

## 201 – Leakage of Confidential Files

### Team Information

Team Name: ISEGYE\_IDOL

Team Member: Eungchang Lee, Sojeong Kim, Mingyu Seong, Donghyun HA

Email Address: dfc-isegyeidol@googlegroups.com

### Instructions

**Description** An employee in DFC company leaked files containing confidential information. A police received a call from the DFC company and started an investigation. Under the investigation, the digital forensic unit of the police collected smartphone data of a suspect. Analyze digital traces relating to the leakage of confidential files to answer the following questions.

Target	Hash (MD5)
data.zip	6dcbb9bcff6e0e0d133e723fcf2a9d0f

### Questions

- # Please solve all problems based on UTC+9 time zone.
- 1) Provide the name of the application that the suspect used to share the leaked confidential data. (50 points)
  - 2) Provide the private number of the person who received the confidential data. (50 points)
  - 3) Provide names, shared times, and expiration times of all the leaked files. (50 points)
  - 4) Provide read times of all the leaked files. (50 points)

Teams must:

- Develop and document the step-by-step approach used to solve this problem to allow another examiner to replicate team actions and results.
- Specify all tools used in deriving the conclusion(s).

**Tools used:**

Name:	DB Browser for SQLite	Publisher:	sqlitebrowser
Version:	3.12.2		
URL:	<a href="https://sqlitebrowser.org/">https://sqlitebrowser.org/</a>		

Name:	jadx-gui-1.3.5-with-jre-win	Publisher:	skylot
Version:	1.3.5		
URL:	<a href="https://github.com/skylot/jadx/releases">https://github.com/skylot/jadx/releases</a>		

Name:	samsung-private-share-1-1-10-41.apk	Publisher:	APKMirror
Version:	1.1.10.41		
URL:	<a href="https://www.apkmirror.com/apk/samsung-electronics-co-ltd/samsung-private-share/samsung-private-share-1-1-10-41-release/">https://www.apkmirror.com/apk/samsung-electronics-co-ltd/samsung-private-share/samsung-private-share-1-1-10-41-release/</a>		

Name:	JSON Viewer	Publisher:	CodeBeautify
Version:	6.2		
URL:	<a href="https://codebeautify.org/jsonviewer">https://codebeautify.org/jsonviewer</a>		

Name:	Autopsy	Publisher:	CodeBeautify
Version:	6.2		
URL:	<a href="https://codebeautify.org/jsonviewer">https://codebeautify.org/jsonviewer</a>		

## Step-by-step methodology:

**1. Provide the name of the application that the suspect used to share the leaked confidential data. (50 points)**

용의자의 기밀 유출에 사용된 어플리케이션을 용이하게 찾기 위해 안드로이드 데이터 2575개의 폴더 중 실제 데이터가 0 이상인 파일로만 선별했고, 1620개의 폴더로 제한했다.

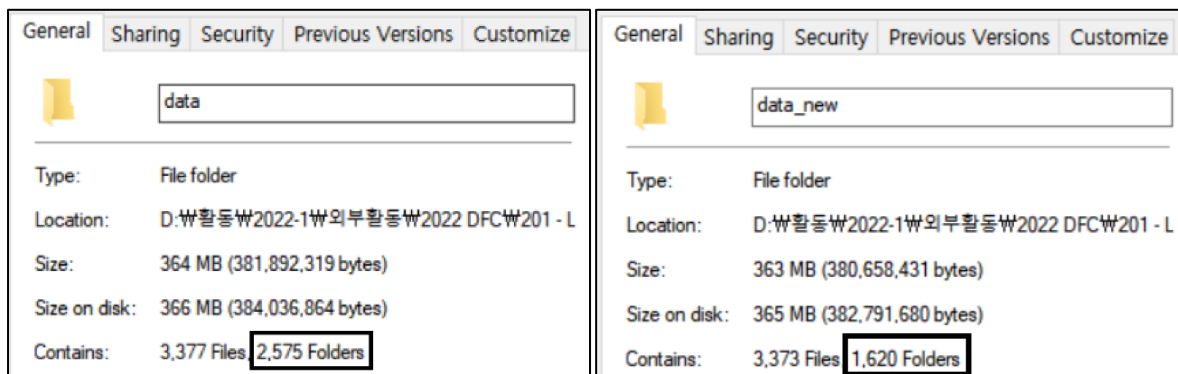
```
def get_dir_size(path='.'):
    total = 0
    with os.scandir(path) as it:
        for entry in it:
            if entry.is_file():
                total += entry.stat().st_size
            elif entry.is_dir():
                total += get_dir_size(entry.path)
    return total

def Finder(path):
    data_folder = path + 'data/'
    data_new_folder = path + 'data_new/'

    # create data_new_folder
    create_folder(data_new_folder)

    # Finder [1] Size > 0
    for f in os.scandir(data_folder):
        # subdir and sizeof(subdir) > 0
        if f.is_dir() and get_dir_size(f.path) > 0:
            # copy dir
            shutil.copytree(f.path, data_new_folder + f.name)
```

[그림 1] 폴더 선별



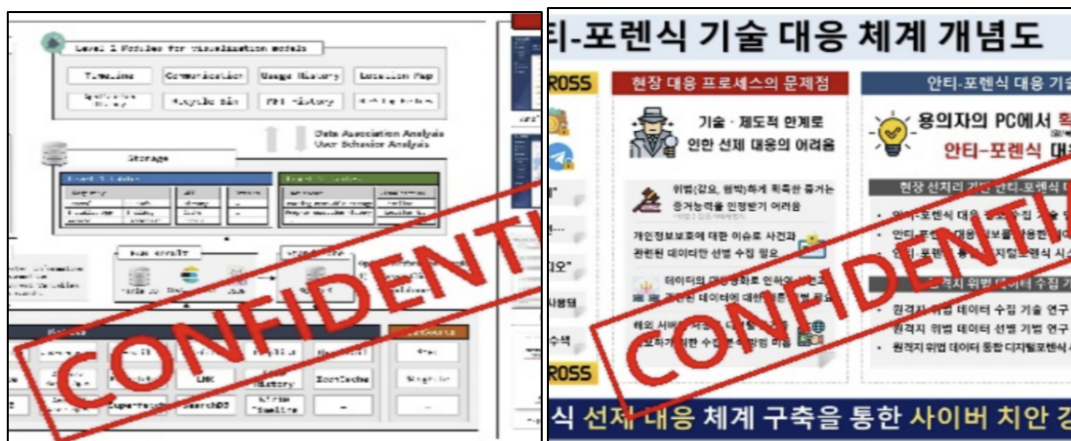
[그림 2] [그림 3] 폴더 및 파일 정보

Private share App 하위 데이터는 모자이크(블러) 처리가 되어 있는 PNG 이미지 파일 두 장이 있는데, 이는 Gallery3d 캐시 이미지들과 시각적으로 유사할 뿐만 아니라 2022년 4월 27일 수요일, 오후 2시 7분 경 동일 시간대에 생성되었다. Gallery3d는 아카이브 형태의 캐시로, 안드로이드 운영체제에서 파일을 다시 열 때 더 빨리 로드할 수 있도록 설계되어 사용자의 파일 접근 행위를 추적할 수 있다.



[그림 4] [그림 5] com.samsung.android.privateshare

그림 4	ap-northeast-2x88ec45c3193440e1af0212de3d1b04f3	2022년 4월 27일 수요일, 오후 2:07:12
그림 5	ap-northeast-2x4265581063e04d90b24047ff13f7082b	2022년 4월 27일 수요일, 오후 2:07:08



[그림 6] [그림 7] com.sec.android.gallery3d/cache/

그림 6	-350089916436148819.0	2022년 4월 27일 수요일, 오후 2:07:00
그림 7	5087384362478750570.0	2022년 4월 27일 수요일,

	오후 2:07:00
--	------------

Gallery3d 캐시 이미지 내부에 “CONFIDENTIAL” 워터마크가 삽입되어 있다. 따라서 Gallery3d 캐시 이미지로부터 용의자는 기밀 파일에 접근했으며 이러한 기밀 파일을 유출할 때 사용한 어플은 Private share Application로, 공유한 파일이 모자이크(블러) 처리되어 캐시가 남아 있는 상황이다.

Private share App은 블록체인 기술을 이용하여 신용카드나 비밀번호, 사진, 동영상, 녹음 파일 등 콘텐츠 공유 시 제한된 사람에게 제한된 권한만 부여하여 개인정보를 보호할 수 있는 솔루션으로, 제한된 수신에게 읽기 권한만 주고, 내가 원하면 언제든지 삭제하거나 정해 놓은 시간에 맞춰서 삭제할 수도 있어 걱정 없이 파일을 공유할 수 있는 어플이다.

## 2. Provide the private number of the person who received the confidential data. (50 points)

Private Share App 데이터의 하위 데이터 [SamsungAnalyticsPrefs.xml] 내부 appVersion 태그에서 용의자가 사용한 어플리케이션의 버전이 1.1.10.41임을 확인하여 동일한 apk를 다운로드 받아 정적 분석을 진행했다.

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
  <int name="auIdType" value="1" />
  <long name="sendCommonTime" value="1650985749266" />
  <string name="appVersion">1.1.10.41</string>
  <string name="deviceId">X4WhOhj8tvgqRhzw3KI5g2Zjcdxe3AWM</string>
  <boolean name="sendCommonSuccess" value="true" />
</map>
```

[그림 8] XML 내부의 어플리케이션 버전 확인

Private share App의 decoding된 코드를 보면 “a1”, “a2”부터 “a8”까지 어떤 정보를 가지고 있는지 확인할 수 있다. “a3” 변수는 toAddress로, 파일을 받는 사람(이하 파일 수신자)을 지칭한다.

```

public final class ShareSmartContractArgument$Share {
    public static final a Companion = new a(null);
    @c("a7")
    public final int fileCount;
    @c("a8")
    public final FileMetadata fileMetadata;
    @c("a2")
    public final String fromAddress;
    @c("a5")
    public final String fromSymmetricKey;
    @c("a9")
    public String reserved3;
    @c("a10")
    public String reserved4;
    @c("a1")
    public final String shareId;
    @c("a6")
    public final long timestamp;
    @c("a3")
    public final String toAddress;
    @c("a4")
    public final String toSymmetricKey;
}

```

[그림 9] 디컴파일러로 식별한 변수 정보

Private share App 데이터 중 용의자의 파일 송수신 트랜잭션 로그는 Transaction.db에서 확인 가능하다. DB 내 Transaction 테이블에서 smartContractFunctionId가 40인 행의 smartContractValues를 살펴보면 파일 수신자(a3)를 확인할 수 있으며, SmartContractValues는 JSON 형식으로 구성되어 있다.

smartContractFunctionId ▼	smartContractValues
필터	필터
10	{"members": ...
40	{"a7":1,"a8":{"f2":{"fileName":"[2020] Annual Confidential ...
40	{"a7":2,"a8":{"f2":{"fileName":"[classified] new business ...
40	{"a7":2,"a8":{"f2":{"fileName":"[top-secret] core ...
40	{"a7":1,"a8":{"f2":{"fileName":"[2021] Annual Confidential ...

[그림 10] DB에 저장된 JSON 정보

```

▼ object {8}
  a7 : 1
  ▼ a8 {6}
    ▼ f2 {2}
      fileName : [2020] Annual Confidential Reports.pdf
      thumbnailKey : ap-northeast-2xa1172045aa6b4d9db656c1109c790d18
    f5 : 1651207847048 2022-04-29T04:50:47.048Z
    f6 : GpA1VGC8YY7+kERaqKKirQ==
    f1 : ap-northeast-2xc9dba38e6ef54b10be0a316ac6c243a7
    f3 : TEXT
    f4 : NONE
  a2 : E7XSvCZTCpVt87zAmJvs
  a5 : MIIBhgIBAASCAQBV8XZwW51XpGZhjdEz3JPOQBpiYNT07Bjz1K5iZjw2R+qEFBFZsfAaRND5weWdXeEnMsjwLXHwqNdI4PJHd4hA9
SDycj8M81e6uLwr3h5a5qh5Gw1hx1GrAFp8a/XARzucTyhNPEbgdgH7Jd9RnK20wuQ5PJeFPS1sYLrTREFUY3nN0q81rOf5UYF21nD
u5yb0vj3sSJu4Hw2Q7MYR20s2eFAG1n7zDuHJVZvenXjfeaQBr3j4ZQUBFPDXdo0+q/Bc4wTqokbU1vZsUN12/c51Gb1+j02204hBM
Hp/axgApbvvyPPP7Fv+/jx6biJ1cqAxp3Y/vghKB2mYSsLKKwcDBAw8gIMN8EkH3A9sJDQwOwIBAZA2oQgxBgIBAAIBAAIDAqEgowQC
AgEApAUxAwIBAqUIMQYCAQICASmCDEGAgEBAgFAv4N3AgUABCDsTQo6Maxx2SCOAktHCdrbr9UUubcoBr8hmbM9GWr1EwQQqRtdYH
VYPVvAZp+w7RnB2g==
  a1 : Ma/x1L945pBLDMcLDs2XZAUGLwUJhB1cQmsUkFd8CxU=
  a6 : 1651035047049 2022-04-27T04:50:47.049Z
  a3 : loPpsK5nyxl2nESISf9l
  a4 : MIIBhgIBAASCAQCCs9qys20g1jwT0Cx18fgyPjozNtNkS2TZzuq92LTMQEdHVkQPpFM/Vf9zjzQ8Iwab6N7uMyDFm3XC+302f0yvw3
04Vx0god7Ke6CAQOs/L2ou1pJ7xZiQwPYMKZ6a0Twp0AeAutBZoM1V/rbuJUwey+mGLu2/QXcZFen51d9Yyr1+1PGzBP21X72CN14e
vEda/HRAH089k1nyxIx155gJrGOINPE6p881XNAoDMZafeKu+QvU6N8LmuoAK65vYpcByRquy/dVH29jduViTLM/eIRPM5c/p8Sgpf
V7e6b25rxWQy94dObaHmkrpUDWoPR/T9OPQZA2HC1S0gIB807jBAzmD4Mw7SrpoVYAqnMwOwIBAZA2oQgxBgIBAAIBAAIDAqEgowQC
AgEApAUxAwIBAqUIMQYCAQICASmCDEGAgEBAgFAv4N3AgUABCDsTQo6Maxx2SCOAktHCdrbr9UUubcoBr8hmbM9GWr1EwQQqRtdYH
xTewIVqoS2RYbVZA==

```

[그림 11] JSON Lint 결과

네 번의 트랜잭션 로그가 발견됐고, 모든 트랜잭션의 파일 수신자(a3)는 [loPpsK5nyxl2nESISf9l]이며 용의자가 파일 수신자에게 공유한 파일명은 다음과 같다.

Filename(a8->f2)	파일명	[2020] Annual Confidential Reports.pdf
		[classified] new business plan.png
		[top-secret] core technology.png
		[2021] Annual Confidential Reports.pdf
toAddress(a3)	파일 수신자	loPpsK5nyxl2nESISf9l

DB 내 Transaction 테이블에서 samrtContractFuctionId가 10인 행의 smartContractValues를 살펴보면 멤버 설정 트랜잭션을 확인할 수 있고, 멤버 별 id와 hashedPhoneNumber의 매핑을 확인할 수 있다.

smartContractFunctionId ▼ <sup>1</sup>	smartContractValues
필터	필터
10	{"members":...

[그림 12] DB에 저장된 members 정보

파일 수신자[loPpsK5nyxl2nESlSf9l]의 "hashedPhoneNumber"는 [#5334773805]이다.

```
{
  "members": [
    {
      "address": "E7XSvCZTCpVt87zAmJvs",
      "hashedPhoneNumber": "#8760887424",
      "lastPhoneNumberDigits": "#8760887424",
      "publicKey": "MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsrKVIJUMt8iAZtO+VF24LHBjIE4tZLYPTJnFBdSYQ
+abPuGn9cXzsk80f+l64ewjLzQPMoGSGFD1a1m8KQ/ALuh4UXaSoUZdxXlJpV5hTxNgmFgX+txS1U5o+/KF8wTo0zQUcTdh4
+tm7BYbJ50s99/9q1UR9h8TCOLKpGzb3tXoh4BiUZxyteXC/luUgaPIyTWTHtw6Hg6DwZ59l61oFs5BrXHPF
+qfwJWdp7BYdouVvMbGHEuWfbf+2VSUBPNHJDU1hi2S4q5+5lJGJ0reBMBLX5dxN71hjR8nc1Svkix5PVxwbaVvMhKujfKHo/y
/4/D22ucN2oEHj9lgc0C2nQIDAQAB"
    },
    {
      "address": "loPpsK5nyxl2nESlSf9l",
      "hashedPhoneNumber": "#5334773805",
      "lastPhoneNumberDigits": "#5334773805",
      "publicKey": "MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvc1pEq7l3I7ikFSfBdvtvy3n5s8BPpa0nNTwZrt4S2u
Faym+mYNjfxczThUIY6PP2soBxdZi3xQLhGY6ZGB+Ms/LECYXGE5C1P9xCRpQcMh1h5Y3BWWcK
/2KKmF3VVZhFgYAjEFWEDQUE6QKqW10xhV
+qZiYn36e1sIyCSOMDj4faKCrxAxvUDMUTgl60DjQprLJkS54f0dVyKGNckHZ81hg4kJZ5/cJ0UESkOuZHXzSi1h
/fj3R4Cff9mtEySvyvW502E9wYw5N0pMikZzZjowh
/sQmIsZwx0THzIGvxBks0lshxKTmUaQG0wiViVU1UQoK4QW2hb81NUgaV2DudQIDAQAB"
    }
  ]
}
```

[그림 13] members 내부에 저장된 Address, hashedPhoneNumber

## hashedPhoneNumber

Private share의 decoding된 코드의 Recipient 함수를 보면, 세 번째 인자로 받은 str2 파라미터가 hashedPhoneNumber 값으로 들어간다.

```
public Recipient(Long l2, String str, String str2, Uri uri) {
    j.b(str, "displayName");
    j.b(str2, "hashedPhoneNumber");
    this.contactId = l2;
    this.displayName = str;
    this.hashedPhoneNumber = str2;
    this.thumbnailUri = uri;
}
```

[그림 14] hashedPhoneNumber 변수 파라미터

Recipient를 생성자로 사용하는 코드(c.e.a.C1065k)를 보면, 세 번째 인자를 [a(contact.getPhoneNumber())]로 주는 것을 볼 수 있는데, 이때 a 함수는 phoneNumber가 PrivateNumber이면 그대로 값을 유지하고, 아니라면 C1065k.a를 호출한다.

```
public final List<Recipient> a(List<Contact> list) {
    j.b(list, "contacts");
    ArrayList arrayList = new ArrayList(n.a(list, 10));

    for (Contact contact : list) {
        arrayList.add(new Recipient(null,
            (contact.getExistOnContactProvider()
            PrivateNumberFunctionsKt.isPrivateNumber(contact.getPhoneNumber()))
        ));
    }
}
```



```

contact.getDisplayName()          :          C1054hd.a(contact.getPhoneNumber()),
a(contact.getPhoneNumber(), contact.getThumbnailUri(), 1, null));
    }
    return arrayList;
}

```

[그림 15] 인자 전달 과정 분석

```

public final String a(String str) {
    j.b(str, "phoneNumber");
    return PrivateNumberFunctionsKt.isPrivateNumber(str) ? str : C1065k.a(this.f13347b.a(str, a()));
}

```

[그림 16] C1065k.a 호출 분석

C1065k.a 함수는 phoneNumber을 입력 받아서 SHA3.Digest256()으로 전화번호를 해시한 후 C0850d.a 함수에서 Base64 encoding하는 것을 볼 수 있다.

```

public final class C1065k {
    public static final String a(String str) {
        j.b(str, "$this$sha256");
        b bVar = new b();
        byte[] bytes = str.getBytes(C1157c.f13608a);
        j.a((Object) bytes, "(this as java.lang.String).getBytes(charset)");
        byte[] digest = bVar.digest(bytes);
        j.a((Object) digest, "SHA3.Digest256().digest(this.toByteArray())");
        return C0850d.a(digest);
    }
}

```

[그림 17] SHA3 전화번호 해시 로직

```

public final class C0850d {
    public static final String a(byte[] bArr) {
        j.b(bArr, "$this$encodeToString");
        String encodeToString = Base64.getEncoder().encodeToString(bArr);
        j.a((Object) encodeToString, "Base64.getEncoder().encodeToString(this)");
        return encodeToString;
    }
}

```

[그림 18] Base64 인코딩 로직

hashedPhoneNumber는 phoneNumber가 PrivateNumber인지 아닌지 PrivateNumberFunctionKt의 isPrivateNumber 함수로 검사한다. isPrivateNumber 함수에서 (str, "#", false, 2, null)을 파라미터로 호출한다.

```

public final class PrivateNumberFunctionsKt {
    public static final boolean isPrivateNumber(String str) {
        j.b(str, "$this$isPrivateNumber");
        return y.b(str, "#", false, 2, null);
    }
}

```

[그림 19] isPrivateNumber를 통한 Private Number 검증

변수 i2가 2가 아니라면 false이지만, 호출할 때 i2가 2로 입력 받았으므로 함수 c를 수행한다.

```
public static /* synthetic */ boolean b(String str, String str2, boolean z, int i2, Object obj) {  
    if ((i2 & 2) != 0) {  
        z = false;  
    }  
    return c(str, str2, z);  
}
```

[그림 20] 결과 값 반환 로직

해당 함수를 통해 첫 글자가 "#"이라면 True를 반환하고, 즉 phoneNumber [#숫자] 형식이라면 hashedPhoneNumber에 phoneNumber가 들어가게 된다.

```
public static final boolean c(String str, String str2, boolean z) {  
    j.b(str, "$this$startsWith");  
    j.b(str2, "prefix");  
    return !z ? str.startsWith(str2) : a(str, 0, str2, 0, str2.length(), z);  
}
```

[그림 21] 번호 형식 구성 로직

따라서 hashedPhoneNumber는 phoneNumber가 Private Number이 아니면 SHA256으로 해시하여 Base64 형태로 바꿔주고, phoneNumber가 Private Number이라면 [#숫자] 형식을 갖춘다.

로그 ps.log를 보면 hashedPhonenumber과 phoneNumber가 동일한 것을 확인할 수 있다. 위 Subscription 로그의 세번째 인자에 "phoneNumberSource=PRV"이 포함된다.

```
268 04-27 13:44:11.049 PrivateShare: [MainActivity] onResume  
269 04-27 13:44:11.051 PrivateShare: [BaseFragment:SelectContactsFragment] onResume  
270 04-27 13:44:11.062 PrivateShare: [SelectContactsViewModel] cursor: 0  
271 04-27 13:44:11.077 PrivateShare: [SelectContactsFragment] mySubscription, (Subscription(  
    hashedPhoneNumber=#8760887424, phoneNumber=#8760887424, phoneNumberSource=PRV, simCountryCode=KR,  
    isAvailable=true, simSlotIndex=-1), false)  
272 04-27 13:44:11.077 PrivateShare: [SelectContactsFragment] mySubscription: #8760887424/false
```

[그림 22] 로그 내부의 phoneNumber 조회

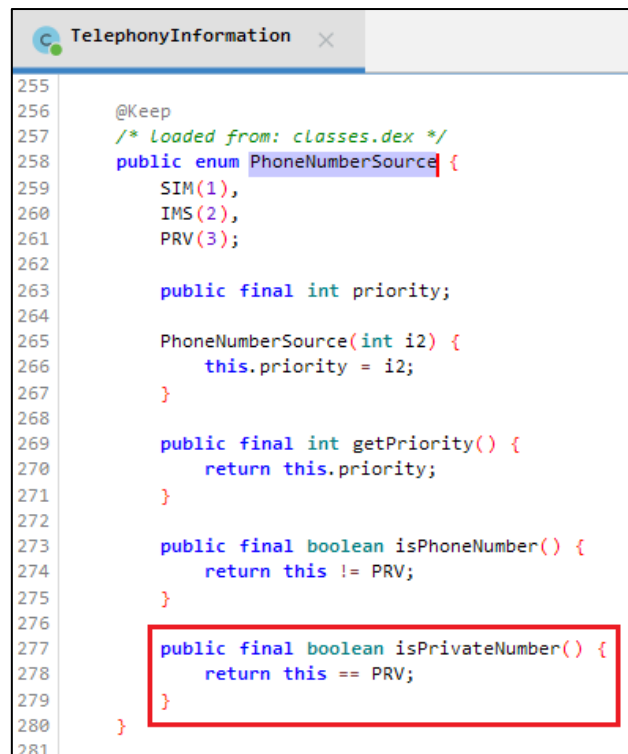
Private Share App의 decoding된 코드 내 Subscription 객체의 세 번째 인자는 phoneNumberSource이며, "PRV" 값을 지니면 PrivateNumber이다.

```

public Subscription(String str, String str2, TelephonyInformation.PhoneNumberSource phoneNumberSource, String str3, boolean z) {
    this(str, str2, phoneNumberSource, str3, z, -1);
    j.b(str, "hashedPhoneNumber");
    j.b(str2, "phoneNumber");
    j.b(phoneNumberSource, "phoneNumberSource");
    j.b(str3, "simCountryCode");
}

```

[그림 23] 로깅 함수와의 비교



```

255
256 @Keep
257 /* Loaded from: classes.dex */
258 public enum PhoneNumberSource {
259     SIM(1),
260     IMS(2),
261     PRV(3);
262
263     public final int priority;
264
265     PhoneNumberSource(int i2) {
266         this.priority = i2;
267     }
268
269     public final int getPriority() {
270         return this.priority;
271     }
272
273     public final boolean isPhoneNumber() {
274         return this != PRV;
275     }
276
277     public final boolean isPrivateNumber() {
278         return this == PRV;
279     }
280 }
281

```

[그림 24] 로깅 함수와의 비교

따라서, "Private Number"와 "hashedPhoneNumber"와 "phoneNumber" 이 세가지 값이 모두 동일한 값이므로, 파일 수신자 [IoPpsK5nyxl2nESISf9l]의 Private Number는 [#5334773805] 이다.

### 3. Provide names, shared times, and expiration times of all the leaked files. (50 points)

Private share App의 decoding된 코드의 "a1"부터 "a8"까지의 내포된 의미는 다음과 같이 정리한다.

a1	공유 ID	a6	Timestamp
a2	파일 공유자 주소	a7	파일 수
a3	파일 수신자 주소	a8	파일 메타데이터
a4	파일 수신자의 대칭키	a9	예약영역 3
a5	파일 공유자의 대칭키	a10	예약영역 4

Private share App 데이터 중 용의자의 파일 송수신 트랜잭션 로그는 Transaction\_database.db에서 확인 가능했고, DB 내 Transaction 테이블에서 SmartContractValues의 JSON 형식으로 트랜잭션 내용이 포함되어 있다. 트랜잭션 데이터를 해석한 결과는 다음과 같다.

행위 (KST)
<p>ID :1</p> <p><b>멤버정보</b></p> <p>1번 멤버</p> <p>privateNum : #8760887424</p> <p>address: E7XSvCZTCpVt87zAmJvs</p> <p>publicKey: 생략</p> <p>2번 멤버</p> <p>privateNum : #5334773805</p> <p>address: loPpsK5nyxl2nESISf9I</p> <p>publicKey: 생략</p>
<p>ID :2</p> <p><b>파일 공유</b></p> <p>공유한 파일의 수: 1</p> <p>파일이름 : [2020] Annual Confidential Reports.pdf</p> <p>썸네일 키 : ap-northeast-2xa1172045aa6b4d9db656c1109c790d18</p> <p>공유 만료 시간 : 1651207847048</p> <p>iv: 생략</p> <p>원본 파일 키 : ap-northeast-2xc9dba38e6ef54b10be0a316ac6c243a7</p> <p>contentType : TEXT</p> <p>보내는 사람의 주소: E7XSvCZTCpVt87zAmJvs</p> <p>share ID: Ma/x1L945pBLDMcLDs2XZAUGLwUJhB1cQmsUkFd8CxU\u003d</p> <p>timestamp: 1651035047049</p> <p>받는 사람의 주소: loPpsK5nyxl2nESISf9I</p>
<p>ID :3</p> <p><b>파일 전송됨(RECEIVED)</b></p> <p>파일 키: ap-northeast-2xc9dba38e6ef54b10be0a316ac6c243a7</p> <p>timestamp: 1651035049368</p>
<p>ID : 4</p> <p><b>파일 다운로드 됨(DOWNLOADED)</b></p> <p>파일 키: ap-northeast-2xc9dba38e6ef54b10be0a316ac6c243a7</p> <p>timestamp: 1651035070302</p>
<p>ID :5</p> <p><b>만료 안내</b></p> <p>만료 시간 :1651056600000</p>

<p>파일 키: ap-northeast-2xc9dba38e6ef54b10be0a316ac6c243a7 timestamp: 1651035153740</p>
<p>ID :6 <b>파일 열림</b> 파일 키: ap-northeast-2xc9dba38e6ef54b10be0a316ac6c243a7 timestamp: 1651035591700</p>
<p>ID :7 <b>파일 열림</b> 파일 키: ap-northeast-2xc9dba38e6ef54b10be0a316ac6c243a7 timestamp: 1651035750450</p>
<p>ID :8 <b>파일 다운로드 됨(DOWNLOADED)</b> 파일 키: ap-northeast-2xc9dba38e6ef54b10be0a316ac6c243a7 timestamp: 1651035757417</p>
<p>ID :9 <b>파일 공유</b> 공유한 파일의 수: 2 파일이름 : [classified] new business plan.png 썸네일 키 : ap-northeast-2x4265581063e04d90b24047ff13f7082b 공유 만료 시간 : 1651208832753 iv: 생략 원본 파일 키 : ap-northeast-2xa2dfc459dd494c4780e9f5318cfde306 mimeType : IMAGE 보내는 사람의 주소: E7XSvCZTCpVt87zAmJvs share ID: WyUI64oH7GmPRTu4VUNif/XMeVytSPYGxe4T7Hlg6ug\u003d timestamp: 1651036032754 받는 사람의 주소: loPpsK5nyxl2nESISf9I</p>
<p>ID :10 <b>파일 공유</b> 공유한 파일의 수: 2 파일이름 : [top-secret] core technology.png 썸네일 키 : ap-northeast-2x88ec45c3193440e1af0212de3d1b04f3 공유 만료 시간 : 1651208832753 iv: 생략 원본 파일 키 : ap-northeast-2x3f5f17e19c2546ea94b32e0a9b039c42 mimeType : IMAGE 보내는 사람의 주소: E7XSvCZTCpVt87zAmJvs share ID: WyUI64oH7GmPRTu4VUNif/XMeVytSPYGxe4T7Hlg6ug\u003d timestamp: 1651036032754</p>

받는 사람의 주소: loPpsK5nyxl2nESISf9I
ID :11 1. <b>파일 전송됨(RECEIVED)</b> 파일 키: ap-northeast-2xa2dfc459dd494c4780e9f5318cfde306 timestamp: 1651036035235 2. <b>파일 전송됨(RECEIVED)</b> 파일 키: ap-northeast-2x3f5f17e19c2546ea94b32e0a9b039c42 timestamp: 1651036037062
ID :12 <b>만료 안내</b> 만료 시간 1651122420000 파일 키: ["ap-northeast-2x3f5f17e19c2546ea94b32e0a9b039c42","ap-northeast-2xa2dfc459dd494c4780e9f5318cfde306"], timestamp: 1651036082015
ID :13 <b>파일 열림</b> 파일 키: ap-northeast-2xa2dfc459dd494c4780e9f5318cfde306 timestamp: 1651036148561
ID :14 <b>파일 다운로드 됨(DOWNLOADED)</b> 파일 키: ap-northeast-2xa2dfc459dd494c4780e9f5318cfde306 timestamp: 1651036154664
ID :15 <b>파일 열림</b> 파일 키: ap-northeast-2x3f5f17e19c2546ea94b32e0a9b039c42 timestamp: 1651036262415
ID :16 <b>파일 다운로드 됨(DOWNLOADED)</b> 파일 키: ap-northeast-2x3f5f17e19c2546ea94b32e0a9b039c42 timestamp: 1651036273291
ID :17 <b>파일 공유</b> 공유한 파일의 수: 1 파일이름 : [2021] Annual Confidential Reports.pdf 썸네일 키 : ap-northeast-2x5f4de9e20dc343afb5432f616f40448d 공유 만료 시간 : 1651210213792 iv: 생략

<p>원본 파일 키 : ap-northeast-2x157f7b97d26a4018a3ae6749e7f403a1</p> <p>contentType : TEXT</p> <p>보내는 사람의 주소: E7XSvCZTCpVt87zAmJvs</p> <p>share ID: z2PeaYrgUVZECvot/Z3E46p85Bo346Qda62nYwKJII\u003d</p> <p>timestamp: 1651037413792</p> <p>받는 사람의 주소: loPpsK5nyxl2nESISf9I</p>
<p>ID :18</p> <p><b>파일 전송됨(RECEIVED)</b></p> <p>파일 키: ap-northeast-2x157f7b97d26a4018a3ae6749e7f403a1</p> <p>timestamp: 1651037418592</p>
<p>ID :19</p> <p><b>만료 안내</b></p> <p>만료 시간 1651059000000</p> <p>파일 키: ap-northeast-2x157f7b97d26a4018a3ae6749e7f403a1</p> <p>timestamp: 1651037469041</p>
<p>ID :20</p> <p><b>파일 열림</b></p> <p>파일 키: ap-northeast-2x157f7b97d26a4018a3ae6749e7f403a1</p> <p>timestamp: 1651037847427</p>
<p>ID :21</p> <p><b>파일 다운로드 됨(DOWNLOADED)</b></p> <p>파일 키: ap-northeast-2x157f7b97d26a4018a3ae6749e7f403a1</p> <p>timestamp: 1651037855837</p>
<p>ID :22</p> <p><b>파일 열림</b></p> <p>파일 키: ap-northeast-2xc9dba38e6ef54b10be0a316ac6c243a7</p> <p>timestamp: 1651038013566</p>
<p>ID :23</p> <p><b>파일 열림</b></p> <p>파일 키: ap-northeast-2x157f7b97d26a4018a3ae6749e7f403a1</p> <p>timestamp: 1651038083950</p>
<p>ID :24</p> <p><b>파일 열림</b></p> <p>파일 키: ap-northeast-2xa2dfc459dd494c4780e9f5318cfde306</p> <p>timestamp: 1651038091661</p>
<p>ID :25</p> <p><b>파일 열림</b></p> <p>파일 키: ap-northeast-2x3f5f17e19c2546ea94b32e0a9b039c42</p> <p>timestamp: 1651038097070</p>

용의자의 Private Share App 데이터에서 트랜잭션이 발생하여 유출한 모든 파일의 파일명, 공유시간, 만료시간은 다음과 같이 정리한다. 공유시간의 경우, 용의자가 파일 공유를 요청한 시간과 파일 전송이 완료된 시간(RECEIVED가 발생한 시간) 두 시간으로 구분되어 정리한다.

파일명	공유시간 (공유 요청, KST)	공유시간 (RECEIVED, KST)	만료시간 (KST)
[2020] Annual Confidential Reports.pdf	2022년 4월 27일 13:50:47	2022년 4월 27일 13:50:49	2022년 4월 29일 13:50:47
[classified] new business plan.png	2022년 4월 27일 14:07:12	2022년 4월 27일 14:07:15	2022년 4월 29일 14:07:12
[top-secret] core technology.png	2022년 4월 27일 14:07:12	2022년 4월 27일 14:07:17	2022년 4월 29일 14:07:12
[2021] Annual Confidential Reports.pdf	2022년 4월 27일 14:30:13	2022년 4월 27일 14:30:18	2022년 4월 27일 14:30:13

#### 4. Provide read times of all the leaked files. (50 points)

용의자의 Private Share App 데이터에서 트랜잭션이 발생하여 유출한 모든 파일의 읽은 시간은 다음과 같이 정리한다.

파일 명	읽은 시간 (KST)
[2020] Annual Confidential Reports.pdf	2022년 4월 27일 13:59:51 2022년 4월 27일 14:02:30 2022년 4월 27일 14:40:13
[classified] new business plan.png	2022년 4월 27일 14:09:08 2022년 4월 27일 14:09:14 2022년 4월 27일 14:41:31
[top-secret] core technology.png	2022년 4월 27일 14:11:02 2022년 4월 27일 14:41:37
[2021] Annual Confidential Reports.pdf	2022년 4월 27일 14:37:27 2022년 4월 27일 14:41:23