TRƯỜNG ĐH CÔNG NGHỆ THÔNG TIN
KHOA MẠNG MÁY TÍNH & TRUYỀN THÔNG

Digital Forensics
Pháp chứng Kỹ thuật số

#4: Memory Forensics

Spring 2022

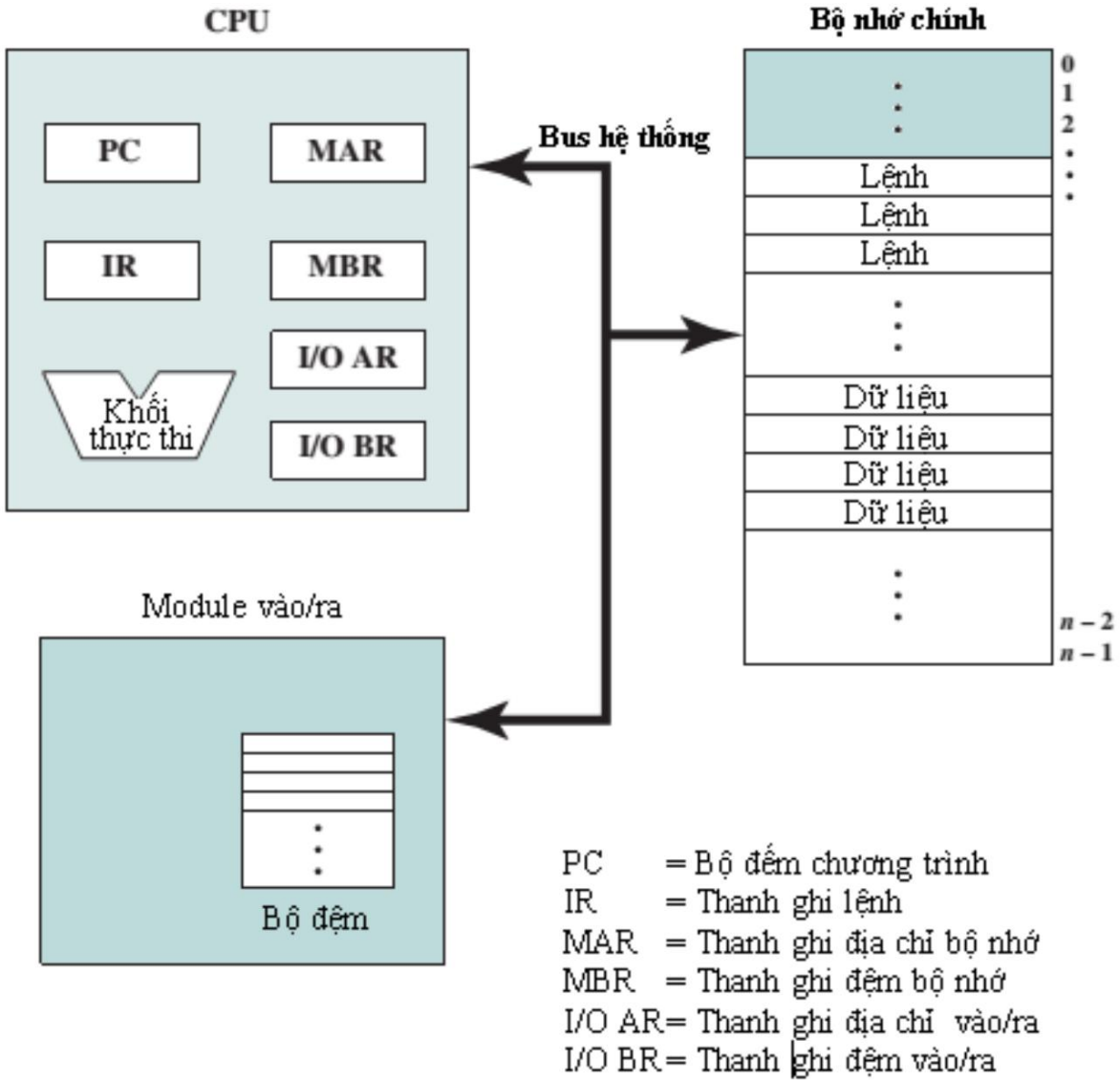
ThS. Lê Đức Thịnh
thinhld@uit.edu.vn

Nội dung trình bày

- Hoạt động của bộ nhớ máy tính?
- Vì sao cần pháp chứng bộ nhớ máy tính?
- Phương pháp thực hiện pháp chứng bộ nhớ?
- Các công cụ thực hiện pháp chứng bộ nhớ?

Kiến trúc máy tính

- Chức năng cơ bản của máy tính là gì?
- Máy tính được cấu thành bởi những thành phần cơ bản nào?



Hình 3.2. Các thành phần máy tính

Cell nhớ?

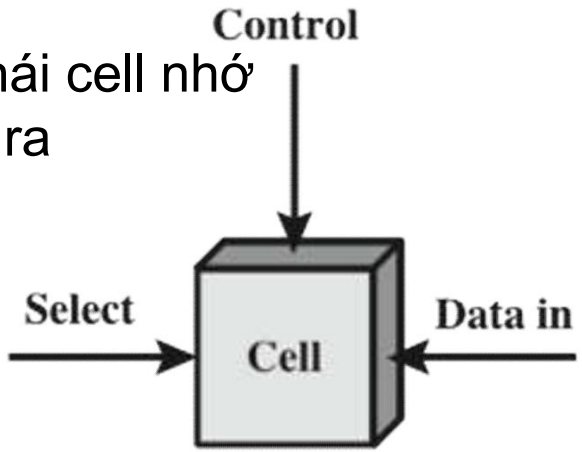
Cell nhớ là phần tử nhớ được 1 bit thông tin

Tính chất cell nhớ

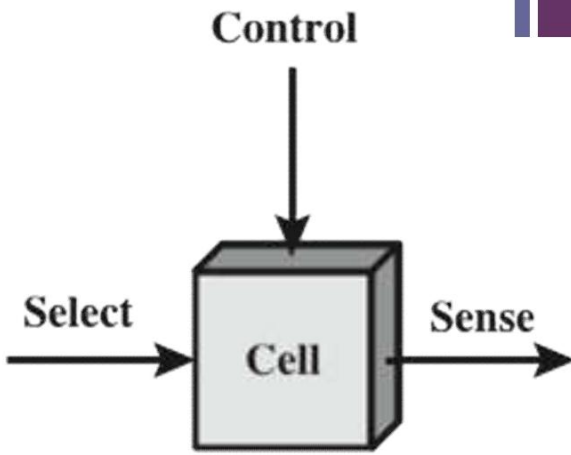
- Hai trạng thái ổn định
- Có thể ghi vào cell nhớ để thiết lập trạng thái
- Có thể đọc cell nhớ (cảm nhận trạng thái)

Các tín hiệu

- Tín hiệu select - chọn 1 cell nhớ
- Tín hiệu control - chỉ định đọc hoặc ghi
- Dữ liệu
- Data in: đặt trạng thái cell nhớ
- Sense: dữ liệu đầu ra



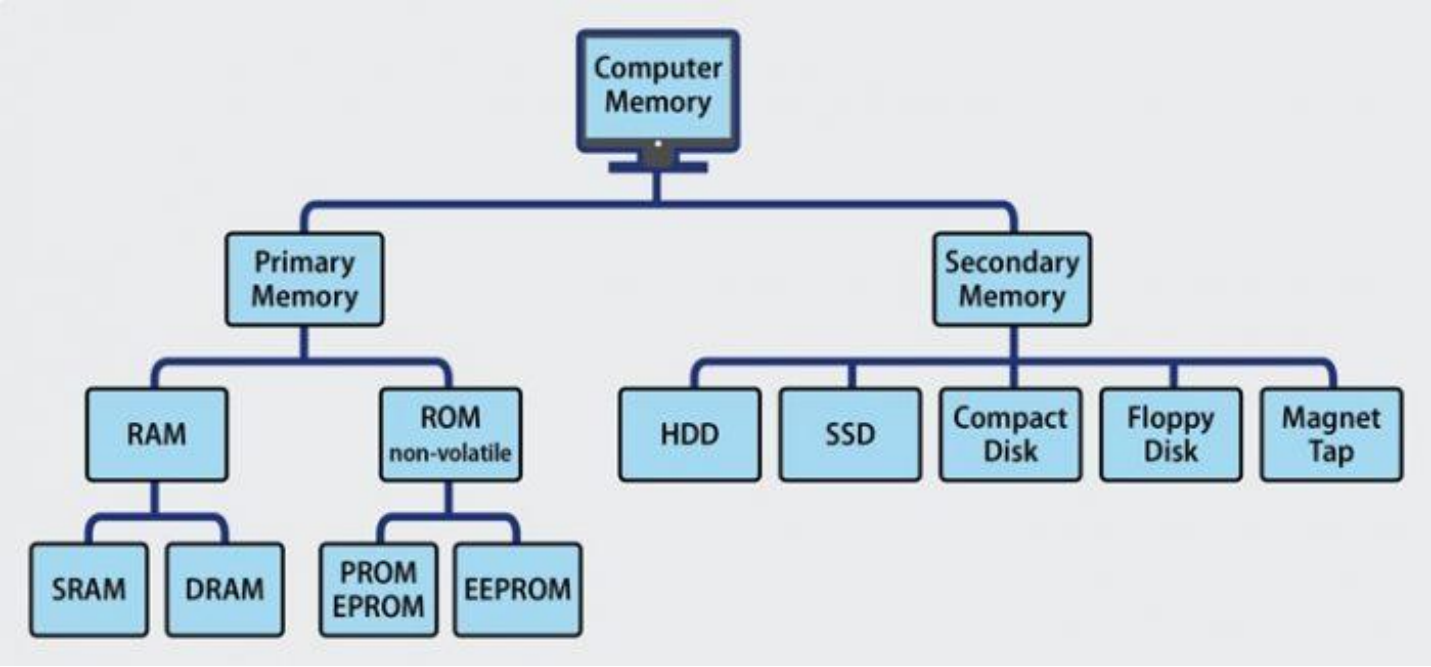
(a) Write



(b) Read

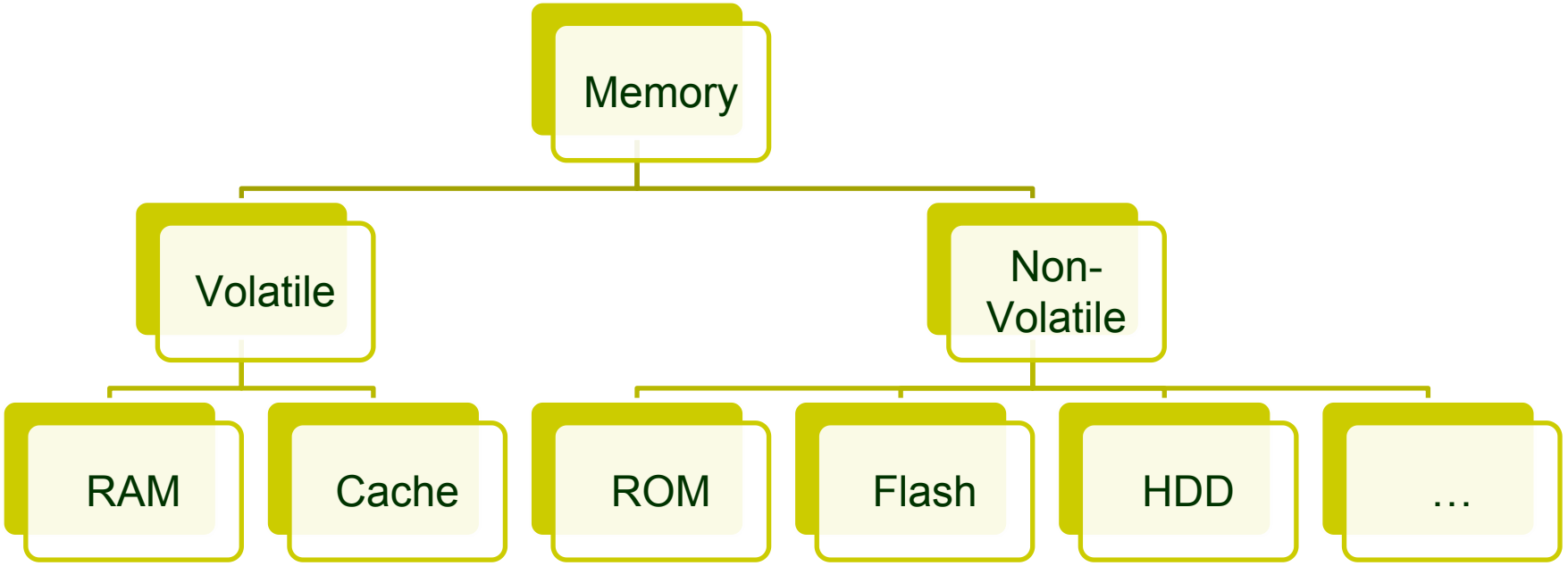
Bộ nhớ - Memory?

- Bộ nhớ máy tính là gì?
- Hãy kể tên các loại bộ nhớ máy tính?
- Cho biết những vị trí đặt của bộ nhớ máy tính?



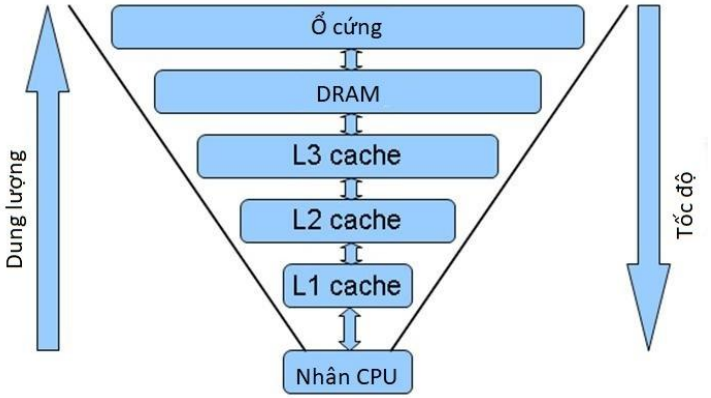
Bộ nhớ - Memory?

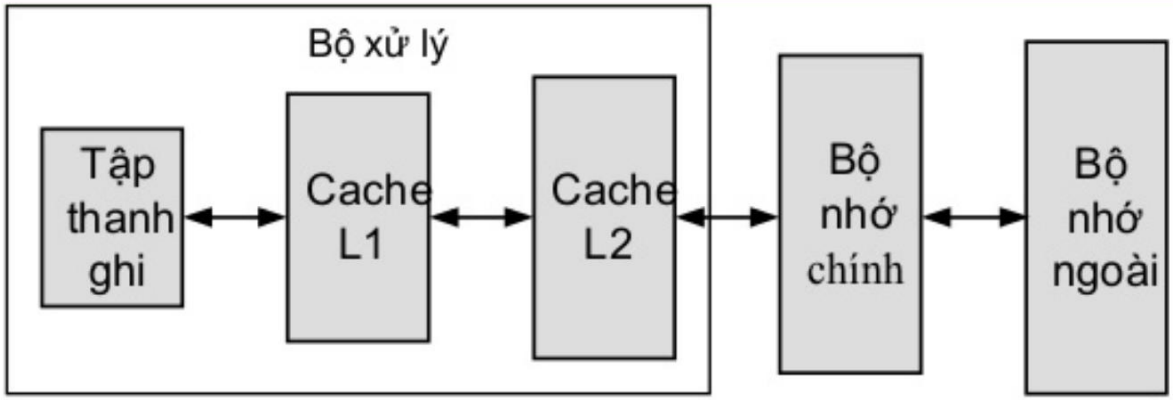
- **Phân loại theo đặc trưng vật lý:**



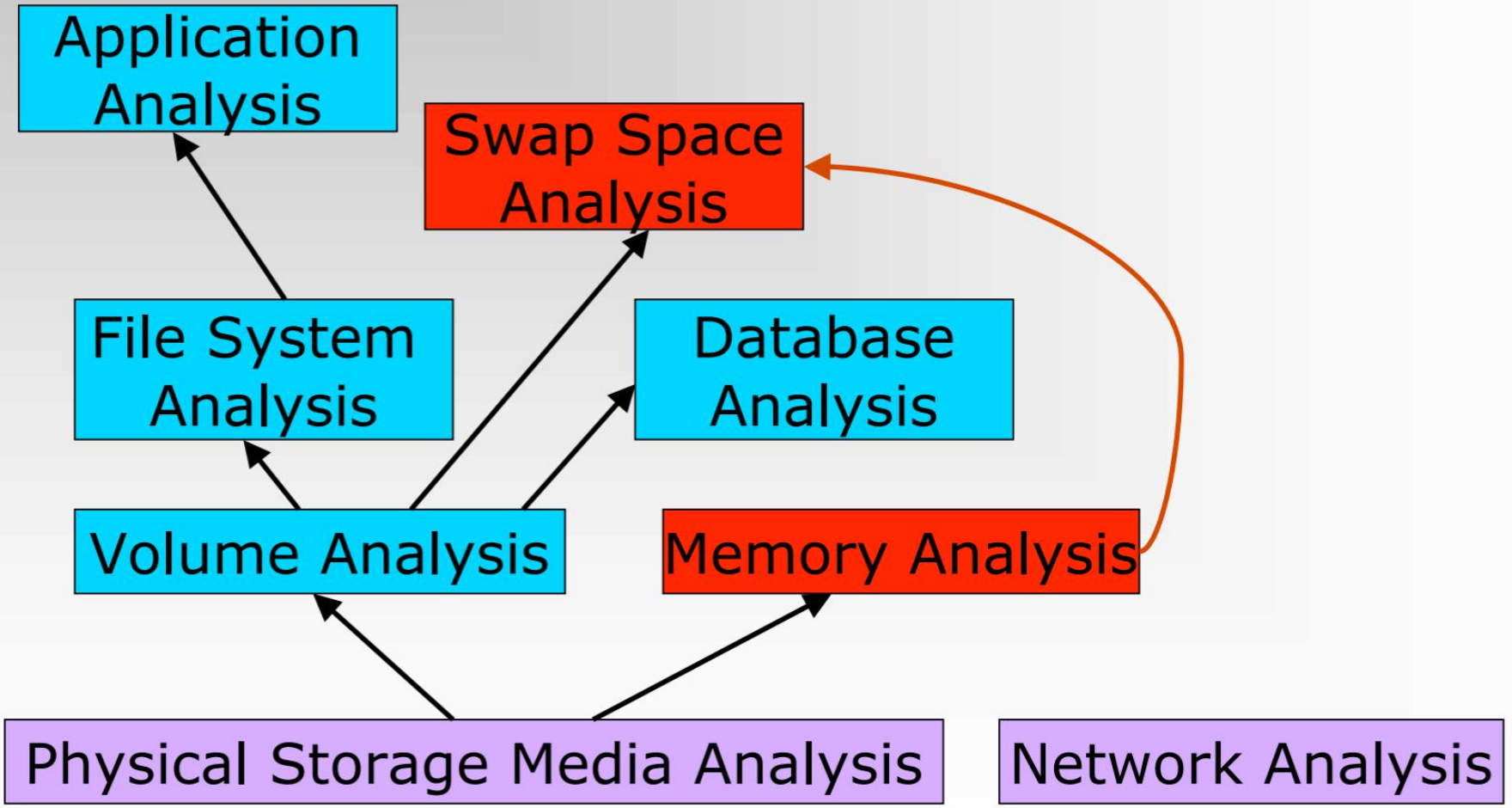
Phân cấp hệ thống nhớ

- **Từ trái sang phải:**
  - Dung lượng tăng dần
  - Tốc độ trao truy xuất dữ liệu giảm dần
  - Giá thành trên 1 bit giảm dần
  - Tần suất CPU truy cập giảm dần
  - Mức trái chứa 1 phần dữ liệu của mức phải



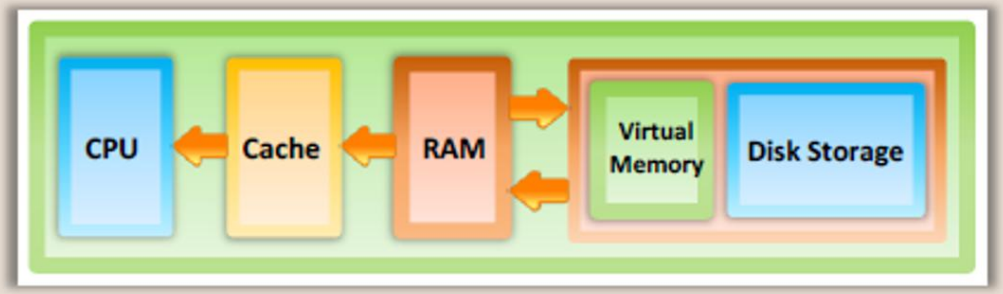


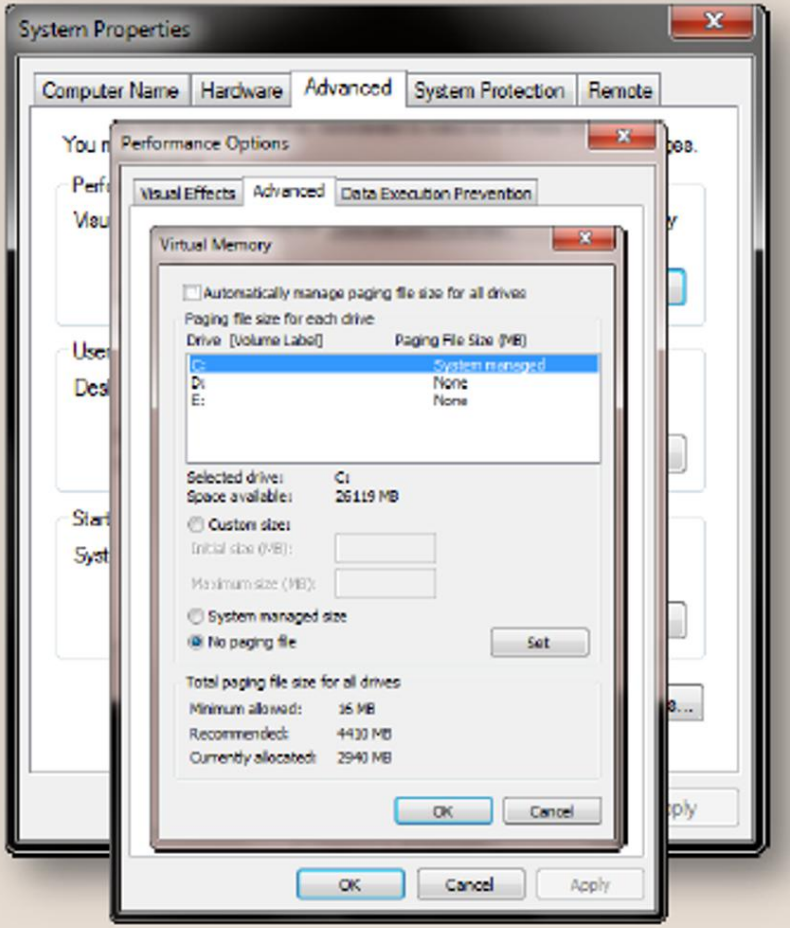
Analysis Types



Virtual Memory

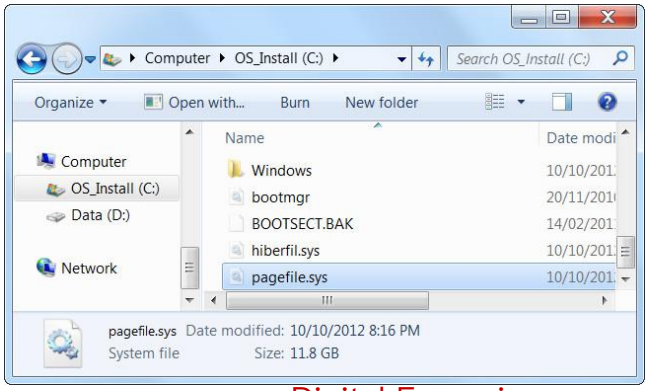
- Virtual (or logical) memory is a concept that, when implemented by a computer and its OS, allows programmers to use a large range of memory or storage addresses for stored data
- Virtual memory can be scanned to find out the hidden running processes
- Use X-Ways Forensics tool to scan virtual memory





Pagefile.sys?

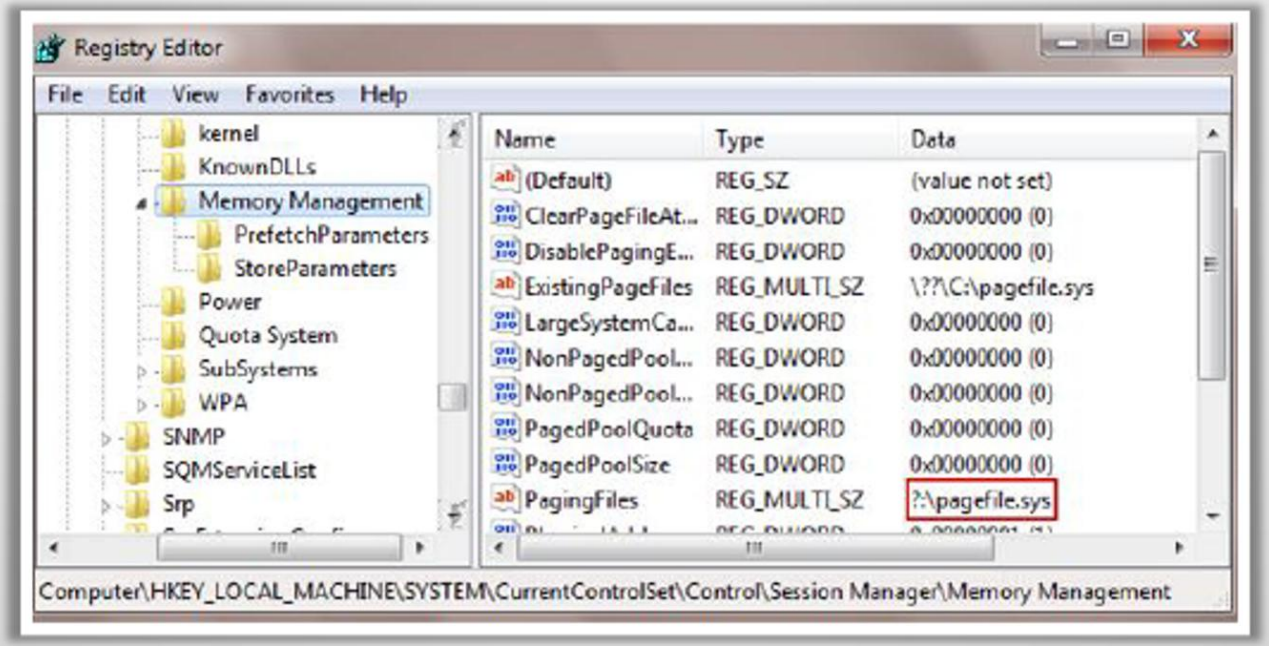
- Là một tập tin được windows sử dụng để làm bộ nhớ ảo trên hard drive.
- C:\pagefile.sys (thuộc tính ẩn)
- Khi RAM "đầy" windows sẽ sử dụng pagefile để lưu trữ
- Tùy chỉnh tại *"Advanced System Setting"*
- *Có thể pháp chứng trên file này.*



Swap File

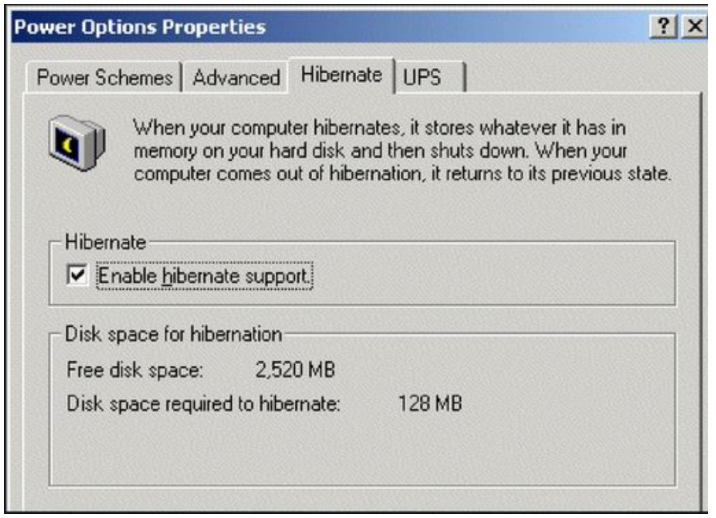
- A swap file is a space on a hard disk used as the virtual memory extension of a computer's RAM
- Swap files contain information about:
  - Files opened and their contents
  - Online chats
  - Websites visited
  - Emails sent and received

- On Windows, the swap file is a hidden file in the root directory called pagefile.sys
- The registry path for the swap file is:
  - `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management`



Hibernate?

- Lưu lại trạng thái vào đĩa để khởi động nhanh hơn.
- Nén bộ nhớ máy tính và ghi vào tập tin c:\hiberfil.sys (windows)
- Mặc định không bật ở các hệ điều hành Windows Vista về sau, Linux các phiên bản gần đây
- Có thể pháp chứng trên file này



RAM (Random Access Memory)

- Là bộ nhớ khả biến (Volatile)
- Đọc/ghi dữ liệu dễ dàng và nhanh chóng
- Lưu trữ thông tin tạm thời
- Công nghệ RAM:
  - RAM động – Dynamic RAM (DRAM)
  - RAM tĩnh – Static RAM (SRAM)

DRAM vs SRAM

- Giống: đều có tính khả biến; phải cấp nguồn điện liên tục để duy trì giá trị bit.
- Khác:

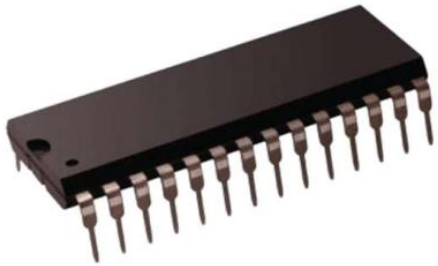
DRAM	SRAM
Dễ chế tạo, kích thước lớn hơn /cell nhớ	Cấu trúc phức tạp, kích thước lớn hơn /cell nhớ
Mật độ cell nhớ lớn hơn	Mật độ cell nhớ nhỏ hơn
Giá thành rẻ hơn	Giá thành đắt
Tốc độ truy xuất chậm hơn	Tốc độ truy xuất nhanh hơn
Cần hệ mạch refress hỗ trợ	Không cần hệ mạch refress hỗ trợ
Sử dụng cho bộ nhớ chính	Sử dụng trong cache (trong/ngoài bộ vi xử lý)

Bộ nhớ chỉ đọc (ROM)

- Chứa 1 mẫu dữ liệu cố định, không thể thay đổi hay thêm vào
- Bất biến: Không cần cấp nguồn điện để duy trì giá trị bit
- Dữ liệu hay chương trình được lưu trữ vĩnh viễn trong bộ nhớ
  - Lưu trữ chương trình hệ thống (**BIOS**), thư viện các chương trình con, Bảng chức năng, Vi chương trình
- Dữ liệu được nạp vào chip như một phần của quy trình sản xuất chip.
  - Nhược điểm của điều này:
    - Không cho phép có lỗi, nếu sai 1 bit thì toàn bộ lô ROM bị hủy
    - Việc nạp dữ liệu vào ROM tốn một khoản chi phí cố định khá lớn

ROM lập trình được - PROM

- Phương án ít tốn kém hơn
- Bất biến (non-volatile)
- Chỉ có thể ghi một lần duy nhất
- Quá trình ghi được thực hiện bằng điện, do nhà cung cấp hoặc khách hàng thực hiện tại thời điểm sau thời điểm sản xuất chip
- Cần có thiết bị đặc biệt để thực hiện quá trình ghi
- Linh hoạt và tiện lợi
- Thích hợp với sản xuất một số lượng lớn



In-memory data

- Current running processes and terminated processes
- Open TCP/UDP ports/raw sockets/active connections
- Memory mapped files
  - Executable, shared, objects (modules/drivers), text files
- Caches
  - Web addresses, typed commands, passwords, clipboards, SAM database, edited files
- Hidden data and many more

Pháp chứng bộ nhớ là gì?

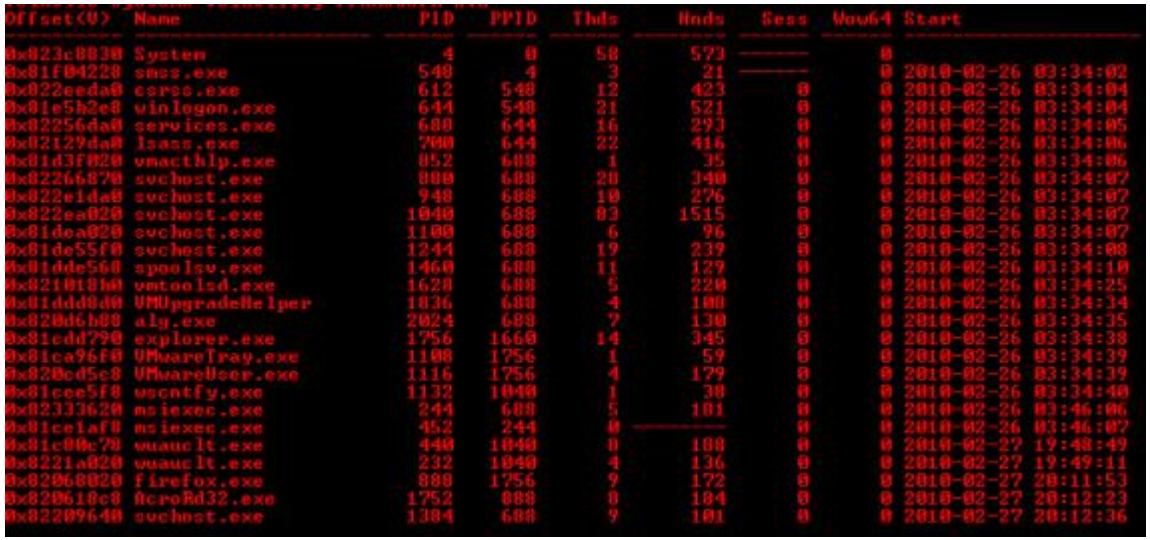
- "Memory forensics" là một hình thức điều tra, phân tích quan trọng trong kỹ thuật điều tra số giúp xác định xác hành vi bất thường, không được phép trên máy tính, máy chủ mục tiêu.
- Phân tích dữ liệu khả biến (volatile) trên file chụp từ bộ nhớ máy tính để điều tra/xác định các tấn công, hành vi độc hại mà không dễ phát hiện trên dữ liệu đĩa cứng lưu trữ.
- Đôi khi được gọi là *"memory analysis"*.

Vì sao phải điều tra bộ nhớ?

- Mọi thứ trước khi nạp vào HĐH đều phải qua bộ nhớ (RAM), như:
  - Process đang chạy
  - Registry Handles và các tập tin đang mở
  - Các kết nối mạng đang có trên hệ thống
  - Password & Encrypt
  - Các mã độc hại và các tập tin bị lây nhiễm

Vì sao phải điều tra bộ nhớ?

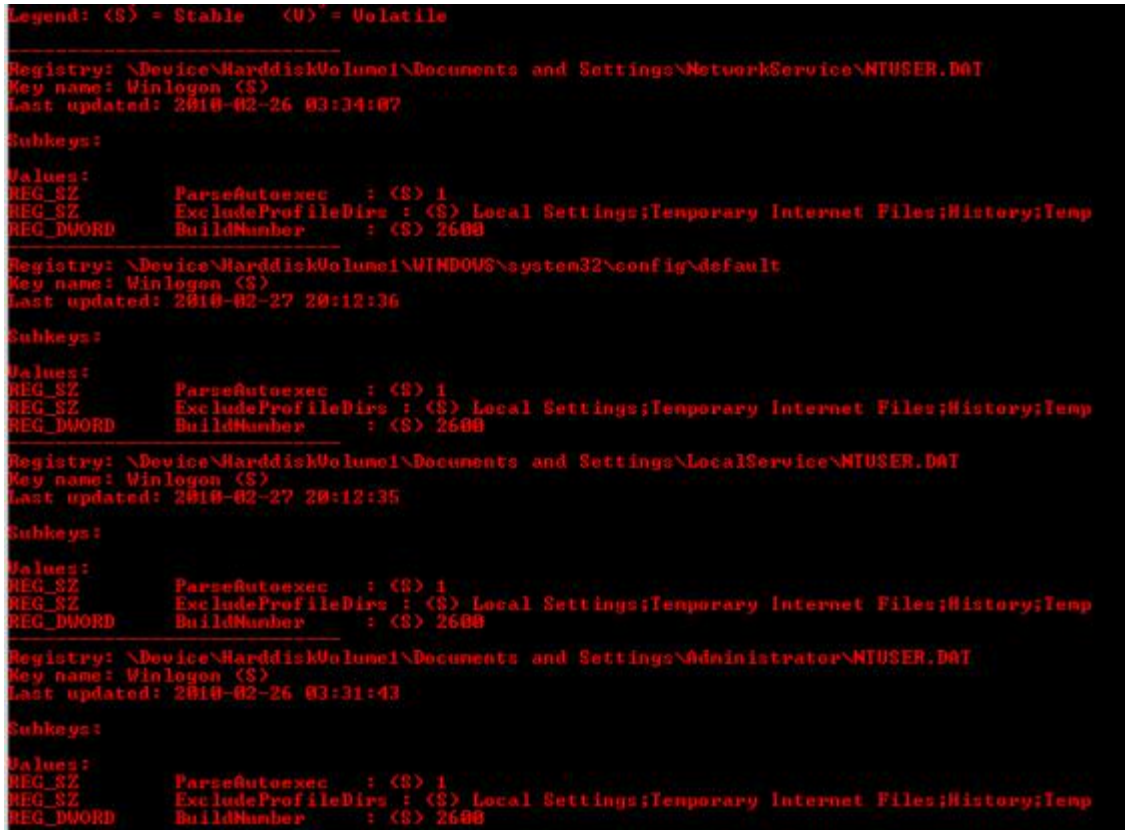
- **Process đang chạy:**
  - Tất cả các tiến trình đang chạy trên hệ thống được lưu ở bộ nhớ RAM.
  - Tiến trình ẩn cũng có thể được trích xuất ra
  - Khi tiến trình kết thúc nó vẫn có thể được lưu trữ trong bộ nhớ vì không gian lưu trữ vẫn chưa được phân bổ lại.



Offset(V)	Name	PID	PPID	Thds	Hnds	Sess	Wow64	Start
0x823c8830	System	4	0	58	573	------	0	
0x81f04228	smss.exe	548	4	3	21	------	0	2010-02-26 03:34:02
0x822eeda0	csrss.exe	612	548	12	423	0	0	2010-02-26 03:34:04
0x81e5b2e8	winlogon.exe	644	548	21	521	0	0	2010-02-26 03:34:04
0x82256da8	services.exe	688	644	16	293	0	0	2010-02-26 03:34:05
0x82129da8	lsass.exe	700	644	22	416	0	0	2010-02-26 03:34:06
0x81d3f020	vmacthlp.exe	852	688	1	35	0	0	2010-02-26 03:34:06
0x8226d870	svchost.exe	888	688	20	340	0	0	2010-02-26 03:34:07
0x822e1da8	svchost.exe	948	688	10	276	0	0	2010-02-26 03:34:07
0x822ea020	svchost.exe	1040	688	83	1515	0	0	2010-02-26 03:34:07
0x81d0a020	svchost.exe	1100	688	6	96	0	0	2010-02-26 03:34:07
0x81de55f8	svchost.exe	1244	688	19	239	0	0	2010-02-26 03:34:08
0x81dde568	spoolsv.exe	1460	688	11	129	0	0	2010-02-26 03:34:10
0x821018b0	vmtoolsd.exe	1628	688	5	220	0	0	2010-02-26 03:34:25
0x81ddd8d0	VMUpgradeHelper	1836	688	4	100	0	0	2010-02-26 03:34:34
0x820d6b88	alg.exe	2024	688	7	130	0	0	2010-02-26 03:34:35
0x81edd790	explorer.exe	1756	1660	14	345	0	0	2010-02-26 03:34:38
0x81ca96f0	VMwareTray.exe	1108	1756	1	59	0	0	2010-02-26 03:34:39
0x820cd5c8	VMwareUser.exe	1116	1756	4	179	0	0	2010-02-26 03:34:39
0x81cee5f8	wscntfy.exe	1132	1040	1	38	0	0	2010-02-26 03:34:40
0x82333620	msiexec.exe	244	688	5	181	0	0	2010-02-26 03:46:06
0x81c1af8	msiexec.exe	452	244	0	------	0	0	2010-02-26 03:46:07
0x81c00c78	wuauclt.exe	440	1040	8	108	0	0	2010-02-27 19:48:49
0x8221a020	wuauclt.exe	232	1040	4	136	0	0	2010-02-27 19:49:11
0x82068020	firefox.exe	888	1756	9	172	0	0	2010-02-27 20:11:53
0x820618c8	AcroRd32.exe	1752	888	8	184	0	0	2010-02-27 20:12:23
0x82209640	svchost.exe	1384	688	9	101	0	0	2010-02-27 20:12:36

Vì sao phải điều tra bộ nhớ?

- **Registry Handles và các tập tin đang mở:**
  - Các tập tin đang mở cũng như bất kỳ một xử lý registry (registry handles) nào được truy xuất bởi một tiến trình đều được lưu trữ trong bộ nhớ.



sử dụng lệnh printkey của volatility trong Registry winlogin

Vì sao phải điều tra bộ nhớ?

- **Các kết nối mạng đang có trên hệ thống**:
  - Các cổng đang lắng nghe trên hệ thống
  - Các kết nối đang được thiết lập
  - Các thông tin liên kết giữa hệ thống với các kết nối từ xa

Offset(P)	Local Address	Remote Address	Pid
0x01e6a9f0	192.168.0.176:1176	212.150.164.203:80	888
0x01ec57c0	192.168.0.176:1189	192.168.0.1:9393	1244
0x01ed4270	192.168.0.176:2869	192.168.0.1:30379	1244
0x01eef808	192.168.0.176:2869	192.168.0.1:30380	4
0x01ffa7f8	0.0.0.0:0	80.206.204.129:0	0
0x02041108	127.0.0.1:1168	127.0.0.1:1169	888
0x0225a448	192.168.0.176:1172	66.249.91.104:80	888
0x0226ac58	127.0.0.1:1169	127.0.0.1:1168	888
0x0227ac58	192.168.0.176:1171	66.249.90.104:80	888
0x02308890	192.168.0.176:1178	212.150.164.203:80	1752
0x02323008	192.168.0.176:1184	193.104.22.71:80	880
0x02410440	192.168.0.176:1185	193.104.22.71:80	880

Vì sao phải điều tra bộ nhớ?

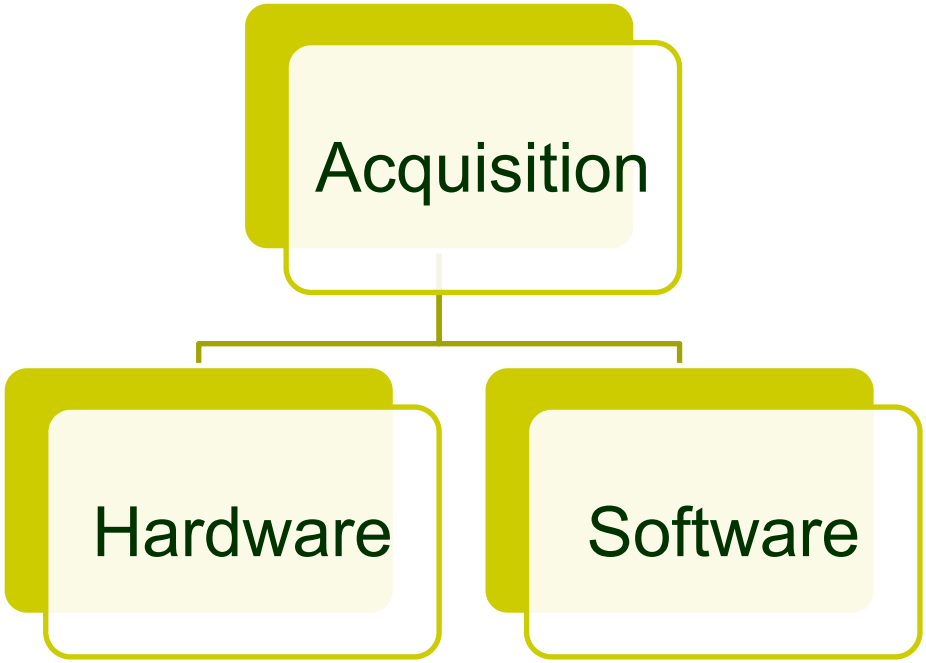
- **Password & Encrypt**
  - Mật khẩu, khóa mật mã không bao giờ lưu trên đĩa cứng mà không có sự bảo vệ nào.
  - Tuy nhiên chúng lại được lưu trữ trọng bộ nhớ RAM

Vì sao phải điều tra bộ nhớ?

- **Các mã độc hại và các tập tin bị lây nhiễm**
  - Kẻ tấn công có thể chạy mã khai thác từ bộ nhớ thay vì lưu trữ chính nó trên ổ đĩa.
  - Điều này có thể qua mặt các phần mềm diệt virus.

Làm sao để có được bộ nhớ?

→ **Memory Imaging:** tạo ra một bản sao của bộ nhớ vật lý (memory dump)



Làm sao để có được bộ nhớ?

- **Acquisition: Hardware**
  - Dùng phần cứng chuyên dụng thực hiện truy cập bộ nhớ trực tiếp để có được bản sao của bộ nhớ.
  - Kết quả có độ tin cậy cao
  - Chi phí cao
  - Công cụ: Firewire, Cold Boot attack,Tribble Card, https://www.youtube.com/watch?v=vJszLtaIyIk

Làm sao để có được bộ nhớ?

- **Acquisition: Software**
  - Sử dụng các bộ phần mềm chạy trên máy tính để có được bản sao của bộ nhớ.
  - Phương pháp này thường được sử dụng bởi chi phí rẻ, tiện lợi.
  - Độ tin cậy kém hơn so với sử dụng phần cứng
  - Công cụ phổ biến: Volatility, Memoryze, dumpit, win32dd, Mandiant Redline,... dd, memdump trong linux.

Virtual Machine imaging

- Chụp ảnh bộ nhớ máy ảo một cách đáng tin cậy
- VD: Virtual Box

```
VBoxManage debugvm <vmname> dumpguestcore --filename <name>
```

Các công cụ thường dùng khi điều tra bộ nhớ

- Thời kỳ thứ 0
  - Trước 2004
  - Tool dựa trên phân tích ‘strings’ và ‘grep’
  - Các tool này không sử dụng chuyên để làm pháp chứng bộ nhớ, thông tin cung cấp giới hạn, công dụng chủ yếu extract text từ file memory dump.

Các công cụ thường dùng khi điều tra bộ nhớ

- Thời kỳ thứ 1
  - Từ 2004 – 2005
  - Tools chuyên biệt cho phân tích bộ nhớ được tạo ra
  - Tools: Crash dump, memget, mempeek

Các công cụ thường dùng khi điều tra bộ nhớ

- Thời kỳ thứ 2
  - 2005 – 2010
  - Trở nên phổ biến, các công cụ phân tích tự động
  - Hỗ trợ nhiều OS
  - Tools: Volatality, Rekall, Responder PRO, Memoryze, MoonSols Windows Memory Toolkit, winen, Belkasoft Live RAM Capturer, etc.

Các công cụ thường dùng khi điều tra bộ nhớ

- Thời kỳ thứ 3
  - Từ 2010 về sau
  - Visualiazation, Virtualization
  - Tools: MoonSols LiveCloudKd, Microsoft LiveKd

Volatility tool

- Là một framework mở rộng mã nguồn mở dùng cho pháp chứng bộ nhớ.
- Được viết bằng python
- Theo kiến trúc module plug-in
- Hỗ trợ nhiều hệ thống, kiến túc
- Được cung cấp tại: https://github.com/volatilityfoundation/volatility
- Video: https://www.youtube.com/watch?v=Cs0Gc3GtfZY

Volatility tool Example

```
root@kali: ~/Documents/forensics/memoryforensics/mem-forensic-01
File  Edit  View  Search  Terminal  Help
0x000000003f7afcb0 SearchProtocol     1704    812 0x3eb48400 2017-10-07 19:00:46 UTC+0000
0x000000003f7b9be8 dllhost.exe        1224    624 0x3eb48600 2017-10-07 19:03:14 UTC+0000
0x000000003f7dad40 dllhost.exe        2404    624 0x3eb48680 2017-10-07 19:03:11 UTC+0000   2017-10-07 19:03:16 UTC+0000
0x000000003fc8a808 kleopatra.exe      2044   1336 0x3eb48620 2017-10-07 18:55:29 UTC+0000   2017-10-07 18:55:32 UTC+0000
0x000000003fcd15d0 gpg-agent.exe      3576   3556 0x3eb48640 2017-10-07 18:45:41 UTC+0000
0x000000003fffaa20 System                4      0 0x00185000 2017-10-07 18:41:20 UTC+0000
root@kali:~/Documents/forensics/memoryforensics/mem-forensic-01# volatility -f find-me.bin --profile=Win7SP1x86 hivelist
Volatility Foundation Volatility Framework 2.6
Virtual    Physical   Name
---------- ---------- ----
0x87a0c420 0x27d12420 [no name]
0x87a1a250 0x27dde250 \REGISTRY\MACHINE\SYSTEM
0x87a449d0 0x27bca9d0 \REGISTRY\MACHINE\HARDWARE
0x88273008 0x1ff6c008 \SystemRoot\System32\Config\SECURITY
0x8828b9d0 0x1ff269d0 \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
0x882ea460 0x24869460 \SystemRoot\System32\Config\SAM
0x8a47f008 0x24286008 \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0x8bbc39d0 0x258df9d0 \Device\HarddiskVolume1\Boot\BCD
0x8bbde008 0x25970008 \SystemRoot\System32\Config\SOFTWARE
0x8e9b19d0 0x2538a9d0 \SystemRoot\System32\Config\DEFAULT
0x906af9d0 0x1a6ab9d0 \??\C:\Users\Black Eagle\ntuser.dat
0x906f39d0 0x2bb679d0 \??\C:\Users\Black Eagle\AppData\Local\Microsoft\Windows\UsrClass.dat
0x957579d0 0x0a3d79d0 \??\C:\System Volume Information\Syscache.hve
root@kali:~/Documents/forensics/memoryforensics/mem-forensic-01# volatility -f find-me.bin --profile=Win7SP1x86 hashdump -y 0x87a1a250 -s 0x882ea460 > pwdhashes.txt
Volatility Foundation Volatility Framework 2.6
```

```
+ Processing...
root@kali:~/Documents/forensics/memoryforensics/mem-forensic-01# ls
find-me.bin  find-me.zip  pwdhashes.txt  text.txt
root@kali:~/Documents/forensics/memoryforensics/mem-forensic-01# cat pwdhashes.txt
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Black Eagle:1000:aad3b435b51404eeaad3b435b51404ee:a39b211d0441a8380ec21a97e88531ff:::
root@kali:~/Documents/forensics/memoryforensics/mem-forensic-01#
```

Liệt kê toàn bộ tài khoản có trên hệ thống kể cả tài khoản disable

LAB

- Sinh viên thực hành điều tra bộ nhớ LAB2: Memory forensics

References

- CHFIv8
- Kiến trúc máy tính, Hang-Phuong Nguyen
- Physical Memory Forensics, Mariusz Burdach
- Wikipedia
- Memory Forensics, Phulc

Q&A

TRƯỜNG ĐH CÔNG NGHỆ THÔNG TIN
KHOA MẠNG MÁY TÍNH & TRUYỀN THÔNG

Digital Forensics
Pháp chứng Kỹ thuật số

#4: Memory Forensics

Spring 2022

ThS. Lê Đức Thịnh
thinhld@uit.edu.vn