

International Journal of Engineering Sciences & Research Technology

(A Peer Reviewed Online Journal)
Impact Factor: 5.164



Chief Editor
Dr. J.B. Helonde

Executive Editor
Mr. Somil Mayur Shah

ABSTRACT

Mobile forensics is a sub-set of digital forensics which includes the investigation and acquisition of artifacts of mobile phones. With the advancement of technology threats to mobile phones made forensic science a challenging Endeavour. Number of mobile users is increasing worldwide and creates tremendous problems and challenges. As the technology is advancing the criminals are also getting advanced day by day. Investigation agencies come across various crimes committed through different modes, forgery of IMEI number(s) of mobile device being one of them. This paper presents a case study in which mobile phones of duplicate IMEI's, hardware tools capable of duplicating IMEI along with other evidences have been received and examined in the laboratory.

KEYWORDS: Duplicate IMEI, Smartphone forensics, digital forensics, security, Anti-forensic and smartphone security.

1. INTRODUCTION

Mobile forensics is a branch of digital forensics which includes collection and investigation of digital evidence from a mobile phone. It relies on evidence extraction from the internal memory of a mobile phone when there is capability to access the data. Mobile phone technologies witnessed rapid development in recent years like upgradation of operating system, security patches, configurations etc. Every digital device has unique identity like serial number, IMEI number etc. If we talk about mobile phones then every mobile device contained its unique identity number i.e. IMEI. An International Mobile Equipment Identity abbreviated as IMEI is an integral part of 3GPP, iDEN mobile phones and satellite phones [1]. IMEI is usually found printed inside the battery compartment of the phone and mobile phones with inbuilt battery it is printed on back side of mobile phones. It can also be displayed on-screen by dialing *#06# MMI Supplementary Service code or can be found in the settings menu on smartphone operating systems. The role of IMEI number is very important in the investigation of the crime. When a user is using SIM card or internet of XYZ company in his mobile phone then the details of the particular mobile phone like company of the mobile device, model number, device ID, UDID and IMEI number got save on the server of network service provider/Internet service provider company. We take a crime scenario that if a person did cyber-crime using his/her mobile phone and during police investigation he refuses to accept that mobile phone belongs to him in that condition the investigation agency can ask for the IMEI number of the mobile phone in which SIM card was installed from SIM card provider company/Internet service provider (ISP) and then tally both IMEI numbers from which it can validate the specific mobile phone used in the crime and belongs to the criminal. New tools are developing which can be easily used to manipulate and tampered information such as creating forged IMEI numbers which are embedded on mobile packages and stored internally for illicit activities. These types of tools are easily available in the market or online. It can be software or hardware or a combination of both. So using these tools criminals can easily change the IMEI numbers and can use the stolen mobile phones. In such conditions tracking of criminals become impossible because an Investigation agency shares the original IMEI numbers to the network or internet provider companies. Country of Origin of Mobile Phone in which the phone was manufactured or assembled can be identified from the 7th and 8th digit of the IMEI number which is listed in Table 1:

Table 1: The IMEI Codes and the country of origin of mobile phones.

7th/8th digit	Country of origin
01/10/70/91	Finland
02	UAE/India
03/04	France/Canada
03/30	Korea/ China
04/40	China/Hong Kong
05/50	Brazil/USA/Finland
06/60	China/Mexico
07/08/80/20	Germany
09	India
18	Singapore
41/44	Uk
67	Usa
71	Malaysia
80	Hungary

There are various tools available used for changing the IMEI's of Smartphone based on chipsets of various chipset manufacturer, few of them are portrayed in Table 2.

Table 2: Tools available for changing the IMEI's based on chipsets

S. No.	Chipset manufacturer	Tools Used In changing the IMEI's	Chipset used by Mobile phone Manufacturer
1.	MediaTek (MTK)	MTK Droid Root and Tools, MobileUncleApp, Chamelephon App	Xiaomi, Oppo, Realme, Mototrola, Samsung, Nokia
2.	QualCommSnapdragon	qualcomm write IMEI tool, NV-items_Reader_Writer_tool, Sigmakey	Samsung Galaxy, Sony Xperia, Asus Zenfone, Xiaomi Mi, Razer Phone,
3.	Broadcom	Broadcom Code reader, Sigmakey, Repair 3G tool, Brcm FlashTool_V2.0.7.0, MultiFun Tool Setup	Samsung, Lava, Karbonn, Micromax etc
4.	Apple A14 Bionic	Ziphone	Apple iphone, ipad
5.	Kirin 990 5G	Sigma Software	Huawei ,Honor

2. MATERIAL AND METHODS

Incident summary

One racket running in northern part of India had been cracked and filed the case under sections 420 IPC and 66 IT Act. The IO seized three mobile phones, two hard disks and three hardware devices and sent to laboratory. The query was to identify whether the IMEI has been changed or not and if yes the what is the real IMEI of the mentioned mobile phones and whether the provided evidence devices can be used to change the IMEI and finally whether the hard disks contain any softwares for changing IMEIs.

Exhibits received

The details of the exhibits received are given below:-

Three mobile phones

- i. Lava Model: X17
- ii. Samsung Duos Model: SM-G531H/DS
- iii. Mi Model: 20160320

Two hard disks

- i. Seagate of 500 GB
- ii. Seagate of 1000 GB

Three devices

- i. Z3X-Box.
- ii. Octoplus Box
- iii. Miracle box GSM Campus.com

3. RESULTS AND DISCUSSION

Mobile Phone Devices

The hardware/software UFED Touch 2, Physical Analyser Version 7.3, Mobile edit Xpress Pro Version 6.0 and mobile check Version 3.0 have been used to examine all three mobile phones. The IMEIs of the mobile phones have been found from the various methods. The details of the IMEIs found at the mobile devices itself, in settings of the mobile phones, by dialing *#06# and generated through mobile forensic tools used for the extracting data is as given below in Table 3:-

Table 3: The IMEI's of mobile phones through various modes

Mobile Device	IMEIs of mobile phones using different methods				Remarks
	At device	About Phone	*#06#	In report (using mobile forensic software)	
Lava	911523700415788 911523701360785	351963039188051 351963039188077	351963039188051 351963039188077	351963039188051 351963039188077	IMEI Changed
Samsung	354621071953603 354622071953601	351963039187020	351963039187020 351963039187012	351963039187020	IMEI Changed
Mi	Not printed	353183038352248 353183038352249	353183038352248 353183038352249	353183038352248 353183038352249	IMEI Changed

The IMEIs of Lava and Samsung mobile phones is found to be of Lava and Samsung respectively, printed on the devices itself but when searched in settings, while dialing *#06# and using mobile forensic softwares it is found to be of Nokia mobile (table 3). Whereas the IMEI of Mi is not found printed on the device however by other methods as tabulated in table 3 it is found to be of Nokia mobile.

On the pre-examination of the devices and literature survey, the devices are found capable to change IMEI.

Z3X Box: It is a tool to allow owner of Samsung or LG phone to customize their device (alter its original service provider), unlocking phone and the tool can also be used to change IMEI (Fig.1).

Octoplus Box: It is used to unlock & lock reset phone, to repair and change IMEI (Fig 2).

Miracle box: used to flashing O/S, auto pin finder, mobile unlocking software and to change IMEI (Fig 3).



Fig.1 Z3X Box



Fig. 2 Octoplus Box



Fig.3 Miracle Box

*Due to the integrity of case we are representing the image of hardware tools from the source of internet. Whereas both the hard disks have been analysed using computer forensic tools FTK Imager and Guidance Encase Version 8.05. A number of software's such as Infinity box, Miracle box, Ultimate multi tool-GSM (Data) etc found installed and uninstalled list of both the hard disks.

4. CONCLUSION

Tempering of IMEI number is a punishable offence under the Prevention of tampering of the Mobile Device Equipment Identification Number Rules, 2017 which states that it shall be unlawful, if a person, except the manufacturer – (i) intentionally removes, obliterates, change, or alter unique Mobile Device Equipment Identification Number; or (ii) intentionally use, produce, traffic in, have control or custody of, or possess hardware or software, knowing it has been configured as specified above. The IMEI number is a fingerprint of the device and can be identified from various methods. Everytime a case is received the forensic expert should check the IMEI using every available method as well as mobile forensic tools.

5. ACKNOWLEDGEMENT

The authors are thankful to Dr. S. K. Jain (Director cum Chief Forensic Scientist Directorate of Forensic Science Services), Sh. D. P. Gangwar (Head of the division, Physics) and Sh. Akhlesh Kumar (Assistant Director, Physics) for the valuable guidance during the course of writing this paper.

REFERENCES

- [1] "3GPP TS 22.016: International Mobile Equipment Identities (IMEI)" (ZIP/DOC; 36 KB). 2009-10-01.
- [2] <https://economictimes.indiatimes.com/tech/hardware/tampering-mobile-imei-number-to-attract-up-to-3-years-jail-fine/articleshow/60816729.cms?from=mdr>
- [3] <https://dot.gov.in/circulars/prevention-tampering-mobile-device-equipment-identification-number-rules-2017>.
- [4] "What is an IMEI number? - Where Can You Find It? Activation". TechPayout.com.
- [5] Bostock, Bill (12 June 2019). "The Saudi government is hunting down women who flee the country by tracking the IMEI number on their cellphones". Business Inside.
- [6] Krishan Kumar, Prabhpreet Kaur (5 May 2015) "Vulnerability Detection of International Mobile Equipment Identity Number of Smartphone and Automated Reporting of Changed IMEI Number".
- [7] <http://www.mobilecellphonerepairing.com/how-to-know-country-of-origin-of-mobile-phone-from-imei-number.html>