3.2. Data Hiding Techniques

Data hiding involves changing or manipulating a file to conceal information. Datahiding techniques include hiding entire partitions, changing file extensions, setting file attributes to hidden, bit-shifting, using encryption, and setting up password protection.

Addressing Data-hiding Techniques

- File manipulation
  - Filenames and extensions
  - Hidden property
- Disk manipulation
  - Hidden partitions
  - Bad clusters
- Encryption
  - Bit shifting
  - Steganography

Hiding Partitions

- Delete references to a partition using a disk editor
  - Re-create links for accessing it
- Use disk-partitioning utilities
  - GDisk
  - PartitionMagic
  - System Commander
  - LILO
- Account for all disk space when analyzing a disk

Marking Bad Clusters

- Common with FAT systems
- Place sensitive information on free space
- Use a disk editor to mark space as a bad cluster

- To mark a good cluster as bad using Norton Disk Edit
  - Type B in the FAT entry corresponding to that cluster

Bit-shifting

- Old technique
- Shift bit patterns to alter byte values of data
- Make files look like binary executable code
- Tool
  - Hex Workshop

Using Steganography to Hide Data

- Greek for —hidden writing
- **Steganography** tools were created to protect copyrighted material
  - By inserting digital watermarks into a file
- Suspect can hide information on image or text document files
  - Most steganography programs can insert only small amounts of data into a file
- Very hard to spot without prior knowledge
- Tools: S-Tools, DPEnvelope, jpgx, and tte

Examining Encrypted Files

- Prevent unauthorized access
  - Employ a password or passphrase
- Recovering data is difficult without password

Key escrow

- Designed to recover encrypted data if users forget their passphrases or if the user key is corrupted after a system failure – Cracking password
- Expert and powerful computers
  - Persuade suspect to reveal password

Recovering Passwords

- Techniques
  - Dictionary attack

- Brute-force attack
- Password guessing based on suspect's profile

- **Tools**
  - AccessData PRTK
  - Advanced Password Recovery Software Toolkit
  - John the Ripper
- Using AccessData tools with passworded and encrypted files
  - AccessData offers a tool called ***Password Recovery Toolkit (PRTK)***
- Can create possible password lists from many sources
  - Can create your own custom dictionary based on facts in the case
  - Can create a suspect profile and use biographical information to generate likely passwords
- Using AccessData tools with passworded and encrypted files (continued)
- FTK can identify known encrypted files and those that seem to be encrypted and export them
  - You can then import these files into PRTK and attempt to crack them