available at www.sciencedirect.com

ScienceDirect

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

Digital Investigation

Recovering erased digital evidence from CD-RW discs in a child exploitation investigation

James Wardwell[a], *G. Stevenson Smith*[*,b]

[a]*Computer Forensic Unit, New Britain Police Department, United States*
[b]*Southeastern Oklahoma State University, School of Business, Durant, OK 74701, United States*

ARTICLE INFO

Article history:
Received 24 January 2008
Received in revised form
16 June 2008
Accepted 16 June 2008

Keywords:
Digital evidence
EnCase
Criminal investigation
CD-RW discs
Child exploitation

ABSTRACT

The paper describes an innovative method used to recover digital images and videos from an evidentiary CD-RW disc that had been erased. The digital evidence had been erased by the subject of the investigation in an attempt destroy incriminating evidence of the crime. Without the recovery of the digital evidence, there would have been no conviction in the child exploitation case as there was no physical or testimonial evidence.

For many tech-savvy criminals, the Internet has become a highway of criminal opportunity. Crimes such as identity theft, Nigerian letter scams and its variants, spam, botnet extortion attacks, counterfeit checks or postal orders, pharming, pump and dump stock schemes, advance fee frauds, and numerous fake e-mails are used to support financial crimes that net criminals millions of dollars. All these Internet crimes tend to be committed by criminals with well-developed technological skills. Another common characteristic among virtual criminals are their attempts to hide any digital evidence of their activities. This paper examines such an attempt by one criminal to destroy the digital evidence depicting his crimes. This criminal investigation and subsequent sentencing was based on the recovery of digital evidence. This paper describes the innovative recovery method used to find digital evidence of criminal activity on a CD-RW disc. Prior to describing the method used to recover digital evidence, CD-RW discs are briefly explained followed by an overview of U.S. laws affecting this criminal case.

1. Recording data on CD-RW discs

Data on a CD-RW disc can be recorded, erased, and rewritten. As such these discs have properties that are slightly different than CDs or CD-Rs and other discs. When an attempt is made to forensically recover data from recordable media, it is important to be familiar with its unique characteristics. Therefore, a brief description of those characteristics is presented here for CD-RW discs.

Recording data on CD-RW discs is done with a laser. The laser follows a spiral pattern as it linearly writes on a layer of metallic alloy that can be erased and then rewritten over again. CD-RW discs consist of a six-layer design. A polycarbonate plastic substrate with a spiral groove beginning on

* *Corresponding author*. Tel.: +1 580 745 2490; fax: +1 580 745 7485.
E-mail address: sgsmith@sosu.edu (G.S. Smith).
1742-2876/$ – see front matter © 2008 Elsevier Ltd. All rights reserved.
doi:10.1016/j.diin.2008.06.002

the inside central and stretching to the outside edge is covered with a dielectric layer of zinc sulfide and silicon dioxide. On top of this dielectric layer is a phase changing alloy, followed by another dielectric layer and a thin alloy reflective layer. A protective lacquer coat is place on top of the other five layers on the disc. The metallic alloy on the disc is covered by a top layer of clear lacquer and a second reflective aluminum layer (indium, silver, tellurium and antimony). The metallic alloy contains the information that is read by the output device as music, videos, or documents. When the laser records data on a disc, a temperature of between 500 and 700 °C is reached, and it changes the chemical structure of the alloy through liquefaction. Liquefaction causes the alloy to lose its highly reflective composition and develop a less reflective state. Once data is recorded on a disc, the disc's format changes to show a pattern of reflective surfaces, called lands, and less reflective surfaces called pits. The disc reader distinguishes the differences in the reflective quality on the disc and turns the results into binary data composed of zeros and ones. Once the binary data is processed, it is turned into information. With re-writable discs, the less reflective metallic alloy can be changed back to a less reflective state, through erasure, where it becomes more reflective again; thus indicating that no data is stored at that point. A full erasure is done as the laser scans the entire disc at a lower power level (200 °C) and changes the alloy, containing data, back to a reflective state. CD-RW discs hold approximately 700 MB of data. The data on re-writable discs has a limited life; therefore, forensic evidence needs to be collected within about 6 months otherwise the data may become degraded (Crowley, 2007).

ISO9660 is used as the standard for the CDs and RW-CDs disc creation, directory structure, and international compatibility. These standards are published by the International Organization for Standardization in Geneva, Switzerland. ISO9660 standardized the logic layout and logic record extensions on CD ROM media.[1] The descriptor information is likely to include the creation date of the disc, time zone information, the software used to create the disc, and file modification information.

The logical record on the disc shows the layout location of files and provides the control information related to the disc. CDs are divided into sections with 2352 bytes of audio data or 2048 bytes of data in each sector. On a disc, a track is a group of sectors that are written to at one time. One example of a track is the border zone containing the content information about the disc, i.e., whether it is music or videos for example. Sessions are a group of these tracks recorded at the same time, and the table of contents (TOC) records the start address for the session on the disc. One example of a session is the table of contents (TOC) which contains track information such as type of track (music or video), session number, and start address location. Each session contains a TOC, and if the drive cannot read the TOC, it will not recognize the disc. On CDs, the TOC is contained on the disc's *lead in* which is a reserved section on the disc that provides identification information to the drive about the disc.

When a quick erase of a CD-RW disc is made, it does not delete the information on the disc, i.e., the lands and pits, it only deletes the logic directory information on the disc showing the disc sectors are available for re-writing. All references to tracks and sessions are deleted making the disc inaccessible by the drive. When the disc is placed in the CD drive, the driver reads the disc as being empty, and it will not read the disc. Only a full erase on a disc will eliminate all information stored on that disc.

2. U.S. child pornography and abuse laws

In the United States, child pornography laws are in effect at both the Federal and state levels. At the Federal level, child pornography is defined as possessing images of children under the age of 18 who are engaged in sexually explicit conduct. Such images are considered illegal contraband.[2] Under the statutes, it is not necessary for the image to show sexual activity only sexually suggestive material. The 1996 Child Pornography Prevention Act, banned "virtual child pornography," and criminalized the use of computer-generated images or virtual representations of minors engaged in sexually explicit acts.[3] The law banned the "production" and possession of such images. These laws cover the possession of visual images contained in photographs, videotapes, and electronic data stored on CDs, hard drives, DVD, etc. Such crimes are prosecuted under sexual abuse or possession of child pornography statutes. Penalties under the statutes include financial restitution, forfeitures, and incarceration. States have the right to ban sexual abuse or possession of child pornography in their own statutes as well. In Connecticut, where this case occurred, the state statues include laws against the possession of child pornography and child sexual assault.[4] Sexual predators can be prosecuted under Federal or state laws. The prosecution can be for the possession of child pornography, or if they are involved in the production of these images, then the prosecution can be based on the sexual abuse of the child, which is a more serious crime.

3. The Kaminski case

The case began in February 2004, with a complaint to the New Britain Police Department regarding the possible sexual exploitation of a 14-year old female. The 14-year old girl had semi-nude pictures of herself that had been taken by John Kaminski, a family friend. After an initial inquiry and understanding the seriousness of Kaminski's actions, a police investigation into the complaint was initiated. A search warrant was executed on Kaminski's home. The search resulted in the confiscation of a digital camera, home computer, CDs, and CD-RW discs. After examining the electronic evidence, it was apparent that Kaminski erased much of the data on the

[1] *Rock Ridge* and *Joliet* are two extensions of this ISO.

[2] 18 U.S.C. §2256. Specifically Sections 1, 2, and 8.

[3] 18 U.S.C. §2256.

[4] Conn. Gen. Stat. Ann. §53a-70, § 53a-196, and §54-193.