University of Roma
TOR VERGATA
Italy

MIAT
(Mobile Internal Acquisition Tool)

Forensic acquisition IN smartphones

Gianluigi Me

Summary

- Introduction
- Preliminaries
- A new methodology
- MIAT : Mobile Investigation Acquisition Tool
- MIAT behaviour
- Forensic properties
- MIAT at work
- Future importance of mobile forensics
- Conclusions

Scenario

- **MIAT is a Mobile Forensic Tool designed to acquire Symbian (and Windows Mobile) smartphones internal memory data without cables, directly from the internal memory slot;**
- **Overwhelming effort for forensic operators, due to "tons" of proprietary plugs to be used in crime scene;**
- **NIST states that "*To acquire data from a phone, a connection must be established to the device from the forensic workstation…*";**
- **But most devices have proprietary protocols to gain internal memory access (like DBUS for Nokia), while common protocols (like OBEX) are insufficient;**
- **While mobile devices popularity increases the capability to perform forensic analysis is still limited. Furthermore, most of the forensic tools (all) are proprietary.**
- **Currently the low-level forensic imaging of internal memory is one of the most important challenges due to lack of standards to get memory access;**
- **Open source acquisition**

Preliminaries: the requirement

- **GSM Mobile Device and Associated Media Tool Specification,** Lines 108-113, NIST (1 feb 08)
- *The central requirement for a sound forensic examination of digital evidence is that the original evidence must not be modified (i.e., the examination or capture of digital data from a mobile device and associated media must be performed without altering the device or media content). In the event that data acquisition is not possible using current technology to access information without configuration changes to the device (e.g., loading a driver), the changes must be documented and minimal (i.e., file size) to accomplish the required task.*

*OS Preliminaries: Daubert test

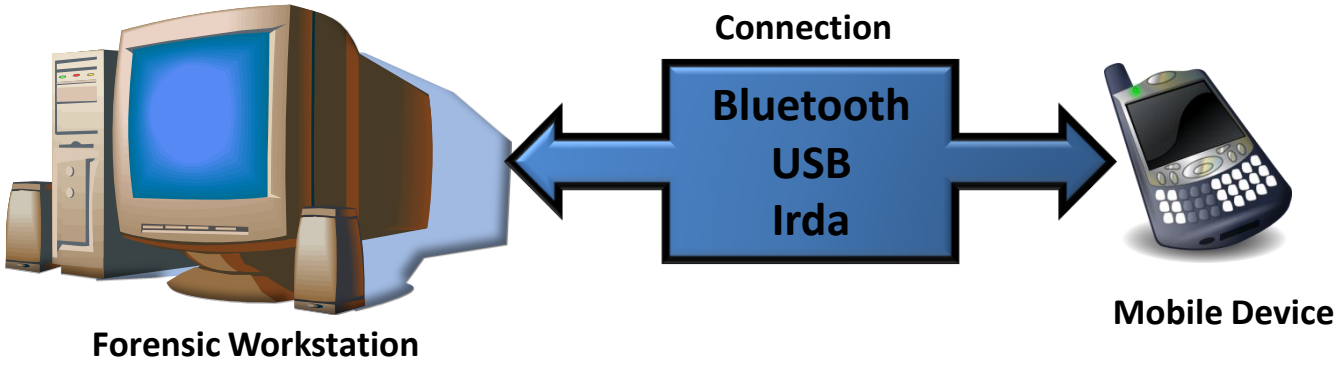
- **Testing:** Can and has the procedure been tested?
- **Error Rate:** Is there a known error rate of the procedure?
- **Publication:** Has the procedure been published and subject to peer review?
- **Acceptance:** Is the procedure generally accepted in the relevant scientific community?

*B.Carrier: Open Source Digital Forensics Tools: The Legal Argument

State of the Art

- Currently both Free Open Source (e.g. TULP2G) and COTS (e.g. Paraben Device Seizure) tools exist;

- Currently used tools establish a connection with mobile device;



- Forensic examination of flash memory can be found in (JTAG) (Breeuwsma, M., de Jongh, M. Klaver, C. van der Knijff, R. and Roeloffs, M., (2007) "Forensic Data Recovery from Flash Memory", (http://www.ssddfj.org/papers/SSDDFJ_V1_1_Breeuwsma_et_al.pdf))
- Paraben Corporation released the CSI stick (currently, only for Motorola and Samsung).
- Our idea is to use the OS as the only intermediary, phisically accessed via the memory slot.

The New Idea

- The main issues of classic acquisition are:
  - Largely unviable in practice, due to a plethora of proprietary cables and (not) standard wireless connectivity, as IRdA and Bluetooth;
  - Low parallelism due to single license usage (Cost related);
  - Reduced coverage of internal memory file system due to remote connection;
  - Low compatibility due to different communication protocol;
  - Tecnical skills required for the forensic operators;

- A good mobile forensic acquisition methodology (our vision):
  - Must examines SIM card, removable memory card and internal memory;
  - Should improve parallelism (at a reasonable cost) in device memory acquisition;
  - Should not require the forensic operator (during the acquisition phase) to be a mobile hw/sw expert, without overwhelming him by multiple one-on-one tools for every single mobile device
  - Should use Open Source acquisition tools;

- MIAT represents a new (Open Source) acquisition forensic tool which acquires LOGICALLY the internal memory data without cables, improving the parallelism, via the internal memory slot (mini SD, MMC).

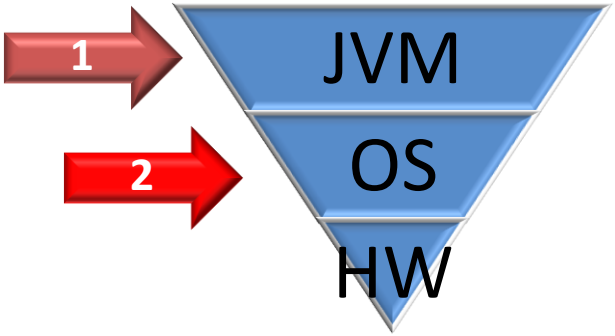
The MIAT Idea

- **In order to avoid the remote connection the tool should execute at mobile device side and imaging the internal memory into a removable one;**

- **How?**
  1. **Java application: fully portable but less powerful**

     OR

  2. **Application using OS APIs: less portable but closer to OS**

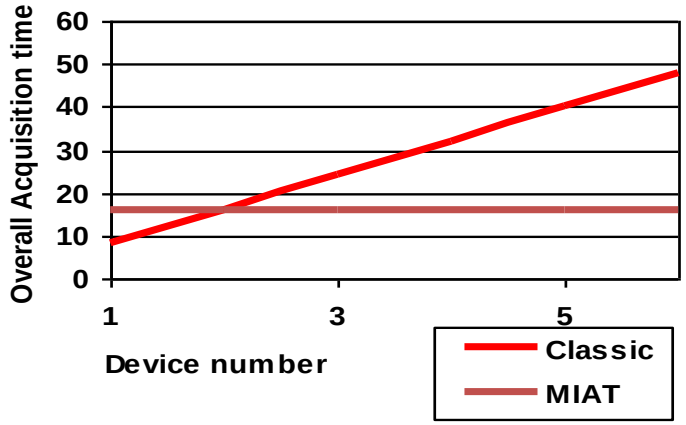


The MIAT benefits

- **Regarding to the classic methodology, the MIAT acquisition presents two major benefits:**

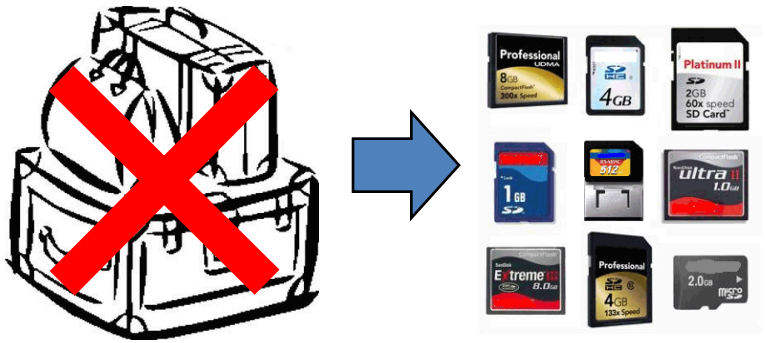
Parallelism

- **Althogh a single MIAT acquisition is, currently, slightly slower than the cable-based one;**
- **MIAT Multiple acquisition time is approximately constant while other is linear;**
- **This time benefit increases with the number of devices to be acquired.**



Lack of specific HW

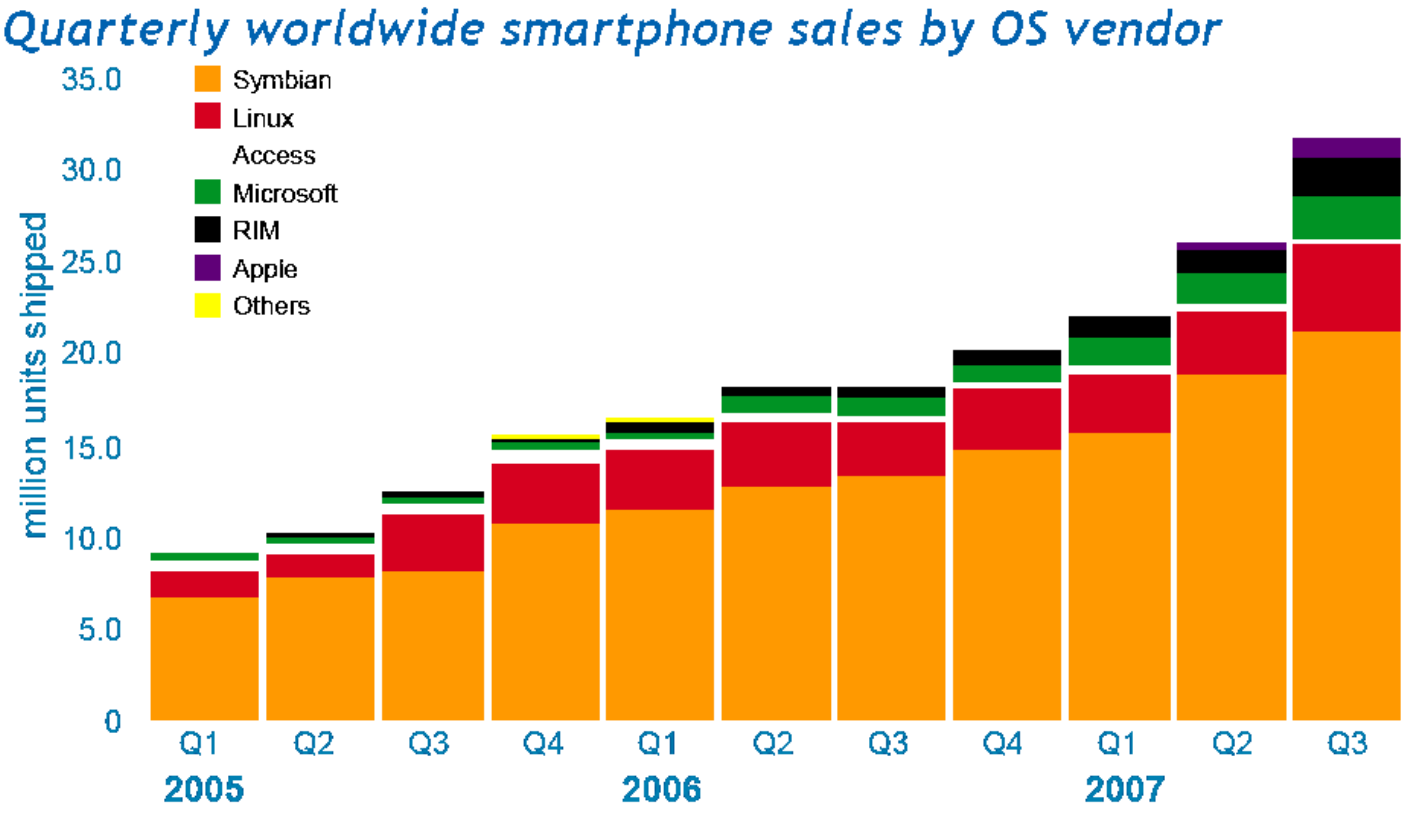
- **MIAT acquisition does not require any device model specific HW (eg. Usb cable);**
- **Every type of memory card (eg. SD, MMC, …) can be used with a number of different devices;**
- **The overall crime scene needed equipment is reduced to some memory cards (or compiling on-the-fly).**



What's MIAT application?

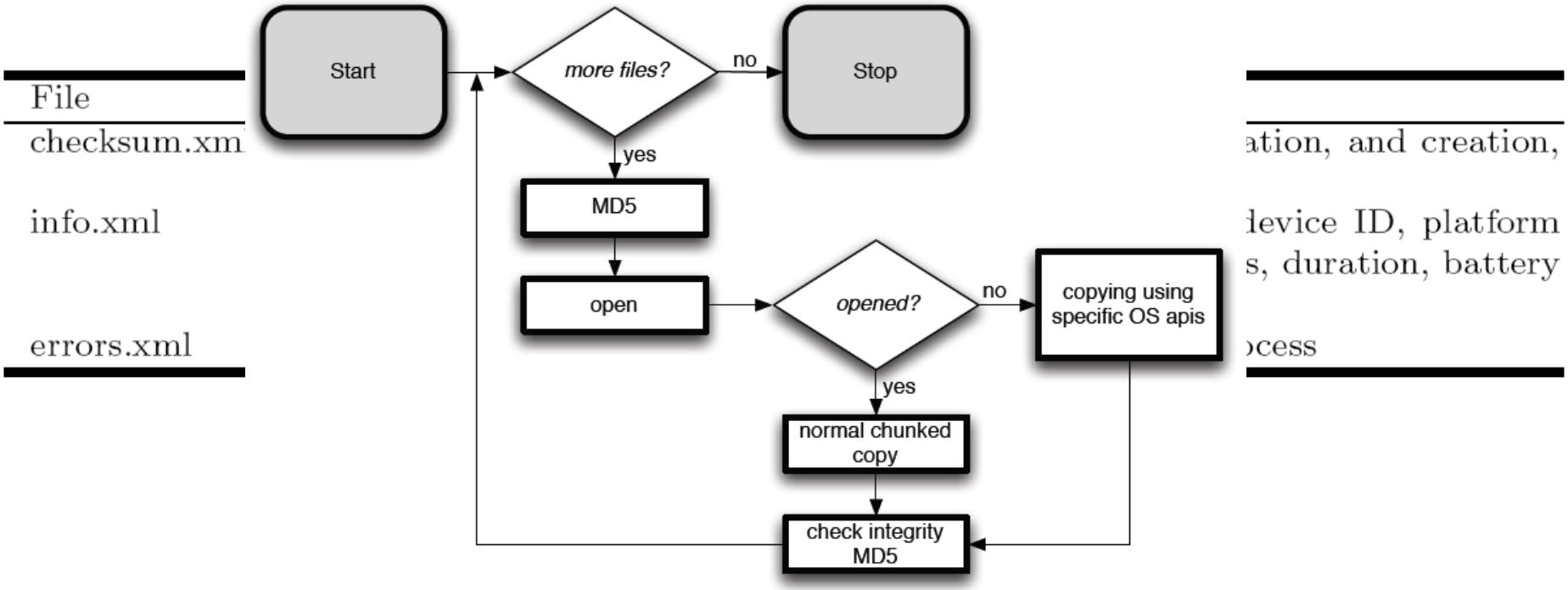
- **MIAT is an application which uses OS APIs to scan and copy the entire internal memory file system to removable memory card;**
- **Currently available both for Windows Mobile v5 and Symbian S60;**

- **Shipments 2007**
  - **Symbian 65%**
  - **Microsoft 12%**
  - **RIM 11%**



How MIAT works

- **The scanning algorithm is iterative, starting at File System root and ending when all entries are seized;**
- **Directory entries are replicated in backup memory;**
- **For each file entry the acquisition is made iteratively and an hashing code is computed.**



- **Copy step is chunk based to avoid big file failures**

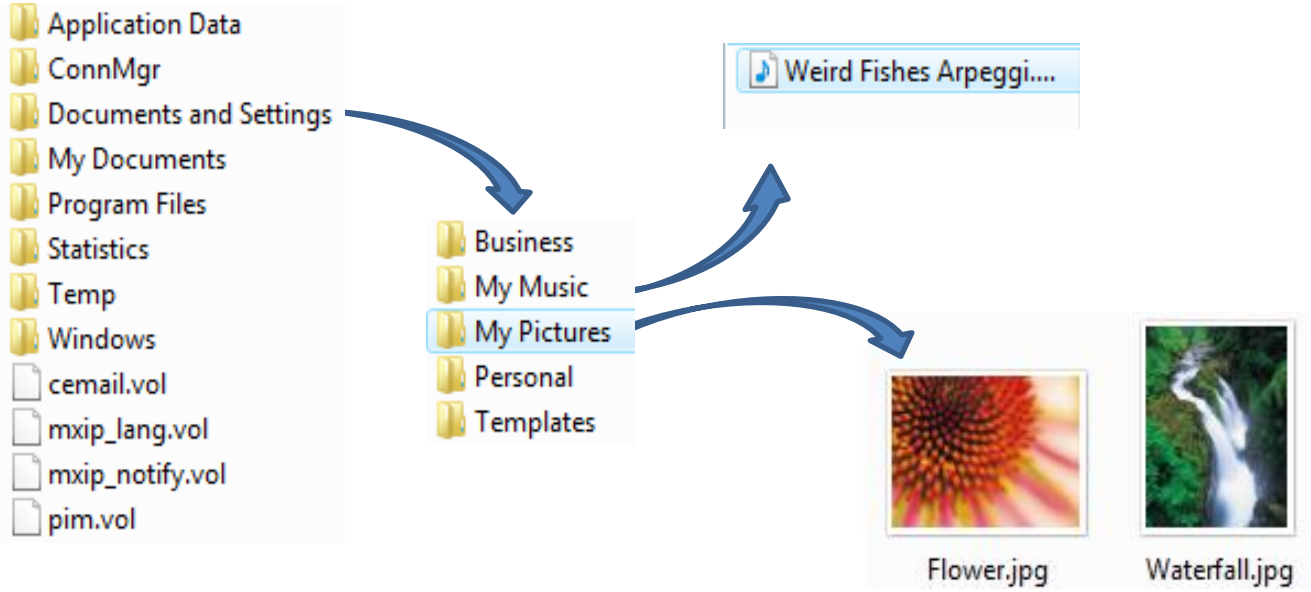
Summary of MIAT properties

- **Properties of interest are:**
  - **Coverage of internal memory FS;**
  - **Parallelism in acquisition;**
  - **Respect of integrity.**
  - **No further needs of one-on-one cables. MIAT-WM5 transformed hardware incompatibility in software compilation! (grams ->seconds)**

- **Coverage of internal memory file system :**
  - \+ **All entries in FS logical structure are seized;**
  - \+ **Deleted entries of Symbian Databases (SMS, contacts, agenda) are recovered;**
  - – **Deleted entries are not acquired (e.g. deleted files).**
- **Respect of Integrity:**
  - \+ **The chunked acquisition process does not corrupt any file;**
  - – **Some files are modified because can be accessed only via EDB CEDB API :these are the same modified by Paraben.**
- **Parallelism:**
  - \+ **MIAT supports multiple parallel acquisitions.**

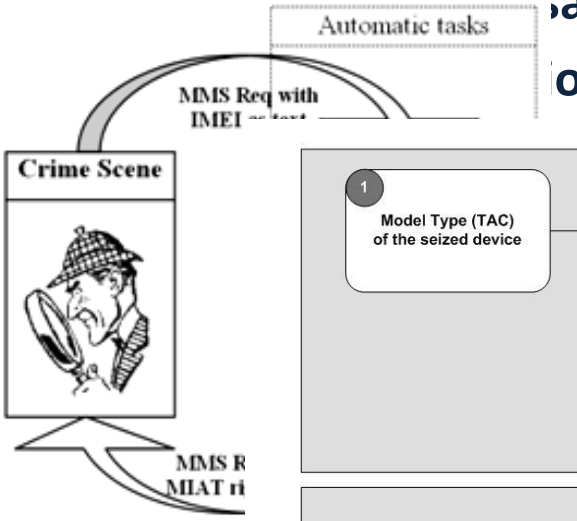
Example:the MIAT procedure

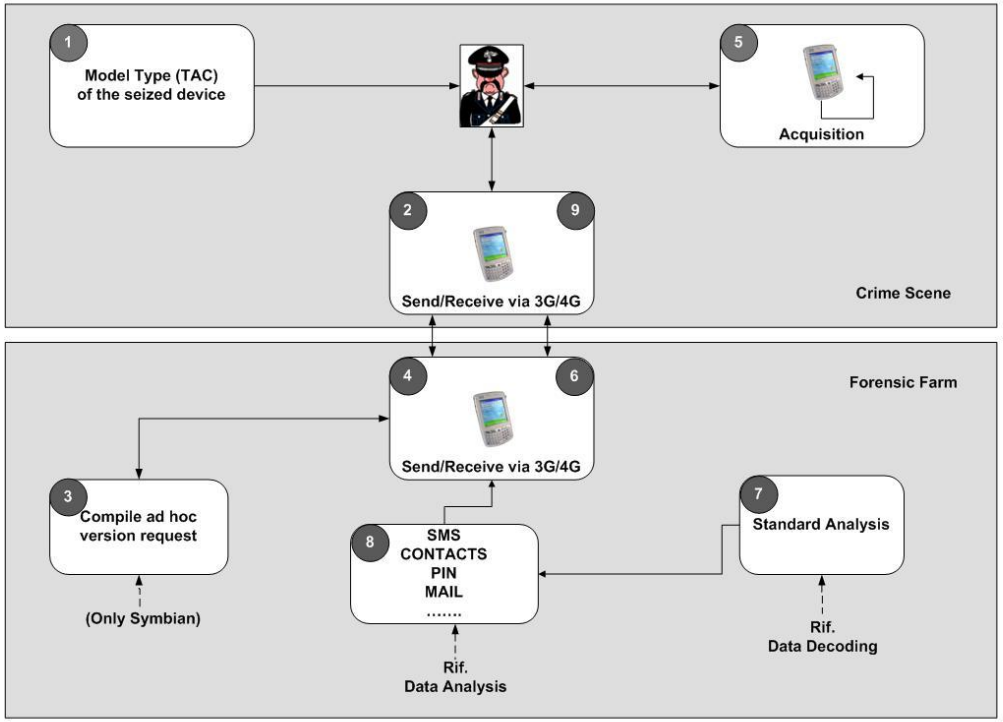
- **Suppose the need to perform forensic collection of data from Nokia N70 ;**
  1. **Remove the SD card and collect (dd) data;**
  2. **Prepare a new autorunnable SD and insert in the device;**
  3. **If necessary force MIAT to start from the SD.**
  4. **Choose the destination folder for seized data and click “Seize” button;**
  5. **Wait while MIAT performs acquisition (Successful seize! message box);**
  6. **Shut down MIAT and eject memory card.**

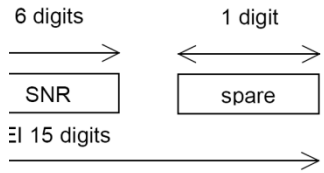


Operational Support

- Currently we are working to provide an operational support to MIAT;
- The capability to acquire data on Crime Scene is definitively valuable:
- Data stored in mobile devices changes due to internal (alarms, …) and environment (calls, messages, …) events;
- …on should be made as soon as possible!
  - TAC number (portion of IMEI) could be used to identify mobile device







… compiled copy of …ent back.

MIAT – Symbian

- The only interaction with the forensic operator is the startup of the acquisition;
- Depending both on device capability and internal memory occupation, the process completes in few minutes;
- Internal memory file system is logically copied to removable memory card;
- For each seized element:
  - the MD5 hash code is computed and stored;
  - The last modification time is stored;
- These information are stored according to an XML schema;

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.

Experimental assessment

- **In order to test correct functionalities of MIAT, experiments are required;**
- **MIAT – S60 and Paraben Device Seizure v1.3.2824.32812 were used on Nokia N70 and 6630.**

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

- **Different size values depend on additional information schema (e.g. distributed property files used by Paraben).**
- **MIAT time values depend on device capabilities.**

- **Paraben misses some entries (eg "_PAlbTN" dirs), this affects coverage.**
- **Both tools respect integrity.**

Property	MIAT	Paraben
Coverage	+	±
Integrity	+	+

- **More experiments for MIAT are needed (currently with Italian LEAs).**

Future work

- **Release in Open Source!**

- **Test MIAT on more Symbian smartphones (as possibile), WIP;**

- **Porting for Blackberry, Android;**

- **Automate the process of compiling the TAC recognition for ad-hoc version of MIAT:**

- **How to welcome Symbian 9 devices?**

- **Testing the usability for forensic operators, WIP;**

- **Rigorous proof of integrity on all the new smartphones;**

Conclusions

- New Forensic acquisition methodology for smartphones;
- MIAT is the tool for this methodology;
- MIAT evolves the classic remote acquisition to local :
  - Avoiding the use of HW specific accessories (eg USB cables);
  - Avoiding the use of a “forensic workstation”;
  - Improving the parallelism in acquisition;
  - Avoiding drawbacks due to communication protocol and remote access to internal memory;
  - Reduced costs (currently)
- Experiments show that MIAT performs as well as Paraben Device Seizure.
- Further experiments on models are needed.

University of Roma
TOR VERGATA
Italy

Q&A
To obtain a copy of MIAT write to me@disp.uniroma2.it