AAFS - February 19th, 2015

Graphic File Carving Tool Testing

Jenise Reyes-Rodriguez
National Institute of Standards and Technology

Disclaimer

Certain company products may be mentioned or identified. Such identification does not imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that these products are necessarily the best available for the purpose.

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

Outline

- Computer Forensic Tool Testing Program (CFTT)
- Why test carving tools?
- File Carving vs Deleted File Recovery
- Brainstorming before testing
- Testing Methodology
- Results Overview

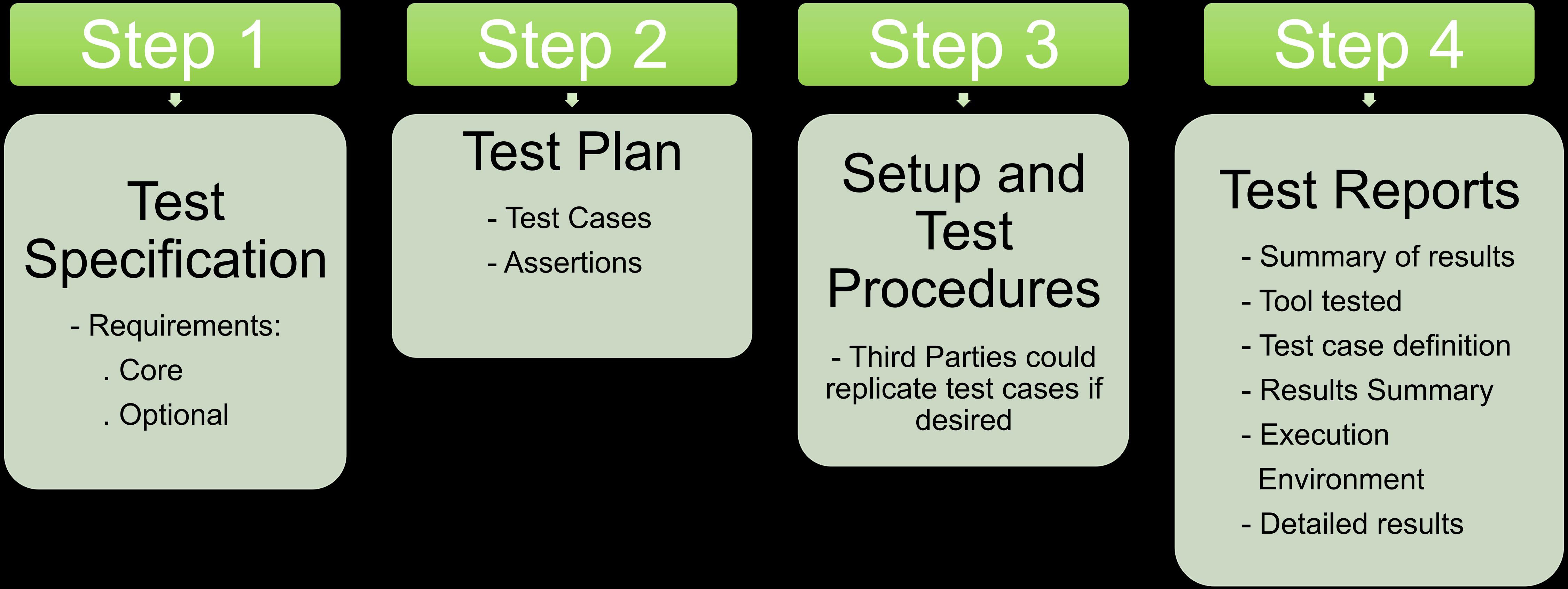
Computer Forensic Tool Testing Program (CFTT)

- Validate tools used in computer-based crime investigations

- Steering Committee

- Sponsors: Law Enforcement Standards Office, Department of Homeland Security, Federal Bureau of Investigations, National Institute of Justice, among other agencies

CFTT Methodology



Step 1

Test Specification

- Requirements:

. Core

. Optional

Step 2

Test Plan

- Test Cases

- Assertions

Step 3

Setup and Test Procedures

- Third Parties could replicate test cases if desired

Step 4

Test Reports

- Summary of results
- Tool tested
- Test case definition
- Results Summary
- Execution Environment
- Detailed results

Outline

- Computer Forensic Tool Testing Program (CFTT)
- Why test carving tools?
- File Carving vs Deleted File Recovery
- Brainstorming before testing
- Testing Methodology
- Results Overview

Why test file carving tools?

- To provide the law enforcement community valuable information so they can choose tools they can rely on.
- Help vendors to improve their tools
- Inform the users of the tools capabilities

Outline

- Computer Forensic Tool Testing Program (CFTT)
- Why test carving tools?
- File Carving vs Deleted File Recovery
- Brainstorming before testing
- Testing Methodology
- Results Overview

File Carving vs Deleted File Recovery

File Carving

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

Deleted File Recovery

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

Outline

- Computer Forensic Tool Testing Program (CFTT)
- Why test carving tools?
- File Carving vs Deleted File Recovery
- Brainstorming before testing
- Testing Methodology
- Results Overview

Carving graphic files: things to consider

- Multiple graphic file types – test them all?
- File type specifics
  - header and footer
  - thumbnails (embedded files)
  - header only
- Testing multiple tools

Carving graphic files: more to consider

- Tools support different parameters
  - Smart Carving
- File systems behavior

Our focus

- Default settings
- Completion of the files
- Fragmentation
- Thumbnails
- Files landing in/out sector boundary

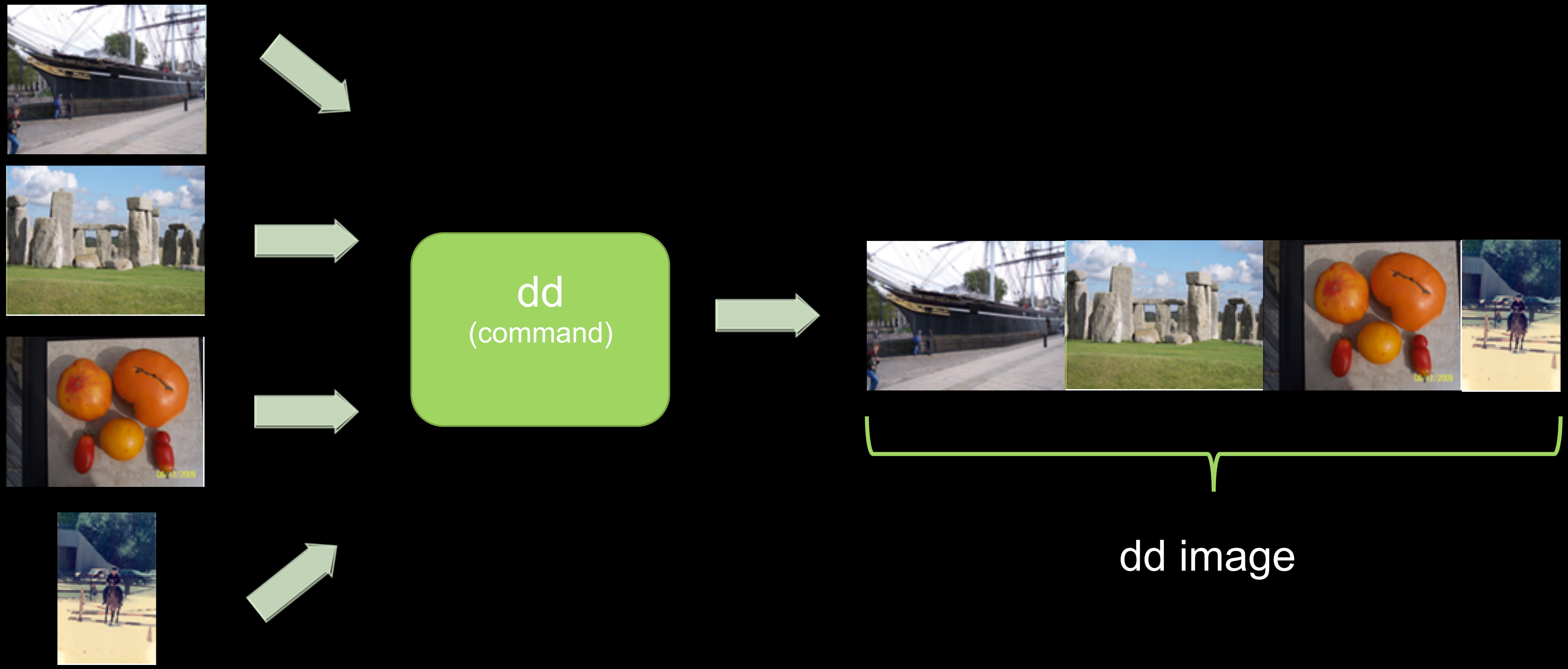
Outline

- Computer Forensic Tool Testing Program (CFTT)
- Why test carving tools?
- File Carving vs Deleted File Recovery
- Brainstorming before testing
- Testing Methodology
- Results Overview

Data Sets (Test Cases) Creation

- Graphic files selection – most common
- File types used:
  - .gif .bmp .png
  - .jpg .tiff
- 8 files of each type were selected
  - 7 thumbnails (.jpg)

Data Sets (Test Cases) Creation



dd
(command)

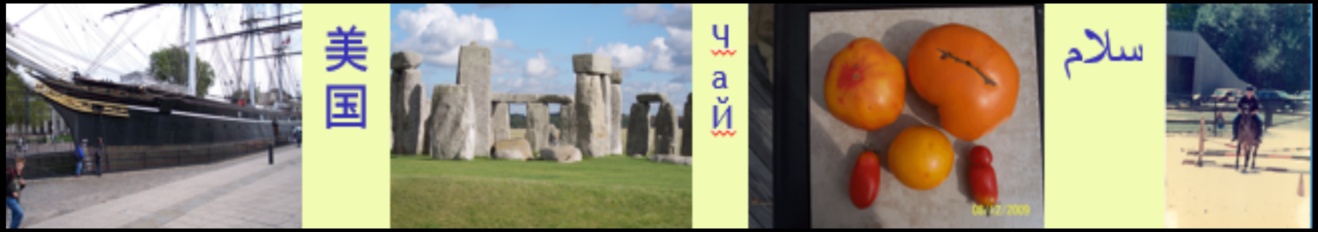
dd image

Test Cases: 1 & 2

- No Padding - no fill

Zero fill to end of last sector

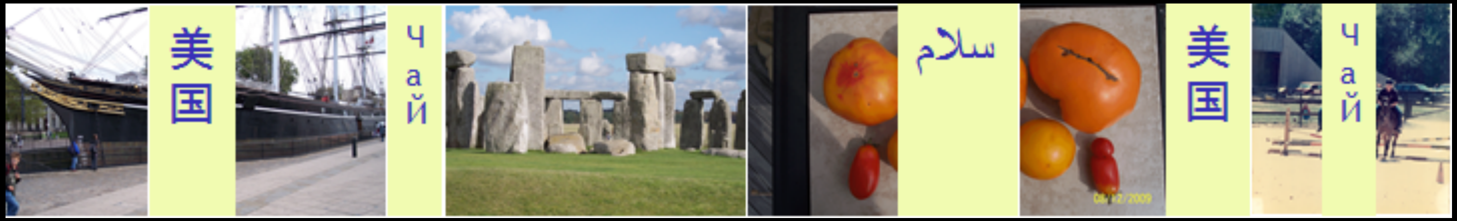
- Cluster Padded - basic



cluster sized blocks of text between pictures

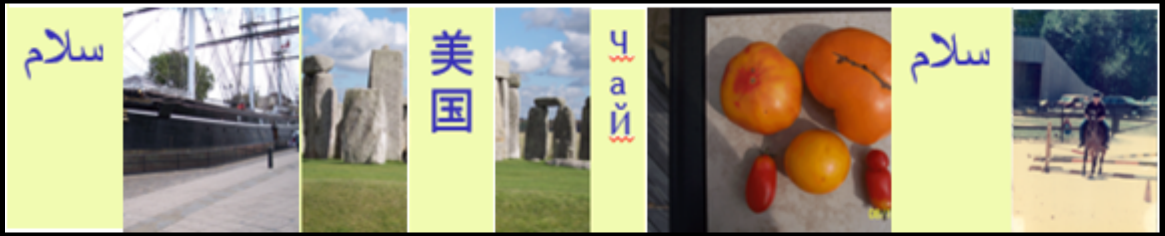
Test Cases: 3 & 4

- Fragmented in order



cluster sized blocks of text fragmenting pictures in order

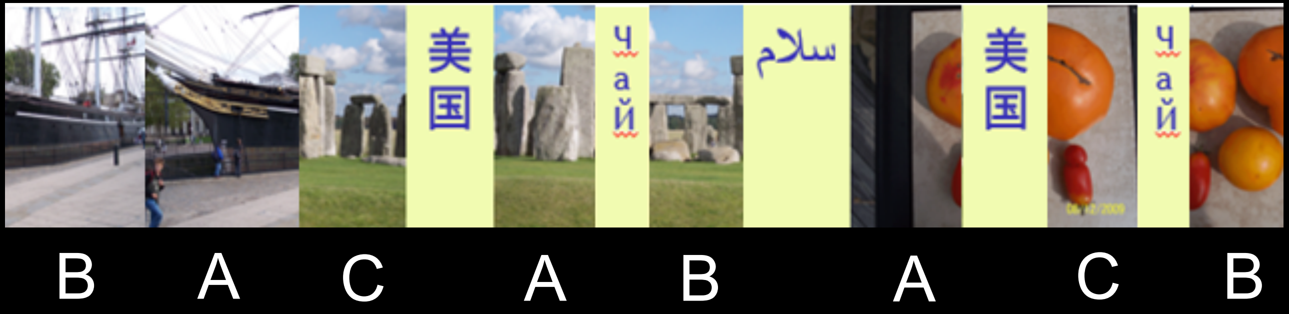
- Incomplete



cluster sized blocks of text between pictures with missing fragments

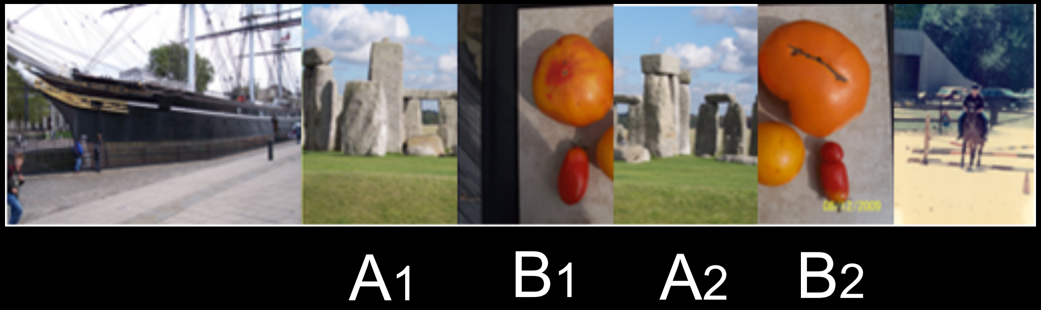
Test Cases: 5 & 6

- Fragmented out of order



cluster sized blocks of text fragmenting pictures in disorder

- Braided



Test Cases: 7

- Byte Shifted

dd image starts here

Tools Testing

- We had
  - 7 test cases
  - 11 tools to test

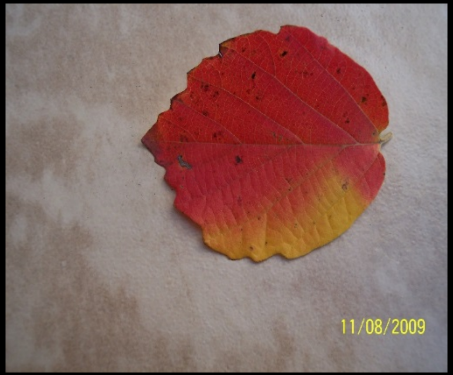
Measuring Methods

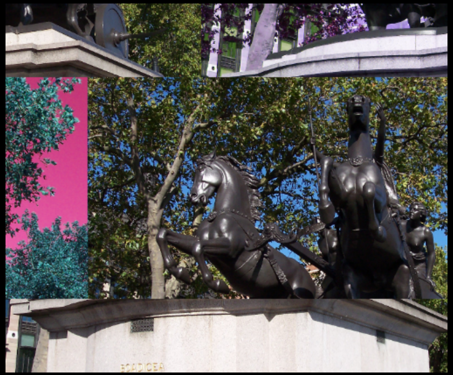
- Visibility of files carved
  - Is the data in a usable format? - viewable
- Data recovered analysis
  - Is the data a 100% match?

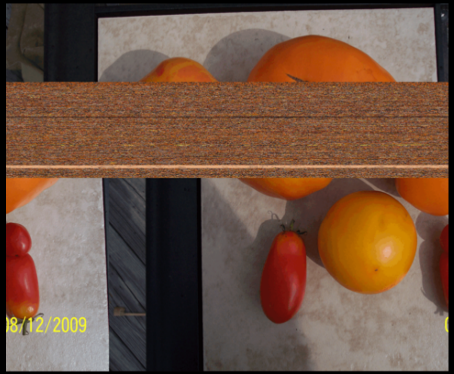
Visibility Categories and Definitions

❖ Viewable Complete – minor alteration

Files Recovered



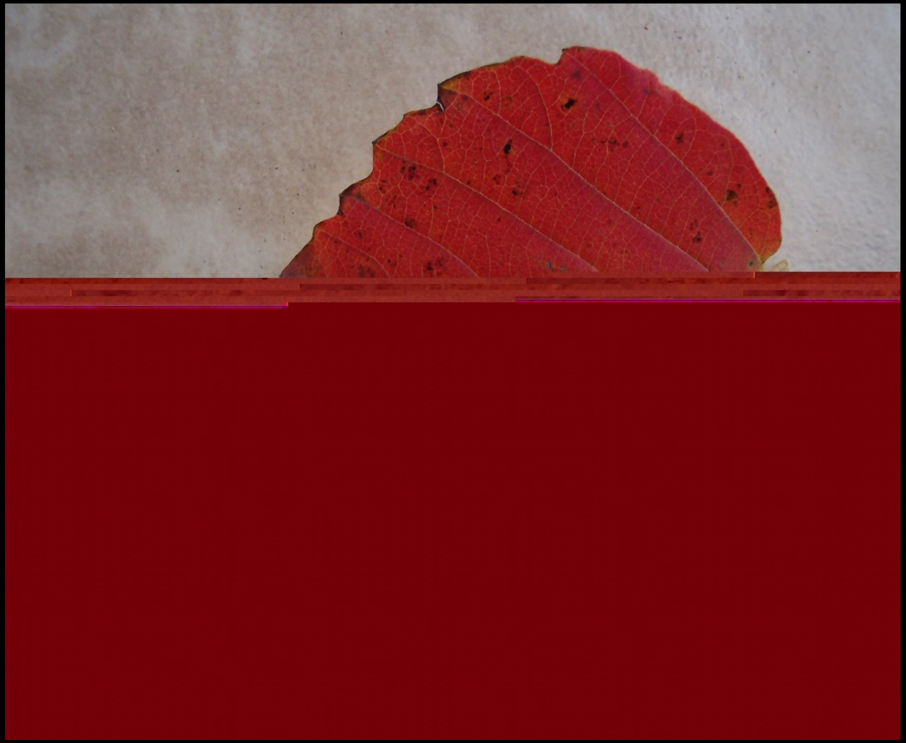




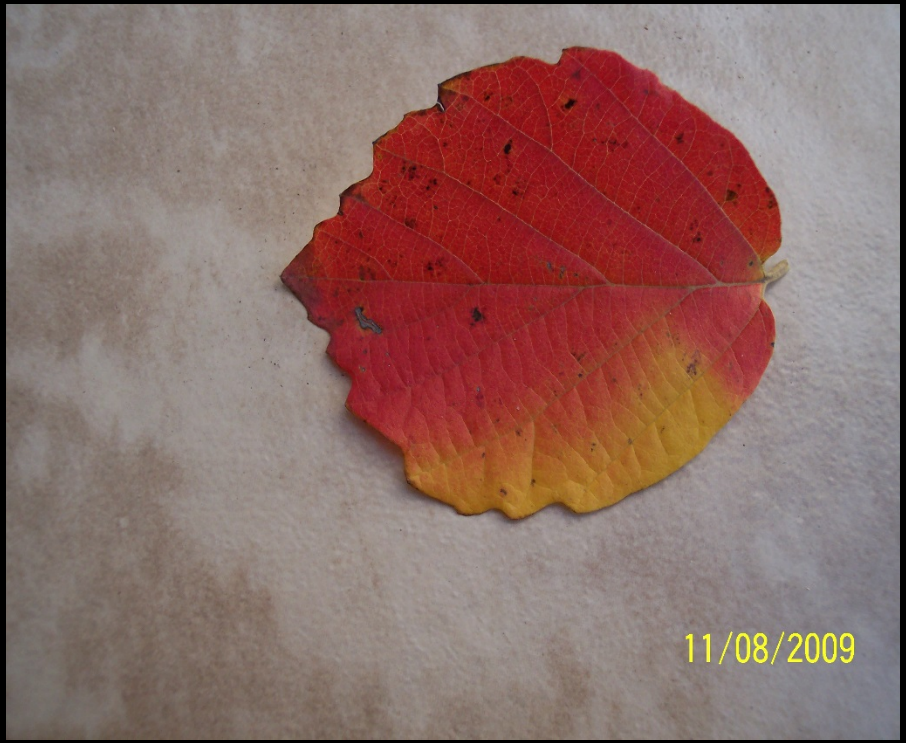
Original Files

Visibility Categories and Definitions

- Viewable Incomplete – major alteration



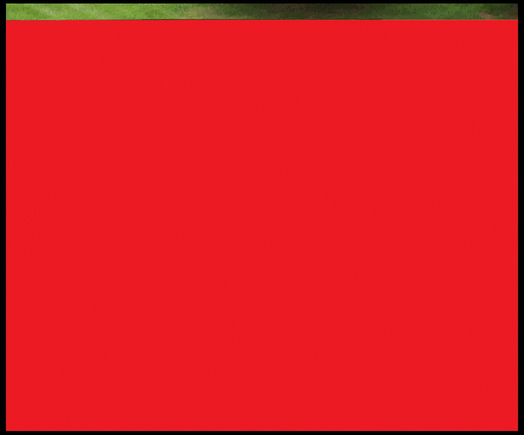
File Recovered



Original File

Visibility Categories and Definitions

- Not Viewable



File Recovered

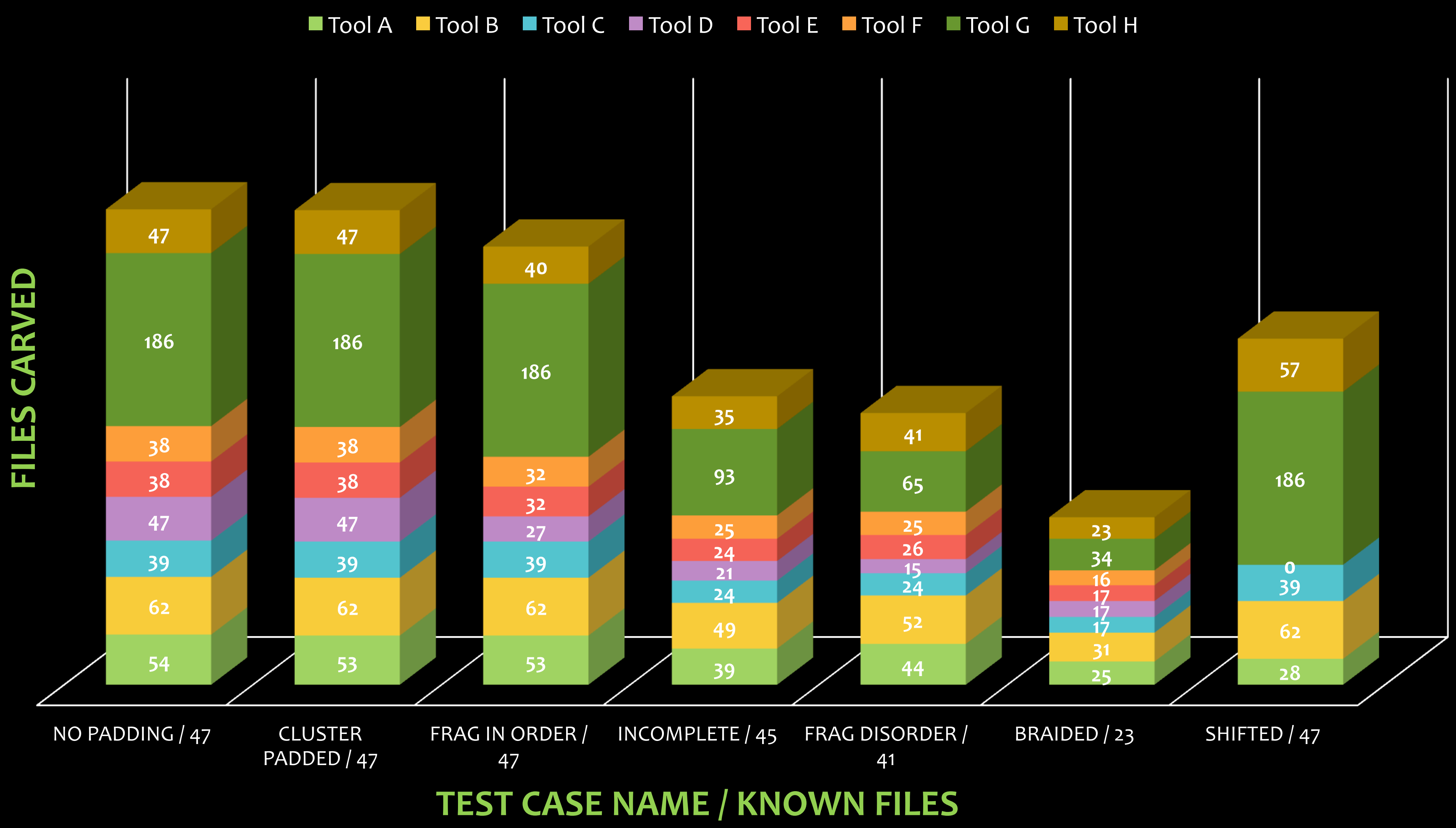
Original File

- False Positive

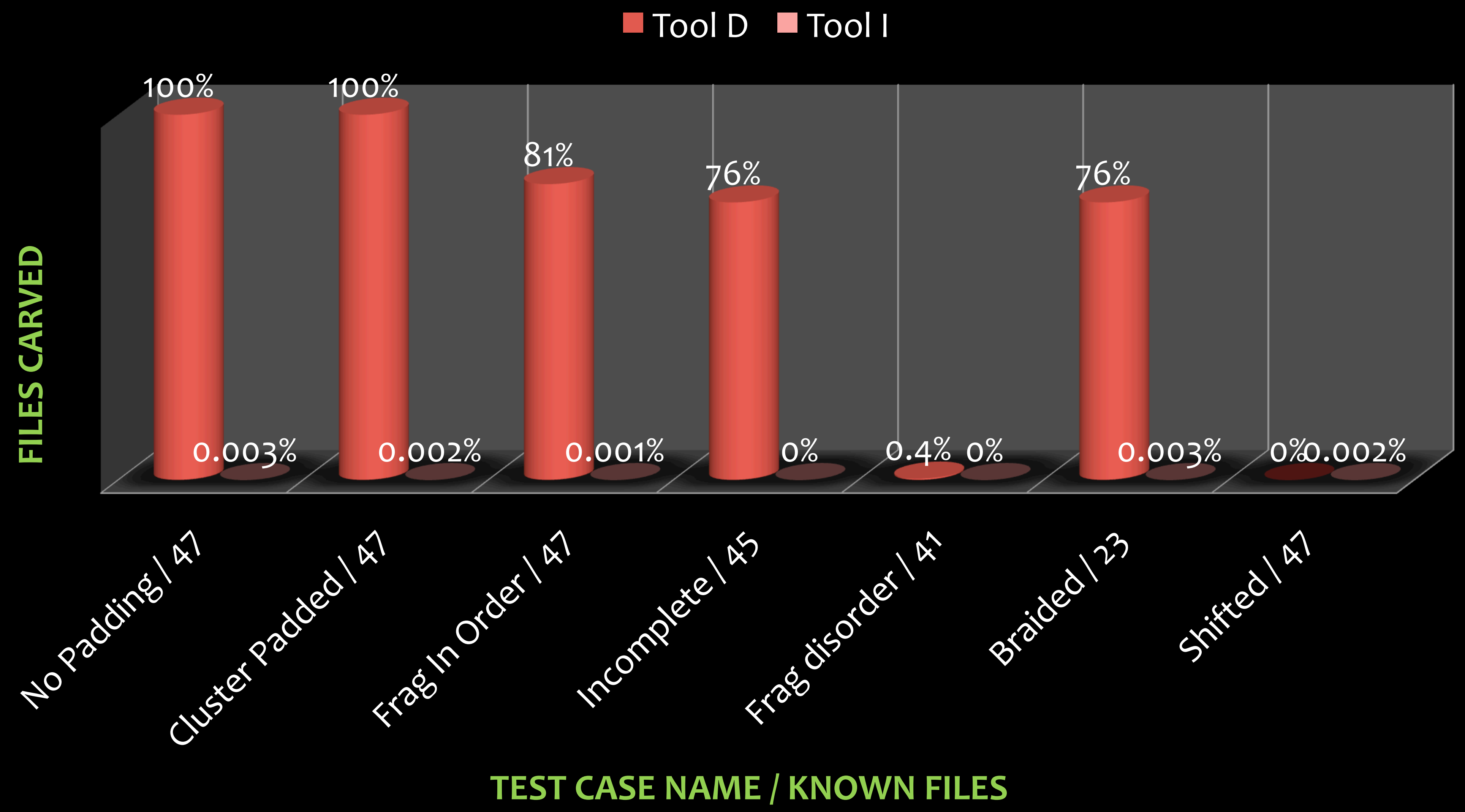
Outline

- Computer Forensic Tool Testing Program (CFTT)
- Why test carving tools?
- File Carving vs Deleted File Recovery
- Brainstorming before testing
- Testing Methodology
- Results Overview

Files Recovered per Tool



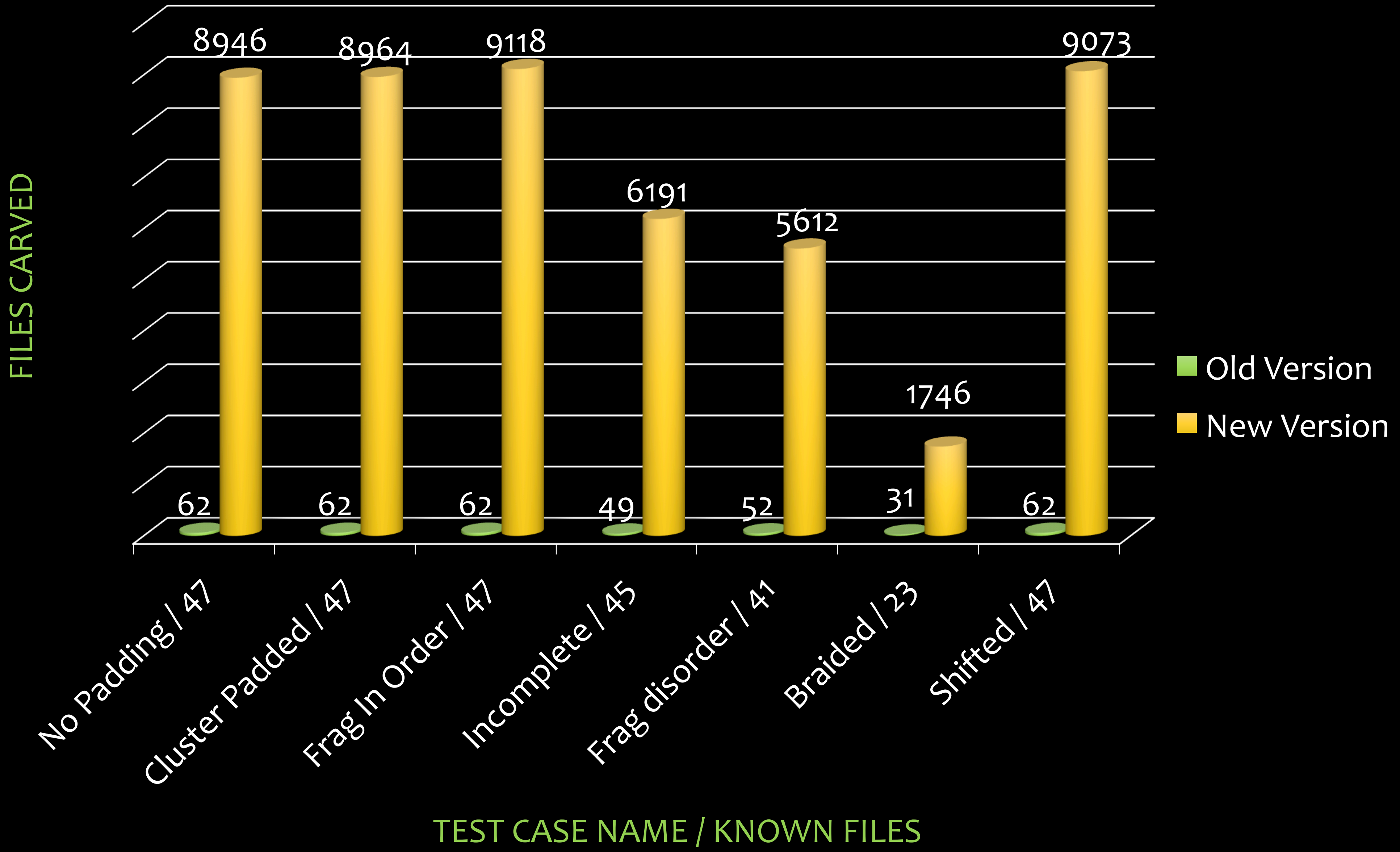
Percentage of usable data



Results Overview

- 10 reports published at http://www.cyberfetch.org/
- Interesting findings
  - multiple files but only one file is viewable
  - same tool, 2 different versions = close results?

Files recovered by same tool



Contacts

James Lyle (project leader)

james.lyle@nist.gov

Rick Ayers

richard.ayers@nist.gov

Jenise Reyes-Rodriguez

jenise.reyes@nist.gov

www.cftt.nist.gov

www.cfreds.nist.gov

http://www.cyberfetch.org/