

Virtual Forensics 2.0

Investigating virtual environments

Christiaan Beek



There is
no substitute
for experience

Agenda

- Who am I?
- Traditional vs Virtual
- Challenges
- Citrix & Vmware
- Windows 7
- Summary



There is
no substitute
for experience





There is
no substitute
for experience

largo

waldorf

Parameter	Value	MOD	Dir	Wr
F1 Cutoff	184			None

Oscillators

Mixer

Filters

1 Octave

Shape: All Waves

+00 Bend Range +1000 Keytrack

FM Dec2

Wave LFO1

Semitone

Detune

Sub Oscillator

Balance

F1 F2 Balance

Oct 1 Level

1

Drive Type: Hard

Filter Type: LFO LP

Drive

Resonance

Routing

Parallel Serial

Cutoff

Keytr: +1000

Env Amount

Env Velocity

Mod

Level

Volume Velocity

2 Octave

Shape: All Waves

+00 Bend Range +1000 Keytrack

FM Dec3

Wave LFO2

Semitone

Detune

Sub Oscillator

Balance

F1 F2 Balance

Oct 2 Level

Ring Mod

2

Drive

Resonance

Routing

Parallel Serial

Cutoff

Keytr: +1000

Env Amount

Env Velocity

Mod

Level

3 Octave Sync

Shape: Pulse

+00 Bend Range +1000 Keytrack

FM off

Wave LFO1

Semitone

Detune

Sub Oscillator

Source: LFO2

Occ Pitch Mod

Balance

F1 F2 Balance

Oct 3 Level

Noise Level

Colour

2

Drive

Resonance

Routing

Parallel Serial

Cutoff

Keytr: +1000

Env Amount

Env Velocity

Mod

Level

- LFOs
- Envelopes
- Matrix
- Arpeggiator
- Effects
- Global

1 014

Shape: Triangle

Delay

Keytr: +0000

2 044

Shape: Saw

Delay

Keytr: +0000

3 12 Bars

Shape: Step

Delay

Keytr: +0000

Gate

Unison

Reverb

Delay

Level







There is
no substitute
for experience

This session is NOT:

- A negative talk about virtualization
- Sponsored by any of the vendors of VM products
- About using VM as a forensic research platform



There is
no substitute
for experience

Ok ?



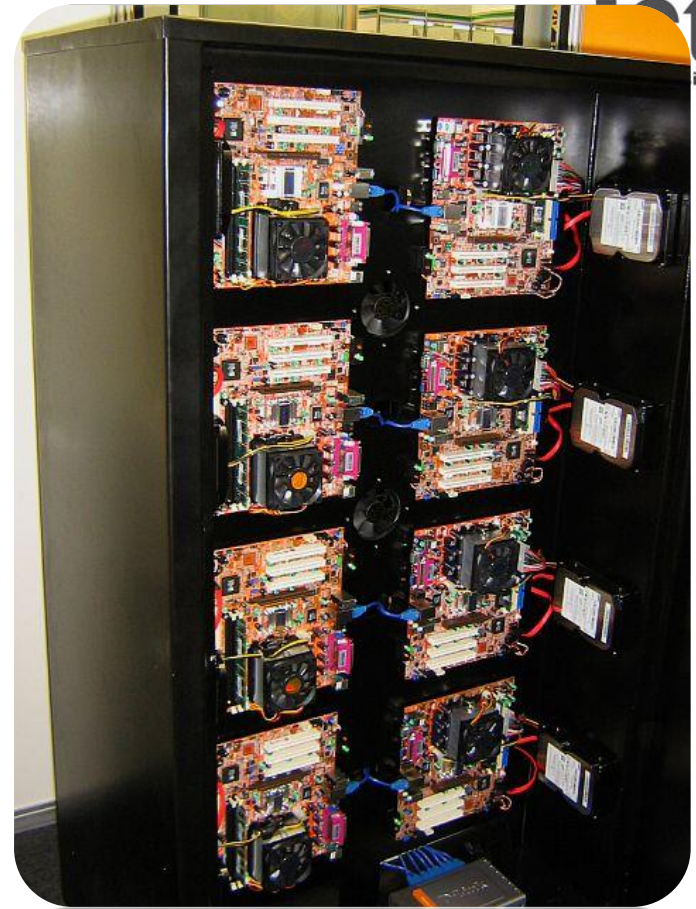
There is
no substitute
for experience

Traditional vs:



There is
no substitute
for experience

Virtual:



There is
no substitute
for experience

Challenges:

- What to expect?
- What tools to use?
- Where is the data?
- Who owns the data?
- Which Forensic techniques to use?
- How to acquire data from a Cloud?
- Jurisdiction?



There is
no substitute
for experience

What must be acquired?



There is
no substitute
for experience

Moooh, where is my data?



There is
no substitute
for experience

Statement MS Azure:



'We have four datacenters in the US, two in Europe and two in Asia. Even though you choose to store your data in Europe instead of Worldwide, your data will be stored at least three times. Two times on your main location and one time at a secondary data center'



There is
no substitute
for experience

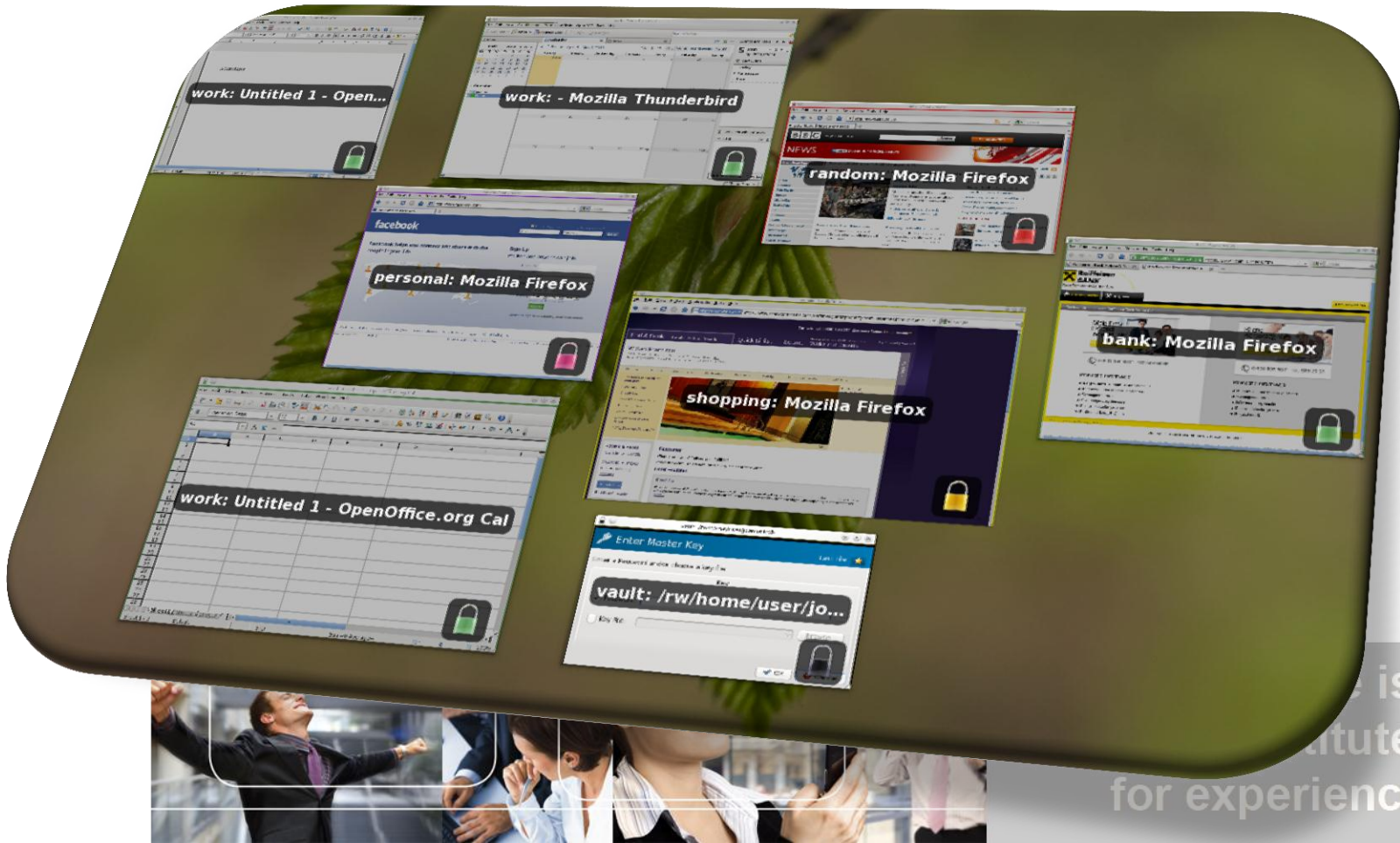
Where is my evidence?



There is
no substitute
for experience

Disposable VM's Qubes OS

- Joanna Rutkowska
- E.g. opening a P(enetration)DF file



Portable VM's

- Mojopac
- Portable Virtualbox
- Qemu
- Mokafive



There is
no substitute
for experience

Jurisdiction

A pedophile is using cloud resources to facilitate his crimes.

The data is located over several jurisdictional precincts

Do you know your limits?



There is
no substitute
for experience

We need to:

- *Understand the technology*
- *Understand implementations of the products*
- *Which files are interesting for research*
- *Understand which tools to use*
- *How tools are acting in Virtual Environments*
- *Develop an approach*



There is
no substitute
for experience

Decision vs Impact:



There is
no substitute
for experience

Next:

- *Citrix*
- *VMware*
- *Windows 7*



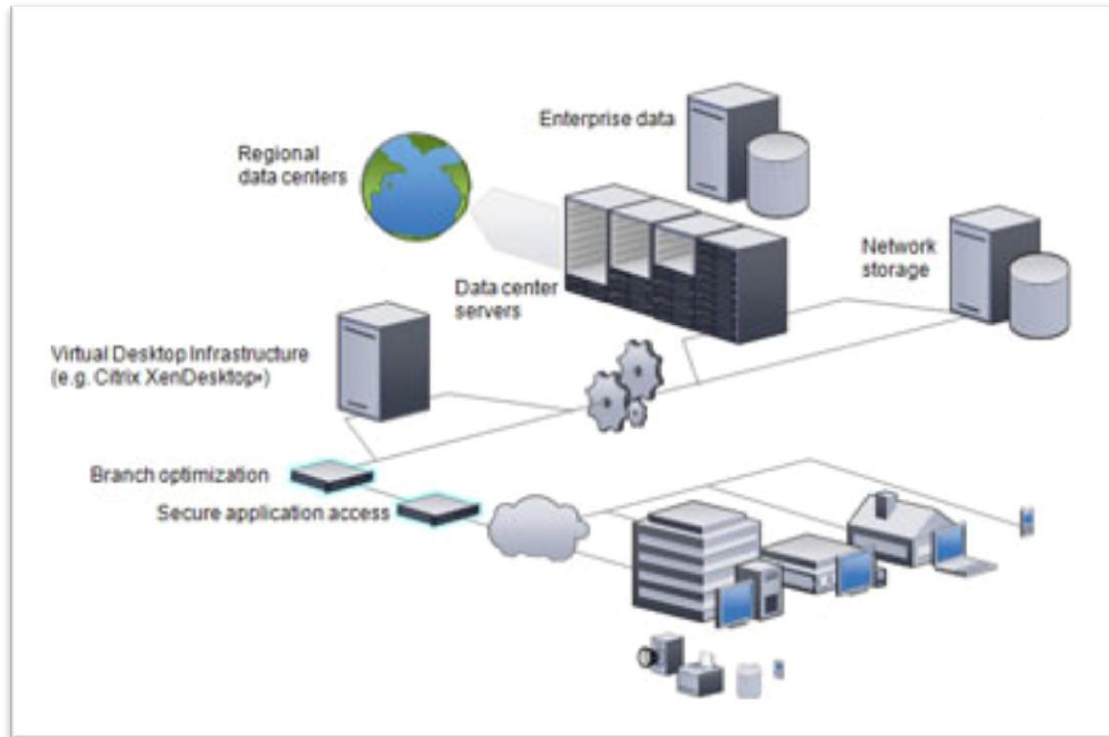
Which files are interesting for research



There is
no substitute
for experience

Citrix:

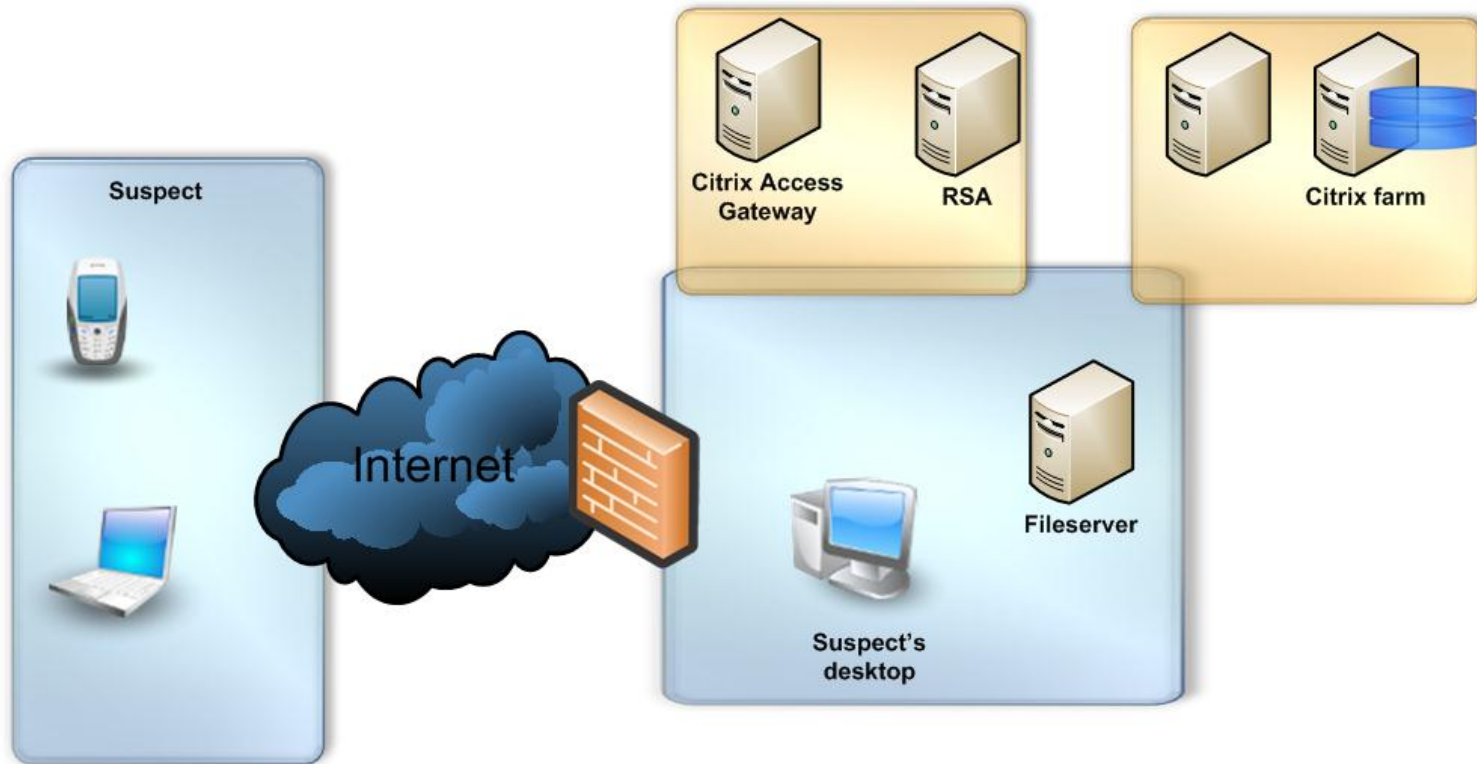
- Many ways to implement/use:



There is
no substitute
for experience

Citrix:

- scenario:



There is
no substitute
for experience

Citrix:

- Last logon logfile
%appdata%\icaclient (or citrix\icaclient)
- Configuration log (default not enabled)
- User profile (NTUser.dat;registry;temp files)
- Citrix Access Gateway logs
- Radius logs



There is
no substitute
for experience

Citrix tools:

- To retrieve data: normal tools like FTK-imager, Encase.
- Volatile data extraction:

VIX tools



There is
no substitute
for experience

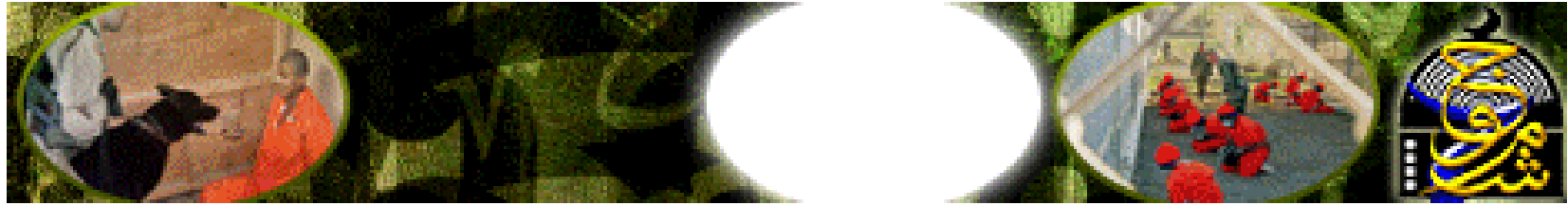
VMware:

- VMWare workstation & ESX server are popular
- Static or live need different tools and approach
- Many used as testing platform
- Suspect deletes VM after activity or return to previous Snapshot



There is
no substitute
for experience

Example IRL



-   **Sticky: Are you my brother ... watched by the intelligence services!?! (12)**
Soldiers of God 08-21-2009
-   **Sticky: exclusive jihadist forums: Several explanations on how stealth video online**
Baghi guidance 09-16-2009

-   **Modern methods of hiding during the use of the Internet**
irhabi_001 5 days ago
-   **With Alnorcon choose the appropriate protection, with direct links**
reem 2 weeks ago
-   **Program Kalik - Portable - Run non-step**
Muhammad Idrees 6 days ago
-   **VMWare_Workstation the latest version (Lite) + with the latest version before Altolz only and exclusively terrorists**
Time Of Terror since one week

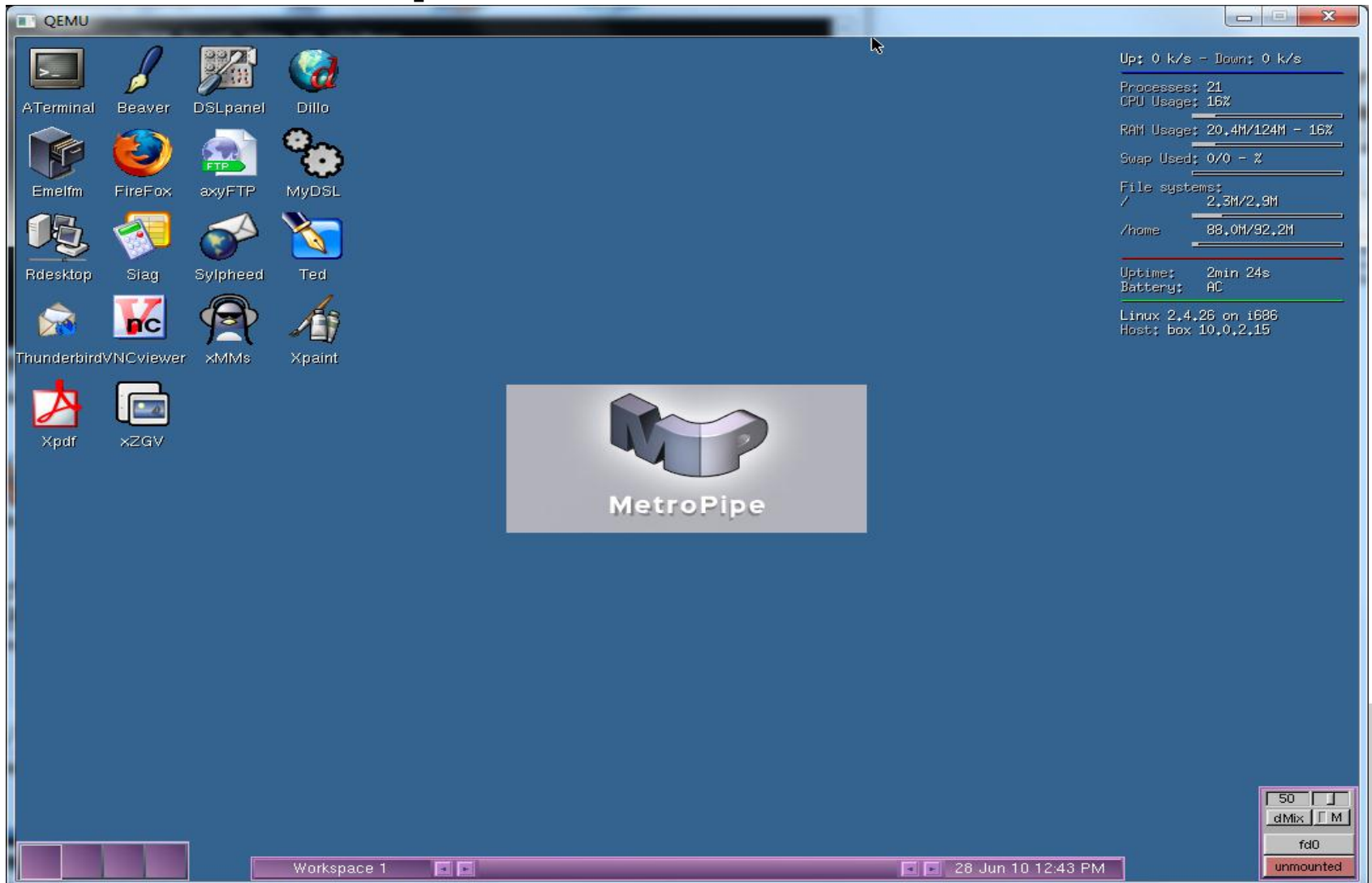


There is
no substitute
for experience

Example IRL



Portable virtual private machine



Vmware files of interest:

File Extention	Description
vmx	<i>Primary virtual machine configuration file</i>
vmsd	<i>Snapshot Descriptor file</i>
vmtm	<i>Configuration file for the teaming features containing teaming data</i>
vmxf	<i>If a VM is removed from a team this config file remains</i>
vmdk	<i>The disk descriptor file, it contains the disk layout, structure, geometry and physical properties.</i>
log	<i>Vmware logfiles</i>
nvram	<i>Bios settings of the VM</i>
vswp	<i>Swap file</i>
vmss	<i>Suspend file. It stores the state of a suspended VM</i>
vmsn	<i>Snapshot files</i>
vmsd	<i>Snapshot Descriptor file</i>
vmem	<i>Virtual machines' paging file</i>



There is
no substitute
for experience

Vmware tools:

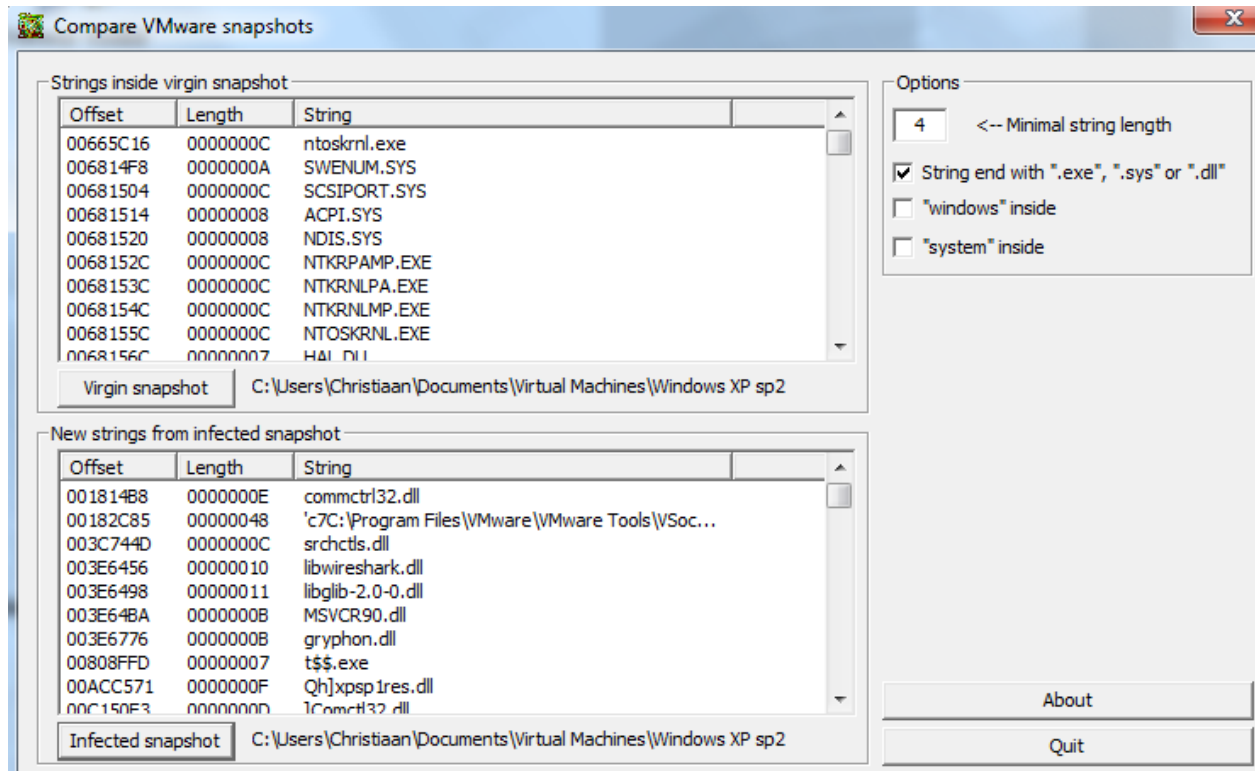
- FTK imager
- Liveview
- Encase
- MMLS & DD (getting partitions)
- Raw2vmdk
- Mount & Carve with Foremost or Photorec



There is
no substitute
for experience

Vmware tools:

- Compare Snapshots



Tool by Zairon



There is
no substitute
for experience

Vmware tools:

Analyzing Vmem with Memparser by Chris Betz

C:\Somedir>memparser EvilBert-Snapshot2.vmem

Process List:

<i>Proc#</i>	<i>PPID</i>	<i>PID</i>	<i>InProcList</i>	<i>Name:</i>	<i>Threads: 10</i>
<i>0</i>	<i>0</i>	<i>0</i>	<i>Yes</i>	<i>Idle</i>	
<i>1</i>	<i>5</i>	<i>8</i>	<i>Yes</i>	<i>System</i>	
<i>2</i>	<i>9</i>	<i>120</i>	<i>Yes</i>	<i>EvilBertNotepad.EXE</i>	
<i>3</i>	<i>110</i>	<i>134</i>	<i>Yes</i>	<i>CSRSS.EXE</i>	



There is
no substitute
for experience

Openvmfs drivers

```
#>java -jar fvmfs.jar /mnt/mnt/e1/vmfs_part_esx.dd info
```

```
VMFS label      = Datavault1  
VMFS creation date = Mon Jun 21 14:13:25 GMT-05:00 2010  
VMFS capacity   = 155.45 GB  
VMFS UUID      = 2b4ac011-3228e765-7bcd-00125436b14a  
VMFS block size = 1.00 MB  
VMFS version    = 3.33  
VMFS # of FD/PB/SB = 30720 / 61440 / 3968  
VMFS volume type =  
VMFS volume UUID = 2b4ac012-213736ba-3c5b-00125436b14a  
VMFS volume size = 155.45 GB  
VMFS volume ver  = 4
```

Example other option: **filecopy path size position**

Restoration of: vmdk, vmsn, metadata, or log files



There is
no substitute
for experience

Windows 7:

- Virtualization technique included:
- *VHD*
- *XP mode*
- *Virtual PC*



Windows 7™

Windows 7™



There is
no substitute
for experience

Windows 7:

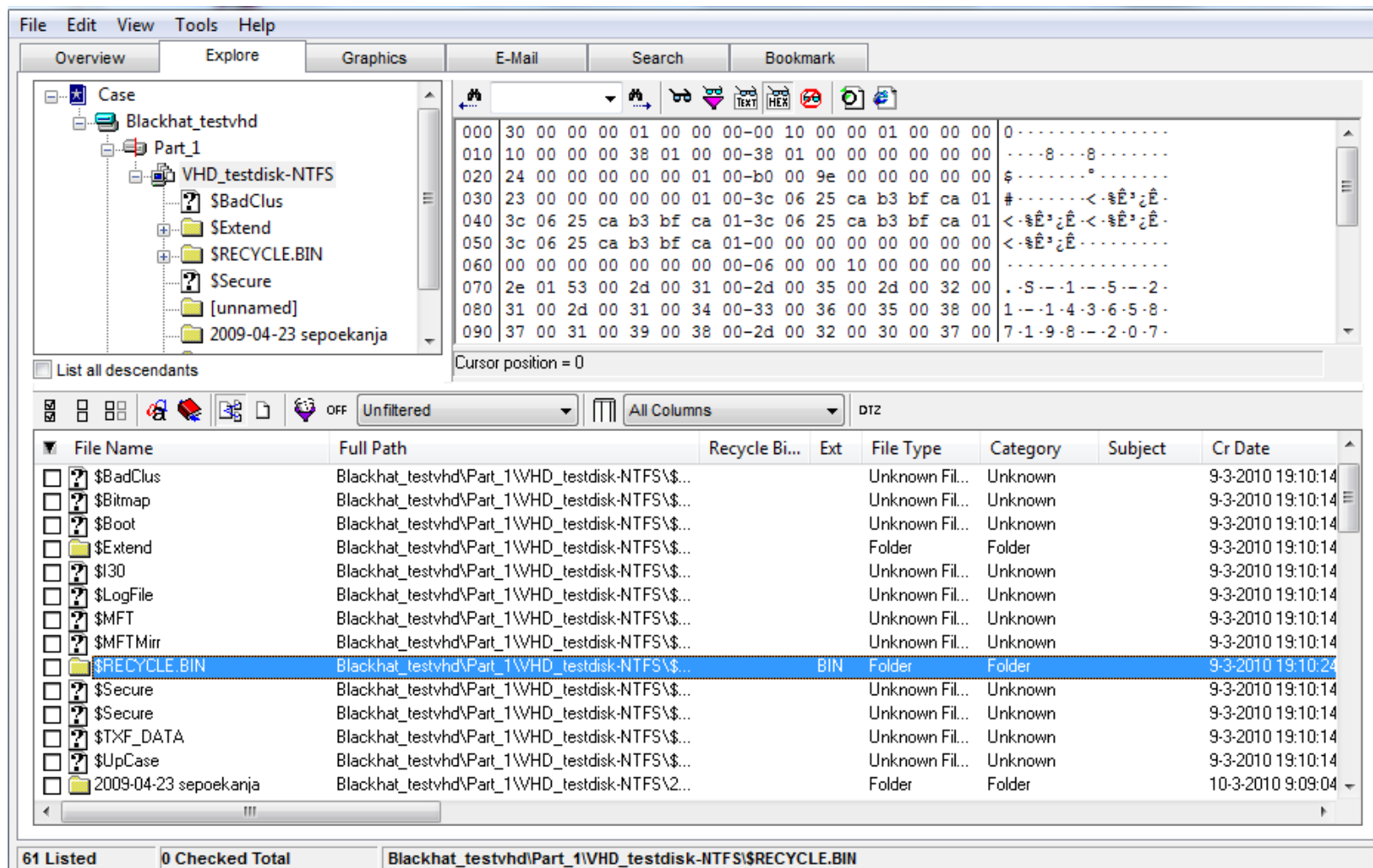
- VHD mount (read-only)
- Boot from VHD
- *System backup is made in VHD format*



There is
no substitute
for experience

Windows 7:

- *Mount & investigate VHD with FTK:*



The screenshot displays the FTK (Forensic Toolkit) interface. The left pane shows a file tree for a mounted VHD disk named 'Blackhat_testvhd', with the current view set to 'Part_1' and 'VHD_testdisk-NTFS'. The right pane shows a hex editor view of the selected file, displaying hexadecimal data and its corresponding ASCII representation. Below the hex editor is a file list table.

File Name	Full Path	Recycle Bi...	Ext	File Type	Category	Subject	Cr Date
[\$BadClus]	Blackhat_testvhd\Part_1\VHD_testdisk-NTFS\...			Unknown Fil...	Unknown		9-3-2010 19:10:14
[\$Bitmap]	Blackhat_testvhd\Part_1\VHD_testdisk-NTFS\...			Unknown Fil...	Unknown		9-3-2010 19:10:14
[\$Boot]	Blackhat_testvhd\Part_1\VHD_testdisk-NTFS\...			Unknown Fil...	Unknown		9-3-2010 19:10:14
[\$Extend]	Blackhat_testvhd\Part_1\VHD_testdisk-NTFS\...			Folder	Folder		9-3-2010 19:10:14
[\$30]	Blackhat_testvhd\Part_1\VHD_testdisk-NTFS\...			Unknown Fil...	Unknown		9-3-2010 19:10:14
[\$LogFile]	Blackhat_testvhd\Part_1\VHD_testdisk-NTFS\...			Unknown Fil...	Unknown		9-3-2010 19:10:14
[\$MFT]	Blackhat_testvhd\Part_1\VHD_testdisk-NTFS\...			Unknown Fil...	Unknown		9-3-2010 19:10:14
[\$MFTMirr]	Blackhat_testvhd\Part_1\VHD_testdisk-NTFS\...			Unknown Fil...	Unknown		9-3-2010 19:10:14
[\$RECYCLE.BIN]	Blackhat_testvhd\Part_1\VHD_testdisk-NTFS\...		BIN	Folder	Folder		9-3-2010 19:10:24
[\$Secure]	Blackhat_testvhd\Part_1\VHD_testdisk-NTFS\...			Unknown Fil...	Unknown		9-3-2010 19:10:14
[\$Secure]	Blackhat_testvhd\Part_1\VHD_testdisk-NTFS\...			Unknown Fil...	Unknown		9-3-2010 19:10:14
[\$TXF_DATA]	Blackhat_testvhd\Part_1\VHD_testdisk-NTFS\...			Unknown Fil...	Unknown		9-3-2010 19:10:14
[\$UpCase]	Blackhat_testvhd\Part_1\VHD_testdisk-NTFS\...			Unknown Fil...	Unknown		9-3-2010 19:10:14
2009-04-23 sepoekanja	Blackhat_testvhd\Part_1\VHD_testdisk-NTFS\2...			Folder	Folder		10-3-2010 9:09:04

Windows 7:

XP mode:

Used for 'old applications'

1. *a VHD file is created*
2. *Installation of Virtual PC*
3. *Windows XP with SP 3*
4. *Application published in Win7*



Note: automatic updates / everything shared



There is
no substitute
for experience

Windows 7 files of interest:

File Extension	Description
VHD	Contains virtual Operating system and data
VMC	VM's configuration file: disks, memory, network, undo function
VSV	Saved state file - information about last running programs
VUD	Undo disk file - stored separate from VHD file

Default location:

C:\Users



There is
no substitute
for experience

Windows 7 VUD:

Undo disk: temporary file

Is it enabled ?

Investigate VMC file:

<undo_pathname>

*<absolute type="string">C:\Users\Christiaan\AppData\Local\Microsoft\Windows
Virtual PC\Virtual machines\VirtualPCUndo_Windows XP
Mode_0_0_18563103292010.vud</absolute>*

*<relative type="string">.\VirtualPCUndo_Windows XP
Mode_0_0_18563103292010.vud</relative>*



There is
no substitute
for experience

Summary:

- Virtualized environments can make forensic research a tough job
- Virtualization of hosts, applications and operating systems will scatter the evidence
- understand the rapidly improving techniques, differences between the products and what files are interesting to acquire



There is
no substitute
for experience

For the future:

- We need more research on VM
- Community, please **SHARE** !
- Forensic proof tools for VM research
- Next topic for DFRWS /Blackhat?



There is
no substitute
for experience

Questions?



There is
no substitute
for experience

Thanks for staying !

Name: Christiaan Beek

Email: Christiaan dot Beek@ tenict dot nl / dot com

Twitter: @ChristiaanBeek

Blog: <http://securitybananas.com>



There is
no substitute
for experience