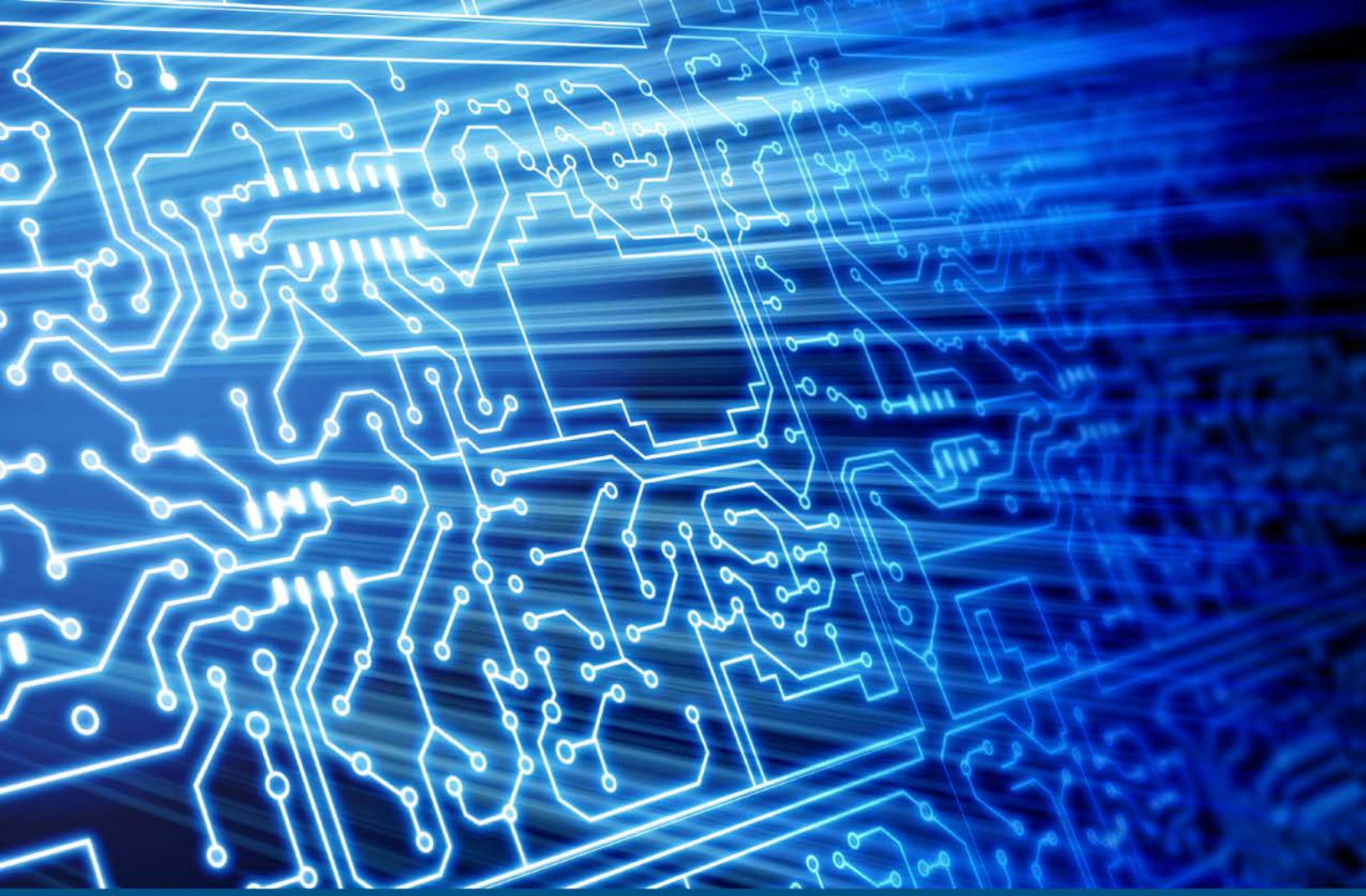

X-Ways Forensics v17.6

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:
X-Ways Forensics v17.6

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 X-Ways Forensics version 17.6 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 X-Ways Forensics v17.6 runs, see http://www.cftt.nist.gov/CFTT-Test-Run-Raw-Files.html.

Test Results for Digital Data File Carving Tool

Tool Tested:	X-Ways Forensics
Software Version:	v17.6
Supplier:	X-Ways Software Technology AG
Address:	Agrippastr. 37-39 50676 Cologne, Germany
Tel:	+49-221-420 486 5
Fax:	+49-3212-123 2029
Email:	mail@x-ways.com
WWW:	http://x-ways.net

1 Results Summary

Below are summaries on how X-Ways Forensics v17.6 performed when carving raw disembodied “dd” images containing various layouts of fragmentation and completeness.

X-Ways Forensics was successful at carving gif, bmp, png, jpg and tiff files in a viewable state for all non-fragmented “dd” images. Fragmented “dd” images mostly returned fewer viewable-complete ratings for all file types.

For more test result details see section 4.

2 Test Case Selection

X-Ways Forensics 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 with filler
- **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

X-Ways Forensics version 17.6 was installed on Windows XP v5.1.2600.

The following modifications to the default settings for X-Ways were made for the following scenarios:

- Thumbnails were recovered by selecting: *uncover embedded data in various file types*.

- Files landing on non-sector boundaries were recovered by selecting: *in selected evidence objects*, *extensive byte level search* and *always ignore start sectors of known files*.

3.2 Support Software

A package of programs to support test analysis, rel-9, was used. The software can be obtained from: http://www.cftt.nist.gov/filecarving/rel-9.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 47 files were carved – all the carved files were *Viewable – Complete.*

All thumbnails were carved.

Summary: The tool was successful at carving all file types.

Test: No Padding	Total Carved	Viewable Complete/minor alteration	Viewable Incomplete/major alteration	Not Viewable	False Positive
40 files + 7 thumbnails	**47**	**47**			
8 gif	**8**	**8**			
8 bmp	**8**	**8**			
8 png	**8**	**8**			
8 jpg	**8**	**8**			
8 tiff	**8**	**8**			
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 47 files were carved – all the carved files were *Viewable – Complete.*

All 7 thumbnails were carved.

Summary: The tool was successful at carving all file types.

Test: Cluster Padded	Total Carved	Viewable Complete/minor alteration	Viewable Incomplete/major alteration	Not Viewable	False Positive
40 files + 7 thumbnails	**47**	**47**			
8 gif	**8**	**8**			
2 No Fill	↳ ***2***	↳ ***2***			
6 Filler	↳ ***6***	↳ ***6***			
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	**8**	**8**			
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 filler that ranges in size from 1, 2, 4, 8, …128 sectors.

Out of the 40 graphic files a total of 47 files were carved – 23 of the carved files were *Viewable – Complete* and 18 files were *Viewable - Incomplete.*

All 7 thumbnails were carved.

The remaining 6 carved files were *Not Viewable*.

Summary: In the presence of sequentially fragmented files, the tool had a reduced ability to recover viewable complete gif, png, jpg 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	**40**	**16**	**18**	**6**	
8 gif	**8**	**2**	**6**		
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	**8**	**2**	**6**		
2 Contiguous	↳ ***2***	↳ ***2***			
6 Frag w/fill	↳ ***6***		↳ ***6***		
8 tiff	**8**	**2**		**6**	
2 Contiguous	↳ ***2***	↳ ***2***			
6 Frag w/fill	↳ ***6***			↳ ***6***	
7 thumbnails					
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 35 files were carved – 16 of the carved files were *Viewable – Complete* and 15 files were *Viewable - Incomplete.*

All 5 thumbnails were carved.

The remaining 4 carved files were *Not Viewable*.

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

Test: Incomplete	Total Carved	Viewable Recovery of all available/minor alteration	Viewable Incomplete/major alteration	Not Viewable	False Positive
40 files + 5 thumbnails	**35**	**16**	**15**	**4**	
8 gif	**6**	**2**	**4**		
3 Complete	↳ ***3***	↳ ***2***	↳ ***1***		
5 Partial	↳ ***3***		↳ ***3***		
8 bmp	**6**	**3**	**3**		
3 Complete	↳ ***2***	↳ ***2***	↳ ***1***		
5 Partial	↳ ***3***	↳ ***1***	↳ ***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	**6**	**2**		**4**	
3 Complete	↳ ***3***	↳ ***2***		↳ ***1***	
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 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 40 graphic files a total of 41 files were carved – 10 of the carved files were *Viewable – Complete* and 24 files were *Viewable - Incomplete.*

All 6 thumbnails were carved.

The remaining 7 carved files were *Not Viewable.*

Summary: In the presence of disordered fragmented files, the tool had a reduced ability to recover viewable complete bmp and png files. Recovered gif and jpg files were viewable incomplete. All tiff files were not viewable.

Test: Fragmented Out of Order	Total Carved	Viewable Complete/minor alteration	Viewable Incomplete/major alteration	Not Viewable	False Positive
35 files + 6 thumbnails	**41**	**10**	**24**	**7**	
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**	**3**	**4**		
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 png	**7**	**1**	**6**		
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	**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	**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	**7**	**7**			
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 40 graphic files a total of 23 files were carved – 13 of the carved files were *Viewable – Complete* and 8 files were *Viewable - Incomplete.*

All 3 thumbnails were carved.

The remaining 2 carved files were *Not Viewable*.

Summary: In the presence braided files, the tool had a reduced ability to recover viewable complete files.

Test: Braided Pair	Total Carved	Viewable Complete/minor alteration	Viewable Incomplete/major alteration	Not Viewable	False Positive
20 files + 3 thumbnails	**23**	**13**	**8**	**2**	
4 gif	**4**	**2**	**2**		
2 Contiguous	↳ *2*	↳ *2*			
2 Braided	↳ *2*		↳ *2*		
4 bmp	**4**	**2**	**2**		
2 Contiguous	↳ *2*	↳ *2*			
2 Braided	↳ *2*		↳ *2*		
4 png	**4**	**2**	**2**		
2 Contiguous	↳ *2*	↳ *2*			
2 Braided	↳ *2*		↳ *2*		
4 jpg	**4**	**2**	**2**		
2 Contiguous	↳ *2*	↳ *2*			
2 Braided	↳ *2*		↳ *2*		
4 tiff	**4**	**2**		**2**	
2 Contiguous	↳ *2*	↳ *2*			
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 fragmentation

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 57 files were carved – 47 of the carved files were *Viewable – Complete*.

All 7 thumbnails were carved.

The remaining 10 carved files were *False Positive.*

Summary: The tool was successful at carving all file types landing on a non-sector boundary.

Test: Byte Shifted	Total Carved	Viewable Complete/minor alteration	Viewable Incomplete/major alteration	Not Viewable	False Positive
40 files + 7 thumbnails	**57**	**47**			**10**
8 gif	**8**	**8**			
8 bmp	**8**	**8**			
8 png	**8**	**8**			
8 jpg	**8**	**8**			
8 tiff	**18**	**8**			**10**
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 X Ways_v17.6						
Test Case	**Recovered and Relevant Sectors**	**Recovered Sectors**	**P**	**Relevant Sectors**	**R**	**F**
No Padding	648770	648896	1.000	648837	1.000	1.000
Cluster Padded	648770	648896	1.000	648837	1.000	1.000
Fragmented In Order	545933	546862	0.998	648837	0.841	0.913
Incomplete	303126	366407	0.773	462222	0.613	0.683
Fragmented Out of Order	286136	365051	0.699	528089	0.483	0.571
Braided Pair	223740	249968	0.895	280889	0.796	0.843
Byte Shifted	648770	653035	0.993	648837	1.000	0.997

Table 8: Relevant and Recovered Data Score Summary

Relevant and Recovered Data Scores by file type for X Ways_v17.6						
File Extension	**Recovered and Relevant Sectors**	**Recovered Sectors**	**P**	**Relevant Sectors**	**R**	**F**
gif	164243	188163	0.873	242512	0.677	0.763
bmp	1089303	1194699	0.912	1184895	0.919	0.916
png	581096	581437	0.999	843957	0.689	0.815
jpg	102435	103161	0.993	120495	0.850	0.916
tif	1316902	1411655	0.933	1474689	0.893	0.913

Table 9: Relevant and Recovered Data Scores by file type