Virtual Machines in Computer Forensics Research

NSRL

National
Software
Reference
Library

John Tebbutt & Doug White

NIST United States Department of Commerce
National Institute of Standards and Technology

Disclaimer

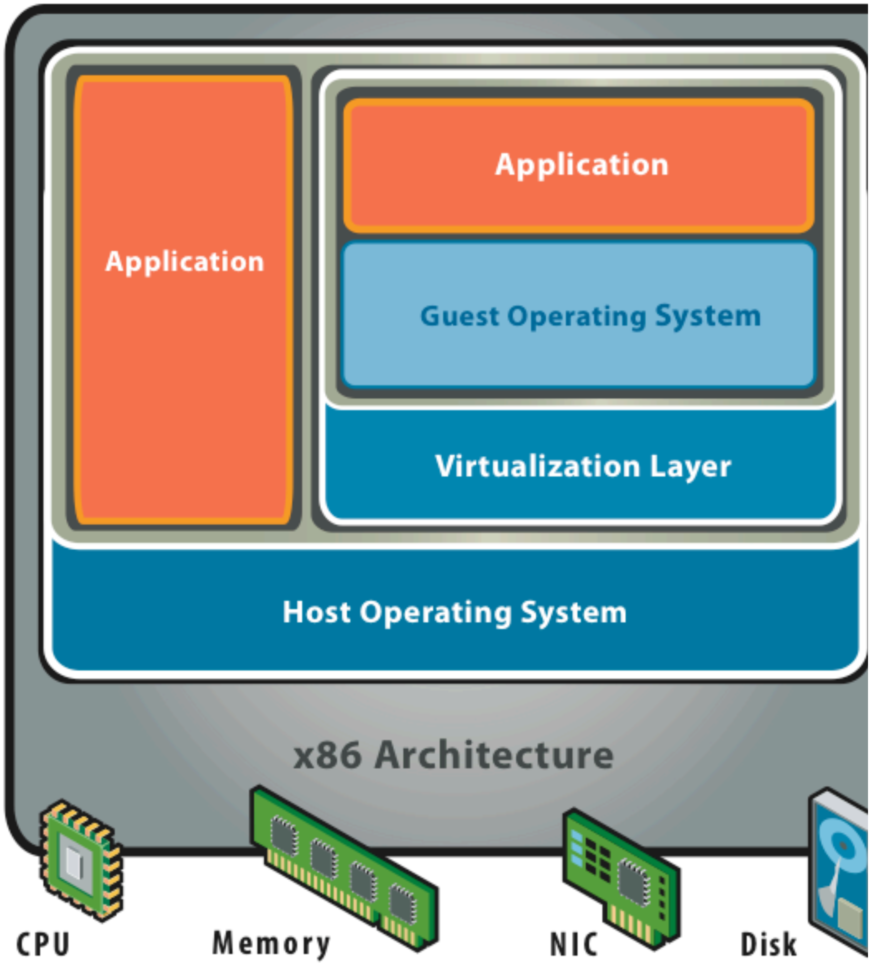
Trade names and company products are mentioned in the text or identified. In no case does such identification imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the products are necessarily the best available for the purpose.

Statement of Disclosure

This research was funded by the National Institute of Standards and Technology Office of Law Enforcement Standards, the Department of Justice National Institute of Justice, the Federal Bureau of Investigation and the National Archives and Records Administration.

What is a Virtual Machine?

- VM Application simulates a physical computer
- Install operating system, applications, etc.
- Behaves exactly as a separate machine
- A “computer in a computer”



Advantages of Virtual Machines

- Standard machine state
- Control
  - resources, configuration, connectivity, etc.
- “Snapshots” capture machine state
  - before and after comparisons
- Isolated “lab” environment within the host computer

NSRL and VMs

- Document cause-effect relationships
- Measure RDS data set coverage
- Provide raw material for data set creation

Cause and effect

- Changes in system characteristics resulting from specific actions
  - Software/malware installation/uninstallation
  - Attempts to delete files, etc
- Begin state ⇒ Action ⇒ End state
  - Compare Begin and End States
  - Record differences
- Addition/deletion/modification of filesystem and/or Windows® registry entries

Data set coverage

- RDS data set is produced from installation media
- How does this compare with real systems?
- Begin state ⇒ Action (installation) ⇒ End state
  - Record changes
  - Compare with RDS
- Measurements of RDS coverage for standard packages ⇒ 75% - 90%

Reference Data Production

- Problem:
  - Need very high coverage?
  - Cannot access all data on installation media (DRM or unknown format)?
  - Time constraints?

Reference Data Production

- Solution:
  - Create VM w/4GB virtual hard drive
  - Install software into VM
  - Burn VM hard drive image to DVD
  - Process DVD in regular fashion
  - Archive hard drive image DVD with installation media

Thank You

John Tebbutt
Computer Scientist
National Software Reference Library

National Institute of Standards and Technology
100 Bureau Drive STOP 8970
Gaithersburg, MD 20899-8970

Contacts

John Tebbutt
www.nsrl.nist.gov
nsrl@nist.gov

Barbara Guttman
Software Diagnostics & Conformance Testing Division
barbara.guttman@nist.gov

Sue Ballou, Office of Law Enforcement Standards
Rep. For State/Local Law Enforcement
susan.ballou@nist.gov