

문제 4.

4. 나보석이 절도품을 은닉한 장소를 알 수 있는 파일을 찾고, 해당 증거파일의

① 시작섹터 ② MD5 해쉬값 ③ 시간정보 ④ 파일의 용량을 기술하시오

/vol\_vol2/2022-서울-국제-주얼리.docx 파일은 시그니처훼손파일로, HxD를 사용하여 다음과 같이 복구 후 파일을 열람해보았음.

AccessData FTK Imager 4.7.1.2

File View Mode Help

Evidence Tree

- jewel [NTFS]
  - [orphan]
  - [root]
    - \$BadClus
    - \$Extend
    - \$RECYCLE.BIN
    - \$Secure
    - \$UpCase
    - 12\_10\_중형\_표지+왕데뷰+190g\_내지+왕데뷰+160g\_새로+만들기 최종.pdf
    - 12178743.png
    - 13725837.png
    - 15149574.png
    - 2022\_JBM브로슈어(월용).pdf
    - 2022년+15회+국제귀금속장신구대전.hwp
    - 2022년+15회+국제귀금속장신구대전+및+수상작품,+산학협력전시회.hwp
    - 2022년-라이노-캐드-고급과정-교육-신청서.hwp
    - 2022-서울-국제-주얼리.docx
    - 2022-서울-국제-주얼리-엑세서리-쇼참가-신청서.docx
    - 35092919.png
    - 62271795.png

Properties

2022-서울-국제-주얼리.docx

Name	2022-서울-국제-주얼리.docx
File Class	Regular File
File Size	350,230
Physical Size	352,256
Start Cluster	19,582
Date Accessed	2022-11-10 오전 7:33:23
Date Created	2022-11-10 오전 7:33:23
Date Modified	2022-10-19 오전 6:10:44
Encrypted	False
Compressed	False
Actual File	True
Start Sector	156,784
Alternate Data Stream Count	1

DOS Attributes

Hidden False

Properties Hex Value Interpreter

Listed: 113 Selected: 1 북구 022-2-1-168.001/Partition 1 [1021MB]/jewel [NTFS]/[root]/2022-서울-국제-주얼리.docx

File List

Name	Size	Type	Date Modified
1642408906_86.jpg	348	Regular F...	2022-10-19
1642408955_99.jpg	284	Regular F...	2022-10-19
1642408972_1.jpg	375	Regular F...	2022-10-19
1642409039_32.jpg	380	Regular F...	2022-10-19
2022-서울-국제-주얼리-엑...	34	Regular F...	2022-10-19
2022-서울-국제-주얼리.do...	343	Regular F...	2022-10-19
20221018_100334.jpg	79	Regular F...	2022-10-18
20221018_105631.jpg	471	Regular F...	2022-10-18
20221018_105727.jpg	308	Regular F...	2022-10-18
20221018_105749.jpg	202	Regular F...	2022-10-18
20221018_110026.jpg	220	Regular F...	2022-10-18
20221018_110114.jpg	521	Regular F...	2022-10-18
20221018_112126227.docx	805	Regular F...	2022-10-19
2022_JBM브로슈어(월용)...	990	Regular F...	2022-10-19
2022년+15회+국제귀금속...	3,060	Regular F...	2022-10-19
2022년+15회+국제귀금속...	1,570	Regular F...	2022-10-19
2022년-라이노-캐드-고급...	54	Regular F...	2022-10-19
35092919.png	185	Regular F...	2022-10-19

Cursor pos = 0; dus = 19582; log sec = 156656; phy sec = 156784

## Metadata

Name: /img\_복구\_022-2-1-168.001/vol\_vol2/2022-서울-국제-주얼리.docx

Type: File System

MIME Type: application/octet-stream

Size: 350230

File Name Allocation: Allocated

Metadata Allocation: Allocated

Modified: 2022-10-19 15:10:44 KST

Accessed: 2022-11-10 16:33:23 KST

Created: 2022-11-10 16:33:23 KST

Changed: 2022-10-19 15:10:44 KST

MD5: a8429e10840acdedc6954e61dc5306a5

SHA-256: dbdfd9e54f3a1442cf76b59142687eb9f7c4d69b77b4cf8813424600da22f07

Hash Lookup Results: UNKNOWN

Internal ID: 326

HxD - [C:\autopsy\_case\Scenario2\Scenario2\Export\2022-서울-국제-주얼리.docx]

16 Windows (ANSI) 16진수

파일(F) 편집(E) 찾기(S) 보기(V) 분석(A) 도구(T) 창 설정(W) 도움말(H)

2022-서울-국제-주얼리.docx

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	50	4B	B3	04	14	00	06	00	08	00	00	21	00	1C	41	PK	.....!...A
00000010	A8	2E	66	01	00	00	54	05	00	00	13	00	08	02	5B	43	".f...T.....[C
00000020	6F	6E	74	65	6E	74	5F	54	79	70	65	73	5D	2E	78	6D	ontent_Types].xm
00000030	6C	20	A2	04	02	28	A0	00	02	00	00	00	00	00	00	00	l <..( ..... .....
00000040	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....

시작섹터	156,784
MD5 해시값	a8429e10840acdedc6954e61dc5306a5
시간정보	Modified : 2022-10-19 15:10:44 KST Accessed : 2022-11-10 16:33:23 KST Created : 2022-11-10 16:33:23 KST
파일의 용량	350,230 (Bytes)

확인한 해당 파일 내용은 아래와 같음.

