Virtual Traces

Diane Barrett
Associate Professor
University of Advancing Technology

Background

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

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

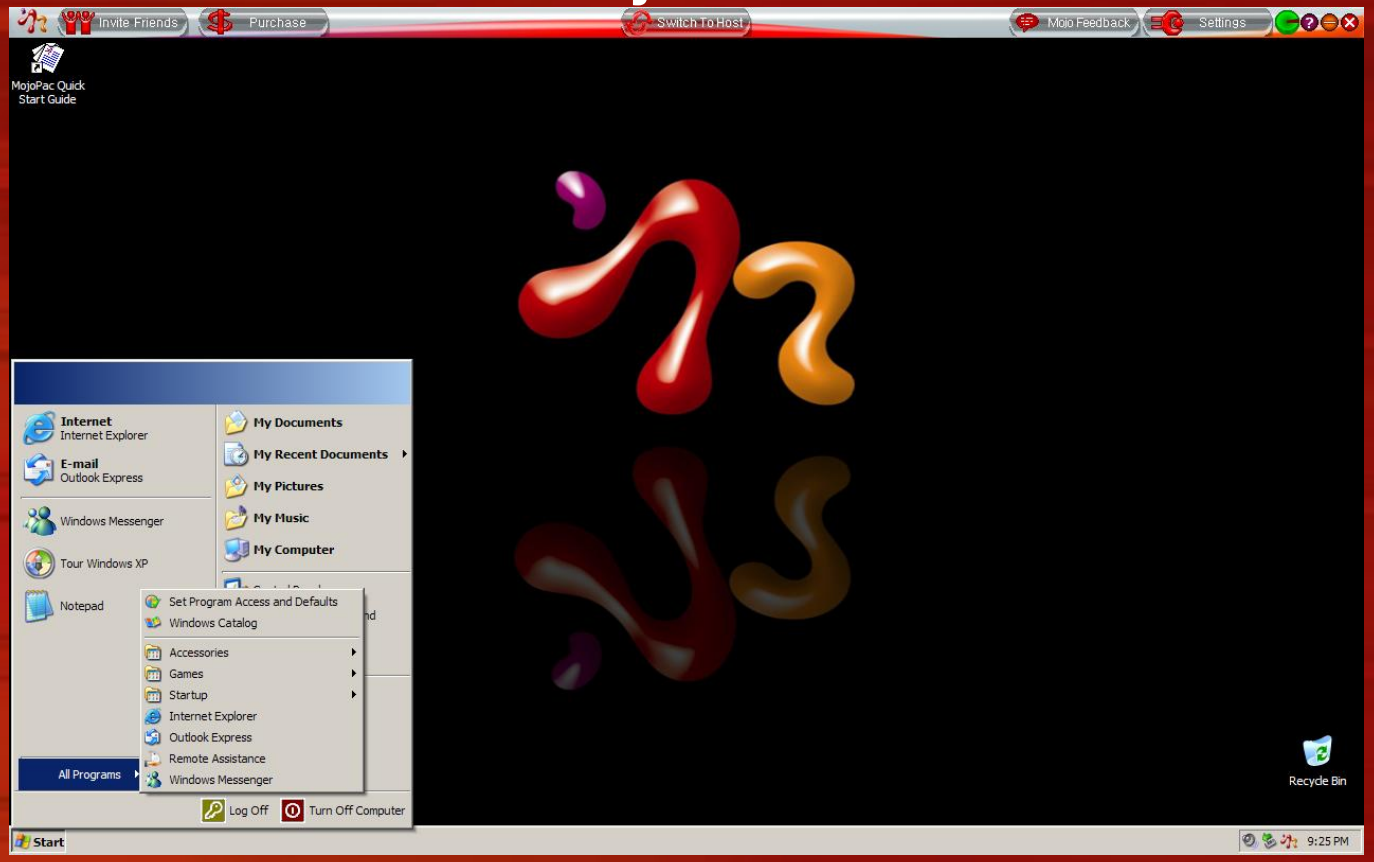
Virtual Applications

VM- Thinstall

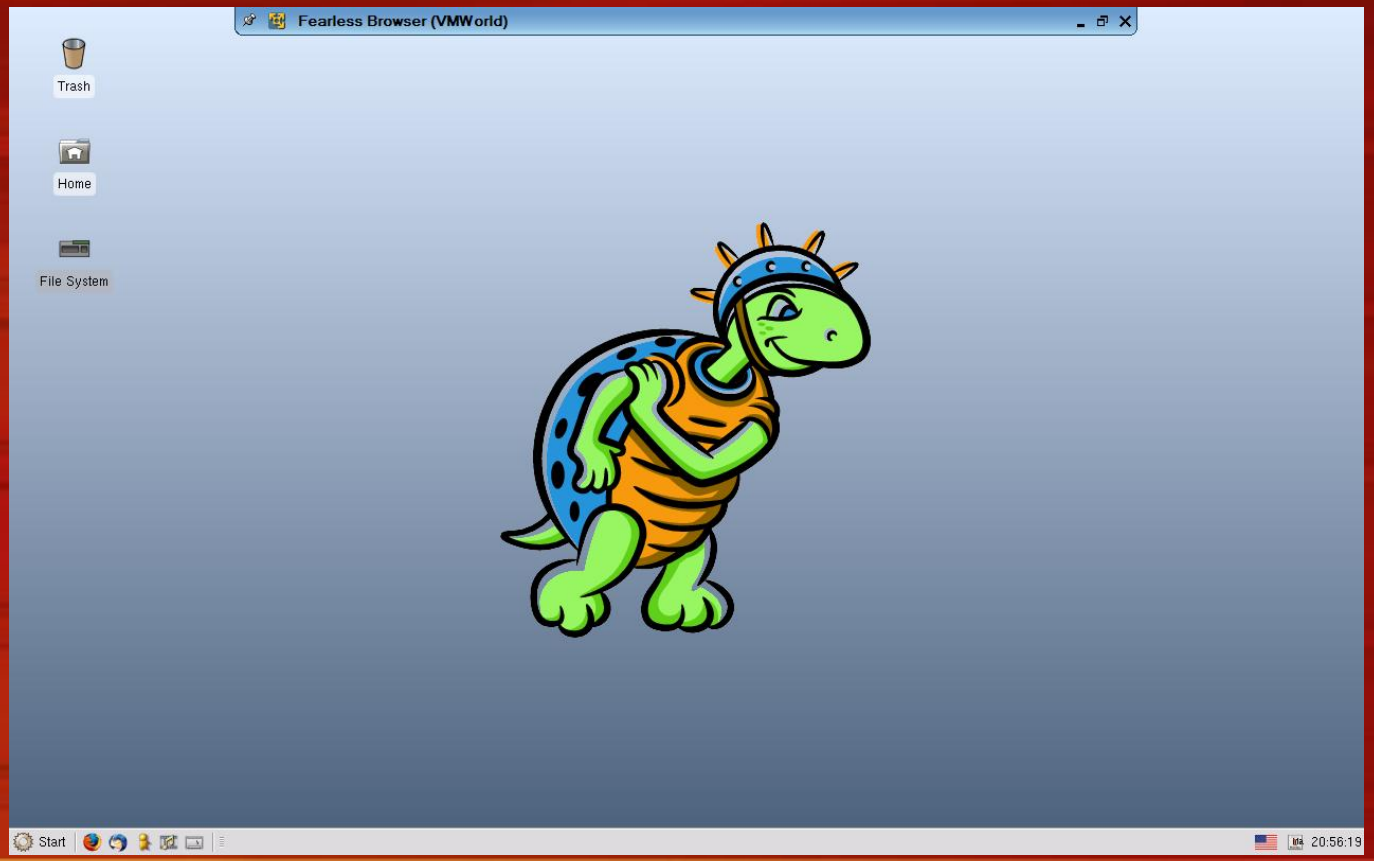
Qumranet – SPICE Protocol

Streamed or individually contained

MojoPac

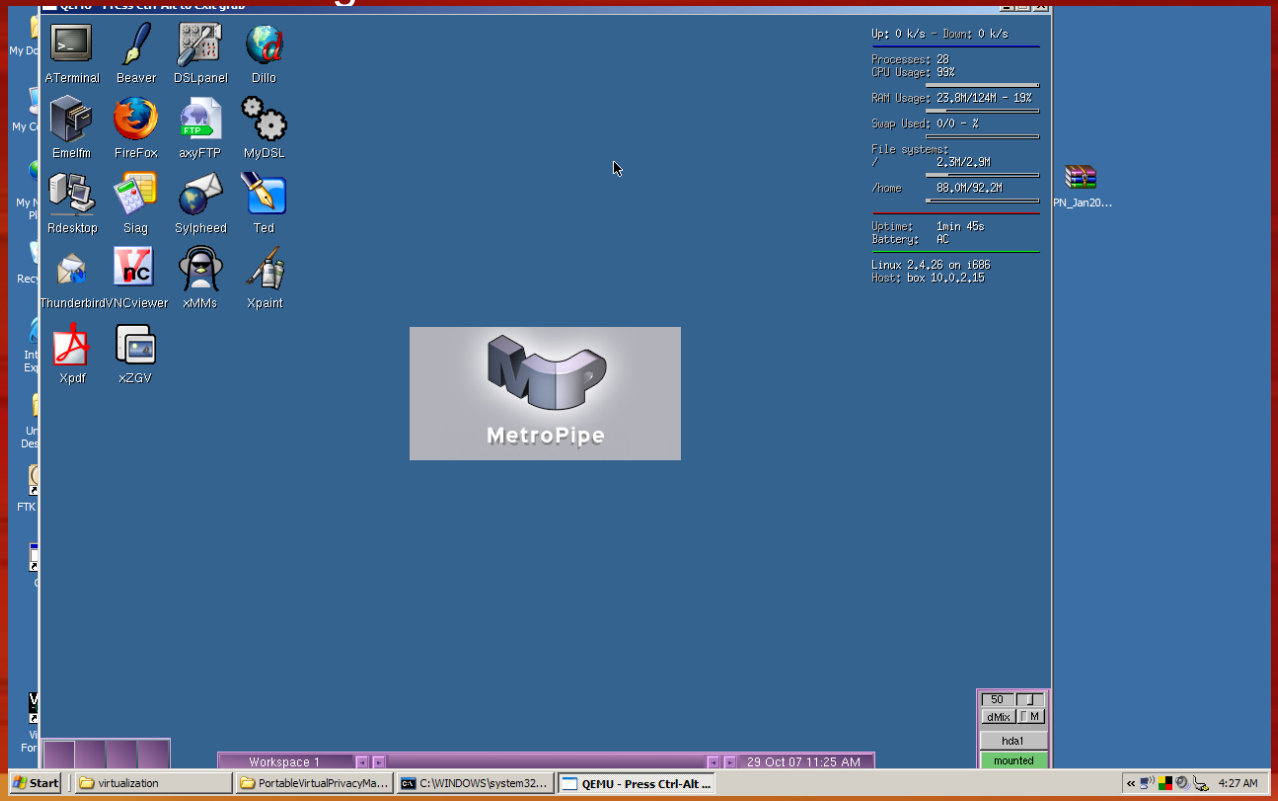

Invite Friends
Purchase
Switch To Host
Mojo Feedback
Settings
MojoPac Quick Start Guide
Internet
Internet Explorer
E-mail
Outlook Express
Windows Messenger
Tour Windows XP
Notepad
My Documents
My Recent Documents
My Pictures
My Music
My Computer
Set Program Access and Defaults
Windows Catalog
Accessories
Games
Startup
Internet Explorer
Outlook Express
Remote Assistance
Windows Messenger
All Programs
Log Off
Turn Off Computer
Recycle Bin
Start
9:25 PM

Moka5


Fearless Browser (VMWorld)
Trash
Home
File System
Start
20:56:19

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

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 to 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