

# Blue Screen Of Death Is Dead

Matthieu Suiche  
Founder, MoonSols SARL  
*[msuiche@moonsols.com](mailto:msuiche@moonsols.com)*



# Who am I ?

Founder of MoonSols SARL, based in France

Various security services, Forensics Products, **Trainings**, Kernel code consulting

Co-Organizer of **Hackito Ergo Sum** (April 2011, Paris – France)

Author of

SandMan (Windows Hibernation File)

Win**32/64**dd (Windows Memory Acquisition)

Mac OS X Physical Memory Analysis Research

MoonSols Windows Memory Toolkit

LiveCloudKd

<http://msdn moonsols.com> (Online resource for undocumented structure definition)

BlackHat, PacSec, CanSecWest etc. speakers.



# Agenda

- Who ?

# Who ?

- Memory (crash) Dumps are interesting for
  - Kernel developers
  - Kernel troubleshooters
  - Bug hunter
  - Investigator
  - Forensic Expert
  - Malware Analyst
  - Incident Responder

# Agenda

- Who ?
- **Why ?**

# Why ?

- Bug hunter:
  - Hey man ! I just wrote my fuzzer of 10 lines Python ! I got a remote BSOD ! And all I got is this crash dump ! (CVE-2009-3103)
- Kernel Developer
  - F\*\*\* ! What the F\*\*\* is why with this null pointer ?

# Why ?

- Investigator / Forensic Expert
  - Inspector Gadget just made a memory dump of Dr. Claw computer to extract his Facebook and Twitter activity. Moreover, the login/passwd he used to connect to his pr0n server.
- Malware Analyst
  - I got this crazy packed Rootkit for Win 7 64-bits ! Why the Numega guys stopped to dev SoftIce ? I rather disassemble memory area and the dumper driver.

# Why ?

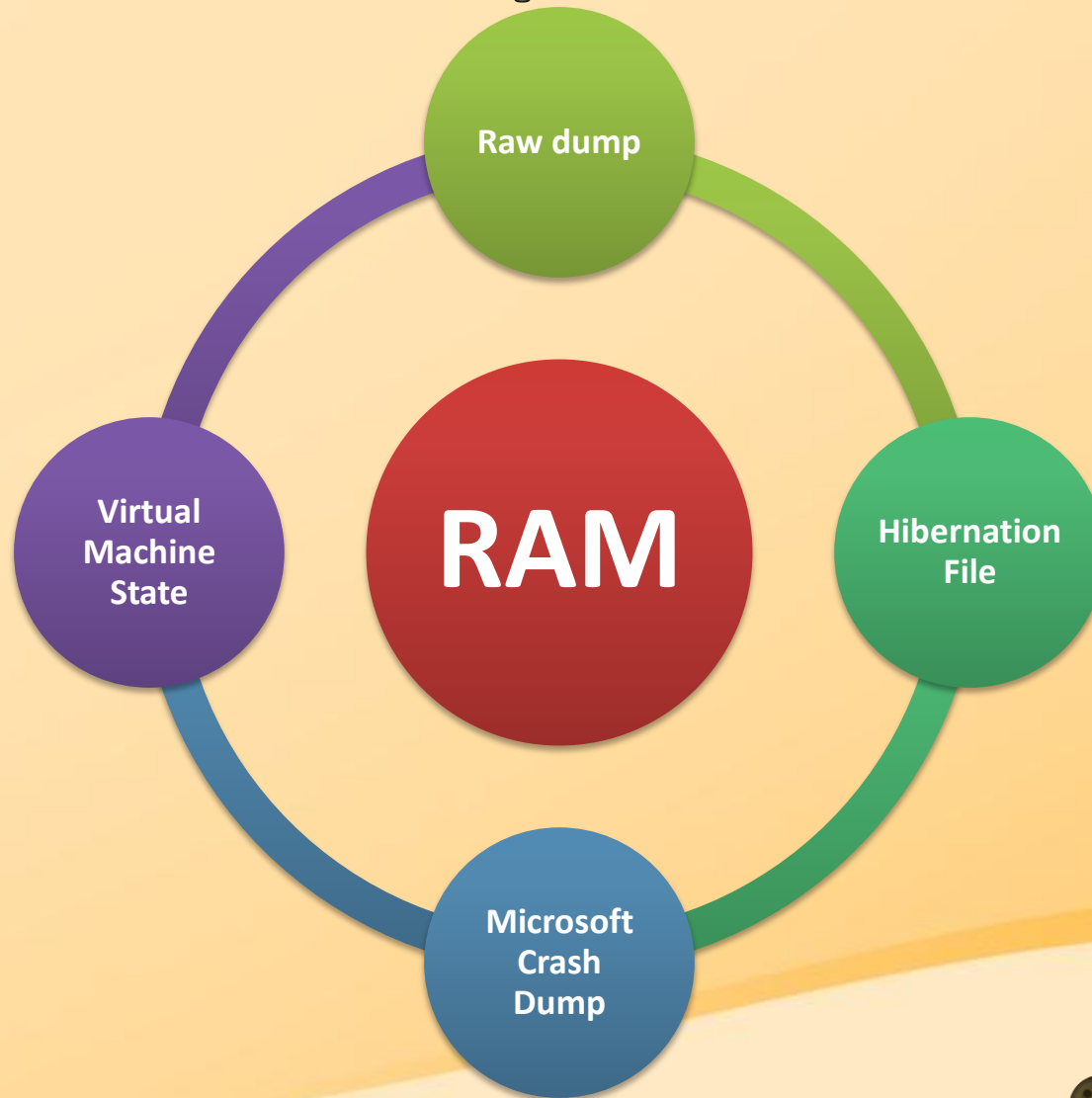
- Incident Responder
  - We just got pwned ! There is not artifact of the exploit on disk ! Let's do a memory dump to find the source of this ! @!&\$``^ WTF Adobe Acrobat Reader is using 400MB of the physical address space with only 90 90 90 90 90 90 90 everywhere ?



# Agenda

- Who ?
- Why ?
- What / How ?

# What / How ?



# What / How ?

- Physical Attacks too
  - DMA via Bus PCI (FireWire, PCMCIA, ExpressCard, ...)
  - See VirtDbg
    - (Damien Aumaitre, Christophe Devine – 2010)
    - FPGA over CardBus for DMA I/O
    - Early stage of Dev, but looks interesting. Unfortunately, there is no release yet.

# Software versus Physical

- Software's way do not require any hardware specification.
- Can also be an artifact
  - E.g. hibernation file never wiped.
- Can be acquired remotely over TCP
- Click'n'go.

# Software versus Physical

- Whatever you can say.
  - It's easy to bypass the O.S. [...] the cat and mouse game blabla [...]
  - What people tell you is that it works in both ways !
- Software is everywhere – even in virtualization.

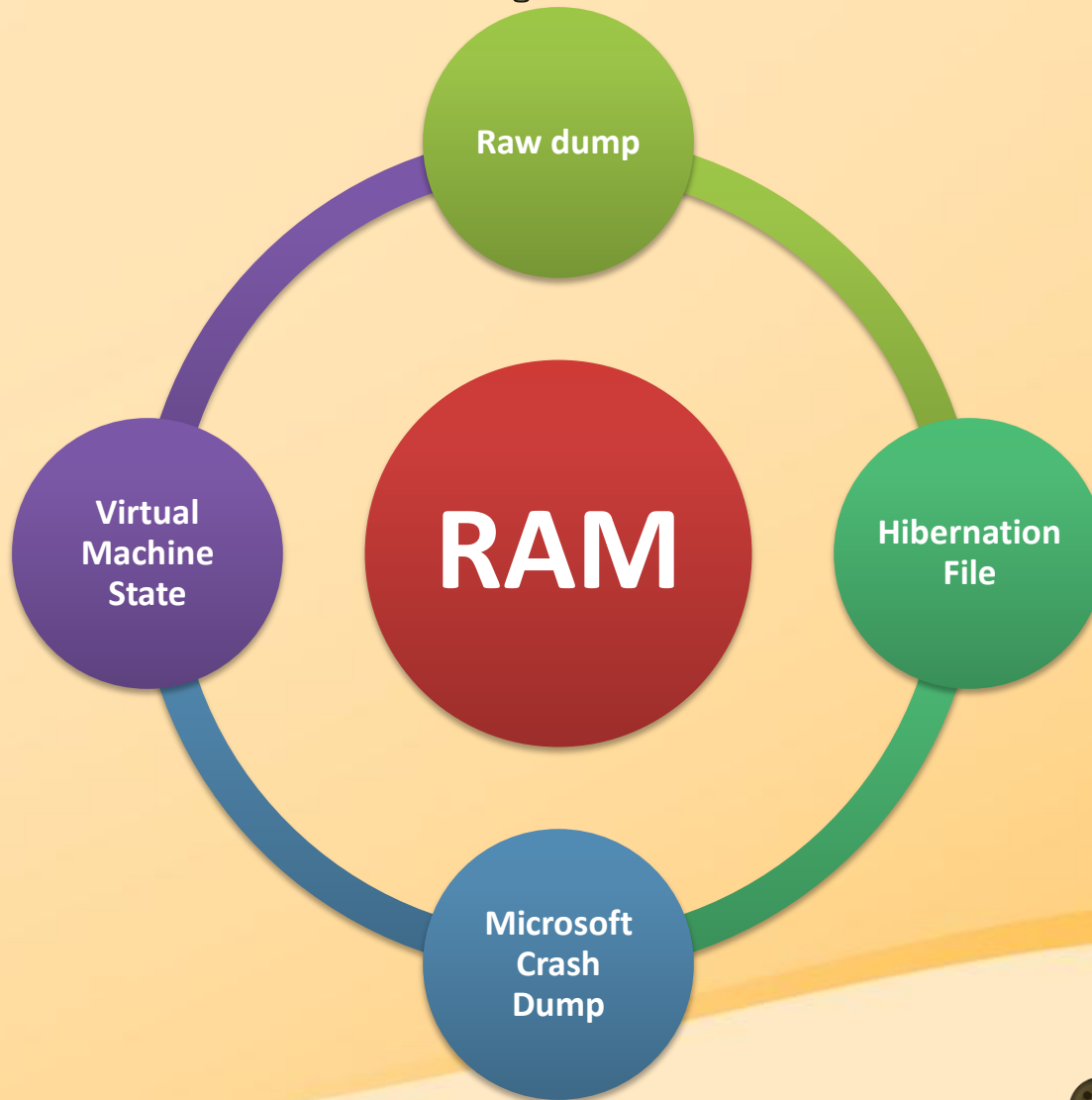
# Virtualization

- Since virtualization is widely used for servers.
- Most of Hypervisors do have an “pause”/ “suspend” feature of the state of the virtual machine.
  - State is saved and/or maintained on disk.
  - E.g. **.vmem** file with VMWare Workstation
  - E.g. **.bin** file with Microsoft Hyper-V

# Main

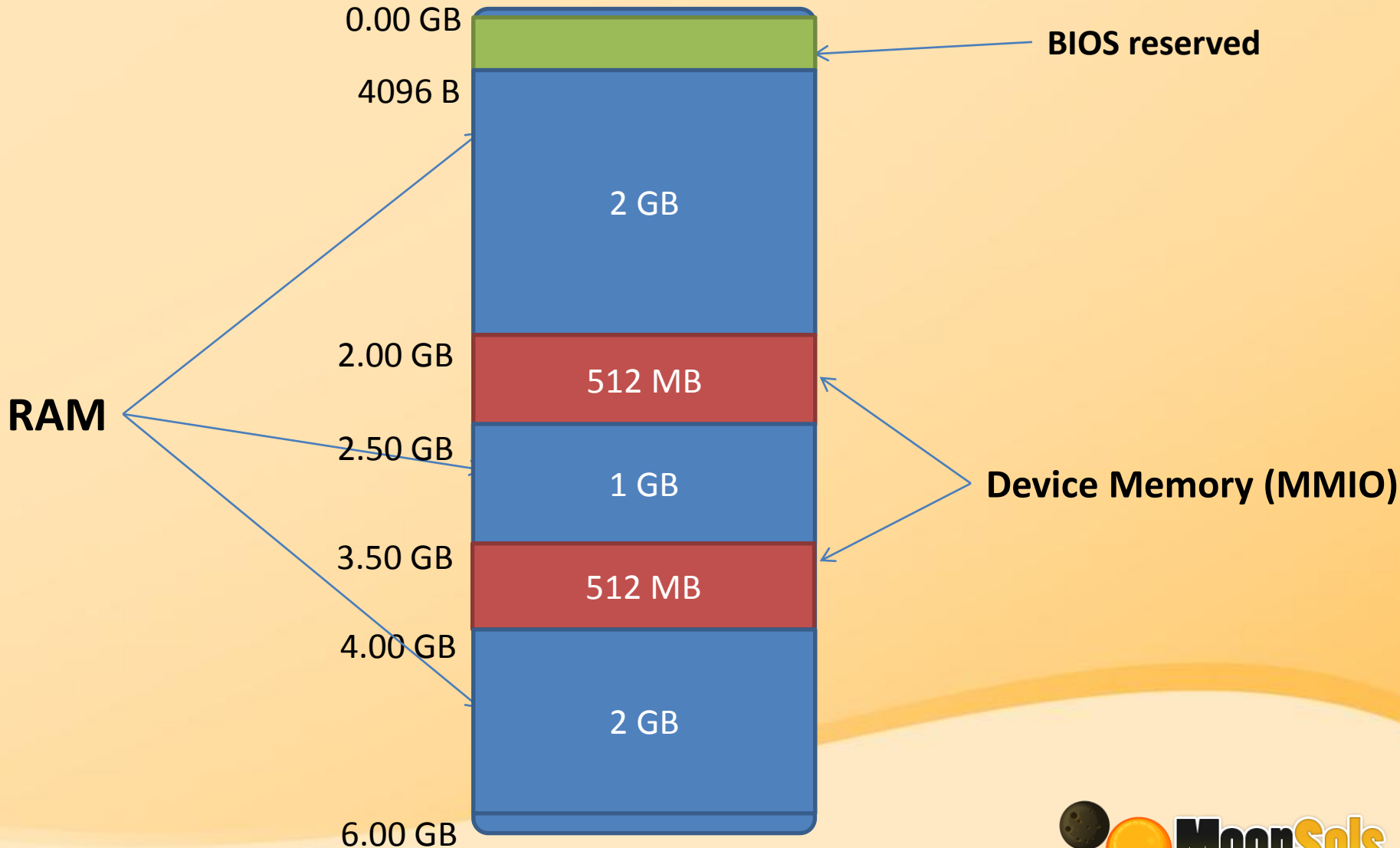
- Hibernation file
  - Compressed
- Microsoft Crash Dump
  - B.S.O.D.
- Raw
  - \Device\PhysicalMemory

# What / How ?





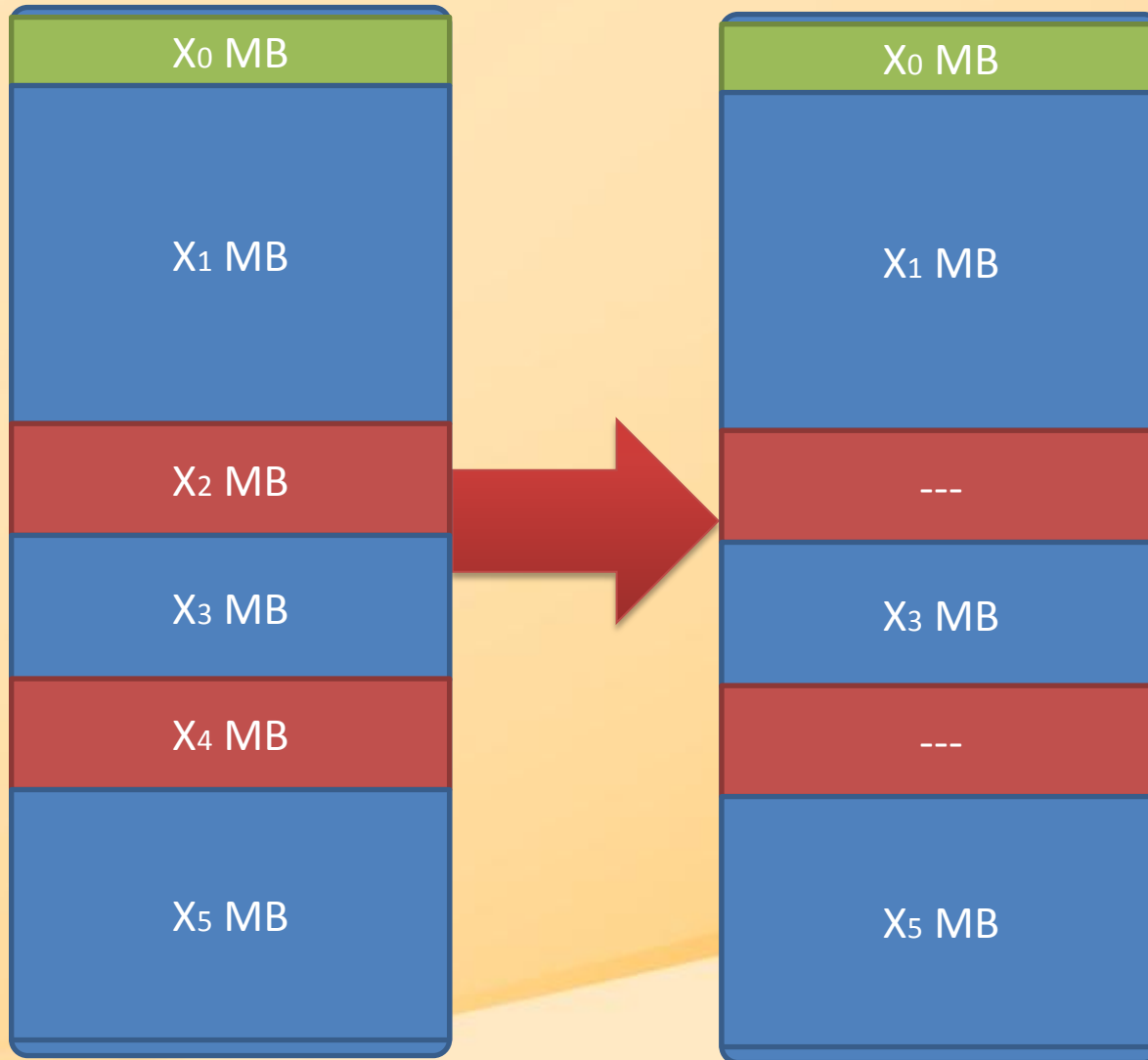
# Physical Memory Mapping



# Physical Memory Mapping

- Blue Blocks are the physical memory
- These blocks are copied into the
  - Microsoft hibernation file
    - 4GB limitation (Patched/Improved in Win7)
  - Microsoft crash dump file
    - 2GB limitation

# Raw Memory Dump



# Agenda

- **MoonSols Windows Memory Toolkit**
  - win32dd
  - win64dd
  - dmp2bin
  - bin2dmp
  - hibr2dmp
  - hibr2bin

# Win32dd & Win64dd

- Physical memory acquisition utility for Windows (*x86 and x64, from NT 5.1 to 6.1*)
- Supported format
  - Raw format
  - Microsoft crash dump (*don't need to be in debug mode*)
- Hashing features (MD5, SHA1, SHA-256)
- 3 different memory mapping techniques
- Let you chose what you want to copy
  - **Blue**, **Red**, **Green** blocks

# Win32dd & Win64dd

- Can send a memory dump remotely from kernel-land
- **AND** does have a server feature to receive the dump
- Super-fast
- Support SMB file system as target path
- NO SYMBOLS REQUIRED
  - Unlike Sysinternal's livekd.

# Server Mode

Host to acquire

Server Mode

```
windd /t sample moonsols.com /d
```



```
Windd /l /f F:\ moonsols.dmp
```

**sample.moonsols.com**

Send data to collect from the host to sample.moonsols.com.

C:\Windows\system32\cmd.exe - win64dd.exe /l /f D:\Dumps\Windows\Crash\remote.dmp

I:\MoonSols\Products>win64dd.exe /l /f D:\Dumps\Windows\Crash\remote.dmp

```
I:\MoonSols\Products\win64dd.exe
win64dd - 1.3.1.20100405 - (Professional Edition - Single User Licence)
Kernel land physical memory acquisition
Copyright (C) 2007 - 2010, Matthieu Suiche <http://www.msuiche.net>
Copyright (C) 2009 - 2010, MoonSols <http://www.moonsols.com>

Remote server:          0.0.0.0:1337

Remote client:         127.0.0.1
Acquisition started at: [2/6/2010 (DD/MM/YYYY) 11:36:17 (UTC)]

Processing...Done.

Acquisition finished at: [2010-06-02 (YYYY-MM-DD) 11:36:17 (UTC)]
Time elapsed:          1:21 minutes:seconds (81 secs)

--> 4147847168 bytes received.
```

Server Side

Client Side

Commands

C:\Windows\system32\cmd.exe - win64dd.exe /t localhost /d

I:\MoonSols\Products>win64dd.exe /t localhost /d

```
I:\MoonSols\Products\win64dd.exe
Paging file size:      8099348 Kb ( 7909 Mb)
Paging file available: 5967432 Kb ( 5827 Mb)

Virtual memory size:   8589934464 Kb (8388607 Mb)
Virtual memory available: 8589882020 Kb (8388556 Mb)

Extentd memory available:      0 Kb ( 0 Mb)

Physical page size:      4096 bytes
Minimum physical address: 0x00000000000001000
Maximum physical address: 0x00000000137FFF000

Address space size:      5234491392 bytes (5111808 Kb)

--> Are you sure you want to continue? [y/n] y

Acquisition started at: [2/6/2010 (DD/MM/YYYY) 11:36:17 (UTC)]

Processing...Done.

Acquisition finished at: [2010-06-02 (YYYY-MM-DD) 11:37:39 (UTC)]
Time elapsed:          1:21 minutes:seconds (81 secs)

Created file size:      4147847168 bytes ( 3955 Mb)

NtStatus (troubleshooting): 0x00000000
Total of written pages:    1012658
Total of inaccessible pages: 0
Total of accessible pages: 1012658

MD5: 5B2044C4265DFB0715DAF769F737A485

Physical memory in use:    41%
Physical memory size:     4050624 Kb ( 3955 Mb)
Physical memory available: 2384772 Kb ( 2328 Mb)

Paging file size:        8099348 Kb ( 7909 Mb)
Paging file available:   5993368 Kb ( 5852 Mb)

Virtual memory size:     8589934464 Kb (8388607 Mb)
Virtual memory available: 8589882020 Kb (8388556 Mb)

Extentd memory available:      0 Kb ( 0 Mb)

Physical page size:      4096 bytes
Minimum physical address: 0x00000000000001000
Maximum physical address: 0x00000000137FFF000

Address space size:      5234491392 bytes (5111808 Kb)
```



```
I:\MoonSols\Products>whoami  
win-usqpn6k58fb\msuiche
```

```
I:\MoonSols\Products>win64dd.exe /d /f D:\Dumps\Windows\Crash\win2008r2.dmp
```

```
I:\MoonSols\Products\win64dd.exe
```

```
win64dd - 1.3.1.20100405 - (Professional Edition - Single User Licence)  
Kernel land physical memory acquisition  
Copyright (C) 2007 - 2010, Matthieu Suiche <http://www.msuiche.net>  
Copyright (C) 2009 - 2010, MoonSols <http://www.moonsols.com>
```

Name	Value
File type:	Microsoft memory crash dump file
Acquisition method:	PFN Mapping
Content:	Memory manager physical memory block

Destination path: D:\Dumps\Windows\Crash\win2008r2.dmp

O.S. Version: Microsoft Windows Server 2008 R2 Server Enterprise, 64-bit (build 7600)  
Computer name: WIN-USQPN6K58FB

Physical memory in use: 37%  
Physical memory size: 4050624 Kb ( 3955 Mb)  
Physical memory available: 2536644 Kb ( 2477 Mb)

Paging file size: 8099348 Kb ( 7909 Mb)  
Paging file available: 6181984 Kb ( 6037 Mb)

Virtual memory size: 8589934464 Kb (8388607 Mb)  
Virtual memory available: 8589886004 Kb (8388560 Mb)

Extended memory available: 0 Kb ( 0 Mb)

Physical page size: 4096 bytes  
Minimum physical address: 0x0000000000001000  
Maximum physical address: 0x0000000137FFF000

Address space size: 5234491392 bytes (5111808 Kb)

--> Are you sure you want to continue? [y/n] y

Acquisition started at: [2/6/2010 (DD/MM/YYYY) 8:47:12 (UTC)]

Processing...Done.

Acquisition finished at: [2010-06-02 (YYYY-MM-DD) 8:48:13 (UTC)]  
Time elapsed: 1:00 minutes:seconds (60 secs)

Created file size: 4147847168 bytes ( 3955 Mb)

NtStatus (troubleshooting): 0x00000000  
Total of written pages: 1012658  
Total of inaccessible pages: 0  
Total of accessible pages: 1012658

- UAC Compliant
- Report on memory activity
- 60 seconds for 4GB

D:\MoonSols\Products\Windows Memory Toolkit\Professional\win32dd.exe

```
win32dd - 1.3.1.20100405 - <Professional Edition - Single User Licence>  
Kernel land physical memory acquisition  
Copyright (C) 2007 - 2010, Matthieu Suiche <http://www.msuiche.net>  
Copyright (C) 2009 - 2010, MoonSols <http://www.moonsols.com>
```

Computer Name: BBPP

#1 Do you want to acquire physical memory of this local computer ?

- y Yes (default)
- n No
- a Abort

[y/n/a] (default: Yes) **y**

#2 What kind of memory dump you want to produce ?

- 1 Raw memory dump (default)
- 2 Microsoft crash dump
- a Abort

[1/2/a] (default: Raw) **2**

#3 Do you want to use an hash algorithm during the memory dump generation ?

- 1 None
- 2 MD5 (default)
- 3 SHA1
- 4 SHA256
- a Abort

[1/2/3/4/a] (default: MD5) **3**

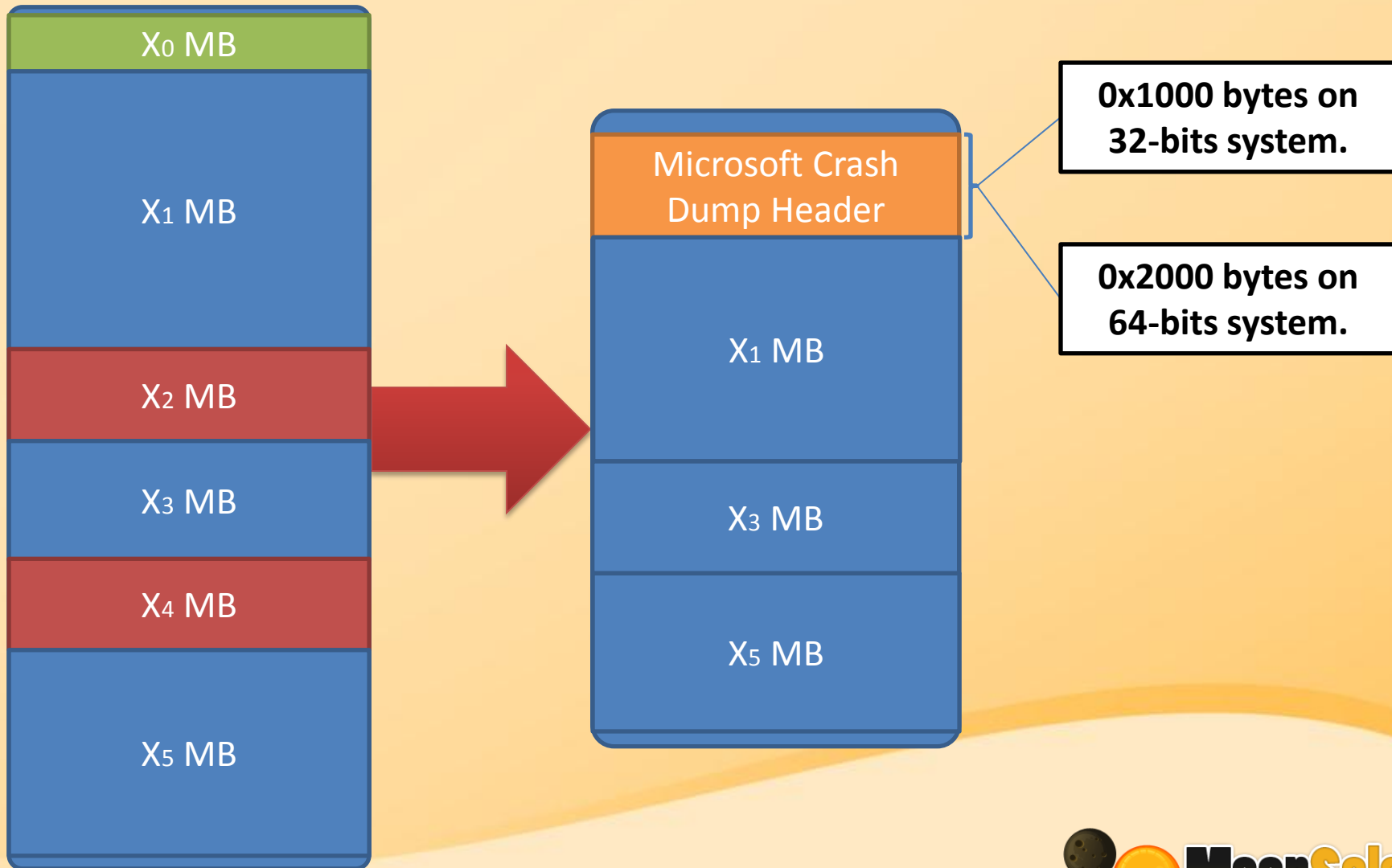
#4 What action do you plan to do ?

- 1 Acquire the memory dump on a disk (With a string path to a local HDD, a USB stick, a SMB share, ..) (default)
- 2 Send the memory dump over the network (IP address or Hostname)
- a Abort

[1/2/a] (default: Storage Disk, SMB) **1**

#5 Destination path: **magic.dmp**

# Microsoft Full Crash Dump



# Agenda

- **MoonSols Windows Memory Toolkit**
  - win32dd
  - win64dd
  - **dmp2bin**
  - bin2dmp
  - hibr2dmp
  - hibr2bin

# dmp2bin

- **dmp2bin** <input> <output>
  - Convert a Microsoft full crash dump into a linear memory dump (*raw*)
  - Print a MD5 hash of the output file.
- Works on both x86 and x64 Microsoft full crash dump.

```
C:\Windows\system32\cmd.exe - dmp2bin.exe D:\Dumps\Windows\Crash\win2008r2.dmp D:\Dumps\Windows\Crash\win...

I:\MoonSols\Products>whoami
win-usqpn6k58fb\msuiche

I:\MoonSols\Products>win64dd.exe /d /f D:\Dumps\Windows\Crash\win2008r2.dmp

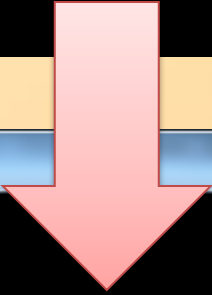
I:\MoonSols\Products>dmp2bin.exe D:\Dumps\Windows\Crash\win2008r2.dmp D:\Dumps\Windows\Crash\win2008r2.bin

dmp2bin - 1.0.20100405 - (Professional Edition - Single User Licence)
Convert Microsoft crash dump files into raw memory dump images.
Copyright (C) 2007 - 2010, Matthieu Suiche <http://www.msuiche.net>
Copyright (C) 2009 - 2010, MoonSols <http://www.moonsols.com>

Initializing memory descriptors... Done.
Sorting 8 entries... 0 seconds.
Loading file... Done.

[0x00000000B1E00000 of 0x0000000013800000]
```

- MD5 hash



```
C:\Windows\system32\cmd.exe

I:\MoonSols\Products>whoami
win-usqpn6k58fb\msuiche

I:\MoonSols\Products>win64dd.exe /d /f D:\Dumps\Windows\Crash\win2008r2.dmp

I:\MoonSols\Products>dmp2bin.exe D:\Dumps\Windows\Crash\win2008r2.dmp D:\Dumps\Windows\Crash\win2008r2.bin

dmp2bin - 1.0.20100405 - (Professional Edition - Single User Licence)
Convert Microsoft crash dump files into raw memory dump images.
Copyright (C) 2007 - 2010, Matthieu Suiche <http://www.msuiche.net>
Copyright (C) 2009 - 2010, MoonSols <http://www.moonsols.com>

Initializing memory descriptors... Done.
Sorting 8 entries... 0 seconds.
Loading file... Done.

[0x0000000013800000 of 0x0000000013800000]
MD5 = 215A32166072DCC2645C401E19374EB0

Total time for the conversion: 3 minutes 12 seconds.

I:\MoonSols\Products>
```

# Agenda

- **MoonSols Windows Memory Toolkit**
  - win32dd
  - win64dd
  - dmp2bin
  - **bin2dmp**
  - hibr2dmp
  - hibr2bin

# bin2dmp

- **bin2dmp** <input> <output>
  - Convert a linear memory dump in to a Microsoft full memory crash dump.
  - Print a MD5 hash of the output file.
- Works on both x86 and x64 linear memory dump from NT 5.1 (*WinXP*) to NT 6.1 (*Win7*)
  - **HOT**: Can work on live VMWare virtual machine !



```
C:\Windows\system32\cmd.exe - bin2dmp D:\Dumps\Windows\Crash\win2008r2.bin D:\Dumps\Windows\Crash\win2008r2_2.dmp

I:\MoonSols\Products>bin2dmp D:\Dumps\Windows\Crash\win2008r2.bin D:\Dumps\Windows\Crash\win2008r2_2.dmp

bin2dmp - 1.0.20100405 - (Professional Edition - Single User Licence)
Convert raw memory dump images into Microsoft crash dump files.
Copyright (C) 2007 - 2010, Matthieu Suiche <http://www.msuiche.net>
Copyright (C) 2009 - 2010, MoonSols <http://www.moonsols.com>

Initializing memory descriptors... Done.
Looking for kernel variables... Done.
Loading file... Done.

Rewriting CONTEXT for Windbg...
-> Context->SegCs at physical address 0x0000000005C01F78 is already equal to 10
-> Context->SegDs at physical address 0x0000000005C01F7A is already equal to 2b
-> Context->SegEs at physical address 0x0000000005C01F7C is already equal to 2b
-> Context->SegFs at physical address 0x0000000005C01F7E is already equal to 53
-> Context->SegGs at physical address 0x0000000005C01F80 modified from 2b into 00
-> Context->SegSs at physical address 0x0000000005C01F82 is already equal to 18

[0x00000000101FE000 of 0x0000000013800000]
```

• MD5 hash

```
I:\MoonSols\Products>bin2dmp D:\Dumps\Windows\Crash\win2008r2.bin D:\Dumps\Windows\Crash\win2008r2_2.dmp

bin2dmp - 1.0.20100405 - (Professional Edition - Single User Licence)
Convert raw memory dump images into Microsoft crash dump files.
Copyright (C) 2007 - 2010, Matthieu Suiche <http://www.msuiche.net>
Copyright (C) 2009 - 2010, MoonSols <http://www.moonsols.com>

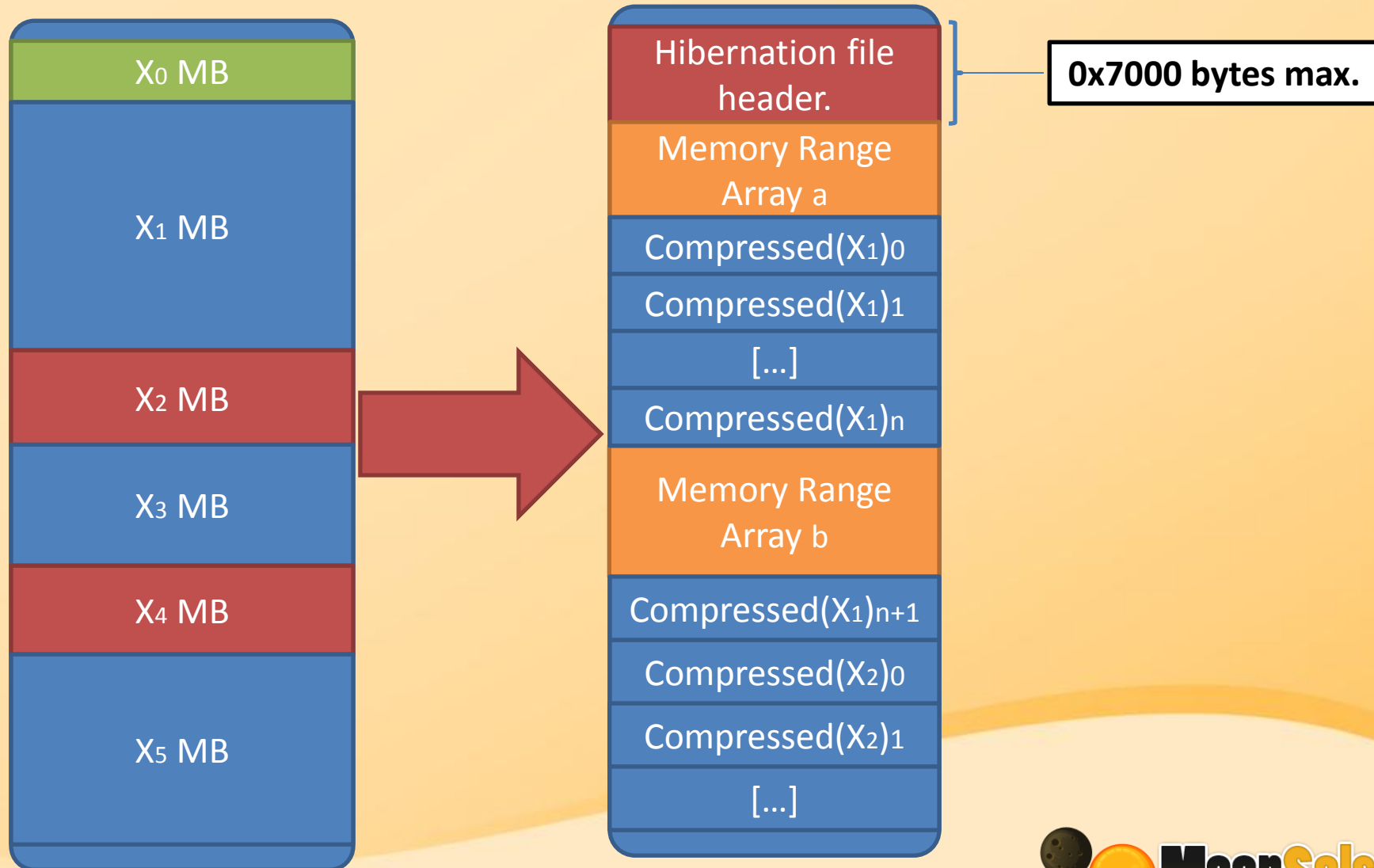
Initializing memory descriptors... Done.
Looking for kernel variables... Done.
Loading file... Done.

Rewriting CONTEXT for Windbg...
-> Context->SegCs at physical address 0x0000000005C01F78 is already equal to 10
-> Context->SegDs at physical address 0x0000000005C01F7A is already equal to 2b
-> Context->SegEs at physical address 0x0000000005C01F7C is already equal to 2b
-> Context->SegFs at physical address 0x0000000005C01F7E is already equal to 53
-> Context->SegGs at physical address 0x0000000005C01F80 modified from 2b into 00
-> Context->SegSs at physical address 0x0000000005C01F82 is already equal to 18

[0x0000000013800000 of 0x0000000013800000]
MD5 = F1C7E012FEF2F595F23A10AA35B3A5DB

Total time for the conversion: 3 minutes 16 seconds.
```

# Microsoft hibernation file



# Agenda

- **MoonSols Windows Memory Toolkit**
  - win32dd
  - win64dd
  - dmp2bin
  - bin2dmp
  - **hibr2dmp**
  - hibr2bin

# hibr2dmp

- **hibr2dmp** <input> <output>
  - Convert a Microsoft hibernation file into a Microsoft full memory crash dump.
  - Print a MD5 hash of the output file.
- Works on both x86 and x64 linear memory dump from NT 5.1 (*WinXP*) to NT 6.1 (*Win7*)

```
C:\Windows\system32\cmd.exe - hibr2dmp.exe D:\Dumps\Windows\Hibernat\win7rtm_x64.sys D:\Dumps\Windows\Cras...
I:\MoonSols\Products>hibr2dmp.exe D:\Dumps\Windows\Hibernat\win7rtm_x64.sys D:\Dumps\Windows\Crash\win7rtm_x64.dmp

hibr2dmp - 1.0.20100405 - (Professional Edition - Single User Licence)
Convert Microsoft hibernation files into Microsoft crash dump files.
Copyright (C) 2007 - 2010, Matthieu Suiche <http://www.msuiche.net>
Copyright (C) 2009 - 2010, MoonSols <http://www.moonsols.com>

Initializing memory descriptors... Done.
Sorting 110091 entries... 39 seconds.
Looking for kernel variables... Done.
Loading file... Done.

Rewriting CONTEXT for Windbg...
-> Context->SegCs at physical address 0x0000000004FE1F78 is already equal to 10
-> Context->SegDs at physical address 0x0000000004FE1F7A is already equal to 2b
-> Context->SegEs at physical address 0x0000000004FE1F7C is already equal to 2b
-> Context->SegFs at physical address 0x0000000004FE1F7E is already equal to 53
-> Context->SegGs at physical address 0x0000000004FE1F80 modified from 2b into 00
-> Context->SegSs at physical address 0x0000000004FE1F82 modified from 00 into 18

[0x00000000043FE000 of 0x0000000040000000]
```

- MD5 hash

```
hibr2dmp - 1.0.20100405 - (Professional Edition - Single User Licence)
Convert Microsoft hibernation files into Microsoft crash dump files.
Copyright (C) 2007 - 2010, Matthieu Suiche <http://www.msuiche.net>
Copyright (C) 2009 - 2010, MoonSols <http://www.moonsols.com>

Initializing memory descriptors... Done.
Sorting 110091 entries... 39 seconds.
Looking for kernel variables... Done.
Loading file... Done.

Rewriting CONTEXT for Windbg...
-> Context->SegCs at physical address 0x0000000004FE1F78 is already equal to 10
-> Context->SegDs at physical address 0x0000000004FE1F7A is already equal to 2b
-> Context->SegEs at physical address 0x0000000004FE1F7C is already equal to 2b
-> Context->SegFs at physical address 0x0000000004FE1F7E is already equal to 53
-> Context->SegGs at physical address 0x0000000004FE1F80 modified from 2b into 00
-> Context->SegSs at physical address 0x0000000004FE1F82 modified from 00 into 18

[0x0000000004000000 of 0x0000000040000000]
MD5 = 053938F555A03BC22F61892DFB026FF2

Total time for the conversion: 2 minutes 24 seconds.
```

# Agenda

- **MoonSols Windows Memory Toolkit**
  - win32dd
  - win64dd
  - dmp2bin
  - bin2dmp
  - hibr2dmp
  - **hibr2bin**

# bin2dmp

- **hibr2bin** <input> <output>
  - Convert a Microsoft hibernation file into a linear memory dump.
  - Print a MD5 hash of the output file.
- Works on both x86 and x64 linear memory dump from NT 5.1 (*WinXP*) to NT 6.1 (*Win7*)

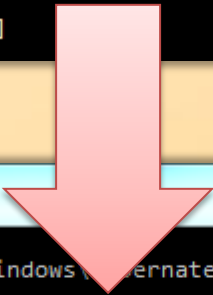
```
C:\Windows\system32\cmd.exe - hibr2bin.exe D:\Dumps\Windows\Hibernat\win7rtm_x64.sys D:\Dumps\Windows\Raw\...
I:\MoonSols\Products>hibr2bin.exe D:\Dumps\Windows\Hibernat\win7rtm_x64.sys D:\Dumps\Windows\Raw\win7rtmx64.b
in

hibr2bin - 1.0.20100405 - (Professional Edition - Single User Licence)
Convert Microsoft hibernation files into raw memory dump images.
Copyright (C) 2007 - 2010, Matthieu Suiche <http://www.msuiche.net>
Copyright (C) 2010, MoonSols <http://www.moonsols.com>

Initializing memory descriptors... Done.
Sorting 110091 entries... 39 seconds.
Looking for kernel variables... Done.
Loading file... Done.

[0x000000007C00000 of 0x0000000040000000]
```

- MD5 hash



```
C:\Windows\system32\cmd.exe
I:\MoonSols\Products>hibr2bin.exe D:\Dumps\Windows\Hibernat\win7rtm_x64.sys D:\Dumps\Windows\Raw\win7rtmx64.b
in

hibr2bin - 1.0.20100405 - (Professional Edition - Single User Licence)
Convert Microsoft hibernation files into raw memory dump images.
Copyright (C) 2007 - 2010, Matthieu Suiche <http://www.msuiche.net>
Copyright (C) 2010, MoonSols <http://www.moonsols.com>

Initializing memory descriptors... Done.
Sorting 110091 entries... 39 seconds.
Looking for kernel variables... Done.
Loading file... Done.

[0x0000000040000000 of 0x0000000040000000]
MD5 = 70ECD88F04E2D65C0CCB72686823E3AA

Total time for the conversion: 2 minutes 25 seconds.
```



# Outline

- **Raw dump**
  - No file format, then no additional information.
  - Most available tools only support this one, but this is really limited.
- **Hibernation file**
  - File format makes our life easier
  - Around 7-8 versions of the file format from WinXP to Win7, moreover it is architecture dependent.

# Outline

- **Microsoft Crash Dump**
  - Has been used for years by kernel developers, and trouble shooters.
  - Microsoft is maintaining a free tool called **“Windows Debugger”**
    - Does load automatically Debugging Symbols
    - Makes it working with every Windows version memory dump.
    - Does have an SDK

# Memory Imaging Overview

## MEMORY IMAGING

### Windows

Crash dump  
file (BSOD)

Hibernation  
File  
(Hibernate)

### Third Party Tools

win32dd & win64dd

Raw dump  
file.

Crash dump  
file (without  
BSOD)

Others

Raw dump  
file.

# Microsoft Windows Debugger

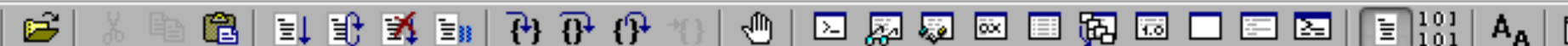
- Maintained by Microsoft itself for years.
- Firstly, designed for developers for troubleshooting such as crash dump analysis.

# Microsoft Windows Debugger

- **WinDbg** is a multipurpose graphical debugger for Microsoft Windows, distributed by Microsoft. It can be used to debug user mode applications, drivers, and the operating system itself in kernel mode.
- Available in Windows SDK [13] or WDK [14].

Dump D:\Dumps\Windows\Crash\win7rtm\_x64.dmp - WinDbg:6.12.0002.633 AMD64

File Edit View Debug Window Help



Command

```
Microsoft (R) Windows Debugger Version 6.12.0002.633 AMD64
Copyright (c) Microsoft Corporation. All rights reserved.
```

```
Loading Dump File [D:\Dumps\Windows\Crash\win7rtm_x64.dmp]
Kernel Complete Dump File: Full address space is available
```

```
Comment: 'Hibernation file converted with MoonSols Memory Toolkit'
```

```
Symbol search path is: SRV*c:\symbols*http://msdl.microsoft.com/download/symbols
```

```
Executable search path is:
```

```
Windows 7 Kernel Version 7600 UP Free x64
```

```
Product: WinNt, suite: TerminalServer SingleUserTS
```

```
Built by: 7600.16385.amd64fre.win7_rtm.090713-1255
```

```
Machine Name:
```

```
Kernel base = 0xfffff800`02606000 PsLoadedModuleList = 0xfffff800`02843e50
```

```
Debug session time: Wed Jun 2 11:43:24.291 2010 (UTC + 2:00)
```

```
System Uptime: 0 days 0:01:03.211
```

```
Loading Kernel Symbols
```

```
.....
.....
.....
```

```
Loading User Symbols
```

```
Loading unloaded module list
```

```
.....
```



# Virtualization

- Bin2dmp
  - The Professional Edition can work with running VMWare Workstation Virtual Machine on vmem files.
- **MoonSols LiveCloudKd**
  - Works with Microsoft Hyper-V R2 Virtual Machines.

```
LiveCloudKd - 1.0.20100813
Microsoft Hyper-U Virtual Machine Live Kernel Debugger
Microsoft Hyper-U Virtual Machine Physical Memory Dumper
Copyright (C) 2010, MoonSols SARL <http://www.moonsols.com>
Copyright (C) 2010, Matthieu Suiche
All rights reserved.
```

```
Virtual Machines:
--> [0] Windows 7 x64
--> [1] Windows XP SP3
```

```
Please select the ID of the virtual machine you want to play with
> 1
You selected the following virtual machine : Windows XP SP3
```

```
Action List:
--> [0] Live kernel debugger
--> [1] Linear physical memory dump
--> [2] Microsoft crash memory dump
```

```
Please select the Action ID
> 0
```

```
Microsoft (R) Windows Debugger Version 6.12.0002.633 AMD64
Copyright (c) Microsoft Corporation. All rights reserved.
```

```
Loading Dump File [C:\Windows\hddd.dmp]
Kernel Complete Dump File: Full address space is available
```

```
Comment: 'Hyper-U Memory Dump. (c) 2010 MoonSols SARL <http://www.moonsols.com>'
```

```
Symbol search path is: srv*c:\Symbols*http://msdl.microsoft.com/download/symbols
```

```
Executable search path is:
Windows XP Kernel Version 2600 (Service Pack 3) UP Free x86 compatible
Product: WinNt, suite: TerminalServer SingleUserTS
Built by: 2600.xpsp.080413-2111
Machine Name:
```

```
Kernel base = 0x804d7000 PsLoadedModuleList = 0x80553fc0
Debug session time: Sun Aug 22 20:56:14.064 2010 (UTC + 2:00)
System Uptime: 0 days 0:00:03.609
Loading Kernel Symbols
```

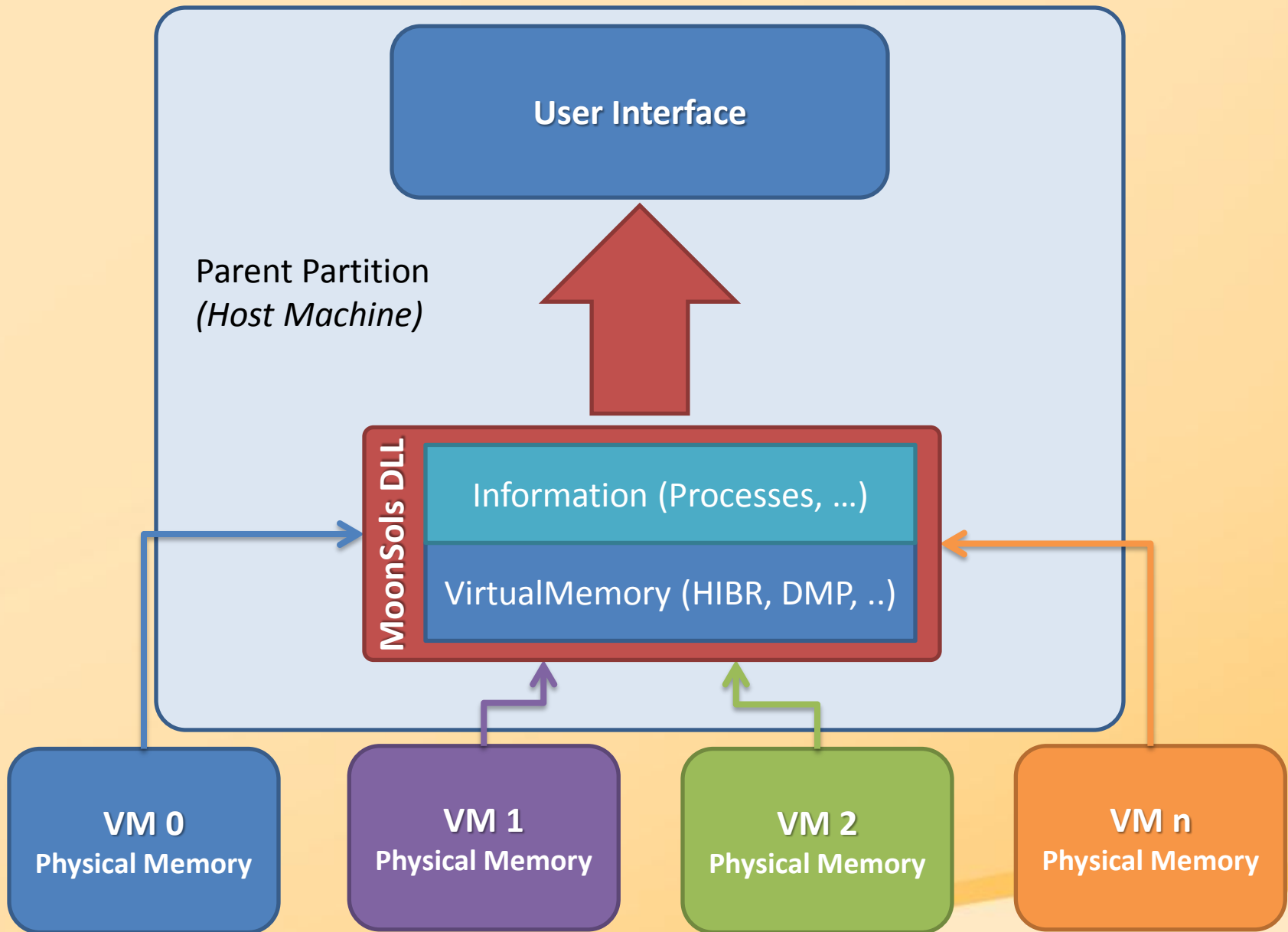
```
.....
Loading User Symbols
```

```
*****
```



# LiveCloudKd

- Works from the Hyper-V Hypervisor
  - Make possible to crash dump analyze VM
  - No debug mode required
  - Can also create either a raw or a Microsoft memory crash dump.
  - Windbg/Kd Write commands (eb/ed/e\*) works!
    - In other words you can modify the guest memory if you want.
  - Similar feature will be implemented in LiveKd 5



Bin

```

C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601.17514]
Copyright (c) 2009 Microsoft Corporation

C:\Users\hlop>whoami
hlop-pc\hlop

C:\Users\hlop>whoami
nt authority\system

C:\Users\hlop>_

```

```

C:\Program Files\Debugging Tools for Windows (x64)\hvkdgb.exe

PROCESS fffffa800157ba90
  SessionId: 0 Cid: 07d4 Peb: 7fffffff8000 ParentCid: 0200
  DirBase: 07f59000 ObjectTable: fffff8a00104eb50 HandleCount: 596.
  Image: SearchIndexer.exe

PROCESS fffffa80009aaa70
  SessionId: 1 Cid: 05e4 Peb: 7fffffffdd000 ParentCid: 0200
  DirBase: 1131b000 ObjectTable: fffff8a001ac1b60 HandleCount: 130.
  Image: taskhost.exe

PROCESS fffffa8000e609b0
  SessionId: 1 Cid: 0674 Peb: 7fffffff3000 ParentCid: 0354
  DirBase: 12081000 ObjectTable: fffff8a001da4c00 HandleCount: 69.
  Image: dwm.exe

PROCESS fffffa8000e75600
  SessionId: 1 Cid: 0318 Peb: 7fffffffdc000 ParentCid: 06d4
  DirBase: 1213c000 ObjectTable: fffff8a000f2f820 HandleCount: 709.
  Image: explorer.exe

PROCESS fffffa8000e4c060
  SessionId: 1 Cid: 05dc Peb: 7fffffffdf000 ParentCid: 0318
  DirBase: 11c54000 ObjectTable: fffff8a00047b3a0 HandleCount: 20.
  Image: cmd.exe

PROCESS fffffa8000f2a920
  SessionId: 1 Cid: 0430 Peb: 7fffffffdd000 ParentCid: 01a8
  DirBase: 13c39000 ObjectTable: fffff8a00042d640 HandleCount: 50.
  Image: conhost.exe

kd> dt nt!_EPROCESS fffffa8001825040 Token
+0x208 Token : _EX_FAST_REF
kd> dq fffffa8001825040+208
fffffa80`01825248 fffff8a0`00442047 00000000`00016402
fffffa80`01825258 00000000`00000000 00000000`00000000
fffffa80`01825268 00000000`00000000 00000000`00000000
fffffa80`01825278 00000000`00000000 00000000`00000000
fffffa80`01825288 00000000`00000043 00000000`00000000
fffffa80`01825298 00000000`00000000 00000000`00000000
fffffa80`018252a8 fffff8a0`004414a0 00000000`47hc0000
fffffa80`018252b8 00000000`82ddb3ac 00000000`00000000

kd> dt nt!_EX_FAST_REF fffffa8001825040+208
+0x000 Object : 0xfffff8a0`00442047 Void
+0x000 RefCnt : 0y0111
+0x000 Value : 0xfffff8a0`00442047
kd> dt nt!_EX_FAST_REF fffffa8000e4c060+208
+0x000 Object : 0xfffff8a0`01c47066 Void
+0x000 RefCnt : 0y0110
+0x000 Value : 0xfffff8a0`01c47066
kd> eq fffffa8000e4c060+208 0xfffff8a0`00442047
kd> dt nt!_EX_FAST_REF fffffa8000e4c060+208
+0x000 Object : 0xfffff8a0`00442047 Void
+0x000 RefCnt : 0y0111

```

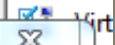
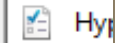
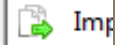
### Virtual Machines

Name	State	CPU Usage	Current Memory	Memory A
Windows 7 x64	Running	0 %	512 MB	
Windows 7 x86	Running	0 %	512 MB	
Windows XP SP3	Running	0 %	512 MB	


### Actions

WIN-US

New



VMExp



Refresh

Windows 7 x64 Windows XP SP3 Windows 7 x86

System

- smss.exe
- csrss.exe
- wininit.exe
- csrss.exe
- winlogon.exe
- services.exe
- lsass.exe
- lsm.exe
- svchost.exe
- svchost.exe
- svchost.exe

Unlock

Evil Virtual  
Machine  
Manager

Code injection



VM1

Code injection



VM2

Code injection



VM3

# +WX

- Hypervisor APIs has APIs to
  - Write Memory
  - Modify the processor state
    - EIP/RIP registers.
- Half-documented kernel functions (winhv.sys)

## Hypervisor C-Language Functions

<http://msdn.microsoft.com/en-us/library/ff543229%28VS.85%29.aspx>

But mentioned functions do not exist ... And there is no library in the WDK. (Create your own winhv.lib)

HvWriteGpa -> WinHvWriteGpa Vid.h VidDefs.h (Singularity Version – Google it)

Not in the WDK – Interface for vid.sys

It looks like an intern copied the wrong files 😊

# +WX

- Administrator rights access required on the Hypervisor, to use these APIs.
- But I don't know if it's common for an Hypervisor to inject code in his Virtual Machines.

# Conclusion

- No more need to get a Blue Screen of Death to get Microsoft Crash Dump.
- Converting a Windows hibernation file into a Microsoft crash dump is super cool
- Dumping a Live Virtual Machine too.
- LiveCloudKd open a large scope of possibilities
  - And not only for “Cloud Offensic” and Hyper-V Rootkit
    - I mean stuff that could be useful in real life.



# Future

- You'll see it's going to be fun.

Twitter: [MoonSols](#) or [msuiche](#)

Email: [msuiche@moonsols.com](mailto:msuiche@moonsols.com)

Web: <http://www.moonsols.com>

Download tools @ [www.moonsols.com](http://www.moonsols.com)

**OBRIGADO**

**MUCHAS GRACIAS**

