

TALK

디지털 포렌식 관점의 카카오톡 분석 및 메시지 복구 솔루션 개발



1주차 발표

전유민, 조재현, 김우종

01

경로 탐색

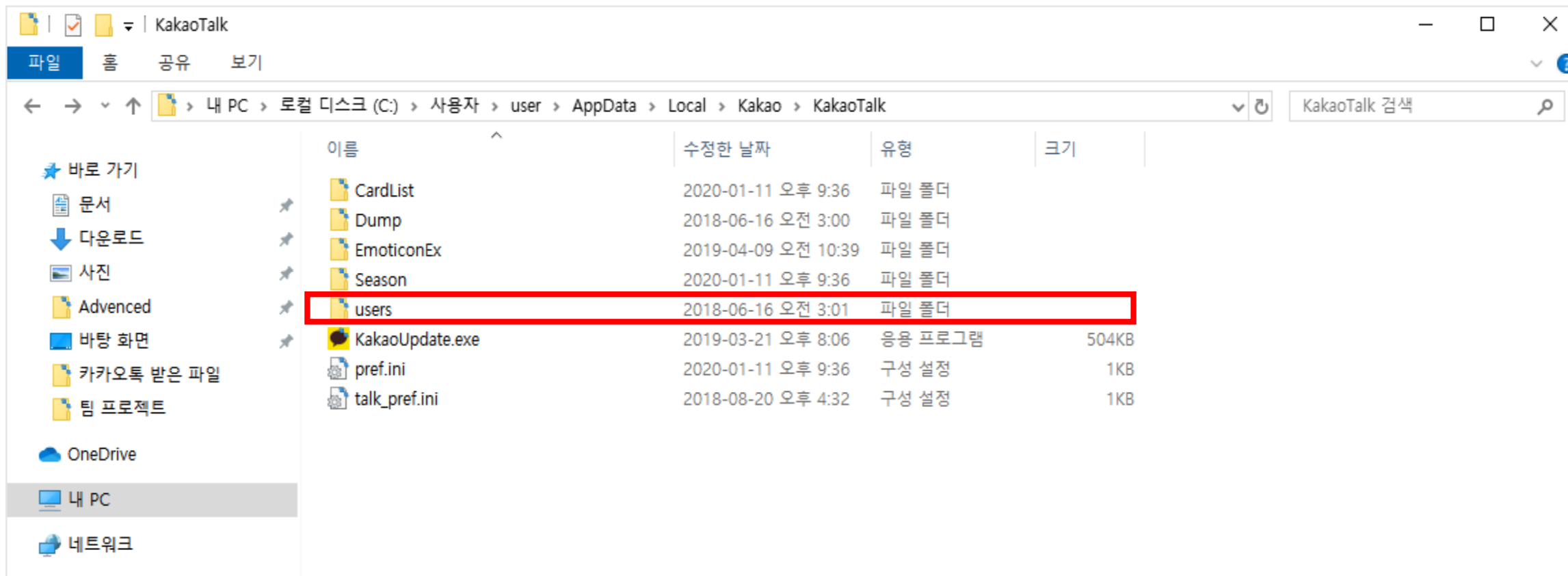
02

정적 분석

03

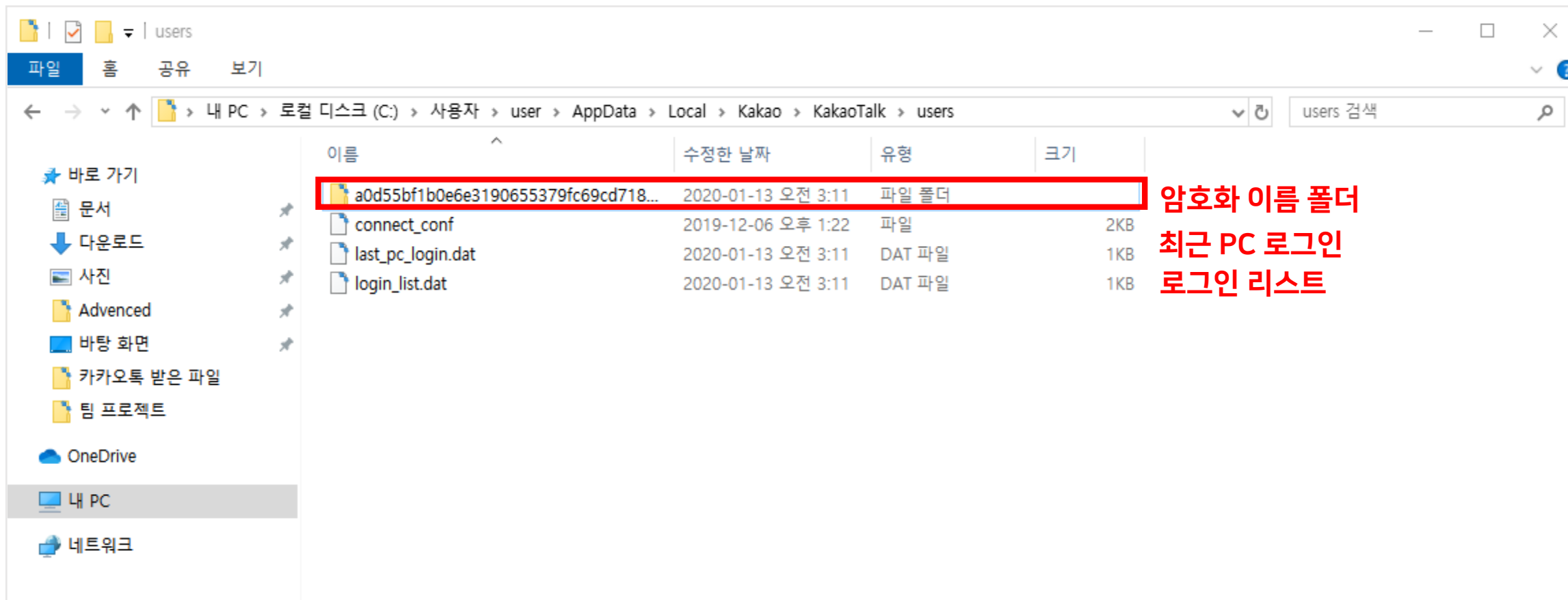
동적 분석 계획

01 경로 탐색



경로 : C:\[사용자]\user\AppData\Local\Kakao\KakaoTalk

02 정적 분석



users

파일 홈 공유 보기

← → ↕ ↗ > 내 PC > 로컬 디스크 (C:) > 사용자 > user > AppData > Local > Kakao > KakaoTalk > users

이름	수정한 날짜	유형	크기
a0d55bf1b0e6e3190655379fc69cd718...	2020-01-13 오전 3:11	파일 폴더	
connect_conf	2019-12-06 오후 1:22	파일	2KB
last_pc_login.dat	2020-01-13 오전 3:11	DAT 파일	1KB
login_list.dat	2020-01-13 오전 3:11	DAT 파일	1KB

바로 가기

- 문서
- 다운로드
- 사진
- Advanced
- 바탕 화면
- 카카오톡 받은 파일
- 팀 프로젝트
- OneDrive
- 내 PC
- 네트워크

암호화 이름 폴더
최근 PC 로그인
로그인 리스트

02 정적 분석

File Explorer window showing the directory structure of a user's AppData folder. The path is: < 사용자 > user > AppData > Local > Kakao > KakaoTalk > users > a0d55bf1b0e6e3190655379fc69cd71876f70dc2. The search bar contains: a0d55bf1b0e6e3190655379...

이름	수정한 날짜	유형	크기
BalloonFactory	2019-12-27 오전 11:56	파일 폴더	
chat_data	2020-01-13 오전 3:11	파일 폴더	
Contacts	2020-01-13 오전 3:11	파일 폴더	
DigitalItem	2018-06-16 오전 3:01	파일 폴더	
Moim	2018-06-18 오후 9:25	파일 폴더	
OCH	2020-01-13 오전 3:11	파일 폴더	
CalendarDB.edb	2020-01-13 오전 3:21	EDB 파일	496KB
chatWindowUi.db	2020-01-13 오전 3:11	Data Base File	20KB
chatWindowUi.db-shm	2020-01-13 오전 3:11	DB-SHM 파일	32KB
chatWindowUi.db-wal	2020-01-13 오전 3:11	DB-WAL 파일	0KB
contactGroup.edb	2018-06-16 오후 10:24	EDB 파일	24KB
emoticon.edb	2019-09-30 오후 2:14	EDB 파일	32KB
emoticon.edb-shm	2020-01-13 오전 3:11	EDB-SHM 파일	32KB
emoticon.edb-wal	2020-01-13 오전 3:11	EDB-WAL 파일	0KB
floatingList.edb	2019-09-30 오후 2:14	EDB 파일	12KB
RecentEmoticon.db	2019-09-30 오후 2:14	Data Base File	8KB
RecentEmoticon.db-shm	2020-01-13 오전 3:11	DB-SHM 파일	32KB
RecentEmoticon.db-wal	2020-01-13 오전 3:11	DB-WAL 파일	0KB
talk_user_pref.ini	2018-08-20 오후 1:56	구성 설정	1KB
talk_user_prf.edb	2020-01-13 오전 3:11	EDB 파일	20KB
talk_user_prf.edb-shm	2020-01-13 오전 3:11	EDB-SHM 파일	32KB
talk_user_prf.edb-wal	2020-01-13 오전 3:11	EDB-WAL 파일	49KB
TalkUserDB.edb	2020-01-13 오전 3:11	EDB 파일	602KB

26개 항목

캘린더DB파일

02 정적 분석

File Explorer window showing the directory structure of a user's AppData folder. The path is: < 사용자 > user > AppData > Local > Kakao > KakaoTalk > users > a0d55bf1b0e6e3190655379fc69cd71876f70dc2. The search bar contains: a0d55bf1b0e6e3190655379...

이름	수정한 날짜	유형	크기
BalloonFactory	2019-12-27 오전 11:56	파일 폴더	
chat_data	2020-01-13 오전 3:11	파일 폴더	
Contacts	2020-01-13 오전 3:11	파일 폴더	
DigitalItem	2018-06-16 오전 3:01	파일 폴더	
Moim	2018-06-18 오후 9:25	파일 폴더	
OCH	2020-01-13 오전 3:11	파일 폴더	
CalendarDB.edb	2020-01-13 오전 3:21	EDB 파일	496KB
chatWindowUi.db	2020-01-13 오전 3:11	Data Base File	20KB
chatWindowUi.db-shm	2020-01-13 오전 3:11	DB-SHM 파일	32KB
chatWindowUi.db-wal	2020-01-13 오전 3:11	DB-WAL 파일	0KB
contactGroup.edb	2018-06-16 오후 10:24	EDB 파일	24KB
emoticon.edb	2019-09-30 오후 2:14	EDB 파일	32KB
emoticon.edb-shm	2020-01-13 오전 3:11	EDB-SHM 파일	32KB
emoticon.edb-wal	2020-01-13 오전 3:11	EDB-WAL 파일	0KB
floatingList.edb	2019-09-30 오후 2:14	EDB 파일	12KB
RecentEmoticon.db	2019-09-30 오후 2:14	Data Base File	8KB
RecentEmoticon.db-shm	2020-01-13 오전 3:11	DB-SHM 파일	32KB
RecentEmoticon.db-wal	2020-01-13 오전 3:11	DB-WAL 파일	0KB
talk_user_pref.ini	2018-08-20 오후 1:56	구성 설정	1KB
talk_user_prf.edb	2020-01-13 오전 3:11	EDB 파일	20KB
talk_user_prf.edb-shm	2020-01-13 오전 3:11	EDB-SHM 파일	32KB
talk_user_prf.edb-wal	2020-01-13 오전 3:11	EDB-WAL 파일	49KB
TalkUserDB.edb	2020-01-13 오전 3:11	EDB 파일	607KB

26개 항목

그 외 이모티콘 & 유저 관련 파일

02 정적 분석

File Explorer window showing the directory structure of a user's AppData folder. The path is: < 사용자 > user > AppData > Local > Kakao > KakaoTalk > users > a0d55bf1b0e6e3190655379fc69cd71876f70dc2. The search bar contains the same ID.

Left sidebar shows navigation options: 바로 가기 (QuickTime), 문서 (Documents), 다운로드 (Downloads), 사진 (Pictures), Advenced, 바탕 화면 (Desktop), 카카오톡 받은 파일 (KakaoTalk received files), 팀 프로젝트 (Team Project), OneDrive, 내 PC (This PC), 네트워크 (Network).

Main pane shows a list of files and folders. The 'chat_data' folder is highlighted with a red box, indicating it is the message file folder.

이름	수정한 날짜	유형	크기
BalloonFactory	2019-12-27 오전 11:56	파일 폴더	
chat_data	2020-01-13 오전 3:11	파일 폴더	
Contacts	2020-01-13 오전 3:11	파일 폴더	
DigitalItem	2018-06-16 오전 3:01	파일 폴더	
Moim	2018-06-18 오후 9:25	파일 폴더	
OCH	2020-01-13 오전 3:11	파일 폴더	
CalendarDB.edb	2020-01-13 오전 3:21	EDB 파일	496KB
chatWindowUi.db	2020-01-13 오전 3:11	Data Base File	20KB
chatWindowUi.db-shm	2020-01-13 오전 3:11	DB-SHM 파일	32KB
chatWindowUi.db-wal	2020-01-13 오전 3:11	DB-WAL 파일	0KB
contactGroup.edb	2018-06-16 오후 10:24	EDB 파일	24KB
emoticon.edb	2019-09-30 오후 2:14	EDB 파일	32KB
emoticon.edb-shm	2020-01-13 오전 3:11	EDB-SHM 파일	32KB
emoticon.edb-wal	2020-01-13 오전 3:11	EDB-WAL 파일	0KB
floatingList.edb	2019-09-30 오후 2:14	EDB 파일	12KB
RecentEmoticon.db	2019-09-30 오후 2:14	Data Base File	8KB
RecentEmoticon.db-shm	2020-01-13 오전 3:11	DB-SHM 파일	32KB
RecentEmoticon.db-wal	2020-01-13 오전 3:11	DB-WAL 파일	0KB
talk_user_pref.ini	2018-08-20 오후 1:56	구성 설정	1KB
talk_user_prf.edb	2020-01-13 오전 3:11	EDB 파일	20KB
talk_user_prf.edb-shm	2020-01-13 오전 3:11	EDB-SHM 파일	32KB
talk_user_prf.edb-wal	2020-01-13 오전 3:11	EDB-WAL 파일	49KB
TalkUserDB.edb	2020-01-13 오전 3:11	EDB 파일	602KB

26개 항목

메시지 파일 폴더

02 정적 분석

File Explorer window showing the directory structure of KakaoTalk chat data. The path is: user > AppData > Local > Kakao > KakaoTalk > users > a0d55bf1b0e6e3190655379fc69cd71876f70dc2 > chat_data. The search bar contains "chat_data 검색".

이름	수정된 날짜	유형	크기
chatListInfo.edb-wal	2020-01-13 오전 3:33	EDB-WAL 파일	61KB
chatLogs_213621355510884.edb-wal	2020-01-13 오전 3:33	EDB-WAL 파일	85KB
chatLogs_213621355510884.edb-shm	2020-01-13 오전 3:29	EDB-SHM 파일	32KB
chatAttachmentInfo.edb-shm	2020-01-13 오전 3:11	EDB-SHM 파일	32KB
chatAttachmentInfo.edb-wal	2020-01-13 오전 3:11	EDB-WAL 파일	0KB
chatLinkInfo.edb-shm	2020-01-13 오전 3:11	EDB-SHM 파일	32KB
chatLinkInfo.edb-wal	2020-01-13 오전 3:11	EDB-WAL 파일	0KB
chatListInfo.edb-shm	2020-01-13 오전 3:11	EDB-SHM 파일	32KB
cli_http_v2.edb-shm	2020-01-13 오전 3:11	EDB-SHM 파일	32KB
cli_http_v2.edb-wal	2020-01-13 오전 3:11	EDB-WAL 파일	0KB
drawermedia.edb-shm	2020-01-13 오전 3:11	EDB-SHM 파일	32KB
drawermedia.edb-wal	2020-01-13 오전 3:11	EDB-WAL 파일	0KB
fci_v2.edb-shm	2020-01-13 오전 3:11	EDB-SHM 파일	32KB
fci_v2.edb-wal	2020-01-13 오전 3:11	EDB-WAL 파일	0KB
mci_v2.edb-shm	2020-01-13 오전 3:11	EDB-SHM 파일	32KB
mci_v2.edb-wal	2020-01-13 오전 3:11	EDB-WAL 파일	0KB
oci_v2.edb-shm	2020-01-13 오전 3:11	EDB-SHM 파일	32KB
oci_v2.edb-wal	2020-01-13 오전 3:11	EDB-WAL 파일	0KB
ocii_v2.edb-shm	2020-01-13 오전 3:11	EDB-SHM 파일	32KB
ocii_v2.edb-wal	2020-01-13 오전 3:11	EDB-WAL 파일	0KB
openLinkListInfo.edb-shm	2020-01-13 오전 3:11	EDB-SHM 파일	32KB
openLinkListInfo.edb-wal	2020-01-13 오전 3:11	EDB-WAL 파일	0KB
url_image_v2.edb-shm	2020-01-13 오전 3:11	EDB-SHM 파일	32KB

355개 항목 | 1개 항목 선택함 104KB

전체 특방에서 메시지 전송 시 저장

02 정적 분석

File Explorer window showing the directory structure of KakaoTalk users. The path is: user > AppData > Local > Kakao > KakaoTalk > users > a0d55bf1b0e6e3190655379fc69cd71876f70dc2 > chat_data. The search bar contains "chat_data 검색".

이름	수정된 날짜	유형	크기
chatListInfo.edb-wal	2020-01-13 오전 3:33	EDB-WAL 파일	61KB
chatLogs_213621355510884.edb-wal	2020-01-13 오전 3:33	EDB-WAL 파일	85KB
chatLogs_213621355510884.edb-shm	2020-01-13 오전 3:29	EDB-SHM 파일	32KB
chatAttachmentInfo.edb-shm	2020-01-13 오전 3:11	EDB-SHM 파일	32KB
chatAttachmentInfo.edb-wal	2020-01-13 오전 3:11	EDB-WAL 파일	0KB
chatLinkInfo.edb-shm	2020-01-13 오전 3:11	EDB-SHM 파일	32KB
chatLinkInfo.edb-wal	2020-01-13 오전 3:11	EDB-WAL 파일	0KB
chatListInfo.edb-shm	2020-01-13 오전 3:11	EDB-SHM 파일	32KB
cli_http_v2.edb-shm	2020-01-13 오전 3:11	EDB-SHM 파일	32KB
cli_http_v2.edb-wal	2020-01-13 오전 3:11	EDB-WAL 파일	0KB
drawermedia.edb-shm	2020-01-13 오전 3:11	EDB-SHM 파일	32KB
drawermedia.edb-wal	2020-01-13 오전 3:11	EDB-WAL 파일	0KB
fci_v2.edb-shm	2020-01-13 오전 3:11	EDB-SHM 파일	32KB
fci_v2.edb-wal	2020-01-13 오전 3:11	EDB-WAL 파일	0KB
mci_v2.edb-shm	2020-01-13 오전 3:11	EDB-SHM 파일	32KB
mci_v2.edb-wal	2020-01-13 오전 3:11	EDB-WAL 파일	0KB
oci_v2.edb-shm	2020-01-13 오전 3:11	EDB-SHM 파일	32KB
oci_v2.edb-wal	2020-01-13 오전 3:11	EDB-WAL 파일	0KB
ocii_v2.edb-shm	2020-01-13 오전 3:11	EDB-SHM 파일	32KB
ocii_v2.edb-wal	2020-01-13 오전 3:11	EDB-WAL 파일	0KB
openLinkListInfo.edb-shm	2020-01-13 오전 3:11	EDB-SHM 파일	32KB
openLinkListInfo.edb-wal	2020-01-13 오전 3:11	EDB-WAL 파일	0KB
url_image_v2.edb-shm	2020-01-13 오전 3:11	EDB-SHM 파일	32KB

355개 항목 | 1개 항목 선택함 104KB

해당 특방에서 메시지 전송 시 저장
해당 특방 접속 시 저장 / 32KB

02 정적 분석

File Explorer window showing the contents of the folder: < user > AppData > Local > Kakao > KakaoTalk > users > a0d55bf1b0e6e3190655379fc69cd71876f70dc2 > chat_data

Search: chat_data 검색

이름	수정된 날짜	유형	크기
chatLogs_238955094580084.edb	2020-01-13 오전 2:24	EDB 파일	104KB
chatLogs_227662661066232.edb	2020-01-13 오전 2:24	EDB 파일	5,412KB
chatLogs_206655508573450.edb	2020-01-13 오전 2:24	EDB 파일	4,348KB
chatLogs_4753655579742236.edb	2020-01-13 오전 2:24	EDB 파일	40KB
chatLogs_168326346386457.edb	2020-01-13 오전 2:22	EDB 파일	168KB
chatLogs_27989209283572.edb	2020-01-13 오전 2:19	EDB 파일	248KB
chatLogs_204904444584045.edb	2020-01-13 오전 12:09	EDB 파일	308KB
chatLogs_261240855789568.edb	2020-01-12 오후 10:26	EDB 파일	92KB
chatLogs_262586295985617.edb	2020-01-12 오후 7:01	EDB 파일	28KB
chatLogs_205858546946460.edb	2020-01-12 오후 6:44	EDB 파일	152KB
chatLogs_262571653137895.edb	2020-01-12 오후 3:43	EDB 파일	36KB
chatLogs_204904063842381.edb	2020-01-11 오후 9:36	EDB 파일	2,860KB
chatLogs_262850194942122.edb	2020-01-11 오후 9:36	EDB 파일	44KB
chatLogs_213621355510884.edb	2020-01-11 오후 2:14	EDB 파일	284KB
chatLogs_253879457967207.edb	2020-01-11 오후 2:14	EDB 파일	440KB
chatLogs_263303454415109.edb	2020-01-11 오전 1:47	EDB 파일	112KB
chatLogs_240795903235566.edb	2020-01-10 오후 9:25	EDB 파일	512KB
chatLogs_205439607043073.edb	2020-01-10 오후 9:25	EDB 파일	1,420KB
chatLogs_235210606496936.edb	2020-01-09 오전 2:25	EDB 파일	468KB
chatLogs_189472497579063.edb	2020-01-09 오전 1:48	EDB 파일	136KB
chatLogs_151801208802536.edb	2020-01-09 오전 1:48	EDB 파일	1,304KB
chatLogs_218873673603419.edb	2020-01-05 오후 5:12	EDB 파일	80KB
chatLogs_245602526415338.edb	2020-01-04 오후 10:46	EDB 파일	44KB

359개 항목 | 1개 항목 선택함 4.24MB

채팅방마다 모든 대화 내용이 저장된 edb 파일



EDB

Windows와 같은 운영체제에서 사용되는 데이터베이스 암호화 파일



WAL

기본 데이터베이스에 아직 적용되지 않은 트랜잭션을 기록하는 롤 포워드 저널



SHM

실제로 파일로 잘 사용되지 않으며 wal 파일 내에서 프레임을 찾기 위한 캐시로 사용

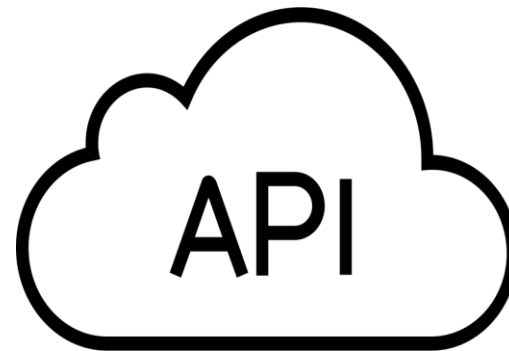
03 동적 분석 계획



X64 DBG



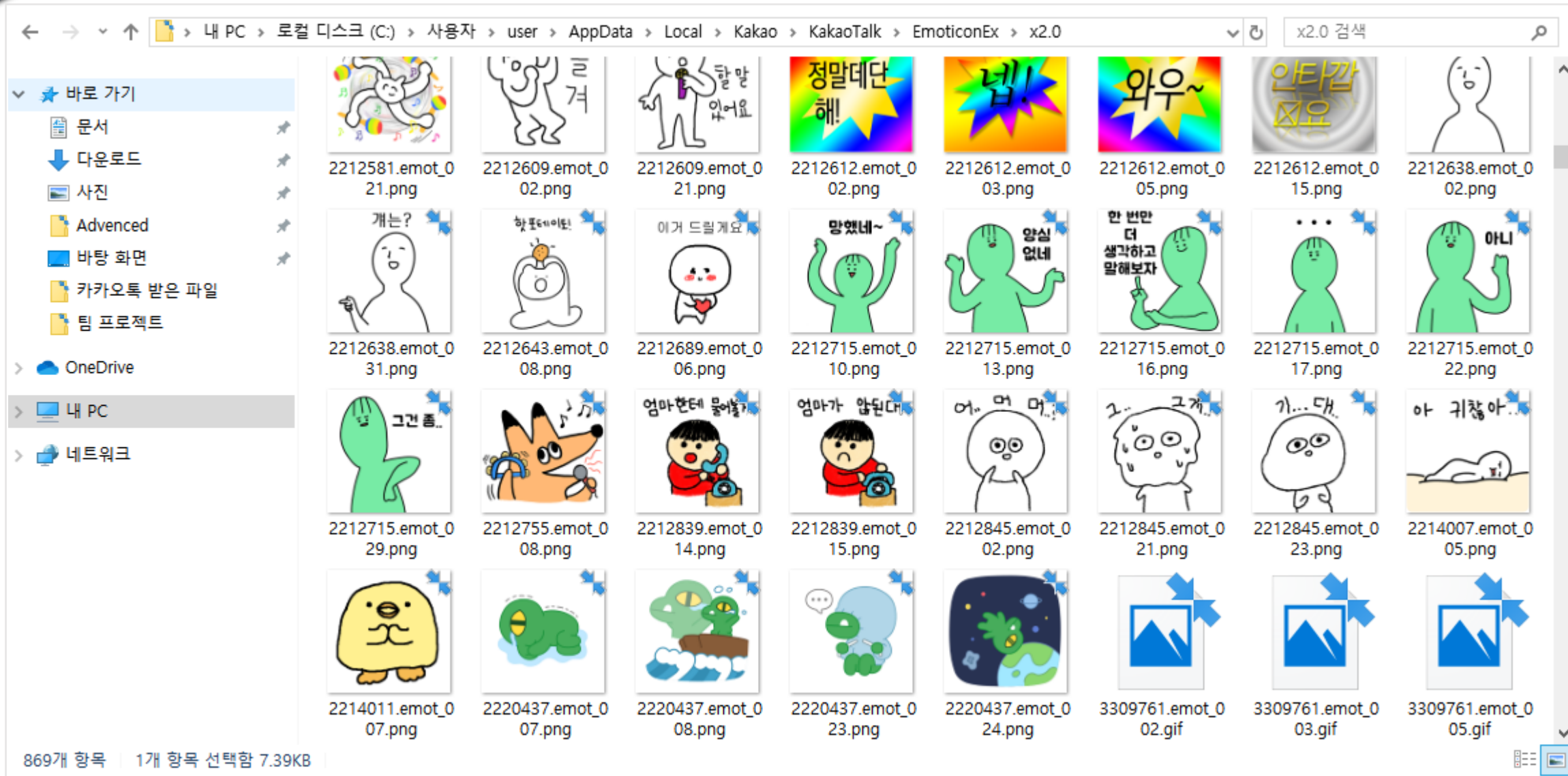
Process Monitor



API Monitor



CUCKOO Sandbox



EmoticonEx -> 나 or 상대방이 사용했던 이모티콘이 사진 파일로 저장

Thank You

TALK



Coming Soon!