문제 14.

14. 박성민이 이현수에게 범행을 지시하기 위해 작성한 문서를 찾고, 이 문서를 전달한 방법을 알 수 있는 증거를 찾아 기술하시오.

- 문제13에서 박성민이 이현수에게 보낸 메일 중 FTP 서버주소와 함께 ID, PW를 보내며 접속 후 다운로드를 유도한 내용으로 미루어보아, FTP 서비스를 이용하여 이현수에게 범행을 지시하기 위해 작성한 문서를 전달한 것으로 추정됨. 이에 따라 filezilla 설치 흔적을 다음과 같이 탐색하였음.

Metadata

Name:	/img_파티션2개복구_Reimaging_Scenario3.001/vol_vol2/Users/bbb/Downloads/FileZilla_3.62.0_win64_sponsored2-setup.exe
Type:	File System
MIME Type:	application/x-dosexec
Size:	12332192
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2022-11-11 14:36:08 KST
Accessed:	2022-11-11 16:47:46 KST
Created:	2022-11-11 16:47:46 KST
Changed:	2022-11-11 15:02:31 KST
MD5:	c0542ee37edc7b7d1f0367a2e91268c6
SHA-256:	9be14dd6e8ae94d32d6b68cf664b43f4ff83818c8880d474682f3e4f6ab727dd
Hash Lookup Results:	UNKNOWN
Internal ID:	16803
Downloaded From:	https://download.filezilla-project.org/client/FileZilla_3.62.0_win64_sponsored2-setup.exe

- filezilla 응용프로그램이 설치된 것으로 미루어보아, filezilla를 이용해 ftp로 해당 문서를 이현수에게 전달한 것으로 추정하여 filezilla 로그파일인 filezilla.log파일을 다음과 같이 탐색, 분석함.

```
2022-08-31 16:58:59 32556 1 상태: psm.ftp.com 주소 해석
2022-08-31 16:58:59 32556 1 상태: 123.456.78.901:21에 연결...
2022-08-31 16:58:59 32556 1 상태: 연결 수립, 환영 메시지를 기다림...
2022-08-31 16:58:59 32556 1 응답: 220 (vsFTPd 2.2.2)
2022-08-31 16:58:59 32556 1 명령: AUTH TLS
2022-08-31 16:58:59 32556 1 응답: 530 Please login with USER and PASS.
2022-08-31 16:58:59 32556 1 명령: AUTH SSL
2022-08-31 16:58:59 32556 1 응답: 530 Please login with USER and PASS.
2022-08-31 16:58:59 32556 1 상태: 보안되지 않은 서버입니다. TLS를 통한 FTP를 지원하지 않습니다.
2022-08-31 16:59:00 32556 1 명령: USER psm
2022-08-31 16:59:00 32556 1 응답: 331 Please specify the password.
2022-08-31 16:59:00 32556 1 명령: PASS **********
2022-08-31 16:59:02 32556 1 응답: 530 Login incorrect.
2022-08-31 16:59:02 32556 1 오류: 치명적 오류: 서버에 연결하지 못함
2022-08-31 16:59:03 32556 1 상태: 서버와의 연결이 종료됨
2022-08-31 16:59:03 32556 1 상태: 직전 연결 실패로 5초 연결 지연...
```

2022-08-31 16:59:07 32556 1 상태: psm.ftp.com 주소 해석
2022-08-31 16:59:07 32556 1 상태: 123.456.78.901:21에 연결...
2022-08-31 16:59:07 32556 1 상태: 연결 수립, 환영 메시지를 기다림...
2022-08-31 16:59:07 32556 1 응답: 220 (vsFTPd 2.2.2)
2022-08-31 16:59:07 32556 1 명령: AUTH TLS
2022-08-31 16:59:07 32556 1 응답: 530 Please login with USER and PASS.
2022-08-31 16:59:07 32556 1 명령: AUTH SSL
2022-08-31 16:59:07 32556 1 응답: 530 Please login with USER and PASS.
2022-08-31 16:59:07 32556 1 상태: 보안되지 않은 서버입니다. TLS를 통한 FTP를 지원하지 않습니다.
2022-08-31 16:59:07 32556 1 명령: USER psm
2022-08-31 16:59:07 32556 1 응답: 331 Please specify the password.
2022-08-31 16:59:07 32556 1 명령: PASS **********
2022-08-31 16:59:07 32556 1 응답: 230 Login successful.
2022-08-31 16:59:07 32556 1 명령: SYST
2022-08-31 16:59:07 32556 1 응답: 215 UNIX Type: L8
2022-08-31 16:59:07 32556 1 명령: FEAT
2022-08-31 16:59:08 32556 1 응답: 211-Features:
2022-08-31 16:59:08 32556 1 응답: EPRT
2022-08-31 16:59:08 32556 1 응답: EPSV
2022-08-31 16:59:08 32556 1 응답: MDTM
2022-08-31 16:59:08 32556 1 응답: PASV
2022-08-31 16:59:08 32556 1 응답: REST STREAM
2022-08-31 16:59:08 32556 1 응답: SIZE
2022-08-31 16:59:08 32556 1 응답: TVFS
2022-08-31 16:59:08 32556 1 응답: UTF8
2022-08-31 16:59:08 32556 1 응답: 211 End
2022-08-31 16:59:08 32556 1 명령: OPTS UTF8 ON
2022-08-31 17:02:42 32556 1 상태: psm.ftp.com 주소 해석
2022-08-31 17:02:42 32556 1 상태: 123.456.78.901:21에 연결...
2022-08-31 17:02:53 32556 1 오류: 사용자에 의해 연결 시도 중단
2022-08-31 17:02:53 32556 1 상태: 서버와의 연결이 종료됨
2022-08-31 17:02:53 32556 1 상태: psm.ftp.com 주소 해석
2022-08-31 17:02:53 32556 1 상태: 123.456.78.901:21에 연결...
2022-08-31 17:02:53 32556 1 상태: 연결 수립, 환영 메시지를 기다림...
2022-08-31 17:02:53 32556 1 응답: 220 (vsFTPd 2.2.2)
2022-08-31 17:02:53 32556 1 명령: AUTH TLS
2022-08-31 17:02:53 32556 1 응답: 530 Please login with USER and PASS.
2022-08-31 17:02:53 32556 1 명령: AUTH SSL
2022-08-31 17:02:53 32556 1 응답: 530 Please login with USER and PASS.

2022-08-31 17:02:53 32556 1 상태: 보안되지 않은 서버입니다. TLS를 통한 FTP를 지원하지 않습니다.
2022-08-31 17:02:53 32556 1 명령: USER psm
2022-08-31 17:02:53 32556 1 응답: 331 Please specify the password.
2022-08-31 17:02:53 32556 1 명령: PASS **********
2022-08-31 17:02:53 32556 1 응답: 230 Login successful.
2022-08-31 17:02:53 32556 1 명령: OPTS UTF8 ON
2022-08-31 17:02:53 32556 1 응답: 200 Always in UTF8 mode.
2022-08-31 17:02:53 32556 1 상태: 로그인
2022-08-31 17:02:53 32556 1 상태: 디렉터리 목록 조회...
2022-08-31 17:02:53 32556 1 명령: PWD
2022-08-31 17:02:53 32556 1 응답: 257 "/"
2022-08-31 17:02:53 32556 1 명령: TYPE I
2022-08-31 17:02:53 32556 1 응답: 200 Switching to Binary mode.
2022-08-31 17:02:53 32556 1 명령: PASV
2022-08-31 17:02:53 32556 1 응답: 227 Entering Passive Mode (182,162,95,167,25,141).
2022-08-31 17:02:53 32556 1 명령: LIST
2022-08-31 17:02:54 32556 1 응답: 150 Here comes the directory listing.
2022-08-31 17:02:54 32556 1 응답: 226 Directory send OK.
2022-08-31 17:02:54 32556 1 상태: "/" 디렉터리 목록 조회 성공
2022-08-31 17:02:58 32556 2 상태: psm.ftp.com 주소 해석
2022-08-31 17:02:58 32556 2 상태: 123.456.78.901:21에 연결...
2022-08-31 17:02:58 32556 3 상태: psm.ftp.com 주소 해석
2022-08-31 17:02:58 32556 3 상태: 123.456.78.901:21에 연결...
2022-08-31 17:02:58 32556 3 상태: 연결 수립, 환영 메시지를 기다림...
2022-08-31 17:02:58 32556 3 응답: 220 (vsFTPd 2.2.2)
2022-08-31 17:02:58 32556 3 명령: AUTH TLS
2022-08-31 17:02:58 32556 3 응답: 530 Please login with USER and PASS.
2022-08-31 17:02:58 32556 3 명령: AUTH SSL
2022-08-31 17:02:58 32556 3 응답: 530 Please login with USER and PASS.
2022-08-31 17:02:58 32556 3 상태: 보안되지 않은 서버입니다. TLS를 통한 FTP를 지원하지 않습니다.
2022-08-31 17:02:58 32556 3 명령: USER psm
2022-08-31 17:02:58 32556 3 응답: 331 Please specify the password.
2022-08-31 17:02:58 32556 3 명령: PASS **********
2022-08-31 17:02:58 32556 3 응답: 230 Login successful.
2022-08-31 17:02:58 32556 3 명령: OPTS UTF8 ON
2022-08-31 17:02:58 32556 3 응답: 200 Always in UTF8 mode.
2022-08-31 17:02:58 32556 3 상태: 로그인
2022-08-31 17:02:58 32556 3 상태: C:\Users\admin\Desktop\건축계획서.hwp 업로드 시작

2022-08-31 17:02:58 32556 3 명령: CWD /
2022-08-31 17:02:58 32556 3 응답: 250 Directory successfully changed.
2022-08-31 17:02:58 32556 3 명령: PWD
2022-08-31 17:02:58 32556 3 응답: 257 "/"
2022-08-31 17:02:58 32556 3 명령: TYPE I
2022-08-31 17:02:58 32556 3 응답: 200 Switching to Binary mode.
2022-08-31 17:02:58 32556 3 명령: PASV
2022-08-31 17:02:58 32556 3 응답: 227 Entering Passive Mode (123,456,78,901,123,456).
2022-08-31 17:02:58 32556 3 명령: STOR 건축계획서.hwp
2022-08-31 17:02:58 32556 3 응답: 150 Ok to send data.
2022-08-31 17:02:59 32556 3 응답: 226 Transfer complete.
2022-08-31 17:02:59 32556 3 상태: 파일 전송 성공, 192,512 바이트를 1 초에 전송
2022-08-31 17:03:05 32556 2 상태: 연결 수립, 환영 메시지를 기다림...
2022-08-31 17:03:05 32556 2 응답: 220 (vsFTPd 2.2.2)
2022-08-31 17:03:05 32556 2 명령: AUTH TLS
2022-08-31 17:03:05 32556 2 응답: 530 Please login with USER and PASS.
2022-08-31 17:03:05 32556 2 명령: AUTH SSL
2022-08-31 17:03:05 32556 2 응답: 530 Please login with USER and PASS.
2022-08-31 17:03:05 32556 2 상태: 보안되지 않은 서버입니다. TLS를 통한 FTP를 지원하지 않습니다.
2022-08-31 17:03:05 32556 2 명령: USER psm
2022-08-31 17:03:05 32556 2 응답: 331 Please specify the password.
2022-08-31 17:03:05 32556 2 명령: PASS **********
2022-08-31 17:03:05 32556 2 응답: 230 Login successful.
2022-08-31 17:03:05 32556 2 명령: OPTS UTF8 ON
2022-08-31 17:03:05 32556 2 응답: 200 Always in UTF8 mode.
2022-08-31 17:03:05 32556 2 상태: 로그인
2022-08-31 17:03:05 32556 2 상태: C:\Users\admin\Desktop\20220831_163840.jpg 업로드 시작
2022-08-31 17:03:05 32556 2 명령: CWD /
2022-08-31 17:03:05 32556 2 응답: 250 Directory successfully changed.
2022-08-31 17:03:05 32556 2 명령: TYPE I
2022-08-31 17:03:05 32556 2 응답: 200 Switching to Binary mode.
2022-08-31 17:03:05 32556 2 명령: PASV
2022-08-31 17:03:05 32556 2 응답: 227 Entering Passive Mode (182,162,95,167,227,173).
2022-08-31 17:03:05 32556 2 명령: STOR 20220831_163833.jpg
2022-08-31 17:03:08 32556 2 응답: 150 Ok to send data.
2022-08-31 17:03:09 32556 2 응답: 226 Transfer complete.
2022-08-31 17:03:09 32556 2 상태: 파일 전송 성공, 2,230,807 바이트를 3 초에 전송
2022-08-31 17:03:09 32556 2 상태: "/" 디렉터리 목록 조회...
2022-08-31 17:03:09 32556 2 명령: PASV

```
2022-08-31 17:03:09 32556 2 응답: 227 Entering Passive Mode (182,162,95,167,174,32).
2022-08-31 17:03:09 32556 2 명령: LIST
2022-08-31 17:03:09 32556 2 응답: 150 Here comes the directory listing.
2022-08-31 17:03:09 32556 2 응답: 226 Directory send OK.
2022-08-31 17:03:09 32556 2 상태: "/" 디렉터리 목록 조회 성공
```

Metadata

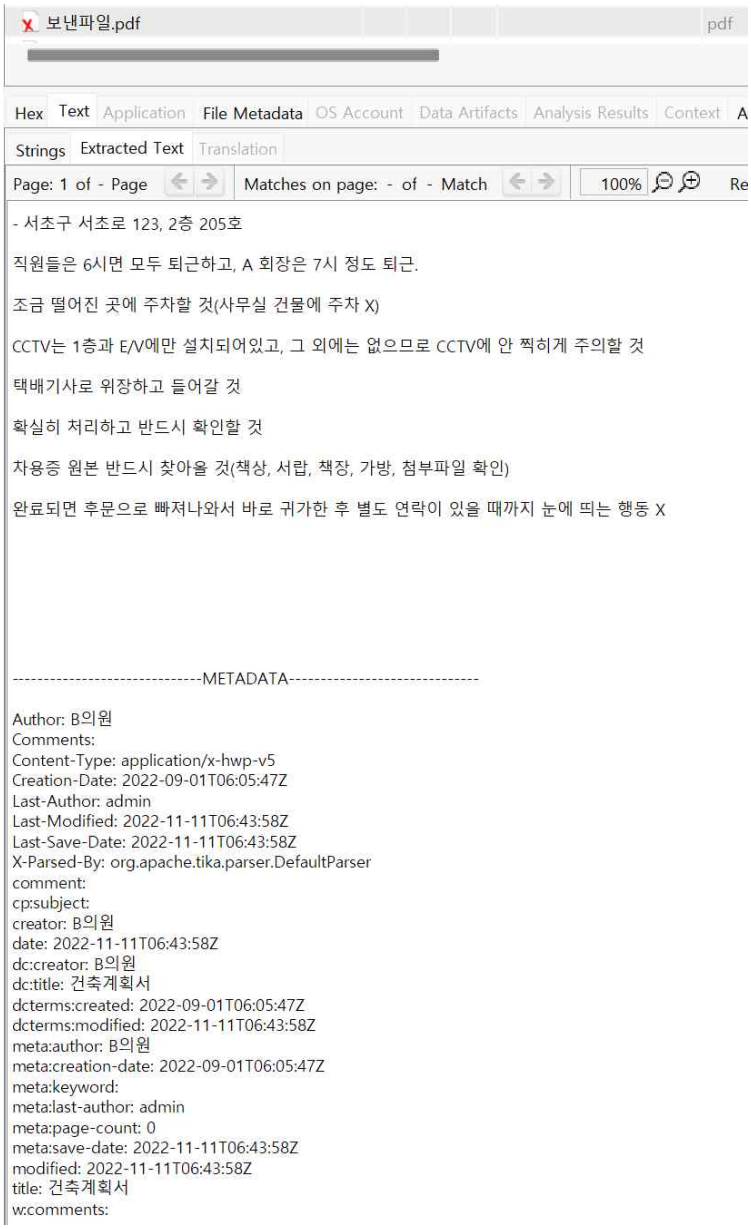
Name:	/img_파티션2개복구_Reimaging_Scenario3.001/vol_vol2/Program Files/FileZilla FTP Client/filezilla.log
Type:	File System
MIME Type:	text/x-log
Size:	8589
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2022-11-11 15:45:39 KST
Accessed:	2022-11-11 16:46:53 KST
Created:	2022-11-11 16:46:53 KST
Changed:	2022-11-11 16:16:10 KST
MD5:	302ad7273e440261e6d06464fce9642e
SHA-256:	8dc31d7c55950e8a65e7dff8e9f5fe0916a0470866aedddde10569b7761ac97b
Hash Lookup Results:	UNKNOWN
Internal ID:	17706

- 박성민이 이현수에게 전달하기 위한 파일을 FTP를 이용하여 서버에 업로드하였을 것이므로, FTP 명령어인 STOR을 대상으로 탐색하여 '건축계획서.hwp'와 '20220831_163833.jpg'을 업로드한 것으로 확인함.

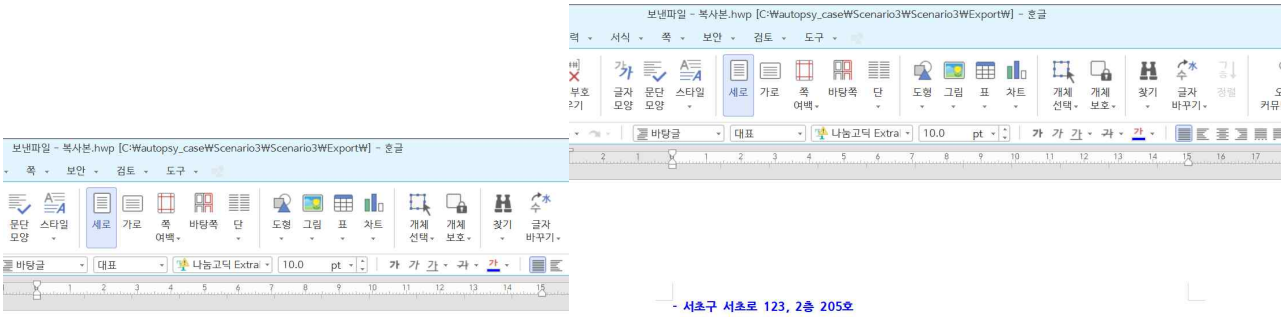
- 이후, 범행을 지시하기 위해 작성한 것으로 추정되는 다음 파일을 발견함.

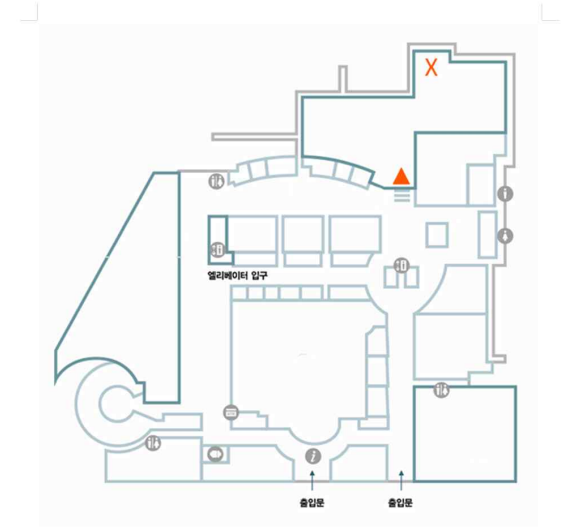
Metadata

Name:	/img_파티션2개복구_Reimaging_Scenario3.001/vol_vol2/Users/bbb/Desktop/보낸파일.pdf
Type:	File System
MIME Type:	application/x-hwp-v5
Size:	192512
File Name Allocation:	Unallocated
Metadata Allocation:	Unallocated
Modified:	2022-11-18 14:54:35 KST
Accessed:	2022-11-18 14:54:13 KST
Created:	2022-11-18 14:54:13 KST
Changed:	2022-11-18 14:59:16 KST
MD5:	Not calculated
SHA-256:	Not calculated
Hash Lookup Results:	UNKNOWN
Internal ID:	20593

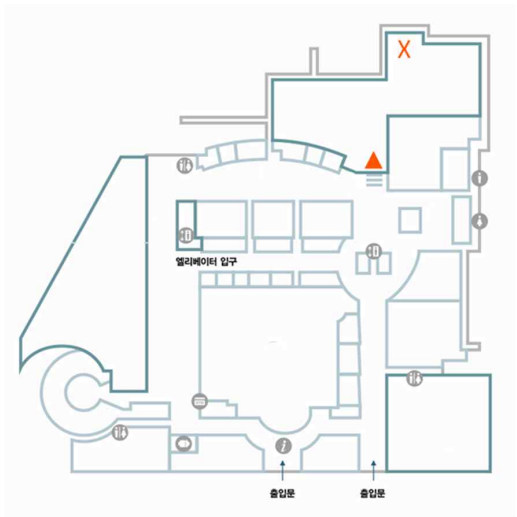


- 해당 파일의 메타데이터에서 'title: 건축계획서', 'Content-Type: application/x-hwp-v5'(한글파일(.hwp))를 발견하여 확장자변조파일로 추측하여 해당파일을 .hwp로 확장자 복구하여 열어봄.





- 서초구 서초로 123, 2층 205호
- 직원들은 6시면 모두 퇴근하고, A 회장은 7시 정도 퇴근.
- 조금 떨어진 곳에 주차할 것(사무실 건물에 주차 X)
- CCTV는 1층과 E/V에만 설치되어있고, 그 외에는 없으므로 CCTV에 안 찍히게 주의할 것
- 택배기사로 위장하고 들어갈 것
- 확실히 처리하고 반드시 확인할 것
- 차용증 원본 반드시 찾아올 것(책상, 서랍, 책장, 가방, 첨부파일 확인)
- 완료되면 후문으로 빠져나와서 바로 귀가한 후 별도 연락이 있을 때까지 눈에 띄는 행동 X



- 그 결과 해당 파일 내용 초기 확인 시 어느 건물 구조도로, 일반적인 건축계획서 내용에 부합하는 문서로 생각되었지만, 이미지 위치를 옮기고 전체 선택 후 글자색을 바꿔보니 다음과 같이 범행을 지시하기 위해 작성된 것으로 보이는 내용이 다음과 같이 쓰여짐.

- 서초구 서초로 123, 2층 205호
- 직원들은 6시면 모두 퇴근하고, A 회장은 7시 정도 퇴근.
- 조금 떨어진 곳에 주차할 것(사무실 건물에 주차 X)
- CCTV는 1층과 E/V에만 설치되어있고, 그 외에는 없으므로 CCTV에 안 찍히게 주의할 것
- 택배기사로 위장하고 들어갈 것
- 확실히 처리하고 반드시 확인할 것
- 차용증 원본 반드시 찾아올 것(책상, 서랍, 책장, 가방, 첨부파일 확인)
- 완료되면 후문으로 빠져나와서 바로 귀가한 후 별도 연락이 있을 때까지 눈에 띄는 행동 X

- 위 내용 중 '**- 서초구 서초로 123, 2층 205호** '에 대한 내용은 피해자가 살해된 장소(서초구)와 일치함.

- 추가적으로, 해당 파일이 휴지통 하위에서도 다음과 같이 탐색되어짐.

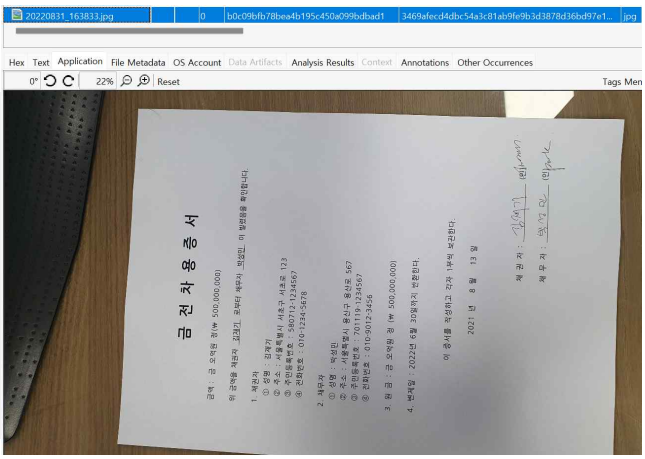
Metadata

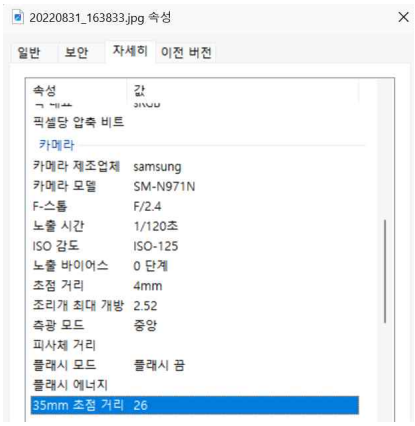
Name:	/img_파티션2개복구_Reimaging_Scenario3.001/vol_vol2/$RECYCLE.BIN/S-1-5-21-952798693-306004704-1019202299-1001/$R9RMM33.pdf
Type:	File System
MIME Type:	application/x-hwp-v5
Size:	192512
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2022-11-11 15:43:58 KST
Accessed:	2022-11-18 14:54:13 KST
Created:	2022-11-18 14:54:13 KST
Changed:	2022-11-18 14:59:16 KST
MD5:	b1477cc581092914d91082a0a951258a
SHA-256:	7ac347e67ef636e48dc4eb7cdff8eb4c49d3530ad6df767d0847043ac000c590
Hash Lookup Results:	UNKNOWN
Internal ID:	17330

- 또한, '20220831_163833.jpg' 파일은 채권자 김재기 채무자 박성민 5억원의 금전차용증서를 발견 exif 속성정보 다음과 같이 확인. 위 내용에서 확인할 수 있는 '**- 차용증 원본 반드시 찾아올 것(책상, 서랍, 책장, 가방, 첨부파일 확인)**'에서의 첨부파일로 보여짐.

Metadata

Name:	/img_파티션2개복구_Reimaging_Scenario3.001/vol_vol4/20220831_163833.jpg
Type:	File System
MIME Type:	image/jpeg
Size:	2230807
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2022-11-11 15:38:20 KST
Accessed:	2022-11-18 09:11:20 KST
Created:	2022-11-18 09:11:20 KST
Changed:	2022-11-11 15:40:23 KST
MD5:	b0c09bfb78bea4b195c450a099bdbad1
SHA-256:	3469afecd4dbc54a3c81ab9fe9b3d3878d36bd97e13398feb94cf3bdde1afc59
Hash Lookup Results:	UNKNOWN
Internal ID:	20519





- 박성민과 김재기의 채무관계가 있었음을 위 내용들에 대해 확인할 수 있었으며 해당 내용이 박성민의 범행 동기로 보여짐.

- 결론적으로, 해당 문서가 범행을 지시하게 작성된 문서로 보이며, 문서를 전달한 방법은 FTP 서버를 이용한 것으로 보여짐.

- 또한, 휴지통에서 범행을 지시하기 위해 작성된 문서가 발견된 것과 와이핑 도구인 eraser 설치의 정황도 아래와 같이 포착된 것으로 미루어 보아 박성민의 추가적인 증거 인멸의 우려가 있음.

Metadata

Name:	/img_파티션2개복구_Reimaging_Scenario3.001/vol_vol2/Users/bbb/Downloads/Eraser 6.2.0.2993.exe
Type:	File System
MIME Type:	application/x-dosexec
Size:	8756728
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2022-09-05 17:35:14 KST
Accessed:	2022-11-11 16:47:46 KST
Created:	2022-11-11 16:47:46 KST
Changed:	2022-09-05 17:35:33 KST
MD5:	ccc33a97215d0f681f0a93e9c2cbea21
SHA-256:	062ccb4e9e6f90d3e5b0df23a4c85c65690a1b527a70015c914e17468fc74bbc
Hash Lookup Results:	UNKNOWN
Internal ID:	16799
Downloaded From:	https://jaist.dl.sourceforge.net/project/eraser/Eraser%206/6.2/Eraser%206.2.0.2993.exe