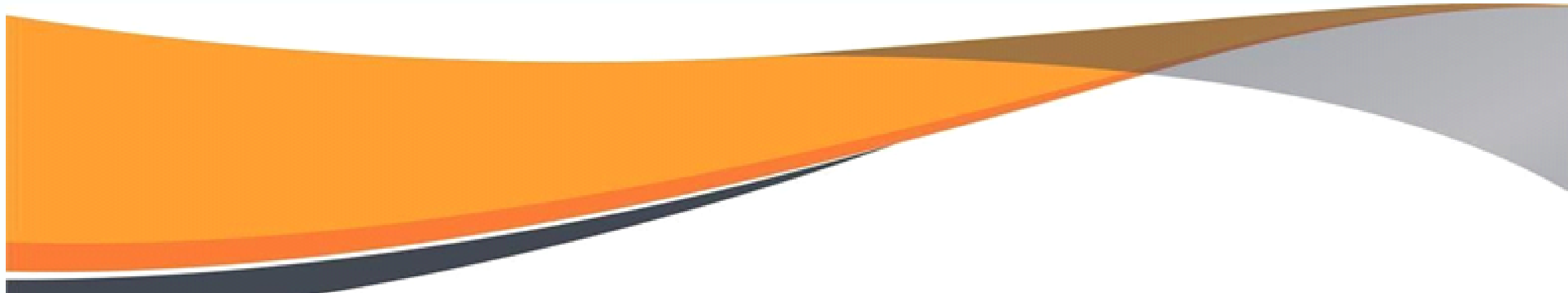


# OSI Layer Packet Simulation using Wireshark

Presented by  
**Ritika Sharma 2023a7r002**



Model Institute of Engineering & Technology (Autonomous)  
(Permanently Affiliated to the University of Jammu, Accredited by NAAC with “A” Grade)  
Jammu, India 2024



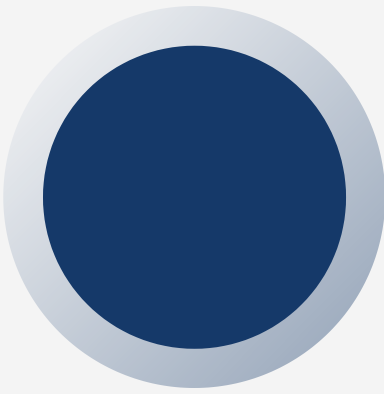
# Mini Project: OSI Layer Packet Simulation using Wireshark

This project aims to capture, analyze, and map network packets to the OSI model layers using Wireshark. By generating controlled traffic (e.g., TCP, HTTP, ICMP), we will:

- Observe encapsulation (how data is wrapped layer-by-layer).
- Identify protocol-specific headers (e.g., MAC/IP addresses, TCP ports, HTTP methods).
- Create a reference guide for troubleshooting real-world networks.

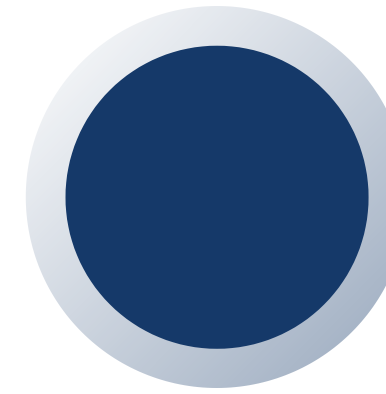
**Key Topics:** OSI Model, Packet Structure, Application Layer Protocols

**Tools used:** 2 VMs , Wireshark, Netcat



# Setup & Tools Required

- Wireshark (Packet capture & analysis)
- Netcat (nc) (Generate Layer 4 traffic)
- Telnet/HTTP (Generate Layer 7 traffic)
- Ping (ICMP) (Layer 3 example)
- ARP (arping) (Layer 2 example)



# VMs used

1. Kali Linux is used for:  
(Attacker machine)  
Generating traffic (arping, ping, nc, curl, dig).  
Running Wireshark for analysis.
2. Windows is used for: (target machine)  
Acting as the target for TCP connections.

# OSI

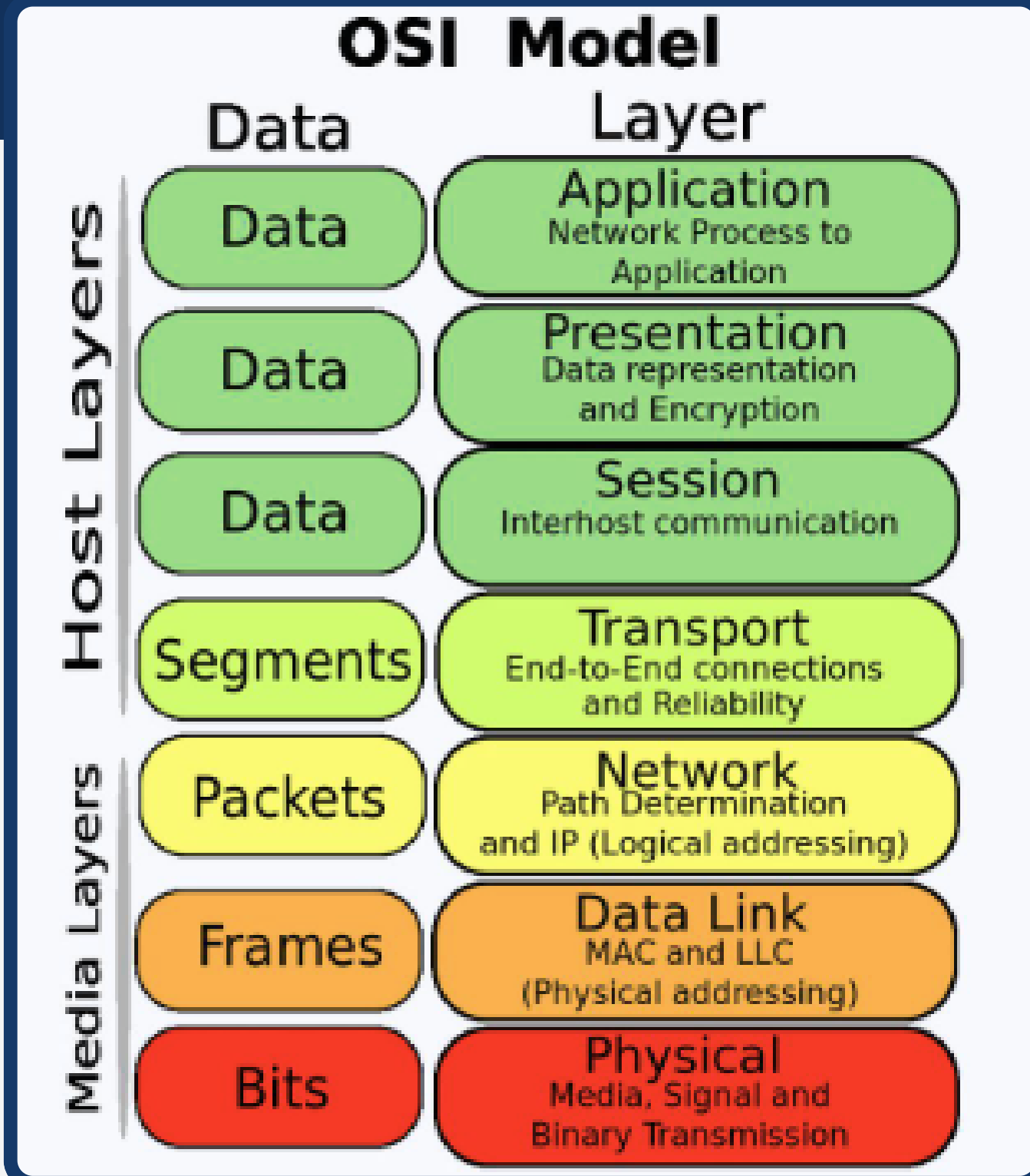
- It's a conceptual framework for how computers communicate over network.
- Developed by the International Organization for Standardization (ISO).
- Divides network communication into seven distinct layers.

OSI Layer	Layer Name	Key Protocols	Tool/Command (Capture / Generate Traffic)
7	Application	HTTP, DNS, FTP, SSH	curl <a href="http://example.com">http://example.com</a> , dig example.com
6	Presentation	SSL/TLS, JPEG, MPEG	(Part of HTTP/HTTPS, captured in Wireshark)
5	Session	NetBIOS, RPC	(Automatically handled in TCP/UDP)
4	Transport	TCP, UDP	nc -lvnp 4444 (Netcat for TCP)
3	Network	IP, ICMP, ARP	ping google.com,
2	Data Link	Ethernet, MAC, VLAN	arping (for MAC), Wireshark (Ethernet frames)
1	Physical	Cables, Hubs, Signals	(Not captured in software; hardware-dependent)



# OSI

- It's a conceptual framework for how computers communicate over a network.
- Developed by the International Organization for Standardization (ISO).
- Divides network communication into seven distinct layers.



- **Application Layer (Layer 7)**
- **Presentation Layer (Layer 6)**
- **Session Layer (Layer 5)**
- **Transport Layer (Layer 4)**
- **Network Layer (Layer 3)**
- **Data Link Layer (Layer 2)**
- **Physical Layer (Layer 1)**

## OSI Model



## Function

Its primary function is to provide network services directly to the end-user applications.

## Protocols

- HTTP (Hypertext Transfer Protocol)
- HTTPS (Hypertext Transfer Protocol Secure)
- DNS (Domain Name System)
- FTP (File Transfer Protocol)
- SFTP (SSH File Transfer Protocol)
- SCP (Secure Copy Protocol)
- SSH (Secure Shell)
- SMTP (Simple Mail Transfer Protocol)
- POP3 (Post Office Protocol version 3)
- IMAP (Internet Message Access Protocol)
- DHCP (Dynamic Host Configuration Protocol)
- SNMP (Simple Network Management Protocol)

# APPLICATION LAYER

The Application Layer (Layer 7) of the OSI model is the topmost layer, and it's the one that interacts directly with user applications and provides network services to them.