KMU 국민대학교 KOOKMIN UNIVERSITY

DF&C Lab. Digital Forensic & Cryptanalysis KOOKMIN UNIVERSITY

Mobile Forensics

강수진

국민대학교 금융정보보안학과, DF&C 연구실

dfnc@kookmin.ac.kr

CONTENTS

01

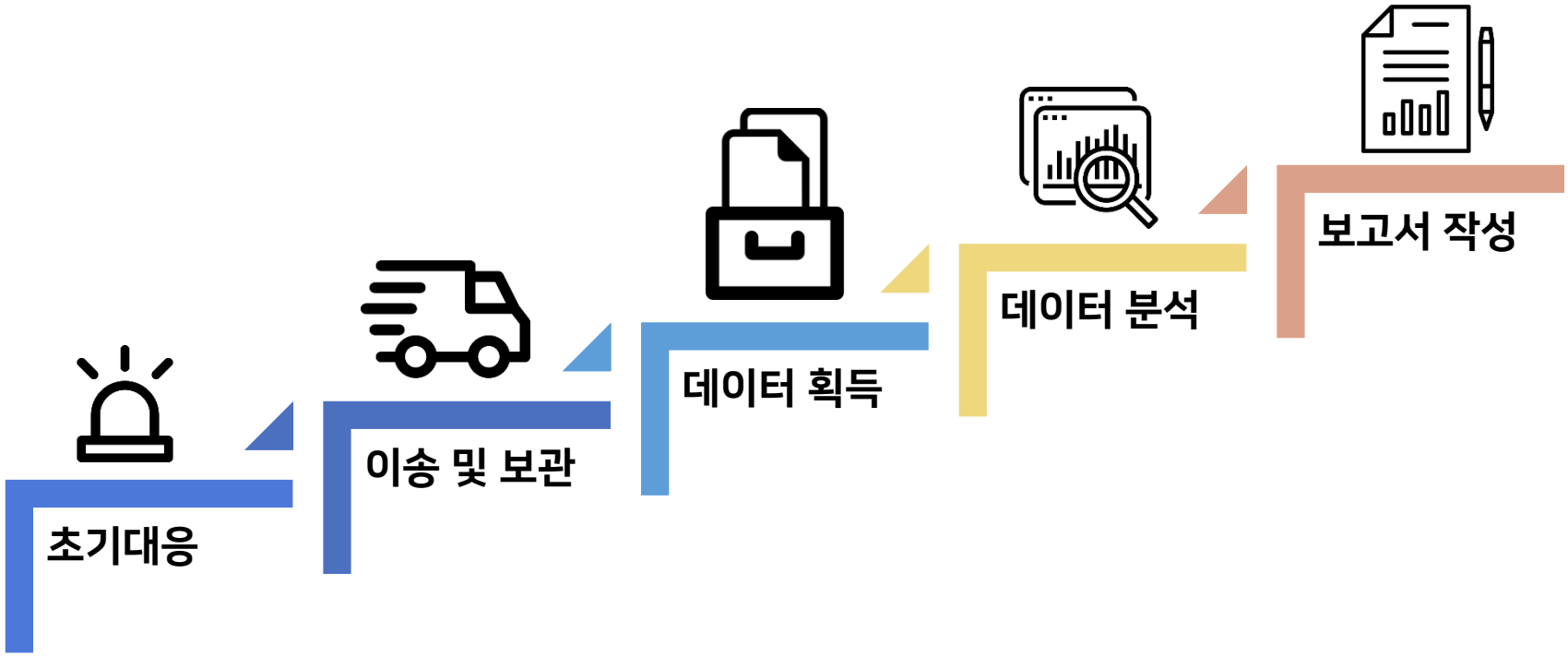
모바일 포렌식 개요

1. 모바일 포렌식 개요

- **모바일 포렌식이란?**
  - 모바일 기기 내부에 저장된 디지털 정보를 분석하고 이를 증거화
    - 모바일 기기: 스마트폰, 태블릿 PC, 휴대용 메모리카드, USB 저장장치, 스마트 워치 등
  - 모바일 기기에는 사용자가 생성한 데이터가 저장

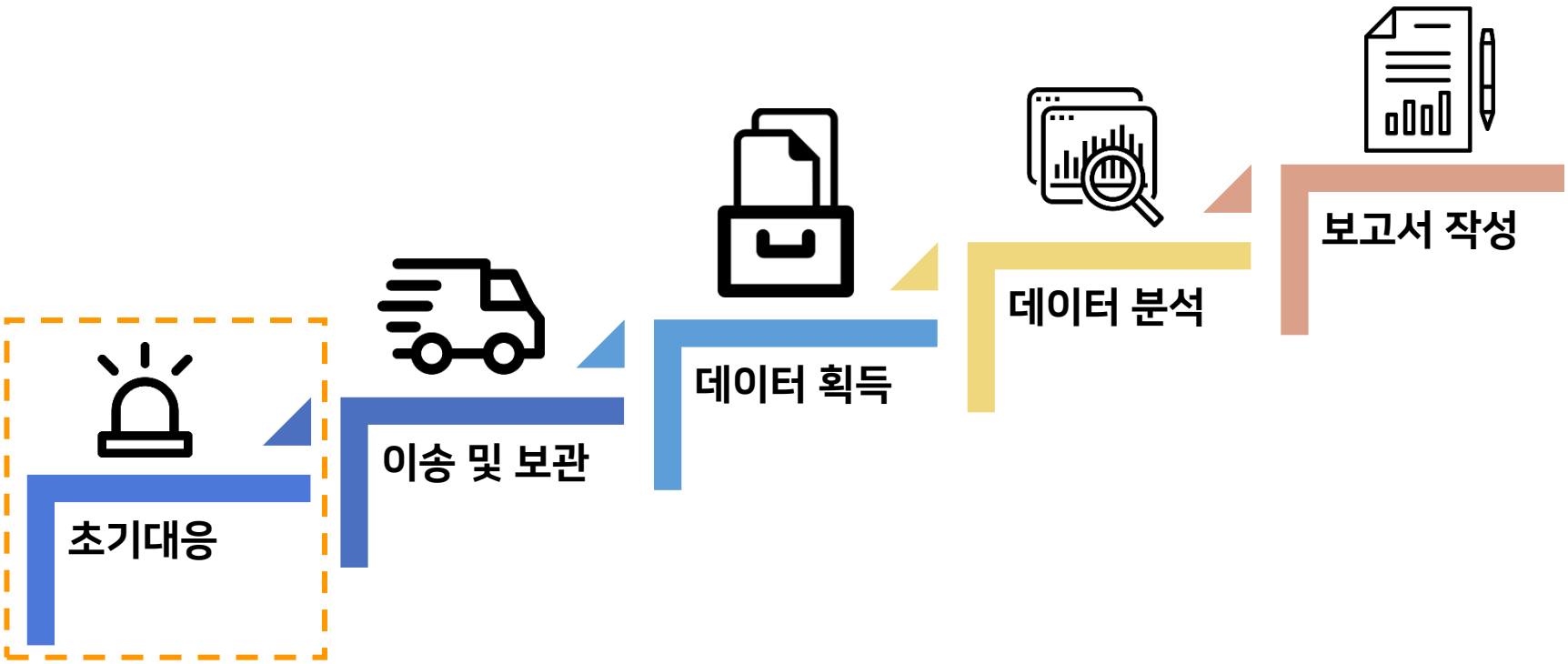
1. 모바일 포렌식 개요

- **모바일 포렌식 절차**
  - 한국 정보 통신 기술 협회(TTA) - TTAK.KO-12.0059/R1



1. 모바일 포렌식 개요

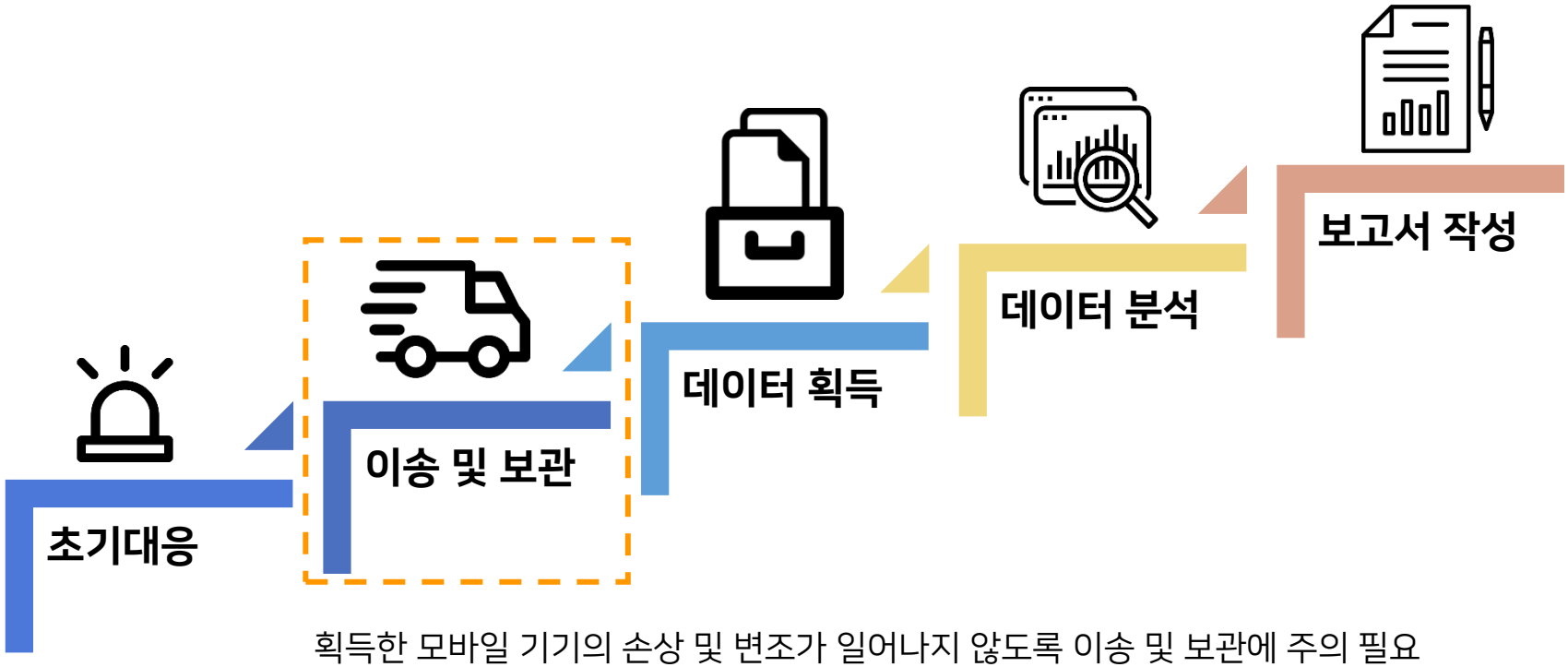
- **모바일 포렌식 절차**
  - 한국 정보 통신 기술 협회(TTA) - TTAK.KO-12.0059/R1



사건 및 현장과 관련한 정보가 저장된 모바일 기기를 초기에 획득하는 과정

1. 모바일 포렌식 개요

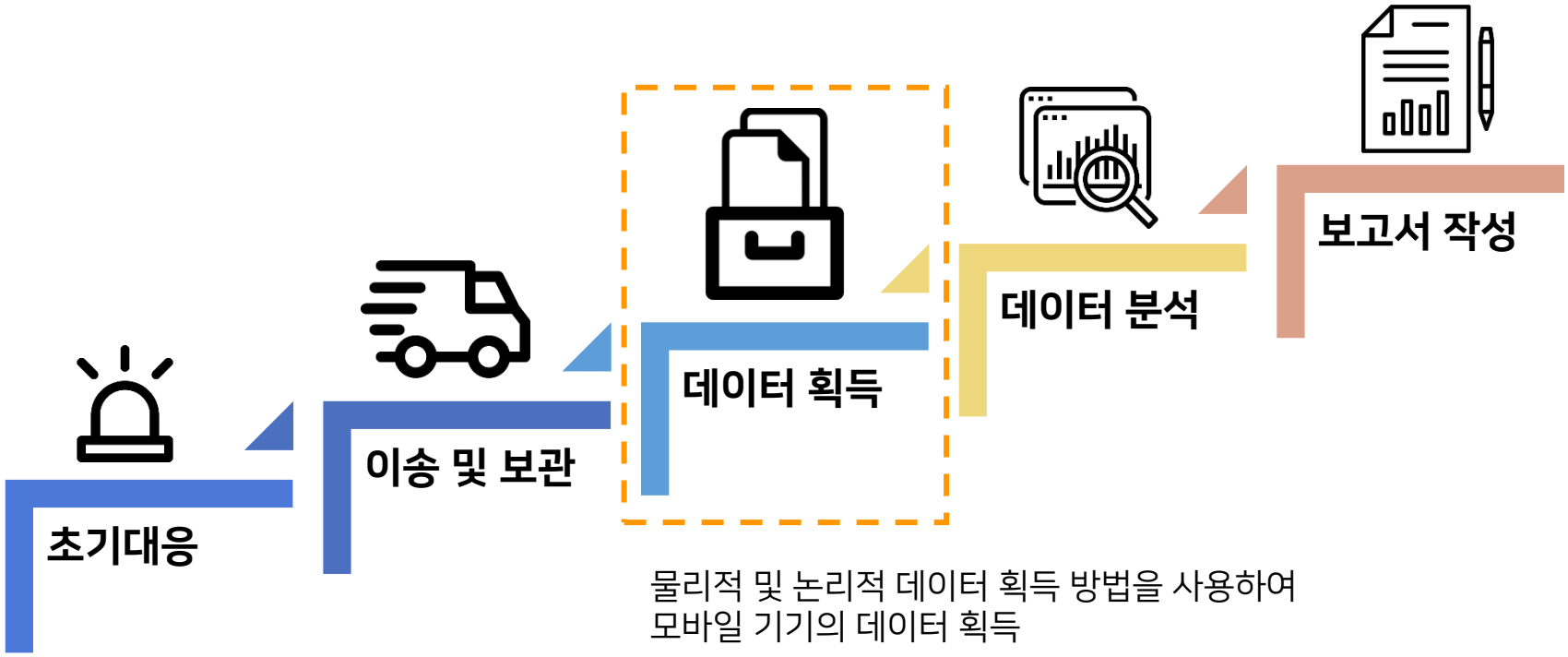
- **모바일 포렌식 절차**
  - 한국 정보 통신 기술 협회(TTA) - TTAK.KO-12.0059/R1



획득한 모바일 기기의 손상 및 변조가 일어나지 않도록 이송 및 보관에 주의 필요

1. 모바일 포렌식 개요

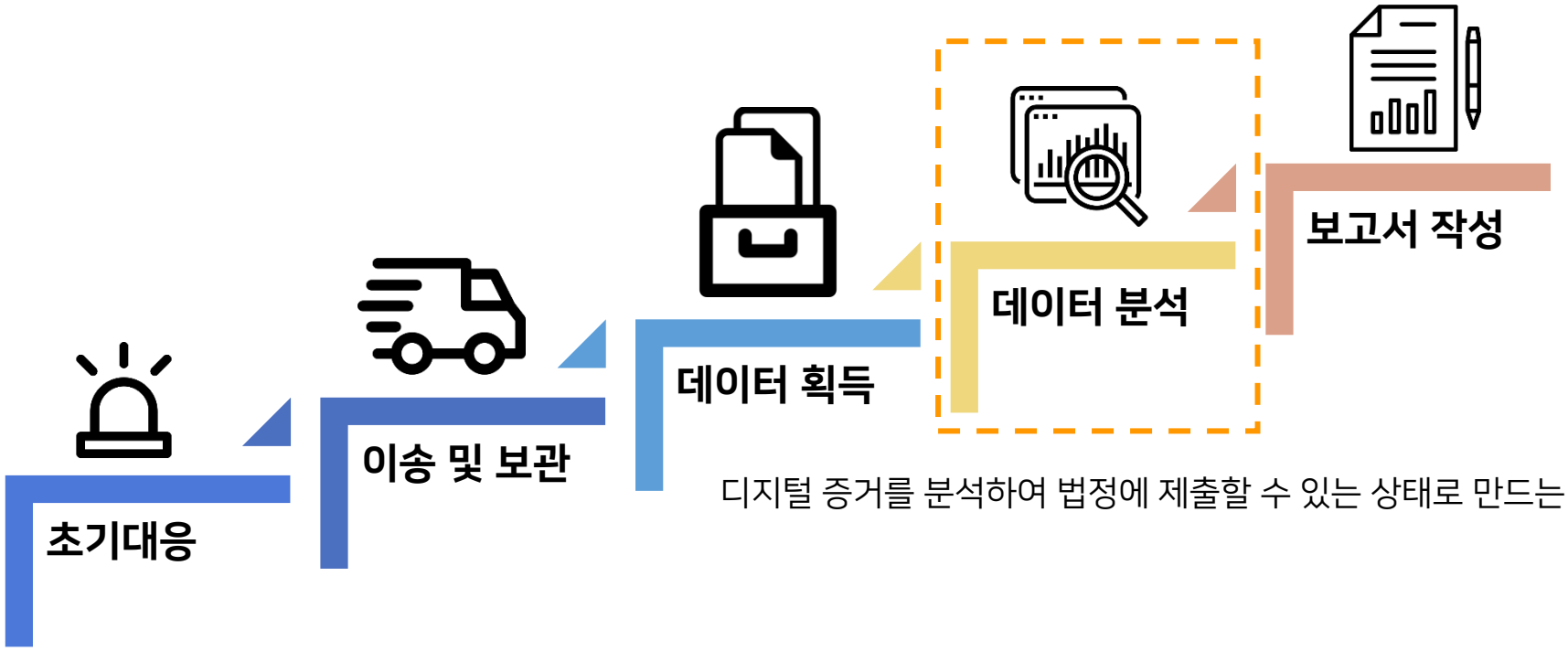
- **모바일 포렌식 절차**
  - 한국 정보 통신 기술 협회(TTA) - TTAK.KO-12.0059/R1



물리적 및 논리적 데이터 획득 방법을 사용하여
모바일 기기의 데이터 획득

1. 모바일 포렌식 개요

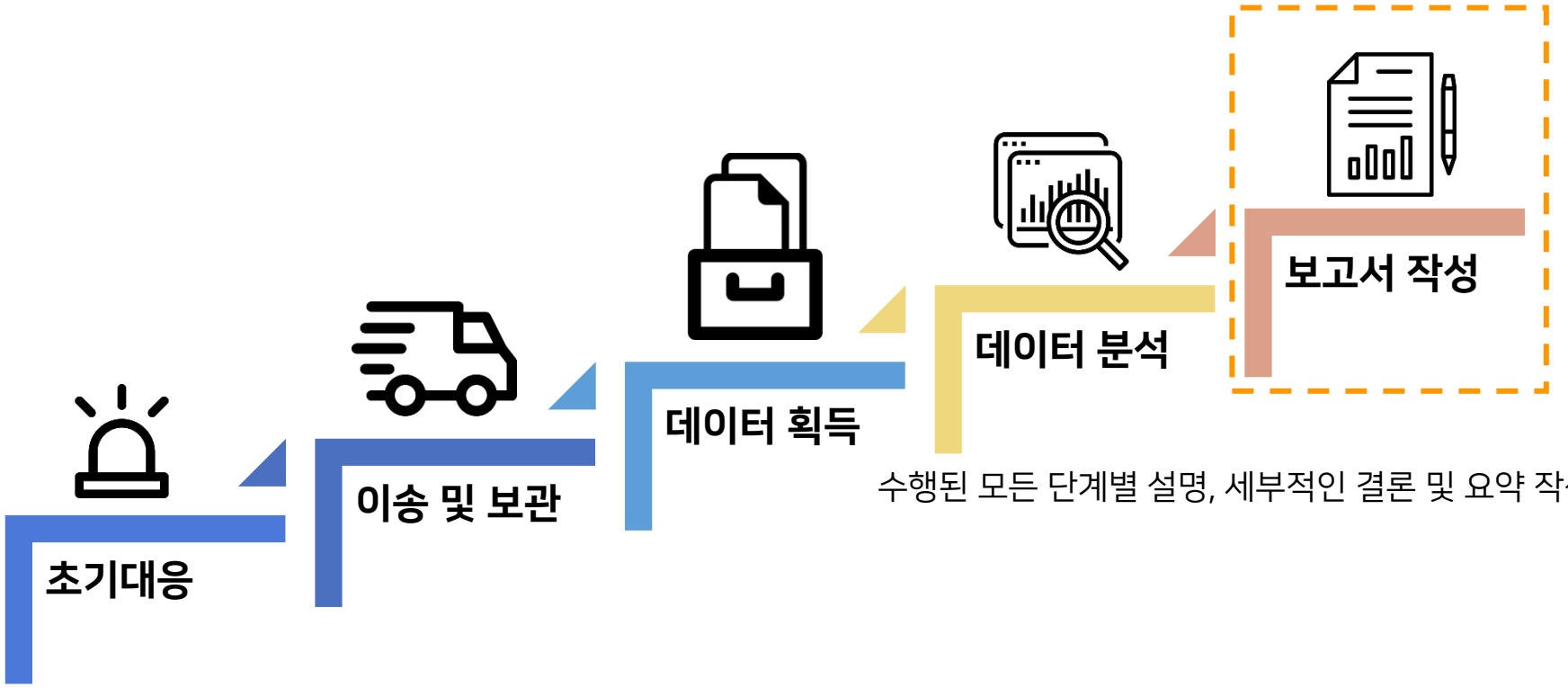
- **모바일 포렌식 절차**
  - 한국 정보 통신 기술 협회(TTA) - TTAK.KO-12.0059/R1



디지털 증거를 분석하여 법정에 제출할 수 있는 상태로 만드는 과정

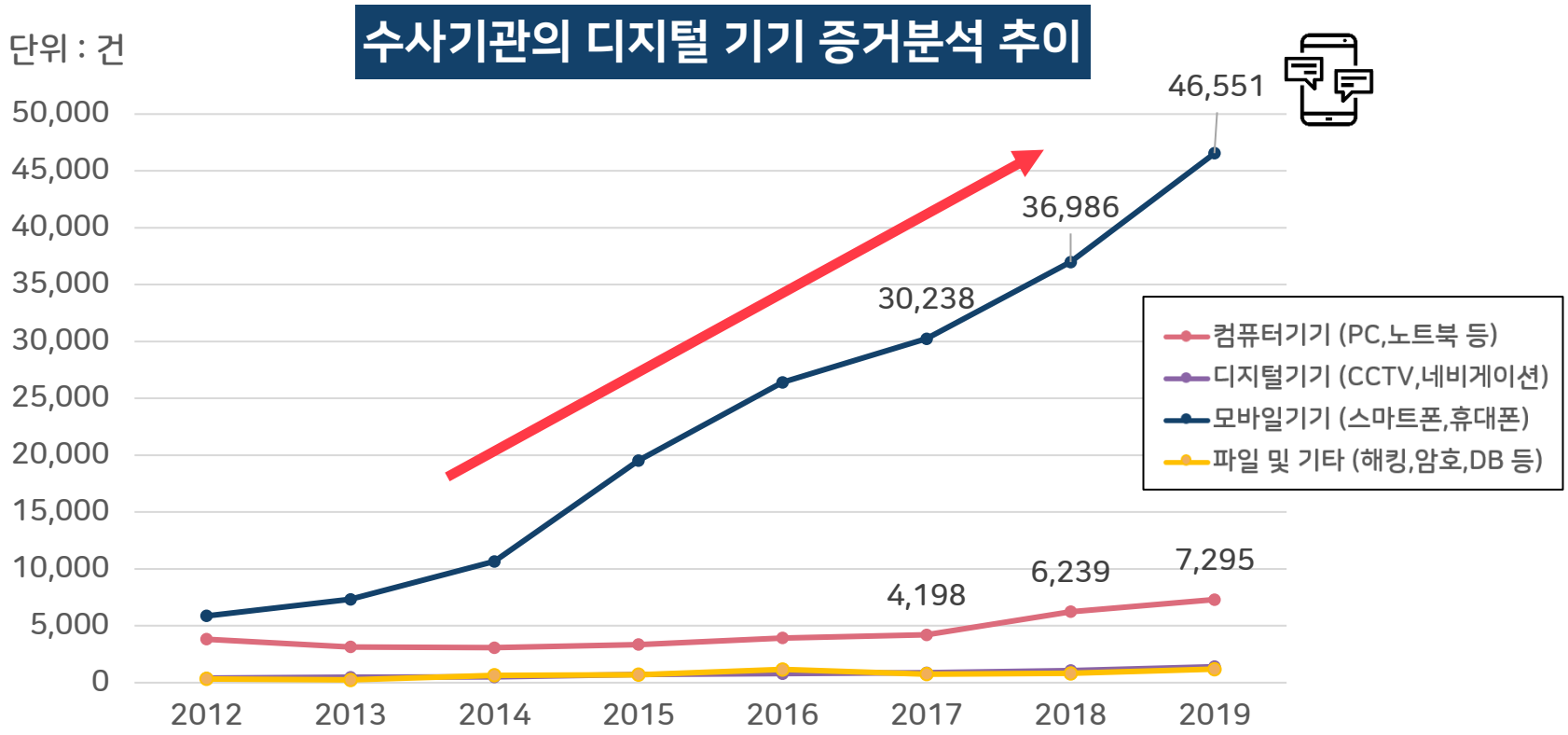
1. 모바일 포렌식 개요

- **모바일 포렌식 절차**
  - 한국 정보 통신 기술 협회(TTA) - TTAK.KO-12.0059/R1



1. 모바일 포렌식 개요

- **스마트폰 포렌식의 중요성**
  - 스마트폰은 디지털 포렌식 대상 기기 중 가장 큰 비율을 차지하고 있음



[출처 : 경찰청 2009~2019 디지털 증거분석 현황]

1. 모바일 포렌식 개요

- **스마트폰 포렌식 사례**

수퍼카 몰던 BJ의 두얼굴...휴대전화에 女화장실 몰카 수두룩

[중앙일보] 입력 2019.12.19 06:24 수정 2019.12.19 10:16

[연합뉴스, 서울시]

공중화장실 등에서 여성들을 불법 촬영한 혐의로 붙잡힌 인기 인터넷 개인방송 진행자(BJ)가 경찰에 구속됐다.

출처 : 중앙일보(https://news.joins.com)

1. 모바일 포렌식 개요

- **스마트폰 포렌식 사례**

130억 대 짝퉁 명품 밀수업자 구속

부산세관, 위조 가방·담배 등 중국산 숯 위장해 들여온 혐의

국제신문 김미희 기자 maha@kookje.co.kr | 입력 : 2020-02-05 23:07:07 | 본지 10면

중국산 숯을 수입하는 것처럼 속여 130억 원대의 짝퉁 명품과 담배를 밀수하려던 업자가 세관에 적발됐다.

5일 부산 강서구 부산본부세관 신항 지정장치장 압수창고에서 세관 관계자들이 압수한 짝퉁 명품과 담배 등을 공개하고 있다. 김종진 기자 kjj1761@kookje.co.kr

부산본부세관은 위조 명품 가방·시계 1449점(시가 123억 원 상당)과 외국으로 수출했던 국산 담배 8만9580갑(시가 4억 원 상당)을 밀수입한 혐의로 수입업자 A 씨를 구속했다고 5일 밝혔다.

출처 : 국제신문(www.kookje.co.kr)

1. 모바일 포렌식 개요

- **스마트폰 포렌식 사례**
  - WhatsApp 마약 갱단 검거

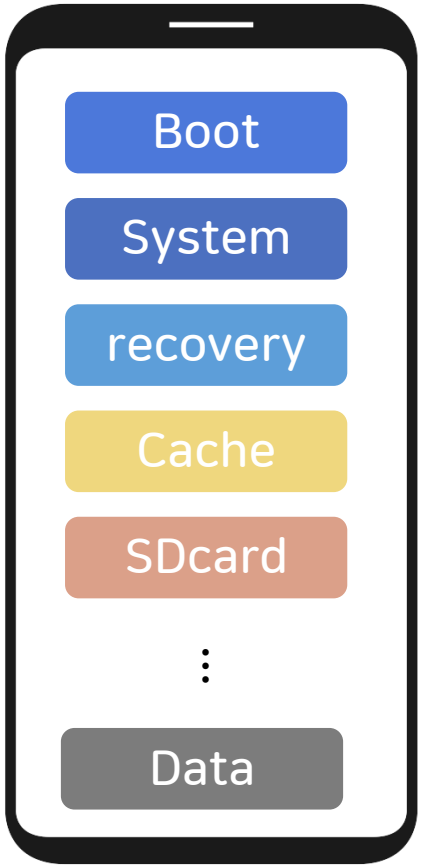
출처 : Bristol Post (https://www.bristolpost.co.uk)

02

스마트폰 데이터 수집

2. 스마트폰 데이터 수집

- **스마트폰 데이터**
  - Android 는 역할에 따라 다양한 partition으로 구분되어 작동함
    - Boot : 스마트폰 부팅에 사용되는 데이터 저장
    - System: 스마트폰 운영과 관련된 데이터 저장
    - Recovery: 스마트폰 복구에 사용되는 데이터 저장
    - Cache: 스마트폰 캐시 데이터 저장
    - SDcard: 문서, 미디어, 사진 등이 저장
    - Data: 사용자가 스마트폰을 사용하며 생성된 사용자 데이터 저장

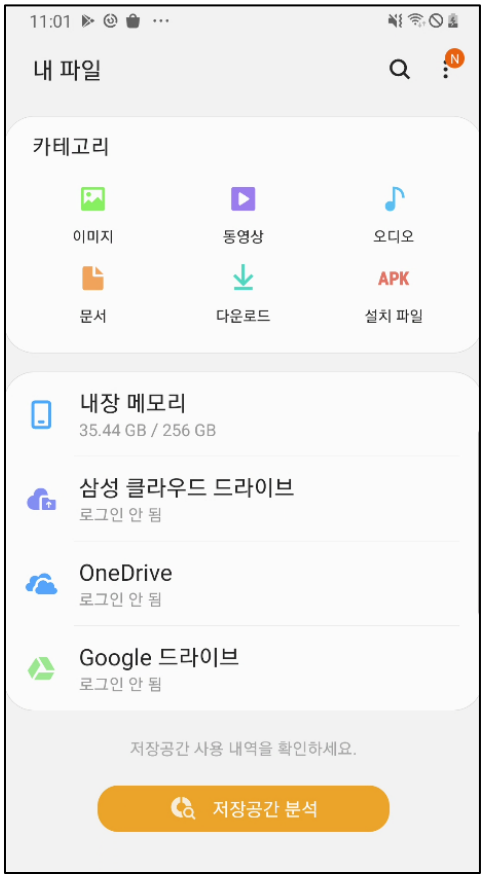


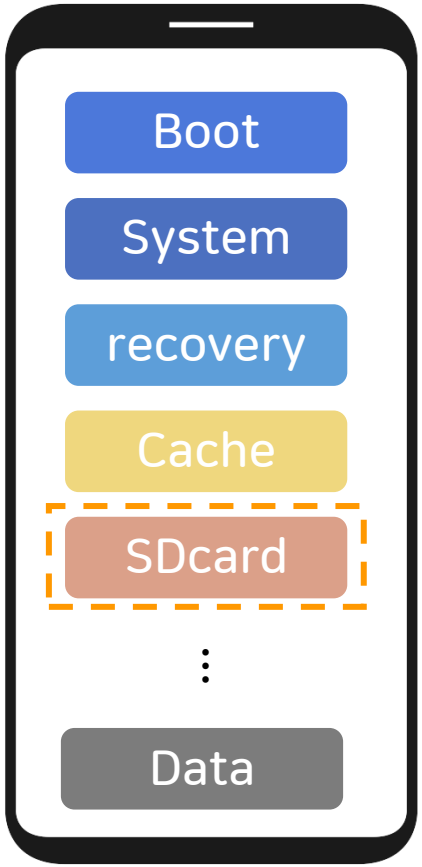
[스마트폰 partition]

2. 스마트폰 데이터 수집

- **스마트폰 데이터**
  - SDcard: 문서, 미디어, 사진 등이 저장

[삼성의 파일 관리 앱]

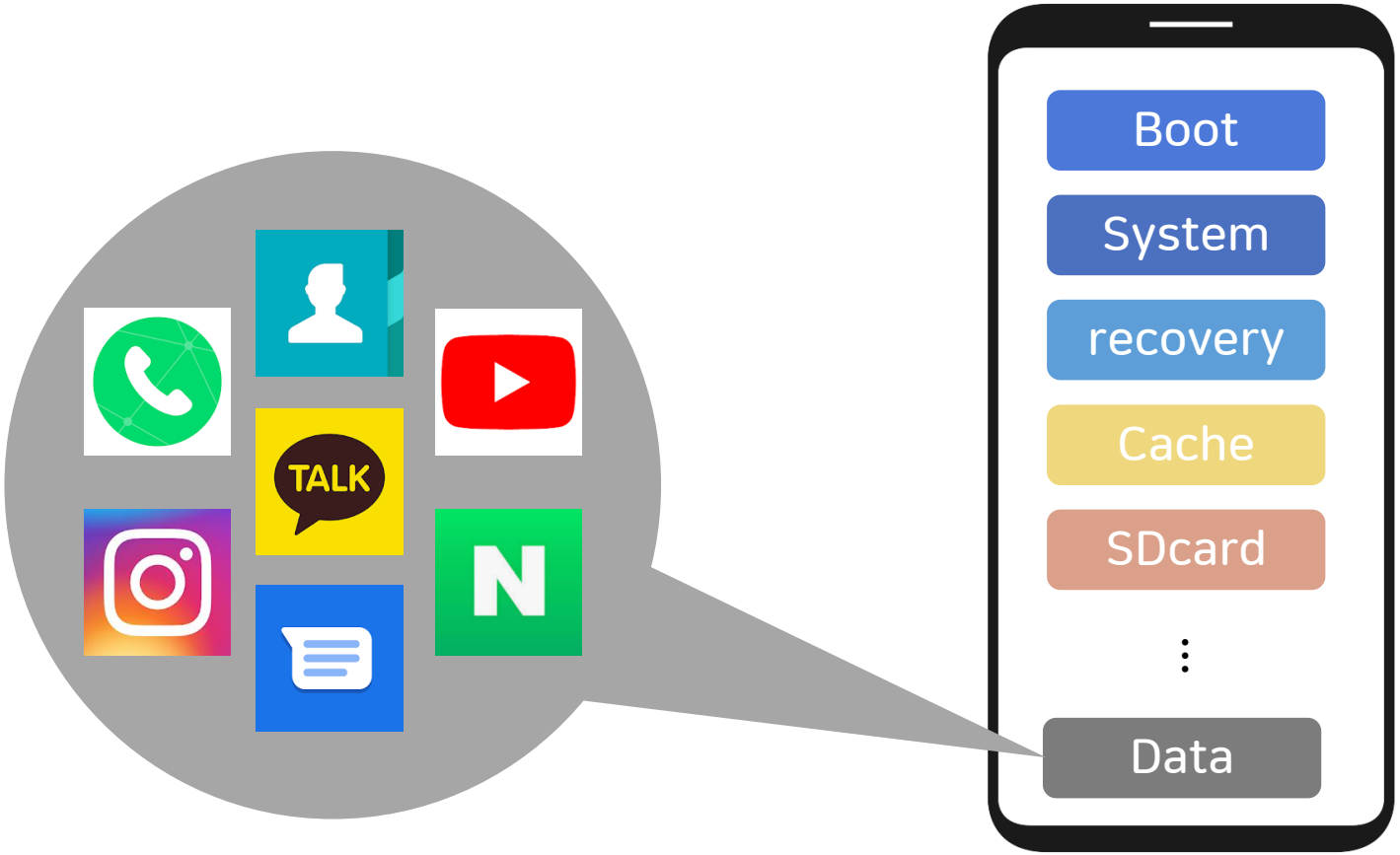




[스마트폰 partition]

2. 스마트폰 데이터 수집

- **스마트폰 데이터**
  - data 파티션에는 사용자가 스마트폰을 사용하며 생성된 데이터가 저장



2. 스마트폰 데이터 수집

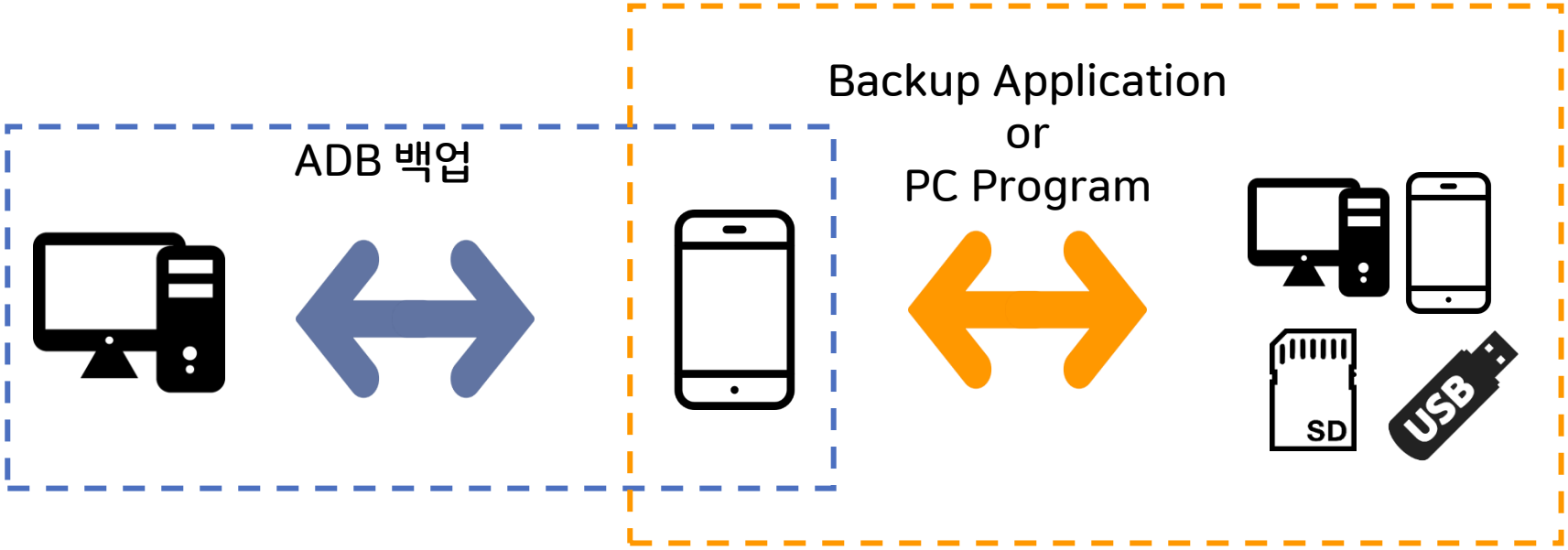
- **스마트폰 데이터**
  - 데이터 영역은 일반적인 접근이 불가능하게 설정
  - 접근 시 루트 권한이 요구됨

2. 스마트폰 데이터 수집

- **루팅**
  - Rooting : 안드로이드 운영체제의 최상위 권한(루트 권한)을 획득하는 것
  - 최상위 권한을 획득하여 스마트폰 내 여러 파티션에 접근 가능

2. 스마트폰 데이터 수집

- **백업**
  - Android 백업
    - 애플리케이션에서 데이터 추출 가능 여부가 설정된 경우에만 백업 가능
  - **제조사 백업**
    - 스마트폰 제조사는 스마트폰의 분실, 파손, 기기변경 시 데이터의 보존을 위해 백업 서비스를 제공
    - 따라서 백업된 데이터에는 스마트폰 내의 거의 모든 데이터가 저장



2. 스마트폰 데이터 수집

- **제조사 백업**
  - 삼성, LG, 애플, 화웨이 등 제조사별 백업 방식 상이


SmartSwitch


LG Bridge


iTunes


HiSuite

✓ 백업 데이터로부터 사용자 데이터 복구를 하기 위해 제조사별로 백업 방식을 분석해야 함

✓ 제조사 별로 사용자의 정보를 포함하는 데이터의 경우, 암호화하여 저장함.

2. 스마트폰 데이터 수집

- **제조사 백업**
  - 백업 데이터 암호화 과정

PIN 또는 패스워드 등 비밀 값 입력

비밀 값 기반 암호키 생성

- SHA256, MD5 등 …
- PBKDF2-HMAC-SHA1
- PBKDF2-HMAC-SHA256 등

백업 데이터 암호화

- 블록암호 : AES, SEED 등
- 운영모드 : CBC, CTR 등
- 패딩 : Zero-padding , PKCS#7Padding 등

랜덤한 SALT

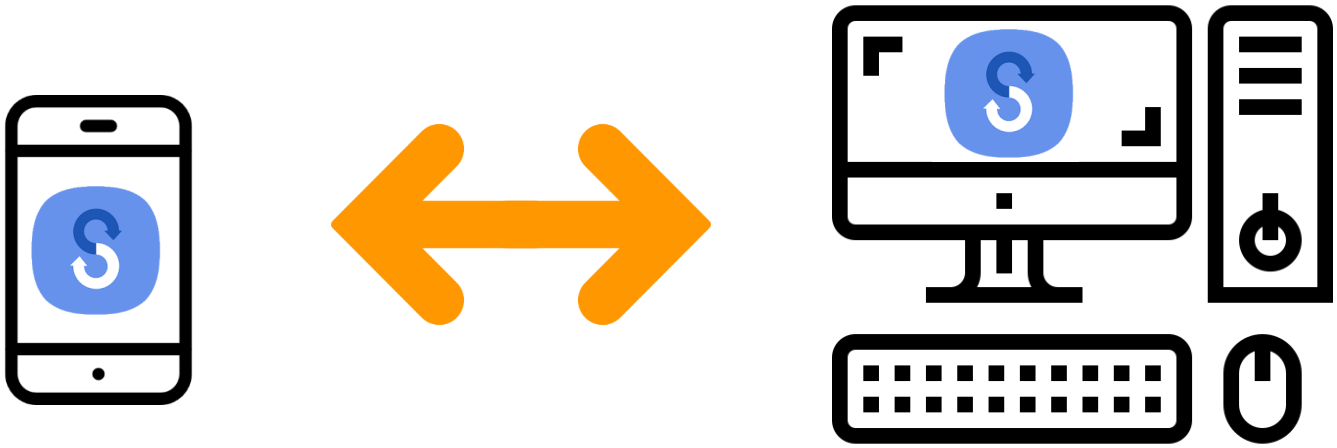
암호키 = PBKDF(비밀 값, SALT, ITERATION)

암호키 = HASH(비밀 값 || SALT)

암호문 = 블록암호-운영모드-패딩(평문, 암호키)

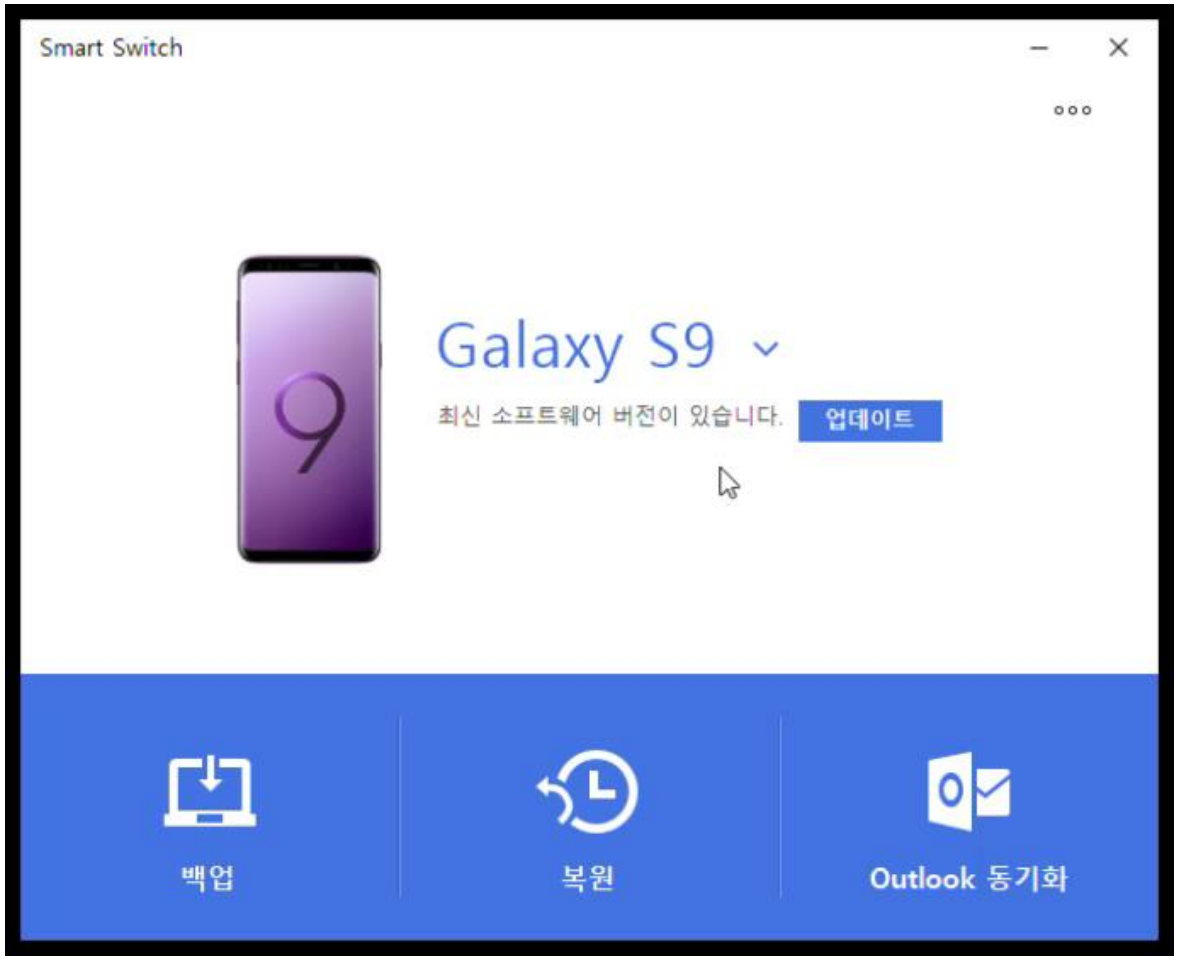
2. 스마트폰 데이터 수집

- **제조사 백업 – Samsung**
  - 모바일 앱 : Samsung Smart Switch Mobile
  - 모바일 앱 패키지명 : com.sec.android.easyMover



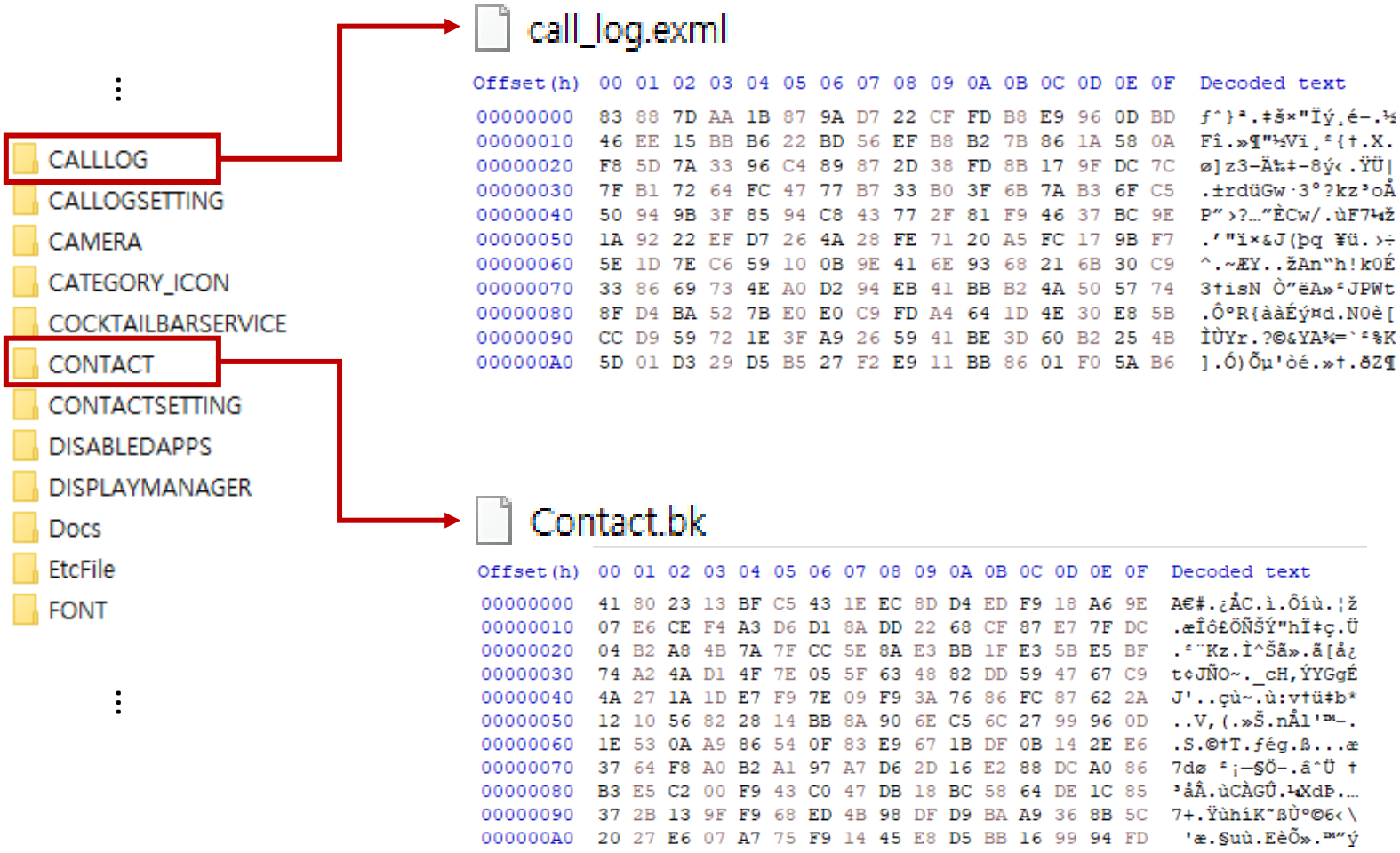
2. 스마트폰 데이터 수집

- 제조사 백업 – Samsung



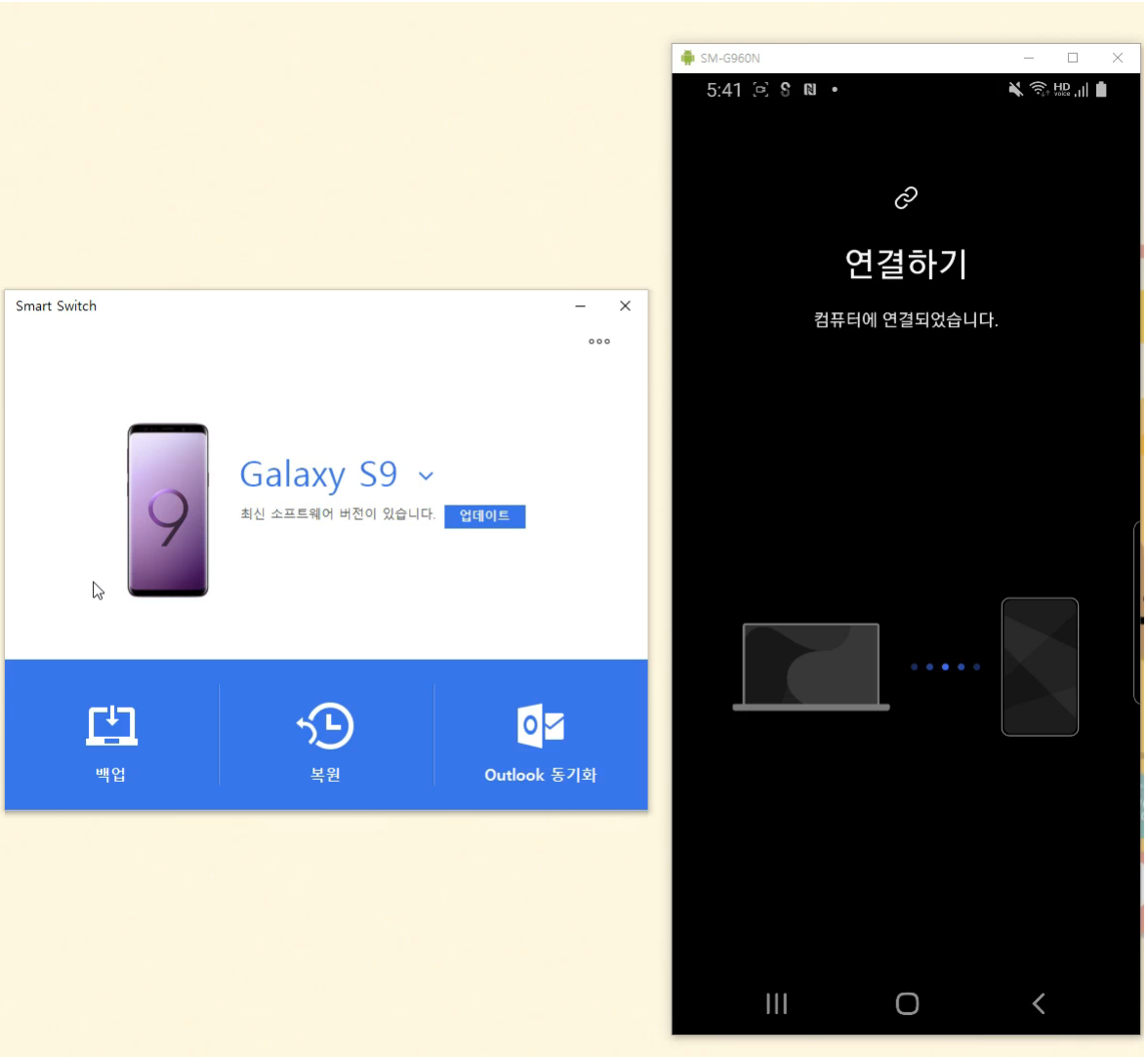
2. 스마트폰 데이터 수집

- **제조사 백업 – Samsung**
  - 암호화된 백업 데이터



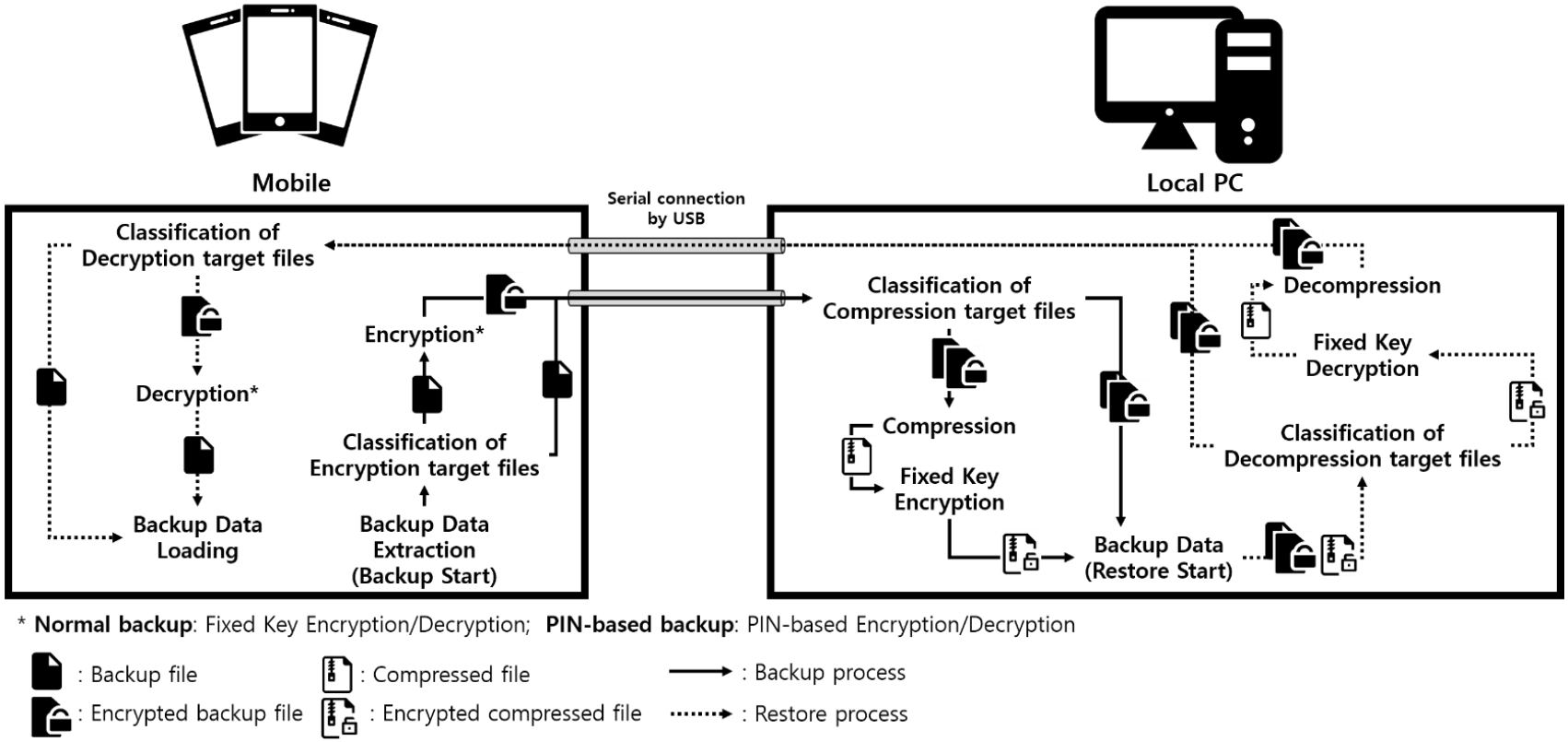
2. 스마트폰 데이터 수집

- 제조사 백업 – Samsung



2. 스마트폰 데이터 수집

- **제조사 백업 – Samsung**



Park, Myungseo, Hangi Kim, and Jongsung Kim. "How to decrypt PIN-Based encrypted backup data of Samsung smartphones." Digital Investigation 26 (2018): 63-71.

2. 스마트폰 데이터 수집

- **제조사 백업 – Samsung**

call_log.exml

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	83	88	7D	AA	1B	87	9A	D7	22	CF	FD	B8	E9	96	0D	BD	ƒˆ}ª.‡š×"Ïý¸é–.½
00000010	46	EE	15	BB	B6	22	BD	56	EF	B8	B2	7B	86	1A	58	0A	Fî.»¶"½Vï¸²{†.X.
00000020	F8	5D	7A	33	96	C4	89	87	2D	38	FD	8B	17	9F	DC	7C	ø]z3–Ä‰‡-8ý‹.ŸÜ|
00000030	7F	B1	72	64	FC	47	77	B7	33	B0	3F	6B	7A	B3	6F	C5	.±rdüGw·3°?kz³oÅ
00000040	50	94	9B	3F	85	94	C8	43	77	2F	81	F9	46	37	BC	9E	P"›?…"ÈCw/.ùF7¼ž
00000050	1A	92	22	EF	D7	26	4A	28	FE	71	20	A5	FC	17	9B	F7	.'"ï×&J(þq ¥ü.›÷
00000060	5E	1D	7E	C6	59	10	0B	9E	41	6E	93	68	21	6B	30	C9	^.~ÆY..žAn"h!k0É
00000070	33	86	69	73	4E	A0	D2	94	EB	41	BB	B2	4A	50	57	74	3†isN Ò"ëA»²JPWt
00000080	8F	D4	BA	52	7B	E0	E0	C9	FD	A4	64	1D	4E	30	E8	5B	.Ô°R{ààÉý¤d.N0è[
00000090	CC	D9	59	72	1E	3F	A9	26	59	41	BE	3D	60	B2	25	4B	ÌÙYr.?©&YA¾=`²%K
000000A0	5D	01	D3	29	D5	B5	27	F2	E9	11	BB	86	01	F0	5A	B6	].Ó)Õµ'òé.»†.ðZ¶
000000B0	32	90	A7	8C	FB	50	6D	E8	42	E8	2C	03	44	CC	38	60	2.§ŒûPmèBè.,.DÌ8`

dec_call_log.exml

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	3C	3F	78	6D	6C	20	76	65	72	73	69	6F	6E	3D	27	31	<?xml version='1
00000010	2E	30	27	20	65	6E	63	6F	64	69	6E	67	3D	27	55	54	.0' encoding='UT
00000020	46	2D	38	27	20	73	74	61	6E	64	61	6C	6F	6E	65	3D	F-8' standalone=
00000030	27	79	65	73	27	20	3F	3E	3C	43	61	6C	6C	4C	6F	67	'yes' ?><CallLog
00000040	73	3E	3C	43	61	6C	6C	4C	6F	67	3E	3C	64	61	74	65	s><CallLog><date
00000050	3E	31	35	37	36	38	30	34	35	32	37	36	33	31	3C	2F	>1576804527631</
00000060	64	61	74	65	3E	3C	64	75	72	61	74	69	6F	6E	3E	30	date><duration>0
00000070	3C	2F	64	75	72	61	74	69	6F	6E	3E	3C	6E	75	6D	62	</duration><numb
00000080	65	72	3E	30	30	37	37	37	37	31	31	31	31	31	31	31	er>00777711111111
00000090	31	3C	2F	6E	75	6D	62	65	72	3E	3C	74	79	70	65	3E	1</number><type>
000000A0	31	3C	2F	74	79	70	65	3E	3C	6C	6F	67	74	79	70	65	1</type><logtype
000000B0	3E	33	30	30	3C	2F	6C	6F	67	74	79	70	65	3E	3C	6D	>300</logtype><m

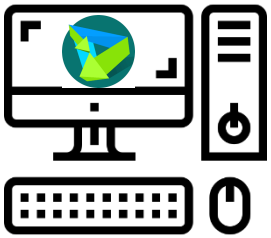
통화날짜

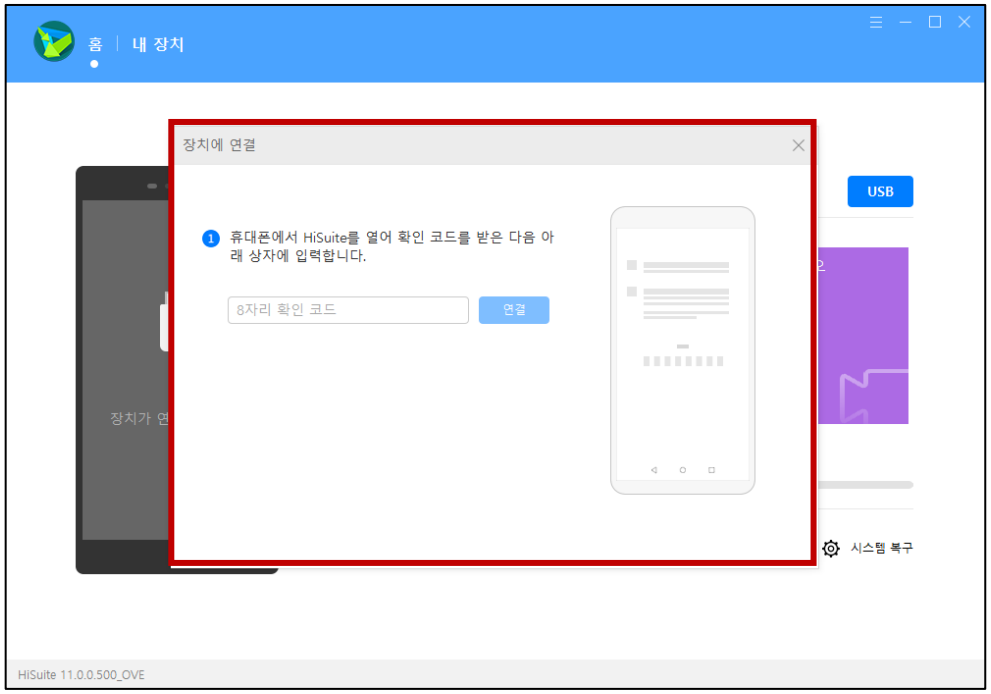
통화 시간

통화 대상 전화번호

2. 스마트폰 데이터 수집

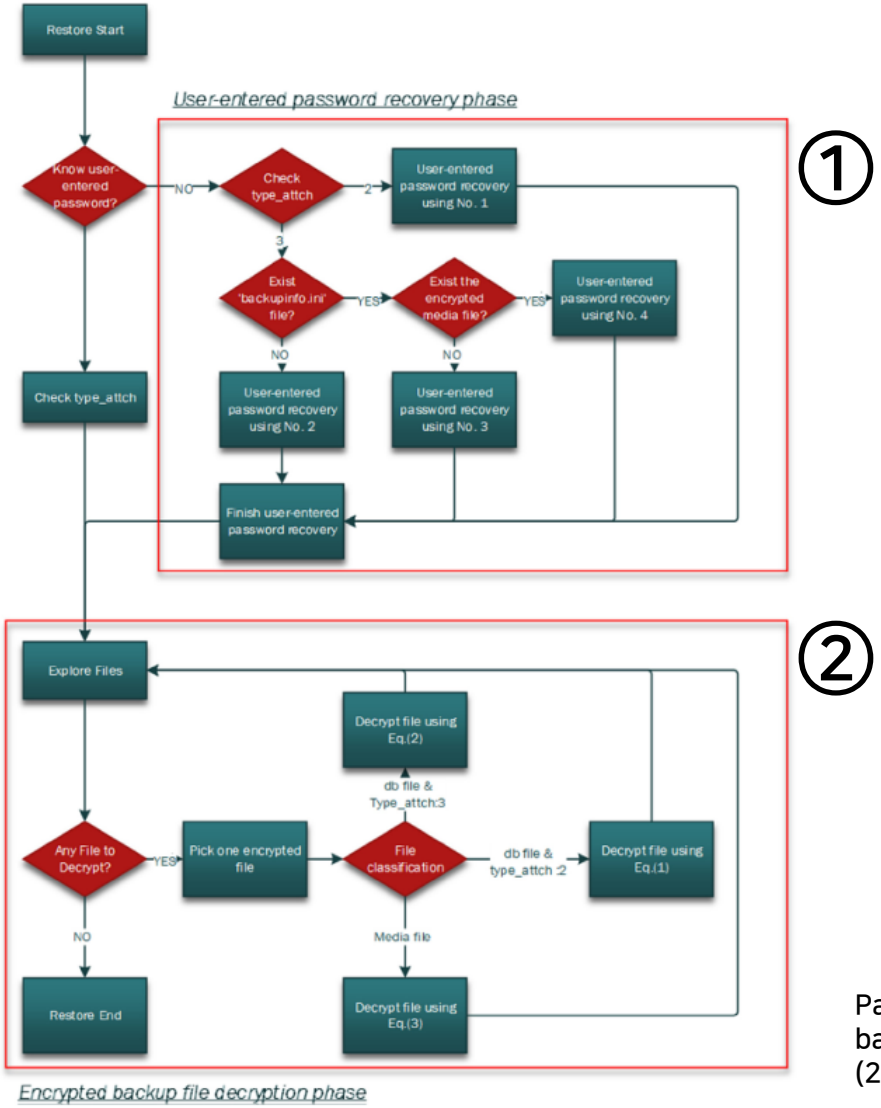
- **제조사 백업 – Huawei**
  - PC 앱 : HiSuite
  - 모바일 앱 패키지명 : com.huawei.hisuite





2. 스마트폰 데이터 수집

- 제조사 백업 – Huawei



Park, Myungseo, et al. "Decrypting password-based encrypted backup data for Huawei smartphones." Digital Investigation 28 (2019): 119-125.

2. 스마트폰 데이터 수집

- **제조사 백업 – Huawei**

sms.db

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	A4	2D	9B	96	BD	AE	C6	88	23	B8	4C	12	8F	D6	F7	83	¤-›–½®Æˆ#¸L..Ö÷ƒ
00000010	4B	13	6B	5A	D2	0B	78	80	FA	80	5F	7A	30	15	C7	59	K.kZÒ.x€ú€_z0.ÇY
00000020	D5	AB	33	A8	2A	E5	C6	5A	E0	B8	39	2D	82	1E	F7	EF	Õ«3¨*åÆZà¸9-‚.÷ï
00000030	80	44	3A	7E	EE	0E	42	6A	E1	3B	E0	91	F8	D4	FE	1B	€D:~î.Bjá;à‘øÔþ.
00000040	4B	3D	69	E7	E6	60	89	5D	36	6B	34	8D	6F	5C	22	03	K=içæ`‰]6k4.o\".
00000050	EE	2C	90	76	84	02	55	9E	FE	90	D6	50	4D	58	1A	B5	î,.v„.Užþ.ÖPMX.µ
00000060	0A	6D	C2	9D	27	C7	74	A2	61	C0	28	53	91	67	89	8F	.mÂ.'Çt¢aÀ(S‘g‰.
00000070	14	13	57	46	1A	56	78	DA	AF	2B	B6	97	44	A6	2D	F8	..WF.VxÚ¯+¶—D¦-ø
00000080	7B	47	94	63	2B	C3	C1	BE	7A	FC	B3	9C	23	7A	86	89	{G”c+ÃÁ¾zü³œ#z†‰
00000090	A6	87	4E	49	19	E5	01	D7	DC	9F	2B	1F	DC	57	C0	71	¦‡NI.å.×ÜŸ+.ÜWÀq
000000A0	9F	88	52	9B	E5	4E	D0	EC	92	58	C8	FF	9F	21	2F	CF	ŸˆR›åNÐì’XÈÿŸ!/Ï
000000B0	72	ED	57	7C	CA	89	3E	36	D0	EA	84	61	85	E8	DF	61	ríW|Ê‰>6ÐÊ„a…èßa

[암호화된 sms.db]

body
필터
[국외발신]<#> Your WhatsApp code: 367-967
[Web발신]<#> LINE 인증번호 : 781255 (30분간 유효합니다)
[Web발신]<#> LINE 인증번호 : 878917 (30분간 유효합니다)
[국외발신]Your Messenger verification code is G-956264
[Web발신] [KT안내] 자급단말은 통화/MMS/데이터 서비스의 품…
Waiting
ㅎㅇ
hi~
Nice to meet you
Hi
[Web발신]잔액 11385원(사용기한 21년07월25일), 음성망내통화 …
[Web발신] [KT안내] 자급단말은 통화/MMS/데이터 서비스의 품…

[복호화된 sms.db 일부]

Thank you