

Πανεπιστήμιο Πειραιά

Σχολή Τεχνολογιών Πληροφορικής και Επικοινωνιών

Τμήμα Ψηφιακών Συστημάτων

Π.Μ.Σ. Ασφάλεια Ψηφιακών Συστημάτων

Καθηγητής: Ξενάκης Χρήστος

Διπλωματική Εργασία: "Ψηφιακή Εγκληματολογία σε Android 10" Master Thesis: 'Android 10 Forensics'

Χρυσανθακοπούλου Γερασιμίνα Α.Μ.: ΜΤΕ 1831

ΠΕΙΡΑΙΑΣ 2021

Στον εαυτό μου

ΕΥΧΑΡΙΣΤΙΕΣ

Οα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή μου κ. Ξενάκη για την εμπιστοσύνη που μου έδειξε, την βοήθειά του ώστε να μπορέσω να ολοκληρώσω την διπλωματική εργασία μου και για το ενδιαφέρον που μου ενέπνευσε για τον τομέα της ασφάλειας υπολογιστών.

Θα ήθελα να ευχαριστήσω τους γονείς μου και τους φίλους μου για την διαρκή υποστήριξη, την υπομονή, την ενθάρρυνση τους και την πίστη τους σε εμένα.

Περιεχόμενα

| ΕΥΡΕΤΗΡΙΟ ΕΙΚΟΝΩΝ | 5 |
|--|-----|
| ABSTRACT | 9 |
| ΕΙΣΑΓΩΓΗ | 10 |
| MOBILE FORENSICS – ΘΕΩΡΗΤΙΚΟ ΥΠΟΒΑΘΡΟ | 13 |
| 1. ΥΛΙΚΟ ΚΑΙ ΛΟΓΙΣΜΙΚΟ | 17 |
| 1.1 Γενικές Πληροφορίες Συσκευής | 17 |
| 1.2 Διαδικασία Απόκτησης Root Πρόσβασης στην Συσκευή | 19 |
| 1.3 Santoku | 41 |
| 2. ΠΑΡΑΚΑΜΨΗ ΜΗΧΑΝΙΣΜΩΝ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΚΛΕΙΔΩΜΑΤΟΣ ΟΘΟΝΗΣ | 42 |
| 2.1 Pattern | 42 |
| 2.2 Pin | 49 |
| 2.3 Password | 54 |
| 3. ANDROID 10 SECURITY AND PRIVACY FEATURES | 58 |
| 3.1 Android 10 Permissions & Scoped Storage | 58 |
| 3.2 Απενεργοποίηση Κρυπτογράφησης | 61 |
| 3.3 Απεγκατάσταση Knox | 63 |
| 4. LOGICAL ANALYSIS | 74 |
| 4.1 AFLOGICAL | 74 |
| 4.2 FONEPAW | 85 |
| 5. PHYSICAL IMAGE ACQUISITION | 94 |
| 6. PHYSICAL ANALYSIS | 100 |
| 6.1 AUTOPSY | 100 |
| 6.2 ANDRILLER | 110 |
| 7. ΣΥΜΠΕΡΑΣΜΑΤΑ-ΕΠΙΛΟΓΟΣ | 116 |
| ΧΡΗΣΙΜΑ LINKS | 118 |
| ΒΙΒΛΙΟΓΡΑΦΙΚΕΣ ΑΝΑΦΟΡΕΣ | 119 |

ΕΥΡΕΤΗΡΙΟ ΕΙΚΟΝΩΝ

| Εικόνα 1 - Κυρίαρχα Λειτουργικά Συστήματα (statcounter, 2019 - 2020) | 10 |
|--|----|
| Εικόνα 2 - Ενεργές Κινητές Συσκευές Παγκοσμίως (statista, 2020) | 10 |
| Εικόνα 3 - Samsung Market share (statcounter, 2019-2020) | 11 |
| Εικόνα 4 - Γενικές Πληροφορίες Συσκευής 1 | 17 |
| Εικόνα 5 - Γενικές Πληροφορίες Συσκευής 2 | 17 |
| Εικόνα 6 - Γενικές Πληροφορίες Συσκευής 3 | 18 |
| Εικόνα 7 - Developer Options | 19 |
| Εικόνα 8 - Developer Options Allow USB Debugging Question | 20 |
| Εικόνα 9 - USB Debugging Ενεργοποιημένο | 20 |
| Εικόνα 10 - OEM Unlocking Ενεργοποιημένο | 21 |
| Εικόνα 11 - Download Mode 1 | 22 |
| Εικόνα 12 - Download Mode 2 | 22 |
| Εικόνα 13 - Download Mode 3 | 23 |
| Εικόνα 14 - Unlock Bootloader | 24 |
| Εικόνα 15 - Bootloader Unlocked Message | 24 |
| Εικόνα 16 - Device Model Number | 25 |
| Εικόνα 17 - Firmware Files | 25 |
| Εικόνα 18 - Αντιγραφή ΑΡ Αρχείου στην Συσκευή | 26 |
| Εικόνα 19 - Magisk Manager Google | 26 |
| Εικόνα 20 - Download Magisk Manager | 27 |
| Εικόνα 21 - Magisk Manager Εγκατάσταση (Εντός App) | 28 |
| Εικόνα 22 - Magisk Manager NEXT | 29 |
| Εικόνα 23 - Magisk Manager Select & Patch a File | 30 |
| Εικόνα 24 - Magisk Manager Επιλογή ΑΡ Αρχείου | 31 |
| Εικόνα 25 - Magisk Manager Έναρξη Διαδικασίας Patch | 32 |
| Εικόνα 26 - Magisk Manager Πρόοδος Διαδικασίας | 33 |
| Εικόνα 27 - Download Mode Warning | 34 |
| Εικόνα 28 - Odin Added Message | 35 |
| Εικόνα 29 - Odin Auto Reboot Αποεπιλογή | 35 |
| Εικόνα 30 - Odin Επιλογή AP magisk_patched.tar | 36 |
| Εικόνα 31 - Odin Επιλογή Υπόλοιπων Αρχείων Firmware | 37 |
| Εικόνα 32 - Odin PASS! Message | 37 |
| Εικόνα 33 - Wipe Data / Factory Reset 1 | 38 |
| Εικόνα 34 - Wipe Data / Factory Reset 2 | 39 |
| Εικόνα 35 - Root Checker App 1 | 40 |
| Εικόνα 36 - Root Checker App 2 | 40 |
| Εικόνα 37 - Santoku VM Settings | 41 |
| Εικόνα 38 - Pattern Lock Screen | 42 |
| Εικόνα 39 - Pattern Removal - adb devices | 43 |
| Εικόνα 40 – Pattern Removal - cd data | 43 |
| Εικόνα 41 – Pattern Removal - Data Directory Is | 44 |
| Εικόνα 42 – Pattern Removal - Directory /data/system ls 1 | 45 |
| | |

| Εικόνα 43 - Pattern Removal - Directory /data/system ls 2 | . 46 |
|--|------|
| Εικόνα 44 - Pattern Removal - Directory /data/system Delete Files | . 46 |
| Εικόνα 45 - Pattern Removal - Reboot Device | . 47 |
| Εικόνα 46 - Pattern Removed Lock Screen 1 | . 47 |
| Εικόνα 47 - Pattern Removed Lock Screen 2 | . 48 |
| Εικόνα 48 - Pin Lock Screen | . 49 |
| Εικόνα 49 - Pin Removal - adb devices | . 49 |
| Εικόνα 50 - Pin Removal - su shell | . 50 |
| Εικόνα 51 - Pin Removal - Directory /data/system Is 1 | . 50 |
| Εικόνα 52 - Pin Removal - Directory /data/system Is 2 | . 51 |
| Εικόνα 53 - Pin Removal - Directory /data/system Delete Files | . 51 |
| Εικόνα 54 - Pin Removal - Reboot Device | . 52 |
| Εικόνα 55 - Pin Removed Lock Screen 1 | . 52 |
| Εικόνα 56 - Pin Removed Lock Screen 2 | . 53 |
| Εικόνα 57 - Password Lock Screen | . 54 |
| Εικόνα 58 - Password Removal - adb devices & su shell | . 54 |
| Εικόνα 59 - Password Removal - cd /data/system | . 55 |
| Εικόνα 60 - Password Removal - Directory /data/system ls 1 | . 55 |
| Εικόνα 61 - Password Removal - Directory /data/system Is 2 | . 56 |
| Εικόνα 62 - Password Removal - Directory /data/system Delete Files | . 56 |
| Εικόνα 63 - Password Removal - Reboot Device | . 56 |
| Εικόνα 64 - Password Removed Lock Screen 1 | . 57 |
| Εικόνα 65 - Password Removed Lock Screen 2 | . 57 |
| Εικόνα 66 - Device App List | . 59 |
| Εικόνα 67 - Permission Manager | . 60 |
| Εικόνα 68 - Call Logs Permissions | . 60 |
| Εικόνα 69 - Disable Encryption | . 61 |
| Εικόνα 70 - Encryption Disabled | . 62 |
| Εικόνα 71 - Knox Apps | . 64 |
| Εικόνα 72 - Terminal Emulator App | . 65 |
| Εικόνα 73 - Magisk Modules - Debloater | . 66 |
| Εικόνα 74 - Terminal Emulator App - su shell | . 67 |
| Εικόνα 75 - Terminal Emulator App - debloat | . 68 |
| Εικόνα 76 - Debloater Module Menu | . 68 |
| Εικόνα 77 - Uninstalling Knox Apps 1 | . 69 |
| Εικόνα 78 - Uninstalling Knox Apps 2 | . 70 |
| Εικόνα 79 - Uninstalling Knox Apps 3 | . 70 |
| Εικόνα 80 - Uninstalling Knox Apps 4 | . 71 |
| Εικόνα 81 - Uninstalling Knox Apps 5 | . 72 |
| Εικόνα 82 - Uninstalling Knox Apps 6 | . 72 |
| Εικόνα 83 - Knox No Results Found | . 73 |
| Εικόνα 84 - aflogical-ose terminal | . 74 |
| Εικόνα 85 - AFLogical OSE App | . 75 |
| Εικόνα 86 - AFLogical OSE App Message | . 75 |
| Εικόνα 87 - AFLogical OSE App Menu | . 76 |

| Εικόνα 88 - Collected Files | . 76 |
|--|--|
| Εικόνα 89 - Call Logs File | . 77 |
| Εικόνα 90 - SMS File 1 | . 77 |
| Εικόνα 91 - SMS File 2 | . 78 |
| Εικόνα 92 - SMS File 3 - IMSI | . 78 |
| Εικόνα 93 - Contacts File Empty | . 79 |
| Εικόνα 94 - Manage Contacts Menu | . 79 |
| Εικόνα 95 - Import or Export Contacts | . 80 |
| Εικόνα 96 - Internal Storage Export 1/2 | . 80 |
| Εικόνα 97 - Internal Storage Export 2/2 | . 81 |
| Εικόνα 98 - Contacts Exported | . 81 |
| Εικόνα 99 - Internal Storage File Selection | . 82 |
| Εικόνα 100 - Move File to Forensics Folder | . 82 |
| Εικόνα 101 - Forensics Folder Internal Storage | . 83 |
| Εικόνα 102 - Collected Files with Contacts File | . 83 |
| Εικόνα 103 - Exported Contacts File | . 84 |
| Εικόνα 104 - FonePaw - Android Data Recovery | . 85 |
| Εικόνα 105 - Allow USB Debugging Message | . 86 |
| Εικόνα 106 - Choose Files to Recover | . 87 |
| Εικόνα 107 - File Recovery Process | . 87 |
| Εικόνα 108 - FonePaw Collected Evidence 1 | . 88 |
| Εικόνα 109 - FonePaw Collected Evidence 2 | . 88 |
| | 29 |
| Elkovα 110 - FonePaw - Contacts 1 | . 05 |
| Εικόνα 110 - FonePaw - Contacts 1 Εικόνα 111 - FonePaw - Contacts 2 | . 89 |
| Εικόνα 110 - FonePaw - Contacts 1 Εικόνα 111 - FonePaw - Contacts 2 Εικόνα 112 - FonePaw - SMS 1 | . 89 . 90 |
| Εικόνα 110 - FonePaw - Contacts 1 Εικόνα 111 - FonePaw - Contacts 2 Εικόνα 112 - FonePaw - SMS 1 Εικόνα 113 - FonePaw - SMS 2 | . 89 . 89 . 90 . 90 |
| Εικόνα 110 - FonePaw - Contacts 1 Εικόνα 111 - FonePaw - Contacts 2 Εικόνα 112 - FonePaw - SMS 1 Εικόνα 113 - FonePaw - SMS 2 Εικόνα 114 - FonePaw - SMS 3 | . 89 . 90 . 90 . 90 |
| Εικόνα 110 - FonePaw - Contacts 1 Εικόνα 111 - FonePaw - Contacts 2 Εικόνα 112 - FonePaw - SMS 1 Εικόνα 113 - FonePaw - SMS 2 Εικόνα 114 - FonePaw - SMS 3 Εικόνα 115 - FonePaw - Call Logs | . 89 . 90 . 90 . 90 . 90 . 91 |
| Εικόνα 110 - FonePaw - Contacts 1 Εικόνα 111 - FonePaw - Contacts 2 Εικόνα 112 - FonePaw - SMS 1 Εικόνα 113 - FonePaw - SMS 2 Εικόνα 114 - FonePaw - SMS 3 Εικόνα 115 - FonePaw - Call Logs Εικόνα 116 - FonePaw - Pictures 1 | . 89 . 90 . 90 . 90 . 91 . 91 |
| Εικόνα 110 - FonePaw - Contacts 1 Εικόνα 111 - FonePaw - Contacts 2 Εικόνα 112 - FonePaw - SMS 1 Εικόνα 113 - FonePaw - SMS 2 Εικόνα 114 - FonePaw - SMS 3 Εικόνα 115 - FonePaw - Call Logs Εικόνα 116 - FonePaw - Pictures 1 Εικόνα 117 - FonePaw - Pictures 2 | . 89 . 90 . 90 . 90 . 91 . 91 . 91 |
| Eικόνα 110 - FonePaw - Contacts 1 Εικόνα 111 - FonePaw - Contacts 2 Εικόνα 112 - FonePaw - SMS 1 Εικόνα 113 - FonePaw - SMS 2 Εικόνα 114 - FonePaw - SMS 3 Εικόνα 115 - FonePaw - Call Logs Εικόνα 116 - FonePaw - Pictures 1 Εικόνα 117 - FonePaw - Pictures 2 Εικόνα 118 - FonePaw - Pictures 3 | . 89 . 90 . 90 . 90 . 91 . 91 . 91 . 92 |
| Eικόνα 110 - FonePaw - Contacts 1 Εικόνα 111 - FonePaw - Contacts 2 Εικόνα 112 - FonePaw - SMS 1 Εικόνα 113 - FonePaw - SMS 2 Εικόνα 114 - FonePaw - SMS 3 Εικόνα 115 - FonePaw - Call Logs Εικόνα 116 - FonePaw - Pictures 1 Εικόνα 117 - FonePaw - Pictures 2 Εικόνα 118 - FonePaw - Pictures 3 Εικόνα 119 - Gallery Trash. | . 89 . 90 . 90 . 90 . 91 . 91 . 91 . 92 . 92 |
| Eικόνα 110 - FonePaw - Contacts 1 Eικόνα 111 - FonePaw - Contacts 2 Eικόνα 112 - FonePaw - SMS 1 Eικόνα 113 - FonePaw - SMS 2 Eικόνα 114 - FonePaw - SMS 3 Eικόνα 115 - FonePaw - Call Logs Eικόνα 116 - FonePaw - Pictures 1 Eικόνα 117 - FonePaw - Pictures 2 Eικόνα 118 - FonePaw - Pictures 3 Eικόνα 119 - Gallery Trash | . 89 . 90 . 90 . 90 . 91 . 91 . 91 . 92 . 92 . 93 |
| Eικόνα 110 - FonePaw - Contacts 1 Εικόνα 111 - FonePaw - Contacts 2 Εικόνα 112 - FonePaw - SMS 1 Εικόνα 113 - FonePaw - SMS 2 Εικόνα 114 - FonePaw - SMS 3 Εικόνα 115 - FonePaw - Call Logs Εικόνα 116 - FonePaw - Call Logs Εικόνα 117 - FonePaw - Pictures 1 Εικόνα 117 - FonePaw - Pictures 2 Εικόνα 118 - FonePaw - Pictures 3 Εικόνα 119 - Gallery Trash. Εικόνα 120 - FonePaw - Videos Εικόνα 121 - FonePaw - Documents. | . 89 . 90 . 90 . 90 . 91 . 91 . 91 . 91 . 92 . 92 . 93 . 93 |
| Eικόνα 110 - FonePaw - Contacts 1 Eικόνα 111 - FonePaw - Contacts 2 Eικόνα 112 - FonePaw - SMS 1 Eικόνα 113 - FonePaw - SMS 2 Eικόνα 114 - FonePaw - SMS 3 Eικόνα 115 - FonePaw - Call Logs Eικόνα 116 - FonePaw - Call Logs Eικόνα 117 - FonePaw - Pictures 1 Eικόνα 117 - FonePaw - Pictures 2 Eικόνα 118 - FonePaw - Pictures 3 Eικόνα 119 - Gallery Trash Eικόνα 120 - FonePaw - Videos Eικόνα 121 - FonePaw - Documents. Eικόνα 122 - BusyBox Welcome Message | . 89 . 90 . 90 . 91 . 91 . 91 . 91 . 92 . 93 . 93 . 94 |
| Etkövα 110 - FonePaw - Contacts 1 Etkövα 111 - FonePaw - Contacts 2 Etkóvα 112 - FonePaw - SMS 1 Etkóvα 113 - FonePaw - SMS 2 Etkóvα 114 - FonePaw - SMS 3 Etkóvα 115 - FonePaw - Call Logs Etkóvα 116 - FonePaw - Call Logs Etkóvα 116 - FonePaw - Pictures 1 Etkóvα 117 - FonePaw - Pictures 2 Etkóvα 118 - FonePaw - Pictures 3 Etkóvα 119 - Gallery Trash Etkóvα 120 - FonePaw - Videos Etkóvα 121 - FonePaw - Documents. Etkóvα 122 - BusyBox Welcome Message Etkóvα 123 - BusyBox App. | . 89 . 90 . 90 . 90 . 91 . 91 . 91 . 91 . 92 . 92 . 93 . 93 . 94 . 95 |
| Etkövα 110 - FönePaw - Contacts 1 Etkövα 111 - FönePaw - Contacts 2 Etkövα 112 - FönePaw - SMS 1 Etkövα 113 - FönePaw - SMS 2 Etkövα 114 - FönePaw - SMS 3 Etkövα 115 - FönePaw - Call Logs Etkövα 116 - FönePaw - Pictures 1 Etkövα 117 - FönePaw - Pictures 2 Etkövα 118 - FönePaw - Pictures 3 Etkövα 119 - Gallery Trash. Etkövα 120 - FönePaw - Videos . Etkövα 121 - FönePaw - Documents. Etkövα 122 - BusyBox Welcome Message. Etkövα 123 - BusyBox App. Etkövα 124 - BusyBox Installed. | . 89 . 90 . 90 . 91 . 91 . 91 . 91 . 92 . 93 . 93 . 94 . 95 . 95 |
| Elkovα 110 - FonePaw - Contacts 1 Elkóvα 111 - FonePaw - Contacts 2 Elkóvα 112 - FonePaw - SMS 1 Elkóvα 113 - FonePaw - SMS 2 Elkóvα 114 - FonePaw - SMS 3 Elkóvα 115 - FonePaw - Call Logs Elkóvα 116 - FonePaw - Pictures 1 Elkóvα 117 - FonePaw - Pictures 2 Elkóvα 118 - FonePaw - Pictures 3 Elkóvα 119 - Gallery Trash Elkóvα 120 - FonePaw - Videos Elkóvα 121 - FonePaw - Documents Elkóvα 122 - BusyBox Welcome Message Elkóvα 123 - BusyBox App Elkóvα 124 - BusyBox Installed Elkóvα 125 - Device Partitions 1 | . 89 . 90 . 90 . 91 . 91 . 91 . 91 . 92 . 93 . 93 . 93 . 95 . 95 . 96 |
| Etkövα 110 - FonePaw - Contacts 1 Etkövα 111 - FonePaw - Contacts 2 Etkóvα 112 - FonePaw - SMS 1 Etkóvα 113 - FonePaw - SMS 2 Etkóvα 114 - FonePaw - SMS 3 Etkóvα 115 - FonePaw - Call Logs Etkóvα 115 - FonePaw - Call Logs Etkóvα 116 - FonePaw - Pictures 1 Etkóvα 117 - FonePaw - Pictures 2 Etkóvα 117 - FonePaw - Pictures 3 Etkóvα 118 - FonePaw - Pictures 3 Etkóvα 119 - Gallery Trash Etkóvα 120 - FonePaw - Videos Etkóvα 121 - FonePaw - Documents Etkóvα 122 - BusyBox Welcome Message Etkóvα 123 - BusyBox App Etkóvα 124 - BusyBox Installed Etkóvα 125 - Device Partitions 1 Etkóvα 126 - Device Partitions 2. | . 89 . 90 . 90 . 91 . 91 . 91 . 91 . 92 . 93 . 93 . 93 . 94 . 95 . 95 . 96 |
| Etkovα 110 - FonePaw - Contacts 1 Etkóvα 111 - FonePaw - Contacts 2 Etkóvα 112 - FonePaw - SMS 1 Etkóvα 113 - FonePaw - SMS 2 Etkóvα 114 - FonePaw - SMS 3 Etkóvα 115 - FonePaw - Call Logs Etkóvα 115 - FonePaw - Pictures 1 Etkóvα 116 - FonePaw - Pictures 2 Etkóvα 117 - FonePaw - Pictures 3 Etkóvα 118 - FonePaw - Pictures 3 Etkóvα 119 - Gallery Trash. Etkóvα 120 - FonePaw - Videos Etkóvα 121 - FonePaw - Videos Etkóvα 122 - BusyBox Welcome Message Etkóvα 123 - BusyBox App. Etkóvα 124 - BusyBox Installed. Etkóvα 125 - Device Partitions 1. Etkóvα 127 - Device Partitions 3. | . 89 . 90 . 90 . 91 . 91 . 91 . 91 . 92 . 93 . 93 . 93 . 93 . 95 . 95 . 96 . 97 |
| ELKOVΩ 110 - FONEPaW - CONTACTS 1 ELKÓVΩ 111 - FONEPaW - CONTACTS 2 ELKÓVΩ 112 - FONEPaW - SMS 1 ELKÓVΩ 113 - FONEPaW - SMS 2 ELKÓVΩ 114 - FONEPaW - SMS 3 ELKÓVΩ 115 - FONEPaW - Call Logs ELKÓVΩ 116 - FONEPaW - Call Logs ELKÓVΩ 116 - FONEPaW - Pictures 1 ELKÓVΩ 117 - FONEPaW - Pictures 2 ELKÓVΩ 118 - FONEPaW - Pictures 3 ELKÓVΩ 118 - FONEPaW - Pictures 3 ELKÓVΩ 119 - Gallery Trash. ELKÓVΩ 120 - FONEPaW - Videos ELKÓVΩ 120 - FONEPaW - Videos ELKÓVΩ 121 - FONEPaW - Documents. ELKÓVΩ 122 - BusyBox Welcome Message. ELKÓVΩ 123 - BusyBox App. ELKÓVΩ 124 - BusyBox Installed. ELKÓVΩ 125 - Device Partitions 1. ELKÓVΩ 127 - Device Partitions 3. ELKÓVΩ 128 - adb forward. | . 89 . 90 . 90 . 91 . 91 . 91 . 91 . 92 . 93 . 93 . 93 . 93 . 95 . 95 . 96 . 96 . 97 . 98 |
| ELKOVΩ 110 - FONEPAW - CONTACTS 1 ELKÓVΩ 111 - FONEPAW - CONTACTS 2 ELKÓVΩ 112 - FONEPAW - SMS 1 ELKÓVΩ 113 - FONEPAW - SMS 2 ELKÓVΩ 114 - FONEPAW - SMS 3 ELKÓVΩ 115 - FONEPAW - Call Logs ELKÓVΩ 115 - FONEPAW - Call Logs ELKÓVΩ 116 - FONEPAW - PICTURES 1 ELKÓVΩ 117 - FONEPAW - PICTURES 2 ELKÓVΩ 118 - FONEPAW - PICTURES 3 ELKÓVΩ 118 - FONEPAW - PICTURES 3 ELKÓVΩ 119 - Gallery Trash ELKÓVΩ 120 - FONEPAW - VIdeos ELKÓVΩ 120 - FONEPAW - VIdeos ELKÓVΩ 121 - FONEPAW - Documents ELKÓVΩ 122 - BUSYBOX Welcome Message ELKÓVΩ 123 - BUSYBOX App ELKÓVΩ 124 - BUSYBOX Installed ELKÓVΩ 125 - Device Partitions 1 ELKÓVΩ 127 - Device Partitions 3 ELKÓVΩ 128 - adb forward ELKÓVΩ 129 - dd for sda partition | . 89 . 90 . 90 . 91 . 91 . 91 . 91 . 92 . 93 . 93 . 93 . 93 . 95 . 95 . 95 . 96 . 97 . 98 . 98 |
| ELKOVΩ 110 - FONEPAW - Contacts 1 ELKOVΩ 111 - FONEPAW - Contacts 2 ELKÓVΩ 112 - FONEPAW - SMS 1 ELKÓVΩ 113 - FONEPAW - SMS 2 ELKÓVΩ 114 - FONEPAW - SMS 3 ELKÓVΩ 115 - FONEPAW - Call Logs ELKÓVΩ 115 - FONEPAW - Call Logs ELKÓVΩ 116 - FONEPAW - Pictures 1 ELKÓVΩ 117 - FONEPAW - Pictures 2 ELKÓVΩ 117 - FONEPAW - Pictures 3 ELKÓVΩ 118 - FONEPAW - Pictures 3 ELKÓVΩ 119 - Gallery Trash ELKÓVΩ 120 - FONEPAW - Videos ELKÓVΩ 120 - FONEPAW - Videos ELKÓVΩ 121 - FONEPAW - Documents ELKÓVΩ 122 - BusyBox Welcome Message ELKÓVΩ 123 - BusyBox App ELKÓVΩ 124 - BusyBox Installed ELKÓVΩ 125 - Device Partitions 1 ELKÓVΩ 127 - Device Partitions 3 ELKÓVΩ 128 - adb forward ELKÓVΩ 129 - dd for sda partition ELKÓVΩ 130 - netcat. | . 89 . 90 . 90 . 91 . 91 . 91 . 91 . 92 . 93 . 93 . 93 . 93 . 93 . 95 . 95 . 96 . 96 . 97 . 98 . 98 . 99 |
| ELKOVA 110 - FONEPAW - Contacts 1 ELKÓVA 111 - FONEPAW - Contacts 2 ELKÓVA 112 - FONEPAW - SMS 1 ELKÓVA 113 - FONEPAW - SMS 2 ELKÓVA 114 - FONEPAW - SMS 3 ELKÓVA 114 - FONEPAW - Call Logs ELKÓVA 115 - FONEPAW - Call Logs ELKÓVA 116 - FONEPAW - Pictures 1 ELKÓVA 117 - FONEPAW - Pictures 2 ELKÓVA 117 - FONEPAW - Pictures 3 ELKÓVA 118 - FONEPAW - Pictures 3 ELKÓVA 119 - Gallery Trash. ELKÓVA 119 - Gallery Trash. ELKÓVA 120 - FONEPAW - Videos ELKÓVA 121 - FONEPAW - Videos ELKÓVA 122 - BUSYBOX Welcome Message. ELKÓVA 123 - BUSYBOX Velcome Message. ELKÓVA 124 - BUSYBOX Installed. ELKÓVA 125 - Device Partitions 1. ELKÓVA 126 - Device Partitions 2. ELKÓVA 127 - Device Partitions 3. ELKÓVA 128 - adb forward. ELKÓVA 130 - netcat. ELKÓVA 131 - Physical Image Finished 1. | . 89 . 90 . 90 . 91 . 91 . 91 . 91 . 92 . 93 . 93 . 93 . 93 . 93 . 95 . 95 . 95 . 96 . 97 . 98 . 98 . 99 . 99 |

| Εικόνα 133 - Physical Image MD5 & SHA 1 Hashes | 99 |
|--|-----|
| Εικόνα 134 - Autopsy Modules | 100 |
| Εικόνα 135 - Evidence Tree - Volumes | 101 |
| Εικόνα 136 - Evidence Tree - File Types | 102 |
| Εικόνα 137 - Evidence Tree - Deleted Files | 102 |
| Εικόνα 138 - Databases | 103 |
| Εικόνα 139 - Databases Listing | 103 |
| Εικόνα 140 - Περιεχόμενα Database | 104 |
| Εικόνα 141 - Device Partitions File Systems | 105 |
| Εικόνα 142 - /data/data/com.samsung.android.providers.contacts/databases | 106 |
| Εικόνα 143 - adb pull database contacts2.db from sdcard | 106 |
| Εικόνα 144 - Gmail on Device | 107 |
| Εικόνα 145 - Raw Contacts on Device 1 | 108 |
| Εικόνα 146 - Raw Contacts on Device 2 | 108 |
| Εικόνα 147 - Raw Contacts on Device 3 | 109 |
| Εικόνα 148 - Raw Contacts on Device 4 | 109 |
| Εικόνα 149 - Andriller | 110 |
| Εικόνα 150 - Andriller - Allow USB debugging? | 111 |
| Εικόνα 151 - Andriller Results Folder | 111 |
| Εικόνα 152 - Andriller – Extract | 112 |
| Εικόνα 153 - Andriller - Finished | 112 |
| Εικόνα 154 - Andriller Full Log File | 113 |
| Εικόνα 155 - Andriller Results 1 | 114 |
| Εικόνα 156 - Andriller Report | 114 |
| Εικόνα 157 - Andriller Recovered Files | 115 |

ABSTRACT

The purpose of this thesis is to investigate the research field of digital forensics, specifically the scientific branch of mobile forensics. The field of research was limited to mobile phones using the operating system android 10. Throughout the survey a Samsung Galaxy A70 phone was used and not an emulator.

The research began by rooting the device. First we showed the removal of lock screen protections and the process to uninstall Knox which may cause problems in the forensic process of securing a mobile device.

Furthermore, we managed to acquire a logical level image of the device using tools from the Santoku collection and the capabilities provided from the android 10 device, this method wasn't efficient since it provided little to no data. It provided though an interesting finding the IMSI, which is information that shouldn't be this easy to find in a logical extraction. We also managed to get a logical level image of the device using the 30 days free trial version of the program FonePaw, this logical extraction proved more efficient than the one from Santoku and provided more data from the device, it didn't provide the IMSI.

Afterwards we managed to acquire a physical image of the entire device using the tools dd and netcat. We tried to analyze the physical image using Autopsy but didn't manage to do so successfully. We also used andriller which is another open source solution to perform a physical analysis of the device but got only the general information of the device.

We found no open source available programs to the public that can do a successful physical image analysis of android 10.

ΕΙΣΑΓΩΓΗ

Το λειτουργικό σύστημα Android είναι το κυρίαρχο λειτουργικό σύστημα στις κινητές συσκευές εφόσον κατέχει το μεγαλύτερο μερίδιο της αγοράς παγκοσμίως (Εικόνα 1) με συντριπτικό ποσοστό της τάξεως του 72.48% (Hazra & Mateti, 2017) (statcounter, 2019 - 2020).



Εικόνα 1 - Κυρίαρχα Λειτουργικά Συστήματα (statcounter, 2019 - 2020)

Ο αριθμός των κινητών συσκευών που λειτουργούσαν παγκοσμίως για το έτος 2020 ανέρχεται στα 14 δισεκατομμύρια (Εικόνα 2) και αναμένεται να αυξηθεί (statista, 2020).



Εικόνα 2 - Ενεργές Κινητές Συσκευές Παγκοσμίως (statista, 2020)

Από τις κινητές συσκευές για το έτος 2020 τις μεγαλύτερες πωλήσεις καταγράφει η Samsung (Εικόνα 3), κατέχοντας σταθερά το μεγαλύτερο μερίδιο της παγκόσμιας αγοράς με τις συσκευές τους κατά κύριο λόγο να έχουν το λειτουργικό σύστημα Android (statcounter, 2019-2020).



Εικόνα 3 - Samsung Market share (statcounter, 2019-2020)

Ο μέσος χρήστης περνάει κατά μέσο όρο 3 ώρες και 15 λεπτά την ημέρα στο κινητό του τηλέφωνο (Spajic, 2020) (Lin, 2020) (Matei, 2019). Οι επιλογές που δίνονται πλέον με ένα κινητό τηλέφωνο είναι απεριόριστες, από ανταλλαγή μηνυμάτων, κλήσεων, λήψη φωτογραφιών, βίντεο, διενέργεια οικονομικών συναλλαγών, διαχείριση αρχείων, web browsing και πολλά ακόμα. Οι κινητές συσκευές καταλήγουν λοιπόν να έχουν μια πληθώρα προσωπικών δεδομένων αποθηκευμένα (Ranjan Roy, et al., 2016) (Nunez, 2020).

Η τεχνολογική εξέλιξη στις κινητές συσκευές έχει προσελκύσει και το ενδιαφέρον τον εγκληματιών δίνοντας τους νέες δυνατότητες για τη διενέργεια παράνομων ενεργειών (Casey, 2011). Από τις κινητές συσκευές συλλέγεται πληθώρα στοιχείων σε έρευνες των διωκτικών αρχών και είναι στατιστικά πιθανό οι κινητές συσκευές προς έρευνα να έχουν λειτουργικό σύστημα android (Hazra & Mateti, 2017).

Πέρα από την χρησιμότητα για τις διωκτικές αρχές η διενέργεια μιας forensics analysis σε κινητές συσκευές μπορεί να ενημερώσει τους χρήστες τι θα πρέπει να αποθηκεύουν τελικά στις συσκευές τους και ποια δεδομένα κρατάνε τελικά οι συσκευές για τους χρήστες (Ranjan Roy, et al., 2016).

Για τους προαναφερθέντες λόγους έγινε η επιλογή να πραγματοποιηθεί η έρευνα σε κινητή συσκευή Samsung (Samsung Galaxy A70) με μοντέλο SM-A705FN/DS) και λειτουργικό σύστημα Android 10. Στην παρούσα διπλωματική εργασία εξετάσθηκαν αναλυτικά οι διαδικασίες:

- Απόκτησης root πρόσβασης στην συσκευή
- Παράκαμψης μηχανισμών ασφάλειας και κλειδώματος οθόνης
- Διαχείρισης permissions, απενεργοποίηση κρυπτογράφησης και απεγκατάστασης Knox
- Logical Level Forensic Image Acquisition and Analysis
- Physical Forensic Image Acquisition
- Physical Forensic Image Analysis

Είδαμε όλες τις πληροφορίες που αποθηκεύει η κινητή συσκευή για την δραστηριότητα και τις επικοινωνίες που έχουν πραγματοποιηθεί καθώς και τα προβλήματα που μπορεί να αντιμετωπίσει ένας ερευνητής με εργαλεία που είναι ελεύθερα διαθέσιμα στο κοινό.

MOBILE FORENSICS – ΘΕΩΡΗΤΙΚΟ ΥΠΟΒΑΘΡΟ

Η εκτέλεση μιας mobile forensics έρευνας έχει ως σκοπό την ανάκτηση δεδομένων από την κινητή συσκευή που ερευνάται τα οποία και θα πρέπει να παραμείνουν αναλλοίωτα, δηλαδή σε μια forensically sound κατάσταση. Αυτό συμβαίνει για να μπορούν να χρησιμοποιηθούν στην συνέχεια της έρευνας ως ψηφιακά πειστήρια (Kostadinov, 2019).

Forensically sound είναι ένας όρος που χρησιμοποιείται εκτενώς στα digital forensics και αφορά την μη αλλοίωση των αρχικών δεδομένων που βρίσκονται στην συσκευή που είναι προς εξέταση από τους ερευνητές. Η βασική αρχή κάθε forensics έρευνας είναι ότι τα δεδομένα δεν πρέπει να υποστούν κανενός είδους επεξεργασία. Αυτό είναι ιδιαιτέρως δύσκολο στην έρευνα των κινητών συσκευών. Ορισμένα εργαλεία απαιτούν επικοινωνία με την κινητή συσκευή που ερευνάται, το γεγονός αυτό αποκλείει τους write protectors. Άλλα εργαλεία προϋποθέτουν την root πρόσβαση στην συσκευή για να παρέχουν αποτελέσματα (Bommisetty, et al., 2014).

Στις περιπτώσεις που η mobile forensics έρευνα απαιτεί την οποιαδήποτε επέμβαση στην συσκευή η διαδικασία που ακολουθείται από τον ερευνητή και οι αλλαγές θα πρέπει να καταγράφονται αναλυτικά και να ακολουθούνται οι προτεινόμενες μεθοδολογίες. Η παράληψη καταγραφής κάποιου βήματος μπορεί να οδηγήσει σε απόρριψη των αποτελεσμάτων της έρευνας στο δικαστήριο (Soufiane, 2016).

Ένα από τα βασικότερα προβλήματα στην forensics έρευνα των κινητών συσκευών αφορά το γεγονός ότι τα δεδομένα που είναι αποθηκευμένα σε αυτές μπορούν να είναι προσβάσιμα από άλλες κινητές συσκευές ή υπολογιστές. Τα δεδομένα που είναι αποθηκευμένα σε κινητές συσκευές χαρακτηρίζονται volatile καθώς μπορούν να τροποποιηθούν και να διαγραφούν μέσα σε σύντομο χρονικό διάστημα απομακρυσμένα. Συνεπώς απαιτείται μεγαλύτερη προσοχή και προσπάθεια από τους ερευνητές προκειμένου να διατηρηθούν ανέπαφα και να μπορεί να αποδειχθεί η μη αλλοίωσή τους κατά την διάρκεια της έρευνας (Bommisetty, et al., 2014).

Κατά την διάρκεια μιας mobile forensics έρευνας μπορούν να προκύψουν διάφορα προβλήματα που αφορούν την απόκτηση των ψηφιακών πειστηρίων από τις κινητές συσκευές. Τα προβλήματα αυτά οφείλονται κυρίως στα ακόλουθα (Bommisetty, et al., 2014):

- Ποικιλία hardware
- Εκδόσεις λειτουργικών συστημάτων κινητών συσκευών
- Μέτρα ασφάλειας
- Έλλειψη υλικού
- Κατάσταση της συσκευής
- Τεχνικές anti-forensics
- Αθέμιτο reset
- Τροποποίηση των δεδομένων της συσκευής
- Παράκαμψη προστασιών οθόνης της συσκευής
- Αποκοπή της επικοινωνίας της συσκευής με το δίκτυο μετά την κατάσχεσή της
- Υπαρξη malware στην συσκευή
- Νομικά ζητήματα

ΔΙΑΔΙΚΑΣΙΑ ΕΡΕΥΝΑΣ MOBILE FORENSICS

Η διαδικασία μιας mobile forensics έρευνας μπορεί να χωριστεί σε τρία βασικά στάδια (Kostadinov, 2019):

- Seizure: Κατάσχεση της κινητής συσκευής
- Acquisition: Συλλογή στοιχείων
- Examination/Analysis: Εξέταση/Ανάλυση στοιχείων

ΚΑΤΑΣΧΕΣΗ ΚΙΝΗΤΗΣ ΣΥΣΚΕΥΗΣ

Η κατάσχεση μιας κινητής συσκευής θα πρέπει να γίνεται σύμφωνα με κάποιες διαδικασίες που διασφαλίζουν ότι μια συσκευή δεν θα υποστεί τροποποιήσεις μέχρι να φτάσει στο εργαστήριο (Brunty, 2016) (Bommisetty, et al., 2014) (Kostadinov, 2019).

Secure the Phone: Αποτρέπεται η επαφή των ατόμων που υπάρχουν στο σημείο με την συσκευή, είτε η συσκευή είναι ενεργή είτε όχι.

Capture the Information on Display: Γίνεται καταγραφή όλων των πληροφοριών που εμφανίζονται στην οθόνη με την χρήση κάμερας.

Prevent Network Access: Αποτρέπεται η σύνδεση της συσκευής με το τηλεπικοινωνιακό δίκτυο, αυτό γίνεται τοποθετώντας την συσκευή μέσα σε faraday bag.

Seize Relevant Hardware: Ο ερευνητής θα πρέπει να κατασχέσει μαζί με την συσκευή και πιθανό hardware που μπορεί να σχετίζεται με αυτή.

Seize Relevant Documentation: Ο ερευνητής θα πρέπει επιπρόσθετα να κατασχέσει και πιθανά έγγραφα που σχετίζονται με την συσκευή.

Secure Transportation: Πραγματοποίηση ασφαλούς μεταφοράς από τον τόπο κατάσχεσης στο εργαστήριο.

Document Everything: Γίνεται λεπτομερής καταγραφή όλων των ενεργειών που σχετίζονται με την κινητή συσκευή που είναι προς έρευνα από την στιγμή που βρέθηκε μέχρι να φτάσει στο εργαστήριο. Καταγράφονται επιπρόσθετα και τα άτομα που πραγματοποιούν τις συγκεκριμένες ενέργειες.

ΣΥΛΛΟΓΗ ΣΤΟΙΧΕΙΩΝ

Στην συγκεκριμένη φάση μιας mobile forensics έρευνας στόχος του ερευνητή είναι να συλλέξει όσες περισσότερες πληροφορίες μπορεί προκειμένου να πραγματοποιήσει έπειτα την διαδικασία της ανάλυσής τους. Οι πηγές πληροφοριών είναι (Brunty, 2016) :

- Η συσκευή
- Η κάρτα SIM
- Η κάρτα μνήμης SD
- To Documentation
- Ο πάροχος του δικτύου κινητής τηλεφωνίας
- Οι άνθρωποι
- Οι υπολογιστές

ΕΞΕΤΑΣΗ/ΑΝΑΛΥΣΗ ΣΤΟΙΧΕΙΩΝ

Πρώτο στάδιο στην διαδικασία εξέτασης των στοιχείων είναι η φάση αναγνώρισης/ identification phase. Εδώ ο ερευνητής θα πρέπει να μπορεί να αναγνωρίσει και να καταγράψει (Bommisetty, et al., 2014):

- Νομική Αρχή
- Στόχο Έρευνας
- Βασικές Πληροφορίες για την Κινητή Συσκευή
- Πρόσθετα αποθηκευτικά μέσα (sd/microsd card)
- Πιθανές πηγές άλλων πειστηρίων

Η διαδικασία της ανάλυσης μιας κινητής συσκευής μπορεί να χωριστεί σε πέντε επίπεδα, τα επίπεδα αυτά απαριθμούνται στην συνέχεια ξεκινώντας από αυτό που απαιτεί την μικρότερη επέμβαση στην κινητή συσκευή (Kostadinov, 2019) (Bommisetty, et al., 2014).

Manual/ Scroll Analysis: Η συγκεκριμένη διαδικασία πραγματοποιείται όταν εντοπιστεί η κινητή συσκευή και πριν τοποθετηθεί σε faraday bag. Ο ερευνητής πραγματοποιεί scroll κατευθείαν στην συσκευή και καταγράφει με την χρήση κάμερας όλα τα μενού και τις πληροφορίες που φαίνονται στην συσκευή.

Logical Analysis: Η Logical ανάλυση προϋποθέτει την σύνδεση της κινητής συσκευής και του forensic workstation, δηλαδή του υπολογιστή στον οποίο θα πραγματοποιηθεί όλη η διαδικασία ανάλυσης των δεδομένων που έχουν ανακτηθεί από την συσκευή. Η σύνδεση μεταξύ συσκευής και workstation πραγματοποιείται συνήθως με την χρήση usb καλωδίου. Στην συνέχεια από τον υπολογιστή με την χρήση συγκεκριμένων εντολών ή του κατάλληλου προγράμματος γίνεται η ανάκτηση των δεδομένων. Στο συγκεκριμένο στάδιο σπάνια έχουμε την ανάκτηση διαγραμμένων αρχείων από την συσκευή.

Physical Analysis: Κατά την διαδικασία της physical ανάλυσης μιας συσκευής ο ερευνητής αποκτά physical forensic image της συσκευής και μετά το αναλύει με την βοήθεια λογισμικού.

Η απόκτηση physical forensic image πραγματοποιείται με την βοήθεια εγκατάστασης κάποιου agent στην συσκευή. Ο ερευνητής θα πρέπει να αποθηκεύσει το image σε κάποιον εξωτερικό σκληρό δίσκο και να υπολογίσει τα MD5 και SHA1 hashes του image. Τα συγκεκριμένα hashes θα πρέπει να μείνουν τα ίδια σε όλη την διάρκεια της έρευνας, έτσι ο ερευνητής θα μπορεί να αποδείξει την μη αλλοίωση του image. Αποθηκεύοντας το image σε εξωτερικό σκληρό δίσκο και να υπολογίσει τα αλλαγή από το workstation του ερευνητή. Ο ερευνητής συνήθως δουλεύει σε αντίγραφο του image για να διασφαλίσει την ακεραιότητα του.

Chip- Off: Κατά την συγκεκριμένη διαδικασία ανάλυσης ο ερευνητής παίρνει δεδομένα κατευθείαν από το memory chip της κινητής συσκευής. Το chip αποσυνδέεται από την κινητή συσκευή και εισάγεται είτε σε έναν chip reader είτε σε άλλη κινητή συσκευή στην οποία και θα γίνει η εξαγωγή των δεδομένων.

Micro Read: Εδώ ο ερευνητής εξετάζει τα δεδομένα που φαίνονται στο memory chip της συσκευής, εξάγοντας το chip από την συσκευή και στην συνέχεια χρησιμοποιώντας ηλεκτρονικό μικροσκόπιο ο ερευνητής μπορεί να αναλύσει τα gates που είναι ορατά στο chip.

1. ΥΛΙΚΟ ΚΑΙ ΛΟΓΙΣΜΙΚΟ

1.1 Γενικές Πληροφορίες Συσκευής

Στην έρευνα χρησιμοποιήθηκε η κινητή συσκευή SAMSUNG GALAXY A70. Συγκεκριμένα το μοντέλο με κωδικό SM-A705FN/DS (Εικόνα 4). Στην συσκευή υπήρχε η έκδοση Android 10 One UI version 2.0 (Εικόνα 5).



Εικόνα 4 - Γενικές Πληροφορίες Συσκευής 1



Εικόνα 5 - Γενικές Πληροφορίες Συσκευής 2

Η επιλογή του usb debugging από το μενού Developer Options ήταν ενεργοποιημένη (Εικόνα 6). Επιπλέον είχε αποκτηθεί root πρόσβαση στην συσκευή χρησιμοποιώντας το Odin, η συγκεκριμένη διαδικασία θα αναλυθεί στην συνέχεια.

| 01.20 - FI | ★ 39+111 |
|---|------------|
| < Developer options | Q |
| On | • |
| Debugging | |
| USB debugging Debug mode when USB is connected | |
| Revoke USB debugging authoriza | ations |
| Bug report shortcut Show a button in the power menu for taking a bug report | |
| Select mock location app No mock location app set | |
| Force full GNSS measurements Track all GNSS constellations and frequencie with no duty cycling. | es 🔘 |
| Enable view attribute inspection | \bigcirc |
| Select debug app No debug application set | |
| Wait for debugger Debugged application waits for debugger to attach before executing | \bigcirc |
| Verify apps over USB | - |
| | < |

Εικόνα 6 - Γενικές Πληροφορίες Συσκευής 3

1.2 Διαδικασία Απόκτησης Root Πρόσβασης στην Συσκευή

UNLOCKING THE BOOTLOADER

Για να ενεργοποιήσουμε τα Developer Options πηγαίνουμε στα Settings ->About Phone-> Κάνουμε tap 7 φορές το Build Number και ενεργοποιούμε τα Developer Options (Εικόνα 7).

Στα Developer Options ενεργοποιούμε την επιλογή USB debugging (Εικόνα 8, Εικόνα 9) και OEM unlocking (Εικόνα 10).

| 02:22 🖬 👪 | a 🕄 🖉 |
|---|------------|
| < Developer options | Q |
| On | • |
| Quick settings developer tiles | |
| Trust agents only extend unlock Trust agents will keep your phone unlocked fo longer, but won't unlock your phone if it's locke | or D |
| Lock screen when trust is lost Automatically lock the screen when the last trust agent loses trust. | \bigcirc |
| Debugging | |
| USB debugging Debug mode when USB is connected | \bigcirc |
| Revoke USB debugging authoriza | tions |
| Bug report shortcut Show a button in the power menu for taking a bug report | \bigcirc |
| Select mock location app No mock location app set | |
| Force full GNSS measurements Track all GNSS constellations and frequencies with no duty cycling. | s D |
| Enable view attribute inspection | \bigcirc |
| | |

Εικόνα 7 - Developer Options



Εικόνα 8 - Developer Options Allow USB Debugging Question

| 02:25 🖬 🕄 | ¥ 🖘 🛯 🗎 |
|--|------------|
| < Developer options | Q |
| On | |
| Debugging | |
| USB debugging Debug mode when USB is connected | |
| Revoke USB debugging authoriza | tions |
| Bug report shortcut Show a button in the power menu for taking a bug report | \bigcirc |
| Select mock location app No mock location app set | |
| Force full GNSS measurements Track all GNSS constellations and frequencies with no duty cycling. | s D |
| Enable view attribute inspection | \bigcirc |
| Select debug app No debug application set | |
| Wait for debugger Debugged application waits for debugger to attach before executing | |
| Verify apps over USB | - |
| | (|

Εικόνα 9 - USB Debugging Ενεργοποιημένο

| 18:50 🖬 | 🖌 🖘 📖 🛢 |
|--|------------|
| < Developer options | Q |
| On | |
| Approx. 2.6 GB of 5.8 GB memory use | ed |
| Bug report | |
| Desktop backup password Desktop full backups aren't currently protected | đ |
| Stay awake Screen will never sleep while charging | \bigcirc |
| Enable Bluetooth HCI snoop log | |
| OEM unlocking Allow the bootloader to be unlocked | |
| Running services View and control currently running services | |
| Picture color mode Use sRGB | \bigcirc |
| WebView implementation Android System WebView | |
| III O < | |

Εικόνα 10 - OEM Unlocking Ενεργοποιημένο

Στην συνέχεια απενεργοποιούμε την συσκευή. Βάζουμε την συσκευή σε Download Mode πατώντας ταυτόχρονα τα κουμπιά volume up και volume down και βάζοντας ταυτόχρονα usb καλώδιο που συνδέεται σε υπολογιστή (Εικόνα 11, Εικόνα 12, Εικόνα 13).



Εικόνα 11 - Download Mode 1



Εικόνα 12 - Download Mode 2



Εικόνα 13 - Download Mode 3

Πατάμε Volume up για να κάνουμε Unlock Bootloader (Εικόνα 14, Εικόνα 15).



Εικόνα 14 - Unlock Bootloader



Εικόνα 15 - Bootloader Unlocked Message

NECESSARY DOWNLOAD FILES

Κατεβάζουμε και εγκαθιστούμε στον υπολογιστή μας τους usb drivers για την κινητή συσκευή μας.

Κατεβάζουμε το λογισμικό Odin3-v3.14.1 που αντιστοιχεί στα android 10.

Κατεβάζουμε το κατάλληλο firmware για την συσκευή. Από το Model number της κινητής συσκευής (Εικόνα 16) μπορούμε να αναζητήσουμε στο διαδίκτυο το firmware που αντιστοιχεί σε αυτό (Εικόνα 17).



Εικόνα 16 - Device Model Number

| 😋 🔾 🗢 🚺 🕨 ΔΙΠΛΩΜΑΤ | IKH ANDROID FORENSICS 🕨 A705FNXXU5BTJ4_A705FNOXM5BTJ4_EUR | |
|----------------------|--|--------------------|
| Οργάνωση 🔻 Συμπερίλι | ιψη στη βιβλιοθήκη ▼ Κοινή χρήση με ▼ Εγγραφή Νέος φάκελος | ii • 🔟 🔞 |
| 🛛 🔆 Αγαπημένα | νομα | Ημερομηνία τροπ |
| 😻 Dropbox | AP_A705FNXXU5BTJ4_CL19516864_QB35071200_REV00_user_low_ship_MULT1_CERT_meta_OS10.tar.md5 | 20/10/2020 6:40 µµ |
| 🧮 Επιφάνεια εργασίας | BL_A705FNXXU5BTJ4_CL19516864_QB35071200_REV00_user_low_ship_MULTI_CERT.tar.md5 | 20/10/2020 6:40 µµ |
| 🚺 Λήψεις | CP_A705FNXXU5BTH4_CP16621513_CL19516864_QB33764973_REV00_user_low_ship_MULTI_CERT.tar.md5 | 20/10/2020 6:48 µµ |
| 🖳 Πρόσ.θέσεις | CSC_OMC_OXM_A705FNOXM5BTJ4_CL19516864_QB35071200_REV00_user_low_ship_MULTI_CERT.tar.md5 | 20/10/2020 6:49 μμ |
| 📑 Έγγραφα | HOME_CSC_OMC_OXM_A705FNOXM5BTJ4_CL19516864_QB35071200_REV00_user_low_ship_MULTI_CERT.tar.md5 | 20/10/2020 6:48 µµ |
| ▲ ○ Βιβλιοθήκες | | |

Εικόνα 17 - Firmware Files

Αντιγράφουμε το ΑΡ αρχείο στην συσκευή (Εικόνα 18).

| | 100 C 100 | | | |
|--|---|--|---|--------------------|
| | IKH ANDROID FORENSICS + A705FNXXUSBTJ4_A705FN0XMSBTJ4_EUR | 4) [Αναζήτηση - β | 🕒 🔍 📲 ζ. • Υπολογιστής • Galaxy Α70 • | • +9 Avačhtnan - P |
| Οργάνωση 🔻 🗋 Άνοιγι | μα Κοινή χρήση με 👻 Εγγραφή Νέος φάκελος | i= • 🗇 🛛 | Οργάνωση 🕶 | 8 · 0 0 |
| Αγοπημένα Ότορδακ Επυράνεια εργασίας Λήψτις Πρόα,θέσεις Εγγραφα | Organ Patrix ADSPINOUUSETH_CLISSIBAE4, QEISOTIZIO_IEROD, user, Jone, John, JMULTL, BL_ADSPINOUUSETH_CLISSIBAE4, QEISOTIZIO_IEROD, user, Jone, John, JMULTL, Patrix ADSPINOUUSETH_CLISSIBAE4, QEISOTIZIO_IEROD, user, Jone, John, JMULTL, C_ADSPINOUUSETH_CLISSIBAE4, QEISOTIZIO_IEROD, user, Jone, John, JMULTL, Patrix ADSPINOUUSETH_CLISSIBAE4, QEISOTIZIO_IEROD, user, Jone, JMULTL, C_ADSPINOUUSETH_CLISSIBAE4, QEISOTIZIO_IEROD, USER, JONE, JANON, USER, | Никориния трет IEIT_meta_0S10.taxmd5 2010/2026.669 µ EIT_axmd5 2010/2026.669 µ John 2026.c68 3010/2026.668 µ John 2020.c68 3010/2026.678 µ John 2020.c68 3010/2026.678 µ John 2020.c68 3010/2026.678 µ </td <td>Ayemyukov Oropbox Torpbox Torpbox</td> <td></td> | Ayemyukov Oropbox Torpbox Torpbox | |
| Βιβλιοθήκες Podcasts Βιντεο Εγγραφα Εκόνες Μουσική | | Προς 'Gelary A70/Phone' | Asupo | |
| 🜏 Οικιακή ομάδα | | | 🔫 Οικεική ομάδα | |
| Υπολογιστής System (C:) Movoδα CD (E:) Movoδα CD (F:) Movoδα CD (H:) Galaxy A70 | | | W Yaoloyurniç B. System (C) Morriska CD (F) Morriska CD (F) Morriska CD (H) Morriska CD (H) Statny A70 | |
| 📬 Δίκτυο 💡 | * (| | | |
| AP_A705FNX0 Apytio MD5 | KUSBTJ4_CL19516864_Q8350 Ката́отоал, 28 Ком⁄арлата Нµ/\ Никроулука трат 20/10/2020 640 µµ К Мукевос 4.61 GB | κα δημιουργί 20/11/2020 640 μμ ίοιτή χρήση με: Οικιακή ομόδα | | |

Εικόνα 18 - Αντιγραφή ΑΡ Αρχείου στην Συσκευή

Κατεβάζουμε και εγκαθιστούμε στην συσκευή την εφαρμογή Magisk Manager (Εικόνα 19, Εικόνα 20).

| | 7 D Q · | | | | Ø |
|---------------------------------------|--|---|---|--------------------------------------|--------|
| <u>ک</u> | google. | com/searc | ch?q=ma | g 1 | : |
| = | | Goog | le | (| s |
| Q r | magisk man | ager | | | × |
| ολα | ΕΙΚΟΝΕΣ | BINTEO | ειδησεις | ΧΑΡΤΕΣ | A |
| 🛞 ma | agiskmanager.c | om | | | |
| Dowr 8.0.2 | nload Magi For Andro | sk Manag id 2020 | er Latest | Version | |
| Magis phone and | k Manager is a . With the help | an app which o of Magisk y | helps user ou can run | s to root thei banking app | r s |
| Total [| Downloads: 50 |),000,000+ | | | |
| Androi | id Version Rec | uires: 4.2+ | | | |
| App Si | ze: 1.85 MB | | | | |
| Last U | pdated: Octob | per 08, 2020 | | | |
| What | t is Rooting? | What is Ma | agisk? | What is Magi | sk N |
| How both o Flashir recom | ww.xda-develope to Install N f which are pr ng Magisk usi mended | ers.com⇒ho <mark>/agisk - X[</mark> esent in Mag ng a custom | A Develo isk Manage recovery is | o pers er. However, the | |
| | | | | | |
| A wi | ww.apkmirror.co | m ⇒topjohnwu | | | |
| 🔺 🐝 Magi | ww.apkmirror.co sk Manage | er APKs - A | PKMirro | r | |
| Magi Install, Systen are sol | ww.apkmirror.co sk Manage , upgrade, mar nless Interfac me key | m - topjohnwu er APKs - A nage, configu e - Magisk wi | PKMirro re the Unive thin a singl | r ersal e app! Here | |

Εικόνα 19 - Magisk Manager Google



| | \bigcirc | < | |
|--|------------|---|--|



Εντός της εφαρμογής επιλέγουμε εγκατάσταση για το Magisk (Εικόνα 21).

| 19:16 🖬 🕤 জিল | d 2 | | | | | | |
|--|---|--|--|--|--|--|--|
| Home | 礅 | | | | | | |
| | | | | | | | |
| 🖗 Magisk 🖪 Εγκατάστασ | η | | | | | | |
| Latest 20.4 (20400) Α/Β Νο Εγκαταστάθηκε Ν/Α SAR Yes Ramdisk Νο Crypto File | | | | | | | |
| 🧧 Manager 🕄 Εγκατάστασ | η | | | | | | |
| Latest 8.0.3 (314) (14) Εγκαταστάθηκε 8.0.3 (314) Package com.topjohnwu.magisk | Latest 8.0.3 (314) (14) Εγκαταστάθηκε 8.0.3 (314) Package com.topjohnwu.magisk | | | | | | |
| Check SafetyNet | | | | | | | |
| Support Us Magisk is, and always will be, free and open-source. You can however show us that you care by sending a small conation. @copjohnwu @ (appingen) @ (apping | | | | | | | |
| | | | | | | | |
| | | | | | | | |

Εικόνα 21 - Magisk Manager Εγκατάσταση (Εντός App)

Επιλέγουμε ΝΕΧΤ (Εικόνα 22).



Εικόνα 22 - Magisk Manager NEXT

Στην συνέχεια το Magisk θα ζητήσει ένα αρχείο zip ή ένα patched recovery image. Επιλέγουμε select and patch a file (Εικόνα 23).



Εικόνα 23 - Magisk Manager Select & Patch a File

Επιλέγουμε το ΑΡ αρχείο του firmware που είχαμε αντιγράψει στην συσκευή (Εικόνα 24).



Εικόνα 24 - Magisk Manager Επιλογή ΑΡ Αρχείου

Εκκινούμε την διαδικασία (Εικόνα 25, Εικόνα 26).



Εικόνα 25 - Magisk Manager Έναρξη Διαδικασίας Patch



Εικόνα 26 - Magisk Manager Πρόοδος Διαδικασίας

Το αρχείο που προκύπτει το αντιγράφουμε στον υπολογιστή μας από την συσκευή καθώς θα το χρησιμοποιήσουμε στην συνέχεια.

ODIN

Για να κάνουμε flash τα αρχεία στην συσκευή χρησιμοποιήσαμε το Odin3v3.14.1 που αντιστοιχεί στα android 10. Χρησιμοποιώντας το συγκεκριμένο λογισμικό μπορεί κανείς να εγκαταστήσει επίσημο firmware της Samsung σε κινητές συσκευές, να εγκαταστήσει custom roms, να κατεβάσει τις τελευταίες ενημερώσεις για kernels και να αποκτήσει root πρόσβαση σε κινητές συσκευές.

Απενεργοποιούμε την συσκευή και την βάζουμε σε Download mode πατώντας ταυτόχρονα το volume up και volume down και συνδέοντας την συσκευή στον υπολογιστή με usb καλώδιο.

Στο warning που εμφανίζεται (Εικόνα 27) αφού βάλουμε την συσκευή σε Download mode πατάμε volume up για να συνεχίσουμε.



Εικόνα 27 - Download Mode Warning

Ανοίγουμε το Odin που θα πρέπει να εμφανίσει το μήνυμα Added για να έχει αναγνωρίσει σωστά την συσκευή (Εικόνα 28).

| 📮 Odin3 v3.14 | | | | | |
|---|---|--|--|--|--|
| Odin3 | | | | | |
| | | | | | |
| ID:COM 0:[COM4] | | | | | |
| Log Options Pit CID:0/004> Added!! | Tips - How to download HOME binary OLD model : Download one binary "(BUILD_VER)_XXX_HOME.tar.md5" ex) G925FXXU3DPA5_G925FXXU3DPA5_G925FXXU3DPA5_HOME.tar.md5 NEW model : Download BL + AP + CP + HOME_CSC BL CP CP CSC USERDATA | | | | |
| | Mass D/L ► | | | | |
| - | Start Reset Exit | | | | |
| Odin Community : http://mobilerndhub.sec.samsung.net/hub/site/odin/ | | | | | |

Εικόνα 28 - Odin Added Message

Στην καρτέλα Options αποεπιλέγουμε το Auto Reboot (Εικόνα 29). Πατάμε το κουμπί ΑΡ και επιλέγουμε το αρχείο magisk_patched.tar (Εικόνα 30).

| 📮 Odin3 v3.14 | |
|---|--|
| Odin3 | |
| | |
| ID:COM 0:[COM4] | |
| Log Options Pit | Tips - How to download HOME binary OLD model : Download one binary "(BUILD_VER)_XXX_HOME.tar.md5" ex) G925FXXU3DPA5_G925F0XA3DPA5_G925FXXU3DPA5_HOME.tar.md5 NEW model : Download BL + AP + CP + HOME_CSC |
| Nand Erase Re-Partition | BL |
| F. Reset Time | AP AP |
| Elash Lock | CP CP |
| Decompress Data | CSC |
| | USERDATA |
| AutoStart | Mass D/L ► |
| recourd download in possible | Start Reset Exit |
| Odin Community : http://mobilerndhub.sec.samsung.net/hub/site | <u>/odin/</u> |

Εικόνα 29 - Odin Auto Reboot Αποεπιλογή

| 📮 Odin3 v3.14 | | | |
|--|-------------|--|--|
| Odin3 | | | |
| ID:COM | | | |
| 0.[COM+] | | | |
| Log Options Pit | - Tips - I | How to download HC OLD model : Dow ex) G925FX NEW model : Dow | JME binary vnload one binary "(BUILD_VER)_XXX_HOME.tar.md5" XXIJ3DPA5_G925FOXA3DPA5_G925FXXU3DPA5_HOME.tar.md5 vnload BL + AP + CP + HOME_CSC |
| | | | |
| RePartition | | BL | |
| F. Reset Time | | | ;\Σεμίνα\Desktop\ΔΙΠΛΩΜΑΤΙΚΗ ANDROID FORENSICS\magisk_patched.tar |
| | | | |
| Flash Lock | | СР | |
| Decompress Data | | CSC | |
| | | USERDATA | |
| AutoStart Reboot download if possible | | | Mass D/L ► |
| Odin Community : http://mobilerndhub.sec.samsung.net/hub/site/or | <u>din/</u> | | Start EXIT |

Εικόνα 30 - Odin Επιλογή AP magisk_patched.tar

Στην συνέχεια επιλέγουμε τα αντίστοιχα firmware αρχεία στις υπόλοιπες επιλογές (Εικόνα 31) του Odin από το firmware που είχαμε κάνει download:

ΒL

СР

CSC
| Odin3 | | Ę |
|---|--|---|
| D:COM 0:[COM4] | | |
| | Tips - Herrite deveload HOME bioasy | |
| Log Options Pit <id:0 004=""> Added!! <osm>> Enter CS for MD5 <osm>> Check MD5 on unplug the cable <osm>> Please wait</osm></osm></osm></id:0> | OLD model : Download one binary "(BUILD_VER)_XXX_HOME.tar.m ex) G925FXXU30PA5_G925FXXA30PA5_G925FXXU30PA5_HOM NEW model : Download BL + AP + CP + HOME_CSC | d5" 1E.tar.md5 ship MULTI CERT.tar.md |
| <osm> Checking MD5 thrished Sucesstully <osm> Leave CS <osm> Enter CS for MD5 <osm> Check MD5 Do not unplug the cable</osm></osm></osm></osm> | ΔL - | NSICS\magisk_patched.t |
| <osm> Please wait <osm> Checking MD5 finished Sucessfully <osm> Leave CS</osm></osm></osm> | CP .3_CL 19516864_QB33764973_REV00_user_jow_ | ship_MULTI_CERT.tar.mo |
| <usm> Enter CS for MD5 <osm> Check MD5 Do not unplug the cable <osm> Please wait</osm></osm></usm> | CSC I4_CL 19516864_QB35071200_REV00_user_low | ship_MULTI_CERT.tar.mo |
| <osm> Criecking MUS Innisned Successfully</osm> <osm> Leave CS</osm> | USERDATA | Mass D/L + |
| | Start Reset | Exit |

Εικόνα 31 - Odin Επιλογή Υπόλοιπων Αρχείων Firmware

Πατάμε Start για να ξεκινήσει η διαδικασία, μόλις ολοκληρωθεί το Odin θα μας εμφανίσει μήνυμα Pass (Εικόνα 32).

| Odin3 v3.14 | | |
|--|-----------|--|
| Odin3 | | |
| PASS! | | |
| 03:53 | | |
| 0.[00m4] | - | |
| Log Options Pit <1D:0/004> NON+HLOS.bin <1D:0/004> dspso.bin <1D:0/004> ueft ser.mbn | * | OLD model : Download one binary "(BUILD_VER)_XXX_HOME.tar.md5" ex) G925FXXU3DPA5_G925FXXU3DPA5_G925FXXU3DPA5_HOME.tar.md5 NEW model : Download BL + AP + CP + HOME_CSC |
| <id:0 004=""> vbmeta.img <id:0 004=""> vendor.img.ext4</id:0></id:0> | | BL I4_CL19516864_QB35071200_REV00_user_low_ship_MULTI_CERT.tar.md |
| <id:0 004=""> system.ing.ext4 <id:0 004=""> dtbo.img <id:0 004=""> userdata.img.ext4</id:0></id:0></id:0> | V | کوبیانده \Σوبیانده \Desktop \ΔΙΠΛΩΜΑΤΙΚΗ ANDROID FORENSICS \magisk_patched.ta |
| <id:0 004=""> persist.img.ext4 <id:0 004=""> vbmeta.img <id:0 004=""> boot.img</id:0></id:0></id:0> | | CP .3_CL19516864_QB33764973_REV00_user_low_ship_MULTI_CERT.tar.md |
| <id:0 004=""> recovery.img <id:0 004=""> modem.bin <id:0 004=""> code img ext4</id:0></id:0></id:0> | | CSC I4_CL19516864_QB35071200_REV00_user_low_ship_MULTI_CERT.tar.md |
| <id:0 004=""> omr.img.ext4 <id:0 004=""> product.img.ext4</id:0></id:0> | | USERDATA |
| <pre><id:0 004=""> RQI_CLOSE !! <id:0 004=""> RES OK !! <id:0 004=""> Remain Port 0 <osm> All threads completed. (succeed 1 / failed 0)</osm></id:0></id:0></id:0></pre> | = | Mass D/L ► |
| | • | Start Reset Exit |
| din Community : http://mobilerndhub.sec.samsung.net/hub/si | ite/odin/ | |

Εικόνα 32 - Odin PASS! Message

Μόλις ολοκληρωθεί η διαδικασία πατάμε το Volume down και το power button για να βγούμε από το Download mode και όταν σβήσει η οθόνη πατάμε κατευθείαν το volume up και το power για να μπούμε στο recovery mode.

Από το μενού που εμφανίζεται επιλέγουμε wipe data/factory reset (Εικόνα 33, Εικόνα 34) έτσι ολοκληρώνουμε την διαδικασία απόκτησης root πρόσβασης στην συσκευή, αυτό θα σβήσει όλα τα δεδομένα στην συσκευή.



Εικόνα 33 - Wipe Data / Factory Reset 1



Εικόνα 34 - Wipe Data / Factory Reset 2

Για να επανεκκινήσουμε την συσκευή σε rooted os πατάμε παρατεταμένα το volume up και το power και τα αφήνουμε όταν εμφανιστεί το bootloader warning.

Η rooted συσκευή πλέον θα πρέπει να σεταριστεί από την αρχή.

VERIFY ROOT ACCESS

Κατεβάζουμε και εγκαθιστούμε στην συσκευή την εφαρμογή Root Checker από το Play Store για να επαληθεύσουμε εάν πραγματοποιήσαμε με επιτυχία την διαδικασία στην συσκευή.

Στην εφαρμογή Root Checker επιλέγουμε VERIFY ROOT και μας εμφανίζει ότι η διαδικασία της απόκτησης root πρόσβασης στην συσκευή έχει πραγματοποιηθεί με επιτυχία (Εικόνα 35, Εικόνα 36).



Εικόνα 35 - Root Checker App 1



Εικόνα 36 - Root Checker App 2

1.3 Santoku

Για την συνέχεια της έρευνας χρησιμοποιήθηκε το Santoku σαν περιβάλλον workstation, αναλυτικότερα χρησιμοποιήθηκε στις διαδικασίες παράκαμψης ασφάλειας και κλειδώματος οθόνης, στο AFLogical και στο physical image acquisition.

Το Santoku είναι μια open source πλατφόρμα βασισμένη στο Linux. Η έκδοση του Santoku που χρησιμοποιήθηκε για την διενέργεια της έρευνας ήταν η 0.5 εγκατεστημένη σε Virtual Machine που έτρεχε σε περιβάλλον VMware Workstation 15 Pro (Εικόνα 37).

| 🔲 Santoku | |
|--|--------------------|
| Power on this virtual n Edit virtual machine se | nachine ettings |
| ▼ Devices | |
| 📟 Memory | 8 GB |
| Processors | 8 |
| 🖂 Hard Disk (SCSI) | 20 GB |
| 💿 CD/DVD (SATA) | Using file C:\Use |
| 🔁 Network Adapter | NAT |
| 🚭 USB Controller | Present |
| ⊲ಿ Sound Card | Auto detect |
| 🖶 Printer | Present |
| Display | Auto detect |
| Description | |

Type here to enter a description of this virtual machine.

Εικόνα 37 - Santoku VM Settings

To Santoku παρέχει μια σουίτα εργαλείων στους χρήστες που αφορούν τους τομείς (Hoog, 2013):

- Mobile Forensics
- Mobile Malware Analysis
- Mobile Securtiy Testing

2. ΠΑΡΑΚΑΜΨΗ ΜΗΧΑΝΙΣΜΩΝ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΚΛΕΙΔΩΜΑΤΟΣ ΟΘΟΝΗΣ

2.1 Pattern

Έστω ότι η αρχική οθόνη της συσκευής μας είναι κλειδωμένη με pattern (Εικόνα 38).



Εικόνα 38 - Pattern Lock Screen

Από το workstation μας συνδεόμαστε στην συσκευή με su shell. Οι εντολές που χρησιμοποιούμε είναι:

adb devices : αναγνώριση της συσκευής (Εικόνα 39)

adb shell : απόκτηση shell στην συσκευή (Εικόνα 40)

su : απόκτηση su shell στην συσκευή (Εικόνα 40)

santoku@santoku-virtual-machine:~\$ adb devices
* daemon not running. starting it now on port 5037 *
* daemon started successfully *
List of devices attached
R58Mb device

Εικόνα 39 - Pattern Removal - adb devices

Μετακινούμαστε στο directory data (Εικόνα 40):

cd data

| santoku@santoku-virtua | l-machine:~\$ adb shell | |
|------------------------|----------------------------------|------------------|
| a70q:/ \$ su | | |
| a70q:/ # ls | | |
| acct | etc | oem |
| apex | init | omr |
| audit filter table | init.container.rc | proc |
| bin | init.display.rc | product |
| bugreports | init.environ.rc | product_services |
| cache | init.rc | publiccert.pem |
| charger | <pre>init.recovery.qcom.rc</pre> | res |
| config | <pre>init.usb.configfs.rc</pre> | sbin |
| d | init.usb.rc | sdcard |
| data | <pre>init.zygote32.rc</pre> | sepolicy_version |
| debug_ramdisk | <pre>init.zygote64_32.rc</pre> | storage |
| default.prop | lost+found | sys |
| dev | metadata | system |
| dpolicy | mnt | ueventd.rc |
| efs | odm | vendor |
| a70q:/ # cd data | | |
| a70q:/data # ls | | |

Εικόνα 40 – Pattern Removal - cd data

| a70q:/data # ls | |
|-----------------|---------------------------|
| DownFilters | misc |
| adb | misc_ce |
| anr | misc_de |
| apex | nfc |
| арр | nfc_log |
| app-asec | ota |
| app-ephemeral | ota_package |
| app-lib | overlays |
| app-private | pdp_bkup |
| app-staging | preloads |
| app_fonts | property |
| backup | resource-cache |
| bootchart | rollback |
| cache | rollback-observer |
| clipboard | sec |
| custom_image | security |
| dalvik-cache | server_configurable_flags |
| data | snd |
| drm | SS |
| enc_user | system |
| fota | system_ce |
| gsi | system_de |
| hostapd | tad |
| keyfota | tombstones |
| knox | unencrypted |
| local | user |
| log | user_de |
| lost+found | vendor |
| | |

Εικόνα 41 – Pattern Removal - Data Directory Is

Μετακινούμαστε στο directory system (Εικόνα 42):

cd system

Βρισκόμαστε στο directory /data/system , στο συγκεκριμένο directory βρίσκονται τα αρχεία που θα διαγράψουμε.

Διαγράφουμε τα ακόλουθα αρχεία χρησιμοποιώντας την εντολή rm και το όνομα του αρχείου:

gatekeeper.password.key : περιέχει τη σύνοψη του PIN

gatekeeper.pattern.key :περιέχει τη σύνοψη του μοτίβου

locksettings.db :αποθηκεύεται το salt

Επιπρόσθετα διαγράφουμε και τα αρχεία locksettings.db-shm και locksettings.db-wal (Εικόνα 42, Εικόνα 43, Εικόνα 44).

```
a70q:/data # cd system
a70q:/data/system # ls
HWParamTime.bin
PkgPredictions.db
PkgPredictions.db-journal
SimCard.dat
WifiHistory.db
WifiHistory.db-journal
analytics.db
analytics.db-journal
appops.xml
audioservice sec.db
audioservice sec.db-journal
battery-history
battery-saver
batterystats-checkin.bin
batterystats-daily.xml
batterystats.bin
big data sensor usage pkg.txt
big data usage call gesture.txt
bigdata-pkgaccuracy
cachequota.xml
clipboardimage.db
clipboardimage.db-journal
container
conventionalmode
device policies.xml
deviceidle.xml
diskstats cache.json
display-manager-state.xml
```

```
ipm input data.txt
job
last-fstrim
last-header.txt
locksettings.db
locksettings.db-shm
locksettings.db-wal
log-files.xml
ndebugsocket
netpolicy.xml
netstats
notification log.db
notification log.db-journal
notification policy.xml
overlays.xml
package-cstats.list
package-dcl.list
package-dex-usage.list
package-usage.list
package-watchdog.xml
package_cache
packages-warnings.xml
packages.list
packages.xml
packages.xml.mbak
pda.db
pda.db-journal
pre boot csc.dat
```

Εικόνα 42 – Pattern Removal - Directory /data/system Is 1

deviceidle.xml diskstats cache.json display-manager-state.xml displaysolution.db displaysolution.db-journal dmappmgr.db dmappmgr.db-journal dropbox enterprise.conf enterprise.db enterprise.db-journal enterprise.db-shm enterprise.db-wal enterprise cacerts.bks enterprise nativecerts.bks enterprise untrustedcerts.bks enterprise usercerts.bks entropy.dat fmmpassword.key friends gamemanager.db gamemanager.db-journal gatekeeper.password.key gatekeeper.pattern.key graphicsstats harmony_third_party_apps.xml hcm info hcm info-journal heapdump ifw

pda.db pda.db-journal pre boot csc.dat predictor-model predictor-structure procstats recoverablekeystore recoverablekeystore.db recoverablekeystore.db-shm recoverablekeystore.db-wal registered_ucm_services screen_on_time
sensor_big_data_usage.txt
sensor_service
shared_prefs shortcut service.xml slice slocation slocation.db slocation.db-journal slocation.db-se stats companion timezone ucm_ca_cert uiderrors.txt usagestats users watchlist report.db watchlist report.db-journal

Εικόνα 43 - Pattern Removal - Directory /data/system Is 2

enterprise_cacerts.bks enterprise_nativecerts.bks shared_prefs shortcut service.xml enterprise untrustedcerts.bks enterprise usercerts.bks slice entropy.dat slocation fmmpassword.key slocation.db friends slocation.db-journal slocation.db-se gamemanager.db stats_companion gamemanager.db-journal gatekeeper.password.key gatekeeper.pattern.key timezone graphicsstats ucm ca cert harmony third party apps.xml uiderrors.txt hcm info usagestats hcm_info-journal users watchlist_report.db
watchlist_report.db-journal
watchlist_settings.xml heapdump install_sessions install sessions.xml wifigeofence.db wifigeofence.db-journal ipm hitcount.txt a70q:/data/system # rm lo rm: can't remove 'lo': No such file or directory 1|a70q:/data/system # rm locksettings.db a70q:/data/system # rm locksettings.db-shm a70q:/data/system # rm locksettings.db-wal a70q:/data/system # rm gatekeeper.password.key a70q:/data/system # rm gatekeeper.pattern.key a70q:/data/system # exit a70q:/ \$ exit santoku@santoku-virtual-machine:~\$

Εικόνα 44 - Pattern Removal - Directory /data/system Delete Files

Κάνουμε επανεκκίνηση της συσκευής (Εικόνα 45).



Εικόνα 45 - Pattern Removal - Reboot Device

Η διαγραφή του pattern ήταν επιτυχής (Εικόνα 46, Εικόνα 47).



Εικόνα 46 - Pattern Removed Lock Screen 1



Εικόνα 47 - Pattern Removed Lock Screen 2

2.2 Pin

Έστω ότι η αρχική οθόνη της συσκευής μας είναι κλειδωμένη με pin (Εικόνα 48).



Εικόνα 48 - Pin Lock Screen

Από το workstation μας συνδεόμαστε στην συσκευή με su shell. Οι εντολές που χρησιμοποιούμε είναι (Εικόνα 49, Εικόνα 50):

adb devices

adb shell

su



Εικόνα 49 - Pin Removal - adb devices

santoku@santoku-virtual-machine:~\$ adb shell a70q:/ \$ su

Εικόνα 50 - Pin Removal - su shell

Μετακινούμαστε στο directory /data/system (Εικόνα 51, Εικόνα 52).

Από το συγκεκριμένο directory διαγράφουμε τα αρχεία locksettings.db locksettings.db-shm και locksettings.db-wal (Εικόνα 53).

Τα αρχεία gatekeeper.password.key και gatekeeper.pattern.key δεν υπάρχουν στο directory εφόσον έχει γίνει ήδη διαγραφή κατά την αφαίρεση του pattern, σε περίπτωση που δεν τα είχαμε ήδη διαγράψει προηγουμένως θα υπήρχαν και θα έπρεπε να διαγράψουμε κα αυτά πάλι.

a70q:/data # cd system a70q:/data/system # ls HWParamTime.bin PkgPredictions.db PkgPredictions.db-journal SimCard.dat WifiHistory.db WifiHistory.db-journal analytics.db analytics.db-journal appops.xml audioservice sec.db audioservice sec.db-journal battery-history battery-saver batterystats-checkin.bin batterystats-daily.xml batterystats.bin big data sensor usage pkg.txt big data usage call gesture.txt bigdata-pkgaccuracy cachequota.xml clipboardimage.db clipboardimage.db-journal container conventionalmode device policies.xml deviceidle.xml diskstats cache.json display-manager-state.xml

last-fstrim
last-header.txt
locksettings.db
locksettings.db-shm
locksettings.db-wal
log-files.xml

ndebugsocket

netpolicy.xml
netstats

notification_log.db notification_log.db-journal notification_policy.xml overlays.xml package-cstats.list package-dcl.list package-dex-usage.list package-usage.list package-watchdog.xml

package_cache

packages-warnings.xml
packages.list
packages.xml
packages.xml.mbak
pda.db
pda.db-journal
pre_boot_csc.dat
predictor-model
predictor-structure

Εικόνα 51 - Pin Removal - Directory /data/system Is 1

```
displaysolution.db
displaysolution.db-journal
dmappmgr.db
dmappmgr.db-journal
dropbox
enterprise.conf
enterprise.db
enterprise.db-journal
enterprise.db-shm
enterprise.db-wal
enterprise cacerts.bks
enterprise nativecerts.bks
enterprise untrustedcerts.bks
enterprise usercerts.bks
entropy.dat
fmmpassword.key
friends
gamemanager.db
gamemanager.db-journal
graphicsstats
harmony third party apps.xml
hcm info
hcm info-journal
heapdump
ifw
install sessions
install sessions.xml
ipm hitcount.txt
ipm input data.txt
job
```

procstats recoverablekeystore recoverablekeystore.db recoverablekeystore.db-shm recoverablekeystore.db-wal registered ucm services screen on time sensor big data usage.txt sensor service shared prefs shortcut service.xml slice slocation slocation.db slocation.db-journal slocation.db-se stats companion storage.xml sync timezone ucm ca cert uiderrors.txt usagestats users watchlist report.db watchlist report.db-journal watchlist settings.xml wifigeofence.db wifigeofence.db-journal

Εικόνα 52 - Pin Removal - Directory /data/system Is 2

| a70q:/data/system | # | rm locksettings.db |
|-------------------|---|-----------------------------------|
| a70q:/data/system | # | <pre>rm locksettings.db-wal</pre> |
| a70q:/data/system | # | rm locksettings.db-shm |
| a70q:/data/system | # | exit |
| a70q:/ \$ exit | | |

Εικόνα 53 - Pin Removal - Directory /data/system Delete Files

Κάνουμε επανεκκίνηση της συσκευής (Εικόνα 54).



Εικόνα 54 - Pin Removal - Reboot Device

Η διαγραφή του pin ήταν επιτυχής (Εικόνα 55, Εικόνα 56).



Εικόνα 55 - Pin Removed Lock Screen 1



Εικόνα 56 - Pin Removed Lock Screen 2

2.3 Password

Έστω ότι η αρχική οθόνη της συσκευής μας είναι κλειδωμένη με password(Εικόνα 57).



Εικόνα 57 - Password Lock Screen

Από το workstation μας συνδεόμαστε στην συσκευή με su shell (Εικόνα 58).



Εικόνα 58 - Password Removal - adb devices & su shell

Μετακινούμαστε στο directory /data/system (Εικόνα 59).



Εικόνα 59 - Password Removal - cd /data/system

Από το συγκεκριμένο directory διαγράφουμε τα αρχεία locksettings.db locksettings.db-shm και locksettings.db-wal (Εικόνα 60, Εικόνα 61, Εικόνα 62).

Τα αρχεία gatekeeper.password.key και gatekeeper.pattern.key δεν υπάρχουν στο directory εφόσον έχει γίνει ήδη διαγραφή κατά την αφαίρεση του pattern, σε περίπτωση που δεν τα είχαμε ήδη διαγράψει προηγουμένως θα υπήρχαν και θα έπρεπε να διαγράψουμε κα αυτά πάλι.

a70q:/data/system # ls HWParamTime.bin PkgPredictions.db PkgPredictions.db-journal SimCard.dat WifiHistory.db WifiHistory.db-journal analytics.db analytics.db-journal appops.xml audioservice sec.db audioservice sec.db-journal battery-history battery-saver batterystats-checkin.bin batterystats-daily.xml batterystats.bin big data sensor usage pkg.txt big data usage call gesture.txt bigdata-pkgaccuracy cacheguota.xml clipboardimage.db clipboardimage.db-journal container conventionalmode device policies.xml deviceidle.xml diskstats cache.json display-manager-state.xml displaysolution.db

last-fstrim last-header.txt locksettings.db locksettings.db-shm locksettings.db-wal log-files.xml ndebugsocket netpolicy.xml netstats notification log.db notification log.db-journal notification policy.xml overlays.xml package-cstats.list package-dcl.list package-dex-usage.list package-usage.list package-watchdog.xml package cache packages-warnings.xml packages.list packages.xml packages.xml.mbak pda.db pda.db-journal pre boot csc.dat predictor-model predictor-structure procstats

Εικόνα 60 - Password Removal - Directory /data/system Is 1

displaysolution.db-journal dmappmgr.db dmappmgr.db-journal dropbox enterprise.conf enterprise.db enterprise.db-journal enterprise.db-shm enterprise.db-wal enterprise cacerts.bks enterprise nativecerts.bks enterprise untrustedcerts.bks enterprise usercerts.bks entropy.dat fmmpassword.key friends gamemanager.db gamemanager.db-journal graphicsstats harmony third party apps.xml hcm info hcm info-journal heapdump ifw install sessions install sessions.xml ipm hitcount.txt ipm input data.txt iob

recoverablekeystore recoverablekeystore.db recoverablekeystore.db-shm recoverablekeystore.db-wal registered ucm services screen on time sensor big data usage.txt sensor service shared prefs shortcut service.xml slice slocation slocation.db slocation.db-journal slocation.db-se stats_companion storage.xml sync timezone ucm ca cert uiderrors.txt usagestats users watchlist report.db watchlist report.db-journal watchlist settings.xml wifigeofence.db wifigeofence.db-journal

Εικόνα 61 - Password Removal - Directory /data/system Is 2

a70q:/data/system # rm locksettings.db a70q:/data/system # rm locksettings.db-wal a70q:/data/system # rm locksettings.db-shm a70q:/data/system # exit a70q:/ \$ exit

Εικόνα 62 - Password Removal - Directory /data/system Delete Files

Κάνουμε επανεκκίνηση της συσκευής (Εικόνα 63).



Εικόνα 63 - Password Removal - Reboot Device

Η διαγραφή του password ήταν επιτυχής (Εικόνα 64, Εικόνα 65).



Εικόνα 64 - Password Removed Lock Screen 1



Εικόνα 65 - Password Removed Lock Screen 2

3. ANDROID 10 SECURITY AND PRIVACY FEATURES

3.1 Android 10 Permissions & Scoped Storage

To Android σαν λειτουργικό σύστημα έχει κάποια χαρακτηριστικά σε επίπεδο αρχιτεκτονικής τα οποία υπάρχουν για να διασφαλίσουν την ασφάλεια των χρηστών, των εφαρμογών και των δεδομένων που διαχειρίζεται η συσκευή.

Τα συγκεκριμένα security features υπάρχουν στο λειτουργικό σύστημα και έχουν τους ακόλουθους στόχους (Skulkin, et al., 2018) (Android Developers, 2020):

- Την προστασία των δεδομένων του χρήστη.
- Την προστασία των πόρων του συστήματος.
- Την προστασία των δεδομένων των εφαρμογών από μη εγκεκριμένη πρόσβαση από άλλες εφαρμογές.

Το Android 10 εισάγει νέα features που σκοπό έχουν την ασφάλεια των χρηστών και την προστασία της ιδιωτικότητας τους, ένα από αυτά τα features αφορά το scoped storage access που έχουν πλέον οι εφαρμογές. Το scoped storage περιορίζει την πρόσβαση που έχουν οι εφαρμογές στο storage της συσκευής. Οι εφαρμογές δεν έχουν πρόσβαση σε όλο το storage της συσκευής, όπως συνέβαινε σε παλιότερες εκδόσεις android, πλέον η κάθε εφαρμογή έχει πρόσβαση μόνο σε συγκεκριμένο directory (Singh, 2020) (Goyal, 2020) (Solution Analysts, 2020) (Dwivedi, 2020).

Η διαχείριση του σε τι δεδομένα έχει πρόσβαση η κάθε εφαρμογή και τα permissions που παίρνει στην συσκευή περνάνε στην κυριότητα του χρήστη (Android Developers, 2020). Η διαχείριση των permissions για κάθε εφαρμογή έχει γίνει αναλυτικότερη και περισσότερο user friendly προκειμένου ο χρήστης να κατανοεί ευκολότερα τι permissions παρέχει σε κάθε εφαρμογή (Hindy, 2019) (Wallen, 2019) (VisiHow, n.d.). Επιπρόσθετα έχει δοθεί η επιλογή στους χρήστες να μπλοκάρουν εφόσον το επιθυμούν την background πρόσβαση στην τοποθεσία της συσκευής για εφαρμογές (Ansari, 2020) (Davenport, 2020) (Android Developers, 2020).

Παρόλο που τα συγκεκριμένα security features έχουν ως σκοπό την προστασία των δεδομένων και της ιδιωτικότητας του χρήστη, πολλές φορές δημιουργούν προβλήματα στους forensic investigators από το να αποκτήσουν πρόσβαση στα δεδομένα της συσκευής (Skulkin, et al., 2018).

Από την σκοπιά μιας forensics έρευνας είναι πολύ σημαντικό η κατανόηση των συγκεκριμένων security features και το πώς αυτά επηρεάζουν το ποια δεδομένα

μπορούν να ανακτηθούν από την εκάστοτε συσκευή και κάτω από ποιες συνθήκες (Skulkin, et al., 2018).

Για την συνέχεια της διπλωματικής στην συσκευή μέσω των Settings->Apps θα επιλέξουμε Show System Apps και θα πάμε σε κάθε εφαρμογή ξεχωριστά για να διαχειριστούμε τα permissions. Προκειμένου να μην αντιμετωπίσουμε πρόβλημα με την ανάκτηση δεδομένων από το physical image θα παρέχουμε σε κάθε εφαρμογή όλα τα δυνατά permissions που μπορεί να πάρει.

Πηγαίνοντας στα Settings->Apps->Permission Manager (Εικόνα 66) μπορούμε να διαχειριστούμε τα permissions των εφαρμογών (Εικόνα 67). Μέσω του permission manager μπορούμε να δούμε σε τι παρέχεται permission στην συσκευή και ανοίγοντας την κάθε επιλογή μπορούμε να δούμε τις εφαρμογές που έχουν αποκτήσει το συγκεκριμένο permission.



Εικόνα 66 - Device App List

| 16: | 21 🖬 🛡 🖽 🔸 | S |
|-----|--|---|
| ÷ | Permission manager | ۹ |
| \$ | Body sensors 0 of 2 apps allowed | |
| | Calendar 6 of 9 apps allowed | |
| G | Call logs 8 of 8 apps allowed | |
| ۵ | Camera 11 of 28 apps allowed | |
| * | Contacts 15 of 36 apps allowed | |
| 0 | Location 15 of 27 apps allowed | |
| ٩ | Microphone 8 of 22 apps allowed | |
| ç | Phone 15 of 26 apps allowed | |
| ÷~ | Physical activity 2 of 3 apps allowed | |
| | SMS 7 of 7 apps allowed | |
| | Storage 32 of 48 apps allowed | |
| := | Additional permissions 3 more | |

Εικόνα 67 - Permission Manager



Εικόνα 68 - Call Logs Permissions

3.2 Απενεργοποίηση Κρυπτογράφησης

Τα android 10 έχουν ενεργοποιημένη την κρυπτογράφηση συσκευής ως προεπιλογή (Εικόνα 69). Μέσα από το μενού Settings->Biometrics and security απενεργοποιούμε την επιλογή Strong protection (Εικόνα 70) δηλαδή την κρυπτογράφηση της συσκευής για να μπορούμε να έχουμε πρόσβαση στα δεδομένα της συσκευής σε μορφή plaintext κατά την διαδικασία της forensic analysis (Skulkin, et al., 2018).

| 17:32 🖬 | X { 🖘 di 🛔 |
|---|-------------------|
| < Other security settings | |
| Device admin apps No active apps | |
| Credential storage | |
| Storage type Back up to hardware. | |
| View security certificates Display trusted CA certificates. | |
| User certificates View user certificates. | |
| Install from device storage Install certificates from storage. | |
| Clear credentials Remove all certificates. | |
| Data protection | |
| Strong protection Encrypt your phone using your secure lock type. | |
| Advanced | |
| Trust agents Set screen lock type to use. | |
| Pin windows | \square |
| III O | < |

Εικόνα 69 - Disable Encryption

| 17:32 🖬 | NI 🖘 🛔 |
|--|-----------|
| < Other security setting | IS |
| Device admin apps No active apps | |
| Credential storage | |
| Storage type Back up to hardware. | |
| View security certificates Display trusted CA certificates. | |
| User certificates View user certificates. | |
| Install from device storag Install certificates from storage. | e |
| Clear credentials Remove all certificates. | |
| Data protection | |
| Strong protection Encrypt your phone using your secutype. | ire lock |
| Advanced | |
| Trust agents Set screen lock type to use. | |
| Pin windows | \square |
| III O | < |

Εικόνα 70 - Encryption Disabled

3.3 Απεγκατάσταση Knox

KNOX PROBLEMS

Ένα βασικό χαρακτηριστικό των συσκευών Samsung είναι το σύστημα ασφάλειας που έχουν, Samsung Knox. Το Knox έκανε την εμφάνιση του το 2013 στο Samsung Galaxy S4 με το 4.3 update. Παρέχει πολυεπίπεδη ασφάλεια τόσο σε επίπεδο hardware όσο και σε software και δίνει την δυνατότητα στους χρήστες να απομονώνουν δεδομένα, συνήθως εργασίας, στην συσκευή σε κρυπτογραφημένο περιβάλλον (Samsung, n.d.) (Gillware, n.d.). Το γεγονός αυτό μπορεί να προκαλέσει προβλήματα σε μια forensic analysis συσκευής Samsung που έχει χρησιμοποιηθεί το συγκεκριμένο περιβάλλον, παρόλο που πλέον υπάρχουν εργαλεία που μπορούν να το αντιμετωπίσουν όπως το cellebrite (Cellebrite, 2021).

Ένα άλλο πρόβλημα που προκύπτει με την ύπαρξη του Knox αφορά την απομόνωση της συσκευής. Η σωστή απομόνωση της συσκευής από εξωτερικές παρεμβολές αποτελεί σημαντικό κομμάτι μιας forensics έρευνας (Kostadinov, 2019). Στην περίπτωση που υπάρχει το Knox στην συσκευή είναι ακόμα πιο σημαντικό να πραγματοποιηθεί σωστά η απομόνωση της συσκευής γιατί οι χρήστες με το MyKnox μπορούν να συνδεθούν απομακρυσμένα στην συσκευή και να τροποποιήσουν δεδομένα ακόμα και να διαγράψουν όλα τα δεδομένα της συσκευής, ή να πραγματοποιήσουν remote code injection καταλήγοντας σε κάποια επίθεση μέσω του κινητού. Είναι σημαντικό λοιπόν οι forensic examiners να γνωρίζουν τις δυνατότητες που παρέχει το Knox εάν δουλεύουν σε συσκευές Samsung (Gillware, n.d.) (Samsung, n.d.).

UNINSTALLING KNOX

Στην προκείμενη περίπτωση δεν θα μας απασχολήσει η εφαρμογή Knox συνεπώς προτείνουμε την απεγκατάσταση του Knox και όλων των applications που το αφορούν (Εικόνα 71) (Vivek, 2019).

| 19:44 | M 🔛 🕰 | | NI 🖘 🔐 🛔 |
|------------------------|--------------------------|----------------------------|--------------|
| < | Knox | | × : |
| | COM.SAMS | ung.android | l.knox.attes |
| | com.sec.e 86.02 KB | nterprise. <mark>kn</mark> | ox.attestati |
| 8 | Knox Analy 147 KB | tics Upload/ | ler |
| Ð | Knox Enrol 3.41 MB | Iment Servi | ce |
| | Knox Key (139 KB | Chain | |
| | KnoxVpnP 139 KB | acProcesso | r |
| Look Stora Batte | ing for some ge ry | ething else? | |
| | | | |
| | | | |
| | Ш | 0 | < |
| | | | |

Εικόνα 71 - Knox Apps

Αρχικά μέσω του PlayStore εγκαθιστούμε την εφαρμογή Terminal Emulator (Εικόνα 72).



Εικόνα 72 - Terminal Emulator App

Στην συνέχεια μέσα από την εφαρμογή Magisk στην συσκευή και το μενού των Modules επιλέγουμε το Debloater και το εγκαθιστούμε στην συσκευή (Εικόνα 73).



Εικόνα 73 - Magisk Modules - Debloater

19:54 🖬 🖬 🍵 🔹 \oplus Window 1 × : \$ su # Terminal Emulator was granted Superuser rights Ĩ* (T) 🙂 \$ 9 GIF 1 2 3 4 5 6 7 8 9 0 r t i q W е у u 0 р d f h j k L а S g 1 z Х С ٧ b n m × !#1 Intersection ■ English (US) ■ 4 , • Ш Ο :....: Εικόνα 74 - Terminal Emulator App - su shell

Στην συνέχεια επανερχόμαστε στην εφαρμογή Terminal Emulator. Δίνουμε την εντολή su για να μπούμε σε su shell στην συσκευή (Εικόνα 74).

Etkova 74 - Terminal Emulator App - Su

Στην συνέχεια δίνουμε την εντολή:

debloat (Εικόνα 75)

Η συγκεκριμένη εντολή θα ξεκινήσει αυτόματα το Debloater Magisk Module στο terminal (Εικόνα 76).



Εικόνα 75 - Terminal Emulator App - debloat



Εικόνα 76 - Debloater Module Menu

Επιλέγουμε System Apps και System Priv-Apps στο μενού του Debloater και αναζητούμε όλες τις εφαρμογές του Knox στους καταλόγους των εφαρμογών, τις επιλέγουμε χρησιμοποιώντας τον αριθμό τους και δίνουμε γ για να γίνει η απεγκατάσταση τους (Εικόνα 77, Εικόνα 78, Εικόνα 79, Εικόνα 80).

| | a 🖬 | | | | | | 1 } ?}* | sail 🔳 |
|---|---|--|--|--|---|------------------------------------|------------------|----------------------|
| Windo | ow 1 - | | | | (| Ð | \times | : |
| 114 - Slow 115 - Smart 116 - Smart 117 - Smart 117 - Smart 120 - Systc 121 - Teich 122 - Tricc 123 - Videe 124 - User 125 - Videe 127 - Videe 127 - Videe 128 - Wil-Fi 133 - Wil-Fi 133 - Wil-Fi 133 - Wil-Fi 134 - Wilan 135 - YouTr | motion Switc View Fittin SoundS am Trace FingAu Frome L SoundS Manual De Edito De Trimm Service DaperBa able Ma De Callii i Direc i Callii J Direc i Tips Test (W ube (Yo kby\" v | editor h Agent (Smarth gServic r (Sour ervice ing (Tr tomatic ibrary (USBSe (WebMa r (Vide er (Vid (vsims ckup (W nager 1) ather S ng (Uni t (Alls (WifiGu lanTest uTube)) oice wa | <pre>(Slow (Smar dirrori ce (Smar dirrori ce (Split (Split (Split (Split (Split (Split (Split)) (Split (Split)) coEdito deoTrim service vallpap (Stall) SeP11.0 (FiedWF) shareFi ider) (Split)</pre> | MotionV tSwitch ng) rtFitti r) SoundSe heringA rromeLib) rrLite D mmer)) erBacku er (Gea) C) leShare | ideoEdit Agent) ngServic rvice) utomatic rary) ream N) p) rManager) | cor BGM ce) on) | ₽rovide | F) |
| An error w To uninstal 23" x - Back te r - Refresh 0 - Exit [CHOICE]: 64 Uninstalling t) App Label: App Dir: /j Proceed? < | o Menu h list 69 g Knox com.se system/ (v)es | cted wh iple ap Enrolls c.enter app/Uni | nile de ops, en nent Se rprise. (versal | rvice (knox.cl MDMClie | system tiple nu ==== /system/ oudmdm.s nt | apps. mbers. 'app/Ur mdms | Exampl | e: "1 11 MDMClien |
| (T) | - | | 1 | GIF | | | | |
| | 9 | | | | ē | | ** | |
| 1 2 | 3 | 4 | 5 | 5 6 | 7 | 8 | 9 | 0 |
| 1 2 q w | 9 3 1 e | 4 1 | - 5 t | 5 6 ; y | 9 7 u | 8 i | 9 0 | 0 p |
| 1 2 q w a | 9 3 7 8 | 4 r d | - 5 t | 5 6 : y g | و 7 u h | 8 i j | 9 0 k | 0 p |
| 1 2 q w a | 3 2 3 7 e 5 z | d x | f c | 5 6 ; y g v | و 7 u h b | 8 j n | 9 0 k m | 0 p l |
| 1 2 q w a • | 3 7 e 5 7 | d x | f c | g glish (U | 0 7 4 h b | 8 j n | 9 0 k m | 0 p I |

Εικόνα 77 - Uninstalling Knox Apps 1



Εικόνα 78 - Uninstalling Knox Apps 2

| | | | - 0 | | | | | | | | | | - | | all I | |
|---|--|---|---|--|---|--|---|--|--|--|-------------|--------|------------|--------------|-------|--------|
| | Win | Idov | w 1 | | | | | | | | Ð | | > | < | | : |
| 177 179 180 18 18 18 18 18 18 18 18 18 18 18 18 18 | 7 - S1 8 - S1 9 - S1 2 - S1 2 - S1 2 - S1 3 - S5 3 - Ti 6 - Ti 7 - Tj 8 - Uj 9 - Ti 7 - Tj 8 - Uj 9 - S1 4 - Tj 3 - S5 3 - Ti 5 - Vi 6 - Vi 9 - Vi 1 - Vi | ticke torag torag toryS tw/Scr VC Ag ystem ADowr ags (ime 2 ips (IBCVii ofay ser D ideo pnDia allpa allpa allpa allpa allpa allpa allpa bork S ork p ork S | erCe ge b ge M Serv. ript gent MUB MUB MUB MUB MUB Cone Tip irtu (Upp Cone Tip irtu (Upp Cone Tip irtu (Upp Cone Tip Firtu Serv. Serv. Tag Sone Tip Serv. Se | nter oostd anag ice Play (SV der) Upd s) alSo day) ional ss (V ser -res (Cropp ss (D w (S ser -res (D) p (M | (St er () (Sto er () CAgee 2 (S (TAD ater ftke (Sam pnDi Vice (Wa prDi vice (Wa promotion (Con anaggampan | icke Memo Stor rySe SuwS nt) (Sa (Sa y (U User (Sa g (D User (Val Room ngSo (Val (Wal (Wal (Wal Room ngSo (C) (Sa (Sa () (Sa () (Sa () (Sa () (Sa () (Sa () (Sa () (Sa () (Sa () (Sa () (Sa () (Sa () (Sa () (Sa () (Sa () (Sa () (Sa ()) (Sa () (Sa ()) (Sa ()) (Sa ()) (Sa ()) (Sa ()) (Sa ()) (Sa ()) (Sa ()) (Sa ()) (Sa ()) (Sa ()) (Sa ()) (Sa ()) (Sa ()) (Sa ()) (Sa ()) (Sa ()) (Sa ()) (Sa ()) (Sa (Sa ()) (Sa ()) (Sa ()) (Sa ()) (Sa ()) | rCen rySa ageW rvic crip mUIB oade msun IBCV Dict Vide s) ynam per- lpap) cial erAg ovis (You | tter) lanag (e) ttPla itxby. r) gTim 'irtu iona oPla icto ertr) eent3 ionii rPho |) Ref er) ver) 2) alSof ver) ckscr ver) ckscr opper | Upda tkey vide een)) ub) | | | | | | |
| To 14 | unin: | stall | . mui | | | | | | | | | | | mpl | | |
| r | - Refr - Exit | resh | lis | | | | | | | | | | | | | |
| [CHI Unin sage | OICE]: nstall ent) | : 99 ling | 100 Knot | 101 k Ani | 102 alyt | | | | (/s) | stem | /pr | v- | app/i | nox | ana | lytic |
| App | p Labe | el: c | | | | | | | | | | | | | | |
| App Pro | oceed | /sy < (| y)e: | samsi m/pr: s i | ung. iv-a (n)o | andr pp/k | oid. noxa a)ll | knox naly >: | anal | ytic | s.u | olo | ader | | | |
| App Pro | oceed | /59 | (y)e | samsı n/pr; s i | iv-a (n)o | andr pp/k (| oid. noxa a)11 | knox naly >: | anal ticsa | ytic gent | s.u | 210 | ader SÇ | ••• | | |
| App Pro | (t) | 2 2 | (y)e | sams n/pr s 1 | (n)o | andr pp/k (| oid. noxa a)11 | knox naly >: GIF | anal ticsa | ytic gent | s.u | 8 | ader K | 9 | | • |
| App Pro | (t) 1 9 | 2 W | Ster (y)e | 3 e | | andr pp/k 1 C | 5 t | knox naly >: ; | 6 y | ytic gent 7 U | 5.u | 8 | ader S | \$ 9 0 | | 0 p |
| App Pro | reed (†) 1 q a | 2 W | stee sy)er | 3 e | (n)o (n)o (n)o (n)o | ndr pp/k l l l f | oid. noxa a)11 | knox naly >: g | ana) ticsa 6 y | ytic gent 7 U | у. | 8 i | sder S | 9 | | 0 P |
| App Prc | cceed () 1 q a | 2 w | s S Z | 3 e | ung iv-a (n)o 4 r d d | f | oid. noxa a)11 | knox naly 2: GF g | ana) ticsa d f f t t t | ytic gent 7 U |) j n | 8 i | sder ¢ | 9 | 1 | 0 p |
| | occedi (†) 1 q a ↑ !#1 | 2 W | s s z | 3 e | d x | f | 5 t | knox naly >: g y ish (| 6 y Lusy | ytic gent 7 u | j n | 8 i | k k | 9 | - | 0 p |

Εικόνα 79 - Uninstalling Knox Apps 3



Εικόνα 80 - Uninstalling Knox Apps 4

Όταν τελειώσουμε με την απεγκατάσταση των εφαρμογών το Debloater θα μας προτείνει να κάνουμε reboot την συσκευή (Εικόνα 81, Εικόνα 82) για να γίνουν οι αλλαγές. Πραγματοποιούμε το reboot της συσκευής.

| 00:27 🖬 🖬 | | | | 10 |
|--|--|--|-----------------|--------------------|
| Window 1 🔻 | | \oplus | × | : |
| 154 - Secure Wi-Fi (Fast) 155 - SelFactoryAp (SBE 157 - Seplate app cound 158 - Service and sup cound 158 - Service and RL (M 159 - Settings (SecSettin 160 - Settings (SecSettin 161 - Settings (SecSettin 162 - SettingsHoby (Set 163 - SaretSorageBackp 164 - SNMSgentService (Sec 165 - Saret Call (Smar Ca 167 - Saret SuthAmerican 168 - Saret Sorage Banager (St 179 - Sortsare update (Ga 170 - Sortsare update (Ga 170 - Sortsare update (Ga 170 - Saret SuthAmerican 173 - StickerCenter (Stic 175 - Saret SuthAmerican 174 - Storage Banager (St 175 - Saret SuthAmerican 175 - Storage Banager (St 176 - Sortsare Updater (St 177 - SuckerCenter (Stic 178 - Storage Banager (St 178 - Storage Banager (St 179 - St 189 - Wollpaper services) 180 - Wollpaper services) 191 - Wollpaper (St 193 - Wollpaper (St 193 - Wollpaper (St 193 - Wollpaper (St 194 - Wollpaper (St 194 - Wollpaper (St 195 - Wollpaper (St 194 - Wollpaper (St 195 - Wol | actory/wpg) (MulliSchudderti (MulliSchudderti (Schuddakap FF) odemServiceMode) (F) (SharedStorageE (MSAgent) (SharedStorageE (MSAgent) (SharedStorageE (SharetStrictAd Manager) (F) (SharedStorageE (SharetStrictAd Manager) (F) (SharetStrictAd Manager) (F) (SharetStrictAd Manager) (SharetStrictAd (SharetStrictAd Manager) (SharetStrictAd (UBCVirtualSoft erOidLawer) (SharetStrictAd (UBCVirtualSoft erOidLawer) (SharetStrictAd (SharetS | ng) itelligenci issistant) pdater) key) ider) ien) b) station itiongent tiongent talled | •) , Example | : *1 16 riv-app |
| Tap here to fill entire screen | | | | |
| III | 0 | | < | |

Εικόνα 81 - Uninstalling Knox Apps 5



Εικόνα 82 - Uninstalling Knox Apps 6
Στην συνέχεια από τα Settings της συσκευής επιλέγουμε Apps και ενεργοποιούμε την επιλογή Show System Apps. Πραγματοποιούμε αναζήτηση για Knox και βλέπουμε ότι δεν υπάρχει πλέον στην συσκευή καμία εφαρμογή του Knox (Εικόνα 83), άρα απεγκαταστήσαμε επιτυχώς όλες τις εφαρμογές του Knox από την συσκευή.

| 17:43 | | NE 🖘 🔐 🛔 |
|--------|-------------------|----------|
| < knox | 4 | ×: |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | No results found. | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| 111 | 0 | < |

Εικόνα 83 - Knox No Results Found

4. LOGICAL ANALYSIS

4.1 AFLOGICAL

Η ανάλυση σε logical επίπεδο προϋποθέτει την σύνδεση της συσκευής με τον υπολογιστή, συνήθως με τη χρήση ενός usb καλωδίου. Ο υπολογιστής αναλαμβάνει να στείλει τις ανάλογες εντολές ώστε ο επεξεργαστής της συσκευής να του παρέχει τα δεδομένα που ζήτησε (Bommisetty, et al., 2014).

Στο Santoku υπάρχει η εφαρμογή AFLogical OSE που παρέχει την συγκεκριμένη δυνατότητα. Δίνοντας την εντολή aflogical-ose (Εικόνα 84) (Hoog, 2013) ένα apk δημιουργείται με όνομα AFLogical OSE (Εικόνα 85), το οποίο στη συνέχεια αποστέλλεται στη συσκευή και εγκαθίσταται.

\$ aflogical-ose -h run 'aflogical-ose' with usb debugging enabled in your android device santoku@santoku-virtual-machine:~\$ aflogical-ose Make sure android device is connected to USB [sudo] password for santoku: 691 KB/s (28794 bytes in 0.040s) Success Starting: Intent { cmp=com.viaforensics.android.aflogical ose/com.viaforensics.a ndroid.ForensicsActivity } Press enter to pull /sdcard/forensics into ~/aflogical-data/ pull: building file list... pull: /sdcard/forensics/20201208.0111/info.xml -> /home/santoku/aflogical-data/2 0201208.0111/info.xml pull: /sdcard/forensics/20201208.0111/Contacts Phones.csv -> /home/santoku/aflog ical-data/20201208.0111/Contacts Phones.csv pull: /sdcard/forensics/20201208.0111/CallLog Calls.csv -> /home/santoku/aflogic al-data/20201208.0111/CallLog Calls.csv pull: /sdcard/forensics/20201208.0111/MMSParts.csv -> /home/santoku/aflogical-da

Εικόνα 84 - aflogical-ose terminal



Εικόνα 85 - AFLogical OSE App

Αξίζει να σημειωθεί ότι το συγκεκριμένο apk έχει αναπτυχθεί για παλαιότερες εκδόσεις android (Εικόνα 86) και δεν έχει πραγματοποιηθεί κάποιο update που να αφορά στα android 10. Παρόλα αυτά όμως δίνει αποτελέσματα και σε android 10 συσκευές.

| 01:37 🖼 | | | N 🖘 🖻 |
|--|--------------------------------|--------------------------------------|----------------------------|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| AFLogical OSE | | | |
| This app was built fo Android and may not checking for updates | r an old work p , or cor | ler version roperly. Thact the | on of Try developer. |
| Check for upda | ate | ţ. | ок |
| III | 0 | | < |

Εικόνα 86 - AFLogical OSE App Message

Μετά την εγκατάστασή της, η εφαρμογή ξεκινάει αυτόματα και εφόσον πατήσουμε την επιλογή Capture (Εικόνα 87), τα δεδομένα που επιθυμούμε συλλέγονται και μεταφέρονται στο Santoku.

| 01:37 🖿 | | | ¥ 🖘 🗉 🛙 |
|----------------------|----------------|--------------|---------|
| AFLogical OSE | _ | _ | |
| Available providers: | | | |
| CallLog Call | S | | |
| Contacts Ph | iones | | |
| MMS | | | |
| MMSParts | | | |
| SMS | | | |
| | | | |
| | Select All | Deselect All | Capture |
| Тар | here to fill e | ntire screen | |
| 111 | Ο | < | |

Εικόνα 87 - AFLogical OSE App Menu

Μετά την ολοκλήρωση της διαδικασίας μπορούμε να δούμε τα δεδομένα που συλλέξαμε, τα οποία είναι σε μορφή csv (Εικόνα 88), με την χρήση οποιουδήποτε προγράμματος spreadsheet.

| 1 | | | | 11 | |
|-------|---|---|---|----|--|
| 1.00 | _ | _ | - | ы | |
| 1.000 | _ | _ | - | | |
| 100 | _ | _ | - | | |
| 1.00 | _ | _ | - | | |
| | - | - | - | 1 | |
| | | | | | |

| . 1 | _ | |
|-----|---|--|
| | _ | |
| | _ | |
| | - | |
| | - | |
| | - | |



| Con | tacts |
|------|--------|
| Phon | es.csv |

| | - | - | |
|----|----|-----|----|
| in | fo | .XI | ml |



MMS.csv

| _ | |
|---|--|
| _ | |
| _ | |

| - 11 | | | |
|------|---|---|-----|
| | | | |
| - 1 | | | = 1 |
| - 1 | | _ | = 1 |
| - 1 | - | | = 1 |

MMSParts.cs SMS.csv v

| Εικόνα | 88 - | Collected | Files |
|--------|------|-----------|--------------|
| | | | |

Μπορούμε να διαβάσουμε τις κλήσεις από και προς τον χρήστη της συσκευής (Εικόνα 89) αλλά και τα μηνύματα που έχει λάβει και έχει στείλει ο

χρήστης (Εικόνα 90, Εικόνα 91). Μεταξύ άλλων βλέπουμε την ημερομηνία και την ώρα, καθώς και τη διάρκεια της κάθε κλήσης, αλλά και το όνομα με το οποίο είναι αποθηκευμένη η κάθε επαφή στη συσκευή.

| B | | | CallLog Cal | ls.csv - G | inumeric | | | |
|--------|-------------|--------------|---------------------|------------|-------------|------------|--------------------|---------|
| File E | dit View | Insert Forma | at Tools Statistics | Data He | lp | | | |
| + | ΰŏ | 凸 曲 | | < | ~ · | 1 | $\sum f(x)$ | :U :A |
| Sans | 10 a | <u>a a</u> | | | == 5 | % | • \$.0 | |
| | 0 | \ <u> </u> | e ok | | | Ĩ | | |
| | | | | | | <u>لله</u> | | |
| AT | V | × ^ | | V | v - | V | v - | × > |
| | A | В | C | D | E | F | G | н |
| 1 | Id | number | date | duration | type | new | name | numbert |
| 2 | 24 | 306946 | 1607301005434 | 0 | 5 | 1 | Dimitra | 2 |
| 3 | 21 | 6946 | 1607296002326 | 0 | 2 | 1 | Semina | 2 |
| 4 | 20 | 302109 | 1607295238125 | 36 | 2 | 1 | Home | 2 |
| 5 | 18 | 302109 | 1607295204988 | 0 | 5 | 1 | Home | 2 |
| 6 | 17 | 6946 | 1607294489990 | 81 | 2 | 1 | Dimitra | 2 |
| 7 | 16 | 6946 | 1607292755871 | 0 | 2 | 1 | Dimitra | 2 |
| 8 | 15 | 6946 | 1607291576456 | 4 | 2 | 1 | Semina | 2 |
| 9 | 8 | 6940 | 1607290146600 | 0 | 2 | 1 | Theodor | 2 |
| 10 | 7 | 6946 | 1607290118060 | 11 | 2 | 1 | Dimitra | 2 |
| 11 | 6 | 6946 | 1607290105423 | 0 | 2 | 1 | Semina | 2 |
| 12 | 5 | 6946 | 1607290094999 | 0 | 2 | 1 | Semina | 2 |
| 13 | 4 | 302109 | 1607290075494 | 5 | 2 | 1 | Home | 2 |
| 14 | 3 | 302109 | 1607290066193 | 1 | 1 | 1 | Home | 2 |

Εικόνα 89 - Call Logs File

| E | | | | SMS.csv | - Gnumeric | | |
|---|---|--|---|------------|--|--|--|
| File | Edit View | Insert F | ormat Tools | Statistics | Data Help | | |
| + | ΰŏ | 也 (| <u>事 口 (</u> | Ì | $\langle \cdot \rangle \rightarrow \cdot$ | | <i>f(x)</i> |
| Sans | s 10 a | a | | : = | = == 🧐 | 1 % . | ₽ .0 |
| | • | 12 | ° 9 (0 | ОК | | | |
| A1 | | r | x ~ - | = _id | | | |
| | | | | | | | |
| | A) | В | С | D | E | F | |
| 1 | A id | B thread_ic | C address | D | E date | F date_sent | |
| 1 2 | A id 10 | B thread_ic 10 | C address | D | E date 1607549799461 | F date_sent 1607549799 | 9000 |
| 1 2 3 | A id 10 9 | B thread_ic 10 6 | C address 302109 | D | E date 1607549799461 1607549794758 | F date_sent 1607549799 1607549794 | 0000 |
| 1 2 3 4 | A id 10 9 8 | B thread_ic 10 6 5 | C address 302109 306946 | D | E date 1607549799461 1607549794758 1607387574332 | F date_sent 1607549799 1607549794 1607387573 | 0000 0000 0000 |
| 1 2 3 4 5 | A id 10 9 8 7 | B thread_ic 10 6 5 3 | C address 302109 306946 306946 | D | E date 1607549799461 1607549794758 1607387574332 1607387541721 | F date_sent 1607549799 1607549794 1607387573 1607387540 | 0000 0000 0000 |
| 1 2 3 4 5 6 | A id 10 9 8 7 6 | B thread_ic 10 6 5 3 8 | C address 302109 306946 306946 Google | D | E date 1607549799461 1607549794758 1607387574332 1607387541721 1607384728935 | F date_sent 1607549799 1607549794 1607387573 1607387540 1607377523 | 0000 0000 0000 0000 7000 |
| 1 2 3 4 5 6 7 | A id 10 9 8 7 6 5 | B thread_ic 10 6 5 3 8 3 | C address 302105 306946 306946 Google 306946 | D | E date 1607549799461 1607549794758 1607387574332 1607387541721 1607384728935 1607383063018 | F date_sent 1607549799 1607549794 1607387573 1607387540 1607377523 1607383062 | 9000 4000 8000 9000 7000 2000 |
| 1 2 3 4 5 6 7 8 | A id 10 9 8 7 6 5 4 | B thread_ic 10 6 5 3 8 3 7 | C address 302105 306946 306946 Google 306946 SAMSU | D | E date 1607549799461 1607549794758 1607387574332 1607387541721 1607384728935 1607383063018 1607381718796 | F date_sent 1607549799 1607549799 1607387573 1607387540 1607377527 1607383062 1607374518 | 0000 0000 0000 0000 0000 0000 0000 0000 0000 |
| 1 2 3 4 5 6 7 8 9 | A id 10 9 8 7 6 5 4 3 | B thread_ic 10 6 5 3 8 3 7 3 | C address 302105 306946 306946 Google 306946 SAMSU 306946 | D | E date 1607549799461 1607549794758 1607387574332 1607387541721 1607384728935 1607383063018 1607381718796 1607301013967 | F date_sent 1607549799 1607549799 1607387573 1607387540 1607377523 1607383062 1607374518 1607301013 | 0000 0000 0000 0000 0000 0000 0000 0000 0000 |
| 1 2 3 4 5 6 7 8 9 10 | A id 10 9 8 7 6 5 4 3 2 | B thread_ic 10 6 5 3 8 3 7 3 6 | C address 302105 306946 306946 Google 306946 SAMSU 306946 302105 | D | E date 1607549799461 1607549794758 1607387574332 1607387541721 1607384728935 1607383063018 1607381718796 1607301013967 1607295217255 | F date_sent 1607549799 1607549799 1607387573 1607387540 1607377523 1607383062 1607374518 1607301013 1607295216 | 9000 9000 9000 9000 9000 9000 8000 8000 |

Εικόνα 90 - SMS File 1

| E | | | *SMS.cs | v - Gnumeric | | | |
|--------|-----------|----------|-------------------------|------------------|--------|-----------|--------|
| File E | Edit View | Insert F | Format Tools Statistics | Data Help | | | |
| + | ÔŎ | டி | ≞ ∩ ∩ ≘ | (~ · ~) · | ۵ 🔊 | f(x) | 1 :1 |
| Sans | 10 a | a | | - = = • | % · | ÷ | .00 |
| | 0 | | ° • • • | | 1 | | |
| _ | - L | | U | | Ш | | |
| A1 | | * | × | | | | |
| - | K | L | M | N | 0 | P | Q |
| 1 | reply_pa | subject | body | service_center | locked | error_coo | sub_id |
| 2 | 0 | | EXETE NEA HXHTIKA MH | 3069 | 0 | -1 | 1 |
| 3 | 0 | | ΔΩΡΕΑΝ ΕΝΗΜΕΡΩΣΗ: ΕΙ | 3069 | 0 | -1 | 1 |
| 4 | 0 | | Hi how r u? | 3069 | 0 | -1 | 1 |
| 5 | 0 | | ΣΕΜΙΝΑ ΜΗΠΩΣ ΠΡΕΠΕΙ Ι | 3069 | 0 | -1 | 1 |
| 6 | 0 | | G-811950 is your Google | 34607001 | 0 | -1 | 1 |
| 7 | 0 | | ΓΕΙΑ ΣΟΥ ΣΕΜΙΝΑ. | 3069 | 0 | -1 | 1 |
| 8 | 0 | | <#> Account: 323813 is | 3460700 | 0 | -1 | 1 |
| 9 | 0 | | ΔΩΡΕΑΝ ΕΝΗΜΕΡΩΣΗ: ΕΙ | 3069 | 0 | -1 | 1 |
| 10 | 0 | | ΔΩΡΕΑΝ ΕΝΗΜΕΡΩΣΗ: ΕΙ | 3069 | 0 | -1 | 1 |
| 11 | 0 | | ΤΑ ΔΩΡΑΚΙΑ ΤΟΥ ΜΗΝΑ! | 3069 | 0 | -1 | 1 |

Εικόνα 91 - SMS File 2

Στο αρχείο μηνυμάτων παρατηρούμε ότι το apk έχει καταφέρει να τραβήξει και το imsi της κάρτας sim της κινητής συσκευής (Εικόνα 92).

| E | | | | | , | SM | S.cs | v - G | nume | ric |
|------|-------------|--------|----------|--------------|----------|------|------|-------|-------|-----|
| File | Edit View | Insert | For | mat To | ols SI | atis | tics | Data | Help | |
| + | ΰŏ | டு | ≞ | | Ô | |) | \$ | • • | > |
| Sans | 10 a | а | <u>a</u> | ≣ | ≞ | ≣ | +a- | 9 🗆 | | 3 |
| | | 1 | 2 | 9 | • • | ٢. | A I | | | |
| A1 | | \$ | × | \checkmark | v | = (| _id | | | |
| | U | | V | |) V | / | | X | Y | |
| 1 | sim_slot | sim_im | si | | hidd | en | grou | up_id | group | ty |
| 2 | 0 | 202052 | 9 | | | 0 | | | | |
| 3 | 0 | 202052 | | | | 0 | | | | |
| 4 | 0 | 202052 | | | | 0 | | | | |
| 5 | 0 | 202052 | | | | 0 | | | | |
| 6 | 0 | 202052 | | | | 0 | | | | |
| 7 | 0 | 202052 | | | | 0 | | | | |
| 8 | 0 | 202052 | | | | 0 | | | | |
| 9 | 0 | 202052 | | | | 0 | | | | |
| 10 | 0 | 202052 | | | | 0 | | | | |
| 11 | 0 | 202052 | 9 | | . | 0 | | | | |
| 12 | 4 | | | | _ | | | | | |
| 14 | | | | | 1 | | | | | |

Εικόνα 92 - SMS File 3 - IMSI

Παρόλο που έχουμε δώσει τα κατάλληλα permissions στην εφαρμογή των επαφών παρατηρούμε ότι το AFLogical OSE δεν κατάφερε να τραβήξει τις επαφές που υπάρχουν στην συσκευή (Εικόνα 93).

| E | | Cor | ntacts P | hones.cs | v - Gnu | meric | | - | + × |
|----------------------------------|-----------------|---------------------|----------------------|---------------|---------------------|-------------------------|---|-----------|------|
| File | Edit View | Insert F | ormat To | ools Stat | istics D | ata Help | | | |
| + | ΰů | <u>ط</u> و | <u> </u> 上 に | | | 5 T / | ⇒ • (| δ | • |
| Sans | 10 a | a | ₫ 📄 | ≡ ₹ | +a+ | | | % · | * |
| | •• | 1 | ° 🗹 | • ок | | | Recta | | |
| | | | | | | | | | |
| A1 | | \$ | x v | * = | phone | tic_name | | | |
| A1 | A | ک B | × ✓ | * = | phone | tic_name | G | H | |
| A1 | A phonetic | ₽ B last_time | C send_to | D custom_r | phone E notes | etic_name F label | G display_r | H type | ispr |
| A1 | A phonetic | ₽ B last_time | X ✓ C send_to_ | D custom_r | Phone E notes | etic_name F label | G display_r | H type | ispr |
| A1 | A phonetic | ▶ B last_time | C send_to_ | D custom_r | Phone E notes | etic_name F label | G display_r | H type | ispr |
| A1 | A [phonetic] | ↓ B last_time | X ✓ C send_to_ | D custom_r | E notes | etic_name F label | G display_r | Н type | ispr |
| A1 1 2 3 4 5 | A [phonetic] | ₹ B last_time | C Send_to_ | D custom_r | Phone E notes | F label | G display_r | Н type | ispr |
| A1 1 2 3 4 5 6 | A [phonetic] | ↓ B last_time | C Send_to_ | D Custom_r | Phone E notes | Etic_name F label | G display_r | н type | ispr |

Εικόνα 93 - Contacts File Empty

Από την εφαρμογή των επαφών στην συσκευή και το μενού επιλογών μπορούμε να πάμε στην επιλογή Manage contacts-> Import or export contacts (Εικόνα 94).



Εικόνα 94 - Manage Contacts Menu

 1438
 1

 Import or export contacts

 Import contacts

 Import contacts from your SIM card or vCard files.

 Export contacts to your SIM card or vCard files.

 Export contacts to your SIM card or vCard files.

 Import

Επιλέγουμε export (Εικόνα 95).

Εικόνα 95 - Import or Export Contacts

Επιλέγουμε το internal storage για να κάνουμε export το αρχείο των επαφών (Εικόνα 96, Εικόνα 97, Εικόνα 98).

| 14:40 | ⊑ <u>†</u> <u>†</u> • | | S |
|-------|-----------------------|------------|----------------|
| < | Export conta | acts | |
| Ste | p 1 of 2 | | 0 |
| Sele | ct where to ex | portitiese | o contacts to. |
| | 8 contacts | > | То |
| 0 | Internal sto | orage | |
| 0 | SD card | | |
| 0 | SIM 1 | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | Export | |
| | Ш | 0 | < |

Εικόνα 96 - Internal Storage Export 1/2

| | 14:40 🖬 ± ± • 😪 al 🛔 |
|----|--|
| | < Export contacts |
| | Step 2 of 2 |
| | Contacts_005.vcf will be exported to your internal storage. Tap Export to start. |
| | (B contacts) > |
| | Internal storage |
| | ○ SD card |
| | O SIM 1 |
| | |
| | Export |
| | |
| Eu | κόνα 97 - Internal Storage Export 2/2 |
| | 14:41 호교 호 · · · · · · · · · · · · · · · · · |
| | < Export contacts |
| | Contacts exported Contacts_005.vcf has been exported to your internal storage. |
| | (8 contacts) > |
| | |
| | ОК |
| | |

Εικόνα 98 - Contacts Exported

Στην συνέχεια από το internal storage της συσκευής επιλέγουμε το αρχείο που κάναμε export και επιλέγουμε move για να μετακινήσουμε το αρχείο εντός του φακέλου forensics (Εικόνα 99, Εικόνα 100, Εικόνα 101).

Ο φάκελος forensics έχει δημιουργηθεί από το apk AFLogical OSE στην συσκευή.



Εικόνα 99 - Internal Storage File Selection



Εικόνα 100 - Move File to Forensics Folder



Εικόνα 101 - Forensics Folder Internal Storage

Χρησιμοποιώντας πάλι την εφαρμογή AFLogical OSE από το Santoku με τον ίδιο τρόπο που αναφέρθηκε προηγουμένως, η εφαρμογή θα τραβήξει και το αρχείο με τις επαφές που κάναμε export από την εφαρμογή των επαφών (Εικόνα 102,Εικόνα 103).



Εικόνα 102 - Collected Files with Contacts File



Εικόνα 103 - Exported Contacts File

4.2 FONEPAW

Logical analysis μας παρέχει και το πρόγραμμα FonePaw, έχουμε χρησιμοποιήσει την free trial version που παρέχεται για διάρκεια 30 ημερών.

Ανοίγοντας το πρόγραμμα επιλέγουμε Android Data Recovery (Εικόνα 104).



Εικόνα 104 - FonePaw - Android Data Recovery

Στο μήνυμα που εμφανίζεται στην συσκευή επιλέγουμε Allow (Εικόνα 105).



Εικόνα 105 - Allow USB Debugging Message

Στην συνέχεια το FonePaw μας αφήνει να επιλέξουμε τα δεδομένα που θέλουμε να ανακτήσουμε από την συσκευή (Εικόνα 106).

Παρατηρούμε ότι το συγκεκριμένο πρόγραμμα μας δίνει περισσότερες επιλογές ανάκτησης δεδομένων σε logical επίπεδο καθώς μας αφήνει να ανακτήσουμε και εικόνες, βίντεο και αρχεία που υπάρχουν στην συσκευή και δεδομένα από την εφαρμογή what's up αν υπάρχει στην συσκευή, στην προκειμένη περίπτωση εφαρμογή what's up δεν έχει εγκατασταθεί στην συσκευή. Πατάμε Next για να πραγματοποιήσει το πρόγραμμα το logical level extraction (Εικόνα 106, Εικόνα 107).

| FonePav | | | 👻 s 🗹 🖳 🖓 | - 🖻 |
|--------------------------------------|---|--|--------------------------|--------------------------------------|
| ← Back | | | the "Next " button | |
| | Please choose the file typ | pes you want to recover and then click t | the "Next" button. | |
| | Contacts & Message | es | | |
| | 🗹 👤 Contacts | 🗹 🧮 Messages | 🗹 🧭 Message Attachments | |
| | 🗹 🔇 Call Logs | 🗹 💽 WhatsApp | 🗹 💊 WhatsApp Attachments | |
| | 🗹 Media | | | |
| | 🗹 🎦 Gallery | 🗹 🞯 Picture Library | 🗹 附 Videos | |
| | 🗹 🌏 Audio | 🗹 🧮 Documents | | |
| | ☑ Select All | | | |
| | | | | |
| | Εικο | όνα 106 - Choose Files to Recov | er | |
| FonePav | EtKo v - Android Data Recovery (Unr | óvα 106 - Choose Files to Recov registered) | er 🕱 성 f 💐 📼 - | : |
| ► FonePav | ELK(v - Android Data Recovery (Unr | óvα 106 - Choose Files to Recov registered) | er 〒 & 王 루 . | : |
| n FonePav ← Back | ELK(w - Android Data Recovery (Unr | óνα 106 - Choose Files to Recov registered) | er 🐂 등 💽 🗟 🖂 😁 | : |
| ■ FonePav | ELKO | óvα 106 - Choose Files to Recov ^{registered}) | er 🐂 등 ք 🗟 📼 - | - • : |
| FonePav Back | EtK(| <mark>óvα 106 - Choose Files to Recov</mark> registered) Checking device information completed. | er 🐂 ් f 🖪 📼 - | • |
| ■ FonePav | ELKO | <mark>óνα 106 - Choose Files to Recov</mark> registered) Checking device information completed. | er 🐂 & 🗊 🗣 💬 - | • |
| r FoncPav | EtKr | <mark>óνα 106 - Choose Files to Recov</mark> registered) Checking device information completed. Getting ready for scanning device | er 👿 6 💽 🖓 📼 | ■ : ■ : |
| r FoncPav - Back | EtKe | όνα 106 - Choose Files to Recov registered) Checking device information completed. Getting ready for scanning device | er 🐂 ő f ঝ 🚥 - | • • |
| r FonePav ← Back | ELK | όνα 106 - Choose Files to Recov registered) Checking device information completed. Getting ready for scanning device | er | • • |
| ■ FonePav | Etke | όνα 106 - Choose Files to Recov registered) Checking device information completed. Getting ready for scanning device | er | ■ |
| ■ FonePav | Eux • - Android Data Recovery (Unit SAMSUNG (SM-A705FN) | by α 106 - Choose Files to Recov registered) Checking device information completed. Getting ready for scanning device | er | • • |
| ■ FonePav | t - Android Data Recovery (Uni Time Samsung (SM-A705FN) | όνα 106 - Choose Files to Recov registered) Checking device information completed. Getting ready for scanning device | er | ■ |
| FonePav ← Back | Etke • Android Data Recovery (Uni SAMSUNG (SM-A705FN) | όνα 106 - Choose Files to Recov registered) Checking device information completed. Getting ready for scanning device | er | ■ |

Εικόνα 107 - File Recovery Process

Το πρόγραμμα έχει καταφέρει να αναγνωρίσει σωστά το μοντέλο της συσκευής (Εικόνα 108) και κάτω από αυτό μας εμφανίζει αθροιστικά για κάθε κατηγορία όλα τα δεδομένα που κατάφερε να ανακτήσει (Εικόνα 109).





| 🟫 FonePaw - Android Data Recovery (Unregistered) | | | | 🗑 ő f 🔍 🖂 🗕 🗆 🗙 |
|--|---------------|---------------------------------|-------|------------------|
| Scanning device, please wa | it | 34% | | Pause Stop |
| 🗹 📋 SAMSUNG (SM-A705FN) | ☑ Name | | Email | Dimitra |
| Contacts & Messages | 🗹 Dimitra | 69462 | | |
| Contacts (15) | 🗹 Dimitra | 694628 | | |
| Messages (8) | 🗹 Home | +3021 | | |
| Message Attachments (0) | ✓ Home | +3021 | | Phone 6946 |
| WhatsApp (0) | 🗹 Mariatzela | 698371 | | Produce Ophics |
| 🔲 🔕 WhatsApp Ahments (0) | Mariatzela | 69837 | | |
| Media | Semina | 69460 | | · |
| 🗹 🎽 Gallery (209) | Semina | 69460 | | |
| Picture Library (0) | | 69467 | | |
| Videos (0) | | 69467 | | |
| Documents (0) | | 10000 | | |
| | | 13830 | | |
| | ΕΞΥΠΗΡΕΤΗΣΗ Π | 13830 | | |
| | | Total: 254 item/s) 116 64 MB | | |
| ← Back | | selected: 254 item(s) 116,64 MB | | Q Recover |

Εικόνα 109 - FonePaw Collected Evidence 2

| fonePaw - Android Data | 🗑 5 f 🖳 🖂 🗕 🗆 🗙 | | |
|--------------------------|---------------------|---|------------------|
| SAMSUNG (SM-A705FN) | OFF Only display th | e deleted item(s) | Q Search |
| Contacts & Messages | ✓ Name | Phone Email | Dimitra |
| 🗹 👤 Contacts (15) | 🗹 Dimitra | 69462 | |
| Messages (8) | 🗹 Dimitra | 69462 | |
| Call Logs (22) | Home | +302 | |
| 🔲 💽 WhatsApp (0) | Home | +302 | Phone 69452 |
| 🔲 💿 WhatsApp Ahments (0) | Mariatzela | 69837 | |
| Media | 🗹 Mariatzela | 69837 | |
| Gallery (209) | Semina | 69460 | - |
| Videos (5) | Semina | 69460 | |
| 🗹 🌏 Audio (2) | ☑ Theodor | 69467 | |
| 🗹 🧮 Documents (25) | ☑ Theodor | 69467 | |
| | 🗹 ΕΞΥΠΗΡΕΤΗΣΗ Π | 13830 | |
| | 🗹 ΕΞΥΠΗΡΕΤΗΣΗ Π | 13830 | - |
| | ПЛНР.ТНЛЕФ.КАТ | 11833 | |
| | _ | | Ŧ |
| ← Back | | Total: 1802 item(s) 363,96 MB selected: 1802 item(s) 363,96 MB | Q Recover |

Εικόνα 110 - FonePaw - Contacts 1

To FonePaw κατάφερε να ανακτήσει επιτυχώς τις επαφές που υπάρχουν στην συσκευή με όνομα επαφής και νούμερο (Εικόνα 110,Εικόνα 111).

| fonePaw - Android Data | Recovery (Unregiste | red) |
|--------------------------------------|----------------------|-------------------|
| 🗹 📋 SAMSUNG (SM-A705FN) | OFF Only display the | e deleted item(s) |
| Contacts & Messages | ✓ Name | Phone |
| Contacts (15) | 🗹 Dimitra | 694628 |
| Messages (8) Message Attachments (0) | 🗹 Dimitra | 694628 |
| Call Logs (22) | ☑ Home | +30210 |
| 🔲 💽 WhatsApp (0) | ☑ Home | +30210 |
| 🔲 💊 WhatsApp Ahments (0) | 🗹 Mariatzela | 698371 |
| Media | 🗹 Mariatzela | 698371 |
| Gallery (209) | 🗹 Semina | 694609 |
| Videos (5) | 🗹 Semina | 694609 |
| 🗹 📀 Audio (2) | ☑ Theodor | 694674 |
| 🗹 🚞 Documents (25) | ☑ Theodor | 694674 |
| | 🗹 ΕΞΥΠΗΡΕΤΗΣΗ Π | 13830 |
| | 🗹 ΕΞΥΠΗΡΕΤΗΣΗ Π | 13830 |
| | ΠΛΗΡ.ΤΗΛΕΦ.ΚΑΤ | 11833 |
| | ΠΛΗΡ.ΤΗΛΕΦ.ΚΑΤ | 11833 |
| | 🗹 Σπίτι Μαριατζελα | 210973 |
| | | |

Εικόνα 111 - FonePaw - Contacts 2

Στην συνέχεια βλέπουμε ότι το πρόγραμμα έχει καταφέρει να ανακτήσει επιτυχώς τα μηνύματα σε μορφή συνομιλίας όπως εμφανίζονται και στην συσκευή (Εικόνα 112, Εικόνα 113, Εικόνα 114).

| FonePaw - Android Data | a Recovery (Unregistered) | |
|---|--------------------------------------|------------|
| SAMSUNG (SM-A705FN) | OFF Only display the deleted item(s) | |
| Contacts & Messages | ✓ Name | |
| Contacts (15) | ☑ CUinfo | 26/12/2020 |
| Message Attachments (0) | ☑ CUoffer | 11/12/2020 |
| 🗹 🐛 Call Logs (22) | ☑ 121 | 9/12/2020 |
| 🔲 🔯 WhatsApp (0) | Home | 9/12/2020 |
| 🔲 💊 WhatsApp Ahments (0) | ☑ Semina | 8/12/2020 |
| Media | 🗹 Dimitra | 8/12/2020 |
| Gallery (209) @ Picture Library (1516) | ☑ Google | 8/12/2020 |
| Videos (5) | SAMSUNG | 8/12/2020 |

Εικόνα 112 - FonePaw - SMS 1

| 2 | Name | Date | To:Semina (+3069 |
|-----------|------|------------|------------------|
| CUinfo | | 26/12/2020 | Total: 1 |
| CUoffer | | 11/12/2020 | 8/12/2020 02:32 |
| 2 121 | | 9/12/2020 | Hiterard (|
| Home | | 9/12/2020 | Hinow Fu: |
| 🖸 Semina | | 8/12/2020 | |
| 🗹 Dimitra | | 8/12/2020 | |
| 🗹 Google | | 8/12/2020 | |
| SAMSUNG | | 8/12/2020 | |

Εικόνα 113 - FonePaw - SMS 2

| 2 | Name | Date | To:Dimitra(+3069-462 | |
|-----------|------|------------|--------------------------------|---|
| CUinfo | | 26/12/2020 | Total: 3 | |
| CUoffer | | 11/12/2020 | 7/12/2020 02-30 | |
| 121 | | 9/12/2020 | AOPEAN | |
| Home | | 9/12/2020 | ΕΝΗΜΕΡΩΣΗ: ΕΙΧΑΤΕ | ~ |
| 🗹 Semina | | 8/12/2020 | 02:30) EN(7H2AETAN | Ð |
| 🗹 Dimitra | | 8/12/2020 | ΚΑΤΕΙΛΗΜΜΕΝΟΣ | |
| 🗹 Google | | 8/12/2020 | 8/12/2020 01:17 | |
| SAMSUNG | | 8/12/2020 | ΓΕΙΑ ΣΟΥ ΣΕΜΙΝΑ. ΕΙΣΑΙ ΚΑΛΑ | n |
| | | | ΠΩΣ ΕΙΝΑΙ ΤΑ ΠΡΑΓΜΑΤΑ ΕΚΕΙ. | |
| | | | 8/12/2020 02:32 | |
| | | | ΣΕΜΙΝΑ ΜΗΠΩΣ | ~ |
| | | | KOIMHGOYME. | Ð |
| | | | • | |



Όλες οι εισερχόμενες, εξερχόμενες, απορριφθείσες κλήσεις έχουν ανακτηθεί με επιτυχία όπως και η ημερομηνία και ώρα που έχουν πραγματοποιηθεί η διάρκειά τους καθώς και από ποιον έχουν γίνει (Εικόνα 115).

| SAMSUNG (SM-A705FN) | Cry diplay the deleted itam(s) | | | | | | |
|--------------------------|--------------------------------|----------|-------------------|----------|---------------------|--|--|
| Contacts & Messages | 2 Name | Phone | Date | Туре | Duration | | |
| Contacts (15) | No Name | 121 | 9/12/2020 23:57 | Outgoing | 26 seconds | | |
| 🗹 📩 Messages (8) | ☑ Home | +302109 | 9/12/2020 23:36 | Rejected | 0 second | | |
| Call Logs (22) | ☑ Home | +302109 | 9/12/2020 23:35 | Rejected | 0 second | | |
| III S WhatsApp (0) | ☑ Home | +302109 | 9/12/2020 23:13 | Outgoing | 0 second | | |
| 🗏 🔕 WhatsApp Ahments (0) | Theodor | +30694/0 | 9/12/2020 23:12 | Incoming | 24 seconds | | |
| Media | Pimitra | +30694/ | 9/12/2020 21:53 | Missed | 0 second | | |
| Gallery (209) | No Name | 1237 | 8/12/2020 19:16 | Missed | 0 second | | |
| Picture Library (1516) | ✓ Dimitra | +30694/ | 8/12/2020 01:15 | Incoming | 56 seconds | | |
| Audio (2) | ✓ Dimitra | +30(04) | 7/12/2020 02:30 | Rejected | 0 second | | |
| 🗹 🧮 Documents (25) | Semina | 6946093 | 7/12/2020 01:06 | Outaoina | 0 second | | |
| | Mome | +302100 | 7/12/2020 00-53 | Outgoing | 36 seconds | | |
| | Mome | +302100 | 7/12/2020 00:53 | Rejected | 0 second | | |
| | | 69462202 | 7/12/2020 00:41 | Outanina | 1 minute 21 seconds | | |
| | Dimitra | 69462802 | 7/12/2020 00:12 | Outgoing | 0 second | | |
| | Semios | 6046000 | 6 (1 2/2020 22:52 | Outgoing | A second | | |
| | 2 Stimu | 0140300 | 6 113 10000 20:32 | Outgoing | 4 second | | |
| | | 6946749 | 6/12/2020 23:29 | Outgoing | u second | | |
| | | 09402807 | 0/12/2020 23:28 | Outgoing | 11 seconds | | |
| | e semina | 69460515 | 6/12/2020 23:28 | Outgoing | U second | | |
| | ≥ semina | 69460981 | 6/12/2020 23:28 | Outgoing | 0 second | | |
| | ≥ Home | +302105 | 6/12/2020 25:27 | Outgoing | 5 seconds | | |
| | Me Home | +302105 | 6/12/2020 23:27 | Incoming | 1 second | | |
| | M No Name | 2109610- | 6/12/2020 23:26 | Outgoing | 0 second | | |

Εικόνα 115 - FonePaw - Call Logs

Έχουν ανακτηθεί επιτυχώς και όλες οι εικόνες που υπάρχουν στο Gallery της συσκευής (Εικόνα 116).



Εικόνα 116 - FonePaw - Pictures 1

Στην καρτέλα Picture Library παρατηρούμε ότι το πρόγραμμα έχει ανακτήσει και φωτογραφίες από το Trash της συσκευής (Εικόνα 117, Εικόνα 118, Εικόνα 119).



Εικόνα 117 - FonePaw - Pictures 2





after 30 days. Remember to empty the Trash before removing your SD card to make sure anything you've added to the Trash is completely deleted.





| 111 | 0 | < |
|-----|---|---|

Εικόνα 119 - Gallery Trash

| 🗹 📋 SAMSUNG (SM-A705FN) | OFF Only display t | he deleted item(s) | | | |
|-----------------------------|--------------------|--------------------|--------------|--------------|--------------|
| Contacts & Messages | | | | | |
| 🗹 👤 Contacts (15) | H-H | e | HH | er e | |
| 🗹 📩 Messages (8) | | | | | |
| 🔳 🔗 Message Attachments (0) | 88 | 88 | | 88 | |
| 🗹 🐛 Call Logs (22) | | | | | |
| WhatsApp (0) | 20201211.mp4 | 🗹 20201212.mp4 | 20201222.mp4 | 20201252.mp4 | 20201225.mp4 |
| 🔲 💊 WhatsApp Ahments (0) | | | | | |
| Media | | | | | |
| 🗹 🎽 Gallery (209) | | | | | |
| 🗹 🙆 Picture Library (1516) | | | | | |
| Videos (5) | | | | | |
| 🗹 📀 Audio (2) | | | | | |
| 🗹 🧮 Documents (25) | | | | | |

Έχουν ανακτηθεί επιτυχώς και πέντε βίντεο από την συσκευή (Εικόνα 120).

Εικόνα 120 - FonePaw - Videos

Τέλος το FonePaw έχει καταφέρει να ανακτήσει και κάποια xml αρχεία από την συσκευή (Εικόνα 121).

| SAMSUNG (SM-A705FN) | 017 Orly daylay the deleted item(2) | | | | | |
|-----------------------------|-------------------------------------|------|-----------|--------|--|--|
| Contacts & Messages | • | Name | Size | Format | | |
| Contacts (15) | ☑ info.xml | | 365,58 KB | XML | | |
| 🗏 💋 Message Attachments (0) | ☑ info.xml | | 365,58 KB | XML | | |
| 🗹 💽 Call Logs (22) | ☑ info.xml | | 365,58 KB | XML | | |
| III 🔯 WhatsApp (0) | ☑ info.xml | | 365,58 KB | XML | | |
| WhatsApp Ahments (0) | ☑ info.xml | | 365,58 KB | XML | | |
| Media | ☑ info.xml | | 365,58 KB | XML | | |
| Gallery (209) | 🗹 info.xml | | 365,58 KB | XML | | |
| Videos (5) | ☑ info.xml | | 365,58 KB | XML | | |
| Audio (2) | 🗹 info.xml | | 365,58 KB | XML | | |
| Documents (25) | ☑ info.xml | | 365,58 KB | XML | | |

Εικόνα 121 - FonePaw - Documents

Η free trial εκδοχή που χρησιμοποιούμε δεν μας παρέχει την δυνατότητα να κάνουμε recover κάποιο αρχείο ενδιαφέροντος στον υπολογιστή μας.

Συγκριτικά με το AFLogical OSE που παρέχει το Santoku το FonePaw έχει καλύτερη απόδοση στα android 10 σε logical level εφόσον μπορεί να ανακτήσει επιτυχώς επαφές, κλήσεις, μηνύματα, εικόνες, βίντεο, αρχεία ενώ το AFLogical OSE δεν μπορούσε να ανακτήσει το αρχείο των επαφών και έπρεπε να πραγματοποιήσουμε εμείς το export από την συσκευή και μπορούσε να ανακτήσει μόνο κλήσεις και μηνύματα. Επιπλέον το FonePaw παρέχει αυτές τις δυνατότητες σε ένα φιλικό προς τον χρήστη περιβάλλον.

5. PHYSICAL IMAGE ACQUISITION

Πριν πραγματοποιήσουμε την διαδικασία της physical image forensics analysis πρέπει πρώτα να πάρουμε ένα image της συσκευής. Για να το πετύχουμε αυτό εγκαθιστούμε στην συσκευή την εφαρμογή BusyBox (Stericson) μέσω Play Store (Εικόνα 122). Η συγκεκριμένη εφαρμογή παρέχει την δυνατότητα να χρησιμοποιηθούν βασικά εργαλεία unix σε κινητές συσκευές.



Εικόνα 122 - BusyBox Welcome Message



Εικόνα 123 - BusyBox App

Μέσα από την εφαρμογή πατάμε install για να εγκαταστήσουμε όλες τις παροχές του BusyBox στην συσκευή (Εικόνα 123, Εικόνα 124).

| 21:23 🖬 🕈 🗱 • | N 🖓 11 🛔 |
|--|---|
| BUSYBOX | |
| Install Busybox | About BusyBox |
| BusyBox combines UNIX utilities into a replacements for n in GNU fileutils, she generally have fews GNU cousins, howe provide the expect much like their GN fairly complete env system. | |
| BusyBox has been and limited resource modular as you can or features! at cor to customize your- working system. Ju few configuration fi | written with size-optimization ceasin mind. It is also axtremaly reality include on socials commands ambadded systems. To create a st add some device nodes in /dex a les in /etc. and a Linux kernel. |
| It looks like the | e installation of BusyBox was |
| successful! Cor | ngratulations! |
| Keep in mind you will be not BusyBox is rea | that by Keeping this installed fied whenever a new version of dy to be installed. |
| If you need an app | let added, please email me at |
| | |
| BusyBox Fre | ee was granted Superuser rights |
| Install | Uninstall |
| Ш | 0 < |

Εικόνα 124 - BusyBox Installed

Από το adb shell προβάλουμε στο terminal τον πίνακα με τα διαφορετικά partitions της συσκευής, χρησιμοποιώντας την εντολή:

cat /proc/partitions (Εικόνα 125, Εικόνα 126, Εικόνα 127)

| santoku List of R58M | u@santoku f devices | -virtual-m attached device | nachine:~\$ | adb | device |
|---|--|--|--|-----|--------|
| santoku a70q:/ a70q:/ major m | u@santoku \$ su # cat /p ninor #b | -virtual-m proc/partit locks nam | machine:~\$ tions me | adb | shell |
| 1 | 0 1 2 3 4 5 6 7 8 9 10 11 12 13 | 8192 8192 8192 8192 8192 8192 8192 8192 | ram0 ram1 ram2 ram3 ram4 ram5 ram6 ram7 ram8 ram9 ram10 ram11 ram12 ram13 | | |
| 1 254 8 8 8 8 | 14 15 0 1 2 3 | 8192 8192 2097152 124874752 2048 2048 4 | ram14 ram15 zram0 sda sda1 sda2 sda3 | | |

Εικόνα 125 - Device Partitions 1

| 8 | 4 | 8 | sda4 |
|-----|----|-----------|-------|
| 8 | 5 | 32768 | sda5 |
| 8 | 6 | 20480 | sda6 |
| 8 | 7 | 12288 | sda7 |
| 8 | 8 | 10240 | sda8 |
| 8 | 9 | 20480 | sda9 |
| 8 | 10 | 1024 | sda10 |
| 8 | 11 | 512 | sdall |
| 8 | 12 | 40960 | sda12 |
| 8 | 13 | 21504 | sda13 |
| 8 | 14 | 512 | sdal4 |
| 8 | 15 | 4096 | sda15 |
| 259 | Θ | 16384 | sdal6 |
| 259 | 2 | 97280 | sda17 |
| 259 | 4 | 87040 | sda18 |
| 259 | 6 | 32768 | sda19 |
| 259 | 8 | 10240 | sda20 |
| 259 | 9 | 65536 | sda21 |
| 259 | 11 | 80884 | sda22 |
| 259 | 13 | 5632000 | sda23 |
| 259 | 15 | 1024000 | sda24 |
| 259 | 17 | 614400 | sda25 |
| 259 | 19 | 409600 | sda26 |
| 259 | 21 | 10240 | sda27 |
| 259 | 23 | 51200 | sda28 |
| 259 | 26 | 116573020 | sda29 |
| 8 | 16 | 8192 | sdb |
| 8 | 17 | 4096 | sdb1 |
| 8 | 18 | 3940 | sdb2 |

Εικόνα 126 - Device Partitions 2

| 8 | 32 | 8192 | sdc |
|-----|----|-------|-------|
| 8 | 33 | 4096 | sdc1 |
| 8 | 34 | 3940 | sdc2 |
| 8 | 48 | 61440 | sdd |
| 8 | 49 | 1024 | sdd1 |
| 8 | 50 | 4096 | sdd2 |
| 8 | 51 | 2048 | sdd3 |
| 8 | 52 | 512 | sdd4 |
| 8 | 53 | 4096 | sdd5 |
| 8 | 54 | 4 | sdd6 |
| 8 | 55 | 1024 | sdd7 |
| 8 | 56 | 384 | sdd8 |
| 8 | 57 | 512 | sdd9 |
| 8 | 58 | 512 | sdd10 |
| 8 | 59 | 512 | sdd11 |
| 8 | 60 | 256 | sdd12 |
| 8 | 61 | 256 | sdd13 |
| 8 | 62 | 4 | sdd14 |
| 8 | 63 | 4 | sdd15 |
| 259 | 1 | 8192 | sdd16 |
| 259 | З | 128 | sdd17 |
| 259 | 5 | 512 | sdd18 |
| 259 | 7 | 64 | sdd19 |
| 259 | 10 | 128 | sdd20 |
| 259 | 12 | 32 | sdd21 |
| 259 | 14 | 2048 | sdd22 |
| 259 | 16 | 2048 | sdd23 |
| 259 | 18 | 1024 | sdd24 |
| 259 | 20 | 512 | sdd25 |

Εικόνα 127 - Device Partitions 3

To partition που θα κάνουμε physical image είναι το sda.

Χρησιμοποιώντας τα εργαλεία dd και netcat παίρνουμε το physical forensic image της συσκευής.

To dd είναι προεγκατεστημένο στο Santoku, θα πρέπει όμως να εγκαταστήσουμε το netcat χρησιμοποιώντας την εντολή:

sudo apt-get install netcat

Η διαδικασία του physical image acquisition θα πραγματοποιηθεί με την χρήση δύο terminal, ένα θα είναι su shell στην κινητή συσκευή και ένα θα είναι στον υπολογιστή μας.

Στο terminal που αφορά τον υπολογιστή μας μετακινούμαστε στον φάκελο που θέλουμε να αποθηκεύσουμε το image και εκτελούμε την εντολή (Εικόνα 128):

adb forward tcp:8888 tcp:8888

Η συγκεκριμένη εντολή δημιουργεί μια σύνδεση ανάμεσα στον υπολογιστή μας (στον σκληρό δίσκο που αποθηκεύουμε το image) και στο τηλέφωνο στην tcp port 8888.

santoku@santoku-virtual-machine:/media/santoku/ADATA SD700\$ adb forward tcp:8888 tcp:8888
santoku@santoku-virtual-machine:/media/santoku/ADATA SD700\$

Εικόνα 128 - adb forward

Στο terminal που αφορά στην συσκευή βρισκόμαστε σε su shell και εκτελούμε την εντολή (Εικόνα 129):

dd if=/dev/block/sda | busybox nc -l -p 8888

Αναλυτικότερα η συγκεκριμένη εντολή:

dd if=/dev/block/sda: Δίνει input το sda partition στο dd, το dd λοιπόν θα διαβάσει bit per bit το sda partition.

| busybox nc -l -p 8888: Δίνουμε το output του dd στο busybox το οποίο τρέχει το netcat.

-l -p 8888: Το -l σημαίνει ότι έχουμε ενεργοποιήσει το listen switch, κάνουμε έτσι το τηλέφωνο να ανοίγει μια listen port στο tcp port 8888, κάνοντας το συγκεκριμένο με το –p 8888.

Έτσι λοιπόν όταν έρχεται μια εισερχόμενη σύνδεση στο συγκεκριμένο port το dd θα στέλνει ανά bit όλο το sda partition.

Δεν πατάμε enter στην εντολή και επιστρέφουμε στο terminal που αφορά το workstation μας.

| 259 | 20 | 512 | sdd25 | | | | | | |
|--------|------------|-----------|-------|---------|----|----|-----|------|--|
| 259 | 22 | 2048 | sdd26 | | | | | | |
| 259 | 24 | 2048 | sdd27 | | | | | | |
| 259 | 25 | 27256 | sdd28 | | | | | | |
| a70q:/ | # dd if=/0 | dev/block | /sda | busybox | nc | -1 | - p | 8888 | |
| | | | | | | | | | |

Εικόνα 129 - dd for sda partition

Χρησιμοποιώντας το netcat τώρα από τον υπολογιστή μας θα κάνουμε μια σύνδεση στο localhost στην tcp port 8888 , η οποία γίνεται forward από το adb και το input από εκεί θα το αποθηκεύσουμε στο αρχείο A70F.dd.

Η εντολή (Εικόνα 130):

nc 127.0.0.1 8888 > A70F.dd

Επιστρέφουμε στο terminal της συσκευής και πατάμε enter στην εντολή:

dd if=/dev/block/sda | busybox nc -l -p 8888

Στην συνέχεια πηγαίνουμε στο terminal που αφορά τον υπολογιστή μας και πατάμε enter στην εντολή:

nc 127.0.0.1 8888 > A70F.dd

santoku@santoku-virtual-machine:/media/santoku/ADATA SD700\$ adb forward tcp:8888 tcp:8888 santoku@santoku-virtual-machine:/media/santoku/ADATA SD700\$ nc 127.0.0.1 8888 > A70F.dd

Εικόνα 130 - netcat

Μόλις ολοκληρωθεί η διαδικασία στο terminal της συσκευής μπορούμε να δούμε τα αποτελέσματα, τα συνολικά bytes που αντιγράφθηκαν , πόσο διήρκησε η διαδικασία και τον ρυθμό που γινόταν η αντιγραφή σε kb/s (Εικόνα 131).

```
a70q:/ # dd if=/dev/block/sda | busybox nc -l -p 8888
249749504+0 records in
249749504+0 records out
127871746048 bytes (119.1GB) copied, 143163.145502 seconds, 872.3KB/s
a70q:/ # exit
a70q:/ $ exit
santoku@santoku-virtual-machine:~$ []
```

Εικόνα 131 - Physical Image Finished 1

Στο terminal στο workstation μας η διαδικασία ολοκληρώνεται εφόσον έχει γίνει exit από την εντολή (Εικόνα 132).

```
santoku@santoku-virtual-machine:/media/santoku/ADATA SD700$ adb forward tcp:8888 tcp:8888
santoku@santoku-virtual-machine:/media/santoku/ADATA SD700$ nc 127.0.0.1 8888 > A70F.dd
santoku@santoku-virtual-machine:/media/santoku/ADATA SD700$
```

Εικόνα 132 - Physical Image Finished 2

Τέλος υπολογίζουμε τις συνόψεις MD5 και SHA1 του physical image (Εικόνα 133) προκειμένου να μπορούμε να επιβεβαιώσουμε και να αποδείξουμε την ακεραιότητά του στο τέλος της διαδικασίας της ανάλυσης. Οι συγκεκριμένες συνόψεις θα πρέπει να παραμείνουν ίδιες σε όλη την διαδικασία της ανάλυσης, σε περίπτωση που στο τέλος της διαδικασίας της ανάλυσης οι συνόψεις διαφέρουν από αυτές που υπολογίσαμε στην αρχή της διαδικασίας σημαίνει ότι συνέβη τροποποίηση στο physical image και τα δεδομένα δεν είναι ίδια με αυτά που εξήχθησαν κατά την διαδικασία του physical image acquisition.

| C:\Users\Σεμίνα\Desktop>CertUtil -hashfile A70F.dd MD5 Κατακερματισμός MD5 του αρχείου A70F.dd: |
|---|
| c6 9d e8 d8 60 e7 cd f9 75 05 16 25 7e a5 08 22 CertUtil: Η εντολή -hashfile ολοκληρώθηκε με επιτυχία. |
| C:\Users\Σεμίνα\Desktop>CertUtil -hashfile A70F.dd SHA1 Ματακερματισμές SHA1 του σονείου A20F.dd: |
| 48 21 b9 11 31 29 f7 2c 3c a0 67 db f2 48 50 52 3f ac 34 5d CertUtil: Η εντολή -hashfile ολοκληρώθηκε με επιτυχία. |

Εικόνα 133 - Physical Image MD5 & SHA 1 Hashes

6. PHYSICAL ANALYSIS

6.1 AUTOPSY

Για την ανάλυση του physical image χρησιμοποιήσαμε το Autopsy version 4.17.0. Το Autopsy παρέχει γραφικό περιβάλλον, ομαδοποίηση των δεδομένων σύμφωνα με συγκεκριμένους τύπους αρχείων, παρέχεται επίσης η δυνατότητα keyword search και δημιουργίας timeline. Επιπρόσθετα με το Android Analyzer Module μπορεί να αναλύσει physical images από android συσκευές (Εικόνα 134).

| * | Add Data Source × |
|---|--|
| Steps 1. Select Type of Data Source To Add 2. Select Data Source 3. Configure Ingest Modules 4. Add Data Source | Configure Ingest Modules Run ingest modules on: All Files, Directories, and Unallocated Space Image: Picture Analyzer Image: Picture Analyzer Image: Email Parser Image: Email Parser Image: Picture Analyzer Image: Email Parser Image: Picture Analyzer |
| | Interesting Files Identifier Central Repository PhotoRec Carver Virtual Machine Extractor Data Source Integrity Drone Analyzer Plaso IOS Analyzer (ILEAPP) |
| | Image: Android Analyzer Image: Comparison of the compa |
| | < Back Next > Finish Cancel Help |

Εικόνα 134 - Autopsy Modules

To autopsy ανοίγοντας το image δημιουργεί ένα evidence tree (Εικόνα 135). Στην συγκεκριμένη περίπτωση έχουμε ανοίξει το image A70F.dd, το autopsy θα αναλύσει το συγκεκριμένο image σε volumes/partitions όπως ήταν δομημένη και η κινητή συσκευή.

| 🗐 🖳 Data S | ources |
|------------|--|
| 📄 🧾 A7 | 0F.dd |
| 🗃 | vol1 (Unallocated: 0-263) |
| 🛨 ·· 🗃 | vol4 (modemst1: 264-775) |
| 🗃 | vol5 (modemst2: 776-1287) |
| 🗃 | vol6 (fsc: 1288-1288) |
| 🗃 | vol7 (ssd: 1289-1290) |
| 🛨 ·· 🗃 | vol8 (persist: 1291-9482) |
| 🛨 ·· 📷 | vol9 (efs: 9483-14602) |
| 🗃 | vol10 (param: 14603-17674) |
| 🗃 | vol11 (debug: 17675-20234) |
| 🛨 ·· 📷 | vol12 (sec_efs: 20235-25354) |
| 🗃 | vol13 (misc: 25355-25610) |
| 🗃 | vol14 (keystore: 25611-25738) |
| 🗃 | vol15 (bota: 25739-35978) |
| 18 | vol16 (fota: 35979-41354) |
| 🗃 | vol17 (persistent: 41355-41482) |
| 18 | vol18 (steady: 41483-42506) |
| 🗃 | vol19 (dqmdbg: 42507-46602) |
| 🕂 ·· 🗃 | vol20 (apnhlos: 46603-70922) |
| 🕂 ·· 🗃 | vol21 (modem: 70923-92682) |
| 🕂 ·· 🗃 | vol22 (dsp: 92683-100874) |
| 🗃 | vol23 (dtbo: 100875-103434) |
| 🗃 | vol24 (boot: 103435-119818) |
| 🗃 | vol25 (recovery: 119819-140039) |
| 🕂 ·· 🗐 | vol26 (system: 140040-1548039) |
| 🕂 · 🗐 | vol27 (vendor: 1548040-1804039) |
| 🕂 ·· 🗐 | vol28 (product: 1804040-1957639) |
| 🕂 ·· 😑 | vol29 (cache: 1957640-2060039) |
| 🗃 | vol30 (hidden: 2060040-2062599) |
| 🕂 ·· 😑 | vol31 (omr: 2062600-2075399) |
| 🕂 · 🗑 | vol32 (userdata: 2075400-31218654) |
| | vol33 (Unallocated: 31218655-31218687) |

Εικόνα 135 - Evidence Tree - Volumes

Στην συνέχεια του evidence tree το autopsy ομαδοποιεί διάφορα δεδομένα με βάση τον τύπο αρχείου, επιπρόσθετα έχει εντοπίσει όλα τα deleted files (Εικόνα 136, Εικόνα 137).



Εικόνα 136 - Evidence Tree - File Types



Εικόνα 137 - Evidence Tree - Deleted Files

Πηγαίνοντας όμως να δούμε τις βάσεις δεδομένων (Εικόνα 138) που έχει αναγνωρίσει το autopsy παρατηρούμε ότι πέρα από κάποιες βάσεις που δεν διαθέτουν ιδιαίτερες πληροφορίες το autopsy αναγνωρίζει τις βάσεις ως contents.db (Εικόνα 139) και δεν αναγνωρίζει τις βασικές βάσεις που διαχειρίζεται το android για να αποθηκεύει δεδομένα.



Εικόνα 138 - Databases

| Listing |
|---------------------------------|
| Databases |
| Table Thumbnail Summary |
| |
| Name |
| iop_bt.db |
| ObjDet.polarr.db |
| SmartCrop.polarr.db |
| OSC2.5_2ndtrained_reduce_fix.db |
| preview_verification_svm.db |
| contents.db |

Εικόνα 139 - Databases Listing

Οι βάσεις contents.db δεν διαθέτουν δεδομένα από την δραστηριότητα του χρήστη στην συσκευή (Εικόνα 140).

| Hex Text | Application | File Metadata Context Results Annotations Other Occurrences | | | | | |
|--|-------------|--|----------|--|--|--|--|
| Table contents v 416 entries Page 1 of 5 Export to CSV | | | | | | | |
| salesCode | _id | filePath | fileSize | | | | |
| | 1 | /product/omc/PHE/etc/default_workspace.xml | 7120 | | | | |
| | 2 | /product/omc/PHE/etc/enforcedeletepackage.txt | 142 | | | | |
| | 3 | /product/omc/PHE/etc/sales_code.dat | 4 | | | | |
| | 4 | /product/omc/PHE/etc/cid/sysconfig/eea_search_chrome.xml | 227 | | | | |
| | 5 | /product/omc/PHE/etc/enforceskippingpackages.txt | 6056 | | | | |
| | 6 | /product/omc/PHE/etc/permissions/permission_ignite_com.dti.samsung.xml | 289 | | | | |
| | 7 | /product/omc/PHE/etc/default_application_order.xml | 8745 | | | | |
| | 8 | /product/omc/PHE/etc/byoddeletepackagenames.txt | 1724 | | | | |
| | 9 | /product/omc/PHE/etc/PHE_keystrings.dat | 12736 | | | | |
| | 10 | /product/omc/PHE/etc/sysconfig/whitelist_com.dti.samsung.xml | 284 | | | | |
| | 11 | /product/omc/PHE/etc/hidden_apks_list.txt | 0 | | | | |
| | 12 | /product/omc/PHE/conf/cscfeature_network.xml | 651 | | | | |
| | 13 | /product/omc/PHE/conf/cscfeature.xml | 757 | | | | |
| | 14 | /product/omc/PHE/conf/omc.info | 6845 | | | | |
| | 15 | /product/omc/PHE/conf/customer.xml | 47183 | | | | |
| | 16 | /product/omc/ITV/etc/default_workspace.xml | 7515 | | | | |
| | 17 | /product/omc/ITV/etc/enforcedeletepackage.txt | 142 | | | | |
| | 18 | /product/omc/ITV/etc/sales_code.dat | 4 | | | | |
| | 19 | /product/omc/ITV/etc/cid/sysconfig/eea_search_chrome.xml | 227 | | | | |

Εικόνα 140 - Περιεχόμενα Database

To autopsy συνεπώς μπορεί να ανοίξει το image μόνο σε high level, δηλαδή σε επίπεδο partitions και δεν μπορεί να διαβάσει τα δεδομένα.

Το Autopsy υποστηρίζει τα ακόλουθα file systems:

- NTFS
- FAT 12/16/32
- ExFAT
- HFS+
- Yaffs2
- UFS1/2
- EXT2/3/4
- ISO9660 (CD-ROM)

Σε su shell στην συσκευή δίνουμε την εντολή blkid (Εικόνα 141) για να δούμε τι file systems είναι τα partitions. Παρατηρούμε ότι τα partitions της συσκευής είναι ext4 και vfat , τα partitions που είναι ext4 υποστηρίζονται από το autopsy ενώ το vfat δεν υποστηρίζεται από το autopsy.

| santoku@santoku-virtual-machine:~\$ adb shell |
|--|
| a70q:/ \$ su |
| a70q:/ # blkid |
| /dev/block/vold/public:179,1: UUID="3701-06FD" TYPE="vfat" |
| /dev/block/zram0: UUID="2ba2f469-02c6-4e82-94be-556421e6f993" TYPE="swap" |
| /dev/block/sda18: UUID="00BC-614E" TYPE="vfat" |
| /dev/block/sda29: LABEL="data" UUID="3eef01a3-9a84-4f67-acc4-f6680cc19154" TYPE= |
| "ext4" |
| /dev/block/mmcblk0p1: UUID="3701-06FD" TYPE="vfat" |
| /dev/block/sda17: UUID="00BC-614E" TYPE="vfat" |
| /dev/block/sda5: LABEL="persist" UUID="bf85faa3-c647-56cc-bdbb-cc04a4b1cad9" TYP |
| E="ext4" |
| /dev/block/sda19: LABEL="dsp" UUID="af32c008-2a39-7e5b-a5dc-201456d93103" TYPE=" |
| ext4" |
| /dev/block/sda9: LABEL="sec_efs" UUID="736edfa6-0b7c-5264-800a-7bb203039c7d" TYP |
| E="ext4" |
| /dev/block/sda26: LABEL="cache" UUID="6e9bd3c2-5ec5-4399-9bf7-c5e23dfebeac" TYPE |
| ="ext4" |
| /dev/block/sda28: LABEL="omr" UUID="b938e0b2-b515-53a5-9fd5-d72c52a610ba" TYPE=" |
| ext4" |
| /dev/block/sda6: LABEL="efs" UUID="563d3d87-578d-5542-b8fe-7ffa3ca08c8a" TYPE="e |
| xt4" |

Εικόνα 141 - Device Partitions File Systems

Συνεπώς το Autopsy μπορεί να αναγνωρίσει το image και να το ανοίξει σε high level επίπεδο εφόσον αναγνωρίζει μερικώς τα file systems που χρησιμοποιούν τα partitions της συσκευής. Το Autopsy μπορεί και δημιουργεί το evidence tree και την δομή των partitions με τα αρχεία τους , δεν μπορεί όμως να αναλύσει το image σε βαθύτερο επίπεδο. Αυτό συμβαίνει πιθανώς γιατί το Autopsy δεν υποστηρίζει το vfat file system και το scoped storage που έχουν εισάγει τα android 10. Αξίζει να αναφέρουμε ότι στο χρονικό διάστημα που έχει πραγματοποιηθεί η έρευνα της διπλωματικής στο documentation του προγράμματος δεν αναφέρεται κάτι για το συγκεκριμένο πρόβλημα.

Γνωρίζουμε ότι το λειτουργικό σύστημα android απαρτίζεται ουσιαστικά από ένα σύνολο βάσεων δεδομένων, μπορούμε λοιπόν να αποδείξουμε ότι οι βάσεις δεδομένων υπάρχουν στην συσκευή και έχουν καταγράψει δεδομένα απλώς το autopsy δεν μπορεί να τις αναγνωρίσει. Αυτό μπορούμε να το κάνουμε εισάγοντας μια microsd κάρτα στην συσκευή και αντιγράφοντας τις βάσεις δεδομένων εκεί για να εξετάσουμε τα περιεχόμενά τους. Στόχος μας είναι να πάρουμε και να εξετάσουμε τα περιεχόμενα της βάσης contacts2.db.

Από su shell στην συσκευή μετακινούμαστε στο directory /data/data/com.samsung.android.providers.contacts/databases και δίνουμε την εντολή ls για να δούμε τις βάσεις δεδομένων που υπάρχουν στο directory (Εικόνα 142).

| a70q:/data/data # | cd com.samsung.and | roid.providers.con | tacts/databases | | | | |
|---|--------------------|--------------------|-------------------|--|--|--|--|
| a70q:/data/data/com.samsung.android.providers.contacts/databases # ls | | | | | | | |
| calllog.db | contacts2.db | profile.db | profile sa.db | | | | |
| calllog.db-shm | contacts2.db-shm | profile.db-shm | profile sa.db-shm | | | | |
| calllog.db-wal | contacts2.db-wal | profile.db-wal | profile sa.db-wal | | | | |
| a70q:/data/data/com.samsung.android.providers.contacts/databases # | | | | | | | |

Εικόνα 142 - /data/data/com.samsung.android.providers.contacts/databases

Δίνουμε την ακόλουθη εντολή για να αντιγράψουμε την βάση δεδομένων contacts2.db με τα περιεχόμενά της στην sd card (Εικόνα 143):

cp contacts2.db /sdcard/contacts2.db

Στην συνέχεια κάνουμε exit από το su shell και στο terminal δίνουμε την εντολή (Εικόνα 143):

adb pull /sdcard/contacts2.db

Και παίρνουμε την βάση δεδομένων στον υπολογιστή μας.

| | +30694 | '₿a70q:/dat | a/data/com.samsung.and | roi | | | |
|---|--------------------|----------------|------------------------|-----|--|--|--|
| .providers.contact | ts/databases # ls | | | | | | |
| calllog.db | contacts2.db | profile.db | profile_sa.db | | | | |
| calllog.db-shm | contacts2.db-shm | profile.db-shm | profile sa.db-shm | | | | |
| calllog.db-wal | contacts2.db-wal | profile.db-wal | profile sa.db-wal | | | | |
| p contacts2.db /sc | dcard/contacts2.db | | | < | | | |
| a70g:/data/data/com.samsung.android.providers.contacts/databases # exit | | | | | | | |
| a70q:/ \$ exit | | | | | | | |
| santoku@santoku-virtual-machine:~\$ adb pull /sdcard/contacts2.db | | | | | | | |
| 1629 KB/s (491520 | bytes in 0.294s) | | | | | | |
| santoku@santoku-v: | irtual-machine:~\$ | | | | | | |

Εικόνα 143 - adb pull database contacts2.db from sdcard

Ανοίγουμε την βάση contacts2.db χρησιμοποιώντας το πρόγραμμα Sqliteman από το Santoku. Το Google Account που βρίσκεται σε synchronization state με την συσκευή είναι το <u>ptyxiakidummy@gmail.com</u> (Εικόνα 144).



Εικόνα 144 - Gmail on Device

Στην συνέχεια στο table raw_contacts μπορούμε να δούμε όλες τις υπάρχουσες επαφές στην συσκευή (Εικόνα 145, Εικόνα 146, Εικόνα 147, Εικόνα 148).



Εικόνα 145 - Raw Contacts on Device 1



Εικόνα 146 - Raw Contacts on Device 2


Εικόνα 148 - Raw Contacts on Device 4

Παρατηρούμε λοιπόν ότι τα δεδομένα υπάρχουν στις βάσεις δεδομένων και το autopsy δεν μπορεί να τα ανακτήσει από το physical image.

6.2 ANDRILLER

Μία άλλη open source εκδοχή προγράμματος για ανάλυση σε physical level χρησιμοποιώντας σωστές πρακτικές forensics είναι το Andriller. Το πρόγραμμα αυτό απαιτεί root πρόσβαση στο τηλέφωνο και ενεργοποιημένο usb debugging για να λειτουργήσει. Το πρόγραμμα αυτό προσπαθεί να πάρει πρόσβαση στις βάσεις δεδομένων του android που έχουν τις πληροφορίες που μας ενδιαφέρουν.

Στην αρχική οθόνη του Andriller επιλέγουμε Check και στο κινητό επιλέγουμε Allow στο μήνυμα που θα εμφανιστεί (Εικόνα 150). Με αυτό τον τρόπο αναγνωρίζει το andriller την συσκευή. Εάν έχει γίνει επιτυχημένη αναγνώριση συσκευής θα εμφανιστεί το serial number της συσκευής (Εικόνα 149).

| Andriller CE - 3.5.3 | |
|---|----------|
| File Decoders Apps Utils Lockscreens Tools ADB Help | |
| Andriller | |
| | |
| Global Output Location (Decoders / Extraction / Parsing) | |
| Output | |
| Extraction (USB) Parse (Folder) Parse (.TAR) Parse (.AB) | |
| Check Serial ID: R38MB | |
| Extract | |
| If If rooted - force Android Backup extraction instead | |
| Started: Andriller CE 3.5.3 | |
| Time settings/format: Y-m-d H:M:S Z Detected/PC time: 2021-01-19 18:21:58 | |
| Universal time: 2021-01-19 16:21:58 UTC Time in reports: 2021-01-19 16:21:58 UTC < | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| Clear Log | Save Log |
| Ready | |

Εικόνα 149 - Andriller



Εικόνα 150 - Andriller - Allow USB debugging?

Στην συνέχεια επιλέγουμε output και επιλέγουμε έναν φάκελο στο workstation μας για να αποθηκεύσει το Andriller τα αποτελέσματα (Εικόνα 151).

| Π Επιλογή φακέλου | Tel harden |
|--|--|
| The second seco | 4₂ Αναζήτηση andriller results |
| Οργάνωση 🔻 Νέος φάκελος | III - |
| 🔆 Αγαπημένα 🌔 Όνομα | Ημερομηνία τροπ Τύπος Μέγεθος |
| Uropbox | Δεν βρέθηκαν αποτελέσματα για την αναζήτησή σας. |
| μα επιφανεία ε | |
| 🔢 Πρόσ.θέσεια | |
| 📑 Έγγραφα 😑 | |
| 🥽 Βιβλιοθήκες | |
| (Podcasts | |
| Βίντεο | |
| Ε Εικόνες | |
| 👌 Μουσική | |
| 🤣 Οικιακή ομάδ | |
| 💻 Υπολογιστής 🔻 | |
| Φάκελος: andriller results | |
| | Επιλογή φακέλου Άκυρο |

Εικόνα 151 - Andriller Results Folder

Πατάμε Extract για να εκκινήσει η διαδικασία (Εικόνα 152).

| (f) Andriller CE - 3.5.3 | | | | |
|--|--|--|--|--|
| File Decoders Apps Utils Lockscreens Tools ADB Help | | | | |
| Anderillan | | | | |
| Alluritter | | | | |
| Global Output Location (Decoders / Extraction / Parsing) | | | | |
| Output C:\Users\Σεμίνα\Desktop\andriller results | | | | |
| Extraction (USB) Parse (Folder) Parse (.TAR) Parse (.AB) | | | | |
| Check Serial ID: R58MB | | | | |
| Extract | | | | |
| Use AB method (ignore root) | | | | |
| Extract Shared Storage | | | | |
| Started: Andriller CE 3.5.3 | | | | |
| Detected/PC time: 2021-01-19 18:21:58 | | | | |
| Time in reports: 2021-01-19 16:21:58 UTC < | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| Classing | | | | |
| Save Log | | | | |
| Ready | | | | |

Εικόνα 152 - Andriller – Extract



Εικόνα 153 - Andriller - Finished

| 2 | C:\Us | ;ers\Σεμίνα\Desktop\andriller results\andriller.log - Notepad++ |
|---|-------|---|
| A | ρχείο | Επεξεργασία Εύρεση Προβολή Κωδικοποίηση Γλώσσα Ρυθμίσεις Μακροεντολή Εκτέλεση Πρόσθετ |
| | 6 |) 🗄 🛸 🕞 🕞 😂 🚜 🖒 🇈 Ə 🗲 🏙 🍢 🍕 👒 🖫 🔤 🎫 💵 💷 💌 |
| E | andr | iller.log |
| Γ | 1 | Started: Andriller CE 3.5.3 |
| | 2 | Time settings/format: Y-m-d H:M:S Z |
| | з | Detected/PC time: 2021-01-19 18:21:58 |
| | 4 | Universal time: 2021-01-19 16:21:58 UTC |
| | 5 | Time in reports: 2021-01-19 16:21:58 UTC < |
| | 6 | Reading information |
| | 7 | Acquiring data |
| | 8 | Acquiring databases via root |
| | 9 | /data/data/com.android.chrome/app_chrome/Default/History (196608 bytes) |
| | 10 | Failed getting file: History |
| | 11 | /data/data/com.android.chrome/app_chrome/Default/History-journal (8720 bytes) |
| | 12 | Failed getting file: History-journal |
| | 13 | /data/data/com.android.chrome/app_chrome/Default/Login Data (36864 bytes) |
| | 14 | Failed getting file: Login Data |
| | 15 | /data/data/com.android.providers.calendar/databases/calendar.db (204800 bytes) |
| | 10 | Failed getting file: calendar.do |
| | 10 | /data/data/com.android.providers.calendar/databases/calendar.db-journal (25136 bytes) |
| | 19 | failed getting file. Calendar.db-Journal |
| | 20 | Failed getting file: downloads db |
| | 21 | /data/data/com android providers downloads/databases/downloads db-journal (12824 bytes) |
| | 22 | Failed getting file: downloads.db-journal |
| | 23 | /data/data/com.android.providers.telephonv/databases/mmssms.db (389120 bvtes) |
| | 24 | Failed getting file: mmssms.db |
| | 25 | /data/data/com.android.providers.telephony/databases/mmssms.db-shm (32768 bytes) |
| | 26 | /data/data/com.android.providers.telephony/databases/mmssms.db-wal (362592 bytes) |
| | 27 | Failed getting file: mmssms.db-wal |
| | 28 | /data/data/com.facebook.orca/databases/threads_db2 (307200 bytes) |
| | 29 | Failed getting file: threads_db2 |
| | 30 | /data/data/com.facebook.orca/databases/threads_db2-journal (51200 bytes) |
| | 31 | Failed getting file: threads_db2-journal |
| | 32 | /data/data/com.google.android.apps.photos/databases/gphotos-1.db (1589248 bytes) |
| | 33 | Failed getting file: gphotos-1.db |
| | 34 | /data/data/com.google.android.apps.photos/databases/gphotos-1.db-shm (32768 bytes) |
| | 35 | Failed getting file: gphotos-1.db-shm |
| | 36 | /data/data/com.google.android.apps.photos/databases/gphotos-1.db-wal (524288 bytes) |
| | 37 | failed getting file: gpnotos-i.ab-wai |
| | 39 | Failed getting file: wher data |
| | 40 | /data/data/com.viber_voip/databases/viber_data-journal_(123632_bytes) |
| | 41 | Failed getting file: viber data-journal |
| | 42 | /data/data/com.viber.voip/databases/viber messages (323584 bytes) |
| | 43 | Failed getting file: viber messages |
| | 44 | /data/data/com.viber.voip/databases/viber_messages-journal (29240 bytes) |
| | 45 | Failed getting file: viber_messages-journal |
| | 46 | /data/system/locksettings.db (20480 bytes) |
| | 47 | /data/system/locksettings.db-shm (32768 bytes) |
| | 48 | /data/system/locksettings.db-wal (173072 bytes) |
| | 49 | Failed getting file: locksettings.db-wal |
| | 50 | Extracting data from source |
| | 51 | Decoding extracted data |
| | 52 | Decoding locksettings.db using LocksettingsDecoder |
| | 53 | Generating HIML report |
| | 54 | Generating XLSX report |
| | 55 | finished. |

Εικόνα 154 - Andriller Full Log File

Τελειώνοντας την διαδικασία παρατηρούμε ότι το Andriller έχει αποτύχει να κάνει recover σχεδόν όλες τις βάσεις δεδομένων (Εικόνα 153, Εικόνα 154). Πιθανώς εξαιτίας των αλλαγών που έχουν γίνει στα android 10 με την χρήση του scoped storage και των νέων permissions ή εξαιτίας της μη επαρκούς υποστήριξης των file systems της συσκευής. Αξίζει να αναφέρουμε ότι στο χρονικό διάστημα που έχει πραγματοποιηθεί η έρευνα της διπλωματικής στο documentation του προγράμματος δεν αναφέρεται κάτι για το συγκεκριμένο πρόβλημα.

Στον φάκελο των αποτελεσμάτων βλέπουμε ότι το Andriller έχει φτιάξει ένα report επιπρόσθετα από τον φάκελο data στον οποίο έχουν αποθηκευτεί οι βάσεις και τα αρχεία που κατάφερε να κάνει recover το πρόγραμμα (Εικόνα 155).

| | esults andriller_extraction_20. | 21-01-19_18.24.34 > | | | | 140. BP1 |
|----------------------|---|-----------------------|------------------|------------------|---------|----------|
| Οργάνωση 👻 Συμπερ | ίληψη στη βιβλιοθήκη 🔻 🛛 Κ | ίοινή χρήση με 🔻 🛛 Εγ | γραφή Νέος φ | άκελος | | |
| 🔆 Αγαπημένα | Όνομα | н | μερομηνία τροπ | Τύπος | Μέγεθος | |
| 😌 Dropbox | 퉬 data | 19 | 9/1/2021 6:36 µµ | Φάκελος αρχείων | | |
| 🧮 Επιφάνεια εργασίας | 📜 DataStore.tar | 19 | 9/1/2021 6:36 µµ | WinRAR archive | 90 KB | |
| 鷆 Λήψεις | DataStore.tar.md5 | 19 | 9/1/2021 6:36 µµ | Αρχείο MD5 | 1 KB | |
| 💹 Πρόσ.θέσεις | REPORT.html | 19 | 9/1/2021 6:36 µµ | Chrome HTML Do | 5 KB | |
| 📑 Έγγραφα | REPORT.xlsx | 19 | 9/1/2021 6:36 µµ | Φύλλο εργασίας τ | 6 KB | |
| | | | | | | |

Εικόνα 155 - Andriller Results 1

Ανοίγοντας το REPORT αρχείο βλέπουμε ότι το Andriller μας παρέχει κάποιες γενικές αναγνωριστικές πληροφορίες για την συσκευή (Εικόνα 156).

This report was generated using Andriller CE # (This field is editable in Proferences)

| | [|
|--------------------------|--|
| Туре | Data |
| Serial | R58M |
| Status | device |
| Permisson | root-su |
| Ro.Build.Version.Release | 10 |
| Ro.Build.Display.Id | QP1A.190711.00 |
| Wifi <mark>Ma</mark> c | 8e:22:0 |
| Local_Time | 2021-01-19 18:24:34 000000000000000000000000000000000000 |
| Device_Time | 2021-01-19 18:24:33 EET |
| Currentsimserialnumber | 89300500 |
| Currentsimoperatorname | vodafone GR |
| Previoussimserialnumber | null |
| Previoussimphonenumber | null |
| Accounts | com.google: ptyxiakidummy@gmail.com com.microsoft.office: Office com.osp.app.signin: ptyxiakidummy@gmail.cor |

Εικόνα 156 - Andriller Report

Πέρα όμως από τις πληροφορίες που παρέχονται στο REPORT αρχείο και το andriller δεν κατάφερε να κάνει recover τις βάσεις δεδομένων με τις πληροφορίες που μας ενδιαφέρουν (Εικόνα 157).

| 😋 🔿 🔻 🕨 andriller resu | Ilts • andriller_extraction_2021-01-19_18. | 24.34 🕨 data | - | |
|------------------------|--|---------------------|---------------|---------|
| Οργάνωση 👻 Συμπερίλη | ψη στη βιβλιοθήκη 🔻 🛛 Κοινή χρήση μ | με 🕶 Εγγραφή Νέος φ | άκελος | |
| 🛯 🔆 Αγαπημένα | Όνομα | Ημερομηνία τροπ | Τύπος | Μέγεθος |
| 👯 Dropbox | Iocksettings.db | 19/1/2021 6:36 μμ | Αρχείο DB | 20 KB |
| 🧾 Επιφάνεια εργασίας | locksettings.db-shm | 19/1/2021 6:36 μμ | Αρχείο DB-SHM | 32 KB |
| 〕 Λήψεις | locksettings.db-wal | 19/1/2021 6:36 μμ | Αρχείο DB-WAL | 0 KB |
| 彊 Πρόσ.θέσεις | mmssms.db-shm | 19/1/2021 6:29 μμ | Αρχείο DB-SHM | 32 KB |
| 🖹 Έγγραφα | | | | |
| | | | | |

Εικόνα 157 - Andriller Recovered Files

7. ΣΥΜΠΕΡΑΣΜΑΤΑ-ΕΠΙΛΟΓΟΣ

Τα android 10 έχουν εισαγάγει νέα security features. Αναλυτικότερα έχει υιοθετηθεί νέος τρόπος διαχείρισης των permissions που παίρνουν οι εφαρμογές πάνω στην συσκευή και το scoped storage που δίνει νέο τρόπο αποθήκευσης δεδομένων στην συσκευή. Οι συγκεκριμένες αλλαγές έχουν ως σκοπό την προστασία της ιδιωτικότητας των χρηστών.

Μεγάλο ενδιαφέρον παρουσιάζει το γεγονός ότι τα open source εργαλεία για mobile forensics που είναι διαθέσιμα δεν έχουν καταφέρει ακόμα να προσαρμοστούν στις συγκεκριμένες αλλαγές και στον τρόπο αποθήκευσης και διαχείρισης των δεδομένων στην συσκευή που χρησιμοποιεί android 10. Επιπρόσθετα παρουσιάζουν ανεπαρκή στήριξη σε ό,τι αφορά τα file systems.

Μέσα από την έρευνα παρατηρήσαμε πως σε ό,τι αφορά το logical επίπεδο το AFLogical δεν είναι αποδοτικό καθώς δεν είναι προσαρμοσμένο στα android 10 και πρέπει να πραγματοποιήσουμε επιπρόσθετο export πληροφοριών κατευθείαν από την συσκευή.

To free trial του FonePaw είναι αποδοτικότερο συγκριτικά με το AFLogical σε σχέση με τις πληροφορίες που μπορεί να κάνει recover από την συσκευή όμως δεν μας δίνει την δυνατότητα να κάνουμε export κάποιες από αυτές τις πληροφορίες στο workstation μας.

Επομένως οι λύσεις που εξετάσαμε για ανάλυση σε logical επίπεδο μας παρέχουν ικανοποιητικά αποτελέσματα. Για να έχουμε την μέγιστη απόδοση σε logical επίπεδο χωρίς να πρέπει να κάνουμε manual export από την συσκευή που ερευνάται και να μπορούμε να κάνουμε export πληροφορίες ενδιαφέροντος στο workstation μας θα πρέπει να στραφούμε σε κάποια επί πληρωμή λύση.

Η ανάλυση σε physical επίπεδο του image του κινητού δεν ήταν επιτυχής καθώς το autopsy δεν μπορεί να φτάσει στα δεδομένα που είναι αποθηκευμένα στις βάσεις εφόσον δεν είναι προσαρμοσμένο στις αλλαγές που έχουν συμβεί στα android 10 και δεν παρέχει ικανοποιητική υποστήριξη των file systems της συσκευής. Το andriller παρουσιάζει και αυτό το ίδιο πρόβλημα.

Συνεπώς κάποιος για να επιτύχει forensics ανάλυση σε physical επίπεδο, χρησιμοποιώντας ελεύθερα διαθέσιμες λύσεις στο κοινό, θα πρέπει να κάνει export των βάσεων δεδομένων κατευθείαν από την κινητή συσκευή σε micro sd card και στην συνέχεια να πάρει τις βάσεις στο workstation του. Η συγκεκριμένη διαδικασία δεν θεωρείται δόκιμη σε ό,τι αφορά τις σωστές πρακτικές forensics και δεν είναι αποδοτική καθώς το android χρησιμοποιεί πολλές βάσεις για να αποθηκεύσει δεδομένα. Εναλλακτικά για μια επιτυχημένη ανάλυση σε physical επίπεδο κάποιος θα πρέπει να στραφεί σε επί πληρωμή λύση, μέχρι τα open source εργαλεία να προσαρμοστούν στις αλλαγές των android 10 και να παρέχουν επαρκή στήριξη των file systems που μπορεί κανείς να συναντήσει σε κινητές συσκευές.

Με τα android 11 να υπάρχουν ήδη από τις 19 Φεβρουαρίου 2020 στην αγορά είναι πολύ σημαντική η προσαρμογή των open source εργαλείων για mobile forensics στις αλλαγές που έχουν φέρει τα android 10 καθώς πρέπει να παρέχεται και στο ευρύ κοινό γνώση για το τι αποθηκεύεται πραγματικά στις κινητές συσκευές που χρησιμοποιεί.

ΧΡΗΣΙΜΑ LINKS

https://play.google.com/store/apps/details?id=com.joeykrim.rootcheck&hl=en

https://www.androidinfotech.com/root-samsung-galaxy-sm-a705-a70-android-10/

https://www.androidinfotech.com/download-odin-all-versions/

https://www.sammobile.com/samsung/galaxy-a70/firmware/SM-

A705FN/EUR/download/A705FNXXU5BTJ4/536942/? cf_chl_jschl_tk =e06ec8c054be384 63512e18b89437a22b7931f1e-1609857939-0-

AcZKhGcLJognsRLRQfUu04LNf3g6h5llZJIx3bqfT8pNgkfDi_nKo3Vrl8i_75muTOeCU1y68KXQpg 7 CS8el29YxXhJo3ClRp3 qKP7RJ8GCqLQ-wCuqKbwK1hKAeCPKagD Msm-

8I9YM6dDgnAPfjnvSV7s48kHfaUlizWUpBgoPqa3ulJsf-

hkE7ZD5fOicbZEe4q8voF4UU0Q9gxL5YADxfT07DOEV9Sje3jT-

x2t1qVdKKalfqRsCHIJfN5bXsrwv9aRnoD6vdMLCbWviURml__JGSAphyJTNZyArkBByTnINmar MxMwI0TObjtChiy9_hMmcKQx9MjG3r-

GxV1FdCZBQnb80MZ0fPJdOpzSuAHloIPZWVZjpZuBTC1MQ-Fd4eU4LdaG49ULvPmV6A

https://www.androidinfotech.com/samsung-galaxy-usb-driver-all-versions/

https://www.androidinfotech.com/magisk-versions-download/

https://magiskmanager.com/

https://www.samsungknox.com/en/about-knox

https://www.cellebrite.com/en/cas-supported-devices/

https://santoku-linux.com/

https://www.fonepaw.com/

https://play.google.com/store/apps/details?id=stericson.busybox&hl=en

https://www.unixmen.com/play-with-netcat-in-ubuntu/

https://www.youtube.com/watch?v=UQYuaOC5v0I&list=PL3dfduuyhbBcFrg7-TPKis1RExcYWrXd0&index=5&t=977s

https://www.sleuthkit.org/autopsy/

https://www.sleuthkit.org/autopsy/desc.php

https://www.sleuthkit.org/autopsy/features.php

https://github.com/den4uk/andriller

https://sleuthkit.discourse.group/t/android-image-cannot-define-file-system-type/1709

ΒΙΒΛΙΟΓΡΑΦΙΚΕΣ ΑΝΑΦΟΡΕΣ

Android Developers, 2020. *Android Developers*. [Ηλεκτρονικό] Available at: <u>https://developer.android.com/about/versions/10/privacy/changes</u> [Πρόσβαση January 2021].

Ansari, M., 2020. *Medium*. [Ηλεκτρονικό] Available at: <u>https://medium.com/codixlab/what-is-the-difference-between-android-9-and-android-10-500b6e5bb991</u> [Πρόσβαση January 2021].

Bommisetty, S., Tamma, R. & Mahalik, H., 2014. Practical Mobile Forensics. s.l.:s.n.

Brunty, J., 2016. Mobile Forensics: An Introduction. Virginia, s.n.

Casey, E., 2011. Digital Evidence and Computer Crime Forensic Science, Computers and the Internet. 3η Έκδοση επιμ. s.l.:s.n.

Cellebrite, 2021. *Cellebrite*. [Ηλεκτρονικό] Available at: <u>https://www.cellebrite.com/en/cas-supported-devices/</u> [Πρόσβαση January 2021].

Davenport, C., 2020. Android Police. [Ηλεκτρονικό] Available at: <u>https://www.androidpolice.com/2020/05/12/10-android-10-features-to-look-for-when-your-phone-gets-updated/</u> [Πρόσβαση January 2021].

Dwivedi, H., 2020. *Heartbeat.* [Ηλεκτρονικό] Available at: <u>https://heartbeat.fritz.ai/implementing-scoped-storage-in-android-10-4b657280c066</u> [Πρόσβαση January 2021].

Gillware, n.d. *Gillware.* [Ηλεκτρονικό] Available at: <u>https://www.gillware.com/phone-data-recovery-services/samsung-forensics/</u> [Πρόσβαση January 2021].

Goyal, G., 2020. *Medium*. [Ηλεκτρονικό] Available at: <u>https://medium.com/microsoft-mobile-engineering/scoped-storage-in-android-10-android-11-28d58d989f3c</u> [Πρόσβαση January 2021].

Hazra, S. & Mateti, P., 2017. *ResearchGate*. [Ηλεκτρονικό] Available at: <u>https://www.researchgate.net/publication/320952681_Challenges_in_Android_Forensics</u> [Πρόσβαση January 2021]. Hindy, J., 2019. Android Authority. [Ηλεκτρονικό] Available at: <u>https://www.androidauthority.com/android-10-permissions-1040121/</u> [Πρόσβαση January 2021].

Hoog, A., 2013. *APPSEC USA*. [Ηλεκτρονικό] Available at: <u>https://2013.appsecusa.org/2013/wp-content/uploads/2013/12/viaForensics-</u> <u>AppSecUSA-Nov-2013.pdf</u> [Πρόσβαση January 2021].

Kostadinov, D., 2019. *INFOSEC*. [Ηλεκτρονικό] Available at: <u>https://resources.infosecinstitute.com/category/computerforensics/introduction/mobile-forensics/the-mobile-forensics-process-steps-types/#gref</u> [Πρόσβαση January 2021].

Lin, Y., 2020. *OBERLO*. [Ηλεκτρονικό] Available at: <u>https://www.oberlo.com/blog/mobile-usage-statistics</u> [Πρόσβαση January 2021].

Matei, A., 2019. *The Guardian*. [Ηλεκτρονικό] Available at: <u>https://www.theguardian.com/lifeandstyle/2019/aug/21/cellphone-screen-time-average-habits</u> [Πρόσβαση January 2021].

Nunez, S., 2020. *INSIGHTS - SAMSUNG*. [Ηλεκτρονικό] Available at: <u>https://insights.samsung.com/2020/08/07/your-phone-is-now-more-powerful-than-your-pc-2/</u> [Πρόσβαση January 2021].

Ranjan Roy, N., Kanchan Khanna, A. & Aneja, L., 2016. *ResearchGate.* [Ηλεκτρονικό] Available at: <u>https://www.researchgate.net/publication/312559420_Android_phone_forensic_Tools_and</u>

<u>techniques</u>

[Πρόσβαση January 2021].

Samsung, n.d. *Samsung Knox*. [Ηλεκτρονικό] Available at: <u>https://docs.samsungknox.com/admin/whitepaper/kpe/remote-control.htm</u> [Πρόσβαση January 2021].

Singh, A., 2020. *raywenderlich*. [Ηλεκτρονικό] Available at: <u>https://www.raywenderlich.com/9577211-scoped-storage-in-android-10-getting-started</u> [Πρόσβαση January 2021].

Skulkin, O., Tindall, D. & Tamma, R., 2018. Learning Android Forensics. s.l.:s.n.

Solution Analysts, 2020. *Solution Analysts*. [Ηλεκτρονικό] Available at: <u>https://www.solutionanalysts.com/blog/scoped-storage-in-android-10/</u> [Πρόσβαση January 2021].

Soufiane, T., 2016. Mastering Mobile Forensics. s.l.:s.n.

Spajic, D. J., 2020. *Kommando Tech*. [Ηλεκτρονικό] Available at: <u>https://kommandotech.com/statistics/how-much-time-does-the-average-person-spend-on-their-phone/</u> [Πρόσβαση January 2021].

statcounter, 2019 - 2020. *statcounter*. [Ηλεκτρονικό] Available at: <u>https://gs.statcounter.com/os-market-share/mobile/worldwide</u> [Πρόσβαση January 2021].

statcounter, 2019-2020. *statcounter*. [Ηλεκτρονικό] Available at: <u>https://gs.statcounter.com/vendor-market-share/mobile</u> [Πρόσβαση January 2021].

statista, 2020. *statista*. [Ηλεκτρονικό] Available at: <u>https://www.statista.com/statistics/245501/multiple-mobile-device-ownership-worldwide/</u> [Πρόσβαση January 2021].

VisiHow, n.d. *VisiHow*. [Ηλεκτρονικό] Available at: <u>https://visihow.com/Use_the_Permission_Manager_in_Android_10</u> [Πρόσβαση January 2021].

Vivek, 2019. *DroidViews*. [Ηλεκτρονικό] Available at: <u>https://www.droidviews.com/debloater-magisk-module-uninstall-system-apps-android/</u> [Πρόσβαση January 2021].

Wallen, J., 2019. *TechRepublic*. [Ηλεκτρονικό] Available at: <u>https://www.techrepublic.com/article/how-to-use-the-new-app-permissions-in-android-10/</u> [Πρόσβαση January 2021].