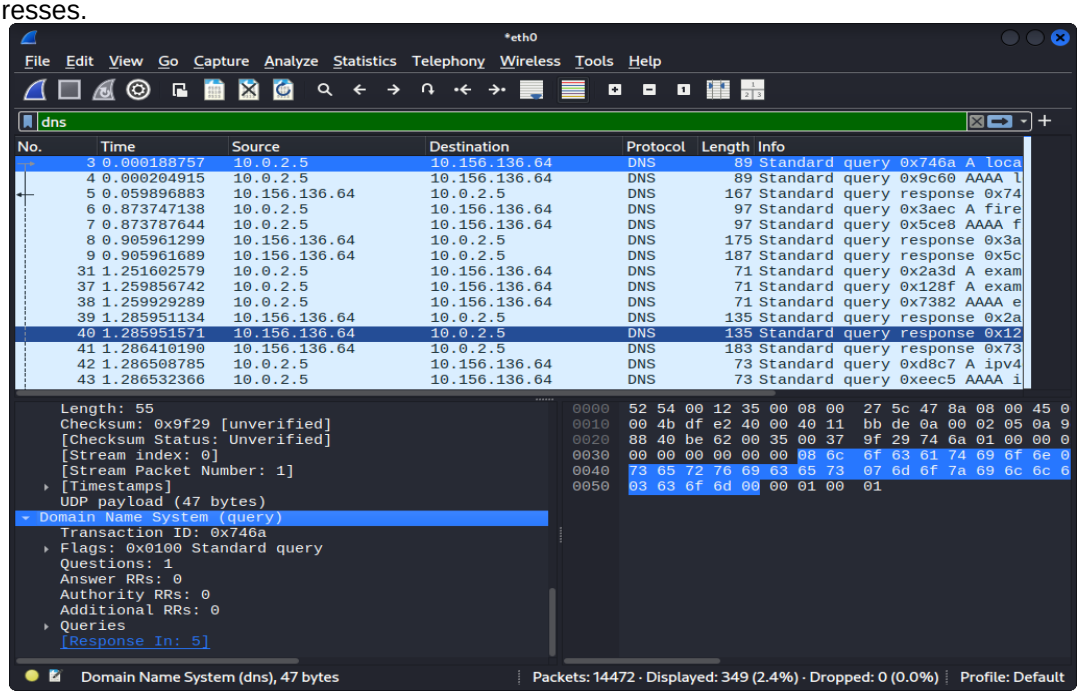
Wireshark Packet Capture Report

This report provides an analysis of network traffic captured using Wireshark. The capture session involved browsing websites and generating network activity. The data was filtered by different protocols including DNS, HTTP, and TCP to identify key traffic patterns.

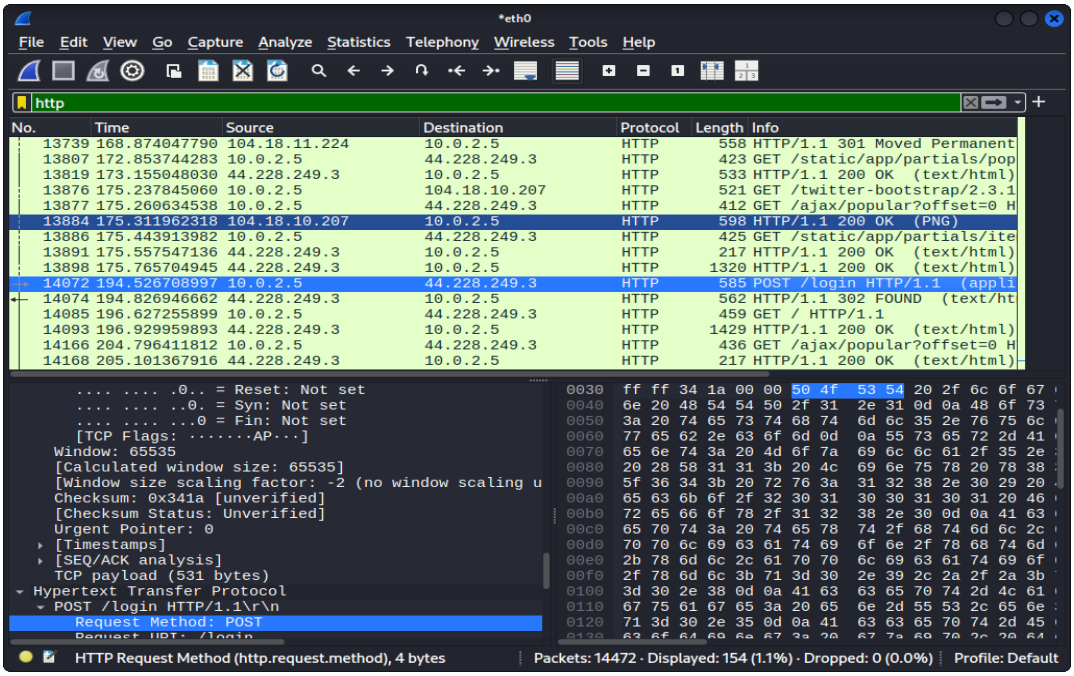
1. DNS Protocol Analysis

The DNS (Domain Name System) protocol was captured showing domain resolution queries and responses. DNS packets are essential for translating human-readable domain names into IP addresses.



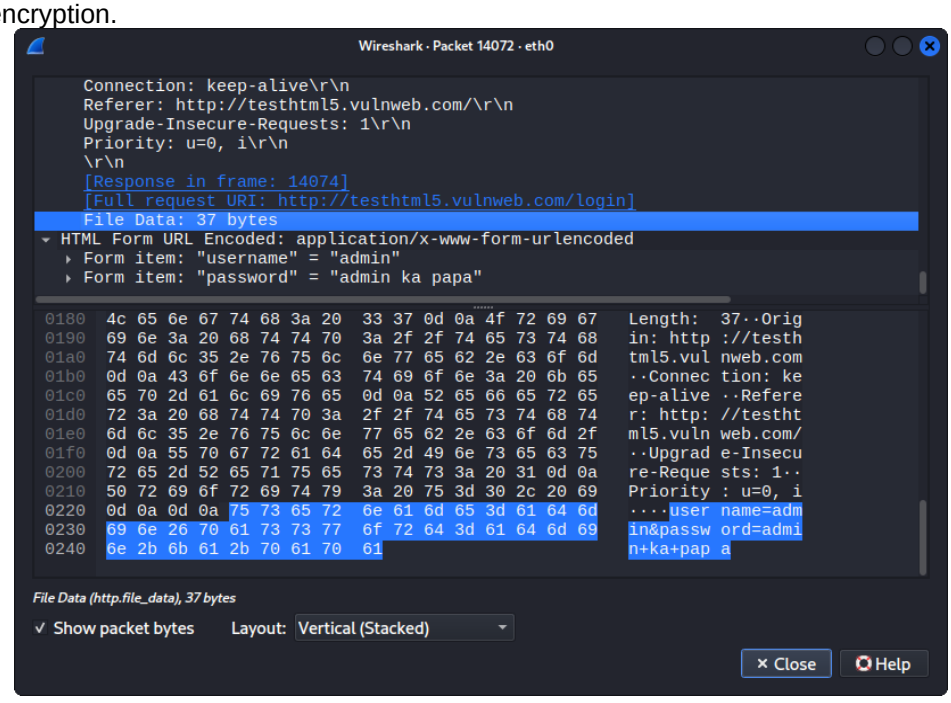
2. HTTP Protocol Analysis

HTTP traffic was captured, showing both GET and POST requests. One notable POST request included login form data being sent in plaintext, which indicates an insecure transmission.



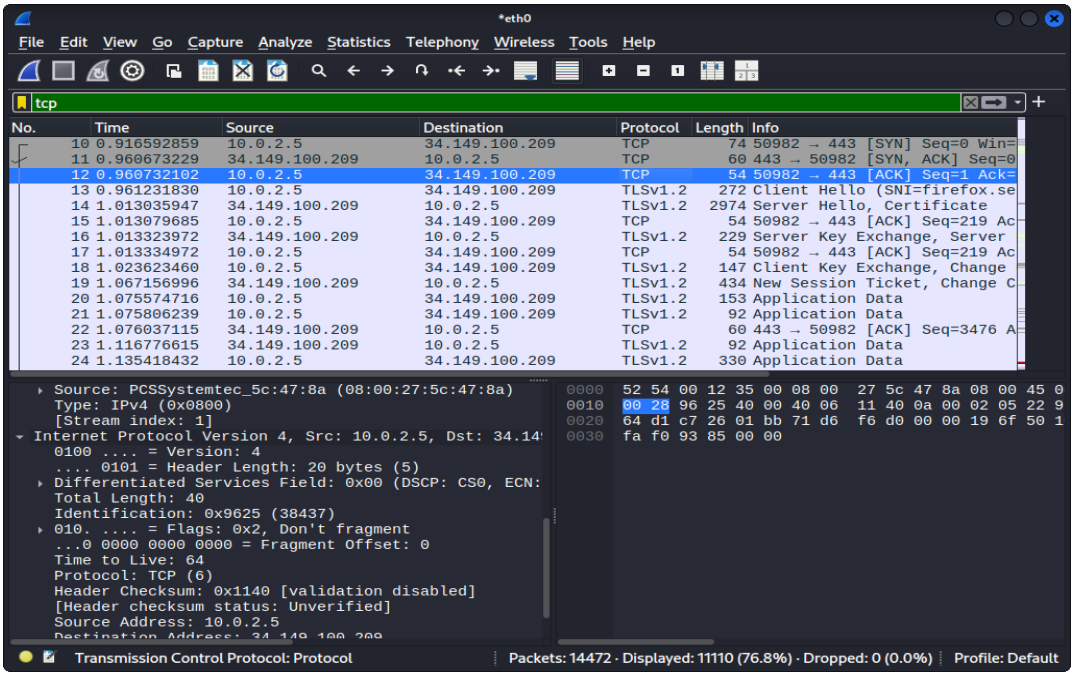
3. Sensitive Data Exposure

The captured HTTP POST request to 'testhtml5.vulnweb.com/login' contained plaintext credentials: - Username: admin - Password: admin ka papa This highlights the risk of transmitting sensitive data without encryption.



4. TCP Protocol Analysis

TCP packets show the handshake and data transfer process between the client and server. Several TLS-encrypted sessions were observed, indicating secure communication channels.



Summary of Findings

1. DNS queries reveal the domains being accessed. 2. HTTP traffic shows unencrypted credentials being transmitted. 3. TCP packets indicate both encrypted and unencrypted communication. 4. Sensitive information should always be transmitted over HTTPS to ensure security.