

2021 디지털포렌식개론

Encase를 활용한 컴퓨터 포렌식

신수민

국민대학교 금융정보보안학과, DF&C 연구실

tnals523@kookmin.ac.kr

CONTENTS

1. 윈도우 아티팩트 소개
2. 시나리오 소개
3. Encase를 활용한 시나리오 분석
4. 결론

1. 윈도우 아티팩트 소개

■ 아티팩트

- 사전적인 의미는 유물
- 디지털 포렌식에서는 운영체제 및 애플리케이션을 동작시켰을 때 남게 되는 흔적
 - 인터넷 사용 기록
 - 레지스트리
 - 프리패치
 - 바로가기 파일
 - 이벤트 로그
 - 파일시스템 로그
 - 휴지통 등



1. 윈도우 아티팩트 소개

■ 인터넷 사용 기록

- 컴퓨터에 설치되어 있는 Browser의 정보를 수집하여 사용자의 인터넷 사용 기록을 분석
- 범행의 계획, 수단, 방법과 처리 등의 기록을 획득할 가능성 존재
- 사용자의 최근 관심사 등을 획득
- 따라서, 프로파일링 하는데 도움이 됨

파일명	내용
Cache	웹 사이트 접속 시 재방문을 용이하게 하기 위한 파일로써 자동으로 다운로드된 파일이 저장 (이미지파일, 텍스트파일, HTML 파일, xml 파일, 스크립트 등 웹페이지를 구성하기 위한 데이터가 다양하게 저장)
History	사용자가 방문한 사이트의 기록을 수집하여 저장
Download	사용자가 웹 브라우저를 통해 직접 다운로드 한 파일의 리스트 수집하여 저장

1. 윈도우 아티팩트 소개

■ 레지스트리

- 마이크로소프트 윈도우 운영체제에서 운영체제와 응용프로그램 운영에 필요한 정보를 저장하기 위해 고안한 계층형 데이터베이스
- 사용자, 시스템, 저장매체와 관련된 다양한 데이터 저장
 - 운영체제 정보
 - 사용자 계정 정보
 - 시스템 정보
 - 응용프로그램 실행 흔적
 - 최근 접근 문서
 - 저장매체 사용 흔적(하드디스크, CD-ROM, USB 등) 등

1. 윈도우 아티팩트 소개

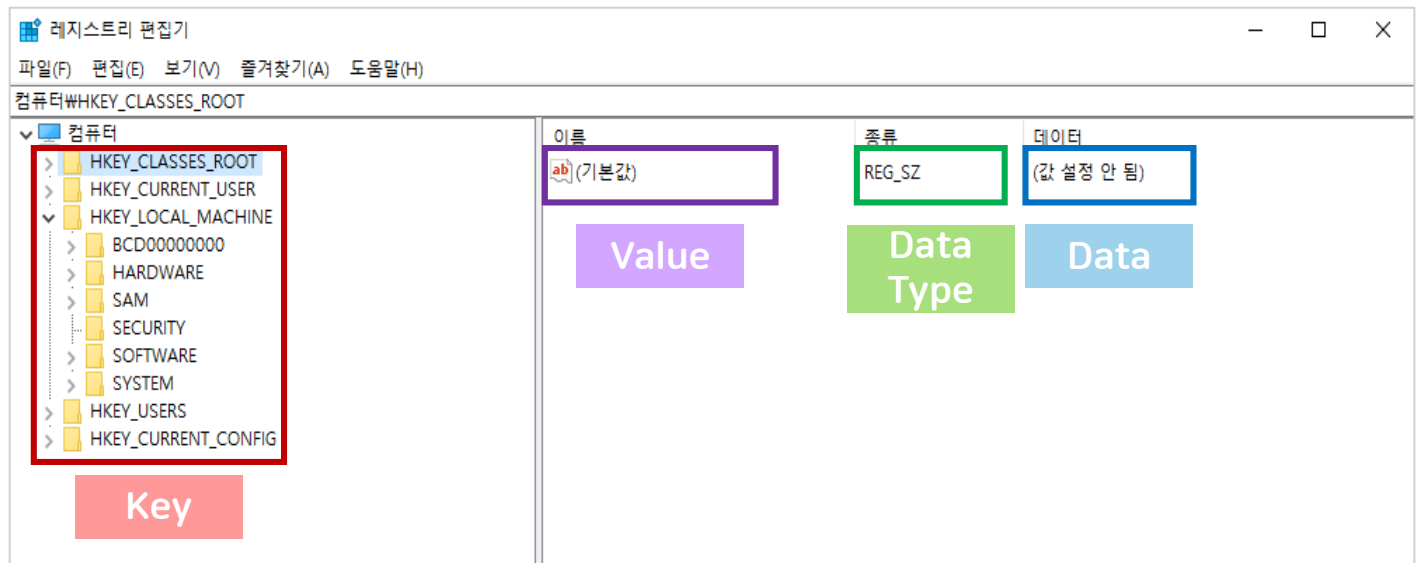
■ 레지스트리

- 활성화 시스템에서 레지스트리 분석은 레지스트리 편집기(RegEdit.exe) 이용



레지스트리 편집기

앱



1. 윈도우 아티팩트 소개

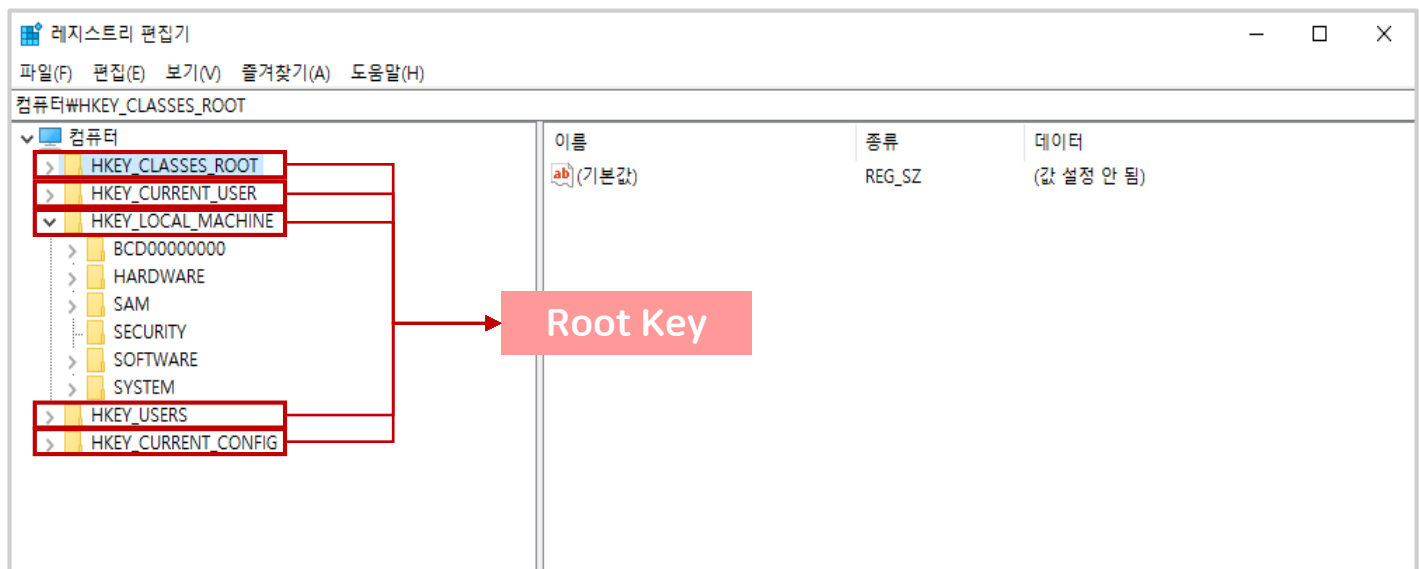
■ 레지스트리

- 활성화 시스템에서 레지스트리 분석은 레지스트리 편집기(RegEdit.exe) 이용



레지스트리 편집기

앱



1. 윈도우 아티팩트 소개

■ 레지스트리

- 활성화 시스템에서 레지스트리 분석은 레지스트리 편집기(RegEdit.exe) 이용
 - Root Key

Root Key	내용
HKEY_CLASSES_ROOT	윈도우에서 사용하는 각종 파일정보 저장
HKEY_CURRENT_USER	현재 시스템에 로그인하고 있는 사용자와 관련된 시스템 정보 저장
HKEY_LOCAL_MACHINE	시스템에 설치된 소프트웨어와 하드웨어에 대한 정보, 운영체제에 관련된 설정, 서비스 및 보안 관련 설정 등의 정보를 저장
HKEY_USERS	시스템에 있는 모든 계정과 그룹에 관한 정보 저장
HKEY_CURRENT_CONFIG	시스템이 시작할 때 사용하는 하드웨어 프로필 정보 저장 HKLM\SYSTEM\CurrentControlSet\Hardware Profiles\Current의 내용

1. 윈도우 아티팩트 소개

■ 레지스트리

- 비활성화 시스템에서 레지스트리 분석은 하이브 파일을 수집하여 분석
 - 하이브 파일: 레지스트리 정보를 저장하고 있는 물리적 파일
SAM, SECURITY, SOFTWARE, DEFAULT, SYSTEM 등
 - 경로: C:\Windows\System32\config

하이브 파일	해당 레지스트리 키
SAM	HKEY_LOCAL_MACHINE/SAM
SECURITY	HKEY_LOCAL_MACHINE/SECURITY
SOFTWARE	HKEY_LOCAL_MACHINE/SOFTWARE
DEFAULT	HKEY_USER/.DEFAULT
SYSTEM	HKEY_LOCAL_MACHINE/SYSTEM HKEY_CURRENT_CONFIG

1. 윈도우 아티팩트 소개

▪ 프리패치

- 실행 파일이 사용하는 시스템 자원을 특정 파일에 미리 저장
- 사용자가 파일을 실행할 경우 미리 저장된 정보를 메모리에서 실행하여 실행 속도를 향상
- 프리패치 파일은 최대 128개 생성
- 최대치에 도달하면 오래된 파일부터 삭제
- 응용프로그램의 다양한 정보를 저장
 - 응용프로그램 이름
 - 응용프로그램 실행 횟수
 - 응용프로그램 마지막 실행 시각 (Windows 64-bit Time stamp, FILETIME)
 - 참조 목록 (파일 수행에 필요한 DLL, SDB, NLS, INI 등의 전체경로)
 - 파일시스템 시간 정보(생성, 수정, 마지막 접근 시간 등)를 이용한 통합 타임라인 분석

1. 윈도우 아티팩트 소개

▪ 바로가기 파일

- LNK (Windows Shortcut) 파일
- 윈도우에만 존재하는 기능
- 응용프로그램, 디렉터리, 파일, 문서 뿐만 아니라 관리 콘솔 등의 특정 객체를 참조하는 파일
- 바탕화면, 최근 문서 폴더, 시작 프로그램, 빠른 실행에 수동 혹은 자동으로 생성되어 저장
- 바로가기 파일을 통해 알 수 있는 정보
 - 원본 파일 위치
 - 시스템 이름
 - 볼륨 정보
 - 파일의 MAC Time

1. 윈도우 아티팩트 소개

■ 이벤트 로그

- 윈도우 운용과정에서 발생하는 특정 이벤트들을 종합적이고 체계적으로 로그 기록
 - 시스템의 성능, 오류, 경고 및 운용정보 등의 중요정보 기록
- 주요 이벤트 로그

파일명	내용
Application.evtx	소프트웨어를 비롯해서 사용자의 애플리케이션의 이벤트를 기록
Security.evtx	보안 관련된 이벤트 로그, Windows 로그인, 네트워크 등 다양한 로그 기록
System.evtx	서비스 실행 여부나 파일 시스템, 디바이스 오류 등의 정보 기록
Setup.evtx	애플리케이션 설치 시 발생하는 이벤트를 기록하고 프로그램이 잘 설치되었는지, 호환성 관련 정보 기록

1. 윈도우 아티팩트 소개

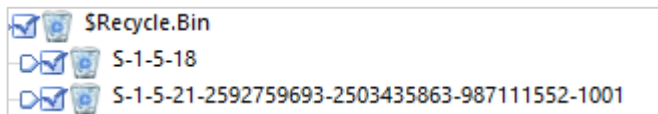
▪ 파일시스템 로그

- 파일 시스템: 컴퓨터가 보조저장장치를 사용함에 있어, 파일이나 자료를 쉽게 찾거나 접근하여 활용할 수 있도록 내용을 조직하는 체계
- 특정 기간 동안 발생한 파일시스템 이벤트를 분석 가능
- NTFS의 로그 파일
 - \$LogFile: 트랜잭션 로그
(시스템 오류나 갑작스런 전원 차단 발생 시, 작업중인 파일 복구를 위해 사용)
 - \$UsnJrnl: 변경 로그
(응용 프로그램이 특정 파일의 변경 여부를 파악하기 위해 사용)

1. 윈도우 아티팩트 소개

▪ 휴지통

- 파일을 삭제했을 때 임시로 저장되는 폴더
- 볼륨마다 휴지통 폴더 존재
 - 각 볼륨마다 독립된 휴지통 공간
 - 특정 볼륨에서 지운 파일은 해당 볼륨의 휴지통으로 이동
- 사용자 SID (Security ID) 별로 휴지통 폴더 존재
 - 각 사용자마다 독립된 휴지통 공간
 - 특정 사용자가 지운 파일은 해당 사용자 SID 휴지통으로 이동



[사용자 SID별 휴지통]

1. 윈도우 아티팩트 소개

■ 아티팩트

- 분석 시 사용 도구

아티팩트	분석 내용	사용 도구
인터넷 사용 기록 흔적	검색 기록, 방문 사이트, 다운로드 목록 등	WEFA, DB Browser
레지스트리	자동 실행 프로그램, 시스템 정보 등	REGA
프리패치	프로그램의 실행 여부 및 실행 시점	WinPrefetchView, APFA
바로가기 파일	파일 또는 프로그램의 실행 및 열람 여부	LNK Parser
이벤트로그	서비스 시작, 저장장치 해제, 응용프로그램 자체 이벤트 등	Event Log Explorer, EventLog Analyzer
파일시스템 로그	파일 및 폴더의 생성, 삭제, 복사 흔적	NTFS Log Tracker

2. 시나리오 소개

- 모의 시나리오 소개
- 기밀 자료 유출
 - **최 모씨(용의자)**는 국내 노트북 제조 회사(D사)에 재직
 - 용의자는 회사 **신제품 개발 프로젝트**에 참여
 - 프로젝트를 위한 별도 PC 지급
 - PC는 업무시간에만 사용 가능(10:00 ~ 18:00)
 - D사의 신제품이 완성될 무렵 **최 모씨**는 **갑작스럽게 퇴사**
 - 1주일 뒤, **경쟁사(C사)**에서 **동일한 사양의 신제품 출시**
 - 기술 개발 팀장의 의심으로 용의자 **최 모씨**에 대한 수사 의뢰



2. 시나리오 소개

- 증거로 압수된 압수 물품 목록
 - 프로젝트용 PC
 - 용의자 개인 소유 USB 1개
- 압수 물품 상세 정보

대상	모델명	시리얼 정보	장치용량	하드웨어 정보
증거물1	VMWare Virtual Disk	-	30GB	VMWare Virtual Disk
증거물2	SanDisk USB Device	4C530001250824104225	32GB	USB

3. Encase를 활용한 시나리오 분석

■ 레지스트리

• 경로

- C:\Windows\System32\Config\Software
- C:\Windows\System32\Config\System
- C:\Windows\System32\Config\SAM
- C:\Windows\System32\Config\Security

• 운영체제 정보

속성	값
운영체제	Windows 10 Pro
설치 시각	2021년 4월 28일 11:00
타임존	KST(UTC+09:00)
관리자 계정	Yong

3. Encase를 활용한 시나리오 분석

■ 인터넷 사용기록 흔적

- 경로: C\Users\<user name>\AppData\Local\Google\Chrome\User Data\Default

	Is Deleted	Name	Item Path	File Ext	
1		Accounts	Windows 10 x64\Users\ yong\AppData\Local\Google\Chrome\User Data\Default\Accounts		20
2		AutofillStrikeDatabase	Windows 10 x64\Users\ yong\AppData\Local\Google\Chrome\User Data\Default\Autofill...		20
3		blob_storage	Windows 10 x64\Users\ yong\AppData\Local\Google\Chrome\User Data\Default\blob_st...		20
4		BudgetDatabase	Windows 10 x64\Users\ yong\AppData\Local\Google\Chrome\User Data\Default\Bookma...		20
5		Bookmarks	Windows 10 x64\Users\ yong\AppData\Local\Google\Chrome\User Data\Default\Bookma...		20
6		BudgetDatabase	Windows 10 x64\Users\ yong\AppData\Local\Google\Chrome\User Data\Default\Budget...		20
7		Cache	Windows 10 x64\Users\ yong\AppData\Local\Google\Chrome\User Data\Default\Cache		20
8		Code Cache	Windows 10 x64\Users\ yong\AppData\Local\Google\Chrome\User Data\Default\Code C...		20
9		Cookies	Windows 10 x64\Users\ yong\AppData\Local\Google\Chrome\User Data\Default\Cookies		20
10		Cookies-journal	Windows 10 x64\Users\ yong\AppData\Local\Google\Chrome\User Data\Default\Cookies...		20
11		data_reduction_proxy_leveldb	Windows 10 x64\Users\ yong\AppData\Local\Google\Chrome\User Data\Default\data_re...		20
12		databases	Windows 10 x64\Users\ yong\AppData\Local\Google\Chrome\User Data\Default\databas...		20
13		DownloadMetadata	Windows 10 x64\Users\ yong\AppData\Local\Google\Chrome\User Data\Default\Downlo...		20
14		Extension State	Windows 10 x64\Users\ yong\AppData\Local\Google\Chrome\User Data\Default\Extensi...		20
15		Extensions	Windows 10 x64\Users\ yong\AppData\Local\Google\Chrome\User Data\Default\Extensi...		20
16		Favicons	Windows 10 x64\Users\ yong\AppData\Local\Google\Chrome\User Data\Default\Favicons		20
17		Favicons-journal	Windows 10 x64\Users\ yong\AppData\Local\Google\Chrome\User Data\Default\Favicon...		20
18		Feature Engagement Tracker	Windows 10 x64\Users\ yong\AppData\Local\Google\Chrome\User Data\Default\Feature...		20
19		File System	Windows 10 x64\Users\ yong\AppData\Local\Google\Chrome\User Data\Default\File Syst...		20
20		GCM Store	Windows 10 x64\Users\ yong\AppData\Local\Google\Chrome\User Data\Default\GCM St...		20
21		Google Profile Picture.png	Windows 10 x64\Users\ yong\AppData\Local\Google\Chrome\User Data\Default\Google ...	png	20
22		Google Profile.ico	Windows 10 x64\Users\ yong\AppData\Local\Google\Chrome\User Data\Default\Google ...	ico	20
23		GPUCache	Windows 10 x64\Users\ yong\AppData\Local\Google\Chrome\User Data\Default\GPUCac...		20

⇒ Cookies, History, Cache 등 인터넷 관련 파일 존재

3. Encase를 활용한 시나리오 분석

■ 인터넷 사용기록 흔적

- History 파일

- 사용자가 접속한 인터넷 사이트의 목록을 저장
- 다운로드한 내역도 알 수 있음



다운로드 목록

검색한 키워드

접속한 사이트 주소

[DB Browser for SQLite를 통해 확인한 History]

3. Encase를 활용한 시나리오 분석

■ 인터넷 사용기록 흔적

- History 파일 분석 결과
 - CCleaner를 다운받은 흔적을 알 수 있음

테이블(T): downloads

	guid	current_path	target_path	start_time
필터	필터	필터	필터	필터
1	25bb5104-11d6-4a0d-b635-0f21a355c791	C:\Users\W...	C:\Users\Wyeong\Downloads\Everything-1.4.1.1005.x64-Setup.exe	13264607578552011
2	b4d9cca8-be58-400e-a167-2265c5b39a75	C:\Users\W...	C:\Users\Wyeong\Downloads\cctrialsetup.exe	13264770223566204

DCode v4.02a (Build: 9306)

Convert Data to Date / Time Values

Add Bias: UTC +09:00 ☐ Window on top

Decode Format: Google Chrome Value

Example: 12883423549317375

Value to Decode: 13264770223566204

Date & Time: Thu, 06 May 2021 19:23:43 +0900

www.digital-detective.co.uk

업무시간 아님

⇒컴퓨터 최적화 프로그램인 "CCleaner"를 업무시간 외에 다운 받음

3. Encase를 활용한 시나리오 분석

■ 인터넷 사용기록 흔적

- History 파일 분석 결과

- "기밀유출 처벌", "이직", "검색기록 삭제" 등과 관련된 키워드 들을 검색한 사실을 알 수 있음

테이블(T): keyword_search_terms

	keyword_id	url_id	term	normalized_term
	필터	필터	필터	필터
1	2	1	gmail	gmail
2	2	18	usb 삭제 프로그램	usb 삭제 프로그램
3	2	27	everything 프로그램	everything 프로그램
4	2	41	기밀유출 처벌	기밀유출 처벌
5	2	46	ccleaner	ccleaner
6	2	49	인터넷 흔적 지우기	인터넷 흔적 지우기
7	2	51	검색기록삭제	검색기록삭제
8	2	55	프로그램 삭제	프로그램 삭제
9	2	57	이직	이직
10	2	58	기밀유출 이직	기밀유출 이직

3. Encase를 활용한 시나리오 분석

■ 인터넷 사용기록 흔적

• History 파일 분석 결과

- 업무시간 외 시간에 이메일, 기밀유출 및 흔적 삭제 관련하여 많은 사이트 방문

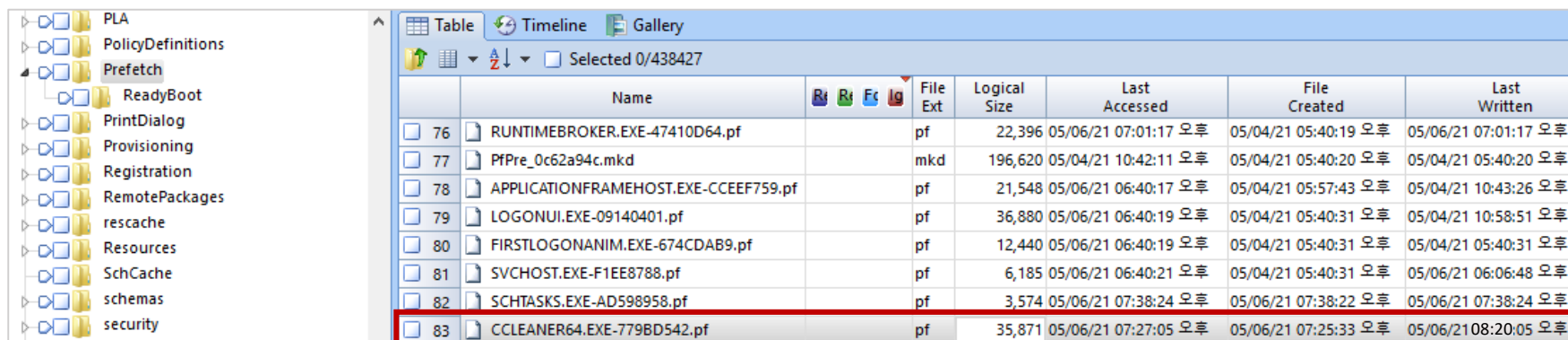
테이블(T):  urls    

	id	url	title	visit_count	typed_count	last_visit_time
	필터	필터	필터	필터	필터	필터
18	18	https://www....	usb 삭제 프로그램 - Google 검색	2	0	13264603615495429
19	20	https://www....	USB 드라이브에서 파일을 영구적으로 삭제 / 지우는 방법-EaseUS	1	0	13264603733848752
20	25	https://mail....	받은편지함 - choiyonghun808@gmail.com - Gmail	1	0	13264603788581427
21	19	https://ittalk....	usb 기록 삭제 프로그램 usbdeview 다운로드 및 사용법 - IT Talk	1	0	13264605929583612
⋮						
37	42	https://www....	'ADD 68만건 기밀 유출'... "'집유' 남발' 솜방망이 처벌이 원인" - 아주경제	1	0	13264765002450112
38	43	http://m.blog...	영업비밀침해, 회사기밀유출 법적 대응을 알아보자! : 네이버 블로그	1	0	13264765063909974
39	44	https://m.blo...	영업비밀침해, 회사기밀유출 법적 대응을 알아보자! : 네이버 블로그	1	0	13264765063909974
40	45	https://m.blo...	영업비밀침해, 회사기밀유출 법적 대응을 알아보자! : 네이버 블로그	3	0	13264765069479222
41	30	https://mail....	설정 - choiyonghun808@gmail.com - Gmail	2	0	13264765087067234
42	41	https://www....	기밀유출 처벌 - Google 검색	2	0	13264770174634350
43	46	https://www....	ccleaner - Google 검색	2	0	13264770191450811
44	47	https://www....	Download CCleaner Clean, optimize & tune up your PC, free!	1	0	13264770203667107
45	48	https://www....	Thanks for downloading CCleaner	1	0	13264770217960319
46	49	https://www....	인터넷 흔적 지우기 - Google 검색	2	0	13264770460029420
47	50	https://www....	Google	2	0	13264770470692573
48	51	https://www....	검색기록삭제 - Google 검색	2	0	13264770494443496

3. Encase를 활용한 시나리오 분석

■ 프리패치

- 경로: C:\Windows\Prefetch
- 업무시간이 아닌 시간에 CCleaner를 설치 및 실행한 기록이 남아있음



The screenshot shows the Windows Prefetch folder structure on the left and a table of prefetch files on the right. The table has columns for Name, File Ext, Logical Size, Last Accessed, File Created, and Last Written. The file CCLEANER64.EXE-779BD542.pf is highlighted with a red box.

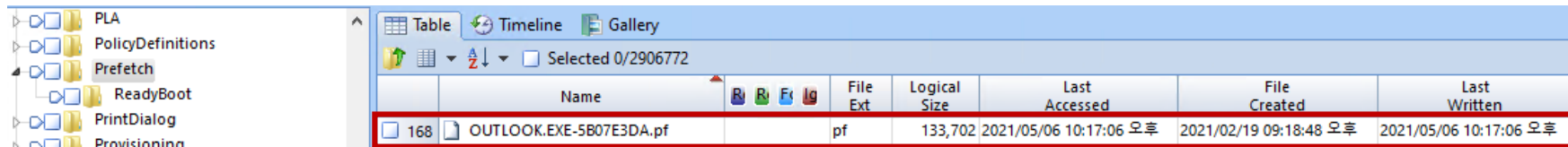
	Name	File Ext	Logical Size	Last Accessed	File Created	Last Written
76	RUNTIMEBROKER.EXE-47410D64.pf	pf	22,396	05/06/21 07:01:17 오후	05/04/21 05:40:19 오후	05/06/21 07:01:17 오후
77	PfPre_0c62a94c.mkd	mkd	196,620	05/04/21 10:42:11 오후	05/04/21 05:40:20 오후	05/04/21 05:40:20 오후
78	APPLICATIONFRAMEHOST.EXE-CCEEF759.pf	pf	21,548	05/06/21 06:40:17 오후	05/04/21 05:57:43 오후	05/04/21 10:43:26 오후
79	LOGONUI.EXE-09140401.pf	pf	36,880	05/06/21 06:40:19 오후	05/04/21 05:40:31 오후	05/04/21 10:58:51 오후
80	FIRSTLOGONANIM.EXE-674CDAB9.pf	pf	12,440	05/06/21 06:40:19 오후	05/04/21 05:40:31 오후	05/04/21 05:40:31 오후
81	SVCHOST.EXE-F1EE8788.pf	pf	6,185	05/06/21 06:40:21 오후	05/04/21 05:40:31 오후	05/06/21 06:06:48 오후
82	SCHTASKS.EXE-AD598958.pf	pf	3,574	05/06/21 07:38:24 오후	05/06/21 07:38:22 오후	05/06/21 07:38:24 오후
83	CCLEANER64.EXE-779BD542.pf	pf	35,871	05/06/21 07:27:05 오후	05/06/21 07:25:33 오후	05/06/21 08:20:05 오후

- 파일 생성 시간: 2021년 5월 6일 19시 25분 33초
- 마지막 접근시간: 2021년 5월 6일 20시 20분 5초

3. Encase를 활용한 시나리오 분석

■ 프리패치

- 업무시간이 아닌 시간에 OUTLOOK을 실행한 기록이 남아있음



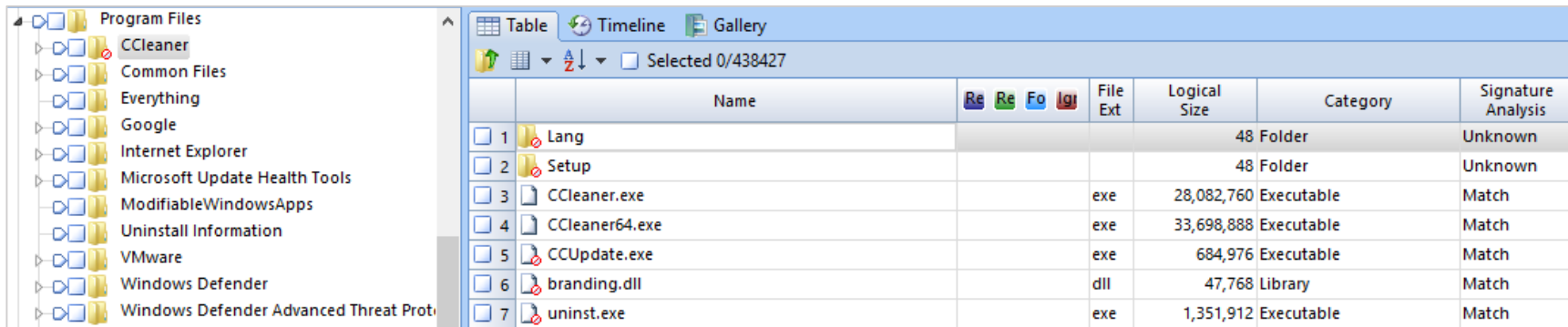
	Name	File Ext	Logical Size	Last Accessed	File Created	Last Written
168	OUTLOOK.EXE-5B07E3DA.pf	pf	133,702	2021/05/06 10:17:06 오후	2021/02/19 09:18:48 오후	2021/05/06 10:17:06 오후

- 마지막 접근시간: 2021년 5월 6일 20시 17분 6초

3. Encase를 활용한 시나리오 분석

■ 프로그램 삭제

- CCleaner를 설치 및 실행한 후 삭제한 사실을 알 수 있음



	Name	Re	Re	Fo	Log	File Ext	Logical Size	Category	Signature Analysis
<input type="checkbox"/> 1	Lang						48	Folder	Unknown
<input type="checkbox"/> 2	Setup						48	Folder	Unknown
<input type="checkbox"/> 3	CCleaner.exe					exe	28,082,760	Executable	Match
<input type="checkbox"/> 4	CCleaner64.exe					exe	33,698,888	Executable	Match
<input type="checkbox"/> 5	CCUpdate.exe					exe	684,976	Executable	Match
<input type="checkbox"/> 6	branding.dll					dll	47,768	Library	Match
<input type="checkbox"/> 7	uninst.exe					exe	1,351,912	Executable	Match

🚫 : 삭제된 파일

3. Encase를 활용한 시나리오 분석

■ 파일시스템 로그

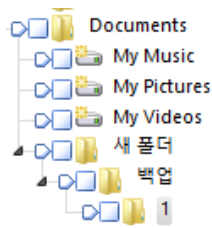
- 업무시간이 아닌 시간에 CCleaner를 설치, 실행 및 삭제한 기록이 남아있음

TimeStamp	FileName	Event
Filter	Filter	Filter
2021-05-06 19:25:20	CCleaner64.exe	File_Created
2021-05-06 19:25:20	CCleaner64.exe	File_Created / Data_Added
2021-05-06 19:25:21	CCleaner64.exe	File_Created / Attr_Changed / Data_Added
2021-05-06 19:25:21	CCleaner64.exe	File_Created / Attr_Changed / Data_Added / File_Closed
2021-05-06 19:25:22	CCleaner64.exe	Object_ID_Changed
2021-05-06 19:25:22	CCleaner64.exe	Object_ID_Changed / File_Closed
2021-05-06 20:38:24	CCleaner64.exe	File_Closed / File_Deleted
2021-05-06 19:25:22	CCleaner.Ink	File_Created
2021-05-06 19:25:22	CCleaner.Ink	File_Created / Data_Added
2021-05-06 19:25:22	CCleaner.Ink	File_Created / Data_Added / File_Closed
2021-05-06 19:25:22	CCleaner.Ink	File_Created
2021-05-06 19:25:22	CCleaner.Ink	File_Created / Data_Added
2021-05-06 19:25:22	CCleaner.Ink	File_Created / Data_Added / File_Closed
2021-05-06 20:38:24	CCleaner.Ink	File_Closed / File_Deleted
2021-05-06 20:38:24	CCleaner.Ink	File_Closed / File_Deleted
2021-05-06 19:25:20	CCleaner.exe	File_Created
2021-05-06 19:25:20	CCleaner.exe	File_Created / Data_Added
2021-05-06 19:25:20	CCleaner.exe	File_Created / Attr_Changed / Data_Added
2021-05-06 19:25:20	CCleaner.exe	File_Created / Attr_Changed / Data_Added / File_Closed
2021-05-06 20:38:24	CCleaner.exe	File_Closed / File_Deleted

3. Encase를 활용한 시나리오 분석

■ 확장자 변경

- 문서파일에 하위 폴더를 많이 생성하여 기밀자료 백업해둔 사실을 알 수 있음
 - 알고리즘.png
 - 자료.png
 - 비밀자료.hwp
 - 설계도.hwp



	Name	Re	Re	FC	Log	File Ext	Logical Size	Category	Signature Analysis	File Type
<input type="checkbox"/> 1	알고리즘.png					png	20,353	Picture	Match	Portable Network Graphic
<input type="checkbox"/> 2	자료.png					png	56,486	Picture	Match	Portable Network Graphic
<input type="checkbox"/> 3	비밀자료.hwp					hwp	280,576	Document	Alias	Compound Document File
<input type="checkbox"/> 4	설계도.hwp					hwp	93,683	Picture	Alias	JPEG Image Standard

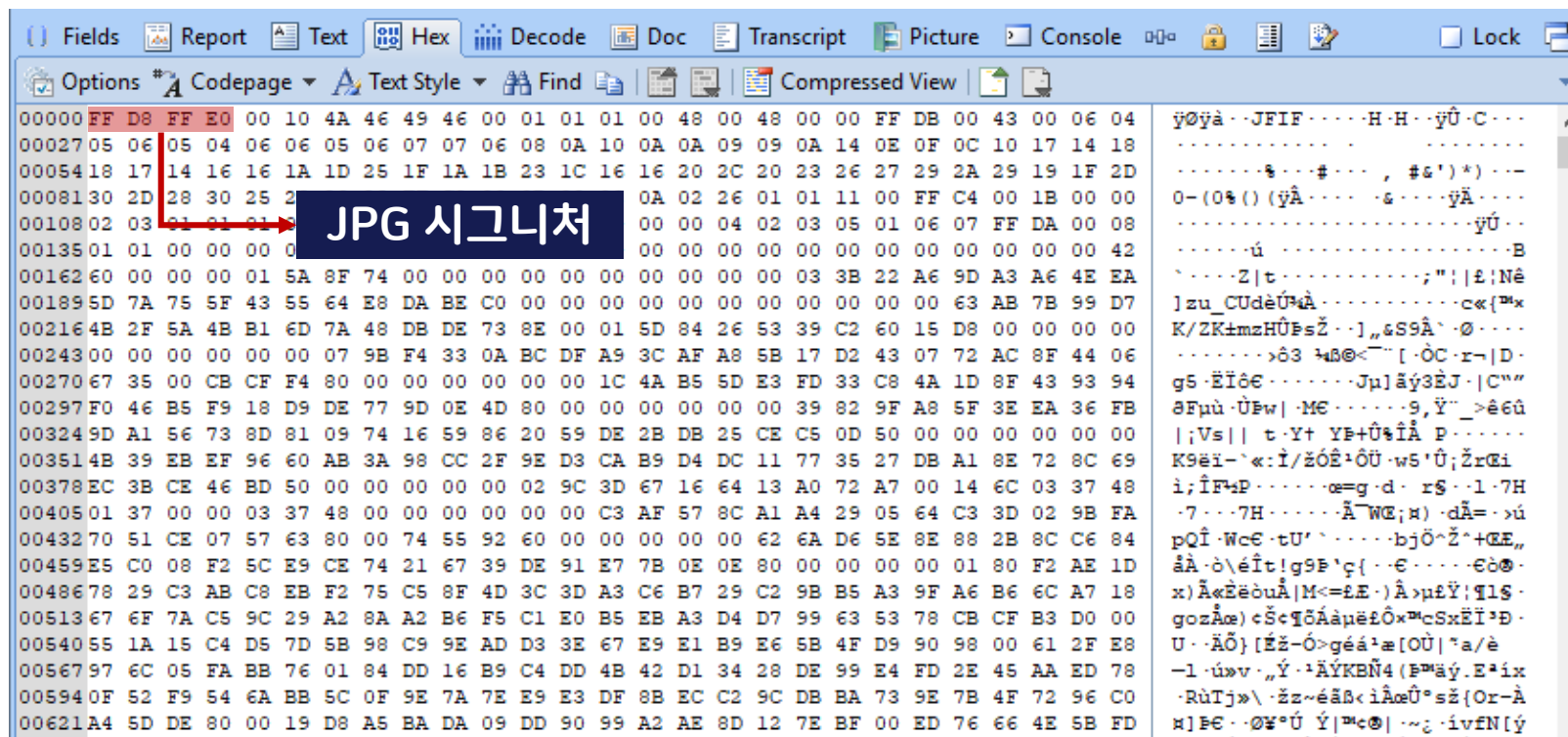
Last Accessed	File Created	Last Written	Is Picture
05/06/21 07:35:58 오후	05/04/21 06:42:20 오후	05/04/21 06:42:18 오후	•
05/06/21 07:35:31 오후	05/04/21 08:12:54 오후	05/04/21 08:14:29 오후	•
05/06/21 06:24:26 오후	05/04/21 08:15:52 오후	05/04/21 08:15:52 오후	
05/04/21 09:43:35 오후	05/04/21 06:12:40 오후	05/04/21 06:08:54 오후	•

3. Encase를 활용한 시나리오 분석

■ 확장자 변경

- 설계도.hwp

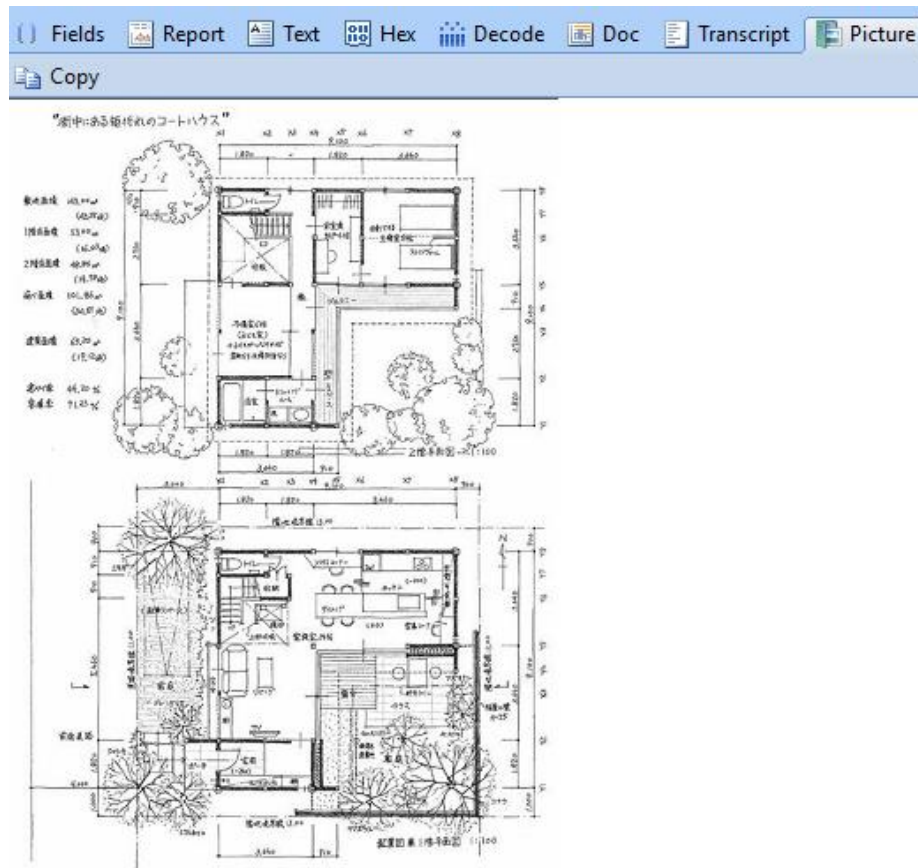
- 확장자는 hwp지만 실제로는 사진파일인 것을 알 수 있음



3. Encase를 활용한 시나리오 분석

■ 확장자 변경

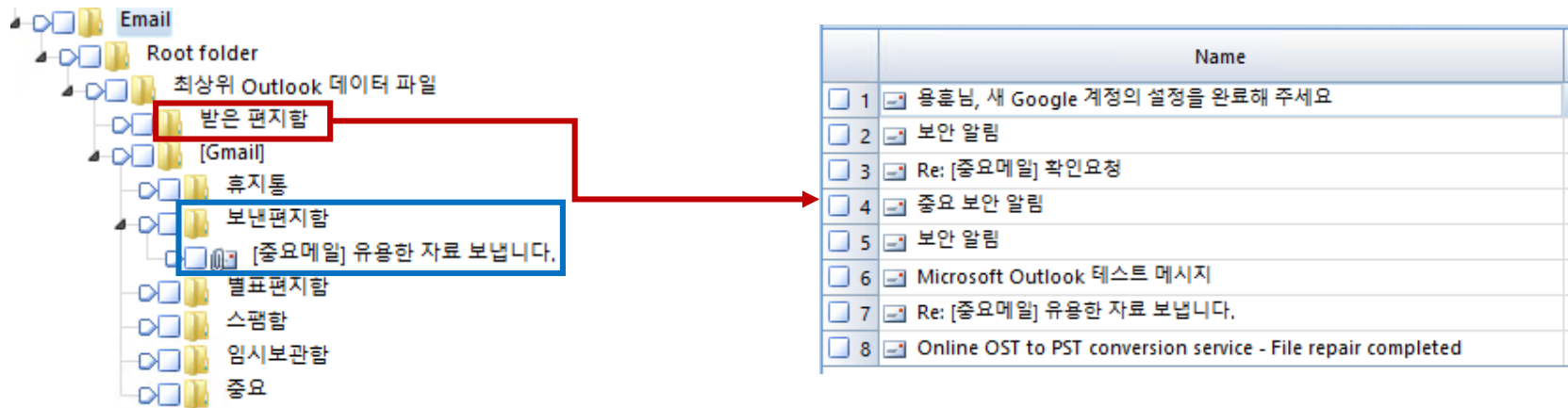
- 설계도.hwp
 - Picture 탭에서 사진파일을 확인할 수 있음



3. Encase를 활용한 시나리오 분석

■ 이메일


- 경로: C\Users\<user name>\Documents\Outlook 파일\backup.pst
- Gmail에서 수/발신한 이메일 내역 확인 가능



3. Encase를 활용한 시나리오 분석

■ 이메일

- 이메일을 이용한 기밀 유출 여부 분석 결과

시간 (UTC+09:00)	내용	아티팩트
2021/05/04 22:15:59	기밀 유출 상대 확인	PST 파일
2021/05/04 22:35:53	기밀 유출 상대 확인 완료	PST 파일
2021/05/06 18:26:29	 기밀유출 상대에게 내부자료를 포함한 메일 발신	PST 파일
2021/05/06 18:32:50	기밀유출 상대에게 확인 메일 수신	PST 파일

3. Encase를 활용한 시나리오 분석

■ 이메일

- 이메일을 이용한 기밀 유출 여부 분석 결과

안녕하세요

좋은 자료 찾아서 파일 첨부하여 공유합니다.

확인 후 연락주세요.

Windows 10용 메일 [<https://go.microsoft.com/fwlink/?LinkId=550986>] 에서 보냄

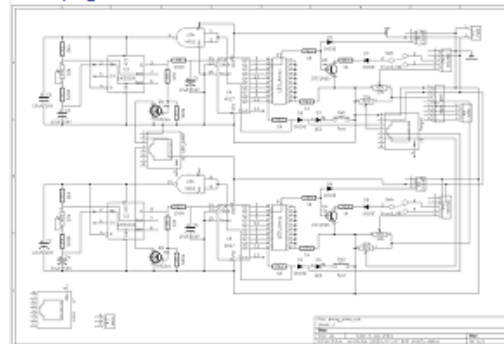
Attachments

Name	비밀자료.hwp
Logical Size	280,576

[비밀자료.hwp](#)

Name	자료.png
Logical Size	56,486

[자료.png](#)

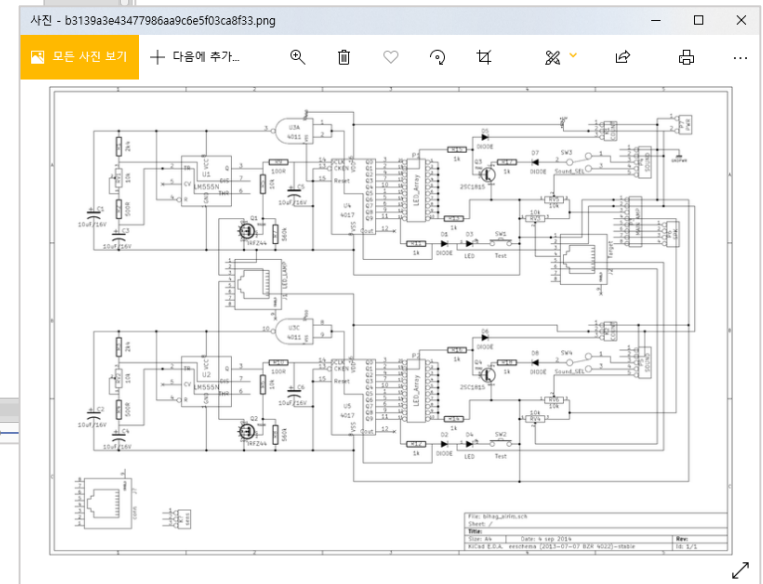
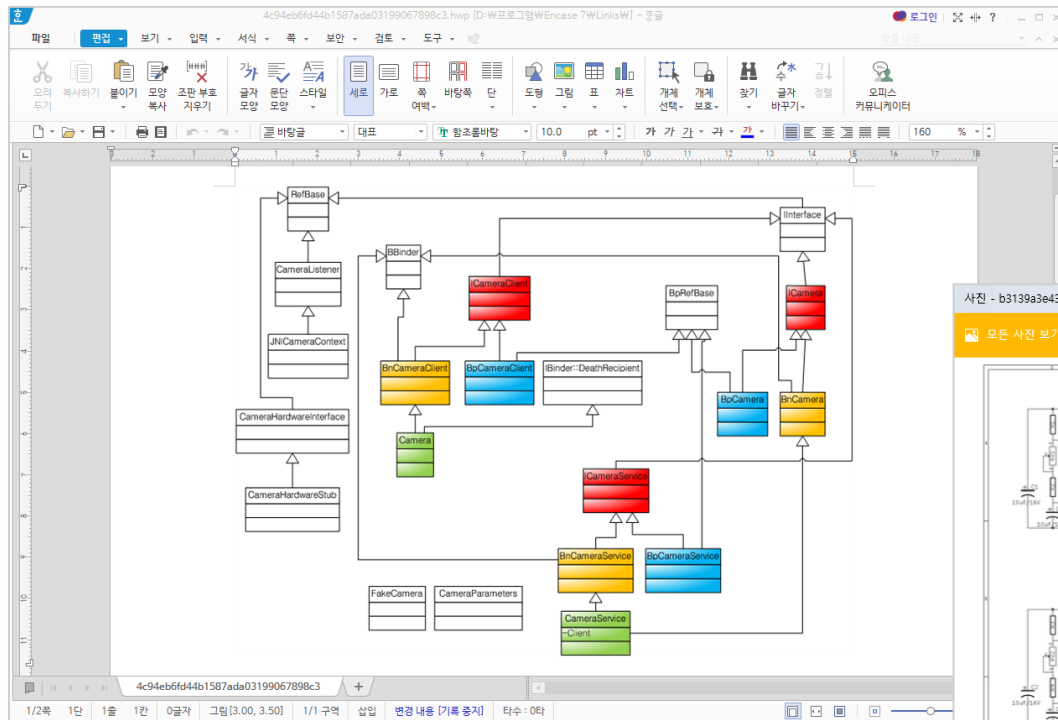


첨부파일을 통해 기밀 유출

3. Encase를 활용한 시나리오 분석

■ 이메일

- 이메일을 이용한 기밀 유출 여부 분석 결과
 - 첨부파일 획득



3. Encase를 활용한 시나리오 분석

■ USB 분석

- USB 연결 흔적

USB Records

Table Timeline

Selected 0/1

	Name	Friendly Name	Vendor	Product	Serial Number	Last Connected Date
1	SanDisk Ultra USB Device	SanDisk Ultra USB Device	SanDisk	Ultra	4C530001250824104225&0	05/06/21 08:06:41 오후

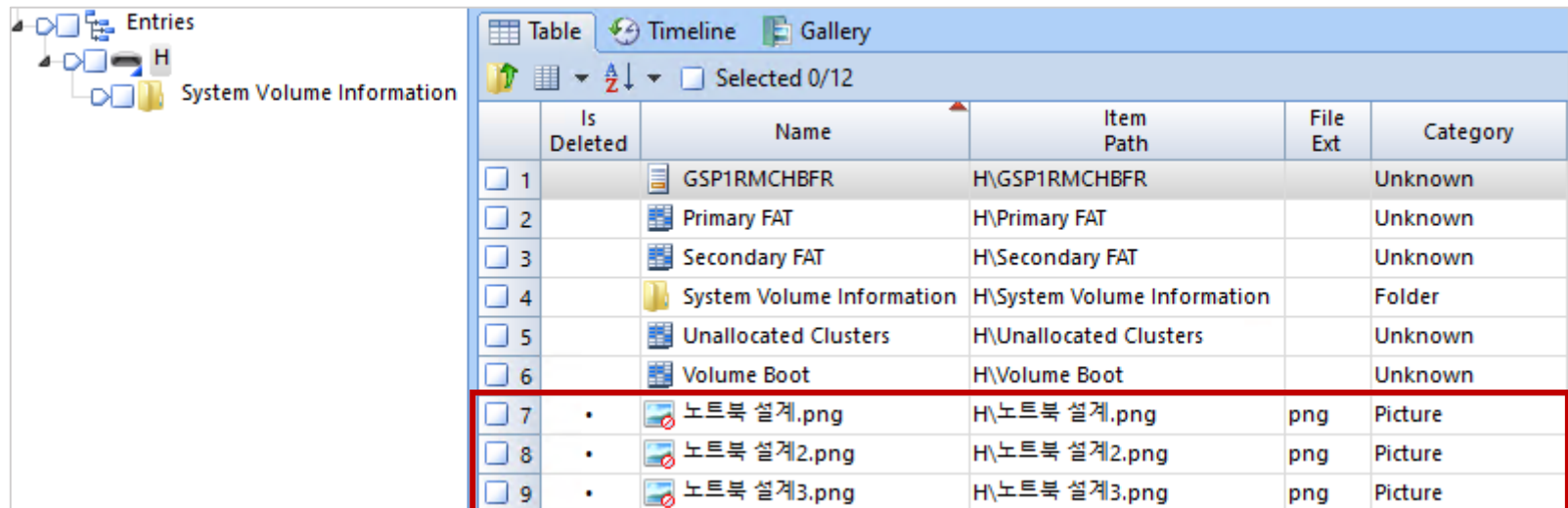
- USB 이름: SanDisk Ultra USB Device
- 시리얼 넘버: 4C530001250824104225
- 마지막 연결 시각: 2021년 5월 6일 20시 6분 41초

⇒ 증거로 획득한 USB의 시리얼 넘버와 동일

3. Encase를 활용한 시나리오 분석

■ USB 분석

- 삭제된 파일 3개 존재

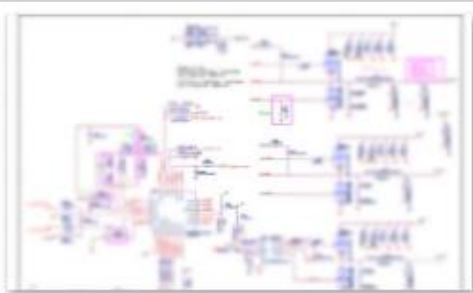


	Is Deleted	Name	Item Path	File Ext	Category
<input type="checkbox"/> 1		GSP1RMCHBFR	H\GSP1RMCHBFR		Unknown
<input type="checkbox"/> 2		Primary FAT	H\Primary FAT		Unknown
<input type="checkbox"/> 3		Secondary FAT	H\Secondary FAT		Unknown
<input type="checkbox"/> 4		System Volume Information	H\System Volume Information		Folder
<input type="checkbox"/> 5		Unallocated Clusters	H\Unallocated Clusters		Unknown
<input type="checkbox"/> 6		Volume Boot	H\Volume Boot		Unknown
<input type="checkbox"/> 7	•	노트북 설계.png	H\노트북 설계.png	png	Picture
<input type="checkbox"/> 8	•	노트북 설계2.png	H\노트북 설계2.png	png	Picture
<input type="checkbox"/> 9	•	노트북 설계3.png	H\노트북 설계3.png	png	Picture

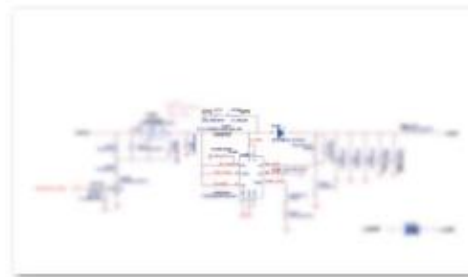
3. Encase를 활용한 시나리오 분석

▪ USB 분석

- 삭제된 파일 3개 복구 결과
 - 노트북 설계.png
 - 노트북 설계2.png
 - 노트북 설계3.png



노트북 설계.png



노트북 설계2.png



노트북 설계3.png

4. 결론

- 다운로드 및 삭제
 - 컴퓨터 최적화 프로그램인 "CCleaner"를 설치, 실행 후 삭제
- 검색 기록
 - 기밀유출, 기밀유출 처벌 및 흔적 삭제 등과 관련하여 검색
- 확장자 변경
 - jpg 파일을 hwp로 은닉
- 이메일
 - 용의자 최 모씨가 기밀 유출 대상자에게 내부자료를 포함한 메일을 전송

모두 "업무시간 외"에 발생한 일



4. 결론

■ 타임라인



2021년 4월 28일

- 11:00 - 윈도우 설치

2021년 5월 4일

- 19:00 ~ 22:00 - 새 이메일 계정 생성, USB 삭제 프로그램 검색
- 22:15 - 이메일을 통해 기밀 유출 상대 확인
- 22:35 - 이메일을 통해 기밀 유출 상대 확인 완료



2021년 5월 6일

- 18:26 - 기밀유출 상대방에게 내부자료를 포함한 메일 발신
- 18:32 - 기밀유출 상대방에게 확인 메일 수신
- 19:00 ~ 20:00 - 기밀유출 처벌, 기밀유출 이직, CCleaner, 인터넷 흔적 지우기, 프로그램 삭제 검색
- 19:23 - CCleaner 설치
- 20:06 - USB 연결
- 20:38 - CCleaner 삭제

Thank you
