Leggere la cenere: acquisizione e analisi dopo un factory reset

DIGITAL FORENSICS LAB
UNIVERSITY OF PAVIA

Milano, 16 marzo 2022

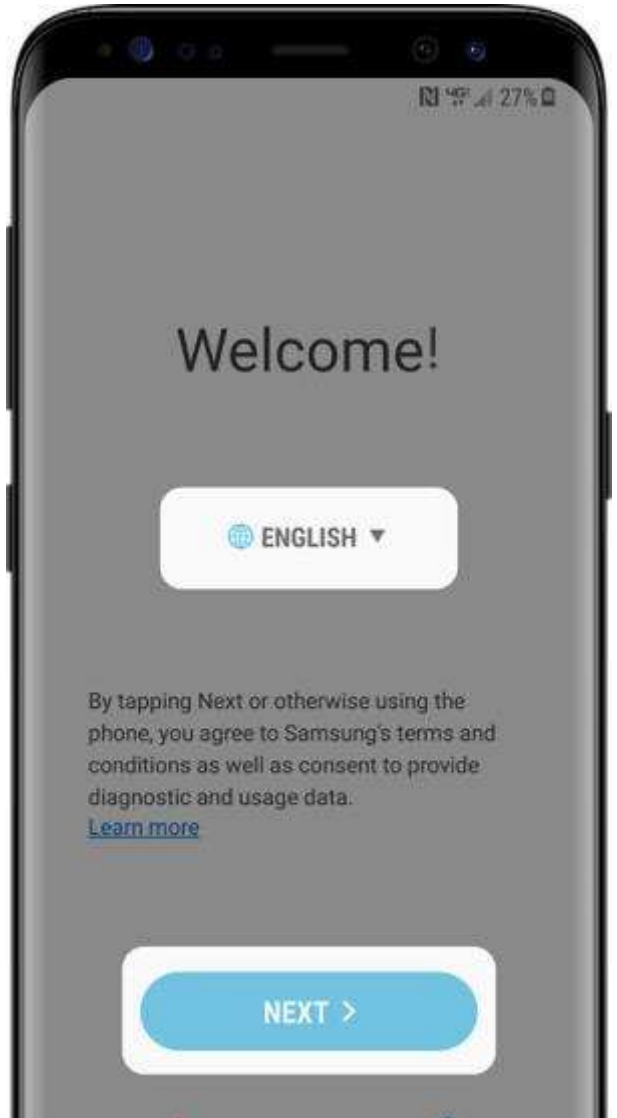
Chi vi parla

Davide ‘Rebus’ Gabrini

- Professore a contratto in Informatica e Sicurezza Informatica presso il Dipartimento di Giurisprudenza dell’Università degli Studi di Pavia, A.A. 2021/2022
- Collaboratore del Laboratorio di Informatica Forense dell’Università degli Studi di Pavia, afferente al Laboratorio Nazionale di Cyber Security
- Membro del Comitato Scientifico dell’Area di Diritto e Informatica del Centro Ricerca e Didattica Universitaria del Collegio Ghislieri di Pavia
- Contributor di Tsurugi Linux
- Project Manager di Bento
- Socio fondatore di Inclusive Hacker Framework, già *Italian Gr.A.P.P.A.*
- Socio fondatore del Linux User Group di Pavia
- Curatore della newsletter Rebus’ Digest

Hello!

- Questo non è un buon giorno per un analista...



Cosa possiamo fare per recuperare i dati?

Niente.

Grazie per l'attenzione!

Agenda

- Factory reset
  - Locale, remoto, programmato
- Factory Reset Protection
- Tracce residue
  - Filesystem cifrati
  - Acquisizione log di sistema
- Analisi dei log
  - Log Android
  - Log iOS
- Case study
  - Hack della FRP di Android

Factory reset

Cos'è il Factory Reset

- Ripristino del dispositivo alle condizioni di fabbrica
  - Cancellazione applicazioni, dati, configurazioni
- Analogo a una formattazione, ma peggio :p
- Buona pratica prima di una dismissione, restituzione, cessione, vendita…
- Utile misura di contenimento in caso di furto o smarrimento
- Utilissimo metodo di anti-forensics ☹

Cos'è il Factory Reset

- Quando viene avviato un factory reset, il sistema esegue numerose azioni, alcune delle quali producono log
- Soprattutto il primo boot eseguito dopo il factory reset causa la registrazione di log utili
- Da tali log può risultare il metodo impiegato e il momento in cui è stato eseguito il factory reset
- In mancanza di meglio, queste informazioni possono suggerire il coinvolgimento dell'utente e le sue motivazioni

Remote Factory Reset

- Perché avvenga un reset da remoto, devono verificarsi condizioni favorevoli (che andrebbero prevenute):
  - Dispositivo acceso
  - Disponibilità di collegamento a Internet
  - Accesso a un account registrato in precedenza
    - Da entrambe le parti
  - Funzioni di gestione remota configurate in precedenza

Modalità per il Factory reset – Android

- Da locale
  - Impostazioni > Gestione generale > Ripristina > Ripristina dati di fabbrica
  - Da Recovery
- Da remoto
  - Google Find My Device
    - Attivabile da Android 2.2 (dicembre 2013)
  - Google Family Link
  - Samsung Find My Mobile
  - Huawei Find My Phone, Mi Cloud Find Device ecc.
  - MDM (Mobile Device Management)
- Automaticamente
  - Impostazioni > Schermata di blocco > Impostazioni blocco sicuro > Ripristino impostazioni automatiche (dopo 15 accessi falliti)

Modalità per il Factory reset – iOS

- Da locale
  - Impostazioni > Generali > Trasferisci o inizializza iPhone > Inizializza contenuto e impostazioni
- Da remoto
  - Da iOS 4.2 (novembre 2010)
  - iCloud
  - MDM
- Automaticamente
  - Impostazioni > [Touch ID|Face ID] e codice > Inizializza dati (dopo 10 accessi falliti)

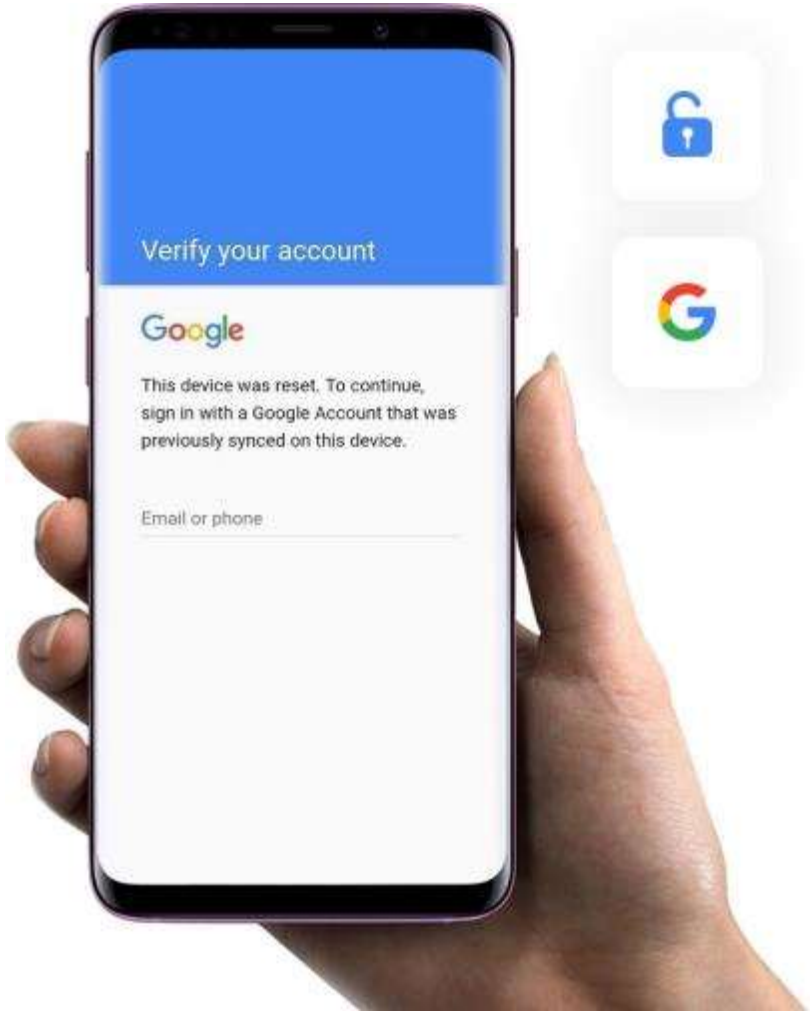
Bonus tip: iPhone disabilitati

- Se l'utente non ha configurato il factory reset, per impostazione di default dopo 10 inserimenti errati del PIN il dispositivo si pone in stato "disabilitato"
- Cracking degli iPhone disabilitati:
  - versione di iOS < 12
    le chiavi di cifratura non sono state distrutte, quindi essiste possibilità di cracking
  - Versione di iOS >= 12
    le chiavi di cifratura vengono distrutte, quindi non esiste speranza di cracking

Davvero tutto perso?

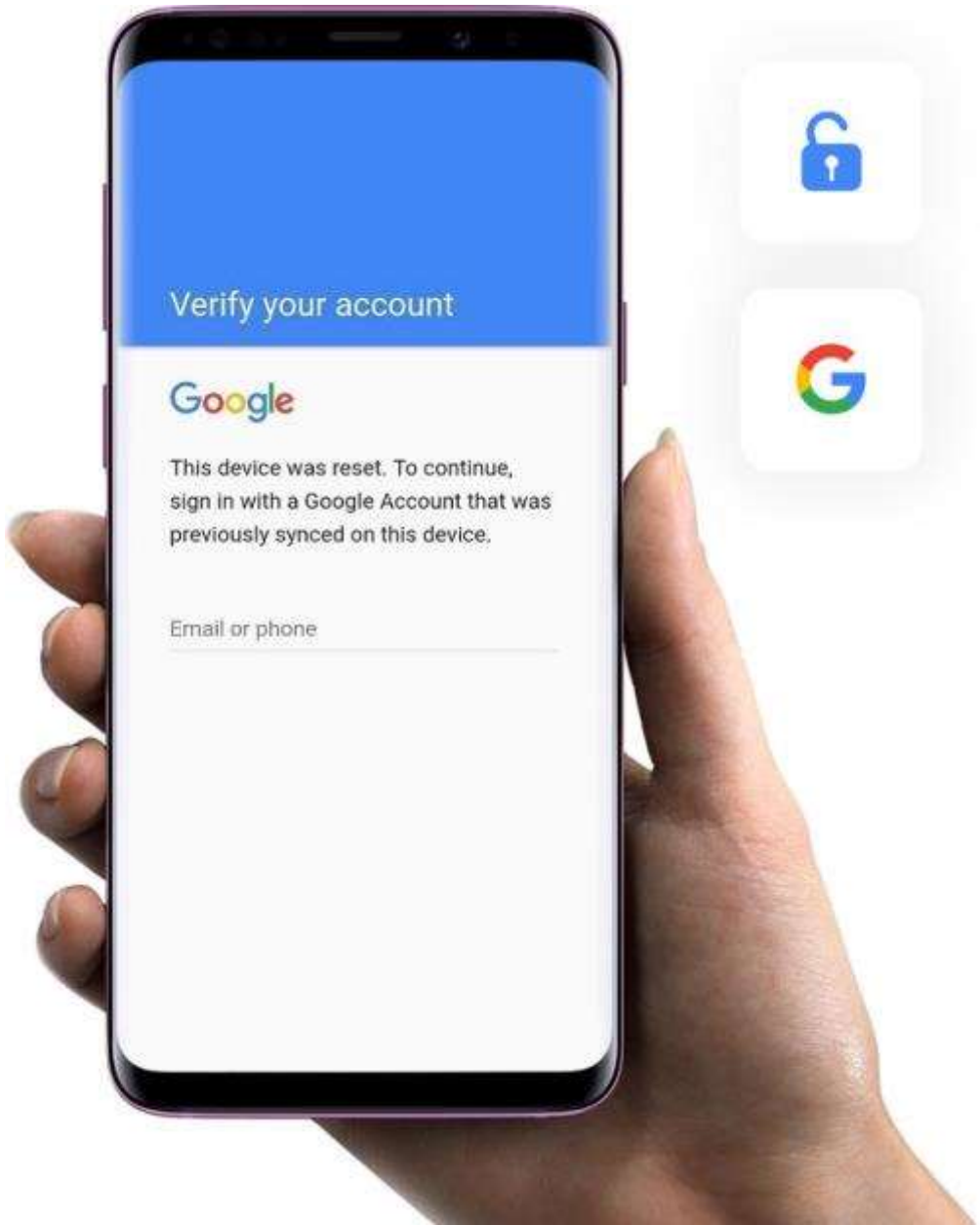
- C'è stato un tempo in cui i filesystem erano in chiaro
- Potendo eseguire un dump fisico, si poteva tentare il carving nell'area deallocata
- Anche in presenza di **Full Disk Encryption** si potrebbe fare carving, a patto di avere la chiave di decrittazione
  - ...che però viene distrutta dal Factory Reset
- Con i filesystem cifrati con **File Based Encryption**, ogni speranza è vana:
  - le chiavi necessarie non ci sono più
  - anche un dump fisico sarebbe inutile

Factory Reset Protection



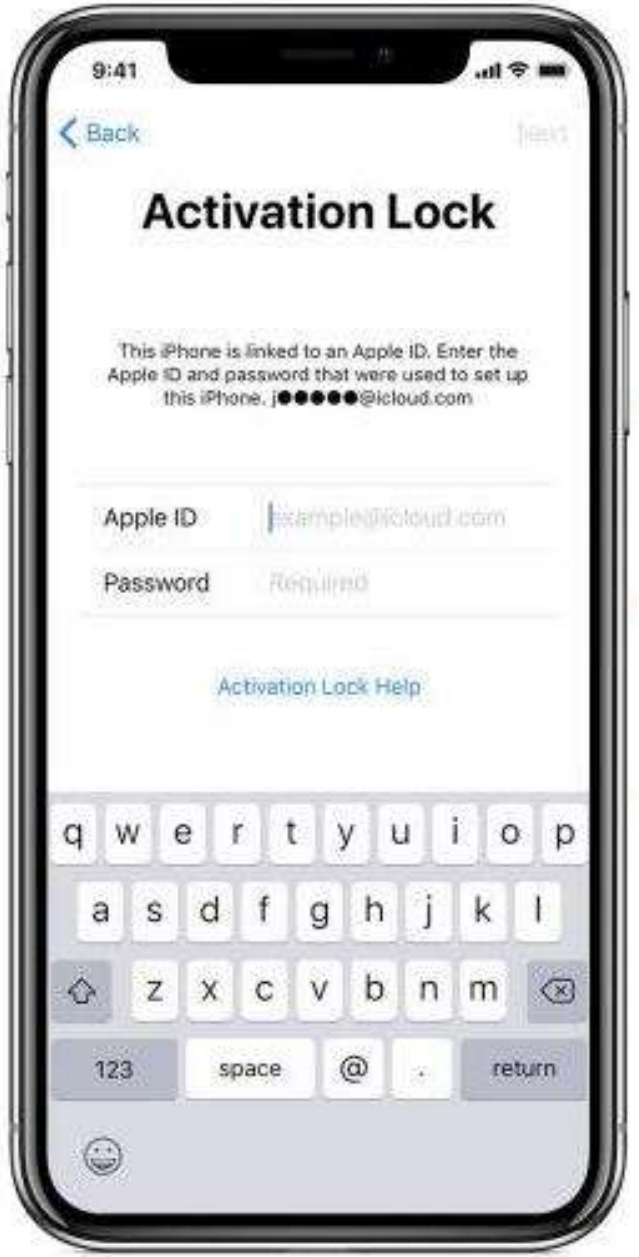
Factory Reset Protection – Android

- Introdotto da Android 5.1 (feb 2015)
- Automatico, in presenza di
  - Un account registrato
  - Un passcode



Factory Reset Protection – iOS

- Da iOS 6 (settembre 2012)
- Particolarmente accurato:
  - Blocco bootloader
  - Secureboot chain
  - Attivazione on-line obbligatoria
  - Nessun by-pass noto



What Do I Do Now

Log di Android

- Partizioni USERDATA, CACHE e EFS
- La presenza dei file, il loro nome e persino il contenuto può variare a seconda dello specifico *environment*
  - Produttore, versione di Android, aggiornamenti installati…
- USERDATA
  - /log/recovery.log
  - /log/recovery_history.log
  - /log/recovery_extra_history.log
- CACHE
  - /recovery/last_log.#
  - /recovery/last_history
  - /recovery/last_extra_history
- EFS
  - /recovery/last_history
  - /recovery/last_extra_history
- Serve un'estrazione fisica o full filesystem

Log di iOS

- Nessuno ☺
- Tuttavia, la creazione di alcuni file e alcuni eventi in essi registrati possono far desumere informazioni sul reset
- Normalmente, l'interazione col dispositivo è possibile solo completando la configurazione iniziale
  - Paese, lingua, rete, FRP…
- Se il device è vulnerabile a checkm8, è possibile acquisire l'intero filesystem, e quindi tutti i log
  - L'esecuzione di un *sysdiagnose* prima del dump non aggiunge informazioni, ma può essere utile a organizzarle
- Sia l'estrazione FFS che il backup iTunes consentono di stimare il momento del factory reset

sysdiagnose

- La funzione Sysdiagnose permette di generare dei log acquisibili poi in *user space*
- Sono informazioni già presenti in log di sistema, ma normalmente non esposte e acquisibili solo con accesso FFS
  - premere i pulsanti Vol Up + Vol Down + Power
  - mantenerli premuti 1-1.5 secondi
  - rilasciare i pulsanti
- Si avverte una vibrazione e dopo pochi minuti i report generati sono disponibili in Settings > Privacy > Analytics > Analytics Data, o in una cartella acquisibile con iTunes o altri strumenti
- Per esportare i file occorre comunque completare l'inizializzazione e il pairing
  - Da iOS 8, il Factory Reset revoca i certificati di lockdown
- In presenza di FRP si può solo sperare in un accesso FFS (checkm8)

Analisi dei log

Android

- I log *recovery history* riportano la modalità del reset:

Evento registrato	Modalità di reset associata
MasterClearConfirm	da menù Impostazioni
Find My Device wiping device remotely	Google Find My Device
DevicePolicyManager.wipeData[…] from com.google.android.gms/.mdm.receivers.MdmDeviceAdminReceiver	Google Find My Device
DevicePolicyManager.wipeData[…] from [nomeApp]	MDM di terze parti
FamilyLinkManager wiping device remotely	Google Family Link
Fmm.RemoteWipeOut	Samsung Find My Device:
ResetDeviceUtils_FACTORY_RESET,attractsCount=15	Reset automatico
CryptKeeper.showFactoryReset()corrupt=4	Reset automatico

- Per ogni evento sono riportati data e ora in formato ISO8601 (Zulu time)
- Il Factory Reset eseguito da *recovery* non viene riportato in questi log

Samsung

- /efs/recovery/history
  - Mantiene una cronologia persistente dei reset
  - Disponibile solo in copie fisiche o FFS

```
+ [oj | 2021/08/10 11:39:52 | A305GUBU4BTC8]
--wipe_data
--requested_time=2021/08/10 07:39:27.062
--reason=MasterClearConfirm,2021-08-10T07:39:27Z
--locale=en-US
RP
reboot_reason=Reboot:1382 RecoverySystemMasterClearConfirm,2021-08-10T07:39:27Z
[S]    22.4G
[E]    22.4G
_
```

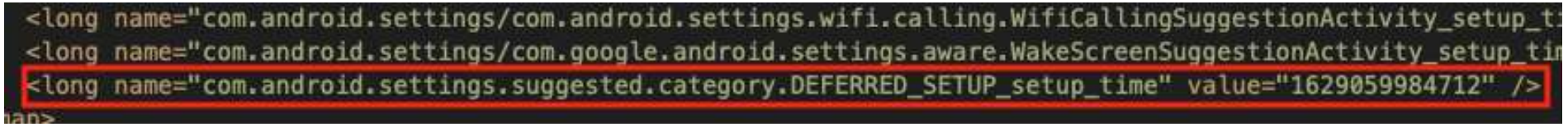
```
+ [tr | 2021/08/18 19:48:33 | A305GUBU4BTC8]
NP
reboot_reason=BL:Recovery Mode Set by key
[S]    22.4G
[E]    22.4G
_
+ [OZ | 2021/08/18 19:49:55 | A305GUBU4BTC8]
RP
reboot_reason=UNKNOWN
[S]    22.4G
[E]    22.4G
_
```

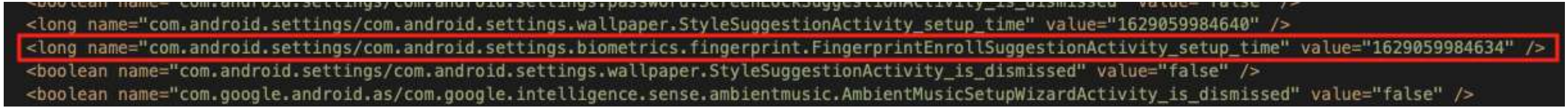
- /data/system/users/service/data/eRR.p

```
2021-08-15 16:59:40-0400 |  REBOOT  |       | REASON: recovery

2021-08-15 18:16:04-0400 |    ON    | RP    | A305GUBU4BTC8

2021-08-18 08:08:59-0400 |  REBOOT  |       | REASON: userrequested

2021-08-18 14:41:20-0400 |    ON    | RP    | A305GUBU4BTC8

2021-08-18 14:42:06-0400 |  REBOOT  |       | REASON: adb
```

Altri riscontri

- File **suggestions.xml**
  - Android 10 e 11
    - /data/data/com.google.android.settings.intelligence/shared_prefs
  - Android 11
    - /data/user/%USER%/com.google.android.settings.intelligence/shared_prefs
- Valori (timestamp Epoch) impostati per:
  - com.android.settings.suggested.category.DEFERRED_SETUP_setup_time
  - com.android.settings/com.android.settings.biometrics.fingerprint.FingerprintEnrollSuggestionActivity_setup_time





Altri riscontri

- /data/user/%USER%/com.google.android.settings.intelligence/shared_prefs/**setup_wizard_info.xml**
  - tag suw_finished_time_ms, valore Epoch
- /data/property/**persistent_properties**
  - Evento reboot,factory_reset , a cui è associato un timestamp Epoch
  - Il file mantiene uno storico dei boot di sistema. Lo storico però non è illimitato: su alcuni modelli sono mantenuti soltanto gli ultimi 3 o 4 eventi. Quindi, se il dispositivo è riavviato più volte dopo il reset, l'evento "reboot,factory_reset" e il timestamp associato potrebbero non comparire nel log.
  - **Android Triage** raccoglie il dato tra le "Basic Information" del device (getprop.txt)
  - adb shell **getprop** (non servono privilegi di root)

Altri riscontri

- In /data/system/appops.xml
  - tag com.google.android.setupwizard
- Samsung usa una sua applicazione di setup
  - tag com.sec.android.SecSetupWizard
- E a proposito di Samsung
  - /data/data/com.sec.android.app.setupwizardlegalprovider/databases/swlpdb.db traccia nella tabella db_agreement quando l'utente accetta la EULA
  - Disponibile in acquisizioni Full logical e FFS

Altri riscontri

- Da Android 11
  - /data/misc/bootstat/factory_reset
  - File vuoto, il cui timestamp di ultima modifica indica il reset
  - Serve estrazione fisica/FFS
  - Anche il comando *adb shell bootstat -p* richiede privilegi di root
- Digital Wellbeing
  - /data/data/com.google.android.apps.wellbeing/databases/app_usage
- internal.db mantiene metadata sui file allocati nella memoria interna, incluso il timestamp relativo alla creazione dei file. Anche quelli di sistema.
  - /data/data/com.android.providers.media/databases
  - /data/user/%USER%/com.google.android.providers.media.module/database
  - /data/user/%USER%/com.android.providers.media.module/databases

iOS

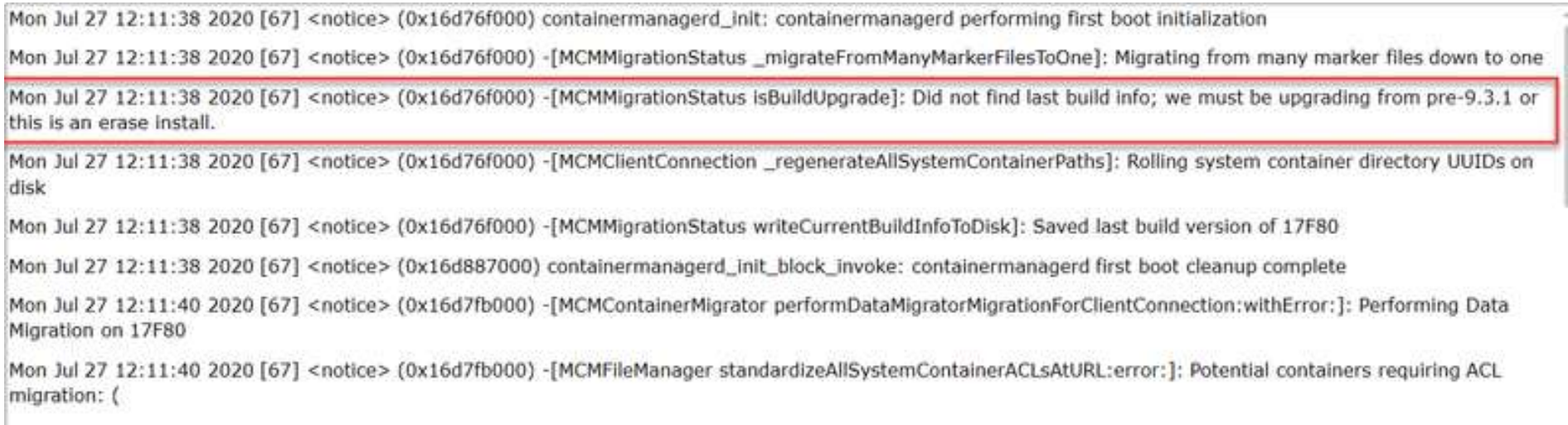
- File utili possono essere:
  - /private/var/root/.obliterated
  - com.apple.purplebuddy.plist
  - RoleUserMigration.Plist
  - PLdataMigrationinfo.Plist
  - Addressbook.sqlitedb, Call_History.storedata e altri db analoghi
- Sono file creati dopo il factory reset, e i loro timestamp di creazione documentano quindi il primo avvio successivo
  - Questo potrebbe non coincidere esattamente col reset
  - Eventi pur sequenziali possono essere distanziati nel tempo, e persino in diverse *timezone* a seconda dell'*environment*, per cui è raccomandabile confrontare tra loro più eventi

iOS

- /root/private/var/mobile/Library/Preferences/**com.apple.purplebuddy.plist**
  - Valore di GuessedCountry
  - È la prima cosa che il device fa dopo il reset
  - Occorre però verificare che il valore di SetupState sia SetupUsingAssistant
  - Se SetupState riporta RestoredFromiCloudBackup, allora il timestamp è riferito a un precedente reset.
  - Il file è presente nel backup iTunes

iOS

- Cartella /private/var/root/Library/Logs/MobileContainerManager
  - File containermanagerd.log.###
  - Più alto il numero, più vecchio il file
  - Il log annota la verifica, eseguita all'avvio, della versione di build avviata rispetto al boot precedente. Al primo boot dopo un reset però, non essendoci un valore precedente da confrontare, viene annotato un messaggio errore.
  - L'evento ha un timestamp (local time)
  - Il file stesso ha un timestamp di creazione



Altri riscontri utili

- /private/var/db/diagnostics/**logd.0.log**
  - Documenta l'aggiornamento della timezone (se diversa da PDT)
- Da CrashLogs o sysdiagnose:
  - \logs\MobileInstallation**mobile_installation.log.0**
    - Evento "*Did not find last build info; we must be upgrading from pre-8.0 or this is an erase install.*"
  - \logs\MobileLockdown**lockdown.log**
    - Evento "*_load_dict: Failed to load /private/var/root/Library/Lockdown/data_ark.plist.*"
  - \logs\powerlogs**powerlog_YYYY-MM-DD_XXXXXXXX.PLSQL**
    - Registra se e quando il dispositivo è stato in carica
  - \WiFi**wifi_scan_cache.txt**
    - Elenca le reti Wi-Fi (SSID e BSSID) rilevate dal dispositivo
- In caso di reset remoto, viene inviata un'email di conferma all'indirizzo associato all'ID Apple.

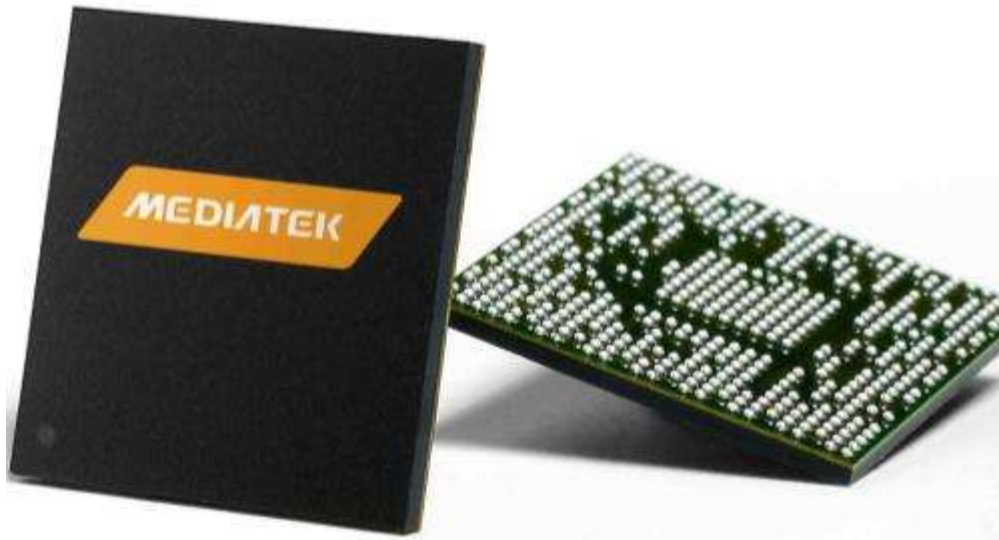

SUBJECT
RESEARCH
METHOD
KNOWLEDGE
CASE
STUDY
CRITERIA
CONCLUSION
EVIDENCE
DATA

Caccia agli IMEI

- Il caso riguarda uno smartphone Android resettato
- I dati sono persi, ma si vorrebbero conoscere almeno gli IMEI del dispositivo
- Esternamente si rileva marca e modello, ma non gli IMEI, nemmeno nell'alloggiamento delle SIM
- Non ci sono SIM
- All'avvio presenta il messaggio di benvenuto post Factory Reset, con richiesta di completare l'installazione
- Dal tastierino delle chiamate di emergenza, *#06# non funziona

Parliamo col chipset

- Secondo documentazione del costruttore, il device contiene un chipset MTK
  - Collegandolo da spento, Windows lo rileva come device MTK, ma non è noto nessun metodo specifico per ottenere un dump fisico
  - I metodi generici per chipset MTK non funzionano
  - Non che il dump fisico, in queste condizioni, abbia molte speranze di contenere da qualche parte gli IMEI…



Proviamo dalla recovery

- Avvio in recovery mode
- Accesso ai recovery logs
  - contengono tante informazioni sul dispositivo, incluso il seriale, ma non sembrano contenere gli IMEI
- Come prevedibile, la recovery stock non ha privilegi elevati e non espone informazioni utili
- Valutabile l'installazione di un'altra recovery, possibilmente con una shell e privilegi di root

Proviamo con fastboot

- Fastboot fortunatamente è disponibile, ma...
  - Impossibile flashare TWRP o simili perché il device è in condizione OEM locked
  - Esistono comandi per rimuovere OEM Lock via fastboot
    - causerebbe la perdita dei dati, ma non ci sono dati da perdere
  - Ogni comando tentato per rimuovere OEM Lock o estrarre informazioni si risolve in "unknown command"

Torniamo a parlare con Android

- Torno ad Android, deciso a proseguire l'inizializzazione
  - è obbligatorio prima configurare un accesso a Internet via WiFi
  - poi è richiesta autenticazione con l'account Gmail preesistente, o col numero di telefono. Entrambi i dati sono ignoti.
  - Collegato a Windows, è riconosciuto come device Android, ma l'accesso è precluso perché Android ancora non è configurato
  - Via MTP viene esposto solo il seriale, già noto
- Idee?
  - Chiamo un numero di emergenza e poi chiedo i tabulati?
  - Installo un IMSI catcher?
  - Chiedo al costruttore se dal seriale mi sa dire gli IMEI?

1) TalkBack

- Ho sfruttato il servizio TalkBack
  - TalkBack è lo screen reader di Google integrato nei dispositivi Android. Una voce sintetizzata legge il contenuto del display. Essendo utile per utenti disabili, la funzione è disponibile anche prima dell'attivazione.
  - Per attivarlo, in assenza di accesso al menù impostazioni, si può premere 3 volte il pulsante Home, o entrambi i tasti Volume
  - Tracciando sul touchscreen il segno di una L si apre il menù contestuale
  - Da qui si accede a "Talkback settings"
  - Da qui si può accedere alla guida: "Help and feedback"
  - Si individua una pagina della guida che integri un video tutorial
  - Si tratta di video YouTube, quindi avviando la riproduzione è poi possibile usare il menù contestuale per lanciare la app YoutTube

2) YouTube

- Dalla app YoutTube, si può chiedere dal menù contestuale di eseguire il login
- Dalla pagina di login si può chiedere di leggere prima le condizioni d'uso del servizio e l'informativa privacy
- Viene così avviata la app Chrome
  - La barra degli indirizzi ora è attiva
    - (nelle schermate di login precedenti era opportunamente disattivata)

3) Chrome

- Con un browser e un accesso a Internet, si può fare tutto:
  - Visitare un sito come addrom.com/bypass
  - Scaricare un pacchetto apk come Setting.apk
  - Aprirlo dalla finestra Download di Chrome
- Il sistema avverte che non si dispone delle autorizzazioni per installare apk in questo modo…
  - …ma offre contestuale accesso alla configurazione per autorizzare l'operazione
- Finita l'installazione viene servito anche il pulsante Open
  - L'apk che ho scelto apre il pannello Settings, da cui possono essere lette le informazioni sul dispositivo e quindi gli IMEI
  - Ci sono anche apk specifici per rimuovere FRP, ma ormai ho l'informazione che mi serviva.

Fonti

- "*Top 10 FRP bypass tools to bypass Google account verification*", Jihosoft, jan 2022
- "*Factory reset (iOS/Android)*", HancomWITH whitepaper, dec 2021
- "*Wipeout! Detecting Android Factory Resets*", J.Hickman, aug 2021
- "*Upgrade from NULL - Detecting iOS wipe artifacts*", H.Mahalik e I.Whiffin, jun 2021
- "*Oh no! I have a wiped iPhone, now what?*", M.Epifani, may 2021
- "*How to extract sysdiagnose logs for forensic purposes on iOS*", A.Fortuna, oct 2020
- "*The iPhone's forensic workflow: steps to access critical evidence*", Elcomsoft, nov 2019
- "*sysdiagnose Logging Instructions*", Apple, 2018

Teniamoci in contatto...

Davide Rebus Gabrini

e-mail: davide.gabrini@unipv.it

GPG Public Key: www.tipiloschi.net/rebus.asc

KeyID: 0x176560F7

DIGITAL FORENSICS LAB
UNIVERSITY OF PAVIA

Queste e altre cazzate su

www.tipiloschi.net

facebook.com/gabrini

twitter.com/therebus

it.linkedin.com/in/rebus

- **Rebus' Digest**
  newsletter su cybercrime, hacking, digital forensics...
- **EventiLoschi**
  calendario delle conferenze pubbliche in materia