2011 First ACIS/JNU International Conference on Computers, Networks, Systems, and Industrial Engineering

An Analysis of Multi-Function Peripheral with a Digital Forensics Perspective

Kwangwoo Lee
Information Security Group,
Sungkyunkwan University
Suwon, Korea
kwlee@security.re.kr

Changbin Lee
Information Security Group,
Sungkyunkwan University
Suwon, Korea
cblee@security.re.kr

Namje Park
Department of Computer Education
Teachers College,
Jeju National University, Korea
namjepark@jejunu.ac.kr

Seungjoo Kim
CIST,
Korea University
Seoul, Korea
skim71@korea.ac.kr

Dongho Won
Information Security Group,
Sungkyunkwan University
Suwon, Korea
dhwon@security.re.kr

***Abstract*—MFP (Multi-Function Peripheral) is an embedded system that serves several functions including printing, copying, scanning, faxing, document storing, and etc. Recently, MFP is becoming a popular option for office workers due to its multi-functionality and economic efficiency. Furthermore, MFP is able to perform several functions such as USB printing, private job printing, stored job printing, and scan-to-server. Due to the rapid growth of MFP market, MFP is widely used in many workspaces. Therefore, if we can extract meaningful information from MFP's storage devices, it may be valuable evidences in digital forensic investigation. However, systematic forensic investigation about MFP has never been studied so far. In this paper, we describe a process for digital forensic examination of MFP and analyze the acquired data and effectively trace the use of MFP in the crime scene.**

Keywords- MFP, forensic, printer, scanner, CC

I. INTRODUCTION

Recently, there has been much research on devices such as PCs, cell phones, digital cameras, camcorders, and portable storages (USB, external hard drive, CD, SD memory, etc.) in regard to digital forensics. However, not much consideration has been given to MFP (Multi-Function Peripheral) and digital forensic methodology on it, in spite of the fact that MFPs are being widely spread in office workspaces. There were some researches on hardcopy devices such as printer, copier, and scanner. The primary research target for those researches focused on device identification [1][2]. However, stored data on hardcopy devices has never been emphasized as a research matter. Since the functions of MFP are increasing and the usefulness of MFP in office workspaces is being recognized, the demand of MFP digital forensic will rapidly increase. In this reason, we will discuss a legitimate data acquisition process, and study data analysis methodology throughout this paper.

The rest of this paper is organized as follows. In Section 2, we describe a background on digital forensics and MFP. Then we present the necessity of the MFP digital forensic in Section 3. In Section 4, we provide a process and factors necessary for digital forensic investigation of MFP. In Section 5, we present our experimental results of MFP digital forensic investigation. Finally, we summarize and conclude our researches in Section 6.

II. BACKGROUND

A. An Overview of Digital Forensics

Digital forensics is a branch of forensic science pertaining to legal evidence found in digital equipments [3]. The objective of digital forensics is to explain the current state of digital equipment. The digital equipment may include computer workstations, laptop computers, mobile phones, and digital cameras. The explanation may show the existing information in the digital equipment and the sequence of events. The fields of digital forensics can be divided into four categories: network forensics, database forensics, mobile forensics and small device forensics. There are several needs to employ the digital forensics techniques [4]:

- In legal cases, digital forensics is frequently used to analyze digital equipments belonging to defendants in criminal cases or litigants in civil cases.
- To analyze digital equipments after a break-in, for example, to determine how the attacker gained access and what the attacker did.
- To gather evidence against an employee that an organization wishes to terminate.
- To gain information about how digital equipments work for the purpose of debugging, performance optimization or reverse-engineering.

Special measures should be taken when conducting digital forensic investigation if it is desired for the results to be used in a court of law. One of the most important measures is to assure that the evidence has been accurately collected and that there is a clear chain of custody from the scene of the crime to the investigator and ultimately to the

978-0-7695-4417-5/11 $26.00 © 2011 IEEE
DOI 10.1109/CNSI.2011.24

court. That is, it is shown the overall process of acquisition, transfer, handling and disposition of physical or electronic materials by documentation.

In order to comply with the need to maintain the integrity of digital evidence, digital forensic examiners would comply with forensic guidelines such as Association of Chief Police Officers (A.C.P.O). It consists of four principles as follows [5]:

- No action taken by law enforcement agencies or their agents should change data held on a computer system or storage media which may subsequently be relied upon in court.
- In exceptional circumstances, where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.
- An audit trail or other record of all processes applied to computer based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.
- The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

B. An Overview of MFP and Common Criteria

Currently, major companies and public organizations are using the devices equipped with functionalities such as large capacity document data storage and network communication, in addition to print/copy/scan/fax, by combining the functionality of copier, scanner and facsimile into a printer to increase work efficiency and reduce costs. Such devices are called MFP, HCD (Hard-Copy Device), MFD (Multi-Function Device), digital printer, etc. In the MFP, storage mediums such as hard drive or non-volatile memory are installed, and it could cause security problems such as the loss of stored data when printing, faxing or scanning. Since the loss of confidential data or documents could cause significant impact to companies or countries, the security functionalities such as encrypting or overwriting the stored data, the identification/authentication and access control functionality for users are being highlighted as a new competitive element in MFP market.

CC (Common Criteria) is a framework in which computer system users can specify their security functionalities and assurance requirements, vendors can then implement and/or make claims about the security attributes of their products, and testing laboratories can evaluate the products to determine if they actually meet the claims [6]. That is, CC provides assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous and standard manner. CC certification is being required for MFP as government procurement standard in Japan, South Korea, and United State, etc. Therefore, many manufacturers of MFP are actively trying to acquire CC certification.

C. Research Trends of MFP Forensics

Khanna et al. have developed a method that enables authorities to trace documents for specific printers. Therefore, law-enforcement agencies could use to investigate counterfeiting, forgeries and homeland security matters [1][2]. The technique uses two methods to trace a document:

- By analyzing a document to identify characteristics that are unique for each printer,
- By designing printers to purposely embed individualized characteristics in documents.

As a result, current technique is able to identify not only which model printer was used but specifically which printer was used. However, as far as we know, researches on MFP forensic, which is examining hard drives or non-volatile memories stored in MFP, have not been studied.

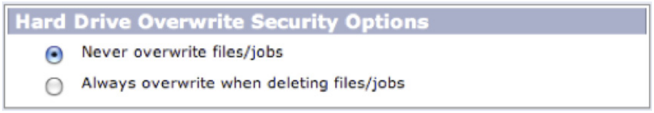
III. NECESSITY OF MFP FORENSICS

Recently, MFP has been widely used in office workspaces due to its multi-functionality and economic efficiency. Therefore, evidences might be contained in MFP without any user awareness. It has significant meaning in a digital forensic perspective since MFP forensic investigation is available for the various crimes.

In the perspective of CC, ST (Security Target) is a document that identifies the security properties of the TOE (target of evaluation). To check the security features of MFPs, we surveyed recently evaluated 40 of 164 CC-certified products' STs [6]. In our survey, Fuji Xerox, Xerox, Samsung Electronics, Konica Minolta, Hewlett Packard, Lexmark, OCE, Toshiba TEC, Cannon were included. According to our survey, most operational environments of MFP are assuming that MFPs are standalone devices, or installed in the intranet. Therefore, the physical protection of MFPs is assumed to be provided since MFPs are generally installed in office workspaces. In addition, for many products, HDDs are considered to be secure owing to the assumption in which they are physically protected. Therefore, several MFP products do not include the HDD encryption. In this case, unauthorized access on MFPs is possible in regard of certain incidents such as expiration of rental contract, discardment of MFP, or technical support on MFP (e.g. repair), and thus unwanted data leakage may take place. It means that forensic investigator can easily access data stored in HDD as well.

Moreover, several products do not include audit log as an encrypted data. Therefore, the audit log is not encrypted, since it makes the MFP performance down. In this case, it is possible to gain useful information from audit log written in plaintext.

Furthermore, the result of analysis on STs of CC-certified products shows that the assumption "*A system administrator shall enable the security functions* (*this includes image overwriting and HDD encryption*) *correctly*" is included. Therefore, we surveyed 10 companies' products and found that most of MFPs did not correctly configure the image overwriting as a security function by default as shown in Fig.1.



Hard Drive Overwrite Security Options

● Never overwrite files/jobs

○ Always overwrite when deleting files/jobs

Figure 1. MFP default setting of Image Overwrite (Xerox's MFP)

Table 1 shows that MFP default settings of image overwriting and HDD encryption. If image overwriting is not enabled by administrator, meaningful data can be extracted from detached HDD, even though HDD encryption is enabled. We will discuss further experiment results in Section 5.

TABLE I. DEFAULT SETTINGS OF MFP SECURITY FEATURES

Make (Model)	MFP default settings	
	Image Overwriting	HDD Encryption
Fuji Xerox DocuCentre-IV C2260 Series (Xerox)	Disable	Disable
Xerox 4112/4127 (Fuji Xerox)	Disable	Disable
e-STUDIO520/600/720/850 (Toshiba)	Disable	Disable
AR-FR4/ AR-FR5/ AR-FR6 (Sharp)	Disable	Enable
MultiXpress SCX-6545N (Samsung Electronics)	Disable	Enable
HP LaserJet M4345 (Hewlett Packard)	Disable	Not supported
Ricoh Aficio MP 4000/5000 (Ricoh)	Enable	Enable
Lexmark X642e/ X644e (Lexmark)	Not supported	Not supported
Bizhub C652 / Bizhub C552 / Bizhub C452 (Konica)	Not supported	Not supported
Oce VarioPrint 41x0 (OCE)	Not supported	Not supported

IV. MFP FORENSICS PROCESS

In this section, we present the MFP forensic process. There are four steps to the MFP forensics [4][7]:

1. Preparation
2. Evidence collection
3. Examination and Analysis of digital evidence
4. Reporting

A. Preparation

Preparation should be made to acquire the equipment required to collect MFP digital evidence. The necessary tools and equipments are dictated by each aspect of the process: documentation, collection, packaging, and transportation. Please refer to [4] for more detail.

B. Collecting Digital Evidence

Digital evidence of MFP can be collected from hard drives or non-volatile memory devices, and so on. Special care must be taken when handling MFP digital evidence: most digital information in MFP can be changed easily, and it is impossible to detect that a change has taken place or to recover the original data.

Imaging is a process that creates a duplicate of the original MFP HDD. Such imaging tools include DCFLdd, IXimager, Guymager, TrueBack, EnCase, FTK Imager or FDAS, and so on. The original drive is then moved to secure storage to prevent tampering. During imaging of static data, a write protection device or application is normally used to prevent changes from being introduced to the evidentiary media during image acquisition.

Therefore, digital forensic investigator should calculate a cryptographic hash (e.g. SHA-1 hash function) of evidence data and record the hash values. Other specific practices that have been adopted in the handling of digital evidence include [4]:

- Imaging HDD using a write-block device to ensure that data/bit is not changed or added/removed.
- Establish and maintain the chain of custody.
- Documenting everything that has been done.
- Only use tools and methods that have been tested and evaluated to validate their accuracy and reliability.

C. Examination and Analysis of Digital Evidence

The examination makes the evidence visible and explains its origin and significance. Analysis differs from examination in that it looks at the product of the examination for its significance and probative value to the case. Examination is a technical review that is the province of the forensic practitioner, while analysis is performed by the investigative team [8]. All digital evidence must be analyzed to determine the type of information that is stored on HDD. Therefore, specialty tools are used that can display information in a format useful to investigators. Such forensic collection and analysis tools include [9]:

- AccessData's FTK
- Guidance Software's EnCase
- Dr. Golden Richard III's file carving tool Scalpel

- Brian Carrier's Sleuth Kit
- SANS Investigative Forensic Toolkit (SIFT)

In the case of MFP forensic investigation, numerous other tools are used to analyze specific portions of information. There are potential evidence list in MFP below.

- FAX: documents, phone numbers, send/receive logs, etc.
- Scanner: image files or documents, user usage logs, time and date stamps, etc.
- Printer: documents, user usage logs, time and date stamps, etc.
- Network Interface: IP setting, ID/password, E-mail, Internet activity logs, configuration files, etc.

D. *Reporting*

Once the analysis is complete, a report is generated. This report may be a written report, oral testimony.

V. MFP Forensic Analysis

The CC certification is a globally accepted standard for evaluating the security features and capabilities of information technology products. In general, CC certified product is considered that forensic analysis is difficult due to its security features. Therefore, we analyzed the certificated model.

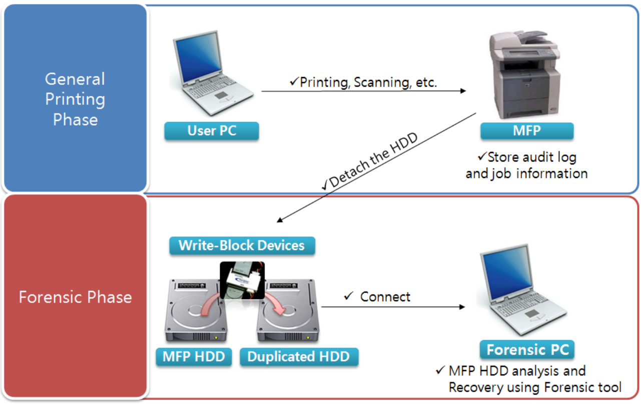


Figure 2. A Flowchart of MFP Forensic Analysis

A. *An Environment for MFP Forensic Investigation*

Fig.2 shows a flowchart of our experiment. It consists of two phases: general printing phase and forensic phase. The general printing phase process is as follows:

1. Send printing jobs to MFP.
2. MFP stores audit log and job information on its HDD.

Next, the forensic phase process is as follows:

1. Detach the HDD from MFP.
2. Use the hardware write-block devices to prevent write operation in MFP HDD.
3. Creates a duplicate of the original MFP HDD.
4. Connect duplicated image to forensic PC.

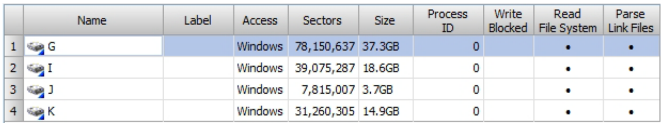
In the step 2 of the forensic phase, we can use the hardware write-block devices such as UltraBlock SCSI, SCSI Write Blocker (SR14A, SR15A), and Ultimate Write Block Kit and so on. Table 2 shows the MFP, forensic PC, and tools used in our experiments. Note that security settings of MFP are configured in regard to practical office workspace environment (See section 3).

TABLE II. An Analysis Environment for MFP Forensic Investigation

Item	Specifications
MFP HDD	80GB SATA
Forensic PC	Intel(R) Core(TM)2 Duo CPU E7200 2.53GHz / 1 GB
Write-block device	Ultimate Write Block Kit
Forensic Tools	Encase Enterprise version 6.15 WinHex v14.4
Secure printing ID/password Setting of MFP	Secure printing ID : kwlee Secure printing password : 2468
Security Settings of MFP	Image Overwriting : Disable HDD Encryption : Enable

B. *Analysis*

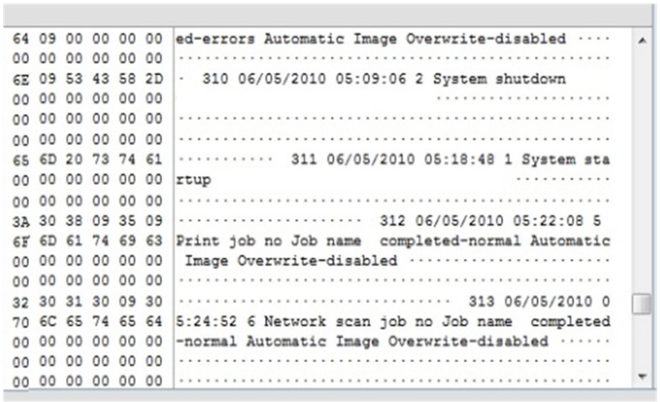
We analyzed the detached HDD image and could find that detached HDD had 4 partitions as shown in Fig.3.



	Name	Label	Access	Sectors	Size	Process ID	Write Blocked	Read File System	Parse Link Files
1	G		Windows	78,150,637	37.3GB	0		•	•
2	I		Windows	39,075,287	18.6GB	0		•	•
3	J		Windows	7,815,007	3.7GB	0		•	•
4	K		Windows	31,260,305	14.9GB	0		•	•

Figure 3. Partition information of HDD in MFP

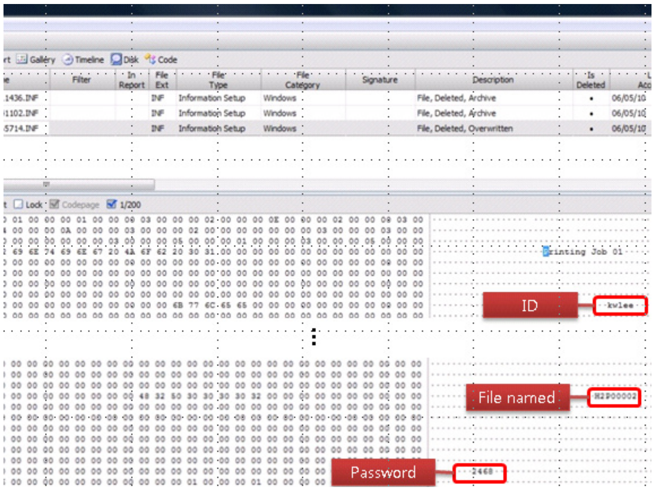
When we examined first partition of HDD, audit log was recorded as plaintext. That is, no encryption had been done to audit logs. It contained information such as startup event, shutdown event, print job event, scan job event, security setting event, and etc. Therefore, we extracted an audit log to get system usage information.



```
64 09 00 00 00 00  ed-errors Automatic Image Overwrite-disabled ····
00 00 00 00 00 00  ················································
6E 09 53 43 58 2D  ·  310 06/05/2010 05:09:06 2 System shutdown
00 00 00 00 00 00                                ····················
00 00 00 00 00 00  ················································
00 00 00 00 00 00  ················································
65 6D 20 73 74 61  ···········  311 06/05/2010 05:18:48 1 System sta
00 00 00 00 00 00  rtup                                  ···········
00 00 00 00 00 00  ················································
3A 30 38 09 35 09  ····················  312 06/05/2010 05:22:08 5
6F 6D 61 74 69 63  Print job no Job name  completed-normal Automatic
00 00 00 00 00 00   Image Overwrite-disabled ·······················
00 00 00 00 00 00  ················································
32 30 31 30 09 30  ·····························  313 06/05/2010 0
70 6C 65 74 65 64  5:24:52 6 Network scan job no Job name  completed
00 00 00 00 00 00  -normal Automatic Image Overwrite-disabled ······
00 00 00 00 00 00  ················································
00 00 00 00 00 00  ················································
```

Figure 4. The Extracted Audit Log of MFP

We examined the extracted audit log. As a result, we found that secure printing job file did not exist but job information such as ID ('kwlee'), password ('2468') and filename ('H2P00002') existed as shown in Fig.6.

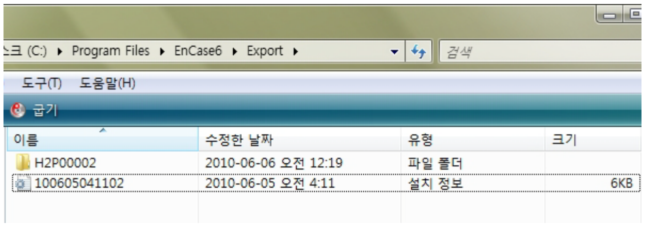


Name	Filter	In Report	File Ext	File Type	File Category	Signature	Description	Is Deleted	Last Accessed
1436.INF			INF	Information Setup	Windows		File, Deleted, Archive	•	06/05/10
1102.INF			INF	Information Setup	Windows		File, Deleted, Archive	•	06/05/10
5714.INF			INF	Information Setup	Windows		File, Deleted, Overwritten	•	06/05/10

```
Printing Job 01
```

Figure 5. Secure Printing Job Information of HDD

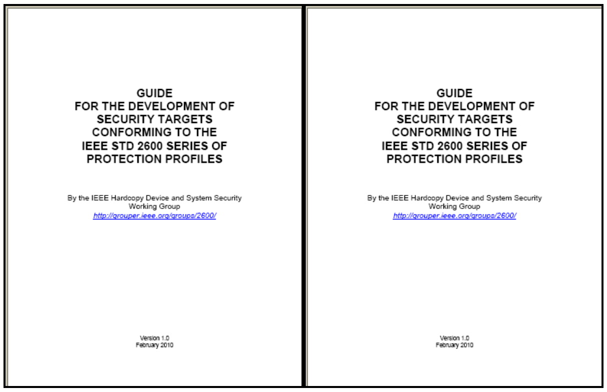
To recover the secure printing job files, we utilized Encase forensic tool referring to filename ('H2P00002') as shown in Fig.6.



이름	수정한 날짜	유형	크기
H2P00002	2010-06-06 오전 12:19	파일 폴더	
100605041102	2010-06-05 오전 4:11	설치 정보	6KB

Figure 6. Recovered Secure Printing Job files of HDD

After storing the recovered files in the appropriate folder, we attached HDD to MFP. Then, we were able to precede the printing job. Fig.7 shows that the output of normal printing job (left) and the output of restored printing job (right) are identical.



GUIDE
FOR THE DEVELOPMENT OF
SECURITY TARGETS
CONFORMING TO THE
IEEE STD 2600 SERIES OF
PROTECTION PROFILES

By the IEEE Hardcopy Device and System Security
Working Group
http://grouper.ieee.org/groups/2600/

Version 1.0
February 2010

GUIDE
FOR THE DEVELOPMENT OF
SECURITY TARGETS
CONFORMING TO THE
IEEE STD 2600 SERIES OF
PROTECTION PROFILES

By the IEEE Hardcopy Device and System Security
Working Group
http://grouper.ieee.org/groups/2600/

Version 1.0
February 2010

Figure 7. A Comparison of Printed Documents
(Left: original document, Right: document from forensic)

As shown in our experiment, after analyzing the audit log, job information can be acquired. Since job information contained information that was necessary to process data recovery, printing job extraction and recovery were possible in our experiment. As a result, we conclude that critical evidences can be collected through MFP forensic investigation.

VI. CONCLUSIONS

Recently, MFP has been widely used in many workspaces. Therefore, if we can extract meaningful information from MFP's storage devices, it may be valuable evidences in digital forensic investigation. Previously, systematic forensic investigation about MFP has never been studied so far. In this paper, we discussed a process for digital forensic examination of MFP, analyzed the acquired data and effectively traced the use of MFP in the crime scene. We expect that our research will help the forensics investigator to examine the MFP in crime scene.

ACKNOWLEDGMENT

This research was supported by the MKE (The Ministry of Knowledge Economy), Korea, under the "ITRC" support program supervised by the NIPA (National IT Industry Promotion Agency)" (NIPA-2011-C1090-1001-0004)

Corresponding Author: dhwon@security.re.kr

REFERENCES

[1] Pei-Ju Chiang, Nitin Khanna, Aravind K. Mikkilineni, Maria V. Ortiz Segovia, Sungjoo Suh, Jan P. Allebach, George T. C. Chiu, Edward J.

Delp, “Printer and Scanner Forensics,” IEEE Signal Processing Magazine, vol.26, no.2, pp.72-83, March 2009.

[2] Nitin Khanna, Aravind K. Mikkilineni, George T. C. Chiu, Jan P. Allebach, Edward J. Delp,” Survey of Scanner and Printer Forensics at Purdue University”, Proceedings of the Second International Workshop on Computational Forensics, Washington DC, August 7-8, 2008, Springer LNCS 5158, pp.22-34.

[3] Yi-Chi Lin, Jill Slay and I. Long Lin, “Computer Forensics and Culture,” Lecture Notes in Computer Science, Volume 5075, pp.288-297, 2010.

[4] "Electronic Crime Scene investigation: A Guide for First Responders", National Institute of Justice, 2008

[5] Association of Chief Police Officers of England, Wales and Northern Ireland webpage, available at http://www.acpo.police.uk/.

[6] Common Criteria Portal Website (Certificated Products), available at http://www.commoncriteriaportal.org/

[7] Brian Carrier, Eugene H.Spafford, "Getting Physical with the Digital Investigation Process," International Journal of Digital Evidence, Volume 2 Issue 2, Fall 2003.

[8] NIST, "Guidelines on Cell Phone Forensic", SP 800-101, May. 2007.

[9] NIST, “Computer Forensics Tool Testing (CFTT) Project Web Site”, available at http://www.cftt.nist.gov/.