



Analysis and Interpretation of Data for Gathering Evidence for the Legal Constitution

Mr. D. S. Jadhav
Research Scholar
Solapur University, Solapur,
India

Mr. V. V. Patil
Assistant Professor,
SICS (MCA), Pandharpur,
India

Dr. S. K. Patil
Associate Professor & H.O.D.,
BPSCC, Barshi,
India

Abstract - Digital forensics is a branch of forensic science concerned with the use of digital information as source of evidence in investigations and legal proceedings. "The use of scientifically derived and proven methods toward the preservation, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations"[1]. Computer forensics is the application of computer investigation and analysis techniques to determine potential legal evidence. Since computers are vulnerable to attack by some criminals, computer forensics is very important. Understanding computer forensic procedures will help to capture vital information which can be used to prosecute an intruder that compromises a computer or network. Also, deciding on the specific tools for computers or other equipment that is needed to correctly analyze evidence is crucial. These tools are very useful but bigger companies that handle more equipment and information might benefit from something that can combine all these tools into one application[2].

Keywords: Source of evidence, Legal proceeding, Data analysis, Cyber crime, Computer forensic.

I. INTRODUCTION

For every researcher, Data analysis is the most important task during entire research process. This is the next step after data collection. Data collected by the researcher must be scientifically and systematically processed or analyzed so as to achieve objectives of research study. Data processing involves editing, coding, classification and tabulation of collected data so that it should be completely ready and capable for analysis in all respects. Data analysis is referred to calculations and computations of data based on certain parameters along with searching for pattern of relationship that exists among data groups which is then tested with hypothesis of the study through the support of statistical tools. The Researcher has collected data from selected Judiciary, Advocates, Police Officers, Experts and Computer Users. Furthermore, this data is classified into four groups namely Judiciary, Advocates, Police, Experts and Computer Users. This research article is devoted to study the performance evaluation through analysis and interpretation of 4 different types of questionnaire, which were prepared for 8 districts in Maharashtra, 323 member respondents from 4 Judiciary, 42 Advocates, 77 Police Officers / policemen, 43 Expert Persons and 157 Computer Users selected.

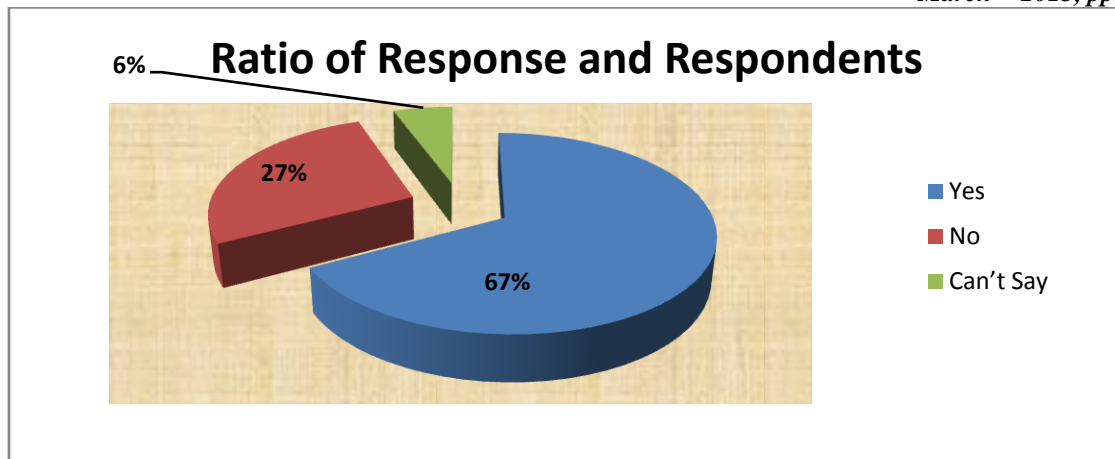
II. ANALYSIS & INTERPRETATION OF DATA

The Researcher has first considered analysis for questions related to fields and then subsequently for critical analysis of hypothesis related questions.

Table 1 : Ratio of Response and Respondents

Response	Respondents	Percentage (%)
Yes	217	67.18
No	88	27.25
Can't Say	18	05.57
Total	323	100

Source : Data compiled from the questionnaire



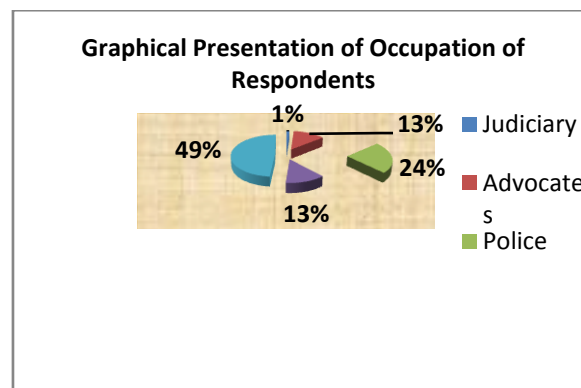
Graph 1 : Ratio of Response and Respondents

The table and graph 1, Observed that total 323 respondents. This implies that 67% of respondents in the favour of Yes, 27% respondents in the favour of No and 6% are neutral that means can't say.

Table 2 : Occupation of the Respondents

Occupation	Respondents	Percentage (%)
Judiciary	4	1.24
Advocates	42	13.003
Police	77	23.84
Expert	43	13.31
Computer User	157	48.607
Total	323	100

Source : Data compiled from the questionnaire



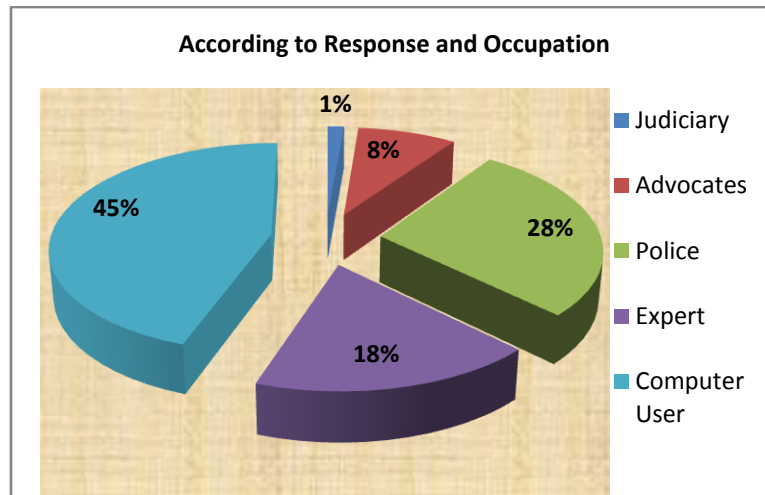
Graph 2 : Graphical representation Occupation of Respondents

The table and graph 2, Observed that pictorial presentation of occupation of respondents. This involves Judiciary(1%), Advocates(13%), Police(24%), Experts(13%) and Computer Users(49%) selected for the analysis of questionnaire.

Table 3 : According to Response & Occupation

Occupation	Response			Total
	Yes	No	Can't Say	
Judiciary	03	01	00	04
Advocates	18	20	04	42
Police	60	15	02	77
Expert	39	04	00	43
Computer User	97	48	12	157
Total	217	88	18	323

Source : Data compiled from the questionnaire



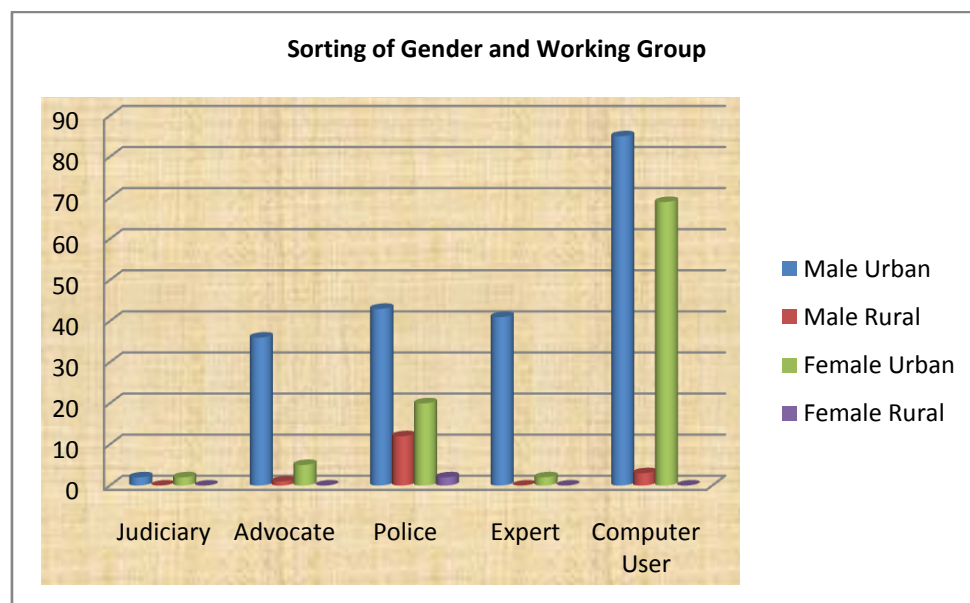
Graph 3 : According to Response & Occupation

The table and graph 3, Observed that total 323 respondents. Total 217 respondents agrees with Yes in which Judiciary(3), Advocates(18), Police(60), Experts(39) and Computer Users(97). Total 88 respondents agrees with No in which Judiciary(1), Advocates(20), Police(15), Experts(4) and Computer Users(48). Total 18 respondents implies Can't Say in which Judiciary(0), Advocates(4), Police(2), Experts(0) and Computer Users(12).

Table 4 : Sorting of Gender and Working Group

Gender	Working Area	Occupation					Total
		Judiciary	Advocate	Police	Expert	Computer User	
Male	Urban	02	36	43	41	85	207
	Rural	00	01	12	00	03	16
Female	Urban	02	05	20	02	69	98
	Rural	00	00	02	00	00	02
Total	Urban	04	41	63	43	154	305
	Rural	00	01	14	00	03	18
Total		04	42	77	43	157	323

Source : Data compiled from the questionnaire



Graph 4 : Sorting of Gender and Working Group

The table and graph 4, Observed that the total ratio of the working area as well as the gender of the respondents 323. If it observed that Male (from 207 urban area and 16 rural area) & Female (from 98 urban area and 02 rural area).

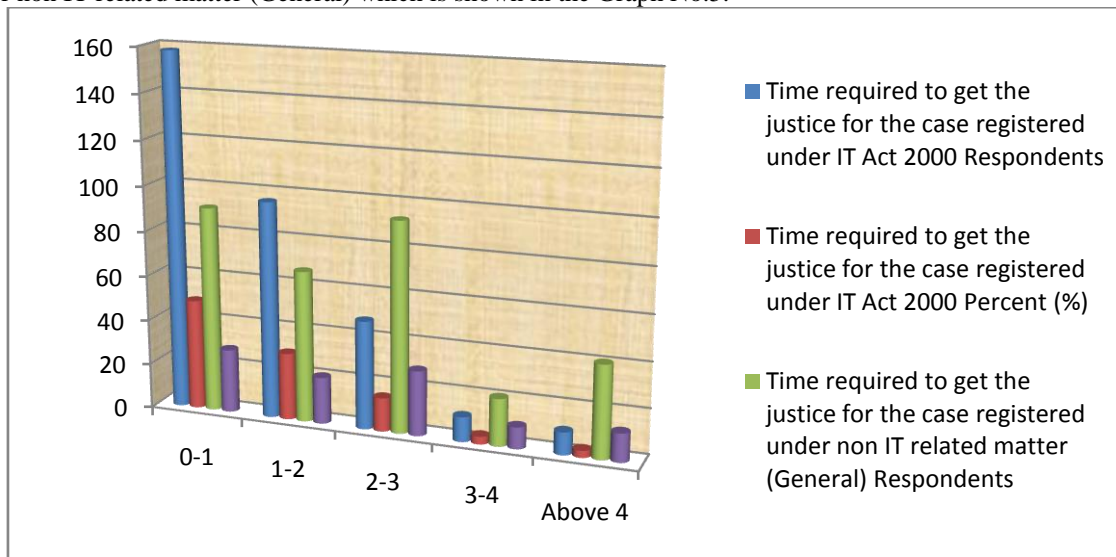
And Judiciary, Advocates, Police, Expert, Computer User which can be in categorized by its gender display in the table and chart.

Table 5 : Difference in disposal time of the two matters (in years)

Period for disposal of the matter (in yrs)	Time required to get the justice for the case registered under IT Act 2000		Time required to get the justice for the case registered under non IT related matter (General)	
	Respondents	Percent (%)	Respondents	Percent (%)
0-1	158	48.9	91	28.2
1-2	96	29.7	67	20.7
2-3	48	14.9	93	28.8
3-4	11	3.4	21	9.6
Above 4	10	3.1	41	12.7
Total	323	100	323	100

Source : Data compiled from the National Crime Report Bureau

Table No. 5 furnishes the difference between the disposal times of the matters (IT Act 2000 & General Matter). General matter indicates the matter other than IT Act like matter registered under section IPC 132 of Negotiable Instruments Act etc. It is observed that 48.9 % people said that less than one year is time required to get the justice for the case registered under IT Act 2000. While 28.2% people said that Time required getting the justice for the case registered under non IT related matter (General) is less than one year. 29.7 % people said that time required to get the justice for the case registered under IT Act 2000 is more than one year & less than two years. While 20.7% people said that time required to get the justice for the case registered under non IT related matter (General) is more than one year & less than Two years. 14.9% people are agree with that more than Two years & less than three years time is required to get the justice for the case registered Under IT Act 2000. 28.8% people are agree that more than two years & less than three time is required to get the justice for the case registration under the non IT related matters (General). 3.4% people said that it takes more than Three years & less than Four years times to get the justice for the case registered under the IT Act 2000. While 9.6 % people said that it takes place more than Three years and less than Four years times to get the justice for the case registered under non IT related matter. 3.1% people are agreeing with that more than Four years ties required to get the justice for the case registered under IT Act 2000. While 12.7% people are with that more than Four years time is required to get the justice for the case registered under the non IT related matter. If we could continuing up to Two years then it is clearly prove that there is difference between the time required to get the justice for the case registered under IT Act 2000 an under non IT related matter (General) which is shown in the Graph No.5.



Graph 5: Difference in disposal time of two meter in years

Table 6 : One sample statistics for IT Act 2000& General Matters

	N	Mean in Years	Standard Deviation	Median in Years	Mode in Years
Time required to get the justice for the case registered under IT Act 2000	323	1.82	1.012	2.00	1
Time required to get the justice for the case registered under non IT related matter (General)	323	2.58	1.329	3.00	3

(N : Number of Respondents)

Source : Data compiled from the questionnaire

Table No. 6 furnishes one sample statistics for IT matter & General matter. It is observed that the Mean time for getting justice for the cases registered under IT Act 2000 is 1.82 years long with 1.012 Standard Deviation. Where Mean time for getting justice for the cases registered under non IT related matter (General) is 2.58 years along with 1.329 Standard Deviation, so there is difference between the times required to get difference between the times required to get the justice for the case registered under IT Act 2000 an under non IT related matter (General). Median time required is 2 years to get justice for the case registered under IT Act 2000 while Median time required to get the justice for the case registered under non IT related matter is 3 years. Mode time is 1 year to get the justice for the case registered under IT Act 2000. And for the case registered under non IT related matter the mode time is 3 years to get the justice. This shows that there is difference between the times required to get the justice for case registered under IT Act 2000 & non IT related matter.

Table 7 : Actual Cyber cases filed in court of Law & decided

Sr No	Case No.	Court	Section No. of IT Act	Date of Registration	Date of Judgment	Duration
1	R.C.C. No. 253/2004	JMFC Pune	67	19/07/2004	25/01/2008	3 Years 6 Months 8 Days
2	R.C.C. No. 103/2004	JMFC Pune	67	04/04/2004	21/02/2005	1 Years 4 Months 17 Days
3	R.C.C. No. 2931/2004	JMFC Pune	67	14/08/2007	10/12/2007	4 Months 25 Days
4	R.C.C. No. 429/105/2004	Court No. 37, Mumbai	67	15/02/2004	26/02/2007	2 Years 11 Months 15 Days
Average Duration						2 Years

Source : Data compiled from the National Crime Report Bureau

Table No. 7, gives thee information about actual cyber cases filed in court of law & decided. In Pune & Mumbai court there are more than 25 cases were pending. The pending cases average time is three years. In short the average of both decided cases & pending cases will lie in between two to three years. The average years calculated through respondents is 1.82 years means near about two years. It shows that respondents reply is supporting to the actual data.

III. FINDINGS

By evaluation the data analysis, interpretation & onsite observations the researchers observed the followings –

- It is observed that, majority of the respondents (69.3%) were cautious to lodge a complaint about the dispute regarding cyber crime. There are various reasons such as people are worried about the reputation, people don't have time for lodging the complaint regarding cyber crime, people are not sure about whether they will get justice, it requires more time to decide the case due to technically & people think that goodwill of the business in the market may diminish. According to categories of respondents such as gender, profession, age wise etc. stated that all the reasons for the hesitation are supporting that people are hesitation to approach the court in case of cyber crimes[3].
- It is found that majority of the respondent said that the time required to get the justice for the case registered under IT Act 2000 is less than one year & one to two years. Average time to get justice regarding cyber crime is 1.82, approximately two years. By observing actual cyber cases filed in the court of law & considering the pending cases the average time required is in between two to three years[4].
- It is observed that there are various reasons such as poor enforcement of IT Act, people are not sure about security, poor knowledge about how to use E-commerce non availability of infrastructure facility (i.e. Computer Machine, Internet connection, etc.) & lack of awareness of IT Act 2000 are affecting on the uses of e-commerce instead of enactment of IT Act 2000. According to category of respondents such as gender, profession & age wise etc., stated that all the reasons for not using e-commerce widely even enactment of IT Act[5].

- It is observed that the average time for getting justice for the cases registered number IT Act 2000 is 1.82 year along with Standard Deviation time is 1.012 where as Mean time for getting justice for the cases registered under non IT related matter (General) is 2.58 years & Standard Deviation time is 1.329.
- It is observed that there are eight parameters which are affecting the speedy disposal of the matters. These parameters are lodging early complaint; role of police as investigation authority, role of prosecutor, role of advocate of accuse, role of Judicial Officer, appointment of special tribunal, non availability of number of cyber forensic labs in comparison with population, & no proper machinery for implementation of the cyber law. According to category respondents stated that all the parameters are affecting the speedy disposal of the matters registered under IT Act[6].
- During the visit at Cyber cell of Commissioner Office at Mumbai, Pune, Kolhapur & Solapur (Western Maharashtra)it is observed that the number staff appointed at the cell is very less as compare to the registration of the cyber cases. While for other district no such cyber cell.
- It is found that the staffs in the cyber cell of Police Commissioner Office are not much qualified where technicality is concern. They have been given the training of how to investigate the cyber crime but still due to shortfall in technicality they are not comfortable about the cyber crime investigation.
- It is observed that the software & hardware available in the cyber cell are not up to mark so the staff of cyber cell has become handicapped in the case of emergency investigation. They need to depend upon the cyber forensic lab which is time consuming, & during this case evidence may get tampered with the offender[7].
- Numbers of cyber forensics lab are very less as compared to the number of cyber crimes taking place in the country.
- There is dependency on Police of Cyber Cell that until the forensic report is not received they are not able to take further step of making charge sheet & approaching the concerned court of law. It is observed that there is much delay in this step. So after making complaint in the police the case may take few months for registration of cases in the court of law.
- It is observed that as Police is under state government authority & their service is transferable, the transfer of officer may break link the cases & the new place of transfer may or may not be related to cyber crime. In this regard even though the willingness of the officers does nothing if he is transferred from any another department to cyber cell or vice versa.
- It is observed that because of justification problem, criminal seating out of the country can do anything offence & no government can arrest the offenders if there is no such treaty of exchange of criminals in between these countries.
- As International Law is considered as a weak law, the crimes related to cyberspace also somewhat related to international category because the offender may be in out of country, if it is out of country & doing against the rule of the nation it is very difficult to arrest the offenders & punish accordingly[8].

IV. CONCLUSION

It is concluded that the people are reluctant to lodge complaint about cyber crime due to various reasons that their reputation is at stake. People don't get time to lodge complaint about the dispute regarding cyber crime, much time will be required to decide the case due to technicalities & people were not too sure that they would get justice but in matters of grave seriousness they have no choice & they do have faith in the justice[9]. It is also concluding that all categories of respondents have supported for the above mentioned reasons for approaching the court of law in case of cyber crimes. Few of the categories conclusion mentioned here are, Professionals do not believe about surety of justice in case of cyber crime cases. Judiciary, Police & Advocates are more worried about their reputations than Business Persons & Experts in case of cyber crime case due to lack of awareness of cyber law[10].

By using parameters of speedy disposal mentioned in this research; time for disposal of the matter should be reduced to the mounts instead of years so that people will not hesitate to approach court of law in case of cyber crimes. If it happens truly for cyber cases then the people will not hesitate to approach the court of law. There should be separate cyber cell office with trained staff & well equipped office with latest software & hardware at every district police commissioner office. Region wise Cyber forensics labs should be presented[11]. There should be provision in cyber law throughout the entire world for creation of e-mail account. The provision should be like the procedure of getting phone number so that email can be treated as evidence. It will help in for reducing the number of cyber crime. The Police Officer appointed at the Cyber Cell off Commissioner Office should posses at least bachelor's degree in Computer Science/Application or Engineering along with latest training about how to investigate the cyber crime. Cyber space is available across the whole world[12]. So the problem of jurisdiction becomes

very complex. The problem can be solved by all the nations together. There should be one law throughout the world for cyber crimes.

REFERENCES

- [1] Casey, E.. *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*. San Diego, CA: Academic Press.
- [2] Icové, D., Seger, K., & VonStorch, W. *Computer Crime*. O'Reilly & Associates.
- [3] Kruse, W. G., & Heiser, J. G.. *Computer Forensics: Incident Response Essentials* Addison Wesley.
- [4] Masters, G., & Turner, P. (2007). Forensic Data Recovery and Examination of Magnetic Swipe Cloning Devices. *Digital Investigation*, 4 (1).
- [5] US-CERT. (2005). Computer Forensics. *US-CERT*, 1 (2).
- [6] Wang, S.-J. (2007). Measures of Retaining Digital Evidence to Prosecute Computer-Based Cyber-Crimes. *Computer Standards & Interfaces*.
- [7] Computer Forensics World. "Computer Forensics Basics: Frequently Asked Questions". (Online) Retrieved April 3rd, 2009
- [8] Dixon, Phillip D. "An overview of computer forensics". 2005 Potentials, IEEE. Volume 24 Issue 5. IEEE International.
- [9] CNN News. "Caylee Blog". (Online) Retrieved April 2nd, 2009, from <http://www.cnn.com/2008/CRIME/09/08/NGfindcayleeblog/index.html?iref=newssearch>
- [10] CNN News. "Bill proposes ISPs, Wi-Fi keep logs for police".(Online) Retrieved April 5th, 2009
- [11] McQuade, Samuel C. "*Understanding and Managing Cybercrime*". (2006). Pearson Education, Inc.
- [12] Hayes, Darren R and Qureshi, Shareq. "A Framework for Computer Forensics Investigations Involving Microsoft Vista". 2008. Systems, Applications and Technology Conference, 2008 IEEE Long Island.
- [13] Allen, William H. "Computer Forensics". 2005. Security & Privacy, IEEE. Volume 3, Issue 4.
- [14] Capital Markets and Inso - vency in a Global Economy, Kluwer Law International, 2000
- [15] Guide to Cyber Laws by Rodney D. Ryder Hand book of Cyber & E-commerce Laws by P.M. Bakshi & R.K.Suri
- [16] DIGITAL EVIDENCE Emerging Problems in Forensic Computing Peter Sommer

Authors Biography



D. S. Jadhav was born in India, Maharashtra, in 1979. He received the BCA, MCA, MBA degrees from Shivaji University, Kolhapur (MS), University of Pune (MS) and Sikkim Manipal University respectively. He is registered student for PhD (2010) as a Research Scholar, from Solapur University, Solapur. From 2008-2010 he was worked as lecturer Smt. K. W. College, Sangli. From 2010 to 2012 he was worked as Asst. Professor at Bharat Ratna Indira Gandhi College of Engineering, Solapur (MS) and Sinhgad Institute of Computer Sciences, Pandharpur(MS) respectively. He has published more than 25 papers in International and National journals and conference Proceedings. He is member of various National & International Professional Bodies and member of Editorial / Reviewer of various International Journals. His research interest includes Cyber Crime, Cyber / Computer Forensic, Information Security.



V. V. Patil was born in India, Maharashtra, in 1983. He received the BSc, MCA degrees from Shivaji University, Kolhapur (MS). From 2008-2011 he was worked as lecturer at G. H. Rasoni College of Engineering & Management, Pune. From 2011 to till date he is working as Asst. Professor at Sinhgad Institute of Computer Sciences, Pandharpur(MS). He has published 2 papers in International and National journals and conference Proceedings. His research interest includes Cyber Crime, Information Security, and ICT.

Dr. S. K. Patil was born in India, Maharashtra, in 1962. He received PhD from, Swami Ramanand Tirth Marathwada University, Nanded. He worked as Lecturer, Assistant Professor & now he is working as Associate Professor & Head of Department at BPSCC, Barshi, (MS). He has published more than 40 papers in International and National journals and conference Proceedings. He is member of various National & International Professional Bodies and member of Editorial / Reviewer of various International Journals. His research interest includes Traditional Law, Cyber Crime, Cyber / Computer Forensic, Information Security, Management.