Computer Forensics using Open Source Tools

COMP 5350/6350 Digital Forensics
Professor: Dr. Anthony Skjellum
TA: Ananya Ravipati
Presenter: Rodrigo Sardinas
Overview

• Use case explanation
• Useful Linux Commands
• Kali
• DCFLDD
• Autopsy
• Use Case Demo
• Foremost
• Scalpel
• Digital Forensics Framework (DFF)
• Try it Yourself
Overview

• Use case explanation
Use Case Explanation

• Suspect machine to examine
  – VirtualBox to Demo
    • Puppy Linux and Kali 1.1.0

• LiveUSB image of Kali
  – Live (Forensics Mode)

• Make and hash bit-by-bit copy of machine
  – Using DCFLDD

• Copy and examine dd image using various open source tools in Kali
  – Autopsy, Foremost, Digital Forensics Framework, etc...
Overview

- Use case explanation
- Useful Linux Commands
Useful Linux Commands

- **fdisk -l**
  - Working with and managing Linux partitions
  - `-l` option is used to view all existing partitions
- **cd**
  - Change to a different directory
- **ls**
  - List contents of a directory (folder)
- **mkdir**
  - Create a folder
- **mount**
  - Mount device to be used as a directory
Overview

- Use case explanation
- Useful Linux Commands
- Kali
Kali

- [Website](#)
- The older, cooler name was BackTrack
- Debian based
- Mostly known for penetration testing
- Loaded with tools for penetration testing, digital forensics, reverse engineering
Kali (cont...)  

• Live (Forensic Mode)  
  – Internal hard disk not auto mounted  
  – Swap partition not used  
    • Previous two points verified by hashing disk before booting into Kali Live forensic mode, and checking hash after removing Kali  
  – Auto-mounting of removable media is disabled (USB thumb drives, CDs, etc...)  
  – See: [http://docs.kali.org/general-use/kali-linux-forensics-mode](http://docs.kali.org/general-use/kali-linux-forensics-mode)
Overview

• Use case explanation
• Useful Linux Commands
• Kali
• DCFLDD
DCFLDD

- Developed by Department of Defense’s Digital Computer Forensics Laboratory.
- A variation of dd designed to make verifiable, legally sound copies
- Ability to “Hash on-the-fly” or hash input data as it is being transferred to ensure data integrity.
- Split/Multiple outputs
  - Can split output to multiple files at the same time with more configurability than the split command
- Piped output and logs
  - Can send all log data and output to commands and files natively
Overview

• Use case explanation
• Useful Linux Commands
• Kali
• DCFLDD
• Autopsy
Autopsy

• Graphical Interface to The Sleuth Kit and other digital forensics tools
• Plug-in architecture allows “easy” addition of file analysis modules written by others or creation of your own in Java or Python
• Timeline analysis – graphical event viewing interface
• Recover files from most common formats
• Email analysis – Parses MBOX format messages
• See:
Overview

- Use case explanation
- Useful Linux Commands
- Kali
- DCFLDD
- Autopsy
- Use Case Demo
Use Case Demo
(Boot Puppy Linux from Kali iso)
Use Case Demo
(Attach usb drive to Puppy Linux VM)
Use Case Demo
(Boot into Live Forensic Mode)
Use Case Demo
(Mount USB to write dd to)
Use Case Demo
(Create and hash dd image 1)
Use Case Demo
(Create and hash dd image 2)
Use Case Demo
(Create and hash dd image 3)

• dcfldd if=/dev/sda hash=md5 of=/media/60E7-A692/puplinimage.dd conv=noerror
  – dcfldd – name of program
  – if – in file or source file
  – hash=md5 – hash + type of has to perform
  – of – out file or output file
  – conv=noerror – continue to make image even if read error occurs (bad sectors, etc...)
Use Case Demo
(Create and hash dd image 4)
Use Case Demo
(Create and hash dd image 5)
Use Case Demo
(Create case using Autopsy 1)
Use Case Demo
(Create case using Autopsy 2)
Use Case Demo
(Create case using Autopsy 3)

WARNING: Your browser currently has Java Script enabled.
You do not need Java Script to use Autopsy and it is recommended that it be turned off for security reasons.

http://www.sleuthkit.org/autopsy/
Use Case Demo
(Create case using Autopsy 4)

CREATE A NEW CASE

1. **Case Name:** The name of this investigation. It can contain only letters, numbers, and symbols.
   - puppy-linux

2. **Description:** An optional, one line description of this case.
   - autopsy demo

3. **Investigator Names:** The optional names (with no spaces) of the investigators for this case.
   - a. Rodrigo_Sardinas
   - b. 
   - c. 
   - d. 
   - e. 
   - f. 
   - g. 
   - h. 
   - i. 
   - j. 

NEW CASE  |  CANCEL  |  HELP

To direct input to this VM, move the mouse pointer inside or press Ctrl-G.
Use Case Demo
(Create case using Autopsy 5)

Creating Case: puppy_linux

Case directory (/var/lib/autopsy/puppy_linux/) created
Configuration file (/var/lib/autopsy/puppy_linux/case.aut) created

We must now create a host for this case.

Please select your name from the list: Rodrigo_Sardinas

Add Host
Use Case Demo
(Create case using Autopsy 6)

1. **Host Name**: The name of the computer being investigated. It can contain only letters, numbers, and symbols.
   - puppy_linux_suspect

2. **Description**: An optional one-line description or note about this computer.
   - image of bad guy's machine

3. **Time zone**: An optional time zone value (i.e., EST5EDT). If not given, it defaults to the local setting. A list of time zones can be found in the help files.
   - EST5EDT

4. **Timeskew Adjustment**: An optional value to describe how many seconds this computer's clock was out of sync. For example, if the computer was 10 seconds fast, then enter 10 to compensate.
   - 0

5. **Path of Alert Hash Database**: An optional hash database of known bad files.

6. **Path of Ignore Hash Database**: An optional hash database of known good files.

---

**Additional Information**

*Note:* The screenshot shows a part of the Autopsy interface where a new host is being added. The details entered in the fields are placeholders for demonstration purposes.
Use Case Demo
(Create case using Autopsy 7)
Use Case Demo
(Create case using Autopsy 8)

1. Location
   Enter the full path (starting with `/`) to the image file. If the image is split (either raw or Encase), then enter `"` for the extension.
   ```plaintext
   /media/60E7-6692/puplinimage.dd
   ```

2. Type
   Please select if this image file is for a disk or a single partition.
   - Disk
   - Partition

3. Import Method
   To analyze the image file, it must be located in the evidence locker. It can be imported from its current location using a symbolic link, by copying it, or by moving it. Note that if a system failure occurs during the move, then the image could become corrupt.
   - Symlink
   - Copy
   - Move
Use Case Demo
(Create case using Autopsy 9)
Use Case Demo
(Create case using Autopsy 10)
Use Case Demo
(Analyzing the Image 1)
Use Case Demo
(Analyzing the Image 2)
Use Case Demo
(Search for Deleted Files 1)
Use Case Demo
(Search for Deleted Files 2)

File Browsing Mode

In this mode, you can view file and directory contents.

File contents will be shown in this window.

More file details can be found using the Metadata link at the end of the list (on the right).

You can also sort the files using the column headers.
Use Case Demo
(Search for Deleted Files 3)
Use Case Demo
(Search for Deleted Files 4)
Overview

- Use case explanation
- Useful Linux Commands
- Kali
- DCFLDD
- Autopsy
- Use Case Demo
- Foremost
- Scalpel
Foremost and Scalpel Video
Overview

• Use case explanation
• Useful Linux Commands
• Kali
• DCFLDD
• Autopsy
• Use Case Demo
• Foremost
• Scalpel
• Digital Forensics Framework (DFF)
Digital Forensics Framework
Overview

• Use case explanation
• Useful Linux Commands
• Kali
• DCFLDD
• Autopsy
• Use Case Demo
• Foremost
• Scalpel
• Digital Forensics Framework (DFF)
Do it Yourself

• Downloads
  – Kali
  – Puppy Linux

• Videos
  – Create VB Image from Puppy Linux
    • Video does not show boot flag being set in GParted. Once you have created your partition, right click the partition, select the flags option, and check the boot option.
  – Autopsy
  – RecoverJPG, Foremost, Scalpel
  – Digital Forensic Framework (DFF)

• Articles
  – DCFLDD in Kali
  – Autopsy in Kali
  – Useful forensics tools