

무료 도구를 이용한 CFReDS 풀이 보고서 (각색)

디지털포렌식 김태룡

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		8E836C891736C4C0C2253C6803399BF0F2A599BA
		cfreds_2015_data_leakage_pc.E04	1.28GB		9159BFFD56097495F73FB8F967B75EB288B1E3DE
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	-	2228554CD6FDD3C85BB80E0A0CD7F21A2364DC99
4	CD-R	cfreds_2015_data_leakage_rm#3_type3.E01	90.2MB	-	75C106FDB2FD2F8068190E951589FF1F9860257E

3. 분석 결과

① 개인용 컴퓨터 (PC)

√ 이메일, 저장장치를 통한 기밀문서 유출 흔적을 발견하였습니다

② USB 이동식 저장장치#1

√ 기밀문서 복사 흔적을 발견하였습니다

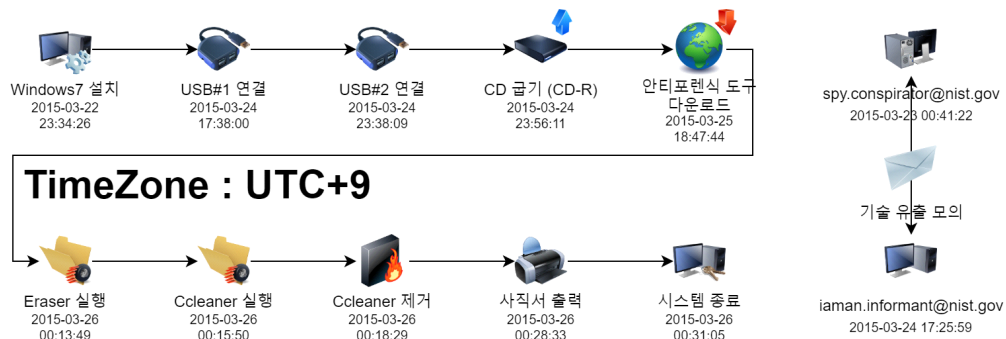
③ USB 이동식 저장장치#2

√ 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

1. 개요

1-1) 사건 개요

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.

1-2) 분석 환경

항목	값	항목	값
OS	Microsoft Windows 10 Home Edition	시스템 종류	64비트 운영 체제
프로세서	Intel(R) Core(TM) i7-1065G7	RAM	16 GB

[표 1-1] 분석 환경

1-3) 분석 대상 이미지

순번	추출 대상	파일 명	크기	OS/FileSystem	IP	SHA1
1	개인용 컴퓨터 (PC)	cfreds_2015_data_leakage_pc.E01	1.99GB	Windows 7 Ultimate SP1 NTFS	10.11.11.129	72432916933F5A309A8C456B40C9601D1F8D2A4F
		cfreds_2015_data_leakage_pc.E02	1.99GB			0CAFA4261ED8432A8B3BAA019B1B28FDF96F79130
		cfreds_2015_data_leakage_pc.E03	1.99GB			BE836C891736C4C0C2253C6803399BF0F2A599BA
		cfreds_2015_data_leakage_pc.E04	1.28GB			9159BFFD56097495F73F8BF967B75EB288B1E3DE
2	USB 이동식 저장장치#1	cfreds_2015_data_leakage_rm#1.E01	74.5MB	exFAT	-	FFD0F3CBA3DFE3291F786B845A06A8AA56C1CD8C
3	USB 이동식 저장장치#2	cfreds_2015_data_leakage_rm#2.E01	243MB	FAT32	-	2228554CD6FDD3C85BB80E0A0CD7F21A2364DC99
4	CD-R	cfreds_2015_data_leakage_rm#3_type3.E01	90.2MB	-	-	75C106FDB2FD2F8068190E951589FF1F9860257E

[표 1-2] 분석 대상

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
RECcmd	1.6.0.0	레지스트리 분석 도구	오픈소스 https://github.com/EricZimmerman/RECcmd
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/moiaistory/winsearchdbanalyzer
XstReader	1.14	이메일 분석 도구	오픈소스 https://github.com/Dijji/XstReader

1-5) 추가 정보

- 기밀 파일은 승인된 외부저장장치 및 보안 네트워크 드라이브에 저장하고 보관해야 한다.
- 기밀 파일은 오후 7시부터 다음날 오전 1시 까지(UTC+9) 허용된 시간에만 접근할 수 있다.
- 노트북, 휴대폰, 저장장치 등은 회사 반입 금지이며, 모든 직원은 보안 검색대를 통과해야한다.

2. USB 이동식 저장장치#1 조사 내역

- 기술 개발 부서장이 승인되지 않은 저장장치(USB 및 CD)를 소지하여 데이터 유출 사고가 의심되는 만큼, PC 이미지를 확인하기 전에 이동식 저장장치를 먼저 조사하였습니다.

2-1) 이미지 무결성 검증

	파일시스템	크기	시간(UTC+9)	SHA1 해시
현장 기록	exFAT	74.5MB	2015년 03월 27일 19시 50분 07초	FFD0F3CBA3DFE3291F786 B845A06A8AA56C1CD8C
검증 결과	exFAT	74.5MB	2015년 03월 27일 19시 50분 07초	FFD0F3CBA3DFE3291F786 B845A06A8AA56C1CD8C

[표 2-1] 이미징 당시 현장 기록과 조사 과정에서 확인된 정보 비교자료

Hex	Text	Application	File Metadata	Context	Results	Annotations	Other Occurrences
Name	/img_cfreds_2015_data_leakage_rm#1.E01						
Type	E01						
Size	4004511744						
MD5	8bfa4230bf4e35db966b8c1a9321a0b1						
SHA1	f6bb840e98dd7c325af45539313fc3978fff812c						
SHA256	Not calculated						
Sector Size	512						
Time Zone	Asia/Seoul						
Acquisition Details	Description: Company's USB Case Number: 0x11 Evidence Number: 0x02-1 Examiner Name: dForensics_Team Notes: data_leakage_case Acquired Date: Fri Mar 27 19:50:07 2015 System Date: Fri Mar 27 19:50:07 2015						

Autopsy

[그림 2-1] USB 이미지 파일에 대한 정보를 확인 한 모습

✓ 현장 기록과 이미지가 동일함을 확인하였습니다

2-2) 삭제된 파일 복구 및 채증

- USB#1 이미지 내에서 다수의 대외비 문서가 발견되었으며, 그중 일부로부터 삭제 흔적을 발견하였습니다.

Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Local
[secret_project]_design_conceptppt			2014-12-04 11:24:50 KST	0000-00-00 00:00:00	2015-02-15 16:52:08 KST	2015-02-15 16:52:08 KST	1810432	Allocated	Allocated	unknown	/img_c
[secret_project]_detailed_design.pptx			2014-12-16 11:10:26 KST	0000-00-00 00:00:00	2015-02-15 16:52:08 KST	2015-02-15 16:52:08 KST	16381123	Allocated	Allocated	unknown	/img_c
[secret_project]_revised_points.ppt			2015-01-23 15:47:10 KST	0000-00-00 00:00:00	2015-02-15 16:52:10 KST	2015-02-15 16:52:10 KST	14547860	Allocated	Allocated	unknown	/img_c

Autopsy

[그림 2-2] 기밀문서가 포함되어있는 모습

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	003CDF76991725251812F9E8BA8477C
~\$secret_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

3. USB 이동식 저장장치#2 조사 내역

3-1) 이미지 무결성 검증

	파일시스템	크기	시간(UTC+9)	SHA1 해시
현장 기록	FAT32	243MB	2015년 03월 26일 04시 21분 33초	FFD0F3CBA3DFE3291F786 B845A06A8AA56C1CD8C
검증 결과	FAT32	243MB	2015년 03월 26일 04시 21분 33초	FFD0F3CBA3DFE3291F786 B845A06A8AA56C1CD8C

[표 3-1] 이미징 당시 현장 기록과 조사 과정에서 확인된 정보 비교자료

Hex	Text	Application	File Metadata	Context	Results	Annotations	Other Occurrences
Name	/img_cfreds_2015_data_leakage_rm#2.E01						
Type	E01						
Size	4004511744						
MD5	b4644902acab4583a1d0f9f1a08faa77						
SHA1	048961a85ca3eced8cc73f1517442d31d4dca0a3						
SHA256	Not calculated						
Sector Size	512						
Time Zone	Asia/Seoul						
Acquisition Details	Description: cfreds_2015_data_leakage_rm#2						
	Case Number: 0x11						
	Evidence Number: 0x02						
	Examiner Name: dForensics_Team						
	Notes: data_leakage_case						
	Model: Cruzer Fit						
	Serial Number: 4C530012550531106501						
	Device Label: SanDisk						
	Acquired Date: Sat Mar 28 04:21:33 2015						
	System Date: Sat Mar 28 04:21:30 2015						

Autopsy

[그림 3-1] USB 이미지 파일에 대한 정보를 확인 한 모습

✓ 현장 기록과 이미지가 동일함을 확인하였습니다

3-2) 삭제된 파일 복구 및 채증

- 다수의 파일 삭제 흔적을 발견하였으며, 파일 시그니처와 확장자명이 일치하지 않는 파일을 일부 발견하였습니다. 이를 통해 기술 개발 부서장은 컴퓨터 지식을 갖춘 인물로 파악됩니다.

Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known
winter Storm.exe			2015-01-23 15:47:10 KST	0000-00-00 00:00:00	2015-09-24 00:00:00 KST	2015-09-24 09:59:27 KST	1454768	Unallocated	Unallocated	unknown
winter_weather_advisory.zip			2014-12-16 12:10:26 KST	0000-00-00 00:00:00	2015-09-24 00:00:00 KST	2015-09-24 09:59:37 KST	16361123	Unallocated	Unallocated	unknown
PRICN-1			2015-09-24 09:57:32 KST	0000-00-00 00:00:00	2015-09-24 00:00:00 KST	2015-09-24 09:59:39 KST	4096	Unallocated	Unallocated	unknown
[current folder]			2015-09-24 09:57:32 KST	0000-00-00 00:00:00	2015-09-24 00:00:00 KST	2015-09-24 09:59:39 KST	4096	Unallocated	Unallocated	unknown

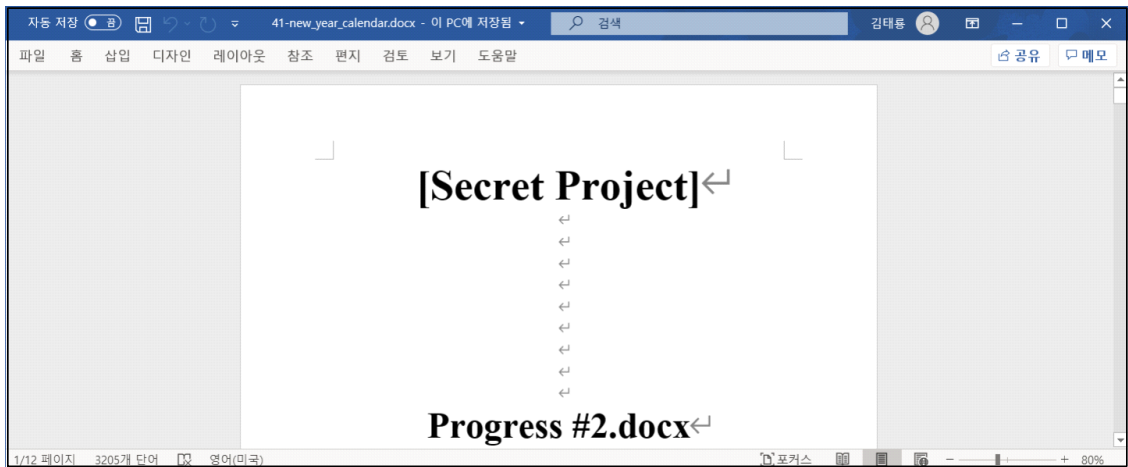
Autopsy

[그림 3-2] 삭제된 문서들

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	50	4B	03	04	14	00	06	00	08	00	00	00	21	00	2C	00	PK.....!.,.
00000010	9B	C6	75	01	00	00	A5	06	00	00	13	00	08	02	5B	43	>Eu...¥.....[C
00000020	6F	6E	74	65	6E	74	5F	54	79	70	65	73	5D	2E	78	6D	ontent_Types].xm
00000030	6C	20	A2	04	02	28	A0	00	02	00	00	00	00	00	00	00	1 <.(.....

HxD

[그림 3-3] 확장자와 파일시그니처가 일치하지 않는 모습



[그림 3-4] 파일 시그니처에 맞는 확장자로 변경 이후 확인할 수 있는 기밀문서

파일 명	크기	수정시각(UTC+9)	접근시각(UTC+9)	생성시각(UTC+9)	MD5 해시
winter_storm.amr	13.8MB	2015-01-23 16:47:10	2015-03-24 00:00:00	2015-03-24 09:59:27	003CDFF76991725251812F9E8BA8477C
winter_whether_advisory.zip	15.6MB	2014-12-16 12:10:26	2015-03-24 00:00:00	2015-03-24 09:59:37	837DC97F6C55FE2EA17FA59FF8CF78BC
my_favorite_cars.db	1.20MB	2015-01-16 15:10:24	2015-03-24 00:00:00	2015-03-24 09:59:39	A23C3ED3CF482A3D5C420F6FF4FEA6F6
my_favorite_movies.7z	97.7KB	2015-01-08 17:08:24	2015-03-24 00:00:00	2015-03-24 09:59:39	975D98575F92D2E466ECB96D39701FC8
new_years_day.jpg	9.76MB	2014-12-01 14:50:26	2015-03-24 00:00:00	2015-03-24 09:59:39	0329D88F08A8CB2C8057A8FA9418F9F3
super_bowl.avi	9.81MB	2014-12-02 13:28:58	2015-03-24 00:00:00	2015-03-24 09:59:40	2EBB8B59B8019A94C7416D9ACBAAD658
my_friends.svg	57.0KB	2015-01-20 11:13:44	2015-03-24 00:00:00	2015-03-24 09:59:43	945FAA85FC3D88C8ACC21D9467FDF43C
my_smartphone.png	4.23MB	2015-01-05 11:57:22	2015-03-24 00:00:00	2015-03-24 09:59:43	83E8B938071484D05BAEE23111A80768
new_year_calendar.one	26.7KB	2015-01-12 14:23:42	2015-03-24 00:00:00	2015-03-24 09:59:44	11A973841CF9DB3255FFFF84F5B277D2
a_gift_from_you.gif	33.5MB	2014-12-18 17:50:58	2015-03-24 00:00:00	2015-03-24 09:59:44	109B7644287DE12880A9A6D75C316C3A
landscape.png	6.18MB	2014-12-19 15:53:46	2015-03-24 00:00:00	2015-03-24 10:00:06	14C3030E006B9C2545BE9D23FC0C284F
diary_#1d.txt	118KB	2015-01-05 17:01:08	2015-03-24 00:00:00	2015-03-24 10:00:12	F7F1C40D7F647EE251D8282CA70A63D9
diary_#1p.txt	448KB	2015-01-05 15:15:08	2015-03-24 00:00:00	2015-03-24 10:00:12	CB274F8616F4F20A8043D09F36AC2DEB
diary_#2d.txt	644KB	2015-01-12 17:25:40	2015-03-24 00:00:00	2015-03-24 10:00:13	A9DBDB7177289F4CA1CC0D8748164B11
diary_#2p.txt	1.10MB	2015-01-12 15:20:26	2015-03-24 00:00:00	2015-03-24 10:00:14	198F35DC5642516E96D99738274CFFD8
diary_#3d.txt	2.25MB	2015-01-20 16:05:00	2015-03-24 00:00:00	2015-03-24 10:00:15	2F500982AEE7CBB0BA9A7AB9F46E902A
diary_#3p.txt	317KB	2015-01-20 14:18:06	2015-03-24 00:00:00	2015-03-24 10:00:18	26EADA303D94F2D1EF5407D44763ECB8

[표 2-2] USB#2에서 발견된 기밀자료

√ 2015년 03월 24일 09시 59분경 USB#2에 기밀자료를 복사한 흔적을 확인하였습니다

4. CD-R 조사 내역

4-1) 이미지 무결성 검증

	파일시스템	크기	시간(UTC+9)	SHA1 해시
현장 기록	-	90.2MB	2015년 03월 27일 00시 30분 10초	75C106FDB2FD2F8068190 E951589FF1F9860257E
검증 결과	-	90.2MB	2015년 03월 27일 00시 30분 10초	75C106FDB2FD2F8068190 E951589FF1F9860257E

[표 4-1] 이미징 당시 현장 기록과 조사 과정에서 확인된 정보 비교자료

Hex	Text	Application	File Metadata	Context	Results	Annotations	Other Occurrences
Name	/img_cfreds_2015_data_leakage_rm#3_type3.E01		E01				
Type	E01						
Size	107546624						
MD5	df914108fb3d86744eb688eba482fddf						
SHA1	7f3c2eb1f1e2db97be6e963625402a0e362a532c						
SHA256	Not calculated						
Sector Size	512						
Time Zone	Asia/Seoul						
Acquisition Details	Description: cfreds_2015_data_leakage_rm#3						
	Case Number: 0x11						
	Evidence Number: 0x03						
	Examiner Name: dForensics_Team						
	Notes: data_leakage_case						
	Model: DVD+-RW GT80N						
	Serial Number: 12/06/27 7U01						
	Device Label: HL-DT-ST						
	Acquired Date: Fri Mar 27 00:30:10 2015						
	System Date: Fri Mar 27 00:30:03 2015						

Autopsy

[그림 4-1] CD-R 이미지 파일에 대한 정보를 확인 한 모습

✓ 현장 기록과 이미지가 동일함을 확인하였습니다

4-2) 삭제된 파일 복구 및 채증

- 모든 파일이 삭제된 흔적을 발견하였으며, Excel, PowerPoint, Word 형식 기밀문서가 존재했던 흔적을 찾았습니다.

Date Sources	Table	Thumbnail	Summary
cfreds_2015_data_leakage_rm#3_type3			
Views			
File Types			
Deleted Files			
All (0)			
MB File Size			
Results			
Extracted Content			
Keyword Hits			
Single Literal Keyword Search (0)			
Single Regular Expression Search (1)			
Email Addresses (3)			
(\w{1,3}@\w{1,3}(\.\w{1,3}){1,3}\.\w{2,3})			
eric_p_javen@omb.eop.gov (1)			
mmun@loc.gov (1)			
wayne.longman@att.net (1)			
Hashset Hits			
E-Mail Messages			
Interesting Items			
Accounts			
Tags			
Reports			

[그림 4-2] 비할당 영역에 보존되어있는 기밀문서

- 파일 존재여부가 확인되었기에 각 확장자의 시그니처 값을 활용하여 비할당 영역에 남겨진 파일을 복구하였습니다.

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
009585B0	04	00	00	00	00	00	00	00	05	01	00	00	00	00	00	00
009585C0	00	00	28	04	C2	07	00	00	50	4B	03	04	14	00	06	00	..(..Å...FK.....
009585D0	08	00	00	00	21	00	56	AE	07	C3	F7	00	00	00	A9	01!.V@.Å+...@.
009585E0	00	00	13	00	08	02	5B	43	6F	6E	74	65	6E	74	5F	54[Content_T
009585F0	79	70	65	73	5D	2E	78	6D	6C	20	A2	04	02	28	A0	00	ypes].xml c..(.
00958600	02	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00958610	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00958620	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

오프셋(h): 9585C8 블록(h): 9585C8-959189 길이(h): BC2 **HxD**

[그림 4-3] 파일 시그니처 값을 기반 하여 카빙 작업을 진행하는 모습

파일 명	크기	수정시각(UTC+9)	접근시각(UTC+9)	생성시각(UTC+9)	MD5 해시
[secret_project]_market_analysis.xlsx	10.2MB	2014-12-01 22:50:25	-	2003-11-24 04:09:57	0329d88f08a8cb2c8057a8fa9418f9f3
[secret_project]_detailed_design.pptx	16.3MB	2014-12-16 11:10:25	-	2005-12-03 11:53:25	837dc97f6c55fe2ea17fa59ff8cf78bc
[secret_project]_proposal.docx	6.48MB	2014-12-19 23:53:00	-	2014-12-18 01:52:00	14c3030e006b9c2545be9d23fc0c284f
[secret_project]_technical_review_#1.docx	121KB	2015-01-05 00:59:00	-	2015-01-05 12:56:00	f7f1c40d7f647ee251d8282ca70a63d9
[secret_project]_progress_#1.docx	4.44MB	2015-01-05 19:57:00	-	2015-01-05 19:56:00	83e8b938071484d05baee23111a80768
[secret_project]_technical_review_#1.pptx	458KB	2015-01-05 23:15:06	-	2003-07-10 17:33:15	cb274f8616f4f20a8043d09f36ac2deb
[secret_project]_price_analysis_#1.xlsx	97.0KB	2015-01-08 01:08:22	-	2004-10-05 18:50:21	975d98575f92d2e466ecb96d39701fc8
[secret_project]_technical_review_#2.docx	658KB	2015-01-12 01:24:00	-	2015-01-12 22:24:00	a9dbdb7177289f4ca1cc0d8748164b11
[secret_project]_progress_#2.docx	27.4KB	2015-01-12 22:23:00	-	2015-01-12 22:23:00	11a973841cf9db3255ffff84f5b277d2
[secret_project]_technical_review_#2.pptx	1.15MB	2015-01-12 23:20:25	-	2003-12-04 22:39:14	198f35dc5642516e96d99738274cffd8
[secret_project]_price_analysis_#2.xlsx	1.20MB	2015-01-16 23:10:23	-	2003-02-04 15:11:17	a23c3ed3cf482a3d5c420f6ff4fea6f6
[secret_project]_technical_review_#3.docx	2.36MB	2015-01-20 00:04:00	-	2015-02-06 00:04:00	2f500982aee7cbb0ba9a7ab9f46e902a
[secret_project]_progress_#3.docx	57.3KB	2015-01-20 19:13:00	-	2015-01-20 10:12:00	9e32861d49b1ddeec233151bb4a8919
[secret_project]_technical_review_#3.pptx	325KB	2015-01-20 22:18:05	-	2001-12-12 20:10:54	26eada303d94f2d1ef5407d44763ecb8

[표 4-2] CD-R에서 발견된 기밀자료

√ CD-R에 기밀자료를 복사했던 흔적을 발견하였습니다

5. Iaman Informant PC 조사 내역

5-1) 이미지 무결성 검증

	OS	크기	시간(UTC+9)	SHA1 해시
현장 기록	Windows 7	20GB	2015년 04월 23일 23시 58분 22초	afe5c9ab487bd47a8a9856 b1371c2384d44fd785
검증 결과	Windows 7	20GB	2015년 04월 23일 23시 58분 22초	afe5c9ab487bd47a8a9856 b1371c2384d44fd785

[표 5-1] 이미징 당시 현장 기록과 조사 과정에서 확인된 정보 비교자료

Hex	Text	Application	File Metadata	Context	Results	Annotations	Other Occurrences
Name	/img_cfreds_2015_data_leakage_pc.E01						
Type	E01						
Size	21474836480						
MD5	a49d1254c873808c58e6f1bcd60b5bde						
SHA1	afe5c9ab487bd47a8a9856b1371c2384d44fd785						
SHA256	Not calculated						
Sector Size	512						
Time Zone	Asia/Seoul						
Acquisition Details	Description: cfreds_2015_data_leakage_pc Case Number: 0x11 Evidence Number: 0x01 Examiner Name: dForensics_Team Notes: data_leakage_case Acquired Date: Thu Apr 23 23:58:22 2015 System Date: Thu Apr 23 23:58:21 2015 Acquiry Operating System: Windows 7 Acquiry Software Version: 7.10						

Autopsy

[그림 5-1] PC 이미지 파일에 대한 정보를 확인 한 모습

✓ 현장 기록과 이미지가 동일함을 확인하였습니다

5-2) 파티션 정보 확인

ID	파티션 이름	파일시스템	크기	비고
1	vol1	-	2,048 섹터	비할당
2	vol2	NTFS	2,045,952 섹터	할당
3	vol3	NTFS	41,527,296 섹터	할당
4	vol4	-	2,048 섹터	비할당

[표 5-2] PC 이미지의 파티션 정보

Name	ID	Starting Sector	Length in Sectors	Description	Flags
vol1 (Unallocated: 0-2047)	1	0	2048	Unallocated	Unallocated
vol2 (NTFS / exFAT (0x07): 2048-206847)	2	2048	204800	NTFS / exFAT (0x07)	Allocated
vol3 (NTFS / exFAT (0x07): 206848-41940991)	3	206848	41734144	NTFS / exFAT (0x07)	Allocated

Hex	Text	Application	File Metadata	Context	Results	Annotations	Other Occurrences
Page: 1 of 64	Page	Go to Page:	Jump to Offset	Launch in HxD			
0x00000190: 6E 67 20 73 79 73 74 65 60 00 40 69 73 73 69 6E	ng system, Missin						
0x000001a0: 67 20 6F 70 65 72 61 74 69 6E 67 20 73 79 73 74	g operating syst						
0x000001b0: 65 60 00 00 00 63 7B 9A 20 57 26 F0 00 00 80 20	ew...c[. W[...						
0x000001c0: 21 00 07 DF 13 DC 00 08 00 00 00 20 03 00 00 DF						
0x000001d0: 14 0C 07 FE FF FF 00 28 03 00 00 00 7C 02 00 00						
0x000001e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00						

Autopsy

[그림 5-2] 파티션 정보를 확인 한 모습

✓ 파티션 조작이 없음을 확인하였습니다

5-3) 시스템 정보 확인

항목	값	항목	값
OS	Windows 7 Ultimate SP 1	설치일(UTC+9)	2015년 3월 22일 23:34:26
버전	6.1	종료일 ¹⁾ (UTC+9)	2015년 3월 26일 00:31:05
컴퓨터 이름 ²⁾	INFORMANT-PC	타임 존	Eastern Standard Time ard Time
소유자	informant	네트워크 주소 ³⁾	10.11.11.129

[표 5-3] 시스템 정보

	CurrentBuild	RegSz	7601	00-00
	SoftwareType	RegSz	System	00-00-00-00-00-00
	CurrentType	RegSz	Multiprocessor Free	65-00-64-00-00-00-6E-00-64-00-69...
	InstallDate	RegDword	1427034866	
	RegisteredOrganization	RegSz		
	RegisteredOwner	RegSz	informant	65-00-72-00-00-00-6C-00
	SystemRoot	RegSz	C:\Windows	00-00-00-00-00-00
	InstallationType	RegSz	Client	00-00-00-00-00-00
	EditionID	RegSz		
	ProductName	RegSz		

RECmD - SOFTWARE 레지스트리

	DaylightBias		-60	
	DaylightName		@tzres.dll,-111	
	DaylightStart		Month 3, week of month 2, day of week 0, Hours:Minutes:Seconds:Milliseconds 2:0:0:0	
	StandardBias		0	
	StandardName		@tzres.dll,-112	
	StandardStart		Month 11, week of month 1, day of week 0, Hours:Minutes:Seconds:Milliseconds 2:0:0:0	
	TimeZoneKeyName		Eastern Standard Time	
	ActiveTimeBias		240	

RECmD - SYSTEM 레지스트리

[그림 5-3] 시스템 정보를 확인 한 모습

✓ 시스템 기본 정보를 확보하였습니다

5-4) 계정 정보 확인

ID	이름	그룹	생성일(UTC+9)	로그인 횟수	최근 접속(UTC+9)
500	Administrator	Administrators	2015-03-25 19:33:22	6	2010-11-21 12:47:20
501	Guest	Guests	2015-03-25 19:33:22	0	-
1000	informant	Administrators	2015-03-22 23:33:54	10	2015-03-25 23:45:59
1001	admin11	Administrators, Users	2015-03-22 00:51:54	2	2015-03-22 00:57:02
1002	ITechTeam	Administrators, Users	2015-03-22 00:52:30	0	-
1003	temporary	Users	2015-03-22 00:53:01	1	2015-03-22 00:55:57

[표 5-4] 계정 정보

Key name	# value	User Id	Invalid Login Count	Total Login Count	Created On	Last Login Time	User Name	Full Name	Groups
		500	0	6	2015-03-25 10:33:22	2010-11-21 03:47:20	Administrator		Administrators
		501	0	0	2015-03-25 10:33:22		Guest		Guests
		1000	0	10	2015-03-22 14:33:54	2015-03-25 14:45:59	informant		Administrators
		1001	0	2	2015-03-22 15:51:54	2015-03-22 15:57:02	admin11	admin11	Administrators, Users
		1002	1	0	2015-03-22 15:52:30		ITechTeam	ITechTeam	Administrators, Users
		1003	1	1	2015-03-22 15:53:01	2015-03-22 15:55:57	temporary	temporary	Users

RECmD - SAM 레지스트리

[그림 5-4] 계정 정보를 확인 한 모습

✓ informant 계정에 대한 활동 기간을 확인하였습니다

- 1) 마지막 시스템 종료 시각 : SYSTEM\ControlSet001\Control\Windows
- 2) 컴퓨터 이름 : SYSTEM\ControlSet001\Control\ComputerName\ComputerName
- 3) 네트워크 정보 : SYSTEM\ControlSet001\services\Tcpip\Parameters\Interfaces

5-5) 프로그램 사용 흔적 확인

- PC정보 수집결과, 기술 개발 부서장은 informant 계정을 사용하였음을 알게 되었습니다. 때문에 informant 계정 생성일(2015년 03월 22일 23:33:54) 부터 최근 종료일(2015년 3월 26일 00:31:05) 사이 활동을 확인하기로 하였습니다.
- 또한 USB 및 CD-R 저장장치에서 기밀문서 복사 흔적과 증거 인멸 시도가 있었으므로, 관련 솔루션 사용 여부를 확인하기로 하였습니다.

[그림 5-5] 안티포렌식 도구가 설치되었던 흔적

프로그램 이름	비고	프로그램 이름	비고
CCleaner	제거됨	Eraser	x64
Google Drive	x86	Google Chrome	x86

[표 5-5] 설치된 응용 프로그램

- CCleaner와 Eraser가 설치된 정황을 통해 안티포렌식 행위가 일어난 시간을 알아내어 해당 시간대를 기준으로 조사를 이어 해 보기로 하고, 안티포렌식 도구의 사용 시간을 알아내기 위해 프리패치 파일을 추출한 다음 확인 해 보았습니다.

[그림 5-6] 프로그램 실행 흔적(프리패치 파일 목록)

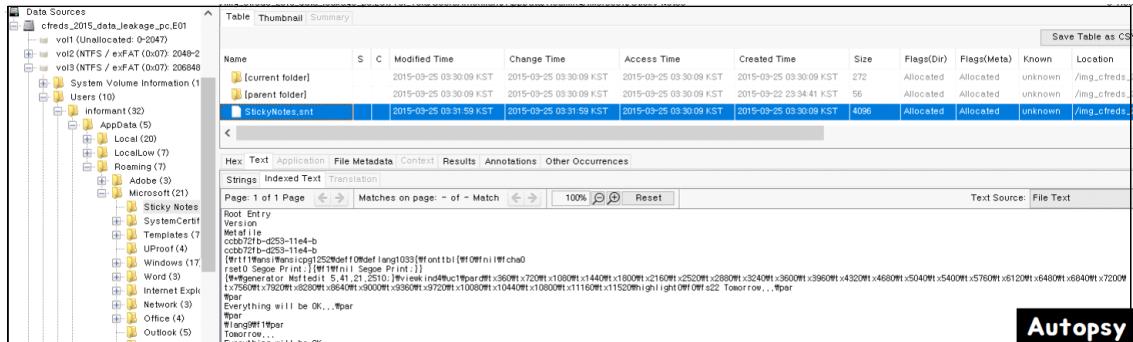
실행 경로	마지막 실행일(UTC+9)	실행 횟수
SYSTEM32/STIKYNOT.EXE	2015-03-25 03:31:55	2
PROGRAM FILES (X86)/GOOGLE/CHROME/APPLICATION/CHROME.EXE	2015-03-25 06:05:38	71
SYSTEM32/SEARCHINDEXER.EXE	2015-03-25 19:17:57	1
PROGRAM FILES/MICROSOFT OFFICE/OFFICE15/OUTLOOK.EXE	2015-03-25 23:41:03	1
INFORMANT/DESKTOP/DOWNLOAD/ERASER 6.2.0.2962.EXE	2015-03-25 23:50:14	1
PROGRAM FILES/ERASER/ERASER.EXE	2015-03-26 00:13:30	2
PROGRAM FILES/CCLEANER/CCLEANER64.EXE	2015-03-26 00:15:50	2
PROGRAM FILES/CCLEANER/UNINST.EXE	2015-03-26 00:18:29	1
PROGRAM FILES (X86)/GOOGLE/DRIVE/GOOGLEDRIVESYNC.EXE	2015-03-26 00:21:31	2
PROGRAM FILES/INTERNET EXPLORER/IEXPLORE.EXE	2015-03-26 00:22:06	2
PROGRAM FILES (X86)/INTERNET EXPLORER/IEXPLORE.EXE	2015-03-26 00:22:07	14
PROGRAM FILES/MICROSOFT OFFICE/OFFICE15/WINWORD.EXE	2015-03-26 00:24:48	3

[표 5-6] 프리패치 기반 프로그램 실행 기록

✓ 안티포렌식 도구를 사용하여 증거인멸을 시도한 흔적을 찾았습니다

5-6) 스티커 메모 내용 확인

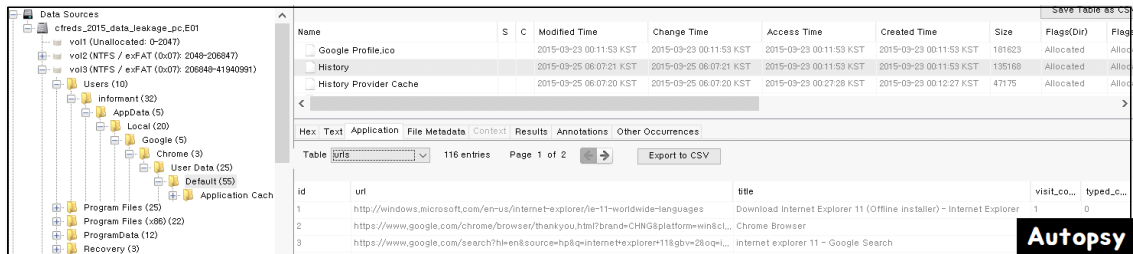
- 프리패치 기록의 가장 첫 번째 실행 목록인 스티커메모에는 “Tomorrow... Everything will be OK...” 문구를 2015-03-25 03:31:59경 작성하였음을 확인할 수 있었습니다.



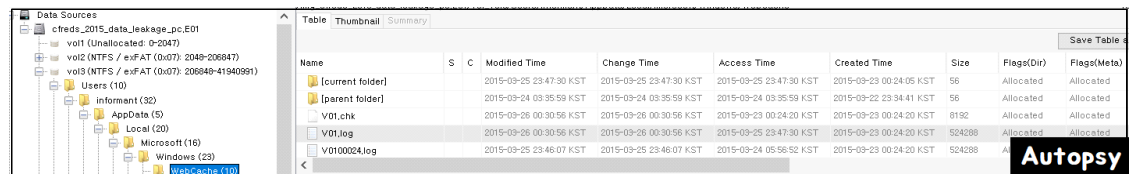
[그림 5-7] 스티커 메모 내용을 확인 한 모습

5-7) 인터넷 사용기록 확인

- 프리패치 기록의 두 번째 실행 목록인 Chrome 브라우저 사용 기록을 확인하는 김에 Internet Explorer 브라우저 사용 기록 또한 함께 확인 해 보기로 하였습니다.



[그림 5-8] Chrome 검색 기록을 확인하는 모습



[그림 5-9] InternetExplorer 로그 파일 추출 위치

검색 내용	검색 내용	검색 내용
outlook 2013 settings	digital forensics	security checkpoint cd-r
emmy noether	how to delete data	anti-forensic tools
data leakage methods	anti-forensics	ccleaner
leaking confidential information	system cleaner	eraser
information leakage cases	how to recover data	file sharing and tethering
intellectual property theft	data recovery tools	Top Stories
how to leak a secret	information leakage cases	external device and forensics
cloud storage	google drive	

[표 5-7] 검색기록

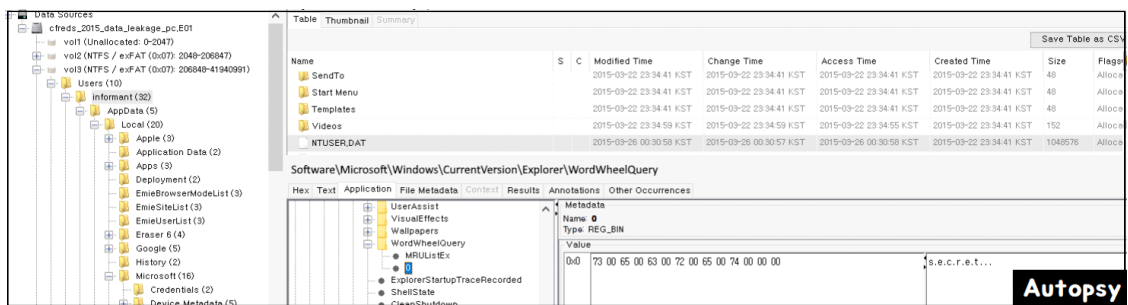
경로	다운로드 완료 시간
C:\Users\Winformant\Downloads\Wicloudsetup.exe	2015-03-24 04:56:53
C:\Users\Winformant\Downloads\Wgoogledrivesync.exe	2015-03-24 04:56:33
C:\Users\Winformant\Desktop\Download\WEraser 6.2.0.2962.exe	2015-03-25 18:47:44
C:\Users\Winformant\Desktop\Download\Wcsetup504.exe	2015-03-25 18:48:30

[표 5-8] 다운로드 기록

✓ 안티포렌식 도구, 클라우드 스토리지 서비스 검색 및 설치 정황을 확인하였습니다

5-8) 윈도우 검색기록 확인

- 프리패치 기록의 세 번째 실행 목록인 윈도우 검색기록 내용을 확인하였습니다.

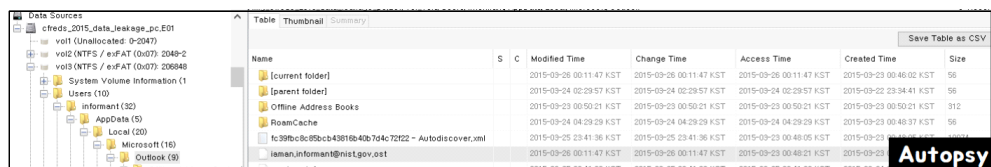


[그림 5-10] secret 단어를 검색 한 모습

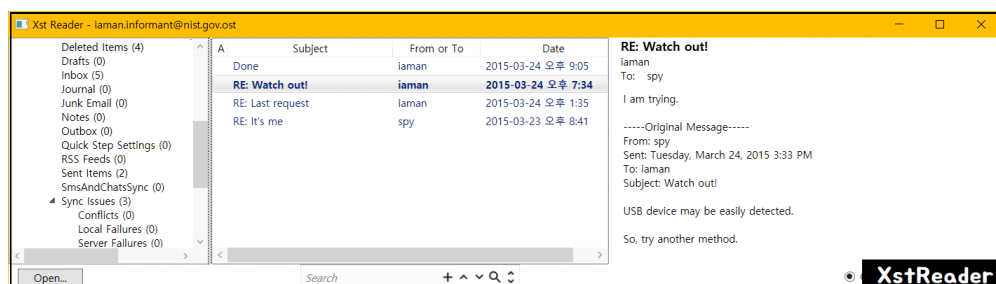
✓ secret 단어가 포함된 파일을 찾는 정황을 확인하였습니다

5-9) 이메일 확인

- 프리패치 기록의 네 번째 실행 목록인 Outlook 전자메일 내용을 확인하였습니다.



[그림 5-11] 이메일 아티팩트를 수집하는 모습



[그림 5-12] 삭제된 메일을 열람한 모습

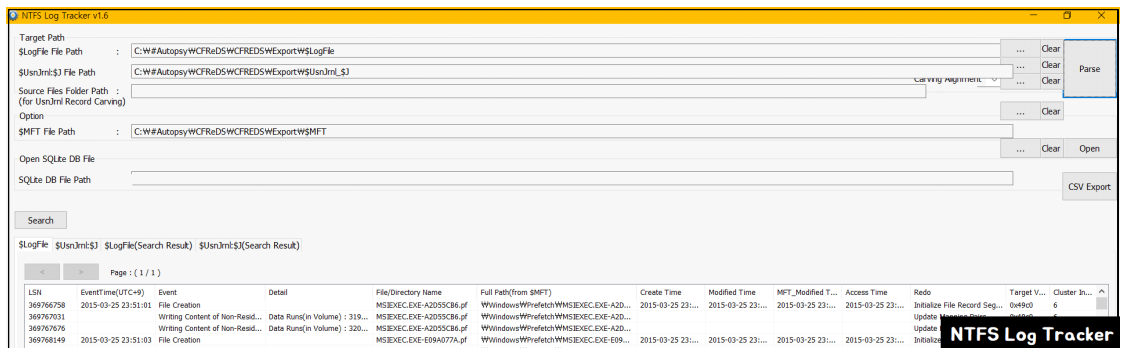
제목	수신자	발신자	생성일(UTC+9)
RE: It's me	iaman.informant@nist.gov	spy.conspirator@nist.gov	2015-03-23 00:41:22
Hello, Iaman	iaman.informant@nist.gov	spy.conspirator@nist.gov	2015-03-23 21:29:29
RE: Hello, Iaman	spy.conspirator@nist.gov	iaman.informant@nist.gov	2015-03-23 22:43:16
Good job, buddy.	iaman.informant@nist.gov	spy.conspirator@nist.gov	2015-03-23 23:15:00
RE: Good job, buddy.	iaman.informant@nist.gov	spy.conspirator@nist.gov	2015-03-23 23:20:41
Important request	iaman.informant@nist.gov	spy.conspirator@nist.gov	2015-03-23 23:26:23
RE: Important request	spy.conspirator@nist.gov	iaman.informant@nist.gov	2015-03-23 23:26:35
RE: Last request	spy.conspirator@nist.gov	iaman.informant@nist.gov	2015-03-24 17:34:47
RE: Watch out!	spy.conspirator@nist.gov	iaman.informant@nist.gov	2015-03-24 23:33:48
Done	spy.conspirator@nist.gov	iaman.informant@nist.gov	2015-03-24 01:03:55
Last request	iaman.informant@nist.gov	spy.conspirator@nist.gov	2015-03-24 17:25:59

[표 5-9] 수집된 전자메일

✓ 이메일을 통한 기술 유출 모의 사실을 확인하였습니다

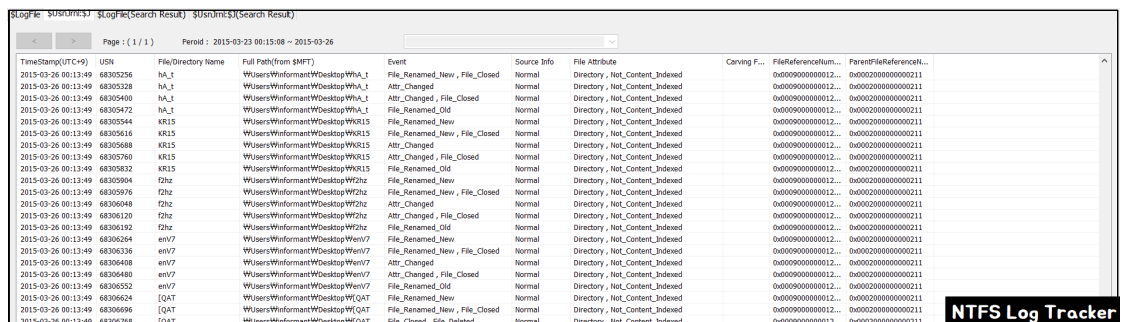
5-10) 안티포렌식 도구 사용기록 확인

- 프리패치 기록의 5, 6, 7, 8 번째 실행 목록인 Eraser와 Ccleaner 사용기록을 알아내기 위하여 W\$Extend\$UsnJrnl\$, WLogFile, WMFT 3가지 파일을 PC 이미지로부터 추출한 다음, NTFS Log Tracker를 통해 파일 시스템 로그를 확인 하였습니다.



[그림 5-13] 파일 시스템 로그를 확인하는 모습

- 2015-03-26 00:13:49경 바탕화면의 temp 디렉터를 이름변경이후 삭제한 흔적을 찾았습니다.

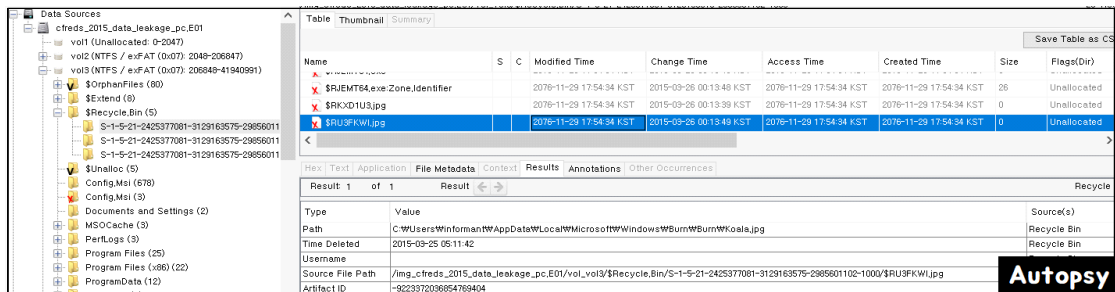


[그림 5-14] 바탕화면의 temp 디렉터를 이름변경 후 삭제하는 모습

✓ 26일, 안티포렌식 도구를 사용하여 바탕화면의 temp 디렉터를 삭제한 흔적을 발견하였습니다

5-11) 휴지통 확인

- 파일시스템 로그를 확인하던 도중, 휴지통 비우기 작업이 실행된 흔적을 확인하였기에 휴지통 내부에 파일이 남아있는지 확인하였습니다.



[그림 5-15] 휴지통을 확인하는 모습

- 휴지통에 남아있는 파일 이름은 Eraser를 이용한 것과 같이 임의성을 띄고 있었으며, 대부분 CD 굽기 작업과 관련된 파일이었습니다.

파일이름	변경시각(UTC+9)	비고
\$140295N	2015-03-25 04:51:47	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\prop
\$155Z163	2015-03-25 04:51:47	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\pd
\$19M7UMY	2015-03-25 04:51:47	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\tr
\$IXWGVWC	2015-03-25 04:51:47	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\prog
\$IDOI3HE.jpg	2015-03-25 05:11:42	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Tulips.jpg
\$IFVCH5V.jpg	2015-03-25 05:11:42	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Penguins.jpg
\$I13FM2A.jpg	2015-03-25 05:11:42	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Desert.jpg
\$1IQGWTT.ini	2015-03-25 05:11:42	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Desktop.ini
\$IKXD1U3.jpg	2015-03-25 05:11:42	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Chrysanthemum.jpg
\$IU3FKWI.jpg	2015-03-25 05:11:42	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Koala.jpg
\$IX538VH.jpg	2015-03-25 05:11:42	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Lighthouse.jpg
\$1508CBB.jpg	2015-03-25 05:11:42	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Hydrangeas.jpg
\$18YP3XK.jpg	2015-03-25 05:11:42	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Jellyfish.jpg
\$R508CBB.jpg	2015-03-26 00:13:39	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Hydrangeas.jpg
\$RI3FM2A.jpg	2015-03-26 00:13:39	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Desert.jpg
\$RKXD1U3.jpg	2015-03-26 00:13:39	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Chrysanthemum.jpg
\$R8YP3XK.jpg	2015-03-26 00:13:48	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Jellyfish.jpg
\$RDOI3HE.jpg	2015-03-26 00:13:49	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Tulips.jpg
\$RFVCH5V.jpg	2015-03-26 00:13:49	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Penguins.jpg
\$RU3FKWI.jpg	2015-03-26 00:13:49	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Koala.jpg
\$RX538VH.jpg	2015-03-26 00:13:49	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Lighthouse.jpg

[표 5-10] 휴지통 속 파일 목록

- 변경시각이 일정한 모습을 통해 적어도 2015-03-25 04:51:47, 2015-03-25 05:11:42, 2015-03-26 00:13:39 3회의 CD 굽기 작업이 있었음을 알 수 있었습니다.

✓ CD 굽기 작업 흔적을 발견하였습니다

5-12) CD 굽기 내역 확인

- 인터넷 사용기록 조사 시 CD 기록용 프로그램에 대한 검색 및 다운로드 내역을 확인 할 수 없었기 때문에, Windows에서 기본으로 제공 해 주는 프로그램을 사용하였음을 짐작할 수 있었습니다.

- 이에 Windows에서 기본적으로 지원하는 isoburn을 사용하였을 가능성이 높아 보였으므로 isoburn 사용 시 AppData/Local/Microsoft/Windows/Burn/Burn 영역에 레코딩 작업에 사용된 임시파일이 남는 특성을 이용하여 해당 디렉터리를 확인 해 보았습니다.

Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
Chrysanthemum.jpg			2015-03-26 05:11:42 KST	2015-03-26 00:13:39 KST	2076-11-29 17:54:34 KST	2076-11-29 17:54:34 KST	0	Unallocated
Desert.jpg			2015-03-26 05:11:42 KST	2015-03-26 00:13:39 KST	2076-11-29 17:54:34 KST	2076-11-29 17:54:34 KST	0	Unallocated
desktop.ini			2015-03-26 05:43:20 KST	2015-03-26 05:43:20 KST	2015-03-26 05:43:20 KST	2015-03-26 05:43:20 KST	174	Allocated
desktop.ini			2015-03-26 05:11:42 KST	2015-03-26 05:11:42 KST	2015-03-26 04:57:20 KST	2015-03-26 04:57:20 KST	174	Unallocated
Hydrangeas.jpg			2015-03-26 05:11:42 KST	2015-03-26 00:13:39 KST	2076-11-29 17:54:34 KST	2076-11-29 17:54:34 KST	0	Unallocated
IE11-Windows6.1-x64-en-us.exe			2015-03-26 05:11:42 KST	2015-03-26 00:13:48 KST	2076-11-29 17:54:34 KST	2076-11-29 17:54:34 KST		
Jellyfish.jpg			2015-03-26 05:11:42 KST	2015-03-26 00:13:48 KST	2076-11-29 17:54:34 KST	2076-11-29 17:54:34 KST		
Koala.jpg			2015-03-26 05:11:42 KST	2015-03-26 00:13:49 KST	2076-11-29 17:54:34 KST	2076-11-29 17:54:34 KST		

[그림 5-16] Burn 디렉터리에 남아있는 CD 굽기 흔적

- CD 굽기 흔적을 통해 2015년 03월 26일 00시 13분 39초부터 49초 까지 작업이 이루어 졌음을 알 수 있었으며, CD-R로 복사된 파일은 아래와 같이 확인되었습니다.

파일이름	변경시각(UTC+9)	파일이름	변경시각(UTC+9)
Chrysanthemum.jpg	2015-03-26 00:13:39	Kolala.jpg	2015-03-26 00:13:49
Desert.jpg	2015-03-26 00:13:39	Lighthouse.jpg	2015-03-26 00:13:49
Hydrangeas.jpg	2015-03-26 00:13:39	Penguins.jpg	2015-03-26 00:13:49
IE11-Windows6.1-x64-en-us.exe	2015-03-26 00:13:48	Tulips.jpg	2015-03-26 00:13:49
Jellyfish.jpg	2015-03-26 00:13:48		

[표 5-11] CD-R로 복사된 항목

✓ isoburn을 이용하여 CD-R에 파일을 복사하였음을 확인하였습니다

5-13) 접근항목 조사

- 프리패치 기록의 9 번째 실행 목록인 GoogleDrive와 함께 연결되어있던 모든 저장장치를 확인 해 보기로 하였으며, 우선 용의자가 실질적으로 관리하였을 저장장치를 추려내기 위하여 쉘백, 링크파일, 섬네일 캐시를 확인하였습니다.

① 쉘백

- Informant가 접근했던 디렉터리 및 파일에 대한 정보를 얻기 위해 쉘백을 확인하였습니다.

Source File	S	C	Path	Key	Data Source
UserClass.dat			My Computer\WE\RM\1\WSecret Project Data	Local Settings\Software\Microsoft\Windows\WS...	cfreds_2015_data_leakage_pc.E01
UserClass.dat			My Computer\WE\RM\1\WSecret Project Data\Wde...	Local Settings\Software\Microsoft\Windows\WS...	cfreds_2015_data_leakage_pc.E01
UserClass.dat			My Computer\WE\Secret Project Data	Local Settings\Software\Microsoft\Windows\WS...	cfreds_2015_data_leakage_pc.E01
UserClass.dat			My Computer\WE\Secret Project Data\Wtechnical r...	Local Settings\Software\Microsoft\Windows\WS...	cfreds_2015_data_leakage_pc.E01
UserClass.dat			My Computer\WE\Secret Project Data\Wproposal	Local Settings\Software\Microsoft\Windows\WS...	cfreds_2015_data_leakage_pc.E01
UserClass.dat			My Computer\WE\Secret Project Data\Wprogress	Local Settings\Software\Microsoft\Windows\WS...	cfreds_2015_data_leakage_pc.E01
UserClass.dat			My Computer\WE\Secret Project Data\Wpricing de...	Local Settings\Software\Microsoft\Windows\WS...	cfreds_2015_data_leakage_pc.E01
UserClass.dat			My Computer\WE\Secret Project Data\Wdesign	Local Settings\Software\Microsoft\Windows\WS...	cfreds_2015_data_leakage_pc.E01

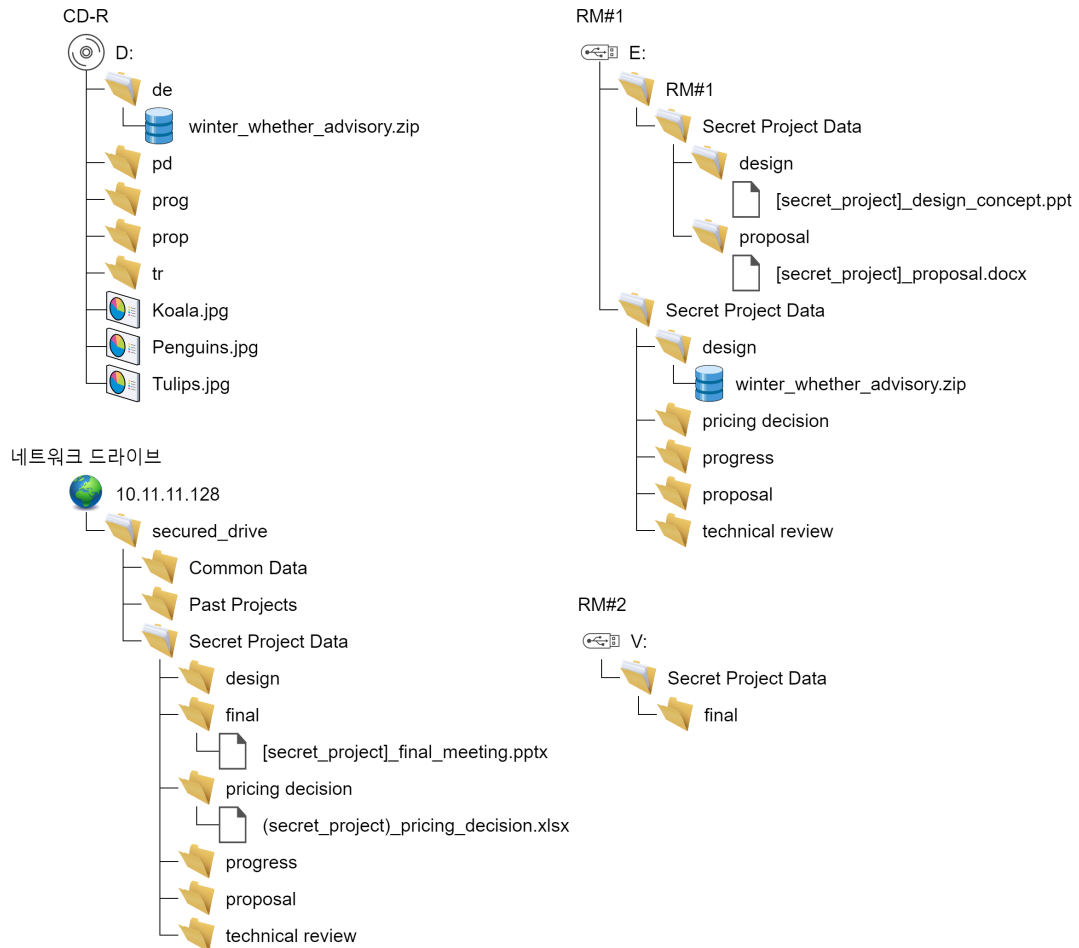
[그림 5-17] Informant가 접근했던 디렉터리 및 파일을 확인하는 모습

② 링크파일

- 링크 파일 목록을 확인하여 최근 실행한 문서의 경로를 수집하였습니다.

Source File	S	C	Path	Date/Time	Data Source
infLink			C:\Windows\inf	2015-03-23 00:57:31 KST	cfreds_2015_data_leakage_pc.f
setupapi.devLink			C:\Windows\WinSxS\setupapi.dev.log	2015-03-23 00:57:30 KST	cfreds_2015_data_leakage_pc.f
(secret_project)_pricing_decision.xlsx.LNK			WW10.11.11.128\WSECURED_DRIVE\Secret Project Data...	2015-03-24 05:26:53 KST	cfreds_2015_data_leakage_pc.f
Desktop.LNK			C:\Users\Winforman\W\Desktop	2015-03-25 03:48:40 KST	cfreds_2015_data_leakage_pc.f
Resignation_Letter_(laman_Informant).docx.LNK			C:\Users\Winforman\W\Desktop\Resignation_Letter_(l...	2015-03-25 03:48:41 KST	cfreds_2015_data_leakage_pc.f
Templates.LNK			C:\Users\Winforman\W\AppData\W\Roaming\Microsoft\W...	2015-03-24 03:36:12 KST	cfreds_2015_data_leakage_pc.f
[secret_project]_design_concept.LNK			E:\WM1\Secret Project Data\W\Design\W[secret_projec...	2015-03-24 03:36:23 KST	cfreds_2015_data_leakage_pc.f
[secret_project]_final_meeting.pptx.LNK			WW10.11.11.128\Wsecured_drive\WSecret Project Data\W...	2015-03-24 05:27:37 KST	cfreds_2015_data_leakage_pc.f
[secret_project]_proposal.LNK			E:\WM1\Secret Project Data\W\Proposal\W[secret_proj...	2015-03-24 03:37:54 KST	cfreds_2015_data_leakage_pc.f
(secret_project)_pricing_decision.xlsx.LNK			WW10.11.11.128\WSECURED_DRIVE\WSecret Project Data...	2015-03-24 05:26:53 KST	cfreds_2015_data_leakage_pc.f

[그림 5-18] 최근 실행된 문서에 대한 LNK파일을 확인 한 모습



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

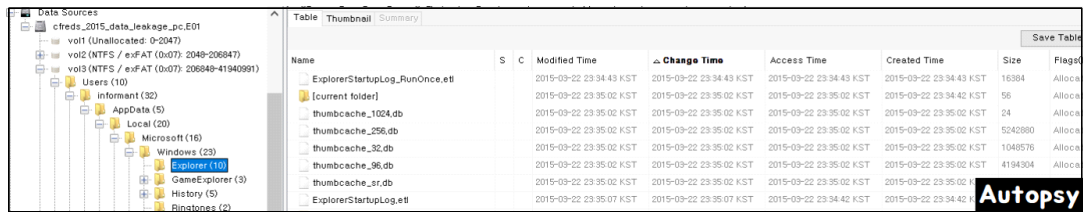
- 추가적으로 바탕화면에서 Resignation_Letter_(laman_Informant).docx 파일을 실행한 흔적을 발견하였으며, 이는 사직서임을 확인하였습니다.

행위	시간(UTC+9)
사직서 파일 생성	2015-03-25 03:48:40
사직서 파일 출력	2015-03-26 00:28:33

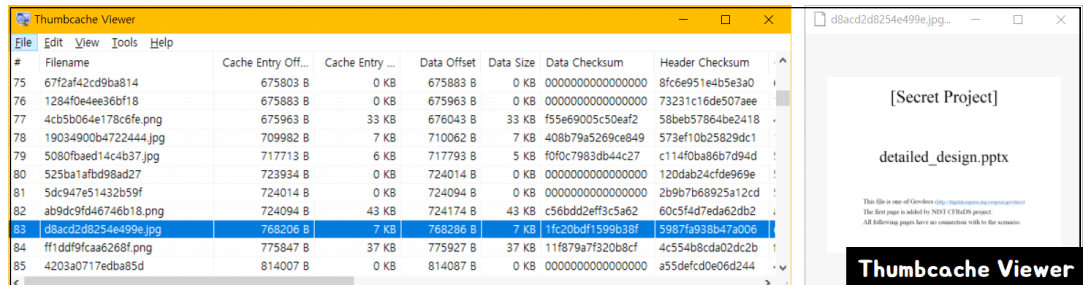
[표 5-12] 사직서에 대한 타임라인

③ 섬네일 캐시

- 셸백 및 링크파일을 통해 각종 기밀자료에 대한 경로는 알아냈지만, 해당 파일이 실제 기밀 문서인지 확실하지 않으므로, PC에 남은 미리보기 이미지를 확인하여 유출 정황을 파악하기로 하였습니다.



[그림 5-20] 미리보기 이미지가 thumbcache 형태로 저장된 모습



[그림 5-21] 기밀문서에 대한 미리보기 이미지가 등록 된 모습

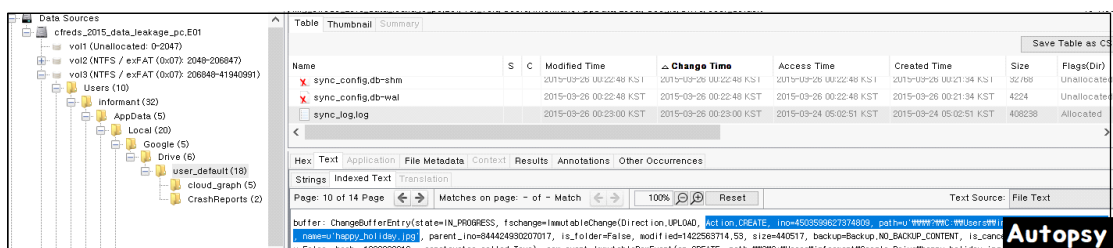
✓ 저장장치에 기밀문서를 복사한 정황을 확인하였습니다

5-14) 기타 저장장치 조사

- 웹백, 다운로드, 인터넷 사용기록 등을 통하여 알아 낸 저장장치 중, 확인하지 못한 구글 드라이브와 볼륨 쉐도우 복사본을 확인하였습니다.

① 구글 드라이브

- 구글 드라이브 로그로부터 사용 기록을 확인하였습니다.
- 사용자 계정 : iaman.informant.personal@gmail.com



[그림 5-22] sync_log.log로부터 동기화 기록을 확인하는 모습

행위	시간(UTC+9)
C:/Users/informant/Google Drive/happy_holiday.jpg 업로드	2015-03-24 01:32:35
C:/Users/informant/Google Drive/do_u_wanna_build_a_snow_man.mp3 업로드	2015-03-24 01:32:35
C:/Users/informant/Google Drive/happy_holiday.jpg 제거	2015-03-24 01:42:17
C:/Users/informant/Google Drive/do_u_wanna_build_a_snow_man.mp3 제거	2015-03-24 01:42:17

[표 5-13] 구글 드라이브 타임라인

② 볼륨 쉐도우 복사본

- 추가적인 단서를 얻기 위해 볼륨 쉐도우 복사본을 확인하였습니다.

Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size
[9b365826-d2ef-11e4-b734-000c29ff2429]{3808876b-c176-4e48-b7ae-04046e6cc752}			2015-03-25 23:57:24 KST	2015-03-25 23:57:24 KST	2015-03-25 23:57:24 KST	2015-03-25 23:57:24 KST	335544
[9b365807-d2ef-11e4-b734-000c29ff2429]{3808876b-c176-4e48-b7ae-04046e6cc752}			2015-03-25 23:57:27 KST	2015-03-25 23:57:27 KST	2015-03-25 23:50:37 KST	2015-03-25 23:50:37 KST	941086
[3808876b-c176-4e48-b7ae-04046e6cc752]			2015-03-25 23:50:37 KST	2015-03-25 23:50:37 KST	2015-03-25 23:50:37 KST	2015-03-25 23:50:37 KST	
tracking.log			2015-03-25 19:16:09 KST	2015-03-25 19:16:09 KST	2015-03-25 19:15:52 KST	2015-03-25 19:15:52 KST	

[그림 5-23] 볼륨 쉐도우 복사본이 기록되어있는 모습

볼륨 쉐도우 복사본	생성 시간(UTC+9)
{9b365826-d2ef-11e4-b734-000c29ff2429}{3808876b-c176-4e48-b7ae-04046e6cc752}	2015-03-25 23:57:24
{9b365807-d2ef-11e4-b734-000c29ff2429}{3808876b-c176-4e48-b7ae-04046e6cc752}	2015-03-25 23:50:37
{3808876b-c176-4e48-b7ae-04046e6cc752}	2015-03-25 23:50:37

[표 5-14] 볼륨 쉐도우 복사본 목록

- 일반적인 방법으로 볼륨 쉐도우 복사본을 열 수 없기에 Arsenal Image Mounter를 이용하여 증거 이미지를 가상 드라이브에 위치시킨 다음, ShadowCopyView를 이용하여 확인하였습니다.

Snapshot Name	Explorer Path	Volume Path	Volume Name	Originating Mach...	Service Machine
WW?WGLOBALROOT#Device#HarddiskVolumeShadowCopy1	WW?Wlocalhost#C\$#@GMT-2021.02...	C:W	WW?WVolume{a96...	GoldBigDragonPC	GoldBigDragonPC
WW?WGLOBALROOT#Device#HarddiskVolumeShadowCopy2	WW?Wlocalhost#C\$#@GMT-2021.02...	C:W	WW?WVolume{a96...	GoldBigDragonPC	GoldBigDragonPC
WW?WGLOBALROOT#Device#HarddiskVolumeShadowCopy3	WW?Wlocalhost#G\$#@GMT-2015.03...	G:W	WW?WVolume{f026...	Informant-PC	Informant-PC

Filename	Modified Time	Created Time	Entry Modifie...	File Size	Attributes	File Extension
run_dir	2015-03-24 오후 10:00	2015-03-24 오후 10:00	2015-03-24 오후 10:00	46	AI	
snapshot.db	2015-03-24 오후 10:00	2015-03-24 오후 10:00	2015-03-24 오후 10:00	20,480	AI	db
sync_config.db	2015-03-24 오후 10:00	2015-03-24 오후 10:00	2015-03-24 오후 10:00			
sync_log.log	2015-03-24 오후 10:00	2015-03-24 오후 10:00	2015-03-24 오후 10:00			

[그림 5-24] 구글 드라이브 스냅 샷이 백업되어있는 모습

- 구글 드라이브 스냅 샷에는 의미 있는 데이터가 남아있지 않았지만, 휴지통 내부에는 구글 드라이브를 통해 업로드 했던 파일과 함께 다양한 기밀 파일을 획득할 수 있었습니다.
- 볼륨 쉐도우 복사본에는 기본적으로 아웃룩 전자메일과 같이 자주 변경되는 데이터를 기록하지 않도록 설정되어있기에, 다른 쓸 만한 데이터는 찾을 수 없었습니다.

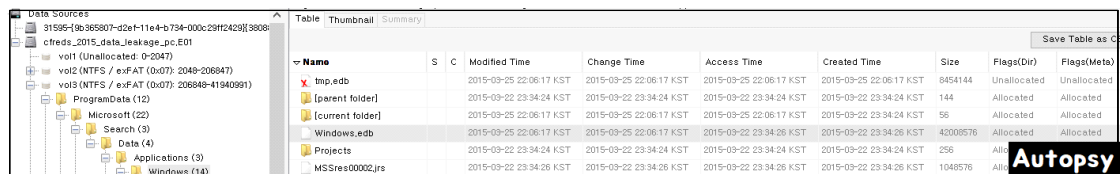
파일 명	올바른 확장자	생성 시간(UTC+9)	주요 내용
\$R9M7UMY/diary_#1d.txt	.docx	2015-03-25 04:46:29	[Secret Project] Technical Review #1.docx
\$R9M7UMY/diary_#1p.txt	.pptx	2015-03-25 04:46:29	[Secret Project] Technical Review #1.pptx
\$R9M7UMY/diary_#2d.txt	.docx	2015-03-25 04:46:29	[Secret Project] Technical Review #2.docx
\$R9M7UMY/diary_#2p.txt	.ppt	2015-03-25 04:46:29	[Secret Project] Technical Review #2.ppt
\$R9M7UMY/diary_#3d.txt	.doc	2015-03-25 04:46:29	[Secret Project] Technical Review #3.doc
\$R9M7UMY/diary_#3p.txt	.ppt	2015-03-25 04:46:29	[Secret Project] Technical Review #3.ppt
\$R55Z163/my_favorite_cars.db	.xls	2015-03-25 04:46:23	[Secret Project] price_analysis_#2.xls
\$R55Z163/my_favorite_movies.7z	.xlsx	2015-03-25 04:46:23	[Secret Project] price_analysis_#1.xlsx
\$R55Z163/new_years_day.jpg	.xlsx	2015-03-25 04:46:23	[Secret Project] market_analysis.xlsx
\$R55Z163/super_bowl.avi	.xls	2015-03-25 04:46:25	[Secret Project] market_shares.xls
\$R40295N/a_gift_from_you.gif	.docx	2015-03-25 04:46:27	[Secret Project] Detailed Proposal.docx
\$R40295N/landscape.png	.docx	2015-03-25 04:46:29	[Secret Project] Proposal.docx
\$RT12FO0/winter_storm.amr	.ppt	2015-03-25 04:46:16	[Secret Project] revised_points.ppt
\$RT12FO0/winter_whether_advisory.zip	.pptx	2015-03-25 04:46:19	[Secret Project] detailed_design.pptx
\$RXWGVWC/my_friends.svg	.ppt	2015-03-25 04:46:27	[Secret Project]
\$RXWGVWC/my_smartphone.png	.docx	2015-03-25 04:46:26	[Secret Project] Progress #1.docx
\$RXWGVWC/new_year_calendar.one	.docx	2015-03-25 04:46:26	[Secret Project] Progress #2.docx

[표 5-15] 볼륨 쉐도우 복사본 휴지통에서 수집된 기밀문서

√ 기밀문서의 확장자를 변경하여 복사한 정황을 확인하였습니다

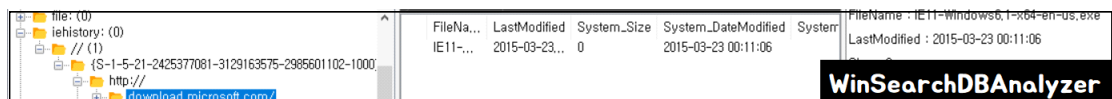
5-15) 윈도우 검색 및 색인 기록 확인

- Windows 색인 기능을 활성화 하여 인덱싱 되어있을 경우, 해당 파일의 내용까지 남아있는 점을 이용하여 기밀문서 유출 정황을 더 확보하고자 하였습니다.



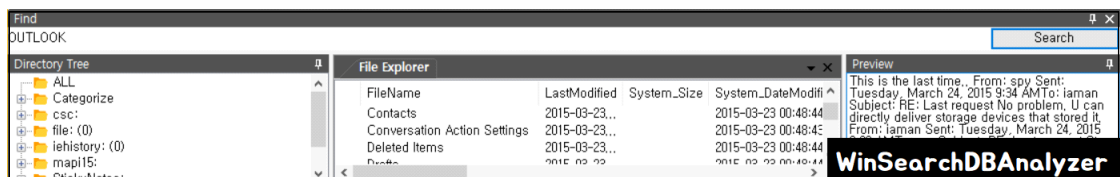
Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)
tmp.edb			2015-03-25 22:06:17 KST	2015-03-25 22:06:17 KST	2015-03-25 22:06:17 KST	2015-03-25 22:06:17 KST	8454144	Unallocated	Unallocated
[parent folder]			2015-03-22 23:34:24 KST	2015-03-22 23:34:24 KST	2015-03-22 23:34:24 KST	2015-03-22 23:34:24 KST	144	Allocated	Allocated
[current folder]			2015-03-25 22:06:17 KST	2015-03-25 22:06:17 KST	2015-03-25 22:06:17 KST	2015-03-25 22:06:17 KST	56	Allocated	Allocated
Windows.edb			2015-03-25 22:06:17 KST	2015-03-25 22:06:17 KST	2015-03-22 23:34:26 KST	2015-03-22 23:34:26 KST	42008576	Allocated	Allocated
Projects			2015-03-22 23:34:24 KST	2015-03-22 23:34:24 KST	2015-03-22 23:34:24 KST	2015-03-22 23:34:24 KST	256	Allocated	Allocated
MSRes00002.jre			2015-03-22 23:34:26 KST	2015-03-22 23:34:26 KST	2015-03-22 23:34:26 KST	2015-03-22 23:34:26 KST	1048576	Allocated	Allocated

[그림 5-25] 색인 정보가 저장된 파일을 확보한 모습



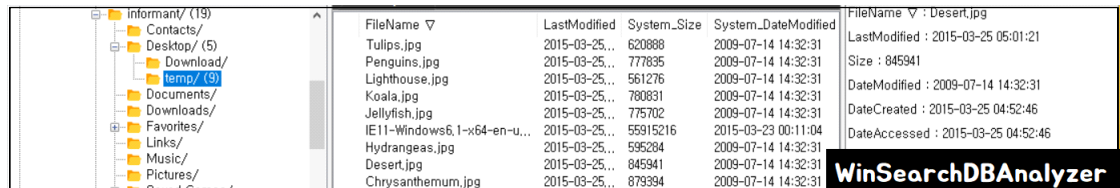
File Name	Last Modified	System Size	System Date Modified	System Date Accessed	File Name
IE11-...	2015-03-23...	0	2015-03-23 00:11:06		IE11-Windows6.1-x64-en-us.exe

[그림 5-26] 인터넷 사용 내역



File Name	Last Modified	System Size	System Date Modified	System Date Accessed
Contacts	2015-03-23...		2015-03-23 00:48:44	
Conversation Action Settings	2015-03-23...		2015-03-23 00:48:44	
Deleted Items	2015-03-23...		2015-03-23 00:48:44	

[그림 5-27] 주고받은 이메일 내역



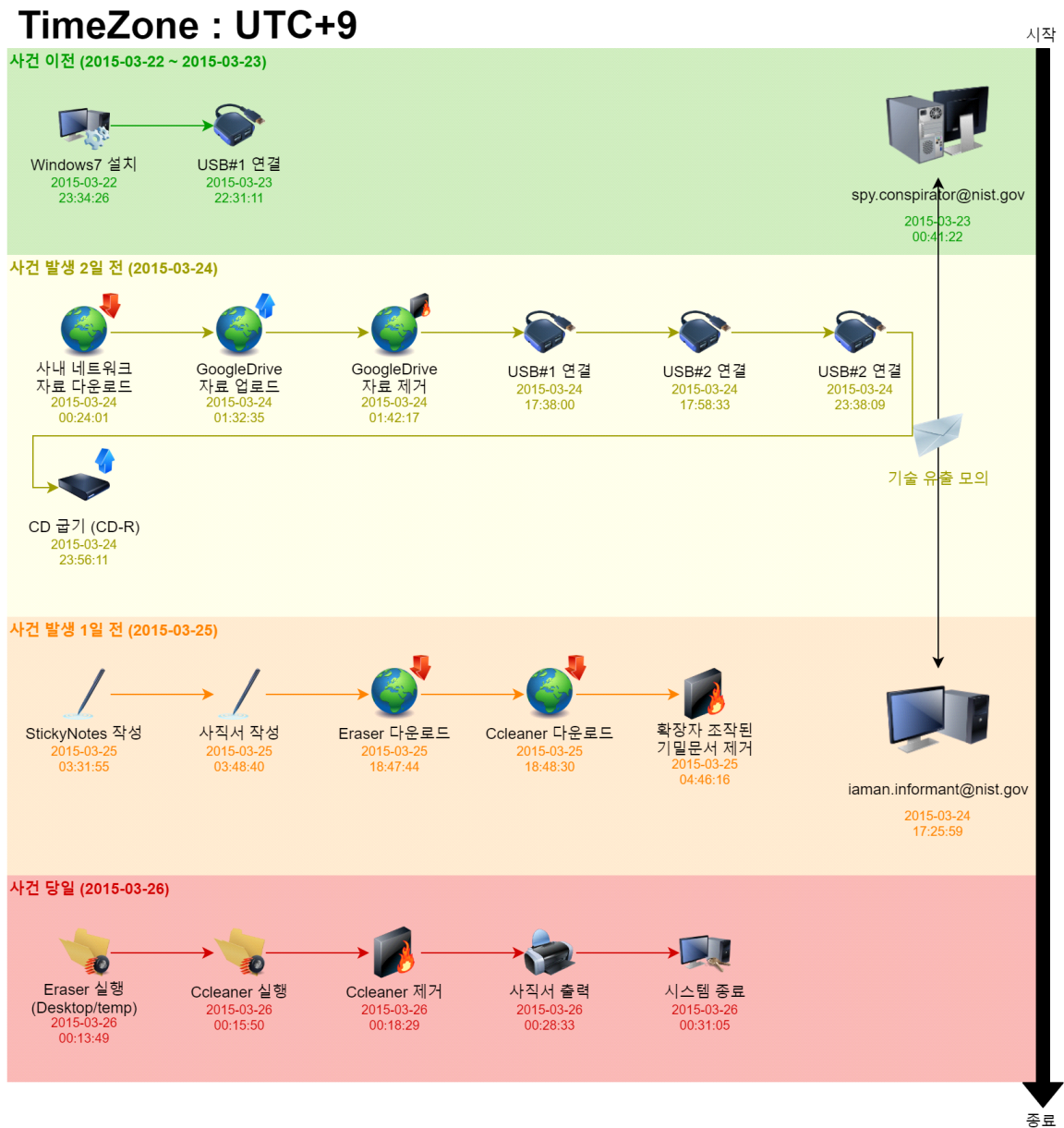
File Name	Last Modified	System Size	System Date Modified	System Date Accessed
Tulips.jpg	2015-03-25...	620888	2009-07-14 14:32:31	
Penguins.jpg	2015-03-25...	777835	2009-07-14 14:32:31	
Lighthouse.jpg	2015-03-25...	561276	2009-07-14 14:32:31	
Koala.jpg	2015-03-25...	780831	2009-07-14 14:32:31	
Jellyfish.jpg	2015-03-25...	775702	2009-07-14 14:32:31	
IE11-Windows6.1-x64-en-u...	2015-03-25...	55915216	2015-03-23 00:11:04	
Hydrangeas.jpg	2015-03-25...	595284	2009-07-14 14:32:31	
Desert.jpg	2015-03-25...	845941	2009-07-14 14:32:31	
Chrysanthemum.jpg	2015-03-25...	879394	2009-07-14 14:32:31	

[그림 5-28] Eraser를 통해 삭제했었던 temp 디렉터리에 대한 기록이 발견된 모습

√ 바탕화면의 temp 디렉터리에는 사진과 IE 11 설치파일이 존재하였음을 확인하였습니다

6. 종합 의견

6-1) 전체 타임라인



6-2) 분석 결과

- Informant의 기밀문서 유출모의 내역과, CD-R, USB 저장장치에 확장자가 변조된 기밀문서를 복사하고, 안티포렌식 도구를 사용하여 증거 인멸 이후, 기밀문서를 회사 밖으로 반출하려던 정황을 확인하였습니다.

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

7. 부록

7-1) CFReDS 문제 대응

1. 각 이미지의 해시 값을 확인하고 검증하시오.
= 5장 5-1) 이미지 무결성 검증
2. PC 이미지의 파티션 정보를 확인하시오.
= 5장 5-2) 파티션 정보 확인
3. 설치된 OS 정보는 무엇인가요? (설치 날짜, OS 이름, 등록된 소유자/조직, ...)
= 5장 5-3) 시스템 정보 확인
4. 시간대 정보는 무엇인가요?
= 5장 5-3) 시스템 정보 확인
5. 컴퓨터 이름은 무엇인가요?
= 5장 5-3) 시스템 정보 확인
6. 모든 계정의 상세 정보를 나열하시오. (계정명, 로그인 횟수, 마지막 로그인 시각 등)
= 5장 5-4) 계정 정보 확인
7. 마지막으로 로그인한 사용자는 누구인가요?
= 5장 5-4) 계정 정보 확인
8. 마지막 시스템 종료 시각은 언제인가요?
= 5장 5-3) 시스템 정보 확인
9. DHCP에 할당된 IP 주소는 무엇인가요?
= 5장 5-3) 시스템 정보 확인
10. OS 설치 후 용의자가 설치한 프로그램은 무엇인가요?
= 5장 5-5) 프로그램 사용 흔적 확인
11. 응용프로그램 실행 로그를 나열하시오. (실행 경로, 실행 시간, 실행 횟수 등)
= 5장 5-5) 프로그램 사용 흔적 확인
12. 시스템 시작/종료, 로그인/로그오프 기록을 나열하시오.
= 5장 5-3) 시스템 정보 확인, 5장 5-3) 계정 정보 확인
13. 사용된 웹브라우저는 무엇인가요?
= 5장 5-5) 프로그램 사용 흔적 확인
14. 웹브라우저 기록과 관련한 디렉터리/파일 경로를 나열하시오.
= 5장 5-7) 인터넷 사용기록 확인
15. 용의자가 접근한 웹 사이트를 나열하시오.
= 5장 5-7) 인터넷 사용기록 확인
16. 웹브라우저를 사용해 검색한 모든 키워드를 나열하시오.
= 5장 5-7) 인터넷 사용기록 확인
17. 윈도우 탐색기 검색 창에 타이핑한 모든 검색 키워드를 나열하시오.
= 5장 5-8) 윈도우 검색기록 확인
18. 전자 메일 통신에 사용된 응용프로그램은 무엇인가요?
= 5장 5-9) 이메일 확인
19. 전자 메일 파일의 모든 위치를 나열하시오.
= 5장 5-9) 이메일 확인
20. 용의자의 전자 메일 계정은 무엇인가요?
= 5장 5-9) 이메일 확인
21. 용의자의 모든 전자 메일을 나열하시오. 가능한 삭제된 전자메일을 식별하시오.

- = 5장 5-9) 이메일 확인
- 22. 시스템에 연결된 모든 외장저장장치를 나열하십시오.
- = 5장 5-13) 접근항목 조사
- 23. 바탕화면 폴더에서 '이름 바꾸기'와 관련한 모든 흔적을 식별하십시오.
- = 5장 5-10) 안티포렌식 도구 사용기록 확인
- 24. 회사의 공유 네트워크 드라이브의 IP 주소는 무엇인가요?
- = 5장 5-13) 접근항목 조사
- 25. 'RM #2'에서 탐색된 모든 디렉토리를 나열하십시오.
- = 5장 5-13) 접근항목 조사
- 26. 'RM #2'에서 열어본 모든 파일을 나열하십시오.
- = 5장 5-13) 접근항목 조사
- 27. 회사 네트워크 드라이브에서 탐색된 모든 디렉토리를 나열하십시오.
- = 5장 5-13) 접근항목 조사
- 28. 회사 네트워크 드라이브를 통해 열어본 모든 파일을 나열하십시오.
- = 5장 5-13) 접근항목 조사
- 29. 시스템에서 클라우드 서비스와 관련된 흔적을 찾으시오. (서비스 이름, 로그 파일 등)
- = 5장 5-13) 접근항목 조사, 5-14) 저장장치 확인
- 30. 구글 드라이브에서 삭제된 파일은 무엇인가요? 파일명과 수정 시간을 찾으시오.
- = 5-14) 저장장치 확인
- 31. 구글 드라이브 동기화를 위한 계정은 무엇인가요?
- = 5-14) 저장장치 확인
- 32. CD-R 굽기에 사용된 방법(또는 소프트웨어)는 무엇인가요?
- = 5장 5-12) CD 굽기 내역 확인
- 33. 용의자는 언제 CD-R를 레코딩 하였나요?
- = 5장 5-12) CD 굽기 내역 확인
- 34. 시스템에서 CD-R로 복사된 파일은 무엇인가요?
- = 5장 5-12) CD 굽기 내역 확인
- 35. CD-R에서 열어본 파일은 무엇인가요?
- = 5장 5-13) 접근항목 조사, 4장 4-2) 삭제된 파일 복구 및 채증
- 36. 바탕화면의 '사직서'와 관련한 모든 타임스탬프를 조사하라.
- = 5장 5-13) 접근항목 조사
- 37. 용의자가 언제 사직서를 인쇄했나요?
- = 5장 5-13) 접근항목 조사
- 38. Thumbcache 파일의 위치는 어디인가요?
- = 5장 5-13) 접근항목 조사
- 39. Thumbcache에 저장된 기밀 파일의 흔적을 찾으시오.
- = 5장 5-13) 접근항목 조사
- 40. 스티커 메모 파일의 위치는 어디인가요?
- = 5장 5-6) 스티커 메모 내용 확인
- 41. 스티커 메모 파일에 저장된 메모를 확인하십시오.
- = 5장 5-6) 스티커 메모 내용 확인
- 42. 윈도우 '검색 및 색인' 기능이 활성화되어 있나요? 'Windows Search' 색인 데이터베이스의 위치는 어디인가요?
- = 5장 5-15) 윈도우 검색 및 색인 기록 확인
- 43. Windows Search 데이터베이스에 저장된 데이터는 무엇인가요?

- = 5장 5-15) 윈도우 검색 및 색인 기록 확인
- 44. Windows Search 데이터베이스에서 Internet Explorer 사용량과 관련한 흔적을 찾으시오.
- = 5장 5-15) 윈도우 검색 및 색인 기록 확인
- 45. Windows Search 데이터베이스에 저장된 전자메일 통신 흔적을 나열하시오.
- = 5장 5-15) 윈도우 검색 및 색인 기록 확인
- 46. Windows Search 데이터베이스에 저장된 윈도우 바탕화면과 관련된 파일과 디렉터리 흔적을 나열하시오.
- = 5장 5-15) 윈도우 검색 및 색인 기록 확인
- 47. 볼륨 새도 복사본의 위치와 각 복사본의 생성 시각은 무엇인가요?
- = 5장 5-12) 저장장치 확인
- 48. 볼륨 새도 복사본에서 구글 드라이브 서비스와 관련한 흔적을 찾으시오.
- = 5장 5-12) 저장장치 확인
- 49. 구글 드라이브에서 삭제된 파일은 무엇인가요? VSC 내 snapshot.db의 cloud_entry 테이블에서 삭제된 레코드를 찾으시오.
- = 5장 5-12) 저장장치 확인
- 50. VSC에서 아웃룩 전자메일 데이터를 찾을 수 없는 이유는 무엇인가요?
- = 5장 5-12) 저장장치 확인
- 51. 시스템의 휴지통을 조사하시오.
- = 5장 5-11) 휴지통 확인
- 52. 마지막 날인 '2015-03-26'에 시스템에 행해진 안티포렌식 행위는 무엇인가요?
- = 5-10) 안티포렌식 도구 사용기록 확인
- 53. 'RM #2'에서 삭제된 파일을 복구하시오.
- = 3장 3-2) 삭제된 파일 복구 및 채증
- 54. 'RM #2'에 행해진 안티포렌식 행위는 무엇인가요?
- = 3장 3-2) 삭제된 파일 복구 및 채증
- 55. 시스템에서 'RM #2'로 복사된 파일은 무엇인가요?
- = 3장 3-2) 삭제된 파일 복구 및 채증
- 56. CD-R 'RM #3'에 숨겨진 파일을 복구하시오.
- = 4장 4-2) 삭제된 파일 복구 및 채증
- 57. CD-R 'RM #3'에 행해진 안티포렌식 행위는 무엇인가요?
- = 4장 4-2) 삭제된 파일 복구 및 채증
- 58. 데이터 유출 타임라인을 구성하시오.
- = 6장 6-1) 전체 타임라인
- 59. 용의자가 수행한 데이터 유출 방법을 열거하고 설명하시오.
- = 6장 6-1) 전체 타임라인, 6장 6-2) 분석 결과
- 60. 결과 요약에 대한 시각적 다이어그램을 만드시오.
- = 6장 6-1) 전체 타임라인