Your Cloud Is In My Pocket

Matthieu Suiche
Founder, MoonSols SARL

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.

This is NOT about

- New vulnerabilities
- 0days
- About guest to host escalation
  - It's more about host to guest descalation
- Free beers
- Hot chicks

This IS about

- A Tool
  - Hyper-V
  - VMWare
- Using physical memory of virtual machine as interface
- Offensive / Defensive / Offensics / Forensics / Rootkits / Utilities /
- **MoonSols LiveCloudKd**

Who ?

- – Kernel developers
- – Kernel troubleshooters
- – Bug hunter
- – Investigator
- – Forensic Expert
- – Malware Analyst
- – Incident Responder

Why

- Your physical memory in a nutshell
  - Debugger
  - Read / Write access ?

- New generation of Rootkits

Remember when folks got excited about Ring - 1 Rootkit (BluePill, Vitriol, ...) ?

Same same, but different

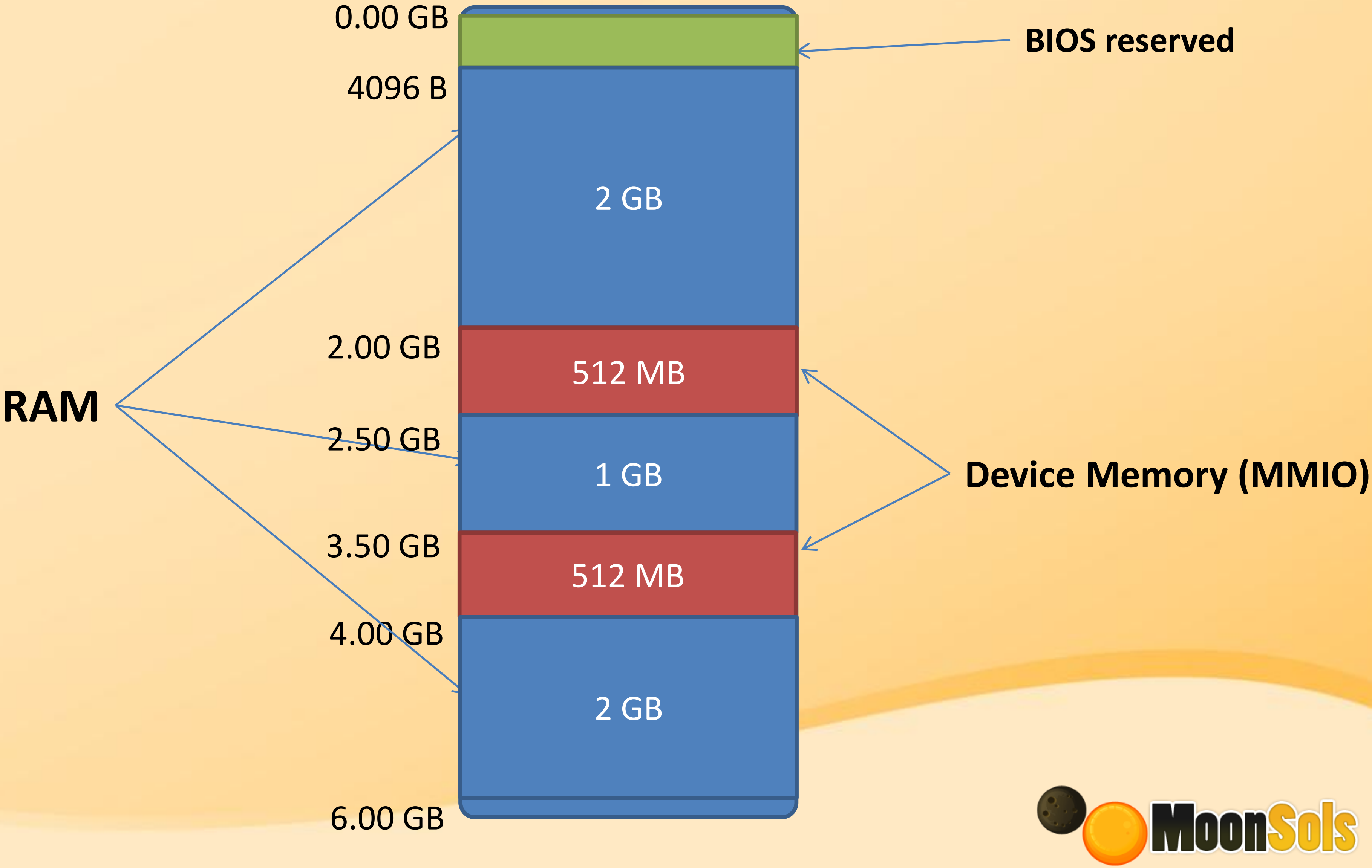
Taking over the existing Hypervisor

The physical memory

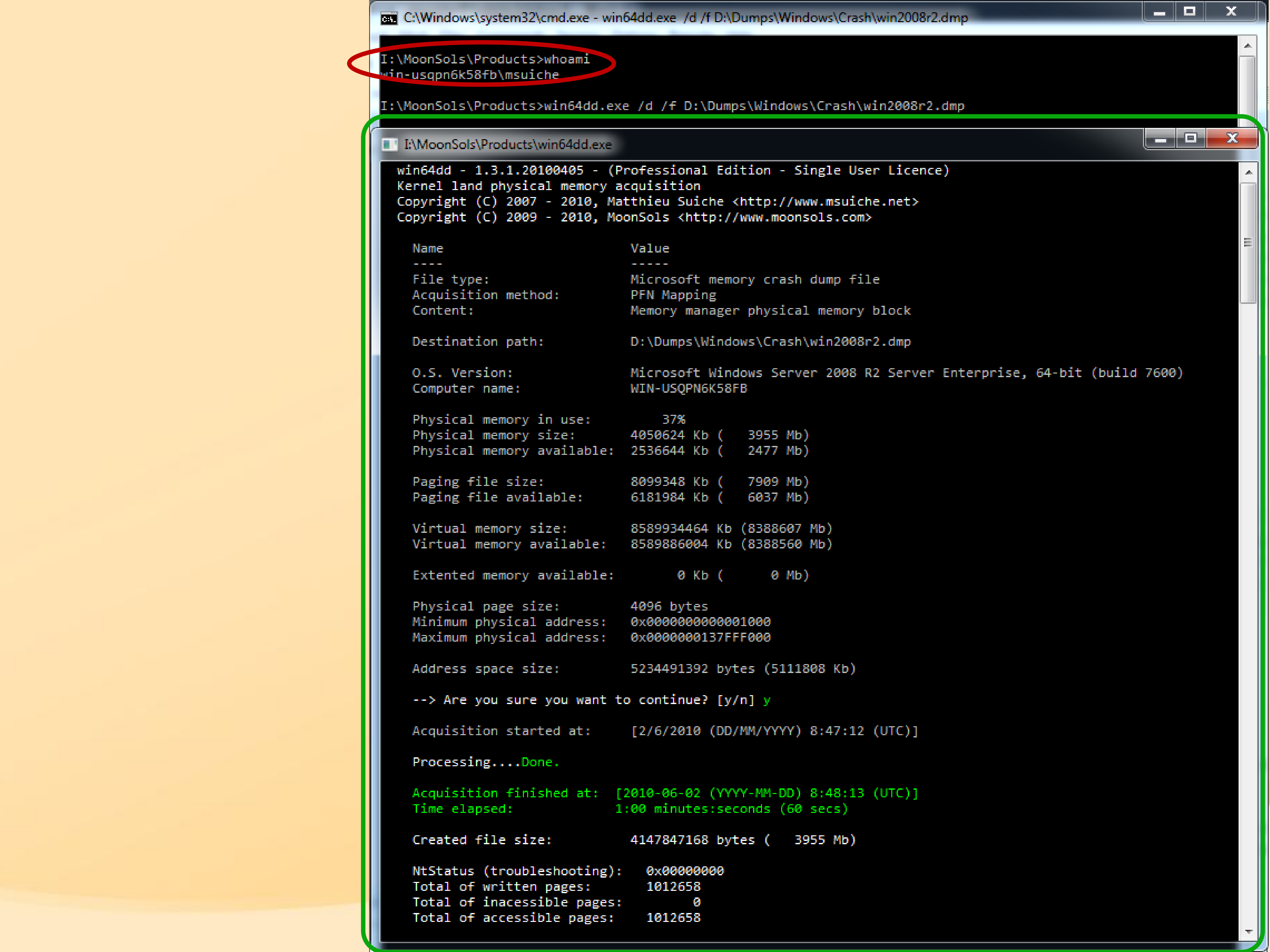
Virtualization

- 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

Physical Memory Mapping

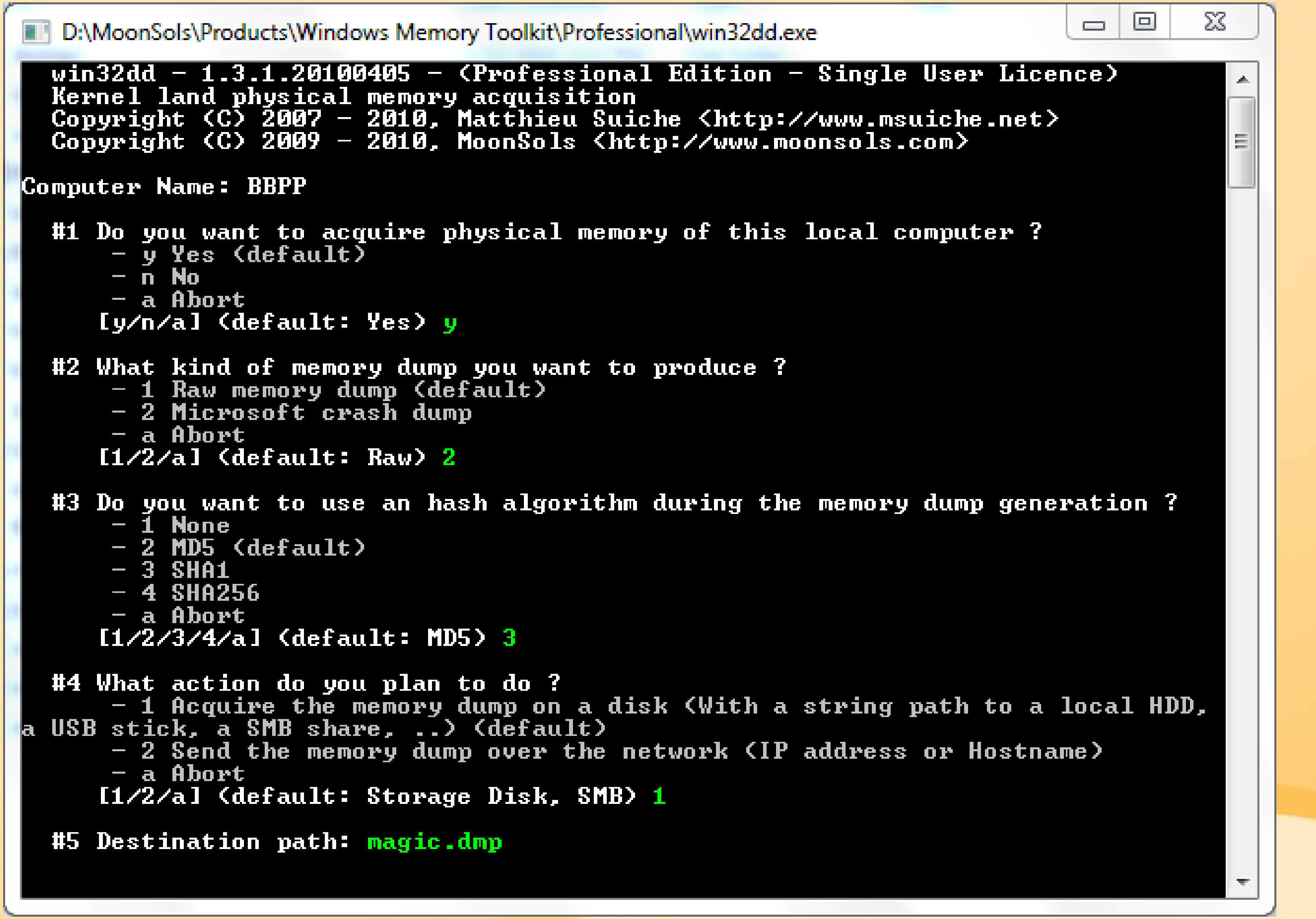


MoonSols


C:\Windows\system32\cmd.exe - win64dd.exe /d /f D:\Dumps\Windows\Crash\win2008r2.dmp
I:\MoonSols\Products\win64dd.exe

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

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

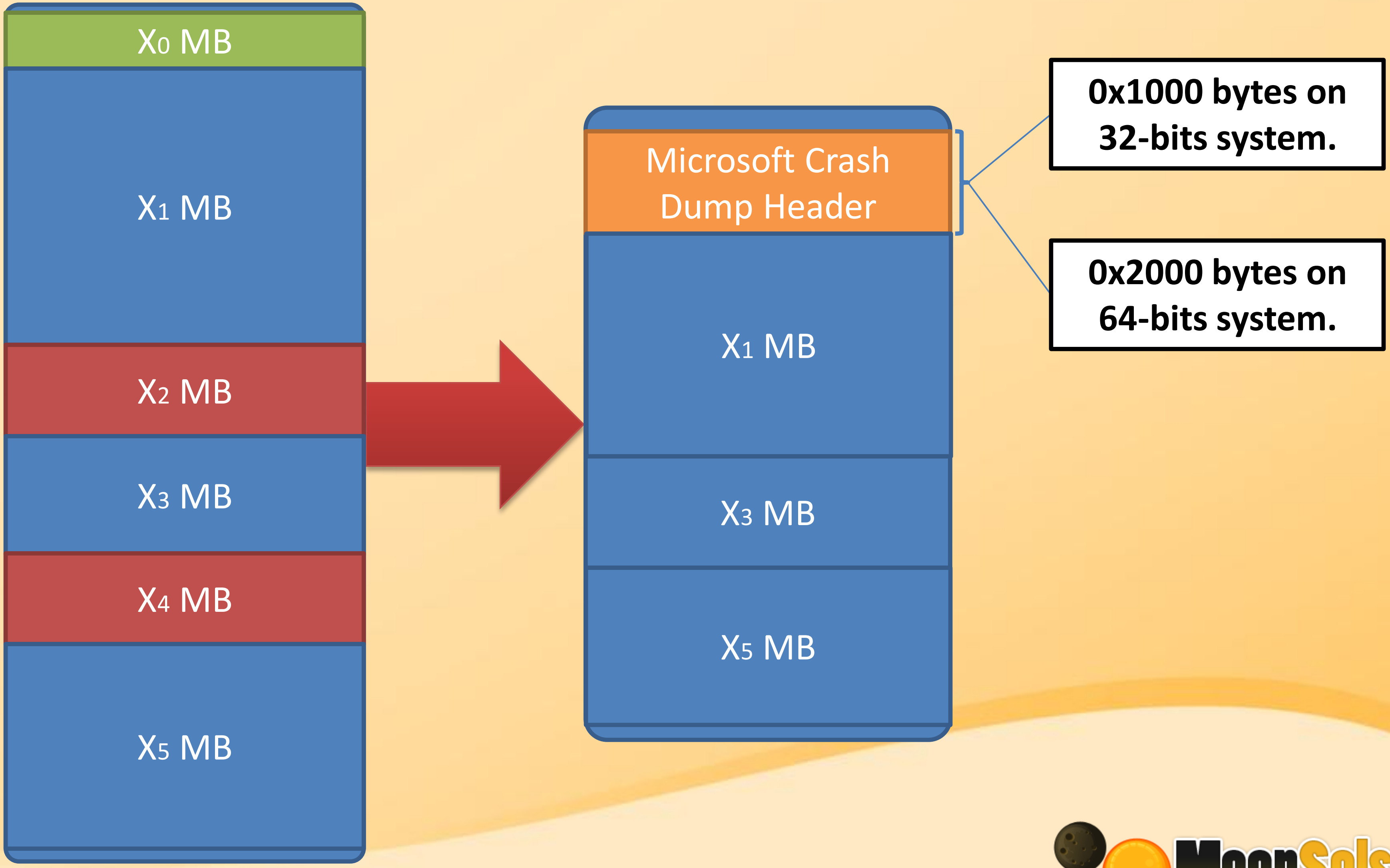
```
 win64dd - 1.3.1.20100405 - (Professional Edition - Single User Licence)
 Kernel land physical memory acquisition
 Copyright (C) 2007 - 2010, Matthieu Suiche <http://www.msuiche.net>
 Copyright (C) 2009 - 2010, MoonSols <http://www.moonsols.com>

   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)

   Extented 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 inacessible pages:          0
   Total of accessible pages:     1012658
```



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


X0 MB
X1 MB
X2 MB
X3 MB
X4 MB
X5 MB
Microsoft Crash Dump Header
X1 MB
X3 MB
X5 MB
0x1000 bytes on 32-bits system.
0x2000 bytes on 64-bits system.

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.

Virtual Machine Interface

- Physical Memory
- VMWare Workstation
  - .vmem files (raw mapping)
- Microsoft Hyper-V
  - VM Infrastructure Driver (Vid.sys)

+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)

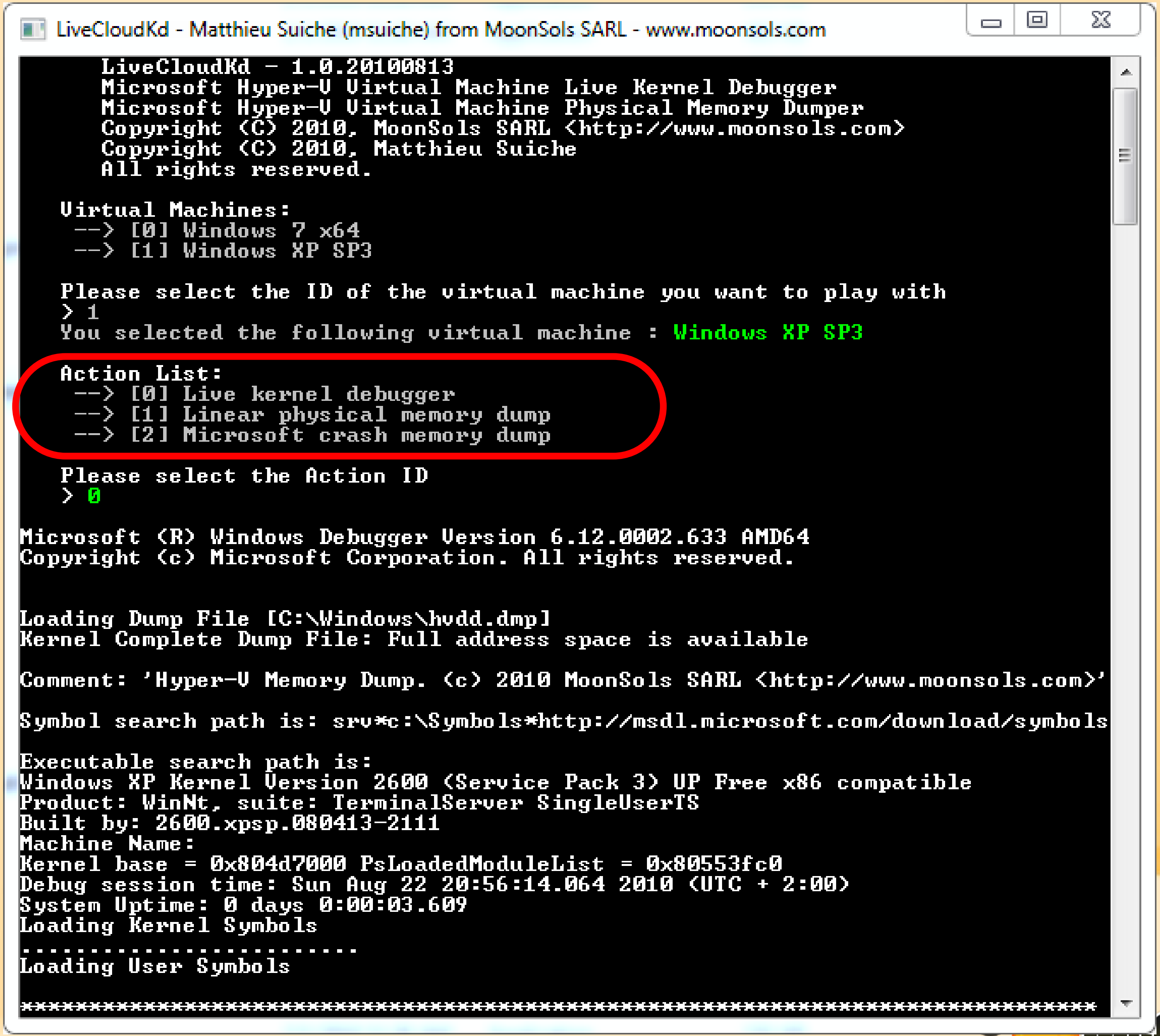
  HvWriteGpa -> WinHvWriteGpa Vid.h VidDefs.h (Singularity Version – Google it)

  Not in the WDK – Interface for vid.sys

  It looks like an intern copied the wrong files ☺

+WX

- Administrator rights access required on the Microsoft Hyper-V hypervisor, to use these APIs.
  - Not with vmem file (SHARE_READ)

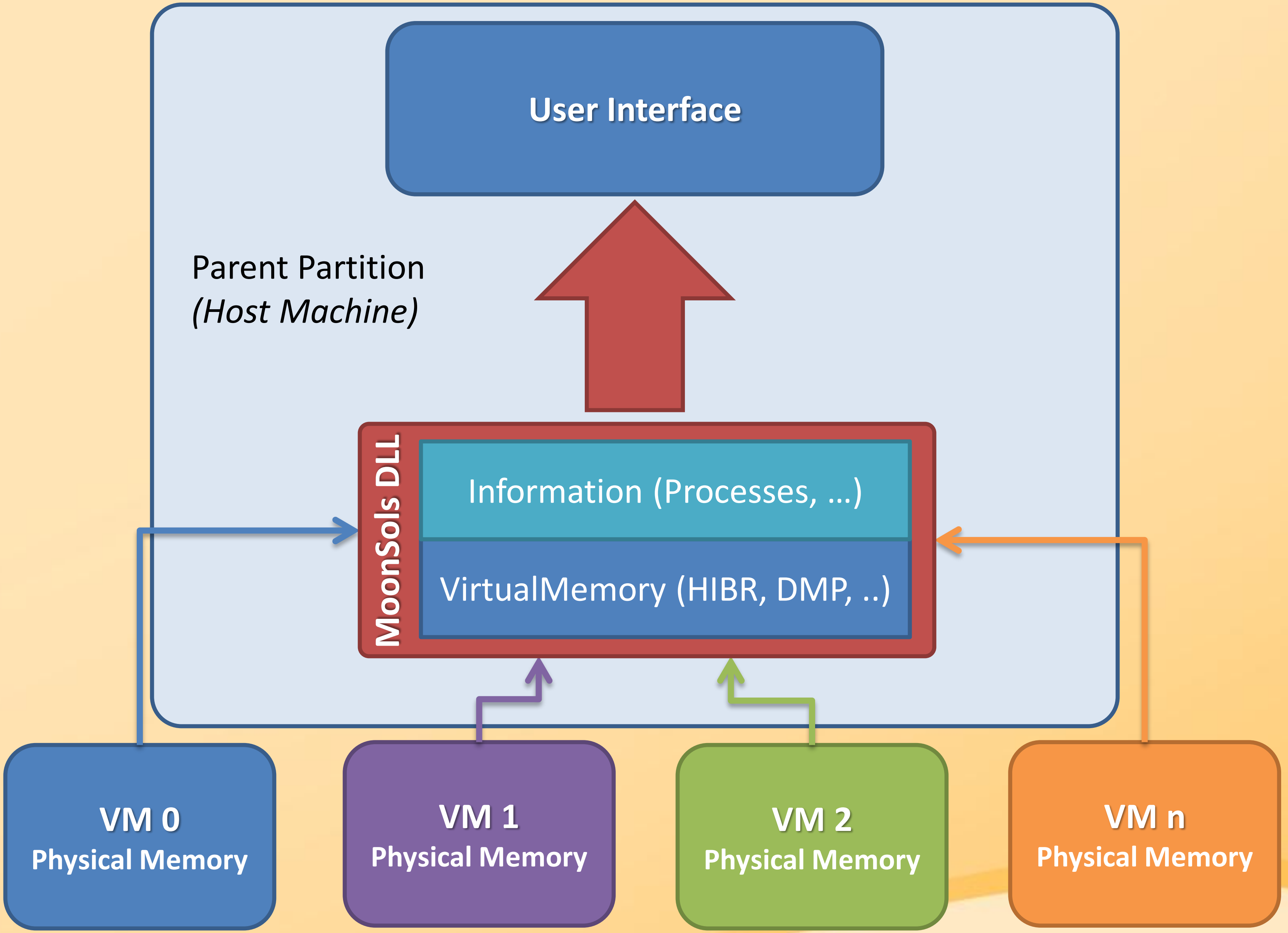


LiveCloudKd - Matthieu Suiche (msuiche) from MoonSols SARL - www.moonsols.com

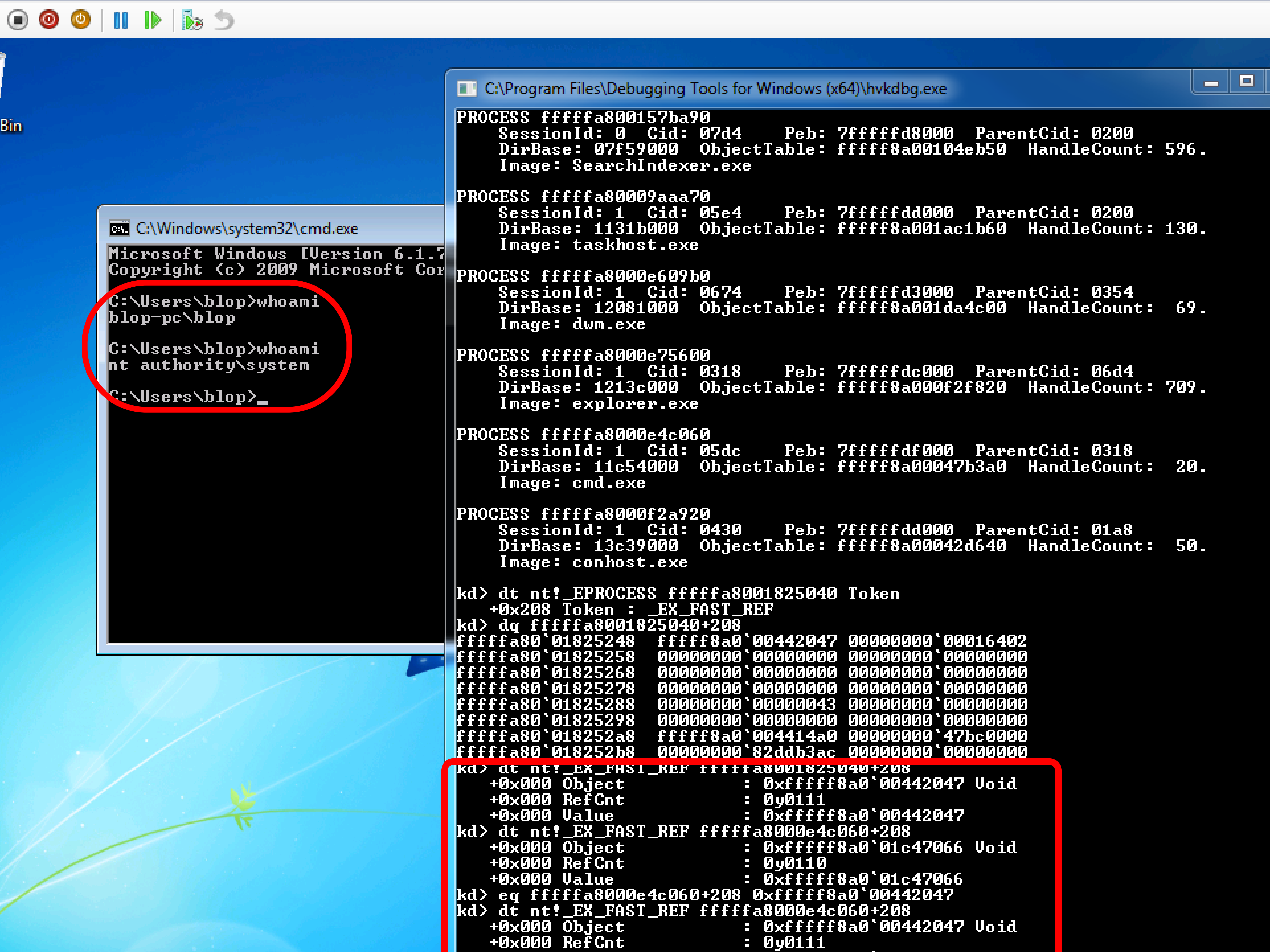
```
      LiveCloudKd - 1.0.20100813
      Microsoft Hyper-V Virtual Machine Live Kernel Debugger
      Microsoft Hyper-V Virtual Machine Physical Memory Dumper
      Copyright (C) 2010, MoonSols SARL <http://www.moonsols.com>
      Copyright (C) 2010, Matthieu Suiche
      All rights reserved.

   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\hvdd.dmp]
Kernel Complete Dump File: Full address space is available

Comment: 'Hyper-V 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 for Hyper-V Hypervisor and VMWare
  - 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.
  - LiveKd 5 update (Hyper-V Only, Read Access only)


User Interface
Parent Partition
(Host Machine)
MoonSols DLL
Information (Processes, …)
VirtualMemory (HIBR, DMP, ..)
VM 0
Physical Memory
VM 1
Physical Memory
VM 2
Physical Memory
VM n
Physical Memory

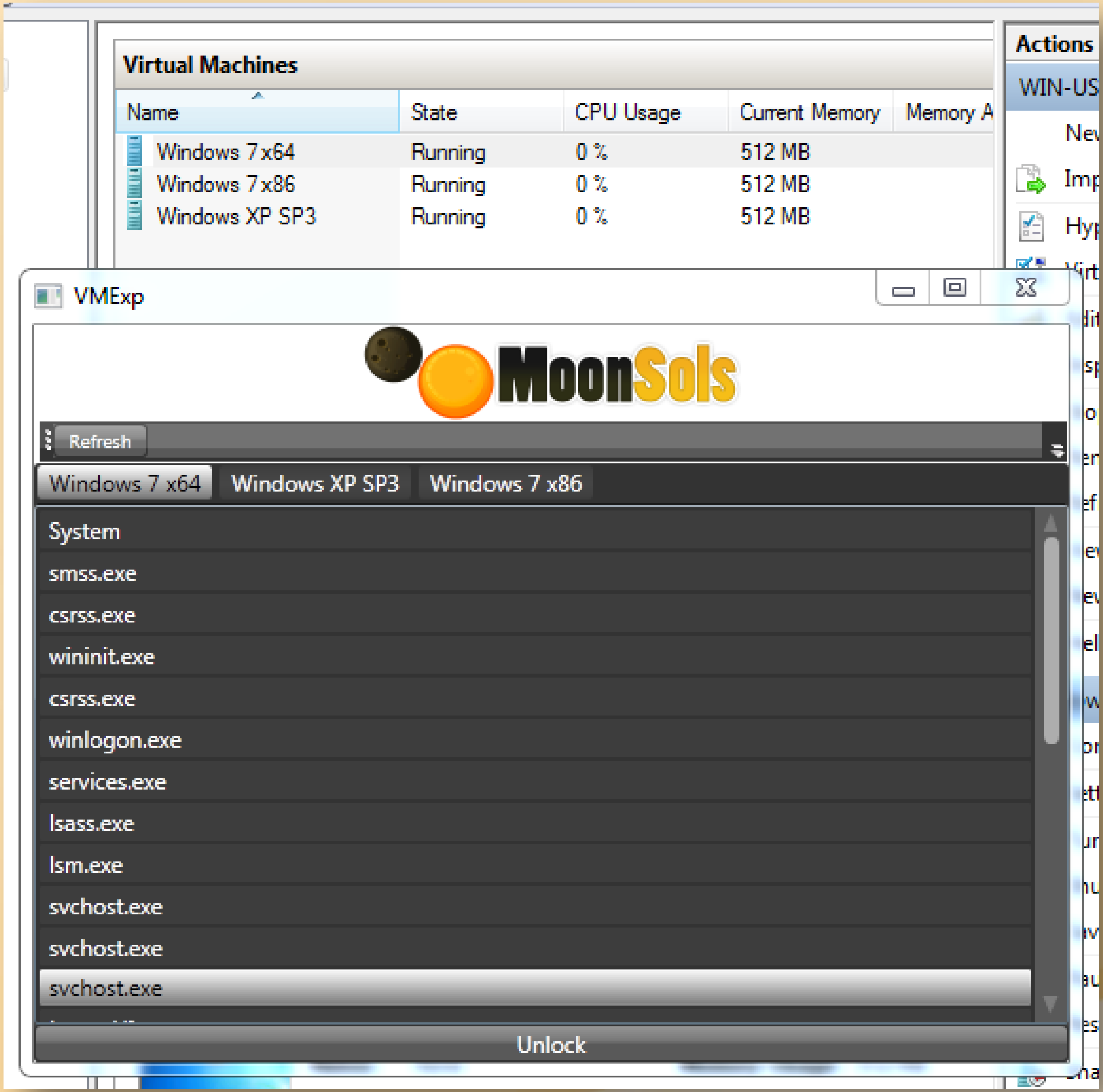
MoonSols



Bin
C:\Windows\system32\cmd.exe
C:\Program Files\Debugging Tools for Windows (x64)\hvkdbg.exe

```
Microsoft Windows [Version 6.1.7
Copyright (c) 2009 Microsoft Cor

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

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

C:\Users\blop>_
```

```
PROCESS fffffa800157ba90
    SessionId: 0  Cid: 07d4    Peb: 7fffffd8000  ParentCid: 0200
    DirBase: 07f59000  ObjectTable: fffff8a00104eb50  HandleCount: 596.
    Image: SearchIndexer.exe

PROCESS fffffa80009aaa70
    SessionId: 1  Cid: 05e4    Peb: 7fffffdd000  ParentCid: 0200
    DirBase: 1131b000  ObjectTable: fffff8a001ac1b60  HandleCount: 130.
    Image: taskhost.exe

PROCESS fffffa8000e609b0
    SessionId: 1  Cid: 0674    Peb: 7fffffd3000  ParentCid: 0354
    DirBase: 12081000  ObjectTable: fffff8a001da4c00  HandleCount:  69.
    Image: dwm.exe

PROCESS fffffa8000e75600
    SessionId: 1  Cid: 0318    Peb: 7fffffdc000  ParentCid: 06d4
    DirBase: 1213c000  ObjectTable: fffff8a000f2f820  HandleCount: 709.
    Image: explorer.exe

PROCESS fffffa8000e4c060
    SessionId: 1  Cid: 05dc    Peb: 7fffffdf000  ParentCid: 0318
    DirBase: 11c54000  ObjectTable: fffff8a00047b3a0  HandleCount:  20.
    Image: cmd.exe

PROCESS fffffa8000f2a920
    SessionId: 1  Cid: 0430    Peb: 7fffffdd000  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`47bc0000
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
```

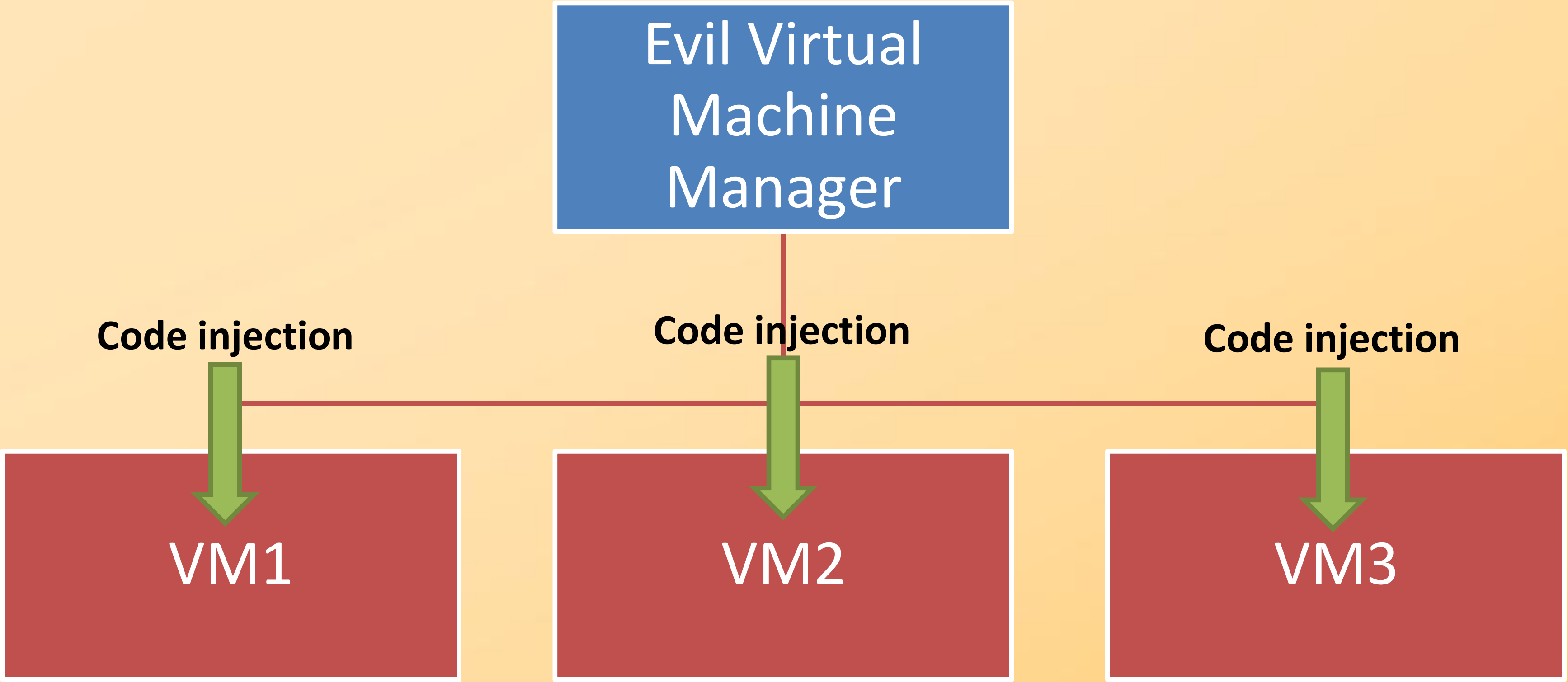


Virtual Machines

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	

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


Evil Virtual Machine Manager
Code injection
Code injection
Code injection
VM1
VM2
VM3

Conclusion

- Be lazy, be efficient.
- Forensic based research of memory analysis can be now used for a lot of things.

Twitter: MoonSols or msuiche
Email: msuiche@moonsols.com
Web: http://www.moonsols.com

Download LiveCloudKd @ www.moonsols.com

QUESTIONS ?

MoonSols