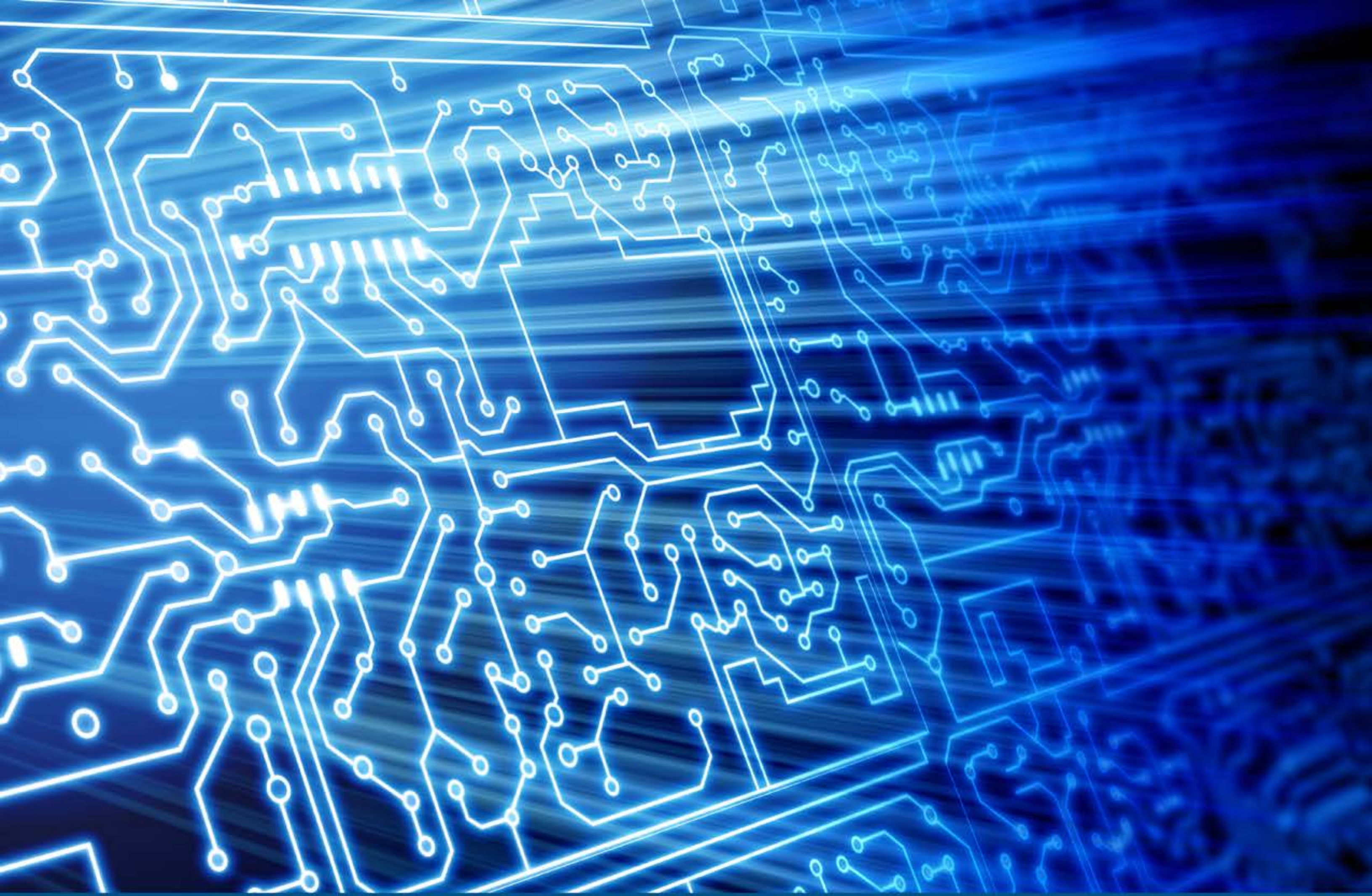

EnCase Forensic v7.09.05

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:
EnCase Forensic v7.09.05

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 EnCase Forensic version 7.09.05 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 EnCase Forensics v7.09.05 runs, see http://www.cftt.nist.gov/CFTT-Test-Run-Raw-Files.html.

Test Results for Graphic File Carving Tool

Tool Tested:	EnCase Forensic
Software Version:	v7.09.05
Supplier:	Guidance Software Inc.
Address:	1055 E.Colorado Blvd. Pasadena, CA 91106-2375
Tel:	(626) 229-9191
Email:	TechnicalSupport@encase.com
WWW:	http://www.encase.com

1 Results Summary

Below are summaries on how EnCase Forensic v7.09.05 performed when carving raw "dd" images containing various layouts of fragmentation and completeness.

EnCase Forensic v7.09.05 was mostly successful at carving contiguous files (i.e., bmp, png and jpg). EnCase does not support carving fragmented files. Recovered gif files were not viewable for most of the test cases. False positives occurred for bmp, tiff and jpg files.

The following test cases are not supported by EnCase Forensic v7.09.05: *Fragmented in Order* (section 4.3), *Incomplete* (section 4.4), *Fragmented Out of Order* (section 4.5) and *Braided Pair* (section 4.6). However, the test case results are included providing users with an overview for reference.

Test case *No Padding* (section 4.1),was run under Windows XP v5.1.2600 as well as Windows 7 v6.1.7601 environments and the results were not consistent. EnCase recovered more viewable files when run under Windows 7.

For more test result details see section 4.

2 Test Case Selection

EnCase Forensic v7.09.05 ability to carve graphics files (i.e., gif, bmp, png, jpg, tiff) 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

EnCase Forensic v7.09.05 was installed on Windows XP v5.1.2600 and Windows 7 v6.1.7601.

The default configuration settings were used for EnCase with the *Bookmark embedded thumbnails as images* option selected.

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 graphic files (8 - gif, bmp, png, jpg, tiff) and 7 thumbnails with no filler between files.

This test was performed twice – once with EnCase running in Windows XP v5.1.2600 and once in Windows 7 v6.1.7601. Reported results are for Windows 7. Encase recovered more viewable files when run under Windows 7. (Recovered GIF files were not viewable in Windows XP. Data from the Windows XP test are available at http://www.cftt.nist.gov/CFTT-Test-Run-Raw-Files.html)

Out of the 40 graphic files a total of 8946 files were carved – 29 of the carved files were *Viewable – Complete* and 2 were *Not-Viewable*.

No thumbnails were recovered.

Of the remaining 8915 carved files: 8882 bmp and 33 tiff files were *False-Positives.*

Summary: The tool was most successful at carving Viewable-Complete gif, 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	**8946**	**29**		**2**	**8915**
8 gif	**8**	**8**			
8 bmp	**8890**	**6**		**2**	**8882**
8 png	**8**	**8**			
8 jpg	**7**	**7**			
8 tiff	**33**				**33**
7 thumbnails					
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. 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 8964 files were carved – 21 of the carved files were *Viewable – Complete* and 10 were *Not-Viewable*.

No thumbnails were recovered.

Of the remaining 8933 carved files: 8900 bmp and 33 tiff files were *False-Positives*.

Summary: The presence of other data between graphic files did not affect tool performance. The tool was most successful at carving Viewable-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	**8964**	**21**		**10**	**8933**
8 gif	**8**			**8**	
2 No Fill	↳***2***			↳***2***	
6 Filler	↳***6***			↳***6***	
8 bmp	**8908**	**6**		**2**	**8900**
2 No Fill	↳***2***	↳***2***			
6 Filler	↳***6***	↳***4***		↳***2***	
8 png	**8**	**8**			
2 No Fill	↳***2***	↳***2***			
6 Filler	↳***6***	↳***6***			
8 jpg	**7**	**7**			
2 No Fill	↳***2***	↳***2***			
6 Filler	↳***5***	↳***5***			
8 tiff	33				33
2 No Fill					
6 Filler					
7 thumbnails					
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 9118 files were carved – 10 of the carved files were *Viewable – Complete*, 11 files were *Viewable-Incomplete* and 10 files were *Not-Viewable.*

No thumbnails were recovered.

Of the remaining 9087 carved files: 9054 bmp and 33 tiff files were *False-Positives*.

Summary: In the presence of sequentially fragmented files, the tool had a reduced ability to recover viewable complete 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	**9118**	**10**	**11**	**10**	**9087**
8 gif	**8**			**8**	
2 Contiguous	↳***2***			↳ ***2***	
6 Frag w/fill	↳***6***			↳ ***6***	
8 bmp	**9062**	**6**		**2**	**9054**
2 Contiguous	↳***2***	↳ ***2***			
6 Frag w/fill	↳***6***	↳ ***4***		↳ ***2***	
8 png	**8**	**2**	**6**		
2 Contiguous	↳***2***	↳ ***2***			
6 Frag w/fill	↳***6***		↳ ***6***		
8 jpg	**7**	**2**	**5**		
2 Contiguous	↳***2***	↳ ***2***			
6 Frag w/fill	↳***5***		↳ ***5***		
8 tiff	**33**				**33**
2 Contiguous					
6 Frag w/fill					
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 6191 files were carved – 9 of the carved files were *Viewable – Complete*, 6 files were *Viewable-Incomplete* and 7 files were *Not-Viewable.*

No thumbnails were recovered.

Of the remaining 6169 carved files: 6148 bmp, 7 jpg and 21 tiff files were *False-Positives.*

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	**6191**	**9**	**6**	**7**	**6169**
8 gif	**6**			**6**	
3 Complete	↳*3*			↳*3*	
5 Partial	↳*3*			↳*3*	
8 bmp	**6153**	**4**		**1**	**6148**
3 Complete	↳*2*	↳*2*			
5 Partial	↳*3*	↳*2*		↳*1*	
8 png	**6**	**2**	**4**		
3 Complete	↳*3*	↳*2*	↳*1*		
5 Partial	↳*3*		↳*3*		
8 jpg	**5**	**3**	**2**		**7**
4 Complete	↳*3*	↳*3*			
4 Partial	↳*2*		↳*2*		
8 tiff	**21**				**21**
3 Complete					
5 Partial					
5 thumbnails					
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 5612 files were carved – 4 of the carved files were *Viewable – Complete*, 14 files were *Viewable-Incomplete* and 8 files were *Not-Viewable.*

No thumbnails were recovered.

Of the remaining 5586 carved files: 5562 bmp and 24 tiff files were *False-Positives.*

Summary: In the presence of disordered fragmented files, the tool had a reduced ability to recover viewable-complete 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	**5612**	**4**	**14**	**8**	**5586**
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	**5568**	**3**	**2**	**1**	**5562**
1 ABC	↳***1***	↳***1***			
1 ACB	↳***1***	↳***1***			
1 BAC	↳***1***	↳***1***			
2 BCA	↳***2***		↳***1***	↳***1***	
1 CAB	↳***1***		↳***1***		
1 CBA					
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	**6**		**6**		
1 ABC	↳***1***		↳***1***		
1 ACB	↳***1***		↳***1***		
1 BAC	↳***1***		↳***1***		
2 BCA	↳***2***		↳***2***		
1 CAB					
1 CBA	↳***1***		↳***1***		
7 tiff	**24**				**24**
1 ABC					
1 ACB					
1 BAC					
2 BCA					
1 CAB					
1 CBA					
6 thumbnails					
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 1746 files were carved – 6 of the carved files were *Viewable – Complete*, 4 files were *Viewable-Incomplete* and 5 files were *Not-Viewable.*

No thumbnails were recovered.

Of the remaining 1731 carved files: 1716 bmp and 15 tiff files were *False-Positives.*

Summary: In the presence of braided files, the tool had a reduced ability to carve viewable-complete bmp, png and jpg files.

Test: Braided Pair	Total Carved	Viewable Complete/minor alteration	Viewable Incomplete/major alteration	Not Viewable	False Positive
20 files + 3 thumbnails	**1746**	**6**	**4**	**5**	**1731**
4 gif	**4**			**4**	
2 Contiguous	↳***2***			↳***2***	
2 Braided	↳***2***			↳***2***	
4 bmp	**1720**	**2**	**1**		**1716**
2 Contiguous	↳***1***	↳***1***			
2 Braided	↳***2***	↳***1***	↳***1***		
4 png	**4**	**2**	**2**		
2 Contiguous	↳***2***	↳***2***			
2 Braided	↳***2***		↳***2***		
4 jpg	**3**	**2**	**1**		
2 Contiguous	↳***2***	↳***2***			
2 Braided	↳***1***		↳***1***		
4 tiff	**15**				**15**
2 Contiguous					
2 Braided					
3 thumbnails					
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 9073 files were carved – 21 of the carved files were *Viewable – Complete* and 10 were *Not-Viewable*.

No thumbnails were recovered.

Of the remaining 9042 carved files: 9009 bmp and 33 tiff files were *False-Positives.*

Summary: The tool was most successful at carving Viewable-Complete 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	**9073**	**21**		**10**	**9042**
8 gif	**8**			**8**	
8 bmp	**9017**	**6**		**2**	**9009**
8 png	**8**	**8**			
8 jpg	**7**	**7**			
8 tiff	**33**				**33**
7 thumbnails					

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 EnCase v7.09.05						
Test Case	**Recovered and Relevant Sectors**	**Recovered Sectors**	**P**	**Relevant Sectors**	**R**	**F**
No Padding	333090	404358	0.823	648837	0.513	0.632
Cluster Padded	302223	373625	0.809	648837	0.466	0.591
Fragmented In Order	213523	286593	0.745	648837	0.329	0.456
Incomplete	179067	232565	0.684	462222	0.344	0.458
Fragmented Out of Order	122641	174829	0.701	528089	0.232	0.349
Braided Pair	85402	110715	0.771	280889	0.304	0.436
Byte Shifted	302127	325825	0.927	648837	0.466	0.620

Table 8: Relevant and Recovered Data Score Summary

Relevant and Recovered Data Scores by file type for EnCase v7.09.05						
File Extension	**Recovered and Relevant Sectors**	**Recovered Sectors**	**P**	**Relevant Sectors**	**R**	**F**
gif	30908	30975	0.998	242512	0.127	0.226
bmp	820716	1209328	0.679	1184895	0.693	0.686
png	581096	581437	0.999	843957	0.689	0.815
jpg	84841	85314	0.994	120495	0.704	0.824
tif	0	1456	0.000	1474689	0.000	0.000

Table 9: Relevant and Recovered Data Scores by file type