Indian Journal of Forensic Medicine and Pathology
Volume 14 Number 3, July - September 2021 | Special Issue
DOI: http://dx.doi.org/10.21088/ijfmp.0974.3383.14321.46



REVIEW ARTICLE

# A Recent Advancement in Techniques for Investigating Cybercrimes, Digital Crimes and Audio Forensics

[1]Abhinav Singh, [2]Sally Lukose

## ABSTRACT

The illegal activities using mobile phones, computers, and the internet are rising, including pornography, online prostitution, identity theft, phishing, sniffing or snooping attacks, spamming or malware attacks. Internet crime or cyber-attacks play a pivotal role in impacting the system since we started using the internet. In this era, of digital world crimes are increasing at par. The advancement in the technology for detection of these crimes has revolutionary affected the forensic field. Starting from, the detection of digital crimes from small scale like Email Bombing to Denial of Services (DOS) at large scale. Furthermore, the sensitivity of detection is quite decisive hence, it is cardinal responsibility of forensic experts to investigate these types of crimes critically. An attempt has been made in this paper to percolate the significance of digital crimes, cybercrimes, and audio forensics. Additionally, it also focus the investigative tools and techniques for such crime.

**KEY MESSAGES:** This paper elaborate the key features for investigation of Digital crimes, cybercrimes & Audio Forensics.

KEYWORDS | digital forensics, audio forensics, cyber-attacks, ethical hacking

**Author's Credentials:**
[1]*Research Scholar,* [2]*Professor, School of Allied Health Sciences, Sharda University, Greater Noida, Uttar Pradesh 244001, India.*

**Corresponding Author:**
*Sally Lukose, Professor, School of Allied Health Sciences, Sharda University, Greater Noida, Uttar Pradesh 244001, India.*

**Email:**
*sally.lukose@sharda.ac.in*

**How to cite this article**
*Singh Abhinav. A Recent Advancement in Techniques for Investigating Cybercrimes, Digital Crimes and Audio Forensics. Indian J Forensic Med Pathol. 2021;14(3 Special):739-742.*

## INTRODUCTION

As technologies are blossoming daily, industrialization and digitalization are facilitating these days. The extension of digital technologies creates a domain for performing various tasks quickly and effortlessly. Nowadays, 90% of the work is going online, whether it is classes, conferences, offices, webinars, official meetings, state or political meetings; everything is online now; hence there is a tremendous rise in digital crimes and cybercrimes. On counting, the User of android phones and Apple iPhone devices are immense in number. About 1.7 billion people are Android users[2] and 700 million banks upon the iPhone devices.[1]

In contrast, Windows users are significantly less in numbers.[3] Modern technologies eased living and made it easy to connect with our friends and families via SMS, WhatsApp, Skype, Telegram, Facebook, Instagram, and other social media platforms. With the advancement in different instant messaging applications with various features and the introduction of the internet, it became an easy task to convey your messages from one end to another in the form of encrypted text messages, documents, or any video and audio file format. As per the record, in April 2015, there were about 800 million users on WhatsApp.[4] These unlawful activities usually remain unnoticeable as encryption technology transfers information from one end to another.[5] Usually, a single message is sent to a large number of victims.[6] The attacks grasp the individual's security by different social media platforms, instant messaging applications, e-mail, and scanning the QR codes.[7] The attackers mimic the electronic environment to steal the victim's private information or

recipients.[8]

**Phishing:** Phishing attacks are tremendously rising and acting as a critical component of cyber-attacks. The word phishing means "password harvesting fishing," which is used to steal a victim's identity via computer networks.[9] The attacker gains access to the username and passwords of the victim's identity and illegally exploits them. There are several types of phishing attacks malware-based phishing.[10] deceptive phishing,[11] hosts file poisoning phishing,[12] search engine-based phishing,[13] and other types of phishing classified based on their attacks. The hacker creates a fake page and tries to steal the personal information of the victim.[14] The primary phishing e-mails which are flourishing these days are related to the topic of competent, legal activity, commitment, security, perceptual contrast financial loss, health, retaliation, socialization and social proofs. On the basis of the evidences, it was reported the URLs tempt the attackers to perform phishing attacks, and the web shortening service bit.ly is used to mask the URL in the browser.[15]

**Malware**

The word malware denotes malicious software.[16] The malware tends to breach the system's device and policies in the integrity of the files, breaking the confidential data, and stored data. The malware is categorized into various types according to their attack, propagation, or exploitation of the targeted device.[17] The malware is assigned as harmful depending upon the different protocols of the antivirus vendors; if one antivirus vendor considers a file as malware, it may be possible that the same file is not malware for another antivirus vendor.[18]

**Viruses**

The prevalence of the virus tends to reproduce, propagates within the system files, duplication. The viruses lack independent movement and require a host for their functioning.

**Worms**

The worm self-replicates or shows self-propagation; hence no host is essential for their functioning. Trojan programs are standard files; they create vulnerabilities for attackers and act as malicious files for the system.

**Spywares**

Spywares attacks the users and spies on them without their knowledge; spyware comprises six types: adware, keylogger, Track ware, cookie, riskware, and sniffer.

**Denial of Service (DoS) Attack**

The Denial of Service creates congestion because of the continuous request, which ceases the system's working or server. The server remains busy working on the same type of files which leads to the overloading of the server due to the processing of the same request, and the whole process is known as a Denial-of-Service attack.

**Mobile & Digital Forensics**

The mobile forensic investigation or digital forensic investigation aids in the investigation of digital devices which are under the suspicion of cyber attacks. These types of investigation are done on the basis of raw data recovered by using hex dumps. Seldom the data is being recovered from the memory chips with the help of specific tools and software.[19]

On the other hand, Autopsy 4.1.1, MOBILedit, Cellebrite Universal forensic extraction device (UFED), XRY software, Andriller, Oxygen Forensic Suites are used for investigation of audio, video, emails, browsing histories, credential information or any third part application install in the suspected mobile and cell phone devices. Likewise, Access data F'TK imager, EnCase, and SQLite software play a pivotal role in digital crime investigation(s)[20,21] as shown in figure 1.

**Audio Forensics:**

*Linguistic and voice authentication*

Authentication of voice is quite crucial for personal identification of an individual. As the offenders try to impersonate a voice note or call,[22] there is an urgent need to compare the questioned audio with admitted exemplars as shown in figure 2.

**Voice: Decipherment and detection**

The decipherment and detection of the voice is feasible by analyzing the audio signals retrieved from the suspect. The manipulation

 

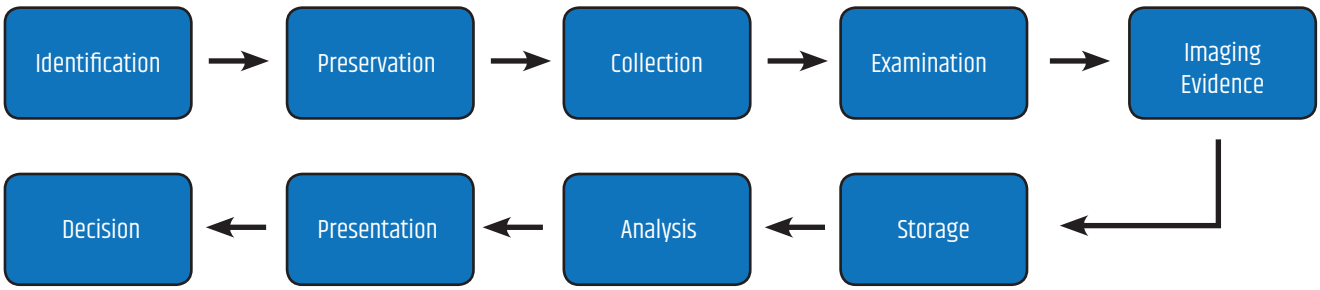


**Figure 1:** Framework for Mobile and digital crime investigation

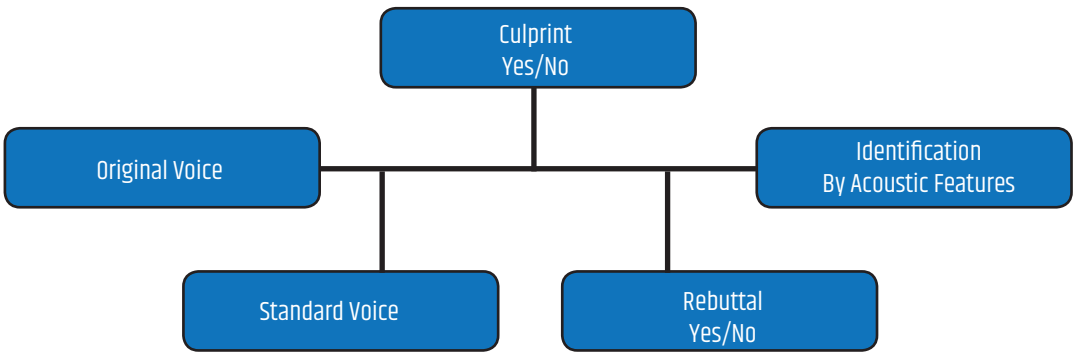


**Figure 2:** Framework for Audio Forensic investigation

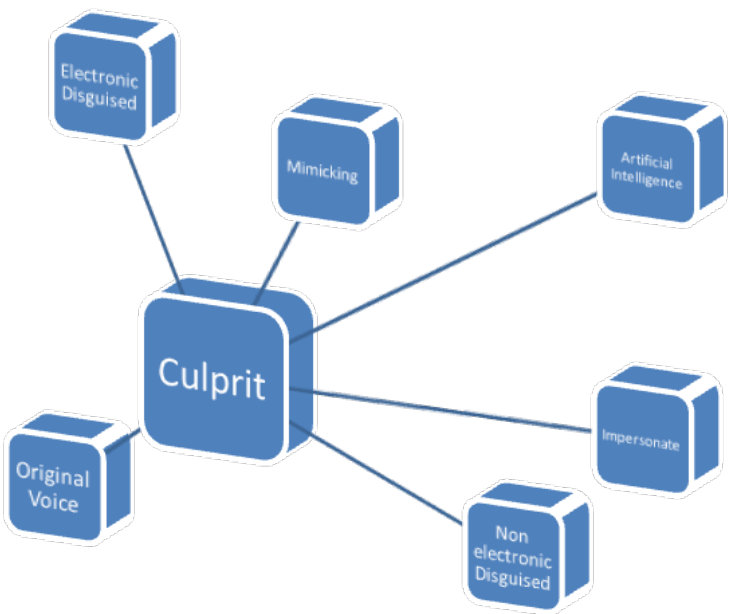


**Figure 3:** Type of cases encountered in Voice Authentication and Identification

impersonation, transplantation, electronic or non-electronic disguised, etc., of audio samples are investigated with the help of certain software such as, Praat, GoldWave, Audacity, Computer Speech Lab (CSL).[23]

The Contemporary, methods for identification and detection of GANs (Generative Adversarial Networks), supervised and unsupervised method like change in the pitch, formants, spectral envelope, intensity, pulses, spectrogram are cumbersome tasks therefore, requires strong expertise[24,25] as shown in figure 3.

## CONCLUSION

In a nutshell, the detection and apprehension of the cyber-attacks, audio authentication, and mobile forensics require sound methodology, procedures, and protocols. There is a strong interlinkage between direct, and indirect investigation proceedings. These identification and detection procedures are quiet crucial for better justice. Even though the price of these original software are quiet expensive, there is no other alternative to investigative protocols. There are many open-source freely available software which are used for the said purpose however, the reliability is scarce. IJFMP

## REFERENCES


1. **Costello S.,** *How Many iPhones Have Been Sold Worldwide? [Online] Available at: http://ipod.about.com/od/glossary/f/how-many-iphones-sold.htm [Accessed 10 June 2015],March 2015.*
2. **Institute, S. B. R.,.** *Android Phone Statistics. [Online] Available at: http://www.statisticbrain.com/android-phone-statistics [Accessed 20 June 2015],March 2015.*
3. **Page C.** *The Inquirer: Windows Phone market share tumbles almost 10 percent as Lumia sales dry up. http://www.theinquirer.net /inquirer/news/ 2360573/windows-phone-market-share-tumbles-almost-10-percent-as-lumia-sales-dry-up [Accessed 20 June 2015].*
4. **Statista.** *Number of monthly active WhatsApp users worldwide from April 2013 to April 2015. http://www.statista.com / statistics/260819/number-of-monthly-active-WhatsApp-users [Accessed 20 June 2015],April 2015.*
5. **Ibrahim M.** *How to Decrypt WhatsApp crypt7 Database Messages. http://www.digitalinternals.com/security/decrypt-whatsapp-crypt7- database-messages/307 [Accessed 20 June 2015].*
6. **HongJ.,** *The state of phishing attacks. Communications of the ACM, Issue 55(1),2012. pp. 74-81.*
7. **Vidas T., Owusu E., WangS., et al.,.** *The susceptibility of smartphone users to QR code phishing attacks. In International Conference on Financial Cryptography and Data Security, 2013, April, (pp. 52-69). Springer, Berlin, Heidelberg.*
8. **Jakobsson M. & Myers S.** *Phishing and countermeasures: understanding the increasing problem of electronic identity theft, 2006. John Wiley & Sons.*
9. **McRae C. & Vaughn R.** *Fighting the phisher: using web bugs and honeytokens to investigate the source of phishing attacks. Proceedings of the 40th Annual Hawaii International Conference on System Sciences (IEEE), Waikoloa,2007,p. 1–7..*
10. **LiS. & Schmitz R.** *A novel anti-phishing framework based on honeypots. eCrime Researchers Summit, IEEE, 2009, p. 1–13..*
11. **Mahmood A. & Rajamani L.,.** *APD: ARM Deceptive Phishing Detector System Phishing Detection in Instant Messengers Using Data Mining Approach. Springer-Verlag Berlin Heidelberg, 2012,Volume 269, pp. 490-502.*
12. **Dadkhah M., LyashenkoV.V., et al.,.** *Methodology of wavelet analysis in research of dynamics of phishing attacks. International Journal of Advanced Intelligence Paradigms,2019, 12(3-4), pp.220-238.*
13. **AltoP.** *HP Networking Communication: Open SSL Vulnerabilities. Hewlett-Packard Development Company, White Paper, 2014, p. 1–4.*
14. **San Martino A. & Perramon X.,** *Phishing secrets: history, effects, and countermeasures. International Journal of Network Security, 2010, 11(3), p. 163–171..*
15. **Arachchilage N. & Hameed M.** *Integrating self-efficacy into a gamified approach to thwart phishing attacks. arXiv preprint arXiv:,2017, 1706.07748*
16. **UcciD., Aniello L. & Baldoni R.** *Survey on the usage of machine learning techniques for malware analysis", pp. , .. arXiv preprint arXiv:1710.08189,2017,pp. 1-67.*
17. **Souri A. & Hosseini R.** *A state-of-the-art survey of malware detection approaches using data mining techniques. Human-centric Computing and Information Sciences, 2018, Issue 8(1), pp. 1-22.*
18. **AllixK., Jérome Q., Bissyandé et al.,.** *A Forensic Analysis of Android Malware--How is Malware Written and How it Could Be Detected?. In 2014 IEEE 38th Annual Computer Software and Applications Conference, 2014, July, (pp. 384-393). IEEE.*
19. **Casey E. & Turnbull B.,** *Digital evidence on mobile devices. Digital Evidence and Computer Crime,2011, Volume 3, pp. pp.1-44...*
20. **Faiz M., Umar R. & Yudhana A.** *Analisis Live Forensics Untuk Perbandingan Kemananan Email Pada Sistem Operasi Proprietary. ILKOM Jurnal Ilmiah,2016, Issue 8(3),pp. 242-247.*
21. **Kostopoulos C. & and Samaras S.** *Mobile phone identification using recorded speech signals. 19th International Conference on Digital Signal Processing IEEE,August 2014, pp. 586-591.*
22. **Garcia-Romero D. a. E.-W. C.,** *Automatic acquisition device identification from speech recordings. In 2010 IEEE International Conference on Acoustics, Speech and Signal Processing, 2010, pp. 1806-1809.*
23. **HanilciC., Ertas F., Ertas T. & Eskidere Ö.,** *Recognition of brand and models of cell phones from recorded speech signals. IEEE Transactions on Information Forensics and Security,2011, Issue 7(2), pp. 625-634..*
24. **Ali Z., Imran M. & Alsulaiman M.,.** *An automatic digital audio authentication/ forensics system. IEEE Access,2017,Issue 5, pp. 2994-3007.*
25. **Price M. Glass J. & Chandrakasan A.** *A low-power speech recognizer and voice activity detector using deep neural networks. IEEE J. Solid-State Circuits,2018, Issue 51 (1) p. 66–75*


 