# Industry Problems

**1. Employee Website Monitoring using Packet Analysis**

This project understands and demonstrates the technique which can be used to monitor the websites accessed by employees based on IP and mac-address on a LAN network by analyzing appropriate packets. Wireshark is combined with port mirroring feature on a switch to achieve the solution

Deliverable:

1. Network Topology
2. Understanding Port Mirroring
3. Wireshark capture with Port mirroring configuration on Cisco switches
4. Wireshark screenshot of websites monitored by employees on the LAN network
5. Wireshark screenshot of websites monitored by employees on the LAN network based on IP address.
6. Wireshark screenshot of websites monitored by employees on the LAN network based on mac-address.

**2. Web Server monitoring techniques**

An organization has deployed a Windows based web server on its network. The network administrator has to identify the appropriate techniques for analyzing the below parameters.

1.TCP traffic (Incoming TCP Syn requests, TCP reset connections, TCP established connections, TCP half open connections)
2.Technique to monitor specific application requests on Web server
3.Technique to monitor HTTP Get requests to on Web server
4.Server bandwidth
5.Port status of the web server

A combination of different types of tools like Wireshark, nmap, netstat is to be used with appropriate commands and filters identified for achieving the required output.

Deliverable:

1. Technique to monitor TCP SYN requests to the web server with wireshark output
2. Technique to monitor TCP reset connections sent to and from the Web Server with wireshark output
3. Technique to monitor established open connections on a Web Server with netstat output
4. Technique to monitor TCP half open connections on the Web Server with netstat output
5. Technique to monitor requests to a specific application on the Web server with wireshark output
6. Technique to monitor HTTP GET requests to the web server with wireshark output
7. Technique to monitor server bandwidth with netstat output
8. Technique to monitor the port status of a Web Server with nmap output

### 3. TCP Port Scanner

The project develops a TCP port scanner with Python and Scapy. The tool would analyze if a corresponding TCP port is open or closed on the destination.

### 4. Web Server fingerprinting tool

The scope of the project is to develop a program , which would fingerprint a web server based on the banner. For this purpose, the FTP service on the web server is leveraged.

FTP banner grabbing is performed on Web services like IIS and Apache and the type of web service is identified using the name returned by the FTP server banners.