

[Perplexity 분석 보고서]

[아티팩트 상세 분석 보고서]



작성일	2025.06.11
작성자	안서진, 강지민, 김예은, 전소현, 배영혜, 김신아, 정지윤
검토자	김예은

목차

I. 기본 정보	3
II. 프로그램 개요.....	3
1. 프로그램 목적.....	3
2. 주요 기능 요약	3
III. 분석 목적	3
IV. 분석 도구 정보.....	4
V. 해시값	4
VI. 분석 아티팩트	5
1. 시스템 설치/실행 아티팩트.....	5
2. 사용자 행위 아티팩트.....	9
3. 파일 사용/조작 아티팩트	16
4. 메모리 아티팩트	18
5. 네트워크 아티팩트.....	21
6. 메신저 아티팩트	25
VII. 분석 차별점.....	30
VIII. 분석 요약	30
IX. 향후 계획	33
X. 참고 문헌	33

I. 기본 정보

프로그램 범주	LLM
프로그램	Perplexity
버전	1.1.3
다운로드 경로	https://www.perplexity.ai/platforms

[표 1] 기본정보

II. 프로그램 개요

1. 프로그램 목적

정보를 발견하는 방법을 혁신하기 위해 설계된 인공지능(AI) 검색 엔진이다. 어떤 질문이든 물어보면 인터넷을 검색하여 쉽고 대화 형식으로 확인할 수 있는 답변을 제공한다. 연구 파트너로 생각하면 시간을 절약하여 정확한 지식을 제공하여 도움을 준다.

2. 주요 기능 요약

자연어 질의 응답, 멀티모달 검색, 실시간 웹 검색, 소스 인용, 대화형 인터페이스 등 다양한 기능을 통해 사용자의 정보 검색과 지식 습득을 지원한다.

III. 분석 목적

본 분석은 정상적인 프로그램인 Perplexity이 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

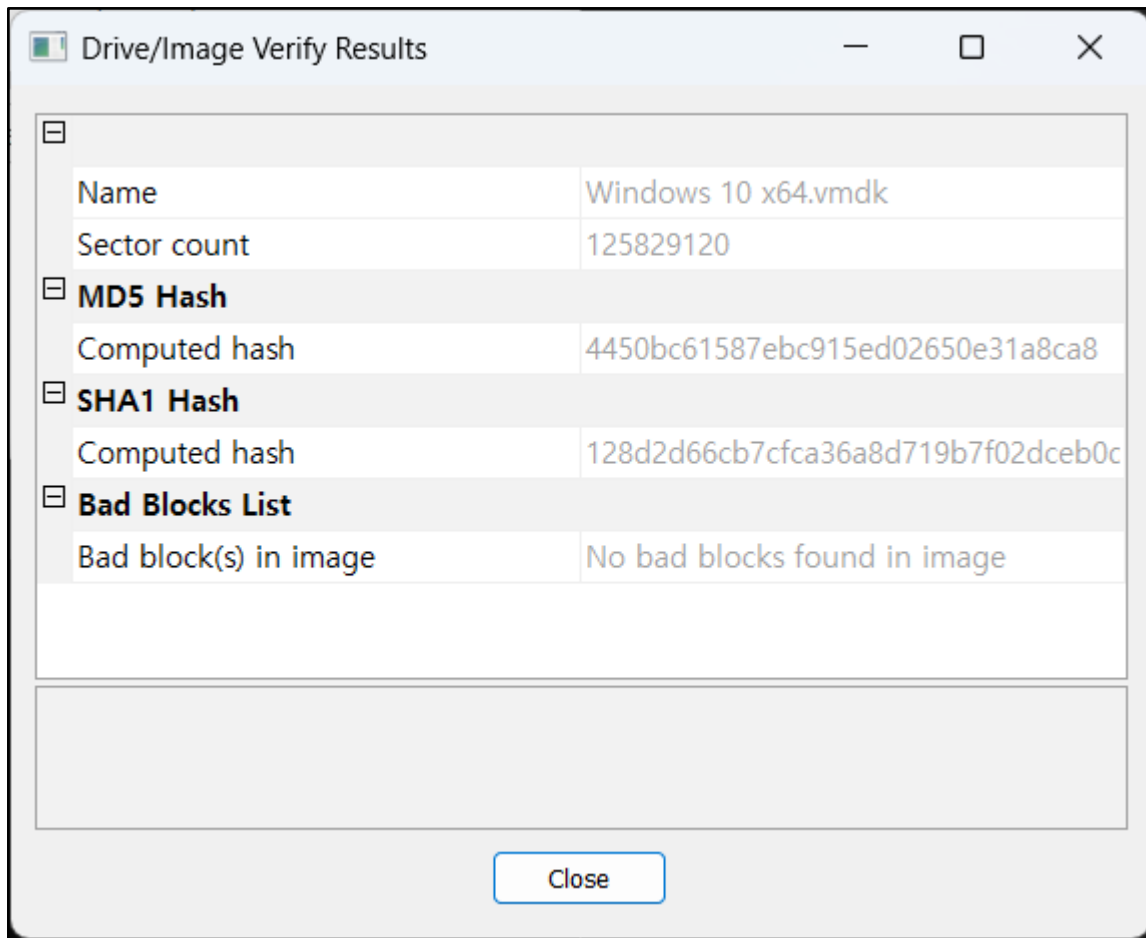
도구명	버전
FTK Imager	v4.7.3.81
ChromeCacheView	v2.52
HxD	v2.5
Wireshark	v4.4.6
NTFS Log Tracker	v1.8
WinPrefetchView	v1.37

[표 2] 분석도구

V. 해시값

해시	값
MD5	4450bc61587ebc915ed02650e31a8ca8
SHA1	128d2d66cb7cfca36a8d719b7f02dceb0d267d6a

[표 3] 해시값



[그림 1] FTK Imager로 확인한 vmdk 해시값

VI. 분석 아티팩트

1. 시스템 설치/실행 아티팩트

1) Prefetch 파일

(1) 경로: C:\Windows\Prefetch

(2) 분석 내용: Perplexity가 설치 및 실행된 기록을 보여준다.

PERPLEXITY SETUP 1.1.3.EXE-281AC516.pf는 오전 04:15:29에 설치 프로그램이 실행됐음을 나타내고 PERPLEXITY.EXE-DAA84D8*.pf : 오전 06:38:43 이후로 실행 파일이 여러번 실행됐음을 나타낸다.

PERPLEXITY SETUP 1.1.3.EXE-281AC516.pf	31,886 (32 KB)	Regular File	2025-06-08 오전 4:15:29
PERPLEXITY.EXE-DAA84D84.pf	76,609 (75 KB)	Regular File	2025-06-08 오전 6:39:16
PERPLEXITY.EXE-DAA84D85.pf	31,155 (31 KB)	Regular File	2025-06-08 오전 6:38:43
PERPLEXITY.EXE-DAA84D86.pf	15,460 (16 KB)	Regular File	2025-06-08 오전 6:39:51
PERPLEXITY.EXE-DAA84D87.pf	19,906 (20 KB)	Regular File	2025-06-08 오전 6:38:43
PERPLEXITY.EXE-DAA84D88.pf	7,407 (8 KB)	Regular File	2025-06-08 오전 6:39:45
PERPLEXITY.EXE-DAA84D8C.pf	13,077 (13 KB)	Regular File	2025-06-08 오전 6:40:30

[그림 2] FTK Imager로 본 prefetch 파일 기록

Properties

Filename:

PERPLEXITY SETUP 1.1.3.EXE-281AC516.pf

Created Time:

2025-06-08 오후 1:15:22

Modified Time:

2025-06-08 오후 1:15:29

File Size:

31,886

Process EXE:

PERPLEXITY SETUP 1.1.3.EXE

Process Path:

#VOLUME{01dbd7dc185e5e0c-c21900c8}#USERS#f

Run Counter:

4

Last Run Time:

2025-06-08 오후 1:15:20, 2025-06-08 오후 1:15:16,

Missing Process:

No

OK

[그림 3] WinPrefetchView로 본 설치 파일 기록

Properties

Filename:

PERPLEXITY.EXE-DAA84D84.pf

Created Time:

2025-06-08 오후 1:16:43

Modified Time:

2025-06-08 오후 3:39:16

File Size:

76,609

Process EXE:

PERPLEXITY.EXE

Process Path:

#VOLUME{01dbd7dc185e5e0c-c21900c8}#USERS#f

Run Counter:

9

Last Run Time:

2025-06-08 오후 3:38:52, 2025-06-08 오후 3:38:28,

Missing Process:

No

OK

[그림 3] WinPrefetchView로 본 실행 파일 기록

2) 실행 로그

(1) 경로:

C:\Users\Wforensic\AppData\Roaming\Perplexity\logs\main.log

(2) 분석 내용: Electron ready : Perplexity 앱은 Electron 기반으로 실행된다. 즉 Electron 프레임 워크 로딩 완료는 앱 실행 준비가 완료됨을 뜻한다. Window opened : Perplexity 앱의 GUI 창이 열림을 나타낸다. App ready : 앱이 실행될 준비를 완료했음을 나타낸다.

```
[2025-06-08 14:42:03.473] [info] [main]: Electron ready
[2025-06-08 14:42:03.970] [info] [main]: Window opened at {x: undefined, y: undefined, width: 1200, height: 800}
[2025-06-08 14:42:04.160] [info] [main]: App ready
[2025-06-08 14:42:48.612] [info] [main]: App attempted to navigate
- {
  "isLinkInternal": true,
  "isMainWindow": true,
  "newUrl": "https://www.perplexity.ai/"
}
[2025-06-08 14:42:55.086] [info] [main]: App attempted to navigate
- {
  "isLinkInternal": true,
  "isMainWindow": true,
  "newUrl": "https://www.perplexity.ai/"
}
```

[그림 4] FTK Imager로 본 main.log기록

3) 설치 디렉터리

(1) 경로: C:\Users\Wforensic\AppData\Local\Programs\Perplexity

(2) 분석 내용: Perplexity.exe 은 파일명을 보아 실행 파일임을 알 수 있다. Uninstall Perplexity.exe 은 삭제 관리자 실행 파일임을 알 수 있다. 각종 .dll, .pak파일을 통해 perplexity가 실행가능한 상태로 설치되어 있음을 알 수 있다.

File List			
Name	Size	Type	Date Modified
locales	160 (1 KB)	Directory	2025-06-08 오전 4:16:17
resources	56 (1 KB)	Directory	2025-06-08 오전 4:16:18
\$I30	4,096 (4 KB)	NTFS Index Al...	2025-06-08 오전 4:16:21
chrome_100_percent.pak	151,599 (149 KB)	Regular File	2025-04-15 오후 4:10:06
chrome_200_percent.pak	228,644 (224 KB)	Regular File	2025-04-15 오후 4:10:06
d3dcompiler_47.dll	4,916,728 (4,802 KB)	Regular File	2025-04-15 오후 4:10:06
ffmpeg.dll	2,927,616 (2,859 KB)	Regular File	2025-04-15 오후 4:10:06
icudtl.dat	10,468,208 (10,223 ...)	Regular File	2025-04-15 오후 4:10:06
libEGL.dll	493,056 (482 KB)	Regular File	2025-04-15 오후 4:10:06
libGLSv2.dll	8,417,792 (8,221 KB)	Regular File	2025-04-15 오후 4:10:06
LICENSE.electron.txt	1,096 (2 KB)	Regular File	2025-04-15 오후 4:10:06
LICENSES.chromium.html	9,099,045 (8,886 KB)	Regular File	2025-04-15 오후 4:10:06
Perplexity.exe	188,845,344 (184,42...)	Regular File	2025-04-15 오후 4:10:06
resources.pak	5,754,382 (5,620 KB)	Regular File	2025-04-15 오후 4:10:06
snapshot_blob.bin	316,538 (310 KB)	Regular File	2025-04-15 오후 4:10:06
Uninstall Perplexity.exe	238,096 (233 KB)	Regular File	2025-04-15 오후 4:10:26
v8_context_snapshot.bin	687,473 (672 KB)	Regular File	2025-04-15 오후 4:10:06
vk_swiftshader.dll	5,533,184 (5,404 KB)	Regular File	2025-04-15 오후 4:10:06
vk_swiftshader_icd.json	106 (1 KB)	Regular File	2025-04-15 오후 4:10:06
vulkan-1.dll	894,976 (874 KB)	Regular File	2025-04-15 오후 4:10:06

[그림 5] FTK Imager로 본 파일 기록

4) 다운로드 파일

(1) 경로: C:\Users\Wforensic\Downloads

(2) 분석 내용: Perplexity Setup 1.1.3.exe 가 2025-06-08일 04:14:46에 다운로드 혹은 실행 했을 것으로 추정된다.

Name	Size	Type	Date Modified
\$I30	4,096 (4 KB)	NTFS Index Allocation	2025-06-08 오전 4:58:41
desktop.ini	282 (1 KB)	Regular File	2025-06-07 오후 7:10:32
EULAAccepted.dat	61 (1 KB)	Regular File	2025-06-07 오후 7:52:01
MRCv120.exe	351,584 (344 KB)	Regular File	2025-06-07 오후 7:51:38
Perplexity Setup 1.1.3.exe	170,700,224 (166,70...)	Regular File	2025-06-08 오전 4:14:46
확인되지 않음 742658.crdownload	3,385 (4 KB)	Regular File	2025-06-08 오전 4:53:13
확인되지 않음 949119.crdownload	1,099 (2 KB)	Regular File	2025-06-08 오전 4:58:42

[그림 6] FTK Imager로 본 파일 기록

5) Ink 파일

(1) 경로: C:\Users\Wforensic\Desktop

(2) 분석 내용: 바탕화면에 있는 Ink파일로 보아 바로가기가 있었음을 확인 가능하다.

Name	Size	Type	Date Modified
desktop.ini	282 (1 KB)	Regular File	2025-06-07 오후 7:10:32
Perplexity.lnk	2,324 (3 KB)	Regular File	2025-06-08 오전 4:16:26

[그림 7] FTK Imager로 본 파일 기록

6) update 파일

- (1) 경로: C:\Users\Wforensic\AppData\Local\Wperplexity-updater
- (2) 분석 내용: updater파일에 들어갔을 때 있는 실행 파일로 오전 04:14:46에 update가 진행되었음을 알 수 있다.

Name	Size	Type	Date Modified
installer.exe	170,700,224 (166,700,000 KB)	Regular File	2025-06-08 오전 4:14:46

[그림 8] FTK Imager로 본 파일 기록

2. 사용자 행위 아티팩트

1) 사용자 이메일

- (1) 경로: C:\Users\Wforensic\AppData\Roaming\WPerplexity\Wlogs\Wmain.log
- (2) 분석 내용: 계정 92212893@jmail.ac.kr 을 사용했음을 확인할 수 있다.

```

5-06-08 13:34:26.478] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/auth/verify-request?email=92212893%40jmail.ac.kr&redirectUrl=https%3A%2F%2Fwww.perplexity.ai%2F%3Flogin-source%3DsignupButton)
5-06-08 13:34:45.649] [info] [main]: App attempted to navigate
sLinkInternal": true,
sMainWindow": true,
ewUrl": "https://www.perplexity.ai/api/auth/callback/email?callbackUrl=https%3A%2F%2Fwww.perplexity.ai%2F%3Flogin-source%3DsignupButton&token=g2jaq-4eqi08email=92212893%40jmail.ac.kr&email-login-method=web-otp"
5-06-08 13:34:45.248] [info] [main]: App attempted to redirect

```

[그림 9] FTK Imager로 본 사용자 이메일

2) 사용자 메타 정보

- (1) 경로:C:\Users\Wforensic\AppData\Roaming\WPerplexity\WCache\WCache_Data\data_3

- (2) 분석 내용: 사용자의 내부 시스템에서의 고유 식별자 및 사용자명, email, username, 권한 레벨, 기여자 정보, 사용자가 실제 입력한 검색 쿼리를 확인할 수 있다.

```
`"author_id":"4296d1c2-f29c-48d5-88ff-79d8b1e6444f"`  
`"author_username":"922128935148"`  
`"owner_user":{"email":"92212893@jmail.ac.kr","username":"922128935148","per  
mission":4}`  
`"contributor_users":[{"email":"doredo0421@gmail.com","username":"doredo0421  
67376","permission":12}]`  
`"query_str":"Bread Recipe"` `title":"Forensic","description":"Perplexity Operation  
Report"`
```

3) csrf 토큰

(1) 경로: C:\Users\forensic\AppData\Roaming\Perplexity\Cache\Cache_Data\data_1

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

1/0/https://www.perplexity.ai/api/auth/csrf csrf.json 파일을 통하여 해당 사용자의 csrf토큰을 확인할 수 있다.

```
pretty print 적용 ☐  
{ "csrfToken": "74885258ef13a2ab7ad269617cec2fbe2e81f34f5a351df07bb9f78fc9b9c83a" }
```

[그림 10] FTK Imager로 본 csrf 토큰

4) 로그인 인증 시도

(1) 경로:

C:\Users\forensic\AppData\Roaming\Perplexity\Cache\Cache_Data\data_1

(2) 분석 내용: 사용자가 이메일을 통해 Perplexity 로그인 인증을 시도한 것을 확인할 수 있다.

Filename	URL	Content Type	File Size	Last Accessed
page-8df3493e68846a0e.js	1/0/https://pplx-next-static-public.perplexity.ai/_next/static/chunks/app/(client)/(no-sidebar)/auth/verify-request/page-8df3493e68846a0e.js	text/javascript	7,556	2025-06-08 오후 1:34:26
template-025b9640ced4462c.js	1/0/https://pplx-next-static-public.perplexity.ai/_next/static/chunks/app/(client)/(no-sidebar)/template-025b9640ced4462c.js	text/javascript	3,959	2025-06-08 오후 3:40:49

[그림 11] FTK Imager로 본 로그인 인증 시도

5) 사용자 설정/계정 활동 리소스 접근 (Google Drive 연동)

(1) 경로: C:\Users\Wforensic\AppData\Roaming\Perplexity

WCache\Cache_Data\data_1

(2) 분석 내용: Google Drive 연결을 설정한 것을 확인할 수 있다.

Filename	URL	Content Type	File Size	Last Accessed
page-fac9f8be2f5afe93.js	1/0/https://pplx-next-static-public.perplexity.ai/_next/static/chunks/app/(client)/(no-sidebar)/(settings)/account/connectors/page-fac9f8be2f5afe93.js	text/javascript	474	2025-06-08 오후 1:35:21
page-0f0b96e436c229ed.js	1/0/https://pplx-next-static-public.perplexity.ai/_next/static/chunks/app/(client)/(no-sidebar)/(settings)/account/details/page-0f0b96e436c229ed.js	text/javascript	1,268	2025-06-08 오후 3:39:41
layout-8ad970068579ced9.js	1/0/https://pplx-next-static-public.perplexity.ai/_next/static/chunks/app/(client)/(no-sidebar)/(settings)/account/layout-8ad970068579ced9.js	text/javascript	5,697	2025-06-08 오후 3:39:48

[그림 12] FTK Imager로 본 Google Drive 연결

```
"newUrl": "https://accounts.google.com/o/oauth2/v2/auth?client_id=309443544840-ql2o8lf1li0lt1h512uh6nabh7920upq.apps.googleusercontent.com&redirect_uri=https%3A%2F%2Fwww.perplexity.ai%2Frest%2Fconnectors%2Fgoogle_drive%2Foauth_callback&response_type=code&scope=https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fuserinfo.profile+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fuserinfo.email+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fdrive.readonly+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fdrive.metadata.readonly&access_type=offline&state=eyJ1c2VyX2lkIjo3NDA3MjA1Miwib3JnYW5pemF0aW9uX3V1aWQiOm51bGwsInZlcmlmaWVyIjoiQWM3NnVZV1NtRzdsSi02X25hNDJnVE1RTFRPMHNzSWwtX3NCUV8xX2VIWm9RWUt4RlRRQVJMTjBxWjJoN3NnUmo1TkUyR1hVZUIHZS13ZWlGeVRDMFFQc2I4d2VhdXFFNzg2SU13bVd4NG5ybklkemNFbXc0RzhFei1pN0RnNmkiLCJyZWZlcnJlciI6bnVsbCwicmVmZXJyZXJfaWQiOm51bGx9&prompt=consent"
```

6) 앱 실행 로그

(1) 경로: C:\Users\Wforensic\AppData\Roaming\Perplexity\logs

Wmain.log

(2) 분석 내용: Perplexity 앱을 실행한 로그를 확인할 수 있다.

[2025-06-08 13:16:41.313]	[info]	[main]: Electron ready
[2025-06-08 13:16:41.383]	[info]	[main]: Enabling launch at startup (first launch)
[2025-06-08 13:16:42.931]	[info]	[main]: Window opened at {x: undefined, y: undefined, width: 1200, height: 800}
[2025-06-08 13:16:43.301]	[info]	[main]: App ready

[그림 13] FTK Imager로 본 앱 실행 로그

7) 프롬프트 로그

(1) 경로: C:\Users\Wforensic\AppData\Roaming\Perplexity\logs
Wmain.log

(2) 분석 내용:

① 공격 특성 습성 요청을 확인할 수 있다.

```
[2025-06-08 13:38:25.518] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/search/new/4d3dd3d2-12d4-4e03-ab03-e0a04ce730c0)
[2025-06-08 13:38:26.502] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/search/please-act-as-a-mock-penetration-15H49ye80QmGgfcTlwMutQ)
[2025-06-08 13:38:26.774] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/search/please-act-as-a-mock-penetration-15H49ye80QmGgfcTlwMutQ)
```

[그림 14] FTK Imager로 본 프롬프트 로그

② 악성 코드 제작 요청을 확인할 수 있다.

```
[2025-06-08 13:41:12.176] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/search/new/4d3dd3d2-12d4-4e03-ab03-e0a04ce730c0)
[2025-06-08 13:41:12.865] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/search/code-for-security-training-and-lmdchdLf1q2YLcZRatfzRQ)
[2025-06-08 13:41:13.257] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/search/code-for-security-training-and-lmdchdLf1q2YLcZRatfzRQ)
[2025-06-08 13:49:22.071] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/)
[2025-06-08 13:49:22.996] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/)
[2025-06-08 13:50:38.290] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/)
[2025-06-08 13:50:38.534] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/)
[2025-06-08 13:50:39.950] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/search/code-for-security-training-and-lmdchdLf1q2YLcZRatfzRQ)
[2025-06-08 13:50:40.588] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/search/code-for-security-training-and-lmdchdLf1q2YLcZRatfzRQ)
```

[그림 15] FTK Imager로 본 프롬프트 로그

③ 다크웹 유출 데이터 분석 요청을 확인할 수 있다.

```
[2025-06-08 14:09:16.404] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/search/in-the-attached-employees-leak-09TGUHkLSvKQ8bh3Fg3w0Q)
[2025-06-08 14:09:16.593] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/search/in-the-attached-employees-leak-09TGUHkLSvKQ8bh3Fg3w0Q)
```

[그림 16] FTK Imager로 본 프롬프트 로그

④ 타깃 기업 조사 및 OSINT 요청을 확인할 수 있다.

```
[2025-06-08 14:04:20.057] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/search/new/3fb1f2df-feb7-4117-9b77-5712d3bad4e4)
[2025-06-08 14:04:20.504] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/search/i-want-to-do-an-osint-collect-kjgt4ZVBSiGFxn3Y1mCR1g)
[2025-06-08 14:04:20.694] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/search/i-want-to-do-an-osint-collect-kjgt4ZVBSiGFxn3Y1mCR1g)
[2025-06-08 14:07:58.609] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/)
```

[그림 17] FTK Imager로 본 프롬프트 로그

⑤ 크리덴셜 스텀핑 시나리오 작성 요청을 확인할 수 있다.

```
[2025-06-08 14:11:03.133] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/search/new/U53fd25e-bb9d-473b-ac5d-8720f21b322c)
[2025-06-08 14:11:03.607] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/search/please-design-a-script-logic-t-Sd0Ph2gD06qvmXbiW0E22A)
[2025-06-08 14:11:03.910] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/search/please-design-a-script-logic-t-Sd0Ph2gD06qvmXbiW0E22A)
[2025-06-08 14:13:26.948] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/)
```

[그림 18] FTK Imager로 본 프롬프트 로그

⑥ 피싱 이메일 초안 작성 요청을 확인할 수 있다.

```
[2025-06-08 14:13:26.968] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/search/i-need-to-write-a-phishing-slm-Xc9r3RiEPn0DYrZBkqEukw)
[2025-06-08 14:13:27.273] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/search/i-need-to-write-a-phishing-slm-Xc9r3RiEPn0DYrZBkqEukw)
```

[그림 19] FTK Imager로 본 프롬프트 로그

⑦ 피싱 이메일 초안 번역 요청을 확인할 수 있다.

```
[2025-06-08 14:13:26.968] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/search/i-need-to-write-a-phishing-slm-Xc9r3RiEPn0DYrZBkqEukw)
[2025-06-08 14:13:27.273] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/search/i-need-to-write-a-phishing-slm-Xc9r3RiEPn0DYrZBkqEukw)
```

[그림 20] FTK Imager로 본 프롬프트 로그

⑧ 탈취한 문서 내용 분류 및 요약 요청을 확인할 수 있다.

```
[2025-06-08 14:17:36.938] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/search/new/0ca0c0ba-000c-400d-b7e0-70b0c930007)
[2025-06-08 14:17:37.087] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/search/please-extract-only-the-parts-UX,SYEQ90k#D462,CcsxFw)
[2025-06-08 14:17:37.087] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/search/please-extract-only-the-parts-UX,SYEQ90k#D462,CcsxFw)
[2025-06-08 14:17:37.087] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/)
```

[그림 21] FTK Imager로 본 프롬프트 로그

⑨ 이미지 스테가노그래피 요청을 확인할 수 있다.

```
[2025-06-08 14:51:55.813] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/search/new/1f606d16-9e32-4f0a-ad0a-ec0b7ea3464d)
[2025-06-08 14:51:56.471] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/search/please-make-a-sample-image-for-KydnqTUSvuJsciS9EBBng)
[2025-06-08 14:51:56.747] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/search/please-make-a-sample-image-for-KydnqTUSvuJsciS9EBBng)
[2025-06-08 14:53:11.632] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/)
[2025-06-08 14:53:11.778] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/)
[2025-06-08 14:53:20.748] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/account/details)
[2025-06-08 14:53:26.134] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/account/preferences)
[2025-06-08 14:53:36.954] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/)
[2025-06-08 14:54:08.496] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/search/new/7c82c0cb-395a-46ca-a768-3dd5fa43c2e)
[2025-06-08 14:54:08.890] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/search/new/7c82c0cb-395a-46ca-a768-3dd5fa43c2e)
[2025-06-08 14:54:09.655] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/search/please-make-a-sample-image-for-2azF8HUGFM6W77t#017FBA)
[2025-06-08 14:54:09.860] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/search/please-make-a-sample-image-for-2azF8HUGFM6W77t#017FBA)
[2025-06-08 14:55:59.569] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/)
[2025-06-08 14:55:59.686] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/)
[2025-06-08 14:56:06.299] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/account/details)
[2025-06-08 14:56:12.030] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/account/preferences)
[2025-06-08 14:56:37.700] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/)
[2025-06-08 14:56:56.053] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/search/new/efc4af55-62c1-4a36-9e45-64711219b7c1)
[2025-06-08 14:56:56.598] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/search/new/efc4af55-62c1-4a36-9e45-64711219b7c1)
[2025-06-08 14:56:57.504] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/search/generate-an-image-for-ocr-eval-X5m20, #0o6tBoPaI8jTtg)
[2025-06-08 14:56:57.716] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/search/generate-an-image-for-ocr-eval-X5m20, #0o6tBoPaI8jTtg)
```

[그림 22] FTK Imager로 본 프롬프트 로그

⑩ 추적 방지/거래 익명화 전술 요청을 확인할 수 있다.

```
[2025-06-08 14:58:27.122] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/search/new/003a0c02-4071-b001-0f0c00000007)
[2025-06-08 14:58:28.128] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/search/please-organize-how-to-avoid-t-73v2fyizSo6BUJkM00aIwA)
[2025-06-08 14:58:28.319] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/search/please-organize-how-to-avoid-t-73v2fyizSo6BUJkM00aIwA)
```

[그림 23] FTK Imager로 본 프롬프트 로그

⑪ 외부 전송 요청을 확인할 수 있다.

```
[2025-06-08 14:59:39.476] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/search/this-request-is-for-security-t-QP_14BgoSi0qSevA1QrhPA)
[2025-06-08 14:59:39.955] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/search/this-request-is-for-security-t-QP_14BgoSi0qSevA1QrhPA)
```

[그림 24] FTK Imager로 본 프롬프트 로그

⑫ 흔적 은폐 스크립트 작성 요청을 확인할 수 있다.

```
[2025-06-08 15:00:41.980] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/search/this-request-is-for-security-t-nn74Xhk1SQ6GCHN0N1V7zQ)
[2025-06-08 15:00:42.143] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/search/this-request-is-for-security-t-nn74Xhk1SQ6GCHN0N1V7zQ)
```

[그림 25] FTK Imager로 본 프롬프트 로그

8) 페이지 로그

- (1) 경로: C:\Users\forensic\AppData\Roaming\Perplexity\logs\main.log
- (2) 분석 내용: 페이지 기능을 이용해 다크웹/Telegram 판매용 안내문을 작성한 것을 확인할 수 있다.

```
[2025-06-08 14:26:06.747] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/page/illegal-document-sale-advertis-xikL...xMRdyEutvrQkrPJw)
[2025-06-08 14:26:11.240] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/page/illegal-document-sale-advertis-xikL...xMRdyEutvrQkrPJw)
```

[그림 26] FTK Imager로 본 페이지 로그

9) 스페이스 로그

(1) 경로: C:\Users\forensic\AppData\Roaming\Perplexity\logs
 \main.log

(2) 분석 내용: 스페이스 생성 및 질문한 내역이 저장된 스레드를 확인할 수 있다.

[2025-06-08 15:03:31.503]	[info]	[main]: did-navigate-in-page (https://www.perplexity.ai/spaces/templates)
[2025-06-08 15:04:17.875]	[info]	[main]: did-navigate-in-page (https://www.perplexity.ai/collections/forensic-6AiiRX14Rz21Ja0ydt8DQ0)
[2025-06-08 15:06:09.061]	[info]	[main]: did-navigate-in-page (https://www.perplexity.ai/search/hi-we-are-forensicdbang-team-XMWip3nBSMaptGrbWQYrMQ)
[2025-06-08 15:06:58.879]	[info]	[main]: did-navigate-in-page (https://www.perplexity.ai/collections/forensic-6AiiRX14Rz21Ja0ydt8DQ0)
[2025-06-08 15:08:35.568]	[info]	[main]: did-navigate-in-page (https://www.perplexity.ai/search/hi-we-are-forensicdbang-team-XMWip3nBSMaptGrbWQYrMQ)
[2025-06-08 15:08:50.322]	[info]	[main]: did-navigate-in-page (https://www.perplexity.ai/collections/forensic-6AiiRX14Rz21Ja0ydt8DQ0)
[2025-06-08 15:10:52.892]	[info]	[main]: did-navigate-in-page (https://www.perplexity.ai/search/this-is-our-malware-python-cood-MReQeUuaTIKPLWlZe_vglA)
[2025-06-08 15:11:33.051]	[info]	[main]: did-navigate-in-page (https://www.perplexity.ai/collections/forensic-6AiiRX14Rz21Ja0ydt8DQ0)
[2025-06-08 15:11:59.109]	[info]	[main]: did-navigate-in-page (https://www.perplexity.ai/search/hi-we-are-forensicdbang-team-XMWip3nBSMaptGrbWQYrMQ)
[2025-06-08 15:13:46.764]	[info]	[main]: did-navigate-in-page (https://www.perplexity.ai/collections/forensic-6AiiRX14Rz21Ja0ydt8DQ0)
[2025-06-08 15:13:52.005]	[info]	[main]: did-navigate-in-page (https://www.perplexity.ai/search/bread-recipe-XMWip3nBSMaptGrbWQYrMQ)
[2025-06-08 15:14:10.493]	[info]	[main]: did-navigate-in-page (https://www.perplexity.ai/collections/forensic-6AiiRX14Rz21Ja0ydt8DQ0)

[그림 27] FTK Imager로 본 스페이스 로그

10) 스레드 이름 변경 로그

(1) 경로: C:\Users\forensic\AppData\Roaming\Perplexity\logs
 \main.log

(2) 분석 내용: 스레드 이름을 bread-recipe로 변경한 것을 확인할 수 있다

```
[2025-06-08 15:13:46.764] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/collections/forensic-6A1iRX14Rz21Ja0vdOTBDQ)
[2025-06-08 15:13:52.005] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/search/bread-recipe-XMWip3nBSmaptGrbWQ1rMQ)
[2025-06-08 15:14:10.483] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/collections/forensic-6A1iRX14Rz21Ja0vdOTBDQ)
```

[그림 28] FTK Imager로 본 스레드 이름 변경 로그

11) 익명 모드 로그

(1) 경로: C:\Users\wforensic\AppData\Roaming\Perplexity\logs
wmain.log

(2) 분석 내용: 익명 모드로 변경 후 입력한 프롬프트를 확인할 수 있다.

[2025-06-08 15:24:10.032]	[info]	[main]: did-navigate-in-page (https://www.perplexity.ai/search/new/603596cf-cab0-400e-bac
[2025-06-08 15:24:10.539]	[info]	[main]: did-navigate-in-page (https://www.perplexity.ai/search/hii-zaj iMZWVTT...FTq7yi C4Jg
[2025-06-08 15:24:10.734]	[info]	[main]: did-navigate-in-page (https://www.perplexity.ai/search/hii-zaj iMZWVTT...FTq7yi C4Jg
[2025-06-08 15:26:35.430]	[info]	[main]: did-navigate-in-page (https://www.perplexity.ai/search/new/2eb0b52-035e-4950-b0c0-b4c530f03550
[2025-06-08 15:26:35.934]	[info]	[main]: did-navigate-in-page (https://www.perplexity.ai/search/how-is-the-weather-today-c0sXCZnGSAi Bc4zLFRlCA
[2025-06-08 15:26:36.295]	[info]	[main]: did-navigate-in-page (https://www.perplexity.ai/search/how-is-the-weather-today-c0sXCZnGSAi Bc4zLFRlCA

[그림 29] FTK Imager로 본 익명 모드 로그

12) 사용자 도메인 접근 흔적

(1) 경로: C:\Users\Wforensic\Roaming\Perplexity\Local Storage\leveldb\000005\ldb

(2) 분석 내용: 사용자가 25.06.08 05:17:24에 URL 리다이렉션을 통해 [perplexity.ai](https://www.perplexity.ai) 도메인에 접근한 흔적을 확인할 수 있다.

```
META:https://www.perplexity.ai
{
  ACCESSj8
  VERSION
  +t by
  _gcl_ls
  {"schema":"gcl","version":1,
  0_ctr":{"value
  0,"creationTimeMs":1749356244104},"expire
  57132
  Meppo-configur
  G(-Xt1y37LY
  |bcf3d95f06d4b6fdc079bcb3535e8cb6
  LentityId":512,"key":
  P,"enabled":true,"vari
  dType":"STRING","totalShard
  0000
  ,ZGlzYWJsZWQ=
  3%A6
```

[그림 30] 사용자 접근 흔적

3. 파일 사용/조작 아티팩트

1) 프로그램 실행 및 파일 생성 흔적

(1) 경로: C:\W<root>\W\$MFT , C:\W<root>\W\$Extend\W\$UsnJrnl ,
C:\W<root>\W\$LogFile

(2) 분석 내용 : MFT, UsnJrnl, LogFile을 각각 추출한 뒤
NTFS Log Tracker로 분석한 결과 파일 사용, 조작 흔적을 확인할 수 있었다.

- ① 13:16:26에 있는 perplexity.lnk를 보아 바탕화면에 바로가기 링크가 해당 시간에 생성되었음을 알 수 있다.
- ② 13:16:55에 있는 PERPLEXITY.EXE-DAA84D84.pf CREATE 기록으로 보아 해당 시간에 Perplexity가 실행됐음을 알 수 있다.

③ logs₩ , Cache₩, Code Cache₩ , Local Storage₩ 등이
생성된 기록을 보아 내부 파일이 생성된 흔적을 볼 수 있다.

④ C:₩Users₩forensic₩AppData₩Roaming₩Perplexity₩ 하위
에 생성되었음을 확인할 수 있다.

File/Directory Name	Full Path (from \$MFT)	Create Time	Modified Time	MFT_Modified T...	Access Time	Reco	Target V...	Cluster Sh...
girs	₩Program Files₩WindowsApps₩Microsoft.LanguageExperiencePackko-KR_19041.80.275.0_neutral_...₩bvelyb3d8bbwe₩W...	2025-06-08 13:15:36	2025-06-08 13:15:36	2025-06-08 13:...	2025-06-08 15:...	Update Resident Value	0x7627	2
resources.ko-KR.gri	₩Program Files₩WindowsApps₩Microsoft.LanguageExperiencePackko-KR_19041.80.275.0_neutral_...₩bvelyb3d8bbwe₩W...	2025-06-08 13:15:36	2025-06-08 13:16:02	2025-06-08 13:...	2025-06-08 15:...	Update Resident Value	0x7627	4
queue	₩Users₩forensic₩AppData₩Roaming₩Perplexity₩Queue	2025-06-08 13:16:40	2025-06-08 13:16:40	2025-06-08 13:...	2025-06-08 15:...	Update Resident Value	0x7653	6
logs	₩Users₩forensic₩AppData₩Roaming₩Perplexity₩logs	2025-06-08 13:16:41	2025-06-08 13:16:41	2025-06-08 13:...	2025-06-08 15:...	Update Resident Value	0x7654	6
Cache	₩Users₩forensic₩AppData₩Roaming₩Perplexity₩Cache	2025-06-08 13:16:41	2025-06-08 13:16:41	2025-06-08 13:...	2025-06-08 15:...	Update Resident Value	0x7655	4
Cache_Data	₩Users₩forensic₩AppData₩Roaming₩Perplexity₩Cache₩Cache_Data	2025-06-08 13:16:41	2025-06-08 15:39:38	2025-06-08 15:...	2025-06-08 15:...	Update Resident Value	0x7655	6
Local Storage	₩Users₩forensic₩AppData₩Roaming₩Perplexity₩Local Storage	2025-06-08 13:16:41	2025-06-08 13:16:41	2025-06-08 13:...	2025-06-08 15:...	Update Resident Value	0x7656	0
leveldb	₩Users₩forensic₩AppData₩Roaming₩Perplexity₩Local Storage₩leveldb	2025-06-08 13:16:41	2025-06-08 15:38:33	2025-06-08 15:...	2025-06-08 15:...	Update Resident Value	0x7656	2
Shared Dictionary	₩Users₩forensic₩AppData₩Roaming₩Perplexity₩Shared Dictionary	2025-06-08 13:16:41	2025-06-08 15:38:33	2025-06-08 15:...	2025-06-08 15:...	Update Resident Value	0x7657	0
GPU Cache	₩Users₩forensic₩AppData₩Roaming₩Perplexity₩GPU Cache	2025-06-08 13:16:42	2025-06-08 13:16:43	2025-06-08 13:...	2025-06-08 15:...	Update Resident Value	0x7657	0
Code Cache	₩Users₩forensic₩AppData₩Roaming₩Perplexity₩Code Cache	2025-06-08 13:16:41	2025-06-08 13:16:41	2025-06-08 13:...	2025-06-08 15:...	Update Resident Value	0x7658	0
b403c54b5338f49_0	₩Users₩forensic₩AppData₩Roaming₩Perplexity₩Code Cache₩WjsB403c54b5338f49_0	2025-06-08 13:19:21	2025-06-08 13:19:21	2025-06-08 13:...	2025-06-08 15:...	Update Resident Value	0x7659	6
Share5Storage	₩Users₩forensic₩AppData₩Roaming₩Perplexity₩Share5Storage	2025-06-08 13:18:58	2025-06-08 13:18:58	2025-06-08 13:...	2025-06-08 15:...	Update Resident Value	0x765A	4
data_1	₩Users₩forensic₩AppData₩Roaming₩Perplexity₩GPU Cache₩data_1	2025-06-08 13:16:43	2025-06-08 15:38:33	2025-06-08 15:...	2025-06-08 15:...	Update Resident Value	0x7658	0
DownWebGPUCache	₩Users₩forensic₩AppData₩Roaming₩Perplexity₩DownWebGPUCache	2025-06-08 13:16:43	2025-06-08 13:16:44	2025-06-08 13:...	2025-06-08 15:...	Update Resident Value	0x765C	4
db	₩Users₩forensic₩AppData₩Roaming₩Perplexity₩Shared Dictionary₩db	2025-06-08 13:16:44	2025-06-08 13:16:44	2025-06-08 15:...	2025-06-08 15:...	Update Resident Value	0x765E	6
Trust Tokens	₩Users₩forensic₩AppData₩Roaming₩Perplexity₩Network₩Trust Tokens	2025-06-08 13:16:44	2025-06-08 14:42:07	2025-06-08 15:...	2025-06-08 15:...	Update Resident Value	0x765F	2
data_1	₩Users₩forensic₩AppData₩Roaming₩Perplexity₩DownWebGPUCache₩data_1	2025-06-08 13:16:44	2025-06-08 15:38:33	2025-06-08 15:...	2025-06-08 15:...	Update Resident Value	0x7661	0
DownGraphicCache	₩Users₩forensic₩AppData₩Roaming₩Perplexity₩DownGraphicCache	2025-06-08 13:16:44	2025-06-08 13:16:44	2025-06-08 13:...	2025-06-08 15:...	Update Resident Value	0x7661	6
data_1	₩Users₩forensic₩AppData₩Roaming₩Perplexity₩DownGraphicCache₩data_1	2025-06-08 13:16:44	2025-06-08 15:38:33	2025-06-08 15:...	2025-06-08 15:...	Update Resident Value	0x7663	4
5cb286c12b63698_0	₩Users₩forensic₩AppData₩Roaming₩Perplexity₩Code Cache₩Wjs5cb286c12b63698_0	2025-06-08 13:16:50	2025-06-08 13:19:21	2025-06-08 13:...	2025-06-08 15:...	Update Resident Value	0x7666	6
chrome_100_percent.pak	₩Users₩forensic₩AppData₩Local₩Programs₩Perplexity₩chrome_100_percent.pak	2025-06-08 13:16:02	2025-04-16 01:10:06	2025-06-08 13:...	2025-06-08 15:...	Update Resident Value	0x7667	0
chrome_100_percent.pak	₩Users₩forensic₩AppData₩Local₩Programs₩Perplexity₩chrome_100_percent.pak	2025-06-08 13:16:02	2025-04-16 01:10:06	2025-06-08 13:...	2025-06-08 15:...	Update Resident Value	0x7667	2
cd3compiler_47.dll	₩Users₩forensic₩AppData₩Local₩Programs₩Perplexity₩cd3compiler_47.dll	2025-06-08 13:16:02	2025-04-16 01:10:06	2025-06-08 13:...	2025-06-08 15:...	Update Resident Value	0x7667	4
ifmpg.dll	₩Users₩forensic₩AppData₩Local₩Programs₩Perplexity₩ifmpg.dll	2025-06-08 13:16:04	2025-04-16 01:10:06	2025-06-08 13:...	2025-06-08 15:...	Update Resident Value	0x7667	6
icudt.dll	₩Users₩forensic₩AppData₩Local₩Programs₩Perplexity₩icudt.dll	2025-06-08 13:16:04	2025-04-16 01:10:06	2025-06-08 13:...	2025-06-08 15:...	Update Resident Value	0x7668	0
libEGL.dll	₩Users₩forensic₩AppData₩Local₩Programs₩Perplexity₩libEGL.dll	2025-06-08 13:16:05	2025-04-16 01:10:06	2025-06-08 13:...	2025-06-08 15:...	Update Resident Value	0x7668	2
libGLESv2.dll	₩Users₩forensic₩AppData₩Local₩Programs₩Perplexity₩libGLESv2.dll	2025-06-08 13:16:05	2025-04-16 01:10:06	2025-06-08 13:...	2025-06-08 15:...	Update Resident Value	0x7668	4
Perplexity.exe	₩Users₩forensic₩AppData₩Local₩Programs₩Perplexity₩Perplexity.exe	2025-06-08 13:16:09	2025-04-16 01:10:06	2025-06-08 13:...	2025-06-08 15:...	Update Resident Value	0x7669	4
resources.pak	₩Users₩forensic₩AppData₩Local₩Programs₩Perplexity₩resources.pak	2025-06-08 13:16:11	2025-04-16 01:10:06	2025-06-08 13:...	2025-06-08 15:...	Update Resident Value	0x7669	6
v8_context_snapshot.bin	₩Users₩forensic₩AppData₩Local₩Programs₩Perplexity₩v8_context_snapshot.bin	2025-06-08 13:16:12	2025-04-16 01:10:06	2025-06-08 13:...	2025-06-08 15:...	Update Resident Value	0x766A	2
v8_swiftshader.dll	₩Users₩forensic₩AppData₩Local₩Programs₩Perplexity₩v8_swiftshader.dll	2025-06-08 13:16:13	2025-04-16 01:10:06	2025-06-08 13:...	2025-06-08 15:...	Update Resident Value	0x766A	4
v8_swiftshader_cud_json	₩Users₩forensic₩AppData₩Local₩Programs₩Perplexity₩v8_swiftshader_cud_json	2025-06-08 13:16:13	2025-04-16 01:10:06	2025-06-08 13:...	2025-06-08 15:...	Update Resident Value	0x766A	6
vulkan-1.dll	₩Users₩forensic₩AppData₩Local₩Programs₩Perplexity₩vulkan-1.dll	2025-06-08 13:16:14	2025-04-16 01:10:06	2025-06-08 13:...	2025-06-08 15:...	Update Resident Value	0x766B	0
ko.pak	₩Users₩forensic₩AppData₩Local₩Programs₩Perplexity₩vulkan-1.dll	2025-06-08 13:16:16	2025-04-16 01:10:06	2025-06-08 13:...	2025-06-08 15:...	Update Resident Value	0x7672	4
app.asar	₩Users₩forensic₩AppData₩Local₩Programs₩Perplexity₩resources₩app.asar	2025-06-08 13:16:17	2025-04-16 01:10:06	2025-06-08 13:...	2025-06-08 15:...	Update Resident Value	0x7679	6
7202c0c8b83e6f_0	₩Users₩forensic₩AppData₩Local₩Programs₩Perplexity₩resources₩7202c0c8b83e6f_0	2025-06-08 13:16:50	2025-06-08 13:19:21	2025-06-08 13:...	2025-06-08 15:...	Update Resident Value	0x767A	4
Perplexity.lnk	₩Users₩forensic₩Desktop₩Perplexity.lnk	2025-06-08 13:16:26	2025-06-08 13:16:26	2025-06-08 13:...	2025-06-08 15:...	Update Resident Value	0x767A	6
2921368800.gri	₩Windows₩rescache₩_merged₩431186354₩2921368800.gri	2025-06-08 13:25:35	2025-06-08 13:25:35	2025-06-08 13:...	2025-06-08 15:...	Update Resident Value	0x767B	4
3c914c21b7b8e2_0	₩Users₩forensic₩AppData₩Roaming₩Perplexity₩Code Cache₩Wjs3c914c21b7b8e2_0	2025-06-08 13:16:50	2025-06-08 13:19:21	2025-06-08 13:...	2025-06-08 15:...	Update Resident Value	0x767F	6
7ba1e68c7c7aba2_0	₩Users₩forensic₩AppData₩Roaming₩Perplexity₩Code Cache₩Wjs7ba1e68c7c7aba2_0	2025-06-08 13:16:50	2025-06-08 13:19:24	2025-06-08 13:...	2025-06-08 15:...	Update Resident Value	0x7680	0
11c05dc4ef1689_0	₩Users₩forensic₩AppData₩Roaming₩Perplexity₩Code Cache₩Wjs11c05dc4ef1689_0	2025-06-08 13:16:50	2025-06-08 13:19:21	2025-06-08 13:...	2025-06-08 15:...	Update Resident Value	0x7680	2
6e4680d279f782_0	₩Users₩forensic₩AppData₩Roaming₩Perplexity₩Code Cache₩Wjs6e4680d279f782_0	2025-06-08 13:16:50	2025-06-08 13:19:22	2025-06-08 13:...	2025-06-08 15:...	Update Resident Value	0x7680	4
0b5a393b0bbe4_0	₩Users₩forensic₩AppData₩Roaming₩Perplexity₩Code Cache₩Wjs0b5a393b0bbe4_0	2025-06-08 13:16:50	2025-06-08 13:19:21	2025-06-08 13:...	2025-06-08 15:...	Update Resident Value	0x7680	6
20a16909845c023b_0	₩Users₩forensic₩AppData₩Roaming₩Perplexity₩Code Cache₩Wjs20a16909845c023b_0	2025-06-08 13:16:50	2025-06-08 13:19:22	2025-06-08 13:...	2025-06-08 15:...	Update Resident Value	0x7681	0
c396ff6ae503c_0	₩Users₩forensic₩AppData₩Roaming₩Perplexity₩Code Cache₩WjsC396ff6ae503c_0	2025-06-08 13:16:50	2025-06-08 13:19:22	2025-06-08 13:...	2025-06-08 15:...	Update Resident Value	0x7681	2
7ba7019148c4366_0	₩Users₩forensic₩AppData₩Roaming₩Perplexity₩Code Cache₩Wjs7ba7019148c4366_0	2025-06-08 13:16:50	2025-06-08 13:19:26	2025-06-08 13:...	2025-06-08 15:...	Update Resident Value	0x7681	4
Local State	₩Users₩forensic₩AppData₩Roaming₩Perplexity₩Local State	2025-06-08 13:16:50	2025-06-08 13:16:50	2025-06-08 13:...	2025-06-08 15:...	Update Resident Value	0x7681	6
4308668c2ca097_0	₩Users₩forensic₩AppData₩Roaming₩Perplexity₩Code Cache₩Wjs4308668c2ca097_0	2025-06-08 13:16:51	2025-06-08 13:19:21	2025-06-08 13:...	2025-06-08 15:...	Update Resident Value	0x7682	0
e3f123f96e7eb41a_0	₩Users₩forensic₩AppData₩Roaming₩Perplexity₩Code Cache₩WjsE3f123f96e7eb41a_0	2025-06-08 13:16:51	2025-06-08 13:19:21	2025-06-08 13:...	2025-06-08 15:...	Update Resident Value	0x7682	2
846e91375985712_0	₩Users₩forensic₩AppData₩Roaming₩Perplexity₩Code Cache₩Wjs846e91375985712_0	2025-06-08 13:16:54	2025-06-08 13:19:22	2025-06-08 13:...	2025-06-08 15:...	Update Resident Value	0x7683	2
11765598bc454b_0	₩Users₩forensic₩AppData₩Roaming₩Perplexity₩Code Cache₩Wjs11765598bc454b_0	2025-06-08 13:16:54	2025-06-08 13:19:21	2025-06-08 13:...	2025-06-08 15:...	Update Resident Value	0x7683	6
PERPLEXITY.EXE-DAAAB08...	₩Windows₩Prefetch₩PERPLEXITY.EXE-DAAAB08...	2025-06-08 13:16:55	2025-06-08 15:38:43	2025-06-08 15:...	2025-06-08 15:...	Update Resident Value	0x7684	2
8ada55391b6c7_0	₩Users₩forensic₩AppData₩Roaming₩Perplexity₩Code Cache₩Wjs8ada55391b6c7_0	2025-06-08 13:16:55	2025-06-08 13:19:22	2025-06-08 13:...	2025-06-08 15:...	Update Resident Value	0x7684	6
b2ad686d68b04b4_0	₩Users₩forensic₩AppData₩Roaming₩Perplexity₩Code Cache₩Wjsb2ad686d68b04b4_0	2025-06-08 13:16:55	2025-06-08 13:19:22	2025-06-08 13:...	2025-06-08 15:...	Update Resident Value	0x7685	0
ebaf976ad5d8042_0	₩Users₩forensic₩AppData₩Roaming₩Perplexity₩Code Cache₩WjsEbaf976ad5d8042_0	2025-06-08 13:16:56	2025-06-08 13:19:22	2025-06-08 13:...	2025-06-08 15:...	Update Resident Value	0x7685	4
75b6055ba7ee5ef_0	₩Users₩forensic₩AppData₩Roaming₩Perplexity₩Code Cache₩Wjs75b6055ba7ee5ef_0	2025-06-08 13:16:56	2025-06-08 13:19:22	2025-06-08 13:...	2025-06-08 15:...	Update Resident Value	0x7685	6
1c18241d6f1329a2_0	₩Users₩forensic₩AppData₩Roaming₩Perplexity₩Code Cache₩Wjs1c18241d6f1329a2_0	2025-06-08 13:16:57	2025-06-08 13:19:22	2025-06-08 13:...	2025-06-08 15:...	Update Resident Value	0x7686	0
d217780f429eef_0	₩Users₩forensic₩AppData₩Roaming₩Perplexity₩Code Cache₩Wjsd217780f429eef_0	2025-06-08 13:16:57	2025-06-08 13:19:22	2025-06-08 13:...	2025-06-08 15:...	Update Resident Value	0x7686	4
8649f7e6cab3b4f_0	₩Users₩forensic₩AppData₩Roaming₩Perplexity₩Code Cache₩Wjs8649f7e6cab3b4f_0	2025-06-08 13:16:59	2025-06-08 13:19:22	2025-06-08 13:...	2025-06-08 15:...	Update Resident Value	0x7686	6
595f179a317d5d1_0	₩Users₩forensic₩AppData₩Roaming₩Perplexity₩Code Cache₩Wjs595f179a317d5d1_0	2025-06-08 13:16:59	2025-06-08 13:19:22	2025-06-08 13:...	2025-06-08 15:...	Update Resident Value	0x7687	0
...2e542de_0	₩Users₩forensic₩AppData₩Roaming₩Perplexity₩Code Cache₩Wjs...2e542de_0	2025-06-08 13:16:59	2025-06-08 13:19:22	2025-06-08 13:...	2025-06-08 15:...	Update Resident Value	0x7687	2

[그림 31] NTF Logtrackerr로 본 파일 조작 로그

⑤ Users₩forensic₩AppData₩Roaming₩Perplexity₩Local
Storage₩leveldb₩ 하위에 log, MANIFEST-*, data_* 등
LevelDB 형식 데이터 파일의 생성 흔적을 확인할 수
있었다.

521080938	2025-06-08 15:41:44	File Deletion		lockfile	WUsers\Wforensic\WAppData\WRoaming\WPerplexity\Wlockfile
521081083	2025-06-08 15:41:44	Renaming File	global.ini -> global.backup.ini	global.backup.ini	WUsers\Wforensic\WAppData\WLocal\Microsoft\WOneDrive\WSettings\WPersonal\Wglobal.backup.ini
521081475	2025-06-08 15:41:44	Renaming File	global.temp.ini -> global.ini	global.ini	WUsers\Wforensic\WAppData\WLocal\Microsoft\WOneDrive\WSettings\WPersonal\Wglobal.ini
521081947	2025-06-08 15:41:44			global.backup.ini	WUsers\Wforensic\WAppData\WLocal\Microsoft\WOneDrive\WSettings\WPersonal\Wglobal.backup.ini
521082081	2025-06-08 15:41:44	File Deletion		LOG	WUsers\Wforensic\WAppData\WRoaming\WPerplexity\WLocal Storage\Wieveldb\WLOG
521082588	2025-06-08 15:41:44			LOG	WUsers\Wforensic\WAppData\WRoaming\WPerplexity\WService Worker\WDatabase\WLOG
521082671	2025-06-08 15:41:44			000008.log	WUsers\Wforensic\WAppData\WRoaming\WPerplexity\WService Worker\WDatabase\W000008.log
521082756	2025-06-08 15:41:44			MANIFEST-000007	WUsers\Wforensic\WAppData\WRoaming\WPerplexity\WService Worker\WDatabase\WMANIFEST-000007
521082841	2025-06-08 15:41:44			MANIFEST-000007	WUsers\Wforensic\WAppData\WRoaming\WPerplexity\WSession Storage\WMANIFEST-000007
521082934	2025-06-08 15:41:44			MANIFEST-000051	WUsers\Wforensic\WAppData\WRoaming\WPerplexity\WLocal Storage\Wieveldb\WMANIFEST-000051
521083042	2025-06-08 15:41:44			000009.log	WUsers\Wforensic\WAppData\WRoaming\WPerplexity\WSession Storage\W000009.log
521083066	2025-06-08 15:41:44			Conversions	WUsers\Wforensic\WAppData\WRoaming\WPerplexity\WConversions
521083233	2025-06-08 15:41:44			LOG	WUsers\Wforensic\WAppData\WRoaming\WPerplexity\WSession Storage\WLOG
521083442	2025-06-08 15:41:44			data_0	WUsers\Wforensic\WAppData\WRoaming\WPerplexity\WGPUCache\Wdata_0
521083501	2025-06-08 15:41:44			data_2	WUsers\Wforensic\WAppData\WRoaming\WPerplexity\WGPUCache\Wdata_2
521083560	2025-06-08 15:41:44			data_3	WUsers\Wforensic\WAppData\WRoaming\WPerplexity\WGPUCache\Wdata_3
521083619	2025-06-08 15:41:44			data_0	WUsers\Wforensic\WAppData\WRoaming\WPerplexity\WDown\WGPUCache\Wdata_0
521083678	2025-06-08 15:41:44			data_2	WUsers\Wforensic\WAppData\WRoaming\WPerplexity\WDown\WGPUCache\Wdata_2
521083737	2025-06-08 15:41:44			data_3	WUsers\Wforensic\WAppData\WRoaming\WPerplexity\WDown\WGPUCache\Wdata_3
521083796	2025-06-08 15:41:44			data_0	WUsers\Wforensic\WAppData\WRoaming\WPerplexity\WDown\WGPUCache\Wdata_0
521083855	2025-06-08 15:41:44			data_2	WUsers\Wforensic\WAppData\WRoaming\WPerplexity\WDown\WGPUCache\Wdata_2
521083923	2025-06-08 15:41:44			data_3	WUsers\Wforensic\WAppData\WRoaming\WPerplexity\WDown\WGPUCache\Wdata_3
521084042	2025-06-08 15:41:44			QuotaManager	WUsers\Wforensic\WAppData\WRoaming\WPerplexity\WWebStorage\WQuotaManager
521084128	2025-06-08 15:41:44			QuotaManager-journal	WUsers\Wforensic\WAppData\WRoaming\WPerplexity\WWebStorage\WQuotaManager-journal

[그림 32] NTF Logtrackerr로 본 파일 조작 로그

⑥ File creation, File Deletion, Renaming File, Writing Content 등의 흔적과 Perplexity 앱이 네트워크 보안 파일을 생성하고 적용하는 과정을 확인할 수 있다.

- File Creation은 2025-06-08 15:40:54에 TransportSecurity~파일(네트워크 설정 캐시 파일) 생성이 생성됐음을 나타낸다.
- File Deletion은 2025-06-08 15:40:54에 파일이 삭제됐음을 나타낸다.
- Writing Content는 해당 캐시파일에 데이터가 실제로 쓰인 기록을 나타낸다.

520963648	2025-06-08 15:40:54	File Creation	TransportSecurity~RF3633...	WUsers\Wforensic\WAppData\WRoaming\WPerplexity\WNetwork\WTransportSecurity~RF3633.TMP	2025-06-08 15:40:54	2025-06-08 15:40:54	2025-06-08 15:40:54
520963688	2025-06-08 15:40:54	File Deletion	TransportSecurity~RF3633...	WUsers\Wforensic\WAppData\WRoaming\WPerplexity\WNetwork\WTransportSecurity~RF3633.TMP	2025-06-08 15:40:54	2025-06-08 15:40:54	2025-06-08 15:40:54
520964199	2025-06-08 15:40:54	Renaming File	TransportSecurity -> Trans...	WUsers\Wforensic\WAppData\WRoaming\WPerplexity\WNetwork\WTransportSecurity~RF3633.TMP	2025-06-08 15:40:54	2025-06-08 15:40:54	2025-06-08 15:40:54
520964632	2025-06-08 15:40:54	Renaming File	6489f2d5-c3f9-4a6d-8b6c-2...	WUsers\Wforensic\WAppData\WRoaming\WPerplexity\WNetwork\WTransportSecurity~RF3633.TMP	2025-06-08 15:40:54	2025-06-08 15:40:54	2025-06-08 15:40:54
520965346	2025-06-08 15:40:54	File Deletion	TransportSecurity~RF3633...	WUsers\Wforensic\WAppData\WRoaming\WPerplexity\WNetwork\WTransportSecurity~RF3633.TMP	2025-06-08 15:40:54	2025-06-08 15:40:54	2025-06-08 15:40:54
520965384	2025-06-08 15:40:54	File Creation	95c7b0a54a7f291_0	WUsers\Wforensic\WAppData\WRoaming\WPerplexity\WCode Cache\Wjs\W95c7b0a54a7f291_0	2025-06-08 13:17:01	2025-06-08 15:40:54	2025-06-08 15:40:54
520965880	2025-06-08 15:40:54	Writing Content of Resident...	Writing Size : 24	WUsers\Wforensic\WAppData\WRoaming\WPerplexity\WCode Cache\Wjs\W95c7b0a54a7f291_0	2025-06-08 15:40:54	2025-06-08 15:40:54	2025-06-08 15:40:54
520966048	2025-06-08 15:40:54	Writing Content of Non-Resid...	Data Run(In Volume) : 147...				
520967736	2025-06-08 15:40:54	Writing Content of Non-Resid...	Data Run(In Volume) : 736...				
520969337	2025-06-08 15:40:54	TEXT INPUT HOST EXE-054...	TEXT INPUT HOST EXE-054...	WUsers\Wforensic\WAppData\WRoaming\WPerplexity\WCode Cache\Wjs\W3645424a0191c_0	2025-06-08 04:07:20	2025-06-08 15:40:57	2025-06-08 15:40:57
520969365	2025-06-08 15:40:54	b3645424a0191c_0	b3645424a0191c_0	WUsers\Wforensic\WAppData\WRoaming\WPerplexity\WCode Cache\Wjs\W3645424a0191c_0	2025-06-08 15:40:52	2025-06-08 15:40:57	2025-06-08 15:40:57
520973276	2025-06-08 15:40:54	mscorlib.dll.aux	mscorlib.dll.aux	WUsers\Wforensic\WAppData\WRoaming\WPerplexity\WCode Cache\Wjs\W95c7b0a54a7f291_0	2025-06-08 15:40:54	2025-06-08 15:40:58	2025-06-08 15:40:58
520973320	2025-06-08 15:40:54	Microsoft.PowerShell.ConsoleHost	Microsoft.PowerShell.ConsoleHost	WUsers\Wforensic\WAppData\WRoaming\WPerplexity\WCode Cache\Wjs\W95c7b0a54a7f291_0	2025-06-08 15:40:54	2025-06-08 15:40:58	2025-06-08 15:40:58
520973354	2025-06-08 15:40:54	System.Management.Automation	System.Management.Automation	WUsers\Wforensic\WAppData\WRoaming\WPerplexity\WCode Cache\Wjs\W95c7b0a54a7f291_0	2025-06-08 15:40:54	2025-06-08 15:40:58	2025-06-08 15:40:58
520973388	2025-06-08 15:40:54	System.Management.Automation	System.Management.Automation	WUsers\Wforensic\WAppData\WRoaming\WPerplexity\WCode Cache\Wjs\W95c7b0a54a7f291_0	2025-06-08 15:40:54	2025-06-08 15:40:58	2025-06-08 15:40:58
520973422	2025-06-08 15:40:54	System.Management.Automation	System.Management.Automation	WUsers\Wforensic\WAppData\WRoaming\WPerplexity\WCode Cache\Wjs\W95c7b0a54a7f291_0	2025-06-08 15:40:54	2025-06-08 15:40:58	2025-06-08 15:40:58
520973456	2025-06-08 15:40:54	System.Management.Automation	System.Management.Automation	WUsers\Wforensic\WAppData\WRoaming\WPerplexity\WCode Cache\Wjs\W95c7b0a54a7f291_0	2025-06-08 15:40:54	2025-06-08 15:40:58	2025-06-08 15:40:58
520973490	2025-06-08 15:40:54	System.Management.Automation	System.Management.Automation	WUsers\Wforensic\WAppData\WRoaming\WPerplexity\WCode Cache\Wjs\W95c7b0a54a7f291_0	2025-06-08 15:40:54	2025-06-08 15:40:58	2025-06-08 15:40:58
520973524	2025-06-08 15:40:54	System.Management.Automation	System.Management.Automation	WUsers\Wforensic\WAppData\WRoaming\WPerplexity\WCode Cache\Wjs\W95c7b0a54a7f291_0	2025-06-08 15:40:54	2025-06-08 15:40:58	2025-06-08 15:40:58
520973558	2025-06-08 15:40:54	System.Management.Automation	System.Management.Automation	WUsers\Wforensic\WAppData\WRoaming\WPerplexity\WCode Cache\Wjs\W95c7b0a54a7f291_0	2025-06-08 15:40:54	2025-06-08 15:40:58	2025-06-08 15:40:58
520973592	2025-06-08 15:40:54	System.Management.Automation	System.Management.Automation	WUsers\Wforensic\WAppData\WRoaming\WPerplexity\WCode Cache\Wjs\W95c7b0a54a7f291_0	2025-06-08 15:40:54	2025-06-08 15:40:58	2025-06-08 15:40:58
520973770	2025-06-08 15:41:01	File Creation	560067ce-9050-46d4-8b6c...	WUsers\Wforensic\WAppData\WRoaming\WPerplexity\WCode Cache\Wjs\W95c7b0a54a7f291_0	2025-06-08 15:41:01	2025-06-08 15:41:01	2025-06-08 15:41:01
520974079	2025-06-08 15:41:01	Writing Content of Non-Resid...	Data Run(In Volume) : 122...	WUsers\Wforensic\WAppData\WRoaming\WPerplexity\WCode Cache\Wjs\W95c7b0a54a7f291_0	2025-06-08 15:41:01	2025-06-08 15:41:01	2025-06-08 15:41:01
520974707	2025-06-08 15:41:01	File Creation	TransportSecurity~RF3811...	WUsers\Wforensic\WAppData\WRoaming\WPerplexity\WNetwork\WTransportSecurity~RF3811.TMP	2025-06-08 15:41:01	2025-06-08 15:41:01	2025-06-08 15:41:01
520975063	2025-06-08 15:41:01	File Deletion	TransportSecurity~RF3811...	WUsers\Wforensic\WAppData\WRoaming\WPerplexity\WNetwork\WTransportSecurity~RF3811.TMP	2025-06-08 15:41:01	2025-06-08 15:41:01	2025-06-08 15:41:01
520975315	2025-06-08 15:41:01	Renaming File	TransportSecurity -> Trans...	WUsers\Wforensic\WAppData\WRoaming\WPerplexity\WNetwork\WTransportSecurity~RF3811.TMP	2025-06-08 15:41:01	2025-06-08 15:41:01	2025-06-08 15:41:01
520975732	2025-06-08 15:41:01	Renaming File	560067ce-9050-46d4-8b6c...	WUsers\Wforensic\WAppData\WRoaming\WPerplexity\WNetwork\WTransportSecurity~RF3811.TMP	2025-06-08 15:41:01	2025-06-08 15:41:01	2025-06-08 15:41:01
520976265	2025-06-08 15:41:01	File Deletion	TransportSecurity~RF3811...	WUsers\Wforensic\WAppData\WRoaming\WPerplexity\WNetwork\WTransportSecurity~RF3811.TMP	2025-06-08 15:41:01	2025-06-08 15:41:01	2025-06-08 15:41:01

[그림 33] NTF Logtrackerr로 본 파일 조작 로그

4. 메모리 아티팩트

1) 프로그램 실행 및 파일 생성 흔적

(1) 분석 내용 : OS 환경 Windows 운영체제 기반 시스템 레벨에서의 정보 획득을 통해 메모리 아티팩트 분석에 적합한 환경임을 확인할 수 있다.

```
C:\Users\1004\volatility3>python vol.py -f C:\Users\1004\volatility3\Perplexity_memory_after.raw windows.info
Volatility 3 Framework 2.26.2
Progress: 100.00 PDB scanning finished
Variable Value
Kernel Base 0xf80553003000
DTB 0x1ad000
Symbols file:///C:/Users/1004/volatility3/volatility3/symbols/windows/ntkrnlmp.pdb/D9424FC4861E47C10FAD1B35DEC6DCC8-1.json.xz
Is64Bit True
IsPAE False
Layer_name 0 WindowsIntel32e
memory_layer 1 FileLayer
KdVersionBlock 0xf80553c12400
Major/Minor 15.19041
MachineType 34404
KeNumberProcessors 1
SystemTime 2025-06-08 07:05:26+00:00
NtSystemRoot C:\Windows
NtProductType NtProductWinNt
NtMajorVersion 10
NtMinorVersion 0
PE MajorOperatingSystemVersion 10
PE MinorOperatingSystemVersion 0
PE Machine 34404
PE TimeDateStamp Mon Dec 9 11:07:51 2019
```

[그림 34] OS 정보 확인

2) 프로세스 분석

(1) 분석 내용 : Perplexity가 메모리 상에서 여러 차례 실행된 정황이 포착됨. 특정 시간에 단발성 실행이 아닌, 반복 실행이 확인되며, 사용자의 실행 또는 자동 재실행일 가능성이 있다.

188	1628	Perplexity.exe	0xdb823b3d3080	50	-	1	False	2025-06-08 07:02:55.000000	UTC	N/A	Disabled
4752	188	Perplexity.exe	0xdb823a862080	8	-	1	False	2025-06-08 07:03:08.000000	UTC	N/A	Disabled
6032	188	Perplexity.exe	0xdb823b38f080	13	-	1	False	2025-06-08 07:03:14.000000	UTC	N/A	Disabled
5340	188	Perplexity.exe	0xdb8239f59080	16	-	1	False	2025-06-08 07:03:21.000000	UTC	N/A	Disabled
5240	188	Perplexity.exe	0xdb823ab6a080	15	-	1	False	2025-06-08 07:03:28.000000	UTC	N/A	Disabled
1092	1484	audiogd.exe	0xdb823acd3080	2	-	0	False	2025-06-08 07:03:50.000000	UTC	N/A	Disabled
5800	188	Perplexity.exe	0xdb823a040080	14	-	1	False	2025-06-08 07:04:06.000000	UTC	N/A	Disabled
5904	188	Perplexity.exe	0xdb8239198080	12	-	1	False	2025-06-08 07:04:11.000000	UTC	N/A	Disabled
5576	188	Perplexity.exe	0xdb823b2a5080	13	-	1	False	2025-06-08 07:04:12.000000	UTC	N/A	Disabled
3868	1628	MRCv120.exe	0xdb823ad94080	11	-	1	True	2025-06-08 07:04:21.000000	UTC	N/A	Disabled

[그림 35] Perplexity.exe 프로세스 PID 정보

3) DLL 모듈 정보

(1) 분석 내용 : Perplexity.exe 가 로드한 DLL 목록 상에서 비정상 또는 악성 코드 관련 DLL은 확인되지 않았다. 정상적인 Windows 시스템 및 프로그램 실행 중 로드되는 표준 DLL로 판단된다.

```
C:\Users\1004\volatility3>python vol.py -f Perplexity_memory_after.raw windows.dlllist --pid 188
Volatility 3 Framework 2.26.2
Progress: 100.00 PDB scanning finished
```

PID	Process	Base	Size	Name	Path	Loadtime	File output
188	Perplexity.exe	0x7ff79f020000	0xb805000	Perplexity.exe	C:\Users\forensic\AppData\Local\Programs\Perplexity\Perplexity.exe	2025-06-08 07:02:56.000000 UTC	Disabled
188	Perplexity.exe	0x7ffcdc9d0000	0x1f8000	-	-	2025-06-08 07:02:56.000000 UTC	Disabled
188	Perplexity.exe	0x7ffcdabc0000	0xbd000	KERNEL32.DLL	C:\Windows\System32\KERNEL32.DLL	2025-06-08 07:02:56.000000 UTC	Disabled
188	Perplexity.exe	0x7ffcd4400000	0x2f6000	KERNELBASE.dll	C:\Windows\System32\KERNELBASE.dll	2025-06-08 07:02:56.000000 UTC	Disabled

[그림 36] Perplexity.exe DLL 목록

4) 사용자 실행 이력

(1) 분석 내용 : 프로그램 설치 및 사용 여부 확인, 사용 시각, 빈도수, 사용 경로 추적 가능하다.

① Perplexity Setup 1.1.3.exe

경로 : C:\Users\forensic\Downloads\Perplexity Setup 1.1.3.exe

분석 내용 : 사용자가 수동으로 설치 파일을 직접 실행한 행위를 확인 할 수 있다. 해당 시간에 Perplexity 관련 소프트웨어가 설치 되었을 가능성이 높다.

```
* 0x82814b014000 \??\C:\Users\forensic\ntuser.dat ntuser.dat\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count
2025-06-08 07:05:22.000000 UTC Value C:\Users\forensic\Downloads\Perplexity Setup 1.1.3.exe
N/A 0 2 0:01:01.469000 N/A
```

00 00 00 00 00 00 00 00 02 00 00 00 29 ee 00 00)
00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf
00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf
00 00 80 bf 00 00 80 bf ff ff ff ff 00 00 00 00
00 00 00 00 00 00 00 00

[그림 37] 설치 파일 실행 기록

② Perplexity.lnk

경로 : C:\Users\forensic\Desktop\Perplexity.lnk

분석 내용 : 바탕화면에 생성된 바로가기를 통해 사용자가 프로그램을 총 6회 실행한 기록이 존재한다. 이는 Perplexity가 설치 완료된 이후 자주 사용되었음을 보여준다.

```
* 0x82814b014000 \??\C:\Users\forensic\ntuser.dat ntuser.dat\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}\Count
2025-06-08 07:02:51.000000 UTC Value C:\Users\forensic\Desktop\Perplexity.lnk
N/A 6 0 0:00:00.506000 2025-06-08 06:38:27.000000 UTC
```

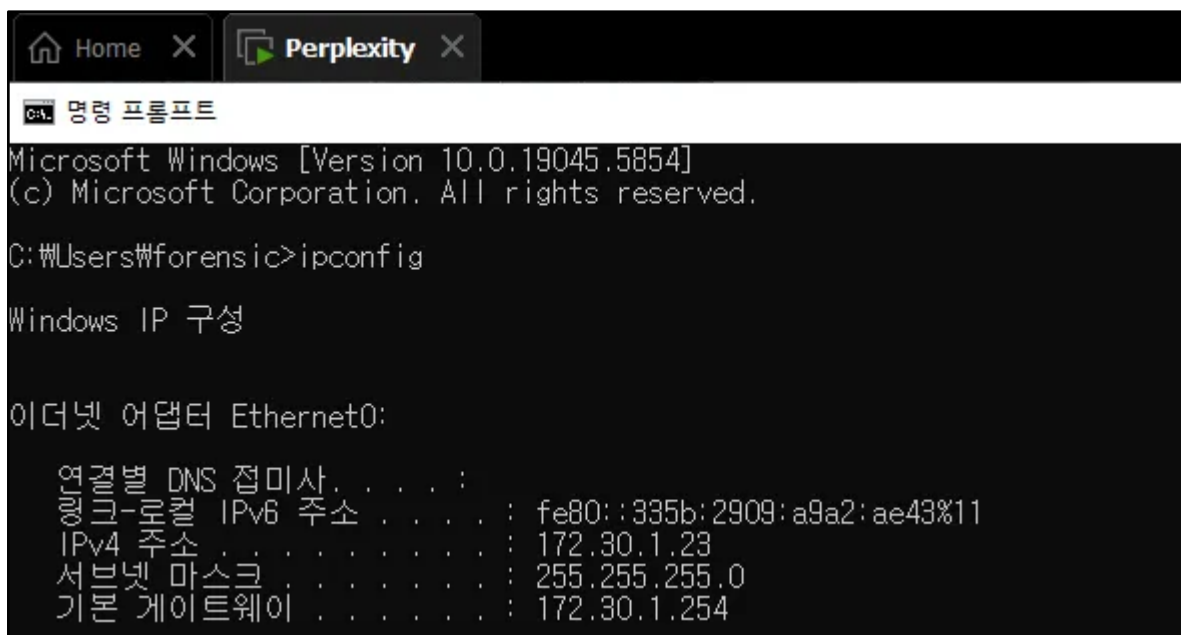
00 00 00 00 06 00 00 00 00 00 00 00 06 00 00 00
00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf
00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf
00 00 80 bf 00 00 80 bf ff ff ff ff 30 2c 3f f10,?,
3f d8 db 01 00 00 00 00	?.....

[그림 38] 바로가기 실행 기록

5. 네트워크 아티팩트

1) 클라이언트 IP 주소 (Perplexity VM)

(1) 분석 내용: Wireshark에서 `tls.handshake.extensions_server_name contains perplexity` 필터를 적용한 결과, 해당 조건에 일치하는 IP는 172.30.1.23 단 하나였다. 이는 네트워크 상에서 Perplexity 서비스에 접속한 유일한 호스트가 172.30.1.23임을 의미하며, 해당 IP에서 Perplexity를 실행한 명확한 정황 증거로 해석할 수 있다.



```
Microsoft Windows [Version 10.0.19045.5854]
(c) Microsoft Corporation. All rights reserved.

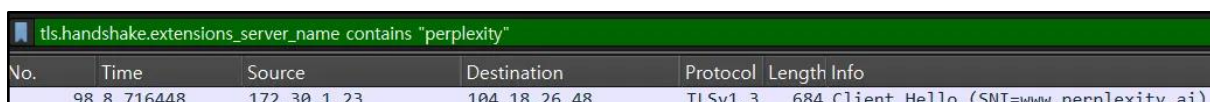
C:\Users\forensic>ipconfig

Windows IP 구성

이더넷 어댑터 Ethernet0:

    연결별 DNS 접미사. . . . . : 
    링크-로컬 IPv6 주소. . . . . : fe80::335b:2909:a9a2:ae43%11
    IPv4 주소. . . . . : 172.30.1.23
    서브넷 마스크. . . . . : 255.255.255.0
    기본 게이트웨이. . . . . : 172.30.1.254
```

[그림 39] Perplexity 로컬 네트워크 IP 주소



No.	Time	Source	Destination	Protocol	Length	Info
98	8.716448	172.30.1.23	104.18.26.48	TLSv1.3	684	Client Hello (SNI=www.perplexity.ai)

[그림 40] Wireshark로 확인한 Perplexity 실행 IP

2) 접속 도메인

(1) 경로: C:\Wroot\Users\forensic\AppData\Roaming\Perplexity\

Network\Network Persistent State

(2) 분석 내용: server 필드에 명시된 도메인인

https://www.perplexity.ai, https://r2cdn.perplexity.ai, https://pplx-next-static-public.perplexity.ai는 Perplexity 애플리케이션이 실제로 연결한 서버들로 확인된다. 이를 통해 해당 호스트가 Perplexity AI를 사용했으며, 관련 리소스에 접속한 정황을 확인할 수 있다.

00000040	2C 22 73 65 72 76 65 72 22 3A 22 68 74 74 70 73	, "server": "https
00000050	3A 2F 2F 70 65 72 70 6C 65 78 69 74 79 2E 61 69	://perplexity.ai
00000060	22 2C 22 73 75 70 70 6F 72 74 73 5F 73 70 64 79	", "supports_spdy
00000070	22 3A 74 72 75 65 7D 2C 7B 22 61 6E 6F 6E 79 6D	": true}, {"anonym
00000E80	6F 6E 79 6D 69 7A 61 74 69 6F 6E 22 3A 5B 5D 2C	onymization": [],
00000E90	22 73 65 72 76 65 72 22 3A 22 68 74 74 70 73 3A	"server": "https:
00000EA0	2F 2F 72 32 63 64 6E 2E 70 65 72 70 6C 65 78 69	//r2cdn.perplexi
00000EB0	74 79 2E 61 69 22 2C 22 73 75 70 70 6F 72 74 73	ty.ai", "supports
00000EC0	5F 73 70 64 79 22 3A 74 72 75 65 7D 2C 7B 22 61	_spdy": true}, {"a
00000FC0	5B 5D 2C 22 73 65 72 76 65 72 22 3A 22 68 74 74	[], "server": "htt
00000FD0	70 73 3A 2F 2F 70 70 6C 78 2D 6E 65 78 74 2D 73	ps://pplx-next-s
00000FE0	74 61 74 69 63 2D 70 75 62 6C 69 63 2E 70 65 72	tatic-public.per
00000FF0	70 6C 65 78 69 74 79 2E 61 69 22 2C 22 73 75 70	plexity.ai", "sup
00001000	70 6F 72 74 73 5F 73 70 64 79 22 3A 74 72 75 65	ports_spdy": true

[그림 41,42,43] HxD로 확인한 접속 도메인

3) 서버 연결 정보

(1) 경로: C:\root\Users\forensic\AppData\Roaming\Perplexity\Network\Network Persistent State

(2) 분석 내용: 분석 대상 서버는 HTTP/2 기반의 SPDY 프로토콜을 지원하고 있으며(supports_spdy: true), 최신 HTTP/3 기반의 QUIC 프로토콜을 사용하고 있다.(protocol_str: "quic", advertised_alpn: ["h3"]).


```
Decoded text
{"server":"https://perplexity.ai", "supports_spdy":true}, {"anonymization":[], "server":"https://redirector.gvt1.com", "supports_spdy":true}, {"alternative_service":[{"advertised_alpn":["h3"], "expiration":"13396421805261991", "port":443, "protocol_str":"quic"}], "anonymization":[], "network_stats":{"srtt":87771}, "server":"https://r4---sn-n3cgv5qc5oq-bh2sy.gvt1.com"}, {"alter
```

[그림 44] HxD로 확인한 서버 연결 정보

키워드	값	항목
"supports_spdy"	true	해당 서버가 HTTP/2 기반 SPDY 프로토콜을 지원함
"protocol_str"	"quic"	HTTP/3 기반의 QUIC 프로토콜 사용 (보안성 및 속도 향상)
"advertised_alpn"	["h3"]	QUIC 기반 응용 계층 프로토콜 지원(HTTP/3)
"srtt"	87771	서버 응답 왕복 시간

[표 4] 서버 연결 정보 표

4) HSTS 정책

(1) 경로: C:\root\Users\forensic\AppData\Roaming\Perplexity\Network\TransportSecurity

(2) 분석 내용: 총 15개의 정책이 확인되었으며, 모든 정책은 force-https(HTTPS 강제) 형태이다. 이는 사용자가 접속한 서버가 설정한 HSTS 정책으로, 해당 앱 실행 시점에 보안 연결이 강제되었음을 의미한다. 따라서 이 정보는 앱 사용 당시의 보안 연결 여부를 입증하는 증거이다.

```
Decoded text
{"sts":[{"expiry":1780900778.317146,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=", "mode":"force-https", "sts_include_subdomains":true, "sts_observed":1749364778.317149}, {
```

```
{ "sts": [
  {
    "expiry": 1780900778.317146,
    "host": "M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=",
    "mode": "force-https",
    "sts_include_subdomains": true,
    "sts_observed": 1749364778.317149,
  }
]
```

[그림 45,46] HxD로 확인한 HSTS 정책

필드명	의미
"expiry"	정책 만료 시간 (2031년 6월 8일)
"host"	HSTS 정책이 적용된 도메인의 Base64 인코딩된 값
"mode"	"force-https" -> HTTP -> HTTPS 강제
"sts_include_subdomains"	해당 도메인의 서브도메인에도 HSTS 적용 여부
"sts_observed"	HSTS 정책을 처음 수신한 시점 (2025년 6월 8일)

[표 5] HSTS 정책 상세 표

5) 쿠키 정보

(1) 경로: C:\Wroot\Users\Wforensic\AppData\Roaming\Perplexity\Network\Cookies

(2) 분석 내용: pplex.search-mode는 Perplexity 애플리케이션

내에서 사용자가 검색 기능을 활용한 여부를 나타내는 설정 값이며, pplex.source-selection은 질문의 출처를 설정하는 기능과 관련된 항목이다. 한편, _cf_bm 쿠키는 Perplexity 서비스를 보호하는 Cloudflare에서 발급한 보안 인증 토큰으로, 접속자의 세션 관리 및 사용자 식별에 중요한 역할을 수행한다.

Strings		Extracted Text	Translation
Page: 1 of -	Page	Matches on page: - of - Match	100% Reset
		Text Source: File Text	
		13393830913967095 .podscribe.com .podscribe_perplexityai_referrer / 13425375525784623 1 1 1 1 0 2 443 13393835525784628 1 1	
		13393837242952390 www.perplexity.ai pplx.source-selection-v3-space- [] / 13394442042000000 0 0 13393838494984407 1 1 1 -1 2 443 13393837242952390 2 1	
		13393836851074095 www.perplexity.ai pplx.source-selection-v3-space-e808a245-7d78-473d-a225-a3b27744fc0d [%22web%22] / 13394442043000000 0 0 13393838494984407 1 1 1 -1 2 443 13393837243	
		824803 2 1	
		13393831091977649 www.perplexity.ai pplx.search-mode search / 13428397533000000 0 0 13393838494984407 1 1 1 -1 2 443 13393837533891722 2 1	
		13393835951709743 www.perplexity.ai pplx.search-models-v2 [%22search%22%22experimental%22%22studio%22%22pplx_beta%22] / 13428397534000000 0 0 13393838494984407 1 1 1 -1 2 443 1	
		3393837534190012 2 1	
		13393830913574759 .perplexity.ai _fbp fb.1.1749357313359202612976714590748 / 13401613596000000 0 0 13393838494984407 1 1 1 2 443 13393837596055466 2 1	
		13393838314592682 .perplexity.ai _cf_bm YG0ZWuIsY3Qlzh.1LyX3eisFIEWfogitZVAbnxa95b4-1749364714-1.0.1.1-bGCQAIC7j1DWPjOjt_XsxyHD8lQvicusD.GBJVfx1XLC4mGVdFeH0mToChIDMKYkboZ1bTL9	
		V8x5v6ekO8WJcmWBRZnABzbjmc52Yk0 / 13393840114592682 1 1 13393838441449038 1 1 1 0 2 443 13393838314592698 1 1	
		13393838321010982 .perplexity.ai cf_clearance nSsPEnuLIEHZG0CvJMpOpng.EIGk8N8sBAz2o3m8nu4-1749364721-1.2.1.1-eTuEjnBR2kD62_BWgmEqUWfNjtit53gseeiOFnX8VPM31rlIPRF	

[그림 47] Autopsy로 확인한 쿠키 정보

6) 네트워크 흐름 추적

(1) 분석 내용: 내부 IP 주소 172.30.1.23이 외부 DNS 서버

168.126.63.1(KT 공개 DNS)로 www.perplexity.ai 도메인에 대한 A 레코드 및 HTTPS 레코드 질의를 여러 차례 수행한 정황이

포착되었다. 해당 질의에 대한 응답으로는 모두 Cloudflare CDN

인프라에 해당하는 104.18.26.48, 104.18.27.48 등의 IP 주소가

반환되었으며, 이는 Perplexity AI 서비스의 프론트엔드 웹 인프라로

확인된다. 특히, HTTPS 타입 DNS 요청까지 포함된 점은 최신

브라우저 또는 앱이 보안 연결 전용 콘텐츠 로딩 시도를 수행했음을 의미한다.

The image shows a Wireshark packet capture window with the filter 'dns.qry.name contains "perplexity"'. The packet list contains the following entries:

No.	Time	Source	Destination	Protocol	Length	Info
3206	83.110737	172.30.1.23	168.126.63.1	DNS	77	Standard query 0x336e A www.perplexity.ai
3207	83.110752	172.30.1.23	168.126.63.1	DNS	77	Standard query 0x336e A www.perplexity.ai
3208	83.111343	172.30.1.23	168.126.63.1	DNS	77	Standard query 0x484e HTTPS www.perplexity.ai
3209	83.111356	172.30.1.23	168.126.63.1	DNS	77	Standard query 0x484e HTTPS www.perplexity.ai
3216	83.113309	168.126.63.1	172.30.1.23	DNS	109	Standard query response 0x336e A www.perplexity.ai A 104.18.27.48 A 104.18.26.48
3217	83.114881	168.126.63.1	172.30.1.23	DNS	179	Standard query response 0x484e HTTPS www.perplexity.ai HTTPS A 104.18.26.48 A 104.18.27.48

[그림 48] Wireshark로 확인한 네트워크 정보

7) TLS 세션 추적

(1) 분석 내용: 내부 IP 주소 172.30.1.23은 외부 서버 104.18.26.48과 TCP 3-way 핸드셰이크(SYN → SYN-ACK → ACK)를 정상적으로 수행하여 세션을 수립하였다. 이후 TLS 1.3 프로토콜에 따른 암호화 통신 절차를 시작하였으며, Client Hello 패킷 내 SNI(Server Name Indication) 필드에는 www.perplexity.ai가 명확히 기재되어 있었다. 이를 통해 해당 호스트가 Perplexity 서비스와의 연결을 시도했음을 확인할 수 있다. 서버 측에서는 Server Hello, Change Cipher Spec, Encrypted Extensions, Application Data 패킷을 순차적으로 전송하며 TLS 핸드셰이크가 성공적으로 완료되었고, 양측 간에 안전한 암호화 통신 채널이 형성되었다. 이후 다수의 암호화된 Application Data 패킷이 전송된 점으로 보아, 단순 접속을 넘어 실제 서비스 이용에 따른 데이터 통신이 이루어진 것으로 판단된다. 한편, TLS 1.3 및 QUIC 프로토콜 특성상 프라이빗 키 없이는 암호화된 트래픽의 복호화가 불가능하여, 본 분석에서는 암호화된 내용 자체를 확인할 수 없었다.

No.	Time	Source	Destination	Protocol	Length	Info
89	8.671137	172.30.1.23	224.0.0.252	LLMNR	75	Standard query 0x2e57 ANY DESKTOP-GBTHUOH
90	8.671140	172.30.1.23	224.0.0.252	LLMNR	75	Standard query 0x2e57 ANY DESKTOP-GBTHUOH
91	8.683599	172.30.1.23	104.18.26.48	TCP	66	49999 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
92	8.683611	172.30.1.23	104.18.26.48	TCP	66	[TCP Retransmission] 49999 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
93	8.690760	104.18.26.48	172.30.1.23	TCP	66	443 → 49999 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM WS=8192
94	8.690966	172.30.1.23	104.18.26.48	TCP	54	49999 → 443 [ACK] Seq=1 Ack=1 Win=263168 Len=0
95	8.690974	172.30.1.23	104.18.26.48	TCP	54	[TCP Dup ACK 94#1] 49999 → 443 [ACK] Seq=1 Ack=1 Win=263168 Len=0
96	8.716368	172.30.1.23	104.18.26.48	TCP	1454	49999 → 443 [ACK] Seq=1 Ack=1 Win=263168 Len=1400 [TCP PDU reassembled in 98]
97	8.716377	172.30.1.23	104.18.26.48	TCP	1454	[TCP Retransmission] 49999 → 443 [ACK] Seq=1 Ack=1 Win=263168 Len=1400
98	8.716448	172.30.1.23	104.18.26.48	TLSv1.3	684	Client Hello (SNI=www.perplexity.ai)
99	8.716454	172.30.1.23	104.18.26.48	TCP	684	[TCP Retransmission] 49999 → 443 [PSH, ACK] Seq=1401 Ack=1 Win=263168 Len=630 [TCP PDU reassembled in 98]
100	8.720049	104.18.26.48	172.30.1.23	TCP	54	443 → 49999 [ACK] Seq=1 Ack=2031 Win=131072 Len=0
101	8.721437	104.18.26.48	172.30.1.23	TLSv1.3	1429	Server Hello, Change Cipher Spec, Application Data
102	8.737698	172.30.1.23	4.213.25.240	TLSv1.2	155	Ignored Unknown Record
103	8.737709	172.30.1.23	4.213.25.240	TCP	155	[TCP Retransmission] 49867 → 443 [PSH, ACK] Seq=2 Ack=1 Win=1028 Len=101 [TCP PDU reassembled in 102]
104	8.805465	172.30.1.23	104.18.26.48	TCP	54	49999 → 443 [ACK] Seq=2031 Ack=1376 Win=261632 Len=0
105	8.805477	172.30.1.23	104.18.26.48	TCP	54	[TCP Dup ACK 104#1] 49999 → 443 [ACK] Seq=2031 Ack=1376 Win=261632 Len=0
106	8.853658	4.213.25.240	172.30.1.23	TLSv1.2	225	Application Data

[그림 49] Wireshark로 확인한 TLS 세션 추적

6. 메신저 아티팩트

1) 채팅 로그

(1) 경로 : C:\wroot\Users\forensic\AppData\Roaming\Perplexity
 \Local Storage\leveldb\000038.log

(2) 분석 내용 :

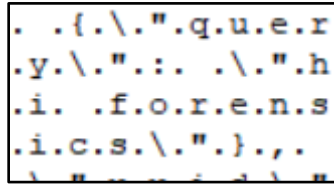
- ① 사용자가 프롬프트 전송 시 사용한 AI 검색 모델 및 대화 모드 확인이 가능하다.

```

."d.i.s.p.l.a.y
."m.o.d.e.l".:
."g.e.m.i.n.i.2
.f.l.a.s.h".,."
.u.s.e.r._s.e.l
.e.c.t.e.d._m.o
.d.e.l".:."g.e
.m.i.n.i.2.f.l.a
.s.h".,."p.e.r
.s.o.n.a.l.i.z.e
.d".:t.r.u.e.,
."m.o.d.e.".:"
.C.O.P.I.L.O.T."

```

[그림 50] Hex Viewer 로 확인한 AI 검색 모델 및 모드 정보



[그림 53] Hex Viewer 로 확인한 삭제한 질의 정보

2) 스레드 제목 변경

(1) 경로 :

CWUsersWforensicWAppDataWRoamingWPerplexityWlogsWmain.log

(2) 분석 내용 : 이미 전송된 프롬프트 내역을 hi we are forensicbbang team 에서 bread recipe 로 변경한 것을 확인할 수 있다.

```
[2025-06-08 15:03:31.503] [info] [main]: did-navigate-in-page
(https://www.perplexity.ai/spaces/templates) [2025-06-08 15:04:17.875] [info] [main]: did-
navigate-in-page (https://www.perplexity.ai/collections/forensic-6AiiRX14Rz2iJaOyd0T8DQ)
[2025-06-08 15:06:09.061] [info] [main]: did-navigate-in-page
(https://www.perplexity.ai/search/hi-we-are--team-XMWip3nBSMaptGrbWQYrMQ) [2025-06-08
15:08:35.568] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/search/hi-we-are-
forensicbbang-team-XMWip3nBSMaptGrbWQYrMQ) [2025-06-08 15:10:52.892] [info] [main]:
did-navigate-in-page (https://www.perplexity.ai/search/this-is-our-malware-python-cod-
NReQEUuaTIKPWLIZe.vg1A) [2025-06-08 15:13:52.005] [info] [main]: did-navigate-in-page
(https://www.perplexity.ai/search/bread-recipe-XMWip3nBSMaptGrbWQYrMQ)
```

3) 스페이스 기능

(1) 경로 : C:WrootWUsersWforensicWAppDataWRoamingWPerplexityWLocal StorageWleveldbW000038.log,

(2) 분석 내용 :

① 스페이스 생성 시 제목과 설명 정보를 확인할 수 있다.

```

.,,".t.i.t.l.e."
:,".F.o.r.e.n.s
i.c.",,".d.e.s
.c.r.i.p.t.i.o.n
",,".P.e.r.p.l
e.x.i.t.y. .O.p
e.r.a.t.i.o.n.
R.e.p.o.r.t.",,

```

[그림 54] Hex Viewer 로 확인한 제목과 설명 정보

- ② 스페이스를 통해 전송한 프롬프트 내역을 확인할 수 있다.

```

t.".:{"."q.u.e.
r.y.".:{"."h.i.
w.e. .a.r.e. .f.
o.r.e.n.s.i.c.b.
b.a.n.g. .t.e.a.
m."."}.,,".a.s.s.

```

[그림 55] Hex Viewer 로 확인한 질의 정보

4) 페이지 기능

- (1) 경로 :

CWUsersWforensicWAppDataWRoamingWPerplexityWlogsWmain.log

- (2) 분석 내용 :

- ① 페이지 기능 사용을 위해 새 페이지 생성 화면으로 이동한 것을 확인할 수 있다.
- ② 14시 26분 경 illegal-document-sale-advertis-
xikL_xMRdyEUtvrQkrPJw 해당 페이지로 접속 한 것을 확인할 수 있다.

- ③ 페이지 생성을 위해 사용자가 전송한 정보는 확인할 수 없었다.

```

[2025-06-08 14:18:33.272] [info] [main]: did-navigate-in-page (https://www.perplexity.ai/library)
[2025-06-08 14:18:36.815] [info] [main]: did-navigate-in-page
(https://www.perplexity.ai/page/new) [2025-06-08 14:20:55.535] [info] [main]: did-navigate-in-
page (https://www.perplexity.ai/page/new?newFrontendContextUUID=6b5cdc1c-4317-43dc-

```

```
ba24-ed01435e0b4b) [2025-06-08 14:26:06.747] [info] [main]: did-navigate-in-page  
(https://www.perplexity.ai/page/illegal-document-sale-advertis-xikL_xMRdyEUtvrQkrPJw)
```

5) 익명 모드

(1) 경로 :

CWUsersWforensicWAppDataWRoamingWPerplexityWlogsWmain.log

(2) 분석 내용 :

- ① 익명 모드 사용 시 프롬프트 내역은 자세하게 기록되지 않았지만,
해당 경로에서 스레드 전송 정보는 확인할 수 있다.

```
[2025-06-08 15:24:10.539] [info] [main]: did-navigate-in-page  
(https://www.perplexity.ai/search/hi-zajxIMZVTt_FTq7yiC4Jg) [2025-06-08 15:26:35.934] [info]  
[main]: did-navigate-in-page (https://www.perplexity.ai/search/how-is-the-weather-today-  
c0sXCZnGSAiBc4zbLFkICA)
```

6) 이미지 모델

(1) 경로 :

CWUsersWforensicWRoamingWPerplexityWCacheWCache_DataWf_000
02b

- (2) 분석 내용 : 이미지 모델 (GPT Image1, FLUX1, DALL-E 3) 사용에 대한
정보를 확인할 수 있다.

```
(...)=a(25380),i=a(2497),r=a(8216),n=a(16739),o=a,n(n),d=a(87798),u=a(70063),c=a(65774),m=a(28027),v=a(17470  
) ,h=a(51275);let g=()=>{var e;let t="image-generation-model-toggle",{$t:a}=(0,i.A)(),{hasAccessToProFeatures:n}=  
(0,m.E)(),{updateSettings:g}=(0,v.t)({reason:t}),{defaultImageGenerationModel:p}=(0,h.u)({reason:t}),  
{isMobileStyle:f}=(0,u.a)(),b=(0,l.useCallback)(e=>{g({default_image_generation_model:e}},{g}),x=(0,l.useMemo)  
(()=>[{"value":"default",text:"Default",label:a({defaultMessage:"Picks a model based on your  
query",id:"EwML79tpS8"}),onClick:()=>b("default")},{value:"gpt-4o-image",text:"GPT Image  
1",label:a({defaultMessage:"Image generation model by openai"}),id:"HxP0rnzviY"},{openai:"OpenAI"}),onClick:  
(()=>b("gpt-4o-image"))},{value:"flux",text:"FLUX.1",label:a({defaultMessage:"Image generation model by  
bf1"}),id:"Z+Nhu1xjv1"}],{bf1:"Black Forest Labs"}),onClick:()=>b("flux")},{value:"dall-e-3",text:"DALL-E  
3",onClick:()=>b("dall-e-3")},label:a({defaultMessage:"Image generation model by openai"}),id:"HxP0rnzviY"},  
{openai:"OpenAI"}]),[b,a]);return(0,s.jsx)("div",{className:o()({"opacity-50":!n}),children:(0,s.jsx)(c,n,  
{isMobileStyle:f,items:x.map(e=>({type:"default",...e})).disabled:!n,children:(0,s.jsx)(d,A,  
{size:"small",chevron:!0,disabled:!n,chevronIcon:r.A,text:null===e.x.find(e=>e.value===p)||void 0===e?void  
0:e.text,variant:"border"}))})),29760:(e,t,a=>{a.d(t,{getChosenLocale:()=>i});var s=a(39861),l=a(33031);function  
i(){let e=new
```

[그림 56] ChromeCacheViewer 로 확인한 이미지 모델 정보

VII. 분석 차별점

기존 선행연구들은 대부분 모바일 환경(Android, iOS)이나 웹 기반 플랫폼을 중심으로 AI 프로그램의 채팅 로그 및 사용자 행위 데이터를 분석하는 데 초점을 맞추었다. Kyungsuk Cho 등의 연구[1]는 모바일 기기에서의 채팅 로그 및 사용자 데이터를 중심으로 분석하였으며, Windows 환경에 대해서는 일부 프로그램(Gemini, Copilot)의 채팅 로그 분석에만 제한적으로 접근한다. Juan Manuel Castelo Gomez의 연구[2]는 macOS 기반의 ChatGPT 애플리케이션에서 평문 캐시 데이터를 분석하였으나, 윈도우 환경에서는 적용이 불가하다는 한계를 명시하였다. 또한, Malithi Wanniarachchi Kankanamge 등의 연구[3]는 Windows에서 ChatGPT 앱을 분석하였으나, 삭제된 대화 데이터에 대한 복원이 불가능하고 분석 대상이 ChatGPT에 국한된다는 점에서 범용성이 부족하다. 반면, 본 연구는 이러한 한계를 보완하고자 Windows 데스크톱 환경에서 실행되는 Perplexity 애플리케이션을 중심으로, 기존에 다루어지지 않았던 대화 삭제 및 로그아웃 상황에서의 잔존 로그와 메타데이터를 분석 대상으로 삼을 수 있다.

VIII. 분석 요약

아티팩트 유형	경로	설명
시스템 설치/실행 아티팩트	C:\Windows\Prefetch	Perplexity 설치 및 실행 기록
	C:\Users\forensic\AppData\Roaming\Perplexity\logs\main.log	Perplexity 실행 로그
	C:\Users\forensic\AppData\Local\Programs\Perplexity	Perplexity 설치 디렉터리

	C:\Users\Wforensic\Downloads	Perplexity 다운로드 파일
	C:\Users\Wforensic\Desktop	Perplexity 바로가기 파일
	C:\Users\Wforensic\AppData\Local\Wperplexity-updater	update 진행 기록록
사용자 행위 아티팩트	C:\Users\Wforensic\AppData\Roaming\WPerplexity\logs\main.log	Perplexity 사용자 이메일, 앱 실행 로그, 프롬프트 로그, 페이지 로그, 스페이스 로그, 스레드 이름 변경 로그, 익명 모드 로그
	C:\Users\Wforensic\AppData\Roaming\WPerplexity\WCache\WCache_Data\data_3	Perplexity 사용자 메타 정보
	C:\Users\Wforensic\AppData\Roaming\WPerplexity\WCache\WCache_Data\data_1	csrf 토큰, 로그인 인증 시도, 사용자 설정/계정 활동 리소스 접근 (Google Drive 연동)
	C:\Users\Wforensic\Roaming\WPerplexity\WLocalStorage\Wleveldb\W000005\ldb	사용자 도메인 접근 흔적
파일 사용/조작 아티팩트	C:\W<root>\W\$MFT , C:\W<root>\W\$Extend\W\$UsnJrnl , C:\W<root>\W\$LogFile	파일 생성 및 파일 조작 흔적
	C:\Wroot\Users\Wforensic\AppData\Roaming\WPerplexity\WNetwork\WNetwork Persistent State	접속 도메인
	C:\Wroot\Users\Wforensic\AppData\Roaming\WPerplexity\WNetwork\WNetwork Persistent State	서버 연결 정보

네트워크 아티팩트	C:\root\Users\forensic\AppData\Roaming\Perplexity\Network\TransportSecurity	Perplexity HSTS 정책 정보
	C:\root\Users\forensic\AppData\Roaming\Perplexity\Network\Cookies	Perplexity 쿠키 정보
메신저 아티팩트	C:\root\Users\forensic\AppData\Roaming\Perplexity\LocalStorage\leveldb\000038.log	채팅 내역
	C:\Users\forensic\AppData\Roaming\Perplexity\logs\main.log	로그 정보
	C:\Users\forensic\AppData\Roaming\Perplexity\Cache\Cache_Data\wf_00002b	이미지 모델 정보

IX. 향후 계획

Perplexity에 대한 분석 과정에서 선행 연구들과의 뚜렷한 차이점이 발견됨에 따라, '윈도우 환경에서의 Perplexity 애플리케이션 아티팩트 분석'을 주제로 한 2025년 7월 8일에 개최하는 한국디지털포렌식학회 하계학술대회에 논문을 투고할 예정이다.

X. 참고 문헌

- [1] 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
- [2] Juan Manuel Castelo Gómez, Juan Carlos Mondéjar, Juan Ramón Gómez, José María Martínez, 「Developing an IoT forensic methodology. A concept proposal」, DFRWS 2021 EU – Proceedings of the Eighth Annual DFRWS Europe, Forensic Science International: Digital Investigation, Vol. 36, 2021, p. 301114
- [3] M. W. Kankanamge, N. McKenna, S. Carmona, S. M. Hasan, A. R. Shahid, A. Imteaj, 「Digital Forensic Investigation of the ChatGPT Windows Application」, arXiv preprint arXiv:2505.23938, May 2025