iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** III **Month of publication:** March 2025

DOI: https://doi.org/10.22214/ijraset.2025.67560

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue III Mar 2025- Available at www.ijraset.com

IMEI: An Essential Resource for Device Identification and Security

Tilak Raj[1], Rajat Choudhary[2], Akhlesh Kumar[3], Faray Jamal[4]
Central Forensic Science Laboratory, Bhopal

Abstract: ***The International Mobile Equipment Identity (IMEI) number serves as a unique identifier for mobile devices, playing a crucial role in authenticating devices and securing cellular networks. Linked to the physical device rather than the subscriber, the IMEI provides an essential method for mobile network operators to track, identify, and authenticate devices. The Equipment Identity Register (EIR) stores IMEI data, enabling the blocking of stolen or unauthorized devices. However, recent advancements in digital technology have allowed criminals to alter or spoof IMEI numbers, creating challenges for law enforcement and network operators. This paper explores the impact of IMEI tampering on device security, presenting a case study where investigators successfully restored the original IMEI to uncover the true identity of a mobile device. The research highlights the significance of IMEI in criminal investigations and outlines effective methods used to combat IMEI manipulation, providing valuable insights for investigative agencies working to combat mobile device-related crimes. The findings emphasize the continued importance of IMEI as an investigative tool and stress the need for evolving technologies to secure device identification in an increasingly digital world.***

Keywords: IMEI, mobile devices, tampering, security

I. INTRODUCTION

The International Mobile Equipment Identity (IMEI) is a unique 15-digit number assigned to every mobile device, helping in identification, security, and tracking. The number consists of four groups that look similar to this: AA-BBBBBB-CCCCCC-D. The Type Allocation Code (TAC) is the initial eight-digit portion of the 15-digit IMEI code used to uniquely identify wireless devices. The first two digits represent the country code. The second group of numbers identifies the manufacturer. The third set is the serial number and the last single digit is an additional number (usually 0). For example 99-000033-792410-8: 99 is country code, 000033 is manufacturer, 792410 is the serial number, 8 is the checksum value.

It important in preventing phone theft and fraud, as mobile networks uses IMEI numbers to verify devices and block stolen ones. Unlike the International Mobile Subscriber Identity (IMSI), which is linked to a SIM card and can be transferred, the IMEI is permanently tied to a device.However, criminals often alter IMEI numbers to hide stolen phones, commit fraud, or bypass security measures. This has become a major challenge for law enforcement and mobile network operators. IMEI manipulation can be done through hardware changes (replacing the IMEI chip) or software tools that rewrite the number. These illegal activities make it harder to track lost or stolen devices.To tackle this issue, solutions like GPS-IMEI integration, checksum verification, and centralized databases can help detect unauthorized changes. Strengthening IMEI security is essential to preventing cybercrime, protecting mobile users, and assisting forensic investigations. This paper explores the importance of IMEI, methods of manipulation, and possible solutions to enhance mobile security.

II. BRIEF OF CASE

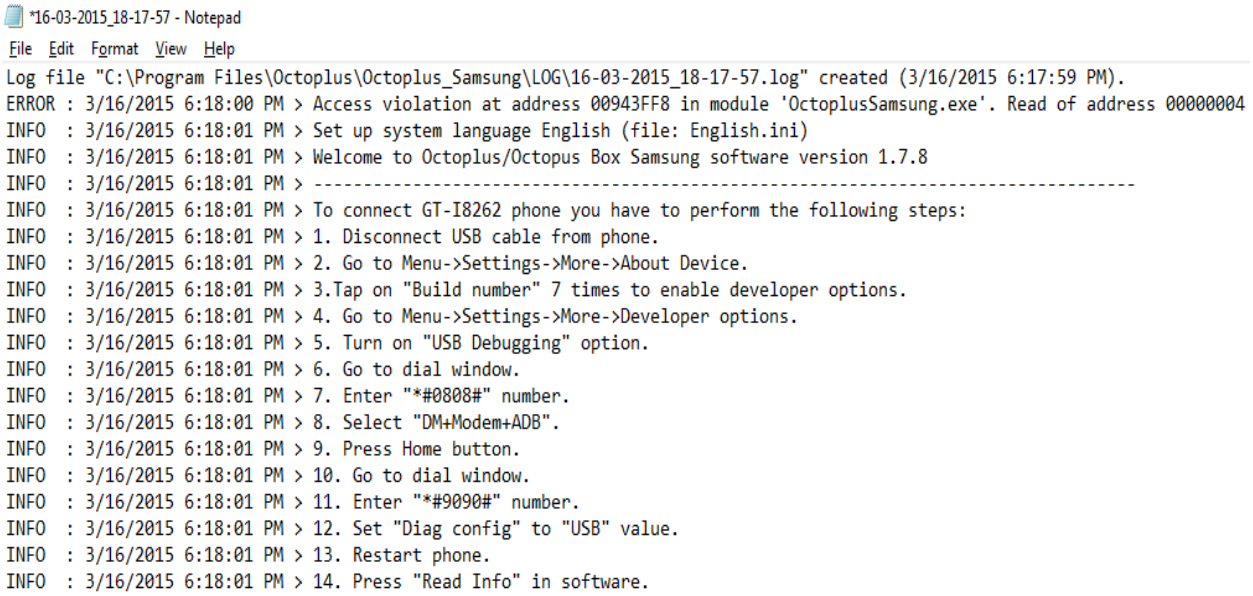
During the investigation of a stolen mobile phone, law enforcement agency received intelligence about an individual involved in the illegal sale and purchase of mobile devices. The suspect was also suspected of altering IMEI numbers to evade tracking.Acting on this information, authorities conducted a search and seized a computer system from the suspect's possession. The device was sent for forensic analysis to identify any evidence related to IMEI tampering, unauthorized software usage, and illicit transactions.

III. LABORATORY EXAMINATION

In the forensic investigation of IMEI modification activities, a structured and methodical approach was employed to ensure the integrity and reliability of the evidence gathered. Initially, a comprehensive list of commonly used IMEI modification software was

compiled through extensive online research, establishing a foundational understanding of the tools involved in the illegal modification process.

The seized hard disk drive (HDD) from the suspect's computer system was then carefully imaged using EnCase software, which ensured that the integrity of the data was preserved in a forensically sound manner. The imaged drive was subsequently indexed in EnCase to facilitate efficient data retrieval and analysis. During the examination of the extracted data, forensic experts discovered traces of several IMEI-changing software programs, including one that was actively installed on the system. A critical breakthrough occurred when a log file from the installed software was recovered, revealing essential details such as the original and altered IMEI numbers, device make and model, and a step-by-step process used for modification (Fig 1 to Fig 4). These findings provided significant evidence linking the suspect to the illegal modification of IMEI numbers, offering a robust basis for legal action and further investigation into the scope of the suspect's activities.


*16-03-2015_18-17-57 - Notepad

File Edit Format View Help

```
Log file "C:\Program Files\Octoplus\Octoplus_Samsung\LOG\16-03-2015_18-17-57.log" created (3/16/2015 6:17:59 PM).
ERROR : 3/16/2015 6:18:00 PM > Access violation at address 00943FF8 in module 'OctoplusSamsung.exe'. Read of address 00000004
INFO  : 3/16/2015 6:18:01 PM > Set up system language English (file: English.ini)
INFO  : 3/16/2015 6:18:01 PM > Welcome to Octoplus/Octopus Box Samsung software version 1.7.8
INFO  : 3/16/2015 6:18:01 PM > --------------------------------------------------------------------------------
INFO  : 3/16/2015 6:18:01 PM > To connect GT-I8262 phone you have to perform the following steps:
INFO  : 3/16/2015 6:18:01 PM > 1. Disconnect USB cable from phone.
INFO  : 3/16/2015 6:18:01 PM > 2. Go to Menu->Settings->More->About Device.
INFO  : 3/16/2015 6:18:01 PM > 3.Tap on "Build number" 7 times to enable developer options.
INFO  : 3/16/2015 6:18:01 PM > 4. Go to Menu->Settings->More->Developer options.
INFO  : 3/16/2015 6:18:01 PM > 5. Turn on "USB Debugging" option.
INFO  : 3/16/2015 6:18:01 PM > 6. Go to dial window.
INFO  : 3/16/2015 6:18:01 PM > 7. Enter "*#0808#" number.
INFO  : 3/16/2015 6:18:01 PM > 8. Select "DM+Modem+ADB".
INFO  : 3/16/2015 6:18:01 PM > 9. Press Home button.
INFO  : 3/16/2015 6:18:01 PM > 10. Go to dial window.
INFO  : 3/16/2015 6:18:01 PM > 11. Enter "*#9090#" number.
INFO  : 3/16/2015 6:18:01 PM > 12. Set "Diag config" to "USB" value.
INFO  : 3/16/2015 6:18:01 PM > 13. Restart phone.
INFO  : 3/16/2015 6:18:01 PM > 14. Press "Read Info" in software.
```

Figure 1: Pairing the Device with Software

16-03-2015_18-17-57 - Copy - Notepad

File Edit Format View Help

```
INFO  : 3/16/2015 6:18:39 PM > Platform: Samsung Anycall
INFO  : 3/16/2015 6:18:39 PM > Selected port: COM42
INFO  : 3/16/2015 6:18:39 PM > Selected model: GT-I8262
INFO  : 3/16/2015 6:18:42 PM > Connecting to phone on COM42
INFO  : 3/16/2015 6:18:48 PM > Mode: Emergency
INFO  : 3/16/2015 6:19:03 PM > Selected firmware file: GT-I8262_for_IM_Repair_2.oct
WARN  : 3/16/2015 6:25:17 PM > Please put the phone into Download Mode and connect USB cable.
WARN  : 3/16/2015 6:25:17 PM > To put GT-I8262 into Download Mode, You have to perform the following steps:
WARN  : 3/16/2015 6:25:17 PM > 1. Reconnect the battery.
WARN  : 3/16/2015 6:25:17 PM > 2. Press and hold "Volume-" + "Home" + "Power ON" keys.
WARN  : 3/16/2015 6:25:17 PM > 3. When phone turns on, press "Volume+" key.
INFO  : 3/16/2015 6:25:17 PM > Found phone on
INFO  : 3/16/2015 6:25:17 PM > Firmware write started.
INFO  : 3/16/2015 6:25:17 PM > Writing APPS section...
INFO  : 3/16/2015 6:25:31 PM > APPS section has been written successfully.
INFO  : 3/16/2015 6:25:31 PM > Writing RECOVERY section...
INFO  : 3/16/2015 6:25:47 PM > RECOVERY section has been written successfully.
INFO  : 3/16/2015 6:25:47 PM > Writing SYSTEM section...
INFO  : 3/16/2015 6:32:18 PM > SYSTEM section has been written successfully.
INFO  : 3/16/2015 6:32:18 PM > Writing FAT section...
INFO  : 3/16/2015 6:33:06 PM > FAT section has been written successfully.
INFO  : 3/16/2015 6:33:06 PM > Writing CACHE section...
INFO  : 3/16/2015 6:33:32 PM > CACHE section has been written successfully.
INFO  : 3/16/2015 6:33:32 PM > Writing HIDDEN section...
INFO  : 3/16/2015 6:33:52 PM > HIDDEN section has been written successfully.
INFO  : 3/16/2015 6:33:52 PM > Firmware writing successfully completed.
```

Figure 2: Changing Firmware Configuration

*16-03-2015_18-17-57 - Copy - Notepad

File Edit Format View Help

```
INFO  : 3/16/2015 6:37:53 PM > Platform: Samsung Anycall
INFO  : 3/16/2015 6:37:53 PM > Selected port: COM42
INFO  : 3/16/2015 6:37:53 PM > Selected model: GT-I8262
INFO  : 3/16/2015 6:37:56 PM > Connecting to phone on COM42
INFO  : 3/16/2015 6:38:38 PM > Mode: Emergency
INFO  : 3/16/2015 6:41:37 PM > Platform: Samsung Anycall
INFO  : 3/16/2015 6:41:37 PM > Selected port: COM42
INFO  : 3/16/2015 6:41:37 PM > Selected model: GT-I8262
INFO  : 3/16/2015 6:41:37 PM > Mode: Normal
INFO  : 3/16/2015 6:41:37 PM > Phone model: GT-I8262
INFO  : 3/16/2015 6:41:37 PM > Firmware compiled date: Apr 10 2013
INFO  : 3/16/2015 6:41:37 PM > Firmware compiled time: 03:00:00
INFO  : 3/16/2015 6:41:37 PM > Firmware released date: May 17 2013
INFO  : 3/16/2015 6:41:37 PM > Firmware released time: 18:17:33
INFO  : 3/16/2015 6:41:37 PM > Phone IMEI: [redacted]
INFO  : 3/16/2015 6:41:37 PM > SW version: 8X25-SSOSKOLYM-2035
INFO  : 3/16/2015 6:41:51 PM > Old IMEI: [redacted]
INFO  : 3/16/2015 6:41:51 PM > New IMEI: [redacted]
INFO  : 3/16/2015 6:46:57 PM > Old IMEI B: [redacted]
INFO  : 3/16/2015 6:46:57 PM > New IMEI B: [redacted]
INFO  : 3/16/2015 6:46:49 PM > Repairing IMEI ...
INFO  : 3/16/2015 6:46:50 PM > IMEI successfully repaired.
WARN  : 3/16/2015 6:46:50 PM > To finish the operation, please restart the phone via phone's menu (don't disconnect the battery!)
```

Figure 3: Changing IMEI Number

*16-03-2015_18-17-57 - Copy - Notepad

File Edit Format View Help

```
INFO  : 3/16/2015 6:41:51 PM > Searching for a phone. Please wait...
INFO  : 3/16/2015 6:41:51 PM > Firmware compiled date: Fri May 17 13:34:15 KST 2013
INFO  : 3/16/2015 6:41:51 PM > PDA version: I8262XXAME8
INFO  : 3/16/2015 6:41:52 PM > CSC version: I8262OJVAME2
INFO  : 3/16/2015 6:41:52 PM > SW version: I8262JVAME1
INFO  : 3/16/2015 6:41:54 PM > Phone SN: [redacted]
INFO  : 3/16/2015 6:41:54 PM > Android version: 4.1.2 (JZO54K)
INFO  : 3/16/2015 6:41:54 PM > Cheking Root
INFO  : 3/16/2015 6:44:31 PM > Phone is Rooted
INFO  : 3/16/2015 6:44:31 PM > Repairing network...
INFO  : 3/16/2015 6:45:14 PM > Network is successfully repair.
INFO  : 3/16/2015 6:45:16 PM > Deactivating MSL...
INFO  : 3/16/2015 6:45:30 PM > MSL deactivate successfully
WARN  : 3/16/2015 6:45:30 PM > Phone will restart now. Please don't disconnect cable!
WARN  : 3/16/2015 6:48:04 PM > To finish the operation, please restart the phone via phone's menu (don't disconnect the battery!)
```

Figure 4: Checking Network, MSL and Root Configuration

IV. RESULT AND CONCLUSIONS

The forensic investigation effectively uncovered evidence of illegal IMEI modification by systematically analyzing a seized computer. Through hard disk imaging, indexing, and data examination, experts identified installed and uninstalled IMEI-changing software. A recovered log file provided crucial details, including original and altered IMEI numbers, device models, and modification steps, directly linking the suspect to the crime. This evidence strengthens legal proceedings against IMEI tampering. To prevent such cybercrimes, forensic tools should be regularly updated, laws strictly enforced, public awareness increased, and stronger collaboration established between law enforcement and telecom authorities.The forensic findings will assist in determining the suspect's involvement and serve as key evidence in legal proceedings. The case highlights the growing issue of mobile phone-related cybercrimes and the need for stringent enforcement measures.

REFERENCES

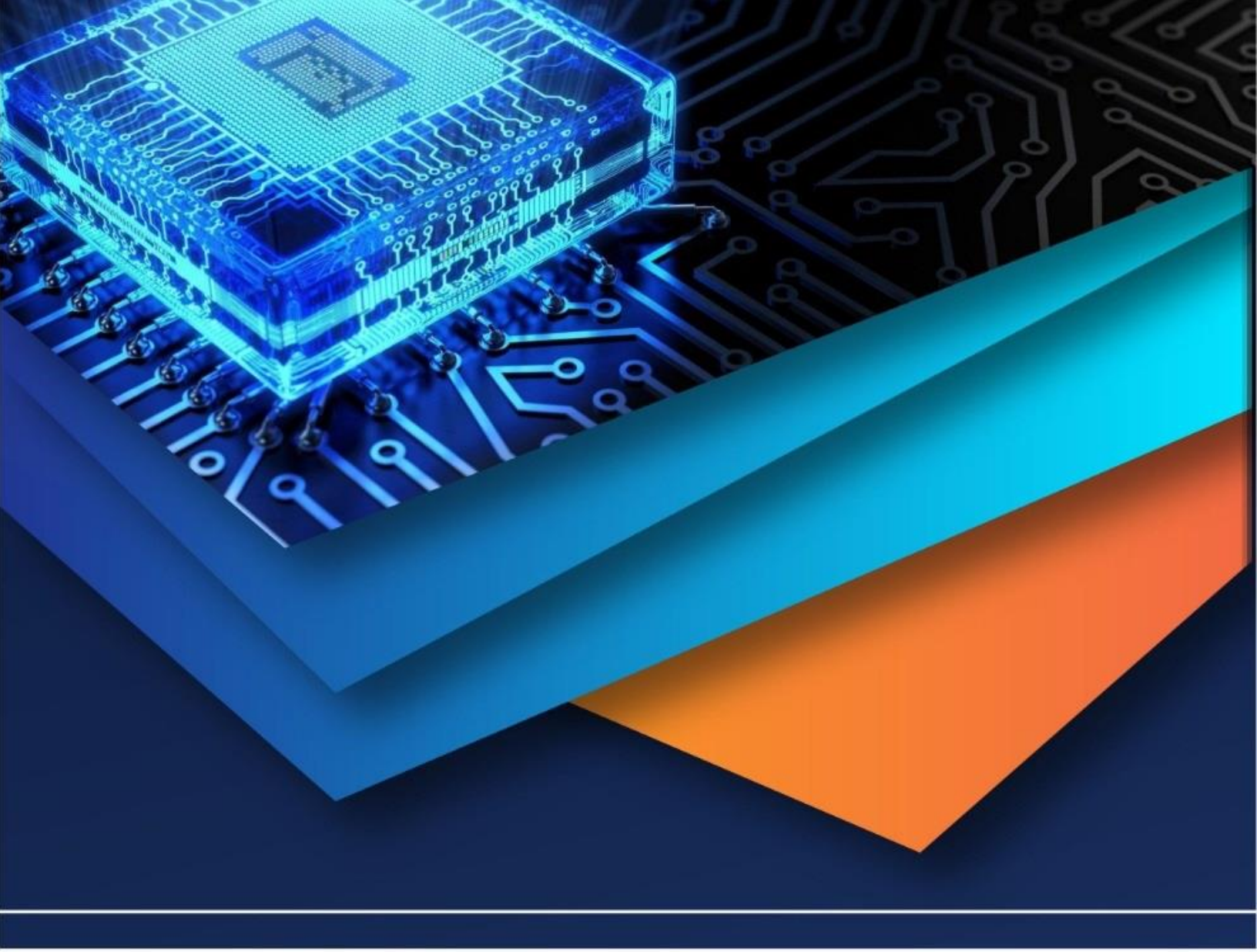
[1] International Journal of Advancements in Research & Technology, Volume 3, Issue 5, May-2014 186 ISSN 2278-7763 Copyright © 2014 SciResPub. IJOART DETECTING AND AUTOMATED REPORTING OF CHANGE IN IMEI NUMBER Mayank Sahni, Guru Gobind Singh Indraprastha University.

[2] Proceedings of the 5th National Conference; INDIACom-2011 Computing For Nation Development, March 10 – 11, 2011 Bharati Vidyapeeth‟s Institute of Computer Applications and Management, New Delhi Copy Right © INDIACom-2011 ISSN 0973-7529 ISBN 978-93-80544-00-7 Model for Tracing of Stolen or Lost Mobile Phone Station Anil Kumar1 and Vibhakar Mansotra2 1,2Department of Computer Science& IT ,University of Jammu 1 akticku@yahoo.com and 2 vibhakar20@yahoo.co.in .

[3] Krishan Kumar et al, International Journal of Computer Science and Mobile Computing, Vol.4 Issue.5, May- 2015, pg. 527-533 © 2015, IJCSMC All Rights Reserved 527 Available Online at www.ijcsmc.com International Journal of Computer Science and Mobile Computing "Vulnerability Detection of International Mobile Equipment Identity Number of Smartphone and Automated Reporting of Changed IMEI Number".

[4] International Journal of Innovations in Engineering and Technology (IJIET), Sniffeer Technology for Mobiles Poonam Singla.

[5] International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 3, March 2016 Copyright to IJARCCE DOI 10.17148/IJARCCE.2016.5348 192 Mobile Tracking Based on Phone Theft Detection B. Srilekha1 , Dr. V. Dhanakoti2.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY