**ĐẠI HỌC BÁCH KHOA HÀ NỘI**

**TRƯỜNG CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG**

**A red and white logo

AI-generated content may be incorrect.**

**BÁO CÁO TUẦN 3**

**Môn học: Project II (IT3931)**

**Đề tài: Tìm hiểu ứng dụng autopsy**

|  |  |
| --- | --- |
| **Sinh viên thực hiện:** | **Ngô Trung Hiếu - 20225316**  **Kỹ thuật máy tính 04 – K67** |
| **Giáo viên hướng dẫn:** | **Nguyễn Đức Toàn** |

**Hà Nội – 2025**

Mục lục

[I. Cơ sở lý thuyết 3](#_Toc193787925)

[1. Autopsy 3](#_Toc193787926)

[2. Lệnh dd trong Linux 3](#_Toc193787927)

[a) Cấu Trúc Lệnh dd 3](#_Toc193787928)

[b) File .dd 5](#_Toc193787929)

[II. Ứng dụng Autopsy để theo dõi, quản lý ổ đĩa trên Windows 5](#_Toc193787930)

[1. Điều kiện 6](#_Toc193787931)

[2. Cách xóa toàn bộ dữ liệu ổ đĩa sử dụng Sdelete 9](#_Toc193787932)

[3. Tạo file .dd từ ổ đĩa 10](#_Toc193787933)

[4. Khôi phục file bằng Autopsy 10](#_Toc193787934)

[III. Mục tiêu báo cáo tuần sau 18](#_Toc193787935)

# Cơ sở lý thuyết

## Autopsy

Autopsy là một công cụ phân tích pháp y kỹ thuật số (Digital Forensics Tool) giúp điều tra ổ đĩa, tìm kiếm dấu vết tội phạm, phục hồi dữ liệu bị xóa, và phân tích hoạt động trên hệ thống. Đây là giao diện đồ họa (GUI) của The Sleuth Kit (TSK) – một bộ công cụ pháp y mạnh mẽ dành cho chuyên gia điều tra.

Dùng cho:

* Điều tra tội phạm mạng
* Phục hồi file bị xóa
* Phân tích ổ đĩa, USB, thẻ nhớ
* Khôi phục lịch sử hoạt động người dùng

Ta có thể truy cập vào trang <https://www.autopsy.com/download> để download Autopsy cho Windows/Linux/OS X.

## Lệnh dd trong Linux

Lệnh dd trong Linux dùng để sao chép và chuyển đổi dữ liệu cấp thấp trên ổ đĩa. Nó hoạt động trực tiếp với các thiết bị lưu trữ như ổ cứng, USB, thẻ nhớ, ISO, giúp sao lưu, tạo file ảnh .img/.iso, hoặc ghi dữ liệu một cách an toàn.

### Cấu Trúc Lệnh dd

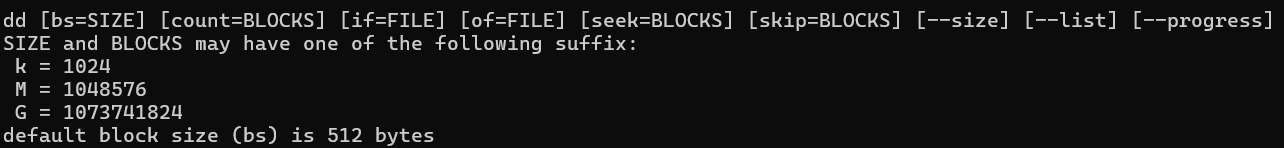


Figure 1: Cấu trúc lệnh dd

**Các Tham Số Cơ Bản**

| **Tham số** | **Ý nghĩa** |
| --- | --- |
| bs=SIZE | Đặt kích thước khối dữ liệu khi đọc/ghi. (Mặc định: 512 bytes) |
| count=BLOCKS | Chỉ định số lượng khối (blocks) cần sao chép. |
| if=FILE | (Input File) Định nghĩa file hoặc thiết bị nguồn cần sao chép. |
| of=FILE | (Output File) Định nghĩa file hoặc thiết bị đích để ghi dữ liệu. |
| seek=BLOCKS | Bỏ qua một số khối đầu khi ghi vào file đích. |
| skip=BLOCKS | Bỏ qua một số khối đầu khi đọc từ file nguồn. |

**Các Tham Số Bổ Sung**

| **Tham số** | **Ý nghĩa** |
| --- | --- |
| --size | Hiển thị kích thước tổng thể của thiết bị hoặc file. |
| --list | Liệt kê tất cả các thiết bị lưu trữ có sẵn trên hệ thống. |
| --progress | Hiển thị tiến trình thực hiện sao chép. |

**Định Dạng Kích Thước SIZE & BLOCKS**

| **Ký hiệu** | **Giá trị tương ứng** |
| --- | --- |
| k | 1 KB = 1024 bytes |
| M | 1 MB = 1048576 bytes (1024 × 1024) |
| G | 1 GB = 1073741824 bytes (1024 × 1024 × 1024) |

**Mặc định:** Nếu không chỉ định bs=, dd sẽ sử dụng 512 bytes.

### File .dd

File .dd (Disk Dump) là một bản sao chép bit-by-bit của ổ đĩa, USB, thẻ nhớ hoặc phân vùng nào đó. Nó được tạo bằng lệnh dd trên Linux/Windows để lưu trữ toàn bộ nội dung của thiết bị lưu trữ thành một file ảnh (image file).

**Đặc điểm của File .dd**

* Sao chép nguyên vẹn dữ liệu, bao gồm cả dữ liệu đã xóa.
* Lưu cả cấu trúc hệ thống tập tin, không chỉ file hiển thị.
* Hỗ trợ phân tích pháp y số, giúp khôi phục file bị xóa.
* Không làm thay đổi dữ liệu gốc, an toàn khi điều tra.

# Ứng dụng Autopsy để theo dõi, quản lý ổ đĩa trên Windows

Mục tiêu của bài báo cáo này là theo dõi và khôi phục lại các file đã bị xóa bằng sử dụng autopsy.

1. Ta phải xóa hoàn toàn dữ liệu từ ổ đĩa.
2. Ta phải tạo file .dd từ ổ đĩa đó (việc tạo file .dd cho ta hình dung được cách thức phân tích các file image disk, bởi vì thường ta sẽ không có **ổ đĩa cần phân tích** có trực tiếp trên hệ thống của ta).
3. Sử dụng Autopsy để phân tích.

## Điều kiện

Em sử dụng 1 ổ cứng HDD ngoài có dung lượng 500GB và tách nó ra thành 1 ổ drive nhỏ hơn có dung lượng 1GB để có thể phân tích nó nhanh hơn.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 2: Ổ H: có dung lượng 1GB

Tuy nhiên, việc tách này không hẳn tạo ra 1 ổ đĩa mới hoàn toàn không có dữ liệu (theo như nó hiển thị), mà các dữ liệu từ các file đã xóa trước từ ổ cứng HDD ngoài vẫn còn trong ổ cứng, nó chỉ được đánh dấu là không có file nào chiếm giữ phần nhớ đó thôi. Nên ta phải sử dụng 1 công cụ khác là **SDelete** để thực sự xóa dữ liệu đi. (<https://learn.microsoft.com/en-us/sysinternals/downloads/sdelete>)

Sau khi giải nén và cài đặt, ta phải thêm đường dẫn đến thư mục đã giải nén đó vào Environment Variables.

A screenshot of a computer program

AI-generated content may be incorrect.

Figure 3 : Thêm đường dẫn vào Environment Variables

Tiếp theo, ta phân tích file .dd (Disk Dump Image) thường được ưu tiên hơn ổ đĩa vì:

* An toàn hơn (tránh ghi đè lên ổ gốc).
* Tốc độ nhanh hơn (phân tích trên file ảnh thay vì ổ vật lý).
* Dễ dàng chia sẻ & sao lưu dữ liệu trong quá trình điều tra.

Nên em sẽ phải chuyển đổi ổ H: sang 1 file .dd để autopsy có thể phân tích được bằng cách sử dụng dd tool. (Link download: <http://www.chrysocome.net/dd>)

A screenshot of a computer

AI-generated content may be incorrect.

Figure 4 : Link download dd tool

Sau đó ta giải nén rồi thêm đường dẫn đến thư mục giải nén trong Environment Variables để có thể sử dụng lệnh dd.

A screenshot of a computer program

AI-generated content may be incorrect.

Figure 5 : Thêm đường dẫn vào Environment Variables

## Cách xóa toàn bộ dữ liệu ổ đĩa sử dụng Sdelete

Ta mở Command Prompt và nhập lệnh “sdelete -c -p 3 -z h:”

Trong đó:

* -c Xóa sạch không gian trống trên ổ đĩa mà không làm mất dữ liệu hiện tại (để tránh khôi phục dữ liệu đã xóa trước đó).
* -p passes Chỉ định số lần ghi đè dữ liệu (mặc định là 1 lần). Giá trị cao hơn giúp tăng mức độ an toàn, nhưng mất nhiều thời gian hơn. Theo như câu lệnh là ghi đè 3 lần.
* -z Ghi đè không gian trống bằng số 0 – thích hợp để tối ưu hóa đĩa ảo (VD: VHD, SSD).
* H: Ổ đĩa đang được phân tích.

A computer screen with white text

AI-generated content may be incorrect.

Figure 6: Kết quả xóa ổ đĩa thành công

Sau đó em tạo 2 file foo.txt và hello world.txt trong ổ H: rồi xóa file hello world.txt đi với mục đích lưu lại hoạt động, sau đó có thể sử dụng autopsy để khôi phục.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 7: file foo.txt

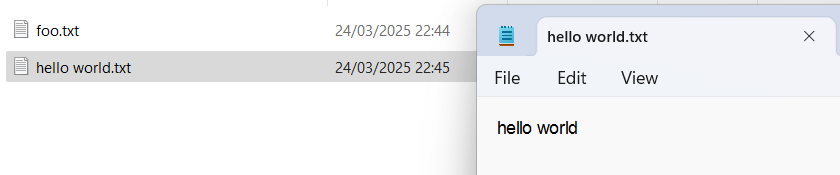


Figure 8: File hello world.txt

## Tạo file .dd từ ổ đĩa

Bây giờ, ta sẽ tạo file .dd từ ổ đĩa H: bằng lệnh dd

**dd if=\\.\h: of=C:\Users\Admin\Desktop\testing\_dd\_file.dd bs=1M --size –progress**

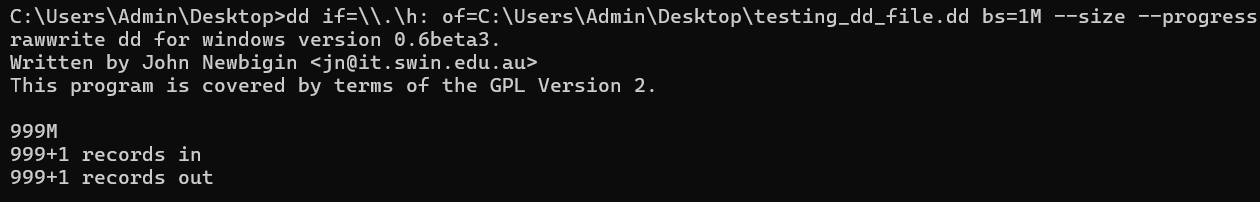
****

Figure 9: Kết quả sau khi chạy xong lệnh dd

Câu lệnh trên có ý nghĩa

* **If=\\.\h:** file đầu vào là ổ đĩa h:
* **of=C:\Users\Admin\Desktop\testing\_dd\_file.dd** là vị trí đặt file đầu ra và chỉ định tên file đầu ra là *testing\_dd\_file.dd*
* **bs=1M** xác định khối dữ liệu là 1 Mega bytes trong mỗi lần sao chép ra file .dd
* **--size** chỉ định câu lệnh dd sẽ dừng sao chép khi nó sao chép xong ổ đĩa H:
* **--process** hiển thị tiến trình thực hiện sao chép.

🡪 Sao chép ổ đĩa h: ra file *testing\_dd\_file.dd* tại vị trí *C:\Users\Admin\Desktop* với tốc độ 1 MB / 1 phép sao chép, dừng sao chép khi sao chép xong ổ h: và hiển thị quá trình sao chép.

## Khôi phục file bằng Autopsy

Ta mở Autopsy và chọn **New Case**

A screenshot of a computer

AI-generated content may be incorrect.

Figure 10: Giao diện Autopsy

Tiếp theo là điền các thông tin cơ bản cho New Case như tên, base directory, thông tin của examiner, case number, rồi chọn Next và Finish.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 11: Thông tin new case (1)

A screenshot of a computer

AI-generated content may be incorrect.

Figure 12: Thông tin New Case (2)

**Chọn data source**

B1: Chọn host hay chọn thiết bị/hệ thống mà đang được điều tra.

Ta chọn mặc định “Generate new host …” cho case mới.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 13: Chọn host

B2: Ta chọn **Disk Image or VM File** (Ảnh đĩa hoặc tệp máy ảo)

* Dùng để phân tích ảnh đĩa pháp y, bao gồm các định dạng như E01, DD, RAW, VMDK (máy ảo VMware), VHD (Virtual Hard Disk).
* Loại này giúp kiểm tra nội dung toàn bộ ổ đĩa hoặc phân vùng một cách chi tiết.

Ngoài ra, nếu ta không tạo ra file .dd mà muốn trực tiếp phân tích ổ đĩa hoặc phân vùng đang kết nối với hệ thống, thì có thể chọn **Local Disk.**

A screenshot of a computer

AI-generated content may be incorrect.

Figure 14: Chọn loại data source

B3: Chọn data source, chọn đường dẫn đến file .dd, và chọn Next.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 15: Chọn data source

B4: Chọn mô-đun xử lý.

Đây là các mô-đun xử lý thể hiện cách thức phân tích dữ liệu để lấy ra các thông tin cụ thể từ data source.

1. **Run ingest modules on** (Chạy mô-đun xử lý trên)

Cho phép chọn phạm vi dữ liệu mà các mô-đun phân tích sẽ chạy, bao gồm:

* *All Files, Directories, and Unallocated Space:* Phân tích tất cả tệp, thư mục và vùng không gian chưa phân bổ.
* *Allocated Space Only:* Chỉ phân tích các tệp và thư mục hiện có.
* *Unallocated Space Only:* Chỉ phân tích không gian chưa phân bổ (dữ liệu đã xóa có thể còn tồn tại).

1. **Một số các mô-đun xử lý** (Ingest Modules)

* *Recent Activity:* Trích xuất hoạt động gần đây của người dùng như lịch sử trình duyệt, mở tệp gần đây, truy cập hệ thống, v.v.
* *Extension Mismatch Detector:* Phát hiện các tệp có phần mở rộng không khớp với nội dung thực tế (ví dụ: tệp .jpg thực chất là một .exe).

Ngoài ra, ta phải *uncheck* 1 số mô-đun mất phí và chỉ dành cho thiết bị di động đó là *Cyber Triage Malware Scanner, iOS Analyzer (iLEAPP), Android Analyzer.* Còn lại ta có thể *check* hết để phân tích các thông tin từ data source.

Rồi bấm Next.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 16: Chọn các mô-đun xử lý

B5: Cuối cùng sau khi chọn hết tất cả đã được configure, Autopsy bắt đầu xử lý.

Bấm finish.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 17: Autopsy bắt đầu xử lý

Đây là giao diện của Autopsy sau khi xử lý xong.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 18: Giao diện Autopsy

Sau đó ta chọn Delete Files 🡪 Chọn All ở phần giao diện bên trái. Để lấy ra danh sách file mà đã bị xóa. Ta có thể tìm file **hello world.txt** mà ta đã xóa trước khi chuyển ổ đĩa h: thành file .dd .

A screenshot of a computer

AI-generated content may be incorrect.

Figure 19: File hello world.txt đã bị xóa

Ta click chuột phải và chọn Extract File(s) để lấy lại file hello world.txt.

Rồi chọn nơi lưu trữ.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 20: Lấy lại file hello world.txt

Và ta đã khôi phục được file hello world.txt

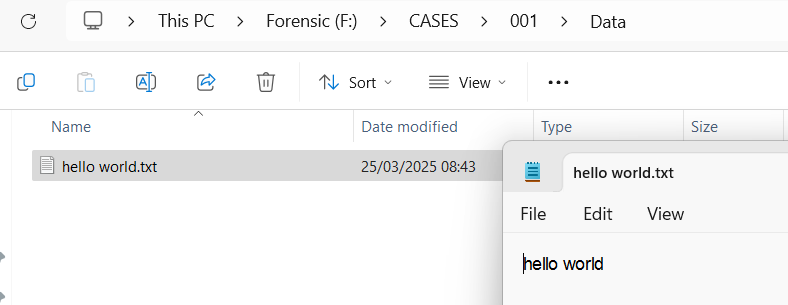


Figure 21: File hello world.txt đã được khôi phục

# Mục tiêu báo cáo tuần sau

Tìm hiểu về các module xử lý của Autopsy, cách hoạt động của các module, và cách sử dụng chúng.

Ngoài ra, học nốt *chapter* *3: windows fundamentals* trong cuốn sách Reversing - Secrets Of Reverse Engineering (2005).

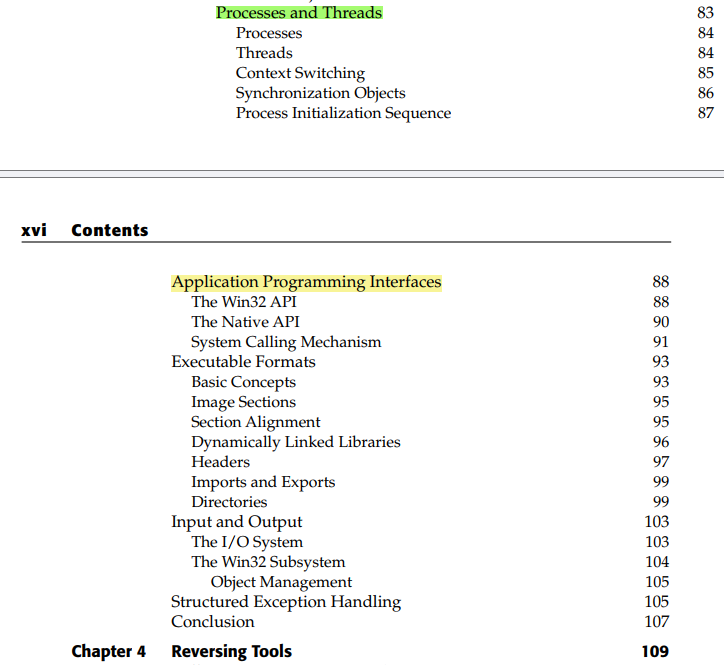


Figure 22: Các chương cần học của chương 3