Hoseo Forensic Center

분석보고서

접 수 일 자	2021-05-20
지 원 번 호	3주차
관 리 번 호	2021-1
분 석 일 자	2021-05-20 ~ 2021-05-22
분 석 장 소	서울특별시 강서구 서울호서전문학교 6층 호서 포렌식센터
분 석 대 상	AAA의 회사 컴퓨터
요 청 기 관	Laugo Arms
요 청 사 항	유출된 내부정보와 공범과 접촉한 흔적, 범행동기 와 과정
분석결과요약	❍ **범행 컴퓨터 확인** - AAA가 신제품 도면을 discord(메신저)로 업로드로 1차 유출 후 삭제한 것을 확인. 회사 탐지에 걸리지 않는 USB를 통하여 도면과 회사 직원신상을 업로드 후 확장자를 변경하여 겉 옷에 지닌 후 2차 유출하려던 것을 확인. ❍ **공범과 접촉한 흔적** - discord(메신저)를 통해 신제품 도면 유출정황과 직원신상정보로 거래협상 기록 확인. ❍ **범행동기와 그 과정** - AAA은 친분이 있는 타 회사직원(공범)과의 메신저 도중 해고사실를 인지. 그 후 공범이 돈을 보상으로 Laugo Arms의 신제품 도면과 회사직원신상을 요구. 그 후 USB로 업로드하여 확장자만 변경한 후 다른 이미지파일에 은닉 후 유출하려고 함. (상세 분석 결과 아래자료 첨부)

Hoseo Forensic Center

상 세 분 석 내 역

1. 사건 개요

AAA가 신제품 도면을 타 회사 직원에게 유출하려는 정황이 포착되어 AAA의 회사PC에서 신제품 도면 자료 확인과 타 회사 직원과 접촉한 흔적, 범행동기와 그 과정 등을 조사해달라는 의뢰

2. 분석 요청사항

가. 신제품 도면자료 확인
나. 공범과 접촉한 흔적
다. 범행 동기와 범행 과정 등

3. 분석대상 정보

관리 번호	사용자	종류	제조사	모델	용량 (GB)	시리얼 번호
21-1	AAA	HDD	Seagate	ST 1000DM003	1000	Z4Y0TNHX

4. 분석 시스템과 도구

가. 분석시스템 운영체제 : Windows 10
나. 복구·분석에 사용한 프로그램 : Encase v21.1, HxD

5. 증거사본작성 및 분석방법

가. 증거사본 작성

나. OS 정보 및 Time zone setting 확인

대 상	OS	OS 설치 일시	Time zone	비고
AAA HDD	Windows 10	2021-05-18	(UTC+09:00) 서울	-

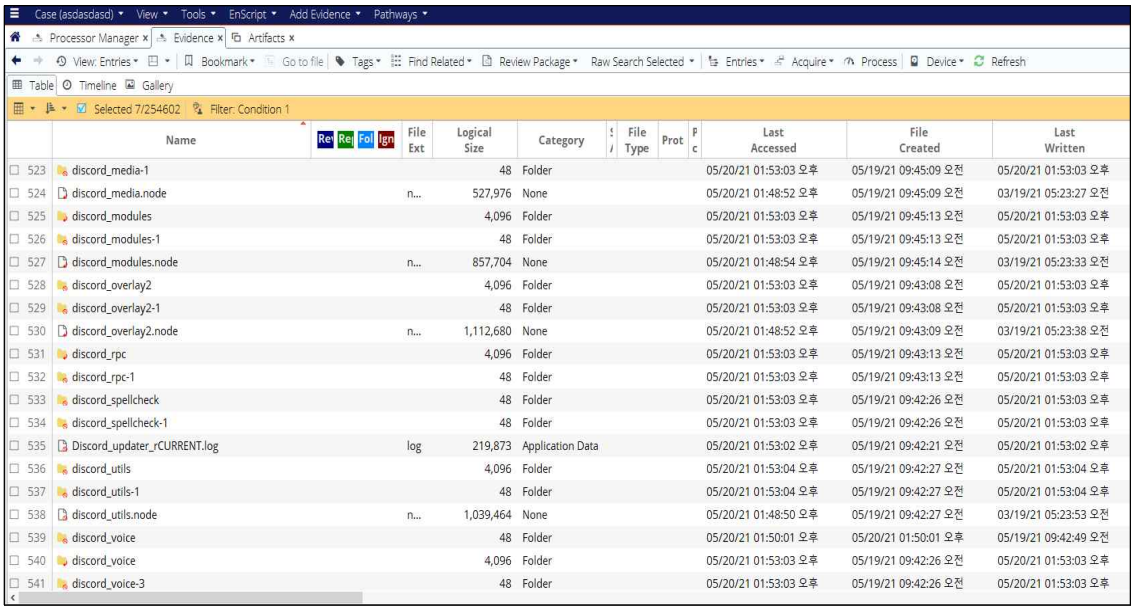
다. 수행한 분석방법

분석 대상	내 용
HDD	피의자 PC의 원본 하드디스크 확보 후 장치를 이용해 사본복제를 한 후 이를 저장해 분석용 툴을 이용하여 분석 작업을 수행
USB	HDD와 같이 사본복제 후 이를 저장해 분석용 툴을 이용하여 분석 작업을 수행

6. 상세 분석 결과

가. 증거이미지

그림 - 1 피의자가 PC에서 사용한 하드디스크



	Name	File Ext	Logical Size	Category	File Type	Prot	Last Accessed	File Created	Last Written
523	discord_media-1		48	Folder			05/20/21 01:53:03 오후	05/19/21 09:45:09 오전	05/20/21 01:53:03 오후
524	discord_media.node	n...	527,976	None			05/20/21 01:48:52 오후	05/19/21 09:45:09 오전	03/19/21 05:23:27 오전
525	discord_modules		4,096	Folder			05/20/21 01:53:03 오후	05/19/21 09:45:13 오전	05/20/21 01:53:03 오후
526	discord_modules-1		48	Folder			05/20/21 01:53:03 오후	05/19/21 09:45:13 오전	05/20/21 01:53:03 오후
527	discord_modules.node	n...	857,704	None			05/20/21 01:48:54 오후	05/19/21 09:45:14 오전	03/19/21 05:23:33 오전
528	discord_overlay2		4,096	Folder			05/20/21 01:53:03 오후	05/19/21 09:43:08 오전	05/20/21 01:53:03 오후
529	discord_overlay2-1		48	Folder			05/20/21 01:53:03 오후	05/19/21 09:43:08 오전	05/20/21 01:53:03 오후
530	discord_overlay2.node	n...	1,112,680	None			05/20/21 01:48:52 오후	05/19/21 09:43:09 오전	03/19/21 05:23:38 오전
531	discord_rpc		4,096	Folder			05/20/21 01:53:03 오후	05/19/21 09:43:13 오전	05/20/21 01:53:03 오후
532	discord_rpc-1		48	Folder			05/20/21 01:53:03 오후	05/19/21 09:43:13 오전	05/20/21 01:53:03 오후
533	discord_spellcheck		48	Folder			05/20/21 01:53:03 오후	05/19/21 09:42:26 오전	05/20/21 01:53:03 오후
534	discord_spellcheck-1		48	Folder			05/20/21 01:53:03 오후	05/19/21 09:42:26 오전	05/20/21 01:53:03 오후
535	Discord_updater_rCURRENT.log	log	219,873	Application Data			05/20/21 01:53:02 오후	05/19/21 09:42:21 오전	05/20/21 01:53:02 오후
536	discord_utils		4,096	Folder			05/20/21 01:53:04 오후	05/19/21 09:42:27 오전	05/20/21 01:53:04 오후
537	discord_utils-1		48	Folder			05/20/21 01:53:04 오후	05/19/21 09:42:27 오전	05/20/21 01:53:04 오후
538	discord_utils.node	n...	1,039,464	None			05/20/21 01:48:50 오후	05/19/21 09:42:27 오전	03/19/21 05:23:53 오전
539	discord_voice		48	Folder			05/20/21 01:50:01 오후	05/20/21 01:50:01 오후	05/19/21 09:42:49 오전
540	discord_voice		4,096	Folder			05/20/21 01:53:03 오후	05/19/21 09:42:26 오전	05/20/21 01:53:03 오후
541	discord_voice-3		48	Folder			05/20/21 01:53:03 오후	05/19/21 09:42:26 오전	05/20/21 01:53:03 오후

그림 - 2 피의자가 사용한 메신저

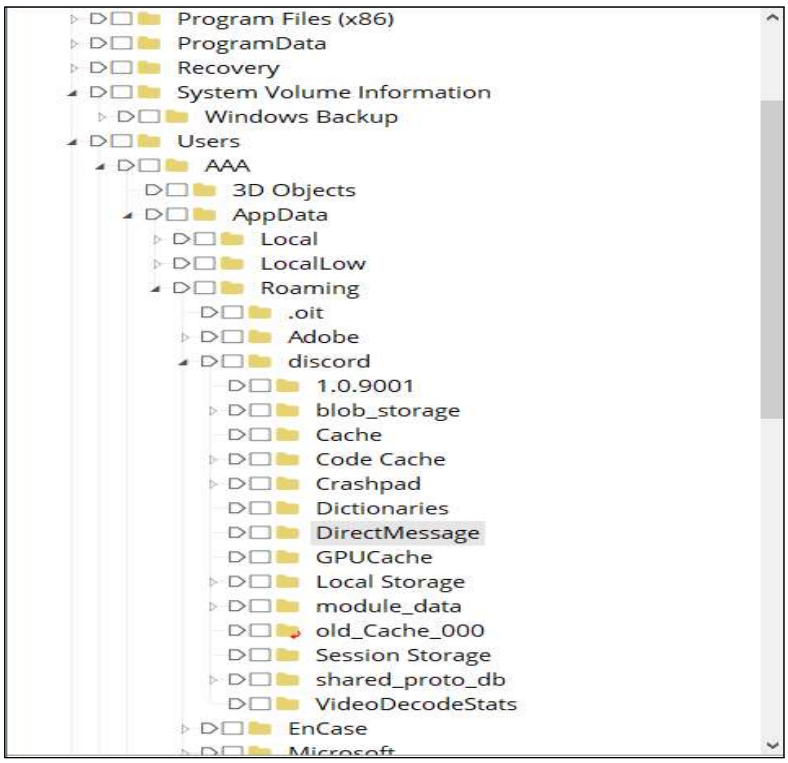


그림 - 3 Users₩AAA₩Roaming₩discord₩DirectMessage₩Message.txt
피의자의 채팅목록 경로

그림 - 4 공범 공조사실 확보(파일첨부)

사용 메신저	이메일	채팅 시작시간	마지막 채팅시간
discord	tedaw72488@trikos.com	2021-05-19 10:08	2021-05-20 13:50
	gatolix822@to200.com	2021-05-19 14:51	2021-05-20 13:50

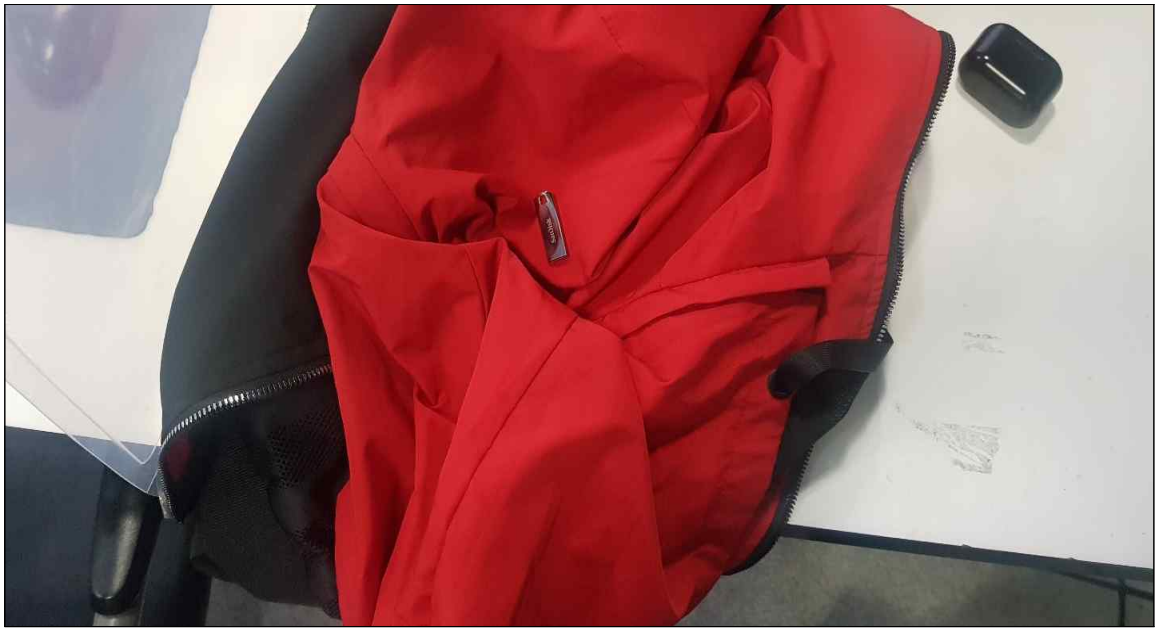


그림 - 5 피의자의 겉 옷에서 발견한 USB

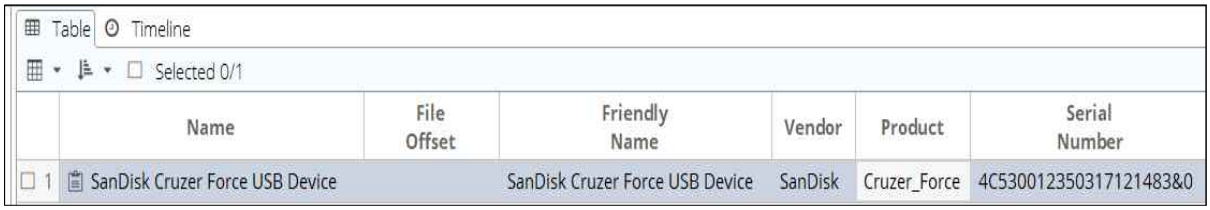


그림 - 6 피의자가 사용한 USB 정보 및 파일목록

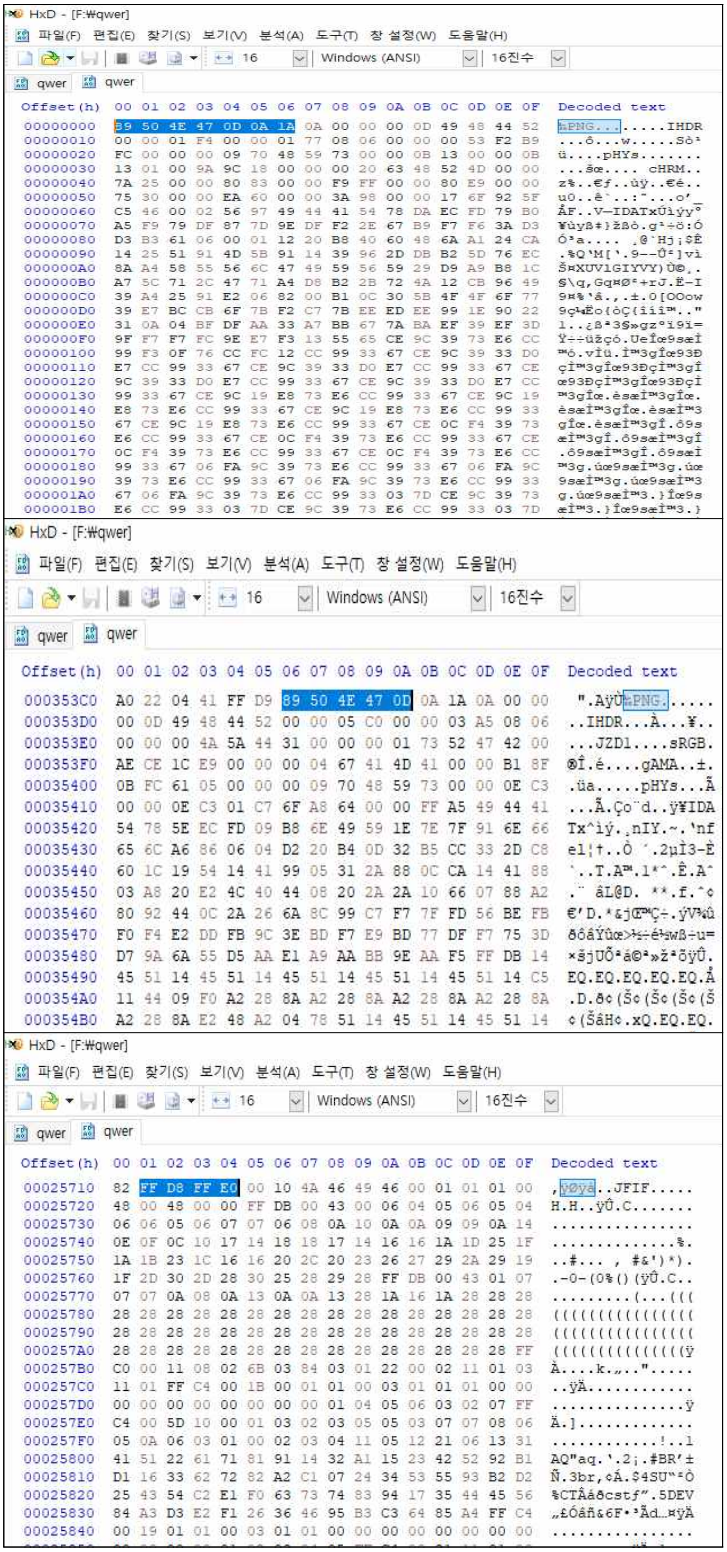


그림 - 7 qwer 파일 확장자(png, png(1), jpeg)

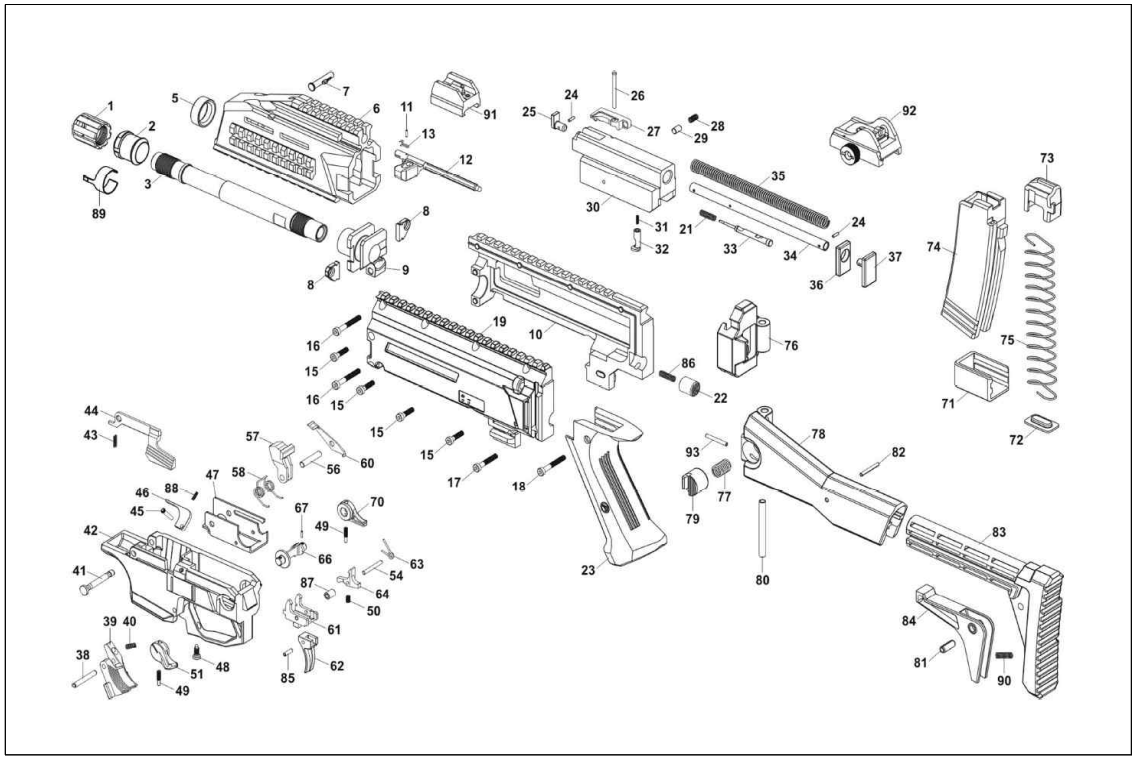


그림 - 8 피의자의 USB에서 발견된 확장자가 은닉되어있던 신제품 제작도면

그림 - 9 피의자의 USB에서 발견된 확장자가 은닉되어있던 신제품 완성도면

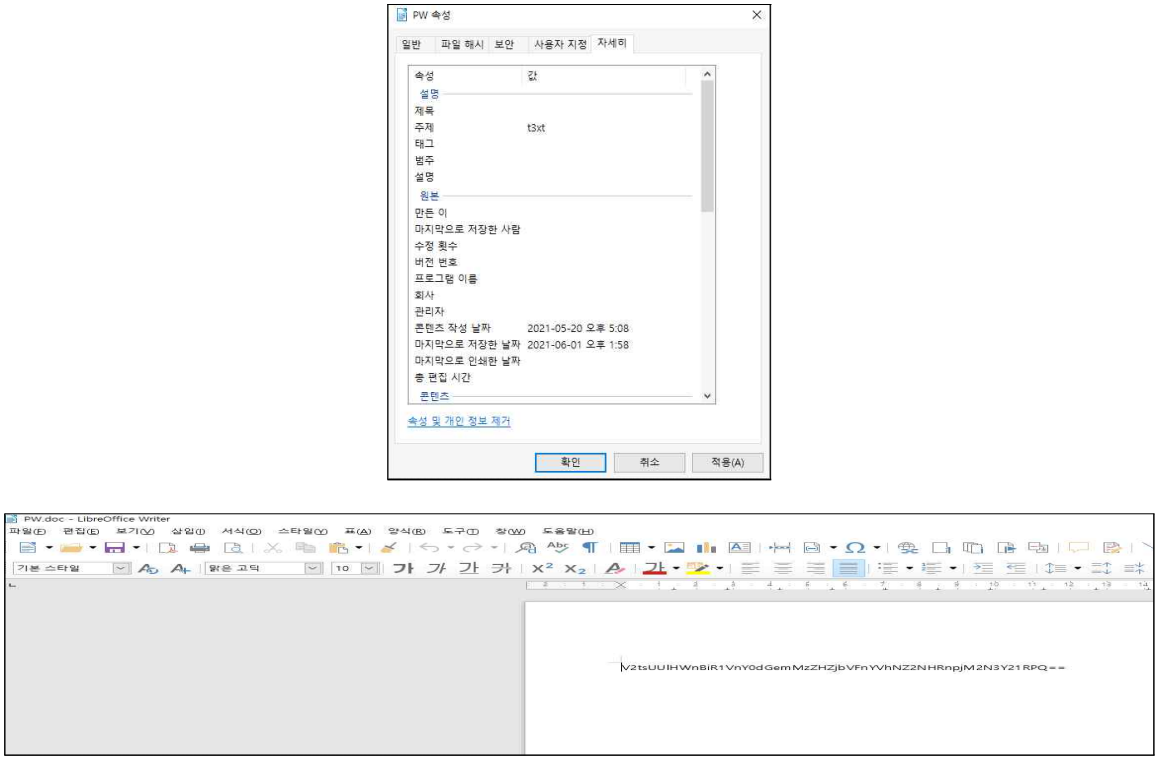


그림 - 10 PW.doc 파일속성 및 파일내용

파일 명	디코딩 횟수	디코딩 전	디코딩 후
PW.doc	디코딩 1번	V2tsUUlHWnBiR1VnY0dGemMzZHZjbVFnYVhNZ2NHRnpjM2N3Y21RPQ==	WklQIGZpbGUgcGFzc3dvcmQgaXMgcGFzc3cwcmQ=
	디코딩 2번	WklQIGZpbGUgcGFzc3dvcmQgaXMgcGFzc3cwcmQ=	ZIP file password is passw0rd

그림 - 11 피의자의 USB에서 발견된 Laugo Arms의 직원신상정보

나. 증거 파일 해시값 목록

파일 명 (디스크)	해시 값		비 고
Disk(HDD)	분석 전	565007172876957b8bab66c76b02b4e3b21ebf5b	원본 디스크
	분석 후	565007172876957b8bab66c76b02b4e3b21ebf5b	
qwer	분석 전	B4158E8FCDCD2B6A67D8D92D64E76C08B362E8F0	-
	분석 후	B4158E8FCDCD2B6A67D8D92D64E76C08B362E8F0	
신제품 완제품 도안	분석 전	B4158E8FCDCD2B6A67D8D92D64E76C08B362E8F0	추출 후
	분석 후	CD682D5B6B113DC8E250575778479E8EF37DBFFD	
신제품 분해 도안	분석 전	B4158E8FCDCD2B6A67D8D92D64E76C08B362E8F0	추출 후
	분석 후	0B668A8B80EE020ECF63A3E949887EE9472E5B37	
BarBora Trnkova.txt	분석 전	9195040F5F6C21E4FD57636BCE702587F176FC14	직원 신상정보(1)
	분석 후	9195040F5F6C21E4FD57636BCE702587F176FC14	
Sheng Pai.txt	분석 전	B216A1682A8C90C378418DF190E17EEABFF49FE5	직원 신상정보(2)
	분석 후	B216A1682A8C90C378418DF190E17EEABFF49FE5	
Thomas S. Crow.txt	분석 전	0F29E7E5CFAE703D5454283B43A69D3F227F0533	직원 신상정보(3)
	분석 후	0F29E7E5CFAE703D5454283B43A69D3F227F0533	
Todd J. Gerhardt.txt	분석 전	182699AEB10ABA2159904BF27EF0EA2D08F695F9	직원 신상정보(4)
	분석 후	182699AEB10ABA2159904BF27EF0EA2D08F695F9	
DirectMessage.txt	분석 전	DCE979609155A7F3521725C226A92A48D6F1E45D	메신저 대화내용
	분석 후	DCE979609155A7F3521725C226A92A48D6F1E45D	
pw.doc	분석 전	4E93CDC934D2D0A62C2F8EFB720ECF716AE0AC28	usb
	분석 후	4E93CDC934D2D0A62C2F8EFB720ECF716AE0AC28	