World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:19, No:01, 2025

Packet Analysis in Network Forensics: Insights ,Tools, and Case Study

Authors : Dalal Nasser Fathi, Amal Saud Al-Mutairi, Mada Hamed Al-Towairqi, Enas Fawzi Khairallah

Abstract : Network forensics is essential for investigating cyber incidents and detecting malicious activities by analyzing network traffic, with a focus on packet and protocol data. This process involves capturing, filtering, and examining network data to identify patterns and signs of attacks. Packet analysis, a core technique in this field, provides insights into the origins of data, the protocols used, and any suspicious payloads, which aids in detecting malicious activity. This paper explores network forensics, providing guidance for the analyst on what to look for and identifying attack sites guided by the seven layers of the OSI model. Additionally, it explains the most commonly used tools in network forensics and demonstrates a practical example using Wireshark.

Keywords : network forensic, packet analysis, Wireshark tools, forensic investigation, digital evidence
Conference Title : ICCSCIT 2025 : International Conference on Computer Science, Cybersecurity and Information Technology
Conference Location : London, United Kingdom
Conference Dates : January 23-24, 2025