2

Session

Hard Drive Forensics

Điều tra bộ nhớ lưu trữ:

Tìm bằng chứng phạm tội trong ổ cứng máy tính

Tài liệu Thực hành

Pháp chứng Kỹ thuật số

GVTH: Nghi Hoàng Khoa

Học kỳ II – Năm học 2021-2022

Tp. HCM, 3.2022

Lưu hành nội bộ

A. TỔNG QUAN

1. Mục tiêu

Bài thực hành này giúp sinh viên được làm quen, sử dụng, tăng cường kiến thức về các kỹ năng điều tra kỹ thuật số liên quan đến việc phân tích đĩa cứng máy tính.

2. Giới thiệu điều tra bộ nhớ lưu trữ

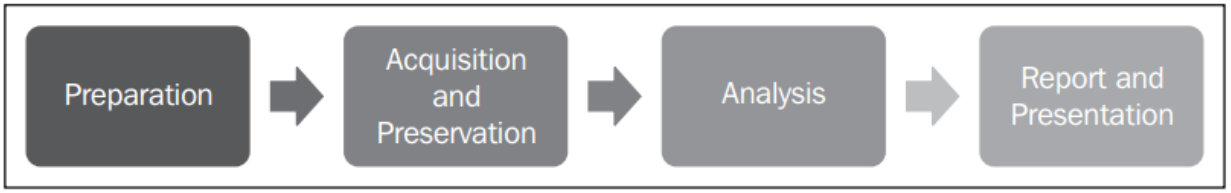
Điều tra máy tính* (*Computer Forensic)

Computer Forensic thường làm việc với những đối tượng sau:

- Memory: Phân tích dữ liệu trên bộ nhớ, thường là dữ liệu lưu trên RAM được dump ra
- Hard Drive (Physical Media, Media Management): Liên quan đến phần cứng, tổ chức phân vùng, phục hồi dữ liệu khi bị xóa…
- File System: Phân tích các file hệ thống, hệ điều hành windows, linux, android…
- Application: Phân tích dữ liệu từ ứng dụng như các file Log, file cấu hình, reverse ứng dụng…
- Network: Phân tích gói tin mạng, sự bất thường trong mạng

Quy trình điều tra pháp chứng trên ổ cứng máy tính

Các giai đoạn chính của việc điều tra pháp chứng trên máy tính (Computer Forensic) được biểu diễn trong sơ đồ bên dưới.



1. **Giai đoạn chuẩn bị (Preparation)**
   Đây là giai đoạn quan trọng đối với điều tra viên, bằng cách chuẩn bị tiến hành qui trình điều tra, các bước lưu ý khi thực hiện. Cụ thể:
   - Xác định được qui trình điều tra phù hợp với yêu cầu
   - Đào tạo huấn luyện kỹ năng liên quan cho đội ngũ điều tra viên
     - Đào tạo kỹ thuật: các kỹ năng liên quan đến việc sử dụng các công cụ điều tra
     - Đào tạo qui trình điều tra: liên quan đến các nguyên tắc, các bước thực hiện trong quá trình điều tra
   - Sự hỗ trợ của các công cụ phần cứng và phần mềm.
2. **Giai đoạn thu thập và bảo quản bằng chứng (Acquisition and preservation)**
   Các thao tác trong giai đoạn này được xem là quan trọng nhất trong qui trình điều tra, do các sai sót, lỗi có thể gây ra những tác động không mong muốn tới bằng chứng. Nguyên tắc cơ bản của điều tra pháp chứng trên máy tính là bảo vệ tính toàn vẹn, nguyên gốc và không bị xâm phạm của bằng chứng.

Việc thu thập bằng chứng được thực hiện dưới sự hỗ trợ của các loại công cụ sau:

- Write blockers (thao tác trên dữ liệu bằng chứng mà không gây ảnh hưởng tới tính toàn vẹn của dữ liệu ổ đĩa – các công cụ phần cứng hoặc phần mềm có tính năng chống ghi)
- Forensic duplicators (sao chép bằng chứng)
- Boot disks
- Remote acquisition (lấy dữ liệu từ xa thông qua kết nối mạng)

3. **Giai đoạn phân tích (Analysis)**
   Giai đoạn này đòi hỏi sử dụng nhiều kỹ thuật và công cụ khác nhau để tìm ra manh mối từ dữ liệu thu thập được ở giai đoạn trước. Khi thực hiện phân tích, điều tra viên cần phải có:
   - Các kiến thức liên quan đến hệ điều hành, ổ cứng lưu trữ, bộ nhớ RAM, ứng dụng, tập tin hệ thống, mạng…
   - Các phần mềm, công cụ chuyên dụng
   - Kỹ năng lọc và tìm kiếm manh mối, bằng chứng tương ứng từ dữ liệu thu thập.
4. **Báo cáo điều tra (Reports and presentation)**
   Đây là bước cuối cùng của quá trình điều tra. Khi nhân viên điều tra tìm ra một số kết quả phân tích nhất định, việc đưa ra kết luận điều tra cần tuân thủ theo các yêu cầu sau:
   - Sử dụng ngôn ngữ, văn phong phù hợp với đối tượng sử dụng báo cáo (người đọc là ai?). Văn phong kỹ thuật chỉ nên sử dụng cho đội ngũ nhân viên điều tra, các hình thức báo cáo sử dụng văn phong, ngữ nghĩa thông dụng hơn nên được sử dụng cho các trường hợp người đọc báo cáo là luật sư hoặc công tố viên.
   - Chú ý đến tính rõ ràng, rành mạch và cô đọng của báo cáo trình bày kết quả, tránh ý kiến chủ quan.
   - Các định dạng tập tin báo cáo khác nhau như pdf, doc, html,…

Ngoài ra để đảm bảo việc truy tìm bằng chứng trong máy tính đối tượng tình nghi, điều tra viên cần chú ý và áp dụng lần lượt các bước sau:

- Kiểm soát hệ thống máy tính để chắc chắn rằng thiết bị và dữ liệu được an toàn. Điều này có nghĩa điều tra viên cần phải nắm quyền bảo mật để không có một cá nhân nào có thể truy cập máy tính và thiết bị lưu trữ đang được kiểm tra. Nếu hệ thống máy tính có kết nối với Internet, điều tra viên phải kiểm soát được kết nối này.
- Tìm kiếm tất cả các file có trong hệ thống máy tính, bao gồm các file đã được mã hóa, được bảo vệ bằng mật khẩu, được ẩn hoặc bị xóa nhưng chưa bị ghi đè. Nhân viên điều tra nên sao chép lại tất cả các file của hệ thống, bao gồm các fiel có trong ổ đĩa của máy tính hay file từ các ổ cứng cắm ngoài. Bởi khi truy cập các file có thể thay đổi nó nên nhân viên điều tra chỉ nên làm việc với các bản copy của các file khi tìm kiếm bằng chứng. Bản nguyên gốc cần được bảo quản và không được động đến.

- Khôi phục lại càng nhiều thông tin bị xóa càng tốt bằng cách sử dụng các ứng dụng có thể tìm kiếm và truy hồi dữ liệu bị xóa.
- Tìm kiếm thông tin của tất cả các file ẩn
- Giải mã và truy cập các file được bảo vệ
- Phân tích các khu vực đặc biệt trên ổ đĩa máy tính, bao gồm các phần thường khó có thể tiếp cận.
- Ghi lại tất cả các bước của quá trình. Điều này rất quan trọng đối với nhân viên điều tra để cung cấp bằng chứng rằng công việc điều tra của họ thực hiện có bảo vệ thông tin của hệ thống máy tính mà không làm thya đổi hoặc làm hỏng chúng. Một vụ điều tra và vụ xử án có thể mất tới hàng năm, nếu không có tài liệu xác thực, bằng chứng thậm chí còn không được chấp nhận.

Tất cả các bước này rất quan trọng, nhưng bước đầu tiên mới là quan trọng nhất. Nếu nhân viên điều tra không thể kiểm soát toàn bộ hệ thống máy tính, bằng chứng họ tìm được sẽ không được công nhận. Do đó đây cũng là việc rất khó. Ngày nay, máy tính bao gồm rất nhiều máy tính, ổ đĩa, ổ cứng cắm ngoài,... thay vì hệ thống máy tính chỉ bao gồm một chiếc máy với một vài chiếc đĩa mềm ở giai đoạn đầu của lịch sử ra đời máy tính. Đó là chưa nói đến tội phạm có thể sử dụng các chương trình và ứng dụng có tên anti-forensic. Điều tra viên sẽ phải dè chừng những chương trình này và tìm cách loại bỏ chúng nếu họ muốn truy cập thông tin trong hệ thống.

Nhân viên điều tra đã làm gì trên ổ cứng máy tính

Ví dụ: Để đối phó với các nhóm tội phạm công nghệ cao, cảnh sát Anh quốc đã áp dụng mọi biện pháp, trong đó một biện pháp khá hữu hiệu là tìm ra những bằng chứng phạm tội của kẻ bị tình nghi từ những chiếc ổ cứng máy tính. Đội đặc nhiệm điều tra tội phạm công nghệ cao NHTCU (National Hi-tech Crime Unit) của nước Anh có nhiệm vụ đấu tranh chống lại các loại tội phạm trực tuyến như hacker, lừa đảo, gieo rắc khiêu dâm trẻ em và bất cứ hành vi phạm tội nào có liên quan đến máy tính. Một trong những công cụ quan trọng mà các chuyên gia máy tính của NHTCU sử dụng là phần mềm EnCase. Hiện EnCase đang được hơn 2.000 cơ quan an ninh trên toàn thế giới sử dụng. Phần mềm này giúp cho các điều tra viên truy tìm các manh mối trong những chiếc ổ cứng mà họ tịch thu được của bọn tội phạm trong quá trình điều tra.

Đầu tiên, các điều tra viên sẽ nối ổ cứng với một máy tính có chứa phần mềm EnCase. Phần mềm này sẽ tạo ra một ổ đĩa ánh xạ hoàn toàn ổ đĩa nói trên, dùng để làm bằng chứng trước tòa án, đồng thời gài thêm một số tính năng bảo mật để đảm bảo rằng dữ liệu trong ổ đĩa không hề bị sửa đổi. Sau đó, EnCase sẽ đọc các file để tìm kiếm bằng chứng về hành vi phạm pháp của kẻ sở hữu chiếc ổ cứng. Phần mềm EnCase sẽ tìm kiếm ở dưới cấp độ hệ điều hành để có thể khảo sát tất cả các file, kể cả không gian trống, không gian chưa được định vị, và các file đã xóa khỏi Windows.

3. Môi trường & cấu hình

- Sử dụng các thiết bị và tài liệu, khuyến cáo được cung cấp bởi GVTH, yêu cầu tác phong nghiêm túc trong quá trình thực hiện.
- Công cụ gợi ý: **FTK, EnCase, Autopsy…**
- Tài liệu nên đọc: Sách ***"Computer Forensics with FTK"*** (tác giả: Fernando Carbone)

B. THỰC HÀNH

Sinh viên thực hiện điều tra theo yêu cầu của GVHD, làm theo nhóm thực hành đã đăng ký trên lớp trong buổi thực hành.

B1. Phân tích dữ liệu bằng công cụ Autopsy

Giúp sinh viên nắm bắt và hiểu rõ các tính năng của công cụ phần mềm Autopsy khi tiến hành điều tra và tìm kiếm thông tin trong một Filesystem.

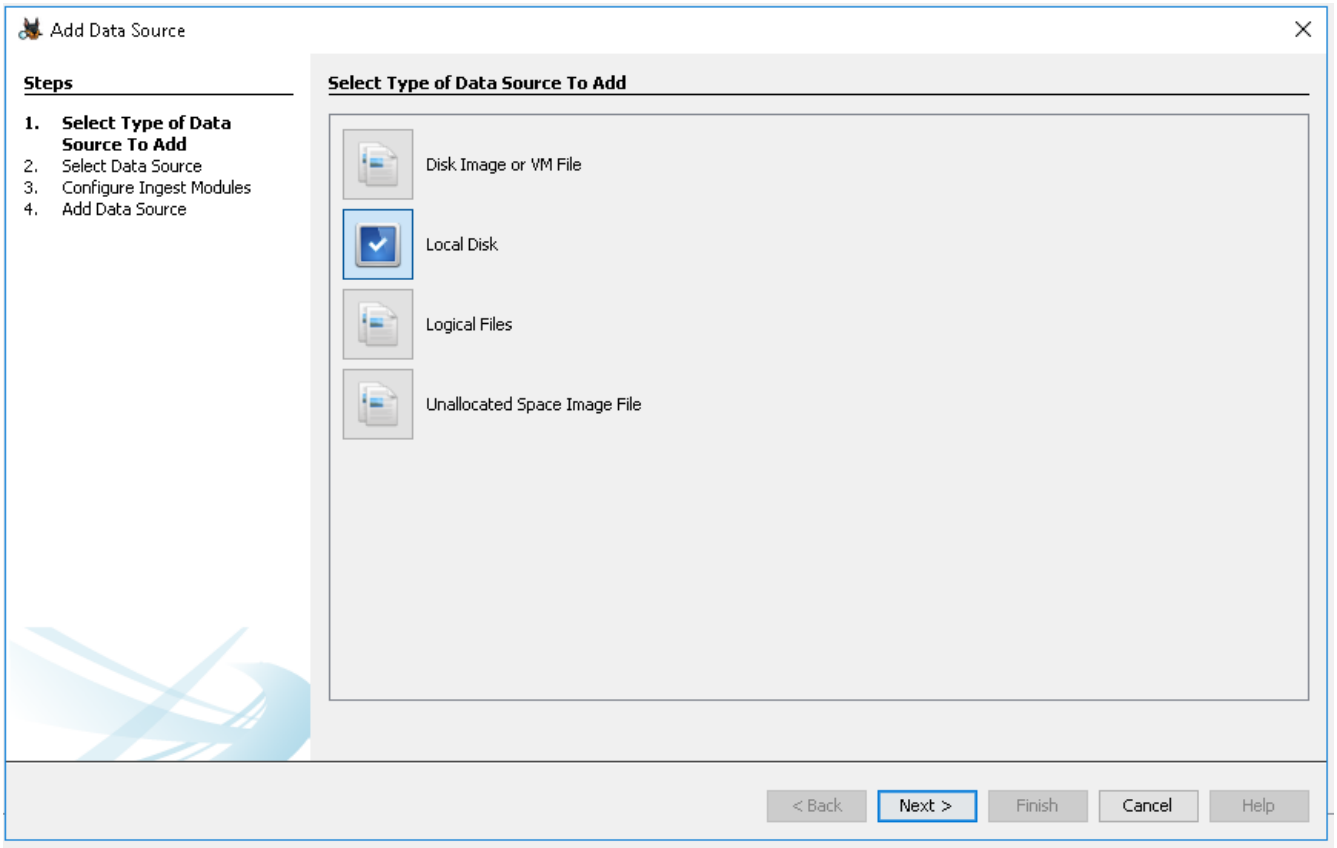
Autopsy là một công cụ phần mềm pháp chứng kỹ thuật số với giao diện đồ họa của bộ phần mềm mã nguồn mở Sleuth Kit, Autopsy có thể được sử dụng để điều tra những gì đã xảy ra trên máy tính. Autopsy cho phép phân tích sự kiện theo thời gian, trình bày các sự kiện truy cập tới File system theo trình tự với giao diện đồ họa.

Link download: https://www.sleuthkit.org/autopsy/download.php

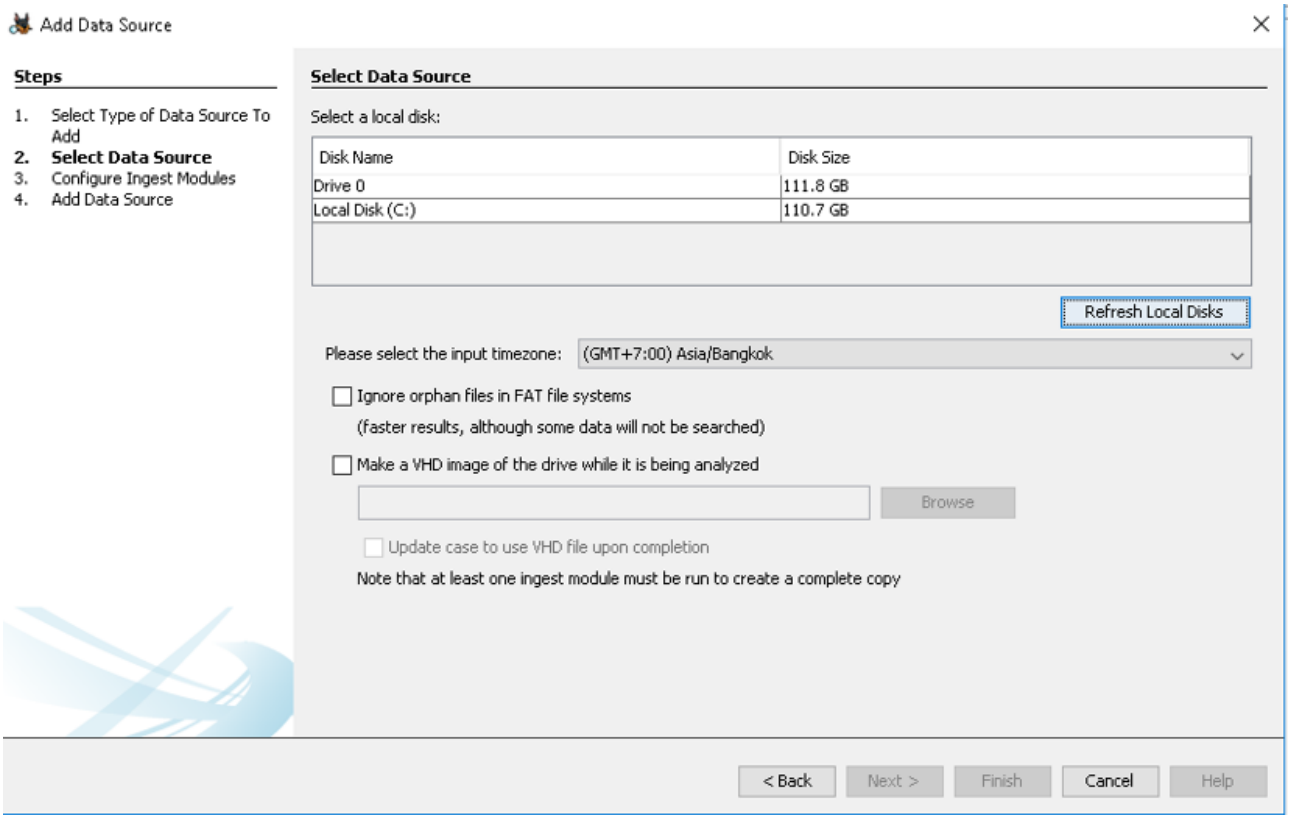
- Khởi động Autopsy để tạo một Case mới, sử dụng lựa chọn "Create New Case".

- Điền tên Case vào khung Case name (cũng là tên của thư mục chứa các file liên quan)

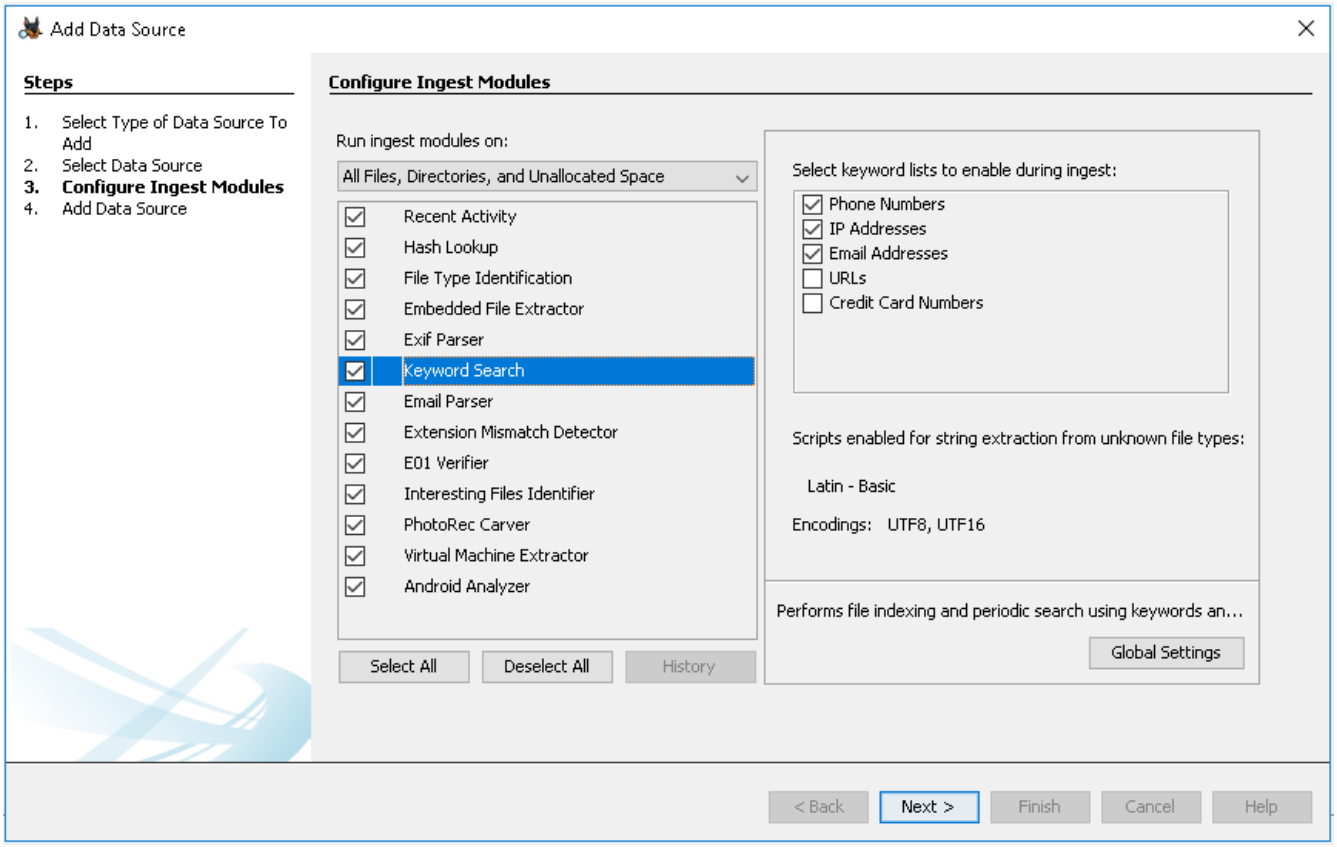
– Chọn Local Disk để phân tích các phân vùng trong máy.



– Chọn Disk Name cần phân tích.

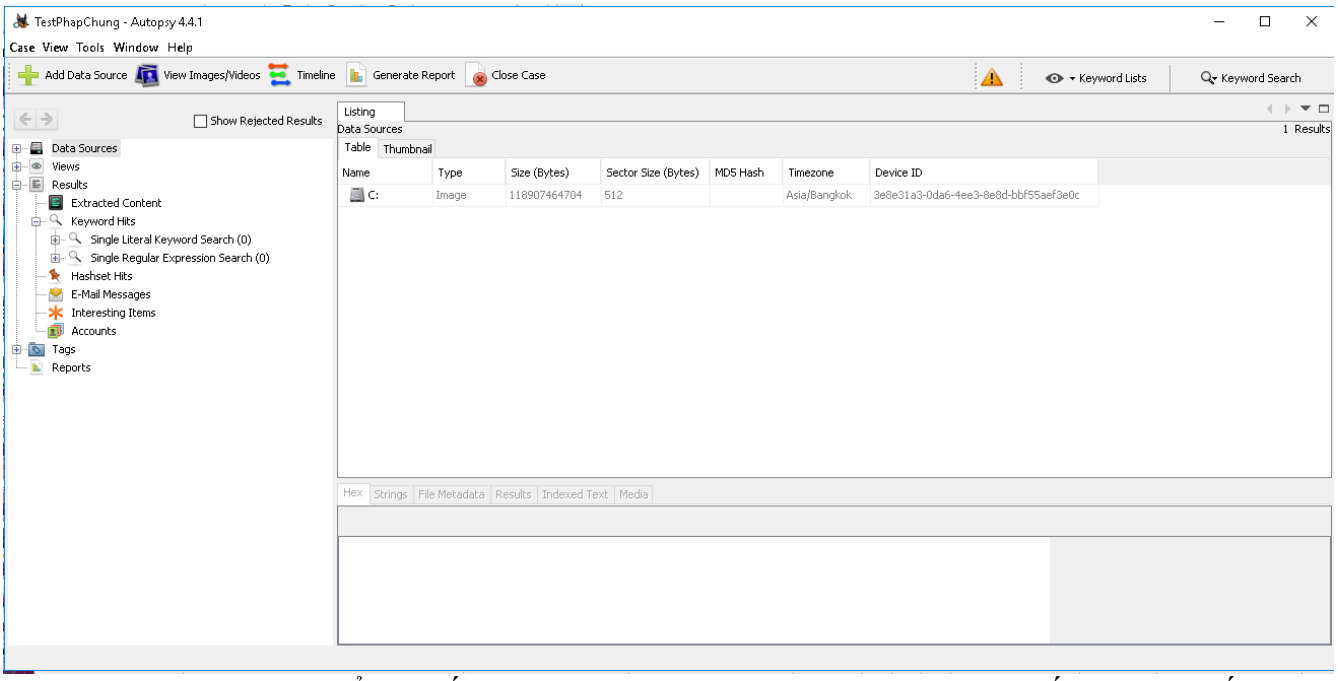


– Chọn ra mô-đun để phân tích, mô-đun Keyword Search sẽ có thêm một số tùy chọn như: IP, email,...



Một số mô-đun trong công cụ:

- ***Recent Activity*** tìm kiếm các hoạt động người dùng như lưu bởi các trình duyệt web và hệ điều hành Windows.
- ***Hash Lookup*** sử dụng cơ sở dữ liệu băm để bỏ qua các tập tin được biết từ NIST NSRL và cờ để tìm các tập tin xấu. Sử dụng nút "Advanced" để thêm và cấu hình cơ sở dữ liệu để sử dụng hash trong quá trình này.
- ***Keyword Search*** sử dụng danh sách từ khoá để xác định các tập tin với những từ cụ thể trong đó. Chúng ta có thể chọn danh sách từ khóa để tìm kiếm tự động và tạo danh sách mới bằng cách sử dụng nút "Advanced".
- ***Archive Extractor*** mở các file có dạng ZIP, RAR, và các định dạng lưu trữ khác và tìm các tập tin từ các tập tin lưu trữ để phân tích thông tin.
- ***Exif Parser*** trích xuất thông tin EXIF từ các tập tin hình ảnh là lưu các kết quả hình ảnh vào cây trong giao diện chính.



- Data Sources: hiển thị tất cả dữ liệu trong Filesystem trong đó có cấu trúc hệ thống tập tin của hình ảnh đĩa hoặc đĩa cục bộ.
- Views: hiển thị các thông tin chi tiết thông tin của các file chứa trong Filesystem.
- Result: hiển thị và phân loại các thông tin mà các mô-đun phân tích được trong Filesystem.

Kịch bản 01. Thực hiện phân tích dựa trên dữ liệu ổ đĩa (tự chọn)

- Chọn tìm các số điện thoại và địa chỉ IP có trong Filesystem.
- Thực hiện việc xem xét toàn bộ Filesystem, xem xét các lựa chọn nằm ô phía bên trái của màn hình.
- Tìm thư mục có nhiều File nhất trong Filesystem.
- Xem các file hình ảnh chứa trong Filesystem bằng chế độ view Thumbnail. Xác định số lượng các files dạng doc và pdf chứa trong Filesystem.
- Sử dụng nút "Generate Report" để tạo ra báo cáo dạng HTML và Excel, xem nội dung báo cáo trong mục Report. Nêu nhận xét, kết luận về nội dung của báo cáo.

Đáp án:

Kịch bản 02. Thực hiện phân tích dựa trên tài nguyên được cung cấp.

Tài nguyên: tải về theo link sau: https://goo.gl/MRLtj4

- Hãy tìm tất cả những hình ảnh có trong ổ đĩa đã cho.
- Với mỗi file hình ảnh tìm được, liệt kê tất cả các thông tin liên quan đến file đó: tên file, loại file, size, thời gian tạo, xoá, sửa, MD5, kích thước hình ảnh …

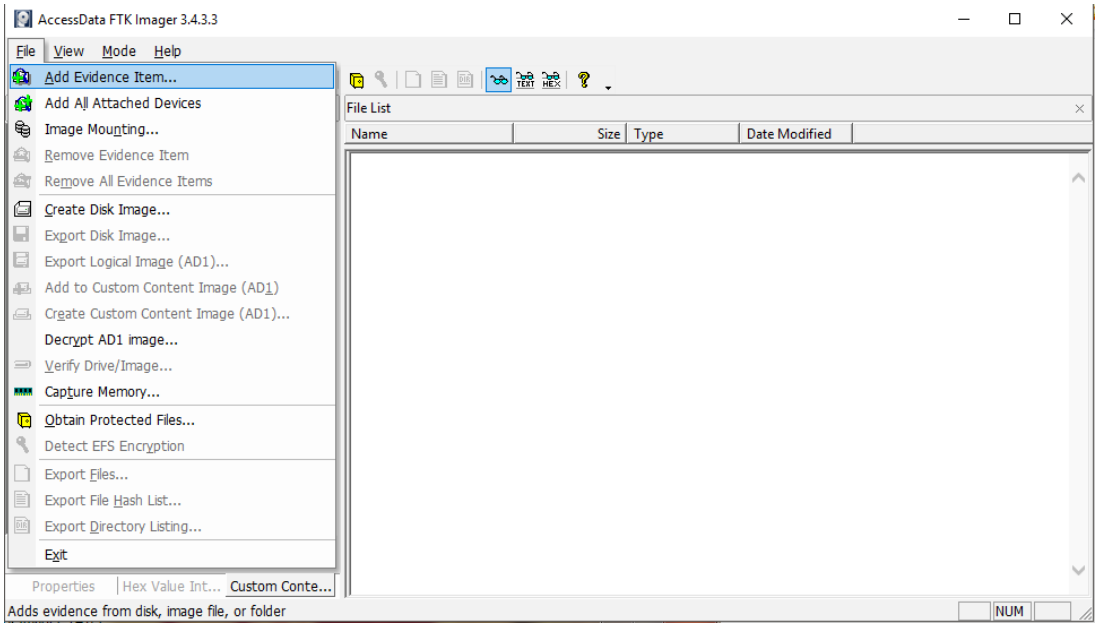
Đáp án:

B2. Phân tích bộ nhớ lưu trữ với công cụ FTK Imager

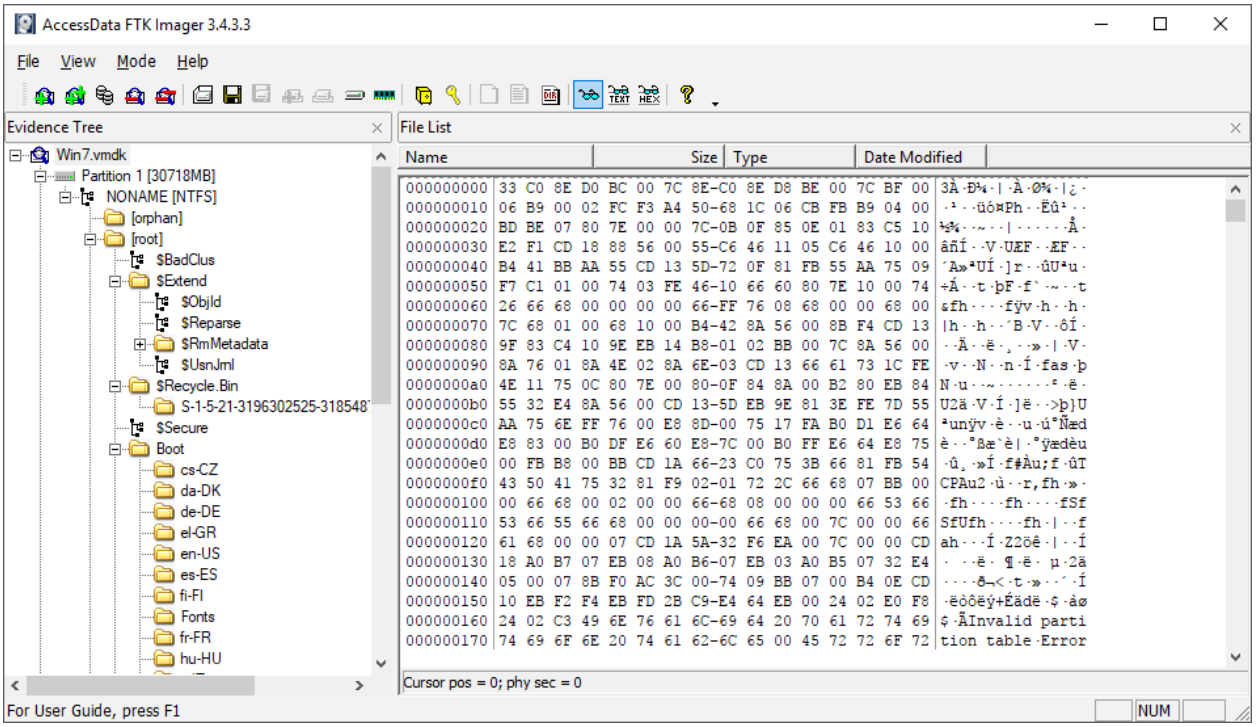
FTK Imager là một công cụ dùng để quan sát dữ liệu của chứng cứ số với mục đích có thể quan sát phân tích sâu hơn. FTK Imager còn có thể tạo ra một bản sao chi tiết (còn được gọi là forensic images) của máy tính mục tiêu mà hoàn toàn không thay đổi cấu trúc của bản gốc.

a. Kịch bản 03

- Cài đặt công cụ FTK Imager, tải về tại: https://accessdata.com/product-download/ftk-imager-version-3.4.3
- Tính năng "Thêm chứng cứ": Chọn File => Add Evidence Item để chọn chứng cứ cần thêm.

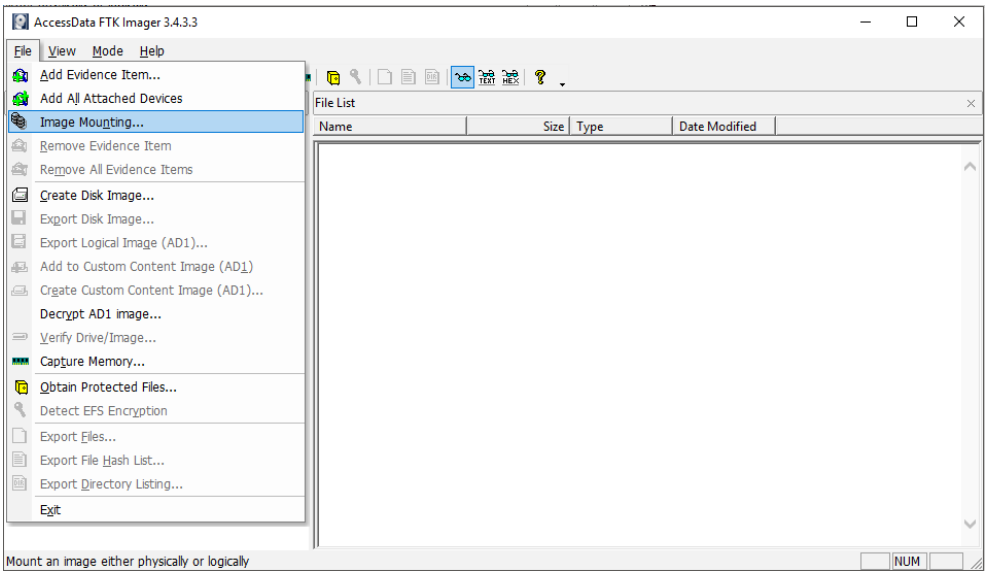


Mục tiêu trong ví dụ này là file dữ liệu ổ đĩa của máy ảo Windows 7. Sinh viên chọn một file đĩa phù hợp để thực hành sử dụng công cụ.

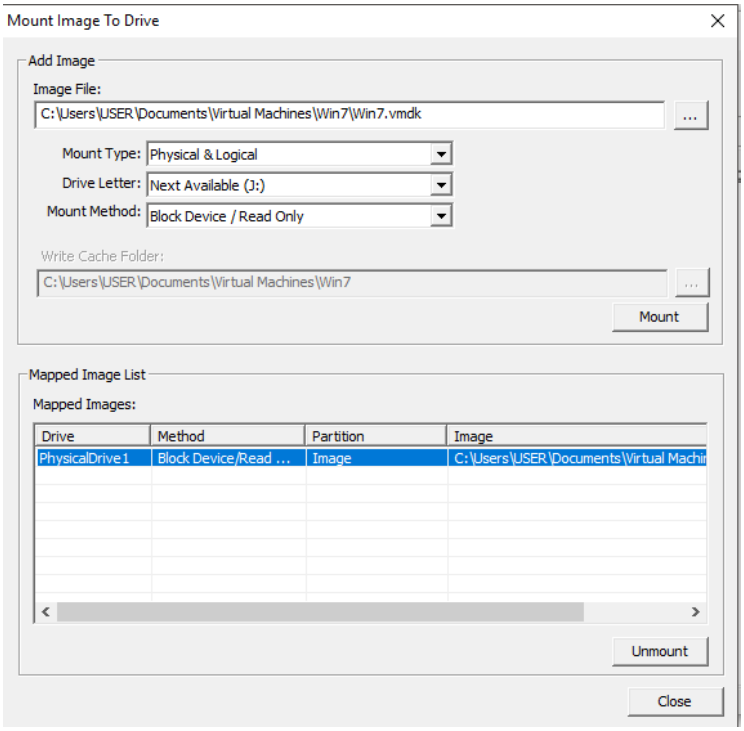


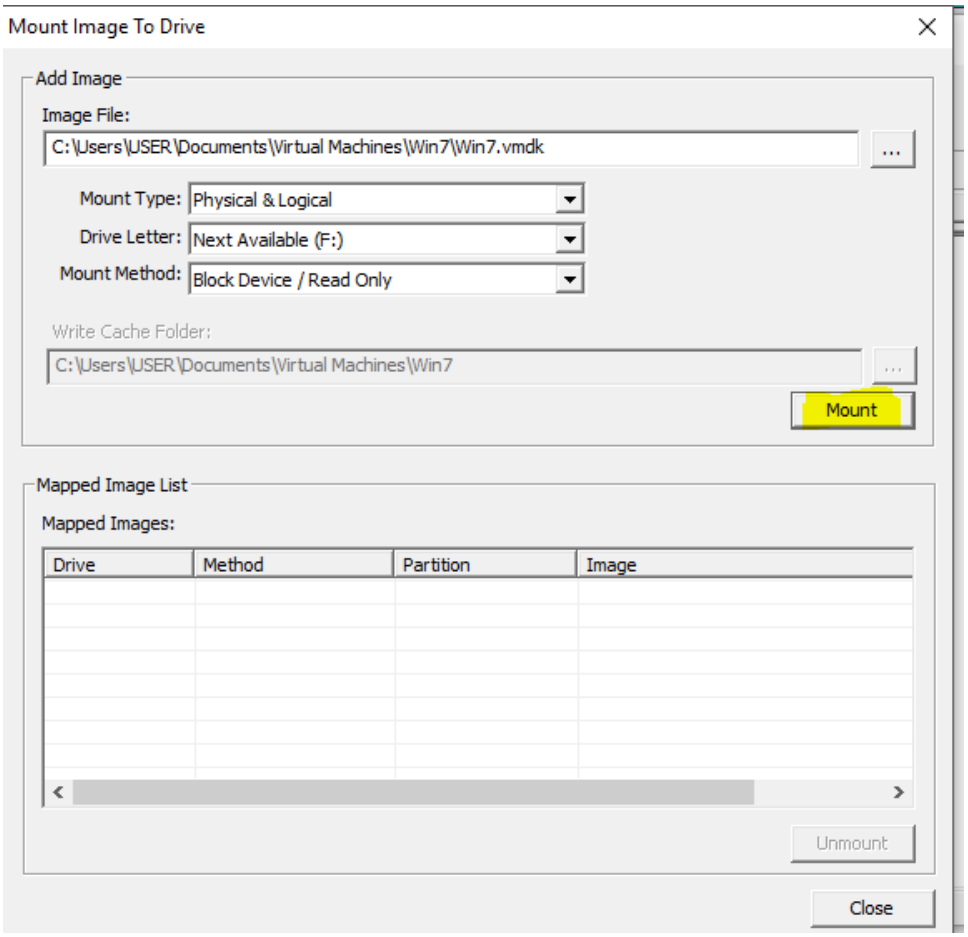
Có thể dễ dàng xem được cây hệ thống của file dữ liệu của ổ đĩa được chọn.

- Gắn (mounting) file ảnh của ổ đĩa (disk images) vào máy tính phân tích:



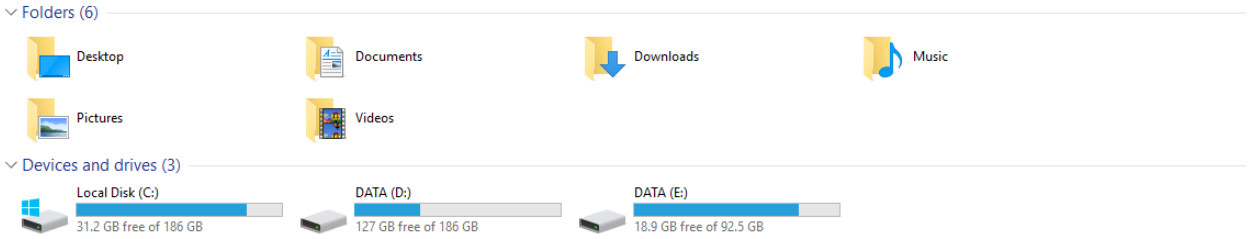
Chọn ảnh đĩa (disk image) mục đích cần phân tích, sau đó chọn Mount để gắn thêm ổ đĩa:



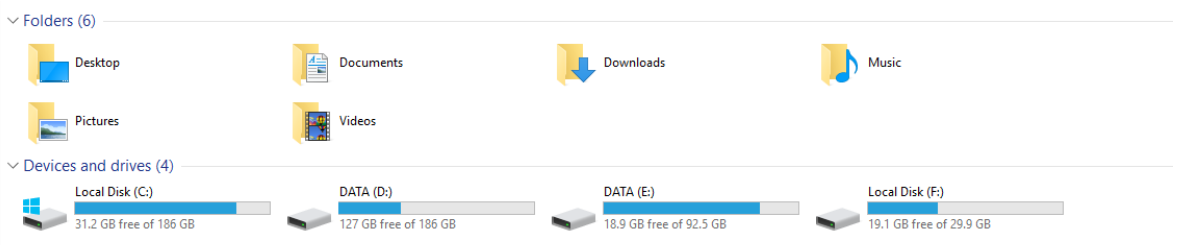


Như vậy, chúng ta đã thêm vào một ổ đĩa với dữ liệu từ file đĩa từ máy ảo Windows 7 để phân tích.

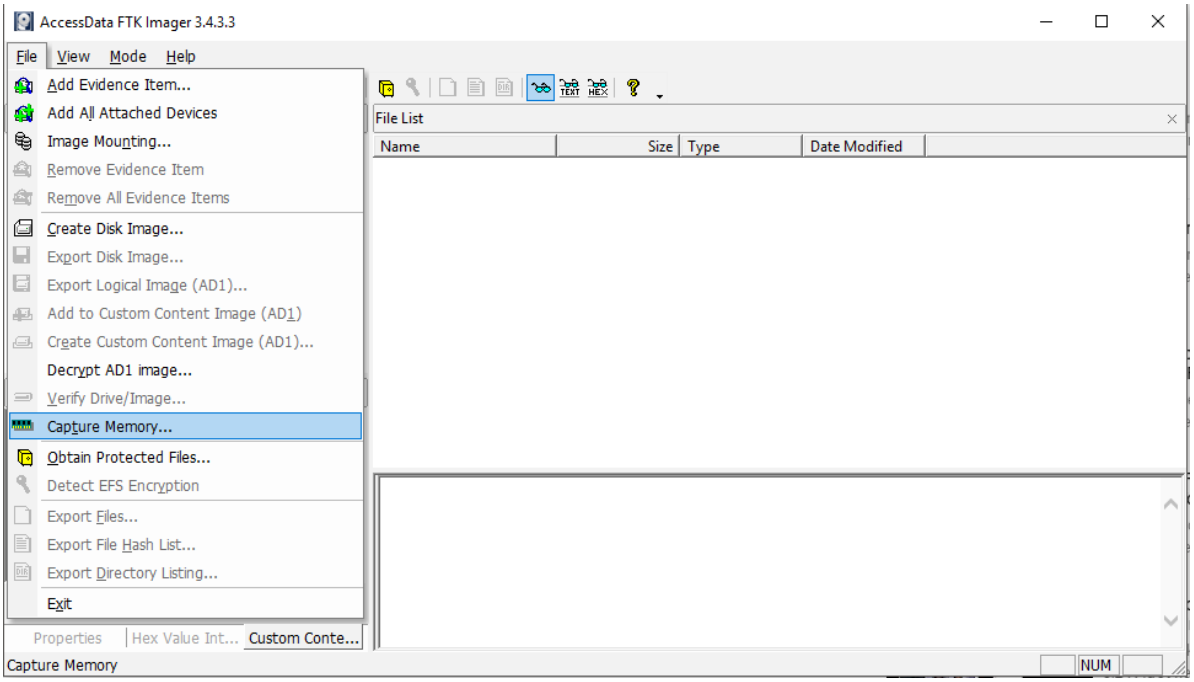
Trước khi thêm:



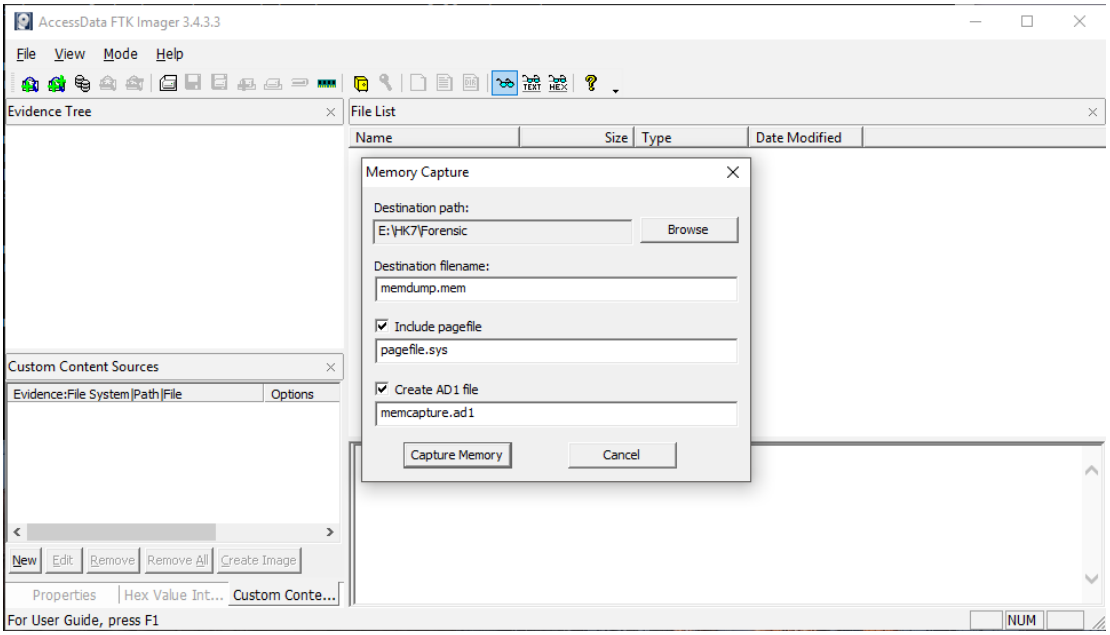
Sau khi gắn thêm file đĩa cần phân tích:



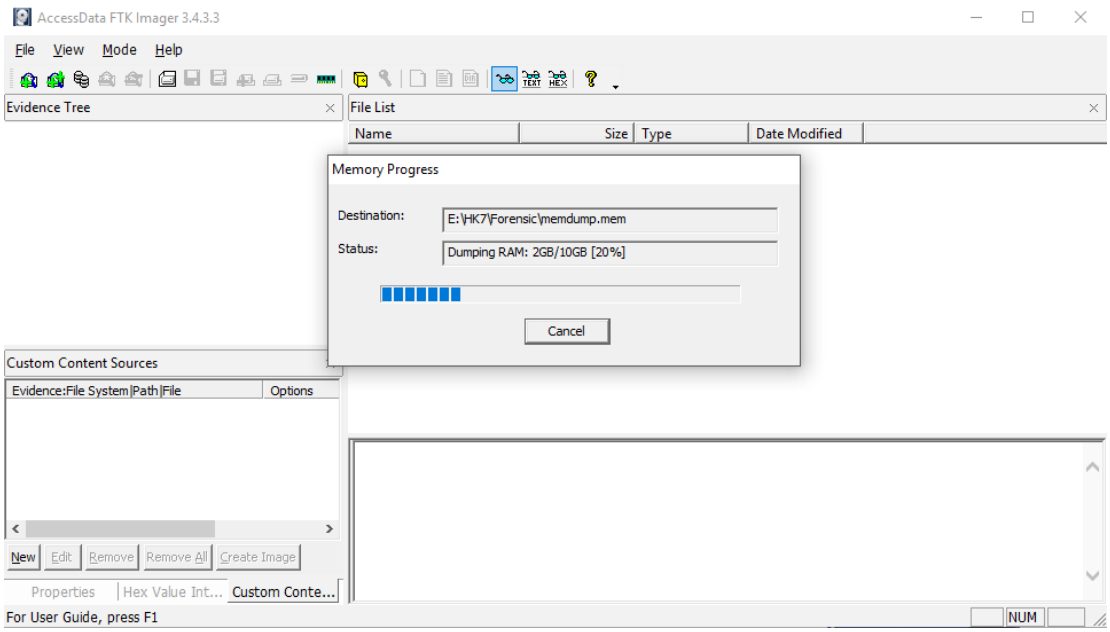
- Tính năng thu dữ liệu RAM:
  Chọn File => Capture Memory.

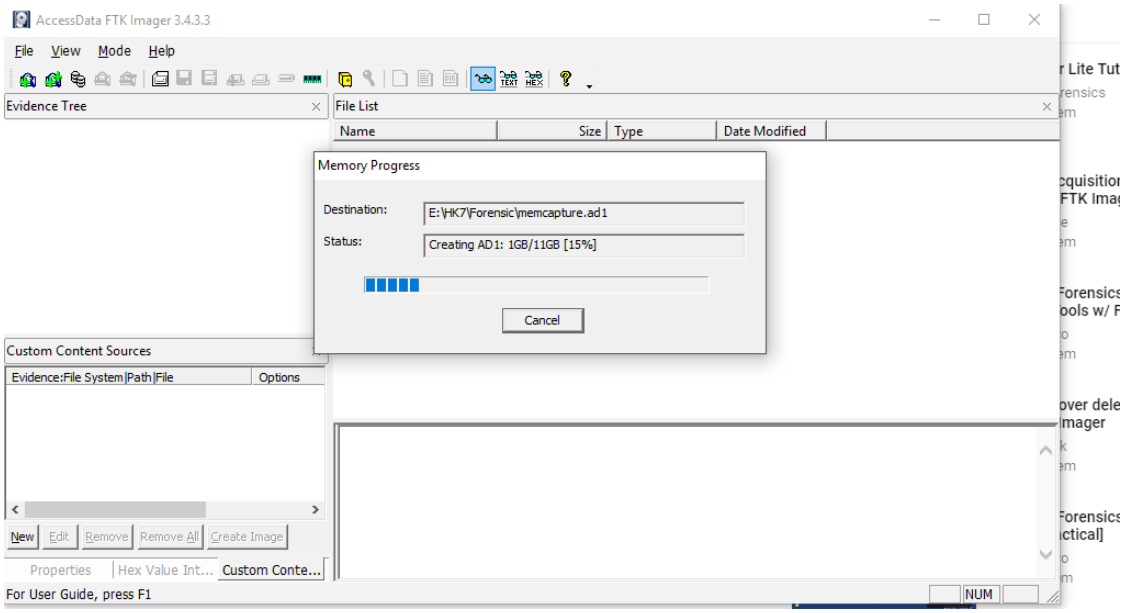


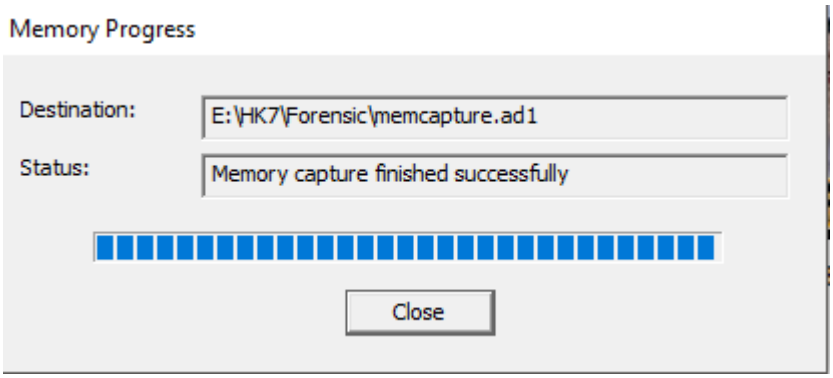
Chọn nơi lưu trữ, tên file và đánh dấu vào các ô còn lại để đảm bảo rằng dữ liệu quan trọng khi thu thập không bị mất.



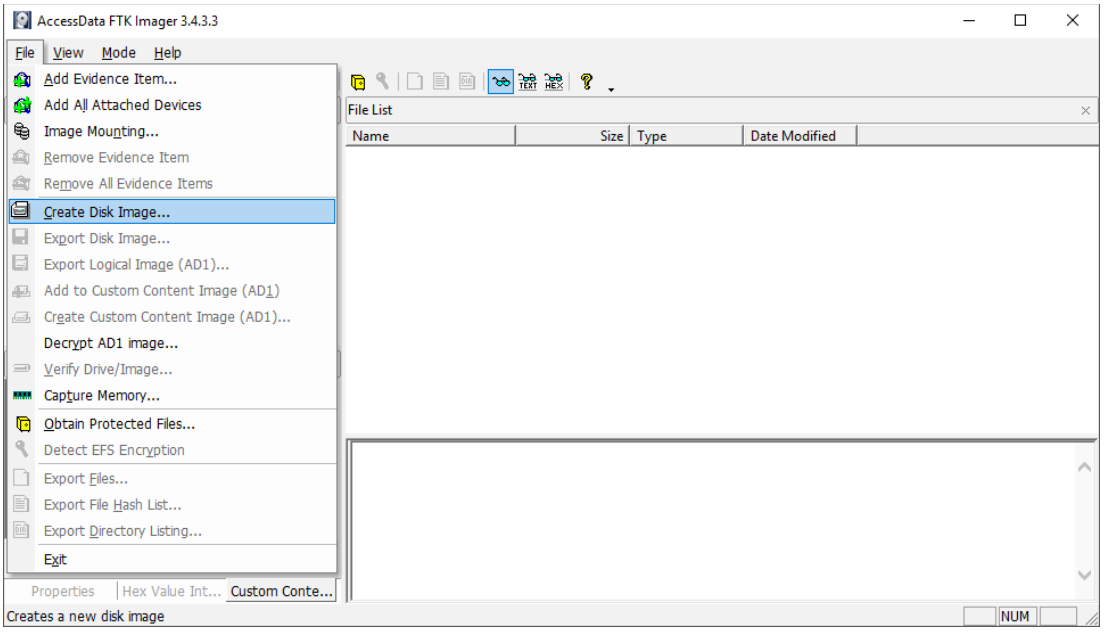
Chờ quá trình công cụ bắt dữ liệu của RAM hoàn tất.



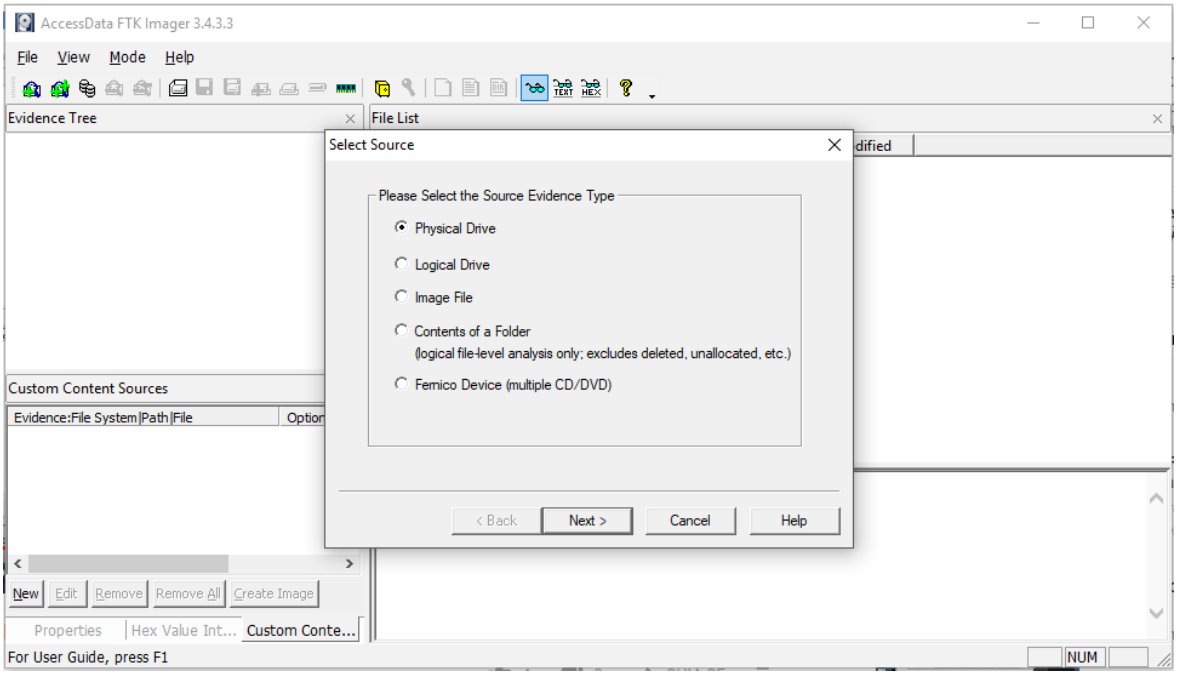




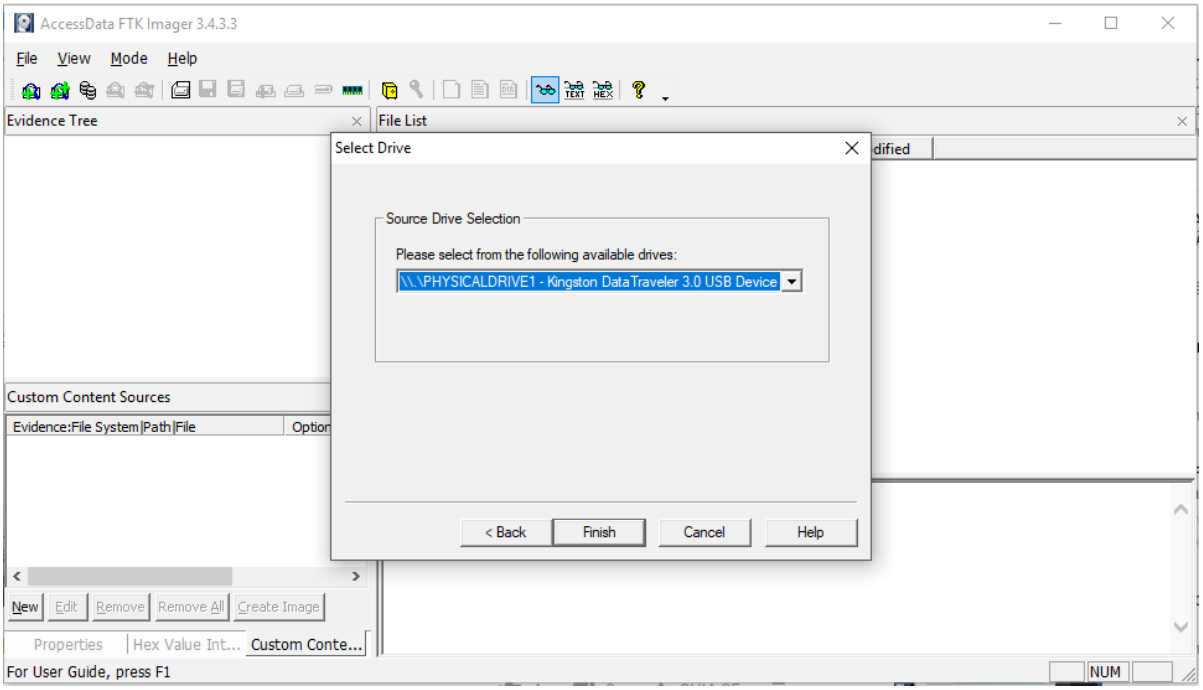
- Chức năng tạo RAW Image:
  Chọn File => Create Disk Image.



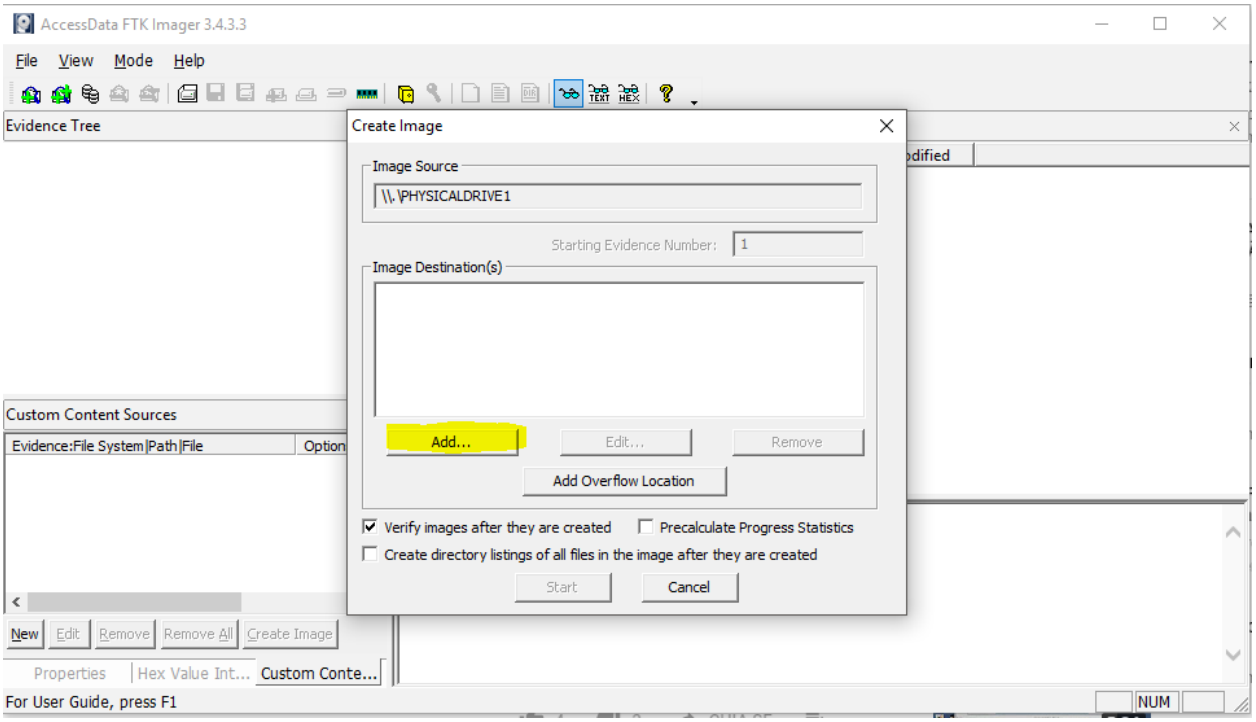
Chọn loại ổ đĩa bằng chứng muốn tạo ra:



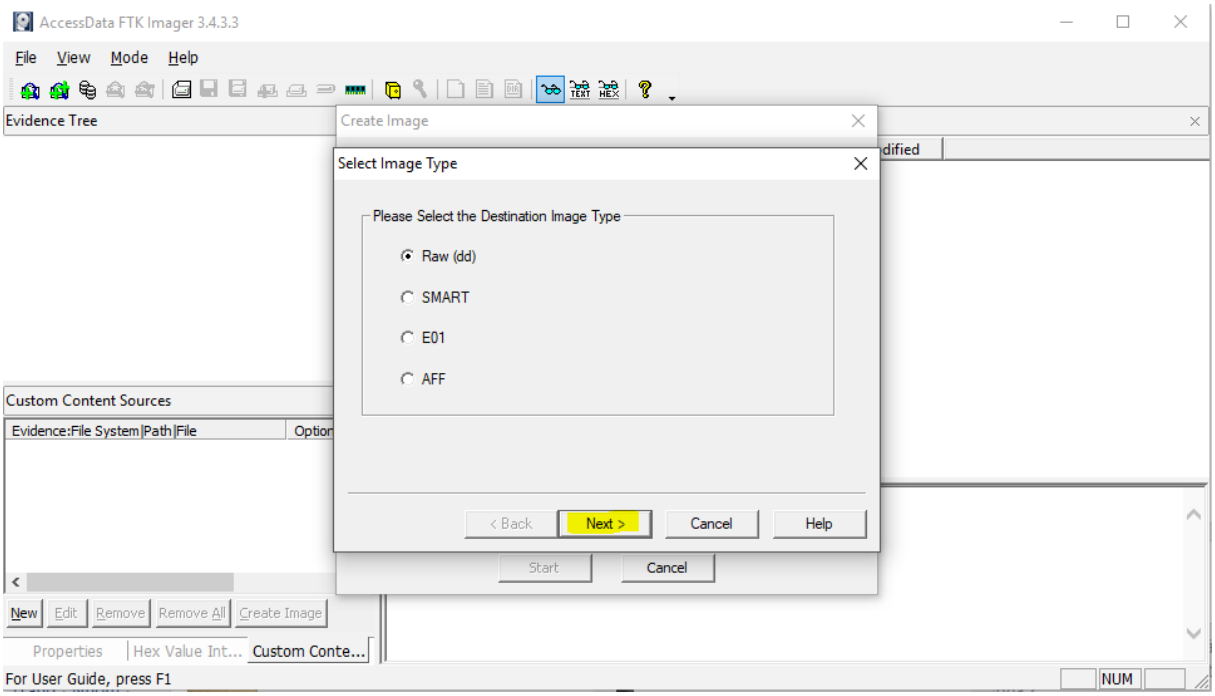
Do dung lượng ổ đĩa của máy tính quá lớn nên trong ví dụ này, chúng ta chọn tạo từ USB với dung lượng vừa đủ.



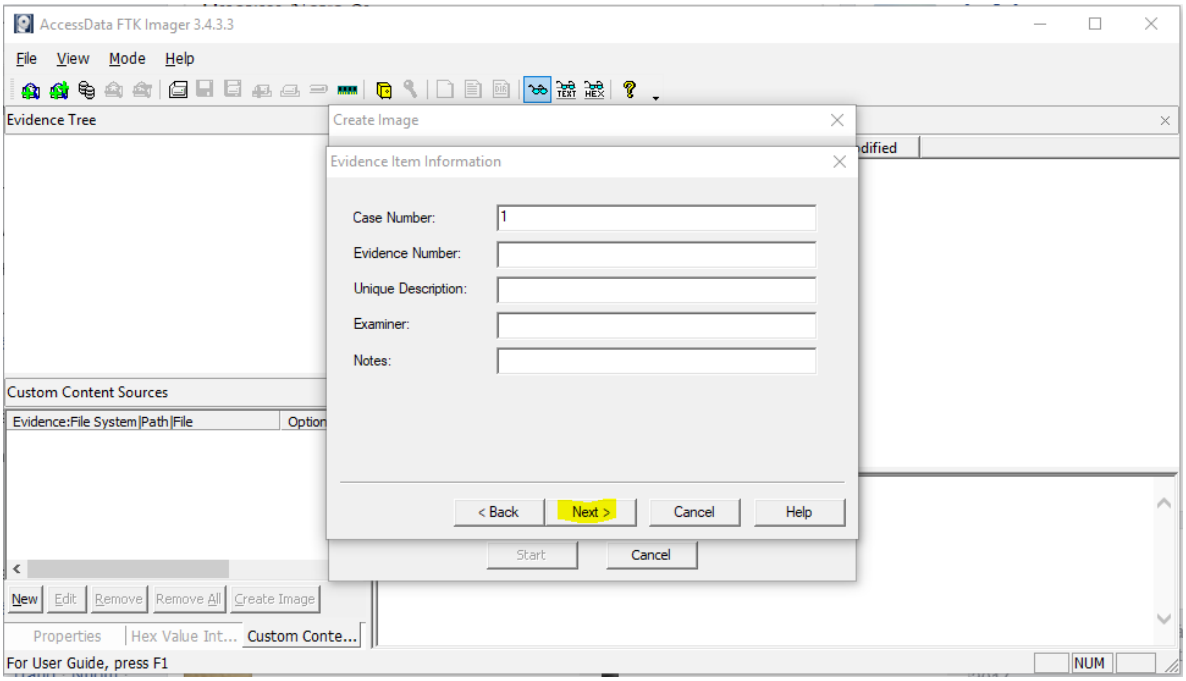
Chọn nơi để lưu file ảnh đĩa.



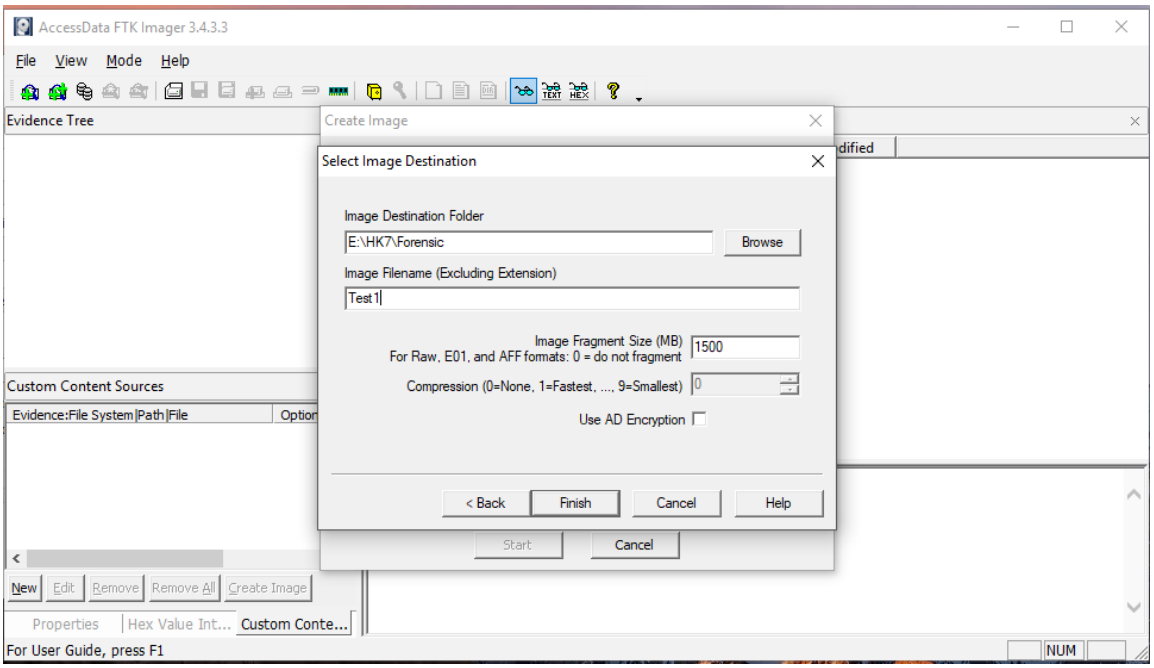
Chọn loại ảnh đĩa muốn tạo ra.

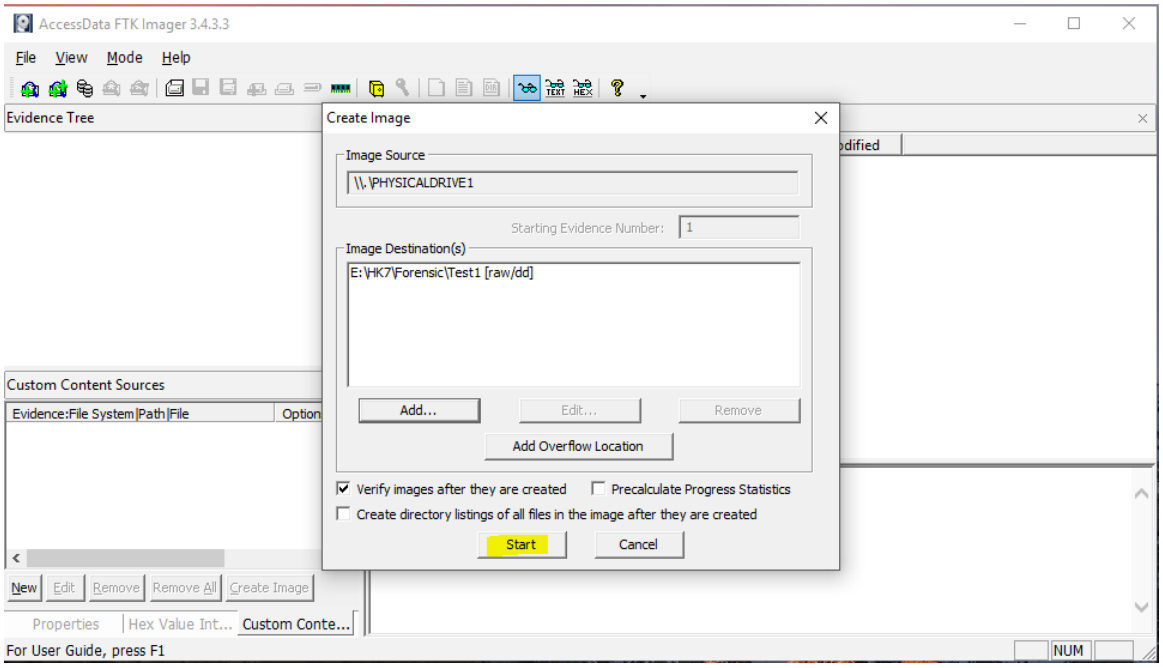


Thực hiện điền thông tin của bằng chứng

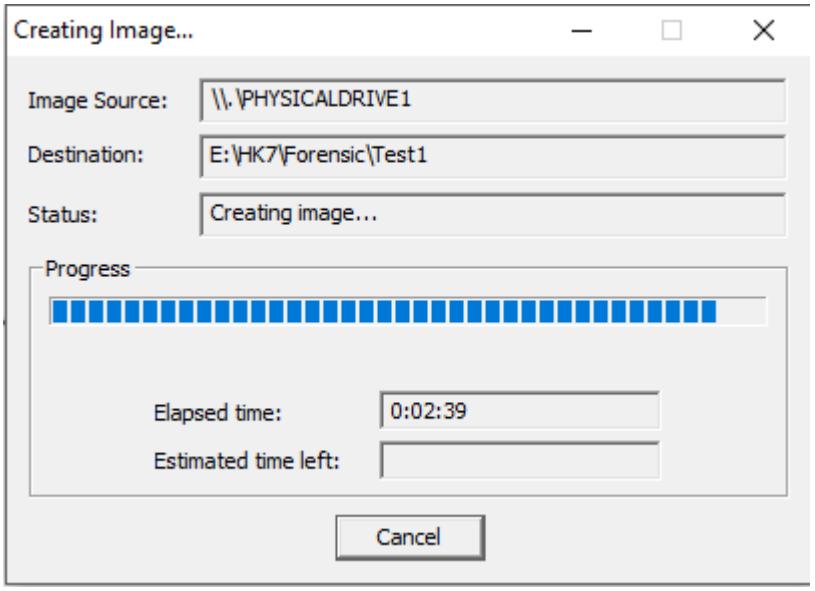


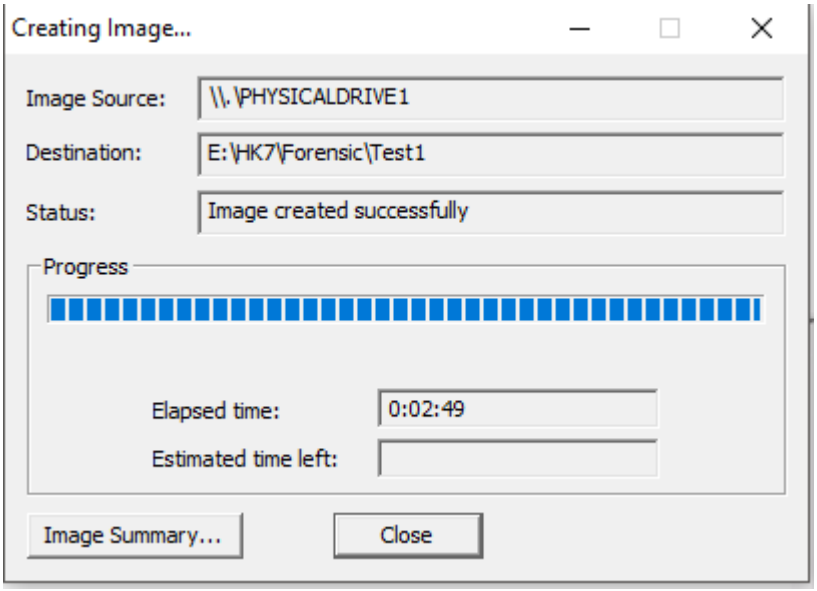
Thực hiện các bước như đặt tên sau đó chọn Start để bắt đầu tạo ảnh đĩa.



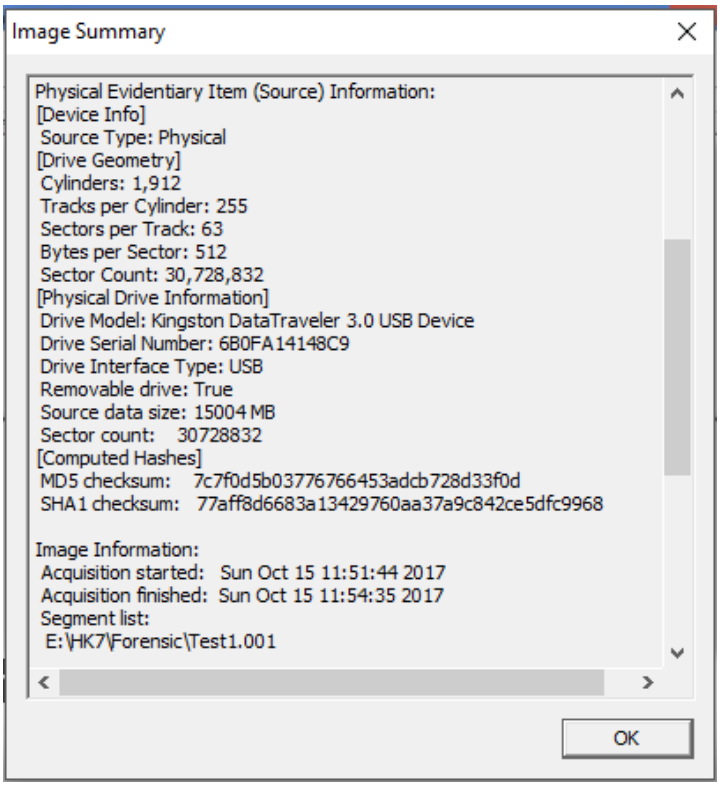


Chọn Start, ảnh đĩa đang được tạo.

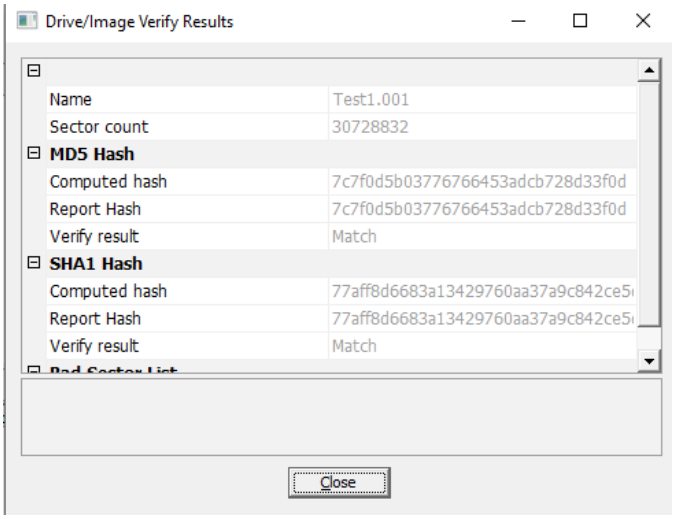




Bảng tóm tắt của ảnh đĩa vừa được tạo xong như sau:



Kết quả, thông tin của ảnh đĩa sau khi tạo như sau:



Kịch bản 03. Thực hiện phân tích theo kịch bản mô tả sau:

- Trên máy tính/máy ảo windows thực hiện tải về hình ảnh và đặt tên ConDao-island.

  Liên kết tải: https://unsplash.com/photos/uXPBXlruX5o
- Thực hiện xóa file ảnh vừa tạo, xóa trong Recycle Bin.
- Tạo một ảnh đĩa -định dạng Raw (dd) sau khi xóa file ảnh trên.
  - Case Number: April_0001
  - Evidence Number: 01
  - Unique Description: Monkey Image
  - Examiner: Your Name (tên của nhóm)
- Tạo một thư mục điều tra dùng cho kịch bản này: KB03, chứa ảnh đĩa đã tạo.
- Thực hiện điều tra, tìm ảnh đã bị xóa trên ổ đĩa bằng công cụ FTK Imager. Sử dụng tính năng phục hồi file ảnh đã bị xóa (tính năng Export Files), lưu trữ file này trong thư mục KB03\images.
- Kiểm tra giá trị hash MD5 của file ảnh vừa được phục hồi với file gốc ban đầu.

Yêu cầu: Các nhóm thực hiện chụp màn hình terminal sau khi hoàn thành điều tra bằng cách gõ các câu lệnh sau:

dir D:\KB03 | findstr "ConDao-island"

date /t

echo "Tên nhóm"

Thí dụ, echo "John, Dung, David, Kris"

B3. Kịch bản tổng hợp

Kịch bản 04. Thực hiện phân tích:

- Tài nguyên: kb04-session02.bin.gz
- Tìm thông tin có liên quan đến từ khóa "key" trong dữ liệu được cung cấp.

Gợi ý: Tìm hiểu các Master File Table (MFT), mmls, dd, strings, foremost/scalpel

Đáp án:

Kịch bản 05. Thực hiện phân tích:

- Tài nguyên: kb05-session02
- Cảnh sát phát hiện một vụ án tình nghi một người đàn ông chết do tự tử. Bằng chứng thu được từ máy tính nạn nhân được gửi cho điều tra viên. Đóng vai làm nhân viên điều tra, hãy tìm manh mối xác định liệu kết luận tình nghi này có đúng hay không.

Đáp án:

Kịch bản 06. Thực hiện phân tích:

- Tài nguyên: kb06-session02.pdf
- Chúng tôi đảm nhiệm vai trò là đội ngũ điều tra viên pháp y trong vụ án tự tử của một thanh niên tên là Eden (đã đổi tên nạn nhân). Anh ta được tìm thấy trong tình trạng đã chết bên ngoài ngôi nhà của mình. Từ những gì đội cảnh sát có thể phục hồi, có vẻ như Eden đã trèo lên mái nhà ba tầng của mình và nhảy xuống vào ban đêm. Eden là một lập trình viên thực sự tài năng tại trường trung học Hacker. Anh ấy luôn có điểm số cao nhất trong lớp. Tuy nhiên, vào đầu ngày hôm nay nhóm điều tra nhận được một tập tin đính kèm pdf có kích thước lớn đáng ngờ, được gửi tới bằng một thư điện tử ẩn danh. Trong bức thư này, chúng tôi cũng nhận được cảnh báo rõ ràng là không được mở trực tiếp tệp tin đính kèm, cũng như gửi nó cho ai khác (thí dụ như chuyên gia điều tra pháp chứng kỹ thuật số có chuyên môn cao như các bạn). Đội ngũ điều tra pháp y của chúng tôi hoàn toàn xuất than từ những sinh viên đại học tốt nghiệp ngành hóa học và sinh học; do đó không có kiến thức liên quan đến điều tra kỹ thuật số. Tuy nhiên, trong trường hợp này, việc điều tra một bằng chứng đáng ngờ từ tập tin đính kèm đáng ngờ này dường như là một manh mối mới. Chúng tôi không thể cung cấp cho nhóm điều tra của các bạn thêm nhiều thông tin khác liên quan đến vụ án, do chính sách bảo mật và kiểm duyệt thông tin được đưa ra bởi hiệu trưởng của ngôi trường mà Eden theo học. Chúng tôi không được phép hỏi các học sinh khác quá nhiều về thông tin liên quan tới Eden, cũng như cha mẹ của anh ta không cho phép phân tích thêm về các vật dụng cá nhân của anh ấy (máy tính xách tay, điện thoại di động, v.v. .). Tất cả chúng ta có là tập tin đính kèm đáng ngờ. Hãy điều tra các thông tin liên quan đến vụ án này theo một số câu hỏi gợi ý sau:
  - Tên trưởng nhóm nhân viên điều tra pháp y là gì?
  - Ai đã gửi thông tin nặc danh tới đội điều tra pháp y?
  - Thông tin đăng nhập của tài khoản truyền thông xã hội của Eden là gì?
  - Mật khẩu cho máy tính xách tay của Alice là gì?
  - Mật khẩu của Bruce là gì?
  - Các thông tin đăng nhập/ bảo mật của trang web NO. CO.?

- Tìm nội dung ghi chú (note/ thư điện tử) về Alice của Eden.
- Giao dịch (transaction) cũ nhất được ghi lại vào ngày nào?
- Tìm thêm manh mối về vụ tự tử của Eden. Có một bức thư điện tử tự thú của Eden đã được gửi. Hãy tìm nội dung bức thư này.

Đáp án:

C. THAM KHẢO

- https://ctf101.org/forensics/what-is-disk-imaging/
- http://www.cse.scu.edu/~tschwarz/coen252_04/Lectures/FPHarddrive.html

D. YÊU CẦU

Bài thực hành được chia làm 2 phần riêng biệt.

- **Class Part (CP):** Sinh viên hoàn thành trên lớp (Bắt buộc).

  0% <= CP< 50%: 1đ

  50% <= CP < 90 %: 5đ

  90% <= CP <= 100%: 10đ

- **Home Part (HP):** Hoàn thành phần còn lại và làm báo cáo sau khi kết thúc buổi thực hành (nộp trên Course môn học theo deadline).
- Điểm Thực hành của mỗi Buổi (Session): **S = (CP + HP)/2**

– Sinh viên tìm hiểu và thực hành theo hướng dẫn.

– Nộp báo cáo kết quả gồm chi tiết những việc bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).

– Sinh viên báo cáo kết quả thực hiện và nộp bài.

Báo cáo:

– File .DOCX và .PDF. Tập trung vào nội dung, không mô tả lý thuyết.

– Chỉ dùng duy nhất 1 loại Font chữ (Times New Roman – cỡ chữ 12)

- Đặt tên theo định dạng: [Mã lớp]-SessionX_GroupY. (trong đó X là Thứ tự buổi Thực hành, Y là số thứ tự Nhóm Thực hành đã đăng ký với GVHD-TH).

  Ví dụ: [NT101.H11.1]-Session1_Group3.

- Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
- Không đặt tên đúng định dạng – yêu cầu, sẽ **KHÔNG** chấm điểm bài Lab.
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Đánh giá: Sinh viên hiểu và tự thực hiện được bài thực hành. Khuyến khích:

- Chuẩn bị tốt và đóng góp tích cực tại lớp.
- Có nội dung mở rộng, ứng dụng trong kịch bản phức tạp hơn, có đóng góp xây dựng bài thực hành.

Bài sao chép, nộp trễ, thực hiện không nghiêm túc ... sẽ được xử lý tùy mức độ vi phạm.

HẾT