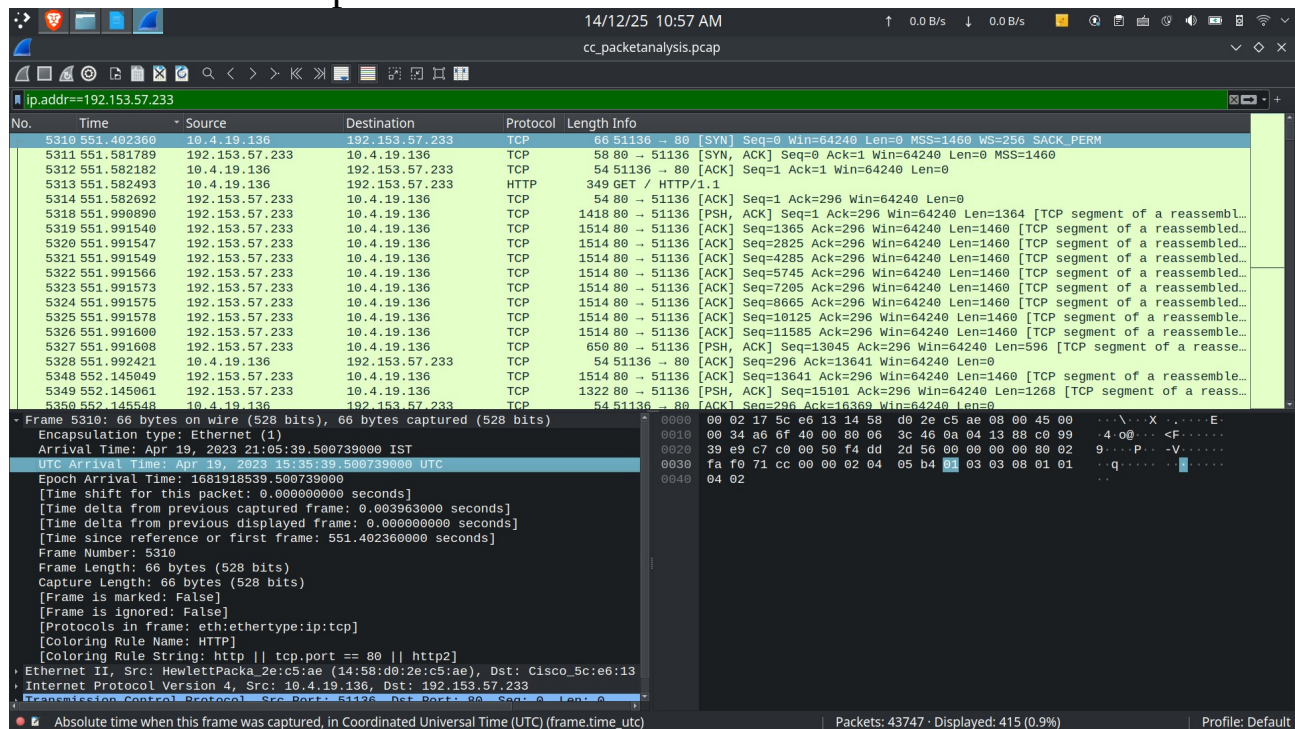


Name: S. Dhanish Ahamed
Reg.No: 25BCE0001

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?

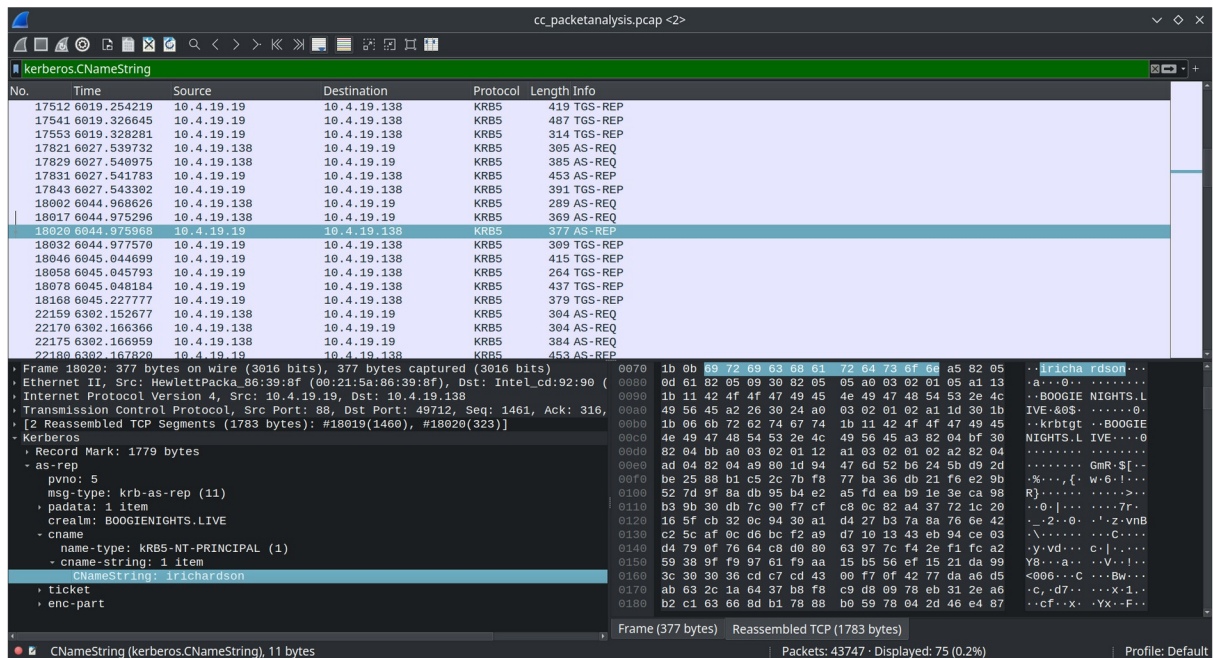
The internal IP of the compromised machine is 10.4.19.136

3. What is the machine's MAC address?

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

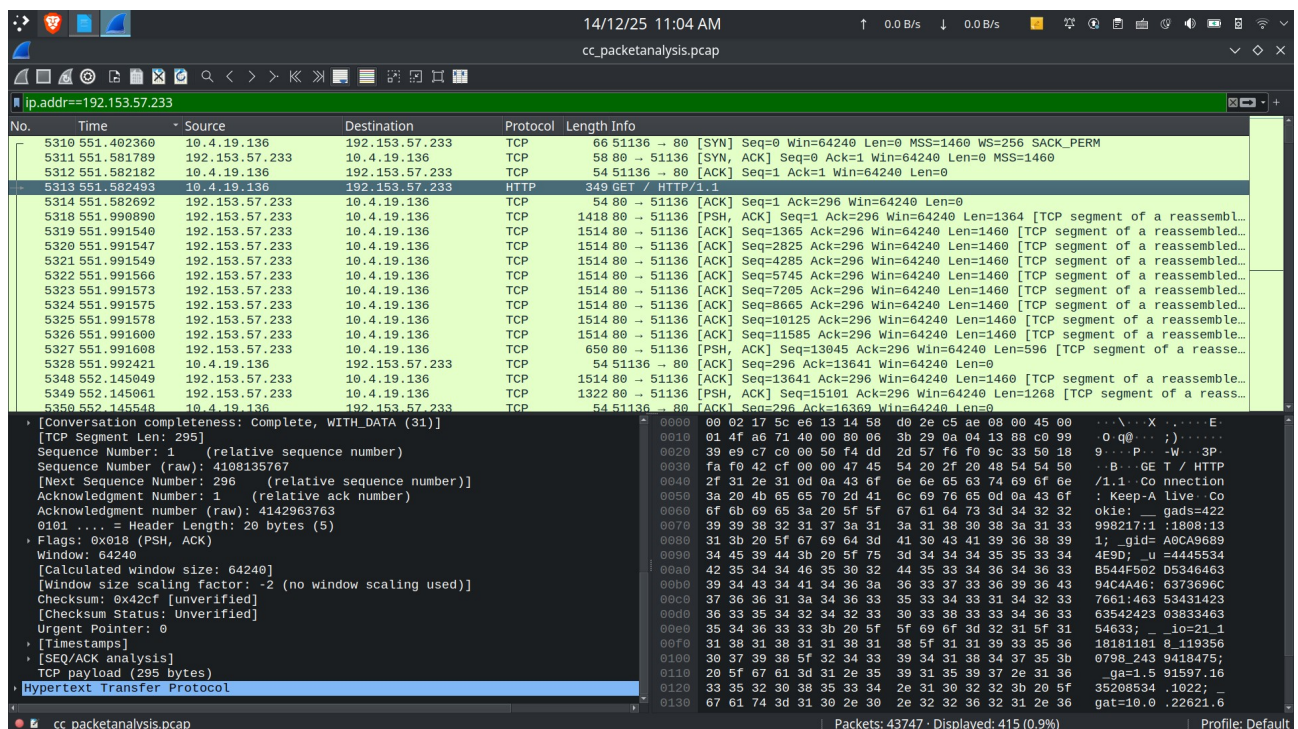
5. Which user account was logged in on the infected host?

'irichardson' is the user logged in 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

14/12/25 11:08 AM
cc_packetanalysis.pcap

ip.addr==192.153.57.233

No.	Time	Source	Destination	Protocol	Length	Info
5729	552.981360	192.153.57.233	10.4.19.136	TCP	1514	80 → 51136 [ACK] Seq=503317 Ack=296 Win=64240 Len=1460 [TCP segment of a reassembled...
5730	552.981366	192.153.57.233	10.4.19.136	TCP	1514	80 → 51136 [ACK] Seq=504777 Ack=296 Win=64240 Len=1460 [TCP segment of a reassembled...
5731	552.981404	192.153.57.233	10.4.19.136	TCP	1514	80 → 51136 [ACK] Seq=506237 Ack=296 Win=64240 Len=1460 [TCP segment of a reassembled...
5732	552.981410	192.153.57.233	10.4.19.136	TCP	1514	80 → 51136 [ACK] Seq=507697 Ack=296 Win=64240 Len=1460 [TCP segment of a reassembled...
5733	552.981412	192.153.57.233	10.4.19.136	TCP	1514	80 → 51136 [ACK] Seq=509157 Ack=296 Win=64240 Len=1460 [TCP segment of a reassembled...
5734	552.981414	192.153.57.233	10.4.19.136	TCP	1514	80 → 51136 [ACK] Seq=510617 Ack=296 Win=64240 Len=1460 [TCP segment of a reassembled...
5735	552.981431	192.153.57.233	10.4.19.136	TCP	1514	80 → 51136 [ACK] Seq=512077 Ack=296 Win=64240 Len=1460 [TCP segment of a reassembled...
5736	552.981438	192.153.57.233	10.4.19.136	TCP	1514	80 → 51136 [ACK] Seq=513537 Ack=296 Win=64240 Len=1460 [TCP segment of a reassembled...
5737	552.981440	192.153.57.233	10.4.19.136	TCP	1514	80 → 51136 [ACK] Seq=514997 Ack=296 Win=64240 Len=1460 [TCP segment of a reassembled...
5738	552.981441	192.153.57.233	10.4.19.136	TCP	1514	80 → 51136 [ACK] Seq=516457 Ack=296 Win=64240 Len=1460 [TCP segment of a reassembled...
5739	552.981442	192.153.57.233	10.4.19.136	TCP	1514	80 → 51136 [ACK] Seq=517917 Ack=296 Win=64240 Len=1460 [TCP segment of a reassembled...
5740	552.981444	192.153.57.233	10.4.19.136	TCP	1514	80 → 51136 [ACK] Seq=519377 Ack=296 Win=64240 Len=1460 [TCP segment of a reassembled...
5741	552.981459	192.153.57.233	10.4.19.136	HTTP	172	HTTP/1.1 200 OK (application/gzip)
5742	552.983720	10.4.19.136	192.153.57.233	TCP	54	51136 → 80 [ACK] Seq=296 Ack=520955 Win=64240 Len=0
5752	612.999374	10.4.19.136	192.153.57.233	TCP	54	51136 → 80 [FIN, ACK] Seq=296 Ack=520955 Win=64240 Len=0
5753	612.999613	192.153.57.233	10.4.19.136	TCP	54	80 → 51136 [ACK] Seq=520955 Ack=297 Win=64239 Len=0
5758	613.143767	192.153.57.233	10.4.19.136	TCP	54	80 → 51136 [FIN, PSH, ACK] Seq=520955 Ack=297 Win=64239 Len=0
5759	613.143977	10.4.19.136	192.153.57.233	TCP	54	51136 → 80 [ACK] Seq=297 Ack=520956 Win=64240 Len=0

Ethernet II, Src: Cisco_5c:e6:13 (00:02:17:5c:e6:13), Dst: HewlettPacka_2e:c5:ae...
Internet Protocol Version 4, Src: 192.153.57.233, Dst: 10.4.19.136
Transmission Control Protocol, Src Port: 80, Dst Port: 51136, Seq: 520837, Ack: 2...
[371 Reassembled TCP Segments (520954 bytes): #5318(1364), #5319(1460), #5320(146...
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Server: nginx\r\n
Date: Wed, 19 Apr 2023 15:35:40 GMT\r\n
Content-Type: application/gzip\r\n
Content-Length: 520803\r\n
Connection: keep-alive\r\n
[HTTP response 1/1]
[Time since request: 1.398966000 seconds]
[Request in frame: 5313]
[Request URI: http://skigmeetroc.com/]
File Data: 520803 bytes
Media Type
Media type: application/gzip (520803 bytes)

Frame (172 bytes) Reassembled TCP (520954 bytes)

Media Type (media), 5,20,803 bytes

Packets: 43747 · Displayed: 415 (0.9%)

Profile: Default