BÁO CÁO CUỐI KỲ SEMINAR

Môn học: Pháp chứng kỹ thuật số

Nhóm: Pha Pha

THÀNH VIÊN THỰC HIỆN:

STT	Họ và tên	MSSV
1	Nguyễn Đoàn Xuân Bình	19521265
2	Trần Hoàng Khang	19521671
3	Nguyễn Mỹ Quỳnh	19520241

Memory SuperTimeline Analysis

Abstract

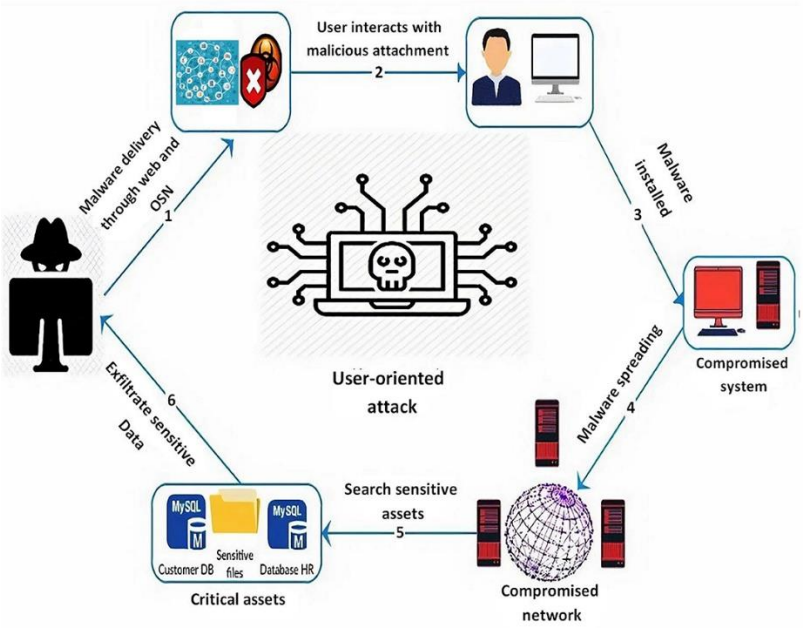
Phân tích dòng thời gian truyền thống có thể cực kỳ hữu ích nhưng đôi khi nó lại bỏ sót những yếu tố quan trọng các sự kiện được lưu trữ bên trong tệp hoặc tạo tác hệ điều hành trên nghi phạm. Bởi chỉ phụ thuộc vào dòng thời gian của hệ thống tệp truyền thống, người điều tra bỏ lỡ ngữ cảnh cần thiết để có được mô tả đầy đủ và chính xác các sự kiện đã diễn ra. Để đạt được mục tiêu này khai sáng, chúng ta cần đào sâu hơn và kết hợp thông tin tìm thấy bên trong các đồ tạo tác hoặc đăng nhập các tệp vào phân tích dòng thời gian của chúng tôi và tạo một số loại dòng thời gian siêu. Này tạo tác hoặc tệp nhật ký có thể nằm trên chính hệ thống đáng ngờ hoặc trong một thiết bị khác, chẳng hạn như tường lửa hoặc proxy. Bài viết này trình bày một khuôn khổ, log2timeline giải quyết vấn đề này vấn đề theo cách tự động. Nó là một khuôn khổ, được xây dựng để phân tích cú pháp các tệp nhật ký khác nhau và tạo tác và tạo ra một siêu thời gian theo cách tự động dễ dàng để hỗ trợ các nhà điều tra trong phân tích dòng thời gian của họ.

1. Introduction:

Phân tích dòng thời gian là một phần quan trọng của mọi cuộc điều tra tội phạm truyền thống. Các cần biết thời gian một sự kiện cụ thể diễn ra và thứ tự có thể thông tin cực kỳ có giá trị cho các nhà điều tra. Điều tương tự cũng áp dụng trong thế giới kỹ thuật số, thông tin dòng thời gian có thể cung cấp cho một chuyên gia pháp y máy tính thông tin quan trọng có thể hoặc giải quyết vụ việc hoặc rút ngắn thời gian điều tra bằng cách hỗ trợ giảm thiểu dữ liệu và chỉ cho người điều tra bằng chứng cần xử lý thêm. Phân tích dòng thời gian có thể cũng chỉ cho điều tra viên bằng chứng rằng họ có thể không tìm thấy bằng cách sử dụng phương pháp truyền thống.

Trọng tâm của phân tích dòng thời gian truyền thống đã được trích xuất và phân tích

dấu thời gian từ hệ thống tệp lưu trữ dữ liệu kỹ thuật số. Mặc dù không phải tất cả các hệ thống tệp lưu trữ cùng một thông tin dấu thời gian về các tệp mà chúng thường có một số dấu thời gian trong thông thường, chẳng hạn như thông tin về lần truy cập cuối cùng và thời gian sửa đổi tệp. Một số hệ thống tệp cũng lưu trữ thông tin về thời gian xóa hoặc tạo tệp hoặc thậm chí thời gian sửa đổi siêu dữ liệu của tệp. Siêu dữ liệu có thể được mô tả là dữ liệu về dữ liệu, hoặc nói cách khác là dữ liệu mô tả hoặc bổ sung thông tin vào nội dung thực tế. Trong ngữ cảnh hệ thống tập tin, đây thường là thông tin về tên của tập tin, vị trí của khối dữ liệu bên trong hệ thống tệp cũng như thông tin về thư mục mẹ lưu trữ dữ liệu. Vì khóa học pháp y SANS, 508, giải thích chi tiết cách tạo và phân tích dòng thời gian của hệ thống tệp truyền thống sẽ chỉ có các tham chiếu nhẹ đến như vậy phân tích trong bài viết này.



2. Artifacts :

Một số Artifacts cơ bản:

Ví dụ trên window ta có:

Prefetch: Kể từ Windows XP, Windows tạo file prefetch mỗi khi bạn chạy ứng dụng lần đầu tiên. File này chứa dữ liệu mà hệ điều hành cần để tăng tốc thời gian load của ứng dụng bất cứ khi nào bạn chạy nó. Và đây là một sự trợ giúp lớn trong quá trình khởi động vì nó giúp Windows load nhanh hơn. Trong file Prefetch (.pf) có lưu những timeline mà ta có thể quan tâm.

Shellbags: cho chúng ta thông tin về thói quen sử dụng của người dùng trên máy tính đó, nó cho người điều tra hình dung được người dùng đó đã truy cập vào những folder nào, tập tin nào đã được mở. Nói cách khác nó sẽ có thể phác họa lại hành vi người dùng qua những thư mục mà họ mở → Điều tra timeline về hành vi người dùng.

Registry: Lưu trữ các thông tin key và value được đăng ký cho hệ thống, những thông tin mật vô cùng quan trọng, và trong chủ đề này thì registry có cung cấp thông tin về timestamp của các services, ứng dụng, … trong hệ thống.

Event Viewer: Ứng dụng lưu lại log và các sự kiện đã xảy ra trên window, rất quan trọng trong việc debug cho User/Dev. Đối với những người forensic thì có thể hiểu rõ

được timeline hoạt động của hệ điều hành.

A. Window (File History):

Trên Window có hỗ trợ một feature (từ phiên bản Window 8+) là File History. Chức năng này cho phép tạo các bản sao lưu các version khác nhau mỗi khi file trong hệ thống có sự thay đổi và có thể đẩy các phiên bản backup này lên các thiết bị lưu trữ ngoại vi. Trong thực tế, ta sẽ luôn bật tính năng này để sau này khi cần ta sẽ có thể forensic lại dấu vết.

a. Usage:

Thiết lập drive cho File History

Trước khi bắt đầu sử dụng File History để sao lưu tệp, trước tiên bạn cần chọn nơi lưu các bản sao lưu của mình. Bạn có thể chọn ổ được kết nối bên ngoài, chẳng hạn như ổ USB hoặc bạn có thể lưu vào ổ trên mạng. Có các lựa chọn khác, nhưng hai lựa chọn này cung cấp các tùy chọn tốt nhất để giúp bảo vệ tệp của bạn khỏi sự cố hoặc các sự cố PC khác.

File History chỉ sao lưu các bản sao của tệp nằm trong thư mục Tài liệu, Nhạc, Ảnh, Video và Máy tính để bàn và các tệp OneDrive khả dụng ngoại tuyến trên PC của bạn. Nếu bạn có các tệp hoặc thư mục ở nơi khác mà bạn muốn sao lưu, bạn có thể thêm chúng vào một trong các thư mục này.

Nếu bạn định sử dụng drive ngoài mới, hãy kết nối nó với PC của bạn. Nếu bạn thấy thông báo hỏi xem bạn có muốn định cấu hình drive cho File History hay không, hãy chọn drive đó, sau đó bật File History trên màn hình xuất hiện.

Nếu không, hãy làm theo các bước sau để chọn drive mạng hoặc drive ngoài đã được kết nối với PC của bạn.

Trượt vào từ cạnh phải của màn hình, sau đó chạm vào Tìm kiếm. (Nếu bạn đang sử dụng chuột, hãy trỏ chuột vào góc dưới bên phải của màn hình, di chuyển con trỏ chuột lên, sau đó nhấp vào Tìm kiếm.)

Nhập cài đặt File History vào hộp tìm kiếm, sau đó chọn cài đặt File History.

Chọn Chọn một drive và chọn mạng hoặc drive ngoài bạn muốn sử dụng.

Bật File History.

Lưu ý: Nếu drive mạng bạn muốn không có trong danh sách các drive khả dụng, hãy chọn Hiển thị tất cả các vị trí mạng. Nếu drive bạn muốn cũng không được liệt kê ở đó, hãy mở File History trong Bảng điều khiển, chọn Thêm vị trí mạng và làm theo hướng dẫn trên màn hình.

Khôi phục tệp hoặc thư mục bằng File History

File History thường xuyên sao lưu các phiên bản tệp của bạn trong các thư mục Tài liệu, Nhạc, Ảnh, Video và Máy tính để bàn và các tệp OneDrive khả dụng ngoại tuyến trên PC của bạn. Theo thời gian, bạn sẽ có toàn bộ lịch sử các tệp của mình. Nếu bản gốc bị mất, bị hỏng hoặc bị xóa, bạn có thể khôi phục chúng. Bạn cũng có thể duyệt và khôi phục các phiên bản tệp khác nhau của mình. Ví dụ: nếu bạn muốn khôi phục phiên

bản cũ hơn của tệp (ngay cả khi tệp đó không bị xóa hoặc bị mất), bạn có thể duyệt qua dòng thời gian, chọn phiên bản bạn muốn và khôi phục nó.

Làm theo các bước sau để khôi phục tệp hoặc thư mục bằng File History:

- Trượt nhanh vào từ cạnh phải của màn hình, chạm vào Tìm kiếm (hoặc nếu bạn đang sử dụng chuột, hãy trỏ chuột vào góc trên bên phải của màn hình, di chuyển con trỏ chuột xuống, sau đó nhấp vào Tìm kiếm), nhập khôi phục tệp của bạn trong hộp tìm kiếm, sau đó chọn Khôi phục tệp của bạn bằng File History.

- Nhập tên tệp bạn đang tìm kiếm vào hộp tìm kiếm hoặc sử dụng mũi tên trái và phải để duyệt qua các phiên bản khác nhau của thư mục và tệp của bạn.

- Chọn những gì bạn muốn khôi phục về vị trí ban đầu của nó, sau đó chọn nút Khôi phục.

- Nếu bạn muốn khôi phục các tệp của mình đến một vị trí khác với vị trí ban đầu, hãy nhấn và giữ hoặc bấm chuột phải vào nút Khôi phục, chọn Khôi phục Đến, sau đó chọn một vị trí mới.

b. Related Artifacts:

- Link tổng quan kiến thức (đã viết trước trên github): Bao gồm thông tin table được lưu trong EDB, file cấu hình và lưu trữ relation XML, thư mục Data cho việc backup bị lỗi, ...
  NT334.M21.ANTN-Digital-Forensic/Deep Understanding-File History.md at main · khangtictoc/NT334.M21.ANTN-Digital-Forensic (github.com)
- Các thông tin cần quan tâm khi điều tra trên feature này: NT334.M21.ANTN-Digital-Forensic/Forensic Analysis.md at main · khangtictoc/NT334.M21.ANTN-Digital-Forensic (github.com)

c. Anti-forensic:

⊗ Files are deleted from external storage:

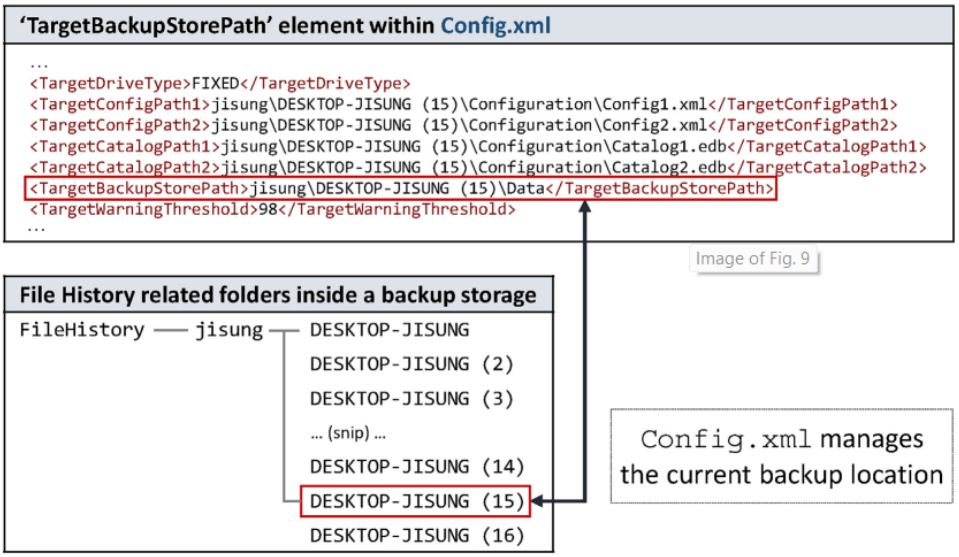
Trong FH có một tính năng là CleanUpVersion (CUV) cho phép xóa các file và thông tin backup trong 1 khoảng thời gian được xác định (Ví dụ: file được backup trong 1 ngày, 1 tháng, 1 năm, ...). Nhưng phiên bản mới nhất của file sẽ không bị thay đổi, luôn được giữ. Tuy vậy việc xóa đi các file backup ở các phiên bản trước sẽ phá hủy cấu trúc timeline của chúng ta mong muốn

➔ Thực chất việc xóa file này chỉ xóa các thông tin liên quan trên bảng namespace của file **Catalog1.edb** và xóa file đó giống như bằng tay**.** Lưu ý ở đây việc xóa như vậy là không an toàn vì giá trị (nội dung) các file vẫn nằm trong *unallocated area* và có thể khôi phục lại bằng phần mềm chuyên dụng, miễn sao vùng nhớ đó chưa bị ghi đè. Vậy nên cách này không thể hoàn toàn anti-forensic.

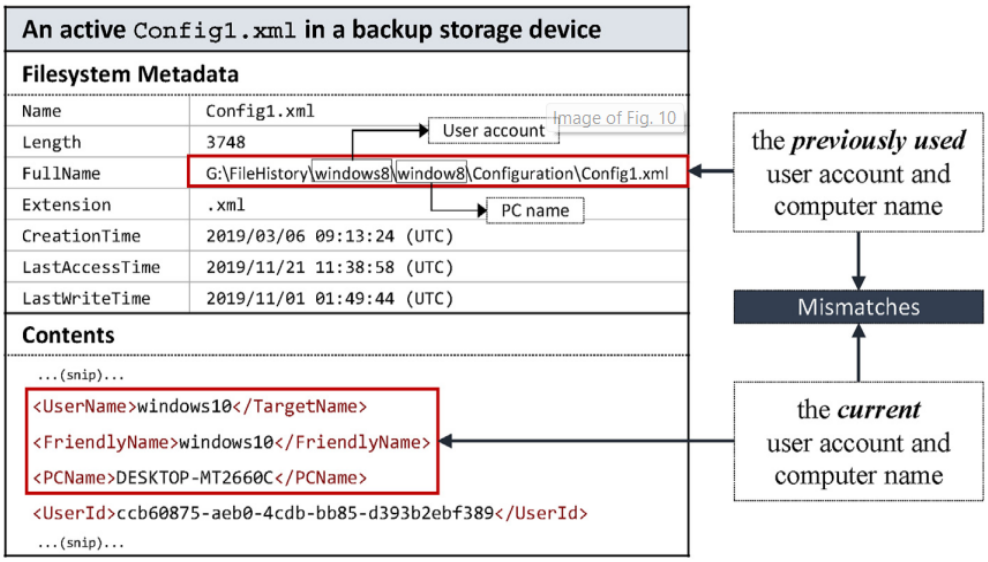
⊗ Disabling and re-enabling of a backup storage device

Ngắt/Tái kích hoạt một thiết bị backup có ảnh hưởng đến việc sao lưu hay không? Kết quả có bị overwrite không ? Câu trả lời là không. FH cho phép nhiều bản sao lưu của nhiều máy tính khác nhau trên cùng một thiết bị lưu trữ và ngược lại, một bản sao lưu có thể lưu trên nhiều thiết bị khác nhau. Thông tin được lưu trong file cấu hình XML trên máy host(máy cần backup thư mục) sẽ lưu thông tin metadata của tình trạng backup folder hiện tại.

Còn thông tin được lưu trong file cấu hình XML trên thiết bị ngoại vi sẽ được tạo ra một thư mục mới mỗi lần thực hiện backup. Và trên backup storage có thể chứa các bản sao lưu trước đó trên nhiều máy tính khác.



Điều này có thể làm cho một số trường thông tin trên file XML giữa Host và backup storage bị mismatch. Nhưng quá trình backup vẫn thực hiện chính xác từ host đẩy qua backup storage.



➔ Không thể anti-forensic

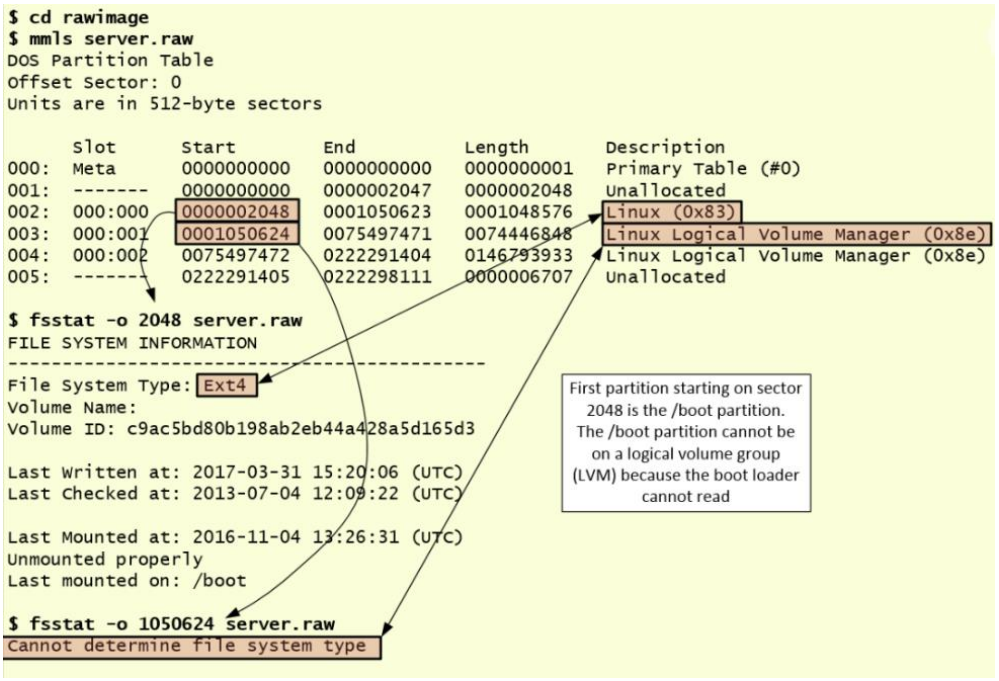
⊗ Disconnecting an active backup storage device

Việc disconnect một thiết bị backup đang trong quá trình thực hiện sao lưu (với dung lượng lớn việc backup sẽ mất nhiều thời gian) thì ngay lập tức sẽ kích hoạt một log event gửi về cho Event Viewer cảnh báo. File backup tất nhiên sẽ không được hoàn tất trên thiết bị lưu trữ, nhưng bù lại FH có cơ chế sao lưu các file backup đích vào tạm vào folder **Data** trên máy host ➔ Không thể anti-foresic

➔ Nếu kỹ lưỡng thực hiện nhiều biện pháp anti-forensic khác nhau thì tất nhiên sẽ không để lại dấu vết (suy nghĩ cá nhân). Nhưng đồng thời sẽ mất rất nhiều thời gian.

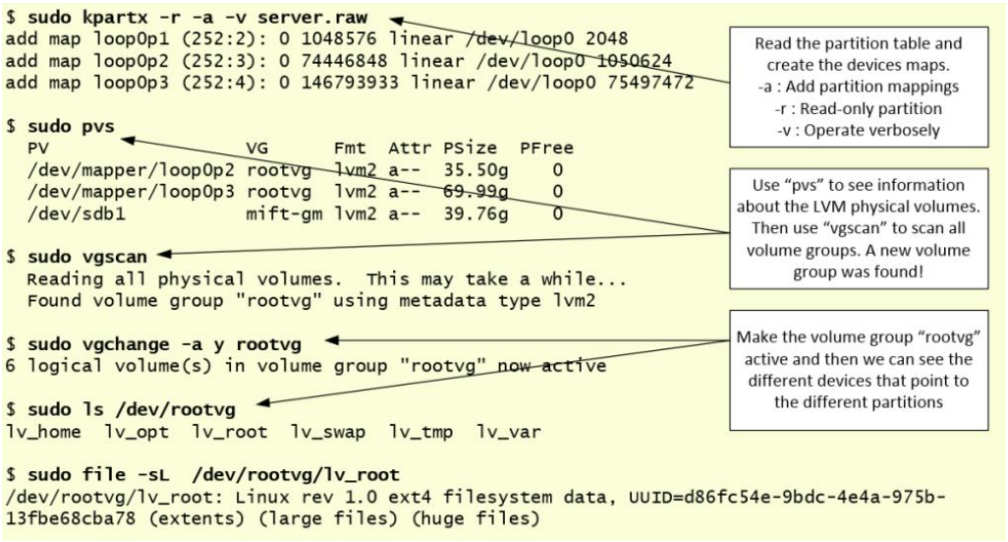
B. Linux:

Step 1. Thông thường trên Linux để forensic được một raw image thì ta phải map image vào một partition của ổ đĩa (không biết hiện tại có tool gì không vì mình tìm chưa ra). Dùng lệnh mmls để xem đầu vào các sector.



➔ Chọn 1 sector để xem thông tin và map. Theo hình trên sector thứ 003 không thể xem thông tin vì đây là LVM partition nên boot loader không thể đọc

Step 2. Sử dụng kpart để tạo các loop partition sao cho hợp lệ với file raw.



Sau đó dùng pvs hoặc vgscan để xem thông tin trạng thái các loop. Rồi thực hiện vgchange tạo và hoàn thành volume group để kích lên trạng thái active.

Step 3. Tạo các thư mục ứng với 6 loop partition đã tạo trên. Mount các loop vào thư mục đích đã tạo

```
$ cd ..
$ mkdir disk_mount
$ mkdir disk1_mount/home/
$ mkdir disk1_mount/opt
$ mkdir disk1_mount/swap
$ mkdir disk1_mount/tmp
$ mkdir disk1_mount/var

$ sudo mount -o ro /dev/rootvg/lv_root disk1_mount/
$ sudo mount -o ro /dev/rootvg/lv_var disk1_mount/var/
$ sudo mount -o ro /dev/rootvg/lv_opt disk1_mount/opt/
$ sudo mount -o ro /dev/rootvg/lv_home disk1_mount/home/
$ sudo mount -o ro /dev/rootvg/lv_tmp disk1_mount/tmp/
```

Create a folder structure that will be used to mount the different partitions

Step 4. Sau khi mount xong thì ta thực hiện forensic như trên window. Ví dụ mình dùng tool **log2timeline** của **Plaso** để tự động trích xuất các timeline artifacts hoặc có thể tìm bằng tay.

```
$ sudo log2timeline.py -z Etc/GMT -t / -p --parsers linux timeline.plaso.disk1 disk1_mount/
Source path                             : /data/disk_mount
Is storage media image or device        : False
2017-04-08 19:54:49,481 [INFO] (MainProcess) PID:2508 <frontend> Starting extraction in multi pro
2017-04-08 19:54:49,566 [INFO] (MainProcess) PID:2508 <frontend> Starting storage process.
2017-04-08 19:54:49,567 [INFO] (MainProcess) PID:2508 <frontend> Starting collection process.
2017-04-08 19:54:49,569 [INFO] (MainProcess) PID:2508 <frontend> Starting worker processes to ext
(..)
2017-04-08 22:16:54,939 [INFO] (MainProcess) PID:2547 <frontend> Processing is done, waiting for storage to complete.
2017-04-08 22:16:56,951 [INFO] (StorageThread) PID:2553 <storage> [Storage] Closing the storage, number of events processed:
540674
2017-04-08 22:16:56,957 [INFO] (MainProcess) PID:2547 <frontend> Storage is done.
2017-04-08 22:16:56,957 [INFO] (MainProcess) PID:2547 <log2timeline> Processing completed.

$ psort.py -z Etc/GMT timeline.plaso.disk1 -o L2tcsv -w filter-timeline.plaso.csv
[INFO] Output processing is done.
[INFO]
********************************** Counter ***********************************
[INFO]              Stored Events : 540674
[INFO]           Events Included : 540674
[INFO]        Duplicate Removals : 94280
```

Create a Supertimeline using the Linux parsers.
-z : Specify the timezone
-p : Activate post-processing

Use psort.py to convert the supertimeline into your favorite format. In this case I will use CSV

Note: Trong phần này mình không đi sâu vào các timeline artifacts trên linux, mình chỉ dừng tới đây.

C. Web:

Trên web thường điều tra timeline bằng công cụ nổi tiếng WayBack Machine:

https://archive.org/web/

D. Demo:

File History

Window Memory Timeline forensics

Log2Timeline-DiskImage