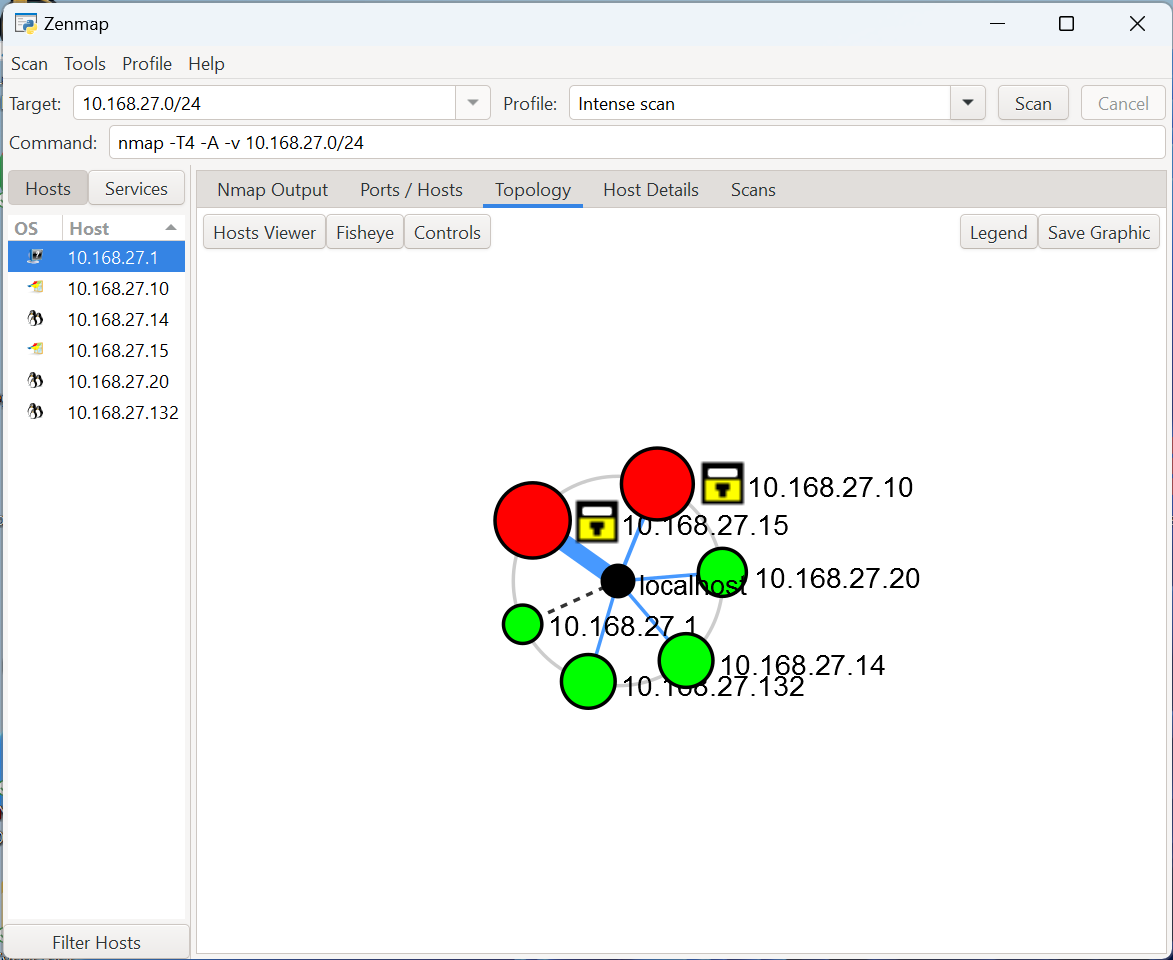
**Getting Started Task 1 Template**

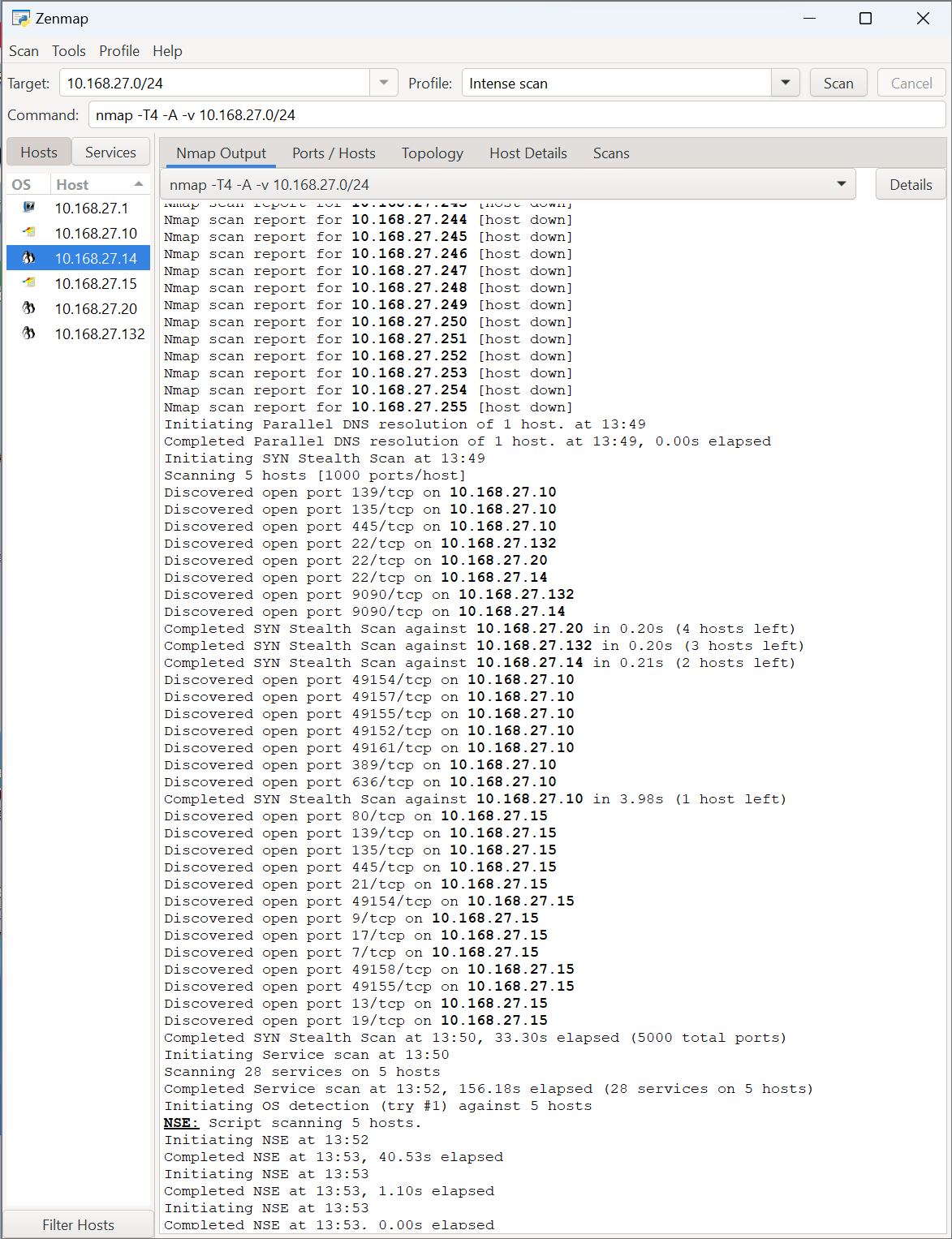
Use the template outline below to capture the rubric requirements and key points and to serve as your task report. After you have captured the appropriate data, massage each section into the required number of paragraphs and ensure you have captured all the required points highlighted.

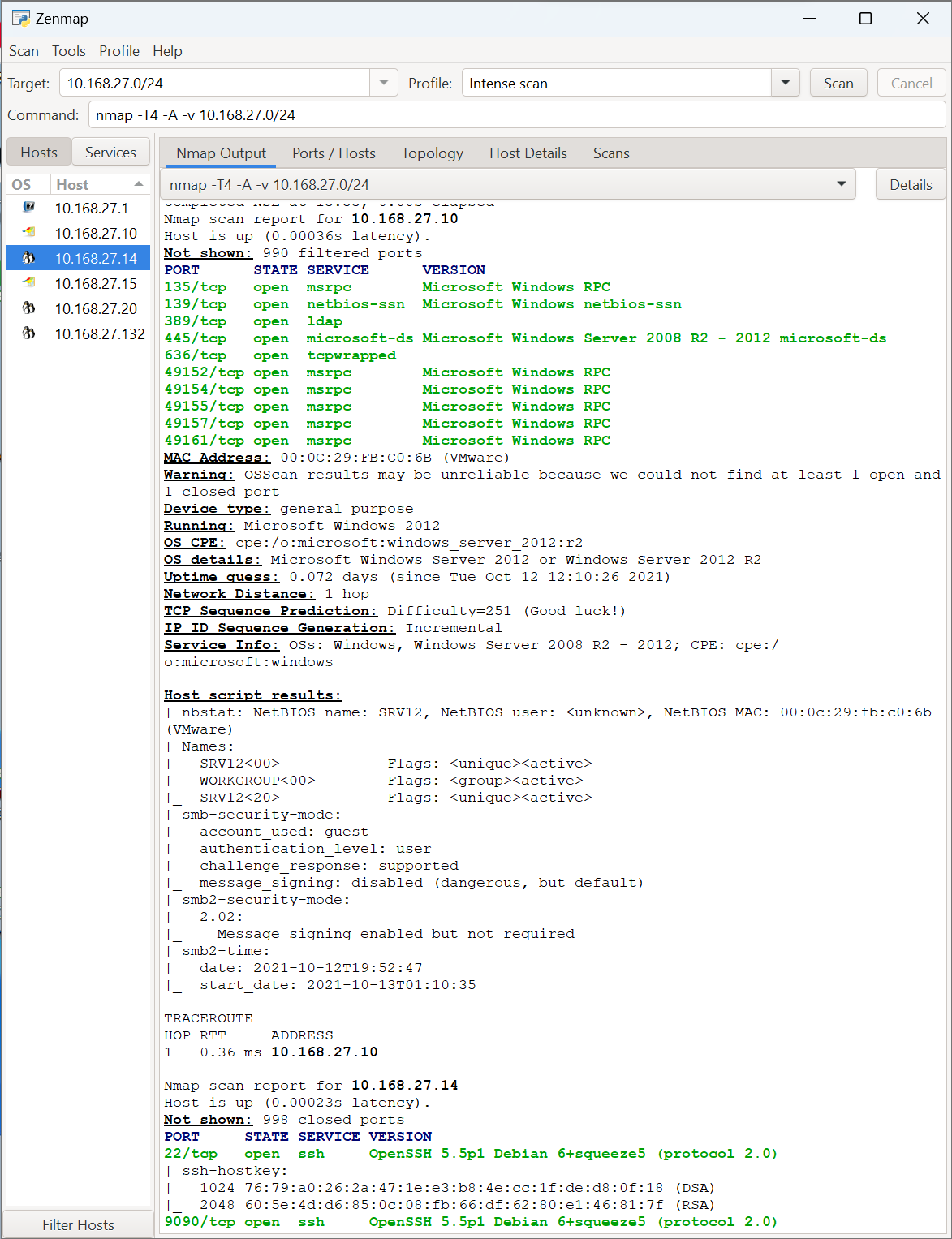
**A. Network Topology**

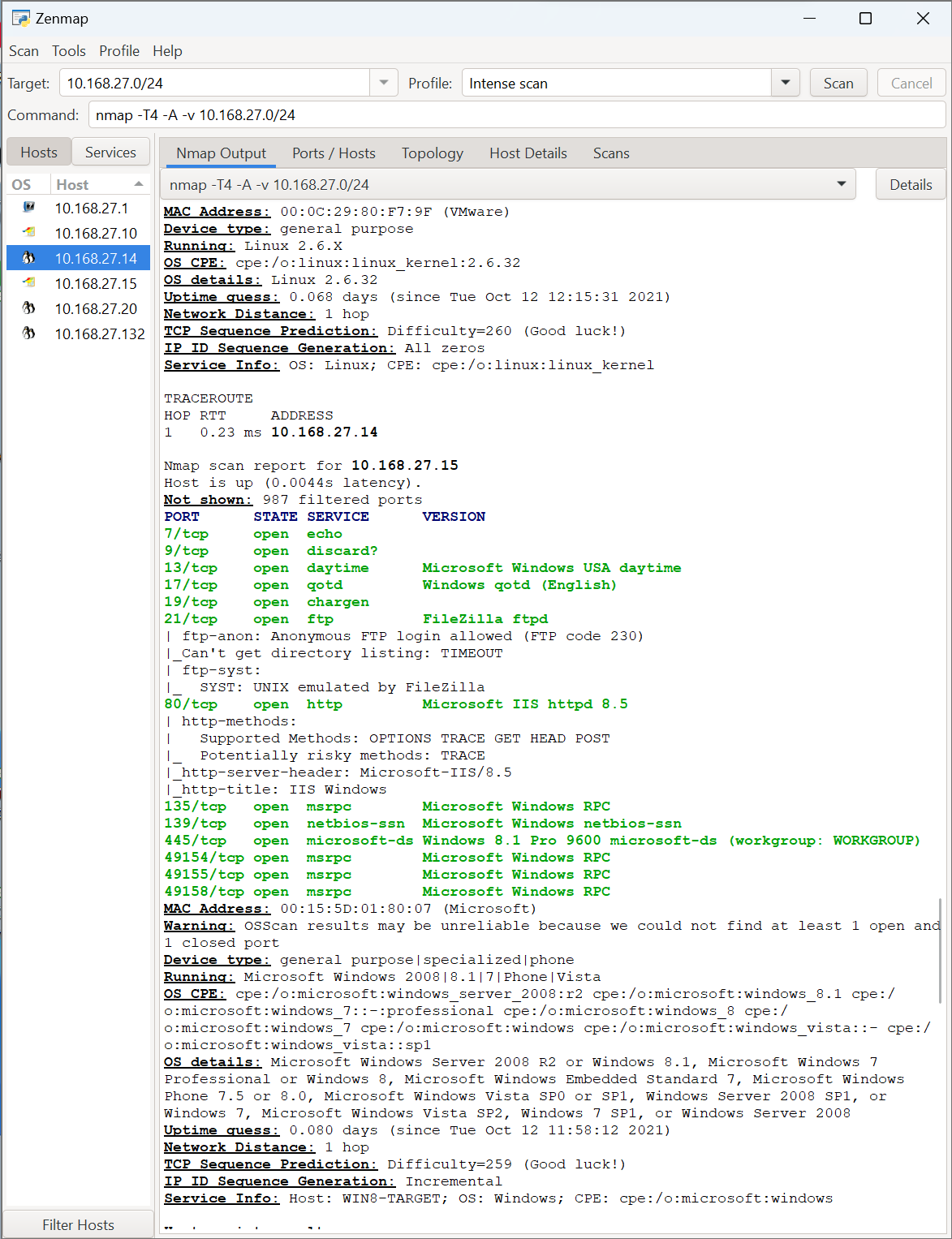


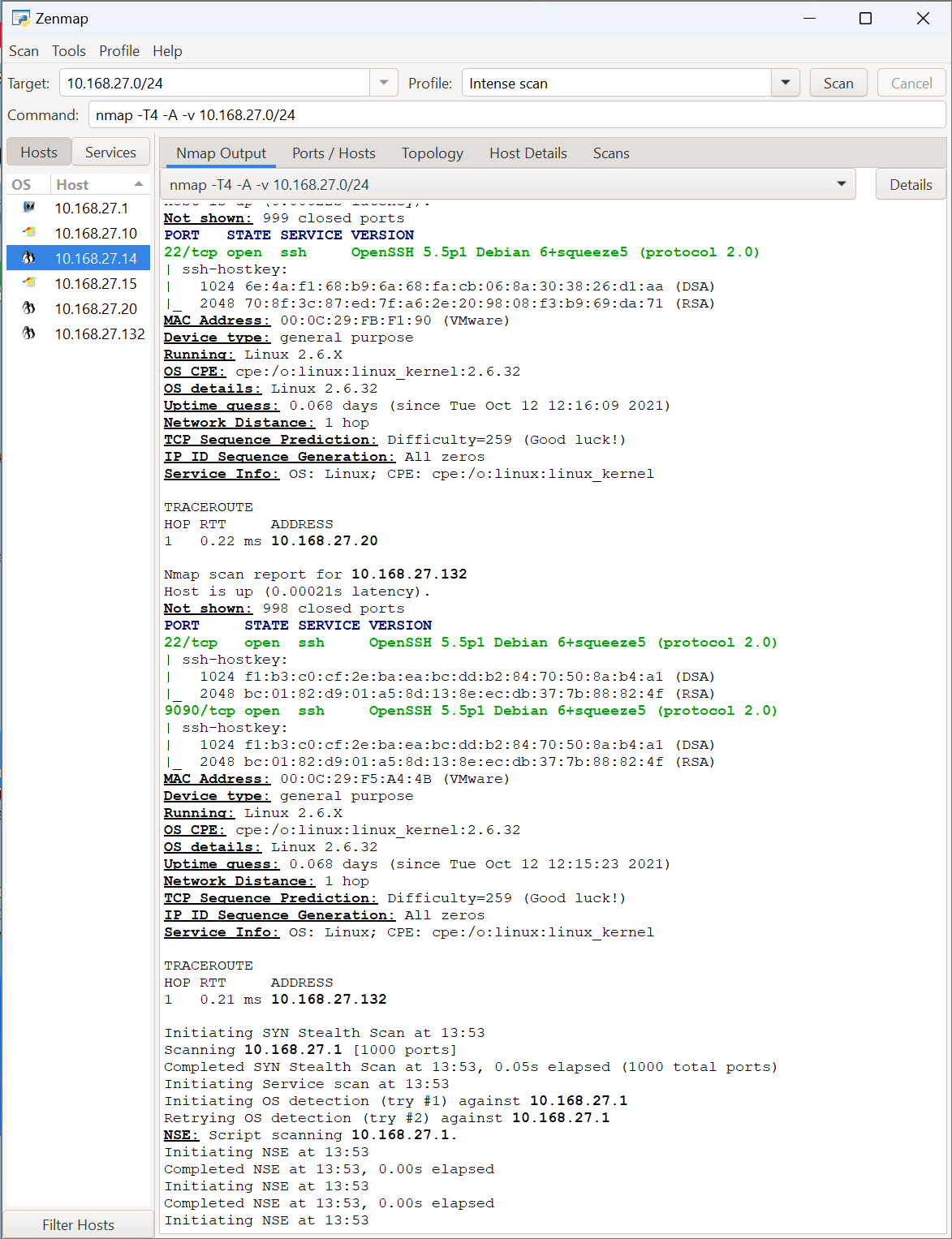
A network scan was conducted using NMAP/ZENMAP tools on the specified IP range of 10.168.27.0/24. The network is organized in a "Star" topology and consists of seven regular hosts. Out of these, four hosts have fewer than three open ports, identified as low-risk (Green), while two hosts exhibit more than six open ports, marked as high-risk (Red). The network architecture does not include any routers, switches, or wireless access points.

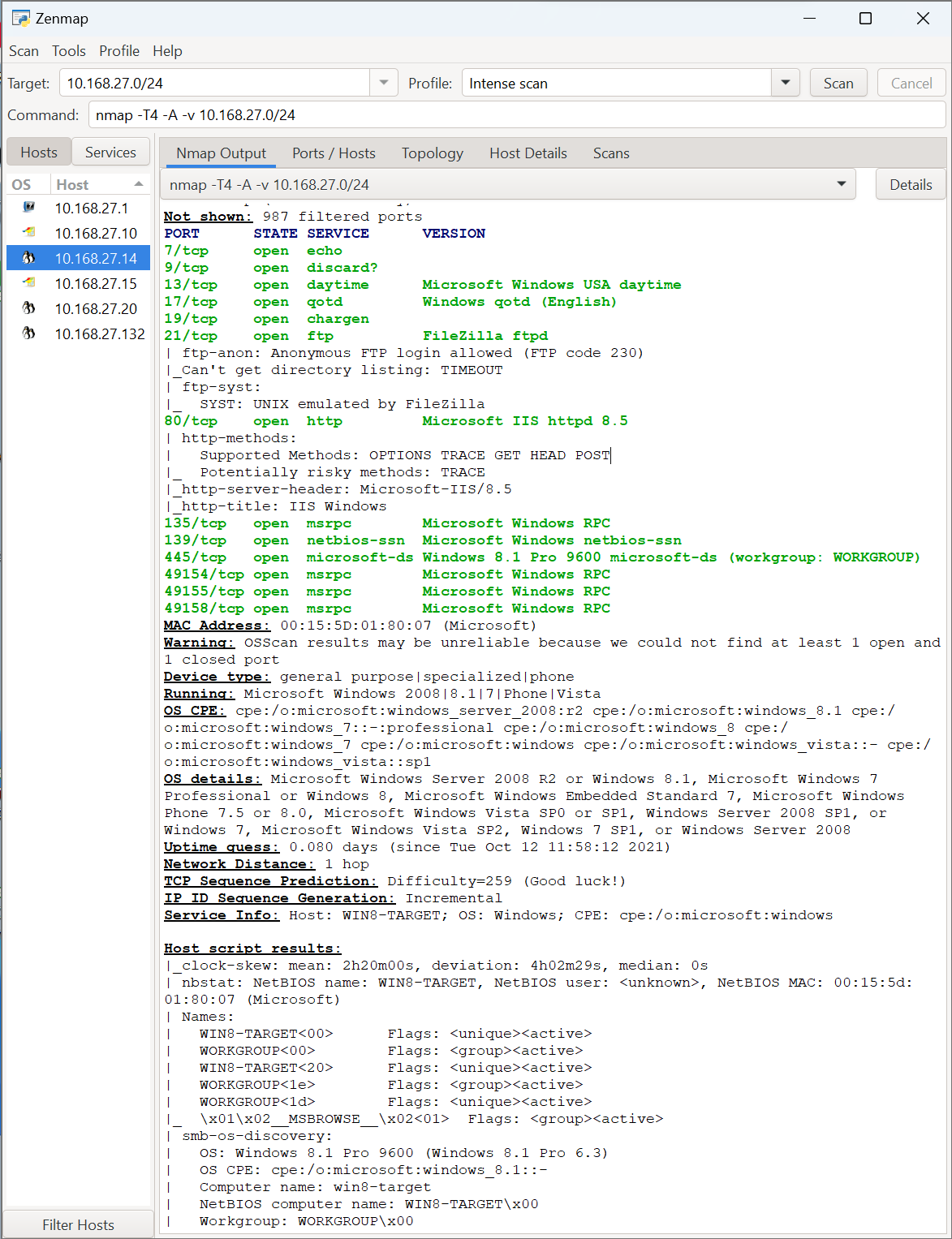
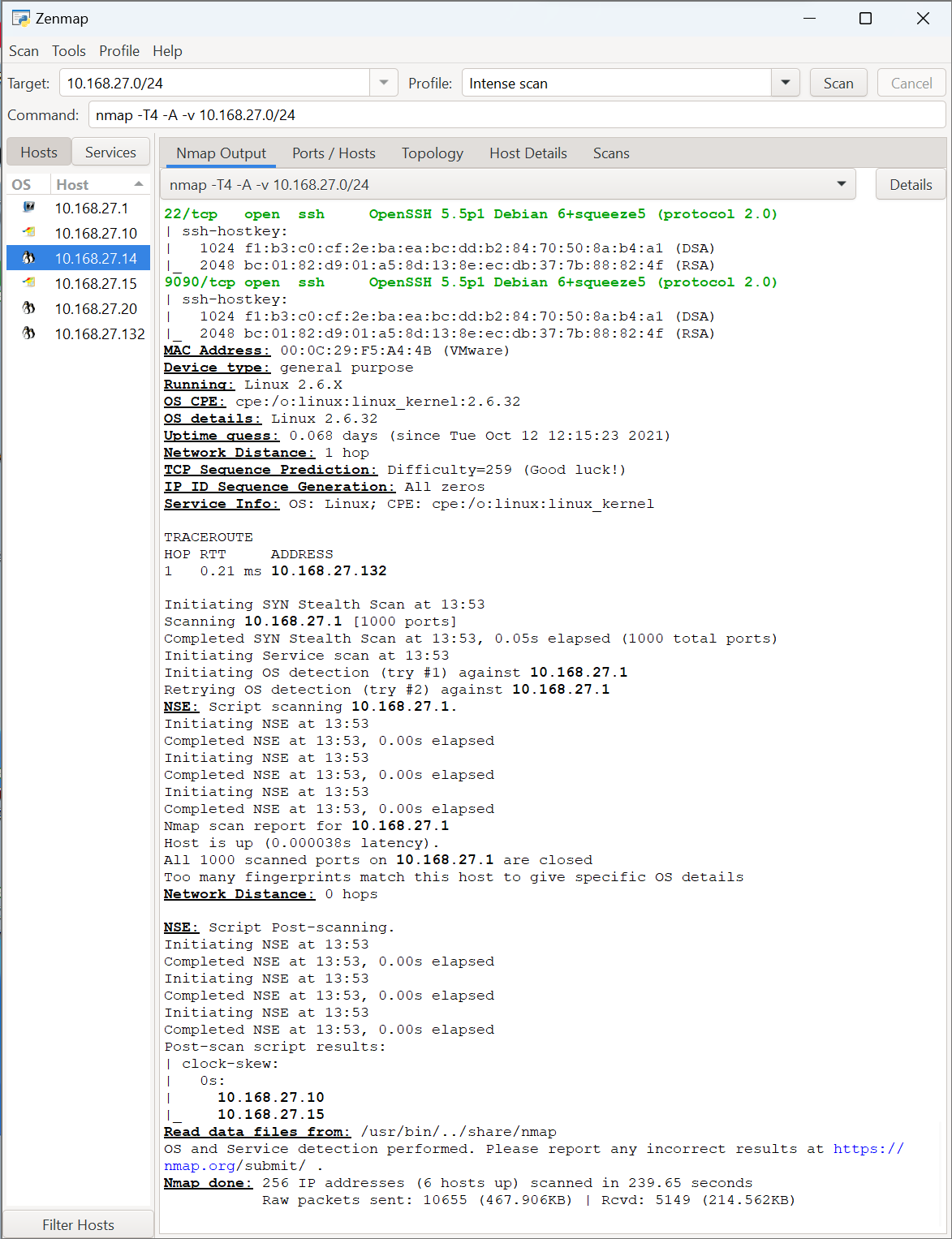
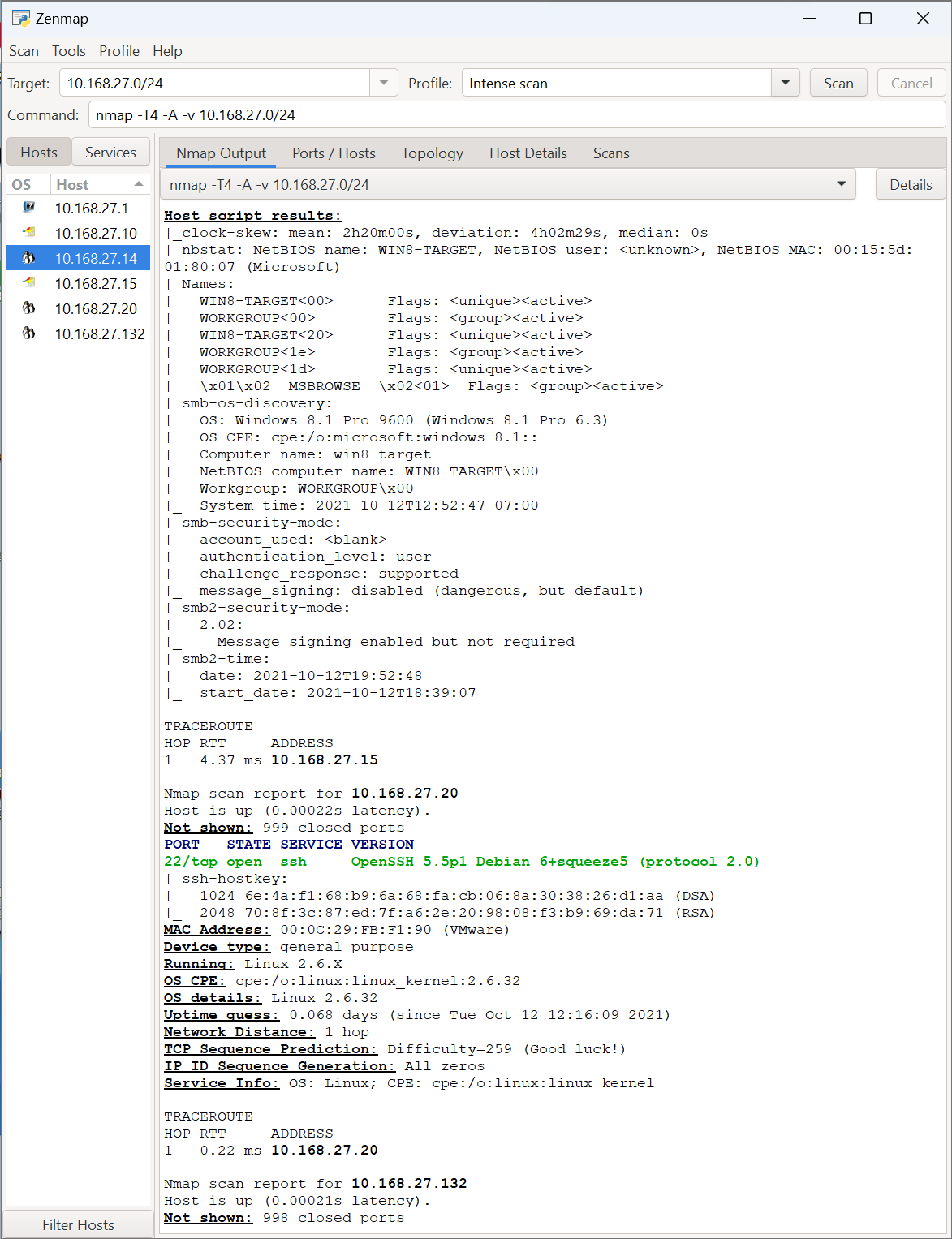
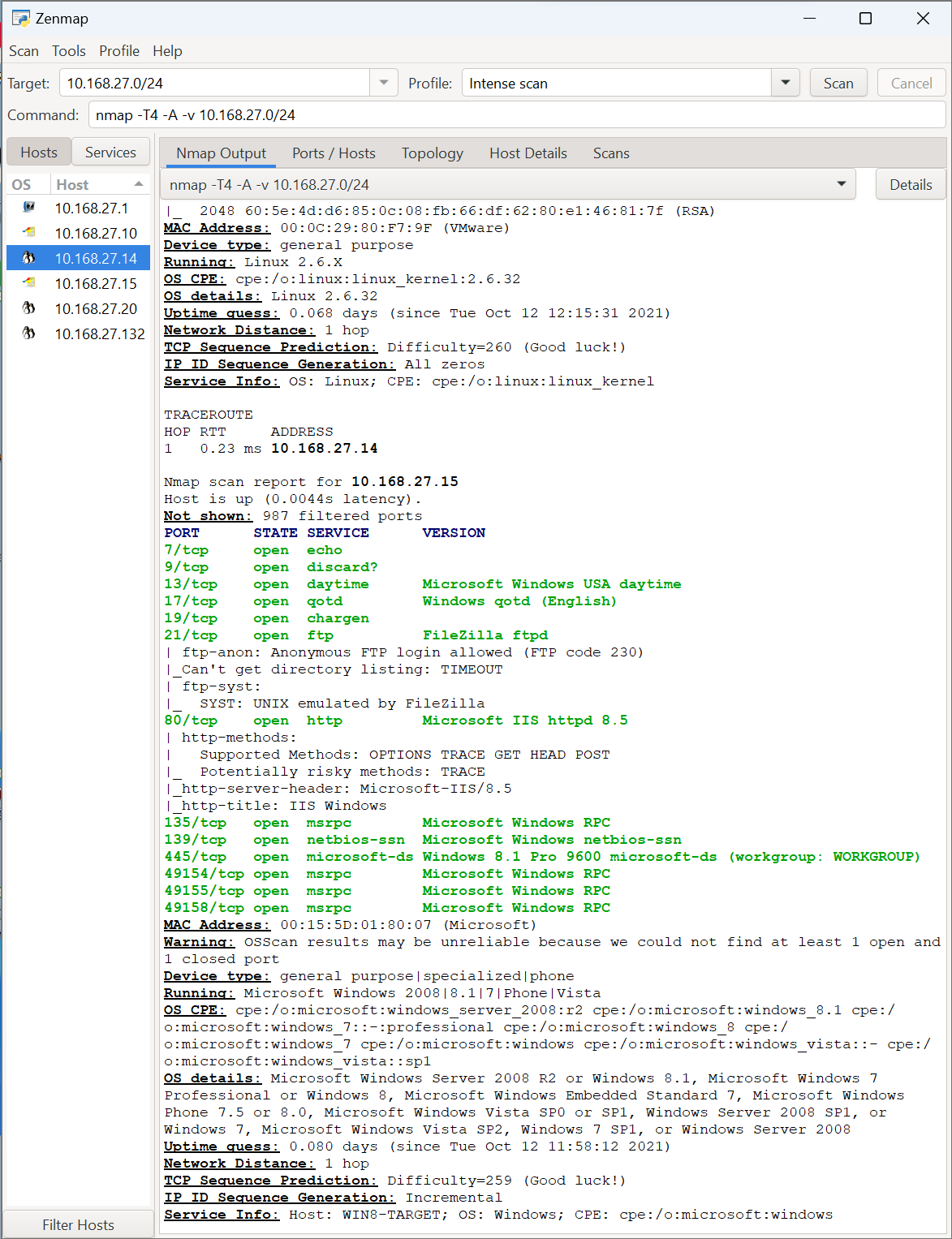












**B Summary of Vulnerabilities and Implications**

**Vulnerability 1 :** The host system utilizes the Microsoft Windows SMB service. SMB can be exploited to conduct remote code execution. If attackers exploit this flaw, they can potentially run arbitrary code on the victim machine, leading to a full system compromise.

**Vulnerability 2 :** Microsoft Windows NetBIOS on Port 139 (Host: 10.168.27.10)

The NetBIOS service running on port 139 in Microsoft Windows Server 2012 or Windows Server 2012 R2 is dated and may be vulnerable to various types of attacks, such as NetBIOS Name Service (NBNS) spoofing and unauthorized information disclosure. NBNS is susceptible to man-in-the-middle attacks, which could allow attackers to capture sensitive data or redirect traffic.

**Third vulnerability**

**FileZilla FTP Vulnerability: Risks and Implications**

The FTP service running FileZilla on port 21 allows for anonymous logins, posing multiple security risks. This vulnerability provides an avenue for unauthorized file access, where attackers can easily download, upload, or delete files from the server.

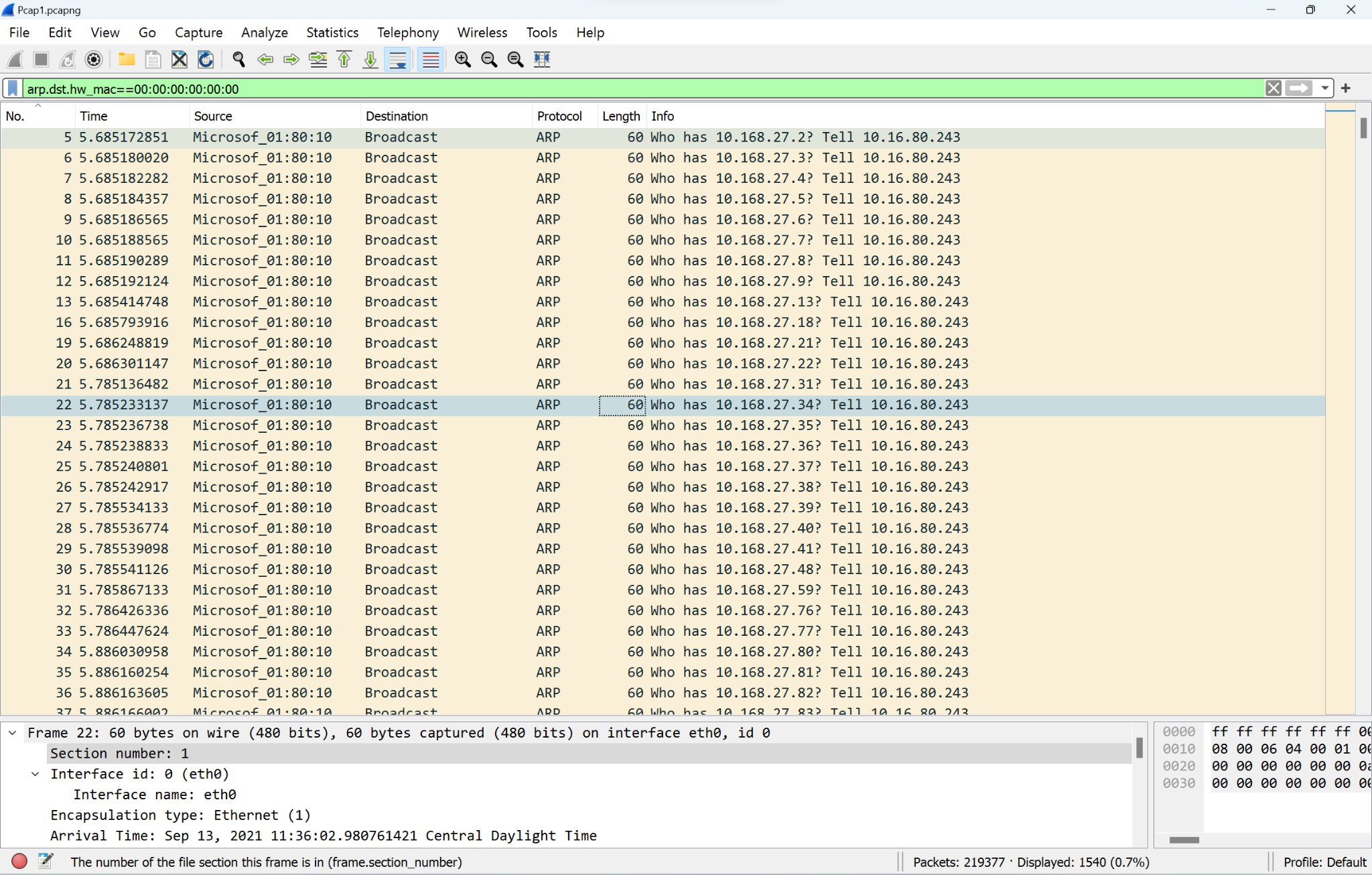
Also, the security lapse risks data leakage, as sensitive information hosted on the FTP server could be accessed and downloaded by unauthorized users.

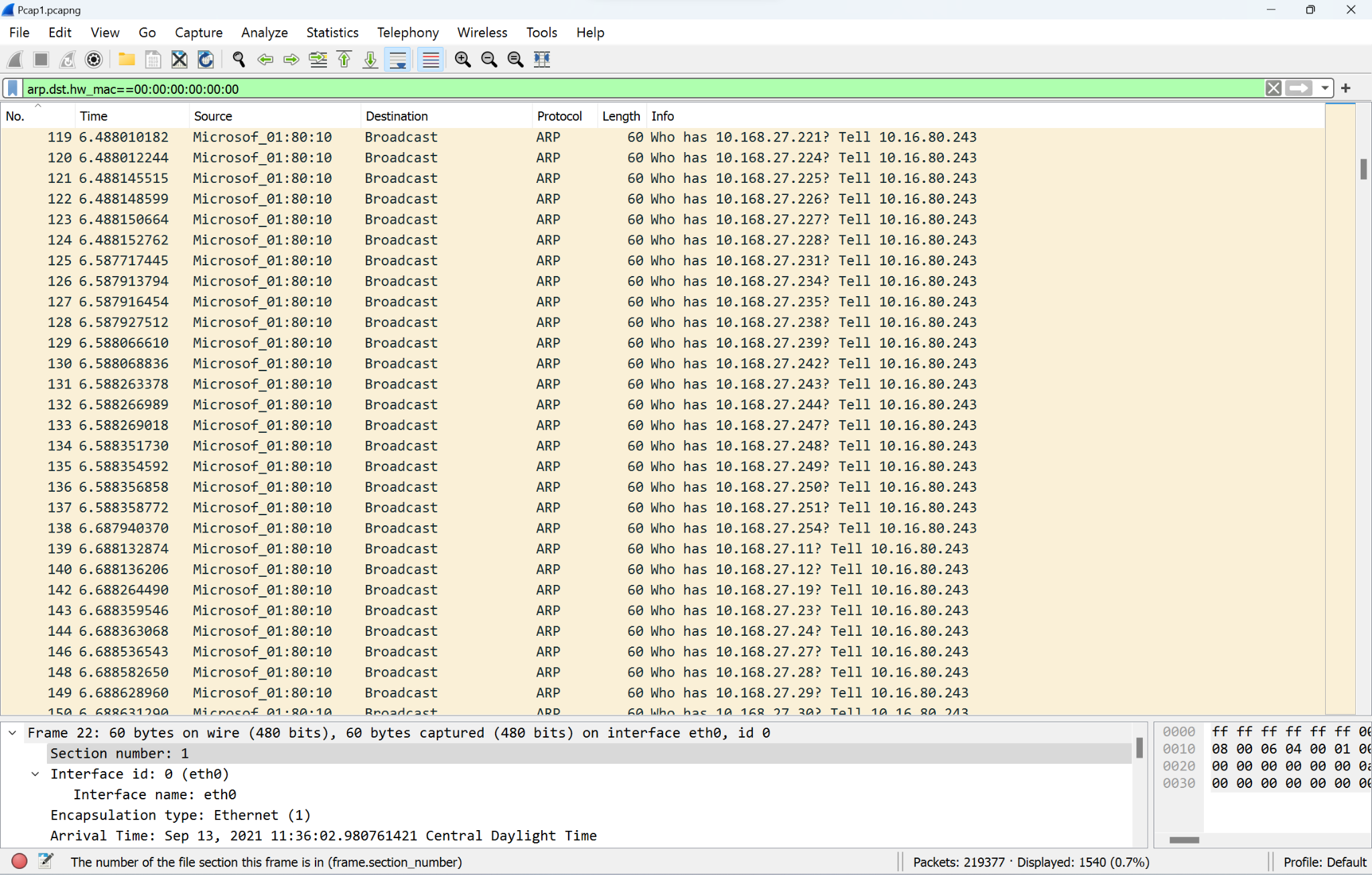
The FTP service's vulnerability opens the possibility for potential code execution; malicious files uploaded to the server could be executed, thereby compromising not only the host but also the entire network

**C. Wireshark Anomalies**

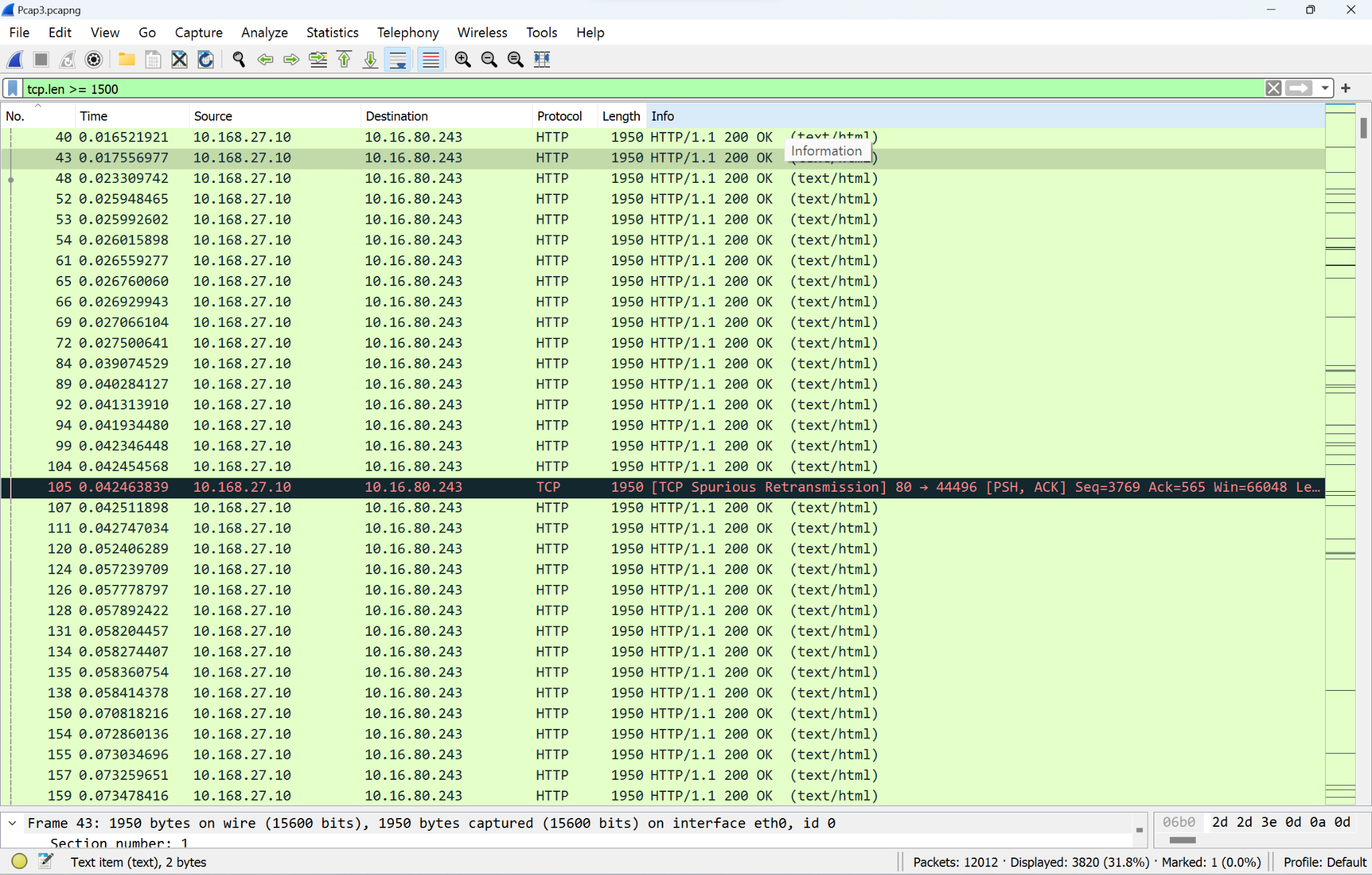
**First Anomaly : Excessive ARP request**

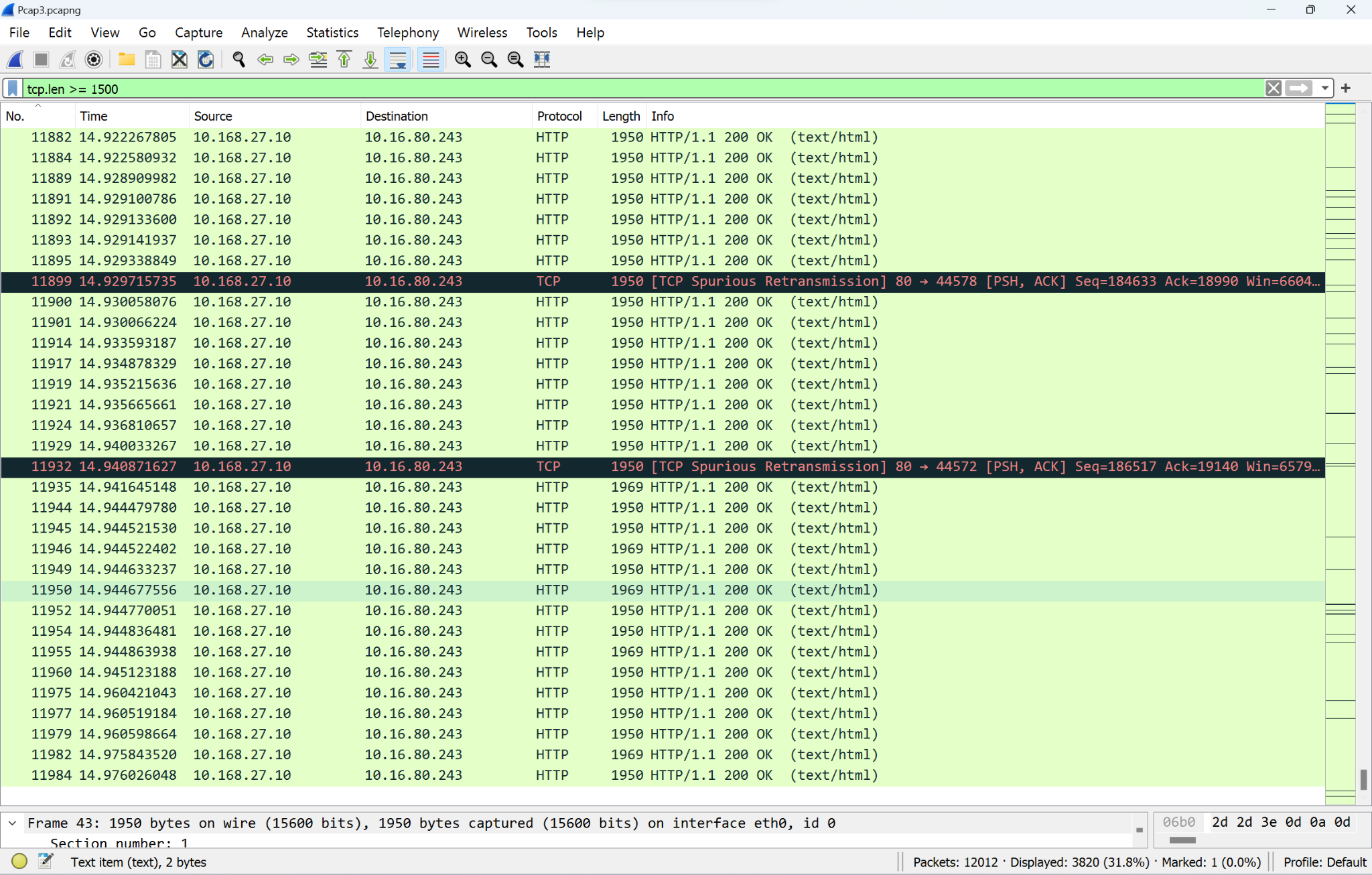
packets 5 - 138

****

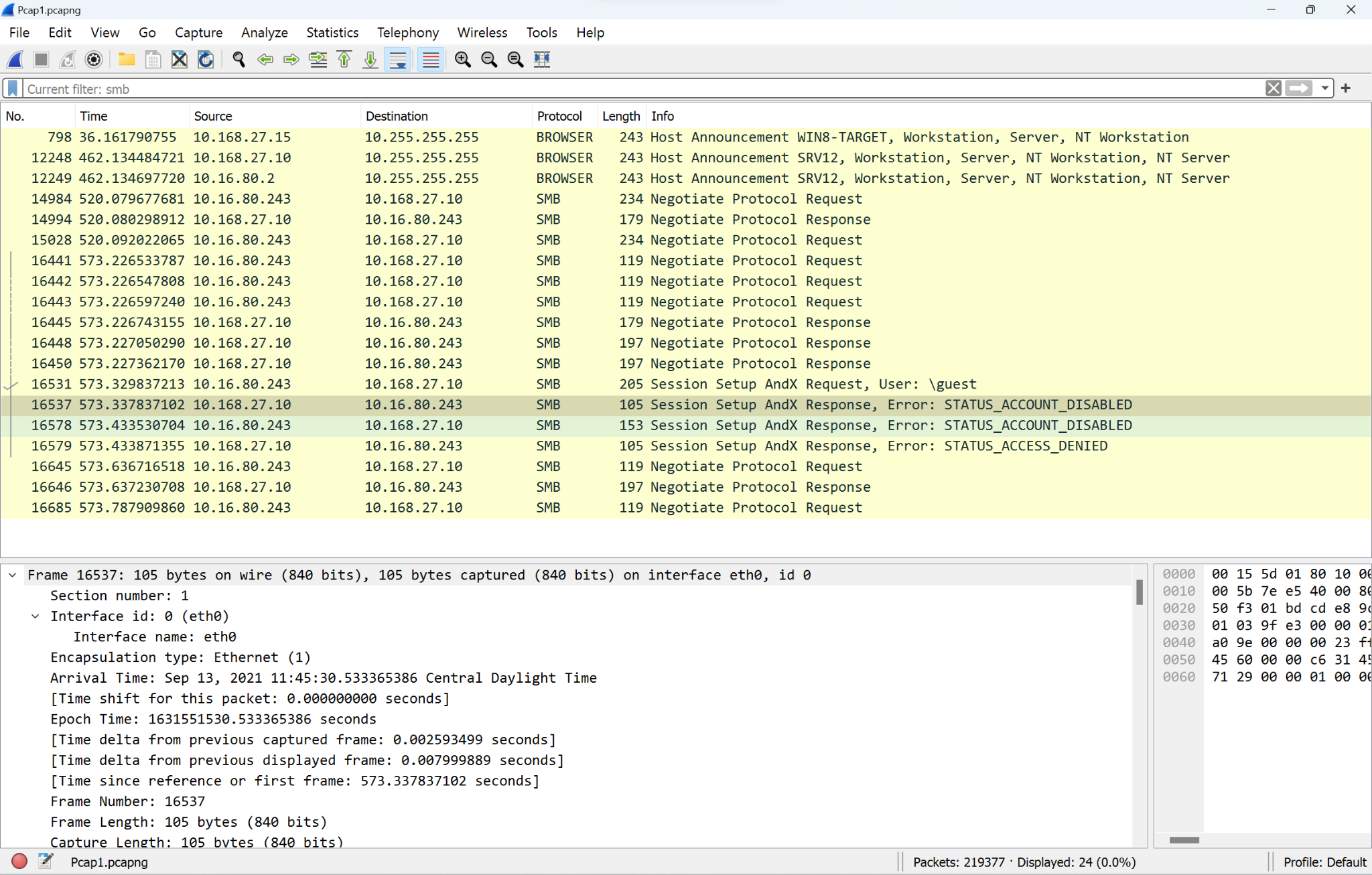
****

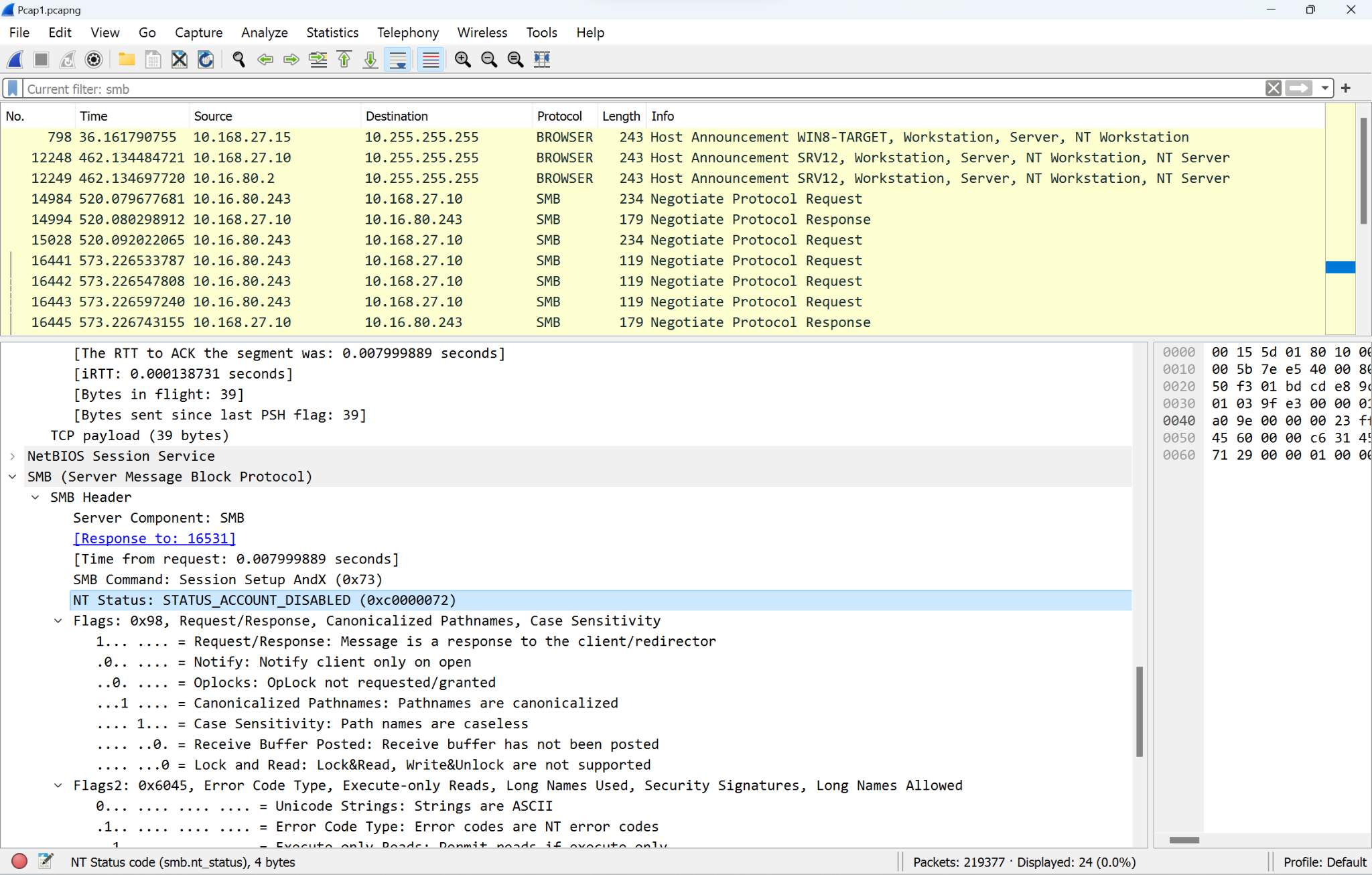
**Second Anomaly: Large size packets, same source to same destination**

****

Packet range 40 -11984

**Third Anomaly: ERROR SMB account access denied Packets 16537,16578,16579**





**D. Implications of each Wireshark Anomaly**

**Implications of taking no action 1**

Failing to address the ARP anomaly can expose the network to security risks such as ARP spoofing attacks. This type of attack can lead to unauthorized data access, posing significant risks to the organization's confidentiality and integrity.

**Implications of taking no action 2**

Failure to address the large, repeated packet transfers between the source and destination addresses could lead to potential data loss, network outages, or degraded system performance.

**Implications of taking no action 3**

The "STATUS\_ACCESS\_DENIED" in the SMB session setup suggests an issue with permission or access controls. This could interfere with legitimate networking operations between the source and destination. Given that SMB is widely used for file sharing and other network resources, this could be a serious concern. If access is being denied where it should be granted, this could hamper workflow or even indicate a security issue, where either a user is prevented from accessing resources they should or a potentially compromised account is appropriately being denied access.

**E. Recommended Solutions**

**First Vulnerability**

Disable SMBv1 and move to a more secure version like SMBv3.

Use SMB signing to protect against man-in-the-middle attacks. This will solve the vulnerability.

*Supported by: National Vulnerability Database (NVD). (n.d.). CVE Details.*

**Second Vulnerability**

Limit the NetBIOS exposure to only internal network segments.

Disable NetBIOS over TCP/IP if it is not necessary for the network. This will solve the vulnerability.

*Supported by: Cybersecurity & Infrastructure Security Agency (CISA). (2021). Security Tip (ST04-010).*

**Third Vulnerability**

Disable anonymous login for the FTP service.

Implement strong authentication methods. This will solve the vulnerability.

*Supported by: National Institute of Standards and Technology (NIST). (2021). Security Configuration Checklist For FileZilla 3.*

**First Anomaly**

To safeguard our network, deploy ARP monitoring tools. These utilities can alert us when there's suspicious ARP action going on, allowing us to take protective measures before anything harmful happens. This will solve the vulnerability. *(IEEE, 2019)*

**Second Anomaly**

It is recommended to deploy a multi-layered security approach. This should involve network segmentation to isolate the anomalous traffic, leveraging anomaly-based intrusion detection systems for real-time network monitoring, and conducting digital forensic investigations to understand the nature and root cause of the anomalies. This will solve the vulnerability. *Cisco. (2018)*

**Third Anomaly**

To resolve the "STATUS\_ACCESS\_DENIED" issue, one straightforward action is to review the account's permissions and security settings in your system administration panel. Ensure that the account is not disabled and that it has the necessary permissions to access the shared resource. If the issue persists, consult the system logs for further diagnosis. This will solve the vulnerability. *Microsoft. (2021)*

**References**

*Cisco, 2018.*

*CISA, 2021.*

*IEEE, 2019.*

*Microsoft, 2021.*

*NIST, 2021.*

*NVD, n.d.*