Computer Forensics

Samuel Chevet

samuel@lse.epita.fr
http://www.lse.epita.fr

18 July 2012

Why this talk ?

- Partnership with OCLCTIC
- Fun
- Dealing with VxStuff
- State of art

McKemmish, 1999

The process of identifying, perserving, analyzing and presenting digital evidence in a manner that is legally acceptable

Farmer & Vennema, 1999

Gathering and analyzing data in a manner as freedom distortion or bias as possible to reconstruct data or what has happened in the past on a system

Computer Forensics

- Part of forensics science
- Electronic evidence
- Computer, Electronic devices

Used for . . .

- Personal / Civil matters

Used for . . .

- Criminal Cases

Case Study

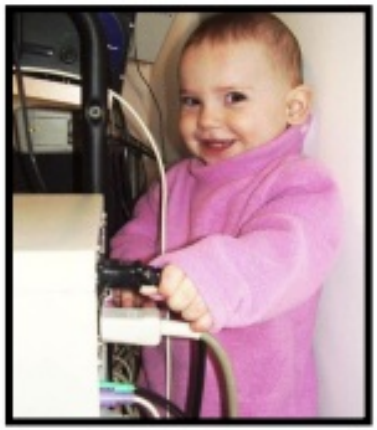
- Human resources
- Money on disk
- Hidden bits
- Disk swap
- Tapes rarely lie
- Narcotics
- Fraud
- Pornography (Child ?)
- Theft
- ...

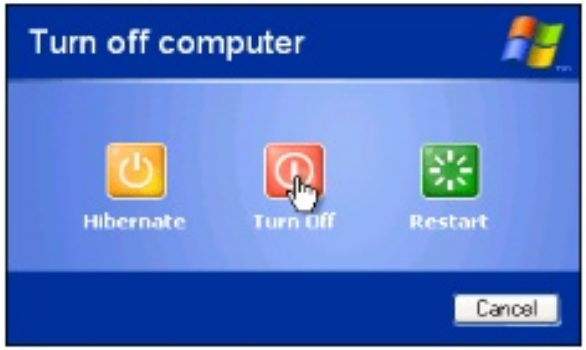
Four Steps

- Acquisition
- Identification - Technical Analysis
- Evaluation - What the lawyers do
- Presentation

Kind of forensics

Dead forensics





Live Forensics

Dead Forensics

- Old school
- Avoid malicious processes
- Deleting evidence
- Snapshots
- EnCase, . . .

Process

1. Approach computer
2. Is computer on ?
3. Turn off computer
4. Remove Hard drive
5. Attach drive to forensic system
6. Make complete copy

Advantages VS Disadvantages

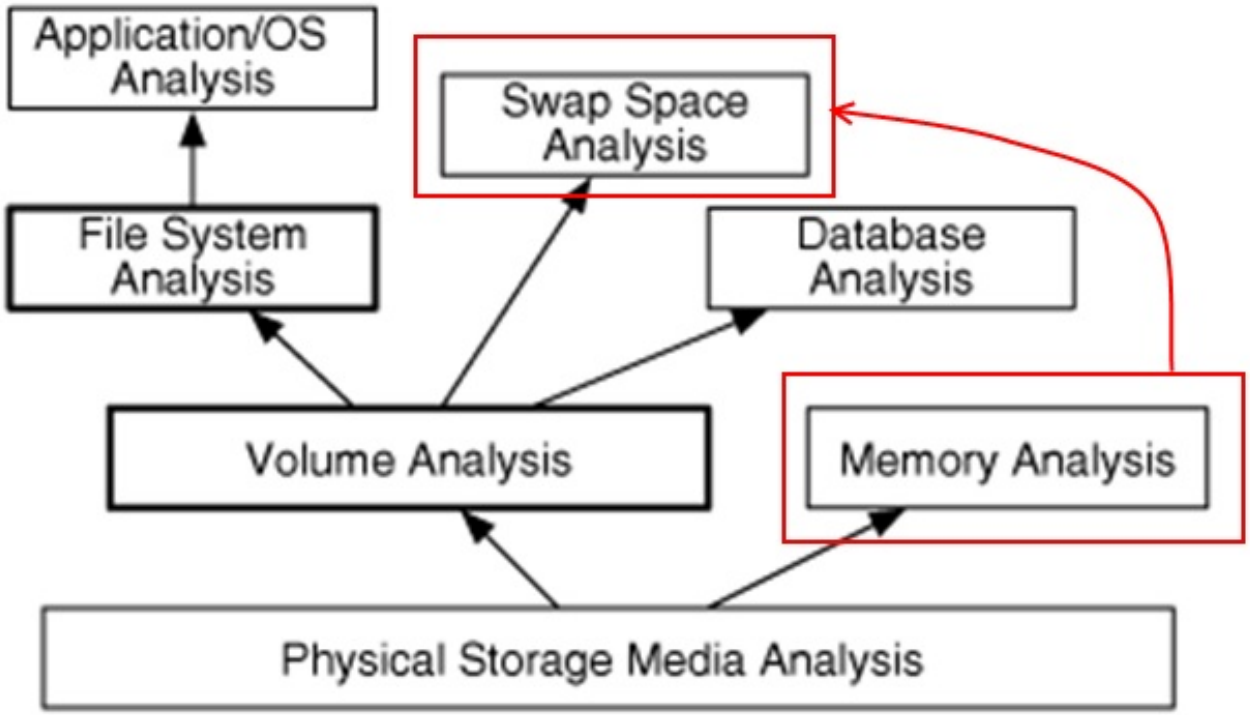
- Avoid data modification

- Cryptography
- Volatile network data
- Gigabytes of data
- Evidence

What is it ?

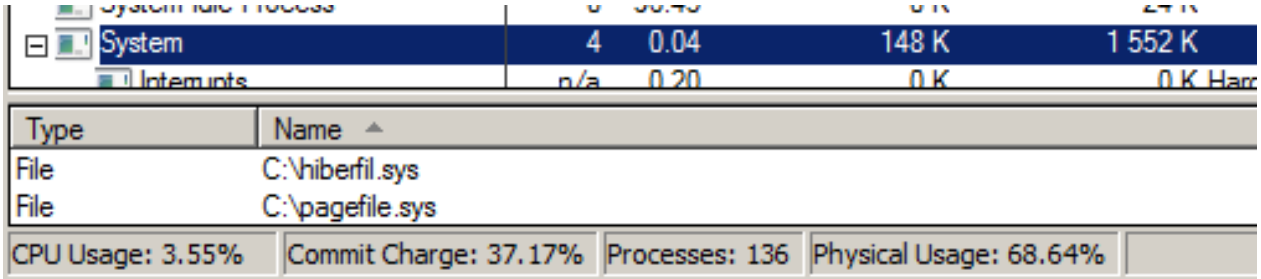
- Growing field
- Vx Analysis
- Judicial search
- Response to incidents

Not Only Memory Images



Not Only Memory Images

- IOCTL
- FSCTL_GET_RETRIEVAL_POINTERS
- Local Cluster Number
- Virtual Cluster Number
- Raw (NTFS)



Why ?

Advantages

- Scope of Information
- Retrieve volatile information
- Combats "dead forensics" countermeasures

But . . .

- Every computer installation is unique
- All actions affect memory
- Cannot be reproduced
- No data integrity

TrueCrypt, etc . . .

- TrueCrypt
- BitLocker
- Cryptography

In-Memory data

- Processes

```
0: kd> dt nt!_EPROCESS
...
+0x070 CreateTime        : _LARGE_INTEGER
...
+0x084 UniqueProcessId   : Ptr32 Void
...
+0x174 ImageFileName     : [16] UChar
...
+0x190 ThreadListHead    : _LIST_ENTRY
```

Network Information

- tcppip.sys

```
typedef struct _TCB {
...
USHORT LocalPort          + 0x2C
USHORT RemotePort         + 0x2E
...
PEPROCESS OwningProcess + 0x164
...
```

- Firewall settings

In-Memory data

- Files, Windows registry

```
0: kd> !handle
0: kd> dt nt!_HHIVE
0: kd> dt nt!_CMHIVE
```

```
0: kd> !reg hivelist

| HiveAddr |Stable Length|Stable Map|Volatile Length|Volatile Map|MappedViews|PinnedViews|U(Cnt)| BaseBlock | FileName
| e1a1c970 |       3000  | e1a1c9d0 |          0    |  00000000  |        1  |        0  |     0| e1d6d000  | \Microsof
| e1aa6b60 |      f0000  | e1aa6bc0 |       2000    |  e1aa6c9c  |       54  |        0  |     0| e1d5f000  | tings\Adm
| e1a43b60 |       1000  | e1a43bc0 |          0    |  00000000  |        1  |        0  |     0| e1a90000  | \Microsof
| e1a75b60 |       3b000 | e1a75bc0 |       1000    |  e1a75c9c  |       15  |        0  |     0| e1a86000  | ettings\L
| e1a34b60 |       1000  | e1a34bc0 |          0    |  00000000  |        1  |        0  |     0| e1a40000  | \Microsof
| e1a57b60 |       3b000 | e1a57bc0 |       1000    |  e1a57c9c  |       15  |        0  |     0| e1a5d000  | tings\Net
| e16fcad0 |     958000  | e14d6000 |       4000    |  e16fcc0c  |      255  |        0  |     0| e14ae000  | emRoot\Sy
| e15a1b60 |       3c000 | e15a1bc0 |          0    |  00000000  |       16  |        0  |     0| e14c2000  | temRoot\S
| e135b758 |       9000  | e135b7b8 |       1000    |  e135b894  |        3  |        0  |     0| e135c000  | emRoot\Sy
| e1718388 |       5000  | e17183e8 |          0    |  00000000  |        2  |        0  |     0| e14c8000  | \SystemRo
| e130b510 |      18000  | e130b570 |       6000    |  e130b64c  |        0  |        0  |     0| e130d000  | <NONAME>
| e102f758 |      2c6000 | e1039000 |      29000    |  e102f894  |      170  |        0  |     0| e1038000  | SYSTEM
| e102f008 |       1000  | e102f068 |       1000    |  e102f144  |        0  |        0  |     0| e1030000  | <NONAME>
```

In-Memory data

- Passwords, Cryptographic Keys (aeskeyfind, . . .)
- Web cache
- Hidden data and malicious code (SSDT, Shadow SSDT, IDT, pIofCallDriver, . . .)

The process

- Acquire physical memory
- Gather extra volatile data
- Offline analysis of memory dump
- Proceed with post-mortem forensics

Collect

\Device\PhysicalMemory

- Require driver (XP SP2 / 2003)
- Split TLB

MmMapIoSpace()

- Kernel API
- Maps the given physical address range to nonpaged system space
- Hook

PFN Mapping

- Page Frame Number
- Unique Number

Collect

Crash Dump

- Lots of methods of acquisition : mouse, driver, Emergency Management Services, . . .
- State of processor
- Size problem
- Erase pagefile.sys

Direct Memory Access

- PCI Express
- FireWire
- . . .

Hibernation

- Suspend to disk (Windows 2000)
- But also in other OS
- \hiberfil.sys
- No hardware prerequisite
- Avoid BSOD
- No standalone tools (Avoid drivers signing)

Hibernation

- Modified code can be executed
- Processor state
- Previous EIP
- GDT, IDT Base Address

Collect (LINUX)

Linux

- /dev/mem
- /dev/kmem
- /proc/kcore

Analyse

Tools

- XWays
- FTK
- SANS Investigate Forensic Toolkit (SIFT)
- ...

Carving

- Extract logical data
- Meta-information insufficient

Open Source ?

Volatility

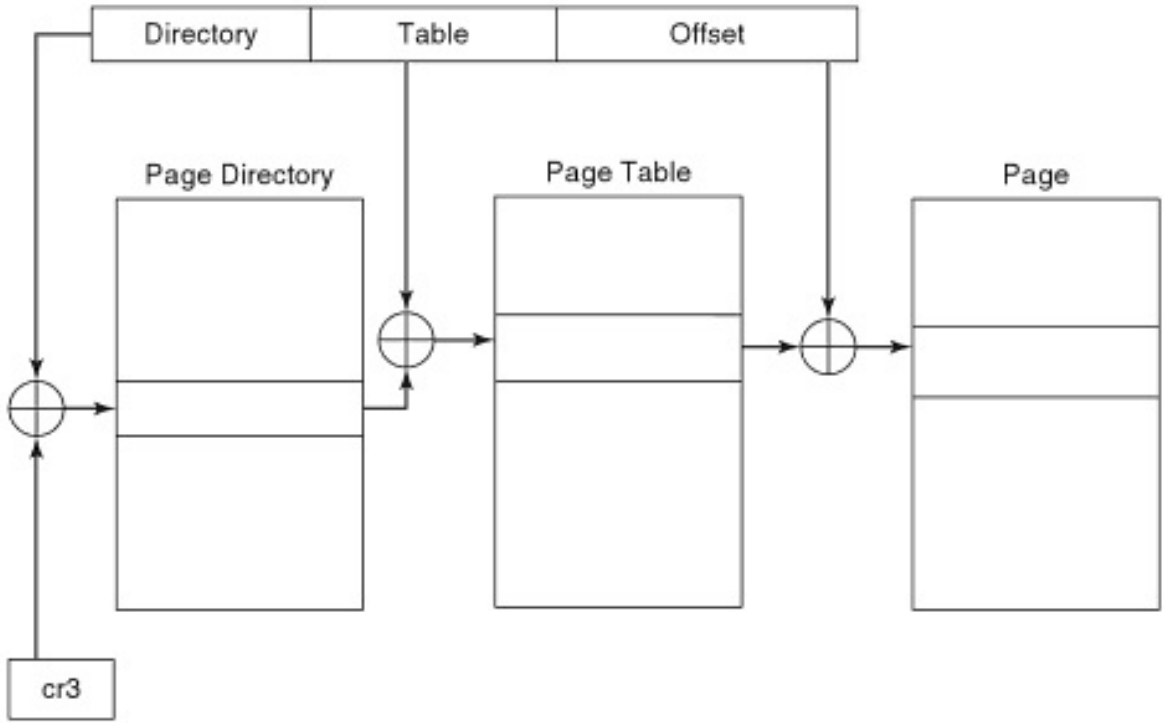
- Image identification
- Processes and DLL
- Process memory
- Kernel Memory and Object
- Networking
- Registry
- Crash Dumps, Hibernation, Conversion
- Malware and Rootkits
- Misc
- Linux / Mac branches

Split TLB

- Translation Lookaside Buffers
- PaX
- Used for unpacking too !

Paging mechanism

- Modern operating system
- CPU always use virtual addresses to reference memory location



Paging mechanism

- PageFault handler
- Store translation in TLB cache
- TLB hit
- TLB miss

1. If translation found in TLB, converted directly
2. TLB miss, pagefault occurs
3. Pagefault handler checks if the virtual address is valid
4. Load corresponding page into memory and store translation into TLB
5. Control is transfered to the original instruction

Split TLB

- Replace Pagefault handler
- Hide data from malicious process or anything else

Hook

- Alter or augment behavior
- Operating System, Applications
- Intercepting functions calls
- Messages
- Events

Other

- Block access to \Device\PhysicalMemory
- DKOM (Direct Kernel Object Manipulaiton)
- Target other process

Conclusion

- Live forensics is a must
- Can be defeated
- Easy to detect some payload

Questions ?

Thank you for your attention

- @w4kfu
- blog.w4kfu.com
- samuel@lse.epita.fr