# **MỤC LỤC**

[**MỤC LỤC** 1](#_Toc173173003)

[**DANH MỤC CÁC HÌNH** 2](#_Toc173173004)

[**CHƯƠNG 1. NỘI DUNG ĐỀ TÀI** 4](#_Toc173173005)

[**1.1.** **Tổng quan về Forensic Investigations** 4](#_Toc173173006)

[**1.1.1.** **Định nghĩa pháp y kỹ thuật số** 4](#_Toc173173007)

[**1.1.2.** **Quy trình điều tra pháp y kỹ thuật số** 4](#_Toc173173008)

[**1.1.3.** **Công cụ và kỹ thuật** 5](#_Toc173173009)

[**1.1.4.** **Thách thức trong pháp y kỹ thuật số** 5](#_Toc173173010)

[**1.1.5.** **Ứng dụng** 5](#_Toc173173011)

[**1.2.** **Tổng quan về công cụ Encase** 6](#_Toc173173012)

[**1.2.1.** **Thông tin về Encase** 6](#_Toc173173013)

[**1.2.2.** **Tệp tin bằng chứng (Evidence Files) và tính toàn vẹn của chúng** 7](#_Toc173173014)

[**1.2.3.** **Các tùy chọn cấu hình quan trọng trong Encase** 8](#_Toc173173015)

[**1.2.4.** **Tìm kiếm dữ liệu trong Encase** 10](#_Toc173173016)

[**1.2.5.** **Thêm dấu trang trong Encase** 12](#_Toc173173017)

[**1.2.6.** **Encase trong việc kiểm tra tính toàn vẹn của tệp tin** 13](#_Toc173173018)

[**1.2.7.** **Sử dụng Encase để phân tích chữ ký** 14](#_Toc173173019)

[**CHƯƠNG 2: NỘI DUNG DEMO.** 16](#_Toc173173020)

[**2.1. Kịch bản và mục tiêu chung của Lab** 16](#_Toc173173021)

[**2.1.1. Kịch bản** 16](#_Toc173173022)

[**2.1.2. Mục tiêu chung** 16](#_Toc173173023)

[**2.2. Lab minh họa** 17](#_Toc173173024)

[**KẾT LUẬN** 47](#_Toc173173025)

[**TÀI LIỆU THAM KHẢO** 48](#_Toc173173026)

# **DANH MỤC CÁC HÌNH**

[Hình 1. Bookmark 15](#_Toc167556156)

[Hình 2. Bookmark Data 16](#_Toc167556157)

[Hình 3. Tạo new case 20](#_Toc167556158)

[Hình 4. Add Device 21](#_Toc167556159)

[Hình 5. Hoàn thành add device 22](#_Toc167556160)

[Hình 6. Xác minh tính toàn vẹn của tệp 23](#_Toc167556161)

[Hình 7. Verify File Integrty 23](#_Toc167556162)

[Hình 8. Chờ để hoàn thành xác minh 24](#_Toc167556163)

[Hình 9. Hashing giúp xác minh tính toàn vẹn 24](#_Toc167556164)

[Hình 10. Hash 25](#_Toc167556165)

[Hình 11. Kết quả của hashing 25](#_Toc167556166)

[Hình 12. Tên của máy tính 26](#_Toc167556167)

[Hình 13. User password hint 27](#_Toc167556168)

[Hình 14. Các tài khoản của hệ điều hành 27](#_Toc167556169)

[Hình 15. Shutdown time 28](#_Toc167556170)

[Hình 16. Thông tin của network interface 29](#_Toc167556171)

[Hình 17. Thực hiện đánh dấu tệp 29](#_Toc167556172)

[Hình 18. Cấu hình nơi lưu đánh dấu 30](#_Toc167556173)

[Hình 19. Kết quả của đánh dấu tệp 30](#_Toc167556174)

[Hình 20. Sao chép các tệp ra ngoài 31](#_Toc167556175)

[Hình 21. Copy/UnErase 31](#_Toc167556176)

[Hình 22. Cấu hình 32](#_Toc167556177)

[Hình 23. Destination 32](#_Toc167556178)

[Hình 24. Kết quả sau khi copy 32](#_Toc167556179)

[Hình 25. Giao diện F-RAT 33](#_Toc167556180)

[Hình 26. Thêm các file system 33](#_Toc167556181)

[Hình 27. Apply để hoàn thành 34](#_Toc167556182)

[Hình 28. Last Shutdown Time 34](#_Toc167556183)

[Hình 29. Startup Programs 35](#_Toc167556184)

[Hình 30. USB Devices 35](#_Toc167556185)

[Hình 31. Software Installed 36](#_Toc167556186)

[Hình 32. Software Install 37](#_Toc167556187)

[Hình 33. Lịch sử của trình duyệt Google 37](#_Toc167556188)

[Hình 34. Đường dẫn lịch sử duyệt web 38](#_Toc167556189)

[Hình 35. Lọc các tệp trò chuyện mail 39](#_Toc167556190)

[Hình 36. Kết quả lọc 39](#_Toc167556191)

[Hình 37. Kernel OST Viewer 40](#_Toc167556192)

[Hình 38. Thêm file ost 41](#_Toc167556193)

[Hình 39. Lịch sử trò chuyện 41](#_Toc167556194)

[Hình 40. Thumbcache file 42](#_Toc167556195)

[Hình 41. Thumbcache Viewer 42](#_Toc167556196)

[Hình 42. Thêm file thumbcache 43](#_Toc167556197)

[Hình 43. Kết quả tìm được 43](#_Toc167556198)

[Hình 44. Tạo keyword mới 44](#_Toc167556199)

[Hình 45. Tiến hành tìm kiếm dựa trên key word 44](#_Toc167556200)

[Hình 46. Kết quả tìm kiếm 45](#_Toc167556201)

[Hình 47. Xuất ổ đĩa theo định dạng Raw 46](#_Toc167556202)

[Hình 48. Mở file ổ đĩa định dạng Raw 46](#_Toc167556203)

[Hình 49. Sau khi mở file 47](#_Toc167556204)

[Hình 50. Khôi phục các file 47](#_Toc167556205)

[Hình 51. Chọn loại file muốn khôi phục 48](#_Toc167556206)

[Hình 52. Kết quả sau khi khôi phục 48](#_Toc167556207)

[Hình 53. Các tệp bị đánh cắp 49](#_Toc167556208)

[Hình 54. Reporting 49](#_Toc167556209)

# **CHƯƠNG 1. NỘI DUNG ĐỀ TÀI**

* 1. **Tổng quan về Forensic Investigations**

Điều tra pháp y (Forensic Investigations) là quá trình thu thập, phân tích và trình bày các chứng cứ liên quan đến tội phạm hoặc hành vi bất hợp pháp để hỗ trợ trong quá trình điều tra và xét xử. Có nhiều lĩnh vực trong điều tra pháp y, bao gồm pháp y kỹ thuật số (digital forensics), pháp y hiện trường (crime scene forensics), pháp y sinh học (biological forensics), và pháp y pháp luật (legal forensics). Trong bối cảnh hiện đại, pháp y kỹ thuật số ngày càng trở nên quan trọng do sự gia tăng của tội phạm công nghệ cao và các vi phạm bảo mật thông tin.

* + 1. **Định nghĩa pháp y kỹ thuật số**

Pháp y kỹ thuật số là lĩnh vực điều tra pháp y liên quan đến việc thu thập, phân tích và bảo quản các chứng cứ số (digital evidence) từ các thiết bị điện tử như máy tính, điện thoại di động, máy chủ, thiết bị lưu trữ và mạng. Mục tiêu là để tìm kiếm, phục hồi và phân tích dữ liệu liên quan đến các hoạt động tội phạm hoặc các vi phạm về bảo mật thông tin.

* + 1. **Quy trình điều tra pháp y kỹ thuật số**

Quy trình điều tra pháp y kỹ thuật số thường bao gồm các bước sau:

* Xác định và Bảo Vệ Hiện Trường: Đảm bảo rằng hiện trường điều tra (các thiết bị số và môi trường mạng) không bị xâm phạm hoặc thay đổi trước khi tiến hành thu thập dữ liệu.
* Thu Thập Chứng Cứ: Sử dụng các công cụ và kỹ thuật để thu thập dữ liệu từ các thiết bị và hệ thống mạng. Điều này bao gồm việc tạo ra các bản sao dữ liệu (forensic images) để bảo quản tính toàn vẹn của chứng cứ.
* Phân Tích Dữ Liệu: Sử dụng các công cụ phân tích pháp y để khám phá, trích xuất và diễn giải dữ liệu từ các thiết bị và bản sao dữ liệu. Quá trình này có thể bao gồm phân tích các tệp tin, email, nhật ký hệ thống, và các hoạt động mạng.
* Báo Cáo và Trình Bày: Tạo ra báo cáo chi tiết về các phát hiện và chuẩn bị các chứng cứ để trình bày trước tòa hoặc cho các bên liên quan.
  + 1. **Công cụ và kỹ thuật**

Các công cụ và kỹ thuật phổ biến trong pháp y kỹ thuật số bao gồm:

* EnCase và FTK (Forensic Toolkit): Các phần mềm pháp y chuyên dụng để thu thập và phân tích dữ liệu.
* Wireshark: Công cụ phân tích mạng dùng để kiểm tra lưu lượng mạng và phát hiện các hoạt động đáng ngờ.
* Autopsy và Sleuth Kit: Bộ công cụ mã nguồn mở dùng để phân tích các hệ thống tệp tin và khám phá các chứng cứ số.
* Write Blockers: Thiết bị dùng để bảo vệ dữ liệu gốc khỏi bị thay đổi trong quá trình thu thập chứng cứ.
  + 1. **Thách thức trong pháp y kỹ thuật số**

Một số thách thức chính trong lĩnh vực pháp y kỹ thuật số bao gồm:

* Khối Lượng Dữ Liệu Lớn: Lượng dữ liệu cần phân tích thường rất lớn, đòi hỏi thời gian và tài nguyên đáng kể.
* Mã Hóa và Bảo Mật: Nhiều dữ liệu có thể được mã hóa hoặc bảo vệ bởi các biện pháp bảo mật, làm cho việc truy cập và phân tích trở nên khó khăn.
* Tính Toàn Vẹn của Chứng Cứ: Đảm bảo rằng chứng cứ không bị thay đổi hoặc xâm phạm trong suốt quá trình điều tra là vô cùng quan trọng.
* Cập Nhật Công Nghệ: Tội phạm công nghệ cao thường sử dụng các kỹ thuật mới và tinh vi, đòi hỏi các nhà điều tra phải liên tục cập nhật và nâng cao kỹ năng.
  + 1. **Ứng dụng**

Pháp y kỹ thuật số có nhiều ứng dụng trong các lĩnh vực như:

* Điều Tra Tội Phạm: Giúp các cơ quan thực thi pháp luật trong việc điều tra và xử lý các vụ án liên quan đến tội phạm mạng, lừa đảo, và vi phạm bản quyền.
* An Ninh Mạng: Hỗ trợ các tổ chức trong việc điều tra các vụ tấn công mạng, vi phạm bảo mật, và mất mát dữ liệu.
* Tranh Chấp Doanh Nghiệp: Cung cấp bằng chứng trong các vụ tranh chấp pháp lý liên quan đến sở hữu trí tuệ, gian lận, và vi phạm hợp đồng.
  1. **Tổng quan về công cụ Encase**
     1. **Thông tin về Encase**

EnCase là một công cụ điều tra pháp y kỹ thuật số được phát triển bởi công ty Guidance Software, hiện nay thuộc sở hữu của OpenText. Đây là một trong những phần mềm hàng đầu trong lĩnh vực pháp y kỹ thuật số, được sử dụng rộng rãi bởi các cơ quan thực thi pháp luật, doanh nghiệp, và các chuyên gia pháp y để thu thập, phân tích và bảo quản bằng chứng số từ các thiết bị điện tử.

***Chức năng chính của EnCase***

Thu thập dữ liệu (Data Acquisition):

* EnCase có khả năng thu thập dữ liệu từ nhiều nguồn khác nhau như máy tính, điện thoại di động, máy chủ, và các thiết bị lưu trữ khác mà không làm thay đổi hoặc hủy hoại dữ liệu gốc.
* Hỗ trợ nhiều loại hệ thống tập tin và hệ điều hành, bao gồm Windows, Mac OS, Linux và các hệ điều hành di động.

Phân tích (Analysis):

* Cung cấp các công cụ mạnh mẽ để phân tích dữ liệu, bao gồm tìm kiếm từ khóa, khôi phục tập tin đã xóa, và phân tích email.
* Cho phép xem và phân tích cấu trúc file hệ thống, nhật ký hệ thống, và các hoạt động người dùng.

Bảo quản bằng chứng (Evidence Preservation):

* Đảm bảo rằng dữ liệu được thu thập và bảo quản theo đúng các quy chuẩn pháp lý, đảm bảo tính nguyên vẹn và đáng tin cậy của bằng chứng.
* Tạo ra các báo cáo chi tiết và toàn diện để sử dụng trong quá trình điều tra và tố tụng.

***Các phiên bản của EnCase***

EnCase có nhiều phiên bản khác nhau, phục vụ cho các nhu cầu điều tra khác nhau:

* EnCase Forensic: Phiên bản dành cho các chuyên gia pháp y, tập trung vào việc thu thập và phân tích bằng chứng số.
* EnCase Endpoint Investigator: Dành cho các tổ chức và doanh nghiệp, giúp theo dõi và điều tra các sự cố an ninh nội bộ.
* EnCase eDiscovery: Dành cho các luật sư và chuyên gia pháp lý để hỗ trợ trong việc tìm kiếm và thu thập bằng chứng trong các vụ kiện tụng.
  + 1. **Tệp tin bằng chứng (Evidence Files) và tính toàn vẹn của chúng**

**Định nghĩa:** Tệp tin bằng chứng là các tệp tin chứa bản sao chính xác của dữ liệu gốc từ thiết bị điện tử. Chúng có thể bao gồm hình ảnh pháp y của ổ cứng, dữ liệu bộ nhớ, tệp nhật ký hệ thống, email, tài liệu và nhiều loại dữ liệu số khác.

**Đặc Điểm:**

* Chính Xác: Tệp tin bằng chứng phải là bản sao chính xác của dữ liệu gốc, không bị thay đổi hoặc chỉnh sửa trong quá trình thu thập.
* Có Thể Kiểm Tra: Tính toàn vẹn của tệp tin bằng chứng có thể được kiểm tra và xác minh bằng cách sử dụng các hàm băm mật mã.
* Bảo Mật: Tệp tin bằng chứng cần được bảo vệ để ngăn chặn truy cập trái phép hoặc thay đổi.

Tính toàn vẹn của tệp tin bằng chứng là một yếu tố cực kỳ quan trọng trong điều tra pháp y kỹ thuật số, vì nó đảm bảo rằng dữ liệu không bị thay đổi hoặc giả mạo từ lúc thu thập đến lúc trình bày trước tòa. Để đảm bảo tính toàn vẹn, các bước sau đây được thực hiện:

* Tạo Hàm Băm (Hashing): MD5, SHA-1, SHA-256: Các thuật toán băm phổ biến được sử dụng để tạo ra giá trị băm duy nhất (hash value) cho dữ liệu gốc. Giá trị băm này được tính toán ngay khi dữ liệu được thu thập và được sử dụng để so sánh với giá trị băm của tệp tin bằng chứng trong quá trình phân tích.
* Sử Dụng Write Blockers: Write Blockers: Các thiết bị này ngăn chặn bất kỳ thay đổi nào đối với thiết bị gốc trong khi dữ liệu đang được sao chép, đảm bảo rằng dữ liệu gốc không bị thay đổi trong quá trình thu thập.
* Lưu Trữ An Toàn: Bảo Mật Vật Lý và Logic: Tệp tin bằng chứng cần được lưu trữ trong môi trường an toàn, với các biện pháp bảo mật vật lý và logic để ngăn chặn truy cập trái phép.
  + 1. **Các tùy chọn cấu hình quan trọng trong Encase**

**1. Thiết Lập Cơ Bản**

***Cài Đặt Thư Mục Làm Việc (Working Directory):***

* Mục Đích: Xác định nơi lưu trữ các tệp tin dự án, dữ liệu thu thập và kết quả phân tích.
* Cách Thực Hiện: Trong phần Tools > Options, vào tab Directories để cấu hình thư mục làm việc.

***Thiết Lập Tùy Chọn Hiển Thị (Display Options):***

* Mục Đích: Tùy chỉnh giao diện làm việc để phù hợp với nhu cầu cá nhân.
* Cách Thực Hiện: Trong Tools > Options, vào tab View để thay đổi các thiết lập hiển thị như phông chữ, màu sắc, và bố cục.

**2. Cấu Hình Thu Thập Dữ Liệu**

***Thiết Lập Chụp Hình Ảnh Pháp Y (Forensic Image Acquisition):***

* Mục Đích: Đảm bảo quá trình tạo hình ảnh pháp y được thực hiện chính xác và an toàn.
* Cách Thực Hiện:
* Chọn New > Case > Add Evidence > Image Device.
* Cấu hình các tùy chọn như định dạng hình ảnh (E01, Ex01), mức độ nén, và tính toàn vẹn bằng cách sử dụng các thuật toán hash (MD5, SHA-1).

***Sử Dụng Write Blocker:***

* Mục Đích: Ngăn chặn việc ghi dữ liệu lên thiết bị gốc trong quá trình thu thập dữ liệu.
* Cách Thực Hiện: Kết nối thiết bị qua write blocker trước khi tiến hành thu thập dữ liệu.

**3. Quản Lý và Phân Tích Dữ Liệu**

***Cấu Hình Bộ Lọc (Filters):***

* Mục Đích: Giúp lọc và hiển thị dữ liệu dựa trên các tiêu chí cụ thể như loại tệp, thời gian tạo, và kích thước tệp.
* Cách Thực Hiện: Trong View > Filters, tạo hoặc chỉnh sửa các bộ lọc theo nhu cầu điều tra.

***Thiết Lập Keyword Search:***

* Mục Đích: Tìm kiếm các từ khóa hoặc cụm từ cụ thể trong các tệp tin và thư mục.
* Cách Thực Hiện: Vào Search > Keyword Search, thêm từ khóa và chọn phạm vi tìm kiếm.

**4. Bảo Mật và Quản Lý Người Dùng**

***Thiết Lập Mã Hóa Dữ Liệu (Data Encryption):***

* Mục Đích: Bảo vệ dữ liệu điều tra khỏi truy cập trái phép.
* Cách Thực Hiện: Trong Tools > Options, vào tab Security, bật tính năng mã hóa và thiết lập các tùy chọn mã hóa.

**5. Cấu Hình Báo Cáo (Reporting)**

***Thiết Lập Tùy Chọn Báo Cáo:***

* Mục Đích: Tạo các báo cáo chi tiết và chuyên nghiệp về các phát hiện điều tra.
* Cách Thực Hiện: Trong Tools > Options, vào tab Report, cấu hình các tùy chọn báo cáo như định dạng, nội dung và mẫu báo cáo.

***Tạo và Xuất Báo Cáo:***

* Mục Đích: Xuất báo cáo cho các bên liên quan hoặc sử dụng trong quá trình xét xử.
* Cách Thực Hiện: Vào Report > Create Report, chọn các mục cần bao gồm và xuất báo cáo dưới các định dạng như PDF, HTML, hoặc Word.
  + 1. **Tìm kiếm dữ liệu trong Encase**

EnCase cung cấp khả năng tìm kiếm mạnh mẽ. Điều tra viên có thể thực hiện tìm kiếm từ khóa ở cấp độ lô-gic (cấp độ tệp) hoặc cấp độ vật lý (theo từng byte). EnCase có thể định vị thông tin ở bất kỳ đâu trên phương tiện vật lý hoặc lô-gic bằng cách sử dụng các tính năng phân tích chuyên sâu của nó. EnCase có các khả năng tìm kiếm nâng cao sau:

Concurrent search (Tìm kiếm đồng thời)

Proximity search (Tìm kiếm gần)

Internet and e-mail search (Tìm kiếm trên Internet và email)

E-mail address search (Tìm kiếm địa chỉ email)

Global Regular Expressions Post (GREP) search (Tìm kiếm Toàn cầu Biểu thức chính quy Bài đăng (GREP)): Tiện ích tìm kiếm GREP cho phép điều tra viên tìm kiếm thông tin có định dạng chung đã biết, chẳng hạn như bất kỳ số điện thoại, số thẻ tín dụng, ID mạng, hồ sơ đăng nhập hoặc địa chỉ IP nào, ngay cả khi không biết số cụ thể

File finder (Trình tìm tệp): Tìm kiếm trong tệp trang, các cụm chưa được phân bổ, các tệp đã chọn hoặc toàn bộ trường hợp, tìm kiếm các loại tệp cụ thể và dữ liệu có cấu trúc

EnCase cung cấp các tùy chọn tìm kiếm sau:

Case sensitive (Phân biệt chữ hoa chữ thường): EnCase chỉ tìm kiếm các từ khóa trong trường hợp chính xác được chỉ định trong hộp văn bản.

GREP: Từ khóa là một biểu thức chính quy.

RTL reading (Đọc RTL): Đây là tìm kiếm từ khóa theo trình tự từ phải sang trái để hỗ trợ ngôn ngữ quốc tế.

Active code page (Trang mã đang hoạt động): Tùy chọn này cho phép điều tra viên nhập từ khóa bằng nhiều ngôn ngữ khác nhau.

Unicode: Cho phép các nhà điều tra tìm kiếm các từ khóa bằng các ký tự ngôn ngữ quốc tế.

Big-endian Unicode: Cho phép các nhà điều tra tìm kiếm các từ khóa bằng các ký tự ngôn ngữ quốc tế.

**1. Tìm Kiếm Từ Khóa (Keyword Search)**

***Cách Thực Hiện:***

* Mở Vụ Án: Mở vụ án (case) bạn đang điều tra trong EnCase.
* Chọn Tìm Kiếm Từ Khóa: Vào Search > Keyword Search.
* Nhập Từ Khóa: Nhập các từ khóa hoặc cụm từ cần tìm kiếm. Có thể nhập nhiều từ khóa cùng lúc.
* Cấu Hình Tùy Chọn Tìm Kiếm:
* Exact Match: Tìm kiếm chính xác từ khóa.
* Case Insensitive: Bỏ qua phân biệt chữ hoa và chữ thường.
* Chọn Phạm Vi Tìm Kiếm: Chọn nơi cần tìm kiếm, có thể là toàn bộ ổ đĩa, một thư mục cụ thể, hoặc một tập hợp các tệp tin.
* Thực Hiện Tìm Kiếm: Nhấn Search để bắt đầu quá trình tìm kiếm.
* Xem Kết Quả: Kết quả sẽ hiển thị trong bảng kết quả tìm kiếm, có thể xem chi tiết từng kết quả.

**2. File finder (Trình tìm tệp)**

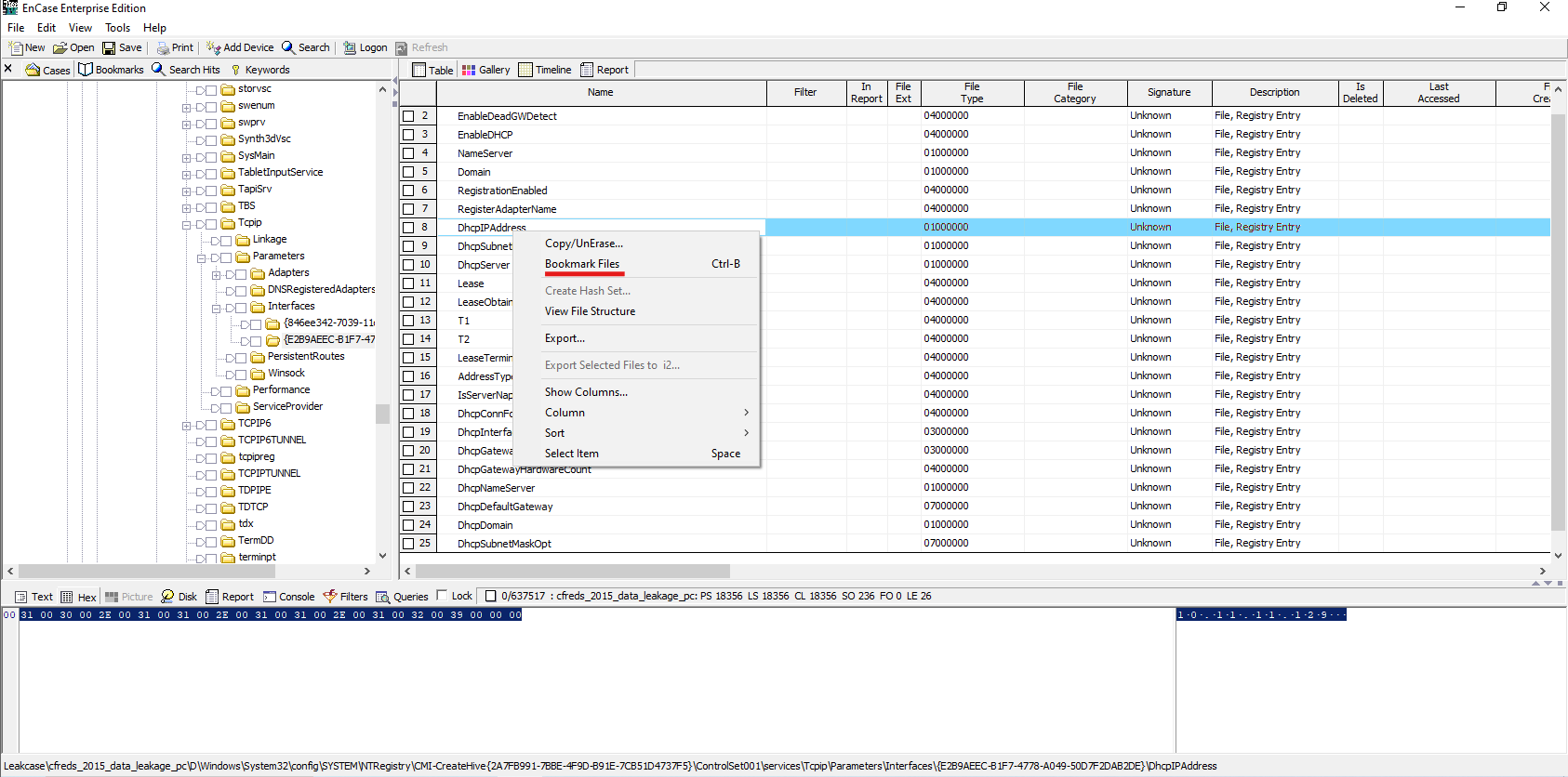
EnCase hỗ trợ tìm kiếm tài liệu và email một cách chi tiết, bao gồm các định dạng như PST, OST, EDB, và NSF.

***Cách Thực Hiện:***

* Mở Vụ Án: Mở vụ án (case) trong EnCase.
* Chọn Tìm Kiếm Tài Liệu và Email: Vào Filter > Document and Email.
* Cấu Hình Tìm Kiếm: Chọn các loại thư, tài liệu, hoặc thư mục email cần tìm kiếm..
* Thực Hiện Tìm Kiếm: Nhấn Search để bắt đầu quá trình tìm kiếm.
* Xem Kết Quả: Kết quả sẽ hiển thị trong bảng kết quả tìm kiếm.
  + 1. **Thêm dấu trang trong Encase**

Bookmark (Thêm dấu trang):

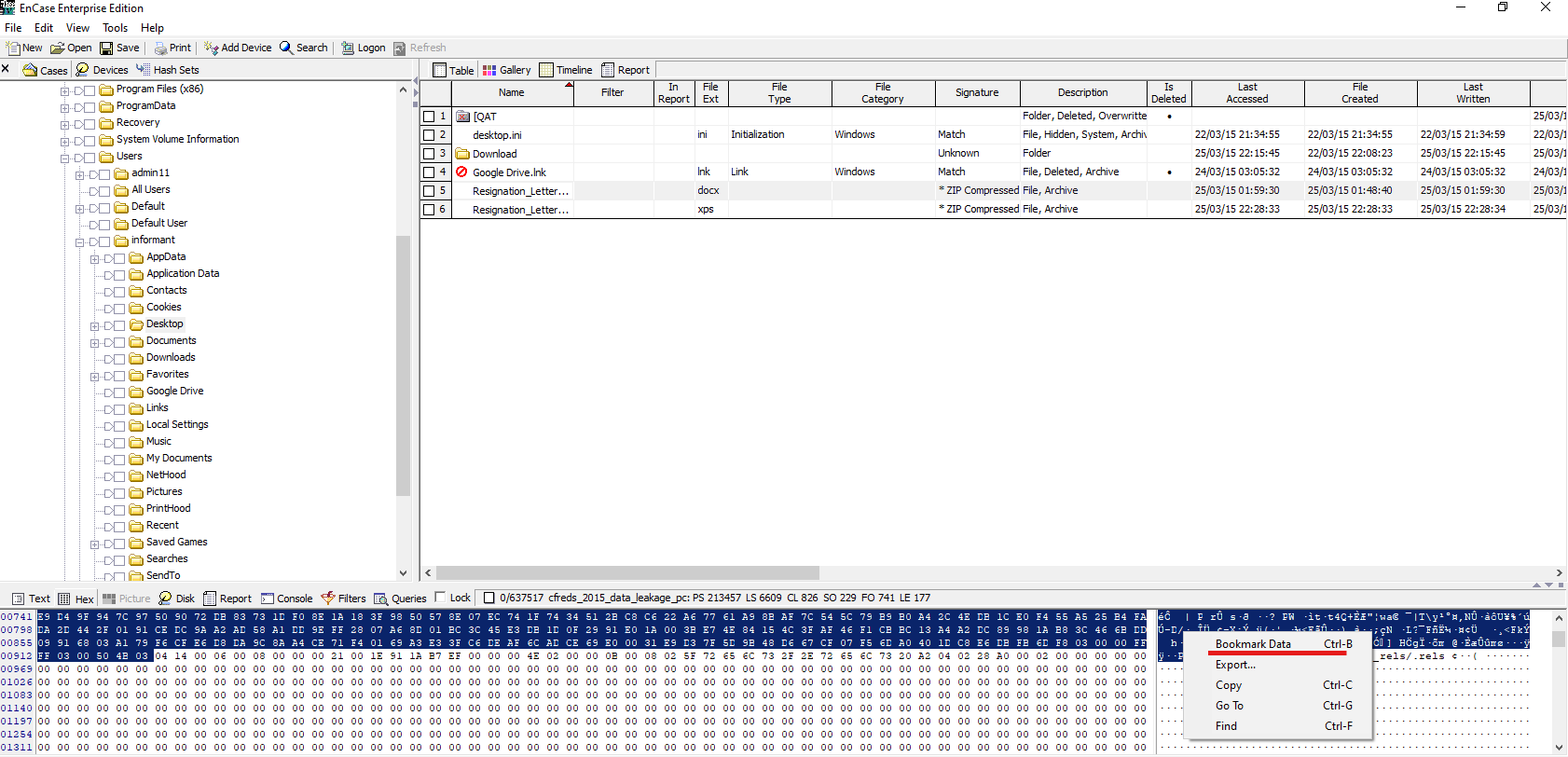
Điều tra viên có thể thêm dấu trang bằng cách nhấp chuột phải vào bất kỳ tệp nào và chọn View => chọn Bookmark, như trong Hình 1.



Hình 1. Bookmark

Bookmarking a Selected Area (Đánh dấu một khu vực đã chọn):

Điều tra viên có thể đánh dấu một khu vực đã chọn bằng cách tô sáng khu vực văn bản và chọn Bookmark Data (Dữ liệu đánh dấu), như trong Hình 2.



Hình 2. Bookmark Data

* + 1. **Encase trong việc kiểm tra tính toàn vẹn của tệp tin**

**1. Kiểm Tra Tính Toàn Vẹn của Tệp Tin**

Kiểm tra tính toàn vẹn của tệp tin là quá trình so sánh giá trị băm hiện tại của tệp tin với giá trị băm ban đầu (được tạo lúc thu thập) để xác nhận rằng tệp tin không bị thay đổi.

***Cách Thực Hiện:***

* Mở Vụ Án (Case): Mở vụ án liên quan trong EnCase.
* Thêm Bằng Chứng (Add Evidence): Thêm tệp tin hoặc thiết bị cần kiểm tra vào vụ án nếu chưa thêm.
* Chọn Tệp Tin: Chọn tệp tin hoặc thư mục mà bạn muốn kiểm tra.
* So Sánh Giá Trị Băm:
* Nhấp chuột phải vào tệp tin và chọn Verify Hash từ menu ngữ cảnh.
* EnCase sẽ tạo lại giá trị băm hiện tại của tệp tin và so sánh với giá trị băm ban đầu.
* Kiểm Tra Kết Quả: EnCase sẽ hiển thị kết quả so sánh. Nếu giá trị băm khớp, tệp tin không bị thay đổi; nếu không khớp, tệp tin đã bị thay đổi.

**2. Báo Cáo Giá Trị Băm**

***Tạo Báo Cáo:***

* Mở Vụ Án (Case): Mở vụ án trong EnCase.
* Chọn Báo Cáo: Vào Report > Create Report.
* Cấu Hình Báo Cáo: Chọn các mục cần bao gồm trong báo cáo, như thông tin vụ án, giá trị băm của tệp tin, và kết quả kiểm tra tính toàn vẹn.
* Xuất Báo Cáo: Xuất báo cáo dưới các định dạng như PDF, HTML, hoặc Word để chia sẻ với các bên liên quan hoặc lưu trữ.
  + 1. **Sử dụng Encase để phân tích chữ ký**

Chữ ký của một tệp tin là một chuỗi byte đặc trưng xuất hiện ở phần đầu (header) hoặc đôi khi ở phần cuối (footer) của tệp tin. Các chữ ký này là duy nhất cho từng loại tệp và được sử dụng để xác định định dạng tệp tin. Ví dụ, các tệp hình ảnh JPEG bắt đầu với chuỗi byte FFD8FF, trong khi các tệp PDF bắt đầu với %PDF.

***Các Chữ Ký Phổ Biến:***

JPEG: FFD8FF

PDF: %PDF

ZIP: 504B0304

DOCX: 504B0304 (giống ZIP do định dạng DOCX thực chất là một tập hợp các tệp tin được nén lại)

PNG: 89504E47

***Vai Trò của Phân Tích Chữ Ký trong Phục Hồi Dữ Liệu***

Phân tích chữ ký đóng vai trò quan trọng trong quá trình phục hồi dữ liệu bị xóa hoặc bị hỏng. Đây là các khía cạnh cụ thể:

*a. Xác Định Định Dạng Tệp Tin:*

Phát Hiện Tệp Tin Bị Đổi Phần Mở Rộng: Khi phần mở rộng của tệp tin bị thay đổi (ví dụ: từ .jpg thành .txt), phân tích chữ ký giúp xác định đúng loại tệp tin dựa trên nội dung thực tế của nó.

Phục Hồi Tệp Tin Bị Xóa: Khi một tệp tin bị xóa, hệ điều hành thường chỉ xóa tham chiếu đến tệp tin trong bảng tệp tin (file table) và dữ liệu thực tế vẫn tồn tại trên đĩa cho đến khi bị ghi đè. Phân tích chữ ký giúp tìm kiếm và phục hồi các tệp tin này bằng cách nhận diện chữ ký đặc trưng của chúng trong các vùng dữ liệu chưa được gán.

*b. Tăng Cường Khả Năng Phát Hiện:*

Phát Hiện Các Tệp Tin Ẩn: Một số tệp tin có thể bị ẩn hoặc mã hóa. Phân tích chữ ký giúp phát hiện các tệp tin này dựa trên mẫu byte đặc trưng, ngay cả khi chúng không xuất hiện trong danh sách tệp tin bình thường.

Phục Hồi Các Tệp Tin Bị Hỏng: Trong trường hợp các tệp tin bị hỏng hoặc phân mảnh, phân tích chữ ký giúp xác định các phần còn lại của tệp tin và phục hồi chúng đến mức tối đa có thể.

**CHƯƠNG 2: NỘI DUNG DEMO.**

## **2.1. Kịch bản và mục tiêu chung của Lab**

### **2.1.1. Kịch bản**

Một người quản lý ('Mr. Informant') tại công ty công nghệ OOO bị nghi ngờ rò rỉ dữ liệu nhạy cảm cho công ty đối thủ thông qua 'Spy Conspirator'. 'Mr. Informant' đã che giấu kế hoạch bằng cách giao tiếp qua email và chia sẻ thông tin mẫu qua bộ nhớ đám mây cá nhân. Khi anh ta cố gắng mang các thiết bị lưu trữ ra khỏi công ty, anh ta đã bị phát hiện tại trạm kiểm soát an ninh. Các thiết bị của anh ta (USB và CD) không có bằng chứng rò rỉ trong lần kiểm tra đầu tiên và được gửi đến phòng thí nghiệm pháp y để phân tích thêm.

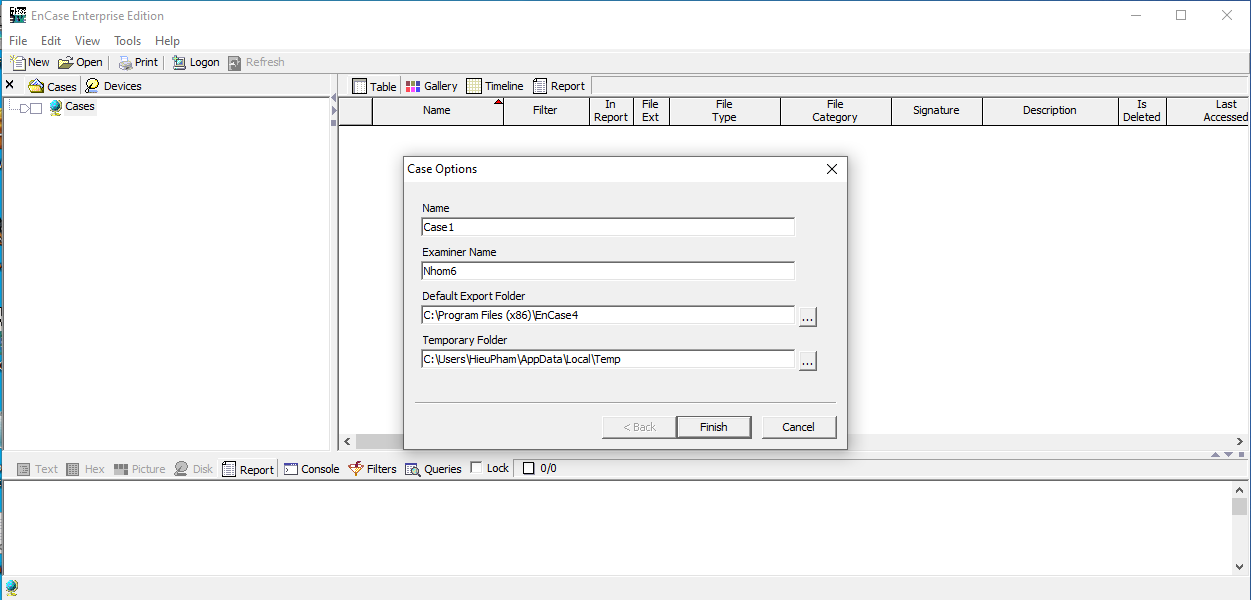
Nhiệm vụ là sử dụng công cụ Encase Forensic tìm bằng chứng về việc rò rỉ dữ liệu và bất kỳ dữ liệu nào có thể đã được tạo ra từ các thiết bị điện tử của nghi phạm.

### **2.1.2. Mục tiêu chung**

* Áp dụng các kỹ năng và kiến thức điều tra pháp y kỹ thuật số cơ bản để phân tích ổ cứng sử dụng EnCase.
* Củng cố kiến thức lý thuyết về các tập tin bằng chứng, hashing, cấu hình EnCase, tìm kiếm dữ liệu,...
* Rèn luyện các kỹ năng quan trọng trong quá trình điều tra pháp y, bao gồm:
* Sử dụng các kỹ thuật (hash) đảm bảo tính toàn vẹn của bằng chứng số
* Thu thập và bảo quản bằng chứng kỹ thuật số.
* Phân tích dữ liệu ổ cứng.
* Tìm kiếm và khôi phục dữ liệu bị xóa.
* Xác định các bằng chứng liên quan đến vụ án.
* Viết báo cáo kết quả phân tích.
* Nâng cao nhận thức về tầm quan trọng của điều tra pháp y kỹ thuật số trong thực tiễn.

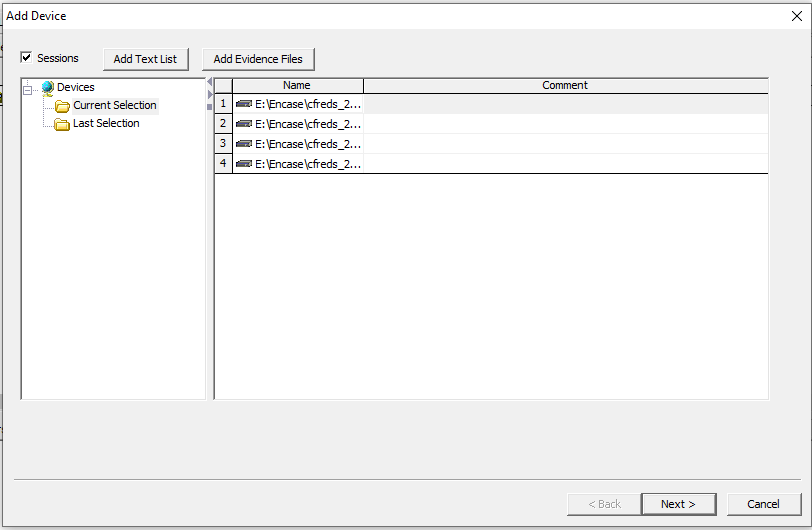
## **2.2. Lab minh họa**

Đầu tiên chúng em sẽ tạo một case mới để bắt đầu quá trình phân tích.

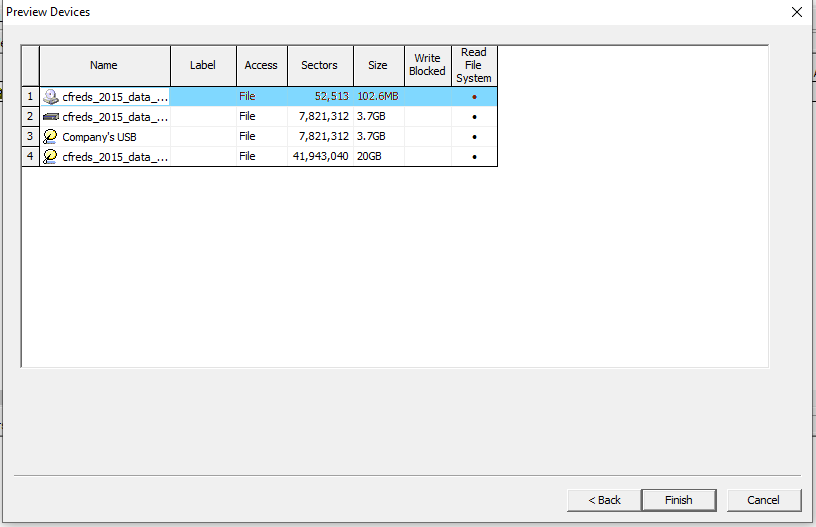


Hình 3. Tạo new case

Sau khi tạo case thì thêm thiết bị đã thu thập được để phân tích.

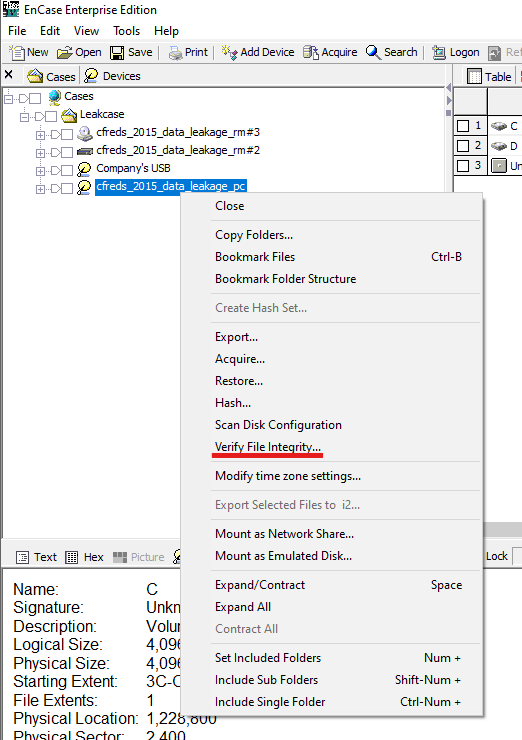


Hình 4. Add Device

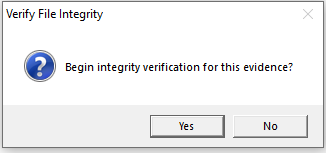


Hình 5. Hoàn thành add device

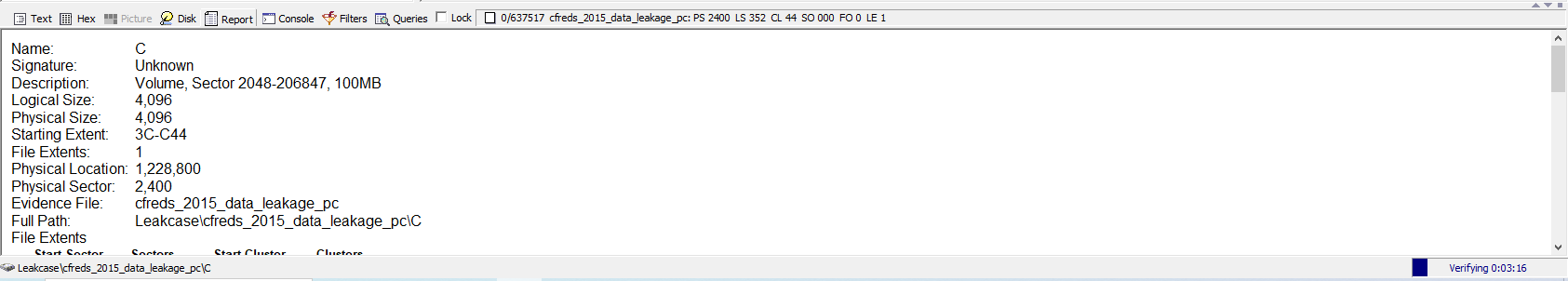
Sau khi thêm thiết bị thì tiến hành xác minh tính toàn vẹn của các file trong thiết bị bằng Verify File Integrty. Và cũng có thể dùng Hashing để giúp xác minh tính toàn vẹn.



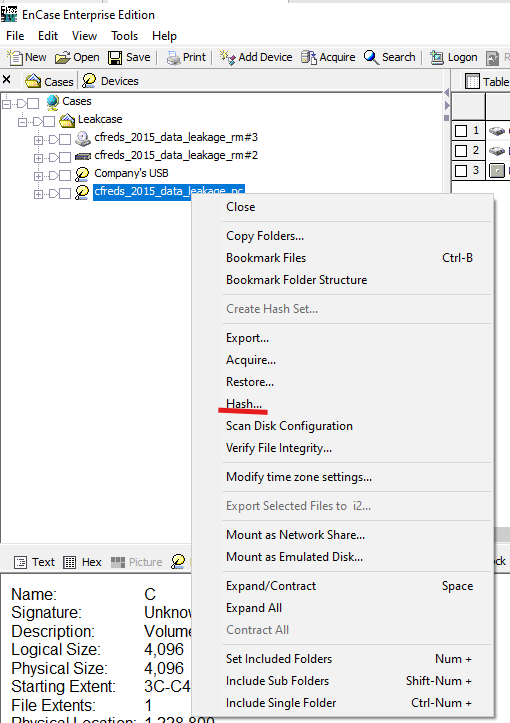
Hình 6. Xác minh tính toàn vẹn của tệp



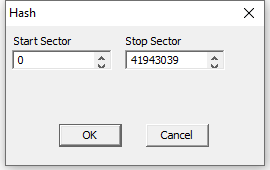
Hình 7. Verify File Integrty



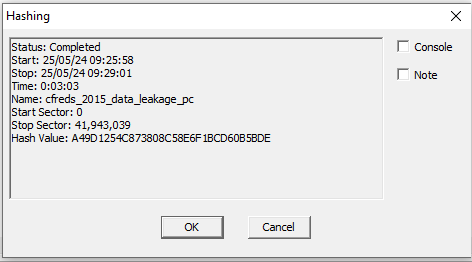
Hình 8. Chờ để hoàn thành xác minh



Hình 9. Hashing giúp xác minh tính toàn vẹn



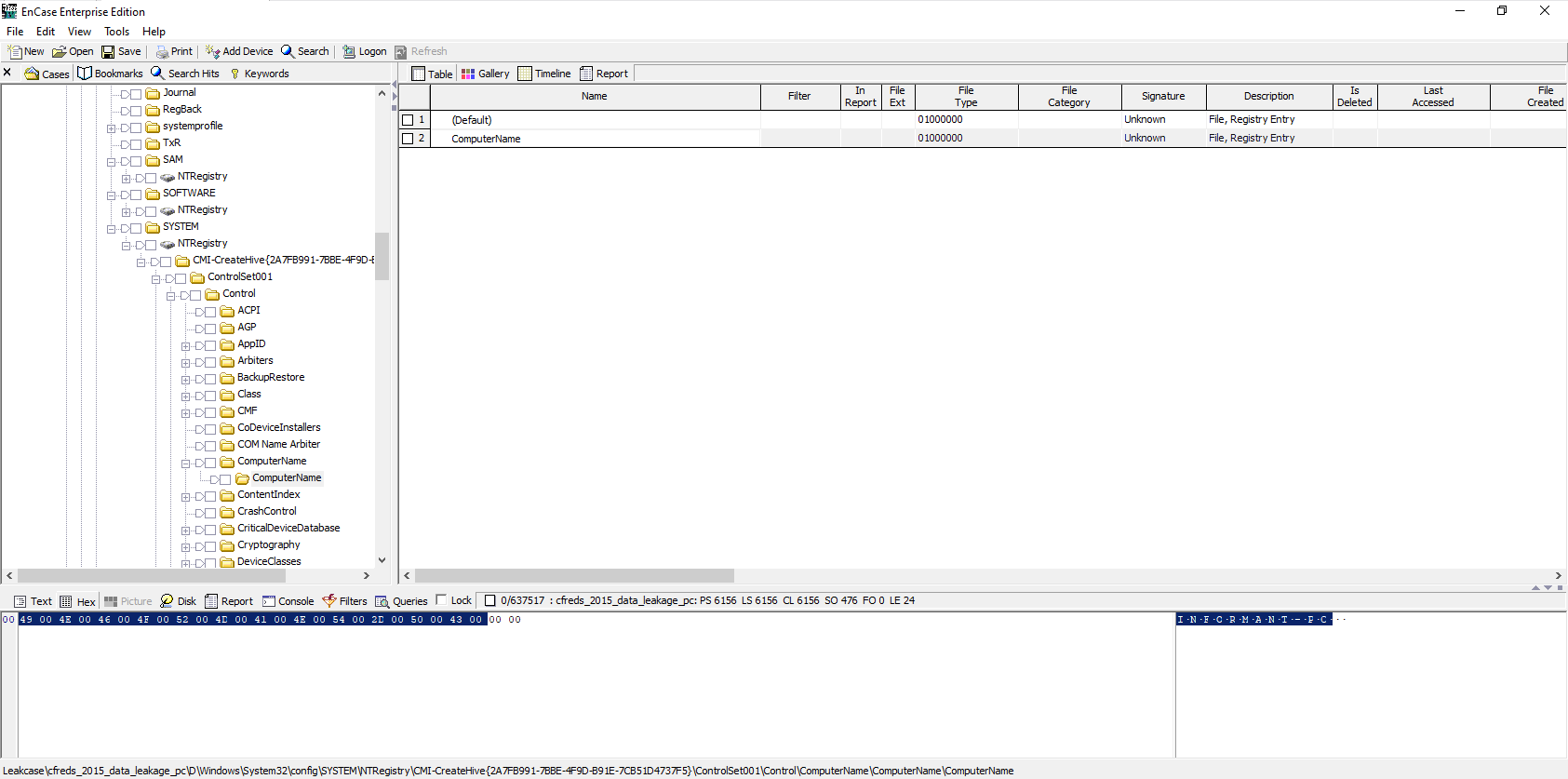
Hình 10. Hash



Hình 11. Kết quả của hashing

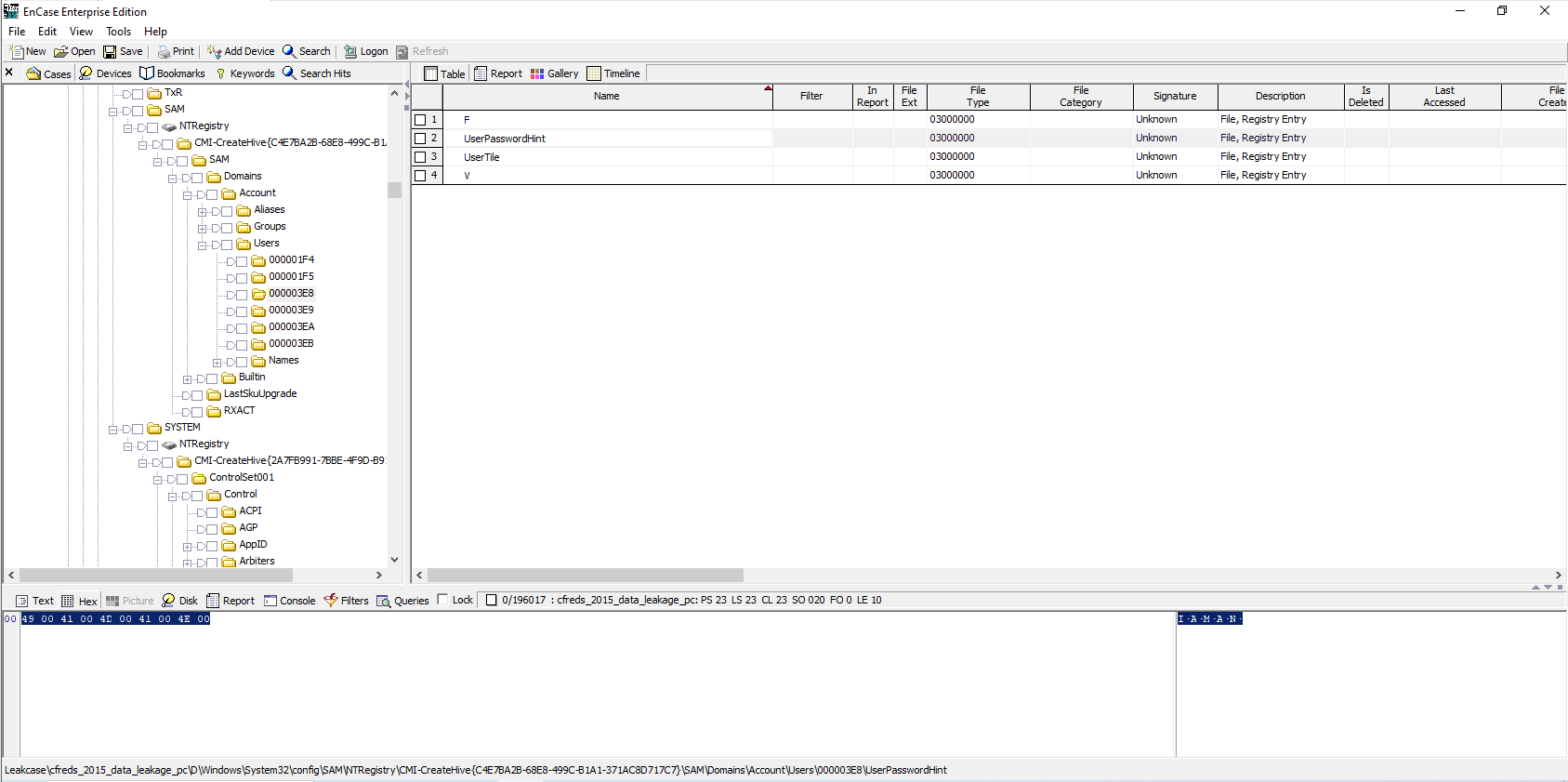
Sau khi xác minh tính toàn vẹn thì bắt đầu phân tích các thiết bị.

Truy cập vô đường dẫn HKLM \SYSTEM\ControlSet###\Control\ComputerName\ComputerName để xem tên của thiết bị là “INFORMANT-PC”.



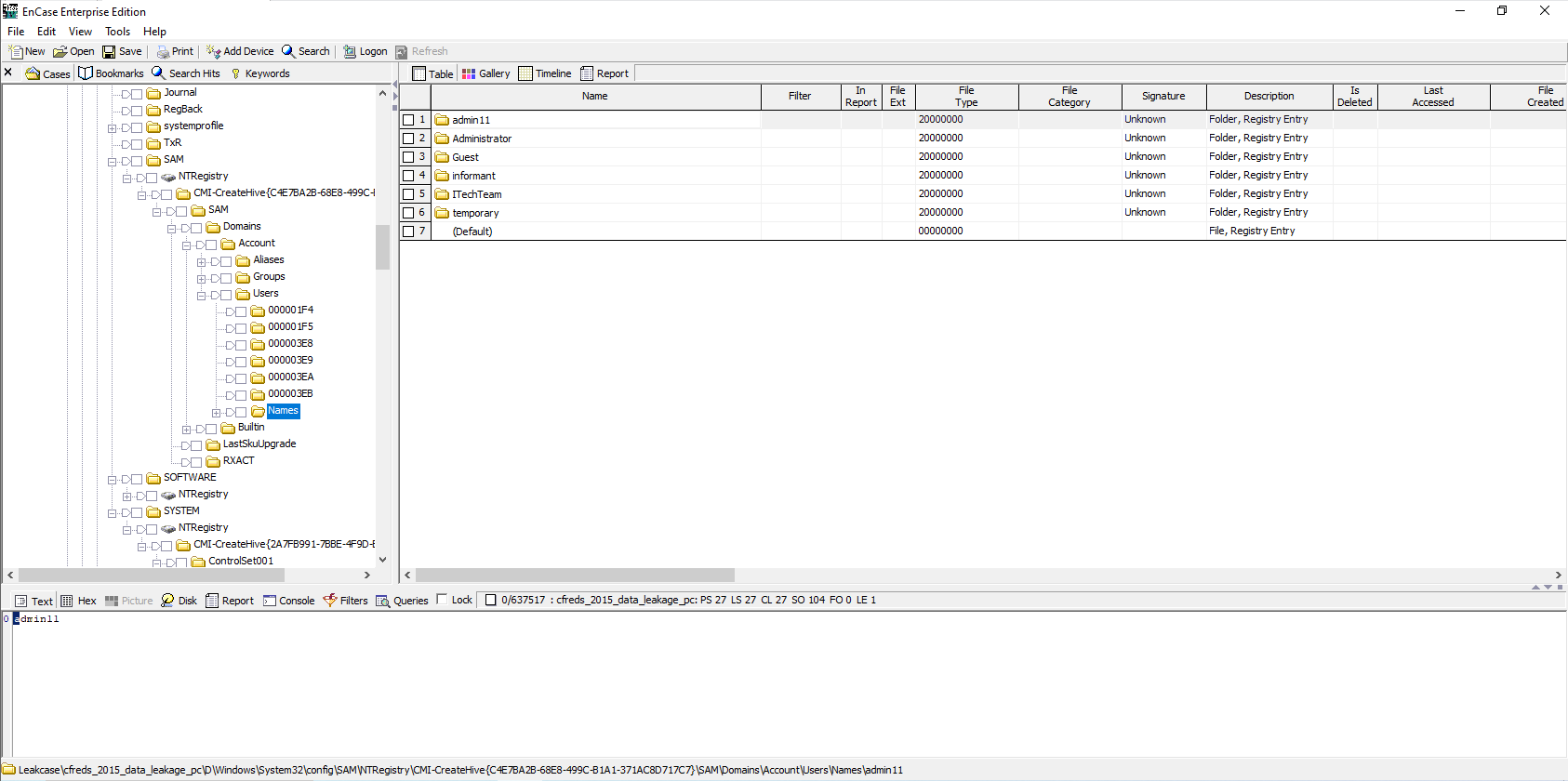
Hình 12. Tên của máy tính

Truy cập vô đường dẫn HKLM \SAM\Domain\Account\Users\000003E8 để có được gợi ý mật khẩu người dùng là “IAMAN”.



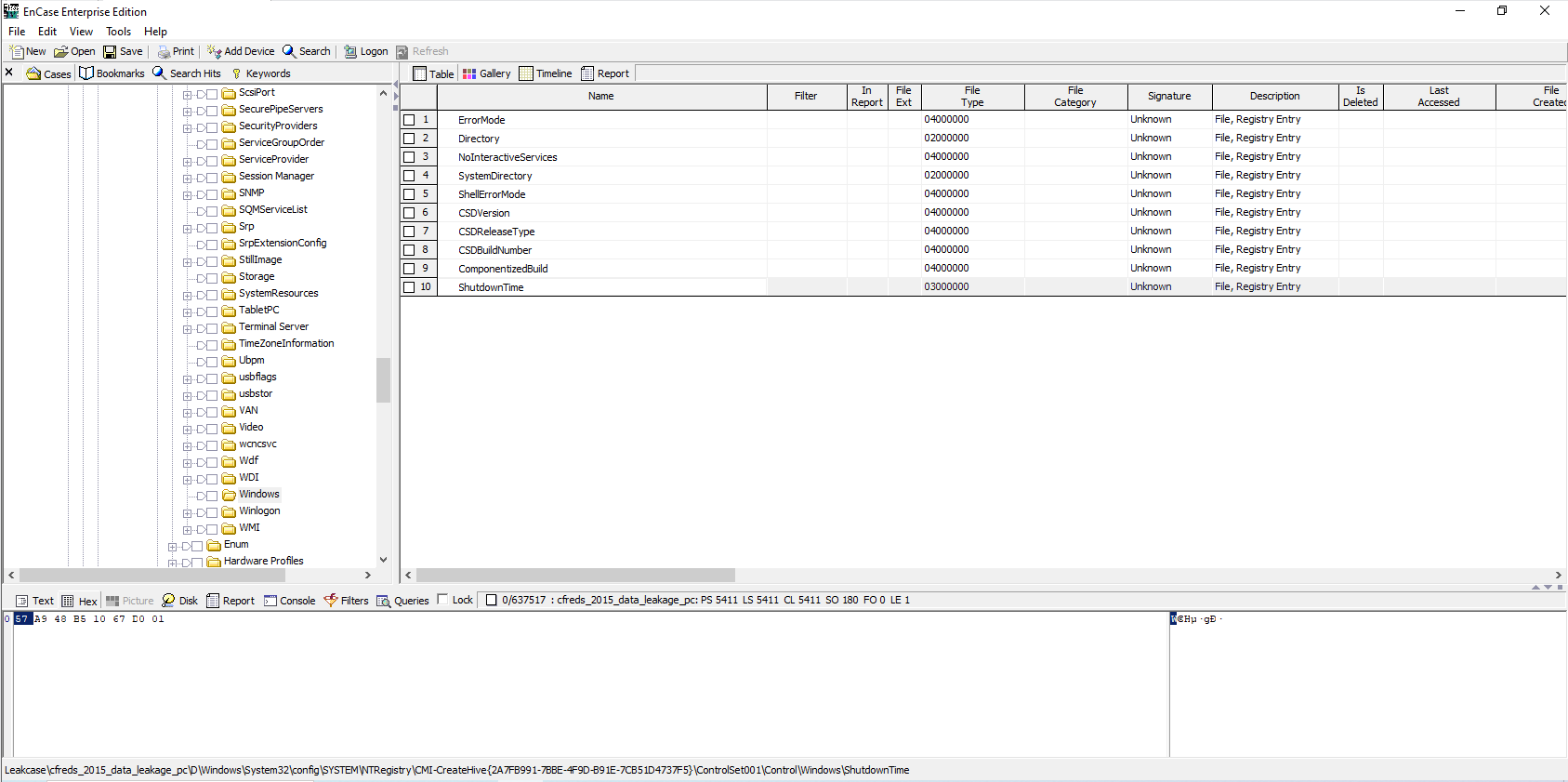
Hình 13. User password hint

Truy cập vô đường dẫn HKLM \SAM\Domain\Account\Users\Names để có được các tài khoản của hệ điều hành.



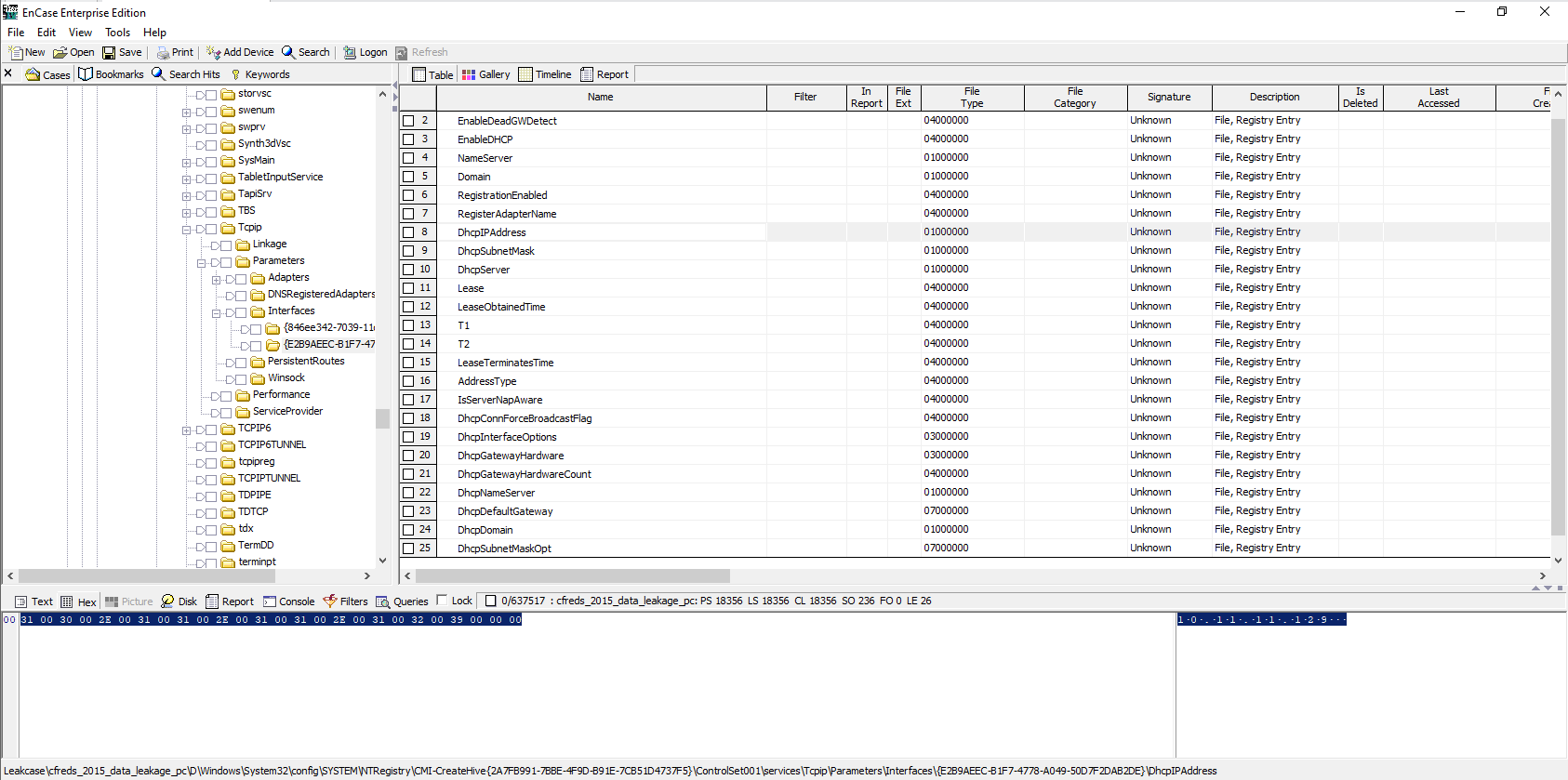
Hình 14. Các tài khoản của hệ điều hành

Truy cập HKLM\SYSTEM\ControlSet###\Control\Windows sẽ thấy được thời gian shutdown. Nhưng do Encase nhóm em sử dụng đang ở phiên bản cũ nên vẫn chưa có chức năng Decode vì vậy không thể thấy tường minh được thời gian.



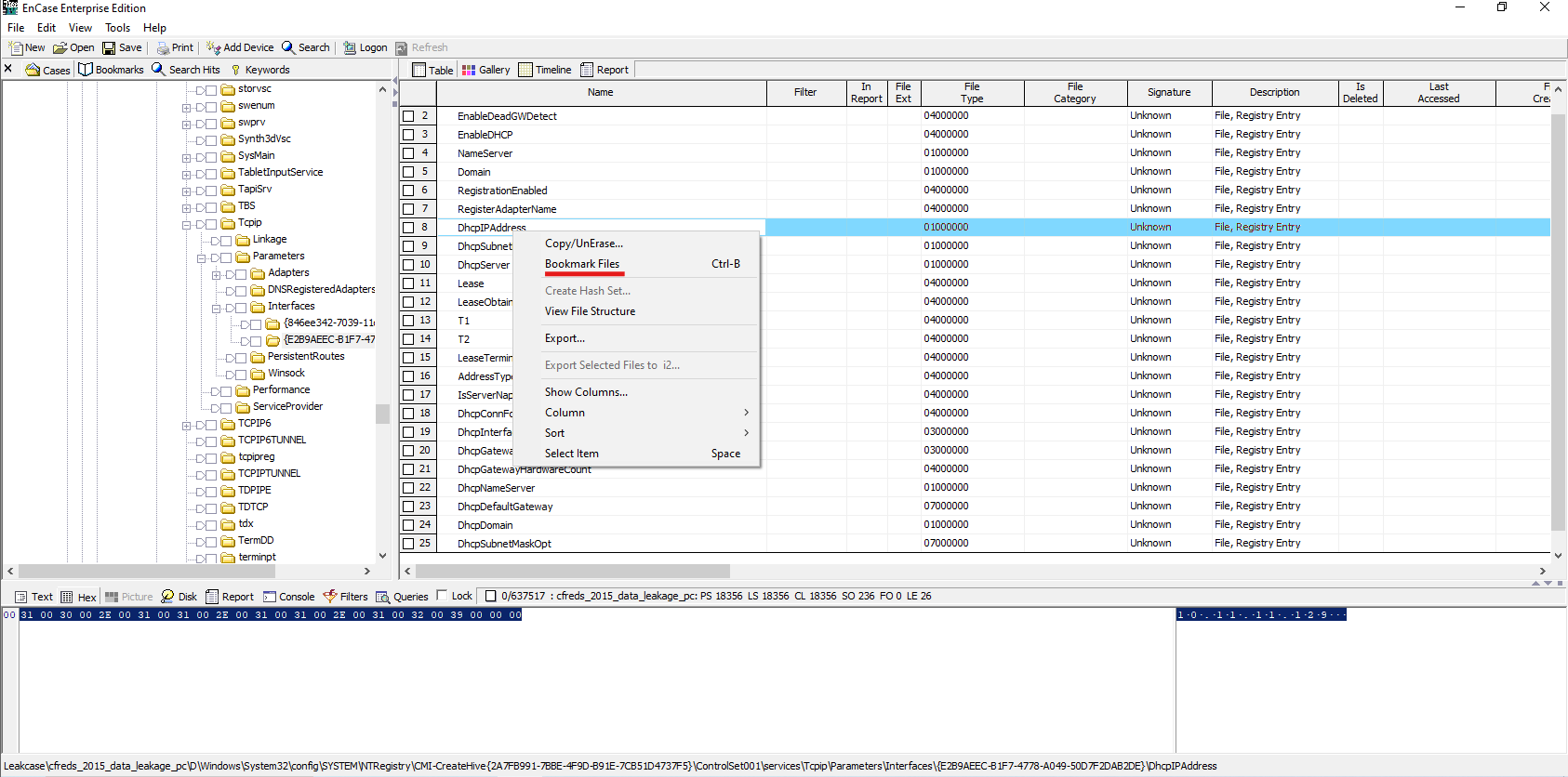
Hình 15. Shutdown time

Truy cập HKLM\SYSTEM\ControlSet###\Services\Tcpip\Parameters\Interfaces\ để lấy thông tin của network interface

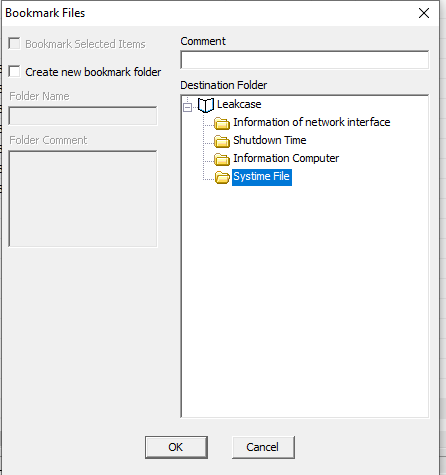


Hình 16. Thông tin của network interface

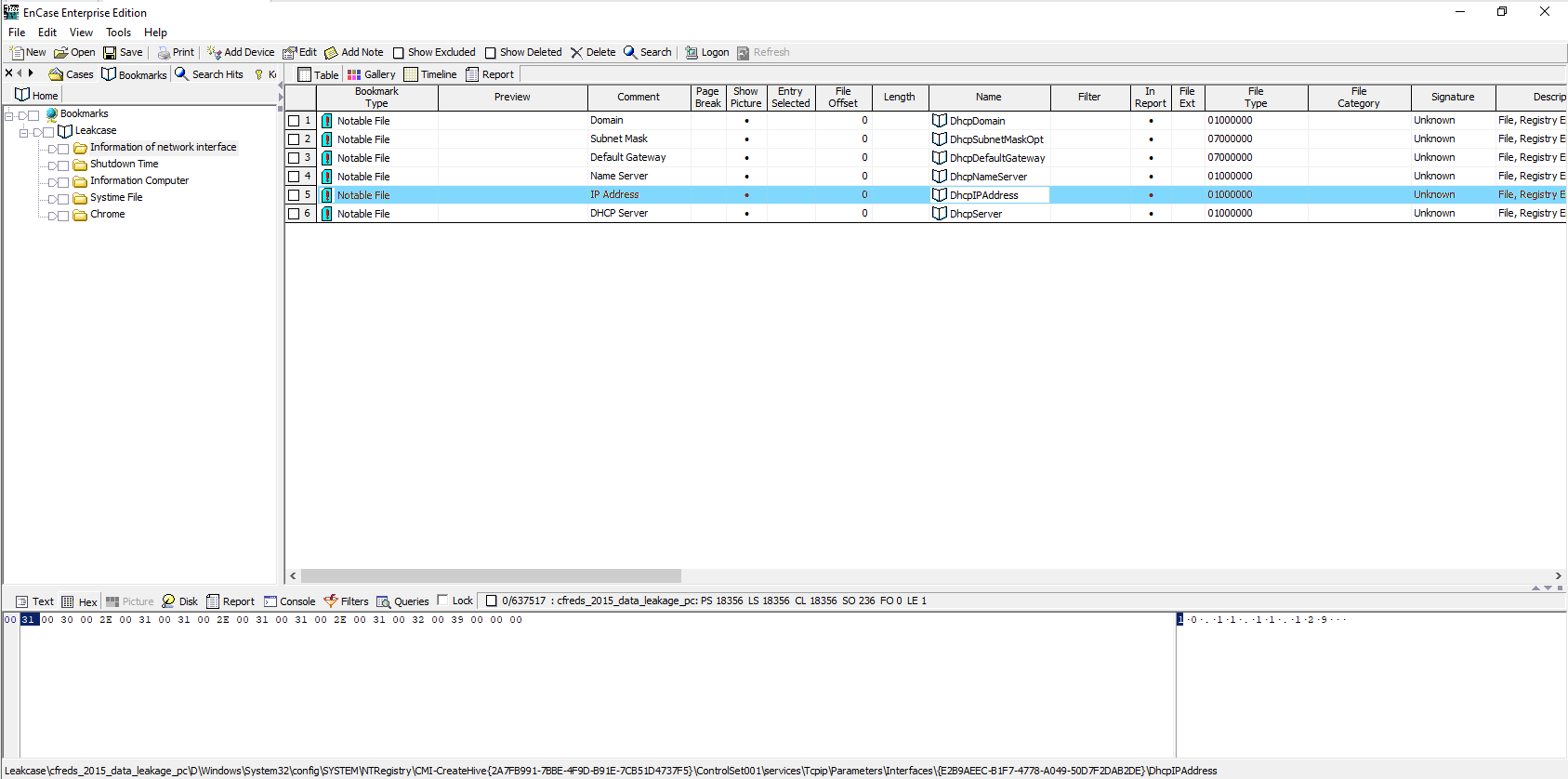
Muốn đánh dấu các tệp quan trọng đã tìm được thì chọn vô tệp muốn đánh dấu => Click chuột phải chọn Bookmark Files (hoặc nhấn Ctrl + B) => Cấu hình nơi lưu tệp được đánh dấu.



Hình 17. Thực hiện đánh dấu tệp

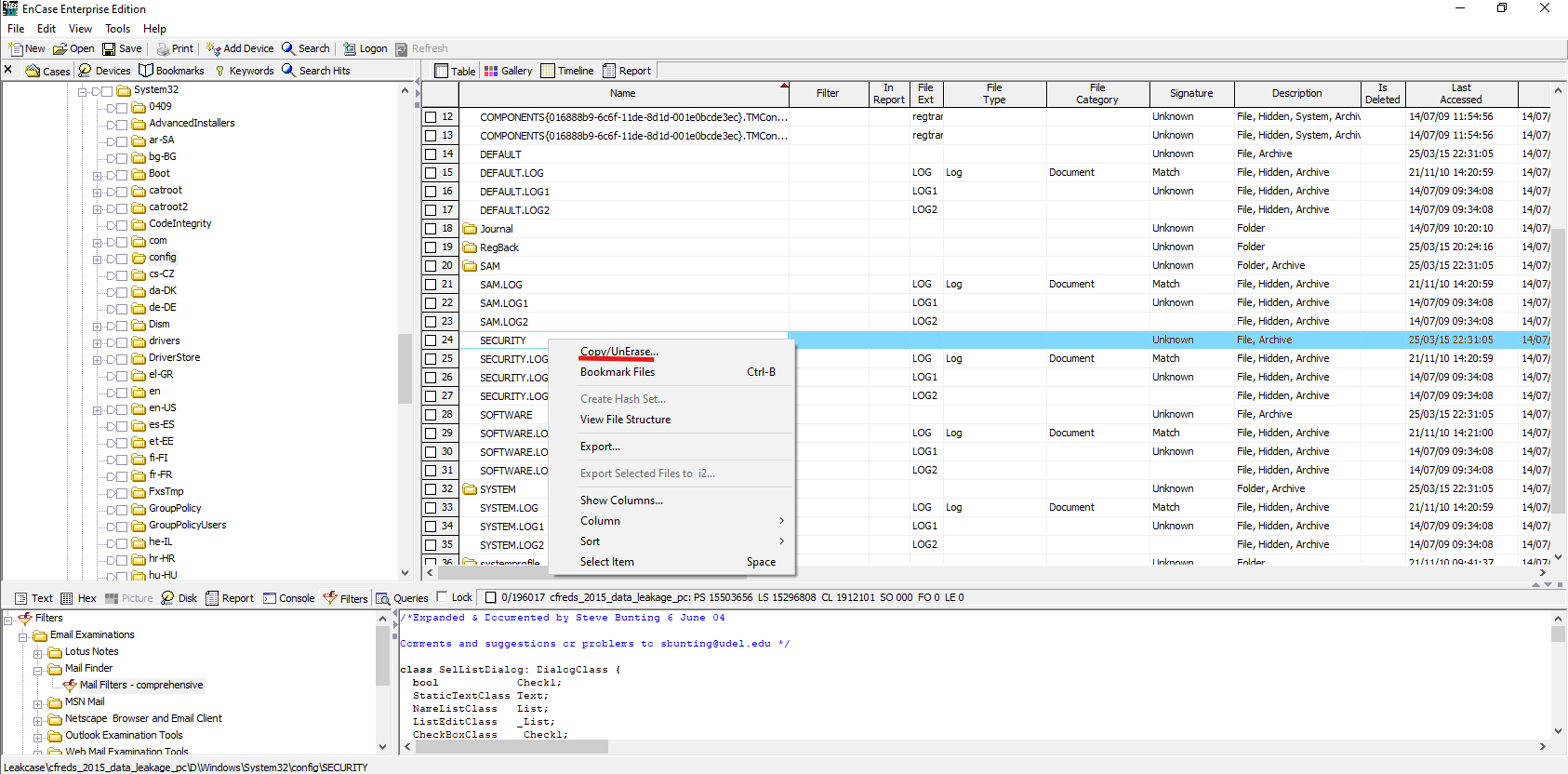


Hình 18. Cấu hình nơi lưu đánh dấu

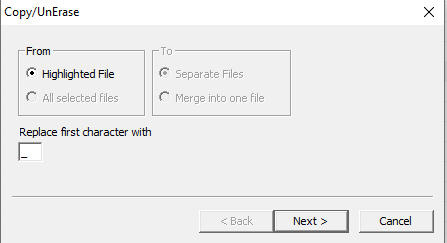


Hình 19. Kết quả của đánh dấu tệp

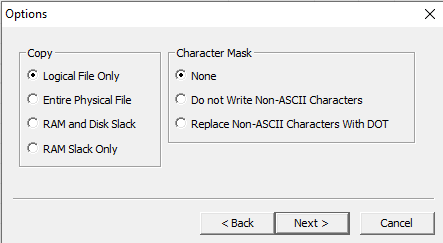
Để sao chép các tệp ra bên ngoài thì có thể Click chuột phải chọn Copy/ UnErase rồi cấu hình cho file copy để hoàn thành.



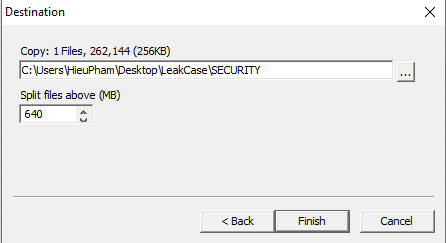
Hình 20. Sao chép các tệp ra ngoài



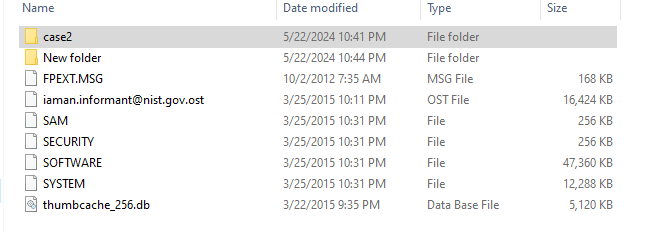
Hình 21. Copy/UnErase



Hình 22. Cấu hình

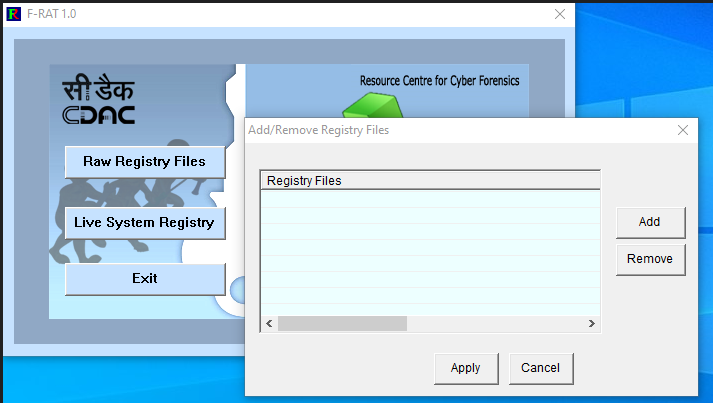


Hình 23. Destination

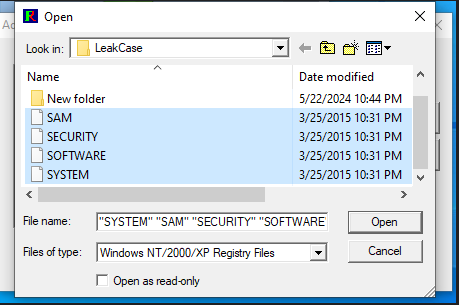


Hình 24. Kết quả sau khi copy

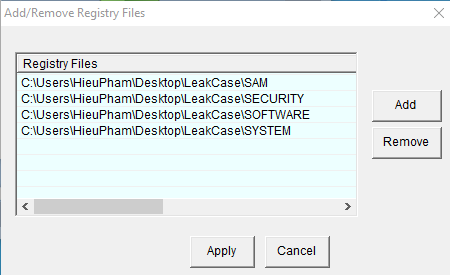
Do nhóm em chỉ xài Encase phiên bản cũ nên còn rất nhiều hạn chế như chưa thể Decode file vì vậy để có thể Decode thì nhóm em có sử dụng công cụ F-RAT để có thể có cái nhìn trực quan hơn trong việc phân tích.



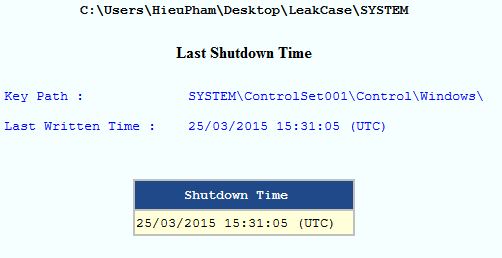
Hình 25. Giao diện F-RAT



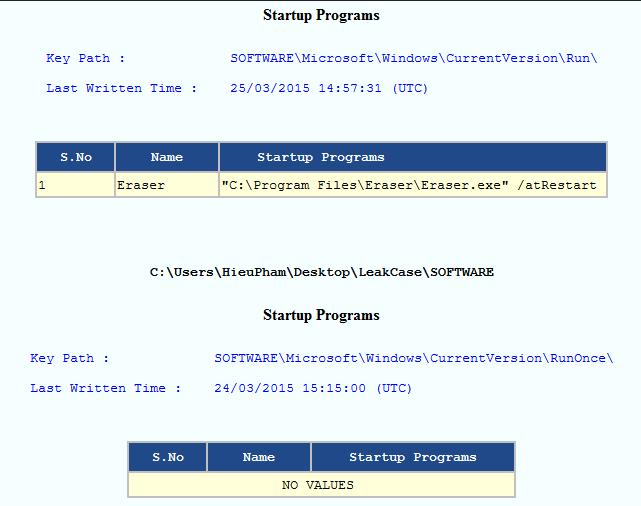
Hình 26. Thêm các file system



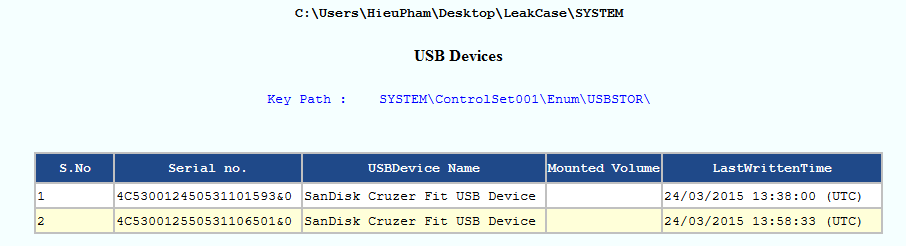
Hình 27. Apply để hoàn thành



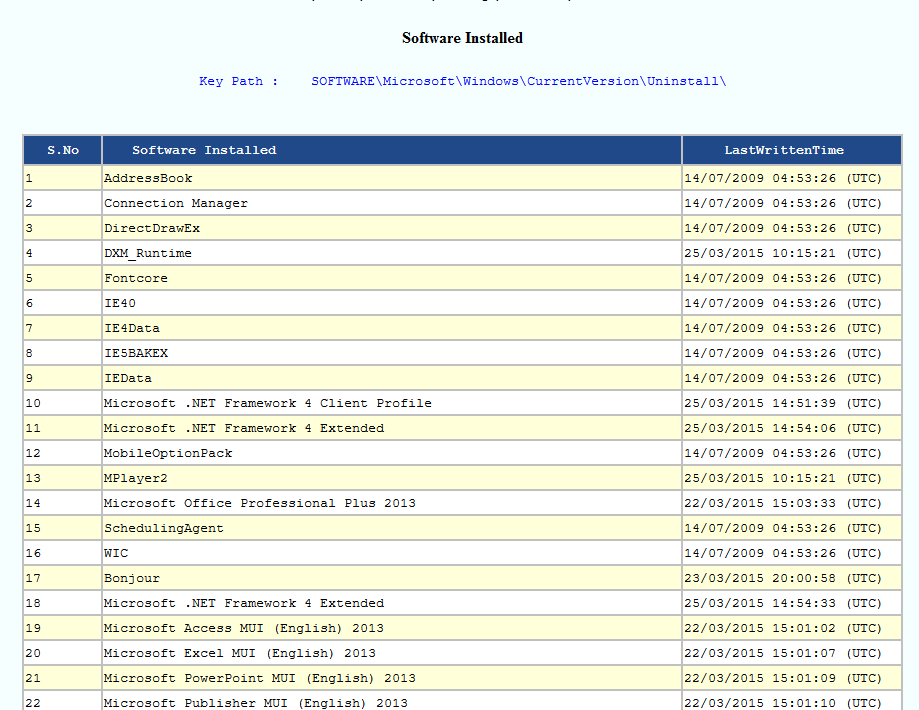
Hình 28. Last Shutdown Time



Hình 29. Startup Programs



Hình 30. USB Devices

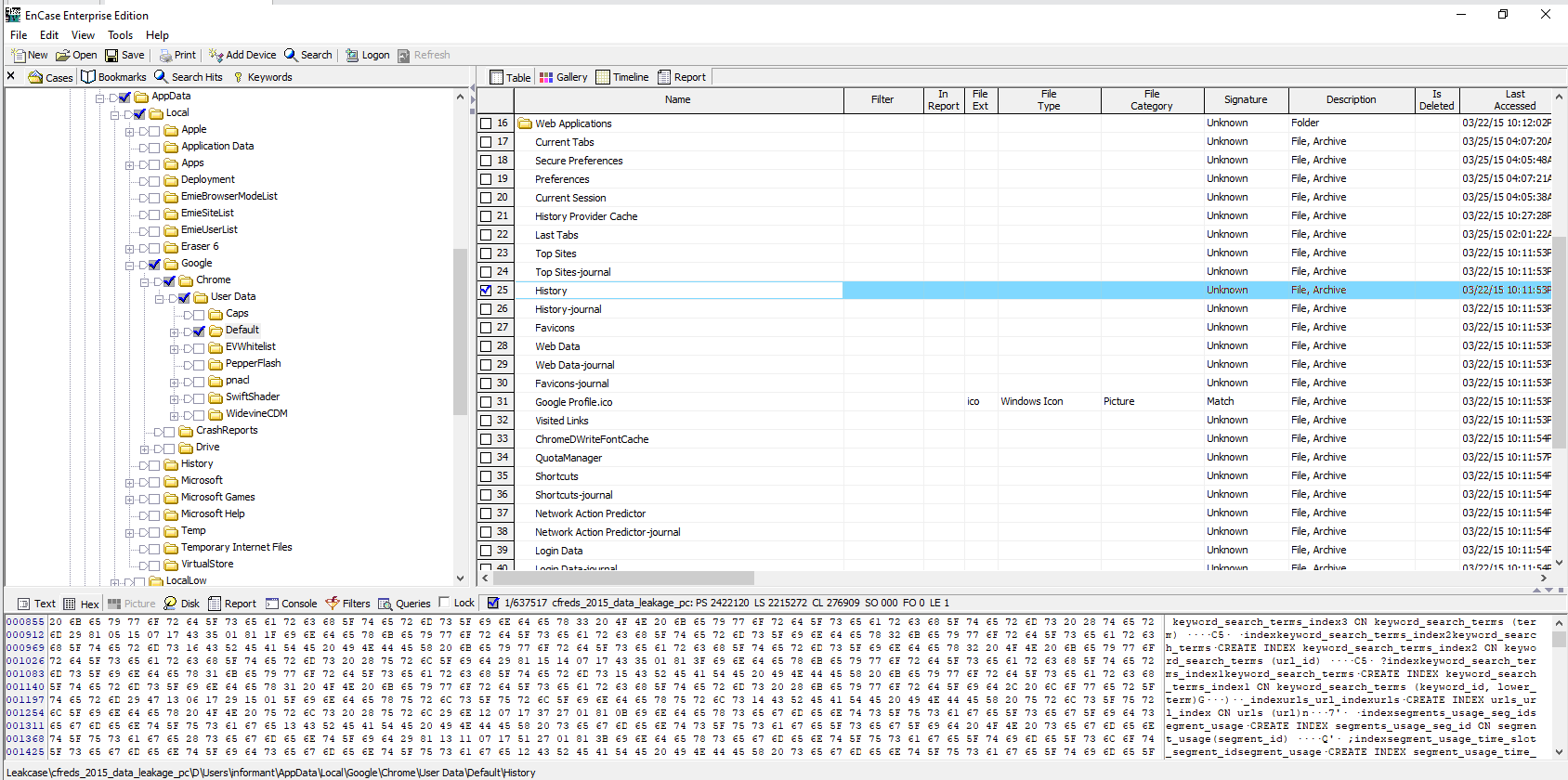


Hình 31. Software Installed

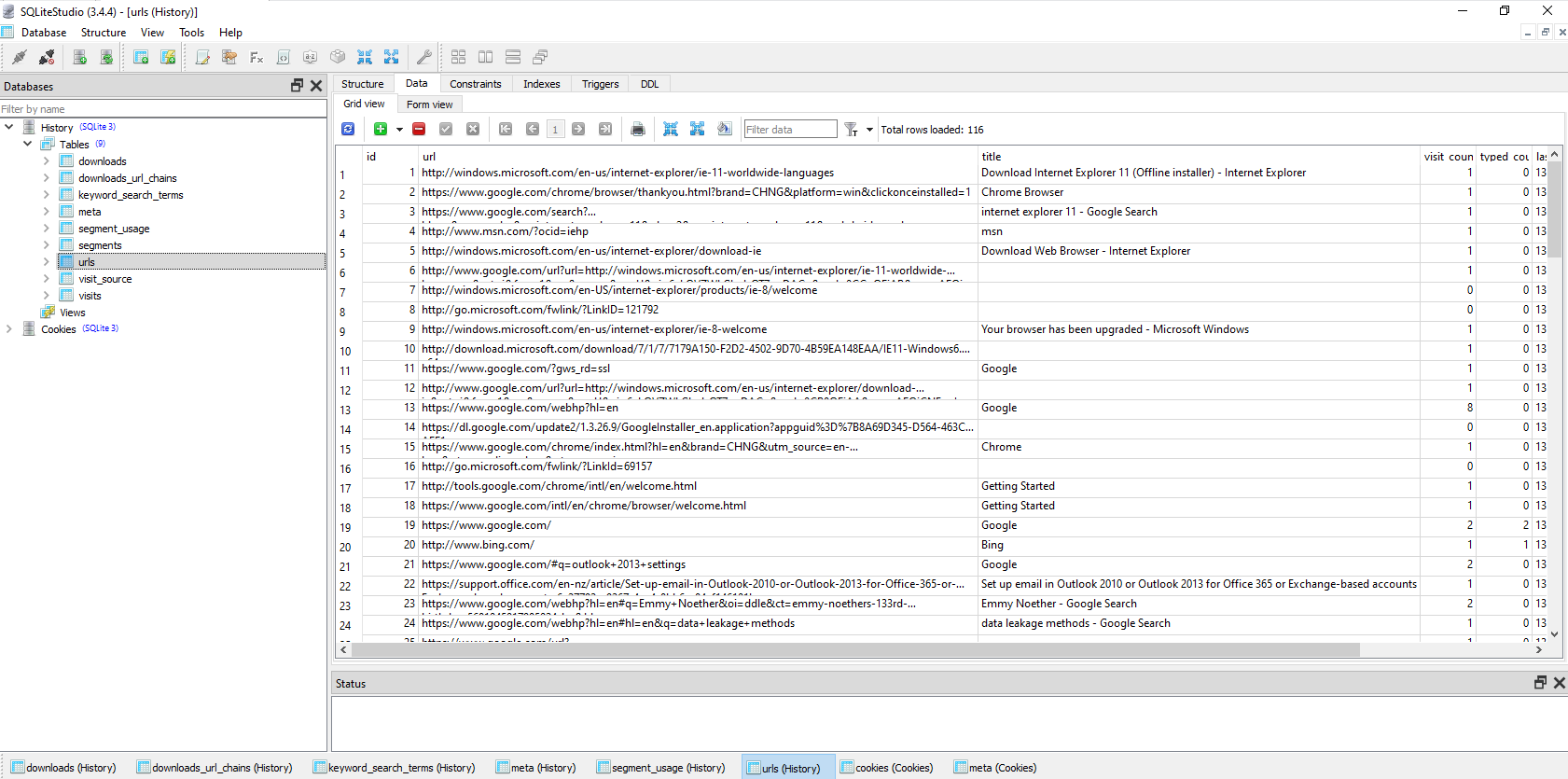


Hình 32. Software Install

Để có thể lấy được file lịch sử duyệt web của Google thì có thể truy cập đường dẫn C:\Users\informant\AppData\Local\Google\Chrome\User Data\Default\History sau đó Copy file ra ngoài rồi dùng công cụ SQLiteStudio để xem được file.



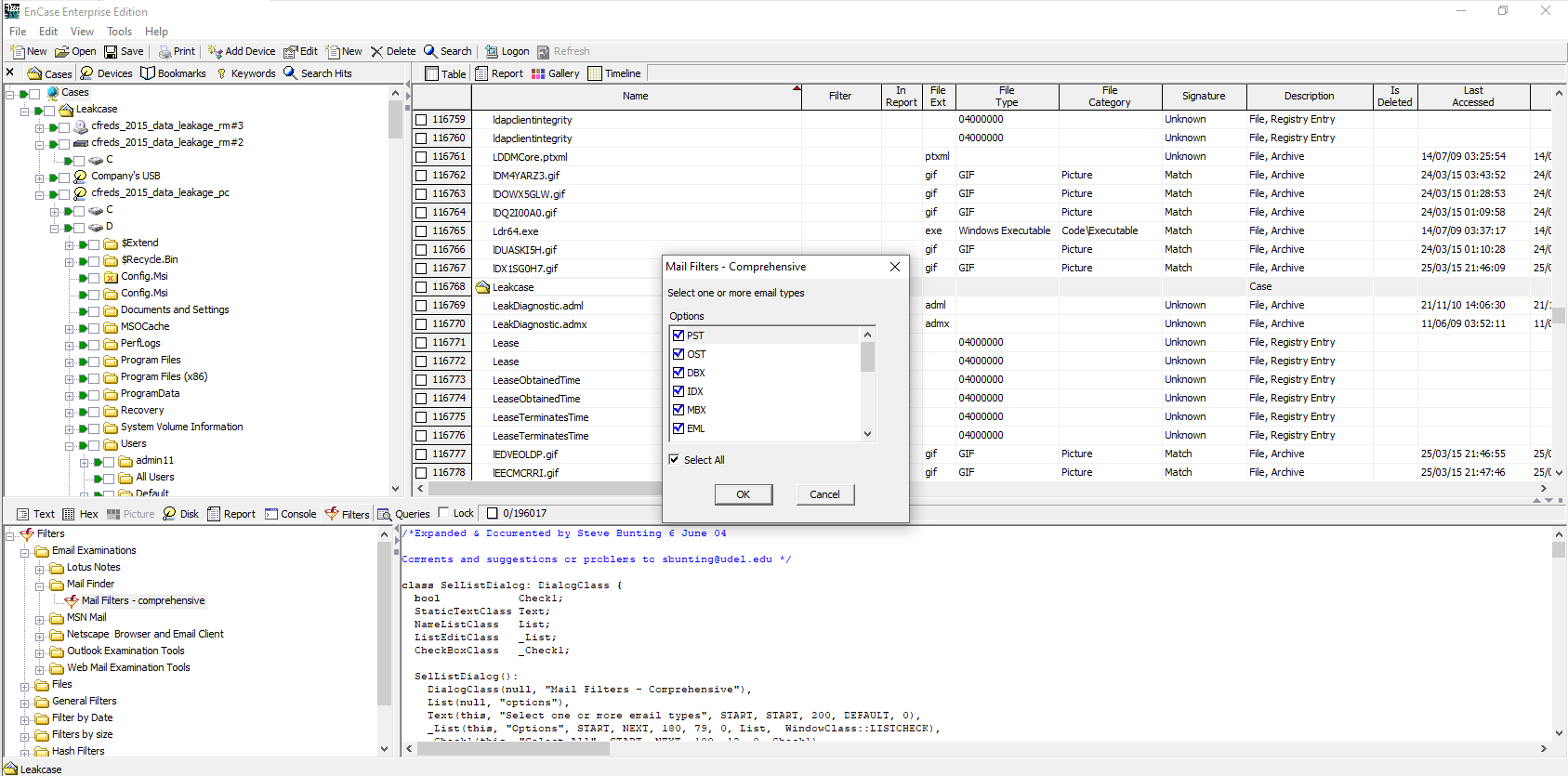
Hình 33. Lịch sử của trình duyệt Google



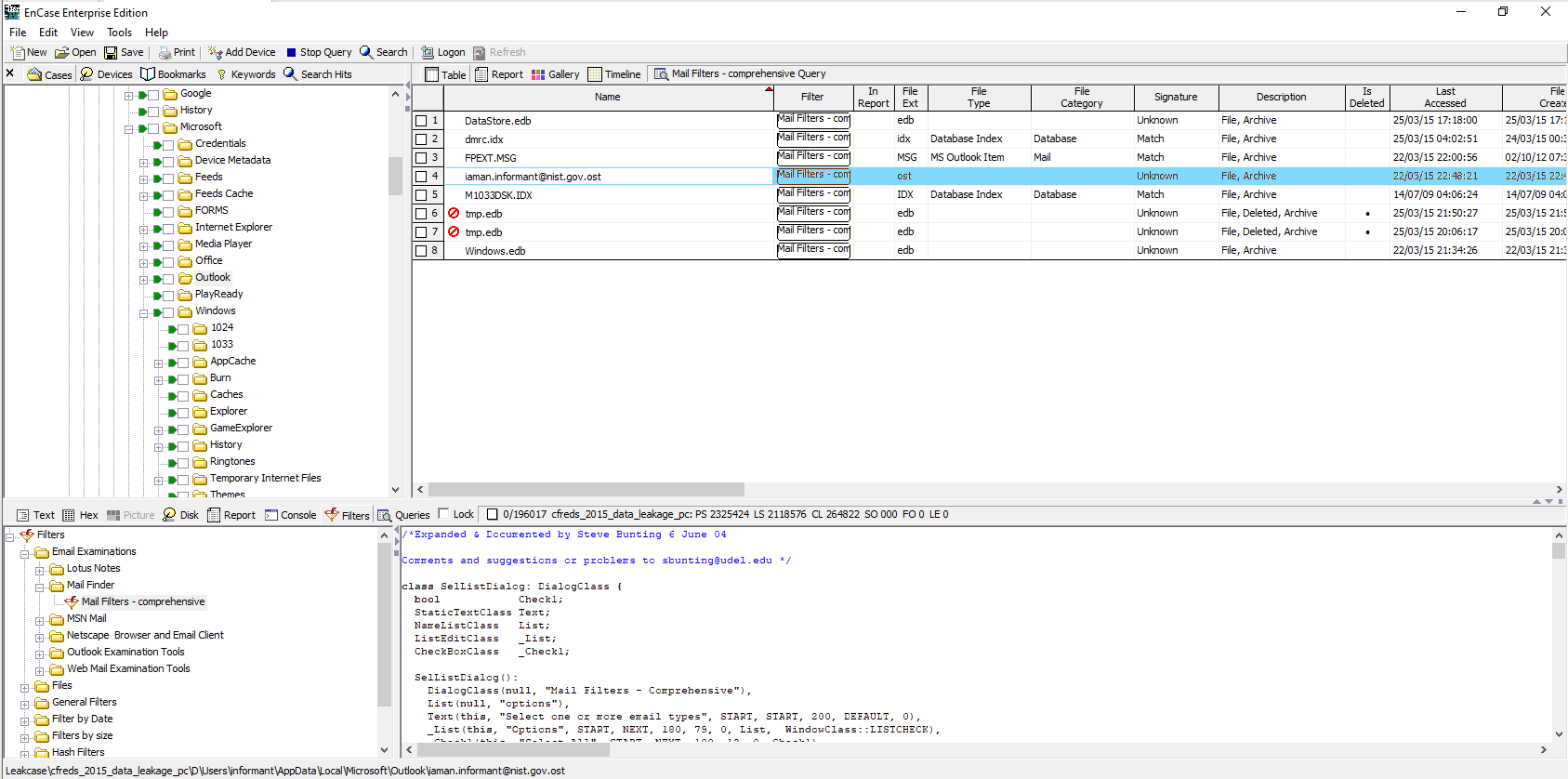
Hình 34. Đường dẫn lịch sử duyệt web

Tiếp theo dùng Filters để lọc các tệp trò chuyện mail.

Chọn Filters => Chọn Email Examinations => Chọn Mail Finder => Chọn loại tệp email muốn lọc => Click OK để hoàn thành.



Hình 35. Lọc các tệp trò chuyện mail

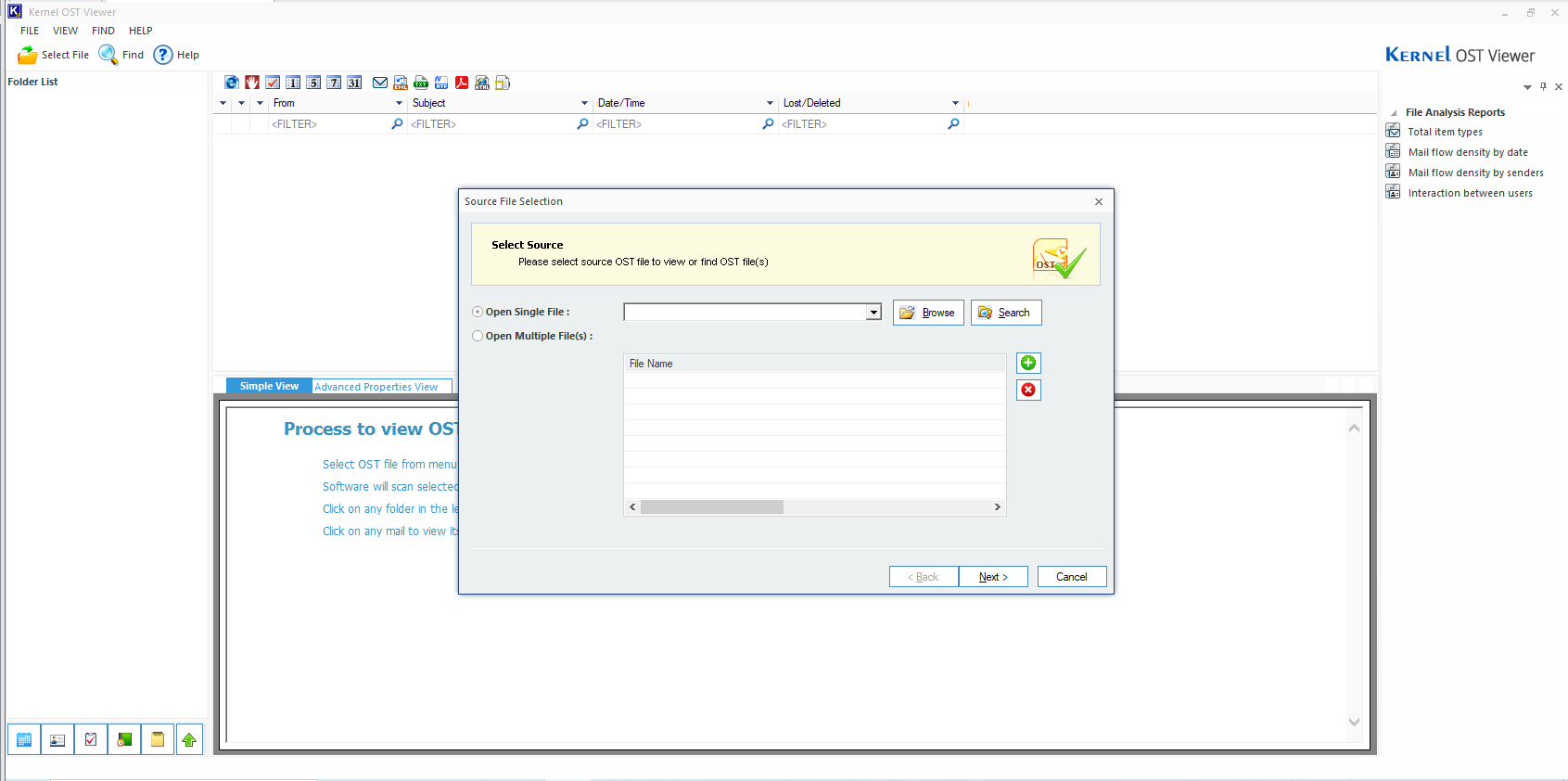


Hình 36. Kết quả lọc

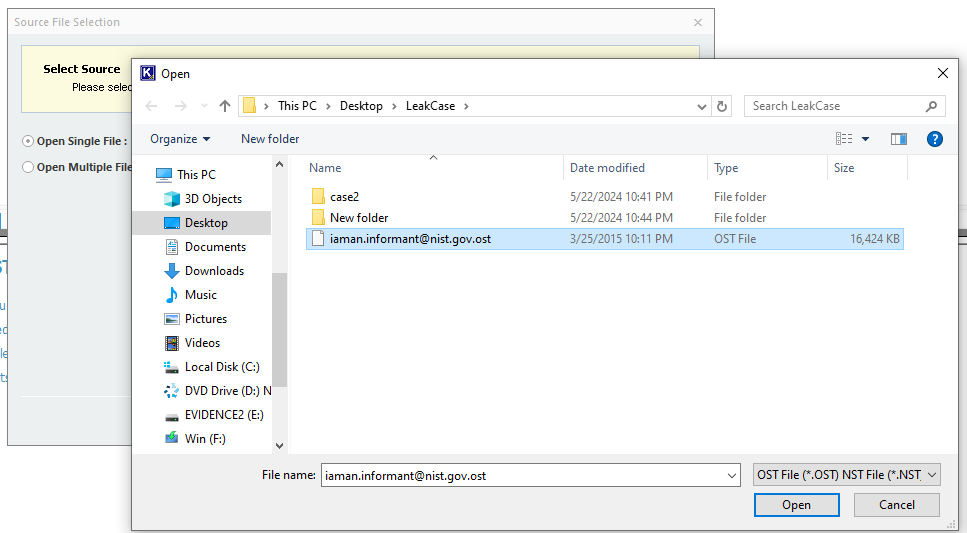
Sau khi lọc thì ta có được các file, nhưng nhìn vào thì chỉ cần chú ý đến file [iaman.informant@nist.gov.ost](mailto:iaman.informant@nist.gov.ost).

Tệp .ost là viết tắt của Offline Storage Table (Bảng Lưu trữ Ngoại tuyến), một định dạng tệp được sử dụng bởi Microsoft Outlook để lưu trữ một bản sao cục bộ của dữ liệu hộp thư từ máy chủ Microsoft Exchange. Tệp này cho phép người dùng truy cập email, lịch, danh bạ và các mục khác ngay cả khi không có kết nối internet. Khi kết nối được thiết lập lại, tệp .ost sẽ tự động đồng bộ hóa với máy chủ Exchange.

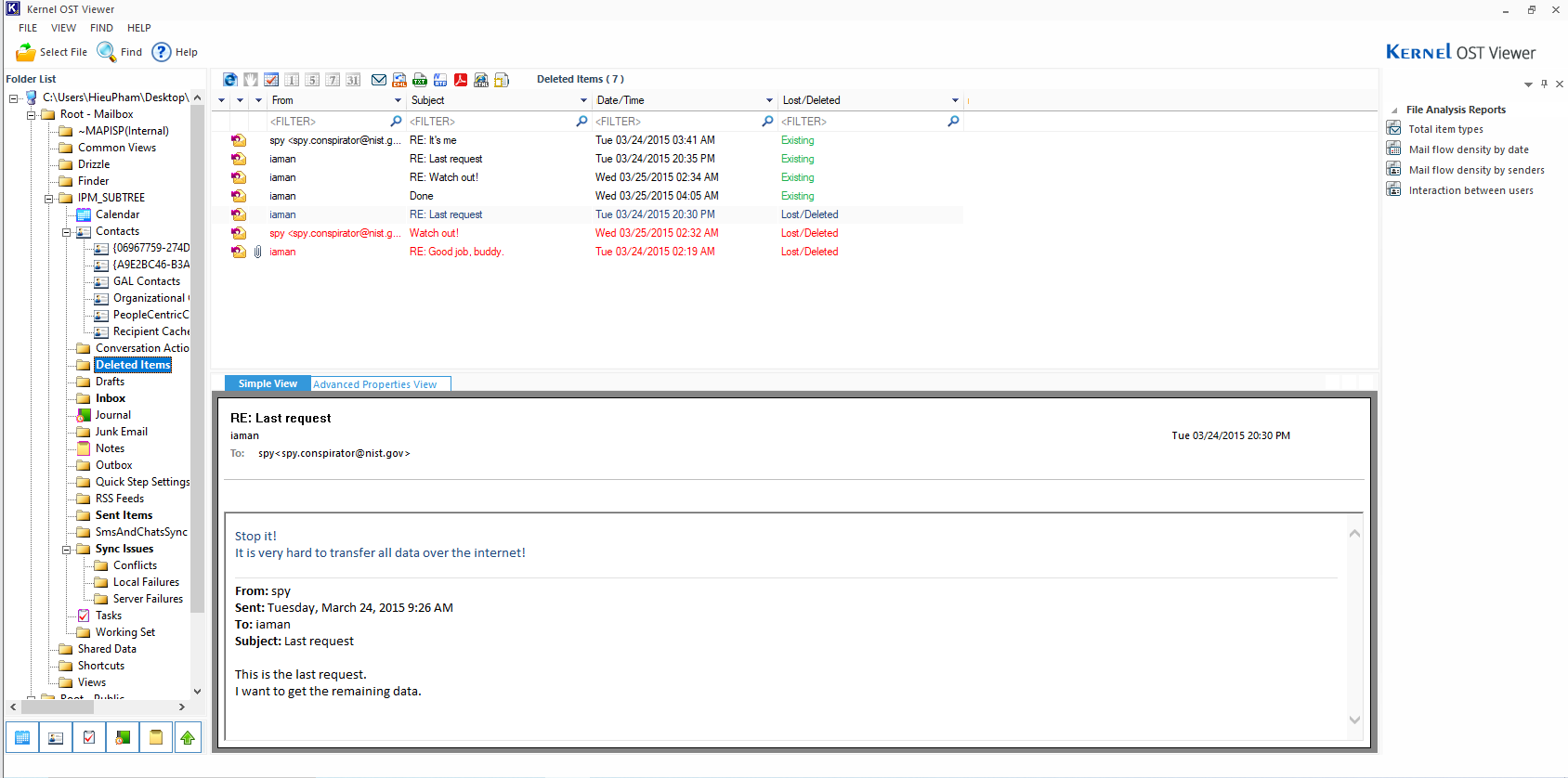
Để đọc được file này thì nhóm em dùng công cụ Kernel OST Viewer để có thể đọc được file.



Hình 37. Kernel OST Viewer

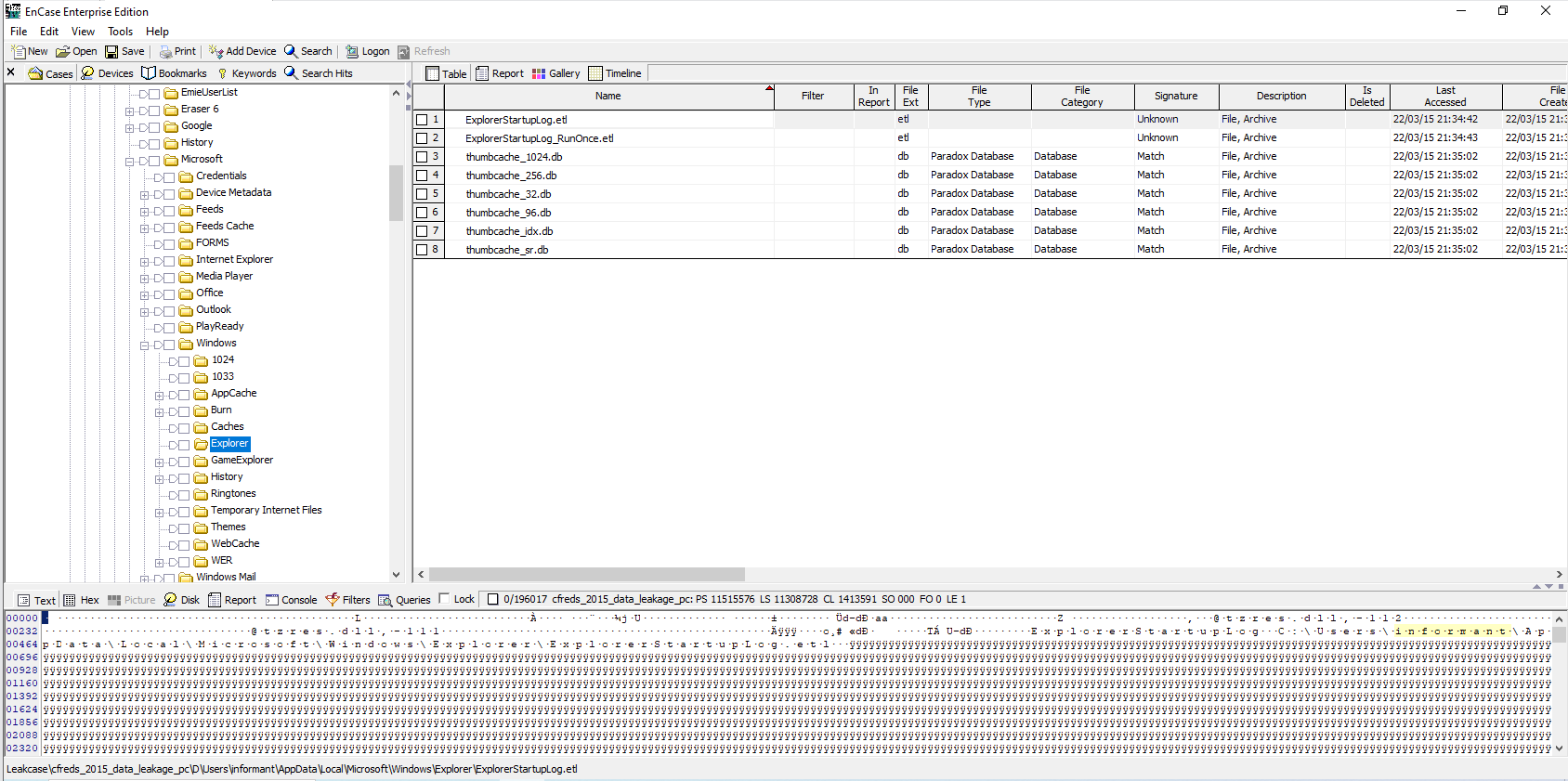


Hình 38. Thêm file ost



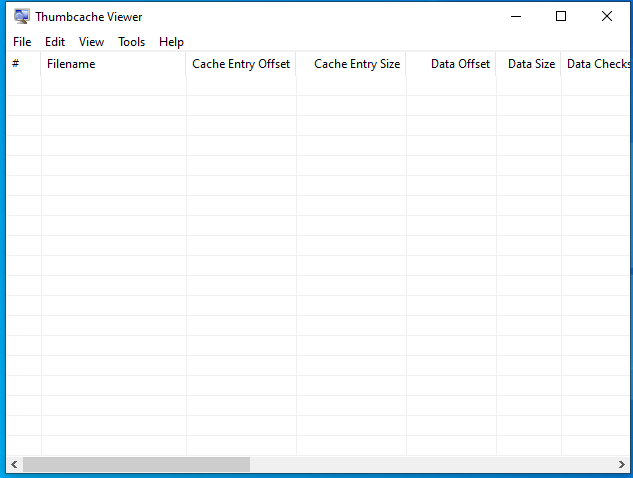
Hình 39. Lịch sử trò chuyện

Truy cập \Users\informant\AppData\Local\Microsoft\Windows\Explorer\ để lấy được các file Thumbcache.

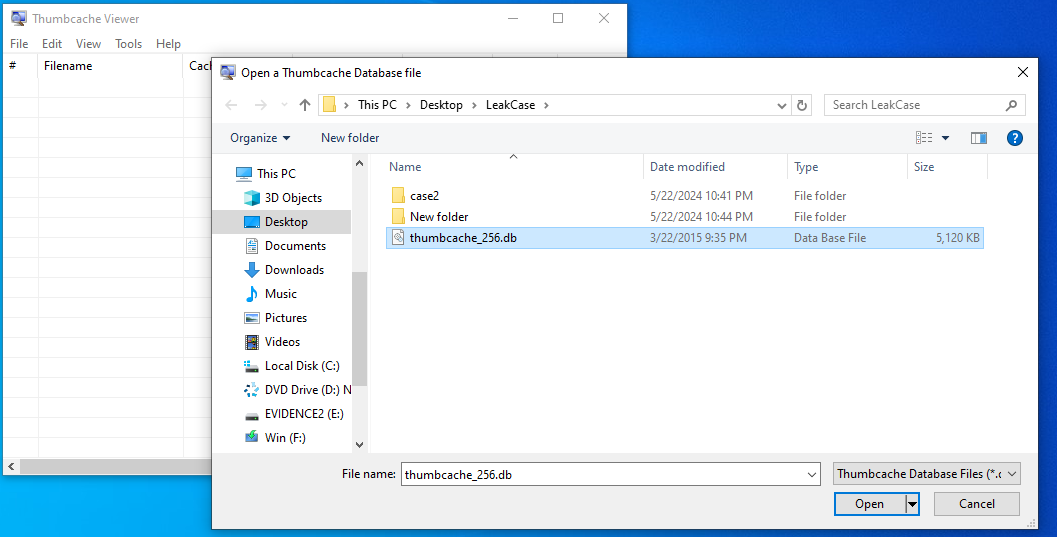


Hình 40. Thumbcache file

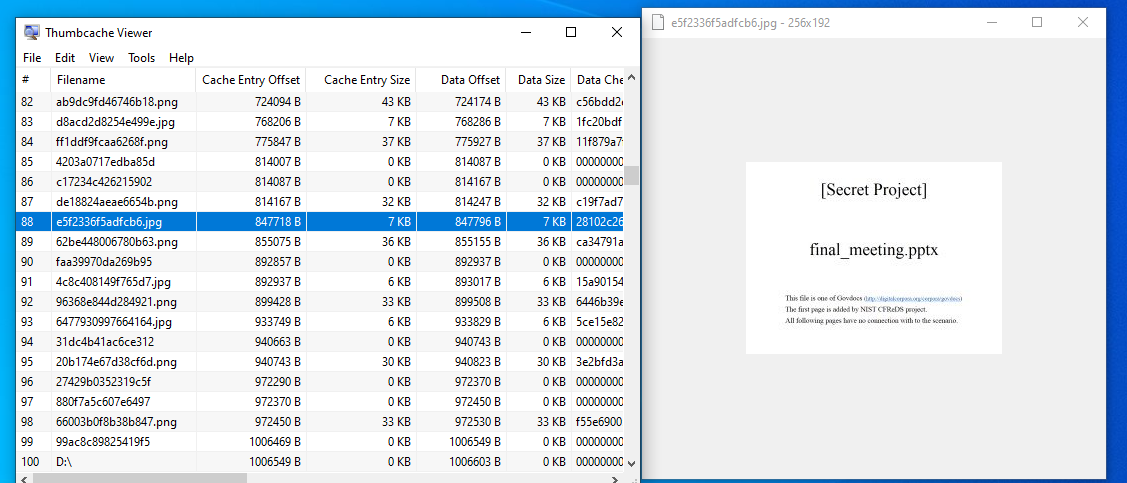
Sau khi lấy được file thì có thể dùng Thumbcache Viewer để xem được trực quan file.



Hình 41. Thumbcache Viewer

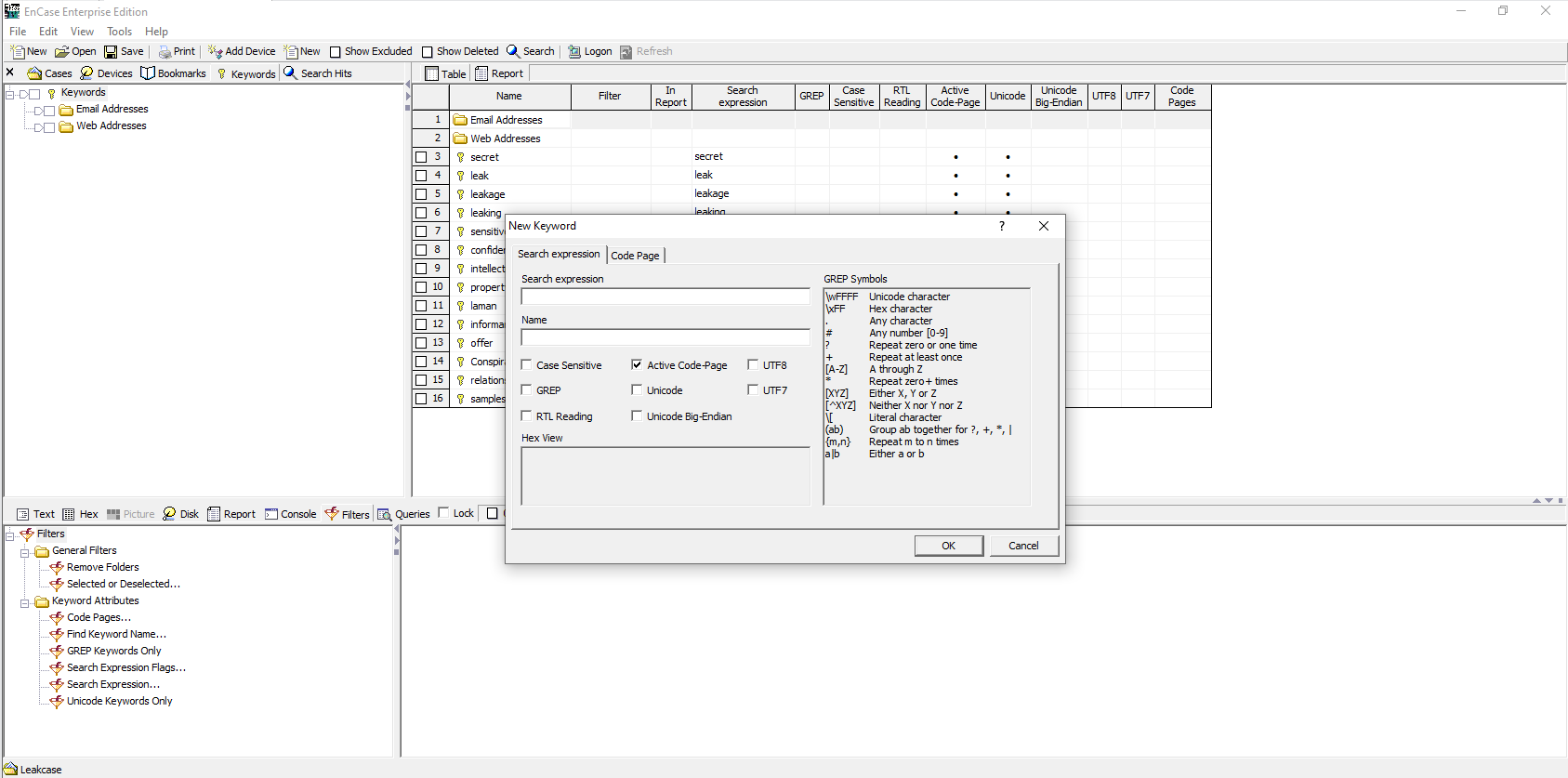


Hình 42. Thêm file thumbcache

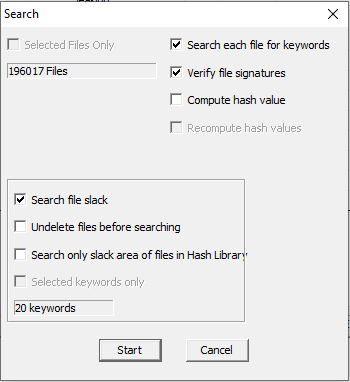


Hình 43. Kết quả tìm được

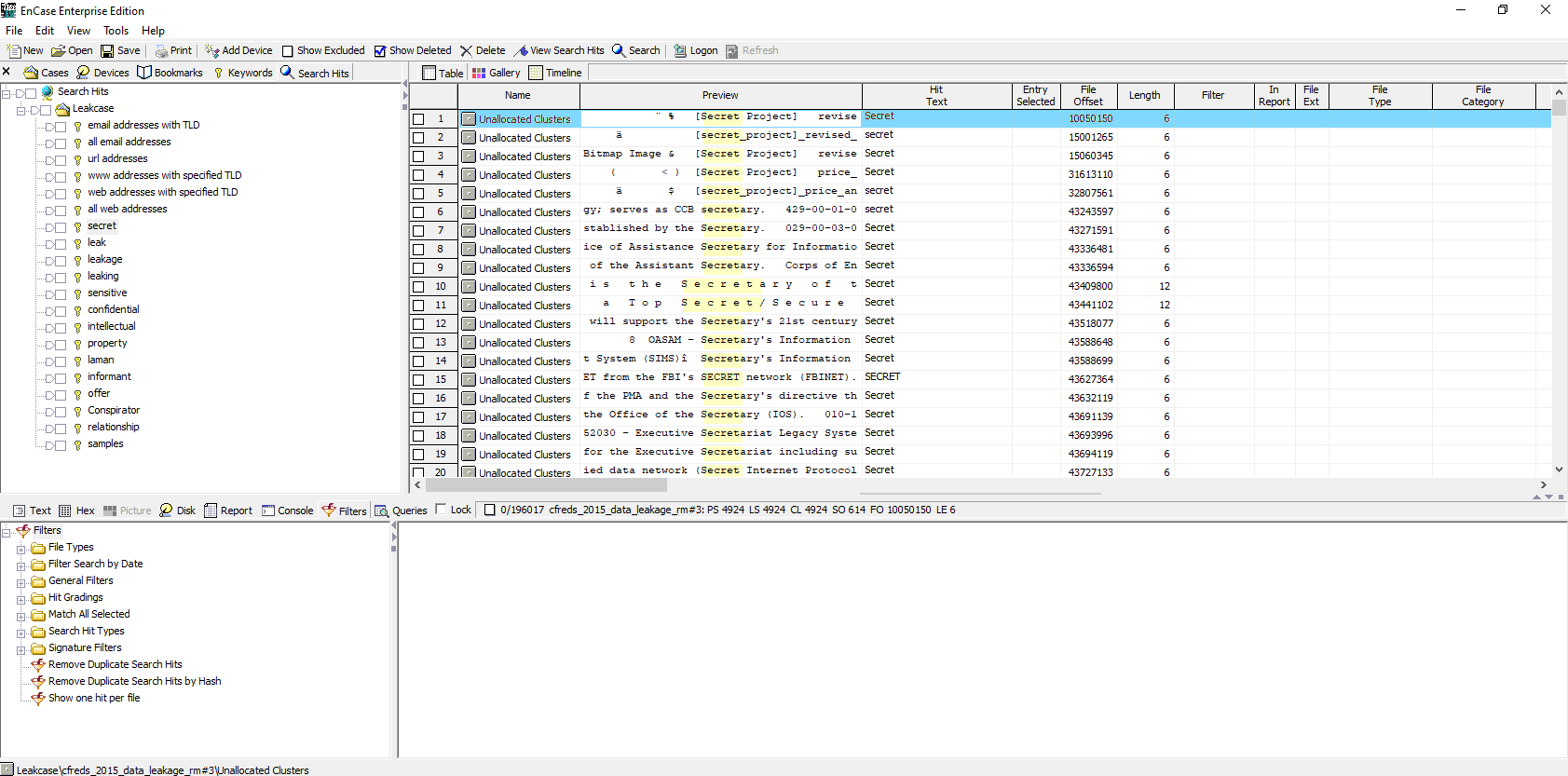
Dựa vào các từ khóa tìm của lịch sử google, các từ khóa của ảnh chụp màn hình lấy được từ việc xem file thumbcache và các từ khóa tổng hợp từ các file tìm kiếm được thì có thể dựa vào đó và tạo ra các keyword để tìm giúp tìm kiếm các file bị tiết lộ.



Hình 44. Tạo keyword mới



Hình 45. Tiến hành tìm kiếm dựa trên key word



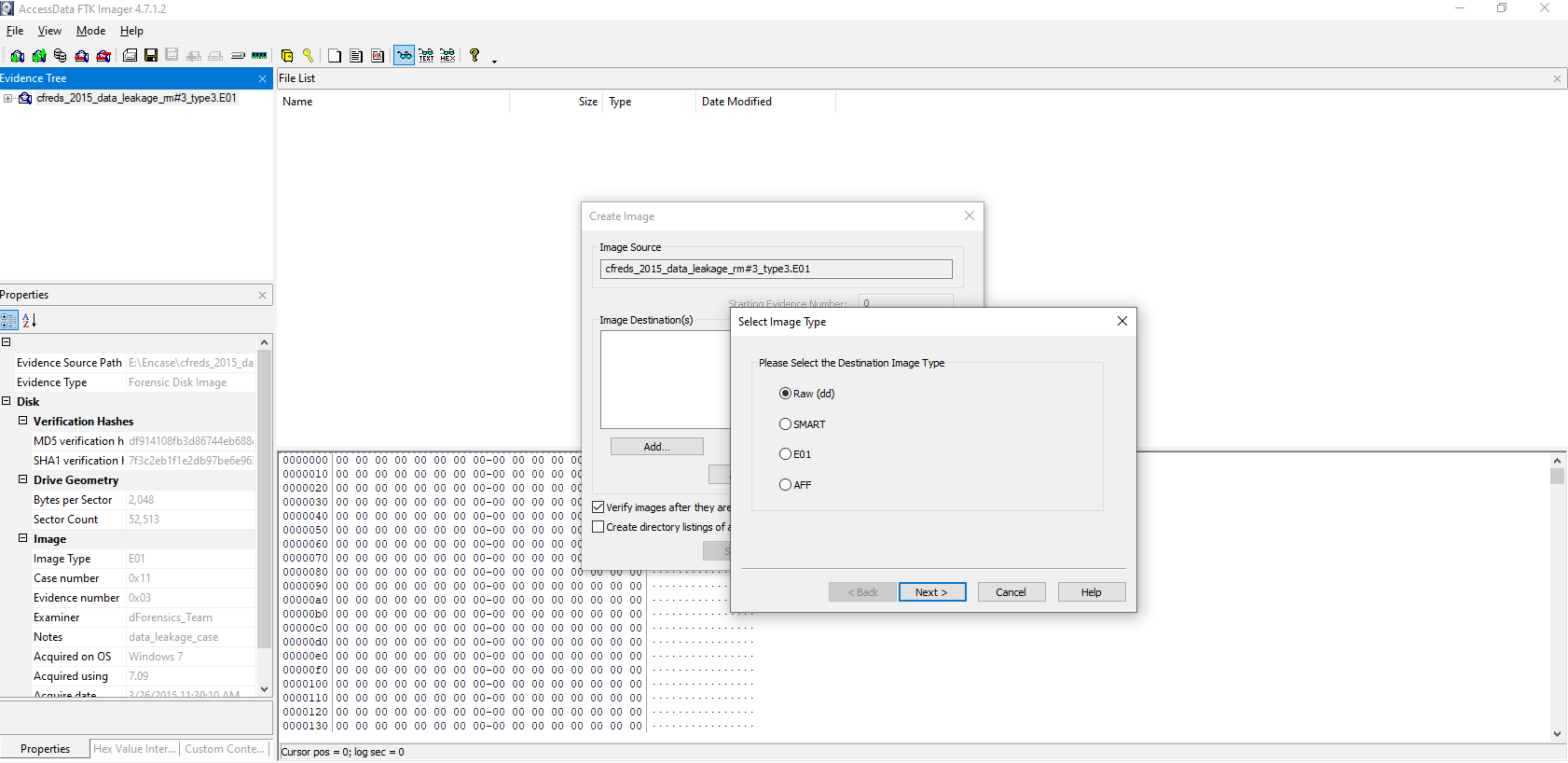
Hình 46. Kết quả tìm kiếm

Sau khi tìm kiếm thì có thể thấy được các file đã bị xóa và nằm trong unallocated clusters.

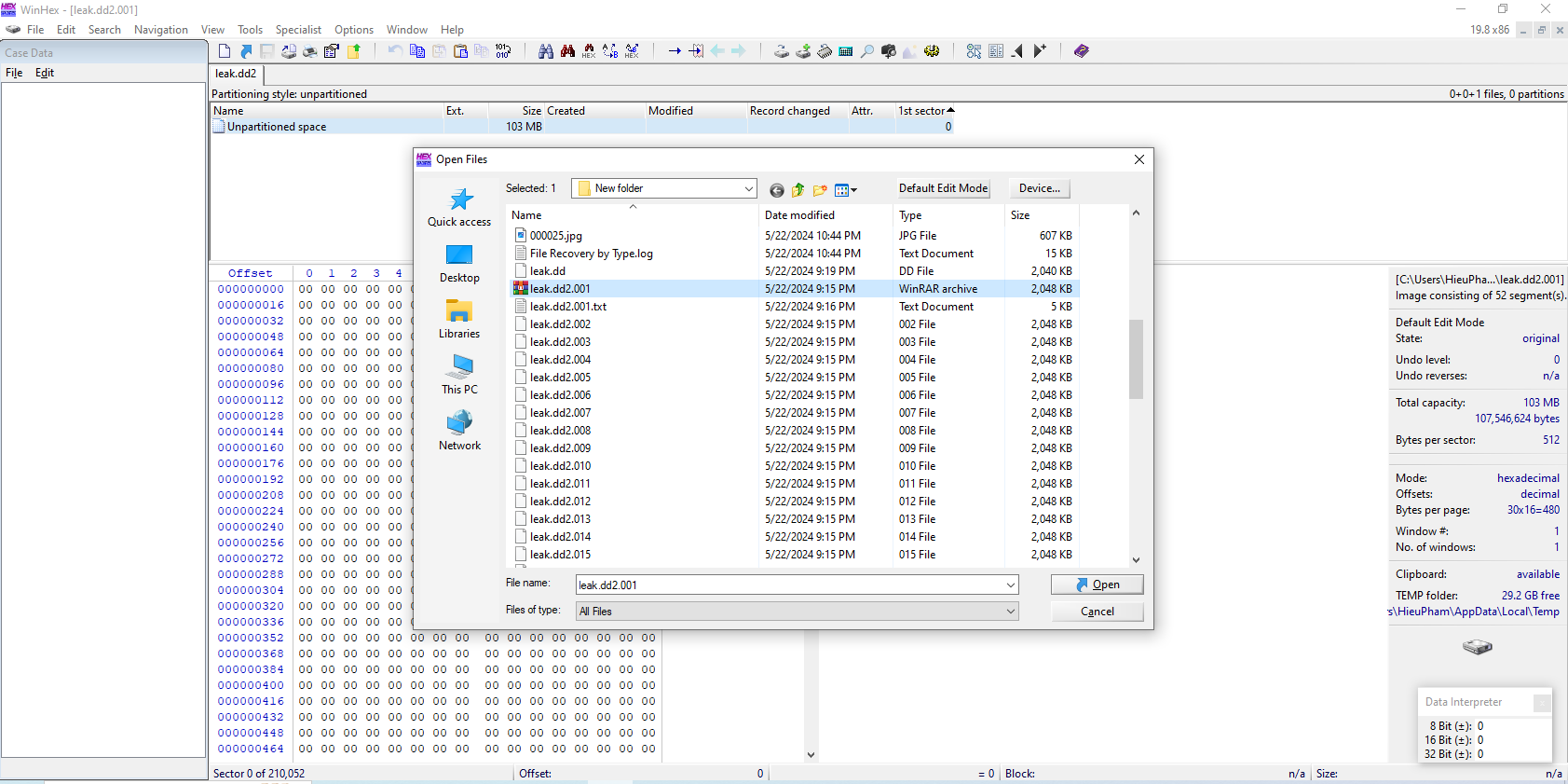
Unallocated clusters là những clusters (cụm) trên ổ đĩa không được hệ điều hành sử dụng để lưu trữ dữ liệu của tệp. Khi một tệp bị xóa, các clusters mà tệp đó sử dụng được đánh dấu là "unallocated" (không được phân bổ) và có thể được sử dụng lại để lưu trữ dữ liệu mới. Tuy nhiên, cho đến khi chúng bị ghi đè, dữ liệu cũ vẫn có thể tồn tại trong các unallocated clusters này.

Để khôi phục lại các file bị xóa này nhóm em sử dụng cộng cụ WinHex để hỗ trợ khôi phục do phiên bản Encase của nhóm em đã cũ và không thể phân tích rõ các Unallocated clusters.

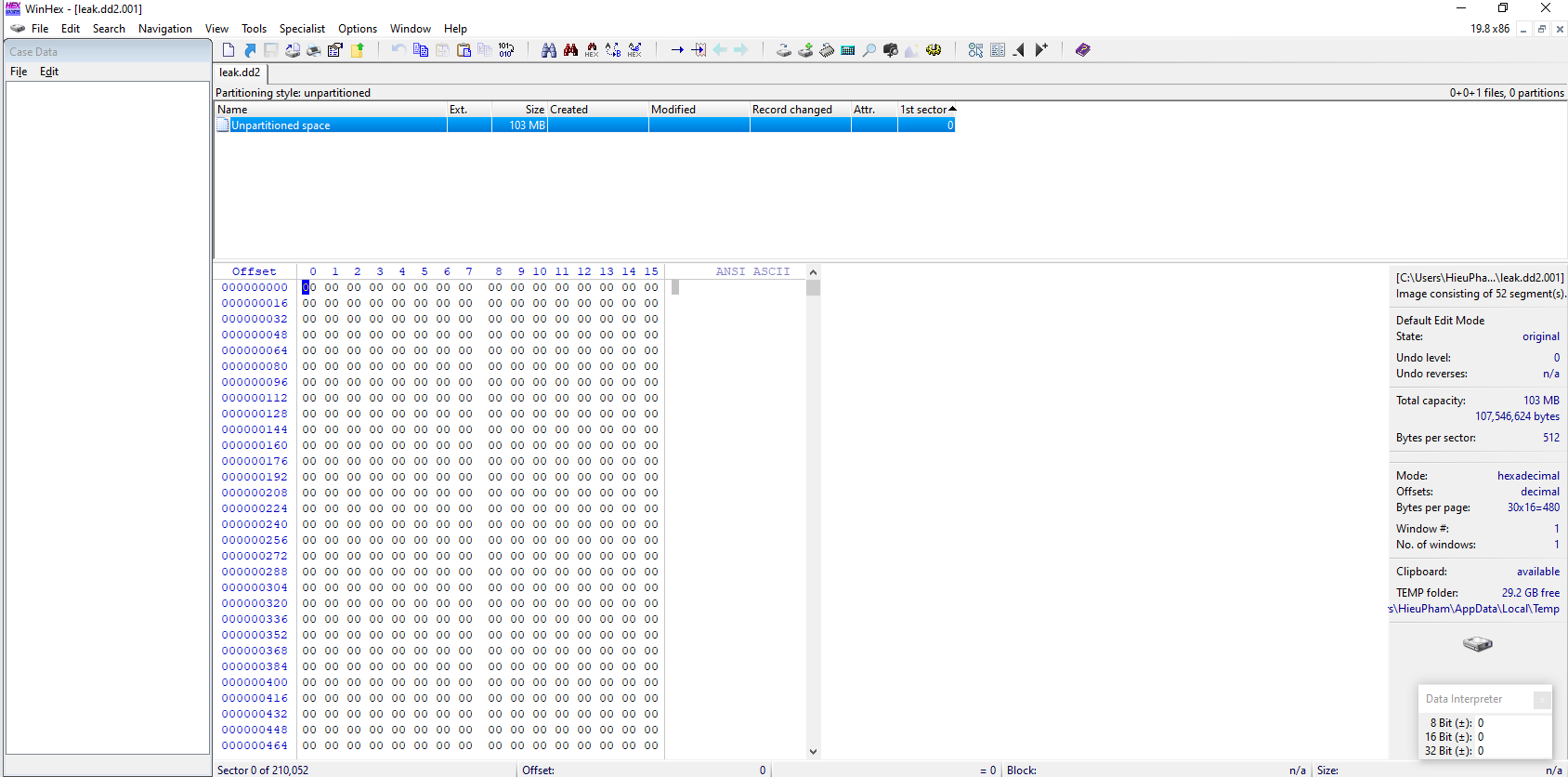
Đầu tiên WinHex không hỗ trợ mở file ở định dạng E01 nên nhóm em dùng công cụ FTK Imager để xuất ổ đĩa theo định dạng Raw. Sau đó vô công cụ WinHex mở tệp và tiến hành khôi phục.



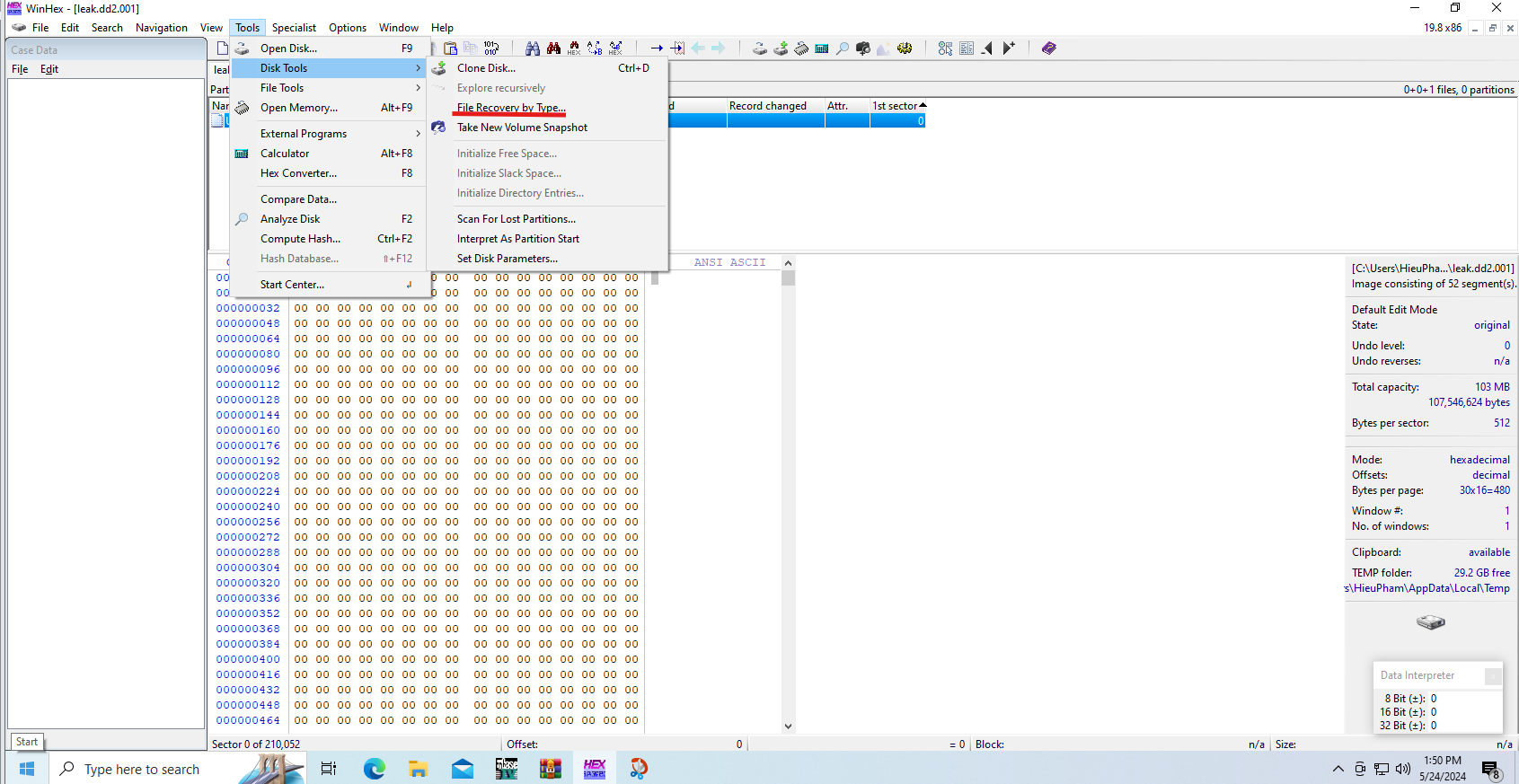
Hình 47. Xuất ổ đĩa theo định dạng Raw



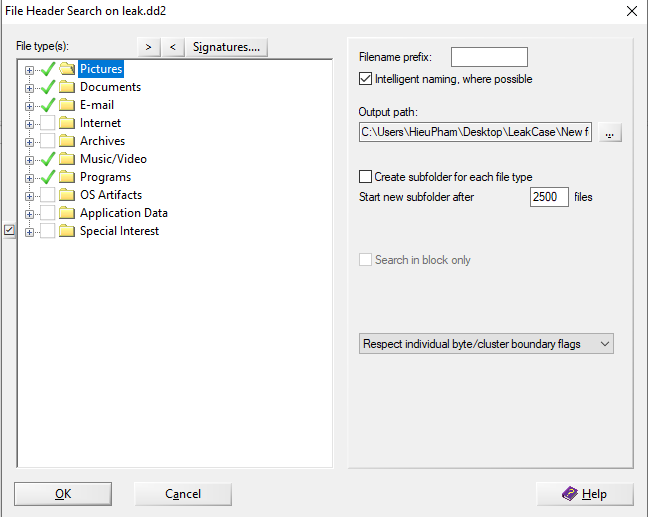
Hình 48. Mở file ổ đĩa định dạng Raw



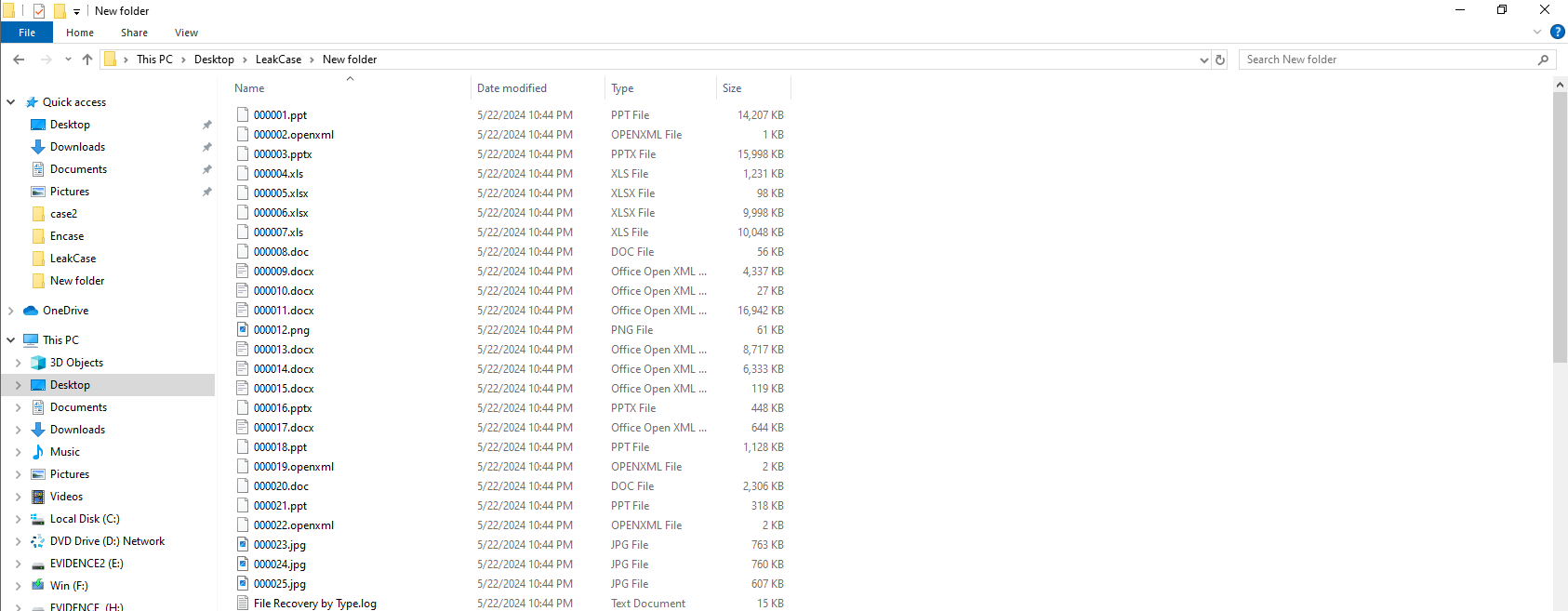
Hình 49. Sau khi mở file



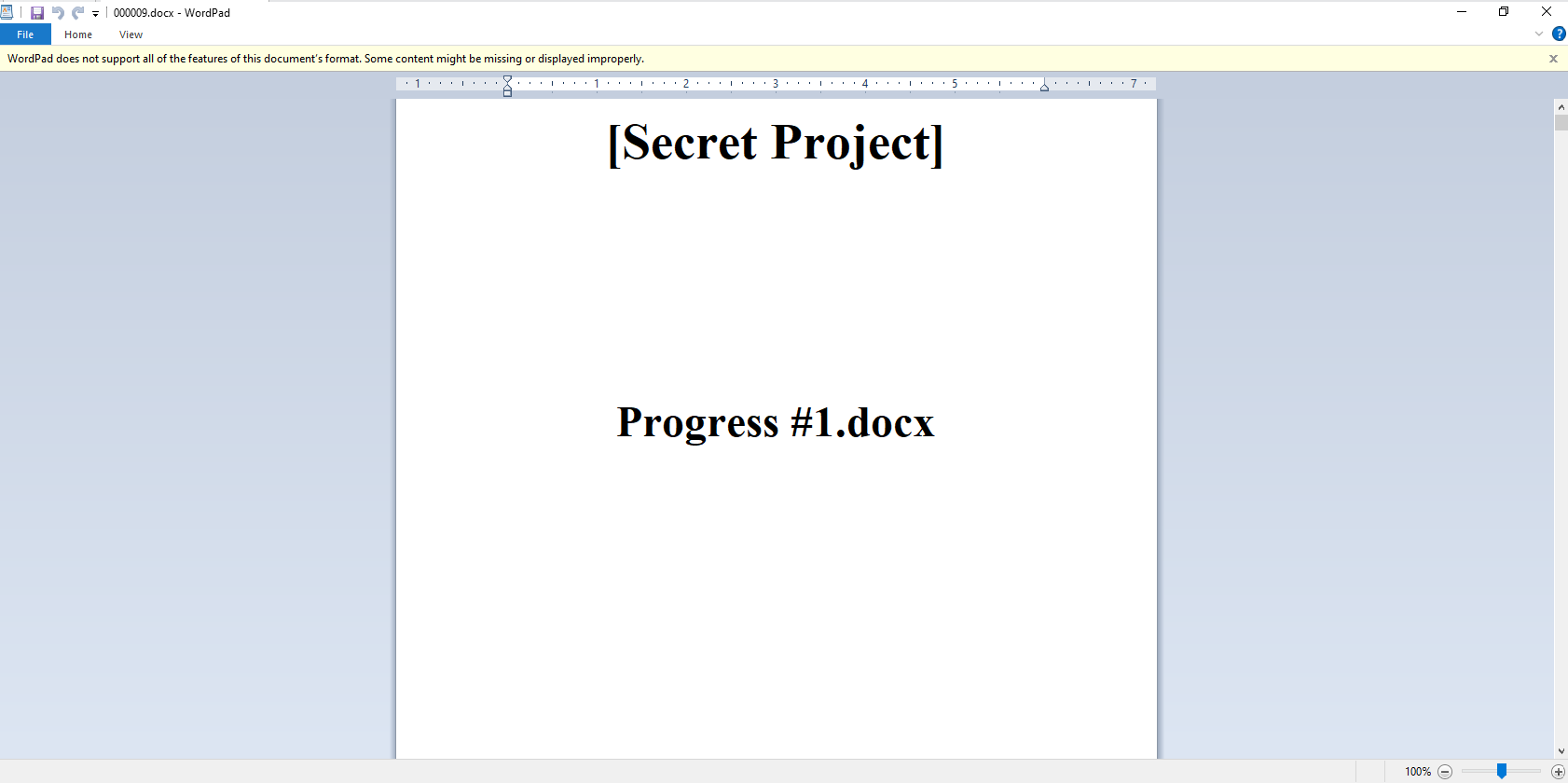
Hình 50. Khôi phục các file



Hình 51. Chọn loại file muốn khôi phục

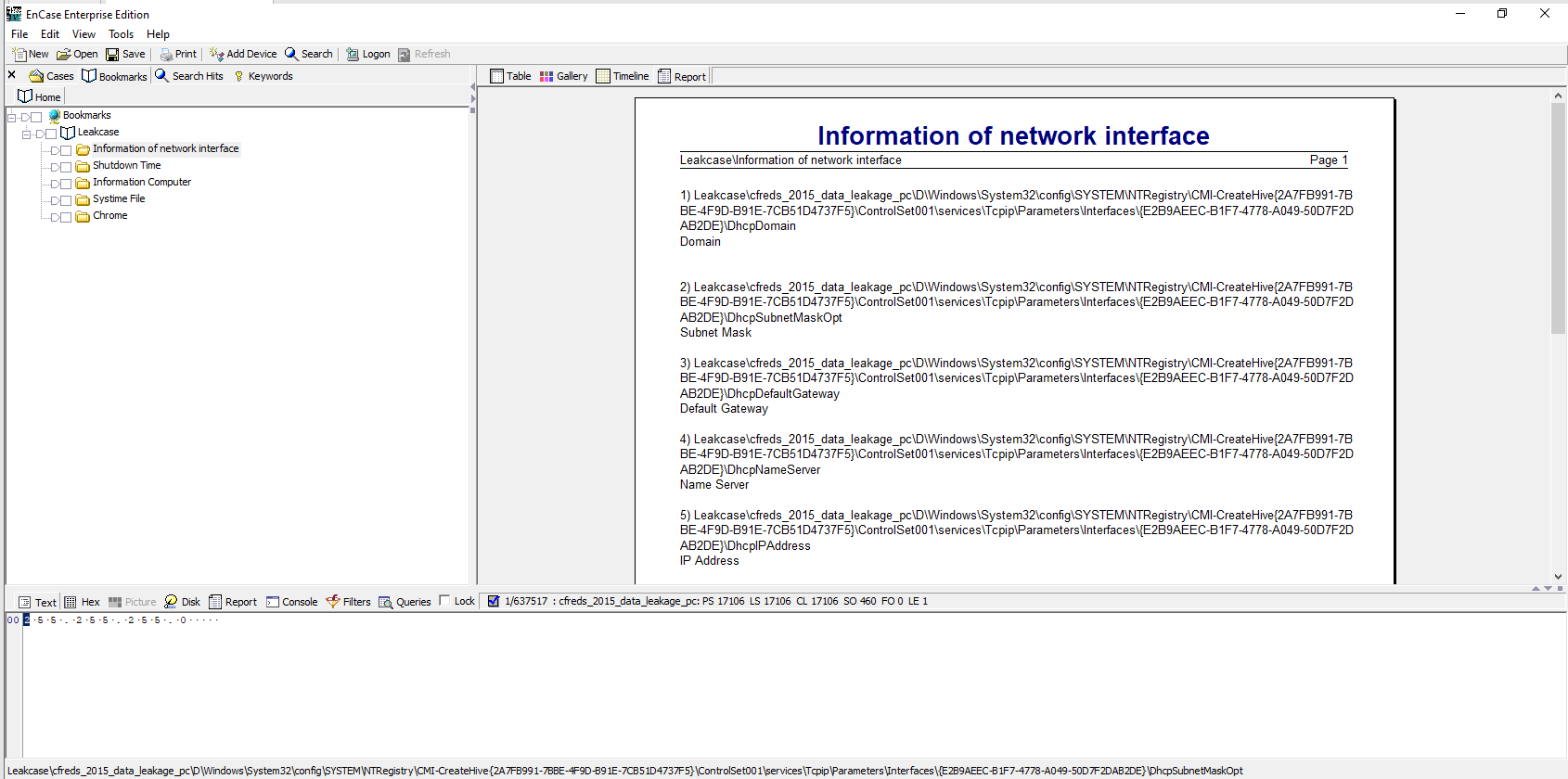


Hình 52. Kết quả sau khi khôi phục



Hình 53. Các tệp bị đánh cắp

Sau khi khôi phục thì có thể tìm thấy các tệp đã bị rò rỉ.



Hình 54. Reporting

Report lại các thông tin bằng chứng đã tìm kiếm được.

# **KẾT LUẬN**

Qua bài báo cáo này, nhóm chúng em đã tìm hiểu về quy trình điều tra số với công cụ Encase. Việc áp dụng kiến thức vào thực tế đã giúp nhóm hiểu rõ hơn về tầm quan trọng của việc thu thập và bảo quản bằng chứng kỹ thuật số, cũng như cách sử dụng các công cụ và kỹ thuật để phân tích dữ liệu ổ cứng, tìm kiếm và khôi phục dữ liệu bị xóa, và xác định các bằng chứng liên quan đến vụ án.

Nhóm chúng em đã học được cách sử dụng Encase để tạo case mới, thêm bằng chứng, xác minh tính toàn vẹn của tệp tin, sử dụng các công cụ để giải mã và phân tích dữ liệu, cũng như tìm kiếm dữ liệu bằng nhiều phương pháp khác nhau.

Tuy nhiên, do hạn chế về phiên bản Encase cũ, nhóm chúng em đã gặp một số khó khăn trong việc phân tích sâu hơn và giải mã một số loại dữ liệu. Điều này cho thấy tầm quan trọng của việc cập nhật công cụ và kỹ thuật điều tra số để đáp ứng với sự phát triển không ngừng của công nghệ.

Bài báo cáo này không chỉ là kết quả của quá trình học tập mà còn là sự trải nghiệm thực tế quý báu, giúp nhóm chúng em hiểu rõ hơn về công việc của một chuyên gia điều tra số. Nhóm chúng em hy vọng rằng những kiến thức và kỹ năng này sẽ là nền tảng vững chắc cho sự phát triển nghề nghiệp trong tương lai.

# **TÀI LIỆU THAM KHẢO**

|  |  |
| --- | --- |
| [1] | EC-Council, "e-learning ptithcm," [Online]. Available: http://e-learning.ptithcm.edu.vn/goto.php?target=file\_4461\_download&client\_id=admin1234. |
| [2] | C. C. S. D. Forensics, "How to add evidence files," 20 11 2023. [Online]. Available: https://www.youtube.com/watch?v=YyHYygkbPQ8&t=41s. |
| [3] | c. archive.nist, "Data leakage case," 23 7 2018. [Online]. Available: https://cfreds-archive.nist.gov/data\_leakage\_case/data-leakage-case.html. |
| [4] | toancaujsc, "GIẢI PHÁP ĐIỀU TRA SỐ – ENCASE FORENSIC," 26 06 2018. [Online]. Available: https://www.toancaujsc.com.vn/giai-phap-dieu-tra-so-encase-forensic.html. |