IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727,
PP 18-21
www.iosrjournals.org

Hurdles in Cyber Forensic Investigation in India

Kirankumar Akate Patil[1], Shrinivas Vyawahare[2,] Kiran Shejul[3] Madhuri Girase[4]
[1](Computer Department, Shivchhatrapati College) Aurangabad)
[2, 3, 4](Computer department, Shivchhatrapati College Aurangabad)

Abstract: *This current era can be called as era of science and technology. With the access use of computers and technology, Criminals have changed their modus operandi. This paper reveals the issues which are faced while handling Cybercrime investigations and which unknowingly slows down the investigation and conviction process at par.*

Keywords: *Cybercrime, documentation, hurdles, Investigation, Pre processing,*

I. Introduction

Cyber-crime is any criminal activity committed with the help of computer, where computers are used as tool or target or both. It differs from physical or "terrestrial" crime in four main ways:

1. Being easy to commit
2. Requiring minimal resources for great potential damage
3. Being committable in a jurisdiction in which the perpetrator is not physically present
4. Often, not being entirely clearly illegal

Virtually any crime, from vandalism to theft, extortion to copyright infringement, can become a cyber-crime. This has created a tremendous challenge for law enforcement or investigation agencies to develop the capacity to confront transnational crimes and follow evidence trails. During the investigation the team of experts or law enforcement agency faces a lot of hurdles. Therefore presenting correct evidences in court of law is must, so the court can gives relevant judgment on the basis of the same.

1.1 Pre-processing (Initial information gathering):

Investigation generally begins by gathering initial information from a variety of sources. Investigators have to understand the characteristics and develop the sources. Information gathering to combat cybercrime should be strategic. System managers and other personnel are potential great informers in important cases. Gathering information from resources is desirable and is encouraged.

1.2 Hurdle's during investigation: [3]

- Unclear Photographs of the evidences such as monitors, CD/DVDs, and other evidences present at the crime scene.
- Power loss or unavailability of power when investigators dealing with volatile evidences present in RAM (Random Access Memory). [3]
- Non availability of sophisticated tools or software's required for collection of information from volatile memory.
- Criminals use more specialized tools for committing crime.
- Lack of the knowledge of standard procedure while dealing with evidences.
- Non availability of skilled cyber investigator.
- Unsafe handling of fragile evidences during transportation
- Unsafe storage of evidences like computers, hard disk drive, CD/DVD, pen drive, etc. [3]
- Improper documentation or chain of custody.

1.2 Challenges:

Cyber-crimes are highly technical as compared to other crimes, so cyber crimes should be investigated at the earliest cause the traces and evidence in cyber space can be easily destroyed. [2]

- A Cyber crime has a borderless scope.
- Tracking the origin of crime is the more prominent challenge in front of investigators. [4]
- Widespread use of pirated software results victimization of user.
- In India one has to obtain courts permission to engage e-surveillance on culprit's network/activity.
- Cyber law in India is not complete.

- India has very few International collaboration which again results as a hurdle in respect to handing over criminals who commit computer crime.

1.3 Consequences of ineffective cyber forensic investigation:

As the report generated by national crime record bureau (NCRB) of India cyber crime are continuously increasing. But because of ineffective investigation the percentage of solved cases are low. NCRB serve report 2015-16 [1]

Sr. no.	**States/UT**	**IT Act**			**IPC Section**		
		2014	**2015**	**%variation**	**2014**	**2015**	**%variation**
1	Andhra Pradesh	349	429	22.9	23	25	8.7
2	Arunachal Pradesh	13	12	-7.7	1	0	-100.0
3	Assam	31	12	-9.7	0	0	0
4	Bihar	25	23	-8.0	13	7	-46.2
5	Chhattisgarh	2	49	2350.0	76	10	-86.8
6	Goa	16	30	87.5	2	2	0.0
7	Gujarat	52	68	30.8	15	10	-33.3
8	Haryana	42	66	57.1	3	116	3766.7
9	Himachal Pradesh	12	20	66.7	0	0	0
10	Jammu & Kashmir	14	35	150.0	0	0	0
11	Jharkhand	8	10	25.0	25	25	0.0
12	Karnataka	151	412	172.8	9	25	177.8
13	Kerala	227	269	18.5	18	43	138.9
14	Madhya Pradesh	90	142	57.8	13	55	323.1
15	Maharashtra	306	471	53.9	87	90	3.4
16	Manipur	0	0	0	0	0	0
17	Meghalaya	6	6	0.0	0	0	0
18	Mizoram	3	0	-100.0	0	0	0
19	Nagaland	0	0	0	0	0	0
20	Orissa	7	14	100.0	5	13	160.0
21	Punjab	59	72	22.0	20	6	-70.0
22	Rajasthan	122	147	20.5	24	7	-70.0
23	Sikkim	3	0	-100.0	1	0	-100.0
37	Tamil Nadu	37	39	5.4	8	2	-75.0
25	Tripura	0	14	0	0	0	0
26	Uttar Pradesh	101	205	103	13	44	238.5
27	Uttarakhand	101	205	103.0	13	44	238.5
28	West Bengal	6	4	-33.3	0	0	0
29	A&N island	0	2	0	0	0	0
30	Chandigarh	10	33	230.0	0	0	0
31	D & N Haveli	3	0	-100.0	3	0	-100.0
32	Daman & Diu	3	0	-100.0	3	0	-100.0
33	Delhi	50	76	52.0	49	8	-83.7
34	Lakshadweep	0	0	0	0	0	0
35	Pondicherry	2	4	100.0	0	0	0
	Total (India)	1791	2876	60.6	422	601	42.4

- **Scenario of metro cities in Maharashtra state:**

Sr.no.	**Cities**	**IT Act**			**IPC Section**		
		2014	**2015**	**%variation**	**2014**	**2015**	**%variation**
1	Aurangabad	19	31	63.2	5	0	-100.0
2	Nasik	2	11	450.0	3	2	-33.3
3	Pune	83	76	-8.4	0	32	@
4	Mumbai	8	33	312.2	25	72	188.0

- **Persons Arrested Under IT Act By Age Group During 2015-16 (States & UTs)**

Sr.no.	State/UT	Below 18yrs	Below 18-30yrs	Below 30-45yrs	Below 45-60yrs	Below 60yrs	Total
1	Andhra Pradesh	0	125	35	10	0	170
2	Arunachal Pradesh	0	0	3	3	0	6
3	Assam	0	5	0	0	0	5
4	Bihar	0	14	3	0	0	17
5	Chhattisgarh	4	25	2	0	0	31
6	Goa	1	3	5	1	0	10
7	Gujarat	1	41	23	7	0	72
8	Haryana	0	12	12	1	0	25
9	Himachal Pradesh	3	19	1	2	0	25
10	Jammu & Kashmir	0	11	6	0	0	17
11	Jharkhand	0	8	0	0	0	8
12	Karnataka	3	35	24	4	0	66
13	Kerala	15	81	44	11	0	151
14	Madhya Pradesh	13	105	32	2	0	152
15	Maharashtra	9	215	75	24	1	324
16	Manipur	0	0	0	0	0	0
17	Meghalaya	0	0	0	0	0	0
18	Mizoram	0	0	0	0	0	0
19	Nagaland	0	0	0	0	0	0
20	Odisha	0	0	1	0	0	1
21	Punjab	0	22	56	8	0	86
22	Rajasthan	13	55	18	4	0	90
23	Sikkim	0	0	0	0	0	0
24	Tamil Nadu	1	20	8	3	1	33
25	Tripura	0	7	3	0	0	10
26	Uttar Pradesh	0	60	47	4	1	142
27	Uttarakhand	0	2	0	0	0	2
28	West Bengal	2	43	22	6	0	73
29	A & N Islands	0	0	0	0	0	0
30	Chandigarh	0	3	2	0	0	5
31	D & N Haveli	0	0	0	0	0	0
32	Daman & Diu	0	0	0	0	0	0
33	Delhi	0	17	10	0	0	27
34	Lakshadweep	0	0	0	0	0	0
35	Pondicherry	0	0	4	0	0	4
Total		65	908	420	90	3	1486

- **Scenario of metro cities in Maharashtra state:**

Sr.no.	UT	Below 18yrs	Below 18 30yrs	Below 30-45yrs	Below 45-60yrs	Below 60yrs	Total
01	AURANGABAD	0	17	3	0	0	20
02	MUMBAI	0	4	7	6	0	17
03	NASIK	0	6	4	1	0	11
04	PUNE	0	23	12	3	0	38

1.4 Precautions:

Precautions taken during seizing, searching, collecting and packaging of computer evidences; [5]

• Photography and Sketching:

Taking pictures of front view and rear view of system, peripherals, monitor and other necessary objects.

• Collecting Volatile Information:

The Cyber Terror Response Centre provides automated tool called “Podomi” is highly recommended for collecting volatile evidence.

• Shutting Down:

The decision of how to shut a system down should depend on the operating system being used. Roughly, server systems follow a normal shut down process and personal computers are unplugged directly.

• Acquiring Physical Media: [6]

Seizing whole systems is principally recommended, some time storage media such as Hard Disk Drive (HDD) are seized separately.

• Labeling and Packaging:

An adequate label should be attached to each item, including case number, collector, date and time, location, specification of the item, serial number if possible, etc. HDD and other electro-magnetic media should be packed individually using proper bags or boxes;

• Documentation: [8]

Chain of custody, process of scene investigation, lists of evidences, interrogation report of suspect and statement of witness (if any) should be documented and preserved·

- **Storage:**[7]

Digital evidences should be protected from;

1. Heat
2. Extreme cold
3. Humidity
4. Water
5. Magnetic fields
6. Vibration

The evidence should be protected for use in court and for returning them to the legitimate owner.

II. Conclusion

It has been observed that due to lack of knowledge and advancements, cyber wings in India are struggling while combating with cyber crimes, this paper presented some issue which should be focused on while dealing with computers crimes and evidences, which will help the investigating authority to upgrade against present scenario.

References

[1]. Crime in India 2015 Statics. – national crime record bureau (NCRB)

[2]. Cyber crime – a growing challenge for government.- July 2014

[3]. Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations

[4]. H. Marshall Jarrett Director, EOUSA . Michael W. Bailie Director, OLE

[5]. ACPO computer evidences and guidelines. (www.acpo.police.uk)

[6]. Baggili et al, 2007 Ibrahim M. Baggili, Richard Mislan, Marcus Rogers, “Mobile Phone Forensics Tool Testing: A Database Driven Approach”, International Journal of Digital Evidence Fall 2007, Vol. 6, Issue 2

[7]. Jansen, Ayers, 2006 Wayne Jansen, Rick Ayers, “Forensic Software Tools for Cell Phone Subscriber Identity Modules”, Conference on Digital Forensics, Security and Law, 2006

[8]. Marcella, Albert, 2008 Marcella Jr., Albert J., “Cyber Forensics: A Field Manual for Collecting, Examining and Preserving Evidence of Computer Crimes”. 2008. Taylor & Francis Group, LLC. Auerbach Publications. pp. 27-48 pp.77-85 pp.87. 118 International Journal of Computer Science, Systems Engineering and Information Technology

[9]. Rogers, 2006 Rogers, M. (2006), “DCSA: A Practical Approach to Digital Crime Scene Analysis”. West Lafayette, Purdue University.