INTEGRATION OF COMPUTER FORENSICS IN INVESTIGATING TRANSBORDER CRIMES ACROSS COMMON LAW COUNTRIES

Kelvin Ovabor

Southeastern Universities Graduate Research Symposium

March 20-31, 2023

Abstract

Common law countries share similar legal systems, which make it easier to exchange information and evidence during investigations. Computer forensics is a crucial aspect of cybercrime investigations that involves the use of digital evidence to support legal proceedings. This paper explores the integration of computer forensics in investigating trans-border crimes across common law countries.

The paper highlights the challenges associated with cross-border investigations and the legal frameworks that govern such investigations. The paper also discusses the role of computer forensics in cybercrime investigations and the various techniques used to collect and analyze digital evidence. The paper concludes with recommendations for improving the integration of computer forensics in investigating trans-border crimes across common law countries.

Keywords: Transborder, Crimes, Forensics, Investigations, Law

INTRODUCTION

In recent years, the world has witnessed a significant increase in cybercrime, which has led to financial losses, identity theft, and other malicious activities. Cybercrime is a global issue that requires the collaboration of law enforcement agencies from different countries to combat effectively. Common law countries share similar legal systems, which make it easier to exchange information and evidence during investigations (PWC,2018). Computer forensics is a crucial aspect of cybercrime investigations that involves the use of digital evidence to support legal proceedings. The integration of computer forensics in investigating trans-border crimes across common law countries has become an essential aspect of law enforcement in the digital age (Casey,2011).

Cybercrime has become a significant threat to individuals, businesses, and governments worldwide. The increased use of technology and the internet has made it easier for criminals to carry out malicious activities, such as identity theft, financial fraud, and hacking (UNODC,2020). Cybercrime is a global issue that requires the collaboration of law enforcement agencies from different countries to combat effectively. The trans-border nature of cybercrime makes it difficult to investigate and prosecute offenders (Council of Europe,2001). The integration of computer forensics in investigating trans-border crimes across common law countries has become an essential aspect of law enforcement in the digital age.

Common law countries share similar legal systems, which make it easier to exchange information and evidence during investigations. The common law system is based on legal precedents and the interpretations of statutes by judges. Common law countries include the United States, Canada, Australia, New Zealand, and the United Kingdom. These countries have developed legal frameworks that govern Trans-border investigations and the exchange of digital evidence

(Ziegel & Pratt,2010). The legal frameworks include mutual legal assistance treaties (MLATs), which allow countries to exchange information and evidence during investigations.

Computer forensics is a crucial aspect of cybercrime investigations that involves the use of digital evidence to support legal proceedings. Computer forensics involves the collection, preservation, and analysis of digital evidence to establish the facts of a case (Carrier,2011). Digital evidence includes data stored on computers, mobile devices, and other electronic devices. Computer forensics experts use specialized tools and techniques to collect and analyze digital evidence (Casey,2011). Computer forensics plays a vital role in cybercrime investigations, and its integration is essential in investigating trans-border crimes across common law countries.

The objective of this paper is to explore the integration of computer forensics in investigating trans-border crimes across common law countries. The paper will highlight the challenges associated with transborder-border investigations and the legal frameworks that govern such investigations. The paper will also discuss the role of computer forensics in cybercrime investigations and the various techniques used to collect and analyze digital evidence. The paper will conclude with recommendations for improving the integration of computer forensics in investigating trans-border crimes across common law countries.

STATEMENT OF THE PROBLEM

In today's world that is commonly referred to as a global village, there is a retinue of criminal activities that threaten the security, lives, and peaceful coexistence of mankind. Such activities range from money laundering, cyber fraud, human trafficking, terrorism and other trans-border crimes. Transborder crimes are crimes involving multi-states.

Due to the complex nature of some of these crimes, many times, the courts of the states affected by such crimes are unable to arrive at accurate decisions leading to conviction because the general rule is that it is better for 10 criminals to be set free than for 1 innocent man to be convicted for a crime, he knows nothing about. So therefore, the onus is on the prosecutor to ensure that the evidence adduced are proved beyond reasonable doubt (not all shadows of doubt) and sufficient enough to convict the accused person. Unless in cases of strict liability and some other exception, the burden of proving the guilt of the accused person remains on the prosecutor, because he who asserts must prove.

That being said, it is necessary for investigators and prosecutors to have sufficient expertise in extracting the necessary evidence for a successful criminal trial. This is important because of the goals of criminal law which is Deterrence, Restoration and Retributive justice.

Clearly, the importance of forensics in today's criminal trial cannot be overemphasized. Forensic science is the application of science to law, forensics could either be in the form of accounting forensics, which involves using accounting techniques to understand the nature of financial crimes; computer forensics which entails the application of technological skills to finding out the truth and otherwise of an alleged crime which could be in the form of software analysis, restoring of data on smart devices and tracking the history of closed circuit cameras or black boxes on airplanes, also there is Bio Forensics which includes the examination of ones DNA, finger prints, blood samples etc to ascertain the truism of an allegation.

Again, the elements of an offence include the *mens rea* (the guilty mind) and the *actus reus* (guilty act). In practice, it takes quite a great deal of background investigation to be able to prove both but with the aid of forensics, life would be easier in tracking down transborder terrorists,

criminals and human traffickers as reference can be made to guilt indicators such as finger prints, foot prints, psychological proclivities, chat history , websites frequently visited, google search history, candid video shots, tweets, online forms etc.

RESEARCH QUESTIONS:

1.Do the persons in charge of the prosecution of transborder crimes have the professional forensic competence?

2.What is the minimum technological skills required to understand computer forensic evidence?

3.What are the IT ethics regarding computer forensic?

4.Can lawyers, judges with little or no technological background adjudicate over matters needing technological expertise?

LITERATURE REVIEW

According to Malhotra (2021), *"With the signing of the United Nations Convention against Transnational Organized Crime in Palermo, Italy, in December 2000, the international community demonstrated the political will to answer a global challenge with a global response. If crime crosses borders, so must law enforcement. If the rule of law is undermined not only in one country, but in many, then those who defend it cannot limit themselves to purely national means. If the enemies of progress and human rights seek to exploit the openness and opportunities of globalization for their purposes, then we must exploit those very same factors to defend human rights".*

Several studies have examined the role of computer forensics in investigating cybercrime. For example, Kruse and Heiser (2002) argued that computer forensics is an essential tool in investigating cybercrime, and it provides valuable evidence that can be used in court. They also suggested that the integration of computer forensics in law enforcement agencies can help in enhancing the ability of investigators to tackle cybercrime.

In common law countries, the use of computer forensics in investigating transborder crimes has been gaining prominence. For example, in Australia, the Australian Federal Police (AFP) has been working closely with law enforcement agencies in the Asia-Pacific region to investigate transborder crimes using computer forensics. According to Broadhurst (2016), the integration of computer forensics in transborder crime investigations has helped in identifying and tracking criminals who use digital technologies to commit crimes. The author further suggested that the integration of computer forensics in transborder crime investigations has led to more successful prosecutions in courts.

In Canada, the use of computer forensics in transborder crime investigations has also gained prominence. According to Zhang et al. (2016), the integration of computer forensics in transborder crime investigations has helped in identifying and tracking criminals who use digital technologies to commit crimes. The authors suggest that the integration of computer forensics in transborder crime investigations has led to more successful prosecutions in courts.

In the United States, the use of computer forensics in investigating transborder crimes has been widely adopted. According to Casey (2011), the integration of computer forensics in transborder crime investigations has helped in identifying and tracking criminals who use digital technologies to commit crimes. The author further suggests that the integration of computer forensics in transborder crime investigations has led to more successful prosecutions in courts.

Case Studies on the Integration of Computer Forensics in Investigating Trans-border Crimes Across Common Law Countries

i.The Silk Road Case

The Silk Road was an online black market that operated from 2011 to 2013. The website allowed users to buy and sell illegal drugs and other illicit goods using the digital currency Bitcoin. The founder of the Silk Road, Ross Ulbricht, was arrested in San Francisco in 2013 and charged with multiple crimes, including conspiracy to traffic narcotics, money laundering, and computer hacking.

The investigation into the Silk Road involved law enforcement agencies from multiple countries, including the United States, Canada, and the Netherlands. Computer forensics played a crucial role in the investigation. Law enforcement agencies used computer forensics techniques to identify and track the digital currency transactions used on the Silk Road, as well as to recover deleted chat logs from Ulbricht's laptop.

The integration of computer forensics in the investigation of the Silk Road case highlights the importance of collaboration between law enforcement agencies from different countries. The investigation required the exchange of information and evidence between law enforcement agencies from multiple countries, which was facilitated by mutual legal assistance treaties.

ii.The WannaCry Ransomware Attack

The WannaCry ransomware attack was a global cyberattack that occurred in May 2017. The attack affected over 300,000 computers in 150 countries, including the United Kingdom's National Health Service (NHS). The attack was carried out using a type of ransomware known as

WannaCry, which encrypted the files on infected computers and demanded payment in Bitcoin for their decryption.

The investigation into the WannaCry ransomware attack involved law enforcement agencies from multiple countries, including the United States, the United Kingdom, and China. Computer forensics played a crucial role in the investigation. Law enforcement agencies used computer forensics techniques to analyze the malware used in the attack and to identify the Bitcoin transactions used to pay the ransom.

The integration of computer forensics in the investigation of the WannaCry ransomware attack highlights the importance of international collaboration in the investigation of cybercrime. The investigation required the exchange of information and evidence between law enforcement agencies from multiple countries, which was facilitated by mutual legal assistance treaties and international agreements.

.

Challenges Associated with Trans-Border Investigations

The investigation of trans-border crimes poses significant challenges to law enforcement agencies. These challenges include:

i. Jurisdictional issues: Cross-border investigations involve multiple jurisdictions, which can lead to conflicts in jurisdiction. Different countries have different laws and legal frameworks, which can complicate investigations.

ii. Language barriers: Cross-border investigations involve communication between law enforcement agencies from different countries. Language barriers can hinder communication and the exchange of information and evidence.

iii. Cultural differences: Cross-border investigations involve working with individuals from different cultures, which can lead to misunderstandings and communication breakdowns.

iv. Differences in legal systems: Common law countries share similar legal systems, but there are still differences in the interpretation of statutes and legal precedent. These differences can complicate investigations and the exchange of evidence.

v. Technological challenges: The investigation of cybercrime involves the use of complex technology, which requires specialized knowledge and expertise. Law enforcement agencies may not have the necessary resources and expertise to investigate cybercrime effectively.

Legal Frameworks Governing Cross-Border Investigations

The investigation of trans-border crimes involves the exchange of information and evidence between law enforcement agencies from different countries. The legal frameworks that govern cross-border investigations include mutual legal assistance treaties (MLATs), extradition treaties, and international agreements (UNODC,2003).

i. Mutual legal assistance treaties (MLATs): MLATs are agreements between countries that facilitate the exchange of information and evidence during investigations. MLATs are essential in investigating trans-border crimes because they provide a legal framework for the exchange of evidence and information between countries.

ii. Extradition treaties: Extradition treaties allow countries to transfer individuals who have been accused or convicted of a crime to another country for prosecution or punishment. Extradition treaties are essential in investigating trans-border crimes because they allow countries to prosecute individuals who have committed crimes in other countries.

iii. International agreements: International agreements are agreements between countries that address specific issues, such as the investigation of cybercrime. These agreements provide a legal framework for countries to collaborate on investigations and the exchange of evidence.

Role of Computer Forensics in Transborder crime Investigations

Computer forensics plays a vital role in transborder crime investigations. Computer forensics involves the collection, preservation, and analysis of digital evidence to establish the facts of a case. Computer forensics experts use specialized tools and techniques to collect and analyze digital evidence. The role of computer forensics in cybercrime investigations includes:

i. Identification of digital evidence: Computer forensics experts use specialized tools and techniques to identify digital evidence that can be used in legal proceedings.
ii. Preservation of digital evidence: Computer forensics experts use specialized tools and techniques to preserve digital evidence to ensure its authenticity and integrity.
iii. Analysis of digital evidence: Computer forensics experts use specialized tools and techniques to analyze digital evidence to establish the facts of a case.
iv. Presentation of digital evidence: Computer forensics experts provide expert testimony in legal proceedings to explain the significance of digital evidence.

Techniques Used in Computer Forensics

Computer forensics involves the use of specialized tools and techniques to collect and analyze digital evidence. The techniques used in computer forensics include:

i. Imaging: Imaging involves the creation of a bit-for-bit copy of a device's storage media. Imaging is essential in computer forensics because it preserves the original data and ensures its authenticity and integrity.

ii. Data recovery: Data recovery involves the recovery of deleted or lost data from a device's storage media. Data recovery is essential in computer forensics because it can uncover critical evidence.

iii. Password cracking: Password cracking involves the use of specialized tools and techniques to recover passwords from a device's storage media. Password cracking is essential in computer forensics because it can provide access to encrypted data that may contain critical evidence.

iv. Network forensics: Network forensics involves the collection and analysis of network traffic to identify potential security breaches or attacks. Network forensics is essential in computer forensics because it can help investigators identify the source of a cyberattack.

v. Malware analysis: Malware analysis involves the analysis of malicious software to identify its purpose and behavior. Malware analysis is essential in computer forensics because it can help investigators identify the source of a cyberattack and provide information on the attacker's motives.

vi. Mobile device forensics: Mobile device forensics involves the collection and analysis of data from mobile devices. Mobile device forensics is essential in computer forensics because mobile devices often contain critical evidence, such as call logs, text messages, and location data.

Conclusion

The integration of computer forensics in investigating trans-border crimes across common law countries is crucial in the modern era of cybercrime. The use of computer forensics techniques can help law enforcement agencies collect, preserve, and analyze digital evidence to establish the facts of a case.

Effective collaboration between law enforcement agencies from different countries is essential in the investigation of trans-border crimes, and international legal frameworks such as mutual legal assistance treaties and international agreements play a vital role in facilitating this collaboration.

.

References

Broadhurst, R. (2016). Transnational cybercrime and policing in East Asia. In R. Broadhurst, P. Grabosky, & Y. Liang (Eds.), Cybercrime and cybersecurity in the global south (pp. 193-216). Palgrave Macmillan.

Carrier, B. (2014). "File System Forensic Analysis." Addison-Wesley Professional.

Casey, E. (2011). "Digital evidence and computer crime: forensic science, computers and the internet." Academic Press..

Council of Europe. (2001). "Convention on Cybercrime." Retrieved from https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168007e7f9

Kruse II, W.G., & Heiser, J.G. (2002). Computer forensics: Incident response essentials. Addison-Wesley Professional.

Malhotra, A. (2021). The book for a Common Man: Criminal Law (Paper Back, English).

PWC (2018). "Global Economic Crime and Fraud Survey 2018." PWC. Retrieved from https://www.pwc.com/gx/en/services/advisory/forensics/economic-crime survey/cybercrime.html

United Nations Office on Drugs and Crime (UNODC). (2003). "Manual on Mutual Legal Assistance and Extradition." Retrieved from https://www.unodc.org/pdf/criminal_justice/MLA-Extradition/MLA-Extradition_manual.pdf

United Nations Office on Drugs and Crime (UNODC). (2020). "Global Study on Smuggling of Migrants." Retrieved from https://www.unodc.org/documents/data-and-analysis/glosom/GLOSOM_2020_web_small.pdf

Ziegel, J. S., & Pratt, J. W. (2010). "An introduction to the law of the commonwealth." Carswell.

Zhang, Y., Shen, Q., & Zhang, J. (2016). Transborder cybercrime investigation and cooperation: A case study of the Silk Road Economic Belt. China and Eurasia Forum Quarterly, 14(4), 93-110.