# AMNESTY INTERNATIONAL

## Digital Forensic Analysis Services Report

## Codename: [PHOOEY 2]

2017-08-22


**Presented To:**

Chris Cole

Information Security and Networks Officer

Amnesty International

1 Easton Street

WC1X 0DW

chris.cole@amnesty.org

0203 036 5055

**Submitted By:**

Andrew Nind

Incident Response Consultant

SecureWorks

United Kingdom House

180 Oxford Street

London W1D 1NN

United States & Canada: +1 877-884-1110

United Kingdom: +44 (0) 808-234-1203

Other international locations: +1 770-870-6343

anind@secureworks.com

+44 7834 806 621

## Report Disclaimer

Customer shall own all right, title, and interest in and to any written summaries, reports, analyses, and findings or other information or documentation prepared for Customer in connection with SecureWorks' provision of the Consulting Services to Customer (the "Customer Reports"). The provision by Customer of any Customer Report or any information therein to any unaffiliated third party shall not entitle such third party to rely on the Customer Report or the contents thereof in any manner or for any purpose whatsoever, and SecureWorks specifically disclaims all liability for any damages whatsoever (whether foreseen or unforeseen, direct, indirect, consequential, incidental, special, exemplary or punitive) arising from or related to reliance by any third party on any Customer Report or any contents thereof.

This document has been prepared solely for the use of the Customer and its officers, directors, and employees. No other third party shall be entitled to rely upon this document. The provision of this document or information herein to the parties other than the Customer shall not entitle such parties to rely on this report or the contents thereof in any manner or for any purpose whatsoever, and SecureWorks Inc. specifically disclaims all liability for any damages whatsoever (whether foreseen or unforeseen, direct, indirect, consequential, incidental, special, exemplary, or punitive) arising from or related to provision of such report or information to such parties.

Our opinions are based on controls and data we evaluated as of this report date. Any projection of such information to the future is subject to the risk that, because of changes within the environment, our evaluation may be based on controls and a system no longer in existence. The potential effectiveness of specific controls is subject to inherent limitations and, accordingly, errors or fraud may occur and not have been detected. Furthermore, the projection of any conclusions to future events, based on our findings, is subject to the risk that changes made to the system or controls, or the failure to make needed changes to the system or controls, may alter the validity of our conclusions.

# Table of Contents

**1. Executive Summary ..... 1**
1.1 Background ..... 1
1.2 Objectives ..... 1
1.3 Findings ..... 1

**2. Analysis Details ..... 2**
2.1 Technical Findings for Samsung Galaxy Note II ..... 2
2.1.1 Acquisition Details ..... 4
2.1.2 Binary Image ..... 5
2.1.3 Evidence of Installed Applications ..... 5
2.1.4 Testing ..... 6
2.1.5 USERDATA (ExtX)/Root/data/Application Folders ..... 6
2.1.6 USERDATA (ExtX)/Root/dalvik-cache/*.dex files ..... 7
2.1.7 Database File examination ..... 7
2.1.8 "Packages" Files ..... 7
2.1.9 Usage Files ..... 8
2.1.10 Batterystats.bin ..... 9

**Appendix A: Points of Contact ..... 11**
A.1 Client Contacts ..... 11
A.2 SecureWorks Contacts ..... 11

**Appendix B: Report Control Activity ..... 12**
B.1 Report Revision and Review History ..... 12
B.2 Report Distribution History ..... 12

# 1. Executive Summary

## 1.1 Background

On July 10, 2017, Amnesty International requested that SecureWorks conduct forensic analysis of a Samsung Galaxy Note II. Amnesty International wished to know if an application by the name of "Bylock" had been installed on the device.

On August 3, 2017 SecureWorks acquired an image of the device at Amnesty International's premises on Easton Street, London, UK.

Contemporaneous notes, made at the time of acquisition, and analysis notes pertaining to this report are maintained and kept by SecureWorks and can be produced upon request by a relevant authority.

## 1.2 Objectives

Amnesty International and SecureWorks personnel established the following engagement objectives:

1) Determine whether the application named "bylock" was or had ever been installed on the device.

## 1.3 Findings

As a result of analysis conducted on the image of the device, SecureWorks concludes that there is no evidence that the bylock application was ever installed on the device.

It should be noted that SecureWorks can only comment on the data that was available at the time of acquisition and using the extraction methods available at the time of analysis.

Details on the process used to come to this conclusion can be found in section 2.

# 2. Analysis Details

## 2.1 Technical Findings for Samsung Galaxy Note II

This section contains the technical findings of the investigation related to the Samsung Galaxy Note II.

| IMEI | Attributes | |
|---|---|---|
| 353627055929742 | Model: | GT-N7100 Galaxy Note II |
| | Vendor: | Samsung GSM |
| | Version: | 6.2.1.17 |
| | Internal Build: | 4.6.1.17 |


**Figure 1 – Front view of the device**


**Figure 2 – Internal back view with battery removed**


**Figure 3 – Manufacturer label in battery compartment**

### 2.1.1 Acquisition Details

Cellebrite's UFED4PC software was used to carry out an acquisition of the device only. No SIM card or External storage was provided. The following details describe the method used.

UED4PC Version 6.3.5.2

Extraction Type: Physical – Android ADB

Connection Type: Cable No. 100

Extraction started: 2017-08-03 09:07:35 UTC

Extraction completed: 2017-08-03 09:44:15 UTC

### 2.1.2 Binary Image

The UFED4PC produced a binary image file with the following attributes:

| Image File Name | Attributes |
|---|---|
| blk0_mmcblk0.bin | Size (in bytes): 15758000128<br>MD5: 00c9c0b8b03c42e2d6f2996c4fc02a92<br>SHA1: c519c9ee28d613e029904974cfe61bd0bd9276e2 |

This binary image file was analysed as detailed in the following sections.

### 2.1.3 Evidence of Installed Applications

There are several files and locations within the internal storage of an Android device that can provide evidence that an application was installed or used. During the examination of the aforementioned device, the following locations were examined for such evidence.

- USERDATA (ExtX)/Root/data/Application Folders
- USERDATA (ExtX)/Root/dalvik-cache/*.dex files
- USERDATA (ExtX)/Root/system/packages.xml
- USERDATA (ExtX)/Root/system/packages.list
- USERDATA (ExtX)/Root/system/netpolicy.xml
- USERDATA (ExtX)/Root/system/usagestats/usage-20170704
- USERDATA (ExtX)/Root/system/usagestats/usage-20170705
- USERDATA (ExtX)/Root/system/usagestats/usage-20170709
- USERDATA (ExtX)/Root/system/usagestats/usage-20170802
- USERDATA (ExtX)/Root/system/usagestats/usage-20170803
- USERDATA (ExtX)/Root/system/usagestats/usage-history.xml
- USERDATA (ExtX)/Root/system/usagestats/usage-20170802.bak (deleted)
- USERDATA (ExtX)/Root/system/usagestats/usage-history.xml.bak (deleted)
- USERDATA (ExtX)/Root/system/batterystats.bin
- USERDATA (ExtX)/Root/data/com.sec.android.app.launcher/databases/launcher.db
- USERDATA (ExtX)/Root/data/com.android.providers.downloads/databases/downloads.db
- USERDATA (ExtX)/Root/system/dmappmgr.db

The following sections present our findings for each of the above locations.

### 2.1.4 Testing

To confirm that relevant artefacts would be found in the above locations, had the bylock application ever been installed on such a device, a copy of the bylock application was obtained and installed on a similar device. This is henceforth referred to as the "test device".

Both devices were examined using the same tools and techniques for evidence of application artefacts.

### 2.1.5 USERDATA (ExtX)/Root/data/Application Folders

This directory is typically where application data is stored on an Android device. For each application installed a directory is created here, named with the application name.

On the test device, as a result of the installation, a folder was created here with the name "net.client.by.lock", as seen in Figure 4

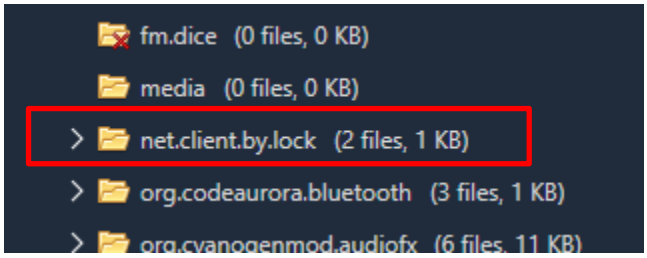


**Figure 4- bylock folder shown on test device**

No such directory was identified on the subject device.

To verify this finding, we examined the binary image produced via UFED4PC using a standard digital forensics tool called "X-Ways Forensics". The details of this tool are:

Software Name: X-Ways Forensics

Software Vendor: X-Ways Software Technology AG

Software Version: 19.0

Manual inspection using this tool revealed no indication of a folder named "net.client.by.lock" on the subject device.

### 2.1.6 USERDATA (ExtX)/Root/dalvik-cache/*.dex files

The Dalvik cache is an area within an Android device that contains .dex files which are compiled Android application code files. Traces of applications can be found in the .dex files. If an application was installed and then deleted, traces may reside in this location.

On the test device, a file existed here called "USERDATA (ExtX)/Root/dalvik-cache/profiles/net.client.by.lock" as seen in Figure 5

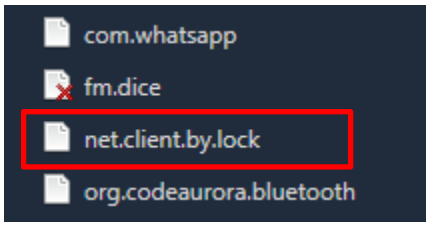


**Figure 5 - bylock file in Dalvik cache of test device**

The Dalvik cache within the subject device was reviewed and no such file was found.

This finding was verified via the X-ways Forensics tool.

### 2.1.7 Database File examination

The following SQLite databases were examined for evidence of application usage associated with the bylock app. Each database was manually extracted from the image, and examined with an SQLite Database viewer called "DB Browser for SQLite".

#### *2.1.7.1 Launcher.db*

Entries related to application usage were identified in a table named "App Order".

No reference to the application name "net.client.by.lock" was identified.

#### *2.1.7.2 Downloads.db*

Entries related to application usage were identified in a table named "downloads".

No reference to "net.client.by.lock" was identified.

#### *2.1.7.3 Dmappmgr.db*

Entries related to application usage were identified in a table named "ApplicationControl"

No reference to "net.client.by.lock" was identified.

### 2.1.8 "Packages" Files

Both the Packages.list and Packages.xml files contain details about applications installed. These files were extracted from the binary image and manually examined for any information related to the bylock application.

No such data was found.

### 2.1.9 Usage Files

Usage files contain statistics about the usage of applications on an Android device, such as the amount of time that the application was active.

These files were extracted from both devices and manually examined for usage statistics related to the bylock application.

Conducting a search across the usage files from the test device produced positive results as seen in Figures 6 and 7

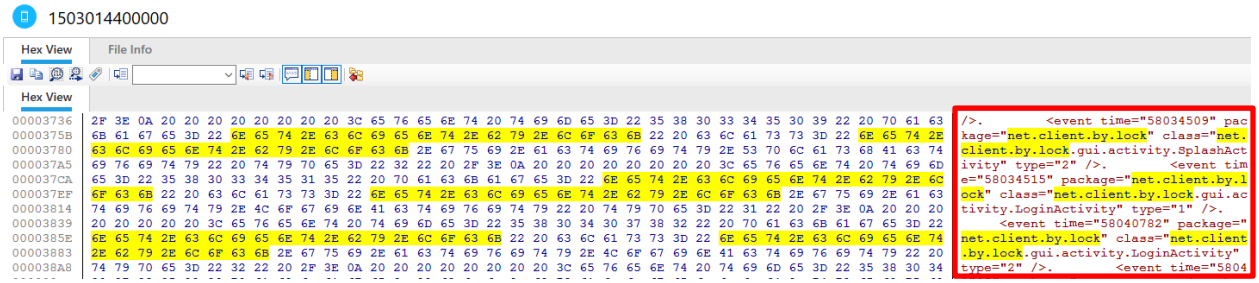


**Figure 6 - Positive results in usage stats files from test device**


**Figure 7 - Close view of results from usage stats file from test device**

No such statistics were found on the subject device.

### 2.1.10 Batterystats.bin

The Batterystats.bin file maintains statistics on battery consumed by individual applications.

Examining this file on the test device produced positive results as seen in Figures 8 and 9:

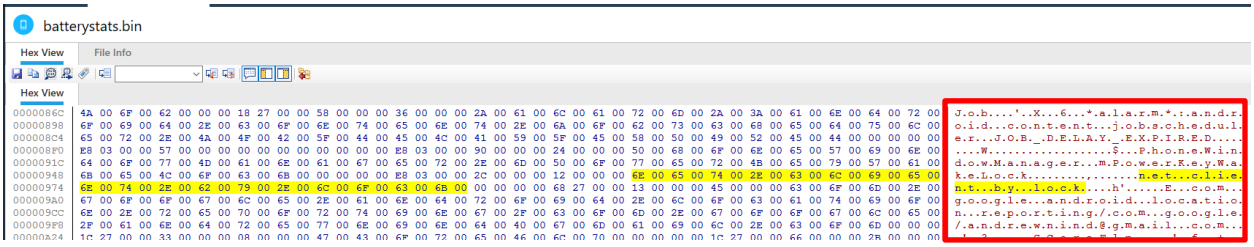


**Figure 8 - Positive results in batterystats.bin from test device**

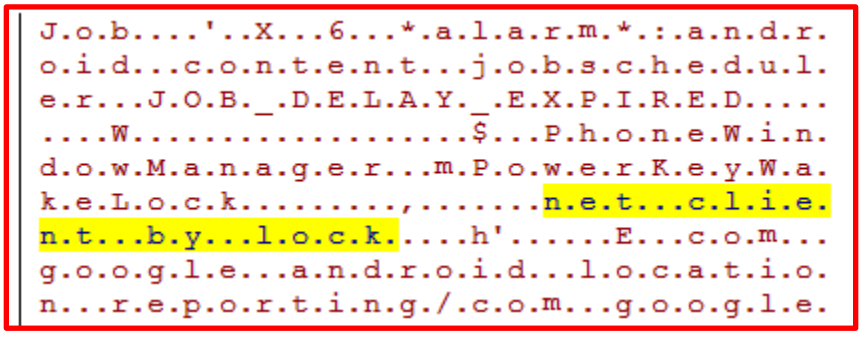


**Figure 9 - close view of results in batterystats.bin from test device**

No statistics relating to the bylock app were found on the subject device.

### 2.1.11 Deletion of the application on the test device

The application was uninstalled from the test device and re-examined for artefacts.

Whilst the application folder was deleted after uninstallation, both Cellebrite and X-ways still present the folder marking it as deleted.

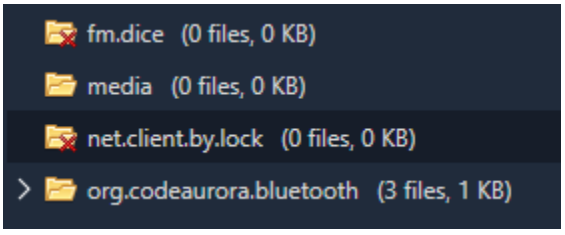


**Figure 10 - application folder showing as deleted by cellebrite**

Similarly, review of the Dalvik cache, shows that the file is still presented by Cellebrite and X-ways marking it as deleted.

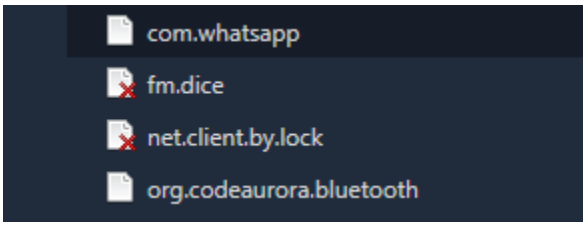


**Figure 11 - dalvik cache file showing as deleted by Cellebrite**

After uninstalling the bylock application from the test device, a keyword search for the term "net.client.by.lock" returned 550 results. Conducting the same keyword search on the subject device returns no results. A partial view of these results can be seen in Figures 12 and 13.

Search [550 results]

Find: net.client.by.lock

| # | Offset | Length | Value | Source |
|---|---|---|---|---|
| 14 | 0x12178126C | 0x24 | net.client.by.lock | /Root/system/batterystats-checkin.bin |
| 15 | 0x12178209C | 0x24 | net.client.by.lock | /Root/system/batterystats-checkin.bin |
| 16 | 0x1217B18EC | 0x24 | net.client.by.lock | /Root/system/batterystats-checkin.bin |
| 17 | 0x1217B1944 | 0x24 | net.client.by.lock | /Root/system/batterystats-checkin.bin |
| 18 | 0x1217B1978 | 0x24 | net.client.by.lock | /Root/system/batterystats-checkin.bin |
| 19 | 0x12388C2BE | 0x12 | net.client.by.lock | |
| 20 | 0x12388C2E6 | 0x12 | net.client.by.lock | |
| 21 | 0x12388C319 | 0x12 | net.client.by.lock | |
| 22 | 0x12394229C | 0x24 | net.client.by.lock | /Root/system/procstats/state-2017-08-20-03-49-34.bin |
| 23 | 0x12394B740 | 0x24 | net.client.by.lock | /Root/system/procstats/state-2017-08-20-03-49-34.bin |
| 24 | 0x125F4E86C | 0x12 | net.client.by.lock | |

**Figure 12 - keyword search results for test device**

Search [0 results]

Find: net.client.by.lock

| # | Offset | Length | Value | Source |
|---|---|---|---|---|

**Figure 13 - keyword search results for subject device**

# Appendix A: Points of Contact

## A.1 Client Contacts

| Client Contacts | |
|---|---|
| Company Name | Amnesty International |
| Company Address | 1 Easton Street<br>WC1X 0DW<br>London |
| Company Contact Name | Chris Cole |
| Contact Title | Information Security and Networks Officer |
| Contact Telephone Number | 0203 036 5055 |
| Contact Email Address | chris.cole@amnesty.org |

## A.2 SecureWorks Contacts

| SecureWorks Contacts | |
|---|---|
| Primary Consultant Name | Andrew Nind |
| Primary Consultant Title | Incident Response Consultant |
| Primary Consultant Telephone Number | +44 7834 806 621 |
| Primary Consultant Email Address | anind@secureworks.com |

# Appendix B: Report Control Activity

## B.1 Report Revision and Review History

| Date | Version | Description | Author |
|---|---|---|---|
| 2017-08-16 | 0.1 | Initial Draft | A Nind |
| 2017-08-18 | 0.2 | Draft Reviewed | J Thoburn |
| 2017-08-21 | 0.3 | Updated Draft | A Nind |
| 2017-08-21 | 0.4 | Draft Reviewed | A Papadopoulos |
| 2017-08-21 | 0.5 | Updated Draft | A Nind |
| 2017-08-22 | 1.0 | Interim Version Released | A Nind |
| YYYY-MM-DD | 1.1 | Interim Version Updated | |
| YYYY-MM-DD | 2.0 | Final Version Released | |

## B.2 Report Distribution History

| Date | Version | Description | Sender | Recipients |
|---|---|---|---|---|
| 2017-08-22 | 1.0 | Sent interim version via encrypted email | A Nind | Chris Cole,<br>Amnesty International |
| YYYY-MM-DD | 2.0 | Sent final version via encrypted email | SCWX-Team-Member | <POC-Name-1>, <POC-Organization-1><br><POC-Name-2>, <POC-Organization-2> |