Testing the Forensic Soundness of Forensic Examination Environments on Bootable Media

By

Ahmed Fathy Abdel Latif Mohamed, Andrew Marrington
Farkhund Iqbal and Ibrahim Baggili

Presented At

The Digital Forensic Research Conference

DFRWS 2014 USA Denver, CO (Aug 3rd- 6th)

DFRWS is dedicated to the sharing of knowledge and ideas about digital forensics research. Ever since it organized the first open workshop devoted to digital forensics in 2001, DFRWS continues to bring academics and practitioners together in an informal environment. As a non-profit, volunteer organization, DFRWS sponsors technical working groups, annual conferences and challenges to help drive the direction of research and development.

http:/dfrws.org

TESTING THE FORENSIC SOUNDNESS OF FORENSICS EXAMINATION ENVIRONMENTS ON BOOTABLE MEDIA

University of New Haven Cyber Forensics Research and Education Group
(UNHcFREG)
Zayed University – Advanced Cyber Forensics Research Laboratory
Ahmed Fathy Latif Mohamed, Andrew Marrington, Ibrahim Baggili

UNIVERSITY OF NEW HAVEN

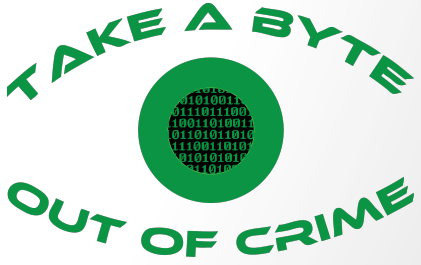
جامعة زايد
ZAYED UNIVERSITY

TAKE A BYTE OUT OF CRIME

www.UNHcFREG.com

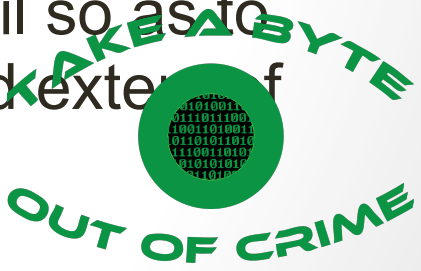
Introduction

- Many forensic bootable CD/DVD/USB Linux Distributions
- Bootable has advantages:
  - Conduct quick analysis on scene on a trusted OS
  - Examining without acquisition
  - Acquiring the RAM
  - Confronting suspect on scene
  - Provide known-good binaries for live examinations
  - No need to disassemble computer
  - Good for legacy hardware



Problem

- Despite utility, they might get called into question
- May change the suspect's system
  - So – its important to test forensic soundness of the live CDs
- We contend that alterations are permissible if:
  - Minimal in terms of their impact upon the data which is of evidentiary value,
  - Well-understood in terms of the nature and extent of those alterations, and
  - Documented properly and in sufficient detail so as to accurately represent the cause, nature, and extent of the alterations.



Apparatus

- Standard equipment found in most DF Labs
  - Suspect computer
    - Single HD and bootable optical drive
    - IBM Thinkpad T42
    - 40 GB disk
  - Forensic workstation
  - TABLEU Hardware writeblocker
  - Knoppix v7.0, Helix P3 Pro 2009R3, Kali Linux v1.0

Methodology

- Scenario performed
- Power down
- Remove Disk – connect to HD blocker
- Image disk (call this image img1)
- Reinstall disk
- Boot from bootable media
- Examine the data on drive and shutdown
- Remove disk, re-image (img2)
- Compare hash values and files

Knoppix Results

- Auto mount read/write
- Allowed us to create files from its graphical shell – logged on as default user
- C:\[root]\$I30
- C:\[root]\$MFT
- C:\[root]\Documents and Settings\Administrator\Local Settings\$I30
- C:\[root]\Program Files]Cisco Packet Tracer 5.3.1\sounds\ simulationTab.wav

Comparison of images for Knoppix v7.0

Image	SHA1 Hash Value
Img	e942df9b391053ce33a2ddfc8cdd19713413e43a
img'	fd041692beb80245c6468ae13a087b0df61cd892

d

Helix 3 Pro results

- C:\[root]\$I30
- C:\[root]\$MFT
- C:\[root]\WINDOWS\bootstat.dat
- Contents did not change, only access time stamp was changed

Comparison of images for Helix3 Pro 2009R3.

Image	SHA1 Hash Value
Img	6aa81d809c1c2bdff55baa8d4a8a95682718344d
img'	d454ab49357118618daaad214a40b66dc0ebd7df

Kali Linux

- Automatically mounted as read/write
- Unmounted partition, and mounted again as read
- 1. C:\[root]\$I30
  2. C:\[root]\$LogFile
  3. C:\[root]\$MFT
  4. C:\[root]\WINDOWS\bootstat.dat
- Contents did not change, only access time stamp was changed

Comparison of images for Kali Linux v1.0

Image	SHA1 Hash Value
Img	1c473f5fee75dec2e9c2703f57d2a2bac0a59b75
img'	693bbfe4fd20b6afbd7f3d581501cd6402af3c6a

Windows USB bootable forensic tool

- 1667 added files ☹

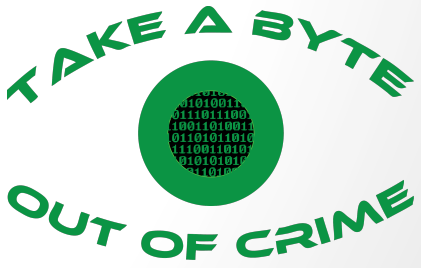
Summary

Summary of results.

	Helix3 Pro 2009R3	Kali v1.0	Knoppix v7.0
Hard disk altered?	Yes	Yes	Yes

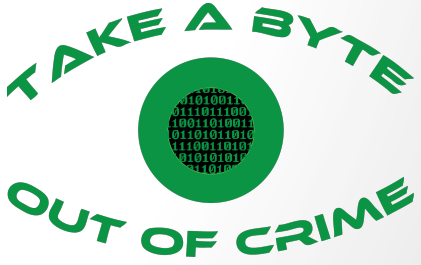
Files changed (hash values differ) during search	`$LogFile`
	`$MFT`
	`C:\WINDOWS\bootstat.dat`
		`C:\$I30`
		`$LogFile`
		`$MFT`
		`C:\WINDOWS\bootstat.dat`
			`C:\$I30`
			`$MFT`
			`C:\Documents And Settings\Administrator\Local Settings\$I30`
			`C:\Program Files\Cisco Packet Tracer 5.3.1\sounds\simulationTab.wav`

Forensic usage acceptable?	Yes	No	No



Future Work

- Predictability
  - Set of experiments with more types and kinds of computers
  - We have to verify predictable alterations (more testing)
- Broader testing
  - Experiments with other bootable environments
  - Test on other filesystems – we did our testing only on NTFS Windows XP systems
  - Deeper survey of all distributions and effects of mounting disks
- Deeper analysis
  - Investigate the causes of the changes
- Automate process
  - Create scripts to automate the testing process



Additional UNHcFREG Projects

- Andrew.marrington@zu.ac.ae
- ibaggili@newhaven.edu

UNIVERSITY OF NEW HAVEN

TAKE A BYTE OUT OF CRIME

www.UNHcFREG.com