The International Journal of Indian Psychology
ISSN 2348-5396 (Online) | ISSN: 2349-3429 (Print)
Volume 9, Issue 3, July- September, 2021
DIP: 18.01.035.20210903, DOI: 10.25215/0903.035
http://www.ijip.in

Case Study

Forensic Psychological Analysis of Call Recording in the Sextortion Case Using LVA Technique - A Crime Case Study

Sarthak Rathod[1]*, Akhlesh Kumar[2], Khevna Maniar[3], Dr. S. K. Jain[4]

ABSTRACT

There were 4.66 billion active internet users globally in January 2021, accounting for 59.5 percent of the global population. 92.6 percent (4.32 billion) of this total used mobile devices to access the internet (Johnson, 2021). With the growing number of internet users and social media platform users, cybercrimes are also growing with new forms coming in now and then. One of the recent trends is Sextortion on social media platforms. Fraudsters ask potential victims to have a nude video call on WhatsApp and they record the act. Then they demand money for not posting it on social media platforms. And they even threaten to send video clips to family members. Trapped victims generally pay the money to get away with the situation. In the present study, one of the victims submitted his call recording with the fraudster, who was claiming to be a major law enforcement agency officer. The fraudster tried to extort the money from the victim on the pretext of taking down the viral video of him in WhatsApp chat. The present research paper is attempting to analyze the audio clip in the Layered Voice Analysis (LVA) Technology. The research paper has explained the analysis process of computerized voice stress analysis of the audio clips. The research paper concluded the case study by explaining the incident through Routine Activity Theory. Analysis of the crime study has proved that fraudster was deceptive in the audio clip using the LVA Technique.

Keywords: *Forensic Psychology, Cyber Crime, Sextortion, Layered Voice Analysis, Cyber Psychology, Criminology*

Cyberspace has become our alternative Avtar. People behave differently in different spaces (Jaishankar, 2008). Any individual will behave differently in physical space and cyberspace. Our online Avatars are far different than the real Avatars. Psychology is a combination of Mind, Feelings, Thoughts, and emotions. Understanding the Psychology

[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]Forensic Professional (FPACT), Central Forensic Science Laboratory, Chandigarh. DFSS, MHA, Government of India
[4]Director-cum-Chief Forensic Scientist, Central Forensic Science Laboratory, Chandigarh. DFSS, MHA, Government of India
*Corresponding Author

Received: June 26, 2021; Revision Received: July 20, 2021; Accepted: August 03, 2021

of any individual was simple through understanding these four combinations. However, after the rise of the digital era, it is very difficult to understand human psychology when it comes to spaces i.e., physical and cyberspaces. Hence, it becomes very challenging in the Forensic setups. Because people leave different types of traces in different spaces.

With the growing need for information and technology in the era of digital and internet different forms of crimes are also being invented and committed. While mentioning the different types of crimes and spaces let us see this in a perspective that wrongdoers need not come into physical spaces while committing cyber frauds unlike traditional crimes like theft and robbery. Cyberspace has given ample amount of opportunity to fraudsters to commit theft and robbery and that too without going into any physical spaces. This has been a driving force for many disciplines such as Psychology, Criminology, and Forensic Science. It is even responsible for the inter-disciplinary understanding of cybercrimes such as Cyber Psychology, Cyber Criminology, and Cyber Forensics. New forms of crimes require new forms of investigation and detection of the crimes. This has even led to a rise in the numbers of cyber police stations, cyber cells, and cyber forensic divisions in the State/Central forensic science laboratories. In addition to this, A Forensic Psychology angle also needs to be added to assist in cyber-crime cases.

There are many cases are registered of frauds through telephonic talk. Where victims have lost their money to fraudsters after giving their details. Few forms of cyber frauds are as follows:

- Bank Frauds: Fraudsters will simply make a random call to the victim, pretending Bank official. They will use very normal and understandable situations such as the victim has a new debit card or there is some money coming in the bank account or some offers by the bank. And if the victim wishes to utilize any of these services, then they have to give One Time Password (OTP) to the fraudster on call. The moment victims give their details and OTP, in the same moment victim lost the money from his/her bank accounts. Money gets transferred to the fraudster's bank account.
- Ponzi Scheme: A Ponzi scheme is a type of fraud in which fraudsters make victims believe that money from more recent investors is used to pay gains to previous investors. The scheme deceives victims into believing that profits are generated through genuine company activity (e.g., product sales or successful investments), while they are ignorant that the funds are coming from other investors. As long as new investors contribute new money and the majority of investors do not demand full repayment and believe in the non-existent assets they are alleged to own, a Ponzi scheme can retain the illusion of a successful business. This type of fraud is very traditional but nowadays fraudsters are using the online platform also to lure the victims into it.
- Online Scams: These are common in the form of advertisements or spam emails/SMS that contain promises of rewards or money. Scams on the internet include alluring offers that are "too good to be true," and when clicked on, can result in malware interfering with and compromising information (Panda Security, 2021).
- Paytm/Google Pay/Phone Pay/UPI Payment Fraud: In recent trends, the fraudster would make a random call to anyone and they will offer a cashback. Fraudsters offer a cashback code/voucher in a lucky draw to the victim. In which the victim has to enter some amount and details in the name of cashback code/voucher instructed by the fraudster on call. If the victim is lured and he/she enters the amount and details then

the money is debited from the victim's account and it gets transfer to the fraudster's account.

- Identity Theft: Identity theft is the theft of another person's personal or financial information to commit fraud, such as making unlawful transactions or purchases, using that person's identity (Kagan, 2021). Identity theft happens when someone, without their permission, uses another person's personal identifying information, such as their name, social security number, or credit card number, to conduct fraud or other crimes. In 1964, the phrase "identity theft" was coined (Oxford English Dictionary Dictionary, 2007).
- Sextortion/Nude Video Call blackmail: Sextortion is the act of threatening to divulge proof of someone's sexual conduct in exchange for money or sexual favors. To extort sexual favors from the victim, sextortion uses non-physical means of coercion. Sextortion refers to both the broad category of sexual exploitation in which abuse of power is used to coerce, and the specific category of sexual exploitation in which threatened publication of sexual photos or information is used to coerce (De la Cerna, 2012).

In the present research paper, an analysis of telephonic conversation was analyzed from the locus of forensic psychology. Call recording of an unreported sextortion incident was received by the authors. The authors decided to analyze the recording using the Layered Voice Analyses (LVA) Technique.

CASE STUDY

Mr. (P) is a 28 years old male living with his family in Ahmedabad City, Gujarat State, India. He was working in a jewelry shop. He was hyperactive in social media like Facebook, Instagram, and WhatsApp. He keeps posting photos of himself and his family members. One fine day he received a new friend request on Facebook from an unknown person. The profile seems to be of a female since the profile picture was of a girl. Mr. P. thought to accept the friend request simply because of interest in the opposite gender. The unknown profile immediately started a conversation on Facebook messenger. Mr. P. also had a conversation in the same place. After talking formally for a while about each other's basic information and common interest, unknown profiles took the conversation ahead and asked Mr. P.'s WhatsApp registered mobile number. Mr. P. gave his mobile number. Unknown profile started the further conversation in WhatsApp. Both continued their chat on WhatsApp. But suddenly, Mr. P. received a video call from the same person and there was a girl naked in the WhatsApp video call. She started a sexually favorable conversation along with showing her body parts. Mr. P. got lured into it and he also participated in the talk. The girl even asked him to show his male sex organ and he participated in this also. Then, the video call quickly ended by the girl and Mr. P. received the screen recording of the video call between them. Immediately, one fraudster called him and threatened him to pay money or else he will spread the video on social media like Facebook, YouTube, Instagram, and WhatsApp. He even threatened Mr. P. that if he will not pay money to him then the fraudster would send this screen recording to his wife and family. Mr. P. got threatened and worried about the situation that his actions will be known to his wife and family. Hence, he decided to pay the money and he became the victim of Sextortion.

Fraudsters became aware of the situation that Mr. P. has become their suitable target since he got ready to pay the money. Initially, the fraudster asked him to pay Ten thousand rupees (INR 10,000/-) as a sextortion and he paid the money. The payment of Mr. P. made fraudsters

extort more money from him. The fraudster again called him and asked to pay more money for deleting the video from all the social media platforms. By this time, fraudsters have understood the psychology of Mr. P. and they knew that he will pay the money. He did pay the money, He paid in total Thirty-Five Thousand Rupees (INR 35,000/-) in Four installments during a week.

Mr. P. was relieved that he has paid the money so now no one will ever know that something like this happened. But the story does not end here. in the following week, Mr. P. received a call from an unknown person stating that he is calling from the Central Bureau of Investigation (CBI), New Delhi. The person introduced himself as a CBI Officer and he even sent him an ID card. Which is shown below.

The ID card is fake. Based on forensic examination of the image it is found that the image is edited. Month and year i.e., Feb 2025 mentioned in the ID card is inserted on the image. In simple words, a fraudster has used an ID card of a person working in the Intelligent Bureau, Ministry of Home Affairs, Government of India. It is a case of Identity Theft. However, He is pretending to be a CBI Officer but actually, CBI and Intelligent Bureau both are different divisions of the Ministry of Home Affairs. Photo, Signatures, Names, and employee codes are masked in the image above to protect the privacy of the person.

During the call, Fraudster instructed Mr. P. that, CBI office, New Delhi has received a case of pornographic content/Video that has gone viral on social media platforms. And the act is a punishable offense under the Information Technology Act. It has become a case of high importance and the video needs to be taken down from social media platforms. To take down the video Mr. P. has to deposit Twenty-Seven Thousand Five Hundred Rupees (INR 27,500/) to the CBI office. Where Two Thousand Five Hundred Rupees (INR 2,500/-) is processing charges and Twenty-Five Thousand Rupees (INR 25,000/-) is the deposit which Mr. P. will receive the refund back after the video has been taken down by the Cyber Experts of the CBI Office. But, to complete the process immediately and close the case, money has to be deposited as soon as possible. Mr. P. negotiated the time frame with him on call. And fraudster allowed him 40 Minutes to pay the money. A screenshot of the chat is shown below.

Forensic examination of this chat revealed that the WhatsApp Number which the fraudster used to chat with Mr. P. is registered with some other name in the Eastern Part of the Uttar Pradesh State, India. He even used an image of a police officer in uniform as the display picture to ensure that Mr. P. will trust him as if he is a CBI Officer. Which can be seen in the image above. The fraudster gave bank details to Mr. P. to deposit the money. Bank details belonged to some other name/person with a bank account in a major private sector bank in Mumbai City, Maharashtra State, India. Photo, Signatures, Names, Employee codes, and Contact Numbers are masked in the image above to protect the privacy of the person. All the information and details used in the incident are fake and created by the fraudster to extort Mr. P. At this point, Mr. P. was worried but he was unable to manage the money. he decides to contact the authors. Mr. P. has recorded their telephonic conversation this time very vigilantly. Since he was already in the trauma of paying a big amount of money earlier. He did not pay the money this time and he submitted the aforementioned screenshots to authors along with the entire call recording of their conversation.

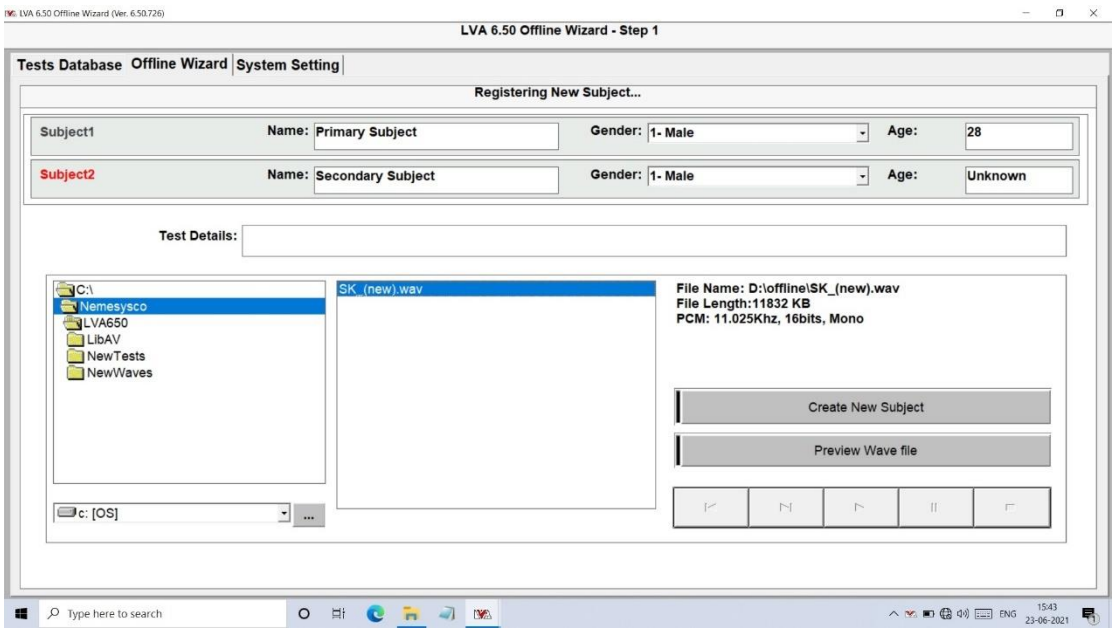
ANALYSIS

The authors decide to test the call recording in the Layered Voice Analysis (LVA) Technology. LVA is a technique of voice stress analysis. Voice stress analysis (VSA) and computer voice stress analysis (CVSA) are two pseudoscientific techniques for inferring deception from voice stress measurements. The CVSA uses a microphone to record the human voice, and the technology is founded on the idea that the non-verbal, low-frequency content of the voice reveals information about the speaker's physiological and psychological

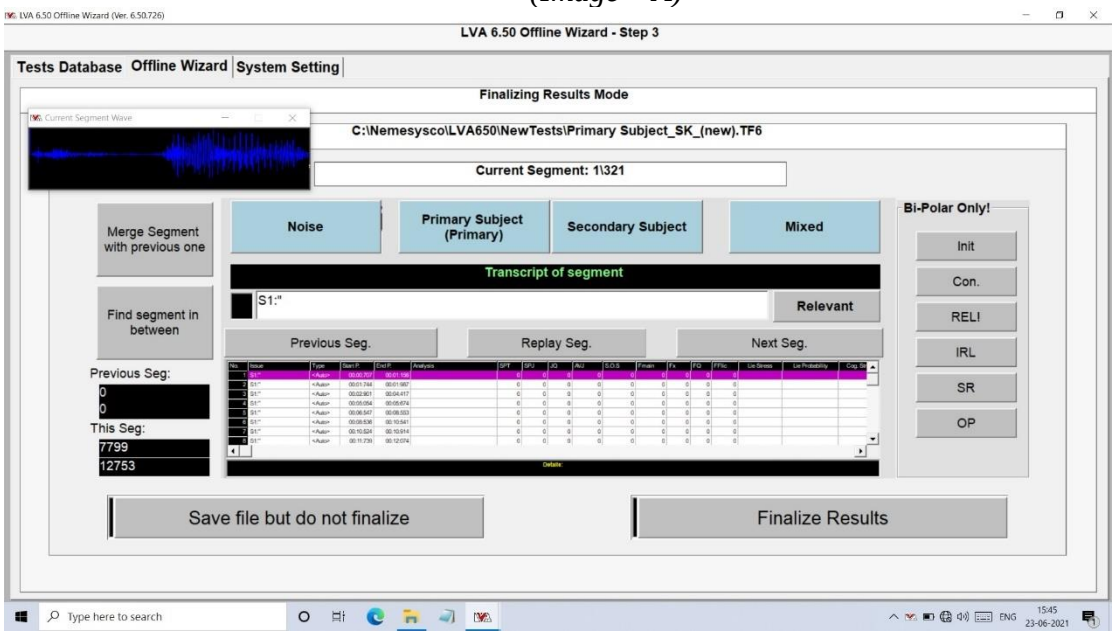
state. The technology, which is most commonly used in investigative situations, tries to distinguish between stressful and non-stressed outputs in response to stimuli (e.g., questions given), with high stress considered as a sign of deceit (National Research Council, 2003). The study of speech sounds for reasons other than linguistic content, such as speech recognition, is known as voice analysis. The majority of these studies include medical voice analysis (phoniatrics), but they also contain speaker identification (Sarangia, Sahidullahb, & Sahaa, 2020). Voice stress analysis or layered voice analysis can be used to identify the sincerity or emotional condition of speakers.

The LVA technology was originally invented in 1997 by Amir Liberman under the company name 'Nemesysco Limited'. The LVA technique is based on a patented set of voice parameters that have been proven to correspond with important human emotions and may be used in various combinations to detect deceptive intentions in "real-life" scenarios. These vocal parameters were discovered using a database of audio files recorded in a variety of settings, including police interrogations and controlled experiments. By identifying hidden emotional indicators in a subject's speech, LVA technology allows for a deeper comprehension of his or her mental state and emotional reaction at any given time. The technology detects a variety of stress levels, cognitive processes, and emotional reactions in the voice, which are reflected in a variety of subtle features. The LVA technology provides information that reveals how the speaker thinks, what bothers him/her, what excites him/her, which parts of his/her speech s/he is unsure of, which questions take more of his/her concentration, and which sections appear to be sensitive topics for the speaker. The LVA technology offers a useful mathematical technique to identify various patterns and abnormalities in speech flow and categories them as stress, excitement, confusion, and other important emotional states, which have been proven to be significantly linked with these emotions over 19 years of study. LVA characteristics focus on the patterns and irregularities in the speech flow rather than the content of what your subject is saying or the language is spoken. LVA also includes capabilities for exploring further into each piece of data that has been recognized. LVA technology may be used in real-time (for a broad overview of any subject/case/suspect/witness) as well as offline (for more in-depth study) mode, with data from nearly any source.

Authors have tested the call recording in the LVA technology to specifically validate the deception of the fraudster and the innocence of Mr. P. in the incident. Call recording was analyzed in the offline mode of the LVA Technique. Because offline mode provides an in-depth detailed analysis of the case compared to online mode. Offline mode is considered the more accurate model of the two. The analysis process starts with loading the audio file in the offline wizard of the LVA system (*Image A*). LVA automatically performs a noise level estimation process. And, it will automatically create vocal segments of up to 2 seconds each from the audio file (*Image B*). Images A and B are shown below.



(Image – A)



(Image – B)

The authors have carefully listened to and reviewed each segment. This process includes marking segments to the belonging speakers or as noise. In this case 'Primary Subject' is Mr. P. and 'Secondary Subject' is the fraudster. Overlapping voices and noises are marked as 'Mixed'. The most relevant segments assuming to be deceptive or important information in the case are marked as 'Relevant'. The LVA system enables the user to merge two segments by marking it as 'Merge Segment with the Previous one'. When a user thinks important information is in between the segment and the entire segment is not necessary It also provides an option to cut the segment and find the segment in between by marking it as 'Find Segment in between'. After all, the segments were reviewed & assigned, and all noises were cleared, results were finalized by clicking the 'Finalize Results' button. The process of analysis provided three levels of messages and all the messages are color-coded for easy identification of the speaker's attributes, which are as follows:

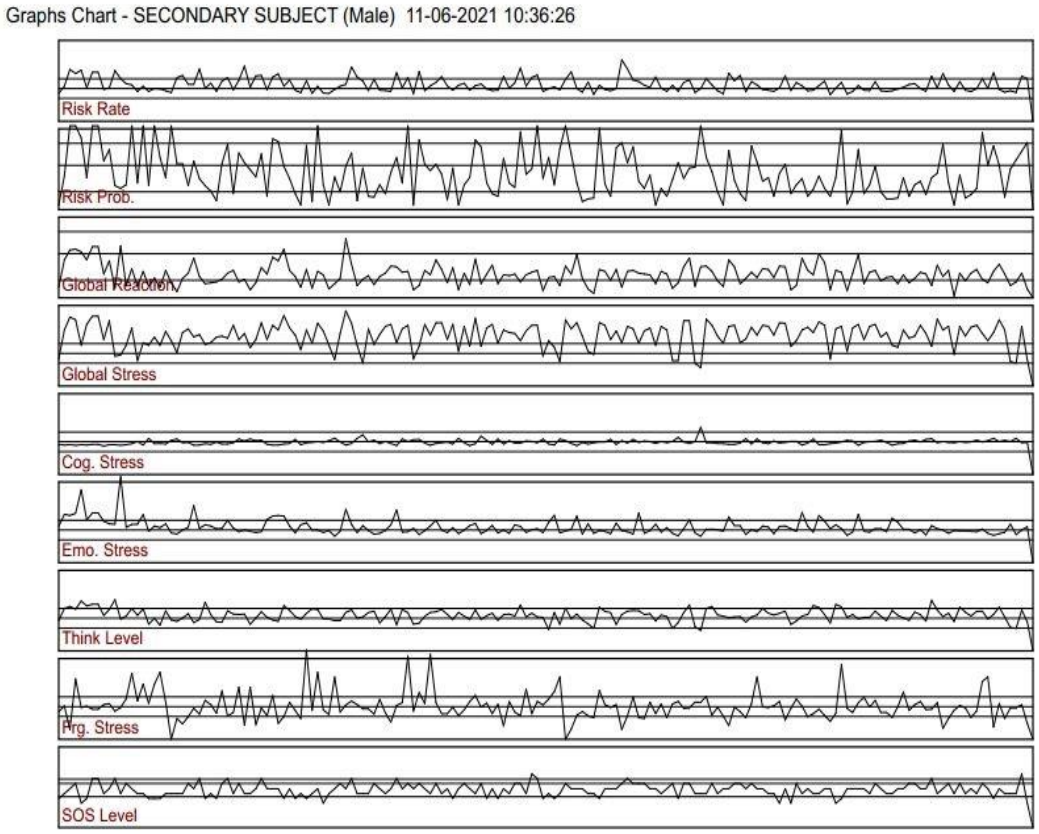
Level – 1 Emotional messages	TRUTH
	HIGH ANTICIPATION
	STRESSED
	EXCITED
	NOT SURE
	HIGH TENSION
Level – 2 Intensive Emotional Reaction messages	HIGHLY STRESSED
	HIGHLY EXCITED
	VOICE MANIPULATION
	EXTREME TENSION
	EXTREME STRESS
Level – 3 Risk messages	INACCURACY
	MEDIUM RISK
	HIGH RISK-FALSE

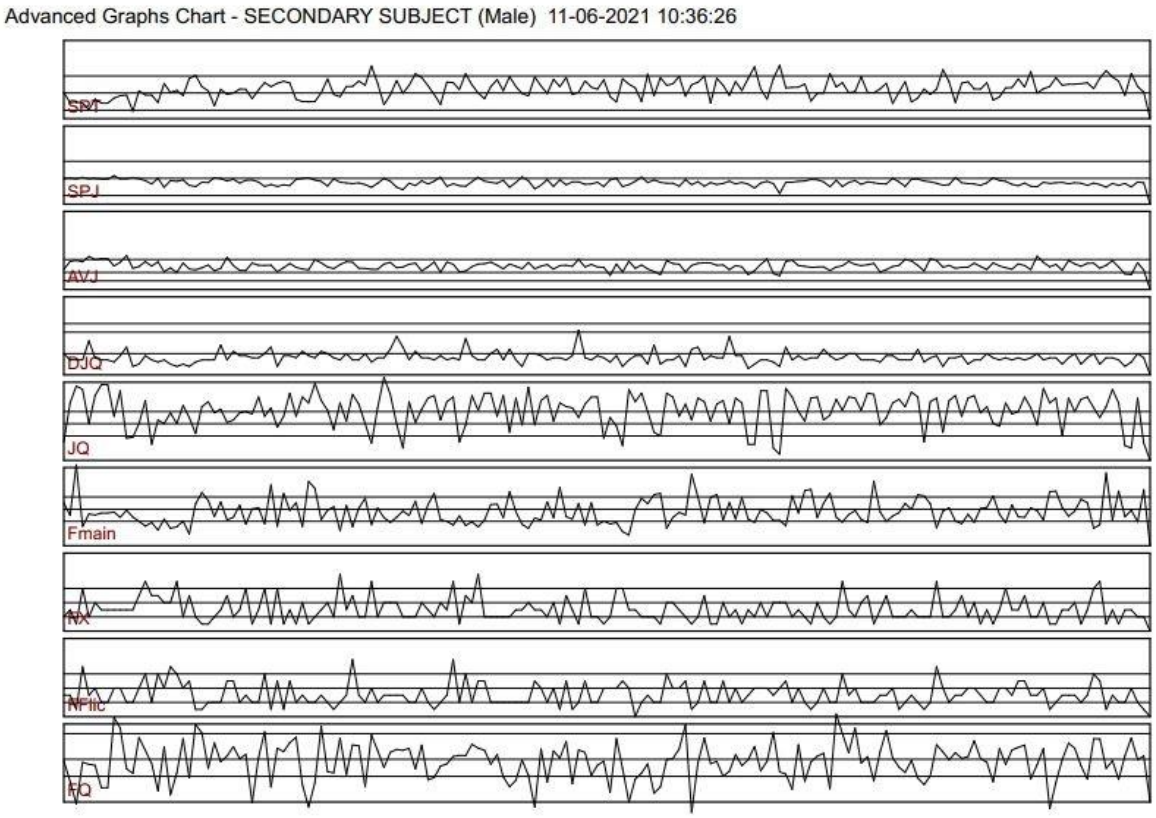
After reviewing all the 168 segments, in the final report, the following types of messages were detected as detection summary from the voice samples of secondary subject i.e. fraudster.

Detection Summary	
Messages	**Number of Segments**
TRUTH	7
STRESSED	31
EXCITED	3
NOT SURE	2
HIGHLY STRESSED	42
HIGH TENSION	14
EXTREME TENION	1
EXTREME STRESS	6
EXTREME EMOTIONS	1
INACCURACY	37
MEDIUM RISK	24
Total	168

The LVA technology is a Computerized Voice Stress Analysis Technique. It automatedly generates the final report based on Nemesysco Ltd.'s owned patented mathematic formulas. The authors have done the entire analysis process vigilantly and carefully. The final decision

in the report described secondary subject i.e., fraudster as HIGH RISK. Screenshot of the final report graphs are shown below.





CONCLUSION

The forensic psychological perspective of such cyber-crimes as sextortion can be understood by the Routine Activity Theory. Marcus Felson and Lawrence E. Cohen created a graphical representation of the Routine activity theory. For most crimes, the routine activity theory provides three necessary conditions: a motivated offender, a suitable victim/target, and the lack of a capable guardian, all of which must be present in time and place (Cohen & Felson, 1979).

- A likely Offender: The fraudster in the case study was motivated by the obvious reason which is easy money. but in his attempt to extort the victim he has committed a bunch of offenses within the ambit of cybercrimes such as Sextortion and Identity

Theft. Unfortunately, this incident went unreported and offenders are roaming free in society. He might be in the search of another suitable target.

- A Suitable Target: The fraudster found Mr. P. a suitable target in the present study since the fraudster might have studies his cyber psychology. His online behavior and later on when they went on to chat on Facebook Messenger and WhatsApp, Fraudster might have judged Mr. P. by that time that he is a user of the social media but he is not aware of the cybercrimes and frauds associated with that. This made Mr. P. the perfect suitable target.
- The absence of a capable guardian: Mr. P. was frightened after watching the video clip of him and the girl showing their sexual organs. He was terrified with the thought only that what his wife and family members would think of about his character and moral conducts. This situation led him to not informing anybody and leaving with him only choice to pay the money. the locus of the situation created is the absence of a capable guardian. Because if Mr. P. would have informed anybody then that person might have played a role of a guardian and his victimization could have been saved.

A combination of above mentioned three factors has contributed to the incidents like this. Social media is indeed a useful platform for internet users to connect with each other irrespective of time and space in the world. But, using social media without awareness of cybercrimes such as sextortion and identity theft is really what makes people victims. Social media is a two-sided sword, it has equal disadvantages and advantages. With the growing digital age and internet users, more awareness about such offenses is also in need. The government indeed has organizations set up to tackle cybercrimes such a State and Central Forensic Science Laboratories have set up the Forensic Psychology Divisions to help in the investigation and detection of such offenses (India Today, 2019).

REFERENCES

Cerna, M. d. (2012, April 15). *Sextortion*. Retrieved June 19, 2021, from newsinfo.inquirer.net: https://newsinfo.inquirer.net/177037/sextortion

Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, *44*(4), 588-608. doi:https://doi.org/10.2307/2094589

Council, N. R. (2003). *The Polygraph and Lie Detection.* National Academies Press.

India, P. T. (2019, December 01). *Six central forensic labs to be upgraded to help probe heinous crimes*. Retrieved June 22, 2021, from www.indiatoday.in: https://www.indiatoday.in/india/story/six-central-forensic-labs-ministry-of-home-affairs-1624123-2019-12-01

Jaishankar, K. (2008). Space Transition Theory of cyber crimes. In F. S. Pittaro., *Crimes of the Internet.* (pp. 283-301). Upper Saddle River, NJ: Prentice Hall.

Johnson, J. (2021, April 07). *Global digital population as of January 2021*. Retrieved June 23, 2021, from www.statista.com: https://www.statista.com/statistics/617136/digital-population-worldwide/

Kagan, J. (2021, February 13). *Identity Theft*. Retrieved June 20, 2021, from www.investopedia.com: https://www.investopedia.com/terms/i/identitytheft.asp

Nemesysco. (n.d.). *Nemesysco's Layered Voice Analysis (LVA™)*. Retrieved June 24, 2021, from www.nemesysco.com: https://www.nemesysco.com/lva-technology/

Oxford English Dictionary Dictionary. (2007). Oxford University Press.

Panda Security. (2021, April 26). *Types of Cybercrime*. Retrieved June 18, 2021, from www.pandasecurity.com: https://www.pandasecurity.com/en/mediacenter/panda-security/types-of-cybercrime/

Sarangia, S., Sahidullahb, M., & Sahaa, G. (2020). Optimization of data-driven filterbank for automatic speaker verification. *Digital Signal Processing*, *104*(102795). DOI:doi:10.1016/j.dsp.2020.102795.

Acknowledgement

The author appreciates all those who participated in the study and helped to facilitate the research process.

Conflict of Interest

The author(s) declared no conflict of interest.

How to cite this article: Rathod S., Kumar A., Maniar K. & Jain S. K. (2021). Forensic Psychological Analysis of Call Recording in the Sextortion Case Using LVA Technique - A Crime Case Study. *International Journal of Indian Psychology*, *9*(3), 321-332. DIP:18.01.035.20210903, DOI:10.25215/0903.035