



QR 로그인 아티팩트  
분석 (Telegram)

정지윤

명지대학교 해킹 동아리

# MJSEC

QR 로그인 악티팩트 분석  
(Telegram)

# 목차

---

1. 연구 배경
2. 연구 목적
3. 실험 환경 및 도구
4. 아티팩트 분석
5. 시나리오
6. 향후 연구 제시



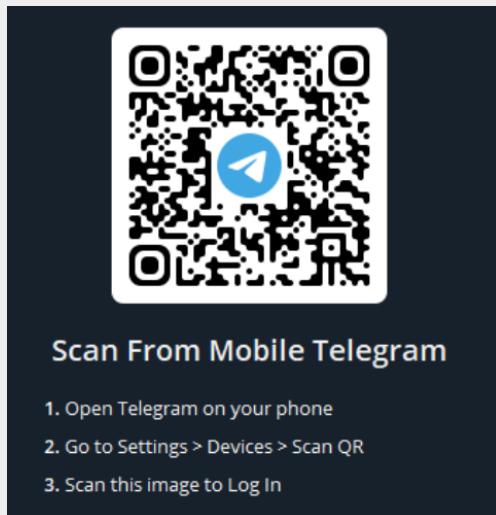
# 연구 배경

---

비밀번호 입력 없는 인증 방식의 보편화되며,  
데스크톱·웹 환경에서 QR 로그인 사용 증가



QR 로그인 여부에 따라 공격 시나리오·책임 주체·침해 경로가 달라져,  
단순 '로그인 성공'만으로는 사건 해석에 한계 존재



More often than not, the site looks pretty modest. The first page displays a message like "Sign in and vote" or "Free access to the trial version of Telegram Premium" – depending on the scheme in question. Next comes the messenger login screen. There are two variants here: those who opened the site on a desktop are prompted to log in using a QR code, while those on a mobile device are asked for their country and phone number. Sometimes (as shown in the screenshots) the attackers let the victim choose the more convenient option.



# 선행 연구

---

윈도우 환경에서 텔레그램 PC에 남은  
아티팩트를 전반적으로 분석한 연구



Forensic Science International: Digital Investigation  
Volume 40, Supplement, April 2022, 301342

DFRWS 2022 EU - Selected Papers of the Ninth Annual DFRWS Europe Conference

Extraction and analysis of retrievable memory artifacts from Windows Telegram Desktop application

Pedro Fernández-Álvarez, Ricardo J. Rodríguez  

Show more 

 Add to Mendeley  Share  Cite

QR 로그인이나 세션 토큰 하나만 확보해도, Telegram 클라우드 전체를 포렌식적으로 복원가능 하다는 연구

[Cloud Extractor](#) offers the ability to extract data from Telegram cloud using a phone number, QR code, or a token extracted from Android devices or found by [Oxygen Forensic® KeyScout](#) on PC. The evidence set will include:

- Authorization sessions
- Contacts
- Private and group chats
- Calls
- Channels data
- Polls



# 연구 목적

---

Telegram Desktop의 로컬 PC 아티팩트 분석  
을 통한 QR 로그인 흔적의 추적 가능성과  
구조적 한계 규명



# 실험 환경 및 도구

---

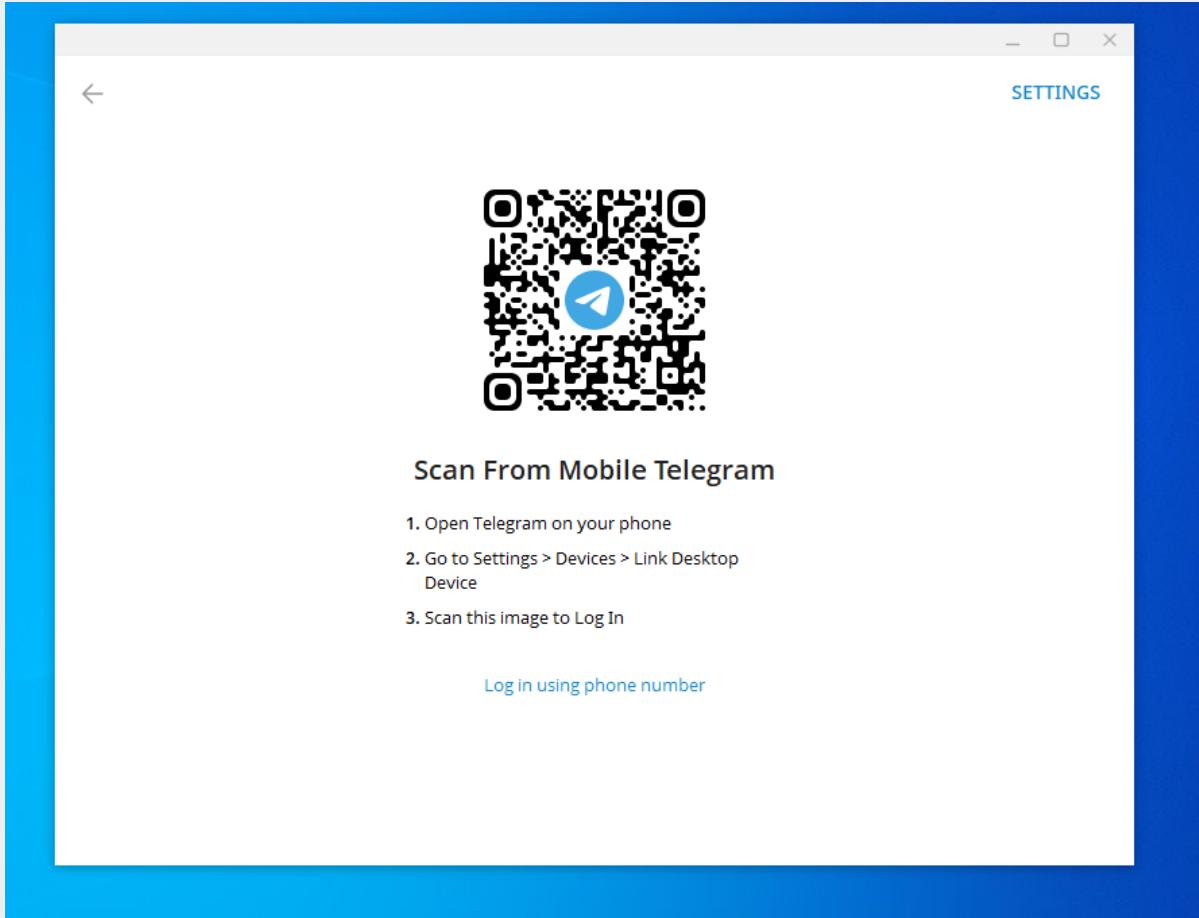
Program	Version	Function
VMWare workstation	17 pro	가상환경 구축 및 vmdk 추출
Windows	10 home	Windows 환경 구축
FTK Imager	4.7.3.81	디스크 이미지 및 파일 추출
Autopsy	4.22.1	아티팩트 분석 활용
HxD	2.5	바이너리 분석



# Telegram 로그인 구조

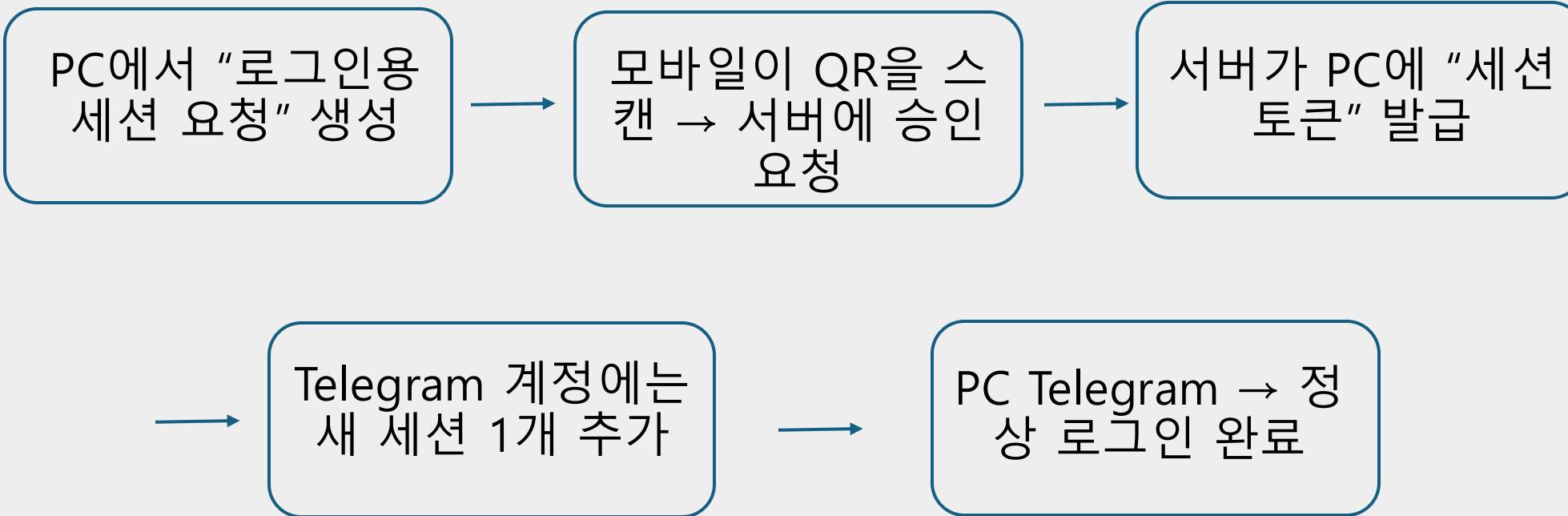
---

- 인증 코드 로그인
- QR 로그인  
(모바일 승인 기반)



# QR Login 방식

---



# 연구 필요성

---

Telegram은 MTProto 프로토콜 사용

## MTProto

: Telegram 내부에서 로그인·메시지·세션 통신을 암호화해서 전달하는 통신 프로토콜, 로그인 과정의 세부 방식은 숨기고, 통신 결과만 서버와 교환

로그인 방식은 **클라이언트 중심 구조**로 설계되어 있으며,  
서버 로그만으로는 로그인 수단(QR/비밀 번호 등)을 식별하기 어렵다.

=> 따라서 제시하는 아티팩트 분석 방법을 통하여 로그인 방법을 분석할 수 있다.

The screenshot shows a navigation bar with tabs: 홈 (Home), 자주묻는질문 (FAQ), 앱 (App), API, **프로토콜** (Protocol), and 스키마 (Schema). The '프로토콜' tab is underlined, indicating it is the active page. Below the tabs, the title 'MTProto Mobile Protocol' is displayed in bold. A blue vertical bar on the left contains the text: 'Please feel free to check out our [FAQ for the Technically Inclined](#). Client developers are required to comply with the [Security Guidelines](#)'.

<https://core.telegram.org/mtproto>



# 아티팩트 분석

- C:\Users\forensic\AppData\Roaming\Telegram Desktop\log.txt

본 로그에서는 401 SESSION\_REVOKED 오류가 확인되며,  
이는 해당 PC에 유효한 Telegram 세션이  
실제로 생성되었다가 이후 서버 측에서 철회되었음

```
[2026.01.10 21:47:31] App Error: Can't read history till unknown local message.  
[2026.01.10 21:47:53] RPC Error: request 121 got fail with code 401, error SESSION_REVOKED  
[2026.01.10 21:47:53] RPC Error in getDifference: 401 SESSION_REVOKED:  
[2026.01.10 21:48:21] Export Info: Destroy top bar by controller removal!
```

로그인 성공 → 세션 생성 의미



QR 코드를 스캔하여 텔레그램 데스크톱 혹은 텔레그램 웹에 연결하세요

▶▶▶ 데스크탑 기기 연결

이 기기

iPhone 16  
Telegram iOS 12.3.2  
Yongin-si, South Korea · 온라인

▶▶▶ 다른 세션 모두 종료

본 기기 밖의 모든 기기에서 로그아웃합니다.

모바일 기기에서 기기 연결 해제를 하였을 때  
있던 세션이 서버 측에서 무효화되었을 때 발생



# 아티팩트 분석

- C:\Users\forensic\AppData\Roaming\Telegram Desktop\data\s

Telegram Desktop은 로그인 성공 시에  
하나의 세션 파일이 아닌,  
여러 개의 암호화된 상태 컨테이너(.s 파일)를 생성

2026-01-10 오후 12:47:00			
2936D16393A135A6s	592,908 (58...)	Regular File	2026-01-10 오후 12:47:07
8B35F5D406432125s	140 (1 KB)	Regular File	2026-01-10 오후 12:49:00
A7FDF864FBC10B77s	348 (1 KB)	Regular File	2026-01-10 오후 12:47:18
countries	21,416 (21 ...)	Regular File	2026-01-10 오후 12:41:17
D877F783D5D3EF8Cs	876 (1 KB)	Regular File	2026-01-10 오후 12:48:58
key_datas	388 (1 KB)	Regular File	2026-01-10 오후 12:47:18

이 파일들은 내부 세션 상태를 분산 저장하기 위한 것으로,  
파일 내용 자체는 해석할 수 없지만  
key\_datas와 동일 시점에 생성·수정된다는 점에서  
실제 세션이 생성되었음을 입증하는 보조 자료

```
00000 | 54 44 46 24 21 9D 5B 00-00 09 0B F0 55 B2 34 AE | TDF$!-[...-8U^4@-aik] "u0-;j-3-00010 | 8C 9E 61 EC 4B 7D 22 75-30 9E 11 BF A1 80 33 9D | -aiK] "u0-;j-3-00020 | 23 00 79 69 97 9B 17 AB-16 09 31 1B 6A AA 3C AA | # yh-...<-1->^<-00030 | 42 26 95 9E AF E7 20 8E-3B FB D1 7C 78 47 7F 3L | Bz-_-ç-;ûñ|xç-100040 | 8C C5 D7 BD E3 4B 20 34-6E 27 6F 89 CB 50 A7 6F | Áx-áK 4n'ó-EP$ó00050 | F5 31 0F 6F 62 C9 C8 11-2A 64 77 9F C4 5B CC 41 | 61 -obÉÉ-xd-Á[IA00060 | 91 3B 4B 9C 99 E2 F0 01-90 F1 06 A1 C9 74 5B DF | ;M-ád-ñ-;É[800070 | 4E 6E AD 56 AF 4E 01 9F-F0 88 07 1E 10 51 23 B7 | Nn-VN-ð-...Q#00080 | E9 84 F1 50 4C A6 19 2B-09 70 DC 88 89 25 94 D3 | è-nPL!-+pÜ-...ó00090 | D2 38 8F 99 B2 74 10 85-61 E3 3E 44 D2 5B 8A A7 | 08-...t-áâDO]-S000A0 | B5 52 7F F5 23 86 07 57-63 32 9A 53 A4 E5 02 | qR-ô#-Wc2-SSñ-000B0 | 23 FC 93 0A 6B 27 EE 95-65 AA 97 34 6D E1 6E 12 | #u-ki'e^4mán-000C0 | 19 FC 3C EB BE 1C B5 41-C4 26 44 EE D4 AD 64 84 | û<ëµ-pâAäDiô-d-000D0 | 4D D3 27 95 10 18 CB 12-E7 A2 89 FD 92 E5 C3 OD | MÖ!...Èçç-y-åÄ-000E0 | 57 CE C4 5D 68 3F 85 8F-12 5F F3 C5 B9 CF C8 D8 | WlA]h-...ôA-íÀö000F0 | 5A BA D1 8F 2C 08 8C 51-8E 60 F6 D6 28 50 FC 8F | ZñN-, -Q-ôô(Pü-00100 | 88 5F 98 B5 CE DA 7D 66-B6 DC AD 31 16 1E 0E C5 | _-ùIÜ)fçÜ-1- Á-00110 | 7C 78 D6 E5 86 16 47 10-D8 30 9E 89 F2 AD BC CF | [xôA-G-00-ô-ñí-00120 | 32 AE 5B 8B 40 52 02 1D-88 EC 52 18 9F 58 13 6C | 2e[...ØR-...IR-X-100130 | D8 A5 9D 0D 86 12 E9 7A-E6 D2 54 13 A1 FF 12 C0 | ØY-...ézaÔt;ý-å00140 | DA E0 4A 81 E4 C6 AC 94-81 E5 CF E1 14 AA 76 60 | ÙÅJ áæ-áia-av-00150 | 74 C4 F8 A2 D2 7F 40 BA-BF B9 E6 F0 F9 B6 F0 75 | cæøô-ôô-ç-ôûñôûu00160 | C4 6E FC 1A BB 79 C4 10-92 39 CA A9 8B 19 A0 44 | Áù-»y-Á-9tô- D00170 | 3E 4C E9 5C 90 4C 0D AD-SD E8 8F 6E 35 D4 02 F9 | >L-L-je-n5ô-û00180 | FC A4 16 66 A1 AD OF E5-D0 70 9E 8E 82 13 27 8C | ùk f;-áBp-..00190 | ED E3 B3 D0 50 A6 56 9E-94 72 22 6D CB E1 74 6F | iâ*Bp|V- r"mâáto001A0 | OE 81 71 77 03 13 72 42-E4 D0 60 33 5C BF EE A1 | .qw- rBâðm3;jèi001B0 | F0 DF 0B 53 93 D3 8D 2F-24 2D BF 78 B0 DA 10 0D | åå-S-ô-/ô-ix'Û..001C0 | 2A 42 39 22 FE 27 D9 B7-2A 10 CE D8 11 7C D7 9E | B9'p'Û-...iô-10-|x-
```



# 아티팩트 분석

- C:\Users\forensic\AppData\Roaming\Telegram Desktop\data\settingss

Telegram Desktop에서 비로그인 상태에서 로그인 상태로 전환될 때,  
사용자 및 세션 관련 설정이 새롭게 구성되며 이 과정에서 settingss 파일이 반드시 갱신

□ \$I30	4,096 (4 KB) NTFS Index...	2026-01-10 오후 12:49:03
□ 2936D16393A135A6s	592,900 (50...) Regular File	2026-01-10 오후 12:47:07
□ 8B35F5D406432125s	140 (1 KB) Regular File	2026-01-10 오후 12:49:00
□ A7FDF064FBC10B77s	348 (1 KB) Regular File	2026-01-10 오후 12:47:18
□ countries	21,416 (21 ...) Regular File	2026-01-10 오후 12:41:17
□ D877F783D5D3EF8Cs	876 (1 KB) Regular File	2026-01-10 오후 12:48:58
□ key_datas	388 (1 KB) Regular File	2026-01-10 오후 12:47:18
□ prefix	24 (1 KB) Regular File	2026-01-10 오후 12:41:19
□ settingss	1,792 (2 KB) Regular File	2026-01-10 오후 12:49:00
□ shortcuts.custom.json	401 (1 KB) Regular File	2026-01-10 오후 12:41:02
□ shortcuts-default.json	4,455 (5 KB) Regular File	2026-01-10 오후 12:41:01
□ usertag	8 (1 KB) Regular File	2026-01-10 오후 12:40:50
☒ working	\$I30 INDX ...	

```
[2026.01.10 21:47:19] Audio Info: recreating audio device and reattaching the tracks  
[2026.01.10 21:47:22] App Info: writing encrypted user settings...  
[2026.01.10 21:47:23] Audio Info: Closing audio playback device.
```

settingss의 수정은  
로그인 상태로의 전이를 보조적으로 확인할 수 있는 아티팩트,  
key\_datas와 .s 파일과 함께 분석할 때 로그인 성공 입증 가능



# 아티팩트 분석

---

- Telegram Desktop 로그에 기록된 이벤트 시각과 로컬 파일의 수정 시각 사이에는 수 초에서 수 분의 차이가 발생할 수 있음
- 설정 저장이 즉시 디스크에 반영되지 않고 내부 버퍼링 및 상태 안정화 이후 지연 기록되기 때문

=> 따라서 본 연구에서는 단일 타임스탬프가 아닌 시간 구간(time window) 기반 상관 분석을 적용



# 아티팩트 분석

- C:\Users\forensic\AppData\Roaming\Telegram Desktop\data\key\_datas

key\_datas: Telegram Desktop에서 로그인 세션의 인증 정보를 저장하는 암호화된 바이너리 컨테이너

파일 내부에는 사람이 해석 가능한 로그인 정보나 QR 관련 문자열은 존재하지 않음

Offset(h)	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F	Decoded text
00000000	54 44 46 24 21 9D 5B 00 00 00 20 14 96 4F F2	TDF\$!.{.... .-Oò
00000010	76 4A 71 5F BC 8C A2 3B 75 5F D2 B1 08 5F 05 65	vJq.4@o;u.Ø±_.-e
00000020	47 76 33 22 2B 83 8D E6 BF D4 73 25 00 00 01 20	Gv3"+f.æçØs%...
00000030	EB 9B 1E 0F E1 66 1E 13 89 F6 61 11 A1 AD 62 B8	é,,..áf..%öa.;.b,
00000040	2C 7C 38 25 D9 D2 EB BD F0 4B BB 8B 6A BE A3 19	, 8%ÙÖëhØK»<j¾£.
00000050	A1 06 BE 29 50 4C B7 EE 07 31 B6 32 B8 7A 41 2B	;.%PL-i.1%Z.zA+
00000060	2C FE A2 E1 74 DB 33 E8 17 F3 A6 41 74 D9 EF 1E	,pcátÙ3è.ó)atÙi.
00000070	45 D3 09 20 F3 1B 97 2B 10 53 31 1D 7A CF 71 DA	EÓ. ó.-+.S1.zÍqÚ
00000080	B1 A7 13 21 D5 A2 BA 82 9A DF B7 F4 71 0A C2 FD	±S.!öç.,šB.öç.Áý
00000090	5A 8B E5 B3 DD F0 8A E6 6B D1 5A CD F9 19 31 DF	Z<å.ÝöšækÑzíù.1B
000000A0	D1 77 AF 6A 41 10 70 34 CB 53 30 1F 90 FB CE C9	Ñw-jA.p4ÉS0..üÍÉ
000000B0	D5 09 A8 0B DE DD 80 74 48 02 02 87 B3 52 6E 67	Ó.".ßYëtH..#^Rng
000000C0	E2 C9 C0 C3 8A B8 F3 47 13 42 CF 86 D4 93 80 AD	åÉÅÄÅ,6G.Bítô"€.
000000D0	72 E3 0A 5C 6F C4 3A 74 CE D5 35 38 FD 4A BD 09	rã.\oÄ:tíÖ5äýJä.
000000E0	9A B5 D9 E4 FF 6B 3A 50 15 01 76 26 EB 60 B5 5C	šuÜäýk:P..væ`µ\
000000F0	8F 8F 29 8E D3 2D E5 B8 78 BB C9 61 1F 2F 2E 92	..)ŽÖ-å,xwÅa./.'
00000100	02 BE AF 76 06 C8 81 50 EB 10 5B E0 8A 8E 9D 48	.¾.v.E.Pë.[äÅ.Z.H
00000110	6A 11 B8 6A 93 A8 8D 19 A8 5D 36 38 00 14 8E 5E	j..j""..]68..Ž^
00000120	7C 08 24 E4 07 83 4A AD CF FC 41 12 DA 98 C5 EA	.Sä.fJ.ÍüA.Ú"Åè
00000130	68 9A 2E B1 AC 40 2B 57 2C DC C5 7C 58 D8 4D F2	hå.±-ø+W,ÙåIXØMò
00000140	0C B3 77 BA 40 24 F1 FE 57 1D 7E D9 44 B9 43 F9	.~w@ØhpW..~Ùd^Cù
00000150	00 00 00 20 0A 9E 69 C6 D8 [79] 69 12 AE D6 A4 89	... .žiEØvi.Øm%
00000160	E6 B9 F1 DD BD DC 05 62 56 E0 6B A0 1C 93 BC 31	æ·ñÝü.Øvàk ."íl
00000170	15 3F 24 CD 97 0F B2 38 4D A0 FF 75 F1 49 06 31	.?§í-.~SM ýuñI.1
00000180	E1 53 0B 14	åS..



# 아티팩트 분석

---

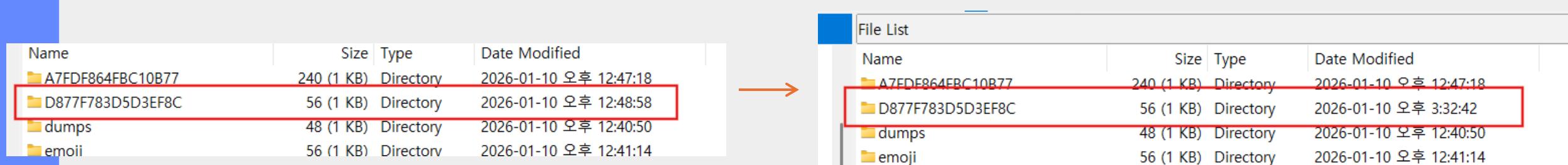
그러나 로그인 승인 직후 해당 파일의 생성·수정이 확인되었고,  
로그인 타임아웃 실험에서는 동일한 변화가 발생하지 않았음을 확인

countries	21,416 (21 ...	Regular File	2026-01-10 오후 12:41:17
D877F783D5D3EF8Cs	876 (1 KB)	Regular File	2026-01-10 오후 12:48:58
key_datas	388 (1 KB)	Regular File	2026-01-10 오후 12:47:18
prefix	24 (1 KB)	Regular File	2026-01-10 오후 12:41:10
settingss	1,792 (2 KB)	Regular File	2026-01-10 오후 12:49:00
shortcuts-custom.icon	191 (1 KB)	Regular File	2026-01-10 오후 12:41:02



# 아티팩트 분석

위 폴더가 QR Login 시에 생긴 세션 폴더  
아래 폴더가 인증 코드를 통하여 생긴 세션 폴더



Name	Size	Type	Date Modified
A7FDF864FBC10B77	240 (1 KB)	Directory	2026-01-10 오후 12:47:18
D877F783D5D3EF8C	56 (1 KB)	Directory	2026-01-10 오후 12:48:58
dumps	48 (1 KB)	Directory	2026-01-10 오후 12:40:50
emoji	56 (1 KB)	Directory	2026-01-10 오후 12:41:14

→

File List			
Name	Size	Type	Date Modified
A7FDF864FBC10B77	240 (1 KB)	Directory	2026-01-10 오후 12:47:18
D877F783D5D3EF8C	56 (1 KB)	Directory	2026-01-10 오후 3:32:42
dumps	48 (1 KB)	Directory	2026-01-10 오후 12:40:50
emoji	56 (1 KB)	Directory	2026-01-10 오후 12:41:14

QR Login, 인증코드 로그인을 2회 진행하였을때,  
인증코드 로그인 폴더만 바뀌었음을 확인 가능

=> QR 로그인은 새로운 PC 세션을 생성하지 않고,  
기존 PC 세션 컨테이너에  
모바일 세션의 승인 토큰만 간신히하는 방식



# 아티팩트 분석

---

## QR 로그인

: 기존 세션 컨테이너 유지 및 모바일 세션 승인으로 authorization key만 갱신  
=> 세션 연속성 유지

## QR 로그인:

- 풀더 생성 시간 유지
- 일부 파일만 수정

## 인증코드 로그인:

- 생성 시간/수정 시간 전반적 변경
- 내부 파일 구조가 통째로 바뀜



# 시나리오

---

## - 사건 개요 및 초기 수사 상황

수사 현장에서 피의자의 PC와 휴대전화가 함께 확보되었으나, 양 기기에 대해 1차 디지털 포렌식을 수행한 결과 Telegram 애플리케이션 설치 이력 및 관련 데이터는 확인되지 않았다. 특히 모바일 포렌식 분석 결과, 휴대전화 내에서는 Telegram과 관련된 잔존 아티팩트가 전혀 존재하지 않는 것으로 확인되었다.



# 시나리오

---

## - PC 포렌식 분석 결과

그러나 확보된 PC에 대해 정밀 포렌식을 수행하던 중,  
Telegram 데스크톱 환경에서 QR 로그인 과정에서 생성되는 인증·세션 관련 아티팩트가 식별되었다.  
해당 아티팩트는 일반적인 ID·비밀번호 기반 로그인에서는 생성되지 않는 특성을 가지며,  
이를 통해 사용자가 QR 코드를 이용하여 Telegram에 로그인하였음을 확인할 수 있었다.



# 시나리오

---

## - 수사적 해석 및 확장

이러한 분석 결과는,  
피의자가 사건 현장에서 확보된 휴대전화가 아닌 제3의 다른 모바일 기기를 이용하여 QR 코드를 스캔하고,  
이를 통해 PC의 Telegram 계정에 접근하였을 가능성을 시사한다.

이에 따라 수사기관은 추가적으로 사용되었을 가능성이 있는 다른 휴대전화의 존재를 특정할 수 있었으며,  
이를 새로운 모바일 기기를 압수하여, 수사를 확장하는 결정적 단서를 확보할 수 있다.



# 향후 연구 제시

---

- 모바일 환경에서의 Telegram QR Login 아티팩트 분석
- Telegram 내부 로그인 관련 암호화 파일 복호화
- 메신저 프로그램 QR 로그인 아티팩트 분석



---

감사합니다.

