Understanding Digital Forensics: Exposing the Origins of a Cybercrime

Eric K. Corpus

Old Dominion University

CRJS 215S (34203): Introduction to Criminology

Dr. Charles R. Gray

July 30, 2023

Understanding Digital Forensics: Exposing the Origins of a Cybercrime

With the increasing integration of technologies into our everyday lives, the digital domain has evolved into a new battleground for a variety of criminal activities. Criminals are utilizing sophisticated strategies to conceal their identities and actions, leveraging obfuscation technologies like Virtual Private Networks (VPNs) and The Onion Router (TOR) network to leave behind complex, electronic traces of their deviant activities. This technological advancement has prompted the rise of digital forensics in the field of criminal justice, a discipline devoted to deciphering these complicated electronic trails. As digital forensics continues to evolve, it equips law enforcement and legal professionals with innovative methods to uncover and provide evidence of criminal activities, despite sophisticated digital misdirection. This paper examines the vital role of digital forensics in criminal justice, focusing on how specific techniques help expose the true origins of crimes conducted over VPNs or TOR networks. Case studies will be presented that discusses the impact on policy and practice and emphasizes the pressing need for robust digital forensics in an increasingly digitized criminal landscape.

In order to appreciate the extent of the challenges faced by law enforcement and digital forensics in cybercrime investigations, it is crucial to understand the tools and technologies often employed for malicious activities. Central to this discussion are VPNs and TOR. As defined by the National Institute of Standards and Technology, “A VPN is a virtual network, built on top of existing physical networks, that can provide a secure communications mechanism for data and other information transmitted between two endpoints” (Frankel et al., 2021). It establishes an encrypted tunnel between a user’s device and a VPN gateway on the edge of the target network.

This tunnel secures data in transit, making it unintelligible to unauthorized entities, and masks the user's IP address, making their online actions practically untraceable.

TOR, conversely, is a network aimed at improving online privacy and security. It works by directing internet traffic through a worldwide volunteer network of relays (i.e. routers), making the identification of the source of the information considerably challenging (Javed, 2023). This complexity is what attracts cybercriminals to TOR. Both VPNs and TOR significantly complicate digital crime investigations due to their fundamental capabilities of obscuring a user's location and identity. Criminals can exploit these technologies to effectively hide their activities, highlighting the necessity for a robust understanding of these technologies and the role digital forensics can play in uncovering their misuse. However, as Minařík & Osula (2016) highlight, this challenge is also associated with complex legal issues. While TOR and VPNs offer valuable services to maintain anonymity and protect data, their potential misuse for criminal activities necessitates a balanced legal approach that considers both the rights of legitimate users and the needs of law enforcement.

The prevalence of digital environments and tools as well as their increasingly association with criminal activities have led to a marked rise in the importance of digital forensics within the criminal justice sector. The key task of digital forensics is to locate, recover, examine, and present digital evidence, and this mandate has expanded and evolved with the advent and complications of tools like VPNs and TOR. Originally designed to preserve privacy and secure online communications, these digital tools have a potential for misuse in criminal activities, posing a complex challenge to investigators that digital forensics is determined to address (Al-Katib, 2022; Vincze, 2016).

Navigating the multifaceted terrain of VPNs and TOR networks, digital forensic investigators are pivotal in piecing together the obscured digital evidence to illuminate the path towards effective criminal investigations and justice. The field is continually evolving its tools and techniques to detect patterns, identify anomalies, and sometimes break through encryptions. These techniques involve integrating scientific methodologies to extract and interpret data from digital networks while maintaining the integrity of the evidence, which is crucial for its admissibility in court. Despite the technical hurdles and ethical dilemmas inherent in handling VPN and TOR-based crimes, the role of digital forensics within the criminal justice system remains integral, with advancements continually making strides in decrypting the obscure digital world. Dhirani, Mukhtiar, Chowdhry & Newe (2023) stress the importance of considering the privacy rights of individuals when formulating regulations and policies pertaining to the use of these technologies. The balance between maintaining the privacy of users and ensuring effective law enforcement is an ongoing challenge.

The effectiveness of digital forensics in uncovering the true origins of crimes conducted over VPNs and TOR networks is powerfully evidenced through several recent case studies. One such instance is the case of Darkode, a prominent cybercrime forum, where digital forensics played a significant role in amassing crucial evidence, leading to the dismantling of the forum and a string of international arrests (Office of Public Affairs (U.S. Department of Justice), 2015). Network forensic tools, similar to Wireshark, have capabilities that allow the analysis of captured internet traffic data, enabling investigators to potentially connect events, times, and locations, an approach that could be applied in such cases ("A Guide to Digital Forensics and Cybersecurity Tools," 2022). Similarly, the investigation of the notorious black-market platform Silk Road, which operated through TOR, highlighted the significance of digital forensic

techniques. Tools comparable to EnCase or Forensic Toolkit offer the capability of analyzing hardware utilized in criminal activities, and such capabilities were crucial in tracing the illegal activities back to the creator, Ross Ulbricht (United States v. Ulbricht, No. 14-cr-68 (KBF), 31F. Supp. 3d 540 - Dist. Court, SD New York, 2014). Both these cases underscore the transformative role of digital forensics in the criminal justice system, capable of tracing illegal activities back to their origin even when confronted with the complex veil of anonymity offered by TOR networks.

VPNs also pose significant challenges to law enforcement. Cases such as Remines v. Commonwealth (Va. Ct. App., 2022) and United States v. Thompson (Dist. Court, WD Washington, 2022) emphasize the potential for digital forensics to overcome these challenges. In both instances, despite the defendants' use of VPN services to hide their illicit activities, digital forensic techniques were key to the successful investigation. Tools such as Cellebrite or Oxygen Forensic Detective, which are capable of retrieving and analyzing data from mobile devices, can provide invaluable information about data transmission times, app usage, and GPS data. These capabilities could be essential in tracing crimes back to their origins (“A Guide to Digital Forensics and Cybersecurity Tools, 2022). The success of these investigations affirms the pivotal role digital forensics plays in criminal justice, revealing the true origins of crimes despite the hurdles posed by VPNs and TOR networks.

The evolving and complex field of digital forensics has a profound influence on the policy and practice of the criminal justice system, with a responsibility on authorities to keep pace with the rapid developments in cybercrime. Steinmetz, Schaefer, Brewer & Kurtz (2023) assert the vital role of digital forensics tools in evidence gathering for cybercrime investigations and emphasize the need for stringent management and regulation to ensure the legality and ethical appropriateness of their use. Policymakers are called upon to accommodate these needs in

their legislation and budgets, ensuring investigators are equipped with contemporary training and tools to keep up with the ever-changing face of cybercrime and effectively extract valuable evidence from VPN and TOR network usage.

Simultaneously, the rapid acceleration of technological innovation necessitates new approaches to the acquisition and analysis of digital evidence. As technology progresses, digital forensics inevitably grows more complicated, and existing practices may become inadequate. The criminal justice system, therefore, has a responsibility to promote and support ongoing research and development in digital forensics, ensuring that investigators are equipped with the most advanced methodologies to combat cybercrime (Novak, 2021; Novak, et al., 2018). This proactive approach to policy and practice extends to the handling of digital evidence. Such evidence is vulnerable to compromise if mishandled; therefore, policies need to enforce strict standards for digital evidence handling to preserve its integrity. Regularly updated training that reflects the best practices in evidence preservation is critical, especially in cases involving VPNs and TOR networks, where the integrity of evidence could be pivotal to the case outcome (Ritter, 2006).

The complex and ever-evolving digital landscape has emerged as a breeding ground for a variety of criminal activities, putting a renewed emphasis on the critical role of digital forensics in the criminal justice system. The use of obfuscation technologies such as VPNs and TOR networks by criminals underscores the challenges faced by investigators and highlights the significance of digital forensics in unmasking their illicit activities. The profound impact of digital forensics is demonstrated through a series of case studies where forensic techniques have successfully penetrated the layers of anonymity offered by these technologies, leading to successful prosecutions and the dismantling of criminal enterprises. Nevertheless, the pace of

technological advancement and the sophistication of cybercriminal activities continue to test the capabilities of digital forensics, demanding continuous research, innovation, and the development of cutting-edge tools and techniques. The responsibility of the criminal justice system is to ensure that these developments are mirrored in legislation, budgets, and policies, thereby bolstering the efficacy of digital forensics as a key tool in modern criminal investigations.

References

A guide to digital forensics and cybersecurity tools. (2022, May 19). Forensics Colleges. https://www.forensicscolleges.com/blog/resources/guide-digital-forensics-tools

Abdullahi, A. (2022, March 22). *Top Digital Forensics Tools & Software 2022*. IT Business Edge. https://www.itbusinessedge.com/security/digital-forensic-tools/

Al-Katib, A. (2022, January 3). *The Role of Digital Forensics in Criminal Investigations*. Mission Critical. https://www.missioncriticalmagazine.com/articles/93914-the-role-of-digital-forensics-in-criminal-investigations

Dhirani, L. L., Mukhtiar, N., Chowdhry, B. S., & Newe, T. (2023). Ethical Dilemmas and Privacy Issues in Emerging Technologies: A review. *Sensors*, *23*(3), Article 1151. https://doi.org/10.3390/s23031151

Frankel, S. E., Hoffman, P., Orebaugh, A., & Park, R. (2021). *Guide to SSL VPNs*. https://doi.org/10.6028/nist.sp.800-113

Javed, A. R., Ahmed, W., Alazab, M., Jalil, Z., Kifayat, K., & Gadekallu, T. R. (2022). A comprehensive survey on computer forensics: State-of-the-Art, tools, techniques, challenges, and future directions. *IEEE Access*, *10*, 11065–11089. https://doi.org/10.1109/access.2022.3142508

Javed, M. H. (2023, June 19). *TOR network architecture, anonymity and Hidden services*. Engrixiv - Engineering Archive. https://engrxiv.org/preprint/view/3054/5595

Minařík, T., & Osula, A. (2016). Tor does not stink: Use and abuse of the Tor anonymity network from the perspective of law. *Computer Law & Security Review*, *32*(1), 111–127. https://doi.org/10.1016/j.clsr.2015.12.002

Novak, M. (2021, December 21). *Improving the collection of digital evidence*. National Institute of Justice. https://nij.ojp.gov/topics/articles/improving-collection-digital-evidence

Novak, M., Grier, J., & Gonzales, D. (2018, October 7). *New Approaches to Digital Evidence Acquisition and Analysis*. National Institute of Justice. https://nij.ojp.gov/topics/articles/new-approaches-digital-evidence-acquisition-and-analysis

Office of Public Affairs (U.S. Department of Justice). (2015, July 15). *Major Computer Hacking Forum Dismantled* [Press release]. https://www.justice.gov/opa/pr/major-computer-hacking-forum-dismantled

REMINES v. Commonwealth, Va: Court of Appeals 2022: Record No. 0737-21-2. (2022, December 20). https://scholar.google.com/scholar_case?case=3728278552087298555

Ritter, N. (2006, July 1). *Digital Evidence: How Law Enforcement Can Level the Playing Field With Criminals*. National Institute of Justice. https://nij.ojp.gov/topics/articles/digital-evidence

Steinmetz, K. F., Schaefer, B. P., Brewer, C. G., & Kurtz, D. L. (2023). The role of computer technologies in structuring evidence gathering in cybercrime investigations: A Qualitative analysis. *Criminal Justice Review*, 073401682311610. https://doi.org/10.1177/07340168231161091

United States v. Thompson, Dist. Court, WD Washington 2022: Case No. CR19-159RSL. (2022, February 28). https://scholar.google.com/scholar_case?case=12780093286974250691

United States v. Ulbricht, 31 F. Supp. 3d 540 - Dist. Court, SD New York 2014: No. 14-cr-68 (KBF). (2014, July 9). https://scholar.google.com/scholar_case?case=14855072057929372382

Vincze, E. A. (2016). Challenges in digital forensics. *Police Practice and Research*, *17*(2), 183–194. https://doi.org/10.1080/15614263.2015.1128163