa lại toàn bộ ổ đĩa, Xóa tệp tin hệ thống, tiêu hủy dữ liệu trong ổ cứng qua sóng, nam châm

1. Data/Metadata Overwriting

* Mục tiêu: Ghi đè lên tệp tin nhằm xóa dấu vết hoặc gây khó khăn cho việc truy vết
* Kỹ thuật: Truy cập vào tập tin nhằm nhiễu loạn thời gian truy cập, thay đổi trạng thái vùng dữ liệu.

1. Encryption

* Mục tiêu: Mã hóa dữ liệu
* Kỹ thuật: sử dụng các công cụ như BitLocker, EFS, cũng như encode và decode.

1. **Các phương pháp chống lại điều tra số môi trường mạng, online như encrypted protocols, program packers, rootkits.**
2. Encrypted Network Protocol

* Mục tiêu: mã hóa dữ liệu mạng nhằm tránh bị truy vết
* Kỹ thuật: Sử dụng SSL/TLS và SSH nhằm tránh bị lộ thông tin cũng như mã hóa đường truyền.

1. Program Packers

* Mục tiêu: Che dấu các công cụ được dùng để xóa dấu vết
* Kỹ thuật: Nén hoặc mã hóa các công cụ được sử dụng

1. Rootkits

* Mục tiêu: Che giấu dữ liệu bằng phương pháp giả danh
* Kỹ thuật: Sử dụng các công cụ để làm giả thông tin sống cũng như là giả dạng thành các ứng dụng hệ thống hoặc đáng tin cậy.

1. **Cách nhân viên điều tra chống lại các phương pháp chống điều tra**
2. Luôn luôn tìm hiểu về các kỹ thuật mới
3. Kiểm tra lại kết quả bằng nhiều phương pháp
4. Hiểu được điểm yếu của các phương pháp chống điều tra
5. Chỉ sử dụng các công cụ được update cũng như kiểm tra
6. Lưu bằng chứng tách biệt với khu vực điều tra, hệ thống điều tra
7. Luôn luôn sẵn sàng phương pháp sao y, sao lưu cũng như lên kế hoạch điều tra để tránh kích hoạt sự kiện có khả năng kích hoạt mã độc chứa trong vật chứng
8. **Hiểu được các khó khăn khi đối mặt với các phương pháp chống điều tra**
9. Các phương pháp chống lại các phương pháp chống điều tra yêu cầu có kĩ năng, trình độ cao cũng như kinh nghiệm nhằm đảm báo tính chính xác của bằng chứng
10. Không có quy tắc, quy trình cụ thể khi chống lại những phương pháp này
11. Yêu cầu điều tra viên hiểu rõ các điểm yếu của phương pháp chống điều tra

Tài liệu tham khảo

1. Cộng đồng AntiForensics. (nd). Giới thiệu về AntiForensics: AntiForenics . Truy cập ngày 13 tháng 5 năm 2011, từ: <http://www.antiforensics.com/>.

2. Apple, Inc. OS X Lion: Giới thiệu về FileVault . 2011; 2 Truy cập ngày 14 tháng 8 năm 2011, từ: <http://support.apple.com/kb/HT4790> ; 2011.

3. Bảo mật đường trục.com. Cơ sở dữ liệu kỹ thuật số Steganography của Backbone vượt quá 925 ứng dụng năm 2011; Truy cập ngày 14 tháng 8 năm 2011, từ: <http://www.sarc-wv.com/news/press_releases/2011/safdb_v39.aspx> ; 2011.

4. Barbara, J. (2008, ngày 01 tháng 12). Pháp y chống kỹ thuật số, Thử thách tiếp theo: Phần 1 . Truy cập ngày 15 tháng 8 năm 2011, từ: <http://www.forensicmag.com/article/anti-digital-forensics-next-challenge-part-1>.

5. Bauchie R, Hazen F, Lund J, Oakley G, Rundatz F. Mã hóa 2000; Truy cập ngày 17 tháng 8 năm 2011, từ: <http://searchsecurity.techtarget.com/definition/encryption> ; 2000.

6. Berghel H. Ẩn Dữ liệu, Pháp y và Chống pháp y. Thông báo của ACM 2007;: 15–20.

7. Caproni V. Going Dark: Giám sát điện tử hợp pháp khi đối mặt với công nghệ mới 2011; Truy cập ngày 15 tháng 8 năm 2011, từ: <http://www.fbi.gov/news/testimony/going-dark-lawful-electronic-surveillance-in-the-face-of-new-technologies> ; 2011.

8. Casey E. Sổ tay Điều tra và Pháp y Kỹ thuật số Burlington, MA: Academic Press; Năm 2009.

9. Casey E. Bằng chứng kỹ thuật số và tội phạm máy tính, xuất bản lần thứ 3: Khoa học pháp y, Máy tính và Internet Waltham, MA: Academic Press; 2011.

10. Tin tức CBS. FBI: 10 điệp viên Nga bị bắt tại Mỹ năm 2010; Truy cập ngày 11 tháng 9 năm 2011, từ: <http://www.cbsnews.com/stories/2010/06/28/world/main6627393.shtml> ; Năm 2010.

11. Dick, Ronald L. Vấn đề xâm nhập vào mạng máy tính của chính phủ 2001; Truy cập ngày 14 tháng 8 năm 2011, từ: [http://www.fbi.gov/news/testimony/issue-of-intrusions-into-go Government-computer-networks](http://www.fbi.gov/news/testimony/issue-of-intrusions-into-government-computer-networks) ; Năm 2001.

12. Công ty TNHH Elcomsoft (nd). Phần mềm Hệ thống & Bảo mật . Truy cập ngày 27 tháng 8 năm 2011, từ: <http://www.elcomsoft.com/esr.html#forgot%20administrator%20password>.

13. Geiger M. Đánh giá phần mềm pháp y thương mại . DFRWS 2005; New Orleans.

14. Gupta MR, Hoeschele MD, Rogers MK. Vùng đĩa ẩn: HPA và DCO. Tạp chí Quốc tế về Bằng chứng Kỹ thuật số 2006;: 1–8.

15. Trang tin An ninh Nội địa. Feds buộc phải sáng tạo để vượt qua mã hóa 2011; Truy cập ngày 14 tháng 8 năm 2011, từ: <http://www.homelandsecuritynewswire.com/feds-forced-get-creative-bypass-encryption> ; 2011.

16. HowStuffWorks, Inc. (nd). Thuật toán máy tính là gì? Truy cập ngày 17 tháng 8 năm 2011, từ: <http://computer.howstuffworks.com/question717.htm>.

17. Kelley J. Hướng dẫn Khủng bố Trực tuyến 2005; Truy cập ngày 14 tháng 8 năm 2011, từ: <http://www.usatoday.com/life/cyber/tech/2001-02-05-binladen-side.htm> ; Năm 2005.

18. Tập đoàn Microsoft. (nd). Tổng quan về mã hóa ổ đĩa BitLocker . Truy cập ngày 20 tháng 6 năm 2011, từ: <http://windows.microsoft.com/en-US/windows-vista/BitLocker-Drive-Encryption-Overview>.

19. Tập đoàn Microsoft. (nd). So sánh Windows . Được truy cập ngày 20 tháng 6 năm 2011, từ: <http://windows.microsoft.com/en-US/windows7/products/compare>.

20. Tập đoàn Microsoft. (nd). Tạo mật khẩu mạnh . Được truy cập ngày 13 tháng 8 năm 2011, từ: <http://www.microsoft.com/security/online-privacy/passwords-create.aspx>.

21. Tập đoàn Microsoft. (nd). Hệ thống tệp mã hóa . Truy cập ngày 11 tháng 9 năm 2011, từ: <http://technet.microsoft.com/en-us/library/cc700811.aspx>.

22. Tập đoàn Microsoft. (nd). Công nghệ độc đáo dành cho khách hàng doanh nghiệp . Được truy cập ngày 27 tháng 8 năm 2011, từ: <http://www.microsoft.com/windows/enterprise/products/windows-7/features.aspx#bitlocker>.

23. Tập đoàn Microsoft. (nd). Hệ thống tệp mã hóa (EFS) là gì? Truy cập ngày 20 tháng 6 năm 2011, từ: <http://windows.microsoft.com/en-US/windows7/What-is-Encrypting-File-System-EFS>.

24. Tập đoàn Microsoft. (nd). Hướng dẫn từng bước về mã hóa ổ đĩa Windows BitLocker: Microsoft Corporation . Được truy cập ngày 13 tháng 5 năm 2011, từ: <http://technet.microsoft.com/en-us/library/cc766295%28WS.10%29.aspx>.

25. Tập đoàn Microsoft. Mã hóa ổ đĩa Windows BitLocker Câu hỏi thường gặp 2009; Được truy cập ngày 18 tháng 8 năm 2011, từ: [http://technet.microsoft.com/enus/library/cc766200%28WS.10%29.aspx#BKMK\_EntireDisk Microsoft](http://technet.microsoft.com/enus/library/cc766200%28WS.10%29.aspx#BKMK_EntireDiskMicrosoft) ; Năm 2009.

26. Quỹ Mozilla. (nd). Duyệt web riêng tư . Được truy cập ngày 27 tháng 8 năm 2011, từ: <http://support.mozilla.com/enUS/kb/Private%20Browsing#w_what-does-private-browsing-not-save>.

27. Phillip A, Cowen D, Davis C. Hacking Exposed Computer Forensics: Computer Forensics Secrets & Solutions New York: McGraw-Hill; Năm 2009.

28. Rogers M. Chống Pháp y . Lockheed Martin 2005; Thành phố San Diego.

29. Schneier B. Bản tin Crypto-Gram 2002; Truy cập ngày 20 tháng 6 năm 2011, từ: <http://www.schneier.com/crypto-gram-0205.html#1> ; Năm 2002.

30. Schneier B. Mật khẩu Bảo mật Giúp Bạn An toàn hơn 2007, ngày 15 tháng 1; Truy cập ngày 25 tháng 8 năm 2011, từ: <http://www.schneier.com/essay-148.html> ; 2007, ngày 15 tháng 1.

31. Strickland, J. (nd). How Stuff Works: Cách hoạt động của máy tính pháp y . Truy cập ngày 13 tháng 5 năm 2011, từ: <http://computer.howstuffworks.com/computer-forensic3.htm>.

32. Tổng công ty Symantec. (nd). Sản phẩm mã hóa PGP . Truy cập ngày 13 tháng 5 năm 2011, từ: <http://www.symantec.com/business/theme.jsp?themeid=pgp>.

33. Tập đoàn Symantec. (nd). Mã hóa toàn bộ đĩa: Symantec Corporation . Truy cập ngày 13 tháng 5 năm 2011, từ: <http://www.symantec.com/business/whole-disk-encryption>.

34. TechTarget. Steganography 2000; Truy cập ngày 15 tháng 8 năm 2011, từ: <http://searchsecurity.techtarget.com/definition/steganography> ; 2000.

35. Hiệp hội các nhà phát triển TrueCrypt. Mã hóa hệ thống 2011; Truy cập ngày 14 tháng 8 năm 2011, từ: <http://www.truecrypt.org/docs/?s=version-history> ; 2011.

36. Hiệp hội các nhà phát triển TrueCrypt. (nd). Tài liệu: Hiệp hội các nhà phát triển TrueCrypt . Truy cập ngày 13 tháng 5 năm 2011, từ: <http://www.truecrypt.org/docs/>.

37. Tyma P. Encryption, Hashing và Obfuscation 2003; Truy cập ngày 20 tháng 6 năm 2011, từ: <http://www.zdnet.com/news/encryption-hashing-and-obfuscation/128604> ; 2003.

38. Hợp Chủng Quốc Hoa Kỳ kiện Christopher R. Metsos, et al . (2010, ngày 1 tháng 6). Quận phía Nam, New York.

39. Vijayan J. Công cụ mã hóa cập nhật cho những người ủng hộ al-Qaeda Cải tiến trên phiên bản đầu tiên, Nhà nghiên cứu nói: Computerworld 2008; Được truy cập ngày 13 tháng 5 năm 2011, từ: <http://www.computerworld.com/s/article/9060939/Updated_encryption_tool_for_al_Qaeda_backers_improves_on_first_version_researcher_says> ; Năm 2008.

40. Wawro A. Chính phủ Hoa Kỳ Sử dụng PS3 để bẻ khóa mã hóa, bắt kẻ ấu dâm 2009; Truy cập ngày 17 tháng 8 năm 2011, từ: [http://www.computerworlduk.com/news/security/17680/us-go Government-using-ps3s-to-crack-encryption-catch-paedophiles /](http://www.computerworlduk.com/news/security/17680/us-government-using-ps3s-to-crack-encryption-catch-paedophiles/) ; Năm 2009.

41. Wetstone Technologies, Inc. (nd). Stego Suite ™ - Khám phá điều ẩn giấu . Truy cập ngày 18 tháng 8 năm 2011, từ: <http://www.wetstonetech.com/product/stego-suite/>.

42. Là gì [Anti-Forensics.com](http://Anti-Forensics.com) ? (nd). Truy cập ngày 14 tháng 8 năm 2011, từ: <http://www.anti-forensics.com/about-anti-forensics>.

# Chương 7: Tư pháp quyền riêng tư (tham khảo tư pháp Hoa Kỳ và thế giới)

**Thông tin trong Chương này:**

Các khía cạnh pháp lý của pháp y kỹ thuật số



Tu chính án thứ tư và tác động của nó đối với pháp y kỹ thuật số



Khám phá điện tử



Nhiệm vụ bảo tồn bằng chứng kỹ thuật số tiềm năng trong các vụ án dân sự



Tìm kiếm riêng tư và thiết lập nhu cầu phân tích ngoài địa điểm



Tổng quan về Đạo luật Bảo mật Truyền thông Điện tử



Tìm kiếm bằng chứng kỹ thuật số có và không có lệnh khám xet tìm kiếm



Cơ quan tìm kiếm pháp lý là bước đầu tiên trong quy trình pháp y kỹ thuật số. Điều này đúng cho cả vụ án dân sự và hình sự. Chương này đóng vai trò là phần giới thiệu về tìm kiếm và thu giữ, khám phá điện tử và Đạo luật Truyền thông Lưu trữ.

Nguyên nhân có thể xảy ra, Khám phá điện tử (eDiscovery), Thông tin được lưu trữ điện tử (ESI), Spoliation, Đạo luật truyền thông được lưu trữ (SCA), Sự đồng ý, Các bên thứ ba, Hoàn cảnh khó khăn, Học thuyết chế độ xem đơn giản, Dịch vụ tính toán từ xa (RCS), Nhiệm vụ bảo quản, Lấy mẫu dữ liệu , United States v. Frye, Daubert v. Merrell Dow Pharmaceuticals

## Giới thiệu

Không có cuộc thảo luận nào về các nguyên tắc cơ bản của pháp y kỹ thuật số có thể hoàn chỉnh mà không bao gồm các khía cạnh pháp lý của ngành. Cộng đồng pháp lý đã chơi trò chơi bắt kịp công nghệ vĩnh viễn ngay từ những ngày đầu tiên. Với việc máy tính và các công nghệ khác trở nên gắn bó với nhau trong công việc và cuộc sống riêng tư của chúng ta, việc dữ liệu điện tử tìm được đường vào tòa án là điều không thể tránh khỏi. Đó không chỉ là những kẻ “đen” và những kẻ trộm danh tính; bằng chứng kỹ thuật số cũng đóng một vai trò rất lớn trong tranh tụng dân sự.

Với những công nghệ mới này đã tạo ra những hành vi tội phạm mới đòi hỏi phải có những đạo luật mới để đặt chúng ra ngoài vòng pháp luật. Một số trong số này chỉ đơn giản là những tội ác cũ với một bước ngoặt mới. Trong trường hợp này, công nghệ chỉ tạo điều kiện cho tội phạm theo cách cập nhật và hiệu quả hơn.

Cơ quan tìm kiếm là bước đầu tiên trong quy trình pháp y kỹ thuật số. Bản thân cơ quan có thể có nhiều hình thức, tùy thuộc vào địa điểm bạn đang làm việc vào thời điểm đó.

Cho dù đó là một vụ án dân sự hay hình sự, có thẩm quyền khám xét hợp lệ là một yêu cầu. Trên thực tế, đó là bước đầu tiên trong quy trình pháp y kỹ thuật số. Trong chương này, chúng ta sẽ xem xét các vấn đề pháp lý cơ bản trong cả tố tụng hình sự và dân sự.

## Tu chính án thứ tư

Tu chính án thứ tư đóng vai trò là “phép thử quỳ” cho tất cả các cuộc khám xét và tịch thu của chính phủ. Bất kỳ bằng chứng nào được cho là bị thu giữ vi phạm Tu chính án thứ tư đều không được chấp nhận trước tòa án. Người Mỹ từ lâu đã chán ghét việc chính phủ xâm nhập vào cuộc sống riêng tư của họ. Trước Cách mạng Hoa Kỳ, binh lính Anh hoạt động dưới sự hỗ trợ của Writs, thường xuyên xâm nhập vào nhà của người dân một cách vô cớ. Tu chính án thứ tư đối với Hiến pháp đã được soạn thảo với tâm trí phản bội này. Tu chính án thứ tư nói: “Quyền của người dân được lệnh khám xet về con người, nhà cửa, giấy tờ và các tác dụng của họ, chống lại việc khám xét và thu giữ bất hợp lý, sẽ không bị vi phạm và sẽ không có Trát nào được đưa ra, nhưng nếu có nguyên nhân có thể xảy ra , được hỗ trợ bởi Lời thề hoặc khẳng định, và đặc biệt là mô tả địa điểm sẽ được khám xét, và những người hoặc những thứ sẽ bị thu giữ ”(FindLaw).

## Luật hình sự — Tìm kiếm mà không cần lệnh khám xét

Có hai câu hỏi chính phải được trả lời ngay từ đầu. Đầu tiên, chính phủ đã hành động? Thứ hai, hành động đó có vi phạm kỳ vọng hợp lý của cá nhân về quyền riêng tư không? Nếu câu trả lời cho câu hỏi đầu tiên là “không” thì Tu chính án thứ tư sẽ không áp dụng. Nó chỉ bao gồm các tìm kiếm của chính phủ (hoặc các đại lý của nó), không phải công dân tư nhân.

Đối với các mục đích của Tu chính án thứ tư, một người trở thành đại diện của chính phủ nếu họ đang hành động theo yêu cầu của cơ quan thực thi pháp luật. Theo kịch bản đó, sẽ không khác gì nếu cảnh sát tiến hành khám xét.

### 3.1 Kỳ vọng hợp lý về quyền riêng tư

Chính xác thì “kỳ vọng hợp lý về quyền riêng tư” là gì? Đó là một câu hỏi tuyệt vời không có câu trả lời dễ dàng. Không có quy tắc hoặc bài điều tra rõ ràng nào có thể giúp chúng ta xác định nó. Phần lớn các diễn giải tập trung vào những gì mà xã hội nói chung coi là hợp lý. Ví dụ, một người sẽ có kỳ vọng về quyền riêng tư trên máy tính cá nhân của họ nhiều hơn so với ở thư viện công cộng. Theo nguyên tắc chung, bạn có thể coi máy tính như một thùng chứa kín. Nếu viên chức không có thẩm quyền để mở ngăn bàn hoặc hộp, thì điều này cũng đúng với máy tính ( [Văn phòng Điều hành Luật sư Hoa Kỳ, 2009](#4__Executive_Office_for_United_S) ).

Nếu người đó có kỳ vọng hợp lý về quyền riêng tư, thì trước tiên chính phủ phải có được lệnh khám xét, hoặc việc khám xét sẽ phải đáp ứng một trong các trường hợp ngoại lệ được ghi nhận đối với yêu cầu về trát.

Còn các tệp riêng lẻ thì sao? Chúng có nên được xem như những thùng chứa riêng biệt, khép kín không? Có vẻ như các tòa án cũng không chắc chắn. Các phán quyết đã được truyền lại để hỗ trợ cả hai vị trí. Tại ( [United States v. Slanina, 2002](#18__United_States_v__Slanina__28) ), Fifth Circuit đã phán quyết rằng khi một cuộc tìm kiếm thích hợp được thực hiện trên một phần của đĩa, các bị cáo không còn có kỳ vọng hợp lý về quyền riêng tư liên quan đến các tệp khác.

Ngược lại, Tenth Circuit đưa ra lập trường ngược lại khi nói rằng “[b] vì máy tính có thể chứa rất nhiều thông tin liên quan đến nhiều lĩnh vực khác nhau trong cuộc sống của một người, nên càng có nhiều khả năng xảy ra việc 'trộn lẫn' các tài liệu và hậu quả là xâm phạm quyền riêng tư khi cảnh sát thực hiện tìm kiếm bằng chứng trên máy tính ”( [United States v. Walser, 2001](#19__United_States_v__Walser__275) ).

Thông tin mà một cá nhân cố ý tiết lộ cho người khác không được Bảo vệ bởi Tu chính án thứ tư. Ví dụ ở đây có thể bao gồm các máy tính công cộng như máy tính trong lớp học hoặc “bộ nhớ dùng chung” trên mạng ( [Văn phòng Điều hành Luật sư Hoa Kỳ, 2009](#4__Executive_Office_for_United_S) ).

### 3.2 Tìm kiếm Riêng tư

Các cuộc khám xét riêng tư không được bảo vệ bởi Tu chính án thứ tư trừ khi việc khám xét được thực hiện theo yêu cầu của chính phủ hoặc với sự hiểu biết hoặc sự tham gia của họ. Lấy ví dụ như Biệt đội Geek ở Best Buy. Giả sử ai đó cho phép họ làm việc trên máy tính ở nhà và trong quá trình đó, họ tìm thấy hình ảnh “đen” trên máy của họ. Những hình ảnh được tìm thấy bởi kỹ thuật viên sửa chữa sẽ được chấp nhận miễn là họ không tìm kiếm theo yêu cầu của chính phủ, do đó họ đóng vai trò là đại lý của họ.

### 3.3 E-mail

Nhìn chung, một cá nhân duy trì các biện pháp bảo vệ của Tu chính án thứ tư của họ khi một e-mail đang được truyền đi, nhưng sẽ mất các biện pháp bảo vệ đó khi nó đến đích cuối cùng. E-mail được xem theo cách tương tự như "thư ốc sên" thông thường. Việc đánh chặn hợp pháp e-mail của một cá nhân hoặc thông tin liên lạc điện tử khác là thứ được kiểm soát chặt chẽ. Được biết đến với tên gọi Đạo luật nghe lén, Tiêu đề III của Đạo luật kiểm soát tội phạm Omnibus và Đường phố an toàn năm 1968 nghiêm cấm theo dõi trái phép và liệt kê các thủ tục cần thiết để có được lệnh nghe lén ( [Bộ Tư pháp Hoa Kỳ, Văn phòng Chương trình Tư pháp, 2010](#16__U_S__Department_of_Justice) ).

### 3.4 Đạo luật về quyền riêng tư của truyền thông điện tử (ECPA)

Mục đích của ECPA là cấm bên thứ ba chặn và / hoặc tiết lộ thông tin liên lạc điện tử mà không có sự cho phép trước. Quy chế liên bang này ban đầu được thông qua vào năm 1968 như một sửa đổi cho Đạo luật nghe lén năm 1968. ECPA đã trải qua lần thay đổi đầu tiên vào năm 1994 khi nó được sửa đổi bởi Đạo luật Hỗ trợ Truyền thông để Thực thi Pháp luật, còn được gọi là CALEA. Nó đã được sửa đổi một lần nữa sau vụ tấn công 11/9 theo Đạo luật Yêu nước của Hoa Kỳ. Đạo luật Yêu nước được ủy quyền một lần nữa vào năm 2006 ( [TechTarget, 2005](#15__TechTarget__Electronic_Disco) ).

### 3.5 Các ngoại lệ đối với Yêu cầu Lệnh khám xet Tìm kiếm

Có một số trường hợp ngoại lệ nổi tiếng đối với yêu cầu về lệnh khám xét. Một cuộc khám xét không có lệnh khám xet có hiệu lực với sự đồng ý miễn là người đưa ra sự đồng ý được cho phép và sự đồng ý đó thực sự tự nguyện. Tính tự nguyện của sự đồng ý được đánh giá dựa trên tổng thể của các tình huống. Tòa án tối cao đã công nhận tuổi tác, trình độ học vấn, trí thông minh và tình trạng thể chất và tinh thần của người đưa ra sự đồng ý là những yếu tố quan trọng cần xem xét. Các cân nhắc khác sẽ là liệu người đó có bị bắt tại thời điểm đồng ý hay không và liệu người đó có được thông báo về quyền từ chối đồng ý hay không. Nếu tính hợp lệ của cuộc tìm kiếm dựa trên sự đồng ý, thì chính phủ sẽ có trách nhiệm chứng minh nó thực sự được đưa ra một cách tự nguyện.

Sự đồng ý có thể bị thu hồi bất cứ lúc nào. Việc khám xét phải chấm dứt ngay lập tức khi rút lại sự đồng ý. Vậy điều gì sẽ xảy ra nếu nghi phạm có suy nghĩ thứ hai sau khi máy tính của anh ta đã được thu thập và đưa đến phòng thí nghiệm để xử lý? Tiêu chuẩn tương tự được áp dụng (hầu như). Việc tìm kiếm phải dừng lại khi họ thu hồi sự đồng ý. Điều đó nói rằng, các tòa án đã nói rằng điều này KHÔNG áp dụng cho sao y pháp y. Nói cách khác, mặc dù bản gốc phải được trả lại, nhưng bất kỳ bản sao nào đã được thực hiện thì không. Bị cáo không có kỳ vọng hợp lý về quyền riêng tư với bản sao pháp y ( [United States v. Megahed, 2009](#17__United_States_v__Megahed__20) ). Vì lý do này, sao chép một ổ đĩa sớm hơn là muộn hơn là một bước đi rất khôn ngoan.

Phạm vi của việc tìm kiếm sự đồng ý đôi khi là vấn đề trong một vụ án hình sự. Nếu họ đồng ý cho bạn khám xét ngôi nhà, liệu đó có bao gồm các thùng chứa và máy tính đóng kín không? Vâng, điều đó phụ thuộc vào các chi tiết cụ thể của tình huống. Tòa án sẽ lại áp dụng tiêu chuẩn “tính hợp lý” để đưa ra quyết định. Một người hợp lý sẽ hiểu được phạm vi của những điều kiện đó là gì?

Bên cấp sự đồng ý có thể đặt ra các hạn chế đối với việc tìm kiếm. Trong trường hợp đó, các sĩ quan phải chấp hành yêu cầu này. Làm theo cách khác rất có thể dẫn đến việc triệt tiêu bất kỳ bằng chứng nào được thu hồi.

Nâng cao hơn

Các mẫu thỏa thuận

Trong các tìm kiếm xoay quanh sự đồng ý, nó thường phụ thuộc vào từ của bên này hơn là từ của bên kia. Chính xác những gì đã được nói, nó được nói như thế nào, và những gì nghi phạm hiểu được vào thời điểm đó đều có thể được xem xét kỹ lưỡng. Một biểu mẫu đồng ý tham gia tìm kiếm được thiết kế kỹ lưỡng sẽ giúp chống lại bất kỳ cuộc tấn công nào nhằm vào tìm kiếm. Biểu mẫu phải bao gồm các chi tiết cụ thể liên quan đến bằng chứng kỹ thuật số. Biểu mẫu phải xin phép để tìm kiếm không chỉ máy tính mà bất kỳ phương tiện lưu trữ nào bao gồm điện thoại di động, sách hướng dẫn, máy in, v.v. Biểu mẫu phải xin phép mang những mục này từ địa điểm để điều tra bên ngoài ( [Văn phòng Điều hành Luật sư Hoa Kỳ, 2009](#4__Executive_Office_for_United_S) ).

Cuối cùng, điều quan trọng cần nhớ là tìm kiếm sự đồng ý có thể mang nhiều sắc thái và phụ thuộc nhiều vào các sự kiện hoặc hoàn cảnh phát sinh trong sự việc cụ thể đó. Mặc dù việc tìm kiếm mà không có lệnh khám xét đôi khi là điều cần thiết, nhưng cách tốt nhất là bạn nên nhận lệnh khám xét bất cứ khi nào có thể. Trường hợp của bạn sẽ được đặt trên một nền tảng vững chắc hơn nhiều khi có lệnh khám xet hơn là không có.

Các bên thứ ba đôi khi có thể đồng ý với việc khám xét tài sản riêng. Bạn cùng phòng, vợ / chồng và cha mẹ chỉ là một vài ví dụ. Thông thường, nếu một thiết bị được chia sẻ, tất cả các bên đều có quyền đồng ý để tìm kiếm các khu vực chung của thiết bị đó. Trong tình huống này, không ai trong số họ có mong đợi hợp lý về quyền riêng tư trong các khu vực chung vì nó được chia sẻ với người khác. Ý niệm về các khu vực chung là đáng kể. Các khu vực chẳng hạn như những khu vực được bảo vệ bằng mật khẩu sẽ không đủ điều kiện là khu vực chung. Bên thứ ba có thể sẽ không có quyền đồng ý với việc tìm kiếm của mình. Tuy nhiên, nếu nghi phạm đã chia sẻ mật khẩu với bên thứ ba, thì ràng buộc này không còn được áp dụng nữa. Kỳ vọng hợp lý về quyền riêng tư của nghi phạm đã giảm đi đáng kể.

Có thể thấy trước rằng cuối cùng, bên thứ ba được đề cập thực sự không có thẩm quyền để đồng ý. Điều này không nhất thiết phải là một công cụ phá vỡ thỏa thuận nếu có liên quan đến khả năng chấp nhận. Các nhân viên tại hiện trường chỉ có thể làm những gì mà một người hợp lý sẽ làm khi xác định được khả năng hợp pháp của bên thứ ba để đưa ra sự đồng ý. Nếu nghi phạm có mặt tại hiện trường, bên thứ ba không được phép đồng ý.

Trong những trường hợp bình thường, vợ hoặc chồng có thể đồng ý tìm kiếm các khu vực chung. Cha mẹ có thể có hoặc không thể đồng ý khám xét tài sản của trẻ. Nếu đứa trẻ được đề cập dưới mười tám tuổi, cha mẹ thường được phép đồng ý. Nếu đứa trẻ trên mười tám tuổi, thì nó sẽ phức tạp hơn một chút. Các yếu tố sẽ ảnh hưởng đến quyết định này bao gồm tuổi của đứa trẻ, việc chúng có trả tiền thuê nhà hay không và những bước nào (nếu có) mà chúng đã thực hiện để hạn chế quyền tiếp cận.

Các kỹ thuật viên thường ở vị trí tìm ra bằng chứng trong quá trình làm việc của họ. Các tòa án đã được phân chia khi quyết định xem kỹ thuật viên có thẩm quyền đồng ý hay không. Các viên chức có thể tạo lại tìm kiếm của kỹ thuật viên hoặc quan sát họ thực hiện lại các bước của họ. Tuy nhiên, họ có thể không mở rộng phạm vi tìm kiếm của kỹ thuật viên hoặc hướng dẫn họ tìm hiểu sâu hơn. Nếu kỹ thuật viên xác định được bằng chứng, phát hiện của họ thường được sử dụng làm cơ sở cho lệnh khám xét.

Các trường hợp cấp thiết thỉnh thoảng phát sinh yêu cầu thu giữ ngay lập tức và có thể khám xét thiết bị kỹ thuật số. Điều này thường được cho phép theo một trong ba điều kiện sau: bằng chứng đang bị đe dọa tiêu hủy vĩnh viễn, mối đe dọa khiến cơ quan thực thi pháp luật hoặc công chúng nói chung gặp nguy hiểm và khi nghi phạm được cho là sẽ trốn thoát trước khi có được lệnh khám xét. Ngoại lệ này có thể áp dụng cho việc thu giữ một vật phẩm hoặc thiết bị, nhưng không tự động tìm kiếm nó. Một khi vật phẩm đã được thu giữ (được lệnh khám xet), quyền hạn có thể không còn nữa, do đó yêu cầu tiếp tục thực hiện lệnh khám xét.

Các viên chức có quyền buộc tội nghi phạm với bằng chứng mà họ xem liệu họ có được phép hợp pháp ở nơi họ đang ở hay không và nếu mục đó rõ ràng là có thể buộc tội ngay lập tức. Đây được gọi là học thuyết quan điểm đơn giản . Tình huống này thường phát sinh trong bối cảnh pháp y kỹ thuật số khi người giám định đang phân tích động cơ tìm bằng chứng của một tội phạm và tìm thấy bằng chứng của một tội phạm hoàn toàn khác. Ví dụ, một giám định viên đang tìm kiếm ảnh của tác phẩm nghệ thuật bị đánh cắp trong ổ cứng thì bắt gặp hình ảnh “đen”. Tại thời điểm này, việc khám xét sẽ dừng lại cho đến khi có được một lệnh riêng liên quan đến việc sở hữu nội dung “đen”.

Các cuộc lục soát và khám xét biên giới do các sĩ quan quản chế và tạm tha có phạm vi lớn hơn nhiều so với các cuộc khám xét do các sĩ quan cảnh sát tiến hành. Từ quan điểm của tòa án, các cá nhân nhập cảnh vào quốc gia này có thể bị khám xét với lý do có thể xảy ra hoặc thậm chí là nghi ngờ hợp lý. Tòa án công nhận sự cần thiết của chính phủ trong việc lệnh khám xet biên giới khỏi hàng lậu và vật chất. Những cá nhân bị quản chế hoặc tạm tha có ít kỳ vọng về quyền riêng tư hơn những công dân khác. Ví dụ: tội phạm tình dục có thể bị cấm sử dụng Internet trong thời gian họ được giám sát phát hành. Quy định này sẽ cho phép viên chức tạm tha hoặc quản chế có quyền khám xét máy tính của phạm nhân bất cứ lúc nào để đảm bảo tuân thủ. Thậm chí có một số án lệ cho phép loại tìm kiếm này mà không có các điều kiện cụ thể này.

Nhân viên tại nơi làm việc có thể có hoặc không có kỳ vọng hợp lý về quyền riêng tư trên máy tính làm việc của họ. Kỳ vọng này sẽ khác nhau tùy thuộc vào thực tế bao gồm cả việc nhân viên đó có phải là nhân viên chính phủ hay không. Thông thường, các viên chức có thể khám xét máy tính của nhân viên mà không cần lệnh nếu chủ lao động hoặc đồng nghiệp khác (có quyền được chia sẻ) cho phép. Các nhân viên chính phủ được nhìn nhận hơi khác một chút. Điều đó không có nghĩa là người sử dụng lao động không thể tìm kiếm trong hệ thống của nhân viên; nó chỉ có nghĩa là việc tìm kiếm phải “ liên quan đến công việc, được chứng minh khi bắt đầu và trong phạm vi cho phép” ( [Văn phòng Điều hành cho Luật sư Hoa Kỳ, 2009](#4__Executive_Office_for_United_S) ).

## Quyền tìm kiếm bằng chứng

Không có một trong các trường hợp ngoại lệ được xác định rõ ràng được mô tả ở đây, các sĩ quan cảnh sát phải có lệnh khám xét trước khi khám xét tài sản riêng của ai đó, bao gồm cả máy tính của họ.

Lệnh khám xét là lệnh do quan chức thực thi pháp luật có được từ thẩm phán, cấp cho họ quyền khám xét một địa điểm cụ thể và bắt giữ những người hoặc vật cụ thể.

Một thẩm phán sẽ ra trát khi họ tin rằng có thể có nguyên nhân nào đó mà tội phạm đã được thực hiện và những người hoặc những thứ được chỉ định trong trát sẽ được tìm thấy tại địa điểm đó. Tòa án tối cao cho rằng nguyên nhân có thể xảy ra được xác định khi có “xác suất hợp lý là hàng lậu hoặc bằng chứng phạm tội sẽ được tìm thấy ở một nơi cụ thể” ( [Illinois v. Gates, 1983](#8__Illinois_v__Gates__462_U_S__2) ). Một cách khác để xem xét nó có nhiều khả năng hơn là không tìm thấy các đồ vật hoặc người bị tịch thu tại địa điểm cụ thể đó. Về mặt toán học, điều này tương đương với xác suất 51%.

Khi nộp đơn xin trát, việc xác định vai trò của máy tính đối với tội phạm là rất hữu ích. Máy tính có thể bị coi là hàng lậu nếu nó chứa nội dung “đen” hoặc là tài sản bị đánh cắp. Máy tính cũng có thể được sử dụng để lưu trữ bằng chứng, chẳng hạn như các tài liệu buộc tội. Cuối cùng, máy tính có thể đóng vai trò như một công cụ hoặc phương tiện phạm tội. Ví dụ như đây là trường hợp máy tính được sử dụng để xâm nhập vào mạng của một công ty.

### 4.1 Nắm bắt phần cứng hay chỉ thông tin?

Từ Tu chính án thứ tư, chúng ta biết rằng lệnh khám xét phải “đặc biệt mô tả địa điểm được khám xét và người hoặc đồ vật sẽ bị thu giữ.” Để đáp ứng hiệu quả yêu cầu đó, trước tiên chúng ta cần hiểu chính xác những gì chúng ta cần nắm bắt. Tóm lại, đó là phần cứng hay thông tin do phần cứng nắm giữ? Nếu máy tính là hàng lậu, bằng chứng, trái cây hoặc công cụ của tội phạm, thì chúng ta cần xác định nguyên nhân có thể xảy ra để thu giữ phần cứng. Nếu không, chúng ta chỉ tập trung vào thông tin.

### 4.2 Tính đặc biệt

Các tòa án cau mày nặng nề về các bản tuyên thệ quá rộng thiếu tính đặc biệt mà Tu chính án thứ tư yêu cầu. Bản tuyên thệ phải nêu rõ những vật dụng nào có thể bị tịch thu và những vật phẩm nào không thể thu giữ. "Đặc biệt" mô tả những thứ mà bạn có thể chưa bao giờ thấy có vẻ như là một nhiệm vụ bất khả thi. Nó thực sự không phải. Số sê-ri và những thứ tương tự không bắt buộc.

Đây là một số ngôn ngữ mẫu có thể được sử dụng:

“Bất kỳ và tất cả (các) máy tính cá nhân / (các) hệ thống máy tính đặt tại nơi cư trú của (CHÈN ĐỊA CHỈ TẠI ĐÂY), để bao gồm các thiết bị đầu vào và đầu ra, phương tiện lưu trữ điện tử, băng máy tính, máy quét, đĩa, đĩa, thiết bị lưu trữ quang học, máy in, màn hình, bộ xử lý trung tâm và tất cả các phương tiện lưu trữ liên quan cho dữ liệu điện tử, cùng với tất cả các thiết bị và vật liệu vận hành liên quan đến máy tính khác. ”

Mô tả thông tin có thể được thực hiện theo cách tương tự. Ví dụ, mặc dù chúng ta có thể không biết tên tệp, nhưng rất có thể chúng ta sẽ biết tên của nghi phạm, khoảng thời gian và tội phạm cụ thể đang được điều tra. Các tòa án đang tìm kiếm một số loại ngôn ngữ hạn chế. Yêu cầu "bất kỳ và tất cả các tệp" trên ổ cứng của nghi phạm có khả năng rất cao bị cho là quá rộng, dẫn đến việc loại bỏ bất kỳ bằng chứng nào được tìm thấy.

### 4.3 Thiết lập nhu cầu phân tích ngoài địa điểm

Việc phân tích pháp y của một ổ cứng có thể là một quá trình rất tốn thời gian. Vì nhiều lý do, việc này tốt nhất nên được thực hiện tại phòng thí nghiệm hoặc đồn cảnh sát. Đối với tất cả các ý định và mục đích, thực hiện việc này tại hiện trường đồng thời với việc tìm kiếm không nên là lựa chọn đầu tiên. Do đó, bản tuyên thệ của trát khám xét phải trình bày bằng các thuật ngữ rõ ràng về logic và sự cần thiết của việc thực hành này. Các lý do có thể bao gồm lượng thời gian và dữ liệu liên quan và khả năng sử dụng các kỹ thuật kháng lâm cũng như nhu cầu thực hiện nhiệm vụ này trong các điều kiện được kiểm soát chặt chẽ hơn (như các điều kiện được tìm thấy trong phòng thí nghiệm). Đây là một cách để làm rõ điều này trong bản tuyên thệ:

“Các thiết bị lưu trữ của máy tính (như đĩa cứng hoặc CD-ROM) có thể lưu trữ hàng triệu trang thông tin. Ngoài ra, nghi phạm có thể cố gắng che giấu bằng chứng tội phạm; người đó có thể lưu trữ nó theo thứ tự ngẫu nhiên với các tên tệp lừa đảo. Điều này có thể yêu cầu cơ quan tìm kiếm xem xét tất cả dữ liệu được lưu trữ để xác định các tệp cụ thể nào là bằng chứng hoặc công cụ của tội phạm. Quá trình sắp xếp này có thể mất vài tuần hoặc vài tháng, tùy thuộc vào khối lượng dữ liệu được lưu trữ, và sẽ không thực tế và có tính xâm phạm nếu cố gắng tìm kiếm loại dữ liệu này tại chỗ.

Yêu cầu kỹ thuật. Việc tìm kiếm các hệ thống máy tính để tìm bằng chứng tội phạm đôi khi đòi hỏi các quy trình kỹ thuật cao đòi hỏi kỹ năng của chuyên gia và môi trường được kiểm soát thích hợp. Một loạt các phần cứng và phần mềm máy tính có sẵn đòi hỏi ngay cả các chuyên gia máy tính cũng phải chuyên về một số hệ thống và ứng dụng, vì vậy rất khó để biết trước khi tìm kiếm chuyên gia nào có đủ trình độ để phân tích hệ thống và dữ liệu của nó. Tuy nhiên, trong mọi trường hợp, các quy trình tìm kiếm dữ liệu là các quy trình khoa học chính xác được thiết kế để bảo vệ tính toàn vẹn của bằng chứng và khôi phục ngay cả các tệp “ẩn”, bị xóa, nén, được bảo vệ bằng mật khẩu hoặc được mã hóa. Bởi vì bằng chứng máy tính dễ bị sửa đổi hoặc phá hủy vô tình hoặc cố ý (cả từ các nguồn bên ngoài hoặc từ mã phá hoại được gắn vào hệ thống như một "bẫy lừa"), một môi trường được kiểm soát có thể cần thiết để hoàn thành một phân tích chính xác. " ( [Văn phòng Điều hành cho Luật sư Hoa Kỳ, 2009](#4__Executive_Office_for_United_S) )

### 4.4 Luật truyền thông được lưu trữ

Đạo luật Truyền thông Lưu trữ (SCA), được ban hành vào năm 1986, cung cấp sự bảo vệ quyền riêng tư theo luật định cho khách hàng của các nhà cung cấp dịch vụ mạng. SCA kiểm soát cách chính phủ có thể truy cập thông tin tài khoản được lưu trữ từ các thực thể như Nhà cung cấp dịch vụ Internet (ISP). Thông tin tài khoản này thường bao gồm e-mail cũng như thông tin về người đăng ký và thanh toán. Cụ thể, SCA đưa ra quy trình mà các quan chức thực thi pháp luật liên bang và tiểu bang phải tuân thủ để buộc nhà cung cấp phải tiết lộ những hồ sơ này.

SCA tìm cách mã hóa loại thông tin được tìm kiếm, các kỳ vọng về quyền riêng tư liên quan đến thông tin đó và công cụ pháp lý cần thiết để chính phủ truy cập thông tin đó. SCA chia các nhà cung cấp dịch vụ thành hai nhóm riêng biệt và khác biệt: các nhà cung cấp “dịch vụ liên lạc điện tử” và các tổ chức cung cấp “dịch vụ máy tính từ xa”. Hiểu được những khác biệt này là điều cần thiết để giải mã SCA và các yêu cầu pháp lý của nó.

Theo SCA, cụ thể là 18 USC § 2510 (15), nhà cung cấp dịch vụ liên lạc điện tử (ECS) là “bất kỳ dịch vụ nào cung cấp cho người dùng khả năng gửi hoặc nhận liên lạc bằng dây hoặc điện tử.” Các ví dụ về ECS sẽ bao gồm các công ty cung cấp dịch vụ điện thoại và e-mail ( [Văn phòng Điều hành cho Luật sư Hoa Kỳ, 2009](#4__Executive_Office_for_United_S) ). America Online xuất hiện trong tâm trí, cũng như Hotmail. Bạn có thể ngạc nhiên khi biết rằng bất kỳ công ty nào, bất kể trọng tâm của nó là gì, đều có thể đủ điều kiện trở thành ECS.

Tiêu đề 18 USC§ 2711 (2) định nghĩa dịch vụ tính toán từ xa (RCS) là “việc cung cấp cho công chúng các dịch vụ lưu trữ hoặc xử lý máy tính thông qua hệ thống truyền thông điện tử”. Nói một cách khác, RCS được cung cấp bởi một “máy tính ngoài cơ sở lưu trữ hoặc xử lý dữ liệu cho khách hàng” ( [Văn phòng Điều hành Luật sư Hoa Kỳ, 2009](#4__Executive_Office_for_United_S) ).

SCA cũng giải quyết nhiều loại thông tin mà các nhà cung cấp này lưu trữ. Điều này có thể bao gồm thông tin người đăng ký cơ bản như tên, địa chỉ và số thẻ tín dụng. Thông tin tiềm năng khác bao gồm nhật ký và các e-mail đã mở, chưa mở, bản nháp và đã gửi.

## Khám phá điện tử (eDiscovery)

Bằng chứng kỹ thuật số vẫn còn sống và tốt trong các vụ án dân sự. Các bên liên quan đến vụ kiện tụng cần phải xem xét tất cả các dữ liệu có thể có liên quan cũng như bất kỳ dữ liệu nào có thể phải được tiết lộ cho bên phản đối. Các phương tiện khám phá thông thường bao gồm thẩm vấn, lưu chiểu và yêu cầu cung cấp tài liệu ( [Hội nghị Sedona, 2007](#14__Sedona_Conference__The_Sedon) ). Thông tin được lưu trữ điện tử (ESI) đưa ra một số thách thức mà hồ sơ giấy không làm được. Ví dụ, ESI dễ bị sửa đổi, dễ bay hơi và dễ bị sao chép và phân tán. Do đó, các quy tắc về bằng chứng cho cả tòa án tiểu bang và liên bang đang thay đổi để giải quyết cụ thể ESI.

( [Hội nghị Sedona, 2007](#14__Sedona_Conference__The_Sedon) ) định nghĩa Khám phá điện tử là “Quá trình thu thập, chuẩn bị, xem xét và sản xuất thông tin được lưu trữ điện tử (“ ESI ”) trong bối cảnh quy trình pháp lý” ( [Hội nghị Sedona, 2007](#14__Sedona_Conference__The_Sedon) )

### 5.1 Nhiệm vụ bảo tồn

Bằng chứng từng bị giới hạn trong các bản ghi nhớ giấy và tủ hồ sơ giờ đây đã được tìm thấy trong các tài liệu Microsoft Word và băng sao lưu. Bằng chứng kỹ thuật số khác biệt đáng kể so với bằng chứng trên giấy nên nhiều luật sư đã quen với việc xử lý. Ví dụ, bằng chứng kỹ thuật số dễ bay hơi hơn nhiều và dễ bị thay đổi hoặc phá hủy hơn. Âm lượng là một điểm khác biệt quan trọng. Có thể có một lượng dữ liệu đáng kinh ngạc như vậy trong một trường hợp có thể tốn hàng triệu đô la chỉ để sản xuất và xem xét chúng.

Vào tháng 12 năm 2006, các tòa án liên bang đã thực hiện bước quan trọng đầu tiên trong việc giải quyết và xử lý bằng chứng kỹ thuật số, thay đổi Quy tắc tố tụng dân sự. Những thay đổi quy tắc này bắt buộc các luật sư đối lập phải làm việc cùng nhau để xử lý thông tin được lưu trữ điện tử (ESI) trong trường hợp rất sớm trong quá trình này. Giải quyết ESI sớm trong một trường hợp giúp giảm chi phí, thời gian và khả năng các bằng chứng liên quan bị bỏ qua. Không phải tất cả các luật sư và thẩm phán đều chấp nhận những thay đổi này. Giống như nhiều người khác, một số luật sư và thẩm phán rất khó chịu với công nghệ, thậm chí còn phải nhờ người khác điều tra rồi in e-mail của họ.

Zubalake v. USB Warburg là một loạt các trường hợp khám phá điện tử mang tính bước ngoặt. Các phán quyết của thẩm phán Shira Scheindlin giải quyết nhiều mối quan tâm cơ bản trong các trường hợp liên quan đến ESI. Một số mối quan tâm bao gồm nghĩa vụ bảo quản dữ liệu điện tử, nghĩa vụ của luật sư giám sát việc khách hàng của họ tuân thủ các nguyên tắc này, lấy mẫu dữ liệu, thay đổi chi phí và các biện pháp trừng phạt.

Nhiệm vụ bảo quản dữ liệu có thể liên quan bắt đầu khi có "dự đoán hợp lý về kiện tụng." Việc không nhận ra yếu tố kích hoạt này và thực hiện hành động có thể dẫn đến việc phân tán bằng chứng và có thể có các biện pháp trừng phạt nghiêm khắc để khởi động. Giống như các tiêu chuẩn pháp lý khác được đề cập trong chương này, việc xác định một dự kiến hợp lý của vụ kiện tụng có thể khó khăn, trên thực tế là khá khó khăn. Nhiệm vụ bảo tồn không chỉ được gây ra bởi sự xuất hiện của trát đòi hầu tòa. Rất có thể nhiệm vụ đã bắt đầu tốt trước thời điểm đó. Đó là một sự xác định rất cụ thể về thực tế sẽ thay đổi theo từng trường hợp. Việc sa thải một nhân viên bất mãn có thể đủ để kích hoạt nó; tương tự như vậy, một lời buộc tội quấy rối tình dục của một nhân viên đối với cấp trên của họ cũng vậy.

Thẩm phán Scheindlin cũng đề cập đến nhiệm vụ của luật sư là giám sát nỗ lực của thân chủ của họ trong việc xác định, bảo quản, thu thập và đưa ra bằng chứng có khả năng liên quan. Cô ấy nói, một phần, "[c] ounsel phải thực hiện các bước khẳng định để giám sát sự tuân thủ để tất cả các nguồn thông tin có thể khám phá được xác định và tìm kiếm." Hơn nữa, cô ấy nói rằng các luật sư nên soạn thảo và phân phối "hồ sơ kiện tụng" hướng dẫn một công ty và nhân viên của công ty bảo vệ dữ liệu có liên quan và đảm bảo chúng không bị phá hủy hoặc bị xâm phạm theo bất kỳ cách nào.

Lấy mẫu dữ liệu là một cách để điều tra một tập hợp lớn ESI về “sự tồn tại hoặc tần suất của thông tin liên quan” ( [Hội nghị Sedona, 2007](#14__Sedona_Conference__The_Sedon) ). Khối lượng dữ liệu liên quan tiềm ẩn có thể đáng kinh ngạc, đặc biệt là trong môi trường doanh nghiệp lớn. Lấy mẫu dữ liệu là một trong những cách tốt nhất để tiết kiệm thời gian và giảm chi phí trong quá trình Khám phá điện tử.

Chi phí phát sinh trong quá trình Khám phá điện tử có thể rất lớn, lên đến hàng trăm nghìn hoặc thậm chí hàng triệu đô la. Thông thường, trong khám phá truyền thống, bên sản xuất chịu chi phí sản xuất. Trong những điều kiện nhất định, chi phí sản xuất có thể được chuyển cho bên yêu cầu. Trong trường hợp Zubalake , thẩm phán Scheindlin đã giải quyết mối lo ngại này và đưa ra một bài điều tra bảy yếu tố được sử dụng để xác định xem việc dịch chuyển chi phí có được đảm bảo hay không.

Bảy yếu tố là “(1) mức độ yêu cầu được điều chỉnh cụ thể để khám phá thông tin liên quan; (2) sự sẵn có của thông tin đó từ các nguồn khác; (3) tổng chi phí sản xuất so với số tiền đang tranh cãi; (4) tổng chi phí sản xuất so với các nguồn lực sẵn có của mỗi bên; (5) khả năng tương đối của mỗi bên trong việc kiểm soát chi phí và động cơ của họ để làm như vậy; (6) tầm quan trọng của vấn đề đang được đề cập trong vụ kiện tụng và; (7) lợi ích tương đối cho các bên trong việc thu thập thông tin ”( Zubulake v. UBS Warburg, 2003 ).

### 5.2 Tìm kiếm Riêng tư trong Nơi làm việc

Không có gì lạ khi máy tính làm việc trở thành đối tượng của việc tìm kiếm các hành động hình sự, dân sự hoặc hành chính. Từ khía cạnh riêng tư, các nhà tuyển dụng có một chút kinh nghiệm để tìm kiếm máy tính công ty của một cá nhân. Chính sách sử dụng máy tính của công ty trình bày rõ ràng rằng máy tính làm việc, e-mail, v.v. chỉ dành cho mục đích công việc và chúng có thể được tìm kiếm bất cứ lúc nào là phương pháp hay nhất được chấp nhận. Đối với các mục đích của Tu chính án thứ tư (cơ quan thực thi pháp luật hoặc đại diện của họ), máy tính làm việc có thể được tìm kiếm với sự đồng ý của người giám sát hoặc nhân viên khác miễn là họ có thẩm quyền chung đối với khu vực được tìm kiếm. Cũng cần lưu ý rằng các quy chế về quyền riêng tư của liên bang và Đạo luật về Truyền thông được Lưu trữ cũng có thể có hiệu lực.

Cuối cùng, hãy tham khảo ý kiến của luật sư truy tố hoặc cố vấn của công ty / nội bộ để được hướng dẫn. Nhận được ý kiến đóng góp của họ có thể giúp đảm bảo rằng vụ kiện trên cơ sở pháp lý vững chắc nhất ( [Văn phòng Điều hành cho Luật sư Hoa Kỳ, 2009](#4__Executive_Office_for_United_S) )

Báo động!

Khám phá điện tử quốc tế

Với môi trường đám mây và dữ liệu thường xuyên bay xuyên biên giới, việc khám phá điện tử quốc tế đang trở thành một vấn đề. Không phải mọi quốc gia đều có cùng quan điểm về quyền riêng tư hoặc các tiêu chuẩn pháp lý và thủ tục khám phá giống nhau. Do đó, việc truy cập dữ liệu ở nước ngoài rất phức tạp. Khung phân tích các xung đột xuyên biên giới của Hội nghị Sedona : Hướng dẫn thực tế để điều hướng các dòng cạnh tranh về quyền riêng tư và khám phá dữ liệu quốc tế là một phần giới thiệu tuyệt vời về những phức tạp liên quan đến Khám phá điện tử quốc tế. Bạn có thể tải xuống miễn phí từ <http://www.thesedonaconference.org/>.

## Bằng chứng chuyên môn

Là một giám định viên pháp y kỹ thuật số, bạn phải chuẩn bị để làm chứng trước tòa với tư cách là một nhân chứng chuyên môn về những phát hiện và thủ tục của bạn. Sự khác biệt giữa nhân chứng và chuyên gia là gì? Một sự khác biệt chính là một nhân chứng chuyên môn đủ điều kiện có thể đưa ra ý kiến, nhưng một nhân chứng “thông thường” thì không thể.

Việc xác định cá nhân có phải là chuyên gia hay không là việc để tòa án quyết định. Một chuyên gia không nhất thiết phải có bằng Tiến sĩ hoặc các bằng cấp cao quý khác. FindLaw định nghĩa một chuyên gia là người “nhờ có kiến thức, kỹ năng, đào tạo hoặc kinh nghiệm đặc biệt có đủ điều kiện cung cấp lời khai để hỗ trợ người tìm hiểu sự thật trong những vấn đề vượt quá kiến thức thông thường của người bình thường” (FindLaw).

Theo định nghĩa này, thợ làm bánh, thợ may, kế toán, bác sĩ y tế và tài xế xe buýt trường học có thể đủ tiêu chuẩn như một chuyên gia. Thông tin xác thực chắc chắn giúp ích, nhưng chúng không phải là một yêu cầu.

Có hai trường hợp tạo nền tảng cho việc chấp nhận lời khai của chuyên gia. Đầu tiên là trường hợp năm 1923, Hoa Kỳ kiện Frye . Vụ án của [Frye (1923)](#5__Frye_v__United_States___293_F) tập trung vào khả năng chấp nhận của công nghệ phát hiện nói dối mới. Trong trường hợp này, cái được gọi là "Thử nghiệm Frye." Thử nghiệm nói rằng “kết quả của các thử nghiệm hoặc quy trình khoa học chỉ được chấp nhận làm bằng chứng khi các thử nghiệm hoặc quy trình đã được chấp nhận chung trong lĩnh vực cụ thể mà chúng thuộc về” ( [United States v. Frye, 1923](#5__Frye_v__United_States___293_F) ).

Cuối cùng, Frye Test đã thất bại. Trong [Daubert kiện Merrell Dow Pharmaceuticals, Inc. , 509 US 579 (1993)](#2__Daubert_v__Merrell_Dow_Pharma) , Tòa án Tối cao Hoa Kỳ đã phán quyết rằng Quy tắc về Bằng chứng Liên bang thay thế Phép thử Frye. Merrell Dow Pharmaceuticals Inc. đã bị kiện bởi các nguyên đơn cho rằng thuốc của họ, Bendectin, đã gây ra các dị tật bẩm sinh nghiêm trọng. Tòa án cấp dưới đã chấp thuận yêu cầu tóm tắt của Merrell Dow với lý do rằng bằng chứng khoa học do nguyên đơn đưa ra vẫn chưa được cộng đồng khoa học chấp thuận. Tòa án tối cao đã đồng ý.

Trong [Daubert (1993)](#2__Daubert_v__Merrell_Dow_Pharma) , Tòa án cho rằng khả năng chấp nhận nên được đánh giá dựa trên “liệu lý luận hoặc phương pháp luận cơ bản của lời khai có hợp lệ về mặt khoa học và có thể được áp dụng đúng vào các sự kiện được đề cập hay không. Sẽ có nhiều cân nhắc đối với cuộc điều tra, bao gồm liệu lý thuyết hoặc kỹ thuật được đề cập có thể được (và đã được) điều tra hay không, liệu nó có được đánh giá và công bố đồng nghiệp hay không, tỷ lệ lỗi đã biết hoặc tiềm ẩn và sự tồn tại và duy trì các tiêu chuẩn kiểm soát. hoạt động của nó, và liệu nó có thu hút được sự chấp nhận rộng rãi trong một cộng đồng khoa học có liên quan hay không ”( [Daubert, 1993](#2__Daubert_v__Merrell_Dow_Pharma) ).

Hiểu rõ cơ sở này sẽ giúp thẩm tra viên hiểu rõ hơn về khả năng chấp nhận lời khai của họ trong bối cảnh của pháp luật.

Tài nguyên bổ sung

Bằng chứng chuyên môn

Cuốn sách của Fred Smith và Rebecca Bace về lời khai của chuyên gia, Hướng dẫn về lời khai pháp y: Nghệ thuật và thực hành trình bày lời khai với tư cách là một nhân chứng kỹ thuật chuyên nghiệp , chứa đựng một lượng lớn thông tin thực tế. Một trong những khía cạnh hay nhất của cuốn sách là nó được viết cho các chuyên gia công nghệ thông tin. Cuốn sách bao gồm chủ đề tốt và khá "dễ đọc."

## Bản tóm tắt

*Đối với chương 7, hiện tại chỉ mang tính chất tham khảo các luật tư pháp tại Hoa Kỳ và trên thế giới về quyền riêng tư.*

Khám xét đúng thẩm quyền là bước đầu tiên cần thiết trong quy trình khám nghiệm pháp y. Bằng chứng được thu thập mà không có nó rất có thể bị loại trừ. Tu chính án thứ tư của Hiến pháp Hoa Kỳ bảo vệ công dân khỏi các cuộc khám xét và tịch thu không hợp lý. Các biện pháp bảo vệ do Tu chính án thứ tư đưa ra chỉ bao gồm các hành động của chính phủ. Nó không áp dụng cho các công dân tư nhân tự hành động. Cơ quan thực thi pháp luật có thể tìm kiếm và thu giữ bằng chứng kỹ thuật số có và không có lệnh khám xét. Từ quan điểm pháp lý, các tìm kiếm có trát luôn tốt hơn các tìm kiếm không có lệnh. Điều đó nói rằng, các tình huống cấp bách có thể và có thể phát sinh cho phép các viên chức làm khác.

Về khía cạnh riêng tư, người giám sát và người sử dụng lao động có thể sẽ có toàn quyền tìm kiếm máy tính của công ty, đặc biệt nếu nhân viên đọc và ký thỏa thuận sử dụng máy tính nêu rõ rằng máy tính, e-mail của công ty, v.v. có thể được tìm kiếm bất cứ lúc nào.

Tham khảo ý kiến của cố vấn pháp lý phù hợp trước khi tìm kiếm hoặc thu giữ bằng chứng kỹ thuật số không bao giờ là một ý tưởng tồi. Nếu bạn có thắc mắc hoặc mối quan tâm, chúng phải luôn được nêu ra trước.

## Tổng kết và kiến thức thêm chương 7

Đối với môi trường Việt Nam hiện tại, có rất nhiều pháp lý đảm bảo quyền riêng tư cho người dân, cá nhân. Tuy nhiên chưa được đưa vào ứng dụng rõ ràng cho mục đích cung cấp quyền tìm kiếm bằng chứng cho mục đích hình sự/dân sự.

Tài liệu tham khảo

1. Casey E. Bằng chứng kỹ thuật số và tội phạm máy tính, xuất bản lần thứ 3: Khoa học pháp y, máy tính và Internet Waltham, MA: Academic Press; 2011.

2. Daubert kiện Merrell Dow Pharmaceuticals, Inc., 509 US 579 (1993).

3. Văn phòng Điều hành cho Luật sư Hoa Kỳ. Truy tố tội phạm máy tính Washington, DC: Bộ Tư pháp Hoa Kỳ; Năm 2007; Phòng Giáo dục Pháp luật.

4. Văn phòng Điều hành cho Luật sư Hoa Kỳ. Tìm kiếm và thu giữ máy tính cũng như thu thập bằng chứng điện tử trong các cuộc điều tra tội phạm Washington, DC: Bộ Tư pháp Hoa Kỳ; Năm 2009; Phòng Giáo dục Pháp luật.

5. Frye kiện Hoa Kỳ, .293 F. 1013 (DC Cir 1923).

6. FindLaw. (nd). Bản sửa đổi thứ tư — Tìm kiếm và thu giữ . Được truy cập ngày 4 tháng 10 năm 2011, từ: <http://caselaw.lp.findlaw.com/data/constitution/amendment04/>.

7. Goldfoot J. Máy tính vật lý và Tu chính án thứ tư. Tạp chí Luật Hình sự Berkley . 2011; 16 (1): 112–167.

8. Illinois kiện Gates, 462 US 213, 238, (1983).

9. Hệ điều hành Kerr. Bằng chứng kỹ thuật số và thủ tục hình sự mới. Tạp chí Luật Columbia . 2005a; 105 (1): 279–318.

10. Hệ điều hành Kerr. Tìm kiếm và thu giữ trong thế giới kỹ thuật số. Tạp chí Luật Harvard . 2005b; 119 (2): 532–585.

11. Kroll OnTrack, Inc. (nd). Zubulake kiện UBS Warburg . Truy cập ngày 10 tháng 10 năm 2011, từ: <http://www.krollontrack.co.uk/zubulake/>.

12. McCullagh, D. (2007, ngày 14 tháng 12). Thẩm phán: Con người không thể bị buộc phải ly hôn cụm mật khẩu mã hóa . Truy cập ngày 3 tháng 10 năm 2011, từ: <http://news.cnet.com/8301-13578_3-9834495-38.html>.

13. Scheindlin S, Capra DJ. Khám phá điện tử và bằng chứng kỹ thuật số: Vỏ và vật liệu Eagan, MN: Thomson West 2008.

14. Hội nghị Sedona. Thuật ngữ Hội nghị Sedona: E-Discovery & quản lý thông tin kỹ thuật số xuất bản lần thứ 2. Sedona, AZ: Hội nghị Sedona; Năm 2007.

15. TechTarget. Khám phá điện tử Được truy cập ngày 6 tháng 11 năm 2011, từ Search Financial Security 2007; www.TechTarget.com: http://searchfinancialsecurity.techtarget.com/definition/electronic-discovery.

16. Bộ Tư pháp Hoa Kỳ, Văn phòng các Chương trình Tư pháp. (2010). Quyền riêng tư và Quyền tự do dân sự . Được truy cập ngày 10 tháng 10 năm 2011, từ: [http://it.ojp.gov/default.aspx?area=privacy&page=1284#contentTop](http://it.ojp.gov/default.aspx?area=privacy%26page=1284#contentTop) .

17. United States v. Megahed, 2009 WL 722481, at \* 3 (MD Fla. 18/03/2009).

18. Hoa Kỳ kiện Slanina, 283 F.3d 670, 680 (5th Cir. 2002).

19. Hoa Kỳ kiện Walser, 275 F.3d 981, 986 (10 Cir. 2001).

20. Zubulake kiện UBS Warburg, 217 FRD 309 (SDNY 2003).

# Chương 8: Internet và E-Mail

**Thông tin trong Chương này:**

Tổng quan về Internet và cách nó hoạt động



Cách thức hoạt động của trình duyệt web và bằng chứng họ có thể tạo



Chức năng E-Mail & Pháp y



Bằng chứng trò chuyện và mạng xã hội



Bằng chứng qua e-mail và Internet có thể đóng một vai trò quan trọng trong bất kỳ cuộc điều tra nào. Chương 8 xem xét các công nghệ đằng sau Internet như HTTP, Địa chỉ IP, mạng ngang hàng, ứng dụng trò chuyện và trình duyệt web. Nó cũng bao gồm việc đọc tiêu đề e-mail và các cách để che giấu danh tính của người gửi.

Bộ định vị tài nguyên thống nhất (URL), Trình duyệt, Giao thức truyền siêu văn bản (HTTP), Tên miền cấp cao nhất (TLD), Tên miền, IP (Giao thức Internet), Máy chủ tên miền (DNS), HTML (Ngôn ngữ đánh dấu siêu văn bản), Whois, Gnutella, Peer-to-Peer (P2P), INDEX.DAT, Cookies, Internet Temporary Files (TIF), NTUSER.DAT, Internet Relay Chat, ICQ, Simple Mail Transfer Protocol (SMTP), Post Office Protocol (POP), Internet Message Access Giao thức (IMAP), Giả mạo, Phát lại ẩn danh, ID tin nhắn

## Giới thiệu

Ban đầu, Internet là một công cụ ít được biết đến bởi một số học giả và quân đội. Ngày nay, nó thực sự là một công cụ dành cho đại chúng. Chúng ta có thể đặt bánh pizza, thanh toán hóa đơn, tra cứu số điện thoại và tham gia một lớp học. Đối với nhiều người trong chúng ta, thật khó để tưởng tượng cuộc sống mà không có nó. Đối với những người giám định, việc sử dụng nó có thể để lại những bằng chứng đáng kể. Duyệt web, trò chuyện, e-mail và mạng xã hội chỉ là một số công nghệ mà chúng ta phải hiểu cách chúng được sử dụng, cách chúng hoạt động và nơi chúng để lại dấu vết.

## Tổng quan về Internet

Chúng ta sẽ bắt đầu bằng phần giới thiệu nhanh về công nghệ liên quan đến việc đưa trang web yêu thích của bạn xuất hiện trên màn hình máy tính của bạn. Có lẽ cách tốt nhất là theo dõi quá trình từ đầu đến cuối. Tất cả bắt đầu khi ai đó nhập địa chỉ web hoặc URL (Bộ định vị tài nguyên đồng nhất) vào thanh địa chỉ của trình duyệt . URL bao gồm ba phần: máy chủ lưu trữ, tên miền và tên tệp. Hãy sử dụng <http://www.digitalforensics.com>làm ví dụ.

Trong ví dụ của chúng ta, “http” hoặc Giao thức truyền siêu văn bản (HTTP) là giao thức được sử dụng trên Internet để duyệt và tương tác với các trang web và những thứ tương tự. Một giao thức không gì khác hơn là một cách được thỏa thuận để các thiết bị giao tiếp với nhau. Tiếp theo là tên miền , “pháp y kỹ thuật số”. Cuối cùng là Tên miền cấp cao nhất (TLD) , “.com.” Nó được gọi là TLD vì nó nằm trên cùng của hệ thống phân cấp tạo nên hệ thống tên miền của Internet. Các TLD khác bao gồm .org, .edu và .net, chỉ để nêu tên một số.

Trình duyệt, sử dụng giao thức HTTP, gửi yêu cầu “nhận” đến máy chủ web lưu trữ [www.digitalforensics.com](http://www.digitalforensics.com) . Trình duyệt là một ứng dụng được sử dụng để xem và truy cập nội dung trên Internet. Có một số trình duyệt để bạn lựa chọn: phổ biến nhất là Internet Explorer của Microsoft, Firefox của Mozilla và Chrome của Google.

Sau khi nhấn enter, công việc đầu tiên là chuyển đổi tên miền thành địa chỉ IP (Giao thức Internet) . Internet hoạt động với địa chỉ IP. Nó không thể làm bất cứ điều gì với chính tên miền. Tên miền dành cho chúng ta, giúp bạn dễ nhớ hơn. Máy chủ tên miền (DNS) chịu trách nhiệm ánh xạ tên miền tới các địa chỉ IP cụ thể. Sau khi DNS thực hiện chuyển đổi, yêu cầu sau đó sẽ được gửi đến máy chủ lưu trữ trang web. Sau khi nhận được yêu cầu, máy chủ sẽ trả về trang web được yêu cầu và nội dung liên quan.

Một trang web bao gồm một số thành phần. Đầu tiên là tài liệu HTML (Ngôn ngữ đánh dấu siêu văn bản) . Điều này chứa khá nhiều thông tin bao gồm hướng dẫn về cách trang sẽ được trình duyệt, nội dung, v.v. hiển thị (hiển thị). Nó cũng chứa tên tệp cho các thành phần con của trang web như hình ảnh. Điều quan trọng cần lưu ý là HTML không phải là một ngôn ngữ lập trình.

Có hai loại trang web: tĩnh và động. Trang web tĩnh là trang được tạo sẵn. Nội dung, bố cục của nó, v.v., đã được xác định trước. Tuy nhiên, một trang động được xây dựng “nhanh chóng”. Nó không tồn tại cho đến khi nó được gọi. Trang được xây dựng từ các phần khác nhau được rút ra từ cơ sở dữ liệu. Amazon là một ví dụ tuyệt vời về một trang web động. Trang của tôi rất có thể sẽ khác với trang của bạn. Những cuốn sách, v.v. xuất hiện trên trang của tôi dựa trên thói quen mua sắm và mua sắm của tôi. Tất cả thông tin này được lưu trữ trong (các) cơ sở dữ liệu cùng với những thứ như hình ảnh cuốn sách, mô tả, v.v. Khi tôi đăng nhập vào Amazon, máy chủ sẽ gửi các mục tiêu chuẩn cho mọi người (như logo Amazon) cùng với nội dung được nhắm mục tiêu đến tôi.

Khi tương tác với một trang web, điều quan trọng là phải hiểu những điều nhất định đang xảy ra ở đâu. Điều này có thể đặc biệt quan trọng khi biết từ góc độ pháp y vì nó có thể cho bạn biết bạn nên tìm kiếm một hiện vật nhất định ở đâu. Các hành động có thể xảy ra ở phía máy khách hoặc phía máy chủ. JavaScript (không liên quan đến ngôn ngữ lập trình Java) là một công nghệ phía máy khách. Nó được sử dụng cho những thứ như cuộn qua trên thanh điều hướng. Mã thực hiện công việc đó được tải xuống và chạy trên máy cục bộ. Các hành động phía máy chủ hoàn toàn ngược lại và được sử dụng khi có nhu cầu gửi thông tin đến một máy tính khác (như nội dung tùy chỉnh của tôi tại Amazon).

Tài nguyên bổ sung

Công nghệ web

Web ngày nay là một nơi phức tạp sử dụng nhiều công nghệ khác nhau để làm cho nó chạy. Hiểu được cách thức hoạt động của những thứ này, ngay cả ở mức độ thô sơ, sẽ rất hữu ích. Trang web Trường học w3 là một nguồn tài liệu giới thiệu tuyệt vời về nhiều công nghệ này. Trang web bao gồm tài liệu tham khảo, bài học, câu đố, hướng dẫn và hơn thế nữa.

<http://www.w3schools.com/>

Việc xác định quyền sở hữu và máy chủ của một tên miền cụ thể có thể trở nên phù hợp trong một vụ án hình sự hoặc dân sự. Truy vấn tìm kiếm được gọi là “whois” có thể giúp bạn xác định một số cá nhân và / hoặc công ty được liên kết với một tên miền nhất định. Tìm kiếm whois có thể cho bạn biết người đăng ký, thời điểm miền được tạo, người liên hệ quản trị và người liên hệ kỹ thuật. Thông tin liên hệ thường cung cấp tên, địa chỉ và số điện thoại. Hầu hết nếu không phải tất cả các công ty đăng ký tên miền hiện cung cấp đăng ký riêng tư. Bất kỳ ai tìm kiếm một tên miền có đăng ký riêng tư thường sẽ nhận được thông tin liên hệ của công ty đăng ký, thay vì chủ sở hữu thực sự ( [Network Solutions, LLC](#5__Network_Solutions__LLC___n_d) ). Nếu bạn muốn thử điều này, hãy truy cập một trong những trang web cung cấp dịch vụ whois. Giải pháp Mạng là một: <http://www.networksolutions.com/whois/index.jsp>.

### 2.1 Peer-to-Peer (P2P)

P2P được sử dụng chủ yếu như một phương tiện để chia sẻ tệp. Một phần lớn lưu lượng truy cập trên mạng P2P là nhạc và phim vi phạm bản quyền cũng như nội dung “đen”. P2P khác với mạng máy khách / máy chủ ở chỗ các máy tính trên mạng P2P có thể phục vụ cả hai vai trò (máy khách và máy chủ). Gnutella là một trong những hệ thống hoặc kiến trúc chính được sử dụng trong mạng P2P.

Nâng cao hơn

Yêu cầu của Gnutella

Trên mạng P2P, điều gì ngăn một yêu cầu tệp chỉ lan truyền mãi mãi? Thực ra có một cơ chế tích hợp sẵn trong các gói thông tin. Trong mỗi gói, có một giá trị Thời gian tồn tại (TTL) được đặt để giảm một giá trị mỗi khi nó được phân phối đến một nút khác trên mạng. Khi số đó chạm 0, gói tin sẽ bị dừng lại.

Để bắt đầu với mạng P2P, trước tiên người dùng phải tải xuống và cài đặt một ứng dụng khách P2P như KaZaA, Frostwire, GigaTribe hoặc eMule. Thông thường, người dùng sau đó tạo một thư mục "chia sẻ" chứa các tệp mà họ muốn cung cấp cho người khác. Để tìm các tệp quan tâm để tải xuống, người dùng thường nhập (các) cụm từ tìm kiếm cho tệp hoặc các tệp mà họ muốn. Nếu tìm kiếm thành công, phần mềm sẽ trả về danh sách các máy tính có (các) tệp được yêu cầu. Cuối cùng, các tệp được tải xuống thư mục do người dùng chọn hoặc đến vị trí mặc định do máy khách chỉ định. Mạng P2P sử dụng HTTP để truyền tệp.

Các nút trên Gnutella được chia thành hai loại. Các nút có băng thông cần thiết cũng như thời gian hoạt động (thời gian trên mạng) được phân loại là Ultrapeer. Những thứ không được gọi là lá. Ultrapeer thực hiện một số nhiệm vụ bổ sung như tìm kiếm, lập chỉ mục và hỗ trợ kết nối.

### 2.2 Tệp INDEX.DAT

INDEX.DAT là một tệp nhị phân, giống như vùng chứa được sử dụng bởi Internet Explorer (MSIE) của Microsoft. Tệp INDEX.DAT có khá nhiều giá trị đối với những người giám định pháp y. Có nhiều tệp INDEX.DAT trên một hệ thống. INDEX.DAT theo dõi một số thông tin liên quan đến các URL được truy cập, số lượt truy cập, v.v. Những tệp này bị ẩn khỏi người dùng và phải được xem bằng một công cụ nào đó. Cả FTK và EnCase đều có thể giải mã các tệp INDEX.DAT. MSIE có ba thư mục: Lịch sử, Cookie và Tệp Internet Tạm thời. Các tệp INDEX.DAT được sử dụng để theo dõi thông tin và nội dung của từng thư mục ( [Casey, 2009](#1__Casey_E__Handbook_of_Digital) ).

## Trình duyệt web — Internet Explorer

Trình duyệt web là một phần không thể thiếu trong trải nghiệm máy tính tổng thể và đóng vai trò như “phương tiện” của chúng ta trên “Siêu xa lộ thông tin” được gọi là World Wide Web. Mặc dù có nhiều trình duyệt trên thị trường, nhưng Internet Explorer của Microsoft ngày càng được sử dụng rộng rãi nhất. Các trình duyệt khác (dành cho PC) cũng nhận được một số sức hút là Firefox của Mozilla và Chrome của Google. Trên máy tính Macintosh, Safari là vua, và Firefox cũng được sử dụng ở đây. Tại nền tảng của họ, các ứng dụng này hoạt động theo cùng một cách. Ví dụ, tất cả chúng đều sử dụng một số loại hệ thống bộ nhớ đệm. Họ cũng có cơ chế xử lý cookie, lịch sử Internet, URL đã nhập, dấu trang, v.v. Chúng khác nhau ở các chi tiết. Không gian không cho phép một cái nhìn toàn diện về tất cả các trình duyệt và chi tiết về hoạt động bên trong của chúng. Thay vào đó, chúng ta sẽ tập trung vào một số chức năng phổ biến như chúng có trong MSIE, công ty dẫn đầu thị trường.

### 3.1 Cookie

Cookie là một tệp văn bản nhỏ được máy chủ web gửi vào máy tính của người dùng. Cookie có thể phục vụ nhiều mục đích khác nhau. Chúng có thể được sử dụng để theo dõi các phiên cũng như ghi nhớ các tùy chọn của người dùng đối với một trang web cụ thể. [Amazon.com](http://Amazon.com) là một ví dụ tuyệt vời. Khi bạn quay lại trang web, bạn thường được chào đón bằng “Xin chào, Susan” cũng như các đề xuất tùy chỉnh dựa trên lịch sử mua hàng và duyệt web của bạn. Mức độ cá nhân hóa đó được thực hiện thông qua cookie.

Cookie có thể cung cấp bằng chứng có giá trị và được theo dõi trong một tệp INDEX.DAT duy nhất. Chúng có thể chứa Bộ định vị tài nguyên thống nhất (URL), ngày và giờ, tên người dùng, v.v. Giải mã một cookie có thể là một thách thức, vì chúng thường không được viết rõ ràng. May mắn thay cho chúng ta, có sẵn các công cụ để thực hiện việc này. Điều quan trọng cần lưu ý là sự tồn tại của một địa chỉ web trong cookie không nhất thiết là bằng chứng cho thấy kẻ tình nghi đã thực sự truy cập trang web ( [Casey, 2009](#1__Casey_E__Handbook_of_Digital) ).

### 3.2 Tệp Internet tạm thời, hay còn gọi là bộ nhớ cache web

Chúng ta rất thiếu kiên nhẫn. Do đó, tốc độ rất quan trọng đối với trải nghiệm Internet của người dùng. Ngày nay, trình duyệt web được cho là gần như không thể phân biệt được với các ứng dụng chạy trên máy của chúng ta. bộ nhớ cache web là một cách mà các nhà sản xuất trình duyệt loại bỏ bớt thời gian tải xuống. Bộ nhớ đệm tăng tốc độ mọi thứ bằng cách tái sử dụng các thành phần của trang web như hình ảnh, tiết kiệm thời gian khỏi việc phải tải xuống các đối tượng nhiều lần.

Trình duyệt của Microsoft, Internet Explorer, đề cập đến bộ đệm web dưới dạng Tệp Internet Tạm thời (TIF) . Trong Microsoft Internet Explorer, TIF được tổ chức thành các thư mục con mang tên ngẫu nhiên gồm tám ký tự. Chúng được tổ chức bằng cách sử dụng một tập hợp các tệp INDEX.DAT. Mỗi tệp trong TIF có một giá trị ngày và giờ tương ứng được liên kết với nó. Điều này bao gồm thời gian “điều tra lần cuối”, được sử dụng bởi trình duyệt để xác định xem phiên bản mới hơn có tồn tại trên máy chủ hay không. Nếu vậy, nó sẽ tải xuống phiên bản mới hơn.

Người dùng có thể xem TIF của họ bất cứ lúc nào bằng Windows Explorer. Bên trong thư mục TIF, người dùng sẽ thấy một danh sách các nội dung của nó. Mỗi mục trong danh sách sẽ hiển thị một biểu tượng hiển thị loại tệp, tên tệp và URL được liên kết. Điều quan trọng là phải hiểu rằng trong trường hợp này, những gì người dùng nhìn thấy là bản trình bày nội dung được ảo hóa. Các mục thực tế được giữ trong các thư mục con TIF. Tệp duy nhất thực sự được giữ ở đây là INDEX.DAT giữ các tab về vị trí các tệp được đặt bên trong các thư mục con khác nhau.

Bằng chứng về email trên web cũng có thể được tìm thấy trong TIF. Hotmail, AOL và Yahoo! tất cả có thể để lại tin nhắn và / hoặc thông tin hộp thư đến có thể chứng minh là hữu ích. Các mục này có thể được nhận dạng bằng tên tệp. Dưới đây là một số ví dụ:

Tin nhắn Outlook web Access — Đọc [#]. Htm



Tin nhắn AOL — Msgview [#]. Htm



Tin nhắn hotmail — getmsg [#]. Htm



Yahoo! —ShowLetter [#]. Htm



Hộp thư đến Outlook web Access — Main [#]. Htm



Hộp thư đến AOL — Msglist [#]. Htm



Hộp thư đến Hotmail — HoTMail [#]. Htm



Yahoo! —ShowFolder.htm



Nâng cao hơn

Bộ nhớ đệm và HTTPS

Nếu bạn đã từng mua bất kỳ thứ gì trên Internet hoặc thực hiện bất kỳ ngân hàng trực tuyến nào, thì rất có thể bạn đã sử dụng giao thức HTTPS. HTTPS không chỉ được sử dụng cho thương mại điện tử. Nó cũng được sử dụng cho e-mail dựa trên web an toàn.

HTTPS là phiên bản an toàn của giao thức HTTP mà chúng ta sử dụng trên Internet. Theo mặc định, và vì lý do bảo mật, MSIE không lưu vào bộ đệm bất kỳ trang web HTTPS nào. Điều này là quan trọng cần lưu ý, đặc biệt nếu bạn đang điều tra một trường hợp có thể liên quan đến một số loại lưu lượng truy cập web HTTPS. Nếu vậy, bạn có thể không tìm thấy bất kỳ tàn tích nào của hoạt động này trong bộ nhớ cache.

bộ nhớ cache web có thể được sử dụng để xác định cả khả năng lừa dối và ý định. Phần lớn những gì trong bộ nhớ cache của web sẽ là hình thu nhỏ (những hình ảnh nhỏ đó) cùng với các bit và phần của trang web.

Kích thước hình ảnh có thể ảnh hưởng đến một trường hợp, đặc biệt là những trường hợp liên quan đến nội dung “đen”. Nếu những hình ảnh tình nghi chỉ bao gồm những hình ảnh nhỏ, giống như bộ nhớ cache, thì một số công tố viên có thể miễn cưỡng buộc tội. Vấn đề sau đó trở thành ý định. Những hình ảnh đó có thể được tải xuống tự động mà không có sự đồng ý của anh ấy. Hình ảnh có kích thước nhỏ như vậy có thể tạo ra một trường hợp yếu hơn nhiều. Những hình ảnh lớn hơn, những hình ảnh không thường được tìm thấy như một phần của trang web, khó giải thích hơn.

### 3.3 Lịch sử trình duyệt Internet

Internet Explorer của Microsoft, vị vua trị vì của các trình duyệt, lưu giữ nhiều hồ sơ người dùng lịch sử. Lịch sử được sử dụng để ngăn người dùng phải nhập lại URL vào thanh địa chỉ của trình duyệt. Các tệp index.dat cũng theo dõi các chi tiết khác. Ví dụ: nó theo dõi số lần trang web được truy cập và tên của tệp. Lịch sử Internet được sắp xếp thành nhiều thư mục và tệp index.dat. Có ba thư mục: Hàng ngày, Hàng tuần và Tích lũy.

Các thư mục này sử dụng quy ước đặt tên dựa trên tiền tố đã đặt, theo sau là phạm vi ngày. Ví dụ: một thư mục bao gồm lịch sử Internet từ ngày 1 tháng 10 năm 2011 đến ngày 8 tháng 10 năm 2011, sẽ trông giống như sau:

MSHist012011100120111008

MSHist01 - Tên / tiền tố thư mục

2011 - Năm (bắt đầu)

1001 - Ngày (bắt đầu)

2011 - Ngày (kết thúc)

1008 - Ngày (kết thúc)

Những người có điều gì đó muốn che giấu thường sẽ xóa lịch sử của họ một cách thường xuyên. Điều này có thể được thực hiện thủ công bởi người dùng hoặc tự động bởi hệ thống. Theo mặc định, lịch sử được đặt để xóa hai mươi ngày một lần. Người dùng có thể thay đổi điều này để xóa nhanh hơn nhiều. Sử dụng một công cụ có thể đọc sổ đăng ký, bạn có thể xem thông tin này tại đây:

NTUSERS \ Software Microsoft \ Windows \ CurrentVersion \ Internet Settings \ URL History

Nâng cao hơn

Tệp NTUSER.DAT

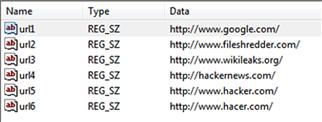
Tệp NTUSER.DAT chứa cài đặt tùy chọn và thông tin riêng cho từng hồ sơ người dùng. Lịch sử trình duyệt là một phần của thông tin này. Có một NTUSER.DAT cho mỗi hồ sơ người dùng trên hệ thống. Mặc dù về mặt kỹ thuật là một tệp đăng ký, NTUSER.DAT nằm trong thư mục người dùng. Lưu ý rằng chúng ta đang nói về "hồ sơ" của người dùng chứ không phải "người dùng". Đưa một người cụ thể lên bàn phím là một điều rất khó nếu không muốn nói là không thể quyết tâm thực hiện. Chỉ vì một người có hồ sơ trên máy không có nghĩa là ngón tay của họ đã ở trên bàn phím tại bất kỳ thời điểm nào.

Nếu giá trị này được đặt nhỏ hơn giá trị mặc định là hai mươi ngày, thì giá trị này có thể được sử dụng để cho thấy bị đơn đã chủ động thực hiện các bước để loại bỏ bằng chứng buộc tội có khả năng xảy ra.

### 3.4 Phần mềm Internet Explorer trong Sổ đăng ký

Là một phần của chức năng hàng ngày của nó, MSIE gửi các đồ tạo tác vào sổ đăng ký. Các mục này được lưu trữ đặc biệt trong tổ ong NTUSER.DAT. Tại đây, chúng ta có thể xem liệu trình duyệt có lưu trữ mật khẩu, công cụ tìm kiếm mặc định, nhà cung cấp dịch vụ tìm kiếm mặc định hay không, v.v.

Cơ quan đăng ký cũng có thể cho chúng ta biết những URL nào đã được nhập ngay vào thanh địa chỉ của trình duyệt. Đây là danh sách từ 1 đến 25 với số thấp nhất là gần đây nhất. Chỉ có thể giữ hai mươi lăm mục nhập cùng một lúc. Các mục nhập được xóa trên cơ sở nhập trước, xuất trước. [Hình 8.1](#F0010_7) cho bạn thấy chúng trông như thế nào thông qua một công cụ pháp y.



Hình 8.1 Các URL đã nhập như được tìm thấy trong Windows Registry. Đồ họa của Jonathan Sisson.

Đây là đường dẫn tệp đến cấu phần đăng ký này:

NTUSER \ Software \ Microsoft \ Internet Explorer \ URL đã nhập

Hãy nhớ rằng, sổ đăng ký không thể đọc được ở dạng nguyên bản của nó. Để điều tra nó, bạn sẽ cần một công cụ thích hợp. Một số công cụ này bao gồm RegEdit của Microsoft, RegRipper của Harlan Carvey và Trình xem sổ đăng ký của AccessData.

### 3.5 Ứng dụng trò chuyện

Các ứng dụng trò chuyện đều phổ biến và nhiều. Chúng được sử dụng để giao tiếp dựa trên văn bản tức thì. Các ứng dụng phổ biến bao gồm AOL Instant Messenger (AIM), Yahoo! Messenger, Windows Live Messenger, Trillian, Digsby, v.v. Những khách hàng này có thể được sử dụng để thực hiện hoặc để tạo điều kiện cho nhiều loại tội phạm. Những kẻ ấu dâm sử dụng những công cụ này để gạ gẫm tình dục trẻ vị thành niên hoặc phát tán nội dung “đen”. Người mua và người bán sử dụng chúng để thương lượng việc mua bán và chuyển giao chất ma tuý. Danh sách có thể tiếp tục và tiếp tục. Chức năng thay đổi từ khách hàng này sang khách hàng khác cũng như các hiện vật mà họ để lại. Chức năng và bằng chứng còn sót lại cũng có thể khác nhau giữa các phiên bản. Thật khó để bắt kịp với tốc độ thay đổi nhanh chóng của những khách hàng này. Các thay đổi có thể dẫn đến việc di chuyển hoặc biến mất hiện vật. Thay vì “tìm đến cỏ dại” với từng ứng dụng và phiên bản, chúng ta sẽ nói chuyện rộng rãi về những loại hiện vật có thể có và cách chúng có thể được sử dụng làm bằng chứng.

Không giống như các phần mềm khác, ứng dụng trò chuyện sẽ để lại các tạo tác của quá trình cài đặt của nó. Đường dẫn và thư mục có thể thay đổi đôi chút. Sự hiện diện hoặc vắng mặt của các tệp và thư mục này có thể giúp chứng minh hoặc bác bỏ rằng một khách hàng cụ thể đã được sử dụng để giao tiếp với nạn nhân hoặc đồng phạm.

Các chương trình trò chuyện duy trì một liên hệ hoặc danh sách "bạn thân". Danh sách tên màn hình này có thể được sử dụng để liên kết các cá nhân với nhau, đặc biệt nếu tên màn hình của các bên khác xuất hiện trong nhật ký hoặc trên ổ đĩa. Tên trên màn hình thường vô nghĩa, như “footballfan7878” và có thể cần một chút nỗ lực để kết nối chúng với một người cụ thể. Nhập tên màn hình như một phần của tìm kiếm từ khóa của bạn cũng có thể rất hữu ích. Để làm phức tạp thêm vấn đề, người dùng có thể có nhiều tên màn hình. Nhiều khi những danh tính thay thế này giả định mối quan hệ cha mẹ-con với danh tính chính.

Người dùng cũng có thể chọn chặn mọi người, ngăn họ giao tiếp với họ. Nếu chức năng này khả dụng, thì cài đặt này nên được theo dõi ở đâu đó, có khả năng để lại các phần mềm có liên quan. Thường thì khách hàng cũng sẽ duy trì một danh sách các cuộc trò chuyện gần đây.

Các tùy chọn khác dưới sự kiểm soát của người dùng bao gồm nhúng ngày giờ vào cuộc trò chuyện, chọn biểu tượng hoặc hình ảnh tùy chỉnh và bật hoặc tắt tính năng ghi nhật ký. Việc ghi nhật ký có thể đóng vai trò là một nguồn bằng chứng to lớn nếu nó được kích hoạt.

Thông thường, ghi nhật ký bị tắt theo mặc định, yêu cầu người dùng kích hoạt chức năng đó. Nhật ký thường ghi lại các cuộc trò chuyện trò chuyện và / hoặc thông tin liên quan khác như chi tiết kết nối, v.v. Ngay cả khi tắt ghi nhật ký, người dùng có thể lưu phiên trò chuyện cụ thể đó theo cách thủ công nếu họ cần. Sự khác biệt chính giữa việc bật ghi nhật ký và lưu nhật ký phiên theo cách thủ công là vị trí lưu tệp kết quả. Các bản ghi được lưu tự động thường sẽ đi đến một vị trí mặc định, trong khi một điểm đến sẽ cần được chọn cho một bản ghi được lưu theo cách thủ công.

Một cài đặt ưu tiên khác được quan tâm liên quan đến việc chấp nhận tự động cuộc gọi điện video, truyền tệp, tin nhắn tức thì thời gian thực, v.v. Theo mặc định, nhiều tính năng này bị tắt. Cài đặt này và chức năng tiếp theo có thể được sử dụng để chứng minh rằng một hình ảnh không được tải xuống mà không có sự đồng ý. Một kẻ tình nghi sẽ có một khẩu hiệu khó nghe để cố gắng khiến bồi thẩm đoàn tin rằng họ “không biết” họ đã tải xuống nội dung “đen” thông qua ứng dụng trò chuyện của họ khi các cài đặt chứng minh rằng họ phải đồng ý chấp nhận.

Một số ứng dụng trò chuyện / IM hiện đang cho phép người dùng kết hợp một điện thoại di động (hoặc nhiều hơn một) với tài khoản của họ. Điều này cho phép họ chuyển tiếp tin nhắn IM đến điện thoại di động của họ. Trong trường hợp này, số ô cùng với thông tin tài khoản có thể được sử dụng để giúp kết nối người đó với một tên màn hình cụ thể.

### 3.6 Trò chuyện chuyển tiếp Internet (IRC)

Ứng dụng khách trò chuyện thương mại như Yahoo! và AOL khá phổ biến và được sử dụng rộng rãi. Có hai ứng dụng khách trò chuyện khác rất đáng để khám phá. Những công cụ này được cho là phù hợp hơn với hoạt động tội phạm. Internet Relay Chat hoặc IRC là một trong những công cụ như vậy. IRC là một mạng lưới trò chuyện lớn có ít hoặc không có sự giám sát vì nó nằm dưới sự kiểm soát của không một thực thể nào. Nó cho phép người dùng gần như vô danh vì không có quy trình đăng ký chính thức. IRC cũng được sử dụng miễn phí. Mạng IRC bao gồm nhiều mạng nhỏ hơn như Undernet, IRCnet và EFnet, chỉ cần kể tên một số ( [Casey, 2011](#2__Casey_E__Digital_Evidence_and_1) ). Người dùng IRC tạo phòng trò chuyện hoặc “kênh” của riêng họ. IRC thu hút bọn tội phạm có nhiều lợi ích tìm cách buôn bán thông tin hoặc hàng lậu. Sự xâm nhập mạng, đánh cắp danh tính và nội dung “đen” đại diện cho một số lợi ích tội phạm chính được tìm thấy trên IRC.

IRC tự hào có một số tính năng khác khiến nó trở nên hấp dẫn đối với bọn tội phạm. Kết nối Máy khách Trực tiếp (DCC) cho phép hai người dùng kết nối trực tiếp từ máy này sang máy kia. Trong chế độ này, thông tin liên lạc là hoàn toàn riêng tư. Lưu lượng truy cập riêng tư này thậm chí còn tránh các máy chủ mạng, không để lại bằng chứng cho các nhà điều tra tìm thấy.

### 3.7 ICQ "Tôi tìm kiếm bạn"

ICQ là công cụ trò chuyện thứ hai đảm bảo việc xem xét kỹ hơn. ICQ xuất hiện vào năm 1996.

Những con số này từ ICQ cung cấp cho bạn ý tưởng về mức độ phổ biến của ứng dụng trò chuyện này:

Hơn 42 triệu người dùng đang hoạt động



Hơn 425 triệu lượt tải xuống



Hơn 1,1 tỷ tin nhắn được gửi và nhận mỗi ngày



Người dùng ICQ trung bình được kết nối hơn năm giờ mỗi ngày



47% nữ và 53% nam



80% người dùng trong độ tuổi từ mười ba đến hai mươi chín



Có sẵn bằng mười sáu ngôn ngữ (ICQ)



Không giống như IRC, ICQ có quy trình đăng ký. Người dùng đăng ký được chỉ định Số nhận dạng người dùng hoặc UIN. Giao tiếp trên ICQ duy trì mức độ riêng tư cao. Một người phải được mời tham gia vào một cuộc trò chuyện. ICQ thực hiện định tuyến lưu lượng truy cập thông qua các máy chủ tập trung nên một số hiện vật có thể tồn tại ở đó nếu máy chủ đó có thể được tìm thấy.

## E-mail

Trong tất cả các nguồn bằng chứng kỹ thuật số tiềm năng, e-mail là một trong những nguồn tốt nhất. Mọi người thường soạn thảo và gửi e-mail mà họ cho rằng sẽ không bao giờ được đọc bởi bất kỳ ai khác ngoài người nhận dự định. Do đó, những cuộc trao đổi thường xuyên thẳng thắn này có thể (và đã) trở lại gây ám ảnh cho các bên liên quan. Nó cũng dai dẳng, cư trú ở nhiều vị trí, do đó khó loại bỏ hơn.

### 4.1 Truy cập E-mail

E-mail được truy cập và quản lý theo một trong hai cách. Đầu tiên là e-mail dựa trên web như Gmail của Google hoặc Hotmail của Microsoft. Các công cụ này hoạt động thông qua trình duyệt web. Thứ hai là thông qua một ứng dụng e-mail (máy khách). Ứng dụng khách e-mail là các chương trình chuyên biệt được thiết kế đặc biệt để làm việc với e-mail. Một số ứng dụng cũng quản lý lịch, tác vụ, danh bạ và hơn thế nữa. Outlook và Windows Live Mail của Microsoft là hai trong số các ứng dụng e-mail phổ biến nhất trên hệ thống Windows. Outlook, phiên bản mạnh mẽ hơn trong số hai, được sử dụng chủ yếu ở nơi làm việc hoặc bởi những người dùng thành thạo. Windows Live Mail và người tiền nhiệm Outlook Express có nhiều chức năng hạn chế hơn.

Outlook lưu trữ dữ liệu trong tệp .pst hoặc .ost. Windows Live Mail và Outlook Express sử dụng .dbx. Việc truy cập các thông báo riêng lẻ từ bên trong các vùng chứa này là một mối quan tâm, nhưng bây giờ ít hơn nhiều vì một số công cụ hiện tại xử lý các loại tệp này một cách nguyên bản. Các tin nhắn e-mail cá nhân (tệp .msg) có thể được xuất ra ngoài và đưa cho các nhà điều tra hoặc luật sư để xem xét.

### 4.2 Giao thức e-mail

E-mail sử dụng nhiều giao thức để gửi và nhận e-mail. Một số trong số đó là:

Giao thức truyền thư đơn giản (SMTP) —Dùng máy khách e-mail để gửi e-mail và bằng máy chủ để gửi và nhận.



Giao thức Bưu điện (POP) —Dùng e-mail client sử dụng để nhận e-mail.



Internet Message Access Protocol (IMAP) —Giao thức giao tiếp hai chiều được khách hàng sử dụng để truy cập e-mail trên máy chủ.



### 4.3 E-mail làm bằng chứng

E-mail được sử dụng rộng rãi và mọi người có xu hướng không bị cấm trong các tin nhắn của họ, nói những điều mà họ có thể không bao giờ nói khác. Do đó, e-mail có thể cung cấp cho chúng ta rất nhiều bằng chứng tiềm năng. Một số điều đó bao gồm:

Thông tin liên quan đến vụ việc



Địa chỉ e-mail



Các địa chỉ IP



Ngày và giờ



Khi điều tra e-mail, điều quan trọng là nhận ra rằng nó có thể được tìm thấy ở một số nơi. Chúng bao gồm: máy của nghi phạm, bất kỳ máy nào của người nhận, máy chủ của công ty hoặc phương tiện dự phòng, điện thoại thông minh, nhà cung cấp dịch vụ và bất kỳ máy chủ nào mà tin nhắn có thể đã đi qua trên đường đến đích cuối cùng. Giống như hầu hết các bằng chứng dựa trên web, thời gian vẫn là một yếu tố. Thu thập bằng chứng sớm hơn là muộn hơn sẽ mang lại cho bạn cơ hội thành công cao hơn.

Các thành phần chính của e-mail là tiêu đề, nội dung và các tệp đính kèm có thể xảy ra. Mỗi thư e-mail được gửi đi đều có tiêu đề . Tiêu đề ghi lại thông tin khi e-mail đi từ người gửi đến người nhận. Hãy coi nó như một tấm hộ chiếu. Tại mỗi điểm dừng (máy chủ) trên đường đi, thông tin được thêm vào tiêu đề. Nội dung của e-mail là chính thông điệp . Cuối cùng, bất kỳ tệp đính kèm nào cũng được thêm vào. Chúng bao gồm những thứ như hình ảnh và các tệp do người dùng tạo như tài liệu, bảng tính, v.v. Giữ cho các tệp đính kèm được kết nối với một thông điệp e-mail liên quan là rất quan trọng từ góc độ chứng cứ.

### 4.4 E-mail — Bao quát Đường mòn

Đặc biệt là những kẻ tình nghi hiểu biết có thể thực hiện các bước để ngăn ai đó truy tìm thông điệp trở lại họ. Ví dụ, họ có thể giả mạo một e-mail (làm cho nó có vẻ là của người khác) hoặc xóa hoặc sửa đổi các tiêu đề. Những kẻ tình nghi cũng có thể tạo một tài khoản e-mail giả mạo.

Có một phần mềm miễn phí trên Internet cho phép người dùng “giả mạo” một e-mail. Giả mạo là hành động làm cho e-mail trông như thể nó thực sự đến từ người khác hoặc từ một địa điểm khác. Có những dịch vụ có sẵn sẽ gửi lại (chuyển tiếp) tin nhắn, loại bỏ thông tin nhận dạng trước khi truyền. Điều này được gọi là phát lại ẩn danh. Nhiều công ty trong số này không lưu giữ nhật ký, đảm bảo hơn nữa quyền riêng tư của người dùng của họ.

Báo động!

Tài khoản e-mail được chia sẻ

E-mail có thể được sử dụng để liên lạc ngay cả khi không được gửi đi. Điều này được thực hiện bằng cách tạo một tài khoản ẩn danh, Yahoo! ví dụ, và chia sẻ thông tin đăng nhập. Sau đó, người dùng chỉ cần tạo tin nhắn và gửi chúng vào thư mục “Thư nháp” để người khác đọc. Sau khi tin nhắn được đọc, nó có thể bị xóa. Các tài khoản này có thể được sử dụng một lần nên gần như không thể theo dõi hoặc theo dõi. Đây là một thực tế phổ biến trong số những kẻ khủng bố. Richard Clarke, cựu chiến sĩ chống khủng bố của Hoa Kỳ cho biết: “Các tài khoản ẩn danh chỉ sử dụng một lần là cực kỳ khó theo dõi.

<http://www.pbs.org/wgbh/pages/frontline/shows/front/special/techsidebar.html>

### 4.5 Truy tìm E-mail

Việc theo dõi một thông điệp e-mail phụ thuộc rất nhiều vào nhật ký. Như chúng ta đã biết trước đó, mỗi máy chủ dọc theo đường dẫn của e-mail sẽ thêm thông tin vào tiêu đề của thư. Một trong những thông tin đó là ID tin nhắn . ID thư là một số duy nhất được máy chủ e-mail gán cho thư. Tương quan ID tin nhắn với nhật ký của máy chủ là bằng chứng chắc chắn rằng tin nhắn đã được nhận và gửi bởi máy cụ thể đó. Một lần nữa, các nhà cung cấp có thể xóa các nhật ký đó một cách thường xuyên nếu họ thậm chí còn giữ chúng. Các nhà cung cấp nước ngoài có thể sẽ rất khó đối phó, khiến việc thu thập bằng chứng này khó hơn nhiều.

### 4.6 Đọc tiêu đề e-mail

Tiêu đề e-mail cung cấp bản ghi về đường dẫn mà thư đi từ người gửi đến người nhận (giả sử không thực hiện các bước để thay đổi hoặc xóa nó). Tiêu đề e-mail nên được đọc từ dưới lên trên. Dưới đây là tiêu đề e-mail mẫu từ một tin nhắn mà tôi có thể đã gửi cho người lót đường huyền thoại của Steeler Jack Lambert.

Đã gửi đến:  
 Lambert58@gmail.com

Đã nhận: bởi 11.48.31.1 với id SMTP1 c2ct279nzg; T6, ngày 25 tháng 10 năm 2011

22:38:23 −0800 (PST)

Đường trở lại:

Nhận được tư  
 [mail.emailprovider.com](http://mail.emailprovider.com)  
 (   
[mail.myisp.com](http://mail.myisp.com)  
 [12.34.567.890]) bởi  
 [mx.gmail.com](http://mx.gmail.com)  
 với id SMTP f27se846431anc.2011.10.25.22.38.19; T6, ngày 25 tháng 10 năm 2011 22:38:23 −0800 (PST)

ID thư: <   
20111025233819.47097.mail@mail.myisp.com   
>

Đã nhận: từ [12.34.567.890] bởi  
 [mail.myisp.com](http://mail.myisp.com)  
 qua HTTP; Thứ sáu, ngày 25 tháng 10 năm 2011 22:38:19 PST

Ngày: Thứ Sáu, ngày 25 tháng 10 năm 2011 22:38:19 −0800 (PST)

Người gửi: John Sammons

Chủ đề: Super Bowl

Tới: Jack Lambert

Đã gửi đến:  
 Lambert58@gmail.com

Người nhận tin nhắn

ID thư: <   
20111025233819.47097.mail@mail.myisp.com   
>

Đã nhận: từ [12.34.567.890] bởi  
 [mail.myisp.com](http://mail.myisp.com)  
 qua HTTP; Thứ sáu, ngày 25 tháng 10 năm 2011 22:38:19 PST

Đây là bản ghi của tin nhắn được gửi qua nhà cung cấp email của Jack Lambert   
,  
 [mail.myisp.com](http://mail.myisp.com)   
.

Đã gửi đến:  
 Lambert58@gmail.com

Đã nhận: bởi 11.48.31.1 với id SMTP1 c2ct279nzg; T6, ngày 25 tháng 10 năm 2011 22:38:23 −0800 (PST)

Đường trở lại:

Nhận được tư  
 [mail.emailprovider.com](http://mail.emailprovider.com)  
 (   
[mail.myisp.com](http://mail.myisp.com)  
 [12.34.567.890]) bởi  
 [mx.gmail.com](http://mx.gmail.com)  
 với id SMTP f27se846431anc.2011.10.25.22.38.19; T6, ngày 25 tháng 10 năm 2011 22:38:23 −0800 (PST)

Cuối cùng, tin nhắn được truyền từ nhà cung cấp dịch vụ email của tôi đến tài khoản Gmail của Jack   
,  
 Lambert58@Gmail.com

Lưu ý ID tin nhắn, 20111025233819.47097.mail@mail.myisp.com . Hãy nhớ rằng, đây là một số duy nhất được chỉ định bởi một máy chủ e-mail ( [Google, 2011](#4__Google___2011__September_21) ).

## Các trang web mạng xã hội

E-mail và mạng xã hội có ít nhất một điểm chung. Dường như không có gì mà mọi người sẽ không gửi, đăng hoặc tweet. Thực tế là mọi người dường như đang ở trên Facebook, Twitter hoặc một số hương vị của phương tiện truyền thông xã hội không bị mất đối với cơ quan thực thi pháp luật hoặc các nhà tuyển dụng tiềm năng cho vấn đề đó. Cả hai nhóm đều thường xuyên tìm kiếm trên mạng xã hội để tìm hiểu thêm về những kẻ tình nghi và những nhân viên tiềm năng.

Bằng chứng trên mạng xã hội có thể được tìm thấy ở một số nơi bao gồm máy tính, điện thoại thông minh của nghi phạm và mạng của nhà cung cấp. Lấy bằng chứng từ nhà cung cấp sẽ yêu cầu hành động tương đối nhanh chóng cùng với trát đòi hầu tòa hoặc lệnh khám xét. Hãy nhớ rằng, nhà cung cấp chỉ lưu giữ thông tin này trong một khoảng thời gian nhất định. Tại một số thời điểm, dữ liệu bạn cần sẽ bị xóa mà không có sự can thiệp của pháp luật. Tất cả những điều được xem xét, thu thập bằng chứng từ nhà cung cấp có thể mang lại kết quả tốt nhất.

Khôi phục bằng chứng trên máy cục bộ có thể là một thách thức. Tệp trang (hoặc hoán đổi không gian) là một vị trí có thể kết quả. Các tệp INDEX.DAT cũng có lời hứa. Nhiều hiện vật có thể được tìm thấy ở đây. Email xác nhận (được gửi khi tạo tài khoản) được tìm thấy trong tệp History.IE5 \ Index.dat. Hồ sơ Facebook của người dùng có thể được tìm thấy trên máy cục bộ trong một tệp có tên hồ sơ [#]. Htm. Điều này nằm trong thư mục Content.IE5. Tệp History.IE Index.dat có thể chứa các tìm kiếm bạn bè trên Facebook.

Tài nguyên bổ sung

Lời chứng xét xử Casey Anthony

Phiên tòa xét xử Casey Anthony đã thu hút sự chú ý của giới truyền thông cả nước. Anthony bị buộc tội giết cô con gái nhỏ Caylee. Pháp y kỹ thuật số đóng một vai trò trung tâm trong trường hợp này, đặc biệt liên quan đến các tìm kiếm cho các từ khóa nhất định như “chloroform”. Lời khai xét xử trong vụ án này do giám định viên pháp y vi tính Sgt. Kevin Stenger cung cấp một số lời khai của chuyên gia sâu sắc về pháp y trình duyệt (ví dụ này là Firefox).

<http://www.myfoxorlando.com/dpp/news/060811-kevin-stenger-testifies>

## Bản tóm tắt

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 điều tra chúng ta có thể điều hướng thông qua nó để tìm bất kỳ bằng chứng hiện có nào.

Chúng ta 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 như nội dung “đen”.

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 điều tra nếu được tìm thấy trên máy tính. Hãy nhớ rằng, ghi nhật ký có thể không được bật theo mặc định.

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.

## Tổng kết và kiến thức thêm chương 8

### E-mail

1. **Hiểu được Email Server, Email Clients, và Email Systems là gì, tính chất của chúng**

Email System (hệ thống email) là một cụm máy chủ thực hiện các chức năng truyền và nhận e-mail trẹn môi trường mạng. Ngoài ra, phần mềm giao diện người dùng trên Email (E-mail Clients) sẽ thực hiện những chức năng như cho phép người dùng xem và tạo email mới. Mọi e-mail sẽ được gửi đến một hệ thống máy chủ trung tâm, sau đó sẽ được gửi tới người nhận.

Email client (Phần mềm giao diện người dùng trên Email) hay còn được gọi là mail user agent, là một chương trình máy tính cung cấp những chức năng như truy cập và quản lý e-mail

Email Servers (máy chủ E-mail) là những máy chủ được kết nối và phục vụ cho nhiều e-mail clients (Gồm các thành phần như POP3, SMTP, IMAP)

SMTP – Còn được biết đến với tên Simple Mail Transfer Protocol là một giao thức truyền tải trên mạng được dùng để truyền tải e-mail thông qua mạng sử dụng IP

POP3 – Còn được biết đến với tên Post Office Protocol version 3 là một giao thức truyền tải mạng được dùng để lấy thông tin từ máy chủ

IMAP – Còn được biết đến với tên Internet Message Access Protocol (IMAP) Server là một giao thức truyền tải mạng được dùng để truy cập vào e-mail được lưu trữ trên máy chủ

1. **Hiểu được vai trò của lưu trữ bản nhật ký số**

Quá trình quản lý bản nhật ký số (Electronic Record) là một phần của quản lý hệ thống, chịu trách nhiệm cho việc lưu trữ những thông tin liên quan đến bản nhật ký số như quá trình tạo ra, bảo trì, sử dụng và xóa đi. Ngoài ra, trong quá trình quản lý này, cần phải đảm bảo ghi lại những bằng chứng liên quan đến các bản lưu trữ số.

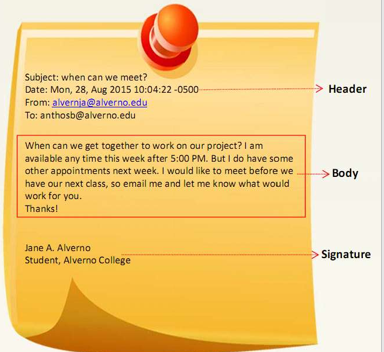
Qúa trình quản lý bản nhật ký số rất quan trọng đối với điều tra số:

* Đảm bảo trong trường hợp cần thiết, những người tham gia trao đổi trên mạng sẽ được ghi lại
* Đảm bảo tính chính xác của thông tin trao đổi thông qua e-mail
* Hỗ trợ truy vết tội phạm hoặc xác định loại hình phạm tội thông qua e-mail

Các loại hình phạm tội thông qua e-mail có thể kể đến như:

* Spamming
* Phising
* Idenity Fraud
* Cyber-stalking

1. **Các thành phần trong một tin nhắn email**



Thông thường, 1 e-mail sẽ có thành phần như:

Header – Chứa những thông tin về e-mail cả về kỹ thuật như Message-id, Priority, IP, lẫn thông tin thông thường như người gửi, người nhận, tiêu đề, thời gian

Body – Chứa nội dụng của e-mail, thông tin, tệp đính kèm.

Signature – Đối với phần chữ ký, thông thường, những phần mềm e-mail có khả năng tự động thêm cho người dùng.

1. **Headers và X-Headers thông dụng**

Headers là tập hợp những header thông dụng như:

Delivered-to

Received

Return-Path

Authentication-Result

X-Headers là tập hợp những thông tin mở rộng từ header thông thường như:

X-Confirm-Reading-To

X-Errors-To

1. **Các bước điều tra e-mail**
2. Hoàn thiện thủ tục liên quan đến luật pháp
3. Xem xét và điều tra nội dung e-mail
4. Sao lưu và ghi lại nội dụng
5. Xem xét e-mail headers
6. Phân tích e-mail headers
7. Truy ngược lại e-mail
8. Thu được những mảnh thông tin
9. Kiểm tra nhật ký e-mail
10. **Các công cụ**

Recover My Email – Được sử dụng nhằm khôi phục những e-mail bị xóa từ Microsoft Outlook

MailXaminer – Kiểm tra, báo cáo và truy xuất những e-mail đáng ngờ

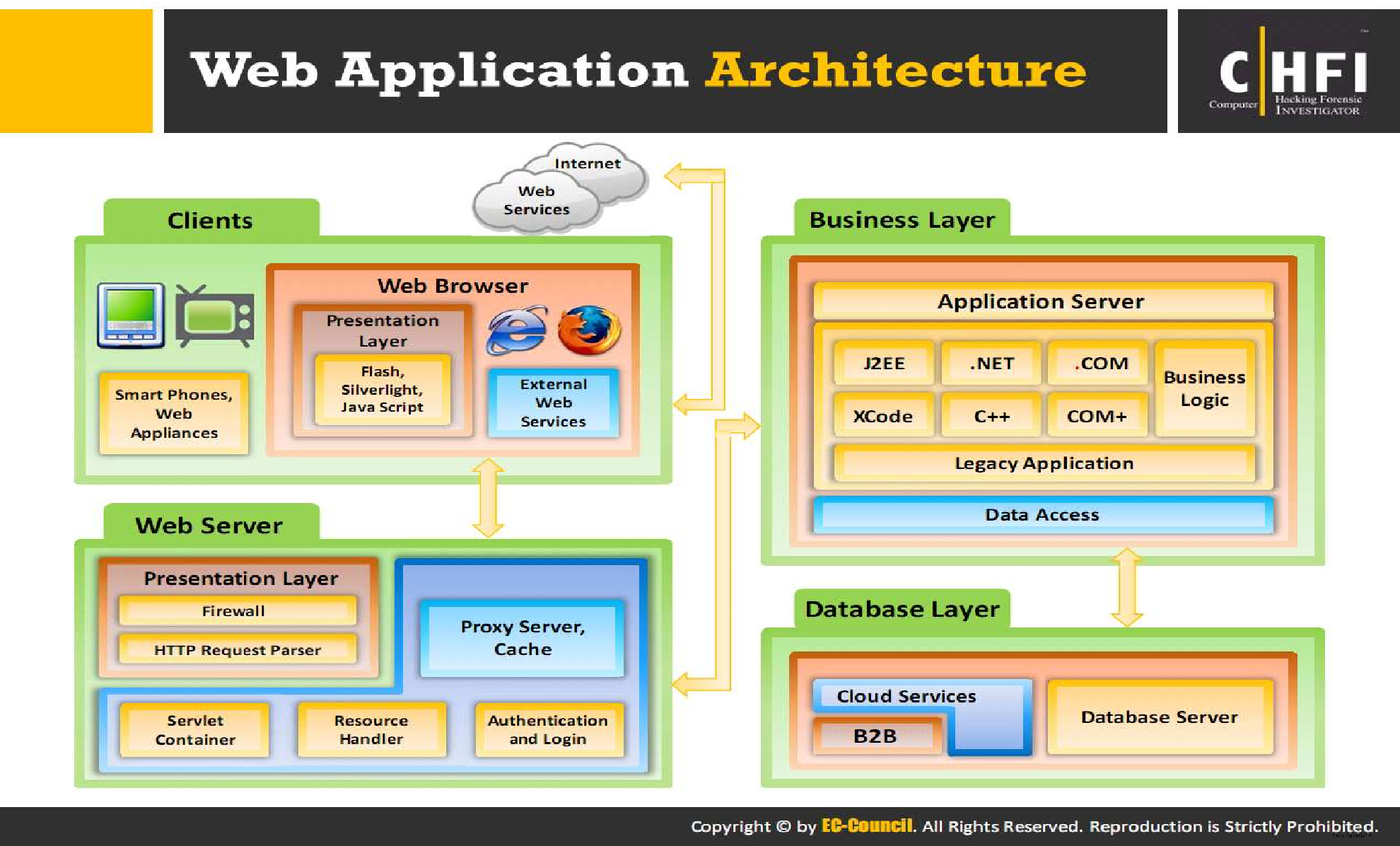
### Internet/browser

1. **Hiểu được mục tiêu của điều tra web**

Ứng dụng Web được hiểu như là màn hình giao diện phục vụ mục đích thao tác giữa người dùng và máy chủ web thông qua các tập trang web được tạo ra từ máy chủ hoặc những đoạn mã được chạy trên trình duyệt web

Mục tiêu của điều tra web là thu thập và phân tích nhật ký và các mảnh bằng chứng từ quá trình web request. Các thông tin, vật chứng được thu thập gồm máy chủ web, máy chủ ứng dụng, máy chủ database, sự kiện trên web, hệ thống nhằm kiếm được bằng chứng, phương pháp tội phạm đã dùng để xâm nhập, tấn công ứng dụng web.

1. **Biết được cấu trúc của web và các khó khăn liên quan**



Ghi chú:

**Người dùng – Clients**

Chức năng: Thao tác với Web Server thông qua giao diện trên trình duyệt Web

**Máy chủ web - Web Server**

Chức năng: Presentation Layer – Nhận request từ Web Browser, Firewall ngăn chặn xâm nhập bhp

Proxy Server, Cache – Lấy thông tin từ máy chủ ứng dụng, xác thực, định danh người dùng

**Lớp chức năng – Business Layer**

Application Server – Chứa mã code, chương trình, ứng dụng

Data Access – Kết nối với lớp Database để lấy dữ liệu được lưu trữ

**Lớp Dữ Liệu – Database Layer**

Database Server – Chứa các dữ liệu liên quan đến người dùng, ứng dụng, …

Khó khăn:

Cấu trúc của một web thường được cấu tạo nên từ nhiều phần khác nhau

* Cần kiểm tra mọi hệ thống cũng như dữ liệu liên quan

Thông thường, với những doanh nghiệp, web gần như luôn luôn phải vận hành

* Điều tra viên sẽ không được ngưng vận hành web lại để kiểm tra

Trong trường hợp người truy cập dùng proxies, vpn, hoặc trình duyệt có khả năng che dấu danh tính, sẽ rất khó để điều tra viên truy ngược lại

1. **Các dấu hiệu, phương pháp liên quan đến tấn công web**

Các phương pháp tấn công web:

* Cookie Poisoning
* Log Tampering
* Buffer Overflow
* DDos
* SQL Injection
* Cross Site Scripting (XSS)
* Cross Site Request Forgery
* Unvalidated Input
* Cookie Snooping
* Network Access Attacks

Các dấu hiệu web bị tấn công:

* Người dùng không thể truy cập web
* Bị dẫn hướng đến trang khác
* Các lỗi hiển thi trên web như 500 error, 100 errors, 101 error
* Máy chủ web thường xuyên bị khởi động lại
* Các sự kiện bất thường liên quan đến hoạt động của người dùng

1. **Các bước điều tra web**
2. Xác định sự cố xảy ra và tính chất của sự cố thông qua công cụ SIEM, Syslog
3. Thu thập thông tin như dịch vụ, các yêu cầu đang thực hiện, ports, kết nối mạng, người dùng đang đăng nhập
4. Nếu hệ thống trên máy ảo, lưu lại hình ảnh. Nếu hệ thống trên máy vật lý, thu thập thông tin sống và tắt máy chủ. Đồng thời chạy các máy chủ backup
5. Sao y lại ổ cứng đối với máy chủ vật lý hoặc sao lưu lại hình ảnh đối với hệ thống trên máy ảo
6. Phân tích cách vận hành của Web
7. Phân tích nhật ký từ web server, application server, database server, ứng dụng, và các sự kiện trong hệ thống nhằm kiếm được các hành động, sự kiện bất thường
8. Kiểm tra các cấu hình của máy chủ và ứng dụng
9. Phân tích các sự kiện, cấu hình, hành động bất thường
10. Kiểm tra các nhật ký, thông báo từ firewall và IDS
11. Ghi lại các IP đáng ngờ và ngắt kết nối, ghi vào blacklist
12. Trong một số trường hợp, nếu có thể, truy ngược lại bằng lệnh tracert
13. Hồ sơ hóa toàn bộ bằng chứng, quá trình
14. **Phương pháp điều tra web được host trên Windows servers**
15. Sử dụng event Viewer để kiểm tra log
16. Kiểm tra các hành động (Các sự kiện nhật ký bị tắt, Windows Defender, firewall, MS telnet Service)
17. Những cố gắng truy cập hoặc truy cập khóa
18. Sử dụng lệnh net và netstat
19. **Hiểu được IIS là gì và cách điều tra nhật ký IIS**

IIS (Internet Information Services) là dịch vụ của Windows Server được sử dụng để chứa thông tin, dữ liệu phục vụ mục đích host web

Nhật ký IIS ghi lại tất cả hành động, người dùng truy cập, yêu cầu thông tin từ hệ thống.

Những thông tin được ghi lại trong nhật ký IIS thông thường bảo gồm:

Thời gian kết nối

Địa chỉ IP của người dùng

Tên tài khoản người dùng

Địa chỉ trang web

Và các hành động như GET, POST, REQUEST

Phương pháp đảm bảo giá trị của nhật ký IIS

Khi điều tra nhật ký IIS, điều tra viên cần cẩn thận và xem như nhật ký IIS này sẽ là bằng chứng số

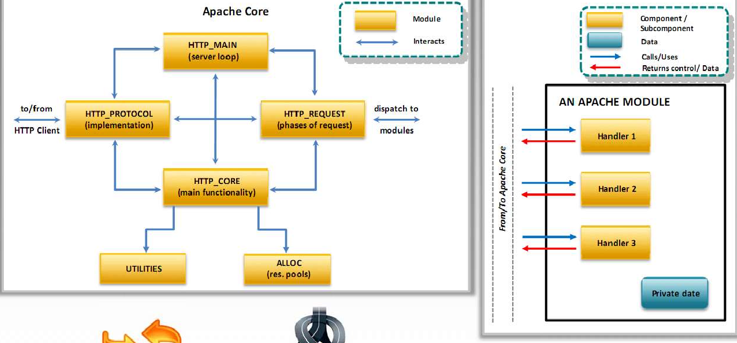
Bằng cách sử dụng nhật ký từ IIS, Firewall, IDS, và TCPdump thì điều tra viên sẽ dễ dàng điều tra nguồn cũng như tội phạm

Đảm bảo cấu hình nhật ký IIS

Thu thập rõ ràng bằng chứng thời gian

Kiểm tra vận hành của nhật ký

1. **Hiểu được Apache web server là gì và cách điều tra nhật ký**



Apache Core gồm:

HTTP\_Main: Khởi động server, tạo vòng lặp để kiểm soát, thiết lập các kết nối cũng như thông báo trong trường hợp client, người dùng không thể kết nối hoặc không được phép kết nối

HTTP\_Protocol: Trao đổi, giao tiếp dữ liệu với các người dùng, client thông qua giao thức

HTTP\_REQUEST: Quản lý các lỗi xảy ra trong quá trình trao đổi dữ liểu, xử lý các lệnh request, và đảm bảo các module được chuyển giao theo thứ tự và phù hợp.

HTTP\_CORE: Các chức năng của Apache (alloc – kiểm soát phân chiua tài nguyên)

Apache HTTP Server là một Web Server có khả năng hỗ trợ nhiều hệ diều hành như Unix, Windows, Linux, Mac OS X, vv

Nhật ký từ Apache server chứa những thông tin liên quan đến hành động trên trang web như:

Địa chỉ IP của người dùng

Địa chỉ MAC của thiết bị

Thời gian

Code trạng thái

Apache Log Format:

Log Format “%h, %l, %u, %t”

Log/access\_log

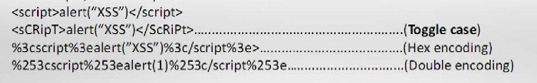
1. **Điều tra các cuộc tấn công trên web**

**Điều tra Cross-site scripting XSS**

Phương pháp XSS: sử dụng các HTML tag liên quan để thực hiện các lệnh <script></script>, <IMG>, <Input>, etc

Tội phạm sử dụng các công cụ để làm nhiễu loạn khả năng theo dõi của tường lửa và IDS/IPS như mã hóa hex, Viết hoa, viết theo hex

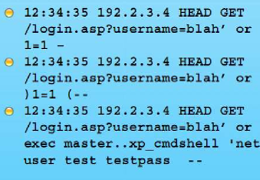
VD:



Với những công cụ hiện này, điều tra viên có thể dễ dàng kiểm tra và phát hiện cách thức này thông qua kiểm tra lại nhật ký truy cập web.

**Điều tra SQL injection**

Thông thường, bằng cách kiểm tra các nhật ký từ IDS, máy chủ web, và máy chủ dữ liệu sẽ lưu lại hành đồng SQL injection.



**Điều tra code injection**

Với những công cụ IDS, firewall, filter, thì việc thực hiện code injection sẽ khó khăn hơn khi trước. Thông thường, IDS sẽ cảnh báo trong trường hợp có quá nhiều mã lệnh ngoài luồng yêu cầu web server thực hiện, thông thường các lệnh này sẽ nằm trong các yêu cầu như Post, GET, Request.

**Điều tra Cookie Poisioning**

Đối vời phương pháp Cookie poisioning, tội phạm sẽ thay đổi thông tin của cookie bị lấy cắp như tên, giá trị, địa chỉ IP gắn liền, thời gian, và phiên làm việc. Do đó, khi sử dụng công cụ kiểm tra lại các cookies được lưu lại trong hệ thống, ta sẽ thấy được sự khác biệt với thông tin giữa 2 cookie này.

### Database

1. **Hiểu được vai trò của điều tra database**

Điều tra database là hành động kiểm tra database, những metadata liên quan nhằm tìm kiếm được bằng chứng số. Những hành động thường được thực hiện trong điều tra database là:

1. Kiểm tra MAC attributes of tables để xác định hành động của tin tặc
2. Phát hiện các trao đổi, giao tiếp bất thường
3. Hồi phục các dòng thông tin bị xóa
4. Kiểm tra lại vận hành DDL và DML
5. **Điều tra MSSQL**

SQL server lưu trữ thông tin và nhật ký trong Primary Data Files (MDF), Secondary Data Files (NDF) và Transaction Log Data Files (LDF).

MDF – là vùng đầu tiên của database, chuyên lưu trữ thông tin người dùng và database objects

NDF – là vùng tuy chọn, được dùng để phân chia các thông tin ra các database khác

LDF – lưu trữ các thông tin liên quan đến nhật ký, trong một số trường hợp, các thông tin này có thể được dùng để khôi phục database. Những thông tin này được chia nhỏ gọi là virtual log files (tệp tin nhật ký ảo)

Tất cả các tệp tin này được kết hợp lại để tạo nên một database

Mỗi một tệp thông tin (trừ các tệp nhật ký) chứa nhiều trang thông tin

Trang thông tin bao gồm:

Page Header – Gồm ID trang, loại trang

Data Row – Chứa thông tin

Offset Table – Đường dẫn tới thông tin

1. **Xác định các bằng chứng số liên quan**

Thông tin mấy chủ SQL được lưu giữ bên trong SQL Server, và trên thiết bị Windows host server ấy. Thông thường, những bằng chứng điều tra viên có thể kiếm được là:

**SQL Server**

Volatile database – Thông tin sống

Primary data file and Active Transaction Logs – MDF và LDF

Database plan cache – các tệp thông tin

**Windows Operating System (OS)**

Windows logs – Nhật ký windows

SQL Server Trace Files - Các dấu vết từ SQL Server

SQL Server Error – Thông báo lỗi từ SQL Server

1. **Thu thập bằng chứng thông qua SQL Server Management Studio**

Bước 1: Kiểm tra Windows Log

Kiểm tra các nhật ký Windows nhằm thu thập các thông tin như xác thực, thay đổi trạng thái, và địa chỉ IP của các người dùng

Bước 2: Kiểm tra nhật ký lỗi

Mở ErrorLog từ C:\ProgramFiles\Microsoft SQLServer\MSSQL11.MSSQLSERVER\MSSQL\LOG

Xem các thông báo có người dùng khác truy cập vào hệ thống không

Bước 3: Kiểm tra tệp tin sự kiện

Mở log\_n.trc từ C:\ProgramFiles\MicrosoftSQLServer\MSSQL.1\MSSQL\LOG

Xem các thông báo có hành động bất thường nào không

Bước 4: Kiểm tra các giao tiếp đang hoạt động

Bước 5: kiểm tra trang thông tin (data page)

Bước 6: Kiểm tra object ID liên quan đến sự kiện

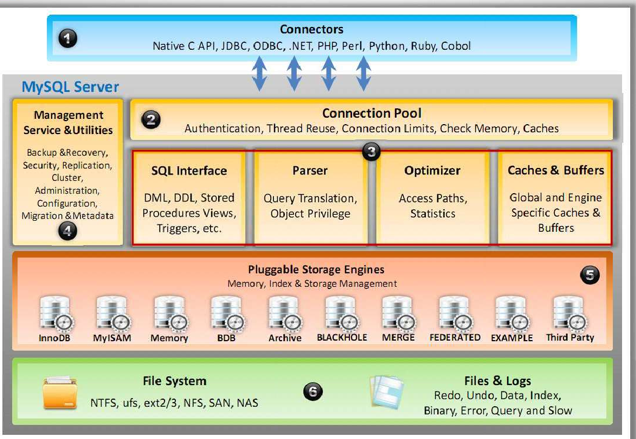
Bước 7: Thu thập và lập bản ghi lại thông tin liên quan đến object ID đó

Bước 8: Kiểm tra nhật ký đã được chỉnh sửa

Bước 9: Xác định loại hình thông tin

Bước 10: So sánh các dòng thông tin nhật ký

1. **Các thức điều tra MySQL**
2. **Cấu trúc của MySQL**



Connectors – Hoạt động như mốc nối để người dùng kết nối với SQL server

Connection Pool – Phụ trách cho kết nối với người dùng như xác thực người dùng, kiểm tra bộ nhớ, quản lý cache

Management Service & Utilities - Cụm công cụ hỗ trợ cho quản trị viên và dịch vụ của doanh nghiệp

Cụm vận hành của My SQL

SQL Interface – UI phụ trách giao tiếp giữa người dùng và hệ thống SQL

Parser – Kiểm tra các thông tin được nhập vào SQL

Query Optimizer – Lọc các yêu cầu, hành động bất thường

Query Execution – Thực hiện yêu cầu và trả về kết quả thông qua giao tiếp

Query Cache – lưu lại cấu trúc và kết quả của yêu cầu

Cache and Buffers – Đảm bảo tính sẵn sàng của hệ thống

Storage enginers – có chức năng là tạo, đọc và nâng cấp thông tin trong database

1. **Các ứng dụng của MySQL được dùng trong điều tra số**

Mysqldump – Dump một hoặc nhiều database nhằm phục vụ mục địch khôi phục thông tin

Mysqlaccess – Kiểm tra các quyền truy cập

Myisamlog – Kiểm tra quá trình hồi phục, phiên bản hệ thống

Myisamchk – Xác định MyISAM table bị lỗi, sửa lỗi cho các bảng ấy

Mysqlbinlog – Hiển thị các nội dung trong bin logs qua dạng văn bản

Mysqldbexport – Truy xuất metada hoặc thông tin, hoặc cả hai từ 1 hoặc nhiều nguồn database

Tài liệu tham khảo

1. Casey E. Sổ tay Điều tra và Pháp y Kỹ thuật số Burlington, MA: Academic Press; Năm 2009.

2. Casey E. Bằng chứng Kỹ thuật số và Tội phạm Máy tính: Khoa học Pháp y, Máy tính và Internet Waltham, MA: Báo chí Học thuật; 2011.

3. EI du Pont de Nemours and Company v. Kolon Industries , Inc., 2011 US Dist. LEXIS 45888 (ED Va. Ngày 27 tháng 4 năm 2011).

4. Google. (2011, ngày 21 tháng 9). Đọc tiêu đề email đầy đủ . Được truy cập ngày 24 tháng 10 năm 2011, từ: [http://mail.google.com/support/bin/answer.py?hl=vi&answer=29436](http://mail.google.com/support/bin/answer.py?hl=en%26answer=29436) .

5. Giải pháp mạng, LLC. (nd). WHOIS đằng sau tên miền đó? Truy cập ngày 13 tháng 10 năm 2011, từ: <http://www.networksolutions.com/whois/index.jsp>.

6. Dữ liệu Refsnes. (nd). Giới thiệu HTML . Truy cập ngày 13 tháng 10 năm 2011, từ: <http://www.w3schools.com/html/html_intro.asp>.

# Chương 9: Pháp y mạng

**Thông tin trong Chương này:**

Các nguyên tắc cơ bản về mạng



Các loại mạng



Công cụ bảo mật mạng



Tấn công mạng



Ứng phó sự cố



Điều tra & Bằng chứng Mạng



Chương này khám phá các nguyên tắc cơ bản về mạng, các cuộc tấn công và hack phổ biến cũng như ứng phó sự cố. Nó bao gồm cả an ninh mạng và các công cụ điều tra. Các bằng chứng và thách thức mạng cũng được giải quyết.

Giao thức điều khiển truyền / Giao thức Internet (TCP / IP), Mạng máy khách / máy chủ, Mạng ngang hàng (P2P), Mạng cục bộ (LAN), Mạng diện rộng (WAN), MAN (Mạng khu vực đô thị), PAN (Cá nhân Mạng khu vực), CAN (Mạng khu vực cơ sở), GAN (Mạng khu vực toàn cầu), địa chỉ IP, Chuyển mạch gói, Điều tra dự phòng theo chu kỳ (CRC), Cầu bộ định tuyến, Cổng, Giao thức truyền siêu văn bản (HTTP), Giao thức Bưu điện 3 (POP3) , Giao thức truyền thư đơn giản (SMTP), Hệ thống phát hiện xâm nhập (IDS), Hệ thống phát hiện xâm nhập mạng (NIDS), Từ chối dịch vụ phân tán (DDoS), Giả mạo danh tính (IP Spoofing), Tấn công người trung gian, Xã hội Kỹ thuật, Dấu chân / Vân tay, Sniffer, Tường lửa

## Giới thiệu

Có vẻ như hầu như không ngày nào trôi qua mà một công ty lớn hoặc tổ chức chính phủ không báo cáo về một sự xâm nhập mạng đáng kể nào đó. Lấy ví dụ như Fidelity National Information Services Inc. (FIS). Bộ xử lý thẻ tín dụng trả trước của Jacksonville đã báo cáo rằng một doanh nghiệp tội phạm quốc tế đã đánh cắp 13 triệu đô la chỉ trong một ngày trong năm 2011. Họ đã tiết lộ hành vi trộm cắp trong báo cáo thu nhập quý đầu tiên được công bố vào ngày 3 tháng 5 năm 2011. Các tin tặc đã thực hiện một kế hoạch cao và ... hoạt động phối hợp liên quan đến các máy ATM từ khắp nơi trên thế giới cùng với thẻ tín dụng trả trước bị đánh cắp (Krebs). FIS chỉ là một trong số rất nhiều nạn nhân của những tội ác như thế này.

Những gì bắt đầu như một nền văn hóa con được thúc đẩy đơn giản bằng cách vượt qua thách thức mà hack được đưa ra nay đã phát triển thành một mối đe dọa đáng kể và nham hiểm hơn nhiều, đến mức giờ đây nó là một vấn đề quan trọng của an ninh quốc gia. Vì vậy, phần lớn cơ sở hạ tầng quan trọng của quốc gia phụ thuộc vào các mạng và thiết bị kỹ thuật số. Chắc chắn không thiếu những mục tiêu cao cấp. Chúng bao gồm các cơ quan chính phủ, lưới điện và các ngành tài chính và chăm sóc sức khỏe. Mối đe dọa này hiện bao gồm các quốc gia, các doanh nghiệp tội phạm có tổ chức, những kẻ khủng bố, cũng như các cá nhân.

Khu vực tư nhân chịu một phần trách nhiệm đáng kể trong việc bảo vệ các mạng lưới này. Vì vậy, làm thế nào để pháp y kỹ thuật số tìm ra tất cả những điều này? Pháp y kỹ thuật số có thể đóng một số vai trò:

Điều tra mạng có một số rào cản cố hữu không phát huy tác dụng trong cuộc điều tra tập trung vào một máy tính độc lập. Không giống như một máy duy nhất, dữ liệu (bằng chứng) có thể được trải rộng trên nhiều máy hoặc thiết bị. Để làm phức tạp thêm mọi thứ, chúng cũng có thể được trải rộng trên một khu vực địa lý rộng lớn. Lượng dữ liệu tuyệt đối có thể liên quan lại đưa ra một thách thức khác. Tùy thuộc vào quy mô của tổ chức và mạng của nó, khối lượng dữ liệu có thể đạt đến tỷ lệ thực sự thiên văn.

Tin tặc có nhiều lựa chọn tấn công theo ý của họ khi tấn công mạng. Các cuộc tấn công có thể khá phức tạp hoặc đơn giản đến kinh ngạc. Một số cuộc tấn công dựa vào các lỗ hổng trong công nghệ; những người khác dựa vào những điểm yếu được tìm thấy ở con người. Phần mềm là một trong những ví dụ về điểm yếu của công nghệ. Flaws trong phần mềm được tìm thấy trong mã bên dưới. Các lỗi này được xác định bởi các nhà phát triển phần mềm, chuyên gia bảo mật hoặc những người khác. Sau đó, tin tặc phát triển các khai thác để tận dụng lỗ hổng. Hy vọng rằng nhà phát triển phần mềm sẽ lưu ý và khắc phục sự cố sớm hơn là muộn. Chúng thường ở dạng “bản vá”. Đây là một cuộc đấu tranh liên tục dường như không bao giờ kết thúc.

Sự yếu kém của con người cũng góp phần vào thành công của hacker theo một số cách. Đầu tiên, mọi người có xu hướng sử dụng mật khẩu yếu. Chúng có xu hướng quá ngắn hoặc quá dễ đoán. Ví dụ, họ sử dụng tên của vật nuôi hoặc trẻ em của họ hoặc họ sử dụng các từ thực tế có thể tìm thấy trong từ điển. Cuối cùng, ngay cả khi mật khẩu mạnh, họ có thể để mật khẩu được viết ra rất gần máy tính. Thứ hai, người dùng không nghi ngờ có thể trở thành con mồi của một cuộc tấn công kỹ thuật xã hội .

### 1.1 Kỹ thuật xã hội

Trong một cuộc tấn công kỹ thuật xã hội, một người dùng được ủy quyền bị thuyết phục bởi một cá nhân không được phép tiết lộ thông tin nhạy cảm. Các cuộc tấn công phổ biến bao gồm tin tặc đóng giả là nhân viên, khách hàng hoặc nhà tư vấn bảo mật.

Các cuộc tấn công khác nhau này cũng có thể được tiến hành kết hợp, tận dụng các lỗ hổng của cả công nghệ và những người kiểm soát nó.

## Các nguyên tắc cơ bản về mạng

Kết nối mạng hoặc liên kết các máy tính với nhau có một số lợi thế riêng biệt. Chia sẻ tài nguyên và cộng tác chỉ là hai lợi ích như vậy.

Một mạng có một số nhu cầu cơ bản được yêu cầu bất kể quy mô hoặc mục đích của nó. Đầu tiên là một số kiểu kết nối giữa các máy tính hoặc thiết bị. Kết nối này có thể là kết nối vật lý (chẳng hạn như qua cáp Ethernet) hoặc không dây. Tiếp theo, mạng phải có một cách thiết lập để giao tiếp. Ngôn ngữ chung này, hoặc tập hợp các quy tắc, được gọi là một giao thức. Giao thức điều khiển truyền / Giao thức Internet (TCP / IP) là một giao thức mạng được sử dụng rất phổ biến và cũng là giao thức được sử dụng trên Internet.

Để đặt nền tảng, chúng ta sẽ bắt đầu bằng cách xác định và xác định các loại mạng khác nhau đang được sử dụng phổ biến hiện nay. Cho đến nay, loại mạng phổ biến nhất gặp phải trong thiết lập thương mại là máy khách / máy chủ. Trong mạng máy khách / máy chủ , mỗi máy tính trên mạng được gán một trong hai vai trò này. Khách hàng được sử dụng bởi người dùng cuối, chẳng hạn như máy trạm trên bàn làm việc của bạn. Các máy này yêu cầu tệp, dịch vụ và thông tin từ máy chủ. Ngược lại, máy chủ lưu trữ và cung cấp tệp, dịch vụ và thông tin cho nhiều máy khách. Về bản chất, bạn có thể có một máy chủ chia sẻ tệp với hàng trăm máy khách. Họ có nhiều quyền kiểm soát hơn trên mạng. Máy chủ có xu hướng hoạt động theo (các) vai trò cụ thể. Máy chủ tệp, máy chủ e-mail và máy chủ in chỉ là một vài ví dụ.

Cấu hình mạng khác thường được sử dụng được gọi là mạng ngang hàng (P2P ). Như tên cho thấy, tất cả các máy trên mạng có thể / làm được chức năng của cả máy khách và máy chủ. Mạng P2P hiếm khi được sử dụng trong môi trường thương mại. Chia sẻ tệp là cách sử dụng chủ yếu của mạng P2P. Nhạc, phim và phần mềm là một số tệp được chia sẻ phổ biến hơn. Thật không may, P2P cũng là một đường dẫn chính cho không chỉ nhạc, video và phần mềm vi phạm bản quyền mà còn cả nội dung “đen”. Đây là một vấn đề lớn không chỉ ở Hoa Kỳ mà còn trên toàn thế giới.

Bây giờ chúng ta đã hiểu cơ bản về cách các mạng được tổ chức, hãy cùng xem cách các mạng này có thể được phân loại.

### 2.1 Các loại mạng

Mạng cục bộ hay mạng LAN thường được coi là mạng văn phòng nhỏ nhất. Nó bao gồm các máy tính và thiết bị trong một văn phòng hoặc tòa nhà. Mạng diện rộng (WAN) lớn hơn, đôi khi là đáng kể. Một mạng WAN bao gồm hoặc các mạng LAN ở các vị trí khác nhau. Mạng WAN có thể được trải rộng trên những khoảng cách xa. Các loại mạng khác bao gồm MAN (Mạng Khu vực Đô thị ), PAN (Mạng Khu vực Cá nhân ), CANs (Mạng Khu vực Cơ sở) và GAN (Mạng Khu vực Toàn cầu ).

Ngược lại với Internet là mạng nội bộ. Mạng nội bộ của một công ty là riêng tư và quyền truy cập vào nó bị hạn chế. Mạng nội bộ thường được sử dụng để chia sẻ tệp, giao tiếp, v.v. Một mạng nội bộ hoạt động giống như Internet, sử dụng các trình duyệt web và thường là cùng một giao thức (TCP / IP).

Trên mạng sử dụng giao thức TCP / IP, mỗi máy tính hoặc thiết bị trên mạng có một định danh hoặc địa chỉ duy nhất được gọi là địa chỉ IP . Địa chỉ IP được sử dụng để gửi tin nhắn và dữ liệu đến đích thích hợp của nó, hoạt động giống như một địa chỉ đường phố. Có hai phiên bản địa chỉ IP mà chúng ta cần quan tâm: phiên bản 4 và phiên bản 6. IPv4 đang bị loại bỏ dần vì số lượng địa chỉ tương đối nhỏ so với số lượng đáng kinh ngạc của các thiết bị và máy tính trên Internet. Đơn giản là chúng ta sắp hết địa chỉ. IPv4 cung cấp khoảng bốn tỷ địa chỉ IP khác nhau. Nó đang được thay thế bằng IPv6. Ngược lại, IPv6 cung cấp cho tất cả các mục đích và mục đích một số lượng địa chỉ vô hạn (Tập đoàn Microsoft).

Địa chỉ IPv4 được tạo thành từ bốn số được phân tách bằng dấu chấm. Mỗi số trong số bốn số này, được gọi là octet, có thể nằm trong khoảng từ 0 đến 255. Một địa chỉ IPv4 điển hình sẽ có dạng như sau: 198.122.55.16. Địa chỉ IPv6 sẽ giống như sau:

Năm 2008: 0eb3: 29a2: 0000: 0000: 8c1d: 0967: 7256.

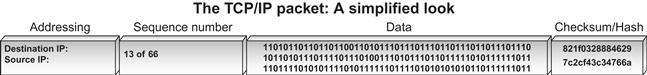
Để so sánh, nếu bạn viết địa chỉ IPv6 bằng ký hiệu IPv4, nó sẽ giống như sau:

65535.65535.65535.65535.65535.65535.65535.65535 ( [Nikkel, 2007](#14__Nikkel__B__J___2007___An_Int) )

Địa chỉ IP có thể là tĩnh hoặc động. Địa chỉ tĩnh thường cố định và không thay đổi. Ngược lại, một địa chỉ động thay đổi thường xuyên. Ví dụ: một số Nhà cung cấp dịch vụ Internet (ISP) sử dụng địa chỉ IP động. Tại đây, mỗi khi bạn đăng nhập, mạng sẽ gán cho bạn một địa chỉ IP từ một nhóm các địa chỉ hiện chưa được gán. Điều này cho phép nhà cung cấp phục vụ một số lượng lớn khách hàng trong số lượng địa chỉ IP cố định mà họ kiểm soát. Điều này hoạt động vì không phải tất cả người đăng ký của họ sẽ trực tuyến vào bất kỳ thời điểm nào.

Dữ liệu trên mạng có thể di chuyển theo nhiều cách khác nhau. Chuyển mạch gói được sử dụng trên Internet và nhiều mạng khác. Chuyển đổi gói chia nhỏ dữ liệu thành các phần nhỏ được gọi là gói. Sau đó, các gói này di chuyển mạng đến đích cuối cùng của chúng bằng cách sử dụng địa chỉ IP.

Mỗi gói được cấu trúc một cách thống nhất. Các gói riêng lẻ bao gồm ba phần; đầu trang, tải trọng và chân trang. Tiêu đề chứa thông tin địa chỉ, xác định địa chỉ IP của người gửi và người nhận. Tiếp theo, gói tin tự nhận dạng chính nó so với tổng số gói. Một cái gì đó như "Tôi gói 26 trong số 234." Sau đó đến tải trọng của chính nó. Cuối cùng, gói tin được kết thúc bằng footer hoặc trailer. Đoạn giới thiệu cho người nhận biết rằng đây là phần cuối của gói tin. Nó cũng tiến hành điều tra dự phòng theo chu kỳ (CRC). CRC là tổng của tất cả những cái trong gói. Nếu các số không khớp, máy tính nhận sẽ tự động gửi lại yêu cầu. Nó được sử dụng để xác minh tính toàn vẹn của gói tin. [Hình 9.1](#F0010_8) mô tả tổ chức của một gói TCP / IP.



Hình 9.1 Một gói IP điển hình. Hình minh họa của Jonathan Sisson.

Mạng thường bao gồm phần cứng ngoài máy tính và máy chủ. Những thiết bị này cũng quan trọng từ góc độ điều tra vì chúng có thể chứa bằng chứng có giá trị.

Cổng là một điểm mạng hoạt động như một lối vào mạng khác ( [TechTarget, 2000](#18__TechTarget___2000__August) ). Ngược lại, một cây cầu được sử dụng để kết nối hai mạng sử dụng cùng một giao thức. Bộ định tuyến hướng dữ liệu, sử dụng địa chỉ IP, trên mạng đến đích cuối cùng của chúng.

## Công cụ bảo mật mạng

Về bảo mật, cách tiếp cận tốt nhất (và thực tế nhất) là chuẩn bị “khi nào” có xâm nhập trái ngược với “nếu” có xâm nhập. Làm việc trên giả định rằng bạn sẽ có thể ngăn chặn tất cả các hacker đã cam kết là không thực tế. Điều đó có nghĩa là các tổ chức chỉ nên thực hiện các biện pháp tối thiểu để bảo vệ mạng của họ, tập trung nhiều nguồn lực hơn vào ứng phó hơn là phòng ngừa? Tuyệt đối không. Luôn luôn phải sử dụng một hệ thống phòng thủ chu vi mạnh mẽ, phạm vi của nó thường được quyết định bởi ngân sách sẵn có và nhân sự cần thiết để điều hành nó.

May mắn thay, có nhiều công cụ phần cứng và phần mềm có thể giúp bảo vệ mạng của chúng ta. Những công cụ này không chỉ phục vụ để ngăn chặn một cuộc tấn công thành công, chúng còn có thể chứa thông tin có giá trị điều tra. Hãy xem xét một vài công cụ này.

Tường lửa là “một tập hợp các chương trình liên quan, đặt tại một máy chủ cổng mạng, bảo vệ tài nguyên của mạng riêng khỏi người dùng từ các mạng khác” ( [TechTarget, 2000](#19__TechTarget___2000__October) ). Tường lửa hoạt động như một bộ lọc cho cả lưu lượng mạng đến và đi. Nó quyết định có cho phép lưu lượng đi qua hay không sau khi điều tra cẩn thận các gói mạng.

Mục đích của Hệ thống phát hiện xâm nhập (IDS) là để phát hiện các cuộc tấn công từ bên ngoài và bên trong một tổ chức. IDS thường giám sát một mạng để tìm kiếm một dạng tấn công mạng được công nhận cũng như các hành động và hoạt động bất thường của hệ thống và người dùng ( [TechTarget, 2000](#19__TechTarget___2000__October) ). Snort là một hệ thống phát hiện xâm nhập mạng mã nguồn mở (NIDS) nổi tiếng . Snort hoạt động như một bộ dò tìm , theo dõi mạng trong thời gian thực và đưa ra các cảnh báo nếu một vấn đề tiềm ẩn được xác định ( [TechTarget, 2002](#21__TechTarget___2002__January) ).

## Tấn công mạng

Có nhiều cách khác nhau để hack và / hoặc tấn công mạng. Những cuộc tấn công này thay đổi với tốc độ tương tự như tốc độ "warp", dẫn đến sự căng thẳng liên tục trong ngành bảo mật. Dưới đây chỉ là một số cuộc tấn công đang được sử dụng ngày nay.

Từ chối dịch vụ phân tán (DDoS) —Tấn công này sử dụng số lượng lớn các máy tính bị xâm nhập để tấn công một hệ thống duy nhất. Các máy tính tấn công áp đảo mục tiêu với số lượng lớn các tin nhắn và yêu cầu. Mục tiêu chỉ đơn giản là không thể đối phó với khối lượng lớn lưu lượng truy cập vào và cuối cùng bị khóa, đóng cửa. “Đội quân” máy tính tấn công được gọi là “mạng botnet”, bao gồm các hệ thống bị xâm nhập riêng lẻ được gọi là “thây ma”.

Giả mạo danh tính (IP Spoofing) - Kẻ tấn công có thể giả mạo hoặc “giả mạo” một địa chỉ IP hợp lệ hoặc “đã biết” để có được quyền truy cập vào một mạng được nhắm mục tiêu.

Man-In-The-Middle-Attack— Trong cuộc tấn công này, tin tặc tự chèn mình vào giữa bạn và người hoặc thực thể mà bạn đang giao tiếp. Thông tin liên lạc của bạn sau đó có thể được theo dõi, thay đổi hoặc xóa. Điều này cũng có thể cho phép kẻ tấn công mạo danh bạn.

Kỹ thuật xã hội là một trong những cách tấn công hiệu quả nhất theo ý đồ của hacker. Kỹ thuật xã hội thường được mô tả là thu thập thông tin được bảo vệ bằng cách “lừa” hoặc “lừa”. TechTarget định nghĩa kỹ thuật xã hội theo cách này: “một thuật ngữ mô tả kiểu xâm nhập phi kỹ thuật chủ yếu dựa vào sự tương tác của con người và thường liên quan đến việc lừa người khác phá vỡ các quy trình bảo mật thông thường” ( [TechTarget, 2001](#20__TechTarget___2001__March___S) ). Tin tặc huyền thoại Kevin Mitnick đã sử dụng rộng rãi kỹ thuật này với thành công vang dội ( [Mitnick, 2011](#12__Mitnick_K__Ghost_in_the_Wire) ).

Đây chỉ là một trong số rất nhiều ví dụ về thành công của Mitnick: Mitnick gọi đến trung tâm điều hành mạng của một công ty điện thoại di động trong một trận bão tuyết. Sau khi kết bạn với một trong những nhà điều hành, anh ta hỏi họ: “Tôi để thẻ SecureID trên bàn làm việc. Bạn sẽ lấy nó cho tôi? " Tất nhiên, các nhà khai thác mạng quá bận rộn để làm điều đó, vì vậy họ làm điều tốt nhất tiếp theo: Họ đọc nó cho anh ta qua điện thoại, cho phép anh ta truy cập vào mạng của họ. Khi vào bên trong, Mitnick đánh cắp mã nguồn của công ty. Trong trường hợp này, Mitnick đã có thể “chứng minh” danh tính của mình bằng cách cho các nhà khai thác mạng biết số văn phòng của anh ta, bộ phận nơi anh ta làm việc và tên của người giám sát của anh ta — tất cả thông tin mà kẻ tấn công đã thu thập được từ các cuộc điện thoại trước đó cho công ty ( [Garfinkel, 2002](#5__Garfinkel__S___2002__October) ).

Năm 2011, Verizon Business, Cơ quan Mật vụ Hoa Kỳ (USSS) và Đơn vị Tội phạm Công nghệ Cao Quốc gia Hà Lan (NHTCU) đã đưa ra một báo cáo chung thú vị sau khi phân tích khoảng tám trăm sự cố an ninh. Những sự cố này đã được điều tra bởi một hoặc nhiều tổ chức này. Là một phần của báo cáo, họ đã xác định các phương pháp hack phổ biến nhất được sử dụng trong các sự cố này. Bao gồm các:

Khai thác cửa hậu hoặc kênh lệnh / điều khiển.



Khai thác thông tin đăng nhập mặc định hoặc có thể đoán được.



Vũ phu và các cuộc tấn công từ điển.



Dấu chân và dấu vân tay.



Sử dụng thông tin đăng nhập bị đánh cắp.



Một số, như khai thác mật khẩu mặc định hoặc sử dụng thông tin đăng nhập bị đánh cắp, khá dễ hiểu. Những người khác, như khai thác kênh lệnh / điều khiển và dấu chân sẽ giải thích thêm một chút. Khai thác kênh lệnh và điều khiển hoặc cửa hậu cho phép kẻ tấn công tránh được các biện pháp đối phó an ninh. Điều này cho phép kẻ tấn công tránh bị phát hiện. Dấu chân hoặc dấu vân tay là một quá trình tự động của kẻ tấn công để quét các cổng hoặc dịch vụ đang mở ( [Verizon Business Global LLC & United States Secret Sevice, 2011](#23__Verizon_Business_Global_LLC) ).

An ninh mạng phải tập trung vào các mối đe dọa không chỉ bên ngoài tường lửa mà còn ở phía sau nó. Các cuộc tấn công nội bộ, chẳng hạn như những cuộc tấn công do những nhân viên bất mãn phát động, có thể rất tàn khốc. Chúng ta hãy xem xét hai cuộc tấn công như vậy.

Báo động!

Mối đe dọa bên trong

Điều quan trọng là phải nhận ra thực tế rằng các mối đe dọa không chỉ đến từ bên ngoài một tổ chức mà còn từ bên trong. Các biện pháp phòng ngừa phải tính đến cả hai khả năng. Mối đe dọa bên trong có một lợi thế đáng kể là nó có thể vượt qua nhiều biện pháp an ninh được áp dụng.

Một nhà phát triển ứng dụng, người bị mất công việc trong lĩnh vực CNTT do cắt giảm quy mô công ty, đã bày tỏ sự không hài lòng khi bị cho nghỉ việc ngay trước kỳ nghỉ lễ Giáng sinh bằng cách phát động một cuộc tấn công có hệ thống vào mạng máy tính của người chủ cũ của mình. Ba tuần sau khi chấm dứt hợp đồng, người trong cuộc đã sử dụng tên người dùng và mật khẩu của một trong những đồng nghiệp cũ của anh ta để truy cập từ xa vào mạng và sửa đổi một số trang Web của công ty, thay đổi văn bản và chèn hình ảnh khiêu dâm. Ông cũng gửi cho mỗi khách hàng của công ty một email thông báo rằng trang web đã bị tấn công. Mỗi tin nhắn e-mail cũng chứa tên người dùng và mật khẩu của khách hàng đó cho trang web. Một cuộc điều tra đã được bắt đầu, nhưng nó không xác định được người trong cuộc là thủ phạm. Một tháng rưỡi sau, anh ta lại truy cập từ xa vào mạng, thực hiện một tập lệnh để đặt lại tất cả mật khẩu mạng và thay đổi bốn nghìn bản ghi giá cả để phản ánh thông tin không có thật. Nhân viên cũ này cuối cùng đã được xác định là thủ phạm và bị truy tố. Anh ta bị kết án 5 tháng tù giam và 2 năm quản chế có giám sát, đồng thời ra lệnh trả 48.600 đô la bồi thường cho chủ cũ của anh ta ( [Keeney, Cappelli, Kowalski, Moore, Shimeall, & Rogers, 2005](#8__Keeney__M___Kowalski__E___Cap) ).

Một quản trị viên hệ thống, tức giận vì vai trò bị giảm sút của anh ta trong một công ty sản xuất quốc phòng đang phát triển mạnh có mạng máy tính do anh ta phát triển và quản lý, đã tập trung phần mềm hỗ trợ các quy trình sản xuất của công ty trên một máy chủ duy nhất, và sau đó dọa đồng nghiệp cung cấp cho anh ta bản sao lưu duy nhất băng cho phần mềm đó. Sau khi quản trị viên hệ thống chấm dứt hợp đồng vì đối xử không phù hợp và lạm dụng đối với đồng nghiệp của mình, một quả bom logic do người trong cuộc gieo rắc trước đó đã phát nổ, xóa bản sao duy nhất còn lại của phần mềm quan trọng khỏi máy chủ của công ty ( [Keeney, Cappelli, Kowalski, Moore, Shimeall và Rogers , 2005](#8__Keeney__M___Kowalski__E___Cap) ). Công ty ước tính chi phí thiệt hại vượt quá 10 triệu đô la, dẫn đến việc sa thải khoảng 80 nhân viên ( [Keeney, Cappelli, Kowalski, Moore, Shimeall, & Rogers, 2005](#8__Keeney__M___Kowalski__E___Cap) ).

## Ứng phó sự cố

Các tổ chức phải có khả năng phản hồi khi vi phạm xảy ra. Có một kế hoạch cùng với các công cụ và nhân sự để ứng phó hiệu quả có thể giúp giảm thiểu thiệt hại một cách lâu dài.

Viện Tiêu chuẩn và Công nghệ Quốc gia (NIST) đã phác thảo vòng đời ứng phó sự cố trong Hướng dẫn Xử lý Sự cố An ninh Máy tính của họ . Chúng ta có thể sử dụng điều này để hướng dẫn chúng ta qua một sự việc từ đầu đến cuối. Các giai đoạn bao gồm: chuẩn bị, ngăn chặn, phát hiện và phân tích ngăn chặn, tiêu diệt và phục hồi, và hoạt động sau khi tuyệt chủng ( [Scarphone, Grance, & Masone, 2008](#17__Scarphone__K___Grance__T) ).

Chuẩn bị —Chuẩn bị là chìa khóa để các tổ chức phản ứng nhanh chóng và hiệu quả với bất kỳ sự kiện an ninh mạng nào. Có nhiều bước mà một thực thể có thể thực hiện trong giai đoạn chuẩn bị. Lập kế hoạch rõ ràng là một trong những bước như vậy. Khả năng phòng thủ của mạng cũng cần được đánh giá và điều tra định kỳ để xác định các lỗ hổng.

Các biện pháp chủ động phải được thực hiện để ngăn chặn sự xâm nhập. Một số hành động phòng ngừa có thể được thực hiện bao gồm hệ thống vá lỗi (cập nhật phần mềm), bảo mật máy chủ (tăng cường các máy tính cá nhân), bảo mật mạng (bảo vệ chu vi của mạng) và tiến hành đào tạo và nâng cao nhận thức của người dùng. Cuối cùng, việc có các chính sách, thủ tục và hướng dẫn được cân nhắc kỹ lưỡng sẽ bổ sung đáng kể vào sự chuẩn bị của tổ chức.

Phát hiện và phân tích —Phát hiện một sự cố bảo mật là một thách thức đáng kể. Các cuộc tấn công tinh vi ngày nay có thể tự che mình là hoạt động mạng “bình thường”. Nhân viên an ninh mạng cần có sự cảnh giác và cẩn thận đến từng chi tiết để cải thiện khả năng bị tấn công của họ. Nó cũng giúp họ đưa ra kết luận đúng đắn sau khi tiến hành phân tích. Một thực tế nổi tiếng là Hệ thống phát hiện xâm nhập tạo ra một số lượng lớn các kết quả dương tính giả. Do đó, nhóm bảo mật phải có khả năng sàng lọc chính xác dữ liệu. Một cuộc tấn công trông như thế nào? Đó có thể là một chút khó khăn để mô tả. Để xác định tốt hơn hoạt động đáng ngờ, tốt nhất là bạn nên có một bức tranh chính xác về lưu lượng mạng hoặc hoạt động “bình thường” dành cho tổ chức. Một số dấu hiệu tiềm ẩn của một cuộc tấn công bao gồm cảnh báo phần mềm chống vi-rút, kết nối Internet chậm bất thường và lưu lượng mạng bất thường.

, Xóa bỏ và Phục hồi— Khi vi phạm xảy ra, nó phải được kiểm soát để giảm thiểu tác động của nó. Nếu không được kiểm soát, bụi phóng xạ từ một cuộc tấn công có thể phát triển theo cấp số nhân. Cách ngăn chặn sự cố khác nhau tùy thuộc vào loại sự cố đang phải đối mặt. Một số tùy chọn ngăn chặn bao gồm tắt hệ thống bị xâm nhập, ngắt kết nối hệ thống khỏi mạng hoặc vô hiệu hóa một số chức năng. Khi cuộc tấn công đã được xác định và ngăn chặn, các bước có thể được yêu cầu để loại bỏ bất kỳ thành phần nguy hiểm tiềm ẩn nào như mã độc hại hoặc các tài khoản bị xâm nhập.

Hoạt động bản sắc - Thật không may, bước có giá trị này thường bị bỏ qua. Một cuộc đánh giá sau khi thực hiện đại diện cho một cơ hội bị bỏ lỡ cho toàn bộ tổ chức và nhân sự của nó để cải tiến. Một bài đánh giá sau khi hoàn thành điển hình tìm cách trả lời các câu hỏi như:

Chúng ta đã làm gì đúng?



Chúng ta đã làm gì sai?



Các chính sách và thủ tục của chúng ta có đầy đủ và hiệu quả không?



Chúng ta có các nguồn lực cần thiết để ứng phó một cách hiệu quả không?



Điều gì, nếu có, chúng ta sẽ làm khác đi?



Để đối phó với một vi phạm bảo mật một cách hiệu quả đòi hỏi các bộ kỹ năng đa dạng. Là một phần của kế hoạch ứng phó sự cố, một tổ chức nên thành lập Nhóm ứng phó sự cố máy tính. Nhóm đa ngành này nên đưa tất cả các kỹ năng cần thiết để quản lý sự cố. Một số kỹ năng cần thiết để phản hồi bao gồm đại diện từ ban quản lý, bảo mật thông tin, hỗ trợ CNTT, pháp lý, quan hệ công chúng / truyền thông và những kỹ năng khác ( [Scarphone, Grance, & Masone, 2008](#17__Scarphone__K___Grance__T) ). Một người nào đó có khả năng pháp y kỹ thuật số nên là một phần của nhóm. Nhiều khi tài nguyên pháp y kỹ thuật số không tồn tại trong chính công ty. Trong những trường hợp này, chức năng này sẽ phải được thuê ngoài. Nếu đây thực sự là tình huống, nguồn lực này cần được xác định rõ ràng trước khi xảy ra sự cố thực tế.

## Điều tra và Bằng chứng Mạng

Cuộc tấn công của tin tặc thường đi theo một đường dẫn đến và xuyên qua mạng được nhắm mục tiêu. Như vậy, tiềm năng tồn tại để xác định vị trí bằng chứng dọc theo tuyến đường. Do đó, “theo dõi” kẻ xâm nhập là một bước quan trọng trong quá trình tìm kiếm và xác định chúng. Lợi thế của chúng ta là xác định, theo dõi và điều tra càng nhiều đường mòn này càng tốt.

Việc điều tra của chúng ta nên bao gồm càng nhiều thiết bị ở giữa hoặc thiết bị trung gian càng tốt. Những thiết bị trung gian này, chẳng hạn như bộ định tuyến và máy chủ, có thể chứa thông tin có giá trị và không nên bị bỏ qua. Bộ định tuyến có thể vừa là nguồn xác thực vừa là mục tiêu của tin tặc. Là một phần quan trọng của mạng, chúng thường là mục tiêu có giá trị đối với tin tặc. Nếu họ có thể xâm phạm một bộ định tuyến, họ có thể đạt được một chỗ đứng đáng kể. Một thách thức đối với các bộ định tuyến như một nguồn bằng chứng là tính không ổn định của chúng. Bạn có thể nhớ lại từ [Chương 2](#Top_of_CHP002_html) rằng bộ nhớ dễ bay hơi đòi hỏi nguồn điện liên tục để duy trì nội dung của nó. Rút phích cắm hoặc khởi động lại thiết bị có thể sẽ làm mất bằng chứng tiềm năng. Điều này rất có thể sẽ yêu cầu điều tra "trực tiếp" thiết bị khi nó đang chạy. Lời khuyên tốt nhất là hãy xử lý cẩn thận và đối xử với nó như với bất kỳ phần ký ức dễ bay hơi nào khác.

Bằng chứng kỹ thuật số là bằng chứng kỹ thuật số, bất kể nguồn của nó. Các nguyên tắc cơ bản và quy trình bảo quản và thu thập vẫn được áp dụng.

### 6.1 Tệp nhật ký

Nhiều thiết bị và máy tính trong mạng tạo ra nhật ký các sự kiện và hoạt động. Do đó, các tệp nhật ký đóng vai trò là nguồn bằng chứng chính trong các cuộc điều tra mạng. Có một số loại tệp nhật ký khác nhau. Một số nhật ký quan tâm bao gồm xác thực, ứng dụng, hệ điều hành và nhật ký tường lửa. Nhật ký xác thực xác định tài khoản (và địa chỉ IP) được kết nối với một sự kiện cụ thể .

Nhật ký ứng dụng ghi lại ngày và giờ cũng như mã định danh ứng dụng. Các tem ngày / giờ cho biết ứng dụng đã được bắt đầu khi nào và nó đã được sử dụng trong bao lâu. Nhật ký hệ điều hành theo dõi hệ thống khởi động lại cũng như việc sử dụng các thiết bị khác nhau. Nhật ký hệ điều hành rất hữu ích trong việc nhận biết các dạng hoạt động cũng như các điểm bất thường (xuất hiện bất thường) trong mạng. Nhật ký thiết bị chẳng hạn như nhật ký được tạo bởi bộ định tuyến và tường lửa cũng đáng được điều tra. Chúng ta sẽ xem xét nhật ký bộ định tuyến nhiều hơn chỉ sau một giây ( [Vacca & Rudolph, 2011](#22__Vacca_JR__Rudolph_K__System) ).

Có một số điều cần lưu ý với các tệp nhật ký. Các tệp nhật ký có thể thay đổi hoặc biến mất khá nhanh chóng. Chúng có thể được dọn dẹp định kỳ để giúp không gian lưu trữ trống. Cũng có một cơ hội tốt là không phải tất cả các bản ghi có liên quan sẽ thuộc quyền sở hữu của bạn. Các cuộc tấn công bắt nguồn từ bên ngoài tổ chức của bạn sẽ đi qua các thiết bị dưới sự kiểm soát của bên thứ ba, chẳng hạn như Nhà cung cấp dịch vụ Internet (ISP). Các bản ghi này có thể phải được trát đòi hầu tòa, có thể mất một thời gian. ISP có thể sẽ không bám vào những nhật ký này mãi mãi. Họ có thể có các chính sách lưu giữ và tiêu hủy tài liệu nhằm kiểm soát những gì được lưu giữ và trong thời gian bao lâu. Nếu thiếu nhu cầu hoặc lý do rõ ràng để giữ nó, những bản ghi đó sẽ bị phá hủy.

Nhật ký bộ định tuyến có thể chứa nhiều thông tin quan tâm. Một số điều chúng ta có thể khám phá là:

Bộ định vị tài nguyên thống nhất được yêu cầu (URL)

Tên máy chủ

Địa chỉ IP máy chủ

URL của khách hàng

Địa chỉ IP máy khách

Ai đã đăng nhập và khi nào

Khi cố gắng thu thập bằng chứng từ một bộ định tuyến, điều rất quan trọng là phải giảm thiểu mọi tương tác. Thay vì truy cập bộ định tuyến thông qua chính mạng, bạn nên đi qua bảng điều khiển của bộ định tuyến. Hãy nhớ rằng, mục tiêu của chúng ta là quan sát và ghi lại những gì chúng ta tìm thấy, không phải để thay đổi hoặc thay đổi bất cứ điều gì. Vì vậy, chúng ta nên tránh bất kỳ lệnh nào có khả năng sửa đổi bất kỳ dữ liệu nào. Ví dụ, một lệnh cấu hình là một lệnh nên tránh. Lệnh "hiển thị" là một lựa chọn tốt hơn nhiều. Dưới đây là một số ví dụ về lệnh "hiển thị":

> (tên bộ định tuyến) # hiển thị chi tiết đồng hồ — Hiển thị thời gian hệ thống

> (tên bộ định tuyến) #show người dùng — Hiển thị những người dùng có quyền truy cập vào bộ định tuyến

### 6.2 Công cụ điều tra mạng

Lưu lượng thực tế (gói tin) di chuyển trên mạng có thể nắm giữ một số manh mối có giá trị. Có một số công cụ, được gọi là "trình đánh giá", có thể nắm bắt và phân tích lưu lượng mạng. Một số công cụ này bao gồm:

Wireshark ( [www.wireshark.org](http://www.wireshark.org) )

NetIntercept ( <http://www.niksun.com/product.php?id=16>)

Công cụ điều tra Netwitness ( <http://www.netwitness.com/products-services/investigator>)

Snort ( <http://www.snort.org/>)

Việc nắm bắt lưu lượng mạng có thể mang lại một số manh mối tuyệt vời. Ví dụ: chúng ta có thể xác định tệp nào đã bị đánh cắp, lệnh nào đã được thực thi, cũng như bất kỳ tải trọng độc hại nào đã được phân phối. Từ góc độ pháp lý, điều quan trọng là phải nhận ra rằng việc giám sát lưu lượng mạng trong một số trường hợp nhất định có thể được coi là nghe lén ( [Casey, 2009](#2__Casey_E__Handbook_of_Digital) ).

### 6.3 Thách thức điều tra mạng

Việc xác định hacker chịu trách nhiệm không phải là một nhiệm vụ đơn giản. Có rất nhiều trở ngại trên đường đi có thể che giấu danh tính của kẻ tấn công. Nghi phạm có thể “giả mạo” địa chỉ IP thực của mình, có khả năng đưa các nhà điều tra vào cuộc truy đuổi ngỗng hoang. Cùng một đường thẳng, hacker có thể chuyển hướng cuộc tấn công của mình thông qua nhiều máy chủ trung gian nằm rải rác trên toàn cầu.

Nhật ký có thể là một nguồn bằng chứng tuyệt vời, nhưng chỉ khi chúng thực sự ở đó để chúng ta điều tra. Đôi khi chức năng ghi nhật ký bị tắt khi bắt đầu, có nghĩa là không có nhật ký nào được tạo. Thời gian thể hiện một mối quan tâm khác. Nếu vi phạm được phát hiện quá muộn, thì có khả năng đáng kể là bất kỳ nhật ký nào được duy trì bởi một tổ chức bên ngoài (chẳng hạn như ISP) sẽ bị phá hủy theo chính sách lưu giữ và tiêu hủy của họ. Tin tặc cũng có thể cố ý xóa các bản ghi có liên quan trong cuộc tấn công của chúng, để che dấu vết của chúng một cách hiệu quả. Cuối cùng, quyền tài phán có thể tạo ra một trở ngại đáng kể. Theo nghĩa đen, dấu vết của kẻ tấn công có thể đi qua các ranh giới tiểu bang, quốc gia và quốc tế. Các khu vực tài phán pháp lý khác nhau, đặc biệt là các khu vực quốc tế, có thể có các yêu cầu cực kỳ khác nhau để có được loại thông tin này. Các quốc gia khác nhau cũng có thể có quan điểm rất khác nhau về tội phạm mạng nói chung, điều này có thể dẫn đến sự thiếu hợp tác ( [Morris, 2005](#13__Morris__D__A___2005__May_3) ).

Tài nguyên bổ sung

Đào tạo và Nghiên cứu

Đào tạo và nghiên cứu là điều bắt buộc trong thế giới pháp y kỹ thuật số. Được thành lập vào năm 1989, Viện SANS là một trong những tổ chức hàng đầu đáp ứng nhu cầu quan trọng này. Họ cung cấp một loạt các khóa học và tài nguyên bao gồm cả bảo mật thông tin và pháp y kỹ thuật số. Ngoài ra, họ cung cấp nhiều chứng chỉ được chấp nhận trong toàn ngành. Họ cũng có một sự hiện diện mạnh mẽ trên Twitter.

<http://www.sans.org/>

<http://computer-forensics.sans.org/blog>

@SANSInsrupt

@sansforensics

## Bản tóm tắt

An ninh mạng phải là một mối quan tâm lớn đối với tất cả chúng ta. Mạng và PC của chúng ta 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 ta 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.

### Tổng kết và kiến thức thêm chương 9

1. **Hiểu được mục tiêu của điều tra mạng**

Mục tiêu của điều tra mạng là chụp hình, ghi lại, và phân tích lưu lượng mạng và nhật ký nhằm kiếm được bằng chứng số hoặc đối tượng phạm tội. Thông thường, cuộc điều tra mạng sẽ điều tra theo 2 hướng, Mạng nội bộ (LAN) và mạng ngoại tuyến (Internetwork)

1. **Hiểu được nhật ký mạng (log) là gì?**

Nhật ký mạng (log) là nơi ghi lại những hành động của người dùng trong hệ thống mạng. Tính chính xác của nhật ký mạng xác định giá trị của chúng. Mọi thay đổi trong nhật ký (logs) sẽ làm ảnh hưởng tới toàn bộ nhật ký ấy.

1. **Hiểu được quy trình điều tra mạng**

Mục tiêu: Chọn đúng phương pháp, công cụ để thực hiện việc điều tra số

1. Hệ thống bị tấn công sử dụng một hay nhiều hệ điều hành
2. Thông tin được trình bày dưới dạng sơ đồ, thông qua thiết bị thứ 3, dựa theo điều kiện – hành động, hay đã được hồ sơ hóa.
3. Hướng tiếp cận dựa trên thông tin thu thập: Tiếp cận theo hướng phân tích thông tin người dùng, tiếp cận theo hướng phân tích điểm yếu, và tiếp cận theo hướng phân tích các ports
4. **Kiểm tra các nhật ký trên router, firewall, ids**

Routers, Firewall, và IDS thông thường sẽ lưu trữ những bằng chứng như:

1. Thời gian
2. Nguồn tấn công
3. Địa chỉ IP
4. Ports

Những thông tin này sẽ giúp điều tra viên biết được thời gian xảy ra sự cố, nguồn tấn công, và các sự kiện liên quan đến kết nối mạng nhằm hỗ trợ cho việc điều tra thiết bị bị tấn công.

1. **Kiểm tra lưu lượng mạng**

Điều tra viên phân tích lưu lượng mạng nhằm xác định những thông tin như:

1. Lưu lượng mạng
2. Các kết nối lỗi
3. Các lưu lượng mạng khác thường
4. Hệ thống mạng bị lỗi hoặc ảnh hưởng sau sự cố
5. **Ghi lại bằng chứng**

Thông thường, các bằng chứng liên quan đến nhật ký sẽ được in ra và giữ dưới dạng tài liệu thay vì tệp tin pcap như thông thường.

1. **Sắp xếp lại bằng chứng**

Các bằng chứng có được thông qua điều tra mạng thông thường sẽ tốn thời gian và rất khó để phân tích nếu không được sắp xếp hợp lý. Do đó, các điều tra viên nên sắp xếp bằng chứng dựa trên tính chất của chúng:

1. Bằng chứng liên quan đến các yếu tố như sự cố ATTT, thời gian xảy ra sự cố, đối tượng tình nghi, và nhân chứng. (Temporal Analysis)
2. Bằng chứng liên quan đến hành động của nạn nhân và đối tượng tình nghi (Relational Analysis)
3. Bằng chứng liên quan đến các phương pháp, kỹ thuật, và hành động gây nên sự cố ATTT (Functional Alnalysis)

Tài liệu tham khảo

1. Bowden M. Worm: The First Digital World War New York: Atlantic Monthly Press; 2011.

2. Casey E. Sổ tay Điều tra và Pháp y Kỹ thuật số Burlington, MA: Academic Press; Năm 2009.

3. Casey E. Bằng chứng Kỹ thuật số và Tội phạm Máy tính: Khoa học Pháp y, Máy tính và Internet Waltham, MA: Báo chí Học thuật; 2011.

4. Conrad E, Misenar S, Feldman J. Hướng dẫn Nghiên cứu CISSP Burlington, MA: Elsevier; Năm 2010.

5. Garfinkel, S. (2002, ngày 7 tháng 10). Kevin Mitnick và Anti-Social Engineering . Truy cập ngày 9 tháng 11 năm 2011, từ CSOOnline.com: <http://www.csoonline.com/article/217395/kevin-mitnick-and-anti-social-engineering->.

6. Hadnagy C. Kỹ thuật xã hội: Nghệ thuật tấn công con người Indianapolis: Wiley; 2011.

7. Krebs, B. (nd). ATM phối hợp Heist Nets Thieves 13 triệu đô la . Truy cập ngày 19 tháng 9 năm 2011, từ: <http://krebsonsecurity.com/2011/08/coordinated-atm-heist-nets-thieves-13m/>.

8. Keeney, M., Kowalski, E., Cappelli, D., Moore, A., Shimeall, T., và Rogers, S. (2005, tháng 5). Nghiên cứu về mối đe dọa nội gián: Sự phá hoại của máy tính trong các lĩnh vực cơ sở hạ tầng quan trọng. Cơ quan Mật vụ Hoa Kỳ và chương trình CERT . Báo cáo có tại <http://www.secretservice.gov>.

9. Maggiora PD, Doherty J. Cisco Networking Simplified Indianapolis: Cisco Press; 2003.

10. McClure S, Scambray J, Kurtz G. Hacking Exposed: Network Security Secrets and Solutions New York: McGraw-Hill; Năm 2009.

11. Tập đoàn Microsoft. (nd). IPv6 . Truy cập ngày 17 tháng 9 năm 2011, từ: <http://technet.microsoft.com/en-us/network/bb530961.aspx>.

12. Mitnick K. Ghost in the Wires: My Adventures as the World's Most Wanter Hacker New York: Little, Brown and Company; 2011.

13. Morris, DA (2005, ngày 3 tháng 5). Theo dõi một Hacker máy tính . Truy cập ngày 19 tháng 9 năm 2011, từ: <http://www.justice.gov/criminal/cybercrime/usamay2001_2.htm>.

14. Nikkel, BJ (2007). Giới thiệu về Điều tra Mạng IPv6 . Điều tra Kỹ thuật số: Tạp chí Quốc tế về Pháp y Kỹ thuật số và Ứng phó Sự cố Vol. 4, số 2. Oxford, Anh: Elsevier.

15. Poulsen K. Kingpin: Làm thế nào một hacker vượt qua tội phạm mạng trị giá hàng tỷ đô la New York: Crown; 2011.

16. Prowell S, Kraus R, Borkin M. Bảy vụ tấn công mạng chết người nhất Burlington, MA: Syngress; Năm 2010.

17. Scarphone, K., Grance, T., & Masone, K. (2008). Hướng dẫn xử lý sự cố bảo mật máy tính . Viện Tiêu chuẩn và Công nghệ Quốc gia, Bộ phận An ninh Máy tính. Gaithersburg, TN: Viện Tiêu chuẩn & Công nghệ Quốc gia.

18. TechTarget. (2000, tháng 8). Phát hiện xâm nhập (ID) . Được truy cập ngày 17 tháng 9 năm 2011, từ: <http://searchmidmarketsecurity.techtarget.com/definition/intrusion-detection>.

19. TechTarget. (2000, tháng 10). Tường lửa . Truy cập ngày 17 tháng 9 năm 2011, từ: <http://searchsecurity.techtarget.com/definition/firewall>.

20. TechTarget. (2001, tháng 3). Kỹ thuật xã hội . Truy cập ngày 18 tháng 9 năm 2011, từ: <http://searchsecurity.techtarget.com/definition/social-engineering>.

21. TechTarget. (2002, tháng 1). Khịt mũi . Truy cập ngày 17 tháng 9 năm 2011, từ: <http://searchmidmarketsecurity.techtarget.com/definition/Snort>.

22. Vacca JR, Rudolph K. System Forensics, Rudolph K. Sudbury, MA: Jones and Bartlett Learning; 2011.

23. Verizon Business Global LLC, & United States Secret Sevice. Báo cáo Điều tra Vi phạm Dữ liệu năm 2011 Ashburn: Verizon Business Global LLC; 0026; United States Secret Sevice, 2011.

# Chương 10: Pháp y thiết bị di động

**Thông tin trong Chương này:**

Mạng di động và cách chúng hoạt động



Tổng quan về Hệ điều hành Điện thoại Di động



Bằng chứng tiềm năng được tìm thấy trên điện thoại di động



Thu thập và xử lý điện thoại di động làm bằng chứng



Công cụ pháp y trên điện thoại di động



Chức năng Hệ thống Định vị Toàn cầu và Bằng chứng Tiềm năng



Nhiều người đặt câu hỏi rằng chúng ta đã từng hoạt động như thế nào nếu không có điện thoại di động. Hầu hết mọi người đều có một chiếc điện thoại di động hoặc một chiếc PDA nào đó; ngay cả trẻ nhỏ bây giờ cũng có điện thoại thông minh trong ba lô. Mặc dù nhiều đứa trẻ thậm chí không thể nhớ cảm giác không có điện thoại di động, nhưng chúng ta phải nhớ rằng đã lâu rồi chúng thậm chí không tồn tại (hoặc chúng ta phải mang chúng trong túi) ! Trong thế giới pháp y kỹ thuật số, điều này mang lại nhiều lợi ích, đặc biệt là giờ đây chúng ta có nhiều địa điểm hơn để tìm kiếm bằng chứng và tiềm năng xác thực dữ liệu cho nhiều thiết bị là cao hơn. Giờ đây, các giám định viên sẽ có thêm thách thức khi điều tra nhiều thiết bị và đảm bảo rằng chúng bảo vệ chuỗi hành trình và ghi lại bằng chứng một cách kỹ lưỡng.

Trong Chương 10, chúng ta sẽ xem xét kỹ hơn về điện thoại di động và công nghệ cung cấp năng lượng cho chúng. Chúng ta sẽ xem xét các loại mạng cũng như các thành phần hình thành chúng. Điện thoại di động không phải là thiết bị di động duy nhất có giá trị chứng minh tiềm năng. GPS hay Hệ thống định vị toàn cầu ngày càng được các nhà điều tra chú ý hơn. Do đó, chúng ta sẽ xem xét loại bằng chứng nào mà chúng ta có thể khôi phục được từ thiết bị GPS. Cuối cùng, chương này sẽ xem xét các kỹ thuật xử lý đặc biệt cần thiết để lưu giữ bằng chứng mỏng manh trên các thiết bị không dây này.

Trang web di động, Hệ thống định vị toàn cầu (GPS), Điểm theo dõi, Nhật ký theo dõi, TDMA, GSM, Mạng nâng cao kỹ thuật số tích hợp (iDEN), Điện thoại thông minh, Mô-đun nhận dạng thuê bao (SIM), Bộ điều khiển trạm gốc (BSC), Trung tâm chuyển mạch di động (MSC) , Đăng ký vị trí khách truy cập (VLR), Đăng ký vị trí nhà (HLR), Trung tâm xác thực (AuC), Trung tâm dịch vụ tin nhắn ngắn (SMSC), Mạng điện thoại chuyển mạch công cộng (PSTN), Số sê-ri điện tử (ESN), Số nhận dạng cá nhân (PIN) , Khóa mở khóa cá nhân (PUK), Bản ghi chi tiết cuộc gọi, Số nhận dạng thiết bị di động quốc tế (IMEI), ESN, MEID, Nhận dạng thuê bao di động quốc tế (IMSI), Số nhận dạng thẻ mạch tích hợp (ICC-ID), Văn bản tiên đoán, Chức năng liên kết, Handoff, Dịch vụ tin nhắn ngắn (SMS), Dịch vụ nhắn tin đa phương tiện (MMS), Tam giác, Ăng ten định hướng, Điểm tham chiếu

## Giới thiệu

Những chiếc điện thoại đeo trên hông và nằm gọn trong túi của chúng ta là những tuyệt tác công nghệ thực sự. Những “máy tính mini” này có khả năng cung cấp nhiều chức năng giống như một tỉnh duy nhất đã từng là máy tính để bàn và máy tính xách tay. Chúng ta có thể duyệt Internet, gửi và nhận e-mail, chụp ảnh và quay video cũng như vẽ vị trí của chúng ta trên bản đồ, chỉ để nêu tên một vài khả năng.

Điện thoại di động và các thiết bị di động khác có thể làm cho vỏ máy kín hơi. Chỉ cần hỏi Boise, Dan Kincaid của Idaho. Khi cảnh sát Boise bắt Kincaid vì tội ăn trộm, họ cũng thu giữ và khám xét điện thoại di động Blackberry của anh ta. Nó trả hết. Email của anh ta chứa một số tin nhắn cuối cùng sẽ giúp thuyết phục anh ta nhận tội. Sau khi bị phát hiện, Kincaid đã gửi e-mail cho bạn gái của mình rằng "Chỉ cố gắng tìm cách thoát khỏi khu phố này mà không bị bắt." “Chó sủa nếu tôi ở giữa hoặc sau nhà…” Anh ấy tiếp tục viết, “Cảnh sát biết tôi mặc áo sơ mi xanh. … Tôi cần phải ra khỏi đây trước khi họ tìm thấy tôi ”( [Shachtman, 2006](#22__Shachtman__N___2006__May_3) ).

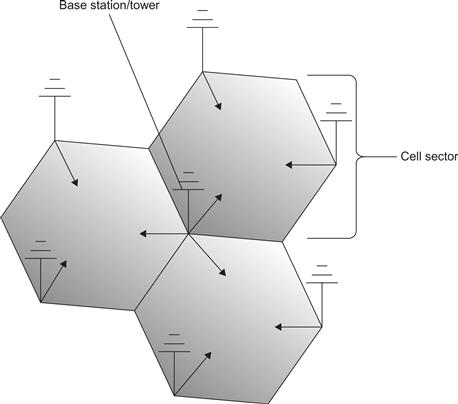
Về cơ bản, điện thoại thông minh ngày nay về cơ bản là máy tính có gắn radio. Có một thế giới phần cứng điện thoại di động không ngừng phát triển và không bị chậm lại. Giống như những người anh em họ lớn hơn của chúng, những thiết bị quy mô nhỏ này có thể tạo ra những đồ tạo tác có thể được phục hồi và sử dụng làm bằng chứng.

Điện thoại di động và các thiết bị di động khác là một thách thức khác đối với các điều tra viên. Bước vào bất kỳ cửa hàng điện thoại di động nào và bạn sẽ đối mặt với vô số loại điện thoại di động, kiểu máy và hệ điều hành. Các thiết bị khác nhau lần lượt hỗ trợ nhiều dịch vụ và ứng dụng khác nhau. Để làm phức tạp thêm mọi thứ, không có một giao diện phần cứng được thiết lập. Bạn có thể gặp phải sự cố này lần này hay lần khác khi nâng cấp điện thoại của mình. Kỳ lạ là khi bạn có một chiếc điện thoại mới, bạn cũng phải mua một bộ sạc mới và cáp dữ liệu. Bắt kịp với hệ thống cáp, hệ điều hành, v.v. là một thách thức khá lớn. Tin tốt là điều này dường như đang trở nên tốt hơn, với nhiều điện thoại hiện nay đã bao gồm một USB mini trong thiết bị cầm tay của họ.

## Mạng di động

Bằng chứng có thể không chỉ nằm trong điện thoại hoặc thẻ nhớ, mà còn nằm trên chính mạng. Là người giám định, chúng ta cần hiểu hoạt động cơ bản của mạng di động và (các) vị trí của bất kỳ bằng chứng tiềm năng nào.

Như tên của nó, mỗi mạng di động bao gồm các ô riêng lẻ. Mỗi tế bào sử dụng một dải tần số được xác định trước để cung cấp dịch vụ cho một khu vực địa lý riêng biệt. Kích thước và hình dạng của mỗi ô khác nhau. Trên thực tế, chúng có thể rất khác nhau. Chúng có thể bao phủ một vài dãy phố trong môi trường đô thị với diện tích hơn vài trăm dặm vuông trong cả nước. Loại địa hình, đặc biệt là các vật cản, là yếu tố hạn chế; xem [Hình 10.1](#F0010_9) .



Hình 10.1 Sơ đồ của một mạng di động điển hình. (Minh họa bởi Jonathan Sisson.)

Cường độ của tín hiệu vô tuyến phát ra từ mỗi ô được kiểm soát chặt chẽ. Điều này được thực hiện có mục đích để giới hạn phạm vi của nó. Bằng cách giới hạn phạm vi, các nhà cung cấp có thể sử dụng lại số lượng tần số tương đối hạn chế mà họ phải làm việc.

Mỗi ô có một trạm gốc bao gồm một ăng-ten (hoặc cột buồm) cùng với các thiết bị vô tuyến liên quan. Cùng với nhau, chúng được biết đến như một địa điểm tế bào . Các vị trí tế bào này cung cấp vùng phủ sóng cho các ô riêng lẻ. Bạn có thể đã nhìn thấy những tòa tháp lớn dọc theo đường liên bang chẳng hạn hoặc những tòa tháp nhỏ hơn trên các mái nhà ở các địa điểm đô thị hơn. Thông thường, mỗi tháp di động sẽ có ba tấm mỗi bên. Bảng điều khiển ở giữa thường là máy phát, với hai bảng còn lại là máy thu. Các tấm thu liên tục lắng nghe các tín hiệu radio đến.

Bạn có thể ngạc nhiên khi biết rằng các vị trí ô không nằm ở trung tâm của mỗi ô. Chúng thực sự nằm ở điểm giao nhau của nhiều ô, tạo điều kiện thuận lợi cho dịch vụ khi người đăng ký di chuyển từ ô này sang ô khác.

### 2.1 Các thành phần mạng di động

Phải mất kha khá cơ sở hạ tầng để có thể gọi điện thoại từ vị trí xa xôi đó trở lại trung tâm văn phòng của bạn. Về mặt pháp lý, mỗi thành phần này có thể cung cấp thông tin liên quan đến một cuộc điều tra.

Trạm gốc bao gồm ăng-ten và các thiết bị liên quan.

Bộ điều khiển trạm gốc (BSC) điều chỉnh tín hiệu giữa các trạm gốc. Chức năng này rất quan trọng khi điện thoại di chuyển từ nơi này sang nơi khác.

Trung tâm Chuyển mạch Di động (MSC) xử lý các cuộc gọi trong mạng. Là một phần quan trọng của mạng không dây, MSC nắm giữ một lượng lớn bằng chứng có thể có. Nó cũng điều phối các cuộc gọi giữa các mạng không dây khác nhau cũng như các đường dây cố định. MSC cũng xử lý các tin nhắn SMS. Các bản ghi và nhật ký chi tiết cuộc gọi được tìm thấy ở đây.

Sổ đăng ký Vị trí Khách (VLR) là cơ sở dữ liệu được liên kết với MSC. Tất cả các thiết bị di động hiện đang được kiểm soát bởi MSC đó đều được ghi lại trong VLR. Các Chức năng Liên kết đóng vai trò như những cánh cửa bên ngoài các mạng dữ liệu chẳng hạn như Internet.

Thông tin về các thuê bao cá nhân được thu thập trong Sổ đăng ký Vị trí Nhà (HLR) . Thông tin này bao gồm nhận dạng thuê bao, thanh toán và các dịch vụ mà họ nhận được, cùng với vị trí hiện tại của thiết bị. HLR cũng lưu trữ các khóa mã hóa. HLR hỗ trợ Trung tâm Xác thực (AuC) , được sử dụng để kiểm soát quyền truy cập vào mạng. AuC sàng lọc các kết nối, chặn người dùng trái phép ( [Jansen & Ayers, 2007](#15__Jansen_W__Ayers_R__Guideline) ).

Tin nhắn văn bản hoặc SMS là trách nhiệm của Trung tâm Dịch vụ Tin nhắn Ngắn (SMSC) . Các tin nhắn có thể được khôi phục từ SMSC, nhưng không có quy tắc cứng và nhanh nào quy định các nhà cung cấp cá nhân phải lưu giữ những tin nhắn này trong bao lâu. Nhà cung cấp tùy thuộc vào quyết định của thông tin đó được lưu giữ trong bao lâu ( [Jansen & Ayers, 2007](#15__Jansen_W__Ayers_R__Guideline) ).

Điều quan trọng cần lưu ý là điện thoại di động của bạn thường xuyên liên lạc với ăng ten di động gần nhất, ngay cả khi bạn không nói chuyện trên đó. Khi bạn bật điện thoại di động của mình, điện thoại sẽ tự động bắt đầu tìm kiếm trang web di động gần nhất. Sau khi tìm thấy ăng-ten, điện thoại sẽ truyền dữ liệu nhận dạng để mạng có thể xác minh bạn là ai và bạn có được phép truy cập hay không. Thông tin này sẽ bao gồm những thứ như số điện thoại di động cùng với tên của nhà cung cấp dịch vụ của bạn.

Khi bạn lái xe, "kết nối" của bạn với mạng phải được chuyển từ tháp di động sang tháp di động. Việc chuyển giao này được gọi là “chuyển nhượng”. Việc chuyển giao được thực hiện khi cường độ tín hiệu bắt đầu giảm dần. Không phải tất cả các phần thưởng được xử lý theo cùng một cách. Ví dụ, GSM (Hệ thống toàn cầu cho truyền thông di động) và Đa truy cập phân chia theo mã (CDMA) cho các mạng xử lý chúng theo cách khác nhau. Mạng GSM sử dụng những gì được gọi là chuyển giao cứng. Ở đây, điện thoại chỉ có thể gắn vào một tháp tại một thời điểm. Cuộc trò chuyện được tách khỏi tháp hiện tại và chuyển sang tháp mới. Sau đó, điện thoại sẽ chuyển sang tần số của tháp mới. Ngược lại, phần thưởng CDMA được coi là phần thưởng “mềm”. Tại đây, một điện thoại có thể kết nối với nhiều tháp cùng một lúc, sử dụng tháp có tín hiệu mạnh nhất.

Các bản ghi cho thấy khi một điện thoại nhất định được kết nối với một tháp cụ thể có thể được sử dụng để đưa ai đó (hoặc chính xác hơn là điện thoại của họ) vào vùng lân cận của tội phạm hoặc để thiết lập chứng cứ ngoại phạm.

Sau khi cuộc gọi của bạn chạm vào tháp di động, cuộc gọi đó sẽ được chuyển đến Trung tâm Chuyển mạch Di động (MSC) . Nếu cuộc gọi được dành cho một điện thoại không có mạng, MSC sẽ chuyển cuộc gọi đến Mạng Điện thoại Chuyển mạch Công cộng (PSTN) . PSTN sau đó sẽ hướng cuộc gọi đến người nhận dự định của nó.

Tất cả chúng ta đều đã gặp phải tình trạng cuộc gọi bị gián đoạn hoặc mất tín hiệu vào lúc này hay lúc khác. Một trong những nguyên nhân tiềm ẩn là điểm chết. Các điểm chết có thể do một khoảng trống trong vùng phủ sóng của tế bào hoặc các vật cản đối với tín hiệu. Điện thoại di động phụ thuộc rất nhiều vào việc có một đường dẫn rõ ràng và không bị cản trở (hoặc rất gần với nó) đến tháp di động. Vật cản có thể là nhà cao tầng, núi và cây lớn.

Điện thoại di động hỗ trợ hai loại dịch vụ nhắn tin, Dịch vụ Tin nhắn Ngắn (SMS) và Dịch vụ Nhắn tin Đa phương tiện (MMS) . SMS là những gì chúng ta thường gọi là tin nhắn văn bản. Chúng ta lấy tên là Thông điệp ngắn do giới hạn về kích thước tối đa của mỗi thông báo. Tin nhắn SMS có độ dài tối đa là 160 ký tự. MMS cung cấp chức năng cải tiến qua SMS. Tin nhắn MMS không giới hạn 160 ký tự.

### 2.2 Các loại mạng di động

Mạng di động có thể được phân biệt hoặc xác định theo cách chúng truyền dữ liệu. Các sơ đồ truyền dẫn này bao gồm Đa truy nhập phân chia theo mã (CDMA) , Hệ thống toàn cầu cho Truyền thông di động (GSM) và Mạng được nâng cao kỹ thuật số tích hợp (iDEN) .

#### 2.2.1 Đa truy cập phân chia theo mã (CDMA)

CDMA ban đầu là một công nghệ quân sự cuối cùng đã được phát hành để công chúng sử dụng. CDMA sử dụng công nghệ trải phổ để truyền dữ liệu. Công nghệ này cho phép một số điện thoại gửi và nhận thông qua một kênh duy nhất. Mỗi phần của các cuộc trò chuyện riêng biệt này được gắn nhãn bằng một mã kỹ thuật số cụ thể. Các nhà cung cấp dịch vụ sử dụng công nghệ CDMA bao gồm Sprint, Verizon, Alltel và NEXTEL. Điện thoại CDMA thường không sử dụng thẻ SIM. Mạng CDMA sử dụng Số sê-ri điện tử (ESN) để xác định từng thiết bị cầm tay ( [Barbara, 2010](#1__Barbara__J__J___2010__October) ).

#### 2.2.2 Hệ thống toàn cầu cho liên lạc di động (GSM)

Như tên cho thấy, điện thoại GSM có thể được sử dụng quốc tế. GSM sử dụng công nghệ Đa truy nhập phân chia theo thời gian (TDMA ). Trên thế giới, GSM là phương thức truyền dẫn được sử dụng rộng rãi nhất. Không giống như CDMA, điện thoại GSM sử dụng thẻ SIM. Các nhà cung cấp dịch vụ GSM bao gồm AT&T, Verizon, T-Mobile và Cellular One. Nhận dạng thiết bị di động quốc tế (IMEI) được sử dụng để nhận dạng thiết bị cầm tay ( [Barbara, 2011](#2__Barbara__J__J___n_d____SIM_Fo) ).

#### 2.2.3 Mạng nâng cao kỹ thuật số tích hợp (IDEN)

iDEN, hoặc Mạng được nâng cao kỹ thuật số tích hợp, cung cấp chức năng giống như radio hai chiều, còn được gọi là “Push to Talk”. Giống như điện thoại GSM, chúng cũng sử dụng thẻ SIM. Các nhà cung cấp dịch vụ iDEN bao gồm NEXTEL, Sprint và Boostmobile.

#### 2.2.4 Điện thoại di động trả trước

Về cốt lõi, điện thoại trả trước hoạt động giống như các điện thoại di động khác ở chỗ chúng sử dụng radio để truyền dữ liệu và phải kết nối với mạng. Sự khác biệt với điện thoại trả trước là chúng tạo ra một số rào cản điều tra đáng kể, đặc biệt là khi cố gắng xác định người đăng ký. Đầu tiên, chúng có thể được thanh toán hoàn toàn bằng tiền mặt, về cơ bản chỉ để lại rất ít hoặc không có gì theo cách của một dấu vết trên giấy tờ. Điều này làm cho việc xác định người mua khó hơn nhiều.

Tuy nhiên, giống như các điện thoại di động khác, chúng ta có thể xác định khu vực mà điện thoại đang được sử dụng cũng như các cuộc gọi được gửi và nhận. Với điện thoại trả trước, thông tin chúng ta đang tìm kiếm sẽ do hai đơn vị nắm giữ. Nhà cung cấp điện thoại sẽ giữ bất kỳ thông tin thuê bao nào và nhà cung cấp mạng sẽ duy trì hồ sơ chi tiết cuộc gọi.

## Các hệ điều hành

Hệ điều hành (OS) của điện thoại có tác động đáng kể đến bất kỳ cuộc khám nghiệm pháp y nào. Hệ điều hành xác định những gì tạo tác được tạo ra và cách chúng được lưu trữ. Hệ điều hành điện thoại di động hiện đại bao gồm Symbian, Apple iOS, Windows CE và Windows Mobile, Android của Google và Blackberry OS.

Ban đầu, hệ điều hành Symbian là sản phẩm của sự hợp tác giữa Nokia, Ericsson, Motorola và Psion. Sony Ericsson tung ra chiếc điện thoại chạy Symbian đầu tiên vào năm 2000. Năm 2008, Nokia đã mua bản quyền của hệ điều hành này. Nokia gần đây đã tạo ra mã nguồn mở Symbian. Ngày nay nó được sử dụng trong các thiết bị cầm tay của Nokia và Sony Ericsson (Barbara, 2010b).

Blackberry lần đầu tiên được giới thiệu vào năm 1999 bởi công ty Canada Research In Motion (RIM). Các doanh nghiệp và các tổ chức chính phủ là những người sử dụng Blackberry nhiều. Điện thoại Blackberry đồng bộ hóa với GroupWise của Novel và Exchange của Microsoft. Do đó, họ khá thành thạo trong việc xử lý e-mail, lịch và những thứ tương tự. Hệ điều hành Blackberry hỗ trợ đa nhiệm cũng như nhiều ứng dụng khác nhau. Hệ điều hành này là độc quyền và các phiên bản dành riêng cho từng nhà cung cấp dịch vụ. Điều đó có nghĩa là phiên bản Verizon của một điện thoại cụ thể sẽ khác với phiên bản AT&T (Barbara, 2010b).

Android là một hệ điều hành mã nguồn mở hiện được phát triển bởi Open Handset Alliance. Năm 2005, Google mua lại hệ điều hành Android từ Android, Inc. Năm 2007, Liên minh thiết bị cầm tay mở được thành lập và đã phát triển hệ điều hành này kể từ đó. Open Handset Alliance “là một nhóm gồm 84 công ty công nghệ và di động đã hợp tác với nhau để thúc đẩy sự đổi mới trong lĩnh vực di động và mang đến cho người tiêu dùng trải nghiệm di động phong phú hơn, ít tốn kém hơn và tốt hơn” ( [Open Handset Alliance, 2007](#21__Open_Handset_Alliance___2007) ). Một số thành viên bao gồm Sprint, T-Mobile, LG Electronics, Inc., Kyocera, Motorola, Google và eBay. Hàng nghìn ứng dụng của bên thứ ba có sẵn để tăng cường chức năng cốt lõi của Android. Android được tìm thấy trên các thiết bị cầm tay do Motorola, Sony Ericsson và HTC sản xuất (Barbara, 2010b).

IOS phổ biến của Apple có thể được tìm thấy không chỉ trên iPhone mà còn trên các thiết bị di động khác như iPad và iPod touch. iOS dựa trên Mac OS X của Apple, được sử dụng trên máy tính xách tay và máy tính để bàn của họ. iPhone sử dụng nhiều ứng dụng của bên thứ ba được mua / tải xuống từ Apple App Store.

Windows Mobile là hệ điều hành của Microsoft được phát triển cho thị trường điện thoại thông minh và thiết bị di động. Giống như các đối thủ cạnh tranh, Windows Mobile cũng hỗ trợ một lượng lớn các ứng dụng.

## Bằng chứng điện thoại di động

Bây giờ chúng ta đã xem xét cách điện thoại di động và mạng hoạt động, chúng ta có thể xem xét một số thông tin mà chúng nắm giữ có thể đủ điều kiện làm bằng chứng. Điều quan trọng là không nên tập trung vào một nguồn, vì bằng chứng liên quan có thể được tìm thấy ở nhiều vị trí trong thiết bị cầm tay và mạng.

[Bảng 10.1](#Top_of_CHP010_html) liệt kê một số vật chứng tiềm ẩn được tìm thấy trong điện thoại thông minh hiện đại.

Bảng 10.1. Bằng chứng điện thoại thông minh tiềm năng

|  |  |  |
| --- | --- | --- |
| Lịch sử cuộc gọi | Tin nhắn | E-mail |
| Hình ảnh & Video | Tin nhắn văn bản đã xóa | Lịch sử trình duyệt |
| Liên lạc | Thông tin vị trí GPS | Phiên trò chuyện |
| Lịch | Ghi nhớ giọng nói | Các tài liệu |

Mã số nhận dạng cá nhân (PIN) được sử dụng để bảo mật điện thoại. Ba lần liên tiếp, không thành công để nhập mã PIN chính xác sẽ dẫn đến việc người dùng bị khóa. Khóa Mở Cá nhân ( PUK) sẽ cần thiết để mở khóa SIM sau khi quá trình khóa này xảy ra. Thông thường, chỉ có nhà cung cấp thẻ SIM mới có thể cung cấp mã PUK ( [Barbara, 2010](#1__Barbara__J__J___2010__October) ).

Có thể bạn đã nhận thấy khi gõ e-mail hoặc văn bản trên điện thoại, nhiều lần điện thoại sẽ điền các từ cho bạn. Đây được gọi là văn bản tiên đoán . Văn bản tiên đoán được phát triển để giúp nhắn tin dễ dàng hơn trên điện thoại không có bàn phím QWERTY đầy đủ. Những điện thoại này sử dụng ba chữ cái cho mỗi phím, buộc người dùng phải “cuộn” qua nhiều tùy chọn chữ cái trước khi chọn một chữ cái. Với công nghệ nhắn tin tiên đoán, thiết bị sẽ cố gắng dự đoán từ mà người dùng có ý định nhất. Những phỏng đoán này dựa trên một từ điển cơ sở dữ liệu chứa hàng nghìn từ, tên, chữ viết tắt, tiếng lóng, v.v. ( [Mobile-phone-directory.org, 2009](#19__Mobile_phone_directory_org) ).

Điều thú vị nhất, từ góc độ pháp y là những hệ thống này có khả năng học hỏi. Các từ, chữ viết tắt, tiếng lóng và những thứ tương tự do người dùng nhập vào sẽ được đồng hóa vào cơ sở dữ liệu. Địa chỉ e-mail và URL cũng có thể được lưu trữ. Nếu cơ sở dữ liệu này được phục hồi, nó có thể tạo ra một số bằng chứng thú vị. Ví dụ: những kẻ ấu dâm có thể đã thường xuyên nhập các từ viết tắt phổ biến cho nội dung “đen” (CP). Một kẻ buôn ma túy có thể thường xuyên nhập tiếng lóng hoặc một từ mã cho sản phẩm của họ khi nhắn tin cho người mua.

Một số công ty sản xuất công nghệ này. Một số ví dụ là Tegic Communication's, T9 ( [www.T9.com](http://www.T9.com) ), Motorola's iTap, and ZiCorp's eZiText ( [Kessler, 2011](#16__Kessler__G__C___2011__June) ).

### 4.1 Bản ghi chi tiết cuộc gọi

Bản ghi chi tiết cuộc gọi (CDR) thường được nhà cung cấp sử dụng để khắc phục sự cố và cải thiện hiệu suất mạng. CDR cũng có giá trị đối với người điều tra. Họ có thể cho chúng ta thấy:

Ngày / giờ cuộc gọi bắt đầu và kết thúc.



Ai đã thực hiện cuộc gọi và ai đã được gọi.



Cuộc gọi kéo dài bao lâu.



Cho dù cuộc gọi đến hay cuộc gọi đi.



Các tháp khởi đầu và kết thúc.



Mặc dù CDR có thể cho bạn biết rất nhiều điều nhưng họ không thể cho bạn biết ai là người thực sự thực hiện cuộc gọi.

Bạn nhận được những gì bạn yêu cầu; do đó điều quan trọng là phải hiểu sự khác biệt giữa CDR và thông tin thuê bao. Thông tin thuê bao và bản ghi chi tiết cuộc gọi không giống nhau. Thông tin thuê bao điển hình sẽ bao gồm những thứ như tên, địa chỉ và điện thoại. Các mục khác đi kèm với thông tin người đăng ký là số tài khoản, địa chỉ e-mail, dịch vụ, cơ chế thanh toán, v.v.

Mọi nhà cung cấp dịch vụ đều lưu giữ tất cả các bản ghi này trong một khoảng thời gian xác định trước. Khoảng thời gian được ghi rõ trong chính sách lưu giữ dữ liệu của họ. Khoảng thời gian lưu giữ cũng không đồng nhất trên tất cả các loại dữ liệu. Ví dụ: một số nhà cung cấp dịch vụ có thể giữ dữ liệu SMS chỉ từ bảy đến mười bốn ngày. Ngược lại, thông tin ngành ô có thể được lưu giữ một năm hoặc lâu hơn. Điều rút ra ở đây là bạn không có thời gian vô hạn để nộp các thủ tục giấy tờ cần thiết để đảm bảo rằng các hồ sơ bạn tìm kiếm sẽ không bị xóa.

Các nhà cung cấp dịch vụ thường duy trì hồ sơ tỉ mỉ về người đăng ký và các hoạt động của họ để thanh toán và các mục đích khác. Kho thông tin này có thể rất hữu ích trong quá trình điều tra. Các hồ sơ của nhà cung cấp dịch vụ này có thể cho chúng ta biết tên, địa chỉ, số điện thoại bổ sung, số An sinh xã hội, v.v. Thông tin tín dụng trong hồ sơ có thể cung cấp cho các nhà điều tra địa chỉ thanh toán, số thẻ tín dụng, v.v.

Bản ghi chi tiết cuộc gọi mô tả chi tiết cụ thể của từng cuộc gọi đến và đi. Chúng không nên nhầm lẫn với hồ sơ thu phí. Hồ sơ thu phí đề cập đến thông tin điện thoại cố định chứ không phải điện thoại di động. Khi yêu cầu bản ghi chi tiết cuộc gọi, bạn phải chỉ định một phạm vi ngày. Đó là một phương pháp khôn ngoan để đưa ra yêu cầu của bạn trong một hoặc hai ngày ở cả hai đầu.

Các bản ghi chi tiết cuộc gọi, khi được kết hợp với địa chỉ thực của các tháp, có thể cho chúng ta thấy vị trí bắt đầu và kết thúc của cuộc gọi. Các bản ghi này cũng hiển thị các trang web di động đã được sử dụng, thời lượng cuộc gọi, thời gian cuộc gọi bắt đầu, các số được gọi bởi điện thoại mục tiêu, v.v. ( [Jansens & Ayers, 2007](#15__Jansen_W__Ayers_R__Guideline) ).

Hồ sơ thanh toán không đại diện cho một danh sách đầy đủ các cuộc gọi đến và đi. Nhật ký cuộc gọi sẽ bao gồm dữ liệu chưa được đưa vào hệ thống thanh toán.

Thông tin được các nhà cung cấp dịch vụ lưu giữ có thể sẽ có thời hạn sử dụng ngắn, được xác định trước. Mỗi nhà cung cấp dịch vụ có một số quyết định về cách bảo quản những dữ liệu này và chúng được lưu trữ trong bao lâu. Điều này thường được mô tả trong các chính sách duy trì của công ty. Theo thực tiễn này, các thủ tục giấy tờ pháp lý nên được tạo ra và cung cấp sớm hơn là muộn hơn. Điều này sẽ giúp đảm bảo rằng bằng chứng của bạn sẽ không bị lật tẩy trước khi nó có thể được bảo quản và thu thập.

Có thể định vị điện thoại di động (với các mức độ chính xác khác nhau) bằng một số phương tiện khác nhau. Phương pháp tam giác là một trong những phương pháp được biết đến nhiều hơn. Trong phương pháp tam giác, vị trí gần đúng của điện thoại được xác định bằng cách sử dụng khoảng cách của nó từ ba tháp khác nhau. Khoảng cách được tính bằng cách xác định độ trễ tín hiệu từ điện thoại (hoặc thiết bị cầm tay) đến ba tháp. Một ăng ten định hướng cũng có thể được sử dụng cho mục đích này. Một lần nữa, độ trễ tín hiệu được sử dụng để xác định khoảng cách, nhưng lần này chỉ cần hai tháp vì chúng cũng có thể xác định hướng. Cuối cùng, vị trí có thể được xác định thông qua GPS bằng cách sử dụng vĩ độ và kinh độ.

### 4.2 Thu thập và Xử lý Bằng chứng Điện thoại Di động

Bởi vì dữ liệu điện thoại di động không giống như các dạng bằng chứng kỹ thuật số khác, các nguyên tắc cơ bản trong việc xử lý bằng chứng kỹ thuật số cũng áp dụng cho điện thoại di động. Công việc đầu tiên khi xử lý điện thoại di động là cách ly nó khỏi mạng. Cô lập điện thoại là bắt buộc. Ngoài nguy cơ bị xóa từ xa (bởi nghi phạm hoặc nhà cung cấp dịch vụ), mọi cuộc gọi đến, tin nhắn hoặc e-mail đều có thể ghi đè lên bất kỳ bằng chứng tiềm năng nào. Chúng ta có thể cách ly điện thoại một cách hiệu quả bằng cách sử dụng Faraday hoặc lon đốt. Túi Faraday, thể hiện trong [Hình 10.2](#F0015_4) , là một thùng chứa đặc biệt được làm bằng vật liệu dẫn điện có tác dụng chặn tín hiệu vô tuyến một cách hiệu quả. Một cái lon đốt thực sự không hơn gì một cái thùng sơn rỗng, sạch sẽ. Những thùng chứa này có thể được tìm thấy trong các cửa hàng phần cứng hoặc đồ gia dụng.



Hình 10.2 Một túi Faraday và điện thoại di động.

Nếu điện thoại đang bật khi bạn khôi phục, hãy để điện thoại bật. Nếu có sự chậm trễ đáng kể trong việc đưa điện thoại đến phòng thí nghiệm, thì bạn có thể cân nhắc việc tắt nó đi. Điều này được thực hiện để đảm bảo rằng pin không bị cạn kiệt hoàn toàn. Nếu có, bạn có nguy cơ bị khóa điện thoại. Nếu điện thoại được bảo vệ bằng mã PIN, việc tắt điện thoại sẽ dẫn đến việc điện thoại bị khóa khi bật lại.

Cách ly điện thoại khi bật nguồn tạo ra một số lo ngại về tuổi thọ pin. Hãy nhớ rằng, trong khi điện thoại đang bật, điện thoại sẽ liên tục cố gắng kết nối với mạng, làm hao pin hơn. Pin hết cũng có thể kích hoạt chức năng bảo mật, khóa điện thoại.

Nếu điện thoại bị tắt, chúng ta có thể tháo pin cũng như tháo và khởi tạo thẻ SIM. Chúng ta cũng sẽ muốn chụp ảnh điện thoại, mặt trước và mặt sau. Trong quá trình này, chúng ta sẽ đặc biệt chú ý đến các số nhận dạng bên dưới pin ( IMEI , ESN / MEID) . Chúng ta cũng sẽ muốn cách ly điện thoại khỏi mạng, giống như điện thoại được cấp nguồn.

Trước khi tiến hành điều tra pháp y, điều quan trọng là phải xác định được sản phẩm và kiểu dáng của thiết bị cầm tay mà bạn đang sử dụng. Thông tin này có thể giúp bạn hiểu đầy đủ về các chức năng, tính năng và khả năng của điện thoại. Thông thường, bạn có thể tìm thấy sản phẩm và kiểu máy của điện thoại bên dưới pin của điện thoại. Thông tin tương tự này cũng có thể được tìm thấy trong hệ thống tệp của điện thoại.

Giống như máy tính, chúng ta chỉ muốn truy cập hoặc điều tra bằng chứng ban đầu như một biện pháp cuối cùng tuyệt đối. Tốt nhất, một công cụ pháp y nên được sử dụng để thu thập dữ liệu trước tiên, cung cấp cho người giám định một bản sao để làm việc. Tuy nhiên, cuối cùng, điều tra thủ công có thể là giải pháp thay thế duy nhất. Nếu điều này là cần thiết, bạn sẽ phải trình bày rõ lý do của mình đằng sau việc thực hiện quá trình hành động này. Tài liệu chi tiết sẽ rất hữu ích trong việc tính toán tương tác của bạn với thiết bị và thiết lập tính toàn vẹn của bất kỳ bằng chứng nào đã được phục hồi. Việc ghi lại một cuộc điều tra thủ công thường chủ yếu dựa vào các bức ảnh thay vì bản thân bằng chứng kỹ thuật số. Trong trường hợp này, điều tra viên cần cẩn thận điều hướng qua điện thoại, chụp ảnh màn hình khi họ di chuyển.

Thư thoại là một nguồn bằng chứng tiềm năng khác không nên bỏ qua. Thông thường, để truy cập thư thoại, bạn sẽ cần mã đặt lại mật khẩu từ nhà cung cấp dịch vụ. Khi thu thập bằng chứng thư thoại, có một số lựa chọn. Nhà cung cấp dịch vụ có thể chỉ cần cung cấp cho bạn mã truy cập hoặc họ có thể cung cấp cho bạn bản sao của chính dữ liệu đó. Chi tiết này nên được làm việc sớm với nhà cung cấp, đặc biệt nếu bạn thích một phương pháp hoặc định dạng khác.

Tại hiện trường, bạn nên đề phòng các thiết bị cầm tay bổ sung, thẻ SIM cũng như cáp nguồn và cáp dữ liệu liên quan. Cáp nguồn sẽ giúp phòng thí nghiệm đảm bảo rằng bộ nhớ biến động vẫn còn nguyên vẹn cho đến khi nó có thể được thu thập và điều tra đúng cách. Đừng quên, trong khi bật điện thoại, nó sẽ liên tục tìm cách kết nối với mạng, làm hao pin nhanh chóng.

### 4.3 Mô-đun nhận dạng người đăng ký

mô-đun nhận dạng thuê bao (SIM) có thể là bằng chứng có giá trị. Chúng lưu trữ một lượng lớn thông tin và cần được thu thập và phân tích.

SIM chứa một vài số sẽ được quan tâm đặc biệt. Đầu tiên là Định danh thuê bao di động quốc tế (IMSI) . Thứ hai là Mã định danh thẻ mạch tích hợp (ICC-ID) . IMSI được sử dụng để xác định thông tin tài khoản và dịch vụ của người đăng ký. ICC-ID là số sê-ri của chính thẻ SIM. SIM có thể chứa:

Nhận dạng người đăng ký (IMSI)



Nhà cung cấp dịch vụ



Nhận dạng thẻ (ICC-ID)



Tùy chọn ngôn ngữ



Vị trí điện thoại khi tắt nguồn



Số điện thoại do người dùng lưu trữ



Số do Người dùng gọi



Tin nhắn văn bản SMS (Có thể)



Tin nhắn văn bản SMS đã xóa (Có thể)



Các thẻ SIM chứa một số thành phần riêng lẻ bao gồm bộ xử lý (CPU), RAM, bộ nhớ không bay hơi dựa trên Flash và chip mật mã. Chúng được sử dụng trong tất cả các điện thoại nhưng có mặt trong các thiết bị cầm tay GSM, iDEN và Blackberry.

Mã số nhận dạng cá nhân (PIN) có thể được sử dụng để bảo vệ dữ liệu SIM. Mã PIN có độ dài từ bốn đến tám chữ số. Là một lớp bảo mật bổ sung, chỉ có thể thực hiện ba lần thử để nhập đúng mã PIN. Sau lần thử thứ ba không thành công, dữ liệu chỉ có thể được truy cập bằng Khóa mở khóa mã pin (PUK) gồm tám chữ số cùng với mã PIN mới. Nỗ lực để vào PUK cũng bị hạn chế. Sau 10 lần thử không thành công, nhiều thẻ SIM sẽ vĩnh viễn từ chối quyền truy cập bằng PUK.

### 4.4 Mua lại điện thoại di động: Vật lý và logic

Dữ liệu trên điện thoại di động có thể được lấy theo một trong hai cách: vật lý hoặc logic. Một chuyển đổi vật lý nắm bắt tất cả dữ liệu trên một phần vật lý của phương tiện lưu trữ. Đây là một bản sao bit-for-bit, giống như bản sao của một ổ cứng. Phương pháp thu nhận này cũng nắm bắt thông tin đã bị xóa. Ngược lại, một chuyển đổi logic chỉ nắm bắt các tệp và thư mục mà không có bất kỳ dữ liệu nào bị xóa. Dữ liệu có thể được thu thập bằng các công cụ phi pháp lý như những công cụ được sử dụng để đồng bộ hóa hoặc sao lưu dữ liệu trên điện thoại di động ( [Jansen & Ayers, 2007](#15__Jansen_W__Ayers_R__Guideline) ). Mặc dù quy trình này tương tự như quy trình được sử dụng để mua ổ cứng, nhưng có một điểm khác biệt quan trọng. Trong trường hợp này, không có thiết bị chặn ghi nào được sử dụng. Điện thoại phải có thể tương tác với phần cứng và phần mềm của điện thoại.

Điều tra thủ công đòi hỏi phải tương tác với thiết bị thông qua bàn phím hoặc màn hình cảm ứng. Mặc dù việc điều tra hoặc tương tác với bằng chứng ban đầu không bao giờ là lựa chọn đầu tiên của chúng ta, nhưng đôi khi nó có thể là lựa chọn duy nhất. Ví dụ, trong trường hợp thời gian là quan trọng, có thể cần phải bỏ qua các thủ tục pháp y thích hợp. Những tình huống đó có thể bao gồm việc xác định vị trí một đứa trẻ mất tích hoặc ngăn chặn một hành động bạo lực sắp xảy ra. Trong các tình huống khác, thậm chí không thể khai thác dữ liệu hoặc trích xuất chúng theo cách có thể bảo toàn tính toàn vẹn của chúng. Điều này có thể xảy ra trong trường hợp các công cụ và kỹ thuật pháp y không bắt kịp với công nghệ mới nhất.

## Công cụ pháp y trên điện thoại di động

Như bạn có thể nghi ngờ, có rất nhiều công cụ khác nhau có sẵn để điều tra điện thoại. Những công cụ này có thể ở dạng phần cứng hoặc phần mềm. Một trong những thực tế là không phải tất cả các công cụ này đều hỗ trợ tất cả các điện thoại di động. Để làm phức tạp thêm vấn đề, hai công cụ thực sự hỗ trợ một điện thoại nhất định có thể không đọc và khôi phục thông tin giống nhau.

Những gì sau đây là một mẫu các công cụ có sẵn cho pháp y điện thoại di động. Một cuộc điều tra kỹ lưỡng về chức năng và các tính năng cho thấy rằng không có công cụ nào làm được tất cả. Một sự khác biệt rõ ràng là số lượng điện thoại được hỗ trợ. Ngân sách cho phép, hầu hết các phòng thí nghiệm sẽ có sẵn nhiều công cụ để tăng khả năng của họ. [Hình 10.3](#F0020_4) cho thấy một thiết bị Cellebrite UFED.



Hình 10.3 Một UFED của Cellebrite.

BitPim là một ứng dụng mã nguồn mở mạnh mẽ không được xây dựng cho các mục đích pháp y. BitPim được thiết kế để hoạt động với điện thoại CDMA được sản xuất bởi một số nhà cung cấp, bao gồm cả LG và Samsung và những nhà cung cấp khác. BitPim có thể khôi phục dữ liệu như danh bạ, lịch, hình nền, nhạc chuông và hệ thống tệp ( <http://www.bitpim.org/>).

Bộ pháp y Oxy là một chương trình pháp y được thiết kế đặc biệt cho điện thoại di động. Đó là một công cụ hỗ trợ hơn hai mươi ba trăm thiết bị. Nó trích xuất dữ liệu như danh bạ, dữ liệu thẻ SIM, danh sách liên lạc, nhóm người gọi, nhật ký cuộc gọi, thư mục SMS / MMS / e-mail tiêu chuẩn và tùy chỉnh, tin nhắn SMS đã xóa, lịch, ảnh, video, ứng dụng JAVA và vị trí GPS ( [http : //www.oxygen-forensic.com/en/](http://www.oxygen-forensic.com/en/) ).

Tập đoàn Paraben cung cấp một số sản phẩm phần cứng và phần mềm nhắm mục tiêu đến pháp y thiết bị di động. Ngoài điện thoại di động, các công cụ của họ cũng hỗ trợ các thiết bị GPS như của Garmin ( <http://www.paraben.com/handheld-forensics.html>).

MPE + của AccessData hỗ trợ hơn ba mươi lăm trăm điện thoại. Đó là một công cụ phục hồi pháp y di động tại hiện trường có thể thu thập lịch sử cuộc gọi, tin nhắn, ảnh, thư thoại, video, lịch và sự kiện. Nó có thể phân tích và tương quan nhiều điện thoại và máy tính sử dụng cùng một giao diện. ( <http://accessdata.com/products/computer-forensics/mobile-phone-examiner>).

Cellebrite UFED (Thiết bị trích xuất pháp y đa năng) là một thiết bị phần cứng độc lập, khép kín được sử dụng để trích xuất Danh bạ, hình ảnh, video, SMS, MMS, lịch sử cuộc gọi và hơn thế nữa. Nó hỗ trợ hơn 25 trăm điện thoại và được thiết kế để trích xuất thông tin tại hiện trường. Nó cũng có một đầu đọc thẻ SIM và bộ sao chép. Ngoài ra, còn có một điều thú vị là các thiết bị Cellebrite (phiên bản không có ở ngoài) có thể được tìm thấy trong nhiều cửa hàng điện thoại di động. Chúng được sử dụng để chuyển dữ liệu của khách hàng từ thiết bị này sang thiết bị khác. ( <http://www.cellebrite.com/forensic-products/forensic-products.html?loc=seg>).

EnCase Smartphone Examiner là một công cụ EnCase được thiết kế để xem xét và thu thập dữ liệu từ điện thoại thông minh và thiết bị máy tính bảng. Nó thu thập dữ liệu từ các bản sao lưu của Blackberries, iTunes và thẻ SD. Khi thông tin được thu thập, nó sẽ dễ dàng được nhập vào bộ EnCase Foreician để tiếp tục điều tra ( <http://www.guidancesoftware.com/encase-smartphone-examiner.htm>).

Vì vậy, bạn sẽ làm gì nếu không có công cụ nào trong số này truy xuất thông tin bạn đang tìm kiếm? Nếu đúng như vậy, đã đến lúc cân nhắc việc chuyển sang “trường cũ” và chỉ đơn giản là sử dụng máy quay phim hoặc ảnh tĩnh. Mặc dù đây không phải là lựa chọn đầu tiên, nhưng vẫn tốt hơn là ra đi tay trắng.

## Hệ thống định vị toàn cầu (GPS)

Giống như điện thoại di động, Hệ thống Định vị Toàn cầu (GPS) có thể là một nguồn bằng chứng to lớn. Chúng có thể được sử dụng để xác định chính xác vị trí của nghi phạm cũng như bản thân các hành vi phạm tội (nếu thiết bị đang hoạt động và thuộc quyền sở hữu của họ vào thời điểm phạm tội). Chúng cũng có thể được sử dụng để chỉ nơi những kẻ tình nghi dự định đi đến. Một số đơn vị GPS có thể cung cấp nhiều bằng chứng hơn, bao gồm nhật ký điện thoại di động, tin nhắn SMS và hình ảnh. Với những khả năng này cùng với dung lượng lưu trữ lớn, việc điều tra các thiết bị này là rất xứng đáng.

GPS ban đầu được sản xuất để sử dụng trong quân sự nhưng cuối cùng đã được chia sẻ với mọi người. Có 27 vệ tinh GPS trong hệ thống GPS. Chỉ có hai mươi tư được sử dụng tại một thời điểm. Ba vệ tinh còn lại được dự trữ trong trường hợp một trong các vệ tinh chính gặp sự cố. Một máy thu GPS tính toán vị trí của nó thông qua một quá trình toán học được gọi là trilateration ( [Brian & Harris, 2011](#9__Brian__M_____Harris__T___n_d) ).

Không phải tất cả các đơn vị GPS đều giống nhau. Một số tính năng phong phú, trong khi những người khác khá cơ bản. Chúng ta có thể tách thiết bị GPS thành bốn loại: đơn giản, thông minh, kết hợp và kết nối. Các đơn vị đơn giản được thiết kế để đưa người dùng từ điểm này đến điểm khác. Hầu hết các đơn vị đơn giản có thể lưu trữ các điểm theo dõi , điểm tham chiếu và nhật ký theo dõi . Các tính năng khác có thể có tùy thuộc vào kiểu dáng và kiểu máy ( [LeMere, 2011](#17__LeMere__B___n_d____Enhancing) ).

Các đơn vị thông minh có thể được chia nhỏ thành các thiết bị lưu trữ trên ô tô và USB. Các thiết bị này thường có bộ nhớ tối thiểu 2GB cùng với thẻ SD. Chúng cung cấp chức năng cơ bản giống như các hệ thống đơn giản. Ngoài ra, họ có thể chơi nhạc MP3, xem hình ảnh và lưu lại những địa điểm yêu thích.

Các đơn vị GPS kết hợp rất phong phú về tính năng và có thể cung cấp rất nhiều bằng chứng. Các thiết bị lai có các tính năng tương tự như các thiết bị thông minh cộng với một số. Đáng chú ý nhất, các thiết bị này cung cấp khả năng truy cập rảnh tay vào điện thoại di động của bạn qua Bluetooth. Khả năng tương tác với điện thoại di động này có thể cung cấp nguồn thứ cấp của phần lớn dữ liệu được tìm thấy trên điện thoại. Điều này sẽ bao gồm nhật ký cuộc gọi, sổ địa chỉ, cũng như địa chỉ MAC của tối đa mười điện thoại cuối cùng đã kết nối với thiết bị. Cuối cùng, tin nhắn SMS cũng có thể được phục hồi ( [LeMere, 2011](#18__LeMere__B___2011__April_25) ).

Một đơn vị được kết nối cung cấp các tính năng kết hợp và khả năng nhận thông tin thời gian thực bao gồm các tìm kiếm trên Google và thông tin giao thông. Các thiết bị này có đài GSM cùng với thẻ SIM. Chức năng này dựa trên đăng ký và như vậy, chúng ta có thể lấy thông tin người đăng ký được liên kết với tài khoản.

Dữ liệu GPS có thể được nhóm thành hai loại: dữ liệu hệ thống và dữ liệu người dùng. Dữ liệu hệ thống sẽ cung cấp cho chúng ta các điểm theo dõi và nhật ký theo dõi. Các điểm theo dõi là một bản ghi về vị trí đơn vị đã ở. Chúng được tạo tự động bởi hệ thống. Người dùng không thể thay đổi điểm theo dõi. Theo mặc định, hệ thống xác định khoảng thời gian mà chúng được ghi lại. Tuy nhiên, người dùng có thể sửa đổi cài đặt này, thay đổi khoảng thời gian hoặc khoảng cách. Nhật ký theo dõi là một danh sách toàn diện của tất cả các điểm theo dõi. Danh sách này nhằm giúp người dùng tìm lại đường dẫn của họ ( [LeMere, 2011](#18__LeMere__B___2011__April_25) ).

Điểm tham chiếu là một phần của dữ liệu do người dùng tạo. Khi diễn giải một điểm tham chiếu, bạn cần ghi nhớ chúng đại diện cho điều gì. Không giống như điểm theo dõi, điểm tham chiếu không phải lúc nào cũng chỉ ra vị trí thực tế mà đơn vị đã ở. Chúng có thể là những địa điểm mà người dùng dự định đến thăm. Người dùng có thể nhập các vị trí này dựa trên địa chỉ, tọa độ thực tế hoặc từ danh sách Điểm ưa thích (POI) do nhà sản xuất đơn vị GPS cung cấp.

Theo nhiều khía cạnh, thiết bị GPS tương tự như điện thoại di động và được xử lý theo cùng một cách. Chúng có thể có bộ nhớ dễ bay hơi cần được bảo tồn. Khi được bật nguồn, các thiết bị này liên tục tương tác với các vệ tinh ở trên. Sự tương tác này có thể gây ra các biến chứng từ góc độ pháp y, có khả năng khiến bằng chứng liên quan bị ghi đè hoặc làm ảnh hưởng đến tính toàn vẹn của nó.

Các thiết bị GPS đang xuất hiện ở nhiều nơi khác nhau. Xe taxi, xe tải giao hàng, v.v. thường xuyên được trang bị các thiết bị GPS. Một ví dụ như vậy về một đơn vị GPS hỗ trợ các nhà điều tra là trường hợp của vũ công Las Vegas Debbie Flores-Narvaez. Vụ giết người tàn bạo vào tháng 12 năm 2010 đã cho thấy giá trị của bằng chứng GPS. Cảnh sát đã có thể xác định vị trí còn lại của cô ấy bằng cách sử dụng dữ liệu GPS từ một chiếc xe tải U-Haul. Nghi phạm, Jason “Blu” Griffith, dường như đã vận chuyển hài cốt của cô ấy trong xe tải và không biết rằng xe tải được trang bị GPS. Cảnh sát đã lấy được dữ liệu GPS và sử dụng chúng để theo dõi các chuyển động của Griffith, dẫn đến thi thể của cô.

Bằng chứng trong vụ án còn có tin nhắn. Mẹ của nạn nhân, Elise Narvaez, nói rằng con gái bà đã gửi cho bà tin nhắn này vào ngày 1 tháng 12 năm 2010: “Trong trường hợp có trường hợp khẩn cấp với tôi, hãy liên hệ với Blu Griffith ở Vegas. Bạn trai cũ của tôi. Không phải bạn thân nhất của tôi ”( [Hartenstein & Sheridan, 2010](#12__Hartenstein__M_____Sheridan) ).

Hỏi và đáp với Christopher Vance

Christopher Vance là Chuyên gia pháp y kỹ thuật số hỗ trợ Đơn vị pháp y kỹ thuật số của Cảnh sát bang Tây Virginia. Trong phần Hỏi & Đáp tại đây, anh ấy chia sẻ một số hiểu biết của mình từ các chiến hào.

[Q] Bạn thấy thách thức pháp y lớn nhất khi xử lý điện thoại di động là gì?

[A] Vance: Thách thức lớn nhất duy nhất khi xử lý pháp y điện thoại di động là có hàng nghìn điện thoại, mỗi loại có hệ điều hành khác nhau. Có rất nhiều sự đa dạng khi xử lý các thiết bị di động, không thể thành thạo mọi cấu trúc hoạt động. Đó là một quá trình học hỏi liên tục bằng cách thử và sai và xác nhận.

[Q] Bạn sẽ đưa ra lời khuyên nào cho một điều tra viên mới muốn tìm hiểu thêm về điện thoại di động?

[A] Vance: Có rất nhiều cơ hội đào tạo ngoài kia, đặc biệt là cho việc thực thi pháp luật. Tuy nhiên, ngay cả với những khóa đào tạo tốt nhất, bạn hoàn toàn có thể sử dụng một số thiết bị và thử nó cho chính mình.

[Q] Giáo dục thường xuyên quan trọng như thế nào?

[A] Vance: Trong lĩnh vực này, có lẽ điều quan trọng nhất là ở đó.

[Q] Bạn thấy điện thoại di động được sử dụng trong việc phạm tội như thế nào?

[A] Vance: Tùy thuộc vào loại trường hợp, có nhiều cách chúng được sử dụng. Tuy nhiên, các bằng chứng lớn nhất thường truy ngược lại các tin nhắn SMS / MMS, hình ảnh được lưu trữ và Nhật ký cuộc gọi. Từ buôn bán ma túy, gạ gẫm, đến giết người, đây dường như luôn là chìa khóa lớn nhất của vụ án nếu có bằng chứng trên thiết bị cầm tay.

[Q] Bạn có thể nói một chút về quy trình chung mà bạn tuân theo khi tiến hành khám bệnh?

[A] Vance: Hai chìa khóa lớn nhất là Isolation và Validation. Bước đầu tiên luôn là cách ly thiết bị của bạn khỏi mạng của nó và giữ nguyên như vậy cho đến khi hoàn thành trường hợp. Sau đó, sử dụng nhiều công cụ và quy trình khác nhau (vì không có “siêu công cụ” nào hoạt động trên mọi thiết bị) tôi sẽ thu thập dữ liệu. Sau khi dữ liệu được thu thập, tôi cố gắng xác thực dữ liệu bằng cách sử dụng nhiều công cụ, giá trị băm hoặc thậm chí xác thực trực quan trong khi điều tra dữ liệu so với những gì điện thoại đang nói.

[Q] Bạn thấy những thiết bị di động nào khác được đưa đến phòng thí nghiệm? Bạn đang phục hồi những bằng chứng nào từ những thứ đó?

[A] Vance: Hai thiết bị di động lớn nhất ngoài điện thoại di động là thiết bị iPod Touch và Máy tính bảng. Vì các thiết bị này có thể chạy cùng hệ điều hành với các thiết bị điện thoại di động của chúng, chúng ta thường có thể sử dụng giống nhau. Trong hầu hết các trường hợp, đó thường là nhật ký trò chuyện từ các ứng dụng của bên thứ ba được cài đặt trên thiết bị, chẳng hạn như Skype, TextNow, Yahoo!, V.v.

[Q] Theo quan điểm của bạn, tương lai nào cho pháp y điện thoại di động?

[A] Vance: Hy vọng rằng "chiếc điện thoại câm" sẽ chết hoặc bị đồng hóa. Nếu các hệ điều hành điện thoại thông minh lớn có thể đi đầu và tiêu chuẩn hóa thị trường một chút, nó sẽ làm cho công việc của các nhà phân tích và kỹ sư dễ dàng hơn nhiều. Theo ý kiến của tôi, một ngày nào đó chúng ta sẽ nói về hệ điều hành thiết bị di động giống như cách chúng ta đề cập đến “bộ ba lớn” Mac, Windows và Linux.

[Q] Bạn có thể nói một chút về các công cụ bạn sử dụng không?

[A] Vance: Tôi sử dụng rất nhiều công cụ để hoàn thành công việc. Không có một công cụ nào có thể tấn công mọi điện thoại mọi lúc và lấy tất cả dữ liệu. Nó chỉ không tồn tại. Trong phòng thí nghiệm của chúng ta, chúng ta sử dụng Cellebrite UFED Physical Pro, Máy điều tra điện thoại di động của AccessData +, Thu giữ thiết bị của Tập đoàn Paraben, viaExtract của Forensic, CellDek của LogicCube, Hộp Flasher và một số công cụ thích hợp khác được sử dụng theo thời gian.

[Q] Bạn có một vài "câu chuyện chiến tranh" có thể chia sẻ không?

[A] Vance: Có một vài trường hợp tôi đã làm việc mà bằng chứng thiết bị di động được chứng minh là súng hút thuốc. Gần đây, trong một cuộc điều tra vụ án mạng, có rất nhiều tin nhắn trên điện thoại từ nghi phạm đến nạn nhân không chỉ thông báo cho nạn nhân rằng nghi phạm đang lên kế hoạch sát hại cô mà còn cho biết tội ác sẽ diễn ra khi nào và như thế nào.   
Sau khi gây án, nghi phạm thậm chí còn sử dụng điện thoại của nạn nhân để gửi tin nhắn cho những người khác thú nhận tội lỗi của mình. Trong một trường hợp trưng cầu, chúng ta có một chiếc iPod Touch duy nhất, chúng ta tìm thấy bằng chứng về không chỉ một tội phạm trong nhật ký trò chuyện mà còn nhiều nạn nhân của cùng một tội phạm, tất cả đều do một cá nhân. Tôi thậm chí đã có trường hợp các cá nhân sẽ lưu trữ toàn bộ thư viện Nội dung “đen” của họ trên bộ nhớ trong điện thoại của họ.

[Q] Có những quan niệm sai lầm mà bạn muốn loại bỏ không?

[A] Vance: Chủ yếu những gì chúng ta gọi là “Hiệu ứng CSI”. Công việc không bao giờ nhanh chóng hay hào nhoáng như các chương trình truyền hình làm được. Trong nhiều trường hợp, công việc của chúng ta đôi khi cũng là một môn nghệ thuật giống như một môn khoa học. Khi xử lý các thiết bị di động, bộ nhớ mà chúng ta phải phân tích rất nhỏ và năng động nên việc khôi phục dữ liệu đã bị xóa trong nhiều trường hợp trở nên khó khăn hơn rất nhiều. Tuy nhiên, nó không phải là không thể.

[Q] Bạn sẽ so sánh và đối chiếu bằng chứng bạn tìm thấy trên điện thoại với bằng chứng thường thấy trên máy tính như thế nào?

[A] Vance: Dữ liệu thực sự liên quan đến nhau. Đã có nhiều trường hợp chúng ta có thể thấy nhật ký trò chuyện bắt đầu trên máy tính rồi chuyển sang thiết bị di động. Rất nhiều lần chúng ta vẫn thấy các loại dữ liệu giống nhau, chủ yếu là thông tin liên lạc và phương tiện do người dùng tạo. Tuy nhiên, khôi phục thông tin đã xóa từ máy tính dễ dàng hơn nhiều so với điện thoại di động.

[Q] Dữ liệu vị trí địa lý có vai trò lớn như thế nào trong các cuộc điều tra của bạn?

[A] Vance: Có rất nhiều vấn đề với dữ liệu vị trí địa lý mà chúng không đóng một vai trò quan trọng nào cho đến nay. Đã có những cuộc điều tra mà chúng ta đã tìm thấy những hình ảnh có nhúng dữ liệu GPS để hỗ trợ các nhà điều tra. Các cuộc tranh luận về "theo dõi" GPS đầu [tiên](#1_Researchers_discovered_that_th) của năm nay là không cần thiết. Mặc dù dữ liệu GPS có thể hỗ trợ một trường hợp, nhưng sẽ cần phải xác thực nghiêm túc để đảm bảo rằng hồ sơ bạn có chính xác là những gì bạn đang tìm kiếm. Chỉ vì bạn có các điểm định vị không phải là một chỉ báo 100 phần trăm mà cá nhân của bạn đang ở chính xác điểm và vị trí đó.

[Q] Bạn muốn thêm điều gì khác không?

[A] Vance: Điện thoại di động hoặc Pháp y di động đang trở thành chuyên môn riêng trong lĩnh vực pháp y kỹ thuật số. Tôi có thể dễ dàng nhận thấy rằng một ngày nào đó làn sóng công nghệ mới này sẽ thay thế các máy cũ của chúng ta giống như cách mà “Đám mây” đe dọa làm.

## 7. Bản tóm tắt

Công nghệ di động của chúng ta cho phép chúng ta điều tra e-mail, duyệt Internet, vạch ra một chuyến đi và truy cập ngay lập tức vào những người khác trong cuộc sống của chúng ta. Nhiều người không thể nhớ khi nào hoặc thậm chí không thể tưởng tượng họ đã làm thế nào để sống cả ngày mà không có điện thoại thông minh. Sự ra đời của công nghệ này vừa tạo ra nguồn chứng cứ vừa là thách thức đối với những người giám định pháp y.

Trong Chương 10, chúng ta đã đề cập đến một loạt các chủ đề về thiết bị di động, đặc biệt là điện thoại di động và thiết bị GPS. Mạng di động bao gồm một số thành phần bao gồm các trạm gốc, Trung tâm Chuyển mạch Di động, Sổ đăng ký Vị trí của Khách truy cập và các thành phần khác. Có nhiều loại mạng di động khác nhau, mỗi loại có những đặc điểm riêng biệt. Đa truy nhập phân chia theo mã (CDMA), Hệ thống toàn cầu cho Truyền thông di động (GSM) và Mạng được nâng cao kỹ thuật số tích hợp (iDEN) là những mạng phổ biến nhất.

Giống như máy tính, có nhiều hơn một hệ điều hành được sử dụng bởi điện thoại di động. Windows Mobile, iOS, Android và Symbian đã được đề cập trong Chương 10. Điện thoại di động có thể chứa rất nhiều bằng chứng kỹ thuật số bao gồm e-mail, nhật ký cuộc gọi, tin nhắn văn bản, hình ảnh, video và hơn thế nữa.

Hồ sơ do nhà cung cấp dịch vụ lưu trữ cũng có thể có giá trị trong quá trình điều tra, đặc biệt là Hồ sơ chi tiết cuộc gọi. Những hồ sơ này có thể cung cấp cho chúng ta ngày, giờ, số điện thoại, cũng như các tháp bắt đầu và kết thúc được sử dụng trong một cuộc gọi. Thông tin về tháp có thể giúp chúng ta xác định vùng lân cận chung mà điện thoại đã được sử dụng.

Bằng chứng điện thoại di động được thu thập và lưu giữ như thế nào là cực kỳ quan trọng. Ưu tiên đầu tiên khi xử lý bất kỳ thiết bị di động nào là cách ly nó khỏi mạng. Một thiết bị được cấp nguồn không bị cô lập là một vấn đề lớn. Ở trạng thái này, bằng chứng có thể bị thay đổi, ghi đè hoặc tiêu hủy. Hãy nhớ rằng một số điện thoại di động nhất định có thể bị kẻ tình nghi hoặc nhà cung cấp dịch vụ xóa từ xa. Cô lập điện thoại di động có thể được thực hiện bằng cách sử dụng túi Faraday hoặc hộp đốt. Mặc dù Mô-đun Nhận dạng Người đăng ký hoặc thẻ SIM chứa dữ liệu đáng được điều tra, nhưng điều quan trọng cần nhớ là không phải tất cả các điện thoại đều có chúng.

GPS hoặc Hệ thống Định vị Toàn cầu ngày nay đang được sử dụng rộng rãi và hoạt động như một nguồn bằng chứng kỹ thuật số khác. Có nhiều loại đơn vị GPS khác nhau bao gồm đơn giản, thông minh, kết hợp và kết nối. Điểm tham chiếu, điểm theo dõi và nhật ký theo dõi là một số dữ liệu được ghi lại bởi các đơn vị mà chúng ta có thể sử dụng. Những hiện vật này có thể cho chúng ta biết đơn vị đã ở đâu và người dùng dự định đi đâu.

## Tổng kết và kiến thức thêm chương 10

1. **Vai trò của điều tra thiết bị di động**

Điều tra thiết bị di động là hành động khôi phục thông tin và bằng chứng từ thiết bị di động. Thông thường, những bằng chứng số liên quan đến thiết bị di động là bộ nhớ trong thiết bị, thẻ SD, và thẻ SIM.

Một số cách thức tấn công thiết bị di động gồm:

Tấn công web

Malware

Social Engineer

DdoS

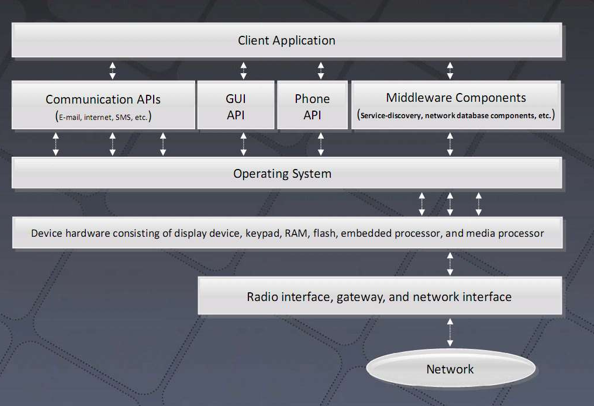
1. **Vai trò của phần cứng và OS của điện thoại khi thực hiện điều tra**

Điều tra điện thoại được chia thành 2 phân lớp:

Điều tra phần cứng – Phụ thuộc vào từng loại phần cứng cũng như thiết kế kỹ thuật các phần cứng. Cần phải sử dụng nhiều phương pháp điều tra, trong một số trường hợp thì sẽ cần sự phối hợp từ nhà cung cấp.

Điều tra hệ điều hành – Phụ thuộc vào hiểu biết của điều tra viên về hệ điều hành, quá trình khởi động hệ điều hành.

1. **Phân lớp kỹ thuật của một thiết bị di động**

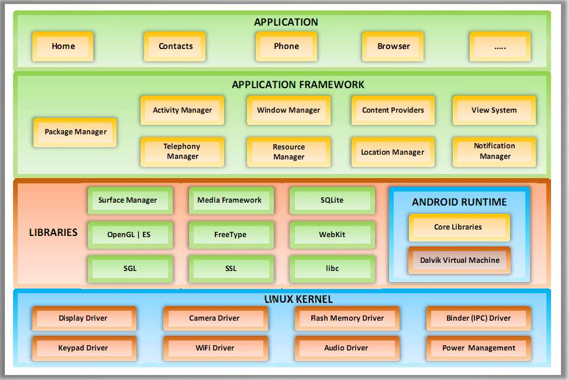


Lớp trình bày (presentation layer): Client Application Communication APIs, GUI API, Phone API, các thành phần middleware

Lớp vận hành (business layer): OS, các phần cứng khác

Lớp dữ liệu (data layer): Các cổng thông tin, kết nối mạng.

1. **Mô hình của một điện thoại dùng hệ điều hành Android**



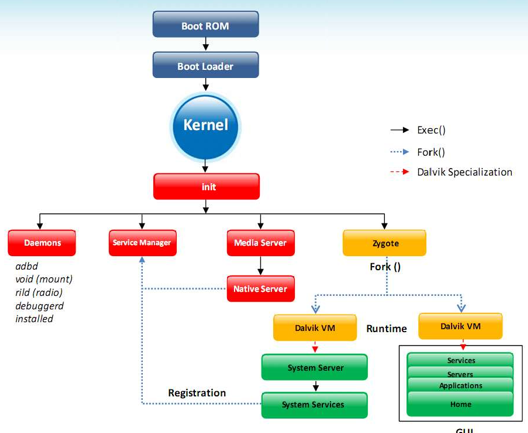
Lớp ứng dụng: Những ứng dụng cơ bản hoặc được cài đặt bởi người dùng

Lớp vận hành ứng dụng: Gồm những API kết nối với các ứng dụng

Lớp thư viện: Bao gồm những thư viện được viết bằng C/C++ được sử dụng để quản lý, vận hành các loại thông tin. Các máy ảo, thư viện của hệ điều hành

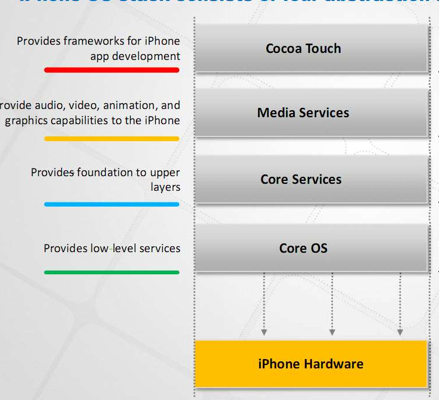
Linux Kernel: Phụ trách giao tiếp với các phần cứng

Mô hình khởi động của hệ điều hành Android



* Linux Kernel giao tiếp và thực hiện quá trình gọi init (một phiên khởi động, làm viêc)
* Init bắt đầu khởi động và chạy các quá trình cần thiết cũng như daemons (Disk And Execution Monitor) đễ thực hiện các middleware cơ bản
* Middleware cơ bản này (được gọi là zygote) sẽ thực hiện thu thập, lấy dữ liệu từ các thư viện Java, các chương trình được lưu trữ
* Sau đó, midleware này sẽ lưu lại và chờ đợi lệnh tiếp theo

1. **Mô hình của một điện thoại dùng hệ điều hành iOS**



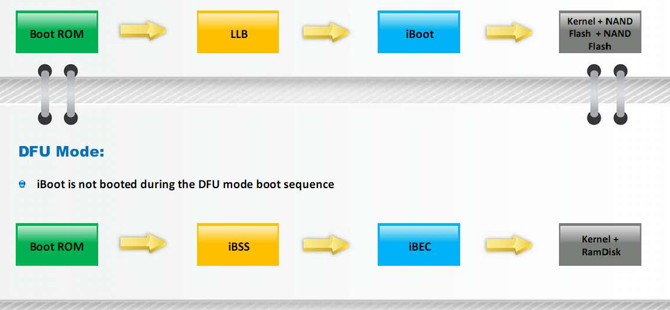
Cocoa Touch – Cung cấp môi trường để chạy các ứng dụng của Iphones

Media Services – Phụ trách cung cấp khả năng nhận diện các hình ảnh, video cho Iphone

Core Services – Cung cấp các dịch vụ nền tảng, hỗ trợ cho các dịch vụ trên

Core OS – Cung cấp các địch vụ nền tảng thiết yếu

Mô hình khởi động hệ điều hành iOS



Thông thường, Iphone sẽ được khởi động theo các bước như:

* BootROM – thực hiện quá trình khởi động
* LLB – Bước đầu tiên trong quá trình khởi động, được tải về sau khi đã kiểm tra tính chính xác
* iBoot – là bước tiếp theo của quá trình khởi động, được chạy sau khi đã kiểm tra thiết bị
* Kernel+NAND Flash – chạy các dịch vụ hệ điều hành và khởi động các phần cứng

Trong trường hợp cần điều tra, điều tra viên phải khởi động dưới dạng DFU, thay vì khởi động LLB, ta cần khởi động iBSS và tránh việc khởi động iBoot để có thể thấy được RAMDISK.

1. **Xác định nơi lưu trữ dữ liệu và các bằng chứng**

Bộ nhớ trong:RAM, ROM, Mobile OS, metadata

Thẻ SIM: Thông tin cá nhân, danh bạ, tin nhắn

Bộ nhớ ngoài: Các phần mềm, tiện ích, hình ảnh được lưu trữ

1. **Quy trình điều tra**

* Xác định loại hình
* Thu thập và bảo toàn thông tin
* Ghi lại thông tin về thiết bị
* Ghi lại những bằng chứng
* Phân tích bằng chứng
* Báo cáo

1. **Thu thập thông tin trên thiết bị di động**

* Thông tin về mạng di động
* Các tệp tin hệ thống được tạo ra bởi SIM
* Các thông số kỹ thuật, bằng chứng số
* Các bằng chứng được lưu trữ trên phần cứng
* Tệp tin hệ điều hành

NGƯỜI GIỚI THIỆU

1. Barbara, JJ (2010, ngày 17 tháng 10). Tìm hiểu thế giới của điện thoại di động: Phần 1 . Được truy cập ngày 13 tháng 11 năm 2011, từ Forensicmag.com: [http://www.forensicmag.com/article/undilities-world-cellular-telephones-part-1?page=0,1](http://www.forensicmag.com/article/understanding-world-cellular-telephones-part-1?page=0,1) .

2. Barbara, JJ (nd). Pháp y SIM: Phần 1 . Truy cập ngày 19 tháng 9 năm 2011, từ: <http://www.forensicmag.com/article/sim-forensics-part-1>.

3. Barbara, JJ (nd). Sim Forensics: Phần 2 . Truy cập ngày 19 tháng 9 năm 2011, từ: <http://www.forensicmag.com/article/sim-forensics-part-2>.

4. Barbara, JJ (nd). Pháp y SIM: Phần 3 . Truy cập ngày 18 tháng 9 năm 2011, từ: <http://www.forensicmag.com/article/sim-forensics-part-3>.

5. Barbara, JJ (nd). Tìm hiểu thế giới của điện thoại di động: Phần 1 . Được truy cập ngày 21 tháng 9 năm 2011, từ: [http://www.forensicmag.com/article/undilities-world-cellular-telephones-part-1](http://www.forensicmag.com/article/understanding-world-cellular-telephones-part-1) .

6. Barbara, JJ (nd). Tìm hiểu thế giới của điện thoại di động: Phần 2 . Truy cập ngày 21 tháng 9 năm 2011, từ: [http://www.forensicmag.com/article/undilities-world-cellular-telephones-part-2](http://www.forensicmag.com/article/understanding-world-cellular-telephones-part-2) .

7. Barbara, JJ (nd). Tìm hiểu thế giới của điện thoại di động: Phần 3 . Truy cập ngày 21 tháng 9 năm 2011, từ: [http://www.forensicmag.com/article/undilities-world-cellular-telephones-part-3](http://www.forensicmag.com/article/understanding-world-cellular-telephones-part-3) .

8. BitPim. (nd). BitPim . Truy cập ngày 22 tháng 9 năm 2011, từ: <http://www.bitpim.org/>.

9. Brian, M., & Harris, T. (nd). Cách hoạt động của bộ thu GPS . Truy cập ngày 14 tháng 9 năm 2011, từ: <http://electronics.howstuffworks.com/gadgets/travel/gps.htm>.

10. Casey E. Sổ tay Điều tra và Pháp y Kỹ thuật số Burlington, MA: Academic Press; Năm 2009.

11. Casey E. Bằng chứng Kỹ thuật số và Tội phạm Máy tính: Khoa học Pháp y, Máy tính và Internet Waltham, MA: Báo chí Học thuật; 2011.

12. Hartenstein, M., & Sheridan, M. (2010, ngày 21 tháng 12). Miss Vegas Showgirl Debbie Flores-Narvaez mang thai, bị đánh đập bởi người yêu cũ, Theo Police . Truy cập ngày 25 tháng 9 năm 2011, từ: <http://articles.nydailynews.com/2010-12-21/news/27085062_1_license-plates-cell-phone-police>.

13. Hoog, A. (2010, ngày 30 tháng 4). Giới thiệu về pháp y Android . Truy cập tháng 9 năm 2011, từ: <http://www.dfinews.com/article/introduction-android-forensics?page=0,0>.

14. Hoog A. Android pháp y: Điều tra, Phân tích và Bảo mật Di động cho Google Android Waltham, MA: Elsevier; 2011.

15. Jansen W, Ayers R. Hướng dẫn về pháp y qua điện thoại di động Gaithersburg, TN: Viện Tiêu chuẩn và Công nghệ Quốc gia; Năm 2007.

16. Kessler, GC (2011, tháng 6). Phân tích Điện thoại Di động: Công nghệ, Công cụ và Quy trình . Truy cập ngày 12 tháng 9 năm 2011, từ: <http://www.garykessler.net/presentations/CellPhone_201106_ICAC-sanitized.pdf>.

17. LeMere, B. (nd). Tăng cường điều tra với Bằng chứng GPS . Truy cập ngày 15 tháng 9 năm 2011, từ: <http://www.forensicmag.com/article/enhancing-investigations-gps-evidence>.

18. LeMere, B. (2011, ngày 25 tháng 4). Tăng cường điều tra với Bằng chứng GPS . Truy cập ngày 15 tháng 9 năm 2011, từ: <http://www.forensicmag.com/article/enhancing-investigations-gps-evidence>.

19. Mobile-phone-directory.org. (nd). Nhập Văn bản Dự đoán . Truy cập ngày 17 tháng 9 năm 2011, từ: [http://www.mobile-phone-directory.org/Glossary/P/Predhesia\_Text\_Input.html](http://www.mobile-phone-directory.org/Glossary/P/Predictive_Text_Input.html) .

20. Morrissey S. Phân tích pháp y iOS: cho iPhone, iPad và iPod Touch New York: Apress; Năm 2010.

21. Mở Liên minh Thiết bị cầm tay. (2007, tháng 11). Câu hỏi thường gặp . Truy cập ngày 19 tháng 9 năm 2011, từ: <http://www.openhandsetalliance.com/oha_faq.html>.

22. Shachtman, N. (2006, ngày 3 tháng 5). Chống lại tội phạm với manh mối của điện thoại di động . Truy cập ngày 19 tháng 9 năm 2011, từ: <http://www.nytimes.com/2006/05/03/technology/techspecial3/03cops.html>.

[1](#1) Các nhà nghiên cứu đã phát hiện ra rằng iPhone hoặc iPad 3G - bất kỳ thứ gì có quyền truy cập dữ liệu 3G - đang ghi dữ liệu vị trí vào một tệp có tên là merge.db với tọa độ kinh độ và vĩ độ cũng như dấu thời gian.

# Chương 11:Nhìn về phía trước

Những thách thức và mối quan tâm theo xu hướng ngay lúc giảng dạy (hiện nay malware, cloud)

### Thông tin trong Chương này:

Tiêu chuẩn và Kiểm soát



Pháp y đám mây



Ổ cứng thể rắn



Tốc độ thay đổi



Sắp tới, có một số thách thức đáng kể mà cộng đồng pháp y kỹ thuật số phải đối mặt. Hai trong số những thách thức này, điện toán đám mây và ổ cứng thể rắn (SSD), là “những người thay đổi cuộc chơi”. Bằng chứng kỹ thuật số trong những môi trường đó rất có thể không thể khôi phục được vì nhiều lý do kỹ thuật hoặc pháp lý.

Ổ cứng thể rắn (SSD), Điện toán đám mây, Nhà cung cấp dịch vụ đám mây (CSP), Đám mây công cộng, Thu gom rác, Nhóm làm việc khoa học về Bằng chứng kỹ thuật số (SWGDE), Ảo hóa, Tiêu chuẩn & Kiểm soát, Cấp độ mòn

## Giới thiệu

Pháp y kỹ thuật số vẫn còn trong giai đoạn sơ khai. Nó rất là một công việc đang được tiến hành do tồn tại tương đối ngắn cũng như tốc độ thay đổi công nghệ nhanh chóng. Tình trạng công việc đang tiến hành này có thể sẽ tiếp diễn trong một thời gian khá dài. Tình trạng này dẫn đến nhiều thách thức và tranh cãi mà cộng đồng pháp lý và pháp y phải đấu tranh. Những thách thức là rất nhiều. Một thách thức như vậy là vật lộn với công nghệ “thay đổi cuộc chơi” mới nổi và có tiềm năng. Một vấn đề khác là đạt được sự đồng thuận với cộng đồng khoa học pháp y nói chung, đặc biệt là khi nói đến các phương pháp hay nhất đã được thiết lập.

Pháp y kỹ thuật số đang gây ra một vụ va chạm lớn nếu bạn muốn, giữa hai lực lượng dường như không thể khuất phục: hệ thống pháp luật và cộng đồng pháp y hoạt động với tốc độ tương đối chậm và có chủ ý so với tốc độ chóng mặt của công nghệ. Không được xây dựng cho tốc độ. Có những lý do chính đáng cho điều đó. Tiền đặt cọc là quá cao để thừa nhận bằng chứng pháp y chưa được chứng minh là đáng tin cậy. Độ tin cậy đã được chứng minh này cần có thời gian và không thể đạt được trong đêm.

Hai công nghệ, điện toán đám mây và ổ cứng thể rắn, đưa ra những thách thức “thay đổi cuộc chơi”. Như hiện tại, bằng chứng kỹ thuật số trong một trong hai môi trường này rất có thể không thể khôi phục được vì lý do kỹ thuật hoặc pháp lý (hoặc cả hai). Những công nghệ này đang được sử dụng ngày nay và đại diện cho một vấn đề mà không có câu trả lời dễ dàng. Vẫn chưa thấy tất cả những thách thức này sẽ được đáp ứng như thế nào.

## Tiêu chuẩn và Kiểm soát

Tiêu chuẩn và kiểm soát là một phần cơ bản của phân tích khoa học, bao gồm cả khoa học pháp y. Tiêu chuẩn là “một mẫu đã được chuẩn bị sẵn có các đặc tính đã biết được sử dụng để kiểm soát trong quá trình phân tích pháp y” (Barbara, 2007).

một thử nghiệm được thực hiện song song với các mẫu thử nghiệm được thiết kế để chứng minh rằng một quy trình đang hoạt động chính xác và kết quả là hợp lệ” (Barbara, 2007). Về bản chất, một đối chứng chỉ đơn giản là một mẫu cung cấp một kết quả đã biết.

Điều đó có thể đúng đối với huyết thanh học, hóa học, độc chất học, và những thứ tương tự, nhưng sự liên quan của nó với pháp y kỹ thuật số là một vấn đề tranh chấp. Các nhà khoa học pháp y truyền thống hơn đang có quan điểm rằng các tiêu chuẩn và kiểm soát là cần thiết cho tất cả các ngành pháp y, bao gồm pháp y kỹ thuật số và đa phương tiện. Một trong những cơ quan pháp y kỹ thuật số lớn, Nhóm Công tác Khoa học về Bằng chứng Kỹ thuật số (SWGDE), đang có quan điểm hoàn toàn ngược lại. Cuộc tranh cãi bắt đầu với một bài báo trên [trang Forensicmag.com](http://Forensicmag.com) vào năm 2007 của John Barbara. Trong bài báo, Barbara đã nêu ra vấn đề về các tiêu chuẩn và kiểm soát trong pháp y kỹ thuật số. Ông là Giám sát viên Phân tích Phòng thí nghiệm điều tra tội phạm của Cục Thực thi Pháp luật Florida (FDLE). Anh ấy cũng là thanh tra ASCLD / LAB và đã làm việc từ năm 1993. Trong bài báo, anh ấy đã trình bày trường hợp của mình với lý do bắt buộc sử dụng các tiêu chuẩn và kiểm soát trong mọi kỷ luật pháp y khác. Ông cho rằng việc sử dụng các tiêu chuẩn và kiểm soát là cần thiết để chứng minh rằng các thử nghiệm đã được thực hiện một cách khoa học và các biện pháp đảm bảo chất lượng đã được tuân thủ.

Cuối cùng, việc tuân thủ chặt chẽ các thực hành khoa học đã được thiết lập này đảm bảo rằng bất kỳ kết quả nào thu được là chính xác, đáng tin cậy và có thể lặp lại. Ông lập luận thêm rằng nếu không sử dụng các tiêu chuẩn và kiểm soát, sẽ “cực kỳ khó hoặc không thể đánh giá một cách khoa học tính hợp lệ của các kết quả thu được từ việc phân tích bằng chứng vật lý” (Barbara, 2007). Cuối cùng, ông đã nâng cao các tiêu chuẩn tuyển sinh theo yêu cầu của trường hợp Daubert .

Tại Daubert , tòa án nói rằng khi xem xét tính khả thi của bất kỳ bằng chứng khoa học nào, cần tập trung vào các nguyên tắc và phương pháp luận chứ không phải các kết luận mà chúng tạo ra.

Nhóm Công tác Khoa học về Bằng chứng Kỹ thuật số (SWGDE ) không đồng ý. Quan điểm của họ là các tiêu chuẩn đang được sử dụng trong pháp y kỹ thuật số, nhưng các biện pháp kiểm soát “không được áp dụng trong chuyên ngành pháp y máy tính” (Nhóm công tác khoa học về bằng chứng kỹ thuật số, 2008).

Vị trí của SWGDE tập trung vào kết quả dương tính giả. Họ nói rằng dương tính giả không tồn tại trong pháp y máy tính. Các công cụ và quy trình có thể bỏ sót bằng chứng, nhưng chúng sẽ không bao giờ tìm thấy bằng chứng không tồn tại. SWGDE cho biết, mục tiêu chính của bất kỳ cuộc điều tra pháp y kỹ thuật số nào là tìm dữ liệu liên quan đến hoạt động tội phạm đã tồn tại. Do đó, không có giá trị thực nào đối với phân tích hoặc kết quả.

Họ kết luận bằng cách nói rằng “xác thực, tính toàn vẹn dữ liệu (thông qua băm) và xác minh hiệu suất” là một giải pháp phù hợp hơn so với việc sử dụng các tiêu chuẩn và kiểm soát truyền thống (Nhóm làm việc khoa học về Bằng chứng kỹ thuật số, 2008).

SWGDE đồng ý rằng “Công nghệ mới, thường là độc quyền về bản chất, xuất hiện hàng ngày. Khi các công nghệ mới này xuất hiện, cần có các giải pháp và kỹ thuật mới để hiểu và điều tra bằng chứng. Sự hiểu biết toàn diện và các kỹ thuật đã được xác nhận cần phải chuyển nhanh chóng từ cộng đồng nghiên cứu sang cộng đồng thẩm định viên ”(Nhóm công tác khoa học về bằng chứng kỹ thuật số, 2008).

## Cloud Forensics (Tìm kiếm / Xác định Bằng chứng Tiềm năng được Lưu trữ Trong Đám mây)

Điện toán đám mây là một chủ đề nóng trong công nghệ thông tin. Nhiều lợi ích mà nó mang lại là không thể phủ nhận và không mất đi đối với các tổ chức trên toàn cầu. Do đó, nó đang được áp dụng rộng rãi. Tuy nhiên, đám mây là một con dao hai lưỡi, và nó là một con dao sắc bén. Với nhiều lợi ích của nó, những thách thức lớn từ cả góc độ pháp lý và pháp lý.

### 3.1 Điện toán đám mây là gì?

Có rất nhiều định nghĩa về điện toán đám mây để bạn lựa chọn. TechTarget mô tả điện toán đám mây là “một thuật ngữ chung cho bất kỳ thứ gì liên quan đến việc cung cấp các dịch vụ được lưu trữ trên Internet” ( [TechTarget, 2007](#6__TechTarget___2007__December) ). Các dịch vụ được lưu trữ này thường thuộc một số danh mục khác nhau bao gồm:

Cơ sở hạ tầng như một dịch vụ (IaaS).



Phần mềm như một dịch vụ (SaaS).



Nền tảng như một dịch vụ (Paas).



Thuật ngữ “điện toán đám mây” có nguồn gốc từ biểu tượng “đám mây” thường được sử dụng trong các sơ đồ mạng để biểu thị Internet.

Viện Tiêu chuẩn và Công nghệ Quốc gia (NIST) đưa ra một định nghĩa phức tạp hơn. Họ định nghĩa đám mây theo cách này: “Điện toán đám mây là mô hình cho phép truy cập mạng phổ biến, thuận tiện, theo yêu cầu vào nhóm tài nguyên máy tính có thể định cấu hình được chia sẻ (ví dụ: mạng, máy chủ, lưu trữ, ứng dụng và dịch vụ) có thể nhanh chóng cung cấp và phát hành với nỗ lực quản lý tối thiểu hoặc tương tác với nhà cung cấp dịch vụ ”( [Mell & Grance, 2011](#2__Mell__P_____Grance__T___2011) ).

Không phải tất cả các đám mây đều giống nhau. Có đám mây riêng và đám mây công cộng. Các đám mây công cộng bán các dịch vụ trên thị trường mở. Những gã khổng lồ về công nghệ như Microsoft (Azure), Amazon (Amazon Web Services), Rackspace và Google chỉ là một số người chơi lớn trên thị trường đám mây. Các nhà cung cấp dịch vụ đám mây hoặc CSP này có thể có các trung tâm dữ liệu nằm rải rác trên khắp thế giới.

Mô hình đám mây chủ yếu dựa vào ảo hóa và dự phòng. TechTarget định nghĩa ảo hóa theo cách này: “ Ảo hóa là việc tạo ra phiên bản ảo (thay vì thực tế) của một thứ gì đó, chẳng hạn như hệ điều hành, máy chủ, thiết bị lưu trữ hoặc tài nguyên mạng” (TechTarget, 2000).

Tài nguyên bổ sung

Đám mây công cộng

Để có cái nhìn sâu hơn về cách các dịch vụ đám mây công cộng được bán và quản lý, hãy truy cập một số nhà cung cấp này.

<http://www.microsoft.com/en-us/cloud/default.aspx?fbid=XBzeu9E4wgy>

<http://aws.amazon.com/>

<http://www.rackspace.com/cloud/>

### 3.2 Lợi ích của đám mây

Nhận thấy nhiều lợi ích của đám mây, các công ty và các tổ chức khác đang đổ xô vào đó hàng loạt. Họ đang tìm kiếm cả sự tiện lợi và tiết kiệm chi phí mà mô hình máy tính này mang lại. Khả năng về cơ bản là "quay số" tài nguyên máy tính khi cần thiết là điều khó có thể không thích. Với đám mây, cơ sở hạ tầng của tổ chức có thể mở rộng và hợp đồng khi cần thiết. Từ góc độ chi phí, cách làm này có thể tiết kiệm một khoản tiền đáng kể. Các công ty có thể tiết kiệm phần lớn vốn đầu tư ban đầu cho phần cứng và phần mềm mạng.

Việc sao chép dữ liệu hoặc dịch vụ trong nhiều trung tâm dữ liệu sẽ cung cấp khả năng dự phòng. Tính chất dự phòng của đám mây đảm bảo rằng các tệp và / hoặc ứng dụng của người dùng được an toàn và luôn sẵn sàng bất cứ khi nào họ cần. Nếu một trung tâm hoặc kết nối của nó bị hỏng, trung tâm thứ hai sẽ có thể phản hồi.

### 3.3 Các quan ngại về pháp lý và pháp lý trên đám mây

Đám mây có thể là giấc mơ trở thành hiện thực đối với những người kinh doanh và công nghệ thông tin, nhưng nó lại là cơn ác mộng đối với những người xử lý bằng chứng kỹ thuật số. Các thách thức chính gồm hai mặt, một là kỹ thuật và còn lại là pháp lý. Về mặt kỹ thuật, chắc chắn đám mây không phải là một môi trường thân thiện với môi trường, đặc biệt là khi so sánh với giới hạn tương đối ấm cúng của các ổ đĩa từ tính. Kéo dữ liệu đã xóa khỏi các ổ đĩa truyền thống từ lâu đã trở thành một yếu tố chính của pháp y kỹ thuật số. Đám mây có thể sẽ chấm dứt điều đó. Các tệp đã xóa trên ổ đĩa từ vẫn còn trên đĩa cho đến khi chúng bị ghi đè. Trong đám mây, khi một tệp bị xóa, ánh xạ sẽ bị xóa ngay lập tức, thường là trong vòng vài giây. Điều này có nghĩa là không có quyền truy cập từ xa vào dữ liệu đã xóa. Như trường hợp của ổ đĩa từ tính, dung lượng đó hiện đã có sẵn và có thể sẽ bị ghi đè trên đám mây ( [Ruan, Carthy, Kechadi, & Crosbie, 2011](#5__Ruan_K__Carthy_J__Kechadi_T) ).

Sự thiếu hụt đáng báo động của các công cụ và quy trình pháp y được thiết lập để thu thập và phân tích bằng chứng kỹ thuật số trên đám mây. Các công cụ và phương pháp luận hiện tại phần lớn không hiệu quả trong môi trường này. Nhiều nghiên cứu cần được thực hiện.

Báo động!

Tính bền trên đám mây — Dropbox

Có nhiều thách thức như chức năng đám mây thể hiện, trong một số trường hợp nhất định, nó có thể hoạt động có lợi cho chúng ta. Ví dụ: Dropbox lưu tất cả các tệp đã xóa (theo mặc định) trong ba mươi ngày.

Dịch vụ “Pack-Rat” của Dropbox có thể giữ dữ liệu vô thời hạn (với tính năng bổ sung Pack-Rat). Được cho là, bạn sẽ cần trát đòi hầu tòa hoặc trát khám xét để có được nó, nhưng thực tế là nó có thể có sẵn là điều tuyệt vời khi biết (Dropbox, 2011).

Về mặt pháp lý, việc giao dịch với nhiều khu vực pháp lý có thể làm nản lòng đáng kể những nỗ lực truy cập dữ liệu liên quan ngay từ đầu. Như chúng ta đã thấy, các CSP có thể đặt trung tâm dữ liệu của họ ở hầu hết mọi nơi trên thế giới. Các yêu cầu và thủ tục pháp lý có thể khác nhau, và khác nhau đáng kể giữa các quốc gia, và từ khu vực tài phán sang khu vực tài phán. Vấn đề này sẽ tăng lên theo cấp số nhân nếu dữ liệu đã vượt qua ranh giới quốc tế.

Quy định có thể hỗ trợ giảm thiểu vấn đề này. Nó có thể hữu ích bằng cách yêu cầu các CSP hoạt động theo cách tạo điều kiện thuận lợi cho việc bảo quản và phục hồi dữ liệu có thể liên quan. Thỏa thuận mức dịch vụ hoặc SLA cũng có thể tạo ra sự khác biệt. SLA là một thỏa thuận bằng văn bản giữa khách hàng và nhà cung cấp. SLA trình bày rất chi tiết những hỗ trợ và dịch vụ mà khách hàng sẽ nhận được từ nhà cung cấp. Là một phần của thỏa thuận đó, khách hàng có thể yêu cầu một số đảm bảo nhất định về bảo mật thông tin và cách bằng chứng kỹ thuật số sẽ được lưu giữ và thu thập nếu điều đó trở nên cần thiết. Ở góc độ khách hàng, đây là một chi tiết quan trọng không thể bỏ qua. Điều này đặc biệt đúng trong các tổ chức có khả năng xảy ra kiện tụng. Có sự sắp xếp này có thể rất có lợi cho người giám định pháp y, đặc biệt là trái ngược với việc bắt đầu lại từ đầu mà không có giao thức, thủ tục hoặc mối quan hệ nào tại chỗ.

## Ổ cứng thể rắn (SSD)

Ổ đĩa từ đã trở thành trụ cột chính trong máy tính cá nhân trong nhiều năm. Về mặt pháp lý, họ cung cấp cho người điều tra khả năng khôi phục lượng dữ liệu đáng kể do người dùng xóa. Những ngày đó, nó xuất hiện, rất có thể sắp kết thúc. Các ổ đĩa từ truyền thống này đang được thay thế ngày càng nhiều. Chào mừng đến với kỷ nguyên của ổ cứng thể rắn (SSD).

### 4.1 Cách các ổ đĩa thể rắn lưu trữ dữ liệu

Truyền động từ tính truyền thống có nhiều bộ phận chuyển động bao gồm các đĩa và cánh tay truyền động (di chuyển đầu đọc / ghi). Như tên của nó, ổ đĩa trạng thái rắn thì không. Ổ SSD hơi giống với RAM và ổ USB, lưu trữ dữ liệu trong các bóng bán dẫn cực nhỏ. Không giống như RAM, SSD không linh hoạt và có thể lưu trữ dữ liệu ngay cả khi không có điện. Để giữ điện tích trong thời gian dài mà không cần nguồn điện, các bóng bán dẫn SSD sử dụng một cổng bổ sung (được gọi là cổng nổi), được sử dụng để chứa điện tích ( [Bell & Boddington, 2010](#1__Bell__Graeme_B___Boddington) ).

Nếu bạn nhớ lại từ [Chương 2](#Top_of_CHP002_html) , các ổ đĩa từ tính chia không gian lưu trữ thành các đơn vị nhỏ hơn. Các đơn vị này bao gồm các ngành, các cụm và các bản nhạc. SSD cũng tách không gian lưu trữ thành các đơn vị nhỏ hơn. Các đơn vị cơ sở được gọi là khối và thường có kích thước 512 KB. Các khối sau đó được chia thành các đơn vị thậm chí còn nhỏ hơn được gọi là các trang. Mỗi trang có kích thước thường là 4 KB.

Mòn là một mối quan tâm với SSD. Mỗi khối chỉ có thể chịu được một số lần ghi nhất định. Một số ước tính đưa con số đó vào khoảng từ một nghìn đến mười nghìn lần. Với hạn chế này, bạn sẽ muốn ổ đĩa tránh ghi nhiều lần vào cùng một khối. Việc ghi vào cùng một không gian nhiều lần sẽ khiến nó bị mòn nhanh hơn những chỗ khác. Các nhà sản xuất đã giải quyết vấn đề này bằng cách thiết lập một quy trình cân bằng độ mòn do SSD thực hiện.

Nâng cao hơn

Lớp dịch tệp

Trên ổ đĩa trạng thái rắn, máy tính nghĩ rằng dữ liệu được lưu trữ ở một vị trí, trong khi trên thực tế, chúng được đặt ở một vị trí khác. Ổ cứng SSD sử dụng Lớp dịch tệp để đảm bảo rằng máy tính không ghi nhiều lần vào cùng một khối. Nếu SSD phát hiện ra điều này đang xảy ra, nó sẽ “dịch” các ghi mới đến một vị trí ít được sử dụng hơn ( [Bell & Boddington, 2010](#1__Bell__Graeme_B___Boddington) ).

Ổ đĩa từ tính có khả năng ghi đè dữ liệu ngay lập tức vào bất kỳ khu vực nào được dán nhãn là chưa phân bổ. SSD thì không. Mỗi bóng bán dẫn phải được "đặt lại" (xóa) trước khi nó có thể được sử dụng lại. Quá trình thiết lập lại này làm chậm ổ đĩa. Để tăng tốc độ, các nhà sản xuất SSD đã định cấu hình bộ điều khiển của ổ đĩa để tự động thiết lập lại các phần không sử dụng của ổ đĩa. Quá trình này được gọi là Thu gom rác .

### 4.2 Vấn đề: Bỏ Thùng rác

Ổ đĩa trạng thái rắn có một tâm trí riêng của chúng. Nhiều ổ đĩa tự khởi động quy trình Thu gom rác hoàn toàn mà không cần bất kỳ sự nhắc nhở nào của máy tính.

Đây là cả một vấn đề và rắc rối từ quan điểm của nhà phân tích pháp y. Đầu tiên, việc xác minh tính toàn vẹn của bằng chứng trở nên vô cùng khó khăn và gây nguy hiểm cho việc chấp nhận của bằng chứng trước tòa. Thứ hai, có việc tự động phá hủy dữ liệu có thể có liên quan trên ổ đĩa. Nếu quy trình Thu gom rác được chạy trong hoặc sau quá trình thu thập, việc xác thực sẽ khó khăn hơn theo cấp số nhân vì các giá trị băm sẽ không khớp.

Ngày nay, chúng ta thường sử dụng các thuật toán băm mật mã, chẳng hạn như MD5 hoặc SHA1, để lấy “dấu vân tay kỹ thuật số” hoặc “DNA kỹ thuật số” của ổ cứng. Sau đó, chúng ta có thể lấy lại "dấu vân tay" của bản sao bất kỳ lúc nào và so sánh nó với "dấu vân tay" của bản gốc. Chúng phải khớp chính xác, xác minh tính toàn vẹn của bằng chứng ( [Bell & Boddington, 2010](#1__Bell__Graeme_B___Boddington) ).

## Tốc độ thay đổi

Bạn có thể nhận thấy rằng tốc độ thay đổi công nghệ là một chủ đề lặp đi lặp lại xuyên suốt cuốn sách này. Tác động của nó thực sự đáng kể và được cảm nhận trên cả pháp y kỹ thuật số và cộng đồng pháp lý. Nó cũng tác động đến các tổ chức dựa vào kết quả như cơ quan thực thi pháp luật và các công ty tư nhân. Lấy ví dụ về các trường hợp tồn đọng. Trong hầu hết, nếu không phải tất cả các phòng thí nghiệm, có một tồn đọng đáng kể các trường hợp bao gồm cả những trường hợp liên quan đến bằng chứng kỹ thuật số. Thay đổi góp phần vào việc tồn đọng này bằng cách làm chậm quá trình điều tra. Sử dụng một ứng dụng cập nhật chẳng hạn như một ứng dụng trò chuyện. Có thể có sự khác biệt lớn về vị trí và cách phần mềm lưu trữ mà người điều tra hiện vật cần xác định vị trí và phân tích. Các phần mềm có thể đã được ghi vào sổ đăng ký trong phiên bản trước hiện được lưu giữ độc quyền trong RAM và biến mất khi máy tắt nguồn.

Các điều tra viên được trình bày với tình huống này sẽ phải cố gắng tìm ra một giải pháp đã được chứng minh từ những người khác trong cộng đồng pháp y kỹ thuật số. Nếu không đạt được điều đó, điều tra viên có thể phải tự mình tiến hành nghiên cứu và xác nhận kết quả. Điều này cần có thời gian. Bảng tin (chẳng hạn như bảng dành cho thành viên HTCIA) và danh sách e-mail có giá trị bằng vàng trong những trường hợp này. Họ cung cấp một kênh sẵn sàng để giao tiếp và giải quyết vấn đề.

Tài nguyên bổ sung

Twitter

Twitter có thể là một nguồn tài nguyên tuyệt vời cho các chuyên gia pháp y kỹ thuật số. Nó có thể cảnh báo bạn về các kỹ thuật mới, bài báo nghiên cứu, quyết định của tòa án, tin tức, v.v. Có rất nhiều cá nhân và công ty chia sẻ rất nhiều tin tức và thông tin liên quan trực tiếp đến pháp y kỹ thuật số. Ngày nay, chúng ta có nhiều thông tin, một số tốt và một số xấu. Theo dõi các thực thể nổi tiếng, được thành lập trên Twitter có thể giúp giảm “tiếng ồn” và giúp bạn cập nhật thông tin. Đây là một công cụ có thể giúp bạn đối phó với tốc độ thay đổi. Đây chỉ là một mẫu của những người và công ty đáng để theo dõi.

|  |
| --- |
| Pháp y kỹ thuật số |
| Nhà cung cấp / Tổ chức | Cá nhân |
| @AccessDataGroup | @robtlee |
| @EnCase | @jtrajewski |
| @sansforensics | @girlunallocated |
| @DFMag | @ keydet89 |
| @HTCIA | @codeslack |
| @MFITraining | @ 4n6woman |
| @cellebrite Hoa Kỳ | @AppleExaminer |
| @syngress | @chadtilbury |
|  | @hal\_pomeranz |
|  | @ 4cast |
|  | @ CyberCrime101 |
| Khám phá điện tử |
| Nhà cung cấp / Tổ chức | Cá nhân |
| @DiscoverTERIS | @sharonnelsonesq |
| @EDDUpdate | @RalphLosey |
| @e\_discoverynews  @KrollOntrack | @EUdiscovery  @InfoGovernance |
| @Clearwell | @ComplexD |
| @PosseList |  |

## 

## Bản tóm tắt

Pháp y kỹ thuật số phải đối mặt với nhiều thử nghiệm trên con đường phía trước. Tốc độ chóng mặt của công nghệ, các công nghệ thay đổi cuộc chơi mới như điện toán đám mây và ổ cứng thể rắn, và những bất đồng với các bộ môn pháp y đã được thành lập, chỉ là một vài cái tên. Tốc độ phát triển không ngừng của công nghệ ảnh hưởng không nhỏ đến cộng đồng DF khi họ chiến đấu để giữ vững tốc độ. Tốc độ thay đổi cũng ảnh hưởng đến hệ thống pháp luật. Bản thân hệ thống nói chung không được “xây dựng cho tốc độ” và chắc chắn không phải cho tốc độ của công nghệ. Kết quả cuối cùng là trong một số tình huống nhất định, các công cụ và giao thức đã được thử nghiệm trước đó sẽ không hiệu quả. Việc nghiên cứu, phát triển và thử nghiệm cần thiết để giải quyết vấn đề cần có thời gian.

Cung cấp các dịch vụ qua Web, bánh mì và bơ của điện toán đám mây, thể hiện một sự thay đổi lớn so với mô hình điện toán mà thế giới đã quen thuộc. Các ứng dụng, phần cứng, nền tảng và cơ sở hạ tầng từ xa có rất nhiều lợi ích; chi phí giảm và độ co giãn chỉ là hai. Ở hậu trường, đám mây chủ yếu dựa vào ảo hóa và dự phòng. Các trung tâm dữ liệu khổng lồ được sử dụng để cung cấp các dịch vụ đám mây công cộng có khả năng được phân tán rộng rãi, cư trú ở nhiều bang hoặc thậm chí các quốc gia khác nhau. Việc đáp ứng các yêu cầu pháp lý để có quyền truy cập vào dữ liệu này có thể mất rất nhiều thời gian. Hoàn toàn có khả năng vào thời điểm gánh nặng pháp lý được đáp ứng, bằng chứng được đề cập có thể không còn tồn tại.

Ổ cứng thể rắn là một công nghệ thay đổi cuộc chơi khác cần được giải quyết. Những thiết bị này có thể phục vụ cùng một chức năng như các ổ đĩa từ quen thuộc của chúng ta, nhưng chúng chắc chắn không hoạt động giống như chúng. Phương pháp lưu trữ mà họ sử dụng, các bóng bán dẫn tích điện nhỏ, phải được "đặt lại" trước khi được ghi vào. Quá trình này làm chậm ổ đĩa, ảnh hưởng đến hiệu suất. Để giảm thiểu sự chậm chạp, các nhà sản xuất ổ đĩa đã xây dựng một quy trình được gọi là Thu gom rác. Quá trình này bắt đầu quá trình đặt lại này chỉ trong vài phút. Thủ tục này phá hủy dữ liệu trên ổ đĩa theo cách mà các công cụ và kỹ thuật hiện tại không thể khôi phục được.

Bằng chứng kỹ thuật số và các quy trình pháp lý liên quan của nó đôi khi hoàn toàn khác với các quy tắc đã được thiết lập khác. Các thực hành pháp y Bedrock như việc sử dụng các tiêu chuẩn và kiểm soát được cho là vô nghĩa đối với một số người trong cộng đồng pháp y kỹ thuật số. Những người phản đối nói rằng không giống như huyết thanh học và chất độc học, đơn giản là không thể nhận được kết quả dương tính giả từ một cuộc điều tra pháp y kỹ thuật số. Họ nói, công cụ này có thể bỏ sót một số bằng chứng, nhưng nó sẽ không bao giờ tìm thấy bằng chứng chưa có ở đó.

Đây chỉ là một vài trong số những thách thức đáng kể mà các học viên tuyến đầu phải đối mặt. Còn nhiều việc phải làm nếu những thách thức này sẽ gặp phải.

## Tổng kết và kiến thức thêm chương 11

Điều tra mã độc

1. **Malware là gì? Xác định được các hướng tiếp cận để malware xâm nhập vào hệ thống?**

Malware là một phần mềm, ứng dụng có khả năng gây ảnh hưởng đến vận hành của hệ thống, thiết bị hoặc cho phép tin tặc kiểm soát một phần hoặc toàn bộ hệ thống.

Thông thường, các malware được lây lan qua:

* Tin nhắn
* E-mail
* Thiết bị lưu trữ ngoài
* Phần mềm lậu
* Phần mềm bị crack
* Các tập tin được tải xuống.

1. **Các phương pháp tin tặc dùng để khiến malware xâm nhập vào hệ thống, thiết bị thông qua Web**

Social Engineerd clickjacking – Khiến người dùng ấn vào link, trang web

Blackhat Search Engine Optimization (SEO)– Hiển thị các trang web có chứa malware trên các công cụ tìm kiếm

Malvertising – Thông qua các quảng cáo, tuy nhiên thông thường malware trong phương pháp này là adware để theo dõi khách hàng.

Spear Phishing – Giả danh web các tổ chức uy tín

Drive-by Downloads – Yêu cầu người dùng phải tải thêm các phần mềm khác ngoài phân mềm họ muốn cài đặt

1. **Cách thức điều tra malware**

Thông thường, các malware được tin tặc sử dụng là virus, worm, trojan, spyware, và ransomware với mục tiêu xâm nhập, kiểm soát hoặc gây ảnh hưởng đến 1 hệ thống.

Điều tra malware là chuỗi hành động nhằm xác định, ghi lại các lệnh, hành động bất thường nhằm tìm kiếm được bằng chứng cũng như phương pháp xâm nhập và mục tiêu, ảnh hưởng của malware đến hệ thống.

1. **Mục tiêu điều tra malware**
2. Xác định các chuỗi sự kiện, hành động đã xảy ra để biết được các nguồn xâm nhập cũng như điểm yếu của hệ thống
3. Xác định mục tiêu của malware cũng như khả năng lây lan, và ảnh hưởng đến vận hành hệ thống
4. Xác định được ai đã cho phép, tải malware vào hệ thống
5. Xác định được danh tính của nguồn tấn công như địa chỉ IP, phần mềm nhằm cấu hình lại cho hệ thống IDS, IPS, firewall
6. **Quy trình khi điều tra malware**

Đảm bảo phòng điều tra, môi trường điều tra có thể

1. Tách rời hoặc kiểm soát malware đang trong hệ thống thực trước khi bắt đầu phân tích
2. Môi trường, phòng điều tra có khả năng chụp, quay lại hình ảnh
3. Có khả năng tích hợp với các hệ thống khác
4. Có khả năng sao lưu và khôi phục lại hệ thống trong trường hợp malware bị khởi động

Các thông tin cần ghi lại trước khi điều tra malware:

1. Nguồn dẫn đến tệp tin
2. Thời gian
3. Tệp tin, dữ liệu có trong thiết bị, hệ thống đó
4. Ai đã báo cáo về tệp tin
5. Công cụ sử dụng để điều tra
6. **Phân tích malware theo hướng Static (thông số được ghi lại) và Dynamic (thông số sống)**

Phân tích Static – Phân tích Static là phân tích các mã nguồn, mã lệnh, cấu trúc của phần mềm malware mà không cần khởi động malware; nhằm hiểu thêm về mục tiêu và tính chất của malware

Phân tích Dynamic – Phân tích Dynamic là phân tích các hành động, sự kiện liên quan xảy ra bằng cách khởi động malware trên môi trường máy ảo hoặc lab.

1. **Các khó khăn liên quan đến phân tích malware**
2. Cần đảm bảo làm theo các quy trình một cách chặt chẽ
3. Phân biệt đâu là phần mềm malware và tính chất của phần mềm này
4. Cần phải phân tích lượng lớn dữ liệu
5. Malware luôn luôn phát triển theo thời gian
6. Phần lớn gặp các phương pháp chống lại điều tra phức tạp như mã hóa, nhiễu loạn mã nguồn.

**Điều tra Cloud**

1. Cloud Computing là gì

Cloud computing là một phương thức cho phép cung cấp các dịch vụ, ứng dụng thông qua hạ tầng mạng trên internet. Nơi người cung cấp các dịch vụ, ứng dụng trả phí cho các hạ tầng mạng thay vì phải đầu tư hạ tầng như trước.

Tính chất của Cloud computing

1. Tự cấu hình tùy theo nhu cầu
2. Cơ động trong dung lượng
3. Thích ứng với thay đổi nhanh chóng
4. Tự động quản lý
5. Đảm bảo truy cập
6. Vùng tài nguyên to lớn
7. Tùy biến dịch vụ
8. Công nghệ máy ảo

Các loại hình dịch vụ Cloud computing

Infrastructure-as-a-Service (IaaS) – Cung cấp các máy ảo, phần cứng, OS có thể được điều khiển thông qua API. VD Amazon EC2, Sungrid

Platform-as-a-Service (PaaS) – Cung cấp công cụ phát triển, cấu hình, và vận hành. VD Google App Engine, Microsoft Azure

Software-as-a-Service (SaaS) – Cung cấp phần mềm cho người dùng thông qua Internet. VD: Google Docs, Salesforce CRM

1. Các phương pháp tấn công could
2. Social Engineering
3. XSS cho Session Hijacking
4. Tấn công DNS
5. SQL injection
6. Network Sniffing
7. Session Riding
8. Side Channel Attacks
9. DDoS
10. Vai trò của điều tra cloud (đám mây)

Điều tra cloud là hành động xem xet, kiểm tra quá trình vận hành, truy cập, kết nối trên môi trường cloud computing. Hiện nay, điều tra cloud được xem là phân nhánh của điều tra mạng. Điều tra cloud gồm những hành dộng như tìm kiếm các truy cập bất thường, vấn đề bảo mật, thu thập nọi dung nhật ký, và khôi phục bằng chứng khác.

1. Sự khác biệt giữa những cuộc điều tra cloud (đám mây)

Thông thường, cloud có 2 loại hình là private và public cloud.

Trong trường hợp là private cloud, điều tra viên sẽ được phép truy cập vật lý vào các thông tin, thiết bị, và máy chủ.

Trong trường hợp là public cloud, điều tra viên sẽ không được phép truy cập vật lý vào các thông tin, thiết bị, và máy chủ.

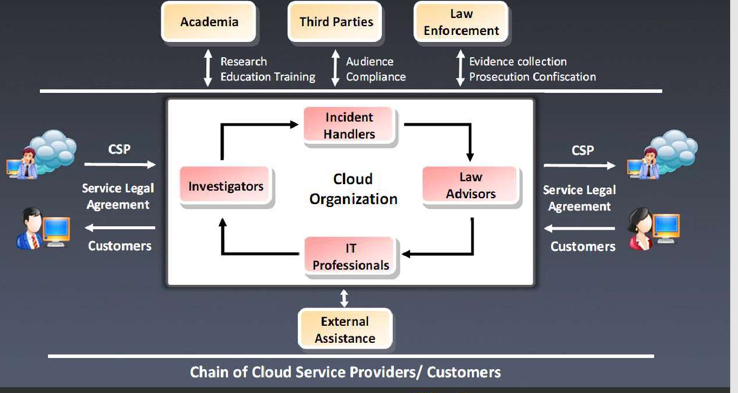
Trong đó, tùy vào cách thức tấn công, điều tra viên sẽ điều tra cloud theo ba hướng:

Cloud as a subject – Hành động, sự cố ATTT được thực hiện trong môi trường Cloud (vd: truy cập tk trái phép)

Cloud as an object - Hành động, sự cố ATTT nhắm vào nhà cung cấp Cloud (vd: DDOS)

Cloud as a tool – Sử dụng cloud như một công cụ để tấn công vào hệ thống khác

1. Hiểu được vai trò của các bên tham gia trong quá trình điều tra cloud



Thông thường một cuộc điều tra Cloud sẽ cần sự phối hợp từ ít nhất 1 nhà cung cấp và 1 k/h. Tuy nhiên, những khó khăn trong luật pháp, thủ tục, chính sách giữa các bên sẽ gây khó khăn lớn cho việc điều tra. Do đó, cần phải đảm bảo khi k/h hoặc nhà cung cấp muốn tổ chức 1 cuộc điều tra, các bên phải đảm bảo được sự phối hợp giữa đội ngũ IT, luật pháp, với đội ngũ điều tra.

1. Các khó khăn trong quá trình điều tra cloud
2. Xóa thông tin trên cloud
3. Khôi phục lại thông tin
4. Khả năng phối hợp giữa các nhà cung cấp
5. Mã độc trong VM được cung cấp
6. Bất khả thi khi cần thu thập các bằng chứng sống
7. Quy mô cuộc tấn công quá lớn
8. Cách biệt về địa lý, luật pháp
9. Không thể dùng chain of custody

NGƯỜI GIỚI THIỆU

1. Bell, Graeme B., Boddington, Richard (tháng 12 năm 2010). Ổ đĩa trạng thái rắn: Khởi đầu kết thúc cho thực hành hiện tại trong phục hồi pháp y kỹ thuật số? Tạp chí Pháp y kỹ thuật số, An ninh và Pháp luật.

2. Mell, P., & Grance, T. (2011, tháng 1). Định nghĩa NIST về Điện toán đám mây . Truy cập ngày 9 tháng 10 năm 2011, từ: <http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf>.

3. Tập đoàn Microsoft. (nd). IPv6 . Truy cập ngày 17 tháng 9 năm 2011, từ: <http://technet.microsoft.com/en-us/network/bb530961.aspx>.

4. Ruan, K., Baggili, I., Carthy, J., & Kechadi, T. (nd). Khảo sát về pháp y trên đám mây và các tiêu chí quan trọng về khả năng pháp y trên đám mây: Phân tích sơ bộ . Dublin, Ireland: Đại học Cao đẳng Dublin.

5. Ruan K, Carthy J, Kechadi T, Crosbie M. Cloud Forensics: An Overview Dublin, Ireland: IBM Ireland Ltd; 2011.

6. TechTarget. (2007, tháng 12). Điện toán đám mây . Được truy cập ngày 11 tháng 10 năm 2011, từ: <http://searchcloudcomputing.techtarget.com/definition/cloud-computing>.