# **CTF Topic: Packet Analysis With Wireshark**

# **1. Introduction**



Packet analysis is a crucial skill for anyone interested in network security, forensics, and troubleshooting. Wireshark is one of the most powerful tools available for this purpose. In this Capture the Flag (CTF) challenge, you'll learn how to use Wireshark to analyze network traffic and solve various tasks.

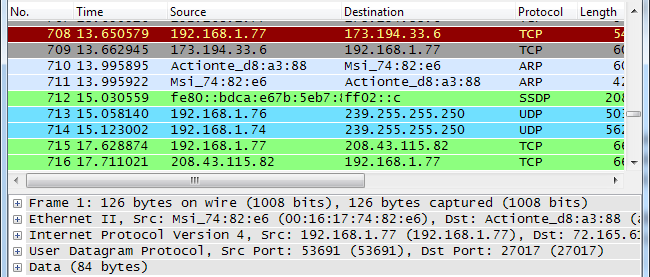
# **2. Tools and requirements**

* [Wireshark](https://www.wireshark.org/download.html) :
* Basic Networking

# **Link**

Log file: <https://www.mediafire.com/file/xin8yatz3c7sgbb/Analysis+the+log.pcapng/file>

# **Scenario**



Use Wireshark to analyze the provided PCAP file, focusing on HTTP traffic to identify if any credentials were transmitted without encryption.

# **Process to Perform**

* Download the log file from Link and analyze the packet
* http.host contains "altoro.testfire.net"
* http.request.method == "POST" and http.request.uri contains "/login.jsp"

# **Let’s start the Challenge**

# **Question**

Flag 1: What is the Password shown in the log file?

Answer: admin

Flag 2: Are the username and password Encrypted or in Plaintext Through Transmission?

Answer: Plaintext

Flag 3: What is the Destination IP?

Answer:65.61.137.117

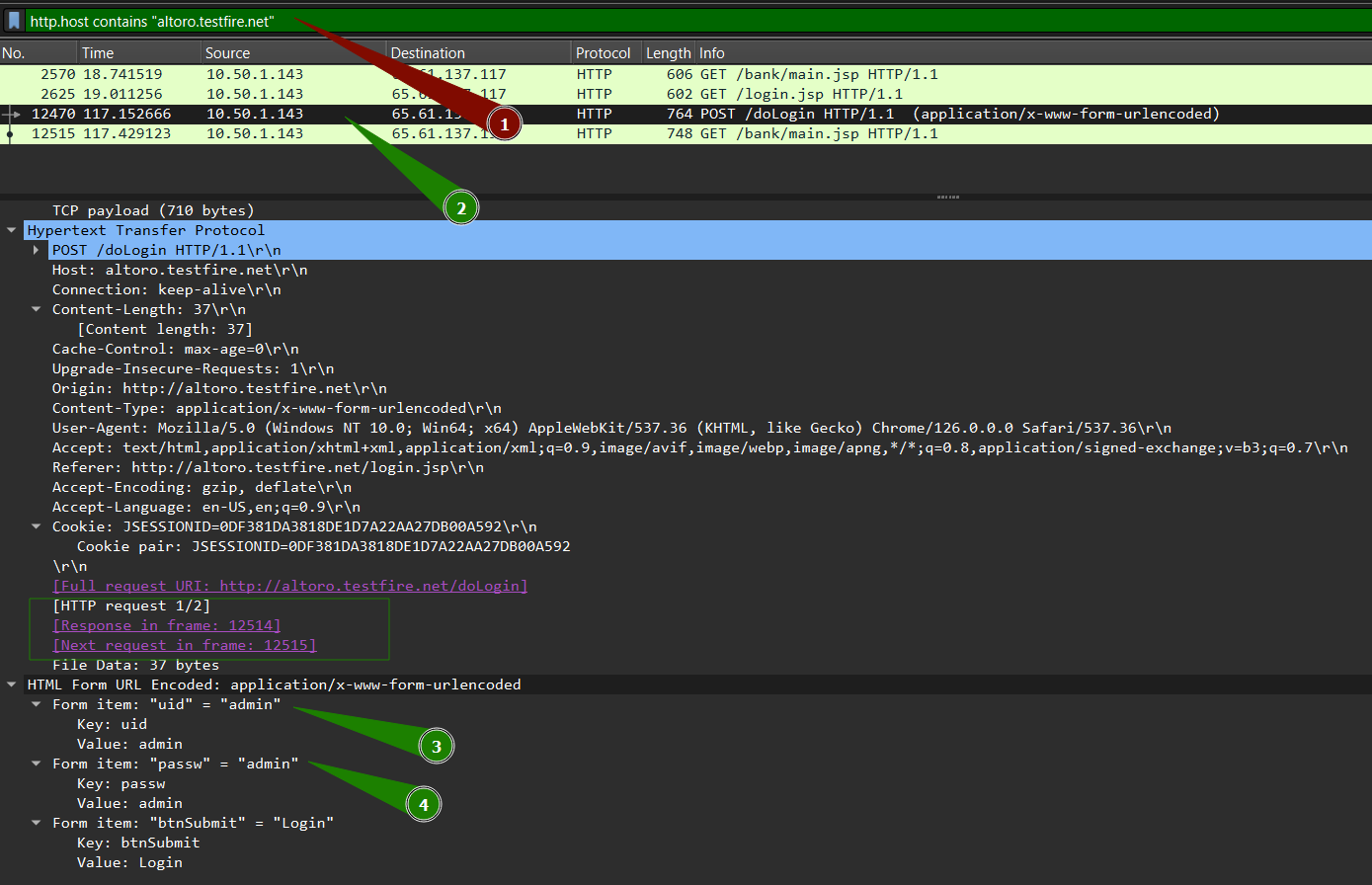
Flag 4: What is the protocol used by the website?

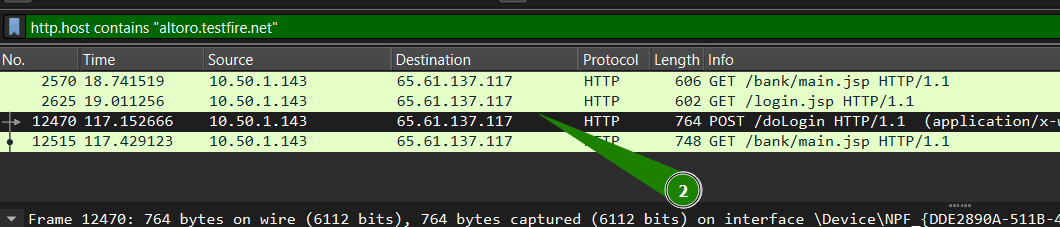
Answer: HTTP

Flag5: Is HTTP Secure Protocol?

Answer: No

# **Hint**



****

**Packet Filteration Command**

* http.host contains "altoro.testfire.net"
* http.request.method == "POST" and http.request.uri contains "/login.jsp"