Volume 3, Issue 12, December 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Investigation and Elucidation of Computer Investigation and Analysis Techniques for Presentation of Gathering Evidence in Legal Constitution

Mr. D. S. Jadhav
Assistant Professor,
Ideal Institute of Management (IIMK),
Kondigre, Maharashtra, India

Dr. S. K. Patil
I/c Principal, Associate Professor
BPSCC, Barshi, India

Mr. S. M. Khandke
Assistant Professor,
Ideal Institute of Management (IIMK),
Kondigre, MS, India

Abstract - The presentation of digital information cannot be well perceived by human senses. This is because the electronic record has been electromagnetically recorded and stored inside the computer system. It is therefore impossible to perceive its content without the help of a suitable toolkit. Before any evidence can be gathered, a warrant must be issued. Just like the need for a warrant to search someone and their property, everyone involved in the computer forensics process needs authorization from the proper authorities to monitor and collect information related to a computer intrusion. Security monitoring tools also have legal implications. Other procedures that need to be followed are the laws that have requirements for safeguarding data. This is not only to keep protected from intruders but to prevent evidence from being dismissed and also to prevent lawsuits or regulatory audits. Three laws that are important for anyone that is involved with computer forensics are the; Wiretap Act; Pen Registers and Trap and Trace Devices Statute; and the Stored Wired and Electronic Communication Act.

Keywords: digital information, electronic record, safeguarding data, laws, computer intrusion.

I. INTRODUCTION

Evidence can be gathered from theft of trade secrets, theft of or destruction of intellectual property, fraud or anything else criminally related to the use of a computer. Evidence, which is also referred to as "digital evidence," is, "any data that can provide a significant link between the perpetrator and the victim".

When experts are ready to retrieve data they take careful steps to identify and attempt to retrieve data that exists on a computer. If the digital evidence is collected aimlessly then not only will there be inefficient use of resources but the evidence could get compromised, thus liberating a criminal from all possible wrong doing. Before this evidence is submitted it must meet three basic requirements to maintain its reliability: "It must be produced, maintained, and used in a normal environment; be professionally authenticated (i.e. the report from the forensic experts is reliable); and also meet the "best evidence rule". This means that what is produced must be the best evidence available and not a substitute for the evidence offered". There are also procedures that must be followed at the crime scene. Just like any other regular crime scene, a computer has to be kept in the same condition as it was found. Doing this prevents any evidence from being questioned

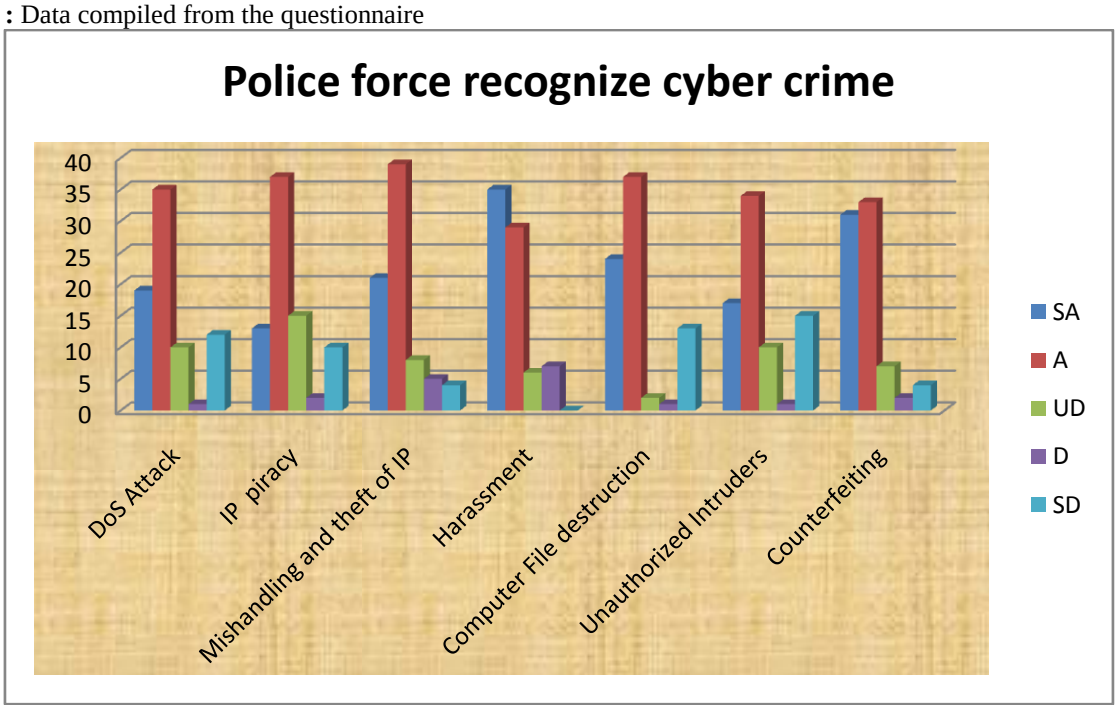
II. ANALYTICAL INTERPRETATION

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

Table 1: Police force recognizes cyber crime.

Police force recognize cyber crime	SA	A	UD	D	SD	Total
DoS Attack	19	35	10	01	12	77
IP piracy	13	37	15	02	10	77
Mishandling and theft of IP	21	39	08	05	04	77
Harassment	35	29	06	07	00	77
Computer File destruction	24	37	02	01	13	77
Unauthorized Intruders	17	34	10	01	15	77
Counterfeiting	31	33	07	02	04	77

Source : Data compiled from the questionnaire



Graph 1: Police force recognizes cyber crime

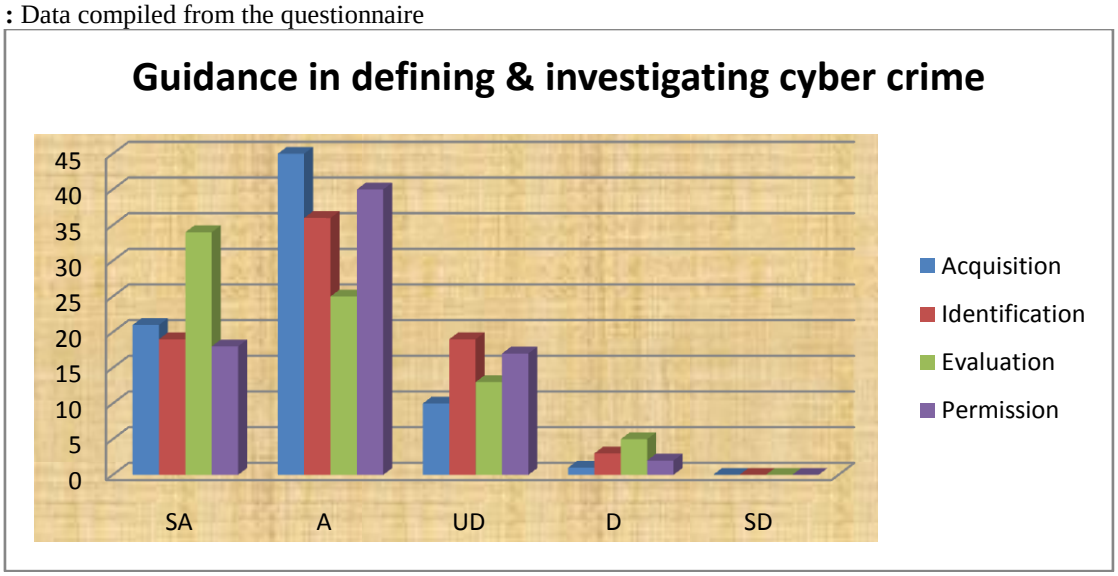
There was 15 in unauthorized intruders and 13 in computer file detections respondents who did strongly disagree respond to this question. 39 in mishandling and theft of IP and 37 in IP piracy respondents agreed that recognized cyber crime issues. 35 in harassment and 31 in counterfeiting respondents strongly agreed to this statement. However there were 07 in harassment respondents who disagreed with the statement and 15 in IP piracy responded as undecided.

The analysis of the above data shows that maximum number of respondents strongly agreed that the reorganization of cyber crime issues.. Their output must cater to the actual need, requirements and expectations of to catch the cyber criminals.

Table 2 : Guidance in defining & investigating cyber crime.

Guidance in defining & investigating cyber crime	SA	A	UD	D	SD	Total
Acquisition	21	45	10	01	00	77
Identification	19	36	19	03	00	77
Evaluation	34	25	13	05	00	77
Permission	18	40	17	02	00	77

Source : Data compiled from the questionnaire



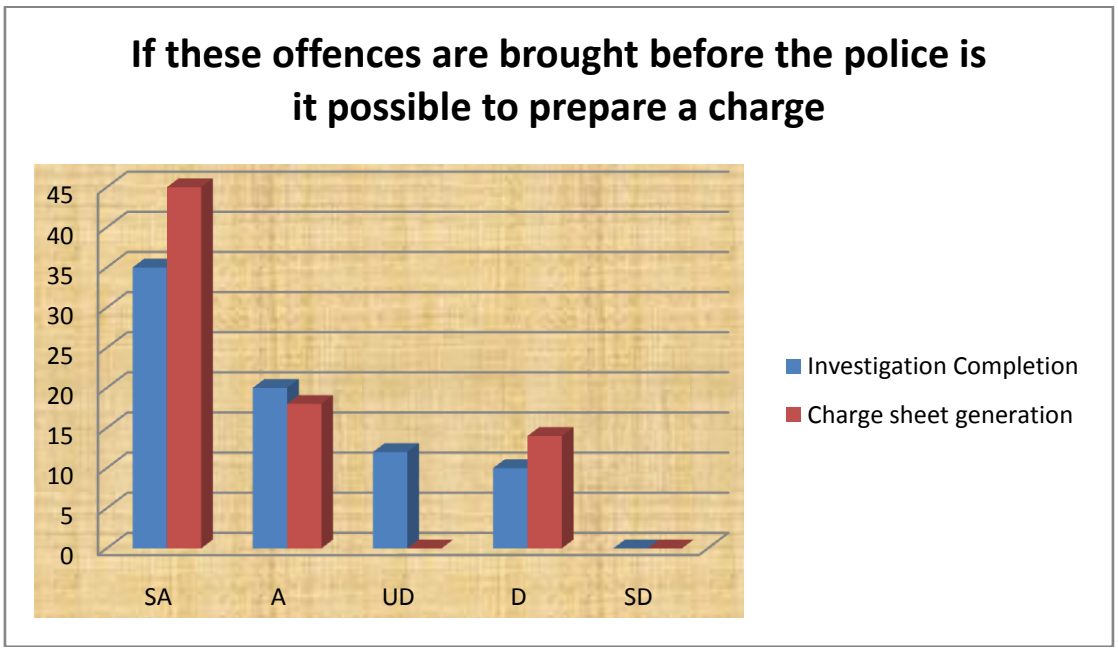
Graph 2 : Guidance in defining & investigating cyber crime.

There was 00 in all issues of cyber crime respondents who did strongly disagree respond to this question. 45 in acquisition and 40 in permission respondents agreed that guidance in defining and investigating cyber crime. 34 in evaluation and 21 in acquisition respondents strongly agreed to this statement. However there were 05 in evaluation respondents who disagreed with the statement and 19 in identification responded as undecided. The analysis of the above data shows that maximum number of respondents strongly agreed that the guidance and investigating cyber crime

Table 3 : If these offences are brought before the police is it possible to prepare a charge.

offences are brought before the police	SA	A	UD	D	SD	Total
Investigation Completion	35	20	12	10	00	77
Charge sheet generation	45	18	00	14	00	77

Source : Data compiled from the questionnaire



Graph 3 : If these offences are brought before the police is it possible to prepare a charge.

There was 00 in all the cyber crime issues if these offences are brought before the police is it possible to prepare a charge respondents who did strongly disagree respond to this question. 20 in investigation completion and 18 in charge sheet generation respondents agreed that recognized cyber crime issues. 45 in charge sheet generation and 35 in investigation completion respondents strongly agreed to this statement. However there were 14 in charge sheet generation respondents who disagreed with the statement and 12 in investigation completion responded as undecided.

The analysis of the above data shows that maximum number of respondents strongly agreed that the reorganization of if these offences are brought before the police is it possible to prepare a charge. Their output must cater to the actual need, requirements and expectations of to catch the cyber criminals.

Table 4 : Methods & techniques are used by cyber investigators to provide valid & reliable result.

Methods & techniques are used by cyber investigators to provide valid & reliable result	SA	A	UD	D	SD	Total
FTK Manager	10	34	08	25	00	77
Forensic Tool Kit	45	30	02	00	00	77
PC Inspector File Recovery	42	32	03	00	00	77
Cross Drive Analysis Kit	15	26	15	21	00	77
Live Analysis Kit	12	29	17	19	00	77

Source : Data compiled from the questionnaire

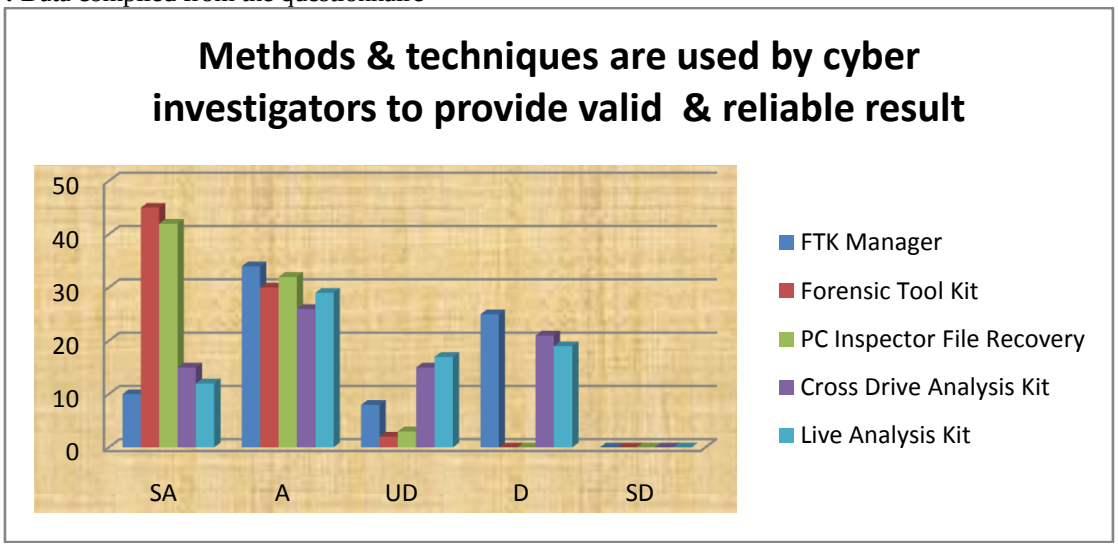


Table 4: Methods & techniques are used by cyber investigators to provide valid & reliable result.

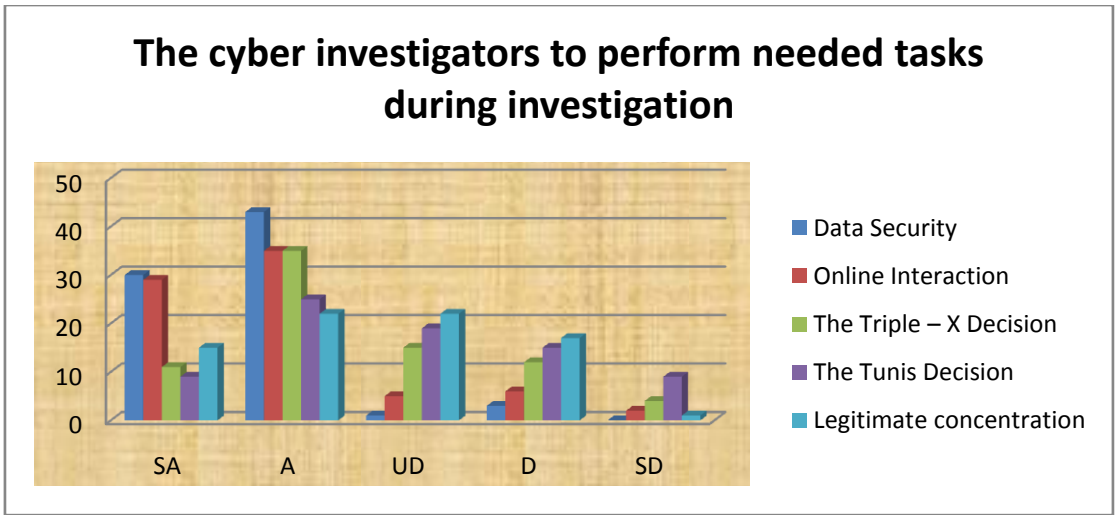
There was 00 in all the cyber crime issues Methods & techniques are used by cyber investigators to provide valid & reliable result respondents who did strongly disagree respond to this question. 32 in PC Inspector file recovery and 30 in forensics tool kit respondents agreed that recognized cyber crime issues in Methods & techniques are used by cyber investigators to provide valid & reliable result. 45 in forensics tool kit and 42 in PC inspector file recovery respondents strongly agreed to this statement. However there were 25 in FTK manager and 21 cross drive analysis kit respondents who disagreed with the statement and 17 in live analysis kit responded as undecided.

The analysis of the above data shows that maximum number of respondents strongly agreed that the reorganization of Methods & techniques are used by cyber investigators to provide valid & reliable result. Their output must cater to the actual need, requirements and expectations to implements the methods and techniques in that computer forensics lab.

Table 5: The cyber investigators to perform needed tasks during investigation.

The cyber investigators to perform needed tasks during investigation	**SA**	**A**	**UD**	**D**	**SD**	**Total**
Data Security	30	43	01	03	00	77
Online Interaction	29	35	05	06	02	77
The Triple – X Decision	11	35	15	12	04	77
The Tunis Decision	09	25	19	15	09	77
Legitimate concentration	15	22	22	17	01	77

Source : Data compiled from the questionnaire



Graph 5 : The cyber investigators to perform needed tasks during investigation.

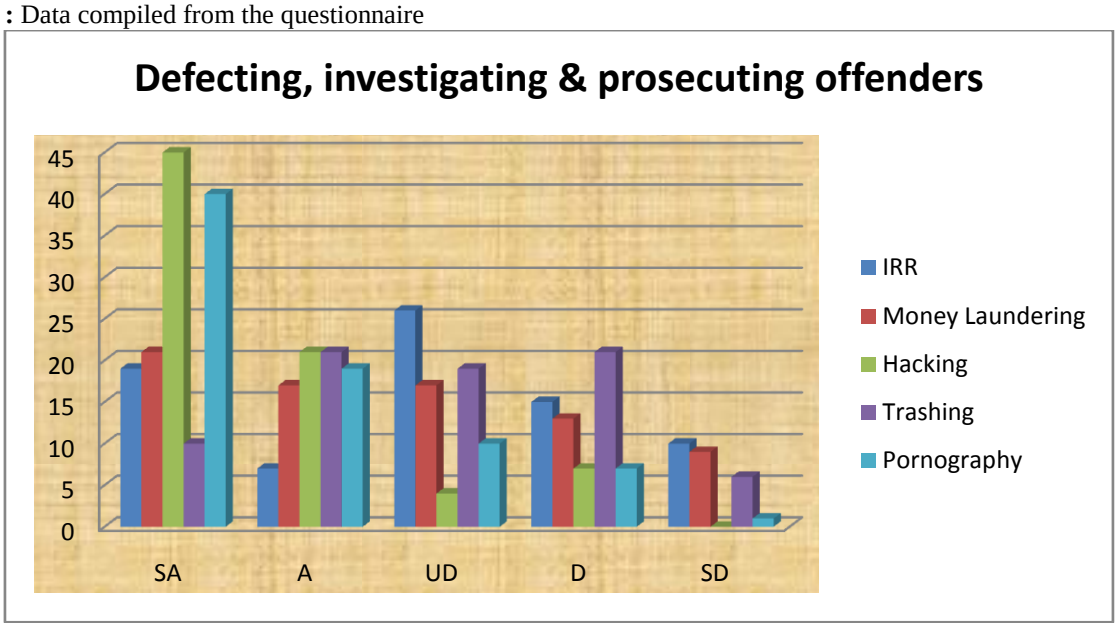
There was 09 in the tunis decision respondents who did strongly disagree respond to this question. 43 in data security and 35 in online interaction and 35 in the triple – x decision respondents agreed that recognized the cyber investigators to perform needed tasks during investigation. 30 in data security and 29 in online interaction respondents strongly agreed to this statement. However there were 17 in legitimate concentration and 15 in the triple – x decision respondents who disagreed with the statement and 22 in legitimate concentration and 19 in the tunis decision responded as undecided.

The analysis of the above data shows that maximum number of respondents strongly agreed that the reorganization of the cyber investigators to perform needed tasks during investigation. Their output must cater to the actual need, requirements and expectations to implements the methods and techniques in that computer forensics lab.

Table 6 : Defecting, investigating & prosecuting offenders.

Defecting, investigating & prosecuting offenders	**SA**	**A**	**UD**	**D**	**SD**	**Total**
IRR	19	07	26	15	10	77
Money Laundering	21	17	17	13	09	77
Hacking	45	21	04	07	00	77
Trashing	10	21	19	21	06	77
Pornography	40	19	10	07	01	77

Source : Data compiled from the questionnaire



Graph 6 : Defecting, investigating & prosecuting offenders.

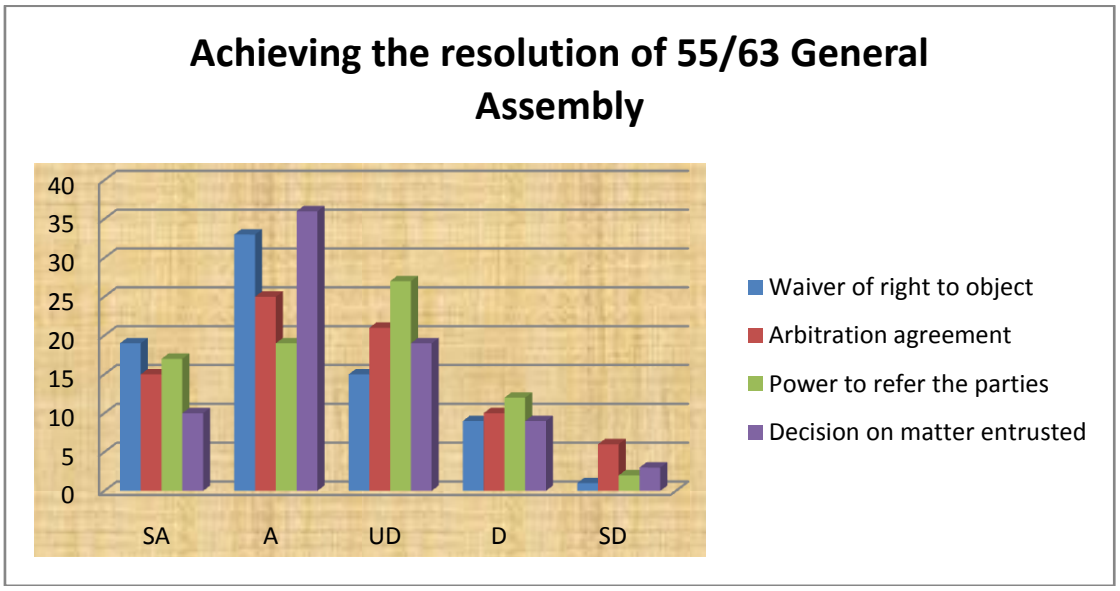
There were 10 in the IRR and 09 in money laundering respondents who did strongly disagree respond to this question. 21 in hacking and trashing and 19 in pornography respondents agreed that recognized Defecting, investigating & prosecuting offenders. 45 in hacking and 40 in pornography respondents strongly agreed to this statement. However there were 21 in trashing and 15 IRR respondents who disagreed with the statement and 26 in IRR and 19 in trashing responded as undecided.

The analysis of the above data shows that maximum number of respondents strongly agreed that defecting, investigating & prosecuting offenders. Their output must cater to the actual need, requirements and expectations to implements defecting, investigating & prosecuting offenders.

Table 7 : Achieving the resolution of 55/63 General Assembly.

Achieving the resolution of 55/63	**SA**	**A**	**UD**	**D**	**SD**	**Total**
Waiver of right to object	19	33	15	09	01	77
Arbitration agreement	15	25	21	10	06	77
Power to refer the parties	17	19	27	12	02	77
Decision on matter entrusted	10	36	19	09	03	77

Source : Data compiled from the questionnaire



Graph 7 : Achieving the resolution of 55/63 General Assembly.

There were 06 in arbitration agreement and 03 in decision in matter entrusted respondents who did strongly disagree respond to this question. 36 in decision on matter entrusted and 33 waiver of right to object respondents agreed that recognized achieving the resolution of 55/63 General Assembly. 19 in waiver of right to object and 17 in power to refer the parties' respondents strongly agreed to this statement. However there were 12 in power to refer the parties and 10 arbitration agreement respondents who disagreed with the statement and 27 in power to refer the parties and 21 arbitration agreements responded as undecided.

The analysis of the above data shows that maximum number of respondents strongly agreed that achieving the resolution of 55/63 General Assembly. Their output must cater to the actual need, requirements and expectations to implements achieving the resolution of 55/63 General Assembly.

III. 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. 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. The investigating authority, like cyber cell of Police Commissioner Office & Cyber computer forensics labs should be equipped with latest software like Header Analyzer Software, Advanced Search Software, Steganography Software Password Cracking Tools, Disc Imaging Tools, Image Recovery Tools & hardware like powerful computer system with standard peripherals like CD ROM drivers & CD- Writers, desktop and laser printers, scanners Card readers for examinations of various kinds of cards that store data used for authentication & communication, eg – SMART cards, Micro Drivers, GSM SIM Cards etc. & latest software required for investigation.

The number of forensic labs should be increased by considering cyber crime cases. The latest software should be equipped in the cyber / computer forensic labs so that the forensics report can be sent back to the police authority as early as possible so that police can file charge sheet in the concerned court of law according to the jurisdiction.

REFERENCES

[1] Casey, E.. *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet.* San Diego, CA: Academic Press.

[2] Icove, 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. From September 2013 to till date he is working as Asst. Professor at Ideal Institute of Management(IIMK), Kondigre – Ichalkaranji (MS). He has published more than 27 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.

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.

S. M. Khandke was born in India, Maharashtra, in 1982. He received the BSc, MCA degrees from Shivaji University, Kolhapur (MS). From 2008-2009 he was worked as lecturer at KES KRP ACS College, Islampur. From 2009-2013 he was worked as lecturer at D. R. Mane College, Kagal. From 2013 to till date he is working as Asst. Professor at Ideal Institute of Management(IIMK), Kondigre – Ichalkaranji (MS). His research interest includes Cyber Crime, Information Security, and ICT.

