문제 6.

6. 유출된 파일을 찾고 그 과정을 상세히 기술하시오.

1) 신청서.pdf

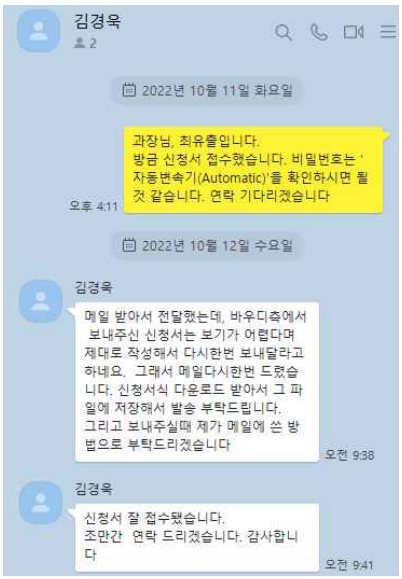
- 확장자변조파일로 의심되는 '신청서.pdf'파일 시그니처 확인 시 정상적 .pdf 파일의 시그니처(25 50 44 46)가 아닌 압축파일의 확장자 .zip의 시그니처(50 4B 03 04)로 변조됨을 확인하여 복원하여 압축파일을 해제하려 하였으나 암호화되었음을 확인함.

Metadata

Name:	/img_파티션복구_RAW_시나리오1_변속기기술유출.001/vol_vol2/Users/yc.choi/Downloads/신청서.pdf
Type:	File System
MIME Type:	application/zip
Size:	114441490
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2022-10-11 16:00:54 KST
Accessed:	2022-10-12 17:28:17 KST
Created:	2022-10-12 17:28:16 KST
Changed:	2022-10-12 09:32:51 KST
MD5:	af93280abed1c26b547ebd63aa9e11e1
SHA-256:	c1787e0138b60ff6931f4ec5b13b9b49a77d55aa3d55cb22be1e5984d98ce1e6
Hash Lookup Results:	UNKNOWN
Internal ID:	19427

2) 출력할가족사진2.jpg

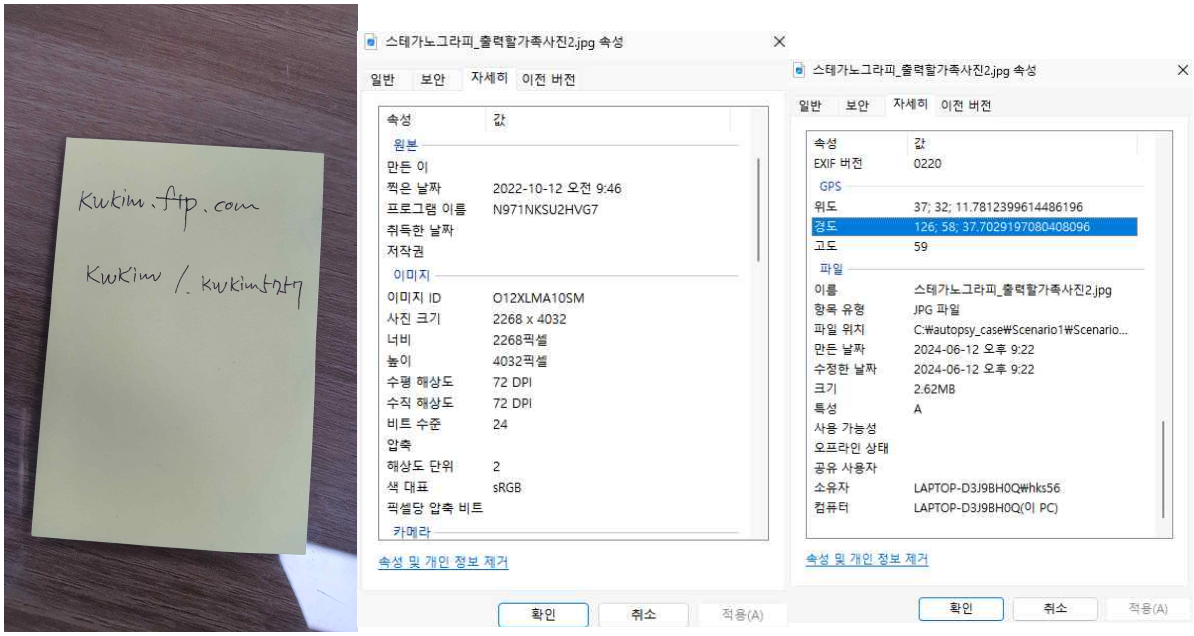
- 헤더시그니처훼손파일로 의심되는 '출력할가족사진2.jpg' 시그니처 확인 시 정상적 .jpg 파일의 시그니처(FF D8 FF D0)가 아닌 00 00 FF D0로 훼손되어 있음을 확인하여 복원하여 확인한 결과, 김경욱과의 카카오톡 대화 캡처본을 확인하였다.



Metadata

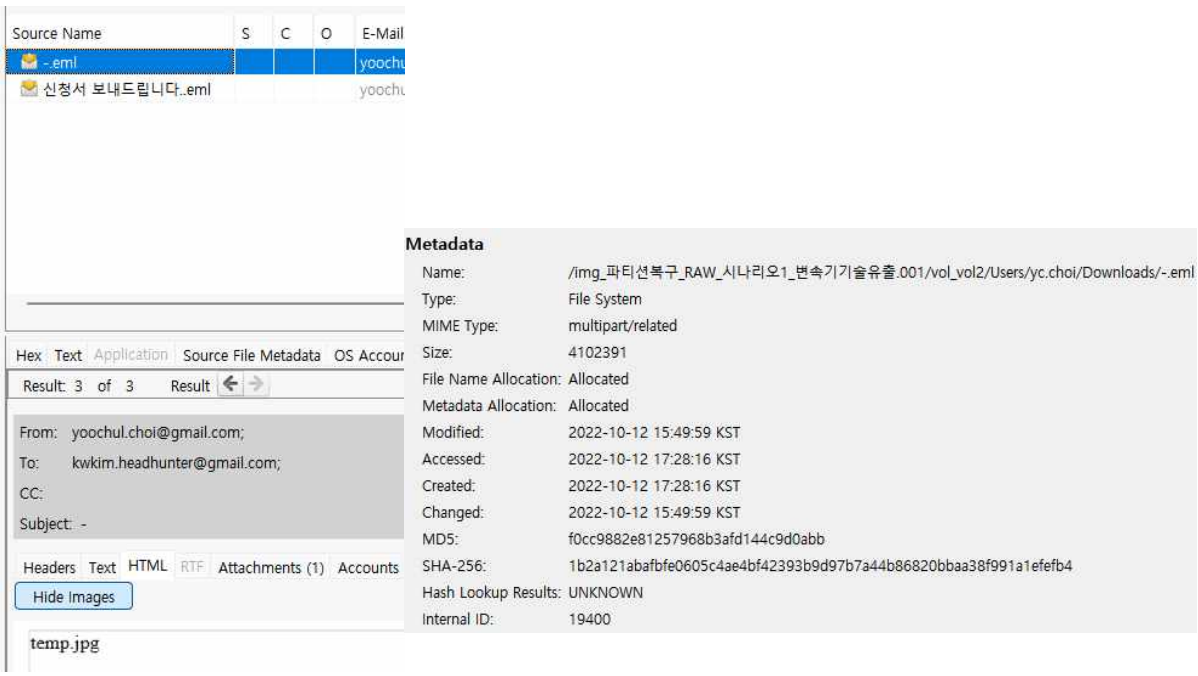
Name:	/img_파티션복구_RAW_시나리오1_변속기기술유출.001/vol_vol4/DCIM/출력할가족사진2.jpg
Type:	File System
MIME Type:	application/octet-stream
Size:	2897290
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2022-10-12 10:06:47 KST
Accessed:	2022-10-12 17:24:08 KST
Created:	2022-10-12 17:24:08 KST
Changed:	2022-10-12 13:44:21 KST
MD5:	5594449eb4f3a3fbaaf780b07cf7e099
SHA-256:	54b77fb71f5a4bd84ea3a14f9203cff8a7af93dc2e5b1a65fc65556a57d4e00c
Hash Lookup Results:	UNKNOWN
Internal ID:	20946

- 또한, 해당 파일에 스테가노그래피 기법을 활용하여 FTP서버 주소와 계정명/PW를 적어놓은 포스트잇을 촬영한 아래 사진을 발견하였고, EXIF 메타데이터 분석을 실시하였음.



3) -.eml

- 위 카카오톡 내용에서 확장자 변조된 압축파일인 '신청서.pdf' 비밀번호를 유추할 수 있는 단서를 발견하여 해당 단서 내용을 기반으로 사전대입을 해보았지만, 비밀번호가 맞지 않았음. 따라서, 비밀번호 내용을 김경욱에게 따로 전달한 것으로 추정하여 김경욱에게 송신한 이메일 파일을 확인한 결과 'temp.jpg' 파일을 김경욱에게 전달한 정황을 발견하였음.

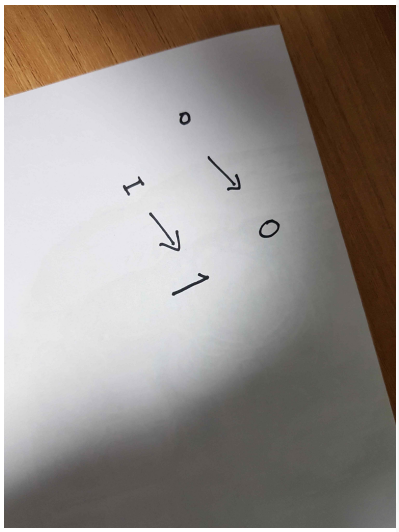


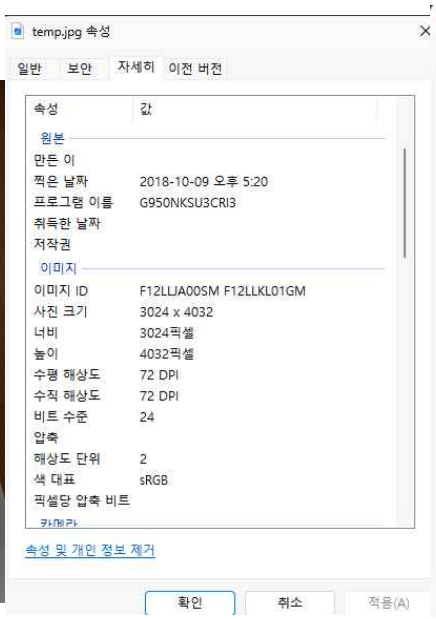
4) temp.jpg

- -.eml 파일에서 최유출이 김경욱에게 메일 송신 시 첨부했던 'temp.jpg'파일에 대한 아래와 같은 원본 파일을 발견함.

Metadata

Name:	/img_파티션복구_RAW_시나리오1_변속기기술유출.001/vol_vol2/Users/yc.choi/Downloads/-.eml/temp.jpg
Type:	Derived
MIME Type:	image/jpeg
Size:	2997182
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	0000-00-00 00:00:00
Accessed:	0000-00-00 00:00:00
Created:	0000-00-00 00:00:00
Changed:	0000-00-00 00:00:00
MD5:	e40ed591e1e48a2ffc9ffec9e2fefdc5
SHA-256:	5ff525e5dc48aa5c7ebf3a00664e16b041f0926d0bd4b172f212656d48da7162
Hash Lookup Results:	UNKNOWN
Internal ID:	33615

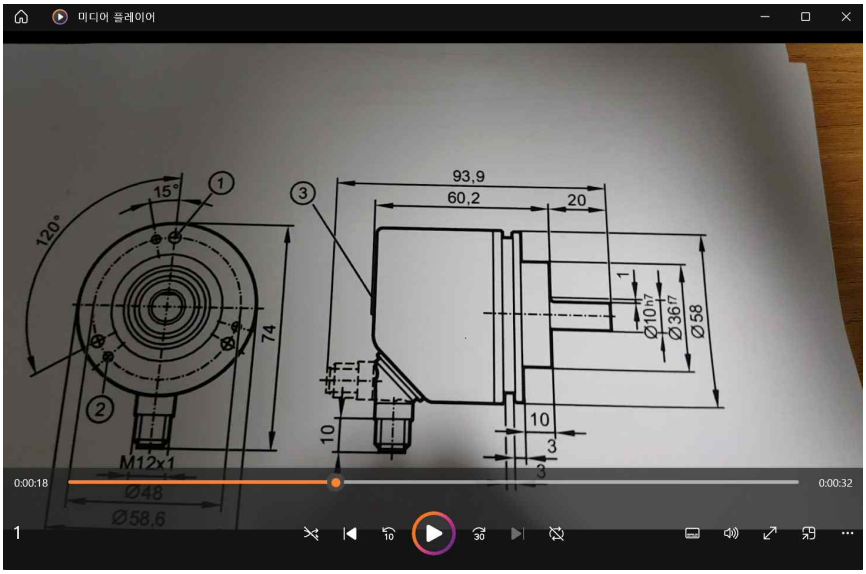




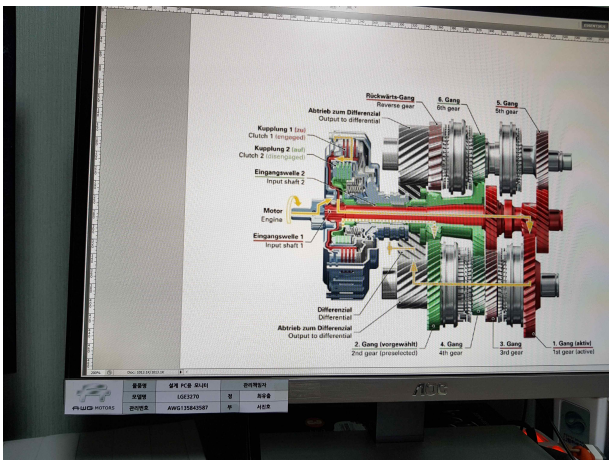
- 'temp.jpg' 이미지 내용을 확인하여 비밀번호를 유추해 'aut0mat1c'으로 확장자변조파일인 '신청서.pdf' 압축파일을 압축해제하여 내용 확인함.

5) 확장자변조압축파일 ‘신청서.pdf’에 대한 압축 풀기 및 내용 확인

- 아래 첨부한 사진은 해당 압축 파일 내의 ‘1.mp4’ 파일로, 설계도면으로 보이는 자료를 넘기고 있었음을 확인.

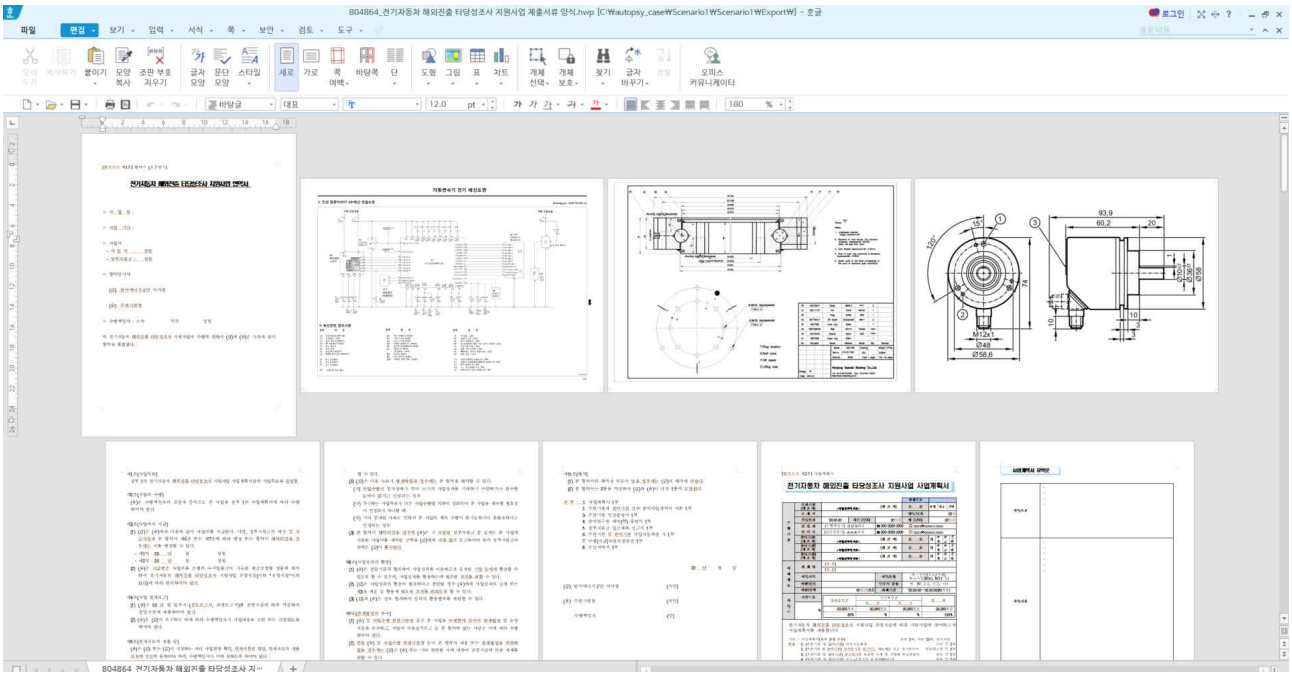


- 아래 첨부한 사진은 해당 압축 파일 내의 ‘2.jpg’ 파일로, 설계도면으로 보이는 자료임을 확인.



6) 전기자동차 해외진출 타당성조사 지원상업 제출서류 양식.hwp

- 김경욱과의 카톡내용을 통해 다른 형식으로의 관련 자료 유출 가능성이 높다고 판단하여 김경욱으로부터 송신받은 이메일 파일을 분석하였음. 김경욱으로부터 송신받은 이메일 첨부파일 중 하나로 전기자동차 해외진출 타당성조사 관련 신청서식을 최유출이 해당 문서를 다운로드한 한 후 아래와 같이 설계도면을 삽입한 정황을 확인하였음. 이는 최유출이 김경욱의 요청에 의해 2차적으로 형식을 바꾸어 자료를 유출한 것으로 보임.



Metadata

Name:	/img_파티션복구_RAW_시나리오1_변속기기술유출.001/vol_vol3/정부사업/전기자동차 해외진출 타당성조사 지원사업 제출서류 양식.hwp
Type:	File System
MIME Type:	application/x-hwp-v5
Size:	804864
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2018-10-09 16:38:00 KST
Accessed:	2022-10-12 00:00:00 KST
Created:	2022-10-12 17:23:00 KST
Changed:	0000-00-00 00:00:00
MD5:	41081b581df45997a08ae37771c507e7
SHA-256:	72af180d669db6b1e839541e59eb4f365b4ddfd312dffc72aaf5ae39e5865b02
Hash Lookup Results:	UNKNOWN
Internal ID:	20599