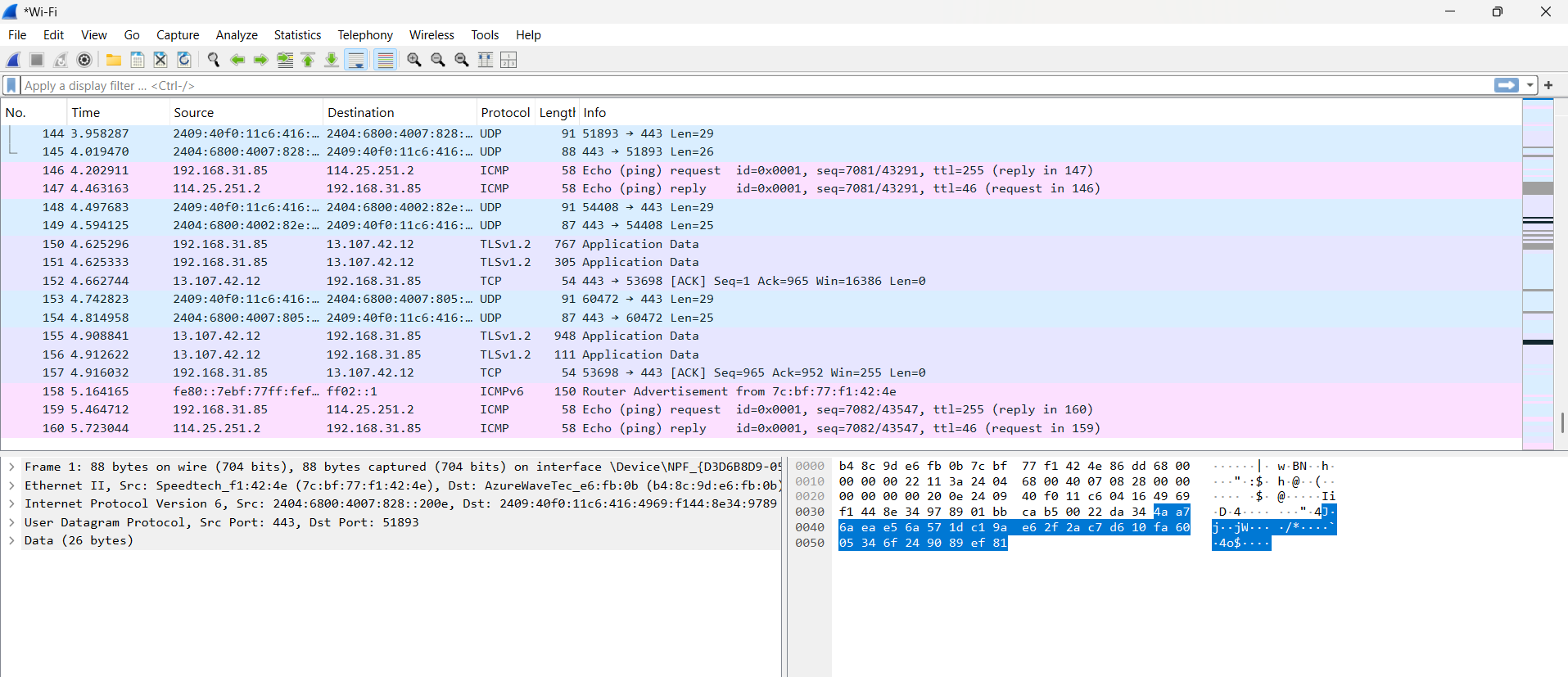
**Wireshark**

****

**Wireshark** is a leading open-source network protocol analyzer available for both command-line interface (CLI) and graphical user interface (GUI) environments, though it is best known for its robust GUI. It is widely used by network administrators, security professionals, and penetration testers for capturing, analyzing, and troubleshooting network traffic.

Wireshark

* **Graphical User Interface (GUI):**
  + **Primary Mode:** Most users interact with Wireshark through its intuitive GUI, which visualizes captured packets in a detailed, navigable format.
  + **Features:**
    - Real-time and offline packet capture and analysis.
    - Advanced filtering and search capabilities to focus on specific traffic or protocols.
    - Protocol dissection for in-depth inspection of headers and payloads.
    - Flow graphs, statistics, and visualizations for traffic analysis.
    - Support for hundreds of protocols out of the box, with extensibility for custom protocols[2](https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html)[3](https://www.techtarget.com/whatis/definition/Wireshark)[5](https://www.knowledgehut.com/blog/security/what-is-wireshark).
  + **Use Cases:** Network troubleshooting, security analysis, performance monitoring, and forensics.

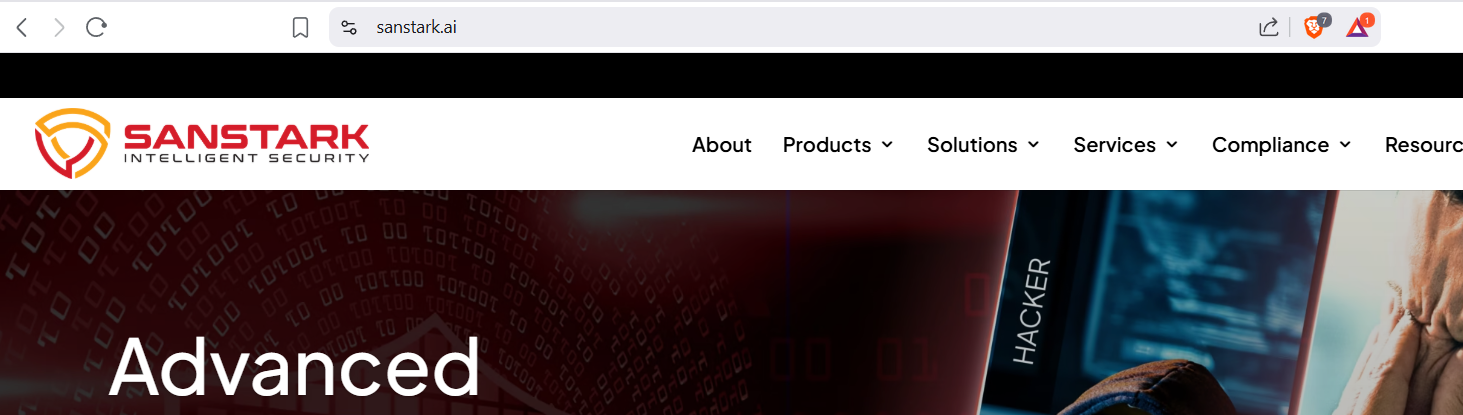
Key Security Uses

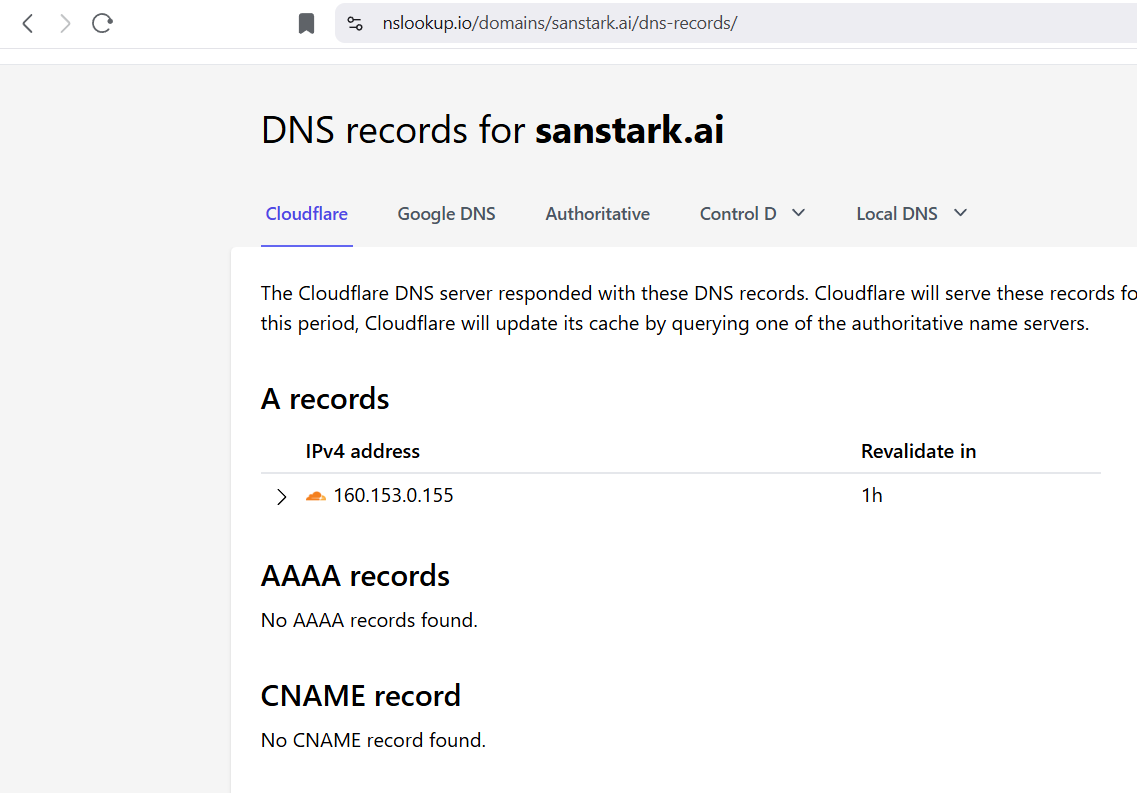
* **Traffic Analysis:** Inspect live or recorded network traffic for anomalies, suspicious patterns, or unauthorized activities.
* **Intrusion Detection:** Identify signs of attacks such as port scanning, unusual payloads, or command-and-control communications.
* **Malware Analysis:** Detect and analyze network-based malware by examining packet contents and communication patterns.
* **Forensics:** Reconstruct network sessions and investigate security incidents by analyzing packet captures.
* **Vulnerability Assessment:** Identify weak authentication, unencrypted data, or risky configurations by inspecting protocol details.

Wireshark in Network Security

Wireshark is an essential tool in both networking and security workflows. Its GUI makes it accessible for interactive analysis, while its CLI counterpart (tshark) enables automation and integration into larger security pipelines.Your networking and security background aligns well with leveraging Wireshark for troubleshooting, monitoring, and threat detection

**Ex site**

****

 **packet capture**