프린터 스풀(SPL, SHD) File 복구를 통한 포렌식 분석*

최준호**, 이상진**, 임종인**

**고려 대학교 정보보호 대학원 / 정보보호기술연구센터

Forensics Analysis through Spool(SPL, SHD) File Recover

Joon-ho Choi**, Sang-jin Lee**, Jong-in Lim**

**Center for Information of Security of Technologies(CIST), Korea University.

요 약

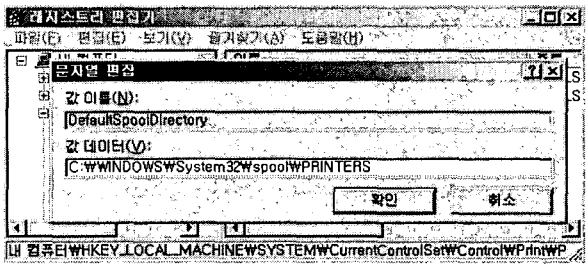
본 논문에서는 원활한 프린터 작업을 위해 컴퓨터와 프린터 사이의 대기시간을 없애기 위한 수단으로 사용되고 있는 스풀작업에 대한 설명과, 포렌식 수사에 있어서 중요한 정보를 가지고 있는 스풀작업정보를 가지고 있는 SHD, SPL 파일의 구조와 분석방법, 스풀 파일을 복구하는 절차와 방법을 제시하였다. SHD, SPL 파일에서 알아낼 수 있는 용의자가 인쇄한 문서의 제목과, 내용, 문서를 인쇄한 시간 정보를 획득하고, 이를 컴퓨터 범죄 수사에 활용하는 방안을 제시하였다.

I. 서론

컴퓨터의 문서를 스풀 한다는 것은, 그것을 읽어서 하드디스크나 대용량 저장매체에 저장함으로써 좀 더 편리한 시간에 프린트되거나 처리될 수 있도록 하는 것이다. 프린트 작업 요청을 위한 문서들의 스풀링은, 많은 사용자들이 자원을 공유하고 있는 메인프레임 컴퓨터들에서 사용되고 있으며, PC의 프린트 작업에서도 만약 프린터가 이미 다른 파일을 출력하고 있다면, 출력 요청한 파일은 하드디스크 상에 스풀처리 된다. 컴퓨터의 문서를 스풀처리 되는 도중 생성되는 SPL, SHD 파일에는 문서를 인쇄하는 사용자의 ID, 인쇄하는 문서의 제목, 인쇄된 문서의 이미지, 문서를 인쇄한 시각등 포렌식 분석에 중요한 정보들을 포함하고 있다.

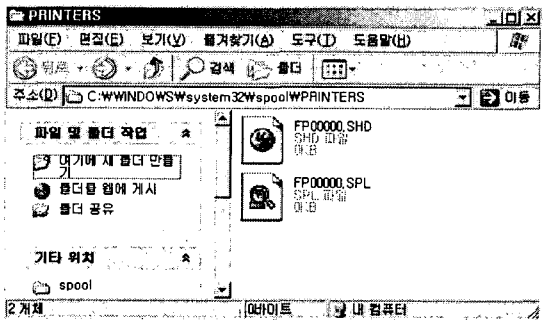
II. 윈도우 스풀 시스템

윈도우 운영체제는 문서를 인쇄하는 도중 생기는 컴퓨터와 프린터 사이의 대기시간을 없애기 위한 수단으로 스풀 방식을 사용한다. 윈도우 운영체제에서 문서를 인쇄하기 위한 스풀작업을 완료하면 윈도우는 스풀(SPL, SHD) 파일을 생성한다.



(그림 1) 레지스트리에서 지정한 스풀 저장 디렉터리

윈도우 스풀파일을 저장하는 디렉터리는 레지스트리 상에서 사용자가 수정 할 수 있으며, 레지스터에서 지정한 기본 스풀파일 저장 디렉터리는 C:\WINDOWS\System32\스풀\PRINTERS 이다.



(그림 2) 스풀작업을 완료한 후 생기는 스풀 파일

생성된 스풀파일들은 사용자의 개인정보 보호를 위해 모든 인쇄 작업이 완료된 뒤 윈도우 시스템에 의해 자동적으로 스풀저장 디렉터리에서 삭제된다.[1]

III. SHD File

```
DWORD dwSignature;
DWORD offUserName;
DWORD offDocumentName;
DWORD offPrinterName;
SYSTEMTIME stSubmitTime;
DWORD offComputername;
DWORD dwSPLSize2;
```

(그림 3) SHD File Format [4]

윈도우 스풀파일 SHD는 문서를 인쇄한 사용자의 ID, 인쇄한 문서의 이름, 문서를 인쇄한 시각, 문서를 인쇄한 프린터 장치명, 문서를 인쇄한 컴퓨터 등에 관한 정보를 가지고 있다.

그림4는 SHD에서 문서를 인쇄한 사용자의 ID(reaper91)정보가 있는 부분이다

```
00 00 3F AD 14 62 C1 27 39 37   ..?-.bÁ'97
82 8B A6 28 01 02 00 00 72 00   ,‹¦(....r.
65 00 61 00 70 00 65 00 72 00   e.a.p.e.r.
39 00 31 00 00 00 72 00 65 00   9.1...r.e.
61 00 70 00 65 00 72 00 39 00   a.p.e.r.9.
```

(그림 4) 문서를 인쇄한 사용자

그림5는 SHD에서 문서를 인쇄한 시각(2006년 6월 10일 4시 20분 41초)정보가 있는 부분이다.

```
00 00 14 04 00 00 00 00 00 00   ..........
D6 07 06 00 06 00 0A 00 07 00   Ö.........
14 00 29 00 28 01 00 00 00 00   ..).(.....
00 00 00 00 5C 2A 00 00 01 00   ....\*....
```

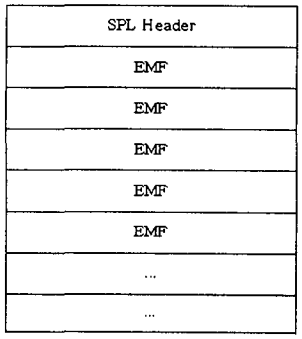
(그림 5) 문서를 인쇄한 시각

그림6은 SHD에서 사용자가 인쇄한 문서의 이름(Text.txt)정보가 있는 부분이다.

```
61 00 70 00 65 00 72 00 39 00   a.p.e.r.9.
31 00 00 00 54 00 65 00 78 00   1...T.e.x.
74 00 2E 00 74 00 78 00 74 00   t...t.x.t.
20 00 2D 00 20 00 54 BA A8 BA   .-. .T°¨°
A5 C7 00 00 4D 00 69 00 63 00   ¥Ç..M.i.c.
```

(그림 6) 인쇄한 문서의 파일 이름

IV. SPL File



(그림 7) SPL File Format [4]

윈도우 스풀파일 SPL은 사용자가 인쇄한 문서의 내용을 가지고 있다. SPL파일은 그림7과 같이 SPL 헤더와 문서의 내용을 가지고 있는 여러 개의 EMF로 이루어져 있다.

1. SPL Header

SPL Header에는 인쇄한 문서의 파일 이름과 문서를 인쇄한 프린터 장치명... 등을 가지고 있다.

그림8은 인쇄한 문서의 이름이 console.txt라는 보여주고 있다.

```
00 00 01 00 84 00 00 00   ....„...
10 00 00 00 34 00 00 00   ....4...
63 00 6F 00 6E 00 73 00   c.o.n.s.
6F 00 6C 00 65 00 2E 00   o.l.e...
74 00 78 00 74 00 20 00   t.x.t. .
2D 00 20 00 54 BA A8 BA   -. .T°¨°
A5 C7 00 00 4D 00 69 00   ¥Ç..M.i.
63 00 72 00 6F 00 73 00   c.r.o.s.
```

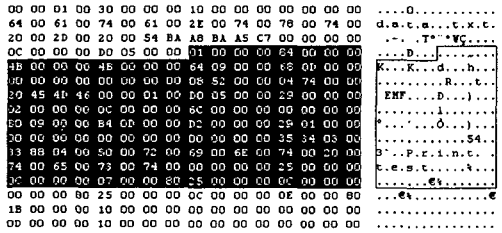
(그림 8) 인쇄한 문서의 파일 이름

2. EMF

SPL 파일은 SPL Header와 EMF로 구성되는데, EMF부분에 실질적으로 사용자가 인쇄한 문서의 내용을 가지고 있다, 각각의 EMF크기는 동일한 크기

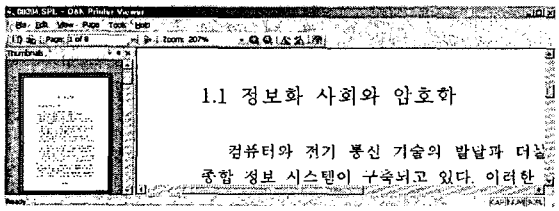
를 가지고 있으며 이 크기는 인쇄를 하는 문서들 마다 각각 다른 크기를 가지고 있다.

그림 9는 SPL파일 내부에 있는 EMF의 일부분을 보여 주고 있다.



(그림 9) SPL 파일의 한 EMF의 일부분

EMF 형식의 데이터는 그림10과 같이 EMF Viewer를 통해 볼 수 있다.[3]



(그림 10) SPL Viewer로 본 SPL File의 EMF

V. 스풀(SHD, SPL) 파일 복구

문서의 인쇄작업과 스풀 작업이 완료되면 생성되는 스풀(SPL, SHD)파일은 디스크용량의 낭비되는 것을 방지하고, 사용자의 개인정보보호를 위해 윈도우 운영체제가 자동적으로 일정 시간이 지난 후 삭제한다. 삭제된 스풀파일은 운영체제의 스풀프로세스(스풀sv.exe), 하드디스크의 스왑파일영역(Pagefile.sys)과 미할당(Unallocated)영역에서 복구 할 수 있다.

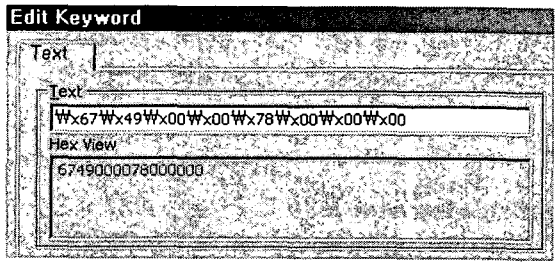
1. SHD 파일 복구

SHD_SIGNATURE_WIN98	$0000494B
SHD_SIGNATURE_WINNT	$00004966
SHD_SIGNATURE_WIN2000	$00004967
SHD_SIGNATURE_WIN2003	$00004968

(그림 11) SHD 파일 시그너처

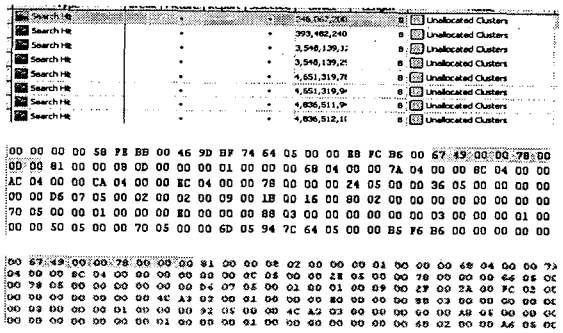
SHD 파일은 그림11과 같이 SHD 파일만이 가지는 고유한 SHD Signature를 활용하여 복구 작업을 수행한다.. 복구한 SHD 파일을 통해서 사용자가 인쇄한 문서의 파일명과, 문서를 인쇄한 시각을 알아 낼 수 있다.

그림12는 EnCase 검색어에 SHD파일 시그너처를 입력하고 시그너처를 이용해 삭제된 SHD 파일을 프로세스, 스왑파일, 미할당영역에서 검색하는 과정을 보여주고 있다.



(그림 12) EnCase SHD 검색

그림13에서는 하드디스크 미할당 영역에서 검색된 삭제된 SHD를 EnCase가 보여주고 있다.



(그림 13) 하드디스크 미할당영역에서 발견된 SHD

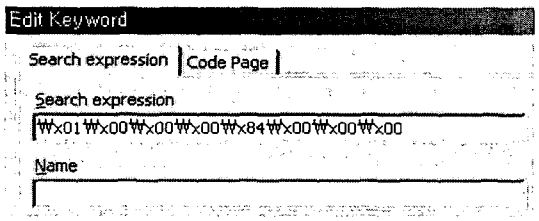
2. SPL 파일 복구

Windows XP	\x01\x00\x00\x00\x5C\x01 \x01\x00\x00\x00\x84\x00
Windows 2000	\x01\x00\x00\x00\xD8\x17 \x01\x00\x00\x00\x58\x6E
Windows NT & 2000	\x01\x00\x00\x00\x18\x17
Windows 9x	\x01\x00\x00\x00\x58\x00

(그림 9) EMF 헤더 [5][6][7]

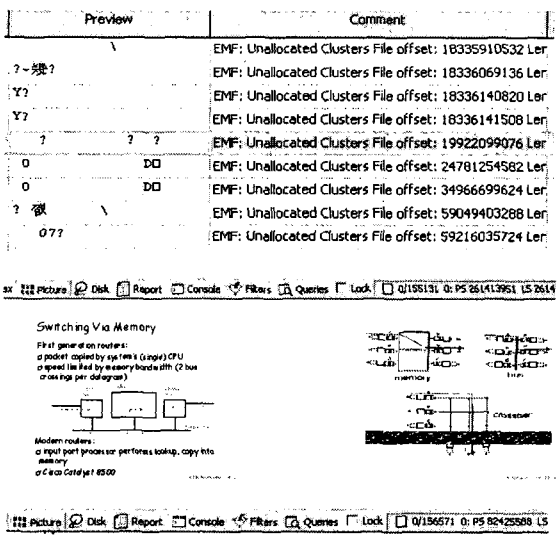
SPL 파일에서 실질적으로 파일의 내용을 담고 있는 부분은 EMF이므로, SPL파일을 복구 하는 것이 아니라, 그림9에서 보여주고 있는 것처럼

운영체제 별로 가지고 있는 EMF 헤더를 활용하여 EMF부분을 복구 작업을 수행한다. SPL 파일이 가지고 있는 여러개의 EMF 중 하나의 EMF만을 복구 할 수 있어도 복구를 성공한 하나의 EMF가 가진 문서의 일부분을 볼 수 있다. 그림14는 EnCase 검색어에 EMF 헤더를 입력하여 하드디스크 미할당영역에서 SPL검색하는 과정을 보여주고 있다.



(그림 14) EnCase SPL 검색

EnCase에서는 EMF를 보다 쉽게 검색하기 위해 EnScript기능을 제공하지만 최신버전인 EnCase 버전에 있는 EnScript에는 EMF헤더에 관한 정보가 잘못 되어 있기 때문에 EMF헤더에 관한 부분을 수정해 주어야 한다.



(그림 15) 미할당 영역에서 발견된 EMF

그림 15는 EnCase EnScript를 활용하여 EMF를 검색하고 하드디스크의 미할당영역에서 복구한 EMF를 보여주고 있는 모습이다.

VI. 결론

이러한 윈도우 스풀(SHD, SPL)파일의 복구를 통해 수집된 스풀파일 분석을 통한 컴퓨터 포렌식 정보 수집은 컴퓨터 범죄 수사에 다음과 같은 단서를 제공한다.

첫째, 용의자가 어떤 특정 단체의 중요 기밀문서를 외부로 유출한 시도를 스풀파일을 통해 증명 할 수 있다.

둘째, 용의자가 외부로 유출한 중요 기밀문서의 파일명과, 인쇄시각을 통해 용의자가 언제 어떤 문서를 유출 시켰는지에 대한 정보를 얻을 수 있다.

셋째, 용의자가 외부로 유출한 문서의 내용을 알아내어 용의자가 어떤 내용의 문서를 유출 시켰는지에 대한 정보를 알아 낼 수 있다.

[참고문헌]

[1] Window Spool System

http://support.microsoft.com/kb/q264662/

[2] EnCase 4.20 Enterprise Edition

http://www.guidancesoftware.com/

[3] O&K Printer Viewer 1.00(EMF Viewer)

http://www.prnwatch.com/

[4] SHD, SPL File Format

http://undocprint.printassociates.com/

[5] Guidance Software Article :

An Explanation of EMF and Print Spooler Files

http://www.guidancesoftware.com/support/articles/ExplainEMF.asp

[6] McGraw-Hill, Hacking Exposed Computer Forensics By David Cowen

[7] Artech House, Computer and Intrusion Forensics By George Mohay, Alison Anderson, Byron Collie, Olivier de Vel, Rod McKemmish