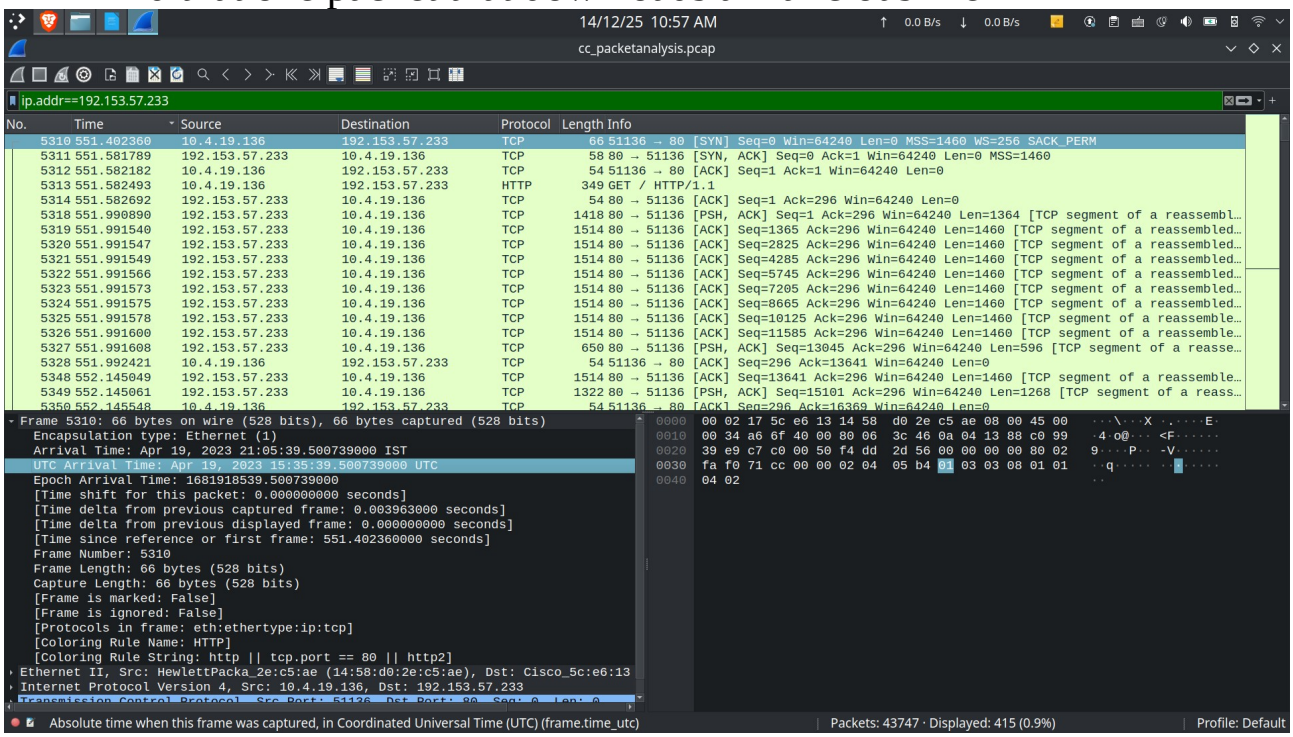
Name: S. Dhanish Ahamed
Reg.No: 25BCE0001

Task 2
Part A: Packet analysis

- A pcap file is given. We have to analyze the network traffic to find malicious packets in the network
- When we filter only the http packets that go out of the network we find that one packet that downloads a malicious file



1. What is the UTC timestamp marking the beginning of the infection?

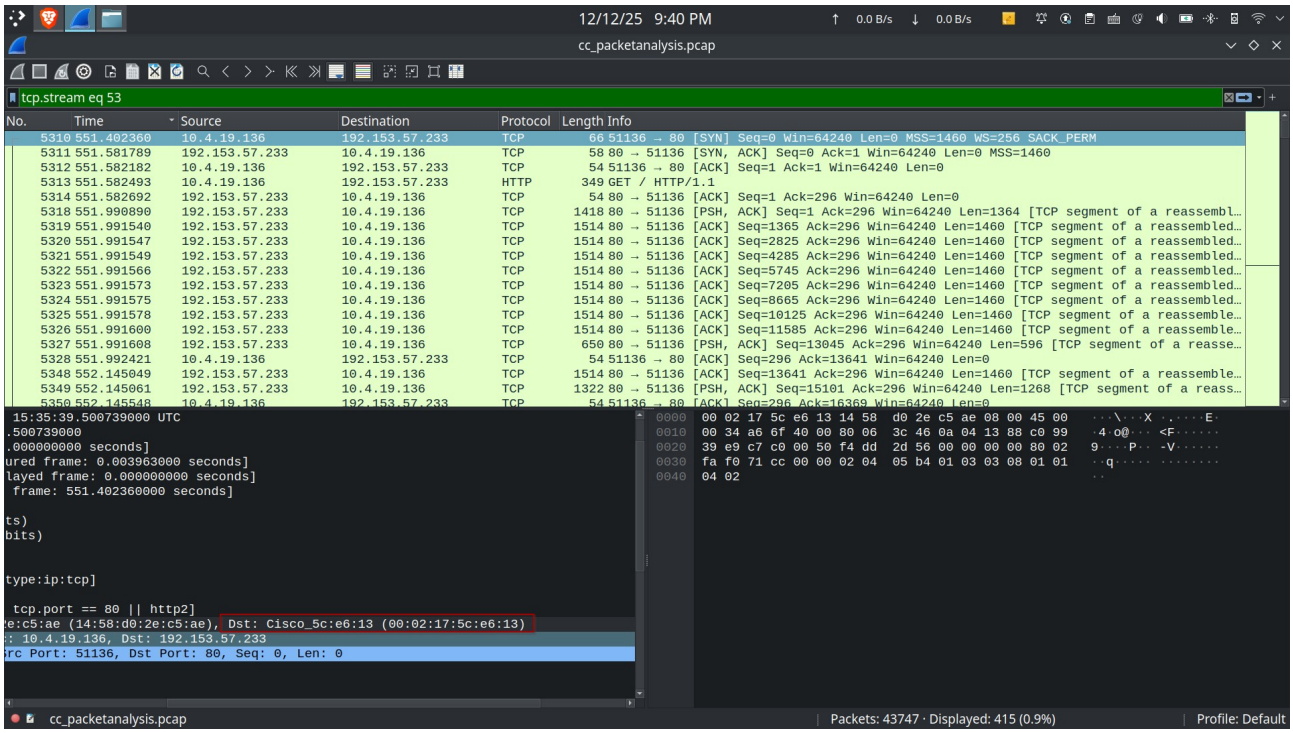
The beginning of the infection is marked at the UTC time stamp 15:35:39.500739000 UTC

2. What internal IP belongs to the compromised Windows machine?

The internal IP of the compromised machine is 10.4.19.136

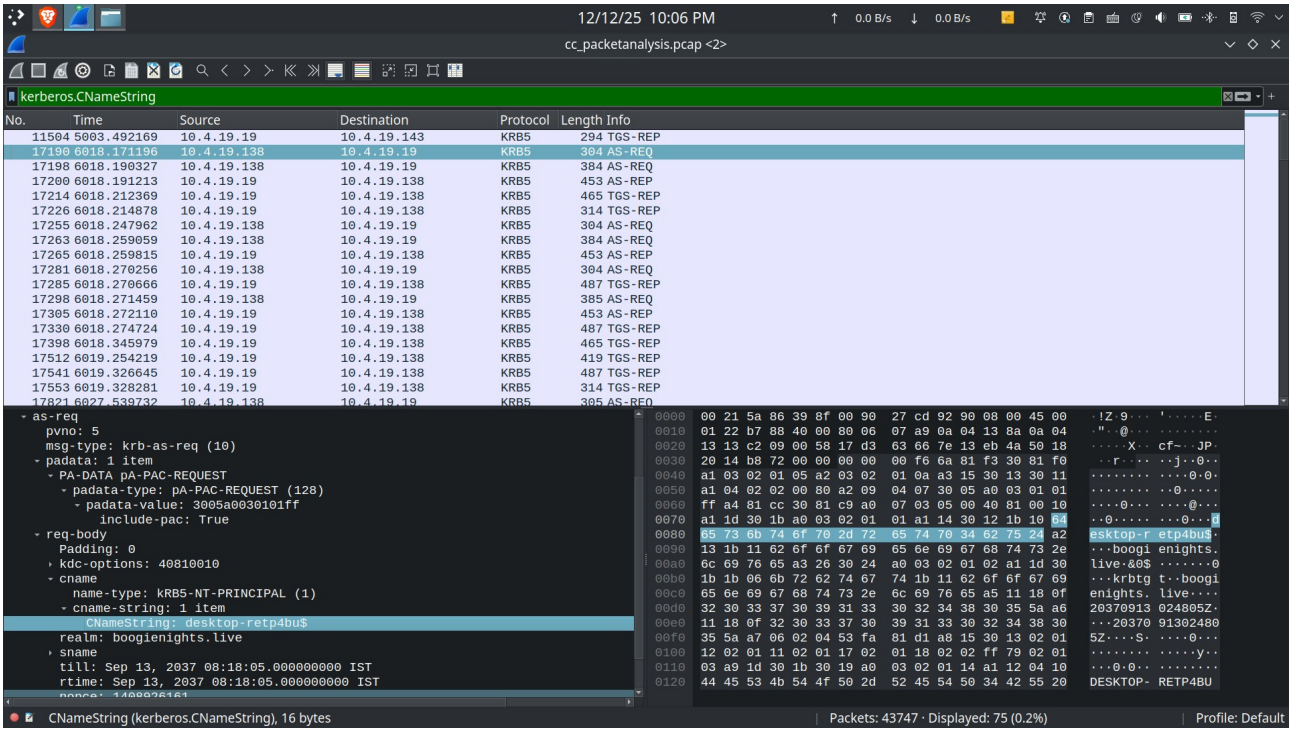
3. What is the machine's MAC address?

The MAC address of the affected machine is 14:58:d0:2e:c5:ae



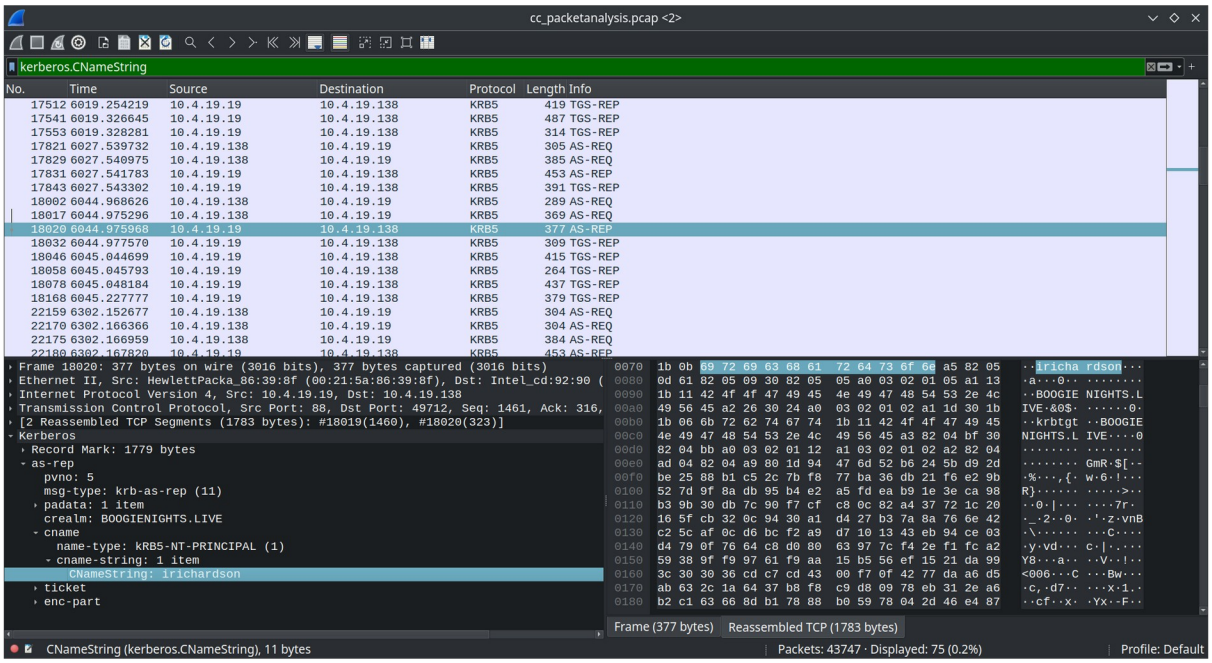
4. What host name is associated with that system?

Kerberos is used for domain authentication. The Client Name is often the hostname followed by a dollar sign. The Client name of the infected system is 'desktop-retp4bu'.



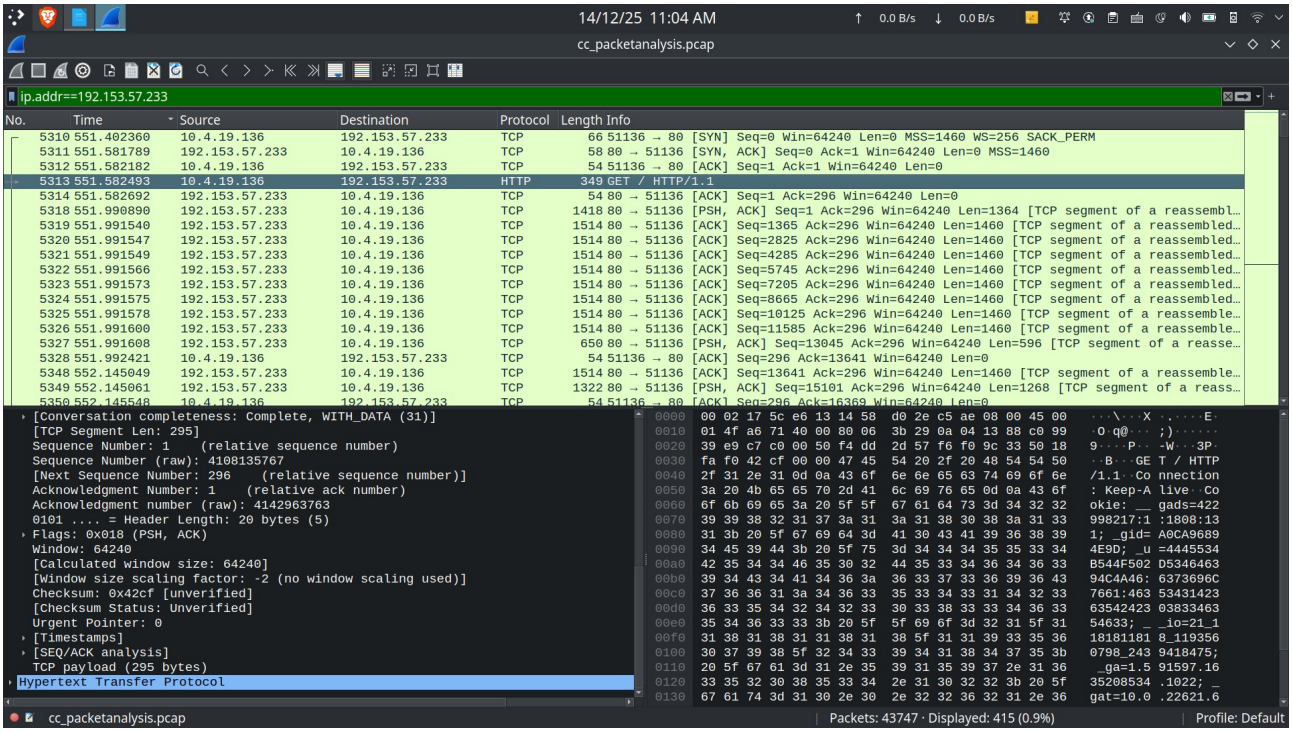
5. Which user account was logged in on the infected host?

‘irichardson’ is the user logged on the infected host. A TGS request contains the current logged in users name



6. Is there evidence of additional malicious activity afterward?

After the three way handshake is done with the external server a malicious file is downloaded



After the initial payload has been downloaded, a malicious zip file is downloaded after some timestamp