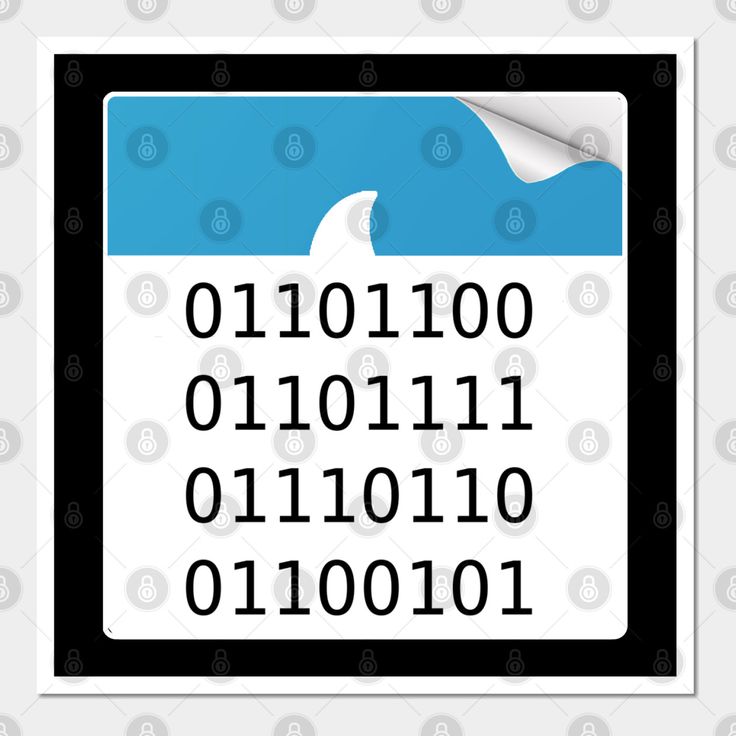
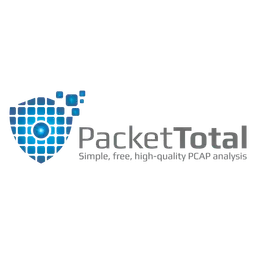
# **CTF Topic: PacketTotal**



# **Introduction**



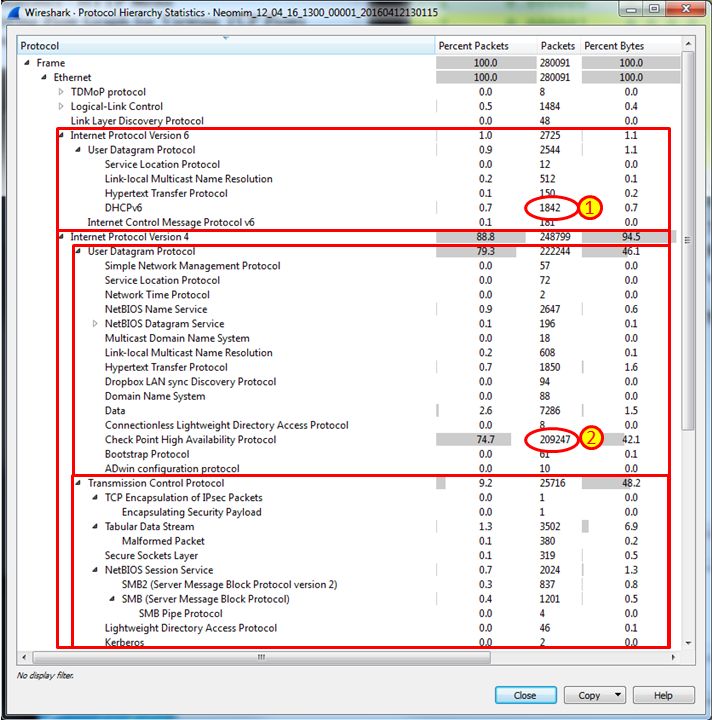
Welcome to the PacketTotal CTF Challenge! This challenge will help you understand how to analyse network packet captures (PCAPs) using PacketTotal, a powerful tool for security professionals and enthusiasts. You'll learn to identify malicious traffic, extract useful information, and interpret results.

# **Tools and requirements**

Packet tool

A computer with internet access

# **Scenario**



You've been provided with a PCAP file that contains network traffic from a suspected security incident. Your task is to analyse this PCAP file using PacketTotal to identify any malicious activity and extract key information.

# **Process to Perform**

Go to your browser and open the link: <https://lab.dynamite.ai/>

Upload to PacketTotal:

Go to PacketTotal.

Upload the PCAP file for analysis which is given below.

<https://www.mediafire.com/file/v3lz4tsaken2vu4/PCAPdroid_02_Jul_21_31_03.pcap/file>

# **Let's Begin The Challenge**

# **Question**

**Question 1**

What is the total number of packets captured in the provided PCAP file?

**Hint 1: 49**

**Question 2**

What is the total number of ip addresses and links in the given .pcap file?

**Hint 4: 15 ip address and 49 links.**

# **Hint**

