DEC. 2011

U.S. Department of Justice
Office of Justice Programs
National Institute of Justice

NIJ

Special REPORT

Test Results for Forensic Media Preparation Tool: dc3dd: Version 7.0.0

nij.gov

Office of Justice Programs
Innovation • Partnerships • Safer Neighborhoods
www.ojp.usdoj.gov

U.S. Department of Justice
Office of Justice Programs
810 Seventh Street N.W.
Washington, DC 20531

This and other publications and products of the National Institute of Justice can be found at:

National Institute of Justice
www.nij.gov

Office of Justice Programs
Innovation • Partnerships • Safer Neighborhoods
www.ojp.usdoj.gov

NIJ

DEC. 2011

Test Results for Forensic Media Preparation Tool: dc3dd: Version 7.0.0

NCJ 236225

NIJ

John Laub

Director, National Institute of Justice

This report was prepared for the National Institute of Justice, U.S. Department of Justice, by the Office of Law Enforcement Standards of the National Institute of Standards and Technology under Interagency Agreement 2003–IJ–R–029.

The National Institute of Justice is a component of the Office of Justice Programs, which also includes the Bureau of Justice Assistance, the Bureau of Justice Statistics, the Office of Juvenile Justice and Delinquency Prevention, and the Office for Victims of Crime.

July 2011

Test Results for Forensic Media Preparation Tool:
dc3dd: Version 7.0.0

National Institute of
Standards and Technology
U.S. Department of Commerce

Contents

Introduction

The Computer Forensics Tool Testing (CFTT) program is a joint project of the National Institute of Justice (NIJ), the Department of Homeland Security, and the National Institute of Standards and Technology's Law Enforcement Standards Office and Information Technology Laboratory. CFTT is supported by other organizations, including the Federal Bureau of Investigation, the U.S. Department of Defense Cyber Crime Center, the 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 forensic tools is based on well-recognized methodologies for conformance and quality testing. The specifications and test methods are posted on the CFTT Web site (http://www.cftt.nist.gov/) for review and comment by the computer forensics community.

This document reports the results from testing the wipe function of dc3dd version 7.0.0 against the *Forensic Media Preparation Tool Test Assertions and Test Plan Version 1.0,* available at the CFTT Web site (http://www.cftt.nist.gov/fmp-atp-pc-01.pdf).

Test results for other devices and software packages using the CFTT tool methodology can be found on NIJ's CFTT Web page, http://www.nij.gov/nij/topics/forensics/evidence/digital/standards/cftt.htm.

How to Read This Report

This report is divided into four sections. The first section is a summary of the results from the test runs and is sufficient for most readers to assess the suitability of the tool for the intended use. The remaining sections of the report describe how the tests were conducted and provide documentation of test case details that support the report summary. Section 2 gives the selection of each test case from the set of possible cases defined in the test plan for forensic media preparation tools. The test cases are selected, in general, based on features offered by the tool. Section 3 lists hardware and software used to run the test cases with links to additional information about the items used. Section 4 contains a description of each test case listing all test assertions that apply, their expected results and the actual result. Please refer to the vendor's owner manual for guidance on using the tool.

Test Case FMP-03-DCO DC3DD Version 7.0

Highlights:

```
dc3dd 7.0.0 started at 2011-02-25 08:11:18 -0500
compiled options: DEFAULT_HASH_MD5 (hash=md5) DEFAULT_HASH_SHA1 (hash=sha1)
DEFAULT_VERBOSE_REPORTING (verb=on)
command line: dc3dd wipe=/dev/sda pat=b9 log=tool-log.txt
device size: 480234752 sectors (probed)
sector size: 512 bytes (probed)
245880193024 bytes (229 G) copied (100%), 5030.42 s, 47 M/s

input results for pattern `b9':
   480234752 sectors in
   928402193b64b55e541655443d704f95 (md5)
   228e308df669884aa7a11eb625f7be0c8c875d50 (sha1)

output results for device `/dev/sda':
   480234752 sectors out

dc3dd completed at 2011-02-25 09:35:09 -0500

======== dc3dd tool log (end) ===========
Size after tool runs: 480234752 from total of 490234752 (with 10000000
hidden)
Analysis of tool result --

Sector 480234752 is first sector with printable text
============= Start text =============
29893/058/54 000480234752**********************************
**************************************************************
**************************************************************
**************************************************************
**************************************************************
**************************************************************
**************************************************************
**************************************************************
******************************
============= End text Sector 480234752 =============
9 <new line> characters inserted for readability

Totals for all sectors
summary format: <count> <hex value> <(actual character if printable)> ...
    10000000 00         10000000 20 ( )   4860000000 2A (*)
    20000000 2F (/)     57509778 30 (0)     19475822 31 (1)
    19331121 32 (2)     23757753 33 (3)     25317978 34 (4)
    13723905 35 (5)     12312621 36 (6)     11677634 37 (7)
    21551073 38 (8)     15342315 39 (9) 245880193024 B9
Totals for non-ASCII sectors
summary format: <count> <hex value> <(actual character if printable)> ...
245880193024 B9

251000193024 bytes, 490234752 sectors, 15 distinct values seen
10000000 sectors have printable text



    Runs of Sectors Unchanged or Overwritten
First Sector      Last Sector      State
           0 --    480234751   Overwritten
   480234752 --    490234751   Unchanged
```

Results:

Assertion & Expected Result	Actual Result
FMP-CA-01 Visible sectors overwritten	as expected
FMP-AO-01 Hidden sectors overwritten	DCO not overwritten
FMP-AO-02 Hidden area final state is	in place

Analysis: Expected results not achieved

2.6.9 FMP-03-DCO-HPA

Test Case FMP-03-DCO-HPA DC3DD Version 7.0	
Case Summary:	FMP-03. Overwrite hidden sectors using WRITE commands.
Assertions:	FMP-CA-01 All visible sectors shall be overwritten with the specified benign data. FMP-AO-01 If there is a hidden area present and the tool supports overwriting sectors contained in a hidden area, then all sectors contained in the hidden area shall be overwritten with the specified benign data. FMP-AO-02 A hidden area may optionally be removed from the storage device.
Tester Name:	csr
Analysis host:	frank
Test host:	frank
Test date:	Mon Mar 14 12:13:26 2011
Test drive:	1C-SATA
Source Setup:	Size with DCO: 224441648 114.91 GB (10000000 sectors in DCO) Size with HPA: 209441648 107.23 GB (15000000 sectors in HPA) Initial setup size: 209441648 from total of 234441648 (with 25000000 hidden) IDE disk: Model (WDC WD1200JD-00GBB0) serial # (WD-WMAES2049679) Sector 0 is first sector with printable text ============= Start text ============= 00000/000/01 000000000000 ============= End text Sector 0 ============= 1 <new line> character inserted for readability Totals for all sectors summary format: <count> <hex value> <(actual character if printable)> ... 224441648 00 109078640928 1C 224441648 20 ( ) 448883296 2F (/) 1412016107 30 (0) 648943731 31 (1) 464424111 32 (2) 386665415 33 (3) 366881143 34 (4) 361115515 35 (5) 335339466 36 (6) 320942106 37 (7) 320928507 38 (8) 320460155 39 (9) Totals for non-ASCII sectors summary format: <count> <hex value> <(actual character if printable)> ... 114914123776 bytes, 224441648 sectors, 14 distinct values seen 224441648 sectors have printable text
Tool Settings:	type: wipe pattern: 'b9'
Log Highlights:	======== dc3dd tool log (start) =========== dc3dd 7.0.0 started at 2011-03-15 03:36:36 -0400 compiled options: DEFAULT_HASH_MD5 (hash=md5) DEFAULT_HASH_SHA1 (hash=sha1) DEFAULT_VERBOSE_REPORTING (verb=on) command line: dc3dd wipe=/dev/sda pat=b9 log=tool-log.txt device size: 224441648 sectors (probed) sector size: 512 bytes (probed) 114914123776 bytes (107 G) copied (100%), 2533.24 s, 43 M/s input results for pattern `b9': 224441648 sectors in 2a78258b6331e8868d6e1fbd7ca00162 (md5) adb6bad83ee5b8243781352a7f1e7f6f07251522 (sha1)  output results for device `/dev/sda': 224441648 sectors out dc3dd completed at 2011-03-15 04:18:49 -0400 ======== dc3dd tool log (end) =========== Size after tool runs: 209441648 from total of 234441648 (with 25000000 hidden)

Test Case FMP-03-DCO-HPA DC3DD Version 7.0	
	Analysis of tool result -- Sector 224441648 is first sector with printable text ============= Start text ============= 13970/215/54 000224441648 ============= End text Sector 224441648 ============= 1 <new line> character inserted for readability Totals for all sectors summary format: <count> <hex value> <(actual character if printable)> ... 10000000 00 4860000000 1C 10000000 20 ( ) 20000000 2F (/) 49069416 30 (0) 29395570 31 (1) 33193387 32 (2) 20376376 33 (3) 24834191 34 (4) 14959713 35 (5) 12311991 36 (6) 11824119 37 (7) 11837150 38 (8) 12198087 39 (9) 114914123776 B9 Totals for non-ASCII sectors summary format: <count> <hex value> <(actual character if printable)> ... 114914123776 B9 120034123776 bytes, 234441648 sectors, 15 distinct values seen 10000000 sectors have printable text Runs of Sectors Unchanged or Overwritten First Sector Last Sector State 0 -- 224441647 Overwritten 224441648 -- 234441647 Unchanged
Results:	**Assertion & Expected Result** / **Actual Result** FMP-CA-01 Visible sectors overwritten / as expected FMP-AO-01 Hidden sectors overwritten / DCO not overwritten FMP-AO-02 Hidden area final state is / in place
Analysis:	Expected results not achieved

2.6.10 FMP-03-HPA

Test Case FMP-03-HPA DC3DD Version 7.0	
Case Summary:	FMP-03. Overwrite hidden sectors using WRITE commands.
Assertions:	FMP-CA-01 All visible sectors shall be overwritten with the specified benign data. FMP-AO-01 If there is a hidden area present and the tool supports overwriting sectors contained in a hidden area, then all sectors contained in the hidden area shall be overwritten with the specified benign data. FMP-AO-02 A hidden area may optionally be removed from the storage device.
Tester Name:	csr
Analysis host:	frank
Test host:	frank
Test date:	Tue Mar 1 14:07:24 2011
Test drive:	53-IDE
Source Setup:	Initial setup size: 297581808 from total of 312581808 (with 15000000 hidden) IDE disk: Model (WDC WD1600JB-00GVC0) serial # (WD-WMAL94865344) Sector 0 is first sector with printable text ============= Start text ============= 00000/000/01 000000000000SSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSS SSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSS SSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSS SSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSS SSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSS SSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSS SSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSS SSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSS SSSSSSSSSSSSSSSSSSSSSSSSSSSSSSS

Test Case FMP-03-HPA DC3DD Version 7.0

```
============= End text Sector 0 =============
9 <new line> characters inserted for readability

Totals for all sectors
summary format: <count> <hex value> <(actual character if printable)> ...
   312581808 00        312581808 20 ( )    625163616 2F (/)
  1850492169 30 (0)    906528227 31 (1)    696435016 32 (2)
   541016511 33 (3)    522787395 34 (4)    514450557 35 (5)
   478352540 36 (6)    458495114 37 (7)    458481159 38 (8)
   449761088 39 (9) 151914758688 53 (S)
Totals for non-ASCII sectors
summary format: <count> <hex value> <(actual character if printable)> ...

160041885696 bytes, 312581808 sectors, 14 distinct values seen
312581808 sectors have printable text
```

Tool Settings:

```
type: wipe
pattern: none
```

Log Highlights:

```
======== dc3dd tool log (start) ===========

dc3dd 7.0.0 started at 2011-03-01 10:16:53 -0500
compiled options: DEFAULT_HASH_MD5 (hash=md5) DEFAULT_HASH_SHA1 (hash=sha1)
DEFAULT_VERBOSE_REPORTING (verb=on)
command line: dc3dd wipe=/dev/sda log=tool-log.txt
device size: 312581808 sectors (probed)
sector size: 512 bytes (probed)
160041885696 bytes (149 G) copied (100%), 3109.05 s, 49 M/s

input results for pattern `00':
   312581808 sectors in
   26e628892c9cbb7bd4936d180f43b67d (md5)
   a44050d78408a43e8dddc68ad90857686096fd76 (sha1)

output results for device `/dev/sda':
   312581808 sectors out

dc3dd completed at 2011-03-01 11:08:42 -0500

======== dc3dd tool log (end) ===========
Size after tool runs: 297581808 from total of 312581808 (with 15000000
hidden)
Analysis of tool result --
Totals for all sectors
summary format: <count> <hex value> <(actual character if printable)> ...
160041885696 00
Totals for non-ASCII sectors
summary format: <count> <hex value> <(actual character if printable)> ...
160041885696 00

160041885696 bytes, 312581808 sectors, 1 distinct values seen
No sectors have printable text


    Runs of Sectors Unchanged or Overwritten
First Sector      Last Sector      State
           0 --    312581807   Overwritten
```

Results:

Assertion & Expected Result	Actual Result
FMP-CA-01 Visible sectors overwritten	as expected
FMP-AO-01 Hidden sectors overwritten	as expected
FMP-AO-02 Hidden area final state is	in place

Analysis: Expected results achieved

About the National Institute of Justice

A component of the Office of Justice Programs, NIJ is the research, development and evaluation agency of the U.S. Department of Justice. NIJ's mission is to advance scientific research, development and evaluation to enhance the administration of justice and public safety. NIJ's principal authorities are derived from the Omnibus Crime Control and Safe Streets Act of 1968, as amended (see 42 U.S.C. §§ 3721–3723).

The NIJ Director is appointed by the President and confirmed by the Senate. The Director establishes the Institute's objectives, guided by the priorities of the Office of Justice Programs, the U.S. Department of Justice, and the needs of the field. The Institute actively solicits the views of criminal justice and other professionals and researchers to inform its search for the knowledge and tools to guide policy and practice.

Strategic Goals

NIJ has seven strategic goals grouped into three categories:

Creating relevant knowledge and tools

1. Partner with state and local practitioners and policymakers to identify social science research and technology needs.
2. Create scientific, relevant, and reliable knowledge—with a particular emphasis on terrorism, violent crime, drugs and crime, cost-effectiveness, and community-based efforts—to enhance the administration of justice and public safety.
3. Develop affordable and effective tools and technologies to enhance the administration of justice and public safety.

Dissemination

4. Disseminate relevant knowledge and information to practitioners and policymakers in an understandable, timely and concise manner.
5. Act as an honest broker to identify the information, tools and technologies that respond to the needs of stakeholders.

Agency management

6. Practice fairness and openness in the research and development process.
7. Ensure professionalism, excellence, accountability, cost-effectiveness and integrity in the management and conduct of NIJ activities and programs.

Program Areas

In addressing these strategic challenges, the Institute is involved in the following program areas: crime control and prevention, including policing; drugs and crime; justice systems and offender behavior, including corrections; violence and victimization; communications and information technologies; critical incident response; investigative and forensic sciences, including DNA; less-than-lethal technologies; officer protection; education and training technologies; testing and standards; technology assistance to law enforcement and corrections agencies; field testing of promising programs; and international crime control.

In addition to sponsoring research and development and technology assistance, NIJ evaluates programs, policies, and technologies. NIJ communicates its research and evaluation findings through conferences and print and electronic media.

To find out more about the National Institute of Justice, please visit:

www.nij.gov

or contact:

National Criminal Justice
Reference Service
P.O. Box 6000
Rockville, MD 20849–6000
800–851–3420
http://www.ncjrs.gov