BACKGROUND:

You work as an analyst at a Security Operation Center (SOC). Someone contacts your team to report a coworker has downloaded a suspicious file after searching for Google Authenticator. The caller provides some information similar to social media posts at:

- https://www.linkedin.com/posts/unit42_2025-01-22-wednesday-a-malicious-ad-led-activity-7288213662329192450-ky3V/
- https://x.com/Unit42_Intel/status/1882448037030584611

Based on the caller's initial information, you confirm there was an infection. You retrieve a pcap of the associated traffic. Reviewing the traffic, you find several indicators matching details from a Github page referenced in the above social media posts. After confirming an infection happened, you begin writing an incident report.

LAN SEGMENT DETAILS FROM THE PCAP:

- LAN segment range: 10.1.17.0/24 (10.1.17.0 through 10.1.17.255)
- Domain: bluemoontuesday.com
- AD environment name: BLUEMOONTUESDAY
- Domain Controller: 10.1.17.2 – WIN-GSH54QLW48D
- LAN segment gateway: 10.1.17.1
- LAN segment broadcast address: 10.1.17.255

TASK:

For this exercise, answer the following questions for your incident report:

- What is the IP address of the infected Windows client?

ANSWER: 10.1.17.215

- What is the mac address of the infected Windows client?

ANSWER: 00:d0:b7:26:4a:74

- What is the host name of the infected Windows client?

ANSWER: Intel_26:4a:74

- What is the user account name from the infected Windows client?

ANSWER: <ROOT>

- What is the likely domain name for the fake Google Authenticator page?

ANSWER: BLUEMOONTUESDAY.COM

- What are the IP addresses used for C2 servers for this infection?

ANSWER: 10.1.17.2