MAC OS X PHYSICAL MEMORY ANALYSIS

Matthieu Suiche – msuiche(at)moonsols.com

JSSI 2010 – Paris

MoonSols

WHO AM I ?

Founder of **MoonSols**.

Microsoft MVP Enterprise Security

SandMan Framework - *Windows hibernation file*

Win32/64dd Utility – *Windows physical memory acquisition utility*

AGENDA

AGENDA

MoonSols

WHO ?

Forensics Experts

Investigators

Incident Responders

Malware Analysts

..

AGENDA

MoonSols

WHY ?

Information goldmine

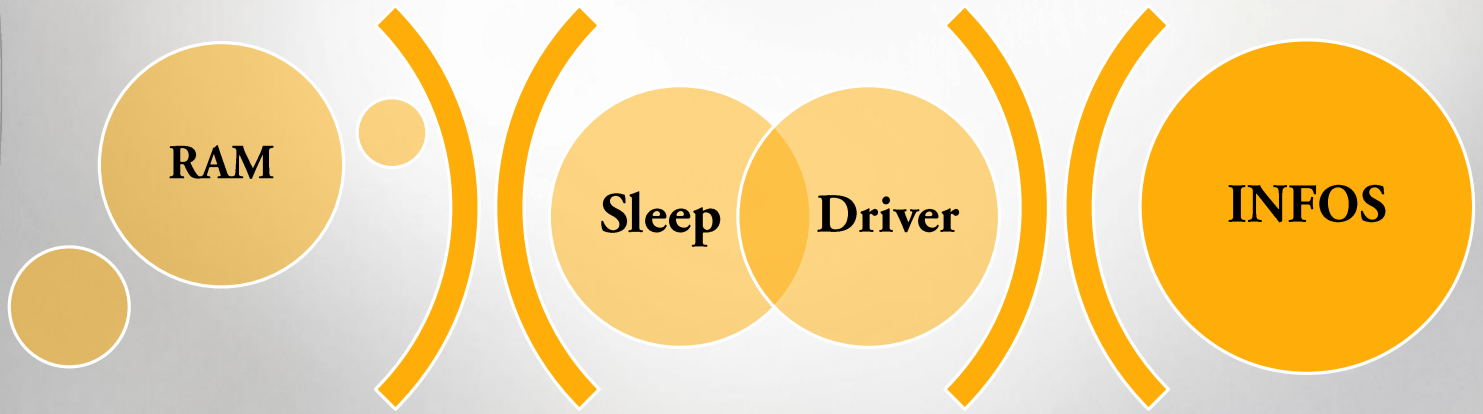
Pros . Non-volatile memory is not enough. That's why we need volatile memory.

Cons. Lack of research

AGENDA

MoonSols

OVERVIEW



MoonSols

MACBOOK

Actual research based on

- Intel Processor only (x86)

- Mac OS X Leopard 10.5
- Mac OS X Snow Leopard 10.6

PHYSICAL MEMORY (1/3)

Software based acquisition methods only

PHYSICAL MEMORY (2/3)

With our own kernel extension.

/dev/mem is disabled by default.

```
void bcopy_phys(addr64_t from,
                addr64_t to,
                int size);
```

is your **friend**.

PHYSICAL MEMORY (3/3)

OS X hibernation called "Safe Sleep"

- `/private/var/vm/sleepimage`
- Compressed *(WKDM)* memory snapshot
- Can be encrypted if *secure virtual memory* mechanism is used
  - *sudo* `pmset -a hibernatemode 1` to disable SVM.

AGENDA

MoonSols

ANALYSIS

No random string searching

ANALYSIS

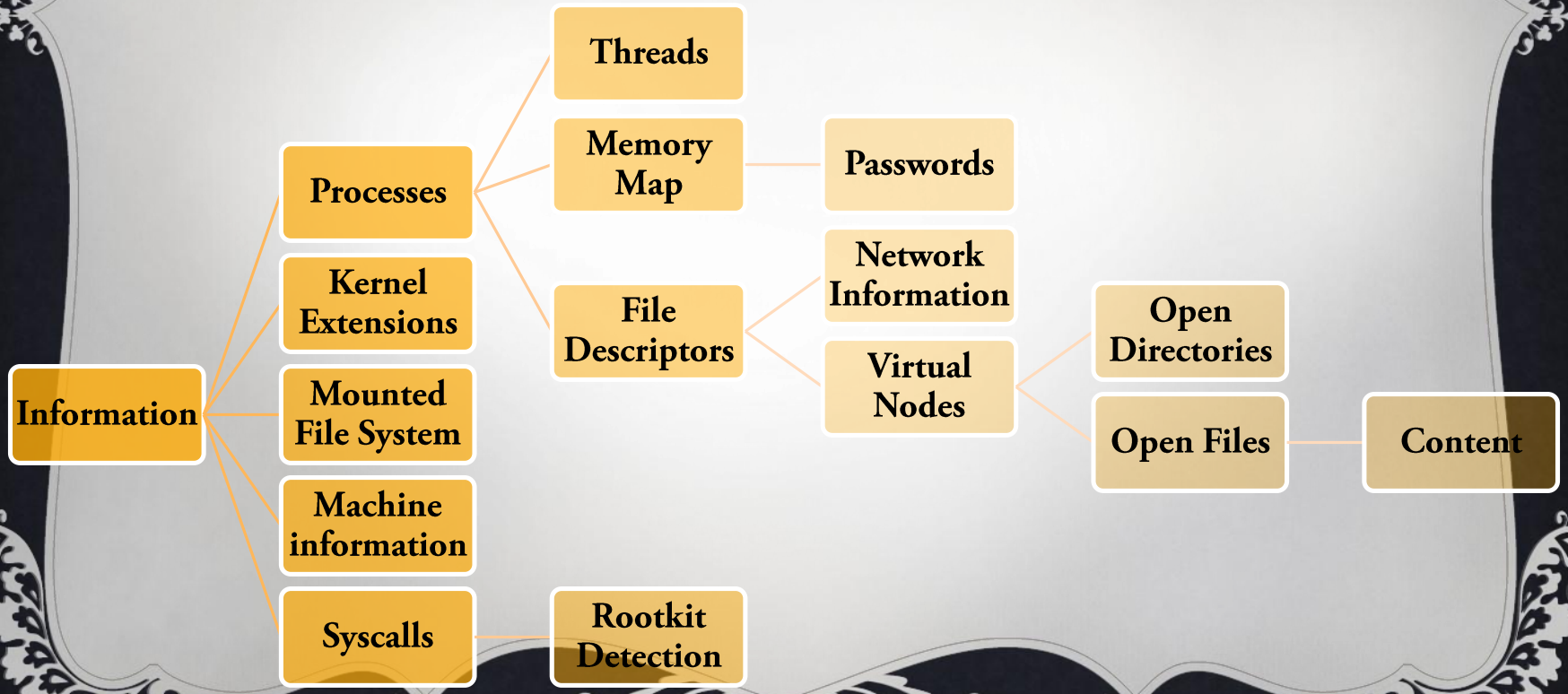
Get kernel symbols.

Initialize kernel memory manager.

Browse kernel virtual address space.

Collect information.

INFORMATION GOLDMINE



MoonSols

AGENDA

MoonSols

SYMBOLS

Windows compiler stores symbols in externals files called *.PDB

Mac OS X compiler stores symbols inside a section which is part of the executable *(mach_kernel)*.

SYMBOLS

__KLD, *__LINKEDIT*, *__PRELINK* and __symtab kernel sections are destroyed as soon as the kernel *(mach_kernel)* is loaded by `removeKernelLinker()` function.

__LINKEDIT section contains variable names and offsets.

SYMBOLS

To read kernel values, we need a quick address translation formula.

Operating System	Quick translation Formula
i386 Linux	KPA = KVA – 0xC0000000
Playstation 3 Linux	KPA = KVA – 0xC000000000000000
Windows	KPA = KVA & 0x1FFFF000
Mac OS X	KPA = KVA

SYMBOLS

Works **only** for the mapped executable kernel *(__text and __data sections)*

Does **NOT** work for allocated buffers.

.data interesting exported variables:

Memory manager variables

AGENDA

MoonSols

MEMORY

Super interesting variables

_IdlePDPT

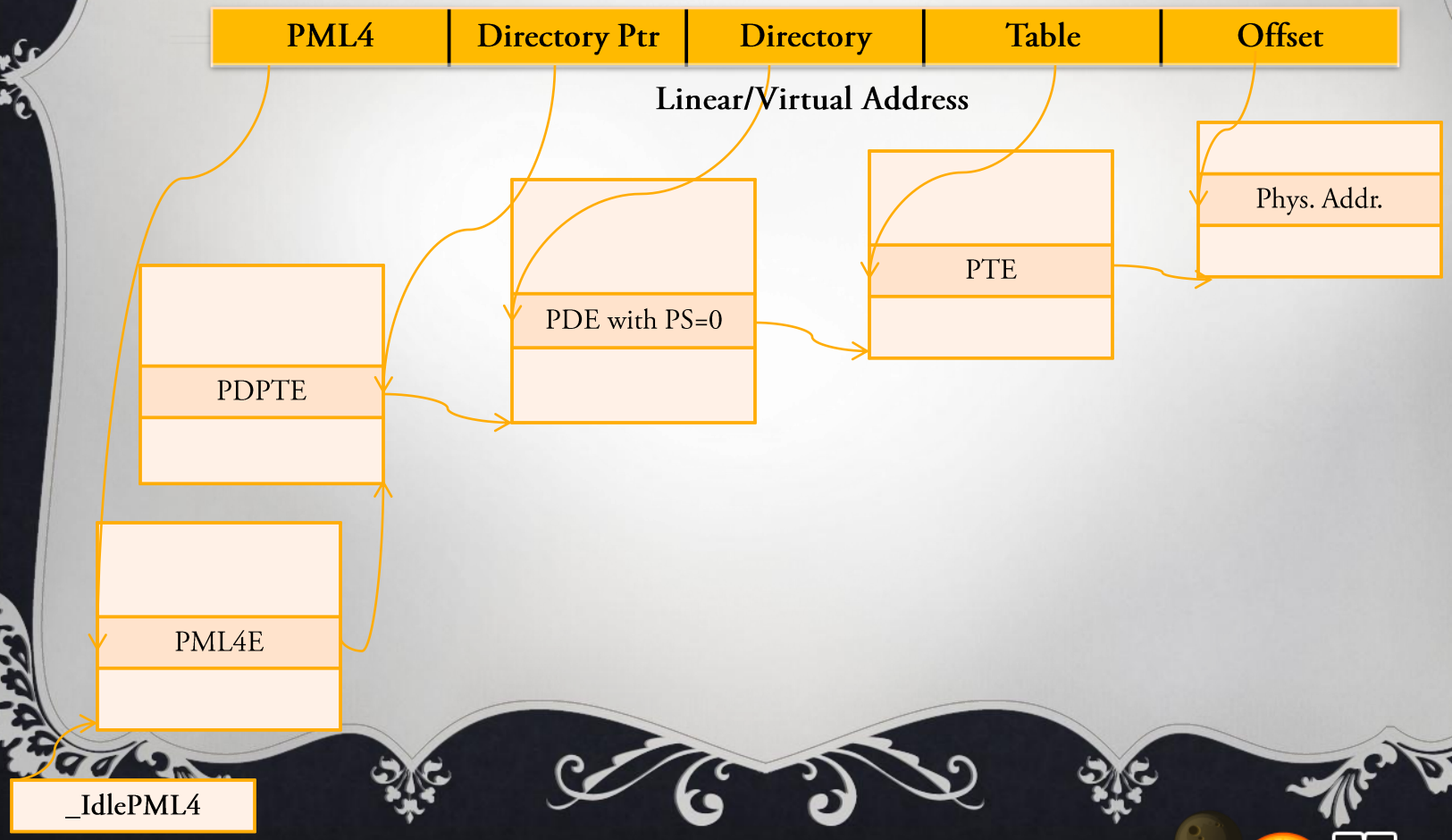
_IdlePDPT64

_IdlePML4

_IdlePTD

Page Map Level 4 is also initialized on x86 version.

TRANSLATION



SYMBOLS

Kernel symbols + Memory manager initialized

=

?

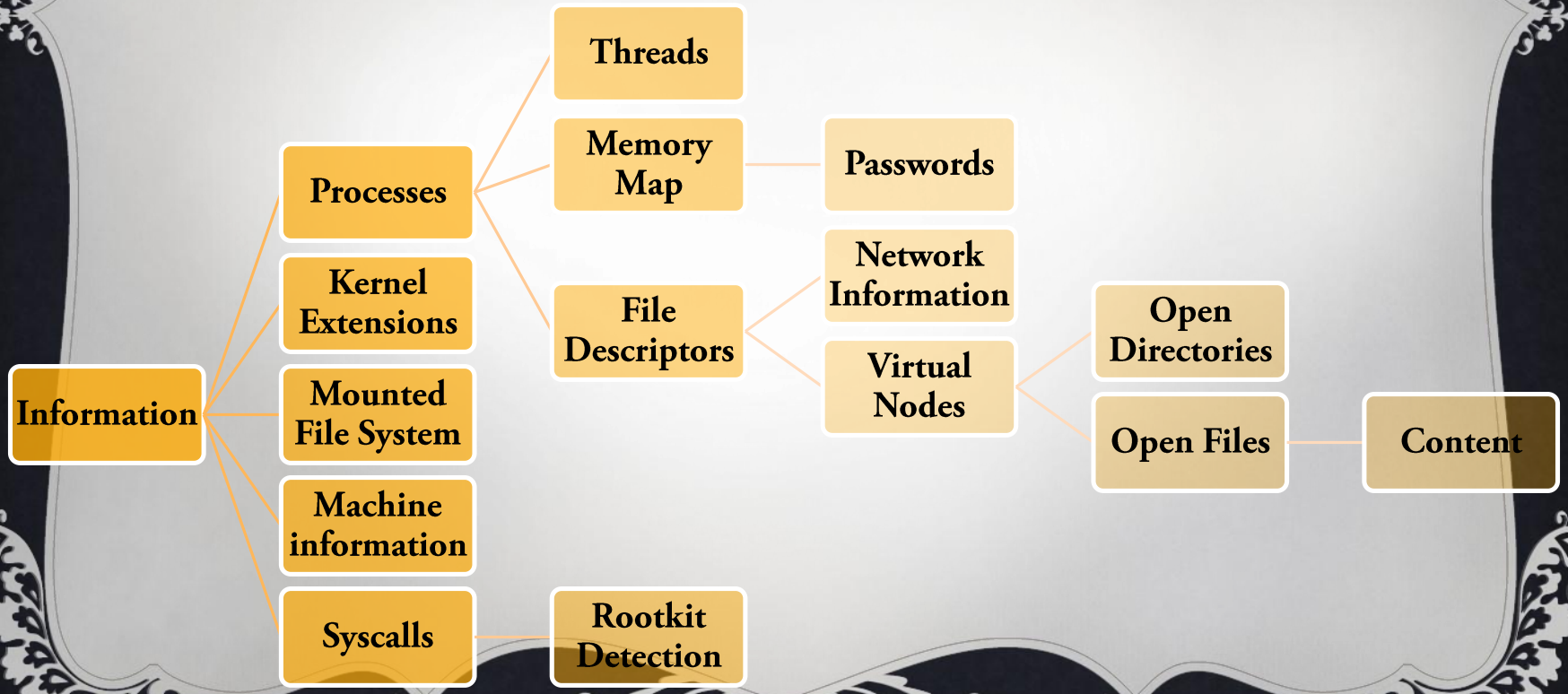
SYMBOLS

Kernel symbols + Memory manager initialized

=

Full kernel address space is browsable (/dev/mem is now /dev/kmem)

INFORMATION GOLDMINE



MoonSols

MACHINE INFORMATION

`version` variable contains a string with kernel version and compilation time

`machine_info` variable / structure contains:

Field Name	Description
major_version	Major OS Version
minor_version	Minor OS Version
max_mem	Physical Memory size
physical_cpu	Number of physical CPU
logical_cpu	Number of logical CPU

MOUNTED FILE SYSTEM

Link-list called `mountlist`, defined by mount structure.

Field Name	Description
f_fstypename	File system type
f_mntonname	Mounted directory
f_mntfromname	Mounted file system

KERNEL EXTENSIONS

`kmod` variable is the list-head of every loaded kernel extensions defined by `kmod` structure.

Field Name	Description
address	Base Address
size	Total Size
hdr_size	Header Size
name	Extension Name
version	Version
next	Pointer to the next entry

PROCESSES

`kernproc` variable is list-head of every BSD processes defined by `proc` structure (PID, Parent PID, open files (file descriptors), children, threads, name and a pointer (`p_pgrp` field) to process group (`pgrp` structure).)

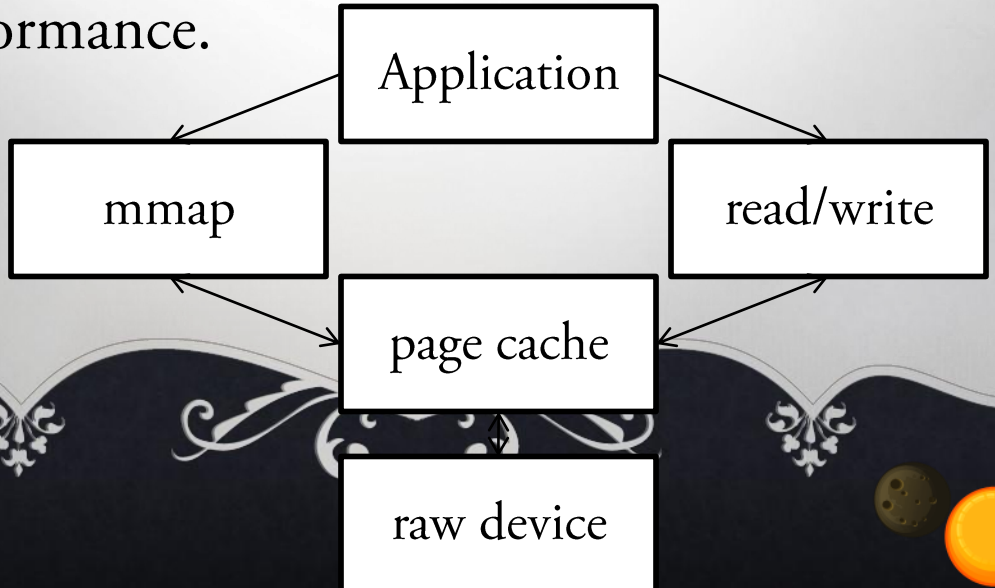
`pgrp` structure -> session structure (`pg_session` field).

`session` structure -> username (`s_login` field).

VNODES – FILES CONTENT

File caching is done via Unified Buffer Cache (UBC) technology under BSD Operating System.

UBC is used to unifying the file system and virtual memory caches of file data, thereby providing increased system performance.



SYSCALLS

Syscalls table address is not exported

Leopard

As explained by Jesse D'Aguanno at BH US 2008

```
&sysent = &nsysent + 0x20
```

Snow Leopard

```
&sysent = &nsysent - ((nsysent) *
  sizeof(sysent))
```

SYSCALLS

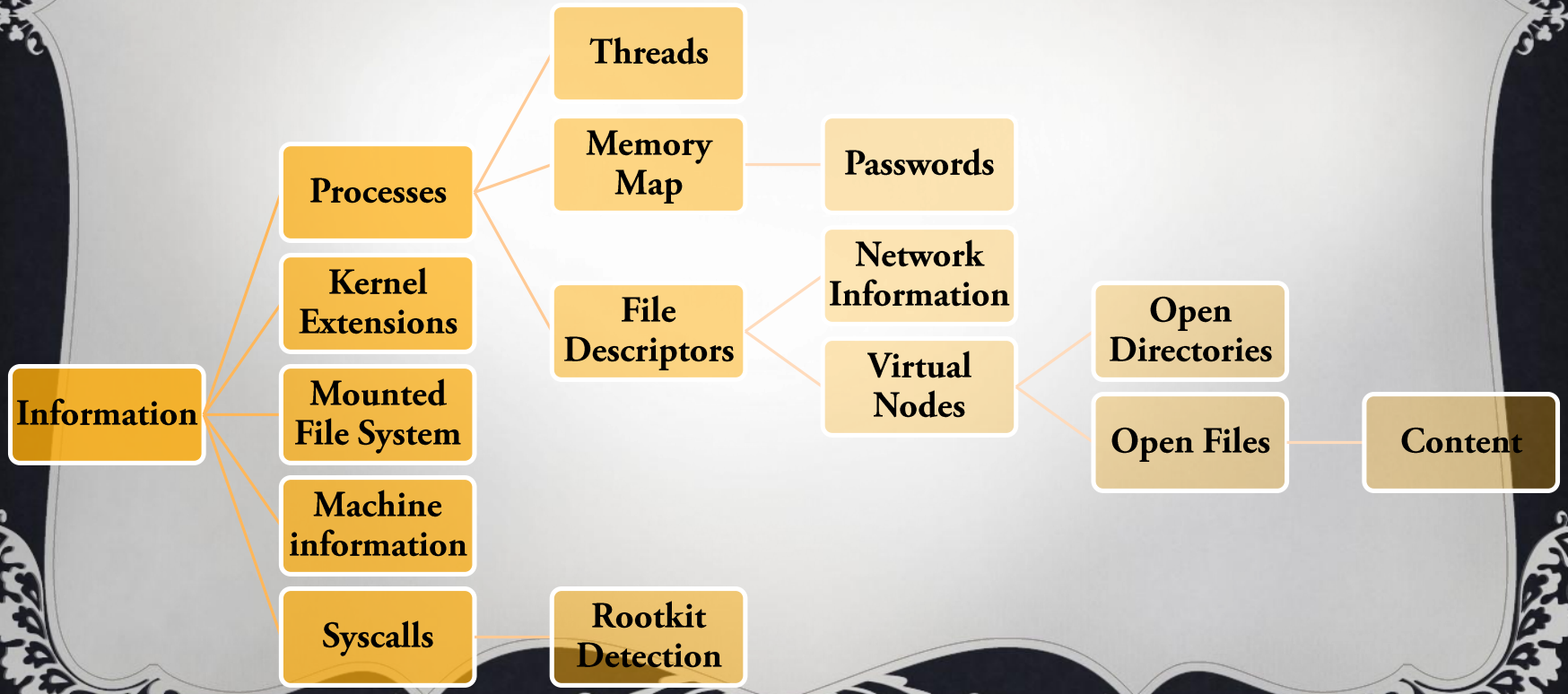
If an offset from a Syscall entry is not in kernel symbols.

Then, this is not normal ☺

Easy & Fast

DEMO

INFORMATION GOLDMINE



MoonSols

Web: *http://www.moonsols.com*

Twitter: *msuiche or MoonSols*

Mail: *msuiche(at)moonsols.com*

QUESTIONS ?