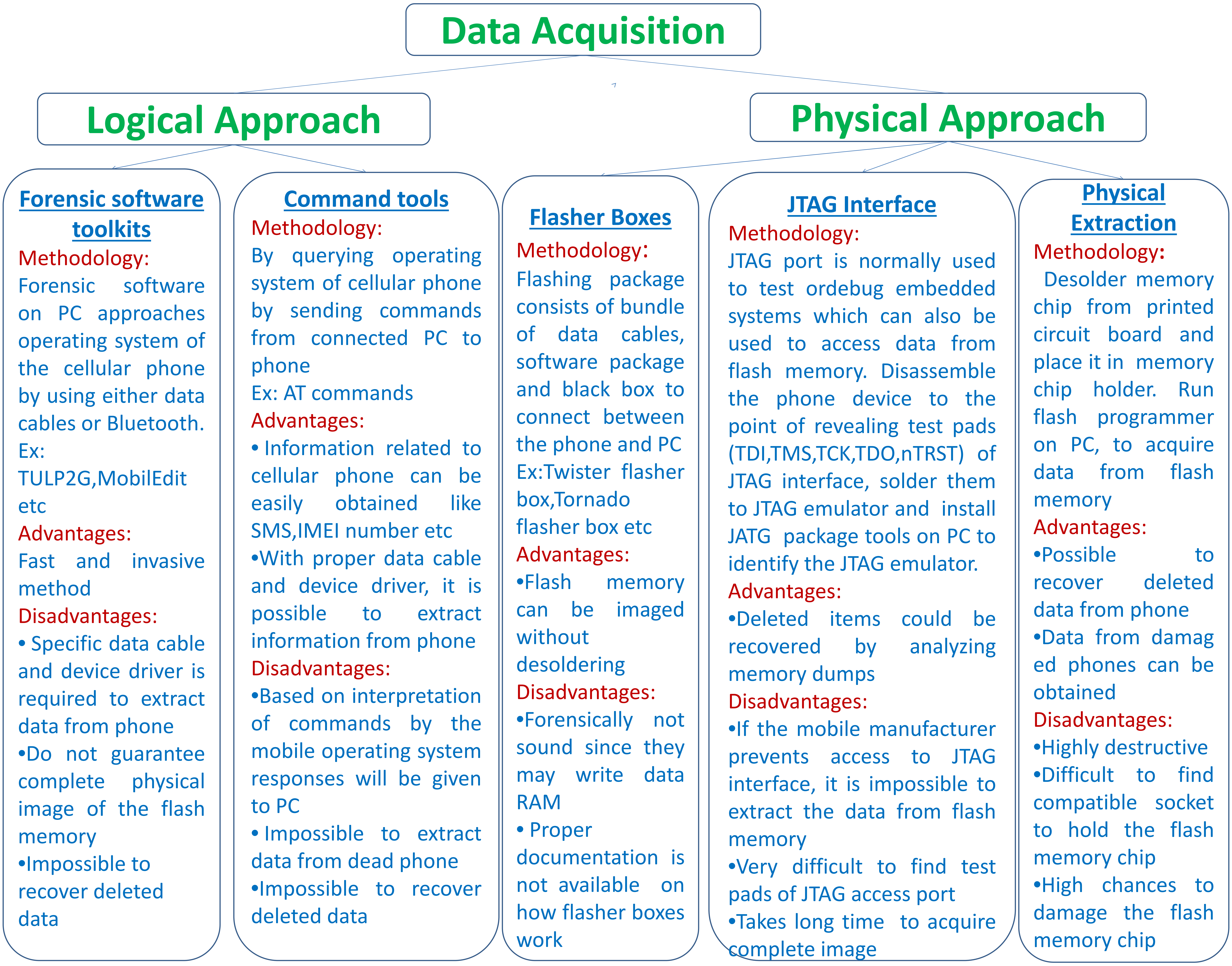
CERIAS

The Center for Education and Research in Information Assurance and Security

Approaches for Acquiring data from flash memory of Cellular Phones

Chandrika Silla, Dr. Sam Liles

Objective: Digital evidence that kept in the flash memory of the cellular phone can be extracted by using forensic tools. Forensic tools use two approaches to extract data. Logical approach is bit-by-bit copy of the flash memory using file system or protocol of the chip provider, physical approach is bit-by-bit copy of entire physical memory. Each method has it own advantages and disadvantages.



Data Acquisition

Logical Approach

Forensic software toolkits

Methodology:

Forensic software on PC approaches operating system of the cellular phone by using either data cables or Bluetooth.

Ex: TULP2G,MobilEdit etc

Advantages:

Fast and invasive method

Disadvantages:

- Specific data cable and device driver is required to extract data from phone
- Do not guarantee complete physical image of the flash memory
- Impossible to recover deleted data

Command tools

Methodology:

By querying operating system of cellular phone by sending commands from connected PC to phone

Ex: AT commands

Advantages:

- Information related to cellular phone can be easily obtained like SMS,IMEI number etc
- With proper data cable and device driver, it is possible to extract information from phone

Disadvantages:

- Based on interpretation of commands by the mobile operating system responses will be given to PC
- Impossible to extract data from dead phone
- Impossible to recover deleted data

Physical Approach

Flasher Boxes

Methodology:

Flashing package consists of bundle of data cables, software package and black box to connect between the phone and PC

Ex:Twister flasher box,Tornado flasher box etc

Advantages:

- Flash memory can be imaged without desoldering

Disadvantages:

- Forensically not sound since they may write data RAM
- Proper documentation is not available on how flasher boxes work

JTAG Interface

Methodology:

JTAG port is normally used to test ordebug embedded systems which can also be used to access data from flash memory. Disassemble the phone device to the point of revealing test pads (TDI,TMS,TCK,TDO,nTRST) of JTAG interface, solder them to JTAG emulator and install JATG package tools on PC to identify the JTAG emulator.

Advantages:

- Deleted items could be recovered by analyzing memory dumps

Disadvantages:

- If the mobile manufacturer prevents access to JTAG interface, it is impossible to extract the data from flash memory
- Very difficult to find test pads of JTAG access port
- Takes long time to acquire complete image

Physical Extraction

Methodology:

Desolder memory chip from printed circuit board and place it in memory chip holder. Run flash programmer on PC, to acquire data from flash memory

Advantages:

- Possible to recover deleted data from phone
- Data from damag ed phones can be obtained

Disadvantages:

- Highly destructive
- Difficult to find compatible socket to hold the flash memory chip
- High chances to damage the flash memory chip

Conclusion: Since there is no method which suites to all platforms, it is always better to perform physical acquisition preceding to logical acquisition.

CERIAS

PURDUE UNIVERSITY