

## PRACTICAL: 11

### AIM:

Wireshark is an open-source tool for profiling network traffic and analysing packets. It is often referred to as a network analyzer, network protocol analyzer, or sniffer. Wireshark intercepts traffic and converts that binary traffic into a human-readable format. Network administrators, Network security engineers, QA engineers, Developers, and other people who troubleshoot network problems, examine security problems, verify network applications, debug protocol implementations, and learn network protocol internals, respectively, can use it. A practical approach to study Wireshark from network security concept.

### THEORY:

Wireshark is a powerful, open-source network protocol analyzer that allows users to capture, analyze, and troubleshoot network traffic. It is a widely used tool in the field of cybersecurity, providing valuable insights into network activity and potential security threats.

Network security is a critical aspect of modern computing, as the increasing reliance on interconnected devices and networks has made organizations more vulnerable to various security threats. Understanding the fundamentals of network security is essential for effectively detecting and mitigating these threats.

#### Common Network Security Threats

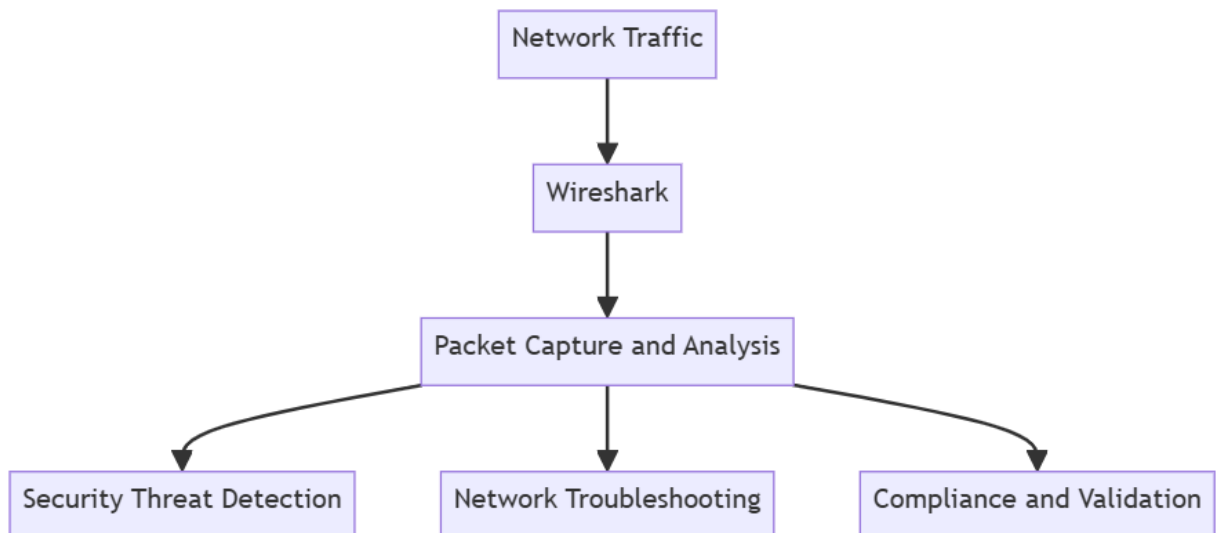
- Unauthorized access: Attackers attempting to gain unauthorized access to network resources or systems.
- Eavesdropping: Intercepting and monitoring network traffic to gather sensitive information.
- Denial-of-Service (DoS) attacks: Attempts to disrupt or overwhelm a network or system, rendering it unavailable to legitimate users.
- Malware propagation: The spread of malicious software, such as viruses, worms, or trojans, through the network.

Effective network monitoring and analysis are crucial for identifying and addressing security threats. By analyzing network traffic, security professionals can detect anomalies, identify potential vulnerabilities, and take appropriate actions to mitigate risks.

#### Wireshark's Role in Cybersecurity

Wireshark is a valuable tool for cybersecurity professionals, as it provides a comprehensive view of network activity, allowing them to:

- Identify and analyze network security incidents
- Detect and investigate suspicious network traffic
- Troubleshoot network issues and performance problems
- Validate the effectiveness of security controls and policies



By understanding the fundamentals of network security and mastering the use of Wireshark, cybersecurity professionals can effectively detect and respond to network security threats, ensuring the overall security and integrity of their organization's network infrastructure.

## CODE:

N/A

## OUTPUT:

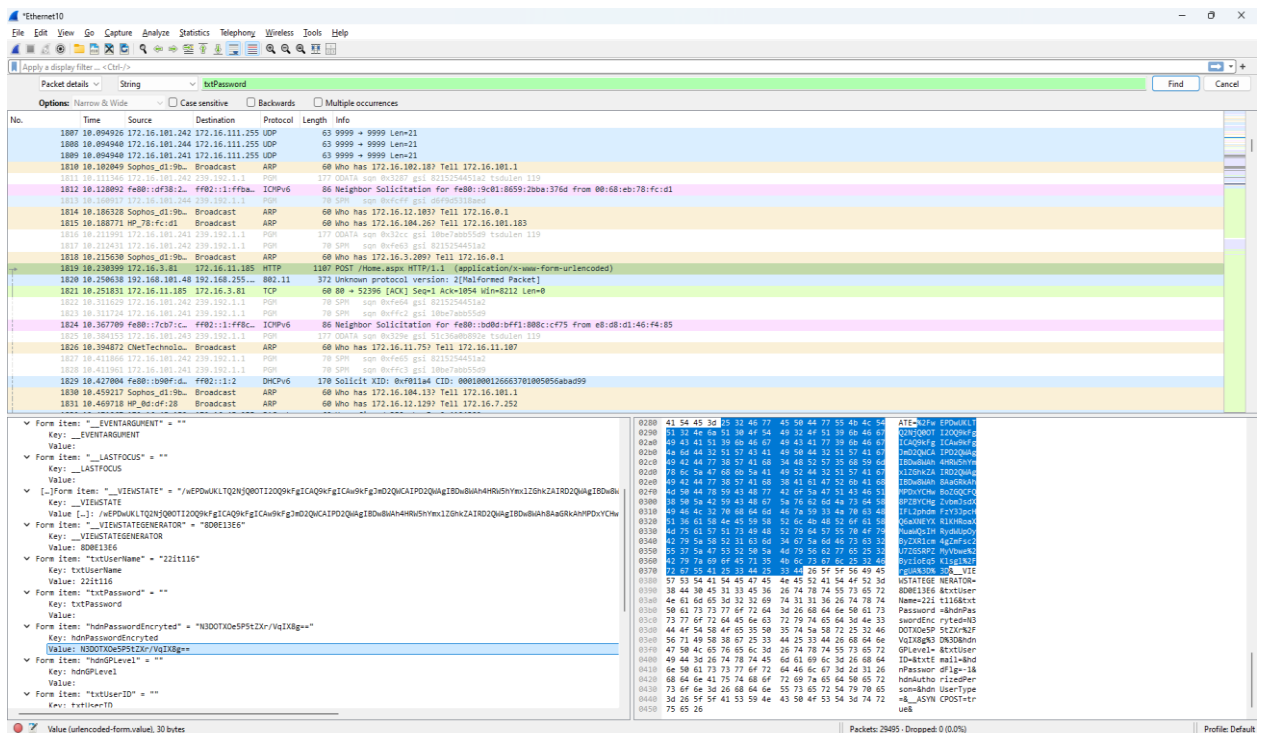


Figure 1: Getting Hash Value of E-Governance login password

```

encrypted_message = "N3D0TX0e5P5tZKv/VqIX8g==" # Replace with your actual encrypted message
decrypted_message = decrypt_message(encrypted_message, secret_key)
print("Decrypted message:", decrypted_message)

```

Collecting pycryptodome

Downloading pycryptodome-3.22.0-cp37-ab13-manylinux\_2\_17\_x86\_64.manylinux2014\_x86\_64.whl.metadata (3.4 kB)

Downloading pycryptodome-3.22.0-cp37-ab13-manylinux\_2\_17\_x86\_64.manylinux2014\_x86\_64.whl (2.3 MB)

2.3/2.3 MB 14.5 MB/s eta 0:00:00

Installing collected packages: pycryptodome

Successfully installed pycryptodome-3.22.0

Decrypted message: Egovernance@28

Figure 2: Decrypt the Hash Password

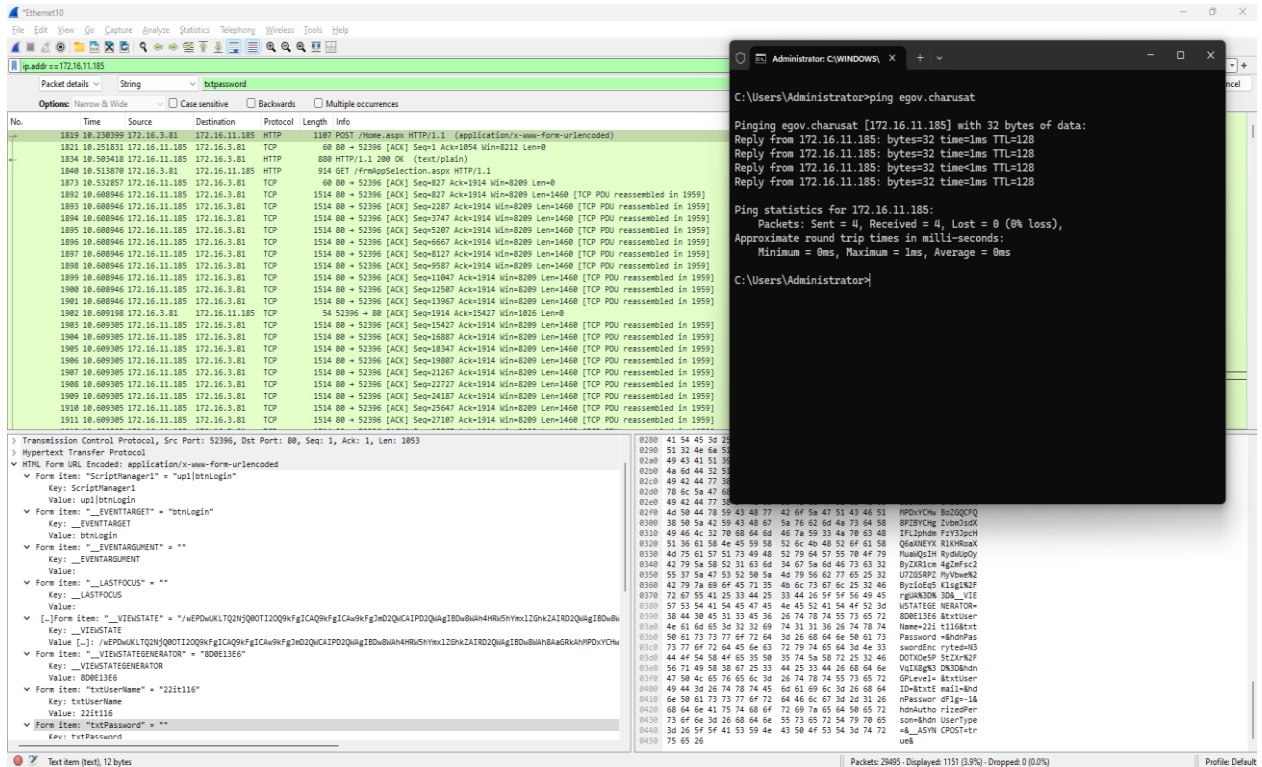


Figure 3: Flitter packet by IP address

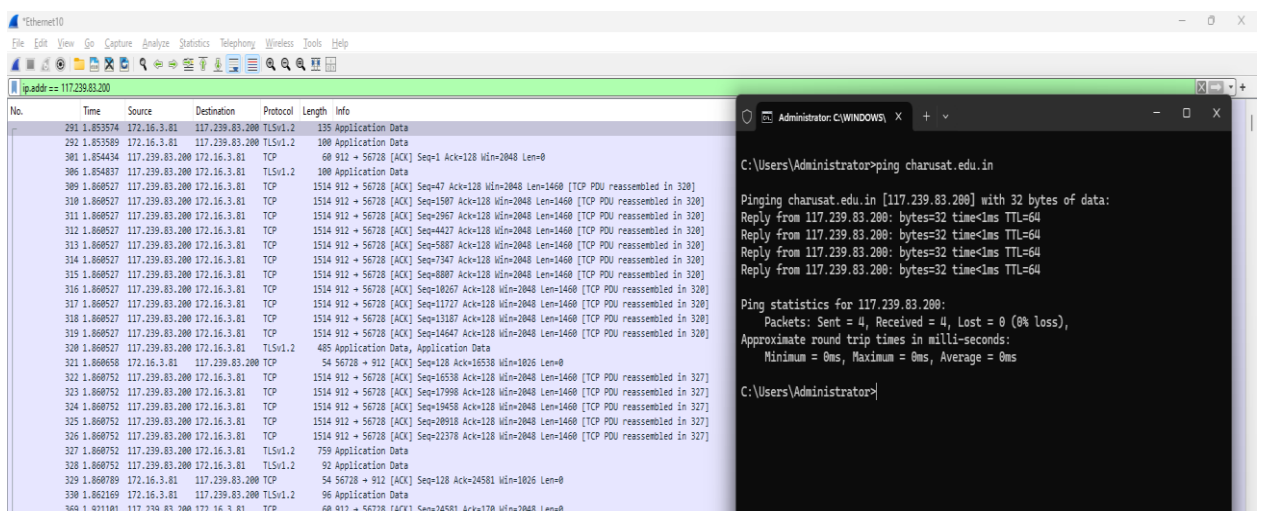


Figure 4: Check the Egovernance Host website IP and Apply filter for IP address

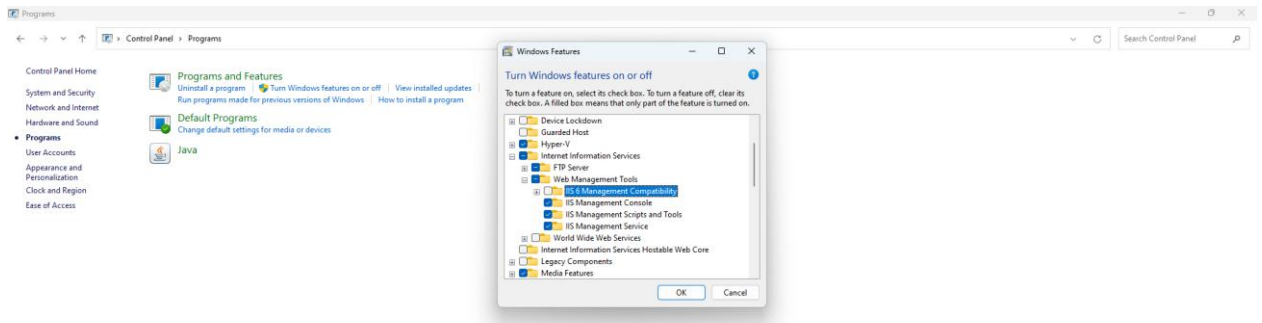


Figure 5: Open Windows Features and Check FTP service (Control Panel -> Programs -> Turn Windows features on or off -> FTP Services)

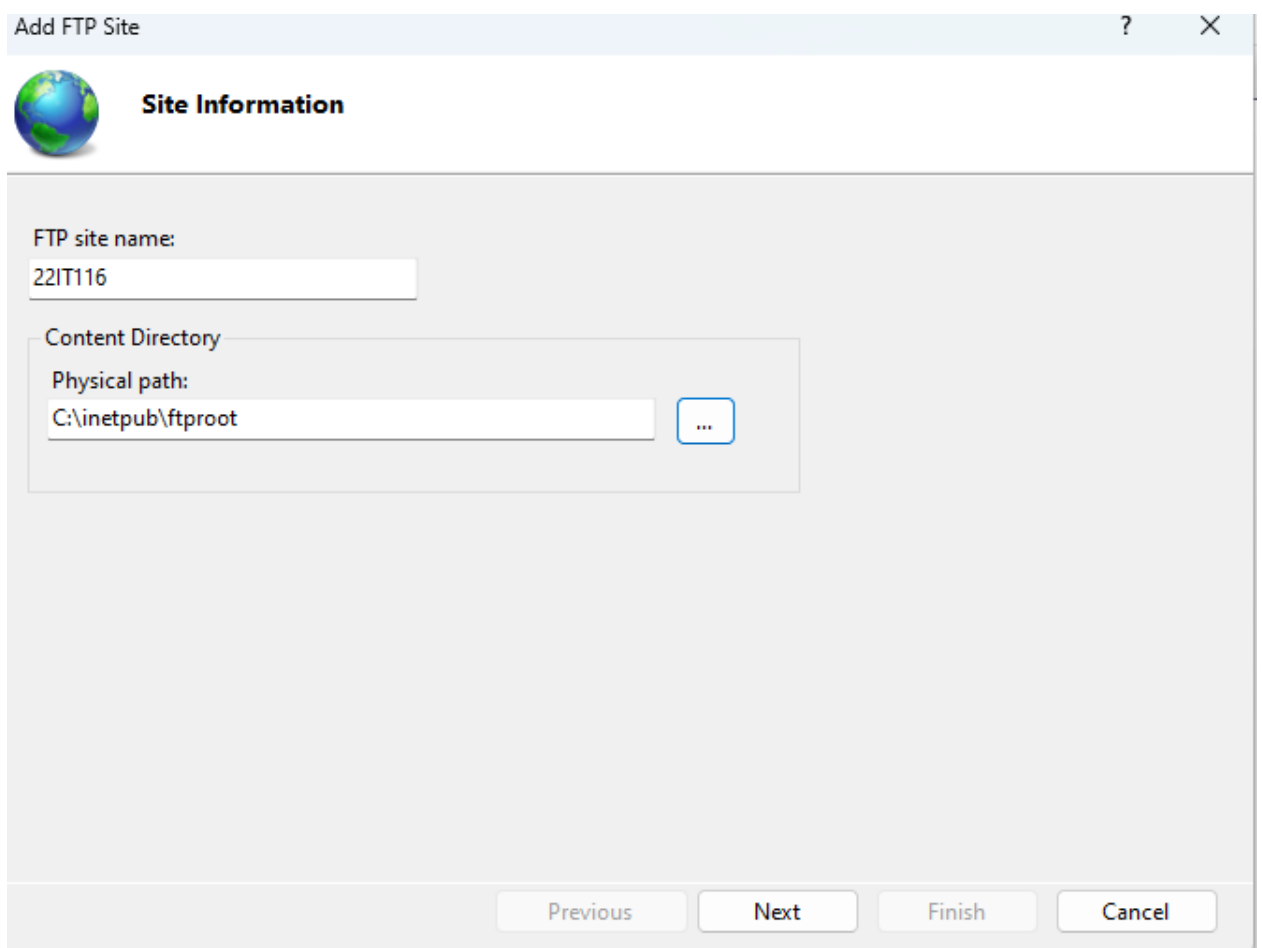
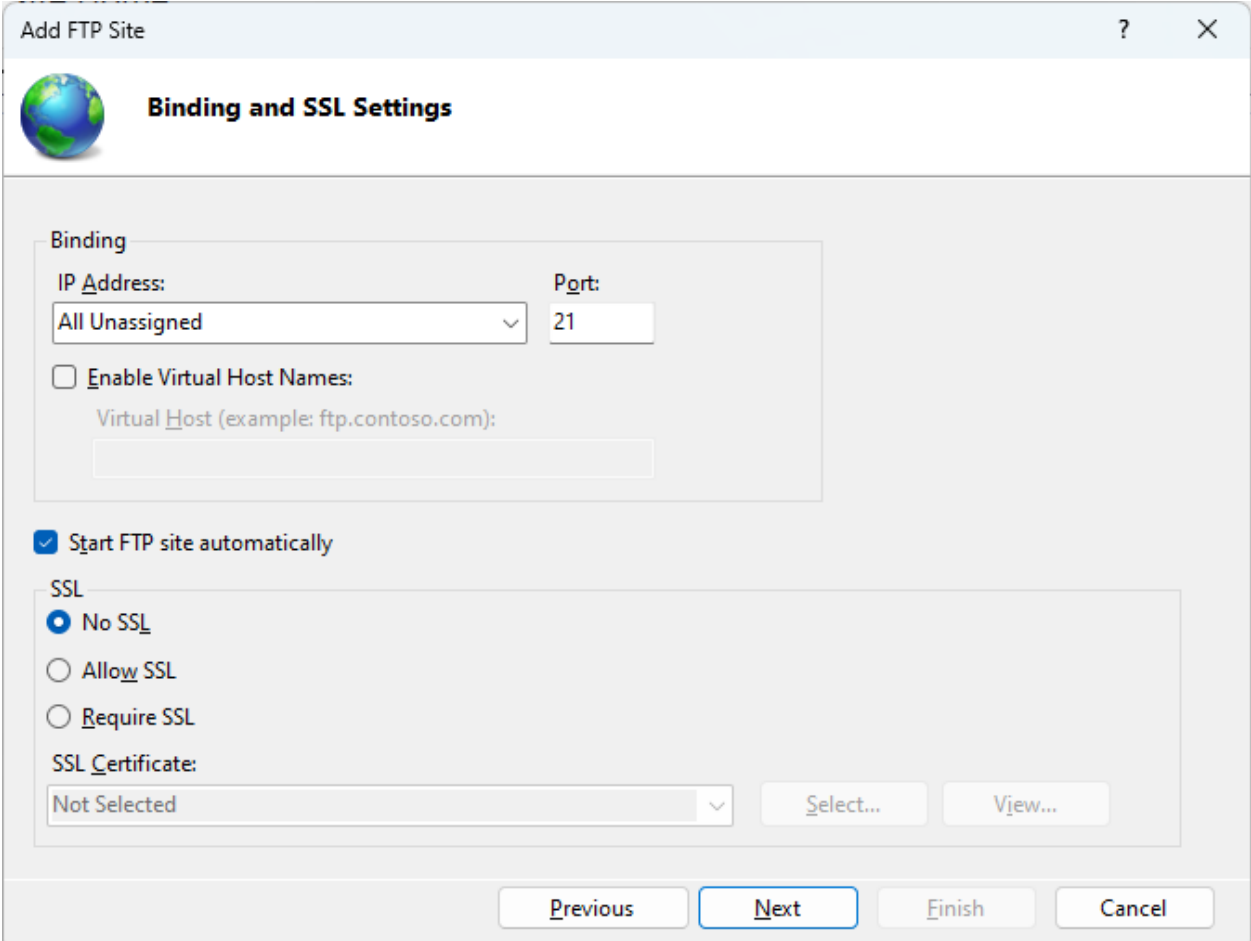


Figure 6: Enter a name for FTP site and specify the path to the folder that you want to use for FTP



The screenshot shows the 'Add FTP Site' wizard, specifically the 'Binding and SSL Settings' step. The window has a title bar with 'Add FTP Site', a help icon, and a close icon. Below the title bar is a header with a globe icon and the text 'Binding and SSL Settings'. The main content area is divided into two sections: 'Binding' and 'SSL'. In the 'Binding' section, there is a group box containing 'IP Address:' with a dropdown menu set to 'All Unassigned', 'Port:' with a text box containing '21', an unchecked checkbox for 'Enable Virtual Host Names:', and a text box for 'Virtual Host (example: ftp.contoso.com):'. Below this, there is a checked checkbox for 'Start FTP site automatically'. The 'SSL' section contains three radio buttons: 'No SSL' (selected), 'Allow SSL', and 'Require SSL'. Below these is an 'SSL Certificate:' dropdown menu set to 'Not Selected', and two buttons: 'Select...' and 'View...'. At the bottom of the window are four buttons: 'Previous', 'Next' (highlighted with a blue border), 'Finish', and 'Cancel'.

Add FTP Site

**Binding and SSL Settings**

Binding

IP Address: All Unassigned Port: 21

☐ Enable Virtual Host Names:

Virtual Host (example: ftp.contoso.com):

☒ Start FTP site automatically

SSL

☒ No SSL

☐ Allow SSL

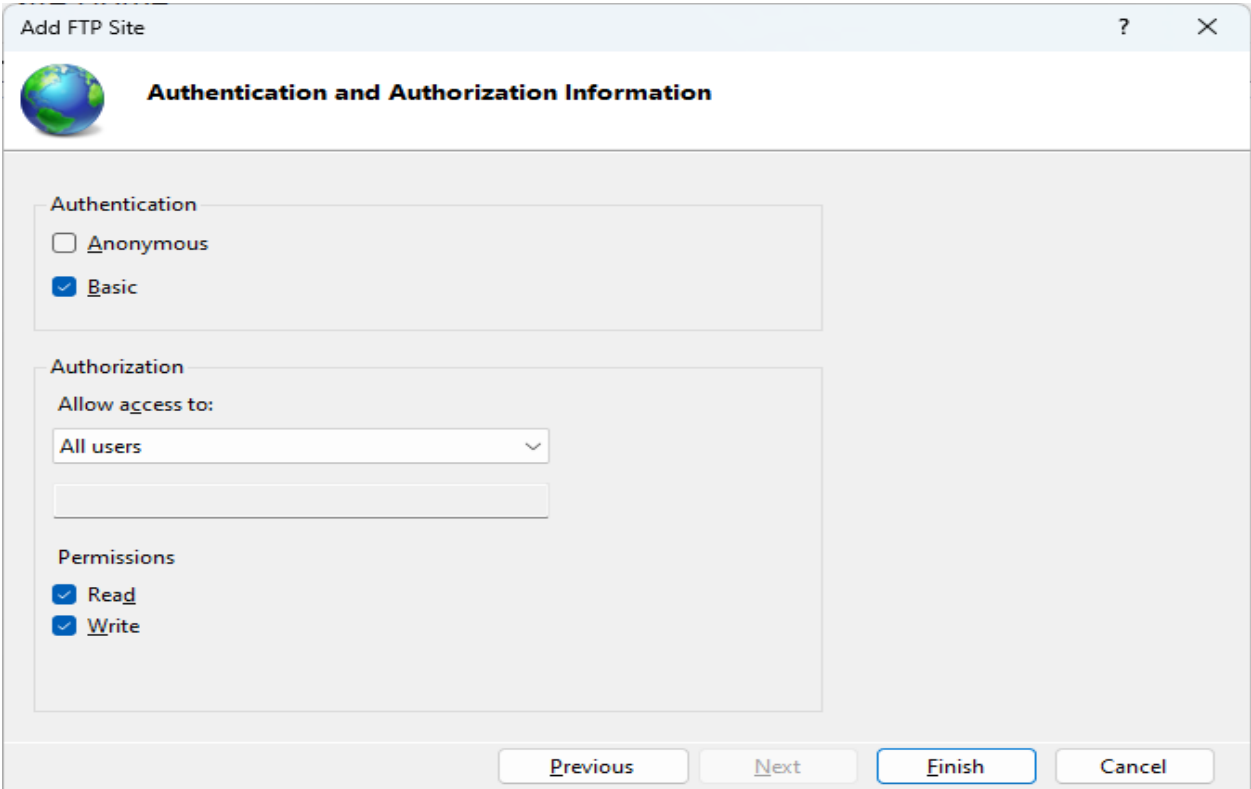
☐ Require SSL

SSL Certificate: Not Selected

Select... View...

Previous Next Finish Cancel

Figure 7: Configure Binding and SSL



The screenshot shows the 'Add FTP Site' wizard, specifically the 'Authentication and Authorization Information' step. The window has a title bar with 'Add FTP Site', a help icon, and a close icon. Below the title bar is a header with a globe icon and the text 'Authentication and Authorization Information'. The main content area is divided into three sections: 'Authentication', 'Authorization', and 'Permissions'. In the 'Authentication' section, there are two radio buttons: 'Anonymous' (unchecked) and 'Basic' (checked). In the 'Authorization' section, there is a group box containing 'Allow access to:' with a dropdown menu set to 'All users' and an empty text box below it. In the 'Permissions' section, there are two checked checkboxes: 'Read' and 'Write'. At the bottom of the window are four buttons: 'Previous', 'Next', 'Finish' (highlighted with a blue border), and 'Cancel'.

Add FTP Site

**Authentication and Authorization Information**

Authentication

☐ Anonymous

☒ Basic

Authorization

Allow access to: All users

Permissions

☒ Read

☒ Write

Previous Next Finish Cancel

Figure 8: Click Finish to create the FTP site and start it

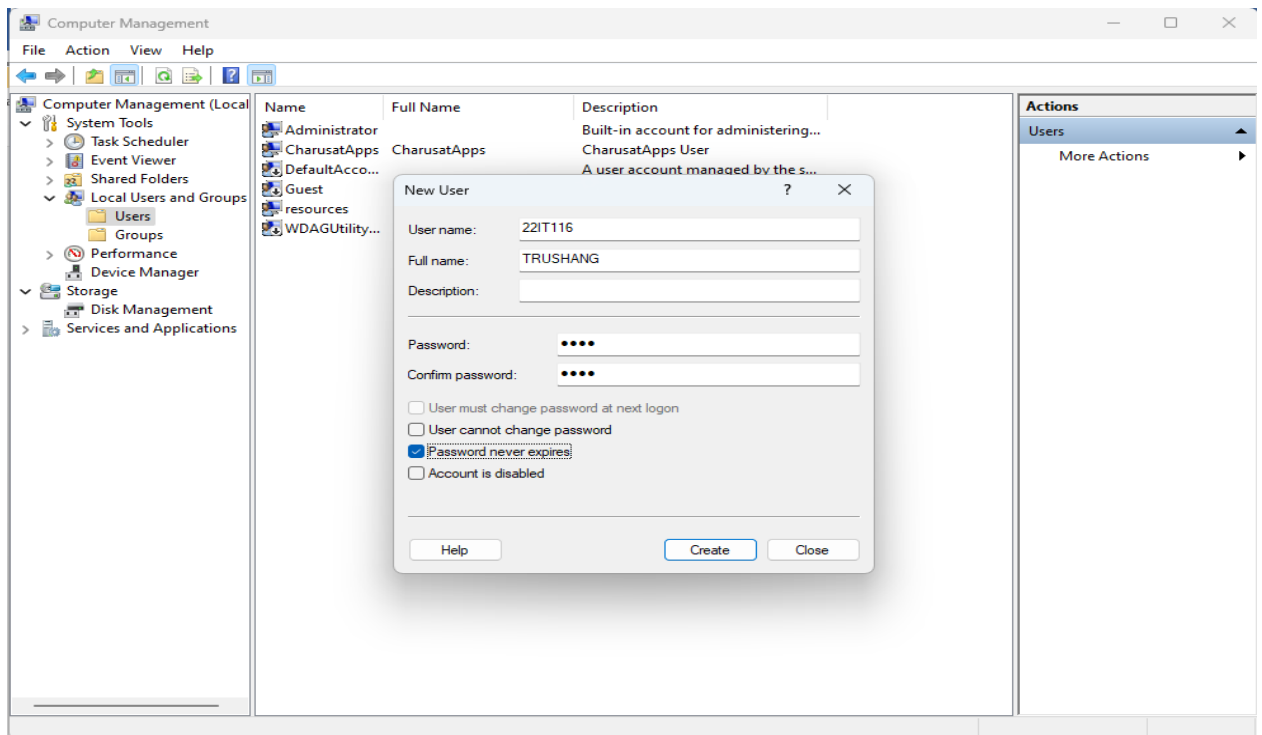


Figure 9: Create a user in computer management (Computer management ->Local Users & Groups -> User-> New User)

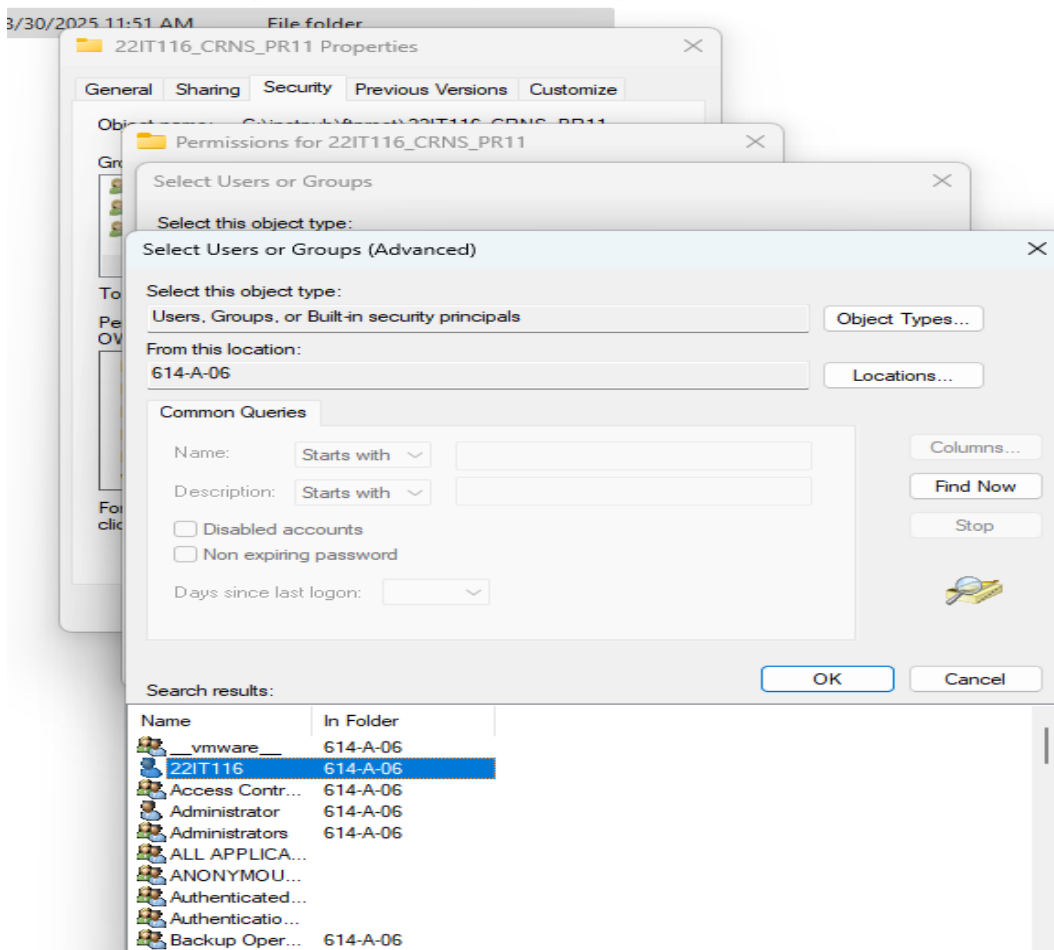


Figure 10: Create a folder and Give permission to user which created in previous step

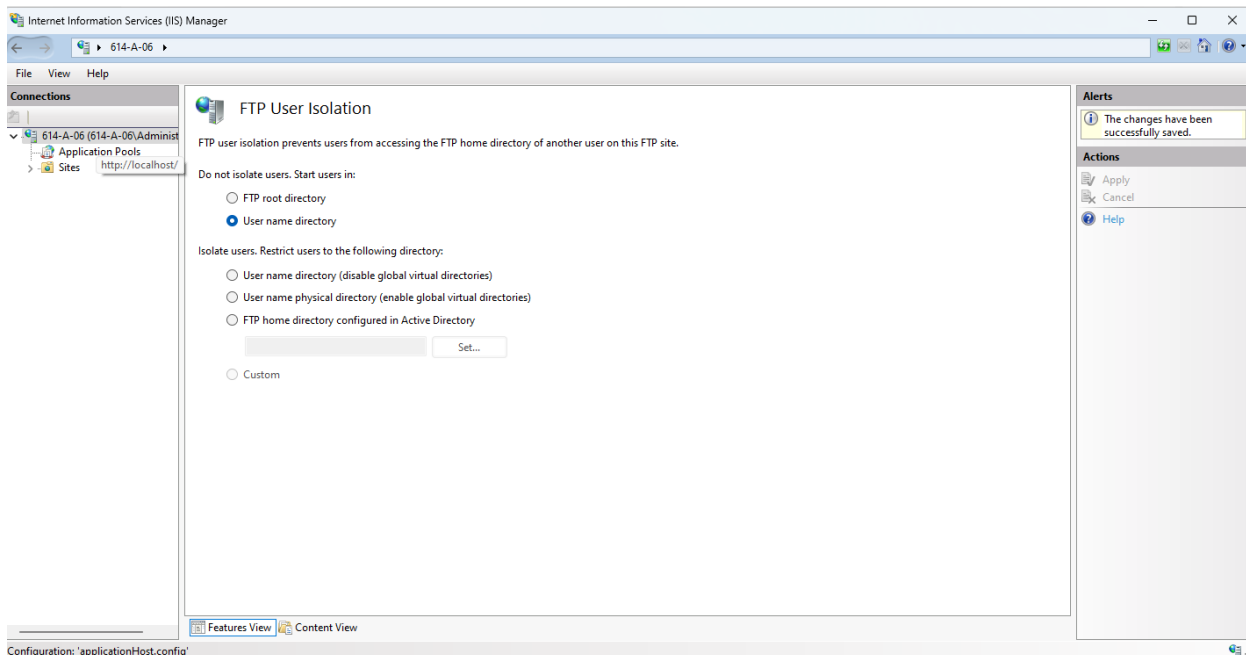


Figure 11: Enable FTP server rule

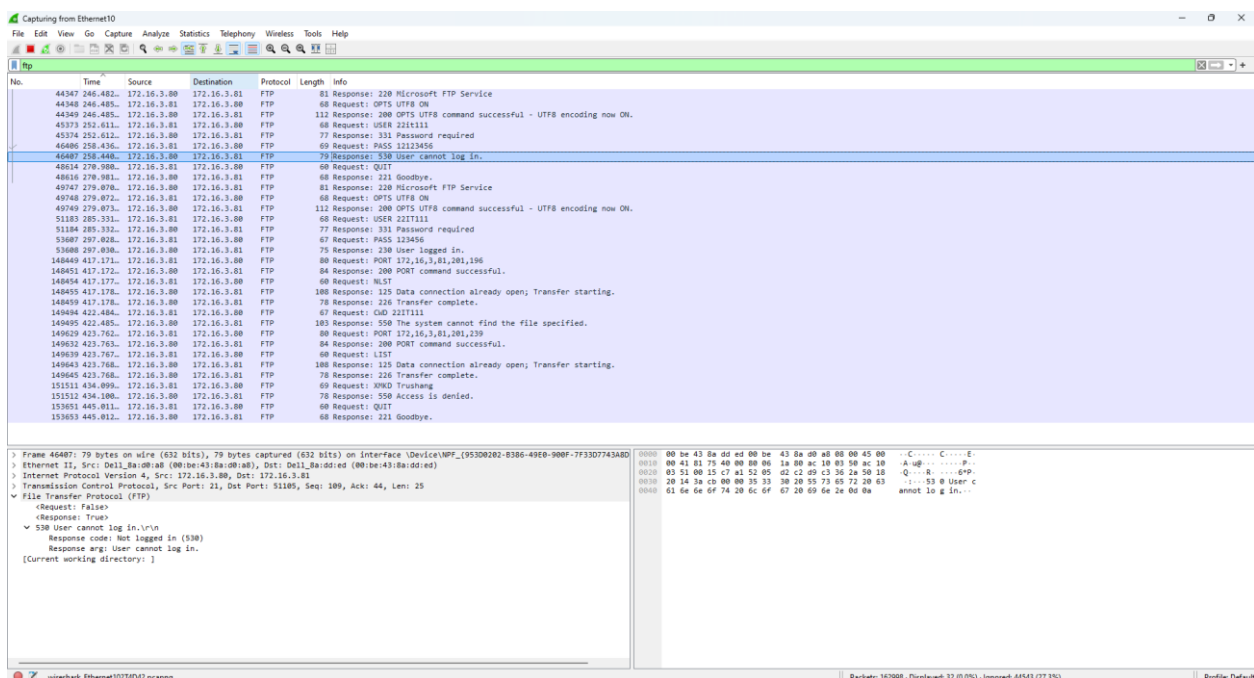


Figure 12: Get Password of FTP using Wireshark



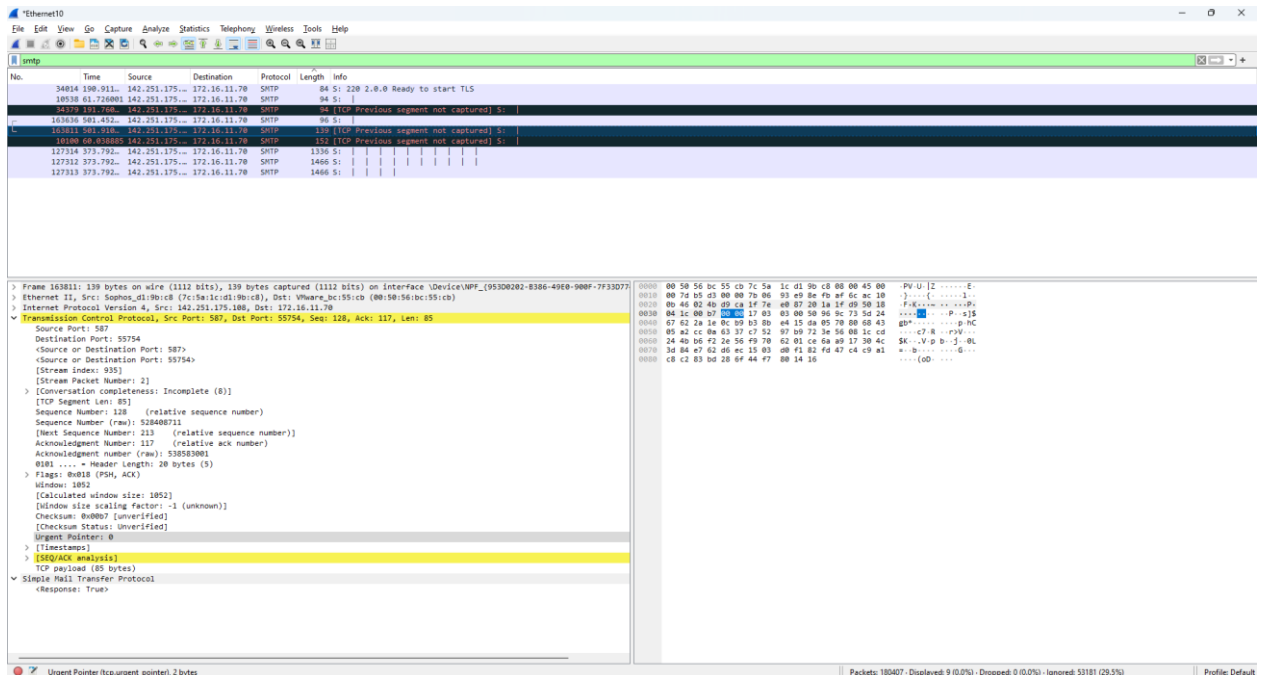


Figure 13: Check SMTP packet in Wireshark

## LATEST APPLICATIONS:

- Advanced Network Traffic Analysis:
- Intrusion Detection and Prevention:
- Malware Analysis:
- Network Forensics:
- Vulnerability Analysis
- Security Monitoring and Incident Response

## LEARNING OUTCOME:

In this practical, I learned how to utilize Wireshark, a network protocol analyzer, to capture and analyze network traffic. By observing packets transmitted over the network, I gained insights into the behavior of various protocols such as HTTP, TCP, and FTP. This hands-on experience enhanced my understanding of network operations and the importance of monitoring for security purposes.

## REFERENCES:

1. YouTube : <https://www.youtube.com/watch?v=yC0e0bSSleo>
2. WireShark : [https://www.wireshark.org/docs/wsug\\_html\\_chunked/](https://www.wireshark.org/docs/wsug_html_chunked/)
3. ChatGPT: <https://chatgpt.com/>