

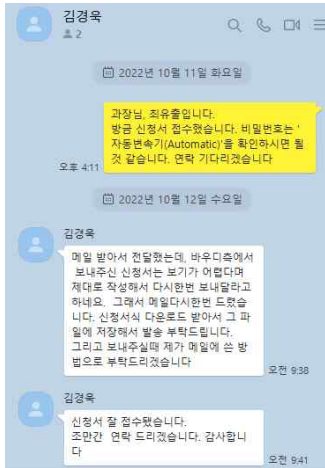
6. 유출된 파일을 찾고 그 과정을 상세히 기술하시오.

/img_파티션복구_RAW_시나리오1_변속기기술유출.001/vol_vol2/Users/yc.choi/Downloads/
신청서.pdf - 원래 zip이었는데 pdf로 바뀜. zip파일 압축풀기 암호화로 실패

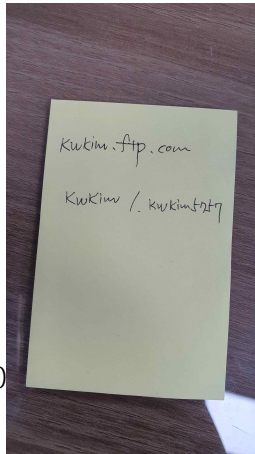
<헤드헌터 최경욱과의 연락 카카오톡>

출력할가족사진으로 헤더시그니처변조, 스테가노그래피

/img_파티션복구_RAW_시나리오1_변속기기술유출.001/vol_vol4/DCIM/출력할가족사진2.jpg



000220D0 / 002C3520



내부사진

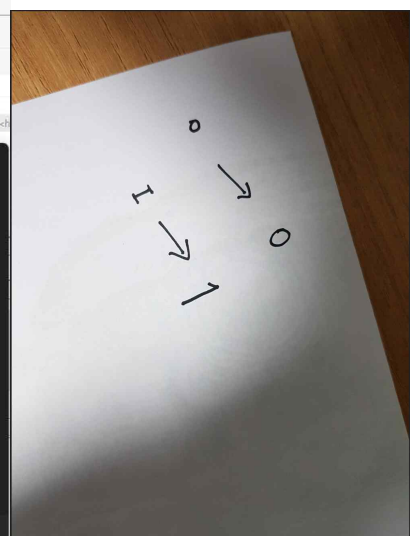
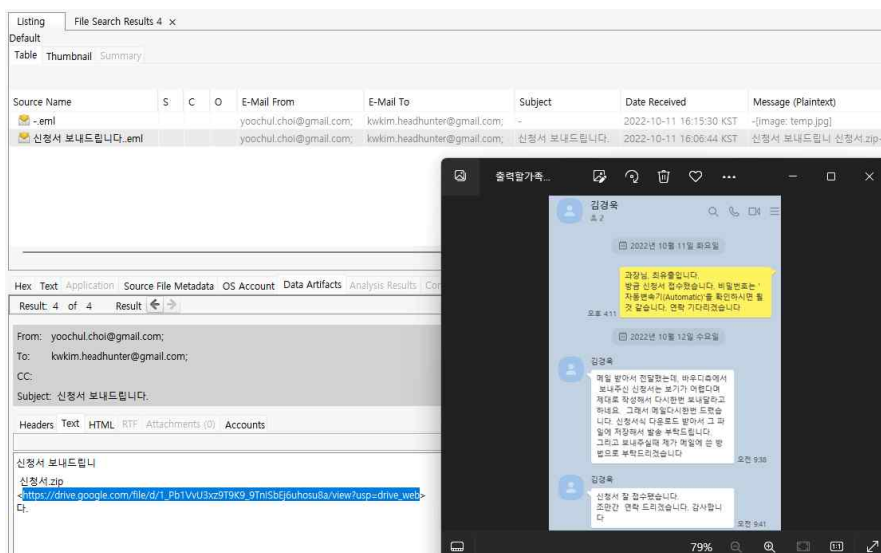
내부 메모장 사진 EXIF 정보확인

<이메일>

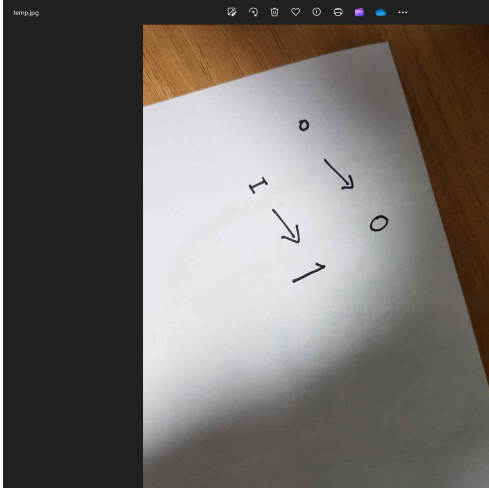
/img_파티션복구_RAW_시나리오1_변속기기술유출.001/vol_vol2/Users/yc.choi/Downloads/- .eml

이메일 파일, 내용x ,최유출 -> kwkim(gmail)로 보냄 temp.jpg 첨부 o->0, l->1

exif 정보



/ i m g _ 파 티 셴 복 구 _ R A W _ 시 나 리 오 1 _ 변 속 기 기 술 유
출.001/vol_vol2/Users/yc.choi/Downloads/temp.jpg
이메일 temp.jpg의 원본파일로, 시그니처 훼손되었음.

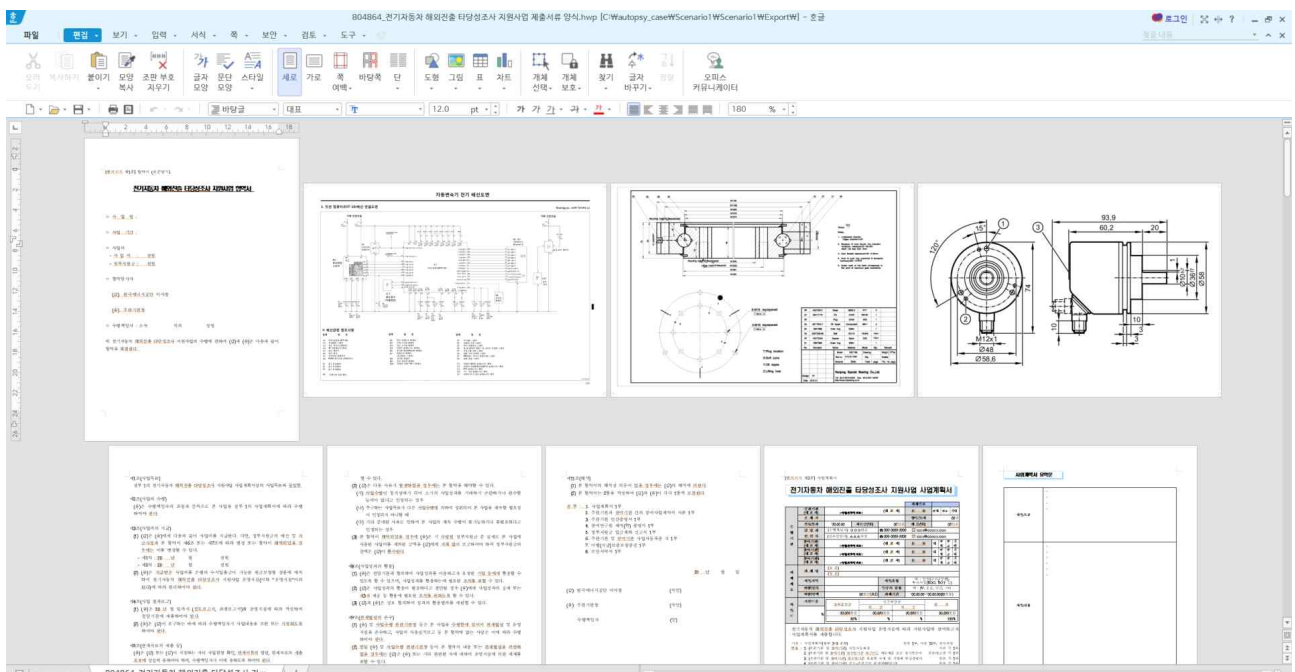


위 내용 기반으로 신청서.pdf로 시그니처 훼손되었던 파일 신청서.zip으로 복구 후 압축해제 비
밀번호를 특정(aut0mat1c)

<1차 유출>

<2차 유출>

/img_파티션복구_RAW_시나리오1_변속기기술유출.001/vol_vol3/정부사업/전기자동차 해외진출
타당성조사 지원사업 제출서류 양식.hwp



ftp 서버를 통해 보낸것으로 추정됨

C:\Users\yc.choi\Desktop\전기자동차 해외진출 타당성조사 지원사업 제출서류 양식.hwp 업로드 시작, 804,864 바이트와 용량 동일

<엔진 토크 도면>

/img_파티션복구_RAW_시나리오1_변속기기술유출.001/vol_vol2/Users/yc.choi/Downloads/

요기에도있음

/img_파티션복구_RAW_시나리오1_변속기기술유출.001/vol_vol3/연구개발/FinalTest_report.pdf

9. 증거 USB의 소유자를 확인할 수 있는 단서를 모두 찾아 기술하시오.

<공인인증서>

/img_파티션복구_RAW_시나리오1_변속기기술유출.001/vol_vol4/NPKI/yessign/User/cn=최유출()0123456984135748754000023,ou=SAH,ou=personal5JC,o=yessign,c=kr/signPri.key

Name	S	C	O	MIME Type	Extension	Modified Time	Size	Change Time	Access Time	Created Time	Flags(Dir)	Flags(Meta)	Known	Location
signPri.key	0	0	0	text/plain	key	2018-10-07 07:04:58 KST	11	2022-10-11 09:49:10 KST	2022-10-12 17:24:12 KST	2022-10-12 17:24:12 KST	Allocated	Allocated	unknown	/img_파티션복구_RAW_시나리오1_변속기기술유출.001/vol_vol4/NPKI/yessign/User/cn=최유출()0123456984135748754000023,ou=SAH,ou=personal5JC,o=yessign,c=kr/signPri.key
signCert.der	0	0	0	text/plain	der	2018-10-07 07:04:40 KST	12	2022-10-11 09:49:10 KST	2022-10-12 17:24:12 KST	2022-10-12 17:24:12 KST	Allocated	Allocated	unknown	/img_파티션복구_RAW_시나리오1_변속기기술유출.001/vol_vol4/NPKI/yessign/User/cn=최유출()0123456984135748754000023,ou=SAH,ou=personal5JC,o=yessign,c=kr/signPri.key
parent folder	0	0	0	text/plain	der	2022-10-12 17:24:12 KST	272	2022-10-12 17:24:12 KST	2022-10-12 17:24:12 KST	2022-10-12 17:24:12 KST	Allocated	Allocated	unknown	/img_파티션복구_RAW_시나리오1_변속기기술유출.001/vol_vol4/NPKI/yessign/User/cn=최유출()0123456984135748754000023,ou=SAH,ou=personal5JC,o=yessign,c=kr/signPri.key
current folder	0	0	0	text/plain	der	2022-10-12 17:24:12 KST	264	2022-10-12 17:24:12 KST	2022-10-12 17:24:12 KST	2022-10-12 17:24:12 KST	Allocated	Allocated	unknown	/img_파티션복구_RAW_시나리오1_변속기기술유출.001/vol_vol4/NPKI/yessign/User/cn=최유출()0123456984135748754000023,ou=SAH,ou=personal5JC,o=yessign,c=kr/signPri.key

Metadata

Name: /img_파티션복구_RAW_시나리오1_변속기기술유출.001/vol_vol4/NPKI/yessign/User/cn=최유출()0123456984135748754000023,ou=SAH,ou=personal5JC,o=yessign,c=kr/signPri.key

Type: File System

MIME Type: text/plain

Size: 11

File Name Allocation: Allocated

Metadata Allocation: Allocated

Modified: 2018-10-07 07:04:58 KST

Accessed: 2022-10-12 17:24:12 KST

Created: 2022-10-12 17:24:12 KST

Changed: 2022-10-11 09:49:10 KST

MD5: 35bd7907674f43b99d01306d0dbx43

SHA-256: f6ea0e106777c4b23f526d980aff744c56d44ed260b4e6e9f7d47a2c7740b09

Hash Lookup Results: UNKNOWN

Internal ID: 21007

From The Sleuth Kit istat Tool:

MFT Entry Header Values:

Entry: 68 Sequence: 1

\$LogFile Sequence Number: 5299739

<AWG 10T50 성능테스트 결과보고서 - 담당자 최유출>

휴지통에서 발견, \$RS4NCLQ

/img_파티션복구_RAW_시나리오1_변속기기술유출.001/vol_vol3/\$RECYCLE.BIN/\$RS4NCLQ.pdf

<영수증 신용카드 영수증 정보 - KTX2개, 주유영수증2개>

/img_파티션복구_RAW_시나리오1_변속기기술유출.001/vol_vol4/scan/20180812-1.jpg



신용카드정보 동일 추정

<신한은행 거래내역>

/img_파티션복구_RAW_시나리오1_변속기기술유출.001/vol_vol4/etc/신한은행_거래내역_E1235436844.xlsx

시그니처 변조후 삭제한거 복구함

신한은행 거래내역

성명	최유철	조회기간	2022.10.05 - 2022.10.20
계좌번호	****-**-****12334	요청일시	2022.10.21 13:40:26

※ 금액앞에 '-' 표시는 출금 금액입니다.

※ 본 거래내역은 법적효력이 없는 참고용 문서입니다.

거래일시	구분	거래금액	거래 후 잔액	취급점	내용	메모
2022.10.05 19:44:00	입금	₩500,000	₩18,035,200	0032	홍길동	
2022.10.06 20:36:11	출금	-₩27,300	₩18,007,900	0056	파리바게뜨	
2022.10.07 10:46:33	출금	-₩730,000	₩17,277,900	0089	김민수	
2022.10.09 13:45:57	출금	-₩9,500	₩17,268,400	0012	CU용산삼각	
2022.10.09 12:28:55	출금	-₩17,600	₩17,250,800	0056	썬스타벅스코	
2022.10.09 20:29:11	출금	-₩78,200	₩17,172,600	0032	나폴리키친	
2022.10.09 22:40:44	출금	-₩48,000	₩17,124,600	0065	골프존티에스	
2022.10.11 10:41:15	출금	-₩14,000	₩17,110,600	0059	GS25서초반	
2022.10.15 19:39:40	출금	-₩275,600	₩16,835,000	0012	(주)롯데마트서초	
2022.10.18 08:40:39	입금	₩300,000,000	₩316,835,000	0134	B	
2022.10.18 08:42:45	입금	₩200,000,000	₩516,835,000	0134	B	
2022.10.18 17:29:03	출금	-₩500,000,000	₩16,835,000	0019	최유철	

10. 최유철이 기술 유출을 한 방법과 그에 대한 댓가는 무엇인지 알 수 있는 증거를 모두 찾고 기술하시오.

<김경욱->최유철 최초 접근 이메일>

/img_파티션복구_RAW_시나리오1_변속기기술유출.001/vol_vol3/정부사업/HeadHunter Korea
안녕하세요 최유철님. 헤드헌터코리아의 김경욱 과장이라고 합니다..msg

<김경욱-> 최유철 이메일>

/img_파티션복구_RAW_시나리오1_변속기기술유출.001/vol_vol3/정부사업/요청하신 신청서 서식 다시 보내드립니다..msg

기존 내용 불가하니 다시 보내라는 카톡 내용과 연관. 내용 ftp 주소와 로그인 정보(포스트잇 확인 내용)을 기재

<헤드헌터와의 연락 - 내용에 BAUDI사가 있음>

/ i m g _ 파 티 셴 복 구 _ R A W _ 시 나 리 오 1 _ 변 속 기 기 술 유
출.001/vol_vol2/Users/yc.choi/Downloads/HeadHunter korea 안녕하세요. 김경욱입니
다..msg

최유출이 궁금해했던 연봉 등 조건에 대한 답변 / 큰 결심 -> 이직결심
유선상 얘기했던 부분 처리 시 별도 보수 지급.

<usb 연결기록>

문제에서 제공한 usb serial no.와 동일한 usb 연결 흔적

Type	Value	Source(s)
Date/Time	2022-10-11 16:31:34 KST	Recent Activity
Device Make	SanDisk Corp.	Recent Activity
Device Model	Product: 557C	Recent Activity
Device ID	4C530012200403114081	Recent Activity
Source File Path	/img_파티션복구_RAW_시나리오1_변속기기술유출.001/vol_vol2/Windows/System32/config/SYSTEM	
Artifact ID	-9223372036854775734	

<ftp로그>

/ i m g _ 파 티 셴 복 구 _ R A W _ 시 나 리 오 1 _ 변 속 기 기 술 유
출.001/vol_vol2/Users/yc.choi/Documents/filezilla.log

C:\Users\yc.choi\Desktop\전기자동차 해외진출 타당성조사 지원사업 제출서류 양식.hwp 업로
드 시작, 804,864 바이트

