Questions Network Forensics Quiz

- Attempt all the questions using tool Wireshark.
- Please give valid reasons and screenshots to support your reasoning.

1. **IP Address Check**
    a. What steps would you take to identify an IP address check performed by an infected Windows host in network traffic?
    b. Why might Trickbot perform an IP address check, and how could this activity be used to identify an infection?
2. **Unusual Port Usage**
    a. How would you filter network traffic in Wireshark to detect HTTPS/SSL/TLS traffic over non-standard ports, such as 447, 449, etc.?
    b. What does the use of non-standard ports suggest about Trickbot's behavior, and how can this knowledge aid in detection?
3. **HTTP Requests Ending in .png**
    a. What would be your approach to determine if .png files in these requests are actually belongs to some different file type?
4. **IP Address Check and Connection Attempts**
    a. How would you investigate multiple attempted TCP connections to different IP addresses over port 443 to determine their purpose and relevance to Trickbot's activity?
5. **Data Exfiltration Investigation**
    a. What filters would you use to inspect the data being exfiltrated from the infected host over TCP port 8082, such as system information or browser cache passwords, etc.?
    b. How can you verify that the data being transmitted corresponds to sensitive information, such as credentials from email clients?