3.1. Validating Forensic Data

- One of the most critical aspects of computer forensics
- Ensuring the integrity of data you collect is essential for presenting evidence in court
- Most computer forensic tools provide automated hashing of image files
- Computer forensics tools have some limitations in performing hashing
  - Learning how to use advanced hexadecimal editors is necessary to ensure data integrity

Validating with Hexadecimal Editors

- Advanced hexadecimal editors offer many features not available in computer forensics tools
  - Such as hashing specific files or sectors
- Hex Workshop provides several hashing algorithms
  - Such as MD5 and SHA-1
  - See the following Figures
- Hex Workshop also generates the hash value of selected data sets in a file or sector

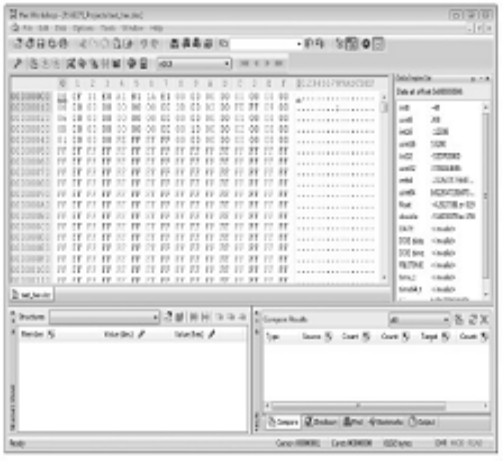

Fig: Viewing a file opened in Hex Workshop

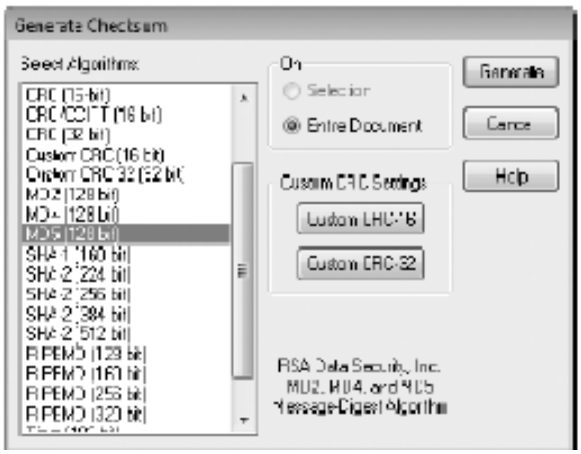

Fig: The Generate Checksum dialog box

- Using hash values to discriminate data
  - AccessData has a separate database, the **Known File Filter (KFF)**
- Filters known program files from view, such as MSWord.exe, and identifies known illegal files, such as child pornography
  - KFF compares known file hash values to files on your evidence drive or image files
  - Periodically, AccessData updates these known file hash values and posts an updated KFF

Validating with Computer Forensics Programs

- Commercial computer forensics programs have built-in validation features
- ProDiscover's .eve files contain metadata that includes the hash value
  - Validation is done automatically
- Raw format image files (.dd extension) don't contain metadata
  - So you must validate raw format image files manually to ensure the integrity of data
- In AccessData FTK Imager
  - When you select the Expert Witness (.e01) or the SMART (.s01) format
  - Additional options for validating the acquisition are displayed – Validation report lists MD5 and SHA-1 hash values