Seized Forensic Data Collection

Cybercrime Lab

U.S. Department of Justice

Computer Crime and intellectual Property Section

Seized Forensic Data Collection

AGENDA

- **Value of Forensic Data Collection**
- **Seized Forensic Data Collection Methods**
  - Volatile Data Collection
  - Live System Imaging
  - Forensic imaging of Digital Media
  - Taken Seized Devices and Media physically

Seized Forensic Data Collection

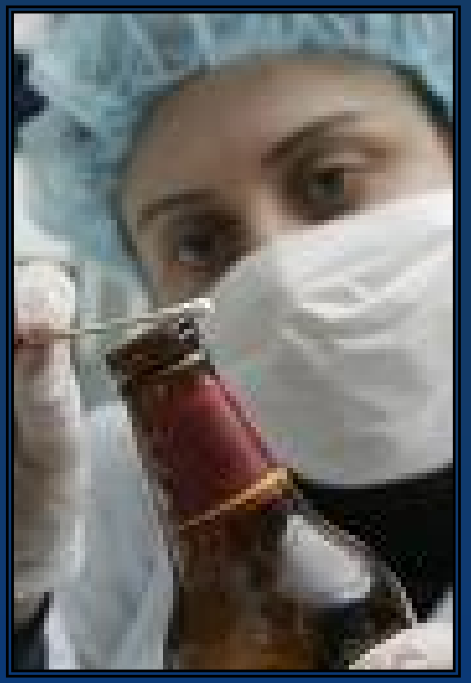
Value of Forensic Data Collection

- Incident Response/Forensic Data Collection is the MOST IMPORTANT step in the entire electronic investigation

- Failure can invalidate or make inadmissible all further information gathered from the forensic data
  - Or at least give your attorneys a headache

What is Volatile Data

- System date and time
- Users Logged On
- Open Sockets/Ports
- Running Processes
- RAM
- And more…



When To Use This Method

- System is running and evidential data will be lost if system is powered off.

- Some Common Situations
  - Device is hacked, being hacked.
  - Device is compromised by virus, Trojans, Bots, etc.
  - Network communication or file transfer may be on going.

Tools for Volatile Data Collection

- Customized tool kit
- Helix (www.e-fense.com/helix)
- Livewire (www.wetstonetech.com)
- Encase Enterprise Edition (www.encase.com)

CAUTION

- Volatile data collection process makes changes on target system.
- Document tools and actions performed.
- Keep the tool media with forensic data if non-standard tools used.

What is Live System Imaging

- Partial or full imaging of data on logical level or physical level on running system.
  - Logical Level: A logical partition on a storage media
  - Physical Level: Every accessible bit on the physical device.
  - Partial imaging: A set of files and/or folders on logical level.
  - Full imaging: The entire content at selected level.

When To Use This Method

- System is running and can't be shutdown for various reasons.
- Some Common Situations
  - Business server of a innocent party or victim
  - Computer running with full disk encryption
  - This is the best method available

Tools for Live System Imaging

- DD
- Encase (www.encase.com)
- FTK (www.accessdata.com)
- Helix (www.e-fense.com/helix)
- Livewire (www.wetstonetech.com)

CAUTION

- Live System Imaging process makes changes on target system.
- Document tools and actions performed.
- Keep the tool media with forensic data if non-standard tools used.

What is Forensic Imaging of Digital Media

- Obtained by a method which does not, in any way, alter any data on the drive being duplicated.
- Duplicate must contain a copy of every bit, byte and sector of the source drive.
- Duplicate will not contain any data except filler characters (for bad areas of the media) other than that which was copied from the source media.
- Data Accurate, Verifiable and Reproducible.

When To Use This Method

- System can be powered off for data collection.
- Some Common Situations
  - System with archive documents such chat logs, financial documents, emails, pictures, downloads of copyright programs, music and movies, etc.
  - Computer running with no disk encryption
- Most optimal way to preserve evidence.
- Most often used method.

Tools For Forensic Imaging

- Write Blocks
  - Software (SW) Write Block
    - PBDLOCK, **RCMP** HDL, etc
  - Hardware (HD) Write Block
    - Firefly, Tableau, etc
  - HW write block is less prone to human error than SW write Block.

www.digitalintelligence.com

http://www.tableau.com

Tools For Forensic Imaging (Cont)

- Imaging Tools
  - Software (SW)
    - DD, Encase, FTK, etc
  - Hardware (HD)
    - Hardcopy, Logicube, Solo III, etc.
  - Generally, HD imaging tools are simpler to use than SW tools.

accessdata.com


Encase.com

www.logicube.com

www.digitalintelligence.com


www.paraben-forensics.com

www.diskology.com

Seized Forensic Data Collection Methods

Forensic Image of Digital Media

The Forensic Imaging Process

- Theoretical Process:

- A Practical Setup:

CAUTION

- Extra care for software write block program. It may not run properly or not working properly.
- Extra for hardware imaging devices. Do not mix up source and destination.

Taken Seized Devices and Media physically

When It's Used

- All other options does not work out.
- Ex. Not enough time, Equipment failure, lack of forensic tools, etc.

Taken Seized Devices and Media physically

Tools for Taken Seized Devices and Media Physically

- Device is off or can be turned off.
  - Easy, no special tools needed
- Device is on or can be turned off.
  - Hotplug

Questions

Cybercrime Lab
Computer Crime and
Intellectual Property Section
United States Department of Justice

Phone: 202-514-1026

Web: ww.cybercrime.gov