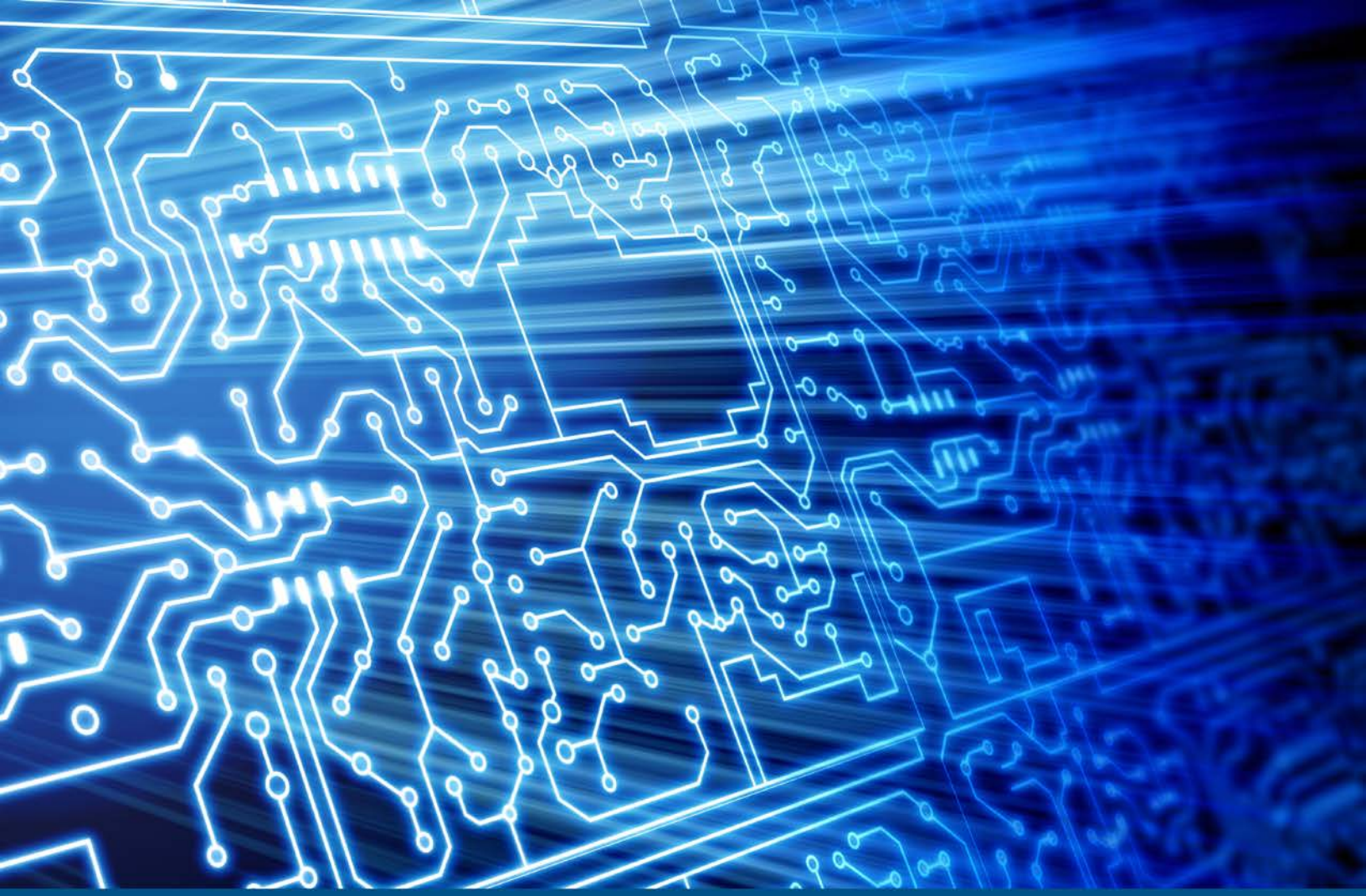

FTK v4.1

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:
FTK v4.1

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 FTK version 4.1 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 FTK v4.1 runs, see http://www.cftt.nist.gov/CFTT-Test-Run-Raw-Files.html.

Test Results for Graphic File Carving Tool

Tool Tested:	Forensic Toolkit (FTK)
Software Version:	v4.1
Supplier:	Access Data
Address:	588 West 400 South Suite 350 Lindon, UT 84042
Tel:	(800)-574-5199
Email:	support@ accessdata.com
WWW:	http://accessdata.com

1 Results Summary

Below are summaries on how FTK v4.1 performed when carving raw disembodied "dd" images containing various layouts of fragmentation and completeness.

FTK 4.1 was mostly successful at carving bmp, png and jpg files across all test images in a viewable state. The majority of carved gif files were incomplete. It does not carve tiff files. Generally, no more than 1 tiff or 2 gif files per test image are carved in a complete or viewable state with minor alteration by using default settings.

For more test result details see section 4.

2 Test Case Selection

FTK v4.1 ability to carve graphics gif, bmp, png, jpg, tiff 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 levels of content 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

FTK version 4.1 was installed on Windows XP v5.1.2600.

The default configuration settings were used for FTK.

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 filler between files.

Out of the 40 graphic files a total of 39 files were carved – 33 of the carved files were *Viewable – Complete* and 3 files were *Viewable - Incomplete.*

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

Of the remaining 3 carved files: 3 gif files were *Not Viewable*. There were no *False Positives.*

Summary: The tool was most successful at carving complete bmp, png, and jpg files.

Test: No Padding	Total Carved	Viewable Complete/minor alteration	Viewable Incomplete/major alteration	Not Viewable	False Positive
40 files + 7 thumbnails	**39**	**33**	**3**	**3**	
8 gif	**8**	**2**	**3**	**3**	
8 bmp	**8**	**8**			
8 png	**8**	**8**			
8 jpg	**8**	**8**			
8 tiff					
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. Filler (random data) separates the files. The filler size ranges from 1, 2, 4, 8, …128 sectors.

Out of the 40 graphic files a total of 39 files were carved – 33 of the carved files were *Viewable - Complete* and 3 files were *Viewable - Incomplete*.

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

Of the remaining 3 carved files: 3 gif files were *Not Viewable*. There were no *False Positives.*

Summary: The tool was most successful at carving complete bmp, png, and jpg files.

Test: Cluster Padded	Total Carved	Viewable Complete/minor alteration	Viewable Incomplete/major alteration	Not Viewable	False Positive
40 files + 7 thumbnails	**39**	**33**	**3**	**3**	
8 gif	**8**	**2**	**3**	**3**	
2 No Fill	↳ ***2***	↳ ***1***	↳ ***1***		
6 Filler	↳ ***6***	↳ ***1***	↳ ***2***	↳ ***3***	
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	**8**	**8**			
2 No Fill	↳ ***2***	↳ ***2***			
6 Filler	↳ ***6***	↳ ***6***			
8 tiff					
2 No Fill					
6 Filler					
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 filler that ranges in size from 1, 2, 4, 8, …128 sectors.

Out of the 40 graphic files a total of 39 files were carved, 14 files were *Viewable - Complete* and 22 files were *Viewable - Incomplete*.

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

Of the remaining 3 carved files: 3 gif files were *Not Viewable*. There were no *False Positives.*

Summary: In the presence of sequentially fragmented files, the tool had a reduced ability to recover viewable complete bmp, png and jpg files.

Test: Fragmented In Order	Total Carved	Viewable Complete/minor alteration	Viewable Incomplete/major alteration	Not Viewable	False Positive
40 files + 7 thumbnails	**39**	**14**	**22**	**3**	
8 gif	**8**		**5**	**3**	
2 Contiguous	↳ ***2***		↳ ***1***	↳ ***1***	
6 Frag w/fill	↳ ***6***		↳ ***4***	↳ ***2***	
8 bmp	**8**	**3**	**5**		
2 Contiguous	↳ ***2***	↳ ***2***			
6 Frag w/fill	↳ ***6***	↳ ***1***	↳ ***5***		
8 png	**8**	**2**	**6**		
2 Contiguous	↳ ***2***	↳ ***2***			
6 Frag w/fill	↳ ***6***		↳ ***6***		
8 jpg	**8**	**2**	**6**		
2 Contiguous	↳ ***2***	↳ ***2***			
6 Frag w/fill	↳ ***6***		↳ ***6***		
8 tiff					
2 Contiguous					
6 Frag w/fill					
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 filler 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 24 files were carved – 13 of the carved files were *Viewable - Complete, and* 10 files were *Viewable - Incomplete.*

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

The remaining carved file was a gif file that was *Not Viewable*. There were no *False Positives.*

Summary: In the presence of partial files, the tool had a reduced ability to recover viewable complete png and jpg files.

Test: Incomplete	Total Carved	Viewable Recovery of all available/minor alteration	Viewable Incomplete/major alteration	Not Viewable	False Positive
40 files + 5 thumbnails	**24**	**13**	**10**	**1**	
8 gif	**3**		**2**	**1**	
3 Complete	↳ ***2***		↳ ***1***	↳ ***1***	
5 Partial	↳ ***1***		↳ ***1***		
8 bmp	**4**	**4**			
3 Complete	↳ ***2***	↳ ***2***			
5 Partial	↳ ***2***	↳ ***2***			
8 png	**6**	**2**	**4**		
3 Complete	↳ ***3***	↳ ***2***	↳ ***1***		
5 Partial	↳ ***3***		↳ ***3***		
8 jpg	**6**	**2**	**4**		
3 Complete	↳ ***3***	↳ ***2***	↳ ***1***		
5 Partial	↳ ***3***		↳ ***3***		
8 tiff					
3 Complete					
5 Partial					
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 that have filler that ranges in size from 1, 2, 4, 8, …128 sectors and the remaining 30 are fragmented files that are disordered.

Out of the 35 graphic files a total of 24 files were carved, 7 files were *Viewable - Complete*, and 16 were *Viewable - Incomplete.*

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

The remaining carved file was a gif file that was *Not Viewable*. There were no *False Positives.*

Summary: In the presence of disordered fragmented files, the tool had a reduced ability to recover viewable complete bmp, png and jpg files.

Test: Fragmented Out of Order	Total Carved	Viewable Complete/minor alteration	Viewable Incomplete/major alteration	Not Viewable	False Positive
35 files + 6 thumbnails	**24**	**7**	**16**	**1**	
7 gif	**1**			**1**	
1 ABC					
1 ACB					
1 BAC					
***2** BCA*	↳***1***			↳***1***	
1 CAB					
***1** CBA*					
7 bmp	**4**		**4**		
1 ABC					
1 ACB					
1 BAC	↳***1***		↳***1***		
***2** BCA*	↳***2***		↳***2***		
1 CAB	↳***1***		↳***1***		
***1** CBA*					
7 png	**6**	**1**	**5**		
1 ABC	↳***1***	↳***1***			
1 ACB					
1 BAC	↳***1***		↳***1***		
***2** BCA*	↳***2***		↳***2***		
1 CAB	↳***1***		↳***1***		
***1** CBA*	↳***1***		↳***1***		
7 jpg	**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 tiff					
1 ABC					
1 ACB					
1 BAC					
***2** BCA*					
1 CAB					
***1** CBA*					
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 17 files were carved – 9 of the carved files were *Viewable – Complete* and 7 files were *Viewable - Incomplete*.

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

The remaining carved file was a gif file that was *Not Viewable*. There were no *False Positives.*

Summary: The tool was most successful at carving bmp, png, and jpg files.

Test: Braided fragmentation	Total Carved	Viewable Complete/minor alteration	Viewable Incomplete/major alteration	Not Viewable	False Positive
20 files + 3 thumbnails	**17**	**9**	**7**	**1**	
4 gif	**4**		**3**	**1**	
2 Contiguous	↳ ***2***		↳ ***2***		
2 Braided	↳ ***2***		↳ ***1***	↳ ***1***	
4 bmp	**3**	**2**	**1**		
2 Contiguous	↳ ***2***	↳ ***2***			
2 Braided	↳ ***1***		↳ ***1***		
4 png	**3**	**2**	**1**		
2 Contiguous	↳ ***2***	↳ ***2***			
2 Braided	↳ ***1***		↳ ***1***		
4 jpg	**4**	**2**	**2**		
2 Contiguous	↳ ***2***	↳ ***2***			
2 Braided	↳ ***2***		↳ ***2***		
4 tiff					
2 Contiguous					
2 Braided					
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 filler that ranges 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 39 files were carved – 33 of the carved files were *Viewable – Complete* and 3 files were *Viewable - Incomplete.*

All of the 7 thumbnails were carved completely, displayed properly and were exact matches of the source files.
Of the remaining 3 carved files: 3 gif files were *Not Viewable*. There were no *False Positives.*

Summary: The tool was most successful at carving bmp, png and jpg files.

Test: Byte Shifted	Total Carved	Viewable Complete/minor alteration	Viewable Incomplete/major alteration	Not Viewable	False Positive
40 files + 7 thumbnails	**39**	**33**	**3**	**3**	
8 gif	**8**	**2**	**3**	**3**	
8 bmp	**8**	**8**			
8 png	**8**	**8**			
8 jpg	**8**	**8**			
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 providing 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 FTK_v4.1						
Test Case	**Recovered and Relevant Sectors**	**Recovered Sectors**	**P**	**Relevant Sectors**	**R**	**F**
No Padding	367651	367750	1.000	401653	0.915	0.956
Cluster Padded	367651	367750	1.000	401653	0.915	0.956
Fragmented In Order	276210	276940	0.997	401653	0.688	0.814
Incomplete	156078	156505	0.870	282028	0.483	0.621
Fragmented Out of Order	127480	127818	0.754	331372	0.291	0.420
Braided Pair	88317	88351	1.000	171847	0.514	0.679
Byte Shifted	367651	367750	1.000	401653	0.915	0.956

Table 8: Relevant and Recovered Data Score Summary

Relevant and Recovered Data Scores by file type for FTK_v4.1						
File Extension	**Recovered and Relevant Sectors**	**Recovered Sectors**	**P**	**Relevant Sectors**	**R**	**F**
gif	15769	16015	0.985	242512	0.065	0.122
bmp	1009080	1060684	0.951	1184895	0.852	0.899
png	572624	572944	0.999	843957	0.678	0.808
jpg	102435	103221	0.992	120495	0.850	0.916
tif						

Table 9: Relevant and Recovered Data Scores by file type