2022.09.17.SAT

김민주 최민주 최유진

[PROJECT]

SWFS APP FORENSICS

: INSTAGRAM

목차

① 상황 설정 : DM (Direct Message)

#인플루언서 #계정사칭

계정사칭 후 위장

인스타그램 유명 인플루언서의 계정을 사칭하고 공동구매 마켓을 여는 것으로 위장하여, 조작된 링크를 통해 현금을 챙기는 방식으로 불특정 다수에게 피해를 입힌다.

실습에서는 마켓에 관련된 문의를 받으며 사기치는 과정을 담는다.

② 실습 게시물 _ DM

#앰플 #마켓위장 #공구사기

공구 홍보 게시물을 업로드한 후, 관련 문의를 dm으로 받으며 사기치는 과정을 담는다.

앰플 1차 공구 시작
#앰플 #속건조 #복합성
공구 6/X~7/X 단독 공구 진행
❤가격 문의 등 기타 문의는 디엠으로 부탁드려요~
❤최소한의 예의를 갖춰주세요

② 실습 메세지 _ DM

실습을 위한 인스타그램 공용 계정을 따로 개설한다.

가해자 – 공용 계정
피해자 – 팀원의 개인 인스타그램 계정

피해자: (게시물을 같이 보내며) 앰플 공구 문의드려요! 속건조 타입도 당김 없이 사용 가능하나요?
가해자: 넵~고객님 가볍게 사용 가능하세요~
피해자: 구매하고 싶은데 결제는 어디서 하면 될까요?
가해자: 제 프로필 상단에 링크 들어가셔서 결제하시면 됩니다 감사합니다~

② 실습 진행 방향 & 계획 _ DM

1) 가해자의 계정을 이용해 피해자들의 계정에 dm을 전송
   가해자의 계정은 실습용 공용 계정으로, 피해자의 계정을 팀원들의 계정을 사용해 실습 진행
2) direct.db를 확인 -> 메시지의 전송시각, 수신자, 발신자 등을 확인
   direct.db에서 활용할 tool은 실습 진행하면서 유동적으로 결정
3) cookies를 통해 인스타그램을 이용한 가해자의 행위 입증
   ex) 특정 아이디를 로그인한 시간 추정

② 실습 진행 방향 & 계획 _ DM

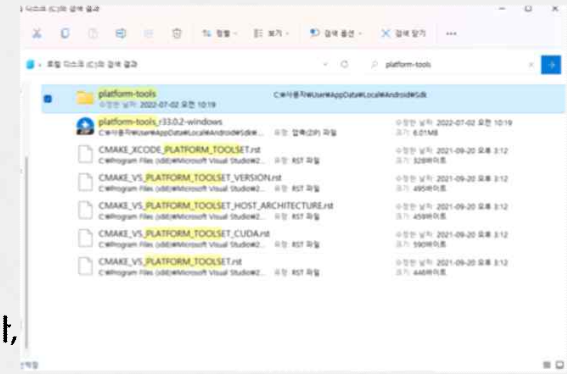
앞선 슬라이드에서 말한 방식으로 최대한 실습을 진행하려고 했지만, 실습 과정에서 실습 환경 설정이나 예상치 못한 여러 변수들로 인해 실습을 설정했던 방향대로 진행하는 데 어려움을 겪음.

1) 기

2) d

3) cookies를 통해 인스타그램을 이용한 가해자의 행위 입증
ex) 특정 아이디를 로그인한 시간 추정

③ 실습 진행 시도 _ DM



1) ADM을 통해 실습을 진행하려고 시도

-터미널을 이용해서 실행시키는 방법

Platform-tools를 검색하여 중간 경로를 탐색

발견한 중간 경로를 터미널 창에 입력하고

모니터 창을 확인했으나 모니터가 실행이 되지 않아,

실습 진행 불가 X.

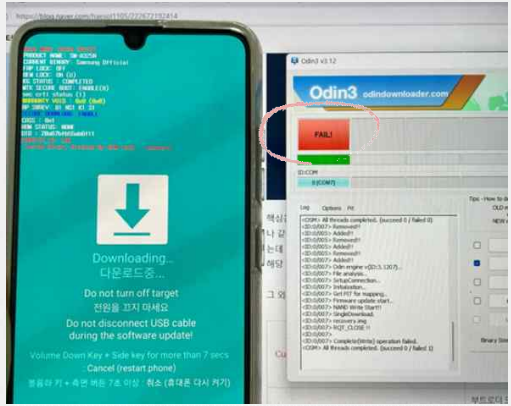
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
새로운 기능 및 개선 사항에 대한 최신 PowerShell을 설치하세요! https://aka.ms/PSWindows
PS C:\Users\User\AndroidStudioProjects\TRY2> cd C:\사용자\user\AppData\Local\Android\Sdk\tools
cd : 'C:\사용자\user\AppData\Local\Android\Sdk\tools' 경로는 존재하지 않으므로 찾을 수 없습니다.
위치 줄:1 문자:1
+ cd C:\사용자\user\AppData\Local\Android\Sdk\tools
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (C:\사용자\user\App...droid\Sdk\tools:String) [Set-Location], I
te    mNotFoundException
    + FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.SetLocationCommand
```

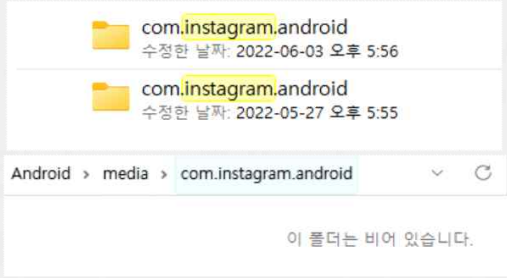
③ 실습 진행 시도 _ DM

2) Autopsy 4.19.1, SQL Browser
& SQL Browser 사용한 실습 시도

-com.instagram.android 디렉토리에서
direct.db를 찾아 dm의 로그를 파악하고자 함.

-계속되는 안드로이드 폰 루팅 실패로 인해
com.instagram.android 폴더에서 dm에 관련된

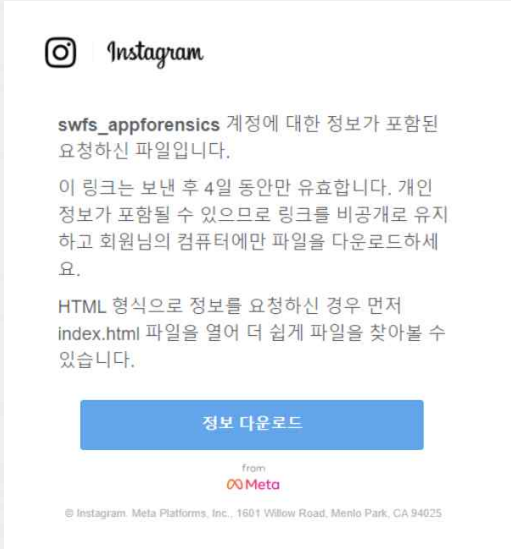




③ 실습 진행 _ DM

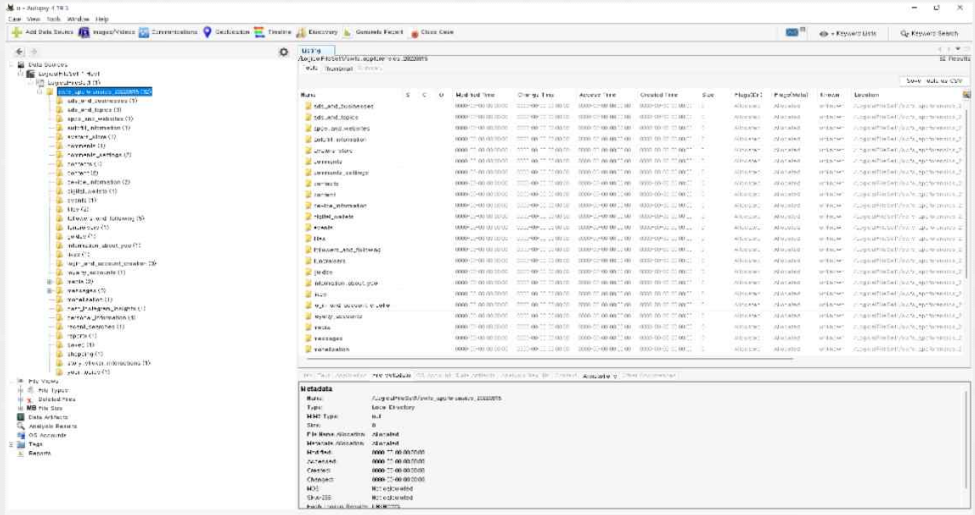
1) Autopsy 4.19.1

데이터 추출 : 사용한 안드로이드 폰의 인스타그램 데이터를 다운받아서 이를 이용해 실습을 진행했습니다.



③ 실습 진행 _ DM

데이터 파일을 'Autopsy' 라는 도구에 넣어 파일들을 차례로 열어보면서 분석을 진행하였다.



③ 실습 진행 _ DM

여러 파일 중에서 messages파일을 살펴보았더니 inbox 파일과 chat.html, secret_conversations.html이 포함됨을 확인할 수 있었다.

③ 실습 진행 _ DM

html파일에선 채팅을 주고받은 사람의 이름을 확인할 수 있었다.

inbox파일에선 message_1.html 등 message관련 html파일들을 확인했다.

- 시나리오상 가해자와 피해자가 주고받은 dm 내용과 주고 받은 시간들을 모두 찾을 수 있었다.

③ 실습 진행 _ DM

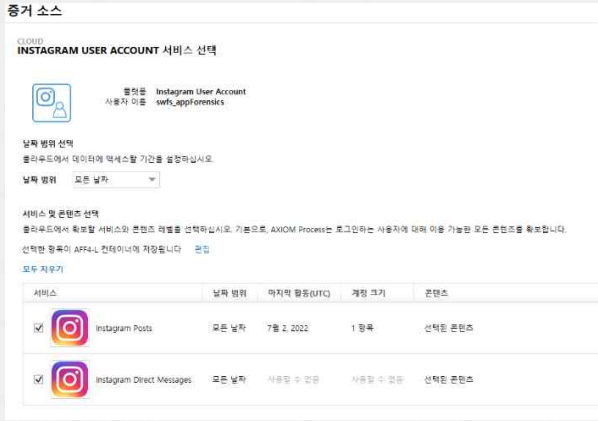
Dm을 전송한 사람의 이름이 한글로 되어있을 경우 조금 깨지는 부분이 있긴 했지만, dm내용과 dm을 전송한 시간들을 모두 찾아낼 수 있었습니다.

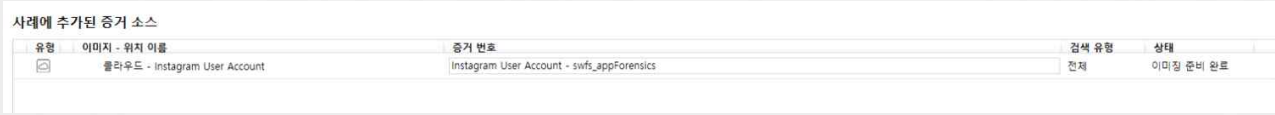
③ 실습 진행 II _ DM

2) Magnet Axiom 툴 사용한 실습 진행

Magnet은 디지털 포렌식 수사 플랫폼이다. 하나의 컴퓨터에서 컴퓨터, 스마트폰, 클라우드 등 데이터를 수집하고 처리하는 플랫폼이다.

인스타그램 포렌식을 선택 후 'INSTAGRAM USER ACCOUNT' 서비스를 선택해 준 후, 로그인이 완료되면 날짜, 상세정보 분석 등의 세팅이 완료되면 이미징이 시작됩니다.





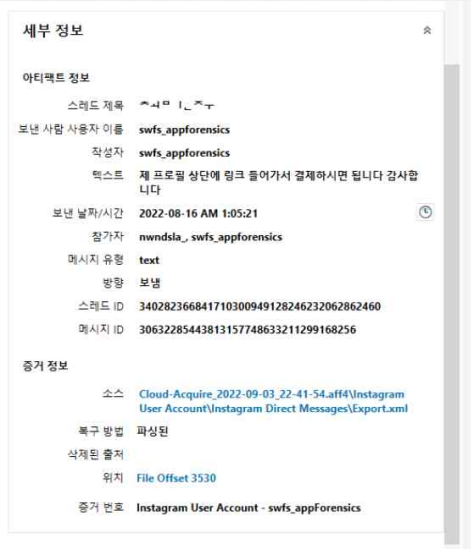
③ 실습 진행 II _ DM

Magnet Axiom Process : 증거 분석 작업

Magnet Axiom Examine : 사용자에게 쉽고 익숙한 방식으로 증거를 보여준다.

콘텐츠 유형에서 대화를 선택하면 dm 내용을 확인할 수 있다.

③ 실습 진행 II _ DM



DM 참가자, 발신자 수신자의 이름과 ID, 텍스트열, 보낸 날짜와 시간 모두 확인할 수 있었다.

이로인해 시나리오상 가해자가 피해자에게 링크를 알려주며 결제유도를 한 대화 내용을 증거로써 수집할 수 있었다.

④ 상황 설정 : 스토리(Story)

#학교폭력

학폭 증거 수집

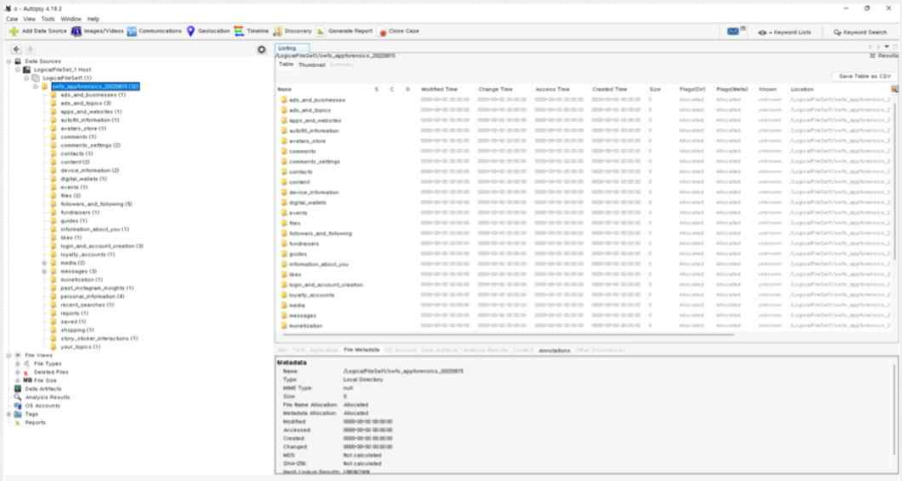
학교 폭력을 주도한 가해자가 피해자를 괴롭히는 장면을 찍어 인스타그램 본인 계정의 스토리에 올려 희롱하고 24시간 이내 스토리를 삭제함.

가해자의 학교 폭력 사실 확인과 사진의 업로드를 입증하기 위해 로그 추적 및 삭제한 스토리 복구하는 실습을 진행한다.

④ 실습 스토리 예시

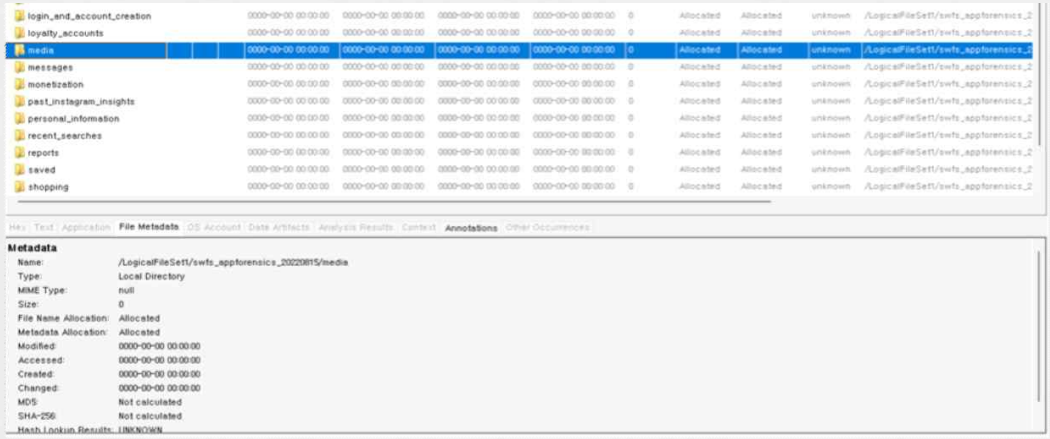
이번에도 공용 계정을 가해자의 계정으로 설정하여
스토리 실습을 진행함.

④ 실습 진행 _ 스토리



마찬가지로, 데이터 파일을 'Autopsy' 라는 도구에 넣어 파일들을 차례로 열어보면서 분석을 진행함.

④ 실습 진행 _ 스토리

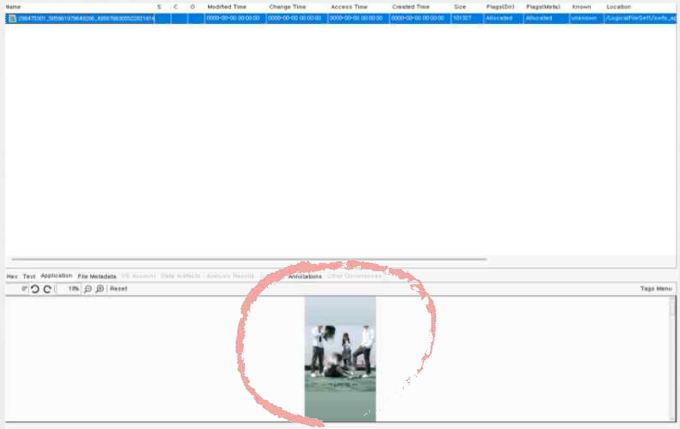


여러 파일들을 확인했고, 그 중에서 media 파일에 주목했다.

④ 실습 진행 _ 스토리

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
posts				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/swfs_appforensics_20220815/medi...
stories				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/swfs_appforensics_20220815/medi...

media의 하위 파일에 stories 파일이 있어서 스토리에 관련된 파일로 짐작하고 이를 확인해보았다.

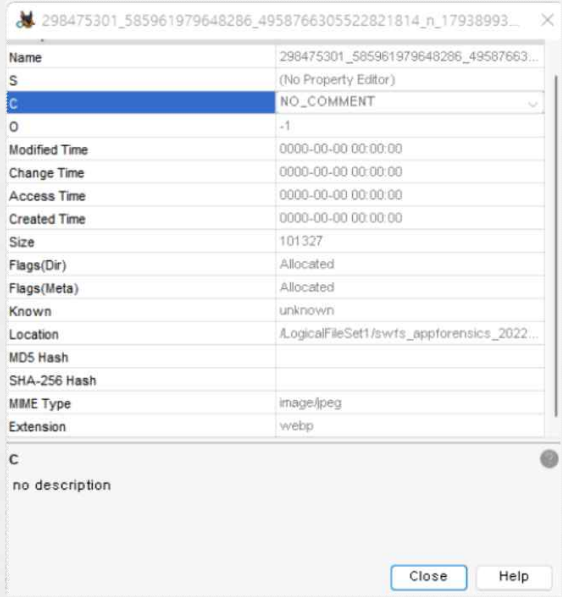


파일을 열어봤더니 사진 파일이 하나 들어있었고, 확인을 위해 눌러봤더니 시나리오 상에 있는 스토리임을 알 수 있었습니다.

④ 실습 진행 _ 스토리

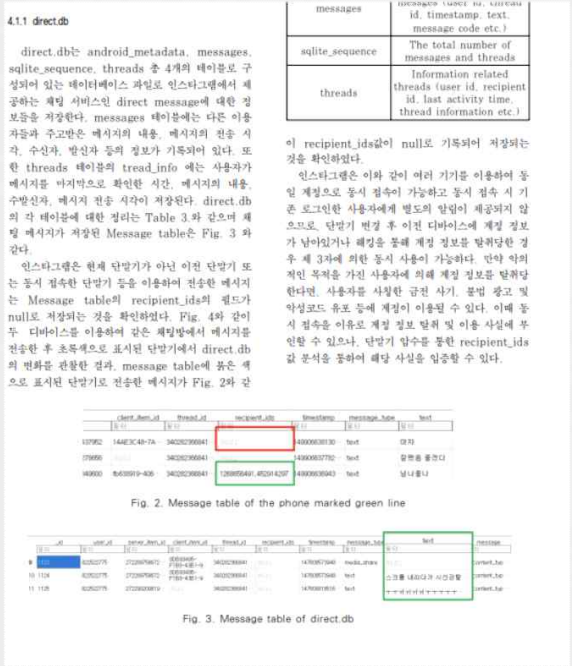
해당 사진의 'properties'를 살펴봤더니 'created time'을 포함한 여러 정보들이 제대로 반영되지 않은 듯 하다.

이 부분에 대해 'created time'이 정확히 설정되지 않아서 생성시간을 알 수 없었다는 점이 아쉬웠다.



참고 논문

[모바일 포렌식 연구를 위한 서드 파티 어플리케이션 분석]
[데이터 획득방법에 따른 최신 삼성 스마트폰의 시스템 로그 분석과 포렌식 활용기법]
[디지털 포렌식 관점에서의 인스타그램 사용자 행위 분석]
[NAND 플래시 메모리에서 디지털 포렌식을 위한 파일 복구기법]
[NAND 플래시 메모리에서 블록치환을 이용한 삭제파일 복구 방지]
[데이터 획득방법에 따른 최신 삼성 스마트폰의 시스템 로그 분석과 포렌식 활용 기법]
[무결성 향상을 위한 모바일 포렌식 모델 연구]
[모바일 포렌식 증거 수집방안 연구 : 제조사 백업 앱 기반 데이터 획득 기법]
[불법촬영 범죄 대응을 위한 현장용 모바일 포렌식 도구 개발에 관한 연구]



4.1.1 direct.db

direct.db는 android_metadata, messages, sqlite_sequence, threads 총 4개의 테이블로 구성되어 있는 데이터베이스 파일로 인스타그램에서 제공하는 채팅 서비스인 direct message에 대한 정보들을 저장한다. messages 테이블에는 다른 이용자들과 주고받은 메시지의 내용, 메시지의 전송 시각, 수신자, 발신자 등의 정보가 기록되어 있다. 또한 threads 테이블의 tread_info 에는 사용자가 메시지를 마지막으로 확인한 시간, 메시지의 내용, 수발신자, 메시지 전송 시각이 저장된다. direct.db의 각 테이블에 대한 정리는 Table 3.와 같으며 채팅 메시지가 저장된 Message table은 Fig. 3 와 같다.

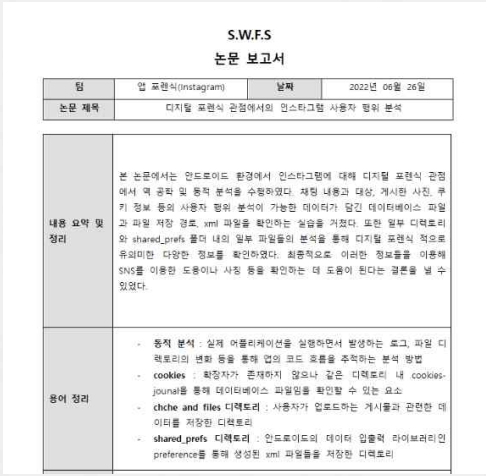
인스타그램은 현재 단말기가 아닌 이전 단말기 또는 동시 접속한 단말기 들을 이용하여 전송한 메시지는 Message table의 recipient_ids의 필드가 null로 저장되는 것을 확인하였다. Fig. 4와 같이 두 디바이스를 이용하여 같은 채팅방에서 메시지를 전송한 후 초록색으로 표시된 단말기에서 direct.db의 변화를 관찰한 결과, message table에 붉은 색으로 표시된 단말기로 전송한 메시지가 Fig. 2와 같이 recipient_ids값이 null로 기록되어 저장되는 것을 확인하였다.

messages	messages (user id, thread id, timestamp, text, message code etc.)
sqlite_sequence	The total number of messages and threads
threads	Information related threads (user id, recipient id, last activity time, thread information etc.)

인스타그램은 이와 같이 여러 기기를 이용하여 동일 계정으로 동시 접속이 가능하고 동시 접속 시 기존 로그인한 사용자에게 별도의 알림이 제공되지 않으므로, 단말기 변경 후 이전 디바이스에 계정 정보가 남아있거나 해킹을 통해 계정 정보를 탈취당한 경우 제 3자에 의한 동시 사용이 가능하다. 만약 악의적인 목적을 가진 사용자에 의해 계정 정보를 탈취당한다면, 사용자를 사칭한 금전 사기, 불법 광고 및 악성코드 유포 등에 계정이 이용될 수 있다. 이때 동시 접속을 이유로 계정 정보 탈취 및 이용 사실에 부인할 수 있으나, 단말기 암수를 통한 recipient_ids 값 분석을 통하여 해당 사실을 입증할 수 있다.

Fig. 2. Message table of the phone marked green line

Fig. 3. Message table of direct.db



S.W.F.S

논문 보고서

팀	업 포렌식(Instagram)	날짜	2022년 06월 26일
논문 제목	디지털 포렌식 관점에서의 인스타그램 사용자 행위 분석		

내용 요약 및 정리	본 논문에서는 안드로이드 환경에서 인스타그램에 대해 디지털 포렌식 관점에서 역 공학 및 동적 분석을 수행하였다. 채팅 내용과 대상, 게시한 사진, 쿠키 정보 등의 사용자 행위 분석이 가능한 데이터가 담긴 데이터베이스 파일과 파일 저장 경로, xml 파일을 확인하는 실습을 거쳤다. 또한 일부 디렉토리와 shared_prefs 폴더 내의 일부 파일들의 분석을 통해 디지털 포렌식 적으로 유의미한 다양한 정보를 확인하였다. 최종적으로 이러한 정보들을 이용해 SNS를 이용한 도용이나 사칭 등을 확인하는 데 도움이 된다는 결론을 낼 수 있었다.
용어 정리	- **동적 분석** : 실제 어플리케이션을 실행하면서 발생하는 로그, 파일 디렉토리의 변화 등을 통해 앱의 코드 흐름을 추적하는 분석 방법 - **cookies** : 확장자가 존재하지 않으나 같은 디렉토리 내 cookies-journal을 통해 데이터베이스 파일임을 확인할 수 있는 요소 - **chche and files 디렉토리** : 사용자가 업로드하는 게시물과 관련한 데이터를 저장한 디렉토리 - **shared_prefs 디렉토리** : 안드로이드의 데이터 입출력 라이브러리인 preference를 통해 생성된 xml 파일들을 저장한 디렉토리

[디지털 포렌식 관점에서의 인스타그램 사용자 행위 분석]

-4.1.1 발췌

왼쪽 같이 direct.db에 관련한 내용처럼 실습에 필요한 부분들 위주로 읽어보고 논문 보고서를 작성하여 공부한 부분을 정리했습니다.

느낀점

실습 환경을 마련하는 것부터 난관을 만나서 어려운 점이 많았습니다.
여러 시행착오를 거쳤음에도 불구하고 생각대로 진행되지 않았던 점들도 있었지만
이번 프로젝트를 진행하면서 배운 게 더 많은 것 같다고 생각합니다.
다음에 기회가 있다면 그땐 이번 실습 때의 한계를 극복하며 폭넓은 포렌식 실습을
진행하는 것을 목표로 삼고 싶습니다.

감사합니다.