**[디스코드 분석 보고서]**

[아티팩트 상세 분석 보고서]



|  |  |
| --- | --- |
| 작성일 | 2025.05.25 |
| 작성자 | 배영혜, 안서진 |
| 검토자 | 김예은, 안서진 |

**목차**

|  |
| --- |
| [**I. 기본 정보 3**](#_3rk4botx0g0i)  [**II. 프로그램 개요 3**](#_j29bm4m42ksx)  [1. 프로그램 목적 3](#_ht31eut9n2b)  [2. 주요 기능 요약 3](#_7npsg73vvw73)  [**III. 분석 도구 정보 3**](#_91m7swmojyuj)  [**IV. 해시값 4**](#_nxi2nmlepsp4)  [**V. 분석 아티팩트 5**](#_iaqdc1v0qlr2)  [1. 시스템 설치/실행 아티팩트 5](#_ednptlrrst73)  [2. 사용자 행위 아티팩트 7](#_27gq0tj9b6g8)  [3. 파일 사용/조작 아티팩트-완료 9](#_k3ylva70fshj)  [4. 메모리 아티팩트 - 완료 1](#_82h6zqtanxb4)1  [5. 네트워크 아티팩트 -완료 12](#_ued8rd4mm1lj)  [6. 메신저 아티팩트 19](#_iuxquui4pwss)  [**VI. 분석 요약 23**](#_h2i203og73c)  [**VII. 참고 문헌 25**](#_sgnkgys9le2x)  [**VIII. 부록 26**](#_9rw69vi7n2at)  [1. store.db 파일 분석 26](#_s4p2ge4e978n) |

# 기본 정보

|  |  |
| --- | --- |
| 프로그램 범주 | 인스턴트 메신저 |
| 프로그램 | Discord |
| 버전 | 1.0.9192 |
| 다운로드 경로 | https://discord.com/download |

[표1. 기본정보]

# 프로그램 개요

## 프로그램 목적

게이밍부터, 교육과 비즈니스 영역의 커뮤니티 생성을 목적으로 설계된 VoIP 응용 소프트웨어이다.

## 주요 기능 요약

채팅 채널에 있는 유저 사이의 텍스트, 이미지, 비디오, 음성 커뮤니케이션에 특화되어 있다.

또한 무료/유료 봇을 통해 디스코드 서버 자동화가 가능하다.

# 분석 도구 정보

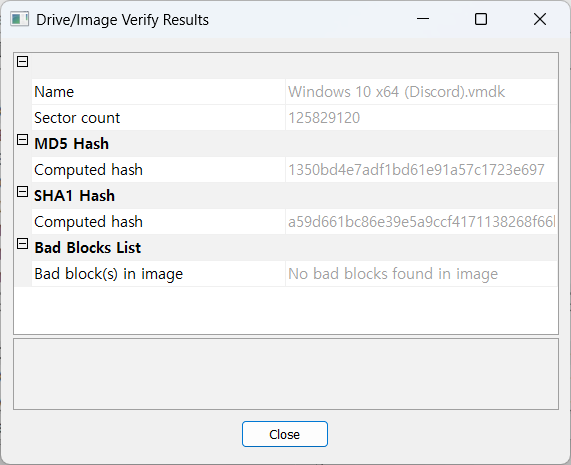
|  |  |
| --- | --- |
| 도구명 | 버전 |
| FTK Imager | v.4.5.1 |
| Registry Explorer | v.2.1.0 |
| WinPrefetchView | v.1.37 |
| NTFS Log Tracker | v.1.8 |
| rla | v.1.6.0.0 |
| SQLite | v.3.49.2 |
| Event Viewer | v1.0 |
| Wireshark | 4.4.6 |
| ChromeCacheView | v2.52 |
| HxD | v2.3 |
| Volatility | v3.0 |

[표2. 분석도구]

# 해시값

|  |  |
| --- | --- |
| 해시 | 값 |
| MD5 | 1350bd4e7adf1bd61e91a57c1723e697 |
| SHA1 | a59d661bc86e39e5a9ccf4171138268f66b0f923 |

[표3. 해시값]

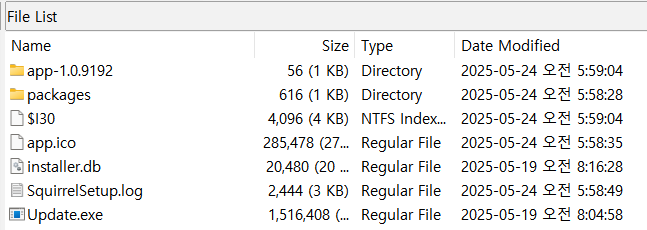


[그림1. FTK Imager로 확인한 vmdk 해시값]

# 분석 아티팩트

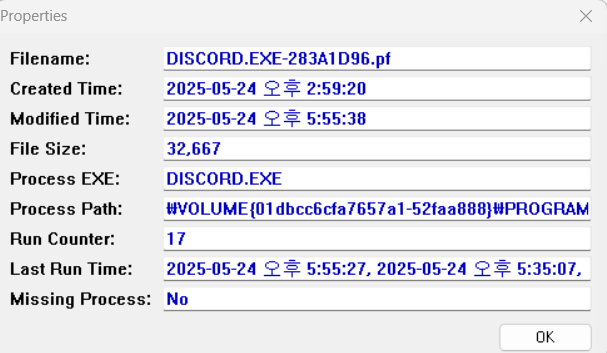
## 시스템 설치/실행 아티팩트

1. 설치 정보
2. 경로: C:\Users\DISCORD-TEST PC\AppData\Local\Discord
3. 분석 내용: 25.05.24 05:58 설치 로그 파일(SquirrelSetup.log)와 버전 폴더(app-1.0.9192), 구성 폴더가 생성되었다.



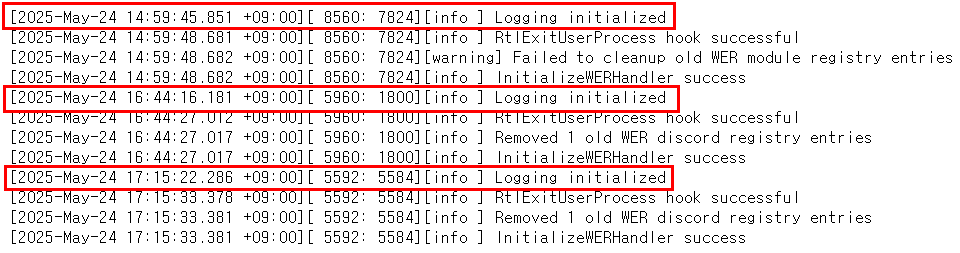
[그림2. 디스코드 설치 폴더]

1. 프리패치(PreFetch)
2. 경로: C:\Windows\Prefetch\DISCORD.EXE-283A1D96.pf
3. 분석 내용: 해당 프리패치 파일을 추출하여 시스템 실행 시각, 누적 실행 횟수 등을 확인할 수 있다. 분석 결과에 따르면, 처음 실행된 시각은 2025.05.24 14:59이고 가장 최근 실행된 시각은 2025.05.24 17:55이다. 또한 프로그램 누적 실행 횟수는 17회인 것을 알 수 있다.



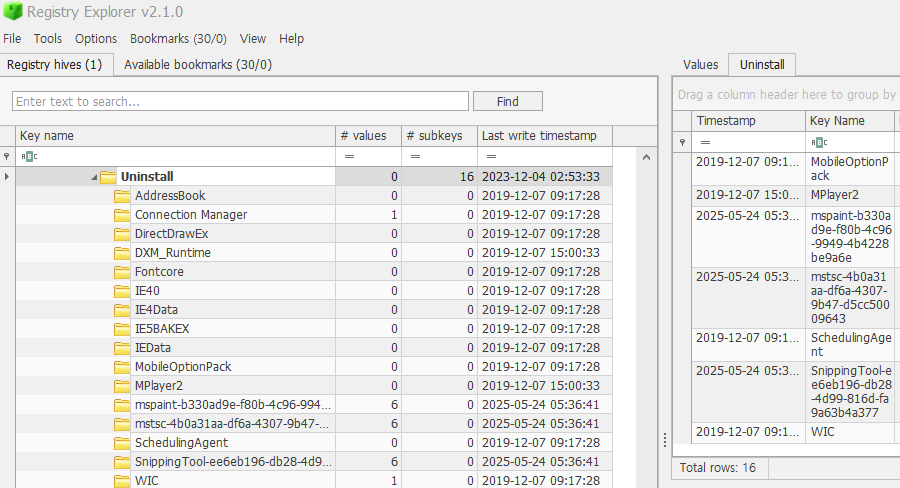
[그림3. 디스코드 프리패치 파일 확인]

1. 시스템 실행 시간
2. 경로: C:\Users\DISCORD-TEST PC\AppData\Roaming\discord\logs 내부의 discord\_utils.log 파일
3. 분석 내용: 해당 경로를 확인한 결과, 디스코드 모듈 총 3회가 실행되었으며, 정확한 시간은 14:59, 16:44, 17:15인 것을 확인할 수 있다.



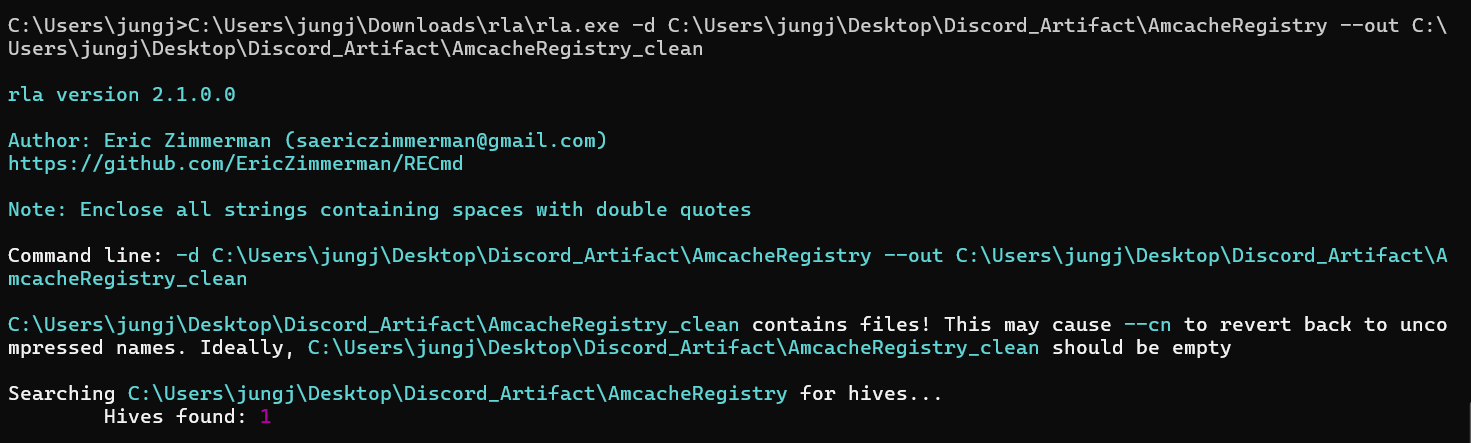
[그림4. 디스코드 실행 로그]

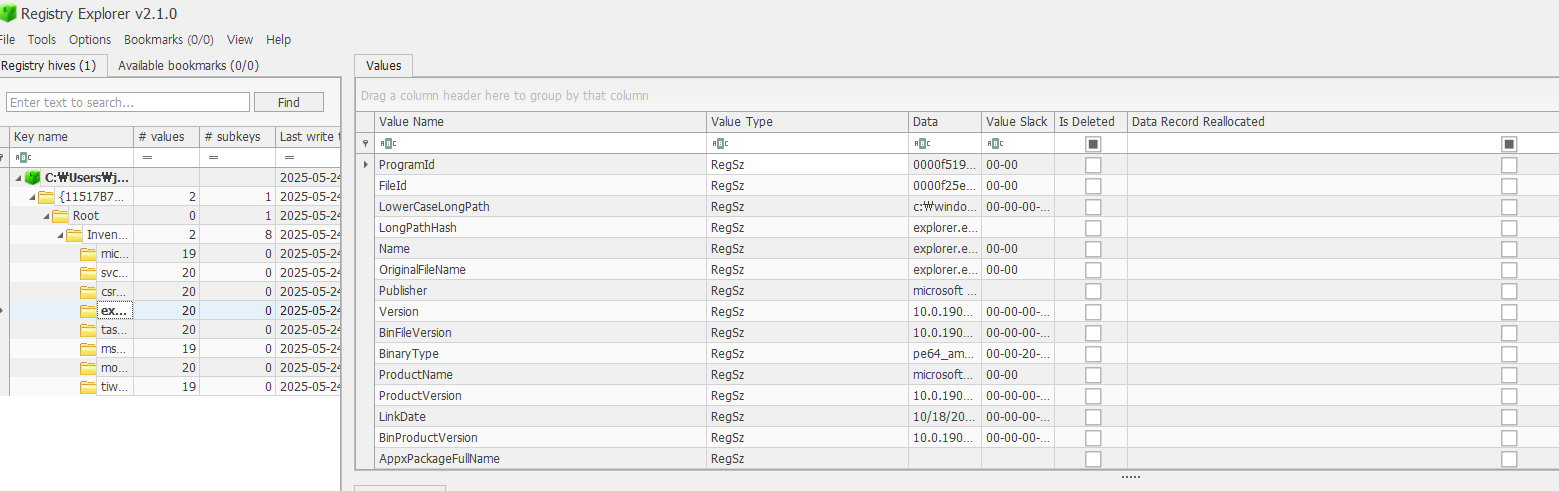
1. 소프트웨어 정보
2. 경로: C:\Windows\System32\config\SOFTWARE
3. 분석 내용: HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall 키 하위에 여러 프로그램이 설치되어 있지만, Discord와 관련된 키는 존재하지 않았다.



[그림5. Uninstall 폴더 내부]

1. Amcache.hve 정보
2. 경로: C:root\Windows\AppCompat\Programs\Amcache.hve, Amcache.hve.LOG1, Amcache.hve.LOG2
3. 분석 내용: 위 경로에 위치한 파일들을 clean 상태의 하이브로 만들어준 후 분석하였지만, Discord에 관한 정보는 추출되지 않았다.



[그림6. rla.exe 실행 터미널]

[그림7. Registry Explorer 분석 화면]

## 사용자 행위 아티팩트

1. 사용자 접근 기록
2. 경로: C:\Users\DISCORD-TEST PC\AppData\Roaming\Microsoft\Windows\Recent
3. 분석 내용: 사용자가 해당 파일에 접근한 시간을 바탕으로 사용자가 최근에 열어본 폴더나 이미지, 파일 접근 기록 등을 확인할 수 있다.



[그림8. Recent 파일에 위치한 흔적]

1. 방문 기록
2. 경로: C:\Users\DISCORD-TEST PC\AppData\Roaming\discord\logs\renderer\_js.log
3. 분석 내용:

① LoginSocket 정보를 통해서 16:48분에 디스코드 재접속을 위한 로그인 행위가 일어났다는 것을 확인할 수 있다.

|  |
| --- |
| [2025-05-24 16:48:54.776] [info] [LoginQRSocket] [144898ms] connected, handshaking with fingerprint: sHG-5TQGXrQaSj9-FRvohX1Fcmnt9ek1dVso-JLCjPI [2025-05-24 16:48:55.014] [info] [LoginQRSocket] [145137ms] computed nonce proof [2025-05-24 16:48:55.239] [info] [LoginQRSocket] [145362ms] handshake complete awaiting remote auth. |

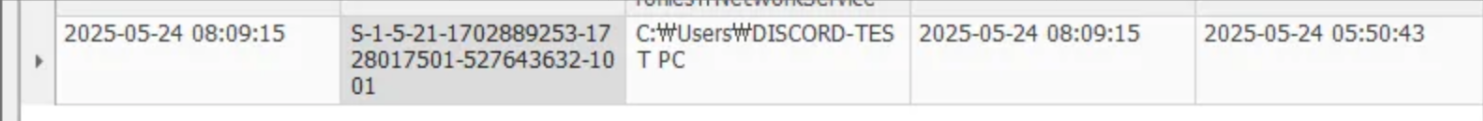
② handshake complete 로그를 통해서 해당 18:13분에 사용자가 디스코드를 종료한 로그를 확인할 수 있다.

|  |
| --- |
| [2025-05-24 18:13:41.723] [info] [LoginQRSocket] [12128ms] connected, handshaking with fingerprint: BXKJDwKulExA6ZQfPB3m70y5d\_1y5LA84YFh-8qQgtY [2025-05-24 18:13:41.960] [info] [LoginQRSocket] [12365ms] computed nonce proof [2025-05-24 18:13:42.159] [info] [LoginQRSocket] [12564ms] handshake complete awaiting remote auth. |

1. 계정 확인
2. 경로: HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList
3. 분석 내용: 레지스트리 ProfileList 경로에서 사용자 계정인 SID S-1-5-21-...-1001을 확인할 수 있고, 이는 C:\Users\DISCORD-TEST PC와 연결되는 것을 알 수 있다.

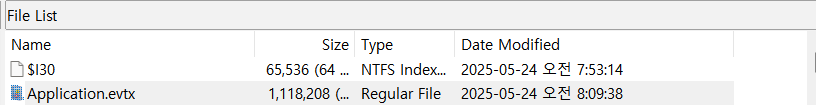
또한 해당 계정은 2025.05.24 17:50에 시스템에서 로그오프한 것으로 기록된다.

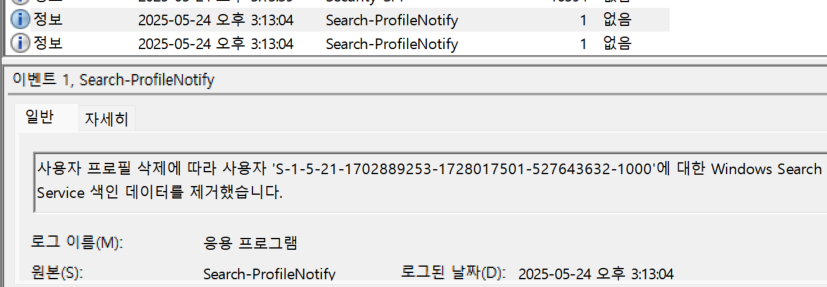
계정 이름은 직접적으로 명시되어 있지 않으며, SID를 통해 식별 가능하다.



[그림9. Registry Explorer 사용자 계정 정보]

1. 사용자 로그
2. 경로: C:\Windows\System32\winevt\Logs\Application.evtx
3. 분석 내용: 사용자 계정의 프로필이 삭제될 때 발생하는 로그를 확인할 수 있다. 또한 해당 SID(보안 식별자)의 검색 색인, 캐시, 임시 설정 등 사용자 기반 데이터가 삭제됨을 알 수 있다.





[그림10. Event View를 사용한 사용자 계정 삭제 로그]

## 파일 사용/조작 아티팩트

1. DB 파일 조작 및 수정
2. 경로:

① MFT (Master File Table) : C:\<root>\$MFT

② USN Journal : C:\<root>\$Extend\$UsnJrnl

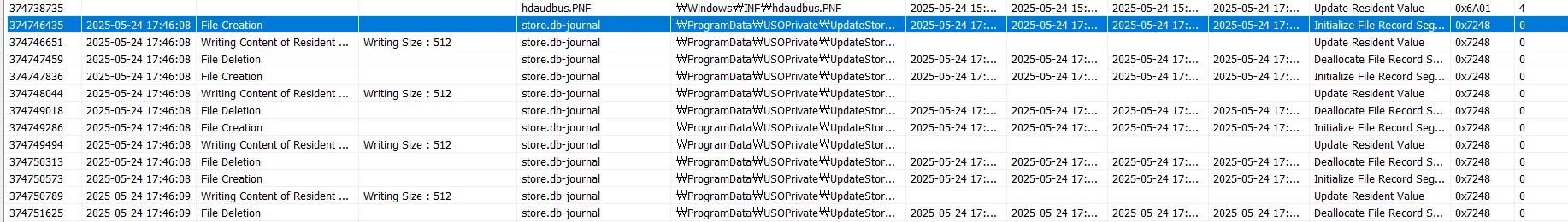
③ NTFS 로그 파일 : C:\<root>\$LogFile

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



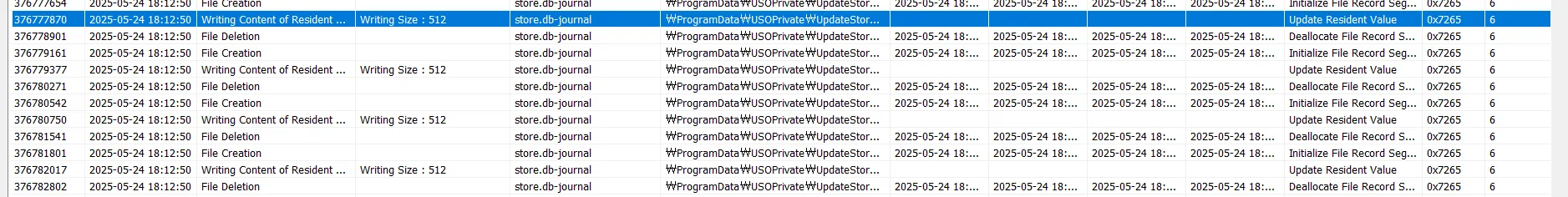
[그림11. NTFS Log Tracker로 파일 사용 및 조작 로그 확인]

① 17:46에 db-journal에서의 파일 삭제와 생성 이벤트가 일어났다는 점을 통해서 해당 시간에 사용자에 대한 db정보가 수정되었음을 알 수 있다.



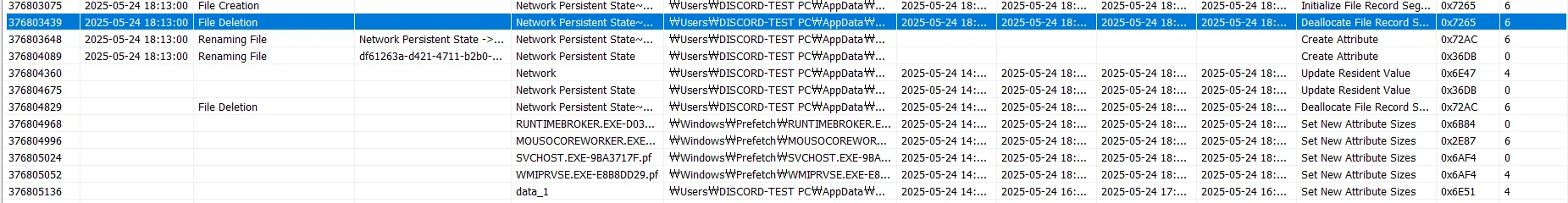
[그림12. ’사용자 ‘정지윤’ 차단]

② 18:12에 db-journal에서의 파일 삭제와 생성 이벤트가 일어났다는 점을 통해서 18:12에 jimin이라는 사용자에 대한 db정보가 수정되었음을 유추할 수 있다.



[그림13. ’jimin’ 친구 차단]

③ 위의 정보를 통해서 Discord의 로컬 네트워크 상태 db-journal에서의 파일 삭제가 일어났다는 점을 알 수 있고, 이는 18:13에 Alice 계정 삭제의 시간과 부합하기 때문에 해당 계정의 삭제 정보임을 유추할 수 있다.



[그림14. Alice 계정 삭제]

④ 사용자의 계정 정보에 관련된 정보가 store.db에 저장됨을 알 수 있어, store.db 파일의 덤프를 생성한 후 해당 파일의 schema와 data에서 공급자 정보, GUID 정보, 타임스탬프, 이벤트 로그, 이벤트 성공 여부 등을 확인할 수 있었다.

|  |
| --- |
| -- Schema: UPDATESPROP --- CREATE TABLE UPDATESPROP ( PROVIDERID TEXT NOT NULL COLLATE NOCASE CHECK(PROVIDERID <> ''), UPDATEID TEXT NOT NULL COLLATE NOCASE CHECK(UPDATEID <> ''), VARIABLE TEXT NOT NULL COLLATE NOCASE CHECK(VARIABLE <> ''), VALUE TEXT, TYPE INTEGER, PRIMARY KEY(PROVIDERID, UPDATEID, VARIABLE) FOREIGN KEY(PROVIDERID, UPDATEID) REFERENCES UPDATES(PROVIDERID, UPDATEID) ON DELETE CASCADE); --- Data: UPDATESPROP --- ('LegacyUOProvider', 'ia133925411000567998', 'CorrelationVector', 'TCY3wFnxukq5MAN8.0', 4) ('LegacyUOProvider', 'ia133925411000567998', 'DiscoveryTime', '1748067502993', 3) ('LegacyUOProvider', 'ia133925411000567998', 'QueueNumber', '1', 2) ('WuProvider', '3f7f91a3-b4ac-4823-8050-046a7743f4e9:200', 'DiscoveryTime', '1748074789355', 3) ('WuProvider', '3f7f91a3-b4ac-4823-8050-046a7743f4e9:200', 'QueueNumber', '2', 2) ('WuProvider', '6500af43-533e-41f8-8413-f70648777d13:201', 'DiscoveryTime', '1748074789503', 3) ('WuProvider', '6500af43-533e-41f8-8413-f70648777d13:201', 'QueueNumber', '3', 2) ('WuProvider', '478e0fe9-52e9-4ebd-b70a-bbb0462a2e54:200', 'DiscoveryTime', '1748074789665', 3) |

## 메모리 아티팩트

1. 파일 분석
2. 분석 내용: 디스코드를 통해 다운로드 받은 PDF 파일과 PNG 파일 확인할 수 있다.



[그림15. Volatility3으로 확인한 파일분석]

1. 행위 분석
2. 분석 내용:

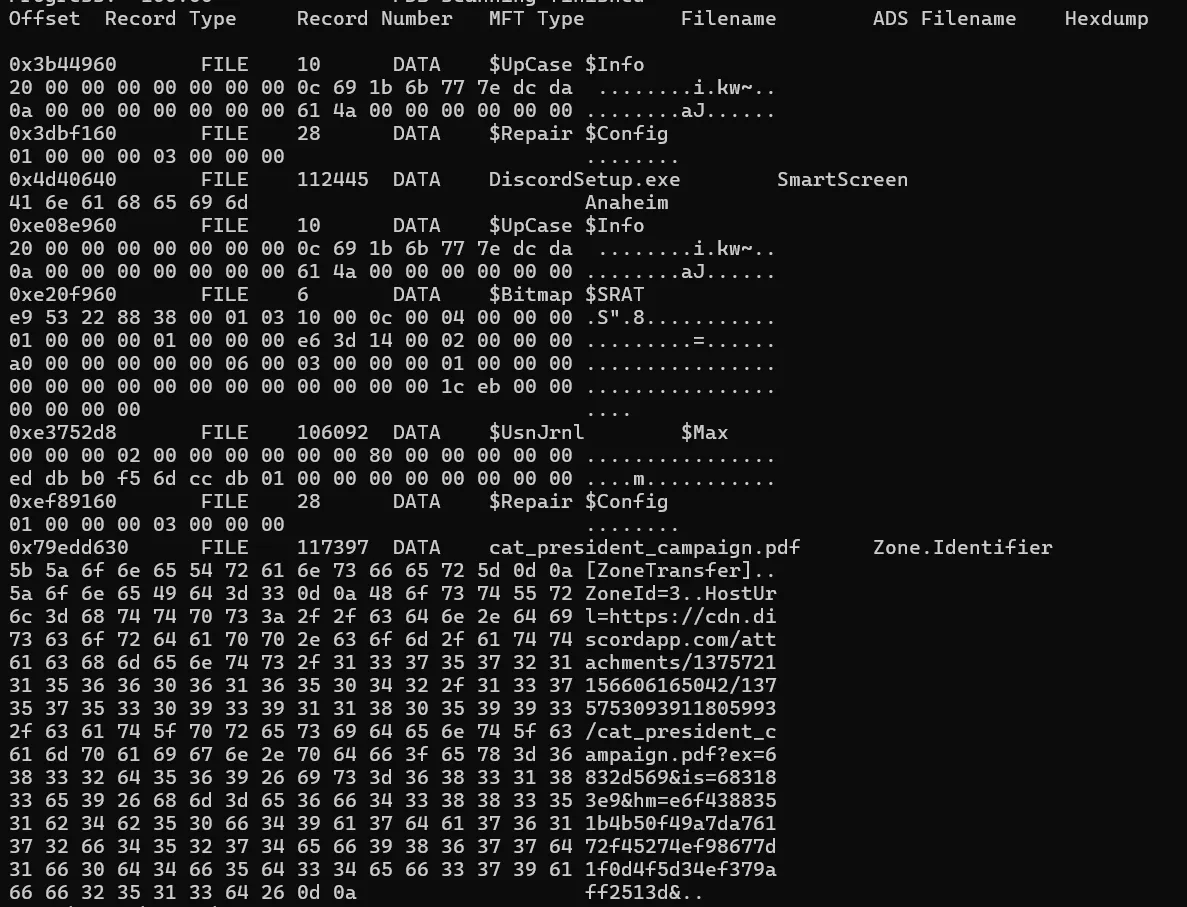
① python [vol.py](http://vol.py/) -f discord.vmem windows.mftscan.ADS 명령어를 통해 확인할 수 있다.

② DiscordSetup.exe가 시스템 내에 존재한다. (사용자가 디스코드 다운로드)

③ SmartScreen이나 Anaheim은 Microsoft SmartScreen 필터와 브라우저 캐시 관련 정보로 보인다.

④ Discord를 통해 cat\_president\_campaign.pdf 다음과 같은 파일을 다운로드 한다.

* ZoneID = 3 : 외부 인터넷에서 다운로드된 파일이다.
* HostUrl : 디스코드의 CDN 을 통해 첨부파일 다운로드, 실제 디스코드 대화방에서 공유된 파일임을 나타낸다.



[그림16. Volatility3으로 확인한 행위 분석]

## 네트워크 아티팩트

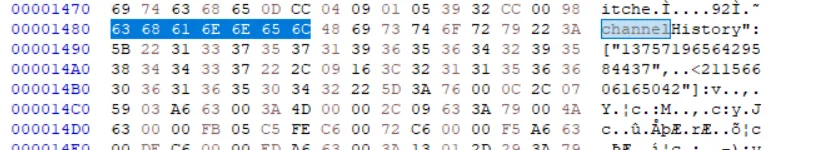
1. 방문 기록
2. 경로: C:\Users\DISCORD-TEST PC\AppData\Roaming\discord\LocalStorage\leveldb\000007.ldb
3. 분석 내용:

① 분석 방법 1: FTK Imager를 통해 채널 ID를 확인할 수 있다.

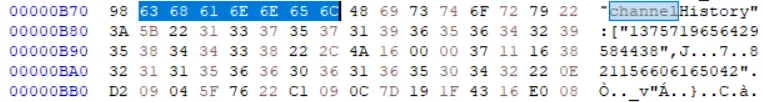


[그림17. FTK Imager로 확인한 channel History값]

② 분석 방법 2: HxD를 통해서 채널 ID를 확인할 수 있다.



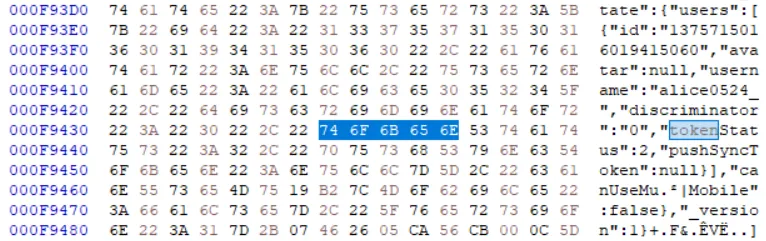
[그림18. HxD로 확인한 channelHistory]

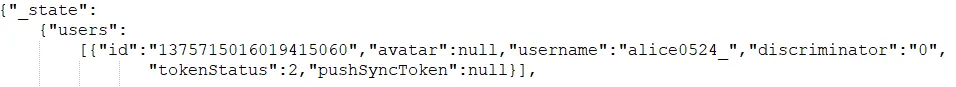


[그림19. HxD로 확인한 channelHistory]

위 두 분석으로 ["1375719656429584437"], [”1375719656429584438”] 값 확인이 가능하다.

1. 세션 토큰
2. 경로: C:\Users\DISCORD-TEST-PC\AppData\Roaming\discord\LocalStorage\leveldb
3. 분석 내용: 토큰과 연관된 캐시 내용을 확인할 수 있다.

[그림20. HxD로 확인한 Token 값]

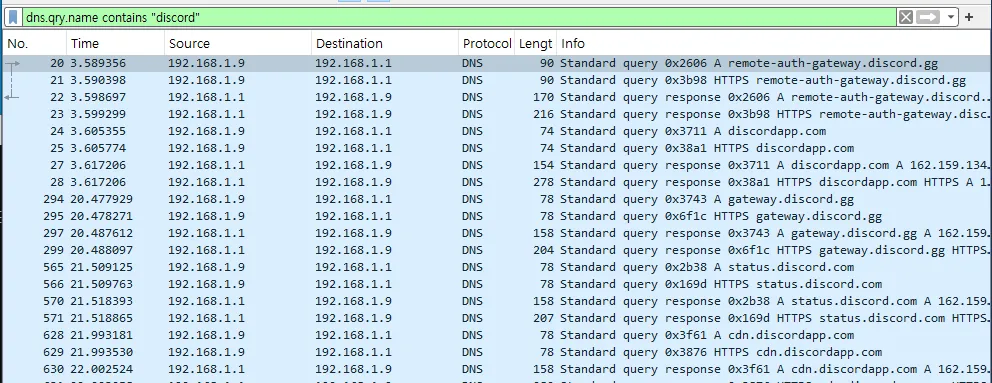


[그림21. Notepad++로 확인한 Token 값]

|  |  |
| --- | --- |
| **키** | **설명** |
| “id : 1375715016019415060” | Discord 사용자의 고유 ID |
| "username : alice0524\_” | 사용자 이름으로, 디스코드 조작 시 설정한 ID와 일치 |
| "discriminator” | Discord가 2023년부터 새롭게 도입한 ‘고유 사용자명’ 구조 적용됨 |
| "tokenStatus": 2 | Discord가 내부적으로 로그인 상태를 유지하고 있다는 의미 (2 = active) |
| "pushSyncToken": null | 푸시 알림용 토큰 비활성화 상태 |

[표4. 세션 토큰 키 정보]

1. 네트워크 연결
2. 분석 내용: DNS 패킷 분석 결과, 사용자 시스템에서 다음과 같은 Discord 관련 도메인에 대한 요청이 순차적으로 발생한다.

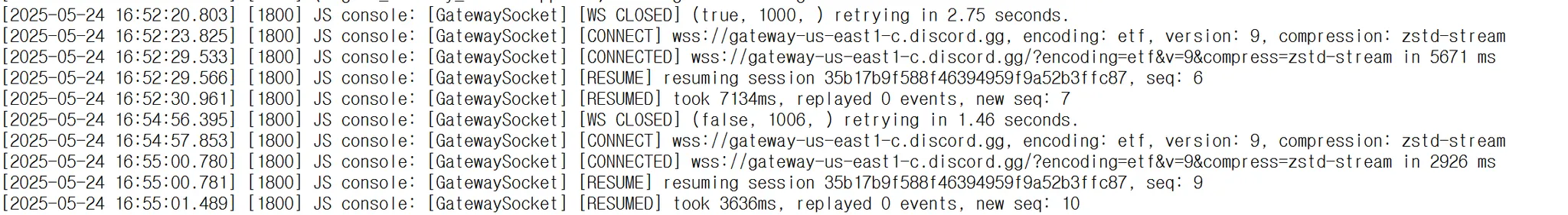


[그림22. Wireshark로 확인한 Discord DNS 패킷 결과]

|  |  |
| --- | --- |
| **도메인** | **용도** |
| remote-auth-gateway.discord.gg | 디바이스 로그인 인증 인증 세션을 처리하는 도메인 |
| discordapp.com | 설치형 앱 및 웹 앱의 공통 엔트리 도메인 |
| gateway.discord.gg | WebSocket 실시간 메시지 연결용 |
| status.discord.com | Cloudflare에 연결된 상태 모니터링 전용 도메인 |
| cdn.discordapp.com | 이미지, 파일 등 콘텐츠 리소스 제공 |

[표5. DNS 패킷 결과 도메인 값 설명]

1. 네트워크 로그
2. 경로: C:\Users\DISCORD-TEST PC\AppData\Roaming\discord\logs
3. 분석 내용: 실제 Discord의 미국 동부 서버 주소의 웹소켓 프로토콜을 사용하는 것을 확인할 수 있다.



[그림23. FTK Imager로 확인한 네트워크 log기록]

|  |  |  |
| --- | --- | --- |
| **시각** | **이벤트** | **설명** |
| 16:52:20.803 | [WS CLOSED] | 기존 연결 종료 |
| 16:52:23.825 | [CONNECT] | 새로운 서버(gateway-us-east1-c.discord.gg)에 연결 시도 |
| 16:52:29.533 | [CONNECTED] | WebSocket 연결 완료 (5671ms 걸림) |
| 16:52:29.566 | [RESUME] | 기존 세션(35b17b9f...) 이어받기 시도 |
| 16:52:30.961 | [RESUMED] | 세션 복구 성공 (7134ms 걸림, 이벤트 재생 0개) |

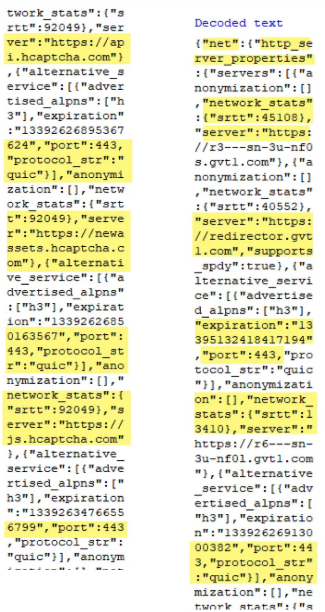
[표6. 네트워크 log 기록 설명]

1. 쿠키 정보
2. 경로: C:\Users\DISCORD-TEST-PC\AppData\Roaming\discord\Network\Cookies
3. 분석 내용: cf\_bmhp8…등 과 같은 고유 세션 키와 cloudflare bot management 쿠키를 확인할 수 있다.



[그림24. HxD로 분석한 도메인 및 세션키]

1. 서버 연결 정보
2. 경로: C:\Users\DISCORD-TEST-PC\AppData\Roaming\discord\Network\Network Persistent State
3. 분석 내용: 사용 프로토콜과 시간 등을 확인할 수 있다.



[그림25. HxD로 분석한 서버 연결 정보]

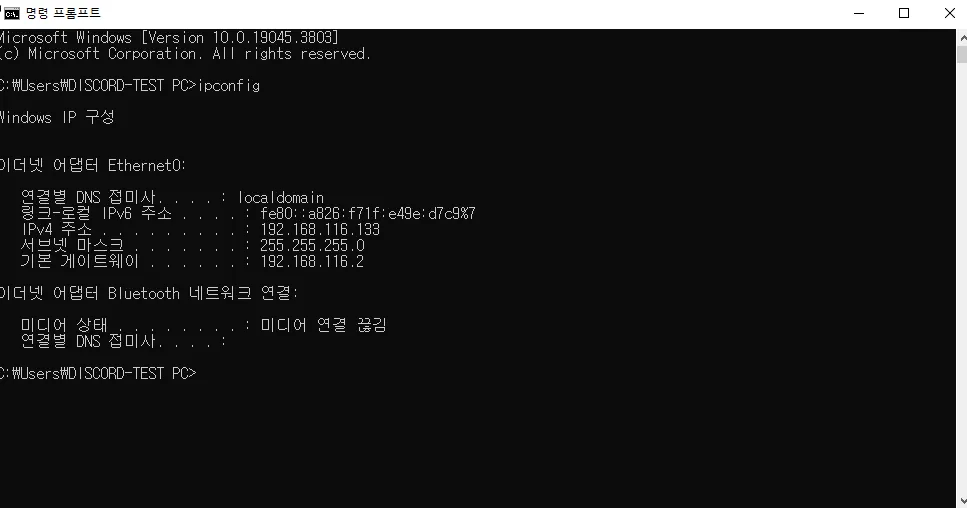
|  |  |
| --- | --- |
| **키** | **설명** |
| "net":{"http\_server\_properties":{"servers":[{...}]}} | 브라우저나 애플리케이션이 최근 연결한 서버, 사용한 프로토콜, 네트워크 응답 시간 등 |
| “protocol\_str" : "quic" | 연결방식, 대부분의 서버가 quic 프로토콜 사용 |
| “port” : 443 | 모든 서버는 443 포트 사용 → HTTPS 통신 |
| “network\_stats” : {”srtt” : 40552} | 네트워크 지연 시간 |

[표7. 서버 연결 정보 키 설명]

1. 사용자 디바이스 IP 정보
2. 경로: C:\Users\DISCORD-TEST PC\AppData\Roaming\discord\Network\Network Persistent State
3. 분석 내용:

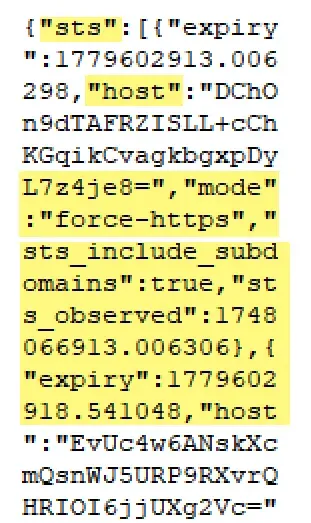
① 실행 디바이스의 IP와 Network Persistent State의 IP를 비교한 결과, IP가 일치했으며 이는 즉, Discord가 192.168.116.133에서 실행된 것을 확인할 수 있다.

[그림26. HxD로 추출한 디바이스 IP 주소]



[그림27. Discord 실행 VMware IP]

1. HSTS 정책 정보
2. 경로: C:\Users\DISCORD-TEST-PC\AppData\Roaming\discord\Network\TransportSecurity
3. 분석 내용:



[그림28. HxD로 추출한 HSTS 정책 캐시 정보]

|  |  |
| --- | --- |
| **키** | **설명** |
| host | HSTS 정책이 적용된 호스트 |
| mode : force-https | 이 호스트와는 반드시 HTTPS로만 통신 |
| sts\_include\_subdomains | true : 하위 도메인도 HTTPS만 허용 |
| sts\_observed | 클라이언트가 이걸 처음 확인한 시간 |
| expiry | 만료 시간 |

[표8. HSTS 정책 캐시 정보]

## 메신저 아티팩트

1. 서버 및 채널 이동
2. 경로: C:\Users\DISCORD-TEST PC\AppData\Roaming\discord\logs\renders\_js.log
3. 분석 내용: 15:25에 사용자가 특정 서버(1375719655884198029)와 채널(1375719656429584437)로 이동했음을 나타낸다.

|  |
| --- |
| [2025-05-24 15:25:45.553] [info] [Routing/Utils] transitionTo - Transitioning to /channels/1375719655884198029/1375719656429584437 [2025-05-24 15:25:45.561] [info] [MessageActionCreators] Fetching messages for 1375719656429584437 between undefined and undefined. jump={"jumpType":"ANIMATED"} [2025-05-24 15:25:45.892] [info] [MessageActionCreators] Fetched 2 messages for 1375719656429584437 isBefore:false isAfter:false [2025-05-24 15:25:45.894] [info] [ChannelMessages] loadComplete: resetting state for channelId=1375719656429584437, sending.length=0 |

1. 메시지 전송
2. 경로: C:\Users\DISCORD-TEST PC\AppData\Roaming\discord\logs\renders\_js.log
3. 분석 내용: 메시지 전송 타임스탬프를 확인할 수 있다.

|  |  |
| --- | --- |
| **Date** | **LogId** |
| 25.05.24 16:06 | 5059 |
| 25.05.24 16:07 | 6124 |
| 25.05.24 16:08 | 7357 |
| 25.05.24 16:09 | 6124 |
| 25.05.24 16:11 | 7778 |
| 25.05.24 16:15 | 2945 |
| 25.05.24 16:17 | 3614 |
| 25.05.24 16:18 | 3237 |
| 25.05.24 16:18 | 7508 |
| 25.05.24 16:19 | 3874 |
| 25.05.24 16:20 | 367 |
| 25.05.24 16:20 | 1261 |
| 25.05.24 17:57 | 5560 |
| 25.05.24 17:58 | 2256 |
| 25.05.24 17:58 | 7185 |
| 25.05.24 17:58 | 8187 |
| 25.05.24 17:58 | 4473 |
| 25.05.24 17:58 | 6514 |

[표9. 메시지 타임 스탬프]

1. 파일 전송
2. 경로: C:\Users\DISCORD-TEST PC\AppData\Roaming\discord\logs\renders\_js.log
3. 분석 내용:

① 25.05.24 17:55 사용자가 CloudUpload.tsx, UploaderBase.tsx와 같은 업로드 모듈을 사용하여 18738 bytes 크기의 파일 1개를 서버에 업로드(전송)했다. 다운로드 경로에서 크기가 동일한 파일을 발견했으며, 해당 파일(cat\_president\_campaign.pdf)을 전송한 것으로 추정한다.

|  |
| --- |
| [2025-05-24 17:55:36.456] [info] [CloudUpload.tsx] Requesting upload url for upload10 [2025-05-24 17:55:36.936] [info] [CloudUpload.tsx] Uploading upload10 [2025-05-24 17:55:38.640] [info] [CloudUploaderBase.tsx] setUploadingTextForUI - total content: 18738 bytes and 1 attachments for Uploader12 [2025-05-24 17:55:39.887] [info] [CloudUpload.tsx] Upload complete for upload10 [2025-05-24 17:55:40.404] [info] [UploaderBase.tsx] \_handleComplete for Uploader12 |

② 25.05.24 17:57 사용자가 위와 같은 모듈을 사용하여 1001 bytes 크기의 파일 1개를 서버에 업로드(전송)했다. 임시 파일의 형태로 다운로드 경로에서 발견했으며, 해당 파일(확인되지 않음 188328.crdownload)을 전송한 것으로 추정한다.



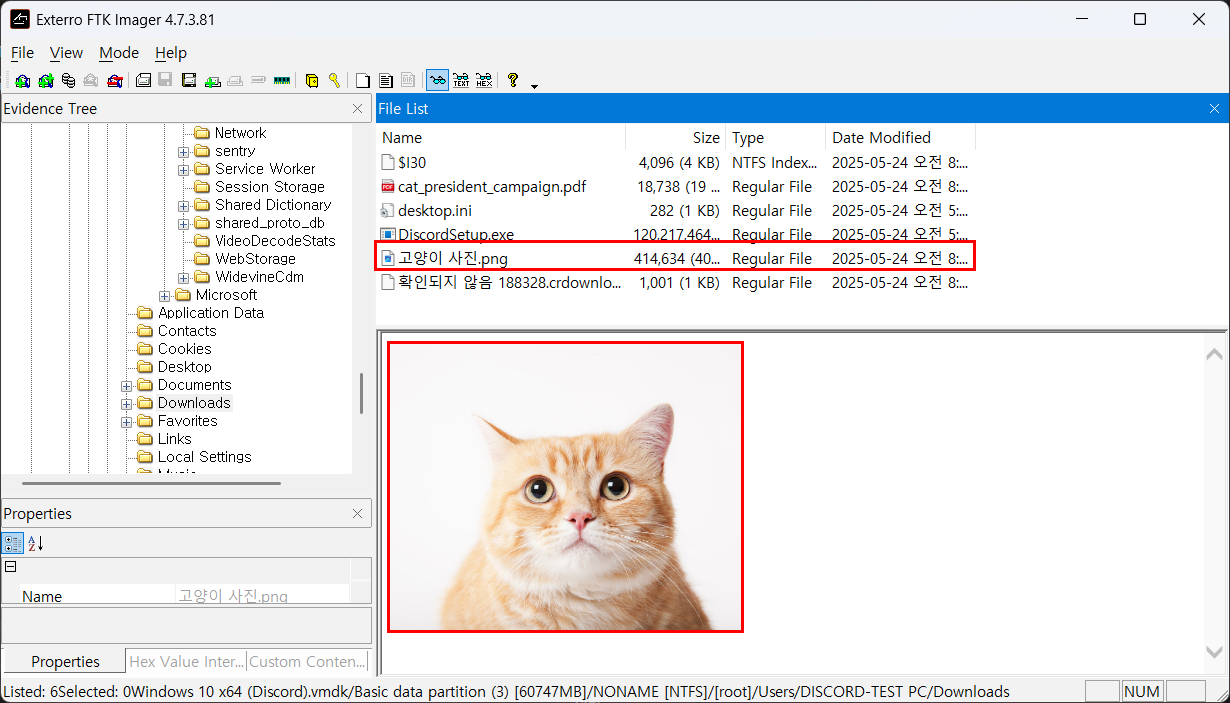
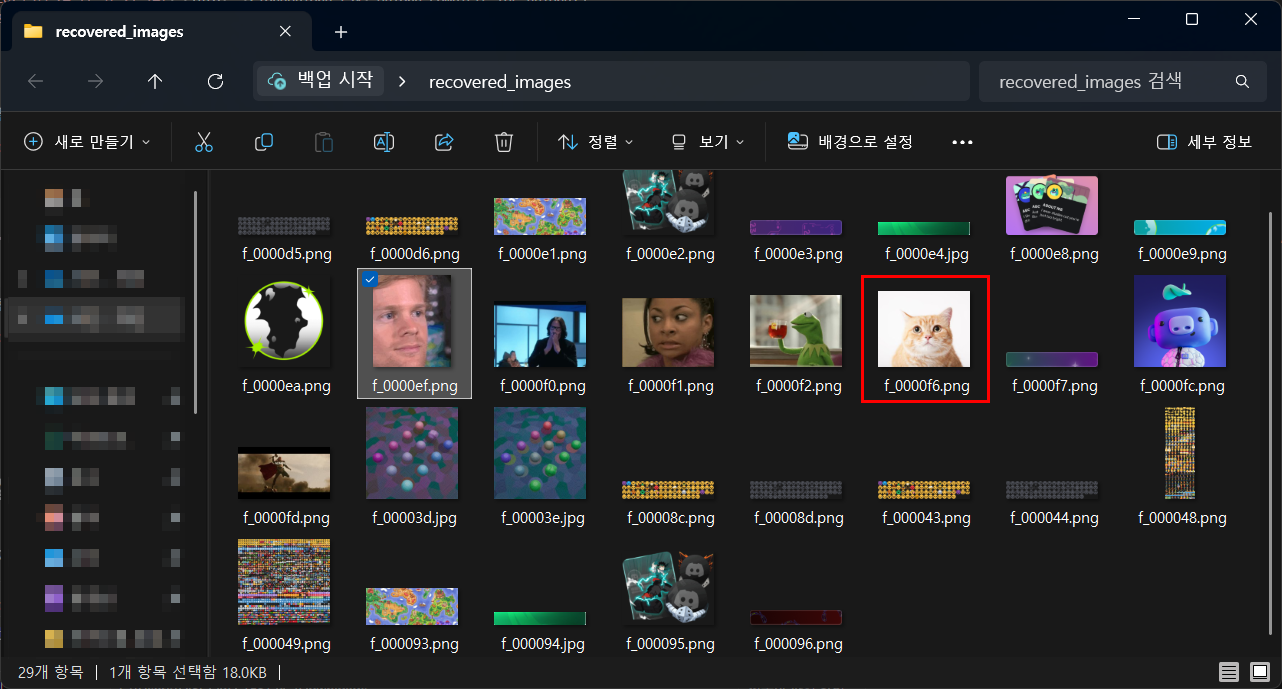
[그림29. 임시 파일로 위장한 명령 실행 cat\_president.ps1 파일]

|  |
| --- |
| [2025-05-24 17:57:23.900] [info] [CloudUpload.tsx] Requesting upload url for upload15 [2025-05-24 17:57:24.338] [info] [CloudUpload.tsx] Uploading upload15 [2025-05-24 17:57:25.925] [info] [CloudUploaderBase.tsx] setUploadingTextForUI - total content: 1001 bytes and 1 attachments for Uploader17 [2025-05-24 17:57:27.147] [info] [CloudUpload.tsx] Upload complete for upload15 [2025-05-24 17:57:27.775] [info] [UploaderBase.tsx] \_handleComplete for Uploader17 |

1. 프로필 (로그인 정보)
2. 경로: C:\Users\DISCORD-TEST PC\AppData\Roaming\discord\LocalStorage\ 내부의 000005.ldb 파일
3. 분석 내용: 최근 로그인한 사용자 정보를 확인할 수 있다.

사용자 이름(username)은 “alice0524”이며, 아이디(id)는 “1375715016019415060”이다.

1. 섬네일 정보
2. 경로: C:\Users\DISCORD-TEST PC\AppData\Roaming\discord\Cache\Cache\_Data
3. 분석 내용: 캐시 파일 이미지 복구와 다운로드 경로의 중복 사진을 발견했으며, 이 사진을 프로필 변경에 사용한 사진으로 추정한다.



[그림30, 31. 캐시 파일 이미지 복구 폴더와 다운로드 경로의 사진]

# 분석 요약

|  |  |  |
| --- | --- | --- |
| 아티팩트 유형 | 경로 | 설명 |
| 시스템 설치/실행 아티팩트 | C:\Users\DISCORD-TEST PC\AppData\Local\Discord\ | 설치 정보 확인 가능 |
| C:\Windows\Prefetch\DISCORD.EXE-283A1D96.pf | 프리패치 파일 확인 가능 |
| C:\Users\DISCORD-TEST PC\AppData\Roaming\discord\logs | 시스템 실행 시간 확인 가능 |
| C:\Windows\System32\config\SOFTWARE | 소프트웨어 정보 확인 가능 |
| C:root\Windows\AppCompat\Programs\Amcache.hve, Amcache.hve.LOG1, Amcache.hve.LOG2 | Amcache.hve 정보 확인 가능 |
| 사용자 행위 아티팩트 | C:\Users\DISCORD-TEST PC\AppData\Roaming\Microsoft\Windows\Recent | 사용자 접근 기록 확인 가능 |
| C:\Users\DISCORD-TEST PC\AppData\Roaming\discord\logs\renderer\_js.log | 방문 기록 확인 가능 |
| HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList | 계정 확인 가능 |
| C:\Windows\System32\winevt\Logs\Application.evtx | 사용자 로그 확인 가능 |
| 파일 사용/조작 아티팩트 | C:\<root>\$MFT | MFT 확인 가능 |
| C:\<root>\$Extend\$UsnJrnl | USN Journal 확인 가능 |
| C:\<root>\$LogFile | NTFS 로그 파일 정보 확인 가능 |
| 네트워크 아티팩트 | C:\Users\DISCORD-TEST PC\AppData\Roaming\discord\LocalStorage\leveldb | 방문 기록 정보 확인 가능 |
| C:\Users\DISCORD-TEST-PC\AppData\Roaming\discord\LocalStorage\leveldb | 세션 토큰 정보 확인 가능 |
| C:\Users\DISCORD-TEST PC\AppData\Roaming\discord\logs\ | 네트워크 로그 정보 확인 가능 |
| C:\Users\DISCORD-TEST-PC\AppData\Roaming\discord\Network\Cookies | 쿠키 정보 확인 가능 |
| C:\Users\DISCORD-TEST-PC\AppData\Roaming\discord\Network\Network Persistent State | 서버 연결 정보 확인 가능 |
| C:\Users\DISCORD-TEST PC\AppData\Roaming\discord\Network\Network Persistent State | Discord의 실행 디바이스 IP 확인 |
| C:\Users\DISCORD-TEST-PC\AppData\Roaming\discord\Network\TransportSecurity | HSTS 정책 정보 확인 가능 |
| 메신저 아티팩트 | C:\Users\DISCORD-TEST PC\AppData\Roaming\discord\Cache\Cache\_Data | 사용자 썸네일 확인 가능 |
| C:\Users\DISCORD-TEST PC\AppData\Roaming\discord\logs\renders\_js.log | 서버 정보 및 채널 이동 정보 확인 가능 |
| C:\Users\DISCORD-TEST PC\AppData\Roaming\discord\logs\renders\_js.log | 메세지 전송 시간(타임스탬프) 확인 가능 |
| C:\Users\DISCORD-TEST PC\AppData\Roaming\discord\logs\renders\_js.log / C:\Users\DISCORD-TEST PC\Downloads | 전송한 파일(다운로드) 확인 가능 |
| C:\Users\DISCORD-TEST PC\AppData\Roaming\discord\LocalStorage\ 내부의 000005.ldb 파일 | 유저 정보 확인 가능 |

[표10. 아티팩트 분석 요약표]

# 참고 문헌

[1] 신수민, 박은후, 김소람, 김종성, 「디지털 포렌식 관점에서의 Slack 및 Discord 메신저 아티팩트 분석」, 디지털콘텐츠학회논문지 제21권 제4호, 2020.4, 799-809.

[2] Michał Motyliński, Áine MacDermott, Farkhund Iqbal, Mohammed Hussain, Saiqa Aleem,「Digital Forensic Acquisition and Analysis of Discord Applications」, 2020 International Conference on Communications, Computing, Cybersecurity, and Informatics (CCCI), 2020.11.

[3] Farkhund Iqbal, Michał Motyliński, Áine MacDermott,「Discord Server Forensics: Analysis and Extraction of Digital Evidence」, 2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS), 2021.5.

[4] Kyle Moffitt, Umit Karabiyik, Shinelle Hutchinson, Yung Han Yoon,「 Discord Forensics: The Logs Keep Growing」, 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC), 2021.1.

[5] Muhammad Koprawi, Fadhli Dzil Ikram「Forensic analysis on discord application using the National Institute of Standards and Technology (NIST) Method」, Jurnal Mandiri IT Vol. 12 No. 1 (2023): July: Computer Science and Field, 2023.8.

[6] Khushi Gupta, Phani Lanka, Cihan Varol,「A holistic digital forensic analysis of Discord – Storage, memory, and network perspectives」, Journal of Forensic Sciences: Volume 69, Issue 4, 2024.6, 1320-1333.

# 부록

## store.db 파일 분석

1. 경로: C:\Users\jungj\Desktop\Discord\_Artifact python dump\_sqlite.py
2. 분석 내용:

① 계정과 관련된 정보가 store.db에 저장되어 있음을 확인하고, 해당 파일의 덤프를 생성하였다.

② dump\_sqlite.py 로 작성한 코드를 위 명령어로 실행시킨 결과, 아래와 같이 계정과 관련된 schema를 확인할 수 있었다.

③ 해당 schema에서는 공급자 정보, GUID 정보, 타임스탬프, 이벤트 로그, 이벤트 성공 여부를 확인할 수 있었다.

|  |
| --- |
| -- Schema: UPDATESPROP --- CREATE TABLE UPDATESPROP ( PROVIDERID TEXT NOT NULL COLLATE NOCASE CHECK(PROVIDERID <> ''), UPDATEID TEXT NOT NULL COLLATE NOCASE CHECK(UPDATEID <> ''), VARIABLE TEXT NOT NULL COLLATE NOCASE CHECK(VARIABLE <> ''), VALUE TEXT, TYPE INTEGER, PRIMARY KEY(PROVIDERID, UPDATEID, VARIABLE) FOREIGN KEY(PROVIDERID, UPDATEID) REFERENCES UPDATES(PROVIDERID, UPDATEID) ON DELETE CASCADE); --- Data: UPDATESPROP --- ('LegacyUOProvider', 'ia133925411000567998', 'CorrelationVector', 'TCY3wFnxukq5MAN8.0', 4) ('LegacyUOProvider', 'ia133925411000567998', 'DiscoveryTime', '1748067502993', 3) ('LegacyUOProvider', 'ia133925411000567998', 'QueueNumber', '1', 2) ('WuProvider', '3f7f91a3-b4ac-4823-8050-046a7743f4e9:200', 'DiscoveryTime', '1748074789355', 3) ('WuProvider', '3f7f91a3-b4ac-4823-8050-046a7743f4e9:200', 'QueueNumber', '2', 2) ('WuProvider', '6500af43-533e-41f8-8413-f70648777d13:201', 'DiscoveryTime', '1748074789503', 3) ('WuProvider', '6500af43-533e-41f8-8413-f70648777d13:201', 'QueueNumber', '3', 2) ('WuProvider', '478e0fe9-52e9-4ebd-b70a-bbb0462a2e54:200', 'DiscoveryTime', '1748074789665', 3) ('WuProvider', '478e0fe9-52e9-4ebd-b70a-bbb0462a2e54:200', 'QueueNumber', '4', 2) ('WuProvider', '6604cea4-ffa0-49ab-b56a-32abe156a2de:200', 'DiscoveryTime', '1748074789894', 3) ('WuProvider', '6604cea4-ffa0-49ab-b56a-32abe156a2de:200', 'QueueNumber', '5', 2) ('WuProvider', '4c344b38-fbe7-48e8-b755-1daf01c12fc0:200', 'DiscoveryTime', '1748074791527', 3) ('WuProvider', '4c344b38-fbe7-48e8-b755-1daf01c12fc0:200', 'QueueNumber', '6', 2) ('WuProvider', '657943f1-1efb-430a-a6c8-f77993103709:1', 'DiscoveryTime', '1748074793304', 3) ('WuProvider', '657943f1-1efb-430a-a6c8-f77993103709:1', 'QueueNumber', '7', 2) ('WuProvider', '0be073ee-34ba-432c-91c8-957a608d0e2f:1', 'CorrelationVector', 'gcDFX1xYvkWxid/m.0', 4) ('WuProvider', '0be073ee-34ba-432c-91c8-957a608d0e2f:1', 'DiscoveryTime', '1748074794644', 3) ('WuProvider', '0be073ee-34ba-432c-91c8-957a608d0e2f:1', 'QueueNumber', '8', 2) ('WuProvider', 'ac3d48b7-e65f-4a70-b314-10f67f00c768:1', 'DiscoveryTime', '1748074795542', 3) ('WuProvider', 'ac3d48b7-e65f-4a70-b314-10f67f00c768:1', 'QueueNumber', '9', 2) ('WuProvider', '6500af43-533e-41f8-8413-f70648777d13:201', 'CorrelationVector', 'gcDFX1xYvkWxid/m.1', 4) ('WuProvider', '478e0fe9-52e9-4ebd-b70a-bbb0462a2e54:200', 'CorrelationVector', 'gcDFX1xYvkWxid/m.1', 4) ('WuProvider', '6604cea4-ffa0-49ab-b56a-32abe156a2de:200', 'CorrelationVector', 'gcDFX1xYvkWxid/m.1', 4) ('WuProvider', '4c344b38-fbe7-48e8-b755-1daf01c12fc0:200', 'CorrelationVector', 'gcDFX1xYvkWxid/m.1', 4) ('WuProvider', '657943f1-1efb-430a-a6c8-f77993103709:1', 'CorrelationVector', 'gcDFX1xYvkWxid/m.1', 4) ('WuProvider', '0be073ee-34ba-432c-91c8-957a608d0e2f:1', 'AttentionRequiredReason', 'SeekerUpdate', 4) ('WuProvider', '0be073ee-34ba-432c-91c8-957a608d0e2f:1', 'AttentionRequiredReasonTime', '1748074803072', 3) ('WuProvider', 'ac3d48b7-e65f-4a70-b314-10f67f00c768:1', 'CorrelationVector', 'gcDFX1xYvkWxid/m.1', 4) ('WuProvider', '478e0fe9-52e9-4ebd-b70a-bbb0462a2e54:200', 'isIpu', '0', 0) ('WuProvider', '478e0fe9-52e9-4ebd-b70a-bbb0462a2e54:200', 'WorkBit', '0', 0) ('WuProvider', '657943f1-1efb-430a-a6c8-f77993103709:1', 'isIpu', '0', 0) ('WuProvider', '657943f1-1efb-430a-a6c8-f77993103709:1', 'WorkBit', '0', 0) ('WuProvider', '6500af43-533e-41f8-8413-f70648777d13:201', 'isIpu', '0', 0) ('WuProvider', '6500af43-533e-41f8-8413-f70648777d13:201', 'WorkBit', '0', 0) ('WuProvider', '6604cea4-ffa0-49ab-b56a-32abe156a2de:200', 'isIpu', '0', 0) ('WuProvider', '6604cea4-ffa0-49ab-b56a-32abe156a2de:200', 'WorkBit', '0', 0) ('WuProvider', '4c344b38-fbe7-48e8-b755-1daf01c12fc0:200', 'isIpu', '0', 0) ('WuProvider', '4c344b38-fbe7-48e8-b755-1daf01c12fc0:200', 'WorkBit', '0', 0) ('WuProvider', '3f7f91a3-b4ac-4823-8050-046a7743f4e9:200', 'isIpu', '0', 0) ('WuProvider', '3f7f91a3-b4ac-4823-8050-046a7743f4e9:200', 'CorrelationVector', 'gcDFX1xYvkWxid/m.2', 4) ('WuProvider', '3f7f91a3-b4ac-4823-8050-046a7743f4e9:200', 'WorkBit', '0', 0) ('WuProvider', '3f7f91a3-b4ac-4823-8050-046a7743f4e9:200', 'Approved', '0', 0) ('WuProvider', '3f7f91a3-b4ac-4823-8050-046a7743f4e9:200', 'OobeApproved', '0', 0) ('WuProvider', '3f7f91a3-b4ac-4823-8050-046a7743f4e9:200', 'CalledFromOobe', '0', 0) ('WuProvider', 'ac3d48b7-e65f-4a70-b314-10f67f00c768:1', 'isIpu', '0', 0) ('WuProvider', 'ac3d48b7-e65f-4a70-b314-10f67f00c768:1', 'WorkBit', '0', 0) |