**SCENARIO**

LAN segment data:

* LAN segment range:  10.0.76.0/24 (10.0.76.0 through 10.0.76.255)
* Domain:  phenomenoc.com
* Domain controller:  10.0.76.6 - Phenomenoc-DC
* LAN segment gateway:  10.0.76.1
* LAN segment broadcast address:  10.0.76.255

**YOUR TASK**

Review the pcap, alerts, and the extracted malware sample to answer the following questions:

* What is the IP address, MAC address, and host name of the infected Windows host?
* What is the Windows user account name for the infected Windows host?
* What was the delivery method for the malware?
* What was the IP address used by the delivery method for this infection?
* What is the SHA256 hash of the EXE retrieved from the infected Windows host?
* Based on the alerts, what type of malware infected the Windows host?
* What is the IP address of the post-infection traffic?
* What is the domain name used for the post-infection traffic?
* Draft an incident report for the pcap.