

Mobile Forensics 실습

강수진

국민대학교 금융정보보안학과, DF&C 연구실

dfnc@kookmin.ac.kr

CONTENTS

01

모바일 포렌식 도구

02

모바일 포렌식 실습

01

모바일 포렌식 도구

1. 모바일 포렌식 도구

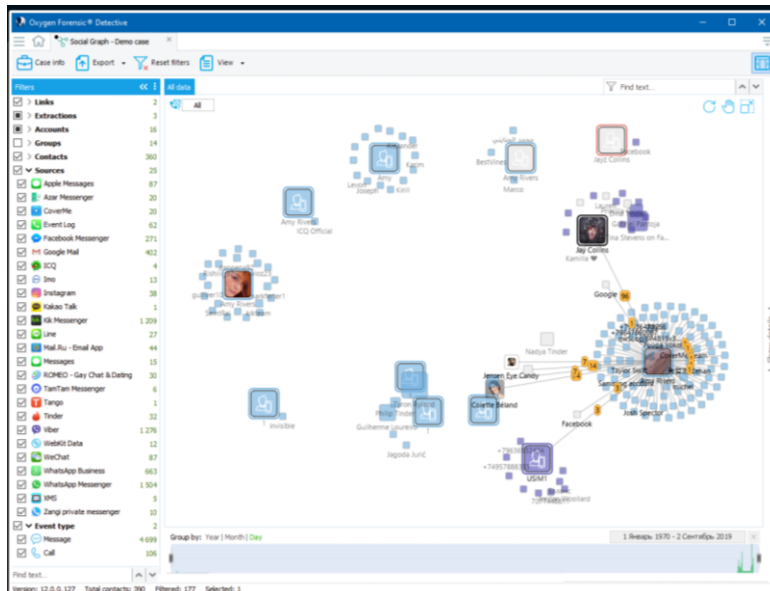
- OXYGEN FORENSIC
- MAGNET AXIOM
- MD-NEXT, MD-RED
- FINALDATA



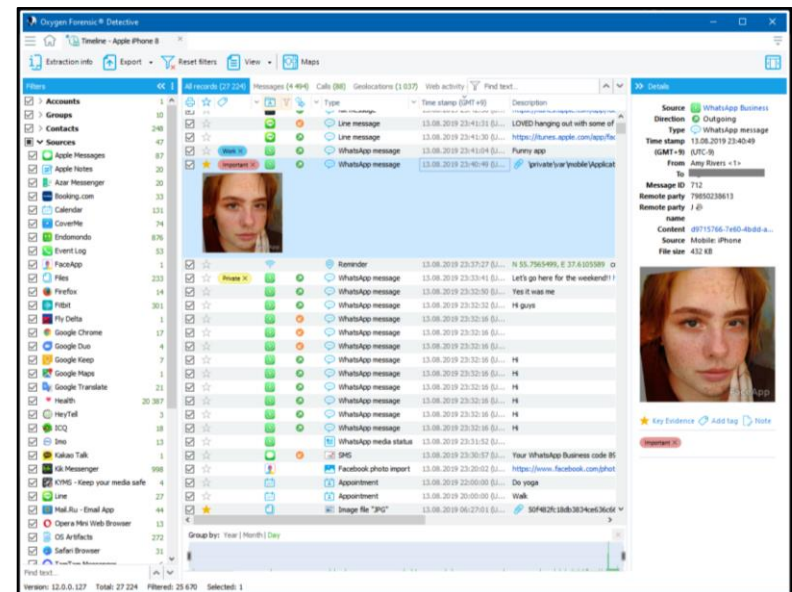
1. 모바일 포렌식 도구

■ OXYGEN FORENSIC

- 모바일 기기, IoT 장치, 백업 데이터, SIM 및 외장 미디어 카드, 드론 및 클라우드 서비스로부터 데이터 추출 및 분석
- 화면 잠금 우회, 암호화된 백업의 암호 찾기, 삭제된 데이터 추출 기능 제공
- 데이터 간의 연결성 찾기, 타임 라인 및 이미지 분류 기능 제공



[소셜 그래프 분석 화면]



[타임 라인 분석 화면]

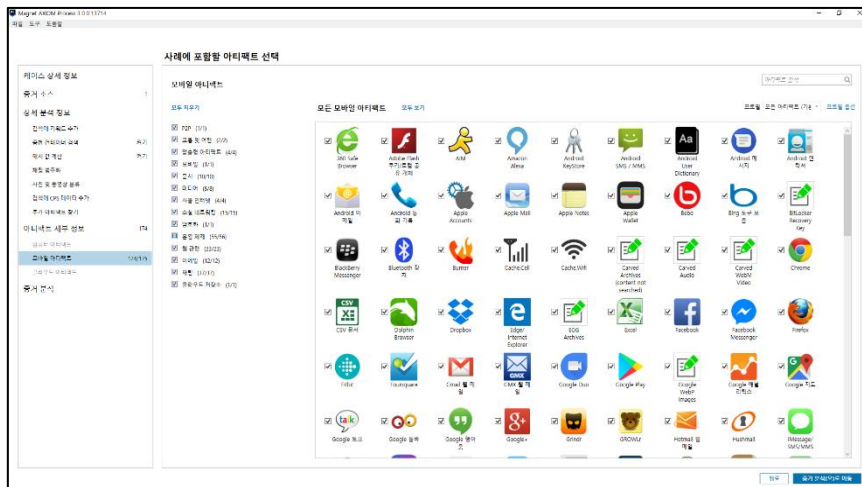
1. 모바일 포렌식 도구

▪ Magnet ACQUIRE

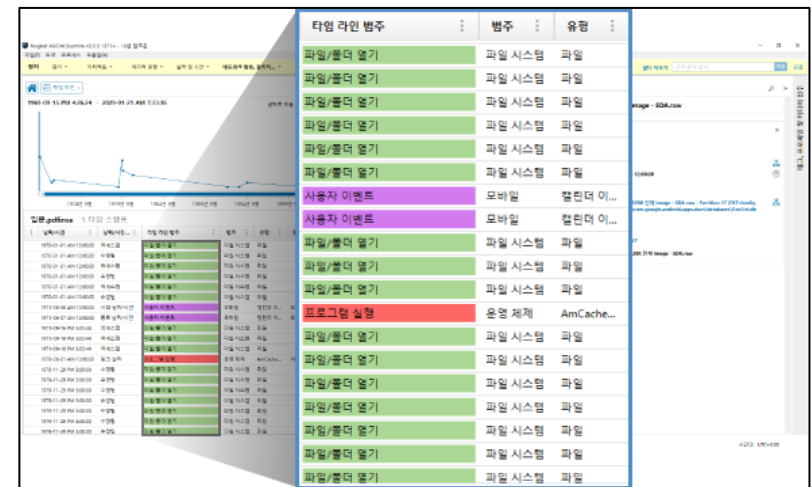
- 데이터 추출 도구로 이를 통해 추출된 스마트폰 증거 데이터는 Magnet AXIOM 또는 기타 모바일 포렌식 도구를 통해 분석 가능

▪ MAGNET AXIOM

- 추출된 데이터의 분석 도구로 아티팩트간 연관분석을 기반한 시각화 제공
- 삭제 / 복구 / 생성 / 수정 / 파일의 공유 / 변경 등의 모든 행위를 기록하여 타임라인 기능 제공



[데이터 분석 화면]



[타임라인 화면]

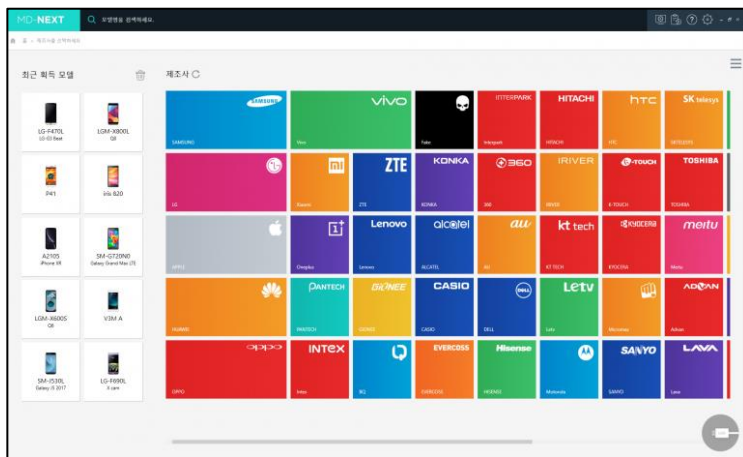
1. 모바일 포렌식 도구

■ MD-NEXT

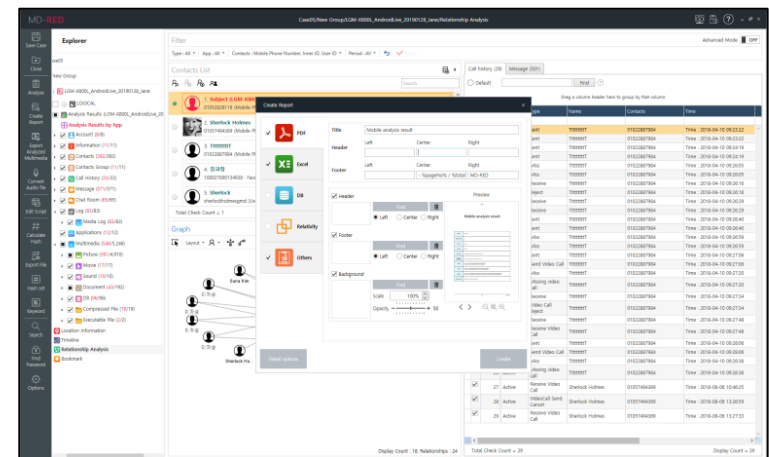
- 스마트폰, 피쳐폰, 드론, 스마트티비, 웨어러블 기기, IoT 기기, USIM카드, SD 메모리 카드 등의 저장 장치의 데이터를 스캔하고 데이터 추출
- Android, iOS 등의 다양한 OS 지원

■ MD-RED

- 모바일 및 디지털 기기로부터 추출한 데이터의 복구, 복호화, 시각화, 분석 및 보고서 생성 기능을 제공



[MD-NEXT 초기화면]



[MD-RED 시각화 화면]

1. 모바일 포렌식 도구

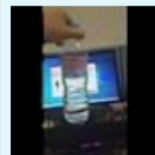

■ MD-RED

• 보고서

모바일 분석 보고서

모델	SM-G950N
제조사	SAMSUNG
파일 종류	Physical (MoviNand)
파일 크기	54.8GB
파일 이름	SM-G950N_Physical_20191125_USERDATA.mdf
획득 일시	2019-11-25 16:31:16 ~ 2019-11-25 17:31:31
SHA256	획득: 7A9655668F079304651A4C1A93AFF2C79B953E99DC83034B3519550A276AAA70 검증: 7A9655668F079304651A4C1A93AFF2C79B953E99DC83034B3519550A276AAA70
분석 도구	MD-RED v3.4.11.439

동영상

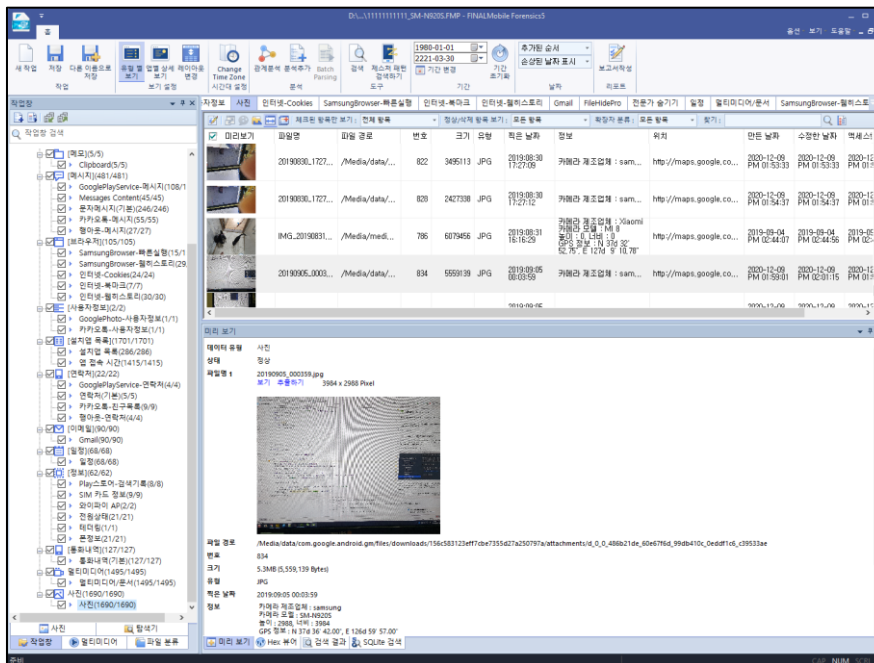
상태	속성	종류	미리 보기	크기 정보	날 짜	App
활성	일반	MP4		너비 : 1,280 높이 : 720 파일 크기 : 9,122,492 오프셋 : 0	생성 일시 : 2019-09-26 16:52:21 수정 일시 : 2019-09-26 16:52:46 접근 일시 : 2019-09-26 16:52:21 변경 일시 : 2019-09-26 16:52:46 재생 시간 : 00:00:08	기본
경로 : /media/0/DCIM/Camera 파일 이름 : 20190926_165221.mp4 촬영 일시 : 2019-09-26 16:52:29 저장 일시 : 2019-09-26 16:52:29 <div> MD5 : C413D87ECD6D95EF1DF4DD36F946F8E SHA1 : 5EECCB2DE631095AEDBD82E05A45A13D81F40AAE SHA256 : 6C85C501761718729973CEBDE5D83BF7E48CBE8B22DB713079ECA1B4FA014E57 </div>						
활성	일반	MP4		너비 : 1,920 높이 : 1,080 파일 크기 : 10,787,641 오프셋 : 0	생성 일시 : 2019-09-26 15:32:49 수정 일시 : 2019-09-26 15:32:56 접근 일시 : 2019-09-26 15:32:49 변경 일시 : 2019-09-26 15:32:56 재생 시간 : 00:00:05	기본
경로 : /media/0/DCIM/Camera 파일 이름 : 20190926_153249.mp4 촬영 일시 : 2019-09-26 15:32:56 저장 일시 : 2019-09-26 15:32:56 <div> MD5 : 29A579FBCCEE3C4860A2FF254D2F18268 SHA1 : BDED9461A2FEC7CA05E99527B9DF7DE7DA656EAC SHA256 : 61F625523750AAA3F38F890B17429D45615C1977734CF5253C833BE4F3A455B3 </div>						

[MD-RED 보고서 일부]

1. 모바일 포렌식 도구

FINALDATA

- 스마트폰, 태플릿, 피쳐폰, SD 메모리 카드나 USIM 으로부터 데이터 추출 및 분석
- 관계 분석 제공
 - 대화 내용을 인물 관계 중심으로 추출 (Contact Line), 대화 내용을 시간 중심으로 추출 (Time Line)
- PDF, Excel, HTML 형식의 보고서지원



[사진 분석 화면]

2. 증거 이미지

1) 획득 이미지 정보

증거 파일 경로	20210517_m20_SM-M205G.mef
증거 파일 크기	9.7MB
MEF 버전	MEF 2.0
비밀번호 보호	No
덤프 압축	No
분석권	default-user
분석 기관	organization
분석 부서	department
확인	Samsung
모델명	SM-M205F
모델명	SM-M205G
미디어 번호	1

2) 해시값 확인

파일 이름	20210517_m20_SM-M205G.mef
파일 크기	9.7MB (10,136,092 Bytes)
SHA-1 해시값	8B7E8696FBB64726F614C774512C17314F1C914D
검증된 SHA-1 해시값	8B7E8696FBB64726F614C774512C17314F1C914D

3) 미디어 정보

1. 미디어01

- 미디어 유형: MEF2
- 플러그인: SamsungBackupRev1.dll
- 미디어 파일 크기: 9.7MB
- 파일 수: 821
- 획득 시간: 2021-05-17 13:40:37
- 덤프 유형: File

[보고서 일부]

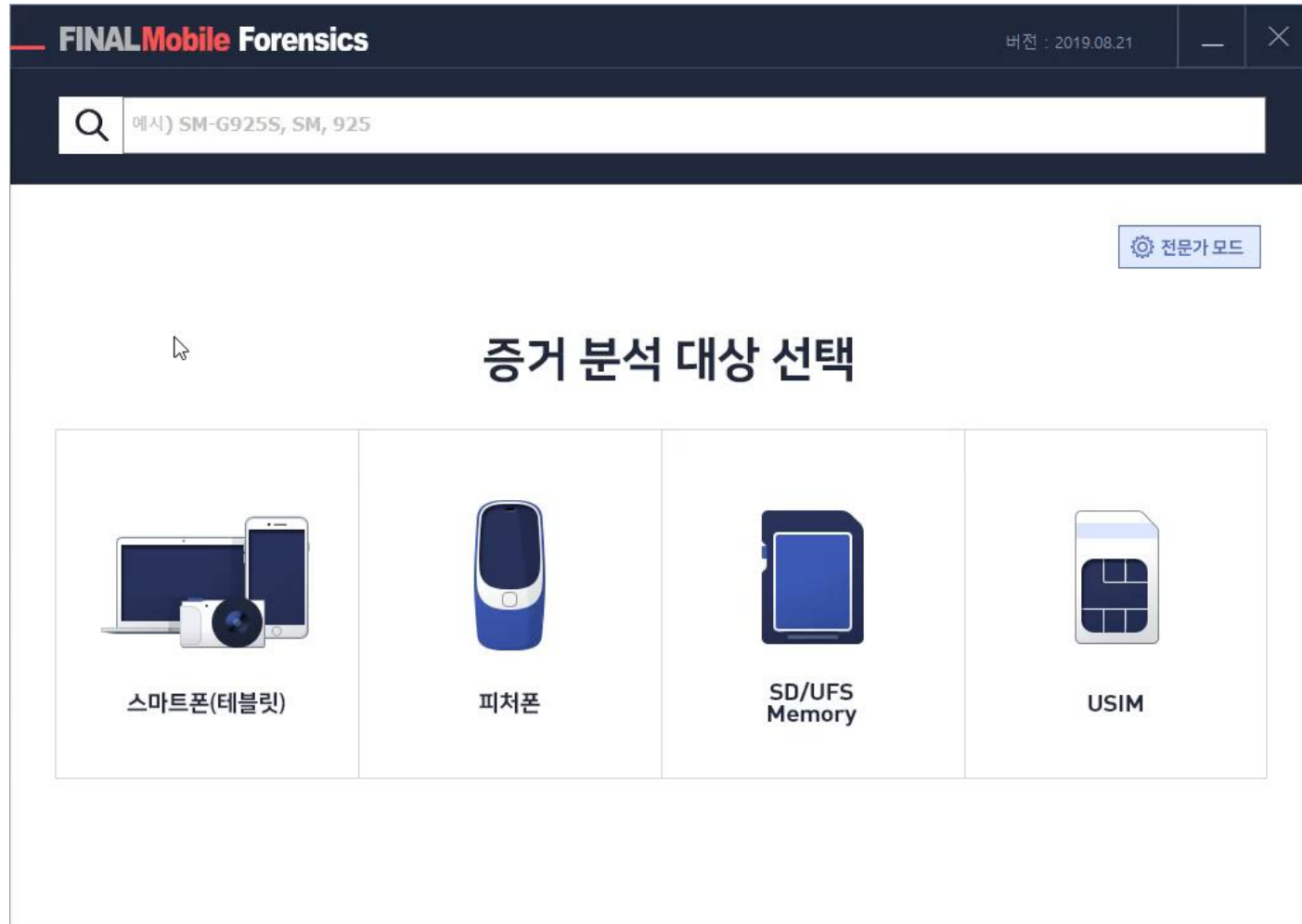
1. 모바일 포렌식 도구

▪ FINALDATA - 기능



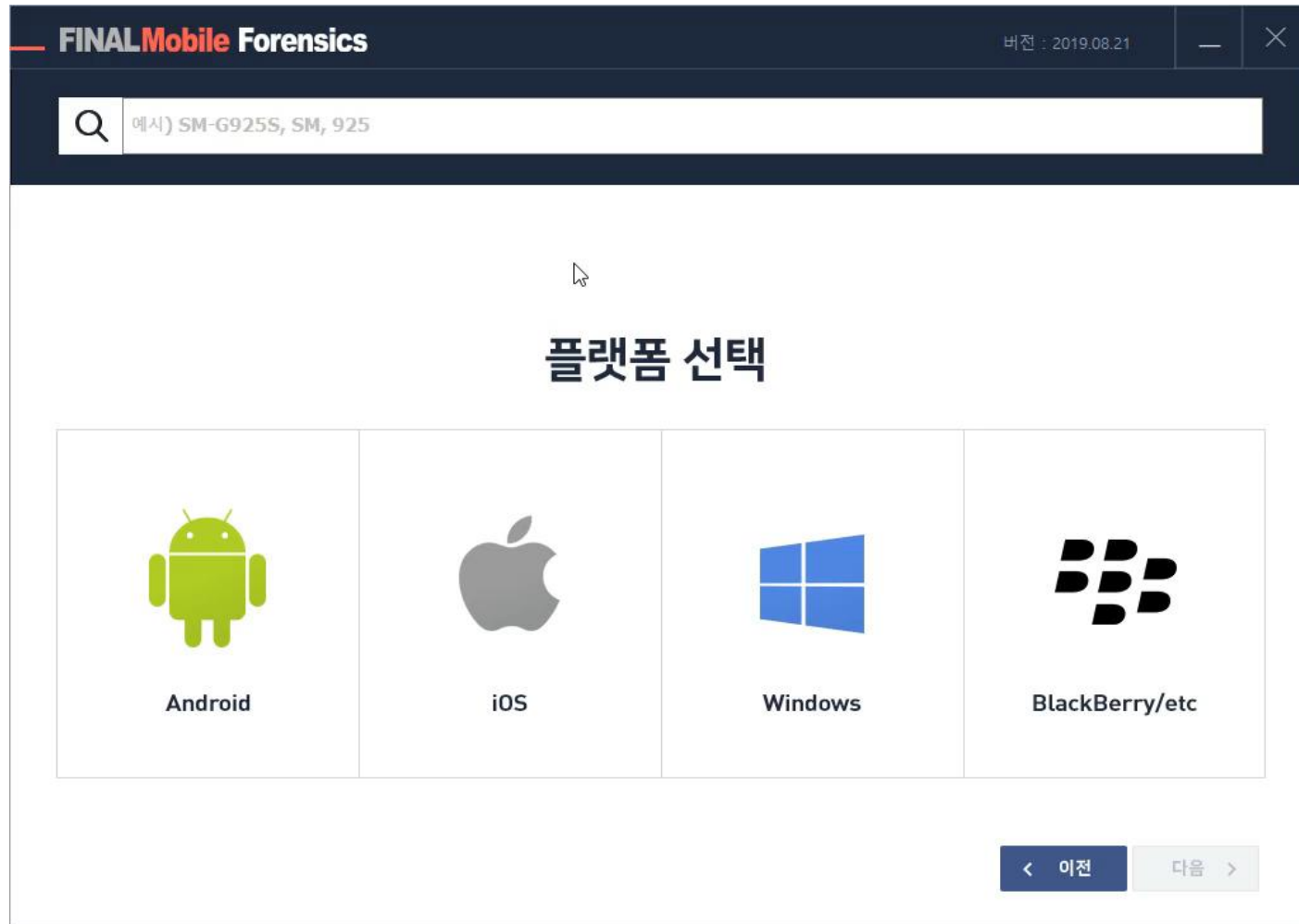
1. 모바일 포렌식 도구

- FINALDATA - 기능
 - 데이터 획득 과정



1. 모바일 포렌식 도구

- FINALDATA - 기능
 - 데이터 획득 과정



1. 모바일 포렌식 도구

▪ FINALDATA - 기능

- 증거 획득 보고서

데이터 추출 과정 시
입력한 사용자 정보

디지털 증거 획득 결과 보고서

1. 획득 사용자 정보

분석관 이름 : default-user
소속 : organization
소속부서 : department
사건 번호 : 20210517

2. 폰 정보

제조사 : Samsung
모델명 : SM-G960N (Galaxy S9)
소유자 이름 : 홍길동
휴대폰 번호 : 01011112222

3. 획득 정보

1) 제품 버전 : 2019.08.21

2) 작업 시간

Local Time	2021-05-17 12:53:00 ~ 2021-05-17 13:00:10
GMT	2021-05-17 03:53:00 ~ 2021-05-17 04:00:10
소요 시간	7 분 10 초

3) mef file

파일 이름	20210517_SM-G960N.mef
파일 크기	1,903,644,996 bytes
SHA-1 해시값	0ACC300F43BEE68A8B79173DE1C6B1A4E9C0B1FC

4. 추출된 파일 목록

* 추출된 파일에 대한 해시값은 다음 파일에 있습니다.

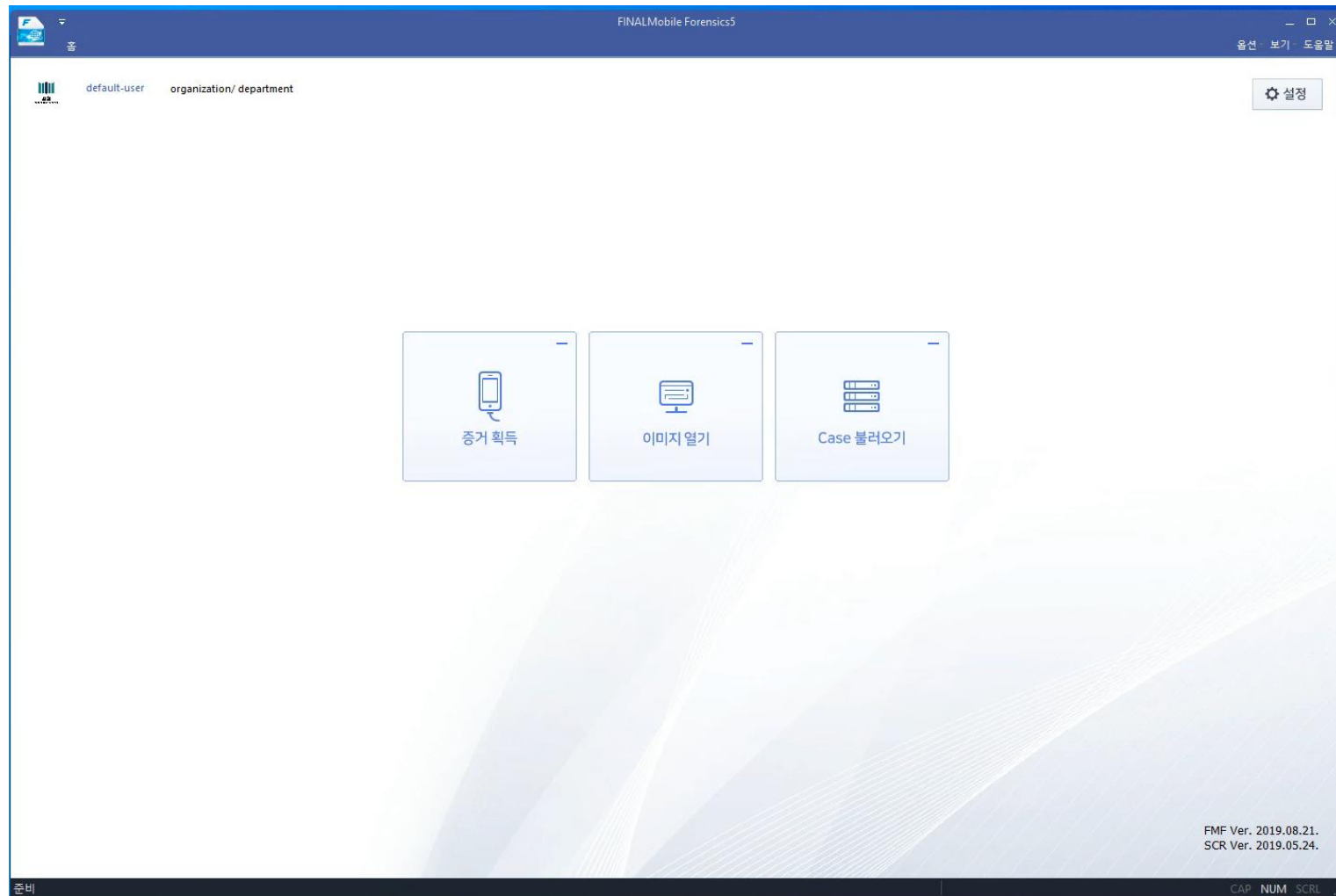
파일 이름	20210517_SM-G960N.FileHash.csv
파일 크기	383,885 bytes
SHA-1 해시값	93372113A86E8065D895240DBF5945A6BBB8DECE

추출된 데이터의 크기 및 해시값

1. 모바일 포렌식 도구

▪ FINALDATA - 기능

- 데이터 분석 과정



1. 모바일 포렌식 도구

▪ FINALDATA - 기능

- 데이터 분석 화면 - 사용자 정보

The screenshot displays the FINALDATA Mobile Forensics 5 software interface. The main window shows a list of extracted data items on the left and a detailed view of the 'User Information' (사용자 정보) category on the right. The 'User Information' section is highlighted with a red box, and its details are shown in the '미리 보기' (Preview) pane at the bottom.

Left Panel (Tree View):

- 20210517_SM-G960N.mef
 - [분석 목록](1058/1058)
 - [멀티미디어첩](2/2)
 - NQVault(1/1)
 - 녹음 파일(1/1)
 - [메시지](10/10)
 - Messages Content(2/2)
 - 문자메시지(기본)(8/8)
 - [사용자정보](1/1)
 - GooglePhoto-사용자정보(1/1)
 - [설치업 목록](2/2)
 - 설치업 목록(2/2)
 - [연락처](17/17)
 - 연락처(기본)(17/17)
 - [일정](43/43)
 - 일정(43/43)
 - [정보](11/11)
 - 폰정보(11/11)** (highlighted)
 - [통화내역](506/506)
 - 통화내역(기본)(506/506)
 - 멀티미디어(116/116)
 - 멀티미디어/문서(116/116)
 - 사진(350/350)
 - 사진(350/350)

Right Panel (Data List):

번호	이름	값
1	계정 : com.google	do[redacted]@gmail.com
2	계정 : com.google	[redacted]5@gmail.com
3	빌드번호	G960NKSU2DTAB
4	기기 이름	SM-G960N
5	계정 : com.whatsapp	WhatsApp
6	제품명	Galaxy S9
7	전화번호	010[redacted]
8	Mobile Id (IMEI)	356069090455457
9	시리얼	R39K502MLZ
10	최초 통화일	20180629
11	표준시간대	Asia/Seoul

Bottom Panel (미리 보기 - Preview):

데이터 유형	폰정보
상태	정상
이름	계정 : com.google
값	do[redacted]@gmail.com

1. 모바일 포렌식 도구

FINALDATA - 기능

- 데이터 분석 화면 - 연락처

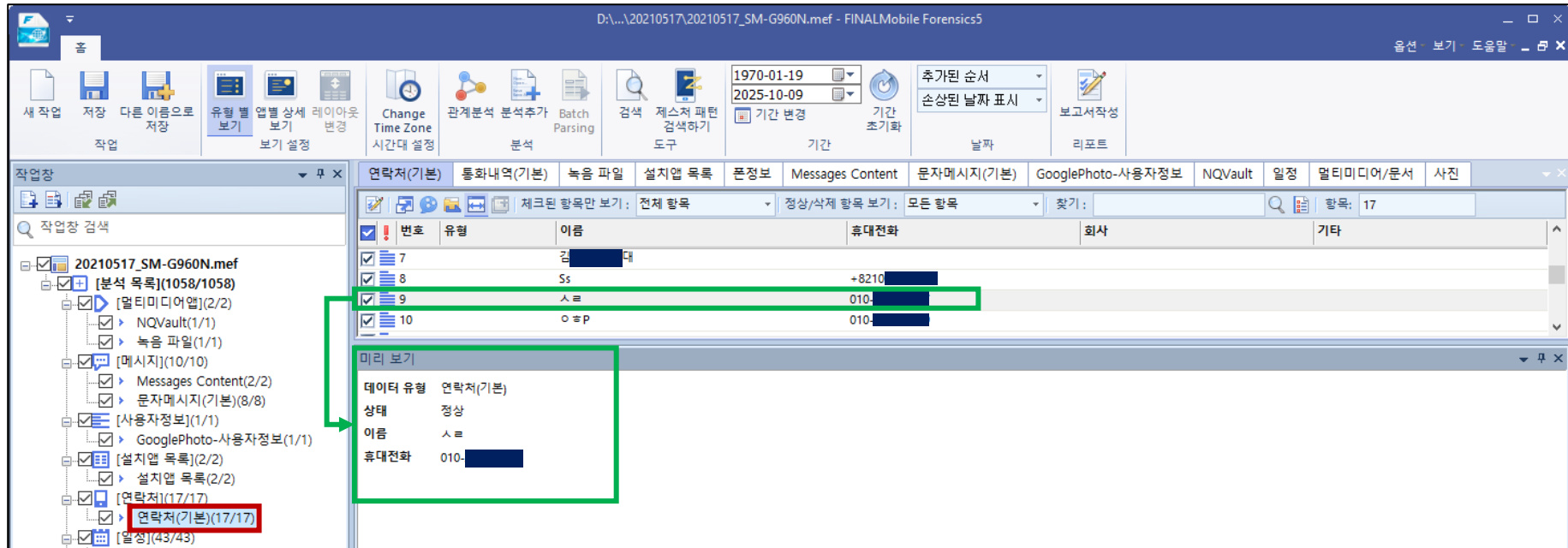


Table:

data

Filter in any column

	_id	package_id	mimetype_id	raw_contact_id	hash_id	is_read_only	is_primary	is_super_primary	data_version	data1 ¹	data2
	Fi...	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
7	449	NULL	7	170	hJHGmfusUW8e5/zR4s6bQ355Ue...	0	0	0	0	김 [redacted] 대	김 [redacted] 대
8	458	NULL	7	173	yZXjJKyWRJIw4Q8+Qpw1PybEC7...	0	0	0	0	오 ㅎ P	오 ㅎ P
9	455	NULL	7	172	oINBwfjZ9ikHlMpaJ9J5Xs4vBm...	0	0	0	0	사 ㄹ	사 ㄹ
10	494	NULL	7	181	b2wDZeAX4ejeAdJrKudkF+MK8U...	0	0	0	0	Ss	Ss

[스마트폰 내 연락처 데이터 베이스 일부]

1. 모바일 포렌식 도구

■ FINALDATA - 기능

• 데이터 분석 화면 - 문자메시지

The screenshot displays the FINALDATA Mobile Forensics software interface. The main window shows a list of messages extracted from a device. The left sidebar contains a tree view of the data structure, with '문자메시지(기본)(8/8)' selected. The main pane shows a table of messages with columns for '번호' (Number), '유형' (Type), '작발신 유형' (Retrieval Type), 'Msg ID', '전화번호' (Phone Number), '날짜' (Date), '미리보기' (Preview), '내용' (Content), and '메시지 확인' (Verify Message).

번호	유형	작발신 유형	Msg ID	전화번호	날짜	미리보기	내용	메시지 확인
1	SMS	수신	114	2021-01-09 오후 02:36:00			SKT> 타사 휴대폰 이용시, 가입된 상품 중 ...	읽음
2	SMS	수신	0077781719565	2021-05-13 오후 03:28:31			[국외발신] <#> Your WhatsApp code: 63...	읽음
3	MMS	수신	3	114	2020-10-22 오후 02:19:23	제목없음	[Web발신][KT] 스마트폰 중 일부는 무선...	읽음
4	MMS	수신	4	114	2020-10-22 오후 02:19:23	제목없음	[Web발신][KT] olleh 일부 스마트폰은 무선...	읽음
5	MMS	수신	6	114	2021-05-13 오후 03:26:09	[KT안내] 자급제 단말기 관련 안내	[Web발신][KT안내] 자급제 단말기는 통화/MM...	읽지않음
6	SMS-Threads		1		2020-02-24 오후 03:43:29			
7	MMS-Threads		4		2021-05-13 오후 03:26:09	[KT안내] 자급제 단말기 관련 안내		
8	SMS-Threads		5		2021-05-13 오후 03:28:31		[국외발신] <#> Your WhatsApp code: 63...	

The '미리 보기' (Preview) pane shows details for the selected message (ID 2):

- 데이터 유형: 문자메시지(기본)
- 상태: 정상
- 유형: SMS
- 작발신 유형: 수신
- 전화번호: 0077781719565
- 날짜: 2021-05-13 15:28:31
- 내용: [국외발신] <#> Your WhatsApp code: 637-471
You can also tap on this link to verify your phone: v.whatsapp.com/637471
Don't share this code with other
- 메시지 확인: 읽음

1. 모바일 포렌식 도구

▪ FINALDATA - 기능

- 데이터 분석 화면 - 사진

The screenshot displays the FINALDATA Mobile Forensics software interface. The main window shows a photo analysis screen for a file named 20210427_154425.jpg. The photo is displayed in the center, and its metadata is shown on the right. The metadata includes the file path, size, type, creation date, and location. The bottom pane shows the hex dump of the photo data, with the decoded text visible on the right.

File Tree (Left):

- 20210517_SM-G960N.mef
- [분석 목록](1058/1058)
- [멀티미디어업](2/2)
- [NQVault](1/1)
- [녹음 파일](1/1)
- [메시지](10/10)
- [Messages Content](2/2)
- [문자메시지(기본)](8/8)
- [사용자정보](1/1)
- [GooglePhoto-사용자정보](1/1)
- [설치업 목록](2/2)
- [설치업 목록](2/2)
- [연락처](17/17)
- [연락처(기본)](17/17)
- [일정](43/43)
- [일정](43/43)
- [정보](11/11)
- [폰정보](11/11)
- [통화내역](506/506)
- [통화내역(기본)](506/506)
- [멀티미디어/문서](116/116)
- [멀티미디어/문서](116/116)
- [사진](350/350)
- [사진(350/350)]

Photo Analysis Window (Center):

미리보기: 20210427_154425.jpg /sdcard/DCIM/Camera 118 5120361 JPG 2021:04:27 15:44:25 카메라 제조업... http://maps.google... 2021-04-27 PM 03:44:25 2021-04-27 PM 03:44:25 2021-04-27 PM 03:44:25

데이터 유형: 사진
상태: 정상
파일명 1: 20210427_154425.jpg
보기: 4032 x 3024 Pixel

파일 정보: /sdcard/DCIM/Camera
번호: 118
크기: 4.9MB (5,120,361 Bytes)
유형: JPG
찍은 날짜: 2021:04:27 15:44:25
정보: 카메라 제조업체: samsung
카메라 모델: SM-G960N
높이: 3024, 너비: 4032
GPS 정보: N 37d 36' 42.43", E 126d 59' 57.03"
위치: http://maps.google.com/maps?q=loc:37.611785,126.999176
만든 날짜: 2021-04-27 15:44:25
수정된 날짜: 2021-04-27 15:44:25
엑세스한 날짜: 2021-04-27 15:44:25

Hex Dump (Bottom):

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	FF	D8	FF	E1	FF	FF	45	78	69	66	00	00	49	49	2A	00	ÿØÿÿExif..II*.
00000010	08	00	00	00	0D	00	00	01	04	00	01	00	00	00	00	C0Ä.
00000020	00	00	01	01	04	00	01	00	00	00	D0	0B	00	00	12	01Ð....
00000030	03	00	01	00	00	00	06	00	00	00	13	02	03	00	01	00
00000040	00	00	01	00	00	00	1A	01	05	00	01	00	00	00	AA	00².
00000050	00	00	1B	01	05	00	01	00	00	00	B2	00	00	00	28	01³.(.
00000060	03	00	01	00	00	00	02	00	00	00	0F	01	02	00	08	00
00000070	00	00	BA	00	00	00	10	01	02	00	09	00	00	00	C2	00	..°.....Ä.
00000080	00	00	31	01	02	00	0E	00	00	00	CB	00	00	00	32	01	..1.....Ë...2.
00000090	02	00	14	00	00	00	D9	00	00	00	69	87	04	00	01	00Û...i#....
000000A0	00	00	ED	00	00	00	25	88	04	00	01	00	00	00	59	03	...i...%^.....Y.
000000B0	00	00	41	04	00	00	48	00	00	00	01	00	00	00	48	00	..A...H.....H.
000000C0	00	00	01	00	00	00	73	61	6D	73	75	6E	67	00	53	4Dsamsung.SM
000000D0	2D	47	39	36	30	4E	00	47	39	36	30	4E	4B	53	55	32	-G960N.G960NKSU2
000000E0	44	54	41	42	00	32	30	32	31	3A	30	34	3A	32	37	20	DTAB.2021:04:27
000000F0	31	35	3A	34	34	3A	32	35	00	24	00	9A	82	05	00	01	15:44:25.9.ä,...

[HxD로 확인한 사진]

1. 모바일 포렌식 도구

▪ FINALDATA - 기능

• 데이터 분석 화면 - 사진

The screenshot displays the FINALDATA mobile forensic tool interface. The sidebar on the left shows a file tree for the case '20210517_SM-G960N.mef'. The main window shows a table of files, with the selected file '20210427_154425.jpg' highlighted. The detailed view of the selected photo shows its metadata, including the file path, size, type, and location.

File Tree (Left Sidebar):

- 20210517_SM-G960N.mef
 - [분석 목록](1058/1058)
 - [멀티미디어첩](2/2)
 - NQVault(1/1)
 - 녹음 파일(1/1)
 - [메시지](10/10)
 - Messages Content(2/2)
 - 문자메시지(기본)(8/8)
 - [사용자정보](1/1)
 - GooglePhoto-사용자정보(1/1)
 - [설치업 목록](2/2)
 - 설치업 목록(2/2)
 - [연락처](17/17)
 - 연락처(기본)(17/17)
 - [일정](43/43)
 - 일정(43/43)
 - [정보](11/11)
 - 폰정보(11/11)
 - [통화내역](506/506)
 - 통화내역(기본)(506/506)
 - [멀티미디어/문서](116/116)
 - 멀티미디어/문서(116/116)
 - [사진](350/350)
 - 사진(350/350)**

File Table (Main Window):

미리보기	파일명	파일 경로	번호	크기	유형	찍은 날짜	정보	위치	만든 날짜	수정한 날짜	엑세스한 ...
	20210427_154425.jpg	/sdcard/DCIM/Camera	118	5120361	JPG	2021:04:27 15:44:25	카메라 제조업...	http://maps.googl...	2021-04-27 PM 03:44:25	2021-04-27 PM 03:44:25	2021-04-27 PM 03:44:25

Photo Details (Right Panel):

미리 보기

데이터 유형: 사진
상태: 정상
파일명: 20210427_154425.jpg
보기: [추출하기](#) 4032 x 3024 Pixel

파일 정보

파일 경로: /sdcard/DCIM/Camera
번호: 118
크기: 4.9MB (5,120,361 Bytes)
유형: JPG
찍은 날짜: 2021:04:27 15:44:25
정보: 카메라 제조업체: samsung
카메라 모델: SM-G960N
높이: 3024, 너비: 4032
GPS 정보: N 37d 36' 42.43", E 126d 59' 57.03"
위치: <http://maps.google.com/maps?q=loc:37.611785,126.999176>
만든 날짜: 2021-04-27 15:44:25
수정한 날짜: 2021-04-27 15:44:25
엑세스한 날짜: 2021-04-27 15:44:25

Location Map (Bottom Right):

37°36'42.4"N 126°59'57.0"E
37.611785, 126.999176

경로, 저장, 주변, 휴대전화로 보내기, 공유

서울특별시 성북구 정릉3동 855-4

1. 모바일 포렌식 도구

▪ 포렌식 도구 검증 방법

- NIST (National Institute of Standards and Technology)에서 진행되고 있는 CFTT (Computer Forensics Tool Testing) 프로젝트
 - 포렌식 조사에서 사용되는 모든 도구에 대해 신뢰성 기준을 제공하기 위한 방법 연구
- 한국정보통신기술협회 TTA (Telecommunications Technology Association)
 - 디지털 포렌식과 관련한 국가 표준 제정
 - 컴퓨터 포렌식을 위한 디지털 데이터 수집도구 요구사항 (TTAS.KO-12.0057)
 - 컴퓨터 포렌식을 위한 디지털 데이터 수집도구 검증규격 (TTAK.KO-12.0075)
 - 컴퓨터 포렌식을 위한 디지털 증거 분석도구 요구사항 (TTAK.KO-12.0081)
 - 컴퓨터 포렌식을 위한 디지털 증거 분석도구 검증 (TTAS.KO-12.0112)

1. 모바일 포렌식 도구

■ 포렌식 도구 검증 방법 - Federated Testing

[Federated Testing 과정 일부]

FT - DI - [01 | 03 | 05 | 10] - [INTERFACE | REMOVABLE MEDIA | FILE SYSTEM]

(1) Set up the test case

* If necessary, label source and destination drives

Test Case	Description
FT-DI-01	Image Physical Device (ATA28/48, FW, SATA28/48, SCSI, USB)
FT-DI-03	Image Removable Media (Compact Flash, SD Card)
FT-DI-05	Image Partition (ExFAT, EXT2/3/4, FAT16/32, NTFS, OSXC/I/CJ)
FT-DI-10	Truncated Image Acquire (without enough space for image file)

Test Case	Description
FT-DI-01	Image Physical Device (ATA28/48, FW, SATA28/48, SCSI, USB)
FT-DI-03	Image Removable Media (Compact Flash, SD Card)
FT-DI-05	Image Partition (ExFAT, EXT2/3/4, FAT16/32, NTFS, OSXC/I/CJ)
FT-DI-10	Truncated Image Acquire (without enough space for image file)

ANALYSIS ENVIRONMENT

(2) Boot 'Analysis PC' with Federated Testing boot CD

- ❖ Interface between Analysis PC and the target drive
 - ATA or SCSI → Need to be attached before booting PC
 - USB or FireWire → Can be attached after booting is finished

(3) Reset the system clock (if necessary)

Command Line Interface

```
date command
> date mmddHHMM
> date 12131415
(e.g., December 13 at 2:15 PM)
```

Desktop Interface

- Click on 'Time & Date Setting'
- Click the 'Manually' radio button
- Adjust Time & Date as needed
- Click the 'Clock' tab
- Toggle the 'Seconds' on and off
- Verify that the date/time updated

(4) Attach and mount 'FT-LOGS' log drive

* If the FT-LOGS drive is already mounted, skip this step

- Attach FT-LOGS log drive
- Click on device icon
- Verify the mounted FT-LOGS drive

(5) Attach the source drive & identify device name

- Attach the source drive
- Click the 'List' link
- Identify attached device name(s)

7. If not already attached interface may be used
 8. List attached devices
 9. Write known content

sda = sda1
 sdb = sdb1
 sdc = sdc1
 ...

(6) Write known content to the source drive

Open a terminal

cftt-di command

```
> cftt-di
```

Create a profile

- Your name
- Analysis PC name
- Test PC name

Write known content

- Select the option '1'

Write known content

- Type a src drive ID (e.g., a1, a2, a3...)
- Select a src drive

<https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt/federated-testing>

02

모바일 포렌식 실습

2. 모바일 포렌식 실습

▪ 스마트폰 데이터 주요 분석 항목

주요 데이터	분석 항목
메시지(SMS)	수/발신 일자, 수신/발신자 전화번호, 문자 내용 등
통화기록(Call log)	수신/발신자 전화번호, 통화 종류, 통화 시간 등
연락처	전화번호, 그룹, 이름 등
일정	일정 내용, 일정 시간, 일정 장소 등
메모	메모 내용, 메모 종류, 작성/수정/삭제 시간 등
사진/ 동영상	위치 정보, 촬영시간, 수정시간 등
인터넷	접속 사이트, 접속 시간, 검색 키워드 등
휴대전화 정보	로그인된 구글 계정, 전화번호, 통신사, 단말기 식별 코드(IMEI), 기기 일련 번호, 기기 종류, 기기 설정명 등

2. 모바일 포렌식 실습

▪ 시나리오

- 카페에서 용의자 A가 불법 촬영을 하던 것을 지나가던 목격자가 발견
 - 2021년 5월 18일, 오전 11시경 사건 발생
- 수사 중 추가 범죄의 정황이 있어, 영장 발부 후 추가 수사 진행



2. 모바일 포렌식 실습

▪ 시나리오

- 증거로 압수된 압수 물품
 - 용의자 소유 스마트폰
- 압수 물품 상세 정보




대상	모델명	장치 용량	OS	모델명
증거물	Galaxy Note 5	32GB	Android	SM-N920S



2. 모바일 포렌식 실습

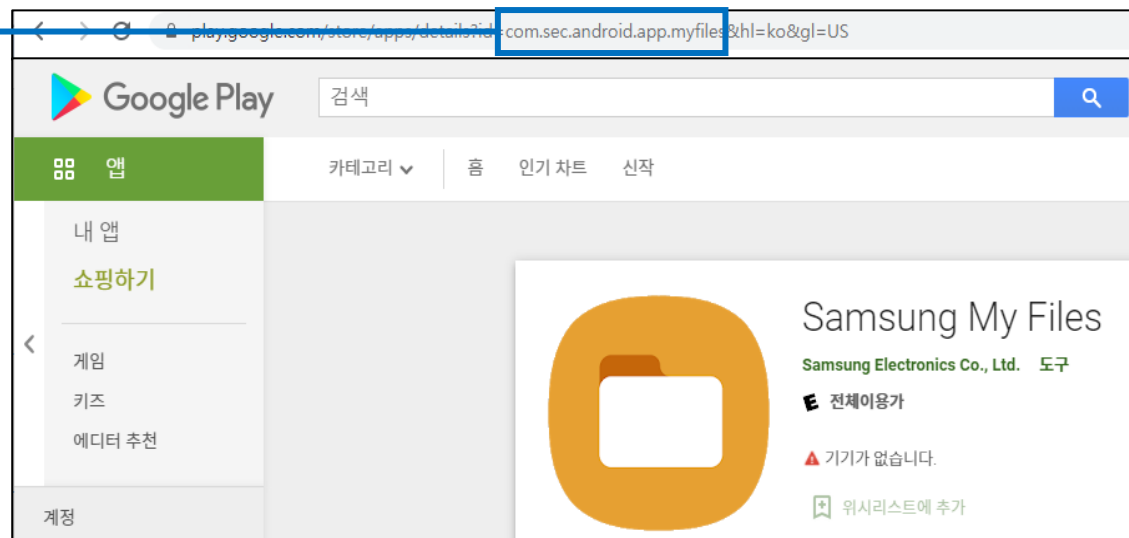
■ 시나리오 분석

• 사진 분석 내용

미리보기	파일명	파일 경로	번호	크기	유형	찍은 ...	정보	위치	만든 날짜
	41.jpg	/Media/data/com.sec.android.app.myfiles/cache	552	14599	JPG		높이 : 320, 너비 : 320		2021-05-17 PM 04:44:54
	37.jpg	/Media/data/com.sec.android.app.myfiles/cache	548	22365	JPG		높이 : 320, 너비 : 320		2021-05-17 PM 04:44:53
	38.jpg	/Media/data/com.sec.android.app.myfiles/cache	549	14483	JPG		높이 : 320, 너비 : 320		2021-05-17 PM 04:44:53

불법 촬영으로 의심되는 사진들

앱 패키지명



2. 모바일 포렌식 실습

■ 시나리오 분석

• 인터넷 검색 기록

제목	URL	날짜
Google	https://www.google.co.kr/#sbfbu=1&pi=	2021-05-17 오후 04:37:26
Google	https://www.google.co.kr/	2021-05-17 오후 04:37:32
사진 숨기기 - Google Search	https://www.google.co.kr/search?q=사진+숨기기&source=hp&ei=Nh2iYL_qAr2Hr7wP4OGXoAc&oq=사진...	2021-05-17 오후 04:37:33
사진 숨기기 - Google Search	https://www.google.co.kr/search?q=사진+숨기기&source=hp&ei=Nh2iYL_qAr2Hr7wP4OGXoAc&oq=사진...	2021-05-17 오후 04:37:36
갤럭시 갤러리에서 사진, 앨범 숨기기	https://lifet revel.tistory.com/377	2021-05-17 오후 04:37:37
사진 숨기기 - Google Search	https://www.google.co.kr/search?q=사진+숨기기&source=hp&ei=Nh2iYL_qAr2Hr7wP4OGXoAc&oq=사진...	2021-05-17 오후 04:37:41
스마트폰 동영상 숨기기, 사진 숨기기 간단하게 해봅시다. : 네이버 블로그	http://m.blog.naver.com/71018025/220183084422	2021-05-17 오후 04:37:48
스마트폰 동영상 숨기기, 사진 숨기기 간단하게 해봅시다. : 네이버 블로그	https://m.blog.naver.com/PostView.naver?blogId=71018025&logNo=220183084422&proxyReferer=https://...	2021-05-17 오후 04:37:48
사진 숨기기 - Google Search	https://www.google.co.kr/search?q=사진+숨기기&source=hp&ei=Nh2iYL_qAr2Hr7wP4OGXoAc&oq=사진...	2021-05-17 오후 04:37:51
갤럭시 S10 갤러리 사진 숨기기 - 엑스트림 매뉴얼	https://www.google.co.kr/amp/s/extrememmanual.net/34352?amp	2021-05-17 오후 04:37:54
사진 숨기기 - Google Search	https://www.google.co.kr/search?q=사진+숨기기&source=hp&ei=Nh2iYL_qAr2Hr7wP4OGXoAc&oq=사진...	2021-05-17 오후 04:37:55
Google	https://www.google.co.kr/	2021-05-17 오후 04:37:57
Google	https://www.google.co.kr/#sbfbu=1&pi=	2021-05-17 오후 04:37:59
Google	https://www.google.co.kr/	2021-05-17 오후 04:38:09
사진 숨기기 어플 - Google Search	https://www.google.co.kr/search?q=사진+숨기기+어플&source=hp&ei=Nh2iYL_qAr2Hr7wP4OGXoAc&oq...	2021-05-17 오후 04:38:09
사진 숨기기 어플 - Google Search	https://www.google.co.kr/search?q=사진+숨기기+어플&source=hp&ei=Nh2iYL_qAr2Hr7wP4OGXoAc&oq...	2021-05-17 오후 04:38:11
https://119mom.tistory.com/38	https://119mom.tistory.com/38	2021-05-17 오후 04:38:13
https://119mom.tistory.com/38	https://119mom.tistory.com/38	2021-05-17 오후 04:38:15
사진 숨기기 어플 - Google Search	https://www.google.co.kr/search?q=사진+숨기기+어플&source=hp&ei=Nh2iYL_qAr2Hr7wP4OGXoAc&oq...	2021-05-17 오후 04:38:19
숨김어플 - Google Search	https://www.google.co.kr/search?q=숨김어플&sa=X&ved=2ahUKEwiM5PbmmtDwAhWowosBHXYXbkAQ1Q...	2021-05-17 오후 04:38:22
숨김어플 - Google Search	https://www.google.co.kr/search?q=숨김어플&sa=X&ved=2ahUKEwiM5PbmmtDwAhWowosBHXYXbkAQ1Q...	2021-05-17 오후 04:38:24
안드로이드 앱 숨기기 LG, 갤럭시 어플 숨김 다 비슷해요	https://gbworld.tistory.com/m/1638	2021-05-17 오후 04:38:25
숨김어플 - Google Search	https://www.google.co.kr/search?q=숨김어플&sa=X&ved=2ahUKEwiM5PbmmtDwAhWowosBHXYXbkAQ1Q...	2021-05-17 오후 04:38:27
갤럭시 앱 숨기기 및 핸드폰 어플숨기기 와 홈페이지 UI구성 설정 방법 알아보기.(노...	https://m.blog.naver.com/olo_5o199939/221642745220	2021-05-17 오후 04:38:31
갤럭시 앱 숨기기 및 핸드폰 어플숨기기 와 홈페이지 UI구성 설정 방법 알아보기.(노...	https://m.blog.naver.com/olo_5o199939/221642745220	2021-05-17 오후 04:38:32

• 앱 검색 기록

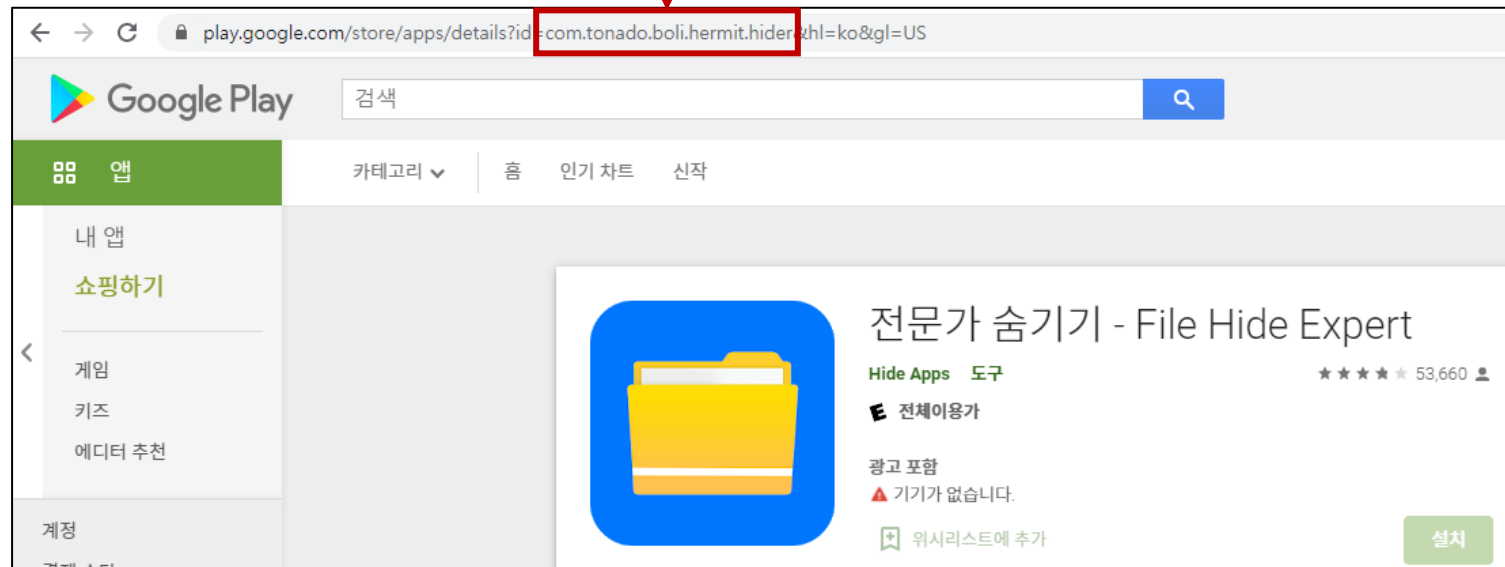
검색어	날짜
whatsapp	2021-05-15 오후 04:23:15
전문가 숨기기	2021-05-17 오후 04:38:39
숨기기어플	2021-05-17 오후 04:38:43
사진숨기기	2021-05-17 오후 04:38:52

2. 모바일 포렌식 실습

■ 시나리오 분석

• 앱 설치 기록

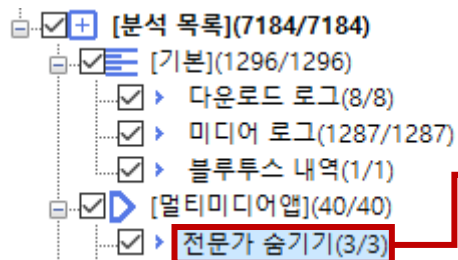
앱 이름	패키지명	패키지경로	계정	설치 날짜
File Hide Expert-Hide Pictures	com.tonado.boli.hermit.hider	/Media/user_de/0/com.tonado.boli.her...	@gmail.com	2021-05-17 오후 04:39:39
WhatsApp Messenger	com.whatsapp	/Media/user_de/0/com.whatsapp	@gmail.com	2021-05-15 오후 04:25:06



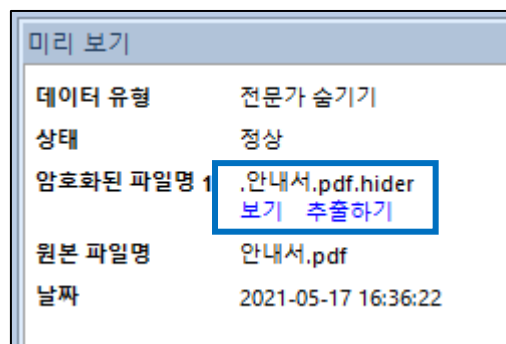
2. 모바일 포렌식 실습

■ 시나리오 분석

- 앱 설치 기록



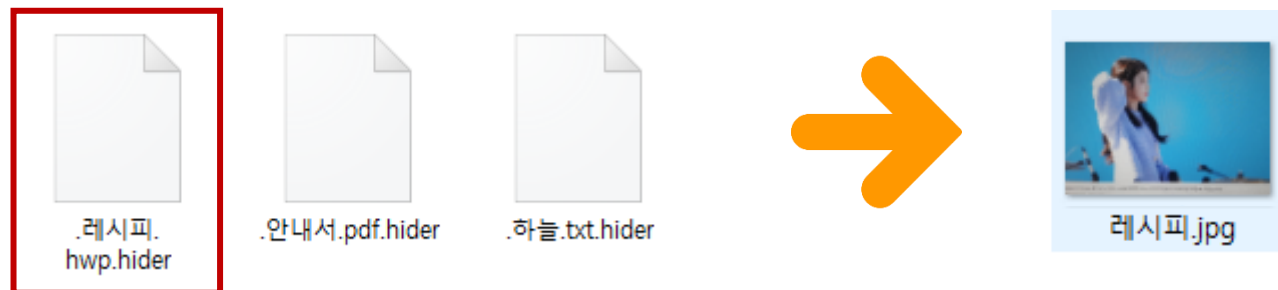
<input checked="" type="checkbox"/>	번호	미리보기: 암호화된 파일명	암호화된 파일명	원본 파일명	날짜
<input checked="" type="checkbox"/>	1		.레시피.hwp.hider	레시피.hwp	2021-05-17 오후 04:41:58
<input checked="" type="checkbox"/>	2	<div>No Preview</div>	.안내서.pdf.hider	안내서.pdf	2021-05-17 오후 04:41:22
<input checked="" type="checkbox"/>	3		.하늘.txt.hider	하늘.txt	2021-05-17 오후 04:41:42



2. 모바일 포렌식 실습

■ 시나리오 분석

• 추출된 데이터 분석



FD 레시피.hwp.hider

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	FF	D8	FF	E1	35	3A	45	78	69	66	00	00	49	49	2A	00	ÿØÿáS:Exif..II*.
00000010	08	00	00	00	0D	00	00	01	04	00	01	00	00	00	90	0F
00000020	00	00	01	01	04	00	01	00	00	00	AC	0B	00	00	0F	01
00000030	02	00	08	00	00	00	AA	00	00	00	10	01	02	00	09	00
00000040	00	00	B2	00	00	00	12	01	03	00	01	00	00	00	01	00	..
00000050	00	00	1A	01	05	00	01	00	00	00	DE	00	00	00	1B	01
00000060	05	00	01	00	00	00	E6	00	00	00	28	01	03	00	01	00
00000070	00	00	02	00	00	00	31	01	02	00	0E	00	00	00	BC	00
00000080	00	00	32	01	02	00	14	00	00	00	CA	00	00	00	13	02	..2.....
00000090	03	00	01	00	00	00	01	00	00	00	69	87	04	00	01	00
000000A0	00	00	EE	00	00	00	25	88	04	00	01	00	00	00	2A	03	..i...\$^.....*
000000B0	00	00	F8	03	00	00	73	61	6D	73	75	6E	67	00	53	4D	...ø...samsung.SM
000000C0	2D	4E	39	32	30	53	00	00	4E	39	32	30	53	4B	53	55	-N920S..N920SKSU
000000D0	32	44	52	47	33	00	32	30	32	31	3A	30	35	3A	31	37	2DRG3.2021:05:17
000000E0	20	31	36	3A	33	35	3A	35	38	00	48	00	00	00	01	00	16:35:58.H....

[추출한 파일을 HxD로 확인한 결과]

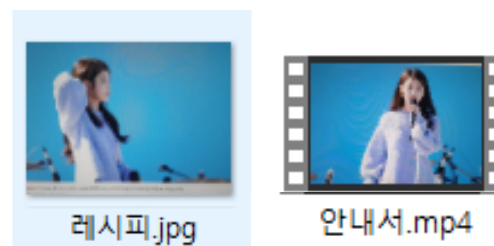
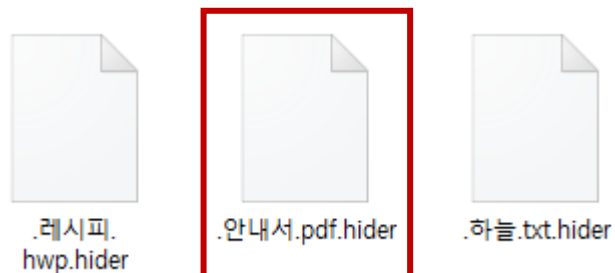


[파일명을 jpg 로 변경 후 확인한 결과]

2. 모바일 포렌식 실습

■ 시나리오 분석

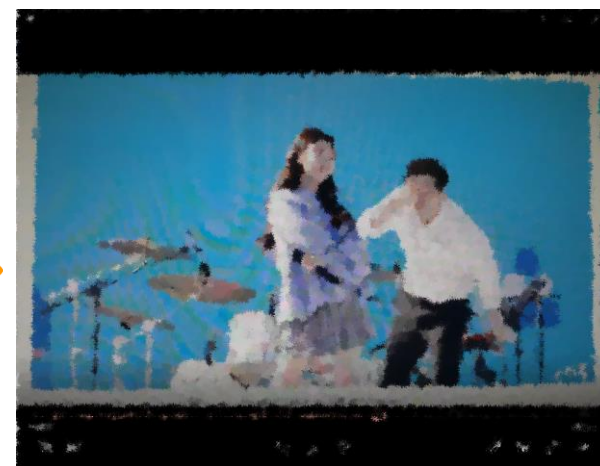
• 추출된 데이터 분석



FD .안내서.pdf.hider

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	00	00	00	18	66	74	79	70	6D	70	34	32	00	00	00	00ftypmp42....
00000010	69	73	6F	6D	6D	70	34	32	02	64	29	31	6D	64	61	74	isommp42.d)lmdat
00000020	21	1B	93	CD	AC	8C	27	08	30	A0	48	24	AF	3C	65	D6	!."í-æ'.0 H9<eÖ
00000030	65	65	85	52	E8	B9	2A	A9	AD	24	A5	C1	20	00	13	CA	ee...Rè'*.0.\$¥Å ..Ê
00000040	5A	E0	0A	8F	FC	1F	3B	FB	A6	74	07	CA	6E	9F	FF	C9	Zà..ü.;û;t.ÊnÿyÉ
00000050	A0	7D	77	94	EA	AC	E8	2F	85	26	43	4C	E0	7C	39	85	}w"è-è/...&CLà 9...
00000060	64	90	A4	69	FA	6E	BF	79	EE	90	78	48	6A	CD	71	06	d.üün;yi.xHjÍq.
00000070	87	F4	CD	F1	03	FE	48	09	1D	99	A9	42	44	21	8C	21	+óÍñ.pH..™@BD!@!
00000080	1A	92	59	28	9E	72	DB	DF	E5	F2	F5	09	86	2A	36	9B	.'Y(žrÜSâòö.†*6>
00000090	48	92	F6	F8	F5	73	DF	00	10	61	86	08	32	8D	4F	87	H'öøöSâ...at.2.O#
000000A0	6F	05	44	C0	38	69	3E	D1	F3	F4	9A	DD	21	80	F6	FF	o.DÀ8i>Ñóöšý!€öy
000000B0	90	FA	9E	8F	0F	77	77	C6	25	95	14	24	50	84	18	C6	úž...wwE\$*. \$P,,.E
000000C0	7B	7C	6F	5B	BD	EF	34	94	AB	61	2C	29	AD	1C	A4	FF	{ o[?i4"«a,)...xÿ
000000D0	01	13	CA	52	E0	8B	26	55	CC	7A	AE	C8	61	A9	C0	AF	..ÊRà< &Uiz@Èa@À-
000000E0	08	CE	82	EA	CD	C7	16	FA	8B	83	EB	97	BE	6E	F5	16	.î,êíç.ú<fë-»nõ.

[추출한 파일을 HxD로 확인한 결과]



[파일명을 mp4 로 변경 후 확인한 결과]

2. 모바일 포렌식 실습

■ 시나리오 분석

- 추출된 데이터 분석



File: .하늘.txt.hider

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	FF	D8	FF	E1	33	7E	45	78	69	66	00	00	49	49	2A	00	ÿøÿá3~Exif..II*.
00000010	08	00	00	00	0D	00	00	01	04	00	01	00	00	00	90	0F
00000020	00	00	01	01	04	00	01	00	00	00	AC	0B	00	00	0F	017.....
00000030	02	00	08	00	00	00	AA	00	00	00	10	01	02	00	09	00^.....
00000040	00	00	B2	00	00	00	12	01	03	00	01	00	00	00	01	00	..^.....
00000050	00	00	1A	01	05	00	01	00	00	00	DE	00	00	00	1B	01P.....
00000060	05	00	01	00	00	00	E6	00	00	00	28	01	03	00	01	00æ... (.....
00000070	00	00	02	00	00	00	31	01	02	00	0E	00	00	00	BC	00l.....4.
00000080	00	00	32	01	02	00	14	00	00	00	CA	00	00	00	13	02	..2.....Ê.....
00000090	03	00	01	00	00	00	01	00	00	00	69	87	04	00	01	00i#....
000000A0	00	00	EE	00	00	00	25	88	04	00	01	00	00	00	2A	03	..i...%^......*
000000B0	00	00	F8	03	00	00	73	61	6D	73	75	6E	67	00	53	4D	..ø...samsung.SM
000000C0	2D	4E	39	32	30	53	00	00	4E	39	32	30	53	4B	53	55	-N920S..N920SKSU
000000D0	32	44	52	47	33	00	32	30	32	31	3A	30	35	3A	31	37	2DRG3.2021:05:17
000000E0	20	31	36	3A	33	36	3A	34	32	00	48	00	00	00	01	00	16:36:42.H....

[추출한 파일을 HxD로 확인한 결과]

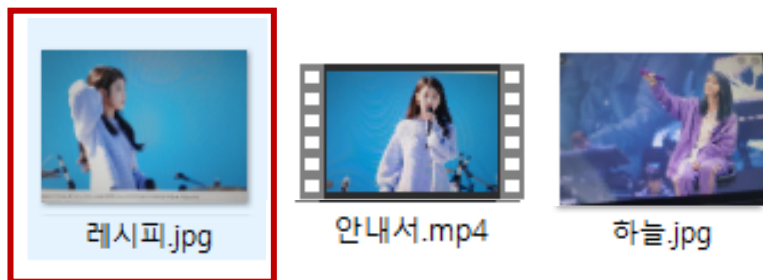


[파일명을 jpg 로 변경 후 확인한 결과]

2. 모바일 포렌식 실습

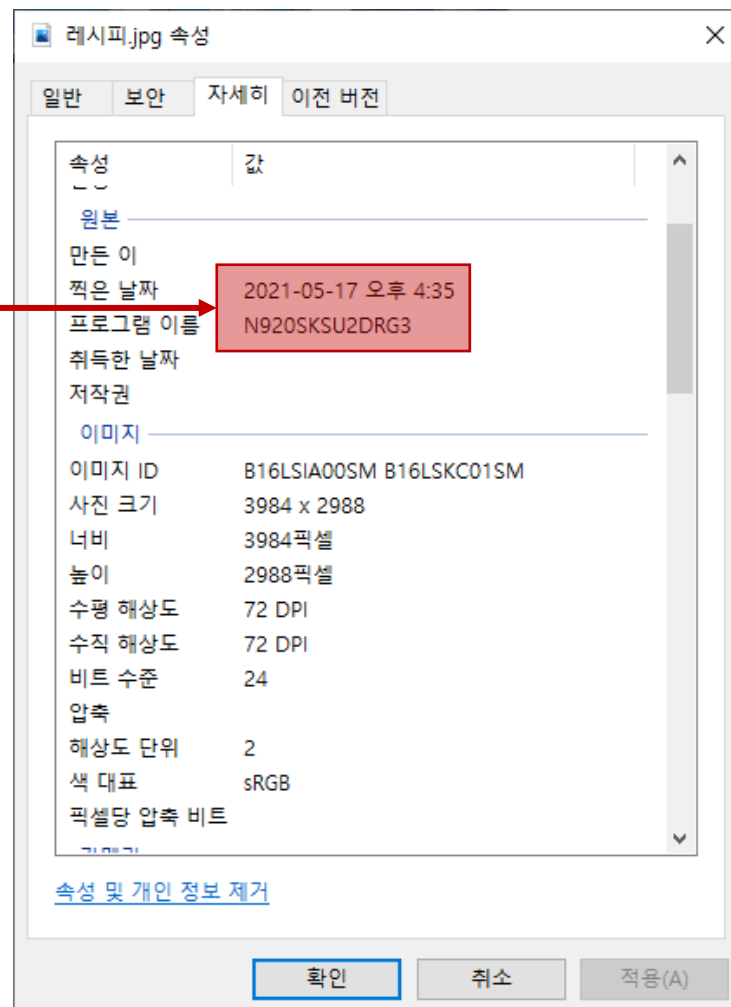
■ 시나리오 분석

• 추출된 데이터 분석



```
레시피.hwp.hider
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text
00000000 FF D8 FF E1 35 3A 45 78 69 66 00 00 49 49 2A 00 ÿÿá5:Exif..II*.
00000010 08 00 00 00 0D 00 00 01 04 00 01 00 00 00 90 0F .....
00000020 00 00 01 01 04 00 01 00 00 00 AC 0B 00 00 0F 01 .....~.....
00000030 02 00 08 00 00 00 AA 00 00 00 10 01 02 00 09 00 .....^.....
00000040 00 00 B2 00 00 00 12 01 03 00 01 00 00 00 01 00 ..^.....
00000050 00 00 1A 01 05 00 01 00 00 00 DE 00 00 00 1B 01 .....P.....
00000060 05 00 01 00 00 00 E6 00 00 00 28 01 03 00 01 00 .....æ...(.
00000070 00 00 02 00 00 00 31 01 02 00 0E 00 00 00 BC 00 .....l.....4.
00000080 00 00 32 01 02 00 14 00 00 00 CA 00 00 00 13 02 ..2.....ê....
00000090 03 00 01 00 00 00 01 00 00 00 69 87 04 00 01 00 .....i#....
000000A0 00 00 EE 00 00 00 25 88 04 00 01 00 00 00 2A 03 ..i...%^.....*.
000000B0 00 00 F8 03 00 00 73 61 6D 73 75 6E 67 00 53 4D ..ø...samsung.SM
000000C0 2D 4E 39 32 30 53 00 00 4E 39 32 30 53 4B 53 55 -N920S...N920SKSU
000000D0 32 44 52 47 33 00 32 30 32 31 3A 30 35 3A 31 37 2DRG3.2021:05:17
000000E0 20 31 36 3A 33 35 3A 35 38 00 48 00 00 00 01 00 16:35:58.H.....
```

[추출한 파일을 HxD로 확인한 결과]



[추출한 파일의 메타데이터 내용]

2. 모바일 포렌식 실습

■ 시나리오 분석

- 문자 메시지 기록

<input checked="" type="checkbox"/>	번호	유형	착발신 유형	Msg ID	전화번호	날짜
-------------------------------------	----	----	--------	--------	------	----

⋮

<input checked="" type="checkbox"/>	27	SMS	발신	010-██████	/돈주머니1	2021-05-17 오후 04:43:03
미리 보기						
데이터 유형	문자메시지(기본)					
상태	정상					
유형	SMS					
착발신 유형	발신					
전화번호	██████ /돈주머니1					
날짜	2021-05-17 16:43:03					
내용	Join the conversation on Hangouts: https://hangouts.google.com/group/SJfbqgsZMerM2iEZA					



용의자



행아웃 초대 메시지



돈주머니

2. 모바일 포렌식 실습

■ 시나리오 분석

• 행아웃 메신저 사용 기록

✓ !	번호	착발신 유형	채팅유형	채팅명	사용자 ID	날짜	내용
✓	27	수신	메시지	iPhone Kim	104390345812877907272	2021-05-17 오후 04:52:50	감사합니다
✓	26	발신	메시지	iPhone Kim	115883403195964023018	2021-05-17 오후 04:52:42	확인해주세요
✓	25	발신	메시지	iPhone Kim	115883403195964023018	2021-05-17 오후 04:48:43	네
✓	24	수신	메시지	iPhone Kim	104390345812877907272	2021-05-17 오후 04:48:37	ks1 지메일입니다
✓	23	발신	메시지	iPhone Kim	115883403195964023018	2021-05-17 오후 04:48:23	이메일 주소 좀
✓	22	수신	메시지	iPhone Kim	104390345812877907272	2021-05-17 오후 04:47:49	네 보냈습니다
✓	21	발신	메시지	iPhone Kim	115883403195964023018	2021-05-17 오후 04:47:41	잠시만요
✓	20	발신	메시지	iPhone Kim	115883403195964023018	2021-05-17 오후 04:47:33	보내려고 하는데
✓	19	발신	메시지	iPhone Kim	115883403195964023018	2021-05-17 오후 04:47:24	입금 확인하고
✓	18	발신	메시지	iPhone Kim	115883403195964023018	2021-05-17 오후 04:46:35	네
✓	17	수신	메시지	iPhone Kim	104390345812877907272	2021-05-17 오후 04:46:26	여기 맞나요?



용의자



입금 확인 요청



G mail 주소 알려줌



돈주머니

2. 모바일 포렌식 실습

■ 시나리오 분석

- 이메일 첨부 파일 기록

번호	제목	미리보기: 내용	내용	보낸 사람	받은사람	회신	날짜
1	스즈	<div dir='auto'...	Body0.html		ks1 [redacted]@gmail.com		2021-05-17 오후 04:51:01

미리 보기

데이터 유형: Gmail
상태: 정상
제목: 스즈
내용 1: Body2.html
[보기](#) [추출하기](#)

<div style="color:rgb(33,33,33);background-color:rgb(255,255,255)" dir="auto">
?뵙뵙 ?각뵙</div>
<div id="m_2123220517425874829ms-outlook-mobile-signature">
<div>

</div>
Get Android??Outlook ?뵙뵙뵙뵙</div>
</div>

보낸 사람: [redacted]@gmail.com
받은사람: ks1 [redacted]@gmail.com
날짜: 2021-05-17 15:23:48
첨부파일명: **레시피.hwp**
안내서.pdf
하늘.txt

첨부파일 URL: <https://mail.google.com/mail/?ui=2ik=4813a65fa6attid=0.1th=17978feb20804deaview=attzw>
첨부파일 URL: <https://mail.google.com/mail/?ui=2ik=4813a65fa6attid=0.2th=17978feb20804deaview=attzw>
첨부파일 URL: <https://mail.google.com/mail/?ui=2ik=4813a65fa6attid=0.3th=17978feb20804deaview=attzw>

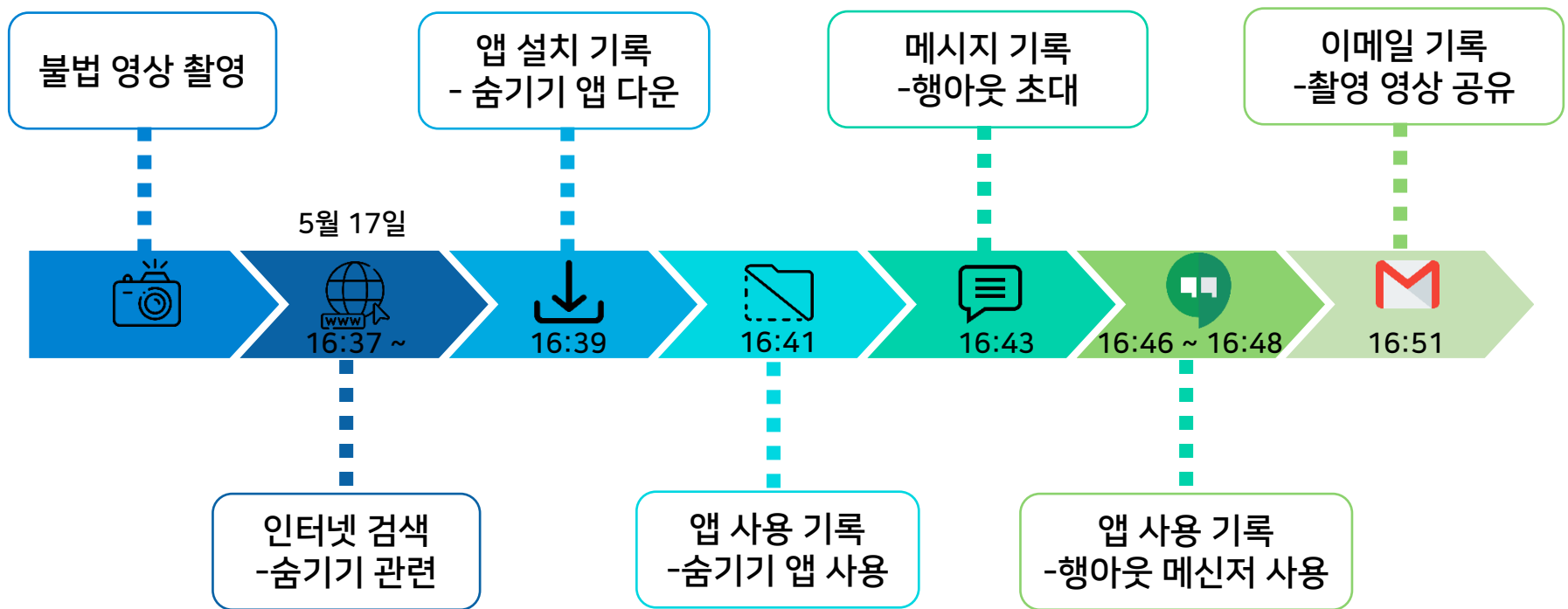
행아웃에서 주고받은 이메일 주소

불법 촬영 영상

2. 모바일 포렌식 실습

■ 시나리오 분석

- 타임라인



Thank you
