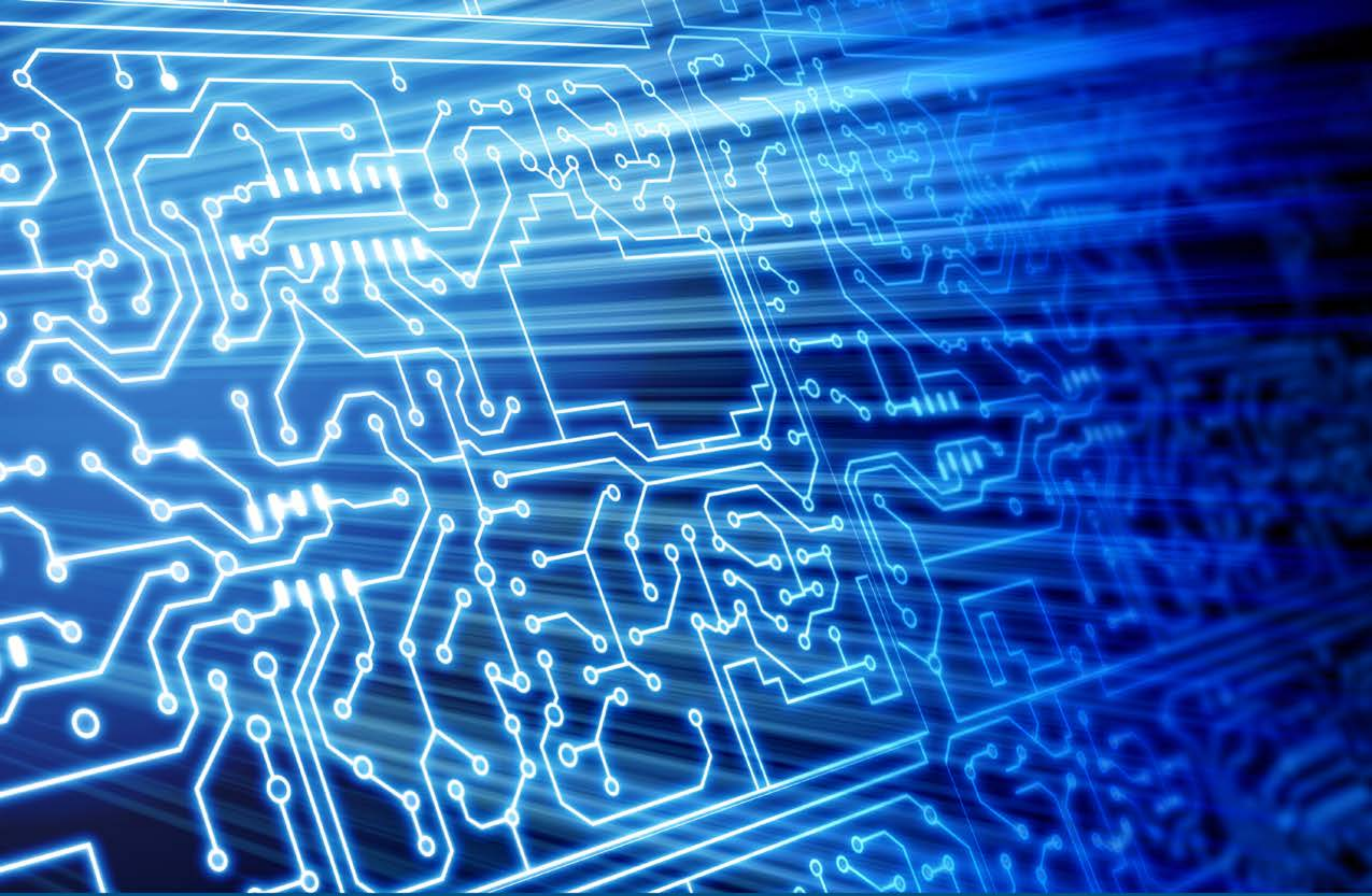

Adroit Photo Forensics 2013 v3.1d

Test Results for Graphic File Carving Tool

July 16, 2014

Homeland Security

Science and Technology

This report was prepared for the Department of Homeland Security Science and Technology Directorate Cyber Security Division by the Office of Law Enforcement Standards of the National Institute of Standards and Technology.

For additional information about the Cyber Security Division and ongoing projects, please visit www.cyber.st.dhs.gov.

July 2014

Test Results for Graphic File Carving Tool:
Adroit Photo Forensics 2013 v3.1d

Contents

Introduction

The Computer Forensics Tool Testing (CFTT) program is a joint project of the Department of Homeland Security (DHS), the National Institute of Justice (NIJ), and the National Institute of Standards and Technology Law Enforcement Standards Office (OLES) and Information Technology Laboratory (ITL). CFTT is supported by other organizations, including the Federal Bureau of Investigation, the U.S. Department of Defense Cyber Crime Center, U.S. Internal Revenue Service Criminal Investigation Division Electronic Crimes Program, and the U.S. Department of Homeland Security's Bureau of Immigration and Customs Enforcement, U.S. Customs and Border Protection and U.S. Secret Service. The objective of the CFTT program is to provide measurable assurance to practitioners, researchers, and other applicable users that the tools used in computer forensics investigations provide accurate results. Accomplishing this requires the development of specifications and test methods for computer forensics tools and subsequent testing of specific tools against those specifications.

Test results provide the information necessary for developers to improve tools, users to make informed choices, and the legal community and others to understand the tools' capabilities. The CFTT approach to testing computer forensics tools is based on well-recognized methodologies for conformance and quality testing. Interested parties in the computer forensics community can review and comment on the specifications and test methods posted on the CFTT Web site (http://www.cftt.nist.gov/).

This document reports the results from testing Adroit version 3.1d against raw disembodied "dd" images that contain various layouts of fragmentation and completeness. The "dd" images are available at the CFREDS Web site (http://www.cfreds.nist.gov).

Test results from other tools can be found on the DHS S&T-sponsored digital forensics web page, http://www.cyberfetch.org/.

How to Read This Report

This report is divided into five sections. Section 1 identifies and provides a summary of any significant anomalies observed in the test runs. This section is sufficient for most readers to assess the suitability of the tool for the intended use. Section 2 identifies the test cases that were selected. The test cases are selected, in general, based on features offered by the tool. Section 3 lists software used to run the test cases with links to additional information about the items used. Section 4 presents for each test case the expected result data used to measure the success of the test and the actual data reported by the tool. Section 5 presents relevant and recovered data results based on the data recovered and whether it is relevant to the carving effort. The data based on informational retrieval performance measures of precision and recall is presented for both test cases and for the individual file types carved. To download a zip file containing data returned for each test case for Adroit v3.1d runs, see http://www.cftt.nist.gov/CFTT-Test-Run-Raw-Files.html.

Test Results for Graphic File Carving Tool

Tool Tested:	Adroit Photo Forensics 2013
Software Version:	v3.1d
Supplier:	Digital Assembly
Address:	137 Varick Street, 2nd Floor New York, NY 10013
Tel:	(760) 483-3282
Email:	Support@digital-assembly.com
WWW:	http://digital-assembly.com

1 Results Summary

Adroit Photo Forensics 2013 recovers graphic files of various types utilizing proprietary SmartCarving™ and GuidedCarving™ technologies. Below are summaries on how Adroit v3.1d performed when carving raw disembodied “dd” images containing various layouts of fragmentation and completeness.

Adroit was mostly successful at carving bmp, png and jpg files in a viewable state. Generally, no more than 1 tiff or 2 gif files per test image were carved in a complete or viewable state with minor alteration. This anomaly has been fixed in version 3.2b. False positives occurred only for jpg files. This occurs when Adroit parses the raw “dd” image file and comes across the string “FF D8” within a file that is not a jpg.

For more test result details see section 4.

2 Test Case Selection

Adroit’s ability to carve gif, bmp, png, jpg, tiff graphics files was measured by analyzing carved graphics files from raw disembodied “dd” images (i.e., an image without a filesystem) that contain various layouts of fragmentation and completeness. The dd image layouts are:

- **No Padding:** contiguous files with no other content between files
- **Cluster Padded:** contiguous files with assorted content between files ranging in size from 1, 2, 4, 8, 16, …128 sectors
- **Fragmented In Order:** contiguous and sequential fragmented files with content separating the files
- **Incomplete:** contiguous and partial (i.e., only a portion of the file is present) files
- **Fragmented Out of Order:** contiguous and disordered fragmented files separated by other content

- **Braided Pair:** contiguous and intertwined fragmented files
- **Byte Shifted:** contiguous files that are not aligned to sector boundaries

3 Testing Environment

The tests were run in the NIST CFTT lab. This section describes the selected test execution environment, using the support software, and notes on other test hardware.

3.1 Execution Environment

Adroit version 3.1d was installed on Windows XP v5.1.2600. The configuration settings used for Adroit were the following:

- Best Recovery – Full Validation Option
- Identify active photos by header signature
- Scan every byte in a sector for photos
- Recover embedded photos in active files
- Recover embedded photos in carve files

3.2 Support Software

A package of programs to support test analysis, rel-8, was used. The software can be obtained from: http://www.cftt.nist.gov/filecarving/rel-8.zip.

3.3 Raw "dd" Image Creation

The scripts used to create the "dd" images used for testing can be obtained from: http://www.cftt.nist.gov/filecarving/mkdd.zip.

4 Test Results

The results in sections 4.1 – 4.7 identify the test image that was carved and the data (i.e., carved files) that were returned. Each test has an associated table that identifies the test, the total number of files carved and whether the carved files were *Viewable - Complete/minor alteration; Viewable – Incomplete/major alteration; Not Viewable* or a *False Positive.*

The *Total Carved* column reports the total number of files carved. This number is often higher than the number of files contained within the image. This is generally due to false positives. False positives often occur when a tool has carved a file based upon a known file signature (e.g., FF D8) string that is not a file header, but a string within another file.

The *Viewable – Complete/minor alteration* column describes carved files in which the picture appears to be unchanged from the original or the changes are so minor that the full content, color, and other attributes of the picture are maintained.

The *Viewable – Incomplete/major alteration* column include partial recoveries (i.e., only parts of the graphic are viewable), scrambled pictures in which the fragments are assembled incorrectly, color shifts and similar changes.

The *Not Viewable* column describes a file that is not viewable, could not be opened or had no content when opened.

Samples of viewable/complete and viewable/incomplete are available at http://www.cftt.nist.gov/filecarving.html.

The *False Positive* column reports a count of files that were incorrectly identified. The left-most column of the report tables provides a count for the individual file types that make up the test image.

The first row in in the tables reports the overall results for all files. Subsequent rows report results by file types (e.g., gif or jpg). The results are further divided based on the test case, e.g., by the amount of fragmentation or the presence of filler (i.e., other content). A bent arrow is used to show the breakdown.

Tables 8 and 9 at the end of the report provide results based on the data recovered and whether it is relevant to the carving effort. The data is presented for both test cases and for the individual file types carved. The tables are based on informational retrieval performance measures of precision and recall. These measurements report the completeness and relevance of the data produced by the tool. The two measures (i.e., precision and recall) are sometimes used together to provide a single measurement for a system known as an f-score.

For this report, the f-score is calculated based on the number of sectors returned within the individually carved files. This provides a different view of the data than the file information provided by each test case.

Full data on the test results including a complete analysis of sectors recovered is available at http://www.cftt.nist.gov/CFTT-Test-Run-Raw-Files.html.

4.1 No Padding

Graphic-nofill_1305121236.dd contains a total of 40 contiguous files with no other content between files.

Out of the 40 graphic files a total of 54 files were carved – 33 of the carved files were *Viewable – Complete.*

All 7 thumbnails were carved completely, displayed properly and were exact matches of the source files.

Of the remaining 21 carved files: 6 gif, 1 bmp, 7 tiff files were *Not Viewable*. The remaining 7 files were *False Positives.*

Summary: The tool was more successful at carving bmp, png and jpg file types than gif and tiff files. The unviewable bmp, on the table below, was the last graphic file on the "dd" image. The tool was unable to recover the last sector, which made the bmp file unviewable.

Test: No Padding	Total Carved	Viewable Complete/minor alteration	Viewable Incomplete/major alteration	Not Viewable	False Positive
40 files + 7 thumbnails	**54**	**33**		**14**	**7**
8 gif	**8**	**2**		**6**	
8 bmp	**8**	**7**		**1**	
8 png	**8**	**8**			
8 jpg	**15**	**8**			**7**
8 tiff	**8**	**1**		**7**	
7 thumbnails	**7**	**7**			
Full results are available at: **http://www.cftt.nist.gov/CFTT-Test-Run-Raw-Files.html**					

Table 1: No Padding

4.2 Cluster Padded

Graphic-basic_1305121231.dd contains a total of 40 contiguous graphic files (8 - gif, bmp, png, jpg, tiff) and 7 thumbnails for a total of 47 files to be carved. Assorted content ranging in size from 1, 2, 4, 8, …128 sectors separates the files.

Out of the 40 graphic files a total of 53 files were carved – 35 of the carved files were *Viewable - Complete*.

All 7 thumbnails were carved completely, displayed properly and were exact matches of the source files.

Of the remaining 18 carved files: 12 were *Not Viewable* and 6 were *False Positives*.

Summary: The presence of other data between the graphics did not significantly affect tool performance.

Test: Cluster Padded	Total Carved	Viewable Complete/minor alteration	Viewable Incomplete/major alteration	Not Viewable	False Positive
40 files + 7 thumbnails	**53**	**35**		**12**	**6**
8 gif	**8**	**2**		**6**	
2 No Fill	↳ *2*	↳ *1*		↳ *1*	
6 Filler	↳ *6*	↳ *1*		↳ *5*	
8 bmp	**8**	**8**			
2 No Fill	↳ *2*	↳ *2*			
6 Filler	↳ *6*	↳ *6*			
8 png	**8**	**8**			
2 No Fill	↳ *2*	↳ *2*			
6 Filler	↳ *6*	↳ *6*			
8 jpg	**14**	**8**			**6**
2 No Fill	↳ *2*	↳ *2*			
6 Filler	↳ *6*	↳ *6*			
8 tiff	**8**	**2**		**6**	
2 No Fill	↳ *2*	↳ *2*			
6 Filler	↳ *6*			↳ *6*	
7 thumbnails	**7**	**7**			
Full results are available at: **http://www.cftt.nist.gov/CFTT-Test-Run-Raw-Files.html**					

Table 2: Cluster Padded

4.3 Fragmented In Order

Graphic-simple-frag_1305121236.dd contains a total of 40 files, 10 which are contiguous and 30 that are sequentially fragmented with content that ranges in size from 1, 2, 4, 8, …128 sectors.

Out of the 40 graphic files a total of 53 files were carved, 25 files were *Viewable - Complete* and 6 files were *Viewable - Incomplete*.

All 7 thumbnails were carved completely, displayed properly and were exact matches of the source files.

Of the remaining 22 carved files, 16 were *Not Viewable and* the remaining 6 files were *False Positives*.

Summary: Retrieval of bmp and jpg files was less affected by fragmentation than png, gif and tiff files.

Test: Fragmented In Order	Total Carved	Viewable Complete/minor alteration	Viewable Incomplete/major alteration	Not Viewable	False Positive
40 files + 7 thumbnails	**53**	**25**	**6**	**16**	**6**
8 gif	**8**			**8**	
2 Contiguous	↳ ***2***			↳ ***2***	
6 Frag w/fill	↳ ***6***			↳ ***6***	
8 bmp	**8**	**8**			
2 Contiguous	↳ ***2***	↳ ***2***			
6 Frag w/fill	↳ ***6***	↳ ***6***			
8 png	**8**	**2**	**6**		
2 Contiguous	↳ ***2***	↳ **2**			
6 Frag w/fill	↳ ***6***		↳ **6**		
8 jpg	**14**	**8**			**6**
2 Contiguous	↳ ***2***	↳ ***2***			
6 Frag w/fill	↳ ***6***	↳ ***6***			
8 tiff	**8**			**8**	
2 Contiguous	↳ ***2***			↳ ***2***	
6 Frag w/fill	↳ ***6***			↳ ***6***	
7 thumbnails	**7**	**7**			
Full results are available at: **http://www.cftt.nist.gov/CFTT-Test-Run-Raw-Files.html**					

Table 3: Fragmented In Order

4.4 Incomplete

Graphic-partials_1305121236.dd contains a total of 40 files, 15 complete files: 10 which are contiguous and 5 that have content that ranges in size from 1, 2, 4, 8, …128 sectors. The remaining 25 files are partial files (e.g., only a portion of the file is present).

Out of the 40 graphic files a total of 39 files were carved – 11 of the carved files were *Viewable - Complete and* 11 files were *Viewable - Incomplete.*

All 5 thumbnails were carved completely, displayed properly and were exact matches of the source files.

Of the remaining 17 carved files: 13 were *Not Viewable* and the remaining 4 were *False Positives*.

Summary: The tool was able to completely recover the majority of the available data from the png complete and partial files, but not the other file types.

Test: Incomplete	Total Carved	Viewable Recovery of all available/minor alteration	Viewable Incomplete/major alteration	Not Viewable	False Positive
40 files + 5 thumbnails	**39**	**15**	**7**	**13**	**4**
8 gif	**6**	**1**		**5**	
3 Complete	↳***3***			↳***3***	
5 Partial	↳***3***	↳***1***		↳***2***	
8 bmp	**6**	**2**	**2**	**2**	
3 Complete	↳***3***	↳***2***	↳***1***		
5 Partial	↳***3***		↳***1***	↳***2***	
8 png	**6**	**5**	**1**		
3 Complete	↳***3***	↳***2***	↳***1***		
5 Partial	↳***3***	↳***3***			
8 jpg	**10**	**2**	**4**		**4**
3 Complete	↳***3***	↳***2***	↳***1***		
5 Partial	↳***3***		↳***3***		
8 tiff	**6**			**6**	
3 Complete	↳***3***			↳***3***	
5 Partial	↳***3***			↳***3***	
5 thumbnails	**5**	**5**			
Full results are available at: **http://www.cftt.nist.gov/CFTT-Test-Run-Raw-Files.html**					

Table 4: Incomplete

4.5 Fragmented Out of Order

Graphic-disorder_1305121235.dd contains a total of 35 files, 5 of which are contiguous fragmented files separated by other content that ranges in size from 1, 2, 4, 8, …128 sectors. The remaining 30 files are fragmented files that are disordered.

Out of the 35 graphic files a total of 44 files were carved, 13 files were *Viewable - Complete*, and 10 were *Viewable - Incomplete.*

All 6 thumbnails were carved completely, displayed properly and were exact matches of the source files.

Of the remaining 21 carved files, 18 were *Not Viewable* and the remaining 4 files were *False Positives*.

Summary: Files containing disordered fragments less affected recovery of jpg files. The tool was unable to recover viewable versions of the majority of bmp, tiff and gif files.

Test: Fragmented Out of Order	Total Carved	Viewable Complete/minor alteration	Viewable Incomplete/major alteration	Not Viewable	False Positive
35 files + 6 thumbnails	**44**	**13**	**10**	**18**	**3**
7 gif	**7**			**7**	
1 ABC	↳ *1*			↳ *1*	
1 ACB	↳ *1*			↳ *1*	
1 BAC	↳ *1*			↳ *1*	
***2** BCA*	↳ ***2***			↳ ***2***	
1 CAB	↳ *1*			↳ *1*	
***1** CBA*	↳ *1*			↳ *1*	
7 bmp	**7**	**1**	**2**	**4**	
1 ABC	↳ *1*		↳ *1*		
1 ACB	↳ *1*	↳ *1*			
1 BAC	↳ *1*			↳ *1*	
***2** BCA*	↳ ***2***		↳ *1*	↳ *1*	
1 CAB	↳ *1*			↳ *1*	
***1** CBA*	↳ *1*			↳ *1*	
7 png	**7**		**7**		
1 ABC	↳ *1*		↳ *1*		
1 ACB	↳ *1*		↳ *1*		
1 BAC	↳ *1*		↳ *1*		
***2** BCA*	↳ ***2***		↳ ***2***		
1 CAB	↳ *1*		↳ *1*		
***1** CBA*	↳ *1*		↳ *1*		
7 jpg	**10**	**6**	**1**		**3**
1 ABC	↳ *1*	↳ *1*			
1 ACB	↳ *1*		↳ *1*		
1 BAC	↳ *1*	↳ *1*			
***2** BCA*	↳ ***2***	↳ ***2***			
1 CAB	↳ *1*	↳ *1*			
***1** CBA*	↳ *1*	↳ *1*			
7 tiff	**7**			**7**	
1 ABC	↳ *1*			↳ *1*	
1 ACB	↳ *1*			↳ *1*	
1 BAC	↳ *1*			↳ *1*	
***2** BCA*	↳ ***2***			↳ ***2***	
1 CAB	↳ *1*			↳ *1*	
***1** CBA*	↳ *1*			↳ *1*	
6 thumbnails	**6**	**6**			
Full results are available at: **http://www.cftt.nist.gov/CFTT-Test-Run-Raw-Files.html**					

Table 5: Fragmented Out of Order

4.6 Braided Pair

Graphic-braid_1305121235.dd contains a total of 20 files, 10 of which are contiguous and 10 fragmented files.
Out of the 20 graphic files a total of 25 files were carved – 11 of the carved files were *Viewable - Complete*.

All 3 thumbnails were carved completely, displayed properly and were exact matches of the source files.

Of the remaining 10 carved files, 8 were *Not Viewable and* the remaining 2 files were *False Positives*.

Summary: Recovery of braided jpg files was more successful compared to other file types.

Test: Braided Pair	Total Carved	Viewable Complete/minor alteration	Viewable Incomplete/major alteration	Not Viewable	False Positive
20 files + 3 thumbnails	**25**	**11**	**4**	**8**	**2**
4 gif	**4**			**4**	
2 Contiguous	↳**2**			↳ ***2***	
2 Braided	↳**2**			↳ ***2***	
4 bmp	**4**	**2**	**1**	**1**	
2 Contiguous	↳**2**	↳ ***2***			
2 Braided	↳**2**		↳ ***1***	↳ ***1***	
4 png	**4**	**2**	**2**		
2 Contiguous	↳**2**	↳ ***2***			
2 Braided	↳**2**		↳ ***2***		
4 jpg	**6**	**3**	**1**		**2**
2 Contiguous	↳**2**	↳ ***2***			
2 Braided	↳**2**	↳ ***1***		↳ ***1***	
4 tiff	**4**	**1**		**3**	
2 Contiguous	↳**2**	↳ ***1***		↳ ***1***	
2 Braided	↳**2**			↳ ***2***	
3 thumbnails	**3**	**3**			
Full results are available at: **http://www.cftt.nist.gov/CFTT-Test-Run-Raw-Files.html**					

Table 6: Braided Pair

4.7 Byte Shifted

Graphic-shifted_1305311317.dd contains a total of 40 files, where all 40 files are contiguous files that have content between files ranging in size from 1, 3, 4, 5, 9, 16, 33, 64, 128, 129 sectors where the files land on non-sector boundaries.
Out of the 40 graphic files a total of 28 files were carved – 23 of the carved files were *Viewable - Complete*.

All 7 thumbnails were carved completely, displayed properly and were exact matches of the source files.

The remaining 6 carved files were *False Positives*.

Summary: Recovery The tool successfully recovered shifted png and jpg files but not gif, bmp or tiff files.

Test: Byte Shifted	Total Carved	Viewable Complete/minor alteration	Viewable Incomplete/major alteration	Not Viewable	False Positive
40 files + 7 thumbnails	**28**	**23**			**5**
8 gif					
8 bmp					
8 png	**8**	**8**			
8 jpg	**13**	**8**			**5**
8 tiff					
7 thumbnails	**7**	**7**			
Full results are available at: **http://www.cftt.nist.gov/CFTT-Test-Run-Raw-Files.html**					

Table 7: Byte Shifted

5 Relevant and Recovered Data Results

The following tables are based on the classification definition of precision and recall. Precision is the fraction of retrieved instances that are relevant, while recall is the fraction of relevant instances that are retrieved. Both precision and recall are therefore based on an understanding and measure of relevance. In simple terms, high recall means that an algorithm returned most of the relevant results, while high precision means that an algorithm returned substantially more relevant results than irrelevant. The two measures are sometimes used together to provide a single measurement for a system known as an f-score.

The precision and recall f-score measures the completeness and relevance of the returned data independently of the tools ability to display the carved graphic files. The f-score results in Tables 8 and 9 are based on the number of sectors carved rather than individual files. One caveat to keep in mind is that it is possible for a tool to return a high f-score where files are not viewable. For example, the majority of relevant sectors may be carved, but critical sectors needed for the graphic to be displayed are excluded. The following tables below provide a summary of data scores for individual test cases and by file types.

Table 8 reports an aggregate score across all files types for each test case, while Table 9 combines each test case and provides a score for individual file types. This yields an understanding of how the tool performed on a specific test case in addition to a particular file type.

Relevant and Recovered Data Score Summary for Adroit_v3.1d						
Test Case	**Recovered and Relevant Sectors**	**Recovered Sectors**	**P**	**Relevant Sectors**	**R**	**F**
No Padding	611710	611857	1.000	648837	0.943	0.97
Cluster Padded	611711	611859	1.000	648837	0.943	0.970
Fragmented In Order	522541	523097	0.999	648837	0.805	0.892
Incomplete	323517	326433	0.930	462222	0.657	0.770
Fragmented Out of Order	296974	297394	0.894	528089	0.504	0.644
Braided Pair	199358	199392	1.000	280889	0.710	0.830
Byte Shifted	158882	158986	0.999	158907	1.000	0.999

Table 8: Relevant and Recovered Data Score Summary

Relevant and Recovered Data Scores by file type for Adroit_v3.1d						
File Extension	**Recovered and Relevant Sectors**	**Recovered Sectors**	**P**	**Relevant Sectors**	**R**	**F**
gif	477	3072	0.155	242512	0.002	0.004
bmp	1089302	1140964	0.955	1184895	0.919	0.937
png	720090	720278	1.000	983215	0.732	0.845
jpg	131299	131958	0.995	140144	0.937	0.965
tif	1343927	1344621	0.999	1474689	0.911	0.953

Table 9: Relevant and Recovered Data Scores by file type