What is the most challenging area of Windows forensics now that Win7 and Sever 2008 (R2) are out?

Matthieu Suiche
Founder, MoonSols SARL

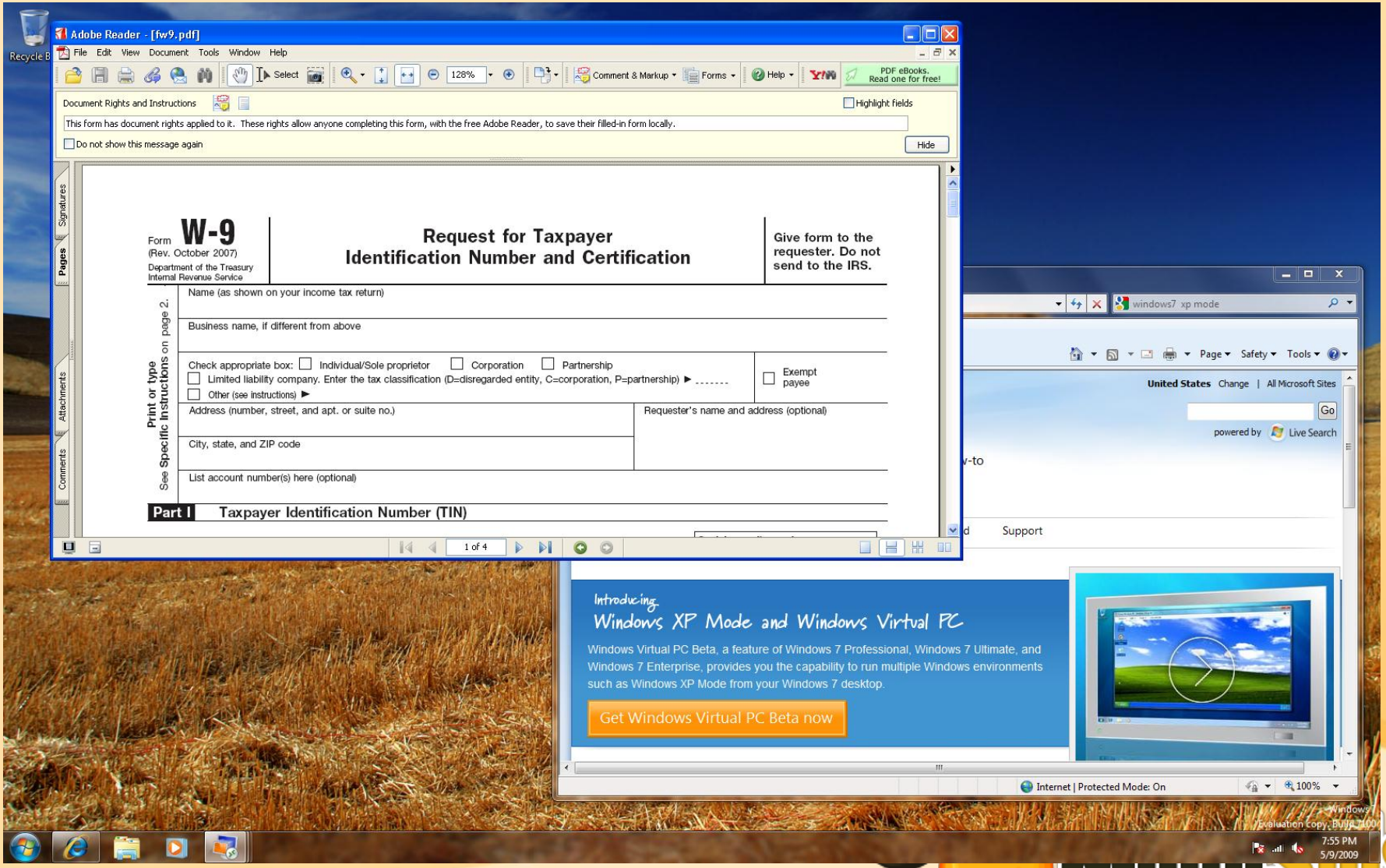
Who Am I ?

- Founder of MoonSols SARL, based in France
  - Services, Products, (Private) **Trainings**, Kernel code consulting
- 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
- BlackHat, PacSec, CanSecWest etc. speakers.

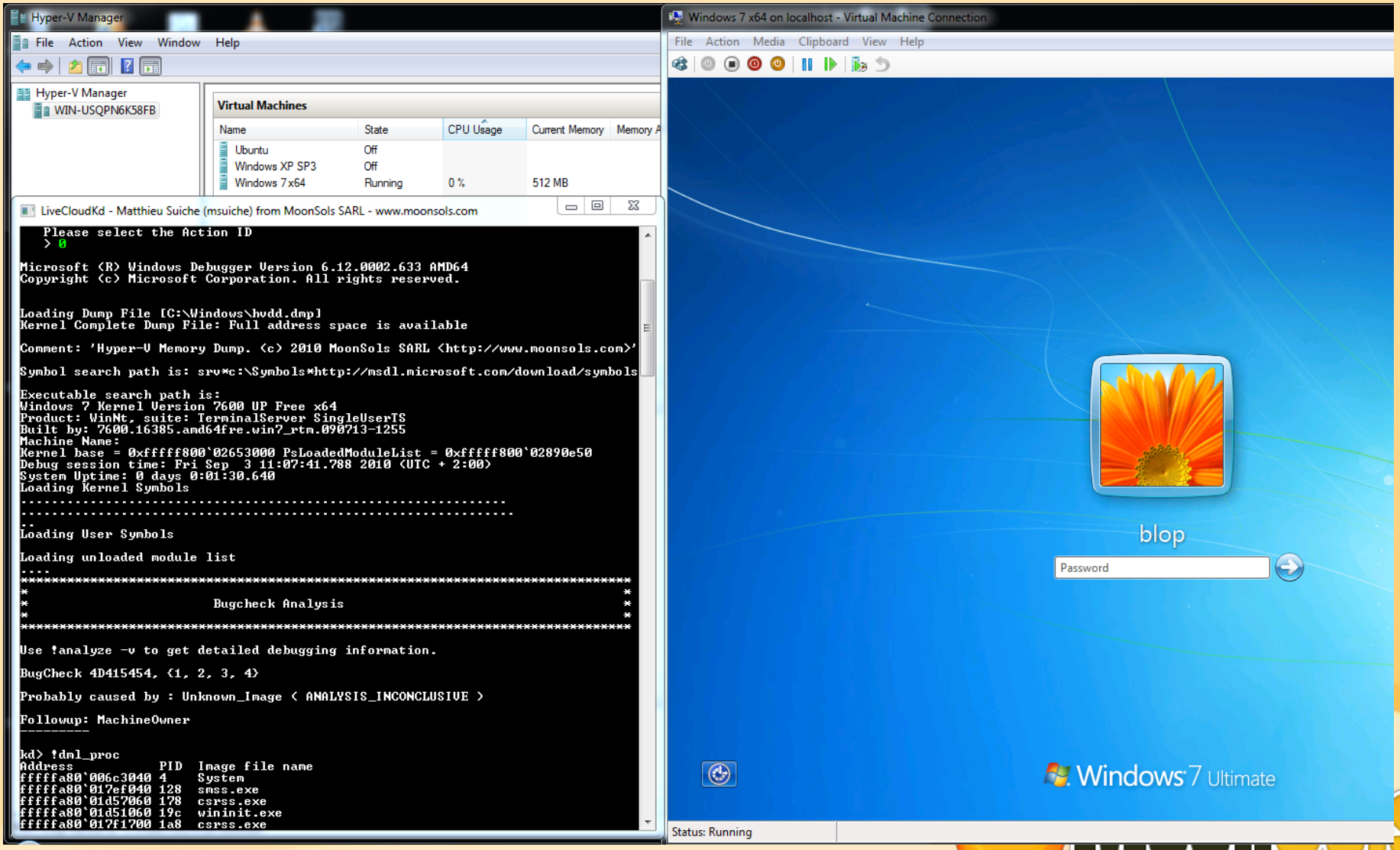
Virtualization

- Windows 7
  - XP Mode
- Windows Server 2008 and Server 2008 R2
  - Hyper-V 1 and Hyper-V 2

XP Mode


Adobe Reader - [fw9.pdf]
File Edit View Document Tools Window Help
Document Rights and Instructions
This form has document rights applied to it. These rights allow anyone completing this form, with the free Adobe Reader, to save their filled-in form locally.
Do not show this message again
Hide
Form W-9 (Rev. October 2007)
Department of the Treasury Internal Revenue Service
Request for Taxpayer Identification Number and Certification
Give form to the requester. Do not send to the IRS.
Name (as shown on your income tax return)
Business name, if different from above
Check appropriate box: Individual/Sole proprietor Corporation Partnership
Limited liability company. Enter the tax classification (D=disregarded entity, C=corporation, P=partnership)
Other (see instructions)
Exempt payee
Address (number, street, and apt. or suite no.)
Requester's name and address (optional)
City, state, and ZIP code
List account number(s) here (optional)
Part I Taxpayer Identification Number (TIN)
Print or type See Specific Instructions on page 2.
Introducing Windows XP Mode and Windows Virtual PC
Windows Virtual PC Beta, a feature of Windows 7 Professional, Windows 7 Ultimate, and Windows 7 Enterprise, provides you the capability to run multiple Windows environments such as Windows XP Mode from your Windows 7 desktop.
Get Windows Virtual PC Beta now
Internet | Protected Mode: On
7:55 PM
5/9/2009

Hyper-V


Hyper-V Manager
File Action View Window Help
Hyper-V Manager
WIN-USQPN6K58FB
Virtual Machines
Name State CPU Usage Current Memory Memory A
Ubuntu Off
Windows XP SP3 Off
Windows 7 x64 Running 0 % 512 MB
LiveCloudKd - Matthieu Suiche (msuiche) from MoonSols SARL - www.moonsols.com
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 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`02653000 PsLoadedModuleList = 0xfffff800`02890e50
Debug session time: Fri Sep 3 11:07:41.788 2010 (UTC + 2:00)
System Uptime: 0 days 0:01:30.640
Loading Kernel Symbols
Loading User Symbols
Loading unloaded module list
Bugcheck Analysis
Use !analyze -v to get detailed debugging information.
BugCheck 4D415454, {1, 2, 3, 4}
Probably caused by : Unknown_Image (ANALYSIS_INCONCLUSIVE)
Followup: MachineOwner
kd> !dml_proc
Address PID Image file name
fffffa80`006c3040 4 System
fffffa80`017ef040 128 smss.exe
fffffa80`01d57060 178 csrss.exe
fffffa80`01d51060 19c wininit.exe
fffffa80`017f1700 1a8 csrss.exe
Windows 7 x64 on localhost - Virtual Machine Connection
File Action Media Clipboard View Help
blop
Password
Windows 7 Ultimate
Status: Running

LiveClouKd

- 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.

Contact

See you on http://www.moonsols.com

msuiche@moonsols.com

Twitter:

@MoonSols

@msuiche