문제 9.

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

1) 최유출의 공인인증서파일 발견

- /img_파티션복구_RAW_시나리오1_변속기기술유출.001/vol_vol4/NPKI/yessign/User/cn=최유출()01234569841357487540000 23,ou=SAH,ou=personal5JC,o=yessign,c=kr/ 하위폴더에서 최유출의 공인인증서 파일인 signPri.key, signCert.der을 발견하여 해당 증거 USB의 소유자가 최유출임을 추정가능.

Metadata

Name:	/img_파티션복구_RAW_시나리오1_변속기기술유출.001/vol_vol4/NPKI/yessign/User/cn=최유출()012345698413574875400002 3,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:	35bd7907e7afcf43b39e01308d0dbc43
SHA-256:	f6ea0e106777ce4b23fd26d980aff74465ed44ed260b4e6e9f7b47a2c7740b09
Hash Lookup Results:	UNKNOWN
Internal ID:	21007

<signPri.key 파일 메타데이터>

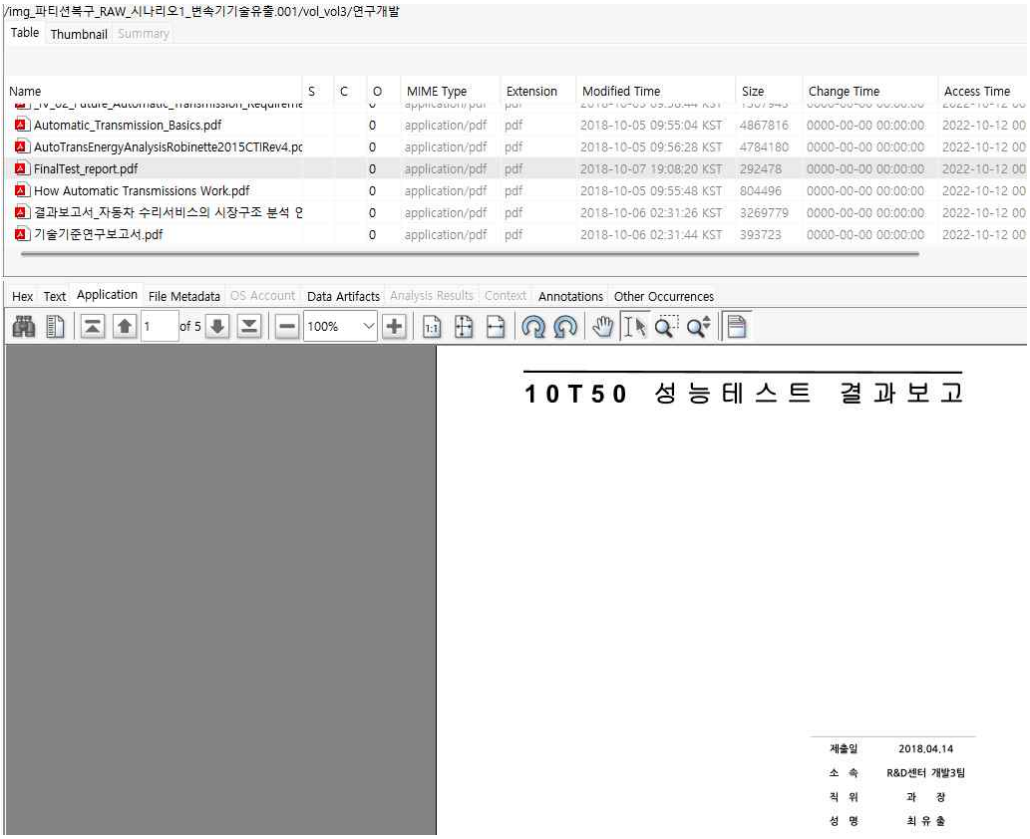
Metadata

Name:	/img_파티션복구_RAW_시나리오1_변속기기술유출.001/vol_vol4/NPKI/yessign/User/cn=최유출()012345698413574875400002 3,ou=SAH,ou=personal5JC,o=yessign,c=kr/signCert.der
Type:	File System
MIME Type:	text/plain
Size:	12
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2018-10-07 07:04:40 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:	ab4d36bec83a241b7a481cc733f2eb91
SHA-256:	2e6d551e32bfa560f0737a6b6038f5b5e138e605584205136b9a2cc4929e0861
Hash Lookup Results:	UNKNOWN
Internal ID:	21006

<signCert.der 파일 메타데이터>

2) 최유출 작성 문건 발견

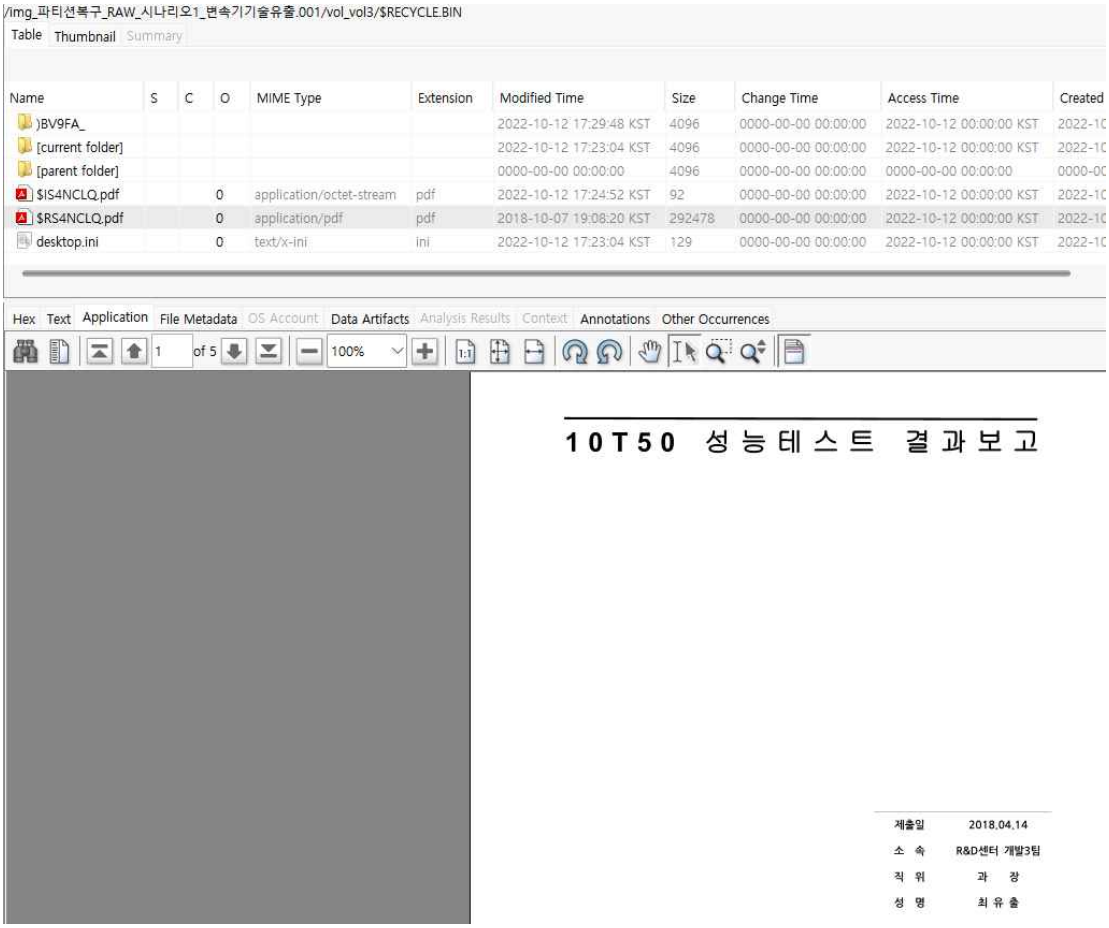
- 최유출이 작성한 문건인 'FinalTest_report.pdf'를 발견하였음.



Metadata

Name:	/img_파티션복구_RAW_시나리오1_변속기기술유출.001/vol_vol3/연구개발/FinalTest_report.pdf
Type:	File System
MIME Type:	application/pdf
Size:	292478
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2018-10-07 19:08:20 KST
Accessed:	2022-10-12 00:00:00 KST
Created:	2022-10-12 17:23:02 KST
Changed:	0000-00-00 00:00:00
MD5:	cc7397dbc62f4c487caee310fb8fb924
SHA-256:	012b0f10afda498d5a970c6d47e1381114d97e94bf99dfb54557af52362f2fa5
Hash Lookup Results:	UNKNOWN
Internal ID:	20773

- 동일한 내용의 문건이 vol3 휴지통 폴더에 들어가 있는 것을 추가로 확인하였고, 해당 증거 USB가 최유출임을 추정 가능.



Metadata

Name:	/img_파티션복구_RAW_시나리오1_변속기기술유출.001/vol_vol3/$RECYCLE.BIN/$RS4NCLQ.pdf
Type:	File System
MIME Type:	application/pdf
Size:	292478
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2018-10-07 19:08:20 KST
Accessed:	2022-10-12 00:00:00 KST
Created:	2022-10-12 17:23:01 KST
Changed:	0000-00-00 00:00:00
MD5:	cc7397dbc62f4c487caee310fb8fb924
SHA-256:	012b0f10afda498d5a970c6d47e1381114d97e94bf99dfb54557af52362f2fa5
Hash Lookup Results:	UNKNOWN
Internal ID:	20790

3. 같은 카드번호의 영수증 신용카드 영수증 정보 - KTX2개, 주유영수증2개

- /img_파티션복구_RAW_시나리오1_변속기기술유출.001/vol_vol4/scan/ 하위폴더에서 같은 카드번호의 총 4개 영수증 스캔 파일을 발견. 해당 카드 소유자가 최유출과 동일하다면 해당 증거 USB의 소유자가 최유출임을 추정 가능.


매출전표(고객용)
신한비자카드 신용승인
거래일시 18-08-12 20:13:19
카드번호 9999-****-****-8888 (S)
유효기간 (년/월) : **/** 일시불
가맹점번호 113945671
승인번호 8568634
매입사 : 신한 (전자서명전표)
수량 : 37.05L 단가: 1619원
유 종 휘발유
판매금액 54,546원
부가가치세 5,454원
봉사료 0원
합 계 60,000원
가맹점명 좋은기름주유소
사업자번호 353-87-52345
대표자명 : 박관식 TEL 02 95151123
주소 : 서울특별시 강남구 밤배로 129
CATID:31532587 전표No:2215680308
감사합니다

Metadata

Name:	/img_파티션복구_RAW_시나리오1_변속기기술유출.001/vol_vol4/scan/20180812-1.jpg
Type:	File System
MIME Type:	image/jpeg
Size:	269830
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2018-10-08 02:21:38 KST
Accessed:	2022-10-12 17:24:12 KST
Created:	2022-10-12 17:24:12 KST
Changed:	2022-10-11 09:49:11 KST
MD5:	c84600a666e52ff2f13e7db642336686
SHA-256:	96b33170d8323fac02e82755f530a1aa407af09edc381395f6f93da41f41667f
Hash Lookup Results:	UNKNOWN
Internal ID:	21017


매출전표(고객용)
신한비자카드 신용승인
거래일시 18-05-05 08:32:44
카드번호 9999-3597-****-8888 (S)
유효기간 (년/월) : **/** 일시불
가맹점번호 213544687
승인번호 5598435
매입사 : 신한 (전자서명전표)
수량 : 35.00L 단가: 1600원
유 종 휘발유
판매금액 50,910원
부가가치세 5,090원
봉사료 0원
합 계 56,000원
가맹점명 SK행복주유소
사업자번호 123-56-98745
대표자명 : 김행복 TEL 042 56891235
주소 : 대전광역시 서구 대덕대로 175번길 32
CATID:11235579 전표No:1235560000
감사합니다

Metadata

Name:	/img_파티션복구_RAW_시나리오1_변속기기술유출.001/vol_vol4/scan/20180505-1.jpg
Type:	File System
MIME Type:	image/jpeg
Size:	271110
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2018-10-08 02:22:14 KST
Accessed:	2022-10-12 17:24:12 KST
Created:	2022-10-12 17:24:12 KST
Changed:	2022-10-11 14:25:59 KST
MD5:	3fea271cf3e0893b969c55860e5911be
SHA-256:	28749f19747f92955ee4c4d40ba2d2195e47ff86a8b9901847a1c58c700b05d1
Hash Lookup Results:	UNKNOWN
Internal ID:	21015


영수증(고객용)
Let's Korail
NO 20180206-125647
2018/02/06 KTX 864 일반실
서울(20:17) → 대전 (21:18)
어른 : 1 어린이 : 0 할인 : 0 비고 :
신용카드 결제 신한 9999-****-****-8888 (일시불) 2018-02-06 18:32:11 ₩23,700
사업자 한국철도공사 314-82-10024
주소 대전광역시 동구 중앙로 240
발매일자 2018-02-06
발행일시 2018-02-06 18:32:11
대표전화 1544-7730

Metadata

Name:	/img_파티션복구_RAW_시나리오1_변속기기술유출.001/vol_vol4/scan/20180206-1.jpg
Type:	File System
MIME Type:	image/jpeg
Size:	88696
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2018-10-07 07:45:46 KST
Accessed:	2022-10-12 17:24:12 KST
Created:	2022-10-12 17:24:12 KST
Changed:	2022-10-11 14:26:11 KST
MD5:	995829cf0944f2f2d6b997752eacf7ec
SHA-256:	d7ebfd6b7fc8159c662ed5a830c74de62124ccfc01eba367213c3e6acd2e1fd3
Hash Lookup Results:	UNKNOWN
Internal ID:	21013


영수증(고객용)
Let's Korail
NO 20180204-225587
2018/02/04 KTX 182 일반실
대전(14:42) → 서울 (15:43)
어른 : 1 어린이 : 0 할인 : 0 비고 :
신용카드 결제 신한 9999-****-****-8888 (일시불) 2018-02-04 13:57:24 ₩23,700
사업자 한국철도공사 314-82-10024
주소 대전광역시 동구 중앙로 240
발매일자 2018-02-04
발행일시 2018-02-04 13:57:24
대표전화 1544-7730

Metadata

Name:	/img_파티션복구_RAW_시나리오1_변속기기술유출.001/vol_vol4/scan/20180204-1.jpg
Type:	File System
MIME Type:	image/jpeg
Size:	88720
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2018-10-07 07:43:02 KST
Accessed:	2022-10-12 17:24:12 KST
Created:	2022-10-12 17:24:12 KST
Changed:	2022-10-11 10:11:06 KST
MD5:	c0d2207b570467ec6b9c5a75e0de98bb
SHA-256:	36c7bcf682f2f04ecfee93d3c4ce62f4c9dfa30fa6b540c1a0335b5b0aca96b5
Hash Lookup Results:	UNKNOWN
Internal ID:	21011

4. 신한은행 거래내역

- /img_파티션복구_RAW_시나리오1_변속기기술유출.001/vol_vol4/etc/신한은행_거래내역_E1235436844.xlsx 시그니처 훼손 후 삭제 한 것 복구하여 분석 진행. 이후 해당 파일 열어 확인 시 신한은행 거래내역이 있었고, 성명이 최유출로 되어있음을 확인.

Metadata

Name:	/img_파티션복구_RAW_시나리오1_변속기기술유출.001/vol_vol4/etc/신한은행_거래내역_E1235436844.xlsx
Type:	File System
MIME Type:	application/octet-stream
Size:	13543
File Name Allocation:	Unallocated
Metadata Allocation:	Unallocated
Modified:	2022-10-12 17:24:37 KST
Accessed:	2022-10-12 17:24:11 KST
Created:	2022-10-12 17:24:11 KST
Changed:	2022-10-12 17:24:37 KST
MD5:	Not calculated
SHA-256:	Not calculated
Hash Lookup Results:	UNKNOWN
Internal ID:	21032

신한은행 거래내역

성명	최유출	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	㈜스타벅스코	
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	최유출	