International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT22815

Cyber Psychological Case Studies of Sextortion for Identifying the Accused in the Offences Committed on Social Media

Sarthak Rathod[1], Akhlesh Kumar[2], Dr. S. K. Jain[3]

[1]Forensic Professional (FPACT PLUS), Central Forensic Science Laboratory, Chandigarh. DFSS, MHA, Government of India

[2]Assistant Director & Scientist – 'C', Central Forensic Science Laboratory, Chandigarh. DFSS, MHA, Government of India

[3]Director-cum-Chief Forensic Scientist, Central Forensic Science Laboratory, Chandigarh. DFSS, MHA, Government of India

Article Info
Volume 8, Issue 1
Page Number : 42-52

Publication Issue :
January-February-2022

Article History
Accepted : 02 Jan 2022
Published : 12 Jan 2022

ABSTRACT

Human behaviors can never fail to astound society. People behave as they want in their privacy and sometimes it can be weirdest, dark, and taboo. Sex is not a routine and normal topic in the conversation of Indian society. Therefore, people are very secretive about their sexual beliefs, thoughts, and sexuality. Whenever anybody does anything where she/he knows that their act is not going to be known by others people tend to involve in such acts. This is the exact angle that blackmailers in sextortion have identified and they get success too in duping people. They threaten people to viral their videos or chat in the sexual act. But, the Majority of the crimes committed on social media go unreported or untraced. Due to lack of procedural setups to identify the accuses. especially in the cases of sextortion where name and shame in the society are attacked of any individual. The present research paper aims to provide a simple procedural method to identify the accused in the offences committed on social media. The authors of the research paper have chatted with the 11 blackmailers of sextortion on social media and the authors were able to identify the location of the accused. The research paper is attempting to explain the dynamics of crime and victimization of sextortion from a cyber psychological perspective.

words: Cyber Psychology, Sextortion, Cyber Crime, Cyber Forensics, Online Blackmailing, Phishing, Organized Crime, Intimate Photo/Video, Nude Video Call

I. INTRODUCTION

There were 4.66 billion active internet users in January 2021, accounting for 59.5 percent of the world's population. 92.6 percent of the total (4.32 billion) used mobile devices to access the internet. (Johnson, 2021). India has the world's second-largest internet population. (Keelery, 2021). The number of

cybercrimes recorded in India increased significantly in 2020 compared to the previous year. Over 50 thousand cybercrime occurrences were reported in that year. During the time period studied, Karnataka and Uttar Pradesh had the largest proportion. In comparison to the rest of the country, the northern state of Uttar Pradesh had the largest number of cybercrimes, with over 6,000 incidents reported to authorities in 2018. Karnataka, India's IT state, followed suit the next year. The bulk of these complaints was filed under the Information Technology Act with the intent of defrauding or sexually exploiting victims. Consumers in India lost approximately 18 billion dollars in 2017 as a result of cybercrime, according to estimates. These were, however, projections based only on published data. Because of a lack of cybercrime knowledge and classification procedures in a nation like India, the true statistics are likely to be under-reported. Recent government measures, such as a dedicated online platform for reporting cybercrimes, might very well be the driving force behind an increase in online crimes starting in 2017. (Keelery, 2021)

Following cybercrimes are known offenses committed in cyberspace:

(1.) Cyber Stalking: The use of the Internet or other electronic methods to stalk or harass a person, group, or organization is known as cyberstalking. False charges, defamation, slander, and libel are all examples. It may also entail surveillance, identity theft, threats, vandalism, sex solicitation, doxing, or blackmail (Oxford Press, n.d.).

(2.) Cyber Defamation: Cyber defamation is not a specific criminal violation, crime, or tort, but rather defamation or insult committed using digital means, most commonly the Internet (Chhetri, 2021).

(3.) Cyber Pornography: Cyber pornography is any pornography that is available over the internet, typically through websites, FTP servers, peer-to-peer file sharing, or Usenet newsgroups. The advent of extensive public access to the World Wide Web in the late 1990s fueled the proliferation of Cyber pornography (Internet pornography, n.d.).

(4.) Morphing: Morphing is the process of seamlessly transitioning from one image to another without making any adjustments utilizing online morphing tools. Usually, girls are harmed by this sort of morphing, which involves downloading photographs of girls from various social media sites via false or genuine profiles and then morphing them. By threatening to publish the modified photographs, these images might be used to blackmail the girl or her family (Morphing, 2021).

(5.) Trolling: Criminal intimidation, sexual harassment, defamation, voyeurism, online stalking, and obscene content are among provisions that trolling victims might use to seek restitution. Obtaining legal recourse, on the other hand, lays the responsibility on the target. Trolling and bullying are not defined under the Indian Penal Code of 1860. Various parts of the Code, when interpreted in conjunction with the Information Technology Act of 2000 ("IT Act"), can be utilized to combat cyberbullies and trolls (Mishra, 2021).

(6.) Identity Theft: Identity theft is a crime in which an attacker obtains personal or sensitive information from a victim through deceit or fraud and then utilizes that information to act in the victim's identity. Typically, such criminals are motivated by personal financial gain (Identity Theft, n.d.).

(7.) Cyber Bullying / Online Harassment: Cyberbullying is a type of online harassment in which an individual or group bullies a victim through the use of the Internet and/or other electronic communication means (Cross, 2014).

(8.) Invasion of Privacy: Hacking, malware, identity theft, financial fraud, medical fraud, and some offences against persons that entail the disclosing of personal information, communications,

photographs, and video and audio recordings without the agreement or authorization of the individuals are examples of cybercrime (UNODC, n.d.).

(9.) Dating Scams: A dating/romance scam is a confidence trick in which the scammer pretends to have romantic feelings for a victim to acquire their affection and then uses that goodwill to persuade the victim to send money to the scammer under pretenses or to commit fraud against the victim. (Foxworth, 2014) Access to the victim's money, bank accounts, credit cards, passports, e-mail accounts, or national identification numbers may be obtained through fraudulent acts, as well as forcing the victims to commit financial fraud on their behalf (Hickey, 2015).

(10.) Cyber Grooming: The technique of 'befriending' a young person online " to enable online sexual interaction and/or a physical meeting with them with the intention of committing sexual abuse" is known as cyber grooming (Child Safe Net, n.d.).

Following cybercrimes are new forms of offences committed in cyberspace:

(1.) Online Virginity Sell/Auction: A virginity auction is an online auction in which a person attempts to sell their virginity. The highest bidder will have the opportunity to have intercourse with the individual first.

(2.) Revenge Porn: The dissemination of sexually graphic photos or films of persons without their agreement is known as revenge porn (Citron & Franks, 2014). The offenders may use the material to blackmail the subjects into performing more sex acts, pressure them into maintaining a relationship or punishing them for terminating one, silence them, harm their reputation, and/or profit financially (Bates, 2015).

(3.) Cyber Prostitution: Obscene and indecent behaviours centered on virtual sexual stimulation and/or intercourse for the purpose of making money or profit (Cabral, 2006).

(4.) Sextortion: Sextortion is the act of threatening to disclose proof of someone's sexual conduct in exchange for money or sexual favours (Definitions from Oxford Languages).

The present study focuses on sextortion offences trending rapidly in India. Modus operandi on Indian sextortion cases are very different from than western world. Authors have published a research paper earlier on a case study of sextortion titled "Tracing of the Blackmailers in Sextortion Case and Tactics to Defend It - An Experimental Cybercrime Case Study" (Rathod, S., 2021). The research paper explained the modus operandi of blackmailers in a sextortion case. How they lure innocent people from Facebook and Instagram. They create a fake Facebook account with a display picture of a female on it. They sent friend requests to a lot of people who may be a suitable target for them. Those who get lured into this, chat with them in the messenger and invite them on WhatsApp for further chat and eventually to have a nude video call. Actually, in the video call, they show a porn video where a young girl is undressing and blackmailers record the entire video call through a screen recorder. Then blackmailers extort the money from the victims threatening to viral the video.

The point of the study is how authors successfully traced a blackmailer's location using a method. Also, explained the tactics to defend the same in the aforementioned research paper. In the present study, authors have successfully traced 11 blackmailers using the same method.

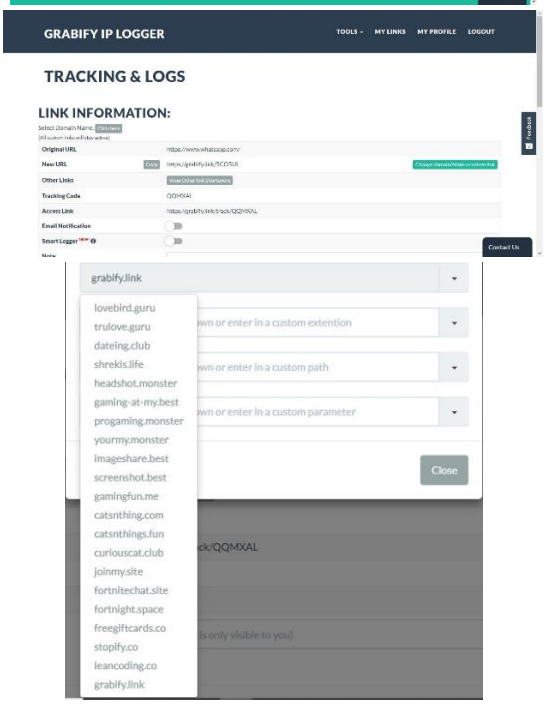
Method

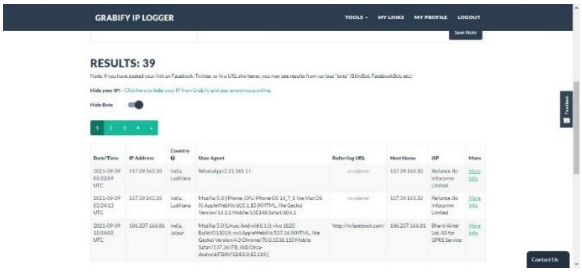
The authors have traced the location in three steps. The steps are as follows.

Step: 1 Getting the IP Address of the device used in the offence:

An Internet Protocol (IP) address, such as 192.0.2.1, is a numerical designation associated with a computer network that communicates using the Internet Protocol. An IP address is used for two purposes: identifying a host or network interface, and addressing a specific location. Few IP Logger websites allow any user to make a spoof link in order to get the IP address of anyone who clicks on the link. A spoofed URL/Link refers to a website that pretends to be another website. Two websites are very famous for this. One is https://grabify.link/ and another is https://iplogger.org/

Grabify portal has been used in the present study for making a spoof link. Any link can be used to make a spoof link. Authors have used www.whatsapp.com because blackmailers generally divert chats from Facebook to WhatsApp. While chatting with the blackmailers authors convinces them to click on the link so they will reach the WhatsApp chat only. And blackmailers did click on the links. Screenshots of the process are herewith.



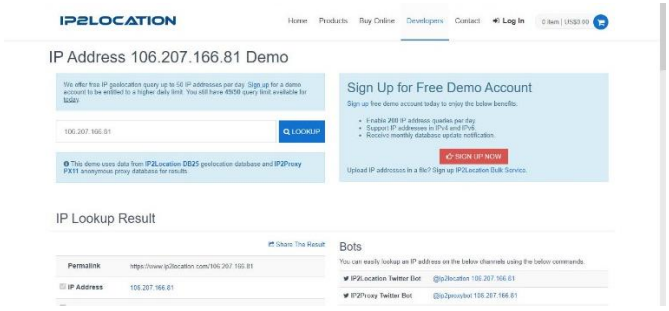


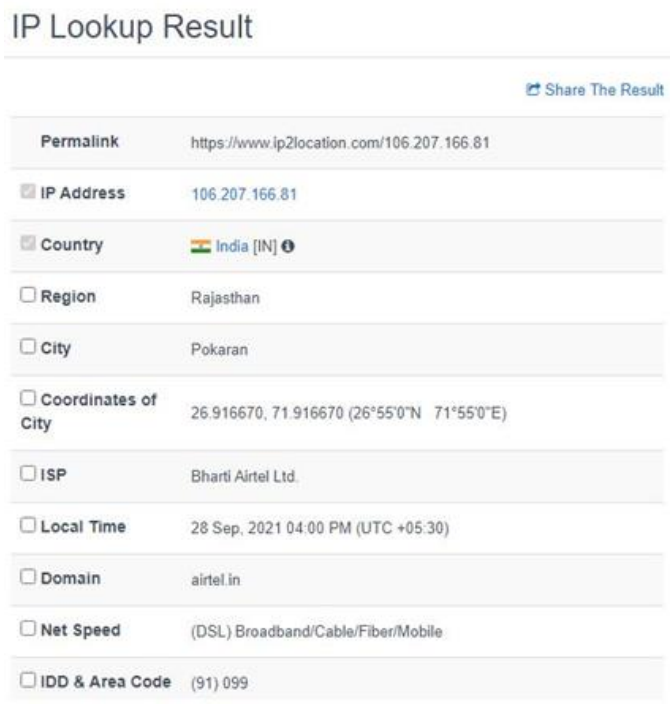
Step: 2 Getting Coordinates from the IP Address:

Grabify gives the IP address at the last stage of the process. Then authors got the coordinates of the blackmailers from the IP addresses. There are two major websites/portals that allow any user to locate

the coordinates using the IP address. One is https://ipinfo.io/ and another is https://www.ip2location.com/

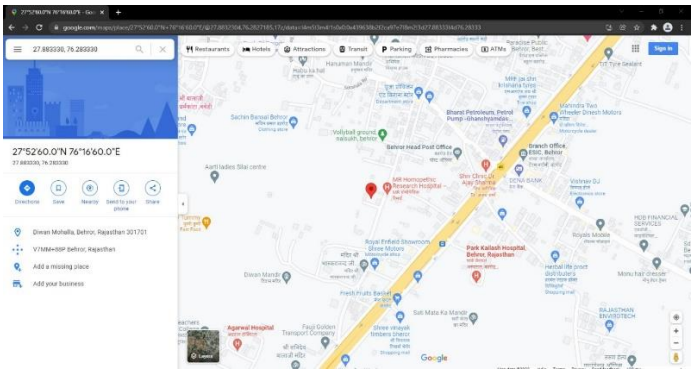
The authors have used the IP2location website in the present study to get the coordinates. The website is very simple to use. Screenshots of the process are herewith.



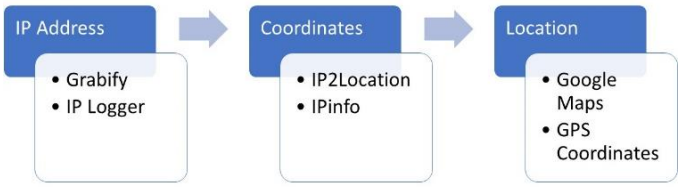


Step: 3 Tracing the location from Coordinates:

Step 2 provides coordinates of the IP address. In this step, the authors have identified the location of the accused from coordinates. This can be done using any of the map services. Like https://www.google.com/maps or https://www.google.com/maps



In the present study, authors have successfully traced 11 blackmailers locations using the same method. A graphical representation is shown below.



Results

Sextortion is one of the most growing cyber crimes in India. Every other Facebook user gets a lot of friend requests from a stranger and an unknown person daily. Similarly, authors have also received this kind of fake Facebook request. Authors have conducted chats with the blackmailers in order to identify the accused location. The authors have followed the method mentioned above. After completing the process authors were able to detect the location and other details of the various accuses. Screenshots below are shown for the same.

ADVANCED LOG

Date/Time	2021-09-09 15:54:05 UTC
IP Address	106.207.166.81
Country	India, Jaipur
Browser	Facebook (324.0.0.15.119)
Operating System	Android 8.1.0
Device	Vivo Y91i
User Agent	Mozilla/5.0 (Linux; Android 8.1.0; vivo 1820 Build/O11019; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/70.0.3538.110 Mobile Safari/537.36 [FB_IAB/Orca-Android;FBAV/324.0.0.15.119;]
Referring URL	http://m.facebook.com/
Host Name	106.207.166.81
ISP	Bharti Airtel Ltd. AS for GPRS Service

Image - 1

ADVANCED LOG

Date/Time	2021-09-20 09:21:44 UTC
IP Address	106.207.153.221
Country	India, Jaipur
Browser	Facebook (329.0.0.12.118)
Operating System	Android 11
Device	Vivo Y11
User Agent	Mozilla/5.0 (Linux; Android 11; vivo 1906 Build/RP1A.200720.012; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/83.0.4103.106 Mobile Safari/537.36 [FB_IAB/Orca-Android;FBAV/329.0.0.12.118;]
Referring URL	https://l.facebook.com/
Host Name	106.207.153.221
ISP	Bharti Airtel Ltd. AS for GPRS Service

Image - 2

ADVANCED LOG

Date/Time	2021-09-15 16:47:00 UTC
IP Address	106.207.191.158
Country	India, Jaipur
Browser	Facebook (329.0.0.12.118)
Operating System	Android 11
Device	OPPO F11 Pro
User Agent	Mozilla/5.0 (Linux; Android 11; CPH1969 Build/RP1A.200720.011; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/87.0.4280.141 Mobile Safari/537.36 [FB_IAB/Orca-Android;FBAV/329.0.0.12.118;]
Referring URL	http://m.facebook.com/
Host Name	106.207.191.158
ISP	Bharti Airtel Ltd. AS for GPRS Service

Image - 3

ADVANCED LOG

Date/Time	2021-09-16 12:02:38 UTC
IP Address	106.207.200.71
Country	India, Jaipur
Browser	Facebook (329.0.0.12.118)
Operating System	Android 10
Device	Vivo Y30
User Agent	Mozilla/5.0 (Linux; Android 10; vivo 1938 Build/QP1A.190711.020; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/78.0.3904.96 Mobile Safari/537.36 [FB_IAB/Orca-Android;FBAV/329.0.0.12.118;]
Referring URL	http://m.facebook.com/
Host Name	106.207.200.71
ISP	Bharti Airtel Ltd. AS for GPRS Service

Image – 4

ADVANCED LOG

Date/Time	2021-09-20 08:53:33 UTC
IP Address	106.207.141.40
Country	India, Jaipur
Browser	Facebook (329.0.0.12.118)
Operating System	Android 11
Device	Vivo Y11
User Agent	Mozilla/5.0 (Linux; Android 11; vivo 1906 Build/RP1A.200720.012; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/83.0.4103.106 Mobile Safari/537.36 [FB_IAB/Orca-Android;FBAV/329.0.0.12.118;]
Referring URL	https://l.facebook.com/
Host Name	106.207.141.40
ISP	Bharti Airtel Ltd. AS for GPRS Service

Image – 5

ADVANCED LOG

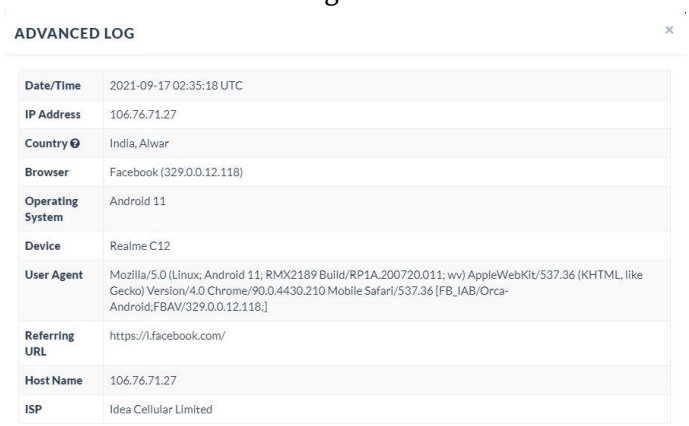
Date/Time	2021-09-14 14:55:58 UTC
IP Address	106.207.151.211
Country	India, Jaipur
Browser	Facebook (327.1.0.9.118)
Operating System	Android 10
Device	Vivo Y20
User Agent	Mozilla/5.0 (Linux; Android 10; V2027 Build/QP1A.190711.020; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/80.0.3987.99 Mobile Safari/537.36 [FB_IAB/Orca-Android;FBAV/327.1.0.9.118;]
Referring URL	http://m.facebook.com/
Host Name	106.207.151.211
ISP	Bharti Airtel Ltd. AS for GPRS Service

Image – 6

ADVANCED LOG

Date/Time	2021-09-21 09:56:35 UTC
IP Address	106.207.194.97
Country	India, Jaipur
Browser	Facebook (330.0.0.12.116)
Operating System	Android 10
Device	Vivo Y30
User Agent	Mozilla/5.0 (Linux; Android 10; vivo 1938 Build/QP1A.190711.020; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/78.0.3904.96 Mobile Safari/537.36 [FB_IAB/Orca-Android;FBAV/330.0.0.12.116;]
Referring URL	http://m.facebook.com/
Host Name	106.207.194.97
ISP	Bharti Airtel Ltd. AS for GPRS Service

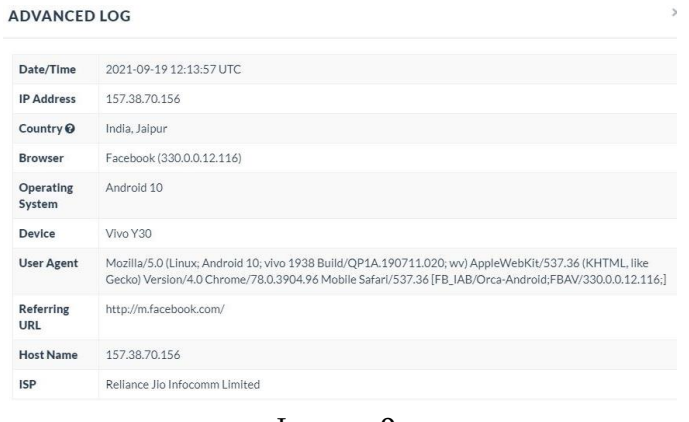
Image – 7



ADVANCED LOG

Date/Time	2021-09-17 02:35:18 UTC
IP Address	106.76.71.27
Country	India, Alwar
Browser	Facebook (329.0.0.12.118)
Operating System	Android 11
Device	Realme C12
User Agent	Mozilla/5.0 (Linux; Android 11; RMX2189 Build/RP1A.200720.011; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/90.0.4430.210 Mobile Safari/537.36 [FB_IAB/Orca-Android;FBAV/329.0.0.12.118;]
Referring URL	https://l.facebook.com/
Host Name	106.76.71.27
ISP	Idea Cellular Limited

Image – 8



ADVANCED LOG

Date/Time	2021-09-19 12:13:57 UTC
IP Address	157.38.70.156
Country	India, Jaipur
Browser	Facebook (330.0.0.12.116)
Operating System	Android 10
Device	Vivo Y30
User Agent	Mozilla/5.0 (Linux; Android 10; vivo 1938 Build/QP1A.190711.020; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/78.0.3904.96 Mobile Safari/537.36 [FB_IAB/Orca-Android;FBAV/330.0.0.12.116;]
Referring URL	http://m.facebook.com/
Host Name	157.38.70.156
ISP	Reliance Jio Infocomm Limited

Image – 9

ADVANCED LOG

Date/Time	2021-09-20 07:29:01 UTC
IP Address	106.207.162.21
Country	India, Jaipur
Browser	Facebook (330.0.0.12.116)
Operating System	Android 10
Device	Vivo Y20
User Agent	Mozilla/5.0 (Linux; Android 10; V2027 Build/QP1A.190711.020; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/80.0.3987.99 Mobile Safari/537.36 [FB_IAB/Orca-Android;FBAV/330.0.0.12.116;]
Referring URL	http://m.facebook.com/
Host Name	106.207.162.21
ISP	Bharti Airtel Ltd. AS for GPRS Service

Image – 10

ADVANCED LOG

Date/Time	2021-09-21 04:35:36 UTC
IP Address	157.38.17.57
Country	India, Jaipur
Browser	Facebook (330.0.0.12.116)
Operating System	Android 11
User Agent	Mozilla/5.0 (Linux; Android 11; V2069 Build/RP1A.200720.012; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/83.0.4103.106 Mobile Safari/537.36 [FB_IAB/Orca-Android;FBAV/330.0.0.12.116;]
Referring URL	https://l.facebook.com/
Host Name	157.38.17.57
ISP	Reliance Jio Infocomm Limited

Image – 11

To summarize the results a tabular form has been shown below.

Image No.	IP Address	Device	Service Provider	Coordinates (Longitude and Latitude)	Location
01.	106.207.166.81	Vivo Y91i	Airtel	26.916670, 71.916670 (26°55'0"N 71°55'0"E)	Pokhran, Rajasthan 345021
02.	106.207.151.211	Vivo Y20	Airtel	24.571170, 73.691830 (24°34'16"N 73°41'31"E)	Udaipur, Rajasthan 313001

03.	106.207.191.158	OPPO F11 Pro	Airtel	30.024370, 73.812930 (30°1'28"N 73°48'47"E)	Koni, Rajasthan 335038
04.	106.207.200.71	Vivo Y30	Airtel	26.916670, 75.816670 (26°55'0"N 75°49'0"E)	Mirza Ismail Rd, Panch Batti, Ashok Nagar, Jaipur, Rajasthan 302002
05.	106.207.141.40	Vivo Y11	Airtel		
06.	106.207.153.221	Vivo Y11	Airtel		
07.	106.207.194.97	Vivo Y30	Airtel		
08.	106.76.71.27	Realme C12	Idea	26.397050, 77.413670 (26°23'49.4"N 77°24'49.2"E)	Jhiri, Rajasthan 328026
09.	157.38.70.156	Vivo Y30	Jio	25.183330, 75.833330 (25°10'60.0"N 75°49'60.0"E)	Chambal River, Kota, Rajasthan
10.	106.207.162.21	Vivo Y20	Airtel	27.650000, 74.383330 (27°39'00.0"N 74°22'60.0"E)	Shaheria Bass, Ladnun, Rajasthan 341306
11.	157.38.17.57	NIL	Jio	26.566670, 76.333330 (26°34'0"N 76°19'60"E)	Lalsot, Rajasthan 303503

II. Conclusion

The authors have analyzed the results thoroughly and found out three common factors associated with the modus operandi of the sextortion cases in the present study.

First Factor: Place of crime

Data revealed that all the blackmailers are present across the state of Rajasthan. Numerous incidents of sextortion have been reported from Rajasthan (Mehta, 2021). State police have arrested a numbers person in the connection of sextortion (Taskin, 2021). Still, sextortion cases are growing at a very fast pace and Rajasthan is one of the major leading states in this crime trend. Most youth of the state is involved in criminal gangs. The social capital of the state is not being utilized properly (Lexico Dictionaries, n.d.). The state government may take up the gigantic task of restoring their social capital. otherwise, it seems a never-ending cycle of unemployment will be in the spin very quickly.

Second Factor: Low budget phone

Mobile phones used in the sextortion are Chinese mobile phones. Which are very cheap mobile phones ranging from INR 7,500/- to INR 15,000/-. Mobile Devices are from Vivo, OPPO, and Realme brands which are Chinese brands that are into the business of cheap mobile devices in India. There can be many explanations regarding blackmailers using cheap mobile phones in crime. (1.) to minimize the expenses and earn more profit (2.). In case of emergency when they are about to get trapped by the law enforcement agencies. They can easily break or damage cheap mobile devices. As it does not hold much financial value. (3.) Blackmailers might be a teenager from rural backgrounds who have a cheap mobile device.

They might belong to the low-income class of society. Probably because of unemployment and poverty.

Third Factor: Internet Service Provider

The majority of the blackmailers were using similar internet providers i.e. the Bharti Airtel Limited aka Airtel. The company is one of the largest Indian telecommunication service providers. There have been many incidents where employees or promotors of Airtel have provided fake sim cards using the fake Aadhaar ids (Zee News, 2020).

The majority of the cases go unreported. Cyber victimization has become very frequent in the daily life of any internet user and cyber victimization will prevail in society due to the following reasons:

(1.) The victim thinks him/herself less powerful in front of the crime and victimization happened.
(2.) When a victim loses a very small amount and it makes him/her think of not reporting and forget it.
(3.) Overgeneralization of the fact that cybercrime happens to everyone.
(4.) The lengthy process of reporting cybercrime and dealing with Law enforcement agencies & the criminal justice system.
(5.) High cost of getting justice.
(6.) Victims tend to pay money to protect themselves from getting Expose or shamming in society.

Blackmailers will continue to take the advantage of the mindset of victims of cybercrimes or sextortion. The question is why do blackmailers commit such crimes? And the answer is it is an easy option to earn money rather than earning money the hard way from the mainstream. Cyberspace enables people to commit crimes globally while sitting at any corner of the world.

III. Acknowledgment

We extend our sincere gratitude to Mr. Krishna Parihar, Forensic Professional (Cyber Forensics), Central Forensic Science Laboratory, Chandigarh. DFSS, MHA, Government of India for his valuable inputs.

IV. REFERENCES

[1]. Bates, S. (2015). Stripped": An analysis of revenge porn victims' lives after victimization (Thesis). Simon Fraser University. Retrieved December 15, 2021
[2]. Cabral, E. I. (2006). Delineation of responsibility in the fight against the occurrence and proliferation of cyber pornography/cyber prostitution. Quezon City: Department of Social Welfare and Development, Republic of Phillippines.
[3]. CHHETRI, S. (2021). The Defamation in the Internet Age: Cyber Defamation. International Journal of Law Management & Humanities, 4(1), 1981-1994. DOI:http://doi.one/10.1732/IJLMH.25957
[4]. Citron, D. K., & Franks, M. A. (2014). Criminalizing Revenge Porn. Wake Forest Law Review, 49(2), 345–392.
[5]. Cross, M. (2014). Chapter 7 - The Dark Side. Elsevier. doi:https://doi.org/10.1016/B978-1-59749-986-6.00007-2
[6]. Cyber Grooming. (n.d.). Retrieved December 12, 2021, from www.childsafenet.org: https://www.childsafenet.org/new-page-15
[7]. Definitions from Oxford Languages. (n.d.). Retrieved December 26, 2021
[8]. Foxworth, D. (2014, February 12). Looking for Love? Beware of Online Dating Scams. Retrieved December 11, 2021, from archives.fbi.gov: https://archives.fbi.gov/archives/sandiego/press-releases/2014/looking-for-love-beware-of-online-dating-scams

[9]. Hickey, S. (2015, August 14). Scammers target lonely hearts on dating sites. Retrieved December 11, 2021, from www.theguardian.com: https://www.theguardian.com/money/2015/aug/14/scammers-target-middle-age-women

[10]. Identity Theft. (n.d.). Retrieved December 7, 2021, from www.eset.com: https://www.eset.com/in/identity-theft/

[11]. Internet pornography. (n.d.). Retrieved December 1, 2021, from en.wikipedia.org: https://en.wikipedia.org/wiki/Internet_pornography

[12]. Johnson, J. (2021, September 10). Global digital population as of January 2021(in billions). Retrieved from www.statista.com: https://www.statista.com/statistics/617136/digital-population-worldwide/

[13]. Keelery, S. (2021, October 25). Number of cyber crimes reported across India from 2012 to 2020. Retrieved from www.statista.com: https://www.statista.com/statistics/309435/india-cyber-crime-it-act/

[14]. Keelery, S. (2021, August 17). Number of internet users in India from 2010 to 2020, with estimates until 2040(in millions). Retrieved from www.statista.com: https://www.statista.com/statistics/255146/number-of-internet-users-in-india/

[15]. Mehta, A. (2021, December 12). Sextortion: New way of Rajasthan conmen to trap victims. Retrieved January 03, 2022, from www.timesofindia.indiatimes.com: https://timesofindia.indiatimes.com/city/jaipur/sextortion-new-way-of-mewat-conmen-to-trap-victims/articleshow/88230985.cms

[16]. Mishra, P. (2021, March 15). Explained: What is Online Trolling and Legal Remedies Available to Victims. Retrieved December 06, 2021, from www.news18.com: https://www.news18.com/news/india/explained-what-is-online-trolling-and-legal-remedies-available-to-victims-3536330.html

[17]. Morphing. (2021, January 17). Retrieved December 5, 2021, from www.cybercrimechambers.com: https://www.cybercrimechambers.com/blog-morphing-134.php

[18]. Press, O. U. (n.d.). Retrieved December 1, 2021, from https://languages.oup.com/

[19]. Rathod, S., Gaur, M., Parihar, K., Kumar, A., & Jain, SK. (2021). Tracing of the Blackmailers in Sextortion Case and Tactics to Defend It - An Experimental Cybercrime Case Study. International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), 7(4), 135-142. doi:https://doi.org/10.32628/CSEIT217414

[20]. Sharma, P. (2020, June 20). Three arrested in Faridabad for hacking WhatsApp chat, blackmailing over 100 girls. Retrieved January 05, 2022, from www.zeenews.india.com: https://zeenews.india.com/india/three-arrested-in-faridabad-for-hacking-whatsapp-chat-blackmailing-over-100-girls-2291070.html?utm_campaign=fullarticle&utm_medium=referral&utm_source=inshorts

[21]. social capital. (n.d.). Retrieved January 04, 2022, from Lexico Dictionaries: https://www.lexico.com/en/definition/social_capital

[22]. TASKIN, B. (2021, October 20). How Rajasthan man ran 'sextortion' racket, fleeced Rs 30 lakh from 300-plus victims. Retrieved January 04, 2022, from www.theprint.in: https://theprint.in/india/how-rajasthan-man-ran-sextortion-racket-fleeced-rs-30-lakh-from-300-plus-victims/753237/

[23]. UNODC. (n.d.). Cybercrime that compromises privacy. Retrieved December 9, 2021, from www.unodc.org: https://www.unodc.org/e4j/en/cybercrime/mod

ule-10/key-issues/cybercrime-that-compromises-privacy.html

Cite this article as :

Sarthak Rathod, Akhlesh Kumar, Dr. S. K. Jain, "Cyber Psychological Case Studies of Sextortion for Identifying the Accused in the Offences Committed on Social Media ", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 8 Issue 1, pp. 42-52, January-February 2022. Available at
doi : https://doi.org/10.32628/CSEIT22815
Journal URL : https://ijsrcseit.com/CSEIT22815