جامعة نايف العربية للعلوم الأمنية
Naif Arab University for Security Sciences

Naif Arab University for Security Sciences
Arab Journal of Forensic Sciences & Forensic Medicine
www.nauss.edu.sa
http://ajfsfm.nauss.edu.sa

الجمعية العربية لعلوم الأدلة الجنائية والطب الشرعي
Arab Society for Forensic Sciences and Forensic Medicine

Original Article

# Recovering Data from Password Protected Data Security Applications in Android Based Smartphones

Open Access

**Hammad Riaz***

*Computer Forensics Department, Punjab Forensic Science Agency, Government of the Punjab, Lahore, Pakistan*

## Abstract

The standard method of mobile forensic analysis is to attach the mobile device to forensic tools and to perform logical, file system, or physical extraction. A hindrance in analysis arises if the mobile is not properly supported or data in the handset is secured using data security android applications. The techniques discussed in this paper help in the analysis and extraction of data files secured using data hiding password protected android based applications. A few well known data protection android applications are analyzed. The analysis was performed on both partially supported and fully supported sets.

**Keywords:** Mobile Forensics, Data Security Applications, Password Protected Android Applications, Data Hiding, Information Security.

* Corresponding author: Hammad Riaz
Email: hammad.riaz@hotmail.com

doi: 10.12816/0026463

Production and hosting by NAUSS

## استعادة البيانات المحمية بكلمة سر من الهواتف النقالة المصممة بنظام أندرويد اعتماداً على تطبيقات أمنية

### المستخلص

إن الطريقة القياسية للتحليل الجنائي للهواتف النقالة هي ربطها مع إلى الأجهزة والأدوات المعدة للاستخدام الجنائي وإجراء استخراج للبيانات بشكل منطقي - نظام الملفات - أو فيزيائي. وهناك العديد من الأمور التي تقف عائقاً أمام نجاح هذه المهمة، منها أن يكون الهاتف النقال غير مدعوم بشكل مناسب، أو أن تكون البيانات داخل الهاتف النقال مؤمّنة باستخدام تطبيقات حماية خاصة بنظام أندرويد. إن التقنيات التي تناقشها هذه الورقة تساعد على تحليل واستخراج ملفات البيانات المحمية باستخدام تطبيقات أمنية تعتمد إخفاء البيانات وحمايتها بكلمة السر، مبنية على نظام أندرويد. حيث تم تحليل عدد من تطبيقات حماية البيانات المعروفة القائمة على نظام أندرويد، وتم إجراء التحليل على مجموعتين من الهواتف النقالة المدعومة جزئياً والمدعومة بشكل كامل.

**الكلمات المفتاحية:** علم الهواتف النقالة الجنائي، تطبيقات حماية البيانات، تطبيقات أندرويد للحماية بكلمة سر، إخفاء البيانات، أمن المعلومات.

## 1. Introduction

Computers and mobile devices are now vastly widespread, and the last two decades have witnessed a rapid development in this field. A study conducted in February 2014 suggests that mobile devices, either smartphones or tablets, will grow from over 7.7 billion in 2014 to over 12.1 billion by 2018 [1]. Another study suggests that there will be more than 2 billion smartphone users in 2016 [2]. The information revolution has turned mobile devices from a simple handset to a very complex device. Messages and calls are just basic functions of any smartphone. Smartphones contain a huge repository of data that is a complete profile of any person. In most cases, mobile devices contain more probative information per byte about any person than can be found on a computer [3]. But even in a simple case, it is comparatively more difficult to perform analysis and extract data from a mobile phone than from any computer hard drive. This is mostly because of media differences, interface issues, and different types of operating systems; each brings with them new challenges for forensic analysts. These are basic mobile forensic problems: smartphone forensics is even more problematic.

Criminals use smartphones for sending SMS messages, making calls, and they also use them to take pictures and record videos and audios for various types of criminal activities. Under normal circumstances, if the mobile phone of a suspect is seized for forensic investigations, it would be quite easy for an investigator to analyse its data using standard forensic analysis tools and procedures. However, a huge problem may arise if data like video and audio files, images, and documents etc., are hidden using data security password protected applications. The applications, which are used to protect pictures, audios, videos, applications, documents, or Zip files etc., in a mobile phone, are called Data Security/Hiding Applications. If files are locked/password protected, then such files will not be visible in the mobile phone when performing visual analysis. Through simple visual analysis, a forensic scientist can easily find data security applications installed on the smartphone (if not hidden), but he cannot ascertain the amount and type of data that has been protected or locked by using these applications.

Further difficulties in visual analysis may arise because a data security application itself may be locked by installing another data security application. In that case, an investigator will only be able to see one application upon visual analysis. Using standard mobile forensic tools may reveal more information than visual analysis, but a problem arises when the phone is not fully supported by the forensic tool. Even if the phone is fully supported, there may be no support for the data security application that has been used to hide/lock the data. In certain cases, a forensic tool is capable of extracting data from previous versions of the same data security application, but after a recent update of that security application, the forensic tool is unable to retrieve protected data.

Further study into the methods and techniques of data extraction from mobile devices is needed to overcome the aforementioned obstacles. Failure to do so may severely affect the outcome of crime investigation due to a lack of evidence linking the suspect to the crime. The present paper describes a manual protocol for recovering the password protected data from android based smartphones.

## 2. Materials and Methods

Different types of android-based smartphones which are commonly available in the market were chosen as a sample for this study. Video and audio files were then copied in the smart phone’s internal memory by connecting the smart phone to a computer using a mobile phone data cable. Data Security/Hiding Applications were then installed in the phone to secure the uploaded files. Data security applications used to protect the uploaded data were the most widely available and commonly used applications representing mechanisms of data protection. Standard mobile data recovery forensic tools were then used to perform analysis of these smartphones. In addition, advanced forensic techniques were used to extract protected files. The techniques used to successfully extract the data were carefully recorded and documented.

For conducting experimentation and research, a workstation was first configured. The following is a list of equipment used to conduct experiments:

### 2.1 Smartphones

Due to their large number, it was not possible to conduct research on all mobile phone operating systems in just a single study. Therefore, only android operating system (AOS) based mobile phones of different companies and origins were used. Accordingly, analysis results varied with software version of OS, so different versions of the android operating system were also analysed:

1. QMobile Noir A9 (Android version: 4.1.1)
2. Samsung Galaxy S II HD LTE SHV-E120L, Origin: Korean (Android version: 4.1.2)
3. Google Nexus 5 D821 (Android version: 5.1.1)
4. Samsung Galaxy Ace GT-S5830i (Android version: 4.1.1, Build: Jelly Blast v3.0.3) with 2GB microSD Card
5. HTC Wildfire S A510b (Android version: 2.3.5) with 2GB micro SD Card
6. Chinese Chipset based Mobile Set Chassis labelled as Sony G4, (Android version: 4.4.4, Build: ALPS. JB3.MP.V1.6)

All stored data in the mobile phones used in this study was erased and each handset was restored to factory settings prior to the experiments. The contents of internal memories or micro SD cards used in the mobile phones were wiped before experimentation.

### 2.2 Android Data Security Applications used in this Study

1. App Lock version 2.06 and version 2.13.
2. App lock bolo version 2.2.0
3. Safe Gallery version 4.0.4
4. Gallery Lock version 4.9

Practically, it is not possible to discuss all android data security applications here. Only the four above mentioned applications are discussed in this paper. After the installation of these applications on the mobile phones, the WIFI function was switched off.

### 2.3 User Account

Email: Andriod.general@gmail.com, Password: general@123.

### 2.4 Software/ Tools Used

1. Access Data FTK Imager v. 3.1.1.8
2. Quick Hash v. 1.5.5
3. SQLiteStudio v. 3.0.6
4. AccessData FTK v. 4.0.2.2
5. Cellebrite UFED Touch
6. Cellebrite UFED Classic

**Table 1-** *Graphics files reference data set*

| File Name | MD5 Hash | Size (in bytes) |
|---|---|---|
| Batman.jpg | 17EEC073B5FD943251DD58E655D77E2B | 574129 |
| Batman.png | 5EC1B502CB82AD39BDF5027E88E778D5 | 3842109 |
| PFSA.jpg | 529DA30E4B4754D1B5B9ADE8D96162AF | 213602 |
| PFSA.png | 31418B38F7C2292C6BDF088BFCAEADFB | 923593 |
| Ship.jpg | A54A717DB58E60C7B9460EF3FF4A7574 | 198633 |
| Ship.png | 7043ACBB6045D1272599AE7A233840BC | 1769959 |
| Turtle.jpeg | 05712D43A98B8C852CBD9CE07C496479 | 45842 |
| Turtle.png | 3B86A5258DB8B0F880BA7C1B4D8DD0CE | 889445 |

**Table 2-** *Video files reference data set*

| File Name | MD5 Hash | Size (in bytes) |
|---|---|---|
| Wildlife.mp4 | 9DFDD5B2A7FE33D84CED91FDDD6408AE | 1517515 |
| Birds.mp4 | 09E9E81B5757126324970C4403C7EC7C | 617504 |
| Horses.mp4 | 841E6533F81B66525AAF745892EF7884 | 879799 bytes |
| Nature.mp4 | 992E40EB45346BD6AFC2D12F8EA56093 | 3002628 bytes |

**Table 3-** *Applications used to secure graphic files*

| Application | Image File and its Location |
|---|---|
| App Lock | [root]:\Image Gallery\Batman.jpg |
| App Lock | [root]:\Image Gallery\Batman.png |
| App Lock bolo | [root]:\Image Gallery\PFSA.jpg |
| App Lock bolo | [root]:\Image Gallery\PFSA.png |
| Safe Gallery | [root]:\Image Gallery\Ship.jpg |
| Safe Gallery | [root]:\Image Gallery\Ship.png |
| Gallery Lock | [root]:\Image Gallery\Turtle.jpg |
| Gallery Lock | [root]:\Image Gallery\Turtle.png |

**Table 4-** *Applications used to lock files/ folders*

| Application Used | Video File and its Locations |
|---|---|
| App Lock | [root]:\Wildlife\Wildlife.mp4 |
| App Lock bolo | [root]:\Birds\Birds.mp4 |
| Safe Gallery | [root]:\Horses\Horses.mp4 |
| Gallery Lock | [root]:\Nature\Nature.mp4 |

7. MSAB XRY Forensics

### 2.5 Data Sets

Data sets consisted of video files and picture files.

### 2.6 Graphics Files Data Set

Eight pictures i.e. JPG and PNG files were taken as a reference graphics files data set. Their file names, MD5 Hashes and file sizes are given in Table-1.

### 2.7 Video Files Data Set

Four video files were taken as a video reference data set. Their file names, MD5 hashes, and files sizes are given in Table-2.

All pictures were stored in one folder named as "Image Gallery", and that folder was stored at the root of the internal memory/memory card (depending on storage structure) by connecting the mobile phone to the computer.

Table-3 shows which image/graphic file was secured using which application. It also shows the location of the picture/image file.

Video files were stored in respective folders at the root directory of the internal memory of the mobile phone or at the root directory of the memory card (depending on the storage structure of the smartphone). Table-4 shows video file names and the respective folders in which each file was stored. Table-4 also shows which application is used to secure which video file from which location.

### 2.8 Forensic Analysis and Research Constraints

The procedures used in this study are repeatable and reproducible for the same models of mobile phone in similar conditions. However, unlike hard drives, it is difficult to make conditions constant in mobile forensics because smartphones are always active and are constantly updating. However, some major constraints regarding mobile forensics are given below.

#### *2.8.1 Forensic extraction can vary according to the following scenarios*

1. Different Mobile phones with the same version of Android OS
2. Same Mobile phones with different version of Android OS.
3. Custom Built OS of any Android Version.
4. Different software or hardware version of standard mobile forensic tools.
5. Different versions of the same data hiding applications
6. A combination of any of the above discussed scenarios.

The above mentioned scenarios show the complexity involved in the forensic analysis of any mobile phone. Smartphone analysis is always challenging as smartphone companies frequently send updates and modify OS, making it hard for analysts to maintain updated versions of their tools [4]. Analysis is even harder if a new version of an OS is not supported. The huge variety of software and hardware of smartphones is a big issue for forensic examiners [5]. It is to be noted that each forensics company launches frequent updates every year to cope with advances in digital forensics. However, considering budget constraints, this technology may be difficult to acquire. All of these constraints make mobile analysis quite challenging for forensic examiners.

## 3. Results

### 3.1 Extraction Using Standard Mobile Forensic Tools

Standard mobile forensic tools failed to extract these password protected files. Results varied for different phone models, OS versions, and data security application versions. Only some images and video files protected using these tools were retrieved using standard tools. However, even a single file could be of evidentiary value.

### 3.2 Extraction using Proposed Techniques

Here, results of analysis using proposed techniques for each data hiding application are discussed and mechanisms are given to extract data from such applications.

### 3.2.1 Mechanisms Used by Data Security Applications for Security of Protected Data

All data security applications lock the files in a certain vault and provide the user a password protected interface. The user enters the password and the vault opens on the screen of the smartphone. In Gallery Vault, separate folders are normally available for images/graphics and videos etc. Each data security application uses a combination of the below mentioned data hiding mechanisms:

I. Copying files to a new location and deleting the secured files from the original location.

II. Copying files to a new location and wiping the secured files from the original location.

III. Copying the secured files in certain complex folder structures.

IV. Renaming the files to be secured and relocating those renamed files.

V. Appending a proprietary file extension to relocated files.

VI. Removing the extension of file so that interpretation of file features is not possible by the software/ operating system.

VII. Appending a certain amount of bits at the start of the actual file to secure them and make them unintelligible to forensic tools.

VIII. Encrypting the files to be secured.

Dr. Edmond Locard succinctly stated the Locard exchange principle that "Every Contact Leaves a Trace". A perpetrator always leaves some trace at the crime scene which can be recovered and used as forensic evidence. In this case, such perpetrators are data security applications.

### 3.2.2 Data Retrieval Techniques from Data Security Applications

#### 3.2.2.1 App Lock

The Folder "Image Gallery" from which pictures 'Batman.jpg' and 'Batman.png' were secured and the folder "Wildlife" from which Video 'Wildlife.mp4' was secured using App lock were shown empty in the operating system. In FTK Imager, secured files were visible as deleted file inside respective folders. When these deleted files were extracted they did not work as their sizes were 0 MB instead

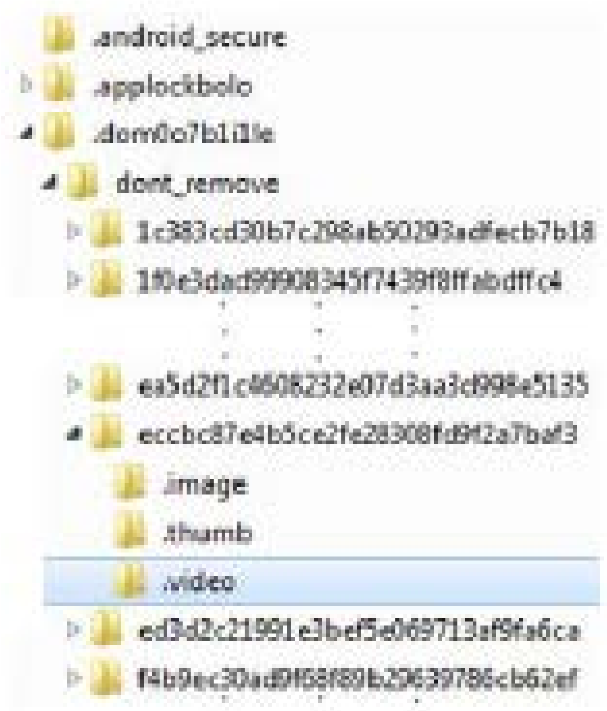

.android_secure
.applockbolo
.dom0o7b1i1le
dont_remove
1c383cd30b7c298ab50293adfecb7b18
1f0e3dad99908345f7439f8ffabdffc4
ea5d2f1c4608232e07d3aa3d998e5135
eccbc87e4b5ce2fe28308fd9f2a7baf3
.image
.thumb
.video
ed3d2c21991e3bef5e069713af9fa6ca
f4b9ec30ad9f68f89b29639786cb62ef

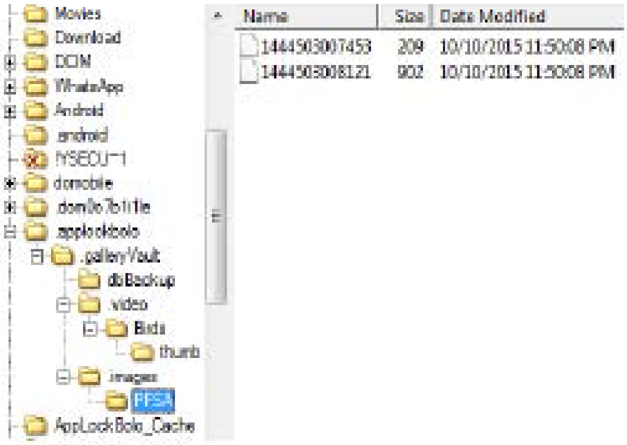
**Figure 1-** *Secured Video Location when using App Lock*

**Table 5-** *Retrieval of secured files from App Lock*

| File | Location of Secured Files |
|---|---|
| Batman.jpg | \.dom0o7b1i1le\dont_remove\6f4922f45568161a8cdf4ad2299f6d23\.image\1444502811635 |
| Batman.png | \.dom0o7b1i1le\dont_remove\98f13708210194c475687be6106a3b84\.image\1444502811974 |
| Wildlife.mp4 | \.dom0o7b1i1le\dont_remove\eccbc87e4b5ce2fe28308fd9f2a7baf3\.video\1444324525275 |
| Thumbnail of 'Wildlife.mp4' | \.dom0o7b1i1le\dont_remove\9a1158154dfa42caddbd0694a4e9bdc8\.thumb\ 1444324525275 |

of their original file sizes which identified that the contents of these files were erased. Table -5 shows locations from where the secured files were retrieved.

The App Lock application renames the secured files and removes the extensions of these files as well. It names the files with a certain number according to an unknown algorithm. App Lock then saves the secured files in complex folder structures. Forensic analysis tools normally fail to extract such files as most tools perform logical analysis and extract data from only known folder structures and databases. Therefore, if a forensic analysis tool supports only logical analysis for a particular smartphone then such secured files will not be extracted. Some forensic tools could search such folders. But as the secured files are without any extension, tools, in most cases, fail to comprehend such files and consider them of no use.



| Name | Size | Date Modified |
|---|---|---|
| 1444503007453 | 209 | 10/10/2015 11:50:08 PM |
| 1444503008121 | 902 | 10/10/2015 11:50:08 PM |

**Figure 2-** *Secured Images Location using App Lock Bolo*

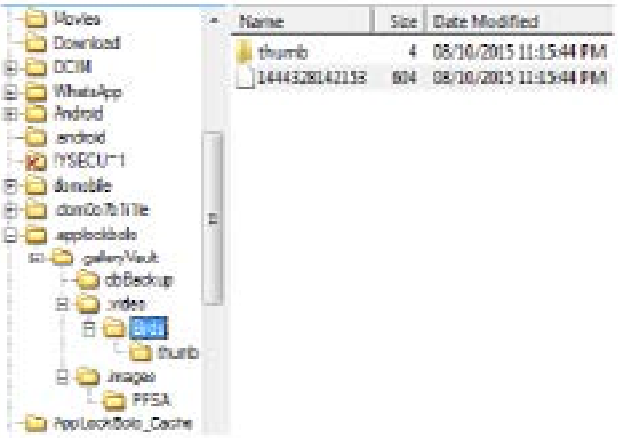
However, a very good forensic software could comprehend the content in the file and might extract it. There is a huge possibility of failure in extraction of such files; therefore, a forensic analyst should know how to extract such files manually from the file system of the smartphone or memory card. The folder in which the video file was secured is shown in Figure-1. Table-5 shows the location from where the secured files were retrieved.

The hash of the respective secured files and original files are exactly the same. Hence, this application does not change the quality of the secured file.

### 3.2.2.2 App Lock Bolo

The folder "Image Gallery" from which graphic files 'PFSA.jpg' and 'PFSA.png' were secured and the folder "Birds" from which video file 'Birds.mp4' was secured are shown empty in the operating system. In FTK Imager, secured files are visible as deleted files inside respective folders. Files are secured in an encrypted format. The folder name 'PFSA' containing graphic/image files is copied inside the '.applockbolo' directory shown in Figure-2. However, file names of images/ graphic files are changed to '1444503007453' and '1444503008121'. Similarly, the folder named as 'Birds' is copied inside the '.applockbolo' directory as shown in Figure-3. The name of the video, however, is changed to '1444328142153'. The thumbnail of the video is also saved in an encrypted format. None of these files work until unlocked by entering the right pass code in App Lock Bolo.

It is observed that the original size of PFSA.jpg was 213,602 bytes, and the size of the secured file was 213,616 bytes, which is 14 bytes larger. The size of 'PFSA.png' was 923,593 bytes, and the size of the secured file was 923,600 bytes. Similarly, the size of the original video was 617,504 bytes, and the size of the secured file was 617,520 bytes, which is 16 bytes larger than the actual file. On viewing the original and secured files in Hex viewer, it was found that the secured files were saved in a totally different format. It was not possible to extract the original files from them. This proved that these files were encrypted.

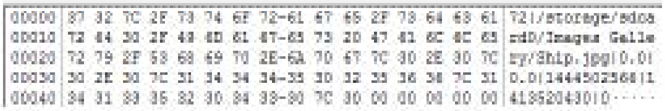


| Name | Size | Date Modified |
|---|---|---|
| thumb | 4 | 08/10/2015 11:15:44 PM |
| 1444328142153 | 604 | 08/10/2015 11:15:44 PM |

**Figure 3-** *Secured Video Location using App Lock Bolo*

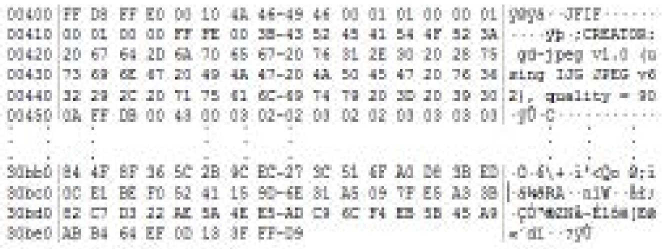
**Table 6-** *Retrieval of secured files from safe gallery*

| File | Location of Secured Files |
|---|---|
| Ship.jpg | [root]:\.SafeGallery\media\20151010235402\1444503242630.slm<br>[root]:\.SafeGallery\media\20151010235402\1444503242630.slt |
| Ship.png | [root]:\.SafeGallery\media\20151010235513\1444503313300.slm<br>[root]:\.SafeGallery\media\20151010235513\1444503313300.slm |
| Horses.mp4 | [root]:\.SafeGallery\media\20151008222403\1444325043471.mp4.slv |



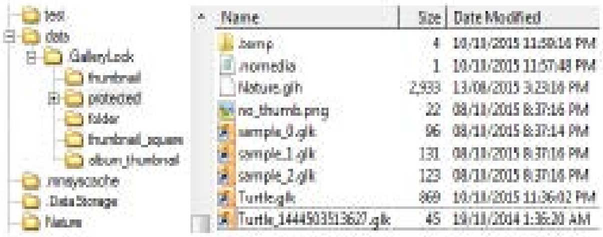
```
00000 37 32 7C 2F 73 74 6F 72-61 67 65 2F 73 64 63 61 72|/storage/sdca
00010 72 64 30 2F 49 6D 61 67-65 73 20 47 61 6C 6C 65 rd0/Images Galle
00020 72 79 2F 53 68 69 70 2E-6A 70 67 7C 30 2E 30 7C ry/Ship.jpg|0.0|
00030 30 2E 30 7C 31 34 34 34-35 30 32 35 36 38 7C 31 0.0|1444502568|1
00040 34 31 38 35 32 30 34 33-30 7C 30 00 00 00 00 00 418520430|0·····
```

**Figure 4-** *Offset 00 of '1444503242630.slm' file*



```
00400 FF D8 FF E0 00 10 4A 46-49 46 00 01 01 00 00 01 ÿØÿà··JFIF······
00410 00 01 00 00 FF FE 00 3B-43 52 45 41 54 4F 52 3A ····ÿþ·;CREATOR:
00420 20 67 64 2D 6A 70 65 67-20 76 31 2E 30 20 28 75  gd-jpeg v1.0 (u
00430 73 69 6E 67 20 49 4A 47-20 4A 50 45 47 20 76 36 sing IJG JPEG v6
00440 32 29 2C 20 71 75 61 6C-69 74 79 20 3D 20 39 30 2), quality = 90
00450 0A FF DB 00 43 00 03 02-02 03 02 02 03 03 03 03 ·ÿÛ·C···········
  .   .   .           .   .   .               .   .   .
  .   .   .           .   .   .               .   .   .
  .   .   .           .   .   .               .   .   .
30bb0 84 4F 8F 36 5C 2B 9C EC-27 3C 51 6F A0 D6 3B ED ·O·6\+·ì'<Qo Ö;í
30bc0 0C E1 BE F0 52 41 16 9D-6E 81 A5 09 7F E6 A3 3B ·á¾ðRA··n·¥··æ£;
30bd0 82 C7 D3 22 AE 5A 4E E5-AD C9 6C F4 EB 5B 45 A9 ·ÇÓ"®ZNå-Élôë[E©
30be0 AB B4 64 EF 0D 13 3F FF-D9                      «´dï··?ÿÙ
```

**Figure 5-** *Offset 1024 to 199656 of 1444503242630.slm file*



```
test
data
  GalleryLock
    thumbnail
    protected
    folder
    thumbnail_square
    album_thumbnail
.nmeyscache
.Data Storage
Nature
```

| Name | Size | Date Modified |
|---|---|---|
| .temp | 4 | 10/10/2015 11:59:16 PM |
| .nomedia | 1 | 10/10/2015 11:57:48 PM |
| Nature.glh | 2,933 | 13/08/2015 3:23:16 PM |
| no_thumb.png | 22 | 08/10/2015 8:37:16 PM |
| sample_0.glk | 96 | 08/10/2015 8:37:14 PM |
| sample_1.glk | 131 | 08/10/2015 8:37:16 PM |
| sample_2.glk | 123 | 08/10/2015 8:37:16 PM |
| Turtle.glk | 869 | 10/10/2015 11:36:02 PM |
| Turtle_1444503513627.glk | 45 | 19/10/2014 1:36:20 AM |

**Figure 6-** *Protected Files in Application 'Gallery Lock'*

**Table 7-** *Retrieval of secured files from gallery lock*

| File | Location of Secured Files |
|---|---|
| Turtle.jpg | [root]:\data\gallerylock\.GalleryLock\protected\Turtle_1444503513627 |
| Turtle.png | [root]:\data\gallerylock\.GalleryLock\protected\Turtle.glk |
| Nature.mp4 | [root]:\data\gallerylock\.GalleryLock\protected\Nature.glh |

App Lock Bolo left security loopholes in its algorithm. App Lock Bolo saves the record of its data in the SQLite database file 'dbBackup.db'. The database contains 13 fields containing complete information about the file's original and secured names, original and secured locations, file types, and extension etc. But there is a big loophole in the programming of this software as it deletes the data from its original location. Therefore, with the help of database 'dbBackup.db', the original files can be recovered from the locations from where respective files were secured by using any data recovery tool.

### *3.2.2.3 Safe Gallery*

The folder "Image Gallery" from which Image files 'Ship.jpg' and 'ship.png' were secured and the folder "Horses" from which video file 'Horses.mp4' was secured are shown empty in the operating system. If a folder itself is secured along with files present in that folder, then the folder along with the files in it will not be visible in the OS. In FTK Imager, secured files are visible as deleted files inside respective folders. When extracted, images and video do not play and their respective sizes are now 0 MB. Table-6 shows the location from where secured files can be retrieved.

It is evident from Table-6 that secured graphic files are stored with '*.slm' extension by safe gallery application. Here, it is to be noted that '.slm' extension is actually associated with Microsoft Visual FoxPro but it will not open in it or in any software. Safe galley is using '.slm' as a proprietary file extension to secure the graphic files. '.slm' is an unknown file extension for graphics, so mobile forensic or computer forensics tools may not identify the file containing valid graphic content. The secured files are analyzed in Hex editor for recovery of valid graphic content from these '.slm' files. It was found that the original extensions i.e. jpg or png etc. along with the location from which the file was secured are visible at offset '00' of these '.slm' files. Figure-4 shows content at offset '00' of file '1444503242630.slm' when file is opened in Hex viewer. The file name and extension shown at offset '00' are 'Ship' and '.jpg' respectively. On close observation, it was found that 1024 bytes are appended before the start of the original file, and the file was then saved with '.slm' extension. In the case of 1444503242630.slm (Figure-5), the original graphic file can be carved from hex offset '400' (1024 in decimal) till the end of file i.e. 30BE8 (199656 in decimal), and that selection can then be saved as a graphic file with the extension given at offset '00'. It is noteworthy that the hash value of the original file and the carved graphic file is exactly the same. The files with extension '.slt' are thumbnails of corresponding '.slm' graphic files.

In the case of the video file, only the '.slv' extension is appended at the end of the file to disguise it. It is done so that the forensic software may wrongly interpret the file with no video content on the basis of a different extension and omit such files during extraction of videos. Secured video file can be extracted from the Gallery Lock folder. The hash value of the original 'Horses.mp4' file and the protected file '1444325043471.mp4.slv' is identical. Hence, data in both files is the same.

#### *3.2.2.4 Gallery Lock*

The Folder "Image Gallery" from which Image files 'Turtle.jpg' and 'Turtle.png' were secured and the folder "Nature" from which Video file 'Nature.mp4' was secured are shown empty in the Windows Operating System. In FTK Imager, secured files are visible as deleted file inside respective folders. When extracted, images and video do not work. Their sizes are now 0 MB. Table-7 shows the location from where we can retrieve the secured files.

Protected files are shown in FTK Imager in Figure-6. On comparing hash values with the original files, it was found that the hashes of respective secured and original files were exactly the same. Only file extensions are changed just to disguise the mobile forensic tools.

It should be noted that the mechanism of retrieval of protected data is the same from almost all android data security applications. All applications use almost the same mechanism of data security as discussed in Data Retrieval Techniques subsection. Here, for simplicity, only the four most widely used data security applications with different methods of securing the files are discussed. However, using similar analysis techniques we can recover data which could be protected using any application.

### 3.3 Smartphone Memory Structure and its Forensic Imaging

Mobile memory structures are of different types. Files secured using data security applications are stored according to the memory structure of the smartphone, which is discussed below:

1. Smartphone with a phone memory (ROM) and a microSD card slot as an external Storage. This type of phone has a memory that ranges from 150MB to almost 500MB. The Samsung Galaxy Ace S5830i and the HTC Wild Fire S are of this type. In this type of device, data security applications make their file structures in the external memory card. The card can be mounted as a Mass Storage Device and then imaged using FTK Imager and can be processed in FTK or Encase etc.
2. Smartphone with a large sized internal memory, normally more than 1 GB, along with an external

SD card slot. The Samsung Galaxy S II SHV-E120L is of this type. In this type of device, data security applications make their file structures and store files in the internal memory. The internal memory can be mounted and then imaged using FTK Imager and can be processed in FTK Tool Kit or Encase etc.

3. Smartphone with a small phone memory, large internal memory, and an external SD card slot for extra storage capacity. In this type of device, phone memory is normally less than 1 GB, and internal memory is normally more than 1 GB. The QMobile Noir is of this type. In this type of device, data security applications make their file structures and store files in the internal memory. The internal memory can be mounted and then imaged using FTK Imager and can be processed in FTK Tool Kit for Encase etc.
4. Smartphone with a large size Internal Memory with no microSD Card Slot. The Google Nexus 5 is of this type. In this type of device, data security applications make their file structures and store files in the internal memory. The internal memory can be mounted as a mass storage devices and then imaged using FTK Imager and can be processed in FTK or Encase etc. If the device's memory is Media Transfer Protocol (MTP) based, then imaging is not possible. MTP devices have to be manually analysed, and it is comparatively difficult to analyse MTP devices as compared to Mass Storage devices because of protocol limitations.
5. Smartphone with a large size internal memory and a microSD card as external storage. The Samsung Galaxy S5 is of this type. In this type of device, relevant data is stored in the internal memory.

File storage mechanism differs with mobile phone type. Therefore, before analysis, the forensic examiner has to verify the type of smartphone storage. FTK Imager can be used to view or to make a forensic image of the internal memory or memory card of the smart phones. Imaging tools like 'dd', 'nandroid', or commercial tools can also be used for imaging [6]. On analyzing the image of internal memory or memory card with FTK Tool Kit or any other computer forensics tool, a huge amount of information can be extracted which is not found when just analyzing the mobile phone with normal mobile forensic tools like Cellebrite UFED or XRY forensics. This is because mobile forensic tools can only read resident data or in cases deleted files if the mobile is properly supported. They cannot perform automated file carving, which can be done by any computer forensics tool. In addition, manual file carving can only be done using computer forensics tools as we have seen in the case of '.slm' files created by the safe gallery application.

## 4. Discussion and Conclusion

To the best of the author's knowledge, this is the first research paper describing techniques to extract data from smartphones secured by android data security applications. We have seen that standard mobile forensic tools failed to extract files secured using data security applications. This is because these tools are unable to interpret the format of secured files. Even if the phone is fully supported, extraction was only successful from only a few data security applications. But in most cases, the files which were not password protected could be extracted.

The techniques proposed in this paper were successful in retrieving the data from smartphones that was secured by android based data security applications. This study suggests that instead of just analyzing the smartphone's data using standard forensics tools and relying upon the results obtained in this way, it is always important to perform manual forensic analysis. It is undeniable that standard smartphone forensic tools extract a gigantic amount of data in an automated way, but sometimes few hidden and well-encrypted files may not work well with conventional or automated forensic tools and, therefore, are difficult to retrieve. Under these circumstances, use of manual forensic tools may offer better chances of their retrieval.

We have seen that performing manual forensic analysis of file system of internal memory or memory card gave remarkable results. A forensic analyst should know what type of file system structures are created by data hiding applications so that when a forensic tool does not identify such files, the analyst could manually extract them. It is, therefore, essential to manually examine all files in the file system rather than just relying on a standard mobile forensic tool extraction report.

Wherever possible, it is recommended to make a forensic image of internal memory of a smartphone and to perform analysis using computer forensics and data carving tools for file carving as mobile forensic tools are not capable of doing that. It is expected that this paper will inspire mobile forensics manufacturers and researchers to develop automated tools for the extraction of data from data security applications.

## References

1. Sara R. Mobile Statistics Report, 2014-2018, The Radicati Group, Usa. http://www.radicati.com/wp/wp-content/uploads/2014/01/ Mobile-Statistics-Report-2014-2018-Executive-Summary.pdf. Accessed on 10.10.2015
2. eMarketer Inc. 2 billion consumers worldwide to get smartphones by 2016. http://www.emarketer.com/Article/2-Billion-Consumers-Worldwide-Smartphones-by-2016/1011694. Accessed on 10.10.2015
3. Lessard J, Kessler GC. Android Forensics: Simplifying Cell Phone Examinations. Small Scale Digital Device Forensics J 2010; 4: 1-12
4. Al Mutawa N, Baggili I, Marrington A. Forensic analysis of social networking applications on mobile devices. Digital Investigation 2012;9: s24-s33.
5. Al Zarouni M. Mobile Handset Forensic Evidence: a challenge for Law Enforcement. Proceedings of the 4th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia, December 4th 2006.
6. Distefano A, Gianluigi Me, Francesco P. Android anti-forensics through a local paradigm. Digital Investigation 2010; 7: s83-s94.