

ManTech
International Corporation®

C Y B E R S E C T O R

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

The screenshot shows a web browser window titled "DING! - Live Updates From southwest.com". The interface features a "Featured Messages" section with a promotional offer: "Warm weather awaits you for only \$49 one-way between Chicago and Florida. Hurry! Offer expires 02/11/2005." Below this, a message states: "Thanks for registering this product from Southwest Airlines. You are now set up to start receiving 'DING!' messages." To the right of the main content is a vertical menu with buttons for "Book Air", "Book Car", "Book Hotel", "Book Cruise", "Check In Online", "Check Flight Status", and "Status Messaging". At the bottom of the page are buttons for "southwest.com", "Rapid Rewards", "Refer A Friend", and the "SOUTHWEST.COM" logo. Three numbered callouts are present: 1. "DING! Icon" pointing to a notification icon in the bottom right corner. 2. "New Message Alert" pointing to a notification bubble in the bottom right corner. 3. "Exclusive Offers and easy access to southwest.com Travel Tools" pointing to the right-hand menu.

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