**Mobile Device Forensics Analysis Report**

**Conducted by Brendan Murphy**

**March 17 2019**

Contents

[1. Executive Summary 2](#_Toc460775153)

[2. Test Parameters 2](#_Toc460775154)

[3. Targets 2](#_Toc460775155)

[4. Analysis 3](#_Toc460775156)

[5. Appendix – Documentation 3](#_Toc460775157)

# Executive Summary

The purpose of this document is to conduct a Forensics Logical Acquisition of an Android Device.

# Test Parameters

The Objective of this evaluation is to conduct Forensics Analysis on an Android Device. The Scope of this evaluation is an **5554:lab. 5554:lab** is an Android Emulator of an Android Device. This Forensic Analysis exercise conducted a data extraction of the following mobile device filesystem directories:

* anr
* app
* backup
* dalvik-cache
* data
* misc
* nativebenchmark
* nativetest
* property
* system

Additionally, this Forensic Analysis exercise conducted a data extraction of the following mobile device settings:

* CallLog Calls
* Contact Phones
* MMS
* MMSParts
* SMS

This Analysis includes Logical Acquisition Forensic Analysis techniques using manual analysis techniques and an automated analysis tool. Forensic Analysis manual techniques include the use of the ***adb shell***. Forensic Analysis tools include: ***AFLogical OSE***.

# Targets

The Scope of the evaluation is as follows:

**Logical Acquisition**

* 1. Android Emulator - 5554:lab

# Analysis

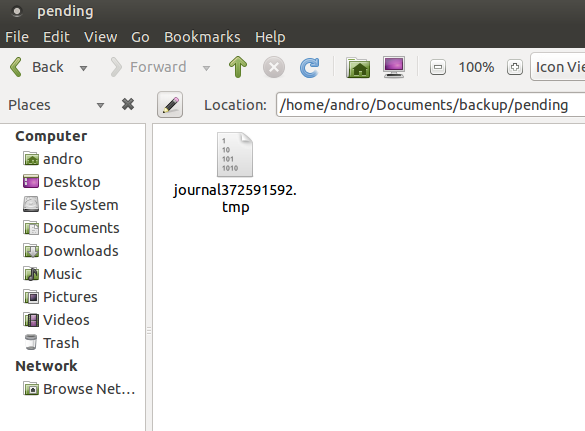
Table 1: 5554:lab – Android Mobile Device Filesystem Analysis

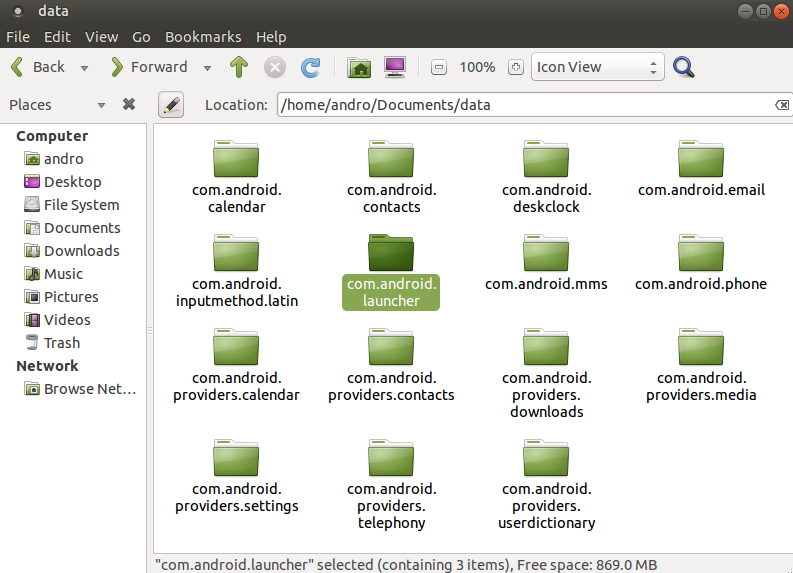
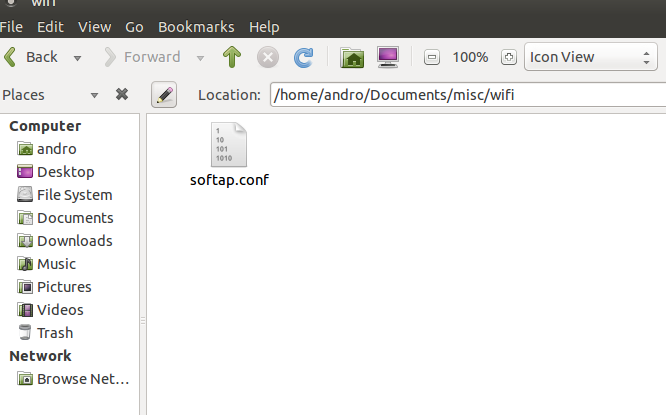
|  |  |  |  |
| --- | --- | --- | --- |
| **FILE SYSTEM DIRECTORY** | **DESCRIPTION** | **RISK ANALYSIS** | **DOCUMENTATION** |
| **anr** | **Provide a summary of what files are stored in this directory and what their function is.** | **If this directory stores files which pose a risk to confidentiality, note such here.** | **Appendix A** |
| **app** | **Unable to locate** |  | **Appendix A** |
| **Backup** | **Journal372591592.tmp** | **These file pose a confidentiality risk** | **Appendix A** |
| **dalvik-cache** | **Unable to locate** |  | **Appendix A** |
| **data** | **Contains many files and folders related to the phone ie contacts and call history** | **These file pose a confidentiality risk** | **Appendix A** |
| **misc** | **Softap.conf** |  | **Appendix A** |
| **nativebenchmark** | **Unable to locate** |  | **Appendix A** |
| **nativetest** | **Unable to locate** |  | **Appendix A** |
| **property** | **Contains documents related to timezone settings** | **These file pose a confidentiality risk** | **Appendix A** |
| **system** | **Contains documents related to system settings** | **These file pose a confidentiality risk** | **Appendix A** |

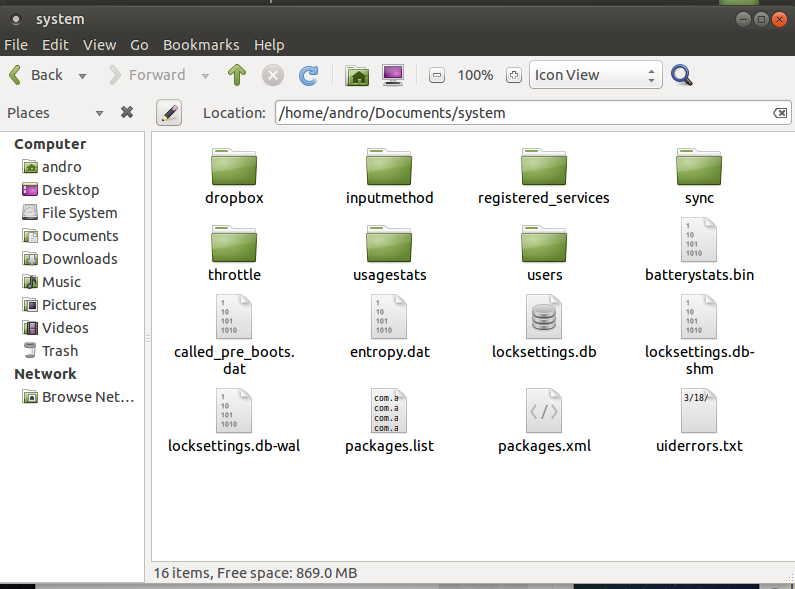
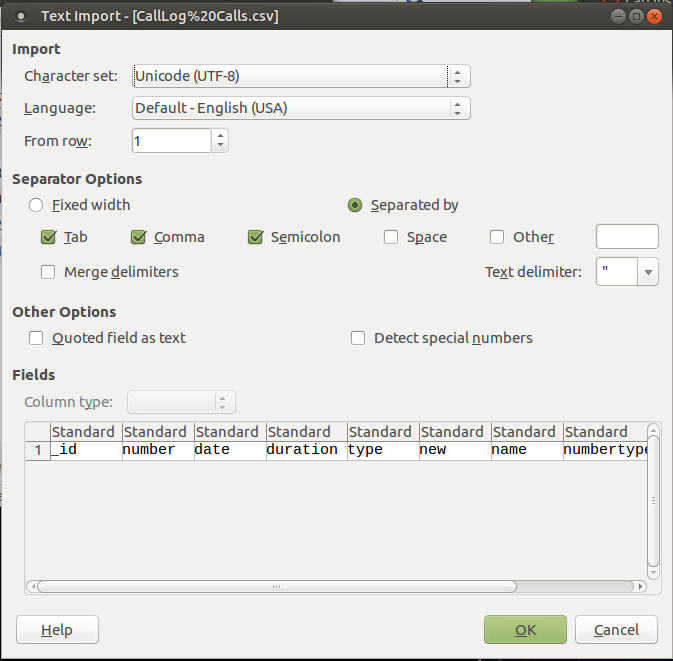
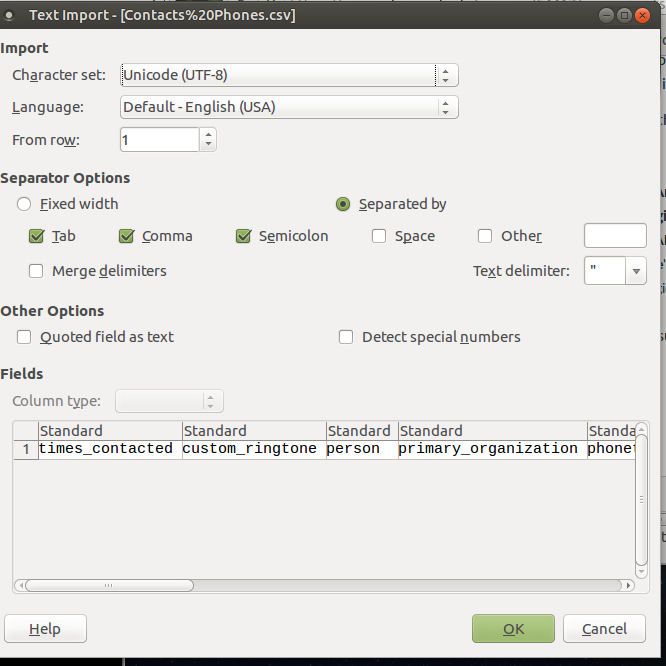
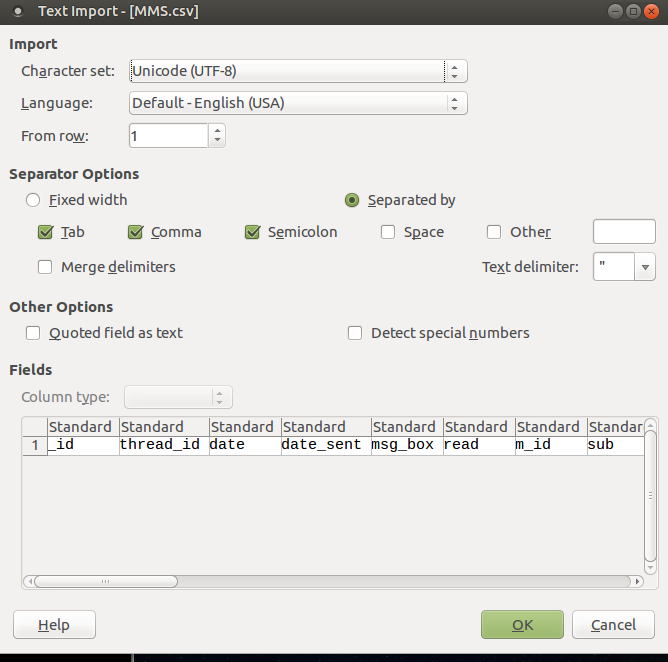
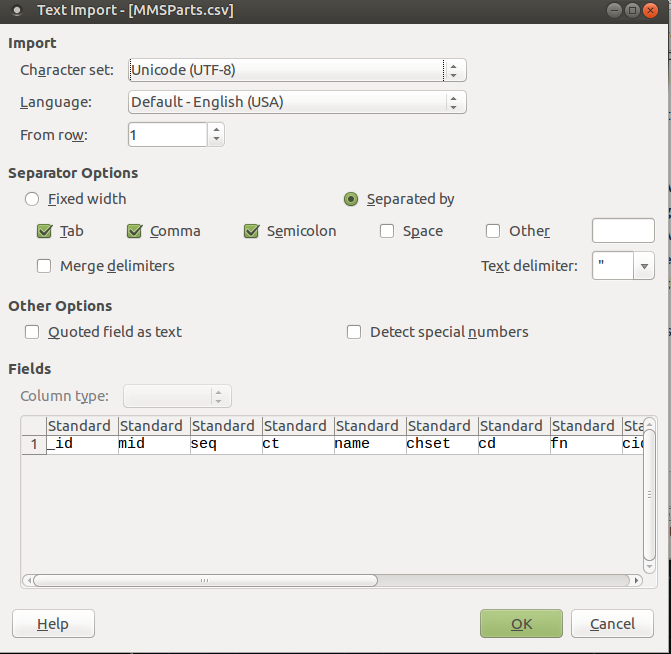
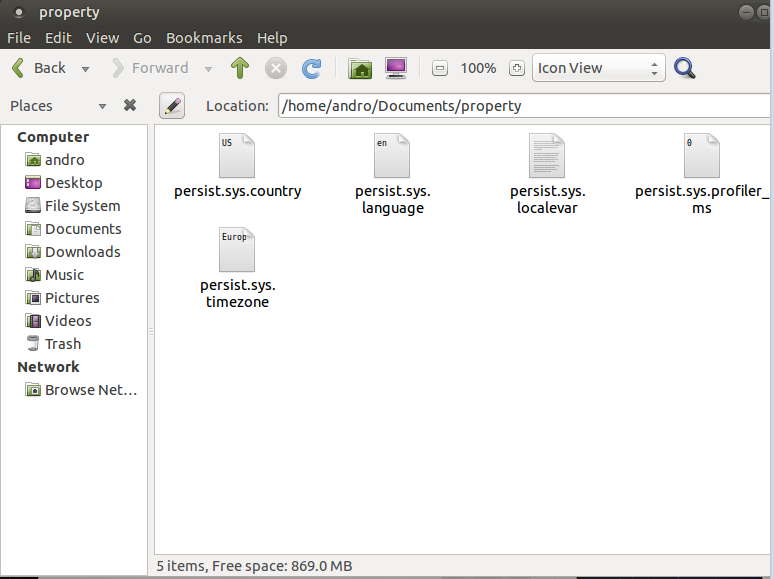
Table 2: 5554:lab – Android Mobile Device Data Analysis

|  |  |  |  |
| --- | --- | --- | --- |
| **DATA EXTRACTION** | **DESCRIPTION** | **RISK ANALYSIS** | **DOCUMENTATION** |
| **CallLog Calls** | **The call logs reveal no recent calls** | **The CallLog Calls could be used by an adversary to steal contact information** | **Appendix B** |
| **Contacts Phones** | **The contact phones reveal no recent calls** | **The contact phones could be used by an adversary to steal contact information or impersonate the user** | **Appendix B** |
| **MMS** | **The mms reveals no recent text messages** | **The mms text history could be used by an adversary to steal passwords or other personal information** | **Appendix B** |
| **MMSParts** | **The mmsParts reveals no recent text messages** | **The mmsparts text history could be used by an adversary to steal passwords or other personal information** | **Appendix B** |
| **SMS** | **The sms reveals no recent text messages** | **The sms text history could be used by an adversary to steal passwords or other personal information** | **Appendix B** |

# Appendix – Documentation

****

****

**     **