MIAT & MobiFAT

Un nuovo paradigma per l'acquisizione e investigazione di reperti forensi in ambito mobile

a cura di **Alessandro Distefano & Daniele Bocci**

Università di Roma Tor Vergata

INDICE DELLA PRESENTAZIONE :

1.1 Scienza forense

- Scienza Forense (Forensics): applicazione di un ampio spettro di discipline scientifiche per rispondere a quesiti in ambito legale:
  - Principali Ramificazioni: Criminologia, Patologia, Tossicologia, Antropologia, ***Digital Forensics***...
- Origini risalenti all'epoca Romana (primi casi di dibattimenti giudiziari);
  - Diviene scienza con l'utilizzo del metodo sperimentale.
- ***Evidenza:*** generica informazione a cui è possibile attribuire carattere probatorio;
- ***Computer Forensics:*** focus on ***Evidenza Digitale.***
- ***Evidenza Digitale VS Evidenza Classica:***
  - Volume, Cancellazione, Modifica, Copia, Potere Espressivo e Disponibilità.

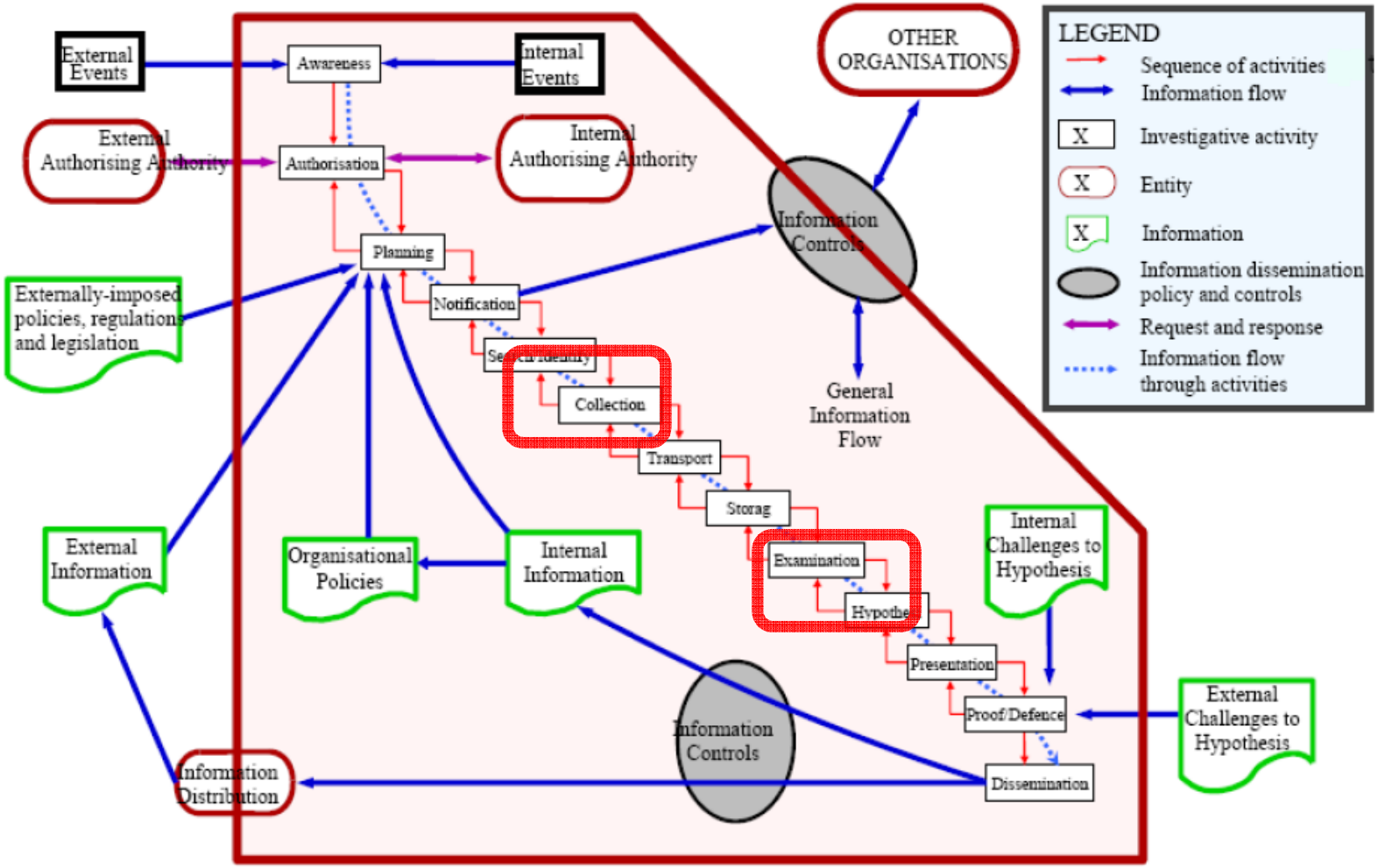
1.2 Computer VS Mobile Forensics

- Rivoluzione digitale → Importanza fondamentale *Computer Forensics* ma non solo...
- Il mercato dei dispositivi digitali è vasto: storage devices, Audio/Video ... e sempre più ***Dispositivi Mobili (DM)***...

	Evidenza Digitale "Classica"	Evidenza Digitale "Mobile"
Isolabilità	**Elevata**	**Impossibile***
Invasività	**Ridotta**	**Variabile**
Interpretabilità	**Elevata**	**Ridotta**
Robustezza	**Elevata**	**Ridotta**
Ampiezza	**Totale**	**Limitata**
Standardizzazione	**Elevata**	**Ridotta**

- Focus su Smartphone.

2.1 Modello investigativo di riferimento [4]



2.2 Fasi modello investigativo

1. ***Awareness***: Comprensione dell'evento scatenante;
2. ***Authorization***: Acquisizione delle autorizzazioni necessarie;
3. ***Planning***: Organizzazione del lavoro di indagine;
4. ***Notification***: Eventuale notifica ai soggetti impattati dal processo di indagine;
5. ***Search & Identification***: Ricerca & Identificazione fonti di informazioni rilevanti;
6. ***Collection***: Collezione delle informazioni;
7. ***Transport***: Trasferimento di ***oggetti*** e/o ***informazioni rilevanti***;
8. ***Storage***: Immagazzinamento sicuro delle informazioni;
9. ***Examination***: Investigazione delle informazioni collezionate;
10. ***Hypothesis***: Formulazione di ricostruzione dei fatti avvenuti;
11. ***Presentation***: Organizzazione delle ipotesi e presentazione ai committenti;
12. ***Proof & Defense***: Discussione delle ipotesi formulate;
13. ***Dissemination***: Eventuale diffusione dei risultati dell'indagine.

2.3 Modello Investigativo: principi

1. Nessuna azione degli investigatori dovrebbe alterare i dati contenuti nel computer o nei dispositivi di memoria:
   - **Implicazioni:** ***Scenari*** e ***tecniche di Collection.***

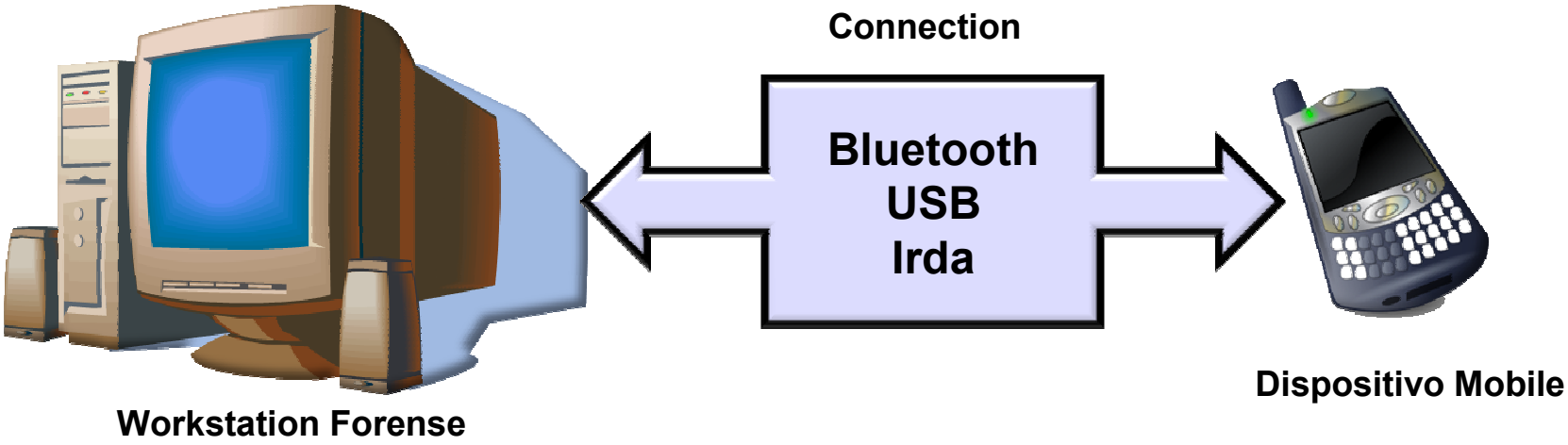
2. Le persone autorizzate ad accedere ai dati originali devono essere competenti;
   - **Implicazioni:** Fasi di Collection, Transport, Storage & Examination.

3. Una cronologia delle operazioni eseguite deve essere mantenuta, terze parti devono ottenere gli stessi risultati applicando le stesse procedure:
   - **Implicazioni:** Tutte le fasi del modello.

4. Assenza di contraddizione tra principi di investigazione e la legge:
   - **Implicazioni:** Azioni che realizzano i flussi di informazioni.

3.1 Collection: approccio attuale

- **NIST[6]:** "...per acquisire dati da un telefono è necessario stabilire una connessione tra il telefono stesso e una workstation forense..."



- Accesso ai dati ottenuto usando una pila di intermediari:
  - Il set di intermediari utilizzato determina la "qualità" della connessione.
- Protocolli ***Open*** (eg. OBEX, comandi AT) VS ***Commerciali*** (eg. DBUS);

3.2 Svantaggi approccio remoto

- Limitazioni dovute all'utilizzo di una connessione remota (protocolli):
  - Copertura del File System e rispetto dell'integrità.

- Forti limitazioni pratiche dovute a necessità di HW specifico:
  - Adattatori e Cavi di collegamento specifici per ogni modello;
  - Ingombro e spesa per gli investigatori.

- Forti limitazioni al parallelismo dovute a HW e workstation forense:
  - Il numero di acquisizioni contemporanee è limitato da:
    - Disponibilità di licenze;
    - Disponibilità di più workstation;
    - Disponibilità di più accessori HW compatibili.

3.3 CSI Stick [7]

- Un miglioramento parziale:
  - Riduzione (non eliminazione) di HW specifico;
  - Eliminazione (temporanea) della workstation;
  - Copia dei dati fisicamente memorizzati;
  - "Riduzione" del costo?

- Tuttavia:
  - Parallelismo ancora limitato;
  - Copia fisica lentissima;
  - Necessità di workstation per Examination;
  - Compatibilità ristretta (Motorola e Samsung):
    - Garanzia incerta sulle funzioni.

4.1 Il nuovo paradigma [1],[2]

- La nostra idea di “buona metodologia”:
  - Esame di tutti i volumi;
  - Supporto al parallelismo;
  - Utilizzo di soli strumenti Open Source;
  - Riduzione drastica del “crime scene equipment”.

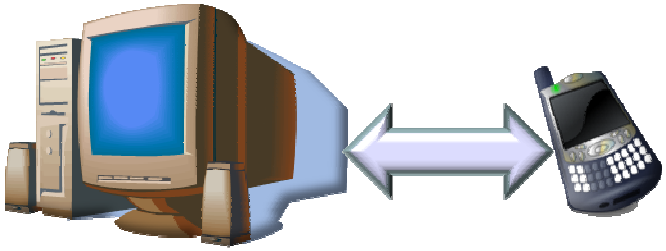
- Necessità di uno strumento di Collection potente per memoria interna;

- Un numero sempre maggiore di smartphone ha un Sistema Operativo;

- Idea cardine: sfruttare il Sistema Operativo come unico intermediario
  - Ottima copertura del FS;
  - Ottimo rispetto dell’integrità;

4.2 Approccio locale

- MIAT è uno strumento SW Forense:
  - Esegue direttamente sul dispositivo mobile;
  - Effettua una copia fedele del FS della memoria interna.
  - I dati sono replicati su supporto rimovibile ed arricchiti (eg. Hashing, attributi).



Acquisizione remota classica

Acquisizione con MIAT

- MIAT è (attualmente) disponibile per:
  - Symbian S60 (versioni precedenti la 9);
  - Windows Mobile 5 e 6.

4.3 Strumenti Open Source

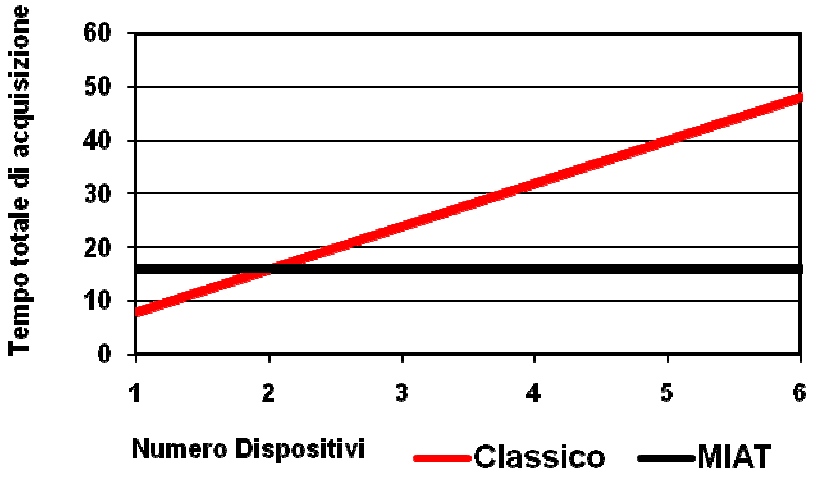
- La metodologia colleziona dati da tutti gli storage tipici degli smartphone:
  - SIM card: dati relativi a chiamate, rubrica e sms;
  - Memory Card rimovibili: dati eterogenei, dati migrati dalla memoria interna;
  - Memoria Interna: dati eterogenei.

- Ogni storage è collezionato con il rispettivo strumento Open Source:
  - SIM card: TULP2G SIM/USIM chip data extraction;
  - Memory Card rimovibili: dd tool;
  - Memoria Interna: MIAT.

4.4 Vantaggi del nuovo paradigma [1]

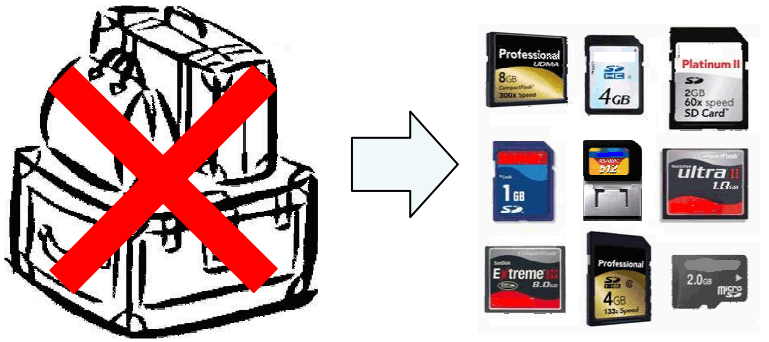
Parallelismo

- Approccio classico → tempo lineare;
- Approccio locale → tempo costante;
- In scenari con molti dispositivi il parallelismo è importante.



Assenza di HW specifico

- Ogni strumento HW -> un modello;
- Ogni memory card -> più modelli;
- Il "crime scene equipment" viene ridotto drasticamente.



5.1 MIAT e il nuovo paradigma

- MIAT è il pilastro della nuova metodologia;
- MIAT è il capostipite della generazione di strumenti forensi che seguiranno il paradigma di acquisizione locale;

- Attualmente per Symbian [1], [2] e Windows Mobile [3];
- In futuro:
  - Altri sistemi operativi per smartphone;
  - Altri tipi di dispositivi: PDA, palmari, etc.

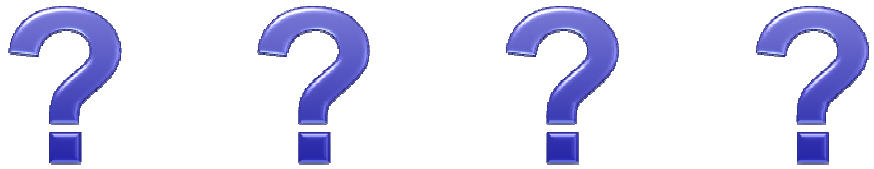
- Requisito fondamentale per acquisizione locale: *i DM devono possedere sufficiente "intelligenza" ;*
- La diffusione di DM con veri e propri sistemi operativi è in crescita.

5.2 Evoluzione workstation forense

- Paradigma locale = scomparsa workstation forense (FW)?
  - Durante la Collection il DM stesso diventa una FW;
  - Le garanzie forensi sul trattamento dei dati sono a carico del sistema operativo:
    - MIAT è liberamente investigabile poiché Open Source.
  - Durante la Examination è necessario soltanto uno strumento di analisi adeguato:
    - Disaccoppiamento di Collection e Examination;
    - Possibile integrazione di più fonti di informazioni;
    - Ampliamento della capacità investigativa...

5.3 Evoluzione incompatibilità HW

- Paradigma remoto = forti problemi di incompatibilità HW (Cavi Usb, etc)
  - Superabile solo con l'utilizzo dell'accessorio HW adatto;
  - The tool you need is the tool you miss!
  - Necessità di fornire supporto alla scelta dei tool.
- MIAT trasforma l'incompatibilità HW in SW:
  - Ogni "serie" di modelli necessita della corretta copia di MIAT;
  - Tipicamente il processo di compilazione non può essere un "crime scene task";



- Fornire automaticamente la corretta copia precompilata di MIAT.

5.4 MIAT: scelte progettuali

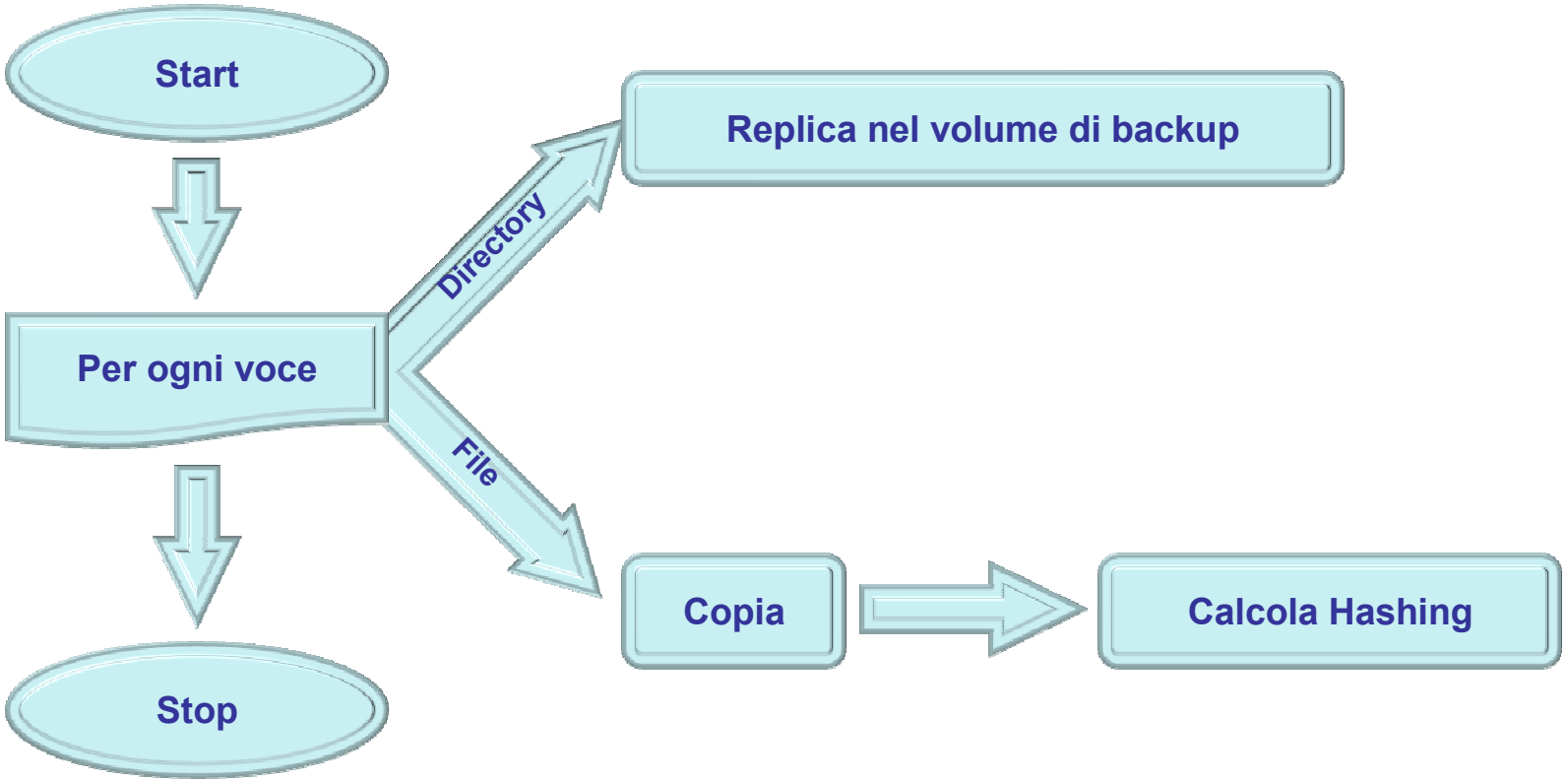
- Migliore prossimità e copertura del FS:
  - Applicazione che utilizza le API native del Sistema Operativo;
  - Il set di intermediari è ridotto al minimo.

- Minima invasività e massima facilità di utilizzo:
  - Applicazione comune;
  - Nessun intervento “spinto” di modifica al SW del dispositivo;
  - Unico passo (eventualmente) necessario: installazione di MIAT.

- Queste scelte consentono un accesso all’intera struttura logica del FS:
  - Tutti i file logicamente presenti sono collezionati;
  - I file logicamente (ma non fisicamente) cancellati non sono collezionati.

6.1 MIAT: Una comune applicazione

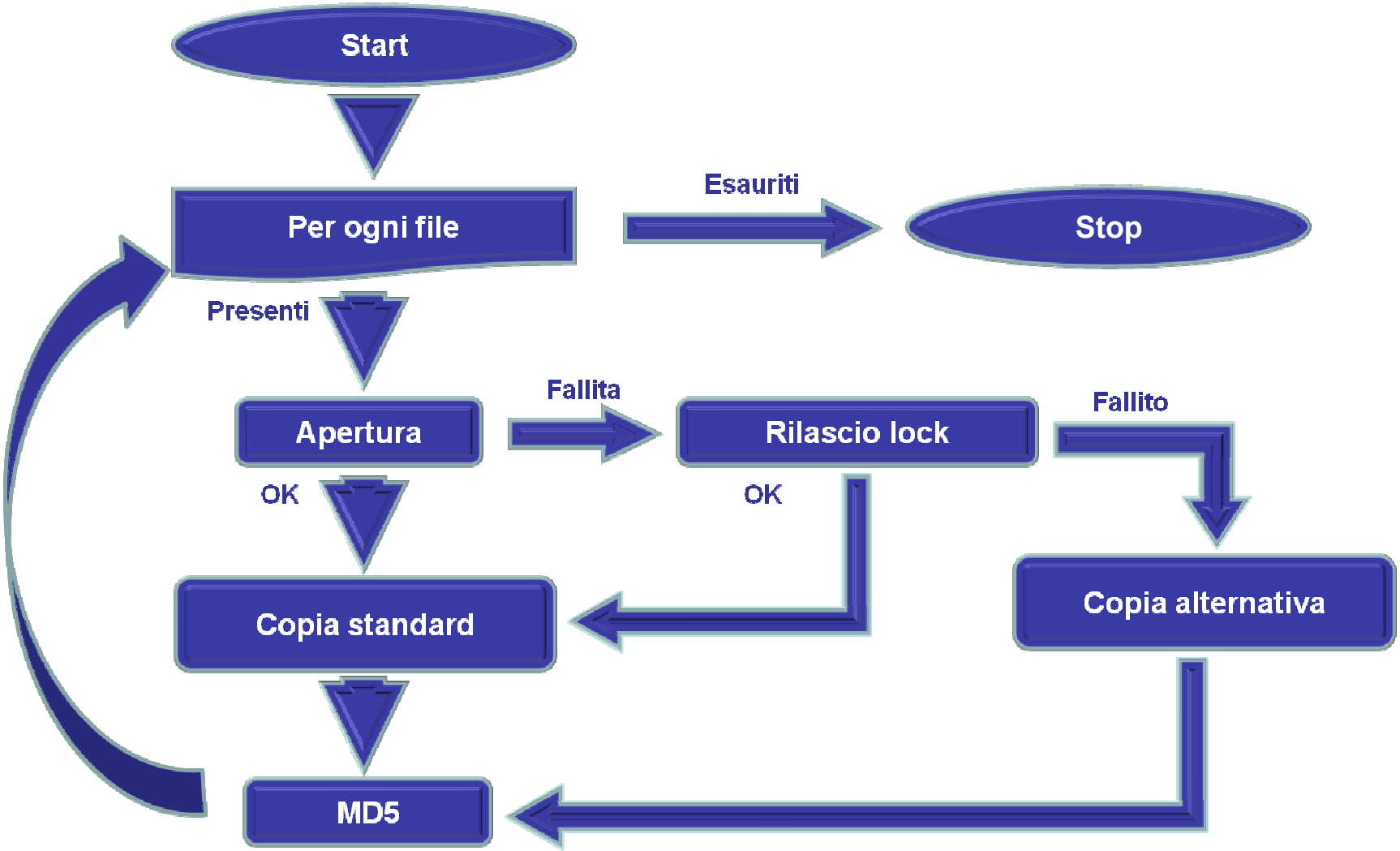
- MIAT iterativamente esplora il FS e replica ogni entry trovata sul volume di backup rimovibile.



6.2 MIAT: Workflow di utilizzo

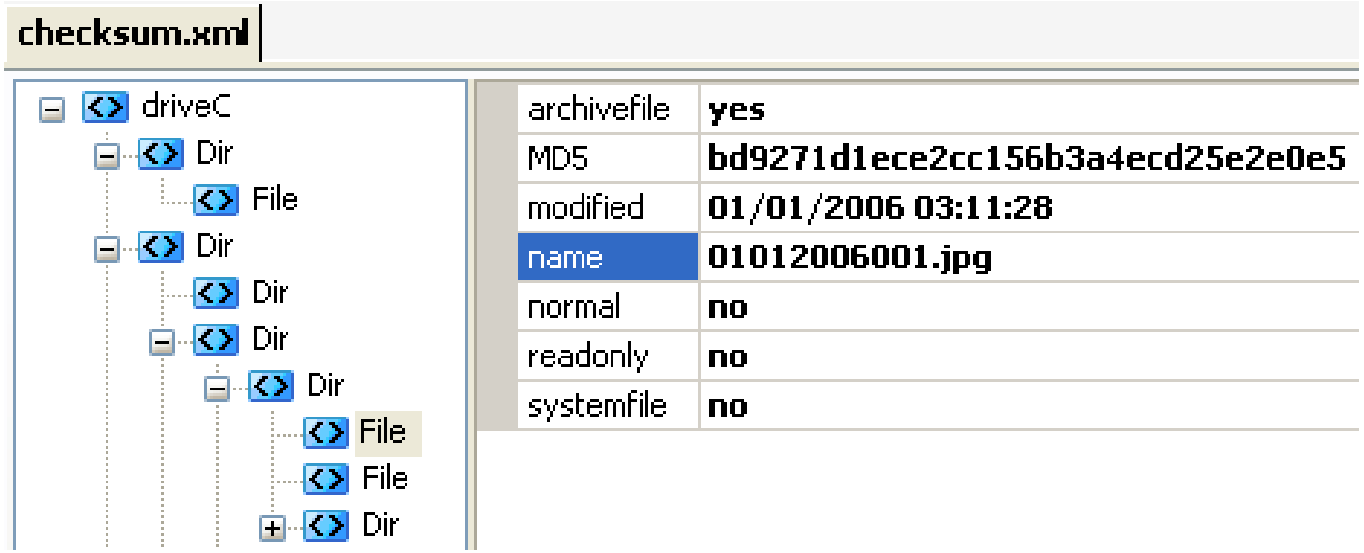
- In generale il workflow di utilizzo è il seguente:

6.3 MIAT: algoritmo di funzionamento



6.4 MIAT: dati estratti

- La sola interazione richiesta all'operatore è l'installazione ed avvio;
- Ogni elemento è marcato con un hash MD-5;
- Per ogni elemento sono collezionati dei dati aggiuntivi;
- Tutte queste informazioni sono organizzate in file Xml;



- La struttura del backup riflette esattamente quella del FS.

7.1 Accertamento: code reading VS esperimenti

- Necessaria fase di accertamento delle proprietà forensi[1]:
  - Rispetto dell'integrità;
  - Copertura del FS.

- MIAT è Open Source:
  - Possibile indagare il suo funzionamento;
  - L'ispezione del codice fornisce molte informazioni (Algoritmo, API, ...) ma...
  - E' necessaria anche la sperimentazione.

- Per tool non Open Source:
  - Non è possibile indagare il funzionamento;
  - Non si possiede alcuna informazione sul codice sorgente;
  - Brian Carrier[5] evidenzia problemi con il Daubert test.

7.2 Accertamento: code reading [1]

- MIAT non ha veri e propri competitor Open Source:
  - L'unico tool forense paragonabile è TULP2G;
  - TULP2G per memoria interna, si basa su OBEX e/o AT-Command;
  - TULP2G = Approccio remoto.
- TULP2G:
  - Open Source ma...
  - Intermediari utilizzati non Open Source;
  - Utilizzo di sequenze di comandi che potrebbero alterare i volumi.
- MIAT:
  - Utilizza esclusivamente API native del Sistema Operativo in sola lettura;
  - Il comportamento è ben definito;
  - Soltanto l'implementazione delle API non è investigabile (Symbian e WM non sono Open Source).

7.3 Accertamento: esperimenti[1]

- La realtà sperimentale ha diversi vantaggi:
  - Impatto evidente e più comprensibile;
  - Dimostra praticamente le proprietà ipotizzate;
  - Fornisce anche misure prestazionali.
- In questo scenario, la capacità di effettuare esperimenti è limitata dal numero di dispositivi.
- E' necessario che ogni dispositivo di test supporti entrambi i *trattamenti.*
- Esperimenti effettuati:
  - Paraben Device Seizure v1.3.2824.32812 vs MIAT-S60;
  - Nokia N70 e Nokia 6630;
  - Sono state effettuate acquisizioni incrociate per valutare la corruzione del FS.

7.4 Accertamento: risultati degli esperimenti[1]

Device	Tool	Time (min)	Size (MByte)
N70	MIAT	≈ 12	6.65
	Paraben	≈ 8	7.28
6630	MIAT	≈ 50	5.73
	Paraben	≈ 15	8.86

- Le differenze nei valori di size dipendono dallo schema di organizzazione delle informazioni addizionali(file distribuiti di Paraben).
- Le prestazioni di MIAT dipendono anche dal dispositivo.
- Considerando il parallelismo...

- Paraben ha mancato alcune directory (_PAlbTN) con entrambi i dispositivi.
- Entrambi i tool rispettano l'integrità*.
- In entrambi i casi, sono state rilevate delle corruzioni in alcuni file di sistema.

Property	MIAT	Paraben
Coverage	+	±
Integrity	+	+

- Attualmente sono in corso sperimentazioni estese e accertamenti formali del set di file modificati.

7.5 Proprietà forensi: Rispetto dell'integrità[1]

- Alcuni file sono modificati:
  - Anche un avvio del dispositivo causa modifiche, tuttavia...
  - File ad uso del Sistema Operativo, quindi di scarsa rilevanza.
  - E' possibile delimitare formalmente il set di file modificati e non utilizzarli.

Table 4 – Paraben last modification time changes

File	Reboot	Acquisition
CommonData.D00	X	X
LocaleData.D05	X	X
backupdb.dat	X	X
btregistry.dat	X	
cbtopicsmsgs.dat	X	
CntModel.ini	X	X
HAL.DAT	X	
ECom.lang	X	
ScShortcutEngine.ini	X	X
nssvasdatabase.db	X	X
100056c6.ini	X	
101f6df0.ini	X	X
System.ini	X	
AlarmServer.ini	X	X

X means that a change happens.

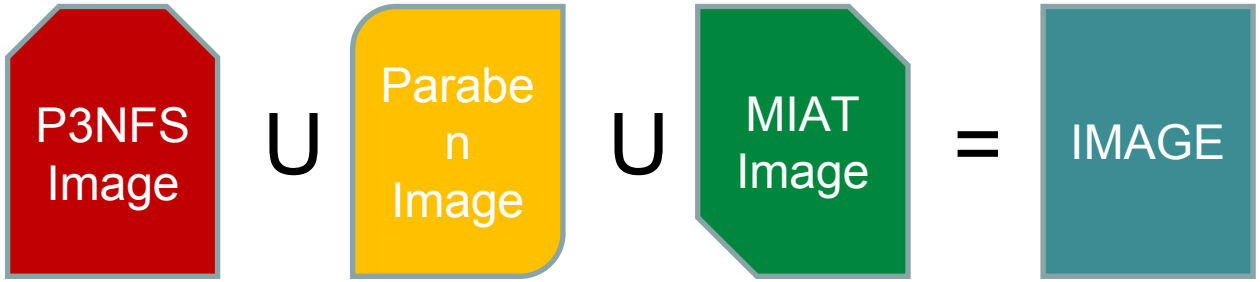
Table 3 – MIAT last modification time changes

File	Reboot	Acquisition
smssmssegst.dat	X	
CommonData.D00	X	
LocaleData.D05	X	
Applications.dat	X	X
backupdb.dat	X	
btregistry.dat	X	
cbtopicsmsgs.dat	X	
CntModel.ini	X	
DRMHS.dat	X	
HAL.DAT	X	
ECom.lang	X	
ScShortcutEngine.ini	X	
nssvasdatabase.db	X	X
100056c6.ini	X	
101f6df0.ini	X	X
System.ini	X	

X means that a change happens.

7.6 Proprietà forensi: Copertura del File System

- Come valutare il livello di copertura del FS?
  - Non si ha un'immagine assoluta di riferimento...
  - Soluzione usata: controllo incrociato tra gli strumenti (P3NFS).



- Il livello di copertura si ottiene per differenza da IMAGE:
  - MIAT presenta un'immagine identica a quella di riferimento...
  - Paraben ha mancato alcune directory (Thumbnails della galleria).
- Estrazione file cancellati non è stata indagata sperimentalmente:
  - MIAT NON è in grado di farlo (copia la struttura LOGICA del FS)...

8.1 Analisi dei dati repertati

- Attualmente Examination ha dipendenze da Collection:
  - Suite integrate di Collection+Examination (eg. XRY, Paraben DS, ...);
  - In generale, non è possibile scindere Collection & Examination.

- Inoltre molte informazioni non sono immediatamente comprensibili (eg. Rubrica, SMS, MMS, ...):
  - Necessità di uno strumento di supporto all'investigatore.

- Tipicamente Examination richiede molto tempo.

- Stabilire i collegamenti tra i dati collezionati è (attualmente) lavoro manuale.

8.2 Analisi: stato dell'arte

- In generale gli strumenti di analisi in commercio sono legati esclusivamente al relativo strumento di collezione;

- Forniscono una ampia visione dei file collezionati:
  - Informazioni immediatamente interpretabili (eg. Immagini, ...);
  - Informazioni non immediatamente interpretabili (eg. Db rubrica, ...);

- Vincolano l'investigatore.

- Non presentano supporti automatici all'investigazione:
  - L'investigatore spende molto tempo (ad esempio) per stabilire collegamenti tra le informazioni.

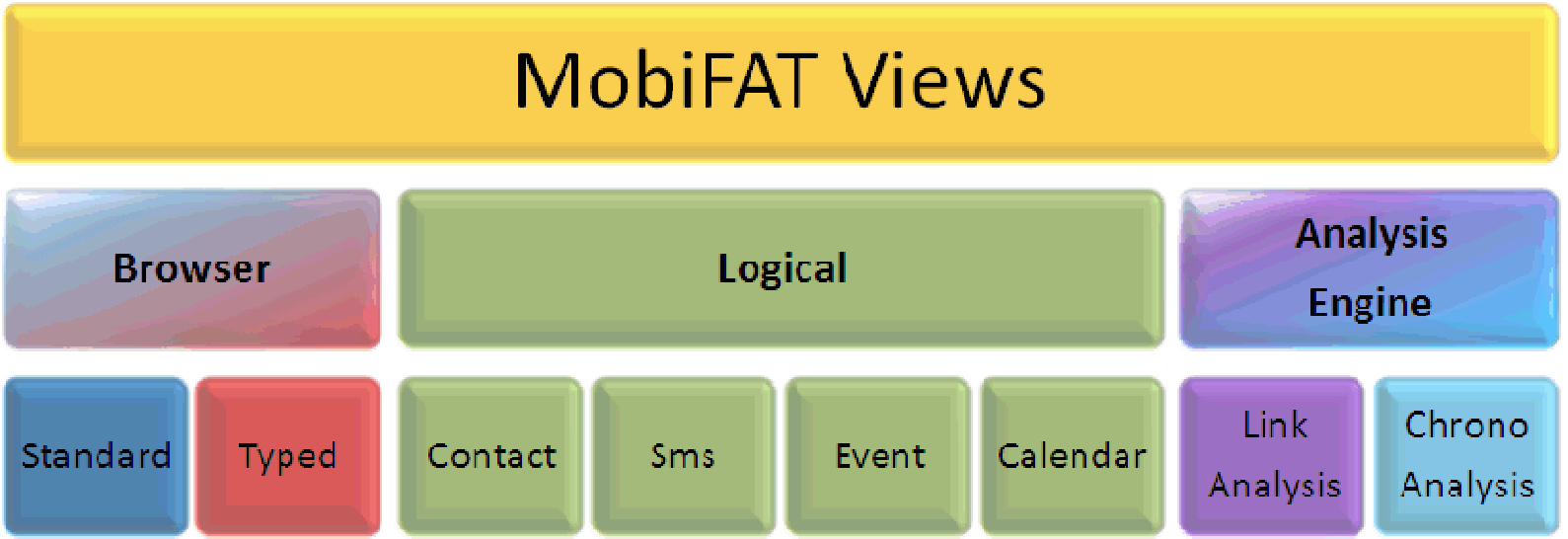
9.1 Necessità di uno strumento nuovo

- Necessità di esaminare i dati collezionati con MIAT;
- Desiderio di "innovazione":
  - Realizzazione di uno strumento dalla compatibilità più ampia;
  - Realizzazione di un effettivo supporto all'investigatore;
  - Realizzazione di uno strumento più "permissivo";

9.2 MobiFAT: principi cardine

- Processo di sviluppo SW prototipale:
  - Con attenzione a strutturazione razionale.
- Strato intermedio informativo Xml:
  - Dati non immediatamente interpretabili tradotti in Xml;
  - Flessibilità di utilizzo e robustezza verso modifiche;
- Insieme di viste complementari e indipendenti:
  - Dati immediatamente interpretabili;
  - Dati non immediatamente interpretabili;
  - Supporto automatico all'investigazione.

9.3 MobiFAT: viste sui dati

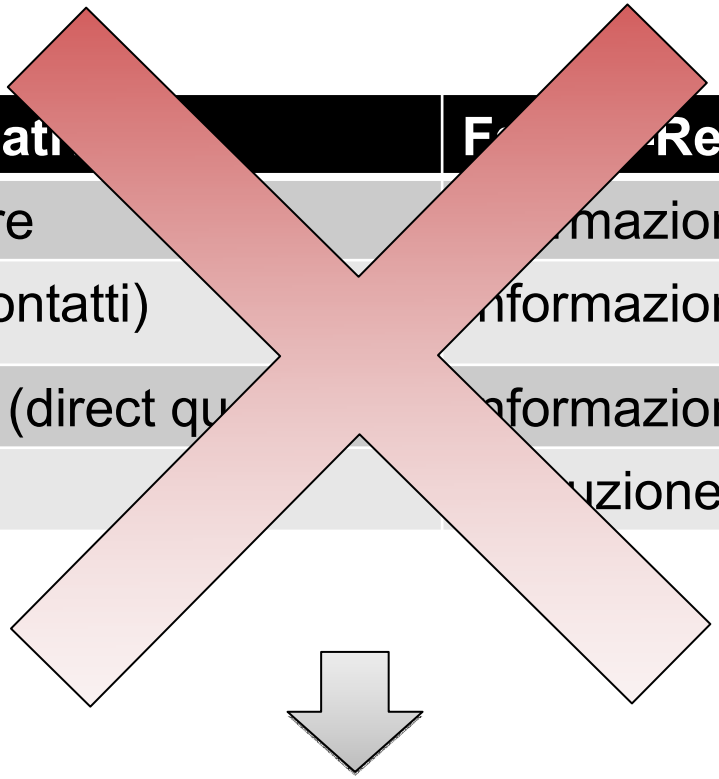


10 MobiFAT: Logical View

- **Obiettivo:** Presentare i dati memorizzati in uno smartphone FS (eg. Rubrica, SMS, LogEventi, Calendario,…)
- **Problema:** Dati non direttamente interpretabili
  - Dati gestiti da DBMS proprietari
  - File in formato proprietario
- **Input:** Immagine del file system della memoria interna
- **Output:** Set di file in formato XML

10.1 Logical view: Soluzioni Alternative

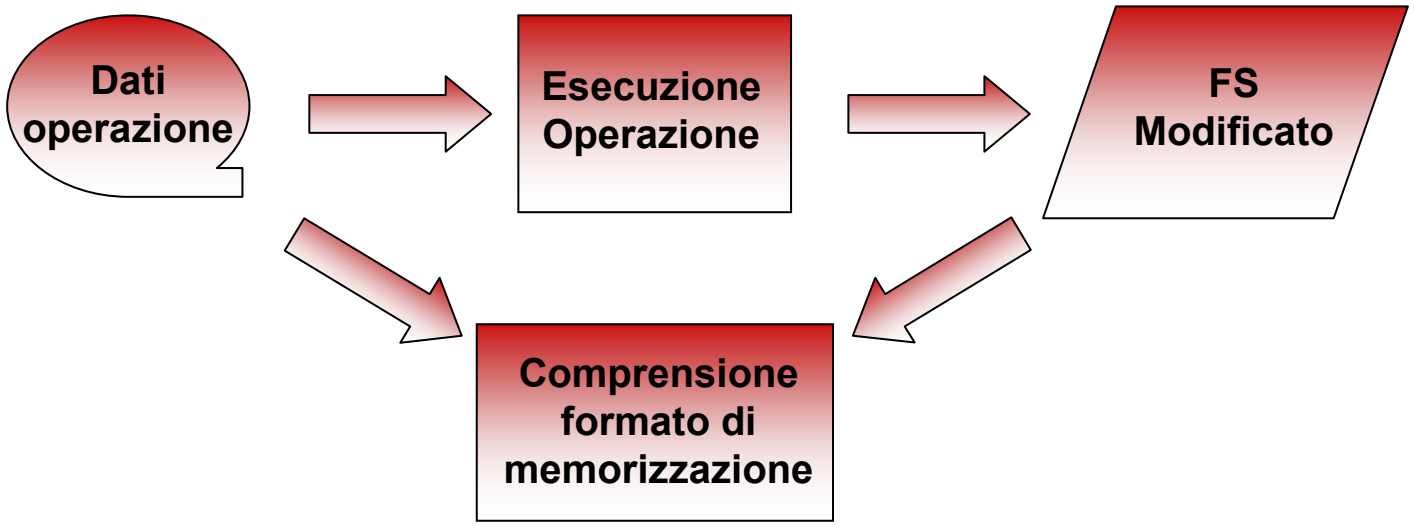
Soluzioni alternati	F -Reason
Utilizzo Emulatore	mazioni parziali
API SO (mod. Contatti)	nformazioni parziali
Python Scripting (direct qu	nformazioni parziali
DBMS-Faking	uzione informazioni



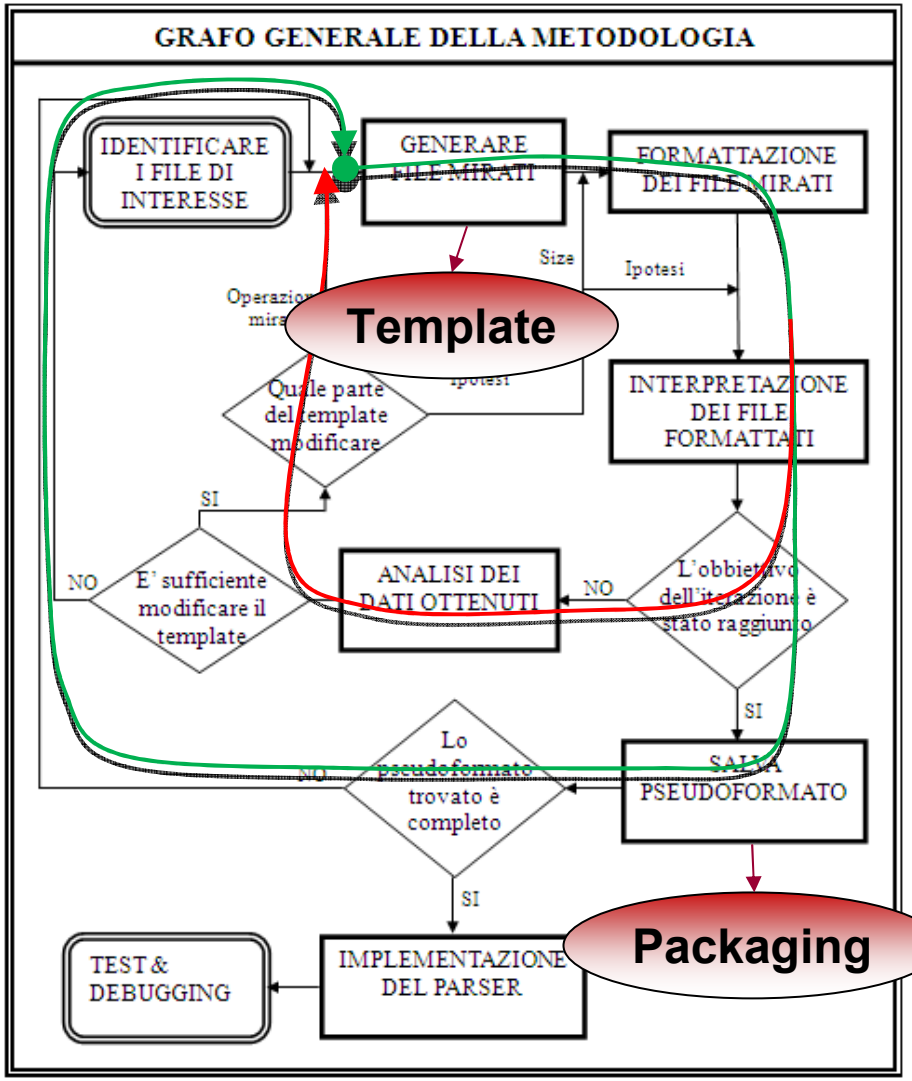
Metodologia 5+3

11 Metodologia 5+3: Idea di base

- Comprendere il formato dei file contenenti i dati di interesse:
  - Definire opportunamente un'operazione con i relativi dati di input
  - Eseguire l'operazione al fine di ottenere il filesystem modificato
  - Comprendere come vengono salvati i dati all'interno del filesystem



11.1 Metodologia 5+3: Best Practice



- Paradigma Divide et impera
- 3 Fasi sequenziali e 5 interne a un processo iterativo incrementale
  - Scenario di successo
  - Scenario Alternativo
- Tracciabilità dei dati tra le fasi
  - Organizzazione Directory
  - Template
- Packaging
  - Template/Obiettivo

11.1 Metodologia 5+3: Fase 1

Fase 1 - Identificare i file di interesse

Scelta Obiettivo

Definire un obettivo, cioè stabilire qual è il dato del quale si vuole scoprire il formato di memorizzazione. Esempi di dato sono:

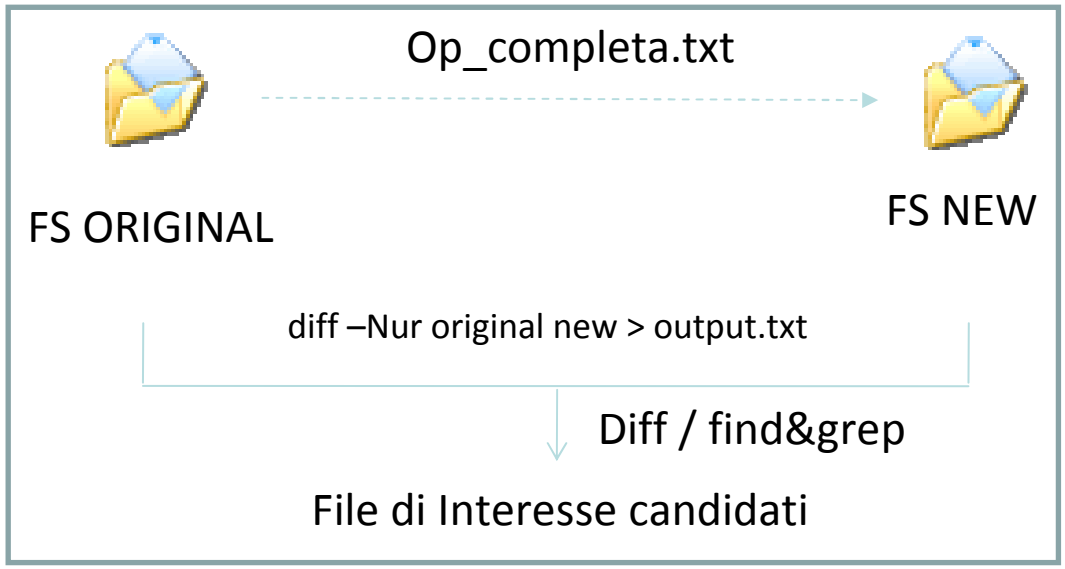
- contatto in rubrica;
- sms;
- file di log;
- etc.

Fase 1 - Identificare i file di interesse

Definizioni:

- ***Operazione Completa***: insieme di una o più operazioni (basate sull'obiettivo) eseguibili dallo smartphone che prevedono un inserimento esaustivo dei dati.
- ***File di interesse***: file influenzato dall'operazione completa.

Strumenti utilizzati: MIAT(o emulatore), diff, find e grep.



11.1 Metodologia 5+3: Fase 1

EventiMisti_Logdbu_Data

Chiamata effettuata al 328...
Chiamata ricevuta dal 328...
Sms inviato al 340... Testo:
Prova
Sms ricevuto dal 340 Testo:
Prova2
MMS inviato al 335...
MMS ricevuto dal 335...
Email inviata al 329...
Email ricevuta dal n.329...
Connessione GPRS
(www.libero.it, www.google.it).

File di interesse: logdbu.dat

```
01 00 00 00 01 48 00 11 6A F1 F0 F0 29 E1 00 01
60 0B 00 00 00 00 00 04 00 00 00 23 02 30 14 3
2 8 4 2 1 5 0 7 7 02 4C 00 2D EE 6D F2
F0 29 E1 00 01 60 0D 00 00 00 02 00 04 00 00 00
23 02 30 1A + 3 9 3 2 8 4 2 1 5 0 7
7 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 3A 41 00 00 00 00 3F 00
54 82 58 82 58 54 4A 05 41 47 86 12 05 2A A1 10
03 10 2E EF 7A F1 29 E1 00 FF A2 02 00 00 00 00
00 04 00 33 0A 50 72 6F 76 61 14 3 4 0 1 0
1 5 1 5 7 18 02 00 00 00 01 00 00 00 01 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 5E 03
F1 70 C7 83 F1 29 E1 00 FF A2 03 00 00 00 05 00
06 00 33 0E 50 72 6F 76 61 20 32 1A + 3 9 3
4 0 1 0 1 5 1 5 7 18 00 00 00 00 01 00
00 00 00 00 00 00 00 05 41 47 86 12 05 2A E1 10
```

11.1 Metodologia 5+3: Fase 1

Stabilire l'obiettivo del processo iterativo, cioè identificare qual è il dato interno al file di interesse del quale si vuole scoprire il formato:

- con il supporto dell'emulatore;
- studiando il file

File di interesse: logdbu.dat

```
01 00 00 00 01 48 00 11 6A F1 F0 F0 29 E1 00 01
60 0B 00 00 00 00 00 04 00 00 00 23 02 30 14 33
32 38 34 32 31 35 30 37 37 02 4C 00 2D EE 6D F2
F0 29 E1 00 01 60 0D 00 00 00 02 00 04 00 00 00
23 02 30 1A 2B 33 39 33 32 38 34 32 31 35 30 37
37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 3A 41 00 00 00 00 3F 00
54 82 58 82 58 54 4A 05 41 47 86 12 05 2A A1 10
03 10 2E EF 7A F1 29 E1 00 FF A2 02 00 00 00 00
00 04 00 33 0A 50 72 6F 76 61 14 33 34 30 31 30
31 35 31 35 37 18 02 00 00 00 01 00 00 00 01 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 5E 03
F1 70 C7 83 F1 29 E1 00 FF A2 03 00 00 00 05 00
06 00 33 0E 50 72 6F 76 61 20 32 1A 2B 33 39 33
34 30 31 30 31 35 31 35 37 18 00 00 00 00 01 00
00 00 00 00 00 00 00 05 41 47 86 12 05 2A E1 10
```

11.2 Metodologia 5+3: Fase 2

Fase 2 – Generare file mirati

Definizioni:

- ***Operazione mirata:*** sequenza di operazioni atte a modificare il file di interesse al fine di facilitare l'esecuzione delle fasi successive.
- ***File mirato:*** file di interesse ottenuto in seguito all'esecuzione dell'operazione mirata.
- ***Template del processo:*** insieme di ipotesi che guideranno l'iterazione attuale del processo iterativo incrementale.

Strumenti utilizzati: MIAT, emulatore

Fase 2 – Generare file mirati

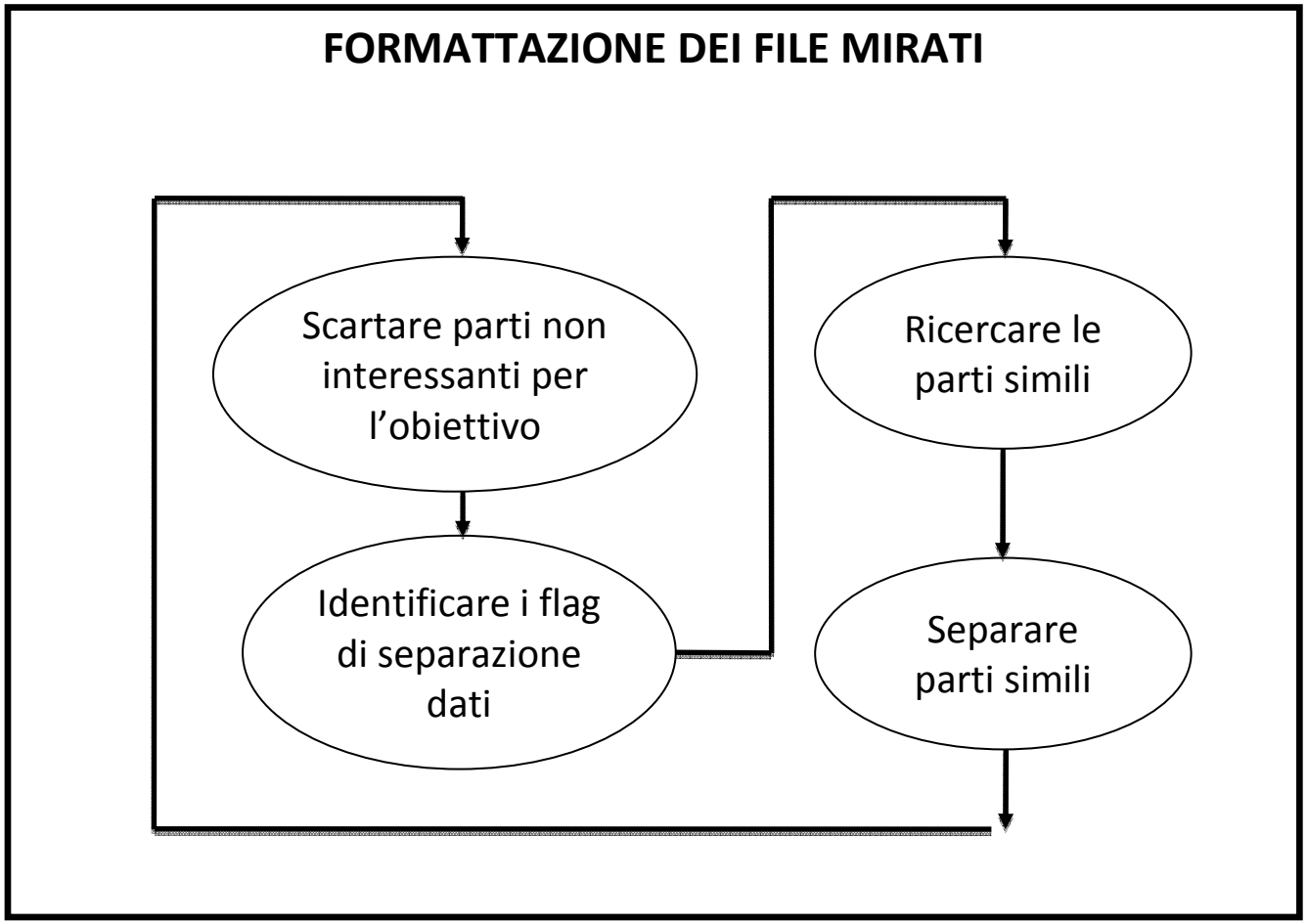
TEMPLATE: FILE MIRATI
Obiettivo: scelta del dato del quale si vuole scoprire il formato di memorizzazione (raffinato nelle iterazioni successive)
Precondizione (in caso di packaging): inserita se il template richiede l'esecuzione di un altro template
Natura, size e tipo obiettivo – controllabile, non controllabile o semicontrollabile. Size in byte. Tipo di dato.
Scala: nominale, ordinale, a intervalli o dei rapporti
Operazione mirata: dati e metadati delle operazioni che la compongono;
Motivazione: perché si pensa che l'operazione mirata porta alla creazione di un file mirato semplice da interpretare?
Nome file di interesse: il nome del file di interesse in esame

11.2 Metodologia 5+3: Fase 2

TEMPLATE: FILE MIRATI (Esempio)

Obiettivo: durata delle chiamate/videochiamate
Natura , Tipo e Size: costante, intero(secondi), 2 o 4 byte
Scala: dei rapporti
Operazione mirata: chiamate al Centro Servizi (119)
07/04/2008 16:31:39 chiamata out di 27 secondi
07/04/2008 16:33:04 chiamata out di 27 secondi
07/04/2008 16:34:46 chiamata out di 1 minuto e 10 secondi
07/04/2008 16:36:27 chiamata out di 1 minuto e 10 secondi
...
Motivazione:
Ogni coppia di chiamate con la stessa durata, avranno sequenze di byte uguali.

11.3 Metodologia 5+3: Fase 3



Condizione di uscita: formattazione adeguata

11.3 Metodologia 5+3: Fase 3

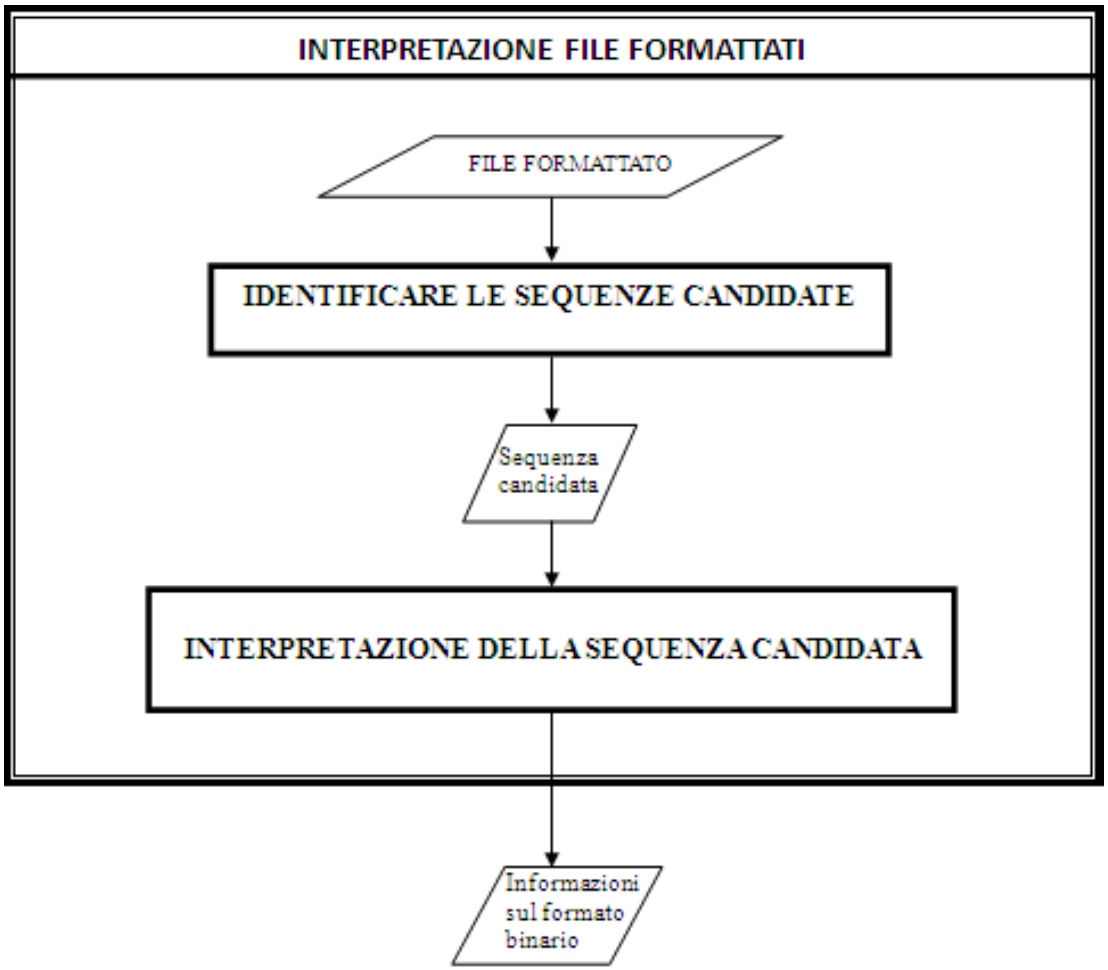
File mirato – durata

00 11 F2 66 B8 58 2A E1 00 01
60 02 00 00 00 00 00 1B 00 00
00 63 02 30 06 31 31 39 02 0C
00 00 00 46 00 DD 6E 82 BD 58
2A E1 00 01 60 03 00 00 00 00
00 1B 00 00 00 63 02 30 06 31
31 39 02 0C 00 00 00 46 00 9C
7F 98 C3 58 2A E1 00 01 60 04
00 00 00 00 00 46 00 00 00 63
02 30 06 31 31 39 02 0C 00 00
00 46 00 C1 EB 9C C9 58 2A
E1 00 01 60 05 00 00 00 00 00
46 00 00 00 63 02 30 06 31 31
39 02 0C 00 00 00 46 00 FB 96
CA CF 58 2A E1 00 01 60 06 00
00 00 00 00 C8 00 00 00 63 02
30 06 31 31 39 02 0C 00 00 00
46

File formattato

00 11 F2 66 B8
58 2A E1 00 01 60 02
00 00 00 00 00 1B
00 00 00 63 02 30 06 NUM
02 0C 00 00 00 46
00 DD 6E 82 BD
58 2A E1 00 01 60 03
00 00 00 00 00 1B
00 00 00 63 02 30 06 NUM
02 0C 00 00 00 46
00 9C 7F 98 C3
58 2A E1 00 01 60 04
00 00 00 00 00 46
00 00 00 63 02 30 06 NUM
02 0C 00 00 00 46 ...

11.4 Metodologia 5+3: Fase 4



11.4 Metodologia 5+3: Fase 4.1

Definizioni:

- ***Zona mirata:*** la parte del file formattato che è stata modificata dopo l'esecuzione dell'operazione mirata.

- ***Zona di confronto:*** la porzione del file formattato che è stata modificata dall'esecuzione di una operazione interna all'operazione mirata.

11.4 Metodologia 5+3: Fase 4.1

Esempio di zona mirata e zone di confronto

Zona mirata

00 11 F2 66 B8
58 2A E1 00 01 60 02
00 00 00 00 00 1B
00 00 00 63 02 30 06 NUM
02 0C 00 00 00 46
00 DD 6E 82 BD
58 2A E1 00 01 60 03
00 00 00 00 00 1B
00 00 00 63 02 30 06 NUM
02 0C 00 00 00 46
00 9C 7F 98 C3
58 2A E1 00 01 60 04
00 00 00 00 00 46
00 00 00 63 02 30 06 NUM
02 0C 00 00 00 46 ...

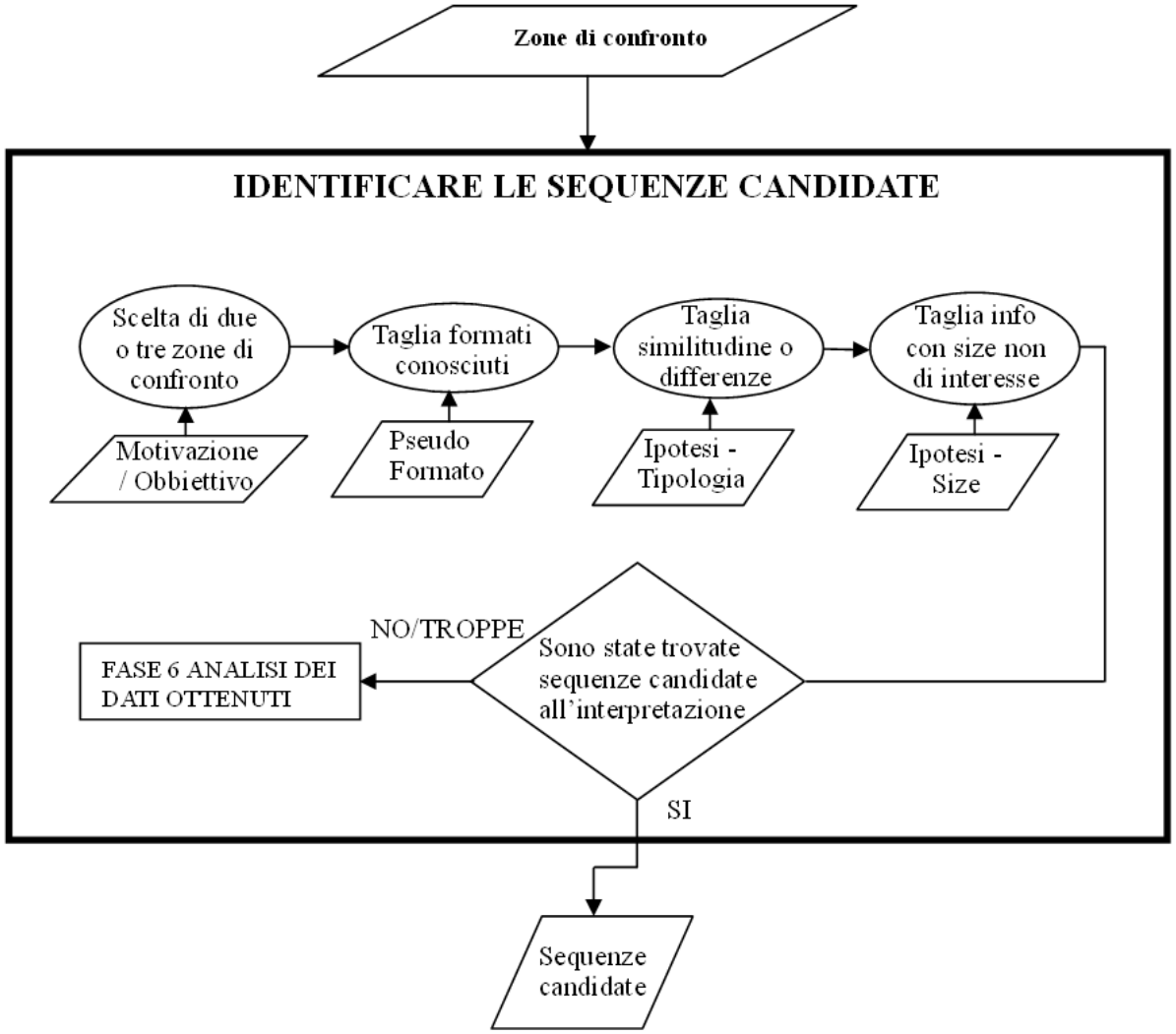
Zone di confronto

00 11 F2 66 B8
58 2A E1 00 01 60 02
00 00 00 00 00 1B
00 00 00 63 02 30 06 NUM
02 0C 00 00 00 46

00 DD 6E 82 BD
58 2A E1 00 01 60 03
00 00 00 00 00 1B
00 00 00 63 02 30 06 NUM
02 0C 00 00 00 46

00 9C 7F 98 C3
58 2A E1 00 01 60 04
00 00 00 00 00 46
00 00 00 63 02 30 06 NUM
02 0C 00 00 00 46 ...

11.4 Metodologia 5+3: Fase 4.1



11.4 Metodologia 5+3: Fase 4.1

Esempio di Identificazione sequenze candidate

----------07/04/2008 16:31:39 chiamata out di 27 secondi----------

00 11 F2 66 B8 **58 2A E1 00 01 60** 02 **00 00 00 00 00** 1B

00 00 00 63 02 30 06 NUM **02 0C 00 00 00 46**

----------07/04/2008 16:33:04 chiamata out di 27 secondi----------

00 DD 6E 82 BD **58 2A E1 00 01 60** 03 **00 00 00 00 00** 1B

00 00 00 63 02 30 06 NUM **02 0C 00 00 00 46**

-------- 07/04/2008 16:34:46 chiamata out di 1 minuto e 10 secondi------

00 9C 7F 98 C3 **58 2A E1 00 01 60** 04 **00 00 00 00 00** 46

00 00 00 63 02 30 06 NUM **02 0C 00 00 00 46** ...

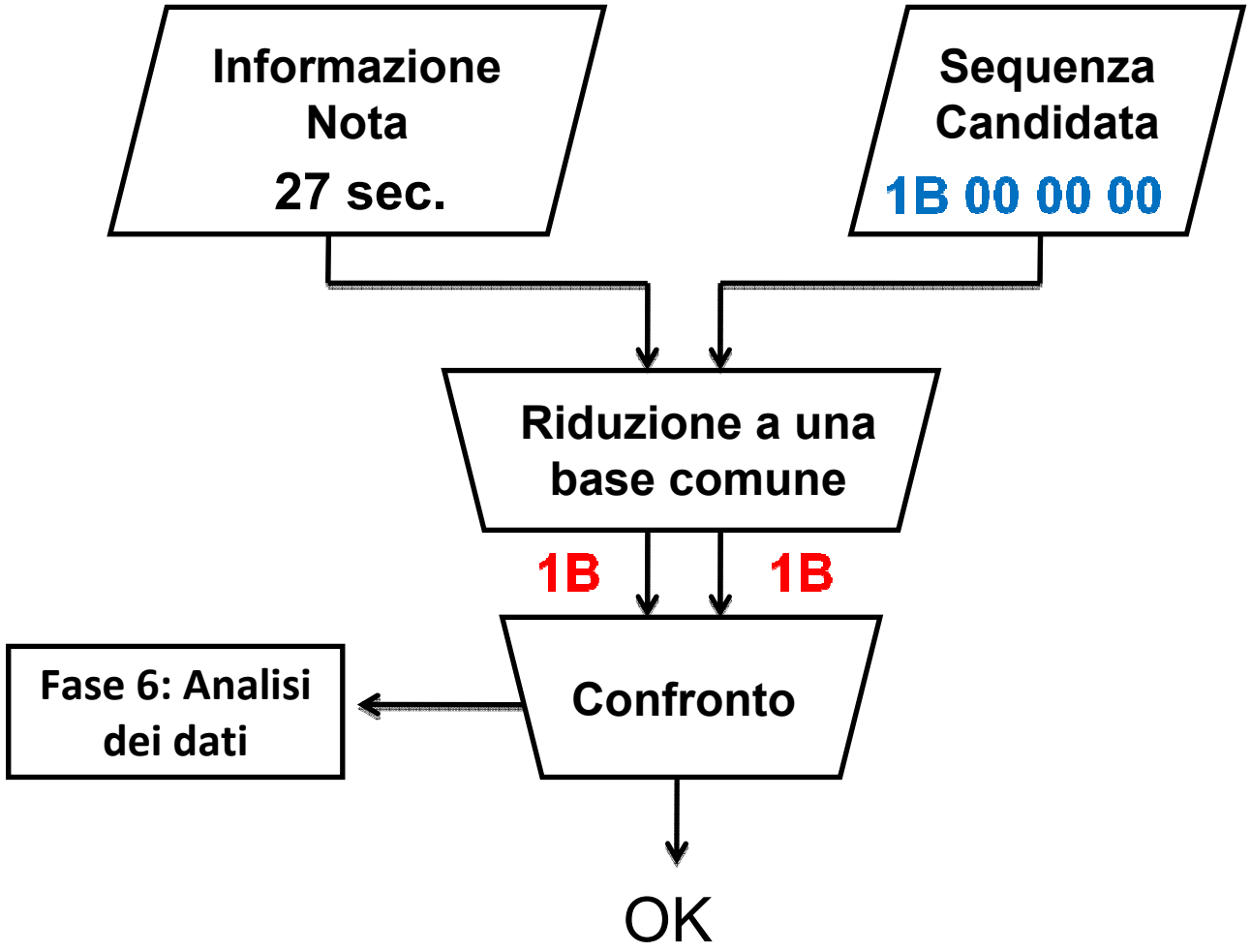
Sequenza Candidata: 1B 00 00 00

***Motivazione*:** Ogni coppia di chiamate con la stessa durata avranno sequenze di byte uguali.

→ Byte diversi tra due coppie di confronto di stessa durata dovranno essere eliminati

→ Se più di due chiamate hanno gli stessi byte questi non saranno indicativi della durata

11.4 Metodologia 5+3: Fase 4.2



11.5 Metodologia 5+3: Fase 5

Fase 5 – Salva pseudoformato

Identificativo	Nome	Size	Tipo di dato	Dettagli di memorizzazione
ID	Id number	4Byte	Intero	Ordine inverso
DC	Duration Call	4Byte	Intero	Ordine esatto

File formattato

00 11 F2 66 B8
58 2A E1 00 01 60 [redacted]
[redacted] 00 00 [redacted]
[redacted] 63 02 30 06 NUM
02 0C 00 00 00 46
00 DD 6E 82 BD
58 2A E1 00 01 60 [redacted]
[redacted] 00 00 [redacted]
[redacted] 63 02 30 06 NUM
02 0C 00 00 00 46

Pseudo Formato

00 11 F2 66 B8
58 2A E1 00 01 60
---ID--- 00 00
---DC--- 63 02 30 06 NUM
02 0C 00 00 00 46
00 DD 6E 82 BD
58 2A E1 00 01 60
---ID--- 00 00
---DC--- 63 02 30 06 NUM
02 0C 00 00 00 46

- Valutare la completezza delle informazioni interpretate
- Utile in fase di test & debugging

Fase 7 – Implementazione del parser

Obiettivo: definizione di linee guida per l'implementazione del parser.

Aspetti critici:
•Nuovi tipi di entità (e.g. Una nuova tipologia di messaggio)
•Nuovi tipi di informazioni (e.g. Foto dei contatti)

Programmazione Procedurale:
- Realizzazione di un file Xml con relativo DTD

Programmazione Object Oriented:
- Ereditarietà da un'unica classe *Event*
- Attributo unknown nella classe *Event*

Fase 8 – Test & Debugging

Obiettivo: validazione degli pseudoformati mediante test case derivati dai template.

Codice con gestione degli errori mirata a identificare la natura del problema:

•la funzione che ha determinato la condizione di errore;

•offset all'interno del file di interesse.

11.8 Informazioni interpretate

Caso di studio	Informazione contenuta	Informazione dettagliata
Logdbu.dat	Log Eventi	Anteprime SMS, MMS e E-Mail Chiamate Videochiamate Connessioni gprs Sostituzione [illegible] (SIM, MC)
Calendar	Memo	DayNote Meeting Anniversary
Contacts.cdb	Rubrica	Informazioni sui contatti presenti in rubrica
/Mail	Sms/MMS/ E-Mail	**Contenuto di SMS, MMS e E-Mail**

HISTORY

Bibliografia e sitografia :

[1] A. Distefano and G. Me, *"An overall assessment of Mobile Internal Acquisition Tool."*, 2008 Digital Forensic Workshop (DFRWS), Journal of Digital Investigation, 2008, Elsevier.
[2] G. Me and M. Rossi, *"Internal forensic acquisition for mobile equipments."*, 4th Int'l Workshop on Security in Systems and Networks (SSN2008), Proceedings of the International Parallel and Distributed Processing Symposium (IPDPS), 2008, IEEE Computer Society Press.
[3] F. Dellutri, V. Ottaviani, G. Me, *"MIAT-WM5: Forensic Acquisition for Windows Mobile PocketPC."*, Proc. of the 2008 Workshop on Security and High Performance Computing Systems, part of HPCS 2008.
[4] S. Ò Ciardhuàin, *"An Extended Model of Cybercrime Investigations"*, International Journal of Digital Evidence, 2004.
[5] B. Carrier, *"Open Source Digital Forensics Tools - The Legal Argument"*, 2003.
[6] W. Jansen and R. Ayers, *"Guidelines on Cell Phone Forensics"*, NIST 2007.
[7] Paraben Corporation, *"Paraben Corporation – sito web ufficiale"*, http://www.parabenforensics.com.
[8] *"Symbian OS – sito web ufficiale"*, http://www.symbian.com/.
[9] *"Windows Mobile – sito web ufficiale"*, http://www.microsoft.com/italy/windowsmobile/6/default.mspx.

Q&A