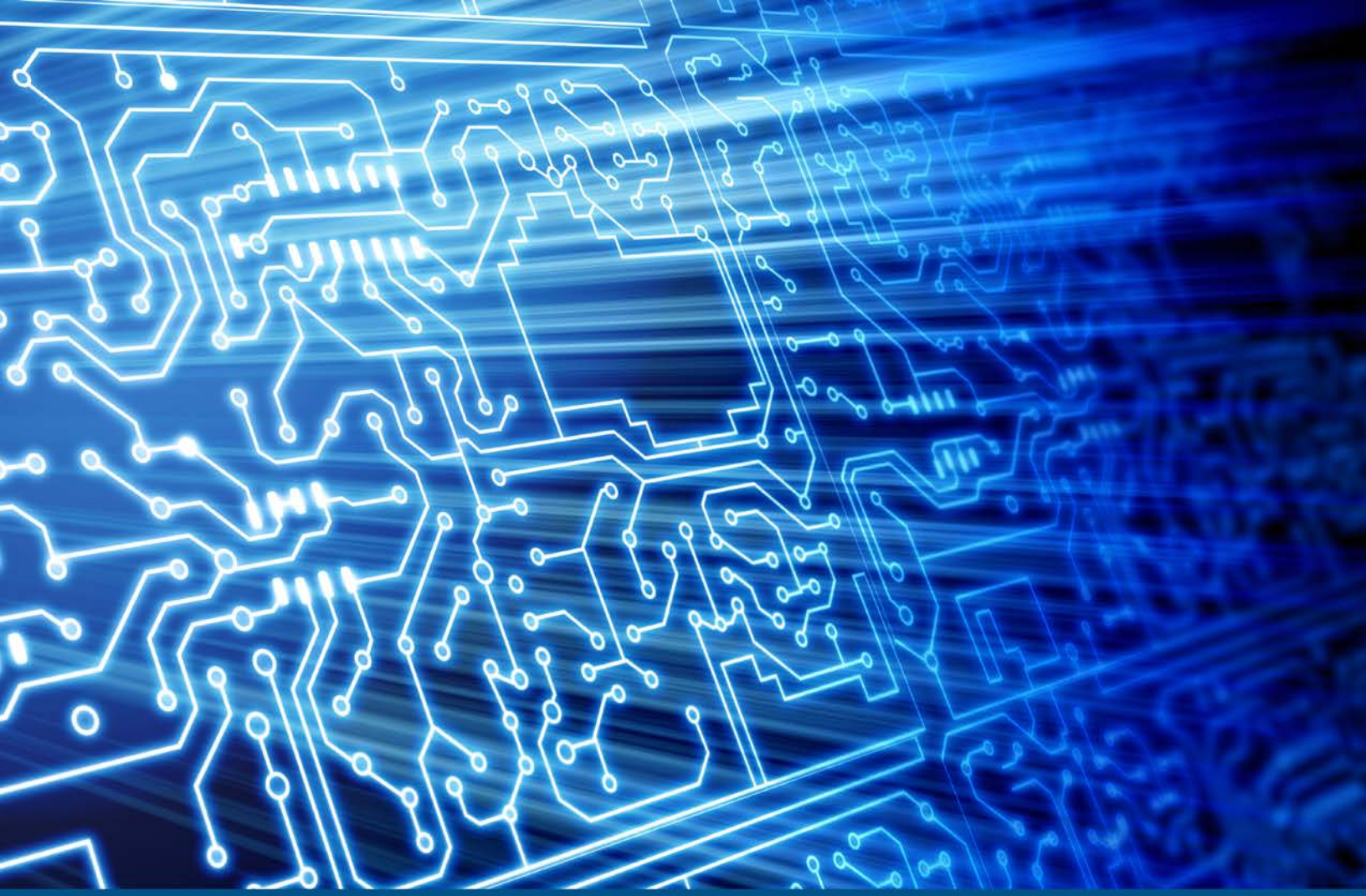

R-Studio v6.2

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:
R-Studio v6.2

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 R-Studio version 6.2 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 R-Studio v6.2 runs, see http://www.cftt.nist.gov/CFTT-Test-Run-Raw-Files.html.

Test Results for Digital Data File Carving Tool

Tool Tested:	R-Studio
Software Version:	v6.2
Supplier:	R-Tools Technology Inc.
Address:	10520 Yonge Street, Unit 35B, Suite 232 Richmond Hill, ON, L4C 3C7, CANADA
Tel:	1-888-9-RTTCOM (1-888-978-8266)
Fax:	1-240-525-7604
WWW:	http://www.r-tt.com/

1 Results Summary

Below are summaries on how R-Studio v6.2 performed when carving raw "dd" images containing various layouts of fragmentation and completeness.

R-Studio was most successful at carving mp4, avi, wmv, 3gp and ogv video files from no padding, braided pair and cluster padded "dd" images. Recovering video files from fragmented images (i.e., Simple, Partial, Disorderd) yielded an increase in *Viewable – Incomplete* and *Not Viewable* rankings. The Non-Sector boundary "dd" image containing a total of 36 files, recovered only 15 files all of which were classified as *False Positive*.

For more test result details see section 4.

2 Test Case Selection

R-Studio's ability to carve mp4, mov, avi, wmv, 3gp and ogv video files 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

R-Studio version 6.2 was installed on Windows XP v5.1.2600.

The default configuration settings were used for R-Studio.

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 classification time for files carved.

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 56 files were carved – 31 of the carved files were *Viewable – Complete*, 25 of the files carved were *Not Viewable.*

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

Test: No Padding	Total Carved	Viewable – Complete/minor alteration	Viewable – Incomplete/major alteration	Not Viewable	False Positive
36 files	**56**	**31**		**25**	
6 mp4	**6**	**6**			
6 mov	**1**	**1**			
6 avi	**6**	**6**			
6 wmv	**6**	**6**			
6 3gp	**6**	**6**			
6 ogv	**31**	**6**		**25**	
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 56 files were carved – 45 of the carved files were *Viewable – Complete*, 11 of the files carved were *Not Viewable.*

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

Test: Cluster Padded	Total Carved	Viewable – Complete/minor alteration	Viewable – Incomplete/major alteration	Not Viewable	False Positive
36 files	**56**	**45**		**11**	
6 mp4	**6**	**6**			
6 mov	**1**	**1**			
6 avi	**6**	**6**			
6 wmv	**6**	**6**			
6 3gp	**6**	**6**			
6 ogv	**31**	**20**		**11**	
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 56 files were carved, 10 files were *Viewable – Complete*, 12 files were *Viewable – Incomplete* and 34 files were *Not Viewable*.

Summary: In the presence of sequentially fragmented files, the tool had a reduced ability to recover files in a viewable complete state.

Test: Fragmented In Order	Total Carved	Viewable – Complete/minor alteration	Viewable – Incomplete/major alteration	Not Viewable	False Positive
36 files	**56**	**10**	**12**	**34**	
6 mp4	**6**	**2**	**4**		
2 Contiguous	↳ ***2***	↳ ***2***			
4 Frag w/fill	↳ ***4***		↳ ***4***		
6 mov	**1**			**1**	
2 Contiguous					
4 Frag w/fill	↳ ***1***			↳ ***1***	
6 avi	**6**	**2**	**4**		
2 Contiguous	↳ ***1***	↳ ***1***			
4 Frag w/fill	↳ ***5***	↳ ***1***	↳ ***4***		
6 wmv	**6**	**2**	**4**		
2 Contiguous	↳ ***2***	↳ ***2***			
4 Frag w/fill	↳ ***4***		↳ ***4***		
6 3gp	**6**	**3**		**3**	
2 Contiguous	↳ ***2***	↳ ***2***			
4 Frag w/fill	↳ ***4***	↳ ***1***		↳ ***3***	
6 ogv	**31**	**1**		**30**	
2 Contiguous	↳ ***11***	↳ ***1***		↳ ***10***	
4 Frag w/fill	↳ ***20***			↳ ***20***	
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 46 files were carved – 8 of the carved files were *Viewable – Complete*, 10 files were *Viewable - Incomplete*, and the remaining 28 files were *Not Viewable*.

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

Test: Incomplete	Total Carved	Viewable – Recovery of all available/minor alteration	Viewable – Incomplete/major alteration	Not Viewable	False Positive
36 files	**46**	**8**	**10**	**28**	
6 mp4	**5**	**2**	**3**		
3 Complete	↳ ***3***	↳ ***2***	↳ ***1***		
3 Partial	↳ ***2***		↳ ***2***		
6 mov	**1**			**1**	
3 Complete	↳ ***1***			↳ ***1***	
3 Partial					
6 avi	**5**	**2**	**3**		
3 Complete	↳ ***3***	↳ ***2***	↳ ***1***		
3 Partial	↳ ***2***		↳ ***2***		
6 wmv	**5**	**2**	**3**		
3 Complete	↳ ***3***	↳ ***2***	↳ ***1***		
3 Partial	↳ ***2***		↳ ***2***		
6 3gp	**5**	**2**	**1**	**2**	
3 Complete	↳ ***3***	↳ ***2***	↳ ***1***		
3 Partial	↳ ***2***			↳ ***2***	
6 ogv	**25**			**25**	
3 Complete	↳ ***20***			↳ ***20***	
3 Partial	↳ ***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

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 56 files were carved, 18 files were *Viewable - Incomplete,* and 38 were *Not Viewable.*

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

Test: Fragmented Out of Order	Total Carved	Viewable – Complete/minor alteration	Viewable – Incomplete/major alteration	Not Viewable	False Positive
36 files	**56**		**18**	**38**	
6 mp4	**6**		**6**		
1 ABC	↳ ***1***		↳ ***1***		
1 ACB	↳ ***1***		↳ ***1***		
1 BAC	↳ ***1***		↳ ***1***		
1 BCA	↳ ***1***		↳ ***1***		
1 CAB	↳ ***1***		↳ ***1***		
1 CBA	↳ ***1***		↳ ***1***		
6 mov	**1**			**1**	
1 ABC					
1 ACB					
1 BAC					
1 BCA					
1 CAB	↳ ***1***			↳ ***1***	
1 *CBA*					
6 avi	**6**		**6**		
1 ABC	↳ ***1***		↳ ***1***		
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***		
1 ACB	↳ ***1***		↳ ***1***		
1 BAC	↳ ***1***		↳ ***1***		
1 BCA	↳ ***1***		↳ ***1***		
1 CAB	↳ ***1***		↳ ***1***		
1 *CBA*	↳ ***1***		↳ ***1***		
6 3gp	**6**			**6**	
1 ABC	↳ ***1***			↳ ***1***	
1 ACB	↳ ***1***			↳ ***1***	
1 BAC	↳ ***1***			↳ ***1***	
1 BCA	↳ ***1***			↳ ***1***	
1 CAB	↳ ***1***			↳ ***1***	
1 *CBA*	↳ ***1***			↳ ***1***	
6 ogv	**31**			**31**	
1 ABC	↳ ***5***			↳ ***5***	
1 ACB	↳ ***6***			↳ ***6***	
1 BAC	↳ ***4***			↳ ***4***	
1 BCA	↳ ***11***			↳ ***11***	
1 CAB	↳ ***3***			↳ ***3***	
1 *CBA*	↳ ***2***			↳ ***2***	
Full results are available at: **http://www.cftt.nist.gov/CFTT-Test-Run-Raw-Files.html**					

Table 4: 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 39 files were carved – 12 of the carved files were *Viewable – Complete*, 10 files were *Viewable – Incomplete*, and the remaining files were *Not Viewable*.

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

Test: Braided Pair	Total Carved	Viewable – Complete/minor alteration	Viewable – Incomplete/major alteration	Not Viewable	False Positive
24 files	**39**	**12**	**10**	**17**	
4 mp4	**4**	**2**	**2**		
2 Contiguous	↳ ***2***	↳ ***2***			
2 Braided	↳ ***2***		↳ ***2***		
4 mov	**1**			**1**	
2 Contiguous					
2 Braided	↳ ***1***			↳ ***1***	
4 avi	**4**	**2**	**2**		
2 Contiguous	↳ ***2***	↳ ***2***			
2 Braided	↳ ***2***		↳ ***2***		
4 wmv	**4**	**2**	**2**		
2 Contiguous	↳ ***2***	↳ ***2***			
2 Braided	↳ ***2***		↳ ***2***		
4 3gp	**4**	**4**			
2 Contiguous	↳ ***2***	↳ ***2***			
2 Braided	↳ ***2***	↳ ***2***			
4 ogv	**22**	**2**	**4**	**16**	
2 Contiguous	↳ ***13***	↳ ***2***		↳ ***11***	
2 Braided	↳ ***9***		↳ ***4***	↳ ***5***	
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 15 files were carved – 15 of the carved files were *False Positives*.

Summary: The tool was unsuccessful at carving files landing on non-sector boundaries.

Test: Byte Shifted	Total Carved	Viewable – Complete/minor alteration	Viewable – Incomplete/major alteration	Not Viewable	False Positive
36 files	**15**				**15**
6 mp4					
6 mov					
6 avi					
6 wmv					
6 3gp					
6 ogv	**15**				**15**
Full results are available at: **http://www.cftt.nist.gov/CFTT-Test-Run-Raw-Files.html**					

Table 7: Byte Shifted