Data and Stream Extrator

Image Ram

Đặt vấn đề: Khi tiếp cận 1 case incident, việc đầu tiên mình nên nghĩ tới là thu thậm dữ liệu từ RAM của máy tính. Đối với window mọi chuyện sẽ dễ dàng nhất vì sự tiện lợi khi có công cụ hỗ trợ (FTK image). Vì sao phải thu thập dữ liệu từ RAM? Thứ nhất dữ liệu của RAM thay đổi liên tục, các process bật rồi tắt, thao tác người dùng (Đánh máy, copy, đọc file, ….). Thứ 2 trường hợp mã độc dù con mã độc có ẩn đến đâu thì khi thực thi nó vẫn phải ló đầu lên, cho dù trường hợp có lấp sau ứng dụng khác, hay nó đã nằm sâu trong máy tính đến anti virus cũng bị qua mặt. Nhưng nếu tắt máy gần như giữ liệu của RAM sẽ bay hơi (có thể còn trong SWAP, pagefile,…)

Các thông tin có thể có từ RAM:

- Processes
- Network Connection
- Open file, Registry keys and devices
- Configuration parameters
- Encryption key and passwords (disk encryption)
- Memory-only exploits / root kit

Phương pháp thu thập RAM

- Khi máy còn mở (Live System)

  Sử dụng các công cụ đọc RAM, các công cụ này sẽ load 1 system drive để xin quyền truy cập xuống (kernel-level access) Memory và đọc nội dung rồi lưu vào file. Nếu đứng trên góc độ là mã độc đây cũng là 1 hành vi độc hại, nên 1 số tool sẽ bị anti virus coi là độc hại nếu không được digitally signed

  Công cụ sử dụng: **FTK image, DunmpIT, WinPMEM, Redline**, …

- Khi máy tắt (DEAD System)

  Khi máy tắt vẫn có 1 số file chứa thông tin của RAM cần lưu ý thu thập: **hiberfil.sys** (hibemation mode), **pagefile.sys**

Lưu ý: đối với RAM không thể kiểm tra tính toàn vẹn của nó trước và sau khi dump (hash) vì bản chất là dữ liệu động, ngay hành động chạy công cụ để dump đã tác động thay đổi RAM.

Check for Disk Encryption

Đặt vấn đề: Sau khi thu thập được dữ liệu từ RAM, thứ tiếp theo cần thu thập là dữ liệu ổ cứng. Đơn giản là, rút ổ cắm, tắt máy, rút ổ cứng rồi clone. KHOAN dừng lại chừng 5s trước khi rút nguồn, tắt máy hãy kiểm tra sơ qua ổ cứng, trường hợp nếu máy được cấu hình cơ chế mã hóa ổ cứng thì sao. ĐÓ ĐÓ, nên hãy bình tĩnh kiểm tra xem ổ cứng có thiết lập cơ chế mã hóa không đã.

Phương pháp kiểm tra: đơn giản là dùng tool thôi, bạn có thể dùng EDD

Create Quick Triage Image

Vấn đề: quá rõ ràng việc clone, hay copy dữ liệu ổ cứng ra một hay nhiều bản là điều tiên quyết (tất nhiên vẫn có thể bạn thao tác trên evidence nhưng nó sẽ đá bay cơ sở pháp lý của bạn). Việc sao chép ổ cứng vừa đảm bảo tính khách quan của kết quả, vừa không làm mất dữ liệu quan trong nếu vô tình bạn xóa trong quá trình điều tra.

Phương pháp thu thập

- Làm sống (live): sử dụng phần mềm FTK Imager's Custom Content Creation, với công cụ này bạn được lựa chọn dữ liệu nào cần lấy (tất nhiên đối với người có kinh nghiệm) để tích kiệm thời gian sao chép hoặc cũng là để lấy các dữ liệu thành image nhỏ hơn để phân tích
- Làm ổ cứng riêng lẻ (DEAD): dùng công cụ thiết bị vật lý, ở đây các thiết bị này có khả năng Block Write, có nghĩa là nó chỉ đọc dữ liệu chứ không ghi. Ở đây nếu cắp trực tiếp ổ cứng vào máy điều tra, chính cái máy điều tra sẽ có thể ghi dữ liệu vào ổ đĩa dù chưa làm gì. Các thiết bị có thể là
    - Phần cứng: FREDDIE forensics, Tableau Forensic Bridges, cru usb 3.0 write blocker, Ultra dock
    - Phần mềm: SAFE Block

Begin analysis of Trage Image

Image Mounting

Đặt vấn đề: Sau khi đã thu thập dữ liệu bộ nhớ thành file image, lúc này đến lúc mount Image ra máy forensics workstation bắt đầu phân tích

Các loại image: Tùy vào công cụ, cách thức sao chép dữ liệu bộ nhớ mà file image ở các dạng khác nhau. Trong đó phổ biến gồm các loại sau: RAW/DD, E01 (Encase Image File Format), S01, AD1, and L)1 images.

Công cụ đọc file image: **FTK Imager, Arsenal Image Mounter**

Windows Filesystems

Đặt vấn đề: Trước tiên hãy lược qua các loại File System (Structure Information). Mình hiểu nôm na như bất động sản là cách quy hoạch đất, mỗi tài sản căn nhà, cây trồng ..v.v sẽ là dữ liệu sẽ đặt trên mảnh đất đó. Vậy sẽ phân bổ dữ liệu thế nào để tối ưu lưu dữ liệu nhiều nhất, truy xuất nhanh nhất,…

FAT 12/16	MS-DOS, Win98/NT/2000
FAT 32	Win95/2000/XP/2003/Vista/win7/8
ExFAT	2008/2012
Windows NTFile System (NTFS)	Win XP/ 2003/2008/2012/Vista/win7/win8
ReFS	Server2012

Mỗi loại sẽ có thông số lưu tối đa dữ liệu khác nhau. Do cách lưu, tao tác dữ liệu khác nhau.

Hiện giờ loại NTFS là phổ biến, thời kỳ thống trị do có nhiều ưu điểm sau. Có 1 số tính năng mà sẽ hỗ trợ trong quá trình điều tra

NTFS Timestamps: NTFS có 4 loại thời gian liên quan đến file:

- Last modification time of file data
- Last access time of file data
- Last modification of the MFT record
- File creation time of MFT record in the volume.

Các rule **Timestamps** khi thao tác file gồm có: copied, accessed, modified, created file.

- Copy: Modified - Inherited from original file, Access — Changed, Creation — Changed
- File Access: Modified — No Change, Access — Changed, Creation — No Change
- File Modify: Modified — Stamped, Access — No Change, Creation — No Change
- File Access: Modified — Change, Access — Change, Creation — Change

Các ẩn dữ liệu vào stream:

```
notepad.exe testfile.txt:hiden.txt
```

The ADS Zone.Indentifier: Hiểu đơn giản đây là 1 trong các thuộc tính của 1 file trong (NTFS). THông tin nó mang lại cung cấp cho ta biết file đó từ internet hay từ biết bị (USB). Dù file có được move sang chỗ khác thì thuộc tính và dữ liệu của nó cũng không thay đổi

NoZone = -1 MyComputer = 0 Intranet = I Trusted 2 Internet = 3 Untrusted = 4

Cách thức kiểm tra:

- KT bằng Powershell:

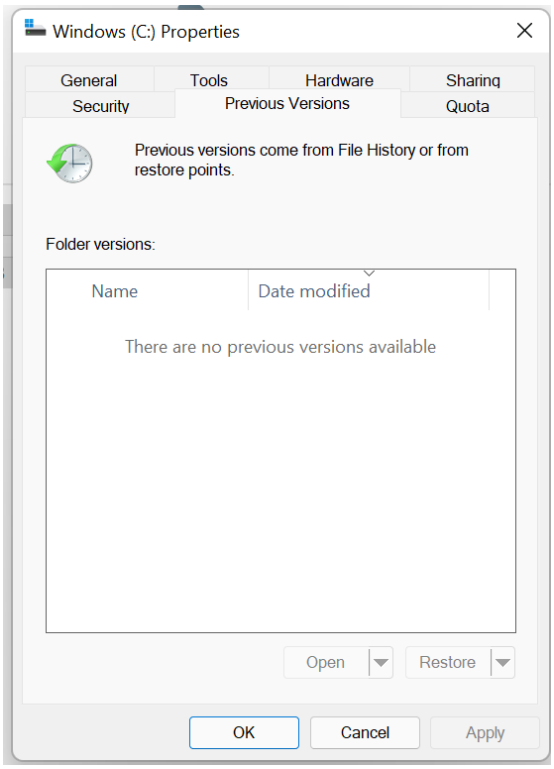
```
\ > Get-Item -path log-file.png -stream *
Stream          : Zone.Identifier
Length          : 168
```

```
\ > Get-Content -path log-file.png -stream Zone.Identifier
[ZoneTransfer]
ZoneId=3
ReferrerUrl=https://uxwing.com/log-file-icon/
HostUrl=https://uxwing.com/wp-content/themes/uxwing/download/04-file-folder-type/log-file.png
```

- Bằng tool: AccessData FTK Imager

Windows Volume Shadow Copy: Đây là 1 cơ chế backup ổ đĩa, lưu lại bản sao (snapshot) trong 1 ngày hoặc 1 vài ngày. Nghĩa là nếu bạn lỡ xóa file ngày hôm nay, thì có thể phục phiên bản từ hồi ngày hôm trước. Mình nghĩ sẽ rất tiện cho các ổ SSD, vì loại này thường rất khó để phục hồi dữ liệu sau khi xóa (Shift-Del).

Để kiểm tra các phiên bản sao lưu của ổ đĩa có thể vào phần **Properties**



- Bằng câu lệnh trên máy live:

C:\> vssadmin list shadows /for=C: Kiểm tra danh sách các bản sao của ổ C
C:\> mklink /d C:\shadowcopy21 \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy21\ Tạo Symbolic link đến bản sao

- Bằng công cụ sau khi mount image

Step 1: Mount disk image in **Arsenal Image Mounter** in "Write Temporary" Mode. Step 2: Launch **ShadowExplorer** as Administrator Step 3: Browse Snapshots. Step: 4 Extract Files using Right Click -> Export

Data Carving:

Là để chỉ kỹ thuật phục hồi dữ liệu ở mức xâu, có thể từ memory/Pagefile, Unallocated space, ... Có 2 loại Data Carving hiện nay là Data Stream Carving và Data file Carving. Data Stream Scarving là thu thập từng mảnh nhỏ data chứ không file nguyên 1 file. Trường hợp xóa 1 file thì phần không gian vùng chứa file đó có thể đã bị ghi đè 1 phần nên phục hồi nguyên file là không thể, nhưng phần còn lại của file thì vẫn còn và có thể phục hồi. File Carving sẽ phục hồi được nguyên vẹn file. Các công cụ theo trường phái file carving thường sẽ đọc nội dung Boot Sector để xác định cluster size, rồi đọc dữ liệu trong filesystem, kiểm tra header file.

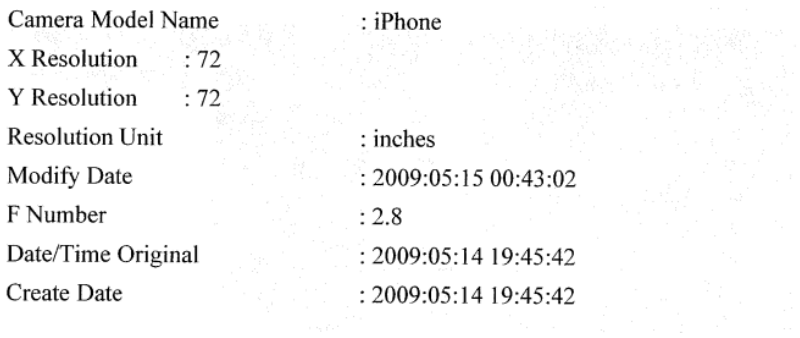
Công cụ để phục hồi dữ liệu:

- Stream carving: The Internet Evidence finder (IEF), bulk extrator

- File carving: photorec

Internal File Metadata: Mỗi file ngoài nội dung nó còn có các thông tin thuộc tính của file đi kèm. Chẳng hạn file tài liệu doc thì có thuộc tính title, version của MS office word, file ảnh thì có EXIF Data, GPS, camera model. Các thông tin này rất hữu ích khi phân tích 1 file. Điều này rất quan trọng, để tránh file bị thay đổi extension nhằm qua mặt điều tra viên

Công cụ sử dụng kiểm tra: exiftool



Camera Model Name	: iPhone
X Resolution : 72	
Y Resolution : 72	
Resolution Unit	: inches
Modify Date	: 2009:05:15 00:43:02
F Number	: 2.8
Date/Time Original	: 2009:05:14 19:45:42
Create Date	: 2009:05:14 19:45:42