

Forensic analysis of digital copiers

Svein Yngvar Willassen, M.Sc,
Investigation Manager, Computer Forensics, Ibas AS

Abstract

Many modern digital copiers store copied and printed information on internal hard drives. Such information may have value as evidence. In order to test the possibilities for evidence extraction from copiers, two digital copiers containing hard drives were dismantled and forensically analyzed. The analysis shows that it is possible to retrieve exact copies of documents that has previously been copied and/or printed on digital copiers. The analysis method is evaluated and found to be applicable on most digital copiers containing hard drives, unless special precautions have been taken to protect the stored material. The ability to retrieve documents that have previously been printed or copied on digital copiers is valuable within forensics, but also raises new questions within information security.

1.0 Introduction

Many aspects of life and business rely on documents. For a long time, document copiers have been a very important tool in most offices. Due to the advances in information technology, modern copiers are digital, processing the documents in digital form. The digital data are intermediary stored on digital memory, like volatile semiconductor memories or hard drives. Of these, the latter have become more and more common, due to their pricing and availability in the market. Implementing a hard drive in a copier also enables the use of an advanced real time operating system in the copier, with files stored on the drive. Such systems make it possible to use a copier as a printer, fax, scanner as well as a whole range of new functions.

A hard drive is however non-volatile. The information stored on a hard drive can be retrieved after a shutdown. With most filesystem, it is even possible to retrieve information that has been deleted. The fact that many modern digital copiers use hard drives for intermediary storage inspired us to perform a test to see if we could retrieve information from the hard drive in a copier. The goal was to retrieve copies of documents that had previously been printed and copied on the copier. To perform this test, we did an analysis of two digital copiers, Xerox DC432ST and Canon iR 2200.

2.0 Analysis of Canon iR 2200

2.1 System overview



The Canon iR2200 in detail

The Canon iR2200 is one of the cheaper models in the Canon ImageRunner series. The layout of the copier is shown in fig. The copier consist of a main unit containing all the electronics, and several add-on units handling paper storage and feeding and extra functions such as stapling. On the top of the main unit, a paper feeder is mounted that allows the copier to copy (or scan for other purposes) more than one paper sheet at once.

The technical specifications of the machine is listed in a brochure [], that can be downloaded from Canon and several of it's resellers. The specifiactions state that the copier image memory is 128 Mb RAM, and a 5.1 Gb HDD, with a maximum capacity of approximately 4000 originals. The copier is able to produce up to 999 copies of any original.

The copier is operated by using a touch-screen located on the top of the main unit, just below the paper feeder. This touch screen contains text and graphical element and is clearly driven by an internal microprocessor running an internal operating system. By operating the touch-screen, the copier can be used to perform a number of different functions related to documents, such as copying, scanning documents, printing and faxing documents, if a additional fax unit is connected to the system. Documents can be printed from a computer via an ethernet cable directly connected to the copier. Conversely, scanned documents can be made available across a computer network.

2.2 Dismantling the machine

With the knowledge that the copier contained a hard-drive, we sought to dismantle the copier in order to be able to retrieve the drive. This proved to be quite easy. By operating from the back of the main unit and removing the back-cover of the copier by unscrewing the 2 screws holding it, the main electronics of the copiers get exposed. The hard drive, a standard ATA 2 ½ " drive was at this point clearly visible. The drive was easily removed by unscrewing the one screw mounting it, and removing the cables from it.

2.3 Hard drive imaging

In order to be able to perform analysis of the system, the hard drive was imaged. The system contained a standard 2 ½ " ATA hard drive of size 5.6 Gb. The drive was easily imaged using EnCase 3.20 through a writer blocker on a standalone computer.

The copier in question was not a piece of actual evidence. It was therefore decided to produce a testbed for the further analysis. The copier was therefore reassembled, and a stack of 20 sheets of paper with known content was copied. After this, the copier was dismantled again and another image copy of the hard drive was made. The copier could now be reassembled and resume its normal operation.

2.4 File system recovery and evaluation

The drive images was loaded in EnCase 3.20 for analysis. The was partitioned into 4 partitions, of which none had a filesystem readable to EnCase. The following table shows the contents of the partition table in the Master Boot Record:

Code	Type	Start Sector	Total Sectors	Size
06	BIGDOS	0	8401995	4,0GB
06	BIGDOS	8401995	1269135	619,7MB
06	BIGDOS	9671130	1028160	502,0MB
06	BIGDOS	10699290	1028160	502,0MB

The four partitions has volume boot headers as follows:

```
1:  adaNF_sFVtsaTltcelba...
2:  V..éSODX.0.4.....p..øð....?.....]□.)
3:  V..éSODX.0.4.....p..üð....?.....°@.)
4:  V..éSODX.0.4.....p..üð....?.....°@.)
```

The occurrence of “SODX” could initially be interpreted as a filesystem of that name. However, such a filesystem is not known.

However, on further evaluation, it was found that swapping the bytes of the entire file systems, the contents could be read. The file systems of partition 2-4 were now readable as a variant of the FAT file system (with headers reading as “VXDOS”). The first partition however contains no clearly visible file system (With header reading “NadaFSFastVCTTable”).

It was however found that the contents of this partition was indeed corresponding to the direct storage of images of previously copied document pages. These pages could be extracted and viewed in a standard image viewer.

3.0 Conclusion

The experiment shows that copied documents are actually stored within digital copiers, and that it is possible to retrieve those documents by performing a forensic analysis on the hard drive found inside most modern copiers. Such documents may show to have crucial value as evidence in criminal as well as civil investigations.