Graphic File Carving Demonstration

Rick Ayers,
Jenise Reyes-Rodriquez

Disclaimer

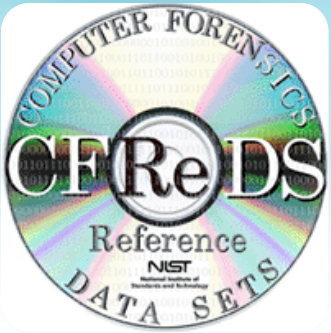
- Certain commercial entities, equipment, or materials may be identified in this presentation in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

CFTT at NIST

- CFTT – Computer Forensic Tool Testing Program provides a measure of assurance that the tools used in the investigations of computer-related crimes produce valid results.

iTL

NIST National Institute of Standards and Technology U.S. Department of Commerce



Disk Imaging

String Searching

Forensic Media Prep

COMPUTER FORENSICS TOOL CATALOG

File Carving

Write Blockers

Deleted File Recovery

Mobile Device Forensics

TEST SPECIFICATIONS

TEST ASSERTIONS AND TEST PLANS

SETUP DOCUMENTS

TEST REPORTS

FEDERATED TESTING

Benefits of CFTT

- Tool validation results issued by the CFTT project at NIST provide information necessary for:
  - Toolmakers to improve tools
  - Users to make informed choices about acquiring and using computer forensic tools
  - And for interested parties to understand the tools capabilities

File Carving vs Deleted File Recovery

File Carving

- Reconstruct deleted files from unallocated storage based on file content, **absence of file system meta-data**

Deleted File Recovery

- Reconstruct deleted files from unallocated storage **based on file system meta-data**

Test Cases: 1 & 2

- **No Padding - no fill**

Zero fill to end of last sector

- **Cluster Padded - basic**

cluster sized blocks of text between pictures

Tools Demonstration

- **Adroit v3.1d**
- **Recover My Files v5.2.1**
- **R-Studio v6.2**

Test Cases: 3 & 4

- **Fragmented in order**

A B A B A B

cluster sized blocks of text fragmenting pictures in order

- **Incomplete**

B C A C A B

cluster sized blocks of text between pictures with missing fragments

Test Cases: 5 & 6

- **Fragmented out of order**

B A C A B A C B

cluster sized blocks of text fragmenting pictures in disorder

- **Braided**

A1 B1 A2 B2

Test Cases: 7

- **Byte Shifted**

dd image starts here

Thank You

Rick Ayers
richard.ayers@nist.gov

Jenise Reyes-Rodriquez
jenise.reyes@nist.gov

Dr. James Lyle (Project Lead)
james.lyle@nist.gov

www.cftt.nist.gov