



Mobile Forensics

Repertamento ed Analisi di Sistemi Radiomobili GSM ed UMTS: la ripetibilità.

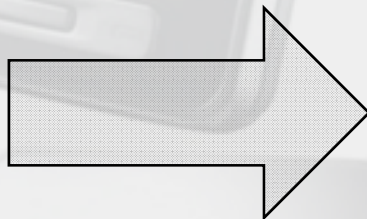
IISFA Forum 2009

Bologna, 8 maggio 2009

Magg. CC Ing. Marco Mattiucci

Mobile Investigation:

- Intercettazione vocale
- Intercettazione digitale
- Radiolocalizzazione
- A-GPS
- ...



Mobile Forensics:

- Repertamento oggetto
- Repertamento dati/virtuale
- Analisi dei dati



Mobile Forensics (“ideale”):

- Si agisce dopo il fatto...
- Il dato è su una memoria digitale...
- Si può applicare a sistemi “live” o “dead”...
- Il sistema radiomobile non rice/trasmette...
- Si esplica in laboratorio...
- Sfrutta metodologie ben assestate...

“...the science of recovering digital evidence from a mobile phone under forensically sound conditions using accepted methods.” (NIST)



Il dato bisogna talvolta aspettare che si depositi nella memoria digitale...

Il sistema radiomobile spesso rice/trasmette...

Sfrutta metodologie spesso da valutare caso per caso...

Mobile Forensics (“reale”):

Si esplica principalmente su 2 fronti:

- 1. Intervento sulla scena del crimine:**
possono svolgersi sia il repertamento fisico dell’oggetto che quello dei dati.
- 2. Attività di laboratorio:** si svolge prettamente il repertamento dei dati e la susseguente analisi.



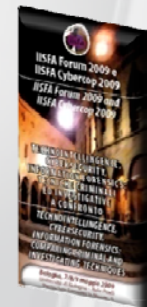
1. Intervento sulla scena del crimine:

Qual è l'obiettivo (limitatamente al MF)?
REPERTARE IN MANIERA CORRETTA
DISPOSITIVI E/O DATI
(più correttamente possibile!)

L'obiettivo NON è risolvere il caso...

La **fretta** e le **aspettative** generano più errori
dell'incompetenza tecnica!





1. Intervento sulla scena del crimine:

1.2 Repertamento dei dati (L.48/2008)

Il repertamento di dati digitali deve sempre ricondursi ad una copia di sequenze di bit.
In tutti gli altri casi (riprese video, fotografiche, ecc) si acquisiscono **informazioni** e non **dati** che riconducano ad un reperto virtuale.

“...adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l’alterazione” (L.48/2008)



1.1 Repertamento dell'oggetto fisico

In assenza di competenze tecniche e di urgenze varie lo si vorrebbe disattivato.

Se vi sono necessità (investigative)
nell'immediato lo si vorrebbe attivo.

A meno di specifiche direttive della AG la **disconnessione dalla rete cellulare è necessaria.**

1. Intervento sulla scena del crimine:

1.2 Repertamento dei dati (L.48/2008)

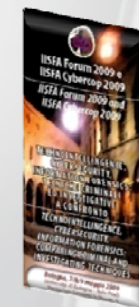
L'ideale è una bit-stream copy ossia la copia del contenuto dati del dispositivo ridotto a flusso di bit.

Ma:

- bit-stream copy di quale memoria?
- qual'è il set di dati originali da preservare e copiare?
- quale metodo di copia (interfaccia) impiegare?

In altre parole:

Com'è definita la ripetibilità per questa attività?

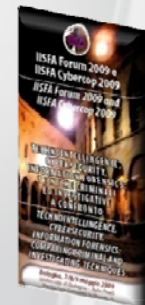


1. Intervento sulla scena del crimine:

1.1 Repertamento dell'oggetto fisico

Mantenere il dispositivo **attivo** sulla scena del crimine, senza accorgimenti specifici, corrisponde quasi con certezza a modificarne lo stato ed il contenuto (spostamenti e rice/trasmissioni).

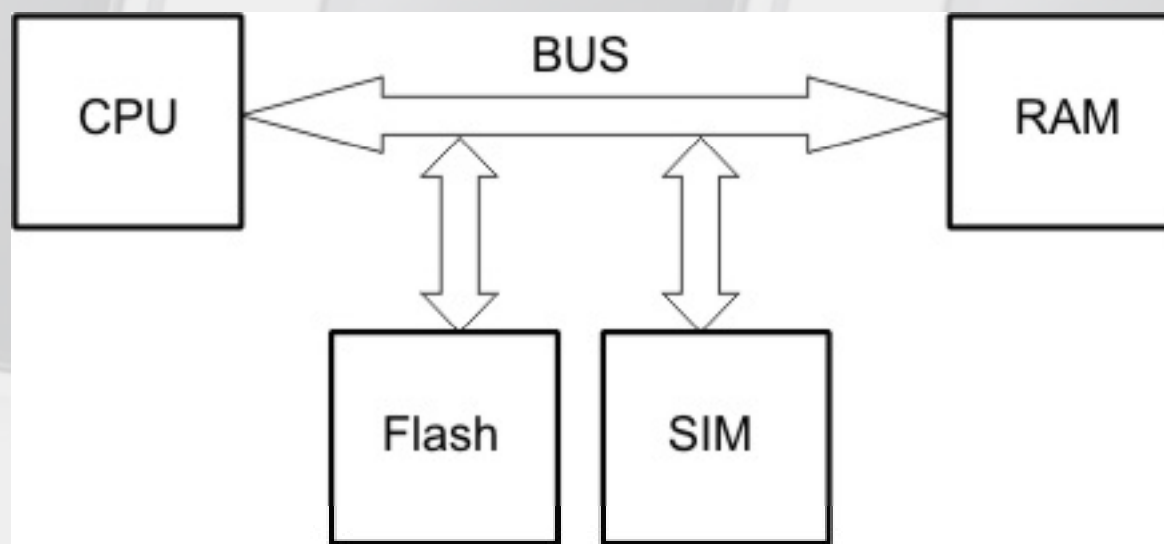
Anche **spegnere** il dispositivo ha i suoi seri problemi: PIN, password, scaricamento batteria, riattivazione successiva, metodologia di spegnimento...



1. Intervento sulla scena del crimine:

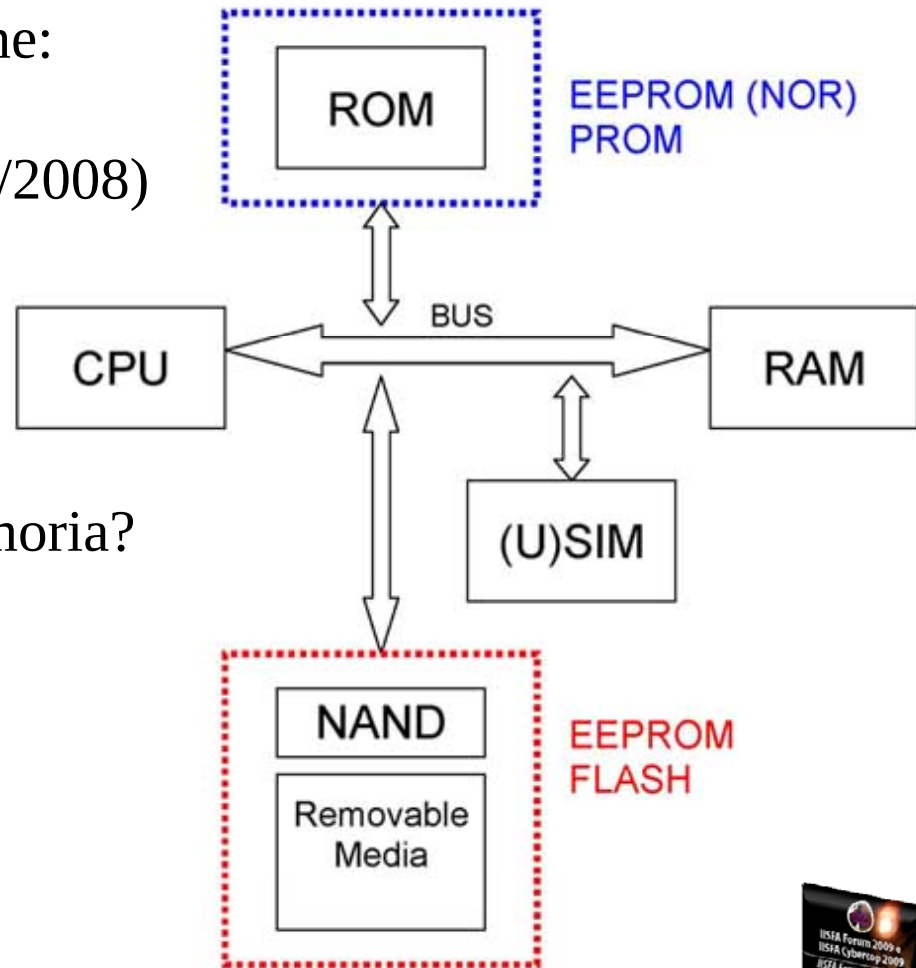
1.2 Repertamento dei dati (L.48/2008)

- bit-stream copy di quale memoria?



1.2 Repertamento dei dati (L.48/2008)

- bit-stream copy di quale memoria?

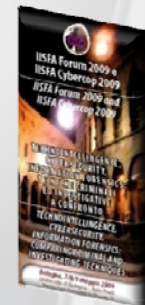


1. Intervento sulla scena del crimine:

1.1 Repertamento dell'oggetto fisico

Mantenere il dispositivo **attivo** in ambiente controllato:

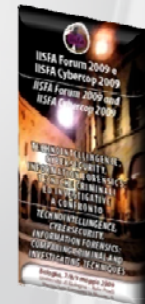
- Jamming device
- Tende di Faraday
- Contenitori Schermati



1. Intervento sulla scena del crimine:

1.1 Repertamento dell'oggetto fisico

Problema del **trasporto**: mantenere il dispositivo attivo fino in laboratorio (limitare al massimo le analisi sulla scena del crimine!)



1. Intervento sulla scena del crimine:

1.2 Repertamento dei dati (L.48/2008)

- qual'è il set di dati originali da preservare e copiare?

I dati presenti sulla RAM o sulla porzione di FLASH impiegata per eseguire i software?

I file del sistema operativo e/o i suoi settings/log, ecc.?

I dati multimediali sulla memoria di massa o removibile?



1. Intervento sulla scena del crimine:

1.2 Repertamento dei dati (L.48/2008)

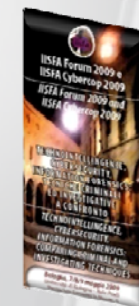
- qual'è il set di dati originali da preservare e copiare?

Si potrebbe anche vociferare qualcosa che negli ultimi anni ha “colpito” computer e network forensics:

... non andrebbero copiati solo i dati strettamente inerenti il procedimento?

Ed in tal caso l'”originale” è costituito solo da essi?

ATTENZIONE: se è “si” la copia va considerata **irripetibile!**



1. Intervento sulla scena del crimine:

1.2 Repertamento dei dati (L.48/2008)

- quale metodo di copia (interfaccia) impiegare?

Si può iniziare a dividere il problema:

1.2.1 La SIM

1.2.2 Le memorie di massa e/o removibili

1.2.3 La memoria interna del terminale radiomobile



1. Intervento sulla scena del crimine:

1.2 Repertamento dei dati (L.48/2008)

- La SIM (ETSI TS 100 977 v8.12.0 - ISO 7816 - ...)

Le SIM/USIM sono unità altamente standardizzate, con un contenuto ed interfacciamento ben noto.

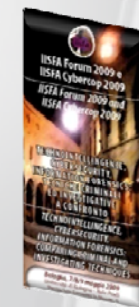
Esistono diversi tool software commerciali (e non) che, attraverso smartcard reader sono in grado sia di copiare i dati di basso livello della SIM che di interpretarli fornendo report utili all'investigatore tecnico.



1. Intervento sulla scena del crimine:

1.2 Repertamento dei dati (L.48/2008)

- Le memorie di massa e/o removibili
COMPUTER FORENSICS!



1. Intervento sulla scena del crimine:

1.2 Repertamento dei dati (L.48/2008)

- La memoria interna del terminale radiomobile

In linea di principio, se si considera “tutta” la memoria interna, quindi anche le aree tmp è “live forensics” quindi non ripetibile.

Ma approcci diversi possono permettere di articolare un ragionamento più complesso...



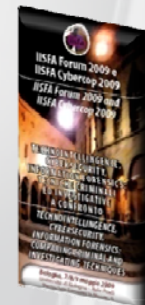
1. Intervento sulla scena del crimine:

1.2 Repertamento dei dati (L.48/2008)

- La memoria interna del terminale radiomobile

Approcci diversi in ragione della problematica mancanza di standard nella realizzazione dei terminali radiomobili:

- Repertamento invasivo;
- Repertamento non invasivo;
- Repertamento semi-invasivo.



1. Intervento sulla scena del crimine:

1.2 Repertamento dei dati (L.48/2008)

- La memoria interna del terminale radiomobile
- Repertamento invasivo:

Lettura diretta dei dati sui chip di memoria contenuti nel dispositivo radiomobile attraverso rimozione fisica dalla scheda o inserimento di sonde sulla piedinatura.

Si tratta di una lettura che avviene mediante EPROM reader, estesa al contenuto dell'hardware che bypassa qualsiasi software (firmware) intermedio.



1. Intervento sulla scena del crimine:

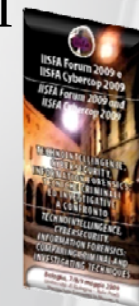
1.2 Repertamento dei dati (L.48/2008)

- La memoria interna del terminale radiomobile
- Repertamento invasivo:

Attività da esplicarsi SOLO in laboratorio.

Attività non ripetibile, utile per sistemi danneggiati.

Hash: il flusso di bit generato dai lettori di EPROM non segue sempre lo stesso ordine per cui talvolta l'hash di set identici di dati risulta differente...



1. Intervento sulla scena del crimine:

1.2 Repertamento dei dati (L.48/2008)

- La memoria interna del terminale radiomobile
- Repertamento non invasivo:

È possibile acquisire la memoria del terminale radiomobile (privato di SIM) mediante un'apposita workstation se il primo dispone di un'interfaccia di basso livello per il **test** e/o per la **riprogrammazione** (non si escludono tra loro).

Interfacce come *JTAG* o quelle impiegate nel *flashing* permettono di riattivare il terminale in *testing mode* e così richiedere il servizio installato da firmware di dump dei dati.



1. Intervento sulla scena del crimine:

1.2 Repertamento dei dati (L.48/2008)

- La memoria interna del terminale radiomobile
- Repertamento non invasivo:

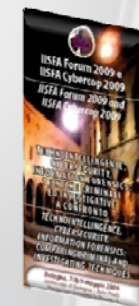
ATTENZIONE!

Non tutti i terminali hanno le citate interfacce.

Quelli che li hanno possono averle bloccate o disattivate...

Il terminale deve essere spento prima dell'attività...

Per la EEPROM (NAND & NOR) si può considerare ripetibile a patto di regularsi sulle peculiarità dello smartphone e del suo spegnimento.

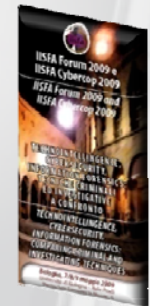


1. Intervento sulla scena del crimine:

1.2 Repertamento dei dati (L.48/2008)

- La memoria interna del terminale radiomobile
 - Repertamento semi-invasivo:

(1) Qualora lo scopo sia quello di analizzare con urgenza il terminale radiomobile e/o lo si abbia spento si può estrarre la SIM ed inserire una **Forensic SIM**, progettata per essere inerte alla rete cellulare e consentire comunque al terminale di operare nella navigazione dei dati senza avvertire il cambio di SIM.



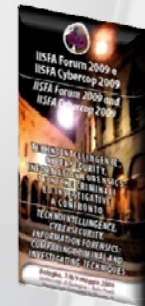
1. Intervento sulla scena del crimine:

1.2 Repertamento dei dati (L.48/2008)

- La memoria interna del terminale radiomobile
- Repertamento semi-invasivo:

(1) ... si può quindi interagire direttamente con il terminale anche senza contenitore schermato, oppure inserire al suo interno un software agent per l'individuazione e la copia dei dati.

Quest'ultimo è l'approccio del **mobile forensics** ormai definito **tradizionale**.



1. Intervento sulla scena del crimine:

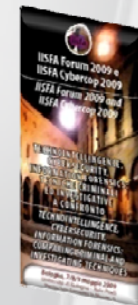
1.2 Repertamento dei dati (L.48/2008)

- La memoria interna del terminale radiomobile
- Repertamento semi-invasivo:

(2) Accesso manuale al dispositivo alimentato elettricamente senza rimozione della SIM, il tutto dall'interno di una camera schermata o di contenitore schermato campale. Attività, talvolta imprescindibile, usata per urgenza, che può risultare ripetibile a patto di mantenere sempre attivo ed isolato il dispositivo.



Slide 29 – Repertamento dei dati – semi-invasivo area schermata





Picture by
<http://www.volontari.org>

Slide 30 – CHE LEGGERISSIMO CAOS!!!



2. Attività di laboratorio:

Qual è l'obiettivo (limitatamente al MF)?
ANALIZZARE IL REPERTO FISICO O
VIRTUALE E GENERARE UN REFERTO
TECNICO



2. Attività di laboratorio:

Si può realizzare su 3 fronti:

2.1 Il repertamento dati

Se si parte dal reperto fisico ed è possibile

2.2 L'analisi del reperto virtuale

Se è già disponibile la copia

2.3 L'analisi diretta da terminale radiomobile

Per urgenza o situazioni non trattabili



2. Attività di laboratorio:

2.1 Il repertamento dati

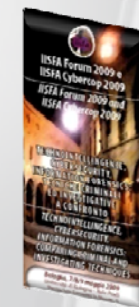
Si ripete quanto già visto con la differenza che l'ambiente controllato e la strumentazione non campale del laboratorio assicurano uno standard di lavoro migliore.



2. Attività di laboratorio:

2.2 L'analisi del reperto virtuale

È bene sempre ricondursi a questa situazione:
un set di bit (reperto virtuale) che proviene
dal repertamento dati (campale o di lab) il
quale deve essere esaminato ai fini legali e/o
di indagine.



IISFA Forum 2009 – Mobile Forensics

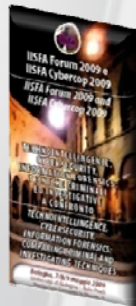
2. Attività di laboratorio:

2.2 L'analisi del reperto virtuale

L'analisi dipende dal tipo di reperto virtuale che si considera e quindi dal tipo di repertamento effettuato:

- Analisi nel caso di rep. invasivo;
- Analisi nel caso di rep. non invasivo;
- Analisi nel caso di rep. semi-invasivo.

Slide 35 – L'Attività di laboratorio – analisi del reperto virtuale #2



IISFA Forum 2009 – Mobile Forensics

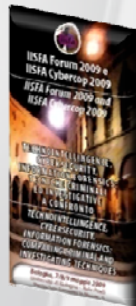
2. Attività di laboratorio:

2.2 L'analisi del reperto virtuale

L'analisi dipende dal tipo di reperto virtuale che si considera e quindi dal tipo di repertamento effettuato:

- Analisi nel caso di rep. invasivo;
- Analisi nel caso di rep. non invasivo;
- Analisi nel caso di rep. semi-invasivo.

Slide 35 – L'Attività di laboratorio – analisi del reperto virtuale #2



IISFA Forum 2009 – Mobile Forensics

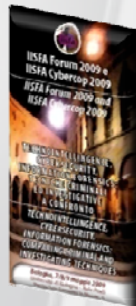
2. Attività di laboratorio:

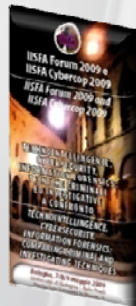
2.2 L'analisi del reperto virtuale

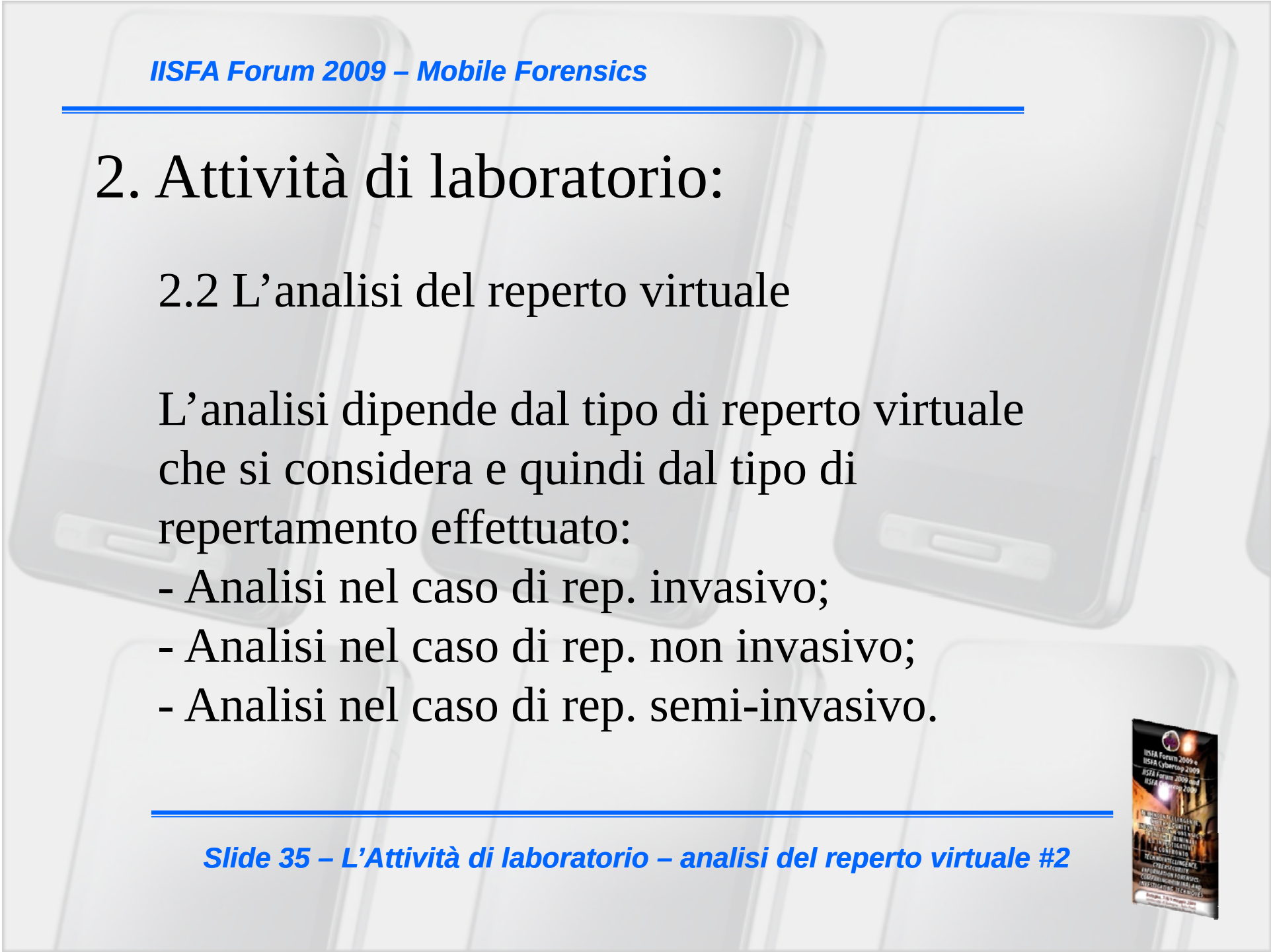
L'analisi dipende dal tipo di reperto virtuale che si considera e quindi dal tipo di repertamento effettuato:

- Analisi nel caso di rep. invasivo;
- Analisi nel caso di rep. non invasivo;
- Analisi nel caso di rep. semi-invasivo.

Slide 35 – L'Attività di laboratorio – analisi del reperto virtuale #2



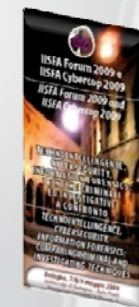
- ## **IISFA Forum 2009 – Mobile Forensics**
-
- # 2. Attività di laboratorio:
- ## 2.2 L'analisi del reperto virtuale
- L'analisi dipende dal tipo di reperto virtuale che si considera e quindi dal tipo di repertamento effettuato:
- Analisi nel caso di rep. invasivo;
 - Analisi nel caso di rep. non invasivo;
 - Analisi nel caso di rep. semi-invasivo.
-
- Slide 35 – L'Attività di laboratorio – analisi del reperto virtuale #2**
- 



2. Attività di laboratorio:

2.2 L'analisi del reperto virtuale

L'analisi nel caso di repertamento **invasivo** deve basarsi sia su di un corretto riordinamento dei dati letti nei vari banchi di memoria (hardware) che su una corretta riorganizzazione ed interpretazione a livello logico (sistema operativo / file system).

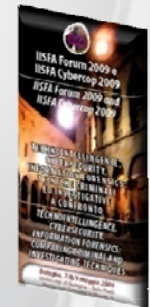


2. Attività di laboratorio:

2.2 L'analisi del reperto virtuale

L'analisi nel caso di repertamento **non invasivo** deve basarsi su una corretta riorganizzazione ed interpretazione a livello logico (sistema operativo / file system).
Ciò in quanto a livello hardware l'interfaccia è standard (es. JTAG).





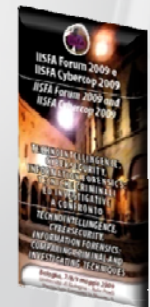
2. Attività di laboratorio:

2.3 L'analisi diretta da terminale radiomobile

Si tratta in realta del metodo (2) del repertamento semi invasivo.

Sarebbe più corretto parlare di acquisizione di informazioni (**ispezione**) che di repertamento dati o analisi.

Può avvenire per interazione diretta con la tastiera o tramite comandi AT da software mediante collegamento remoto ad una workstation.



FINE

Il settore del mobile forensics è chiaramente di frontiera ma i suoi problemi hanno in realtà radici non dissimili da quelli che riguardano computer e network forensics, ossia la necessità di gestire correttamente e con tutte le garanzie possibili, il repertamento ed analisi di sistemi digitali “live”.

<http://www.marcomattiucci.it>

