

Overview

- Introduction

- Next Week
 - Network & Email Forensics
 - Digital Image Forensics
 - Cell and Mobile Device Forensics

 - Video?

 - [Framed by a virus?](#)
 - [The Nigerian connection](#)
 - [Saved by Facebook](#)



Motives for Cybercrimes: the 5 W's

- Finding the motive—answering the 5 Ws helps in criminal investigations:
 - Who?
 - What?
 - Where?
 - When?
 - Why?

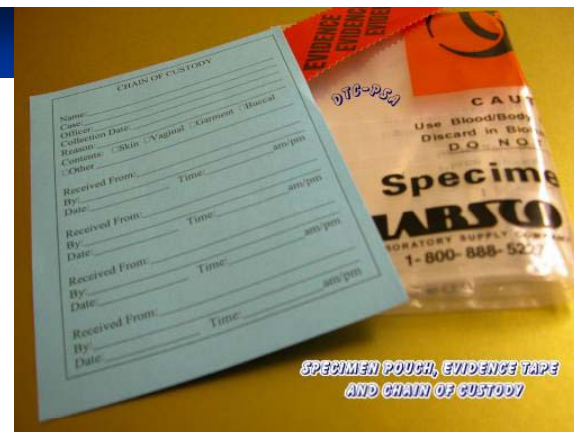
- Possible motives:
 - Financial gain, including extortion and blackmail
 - Cover up a crime
 - Remove incriminating information or correspondence
 - Steal goods or services without having to pay for them
 - Industrial espionage
 - Framing
 - Pranksters?

 - What else?



The 3 C's of E-Evidence – some guidelines

- Care
- Control
- Chain of Custody



- These guidelines are more burdensome for **easily altered digital data** – e.g. e-mail evidence; the investigator would have to establish the **origin** of the message, the **integrity** of the system in which the message was transmitted, and the **chain of custody** of the message
- E-evidence may be affected by magnetic forces, so they should not be placed in a vehicle or truck that also contains electromagnetic equipment (similar to blood needing to be kept at the proper temperature)
- The operations used to actually collect, copy, analyze, control, and present e-evidence **cannot modify the original item** being studied in any manner
- Everyone who touches evidence can **contaminate** it – therefore a strict **chain of custody** is essential in computer forensic investigations – each piece of original evidence that is seized should have a **chain of custody log** associated with it

Chain of Custody Form

EVIDENCE	
Submitting Agency _____	
Date Collected _____	Time _____
Item # _____	Case # _____
Collected By _____	
Description of Evidence _____	

Location Where Collected _____	
Type of Offense _____	
CHAIN OF CUSTODY	
Rec. From _____	By _____
Date _____	Time _____
Rec. From _____	By _____
Date _____	Time _____
Rec. From _____	By _____
Date _____	Time _____

Establishing Chain of Custody

- During an investigation, the following procedures should be followed to ensure the chain of custody:
 1. A record or **evidence log** should be kept to show when all items of evidence, such as server logs, computers, hard drives, and disk, are received or seized and where they are located
 2. If the items are released to auditors, authorities, or the court, those **release dates should be recorded**
 3. Access to evidence should be **restricted** throughout the investigations and any subsequent proceedings
 4. To preserve the chain of custody, the **original hard disk should be placed in an evidence locker** and appropriate notations should be made in the evidence log
 5. All computer forensics should be performed in the **mirror image copy (which should be write-protected)** – never on the original

Basic Steps in Security Forensics (at a glance)

- Generally involves steps similar to those of standard forensics:
 - **Secure the crime scene**
 - organizations/ individuals should call the response unit at the first hint of security issue
 - the surroundings should be documented (e.g. was the computer on?)
 - photographs and equipment should be labeled (digital photography problems?)
 - computer, peripherals, and media should be taken into custody (warrant problems)

 - **Preserve the Data**
 - collect & copy the evidence
 - volatile data must be captured
 - mirror image backup must be performed

Basic Steps in Security Forensics (at a glance)**– Establish a chain of custody**

- details of location of evidence must be documented – and who handled them along the way

– Examine and preserve the evidence

- files, documents, e-mail must be searched
- Windows “page files” must be examined
- RAM slack
- file slack

– Reporting Procedures

Must be strong enough to be admissible in court – in many cases have to be **stronger than traditional evidence** (why)

Securing the Crime Scene

- **Physical surroundings** of the computer should be clearly documented
- **Photographs** of the area should be taken before anything is touched

potential problem with photographs

- **Cables** connected to the computer should be labeled to document the computer's hardware components and how they are connected
- Forensics team takes custody of the entire computer along with the **keyboard and any peripherals – why?**

warrant problems

Preserving the Data

- **Collection Process:**
 - A list should be generated that states what exactly is to be collected and analyzed
 - All log files and intrusion detection output should be examined to provide focus for the investigation
 - If the system is left on, it is important that any monitor output is written down or photographed – why?
 - Why not just “save”
 - All data should be preserved in the state it was prior to the investigation

- Computer forensics team first captures any volatile data that would be lost when computer is turned off - and then moves data to a secure location

- Any digital data copied should be done at the **bit level**, which means **bypassing the operating system** and using special software to extract the data off disks or from memory in raw format
 - Why should the O/S be bypassed?
 - Examples of such software?

Forensic Copy

- Bit-stream copy (bit-for-bit digital copy) of the digital original (why not just copy the files, directories?)
- Make several such copies
- Note – it is possible for a drive to be bit imaged without anyone viewing its contents so privacy or confidentiality issues are not at risk – important in court
- What are examples of these specialized software?
- Create data signature of the copy – (of each copy? why?)
 - Use cryptographic hash verification to ensure integrity of the image (SHA-1 and MD5 – message digest 5)
 - Even if one bit is altered the resulting hash will be different
 - Hashing is a way to ensure that it cannot be reverse engineering to reveal anything about the data except that it has changed

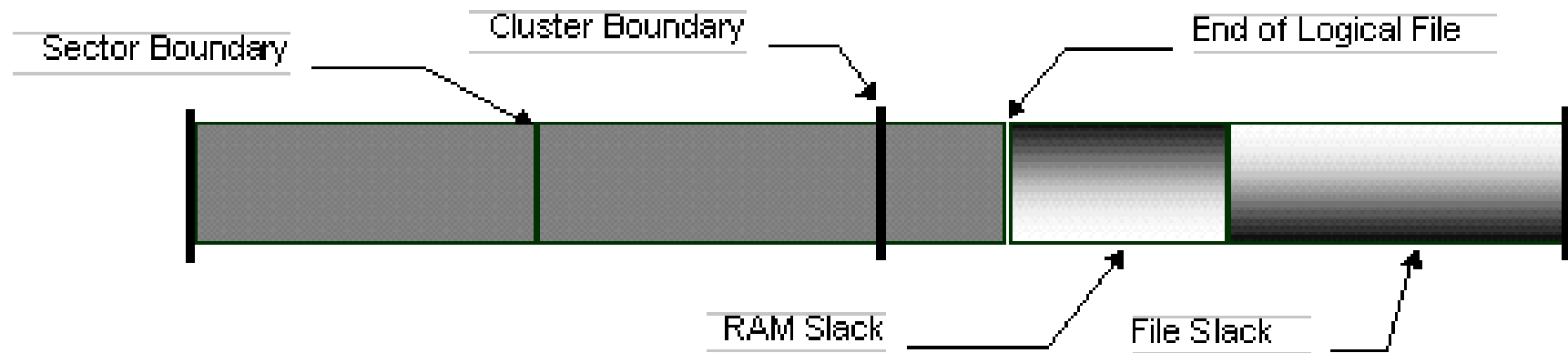
Forensic Copy

- Drive Imaging: captures a snapshot of everything on the drive
 - Mirror Image
 - Noninvasive method of capturing or copying all data on a drive
 - Sector-by-sector image or bit-by-bit stream image
 - Method by which every bit is copied from beginning to the end of the drive without modifying the contents or characteristic of the drive (including file slack and ram slack)

- Residual Data
 - Data that has been deleted but not 'erased'
 - May be found in unallocated storage or file slack space

- Slack
 - extra space from the end of the file to the end of the cluster
 - it exists when the size of the file is less than the size of the cluster
 - (in MS, clusters consist of sectors, each of which are 512 bytes – the smallest individually addressable physical unit of information used by a computer)

RAM Slack & File Slack



RAM Slack

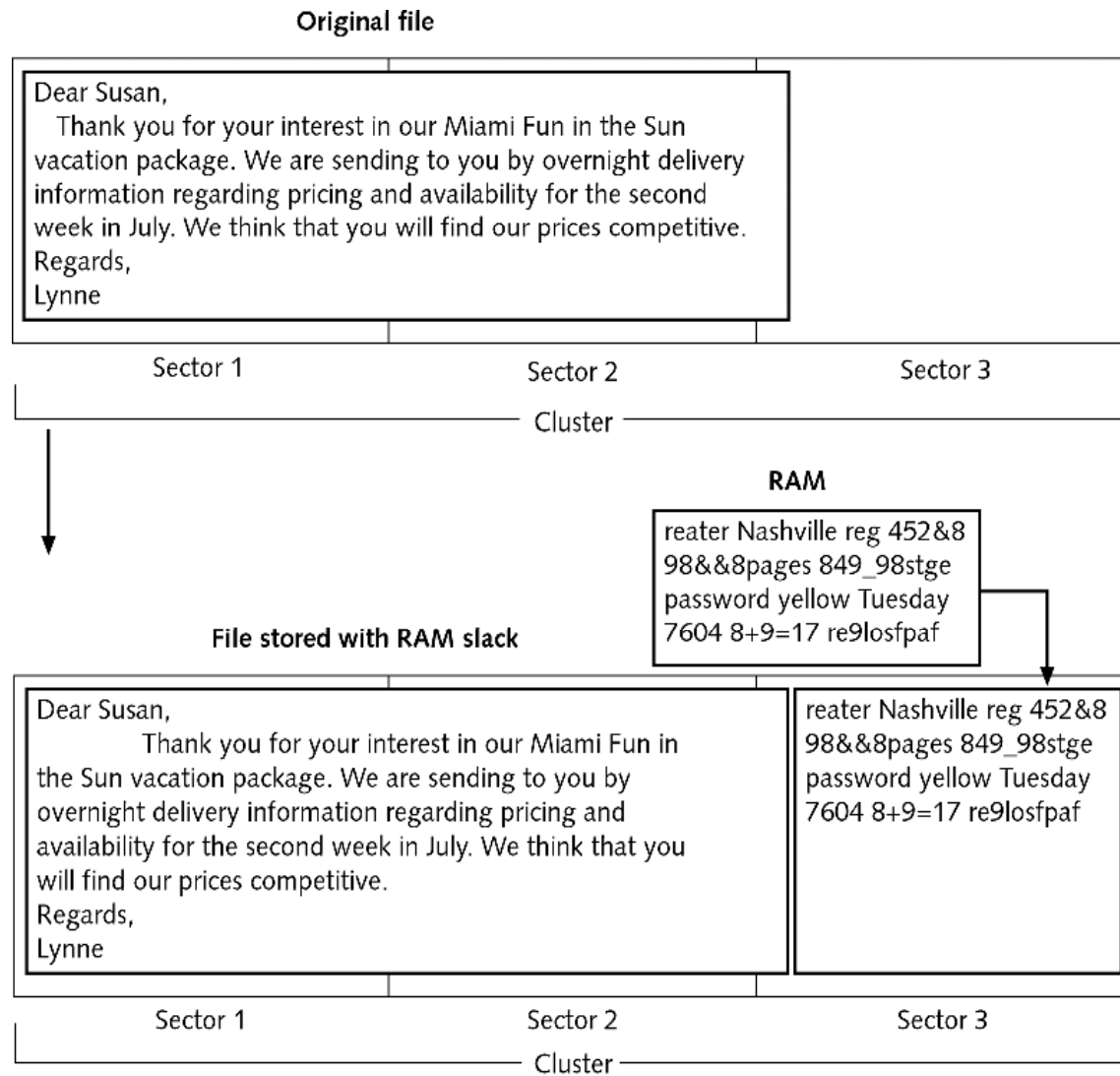
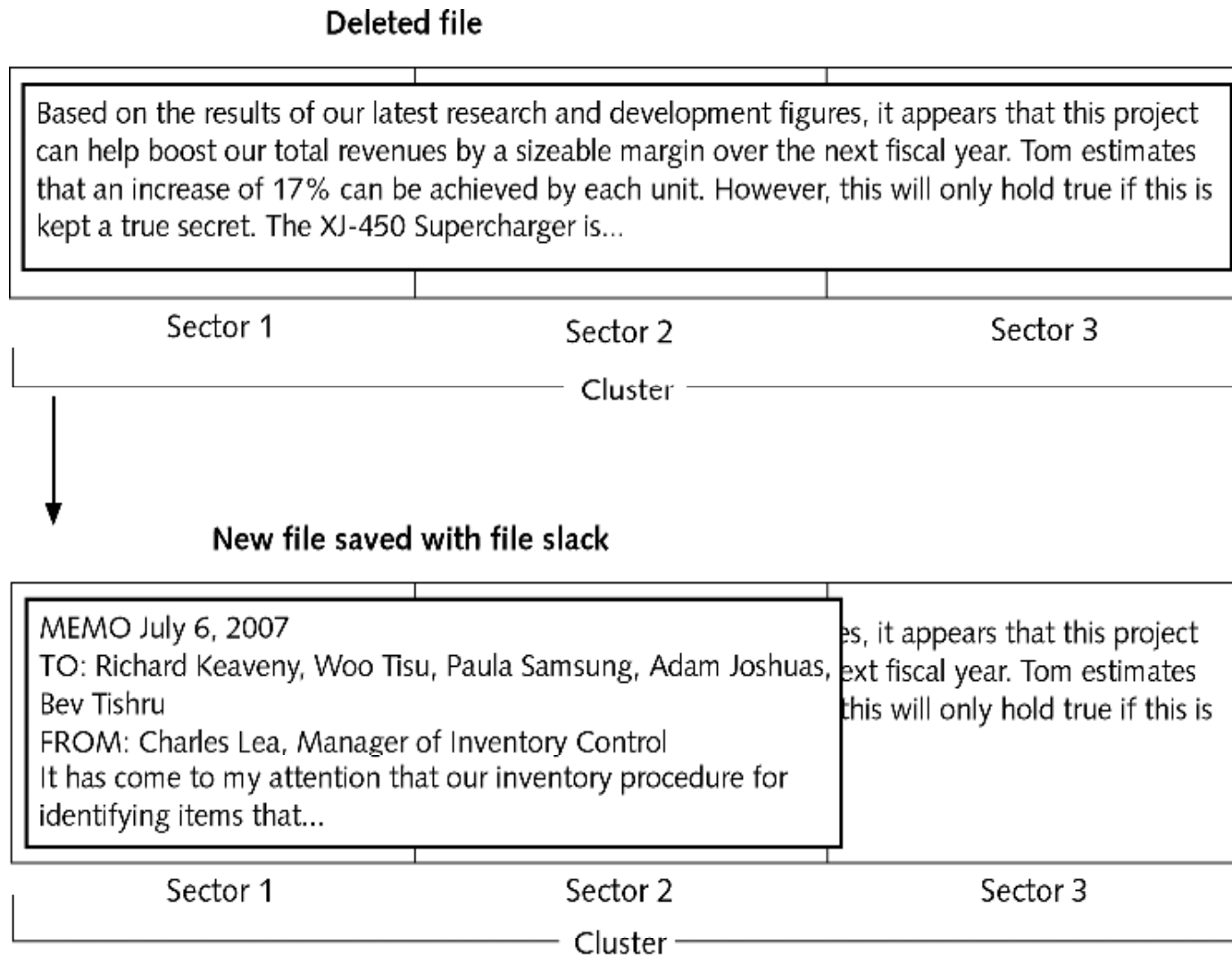


Figure 13-3 RAM slack

File Slack



■ *File slack*: space that remains if a file does not take up an entire sector

Figure 13-4 File slack

Forensic Tools and Toolkits

- EnCase® Forensic Version 5
 - A DOD-approved tool for gathering and evaluating electronic information
 - Supports the following e-mail investigation file types:
 - MSN Hotmail
 - Outlook and Outlook Express
 - Yahoo! and other web mail

Forensic Tools and Toolkits

- Other toolkits for Windows:
 - Forensic Toolkit® (FTK™)—used for finding and examining computer evidence
 - Ultimate Toolkit™—contains FTK plus other modules for recovering passwords, analyzing registry data, and gleaning hard drives
 - WinHex—used for forensics, data recovery and processing, and IT security

Forensic Tools and Toolkits

- Toolkits for UNIX and Linux:
 - Autopsy and Sleuth Kit—for investigating file systems and volumes of suspect computers
 - dtSearch—for combing through large amounts of data for up to 250 different file types

Forensic Tools and Toolkits

- Macintosh forensic software:
 - BlackBag—a set of 19 tools for examining Macintosh computers, including
 - Directory Scan
 - FileSpy
 - HeaderBuilder
 - MacQuisition—forensic acquisition tool used to safely image Macintosh systems