ManTech
International Corporation ®

CYBER SECTOR

Forensics Tools Panel

Jesse Kornblum
jesse.kornblum@mantech.com
http://jessekornblum.com/

Name a simple and reliable technique you use often in your cases

Biography

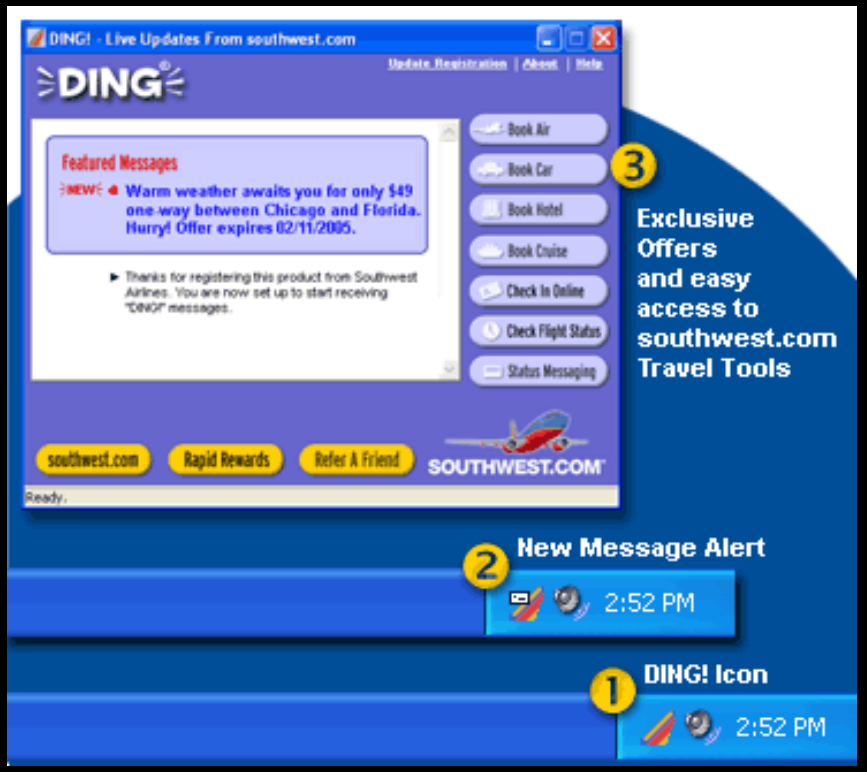
- AFOSI Computer Crime Investigator
- Instructor, U.S. Naval Academy
- ManTech Research and Development geek
- Authored:
  - foremost
  - md5deep and friends
  - hashdeep
  - ssdeep (fuzzy hashing)
  - Miss Identify
  - dc3dd

Searching in Foreign Languages

- Method of reverse engineering file formats
  - Find unique binary identifier
  - Search for binary string
  - Translate results in Chinese, Russian, etc
    - May need to copy and paste text into new window

Hypothetical Example

- DING! from Southwest Airlines
  - Displays promotional information, fare sales
  - Stores information on the user's preferences
    - Frequent flier number
    - Home city
    - Travel preferences



Hypothetical Example

- Searching for “DING! file format”
  - Course notes from college music class
  - Doorbell sound effects
  - Manual for GNU program ‘score’
  - Mr. Ding’s homepage
  - Question from Mr. Ding on Apache log rotation

Hypothetical Example

- Searching for “53 57 41 44 21”
  - Page from Chinese blogger about how DING! works
- Google Translator “slang”
  - Hacker = 黑客 = “Dark Visitor”
    - The visitor
    - The uninvited guest