Universiti Malaysia PAHANG
Engineering • Technology • Creativity

Computer Forensic & Investigation

Lab5: Hiding Data

Editors
Dr. Abdulghani Ali Ahmed
Wan Nurulsafawati Wan Manan
Faculty of Computer Systems & Software Engineering
abdulghani@ump.edu.my

Source: (Vacca et al., Computer Forensics Computer Crime Scene Investigation 2nd Edition, 2005).

This Week

- Computer Forensics Process
  - Identify
  - Secure
  - **Analyse**
  - Present

Source: (Vacca et al., Computer Forensics Computer Crime Scene Investigation 2nd Edition, 2005).

Analysis

- Software Tool Suites
  - Guidance Software Encase
  - Access Data Forensic Toolkit
  - ILook Investigator
    - only for law enforcement
- Should have a good Hex utility
  - WinHex
- Should use multiple tools to corroborate findings

Source: (Vacca et al., Computer Forensics Computer Crime Scene Investigation 2nd Edition, 2005).

Analysis

- Physical Analysis
  - Partition Table Analysis
  - Ambient data
    - areas on disk not accessible at logical or application level
    - file slack space
      - standard applications will not read past EOF marker
      - last sector of file may not be full
        - » sector slack
      - some sectors in cluster may not be used
        - » cluster slack
    - sectors marked as bad
    - system file areas
    - swap files

Source: (Vacca et al., Computer Forensics Computer Crime Scene Investigation 2nd Edition, 2005).

Analysis

- Logical analysis
  - file by file analysis
  - analysis at application level using the application used to create the file
  - more convenient and efficient than physical analysis
  - sometimes more effective
    - finds search strings split across sectors
    - provides high level semantic view of data

Source: (Vacca et al., Computer Forensics Computer Crime Scene Investigation 2nd Edition, 2005).

Analysis

- Deleted Files
  - deletion generally alters file name or deletes a directory or FAT or inode reference
  - data still present just not accessible through file name
  - unused disk sector address lists may be able to be reconstituted
    - could have been overwritten
  - if not a “physical” disk search for byte values of interest is needed
    - sector by sector, byte by byte

Source: (Vacca et al., Computer Forensics Computer Crime Scene Investigation 2nd Edition, 2005).

Analysis

- Hidden areas
  - residue from previously deleted files
  - result of deliberate attempts at hiding data
  - manipulation of disk configuration information e.g. partition table accuracy
  - disks can be configured with system areas not visible to applications
  - steganographic file systems

Source: (Vacca et al., Computer Forensics Computer Crime Scene Investigation 2nd Edition, 2005).

Analysis

- Data hiding techniques
  - using non-printable characters in directory and file names
  - using white font on white background of a document
  - embedding files in other files
  - changing file extensions
  - changing magic numbers
  - encrypted files
  - NTFS alternate data streams

Source: (Vacca et al., Computer Forensics Computer Crime Scene Investigation 2nd Edition, 2005).

Analysis

- File Signature Analysis
  - some file types have magic numbers
  - GIF = GIF8[79]a
  - tools can quickly verify if extension and magic number match
  - can search in ambient space for signatures

Source: (Vacca et al., Computer Forensics Computer Crime Scene Investigation 2nd Edition, 2005).

Analysis

- Hash databases
  - commonplace files have SHA1 hash recorded in hash database
  - produced by NIST/NSRL
  - these files can be safely excluded from further analysis
  - Hashkeeper
    - hash database of US DoJ National Drug Intelligence Center
  - Known File Filters (KFF)
    - import hash sets
    - create custom hash sets (trojans, rootkits, pornographic images)

Source: (Vacca et al., Computer Forensics Computer Crime Scene Investigation 2nd Edition, 2005).

Analysis

- Analysis Summary
  - Start documentation
  - Identify and verify what is acquired
    - if a disk, check geometry vs manufacturer's specification
    - Partitions, folders, files, systems files, logs, etc
  - Identify key search items – keywords, file types etc

Source: (Vacca et al., Computer Forensics Computer Crime Scene Investigation 2nd Edition, 2005).

Analysis

- Profile the acquired image and its files
  - Signature matching
  - KFF to identify known ‘OK’ files, and known ‘not OK’ files
  - MAC time-lining
  - Hidden files
  - File authorship
  - File size (both physical and logical)
- Search all space (incl. ambient space, deleted files) for
  - Keywords
  - File signatures
- Timelining
  - Prepare a time line of “facts” from contents of files, file times
- Prepare report

Source: (Vacca et al., Computer Forensics Computer Crime Scene Investigation 2nd Edition, 2005).

Analysis

- Unix/Linux Tools
  - xxd
    - provides a hex or ascii dump of a file (e.g., an image file) so it is searchable for hex or ascii sequences
  - grep
    - locates patterns in a file and outputs the line in which they are located
  - strings
    - prints out the readable characters from a file
    - will print out strings from a file that are at least four characters long (by default)
    - useful for looking at data files without the originating program, and searching executables for useful strings, etc.

Source: (Vacca et al., Computer Forensics Computer Crime Scene Investigation 2nd Edition, 2005).

Analysis

- Foremost
  - does data carving
    - extracts files from data file by looking for known headers and footers

Source: (Vacca et al., Computer Forensics Computer Crime Scene Investigation 2nd Edition, 2005).

Analysis

- Scalpel
  - open source file carving application
  - operates rapidly
    - runs quite efficiently on legacy systems
  - minimizes time searching for headers and footers
    - algorithm selection
    - indexes all headers and footers on first pass
    - footers with no matching headers are disregarded
    - disk broken into chunks
    - work queues for each chunk created for second pass
    - high performance OS techniques used to reduce amount of data movement
  - performs much better than Foremost

Source: (Vacca et al., Computer Forensics Computer Crime Scene Investigation 2nd Edition, 2005).

This Week

- Computer Forensics Process
  - Identify
  - Secure
  - Analyse
  - **Present**

Source: (Vacca et al., Computer Forensics Computer Crime Scene Investigation 2nd Edition, 2005).

Reporting

- Report preparation process
  - gather data
  - analyse results
  - outline and organize report
  - write a rough draft
  - revise the rough draft
- Document
  - why the analysis was done
  - how the analysis was done
  - what conclusions were reached

Source: (Vacca et al., Computer Forensics Computer Crime Scene Investigation 2nd Edition, 2005).

Reporting

- should achieve these goals
  - accurately describe details of case
  - be understandable
    - know your audience
  - withstand legal scrutiny
  - be unambiguous and not open to misinterpretation
  - be easily referenced
  - contain all information required to explain conclusions
  - offer valid conclusions, opinions, recommendations
  - be timely

Source: (Vacca et al., Computer Forensics Computer Crime Scene Investigation 2nd Edition, 2005).

Questions

?

Source: (Vacca et al., Computer Forensics Computer Crime Scene Investigation 2nd Edition, 2005).