
QR 로그인 아티팩트
분석(Telegram)

정지윤

명지대학교 해킹 동아리

MJSEC

QR 로그인 아티팩트 분석 (Telegram)

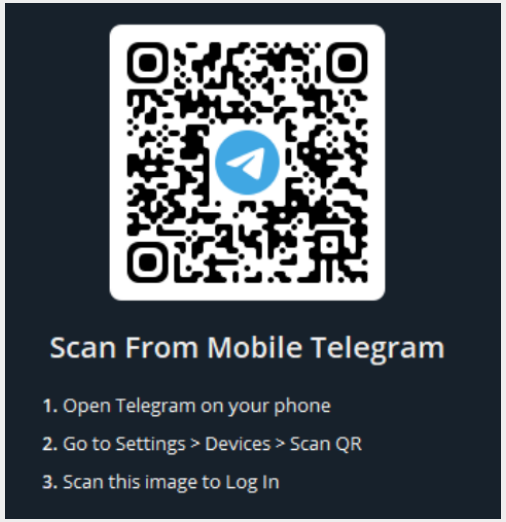
목차

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



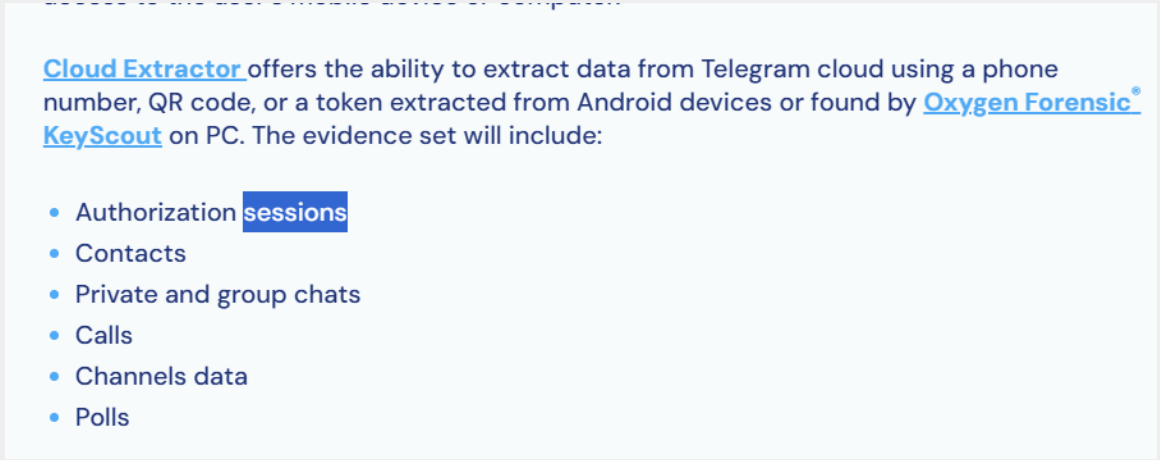
More often than not, the site looks pretty modest. The first page displays a message like "Sign in and vote" or "Free access to the trial version of Telegram Premium" — depending on the scheme in question. Next comes the messenger login screen. There are two variants here: those who opened the site on 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.

A cybercriminal site asking how you'd like to lose your account: by QR code or by entering a phone number

선행 연구

윈도우 환경에서 텔레그램 PC에 남은 아티팩트를 전반적으로 분석한 연구

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



연구 목적

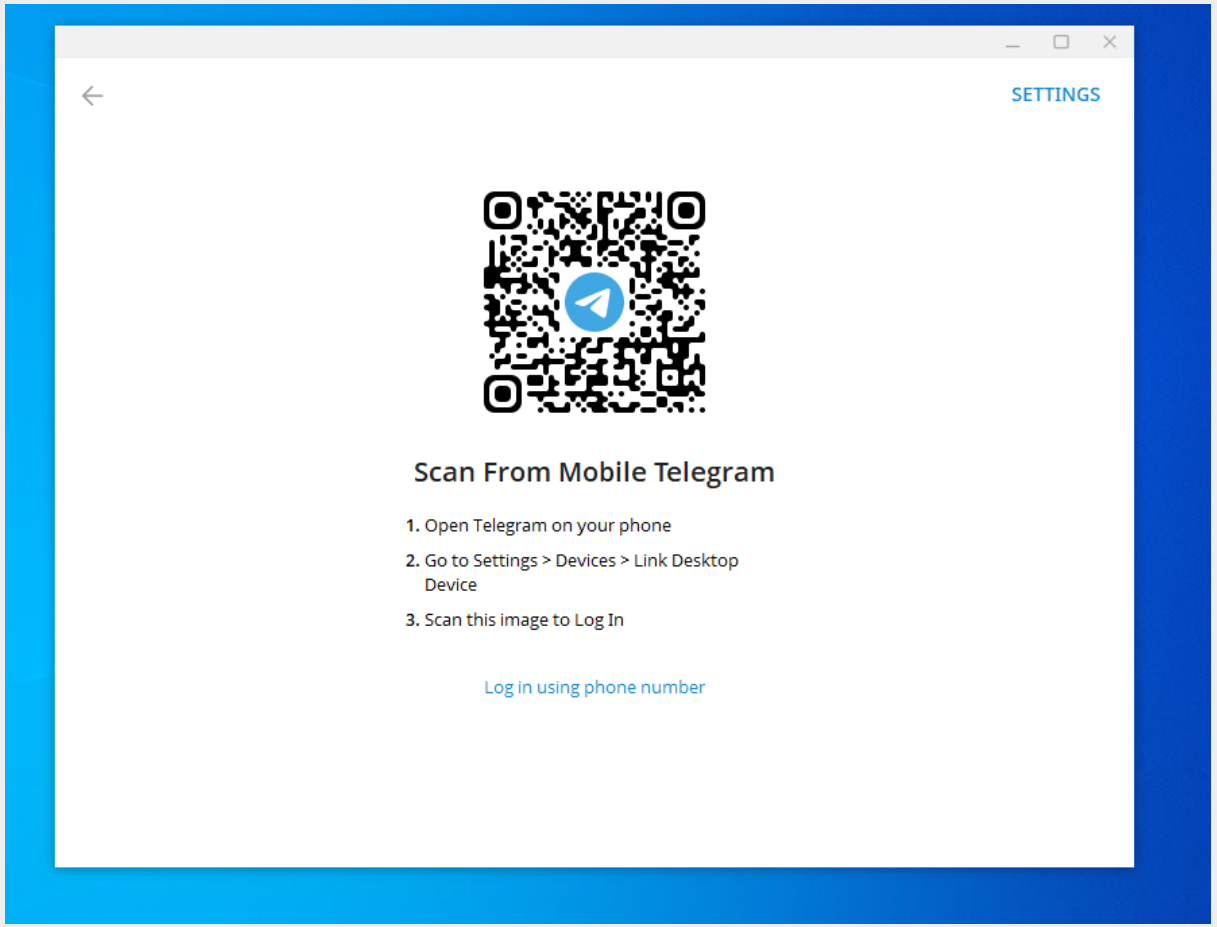
Telegram Desktop의 로컬 PC 아티팩트 분석을 통한 QR 로그인 흔적의 추적 가능성과 구조적 한계 규명

실험 환경 및 도구

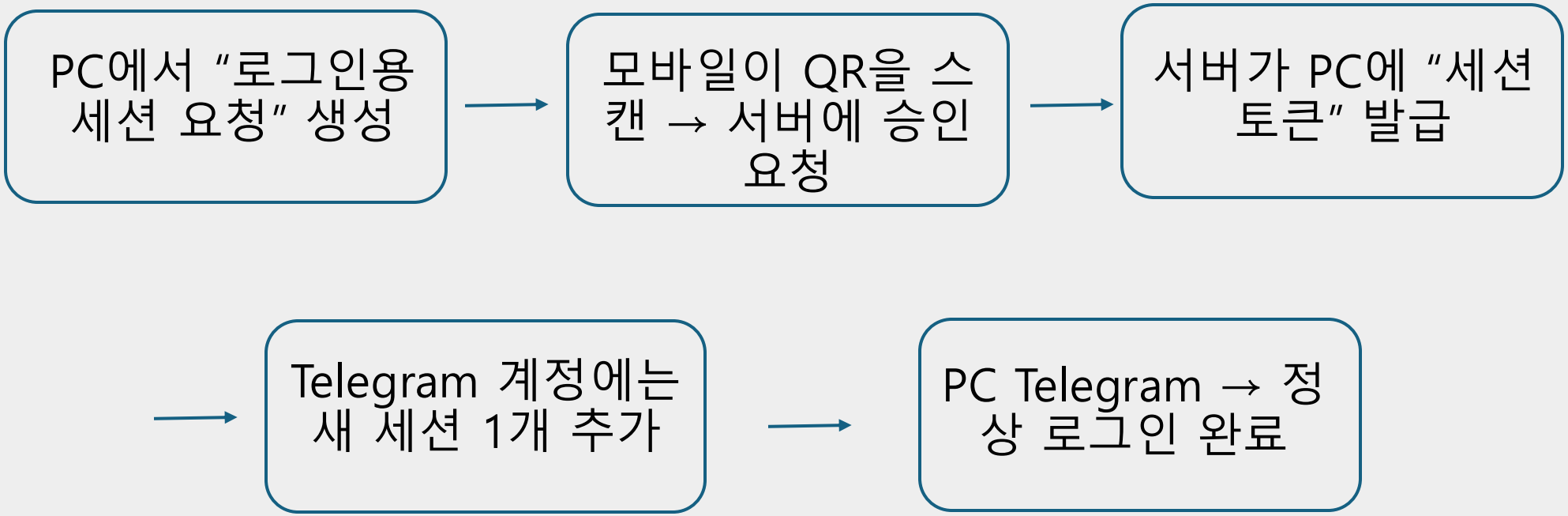
Program	Version	Function
VMWare workstation	17 pro	가상환경 구축 및 vmdk 추출
Windows	10 home	Windows 환경 구축
FTK Imager	4.7.3.81	디스크 이미지 및 파일 추출
Autopsy	4.22.1	아티팩트 분석 활용
HxD	2.5	바이너리 분석

Telegram 로그인 구조

- 인증 코드 로그인
- QR 로그인
(모바일 승인 기반)



QR Login 방식



연구 필요성

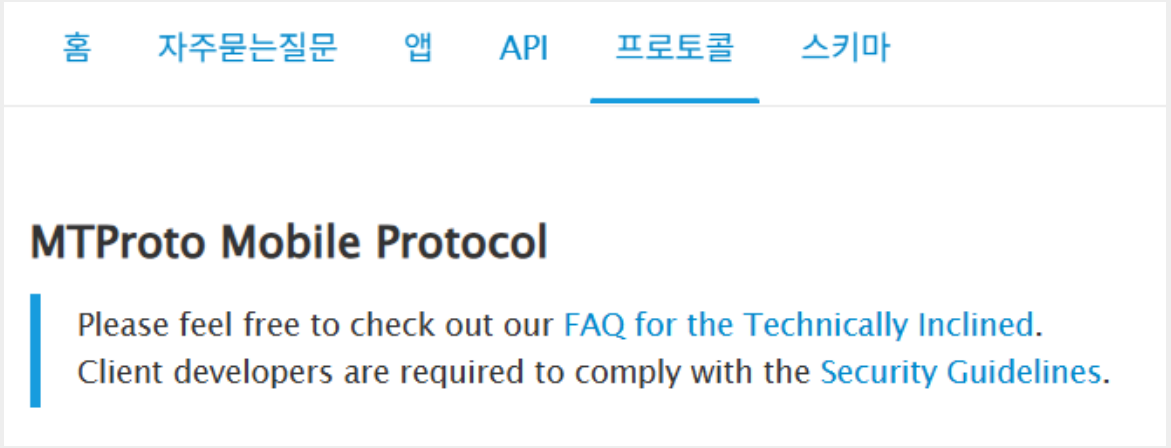
Telegram은 MTProto 프로토콜 사용

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/비밀번호 등)을 식별하기 어렵다.

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



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 Into: Destroy top bar by controller removal
```

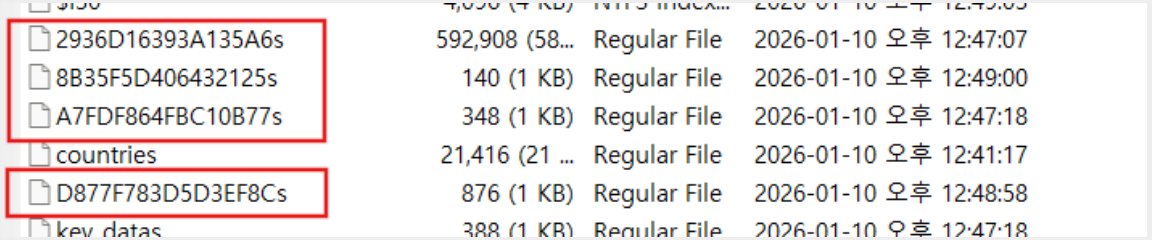
로그인 성공 → 세션 생성 의미

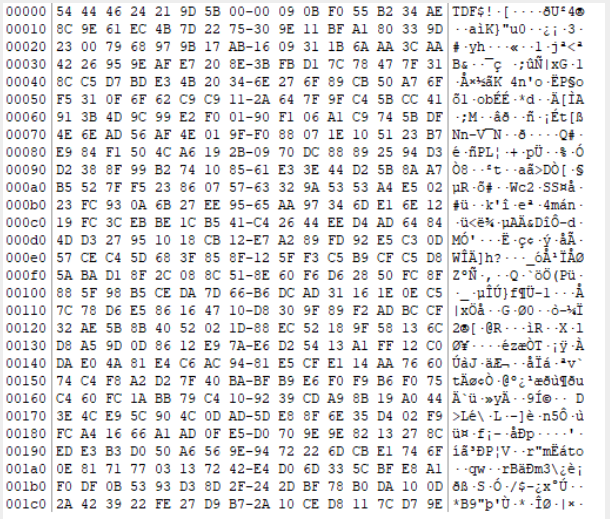
모바일 기기에서 기기 연결 해제를 하였을때
있던 세션이 서버 측에서 무효화되었을 때 발생

아티팩트 분석

- **C:₩Users₩forensic₩AppData₩Roaming₩Telegram Desktop₩tdata₩.s**

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



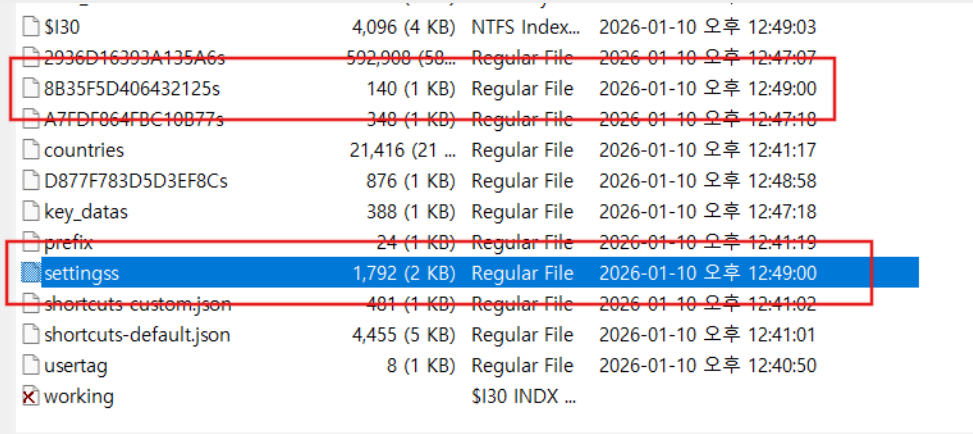


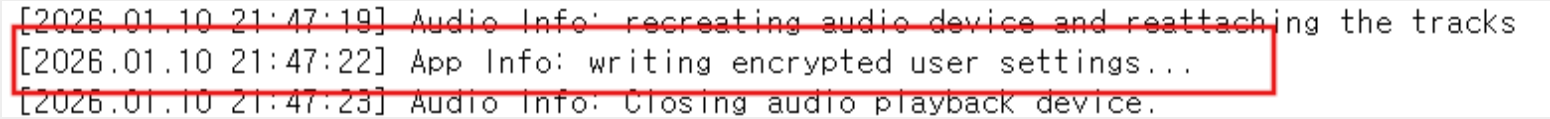
이 파일들은 내부 세션 상태를 분산 저장하기 위한 것으로,
파일 내용 자체는 해석할 수 없지만
key_datas와 동일 시점에 생성·수정된다는 점에서
실제 세션이 생성되었음을 입증하는 보조 자료

아티팩트 분석

- **C:₩Users₩forensic₩AppData₩Roaming₩Telegram Desktop₩tdata₩settingss**

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





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₩tdata₩key_datas**

key_datas: Telegram Desktop에서 로그인 세션의 인증 정보를 저장하는 암호화된 바이너리 컨테이너

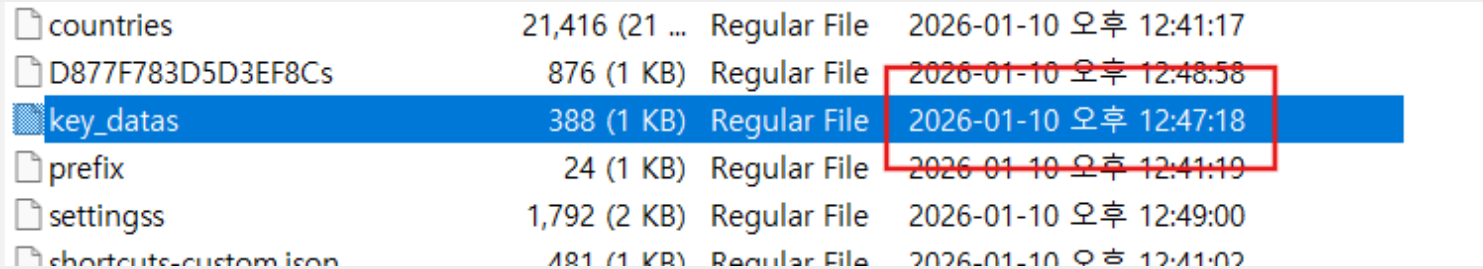
파일 내부에는 사람이 해석 가능한 로그인 정보나 QR 관련 문자열은 존재하지 않음

key_datas

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	00	20	14	96	4F	F2	TDF$!.[.... .–Oò
00000010	76	4A	71	5F	BC	8C	A2	3B	75	5F	D2	B1	08	5F	05	65	vJq_¼Œ¢;u_Ò±._.e
00000020	47	76	33	22	2B	83	8D	E6	BF	D4	73	25	00	00	01	20	Gv3"+ƒ.æ¿Ôs%...
00000030	EB	9B	1E	0F	E1	66	1E	13	89	F6	61	11	A1	AD	62	B8	ë›..áf..‰öa.¡.b¸
00000040	2C	7C	38	25	D9	D2	EB	BD	F0	4B	BB	8B	6A	BE	A3	19	,|8%ÙÒë½ðK»‹j¾£.
00000050	A1	06	BE	29	50	4C	B7	EE	07	31	B6	32	B8	7A	41	2B	¡.¾)PL·î.1¶2¸zA+
00000060	2C	FE	A2	E1	74	DB	33	E8	17	F3	A6	41	74	D9	EF	1E	,þ¢átÛ3è.ó¦AtÙï.
00000070	45	D3	09	20	F3	1B	97	2B	10	53	31	1D	7A	CF	71	DA	EÓ. ó.—+.S1.zÏqÚ
00000080	B1	A7	13	21	D5	A2	BA	82	9A	DF	B7	F4	71	0A	C2	FD	±§.!Õ¢º‚šß·ôq.Âý
00000090	5A	8B	E5	B3	DD	F0	8A	E6	6B	D1	5A	CD	F9	19	31	DF	Z‹å³ÝðŠækÑZÍù.1ß
000000A0	D1	77	AF	6A	41	10	70	34	CB	53	30	1F	90	FB	CE	C9	Ñw¯jA.p4ËS0..ûÎÉ
000000B0	D5	09	A8	0B	DE	DD	80	74	48	02	02	87	B3	52	6E	67	Õ.¨.ÞÝ€tH..‡³Rng
000000C0	E2	C9	C0	C3	8A	B8	F3	47	13	42	CF	86	D4	93	80	AD	âÉÀÃŠ¸óG.BÏ†Ô"€.
000000D0	72	E3	0A	5C	6F	C4	3A	74	CE	D5	35	38	FD	4A	BD	09	rã.\oÄ:tÎÕ58ýJ½.
000000E0	9A	B5	D9	E4	FF	6B	3A	50	15	01	76	26	EB	60	B5	5C	šµÙäÿk:P..v&ë`µ\
000000F0	8F	8F	29	8E	D3	2D	E5	B8	78	BB	C9	61	1F	2F	2E	92	..)ŽÓ-å¸x»Éa./.'
00000100	02	BE	AF	76	06	C8	81	50	EB	10	5B	E0	8A	8E	9D	48	.¾¯v.È.Pë.[àŠŽ.H
00000110	6A	11	B8	6A	93	A8	8D	19	A8	5D	36	38	00	14	8E	5E	j.¸j"¨..¨]68..Ž^
00000120	7C	08	24	E4	07	83	4A	AD	CF	FC	41	12	DA	98	C5	EA	|.$ä.ƒJ.ÏüA.Ú˜Åê
00000130	68	9A	2E	B1	AC	40	2B	57	2C	DC	C5	7C	58	D8	4D	F2	hš.±¬@+W,ÜÅ|XØMò
00000140	0C	B3	77	BA	40	24	F1	FE	57	1D	7E	D9	44	B9	43	F9	.³wº@$ñþW.~ÙD¹Cù
00000150	00	00	00	20	0A	9E	69	C6	D8	79	69	12	AE	D6	A4	89	... .žiÆØyi.®Ö¤‰
00000160	E6	B9	F1	DD	BD	DC	05	62	56	E0	6B	A0	1C	93	BC	31	æ¹ñÝ½Ü.bVàk ."¼1
00000170	15	3F	24	CD	97	0F	B2	38	4D	A0	FF	75	F1	49	06	31	.?$Í–.²8M ÿuñI.1
00000180	E1	53	0B	14													áS..

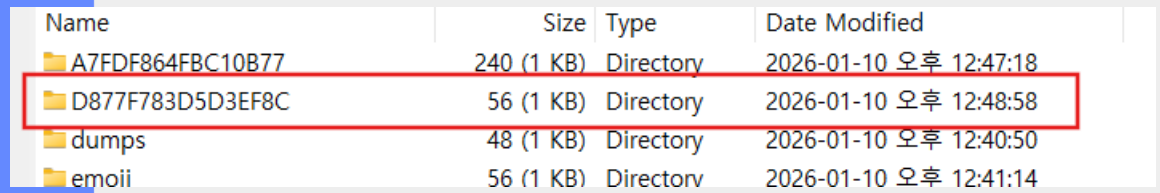
아티팩트 분석

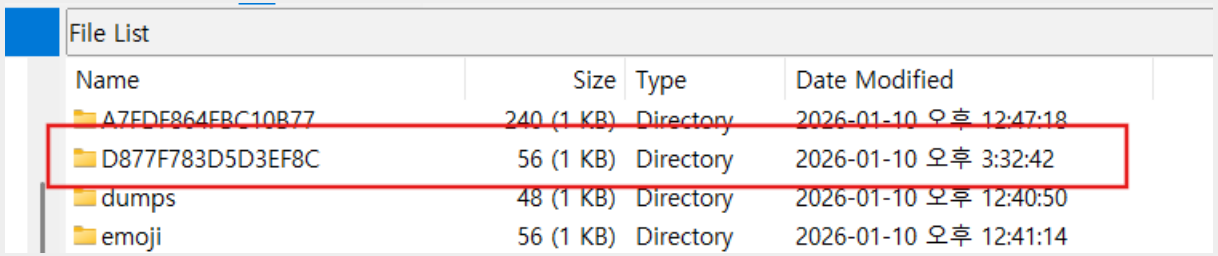
그러나 로그인 승인 직후 해당 파일의 생성·수정이 확인되었고,
로그인 타임아웃 실험에서는 동일한 변화가 발생하지 않았음을 확인



아티팩트 분석

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





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 갱신하는 방식

아티팩트 분석

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

QR 로그인:

- 폴더 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.