Acquisition

- Acquisition, the first task in computer forensics investigations, is making a copy of the original drive.
- Physical data copy
- Logical data copy
- Data acquisition format
- Command-line acquisition
- GUI acquisition
- Remote acquisition
- Verification

.....

- Some computer forensics software suites, such asAccessData FTK and EnCase, provide separate tools for acquiring an image.
- However, some investigators opt to use hardware devices, such as the Logicube Talon, VOOM HardCopy 3, or ImageMASSter Solo III Forensic unit from Intelligent Computer Solutions, Inc., for acquiring an image.
- These hardware devices have their own built-in software for data acquisition.
- No other device or program is needed to make a

duplicate drive; however, you still need forensics software to analyze the data.

.....

- Two types of data-copying methods are used in software acquisitions:
- physical copying of the entire drive and
- logical copying of a disk partition.
- The situation dictates whether you make a physical or logical acquisition

.....

- All computer forensics acquisition tools have a method forverification of the data-copying process that compares theoriginal drive with the image.
- For example, EnCase prompts you to obtain the MD5 hash value of acquired data,
- FTK validates MD5 and SHA-1 hash sets during data acquisition, and Safe Back runs an SHA-256 hash while acquiring data.
- Hardware acquisition tools, such as Image MASSter Solo, can perform simultaneous MD5 and CRC-32 hashing during data acquisition.
- Whether you choose a software or hardware solution for your acquisition needs, make sure the tool has a hashing function for verification purposes.

Validation and Discrimination

- Two issues in dealing with computer evidence are critical.
- First is ensuring the integrity of data being copied—the validation process.
- Second is the discrimination of data, which involves sorting and searching through all investigation data.

- Many forensics software vendors offer threemethods for discriminating data values.

.....

- Hashing
- Filtering
- Analyzing file headers
- Validating data is done by obtaining hash values. This unique hexadecimal value for data,used to make sure the original data hasn’t changed.

……

- The primary purpose of data discrimination is to remove good data from suspicious data.
- Good data consists of known files, such as OS files and common programs (Microsoft Word, for example).
- The National Software Reference Library (NSRL) has compiled a list of known file hashes for a variety of OSs, applications, and images.

Extraction

- The extraction function is the recovery task in a computing investigation and is the most challenging of all tasks to master.
- Recovering data is the first step in analyzing an investigation's data.
- The following sub functions of extraction are used in investigations.
  - Data viewing
  - Keyword searching
  - Decompressing
  - Carving
  - Decrypting

- Bookmarking

- Many computer forensics tools include a data-viewing mechanism for digital evidence.
- Tools such as ProDiscover, X-Ways Forensics, FTK, EnCase, SMART, ILook, and others offer several ways to view data, including logical drive structures, such as folders and files.

.....

- A common task in computing investigations is searching for and recovering key data facts.
- Computer forensics programs have functions for searching for keywords of interest to the investigation.Using a keyword search speeds up the analysis processfor investigators.
- With some tools, you can set filters to select the file types to search, such as searching only PDF documents.
- Another function in some forensics tools is indexing allwords on a drive.
- X-Ways Forensics and FTK 1.6x and earlier offer this feature, using the binary index (Btree) search enginefrom dtSearch.