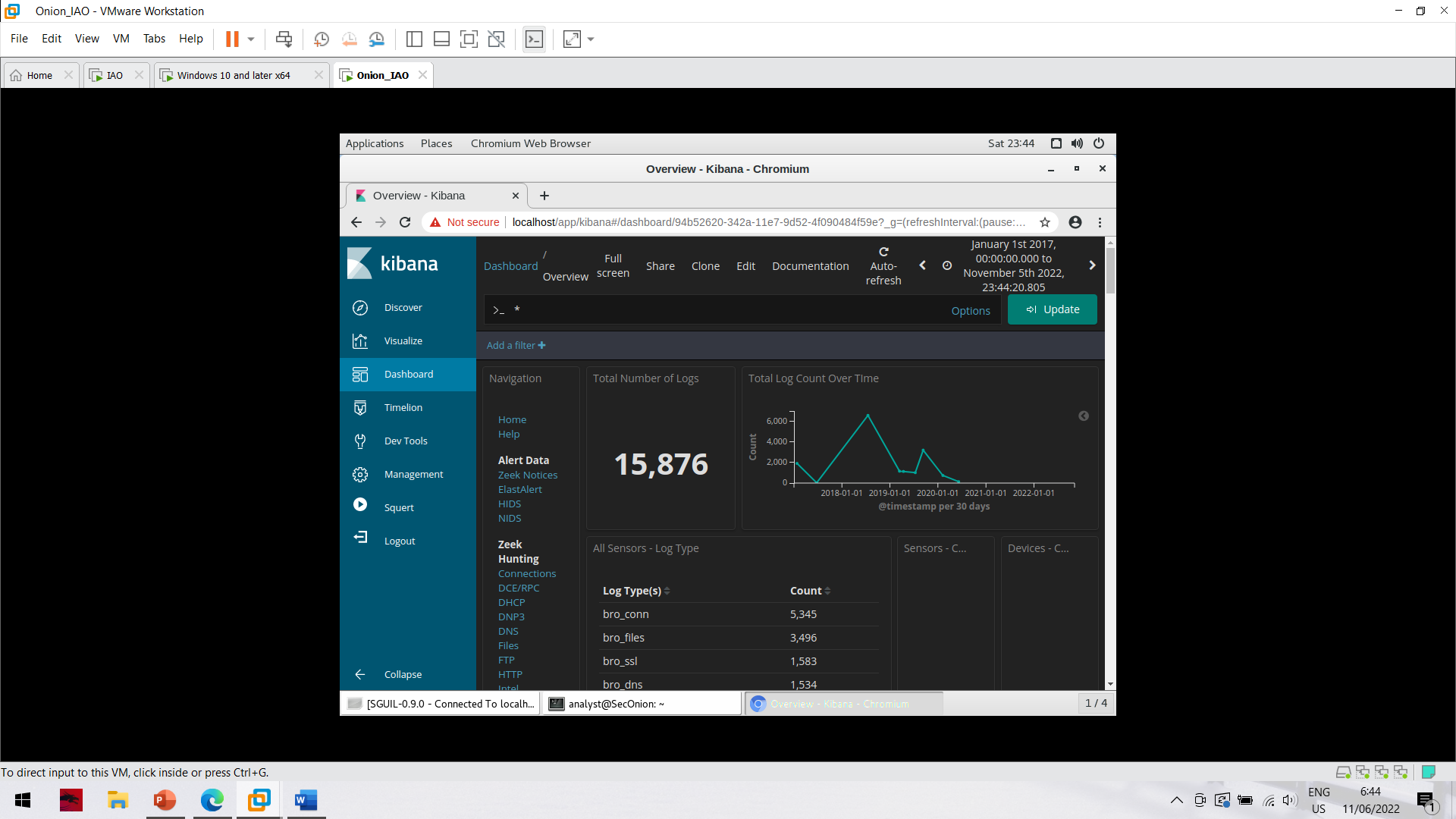
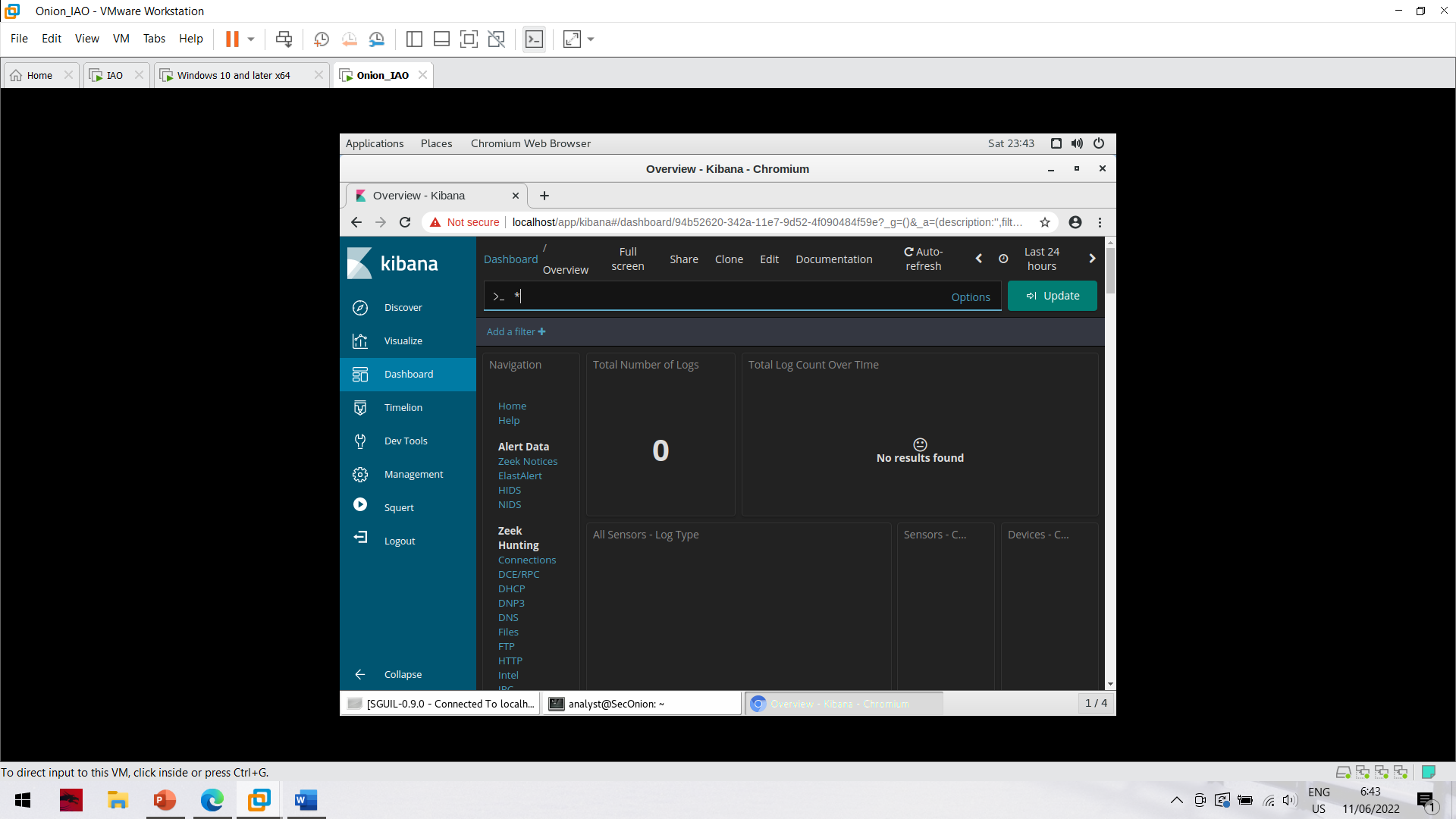
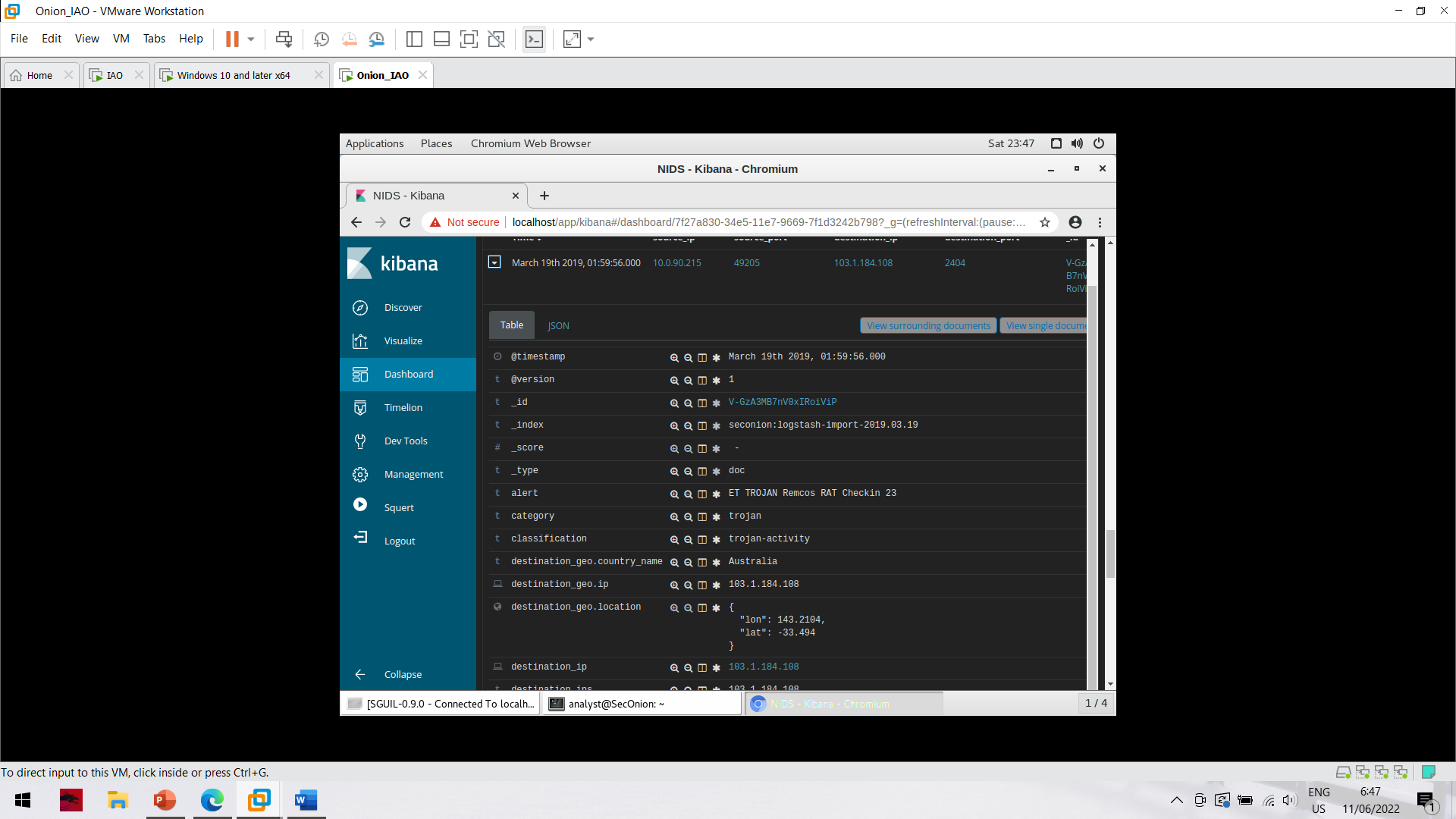
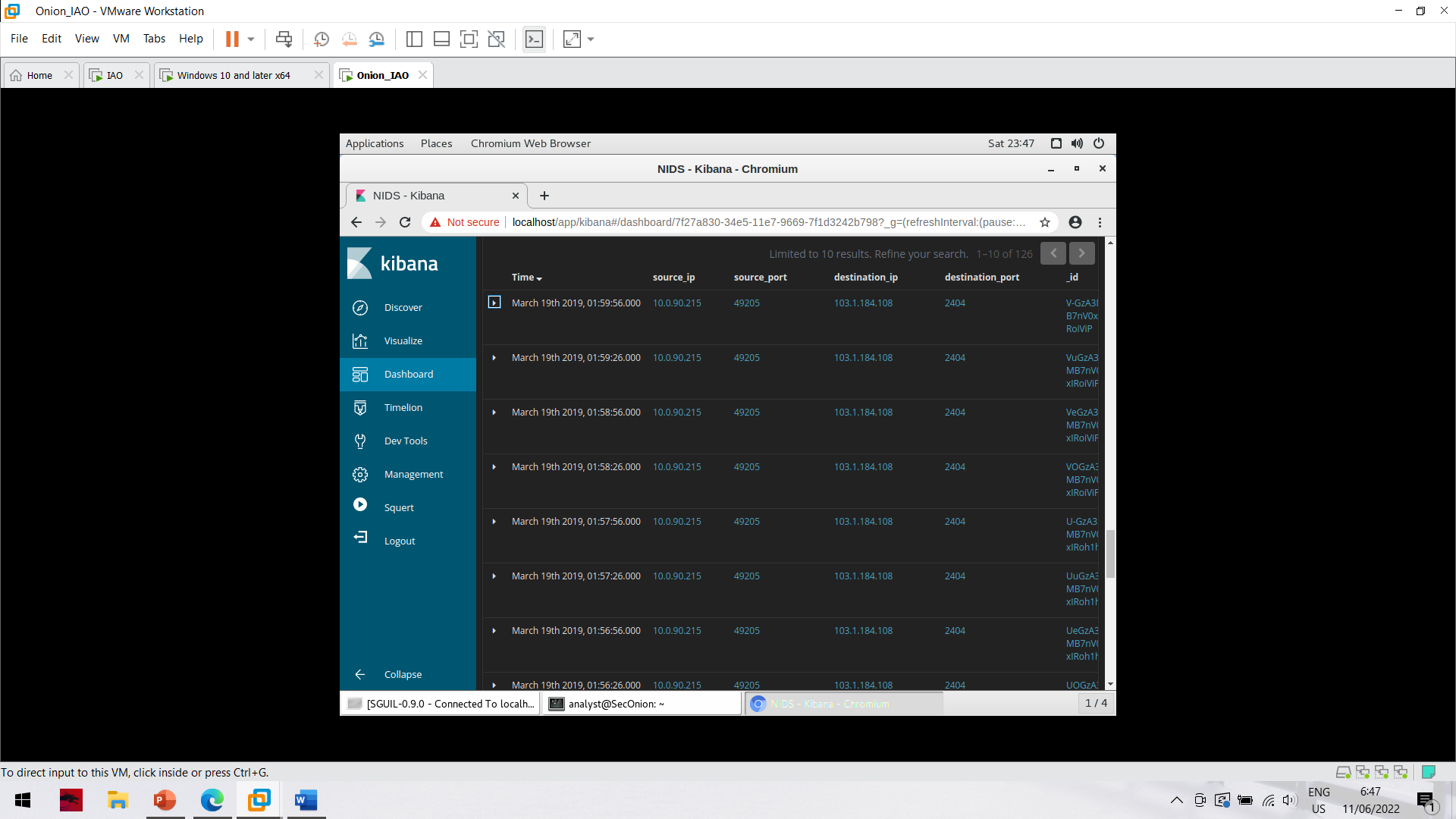
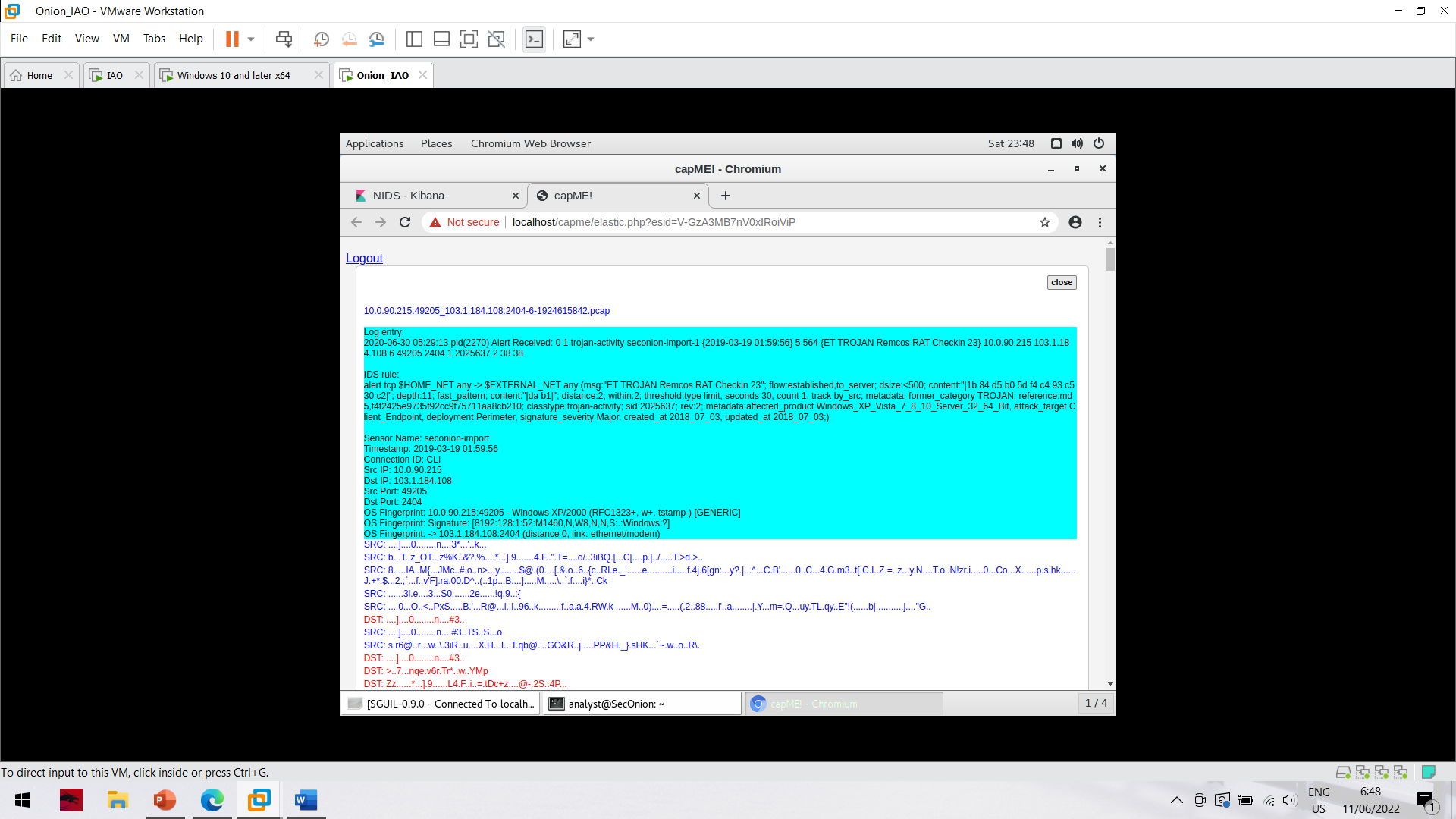
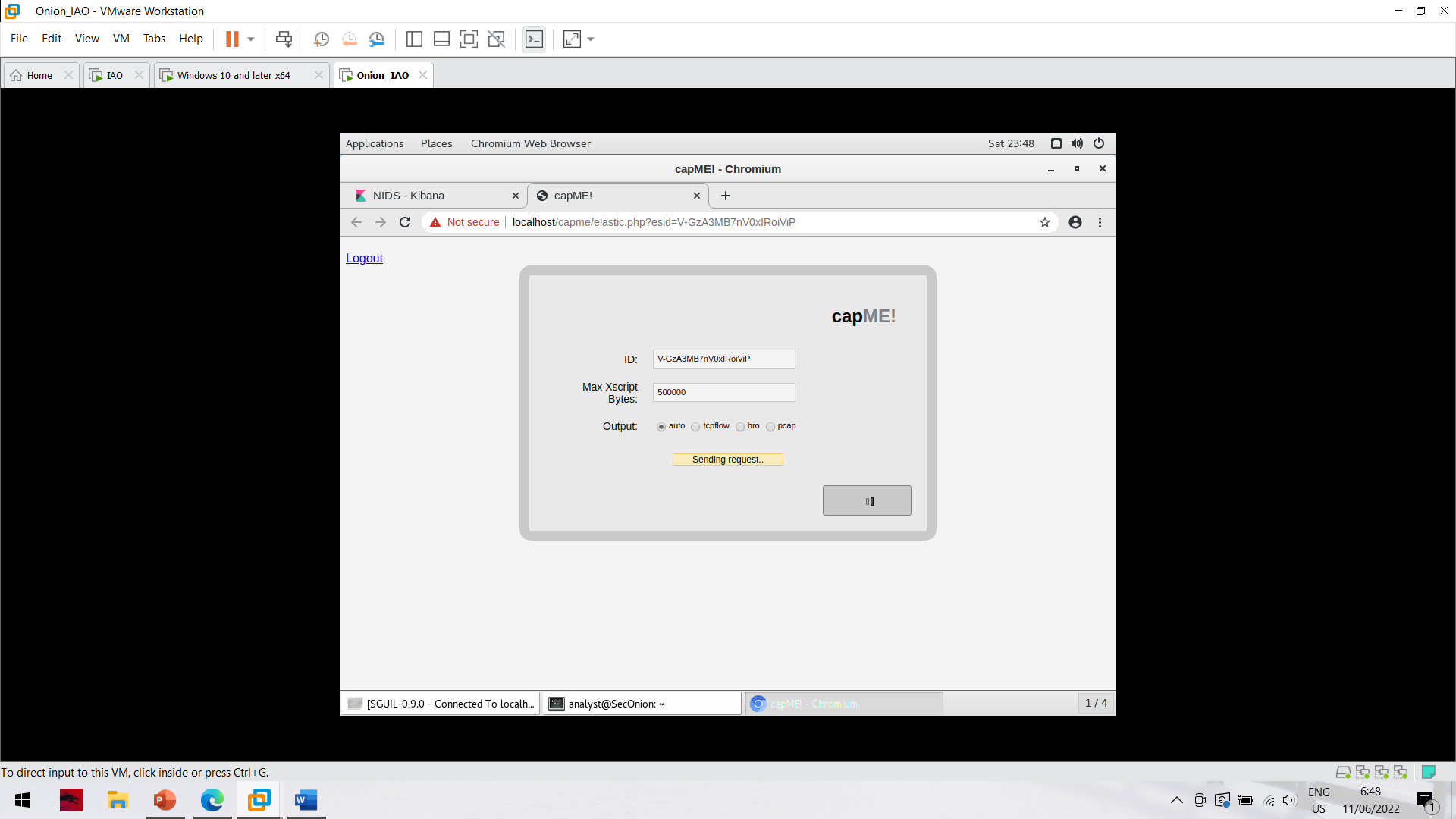
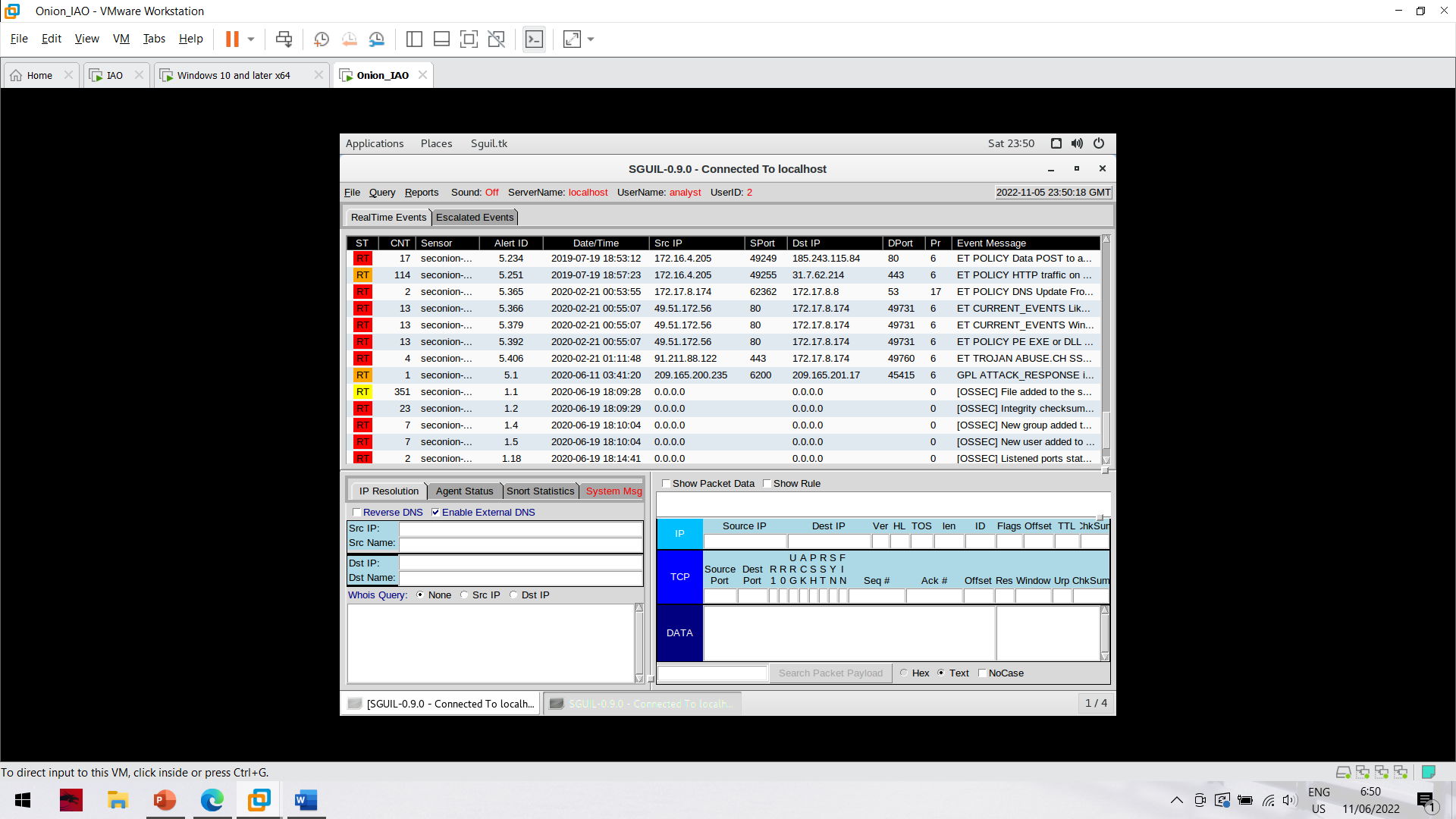
Lab - Investigating a Malware Exploit

Part 1: Use Kibana to Learn About a Malware Exploit

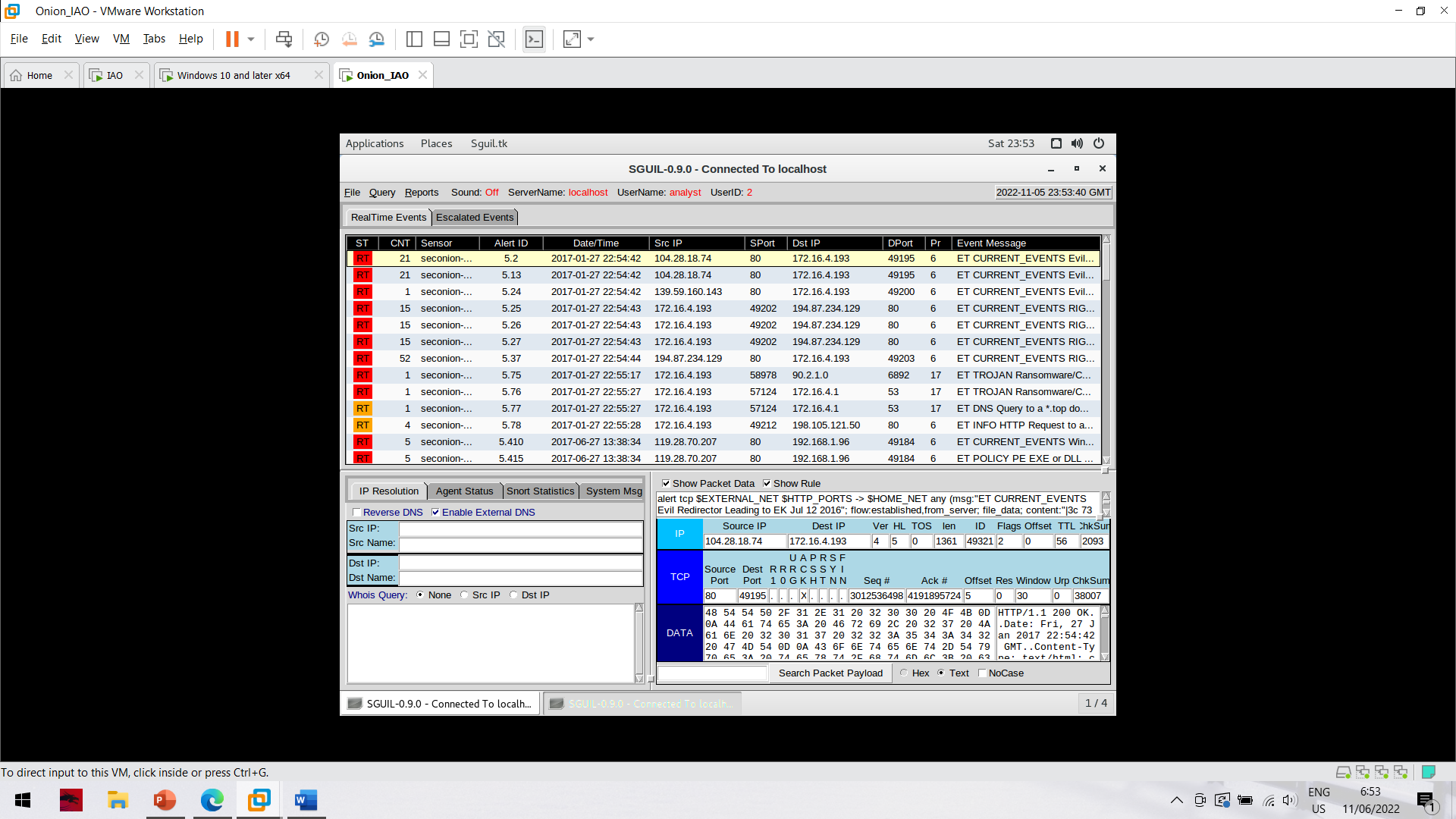
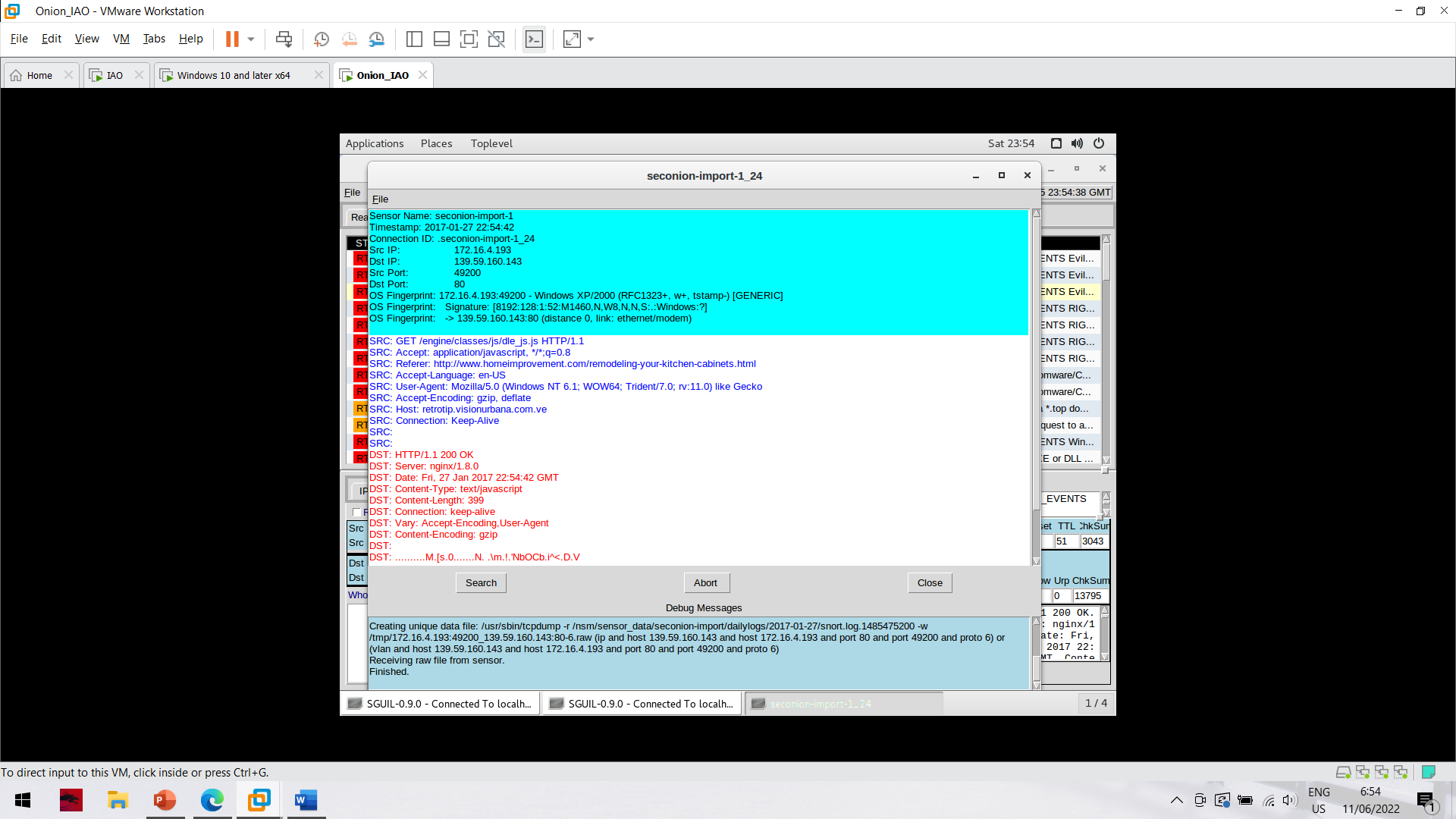
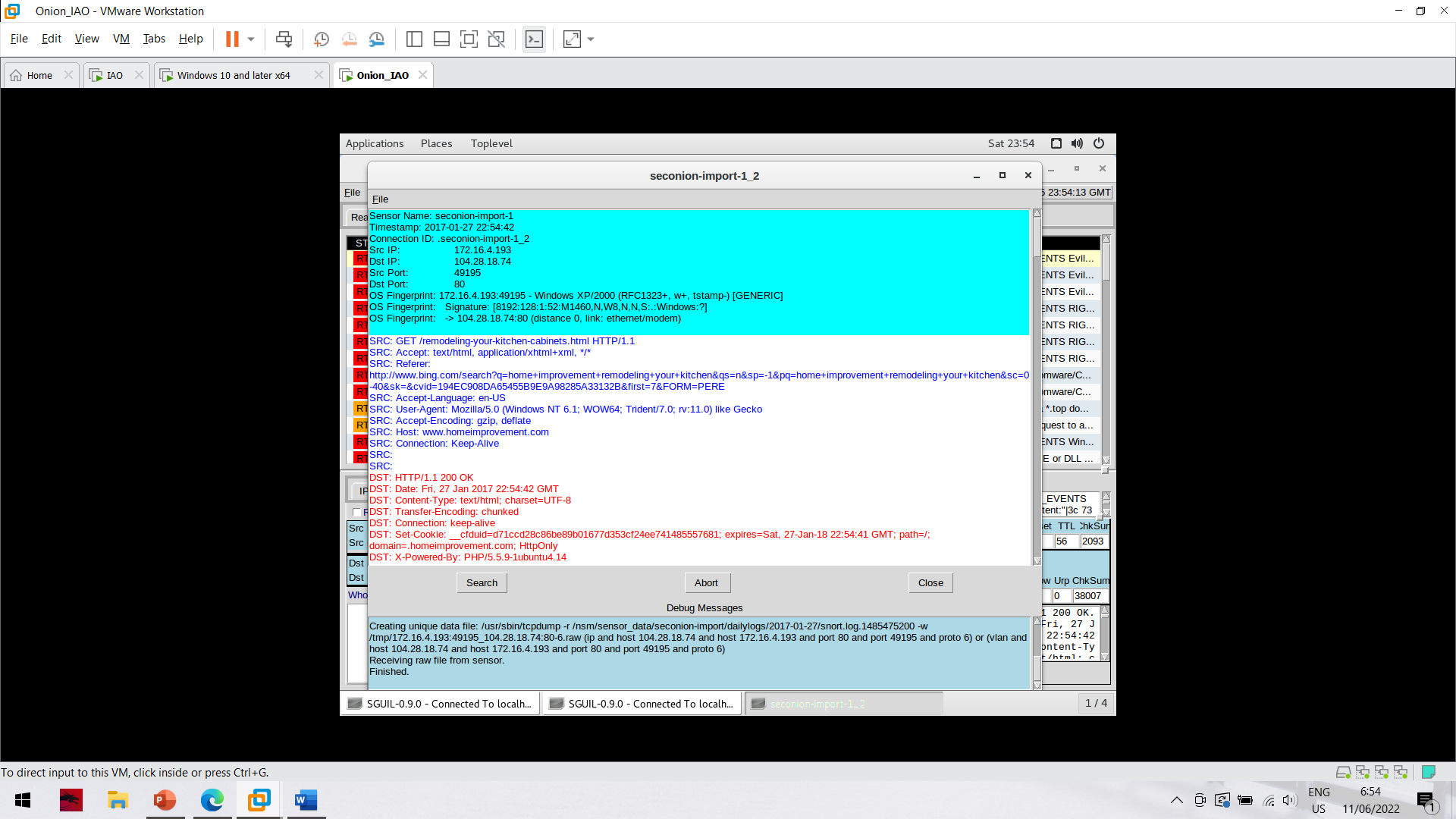
Step 2: Locate the Event in Kibana

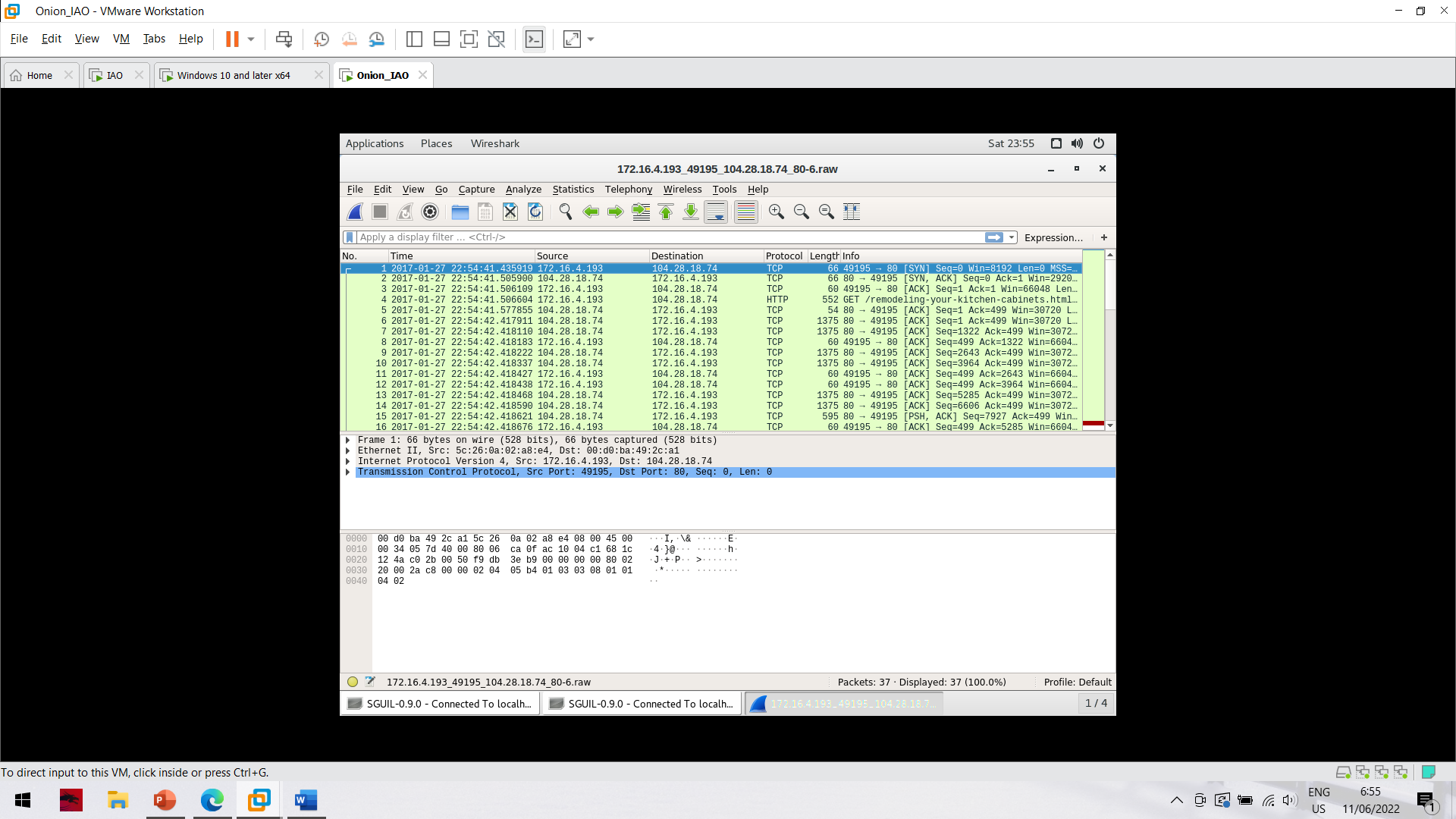
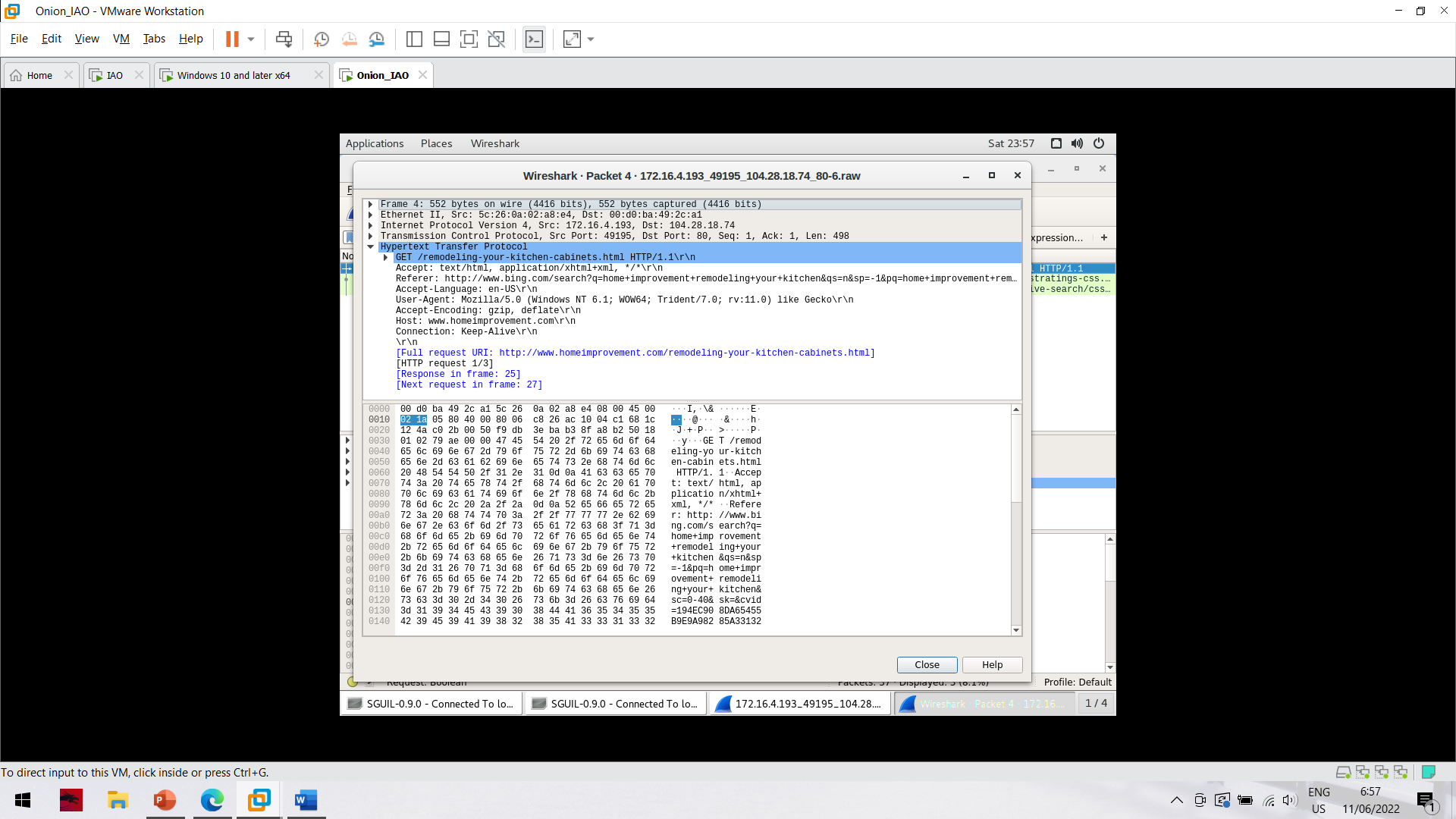
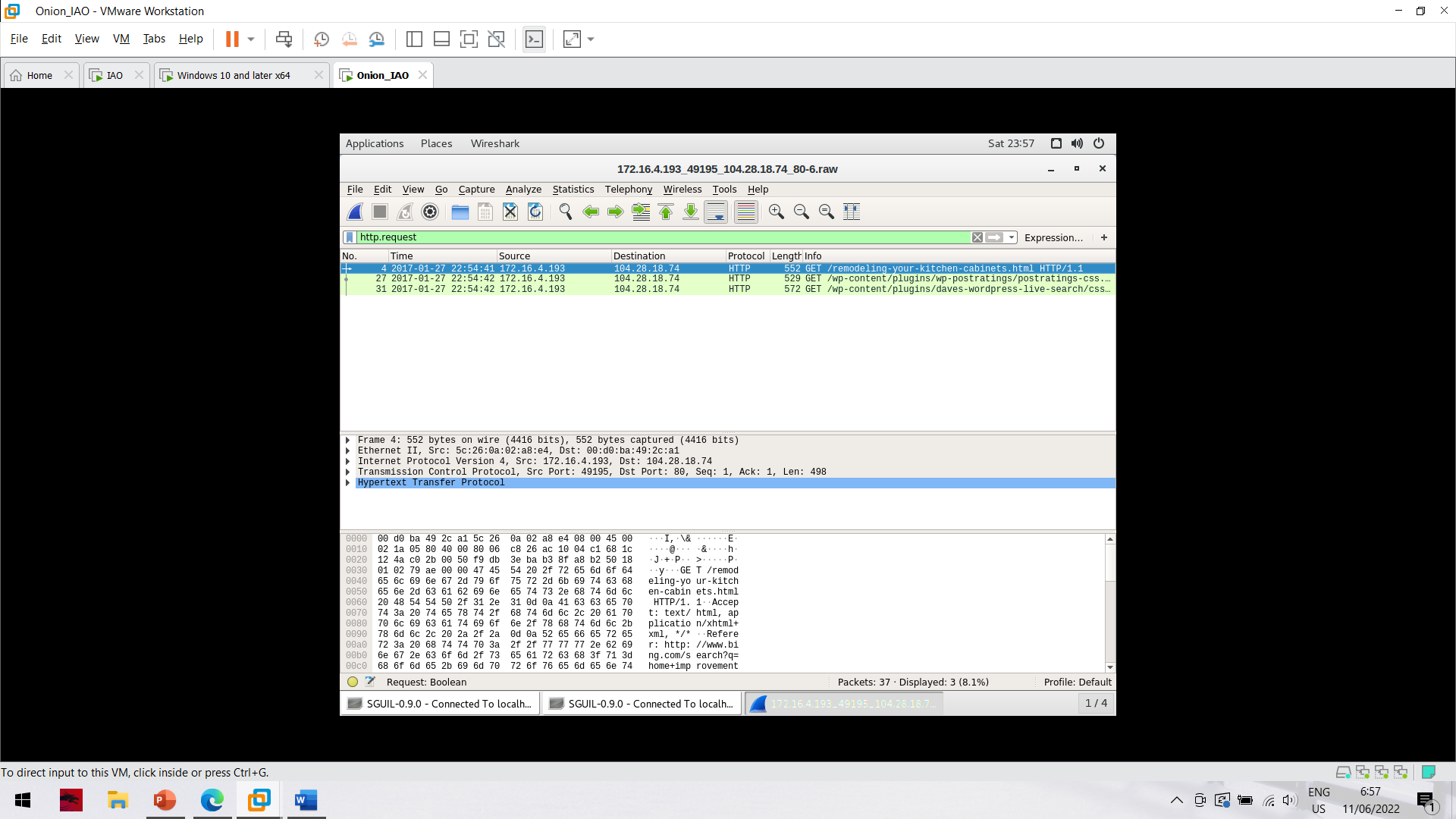
Step 3: View the Transcript capME! Part 2: Investigate the Exploit with Sguil

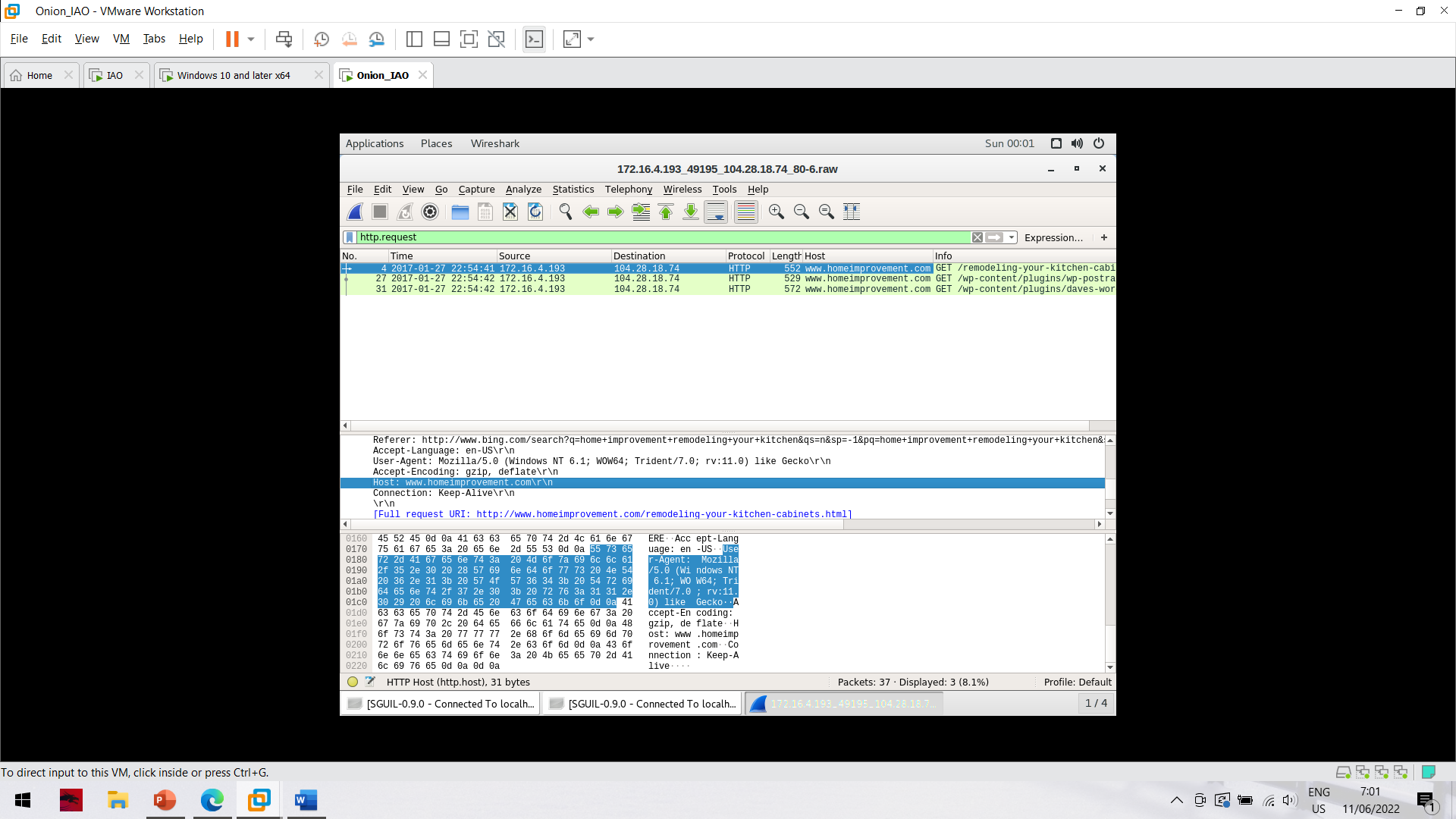
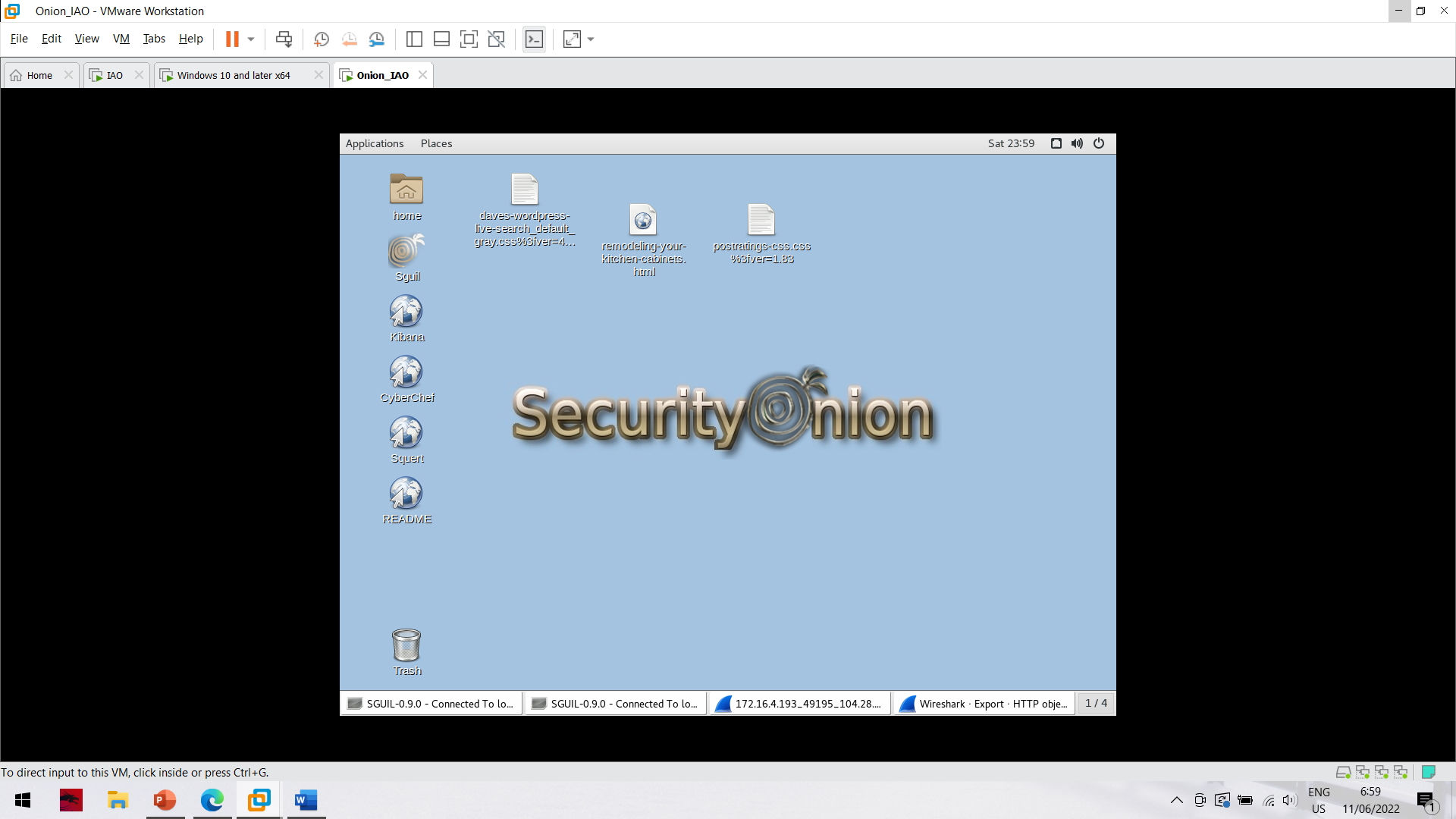
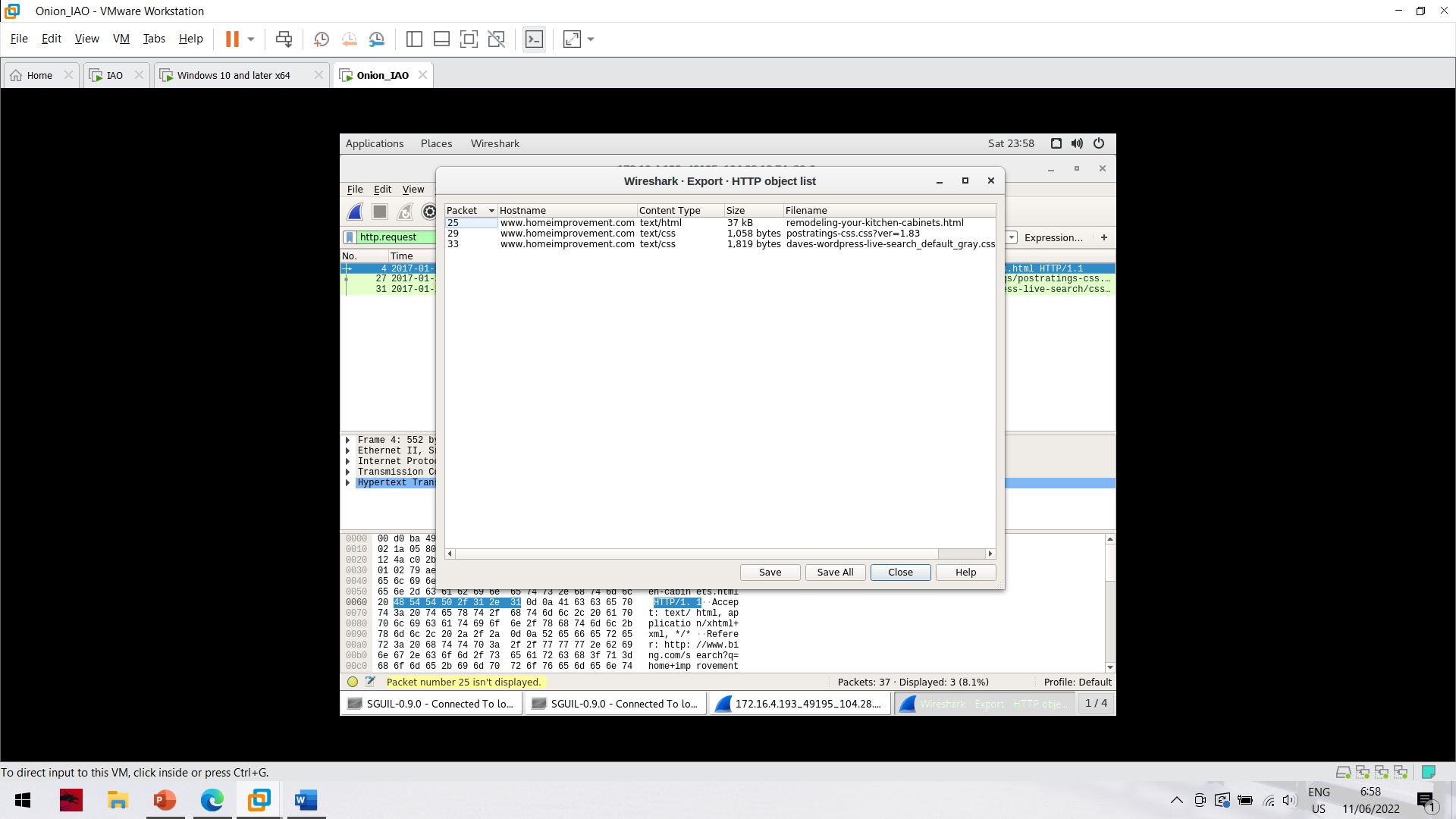
Step 1: Open Sguil and locate the alerts.



Step 2: Investigate the alerts in Sguil.

Step 3: View Transcripts of EventsPart 3: Use Wireshark to Investigate an Attack

Step 1: Pivot to Wireshark and Change Settings. Step 2: Investigate HTTP Traffic. Step 3: View HTTP Objects

Step 4: Create a Hash for an Exported Malware File.

