Tracking the Effects of Software on Systems: A Forensic Metadata Collection

John Tebbutt, Mary Laamanen, Alexander Nelson

The National Software Reference Library

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Disclaimer

This research was funded by the National Institute of Standards and Technology Office of Law Enforcement Standards and the Department of Homeland Security Science and Technology Directorate.

Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.

Introduction

What impact does software have on a computer system? What is its *footprint* ?

Is it diagnostic ?

Is it persistent ?

When in the software lifecycle can its elements be observed ? When should they be expected ?

Motivation

Catalog the effects of software on a system over the lifetime of the software.

Provide digital forensic investigators with new reference data.

Extend the NSRL research environment for use by forensic researchers to develop new tools and techniques.

Application Footprint

Combines the what, where, when and how:

- Nature of changes
- Location of changes
- Actions causing changes
- Stage in application lifecycle

Application Footprint Slices

A “slice” is a collection of metadata derived from a system at a particular moment in time

cf. a slice of time

Application Footprint is the sequence of all slices taken during the software lifecycle

Minimum Slice Set

Package dependent, but must include:

- Installation
- Execution
- Uninstallation
- Post system restart

Systems and Software

All software is part of the NSRL collection
- Known, traceable

Operating Systems
- Focus on Microsoft© Windows® variants

Software applications
- Based on community recommendations and requests

Operating Systems

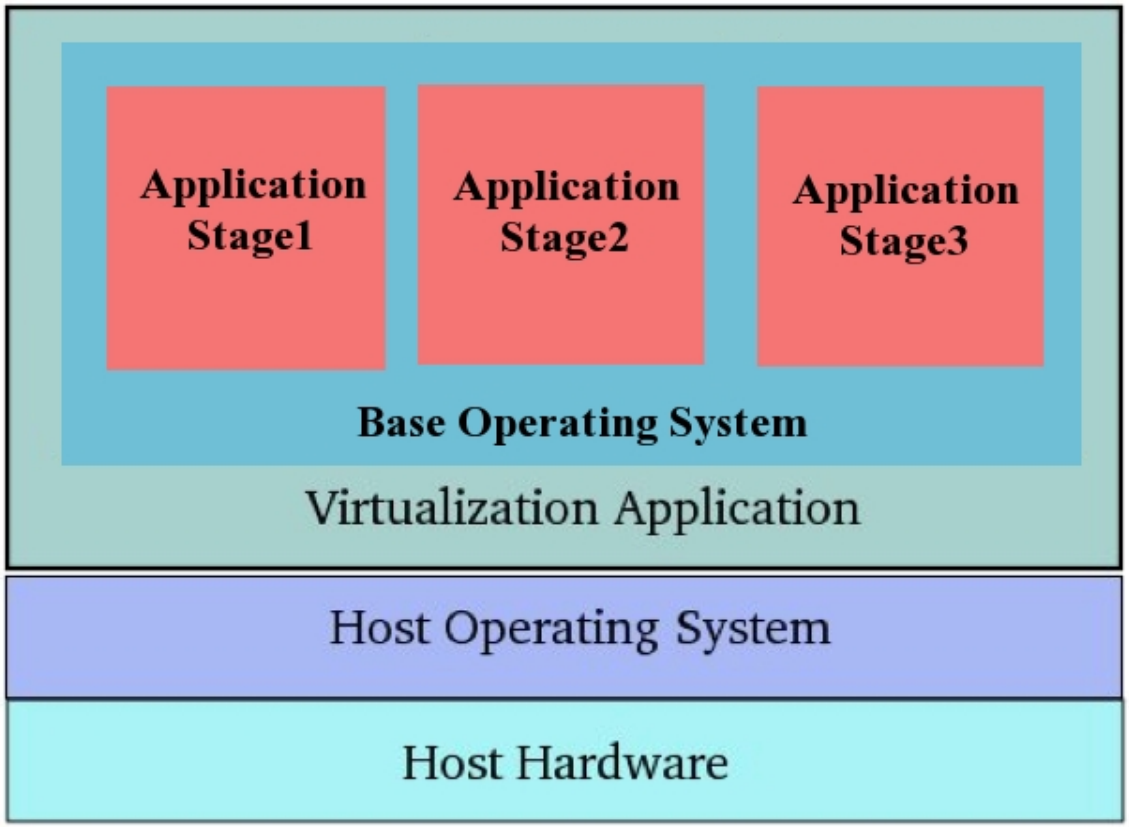
Windows XP, Windows Vista 32/64bit, Windows 7 32/64bit, Windows 8.

Sample Applications

- Browsers: Chrome, Firefox, Safari, IE.
- Archivers : WinZip, WinRAR
- Network Tools: Wireshark, AirSnort, NetCat
- Executable Packer: UPX
- Microsoft Office: 2003 and later
- Messengers: Windows Live, Yahoo! Messenger

Method

Virtual Machine Installation



Virtual Machine Advantages

VM state can be captured at any time
- VM may be paused / suspended

VM is preserved as a set of files
- Hard drive, RAM contents, etc.

Can be copied off for external processing

Save for future reference and further investigation

Changes in a System

File system (file hashes, MAC times, etc)
- Executables
- Libraries
- Documents / Images / Multimedia

Configuration information
- Windows® Registry

Memory mapping information
- System RAM

Network Chatter
- Changes in *external* systems

Method

Step through the minimum slice set:

- Post – Installation
- Post – Execution
- Post – Uninstallation
- Post system restart

Slice Data

Slice ID – Unique ID

Slice State – Stage in the software lifecycle

Slice Notes – All user actions taken when generating the slice including unexpected software behavior

Diskprint Bundle

Diskprint bundle contains:

- VM bundle for each diskprint slice
- File of network chatter for each slice
- SQL file with the notes and captured metadata for each slice

The completed bundle is moved to a server for processing.

Challenges

Slow Process – Saving off the VM is slow

Difficult to isolate software behavior:
e.g. avoid automatic updates

Not totally automated – Human judgment to decide when to take a slice

The decision is not straightforward

Diskprint Use

Study the Windows® Registry
- see Alex Nelson's work

Use case for Digital Forensics standards development:

Digital Forensics XML (DFXML)
Cyber Observable Expression (CybOX™)

What's Next?

Streamline the diskprinting process:

E.g. use snapshot mechanism provided by VM vendor.

Expand technique to capture automatic updates (e.g. software updates) on live systems.

Thank You

John Tebbutt — john.tebbutt
Mary Laamanen — mary.laamanen
Alex Nelson — alex.nelson
} @nist.gov