

# [Chat GPT 분석 보고서]

## [아티팩트 상세 분석 보고서]



작성일	2025.06.06
작성자	강지민, 김예은, 배영혜, 안서진, 전소현, 정지윤
검토자	김예은

# 목차

<b>I. 기본 정보 .....</b>	<b>3</b>
<b>II. 프로그램 개요 .....</b>	<b>3</b>
1. 프로그램 목적 .....	3
2. 주요 기능 요약 .....	3
<b>III. 분석 목적 .....</b>	<b>3</b>
<b>IV. 분석 도구 정보 .....</b>	<b>4</b>
<b>V. 해시값 .....</b>	<b>4</b>
<b>VI. 분석 아티팩트 .....</b>	<b>5</b>
1. 시스템 설치/실행 아티팩트 .....	5
2. 사용자 행위 아티팩트 .....	7
3. 파일 사용/조작 아티팩트 .....	14
4. 메모리 아티팩트 .....	20
5. 네트워크 아티팩트 .....	22
6. 메신저 아티팩트 .....	28
<b>VII. 분석 차별점 .....</b>	<b>30</b>
<b>VIII. 분석 요약 .....</b>	<b>31</b>
<b>IX. 향후 계획 .....</b>	<b>34</b>
<b>X. 참고 문헌 .....</b>	<b>35</b>

## I. 기본 정보

프로그램 범주	LLM
프로그램	Chat GPT
버전	1.2025.139.0
다운로드 경로	<a href="https://openai.com/chatgpt/download/">https://openai.com/chatgpt/download/</a>

[표1] 기본정보

## II. 프로그램 개요

### 1. 프로그램 목적

프로토타입 대화형 인공지능 챗봇으로 대규모 언어 모델(LLM)을 사용하여 사용자의 질문에 대한 자연스러운 응답을 생성한다.

### 2. 주요 기능 요약

단순 채팅뿐 아니라 웹을 활용한 검색, 이미지 생성, 데이터 분석 등의 기능도 지원하여 다양한 형태의 정보 탐색을 가능하게 한다. 깊은 추론으로 어려운 문제를 해결하는 것 또한 가능하다.

## III. 분석 목적

본 분석은 정상적인 프로그램인 Chat GPT이 악의적인 목적으로 활용할 수 있다는 시나리오를 기반으로, 사용 시 생성되는 아티팩트를 포렌식 측면에서 식별하고, 관련 파일 및 레지스트리 등의 저장 경로를 분석하여 디지털 증거 확보 가능성을 평가하는 것을 목적으로 한다.

## IV. 분석 도구 정보

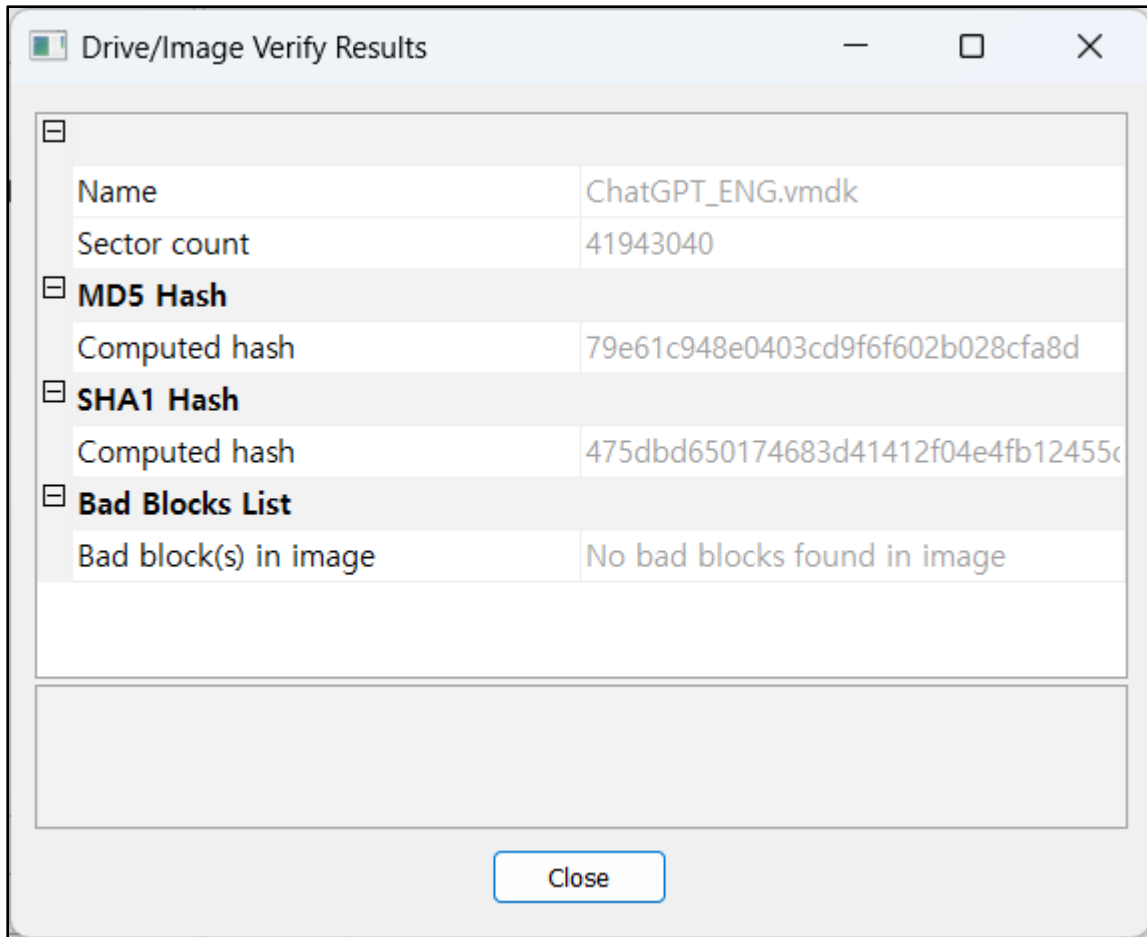
도구명	버전
FTK Imager	v4.7.3.81
WinPrefetchView	v1.37
ChromeCacheview	v2.52
Autopsy	v4.22.1
Registry Explorer	v2.1.0
NTFS Log Tracker	v1.8
HxD	v2.5
Wireshark	v4.4.6
DB Browser for sqlite	v3.13.1
levelDB Viewer	

[표2] 분석도구

## V. 해시값

해시	값
MD5	79e61c948e0403cd9f6f602b028cfa8d
SHA1	475dbd650174683d41412f04e4fb12455c87ced7

[표3] 해시값



[그림 1] FTK Imager로 확인한 vmdk 해시값

## VI. 분석 아티팩트

### 1. 시스템 설치/실행 아티팩트

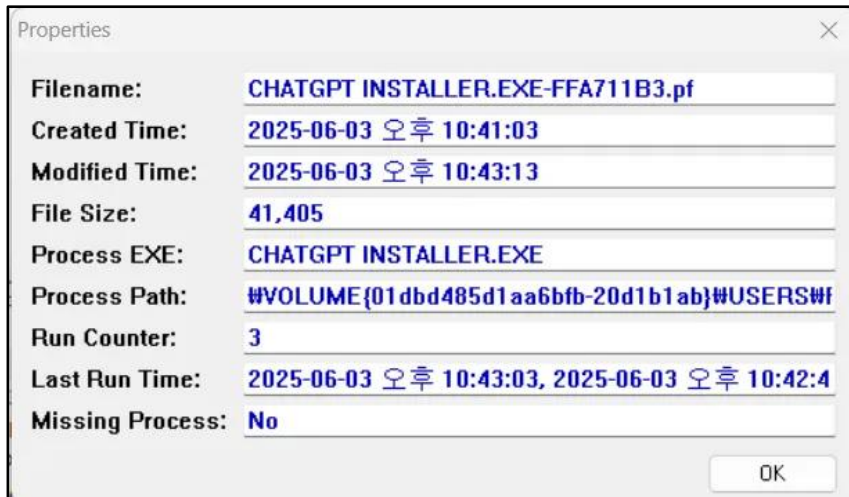
#### 1) 설치 Prefetch 기록

(1) 경로: C:\Windows\Prefetch\CHATGPT INSTALLER.EXE-FFA711B3.pf

(2) 분석 내용: 25.06.03 22:41~22:43, 약 2분에 걸쳐 ChatGPT Installer.exe 파일이 총 3회 실행된 흔적을 확인할 수 있다.

Evidence Tree		File List			
	Performance	Name	Size	Type	Date Modified
	PLA	BACKGROUNDTRANSFERHOST.EXE-621DBAF8.pf	8,433 (9 KB)	Regular File	2025-06-03 오후 1:23:08
	PolicyDefinitions	BYTECODEGENERATOR.EXE-FB938A53.pf	5,916 (6 KB)	Regular File	2025-06-03 오후 1:12:40
	Prefetch	CHATGPT INSTALLER.EXE-FFA711B3.pf	41,405 (41 KB)	Regular File	2025-06-03 오후 1:43:13
	PrintDialog				
	Provisioning				

[그림 2] FTK Imager로 확인한 prefetch파일



[그림 3] WinPrefetchView로 확인한 prefetch파일

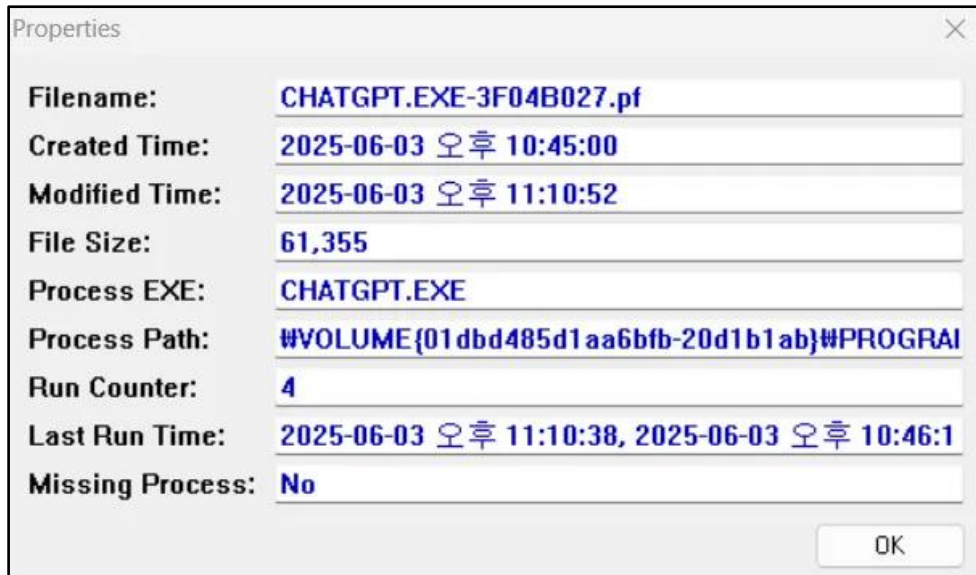
## 2) 실행 prefetch 기록

(1) 경로: C:\Windows\Prefetch

(2) 분석 내용: C:\Windows\Prefetch 경로에서 7개의

CHATGPT.EXE-\*.pf 프리패치 파일이 확인할 수 있다. 대표적으로 CHATGPT.EXE-3F04B027.pf는 분석 결과에 따르면, 처음 실행된 시각은 2025.06.03 10:45이고 가장 최근 실행된 시각은 2025.06.03 11:10이다. 또한 프로그램 누적 실행 횟수는 4회인 것을 알 수 있다.

WinPrefetchView			
File Edit View Options Help			
Filename	Created Time	Modified Time	File Size
CHATGPT INSTALLER.EXE-FFA711B3.pf	2025-06-03 오후 10:41:03	2025-06-03 오후 10:43:13	41,405
CHATGPT.EXE-3F04B027.pf	2025-06-03 오후 10:45:00	2025-06-03 오후 11:10:52	61,355
CHATGPT.EXE-3F04B028.pf	2025-06-03 오후 10:45:01	2025-06-03 오후 11:16:15	27,653
CHATGPT.EXE-3F04B029.pf	2025-06-03 오후 10:45:00	2025-06-03 오후 11:10:52	13,347
CHATGPT.EXE-3F04B02A.pf	2025-06-03 오후 10:45:00	2025-06-03 오후 11:10:52	11,491
CHATGPT.EXE-3F04B02B.pf	2025-06-03 오후 10:45:00	2025-06-03 오후 11:10:52	5,704
CHATGPT.EXE-3F04B02F.pf	2025-06-03 오후 10:46:49	2025-06-03 오후 10:46:49	9,312



[그림 4,5] WinPrefetchView로 확인한 prefetch파일

### 3) 다운로드 기록

- (1) 경로: C:\Users\Wforensic\Downloads\ChatGPT Installer.exe
- (2) 분석 내용: 25.06.03 22:40, Microsoft Store 웹페이지를 통해 다운로드된 것을 확인할 수 있다.



[그림 6] Autopsy로 확인한 History기록

## 2. 사용자 행위 아티팩트

### 1) 사용자 정보

- (1) 경로:

C:\Users\Wforensic\AppData\Local\Packages\OpenAI.ChatGPT  
 Desktop\_2p2nqsd0c76g0\LocalCache\Roaming\ChatGPT\Cache\Cache\_Data

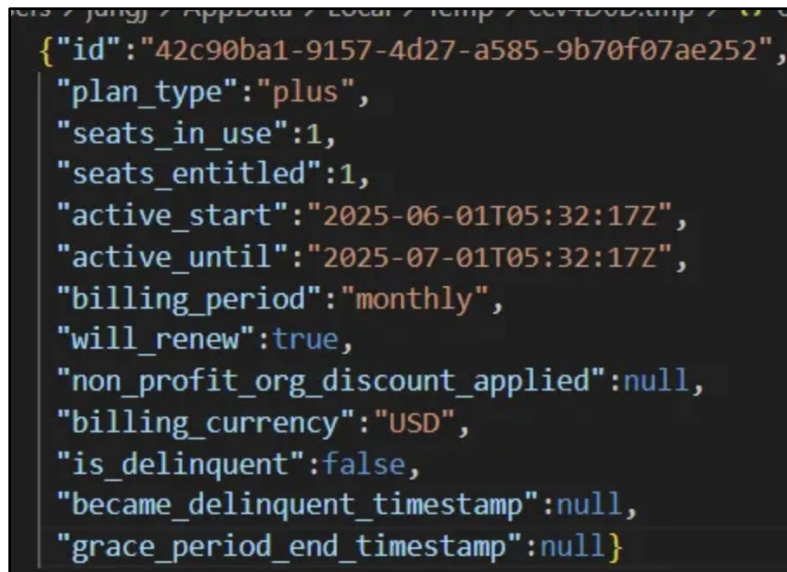
(2) 분석 내용: ChromeCacheView를 사용하여 해당 Cache\_Data 파일을 추출하여 사용자에게 대한 정보를 분석 할 수 있다.

① 1/0/<https://chatgpt.com/api/auth/csrf>의 csrf.json 파일을 통하여 해당 사용자의 csrf 토큰을 확인할 수 있다.



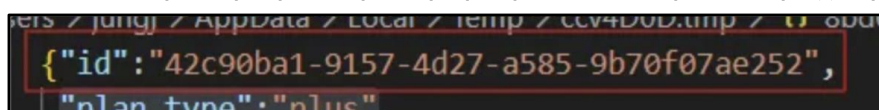
[그림 7] csrf.json 파일로 확인한 csrf 토큰

② 1/0/<https://chatgpt.com/backend-api/client/strings>의 strings.json 파일을 통하여 사용자의 chatGPT 구독 정보를 보여주는 메타데이터를 확인할 수 있다.



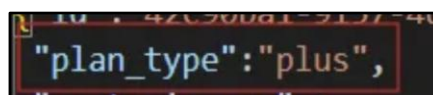
[그림 8] strings.json 파일

- 해당 구독을 식별하기 위한 ID를 확인할 수 있다.



[그림 9] strings.json 파일로 확인한 id 값

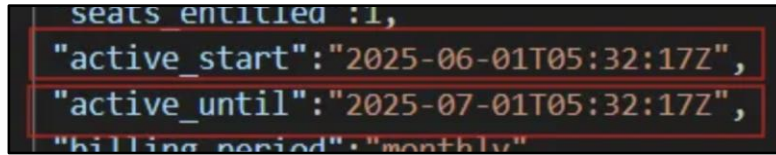
- 현재 사용중인 요금제가 "Plus" 요금제라는 것을 확인할 수 있다.



[그림 10] strings.json 파일로 확인한 plan\_type 값



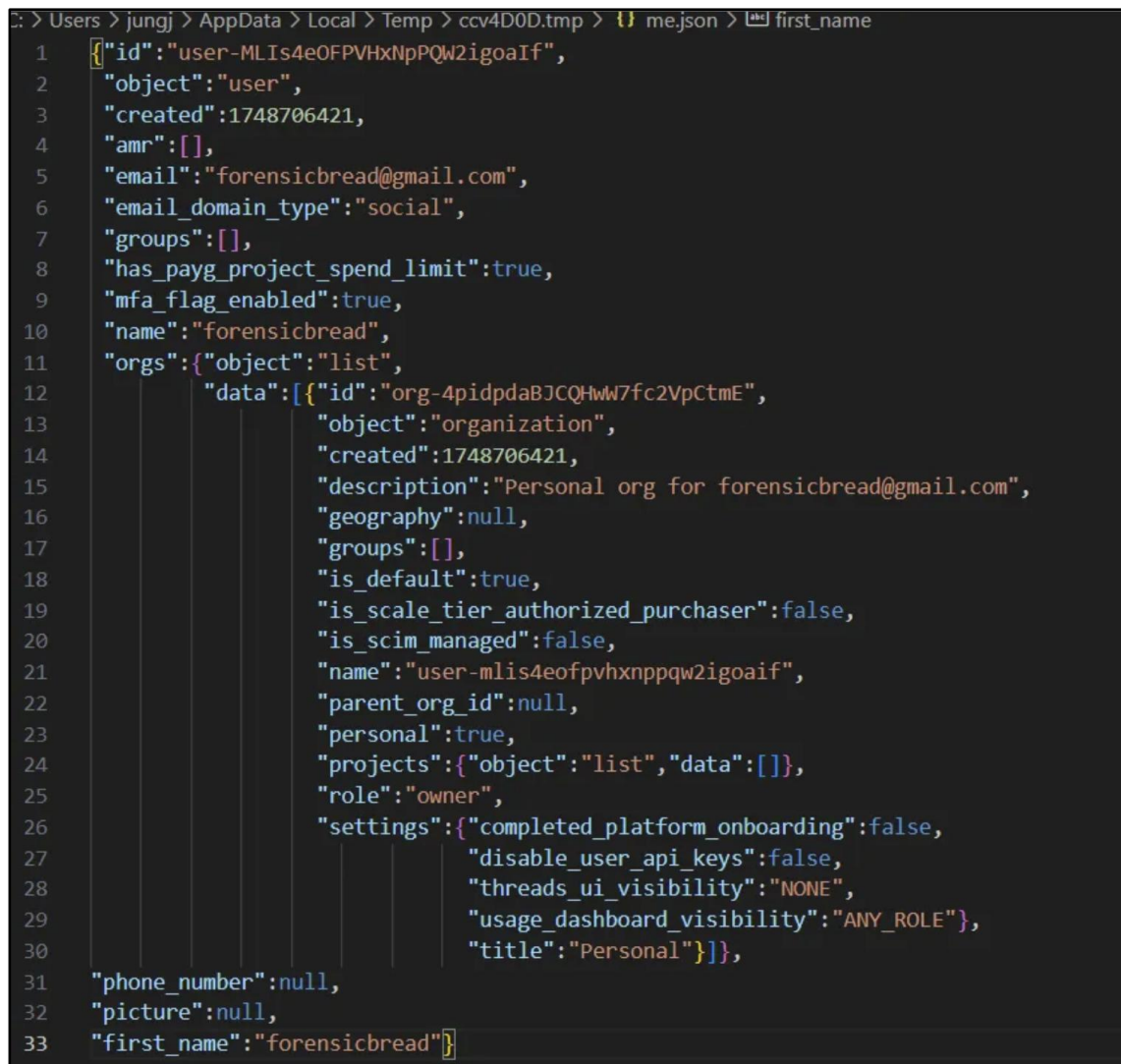
- 구독이 활성화된 시점과 구독 기간이 끝나는 시점을 확인할 수 있다.



A screenshot of a JSON file showing subscription details. The fields 'active\_start' and 'active\_until' are highlighted with red boxes. 'active\_start' is '2025-06-01T05:32:17Z' and 'active\_until' is '2025-07-01T05:32:17Z'. Other visible fields include 'seats\_entitled': 1 and 'billing\_period': 'monthly'.

[그림 11] strings.json 파일로 확인한 active\_start 및 active\_until 값


- ③ 1/0/<https://chatgpt.com/backend-api/me>의 me.json 파일을 통하여 ChatGPT 계정 정보를 확인할 수 있다.



A screenshot of a code editor showing the contents of a me.json file. The file is a JSON object representing a user profile. The 'id' field is 'user-MLIs4e0FPVHxNpPQW2igoaIf'. The 'email' field is 'forensicbread@gmail.com'. The 'name' field is 'forensicbread'. The 'orgs' field contains an array of organizations, with the first one being 'org-4pidpdaBJCQHwW7fc2VpCtmE'. The 'first\_name' field is 'forensicbread'.

[그림 12] me.json

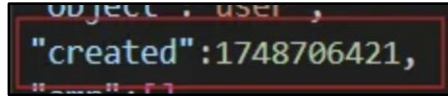
- 계정을 식별하기 위한 ID 확인할 수 있다.



A screenshot of the 'id' field in the me.json file, highlighted with a red box. The value is 'user-MLIs4e0FPVHxNpPQW2igoaIf'.

[그림 13] me.json 파일로 확인한 id 값

- Unix 타임스탬프로 계정이 생성된 시간 확인 가능. 해당 값은 UTC 기준 "2025-06-01 05:27:01" 로 해석할 수 있다.



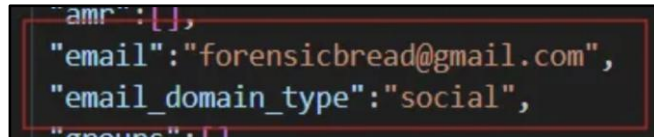
```

"created":1748706421,

```

[그림 14] me.json 파일로 확인한 created 값

- 해당 계정의 이메일 정보 확인할 수 있다.



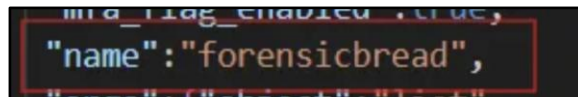
```

"email":"forensicbread@gmail.com",
"email_domain_type":"social",

```

[그림 15] me.json 파일로 확인한 email 및 email\_domain\_type 값

- 사용자의 이름을 확인할 수 있다.



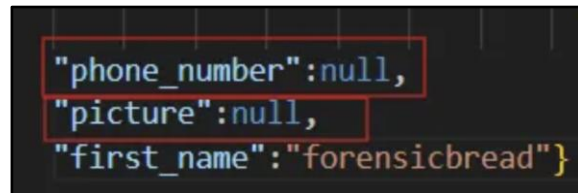
```

"name":"forensicbread",

```

[그림 16] me.json 파일로 확인한 name 값

- 사용자 계정의 전화번호와 프로필 사진 URL 확인할 수 있다.



```

"phone_number":null,
"picture":null,
"first_name":"forensicbread"}

```

[그림 17] me.json 파일로 확인한 phone\_number 및 picture 값

## 2) LevelDB의 사용자 정보

### (1) 경로:

C:\Users\forensic\AppData\Local\WPackages\OpenAI.ChatGPT

Desktop\_2p2nqsd0c76g0\LocalCache\Roaming\ChatGPT\Local Storage\leveldb\00003.log

- (2) 분석 내용: 해당 사용자의 sessionId 정보 확인 가능하다. 또한 startTime과 lastUpdate값을 통해 세션이 시작된 시점과 마지막으로 갱신된 시점을 확인할 수 있다.

- ① sessionId: e3d82b73-5149-47f2-9a11-447cc6f12d55
- ② startTime: 1748958296141 (25.06.03 22:44:56 (KST))

③ lastUpdate: 1748960879276 (25.06.03 23:27:59 (KST))

```
Key: _https://chatgpt.comstatsig.session_id.1792610830
Value: {"sessionId":"e3d82b73-5149-47f2-9a11-447cc6f12d55", "startTime":
1748958296141, "lastUpdate":1748960879276}
```

[그림 18] 파일로 확인한 sessionId, startTime, lastUpdate 값

### 3) Local State

#### (1) 경로:

C:\Users\forensic\AppData\Local\Packages\OpenAI.ChatGPT  
Desktop\_2p2nqsd0c76g0\LocalCache\Roaming\ChatGPT\Local  
State

- (2) 분석 내용: 해당 Local State 파일은 OpenAI ChatGPT 데스크탑  
애플리케이션의 환경설정 및 암호화 관련 메타데이터를 저장하는  
JSON 형식의 파일로, 주요 보안 파라미터가 기록된다.  
audit\_enabled가 true라는 것을 통하여 보안 로그 기록 기능이  
활성화되어 있음을 알 수 있고, encrypted\_key를 통하여 프로그램  
내부 데이터(쿠키, 세션 토큰 등)의 암호화 및 복호화에 사용되는  
마스터키가 암호화되어 저장되어 있음을 알 수 있다.

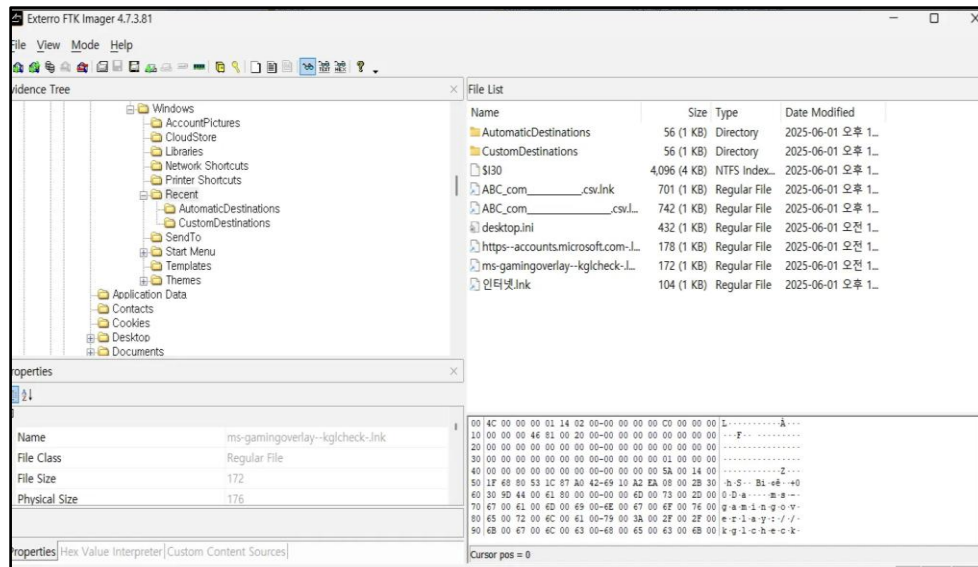
```
{"os_crypt":{"audit_enabled":true,"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDA  
T8KX6wEAAAAuBA5/6LOkRp4s2+ zF2ooREAAAABIAAABDAGgAcgBvAG0AaQB1AG0AAA  
AQZgAAAAEAACAAAADJXpBM46f7IVIgMgz2HkyomAo59Y7EKOLZJgtGD/pftAAAAAOGA  
AAAAIAACAAAABbocHoed2DJwuYvIxXZi54xMRmG3SypGaWmkRZnXyqlDAAAAC5usBPZ2  
tFNA1qxb8c9zZF/px1Vz7i20NOdwguJg6dzIHvMv/sw56QSqiNPsxWoYIAAAAArbW9X0H  
MVcxbljOqp+ BJGEzPIFPRQaFBIT0LykB6o3hGkISGnr2wfiUCYMDIgX9FW8EjI86ihDL34ItEgqPz  
Q=="}}
```

### 4) 사용자 접근 기록

#### (1) 경로:

C:\Users\forensic\AppData\Roaming\Microsoft\Windows\Recent

- (2) 분석 내용: 사용자가 해당 파일에 접근한 시간을 바탕으로 사용자가 최근에 열어본 폴더나 이미지, 파일 접근 기록 등을 확인할 수 있다.



[그림 19] Recent 파일에 위치한 흔적

## 5) 사용자 계정 확인

- (1) 경로: HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList
- (2) 분석 내용: 레지스트리 ProfileList 경로에서 사용자 계정인 SID S-1-5-21-300993033-1413454077-3185911941-1001 을 확인할 수 있고, 이는 C:\Users\forensic 에 연결되는 것을 알 수 있다.

2025-06-03 14:29:23	S-1-5-21-1233276306-1788-545777-1629842736-1001	C:\Users\forensic	2025-06-03 13:29:38	2025-06-03 14:29:23
---------------------	---	-------------------	---------------------	---------------------

[그림 20] Registry Explorer로 확인한 사용자 계정 정보

## 6) 사용자 로그인 기록 (웹)

- (1) 경로: \Users\forensic\AppData\Local\Microsoft\Edge\User Data\Default\History
- (2) 분석 내용: 25.06.03 22:45, 사용자 계정이 Microsoft Edge 브라우저를 통해 OpenAI 로그인 페이지(auth.openai.com)에 접속한 흔적을 확인할 수 있다. 또한, log-in, log-in/password,

/auth 등의 경로 접속을 통해 사용자가 로그인을 시도하고 인증 절차를 진행했음을 확인할 수 있다.

History	1	https://auth.openai.com/api/accounts/authorize?client_id...	2025-06-03 22:45:13 KST	https://auth.openai.com/api/accounts/authorize?client...	로그인 - OpenAI
History	1	https://auth.openai.com/login	2025-06-03 22:45:13 KST	https://auth.openai.com/login	로그인 - OpenAI
History	1	https://auth.openai.com/login/password	2025-06-03 22:45:58 KST	https://auth.openai.com/login/password	로그인 - OpenAI

[그림 21] Autopsy로 확인한 로그인 기록

## 7) 사용자 로그인 인증

### (1) 경로:

C:\Users\Wforensic\AppData\Local\Packages\OpenAI.ChatGPT-Desktop\_2p2nqsd0c76g0\LocalCache\Roaming\ChatGPT\Cache\Cache\_Data\data\_1

### (2) 분석 내용: 25.06:03 22:46:19, OAuth 인증 플로우의 최종 단계인 Callback URL 요청이 기록되었으며, code 파라미터를 통해 인증 서버(Auth0)로부터 로그인 승인 코드를 전달받은 것을 확인할 수 있다.

code=ac_6jPdmRV8sOPgqVxCaE7TVcxj0rME01JuxNO_pyTA...	1/0/https://chatgpt.com/api/auth/callback/openai-sidetr...	0	2025-06-03 오후 10:46:19	2025-06-03 오후 10:46:19
---	--	---	------------------------	------------------------

[그림 21] Chrome CacheView로 확인한 인증 정보

Name	Location	Modified Time	Change Time	Keyword P
data_1	/img_WHS_ChatGPT.E01/vol_vol6/Users/forensic/App...	2025-06-03 23:28:16 KST	2025-06-03 23:28:16 KST	<1/0/https:
<div> <div>Hex</div> <div>Text</div> <div>Application</div> <div>File Metadata</div> <div>OS Account</div> <div>Data Artifacts</div> <div>Analysis Results</div> <div>Context</div> <div>Annotations</div> <div>Other Occurrences</div> </div> <div> <div>Strings</div> <div>Extracted Text</div> <div>Translation</div> </div> <div> <div>Page: 1 of 1 Page</div> <div>Matches on page: 1 of 1 Match</div> <div>100%</div> <div>Reset</div> </div> <div> <div>8acA</div> <div>1/0/https://chatgpt.com/api/auth/callback/openai-sidetr...</div> <div>DshugqnQstq3bjPvATzFRjY6URPoYX42b1z060VM0zc&amp;state=wYxcbAA1YGfOtsqGiTIXmUubqNBfKAb-hEKTl_7cGv4&amp;window_style=main_view</div> </div>				

[그림 22] Autopsy로 확인한 인증 정보

## 8) 모델 변경 기록

### (1) 경로:


C:\Users\Wforensic\AppData\Local\Packages\OpenAI.ChatGPT-Desktop\_2p2nqsd0c76g0\LocalCache\Roaming\ChatGPT\Cache\Cache\_Data\data\_1



- (2) 분석 내용: 사용자가 25.06.03 10:46:30에 gpt-4o 모델을 사용한  
 걸 확인할 수 있고, 이후 25.06.04 11:10:54에는 gpt-4-1로 모델을  
 변경한 것도 확인된다.

limit=8&use_v2=true&model_slug=gpt-4-1.customization	1/0/https://chatgpt.com/backend-api/prompt_library/?limit=8&use_v2=true&model_slug=gpt-4-1	application/json	2,116	2025-06-03 오후 11:10:54	2025-06-03 오후 11:10:54
limit=8&use_v2=true&model_slug=gpt-4o.customization	1/0/https://chatgpt.com/backend-api/prompt_library/?limit=8&use_v2=true&model_slug=gpt-4o	application/json	1,999	2025-06-03 오후 10:46:30	2025-06-03 오후 10:46:30


  

Name	Location	Modified Time	Change Time
 data_1	/img_WHS_ChatGPT.E01/vol_...	2025-06-03 23:28:16 KST	2025-06-03 23:28:16 KST

Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Anno
Strings	Extracted Text	Translation						
Page: 1 of 1 Page		Matches on page: 1 of 1 Match		100%		Reset		
1/0/https://chatgpt.com/backend-api/prompt_library/?limit=8&use_v2=true&model_slug=gpt-4-1								

Name	Location	Modified Time	Change Time
 data_1	/img_WHS_ChatGPT.E01/vol_vol6/Users/forensic/App...	2025-06-03 23:28:16 KST	2025-06-03 23:28:16 KST

Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurren
Strings	Extracted Text	Translation							
Page: 1 of 1 Page		Matches on page: 1 of 1 Match		100%		Reset			
Fn1/0/https://chatgpt.com/backend-api/prompt_library/?limit=8&use_v2=true&model_slug=gpt-4o									

[그림23,24,25] ChromeCacheView와 Autopsy로 확인한 모델 변경 기록

### 3. 파일 사용/조작 아티팩트

#### 1) 이미지 삭제 흔적

- (1) 경로: C:\Users\Wforensic\Desktop\ocr\_test\_invisible\_id.png

- (2) 분석 내용: ocr\_test\_invisible\_id.png 이미지 파일이

C:\Users\Wforensic\Desktop 경로에 존재했다가 25.06.03  
 23:29:04에 삭제된 것을 확인할 수 있다. 또한, NTFS의 \$I30  
 인덱스 기록을 통해 삭제된 파일의 이름(OCR\_TE~1.PNG)과  
 위치, 삭제 시각이 확인되었으며, 파일은 휴지통 경로에  
 \$RUONPBX.png로 남아 있는 것을 확인할 수 있다.

ocr_test_invisible_id.png		2025-06-03 23:29:04 KST	2025-06-03 23:29:04 KST	2025-06-03 23:16:23 KST	2025-06-03 23:16:19 KST	2080			
4									
Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
Result: 1 of 1		Result		↔					
Type	Value								
Associated Artifact	-9223372036854775785								
Source File Path	/img_WHS_ChatGPT.E01/vol_vol6/Users/forensic/Desktop/ocr_test_invisible_id.png								
Artifact ID	-9223372036854775784								

[그림 26] Autopsy로 확인한 삭제 기록

File List			
Name	Size	Type	Date Modified
\$I30	4,096 (4 KB)	NTFS Index...	2025-06-03 오후 2:29:07
desktop.ini	282 (1 KB)	Regular File	2025-06-03 오후 1:05:16
OCR_TE~1.PNG		\$I30 INDX ...	

[그림 27] FTK Imager로 확인한 삭제 기록

## 2) 파일 삭제 흔적

- (1) 경로: ₩\$Recycle.Bin₩S-1-5-21-1233276306-1788545777-1629842736-1001
- (2) 분석 내용: 삭제된 .csv파일, .docx파일, .zip파일, .png파일 등을 확인할 수 있다

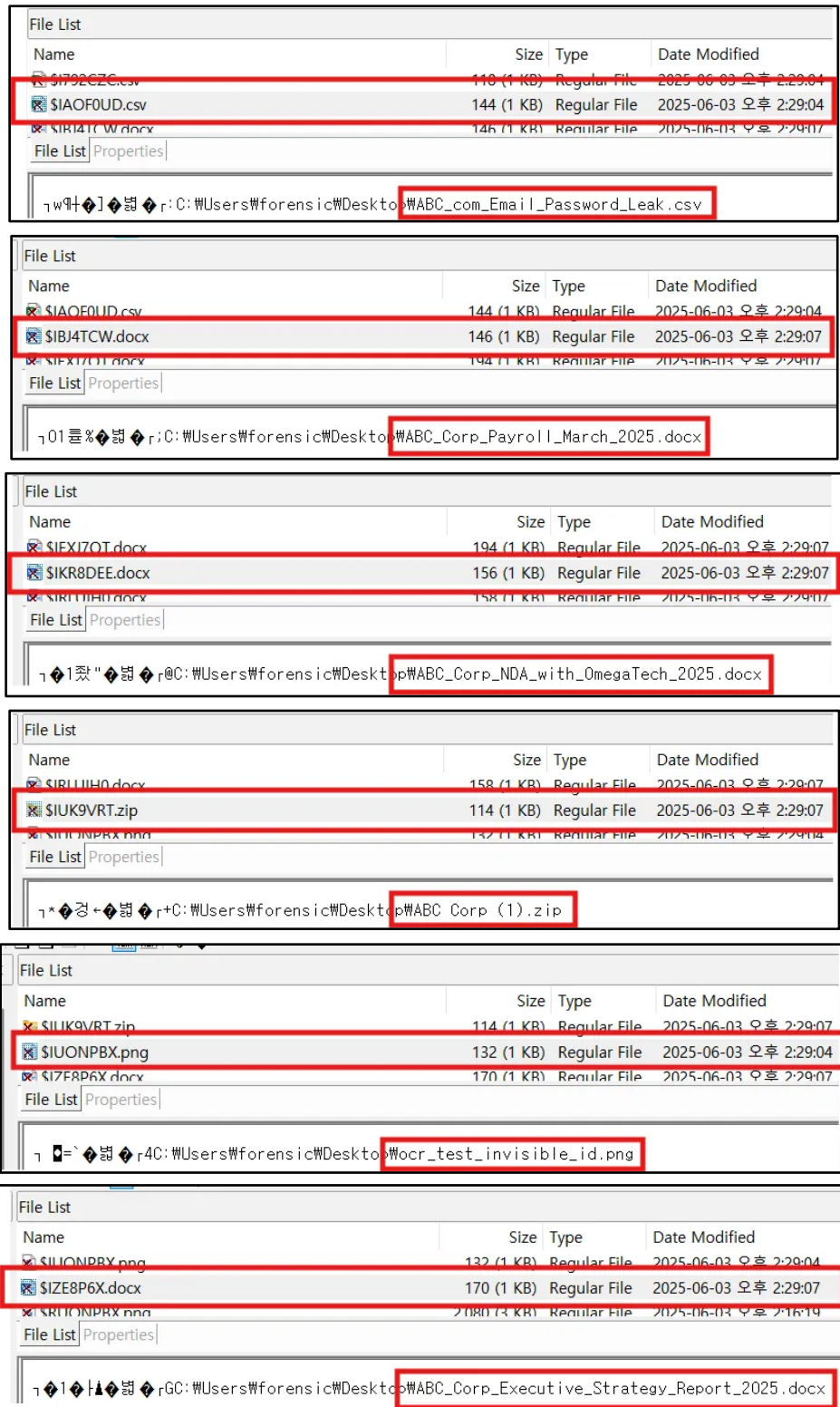
File List			
Name	Size	Type	Date Modified
\$I30	4,096 (4 KB)	NTFS Index...	2025-06-03 오후 2:29:10
\$I792CZC.csv	118 (1 KB)	Regular File	2025-06-03 오후 2:29:04
\$IAOF0UD.csv	144 (1 KB)	Regular File	2025-06-03 오후 2:29:04
\$IBJ4TCW.docx	146 (1 KB)	Regular File	2025-06-03 오후 2:29:07
\$IEXJ7QT.docx	194 (1 KB)	Regular File	2025-06-03 오후 2:29:07
\$IKR8DEE.docx	156 (1 KB)	Regular File	2025-06-03 오후 2:29:07
\$IRLUIH0.docx	158 (1 KB)	Regular File	2025-06-03 오후 2:29:07
\$IUK9VRT.zip	114 (1 KB)	Regular File	2025-06-03 오후 2:29:07
\$IUONPBX.png	132 (1 KB)	Regular File	2025-06-03 오후 2:29:04
\$IZE8P6X.docx	170 (1 KB)	Regular File	2025-06-03 오후 2:29:07
\$RUONPBX.png	2,080 (3 KB)	Regular File	2025-06-03 오후 2:16:19
desktop.ini	129 (1 KB)	Regular File	2025-06-03 오후 1:07:11

File List			
Name	Size	Type	Date Modified
\$I30	4,096 (4 KB)	NTFS Index...	2025-06-03 오후 2:29:10
\$I792CZC.csv	118 (1 KB)	Regular File	2025-06-03 오후 2:29:04
\$IAOF0UD.csv	144 (1 KB)	Regular File	2025-06-03 오후 2:29:04

File List   Properties			
r-C:\Users\forensic\Desktop\₩employees_leak.csv			



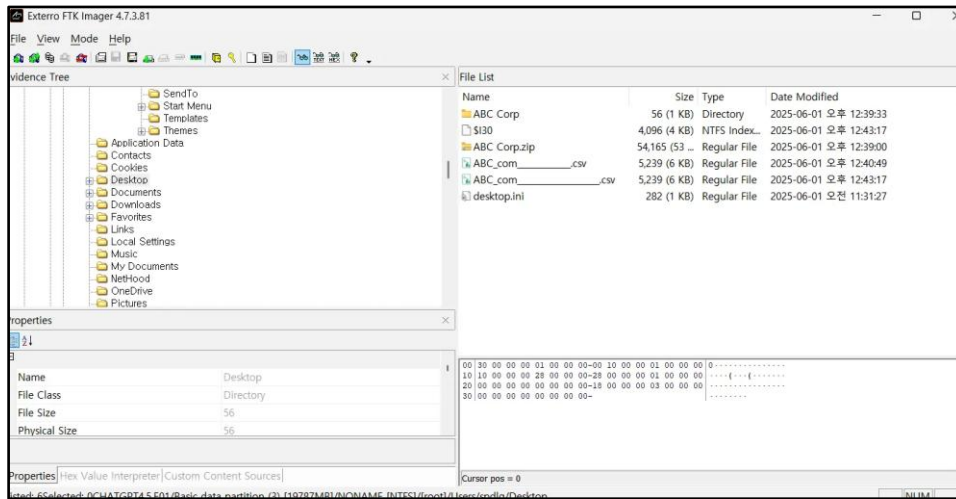
[그림 28,29,30,31,32,33,34,35] FTK Imager로 확인한 삭제 기록

### 3) 저장된 파일 확인

#### (1) 경로: C:\Users\forensic\Desktop



## (2) 분석 내용: ABC\_Corp 관련 파일 확인



[그림 36] FTK Imager로 ABC\_Corp 파일 기록

## 4) 파일 조작 로그

(1) 경로: MFT (Master File Table) : C:\W<root>\W\$MFT, USN Journal: C:\W<root>\W\$Extend\W\$UsnJrnl, NTFS 로그 파일: C:\W<root>\W\$LogFile

(2) 분석 내용: MFT, USN Journal, NTFS 로그 파일을 추출한 뒤 NTFS Logtracker를 사용하여 해당 프로그램의 파일 사용 및 조작 로그를 확인할 수 있다.

2587	2025-06-03 22:54:13	File Creation	f_00001c	\\Users\forensic\AppData\Local\Packag...
2587	2025-06-03 22:54:16	Writing Content of Non-Resident File Data Runs (in Volume) : 360216(11)	*_00001c	\\Users\forensic\AppData\Local\Packag...

[그림 37] 22:54 zip 파일 다운로드 흔적 확인 가능

2587	2025-06-03 22:56:03	File Creation	ABC_Corp_Executive_Strategy_Report_2...	\\Users\forensic\Desktop\ABC_Corp_Exec... 2025-06-03 22:56:03
2587	2025-06-03 22:56:05	Writing Content of Non-Resident File Data Runs (in Volume) : 3601310(4)	ABC_Corp_Executive_Strategy_Report_2...	\\Users\forensic\Desktop\ABC_Corp_Exec...
2588	2025-06-03 22:56:05	File Creation	ABC_Corp_Internal_Security_Meeting_M...	\\Users\forensic\Desktop\ABC_Corp_Int...
2589	2025-06-03 22:56:06	Writing Content of Non-Resident File Data Runs (in Volume) : 3600629(4)	ABC_Corp_Internal_Security_Meeting_M...	\\Users\forensic\Desktop\ABC_Corp_Int...

[그림 38] 22:54 zip 파일 다운로드 흔적 확인 가능

43		File Deletion		Abnormal Timestamp (2025-06-01 ...	\$R792CZC.csv	\
23	2025-06-03 23:29:19	File Deletion			\$I792CZC.csv	\
75	2025-06-03 23:29:19	File Deletion			\$RAOF0UD.csv	\
05	2025-06-03 23:29:19	File Deletion			\$IAOF0UD.csv	\
52	2025-06-03 23:29:19	File Deletion			\$RBJ4TCW.docx	\
99	2025-06-03 23:29:19	File Deletion			\$IBJ4TCW.docx	\
54	2025-06-03 23:29:19	File Deletion			\$REXJ7QT.docx	\
01	2025-06-03 23:29:19	File Deletion			\$IEXJ7QT.docx	\
42	2025-06-03 23:29:19	File Deletion			\$RRR8DEE.docx	\
89	2025-06-03 23:29:19	File Deletion			\$IKR8DEE.docx	\
20	2025-06-03 23:29:19	File Deletion			\$RLUIH0.docx	\
77	2025-06-03 23:29:19	File Deletion			\$IRLUIH0.docx	\
89	2025-06-03 23:29:19	File Deletion			\$RUKSVRT.zip	\
21	2025-06-03 23:29:19	File Deletion			\$IUKSVRT.zip	\
57	2025-06-03 23:29:19	File Deletion			\$RUONFEX.png	\
79	2025-06-03 23:29:19	File Deletion			\$IUONFEX.png	\
30	2025-06-03 23:29:19	File Deletion			\$RZESP6X.docx	\
77	2025-06-03 23:29:19	File Deletion			\$IZESP6X.docx	\

[그림 39] 23:29 PC 내 파일 삭제 흔적 확인 가능

## 5) ChatGPT 버전 정보

- (1) 경로: C:\root\Users\Wforensic\NTUSER.DAT,  
C:\root\Users\Wforensic\Wntuser.dat.LOG1,  
C:\root\Users\Wforensic\Wntuser.dat.LOG2

① NTUSER.DAT\ROOT\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\chatgpt.exe

- (2) 분석 내용: ChatGPT 데스크톱 앱의 버전이 "1.2025.139.0"라는 것을 알 수 있다.

C:\Program Files\WindowsApps\OpenAI.ChatGPT-Desktop\_1.2025.139.0\_x64\_\_2p2nqsd0c76g0\app\ChatGPT.exe 경로를 통해서 프로그램이 설치된 위치를 알 수 있다.

Type viewer	Slack viewer	Binary viewer
Value name	(default)	
Value type	RegSz	
Value	C:\Program Files\WindowsApps\OpenAI.ChatGPT-Desktop_1.2025.139.0_x64__2p2nqsd0c76g0\app\ChatGPT.exe	

[그림 40] 설치 경로 확인 가능

## 6) ChatGPT 실행 정보

- (1) 경로: C:\root\Users\Wforensic\WNTUSER.DAT,  
C:\root\Users\Wforensic\Wntuser.dat.LOG1,  
C:\root\Users\Wforensic\Wntuser.dat.LOG2

① NTUSER.DAT\ROOT\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist

- (2) 분석 내용: ChatGPT-Desktop이 실행된 횟수, 사용된 시간, 마지막으로 실행된 시간 정보를 확인할 수 있다. 해당 화면에 표시된 시간은 UTC 시간이기 때문에 로컬 시간 기준으로 계산하면 23:10:38 에 마지막으로 실행되었다는 것을 알 수 있다.

Program Name	Run Counter	Focus Count	Focus Time	Last Executed
[System32]\Wininit32.exe	1	1	0 0d, 0h, 00m, 00s	2025-06-03 13:12:46
Microsoft.XboxGamingOverlay_8wekyb3d8bbwe!App	1	1	0 0d, 0h, 00m, 00s	2025-06-03 13:29:47
C:\Users\Wforensic\Downloads\ChatGPT Installer.exe	3	3	2 0d, 0h, 00m, 25s	2025-06-03 13:43:02
Microsoft.WindowsStore_8wekyb3d8bbwe!App	1	1	5 0d, 0h, 02m, 28s	2025-06-03 13:41:57
[System32]\WOpenVeh.exe	0	0	1 0d, 0h, 00m, 07s	
OpenAI.ChatGPT-Desktop_2p2nqsd0c76g0f!ChatGPT	1	1	9 0d, 0h, 35m, 47s	2025-06-03 14:10:38
UEFI_C:\LOD\Countdown	0	0	0 0d, 0h, 00m, 00s	
(Common Programs)\Accessories\WinSnipping Tool.lnk	9	9	0 0d, 0h, 00m, 00s	2025-06-03 13:03:37
UEFI_CTL_SESSION	22	22	0 0d, 0h, 00m, 00s	

[그림 41] 실행 시간 정보 확인 가능

## 7) ChatGPT 실행 정보

- (1) 경로: C:\root\Users\Wforensic\WNTUSER.DAT,  
C:\root\Users\Wforensic\Wntuser.dat.LOG1,  
C:\root\Users\Wforensic\Wntuser.dat.LOG2

① SYSTEM\ROOT\ControlSet001\Control\Session Manager\AppCompatCache

- (2) 분석 내용: ChatGPT.exe 파일의 최종 수정 타임스탬프 정보를 바탕으로 2025-06-03 22:44:21경에 해당 파일이 디스크에 올라갔다는 것을 확인할 수 있다.

Type	Viewer	Stack viewer	AppCompatCache
<p>Log a column header here to group by that column.</p>			
Catch Entry Position	Program Name	Modified Time	
#	@#	=	
#	9 C:\Windows Files [x68]W\MicrosoftEdge\WinSxS\edgeRecovery\Mscodex_d429d2_1368395057Mscdexrecov-ent.exe	2023-03-29 08:55:26	
#	10 c:\windows\system32\cmd.exe	2023-12-04 02:46:49	
#	11 C:\Windows Files\WinSxS\AppXOpenL1OutGPTDesktop_1.2025.139.0_a6d..._2c3qasCn6gWz-gppCvGPT.exe	2025-06-03 13:44:21	
#	12 00000009 800187e908B0000 800A00D05850000 B664 Y09RACUmpj 1588000 - 2027/08/07/7697		
#	13 00000009 57AB037E00130000 000A00D05850000 B664 Microsoft Windows Defender Security Center		

[그림 42] 파일 정보 확인 가능

항목 번호	원시 데이터(16진수)	원시 데이터의 의미
레코드 인덱스/플래그	00000009	플래그 정보
마지막 수정 시각 (FILETIME)	000107e9008b0000	2025-06-03 13:44:21 (UTC)
파일 크기 + 실행 여부 플래그	000a0000585d0000	23928 bytes 크기의 파일이 실행된 상태
아키텍처 코드	8664	해당 실행 파일이 64비트(AMD64)
프로그램 식별자	OpenAI.ChatGPT- Desktop_2p2nqsd0c76g0	C:\Program Files\WindowsApps\OpenAI.ChatG PT- Desktop_1.2025.139.0_x64_2p2nqs d0c76g0\ChatGPT.exe" 라는 경로 저장

[표 4] 항목 정리 내용

#### 4. 메모리 아티팩트

### 1) 프로세스 탐지

(1) 분석 내용:

- ① python [vol.py](#) -f gpt.vmem windows.pstree 명령어를 통해 ChatGPT 프로세스 탐지가 가능하다.



[그림 43] 탐지 확인

- ② ChatGPT.exe 가 시스템 내에 존재한다. (사용자가 ChatGPT 다운로드)

- ③ ChatGPT.exe 설치 경로 확인이 가능하다. C:\Program Files\WindowsApps\OpenAI.ChatGPT-Desktop\_1.2025.139.0\_x64\_\_2p2nqsd0c76g0\app\ChatGPT.exe
- ④ ChatGPT.exe 의 PID가 6484 인 것을 확인할 수 있다.

## 2) 핸들 정보

### (1) 분석 내용:

- ① python vol.py -f gpt.vmem windows.handles --pid 6484 명령어를 통해 ChatGPT 관련 핸들 정보 확인이 가능하다.

PID	Process	Offset	HandleValue	Type	GrantedAccess	Name
-----	---------	--------	-------------	------	---------------	------

[그림 44] 핸들 정보 확인

- ② 클라우드 기반 서비스로 핸들 정보가 존재하지 않는 것을 확인할 수 있다.

## 3) 레지스트리 정보

### (1) 분석 내용:

- ① python [vol.py](#) -f gpt.vmem windows.registry.hivelist 명령어를 통해 레지스트리 하이브 파일들의 목록과 위치를 확인할 수 있다.
- ② C:\ProgramData\Packages\OpenAI.ChatGPT-Desktop\_2p2nqsd0c76g0\WS-1-5-21-1233276306-1788545777-1629842736-1001\SystemAppData\Helium\Cache\10c3a893ae2a93d.dat, C:\Users\forensic\AppData\Local\Packages\OpenAI.ChatGPT-Desktop\_2p2nqsd0c76g0\SystemAppData\Helium\User.dat , C:\Users\forensic\AppData\Local\Packages\OpenAI.ChatGPT-Desktop\_2p2nqsd0c76g0\SystemAppData\Helium\UserClasse

s.dat, C:\ProgramData\Packages\OpenAI.ChatGPT-Desktop\_2p2nqsd0c76g0\WS-1-5-21-1233276306-1788545777-1629842736-1001\SystemAppData\Helium\Cache\10c3a893ae2a93d\_COM15.dat , C:\ProgramData\Packages\OpenAI.ChatGPT-Desktop\_2p2nqsd0c76g0\WS-1-5-21-1233276306-1788545777-1629842736-1001\SystemAppData\Helium\Cache\10c3a893ae2a93d.dat  
 ₩ 다음과 같은 ChatGPT 관련 레지스트리 확인이 가능하다.

## 5. 네트워크 아티팩트

### 1) HSTS 정책

#### (1) 경로:

C:\Users\forensic\AppData\Local\Packages\OpenAI.ChatGPT\Desktop\_2p2nqsd0c76g0\LocalCache\Roaming\ChatGPT\Network\TransportSecurity

#### (2) 분석 내용:

```
Decoded text
{"sts":[{"expiry":1780495472.625352,"host":"QEZCZ8XCblyeqbkigQWaVWib+OtwQ/uDZUAp sTcfLY8=", "mode": "force-https", "sts_include_subdomains":true, "sts_observed":1748959472.625354}, {"expiry":1780547846.582688,"host
```

[그림45] HxD로 추출한 HSTS 정책 캐시 정보

키	설명
---	----

"host" : "..."	HSTS 정책이 적용된 호스트
"mode" : "force-https"	HTTP 요청 시 자동으로 HTTPS로 리디렉션
"sts_include_subdomains" : true	서브 도메인까지 HTTPS 강제적용
"sts_observed" : 1748959472.625354	해당 도메인에서 HSTS 헤더를 처음 본 시점
"expiry" : 1780547846.582688	만료 시각


[표5] HSTS 정책 캐시 정보

## 2) 채팅 내역 호출

### (1) 경로:

Users\forensic\AppData\Local\Packages\OpenAI.ChatGPT-Desktop\_2p2nqsd0c76g0W\LocalCache\Roaming\ChatGPT\Cache\Cache\_Data\data\_1

(2) 분석 내용: 해당 API를 통해 사용자의 과거 대화 목록을 불러오는 기능이 수행된 것을 확인할 수 있다. 또한, offset=0, limit=28 파라미터를 통해 대화 중 최대 28개까지 불러오는 것을 확인할 수 있다.

Name	Location	Modified Time	Change Time
 data_1	/img_WHS_ChatGPT.E01/vol_vol6/Users/forensic/App...	2025-06-03 23:28:16 KST	2025-06-03 23:28:16 KST
<hr/>			
Hex	Text	Application	File Metadata
Strings	Extracted Text	Translation	
Page: 1 of 1 Page    < >    Matches on page: 1 of 1 Match    < >    100%    🔍    Reset			
<pre> xwvlj PUg3sv}H 1/0/https://files09.oaiusercontent.com/file-6ur9e5bG9JNMhgFmFmV4Bz?se=2025-06-03T14%3A16%3A11Z&amp;sp=r&amp;sv=2024-08-04&amp; 20private&amp;rscd=attachment%3B%20filename%3Demployees_leak.csv&amp;sig=mow8xjljS16qAmMISW7UyQxPwc8jnlPI9gs8ci4eWnM9 1/0/https://files09.oaiusercontent.com/file-RjB8QyvvAzEcFAHTduvWis?se=2025-06-03T14%3A16%3A11Z&amp;sp=r&amp;sv=2024-08-04&amp;sv 20private&amp;rscd=attachment%3B%20filename%3DABC_com_Email_Password_Leak.csv&amp;sig=CFpIshBxHJuXoJMrjNuWTGxo6elKxtKP x \$I y&lt;0KA {"detail":"Not Found"} _1/0/https://chatgpt.com/backend-api/conversation/683efd51-02b0-800e-b6d4-6ab09258c1d9/interpreter/download?message_id= 2Fdata%2Focr_test_invisible_id.png 1/0/https://chatgpt.com/backend-api/conversations?offset=0&amp;limit=28&amp;order=updated %+`h </pre>			

### 3) 쿠키 정보

#### (1) 경로:

Users\forensic\AppData\Local\Packages\OpenAI.ChatGPT-Desktop\_2p2nqsd0c76g0\LocalCache\Roaming\ChatGPT\Network\Cookies

#### (2) 분석 내용: cf\_bmhp8...등 과 같은 고유 세션 키와 cloudflare bot management 쿠키를 확인할 수 있다.

00004DA0	00 00 28 09 33 0D 09 1B 0F 01 02 01 2E 6F 61 69	..(.3.....oai
00004DB0	75 73 65 72 63 6F 6E 74 65 6E 74 2E 63 6F 6D 5F	usercontent.com_
00004DC0	5F 63 66 5F 62 61 2F 02 01 BB 54 27 09 23 0D 09	cf bm/...»T'.#..
00004DD0	29 0F 01 02 01 63 68 61 74 67 70 74 2E 63 6F 6D	)....chatgpt.com
00004DE0	6F 61 69 2D 6C 61 73 74 2D 6D 6F 64 65 6C 2F 02	oai-last-model/.
00004DF0	01 BB 58 1F 09 23 0D 09 19 0F 01 02 01 63 68 61	..»X..#.....cha

[그림47] HxD로 확인한 쿠키 정보 확인

### 4) 서버 연결 정보

#### (1) 경로:

Users\forensic\AppData\Local\Packages\OpenAI.ChatGPT-Desktop\_2p2nqsd0c76g0\LocalCache\Roaming\ChatGPT\Network\Network Persistent State

#### (2) 분석 내용: 사용 프로토콜과 접속 도메인 등을 확인할 수 있다.



```
Decoded text
google.com"}, {"a
nonymization": []
, "server": "https
://ab.chatgpt.co
m", "supports_spd
y": true}, {"alter
native_service":
[{"advertised_al
pns": ["h3"], "exp
iration": "133960
73838707566", "po
rt": 443, "protoco
l_str": "quic"}],
"anonymization":
[], "network_stat
s": {"srtt": 22156
}, "server": "http
s://o33249.inges
t.us.sentry.io",
"supports_spdy":
true}, {"alternat
ive_service": [{"
advertised_alpns
```

[그림48] HxD로 확인한 서버 연결 정보

키	설명
"server": "https://ab.chatgpt.com"	사용자가 접속한 서버 도메인 (ChatGPT 접속)
"protocol_str" : "quic"	QUIC 프로토콜을 통해 HTTP/3 지원
"port" : 443	모든 서버는 443 포트 사용 → HTTPS 통신
"network_stats"	네트워크 지연 시간
"supports_spdy": true	서버가 SPDY 프로토콜 지원

[표6] 서버 연결 상세 정보

5) CSRF 토큰 기록

(1) 경로:

C:\Users\forensic\AppData\Local\Packages\OpenAI.ChatGP  
T-

Desktop\_2p2nqsd0c76g0WLocalCacheWRoamingWChatGPTWCac  
heWCache\_Data

(2) 분석 내용: csrf 토큰 값을 확인할 수 있다.

```
C: > Users > user > AppData > Local > Temp > ccvF31.tmp > ≡ csrf.customization  
1 {"csrfToken": "3bd607d4cd3cb89a63207b4f55d99324183af96ba0cf9a2a77644c418ed889af"}
```

[그림49] ChromeCacheView로 확인한 csrf 토큰 값

## 6) 사용자 내부 IP 주소

(1) 경로:

C:\Users\넬입\AppData\Local\Packages\OpenAI.ChatGPT  
Desktop\_2p2nqsd0c76g0WLocalCacheWRoamingWChatGPTWNet  
work\Network Persistent State

(2) 분석 내용: 사용자가 ChatGPT를 사용할 당시의 로컬 네트워크 IP  
주소와 Network Persistent State 속 address IP 주소가 일치하다.

```
Command Prompt  
C:\Users\forensic>ipconfig  
  
Windows IP Configuration  
  
Ethernet adapter Ethernet0:  
  
Connection-specific DNS Suffix . : localdomain  
Link-local IPv6 Address . . . . . : fe80::7d2a:26cb:ae8c:5dd6%4  
IPv4 Address. . . . . : 192.168.133.132  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : 192.168.133.2
```

[그림50] ChatGPT를 사용할 당시 로컬 네트워크 IP 주소

```
"https://o33249.ingest.us.sentry.io", "supports_spdy": true, {"alternative_service": {"advertised_alpn": ["h3"],  
"expiration": "13396072505853719", "port": 443, "protocol_str": "quic"}}, "anonymization": {"l", "network_stats": {"srtt": 12539},  
"server": "https://a.nel.cloudflare.com", "supports_spdy": true}, "supports_quic": {"address": "192.168.133.132", "used_quic": true},  
"version": 5}, "network_qualities": {"CAESABiAgICA+P7///8B": "4G"}}}
```

[그림51] Network Persistent State 속 address IP 주소

## 7) 네트워크 흐름 추적

- (1) 분석 내용: 내부 IP 주소 192.168.1.16이 172.64.155.209, 104.18.32.47 등 Cloudflare에 속한 OpenAI 프론트엔드 CDN 서버와 TLS 세션을 수차례 수립한 흔적이 확인되었다.
- 이를 통해 해당 호스트에서 ChatGPT 애플리케이션이 실행되어 OpenAI 인프라와 통신을 시도한 정황이 확인된다.

```

Command Prompt
Microsoft Windows [Version 10.0.19045.3803]
(c) 2019 Microsoft Corporation. All rights reserved.

D:\Users\forensic>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::7d2a:26cb:ae8c:5dd6%4
    IPv4 Address. . . . . : 192.168.1.16
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1
  
```

[그림52] ChatGPT 로컬 네트워크 IP 주소

No.	Time	Source	Destination	Protocol	Length	Info
272	1.294867	192.168.1.16	172.64.155.209	TCP	54	50337 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1023 Len=0
273	1.294883	192.168.1.16	172.64.155.209	TCP	54	[TCP Retransmission] 50337 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1023 Len=0
274	1.295572	192.168.1.16	104.18.32.47	TCP	54	50339 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1028 Len=0
275	1.295579	192.168.1.16	104.18.32.47	TCP	54	[TCP Retransmission] 50339 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1028 Len=0
276	1.304522	172.64.155.209	192.168.1.16	TCP	60	443 → 50337 [FIN, ACK] Seq=1 Ack=2 Win=22 Len=0
277	1.304522	104.18.32.47	192.168.1.16	TCP	60	443 → 50339 [FIN, ACK] Seq=1 Ack=2 Win=10 Len=0
278	1.304909	192.168.1.16	172.64.155.209	TCP	54	50337 → 443 [ACK] Seq=2 Ack=2 Win=1023 Len=0
279	1.304916	192.168.1.16	172.64.155.209	TCP	54	[TCP Dup ACK 278#1] 50337 → 443 [ACK] Seq=2 Ack=2 Win=1023 Len=0
280	1.304995	192.168.1.16	104.18.32.47	TCP	54	50339 → 443 [ACK] Seq=2 Ack=2 Win=1028 Len=0
281	1.304999	192.168.1.16	104.18.32.47	TCP	54	[TCP Dup ACK 280#1] 50339 → 443 [ACK] Seq=2 Ack=2 Win=1028 Len=0
285	2.493858	192.168.1.16	104.18.32.47	TCP	54	50340 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1028 Len=0
286	2.493871	192.168.1.16	104.18.32.47	TCP	54	[TCP Retransmission] 50340 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1028 Len=0
287	2.503890	104.18.32.47	192.168.1.16	TCP	60	443 → 50340 [FIN, ACK] Seq=1 Ack=2 Win=10 Len=0
288	2.504281	192.168.1.16	104.18.32.47	TCP	54	50340 → 443 [ACK] Seq=2 Ack=2 Win=1028 Len=0
289	2.504292	192.168.1.16	104.18.32.47	TCP	54	[TCP Dup ACK 288#1] 50340 → 443 [ACK] Seq=2 Ack=2 Win=1028 Len=0

[그림53] Wireshark를 통해 확인된 로컬 IP(192.168.1.16)와 OpenAI 인프라 간의 통신 흐름

## 8) TLS 세션 추적

- (1) 분석 내용: TLS 핸드셰이크 흐름인 Client Hello → Server Hello → Key Exchange가 관찰되었으며, 이를 통해 통신이 실제로 이루어졌다는 정황과 접속 시점을 파악할 수 있다. 비록 TLS 1.3 또는 QUIC(HTTP/3) 프로토콜로 암호화된 상태이기 때문에, 실제 전송된 데이터 내용(채팅 기록, 사용 모델 등)은 복호화할 수

없으나, Wireshark를 통해 해당 핸드셰이크 흐름이 정상적으로 수립되었음을 확인함으로써 클라이언트의 접속 시도와 서버의 응답이 성공적으로 이루어진 것으로 판단할 수 있다.

또한, TLS 1.3 또는 QUIC은 프라이빗 키 없이 복호화가 불가능하므로, 암호화된 트래픽 자체는 열람할 수 없었다.

Time	Source	Destination	Protocol	Length	Info
4243	192.168.1.16	104.18.41.158	QUIC	1292	Initial, DCID=1a921c40c23fbc4d, PKN: 2, PING, CRYPTO, PING, PING, PING
4248	104.18.41.158	192.168.1.16	QUIC	1242	Initial, SCID=018e121d31d967ca3a8c8b1d06d97a5c47a29822, PKN: 3, CRYPTO
4898	192.168.1.16	104.18.32.47	TLSv1.3	571	Client Hello (SNI=chatgpt.com)
4901	104.18.32.47	192.168.1.16	TLSv1.3	272	Server Hello, Change Cipher Spec, Application Data
5321	192.168.1.16	104.18.32.47	TLSv1.3	681	Client Hello (SNI=ab.chatgpt.com)
5325	104.18.32.47	192.168.1.16	TLSv1.3	1429	Server Hello, Change Cipher Spec, Application Data
5623	192.168.1.16	3.233.158.41	TLSv1.2	571	Client Hello (SNI=http-intake.logs.datadoghq.com)
5626	3.233.158.41	192.168.1.16	TLSv1.2	1514	Server Hello
7376	192.168.1.16	172.64.155.209	TLSv1.3	710	Client Hello (SNI=chatgpt.com)
7380	172.64.155.209	192.168.1.16	TLSv1.3	1429	Server Hello, Change Cipher Spec, Application Data
7476	192.168.1.16	104.18.32.47	TLSv1.3	713	Client Hello (SNI=ab.chatgpt.com)
7479	104.18.32.47	192.168.1.16	TLSv1.3	1429	Server Hello, Change Cipher Spec, Application Data
7513	192.168.1.16	51.132.193.105	TLSv1.2	268	Client Hello (SNI=v10.events.data.microsoft.com)
7549	51.132.193.105	192.168.1.16	TLSv1.2	1369	Server Hello, Certificate, Server Key Exchange, Server Hello Done
7636	192.168.1.16	172.64.155.209	TLSv1.3	678	Client Hello (SNI=chatgpt.com)
7640	172.64.155.209	192.168.1.16	TLSv1.3	1429	Server Hello, Change Cipher Spec, Application Data
8818	192.168.1.4	142.258.206.238	QUIC	1292	Initial, DCID=0b96757f33a59ed6, PKN: 2, PADDING, CRYPTO, PING, PING, C
8834	142.258.206.238	192.168.1.4	QUIC	1292	Initial, SCID=0b96757f33a59ed6, PKN: 3, CRYPTO, PADDING
8890	192.168.1.16	104.18.32.47	TLSv1.3	713	Client Hello (SNI=ab.chatgpt.com)
8894	104.18.32.47	192.168.1.16	TLSv1.3	1429	Server Hello, Change Cipher Spec, Application Data

[그림54] Wireshark를 통해 확인한 TLS 세션

## 6. 메신저 아티팩트

### 1) Leveldb

#### (1) 경로:

C:\Users\forensic\AppData\Local\Packages\OpenAI.ChatGPT\Local Storage\leveldb

#### (2) 분석 내용: 해당 파일을 통해 대화마다 ID, 제목, 생성/수정 시각, 아카이브 여부, 메모리 사용 여부 등 메타데이터가 기록을 확인 가능.

① "total":2 정보를 통해 총 2개의 대화 목록이 저장됨을 확인 가능

```
[{"conversation_origin":null,"snippet":null}],{"total":2,"limit":28,"offset":0}],{"pageParams":{"0}},"timestamp":1748960896867,"version":1}
```

[그림55] LevelDB-Viewer로 추출한 대화 목록 정보

② 첫 번째 대화 제목은 Cream Stew Recipe 라는 것을 알 수 있고, 마지막 수정시간이 23:28분임을 확인 가능. 이는 조작 보고서에 명시된 "23:28 Cream Stew Recipe로 변경"과 동일.

③ "is\_do\_not\_remember": false 를 통하여 privacy 모드가 꺼져있는 일반 대화 모드라는 것을 확인 가능.

```
Value: {"value":{"pages":[{"items":[{"id":"683efd51-02b0-800e-b6d4-6ab09258c1d9","title":"Cream Stew Recipe","create_time":"2025-06-03T13:49:05.305928Z","update_time":"2025-06-03T4:28:11.593787Z","mapping":null,"current_node":null,"conversation_template_id":null,"gizmo_id":null,"is_archived":false,"is_starred":null,"is_do_not_remember":false,"memory_scope":"global_enabled","workspace_id":null,"async_status":4,"safe_urls":[],"blocked_urls":[],"conversation_origin":null,"snippet":null},
```

[그림56] LevelDB-Viewer로 추출한 확인한 첫번째 대화 목록

```
{"id":"683ebbf6-3668-800e-a088-89a83cceaaf10","title":"X h, H","create_time":"2025-06-03T09:10:14.621500Z","update_time":"2025-06-03T09:15:49.778091Z","mapping":null,"current_node":null,"conversation_template_id":null,"gizmo_id":null,"is_archived":false,"is_starred":null,"is_do_not_remember":false,"memory_scope":"global_enabled","workspace_id":null,"async_status":null,"safe_urls":[],"blocked_urls":
```

[그림57] LevelDB-Viewer로 추출한 두번째 대화 목록

④ JSON 데이터를 분석하여 JWT 토큰의 대칭키 정보를 확인 가능. 해당 정보를 확인해보면, HS512 알고리즘을 사용하는 것을 알 수 있고, 해당 키의 값 또한 확인이 가능함.

```
Key: _https://chatgpt.com/client-correlated-secret
Value:
{"alg":"HS512","ext":true,"k":"Wku3VvWw8MiHP4uiNA00lRCSLyXrH_A8ZJzhajzcWC_GvpLn3eC_fNwgXlpFJGOB0voWwy3JWi9EtOKRCcLh4qLIGrJoSXGuiaxFFUrOWpHowN49FpoDcKG0ksGLEMHuOMtASGJIMyAPrgzIfU1h69KRBasWSy4W-ebGkndsgFM","key_ops":["sign","verify"],"kty":"oct"}
```

[그림58] LevelDB-Viewer로 추출한 JWT 대칭키(JSON) 정보

## 2) 프롬프트 내 파일 업로드

(1) 경로:

C:\Users\Wforensic\AppData\Local\Packages\OpenAI.ChatGPT-

Desktop\_2p2nqsd0c76g0\LocalCache\Roaming\ChatGPT\WCache\WCache\_Data

(2) 분석 내용: employee\_leak.csv 파일 업로드 기록 확인 가능

```
C:\Users\user> AppData\Local\Temp> ccvF31.tmp > E file-4G6yJ8edYjxPLGg9a3uqA.customization
1 {"status":"success","download_url":"https://files09.oaiusercontent.com/file-4G6yJ8edYjxPLGg9a3uqA?se=2025-06-03T14%3A16%3A11Z&sp=r&sv=2024-08-04&sr=1"}
2 {"metadata":{"file_name":"employees_leak.csv","creation_time":"2025-06-03 14:04:36.532542+00:00","no_auth_user_upload":false,"mime_type":null}}
```

[그림59] LevelDB-Viewer로 추출한 프롬프트 내 파일 업로드 기록

3) 프롬프트 내 파일 다운로드

(1) 경로:

MFT (Master File Table) : C:\W<root>\W\$MFT,

USN Journal : C:\W<root>\W\$Extend\W\$UsnJrnl,

NTFS 로그 파일 : C:\W<root>\W\$LogFile

(2) 분석 내용: 22:58에 ChatGPT가 생성해준

ABC\_com\_Email\_Password\_Leak.csv 파일 다운로드 흔적 확인 가능

80259			Images		
80714	2025-06-03 22:58:01	File Creation	ABC_com_Email_Password_Leak.csv	\Users\forensic\Desktop\ABC_com_Email_Password_Leak.csv	20
81001	2025-06-03 22:58:01	File Deletion	ABC_com_Email_Password_Leak.csv	\Users\forensic\Desktop\ABC_com_Email_Password_Leak.csv	20
81265	2025-06-03 22:58:01	Move (Before)	8c6ea594-677a-4328-b1d2-800000000000	\Users\forensic\Downloads\8c6ea594-677a-4328-b1d2-800000000000	20
81349	2025-06-03 22:58:01	Move (After)	ABC_com_Email_Password_Leak.csv	\Users\forensic\Desktop\ABC_com_Email_Password_Leak.csv	20
82580	2025-06-03 22:58:01	File Creation	c5bf5c618805c549.automaticDestination...	\Users\forensic\AppData\Roaming\Microsoft\Windows\CurrentVersion\Recent\c5bf5c618805c549.automaticDestination...	20
82813	2025-06-03 22:58:01	Writing Content of Non-Resident File	Data Runs(in Volume) : 2461207 (1)		20
84359	2025-06-03 22:58:01	File Creation	ABC_com_Email_Password_Leak.csv.lnk	\Users\forensic\AppData\Roaming\Microsoft\Windows\CurrentVersion\Recent\ABC_com_Email_Password_Leak.csv.lnk	20
84656		Writing Content of Non-Resident File	Data Runs(in Volume) : 2917877 (1)		20
85750		Writing Content of Non-Resident File	Data Runs(in Volume) : 90654 (16)		20
86667			ABC_com_Email_Password_Leak.csv.lnk	\Users\forensic\AppData\Roaming\Microsoft\Windows\CurrentVersion\Recent\ABC_com_Email_Password_Leak.csv.lnk	20
87532		Writing Content of Non-Resident File	Data Runs(in Volume) : 931682 (2)		20

[그림60] SQLiteDB로 추출한 프롬프트 내 파일 다운로드 기록

## VII. 분석 차별점

기존의 선행 연구들은 주로 안드로이드(Android), iOS와 같은 모바일 환경, 또는 macOS 기반 아티팩트 분석에 집중되어 있으며 윈도우(Windows) 기반 LLM 프로그램에 대한 디지털 포렌식적 접근은 상대적으로 제한적이었다.

본 보고서에서는 이러한 기존 연구의 한계를 극복하고자, Windows 운영체제에서 실행된 Chat GPT 프로그램의 아티팩트를 중심으로 분석을 수행하였다.

이를 통해 기존 모바일 및 macOS 환경과는 구분되는 로컬 사용자 계정 경로 내 AppData\Local 및 Roaming 디렉터리에 저장된 캐시 및 로그 파일을 통해 사용자 정보와 네트워크 사용 정보 등을 발견하였으며, 이로써 기존 논문들과는 명확히 차별화된 분석적 기여를 제공한다.

## VIII. 분석 요약

아티팩트 유형	경로	설명
시스템 설치/실행 아티팩트	C:\Windows\Prefetch\CHATGPT INSTALLER.EXE-FFA711B3.pf	설치파일이 실행된 시간과 실행 횟수 파악 가능
	C:\Windows\Prefetch	CHATGPT.EXE 실행 시각 및 누적 실행 횟수 확인 가능
	C:\Users\forensic\Downloads\ChatGPT Installer.exe	다운로드된 ChatGPT 설치 파일 경로 및 시간 확인가능
사용자 행위	C:/Users/forensic/AppData/Local/Packages/Ope nAI.ChatGPT Desktop_2p2nqsd0c76g0/LocalCache/Roaming/ ChatGPT/Cache/ Cache_Data	사용자 토큰, 구독 상태, 계정 생성일, 이메일, 이름, 전화번호, 프로필 사진 등의 정보 확인 가능
	C:/Users/forensic/AppData/Local/Packages/Ope nAI.ChatGPT Desktop_2p2nqsd0c76g0/LocalCache/Roaming/ ChatGPT/Local Storage/leveldb/00003.log	sessionID, 세션 시작 시각, 마지막 갱신 시각 등을 통해 세션 유지 시간과 사용자 활동 추적 가능
	C:/Users/forensic/AppData/Local/Packages/Ope nAI.ChatGPTDesktop_2p2nqsd0c76g0/LocalCac he/Roaming/ChatGPT/Local State	환경설정 및 암호화 관련 메타데이터 포함. 내부 데이터 암호화 및 복호화에 필요한 정보 포함
	C:\Users\forensic\AppData\Roaming\Micros	사용자가 최근 접근한



아티팩트	oft\Windows\Recent	이미지, 문서, 폴더 등의 흔적 확인 가능
	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList	SID 값과 사용자 계정명이 연결된 경로를 통해 분석 대상 사용자 계정 식별
	/Users/forensic/AppData/Local/Microsoft/Edge/User Data/Default/History	로그인 페이지에 접속한 기록과 로그인 관련 URL 경로 접근 확인
	C:\Users\forensic\AppData\Local\Packages\OpenAI.ChatGPT-Desktop_2p2nqsd0c76g0\LocalCache\Roaming\ChatGPT\Cache\Cache_Data\data_1	OAuth 인증 최종 단계에서 callback URL 호출과 함께 인증 코드가 기록된 로그 확인
	C:\Users\forensic\AppData\Local\Packages\OpenAI.ChatGPT-Desktop_2p2nqsd0c76g0\LocalCache\Roaming\ChatGPT\Cache\Cache_Data\data_1	사용자가 사용한 모델의 변경 시각, 모델명 등의 기록을 통해 모델 전환 내역 확인 가능
파일 사용/조작 아티팩트	C:\Users\forensic\Desktop\ocr_test_invisible_id.png	파일이 삭제된 시간, 위치, 파일의 이름 등 확인 가능
	/\$Recycle.Bin\S-1-5-21-1233276306-1788545777-1629842736-1001	.csv, .docx, .zip, .png 등 삭제된 파일 목록과 삭제 경로 확인 가능
	C:\Users\forensic\Desktop	ABC_Corp 파일 확인 가능
	MFT (Master File Table) : C:\Windows\MFT USN Journal : C:\Windows\Extend\UsnJrnl NTFS 로그 파일 : C:\Windows\LogFile	MFT/USN Journal/NTFS 로그 분석을 통해 파일 생성, 열람, 수정, 삭제 등 조작 시간 및 행위 확인 가능
	C:\root\Users\forensic\NTUSER.DAT, C:\root\Users\forensic\ntuser.dat.LOG1, C:\root\Users\forensic\ntuser.dat.LOG2	레지스트리 경로를 통해 ChatGPT의 설치 버전 및 설치 경로를 식별할 수 있음
	C:\root\Users\forensic\NTUSER.DAT, C:\root\Users\forensic\ntuser.dat.LOG1, C:\root\Users\forensic\ntuser.dat.LOG2	실행 횟수, 마지막 실행 시각, 아키텍처 코드, 파일 크기 + 실행 여부 등 UserAssist,



		AppCompatCache 통해 확인 가능
메모리 아티팩트	python vol.py -f gpt.vmem windows.pstree (명령어)	ChatGPT 프로세스, PID, 설치 경로 등 확인 가능
	python vol.py -f gpt.vmem windows.handles --pid 6484 (명령어)	ChatGPT 프로세스 내 열려있는 리소스(파일 핸들 등) 확인 가능
	python vol.py -f gpt.vmem windows.registry.hivelist (명령어)	ChatGPT 관련 레지스트리 경로 확인 가능
네트워크 아티팩트	C:/Users/forensic/AppData/Local/Packages/OpenAI.ChatGPTDesktop_2p2nqsd0c76g0/LocalCache/Roaming/ChatGPT/Network/TransportSecurity	HTTPS 접속 기록, 적용 도메인, 서버도메인 포함 여부, 최초 적용 시각, 만료 시각 등의 정보 확인
	Users/forensic/AppData/Local/Packages/OpenAI.ChatGPT-Desktop_2p2nqsd0c76g0/LocalCache/Roaming/ChatGPT/Cache/Cache_Data/data_1	ChatGPT API 호출 로그를 통해 offset/limit 파라미터로 과거 대화 목록 불러오기 기능 확인 가능
	Users/forensic/AppData/Local/Packages/OpenAI.ChatGPT-Desktop_2p2nqsd0c76g0/LocalCache/Roaming/ChatGPT/Network/Cookies	Cloudflare 기반 인증 쿠키 및 세션 키 기록 확인 가능
	Users/forensic/AppData/Local/Packages/OpenAI.ChatGPT-Desktop_2p2nqsd0c76g0/LocalCache/Roaming/ChatGPT/Network/NetworkPersistent State	접속한 서버 주소, 프로토콜, 포트, 서버 응답 기록 등 확인 가능
	C:\Users\forensic\AppData\Local\Packages\OpenAI.ChatGPT-Desktop_2p2nqsd0c76g0\LocalCache\Roaming\ChatGPT\Cache\Cache_Data	csrf.json 내 토큰 값 확인 가능
	C:/Users/spdlq/AppData/Local/Packages/OpenAI.ChatGPTDesktop_2p2nqsd0c76g0/LocalCache/Roaming/ChatGPT/Network\Network Persistent State	로컬 네트워크 IP 주소와 기록된 접속 주소 비교를 통해 동일성 확인 가능

	Wireshark 캡처	내부 IP가 OpenAI 인프라와 통신한 정황 확인 가
	Wireshark 캡처	TLS 1.3 또는 QUIC 프로토콜을 통한 Client Hello~Key Exchange 핸드셰이크 흐름 확인 가능
메신저 아티팩트	C:/Users/forensic/AppData/Local/Packages/OpenAI.ChatGPTDesktop_2p2nqsd0c76g0/LocalCache/Roaming/ChatGPT/LocalStorage/leveldb	대화 ID, 제목, 생성/수정 시각, 아카이브 여부, 메모리 사용 여부 등 메타데이터 확인 가능
	C:\Users\forensic\AppData\Local\Packages\OpenAI.ChatGPT-Desktop_2p2nqsd0c76g0\LocalCache\Roaming\ChatGPT\Cache\Cache_Data	employee_leak.csv 등 프롬프트 내 업로드한 파일명, 시각 등 확인 가능
	MFT (Master File Table) : C:\Windows\MFT USN Journal : C:\Windows\Extends\UsnJrnl NTFS 로그 파일 : C:\Windows\LogFile	ABC_com_Email_Password_Leak.csv 등 ChatGPT 생성 파일의 다운로드 흔적 확인 가능

[표 7] 아티팩트 분석 요약표

## IX. 향후 계획

「Digital Forensic Investigation of the ChatGPT Windows Application」 논문에서는 RAM 분석을 통해 프롬프트 대화 내용을 복구하는 방법을 제시하였다. 위 논문에서는 구체적으로, Magnet RAM Capture를 활용하여 ChatGPT 삭제 전과 후 시점의 물리 메모리 덤프를 획득한 뒤, FTK Imager를 통해 Hex/ASCII 뷰에서 ChatGPT 고유 패턴을 검색, 추출함으로써, 디스크에 완전히 삭제된 이후에도 휘발성 메모리에 남아 있는 프롬프트 원문과 응답을 복원하였다. 향후 연구에서는 위 논문에서 검증된 분석 기법을 확장하여 Gemini, Perplexity, Copilot 등 주요 AI 대화형 프로그램의 프롬프트 데이터를

복구할 계획이다. 각 LLM 프로그램의 차이점을 바탕으로 향후 분석 계획은 디스크 기반 분석에서 해당 위치별 흔적을 먼저 검색하고, 메모리 분석 시 프로그램별 고유한 네트워크 요청 파라미터 패턴을 활용하여 휘발성 메모리의 대화 흔적을 추출하는 방식으로 진행할 것이다.

## **X. 참고 문헌**

- [1] OpenAI, 「Chat GPT Overview」, OpenAI, 2025
- [2] Kyungsuk Cho, Yunji Park, Jiyun Kim, Byeongjun Kim, Doowon Jeong, 「Conversational AI forensics: A case study on ChatGPT, Gemini, Copilot, and Claude」, forensic Science International: Digital Investigation, Vol 52, 2025, p. 301855
- [3] Sonali Tyagi, Yufeng Gong, Umit Karabiyik, 「Forensic Analysis and Privacy Implications of LLM Apps: A Case Study of ChatGPT, Copilot, and Gemini」, SSRN Electronic Journal, 2025
- [4] Clinton Walker, Taha Gharaibeh, Ruba Alsmadi, Cory Hall, Ibrahim, 「Forensic Analysis of Artifacts from Microsoft's Multi-Agent LLM Platform AutoGen」, ARES '24: Proceedings of the 19th International Conference on Availability, Reliability and Security, Article No.198, p.1-9, 2024