Cyber Security Internship 2016

**\*DO NOT USE FOR UNETHICAL PURPOSES**

**PROJECT REPORT**

**On**

**MOBILE CRIME &**

**INVESTIGATION**

**SUBMITTED BY:**

**D.K. Rajput,**

**Dinesh Chand Yadav,**

**Divyanshu Shukla,**

**Mohammad Shagil Siddiqui,**

**Pranjal,**

**Preeti Sharma,**

**Rishabh Mishra**

**Under the Guidance of:**

**Rakshit Tandon**

**INDEX**

|  |  |
| --- | --- |
| Title | **Page Number** |
| Acknowledgement | 1 |
| Special Thanks | 2 |
| About The Guide | 3 |
| Abstract | 4 |
| Team Contribution | 5 |
| 1.Introduction  1.1 Impact of cell phone on human life  1.2 Cell phone: Open door for cyber crimes | 6-8 |
| 2. Mobile Statistics | 8 |
| 3. Mobile Crime Threats  3.1 Fake SMS Scandals  3.2Hate Speech And Rumor Spreading  3.3 VOIP Hacking And Vishing  3.4 Spyware  3.5 MMS Malware  3.6App Frauds | 9  13  13-14  14  15-17  17  18-19 |
| 4. Case Studies | 20-26 |
| 5.CDR Analysis | 27-30 |
| 6. Mobile Device Forensics  6.1 Digital Evidence On Mobile  6.2 Investigation Tools  6.3 Forensic Examination And Analysis | 31  31-33  33-34  34-35 |
| 7. Technical Research And Development | 36-40 |
| 8.How To Protect Mobile | 41 |
| 9.Conclusion | 42 |

**ACKNOWLEDGEMENT**

It is with great pleasure that we find our self penning down these lines to express my sincere thanks to various people who helped me a long way completing this project.

The harmonious climate in the cyber cell and the Commissioner of Police office provided proper guidance for preparing the project. It was a privilege to have been guided by Mr. Rakshit Tandon. We really thanks you Rakshit Tandon sir to give such a wonderful environment to grow in field of cyber security.

Thanks to Inspector Sudhir Kumar State Cyber Crime Branch, Gurugram Police for his induction and training on live case studies.

Thanks to all fellow mates who helped me during the development of this project with their constructive criticism and advice.

We would also like to thank the honorable **Commissioner of Police Shri Navdeep Singh Virk** for giving me such a good opportunity to get exposed and updated with the latest technology with the field of the cyber security

**SPECIAL THANKS**

**A** special thanks to the snapdeal who sponsors this cyber security internship 2016.Its really a wonderful environment that does not only gives us with technical aspects about cyber security but also make us able to understand the legal aspects related to the cyber security .And the best part of this internship case studies is what we are given with the live case studies that really appreciate towards cyber security and we get to know many cyber crimes that are not even heard by us .We are also going to know the technical investigation tools used not only for securing us but can took us forward the nations safety and security. We really get motivated from this internship and get a confidence to do something for our nation.



**ABOUT THE GUIDE**



**RAKSHIT TANDON**

* Director – A&R Info Security Solutions Pvt. Ltd.
* Consultant – Internet and Mobile Association of India.
* Member Advisory Board- National Cyber Safety & Security Standards (NCSSS)
* Trustee - “Cyber & Law Foundation " An International NGO involved in Policy, Research & Training related to Cyber & Privacy Issues.
* Advisor- Cyber Crime Unit, Uttar Pradesh Police, Agra.
* Advisor – Cyber Crime Cell, Gurgaon, Haryana Police.
* President- JAT (Joint Action Team) for combating Cyber Crime against Women and Children.
* Consultant - AIWEFA (All India Women's Education Fund Association).
* Resource Person- BPRD Bureau for Police Research and Development, Govt of India
* Visiting Faculty-Lecturer at DR. B.R. Ambedkar Police Academy - Moradabad (U.P) Haryana Police
* Academy -Karnal, Police Radio Training School, Indore, CDTS (Central Detective Training School)Chandigarh, Jaipur and Ghaziabad, Rajasthan Police Academy, Internal Security Academy CRPF, MountAbu.
* Guest Lecturer at Chandigarh Judiciary Academy.

**ABSTRACT**

In today’s world, the mobile become an essential asset as it is used in daily life by every individual. Crime has been an integral part of human civilization from its very beginning. Criminal activities have always inspired human minds. As mobile crimes are increased due to increase in use of internet so we should focus on internet which includes many latest apps that allow users to create an online profile in which users post up-to-the-minute personal and professional information about their lives that can include pictures, videos, and related content. And this credential information should be secure and easy to use. This project’s aim is to create awareness among people & provide security to mobile users.



**TEAM CONTRIBUTION**

1. **MR .D.K. RAJPUT** contributed as project supervisor.
2. **Name :** Dinesh Chand Yadav

**Course :** Pursuing M.Tech.(Cyber Security)2nd year

**University:** Sardar Patel University of Police,Jodhpur

**Contribution:** Content Collection on FAKE SMS SCANDALS.

1. **Name :** Mohammad Shagil Siddiqui

**Course:** Pursuing B.Tech.(Computer Science)3rd year

**University:** UPES, Dehradun

**Contribution:** App Development

1. **Name :** Pranjal

**Course :** Pursuing B.A.L.L.B. 1st year

**University :**Depts. Of Law, MDU, Rohtak

**Contribution:** Case studies and content collection.

1. **Name :** Rishabh Mishra

**Course :** Pursuing B.Tech.(Computer Science) 3rd year.

**University :**Integral University.

**Contribution:** Content Collection and CDR analysis.

1. **Name :** Divyanshu Shukla

**Course :** Pursuing B.Tech.(Computer Science).3rd year

**University :**BBDNITM , Lucknow

**Contribution:** Content Collection on mobile threats and ppt making.

1. **Name :** Preeti Sharma

**Course :** Pursuing M.Tech.(Computer Science) Final year

**University :** Kurukshetra University, Kurukshetra

**Contribution:** Content Analysis And Report Writing.

**1. INTRODUCTION**

M

obile devices such as cell phones and smart phones have become an integral part of peoples’ daily lives, and as such, they are prone to facilitating criminal activity or otherwise being involved when crimes occur. No other computing device is as personal as the mobile phone, effectively providing a computer in a pocket. Whereas computers, laptops, servers, and game machines might have many users, in the vast majority of cases, mobile devices generally belong to an individual.

Although compact, these handheld devices can contain personal information including call history, text messages, e-mails, digital photographs, videos, calendar items, memos, address books, passwords, and credit card numbers. These devices can be used to communicate, exchange photographs, connect to social networks, blog, take notes, record and consume video and audio, sketch, access the Internet, and much more. As the technology develops, higher data

transmission rates are allowing individuals to transfer more data (e.g., digital video), and the computing power in these devices enables us to use them in much the same way as we used laptop systems over the past decade. Because these devices fit in a pocket or bag, they are often carried wherever a person goes and can be used to determine a person’s whereabouts at a particular time.

This rapid development of mobile computing and communication technology creates opportunities for criminals and investigators alike. The information stored on and associated with mobile devices can help address the crucial questions in an investigation, revealing whom an individual has been in contact with, what they have been communicating about, and where they have been. Sexual predators can use a mobile device to make initial contact with victims, exchange photographs or videos, and groom victims, creating a vivid cyber trail for digital investigators to follow. Mobile devices have been instrumental in solving homicides, are used by terrorists for reconnaissance and coordination, can be used to smuggle contraband across borders, and are frequently found in prisons despite being prohibited. Members of major criminal organizations and gangs use mobile devices to coordinate activities.

**1.1 IMPACT OF CELL PHONES ON HUMAN LIFE:**

Communication technology has left no aspect of human life untouched.  Even our morning alarm clocks are been replaced by the mobile cell phones.  Technology is constantly bringing advancement in our mobile cell phones.  Mobile cell phones have now become new personal laptops and desktops which are having capacity to store as much data as our laptops and desktops are and in additional they are providing flexibility and portability.  Internet enabled Smart phones, tablets etc… are performing the functions of our computer,  but one vital feature is missing and that is Security.  Rapid growth in the use of internet enabled mobile cell phones allows us to use manage our banking transaction, official and institutional transactions, rapid communication through email or social networks, and many more.  Virtually we can perform the task of a computer on our mobile; this means alike our computer our mobile phone is also vulnerable to the risk of fraud, theft of financial information and identity theft etc..

The increasing computational power of mobile devices has afforded even greater uses, and with that, greater potential for misuse. For instance, some mobile devices are optimized for data acquisition such as credit card scanning and scientific measurements (e.g., voltage, temperature, acceleration). This flexibility has ramifications beyond the manufacturer’s intentions, and mobile

devices have been used to steal credit cards and trigger bombs.

**1.2 CELL PHONES AN OPEN DOOR FOR CYBER CRIMINALS**

Recent reports have suggested that with the advancement of the telecommunication technology there is increase in cyber crime in the nation.  The technological advancement provided opportunities to the miscreants in the society, who are using technology for their selfish gains. There are cases where hackers have breached in Nokia’s Symbian, Apple’s iOS and Google’s Android operating system.  Thus to be safe we must be vigilant.  But it is really unfortunate that whenever a discussion about cyber crime ignites, a particular class of the people escapes the discussion saying that; they neither use computers nor they use internet for communication and therefore cyber crime is not a threat for them.  People try to hide their ignorance about cyber crimes on the ground that cannot become its victim, but they have absolutely no idea that knowingly or unknowingly they can be adversely affected by cyber crime.  Every person using an internet, blue tooth or even an infra red enabled cell phone is can easily be fished in the web of cyber criminals.

**2. MOBILE CRIME STATISTICS**

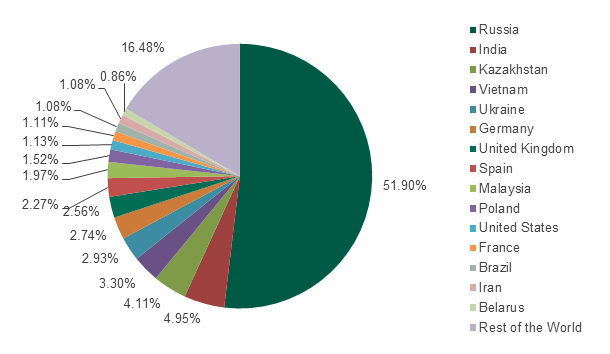


Fig. Mobile Crimes Report 2015

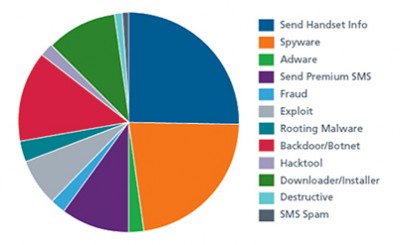


Fig. Different Mobile Crimes In India

**3. MOBIE CRIME THREATS**

1. ID THEFT
2. MMS DEFAMATION
3. WHATSAPP SPOOFING
4. APP FRAUDS
5. VOIP HACKING AND VISHING
6. RUMOUR SPREADING AND HATE SPEECH
7. SEXTING
8. PHOTO MISUSE
9. SMS SCANDALS
10. CAMERA THREATS
11. SS7 HACKING
12. VIRUS AND MALWARE
13. NFC PROXY
14. E-WALLET HACKING/ AIRTIME THEFT



**3.1 FAKE SMS SCANDALS**

It is also called SMS spoofing. Culprit offer the sending text SMS with self-created sender number or name. Spoofing has both legitimate uses(setting the company name from which the message is being sent, setting your own mobile number, or a product name)and illegitimate uses(such as impersonating another person, company, product).This tempting SMS has been received by millions of mobile user in India .However ,the rear no estimates on the number of people who got induced by such sham message sand lost money.

**Various types of SMS fraud are:**

* **Spam:** Spamming is an action where the subscriber receives an unsolicited SMS. An unsolicited SMS is one the subscriber did not request to receive. The act of spamming does not define the content but only the fact that the SMS was received without solicitation. The content of the spam SMS is incidental to the act. The spam SMS may take on various forms of content to include: commercial information, bogus contest and other message generally intended to invite a response from the receiver.
* **Spoofing:** The spoofing case is related to an illegal use of the HPLMN SMS-C by a third party. In this case, an SMS MO with a manipulated A-MSISDN (real or wrong) is coming into the HPLMN network from a foreign VLR (real or wrong SCCP Address).
* **Flooding:** The act of flooding is when a large number of messages are sent to one or more define flooding is the extraordinary number of messages sent.
* **Faking:** A fake SMS is originated from a foreign SS7 network and is terminated to a mobile network. This is a specific case when SCCP or MAP addresses are manipulated. The SCCP or MAP originator (for example:

According to the survey sender sending following type text SMS such as :

1. **Lottery:**

Attacker send text message from unknown number (8470970295) stating that “YOUR MOBILE NUMBER HAS WON 750,000POUNDS FOR ON GOING ICC WORLD CUP T20 AWARD.TO CLAIM YOUR PRIZE, (SEND YOUR NAME, ADDRESS AND MOBILE#) VIA

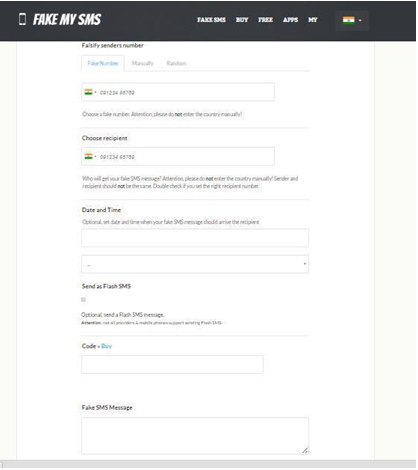
Email[: crkdraw@hotmail.com](mailto:crkdraw@hotmail.com)”.

1. **Use Govt. Organization (RBI, Income TAX):**

Attacker send text message about asking their credential information using the name of big government organizations like: SBI, RBI etc.

**3.1.1 FAKE SMS TOOLS :**

There are many websites and apps that provide us with creating messages with fake number and identity that are normally used by attackers. One of the tool for creating fake message with fake identity is shown as:



**3.1.2 STEPS TO PROTECT YOU FROM TEXT MESSAGE (SMS) SCAM:**

* Never reply to any unsolicited txt message
* Never rely on company names& contact details in an SMS. The genuine contac tdetail will be different you could end up calling a cyber thief if you rely on contact details in an

unsolicited SMS

* Never click any link or visit a web site suggested in an unsolicited txt
* Never call back the number in an unsolicited txt message
* Be aware that you can ever be a winner of anything ,unless you have entered in a competition or a program by yourself
* No company will employs someone, out of the blue
* Never participate in Online Surveys, conducted by unknown entities
* Always remember: scammers use names of well known companies ,to trap victims.

**3.2 HATE SPEECH AND RUMOUR SPREADING THROUGH SOCIAL MEDIA AND MMS**

As the heading itself clears a lot......wrong message, rumor or any information capable of spreading violence between two people or two communities is spread using a mobile, social media.

In a country like India, that is one of the most diverse country of world, rumors and hate speeches are often used by some creepy elements of the society for their personal and political benefits. There are various sensitive issues and topics for almost every part of the country let it be against army and locals in Kashmir, or something related to Jatt andolan in Haryana, to masjid-mandir in UP, and even languages Hindi or Marathi , color and looks for North Eastern and South and above all Hindu-Muslim. So it becomes very difficult for law enforcement agencies to stop the flow of rumor once the mobile and social media is used for spreading it, as it take no time to spread, Face book ,Twitter and Whatsapp are some major services that are used by these creepy minds as it involve a huge audience.

**3.2.1 What LEA's are doing in such cases?**

Our LEA's do take some steps cutting the internet services, tracking of culprit ,but these are often taken late when actual motive of the rumor is achieved.

**3.2.2 WHAT WE SUGGEST:**

Sensitive areas should be marked, and special awareness campaigns should carried out for general public.

LEA's in such conditions should try to take quick and efficient decisions.

Most important is officials should try to spread the correct information among the general public and in this case the same medium that is the mobile and social media can play a major role.

**3.3 VOIP HACKING AND VISHING**

Voice over IP (VOIP) has finally come of age and is being rapidly embraced across most markets as an alternative to the traditional public-switched telephone network (PSTN). VoIP is a broad term, describing many different types of applications (hard phones, soft phones, proxy servers, Instant Messaging clients, peer-to-peer clients, and so on),installed on a wide variety of platforms (Linux, Windows, VxWorks, mobile devices, PCs, and so on), and using a wide variety of both proprietary and open protocols (SIP, RTP, H.323, MGCP, SCCP, Unistim, SRTP, ZRTP, and so on) that depend heavily on your preexisting data network's infrastructure and services (routers, switches, DNS,TFTP, DHCP, VPNs, VLANs and so on). Correspondingly, VoIP security is just as broad a subject thanks to the heterogeneous nature of these environments found in the consumer, enterprise, carrier, and small/medium–sized business markets.

In order to narrow the focus, we decided to cater mainly to the enterprise IT audience and include some of the more popular deployments in our target list. Because VoIP packetizes phone calls through the same routes used by traditional enterprise data networks today, it is consequently prone to the very same cyber threats that plague those same networks. These include denial-of service attacks, worms, viruses, and general hacker exploitation. For

instance, if your enterprise is under attack from a distributed denial of service (DDoS) attack, internal users' web browsing might be slower than normal. A DDoS attack on a VoIP-enabled network can completely cripple your VoIP applications, at least to the point where conversations are unintelligible.

In addition to these traditional network security and availability concerns, there are also a plethora of new VoIP protocol implementations that have yet to undergo detailed security analysis and scrutiny. Most major enterprise VoIP vendors are integrating the up-and-coming Session Initiation Protocol (SIP) into their products. As a result, SIP-specific attacks such as registration hijacking, BYE call teardown, and INVITE flooding are also likely to emerge—not to mention the plethora of financially motivated nuisances such as Spam over Internet Telephony(SPIT) and the voice phishing attacks that are just beginning to bleed into the VoIP realm.

**3.4 SPYWARE**

**Mobile malware** is malicious software that targets mobile phones or wireless-enabled Personal digital assistants (PDA), by causing the collapse of the system and loss or leakage of confidential information. As wireless phones and PDA networks have become more and more common and have grown in complexity, it has become increasingly difficult to ensure their safety and security against electronic attacks in the form of viruses or other malware. About 16 million mobile devices infected by malware in 2014 with hacking attempts on the rise. Mobile malware is on the rise, and 16 million devices are currently estimated to be infected right now in the world.

An epic 16 million mobile devices now in circulation in the world are currently infected by some sort of malware - almost 1% of all mobile devices.

A [new report](http://www.alcatel-lucent.com/blog/2015/under-attack-malware-invades-our-devices-data-and-privacy-2014) released by the security arm of telecoms infrastructure firm Alcatel-Lucent shows that there has been a 25% increase in malware attacks on mobile devices since 2013.

2014 was truly the year of cyber attacks, with huge numbers of big corporations and retail chains being hacked and millions of credit and debit card details stolen, but Alcatel-Lucent says that this entire still paled against the number of malware attacks that were perpetrated on mobile devices.

You know how Windows PCs are considered to be the primary targets and backbone of cybercrime?

Well in mobile networks, it probably won't surprise you to learn that Android devices are where all the malware is headed, with malware only affecting less than 1% of other smartphones like iphones, Windows Phones or Blackberry’s.

**3.4.1 INCREASE IN MOBILE SPYWARE APPS**

There is also an increase in mobile spyware apps infecting mobile devices – of the top 20 malware discovered to be infecting the world's devices, Alcatel-Lucent found that at least six were spyware.

Spyware is used to track everything about a smartphone's owner. These apps can monitor ingoing and outgoing calls and text messages, monitor email and track the victim's web browsing, as well as the location of the owner's phone.

The firm found that the 50% of all malware infections were observed in Android phones and tablets, due to the fact that there is no control of the digital certificates used to sign Android apps.

Since Android apps are usually self-signed and can't be traced to the developer, it's easy to hijack Android apps, inject code into them and then re-sign them.

**3.4.2 MOBILE MALWARE TOOLS :**

* **Cabir:** This malware infects mobile phones running on Symbian OS and was first identified in June 2004. When a phone is infected, the message 'Caribe' is displayed on the phone's screen and is displayed every time the phone is turned on. The worm then attempts to spread to other phones in the area using wireless Bluetooth signals, although the recipient has to confirm this manually.
* **Duts:** This parasitic file infector virus is the first known virus for the Pocket PC platform. It attempts to infect all EXE files that are larger than 4096 bytes in the current directory.
* **Skulls:** A trojan horse piece of code that targets mainly Symbian OS. Once downloaded, the virus replaces all phone desktop icons with images of a skull. It also renders all phone applications useless. This malware also tends to mass text messages containing malicious links to all contacts accessible through the device in order to spread the damage. This mass texting can also give rise to high expenses.
* **Commwarrior :**This malware was identified in 2005. It was the first worm to use MMS messages in order to spread to other devices. It can spread through Bluetooth as well. It infects devices running under OS Symbian Series 60. The executable worm file, once launched, hunts for accessible Bluetooth devices and sends the infected files under a random name to various devices.
* **Gingermaster**: A trojan developed for an Android platform that propagates by installing applications that incorporate a hidden malware for installation in the background. It exploits the frailty in the version Gingerbread (2.3) of the operating system to use super-user permissions by privileged escalation. Then it creates a service that steals information from infected terminals (user ID, number SIM, phone number, IMEI, IMSI, screen resolution and local time) by sending it to a remote server through petitions HTTP.
* **DroidKungFu**: A Trojan content in Android applications, which when executed, obtains root privileges and installs the file com.google. ssearch.apk, which contains a back door that allows files to be removed, open home pages to be supplied, and 'open web and download and install' application packages. This virus collects and sends to a remote server all available data on the terminal.
* **Ikee**: The first worm known for IOS platforms. It only works on terminals that were previously made a process of jail break and spreads by trying to access other devices using the SSH protocol, first through the subnet that is connected to the device. Then, it repeats the process generating a random range and finally uses some preset ranges corresponding to the IP address of certain telephone companies. Once the computer is infected, the wallpaper is replaced by a photograph of the singer Rick Astley, a reference to the Rick roll phenomenon.
* **Gunpoder :** This worm file infector virus is the first known virus that officially infected the Google Play Store in few countries, including Brazil

**3.5 MMS MALWARE**

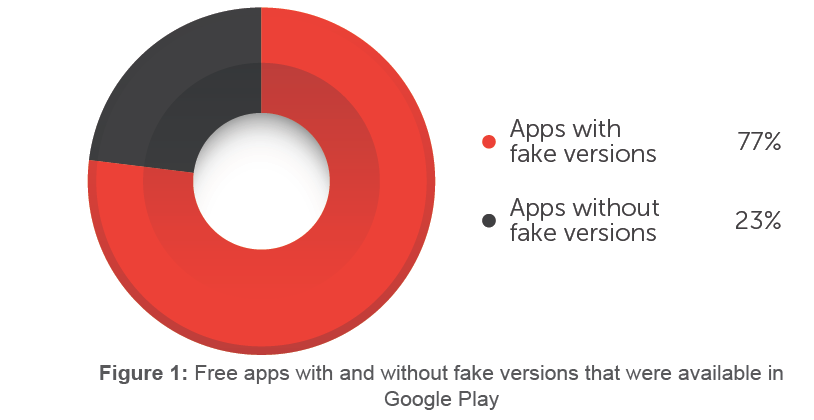
Malware makers are also looking for ways to exploit text-based communication as a way to deliver malware. As noted by CSO Online , a vulnerability in Android's media library, Stage fright, made it possible for attackers to send a text message embedded with malware to any mobile number. Even if users didn't open or acknowledge the text, the malware could still deploy, allowing hackers root access to your mobile device. The problem was quickly patched but offered proof of text-based infections.

**3.6 APP FRAUDS**

As the number of mobile device users grow, It has actually become quite common to see fake apps shortly after legitimate mobile or PC versions come out.

A survey of the top 50 free apps available for download in Google Play revealed that almost 80% of the samples had fake versions.These apps span a wide range of categories in Google Play, including Business, Media & Video, and Games.

12

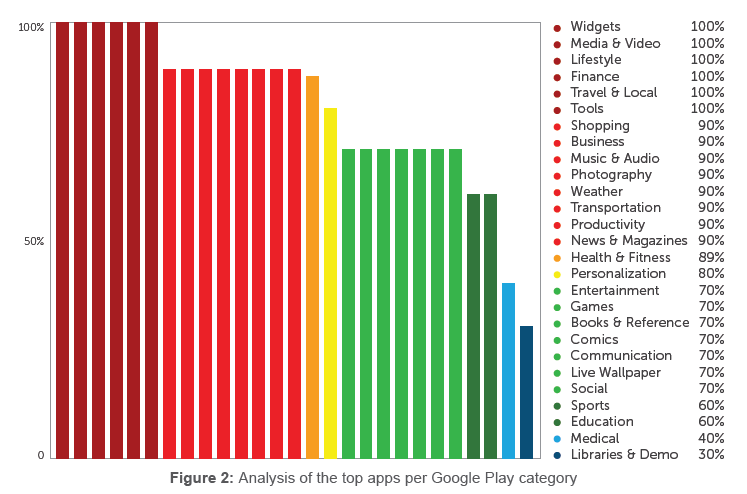


Of roughly the top 10 apps in each category in Google Play, fake versions of the following were available in figure 2:

* 100% of the apps categorized under Widgets, Media & Video, and Finance
* 90% of the apps categorized under Business, Music & Audio, and Weather
* Approximately 70% of the apps categorized under Games, Books and Reference, and live wallpaper.

* Approximately 60% of the apps categorized under Sports and Education

40% of the apps categorized under Medical



Fake apps were more likely to be high-risk apps or malware rather than just mere harmless copycats.2 As of April this year, of the 890,482 sample fake apps discovered from various sources, 59,185 were detected as aggressive adware and 394,263 were detected as malware. Among the fake apps, more than 50% were deemed malicious (see Figure 3).

Malicious No malicious 51% 49% Trend Micro | Fake Apps Trend Micro | Fake Apps **Figure 3:** Ratio of malicious to no malicious fake apps

**4. CASE STUDIES :**

1. **Case study: Obscene Phone Calls**

|  |  |  |
| --- | --- | --- |
| State | : | Karnataka |
| City | : | Bangalore City |
| Sections of Law | : | 67 Of IT Act 2000. |

“Nothing has the power to broaden the mind as the ability to investigate systematically and truly all that comes under thy observation in life.” - Marcus Aurelius

**Background :**  
A written complaint was submitted by the complainant stating that she had been receiving obscene phone calls on her mobile and landline numbers. The complainant learnt from the callers that a doctored profile of hers had been posted on a Website. The profile stated that the complainant loved sex and when the viewers were in Bangalore, they should contact her..The profile also gave out victim’s landline and mobile phone numbers.  
**Investigation :**   
The investigating officer obtained call details of the perpetrator's number from the cellular service provider and observed that the most frequent incoming and outgoing calls were from two other mobile numbers. The investigating officer also obtained the IMEI addresses for these numbers from the mobile service provider.   
  
The investigating officer sent out letters to the Website on which the obscene profile of the complainant had been hosted to obtain details of the date, time of the profile creation, the IP address used for the creation, the access details for the profile and any other details that the Website would be able to provide regarding the profile and the e-mail ID.   
  
The investigating officer then contacted the outlet from where the mobile connection had been purchased and learnt that one of the SIM cards used was a demo card which had been issued to a dealership. Upon further investigation it was found that the other SIM card was allotted to a college student and was being used by his friend. The investigating officer got suspicious and on further enquiry found that the college student was of dubious character.   
  
The investigating officer obtained a search warrant and raided the residence of the college student. Using disk imaging and analysis tools, the team recovered the obscene profile that was posted on the internet from the student's computer. The partners of the accused were also examined in the presence of the complainant. The accused admitted that he was guilty.   
  
It later transpired that the college student was a close family friend of the complainant and that he was suffering from a personality disorder, secondary depression and poor self-esteem.   
  
**CURRENT STATUS**   
The case has been finalised and a report of class “B” has been submitted.

1. **Case study: obscene content**

|  |  |  |
| --- | --- | --- |
| State | : | Karnataka |
| City | : | Bangalore |
| Sections of Law | : | 66 & 67 of IT Act 2000. |

“True problem solving is impossible with the type of the behaviour that tries to shift the responsibility on to others.”- Hosotani

**Background :**  
The complainant approached the police stating that she had been receiving obscene and pornographic material at her e-mail address and mobile phone. She stated that this person appeared to know a lot about her and her family and believed that her e-mail account had been hacked.   
  
**Investigation :**  
The investigating team using a different e-mail ID tried to chat with the accused using the complainant’s e-mail ID. Subsequently the investigating team was able to identify the ISP address of the computer system being used and it was tracked to an organisation in Delhi.   
The investigating team visited the company and through its server logs was able to identify the system from which the obscene material was sent. Using forensic disk imaging and analysis tools the e-mails were retrieved from the system. The residence of the accused was located and the hard disk of his personal computer was seized. On the basis of the evidence gathered the accused was arrested.   
**Current status**   
The case has been finalised and is currently pending administrative approval.

1. **Case study: Morphed Photographs**

|  |  |  |
| --- | --- | --- |
| State | : | Delhi |
| City | : | New Delhi |
| Sections of Law | : | 67 of IT Act, 120-B, 506, 509 IPC |

**“It is capital mistake to theorize before you have all the evidence. It biases the judgment.”**   
- Sir Arthur Conan Doyle

**Background:**   
The complainant was receiving threatening and obscene e-mails from unknown people. The e-mails contained the complainant's obscene morphed photographs. The accused threatened to post these on pornographic Websites and alleged that one such photograph was posted on a popular Website.   
**Investigation :**  
The IP address used for posting the obscene photograph(s) on the Website and the mails sent to the complainant were retrieved and traced to a company in Delhi.   
A search of the computer terminals located in the company's premises was conducted. The log records and cookies were examined. During the process the morphed photograph of the complainant was found in one of the terminals used by the accused. The e-mail accounts mentioned were also accessed after disclosure by the accused. The central processing unit of the computer was seized and sent for a forensic analysis to the central forensic science laboratory. Using disk imaging and analysis tools, the mirror image of the hard disk was taken and analysed which led to the recovery of all the incriminating data/files required for the case.   
During the investigation it was learnt that the accused was an ex-colleague of the complainant.   
  
**Current status**   
Charge sheet has been filed against the accused.

1. **Case study: Sexual Harassment**

|  |  |  |
| --- | --- | --- |
| State | : | West Bengal |
| City | : | Kolkata |
| Sections of Law | : | 419/501/507/509 IPC and 67 IT Act 2000. |

**“You cannot compel people to comply with the standards; compliance must be a voluntary decision.”** - Allan Sayle

**Background**   
A lady (the complainant) lodged a complaint that she was being harassed by a flood of telephone calls from unknown men with sexual intention at all odd hours and from various places around the world. As she was a working lady, most of the calls were received by her aged in-laws. When she had her telephone number changed, and requested the new number to be kept private, her neighbours started receiving the same kind of calls asking for her by name. This was thoroughly harassing her aged in-laws, her husband and also her neighbours. Some men also visited her house, seeking her by name.   
**Investigation**   
A caller ID was installed at the house of the complainant and a few of the local callers were interrogated. During interrogation it was found that the callers had obtained her e-mail ID in one of the chat rooms. All those who sent the mail to her got an auto response giving her residence telephone number and urging them to call during office hours on working days as her husband is away during those hours. On receiving such e-mails these people contacted her on the phone numbers given in the e-mail.   
Police requested for IP addresses of the e-mail IDs from the Website hosting company. In addition they asked for IP logs and registration profiles of the respective e-mail ID's. The logs revealed the service provider (ISP), who subsequently provided the telephone number and the address of the user.   
The ISP provided the details of the IP and addresses/ information connected to it. Raids were conducted at the residential address of the accused. It was found that on the two computers temporary files (of the accused) had been deleted. However using forensic software, few of these deleted files could be re-created. The PC of the accused also had incriminating evidence against him. He confessed to his guilt and was arrested.   
During investigation it was learnt that the complainant was employed as a temporary executive engineer in the same company with the accused. The accused felt that though she was junior to him, she was not giving him proper respect. He started sending auto generated e-mails in her name, giving her telephone numbers and asking males to contact her during office hours.   
  
**Current status**   
It is the first registered cyber crime case in West Bengal.

1. **Case study: VOIP calling (kidnapping)**

|  |  |  |
| --- | --- | --- |
| State | : | Haryana |
| City | : | Faridabad |
| Sections of Law | : | 369 of IPC and 66 of IT act |

**Background**   
A builder complaint that his son has been kidnapped and he got a call from the kidnappers from an international number (it was a VOIP calling), demanded for money.

**Investigation**

The number was immediately taken by police and they asked for the trunk gateway of that call and found it to be the number of germany, so it was not possible at all to trace them by that no.

Police contacted the parents and told them to ask for the proof of their child to be alive, the kidnappers sent the vedio of the child by whatsapp to the builders no, immediately they contacted to whatsapp, sent them a legal notice to give the details of that number but their was no reply at all....

What police did was they used the stagnosploit and embedded an location grabber to an image and sent it to the kidnappers, as they opened it police got the live location of the kidnappers and were able to rescue the child.  
**current status**   
the case is under trial in the court...

1. **Case study: MMS leak**

|  |  |  |
| --- | --- | --- |
| State | : | Delhi |
| City | : | Delhi |
| Sections of Law | : | 66E, 67, 67A of IT act 2000 |

**Background**   
A girl complained that she came to know about a video on one of the porn site by her friend and it was her video but she do not remember that when did just this all happened. In that video the face of the boy was blurred so was not visible at all.  
**Investigation**

The investigation started with the identification of the boy and the place, in which the girl helped the police and identified the place and remembered it and told that it was the place where she went for a party with her boyfriend a moth back, the boy was kept under remand and he told the whole actual story...

He told that when the girl was at the party he drugged her by adding sleeping pills in her drink, and during her unconsciousness entered into sexual relationship and capture that all scene and posted it on a porn site.

Unfortunately were not able to remove that video as the website being foreign did not responded to Indian police, but police blocked it on Indian IP’s.

1. **Case study: Sexting**

State: Meghalaya

**Background**

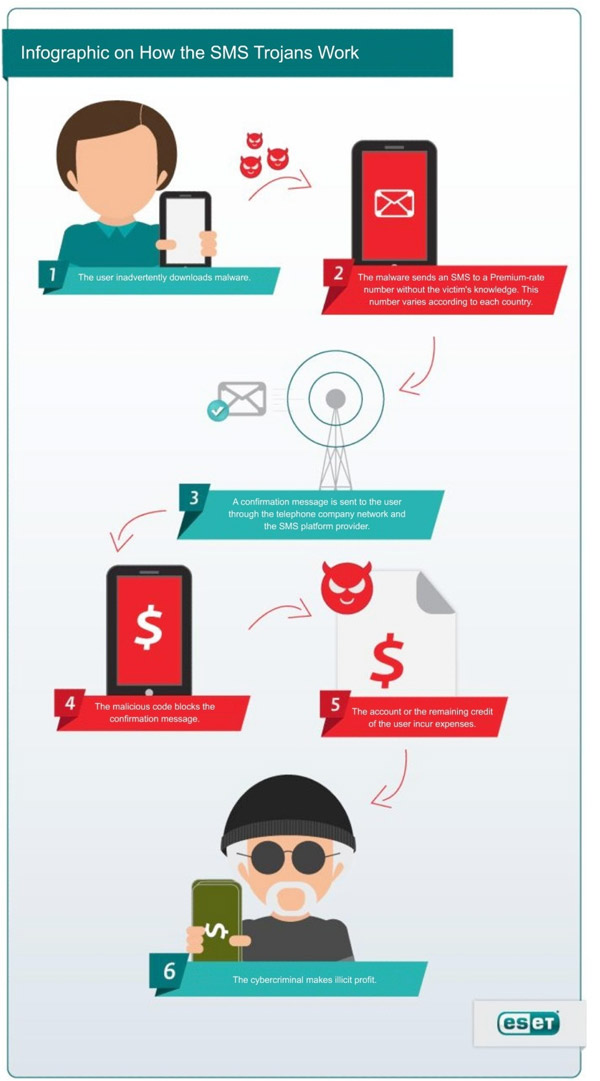
A video came to the lady principal of the school which contained the compromised photos and video of a 14 year girl of her school, she came to that video by a teacher who got it from his son who goes to a coaching where he got it from the students who were sharing it on the coaching whatsapp group**.**

**Investigation**

Principal informed the authority,.. proper councelling was done of the girl, her parents were called, she was asked to tell the whole store and she tol the name of a 1st year student of a college and pass out of their school itself, the boy and his parents were called and his laptop and mobile were seazed and were checked and the authority found 369 files of hardcore pornographic content which was being consumed by the boy......

**Current status**

The girl was a national sports person and due to her deflation issues the parents did not reported to laudge an FIR so he was releaved from the custody without any charge sheet....



**5. CDR (CALL DETAIL RECORD) ANALYSIS:**

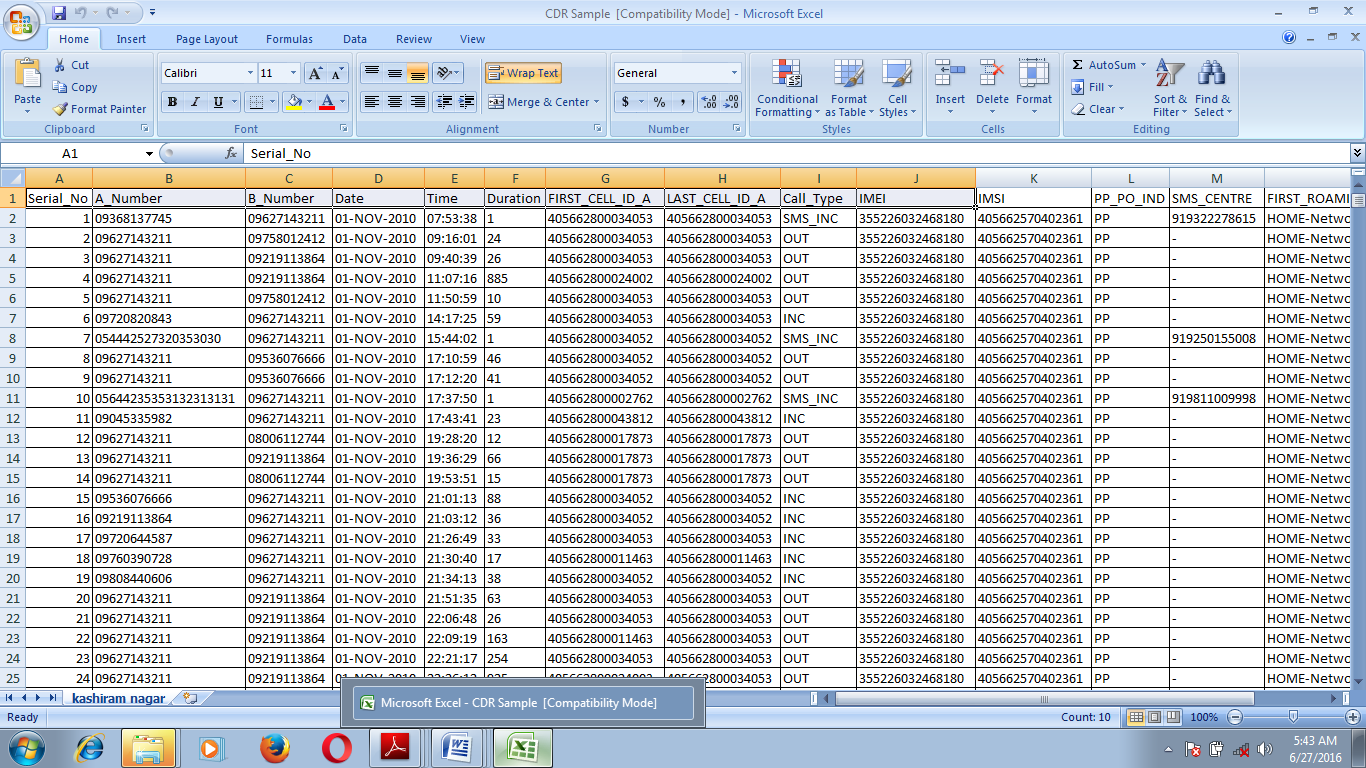
A call detail record (CDR) is a data record produced by a telephone exchange or other telecommunications equipment that documents the details of a telephone call or other communications transaction (e.g., text message) that passes through that facility or device. The record contains various attributes of the call, such as time, duration, completion status, source number, and destination number. Today this is used in about 90% of cases no matter it is a cyber crime or a normal case. Apart from normal CDR we also have GPRS CDR that contains some more additional information (such as amount of data used, source IP, destination IP,2G,3G,4G) than a normal CDR.

**IMPORTANT**=== Not everyone can get a CDR, Only LEA's can get the CDR from the telecom companies that too if they have CRPC 91 document.

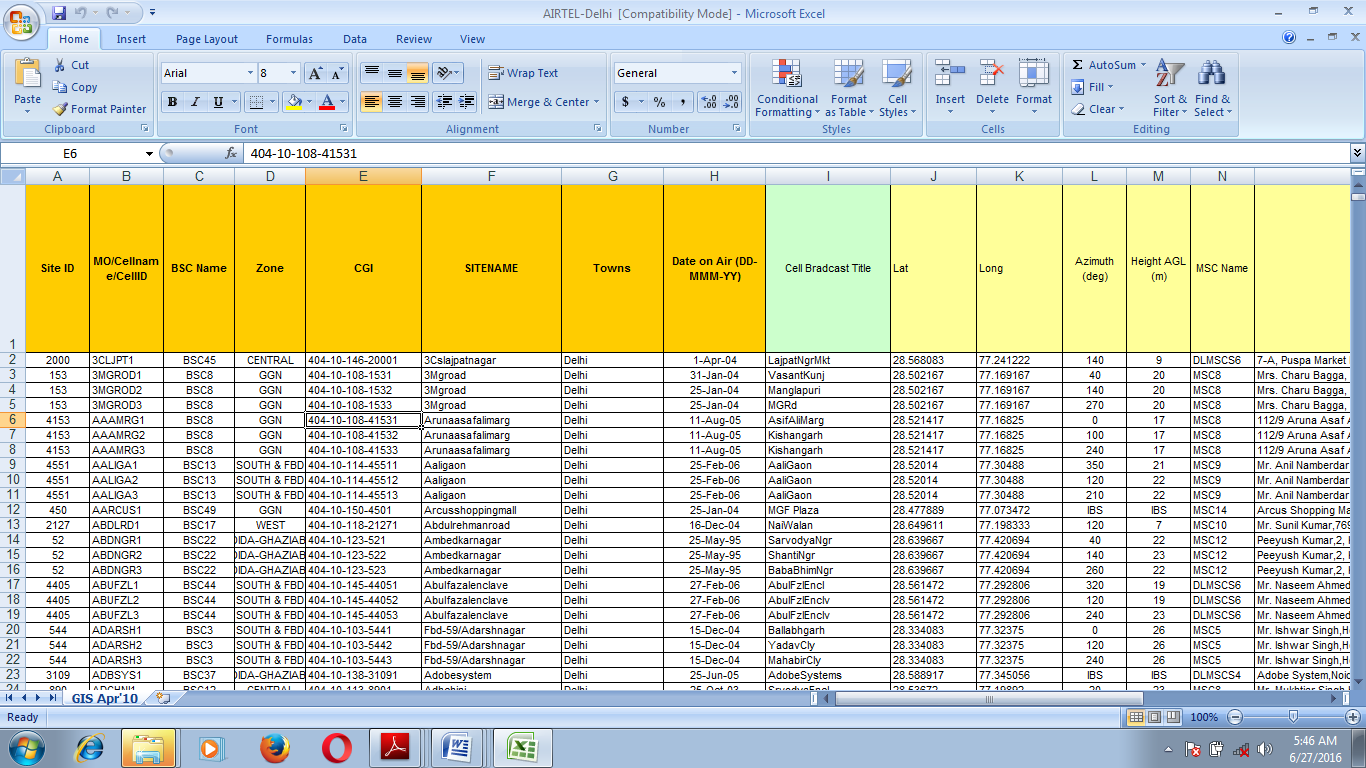
A normal CDR may contain following data :

* the phone number of the subscriber originating the call (calling party, A-party)
* the phone number receiving the call (called party, B-party)
* the starting time of the call (date and time)
* the call duration
* the billing phone number that is charged for the call
* the identification of the telephone exchange or equipment writing the record
* a unique sequence number identifying the record
* additional digits on the called number used to route or charge the call
* the disposition or the results of the call, indicating, for example, whether or not the call was connected
* the route by which the call entered the exchange
* the route by which the call left the exchange
* call type (voice, SMS, etc.)

**5.1 SAMPLE CDR AND GPRS CDR:**

**CDR :** 

**GPRS CDR :**



**5.2 CDR ANALYSIS TOOLS:::**

There are lot of tools available that can be used for analyzing a CDR. These tools make a CDR analysis lot easy and quick as analyzing a typical CDR manually is very difficult. These contain almost all the option that may be require to analyze a CDR from finding, arranging the numbers as needed to generating a final report. A typical tool is shown below:

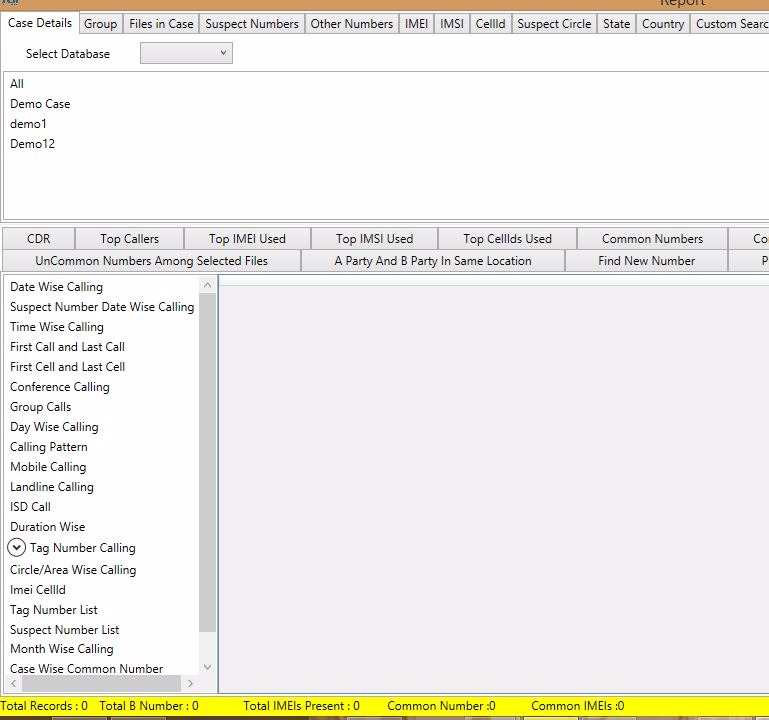


Fig. CDR analysis tool

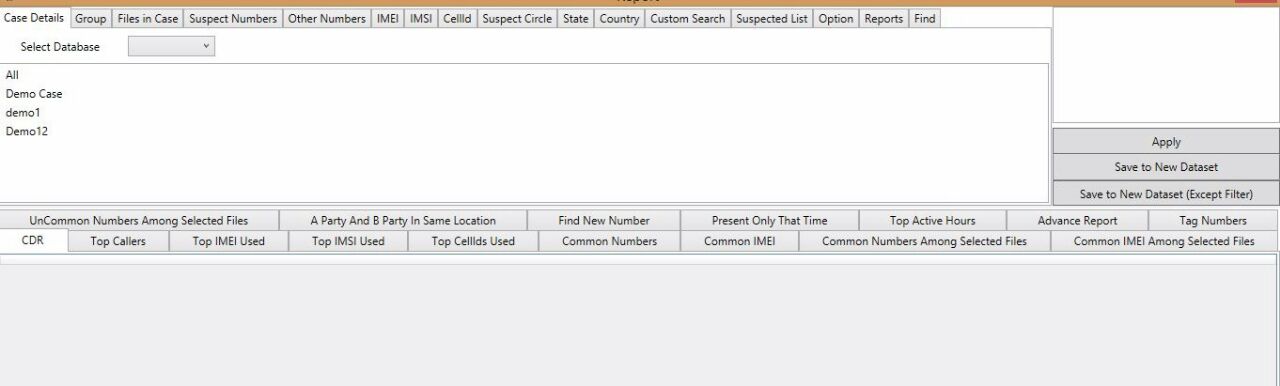


Fig. CDR Analysis Tool

**5.3 CASE STUDY:**

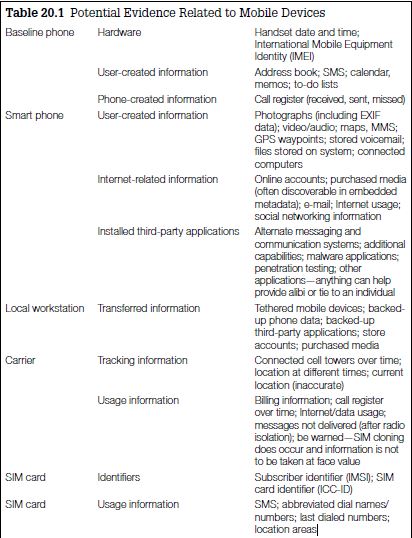
A fake website Job Fraud case recently was solved by Mr. Sudhir (Inspector Cyber cell Gurgaon) with complete dependence on CDR. As the web site was developed by a innocent developer, who just have a cell no. of the culprit. The no. was switched off. When the CDR was analyzed and the shopkeeper of the shop from which the SIM was purchased was investigated, police got the B party which was girl (friend of the culprit), CDR of this girl helped in getting to the culprit who was continiously changing cell phones.

**7**. **MOBILE DEVICE FORENSICS**

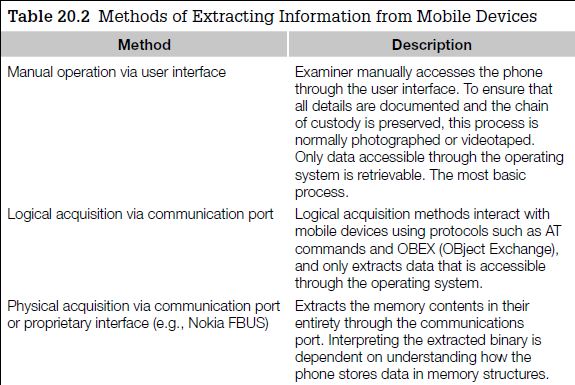
Mobile devices are dynamic systems that present challenges from a forensic perspective. Additionally, new models of phones are being developed globally, with some experts postulating that fi ve new phone models are released every week (Jones, 2008). The growing number and variety of mobile devices makes it difficult to develop a single process or tool to address all eventualities. In addition to a growing variety of smart phones and platforms including Android

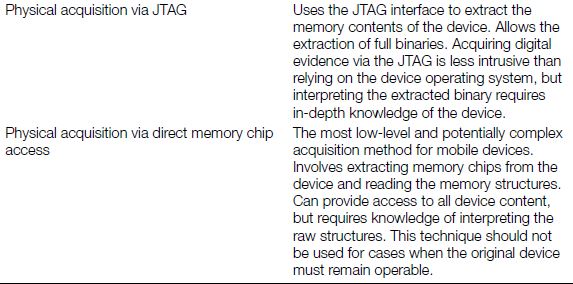
systems, Blackberry, Apple iPhone, and Windows Mobile, there are a massive number of low-end phones using legacy OS systems. Furthermore, there are some unique considerations when preserving mobile devices as a source of evidence. Most mobile devices are networked devices, sending and receiving data through telecommunication systems, Wi-Fi access points, and Bluetooth pioneers. Digital evidence in mobile devices can be lost completely as it is susceptible to being overwritten by new data or remote destruction commands it receives over wireless networks. Additionally, in order to extract information, it is necessary to interact with the device, often altering the system’s state. As with any computer, interacting with a mobile device can destroy or alter existing evidence.

However, a major advantage of mobile devices from a forensic perspective is that they can contain deleted information even after an individual has attempted to render it unrecoverable. The underlying reason for this persistence of deleted data on mobile devices is in the use of Flash memory chips to store data. Flash memory is physically durable against impact, high temperature, and pressure, making it more difficult to destroy. In addition, Flash memory has a limited number of writes and can only be erased block-by-block, and mobile devices generally wait until a block is full before erasing data. Furthermore, mobile devices use proprietary wear leveling algorithms to spread write/erase across Flash memory blocks, which can result in deleted data remaining for some time while new data are written to less used portions of memory. In order to access and recover older/deleted copies of data, it is necessary to acquire a full copy of physical memory.



**6.1 DIGITAL EVIDENCE ON MOBILE DEVICES**





**6.2 EVIDENCE FORENSIC TOOLS**

Forensic tools are in constant development to provide a convenient meansof extracting specifi c data from various mobile devices, typically logically viacable, infrared, and Bluetooth or physically via cable or JTAG. All of these tools function in a similar way, sending commands to the phone and recording responses that contain information stored in the phone’s memory. The

information that can be extracted using these methods depends on both the connection mechanism and model of the phone.Logical mobile phone acquisition systems interact with the phone operating system to extract data, much in the same way the vendor synchronization

systems do. As such, there are limitations to the information retrievable, and only information relevant to the Operating System is available. As such, information potentially relevant in a forensic investigation might not be acquired; information such as deleted items won’t be extracted. Mobile phones generally have a baseline of extractable data from such tools; phone

address book, call register, SMS and photographs, but additional information is not guaranteed.

The limitation to these forms of applications is that it relies on the assumption that the desktop application and the investigator are assuming that the phone’s logic is not making any changes to other areas of the phone’s memory.

However, this assumption cannot be verified without the source code and circuit schematics of the phone’s software and hardware, which are rarely, if ever, publicly available.

There are several commercial forensic tools specifically designed to acquire data from mobile phones. This section introduces some of the more popular commercial tools. Micro Systemation XRY (http://www.msab.com) is one of the market leaders in mobile device acquisition. Micro Systemation sell products to capture mobile phones and other small-scale devices logically via USB, infrared, and Bluetooth. XRY also has an additional component, XACT, that expands capability by performing physical acquisition via the JTAG interface. XACT also allows for the acquisition of specific models of GPS receiver. Cellebrite Universal Forensic Extraction Device (UFED) (http://www.cellebrite.com) is a self-contained, portable mobile phone logical acquisition device. The system is self-powered and copies data to a USB disk or to a second phone. Cellebrite UFED was designed in Israel. Cellebrite also have an additional component,

UFED Physical Pro, that allows physical acquisition of mobile phones and other small-scale devices. UFED systems are also available in a field-ready ruggedized form.

LogicubeCellDEK (http://www.logicubeforensics.com) is a system designed to acquire data from mobile phones and other small-scale devices such as GPS receivers. CellDEK conducts logical extraction of data via USB, infrared, and Bluetooth. MOBILedit! Forensic (http://mobiledit.com) is another logical data acquisition tool. MOBIL edit! Forensic can be purchased as a software-only tool or as part of a kit including cables and infrared reader.

**6.3 FORENSIC EXAMINATION AND ANALYSIS OF MOBILE DEVICES**

The purpose of performing a forensic examination is to find and extract information related to an investigation, including deleted data. Whether data from a mobile device was acquired logically or physically, the general examination approach is the same as outlined in Chapter 6.

■Survey the available items to become familiar with the main sources of information on the mobile device.

■Recover any deleted items including fi les, SMS messages, call logs, and multimedia.

■Harvest metadata from active and recovered items such as date-time stamps, fi le names, and whether messages were read and calls were incoming, outgoing, or missed.

■Conduct a search and methodical inspection of the evidence, including keyword searches for any specifi c, known details related to the investigation.

■Perform temporal and relational analysis of information extracted from memory, including a timeline of events and link chart.

■Validate important results because even forensic tools have bugs.

**7. TECHNICAL RESEARCH & DEVELOPMENT**

Mobile phone tracking is the ascertaining of the position or location of a mobile phone, whether stationary or moving. Localization may occur either via multilateration of radio signals between (several) cell towers of the network and the phone, or simply via GPS. To locate a mobile phone using multilateration of radio signals, it must emit at least the roaming signal to contact the next nearby antenna tower, but the process does not require an active call. The Global System for Mobile Communications (GSM) is based on the phone's signal strength to nearby antenna masts.

The location of a mobile phone can be determined using the service provider's network infrastructure. The advantage of network-based techniques, from a service provider's point of view, is that they can be implemented non-intrusively without affecting handsets. Network-based techniques were developed many years prior to the widespread availability of GPS on handsets.

A GSM Cell ID (CID) is a generally unique number used to identify each Base transceiver station (BTS) or sector of a BTS within a Location area code (LAC) if not within a GSM network.

In some cases the first or last digit of CID represents cells' Sector ID

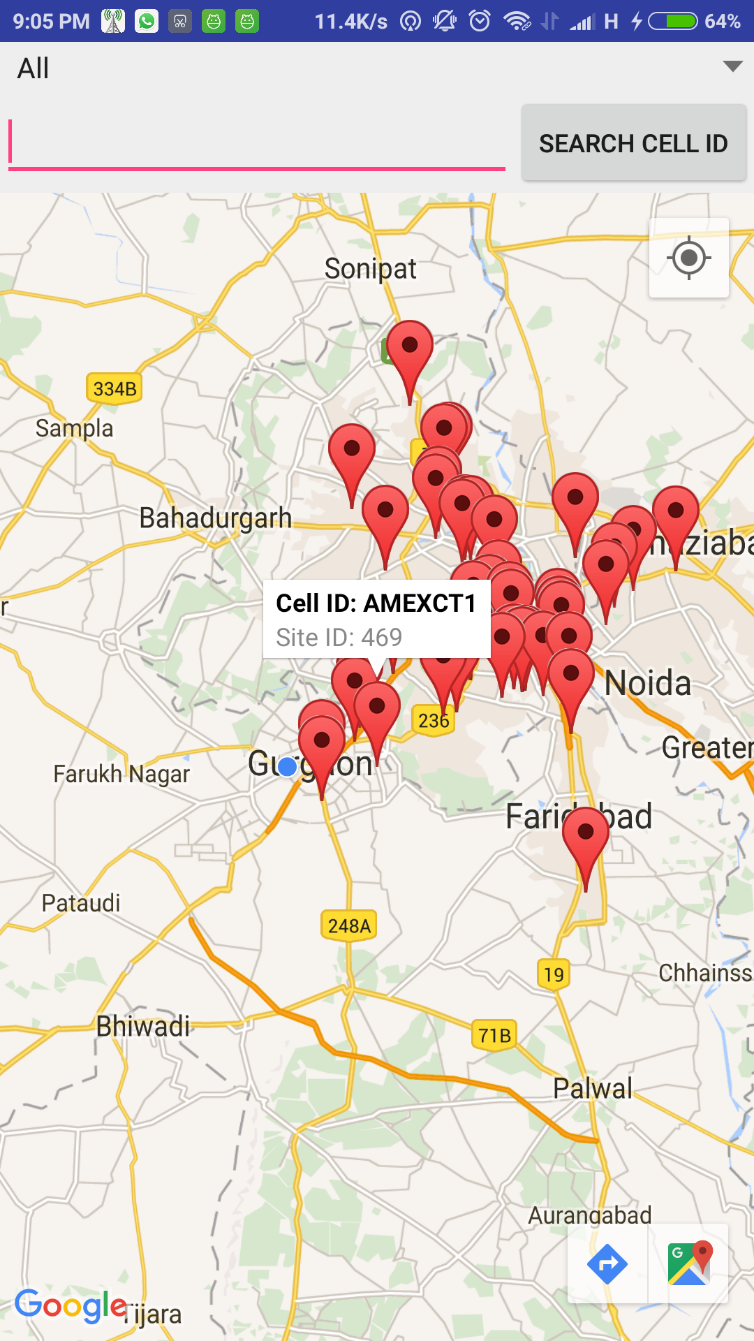
value 0 is used for omnidirectional antenna.

values 1,2,3 are used to identify sectors of trisector or bisector antennas.

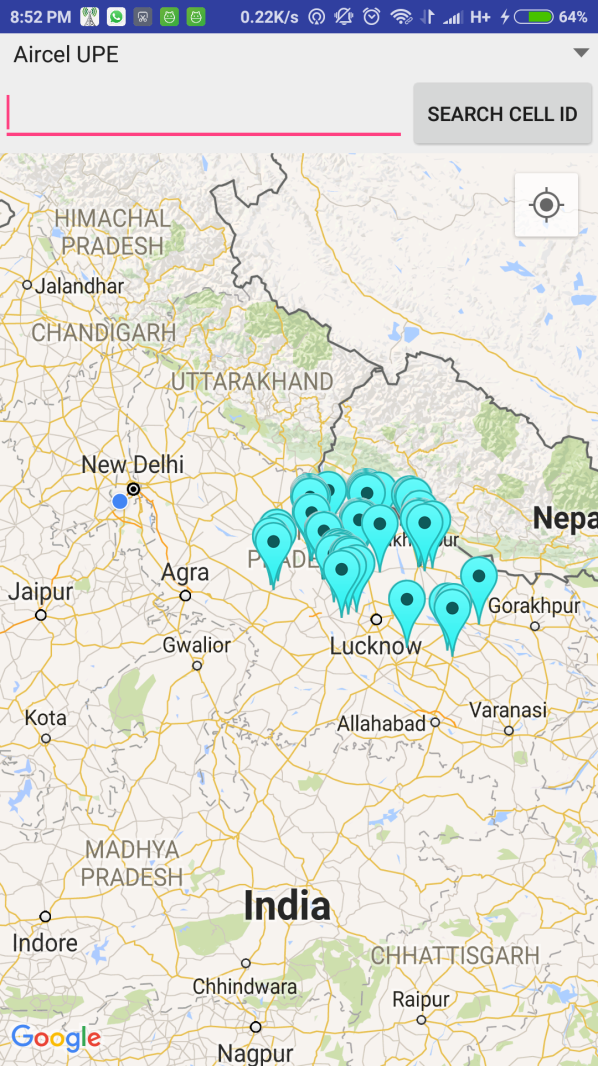
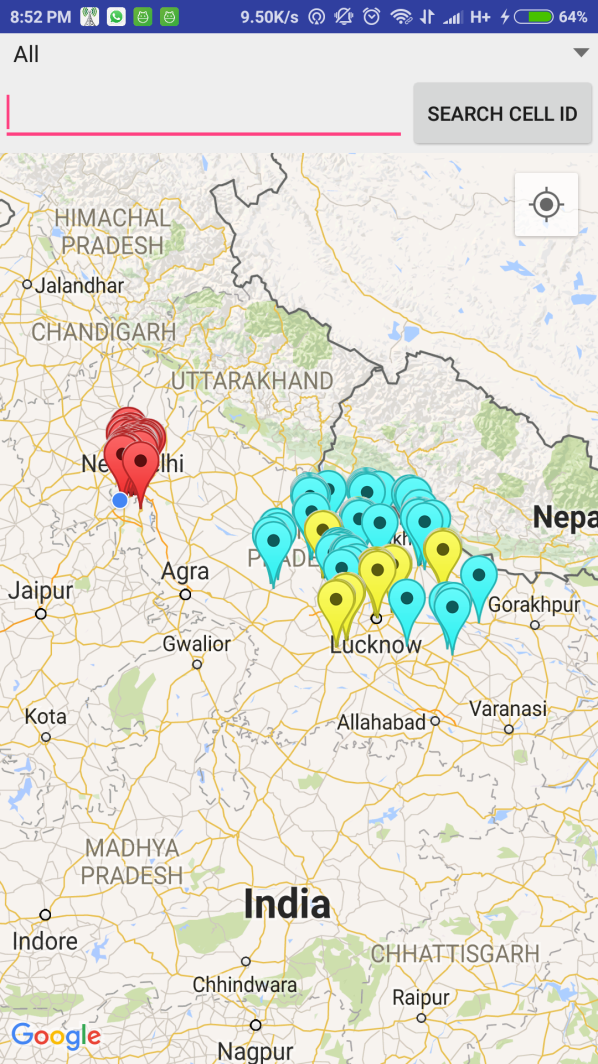
**7.1 OUR APP: TOWER MAP**

The basically focuses on the location of cellular towers of various GSM network providers. The app has marked tower location on the map along with its CELL ID and SITE ID, which would help in tracing the criminal movement. The app also provides the navigation method to navigate to that particular tower.

When the app first opens, it changes the focus to the device location. The nearby towers can be seen on the map. Tap on any of the marker will pop-up the window displaying the Cell ID and Site ID

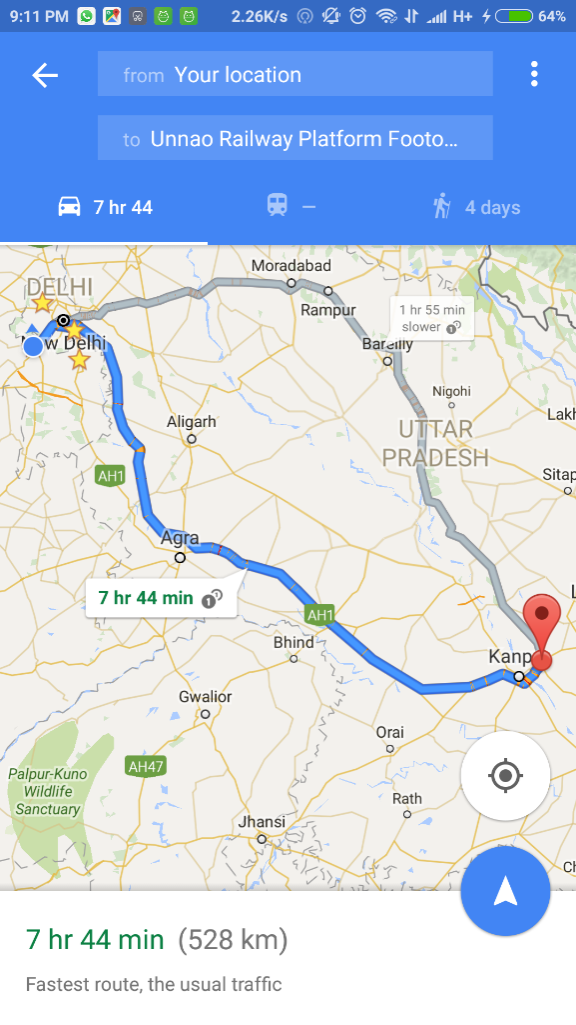


Two search options are present to narrow down the results:

1. Search by Network
2. Search by Cell ID
3. The search by Network displays all the towers with the selected network, making other network’s tower to disappear.
4. Search by Cell ID: This is a very important search method, to search the particular tower from the known Cell ID.



Can navigate to that selected tower location by clicking the arrow button at the bottom



\*The above screenshots were taken at real-time by a real android device Xiaomi Redmi Note 3

1. **HOW TO PROTECT YOUR DEVICE ??**

**Use secure Wi-Fi.**

While this won't stop you from navigating to an infected website, using password-protected Wi-Fi connections keeps unwanted third parties from snooping or carrying out man-in-the-mobile attacks between your device and your intended Web destination.

**Watch your email**

The devices may have changed, but the threat remains the same: Many attackers still rely on malicious email attachments to infect your phone or tablet. Don't click on links in email and other messages, as these may direct you to phishing or malware websites — this applies to all mobile platforms.

**Be consistent**

Only download apps from trusted sources. This ensures that the apps are legitimate and not havens for mobile malware.

**Install antivirus protection**

Antivirus and anti-malware solutions are now popping up for mobile devices; install one from a trusted source, then run it regularly to ensure your device is clean. Also, watch out for malware masquerading as virus protection: only download legitimate apps from trusted sources.

**Don't jailbreak or root your device**

Doing so increases your risk of infection from untrusted third-party sources. Stay rooted and benefit from automatic security updates and patches.

**CONCLUSION**

As the need of mobile phones are increasing day by day it become important to secure our mobile phones .In our project our team developed an app that is helpful for us to get the location of the crime using this app . Here we are able to search by cell id also .But this app is still applicable to only a particular area. So in future we enhance this app for multiple areas. It is very important to secure our mobiles because it includes our personal information and credential information like bank information and data present in Google drive such as photos, videos etc. Hence ,it is concluded that it is very crucial problem for our nation. Hence we should make security tools to prevent us from Mobile crimes.