

Guide to Computer Forensics and Investigations Sixth Edition

Chapter 9 Digital Forensics Analysis and Validation

Objectives

- Determine what data to analyze in a digital forensics investigation
- Explain tools used to validate data
- Explain common data-hiding techniques

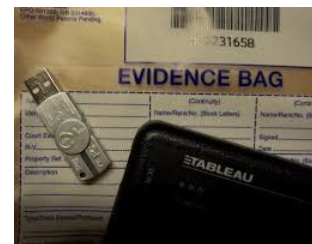


Determining What Data to Collect and Analyze

- Examining and analyzing digital evidence depend on the **nature of the investigation** And
 - the amount of data to process
 - Corporate investigators often locating and recovering a few specific items, such as emails, which simplifies and speeds processing
- **Scope creep** - when an investigation **expands beyond the original description**
 - Because of **unexpected evidence found**
 - Attorneys may ask investigators to examine other areas to recover more evidence
 - Increases the time and resources needed to extract, analyze, and present evidence
 - *Need to document additional time spend on recovering additional evidences!!*

Determining What Data to Collect and Analyze (Cont)

- **Scope creep** has become **more common**
 - Criminal investigations require more detailed examination of evidence just before trial
 - To help prosecutors fend off attacks from defense attorneys
- New evidence discovered often isn't revealed to prosecution
 - It's become more important for prosecution teams to ensure they have analyzed the evidence **exhaustively** before trial



Approaching Digital Forensics Cases

- Begin a case by creating an **investigation plan** that defines the:
 - Goal and scope of investigation
 - Materials needed
 - Tasks to perform
- The approach you take depends largely on the type of case you're investigating
 - **Corporate, civil, or criminal**
 - **Corporate case** tends to be easier due to easy access to evidence
 - **Criminal case** is more difficult because of scope. i.e need to contact ISP to gather evidence

Approaching Digital Forensics Cases (Cont)

- Follow these basic steps for all digital forensics investigations:
 - 1. For target drives, use recently wiped media that have been reformatted and inspected for viruses
 - 2. Inventory the hardware on the suspect's computer, and note condition of seized computer
 - 3. For static acquisitions, remove original drive and check the date and time values in system's CMOS
 - 4. Record how you acquired data from the suspect drive



Approaching Digital Forensics Cases (Cont)

- Follow these basic steps for all digital forensics investigations:
 - 5. Process drive's contents **methodically and logically**. *i.e* *emails → JPG → spreadsheet → word*
 - 6. **List all folders and files** on the image or drive. *Note where a file/picture is found*
 - 7. **Examine contents of all data files** in all folders. *Starting from root directory*
 - 8. **Recover file contents for all password-protected files**. *Use password recovery tools*
 - 9. **Identify function of every executable file** (exe) that doesn't match **known hash values**. *If required run file to find out more*
 - 10. **Maintain control** of all evidence and findings



Approaching Digital Forensics Cases (Cont)

- Refining and Modifying the Investigation Plan
 - Even if initial plan is sound, at times you may need to deviate from it and follow evidence
 - Knowing the types of data to look for helps you make the best use of your time
 - The key is to start with a plan but remain flexible in the face of new evidence



Using OSForensics to Analyze Data

- OSForensics can perform forensics analysis on the following file systems:
 - Microsoft FAT12, FAT16, and FAT32
 - Microsoft NTFS
 - Mac HFS+ and HFSX
 - Linux Ext2fs, and Ext4fs
- OSForensics can analyze data from several sources
 - Including image files from other vendors



Using OSForensics to Analyze Data (Cont)

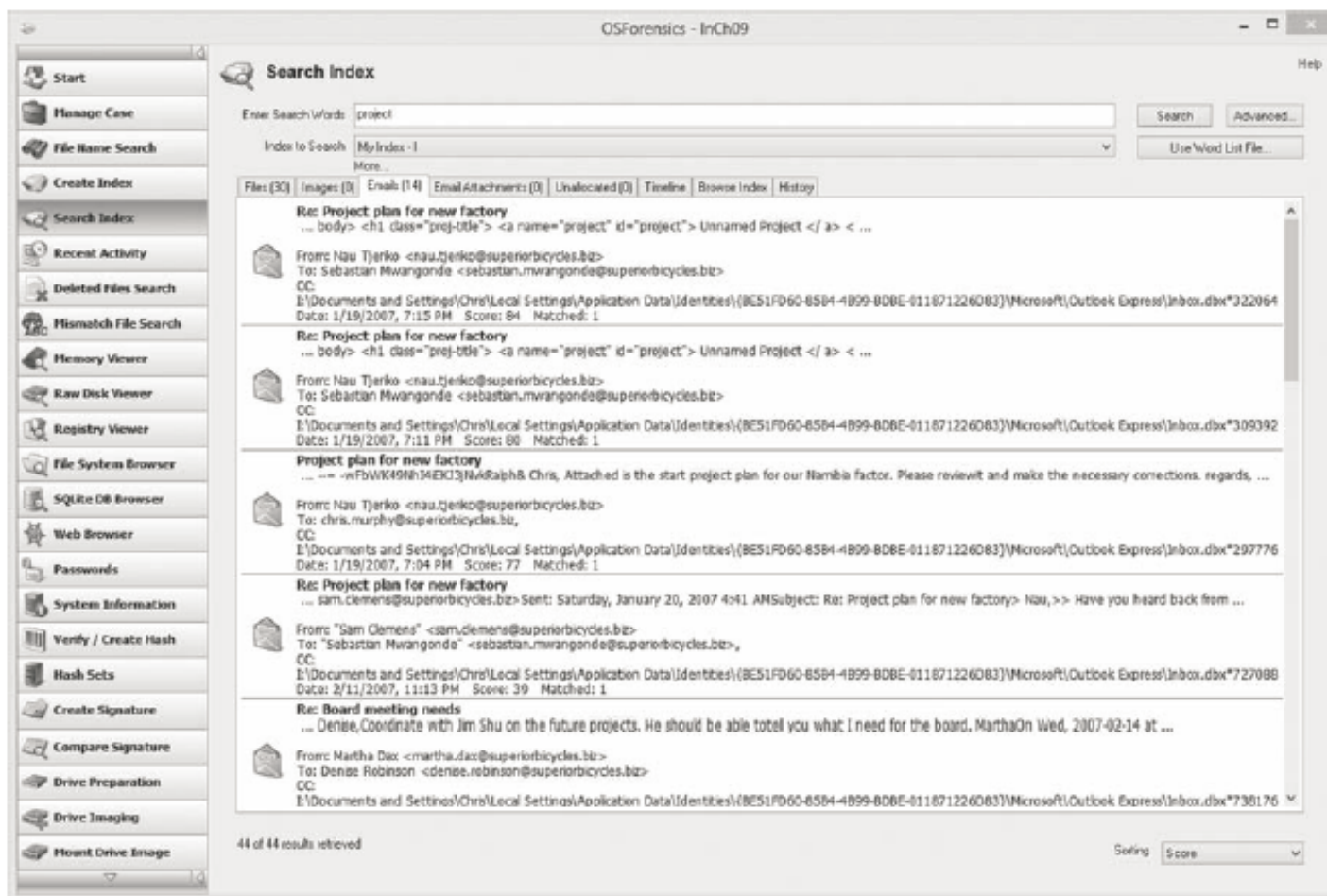
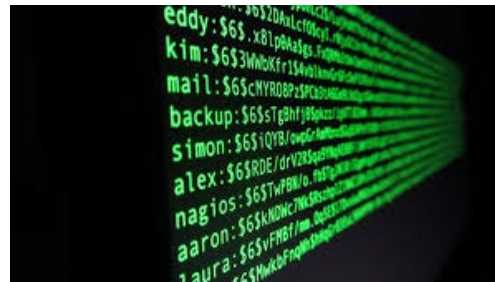


Figure 9-3 Entering a search term

Source: PassMark Software, www.osforensics.com

Validating Forensic Data

- Ensuring the integrity of data collected is essential for presenting evidence in court
- Most forensic tools offer **hashing** of image files
 - Example - when ProDiscover loads an image file:
 - It runs a hash and compares the value with the original hash calculated when the image was first acquired



Validating with Hexadecimal Editors

- *Some digital forensics tools may have some limitations in performing hashing, so using **advanced hexadecimal editors** is necessary to ensure data integrity.*
- Advanced hex editors offer features not available in digital forensics tools, such as:
 - Hashing specific files or sectors
- With the hash value in hand
 - You can use a forensics tool to search for a suspicious file that might have had its name changed to look like an innocuous file
- **WinHex** provides MD5 and SHA-1 hashing algorithms

Validating with Hexadecimal Editors

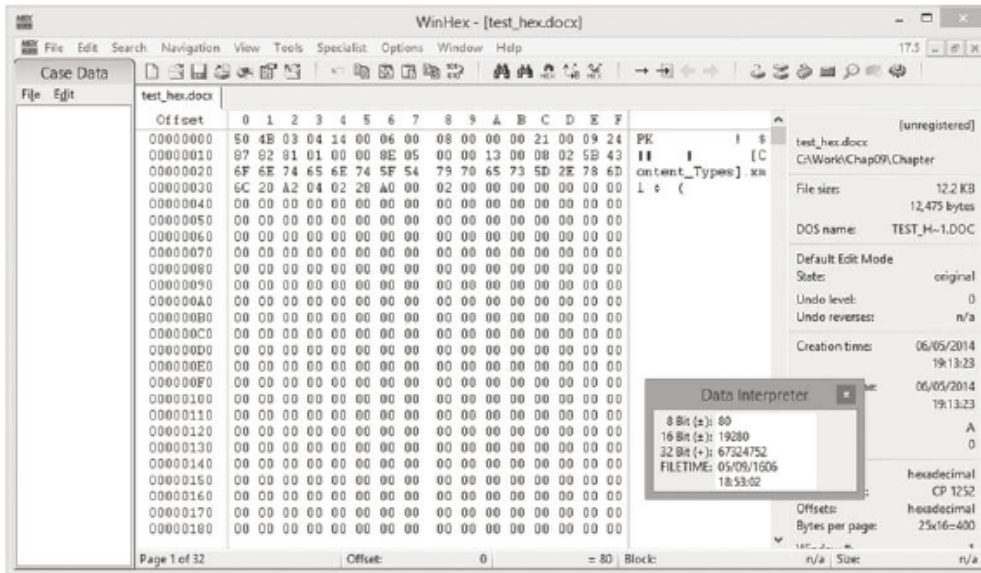


Figure 9-5 Viewing a file opened in WinHex
Courtesy of X-Ways AG, www.x-ways.net

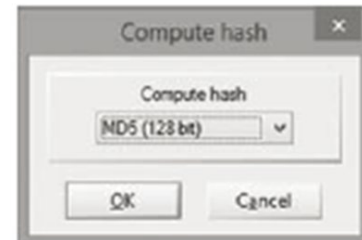


Figure 9-6 The Compute hash dialog box

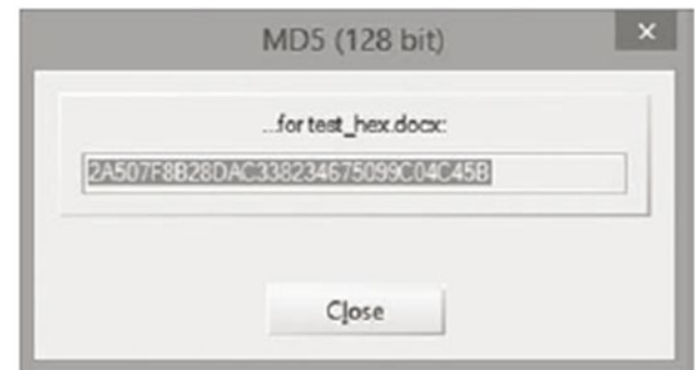


Figure 9-7 MD5 hash results
Courtesy of X-Ways AG, www.x-ways.net

Validating with Hexadecimal Editors (Cont)

- Using Hash Values to **Discriminate Data**
 - AccessData has its own **hashing database**, is known as **Known File Filter (KFF)**
 - KFF filters **known program files** from view and contains hash values of known illegal files
 - It compares known file hash values with files on your evidence drive to see if they contain suspicious data
 - Other digital forensics tools can import the **NSRL database** and run hash comparisons

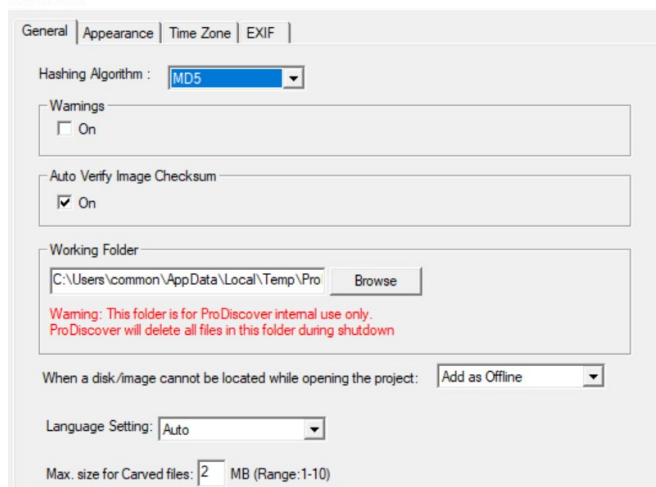
National Software Reference Library (NSRL)



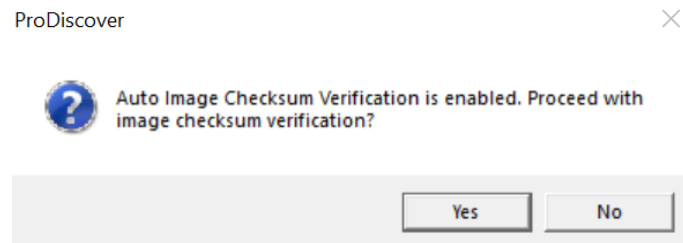
Validating with Digital Forensics Tools

- ProDiscover
 - .eve files contain metadata that includes hash value
 - Has a [preference](#) you can enable for using the [Auto Verify Image Checksum](#) feature when image files are loaded
 - If the Auto Verify Image Checksum and the hashes in the .eve file's metadata don't match
 - ProDiscover will notify that the acquisition is corrupt and can't be considered reliable evidence

Preferences

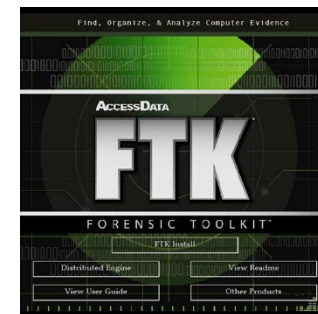
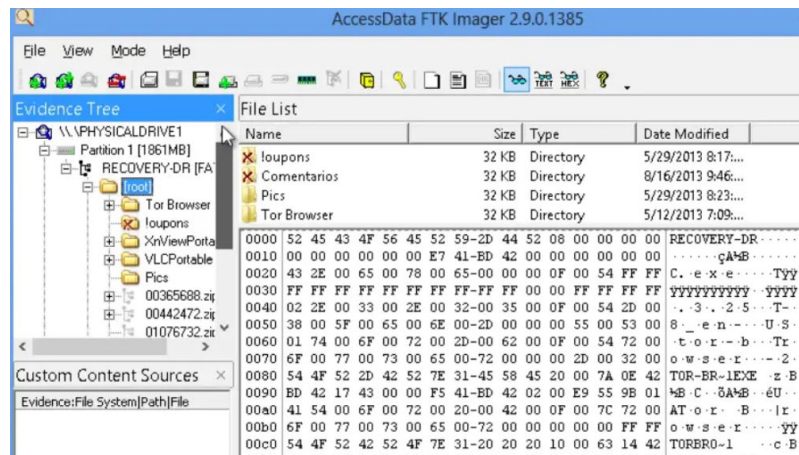


ProDiscover



Validating with Digital Forensics Tools (Cont)

- Raw format image files don't contain metadata
 - You must validate them manually to ensure integrity
- In **AccessData FTK Imager**, when selecting the Expert Witness (.e01) or SMART (.s01) format:
 - Additional options for validating the acquisition are available
 - Validation report lists MD5 and SHA-1 hash values



<https://forensicstore.com/>

Addressing Data-Hiding Techniques

- **Data hiding** - changing or manipulating a file to conceal information
- **Techniques:**
 - Hiding entire partitions
 - *Use Disk Management*
 - Changing file extensions
 - Setting file attributes to hidden
 - *Change file signature*
 - Bit-shifting
 - *Shift 1 bit to left*
 - Using encryption
 - Setting up password protection

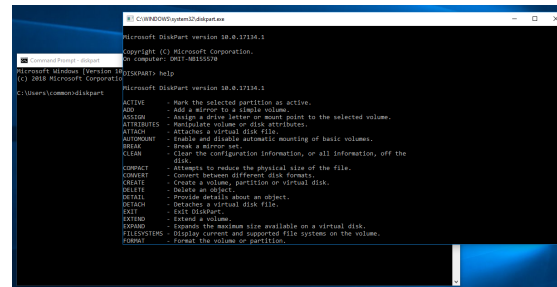


Hiding Files by Using the OS

- One of the first techniques to hide data:
 - Changing file extensions
- Advanced digital forensics tools **check file headers**
 - Compare the file extension to verify that it's correct
 - If there's a discrepancy, the tool flags the file as a **possible altered file**
- Another hiding technique
 - Selecting the **Hidden attribute** in a file's Properties dialog box (*windows*)

Hiding Partitions

- By using the Windows **diskpart** **remove letter** command
 - You can unassign the partition's letter, which hides it from view in File Explorer
- To unhide, use the **diskpart** **assign letter** command
- Other disk management tools:
 - Partition Magic, Partition Master, and Linux Grand Unified Bootloader (GRUB)



```
C:\Users\james> diskpart
Microsoft DiskPart version 10.0.17134.1
Copyright (c) Microsoft Corporation.
On computer: DELL-M815679

Microsoft DiskPart version 10.0.17134.1

ACTIVE          - Mark the selected partition as active.
AND             - Add a mirror to a clone volume.
ASSIGN          - Assign a drive letter or mount point to the selected volume.
ATTRIBUTES     - Manipulate volume or disk attributes.
ATTACH         - Attaches a virtual disk file.
AUTOMOUNT      - Enable and disable automatic mounting of basic volumes.
CLEAN           - Erase a drive or disk.
CLEANALL        - Clear the configuration information, or all information, off the
disk.
COMPACT         - Attempts to reduce the physical size of the file.
CONVERT        - Convert between different disk formats.
CREATE          - Create a volume, partition or virtual disk.
DELETE         - Delete an object.
DETACH         - Detaches a virtual disk file.
EXIT           - Exit DiskPart.
EXTEND         - Extend a volume.
FREE           - Shows the maximum size available on a virtual disk.
HELP           - Display current and supported file systems on the volume.
HELPFILE       - Shows the volume or partition.
```

Hiding Partitions (Cont)

- To detect whether a partition has been hidden
 - Account for all **disk space** when examining an evidence drive
 - Analyze any disk areas containing space you can't account for
- In ProDiscover, a hidden **partition appears as the highest available drive letter** set in the BIOS
 - Other forensics tools have their own methods of assigning drive letters to hidden partitions

Hiding Partitions (Cont)

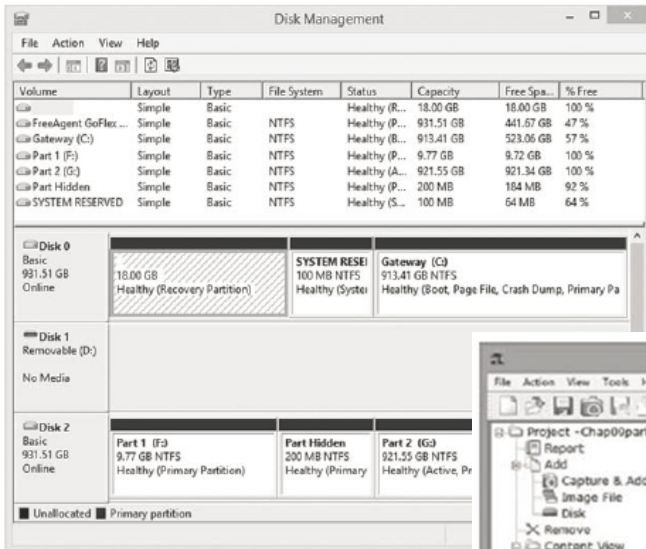


Figure 9-10 The Disk Management window
Courtesy of Microsoft Corporation

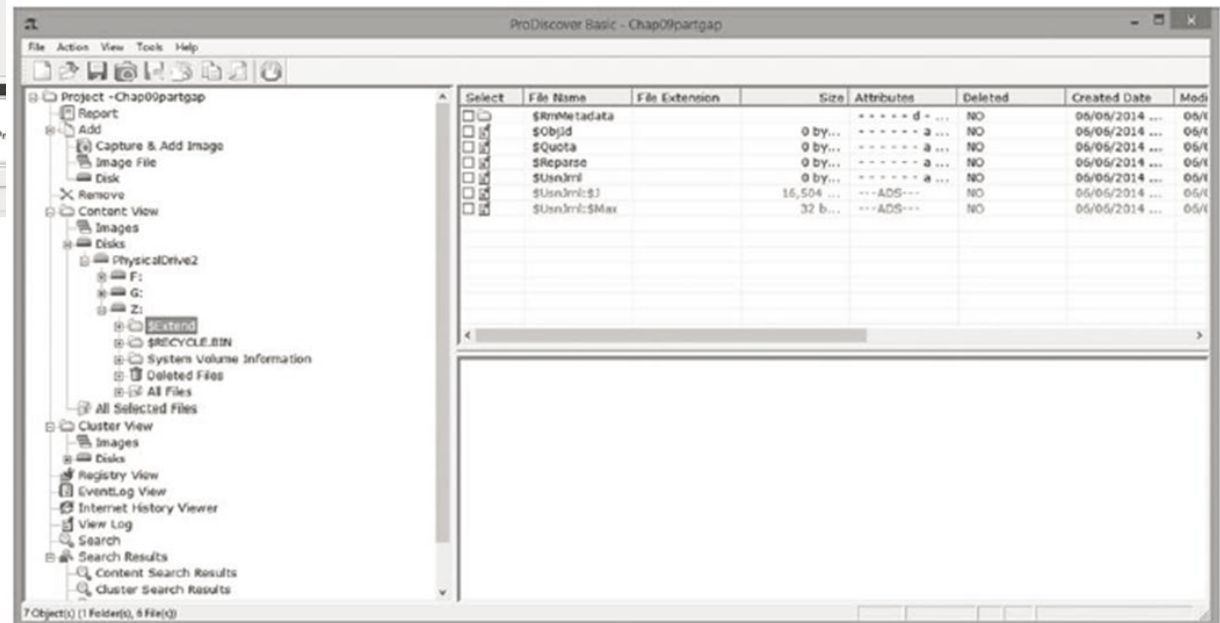
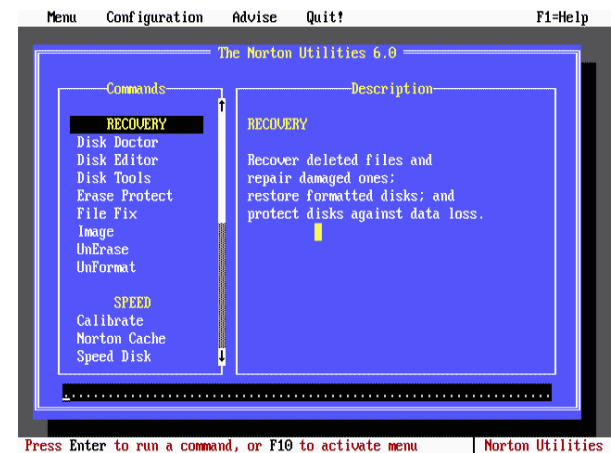


Figure 9-11 Viewing a hidden partition in ProDiscover
Courtesy of Technology Pathways, LLC

Marking Bad Clusters

- A data-hiding technique used in FAT file systems is placing sensitive or incriminating data in **free or slack space** on disk partition clusters
 - Involves using old utilities such as **Norton DiskEdit**
- Can mark good clusters as bad clusters in the FAT table so the OS considers them unusable
 - Only way they can be accessed from the OS is by changing them back to good clusters with a disk editor
- **DiskEdit** runs only in MS-DOS and can access only FAT-formatted disk media



Bit-Shifting

- Some users use a low-level encryption program that **changes the order of binary data**
 - Makes altered data unreadable To secure a file, users run an assembler program (also called a “macro”) to scramble bits
 - Run another program to restore the scrambled bits to their original order
- Bit shifting **changes data from readable code to data that looks like binary executable code**
- WinHex includes a feature for shifting bits

```
; A macro with two parameters  
; Implements the write system call  
%macro write_string 2  
    mov     eax, 4  
    mov     ebx, 1  
    mov     ecx, %1  
    mov     edx, %2  
    int     80h  
%endmacro
```

www.tutorialspoint.com

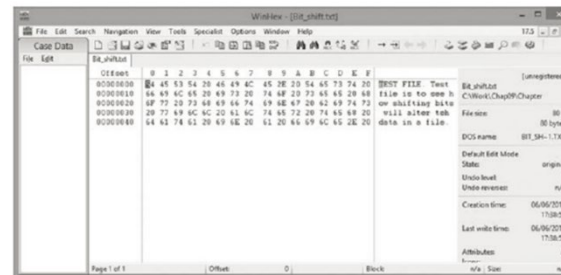


Figure 9-12 Bit_shift.txt open in WinHex
Courtesy of X-Ways AG, www.x-ways.net

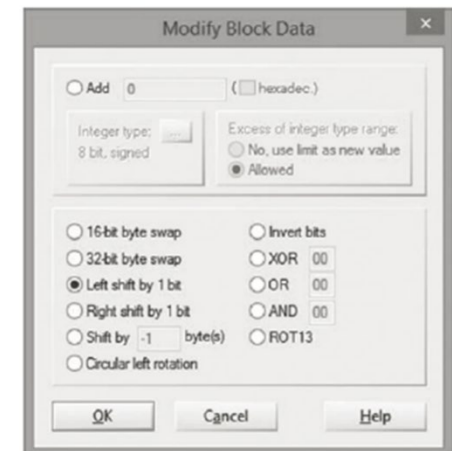


Figure 9-13 The Modify Block Data dialog box
Courtesy of X-Ways AG, www.x-ways.net

Understanding **Steganalysis** Methods

- **Steganography** - comes from the Greek word for “hidden writing”
 - Hiding messages in such a way that only the intended recipient knows the message is there
- **Steganalysis** - term for detecting and analyzing steganography files
- **Digital watermarking** - developed as a way to protect file ownership
 - Usually not visible when used for steganography

Understanding Steganalysis Methods (Cont)

- A way to hide data is to use **steganography tools**
 - Many are freeware or shareware
 - Insert information into a variety of files
- If you encrypt a plaintext file with PGP and insert the encrypted text into a steganography file
 - Cracking the encrypted message is extremely difficult!!!

Understanding Steganalysis Methods (Cont)

- Steganalysis methods
 - Stego-only attack
 - Only have *Converted covered file* to analyze
 - Known cover attack
 - Has both the Covered file and Converted covered file to analyze
 - Known message attack
 - When the hidden *message is revealed later*
 - Chosen stego attack
 - A steganography tool is used
 - Chosen message attack
 - The steganalyst generates a stego-object from some steganography tool or algorithm of a chosen message.

Examining Encrypted Files

- To decode an encrypted file
 - Users supply a **password or passphrase**.
Not easy to crack if without password or passphrase...
- Many encryption programs use a technology called “**key escrow**”
 - Designed to recover encrypted data if users forget their passphrases or if the user key is corrupted after a system failure
- Key sizes of **2048 bits to 4096 bits** make **breaking them nearly impossible** with current technology
- *If do encounter encrypted data in an investigation, make an effort to persuade the suspect to reveal the encryption passphrase.*



Recovering Passwords

- Password-cracking tools are available for handling password-protected data or systems
 - Some are integrated into digital forensics tools
- Stand-alone tools:
 - Last Bit
 - AccessData PRTK
 - ophcrack
 - John the Ripper
 - Passware



<https://www.lifewire.com>

Recovering Passwords (Cont)

- Brute-force attacks
 - Use every possible letter, number, and character found on a keyboard
 - This method can require a lot of time and processing power
- Dictionary attack
 - Uses common words found in the dictionary and tries them as passwords
 - Most use a variety of languages

Recovering Passwords (Cont)

- With many programs, you can **build profiles** of a suspect to help determine his or her password
 - *Names of relatives or pets, favorite colors, and schools attended. We tends to use thing we familiar with...*
- Many password-protected OSs and application store passwords in the form of MD5 or SHA hash values
- A brute-force attack requires converting a dictionary password from plaintext to a hash value
 - Requires additional CPU cycle time



Recovering Passwords (Cont)

- Rainbow table
 - A file containing the hash values for every possible password that can be generated from a computer's keyboard
 - No conversion necessary, so it is faster than a brute-force or dictionary attack
- Salting passwords
 - *Aim to make password cracking difficult*
 - Alters hash values *with additional bits added to password* and makes cracking passwords more difficult

Summary

- Examining and analyzing digital evidence depend on the nature of the investigation and the amount of data to process – *plan may need to be modified!*
- General procedures:
 - Wipe and prepare target drives, document all hardware components on the suspect's computer, check date and time values in the suspect's computer's CMOS, acquire data and document steps, list all folders and files, attempt to open password-protected files, determine function of executable files, and document steps

Summary (Cont)

- Advanced digital forensics tools have features such as indexing text data, making keyword searches faster – *to make your analysis easier*
- A critical aspect of digital forensics is validating digital evidence
 - ensuring the integrity of data you collect is essential for presenting evidence in court
- Data hiding involves changing or manipulating a file to conceal information

Summary (Cont)

- Three ways to recover passwords:
 - Dictionary attacks
 - Brute-force attacks
 - Rainbows tables



- Please read additional material “An Overview of Steganography.docx” in Lesson 6 folder.