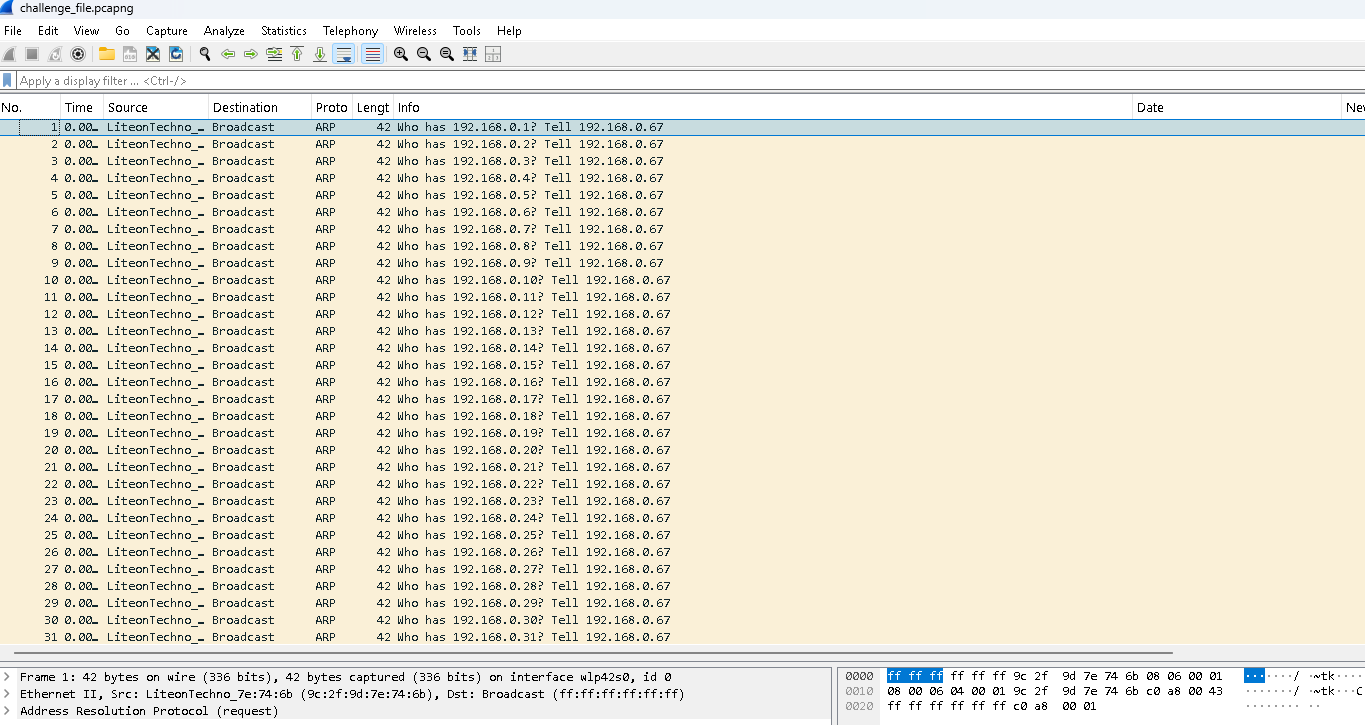
**Introduction**

In this project, you'll learn how to use Wireshark to detect and investigate malware traffic. Identifying malicious network behavior is crucial for protecting networks and responding to security incidents.

**Exercises**

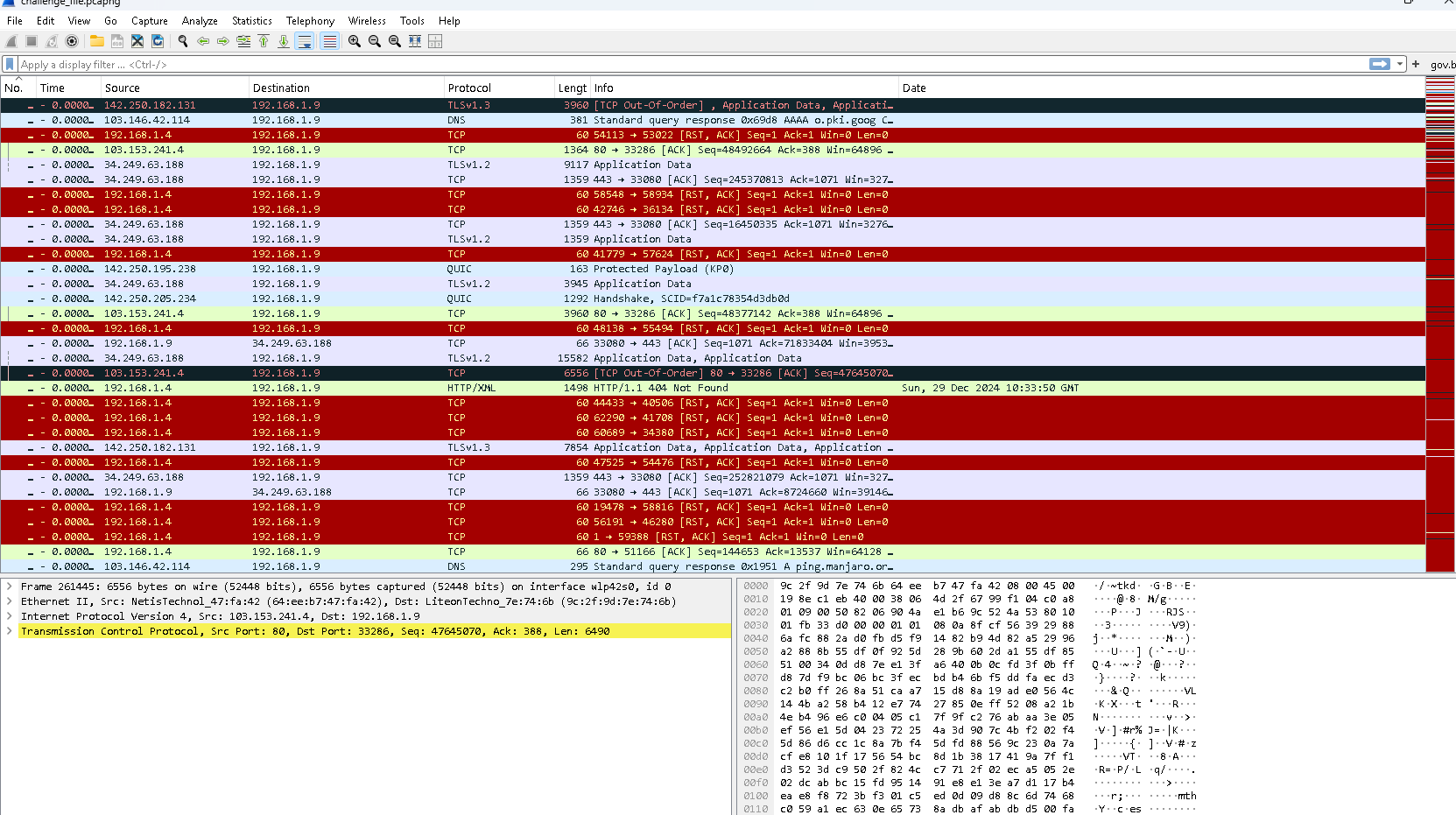
**Exercise 1: Load a Sample PCAP File**

****

**Expected Output**

* The sample PCAP file containing network traffic loaded in Wireshark.

**Exercise 2: Identify Malicious Traffic Patterns**

****

**Expected Output**

* Suspicious traffic patterns identified in the network capture.

**Exercise 3: Analyze Malicious Traffic**

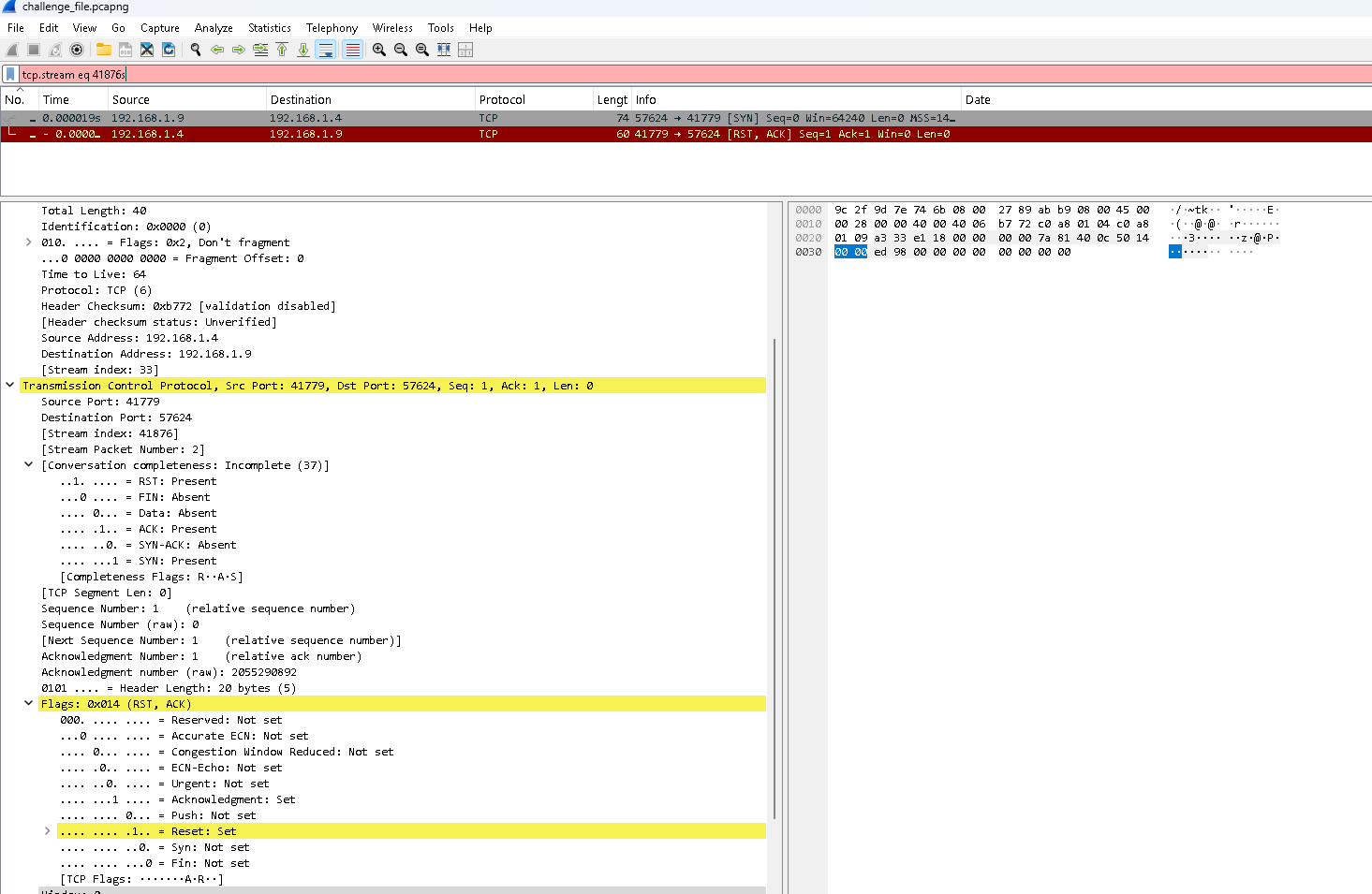
**A screenshot of a computer

Description automatically generated**

**Expected Output**

* Detailed information about a suspicious packet analyzed.

**Exercise 4: Follow the Malware's Communication Stream**

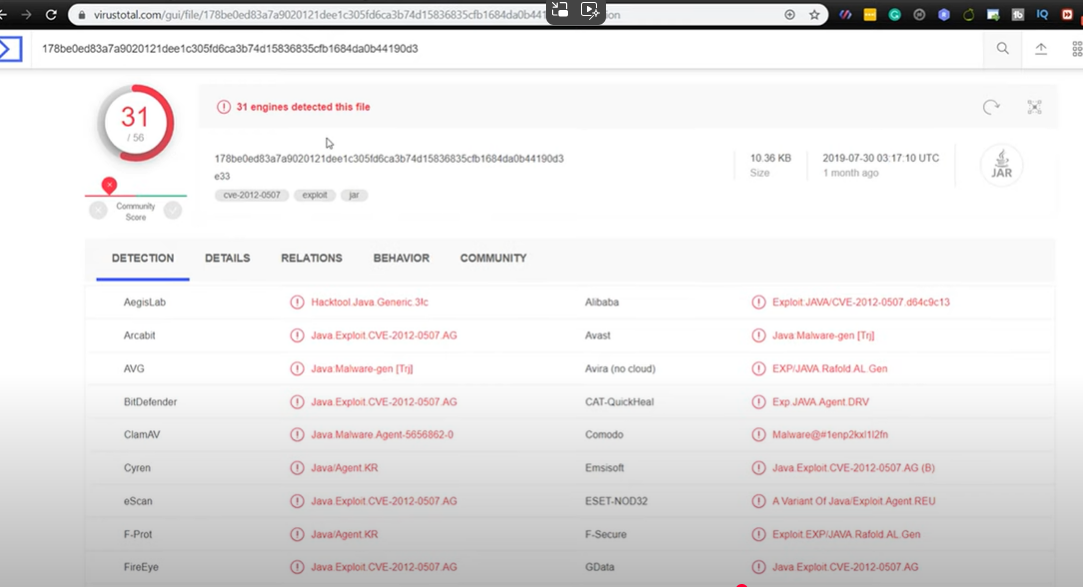
****

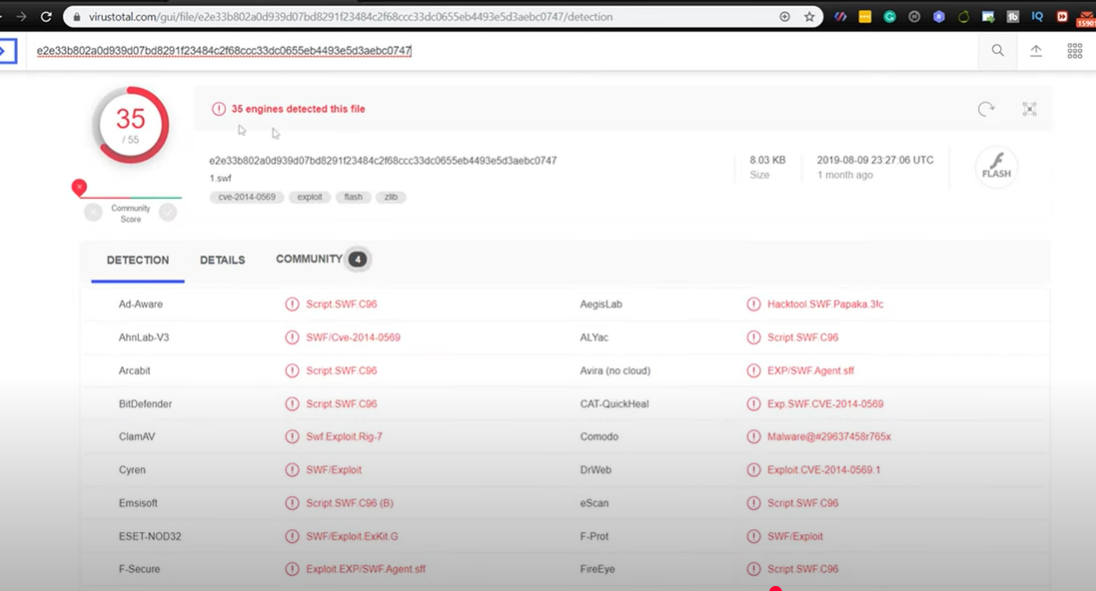
**Expected Output**

* A complete communication stream of the malware analyzed.

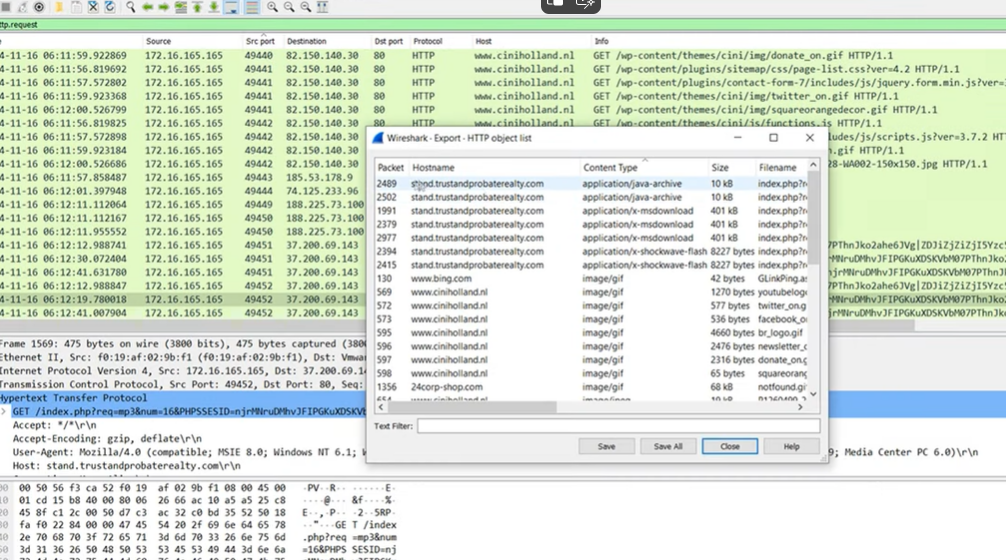
**Problem solving:**

**1.What are the infected files downloaded and their hashes?**

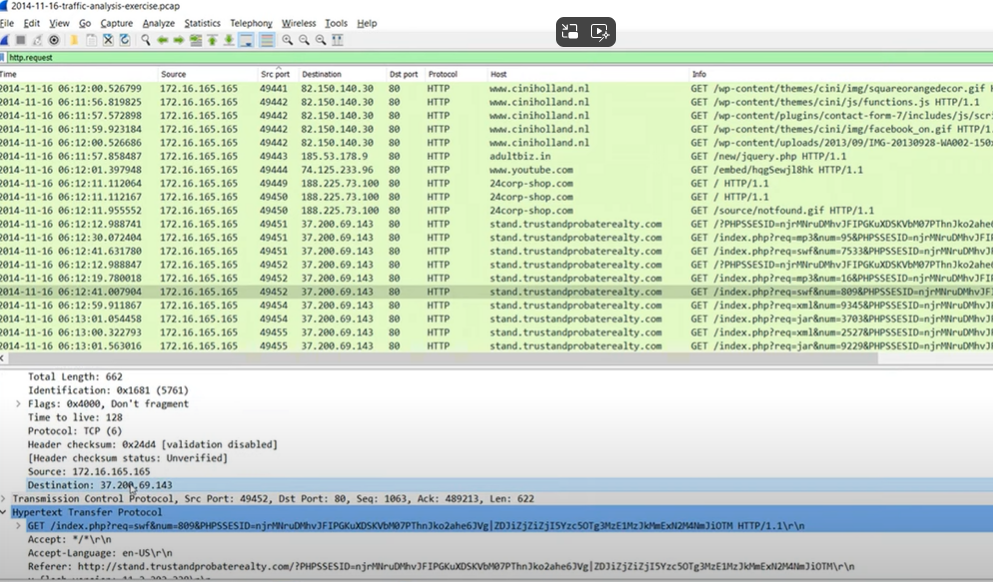
****

****

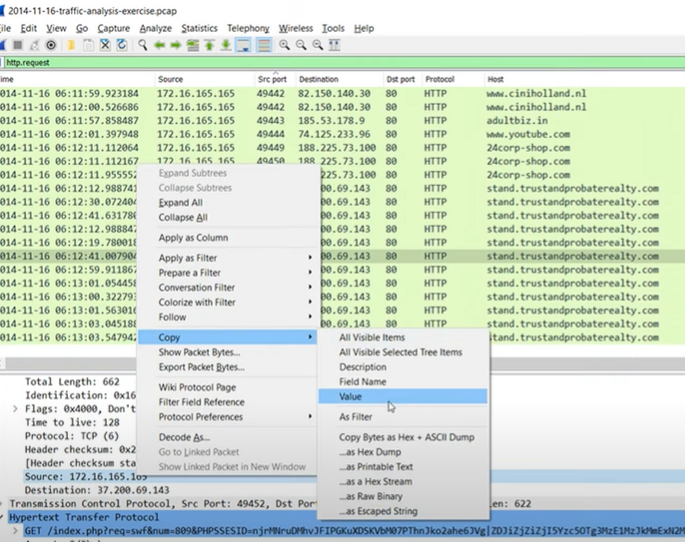
**2.What is URL/Domain of the infected site?**

****

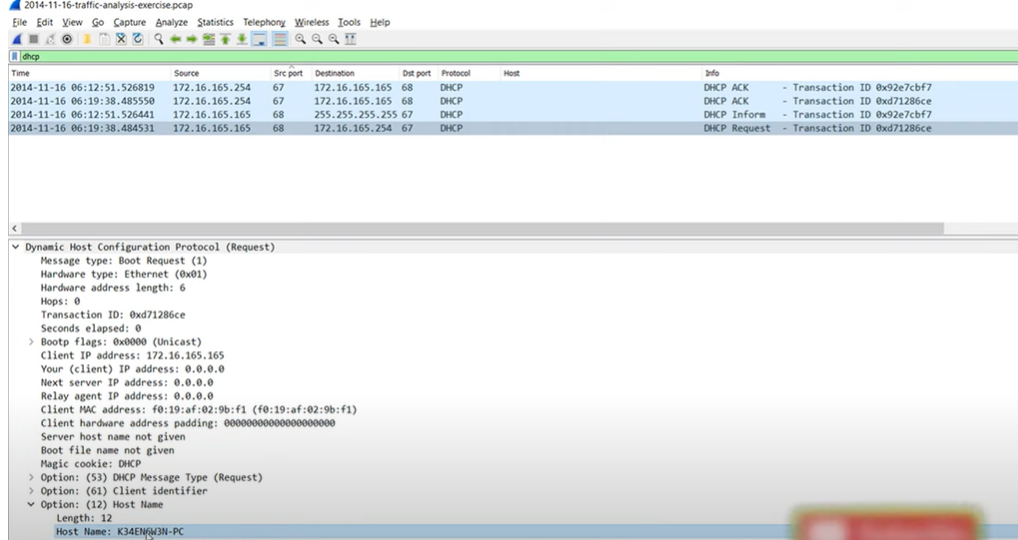
**3.What is the IP address of the infected website?**

****

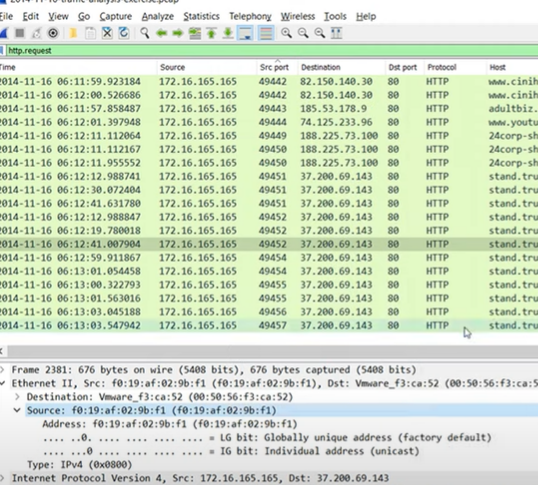
**4.What is the IP address pf the infected machine?**

****

**5.What is the host name of the infected machine?**

**sss**

**6.What is the mac address of infected machine?**

****