BOOK CHAPTER | *"Digital Swims in Murky Waters"*

Forensic Analysis on Streaming Multimedia

Emmanuel Tettey Okan
Digital Forensics & Cyber Security Graduate Programme
Department Of Information Systems And Innovations
Ghana Institute of Management & Public Administration
Greenhill, Accra, Ghana
E-mail: etokan89@gmail.com
Phone: +2330242812619

ABSTRACT

Since the advent of technology and digitalization of multimedia, there has been a massive increase in cybercrime. During streaming, with the availability of a network or internet source, multimedia; audio and visual can easily be accessed whiles being aired live. This technology dates as far back as 1990s. Similar to still videos and images, the user is able to download, pause, reverse or forward the show. The ability to stream multimedia has made it easier for users to partake or retrieve multimedia from the comfort of their homes, offices or personal spaces without necessarily being present. However, there are several challenges that affect the functionality of this technology, slow network connection and cybercrime. The issue of slow network may easily be handled by network providers, but cybercrimes has become rampant over the years. These attackers, also known as cyber criminals, use various activities to attack data. Some of their activities include phishing, data breach, identity theft and harassment. The paper has been written to assess forensic analysis of streaming multimedia. While exploring existing studies, it was realized that despite the rich availability of digital image forensics, video forensics hasn't been explored much. This is because of the difficulty involved in analyzing the video data. Video data is always presented in a compressed form, unlike still images that are obtained in their original state. The compressed data often cancels or totally compromises the existing fingerprints, hence making it difficult to monitor or recover data. It was also revealed that, much has not been done so far as the research area is concerned.

Keywords: Mobile Forensics, Cybersecurity, Streaming, Media, Video, Networks

BOOK Chapter | Research Nexus in IT, Law, Cyber Security & Forensics. Open Access. Distributed Free

Citation: Emmanuel Tettey Okan (2022): Forensic Analysis On Streaming Multimedia
Book Chapter Series on Research Nexus in IT, Law, Cyber Security & Forensics. Pp 221-226
www.isteams.net/ITlawbookchapter2022. dx.doi.org/10.22624/AIMS/CRP-BK3-P36

1. INTRODUCTION

In recent times, the world has witnessed a great technological improvement which has led to availability of inexpensive portable and highly usable digital multimedia devices such as cameras, smart phones, digital recorders, and many others. In addition to these technologies, the availability of the internet has facilitated the production of digital audiovisual data on various platforms.

1.1 Background to The Study

Since the advent of technology and digitalization of multimedia, there has been a massive increase in cybercrime. In almost every home, school or organization, there can be found at least one or more computer or a portable gadget used to store or retrieve data, with the help of the internet. With time, personal computers have gained massive space in the business world. With the availability of a network source, businesses and lives have become easier. Most businesses are done digitally and require a network source to store, retrieve or transfer data. Also, accessing data has transcended from just downloading from a source to the ability to stream live. Service providers transform large data into compressed forms to make it easily accessible.

During streaming, with the availability of a network or internet source, multimedia; audio and visual can easily be accessed whiles being aired live. This technology dates as far back as 1990s. Similar to still videos and images, the user is able to download, pause, reverse or forward the show. The ability to stream multimedia has made it easier for users to partake or retrieve multimedia from the comfort of their homes, offices or personal spaces without necessarily being present. However, there are a number of challenges that affect the functionality of this technology; slow network connection and cybercrime. The issue of slow network may easily be handled by network providers but cybercrimes has become rampant over the years. These attackers, also known as cyber criminals use various activities to attack data. Some of their activities include phishing, data breach, identity theft and harassment.

Fig 1: Identity Theft

Fig 2: Phishing

Fig 3: Data Breaches

Based on this premise, efforts have been made recently to give a great deal of attention to forensic analysis of multimedia data. A greater part of the forensic investigation centers on analyzing data such as still images, since those photographs can be greatly used as objective evidence in court and for surveillance. Unfortunately, there is very little information on video forensics because the video data is often compressed and loses its credibility for investigation (Kurosawa et al., 2012). The forensic investigator is responsible for analyzing and investigating the content of streamed media in order to identify an attack and recover data that has been manipulated. In this study, the researcher will assess forensic analysis of streaming multimedia data.

2. RELATED LITERATURE

The section of the paper highlights on the literature available so far as forensic analysis in steaming multimedia is concerned. In an article published by Jennifer Jeffers (2018), she likens digital forensics to investigations in the actual world, where physical components such as blood sample or cotton swabs can help in a crime investigation. Similarly, virtual fingerprints can be analyzed to reveal the intentions of cyber attackers. Since the digital spheres has become a place where most people spend their time, the modern shift has allowed law enforcement to address internet crimes as intensely as real-world crimes. For that matter, digital evidence has become a legitimate means for enforcing cyber law and prosecuting those that abuse it. In a research by Burmester M. et al., (2010,) some methods adopted by forensic investigators included network traffic, where information from a multimedia content can be extracted, even if the content is encrypted.

Technical experts have adviced individuals and organizations to protect their data or content by encrypting them end-to-end. However, their studies state that content encryption alone is not sufficient to protect the confidentiality of a communication channel. Although certain researchers have stated the lack of credibility in video forensics, Burmester (2010) proposed to use traffic snooping to identify the content of video data. After identification, an intelligent matching algorithm will be designed to monitor the boundary of any monitored video. This method helps to identify other networks that are connected to the network source and also trace the IP address of devices connected to the particular network.

Other researchers such as Kurosawa et al. (2012) were the first to introduce the camcorder fingerprinting solution. They also tried to find a way to help with video forensics but were not totally successful as their work did not help to understand if a given video came from a specific camera. Their research however became a blueprint for other researchers who sought to investigate video sources. Later Chen et al., (2012) successfully found a way around the camcorder fingerprinting problem. They properly chose the right denoising filter designed to remove Gaussian noise which was an impediment in identifying which media belonged to which camera specifically.

Fig 2: Denoising filter designed to remove Gaussian noise
Source: https://petapixel.com/assets/uploads/2016/06/camerafingerprintfeat.jpg

3. RESEARCH GAPS/FINDINGS

While exploring existing studies, it was realized that despite the rich availability of digital image forensics, video forensics hasn't been explored much. This is because of the difficulty involved in analyzing the video data. Video data is always presented in a compressed form, unlike still images that are obtained in their original state. The compressed data often cancels or totally compromises the existing fingerprints, hence making it difficult to monitor or recover data. It was also revealed that, much has not been done so far us the research area is concerned.

4. CONCLUSION

At the end of this study, it can be concluded that indeed digitalization has become the norm of the day. Computers and networks are very vital tools needed in our day-to-day activities. With the help of various networks and means, information can be attained via download or live as they are being shared. However, these same resources needed for multimedia functionality are exactly the resources that are needed by cyber attackers to attack private data. As a result of this, digital forensics have been given the legal right to analyze, investigate and monitor multimedia data in order to recover, restore and fish out multimedia attackers.

5. RECOMMENDATION FOR POLICY AND PRACTICES

The researcher recommends that:

1. Organizations must educate their staff to keep their software and systems fully up-to-date in order to avoid leaving it weak to cyber attackers.
2. The ICT departments must ensure Endpoint Protection for all devices and networks, which is a way to protect them from remotely bridged to devices.
3. Since new data breaches surface each day in addition to existing ones, organizations must install a firewall on their devices and networks.
4. Individuals and organizations must ensure to back up their data always, in case of any unforeseen event.

6. IMPLICATIONS FOR AFRICAN PRACTITIONERS AND CYBER SAFETY

The major implication of the subject matter for African Practitioners and Cyber Safety is the fact that, not much has been done to research into forensic analysis on streaming multimedia making practice and implementation quiet challenging.

7. DIRECTION FOR FUTURE WORKS

This research outlined a few studies that had been done by certain researchers to enhance video forensics. However, the researcher could not conclude on the extent to which the project was successful and usable in this modern day. Future researchers can dwell on the gap in this research to further investigate the success rate of Chen et al., and probably other researchers in reporting the success rate of video forensics.

REFERENCES

1. Ricciato, F. (2006). Traffic monitoring and analysis for the optimization of a 3G network. *IEEE Wireless Communications*, *13*(6), 42-49.
2. Al-Mohannadi, H., Mirza, Q., Namanya, A., Awan, I., Cullen, A., & Disso, J. (2016, August). Cyber-attack modeling analysis techniques: An overview. In *2016 IEEE 4th international conference on future internet of things and cloud workshops (FiCloudW)* (pp. 69-76). IEEE.
3. Crotti, M., Gringoli, F., Pelosato, P., Salgarelli, L.: A statistical approach to IPlevel classification of network traffic. In: IEEE International Conference on Communications, ICC 2006, vol. 1, pp. 170–176 (June 2006)
4. Okabe, T., Kitamura, T., Shizuno, T.: Statistical traffic identification method based on flow-level behavior for fair VoIP service. In: 1st IEEE Workshop on VoIP Management and Security, pp. 35–40 (April 2006)
5. Song, D.X., Wagner, D., Tian, X.: Timing analysis of keystrokes and timing attacks on SSH. In: Proc. the 10th Conference on USENIX Security Symposium, Berkeley, CA, USA, p. 25 (2001)
6. https://cdn.winknews.com/wp-content/uploads/2020/01/ -ABPIZ.jpg
7. https://hakin9.org/wp-content/uploads/2016/10/photo_60916_20160120.jpg
8. https://www.hilyards.com/sites/default/files/image-uploads/data-breach-point.jpg