A Statistical Analysis of IP Packet Size Distribution in Legitimate ATM Transactions

Brian G. Volkmuth
St. Cloud Technical & Community College
bvolkmuth@gmail.com

Abstract

Over the last few decades, consumers have become accustomed to the convenience of Automatic Teller Machines (ATMs) to transfer funds between accounts, provide account balance information, and withdraw cash from savings, checking, and other account types. Along with the convenience and ease of locating an ATM through mobile bank apps, there has been a significant increase in ATM fraud across the globe. Consumer confidence in ATMs, banks, and credit card issuers is significantly impacted by the perceived level of security in ATM transactions and the technology behind them. Confronting the risk associated with ATM fraud and limiting its impact is an essential issue that financial institutions face as the sophistication of fraud techniques has advanced. The process behind verifying these transactions has primarily moved from Plain Old Telephone Systems (POTS) to Ethernet and Transmission Control Protocol/Internet Protocol (TCP/IP) connections to the processors, banks, and card issuers. The attack surface has grown both in size and complexity. These security risks should prompt the industry to research all attack surfaces, and this research looks specifically at the attack surface created by predictable TCP/IP packet size. To obfuscate ATM IP traffic, random or commonly sized packet construction is proposed. Even with the proliferation of retail ATMs in the most common retail spaces, this attack vector has received little attention.

Keywords: ATM, Ethernet, Obfuscation, TCP/IP

Introduction

Over recent decades, Automated Teller Machines (ATMs) have become common, providing bank consumers with easy access to banking services. Consumers can perform several banking tasks, such as checking an account balance, transferring funds between accounts, depositing, and withdrawing funds. ATMs are known as alternative delivery channels. Alternative, because they are an alternative to the human teller, delivery because they are programmed to deliver a specific set of services and significantly reduce bank transaction costs (Krishnan, 2012, p. 10). Banks have capitalized on this technology to lower costs by as much as 37% (Valverde et al., 2004) and provide a convenient service at hundreds of thousands of locations throughout North America. As of 2023, the Automated Teller Machine Industry Association (ATMIA) reported that the United States (U.S.) ATM population grew by about 21,000, and the total number is between 520,000 and 540,000 (Tente, 2023). The Federal Reserve, in its 2022 triennial Payments Study, reports that there were 3.7 billion ATM transactions with a value of $0.73 trillion and an average of $198 per transaction in 2021 (Federal Reserve Board, 2023). However, this convenience has also made them attractive targets for fraud. As ATM technology has transitioned from traditional plain old telephone system (POTS) lines to modern Ethernet networks using Internet Protocol (IP), the potential for attacks has increased significantly. Network Security Theory (NST) provides the foundational knowledge to protect networks and data from unauthorized access, use, disclosure, modification, destruction, or disruption of services. It focuses on understanding and mitigating vulnerabilities within network protocols, including TCP/IP, and analyzing how data is transmitted (Cankaya, 2021). Data Mining techniques (anomaly detection, sequential patterns, and prediction) will be employed to analyze a large data set of packets and determine the uniqueness of the packet sizes found in an ATM transaction transmission. Sequential pattern mining discovers frequent subsequences as patterns in a sequence database (Mabroukeh & Ezeife, 2010, p. 2). Anomaly detection will be performed to detect outliers from the expected patterns in the given data set (Trivedi & Srivastava, 2022, p. 1). Network traffic analysis and prediction are a proactive approach to ensure secure, reliable, and qualitative network communication. Various techniques for analyzing network traffic are proposed and experimented with, including neural network-based and data-mining techniques (Joshi & Hadi, 2015).

Literature Review

Ensuring the security of ATM transactions is vital for maintaining consumer trust, yet the vulnerabilities associated with Ethernet IP-based communication have often been overlooked. This research explores the structure and predictability of ATM Ethernet traffic to identify potential weaknesses and guides the development of more robust security measures. By understanding the underlying network protocols, we can better protect ATMs from new threats and secure consumer funds. The literature is replete with customer satisfaction surveys relating to ATMs. The perceived security in ATM use is a significant variable in this area of research (Nigatu et al., 2023).

The findings indicate that convenience, reliability, ease of use, fulfillment, and security/privacy of ATM service quality dimensions are positively and significantly associated with customer satisfaction. (Idris, 2014) The security of ATM transactions requires a continuous and proactive review of the physical components of the machine related to its connection to a network, the security of the protocols used, and operating system security. ATM customers highly value seamless and efficient ATM operations. In the study "Exploring the Nexus of ATM Service Quality, Customer Satisfaction, and Loyalty in the Private Banking Sector in Bangladesh," the authors found a significant positive correlation between customer satisfaction and loyalty. Satisfied customers are likelier to remain loyal to their banks, indicating that improving ATM service quality can enhance customer retention (Hoque, 2024).

As with many conveniences of the modern age, the ATM has brought, with its popularity, the chance of compromised personal data. "Fraud perpetrated at the Automated Teller Machine (ATM) has suddenly and somewhat unexpectedly exploded to the highest rate in two decades" (Sidel, 2015). The uptick in fraud cases is mainly due to the new, more secure credit and debit cards that banks and credit card companies are rushing to replace the 30-year-old magnetic strip technology. "Criminals 'know there is still vulnerability [at the ATM], and they are trying to capitalize on it,' said Owen Wild, director of security marketing at NCR Corp., one of the largest ATM manufacturers" (Sidel 2015). The process of updating all terminals, including ATMs, that accept credit and debit cards with the Europay, MasterCard, and Visa (EMV) chip was to be completed in 2015, with gas pumps having until 2020 due to regulatory and other complications. This, however, was extended again until April 17, 2021. (Johnson et al., 2024) While many of these cases involve capturing the information while reading the card, this research looks at the possible vulnerability from and on the network the ATM is connected to and the size, construction, and predictability of IP packets. E-commerce technologies such as ATMs and consumer demand for increased functionality and security continue evolving (Abu Hussein & Volkmuth, 2019, p. 141).

Attack Surface

ATMs connected to a Transmission Control Protocol/Internet Protocol (TCP/IP) network are susceptible to several attacks. The IP's job is to route packets over the network to their destination. IP is connectionless and is considered unreliable, meaning that it does not guarantee the delivery of packets that the packets will arrive in order or take the same path (Alqahtani & Iftikar, 2013, p. 42). TCP works with IP, breaks the data into segments or different packets, and numbers the packets. It is considered reliable because it guarantees packet delivery and error correction and can process requests for retransmission of broken, damaged, or missing packets. TCP/IP has an attack surface relevant to network-connected ATMs. The attacks that apply to this study are:

TCP"SYN"

This is caused by the three-way handshake mechanism between host and server to set up a connection. An attacker can exploit the TCP three-way handshake to overwhelm a server with SYN requests. The server allocates resources for each SYN-ACK, but the attacker doesn't send the final ACK, leaving connections half-open. This exhausts the server's resources, preventing it from handling legitimate connections and resulting in a denial-of-service attack (Alqahtani & Iftikar, 2013, p. 43).

IP Spoofing

IP address spoofing involves creating TCP/IP packets using another IP address as a source address to impersonate the owner's identity of the IP address used (Alqahtani & Iftikar, 2013, p. 43). If the source

address is successfully spoofed, the intended host will reply to the spoofed address, using up the host's resources. This is one form of a Denial of Service (DoS) attack.

Man-in-the-Middle

An attacker can hijack a verified network session by spoofing the IP address of an authenticated host. This allows the attacker to intercept and manipulate data between the original hosts (Alqahtani & Iftikar, 2013, p. 43).

Denial of Service (DoS)

Attackers can flood a victim with packets without fear of retaliation, as the replies will be sent to the spoofed IP address. This can overwhelm the victim and cause a denial-of-service attack, hiding the attacker's identity (Alqahtani & Iftikar, 2013, p. 43).

Low-rate Denial of Service (LDoS)

LDoS attacks are the behavior of intentionally degrading the quality of TCP links by throttling TCP flows to a small fraction of its ideal rate with periodic small pulse sequences. LDoS attack traffic is significantly smaller than a DDoS attack, allowing for the behavior to be hidden from standard Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS) (Zhijun et al., 2020, p. 43921).

Research Process

In this proposed study, I will look at the potential of a Denial of Service (DoS) attack based on the predictability of IP data packets in an ATM transaction. I will use Statistical Hypothesis Testing (SHT) and Game Theory (GT) in this study. This study hypothesizes that ATM transactional traffic can be identified in a congested network by one attribute: statistically unique packet sizes. From GT, identifying anomalies allows for detecting patterns first so that anomalies will become evident. Also, the modeled behavior of both attackers (not addressed in this study) and defenders can reveal an attack vector. One such attack vector is a DoS. GT can also help design deceptive techniques, such as obfuscation. Should the hypothesis be correct, obfuscation could be achieved by padding packets so that they are all unidentifiable by the single attribute of packet size or the combination of packet size and port number. DoS attacks are a significant threat to computer networks, host devices, and the data needed to be accessed when completing an e-commerce transaction over an IP network. DoS attacks have become a more prevalent security concern with the transition from POTS-connected ATMs to Ethernet IP network-based communications to processing servers. DoS attacks are successful when the attacker overwhelms the target's resources or causes a condition where the communication stream has been altered or corrupted in a manner that disrupts the (TCP) transactions between host and server (Gu & Liu, 2007, p. 458). The implication of a successful DoS attack against an individual ATM is to create a trust issue with the consumer by disrupting the TCP process, thereby causing the transaction to fail due to a DoS attack.

1. Identifying the host and processing server—Using packet sniffing software WireShark, a series of ATM transactions will be performed to capture the packets that make up each transaction. This will serve two functions: first, to identify the IP addresses for both the ATM and the processing agent server, and second, to determine the number and size of each IP packet sent and received in a transaction.

2. Verifying ATM transaction packet size predictability – multiple transactions will be processed and captured via WireShark (WireShark, n.d.). The transaction types, such as incorrect Personal Identification Number (PIN), balance check, insufficient funds, and expired card, will be captured. Three of each type of transaction will be performed and captured via WireShark. A table will be created to analyze each transaction to determine if each number packet has a consistent size, as found in previous research (Volkmuth, 2019). This has been the case at an earlier work as recently as 2018 (Volkmuth, 2019). Table 1 shows the packet size distribution from five different ATM transactions from the previous study:

Table 1

Packet #	Test 1	Test 2	Test 3	Test 4	Test 5
1	60	**62**	**62**	60	60
2	60	60	60	60	60
3	60	60	60	60	60
4	**269**	**269**	**269**	**269**	**269**
5	**793**	**793**	**793**	**793**	**793**
6	60	60	60	60	60
7	244	244	244	244	244
8	60	60	60	60	60
9	**105**	**105**	**105**	**105**	**105**
10	**320**	**320**	**320**	**320**	**320**
11	60	60	60	60	60
13	60	60	60	60	60
14	**83**	**83**	**83**	**83**	**83**
15	60	60	60	60	60
16	60	60	60	60	60
17	60	60	60	60	60

Table 1: Packet Size Distribution

Bue-shaded cells represent packets that include a payload as part of the e-commerce process. The cells with a value of 60 represent overhead packets that are regular functions of a TCP transmission. They include the TCP three-way handshake, receipt verification, retransmitted requests, and TCP teardown. The original data set included two possible outliers with values of 62. These are shaded green.

3. Identifying the uniqueness of IP packet sizes – Using WireShark, a long-duration packet capture will be completed to compile a data set of at least 200,000 packets each. This capture will be sorted by packet size, and a statistical analysis of each packet size will be conducted and compared to the known packet sizes found in the ATM transactions. As shown in the image below, each packet in a Wireshark capture has the attributes of Packet Number, Time Stamp, Source IP address, Destination IP address, Protocol, Length (size), and Information.

Figure 1

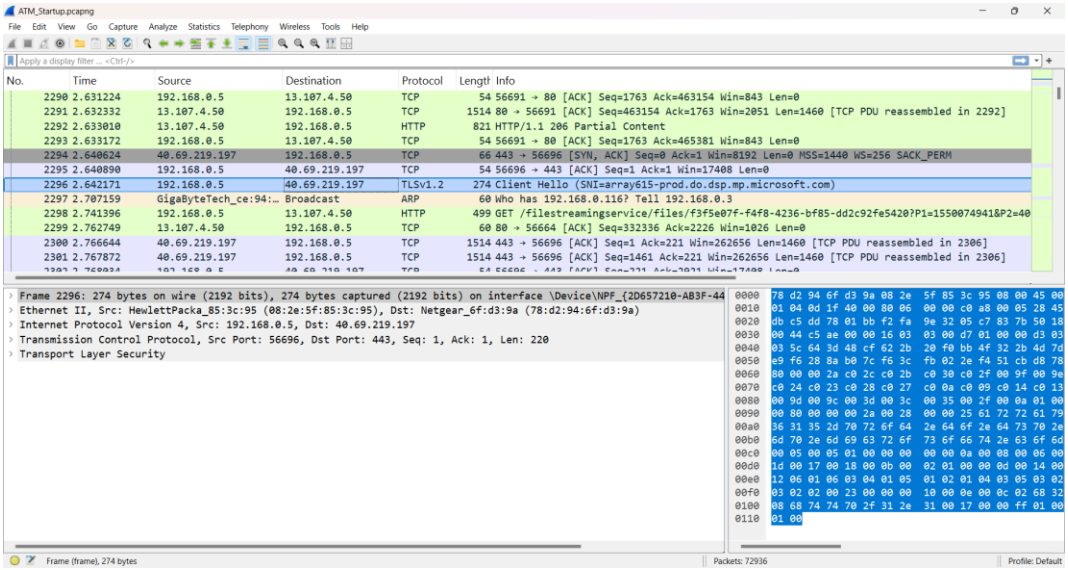
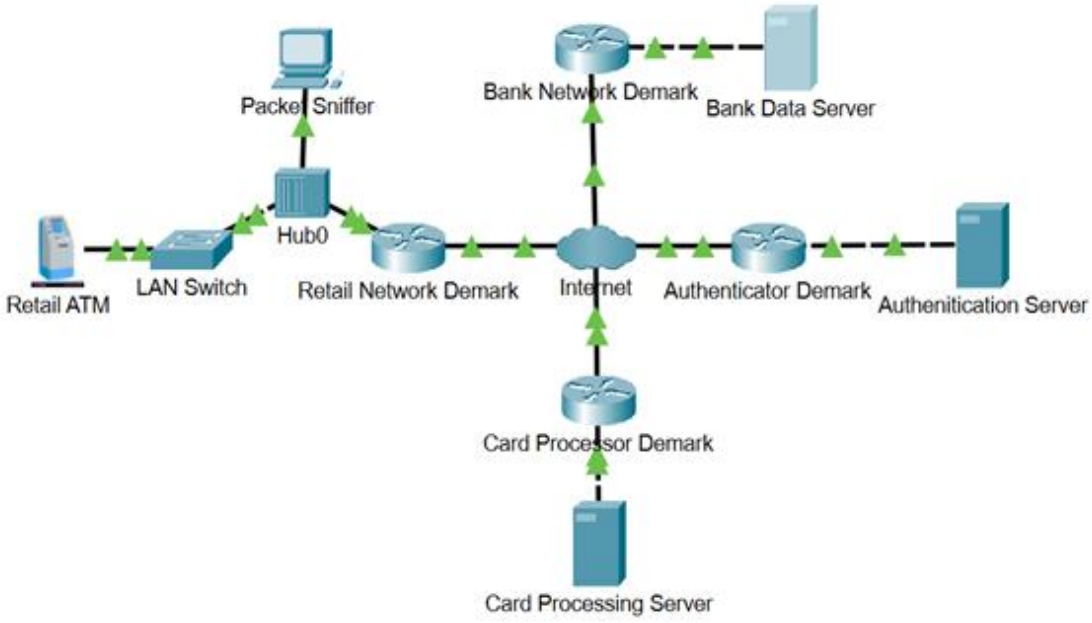


Figure 1: WireShark Sample Capture

Research Environment

Two data collection sessions will be conducted. The first will be in a production environment with an ATM, as shown in Figure 2 below. The host running packet sniffing software will be connected to the ATM production network via a Hub connected to the same Local Area Network (LAN) as the ATM. The first data collection will be to get current packet data from a modern Hyosung Halo II ATM with all current hardware and software updates. The five duplicate transactions used in previous research will be processed, and the data will be collected via WireShark. If similar and unique packet size values are found in the communications stream between the ATM and the processor's server, this will have achieved the study's first goal. All non-unique packet sizes will be analyzed to determine if they are overhead packets and are not of the actual data transfer between the ATM and processing server. In the same way, the unique-sized packets will be analyzed to determine if each is part of the data transmission or overhead.

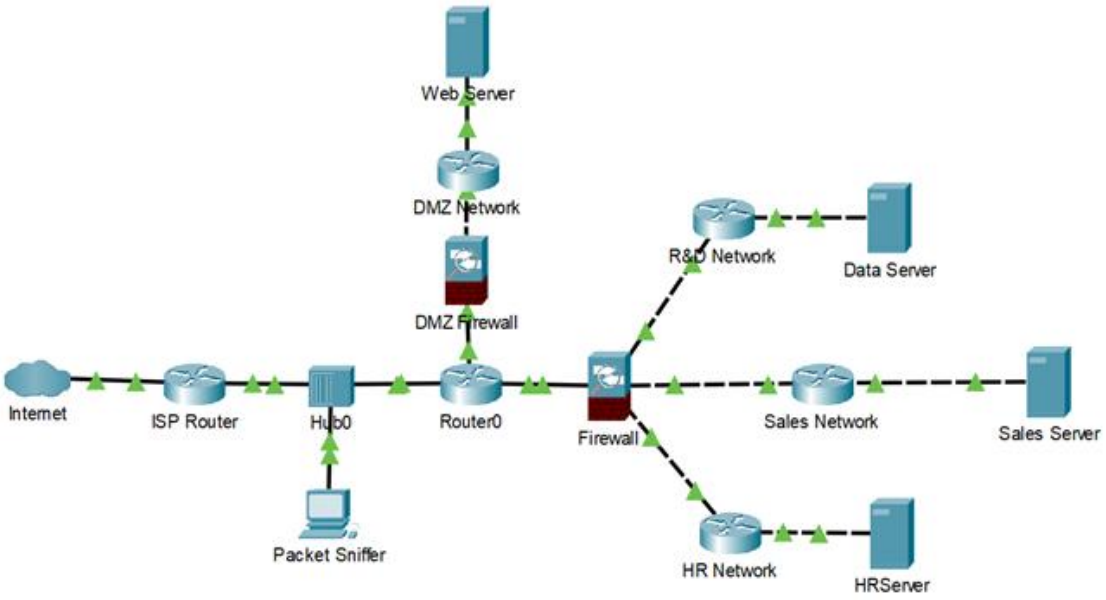
Figure 2 ATM Production Network



The ATM Production Network diagram (Cisco Systems Inc., 2024)

The second data collection will be done on an extensive production network, like the one shown in Figure 3, which may or may not include an ATM. In this data capture, the host running the packet sniffing software will be connected to the production network via a hub positioned between the demark router and the Internet Service Provider's (ISP) router to enable the capture of all inbound and outbound packets of the organization's network. WireShark will collect two fifteen-minute packet sniffing captures long enough to capture 200,000 packets in each session.

Figure 3 Sample Production Network



The Sample Production Network diagram (Cisco Systems Inc., 2024)

Data Analysis

Data analysis of the ATM transaction packets will likely result in static values of payload-carrying packets, as in Table 1 from a previous study. These values will inform the data analysis of the two large packet captures. These captures will be subjected to the process outlined below:

1. ATM traffic is known to use TCP exclusively, so all User Datagram Protocol (UDP) traffic will be excluded from the data set. This can be accomplished within the WireShark application while preserving the raw data. This data can then be exported as a comma-separated value (.csv) file for further analysis.

2. A frequency distribution table will be created from the .csv file for the captured TCP packets, displaying only those packet size values determined to be payload-carrying packets of an ATM transmission.

3. If this analysis determines that there are packet size values that can be identified as being statistically unique to ATM transactions, the goal of this study has been met.

4. If the analysis demonstrates that an ATM transaction does not have a unique packet size, the additional attribute of port number will be added to determine if a suitable level of uniqueness can be discovered.

Conclusion

Attacks on e-commerce solutions such as ATMs have escalated in frequency and sophistication. One method that could be used in this arena is obfuscation. This study hypothesizes that ATM transactions are easily identifiable with only one attribute: the size of the IP packets that make up this process. Proving this hypothesis could pave the way for future work in obfuscation methods in altering packet sizes to be less unique and more difficult to identify with this single attribute.

References

Alqahtani, A. H., & Iftikar, M. (2013). TCP/IP attacks, defenses and security tools. *International Journal of Science and Modern Engineering*, *1*(10), 42–47. Retrieved November 12, 2024, from

Cankaya, E. (2021). Tcp/ip from network security perspective. In *Encyclopedia of cryptography, security and privacy* (pp. 1–4). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-27739-9_1499-1

Cisco Systems Inc. (2024). *Packet Tracer* (Version 8.2.2.0400) [e.g.,[Software]].

Federal Reserve Board. (2023). *Federal reserve payments study 2022*. https://www.federalreserve.gov/paymentsystems/fr-payments-study.htm

Gu, Q., & Liu, P. (2007). Denial of service attacks. *Handbook of Computer Networks: Distributed Networks, Network Planning, Control, Management, and New Trends and Applications*, *3*, 454–468. Retrieved November 8, 2024, from https://s2.ist.psu.edu/paper/DDoS-Chap-Gu-June-07.pdf

Hoque, M. (2024). Exploring the nexus of atm service quality, customer satisfaction, and loyalty in the private banking sector in bangladesh. *Pakistan Journal of Life and Social Sciences (PJLSS)*, *22*(1). Retrieved November 8, 2024, from https://doi.org/10.57239/pjlss-2024-22.1.0074

Idris, B. (2014). *Customer satisfaction of automated teller machine (ATM) based on service quality*. The West East Institute 41 International Academic Conference Proceedings .

Johnson, H. D., Wilson, B. J., & Puterbaugh, J. (2024). BankRate. https://www.bankrate.com/credit-cards/business/what-is-emv-compliance-law-should-your-business-worry/#best

Joshi, M., & Hadi, T. H. (2015). *A review of network traffic analysis and prediction techniques*. https://doi.org/arXiv:1507.05722

Krishnan, D. (2012). Alternate banking channels for customer convenience. *International Journal of Scientific Research*, *2*(2), 9–10. Retrieved November 8, 2024, from https://doi.org/10.15373/22778179/feb2013/4

Mabroukeh, N. R., & Ezeife, C. I. (2010). A taxonomy of sequential pattern mining algorithms. *ACM Computing Surveys*, *43*(1), 1–41. Retrieved November 13, 2024, from https://doi.org/10.1145/1824795.1824798

Nigatu, A., Belete, A., & Habtie, G. (2023). Effects of automated teller machine service quality on customer satisfaction: Evidence from commercial bank of ethiopia. *Heliyon*, *9*(8), e19132. Retrieved November 12, 2024, from https://doi.org/10.1016/j.heliyon.2023.e19132

Parish, D., Bharadia, K., Larkum, A., Phillips, I., & Oliver, M. (2003). Using packet size distributions to identify real-time networked applications. *IEE Proceedings - Communications*, *150*(4), 221. Retrieved November 29, 2024, from https://doi.org/10.1049/ip-com:20030411

Sidel, R. (2015). Theft of debit-card data from ATMs soars. *The Wall Street Journal*. Advance online publication. Retrieved November 8, 2024, from

Tente, D. (2023, August 7). *ATM market in the U.S. continues to thrive*. ATMIA. Retrieved November 8, 2024, from https://www.atmia.com/news/atm-market-in-the-us-continues-to-thrive/20398/

Trivedi, R., & Srivastava, N. (2022). A comprehensive study of outliers. *International Journal of Engineering & Technology, 11*(03). Retrieved November 13, 2024, from https://doi.org/10.17577/IJERTV11IS030051

Valverde, S. C., Humphrey, D. B., & Del Paso, R. L. (2004). *Electronic payments and ATMs: changing technology and cost efficiency in banking*. https://scholar.google.com/scholar?hl=en&as_sdt=0%2C24&q=banks+lower+costs+with+ATMs&btnG=#d=gs_cit&t=1731529184929&u=%2Fscholar%3Fq%3Dinfo%3AxhPkkn8YBJ4J%3Ascholar.google.com%2F%26output%3Dcite%26scirp%3D0%26hl%3Den

Volkmuth, B., & AbuHussein, A. (2019). E-payment security, privacy and trust attributes. In *E-commerce data security with cloud computing* (1st ed.). Cambridge Scholars Publishing.

Volkmuth, B. G. (2019). *Automated teller machine ethernet traffic identification to target forensics detection of IP packets*. The Repository at St. Cloud State University. https://repository.stcloudstate.edu/cgi/viewcontent.cgi?article=1120&context=msia_etds

WireShark Foundation. (2024). *Wireshark 4.4.1 (v4.4.1-0-g575b2bf4746e)* [e.g., [Software]]. https://www.wireshark.org/.

Zhijun, W., Wenjing, L., Liang, L., & Meng, Y. (2020). Low-rate dos attacks, detection, defense, and challenges: A survey. *IEEE Access*, *8*, 43920–43943. Retrieved November 12, 2024, from https://doi.org/10.1109/access.2020.2976609