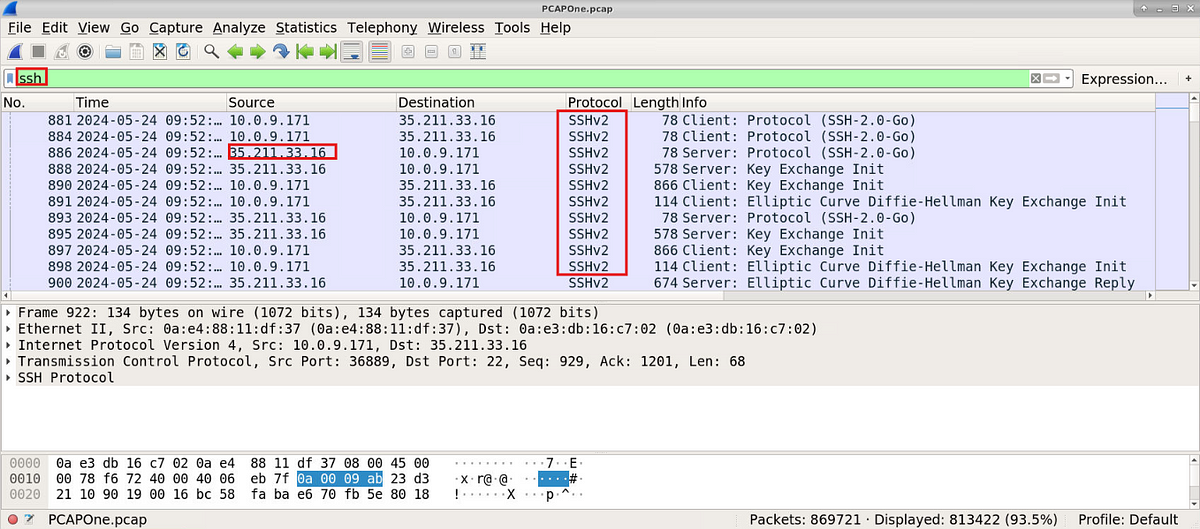
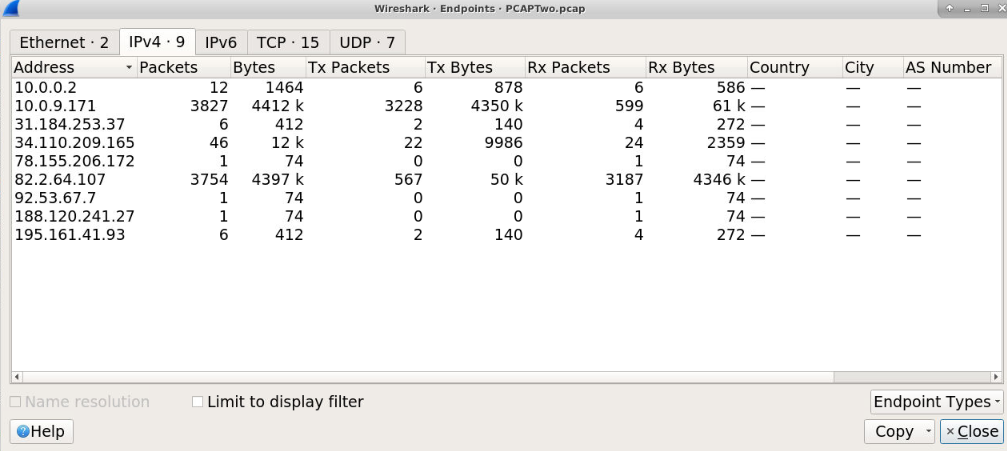
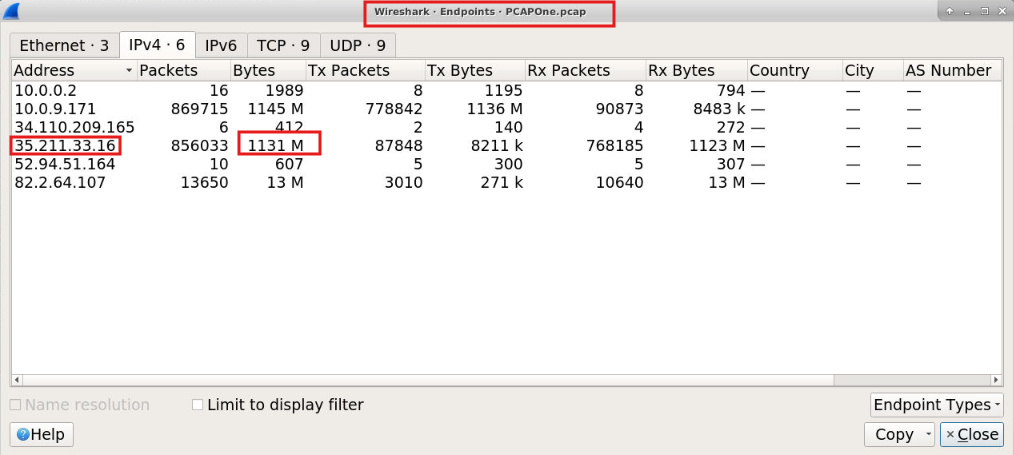
### **PIGGY — BTLO**

Scenario: Investigate some simple network activity in Wireshark! You can launch Wireshark in a terminal with the command ‘Wireshark’. The questions are mapped to the four PCAPs on the Desktop.

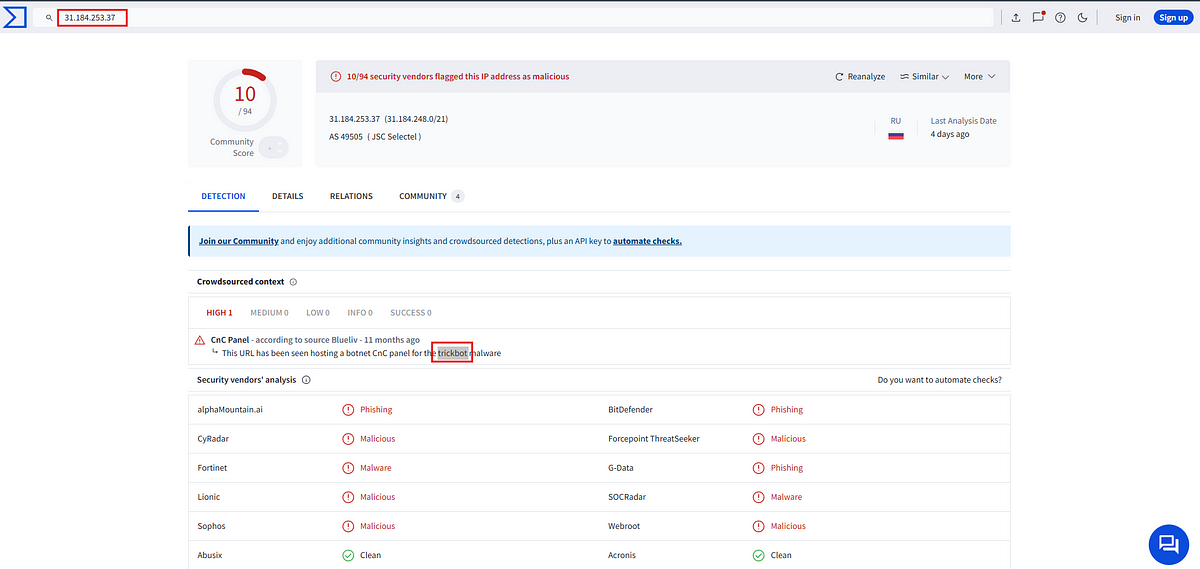
1. PCAP One) What remote IP address was used to transfer data over SSH? (Format: X.X.X.X)



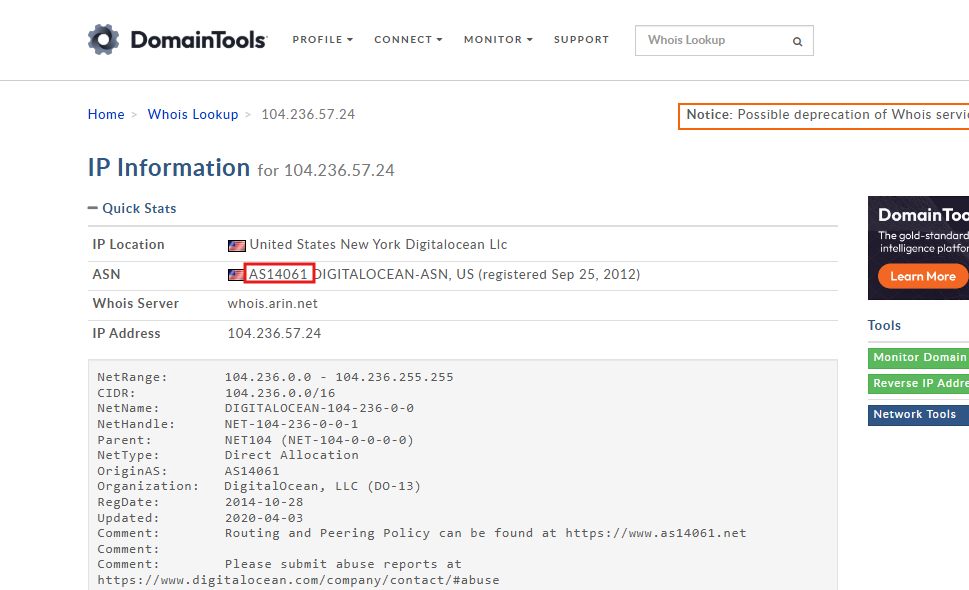
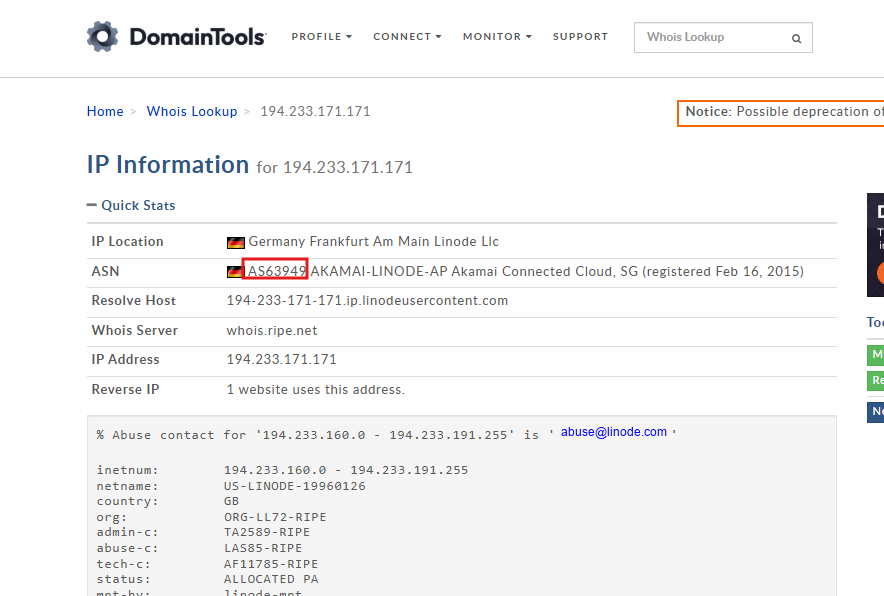
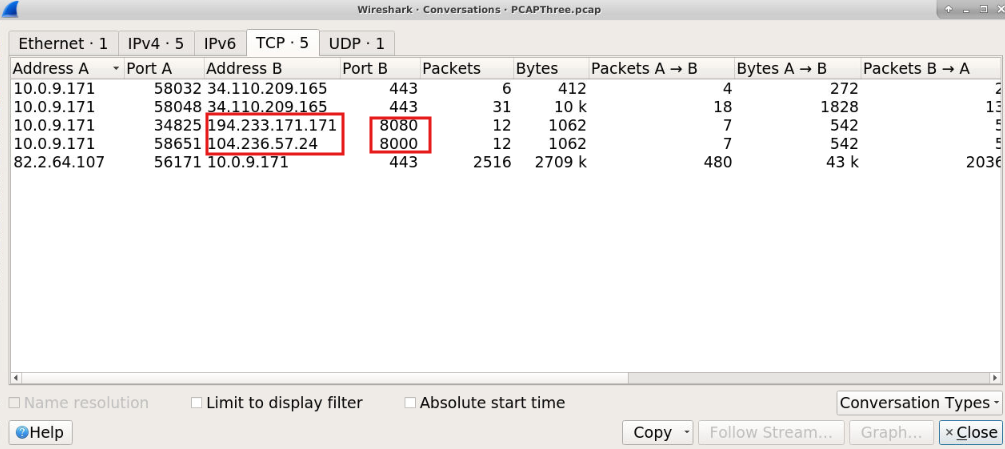
2. PCAP One) How much data was transferred in total? (Format: XXXX M)



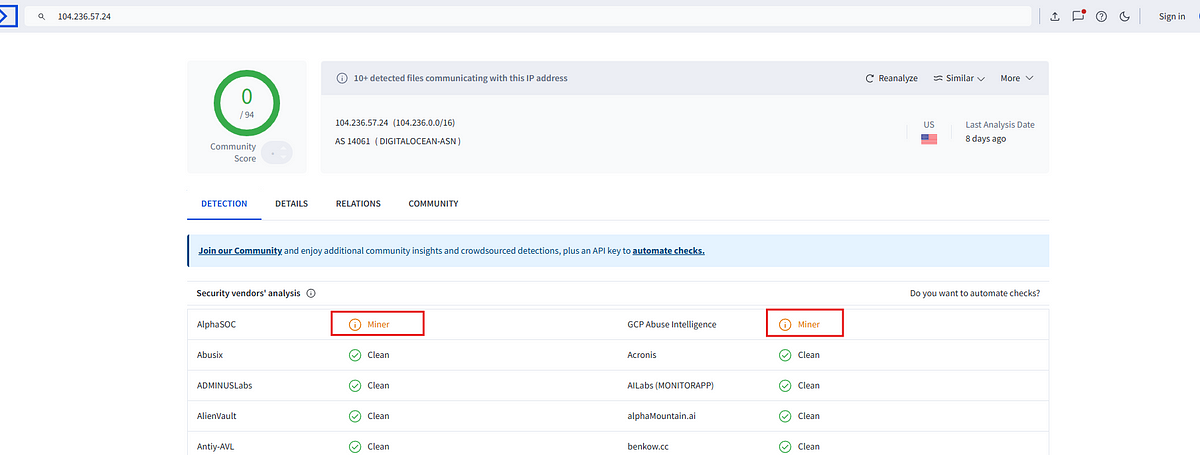
3. PCAP Two) Review the IPs the infected system has communicated with. Perform OSINT searches to identify the malware family tied to this infrastructure (Format: MalwareName)



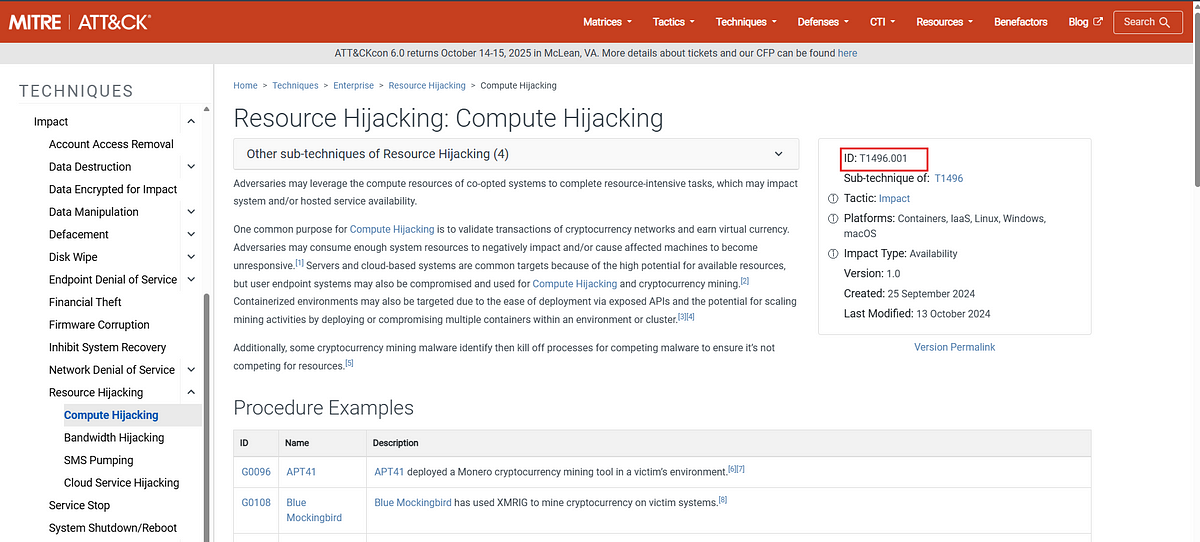
4. PCAP Three) Review the two IPs that are communicating on an unusual port. What are the two ASN numbers these IPs belong to? (Format: ASN, ASN)



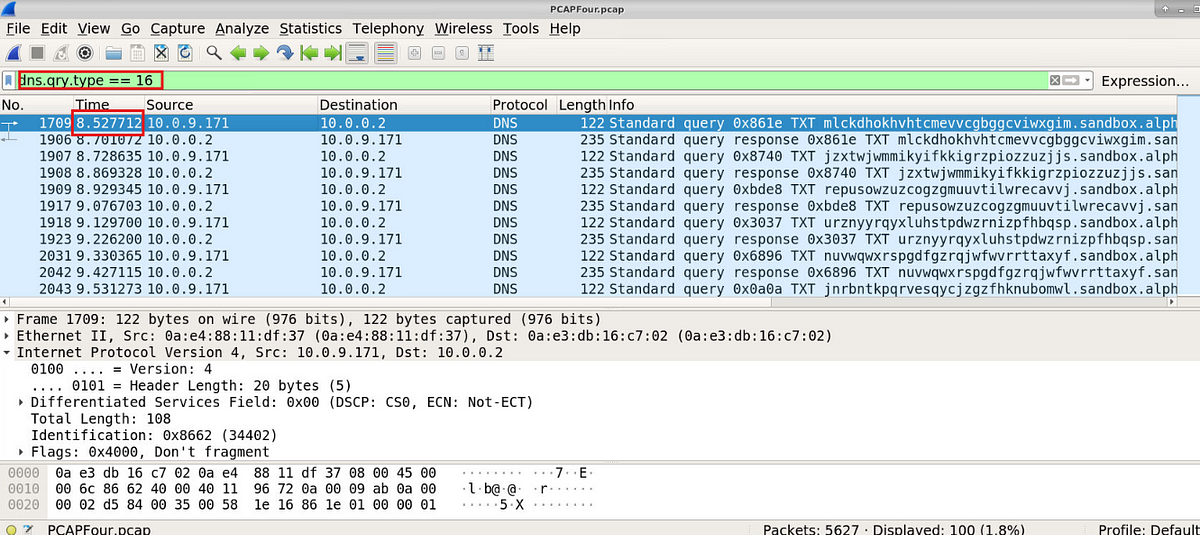
5. PCAP Three) Perform OSINT checks. What malware category have these IPs been attributed to historically? (Format: MalwareType)



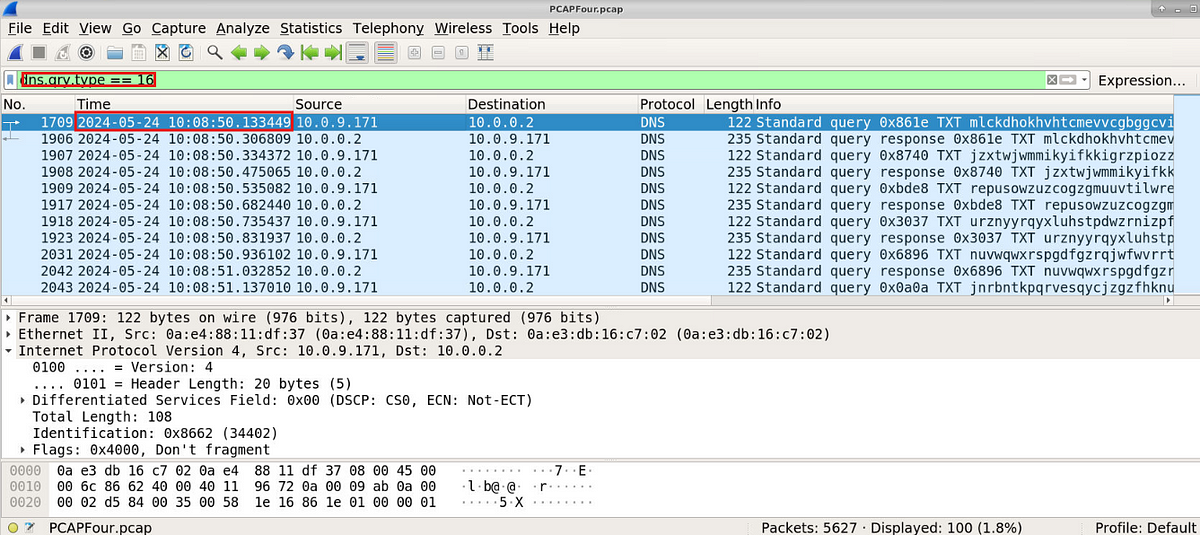
6. PCAP Three) What ATT&CK technique is most closely related to this activity? (Format: TXXXX)



7. PCAP Four) Go to View > Time Display Format > Seconds Since Beginning of Capture. How long into the capture was the first TXT record query made? (Use the default time, which is seconds since the packet capture started) (Format: X.xxxxxx)



8. PCAP Four) Go to View > Time Display Format > UTC Date and Time of Day. What is the date and timestamp? (Format: YYYY-MM-DD HH:MM:SS)



9. PCAP Four) What is the ATT&CK subtechnique relating to this activity? (Format: TXXXX.xxx)

