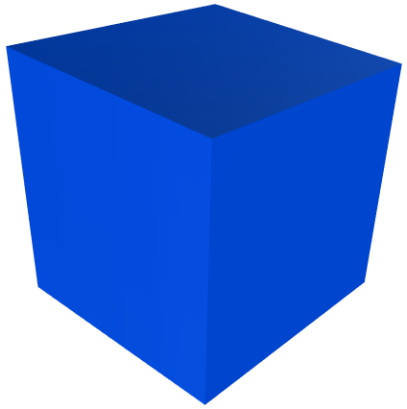


CFReDS

디지털포렌식트랙

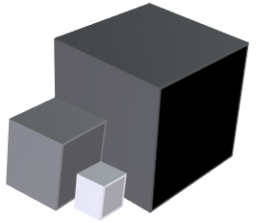
김태룡

INDEX

CFReDS

CFReDS

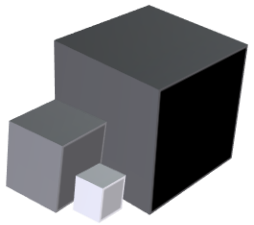
National Institute of
Standards and Technology



Computer Forensic
Reference Data Sets

CFReDS는 NIST에서 제작한 디지털포렌식 데이터 셋입니다.

CFReDS

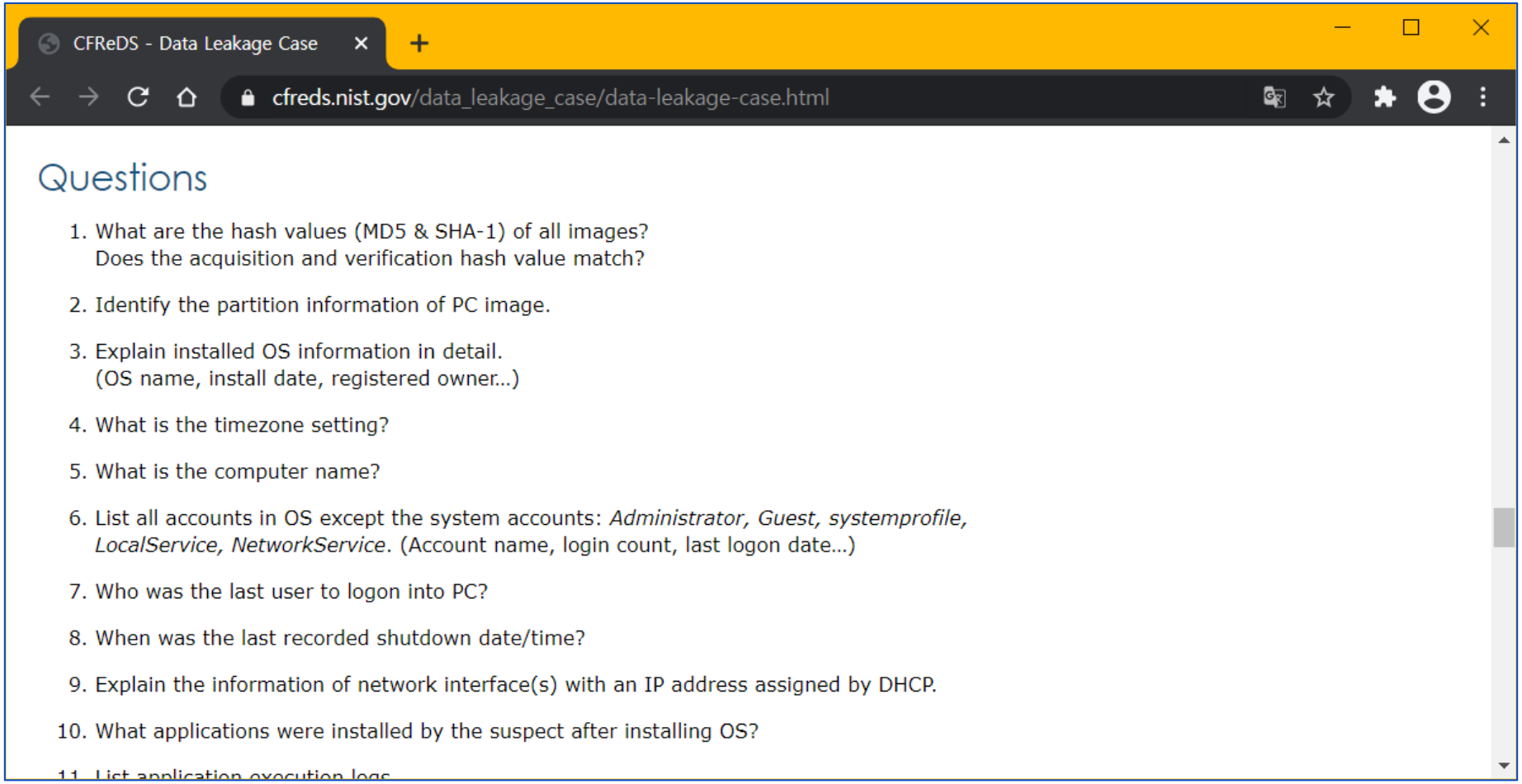


Computer Forensic Reference Data Sets

- Tool Test
- Proficiency Test
- Training

이는 포렌식 도구 검증, 전문성 시험, 교육용으로 사용됩니다.

CFReDS



CFReDS

CFReDS는 다양한 문제와 함께 파일이 제공됩니다.

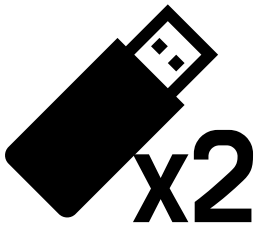
Process

Process

Data Leakage Case

Given data

PC Image



USB Image

CD Image

데이터 유출 사건이 주제였으며, 총 4개의 이미지를 받았습니다.

Process

Data Leakage Case

Questions

01. What are the hash values (MD5 & SHA-1) of all images?
02. Does the acquisition and verification hash value match?

...

59. List and explain methodologies of data leakage performed by the suspect.
60. Create a visual diagram for a summary of results.

문제는 총 60가지였지만...

Process

Data Leakage Case

Dramatized Questions

유명 국제기업 A에서 기술 개발 부서장으로 일하는 'Iaman Informant'가 보안 검색대를 통과하던 도중, 승인되지 않은 저장장치(USB 및 CD)가 검색되었으며, 현장에서 즉시 내용물을 확인하였으나 데이터 유출 흔적을 발견할 수 없었기에 추가 조사를 위하여 사내 디지털포렌식 팀으로 인계되었습니다.

Mentor : Encourage the use of open source tools.

실제 조사에 임하듯 문제없이 분석 흐름을 따라가기로 했습니다.

Process

Mentor : Encourage the use of open source tools.

하지만 멘토님은 오픈소스를 적극 사용하라고 하셨습니다.

Process

Mentor : Encourage the use of open source tools.

1-4) 분석 도구

도구	버전	용도	비고
Arsnal Image Mounter	3.3.138	가상 이미지 마운트 도구	프리웨어 https://arsenalrecon.com/downloads/
Autopsy	4.17.0	통합 포렌식 도구	오픈소스 https://github.com/sleuthkit/autopsy
HashTab	6.0.0	파일 SHA1 해시 검증	프리웨어 http://implbits.com/products/hashtab/
HxD	2.4.0.0(x86-64)	파일 Hex 확인 및 편집	프리웨어 https://mh-nexus.de/en/hxd/
NTFS Log Tracker	1.6	NTFS 파일시스템 로그 분석 도구	프리웨어 https://sites.google.com/site/forensicnote/ntfs-log-tracker
RECmd	1.6.0.0	레지스트리 분석 도구	오픈소스 https://github.com/EricZimmerman/RECmd
Shadow Copy View	1.15	볼륨 쉐도우 복사본 분석 도구	프리웨어 https://www.nirsoft.net/utils/shadow_copy_view.html
Thumbcache Viewer	1.0.3.6	Thumb Cache 분석 도구	오픈소스 https://github.com/thumbcacheviewer
WinPrefetchView	1.36	윈도우 프리패치 파일 확인	프리웨어 https://www.nirsoft.net/utils/win_prefetch_view.html
WinSearchDBAnalyzer	1.0.0.6	Windows edb 파일 분석 도구	오픈소스 https://github.com/moaistory/winsearchdbanalyzer
XstReader	1.14	이메일 분석 도구	오픈소스 https://github.com/Dijji/XstReader

AXIOM의 편리함에 젖어 있었기에 더욱이 힘들게 느껴졌지만,
덕분에 다양한 도구를 알게 되었습니다.

Process

데이터 유출 사례인 만큼 주변기기를 먼저 조사하였습니다.

Process

파일 명	크기	수정시각(UTC+9)	접근시각(UTC+9)	생성시각(UTC+9)	MD5 해시
[secret_project]_design_concept.ppt	1.72MB	2014-12-04 11:24:50	2015-02-15 16:52:08	2015-02-15 16:52:08	C60F97AA4961A462A9A1CDF9EDC6F989
[secret_project]_detailed_design.pptx	15.6MB	2014-12-16 11:10:26	2015-02-15 16:52:08	2015-02-15 16:52:09	837DC97F6C55FE2EA17FA59FF8CF78BC
[secret_project]_detailed_proposal.docx	33.5MB	2014-12-18 16:50:58	2015-02-15 16:52:12	2015-02-15 16:52:12	109B7644287DE12880A9A6D75C316C3A
[secret_project]_proposal.docx	6.18MB	2014-12-19 14:53:46	2015-02-15 16:52:20	2015-02-15 16:52:20	14C3030E006B9C2545BE9D23FC0C284F
[secret_project]_revised_points.ppt	13.8MB	2015-01-23 15:47:10	2015-02-15 16:52:10	2015-02-15 16:52:10	003CDFF7699172525 1812F9E8BA8477C
~$ecret_project]_proposal.docx	162 Bytes	2015-03-23 14:37:54	2015-03-23 14:37:54	2015-03-23 14:37:52	F90CD8CEDCD942B0C886592C497B9457

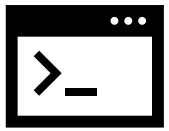
[표 2-2] USB#1에서 발견된 기밀자료

√ USB#1에 기밀자료를 복사한 흔적을 확인하였습니다

주변기기의 데이터 유출 정황을 확인하여
PC로 부터 결정적 증거를 찾기로 하였습니다.

Process

PC Image



Prefetch

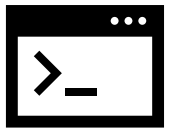
StikyNote	Ccleaner
Chrome	GoogleDrive
SearchIndexer	InternetExplorer
Outlook	Word
Eraser	

가장 먼저 프로그램 사용 기록을 알 수 있는
Prefetch를 확인하였습니다.

Process

"Tomorrow... Everything will be OK..."

D-1



Prefetch

StikyNote	Ccleaner
Chrome	GoogleDrive
SearchIndexer	InternetExplorer
Outlook	Word
Eraser	

Autopsy

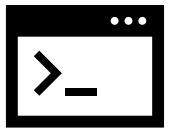
Autopsy를 통하여 StikyNote에 용의자가 퇴사 직전일에 작성한 메시지를 발견하였습니다.

Process

GoogleDrive

Eraser

Ccleaner



Prefetch

StikyNote	Ccleaner
Chrome	GoogleDrive
SearchIndexer	InternetExplorer
Outlook	Word
Eraser	

Autopsy

CFReDS

Autopsy를 통하여 인터넷 검색기록을 확인하여 드라이브 및 파일 제거 프로그램 다운로드 흔적을 발견하였습니다.

Process

Secret

Prefetch

StikyNote	Ccleaner
Chrome	GoogleDrive
SearchIndexer	InternetExplorer
Outlook	Word
Eraser	

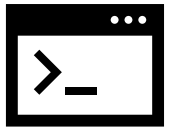
Autopsy

Autopsy를 통하여 윈도우 검색창에 secret 단어를 검색한 정황을 확인하였습니다.

Process

spy.conspirator

iaman.informant



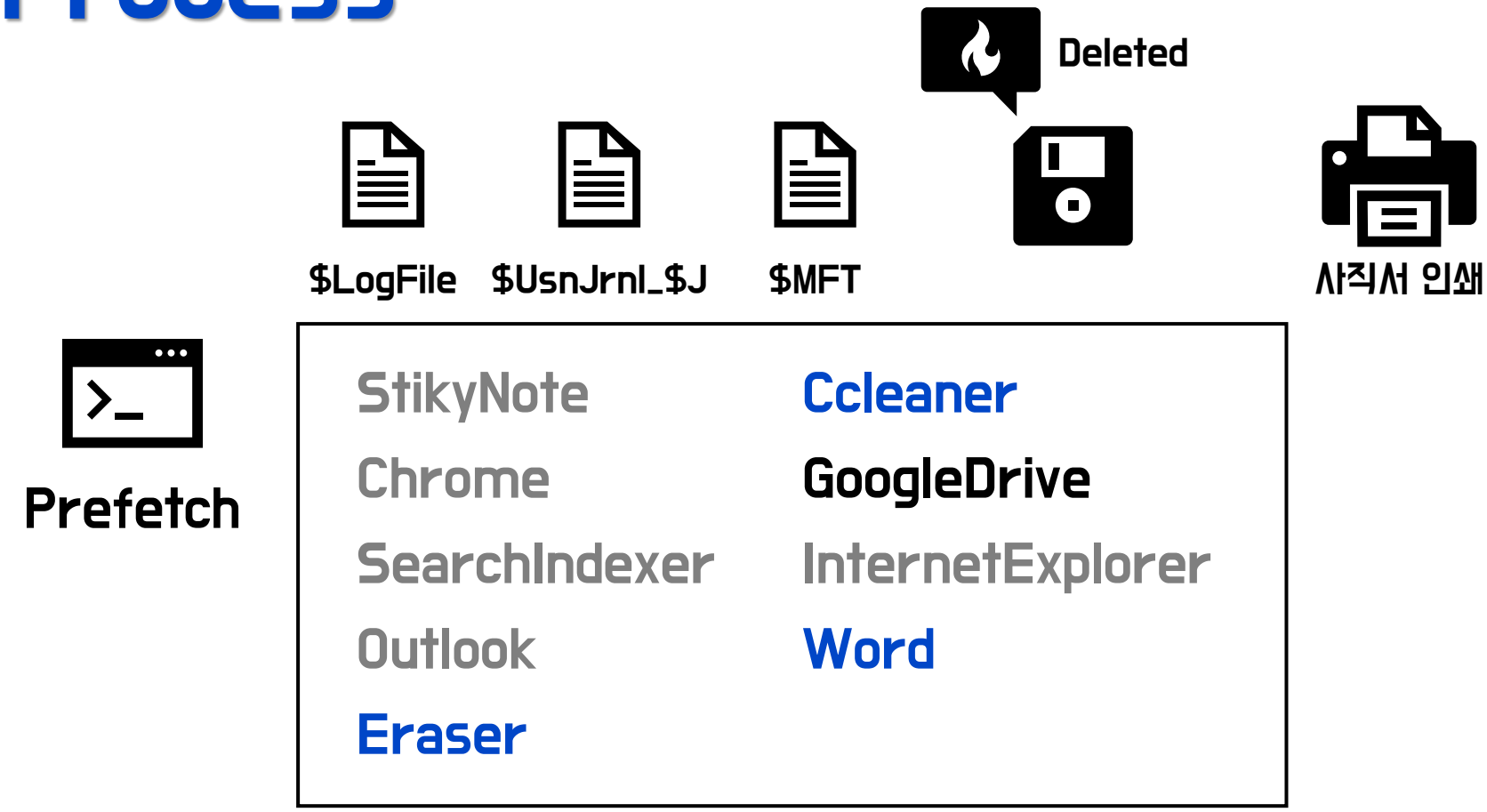
Prefetch

StikyNote	Ccleaner
Chrome	GoogleDrive
SearchIndexer	InternetExplorer
Outlook	Word
Eraser	

XstReader

XstReader를 통하여 Outlook 파일을 검사한 결과,
spy와 용의자간 메일 전달 정황을 확인할 수 있었습니다.

Process

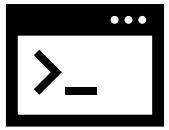


CFReDS

NTFSLogTracker를 통해 $LogFile, $UsnJrnl_$J, $MFT 분석 후, 안티포렌식 행위 및 사직서 인쇄 정황을 확인하였습니다.

Process

sync_log.log



Prefetch

StikyNote	Ccleaner
Chrome	GoogleDrive
SearchIndexer	InternetExplorer
Outlook	Word
Eraser	

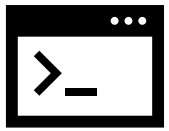
Autopsy

Autopsy를 통해 GoogleDrive를 확인하여 sync log를 확보하였으나, 일부 기록이 제거되어 있었습니다.

Process

sync_log.log

VSC



Prefetch

StikyNote	Ccleaner
Chrome	GoogleDrive
SearchIndexer	InternetExplorer
Outlook	Word
Eraser	

Autopsy

Arsenal Image Mounter

CFReDS

이에 Arsenal Image Mounter를 사용하여 볼륨쉐도우 복사본에서 이전 구글드라이브 기록 및 다양한 파일을 채증하였습니다.

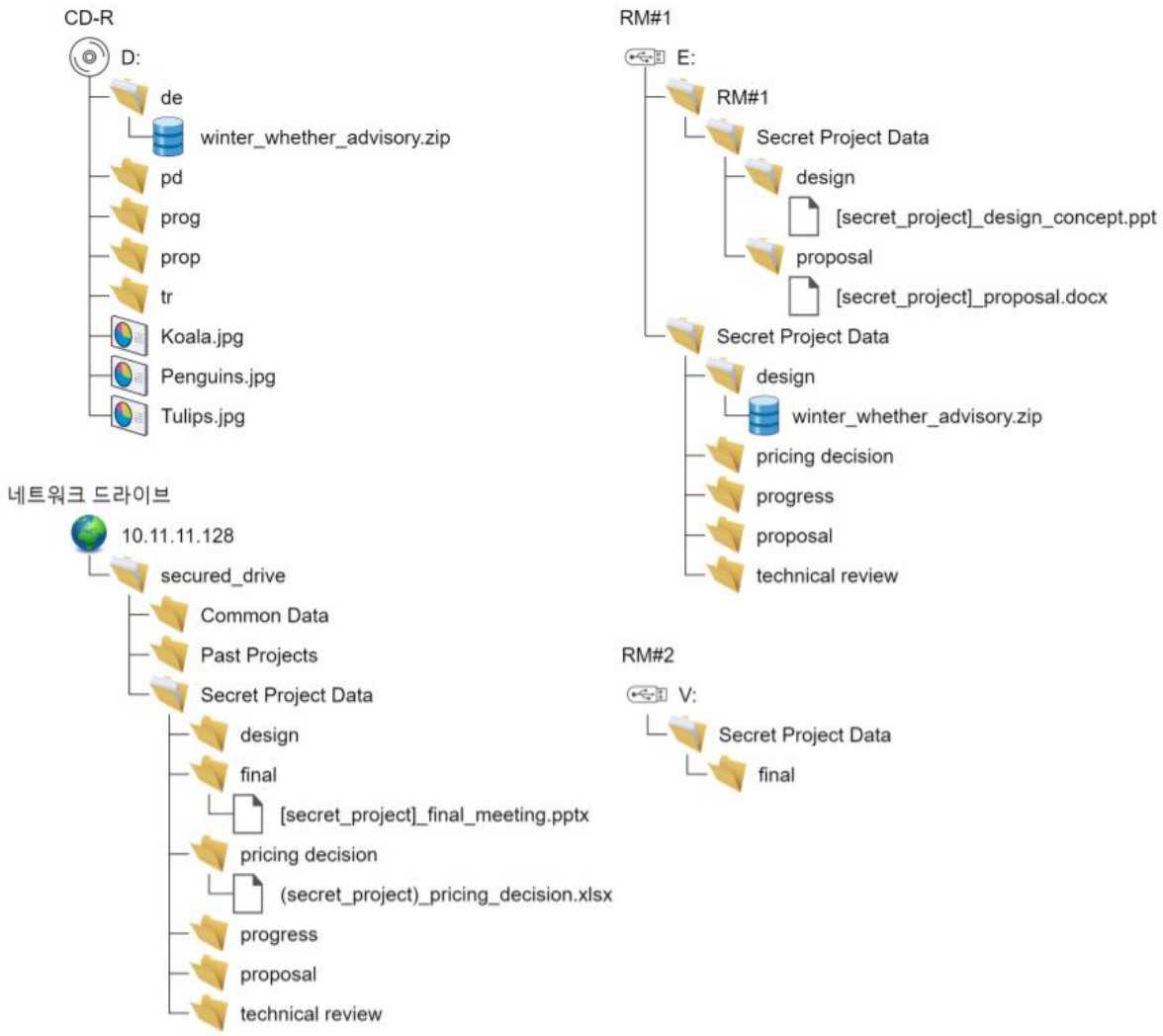
Process

The judge lacks time to read the reports.

- 최원영 Mentor -

모든 정황을 파악한 이후, 보고서를 작성할 때가 되었습니다.
하지만, 최원영 멘토님께서 판사는 보고서를 읽을 시간이
3분 밖에 되지 않는다 하셨습니다.

Process



[그림 5-19] 쉘백과 LNK파일을 기반으로 재구성된 장치별 구성항목

CFReDS

이에 읽기 힘든 테이블 자료를 그림 형식으로 제공하고,

Process

본문 요약

1. 사건 개요

국제기업 A의 기술 개발 부서장 'Iaman Informant'가 보안 검색대 통과 도중 승인되지 않은 저장 장치(USB 및 CD)가 검색되어 A사로부터 디지털포렌식 조사 의뢰를 받았습니다.

2. 이미지 정보

① 이미지 정보

순번	추출 대상	파일 명	용량	OS	SHA1
1	개인용 컴퓨터 (PC)	cfreds_2015_data_leakage_pc.E01	1.99GB	Windows 7 Ultimate SP1	72432916933F5A309A8C456B40C9601D1F8D2A4F
		cfreds_2015_data_leakage_pc.E02	1.99GB		0CAF4261ED8432A8B3BAA019B1B28FDF96F79130
		cfreds_2015_data_leakage_pc.E03	1.99GB		B6836C891736C4C0C2253C6803399BF0F2A599BA
		cfreds_2015_data_leakage_pc.E04	1.28GB		9159BFFD56097495F73F8BF967B75EB28B81E3DE
2	USB 이동식 저장장치#1	cfreds_2015_data_leakage_rm#1.E01	74.5MB	-	FFD0F3CBA3DFE3291F786B845A06A8AA56C1CD8C
3	USB 이동식 저장장치#2	cfreds_2015_data_leakage_rm#2.E01	243MB	-	2228554CD6FDD3CB5BB80E0A0CD7F21A2364DC99
4	CD-R	cfreds_2015_data_leakage_rm#3_type3.E01	90.2MB	-	75C106FD82FD2F8068190E9515B9FF1F9B60257E

3. 분석 결과

① 개인용 컴퓨터 (PC)

√ 이메일, 저장장치를 통한 기밀문서 유출 흔적을 발견하였습니다

② USB 이동식 저장장치#1

√ 기밀문서 복사 흔적을 발견하였습니다

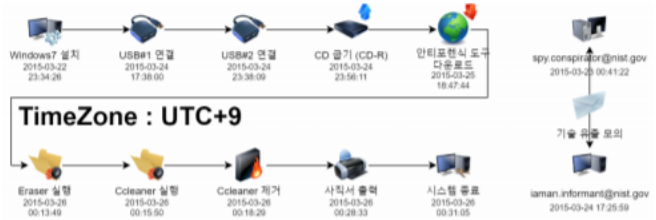
③ USB 이동식 저장장치#2

√ 기밀문서 복사 흔적을 발견하였습니다

④ CD-R

√ 기밀문서 복사 흔적을 발견하였습니다

⑤ 타임라인



4. 결론

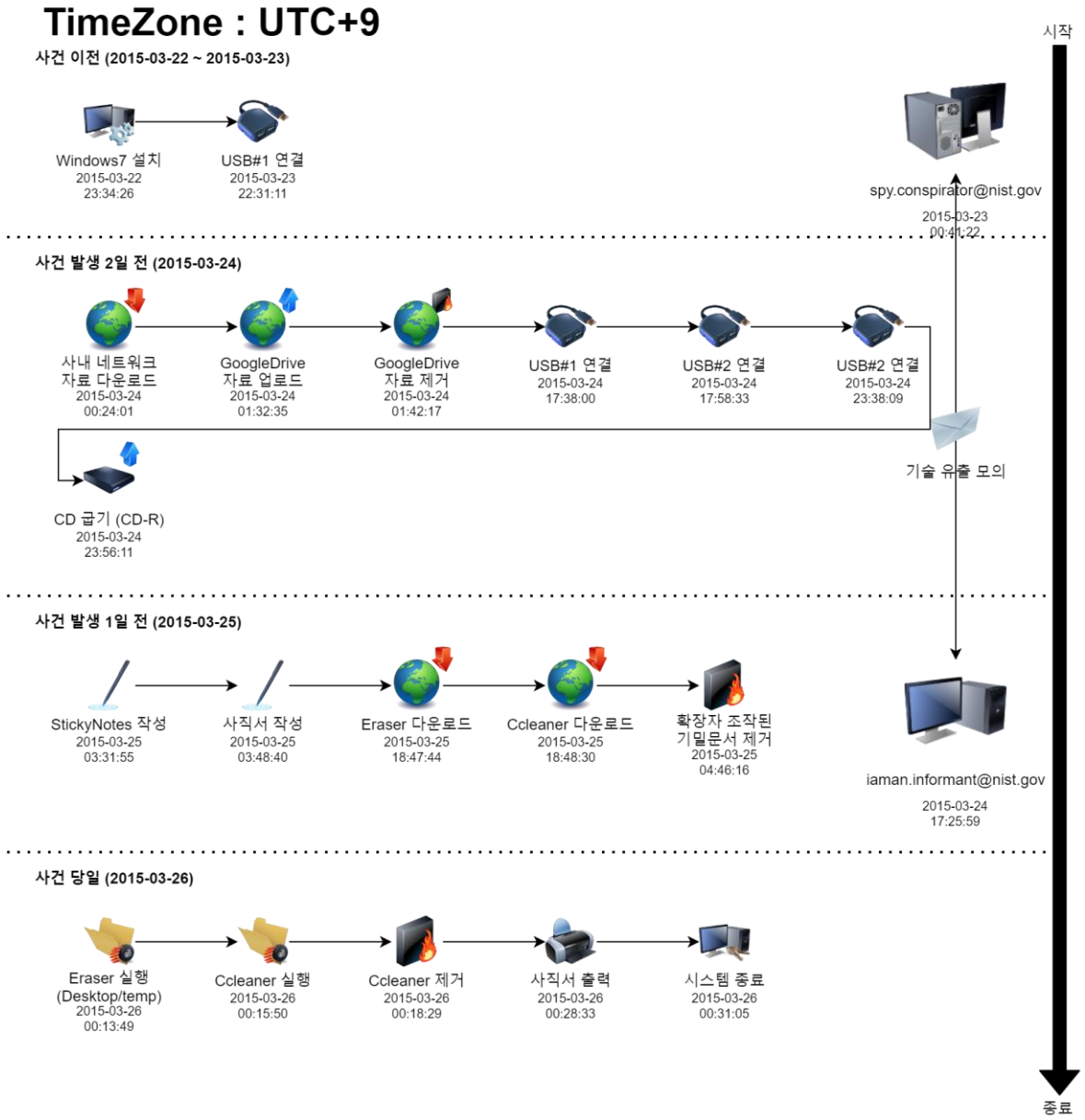
√ 국제기업 A 기술 개발 부서장 'Iaman Informant'는 기밀문서 유출을 시도하였습니다

CFReDS

보고서 첫 장에 전체 내용을 요약하였습니다.

Result

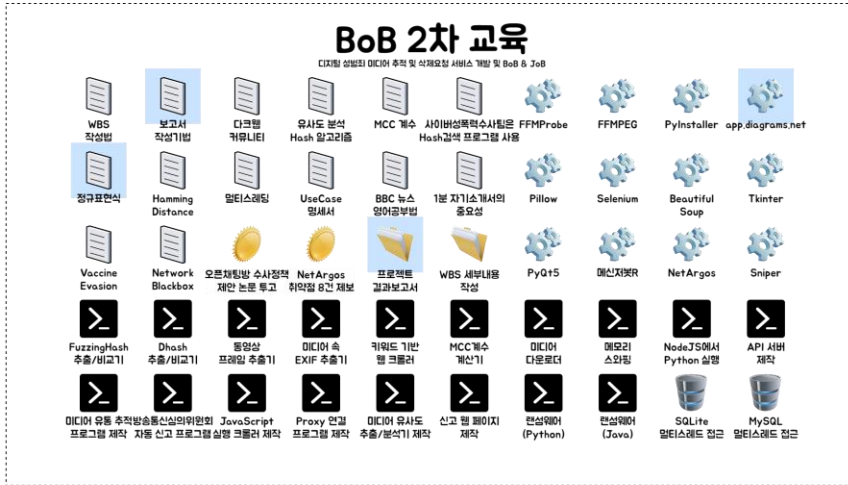
Result



CFReDS

CFReDS 데이터 유출 사건의 전체 타임라인입니다.

Result



CFReDS

CFReDS과제는 BoB를 통해 배운 내용의 약 20%와 관련 있었던 만큼, 그간 배운 다양한 내용을 복습할 수 있었습니다.

Result

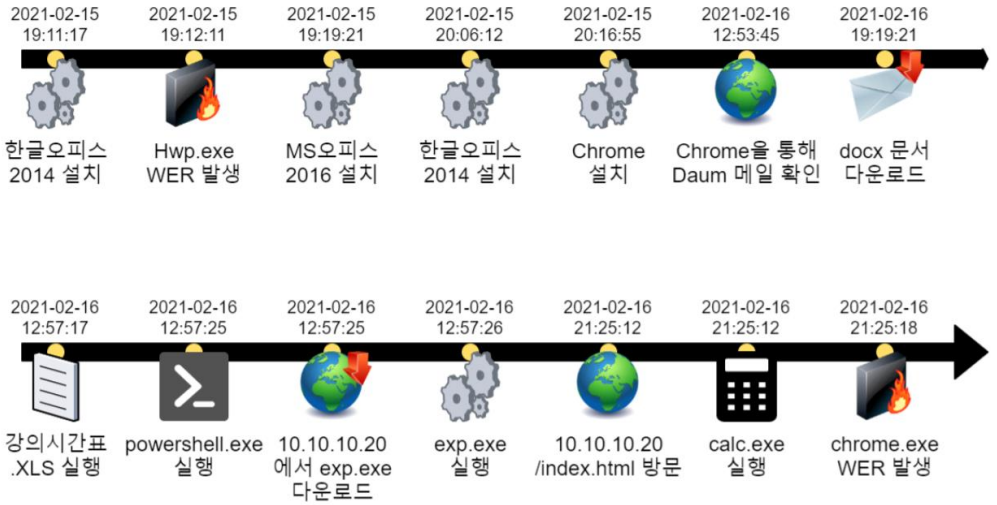
분석 보고서

무료 도구를 이용한
Windows 10 x64 분석 보고서

Windows 10 x64 analysis report
using free wares

2021년 02월 17일 ~ 2021년 02월 19일

Best of Best 9기
디지털포렌식 트랙



CFReDS

뿐만 아니라 CFReDS 풀이는 다양한 과제에 활용되었으며,
사용된 도구도 다양한 분석에 사용되었을 만큼 의미 있었습니다.

Thankyou