available at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/diin

Digital Investigation

Issues with imaging drives containing faulty sectors☆

*James R. Lyle**, *Mark Wozar*

National Institute of Standards and Technology, 100 Bureau Drive Stop 8970, Gaithersburg, MD 20899-8970, United States

Keywords:
Acquisition of digital data
Hard drive imaging
Iximager
Testing forensic tools
Faulty sectors
Linux
FreeBSD
DCFLdd
DCCIdd
dd

ABSTRACT

In the ideal situation when imaging a hard drive, all sectors are completely and accurately acquired and saved to an image file. In reality, occasionally drives will contain faulty sectors such that the original content of the faulty sector cannot be acquired with typical imaging tools. We report on several experiments using non-commercial imaging tools and their behavior when encountering faulty sectors on a hard drive. Investigators should be aware of some behaviors exhibited by the tools that we examined. For example, some accessible sectors adjacent to a faulty sector may be missed when imaged directly from the ATA interface. In addition, more sectors were missed adjacent to the faulty sector when a drive was imaged over the firewire interface using a write blocker.

1. Introduction

In the ideal situation when imaging a hard drive, all sectors are completely and accurately acquired and saved to an image file. In reality, occasionally drives will contain faulty sectors such that the original content of the faulty sector cannot be acquired with typical imaging tools. Imaging tools should meet the following requirements for handling faulty sectors:

1. acquire all sectors that are not faulty,
2. identify all faulty sectors, and
3. for sectors in the image file corresponding to the faulty sectors, replace the faulty sector content with *benign fill*, i.e., data that would have no influence on the results of an investigation.

A more formal statement of these requirements can be found in National Institute of Standards and Technology (2004).

This paper reports on several experiments using non-commercial imaging tools and their behavior when encountering faulty sectors on a hard drive. Our experiments used three *reliably faulty* hard drives. A reliably faulty hard drive has a set of known consistently faulty sectors. These drives can be imaged repeatedly with the same set of sectors reporting failure. The following imaging tools were used in the experiment:

- DCCIdd V 2.0,
- DCFLdd V 1.3.4,
- dd on Helix with Linux kernel 2.6.14,
- dd on FreeBSD V 5.5, and
- IXimager V 2.0 February 1, 2006.

The purpose of this work is to develop testing methodologies and document tool behavior (i.e., encountering hard drives containing faulty sectors) as part of The Computer Forensics Tool Testing (CFTT) Project at the National Institute of Standards and Technology. The CFTT project is responsible for developing methodologies for testing forensic tools and related devices. The Computer Forensics Tool Testing (CFTT) project is a joint project of the National Institute of Justice

☆ Certain trade names and company products are mentioned in the text or identified. In no case does such identification imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the products are necessarily the best available for the purpose.

* *Corresponding author.*
E-mail addresses: jlyle@nist.gov (J.R. Lyle), mark.wozar@nist.gov (M. Wozar).

1742-2876/$ – see front matter © 2007 DFRWS. Published by Elsevier Ltd. All rights reserved.
doi:10.1016/j.diin.2007.06.002

(NIJ), the research and development organization of the U.S. Department of Justice (DOJ), and the National Institute of Standards and Technology's (NIST's) Office of Law Enforcement Standards (OLES) and Information Technology Laboratory (ITL). CFTT is supported by other organizations, including the Federal Bureau of Investigation (FBI), the U.S. Department of Defense Cyber Crime Center (DC3), U.S. Internal Revenue Service Criminal Investigation Division Electronic Crimes Program (IRS-CID), and the U.S. Department of Homeland Security's (DHS) Bureau of Immigration and Customs Enforcement (ICE) and U.S. Secret Service (USSS). The objective of the CFTT project is to provide measurable assurance to practitioners, researchers, and other applicable users that 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. This 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.

2. Reliably faulty test drives

Three reliably faulty ATA interface test drives were used to reveal imaging tool behaviors. The drive system area was manipulated to create a set of faulty sectors. The drives are designated: MAX1 with 54 faulty sectors, Max2 with 398 faulty sectors and WD with 22 faulty sectors. For each faulty drive a reference drive was also prepared with identical content except for the faulty sectors.

3. Methodology

Twelve experimental runs were performed using the five tools and the three test drives. Nine of the runs used the firewire interface through a write blocker, three of the runs were over the ATA interface without a write blocker. Each run followed the following steps:

1. clone the faulty drive to another drive (the clone), and
2. compare the clone to the reference drive corresponding to the faulty drive.

For the dd based commands, the options selected were: `bs=512 conv=sync,noerror`.

3.1. Results

Table 1 presents the results for each test. The column labeled *N* indicates the number of readable sectors not acquired, a value of zero indicates that all sectors were acquired except for the actual faulty sectors. IXimager and FreeBSD dd acquired all sectors that were not faulty. Comparing dd based tools, more sectors were acquired over the ATA interface than over the firewire interface.

Table 1 – Number of sectors not acquired

Tool	Drive	Block	Bus	N
IXimager	MAX1	Block	FW 800	0
HELIX dd	MAX1	Block	FW 800	5034
DCFLdd	MAX1	Block	FW 800	5034
DCCIdd	MAX1	None	ATA	306
BSD dd	MAX1	Block	FW 800	0
IXimager	MAX2	Block	FW 800	0
HELIX dd	MAX2	Block	FW 800	40,802
DCFLdd	MAX2	None	ATA	2266
DCCIdd	MAX2	None	ATA	2266
BSD dd	MAX2	Block	FW 800	0
IXimager	WD	Block	FW 800	0
DCCIdd	WD	Block	FW 800	546

On closer examination we found that for the dd based tools each faulty sector was embedded in a run of sectors that was not acquired. Table 2 shows the layout of the first five runs for each of the tools on the faulty drive MAX1. Results are similar for the other two drives.

The testing procedures have produced the following observations. For IXimager and FreeBSD dd all the run lengths are one, i.e., only the faulty sectors were not obtained. Second,

Table 2 – MAX1 runs of sectors not acquired

Range	Length
BSD dd (FW 800)	
10069095–10069095	1
10069911–10069911	1
12023808–12023808	1
18652594–18652594	1
18656041–18656041	1
DCCIdd (ATA)	
10069088–10069095	8
10069904–10069911	8
12023808–12023815	8
18652592–18652599	8
18656040–18656047	8
DCFLdd (FW 800)	
10068928–10069095	168
10069696–10069911	216
12023744–12023815	72
18652352–18652599	248
18655936–18656047	112
dd (FW 800)	
10068928–10069095	168
10069696–10069911	216
12023744–12023815	72
18652352–18652599	248
18655936–18656047	112
IXimager (FW 800)	
10069095–10069095	1
10069911–10069911	1
12023808–12023808	1
18652594–18652594	1
18656041–18656041	1

for imaging directly to the ATA interface with dd based tools the run length for a single, isolated faulty sector was eight sectors. Lastly, for imaging with dd over the firewire interface, the run lengths associated with a single, isolated faulty sector were a multiple of eight sectors.

Examination of the content of the sectors on the clone drive revealed the following tool behaviors:

- IXimager filled the sectors with the string: `ILookImager_Bad_Sector_No_Data`.
- All the tools running in the Linux environment filled the sectors with zeros (NULL bytes).
- The sectors created by dd running in FreeBSD contained data from an undetermined source.

4. Conclusions

We observed the following behaviors that may be of concern for imaging tools operating on drives with faulty sectors:

- Up to seven accessible sectors adjacent to a faulty sector may be missed when imaged with dd based tools in the Linux environment directly from the ATA interface.
- For imaging with dd over the firewire interface, the length of runs of missed sectors associated with a single, isolated faulty sector was a multiple of eight sectors.
- The source of the content used to replace the sectors not acquired was undetermined in the FreeBSD environment.

5. Future work

This paper presents observations for a limited set of tools and interfaces. The work could be continued to address the following issues:

- Additional interfaces such as SATA and USB.
- Impact of faulty sectors on acquisition time.
- A better understanding of the run length of good sectors not acquired adjacent to a faulty sector.
- Investigation of the content used to replace the sectors not acquired was undetermined in the FreeBSD environment.
- Investigation of the behavior of other imaging tools and run environments.

REFERENCES

National Institute of Standards and Technology. Digital data acquisition tool specification (draft 1 of version 4.0, October 4, 2004), <http://www.cftt.nist.gov/Pub-Draft-1-DDA-Require.pdf>.

James R. Lyle, Computer Scientist

Dr. Lyle is currently the project leader for the Computer Forensics Tool Testing (CFTT) project at the National Institute of Standards and Technology (NIST). He wrote his first FORTRAN program in 1968 and has been programming ever since. He received a B.S. in Mathematics (1972) and an M.S. in Mathematics (1975) from East Tennessee State University; from the University of Maryland at College Park, he received an M.S. (1982) and PhD (1984) in Computer Science.

Before joining NIST full time in 1993, Dr. Lyle was a Faculty Associate at NIST and an Assistant Professor at the University of Maryland, Baltimore County.

Mark Wozar, Computer Scientist

Mr. Wozar is currently a member of the Computer Forensics Tool Testing (CFTT) project at the National Institute of Standards and Technology (NIST).