



Virtual Traces

Diane Barrett

Associate Professor

University of Advancing Technology



Background

- Professor at University of Advancing Technology
 - Forensic Contractor
 - Software Development



Virtual Traces

- Without actually installing anything anywhere
- There is no information left behind on the computer



Objectives

- Explain the methods used for server and desktop virtualization
- Explain how virtualization affects a forensic investigation
- Explore methods to find virtualization artifacts and identify virtual activities



Virtual Market

Everybody's doing it!

Within 3 yrs - between 480 million and 846 million virtualized PCs



Recent Virtual Examples

HP 96 TB virtual storage - The array virtualizes at system initialization.

InstallFree converts a Windows desktop into an encrypted virtual machine file.



Virtual Machine Environment

The hypervisor - thin software layer that controls how access to a computer's processors and memory is shared
(proxy between virtual systems and physical resources)



Virtual Technology Players

VMWare

Microsoft - Hyper V

Parallels

Citrix - XenExpress

Sun – VirtualBox



Virtualization on Phones

Motorola & VirtualLogix

One phone that runs Windows CE,
Blackberry and Android – Embedded VM



Virtual Boxes

Pano

InBoxer Anti-Risk Virtual Appliance



Virtual Applications

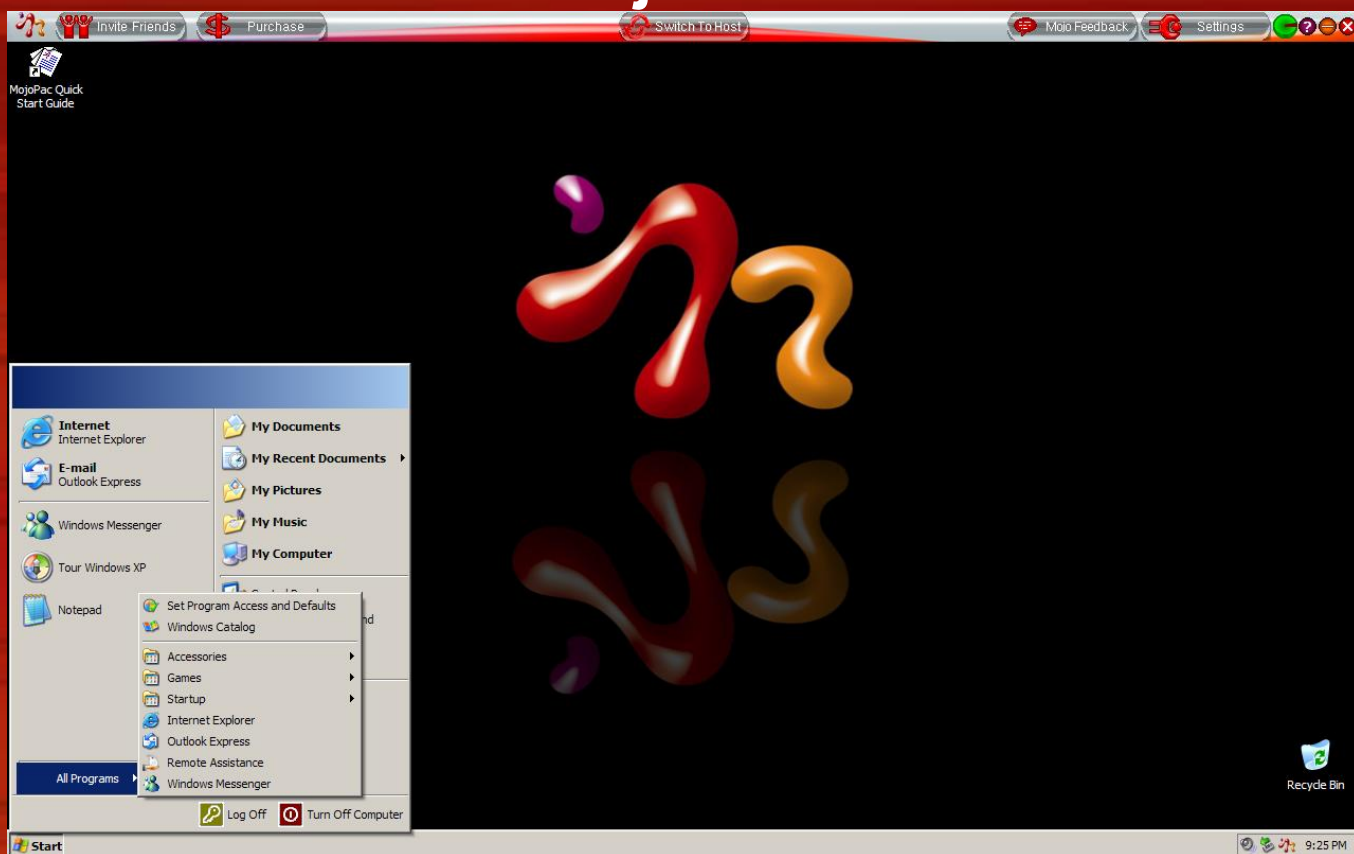
VM- Thinstall

Qumranet – SPICE Protocol

Streamed or individually contained

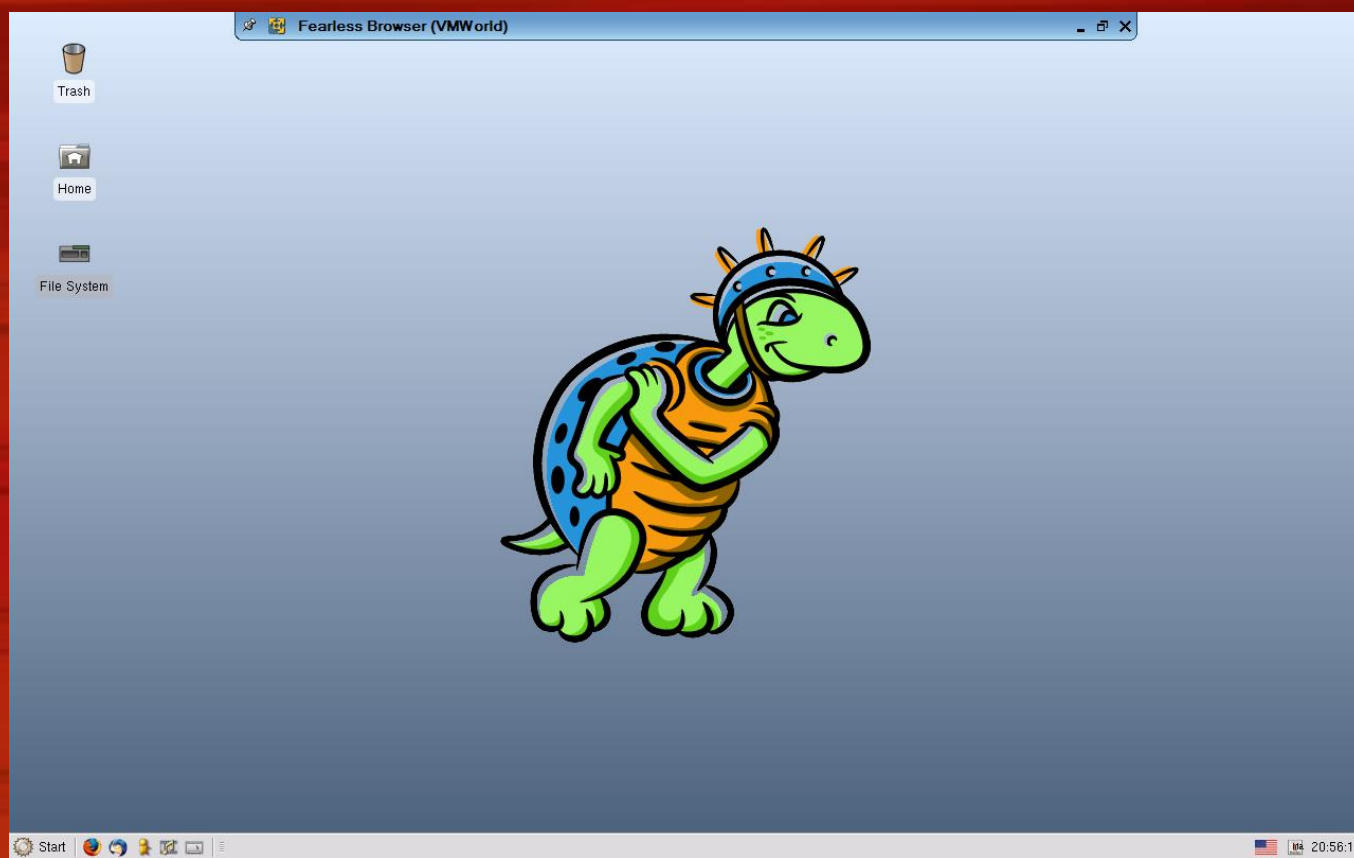


MojoPac





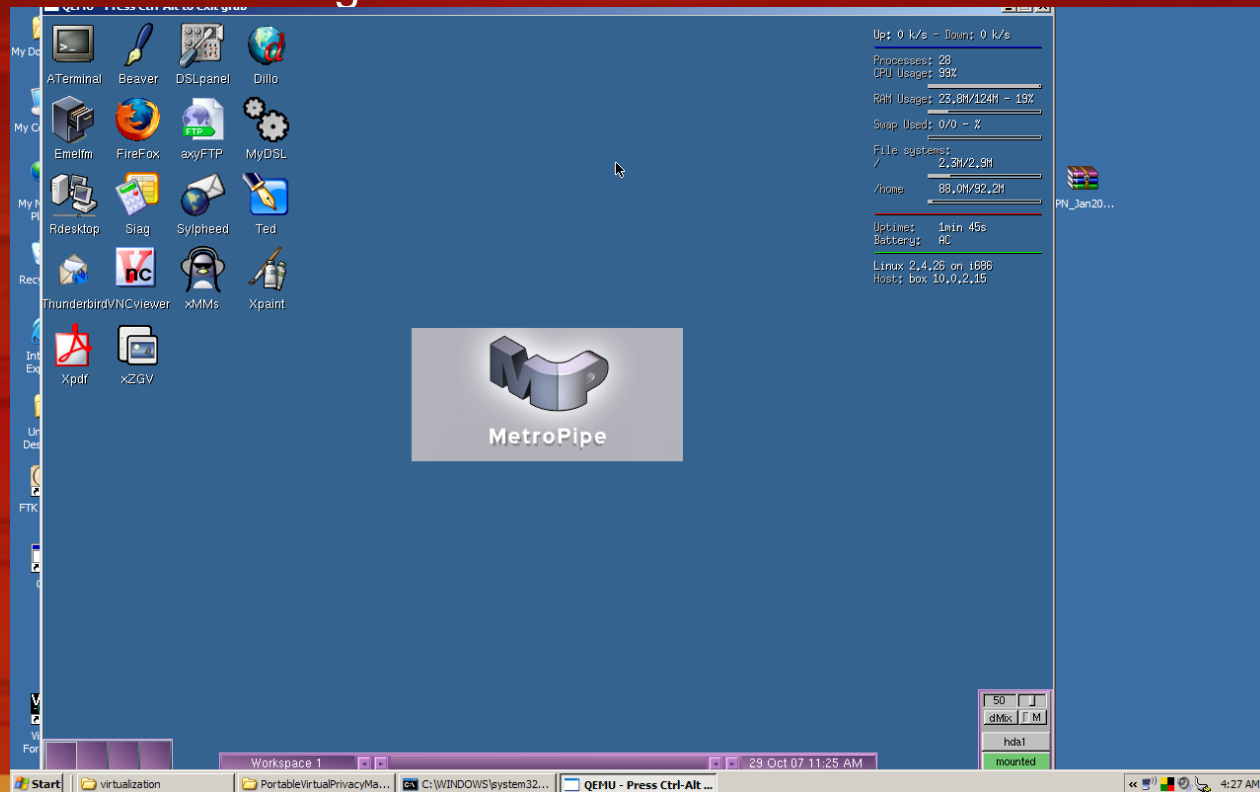
Moka5





Portable Virtual Privacy Machine

DSL designed to boot from a USB drive





VMWare player environments

BackTrack 2 with Metasploit 3





Virtualization Standard

Distributed Management Task Force, Inc. created an open standard for discovering, managing the lifecycles, controlling virtual resources and monitoring virtual systems.



How Does This Affect Forensics?

“The idea that you can make pools of dynamic resources with unlimited capacity available to users anywhere at anytime is extraordinary”. - MSFT



How Does This Affect Forensics?

- Mobile employees can leave hardware behind.
- Entire environments can now be carried on micro devices.
 - Moka 5 - “throw away your desktop”



How Does This Affect Forensics?

Let me get this straight – You are pushing out virtual OSs from a server, apps are serviced as needed – Desktops as a service DaaS.

At the end of day everything goes away



How does this affect investigations?

- Traditional methods may not be enough to find evidence.
 - Browsing and multimedia history stay inside the virtual machine.
- There may be very few traces left behind on the host PC - if there is a host PC



MojoPac Traces

- You can copy all your documents and personal items to the drive.
- Access to the local hard drive is eliminated but not the CD or removable drives.
- Needs administrative rights on the host machine in order to run unless you install usher
 - Currently only run on Windows XP



MojoPac Traces

- MojoPac has it's own separate registry and shell
- MojoPac implements paging between memory and the hard drive to take place on the host PC instead of on the portable drive
 - Process – RingThreeMainWin32
 - Phones home
 - Stores pvm.sys, ringthree.ico



Moka5 Traces

- Installs VMWare Player
- Asks whether you want to leave it installed for easier load next time
 - Streams and prefetches LivePCs
- Session changes are captured in separate file systems on a ramdisk
 - Phones home



Virtual Traces

Both MojoPac and Moka5 - MRU

Moka5 USB Clean 2238

Temp Folder- 23 Moka5-related files



Portable Virtual Privacy Machine Traces

- DSL and QEMU (fast processor emulator)
 - NTUSER.DAT and NTUSER.LOG
 - Pagefile.sys. , prefetch data
 - Phones home



VMWare Player Traces

Processes, Files, Vmtools service, File references to VMware and vmx, references in the registry to “VMware”.



Virtual Box items of interest

Processes – the VirtualBox "service" process
VBoxSVC.

VirtualBox, the GUI for the main window

Another VirtualBox process that was started
with the -startvm parameter



Portable Applications

The screenshot shows the PortableApps.com website in a Microsoft Internet Explorer browser window. The browser's address bar shows the URL <http://portableapps.com/>. The website's header features the PortableApps.com logo and the tagline "YOUR DIGITAL LIFE, ANYWHERE™". Navigation links include "Home", "Applications", "Suite", "Forums", "Development", and "Support". A search bar is located in the top right corner.

The main content area is divided into three columns:

- Left Column:** A "Download Now" button is positioned above a list of portable applications. The list includes: 7-Zip Portable, AbiWord Portable, Audacity Portable, Clementine Portable, Firefox Portable, GIMP Portable, Miranda IM Portable, Ruv Portable, OpenOffice.org Base Portable, OpenOffice.org Calc Portable, OpenOffice.org Draw Portable, OpenOffice.org Impress Portable, OpenOffice.org Math Portable, OpenOffice.org Writer Portable, Soudo Portable, Soudo Portable, Thunderbird Portable, and VLC Media Player Portable.
- Middle Column:** A section titled "Pick a PC. Any PC. Convenient" with the subtext "The NEW PortableApps Suite™". It explains that users can carry their favorite computer programs along with all of their bookmarks, settings, email, and more with them. Below this, there are three sub-sections: "Open" (describing the open platform), "Free" (stating the suite is free and contains no spyware), and "As Seen In..." (with a link to a news article from Oct 16, 2007).
- Right Column:** A section titled "What is a PORTABLE APP" with a "LEARN MORE" link. Below it is a "What's New" section listing recent updates: Mozilla Firefox PE 2.0.0.8 (Oct 22), DOSBox Portable 0.72 (Aug 28), Pidgin Portable 2.1.1 (Aug 23), ClamWin Portable 0.91.2 (Aug 23), WinSCP Portable 4.0.3 (Aug 14), Notepad++ Portable 4.2.2 (Aug 13), Pidgin Portable 2.1.0 (Aug 13), Mozilla Thunderbird PE 2.0.0.6 (Aug 02), Toucan 1.1 (Aug 01), Mozilla Firefox PE 2.0.0.6 (Jul 31), Sumatra PDF Portable 0.7 (Jul 30), and ClamWin Portable 0.91.1 (Jul 25). At the bottom of this column are links for "Get our Monthly Newsletter", "Login Now", and "Register for a Free Account", along with a "Make a Donation" button.

The browser's taskbar at the bottom shows the Start button, several open applications including Microsoft PowerPoint and PortableApps.com, and the system tray with the time 4:58 AM.



General tips

Look at:

- Link files
- Prefetch files
- Page file
- Unique identifiers associated with the program



General tips

Look for:

- Artifacts in processes, file system, and/or registry
 - Artifacts in memory
- VME-specific virtual hardware – i.e. virtual adapters, processor instructions and capabilities



Corporate Environment

- Application-layer security, firewall logging may capture more than the IP address and port number security.
 - Do not allow removable devices



Home Environment

- Home user environments need to be examined very closely for all CDs and removable devices.
- Devices are becoming smaller with larger capacity and can easily be hidden.



Challenges

VMs are applications, registries, and other components bundled into a single file.
Forensic software can't read this file.



Challenges

Tools

Documented processes

Difference in the number of files between
physical and virtual OS installations



Is it Live or is it Memorex?

Red Pill – based on relocation of sensitive data structures

ScoopyDoo

Jerry

Not too useful in investigation - possibly live



Challenges

Example: Cincinnati Bell is pushing out 800 virtual desktops to users daily using 12 images. It doesn't say what happens to these desktops at the end of the day.



Challenges

“Virtual machines are too easy to make, too hard to kill” – InformationWeek, 4/7/08

Many vendors now offer lifecycle management.

VMWare when a virtual machine is no longer in use, it gets archived on a disk.



Conclusion

- Virtualization of environments is growing
- As examiners, we need to be aware of how this affects investigations
 - “Virtual” crimes
- Data retention policies on virtual machines
 - Tools



Thank You
Contact Info:
DBarrett@uat.edu