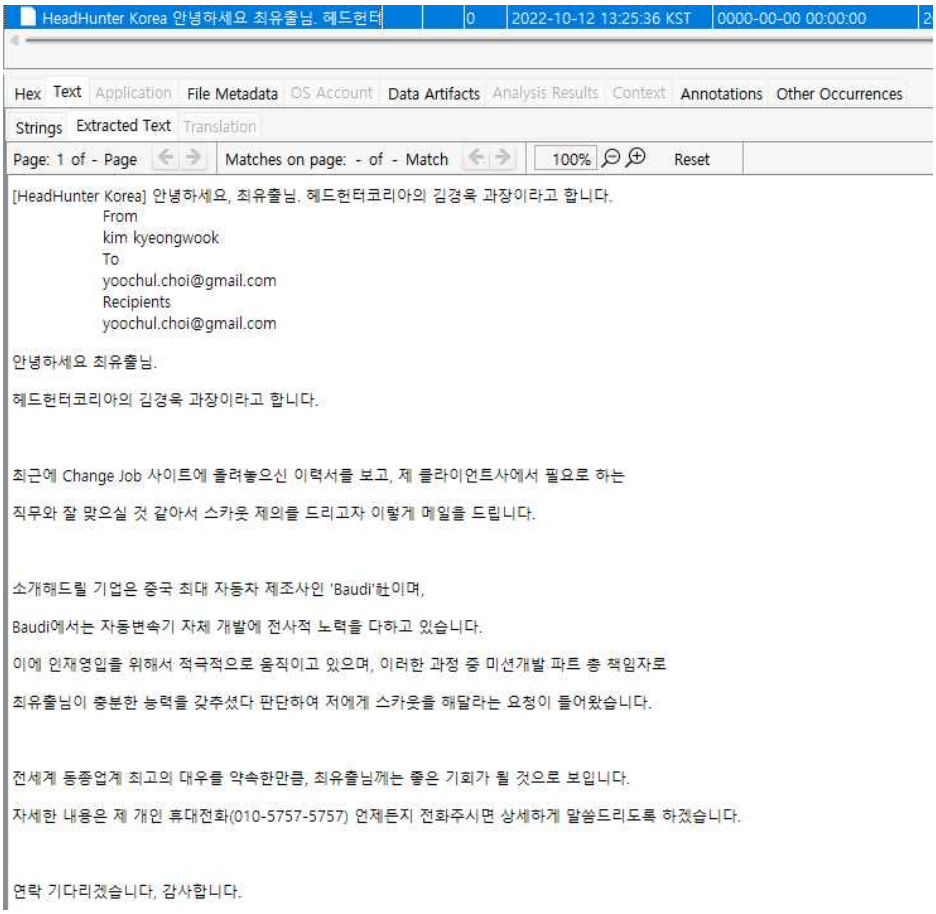
문제 10.

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

1) 이메일 송·수신 흔적

가. 김경욱->최유출 최초 접근

- 헤드헌터코리아 소속의 김경욱 과장이 최유출에게 'Baudi社'로의 스카웃 제의를 이메일을 통해 송부한 이메일 파일을 아래와 같이 발견함.

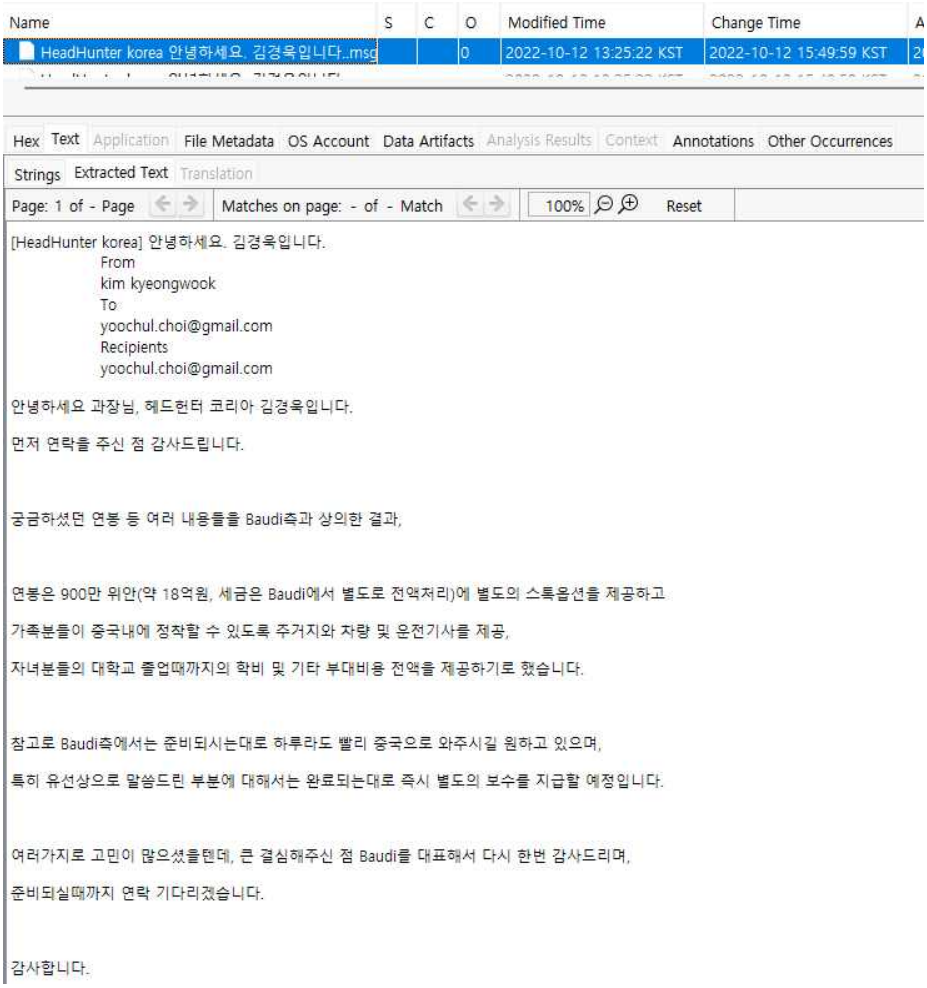


Metadata

Name:	/img_파티션복구_RAW_시나리오1_변속기기술유출.001/vol_vol3/정부사업/HeadHunter Korea 안녕하세요 최유출님. 헤드헌터코리아의 김경욱 과장이라고 합니다..msg
Type:	File System
MIME Type:	application/vnd.ms-outlook
Size:	30720
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2022-10-12 13:25:36 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:	8b05ed8f4d2fdfcbaa37c6e6e1fe6390
SHA-256:	4acab04d4057daeeac3ef8bf2e6d3fcd18b1b6535f41d8be55f6f07738ae130f
Hash Lookup Results:	UNKNOWN
Internal ID:	20579

나. 김경욱->최유출 연봉 등의 내용 이메일 송신

- 김경욱이 최유출에게 연봉 등의 내용을 담은 이메일을 송신하였으며, 유선상으로 말씀드린 부분에 대한 별도의 보수를 지급한다는 내용 등 정보유출에 대한 대가 내용을 담은 것으로 보이는 이메일 파일 확인.



Name	S	C	O	Modified Time	Change Time	A
HeadHunter korea 안녕하세요. 김경욱입니다..msg			0	2022-10-12 13:25:22 KST	2022-10-12 15:49:59 KST	2

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Strings Extracted Text Translation

Page: 1 of - Page Matches on page: - of - Match 100% Reset

[HeadHunter korea] 안녕하세요. 김경욱입니다.
From
kim kyeongwook
To
yoochul.choi@gmail.com
Recipients
yoochul.choi@gmail.com

안녕하세요 과장님, 헤드헌터 코리아 김경욱입니다.

먼저 연락을 주신 점 감사드립니다.

궁금하셨던 연봉 등 여러 내용들을 Baudi측과 상의한 결과,

연봉은 900만 위안(약 18억원, 세금은 Baudi에서 별도로 전액처리)에 별도의 스톡옵션을 제공하고
가족분들이 중국내에 정착할 수 있도록 주거지와 차량 및 운전기사를 제공,
자녀분들의 대학교 졸업때까지의 학비 및 기타 부대비용 전액을 제공하기로 했습니다.

참고로 Baudi측에서는 준비되시는대로 하루라도 빨리 중국으로 와주시길 원하고 있으며,
특히 유선상으로 말씀드린 부분에 대해서는 완료되는대로 즉시 별도의 보수를 지급할 예정입니다.

여러가지로 고민이 많으셨을텐데, 큰 결심해주신 점 Baudi를 대표해서 다시 한번 감사드리며,
준비되실때까지 연락 기다리겠습니다.

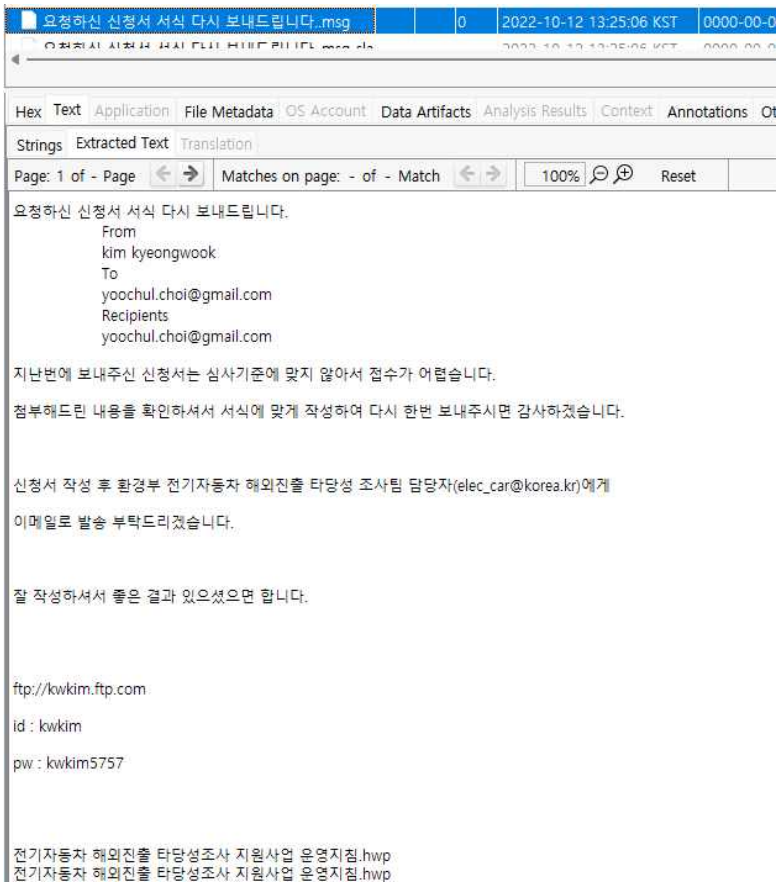
감사합니다.

Metadata

Name:	/img_파티션복구_RAW_시나리오1_변속기기술유출.001/vol_vol2/Users/yc.choi/Downloads/HeadHunter korea 안녕하세요. 김경욱입니다..msg
Type:	File System
MIME Type:	application/vnd.ms-outlook
Size:	30208
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2022-10-12 13:25:22 KST
Accessed:	2022-10-12 17:28:16 KST
Created:	2022-10-12 17:28:16 KST
Changed:	2022-10-12 15:49:59 KST
MD5:	cb83eaaedecc649329a66340e8b38215
SHA-256:	77f7bf93925dbeb8a5a98bbc3868cf9172d65421f6631d2fd07cbd916c225e21
Hash Lookup Results:	UNKNOWN
Internal ID:	19411

다. 최유출의 1차 유출에 따른 김경욱의 답신 확인

- 확장자변조압축파일인 '신청서.pdf' 내 '1.mp4', '2.jpg'파일을 통한 1차 유출 이후 김경욱의 다른 적절한 형식으로의 변환 후 2차 유출요구에 대한 신청서 파일 송부를 확인함. 또한, ftp 서버 정보와 계정명/비밀번호가 있음. 이는 스테가노그래피를 이용해 '출력할가족사진2.jpg'에 숨긴 이미지 파일(포스트잇 촬영 사진)에 담겨 있는 FTP 서버/계정/비밀번호 정보와 일치함을 확인하여 2차 유출은 FTP로 송부함을 추정 가능.



Metadata

Name:	/img_파티션복구_RAW_시나리오1_변속기기술유출.001/vol_vol3/정부사업/요청하신 신청서 서식 다시 보내드립니다..msg
Type:	File System
MIME Type:	application/vnd.ms-outlook
Size:	793088
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2022-10-12 13:25:06 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:	1dfebe9c7e1ad1f7ba0af1645fbd38e5
SHA-256:	8b5ba2f41eabe9add04b5e1b07ef55430f14a56fa8a16c618ae76308a985bee0
Hash Lookup Results:	UNKNOWN
Internal ID:	20586

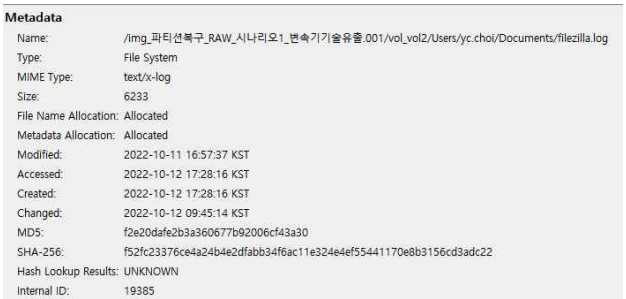
2) FTP 로그

- 위 분석내용에 기초하여 FTP로그인 filezilla 로그파일 filezilla.log파일 탐색 및 분석 진행함. 중요 부분 형광펜 밑줄하였음. kwkim.ftp.com의 주소는 이전에 확인하였던 서버 IP주소임. 또한, 최유출이 2차 유출을 위해 해당 파일 내용 중간에 설계도면을 끼워넣은 파일 '전기자동차 해외진출 타당성조사 지원사업 제출서류 양식.hwp' 업로드하였음을 확인.

```
2022-10-11 16:55:09 1844 1 상태: kwkim.ftp.com 주소 해석
2022-10-11 16:55:09 1844 1 상태: 123.456.78.901:21에 연결...
2022-10-11 16:55:09 1844 1 상태: 연결 수립, 환영 메시지를 기다림...
2022-10-11 16:55:09 1844 1 응답: 220 (vsFTPd 2.2.2)
2022-10-11 16:55:09 1844 1 명령: AUTH TLS
2022-10-11 16:55:09 1844 1 응답: 530 Please login with USER and PASS.
2022-10-11 16:55:09 1844 1 명령: AUTH SSL
2022-10-11 16:55:09 1844 1 응답: 530 Please login with USER and PASS.
2022-10-11 16:55:09 1844 1 상태: 보안되지 않은 서버입니다. TLS를 통한 FTP를 지원하지 않습니다.
2022-10-11 16:55:11 1844 1 명령: USER kwmin
2022-10-11 16:55:11 1844 1 응답: 331 Please specify the password.
2022-10-11 16:55:11 1844 1 명령: PASS **********
2022-10-11 16:55:11 1844 1 응답: 230 Login successful.
2022-10-11 16:55:11 1844 1 명령: SYST
2022-10-11 16:55:11 1844 1 응답: 215 UNIX Type: L8
2022-10-11 16:55:11 1844 1 명령: FEAT
2022-10-11 16:55:11 1844 1 응답: 211-Features:
2022-10-11 16:55:11 1844 1 응답:  EPRT
2022-10-11 16:55:11 1844 1 응답:  EPSV
2022-10-11 16:55:11 1844 1 응답:  MDTM
2022-10-11 16:55:11 1844 1 응답:  PASV
2022-10-11 16:55:11 1844 1 응답:  REST STREAM
2022-10-11 16:55:11 1844 1 응답:  SIZE
2022-10-11 16:55:11 1844 1 응답:  TVFS
2022-10-11 16:55:11 1844 1 응답:  UTF8
2022-10-11 16:55:11 1844 1 응답: 211 End
2022-10-11 16:55:11 1844 1 명령: OPTS UTF8 ON
2022-10-11 16:55:11 1844 1 응답: 200 Always in UTF8 mode.
2022-10-11 16:55:11 1844 1 상태: 로그인
2022-10-11 16:55:11 1844 1 상태: 디렉터리 목록 조회...
2022-10-11 16:55:11 1844 1 명령: PWD
2022-10-11 16:55:11 1844 1 응답: 257 "/"
2022-10-11 16:55:11 1844 1 명령: TYPE I
2022-10-11 16:55:11 1844 1 응답: 200 Switching to Binary mode.
```

```
2022-10-11 16:55:11 1844 1 명령: PASV
2022-10-11 16:55:11 1844 1 응답: 227 Entering Passive Mode (182,162,95,167,209,91).
2022-10-11 16:55:11 1844 1 명령: LIST
2022-10-11 16:55:11 1844 1 응답: 150 Here comes the directory listing.
2022-10-11 16:55:11 1844 1 응답: 226 Directory send OK.
2022-10-11 16:55:11 1844 1 상태: 서버의 시간대 오차 계산...
2022-10-11 16:55:11 1844 1 명령: MDTM 20220831_163840.jpg
2022-10-11 16:55:11 1844 1 응답: 213 20220901170309
2022-10-11 16:55:11 1844 1 상태: Timezone offset of server is 0 seconds.
2022-10-11 16:55:11 1844 1 상태: "/" 디렉터리 목록 조회 성공
2022-10-11 16:55:23 1844 1 상태: "/www" 디렉터리 목록 조회...
2022-10-11 16:55:23 1844 1 명령: CWD www
2022-10-11 16:55:23 1844 1 응답: 250 Directory successfully changed.
2022-10-11 16:55:23 1844 1 명령: PWD
2022-10-11 16:55:23 1844 1 응답: 257 "/www"
2022-10-11 16:55:23 1844 1 명령: PASV
2022-10-11 16:55:23 1844 1 응답: 227 Entering Passive Mode (182,162,95,167,38,163).
2022-10-11 16:55:23 1844 1 명령: LIST
2022-10-11 16:55:23 1844 1 응답: 150 Here comes the directory listing.
2022-10-11 16:55:23 1844 1 응답: 226 Directory send OK.
2022-10-11 16:55:23 1844 1 상태: "/www" 디렉터리 목록 조회 성공
2022-10-11 16:55:24 1844 1 상태: "/" 디렉터리 목록 조회...
2022-10-11 16:55:24 1844 1 명령: CDUP
2022-10-11 16:55:24 1844 1 응답: 250 Directory successfully changed.
2022-10-11 16:55:24 1844 1 명령: PWD
2022-10-11 16:55:24 1844 1 응답: 257 "/"
2022-10-11 16:55:24 1844 1 명령: PASV
2022-10-11 16:55:24 1844 1 응답: 227 Entering Passive Mode (182,162,95,167,170,26).
2022-10-11 16:55:24 1844 1 명령: LIST
2022-10-11 16:55:24 1844 1 응답: 150 Here comes the directory listing.
2022-10-11 16:55:24 1844 1 응답: 226 Directory send OK.
2022-10-11 16:55:24 1844 1 상태: "/" 디렉터리 목록 조회 성공
2022-10-11 16:55:30 1844 2 상태: kwkim.ftp.com 주소 해석
2022-10-11 16:55:30 1844 2 상태: 123.456.78.901:21에 연결...
2022-10-11 16:55:30 1844 2 상태: 연결 수립, 환영 메시지를 기다림...
2022-10-11 16:55:30 1844 2 응답: 220 (vsFTPd 2.2.2)
2022-10-11 16:55:30 1844 2 명령: AUTH TLS
2022-10-11 16:55:30 1844 2 응답: 530 Please login with USER and PASS.
2022-10-11 16:55:30 1844 2 명령: AUTH SSL
2022-10-11 16:55:30 1844 2 응답: 530 Please login with USER and PASS.
```

2022-10-11 16:55:30 1844 2 상태: 보안되지 않은 서버입니다. TLS를 통한 FTP를 지원하지 않습니다.
2022-10-11 16:55:30 1844 2 명령: USER kwmin
2022-10-11 16:55:30 1844 2 응답: 331 Please specify the password.
2022-10-11 16:55:30 1844 2 명령: PASS **********
2022-10-11 16:55:30 1844 2 응답: 230 Login successful.
2022-10-11 16:55:30 1844 2 명령: OPTS UTF8 ON
2022-10-11 16:55:30 1844 2 응답: 200 Always in UTF8 mode.
2022-10-11 16:55:30 1844 2 상태: 로그인
2022-10-11 16:55:30 1844 2 상태: C:\Users\yc.choi\Desktop\전기자동차 해외진출 타당성조사 지원사업 제출서류 양식.hwp 업로드 시작
2022-10-11 16:55:30 1844 2 명령: CWD /
2022-10-11 16:55:30 1844 2 응답: 250 Directory successfully changed.
2022-10-11 16:55:30 1844 2 명령: PWD
2022-10-11 16:55:30 1844 2 응답: 257 "/"
2022-10-11 16:55:30 1844 2 명령: TYPE I
2022-10-11 16:55:30 1844 2 응답: 200 Switching to Binary mode.
2022-10-11 16:55:30 1844 2 명령: PASV
2022-10-11 16:55:30 1844 2 응답: 227 Entering Passive Mode (182,162,95,167,41,214).
2022-10-11 16:55:30 1844 2 명령: STOR 전기자동차 해외진출 타당성조사 지원사업 제출서류 양식.hwp
2022-10-11 16:55:30 1844 2 응답: 150 Ok to send data.
2022-10-11 16:55:30 1844 2 응답: 226 Transfer complete.
2022-10-11 16:55:30 1844 2 상태: 파일 전송 성공, 804,864 바이트를 1 초에 전송
2022-10-11 16:55:30 1844 2 상태: "/" 디렉터리 목록 조회...
2022-10-11 16:55:30 1844 2 명령: PASV
2022-10-11 16:55:30 1844 2 응답: 227 Entering Passive Mode (182,162,95,167,117,11).
2022-10-11 16:55:30 1844 2 명령: LIST
2022-10-11 16:55:30 1844 2 응답: 150 Here comes the directory listing.
2022-10-11 16:55:30 1844 2 응답: 226 Directory send OK.
2022-10-11 16:55:30 1844 2 상태: "/" 디렉터리 목록 조회 성공
2022-10-11 16:55:33 1844 1 상태: 서버와의 연결이 종료됨



Metadata

Name:	/img_파티션복구_RAW_시나리오1_변속기기술유출.001/vol_vol2/Users/yc.choi/Documents/filezilla.log
Type:	File System
MIME Type:	text/x-log
Size:	6233
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2022-10-11 16:57:37 KST
Accessed:	2022-10-12 17:28:16 KST
Created:	2022-10-12 17:28:16 KST
Changed:	2022-10-12 09:45:14 KST
MD5:	f2e20dafe2b3a360677b92006cf43a30
SHA-256:	f52fc23376ce4a24b4e2dfabb34f6ac11e324e4ef55441170e8b3156cd3adc22
Hash Lookup Results:	UNKNOWN
Internal ID:	19385

3) 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. 또한, Baudi社로 추정되는 B로부터 5억원의 입금내용이 기술 유출 이후 기록되어있음을 확인할 수 있었음.

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

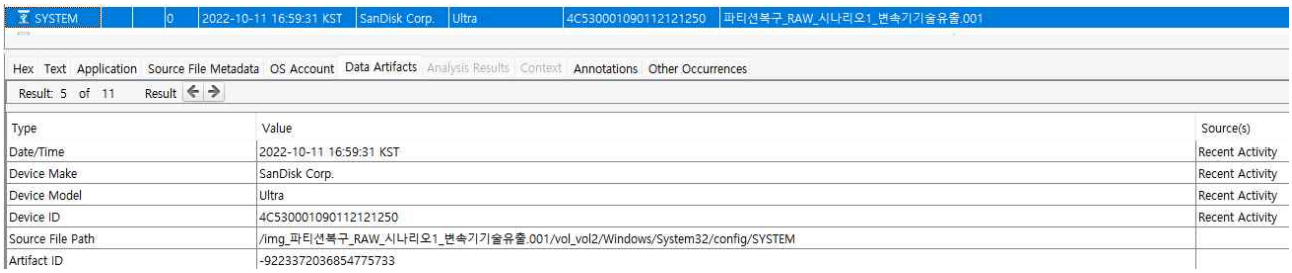
성명	최유출	조회기간	2022.10.05 - 2022.10.20
계좌번호	****-**-***12334	요청일시	2022.10.21 13:40:26

※ 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	

4. usb 연결기록

- AWG社 자체 감사 결과 자료 유출에 사용된 USB의 시리얼 넘버인 '4C530012200403114081'와 하나의 파티션에 운영체제가 설치된 증거 USB의 해당 운영체제에 연결됐던 USB 시리얼 넘버 '4C530012200403114081'이 동일한 것으로 미루어보아, 해당 증거 USB는 AWS社가 확인한 유출에 사용된 USB임을 알 수 있으며, 이는 해당 사건과 최유출의 관계가 더욱 밀접함을 확인시켜준다.



SYSTEM | 0 | 2022-10-11 16:59:31 KST | SanDisk Corp. | Ultra | 4C530001090112121250 | 파티션복구_RAW_시나리오1_변속기기술유출.001

Hex | Text | Application | Source File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Result: 5 of 11 Result

Type	Value	Source(s)
Date/Time	2022-10-11 16:59:31 KST	Recent Activity
Device Make	SanDisk Corp.	Recent Activity
Device Model	Ultra	Recent Activity
Device ID	4C530001090112121250	Recent Activity
Source File Path	/img_파티션복구_RAW_시나리오1_변속기기술유출.001/vol_vol2/Windows/System32/config/SYSTEM	
Artifact ID	-9223372036854775733	