A novel approach for forensic acquisition and analysis of Android mobile devices

C. Rajabhushanam[1*], J. Mohanraj[2]

[1]Dept. of Computer Science & Engineering, Bharath Institute of Higher Education & Research, Chennai, Tamilnadu

[2]Department of CSE, Bharath Institute of Higher Education & Research, Chennai, Tamilnadu

***Corresponding author: E-Mail: rajabhushanam_c@gmail.com**

ABSTRACT

Android is an operating system (OS) developed by the Open Handset Alliance (OHA).Android Smartphone having rich set of features such as emailing, chatting, gaming, video/audio players, pdf readers, advanced computing capabilities and much more. We can undelete the deleted files and retrieve those files from internal storage where all the mobile data stored.It is possible to retrieve the deleted files in Android by this Android Acquisition Tool. In this project, we can retrieve deleted image files in Android device by acquisition (imaging) method.

KEYWORDS: Forensic, Android, Acquisition.

1. INTRODUCTION

Android is a portable working structure (OS) in light of the Linux part and without further ado made by Google. With a customer Interface considering direct control, Android is arranged basically for touch screen PDAs, for instance, phones and tablet PCs, with specific customer interfaces for TVs (Android TV), cars (Android Auto), and wrist watches (Android Wear). The OS uses touch inputs that uninhibitedly identify with veritable exercises, for example, swiping, tapping, pressing, and pivot crushing to control on-screen objects, and a virtual console. Notwithstanding being in a general sense proposed for touch screen information, it has in like manner been used as a piece of diversion consoles, modernized cameras, standard PCs, and distinctive devices. Beginning 2015, Android has the greatest presented base of each and every working game plan of any sort. Android devices have created in extensive rate, an extended recognition with the data they have will comparably create. The dangerous improvement of the stage has been a tremendous win for clients concerning competition and highlights.

On the other hand, criminological investigators and security engineers have battled as there is an absence of learning and bolstered instruments for examining these gadgets. The Thesis tries to address issues not just by giving top to bottom experiences into Android equipment, programming, and record frameworks additionally by sharing methods for the scientific obtaining and ensuing investigation of these gadgets. For peruses with constrained scientific experience, the postulation makes orderly samples that utilization free, open source utilities. A lot of that hobby will originate from digital criminal associations who understand that effective assaults against the stage will yield noteworthy results as the gadgets contain colossal amounts of individual and business data. The answer for this risk requires a profound comprehension of the stage from center Android designers and makers as well as from application engineers and corporate security officers. More secure applications will anticipate loss of touchy data and also solid arrangements that can be placed set up by IT security experts.

Introduction to android devices and android forensics: Google purchased the little organization that created Android working framework, Android Inc., and since its release in 2008, Android gadgets are always expanding their piece of the overall industry. As indicated by Andy Rubin, the senior VP of Google, there are more than 700,000 Android gadgets enacted day by day.

Android was based on the Linux kernel 2.6 and is completely open source (Conti, 2008). Choice to release an open source is Google's methodology which was shocking for some. By doing that Google spares more than twenty percent drop in assembling cost just from the product reserve funds Android gadgets are made by different makers, and its working framework and applications are created by enthusiasts everywhere throughout the World. The primary normal for Android gadgets is its source code accessibility. This is a major downstream with regards to the examination of the gadget by a PC measurable master.

Reality that each producer forms its own particular equipment for the Android gadget does not serve measurable examination of the gadget. With each new model available, scientific master are managing new equipment and programming arrangements executed in the new gadget. Each new model must be analyzed and looked into to begin with, so as to have the capacity to sufficiently react to the examination demands. Hypothetically, each new model of the Android family is another electronic gadget which should be scrutinized keeping in mind the end goal to detail legitimate strategies required for its examination.

Because of the tremendous number of distinctive gadgets, Android legal sciences control is in development. Androids, and the other handheld gadgets, can hold inconceivable data about the clients and their propensities. Criminological examination of the handheld gadget can uncover some fascinating data about the client that can help in an examination. Generally clients feel that the gadget is extremely individual, and that they are the special case who will ever have entry to it. This is the reason that some exceptionally disparaging data could be found on handheld gadgets.

The idea of Android crime scene investigation comprises of strategies to remove the most conceivable information from the gadget without losing, or changing the content of the gadget. Change of the information or information safeguarding is the most serious issue when managing Android gadgets.

The strategy that is most prescribed is live obtaining because of the unstable way of the gadget's memory. Live procurement is prescribed on the grounds that the unstable memory can hold different information which could be of quality for the examination. The samples of information that could be found in the volatile, RAM memory are:

- Passwords
- Encryption keys
- Username
- Application information
- Data from framework forms and benefits

Android forensics challenges: Information in Android gadgets could be put away in a few areas. It could be put away in either NAND flash, the SD card, or the system. Information that could be found in the Android gadgets could be more extensive than the information found in the PCs. A purpose behind picking the NAND Flash memory over alternate sorts depends in its capacities to store huge measure of information in NAND flash memory is non-volatile what's more framework records, it stores a noteworthy segment of client's information. Cases of information found on the Android gadget are:

- Text messages (SMS/MMS)
- Contacts
- Call logs
- Photos/Video
- Web history
- Search history

Information found on the Android gadget while leading live securing can hold data that is unrealistic to discover in other type of obtaining. In this way RAM memory can hold information, for example,

- Passwords
- Encryption keys
- Usernames

Existing components: Removing the memory substance completely through the correspondence port. For MTD gadgets, NAND dump can be utilized to gather NAND information autonomously of the more elevated amount record framework conveyed on the memory. For gadgets that don't utilize MTD, other gathering strategies can be utilized. Case in point, the DD utility can be utilized. It is additionally essential to take note of that not all the information is fundamentally put away in on-board memory. It is required to utilize an unfilled SD card, as for the best practices in legal sciences.

Presently we have a cross-gathered duplicate of nanddump and mtddebug, executable on our gadget. We additionally observe the adaptation of yaffs that is running on our gadget (cat/proc/yaffs). As we probably am aware the mounting purpose of our objective allotment, we can gather some other essential data about it (through cat/proc/mtd). From this, we can perceive how yaffs2 and MTD sort out the NAND flash structure.

```
#cd /sdcard
#./nanddump - o - /sdcard/userdataoobpadbad.nanddump
/dev/mtd/mtd5 -- bb-padbad
```

We additionally create a dump without the OOB range as a percentage of the procedures that we are going to utilize work better without OOB:

```
#./nanddump - /sdcard/userdatapadbad.nanddump/
dev/mtd/mtd5 -- bb-padbad
```

Other than the free applications for consistent extraction of information, various business merchants have the measurable programming those backings Android gadgets. Some of them are:

- XRY
- OXYZEN FORENSIC SUIT
- Cellebrite UFED
- Compelson MOBIL edit

These tools are very expensive and does not support the recent android smart phones released by various manufacturer such as ASUS ZENFONE, XIOMI, SAMSUNG GALAXY S5, S6 etc. Though these commercial does not have the capability to create physical dump or bit-by-bit image of recently released or launched smart android phones.

Proposed components: This tool has the capability to create the bit-by-bit image of the recently launched smart phones. Through this imaging deleted files can be retrieved. To perform forensic acquisition, android devices need to be rooted then only the android device’s primary memory could be accessed. Existing tools have limited accesses to acquire system memory as well as Phone Memory. It has been proposed to develop tools for acquire System and Phone memory for based on Android operating system version. Once, the phone memory acquisition completed then most of the open source tools could be used for pull out / carving out the data or file from the phone memory. Also, malware signatures, web access artifacts, recent file access, user activities and complete time line analysis could be performed from the acquired system memory. This novel approach of acquisition and analysis of android based smart phone devices will yields ultimate results and it may help to resolve the forensic scientists as well as Law Enforcement Agency personnel.

To perform forensic acquisition, android devices need to be rooted, and then only we can access the primary memory of android device. Existing tools have limited accesses to acquire system memory as well as Phone Memory. This project is to taking raw DD images of the various partitions of android devices, such as /data /system and so on. It has been proposed to develop toolkit for acquire Phone memory that is based on the various versions of Android operating system. Automated shell scripts to identify list of existing partition including ‘user data’ partition and perform forensic image of the required partition to the mounted SD card or OTG mounted external drive or forensic workstation. Once, the phone memory acquisition completed then most of the open source tools could be used for pull out / carving out the data or file from the phone memory. Android gadgets are made with SD cards as a kind of capacity gadget to empower clients to effectively move their information: tunes, pictures, recordings and different documents to different gadgets and PCs. The procedure to image the card comprised of essentially evacuating the card and image it utilizing the USB write blocker.

Module description: The deleted records from the android gadgets can be recouped effectively. It should be possible by utilizing the four modules. The modules are

- Phone Detection
- Root
- Acquisition
- Analyze

Phone detection: It is to show the points of interest of mobile, for example, the portable make, model, variant of the android gadget utilized here. Associate the Android gadget with the computer. To perform the physical Acquisition we have to know the Make and Model of the Device. In this automatically it will show the Model of the gadget.

Enabling ADB debugging: Keeping in mind the end goal to utilize adb with a gadget joined over USB, you should empower USB troubleshooting in the gadget framework settings, under Developer alternatives. On Android 4.2 and higher, the Developer choices screen is covered up as a matter of course. To make it obvious, go to Settings >About telephone and tap Build number seven times. Come back to the past screen to discover Developer alternatives at the base.

On a few gadgets, the Developer alternatives screen may be found or named in an unexpected way. When you unite a gadget running Android 4.2.2 or higher to your PC, the framework demonstrates a dialog requesting that whether acknowledge a RSA key that permits investigating through this PC. This security component secures client gadgets in light of the fact that it guarantees that USB troubleshooting and other ADB orders can't be executed unless you're ready to open the gadget and recognize the dialog. This requires you have ADB variant 1.0.31 (accessible with SDK Platform-instruments r16.0.1 and higher) so as to troubleshoot on a gadget running Android 4.2.2 or higher

USB debugging mode: USB Debugging stipends you a level of access to your gadget. This level of access is critical when you require framework level freedom, for example, while coding another application. Then again, there are a couple non-advancement related advantages from this new level of access that can give you a great deal more flexibility of control over your device. USB Debugging Mode can be empowered in Android in the wake of interfacing the gadget straightforwardly to a PC with a USB link. The essential capacity of this mode is to encourage an association between an Android gadget and a PC with Android SDK (programming advancement pack). As the name may propose, Android SDK is a product suite that is intended to help in the improvement of Android applications.

In any case, once more, here's the takeaway: USB Debugging Mode sets up an immediate association between an Android gadget and a PC and prepares it for more profound level activities. That is the essential part. In a few renditions of Android, the USB Debugging Mode highlight may be called Developer Mode. For instance, with Android SDK, you increase direct access to your telephone through your PC and that permits you to do things you typically proved unable, similar to tangle moment screenshots of your gadget or run terminal orders with ADB. These terminal charges can offer you some assistance with restoring a bricked phone–a helpful apparatus for any bold Android proprietor. Without it, you'd need to get a substitution telephone.

USB Debugging is likewise essential on the off chance that you ever need to root your Android gadget. Before an application like One-Click Root can delve into your framework and convey the adventure that roots the gadget, USB Debugging is important to permit that capacity in any case. Consequently, it's best to keep USB Debugging Mode handicapped and just empower it when you truly require it. While running an application, for instance, it'll fill you in regarding whether it needs you to empower the mode before it can do anything. At the point when that happens, you can empower it, let the application do its thing, then cripple it once more. Couple of applications will require your telephone to always be in investigating mode. In conclusion, beginning with Android 4.2, access to the USB Debugging Mode alternative has been covered up naturally. I'm not by any stretch of the imagination beyond any doubt why the improvement group suspected that move was fundamental, however luckily it's not all that quite a bit of a torment to get it obvious.

Root: The establishing is the procedure of getting the administrator energy to get to the gadget. There are a few programming exists to root diverse android mobiles. Establishing is the procedure of permitting clients of cell phones, tablets and different gadgets running the Android mobile working framework to accomplish favoured control (known as root access) over different Android's subsystems. As Android uses the Linux part, establishing an Android gadget gives comparable access to authoritative authorizations as on Linux or whatever other Unix-like working framework, for example, FreeBSD or OS X. Establishing is a procedure that permits you to achieve root access to the Android working framework code. It gives you benefits to alter the product code on the gadget or introduce other programming that the maker wouldn't ordinarily permit you to. Furthermore, for good mobile security reasons: they don't need clients to make changes to the telephones that could bring about mishaps destroyed; it is less demanding for them to offer backing on the off chance that they permit clients to just utilize the same unmodified rendition of the product. Be that as it may, educated clients have officially created establishing systems, which change contingent upon gadget. They are accessible on the web, and more Android clients are falling back on them in light of the effective advantages they give, for example,

- Full customization for pretty much every theme/graphic
- Download of any application, paying little mind to the application store they're posted on
- augmented battery life and included execution
- Overhauls to the most recent rendition of Android if your gadget is obsolete and didn't really redesign by the producer.

Advantages of rooting: "Rooting" your Android telephone affords you various advantages, including;

Running special applications: Super user is an application that must be kept running on a Rooting Android telephone. This permits you to control which applications have admittance to the "root" system. Another prominent application that "establishing" manages is the capacity to tie a PC to your Android telephone so that the PC can get to the Internet utilizing the telephone's information association. Another project can permit your Android to be utilized as a WiFi Hotspot without paying your supplier for the component.

Freeing up memory: When you install an application on the phone, it is stored on the system RAM. "Establishing" permits you to move installed applications to the SD card, consequently arranging for framework memory for extra records or applications.

Custom ROM'S: This is the most capable component of "Rooting" telephones. There are many custom ROM's that can do anything from accelerating the handling rate of your telephone to changing the whole look and feel of your telephone.

Data recovery: Sadly, notwithstanding of continually developing unwavering quality of capacity gadgets, loss of advanced data remains a common phenomenon. Any data spared to a capacity gadget is fortunately quite often recoverable. Be that as it may, you ought to recognize the situations when the data has never been written to a capacity (for instance, made yet not spared report lost because of force disappointment) and therefore is not the slightest bit recoverable. Fortunately, the data that still stays on the capacity can be recuperated to a protected area. Recuperation chances depend much on the information misfortune circumstance itself, yet you ought to consider that no data is recoverable subsequent to overwriting. Consequently you ought to never write anything to the capacity until the last record is recuperated.

Data loss causes: Among the most well-known information misfortune reasons are:

- Accidental erasure of a document or organizer
- File framework design
- Logical harm of a document framework
- Loss of data about parcel
- Storage disappointment

In the event that a disappointment has jumped out at a RAID framework which repetition permits to recuperate information without single stockpiling (one drive disappointment for RAID5, close to two drives disappointment for RAID6 and so forth.), it's conceivable to recoup information without the missing drive.

Information misfortune brought on by record erasure: Any deleted document stays on the capacity until the storage room is re-utilized by other information. After record cancellation OS might re-use plate space at whatever time to store another document. Hence, even minor keep in touch with the capacity might bring about changeless information misfortune. Web program might save so as to bring about overwriting of deleted records also reserve or treats to the capacity. On the off chance that you introduce the product to the same drive, your information are additionally under the danger of overwriting.

Other record frameworks (like FAT) component normal chances for information recuperation. Here just piece of data is pulverized (like data about record parts), yet data about document name, begin estimate still stays on plate. Heuristic calculations still permit "speculating" record sections and recouping great documents. It would be ideal if you remember, that because of absence of genuine data about assignment of record parts any information recuperation programming might neglect to recognize genuine document position, particularly if a few divided records were deleted near the same area on the capacity.

The extent of these elements make any record recuperation programming utilize an arrangement of deterministic and heuristic calculations to figure deleted document area. It would be ideal if you consider that these calculations contrast from merchant to seller making recuperation results vary too.

Recuperation after document framework group: After record framework organize a piece of data on the capacity is obliterated because of overwriting with new data of another document framework. Once more, information recuperation chances after arrangement depend much on the first and new document frameworks. Case in point, if a document framework was organized with FAT, it overwrites tremendous measure of storage room at plate begin with zeros (void square assignment tables) and in this manner devastates any past information. Regardless of the fact that past document framework was additionally FAT, the data about portion of past records will be lost totally. Other document frameworks as a rule dispense more or less structures to diverse stockpiling areas.

Recuperation chances are much subject to unique and new record frameworks. At times recuperation chances are higher if the document framework is organized with the same record framework sort (e.g. NTFS), some of the time - not (e.g. FAT over FAT has more terrible recuperation chances than XFS over FAT).

Effective information recuperation programming for the most part deliver very great recuperation result after record framework group. Most document frameworks (with the exception of those like FAT) may at present keep record distribution data, catalog records, document names and so on that permits to effectively recreate the record framework. On the other hand, subsequent to new structures are written to the disk, some client data can be harmed and a few records or envelopes can be lost.

Deleted files:

Chances for recovery: During the time spent any document erasure, regardless of deliberate or unplanned, the working framework acts to discharge storage room for new records denoting the space utilized by past records as free. Fortunately, the storage room really stays possessed by the past record until the snippet of its overwriting with another one, subsequently leaving would like to recover deleted files. Chances to effectively recuperate deleted documents depend much on the document framework, as every record framework performs distinctively to erase documents. Moreover, you can expand information recuperation chances without anyone else's input in that you pick proficient, protected and solid data recovery software.

Acquisition: It is used to take imaging about the files which is gets deleted from the android device.

Data acquisition procedures: First step is to arrange out the acquisition process. It minimizes the danger of loss or temper of confirmation. It includes planning of apparatuses for gadget examinations. Preparing of individuals includes study and arrangement of different gadgets and data recovery. Second step includes the keeping the tainting and defilement of proofs and security of the wrongdoing scene from unapproved access are the prime worries of this stage. Securing the trustworthiness of the proofs and keep up formal convention for guaranteeing orderly and secure guardianship at the wrongdoing spot. Third step includes keeping up archives, which keeps up the chain of guardianship. Things like the current condition of cellular telephone when simply spotted after the wrongdoing ought to be reported. A record of all noticeable information must which would help in reproducing and incorporate the wrongdoing scene at whatever time amid the examination or say amid an affirmation in the court must be maintained. Fourth step includes keeping up the condition of the gadget in which it is found in. On the off chance that the telephone is in working mode, we have to shield it utilizing a faraday sack. We gather proof from the telephone, later we save and analyze the confirmation. The inspected proof is later sent to investigation of confirmation. After the investigation of proof is finished, the confirmations safeguarded in appropriately made storage spaces. Presentation of entire examination of proofs the last stage in confirmation gathering. Distinctive kind of confirmation incorporates unpredictable memory, non-unstable memory and cloud memory, cell site examination. Non-unstable memory database documents, telephone log records, and so on nonvolatile memory incorporate information put away on RAM, swap spaces.

This segment depicts how the information on an Android gadget can be recovered. In an advanced examination, the essential wellspring of proof is a duplicate of the objective gadget's nonvolatile information. Securing the nonvolatile information is it from a customary hard plate or from NAND powder in a cell phone is known as "posthumous" obtaining, in light of the fact that the information is gathered after the gadget has been controlled off. Posthumous securing is a well-Rooting process, remaining as opposed to live framework procurement, which is a moderately new and rapidly developing procedure, notwithstanding for desktop and PCs. Measurable obtaining of cell phones takes after the same standards as more conventional legal acquisitions, however the devices, systems, and restrictions can be altogether different. The procedure of gaining a framework, whether it be a desktop or a cell phone, is of essential enthusiasm to computerized examiners and episode responders. They regularly hold fast to methods and rehearses that make "forensically-solid" copies. As per Craig Ball,

A forensically-solid copy of a drive is, first and foremost, one made by a strategy which does not, at all, change any information on the drive being copied. Second, a forensically-solid copy must contain a duplicate of each piece, byte and area of the source drive, including unallocated void space and slack space, exactly all things considered information shows up on the source drive in respect to the next information on the drive. (Ball, n.d.)

The forensically-solid copy sketched out by Ball is typically procured by physically removing the hard disk from the objective framework. The hard disk is then appended to a write blocking gadget and replicated utilizing one of numerous conceivable procurement utilities, making an "image" of the drive. For investigators of normal means, making a forensically-stable copy of an Android gadget can be testing. The working framework itself and the larger part of legal ancient rarities (except for pictures, media files, and some application information) are put away on internal flash memory. Evacuating the flash memory and joining it to a write blocker is, while hypothetically conceivable, past the range of most criminology labs because of the complex hardware work included. The NAND memory in numerous gadgets could possibly be gotten to either through the JTAG7 ports in the gadget, or by physically removing the chip. Either system would require significant gadgets work and encourage remaking of the low-level NAND format. Straightforwardly accessing to the NAND flash is a final resort, however it might be the main probability on a legitimately locked gadget (Breeuwsma, 2007).

Further difficulties are exhibited by the powerlessness of standard clients to perform the low-level operations important to forensically obtain a gadget, as the Android security model does not more often than not give root access. Moreover, flash memory stores metadata in a design that is not considered by customary legal securing techniques. What the normal measurable examiner winds up with, then, is just an estimate of a forensically-stable copy of an Android device.

Flow chart diagram:

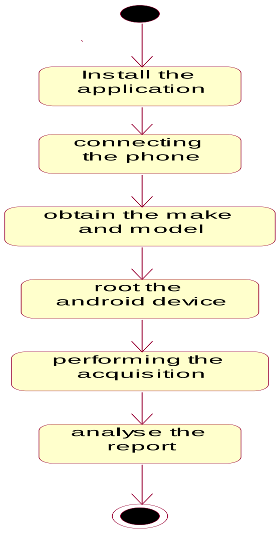

Figure.1

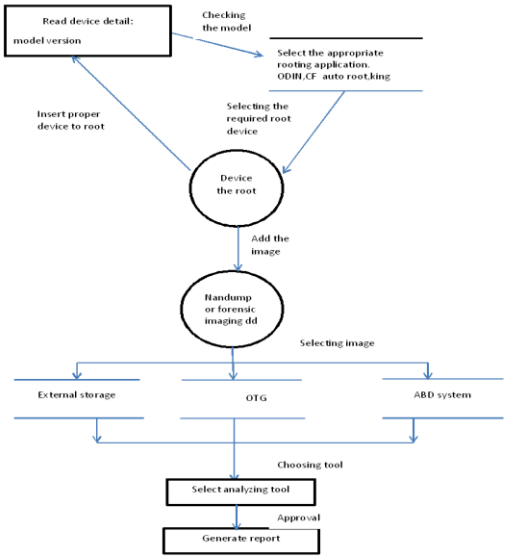

Figure.2

2. CONCLUSION

The Retrieving Process of deleted files in Android devices has been done with this tool. Phone gets administrative privilege through rooting process. Whole mobile partitions can be acquired by using this tool. Retrieved image files can successfully converted into human readable format. Mobile sms also retrieved easily.

REFERENCES

A Comparison between Windows Mobile and Symbian S60 Embedded Forensics, by Antonio Savoldi, Paolo Gubian, and Isao Echizen, 2009.

A Comparison of Forensic Acquisition Techniquesfor Android Devices, A case study investigation of web browsing sessions, by Nedaa Baker Al Barghouthy and Andrew Marrington, 2014.

Brintha Rajakumari S, Nalini C, An efficient data mining dataset preparation using aggregation in relational database, Indian Journal of Science and Technology, 7, 2014, 44-46.

Carving Orphaned JPEG File Fragments, by ErkamUzun and HüsrevTahaSencar, 2015.

Design and Implementation of Live SD Aquisition Tool in Android Smart Phone, by Sheng-Wen Chen, Chung-Huang Yang, Chien-Tsung Liu, 2011.

Fan Zhou, Yitao Yang, Zhaokun Dingy, Guozi Sun, Dump and Analysis of Android Volatile Memory on Wechat, 2015.

Forensic Data Recovery from Android OS Devices: An Open Source Toolkit, by Patrick Dibband Mohammad Hammoudeh, 2013.

Forensic Information Acquisition in Mobile Networks, by David Irwin and Ray Hunt, 2009.

Jayalakshmi V, Gunasekar NO, Implementation of discrete PWM control scheme on Dynamic Voltage Restorer for the mitigation of voltage sag /swell, 2013 International Conference on Energy Efficient Technologies for Sustainability, ICEETS, 2013, 1036-1040.

Kaliyamurthie KP, Parameswari D, Udayakumar R, QOS aware privacy preserving location monitoring in wireless sensor network, Indian Journal of Science and Technology, 6 (5), 2013, 4648-4652.

Kaliyamurthie, K.P., Udayakumar, R., Parameswari, D., Mugunthan, S.N., Highly secured online voting system over network, Indian Journal of Science and Technology, 6 (6), 2013, 4831-4836.

Khanaa V, Thooyamani KP, Saravanan T, Simulation of an all optical full adder using optical switch, Indian Journal of Science and Technology, 6 (6), 2013, 4733-4736.

Khanaa V, Thooyamani KP, Using triangular shaped stepped impedance resonators design of compact microstrip quad-band, Middle - East Journal of Scientific Research, 18 (12), 2013, 1842-1844.

Kumaravel A, Dutta P, Application of Pca for context selection for collaborative filtering, Middle - East Journal of Scientific Research, 20 (1), 2014, 88-93.

Mobile Forensic Data Acquisition in Firefox OS, by MohdNajwadiYusoff, RamlanMahmod, MohdTaufik Abdullah, Ali Dehghantanha, 2014.

Pandit A.A, Anup Kumar, Conceptual Framework and a Critical Review for Privacy Preservation in Context Aware Systems, 2011.

Raj MS, Saravanan T, Srinivasan V, A modified direct torque control of induction motor using space vector modulation technique, Middle - East Journal of Scientific Research, 20 (11), 2014, 1572-1574.

Saravanan T, Raj MS, Gopalakrishnan K, VLSI based 1-D ICT processor for image coding, Middle - East Journal of Scientific Research, 20 (11), 2014, 1511-1516.

Sengottuvel P, Satishkumar S, Dinakaran D, Optimization of multiple characteristics of EDM parameters based on desirability approach and fuzzy modeling, Procedia Engineering, 64, 2013, 1069-1078.

Sundararajan M, Optical instrument for correlative analysis of human ECG and breathing signal, International Journal of Biomedical Engineering and Technology, 6 (4), 2011, 350-362.

Thamotharan C, Prabhakar S, Vanangamudi S, Anbazhagan R, Anti-lock braking system in two wheelers, Middle - East Journal of Scientific Research, 20 (12), 2014, 2274-2278.

Udayakumar R, Khanaa V, Saravanan T, Saritha G, Retinal image analysis using curvelet transform and multistructure elements morphology by reconstruction, Middle - East Journal of Scientific Research, 16 (12), 2013, 1781-1785.

Vanangamudi S, Prabhakar S, Thamotharan C, Anbazhagan R, Design and fabrication of dual clutch, Middle - East Journal of Scientific Research, 20 (12), 2014, 1816-1818.

Vanangamudi S, Prabhakar S, Thamotharan C, Anbazhagan R, Design and calculation with fabrication of an aero hydraulwicclutch, Middle - East Journal of Scientific Research, 20 (12), 2014, 1796-1798.

Volatile Memory Acquisition Using Backup for Forensic Investigation, Farhood Norouzizadeh Dezfouli, Ali Dehghantanha, Ramlan Mahmoud, Nor FazlidaBintiMohdSani,Solahuddin bin Shamsuddin, 2014.