Network Forensics: Further Reading and Resources

Network forensics involves capturing and examining network traffic to investigate security incidents and cybercrimes [1] [2]. It lies at the intersection of incident response, network security and digital forensics [1]. Modern environments generate enormous traffic volumes, so investigators rely on automated analysis and ML techniques (e.g. Rizvi *et al.* survey AI-driven network forensics [1]). Authoritative guides (e.g. NIST SP 800-86) explain that **Network Forensic Analysis Tools (NFATs)** typically combine packet sniffers and protocol analyzers, focusing on collecting and replaying traffic for analysis [2] [3].

Key Surveys and Models

Recent research provides updated frameworks and surveys. For example, Rizvi *et al.* (2022) offer a **comprehensive survey** of AI and ML approaches in network forensics, noting that investigations must handle huge traffic volumes, false positives, and new environments (IoT, cloud) [1]. Alansari (2023) proposes a **six-phase forensic model** (identification, verification, gathering, preservation, examination, analysis, plus reporting) that integrates with standard procedures to ensure complete evidence collection [4]. These works highlight that while many tools exist, there is still a need for systematic guidelines and adaptive models for network investigations [1] [4].

Tools and Techniques

Packet Capture & Analysis: Fundamental tools like **Wireshark** or **tcpdump** capture raw traffic for offline analysis. **Network sniffers/IDSs** (e.g. Snort, Suricata) can log and classify packets as they pass through the network. A 2024 SANS study specifically compares Snort, Suricata and **Zeek** (Bro) for vulnerability detection, showing these open-source tools are widely used in network forensic workflows [5]. For deeper analysis, tools such as **Zeek** provide scripting and high-fidelity logs of network events [6] [5].

Advanced NFATs: NIST notes that specialized NFATs often include features to *replay* recorded traffic sessions (at variable speeds) and to *visualize* host relationships or geolocate IPs [3]. They may also build profiles of normal behavior or search packet contents for keywords. Many investigators integrate these tools with **SIEM platforms** or specialized analyzers to correlate logs, flows, and alerts.

Case Studies and Applications

Academic and industry papers demonstrate network forensics in practice. For instance, Do *et al.* (2019) address **SDN-specific forensics**: they propose *SDNLog-Foren*, a blockchain-based system to secure SDN controller logs against tampering [7]. This work (from Vietnam Nat'l Univ. HCMC) highlights that attackers could erase or alter network logs, so immutable storage (blockchain) can preserve evidence integrity [7]. More generally, surveys cover IoT and cloud forensics, and incident reports often detail how packet evidence or flow data were used to trace attacks (e.g. DDoS or data breaches). Understanding real-world cases reinforces concepts like **chain of custody** and evidence preservation.

Vietnam-Specific Research

Vietnamese researchers are contributing to global network-forensics knowledge. Besides SDN logs [7], other local studies (e.g. by authors at VNIT, VNU, etc.) explore topics like IoT traffic analysis, intrusion forensics or forensic lab design. Practical training centers in the region (e.g. ASEAN-Japan cybersecurity center) have emphasized network forensics in their curricula [8] [7]. While the principles are universal, students should be aware of regional initiatives and tools (e.g. VN-developed honeypots or analysis frameworks) when possible.

Reading Checklist for Students

- **Review network forensic fundamentals:** Read the survey by Rizvi *et al.* [1] to understand how network forensics is defined and why AI/ML methods are increasingly needed. Note the challenges of big data and false positives.
- **Study forensic process models:** Examine Alansari's model [4] outlining stages of a network investigation (identification through reporting). Compare it with the NIST/SP800-86 definitions of NFATs (how traffic is collected and analyzed) [2] [3].
- **Explore tools and hands-on techniques:** Learn key tools (Wireshark, Zeek, Snort). For example, the Zeek documentation [6] describes how Zeek logs network activity. Use NIST guidance to practice packet capture and session reconstruction. Consider reading the SANS whitepaper [5] that compares Snort/Suricata/Zeek, noting each tool's strengths.
- **Analyze case studies:** Read Do *et al.* (2019) on SDNLog-Foren [7] to see a blockchain application for network forensics in SDN. Research additional incident write-ups (e.g. published breach analyses) to see how network evidence is collected in practice.
- **Local context:** Investigate any Vietnamese research projects or tools (e.g. VN honeypot deployments, national CERT reports) related to network forensics. Connect with lab exercises or competitions (e.g. Cyber SEA Games) that feature network traffic analysis.

Key Tools and Resources: Practice capturing network packets (e.g. using Wireshark or tcpdump) and analyzing them with tools like **Zeek**, **Splunk**, or **NetworkMiner**. Review the NIST SP 800-86 Guide for general forensic procedures [2]. Engage with open-source datasets (e.g. CICIDS) to hone skills.

Sources: Authoritative surveys and guides [1] [2] [4], practitioner whitepapers [5], and recent research [7] provide both theory and practical insight. Each reference above contains further bibliographies to explore.

[1] Application of Artificial Intelligence to Network Forensics: Survey, Challenges and Future Directions
https://forensicsandsecurity.com/papers/AIforNetworkForensics.pdf

[2] [3] NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response
https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-86.pdf

[4] Microsoft Word - ETASR_V13_N5_pp11871-11877
https://etasr.com/index.php/ETASR/article/download/6316/3280/23007

[5] Evaluating the Efficacy of Network Forensic Tools: A Comparative Analysis of Snort, Suricata, and Zeek in Addressing Cyber Vulnerabilities
https://www.sans.org/white-papers/evaluating-efficacy-of-network-forensic-tools-comparative-analysis-snort-suricata-zeek-addressing-cyber-vulnerabilities

[6] The Zeek Network Security Monitor
https://zeek.org/

[7] SDNLog-Foren: Ensuring the Integrity and Tamper Resistance of Log Files for SDN Forensics using Blockchain (2019) | Hien Do Hoang | 16 Citations
https://scispace.com/papers/sdnlog-foren-ensuring-the-integrity-and-tamper-resistance-of-o0qqqysge1

[8] 2022 Volume 4 ASEANs Resilience in Capacity Building
https://www.isaca.org/resources/isaca-journal/issues/2022/volume-4/aseans-resilience-in-capacity-building