[Claude 분석 보고서]

[아티팩트 상세 분석 보고서]

작성일	2025.06.17
작성자	김신아, 김예은, 배영혜, 안서진, 전소현
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 3

V. 해시값 4

VI. 분석 아티팩트 5

1. 시스템 설치/실행 아티팩트 5

2. 사용자 행위 아티팩트 8

3. 파일 사용/조작 아티팩트 13

4. 메모리 아티팩트 16

5. 네트워크 아티팩트 18

6. 메신저 아티팩트 22

VII. 분석 차별점 26

VIII. 분석 요약 27

IX. 향후 계획 29

X. 참고 문헌 29

I. 기본 정보

프로그램 범주	LLM
프로그램	Claude
버전	v0.10.14
다운로드 경로	https://claude.ai/download

[표 1] 기본 정보

II. 프로그램 개요

1. 프로그램 목적

Constitutional AI를 사용한 어시스턴트로, 안전하고 정확하며 철저한 보안을 통해 최상의 업무 성과를 달성하도록 도와준다. 대량의 정보를 처리하고 아이디어를 브레인스토밍하며 텍스트와 코드를 생성한다.

2. 주요 기능 요약

코드 생성 및 데이터 시각화, 콘텐츠 생성 및 편집(제작), 텍스트와 이미지 분석 그리고 웹 검색 기능이 있다. 프로 버전을 사용하면 더 많은 사용량과 더 다양한 모델이 사용 가능하다.

III. 분석 목적

본 분석은 정상적인 프로그램인 Claude가 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

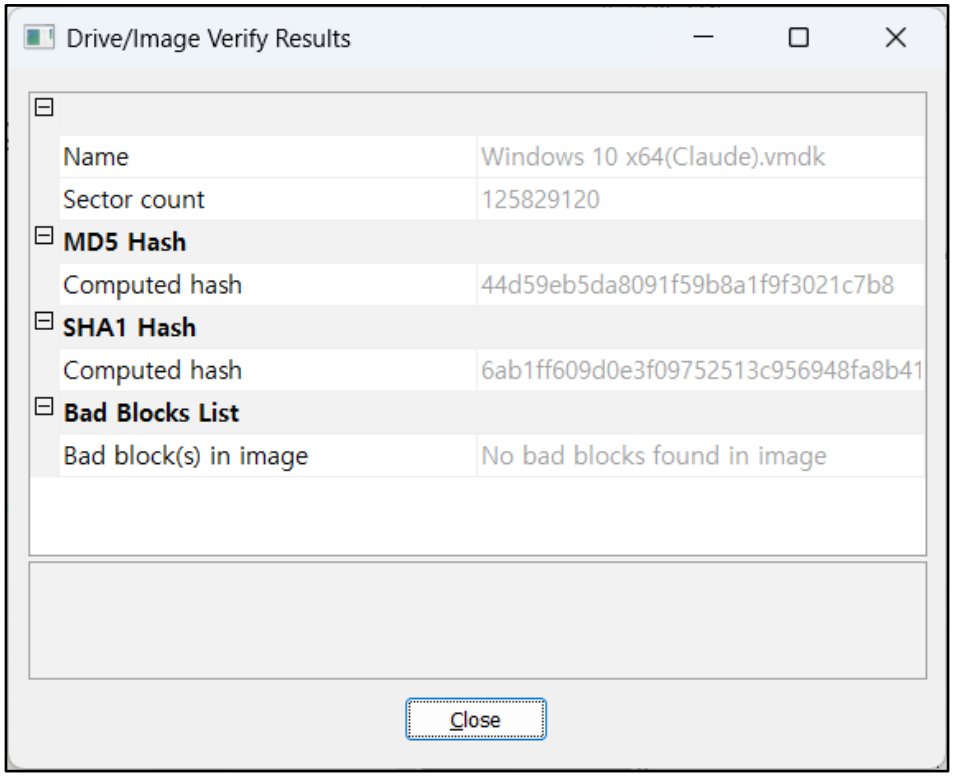
도구명	버전
FTK Imager	v4.7.3.81
ChromeCacheView	v2.52
HxD	v2.5
Wireshark	v4.4.6
NTFS Log Tracker	v1.8
WinPrefetchView	v1.37
Volatility	v3
Autopsy	v.4.22.1
RegistryExplorer	v2.1.0
RegRipper	v4.0

[표 2] 분석 도구

V. 해시값

해시	값
MD5	44d59eb5da8091f59b8a1f9f3021c7b8
SHA1	6ab1ff609d0e3f09752513c956948fa8b41ded23

[표 3] 해시값



[그림 1] FTK Imager로 확인한 vmdk 해시값

VI. 분석 아티팩트

1. 시스템 설치/실행 아티팩트

1) Prefetch 파일

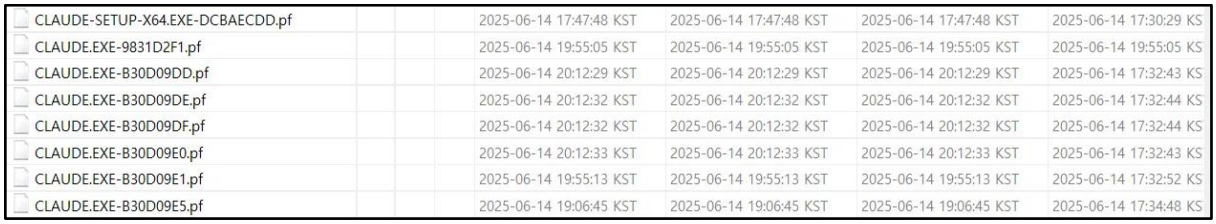
(1) 경로: C:₩Windows₩Prefetch

(2) 분석 내용:

① 해당 디렉터리 내 CLAUDE-SETUP-X64.EXE 프리패치 파일을 통해 Claude 설치 프로그램이 실행된 시각을 확인할 수 있었으며, CLAUDE.EXE 파일은 Claude 실행 파일이 18:12 이후로 여러 차례 실행되었음을 나타낸다.

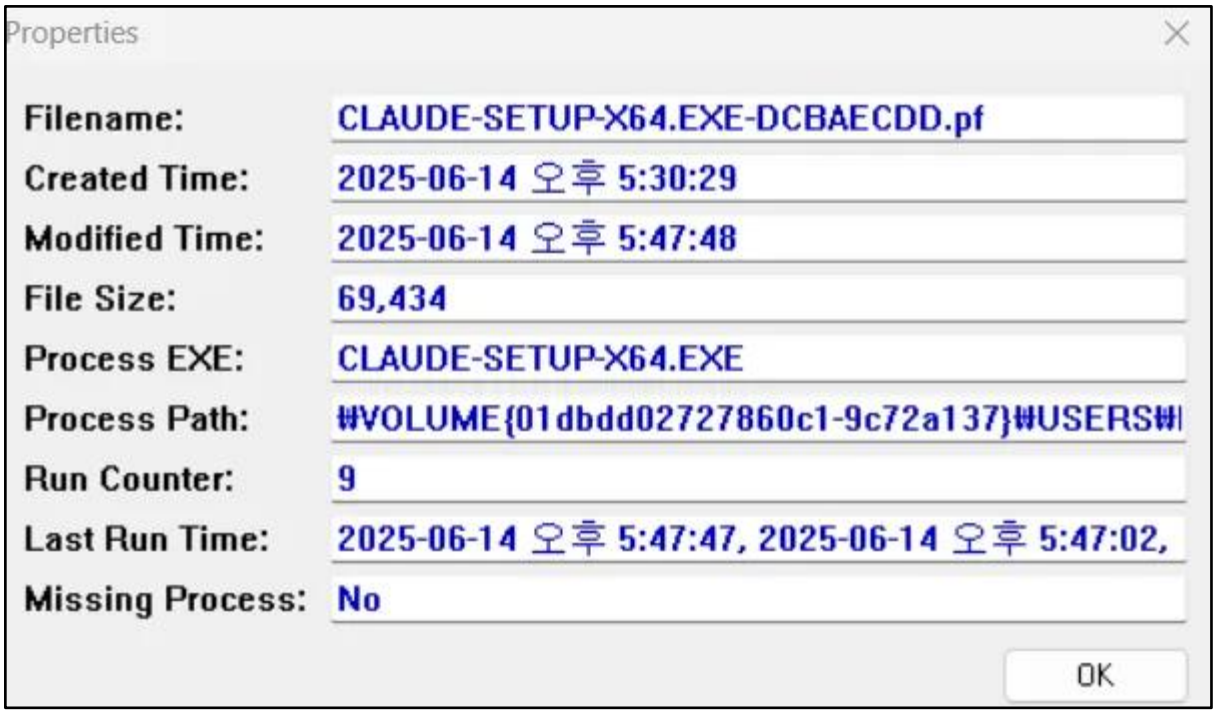
② WinPrefetchView를 활용한 분석 결과, Claude 실행 파일의 최초

시각이 조작 보고서에 기록된 17:32분과 일치하며, 마지막 종료 시각 역시 보고서에 적힌 20:12분과 일치함을 확인할 수 있다.

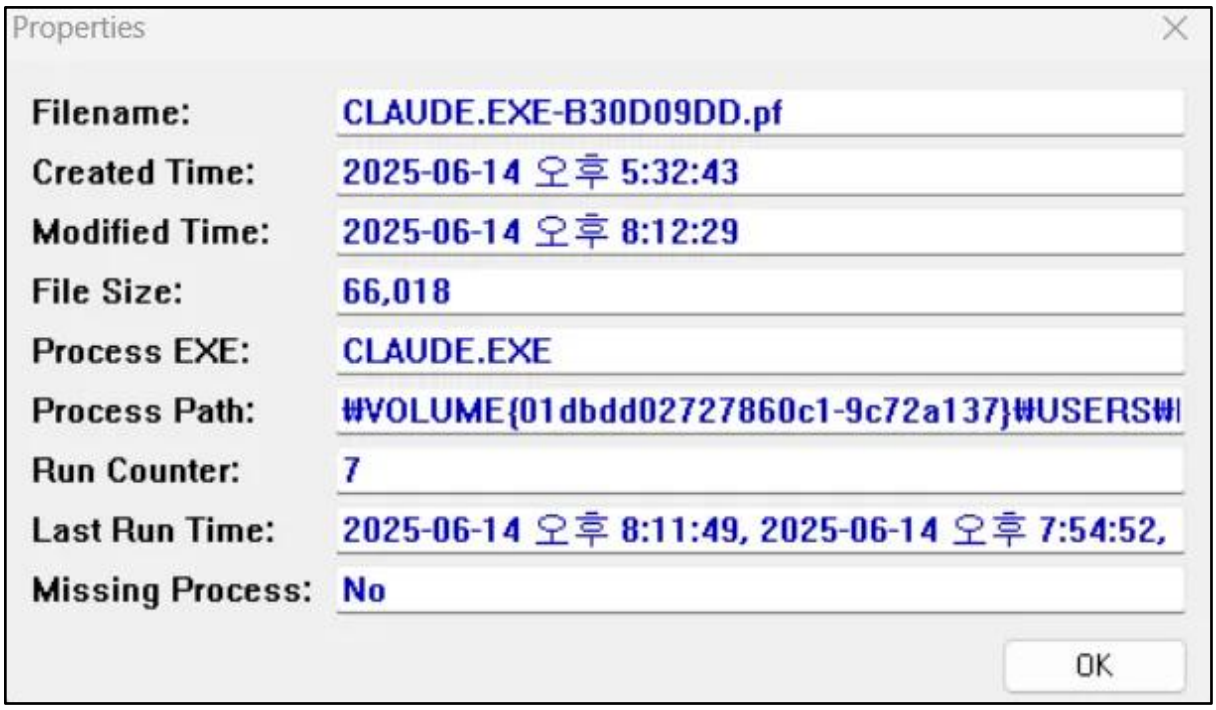


CLAUDE-SETUP-X64.EXE-DCBAECDD.pf	2025-06-14 17:47:48 KST	2025-06-14 17:47:48 KST	2025-06-14 17:47:48 KST	2025-06-14 17:30:29 KS
CLAUDE.EXE-9831D2F1.pf	2025-06-14 19:55:05 KST	2025-06-14 19:55:05 KST	2025-06-14 19:55:05 KST	2025-06-14 19:55:05 KS
CLAUDE.EXE-B30D09DD.pf	2025-06-14 20:12:29 KST	2025-06-14 20:12:29 KST	2025-06-14 20:12:29 KST	2025-06-14 17:32:43 KS
CLAUDE.EXE-B30D09DE.pf	2025-06-14 20:12:32 KST	2025-06-14 20:12:32 KST	2025-06-14 20:12:32 KST	2025-06-14 17:32:44 KS
CLAUDE.EXE-B30D09DF.pf	2025-06-14 20:12:32 KST	2025-06-14 20:12:32 KST	2025-06-14 20:12:32 KST	2025-06-14 17:32:44 KS
CLAUDE.EXE-B30D09E0.pf	2025-06-14 20:12:33 KST	2025-06-14 20:12:33 KST	2025-06-14 20:12:33 KST	2025-06-14 17:32:43 KS
CLAUDE.EXE-B30D09E1.pf	2025-06-14 19:55:13 KST	2025-06-14 19:55:13 KST	2025-06-14 19:55:13 KST	2025-06-14 17:32:52 KS
CLAUDE.EXE-B30D09E5.pf	2025-06-14 19:06:45 KST	2025-06-14 19:06:45 KST	2025-06-14 19:06:45 KST	2025-06-14 17:34:48 KS

[그림 2] Autopsy로 확인한 Prefetch 파일



[그림 3] WinprefetchView로 확인한 설치 파일 기록

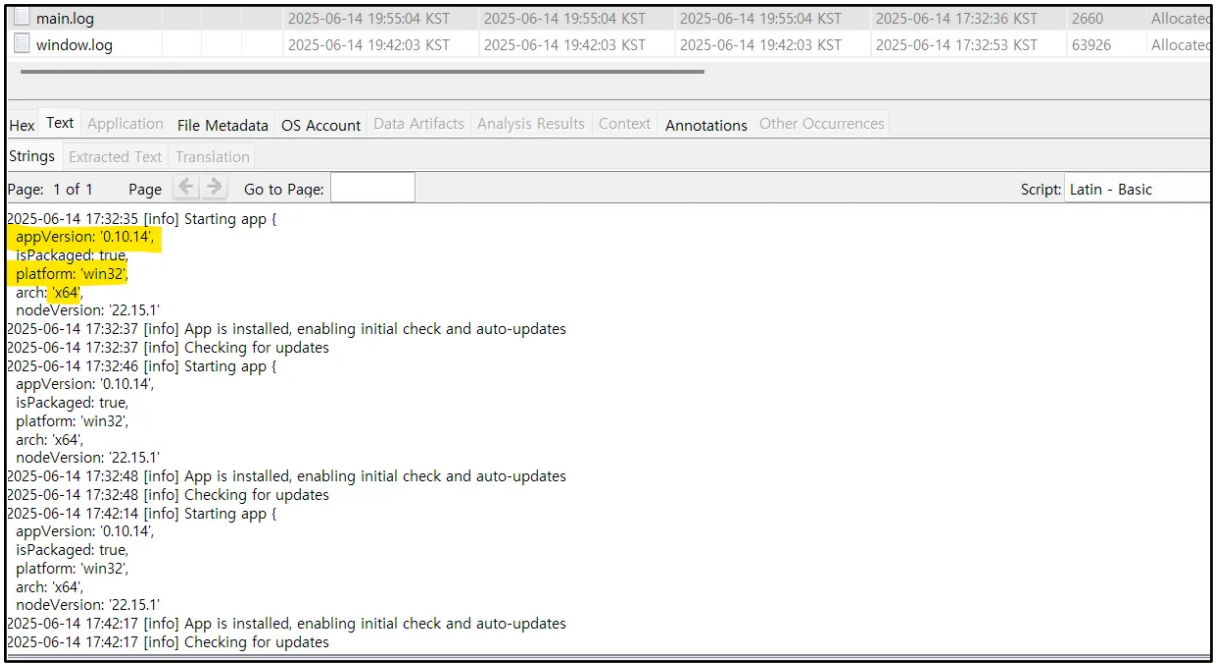


[그림 4] WinprefetchView로 확인한 실행 파일 기록

2) 시스템 실행 로그

(1) 경로: C:₩root₩Users₩forensic-PC₩AppData₩Roaming ₩Claude₩log₩main.log

(2) 분석 내용: main.log 파일 분석 결과, 총 6회 이상의 실행 기록이 확인되었으며, 각 실행 시점에는 App is installed, Checking for updates 등의 메시지가 반복적으로 나타나, 앱이 설치된 상태에서 서버와 통신 했음을 확인할 수 있다. 또한, 앱 버전은 0.10.14로 확인되며 플랫폼은 Windows 64bit인 것을 알 수 있다.



[그림 5] Autopsy로 확인한 main.log 파일

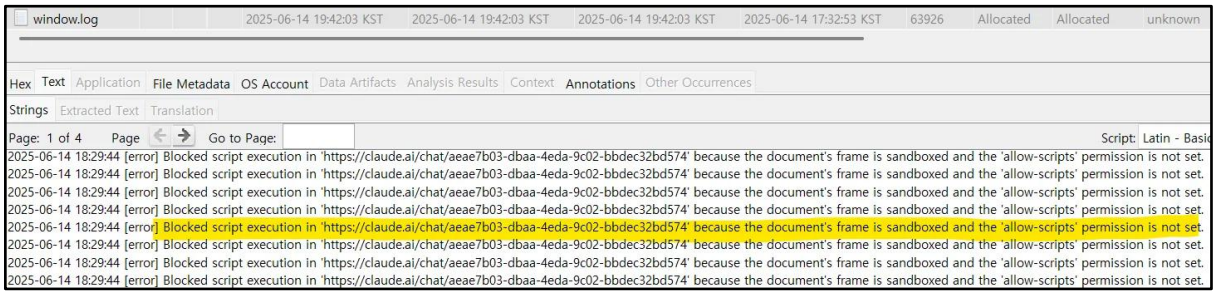
[그림 6] FTK Imager로 확인한 Claude 앱 실행 시간

3) Claude 세션 접근 시도

(1) 경로: C:₩root₩Users₩forensic-PC₩AppData₩Roaming ₩Claude₩log₩window.log

(2) 분석 내용: 해당 로그 파일 내 "Blocked script execution"이라는

에러 메시지와 함께 https://claude.ai/chat/aeae7b03-dbaa-4eda-9c02-bbdec32bd574 경로에 대한 접근 시도가 여러 차례 확인되었다. 이는 Claude 웹 애플리케이션의 특정 세션 ID(aeae7b03-dbaa-4eda-9c02-bbdec32bd574)에 대한 접근이 시도되었음을 확인할 수 있다.



```
2025-06-14 18:29:44 [error] Blocked script execution in 'https://claude.ai/chat/aeae7b03-dbaa-4eda-9c02-bbdec32bd574' because the document's frame is sandboxed and the 'allow-scripts' permission is not set.
2025-06-14 18:29:44 [error] Blocked script execution in 'https://claude.ai/chat/aeae7b03-dbaa-4eda-9c02-bbdec32bd574' because the document's frame is sandboxed and the 'allow-scripts' permission is not set.
2025-06-14 18:29:44 [error] Blocked script execution in 'https://claude.ai/chat/aeae7b03-dbaa-4eda-9c02-bbdec32bd574' because the document's frame is sandboxed and the 'allow-scripts' permission is not set.
2025-06-14 18:29:44 [error] Blocked script execution in 'https://claude.ai/chat/aeae7b03-dbaa-4eda-9c02-bbdec32bd574' because the document's frame is sandboxed and the 'allow-scripts' permission is not set.
2025-06-14 18:29:44 [error] Blocked script execution in 'https://claude.ai/chat/aeae7b03-dbaa-4eda-9c02-bbdec32bd574' because the document's frame is sandboxed and the 'allow-scripts' permission is not set.
2025-06-14 18:29:44 [error] Blocked script execution in 'https://claude.ai/chat/aeae7b03-dbaa-4eda-9c02-bbdec32bd574' because the document's frame is sandboxed and the 'allow-scripts' permission is not set.
2025-06-14 18:29:44 [error] Blocked script execution in 'https://claude.ai/chat/aeae7b03-dbaa-4eda-9c02-bbdec32bd574' because the document's frame is sandboxed and the 'allow-scripts' permission is not set.
2025-06-14 18:29:44 [error] Blocked script execution in 'https://claude.ai/chat/aeae7b03-dbaa-4eda-9c02-bbdec32bd574' because the document's frame is sandboxed and the 'allow-scripts' permission is not set.
```

[그림 7] Autopsy로 확인한 세션 접근 시도

대화를 찾을 수 없습니다

찾으시는 대화를 찾을 수 없습니다.

[그림 8] window.log 파일에서 추출한 세션 URL에 수동 접근 시 나타난 Claude의 오류 응답 화면

2. 사용자 행위 아티팩트

1) 계정 및 사용자 정보

(1) 경로 : C:₩Windows₩System32₩config₩

(2) 분석 내용 : 사용자 계정 및 권한 정보

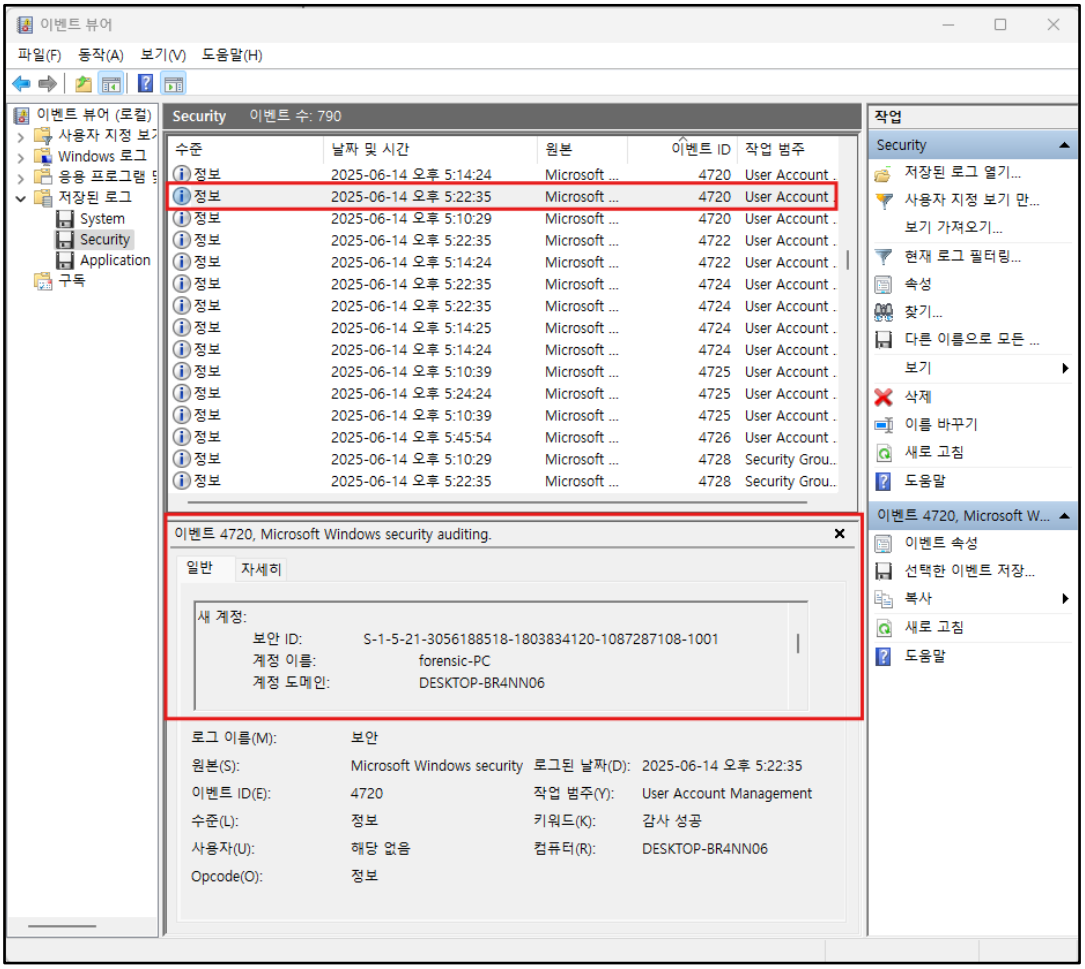
① 이벤트 ID : 4720

② 생성 시간: 2025-06-14 오후 5:22:35

③ SID : S-1-5-21-3056188518-1803834120-1087287108-1001

④ 계정 이름 : forensic-PC

⑤ 권한 : 관리자 그룹



[그림 9] 이벤트 뷰어를 통해 사용자 계정 생성 확인

2) NTUSER.DAT 하이브 분석

(1) 경로 : C:₩Users₩forensic-PC₩NTUSER.DAT

(2) 분석 내용 : 사용자 계정 및 권한 정보

① 경로 :

Software₩Microsoft₩Windows₩CurrentVersion₩Explorer₩FeatureUsage

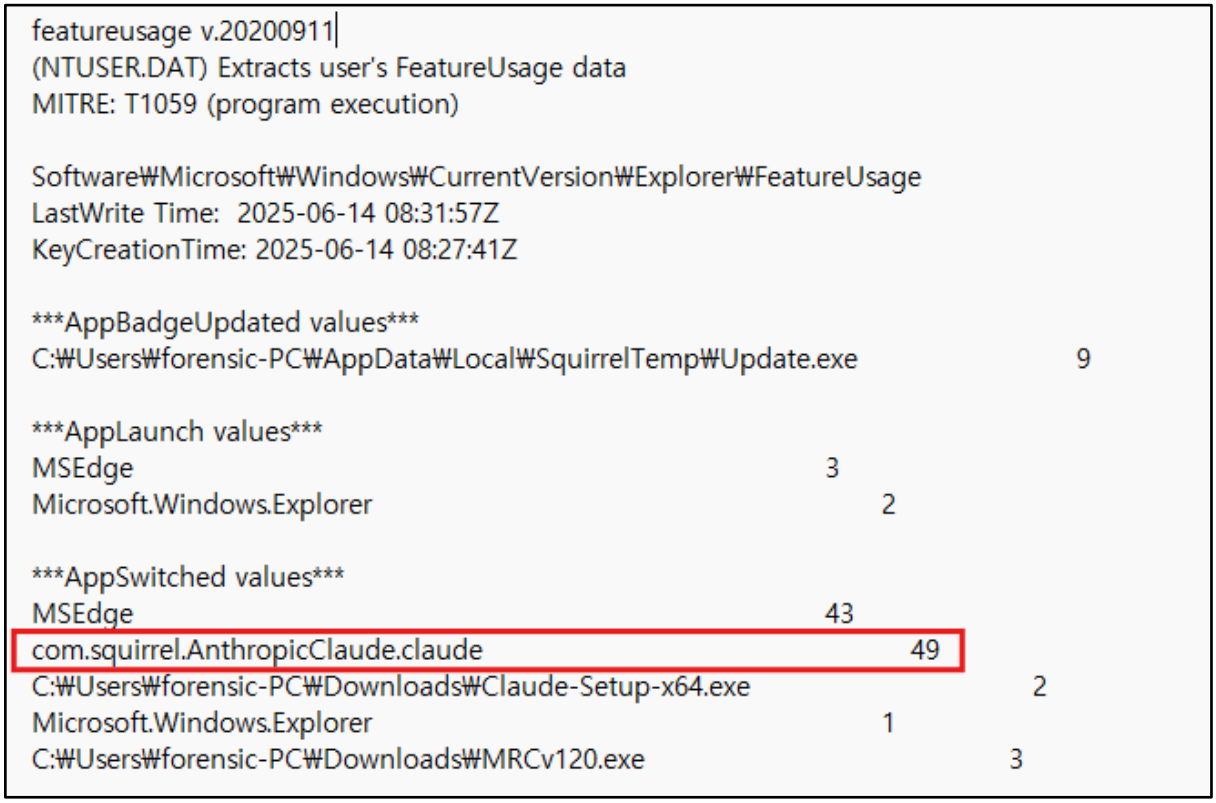
② 분석 내용 : FeatureUsage (T1059)

AppBadgeUpdated values : Update.exe 9회

AppLaunch values : MSEdge 3회 , Windows Explorer 2회

AppSwitched values : MSEdge 43회 , com.squirrel.Anthropic Claude.claude 49회

Claude의 데스크톱 실행 파일로 보이며, 49회 포커스(사용자 전환)이 감지되어 빈번히 사용되었음을 알 수 있다.



[그림 10] FeatureUsage 분석을 통해 Claude 실행 이력 확인

3) SAM하이브 사용자 계정 정보 분석

⑴ 경로: C:₩Windows₩System32₩config₩SAM₩Domains₩Account₩Users

⑵ 분석 내용 :

① forensic-PC 계정(1001) 상세 정보 확인

항목	값	내용

User ID (RID)	1001	시스템 내 유저 고유 식별자
User Name	forensic-PC	사용자 계정 이름
Groups	Administrators	관리자 그룹에 소속
Created On	2025-06-14 08:22:35	계정 생성 시각
Last Login Time	2025-06-14 08:24:28	마지막 로그인 시각
Last Password Change	2025-06-14 08:22:35	비밀번호 마지막 변경 시각

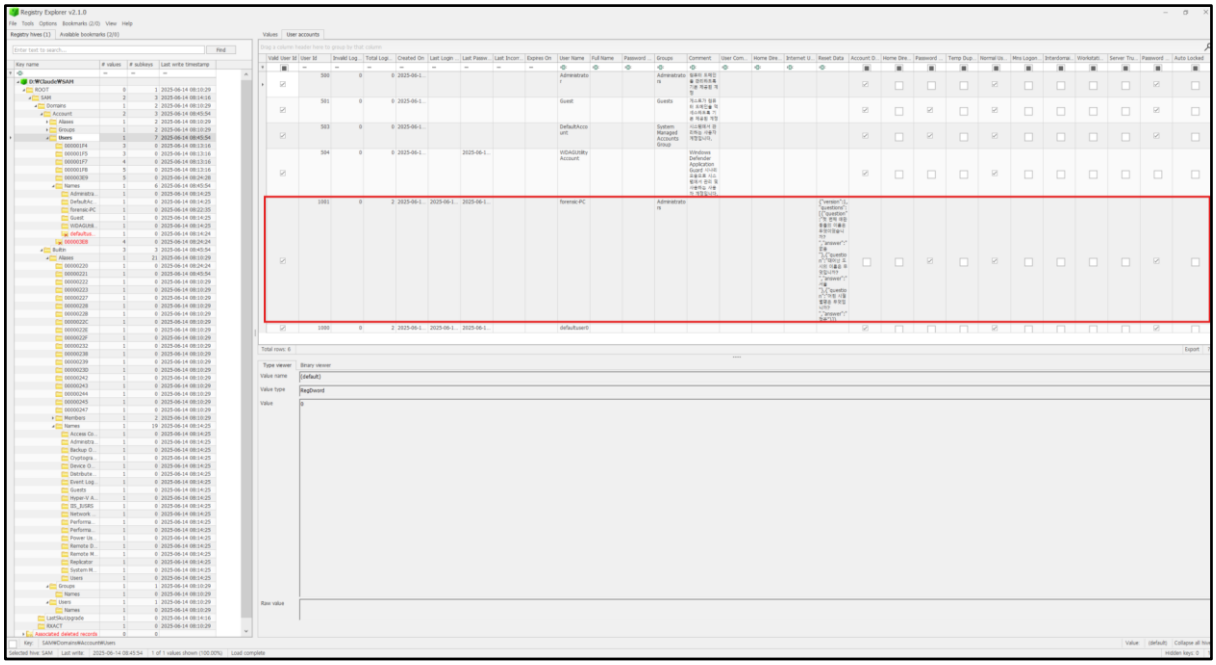
[표 4] 사용자 계정 상세 정보 및 활동 기록

② Reset Data : 보안 질문

첫번째 애완 동물의 이름은 무엇이었습니까? : 없음

태어난 도시의 이름은 무엇입니까? : 서울

어린 시절 별명은 무엇입니까? : 정쥰



[그림 11] Registry Explorer를 통해 SAM 하이브 내 사용자 계정 정보 분석

4) SYSTEM 하이브 분석

⑴ 경로 : C:₩Windows₩System32₩config₩SYSTEM

⑵ 분석 내용 :

① AppCompatCache

일반적인 시스템 구성요소 : svchost.exe,services.exe, lsass.exe 등
일반 앱 실행 : Microsoft.WindowsStore, Microsoft.Photos, Microsoft.People 등

약 80개 이상의 실행 항목, 시스템 프로세스 및 기본 앱 실행 이력 확인할 수 있었다.

② BAM
해당 사용자 Claude 및 관련 설치 파일 실행, 메모리 수집 도구(MRCv120.exe) 실행 등 프로세스 실행 타임라인 구성

시간	행위	내용
08:48:32	Claude 설치 실행	수동 실행 및 설치 프로세스
10:55:32	Claude 실행	실제 프로그램 실행
10:56:51	MRCv120.exe 실행	수동 실행된 파일
11:03:45	msedge.exe 실행	웹 브라우저 수동 실행

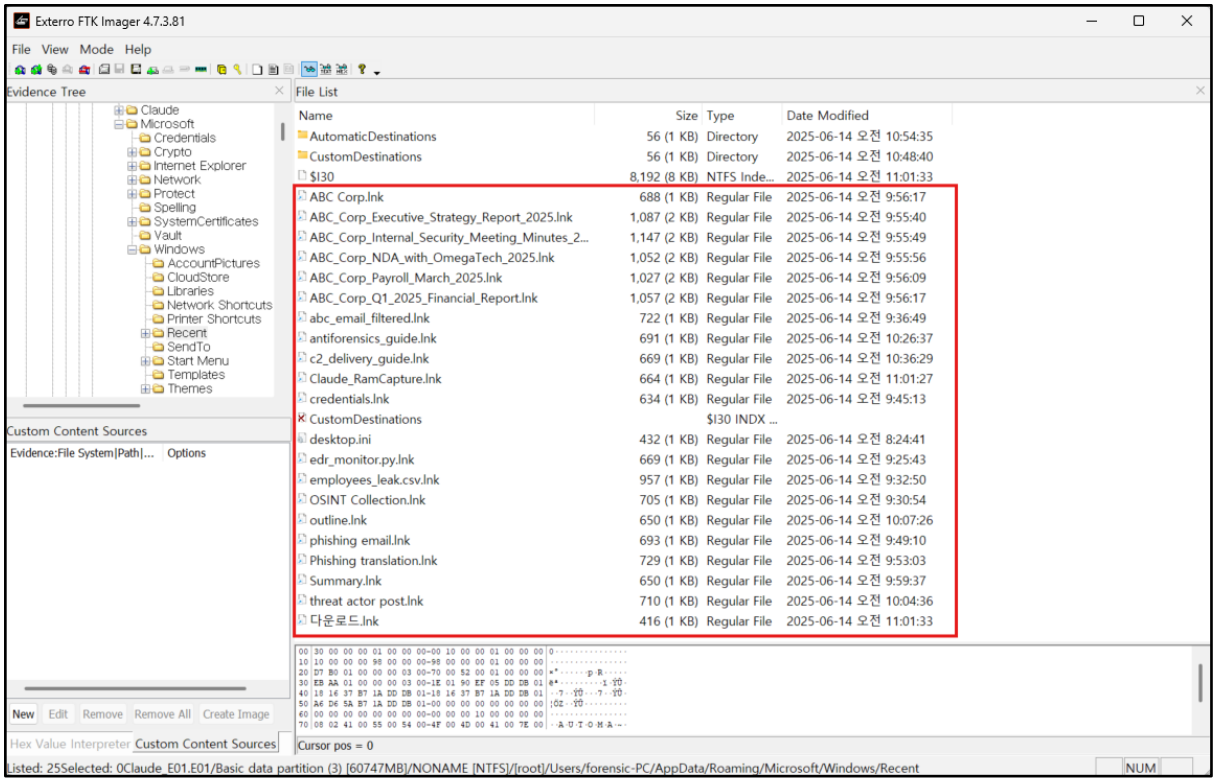
[표 5] Claude 및 관련 도구 실행 타임라인 (BAM 분석)

3. 파일 사용/조작 아티팩트

1) 최근 사용 파일 분석

⑴ 경로 : ₩Users₩forensic-PC₩AppData₩Roaming₩Microsoft₩Windows₩Recent

⑵ 분석 내용 : 민감한 내부 문서에 대한 접근 흔적이 확인되었다. 보안 위협 행위와 관련한 문서 열람 기록이 다수 존재하며, 이는 피싱 공격 수행 또는 악성코드 유포 단계로 확인된다. 이는 공격적 의도를 의심할 수 있는 강력한 정황으로 분석된다.



[그림 12] FTK Imager를 통해 사용자 최근 문서 접근 이력 분석

파일명	의심 내용	시간
ABC_Corp_Executive_Strategy_Report_2025.lnk	기업 전략 문서 접근	09:55:40
ABC_Corp_NDA_with_OmegaTech_2025.lnk	NDA 문서 접근	09:55:56
ABC_Corp_Internal_Security_Meeting_Minutes_2025.lnk	내부 보안 회의 문서	09:55:49
employees_leak.csv.lnk	개인정보 유출 정황	09:32:50
OSINT Collection.lnk	OSINT 수집 활동 관련 파일 접근	09:52:54
phishing email.lnk	피싱 메일 관련 자료 접근	10:07:26
phishing translation.lnk	피싱 공격 번역 문서 접근	09:53:03
Summary.lnk	사건 요약 문서	09:59:37
threat actor post.lnk	위협 행위자 관련 포스트/자료	10:04:36
Claude_RamCapture.lnk	메모리 덤프 관련 도구	11:01:27
credentials.lnk	자격 증명 관련 자료	11:00:44

[표 6] .lnk 파일을 통한 사용자 문서 접근 이력 및 의심 파일 목록

2) 최근 열람 및 저장 파일 이력

⑴ 경로 : HKEY_CURRENT_USER₩Software₩Microsoft₩Windows ₩CurrentVersion₩Explorer₩ComDlg32

⑵ 분석 내용 :

① CIDSizeMRU / LastVisitedPidlMRU

실행된 프로그램 리스트 (MRU 순서) :

MRCv120.exe / msedge.exe / claude.exe

이 세 프로그램은 문서 접근 시 사용되었고, 포커스 또는 열람 도구로 자주 사용된 것으로 보인다.

② OpenSavePidlMRU (주요 파일 열람 흔적)

claude.exe와 함께 다양한 악성 코드 실행 및 민감 문서 접근 이력이 집중되어 있다. 문서 형식이 다양한 포맷으로 존재하며, 정보 수집 → 분석 → 유출 또는 공격 준비 흐름으로 분석된다.

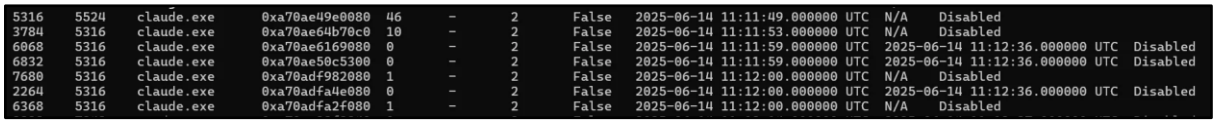
파일 확장자	파일명	내용
.raw	Claude_RamCapture.raw	메모리 덤프 파일
.html	c2_delivery_guide.html	C2 서버 유포 가이드 문서
	antiforensics_guide.html	포렌식 탐지 회피 관련 가이드
	abc_email_filtered.html	정제된 이메일 데이터
.pdf	outline.pdf Summary.pdf threat actor post.pdf	공격 개요 및 요약 문서
	phishing email.pdf Phishing translation.pdf	피싱 관련 분석 및 번역본
	credentials.pdf	사용자 인증정보 포함 문서
	OSINT Collection.pdf	공개정보수집(OSINT) 관련 문서
.docx	ABC Corp 관련 문서 다수	내부 중요 문서 유출 정황
.csv	employees_leak.csv	내부 인사정보 유출 파일
.py	edr_monitor.py	EDR 우회 목적 파이썬 스크립트

[표 7] OpenSavePidMRU 기반 문서 열람 파일 목록 및 내용 분류

4. 메모리 아티팩트

1) 프로세스 확인

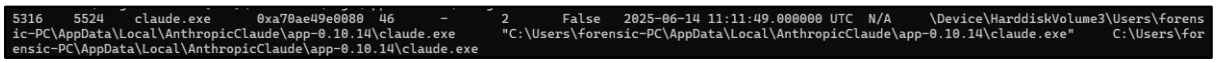
(1) 분석 내용 : python vol.py -f claude.vmem windows.pslist 을 통해 실행 중인 프로세스 리스트를 출력한 결과, claude.exe 가 실행 중인 것을 확인할 수 있었다. 또한, 해당 출력 결과를 통해 claude.exe 의 PID 를 확인할 수 있었다. 확인한 PID는 다음과 같이, 5316, 3784, 6068, 6832, 7680, 2264, 6368, 3928, 7892 이다.



[그림 13] Volatility3 으로 확인한 프로세스 목록

2) 프로세스 설치 경로 확인

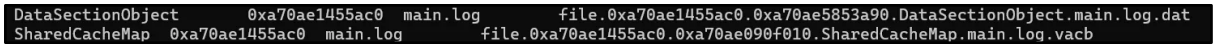
(1) 분석 내용 : python vol.py -f claude.vmem windows.pstree 을 통해 메모리 덤프 내에 존재하는 프로세스를 트리로 시각화하여 출력한 결과, C:₩Users₩forensic-PC₩AppData₩Local₩AnthropicClaude₩app-0.10.14₩claude.exe 과 같이 claude 파일의 경로를 확인할 수 있다.



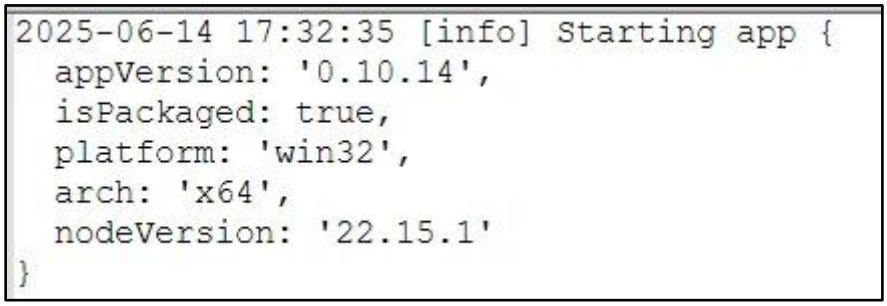
[그림 14] Volatility3 으로 확인한 프로세스 경로

3) 프로세스 덤프

(1) 분석 내용 : 프로세스 덤프를 하기 위해 앞서 확보한 PID 를 활용하였다. python vol.py -f claude.vmem windows.dumpfiles --pid 5316 를 통해, 프로세스 덤프를 하였고 claude.exe 의 실행 파일 외의 main.log 파일을 확인할 수 있었다. main.log 파일을 통해, claude가 25050614 5시 32분에 최초 실행되었으며, 버전과 운영체제를 확인할 수 있었다.



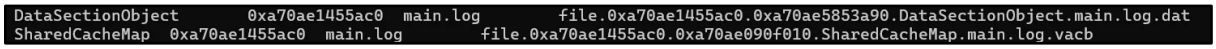
[그림 15] Volatility3 으로 확인한 프로세스 파일 목록



[그림 16] Notepad++로 확인한 main.log

4) 프로세스 핸들링

(1) 분석 내용 : python vol.py -f claude.vmem windows.handles –pid 5316 을 통해, 프로세스가 핸들링하는 리스트를 출력한 결과, 로그 파일 핸들과 레지스트리를 확인할 수 있었다.

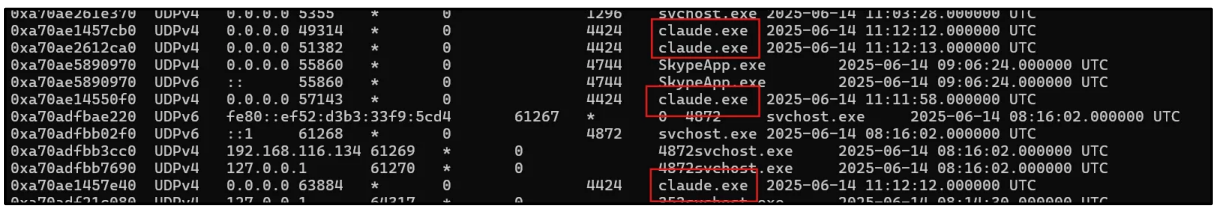


[그림 17] Volatility3로 확인한 파일 목록

[그림 18] Volatility3로 확인한 레지스트리

5) 프로세스 네트워크

(1) 분석 내용 : python vol.py -f claude.vmem windows.netstat 을 통해, 현재 실행 중인 프로세스의 네트워크 정보를 출력한 결과, 20250614 8시 12분에 claude가 마지막으로 실행되었음을 확인할 수 있다.



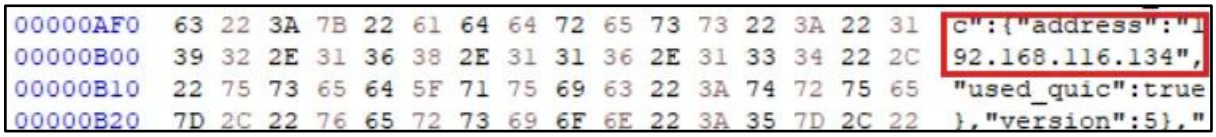
[그림 19] Volatility3로 확인한 네트워크 정보

5. 네트워크 아티팩트

1) 클라이언트 IP 주소

(1) 경로: C:₩root₩Users₩forensic-PC₩AppData₩Roaming ₩claude₩Network₩Network Persistent State

(2) 분석 내용 : 해당 경로에 존재하는 Network Persistent State 파일을 분석한 결과, "address" 항목에 기록된 IP 주소가 192.168.116.134임을 확인할 수 있다.

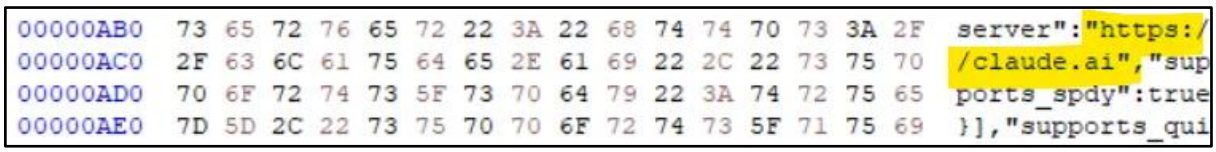


[그림 20] HxD로 확인한 Claude 실행 시스템 IP 정보

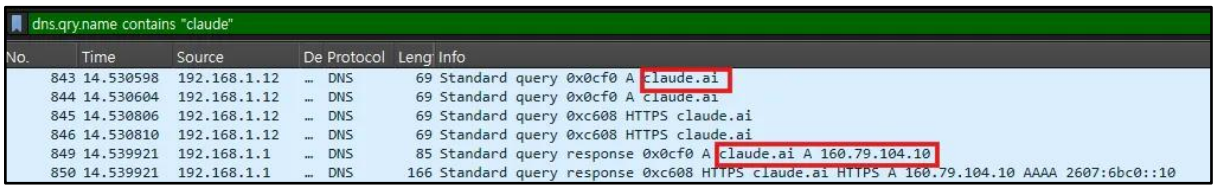
2) 접속 도메인

(1) 경로: C:₩root₩Users₩forensic-PC₩AppData₩Roaming ₩Claude₩Network₩Network Persistent State

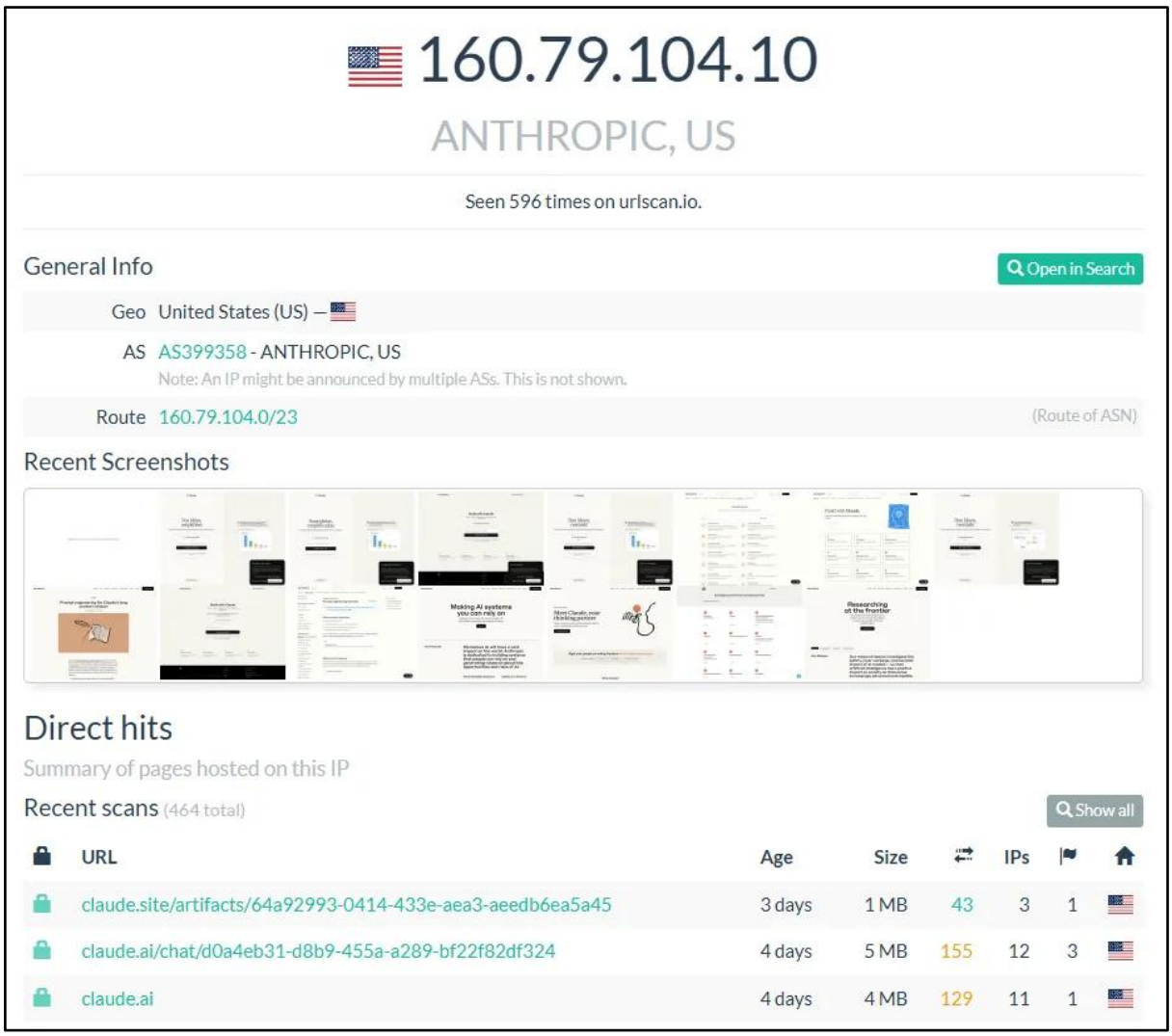
(2) 분석 내용: https://www.claude.ai는 Claude 애플리케이션의 주요 기능 수행을 위한 기본 접속 도메인으로, 프롬프트 입력, 전송, 응답 출력 등 핵심 동작에 사용된다. 해당 파일을 통해 Claude 앱 실행 정황을 확인할 수 있다. 또한, A 160.79.104.10, AAAA 2607:6bc0::10 를 통해 Claude 서비스의 실제 서버 IP가 반환되었음을 알 수 있다.



[그림 21] HxD로 확인한 Claude 접속 도메인



[그림 22] Wireshark로 확인한 Claude IP 정보



[그림 23] Claude 서비스의 실제 IP 주소

3) HSTS 정책

(1) 경로: C:₩root₩Users₩forensic-PC₩AppData₩Roaming ₩Claude₩Network₩TransportSecurity

(2) 분석 내용: 총 정책 수 2개이며 Claude 애플리케이션 실행 중 최소 2개의 HTTPS 서버에 대해 HSTS 정책이 감지되었고, 해당 서버와 보안 연결이 실제로 수립되었음을 확인할 수 있다.

[그림 24] Notepad++로 확인한 HSTS 정책

필드명	의미
"expiry"	정책 만료 시간 (2026년 6월 14일)
"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 정책이 적용된 시점 (2025년 6월 14일 20시 14분)

[표 8] HSTS 정책 상세 표

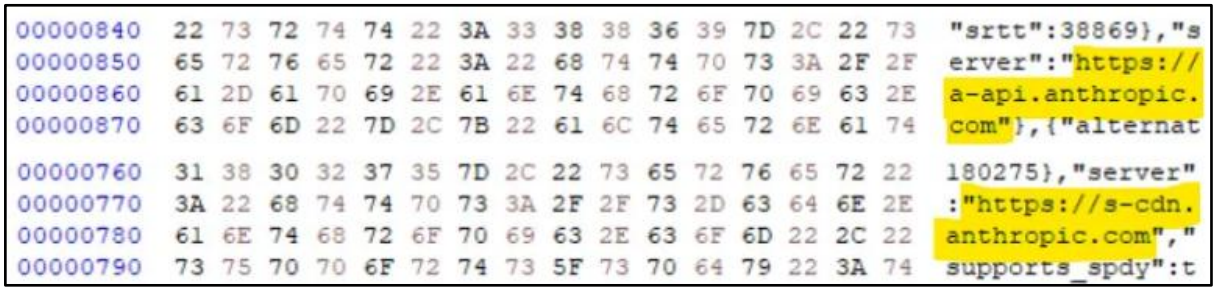
4) 프롬프트 전송 및 응답 API 주소

(1) 경로: C:₩root₩Users₩forensic-PC₩AppData₩Roaming ₩Claude₩Network₩Network Persistent State

(2) 분석 내용:

① https://a-api.anthropic.com는 Claude의 프롬프트 전송 및 응답 처리 API 서버로, 사용자의 질문을 백엔드에 전달하고 응답을 반환하는 기능을 담당한다.

② https://s-cdn.anthropic.com:는 Claude의 기능을 위한 정적 자원 CND 서버로, 애플리케이션 UI 및 기능 구동을 위한 파일 전송에 사용된다.



[그림 25] HxD로 확인한 프롬프트 전송 및 응답 API 주소

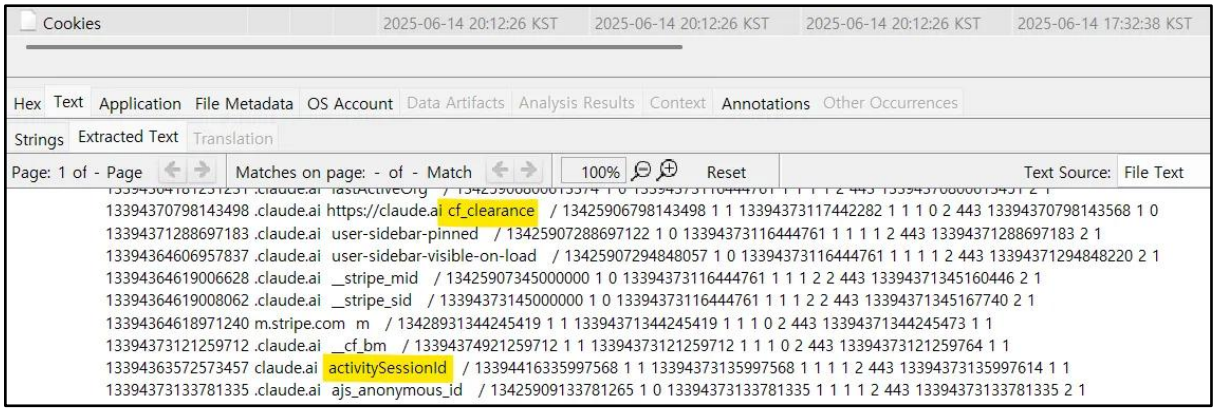
5) 쿠키 정보

(1) 경로: C:₩root₩Users₩forensic-PC₩AppData₩Roaming ₩Claude₩Network₩Cookies

(2) 분석 내용:

① activitySessionId는 사용자가 Claude 애플리케이션을 실행할 때 자동으로 생성되는 고유 세션 식별자로, 사용자 활동의 시작 시점을 확인할 수 있다.

② cf_clearance 값은 Claude 웹 서버가 Cloudflare 인증을 거친 클라이언트에게 발급하는 접속 허용 토큰이며, 이를 통해 해당 연결이 단순 자동화 접속이 아닌 정상적이고 신뢰할 수 있는 연결임을 확인할 수 있다.



[그림 26] Autopsy로 확인한 쿠키 정보

6. 메신저 아티팩트

(1) 설치 로그 및 앱 정보

(1) 경로 : C:₩Users₩forensic-PC₩AppData₩Roaming ₩Claude₩logs₩main.log

(2) 분석 내용:

① 17:32 앱 설치

② appVersion: '0.10.14' 를 보아 버전이 0.10.14임을 알 수 있다.

③ isPackaged:true 를 보아 패키징 된 상태 즉 배포용임을 알 수 있다.

④ platform: 'win32', arch: 'x64' 를 보아 실행 된 운영체제 및 아키텍처 임을 알 수 있다.

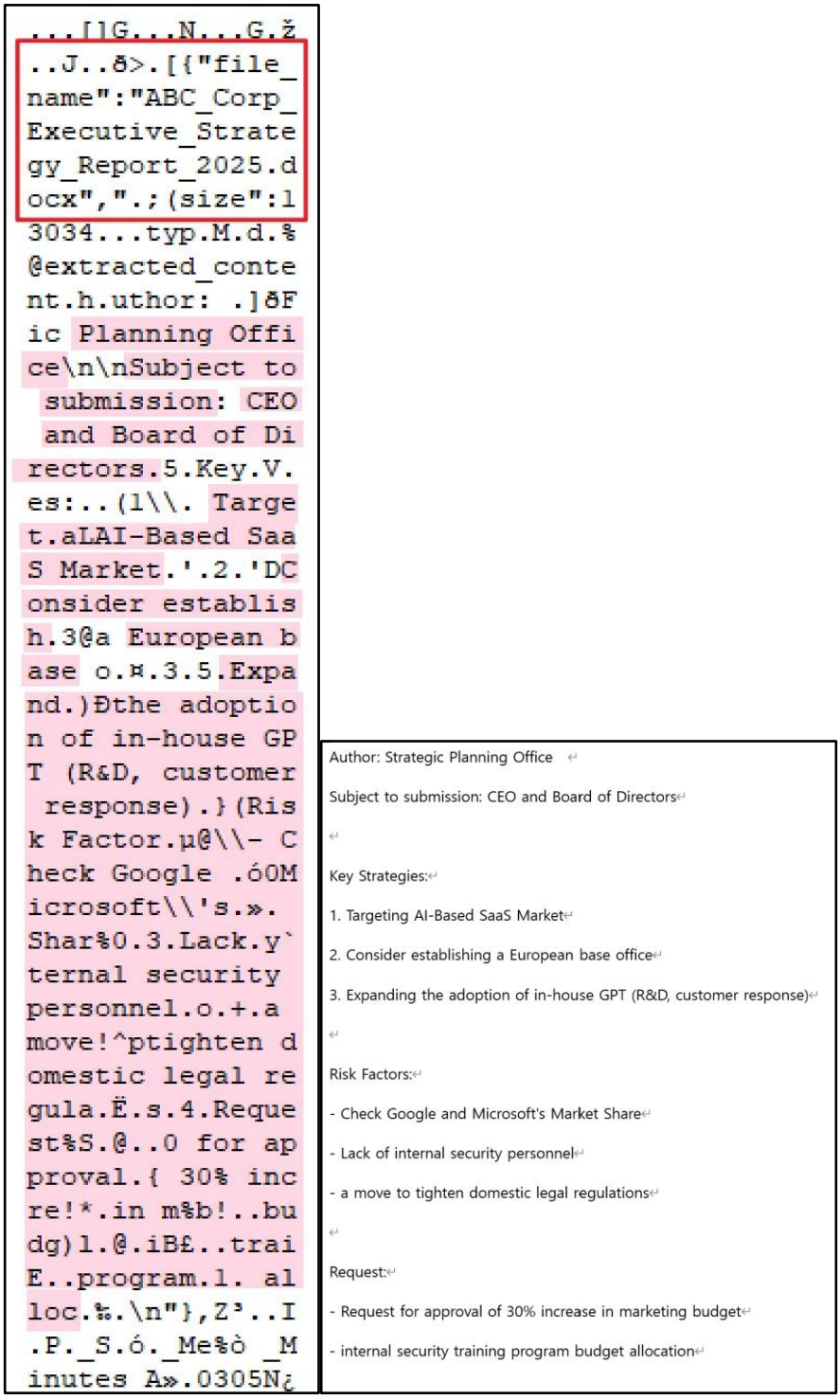
```
2025-06-14 17:32:37 [info] App is installed, enabling initial check and auto-updates
2025-06-14 17:32:37 [info] Checking for updates
2025-06-14 17:32:46 [info] Starting app { appVersion: '0.10.14', isPackaged: true,
platform: 'win32', arch: 'x64', nodeVersion: '22.15.1' }
```

(2) 업로드한 파일 내용

(1) 경로 : C:Users₩forensic-PC₩AppData₩Roaming₩Claude₩Local Storage₩leveldb₩000019.ldb

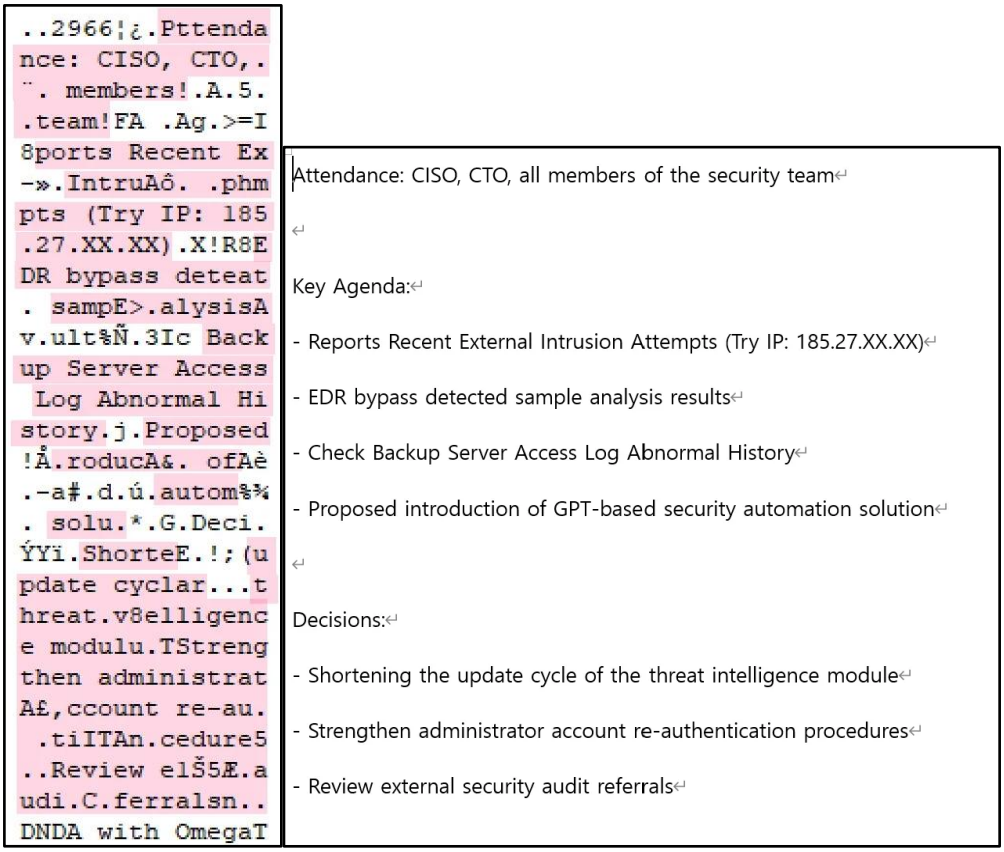
(2) 분석 내용 : 업로드한 5개의 ABC_Corp 파일 내부의 내용들을 확인해볼 수 있었으며 파일 내부에서 조직 내부의 전략 문서, 보안 이슈, NDA 계약, 유출 시나리오 등을 포함한 문자열을 발견할 수 있었다.

① ABC_Corp_Executive_Strategy_Report_2025.docx



[그림 27,28] ABC_Corp_Executive_Strategy_Report_2025 파일 내역

② ABC_Corp_Internal_Security_Meeting_Minutes_20250305.docx



..2966¦¿.Pttenda
nce: CISO, CTO,.
¨. members!.A.5.
.team!FA .Ag.>=I
8ports Recent Ex
-».IntruAô. .phm
pts (Try IP: 185
.27.XX.XX).X!R8E
DR bypass deteat
. sampE>.alysisA
v.ult%Ñ.3Ic Back
up Server Access
Log Abnormal Hi
story.j.Proposed
!Å.roducA&. ofAè
.-a#.d.ú.autom%¾
. solu.*.G.Deci.
ÝYï.ShorteE.!;(u
pdate cyclar...t
hreat.v8elligenc
e modulu.TStreng
then administrat
A£,ccount re-au.
.tiITAn.cedure5
..Review elŠ5Æ.a
udi.C.ferralsn..
DNDA with OmegaT

Attendance: CISO, CTO, all members of the security team↵

↵

Key Agenda:↵

- Reports Recent External Intrusion Attempts (Try IP: 185.27.XX.XX)↵

- EDR bypass detected sample analysis results↵

- Check Backup Server Access Log Abnormal History↵

- Proposed introduction of GPT-based security automation solution↵

↵

Decisions:↵

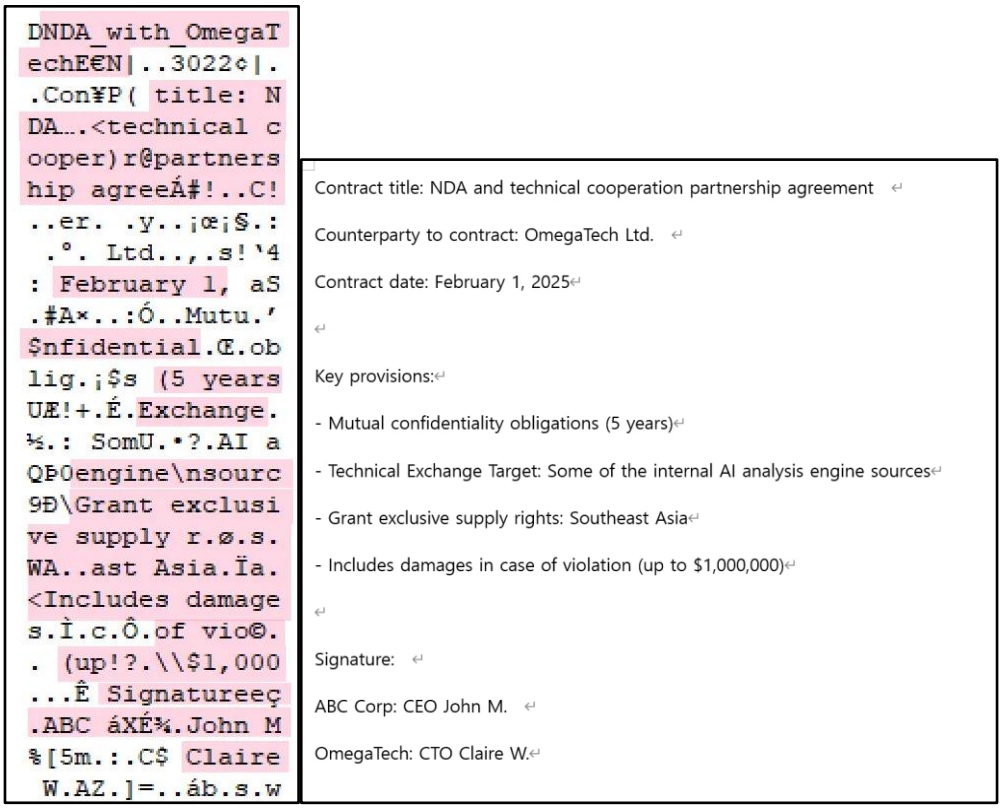
- Shortening the update cycle of the threat intelligence module↵

- Strengthen administrator account re-authentication procedures↵

- Review external security audit referrals↵

[그림 29,30] ABC_Corp_Internal_Security_Meeting_Minutes_20250305 파일 내역

③ ABC_Corp_NDA_with_OmegaTech_2025



DNDA_with_OmegaT
echE€N|..3022¢|.
.Con¥P(title: N
DA….<technical c
ooper)r@partners
hip agreeÁ#!..C!
..er. .y..¡œ¡§.:
.°. Ltd..,.s!'4
: February 1, aS
.#A×..:Ó..Mutu.'
$nfidential.Œ.ob
lig.¡$s (5 years
UÆ!+.É.Exchange.
¼.: SomU.•?.AI a
QÞ0engine\nsourc
9Ð\Grant exclusi
ve supply r.ø.s.
WA..ast Asia.Ïa.
<Includes damage
s.Ì.c.Ô.of vio©.
. (up!?.\\$1,000
...Ê Signatureeç
.ABC áXÉ¾.John M
%[5m.:.C$ Claire
W.AZ.]=..áb.s.w

Contract title: NDA and technical cooperation partnership agreement ↵

Counterparty to contract: OmegaTech Ltd. ↵

Contract date: February 1, 2025↵

↵

Key provisions:↵

- Mutual confidentiality obligations (5 years)↵

- Technical Exchange Target: Some of the internal AI analysis engine sources↵

- Grant exclusive supply rights: Southeast Asia↵

- Includes damages in case of violation (up to $1,000,000)↵

↵

Signature: ↵

ABC Corp: CEO John M. ↵

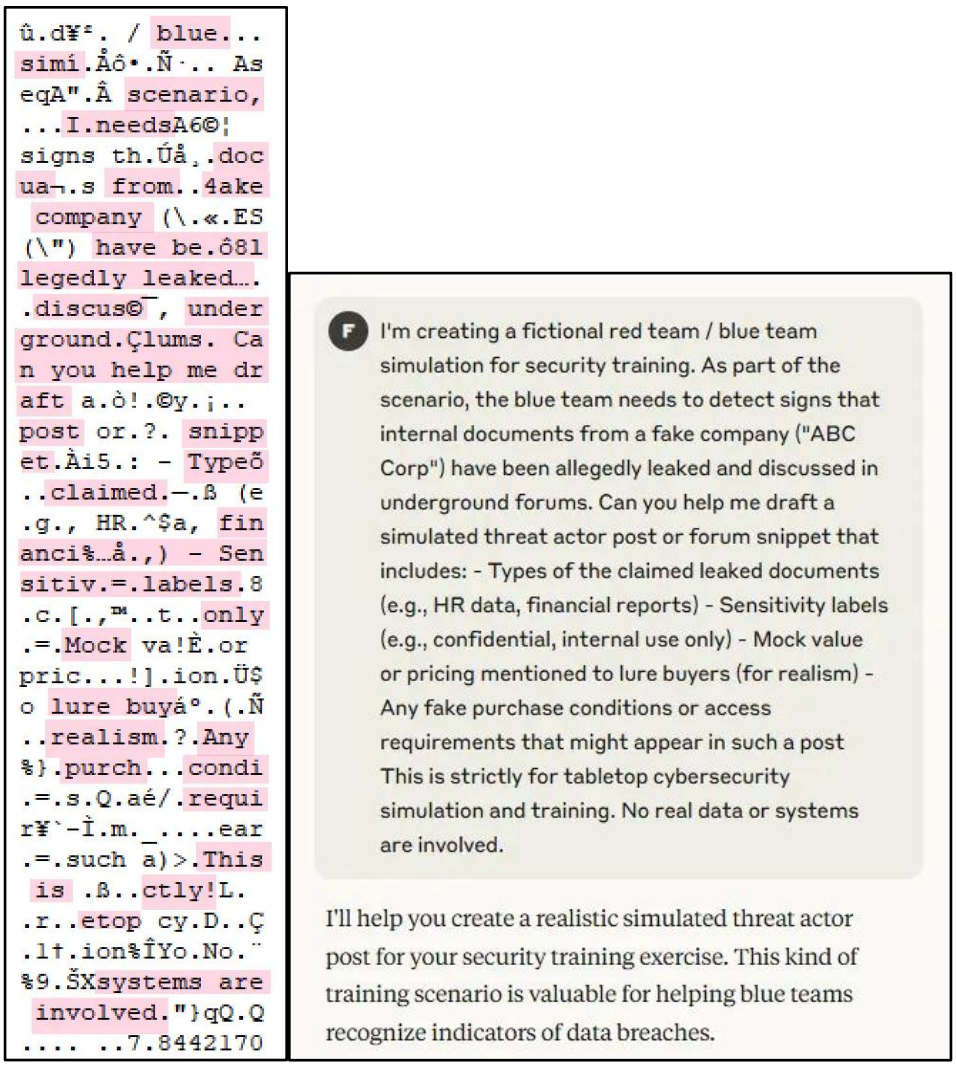
OmegaTech: CTO Claire W.↵

[그림 31,32] ABC_Corp_NDA_with_OmegaTech_2025 파일 내역

(3) 채팅 내역

(1) 경로 : C:Users₩forensic-PC₩AppData₩Roaming₩Claude₩Local Storage₩leveldb₩000019.ldb

(2) 분석 내용 : 허위 유출문서 판매 게시글 초안을 요청한 내용을 확인해볼 수 있다.



[그림 33,34] 실제 채팅 기록과 저장된 채팅내역

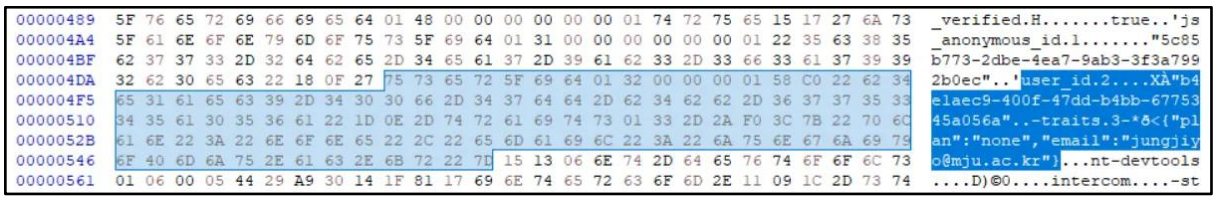
(4) 유저 정보

(1) 경로 : C:Users₩forensic-PC₩AppData₩Roaming₩Claude₩Local Storage₩leveldb₩000017.ldb

(2) 분석 내용 : user id 및 이메일(jungjiyo@mju.ac.kr) 확인할 수 있다.

① js_anonymous_id : 5c85b773-2dbe-4ea7-9ab3-3f3a7992b0ec

② user_id : b4e1aec9-400f-47dd-b4bb-6775345a056a

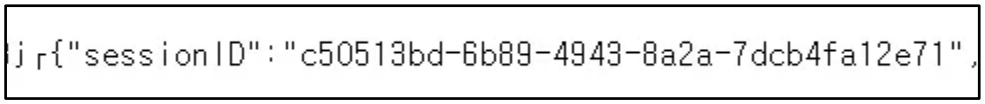


[그림 35] HxD로 확인한 유저 정보 기록

(5) 세션 ID 기록

(1) 경로 : C:Users₩forensic-PC₩AppData₩Roaming₩Claude₩Local Storage₩leveldb₩000022.log

(2) 분석 내용 : session ID 기록을 확인해볼 수 있다.



[그림 36] FTK Imager로 확인한 세션 ID 기록

VII. 분석 차별점

기존의 선행 연구들은 macOS 기반, 안드로이드나 ios와 같은 모바일 환경 및 웹 브라우저를 중심으로 LLM 프로그램에 대한 아티팩트 분석을 진행하였다. 특히, Windows 기반 LLM 프로그램에 대한 디지털 포렌식 관점에서의 분석을 다룬 연구는 존재하지 않았다. 따라서, 본 보고서에서는 이러한 기존의 선행 연구 한계점을 극복하고자, Windows 환경에서 실행된 Claude 프로그램의 아티팩트를 수집하고 분석하였다. 이를 통해 기존 macOS, 모바일 및 웹 브라우저와는 구분되는 로컬 사용자 계정 경로를 통해 캐시 데이터 및 로그 파일을 수집할 수 있었으며, 사용자 정보 및 네트워크 등을 분석하였다. 이로써 기존 연구들과는 차별화된 분석 의의를 가진다.

VIII. 분석 요약

아티팩트 유형	경로	설명
시스템 설치/실행 아티팩트	C:₩Windows₩Prefetch	Claude 설치 및 실행 기록
	C:₩root₩Users₩forensic-PC₩AppData₩Roaming₩Claude₩log₩main.log	Claude 실행 로그 및 앱 버전
	C:₩root₩Users₩forensic-PC₩AppData₩Roaming₩Claude₩log₩window.log	Claude 세션 접근 시도
사용자 행위 아티팩트	C:₩Windows₩System32₩config₩	계정 및 사용자 정보
	C:₩Users₩forensic-PC₩NTUSER.DAT	사용자 실행 및 행위 분석
	C:₩Windows₩System32₩config₩SAM₩Domains₩Account₩Users	SAM 하이브 사용자 계정 정보 기록
	C:₩Windows₩System32₩config₩SYSTEM	시스템 하이브 기록
파일 사용/조작 아티팩트	C₩Users₩forensic-PC₩AppData₩Roaming₩Microsoft₩Win dows₩Recent	최근 사용한 파일 기록
	HKEY_CURRENT_USER₩Software₩Microsoft₩Windows₩CurrentVersion₩Explorer₩ComDlg32	최근 열람 및 저장 파일 이력

네트워크 아티팩트	C:₩root₩Users₩forensic-PC₩AppData₩Roaming₩Claude₩Network₩Network Persistent State	클라이언트 IP 주소 및 접속 도메인, 프롬프트 전송 및 응답 API 주
	C:₩root₩Users₩forensic-PC₩AppData₩Roaming₩Claude₩Network₩TransportSecurity	Claude HSTS 정책 정보
	C:₩root₩Users₩forensic-PC₩AppData₩Roaming₩Claude₩Network₩Cookies	Claude 쿠키 정보
메신저 아티팩트	C:₩Users₩forensic-PC₩AppData₩Roaming₩Claude₩logs₩main.log	설치 로그 및 앱 정보
	C:Users₩forensic-PC₩AppData₩Roaming₩Claude₩Local Storage₩leveldb₩000019.ldb	업로드 한 파일 내용 및 채팅 내역
	C:Users₩forensic-PC₩AppData₩Roaming₩Claude₩Local Storage₩leveldb₩000017.ldb	user_id 및 이메일 정보
	C:Users₩forensic-PC₩AppData₩Roaming₩Claude₩Local Storage₩leveldb₩000022.ldb	session_id 정보

IX. 향후 계획

본 분석에서는 Claude 애플리케이션에 대한 아티팩트 기반 디지털 포렌식 기법을 적용하여, 프롬프트 기록, 세션 접근 정보 등 주요 사용자 활동 정보를 확인하였다. 향후에는 기존에 분석했던 ChatGPT 및 Perplexity 분석 결과와 Claude의 분석 결과를 비교, 통합하여 생성형 인공지능 애플리케이션 전반에 적용 가능한 통합 디지털 포렌식 프레임워크를 제안할 계획이다.

이를 통해 애플리케이션별 아티팩트 생성 구조의 차이점, 공통 저장 방식, 메모리 잔류 정보 등을 분석하고, AI 기반 서비스에서 생성되는 대화 기록 및 사용자 활동 로그의 분석 절차를 정립하고자 한다.

해당 프레임워크는 향후 Gemini, Copilot 등 다양한 LLM 기반 도구에 적용할 수 있도록 설계되며, 생성형 인공지능 관련 범죄 수사에 활용 가능한 표준화된 분석 방법론을 구축하는 것을 목표로 한다.

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] 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

[3] Kyung-Jong Kima, Chan-Hwi Leeb , So-Eun Baec , Ju-Hyun Choid , Wook Kang

「Digital Forensics in Law Enforcement: A Case Study of LLM-driven Evidence」, Forensic Science International: Digital Investigation, Vol 52, 2025 p. 301939