Detection of Trojans and Backdoors in Network Traffic

1 Lab Setup

First, install the required tools (Git and Wireshark) using the following command:

```
sudo apt install git wireshark
```

Next, clone the repository containing the lab materials:

```
git clone https://github.com/Milansuman/sns-trojan-forensics
cd sns-trojan-forensics
```

The file `network-backdoor.pcapng` will be used for this analysis.

2 Analysis Procedure

2.1 Initial Packet Capture Review

Open `network-backdoor.pcapng` using Wireshark. The capture contains packets collected during malware execution mixed with regular network traffic.

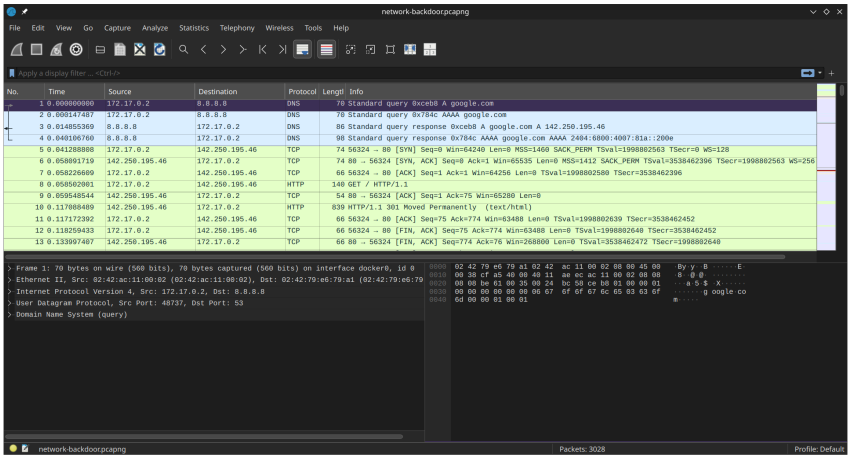

Figure 1: Wireshark main interface showing captured packets

2.2 Identifying Suspicious Traffic

Inspect the packets for suspicious HTTP requests or command-and-control traffic. Pay particular attention to packets containing shell commands or command outputs.

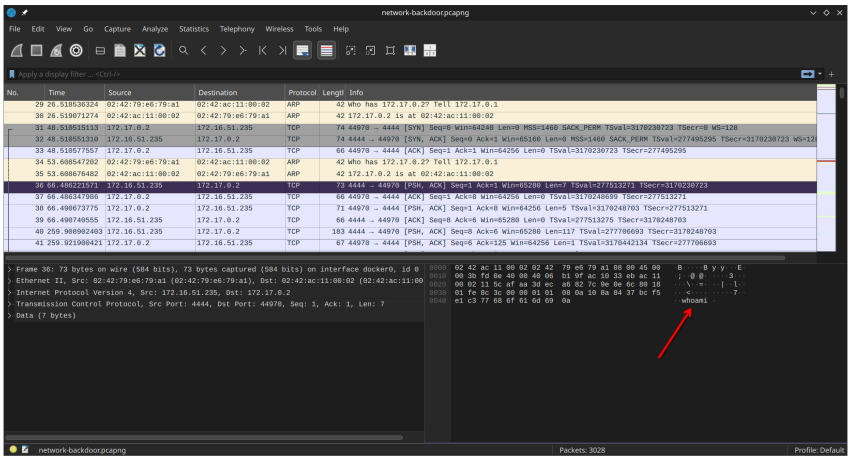

Figure 2: Suspicious command traffic identified in packet capture

2.3 TCP Stream Analysis

To analyze the complete communication:

1. Locate the first packet containing command traffic
2. Right-click and select "Follow TCP Stream"

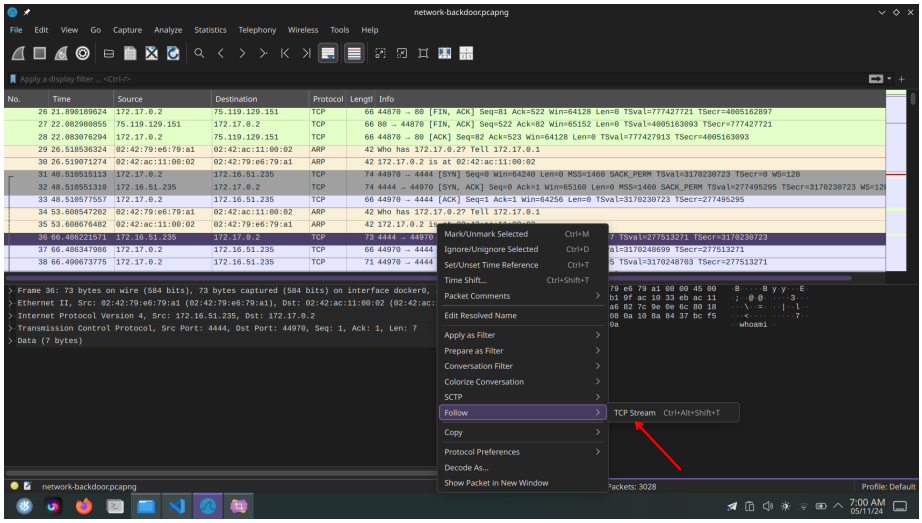

Figure 3: TCP stream analysis showing command and control traffic

2.4 Findings

The analysis reveals:

- Presence of backdoor communication
- Evidence of attempted trojan installation

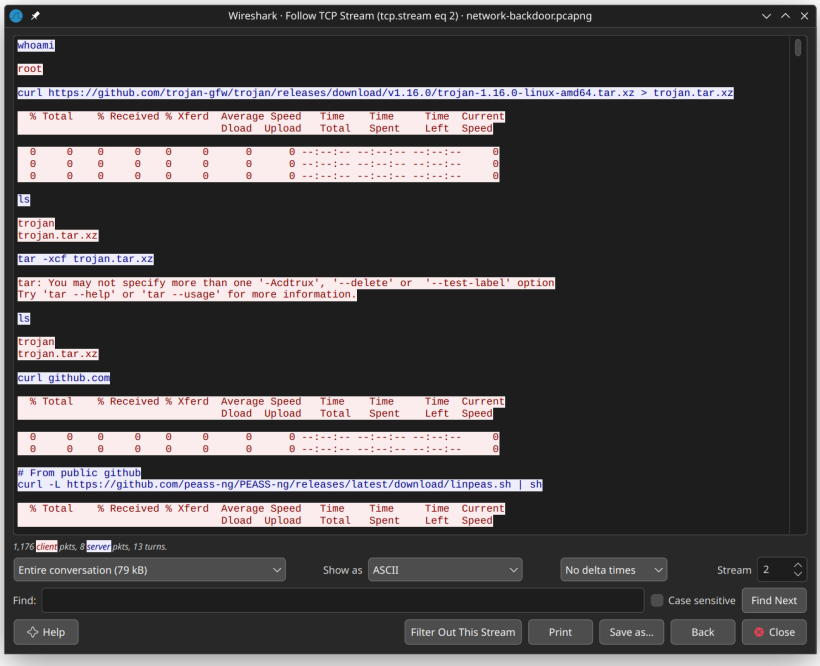

Figure 4: Evidence of trojan installation attempt in network traffic