



# 화이트햇 스쿨 2단계 팀 프로젝트 보고서

차세대 보안리더 양성 프로그램 한국정보기술연구원 BoB 교육센터

멘토명 / PL명	문현지/심주완 팀명 포렌식빵					
프로젝트 주제	윈도우 악성 프로그램 탐지 및	회차	1회차			
	분석		14/7/			
팀원	정지윤(PM) , 강지민, 김신	아, 김예은,	배영혜, 서연정, 안서진, 전소현			
추진현황		목차 . 툴 매 뉴 얼 . 논문 요약	Ξ			





## 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)

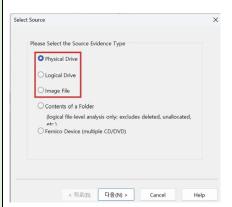
FTK Imager는 디스크 이미징, 데이터 수집, 무결성 검증을 수행한다. 디스크, 메모리 덤프, 이메일 등 다양한 포맷을 지원하며, 수집된 증거를 다른 포렌식 분석 도구와 연계하여 활용할 수 있다.

#### 3. 주요 기능 및 사용법

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

## 기능 1: 디스크 이미지 덤프하기

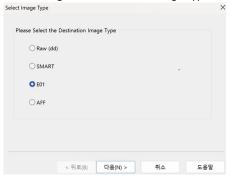
File → Create Disk Image → Select Source → 이미징 할 타입 선택 → 다음



Select Drive Selection : 원하는 드라이브 선택



Create Image  $\rightarrow$  Add  $\rightarrow$  Select Image Type





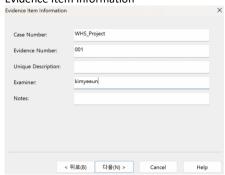


Raw(dd) : 원본과 동일한 이미징 (압축 x)

SMART : 리눅스 운영체제 이미징 E01 : 압축 이미징

AFF : 대용량 디스크 이미징

#### **Evidence Item information**



#### Select Image Destination $\rightarrow$ finish $\rightarrow$ start

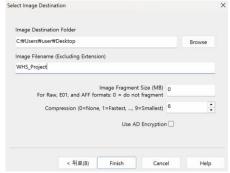


Image Fragment Size : MB를 기준으로 이미지 파일 분할저장 (0 = 분할 저장 안함 ←권장됨) Compression : 압축률 (E01의 기본값 6, Raw(dd)선택시 0 고정) 끝나면 해시값이 뜨는데 이 해시값을 통해 무결성을 입증한다.

## 기능 2: 삭제 파일 복구하기

File  $\rightarrow$  Add Evidence Item  $\rightarrow$  root 로 들어가면 삭제한 파일들을 전부 볼 수 있다.

```
Evidence Tree File List

Sa w.Ms., project EO1 (14895M8) (11875) (11875M8) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (11875) (1
```

복구할 파일을 선택하고 우클릭으로 Export Files를 클릭하면 파일을 복구할 위치가 뜬다. 바탕화면으로 지정하고 추출해봤다.







바탕화면에서 정상적으로 추출된 걸 확인할 수 있다.

#### 기능 3: 이미지 마운팅

 $\mathsf{File} \to \mathsf{Image} \ \mathsf{Mounting} \to \mathsf{Mount}$ 

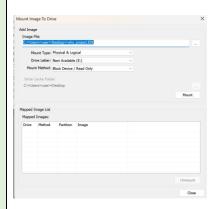


Image File : 마운팅 할 이미지 파일 선택

Mount Type : 마운트 하고자 하는 대상의 범위 선택

Drive Letter : 드라이브 철자 선택

Mount MEthod : 마운트 된 이미지의 접근 및 조작 가능성 선택



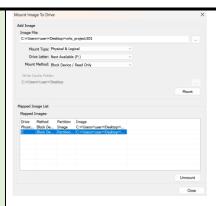
위와 같이 마운트 된 모습을 확인해볼 수 있다.

마운트 해제방법

Mapped Images → 마운트 해제할 드라이브 선택 → Unmount

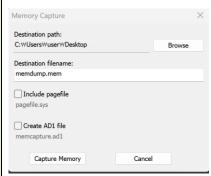






#### 기능 4: 메모리 덤프

File → Capture memory



Include pagefile : pagefiles.sys 덤프 여부

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

#### Result

memdump.mem



## 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





4	Α	В	C	D	E	F	G	Н	1
1	MD5	SHA1	FileNames						
2	1f801bac9	f4631eceb	1ecebtest.vhd₩Partition 1 [497MB]₩새 볼륨 [NTFS]₩[root]₩test.txt						
3	0c041827	1e7367347	test.vhd₩F	Partition 1	[497MB]₩	새 볼륨 [N	ITFS]₩[roo	t]₩test.txt₩	#\$EFS

## 이런식으로 뜬다

(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, .mbox, .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





	Viewer - [One week until Con		- 0						
	ions Windows Language	Help							
One week until	Config ee								
Body Source									
Total and	One week until Config as	One week well foods as							
	gma <announcementa@figma.com></announcementa@figma.com>								
1000									
Te:	bbibbi0425@grrafl.com								
CC:									
BCC:									
Timestamo	2025-09-01 01: 3:01:21		Size: 50,554 B						
Plain HTM									
ki there.									
so you don	't miss a thing. Virtu	y 7 at 9:00MM POT / 12:00PM EDT-rep wal registration is open and always							
so you don Register n [https://r See you at The Figma	't miss a thing. Virtu now wg.config.figma.com/fl : Config, Team	ny 7 at 9:00MP PDT / 12:00PM EDT-rej mal registration is open and always now/figma/config2025/virtual/creatm	gister today free for all. accountPutm_contentscta]						
so you don Register n [https://r See you at The Figma Figma is a Web, Figma faster.	over miss a thing. Virtuous wg.config.figma.com/fl Config. Team	y 7 at 9:88AM PDT / 12:88PM EDT-re al registration is open and always	gister today free for all. accountPutm_content=cta] sorn on the						
so you don Register n [https://r See you at The Figma Figma is a Weeb, Figma faster. Figma [https://s	rt miss a thing. Virtuom way.config.figma.com/fl Config. Team design platform for to helps the entire prod	y 7 at 9:00M PDT / 12:00PM EDT-rep al registration is open and always ow/figma/config1025/virtual/create: reams who build products together.	gister today free for all. accountPutm_content*cta] Born on the tter designs,						
so you don Register n [https://r See you at The Figma Figma is a Web, Figma faster. Figma [https://s https://fi Figma	of miss a thing. Virtuom on mg.config.figma.com/fl config. Texm design platform for t helps the entire prod tatic.figma.com/upload gma.com/#figma	y 7 at 9:000 FOT / 12:000 FOT / 10:000 FOT /	gister today free for all. accounthuts_content+cta)  Born on the tter designs, 13782987]						
so you don Register n [https://r See you at The Figma Figma is a Web, Figma faster. Figma [https://s https://fi Figma [https://s	of miss a thing. Virtuom on mg.config.figma.com/fl config. Texm design platform for t helps the entire prod tatic.figma.com/upload gma.com/#figma	by 7 at 9:080F POT / 12:08PM COT-me al registration is open and always cow/figma/comfig2025/virtual/create command to build products together. I bears who build products together. I buct team create, test, and ship be	gister today free for all. accounthuts_content+cta)  Born on the tter designs, 13782987]						
so you don Register /n [https://n [https://n See you at The Figma is a Web, Figma faster. Figma [https://s https://s Figma [https://s figma [https://s Figma [https://s	It miss a thing. Virtuo one of the control of the control of the config. Config. Team design platform for to the label of the configuration of the configu	y 7 at 9:000 FOT / 12:000 FOT / 10:000 FOT /	gister today free for all. accounthutm_contentucta] form on the tter designs, 13782987] aa3f5300]https://figna.com/pfigna						
so you don Register n [https://r See you at The Figma Figma is a Web, Figma faster. Figma [https://s https://fi Figma [https://s https://s https://s https://s	it miss a thing. Virtuo on way.comfig.figma.com/fl Comfig. team design platform for t helps the entire prod static.figma.com/upload gma.com/mfigms tatic.figma.com/upload static.figma.com/upload	y at 9 jamus por / 1220mm tor-me al registration to poem and allows con/figma/config2025/virtual/create wass also build products together. I buct team create, test, and ship bet st/dpct220c0u93955seas1c4cbdee80mi st/dpct220c0u93955seas1c4cbdee80mi st/20c42578669159386530750633as58h	gister today free for all. accounthutm_contentucta] form on the tter designs, 13782987] aa3f5300]https://figna.com/pfigna						
so you don Register n [https://e See you at The Figma is a Web, Figma faster. Figma [https://s https://s Figma [https://s Twitter [https://s Twitter Twitter	it miss a thing. Virtuo one vag.comig.figma.com/fl. Config. Team design platform for to the lab the entire pro- tatic.figma.com/upload gmm.com/fligma tatic.figma.com/upload tatic.figma.com/upload tatic.figma.com/upload titte.figma.com/upload titte.figma.com/upload	y at 9 jamus por / 1220mm tor-me al registration to poem and allows con/figma/config2025/virtual/create wass also build products together. I buct team create, test, and ship bet st/dpct220c0u93955seas1c4cbdee80mi st/dpct220c0u93955seas1c4cbdee80mi st/20c42578669159386530750633as58h	gister today free for all. seccounthes_contentrata]  form on the tter designs, 13782987] substitute(figna.com/pfigna.com/pfigna.gfm258757)						
so you don Register n [intps://e [intps://s See you at The Figma Figma is a Web, Figma faster. Figma [intps://s Intps://s Intips://s	it miss a thing. Wirtum wag.comfig.figma.com/fig. wag.comfig.figma.com/figma.com/figma.com/figma.com/mpload tatic.figma.com/mpload gma.com/mfigma.com/mpload itatic.figma.com/mpload itatic.figma.com/mpload itatic.figma.com/mpload itatic.figma.com/mpload itatic.figma.com/mpload itatic.figma.com/mpload itatic.figma.com/mpload itatic.figma.com/mpload	y y at siemen pof / iziemen tor-real at registration joen and alboys ow/figma/comfig205/virtual/create sees who build products tagether. buct toen create, test, and ship be fix/fix/2100/mbs/fixesic/des/fixesic/	gister today free for all secounthies_contentivita] Bern un til ster designs, starses] sadf5500[https://figns.com/pfigns spc.55ed]https://sister.com/figns bcc.55ed]https://sister.com/figns						
so you don Register n [https://e Ster you at The Figme Figme is a Meb, Figme faster. Figme [https://s Figme [https://s https://s	of miss a thing. Virtuo owg.comfig.figma.com/fi Cooffig. Team design platform for to the last the thing platform for to the last the thing produced and comfigma thatic.figma.com/wipload tatic.figma.com/wipload itter.com/figma.com/wipload tatic.figma.com/wipload tatic.figma.com/wipload tatic.figma.com/wipload tatic.figma.com/wipload tatic.figma.com/wipload	y y at 9:0000 rof / 12:0000 rof - 20 an ergistration joen and along com/figma/config2025/virtual/create wass also build products together. I but teen create, test, and ship be but teen create, test, and ship be but/scc6-210c000595955eas1c4ccbdeedBoff x/scc6-210c000595955eas1c4ccbdeedBoff x/scc6-210c000595955eas1c4ccbdeedBoff x/scc6-210c000595956eas1c00550ccbdeedBoff x/scc6-2000005950eas1c0050ccbdeedBoff x/scc6-20000050ccbdeedBoff x/scc6-200000000000000000000000000000000000	gister today free for all secounthies_contentivita] Bern un til ster designs, starses] sadf5500[https://figns.com/pfigns spc.55ed]https://sister.com/figns bcc.55ed]https://sister.com/figns						
so you don Register n [https://e Ster you at The Figme is a Web, Figme faster. Figme [https://s https://s	it miss thing. Virtuo way comfig.figma.com/fi Coofig. Team design platform for the helps the entire prod tatic.figma.com/upload gma.com/ifgma tatic.figma.com/upload tatic.figma.com/upload tatic.figma.com/upload tatic.figma.com/upload tatic.figma.com/upload tatic.figma.com/upload tatic.figma.com/upload tatic.figma.com/upload tatic.figma.com/upload	yy a si yaan oof / 12 onen cort	gister today free for all, account being contentrate lines on the tree feelings, 1326971 aab7530]https://figna.com/efigna 13853272 bcc55es]https://fuster.com/figna						
so you don So you don Register n [https://e See you at The Figma The Figma Figma is a Web, Figma [https://s https://s Figma [https://s Figma [https://s hitter [https://s Instagram [https://s Instagram [https://s Instagram	it miss thing. Virtuo way comfig.figma.com/fi Coofig. Team design platform for the helps the entire prod tatic.figma.com/upload gma.com/ifgma tatic.figma.com/upload tatic.figma.com/upload tatic.figma.com/upload tatic.figma.com/upload tatic.figma.com/upload tatic.figma.com/upload tatic.figma.com/upload tatic.figma.com/upload tatic.figma.com/upload	y y at 9:0000 rof / 12:0000 rof - 22:000 rof - 20:000 rof	gister today free for all, account being contentrate lines on the tree feelings, 1326971 aab7530]https://figna.com/efigna 13853272 bcc55es]https://fuster.com/figna						
so you don Register n [https://e Ster you at The Figme is a Web, Figme faster. Figme [https://s https://s	it miss a thing. Virtuo mg.comfig.figma.com/ij comfig.figma.com/ij comfig.figma.com/ij comfig.figma.com/ij comfig.figma.com/ij tatic.figma.c	yy a si yaan oof / 12 onen cort	gister today free for all, account being contentrate lines on the tree feelings, 1326971 aab7530]https://figna.com/efigna 13853272 bcc55es]https://fuster.com/figna						

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)  $\rightarrow$  현재 첨부 없음 표시도 정상

## 기능 2: 메일 본문 및 HTML 미리보기

선택한 메일의 본문 내용을 텍스트와 HTML 형식으로 확인 가능.

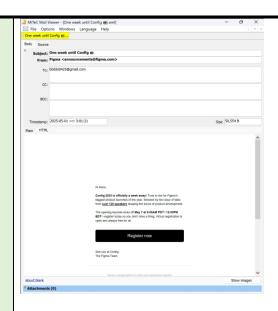
특정 메일 클릭 → 하단에서 HTML 본문 확인 → 링크, 이미지 포함 여부 분석

하단 영역 HTML 탭 활성화 (클릭)

Plain HTML





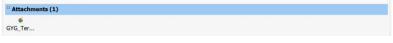


본문 탭(Plain / HTML): HTML 탭에서 시각적 본문 정상 출력됨

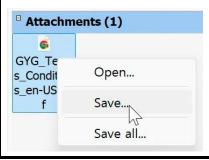
## 기능 3: 첨부파일 추출 및 저장

메일에 포함된 첨부파일을 확인하고 개별 또는 일괄 저장 가능.

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

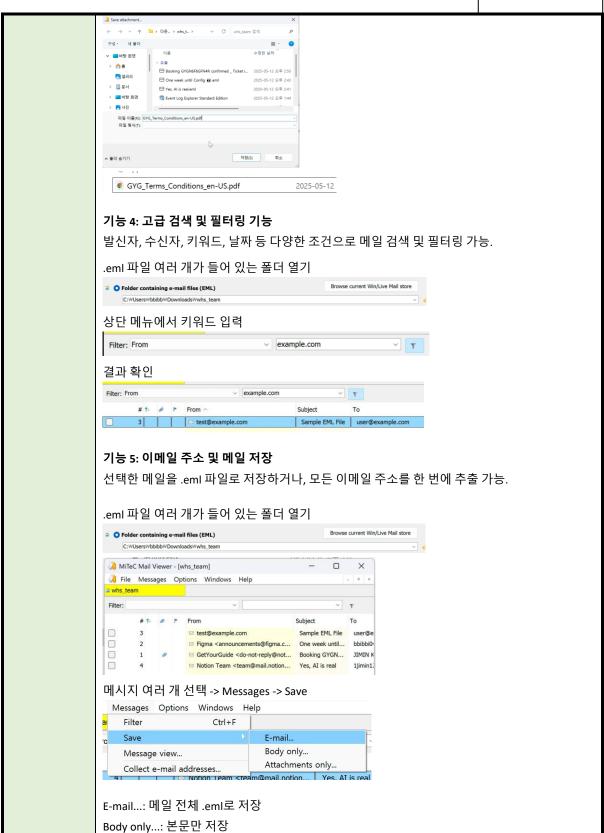


해당 파일 우클릭 -> save













Attachments only...: 첨부파일만 저장

## [WinPrefetchView] 매뉴얼

## 1. 툴 기본 정보

항목	내용			
툴 이름	WinPrefetchView			
ㅂ서킈데ㄱ기	시스템 설치/실행, 파일 사용/조작(일부)			
분석 카테고리	(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 간 단한 유틸리티이다.

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

## 3. 주요 기능 및 사용법

File → Prefetch 파일 저장, 종료

Edit  $\rightarrow$  항목 복사, 선택/해제 기능

View → 컬럼 선택, 새로고침 등 보기 옵션

Options → 시간, 경로 변경 옵션

Help → 프로그램 정보, 버전 확인

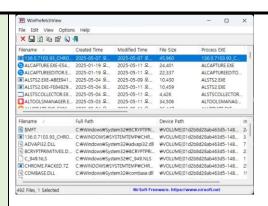
## F WinPrefetchView

File Edit View Options Help

기능 1: 기본 실행





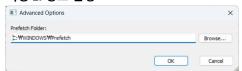


exe 파일을 실행시키면 pf 파일이 생성되고 pf 파일이 만들어진 시각은 exe 프로그램 최초 실행 시각을, pf 파일이 수정된 시각은 exe 프로그램의 마지막 실행 시각을 뜻한다.

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

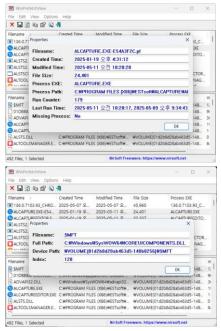
예) 사용자가 ALCAPTURE.EXE를 처음 실행한 시각과 마지막으로 실행한 시각을 파악할 수 있다.

#### 기능 2: 경로 변경



prefetch 파일을 추출해서 사용하는 경우에는 파일 경로를 수동으로 설정할 수 있다.
Options 메뉴 → Advanced Options 혹은 F9을 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



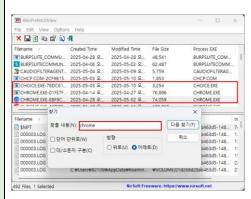




파일 항목을 더블 클릭하면, 파일 이름과 카운터(실행횟수), 생성 시간과 변경 시간, 경로, 마지막 실행시간 등의 상세 정보를 확인할 수 있다. 해당 프로그램을 삭제하거나 경로를 변경하더라도 프리패치는 삭제되지 않는다.

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

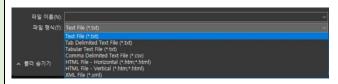
## 기능 4: 특정 단어 검색 (필터링)



Edit 메뉴  $\rightarrow$  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  $\rightarrow$  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 둘이다. 윈도우에서 최근 사용한 파일 및 폴더에 빠르게 접근이 가능하며, 사용자의 행위 파악에 도움이 된다.

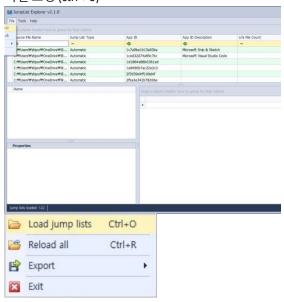
## 3. 주요 기능 및 사용법

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

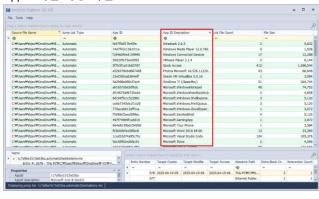
-파일을 불러오면 JumpListExplorer 가 각 파일의 AppID 를 식별하고 프로그램별로 그룹화하여 자동 정리한다.

-사건 당시 Word 문서를 열람했는지 확인하기 위해 해당 사용자의 JumpList 폴더에 서 .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







#### 기능 2: jumplist 아티팩트 분석

jumplist 내부 포함된 Ink 엔트리

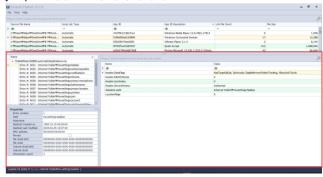


JumpListExplorer 는 각 항목 내부의 Ink 구조를 해석하여 파일 전체 경로, 실행 시간, 실행 횟수 등확인이 가능하다. (해당 소스 파일에 대한 경로, 점프리스트 타입, 해당 앱 ID 및 상세 이름, Ink 파일 클릭 수, 파일 크기)

각 항목에서 실행 횟수가 가장 높은 특정 문서를 식별 → 특정 파일이 자주 실행되었고, 사건 발생 시각과 실행시간이 겹치는 경우 해당 파일과 사건 간의 연관성이 존재한다.

#### 기능 3: jumpilst 상세 정보 확인

jumplist 내부 Ink 의 메타데이터



Target MAC 타임 정보, 호스트 이름, MAC 주소, 네트워크 공유 정보, 파일 상세 경로, Location Flags 등 매우 다양하고 중요한 정보들을 확인할 수 있다.

USB 드라이브에서 실행된 파일의 jumplist 분석 시, volume serial number 를 통해 외부 저장장치임을 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	-Windows 레지스트리 하이브 분석 도구. 키, 값,	.reg, .dat, .LOG1, .	정지윤
Explorer	- 파일 사용/조작	타임스탬프, 삭제된 항목 및 히든 데이터 분석 가능.	LOG2, .blf 등	
	- 사용자 행위	레지스트리 기반 행위 분석		
	- 데이터베이스 아티팩트			
Hashcat	- 파일 사용/조작	-다양한 해시 알고리즘 지원 GPU 기반 해시 크래킹 도구.	.hash, .txt, .potfile, .bin 등	정지윤
DC-1-		암호 해시 분석 및 복구 시 사용. 패스워드 기반 공격	_	
DCode	- 파일 사용/조작	-다양한 형식의 타임스탬프를 사람이 읽을 수 있는	.FILETIME, .Unix, .OLE, .WebKit 등	정지윤
		시간으로 변환. FILETIME, Unix Time 등 윈도우 아티팩트	.old, .webkit 8	
34 -177		시간 분석에 활용		
MailView	- 파일 사용/조작	- 이메일 파일을 분석하는 도구	.pst, .ost, .mbox, .e ml 등	강지민
		- 메일 본문, 송수신자 정보, 첨부파일 목록 등의	iii 6	
F+I		메타데이터를 추출 가능		
EventLog Explorer	- 시스템 설치/실행	- Windows 이벤트 로그(.evtx)를 시각적으로 분석하는	.evtx, .evt, .elf, .log 등	강지민
		도구	0	
HxD		- 주요 시스템 행위를 추적 가능	ove hin ima	71.11.61
IIXD	- 시스템 설치/실행	이진 파일, 디스크, 메모리를 16 진수로 분석하거나	.exe, .bin, .img, .d mp	김신아
	- 파일 사용/조작	편집할 수 있는 도구		
	- 사용자 행위			
	- 메모리 아티팩트			
Pdfstreamd	- 시스템 설치/실행	- 악성 PDF 문서를 정적 분석하기 위한 도구	.pdf, .FlateDecode	김신아
umper	- 시_ 함 글시/ 글링 - 파일 사용/조작	- 의용 PDF 문서를 용의 문의에게 위한 모두 - PDF 내부에 숨겨진 JavaScript, 임베디드 객체, exploit	, .js 등	
	- 씨글 시당/오크 - 사용자 행위	코드 등을 탐지하고 분석할 수 있는 기능 제공		
	- 세당시 8위			
ntfslogtrac	- 시스템 설치/실행	NTFS 파일 시스템에서 생성되는 \$LogFile, \$Usn]rnl,	\$LogFile,	김신아
ker	- 시_ H 글시/ 글링 - 파일 사용/조작	*MFT 핵심 로그 파일 분석 할 수 있는 도구	\$MFT, .evtx, RAW	V
	- 사용자 행위		등	
	- 메모리 아티팩트			
FTK	- 세소리 어디지드	디스크 이미징, 데이터 수집 및 분석, 무결성 검증 등을	E01, AD1, .mem	김예은
Imager	- 씨 프 마일 사용/조작		등	المراب
	- 메모리 아티팩트	, JE 1 ML - 1	1	
WinMerge	- 패오리 하다 그 - 파일 사용/조작	파일과 디렉토리 간의 차이를 시각적으로 비교하고	.txt, .c, .java, .docx	김예은
-	- 사용자 행위	병합할 수 있는 오픈 소스 도구	, binary 등	U-11C
ChromeCac	- 사용자 행위	- Google Chrome 브라우저의 캐시 파일을 분석하는 도구	.CACHE, .DATA, .I	김예은
heView	- 세트워크 아티팩트	- 웹 탐색 기록, 이미지, 동영상 등 캐시 데이터를 열람,	NDEX 등	۵۳۱۲
	4	복사,추출가능		
Volatility	- 시스템 설치/실행	메모리 덤프 파일을 분석하여 실행 중인 프로세스,	.raw, .mem, .bin, .	배영혜
-	- 파일 사용/조작	이젝션 코드, 사용자 활동, 네트워크 연결 등 다양한	dmp, .vmem 등	,, 0 4
	- 사용자 행위	휘발성 데이터를 추출할 수 있는 도구		
	- 메모리 아티팩트			
Wireshark	- 사용자 행위	실시간 네트워크 트래픽을 캡처하고 다양한 프로토콜을	.pcap, .pcapng, .ca	배영혜
	- 네트워크 아티팩트	계층별로 분석할 수 있는 도구	p 등	
Autopsy	- 시스템 설치/실행	- 디지털 증거를 수집·분석할 수 있는 오픈소스 포렌식	.img, .E01, .AFF, .d	서연정
	- 파일 사용/조작	도구	d, .sqlite 등	0
	- 사용자 행위			
	- 네트워크 아티팩트			
	- 메모리 아티팩트		1	
KAPE	- 시스템 설치/실행	- 아티팩트 파서 및 추출 도구	.evtx, .log, .csv, .pf,	안서진
	- 파일 사용/조작	- 파일 수집과 수집된 파일을 하나 이상의 프로그램으로	.lnk 등	
	- 사용자 행위	처리 가능		
WinPrefetc	- 시스템 설치/실행	- 시스템에 저장된 프리패치 파일을 읽고 저장된 정보를	.pf	안서진
hView	- 파일 사용/조작	표시하는 도구		
DB	- 파일 사용/조작	- 데이터베이스 아티팩트 분석 도구	.db, .sqlite, .csv 등	전소현
Browser	1	- 사용자 로그, 검색 기록, 위치 정보, 캐시 등을 조회	.30, .04.1.0, .03, 0	





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

## 3. 논문 요약 표

프로젝트 주제를 정하기 위해 각 팀원이 논문을 각각 3편씩 찾아보았으며, 논문을 협업  $\mathbb{E}$ , 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	관련 아티팩트 유형	논문 요약	방향성
	프로그램	(경로 포함)		
Forensic	Google	- 메신저 아티팩트	- Google	- 악용 가능성:
investigati	Meet	전송 기록, 캐시, 채팅 로그, 실행 기록, 메모리 덤	Meet 사용 중	Google Meet 메
on of	(Web 기	프 (실행 중 RAM에서 획득)	메모리와 브라	모리·브라우저에
Google	반 화상회	- 시스템 설치/실행 아티팩트 Prefetch, 레지스트	우저에 남는	남은 이메일, 채
Meet for	의 애플리	리, 이벤트 로그, LNK 파일	아티팩트를 식	팅, 파일 정보가
memory	케이션)	C:₩Users₩{User}₩AppData₩Roaming₩Microsof	별·분석하고,	피싱·사칭·유출에
and		t₩Windows₩Recent₩	이를 자동 추	악용될 수 있음.
browser		- 메모리 아티팩트: 프로세스 메모리, 명령어 이	출하는 Python	- 자동화 도구 개
artifacts		력 , 메모리 덤프 (실행 중 RAM에서 획득)	도구를 개발함.	발: 이메일, 토큰
		- 사용자 행위 아티팩트: 최근 명령어, 로그인 기		등 민감 정보를
		록, 탐색 기록		시그니처 기반으
		C:₩Users₩{User}₩AppData₩Local₩Google₩Chr		로 자동 추출·위
		ome₩User Data₩Default₩Cache₩		험도 분류.
노션프로	Notion	- 메신저 아티팩트: 전송 기록, 캐시, 채팅 로그,	- Notion 사용	- 악용 가능성:
그램 아티	(PC 및	실행 기록	중 PC와	Notion에 저장된
팩트 분석	Android	₩Users₩{User}₩AppData₩Roaming₩Notion₩n	Android 환경	이메일, 토큰, 삭
을 통한 위	앱)	otion.유	에서 수집된	제된 블록 등이
협 분석 및			사용자 정보와	계정 탈취·문서
대응방안		- 사용자 행위 아티팩트: 최근 명령어, 로그인 기	작업 내용이	유출·사칭에 악용
제시		록, 탐색 기록	암호화 없이	될 수 있음 자
		C:₩Users₩{User}₩AppData₩Roaming₩Notion₩	저장되어 있어	동화 도구 개발:
		notion.db	유출 위험이	디스크 이미지에
			크다는 점을	서 토큰, 삭제 기
			확인하고, 이를	록 등 위험 아티
			분석해 보안	팩트 자동 추출
			위협과 포렌식	및 분류 기능 개
			활용 가능성을	발.
			제시함.	
메신저형	ChannelT	- 메신저 아티팩트 : 전송 기록, 캐시, 채팅 로그,	- 팀 메신저 등	- 채팅 추출,
협업툴 어	alk	실행 기록	모바일 어플리	MAC 타임 분석,





	1			Т
플리케이		- 네트워크 아티팩트 : 방문 기록, 세션 토큰, 네	케이션 아티팩	이상 접속 탐지
션 아티팩		트워크 연결	트를 분석해	자동화 도구 개
트 분석 -		- 사용자 행위 : 최근 명령어, 로그인 기록, 탐색	사용자 행위와	발
ChannelT		기록	사용 내역 기	
alk을 중심		- 시스템 설치/실행 : Prefetch, 레지스트리, 이벤	반 보안 사고	
으로		트 로그, LNK 파일	증거 수집	
안드로이	Telegram	- 메신저 아티팩트 : 전송 기록, 캐시, 채팅 로그,	- Telegram X	- WAL, SQLite
드 환경에	Х	실행 기록	의 다양한 메	분석을 통한 데
서의		/data/data/org.thunderdog.challegram/files/tdli	시지 유형과	이터 변화 추적
Telegram		b → 경로에 위치하는 dp.sqlite파일 →	로그를 분석하	
X 메신저		messages 테이블	여 WAL 파일	
아티팩트			을 통한 삭제	
분석		- 사용자 행위 아티팩트: 최근 명령어, 로그인 기	메시지 복구	
		록, 탐색 기록	가능성을 확인	
		/media/0/Android/data/org.thunderdog.challeg		
		ram/files		
화상 회의	GotoWeb	- 메신저 아티팩트:	- 애플리케이	- 실시간 화상회
애플리케	inar,	C:₩Users₩ <username>₩Documents₩ChatLog[</username>	션 데이터 특	의 데이터 수집
이션	GoToMee	회의명]YYYY_MM_DD HH_mm.rtf	성과 차이 비	자동화 툴 개발
GoToWeb	ting	- 파일 사용/조작: C:₩Users₩ <user< th=""><th>교, 데이터 수</th><th></th></user<>	교, 데이터 수	
inar 및		name>\Documents	집 및 분석 부	
GoToMee		- 사용자 행위	족	
ting 아티				
팩트 분석				
윈도우 환	JANDI(잔	- 메신저 아티팩트: Cache 폴더	- 잔디의 아티	- JANDI 내부 악
경에서의	디)	- 시스템 설치/실행:	팩트 수집 및	용 기능 탐색 및
협업 도구		C:₩Users₩[USERNAME]₩AppData₩Roaming₩J	데이터 분석	분석 자동화 툴
잔디 아티		ANDI	기법 제시, API	개발
팩트 수집		- 사용자 행위: Cache와 Local Storage 폴더 하위	기반 데이터	
및 분석 연		에 존재	획득 방법 제	
구			안	
협업 툴의	Microsoft	- 메신저 아티팩트	- 디지털 포렌	- 협업툴 및 다양
사용자 행	Teams	%APPDATA%₩Microsoft₩Teams₩IndexedDB₩	식 분석에서	한 운영 환경에
위별 아티		https_teams.microsoft.com_0.indexeddb.leveldb	운영 환경별	대한 확장 연구
팩트 분석		- 시스템 설치/실행	증거 확보 중	필요
연구 -		%APPDATA%₩Microsoft₩Teams - 사용자 행위	요성 강조	
Microsoft		%APPDATA%₩Microsoft₩Teams₩Local		
Teams		Storage , %APPDATA%₩Microsoft₩Teams₩Ind		
		exedDB		
협업 툴 아	잔디, 네이	- 메신저 아티팩트	- 협업 툴 사용	- 아티팩트 자동
티팩트 분	버 웍스	%LOCALAPPDATA%₩Microsoft₩Teams₩main.d	증가로 인한	파싱 도구 개발
석 및 삭제		b, %LOCALAPPDATA%₩Microsoft₩Teams₩chat	데이터 유출	
된 데이터		.db	위험 분석, 삭	
복구 연구			제 메시지 복	
		- 시스템 설치/실행 아티팩트	구 가능성 확	
		₩Windows₩AppCompat₩Programs₩Amcache.	인	
		h		
		- 사용자 행위 아티팩트		
		C:₩Windows₩System32₩winevt₩Logs		
Windows	Telegram	- 사용자 행위 아티팩트	- 메모리 덤프	- 메모리 기반 포





Telegram Desktop 애플리케 이션에서 검색 가능 한 메모리 아티팩트 추출 및 분	Desktop	- 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 내 용, 삭제된 흔 적을 추출하는 방법 제시	렌식 도구 개발
Microsoft Office 진 단 로그 분 석 및 포렌 식 활용 방 안	Microsoft Word, Excel, PowerPoi	- 시스템 설치/실행 아티팩트: Prefetch, Amcache.hve, MFT, 임시파일 - 사용자 행위 아티팩트: Pdod, \$UsnJrnl	- Microsoft Office 진단 로 그를 활용해 작업 이력 추 적 가능성 분	- 진단 로그를 통한 문서 작업 흐름 복원 도구 개발
다지털 상 호작용 디 코딩: TeamView er 포렌식 아티팩트 연구	TeamVie wer	- 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₩tvcha tfilecache.db AppData₩Local₩TeamViewer₩Database₩tvcha tfiledownloadhistory.db - 메모리 아티팩트 : 동적 비밀번호, 채팅 내역 - 네트워크 아티팩트 TeamViewer15_Logfile.log ( Android ↔ Windows 간 접속 IP 기록) - 데이터베이스 아티팩트 AppData₩Local₩TeamViewer₩Database₩tvcha tfilecache.db AppData₩Local₩TeamViewer₩Database₩tvcha tfiledownloadhistory.db	- Windows와 Android에서 TeamViewer 사용 시 남는 아티팩트 분석	- TeamViewer 사용 시 로그와 메모리 덤프 파 싱 도구 개발
디지털 포 렌식 관점 에서의 협 업 도구 네 이버웍스 의 데이터 수집 및 분 석	네이버웍 스	- 채팅 기록 - 파일 공유 - 캘린더/일정 - 사용자 계정 정보 - 삭제된 데이터, 로그 파일 C:₩Users[Username]₩AppData₩Local₩WorksM obile₩NaverWorks₩	- 네이버웍스 에서 생성되는 다양한 사용자 행위 기반 데 이터를 수집하 고 분석함	- 안티포렌식 기 능 우회 기술 연 구 및 자동 분석 도구 개발
디지털 포 렌식 관점 의 네이버 밴드 사용 자 행위 수 집 및 분석 연구	네이버 밴 드 (Android 환경)	- 메신저 아티팩트: /data/data/com.nhn.android.band/databases/ch at_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 환 경에서 네이버 밴드의 로컬 데이터와 API 를 분석하여 사용자 정보, 채팅 기록 등 을 수집	- 악용 가능성: 채팅, 이미지 캐 시, user/band ID 등을 통한 신원 도용 및 삭제 대 화 복원





# 인스턴트 메신저

제목	분석 대상	관련 아티팩트 유형	논문 요약	방향성
	프로그램	(경로 포함)		
포렌식 관 점에서의 Element 인스턴트 메신저 아 티팩트 분	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
석				
윈도우 환 경에서 카 카오톡 데 이터 복호 화 및 아 티팩트 분 석 연구	KakaoTalk (카카오톡) PC 버전	- 파일 사용/조작: %LocalAppData%₩Kakao₩Ka kaoTalk₩users₩chat_data - 사용자 행위: %LocalAppData%₩Kakao₩Ka kaoTalk₩users - 메신저 아티팩트: %LocalAppData%₩Kakao₩Ka kaoTalk₩users₩chat_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₩ele 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 안드로이 드 환경에 서의 WeChat 메신저 아 티팩트 분 석 연구	WeChat (인스턴트 메신저)	채팅 기록, Moments, 타임캡 슐, 사용자 계정 정보, 데이터 베이스 파일	- Windows와 Android 환경 에서 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 자동으로 추출하는 메모리 기반 포렌식





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

## 웹

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

## 기타

제목	분석 대상	관련 아티팩트 유형(경로 포함)	논문 요약	방향성





	1			
	프로그램			
안드로이	네이버 지	- 사용자 행위 아티팩트	- 지도 애플리커	베이 GPS 데이터
드 환경에	도, TMAP,	databases 디렉터리의 bookmark.db, search-	션에 분석된 결	
서의 지도	카카오 맵	history.db, route-history.db, subwayMap.db파	의 범위는 한정	· ·
애플리케	PC 버전	일	아티팩트가 변	경 그파일, 위
이션 아티		shared_prefs 디렉터리 내 pubtrans_cache.xml파	되거나 애플리?	게 치기록 캐
팩트 분석		일	이션마다 저장!	되 시기반패
및 복호화		NativeNaviDefaults.xml 파일	는 데이터가 다	양 턴 분석
방안 연구			함.	
			- 최신 버전에서	너의
			데이터 수집 방	안
			연구 필요	
원격 제어	TeamVie	- 메신저 아티팩트: app.db(AirDroid)	- Android 기반	원 악용 가능
용 어플리	wer,	- 네트워크 아티팩트: TVLog.html(TeamViewer),	격 제어 앱의 회	르컬 성: 접속 기
케이션에	AnyDesk,	account_backup(AirDroid),	아티팩트를 분성	석 록, 계정, 전
서의 아티	AirDroid	main_preference_bk(AirDroid)	하여 제어자 정	
팩트 수집	(모두	- 시스템 설치/실행 아티팩트: client.conf	파일 전송·권한	
및 분석	Android	(TeamViewer),	청 등 핵심 데이	
	환경)	com.sand.airdroid_preference.xml(AirDroid)	를 식별	
	•	- 파일 사용/조작 아티팩트: downloads/	_	
		(AnyDesk), TVLog.html(TeamViewer)		
		- 사용자 행위 아티팩트:		
		TVLog.html(TeamViewer), app.db(AirDroid),		
		recursive_file_index_phone(AirDroid)		
무 설치 프	Opera,	- 메모리 아티팩트: 경로 X, 분석 도구는 Hex	- 포터블 프로그	1램 비전통적 아
로그램에	Notepad	Fiend, Volatility	에서의 사용자	
서의 사용	++	- 시스템 설치/실행: C:₩Windows₩Prefetch	위 분석 방안 제	
자 행위 아		- 파일 사용/조작: C:₩Windows₩Temp	시, 메모리 분석	· ·
티팩트 분		- 사용자 행	통해 증거 수집	
석		위: %AppData%₩Roming₩Microsoft₩Windows	능	ession 등)를
		₩Recent	-	파싱할 도구
				개발
폴라리스	폴라리스	- 시스템 설치/실행 아티팩트 :	- Polaris Office	
오피스 포	오피스	C:₩Windows₩Prefetch₩[폴라리스 오피스 설치	용시 Windows	
렌식 아티	. –	파일명].pf (prefetch)	macOS에서 생	
팩트에 관		- 사용자 행위 아티팩트 :	되는 아티팩트	
한 연구		C₩HKCU₩Software₩Infraware₩PolarisOffice의	분석하여 작업	
		"FirstHomeAccessTime" 정보	그 DB 확인	사용자 행위
		- 파일 사용/조작 아티팩	1-	재구성
		=: %UserProfile%₩AppData₩Roaming₩Polari		", 5
		sOffice\Database\InfrawareRecentFiles.sqlite		
		(최근 사용된 파일 목		
		록) , %UserProfile%₩AppData₩Roaming₩Polari		
		sOffice\Database\RecordCommand2.sqlite (작		
		업 과정에 관여된 모든 파일에 대한 액세스 흔		
		적), %UserProfile%₩AppData₩Roamin		
		g\PolarisOffice\Database\InfrawareAutoReco		
		ver.sqlite (자동 복구 정		
		上), %UserProfile%₩AppData₩Roaming₩Polaris		
		Office₩Recover₩Slide₩파일		
		명, %UserProfile%₩AppData₩Roaming₩Polaris		
		C, 7003cm rome 70m pp Data modifing m Olans		





취약점 별 아티팩트 사례 분석 을 통한 아 티팩트 그 룹핑 연구	Adobe Flash Player	Office\Recover\Word\Pi\Pi\Bigs , %UserProfile%\Pi\AppData\Roaming\Polari sOffice\Recover\Sheet\Pi\Bigs	- Adobe Flash Player의 취약점 활용 침해사고 사 례 분석 - 초기 침해 대응 을 위한 '아티팩트 그룹핑' 방안 제시	CVE 취약점 공격 발생 시 Prefetch 및 Web Cache 분석 을 통한 공 격 흔적 확 보
Conversational Alforensics: A case study on ChatGPT, Gemini, Copilot, and Claude	ChatGPT, Gemini, Copilot, Claude	₩macromedia.com₩support₩flas hplayer₩sys(Setting Info)  - 메신저 아티팩트: C:₩Users₩ <user>₩Downloads₩chatgpt_export _<yyyy-mm-dd>₩conversations.json  - 네트워크 아티팩트: C:₩Users₩<user>₩Documents₩Wireshark₩ch atgpt_traffic.pcap</user></yyyy-mm-dd></user>	- 대화형 AI 플랫폼의 대화 이력과 메타데이터를 수 집·분석하여 악성 코드 제작 행위를 입증할 수 있는 아 티팩트 식별	대화형 AI에 입력된 프롬 프트와 삭제 된 대화 로 그를 분석하 여 이상 행 위 탐지 모 델 개발

활동사진 (회의 사진 등)





## 2025.05.06 회의



2025.05.10



2025.05.12



2025.05.13

