

화이트햇 스쿨 2단계 팀 프로젝트 보고서

차세대 보안리더 양성 프로그램

한국정보기술연구원 BoB 교육센터

멘토명 / PL명	문헌지/심주완	팀 명	포렌식빵
프로젝트 주제	윈도우 악성 프로그램 탐지 및 분석	회차	1회차
팀원	정지윤(PM) , 강지민, 김신아, 김예은, 배영혜, 서연정, 안서진, 전소현		
추진현황	<p>목차</p> <p>1. 툴 매뉴얼 분석</p> <p>2. 툴 비교 표</p> <p>3. 논문 요약 분석</p>		

1. 툴 매뉴얼 분석

이번 프로젝트에서는 총 18개의 디지털 포렌식 및 분석 툴을 분석하였습니다. 각 툴의 사용 목적과 주요기능을 정리하였으며, 분석 대상 툴 목록은 다음과 같습니다.

Registry Explorer: 정지윤

Hashcat: 정지윤

DCode: 정지윤

MailView: 강지민

EventLog Explorer: 강지민

HxD: 김신아

PDFStreamDumper: 김신아

NTFSLogTracker: 김신아

FTK Imager: 김예은

WinMerge: 김예은

ChromeCacheView: 김예은

Volatility: 배영혜

Wireshark: 배영혜

Autopsy: 서연정

KAPE: 안서진

WinPrefetchView: 안서진

DB Browser: 전소현

JumpListExplorer: 전소현

총 18개의 디지털 포렌식 툴을 분석한 뒤 매뉴얼을 작성하였고 그중 **FTK Imager**, **MailView**, **WinPrefetchView**, **JumpListExplorer** 의 매뉴얼을 보고서에 포함하였습니다.

[FTK Imager] 매뉴얼

1. 툴 기본 정보

항목	내용
툴 이름	FTK Imager
분석 카테고리	시스템 설치/실행 아티팩트, 메모리 아티팩트, 파일 사용/조작 아티팩트
사용 버전	4.7
다운로드 경로	E-Discovery - Thank you
지원 포맷	E01, DD/RAW, NTFS 등

2. 툴 소개 및 목적

- 도구 설명 및 목적 (2~3줄)

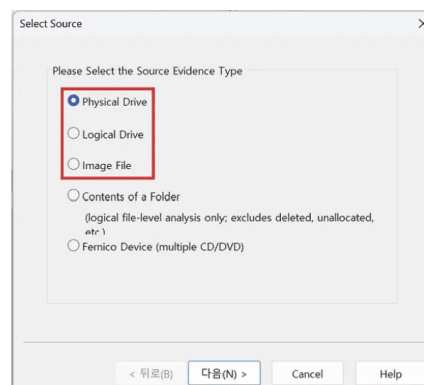
FTK Imager는 디스크 이미징, 데이터 수집, 무결성 검증을 수행한다. 디스크, 메모리 덤프, 이메일 등 다양한 포맷을 지원하며, 수집된 증거를 다른 포렌식 분석 도구와 연계하여 활용할 수 있다.

3. 주요 기능 및 사용법

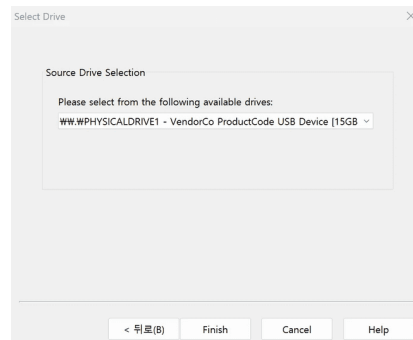
- 초기 화면엔 Evidence Tredd, Properties, File List, Viewer가 존재한다

기능 1: 디스크 이미지 덤프하기

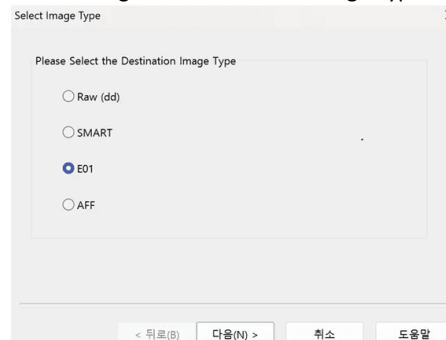
File → Create Disk Image → Select Source → 이미징 할 타입 선택 → 다음



Select Drive Selection : 원하는 드라이브 선택



Create Image → Add → Select Image Type



Raw(dd) : 원본과 동일한 이미징 (압축 x)

SMART : 리눅스 운영체제 이미징

E01 : 압축 이미징

AFF : 대용량 디스크 이미징

Evidence Item information

Evidence Item Information

Case Number: WHS_Project

Evidence Number: 001

Unique Description:

Examiner: kimyeeun

Notes:

< 뒤로(B) 다음(N) > Cancel Help

Select Image Destination → finish → start

Select Image Destination

Image Destination Folder
C:\Users\User\Desktop Browse

Image Filename (Excluding Extension)
WHS_Project

Image Fragment Size (MB) 0
For Raw, E01, and AFF formats: 0 = do not fragment

Compression (0=None, 1=Fastest, ..., 9=Smallest) 6

Use AD Encryption ☐

< 뒤로(B) Finish Cancel Help

Image Fragment Size : MB를 기준으로 이미지 파일 분할저장 (0 = 분할 저장 안함 <권장됨)

Compression : 압축률 (E01의 기본값 6, Raw(dd)선택시 0 고정)

끝나면 해시값이 뜨는데 이 해시값을 통해 무결성을 입증한다.

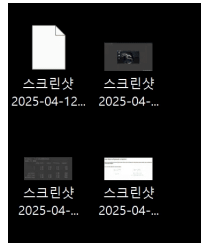
기능 2: 삭제 파일 복구하기

File → Add Evidence Item → root 로 들어가면 삭제한 파일들을 전부 볼 수 있다.

Evidence Tree	File List																																												
<ul style="list-style-type: none">WHS_Project E01<ul style="list-style-type: none">Partition 1 [14999MB]<ul style="list-style-type: none">NONAME [NTFS]<ul style="list-style-type: none">orphan<ul style="list-style-type: none">root<ul style="list-style-type: none">\$BadClus\$Extend\$Secure\$UpCaseSystem Volume Information<ul style="list-style-type: none">기밀회의의.pdf[unallocated space]Unpartitioned Space [basic disk]	<table><thead><tr><th>Name</th><th>Size</th><th>Type</th><th>Date Modif.</th></tr></thead><tbody><tr><td>\$UpCase</td><td>131,07...</td><td>Regul...</td><td>2025-04-0...</td></tr><tr><td>\$Volume</td><td>0 (0 KB)</td><td>Regul...</td><td>2025-04-0...</td></tr><tr><td>기밀_재판회의.pdf</td><td>322,61...</td><td>Regul...</td><td>2025-04-0...</td></tr><tr><td>기밀_재판회의.pdf</td><td>969 (1 File)</td><td>SI...</td><td></td></tr><tr><td>보고자료.docx</td><td>13,896...</td><td>Regul...</td><td>2025-04-0...</td></tr><tr><td>보고자료.docx.FileS...</td><td>2,486...</td><td>File SI...</td><td></td></tr><tr><td>스크린샷 2025-04-...</td><td>745,41...</td><td>Regul...</td><td>2025-04-1...</td></tr><tr><td>스크린샷 2025-04-...</td><td>70,239...</td><td>Regul...</td><td>2025-04-1...</td></tr><tr><td>스크린샷 2025-04-...</td><td>\$130 I...</td><td></td><td></td></tr><tr><td>스크린샷 2025-04-...</td><td>6,421 (... Regul...</td><td></td><td>2025-04-1...</td></tr></tbody></table>	Name	Size	Type	Date Modif.	\$UpCase	131,07...	Regul...	2025-04-0...	\$Volume	0 (0 KB)	Regul...	2025-04-0...	기밀_재판회의.pdf	322,61...	Regul...	2025-04-0...	기밀_재판회의.pdf	969 (1 File)	SI...		보고자료.docx	13,896...	Regul...	2025-04-0...	보고자료.docx.FileS...	2,486...	File SI...		스크린샷 2025-04-...	745,41...	Regul...	2025-04-1...	스크린샷 2025-04-...	70,239...	Regul...	2025-04-1...	스크린샷 2025-04-...	\$130 I...			스크린샷 2025-04-...	6,421 (... Regul...		2025-04-1...
Name	Size	Type	Date Modif.																																										
\$UpCase	131,07...	Regul...	2025-04-0...																																										
\$Volume	0 (0 KB)	Regul...	2025-04-0...																																										
기밀_재판회의.pdf	322,61...	Regul...	2025-04-0...																																										
기밀_재판회의.pdf	969 (1 File)	SI...																																											
보고자료.docx	13,896...	Regul...	2025-04-0...																																										
보고자료.docx.FileS...	2,486...	File SI...																																											
스크린샷 2025-04-...	745,41...	Regul...	2025-04-1...																																										
스크린샷 2025-04-...	70,239...	Regul...	2025-04-1...																																										
스크린샷 2025-04-...	\$130 I...																																												
스크린샷 2025-04-...	6,421 (... Regul...		2025-04-1...																																										

복구할 파일을 선택하고 우클릭으로 Export Files를 클릭하면 파일을 복구할 위치가 뜬다.

바탕화면으로 지정하고 추출해냈다.



바탕화면에서 정상적으로 추출된 걸 확인할 수 있다.

기능 3: 이미지 마운팅

File → Image Mounting → Mount

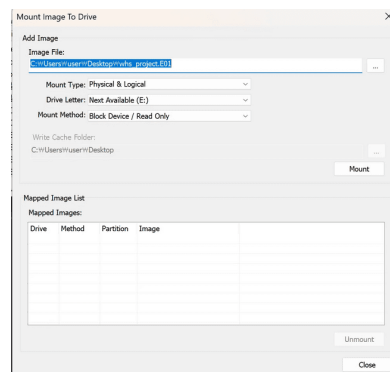
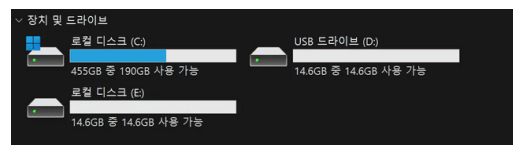


Image File : 마운팅 할 이미지 파일 선택

Mount Type : 마운트 하고자 하는 대상의 범위 선택

Drive Letter : 드라이브 철자 선택

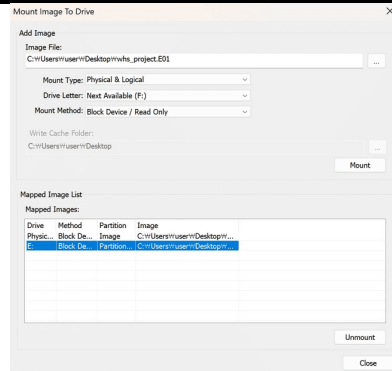
Mount Method : 마운트 된 이미지의 접근 및 조작 가능성 선택



위와 같이 마운트 된 모습을 확인해볼 수 있다.

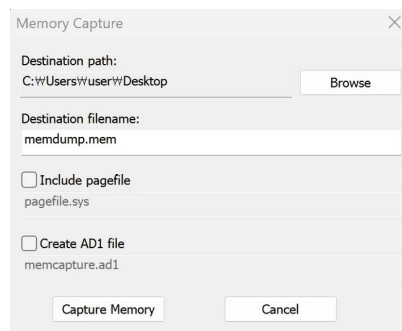
마운트 해제방법

Mapped Images → 마운트 해제할 드라이브 선택 → Unmount



기능 4: 메모리 덤프


File → Capture memory



Include pagefile : pagefiles.sys 덤프 여부

Create AD1 file : AD1 file 생성 여부 → 덤프 시 전체 또는 부분적인 이미지를 저장하여 분석 과정에서 원본 데이터가 변경되거나 손상되는 것을 방지하며 해시값으로 무결성을 입증한다.

Result

 memdump.mem

 pagefile.sys

기능 5: 파일 및 파일 해시 추출

Evidence Tree → 추출하고자하는 파일 우클릭 → Export File Hash List



바탕화면에 hash라는 이름으로 저장이 된 걸 확인 할 수 있다.

파일을 열어보면

	A	B	C	D	E	F	G	H	I
1	MD5	SHA1	FileNames						
2	1f801bac9f4631eceb	test.vhd	Partition 1 [497MB]	W새 볼륨 [NTFS]	W[root]	Wtest.txt			
3	0c0418271e7367347	test.vhd	Partition 1 [497MB]	W새 볼륨 [NTFS]	W[root]	Wtest.txt	W\$EFS		

이런식으로 뜯다

(컴퓨터 오류로 생성한 hash 파일이 열리지 않아 다른 파일을 참고했다.)

[MailView] 매뉴얼

1. 툴 기본 정보

항목	내용
툴 이름	MailView
분석 카테고리	파일 사용/조작 아티팩트 (이메일 아티팩트 분석)
사용 버전	2.5.1.0
다운로드 경로	https://www.mitec.cz/mailview.html
지원 포맷	.pst, .ost, .mbx, .eml 등 다양한 이메일 저장 포맷 지원

2. 툴 소개 및 목적

MailView는 이메일 파일(.pst, .eml 등)을 분석하여 메일 본문, 송수신자 정보, 첨부파일 목록, 날짜 등의 메타데이터를 추출하는 포렌식 도구이다.

디지털 포렌식에서 이메일 기반의 커뮤니케이션 내역을 확인하고, 사용자 활동을 분석하는 데 활용된다.

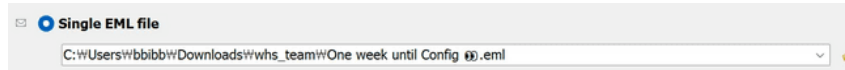
3. 주요 기능 및 사용법

기능 1: 다양한 이메일 포맷 열람

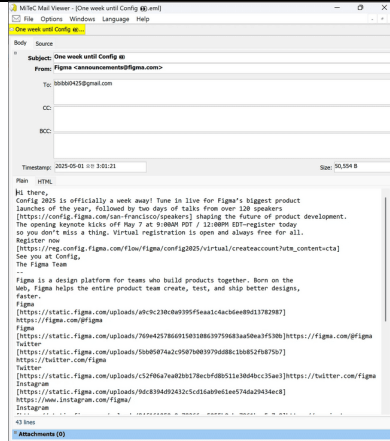
.eml, .dbx, .mbx 등 여러 이메일 포맷을 불러와 메일 목록을 확인할 수 있음.

.eml 파일을 열어 받은 메일 목록 확인 → 제목, 발신자, 날짜 등 기본 정보 분석

첫 화면에서 Single EML file 또는 Outlook Express message database 선택



샘플 파일 선택 → OK



파일명: test_email.eml (좌측 상단에 정상 표시됨)

제목(Subject): Sample EML File

발신자(From): test@example.com

수신자(To): user@example.com

타임스탬프: 2025-05-12 오전 10:00:00

본문 탭(Plain / HTML): Plain 탭에서 본문 정상 출력됨

첨부파일: Attachments (0) → 현재 첨부 없음 표시도 정상

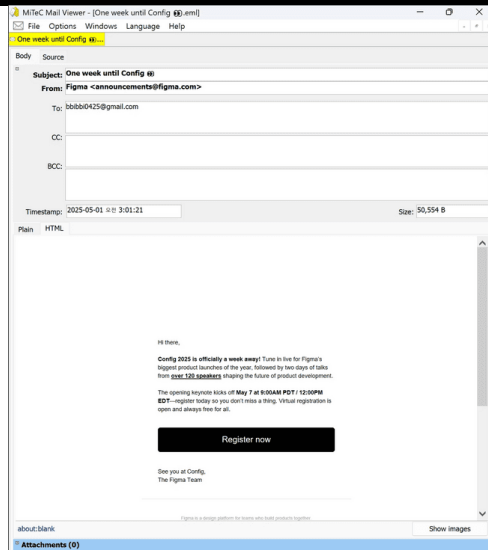
기능 2: 메일 본문 및 HTML 미리보기

선택한 메일의 본문 내용을 텍스트와 HTML 형식으로 확인 가능.

특정 메일 클릭 → 하단에서 HTML 본문 확인 → 링크, 이미지 포함 여부 분석

하단 영역 HTML 탭 활성화 (클릭)

Plain HTML

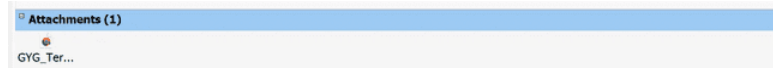


본문 탭(Plain / HTML): HTML 탭에서 시각적 본문 정상 출력됨

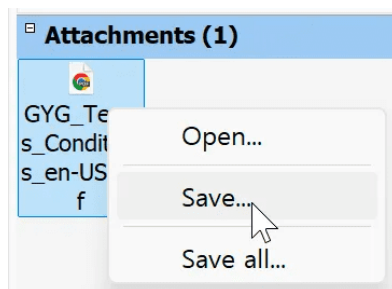
기능 3: 첨부파일 추출 및 저장

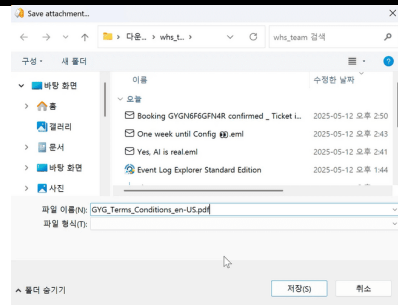
메일에 포함된 첨부파일을 확인하고 개별 또는 일괄 저장 가능.

첨부파일이 포함된 메일 선택 -> 아래쪽 또는 별도 탭에서 Attachments 확인



해당 파일 우클릭 -> save



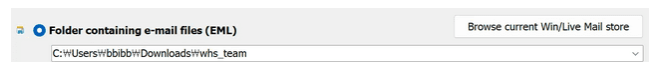


GYG_Terms_Conditions_en-US.pdf 2025-05-12

기능 4: 고급 검색 및 필터링 기능

발신자, 수신자, 키워드, 날짜 등 다양한 조건으로 메일 검색 및 필터링 가능.

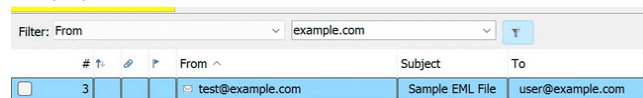
.eml 파일 여러 개가 들어 있는 폴더 열기



상단 메뉴에서 키워드 입력



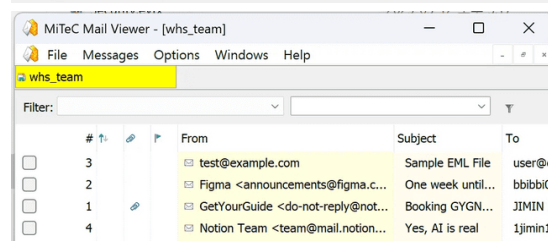
결과 확인



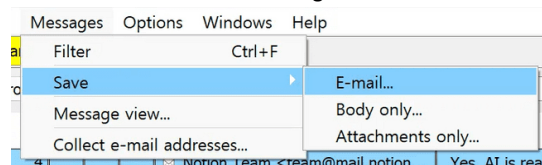
기능 5: 이메일 주소 및 메일 저장

선택한 메일을 .eml 파일로 저장하거나, 모든 이메일 주소를 한 번에 추출 가능.

.eml 파일 여러 개가 들어 있는 폴더 열기



메시지 여러 개 선택 -> Messages -> Save



E-mail...: 메일 전체 .eml로 저장

Body only...: 본문만 저장

Attachments only...: 첨부파일만 저장

[WinPrefetchView] 매뉴얼

1. 툴 기본 정보

항목	내용
툴 이름	WinPrefetchView
분석 카테고리	시스템 설치/실행, 파일 사용/조작(일부) (파일명, 프로그램 이름/경로, 실행 시간/횟수, 로딩된 파일 리스트, 볼륨 정보 등)
사용 버전	1.37
다운로드 경로	View the content of Windows Prefetch (.pf) files
지원 포맷	.pf (prefetch 파일)

2. 툴 소개 및 목적

WinPrefetchView는 시스템에 저장된 프리패치 파일을 읽고 그 안에 저장된 정보를 표시하는 간단한 유틸리티이다.

이 도구를 통해 각 애플리케이션이 어떤 파일을 사용하고 있는지, Windows 부팅 시 어떤 파일이 로드되는지 등을 알 수 있다.

3. 주요 기능 및 사용법

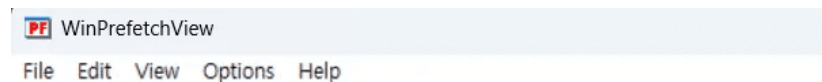
File → Prefetch 파일 저장, 종료

Edit → 항목 복사, 선택/해제 기능

View → 컬럼 선택, 새로고침 등 보기 옵션

Options → 시간, 경로 변경 옵션

Help → 프로그램 정보, 버전 확인



기능 1: 기본 실행

Filename	Created Time	Modified Time	File Size	Process EXE
136.0.7103.93_CHRO...	2025-05-07 오후 4:31:12	2025-05-07 오후 4:31:12	45,960	136.0.7103.93_C...
ALCAPTURE.EXE-E54...	2025-01-19 오후 4:31:12	2025-05-11 오후 10:20:28	24,401	ALCAPTURE.EXE
ALCAPTUREEDITOR.E...	2025-01-19 오후 4:31:12	2025-05-11 오후 10:20:28	22,337	ALCAPTUREEDITO...
ALSTS2.EXE-ABEE941...	2025-05-04 오후 4:31:12	2025-05-09 오후 4:31:12	10,430	ALSTS2.EXE
ALSTS2.EXE-FE84829...	2025-05-04 오후 4:31:12	2025-05-11 오후 10:20:28	10,459	ALSTS2.EXE
ALSTSCOLLECTOR.E...	2025-05-04 오후 4:31:12	2025-05-11 오후 10:20:28	4,426	ALSTSCOLLECTOR...
ALTOOLSMANAGER.E...	2025-05-03 오후 4:31:12	2025-05-11 오후 10:20:28	34,506	ALTOOLSMANAG...

Filename	Full Path	Device Path	In
\$MFT	C:\Windows\System32\BCRYPTPR...	\\VOLUME{01d2b8d28ab463d5-148...	2
136.0.7103.93_CHRO...	C:\WINDOWS\SYSTEMTEMP\CHRO...	\\VOLUME{01d2b8d28ab463d5-148...	3
ADVAPI32.DLL	C:\Windows\System32\advapi32.dll	\\VOLUME{01d2b8d28ab463d5-148...	7
BCRYPTPRIMITIVES.D...	C:\Windows\System32\BCRYPTPR...	\\VOLUME{01d2b8d28ab463d5-148...	2
C_949.NLS	C:\Windows\System32\WC_949.NLS	\\VOLUME{01d2b8d28ab463d5-148...	1
CHROME.PACKED.7Z	C:\WINDOWS\SYSTEMTEMP\CHRO...	\\VOLUME{01d2b8d28ab463d5-148...	2
COMBASE.DLL	C:\Windows\System32\combase.dll	\\VOLUME{01d2b8d28ab463d5-148...	11

exe 파일을 실행시키면 pf 파일이 생성되고 pf 파일이 만들어진 시각은 exe 프로그램 최초 실행 시각을, pf 파일이 수정된 시각은 exe 프로그램의 마지막 실행 시각을 뜻한다.

기본 경로는 C:\Windows\Prefetch이며, 프로그램의 대기시간을 줄이기 위해 사용된다.

예) 사용자가 ALCAPTURE.EXE를 처음 실행한 시각과 마지막으로 실행한 시각을 파악할 수 있다.

기능 2: 경로 변경

Advanced Options

Prefetch Folder:

C:\WINDOWS\Prefetch

Browse...

OK Cancel

prefetch 파일을 추출해서 사용하는 경우에는 파일 경로를 수동으로 설정할 수 있다.

Options 메뉴 → Advanced Options 혹은 F9를 눌러 경로를 변경할 수 있다.

예) 다른 PC에서 복사해온 Prefetch 파일을 분석할 때, 경로를 새로 지정해 분석할 수 있다.

기능 3: 프로그램 상세 정보 확인

WinPrefetchView

Properties

Filename: ALCAPTURE.EXE-E54A3F2C.pl

Created Time: 2025-01-19 오후 4:31:12

Modified Time: 2025-05-11 오후 10:20:28

File Size: 24,401

Process EXE: ALCAPTURE.EXE

Process Path: C:\PROGRAM FILES (X86)\WESTsoft\ALCAPTURE\MAI...

Run Counter: 179

Last Run Time: 2025-05-11 오후 10:20:17, 2025-05-09 오후 9:34:43

Missing Process: No

OK

WinPrefetchView

Properties

Filename: \$MFT

Full Path: C:\Windows\System32\WOW64\COMMON-UI\COMPONENTS.DLL

Device Path: \\VOLUME{01d2b8d28ab463d5-148b8256}\\$MFT

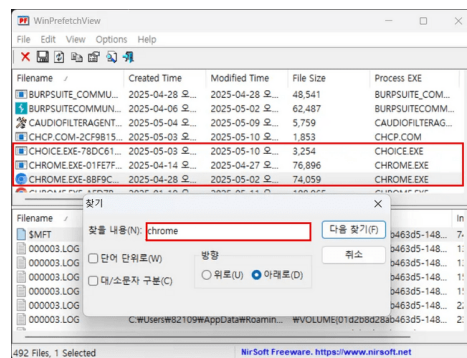
Index: 120

OK

파일 항목을 더블 클릭하면, 파일 이름과 카운터(실행횟수), 생성 시간과 변경 시간, 경로, 마지막 실행시간 등의 상세 정보를 확인할 수 있다. 해당 프로그램을 삭제하거나 경로를 변경하더라도 프리패치는 삭제되지 않는다.

예) 이미 삭제된 프로그램이라도 Prefetch 메타데이터를 통해 실행 이력을 추적할 수 있다.

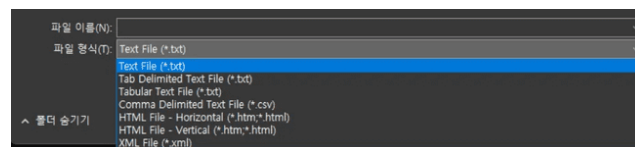
기능 4: 특정 단어 검색 (필터링)



Edit 메뉴 → Find 기능을 통해 파일 목록에서 특정 파일명을 검색할 수 있다. 검색 결과로 관련 Prefetch 항목만 필터링하여 보여준다.

예) chrome 키워드를 검색해 CHROME 실행 기록만 추출하여 분석할 수 있다.

기능 5: Export(내보내기)



File 메뉴 → Save Selected Items 혹은 Ctrl + S 를 통해 Prefetch 분석 데이터를 다양한 포맷 (.csv, .txt, .html, .xml)으로 저장할 수 있다.

모든 데이터를 내보내고 싶다면 Edit 메뉴 → Select All 혹은 Ctrl + A를 통해 전체 선택이 가능하다.

예) Prefetch 분석 결과를 CSV 형태로 저장해 엑셀로 리스트업할 수 있다.

[JumpListExplorer] 매뉴얼

1. 툴 기본 정보

항목	내용
툴 이름	JumpListExplorer
분석 카테고리	시스템 설치/실행 아티팩트
사용 버전	2.1.0
다운로드 경로	https://ericzimmerman.github.io/#index.md
지원 포맷	.lnk

2. 툴 소개 및 목적

JumpListExplorer 는 GUI 기반으로 윈도우 운영체제에서 생성되는 Jump List 아티팩트를 분석해주는 툴이다. 윈도우에서 최근 사용한 파일 및 폴더에 빠르게 접근이 가능하며, 사용자의 행위 파악에 도움이 된다.

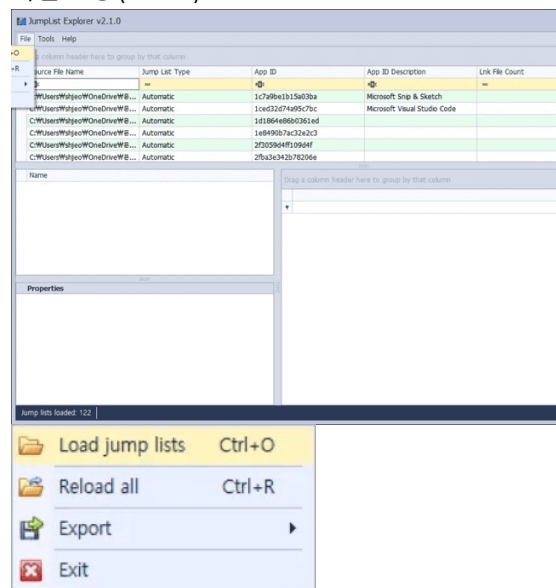
3. 주요 기능 및 사용법

기능 1 : Jump List 파일 로딩 및 AppID 기반 자동 식별

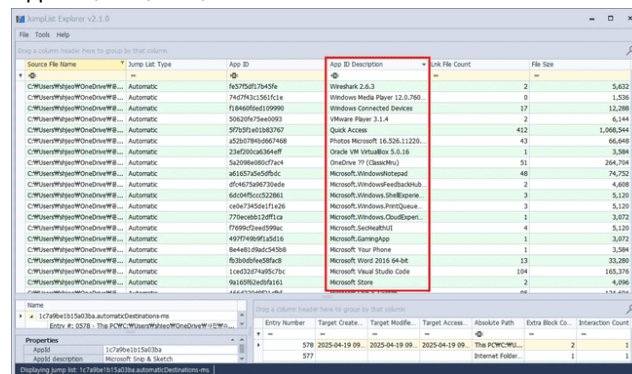
-파일을 불러오면 JumpListExplorer 가 각 파일의 AppID 를 식별하고 프로그램별로 그룹화하여 자동 정리한다.

-사건 당시 Word 문서를 열람했는지 확인하기 위해 해당 사용자의 JumpList 폴더에서 .automaticDestinations-ms 파일을 수집 후 로딩 → AppID가 Microsoft Office Word인 파일에서 실행 문서 경로와 타임스탬프 확인 가능하다.

파일 로딩 (ctrl + o)



AppID 기반 자동 식별



USB 드라이브에서 실행된 파일의 jumplist 분석 시, volume serial number 를 통해 외부 저장장치 임을 식별하거나 호스트 이름과 MAC 주소 분석을 통해 어떤 시스템에서 실행되었는지 식별하여 외부 유출 가능성 추적 및 연결 사용자 확인 가능하다.

2. 툴 매뉴얼 비교 표

툴 이름	분석 카테고리	도구 및 주요 기능 설명	지원 포맷	담당자
Registry Explorer	- 시스템 설치/실행 - 파일 사용/조작 - 사용자 행위 - 데이터베이스 아티팩트	- Windows 레지스트리 하이브 분석 도구. 키, 값, 타임스탬프, 삭제된 항목 및 히든 데이터 분석 가능. 레지스트리 기반 행위 분석	.reg, .dat, .LOG1, .LOG2, .blf 등	정지윤
Hashcat	- 파일 사용/조작	- 다양한 해시 알고리즘 지원 GPU 기반 해시 크래킹 도구. 암호 해시 분석 및 복구 시 사용. 패스워드 기반 공격	.hash, .txt, .potfile, .bin 등	정지윤
DCode	- 파일 사용/조작	- 다양한 형식의 타임스탬프를 사람이 읽을 수 있는 시간으로 변환. FILETIME, Unix Time 등 윈도우 아티팩트 시간 분석에 활용	.FILETIME, .Unix, .OLE, .Webkit 등	정지윤
MailView	- 파일 사용/조작	- 이메일 파일을 분석하는 도구 - 메일 본문, 송수신자 정보, 첨부파일 목록 등의 메타데이터를 추출 가능	.pst, .ost, .mbox, .eml 등	강지민
EventLog Explorer	- 시스템 설치/실행	- Windows 이벤트 로그(.evtx)를 시각적으로 분석하는 도구 - 주요 시스템 행위를 추적 가능	.evtx, .evt, .elf, .log 등	강지민
HxD	- 시스템 설치/실행 - 파일 사용/조작 - 사용자 행위 - 메모리 아티팩트	이진 파일, 디스크, 메모리를 16 진수로 분석하거나 편집할 수 있는 도구	.exe, .bin, .img, .dmp	김신아
PDFstreamdumper	- 시스템 설치/실행 - 파일 사용/조작 - 사용자 행위 - 메모리 아티팩트	- 악성 PDF 문서를 정적 분석하기 위한 도구 - PDF 내부에 숨겨진 JavaScript, 임베디드 객체, exploit 코드 등을 탐지하고 분석할 수 있는 기능 제공	.pdf, .FlateDecode, .js 등	김신아
ntfslogtracker	- 시스템 설치/실행 - 파일 사용/조작 - 사용자 행위 - 메모리 아티팩트	NTFS 파일 시스템에서 생성되는 \$LogFile, \$UsnJrnl, \$MFT 핵심 로그 파일 분석 할 수 있는 도구	.\$LogFile, .\$MFT, .evtx, RAW 등	김신아
FTK Imager	- 시스템 설치/실행 - 파일 사용/조작 - 메모리 아티팩트	디스크 이미징, 데이터 수집 및 분석, 무결성 검증 등을 수행 할 수 있는 도구	E01, AD1, .mem 등	김예은
WinMerge	- 파일 사용/조작 - 사용자 행위	파일과 디렉토리 간의 차이를 시각적으로 비교하고 병합할 수 있는 오픈 소스 도구	.txt, .c, .java, .docx, .binary 등	김예은
ChromeCacheView	- 사용자 행위 - 네트워크 아티팩트	- Google Chrome 브라우저의 캐시 파일을 분석하는 도구 - 웹 탐색 기록, 이미지, 동영상 등 캐시 데이터를 열람, 복사, 추출 가능	.CACHE, .DATA, .INDEX 등	김예은
Volatility	- 시스템 설치/실행 - 파일 사용/조작 - 사용자 행위 - 메모리 아티팩트	메모리 덤프 파일을 분석하여 실행 중인 프로세스, 인젝션 코드, 사용자 활동, 네트워크 연결 등 다양한 휘발성 데이터를 추출할 수 있는 도구	.raw, .mem, .bin, .dmp, .vmem 등	배영혜
Wireshark	- 사용자 행위 - 네트워크 아티팩트	실시간 네트워크 트래픽을 캡처하고 다양한 프로토콜을 계층별로 분석할 수 있는 도구	.pcap, .pcapng, .cap 등	배영혜
Autopsy	- 시스템 설치/실행 - 파일 사용/조작 - 사용자 행위 - 네트워크 아티팩트 - 메모리 아티팩트	- 디지털 증거를 수집, 분석할 수 있는 오픈소스 포렌식 도구	.img, E01, .AFF, .dd, .sqlite 등	서연정
KAPE	- 시스템 설치/실행 - 파일 사용/조작 - 사용자 행위	- 아티팩트 파서 및 추출 도구 - 파일 수집과 수집된 파일을 하나 이상의 프로그램으로 처리 가능	.evtx, .log, .csv, .pf, .lnk 등	안서진
WinPrefetchView	- 시스템 설치/실행 - 파일 사용/조작	- 시스템에 저장된 프리패치 파일을 읽고 저장된 정보를 표시하는 도구	.pf	안서진
DB Browser	- 파일 사용/조작 - 데이터베이스 아티팩트	- 데이터베이스 아티팩트 분석 도구 - 사용자 로그, 검색 기록, 위치 정보, 캐시 등을 조회	.db, .sqlite, .csv 등	전소현

JumpListExplorer	- 파일 사용/조작 - 사용자 행위	- 사용자가 실행한 문서, 앱, 파일 경로, 실행 시간 등의 흔적을 확인 가능한 도구	.lnk	전소현
------------------	------------------------	---	------	-----

3. 논문 요약 표

프로젝트 주제를 정하기 위해 각 팀원이 논문을 각각 3편씩 찾아보았으며, 논문을 협업 툴, 인스턴트 메신저, 웹, 기타로 분류하여 정리했습니다.

이를 통해 각 논문에서 다룬 아티팩트 유형과 경로를 명확히 파악할 수 있었으며, 특정 경로의 아티팩트를 대상으로 연구한 논문이 이미 존재하는 경우, 중복을 피하고 새로운 경로를 탐색할 수 있도록 하였습니다. 또한, 분석 대상 아티팩트의 경로를 표기하여 연구 범위를 명확히 하였으며, 이를 바탕으로 보다 효과적인 연구 주제 설정이 가능하도록 하였습니다.

협업툴

제목	분석 대상 프로그램	관련 아티팩트 유형 (경로 포함)	논문 요약	방향성
Forensic investigation of Google Meet for memory and browser artifacts	Google Meet (Web 기반 화상회의 애플리케이션)	- 메신저 아티팩트 전송 기록, 캐시, 채팅 로그, 실행 기록, 메모리 덤프 (실행 중 RAM에서 획득) - 시스템 설치/실행 아티팩트 Prefetch, 레지스트리, 이벤트 로그, LNK 파일 C:\Users\User\AppData\Roaming\Microsoft\Windows\Recent\ - 메모리 아티팩트: 프로세스 메모리, 명령어 이력, 메모리 덤프 (실행 중 RAM에서 획득) - 사용자 행위 아티팩트: 최근 명령어, 로그인 기록, 탐색 기록 C:\Users\User\AppData\Local\Google\Chrome\User Data\Default\Cache\	- Google Meet 사용 중 메모리와 브라우저에 남은 아티팩트를 식별 분석하고, 이를 자동 추출하는 Python 도구를 개발함.	- 악용 가능성: Google Meet 메모리·브라우저에 남은 이메일, 채팅, 파일 정보가 피싱·사칭·유출에 악용될 수 있음. - 자동화 도구 개발: 이메일, 토큰 등 민감 정보를 시그니처 기반으로 자동 추출·위험도 분류.
노션프로그램 아티팩트 분석을 통한 위협 분석 및 대응방안 제시	Notion (PC 및 Android 앱)	- 메신저 아티팩트: 전송 기록, 캐시, 채팅 로그, 실행 기록 C:\Users\User\AppData\Roaming\Notion\Notion\Users\ - 사용자 행위 아티팩트: 최근 명령어, 로그인 기록, 탐색 기록 C:\Users\User\AppData\Roaming\Notion\Notion\Users\Users.db	- Notion 사용 중 PC와 Android 환경에서 수집된 사용자 정보와 작업 내용이 암호화 없이 저장되어 있어 유출 위험이 크다는 점을 확인하고, 이를 분석해 보안 위협과 포렌식 활용 가능성을 제시함.	- 악용 가능성: Notion에 저장된 이메일, 토큰, 삭제된 블록 등이 계정 탈취·문서 유출·사칭에 악용될 수 있음. - 자동화 도구 개발: 디스크 이미지에서 토큰, 삭제 기록 등 위험 아티팩트 자동 추출 및 분류 기능 개발.
메신저형 협업툴 어	ChannelTalk	- 메신저 아티팩트 : 전송 기록, 캐시, 채팅 로그, 실행 기록	- 팀 메신저 등 모바일 어플리	- 채팅 추출, MAC 타임 분석,

	플리케이션 아티팩트 분석 - ChannelTalk을 중심으로		<ul style="list-style-type: none"> - 네트워크 아티팩트 : 방문 기록, 세션 토큰, 네트워크 연결 - 사용자 행위 : 최근 명령어, 로그인 기록, 탐색 기록 - 시스템 설치/실행 : Prefetch, 레지스트리, 이벤트 로그, LNK 파일 	<ul style="list-style-type: none"> - 케이션 아티팩트를 분석해 사용자 행위와 사용 내역 기반 보안 사고 증거 수집 	<ul style="list-style-type: none"> - 이상 접속 탐지 자동화 도구 개발
	안드로이드 환경에서의 Telegram X 메신저 아티팩트 분석	Telegram X	<ul style="list-style-type: none"> - 메신저 아티팩트 : 전송 기록, 캐시, 채팅 로그, 실행 기록 /data/data/org.thunderdog.challegram/files/tdlib → 경로에 위치하는 dp.sqlite파일 → messages 테이블 - 사용자 행위 아티팩트: 최근 명령어, 로그인 기록, 탐색 기록 /media/0/Android/data/org.thunderdog.challegram/files 	<ul style="list-style-type: none"> - Telegram X의 다양한 메시지 유형과 로그를 분석하여 WAL 파일을 통한 삭제 메시지 복구 가능성을 확인 	<ul style="list-style-type: none"> - WAL, SQLite 분석을 통한 데이터 변화 추적
	화상 회의 애플리케이션 GoToWebinar 및 GoToMeeting 아티팩트 분석	GotoWebinar, GoToMeeting	<ul style="list-style-type: none"> - 메신저 아티팩트: C:\Users\<Username>\Documents\ChatLog[회의명]YYYY_MM_DD HH_mm.rtf - 파일 사용/조작: C:\Users\<Username>\Documents - 사용자 행위 	<ul style="list-style-type: none"> - 애플리케이션 데이터 특성과 차이 비교, 데이터 수집 및 분석 부족 	<ul style="list-style-type: none"> - 실시간 화상회의 데이터 수집 자동화 툴 개발
	윈도우 환경에서의 협업 도구 잔디 아티팩트 수집 및 분석 연구	JANDI(잔디)	<ul style="list-style-type: none"> - 메신저 아티팩트: Cache 폴더 - 시스템 설치/실행: C:\Users\[USERNAME]\AppData\Roaming\JANDI - 사용자 행위: Cache와 Local Storage 폴더 하위에 존재 	<ul style="list-style-type: none"> - 잔디의 아티팩트 수집 및 데이터 분석 기법 제시, API 기반 데이터 획득 방법 제안 	<ul style="list-style-type: none"> - JANDI 내부 악용 기능 탐색 및 분석 자동화 툴 개발
	협업 툴의 사용자 행위별 아티팩트 분석 연구 - Microsoft Teams	Microsoft Teams	<ul style="list-style-type: none"> - 메신저 아티팩트 %APPDATA%\Microsoft\Teams\IndexedDB\https_teams.microsoft.com_0.indexeddb.leveldb - 시스템 설치/실행 %APPDATA%\Microsoft\Teams - 사용자 행위 %APPDATA%\Microsoft\Teams\Local Storage , %APPDATA%\Microsoft\Teams\IndexedDB 	<ul style="list-style-type: none"> - 디지털 포렌식 분석에서 운영 환경별 증거 확보 중요성 강조 	<ul style="list-style-type: none"> - 협업툴 및 다양한 운영 환경에 대한 확장 연구 필요
	협업 툴 아티팩트 분석 및 삭제된 데이터 복구 연구	잔디, 네이버 워크스	<ul style="list-style-type: none"> - 메신저 아티팩트 %LOCALAPPDATA%\Microsoft\Teams\main.db, %LOCALAPPDATA%\Microsoft\Teams\chat.db - 시스템 설치/실행 아티팩트 %Windows%\AppCompat\Programs\Amcache.ah - 사용자 행위 아티팩트 C:\Windows\System32\winevt\Logs 	<ul style="list-style-type: none"> - 협업 툴 사용 증가로 인한 데이터 유출 위험 분석, 삭제 메시지 복구 가능성 확인 	<ul style="list-style-type: none"> - 아티팩트 자동 파싱 도구 개발
	Windows	Telegram	<ul style="list-style-type: none"> - 사용자 행위 아티팩트 	<ul style="list-style-type: none"> - 메모리 덤프 	<ul style="list-style-type: none"> - 메모리 기반 포

	Telegram Desktop 애플리케이션에서 검색 가능한 메모리 아티팩트 추출 및 분석	Desktop	<ul style="list-style-type: none"> - 메모리 아티팩트 UserData, HistoryMessage 객체 구조 분석을 통해 이름, 전화번호 등 추출 - 데이터베이스 아티팩트 메모리 상의 QString, PeerData, ChatData 추적 	를 통해 계정 정보, 대화 내용, 삭제된 흔적을 추출하는 방법 제시	랜싱 도구 개발
	Microsoft Office 진단 로그 분석 및 포렌식 활용 방안	Microsoft Word, Excel, PowerPoint	<ul style="list-style-type: none"> - 시스템 설치/실행 아티팩트: Prefetch, Amcache.hve, MFT, 임시파일 - 사용자 행위 아티팩트: Pdod, \$UsnJrnl 	- Microsoft Office 진단 로그를 활용하여 작업 이력 추적 가능성 분석	- 진단 로그를 통한 문서 작업 흐름 복원 도구 개발
	디지털 상호작용 디코딩: TeamViewer 포렌식 아티팩트 연구	TeamViewer	<ul style="list-style-type: none"> - 시스템 설치/실행 아티팩트 : Program Files\TeamViewer - 파일 사용/조작 아티팩트 AppData\Roaming\TeamViewer\Connections.txt AppData\Roaming\TeamViewer\Connections_incoming.txt AppData\Local\TeamViewer\Database\TVCache\TVCache.db AppData\Local\TeamViewer\Database\TVCache\TVCacheDownloadHistory.db - 메모리 아티팩트 : 동적 비밀번호, 채팅 내역 - 네트워크 아티팩트 TeamViewer15_Logfile.log (Android ↔ Windows 간 접속 IP 기록) - 데이터베이스 아티팩트 AppData\Local\TeamViewer\Database\TVCache\TVCache.db AppData\Local\TeamViewer\Database\TVCache\TVCacheDownloadHistory.db 	- Windows와 Android에서 TeamViewer 사용 시 남는 아티팩트 분석	- TeamViewer 사용 시 로그와 메모리 덤프 파싱 도구 개발
	디지털 포렌식 관점에서의 협업 도구 네이버웍스의 데이터 수집 및 분석	네이버웍스	<ul style="list-style-type: none"> - 채팅 기록 - 파일 공유 - 캘린더/일정 - 사용자 계정 정보 - 삭제된 데이터, 로그 파일 C:\Users[Username]\AppData\Local\WorksMobile\NaverWorks\ 	- 네이버웍스에서 생성되는 다양한 사용자 행위 기반 데이터를 수집하고 분석함	- 안티포렌식 기능 우회 기술 연구 및 자동 분석 도구 개발
	디지털 포렌식 관점의 네이버 밴드 사용자 행위 수집 및 분석 연구	네이버 밴드 (Android 환경)	<ul style="list-style-type: none"> - 메신저 아티팩트: /data/data/com.nhn.android.band/databases/chat_message - 네트워크 아티팩트: /v2.0.0/get_posts, /get_photos, /get_files - 사용자 행위 아티팩트: /databases/member, /shared_prefs/USER.xml, /cache/IMAGE, /cache/VIDEO 	- Android 환경에서 네이버 밴드의 로컬 데이터와 API를 분석하여 사용자 정보, 채팅 기록 등을 수집	- 악용 가능성: 채팅, 이미지 캐시, user/band ID 등을 통한 신원 도용 및 삭제 대화 복원

인스턴트 메신저

제목	분석 대상 프로그램	관련 아티팩트 유형 (경로 포함)	논문 요약	방향성
포렌식 관점에서 Element 인스턴트 메신저 아 티팩트 분 석	Element	- 메신저 아티팩트 - 네트워크 아티팩트 - 메모리 아티팩트 - 사용자 행위	- Signal, Wickr, Threema 등 보안 메신저 암호화 메커니 즘 분석 및 일부 복호화 방 법 제시	- 메타데이터 중심 분석 및 키 추출 도 구 개발
윈도우 환 경에서 카 카오톡 데 이터 복호 화 및 아 티팩트 분 석 연구	KakaoTalk (카카오톡) PC 버전	- 파일 사용/조작: %LocalAppData%\Kakao\Wka kaoTalk\Users\Wchat_data - 사용자 행위: %LocalAppData%\Kakao\Wka kaoTalk\Users - 메신저 아티팩트: %LocalAppData%\Kakao\Wka kaoTalk\Users\Wchat_data	- 윈도우 환경에서 카카오톡 데이터를 복호화하고 아티 팩트를 분석하는 방안을 구 현함	- 썸네일 자동 추출 도구 및 데이터 복 호화 자동화 도구 개발
카카오톡 메신저 백 업 서비스 '톡서랍 플러스' 데이터 수 집 방법 연구	KakaoTalk (카카오톡) PC 버전	- 네트워크 아티팩트 - 사용자 행위 - 데이터베이스 아티팩트	- 클라우드-동기화 서버 기 반 '톡서랍 플러스' 데이터를 Internal API를 통해 수집하 는 방안 제안	- 서버 백업 메시지 및 첨부파일 수집 도구 개발
Windows 에서의 Wire 크리 덴셜 획득 및 아티팩 트 분석	Wire (암호 화 메신저)	채팅 기록, 크리덴셜 데이터, 파일 공유 기록, 계정 정보 경 로: %APPDATA%\Wire\logs\Wele ctron.log	- Wire 메신저의 로그인 정 보와 사용자 행위 기반 아티 팩트를 분석하여 삭제 메시 지 복원 가능성 확인	- 로그 기반 삭제 메 시지 복원 기법 개 발
윈도우 및 안드로이드 환경에서 WeChat 메신저 아 티팩트 분 석 연구	WeChat (인스턴트 메신저)	채팅 기록, Moments, 타임캡 슐, 사용자 계정 정보, 데이터 베이스 파일	- Windows와 Android 환 경에서 WeChat의 사용자 행위 기반 아티팩트를 분석하여 저장 경로 차이 비교	- 자동화된 아티팩 트 수집 도구 및 삭 제 메시지 복구 기 법 연구
Windows Telegram Desktop 애플리케 이션에서 검색 가능 한 메모리	Telegram Desktop	- 메모리 아티팩트 : UserData, HistoryMessage 객체 구조 분 석을 통해 이름, 전화번호 등 추출 - 데이터베이스 아티팩 트 : 메모리 상의 QString, PeerData, ChatData 추적	Windows 환경에서 Telegram Desktop의 메모 리 덤프를 분석하여 디스크 로 접근할 수 없는 사용자 계정, 대화 내용 등을 추출하 였다. 연구진은 Windows Memory Extractor와 IM	- Telegram과 같은 메신저의 메모리 덤 프를 분석하여 계정 정보, 대화 내용, 삭 제된 흔적 등을 자 동으로 추출하는 메 모리 기반 포렌식

아티팩트 추출 및 분석			Artifact Finder를 활용하여 주요 아티팩트를 효과적으 로 식별하였다.	도구를 개발
--------------------	--	--	--	--------

웹

제목	분석 대상 프로그램	관련 아티팩트 유형 (경로 포함)	논문 요약	방향성
윈도우 환 경의 아티 팩트를 활 용한 자동 화된 사용 자 분석 방 안	Windows OS, Google Chrome	- 사용자 행위 아티팩트 : 프리패치, 레지스트리, 문서 목록, 이 벤트 로그 - 시스템 설치/실행 아티팩트 - 데이 터베이스 아티팩트	- 윈도우 시스템의 다양 한 아티팩트를 수집하 여 자동화된 사용자 행 위 분석 기법을 제안 - 웹 브라우저 기록과 시 스템 로그를 Mecab 형 태소 분석기와 결합하 여 관심 키워드 추출, 사용자 분류, 데이터 시 각화 수행	자동화된 사용자 프로파일링 및 이상 행위 탐지 기반 마련
Google 드 라이브의 디지털 포 렌식: 디지 털 아티팩 트 추출 및 분석 기술	Google Drive	- 시스템 설치/실행 아티팩트 ACER\AppData\Local\Google\DriveFS - 파일 사용/ 조작 아티팩트 ACER\AppData\Local\Google\DriveFS\sync_config.db ACER\AppData\Local\Google\DriveFS\snapshot.db ACER\AppData\Local\Google\DriveFS\sync_log.db - 데이터 베이스 아티팩트 ACER\AppData\Local\Google\DriveFS\experiments.db ACER\AppData\Local\Google\DriveFS\metric_store_sqlite.db ACER\AppData\Local\Google\DriveFS\root_preference_sqlite.db	- Google Drive의 클라 우드 환경에서 디지털 포렌식 수행을 위해 NIST 방법론을 적용하 여 주요 아티팩트(사용 자 활동 로그, 문서 메 타데이터, 권한 정보 등) 를 식별	클라우드 포렌식 환경에서 NIST 기반의 단계별 절차 적용 가능 성 평가, Google Drive File Stream의 구조 적 한계와 도구 적합성에 대한 검토

기타

제목	분석 대상	관련 아티팩트 유형(경로 포함)	논문 요약	방향성
----	-------	-------------------	-------	-----

	프로그램			
안드로이드 환경에서의 지도 애플리케이션 아티팩트 분석 및 복호화 방안 연구	네이버 지도, TMAP, 카카오맵 PC 버전	<ul style="list-style-type: none"> - 사용자 행위 아티팩트 databases 디렉터리의 bookmark.db, search-history.db, route-history.db, subwayMap.db파일 shared_prefs 디렉터리 내 pubtrans_cache.xml파일 NativeNaviDefaults.xml 파일 	<ul style="list-style-type: none"> - 지도 애플리케이션에 분석된 결과의 범위는 한정적, 아티팩트가 변경되거나 애플리케이션마다 저장되는 데이터가 다양함. - 최신 버전에서의 데이터 수집 방안 연구 필요 	GPS 데이터를 악용하는 경우 GPS 로그파일, 위치 기록 캐시 기반 패턴 분석
원격 제어용 어플리케이션에서의 아티팩트 수집 및 분석	TeamViewer, AnyDesk, AirDroid (모두 Android 환경)	<ul style="list-style-type: none"> - 메신저 아티팩트: app.db(AirDroid) - 네트워크 아티팩트: TVLog.html(TeamViewer), account_backup(AirDroid), main_preference_bk(AirDroid) - 시스템 설치/실행 아티팩트: client.conf (TeamViewer), com.sand.airdroid_preference.xml(AirDroid) - 파일 사용/조작 아티팩트: downloads/ (AnyDesk), TVLog.html(TeamViewer) - 사용자 행위 아티팩트: TVLog.html(TeamViewer), app.db(AirDroid), recursive_file_index_phone(AirDroid) 	<ul style="list-style-type: none"> - Android 기반 원격 제어 앱의 로컬 아티팩트를 분석하여 제어자 정보, 파일 전송 권한 요청 등 핵심 데이터를 식별 	악용 가능성: 접속 기록, 계정, 전송 파일 등 감청·탈취·사칭 위험
무 설치 프로그램에서의 사용자 행위 아티팩트 분석	Opera, Notepad ++	<ul style="list-style-type: none"> - 메모리 아티팩트: 경로 X, 분석 도구는 Hex Fiend, Volatility - 시스템 설치/실행: C:\Windows\Prefetch - 파일 사용/조작: C:\Windows\Temp - 사용자 행위: %AppData%\Roming\Microsoft\Windows\Recent 	<ul style="list-style-type: none"> - 포터블 프로그램에서의 사용자 행위 분석 방안 제시, 메모리 분석을 통해 증거 수집 가능 	비전통적 아티팩트 (windows Defender, MemCompression 등)를 파싱할 도구 개발
폴라리스 오피스 포렌식 아티팩트에 관한 연구	폴라리스 오피스	<ul style="list-style-type: none"> - 시스템 설치/실행 아티팩트 : C:\Windows\Prefetch\폴라리스 오피스 설치 파일명].pf (prefetch) - 사용자 행위 아티팩트 : C:\HKCU\Software\Infraware\PolarisOffice의 "FirstHomeAccessTime" 정보 - 파일 사용/조작 아티팩트 : %UserProfile%\AppData\Roaming\PolarisOffice\Database\InfrawareRecentFiles.sqlite (최근 사용된 파일 목록), %UserProfile%\AppData\Roaming\PolarisOffice\Database\RecordCommand2.sqlite (작업 과정에 관련된 모든 파일에 대한 액세스 흔적), %UserProfile%\AppData\Roaming\PolarisOffice\Database\InfrawareAutoRecover.sqlite (자동 복구 정보), %UserProfile%\AppData\Roaming\PolarisOffice\Recover\Slide\파일명, %UserProfile%\AppData\Roaming\Polaris 	<ul style="list-style-type: none"> - Polaris Office 사용 시 Windows와 macOS에서 생성되는 아티팩트를 분석하여 작업 로그 DB 확인 	문서 작성 및 수정 기능의 작업 로그 DB 분석을 통한 사용자 행위 재구성

			Office\Recover\Word\파일명, %UserProfile%\AppData\Roaming\Polaris\Office\Recover\Sheet\파일명 - 데이터베이스 아티팩트 : %UserProfile%\AppData\Roaming\Polaris\Office\Database\InfrawareRecentFiles.sqlite, %UserProfile%\AppData\Roaming\Polaris\Office\Database\RecordCommand2.sqlite, %UserProfile%\AppData\Roaming\Polaris\Office\Database\InfrawareAutoRecover.sqlite		
	취약점 별 아티팩트 사례 분석을 통한 아티팩트 그룹핑 연구	Adobe Flash Player	- 시스템 설치/실행 아티팩트 : Prefetch, Event log, - 파일 사용/조작 아티팩트 : \$MFT, \$LogFile, \$UsnJrnl, %Appdata%\Roaming\Microsoft\Windows\Recent\AutomaticDestinations, - 사용자 행위 아티팩트 : %Appdata%\Roaming\Adobe\Flash Player\NativeCache(Flash Cache), %Appdata%\Roaming\Macromedia\Flash Player\Shared Objects (Shared Objects), %Appdata%\Roaming\Macromedia\Flash Player\support\flashplayer\sys(Setting Info)	- Adobe Flash Player의 취약점 활용 침해사고 사례 분석 - 초기 침해 대응을 위한 '아티팩트 그룹핑' 방안 제시	CVE 취약점 공격 발생 시 Prefetch 및 Web Cache 분석을 통한 공격 흔적 확보
	Conversational AI forensics: A case study on ChatGPT, Gemini, Copilot, and Claude	ChatGPT, Gemini, Copilot, Claude	- 메신저 아티팩트: C:\Users\<User>\Downloads\chatgpt_export_<YYYY-MM-DD>\conversations.json - 네트워크 아티팩트: C:\Users\<User>\Documents\Wireshark\chatgpt_traffic.pcap	- 대화형 AI 플랫폼의 대화 이력과 메타데이터를 수집·분석하여 악성 코드 제작 행위를 입증할 수 있는 아티팩트 식별	대화형 AI에 입력된 프롬프트와 삭제된 대화 로그를 분석하여 이상 행위 탐지 모델 개발

활동사진
(회의 사진 등)

2025.05.06 회의



2025.05.10



2025.05.12



2025.05.13

