Facoltà di Scienze
MM.FF.NN.

ANDROID FORENSICS

Davide Barbuto
Francesco Capano
Gaetano Contaldi
Andrea Vallati

Sommario

- **L'evoluzione di Android**
- **Architettura**
- **Evidenze Digitali**
- **Analisi Anti-Forense**
- **Analisi Forense**
- **Sicurezza su Android**
- **Il file system YAFFS**
- **Analisi logica**
- **Analisi fisica**
- **Falso alibi digitale**

Che cos'è Android?

Lo stack Android

- Sistema operativo
- Applicazioni di base
- Tool per lo sviluppo

Open Handset Alliance

Statistiche (1)

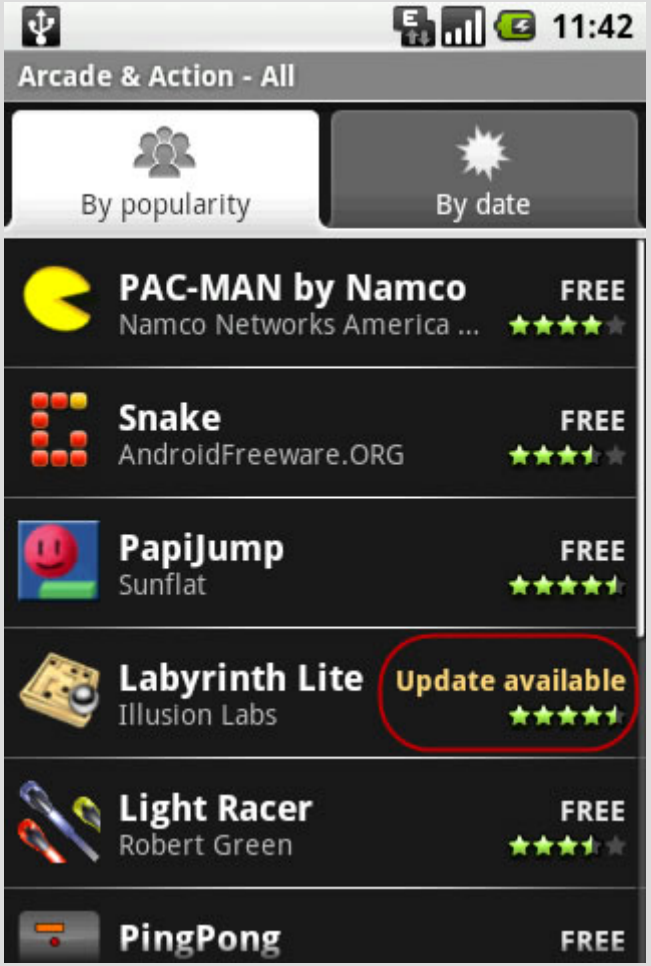
Secondo studi statistici condotti dalla società Canalys, nel primo quarto del 2011, sono stati venduti nel mondo 35.7 milioni di smartphones basati sul sistema operativo Android.

La crescita di Android è stata pari al **35%** spinta dalle ottime vendite dei device di HTC, Samsung, LG, Motorola e Sony Ericsson.

Statistiche (2)

Vendor	1Q11 Unit Shipments	1Q11 Market Share	1Q10 Unit Shipments	1Q10 Market Share	1Q11/1Q10 Change
1. Apple	4.4	20.8%	3.0	24.6%	49%
2. Nokia	4.2	19.6%	4.9	40.6%	-15%
3. Research in Motion	3.5	16.5%	2.4	19.6%	48%
4. HTC	3.5	16.5%	0.9	7.8%	271%
5. Samsung	2.6	12.1%	0.3	2.5%	744%
Others	3.0	14.5%	0.6	4.9%	414%
Total	**21.2**	**100%**	**12.1**	**100%**	**76%**

Market Android



con più di 150.000 applicazioni...

L'evoluzione di Android (1)

L'evoluzione di Android (1)

2008/09

Android 1.0 – 1.1

bug resolution

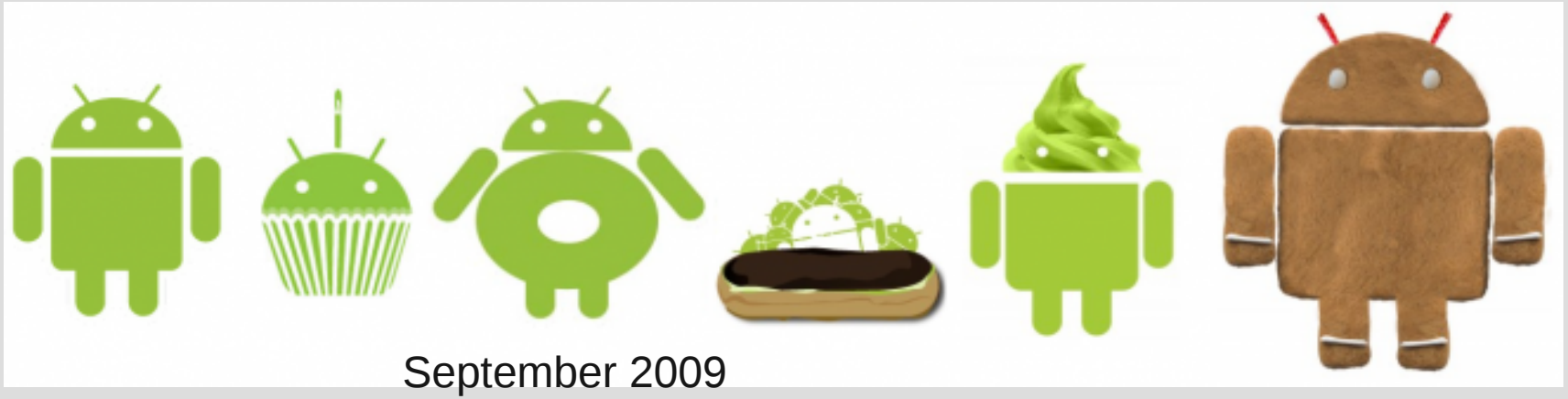
L'evoluzione di Android (1)

April 2009

Android 1.5
(Cupcake)

new interface and new functionality

L'evoluzione di Android (1)



September 2009

Android 1.6
(Donut)

new resolution, text-to-speech and voice-search

L'evoluzione di Android (1)

October 2009
January 2010

Android 2.0 - 2.1
(Enclair)

new browser UI and HTML5 support

L'evoluzione di Android (1)

May 2010

Android 2.2
(Froyo)

Flash support, speed and performance optimizzation

L'evoluzione di Android (1)

December 2010

Android 2.3
(Gingerbread)

NFC support and new UI

L'evoluzione di Android (2)

February 2011

Android 3.0
(Honeycomb)

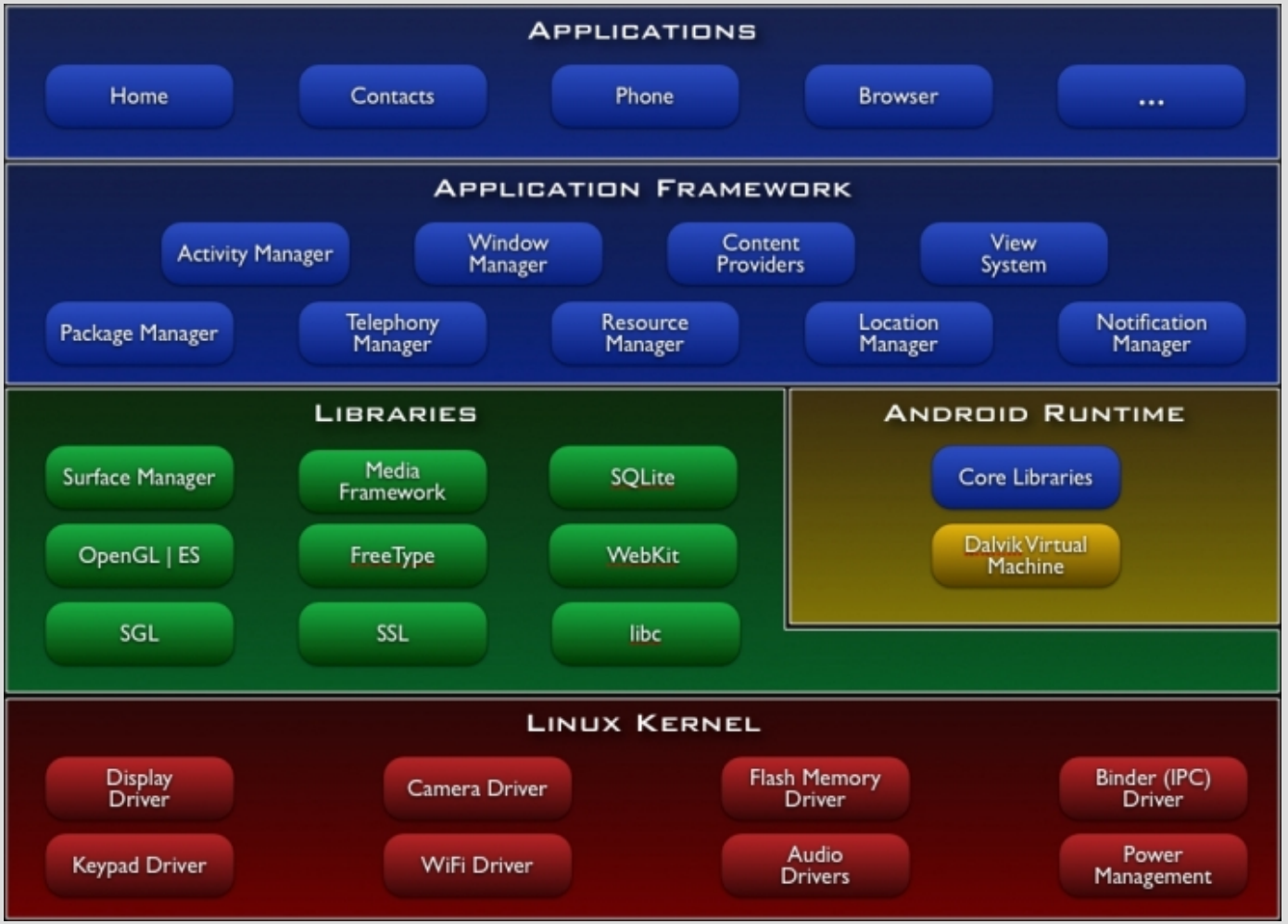
Versione esclusiva per tablet

In arrivo per la metà del 2011
una nuova versione di Android
con nome in codice: ***Ice Cream Sandwich***

L'architettura del sistema operativo

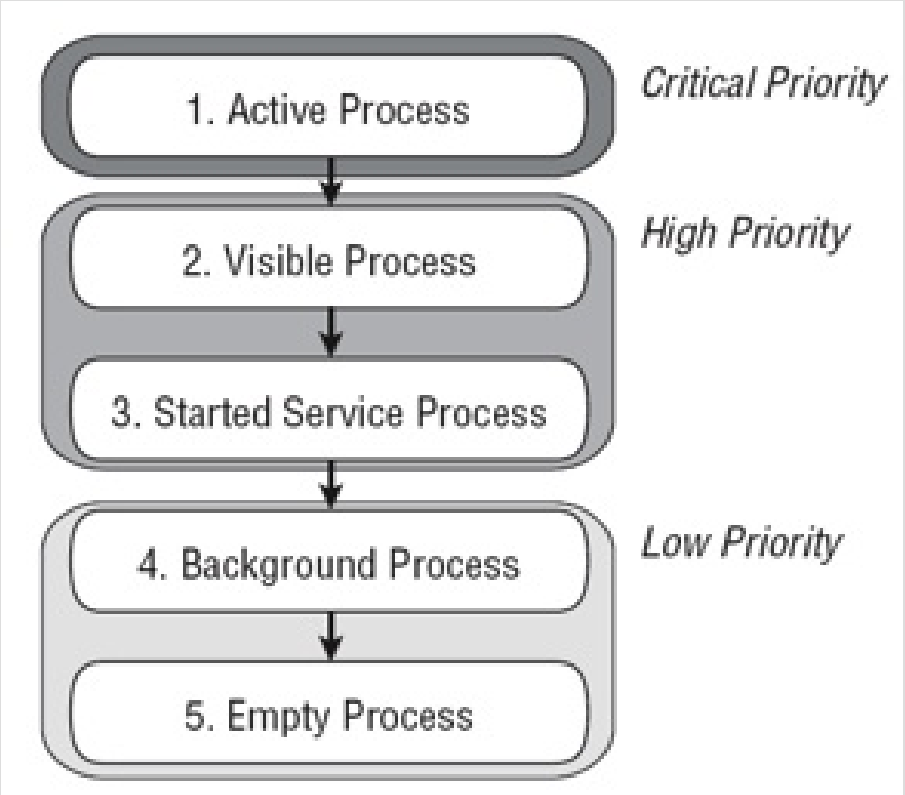
Software composto da cinque strati software:

- Kernel Linux
- Runtime Android
- Librerie
- Application Framework
- Applicazioni



L'architettura del sistema operativo

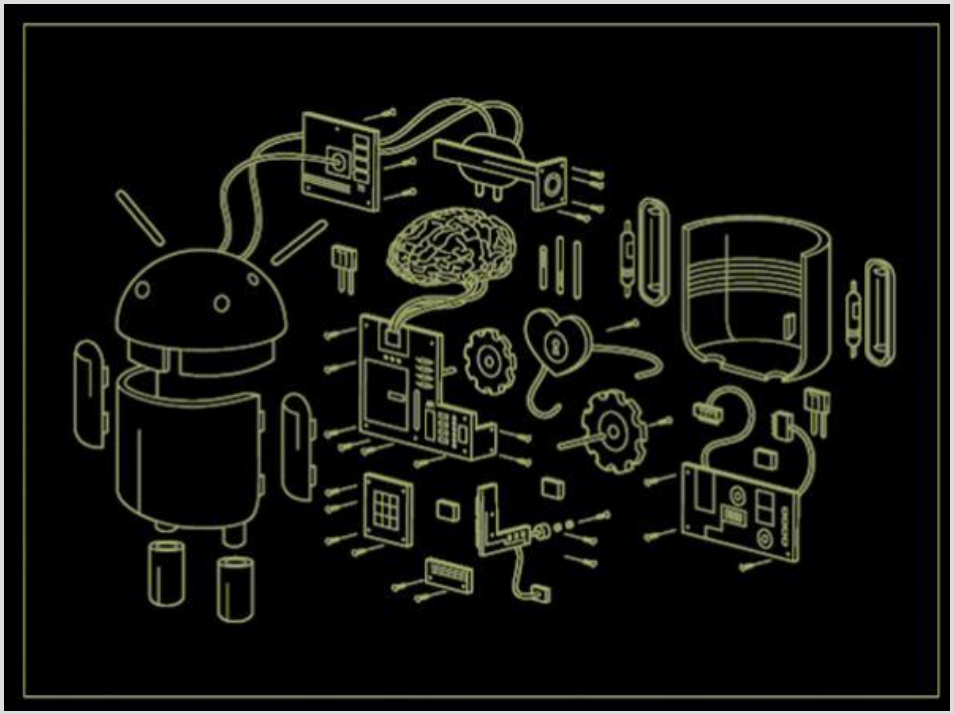
Applicazioni, processi e thread



L'architettura del sistema operativo

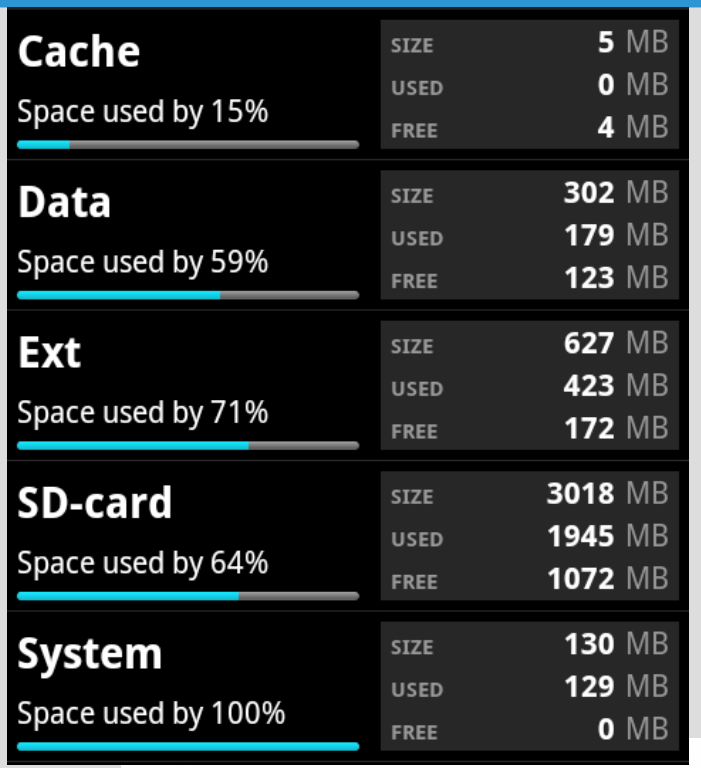
Gestione della RAM

Android è basato su linux
- Per ogni processo in esecuzione il kernel crea una cartella in /proc/$(PID)
- Sono memorizzate le aree di memoria associate ad ogni applicazione
- E' possibile realizzare una Live-Forensic



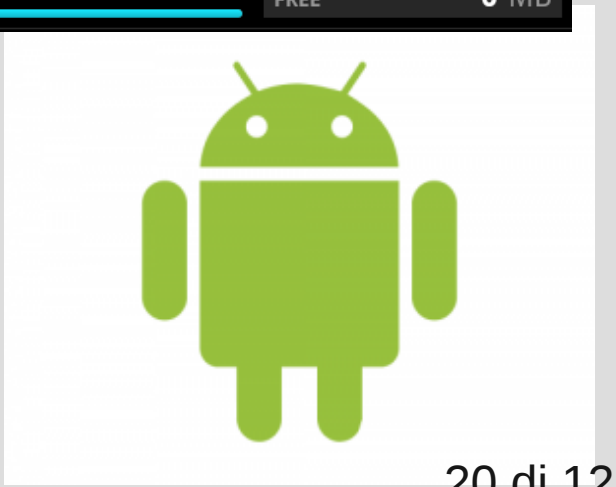
L'architettura del sistema operativo

Partizionamento filesystem




```
# cat /proc/mtd
dev:    size   erasesize  name
mtd0: 000a0000 00020000 "misc"
mtd1: 00480000 00020000 "recovery"
mtd2: 00300000 00020000 "boot"
mtd3: 08200000 00020000 "system"
mtd4: 00500000 00020000 "cache"
mtd5: 12ea0000 00020000 "userdata"
```

```
# /system
/bin/dd if=/dev/mtd/mtd5 of=/sdcard/mtd5.img bs=4096
77472+0 records in
77472+0 records out
317325312 bytes transferred in 66.997 secs (4736410 bytes/sec)
dd if=/dev/mtd/mtd5 2>/dev/null | md5sum | awk '{ print $1 }'
```



Evidenze Digitali

Una evidenza digitale consiste in una qualsiasi informazione, con valore probatorio, che sia memorizzata o trasmessa in formato digitale.
(Scientific Working Group on Digital Evidence, 1998)

Evidenze Digitali

Le evidenze digitali rilevabili sui sistemi Android riguardano:

- Contatti
  - *numeri di telefono, indirizzi, immagini relative al contatto;*
- History del browser;
- File multimediali;
- Chiamate
  - *ricevute ed effettuate;*
- Messaggi di testo;
- Messaggi multimediali;
- Agenda

  appuntamenti, date da ricordare.

Anti-forensic

Disciplina che si pone come obiettivo principale lo studio di una serie di metodologie che possano compromettere la disponibilità e l'usabilità di tracce ed evidenze digitali utilizzabili durante il processo di analisi forense.

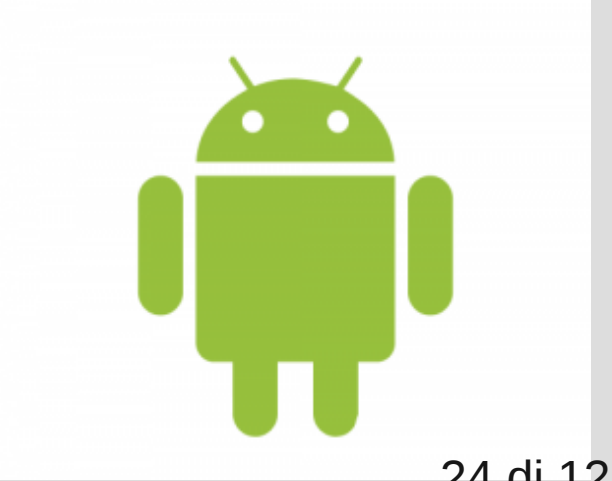
- Compromettere la disponibilità: nascondere l'esistenza delle tracce digitali o manipolarle a proprio piacimento

- Compromettere l'usabilità: cancellando o falsificando le tracce digitali

Tecniche anti-forensic

Tramite delle tecniche anti-forensics sarebbe possibile:

- *distruggere le evidenze;*
- *nascondere le evidenze;*
- *non permettere la generazione delle evidenze;*
- *confutare le evidenze.*



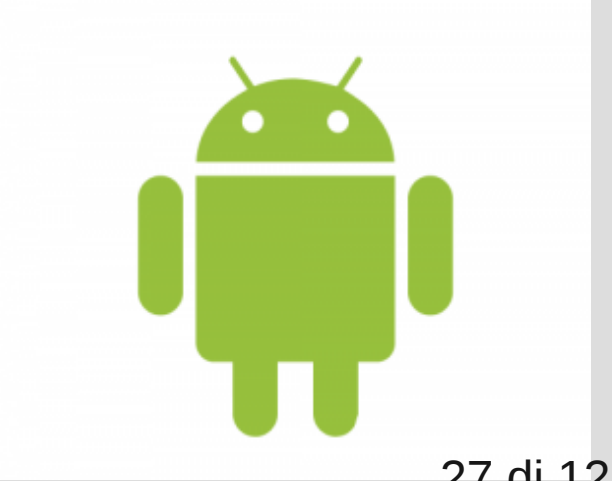
EEP – Evidence Export Process

Il file export.xml

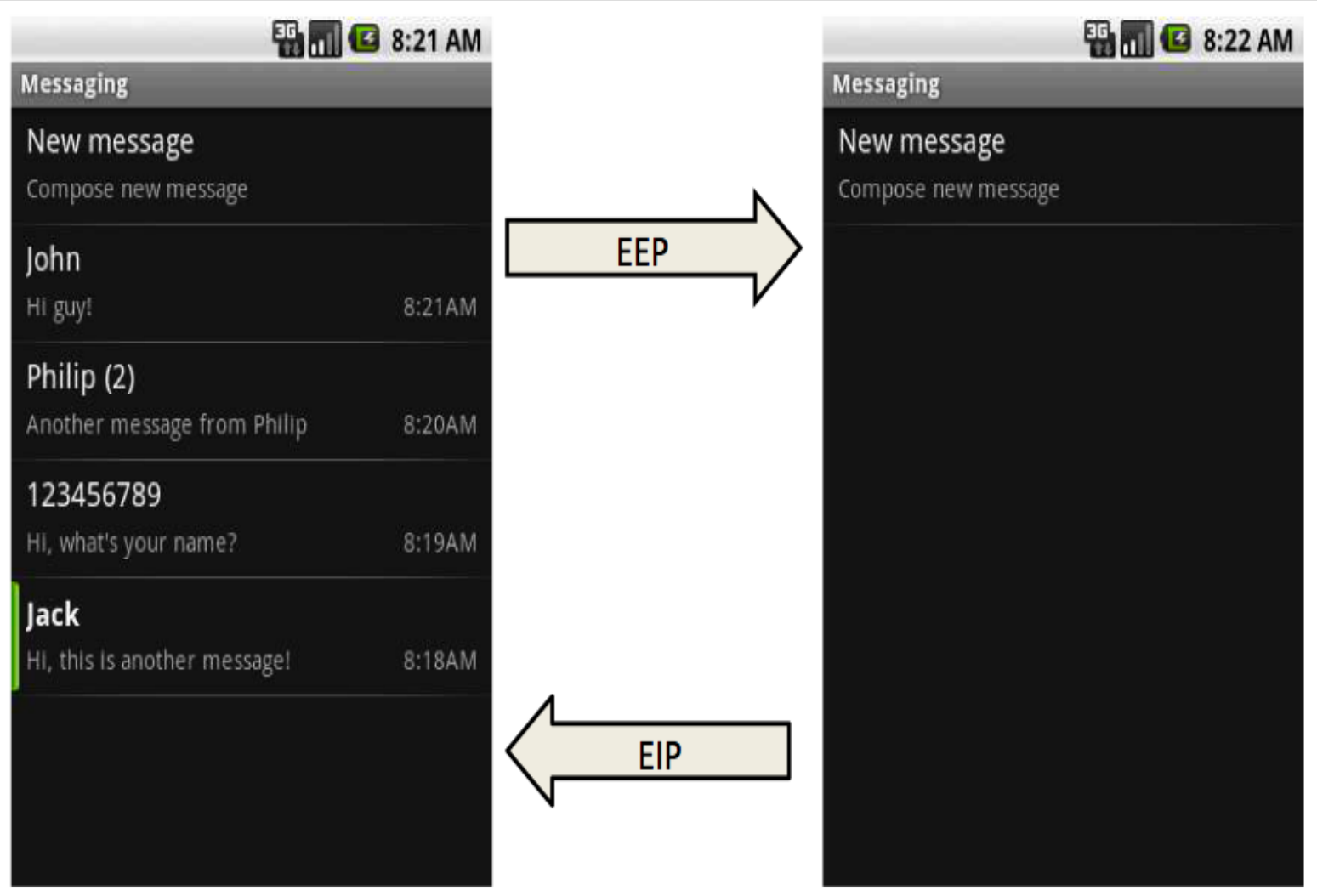
```
<database name='MMSSMS'>
<table name='sms'>
<row>
    <col name='_id'>977</col>
    <col name='thread_id'>15</col>
    <col name='address'>YYYYYYYYYYY</col>
    <col name='person'>1148</col>
    <col name='date'>1265591133661</col>
    <col name='protocol'>0</col>
    <col name='read'>1</col>
    <col name='status'>-1</col>
    <col name='type'>1</col>
    <col name='reply_path_present'>0</col>
    <col name='subject'>null</col>
    <col name='body'>Text of the message</col>
    <col name='service_center'>XXXXXXXXXXXXX</col>
</row>
</table>
</database>
```

EIP – Evidence Import Process

Il processo inverso EIP permette di importare evidenze precedentemente esportate fornendo la possibilità di recuperare uno stato precedente del dispositivo, in modo da raggirare l'analisi forense.



ANDROID AF: PROCESSI EEP/EIP



Analisi forense

Disciplina che studia l'individuazione, la conservazione, la protezione e l'estrazione di informazioni e documenti in formato digitale, reperibili da un qualunque dispositivo elettronico in grado di memorizzare *tracce digitali.*

Analisi forense su Android (1)

Nonostante difficoltà che si presentano, l'analisi forense cerca comunque di sviluppare tecniche e metodologie efficaci per l'analisi delle evidenze digitali

- **Analisi fisica**: studio di qualsiasi tipo di evidenza, anche nascosta o cancellata

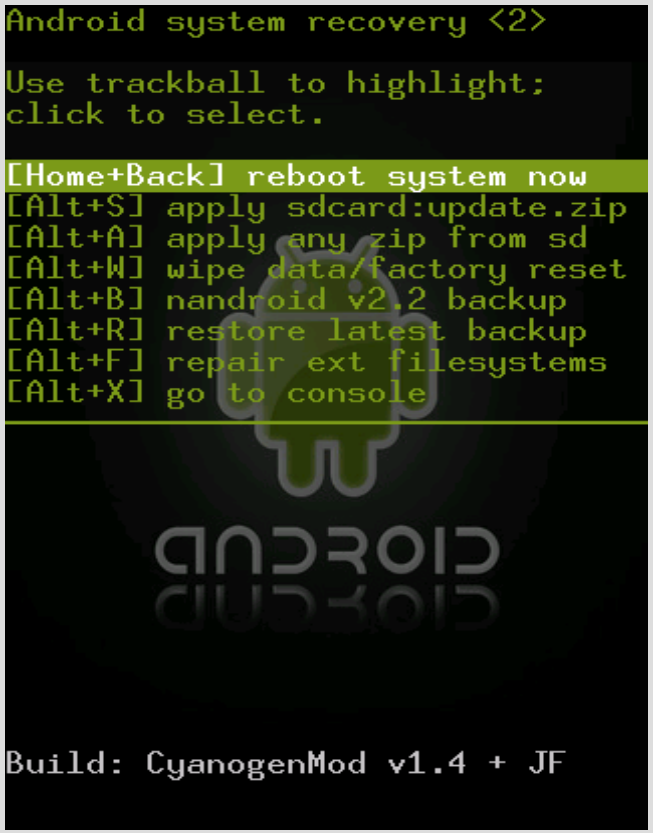
- **Analisi logica**: studio delle evidenze digitali "visibli ad occhio nudo" (contatti, messaggi, browser)

Analisi forense su Android (2)

Android Debug Bridge: strumento software che permette l'interazione tra il dispositivo mobile e una workstation remota.

Analisi forense su Android (3)

NaNdroid Backup: insieme di applicativi software che supportano operazioni di backup e ripristino per i dispositivi Android provvisti dei privilegi di root user.



Analisi forense su Android (4)

Comandi seriali tramite USB: alcuni dispositivi Android supportano la connessione seriale tramite porta USB. Questo meccanismo viene sfruttato per intercettare dati ed informazioni trasmessi attraverso la rete.

Pur essendo una valida tecnica, presenta forti limiti, dovuti, da un lato, all'incompatibilità con alcuni dispositivi, dall'altro, agli scarsi casi di testing finora previsti.

Analisi forense su Android (5)

Applicazioni Software: il sistema Android permette lo sviluppo e l'implementazione di applicazioni personali. In ambito forense, si potrebbe quindi costruire un app “ad hoc” che permetta il recupero delle evidenze digitali

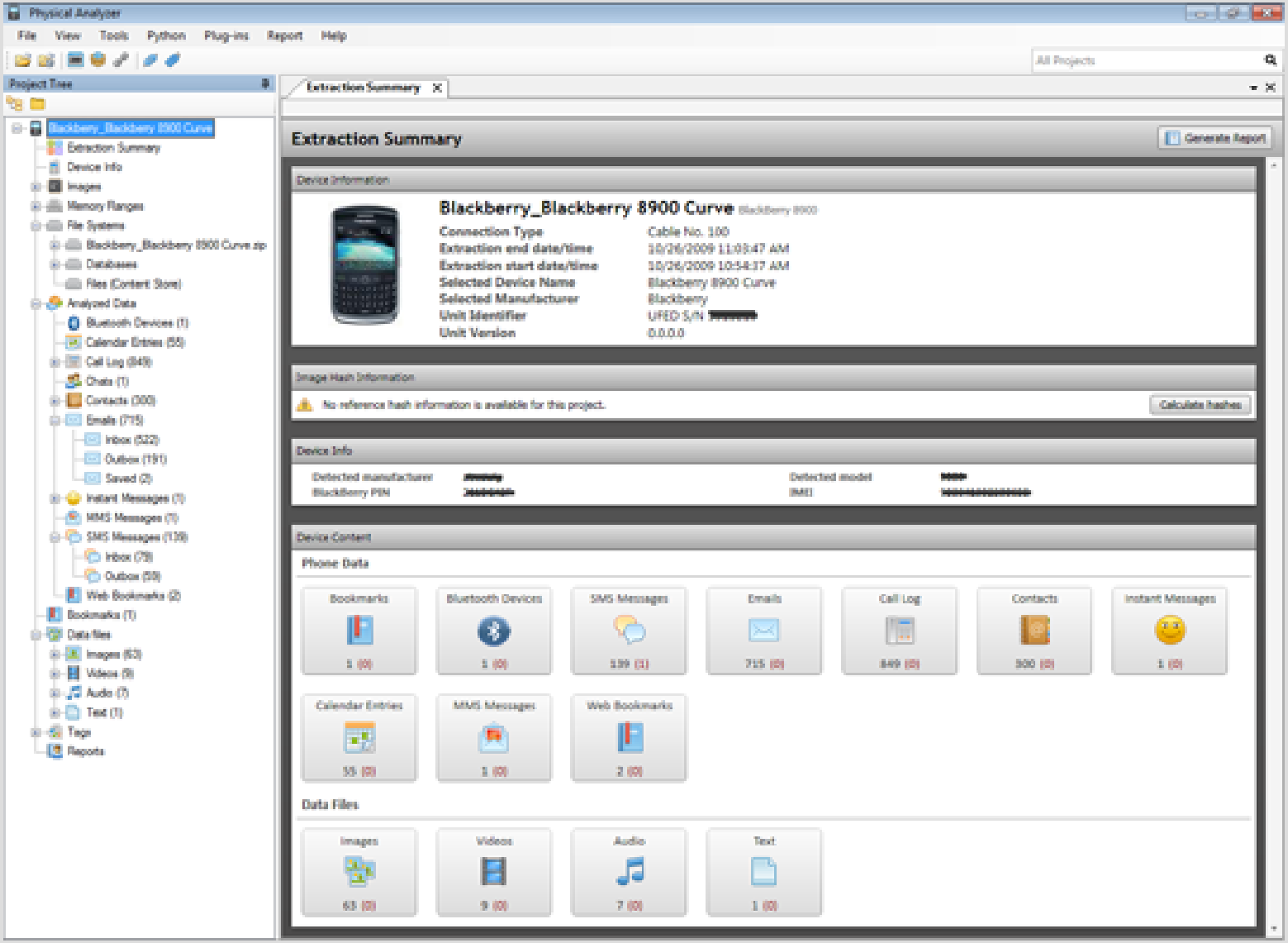
Un valido esempio è l'applicazione **AFDroid**, sviluppata dal dipartimento di informatica dell'università di Roma, che implementa i processi di **EEP** ed **EIP** per l'investigazione digitale dei dispositivi Android.

Un esempio concreto... (1)

Il dipartimento di polizia del Michigan utilizza stabilmente uno scanner particolare per effettuare operazioni di analisi forense su smart phone configurati con un qualsiasi sistema operativo.

Collegando lo scanner al telefono gli ufficiali di polizia possono bypassare le misure di sicurezza ed ottenere informazioni private presenti sul telefono(chiamate, messaggi, immagini.)

Un esempio concreto... (2)



Sicurezza su Android

Con gli smartphone che assomigliano sempre più a dei computer portatili, si delinea allo stesso passo la possibilità di trovarsi davanti a dei “mobile malware”. La sicurezza di tali dispositivi risulta quindi essere un aspetto molto importante.

Il sistema dei permessi

Essendo basato su Linux, Android costruisce le sue misure di sicurezza basandosi sul sistema dei permessi:

- Ogni applicazione installata viene eseguita con un diverso identificatore di sistema ad essa associato (Linux User ID e Linux Group ID)

- Ogni singola parte che compone il sistema operativo viene suddivisa in identità ben distinte tra loro

- Ogni applicazione è isolata sia rispetto ad un'altra applicazione, sia rispetto al sistema operativo

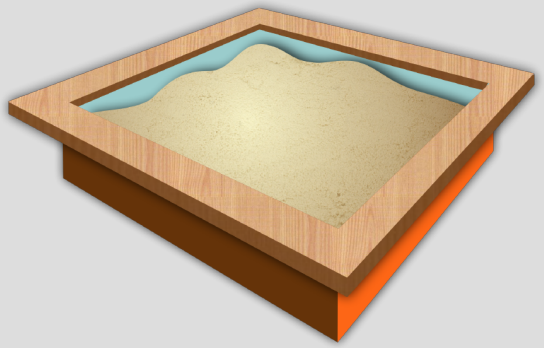
Sandbox

Nessuna applicazione, di default, può interagire con altre applicazioni installate sul sistema.

Il meccanismo è reso disponibile dal sistema di sicurezza garantito dalle sandbox:

- Ogni app viene eseguita nella propria sandbox

- Un' app non può in alcun modo interagire con altre app in esecuzione su altre sandbox



Eccezioni...

Potrebbe essere necessario il *file sharing* tra due diverse applicazioni, in esecuzione in due sandbox diverse

Sarà necessario dichiare dei permessi specifici all'interno del file **AndroidManifest.xml**

Usando il tag **<uses-permission>** sarà possibile specificare operazioni di comunicazione tra due app distinte

In qualunque altro caso, il kernel del sistema garantisce una netta separazione tra diverse app in esecuzione contemporaneamente.

Problemi

Nonostante si cerchi di prendere sempre tutte le precauzioni possibili, è praticamente impossibile rendere un sistema completamente immune da attacchi esterni

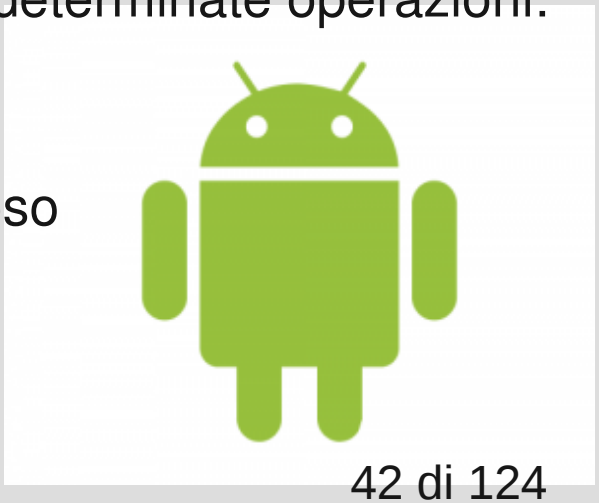
Le vulnerabilità di Android (1)

Insicurity, un team specializzato in sicurezza, ha sviluppato un *rootkit* in grado di inserirsi in uno smartphone android

L'applicazione, una volta installata sul dispositivo, si attiva tramite chiamata o sms

Si aggira in modo furtivo e abile, nascondendo le proprie tracce e utilizzando il più alto livello di accesso garantito dal telefono. In mano ad un hacker, può essere utilizzato per “obbligare” il dispositivo a compiere determinate operazioni:

- Chiamate a raffica
- Reindirizzamento del browser ad un sito web dannoso
- Cancellazione di dati sensibili



Fortunatamente è difficilmente utilizzabile

Le vulnerabilità di Android (2)

Recentemente è stato scoperto un bug che affligge il 99% dei dispositivi android (provvisi della versione del firmware da 2.3.3 in giù)

Cattiva gestione del protocollo **ClientLogin**:

- Ogni device memorizza un *token* **(authToken)** in seguito ad un'autenticazione online

- Il token viene mantenuto in memoria per 14 giorni. I malintenzionati, possono comodamente “rubarlo” con semplici tecniche di *sniffing* ed utilizzarlo per accedere ai dati personali

- In seguito all'autenticazione, i dati trasmessi arrivano da link di tipo non *https*

- Problema risolto con la versione 2.3.4

File System YAFFS

File system più diffuso ed utilizzato all'interno dei dispositivi Android

Qualche dettaglio...

Sviluppato partendo da JFFS e JFFS2, i due file system di Linux che meglio supportano le memorie flash

YAFFS utilizza una memoria flash di tipo NAND:

- Utilizzare molteplici opzioni di formattazione, come ad esempio i marker per identificare i blocchi corrotti

- Riuso del codice

- Possibilità di fare affidamento sulla filosofia *“If it ain't broke, don't fix!”*

YAFFS: Il funzionamento(1)

- Dati memorizzati in blocchi di taglia fissa (512 bytes)

- Ogni pagina è marcata con due etichette: un **file id** e un **numero di blocco**, conservate nell'area di memoria *"spare data"*

- I file *"headers"* sono memorizzati in una singola pagina, per differenziarli dai dati veri e propri

- Se i dati all'interno di un file devono essere sovrascritti, i blocchi interessati vengono sostituiti con un nuovo blocco

  • Il nuovo blocco contiene la pagine con i **nuovi** dati, ma con le **vecchie** etichette

  • Le vecchie pagine vengono marcate come **discarded**

YAFFS: Il funzionamento(2)

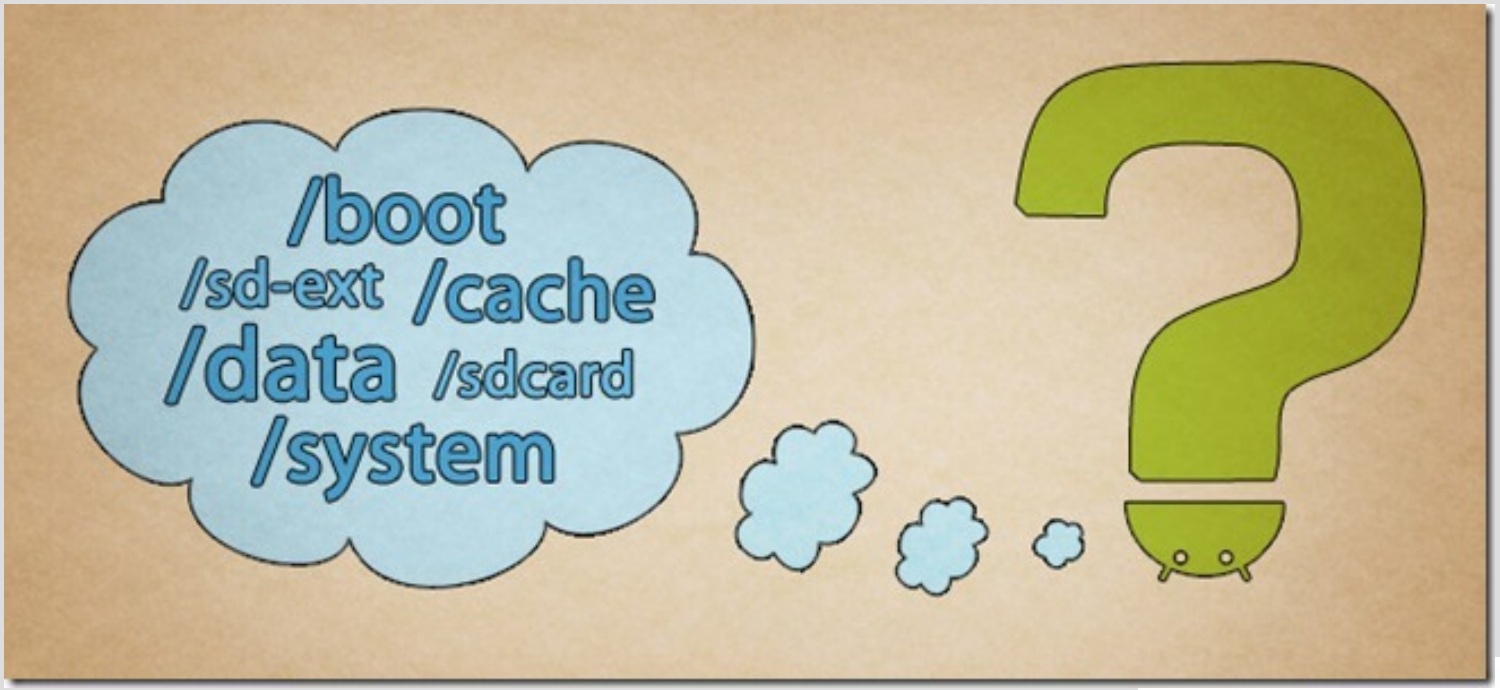
- Le pagine hanno un marker ulteriore, un **numero seriale** di 2 bit, che incrementa in proporzione alla taglia della pagina

  • Se accadesse qualcosa prima che una pagina venga marcata come *“discarded”,* il file system *manterrebbe due pagine con gli stessi tag*

  • Il numero seriale viene usato per distinguere la pagina vecchia da quella nuova

- Un blocco contenente solo pagine marcate come *“discarded”* prende il nome di **dirty block**, e sarà il maggior candidato per il garbage collector

YAFFS: Il partizionamento (1)



YAFFS: Il partizionamento (2)

La memoria interna è suddivisa in 6 partizioni principali:

- */boot*

- */system*

- */recovery*

YAFFS: Il partizionamento (3)

- */data*

- */cache*

- */misc*

Due partizioni ulteriori per la SD-CARD

- */sdcard*

- */sd-ext*

Forse era meglio usare....

VS

Analisi logica

Cosa abbiamo fatto?

• reperito il dispositivo, la batteria é stata rimossa in maniera brutale;

• la SD card del dispositivo é stata sostituita con una SD card vergine;

• é stata inserita nuovamente la batteria;

• il dispositivo é stato avviato in modalità di recovery, dopodiché é stato collegato al computer tramite cavo usb;

• sul computer é stato avviato il server adb per poter effettuare l'immagine della partizione /data;

• l'immagine é stata fatta utilizzando mkyaffs2image.

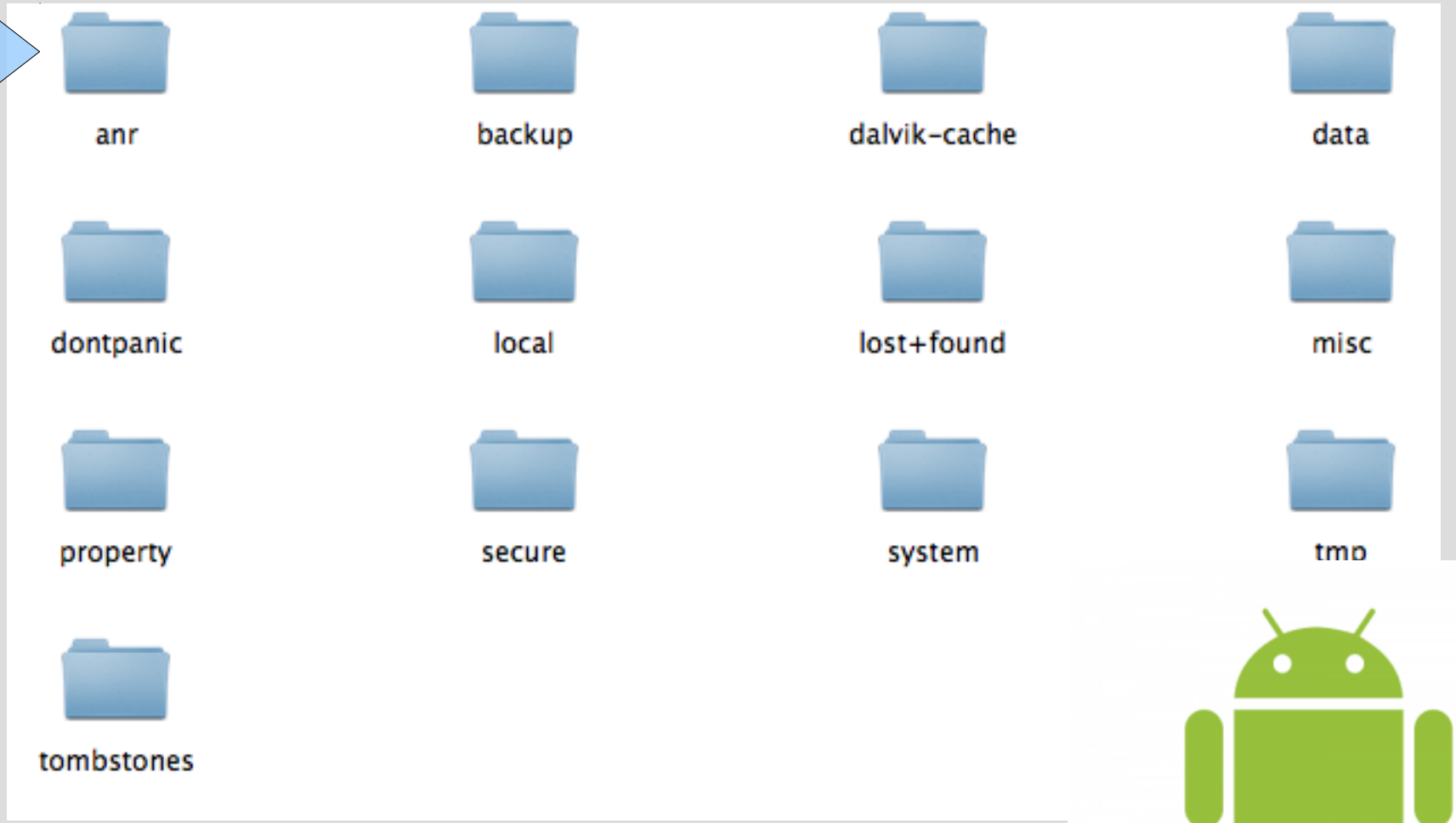
• per navigare l'immagine ottenuta é stato utilizzato unyaffs, che ha prodotto una cartella contente i file del filesystem.

mkyaffs2image

è un utility che permette di creare un'immagine del filesystem yaffs e yaffs2.

```
localhost / # mkyaffs2image /data/ /sdcard/mtd5.img
```

Analisi.... (1)


anr
backup
dalvik-cache
data
dontpanic
local
lost+found
misc
property
secure
system
tmp
tombstones

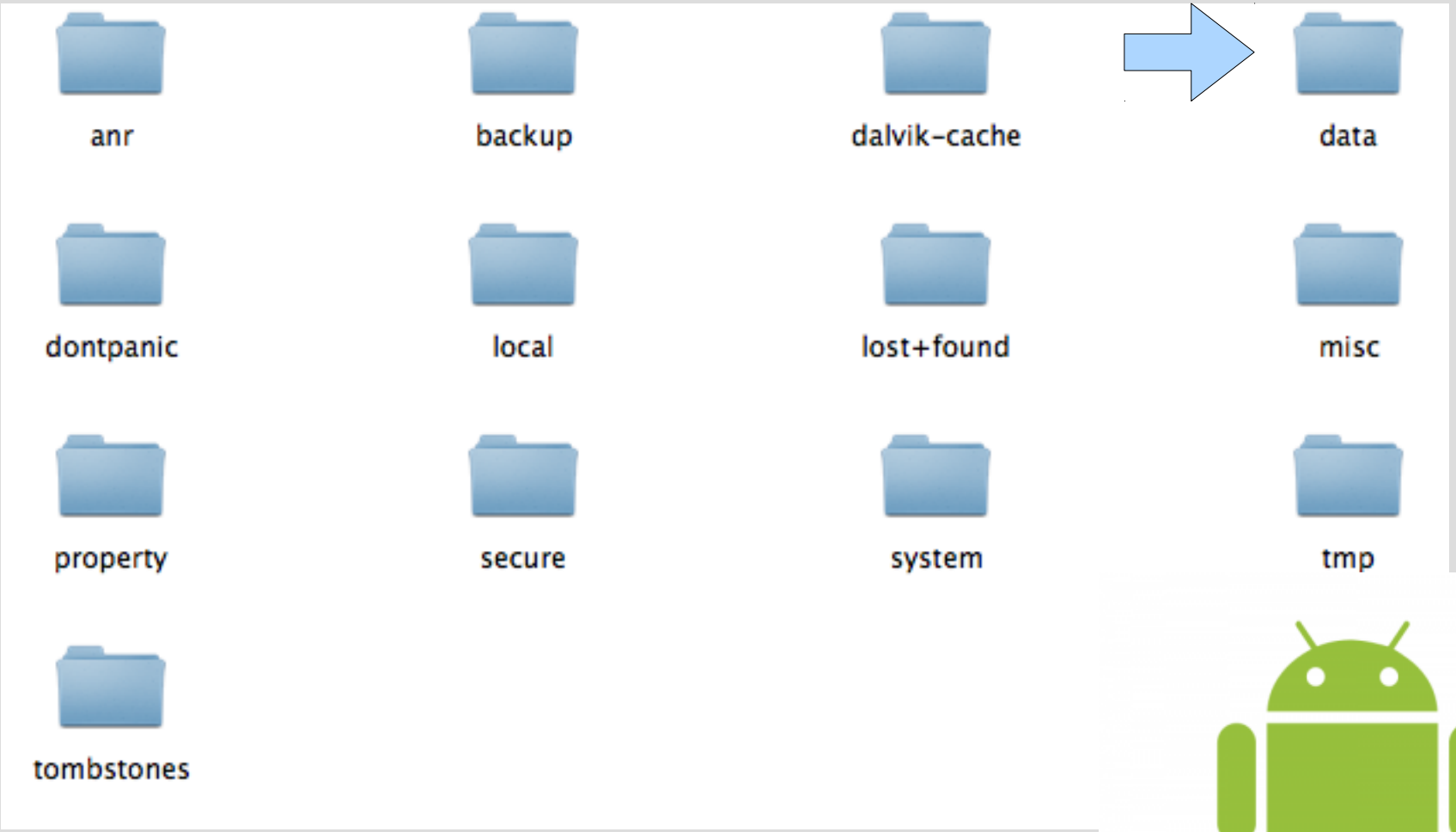
Application Not Responding

traces.txt

File Edit Search Options Help

```
631 ----- pid 8287 at 2011-05-18 21:16:12 -----
632 Cmd line: com.jb.gosms
633
634 DALVIK THREADS:
635 (mutexes: tll=0 tsl=0 tscl=0 ghl=0 hwl=0 hwll=0)
636 "main" prio=5 tid=1 SUSPENDED
637   | group="main" sCount=1 dsCount=0 obj=0x400fd1a0 self=0xce60
638   | sysTid=8287 nice=0 sched=0/0 cgrp=bg_non_interactive handle=-1345006528
639   at com.jb.gosms.ui.preference.notification.ReminderReceiverService.<clinit>(GoSms:~36)
640   at com.jb.gosms.ui.preference.notification.ReminderReceiver.onReceive(GoSms:-1)
641   at android.app.ActivityThread.handleReceiver(ActivityThread.java:1915)
642   at android.app.ActivityThread.access$2400(ActivityThread.java:123)
643   at android.app.ActivityThread$H.handleMessage(ActivityThread.java:989)
644   at android.os.Handler.dispatchMessage(Handler.java:99)
645   at android.os.Looper.loop(Looper.java:123)
646   at android.app.ActivityThread.main(ActivityThread.java:3835)
647   at java.lang.reflect.Method.invokeNative(Native Method)
648   at java.lang.reflect.Method.invoke(Method.java:507)
649   at com.android.internal.os.ZygoteInit$MethodAndArgsCaller.run(ZygoteInit.java:841)
650   at com.android.internal.os.ZygoteInit.main(ZygoteInit.java:599)
651   at dalvik.system.NativeStart.main(Native Method)
652
653 "Thread-55" prio=5 tid=12 NATIVE
654   | group="main" sCount=1 dsCount=0 obj=0x40735638 self=0x2b8150
655   | sysTid=8512 nice=0 sched=0/0 cgrp=bg_non_interactive handle=1683928
656   at org.apache.harmony.luni.platform.OSFileSystem.open(Native Method)
657   at dalvik.system.BlockGuard$WrappedFileSystem.open(BlockGuard.java:232)
658   at java.io.RandomAccessFile.<init>(RandomAccessFile.java:132)
659   at java.io.RandomAccessFile.<init>(RandomAccessFile.java:173)
660   at com.jb.gosms.util.av.I(GoSms:217)
661   at com.jb.gosms.util.av.Code(GoSms:164)
662   at com.jb.gosms.util.ac.Code(GoSms:454)
663   at com.jb.gosms.background.GoMessagingService.Code(GoSms:171)
664   at com.jb.gosms.background.GoMessagingService.StartUploadLoger(GoSms:845)
665   at com.jb.gosms.background.b.run(GoSms:802)
666   at java.lang.Thread.run(Thread.java:1019)
```

Analisi.... (2)


anr
backup
dalvik-cache
data
dontpanic
local
lost+found
misc
property
secure
system
tmp
tombstones

directory Data!!!

• Ogni applicazione ha un proprio spazio privato dove memorizzare le informazioni che ritiene necessarie.

• Un’applicazione non può accedere alla cartella di un’altra applicazione.

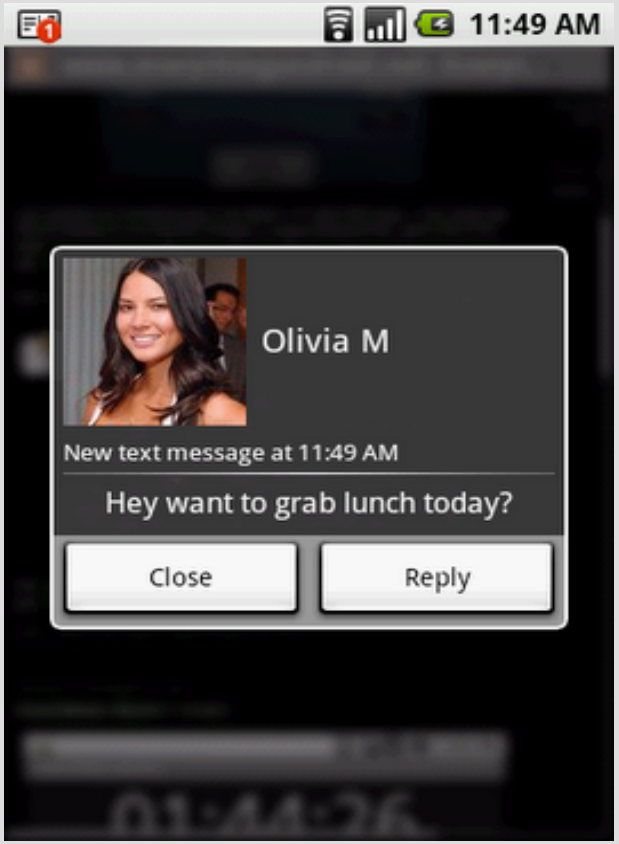
directory Data (1)

com.android.providers.contacts: cartella collegata all'applicazione che si occupa dei contatti

Abbiamo trovato:
- cronologia delle chiamate
- lista dei contatti, comprensivi di mail.

directory Data (2)

com.android.providers.telephony : cartella collegata all'applicazione che dei servizi telefonici del dispositivo



Abbiamo trovato:
- il contenuto degli sms e mms.
- se il messaggio è stato letto.
- la data di invio o ricezione.
- i file multimediali inviati.

directory Data (3)

com.android.providers.calendar : cartella collegata all'applicazione di default per la gestione dell'agenda.

Abbiamo trovato:
• informazioni circa tutti gli eventi salvati dall'utente.

directory Data (4)

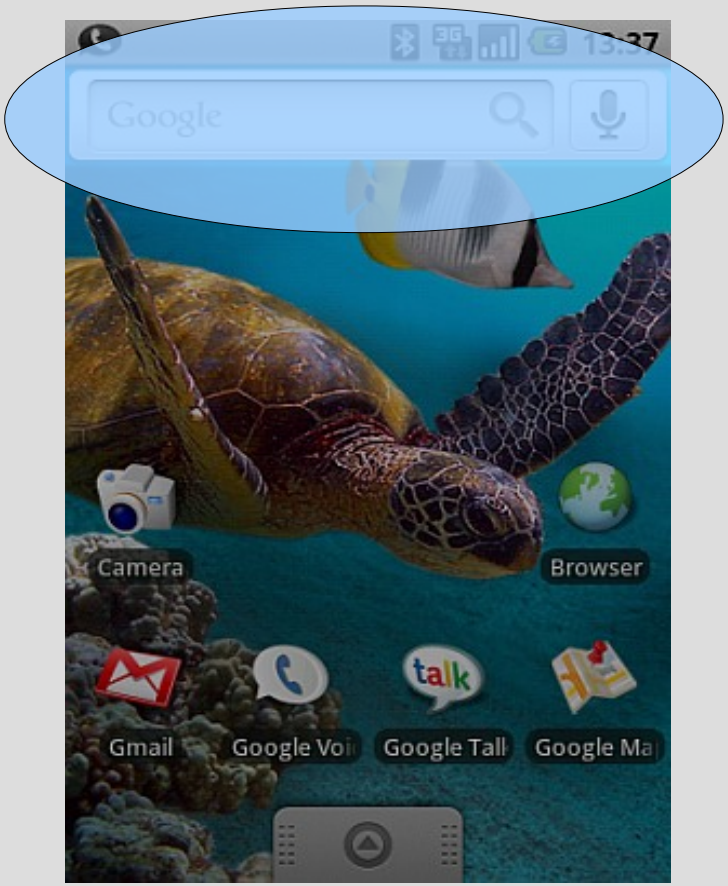
com.google.android.gm : cartella collegata all'applicazione Google Mail.

Abbiamo trovato:

- la lista degli allegati scaricati dalle mail.
- la lista delle conversazioni.
- la lista delle mail collegate all'account.
- la lista delle mail inviate e ricevute.
- le ultime ricerche effettuate attraverso l'applicazione.

directory Data (5)

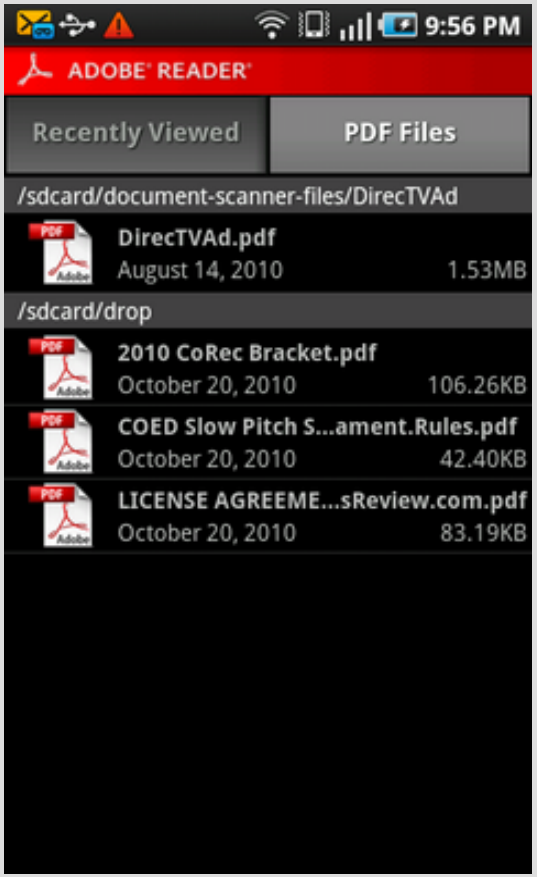
com.google.android.googlequicksearchbox :
cartella collegata all'applicazione che permette di effettuare ricerche sul dispositivo.



Abbiamo trovato:
• le ultime ricerche effettuate, con relativa data ed ora.

directory Data (6)

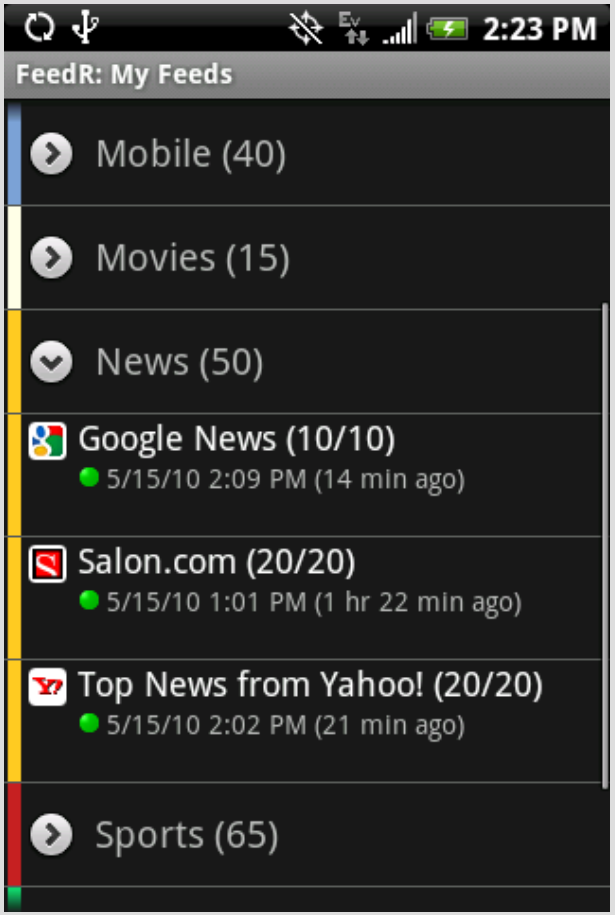
com.adobe.reader : cartella collegata all'applicazione che permette la lettura dei file pdf.



Abbiamo trovato:
• la lista degli ultimi file aperti comprensivi di path.

directory Data (7)

com.google.android.reader : cartella collegata all'applicazione che permette la lettura dei feed rss.

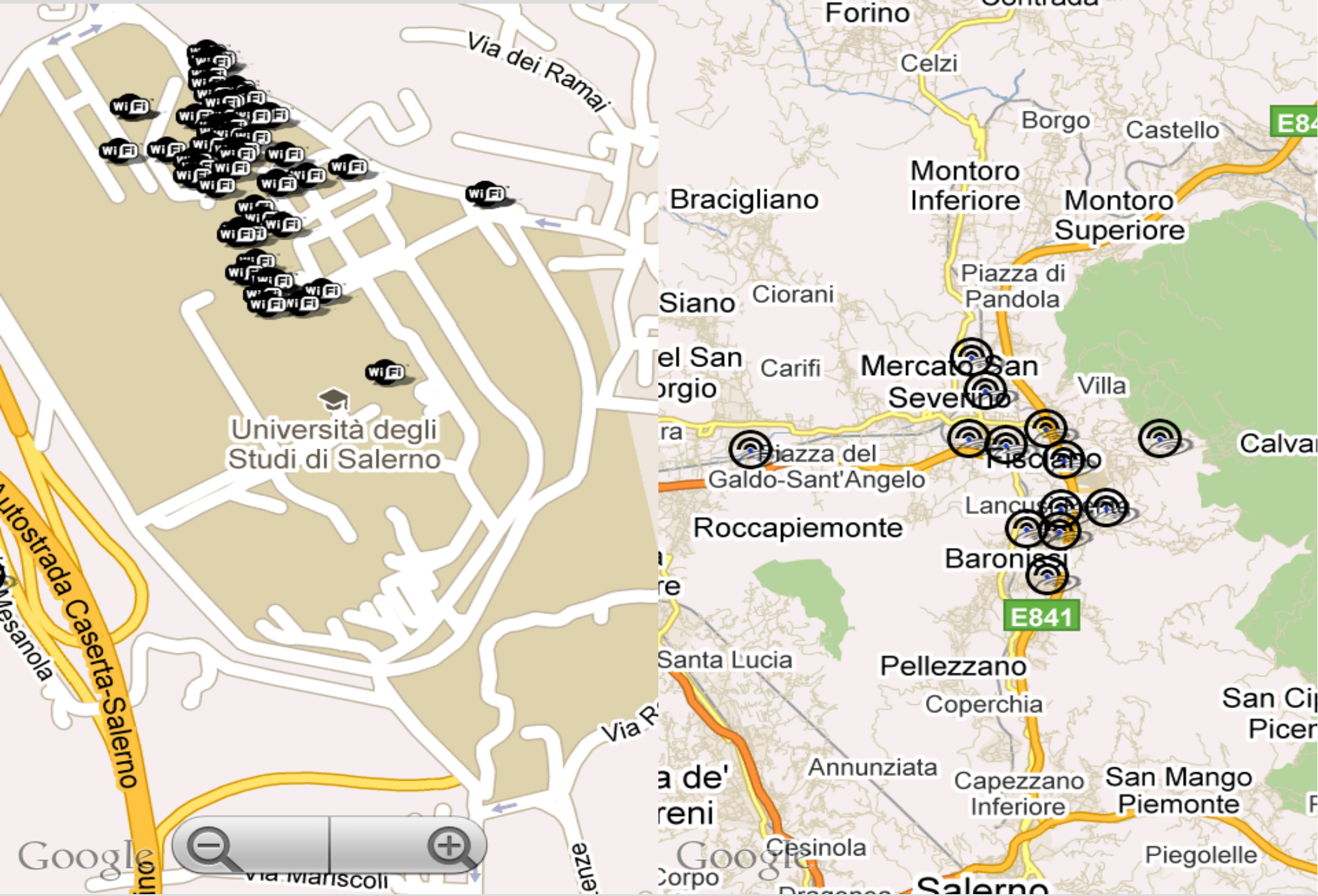


Abbiamo trovato:
- le immagini contenute nei feed letti.
- username dall'account con cui è collegato.
- lista dei feed a cui è iscritto, comprensive di url.
- lista dei singoli articoli, comprensive di titolo e url.
- i file html relativi a gran parte degli ultimi feed letti.

directory Data (8)

com.google.android.location : cartella collegata all'applicazione che permette la localizzazione del dispositivo.

Abbiamo trovato:
- informazioni riguardanti le ultime celle alle quali il cellulare si è collegato
- informazioni riguardanti gli access-point ai quali il cellulare si è collegato.


Via dei Ramai
Università degli Studi di Salerno
Autostrada Caserta-Salerno
Via Mariscoli
Google
Forino
Celzi
Borgo
Castello
E84
Montoro Inferiore
Montoro Superiore
Bracigliano
Piazza di Pandola
Siano
Ciorani
Carifi
Mercato San Severino
Villa
Piazza del Galdo-Sant'Angelo
Roccapiemonte
Baronissi
E841
Santa Lucia
Pellezzano
Coperchia
Annunziata
Capezzano Inferiore
San Mango Piemonte
Cesinola
Piegolelle
Salerno

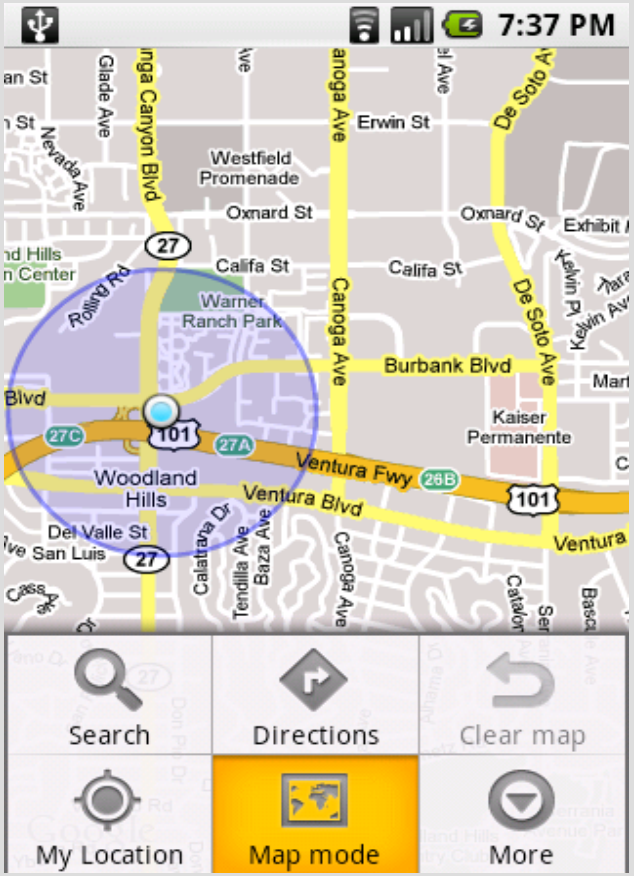
directory Data (9)

com.google.android.street : cartella collegata all'applicazione Google StreetView.

Abbiamo trovato:
• immagini riguardanti le ultime visualizzazioni in streetView.

directory Data (10)

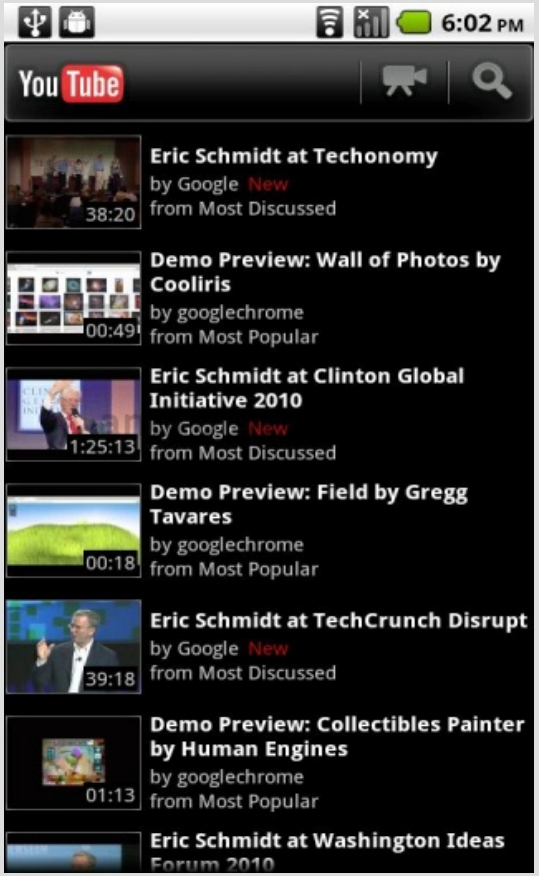
com.google.android.apps.maps : cartella collegata all'applicazione Google Maps.



Abbiamo trovato:
- lo storico dei percorsi ricercati con relativa data e ora.
- le ultime ricerche effettuate.

directory Data (11)

com.google.android.youtube : cartella collegata all'applicazione Youtube per Android.

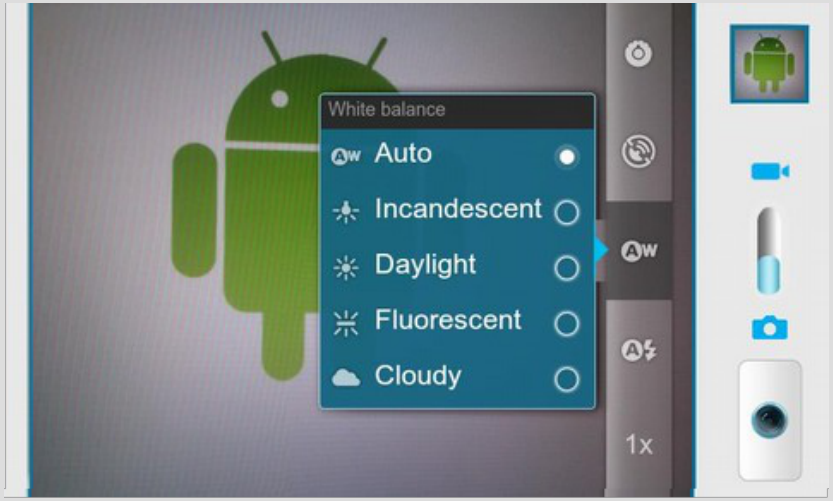


Abbiamo trovato:

- le ultime ricerche effettuate, con relativa data e ora.

directory Data (12)

com.google.providers.media : cartella collegata all'applicazione che gestisce I file multimediali.



Abbiamo trovato:
- lista degli album musicali.
- copertine degli album ascoltati.
- playlists musicali.
- immagini e video. Per questo tipo di file è possibile conoscere la provenienza.

directory Data (13)

com.skype.raider : cartella collegata all'applicazione Skype.

Abbiamo trovato:
- la lista dei partecipanti alle ultime chat.
- la lista degli eventi notificati.

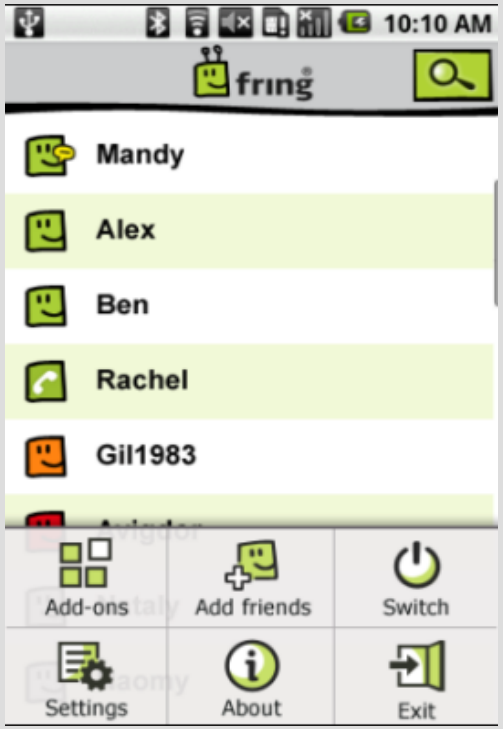
directory Data (14)

com.facebook.katana : cartella collegata all'applicazione Facebook.

Abbiamo trovato:
- le info dell'account che si collega a facebook e la sua password cifrata.
- le sessioni salvate con relativa data e ora.
- le notifiche di facebook che ancora devono essere visualizzate.
- i messaggi della mail di facebook
- la lista degli amici
- non è stato possibile recuperare le conversazioni tra due contatti.

directory Data (15)

com.fring : cartella collegata all'applicazione Fring.



Abbiamo trovato:
• la lista dei contatti e delle conversazione priva di contenuto.
• la lista delle operazioni effettuate.
• la lista delle sessioni.

directory Data (16)

com.google.android.gsf : cartella collegata all'applicazione Google Talk.

Abbiamo trovato:
- i contatti di google Talk
- gli ultimi messaggi inviati e ricevuti.

directory Data (17)

mobi.mgeek.TunnyBrowser : cartella collegata al browser Dolfin

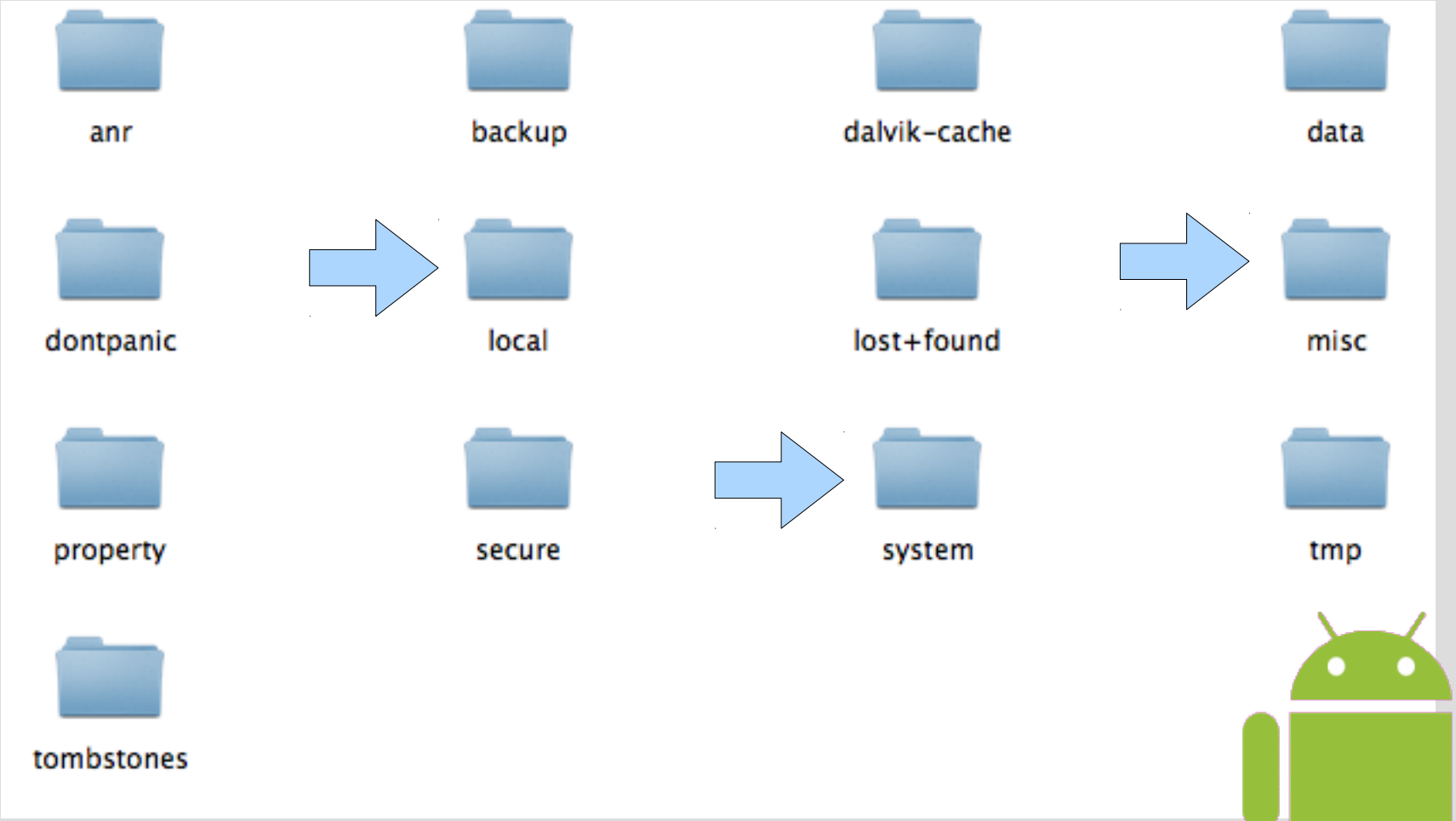
Abbiamo trovato:
- dati memorizzati su richiesta delle pagine web visitate.
- tutte le informazioni introdotte in form di compilazione.
- le ricerche effettuate con la relativa data.
- gli ultimi download effettuati.
- le password in chiaro memorizzate dall'utente.
- le password httpAuth.
- la lista delle operazioni effettuate.
- la lista delle sessioni.
- i cookies.
- la cronologia.
- tutti i segnalibri.

directory Data (18)

com.google.android.gsf : cartella collegata all'applicazione Google Talk.

Abbiamo trovato:
- I dati memorizzati nel local storage di ogni pagina visitata.
- posizione e timestamp.
- cookie delle pagine visitate.
- cronologia.
- preferiti.
- le password memorizzate dall'utente.
- le password httpAuth.
- tutte le informazioni introdotte in form di compilazione.
- i cookies.

Analisi.... (3)


anr
backup
dalvik-cache
data
dontpanic
local
lost+found
misc
property
secure
system
tmp
tombstones

Local – Misc – System

- Nella directory System troviamo:
  - la lista delle applicazioni che utilizzano la sincronizzazione dei dati.
  - la lista dei pacchetti installati.
- Nella directory Local troviamo gli apk temporanei.
- Nella directory Misc troviamo le diverse impostazioni di sistema

Oxygen per HTC Desire

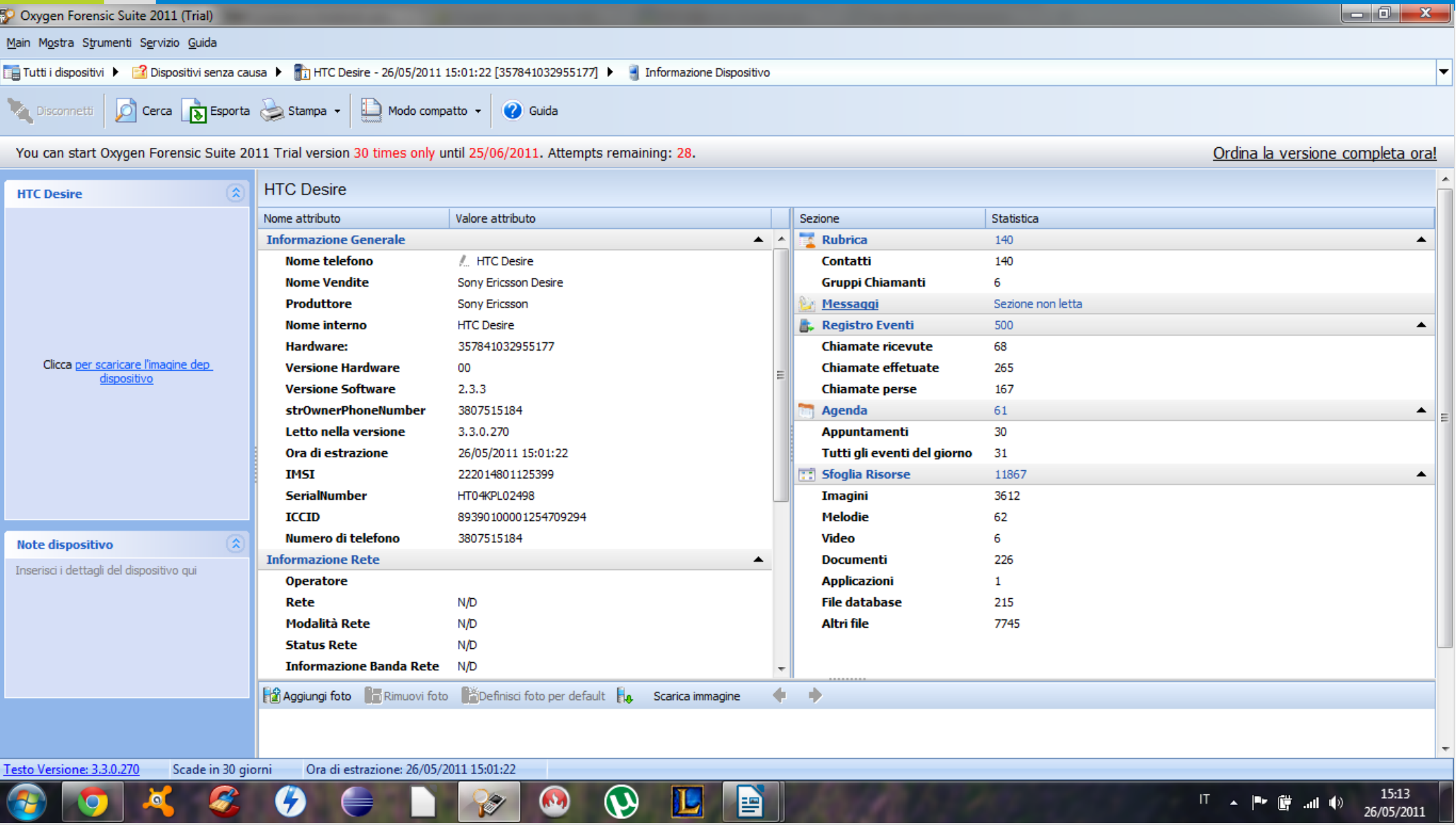
Oxygen

Strumenti necessari per l'installazione di Oxygen

- 100Mb
- Windows

- Driver del dispositivo

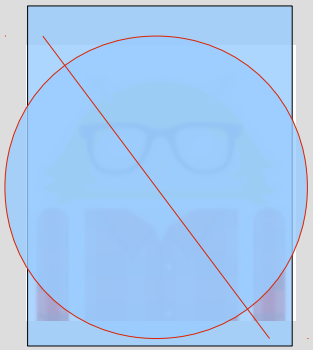
Informazioni generali del dispositivo



Rubrica

Informazioni per ogni account:

- Foto
- Nome
- Lavoro
- Telefono
- Email
- Indirizzo
- Note
- Privato
- Gruppo
- MD5



Messaggi

Informazioni per ogni messaggio:

- Tipo (sms/mms)
- Cartella
- Contatto
- Numero Telefono
- Ora
- Testo
- MD5

Registro eventi

- Chiamate Effettuate 
- Chiamate Ricevute 
- Chiamate Perse 

Oxygen Forensic Suite 2011

Agenda

- Tipo
- Inizio
- Fine
- Allarme
- Testo
- Memo
- Posizione
- Ricorrenza

Risorse

- /sdcard/Android
- /sdcard/Bluetooth
- /sdcard/DCIM/Camera
- /sdcard/External_SD
- /sdcard/Download

Oxygen Forensic Suite 2011

Oxygen VS Unyaffs

Oxygen pro:

- Grafica facile da utilizzare
- Non richiede la root

Oxygen contro:

- Lento nel esportare i dati
- Non completamente compatibile con android
- Modifica il sistema

Unyaffs pro:

- È stato in grado di recuperare tutto quello che è memorizzato all'interno del dispositivo

Unyaffs contro:

- Nessun ambiente grafico
- L'immagine da analizzare è ottenibile solo con permessi di root

Oxygen VS Unyaffs

The winner is...

Unyaffs

Analisi Fisica

Cosa abbiamo fatto?

• reperito il dispositivo, la batteria é stata rimossa in maniera brutale;

• la SD card del dispositivo é stata sostituita con una SD card vergine;

• é stata inserita nuovamente la batteria;

• il dispositivo é stato avviato in modalità di recovery, dopodiché é stato collegato al computer tramite cavo usb;

• sul computer é stato avviato il server adb per poter effettuare l'immagine della partizione /data;

• il dump é stato effettuato utilizzando dd.

• Analisi dell'immagine con Scalpel e Photorec.

Analisi Fisica

Scalpel

- Open source
- Analizza raw data → Indipendente dal file system
- Analizza immagini o dischi alla ricerca di sequenze di bit predefinite
- Lista header da rilevare personalizzabile
- Per ogni header rilevato, il programma considera il **file terminato** solo quando trova il **corrispondente footer o EOF**

Errori nel recupero delle informazioni
File recuperati più volte
Difficoltà ad analizzare grandi quantità di informazioni

Analisi Fisica

Scalpel

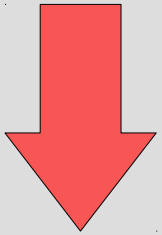
Da un dump di ~300MB Scalpel estrae 40178 file
La quantita di dati estratta è molto superiore a quella dei dati originali

```
sqlitedb with header "\x53\x51\x4c\x69\x74\x65\x20\x66\x6f\x72\x6d\x
** PREVIEW MODE: GENERATING AUDIT LOG ONLY **
** NO CARVED FILES WILL BE WRITTEN **
Carving files from image.
Image file pass 2/2.
../mtd5.dd: 102.4% |*****************************************
../mtd5.dd: 100.0% |*****************************************
Processing of image file complete. Cleaning up...
Done.
Scalpel is done, files carved = 40179, elapsed = 40 s
```

Analisi Fisica

Photorec

- Stessi principi di funzionamento di Scalpel
- Open source
- Analizza raw data → Indipendente dal file system
- Analizza immagini o dischi alla ricerca di sequenze di bit predefinite
- **Algoritmo di ricerca diverso** rispetto a Scalpel



Più veloce
Non tutti i file vengono recuperati!

Cancellazione e recupero di informazioni

Photorec vs Scalpel

Photorec
- Più veloce
- Meno file ridondanti
- Non trova tutti i file

Scalpel
- Trova moltissimi file
- Set di header personalizzabile
- Molto lento
- Molti file duplicati

Soluzione

Analisi del dump con Photorec
Analisi dei restanti dati non estratti con Scalpel

Compromesso tra Tempo, Spazio su disco, File ridondanti

Cancellazione e recupero di informazioni

Esperimento per capire appieno le possibilità di recupero di informazioni su Android e YAFFS

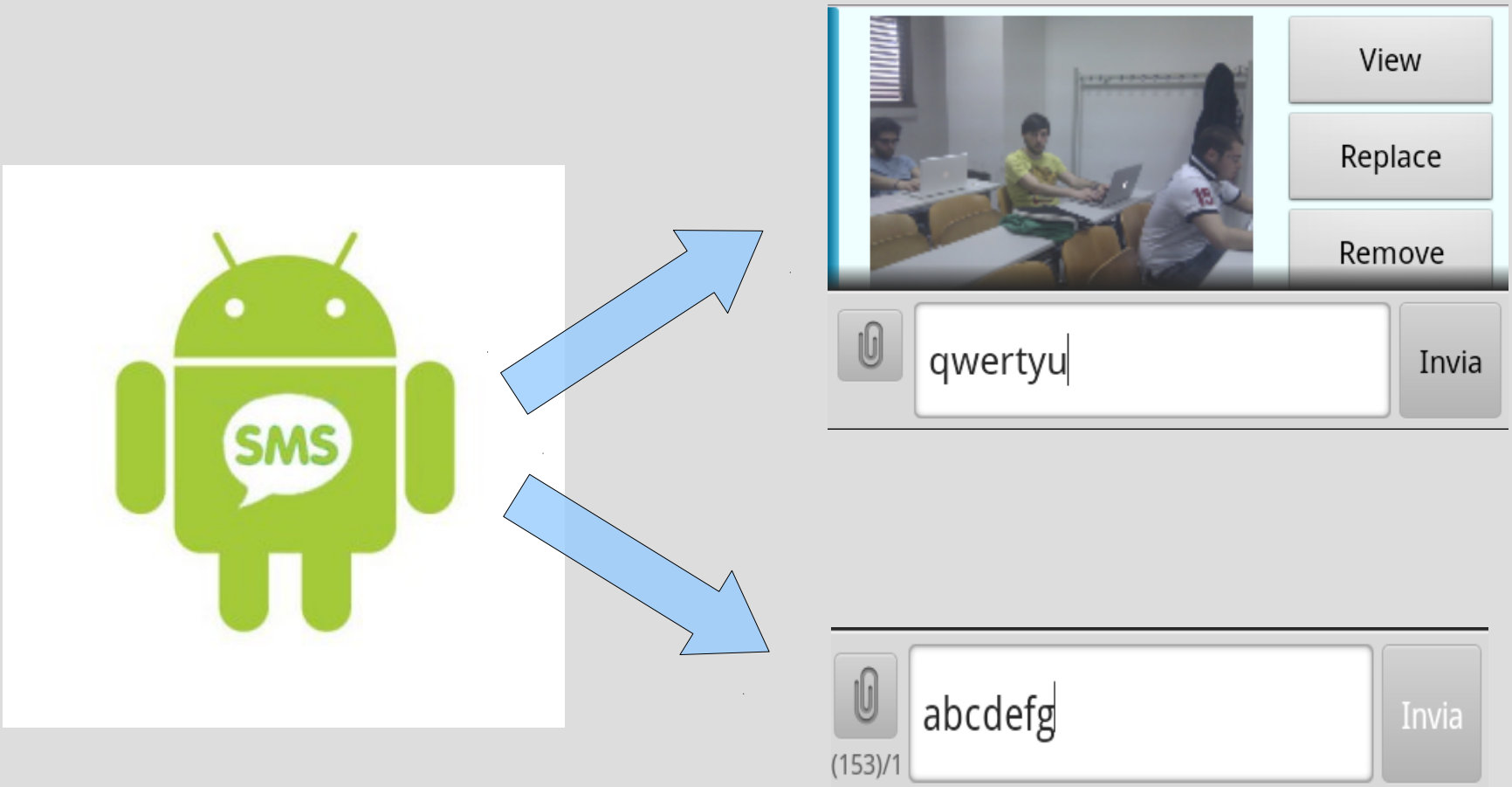
Creazione di informazioni digitali

Rimozione logica delle informazioni

Analisi del dispositivo

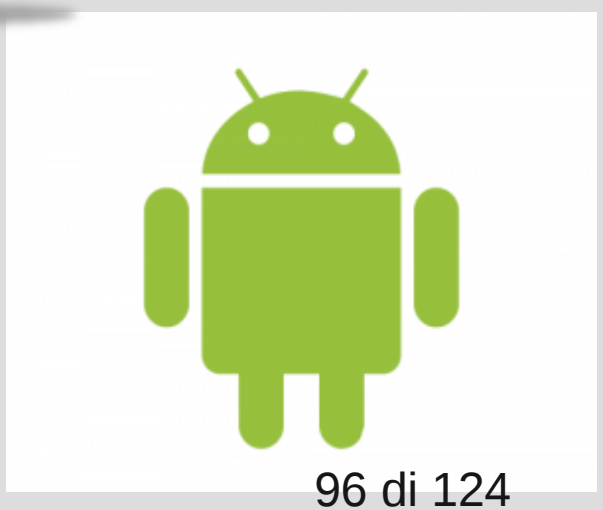
Cancellazione e recupero di informazioni

Creazione ed invio di nuovi messaggi



Cancellazione e recupero di informazioni

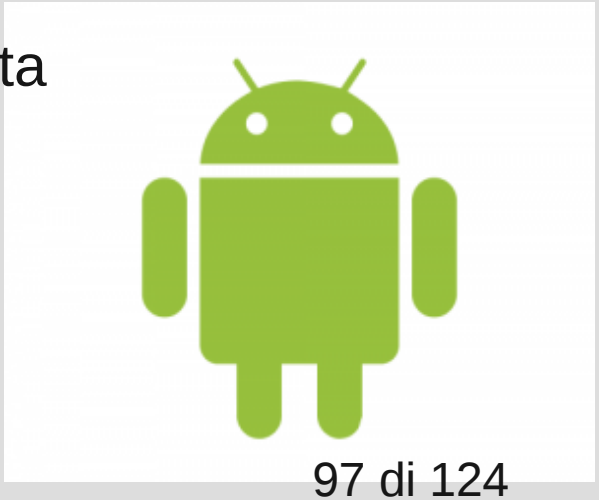
Creazione e modifica di un file di testo



Cancellazione e recupero di informazioni

Cancellazione delle tracce e copia cella partizione data

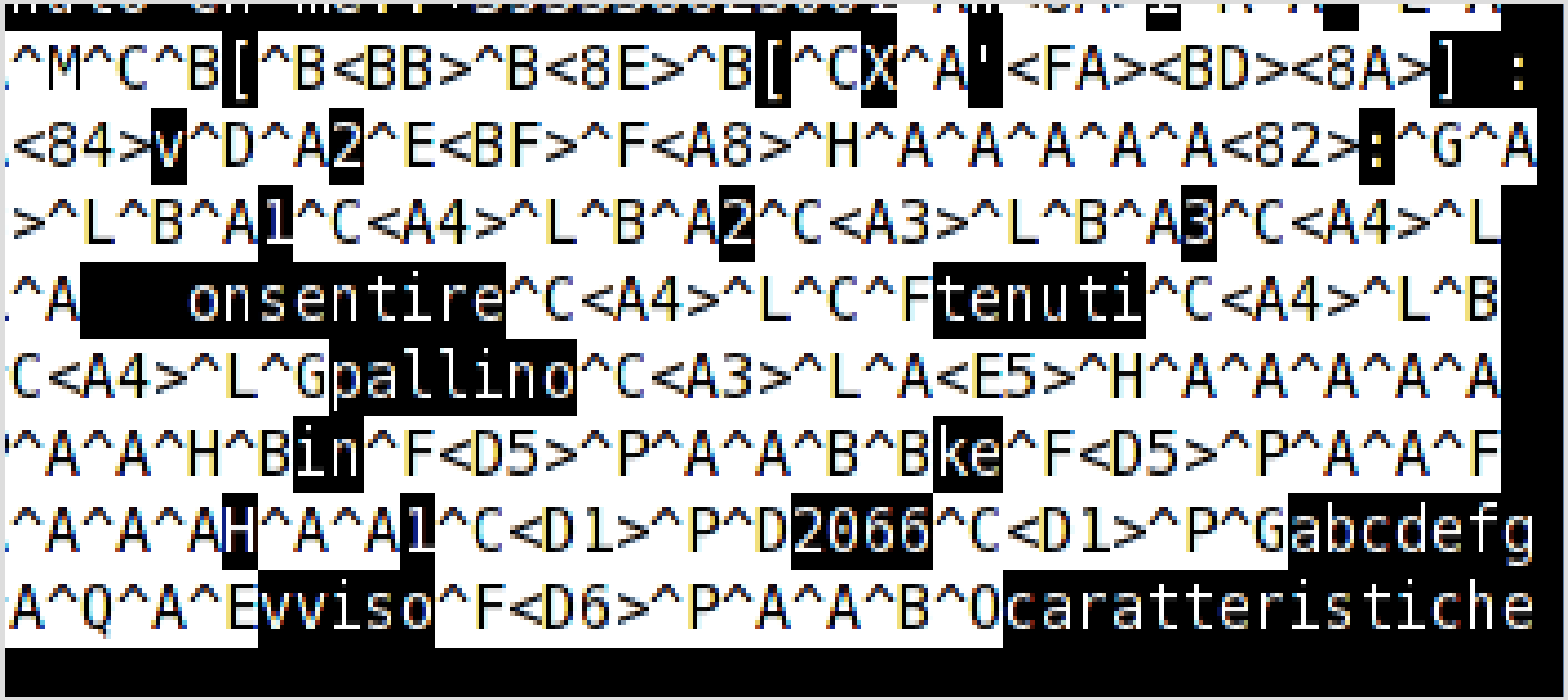
- Cancellazione dei messaggi inviati
- Cancellazione del file creato
- Collegamento al PC tramite cavo usb
- Esecuzione dd della partizione /data
- Esecuzione mkyaffs2image della partizione /data



Cancellazione e recupero di informazioni

Analisi dei dump

Con Unyaffs abbiamo recuperato i messaggi cancellati senza dover ricorrere all'analisi fisica. Android conserva gli ultimi messaggi anche se cancellati!



Cancellazione e recupero di informazioni

Analisi dei dump

Photorec

Le foto inviate
/data/data/cor
Dopo aver elir
cartella, ma P a.

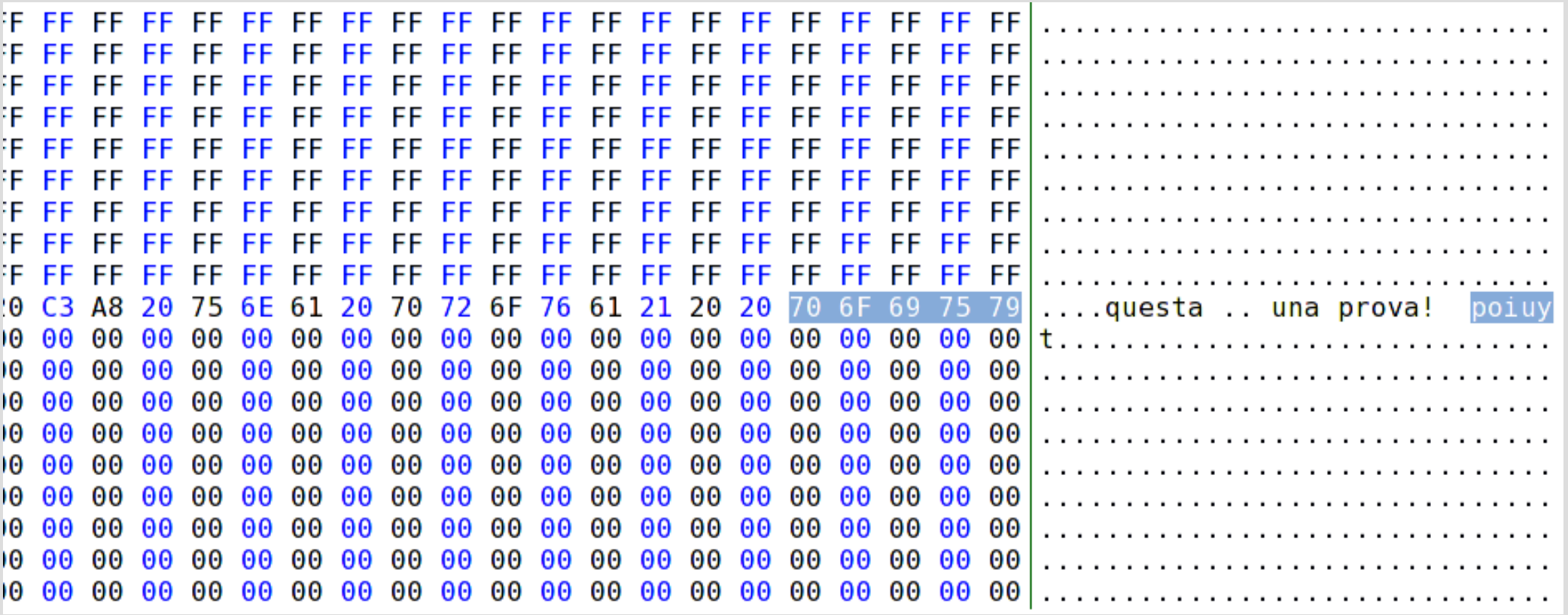
Cancellazione e recupero di informazioni

Analisi dei dump

Ne **Photorec** né **Scalpel** sono stati in grado di trovare il file cancellato

Bless – Editor Esadecimale
E' stata trovata sia la prima versione che la seconda del file di testo

Cancellazione e recupero di informazioni



Alibi Digitale

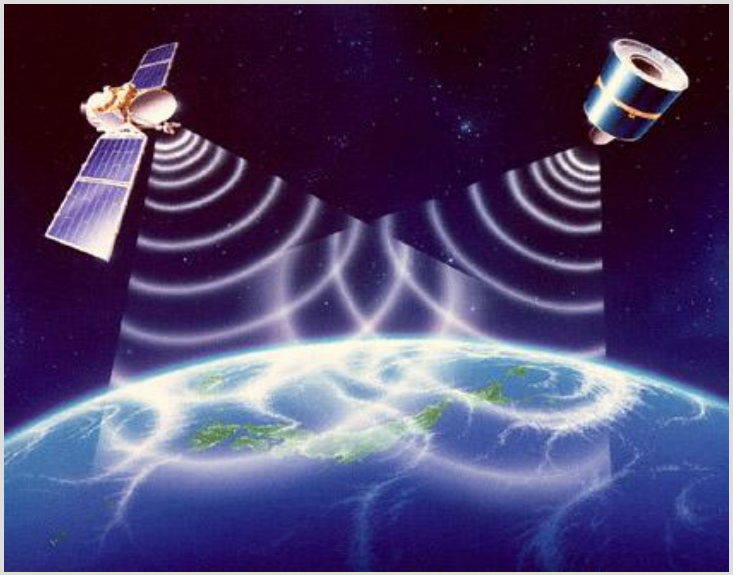
Falso alibi

Insieme di tecniche necessarie per manomettere o cancellare tracce di operazioni illecite.

Con i moderni dispositivi elettronici è possibile utilizzare tecniche apposite per la creazione di un falso alibi attendibile.

Il falso alibi sugli smartphone

La nostra idea si basa sulla modifica e cancellazione di evidenze digitali relative ad applicazioni di geo-localizzazione.



Un primo tentativo: Google Maps...

Applicazione di localizzazione, con navigatore integrato.

- Costruzione dell'itinerario

- Recupero delle informazioni nel navigatore

- Tentativo di modifica delle date e dei luoghi reali

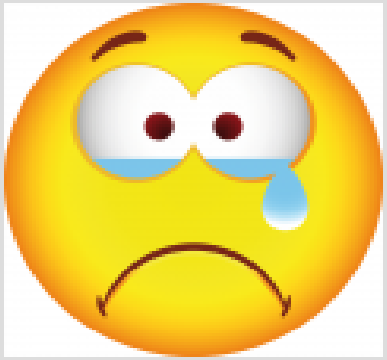
Un primo tentativo: Google Maps...

```
' VDenUSÜ*epMû7ÙµF^é{ÕÆo{ÕÆo{ÕÆo{ÕÆo{ÕÆo@H    @
@ P    @     @@À½!Â±@F@_èQÉþ%ø)@F`_èQÉETöý¿uD"¿Î<~BS D"¿ÐÓCÿ{ÑFD"À¿Ï>@Àñþ<£ /óUÚS(#ë-D" ¿Ï©?çh[¢B@F@_çèéKG7V¯@F`_ç40I)z
nD"¿Ï}YBèM³dÜD" ¿ÎÀAAKt%D"À¿ÐBõ9×ØD"À¿ÎD;KgX<£ /ô.QTAdGBD" ¿ÐÑF s[8Qù G6y°Üæ@F`_æ^ÖEBN@F@_æ¤H@¿¸CN8QúìX_E^
`D"À¿ÍK9}Û¢*4(Àý
GÄÊLoD" ¿ÍÌÞH¡ÝUD"¿Í!ByBÈ4(ÀüWõ9Ò    Q>Ý8Q`úÇXþ<ki<¢à/òêÅGÃÊ°d<£ /ò2@o8Q`ùsB*c
§õhPb1
```

...Tentativo fallito

Idea: modificare i timestamps dei file e, dove necessario, cambiarne il contenuto.

Problemi: esclusi i file vocali, i dati restanti erano memorizzati in un formato sconosciuto.



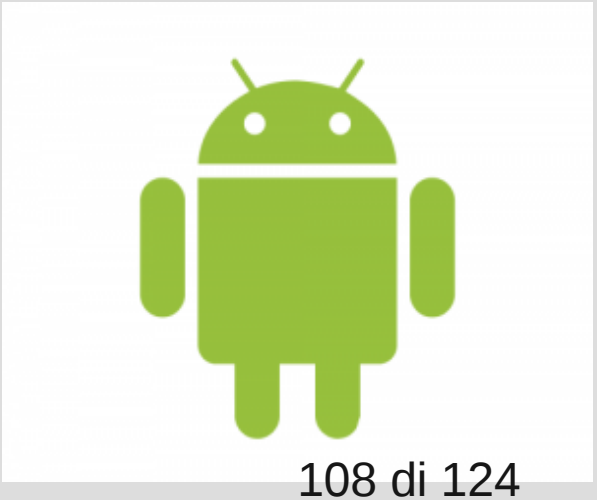
Il secondo tentativo: CoPilot

Applicazione esterna per Android

- Costruzione dell'itinerario

- Recupero delle informazioni nel navigatore

- Tentativo di modifica delle date e dei luoghi reali



Il secondo tentativo: CoPilot

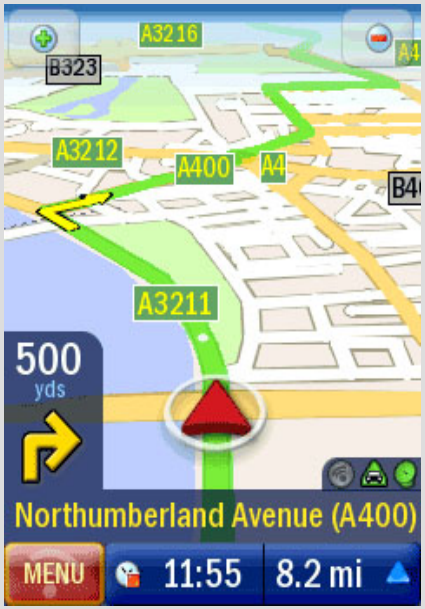
Tutte le informazioni sono memorizzate in plaintext

La struttura di CoPilot

sdcard/copilot: cartella dedicata all'applicazione

- **/copilot/EU/italy/save/[MESE][ANNO]Trip.log**

- **/copilot/gpstracks/[MESE][GIORNO][ANNO].gps**



Dove sono le informazioni di interesse?

CoPilot: Analisi delle tracce

Alcune informazioni sfuggono ad un'analisi “statica” della sd card.

- Installazione del navigatore

- Costruzione e simulazione di un breve viaggio

- Analisi dell'immagine della sd card

Essenziale sapere l'esatto momento in cui i timestamps vengono modificati

CoPilot: Analisi delle tracce(2)

Sviluppo di uno script bash.

Analisi di una specifica directory alla ricerca di file sui quali sia stata effettuata una qualsiasi modifica.

Alcuni file vengono sempre modificati ad ogni esecuzione.

Vediamo il range...

CoPilot: I file

Tre categorie, a seconda delle modifiche riscontrate

- Data di ultimo accesso ad ogni esecuzione

- Timestamp di “change”

- Modifica del contenuto
  [MESE][ANNO]Trip.log &
  [MESE][GIORNO][ANNO].gps

CoPilot: [MESE][GIORNO][ANNO].gps

Il file contiene le informazioni principali per la creazione di un falso alibi attendibile.

Insieme di file con estensione **.gps**

- Il nome coincide con la data in cui è stato effettuato un tragitto.

- Il contenuto comprende informazioni dettagliate riguardo un percorso specifico.

CoPilot: Il formato NMEA

Formato di ogni file **.gps** di CoPilot

Standard di comunicazione per trasmissioni satellitari

Il **talker** invia i dati **(sentences)**
Il **listener** li riceve

$Prefisso,dato1,...,datoN-1,datoN*Checksum

NMEA: Alcune sentences...

- **$GPGGA**
Global Positioning System Fix Data

- **$GPGSA**
GPS DOP and Active Satellites

- **$GPRMC**
Reccomended Minimum Specific GPS/TRANSIT Data

CoPilot: Simulazione

È stata effettuata la simulazione di un percorso su CoPilot...

CoPilot: Modifica delle tracce

Primo passo: modifica del file .gps relativo ad uno specifico percorso

Soluzione: sviluppo di un programma C per la modifica, in pochi secondi, dell'intero file

CoPilot: Modifica delle tracce (2)

Secondo passo: modifica di date di *accesso,modifica,cambiamento e creazione* di uno specifico file

Soluzione: sviluppo di uno script bash per la modifica di tutte le date dei file di interesse

CoPilot: Risultato finale...

CoPilot: Sviluppi Futuri

- Falso alibi su Google Maps

- Automazione del falso alibi direttamente dal cellulare

- Modifica dei file cache.cell in modo che rispecchi gli orari dell'alibi

Grazie per l'attenzione...