BOOK CHAPTER | *“What’s in the Packet”*

A Survey Of Packet Analysis For Network Forensics

Michael Kodjo Agorsah
Digital Forensics & Cyber Security Graduate Programme
Department Of Information Systems & Innovations
Ghana Institute of Management & Public Administration
Greenhill, Accra, Ghana
E-mail: mkagorsah@gmail.com
Phone: +233540443303

ABSTRACT

Network forensics is a branch of the network security paradigm (a collection of rules and configurations for protecting the integrity, confidentiality, and accessibility of computer networks and data using both software and hardware technologies) that focuses on network attack prevention and detection. It solves the present model's lack of specific investigation tools for probing harmful activities in networks. It also monitors the network for attacks and analyzes the attackers' characteristics. Packet analysis is the most common technique in network forensics, and it may replay the whole network traffic for a given period if the packet characteristics gathered are sufficiently detailed. The data collected can be utilized to track down traces of illegal internet activity, data breaches, unauthorized website access, malware infection, and so on across the network. This article provides a thorough packet analysis approach with extensive network traffic categorization and pattern detection capabilities, as well as a broad examination of the use of packet analysis in network forensics. Because not all network data can be used in court, the categories of digital evidence that may be acceptable are described in depth. The features of both hardware appliances and packet analyzer software are examined in light of their potential applications in network forensics.

Keywords: Network Forensics, Computer & Network Security, Digital Forensics, Local and Wide Area Network, Internet

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

Citation: Michael Kodjo Agorsah (2022): Analysis of Attack Intention Recognition
Book Chapter Series on Research Nexus in IT, Law, Cyber Security & Forensics. Pp 263-266
www.isteams.net/ITlawbookchapter2022. dx.doi.org/10.22624/AIMS/CRP-BK3-P42

1. INTRODUCTION

With the growing popularity, if not already grown online services, security experts and law enforcement organizations need to develop new methods for investigating cybercrime and obtaining evidence that can be used in court. Internet services send vast volumes of data via communication networks in various formats, the most common of which are networking packets. When recorded, stored, and analyzed correctly, network packets can be used in the investigation process and potentially give legal evidence in court cases.

1.1 Background to the Study

Analyzing network forensics is more challenging than digital forensics because volatile data is lost once sent over the network. Digital forensics works with data at rest, while network forensics focuses on dynamic information. In surveying packets for network forensics, the following steps are used.

Network Packet Capture and Storage

Purpose-built software can analyze network data and separate network traffic by type. Packet analyzers are protocol analyzers that are specifically built for packet analysis ie packet sniffers and network analyzers Through the act of packet capture, these software tools intercept and log network traffic transiting through a digital network or a portion.

Table 1.0 Literature Review Findings gaps and Recommendations

Literature	Findings	Gaps	Recommendations
Tcpdump	one of the de facto standard command-line tools for recording and dumping network packets for subsequent analysis	It is a command-line tool and packets with invalid checksum are ignored	It's feasible to create a graphical user interface for analyzing the results. This will help to improve the current system's user-friendliness.
Paessler's PRTG Network Monito	a tool for capturing packets, offers additional features, such as displaying the bandwidth usage of various forms of network traffic.	This tool's network analyzing skills are limited to data packet headers,	Lee et al. (2011) introduced an Apache Hadoop-based packet processing tool, which can open even petabyte-sized packet capture files, to address the inefficient processing of large packet capture files with traditional packet analyzers running on a single host with limited computing and storage resources.

Network packets as well as packet flow analysis

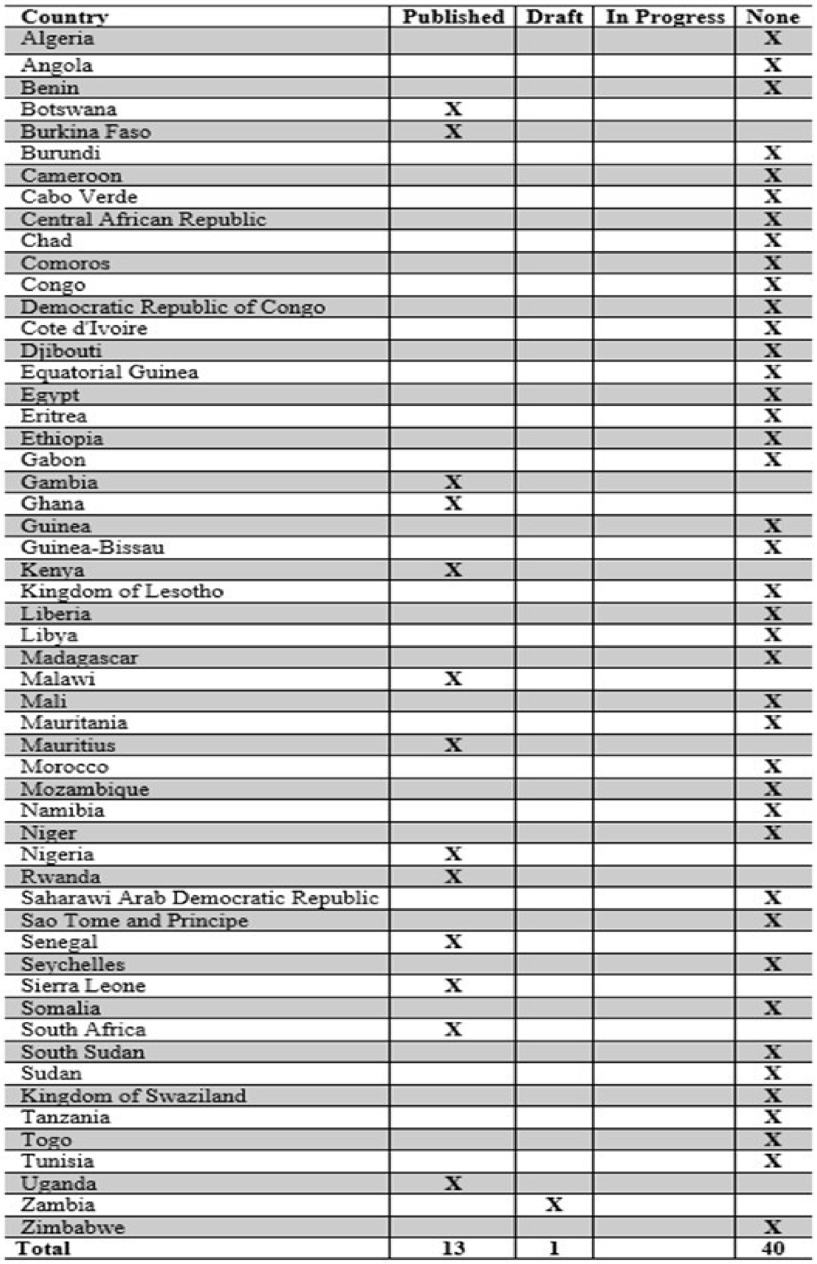
Files that traversed a network can be recovered from network packet streams Using network carvers or packet analyzers developed specifically for file export from packet capture. Deep packet sniffing and packet inspection, artificial captures the semantics of actual network packets using deep packet sniffing and packet inspection and provide terminology to formally convey background knowledge in a machine-interpretable form constituting forensic evidence
Analyzers of network packets. Most packet analyzers are competent in both live and offline analysis. Only packet analyzers that handle hundreds of protocols can do deep packet inspection and analysis of many forms of network traffic. Wireless analyzers are packet analyzers that intercept traffic over wireless networks.

3. AFRICA'S OVERVIEW OF NETWORK FORENSICS, CYBERSECURITY AND INTERNET SAFETY

As the world rebounds from the COVID-19 pandemic's disruptions, coping methods like growing usage of virtual offices, online marketplaces, and e-governance have become the norm. While this gives potential to restructure economies and improve government service delivery, it may also increase cybercrime susceptibility.

To address these flaws, a stronger commitment to network forensics and cybersecurity is required. This necessitates enforceable legislative safeguards, risk prevention and management strategies, as well as technology and infrastructure capable of safeguarding each country's cyber environment, as well as individual and corporate end-user assets.

Table 1: Published Data on Africa’s Cyber Safety Outlook



Country	Published	Draft	In Progress	None
Algeria				X
Angola				X
Benin				X
Botswana	X			
Burkina Faso	X			
Burundi				X
Cameroon				X
Cabo Verde				X
Central African Republic				X
Chad				X
Comoros				X
Congo				X
Democratic Republic of Congo				X
Cote d'Ivoire				X
Djibouti				X
Equatorial Guinea				X
Egypt				X
Eritrea				X
Ethiopia				X
Gabon				X
Gambia	X			
Ghana	X			
Guinea				X
Guinea-Bissau				X
Kenya	X			
Kingdom of Lesotho				X
Liberia				X
Libya				X
Madagascar				X
Malawi	X			
Mali				X
Mauritania				X
Mauritius	X			
Morocco				X
Mozambique				X
Namibia				X
Niger				X
Nigeria	X			
Rwanda	X			
Saharawi Arab Democratic Republic				X
Sao Tome and Principe				X
Senegal	X			
Seychelles				X
Sierra Leone	X			
Somalia				X
South Africa	X			
South Sudan				X
Sudan				X
Kingdom of Swaziland				X
Tanzania				X
Togo				X
Tunisia				X
Uganda	X			
Zambia		X		
Zimbabwe				X
Total	13	1		40

However, according to the International Telecommunication Union's (ITU) 2018 Global Cybersecurity Index (GCI), Africa's commitment to cybersecurity – as well as its capacity to respond to threats remains low in comparison to other continents.

Current State

8 African countries have a national cybersecurity strategy, according to a survey conducted by the African Union Commission (AUC) in 2018[2]. The table 2.0 above depicts this current state. Source: Table 1 State of National Cyber Security Strategy

4. IMPLICATIONS OF NETWORK FORENSICS

Modern network forensic techniques encounter a number of obstacles that must be overcome in order to improve the methodologies. High storage speed, the need for plenty of storage space, data integrity, data privacy, access to IP addresses, and data extraction location are only a few of the major challenges.

5. CONCLUSION

In-network forensics, analyzing network packets is essential for collecting data needed to gain a comprehensive picture of online user actions at a specific moment in time and serving evidence admissible in court. Even if some people are skeptical about the reliability of information retrieved or reconstructed from packet data, network packets complement other data sources, such as corporate firewall logs, and in many cases, they are the only source of information about what happened during an online activity and who was involved. Because packet analysis in network forensics differs from other application areas like intrusion detection, the potential of packets as forensic evidence has been described, as well as the limitations.

REFERENCES

1. Parker, D. (1993). The state of security in cyberspace. Computer Fraud & Security Bulletin, 1993(8), 15–18. https://doi.org/10.1016/s0142-0496(09)90054-6
2. Easttom, C. (2021). *Digital Forensics, Investigation, and Response* (4th ed.). Jones & Bartlett Learning Publishers
3. M. Afanasyev, T. Kohno, J. Ma, N. Murphy, S. Savage, A.C. Snoeren, G.M. Voelker *Privacy-preserving network forensic.* Commun. ACM, 54 (5) (2011), pp. 78-87, 10.1145/1941487.1941508
4. Al-Duwairi, Govindarasu, B. Al-Duwairi, M. Govindarasu (2006). *Novel hybrid schemes employing packet marking and logging for IP traceback.* IEEE T. Parallel. Distr., 17 (5) (2006), pp. 403-418, 10.1109/TPDS.2006.63
5. Alhawi et al., O.M.K. Alhawi, J. Baldwin, A. Dehghantanha (2018): *Leveraging machine learning techniques for Windows ransomware network traffic detection. https://ui.adsabs.harvard.edu/abs/2018arXiv180710440A/abstract*
6. *A.* Dehghantanha, M. Conti, T. Dargahi (Eds) ((2018), *Cyber Threat Intelligence*, Springer, Cham, pp. 93-106, 10.1007/978-3-319-73951-9_5
7. Alshammari and Zincir-Heywood, R. Alshammari, A.N. Zincir-Heywood (2015): *Identification of VoIP encrypted traffic using a machine learning approach*
8. J. King Saud Univ. Comput. Inf. Sci., 27 (1) (2015), pp. 77-92, 10.1016/j.jksuci.2014.03.013
9. Alsmadi et al., I. Alsmadi, R. Burdwell, A. Aleroud, A. Wahbeh, M. Al-Qudah, A. Al-Omari (2018) *Network forensics: lesson plans Practical Information Security: A Competency-Based Education Course*, Springer, Cham (2018), pp. 245-282, 10.1007/978-3-319-72119-4_11
10. Ansari et al., 2003 S. Ansari, S.G. Rajeev, H.S. Chandrashekar *Packet sniffing: a brief introduction.* IEEE Potentials, 21 (5) (2003), pp. 17-19, 10.1109/MP.2002.1166620
11. Taylor CEndicott-Popovsky BFrincke D (2007): Digital Investigation (2007) 4(SUPPL.) 101-104