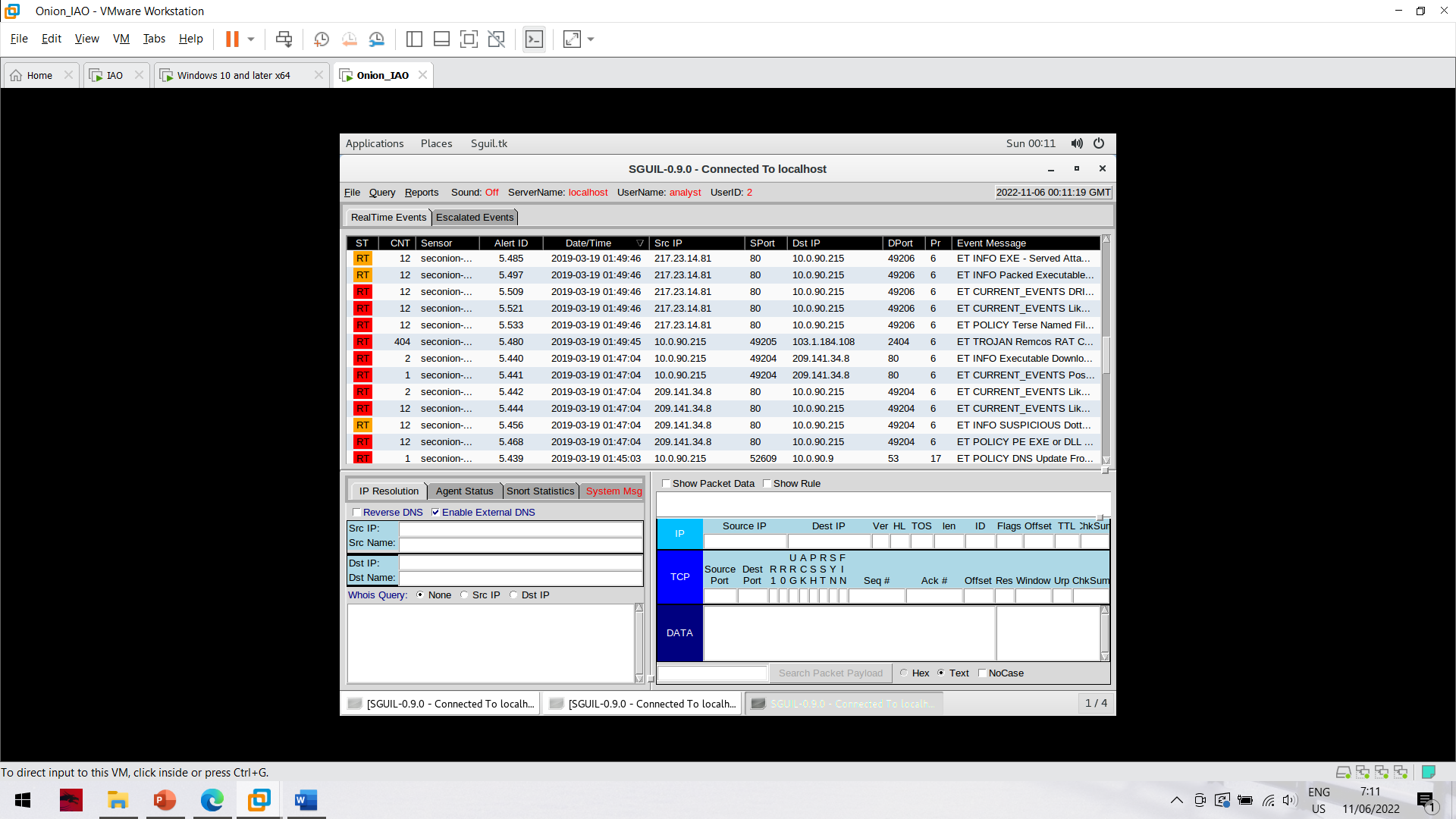
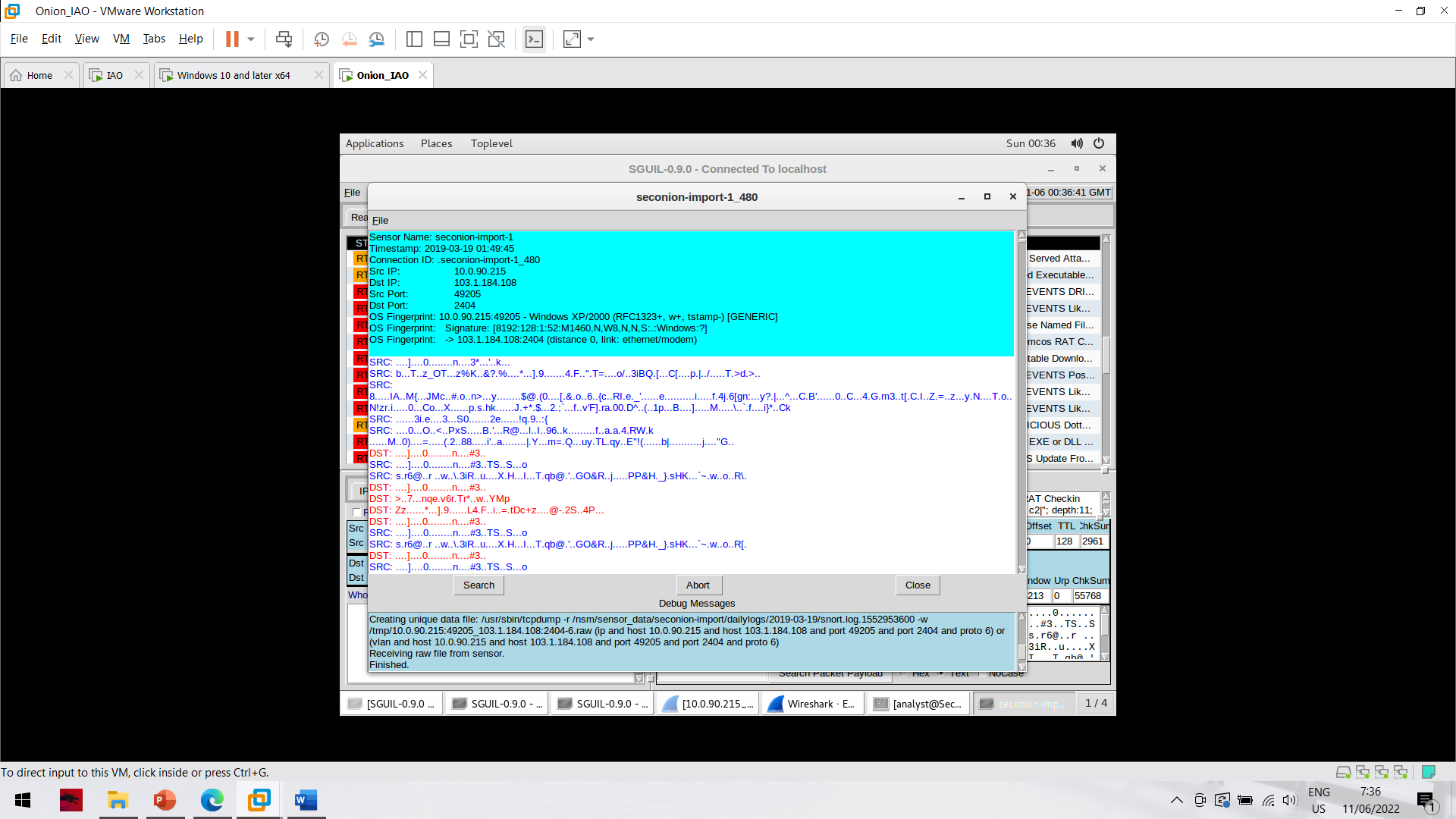
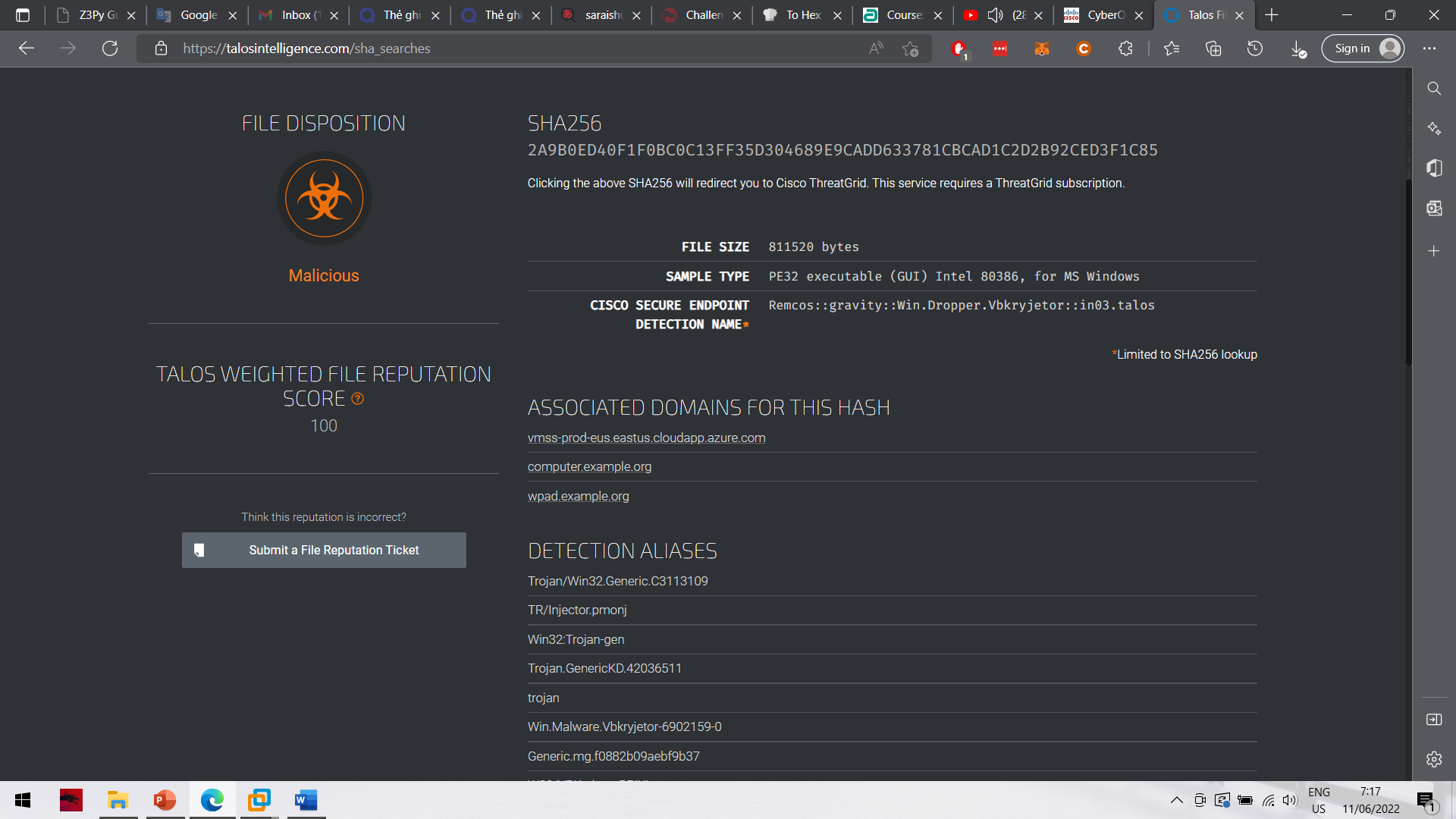
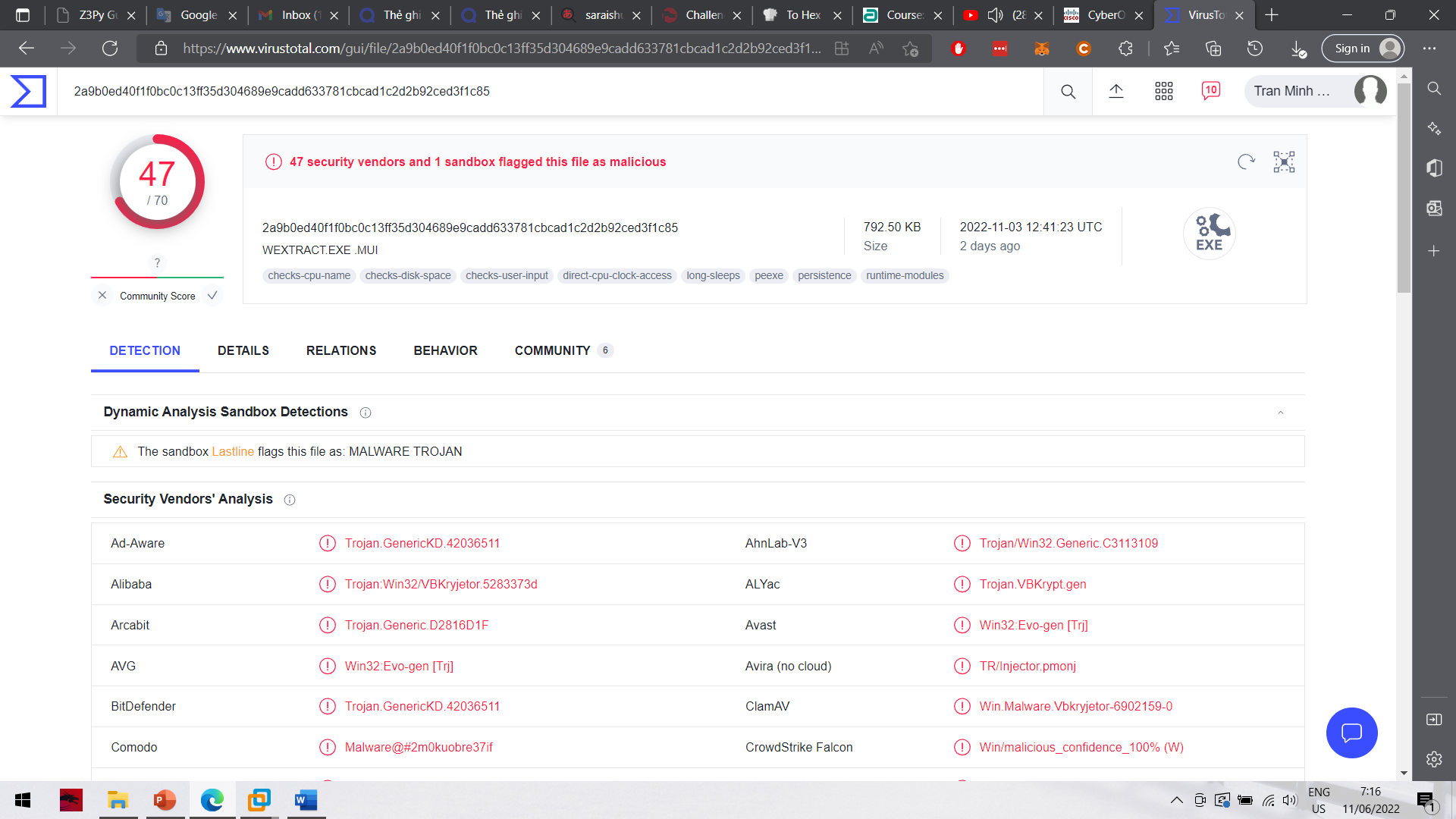
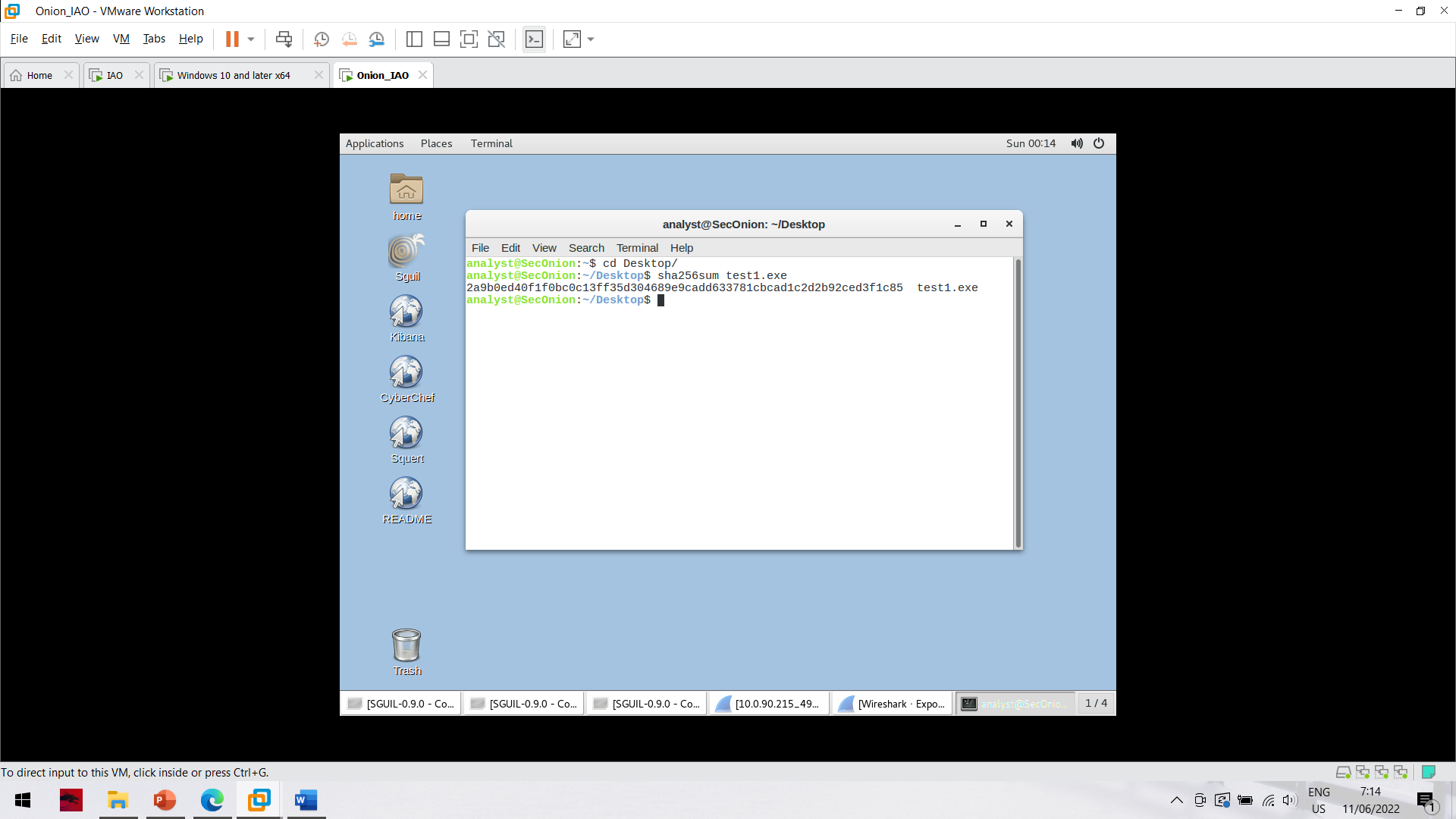
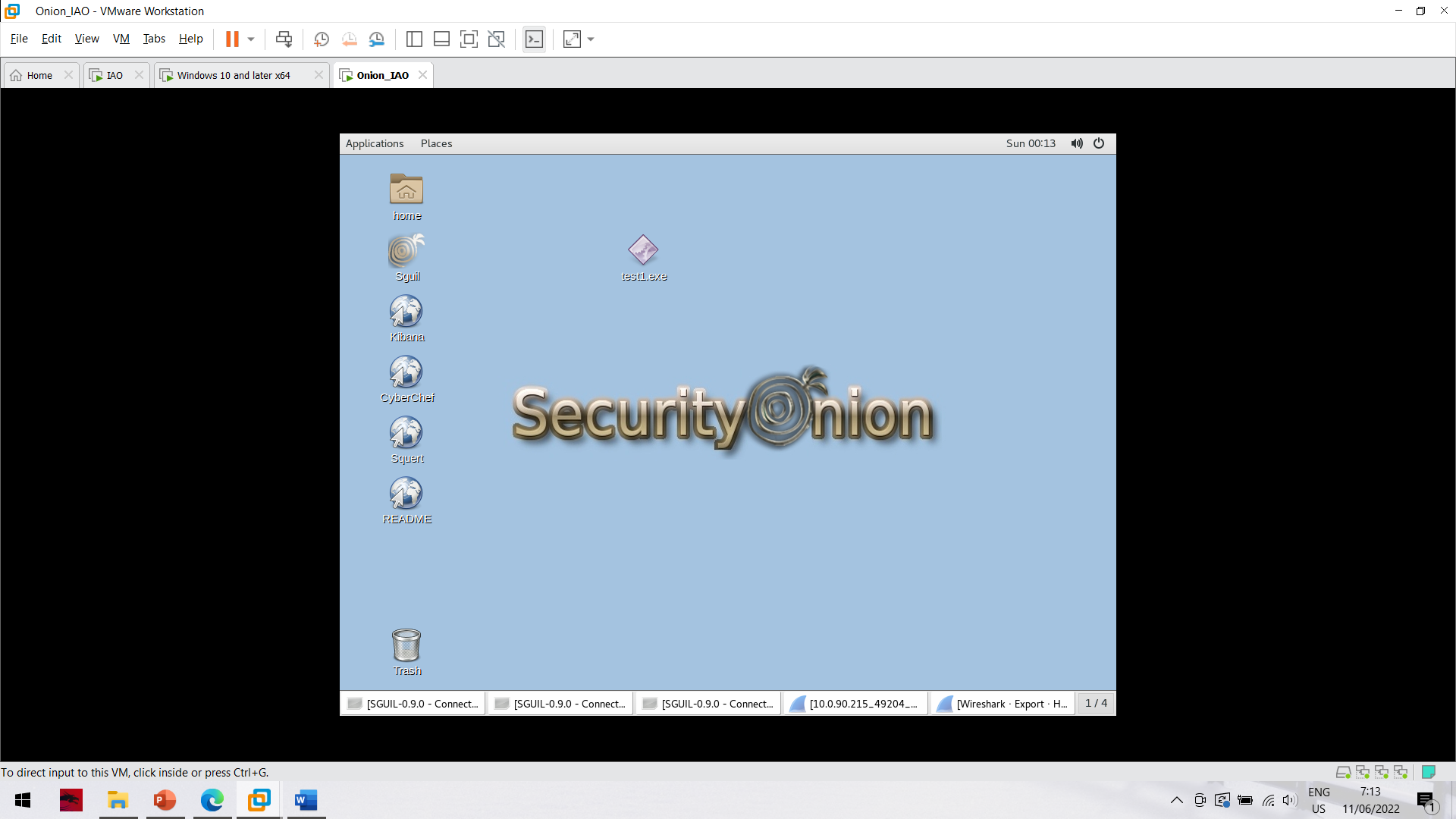
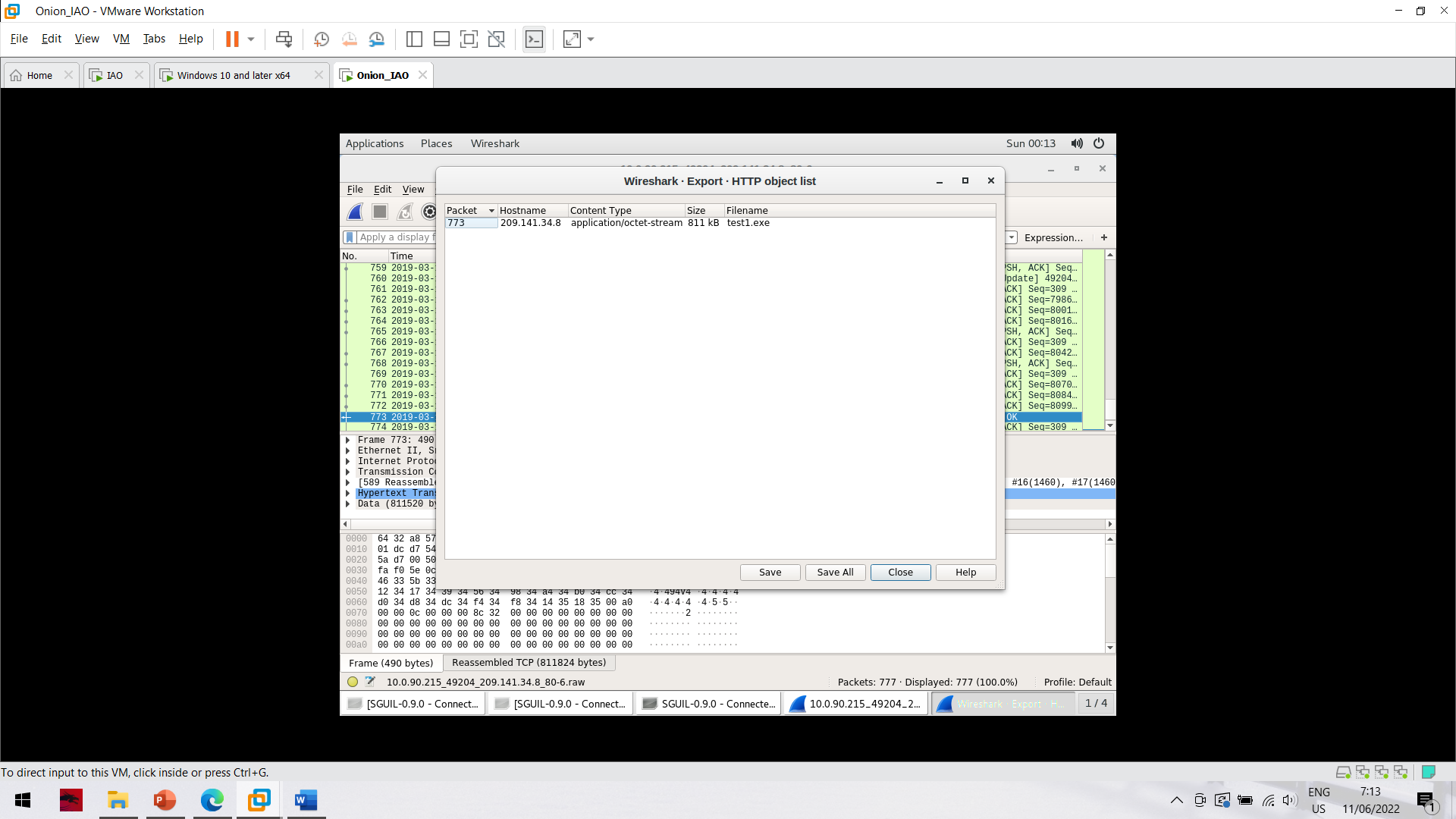
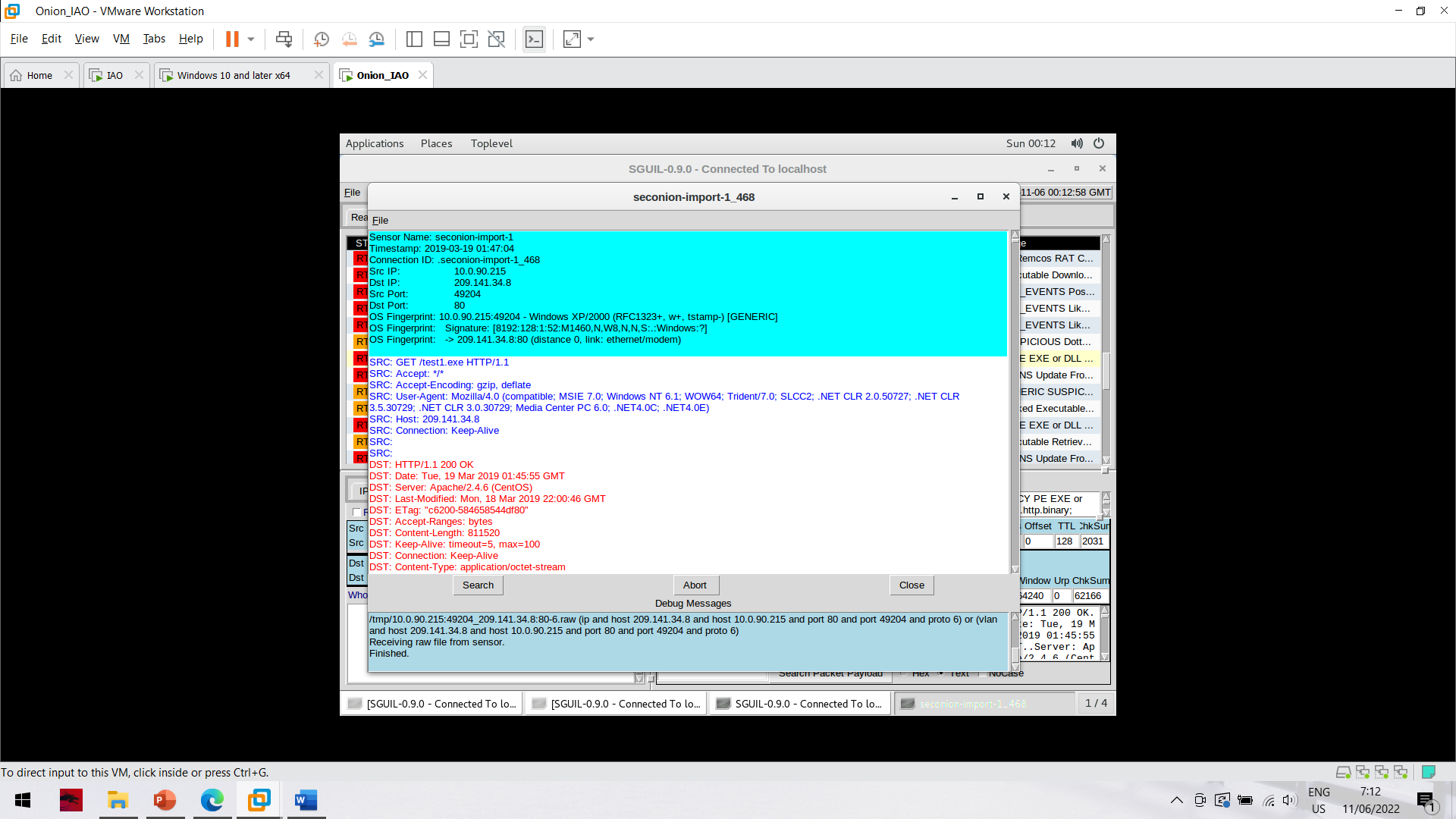
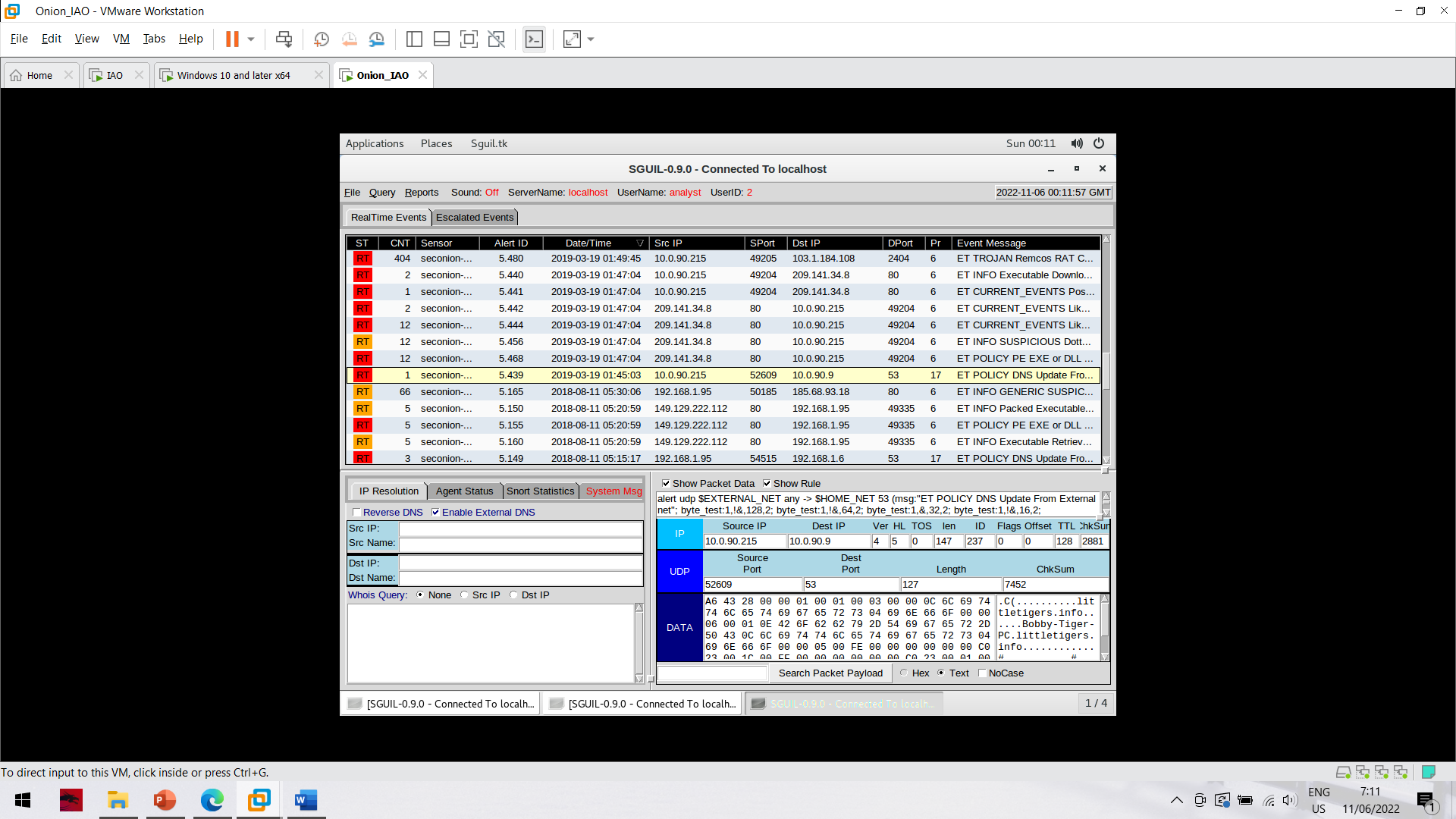
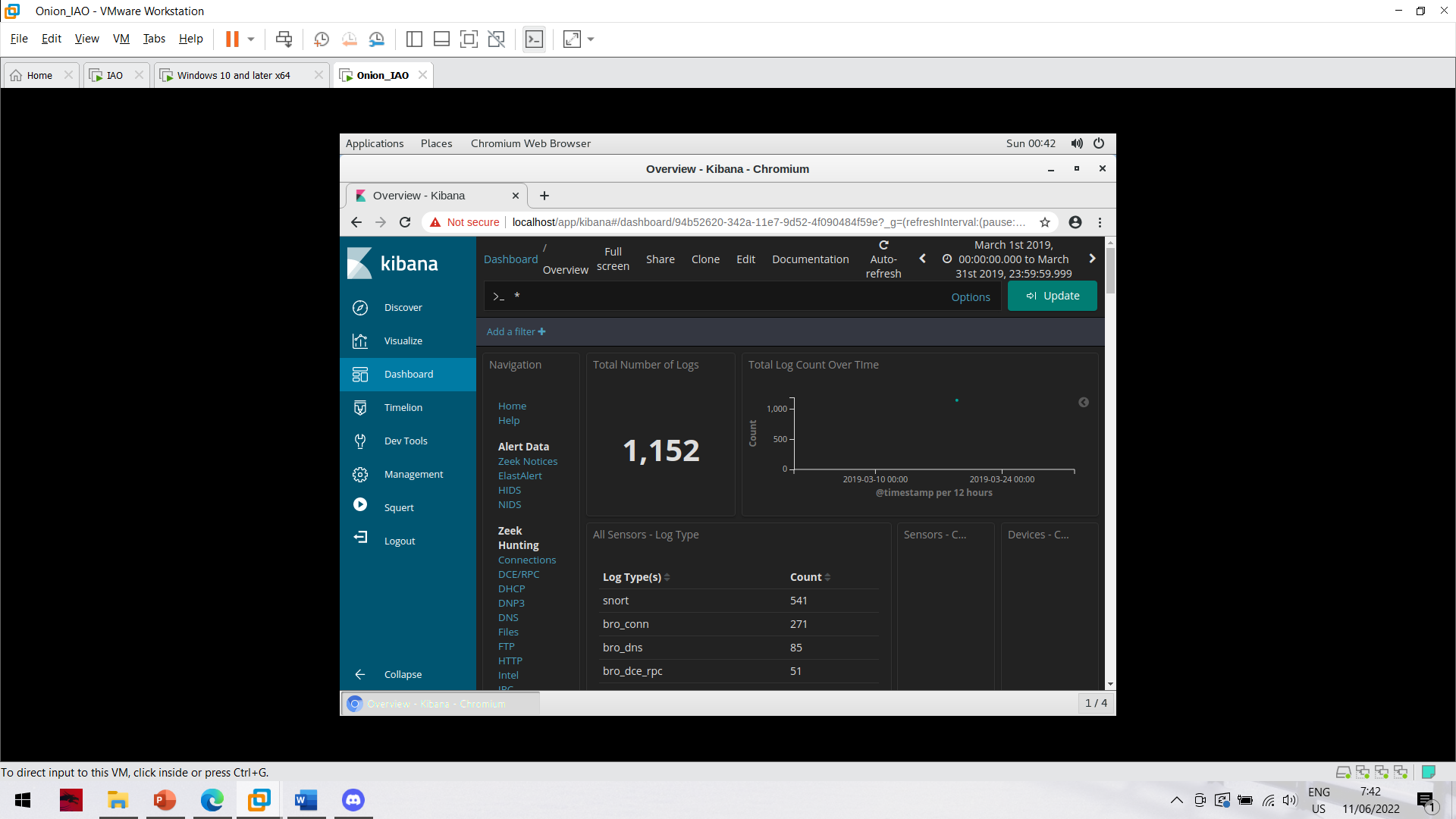
Lab - Investigating an Attack on a Windows Host

Part 1: Investigate the Attack with Sguil

Step 1: Open Sguil and locate the alerts on 3-19-2019.



Step 2: Review the alerts in detail. Part 2: Use Kibana to Investigate Alerts



Step 2: Review the alerts in the narrowed timeframe.

