Blue Screen Of Death Is Dead

Matthieu Suiche
Founder, MoonSols
msuiche@moonsols.com

Who am I ?

- Founder of **MoonSols** *(based in France)*
- Twitter Addict
- Turned 21 *(Beers please !)*
- Reverse Engineering works related to Physical Memory
  - Windows Hibernation file
  - Memory Acquisition
  - Mac OS X Physical Memory Analysis

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 Python fuzzer in 10 lines of code ! I got a remote BSOD ! And all I got is this crash dump !
- 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.

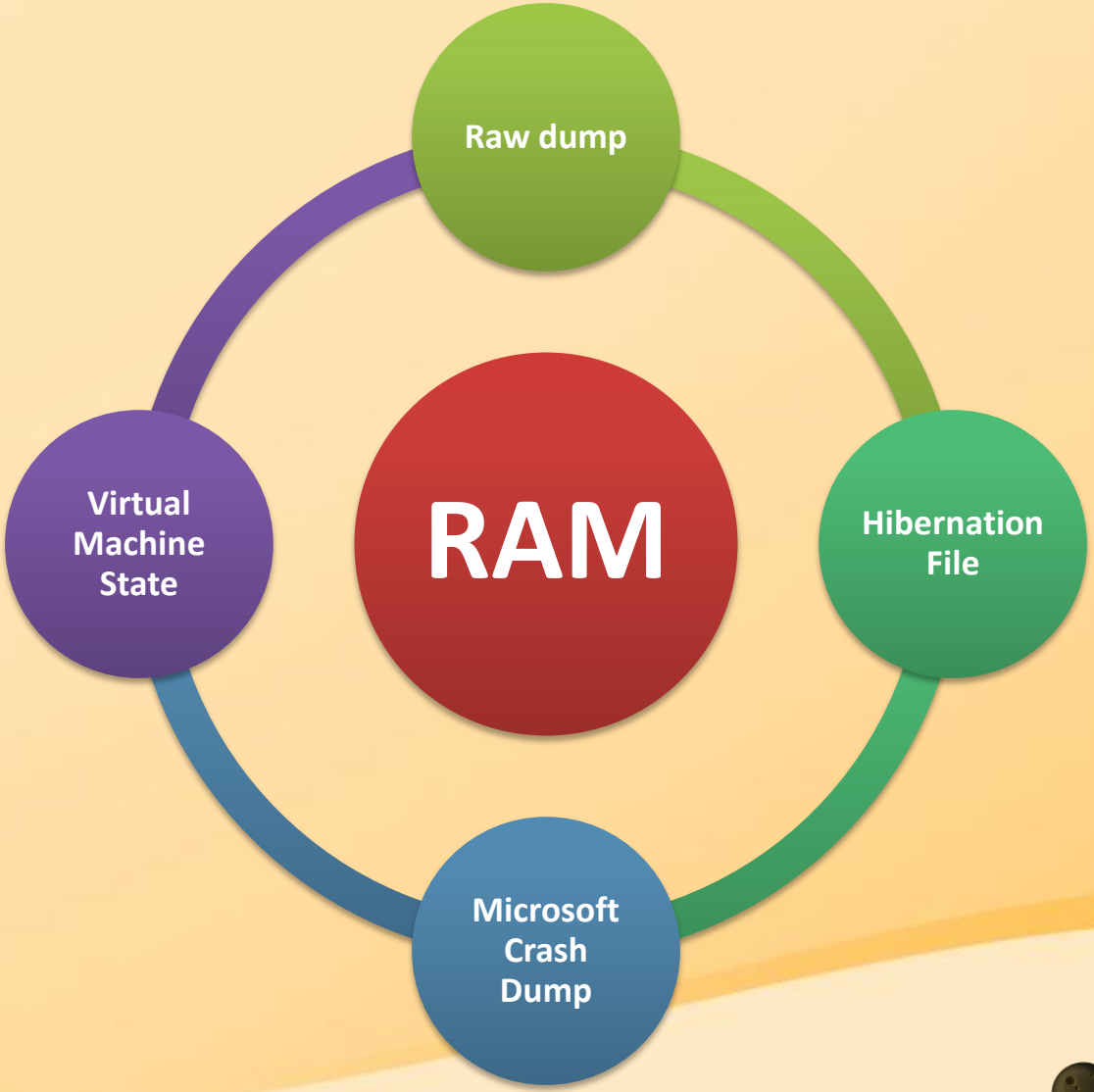
Why ?

- 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.
  - (Unless you are trying to install a NVIDIA driver on your laptop with hardware virtualization j/k)
- 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.

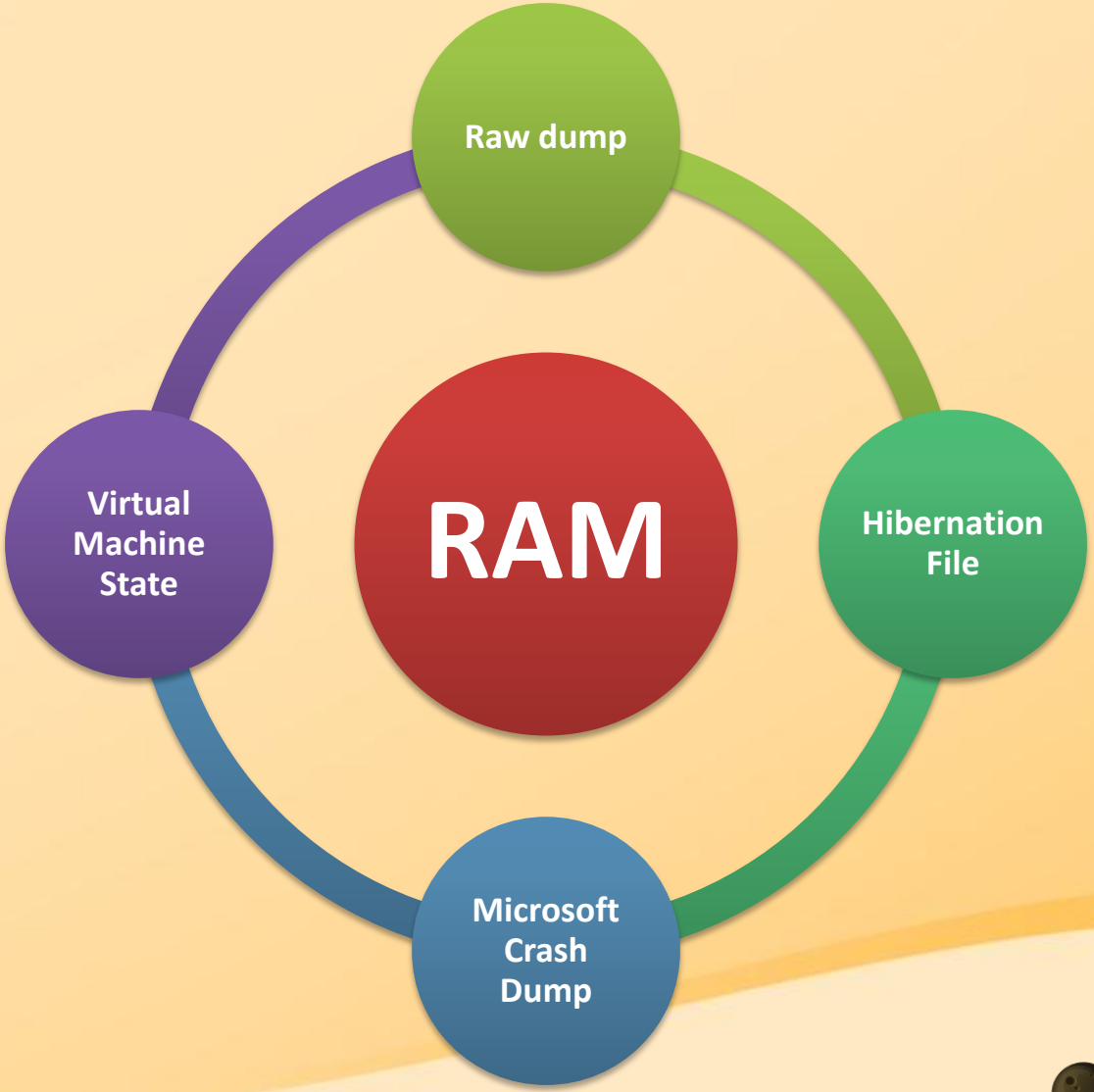
Virtualization

- 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

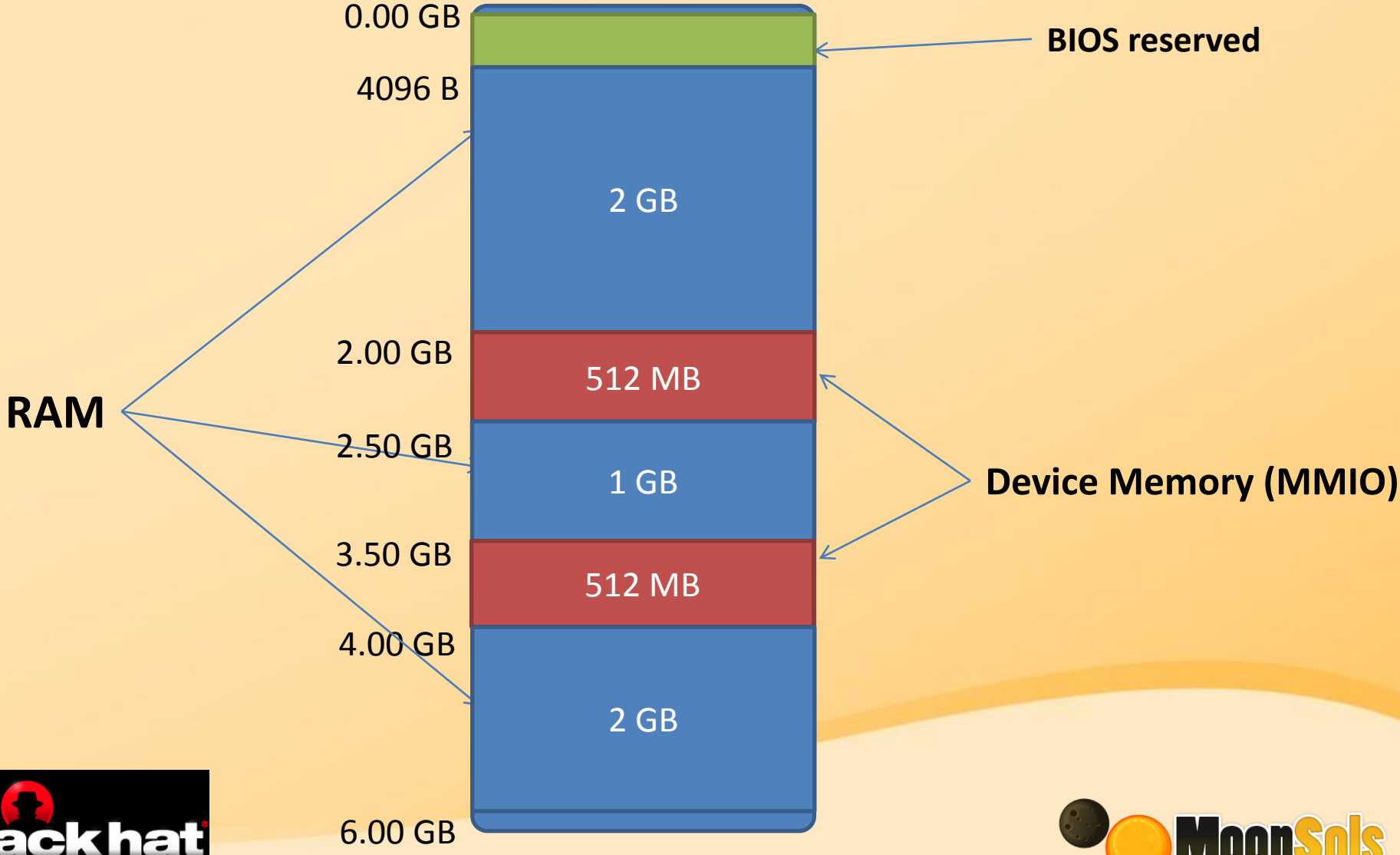
Main

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

What / How ?



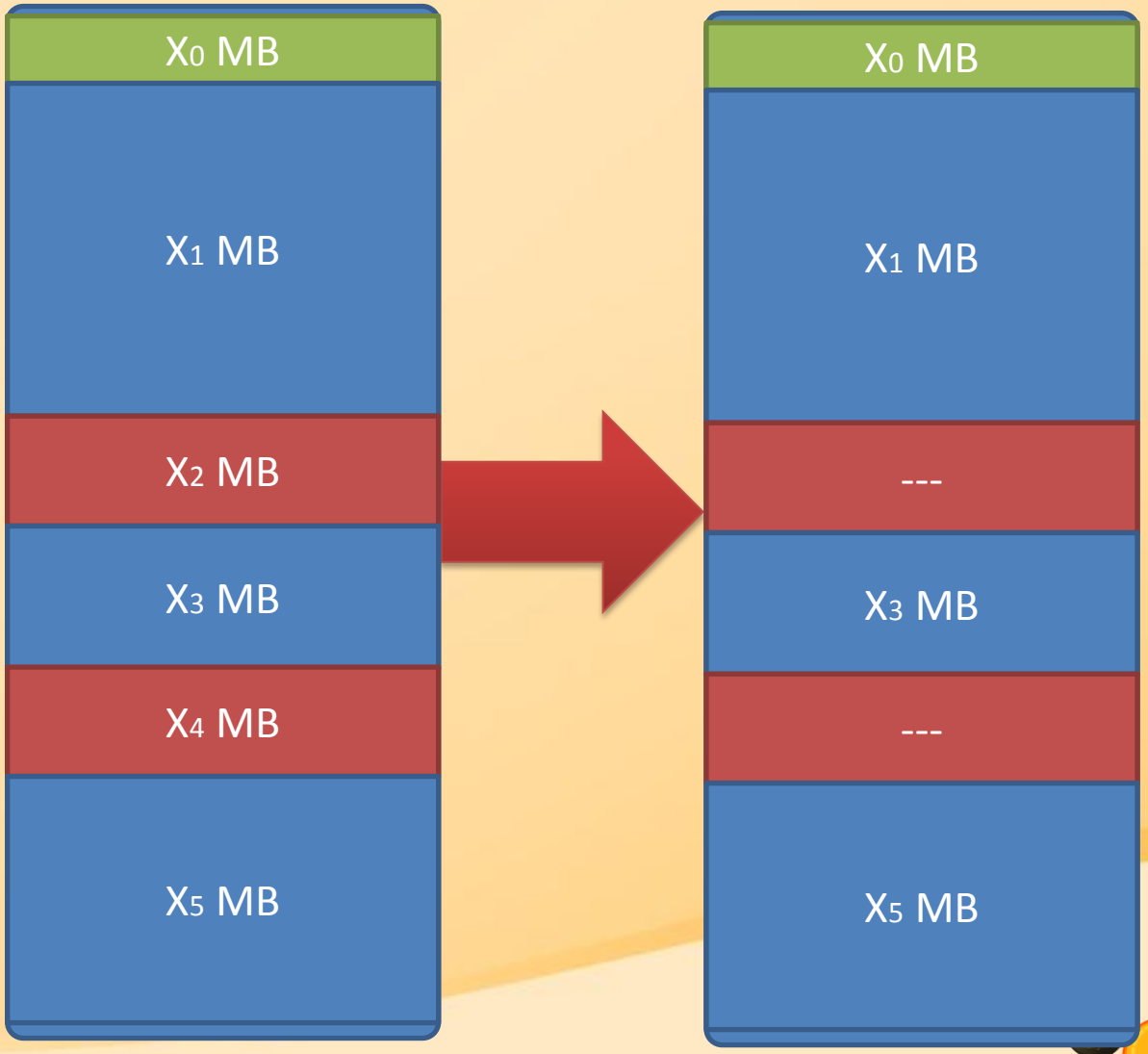
Physical Memory Mapping



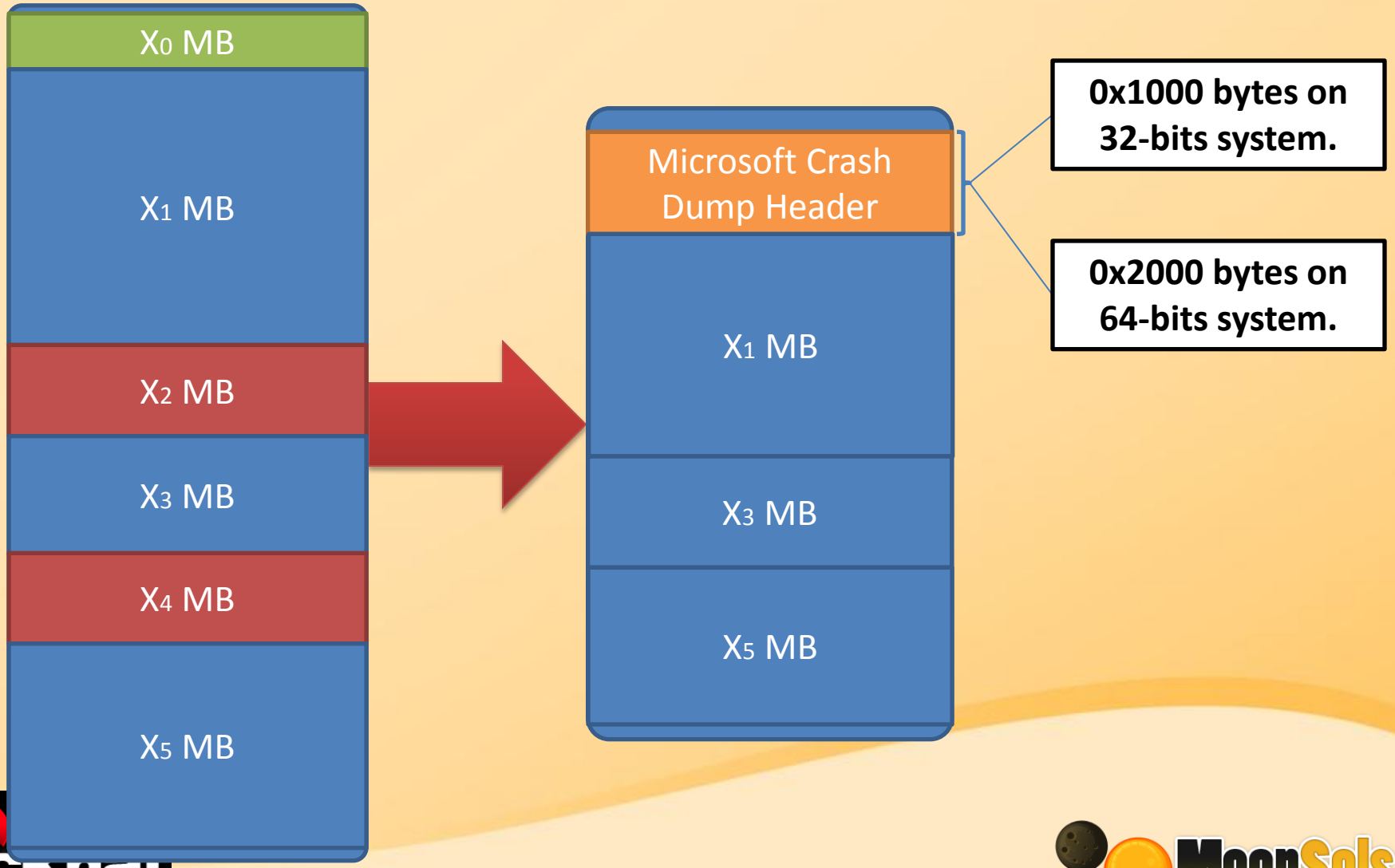
Physical Memory Mapping

- Blue Blocks are the physical memory
- These blocks are copied into the
  - Microsoft hibernation file
    - 4GB limitation
  - Microsoft crash dump file
    - 2GB limitation

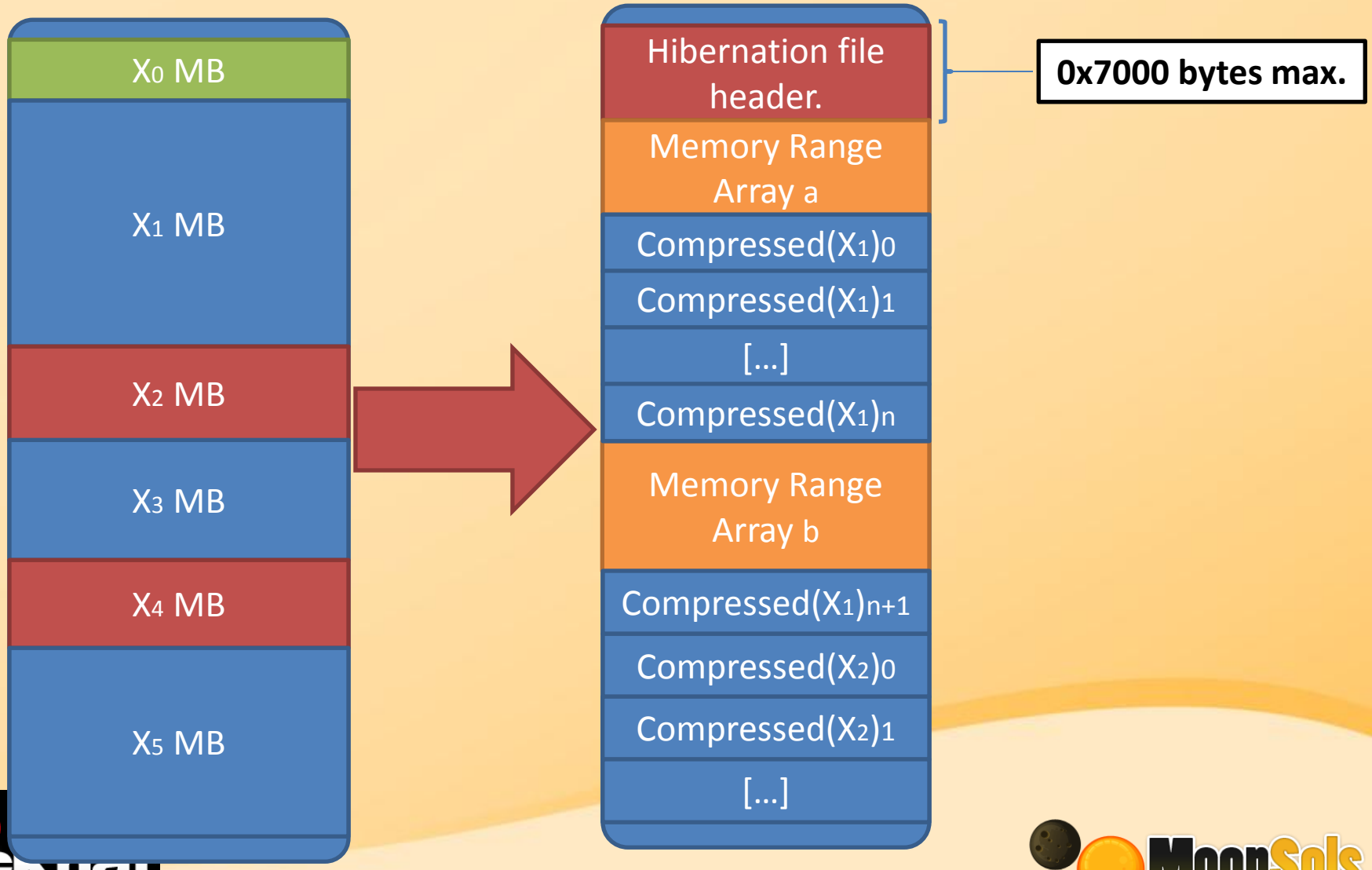
Raw Memory Dump



Microsoft Full Crash Dump



Microsoft hibernation file



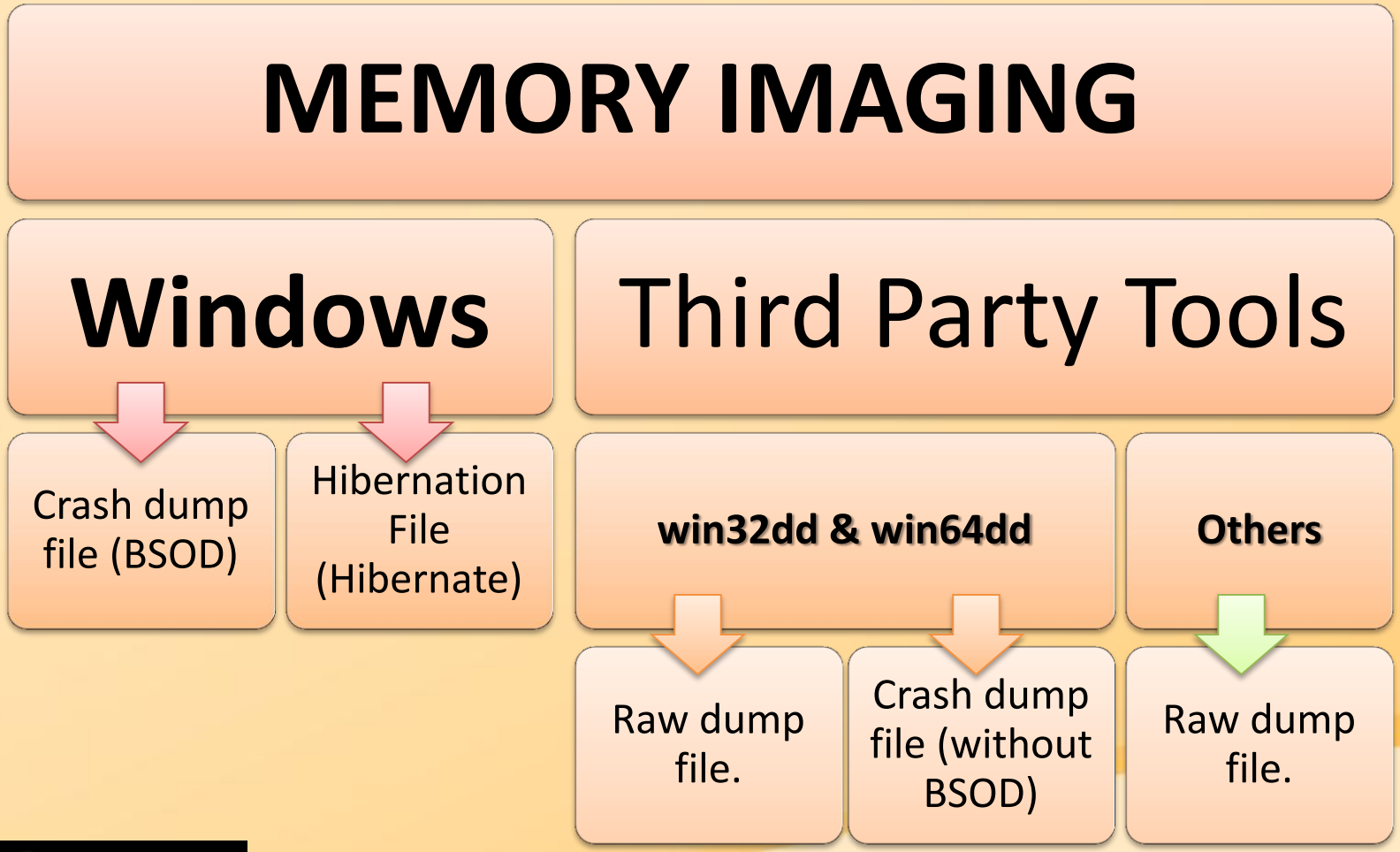
Outline

- **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



Agenda

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

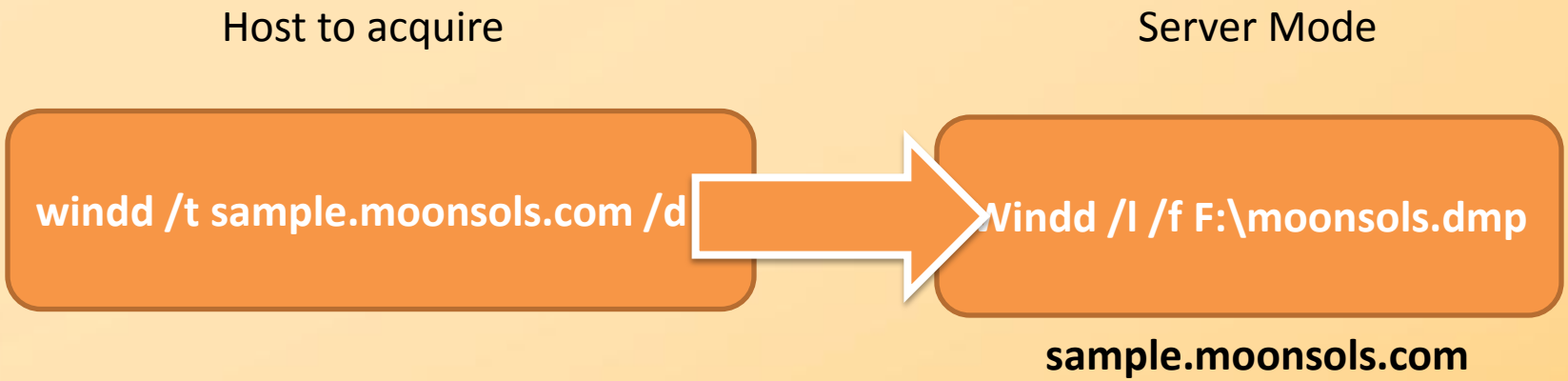
Win32dd & Win64dd

- 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

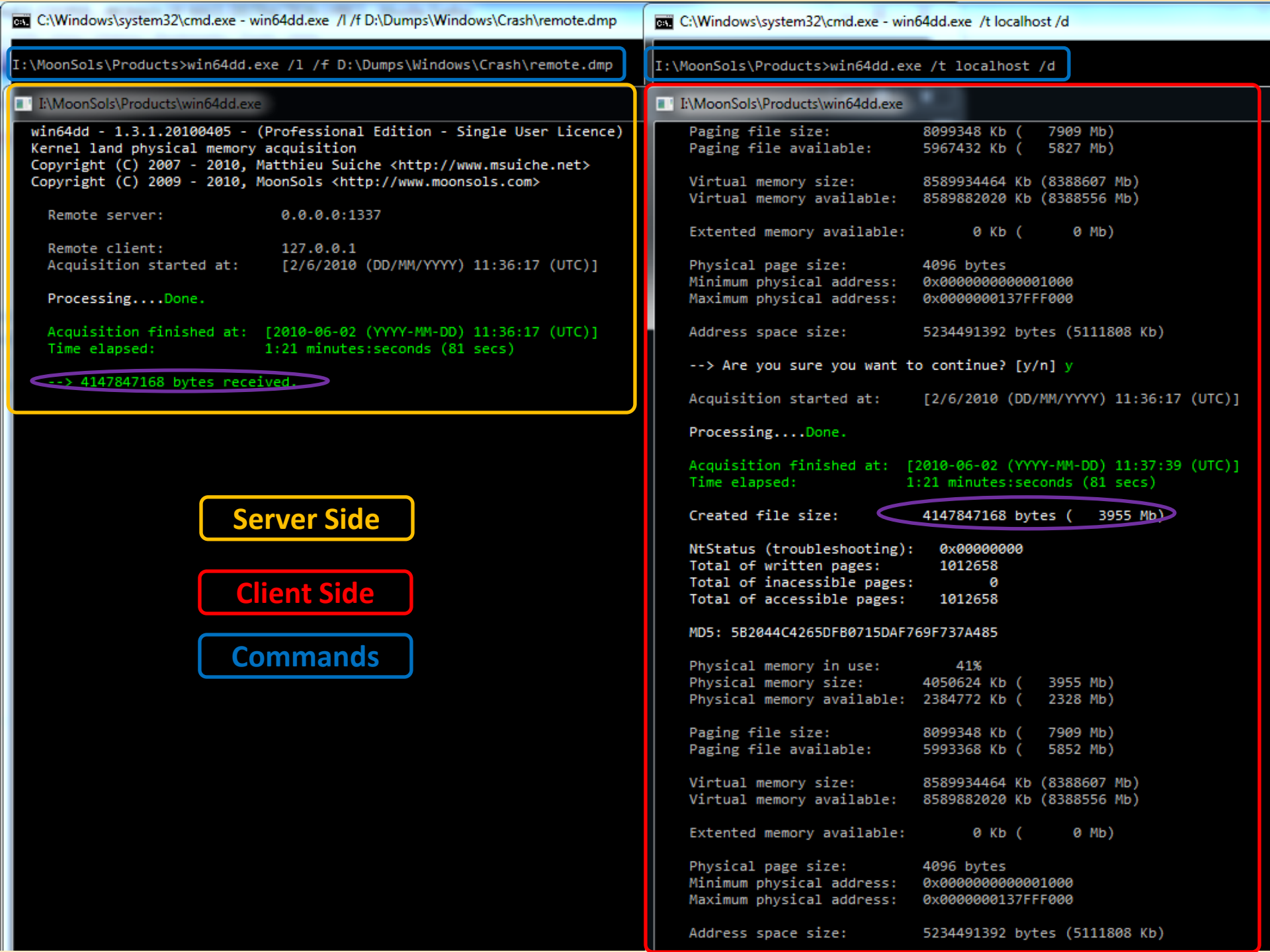
Win32dd & Win64dd

- 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 REQUIERED
  - Unlike Sysinternal's livekd.

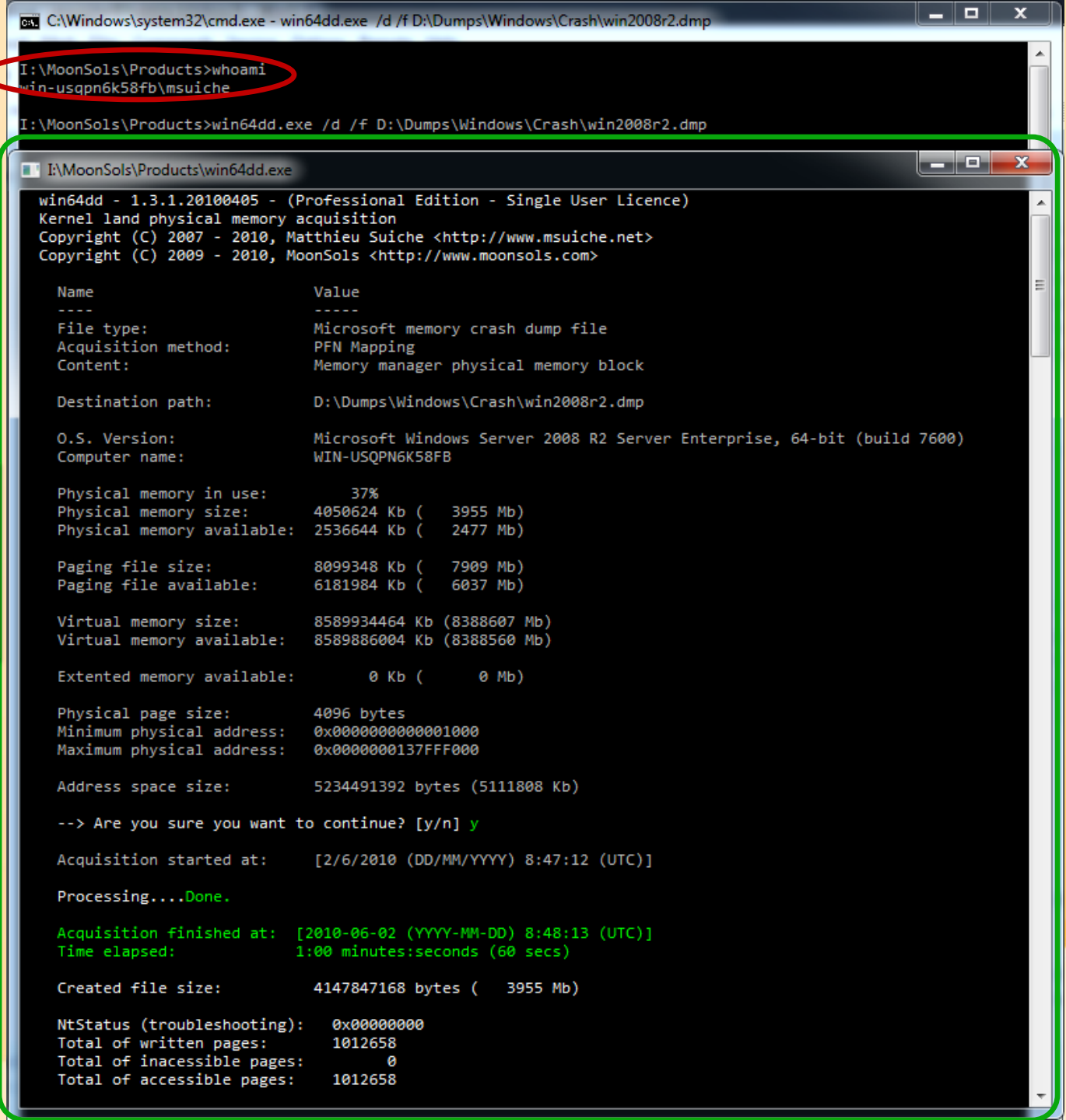
Server Mode



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.
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)
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) 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 inacessible 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)
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)
Server Side
Client Side
Commands

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



Agenda

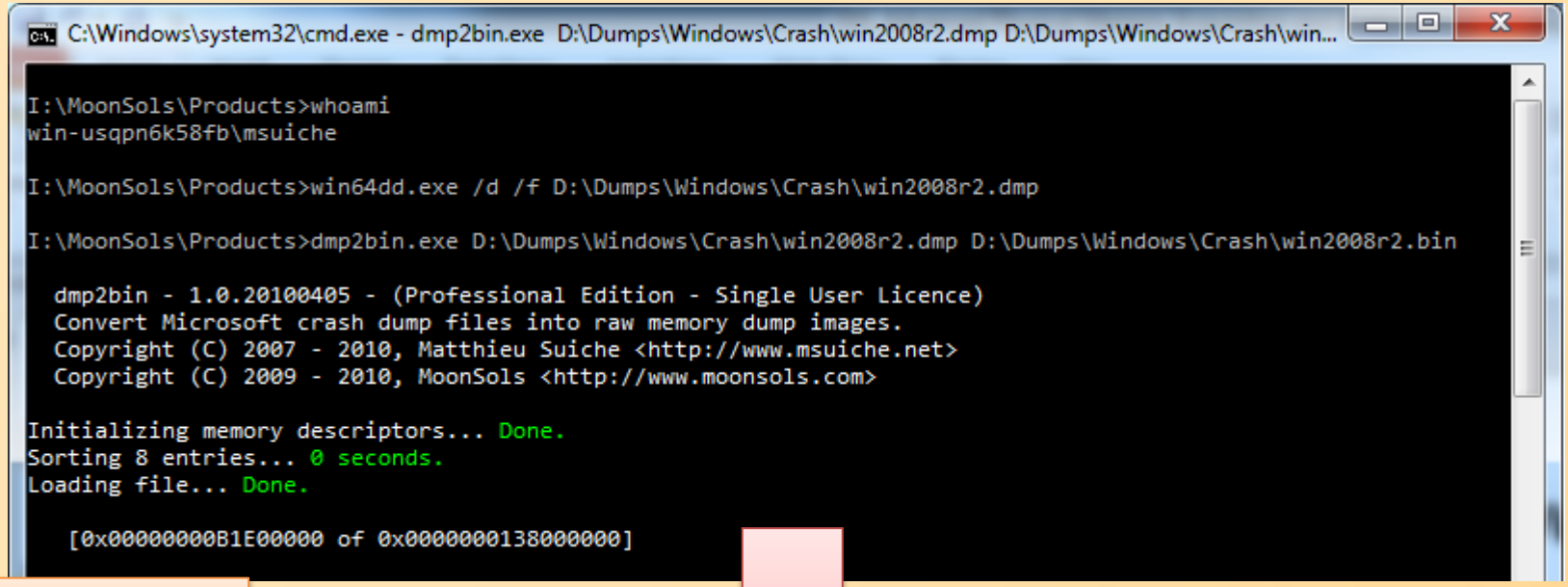
- **MoonSols Windows Memory Toolkit**
  - win32dd
  - win64dd
  - **dmp2bin**
  - bin2dmp
  - hibr2dmp
  - hibr2bin

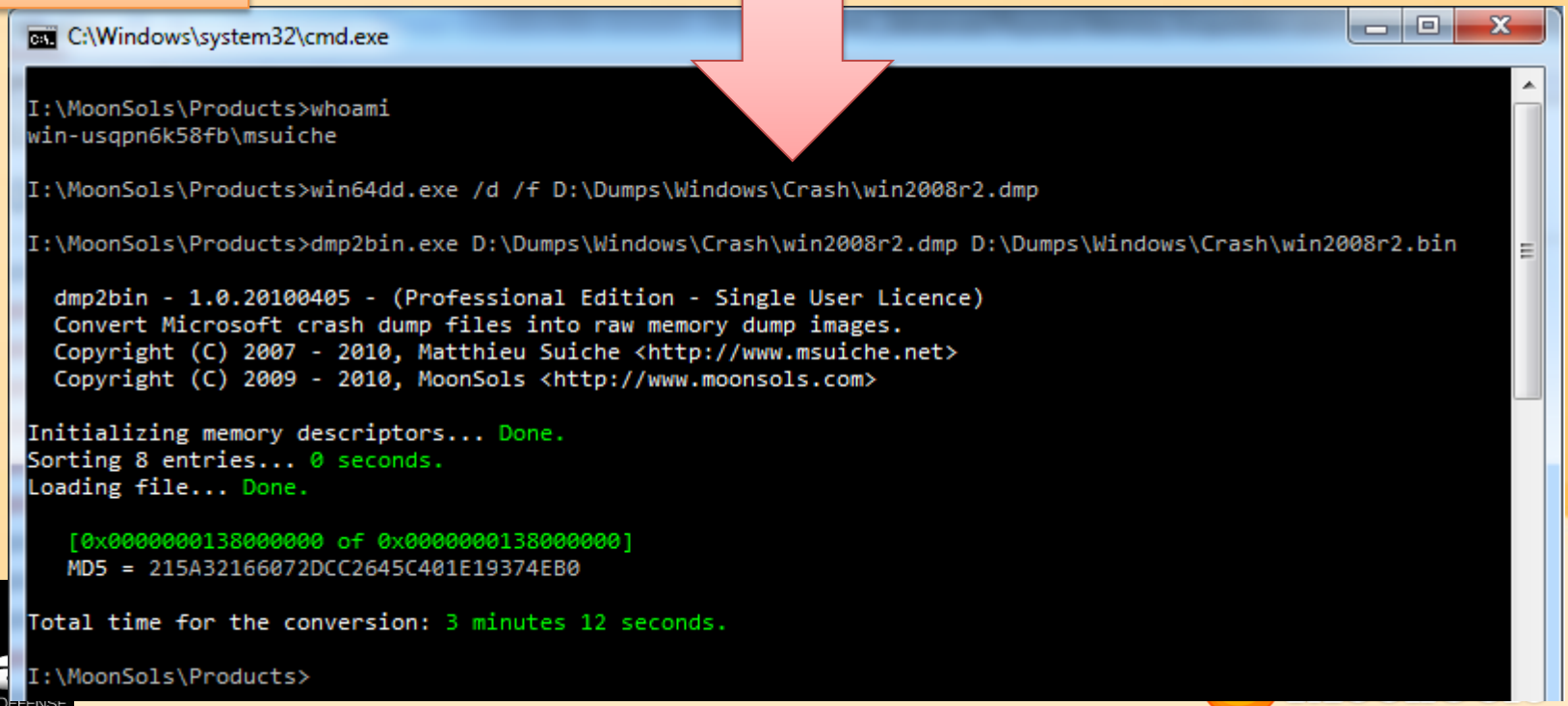
dmp2bin

- **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.

- MD5 hash





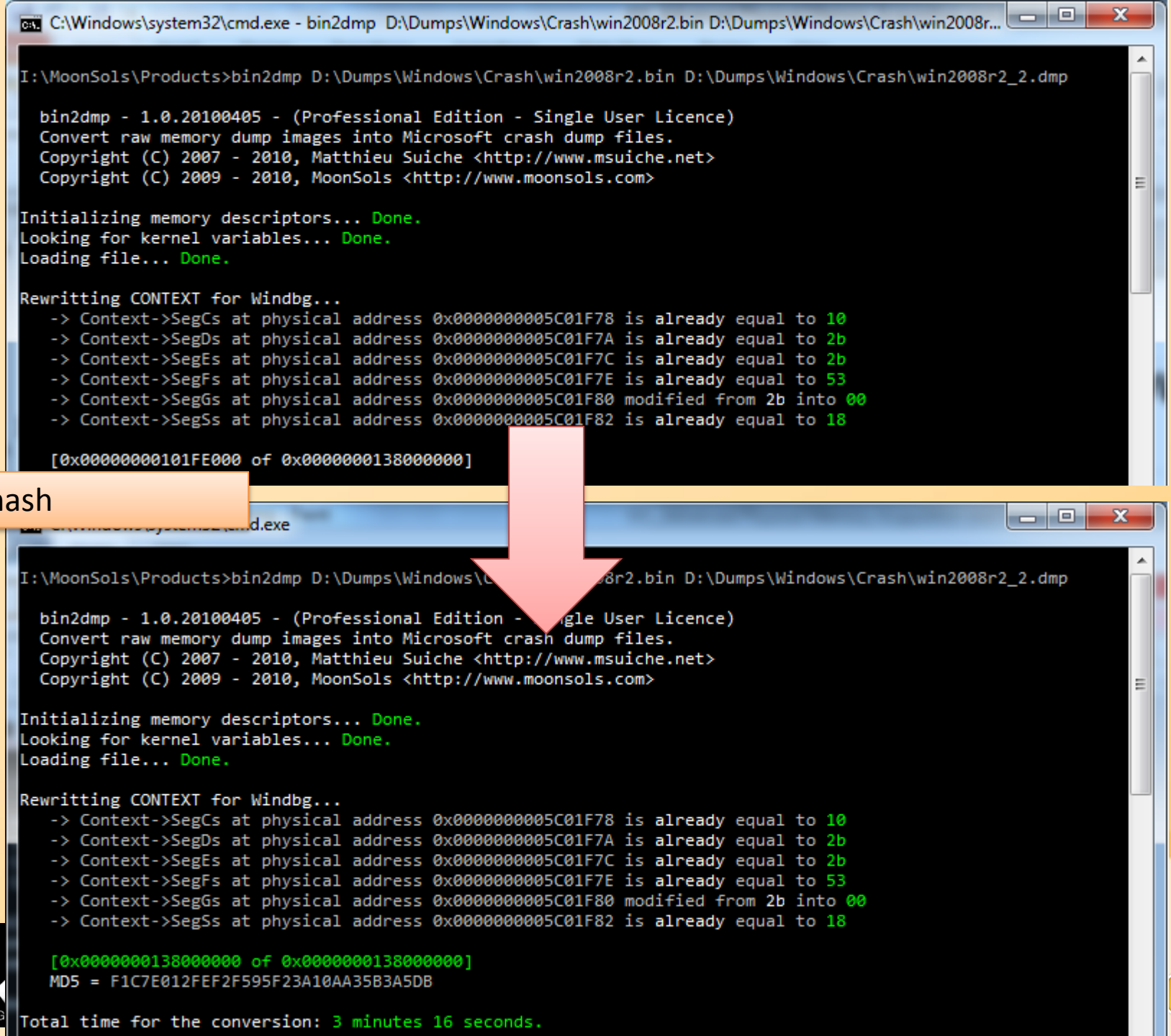
Agenda

- **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\win2008r...
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.
Rewritting 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 0x0000000138000000]
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.
Rewritting 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
[0x0000000138000000 of 0x0000000138000000]
MD5 = F1C7E012FEF2F595F23A10AA35B3A5DB
Total time for the conversion: 3 minutes 16 seconds.

- MD5 hash

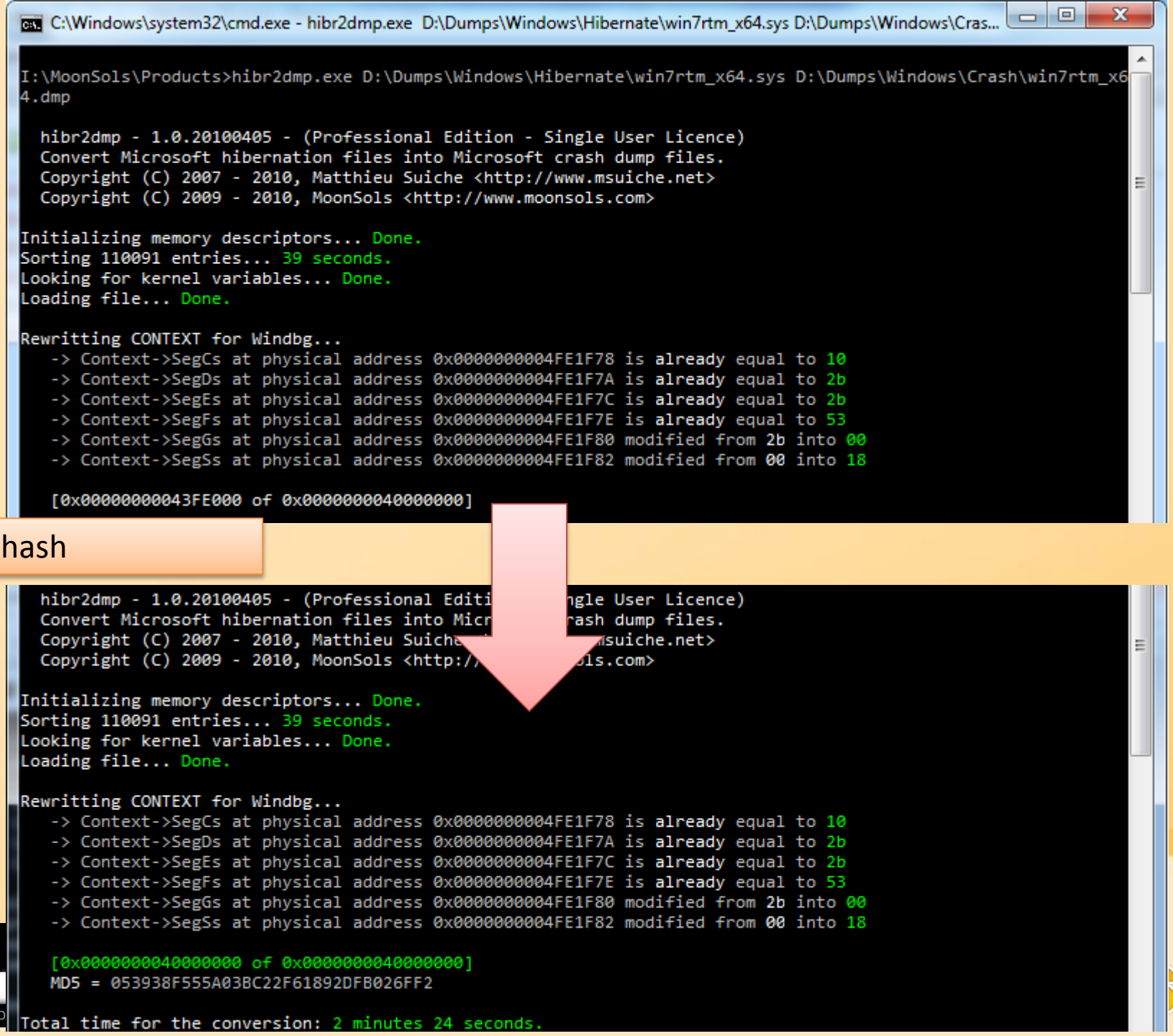
Agenda

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

bin2dmp

- **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\Hibernate\win7rtm_x64.sys D:\Dumps\Windows\Cras...
I:\MoonSols\Products>hibr2dmp.exe D:\Dumps\Windows\Hibernate\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.
Rewritting CONTEXT for Windbg...
-> Context->SegCs at physical address 0x000000004FE1F78 is already equal to 10
-> Context->SegDs at physical address 0x000000004FE1F7A is already equal to 2b
-> Context->SegEs at physical address 0x000000004FE1F7C is already equal to 2b
-> Context->SegFs at physical address 0x000000004FE1F7E is already equal to 53
-> Context->SegGs at physical address 0x000000004FE1F80 modified from 2b into 00
-> Context->SegSs at physical address 0x000000004FE1F82 modified from 00 into 18
[0x00000000043FE000 of 0x0000000040000000]
hibr2dmp - 1.0.20100405 - (Professional Editi ngle User Licence)
Convert Microsoft hibernation files into Micr rash dump files.
Copyright (C) 2007 - 2010, Matthieu Suiche msuiche.net>
Copyright (C) 2009 - 2010, MoonSols <http:// ls.com>
Initializing memory descriptors... Done.
Sorting 110091 entries... 39 seconds.
Looking for kernel variables... Done.
Loading file... Done.
Rewritting CONTEXT for Windbg...
-> Context->SegCs at physical address 0x000000004FE1F78 is already equal to 10
-> Context->SegDs at physical address 0x000000004FE1F7A is already equal to 2b
-> Context->SegEs at physical address 0x000000004FE1F7C is already equal to 2b
-> Context->SegFs at physical address 0x000000004FE1F7E is already equal to 53
-> Context->SegGs at physical address 0x000000004FE1F80 modified from 2b into 00
-> Context->SegSs at physical address 0x000000004FE1F82 modified from 00 into 18
[0x0000000040000000 of 0x0000000040000000]
MD5 = 053938F555A03BC22F61892DFB026FF2
Total time for the conversion: 2 minutes 24 seconds.

- MD5 hash

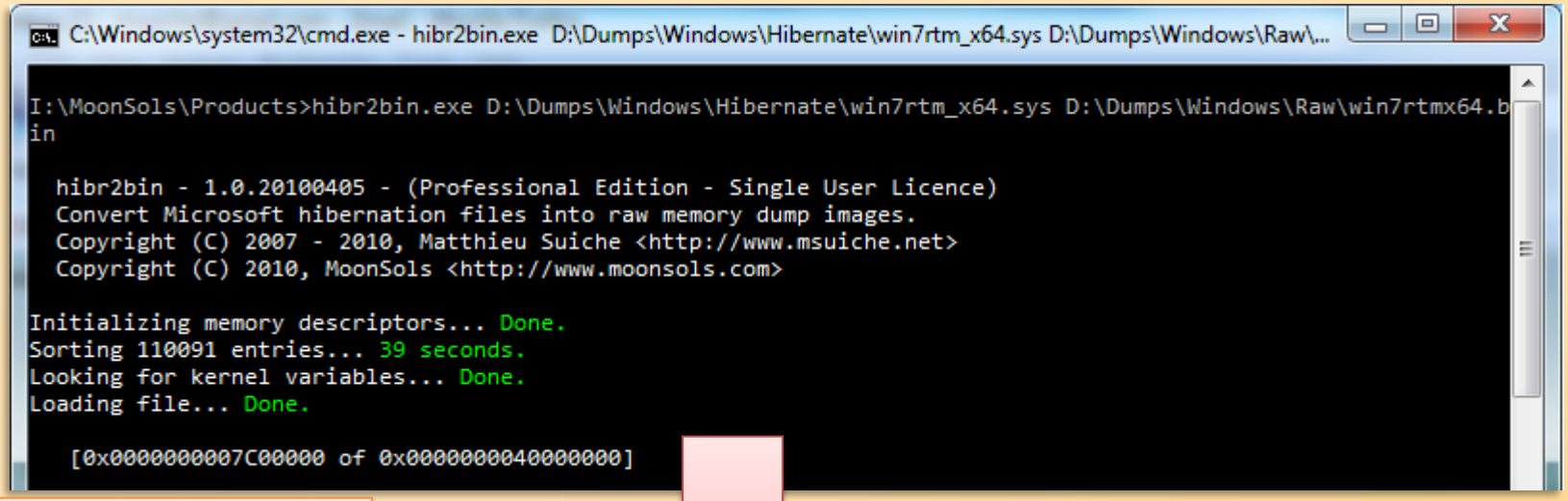
Agenda

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

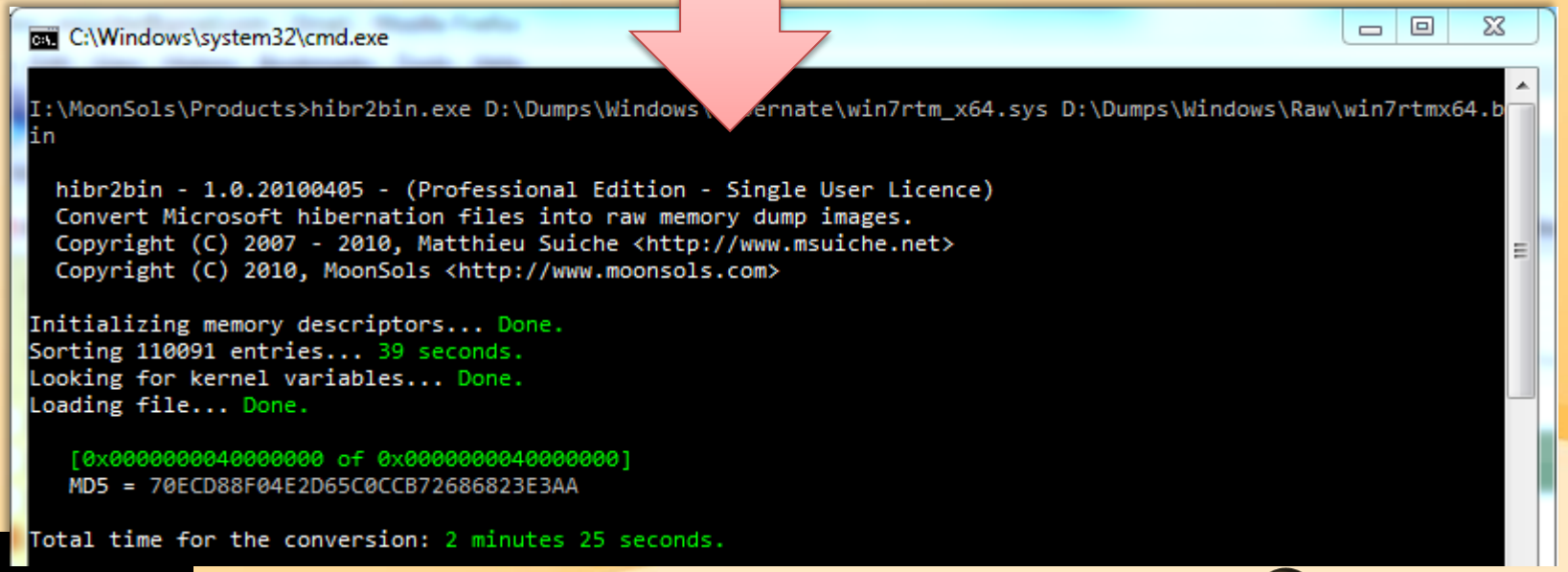
bin2dmp

- **hibr2bin** <input> <output>
  - Convert a Microsoft hibernation file into a linear meomry 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)*



- MD5 hash

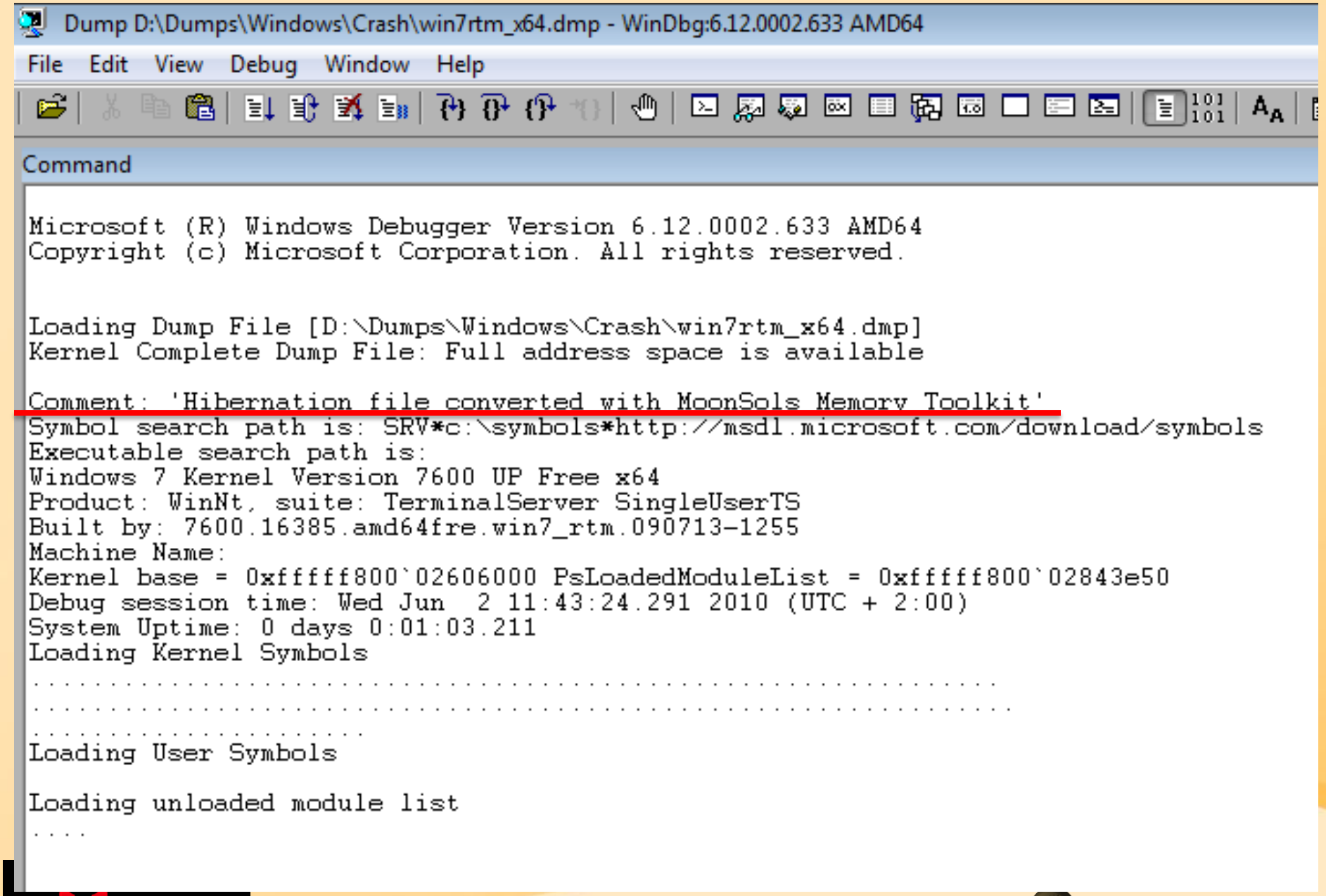


Microsoft Windows Debugger

- 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].



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
- See you at

  http://moonsols.com/component/jdownloads/view.download/3/2

Future

- Virtualization !

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

QUESTIONS ?