unknown-traffic1

The flag is hidden base64-encoded data from ICMP packets. The following script decodes it, and extracts the CTF flag.

```
#!/usr/bin/env python3
import re
import pyshark
from base64 import b64decode

PCAP_FILE = "unknown-traffic1.pcap"
FLAG_PATTERN = r"ctf{[a-f0-9]+}"

def extract_data_from_pcap(filename: str) -> str:
    """Extract and concatenate ICMP payload data from a pcap file."""
    capture = pyshark.FileCapture(filename)
    collected = []

    for packet in capture:
        if "ICMP" not in packet:
            continue

        payload = bytes.fromhex(packet.icmp.data)
        if b"00" in payload:
            continue

        try:
            collected.append(payload.decode())
        except UnicodeDecodeError:
            continue  # skip invalid decodings

    capture.close()
    return "".join(collected)

def find_flag(data: str, pattern: str) -> str:
    """Decode base64 data and search for the flag using regex."""
    decoded = b64decode(data).decode()
    match = re.search(pattern, decoded)
    return match.group(0) if match else None

if __name__ == "__main__":
    full_data = extract_data_from_pcap(PCAP_FILE)
    flag = find_flag(full_data, FLAG_PATTERN)
    if flag:
        print(flag)
```

```
    else:
        print("Flag not found.")
```