

문제 12.

12. 박성민이 범행과 관련된 내용을 출력하려 한 증거를 찾고, 출력에 사용한 프린터의 모델명을 기술하시오.

- '/vol_vol2/Windows/System32/spool/PRINTERS/' 하위에서 출력 관련 아래 두 파일을 찾을 수 있었음.

Metadata	
Name:	/img_파티션2개복구_Reimaging_Scenario3.001/vol_vol2/Windows/System32/spool/PRINTERS/FP00000.SPL
Type:	File System
MIME Type:	image/vnd.microsoft.icon
Size:	1073696
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2022-11-18 10:42:06 KST
Accessed:	2022-11-18 11:17:07 KST
Created:	2022-11-11 16:47:00 KST
Changed:	2022-11-18 11:17:02 KST
MD5:	5cdfcac647c8ae137ba2efcea6b97142
SHA-256:	ee7ecf099b2e52f7872395b10c4ca7ab99140eb87462fc1e442cceb316bf31d4
Hash Lookup Results:	UNKNOWN
Internal ID:	20303

/img_파티션2개복구_Reimaging_Scenario3.001/vol_vol2/Windows/System32/spool/PRINTERS/FP00000.SPL

Metadata	
Name:	/img_파티션2개복구_Reimaging_Scenario3.001/vol_vol2/Windows/System32/spool/PRINTERS/FP00000.SHD
Type:	File System
MIME Type:	application/octet-stream
Size:	4480
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2022-11-18 10:42:06 KST
Accessed:	2022-11-18 11:17:07 KST
Created:	2022-11-11 16:47:00 KST
Changed:	2022-11-18 11:17:00 KST
MD5:	4e69b680bc2a70e0f9913234e2a2be6b
SHA-256:	315d627dafa2c316590fdaffdc7f73ef3079f25da8a94facb311823d348a0b0
Hash Lookup Results:	UNKNOWN
Internal ID:	20301

/img_파티션2개복구_Reimaging_Scenario3.001/vol_vol2/Windows/System32/spool/PRINTERS/FP00000.SHD

- 또한, Autopsy와 HxD를 활용하여 프린터 관련 파일인

'/img_파티션2개복구_Reimaging_Scenario3.001/vol_vol2/Windows/System32/spool/PRINTERS/FP00000.SHD'

의 내용을 확인해본 결과 해당 프린터의 모델명은 'Canon iP110 series'인 것으로 추정됨.

FP00000.SHD 0 application/octet-stream

Hex Text Application File Metadata OS Account Data Artifact

Strings Extracted Text Translation

Page: 1 of 1 Page Go to Page:

Canon iP110 series
BJDM
Canon iP110 series
john
john
.hwp
Canon iP110 series
Canon iP110 series
Canon iP110 series Print Processor
NT EMF 1.008
WWDESKTOP-DF1
S-1-5-21-1998824668-1248911011-2283617520-1002
C:\Windows\system32\spool\PRINTERS\FP00010.SPL

```
68 00 77 00 70 00 00 00 43 00 61 00 6E 00 6F 00 h.w.p...C.s.n.o.  
6E 00 20 00 69 00 50 00 31 00 31 00 30 00 20 00 n..i.P.l.l.o..  
73 00 65 00 72 00 69 00 65 00 73 00 00 00 43 00 s.e.r.i.e.s...C.
```

- 추가적으로, 출력하려던 파일명을 확인하기 위해 HxD를 활용하여

'/img_파티션2개복구_Reimaging_Scenario3.001/vol_vol2/Windows/System32/spool/PRINTERS/FP00000.SPL'

의 내용을 확인해본 결과 출력하려던 파일은 '건축계획서.hwp'로 추정됨.

```
00 00 01 00 24 00 00 10 00 00 00 00 00 00 00 .....$.....  
74 AC 95 CD C4 AC 8D D6 1C C1 2E 00 68 00 77 00 c-+iÄ~.Ö.Ä..h.w.  
70 00 00 00 0C 00 00 00 E4 61 10 00 01 00 00 00 p.....äa.....  
84 00 00 00 75 02 00 00 F5 02 00 00 73 10 00 00 „...u...ö...s...  
1B 18 00 00 00 00 00 00 00 00 00 00 4C 4F 00 00 .....LO..  
E4 70 00 00 20 45 4D 46 00 00 01 00 E4 61 10 00 äp.. EMF....äa..  
14 04 00 00 03 00 00 00 0C 00 00 00 6C 00 00 00 .....l...  
00 00 00 00 C0 12 00 00 AA 1A 00 00 CB 00 00 00 ....Ä...^...Ë...  
21 01 00 00 00 00 00 00 00 00 00 00 00 00 00 !.....  
C0 19 03 00 C7 68 04 00 50 00 72 00 69 00 6E 00 Ä...Çh..P.r.i.n..  
74 00 20 00 74 00 65 00 73 00 74 00 00 00 00 00 t..t.e.s.t....  
25 00 00 00 0C 00 00 00 07 00 00 80 25 00 00 00 %.....€%...  
0C 00 00 00 00 00 00 80 25 00 00 00 0C 00 00 00 .....€%.....  
0E 00 00 80 1B 00 00 00 10 00 00 00 00 00 00 00 ...€.....  
00 00 00 00 0D 00 00 00 10 00 00 00 00 00 00 00 .....  
00 00 00 00 62 00 00 00 0C 00 00 00 01 00 00 00 ....b.....  
64 00 00 00 0C 00 00 00 14 00 00 80 4B 00 00 00 d.....€K...  
40 00 00 00 30 00 00 00 01 00 00 00 20 00 00 00 @...0.....  
01 00 00 00 01 00 00 00 10 00 00 00 B0 FF FF FF .....°ÿÿÿ  
BA FF FF FF 11 13 00 00 22 1B 00 00 B0 FF FF FF °ÿÿÿ...."....°ÿÿÿ
```

2진수 (8비트) 01110100

Int8	이동:	116
UInt8	이동:	116
Int16	이동:	-21388
UInt16	이동:	44148
Int24	이동:	유효하지 않음
UInt24	이동:	유효하지 않음
Int32	이동:	유효하지 않음
UInt32	이동:	유효하지 않음
Int64	이동:	유효하지 않음
UInt64	이동:	유효하지 않음
LEB128	이동:	-12
ULEB128	이동:	116
AnsiChar / char8_t		
WideChar / char16_t	견	✓