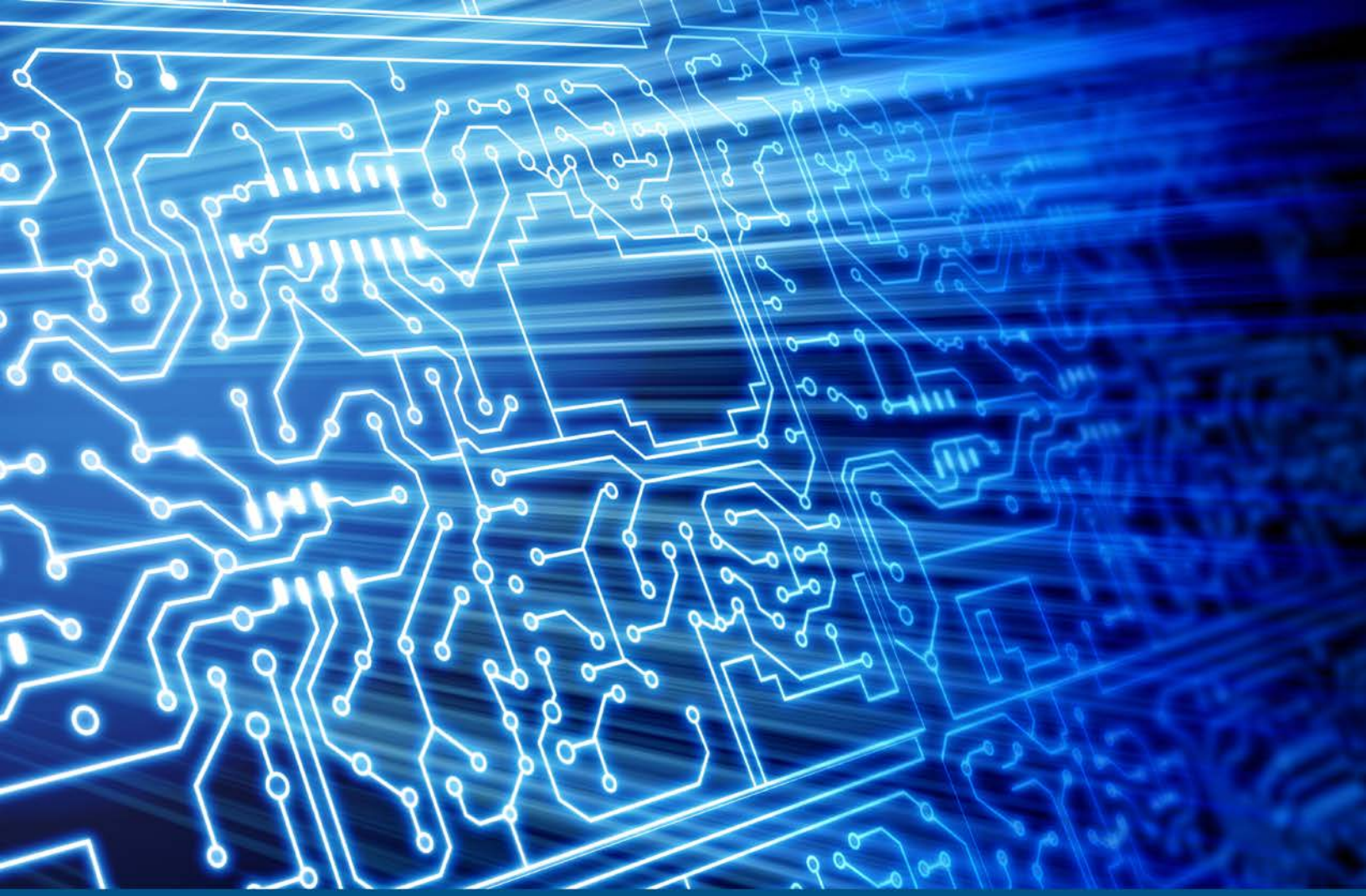

EnCase v7.09.05

Test Results for Video File Carving Tool

October 22, 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.

October 2014

Test Results for Video File Carving Tool:
EnCase 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 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 four 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. To download a zip file containing data returned for each test case for EnCase 7.09.05 runs, see http://www.cftt.nist.gov/CFTT-Test-Run-Raw-Files.html.

Test Results for Video File Carving Tool

Tool Tested:	Encase
Software Version:	7.09.05
Supplier:	Guidance Software
Address:	1055 E. Colorado Blvd. Pasadena, CA 91106-2375
Tel:	1 (626) 229-9191
Fax:	1 (626) 229-9199
WWW:	www.guidancesoftware.com/

1 Results Summary

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

EnCase was most successful at carving video file types mp4, mov, avi, wmv in a viewable state. The carved mp4, mov, avi and wmv files were classified as *Not Viewable* or *False Positive* for all test cases. Video file types 3gp and ogv were not recovered.

For more test result details see section 4.

2 Test Case Selection

EnCase v7.09.05 ability to carve mp4, mov, avi, wmv, 3gp and ogv was measured by analyzing carved video 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 and 32 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 version 7.09.05 was installed on Windows XP v5.1.2600.

The default configuration settings were used for Encase.

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.cfreds.nist.gov/filecarvingtestreports.html.

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 video appears to be unchanged from the original or the changes are so minor that the full content, color, and other attributes of the video are maintained.

The *Viewable – Incomplete/major alteration* column include partial recoveries (i.e., only parts of the video are viewable), scrambled videos 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., mp4, mov). 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.

The VLC media player software was used to interpret the files carved and classify them into the different categories (i.e., Viewable – Complete/minor, Viewable – Incomplete/major). The media player speed used was "faster" to shorten the time for carved file classification.

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

Video-nofill_1401090836.dd contains a total of 36 contiguous files with no filler between files.

Out of the 36 video files a total of 44 files were carved – 16 of the carved files were *Viewable – Complete, 11* of the files were *Viewable – Incomplete,* 11 of the files were *Not Viewable* and 6 were *False Positives.*

Summary: The tool was most successful at carving mp4, mov, wmv and 3gp.

Test: No Padding	Total Carved	Viewable Complete/minor alteration	Viewable Incomplete/major alteration	Not Viewable	False Positive
36 files	**44**	**16**	**11**	**11**	**6**
6 mp4	**8**	**4**	**1**	**2**	
6 mov	**15**	**2**	**6**	**1**	**6**
6 avi	**3**			**3**	
6 wmv	**6**	**5**	**1**		
6 3gp	**12**	**5**	**3**	**4**	
6 ogv					
Full results are available at: **http://www.cftt.nist.gov/CFTT-Test-Run-Raw-Files.html**					

Table 1: No Padding

4.2 Cluster Padded

Video-notshifted_1401090819.dd contains a total of 36 files, where all 36 files are contiguous files that have filler that ranges in size from 1, 3, 4, 5, 9, 16, 32 sectors where the files land on sector boundaries.

Out of the 36 video files a total of 50 files were carved – 17 of the carved files were *Viewable – Complete, 18* of the files were *Viewable – Incomplete,* 8 of the files were *Not Viewable* and 7 were *False Positives.*

Summary: The presence of filler between files did not significantly impact the recovery of Viewable Complete files.

Padded	Carved	Complete/minor alteration	Incomplete/major alteration	Viewable	Positive
36 files	**50**	**17**	**18**	**8**	**7**
6 mp4	**9**	**4**	**1**	**4**	
6 mov	**17**	**1**	**9**		**7**
6 avi	**6**	**2**	**4**		
6 wmv	**6**	**5**	**1**		
6 3gp	**12**	**5**	**3**	**4**	
6 ogv					
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

Video-simple-frag_1401090846.dd contains a total of 36 files, 12 which are contiguous and 24 that are sequentially fragmented with filler that ranges in size from 1, 2, 4, 8, 16 sectors.

Out of the 36 video files a total of 50 files were carved – 9 of the carved files were *Viewable – Complete, 25* of the files were *Viewable – Incomplete,* 9 of the files were *Not Viewable* and 7 were *False Positives.*

Summary: In the presence of sequentially fragmented files, the tool had a reduced ability to recover Viewable-Complete mp4, mov, avi, wmv and 3gp files. An increased number of viewable incomplete, not viewable and false positive files were recovered.

Test: Fragmented In Order	Total Carved	Viewable Complete/minor alteration	Viewable Incomplete/major alteration	Not Viewable	False Positive
36 files	**50**	**9**	**25**	**9**	**7**
6 mp4	**9**	**1**	**4**	**4**	
2 Contiguous	↳ ***3***	↳ *1*		↳ ***2***	
4 Frag w/fill	↳ ***6***		↳ *4*	↳ ***2***	
6 mov	**17**	**1**	**9**		**7**
2 Contiguous	↳ *2*	↳ *1*	↳ *1*		
4 Frag w/fill	↳ *8*		↳ *8*		
6 avi	**9**	**2**	**4**		**3**
2 Contiguous	↳ *2*	↳ *2*			
4 Frag w/fill	↳ *4*		↳ *4*		
6 wmv	**6**	**1**	**5**		
2 Contiguous	↳ ***2***	↳ *1*	↳ *1*		
4 Frag w/fill	↳ ***4***		↳ *4*		
6 3gp	**12**	**4**	**3**	**5**	
2 Contiguous	↳ ***5***	↳ *2*	↳ *1*	↳ *2*	
4 Frag w/fill	↳ ***7***	↳ *2*	↳ *2*	↳ *3*	
6 ogv					
2 Contiguous					
4 Frag w/fill					
Full results are available at: **http://www.cftt.nist.gov/CFTT-Test-Run-Raw-Files.html**					

Table 3: Fragmented In Order

4.4 Incomplete

Video-partials_1401090843.dd contains a total of 36 files, 18 complete files: 12 which are contiguous and 6 that have filler that ranges in size from 1, 2, 4, 8, 16 sectors. The remaining 18 files are partial files (e.g., only a portion of the file is present).

Out of the 36 video files a total of 42 files were carved – 11 of the carved files were *Viewable – Complete*, *18* of the files were *Viewable – Incomplete*, 10 of the files were *Not Viewable* and 3 were *False Positives.*

Summary: In the presence of partial files, the tool had a reduced ability to recover viewable complete avi and wmv files. An increased number of viewable - incomplete were recovered.

Test: Incomplete	Total Carved	Viewable Recovery of all available/minor alteration	Viewable Incomplete/major alteration	Not Viewable	False Positive
36 files	**42**	**11**	**18**	**10**	**3**
6 mp4	**11**	**2**	**2**	**7**	
3 Complete	↳ ***8***	↳ *1*	↳ *1*	↳ *6*	
3 Partial	↳ ***3***	↳ *1*	↳ *1*	↳ *1*	
6 mov	**11**	**3**	**5**		**3**
3 Complete	↳ *2*		↳ *2*		
3 Partial	↳ *6*	↳ *3*	↳ *3*		
6 avi	**5**	**2**	**3**		
3 Complete	↳ *3*	↳ *2*	↳ *1*		
3 Partial	↳ *2*		↳ *2*		
6 wmv	**5**	**1**	**4**		
3 Complete	↳ *3*	↳ *1*	↳ *2*		
3 Partial	↳ *2*		↳ *2*		
6 3gp	**10**	**3**	**4**	**3**	
3 Complete	↳ *8*	↳ *2*	↳ *4*	↳ *2*	
3 Partial	↳ *2*	↳ *1*		↳ *1*	
6 ogv					
3 Complete					
3 Partial					
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

Video-disorder_140190832.dd contains a total of 36 files, 6 of which are contiguous fragmented files that have filler that ranges in size from 1, 2, 4, 8, 16 sectors and the remaining 30 are fragmented files that are disordered.

Out of the 36 video files a total of 50 files were carved – 1 of the carved files were *Viewable – Complete, 34* of the files were *Viewable – Incomplete,* 7 of the files were *Not Viewable* and 8 were *False Positives.*

Summary: In the presence of disordered fragmented files, the tool recovered only 1 viewable - complete file. An increased number of viewable - incomplete, not viewable and false positives were recovered.

Test: Fragmented Out of Order	Total Carved	Viewable Complete/minor alteration	Viewable Incomplete/major alteration	Not Viewable	False Positive
36 files	**50**	**1**	**34**	**7**	**8**
6 mp4	**8**		**5**	**3**	
1 ABC					
1 ACB	↳ *1*		↳ *1*		
1 BAC	↳ *2*		↳ *1*	↳ ***1***	
1 BCA	↳ *3*		↳ *1*	↳ ***1***	
1 CAB	↳ *1*		↳ *1*	↳ ***1***	
1 CBA	↳ *1*		↳ *1*		
6 mov	**19**		**11**		**8**
1 ABC					
1 ACB	↳ *3*		↳ *3*		
1 BAC	↳ *1*		↳ *1*		
1 BCA	↳ *2*		↳ *2*		
1 CAB					
1 *CBA*	↳ *5*		↳ *5*		
6 avi	**5**		**5**		
1 ABC					
1 ACB	↳ *1*		↳ *1*		
1 BAC	↳ *1*		↳ *1*		
1 BCA	↳ *1*		↳ *1*		
1 CAB	↳ *1*		↳ *1*		
1 *CBA*	↳ *1*		↳ *1*		
6 wmv	**6**		**6**		
1 ABC	↳		↳ *1*		
1 ACB	↳		↳ *1*		
1 BAC	↳		↳ *1*		
1 BCA	↳ ***1***		↳ ***1***		
1 CAB	↳ ***1***		↳ ***1***		
1 *CBA*	↳ ***1***		↳ ***1***		
6 3gp	**12**	**1**	**7**	**4**	
1 ABC	↳ *3*		↳ *2*	↳ *1*	
1 ACB	↳ *2*		↳ *1*	↳ *1*	

1 BAC	↳ *2*	↳ *1*	↳ *1*		
1 BCA	↳ *2*		↳ *1*	↳ *1*	
1 CAB	↳ *2*		↳ *1*	↳ *1*	
***1** CBA*	↳ *1*		↳ *1*		
6 ogv					
1 ABC					
1 ACB					
1 BAC					
1 BCA					
1 CAB					
***1** CBA*					
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

Video-braid_1401090830.dd contains a total of 24 files, 12 of which are contiguous and 12 fragmented files.

Out of the 24 video files a total of 36 files were carved – 8 of the carved files were *Viewable – Complete*, *16* of the files were *Viewable – Incomplete*, 7 of the files were *Not Viewable* and 5 were *False Positives*.

Summary: In the presence of braided files, the tool had a reduced ability to recover viewable – complete mov, avi and 3gp files. All wmv files were viewable-incomplete.

Test: Braided Pair	Total Carved	Viewable Complete/minor alteration	Viewable Incomplete/major alteration	Not Viewable	False Positive
24 files	**36**	**8**	**16**	**7**	**5**
4 mp4	**9**	**3**	**2**	**4**	
2 Contiguous	↳ ***1***	↳ ***3***		↳ ***4***	
2 Braided	↳ ***1***		↳ ***2***		
4 mov	**11**	**1**	**5**		**5**
2 Contiguous	↳ ***2***		↳ ***2***		
2 Braided	↳ ***4***	↳ ***1***	↳ ***3***		
4 avi	**4**	**1**	**3**		
2 Contiguous	↳ ***2***	↳ ***1***	↳ ***1***		
2 Braided	↳ ***2***		↳ ***2***		
4 wmv	**3**		**3**		
2 Contiguous	↳ ***1***		↳ ***1***		
2 Braided	↳ ***2***		↳ ***2***		
4 3gp	**9**	**3**	**3**	**3**	
2 Contiguous	↳ ***5***	↳ ***3***	↳ ***1***	↳ ***1***	
2 Braided	↳ ***4***		↳ ***2***	↳ ***2***	

4 ogv					
2 Contiguous					
2 Braided					
Full results are available at: **http://www.cftt.nist.gov/CFTT-Test-Run-Raw-Files.html**					

Table 6: Braided Pair

4.7 Byte Shifted

Video-shifted_1401090819.dd contains a total of 36 files, where all 36 files are contiguous files that have filler that ranges in size from 1, 3, 4, 5, 9, 16, 32 sectors where the files land on non-sector boundaries.

Out of the 36 video files a total of 23 files were carved – 19 of the carved files were *Viewable – Complete, 16* of the files were *Viewable – Incomplete, 9* of the files were *Not Viewable* and 6 were *False Positives.*

Summary: The presence of files not aligned to sector boundaries did not significantly impact the recovery of Viewable Complete files.

Test: Byte Shifted	Total Carved	Viewable Complete/minor alteration	Viewable Incomplete/major alteration	Not Viewable	False Positive
36 files	**50**	**19**	**16**	**9**	**6**
6 mp4	**9**	**3**	**1**	**5**	
6 mov	**17**	**3**	**8**		**6**
6 avi	**6**	**2**	**4**		
6 wmv	**6**	**5**	**1**		
6 3gp	**12**	**6**	**2**	**4**	
6 ogv					
Fu Full results are available at: **http://www.cftt.nist.gov/CFTT-Test-Run-Raw-Files.html**					

Table 7: Byte Shifted