

## An Improvised Methodology to Unbar Android Mobile Phone for Forensic Examination

V. Balajichandrasekhar M<sup>1</sup>, T. Srinivasa Rao<sup>2</sup>, G. Srinivas<sup>3</sup>

<sup>1,3</sup>Department of Computer Science and Engineering, Aditya Institute of Technology and Management, India

<sup>2</sup>Department of Computer Science and Engineering, GITAM University, India

---

### Article Info

#### Article history:

Received Dec 12, 2017

Revised Feb 13, 2018

Accepted Apr 9, 2018

#### Keyword:

Analysis tools

Mobile device analysis

Mobile forensics

Mobile phones

Smart phone

---

### ABSTRACT

At the end of 2015, there were 4.7 billion noteworthy mobile subscribers globally, equivalent to 63% of the world's population. Mobile phones had all the essential components or characteristics neatly fitted into a small space and designed to achieve high speeds, massive storage, and increased functionalities. Smart phones used to carry out imparting or exchanging of information such as calling, texting, Internet browsing, e-mail, photos, videos, and etc. Criminals can use smart phones for a number of activities. Namely, committing a fraud over e-mail, harassment via text messages, drug trafficking, child pornography, etc. In this research paper, We demonstrate, if a mobile phone is identified in a criminal activity and if it is locked by any one of the locking mechanisms such as pattern lock, PIN lock and password lock, then how to unlock the mobile device without data loss for forensic examination. It is a great challenge for forensic experts to extract data from a mobile phone for forensic purpose that can be used as evidence in the court of law. The experimental results show that our approach can break all kinds of pattern locks.

Copyright © 2018 Institute of Advanced Engineering and Science.  
All rights reserved.

---

### Corresponding Author:

G. Srinivas,

Department of Information Technology,

Anil Neerukonda Institute of Technology and Sciences,

Visakhapatnam 530045, Andhra Pradesh, India.

Email: gsrinivas.it@anits.edu.in

---

## 1. INTRODUCTION

Mobile phone forensics is the branch of digital forensics and it is the application of technological methods used to discover and examine the fact of mobile phone data. The Android operating system is currently the most widely used smart phone OS, with a market share of 85% as of the first quarter of 2017 [1]. When the Android users increases, then the potential for evidence of crimes to be stored on Android devices also increases [2]. This gives a clear indication that the mobile phone forensics used for extracting and analyzing evidential data from Android mobile devices. If the mobile device is identified in a criminal activity and if it is locked then it is a difficult task for the mobile phone forensic investigator to unlock the mobile device and extract the data from it, because, Now a day, Mobile phone had different types of screen lock mechanisms, like swipe lock, PIN lock, pattern lock, fingerprint lock, etc. Pattern lock is widely used on Android devices to protect sensitive information. It is preferred by some users over PIN or text-based passwords, as psychology studies show that the human brain remembers and recalls visual information better than numbers and letters [3]. According to a recent study, 40% of the Android users use patterns to protect their devices instead of a PIN [4]. In this paper, we demonstrate how to unlock the mobile device without data loss for forensic examination by using various methodologies. The first step in the forensic exploration is to enter into the Mobile phone by unveil the locked screen by removing the PIN lock, it has been shown in Figure 3, removal of password lock has been shown in Figure 4, and without removal of

pattern lock how to unlock the mobile device has been shown in Figure 6, Figure 7 and Figure 8. The experimental results shows in the Table 1, indicates that an equivalent hash key value and gesture key value obtained for different pattern locks by an improvised methodologies described in this research paper.

## 2. RESEARCH METHOD

Having an established forensic environment prior to begin the examination, it is important as it determines that the data is protected. This paper covers the requirements that should be in place to start a forensic investigation of an Android mobile device. Android SDK furnish the tools that can be of great help during analysis and examination of the mobile phone. During forensic investigation, the SDK helps to connect to and address the data on the Android device. Now a day, the users can easily lock Android mobile phone by the usage of screen lock options. So that bypassing the mobile phone screen lock during investigation is crucial. Android mobile device offers different types of screen lock mechanisms, those are: 1. Pattern, 2. PIN, 3. Password, 4. Fingerprint, etc. There are several techniques to unbar an Android mobile phone: 1. Recovery Login, 2. Aroma File Manager, 3. Rooting and ADB, 4. Unbar the pattern lock without removing the pattern.

### 2.1. Recovery login

- a. Enter the wrong lock screen five times, and then a pop up window will appear and be patient for some time as displayed the screen and make an attempt.
- b. If you have the backup PIN, then press the backup PIN option and enter the four digit PIN. Then Phone will be unlocked.
- c. If you are not having the backup PIN then select the forget password. Make sure the mobile data is enabled and then enter registered google mail id and password to that phone, and then phone will be unlocked.

Drawback: If the mobile data or Wi-Fi is not enabled. Then this technique may not work.

### 2.2. Aroma file manager

- a. "Copy the Aroma File manager ZIP file from the internet" [5].
- b. After download, copy it into the mobile phone's secure digital card, and insert the secure digital card into the mobile phone and lock it.
- c. Make sure the mobile phone is completely shut down. And clench the correct keys to boot the device into recovery process. For Samsung Galaxy Duos 2 GT-S7582 device, hold down the Volume Up button and Home button and Power button.
- d. Release the buttons when the device is powered on. Clench the buttons for some seconds. Now it is in the recovery mode.
- e. Clench the volume up and down keys to move up or down along with menu choices and select install ZIP from secure digital card. Now press the power button and confirm your selection. Now specify the location to install 'aroma file manager' from secure digital card. Subsequently open 'aroma file manager' again.
- f. Open the data folder and then system folder and observe the gesture or password file for pattern or passwords lock. Then remove whichever file and restart the mobile device.
- g. After reloaded the android operating system, if you identify that the password or pattern lock is not destroyed, then don't panic, just produce whichever the pattern, then mobile phone will be open.

### 2.3. Rooting and ADB

Rooting means modify a Mobile phone device to remove restrictions imposed by the manufacturer or operator and allow installation of unauthorized software, remove unwanted bloat ware, enhance the operating system, replace the firmware, run the processor of the device at a speed higher than that intended (over clock) or modifying device circuit timing settings at a lesser clock rate as is specified (under clock) and customize anything and so on. Rooting around in Mobile phone core software might look like a set of instructions for preparing a particular dish. If any interruption happens while doing rooting then the Mobile phone become completely unable to function. It can also void the warranty. Routing introduces an unspecified amount of security risks. It could create security vulnerability and malware gain access of rooted status to steal data.

### 2.3.1. Construct a root

First thing is to backup everything and determine that the device is fully charged prior to start. Turn on USB Debugging. To do that, open Settings on the device. If the Developer Options is not visible then go to the last portion of settings then, proceed the steps to start.

- a. Press on About Phone and observe the Build Number.
- b. Press on the build number seven times then developer option will appear on the screen.
- c. Press on the back key to observe the developer options.
- d. Press on developer option.
- e. Inspect to grant USB debugging.

### 2.3.2. How to root Samsung Galaxy S Duos 2 GT-S7582 with iRoot.

Step 1 : Install Samsung USB Driver [6].

Step 2 : Allow USB Debugging on Mobile phone. To allow USB debugging: open Settings and then Developer Options and then USB Debugging and then Check to enable.

Step 3 : Download and install iRoot application [7].

Step 4 : once iRoot application is installed, then open it.

Step 5 : Once iRoot application is started then connect mobile phone to computer.

Step 6 : Press the root button to start rooting procedure.

Step 7 : The application automatically reboot the mobile phone.

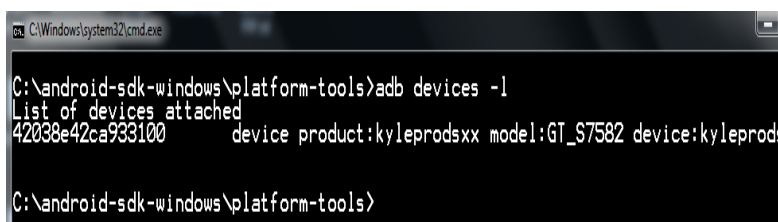
Step 8 : It is rooted.

### 2.3.3. Android debugging bridge (ADB)

The ADB is used to build a viaduct between computer and mobile phone. This can be used to unbar the device and to retrieve the data. This process will only toil if you have authorized USB debugging on Android mobile phone.

- a. Copy the Android SDK package [8] on your computer from internet. When once copied, then draw out the zip file on computer.
- b. Copy the pertinent USB drivers for mobile phone [5]. Obtain the USB drivers for mobile device from manufacturer's website.
- c. Open the command prompt on computer and alter the directory to where the ADB file is situated. Type the following command in the command prompt. C:\android-sdk-windows\platform-tools
- d. Attach the mobile phone to computer by utilizing a USB cable and type the following command. C:\android-sdk-windows\platform-tools> adb devices -l

If mobile phone is identified, then observe serial code (42038e42ca933100), phone model (GT-S7582), device product (Kernel: kyleprodsxx) in the command prompt message. Then list of devices attached to the computer will be shown in Figure 1.



```
C:\Windows\system32\cmd.exe
C:\android-sdk-windows\platform-tools>adb devices -l
List of devices attached
42038e42ca933100    device product:kyleprodsxx model:GT_S7582 device:kyleprods
C:\android-sdk-windows\platform-tools>
```

Figure 1. Displays the list of attached devices

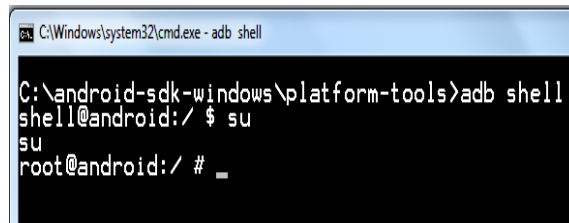
Now enter the subsequent command to eliminate the pattern lock.

```
C:\android-sdk-windows\platform-tools> adb shell
```

```
shell@android:/ $ su
```

su (short for substitute user, super user, or switch user) is usually the straightforward and most appropriate to alter the possession of a login session to root.

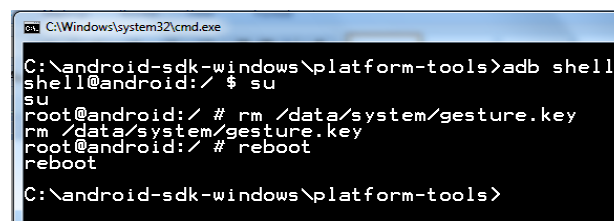
Figure 2 shows the login session as a root.



```
C:\Windows\system32\cmd.exe - adb shell
C:\android-sdk-windows\platform-tools>adb shell
shell@android:/ $ su
su
root@android:/ # _
```

Figure 2. Login Session as a root

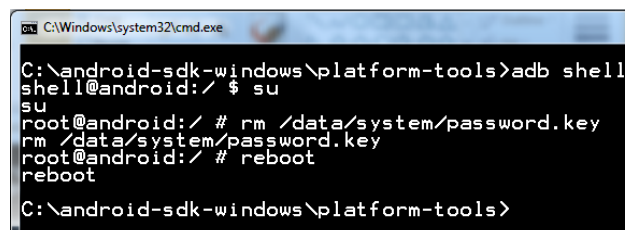
The pattern lock is a medium security mechanism. The drawn pattern is stored in gesture.key file. This file is available in /data/system directory. To remove it then type the following command. root@android:/ # rm /data/system/gesture.key



```
C:\Windows\system32\cmd.exe
C:\android-sdk-windows\platform-tools>adb shell
shell@android:/ $ su
su
root@android:/ # rm /data/system/gesture.key
rm /data/system/gesture.key
root@android:/ # reboot
reboot
C:\android-sdk-windows\platform-tools>
```

Figure 3. Removing the gesture.key

After removing the gesture.key then restart the mobile device by using reboot command. After restarted the mobile device, still it shows draw pattern lock then don't panic just draw any random pattern to unbar the device. If it is a password protected, to eliminate the password then use the following command: root@android:/ # rm /data/system/password.key



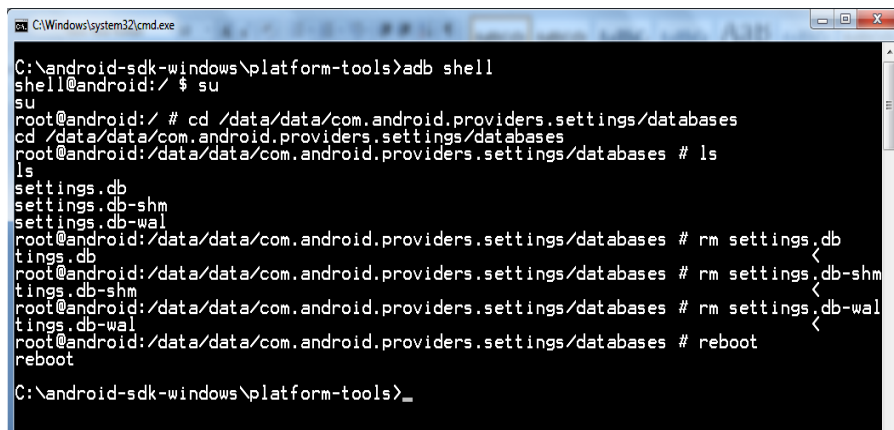
```
C:\Windows\system32\cmd.exe
C:\android-sdk-windows\platform-tools>adb shell
shell@android:/ $ su
su
root@android:/ # rm /data/system/password.key
rm /data/system/password.key
root@android:/ # reboot
reboot
C:\android-sdk-windows\platform-tools>
```

Figure 4. Removing the password.key

After removing the password.key then restart the mobile device by using reboot command. This time the mobile will directly starts without prompt any popup screen on the device. This method works when the device is rooted. If the above procedure is not worked properly then follow the instructions to remove the lock.

1. Connect the mobile phone to the computer using the USB cable.
2. Open the command prompt as said earlier and type the following commands
  - a. C:\android-sdk-windows\platform-tools>adb.exe shell
  - b. shell@android:/ \$ su
  - c. root@android:/ #
  - d. root@android:/ # cd /data/data/com.android.providers.settings/databases
  - e. root@android:/ /data/data/com.android.providers.settings/databases # rm settings.db
  - f. root@android:/ /data/data/com.android.providers.settings/databases # rm settings.db-shm
  - g. root@android:/ /data/data/com.android.providers.settings/databases # rm settings.db-wal
  - h. root@android:/ /data/data/com.android.providers.settings/databases # reboot

Figure 5 shows the removing the settings to unlock the device.



```

C:\Windows\system32\cmd.exe
C:\android-sdk-windows\platform-tools>adb shell
shell@android:/ $ su
su
root@android:/ # cd /data/data/com.android.providers.settings/databases
cd /data/data/com.android.providers.settings/databases
root@android:/data/data/com.android.providers.settings/databases # ls
ls
settings.db
settings.db-shm
settings.db-wal
root@android:/data/data/com.android.providers.settings/databases # rm settings.db
rm settings.db-shm
root@android:/data/data/com.android.providers.settings/databases # rm settings.db-wal
rm settings.db-wal
root@android:/data/data/com.android.providers.settings/databases # reboot
reboot
C:\android-sdk-windows\platform-tools>_

```

Figure 5. Removing the settings to unlock the device

3. Now the Android mobile phone would be unlocked.

#### 2.4. Unbar the pattern lock without removing the pattern

This method will work on the rooted mobile phone. In this method, first identify the `gesture.key` which is available at `/data/system` directory. To see the file, type the following command.

```
C:\android-sdk-windows\platform-tools>adb shell
```

```
shell@android:/ $ su
```

```
su
```

```
root@android:/ # cd /data/system
```

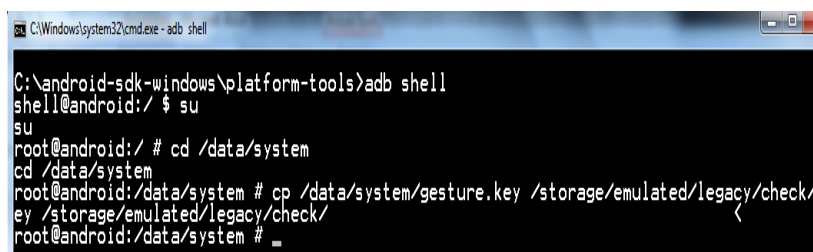
```
cd /data/system
```

```
root@android:/data/system # ls
```

Afterwards, create a folder in the phone memory, all the files in phone memory are available at `/storage/emulated/0`. I have created a folder called `check` in phone memory. Now copy the `gesture.key` into the `check` folder as shown in below.

```
root@android:/data/system # cp /data/system/gesture.key /storage/emulated/legacy/check/
```

```
root@android:/data/system #
```



```

C:\Windows\system32\cmd.exe - adb shell
C:\android-sdk-windows\platform-tools>adb shell
shell@android:/ $ su
su
root@android:/ # cd /data/system
cd /data/system
root@android:/data/system # cp /data/system/gesture.key /storage/emulated/legacy/check/
ey /storage/emulated/legacy/check/
root@android:/data/system # _

```

Figure 6. Copy the gesture.key into phone memory

When you are copying the `gesture.key` into the `check` folder, here you can observe the path, even though `check` folder is available at `/storage/emulated/0` in the phone memory, you should use `legacy` instead of `0` in the path. Now, copy the `gesture.key` from phone memory to computer. Download hexadecimal editor [9] from the internet. Open the file `gesture.key` in hexadecimal editor.

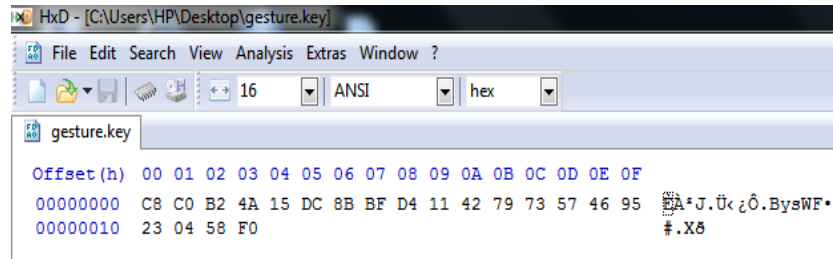


Figure 7. Hexadecimal values of gesture.key

Now, Copy the hexadecimal values alone into the notepad and remove the whitespace among the hexadecimal numbers. Now it looks like this: C8C0B24A15DC8BBFD4114279735746952304580 Afterwards, open the URL: <https://barney.0x539.se/android/> copy the hexadecimal values into the text box and press Get gesture button. Now, entered hash value and gesture key will appear. If you want to see graphical image of the pattern then press Show pattern button. Now use this gesture key to remove the lock of the mobile device.

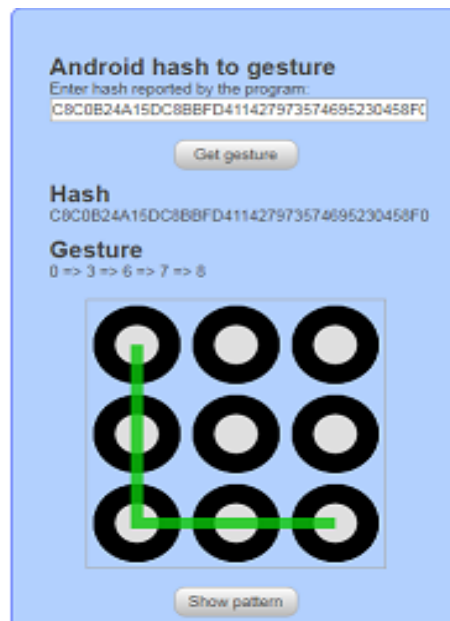


Figure 8. Gesture value and Gesture pattern of Hash Value

### 3. EXPERIMENTAL RESULTS

In this section we present the results obtained by the experiments, the following table summarizes the test results on each test scenario conducted. The test results shows the hash key value and gesture key value of every pattern lock obtained by using an improvised methodologies described in this paper. The hash key value that can be retrieved from the gesture.key file which is located in /data/system directory of the mobile device. The hash value of every pattern that can be tested in the URL: <https://barney.0x539.se/android/>, and obtained the original pattern image. Experimental Results are shown in the Table 1.

Table 1. The Experimental Results of the Pattern, its Hash Value and its Gesture Value

S.No	Pattern lock of a Mobile Phone	Hash key value of pattern lock	Gesture key value of pattern lock
1		A888A56833FF60643925060570552C014BA5AB3D	0345876
2		55570D99B4A7F37B70F2FC924C1846D96FAD0872	034125876
3		F56A6DF0A85F5B0EB1E661B5836ED423542AFA86	6304258
4		2534B1871033318B4FCA4F0AA64C1FF3BAACE4EF	642103
5		23A6E7C835CD75C3F17ECC4D1CD7D840B7409525	210345876
6		2A18C270EB0B29DB51C83A1D2E83F065359D7D1D	036412587
7		47B29DFFAFFB440432A06A97FC11EB4D33530EE4	7301254
8		83F1C27066ECD75EF81924DA5A59A A95AE952F3	87301254
9		FE6AE2C2B76B4971829744BC22E9A5EDB1EB9D87	854367
10		310DA79611A19C5A3F96A1A68FE33EC32834C364	5412
11		8965029F578413B95C6B35CFE25F73359CE4189D	210367458
12		BBEBB2E286A6755150B76F23013C7F1057A806A0	412587630
13		68CB3F46EBD8BCCFF419F66E8AB45B25F0F5FCFE	30147852
14		1B1394BAA3D3828F558C1545159B4D03EA93A76C	14367852
15		3F0B02C8E728DFB4E6902E9480523DF66F42B7AA	125478
16		FAE5DF05B1DF6088069D45C6C300F717BAE368EF	3452103678
17		0EF98B4A77CBCBDB6A02A0DD5A64525C35E2F2FF	4587630
18		6836E6F7003CC83B10E465C0E99F51692000CB53	587630124
19		143175B8D9BE9B4BCB125D9EF856DEC1F5087B42	74521036
20		F20A8DE7883A1870A72BCA45C26BC2CF96B7C140	03452476

#### 4. CONCLUSION

An appropriate setup is essential before conducting investigations on an Android mobile phone. If forensic acquisition needs the android device to be unlocked, then find out the best method to obtain access to the mobile phone. The diverse screen lock bypassing techniques discussed in this paper that help the examiner to bypass the pass code under different circumstances. Depending on the forensic acquisition method and scope of investigation, rooting the device should provide complete access to the files present on the mobile phone.

#### REFERENCES

- [1] Smartphone OS: Market Share, 2017 Q1 from <https://www.idc.com/promo/smartphone-market-share/os>.
- [2] Martin B., *et al.*, "Conceptual evidence collection and analysis methodology for Android devices," *Syngress, an Imprint of Elsevier*, pp. 285-307, 2015.
- [3] A. D. Angeli, *et al.*, "Is a picture really worth a thousand words? exploring the feasibility of graphical authentication systems," *Int. J. Hum.-Comput. Stud.*, 2005.
- [4] D. V. Bruggen, "Studying the impact of security awareness efforts on user behavior," Ph.D. dissertation, University of Notre Dame, 2014.
- [5] Aroma File Manager Software, [forum.xdadevelopers.com/showthread.php](http://forum.xdadevelopers.com/showthread.php) Web site. Retrieved September 27, 2017, from <https://forum.xdadevelopers.com/showthread.php?t=1646108>.
- [6] Samsung USB drivers software, [androidmtk.com](http://androidmtk.com) Web site. Retrieved September 10, 2017, from <https://androidmtk.com/download-samsung-usb-drivers>.
- [7] iRoot Software, [androidmtk.com](http://androidmtk.com) Web site. Retrieved September 27, 2017, from <https://androidmtk.com/download-iroot-application-all-versions>.
- [8] Android Studio Software, [developer.android.com/studio](http://developer.android.com/studio) Website. Retrieved September 25, 2017, from <https://developer.android.com/studio/index.html>.
- [9] HxD Editor Software, [download.cnet.com](http://download.cnet.com) Web site. Retrieved September 27, 2017, from [http://download.cnet.com/HxD-Hex-Editor/3000-2352\\_4-10891068.html](http://download.cnet.com/HxD-Hex-Editor/3000-2352_4-10891068.html).

#### BIOGRAPHIES OF AUTHORS



**V BalajiChandraSekhar M** received the Bachelor's degree in Engineering (CSIT) from Sree Vidyanikethan Engineering College, Tirupati, AP, India, in 2001, and the Master's degree in Engineering (CST) from the Andhra University, Visakhapatnam, AP, India, in 2007. He is currently working as a Associate Professor in Aditya Institute of Technology and Management (AITAM), Tekkali, Srikakulam. His research interests include Mobile Forensics, Data Analytics, Compiler Design, Object Oriented Programming, and Web Technologies. He is a Sun Certified Java Professional. He has published numerous conference proceedings as well as papers in international journals.



**Dr. T. Srinivasa Rao** received the B.Tech. degree from GITAM ,Andhra University, Visakhapatnam, Andhra Pradesh, India. Received the M.Tech. degree in Andhra University, Visakhapatnam, Andhra Pradesh, India. Received the Ph.D. degree in Andhra University, Visakhapatnam, Andhra Pradesh, India. He is currently working as a Associate Professor, Department of CSE, Gitam Institute of Technology, Gitam University, Visakhapatnam. His research interest includes wireless communication (WiFi,WiMax), Mobile Ad hoc networks, Sensor Networks, Neural Networks and fuzzy logic, Communication networks, Data mining, softwareengineering, Machine learning.



**G. Srinivas**, Received M.Tech Degree From Andhra University In 2007, and P.hd. Degree from Andhra University In 2012 Is Currently Working As An Associate Professor In ANIL Neerukonda Institute of Technology and sciences In the Department Of Information Technology .He has overall 15 Years of teaching experience. His Area Of Interest Includes Image Classification, Compression, and Enhancement.