Semana acadêmica dos cursos de TI: Analisando tráfego de rede com Wireshark para identificar padrões.

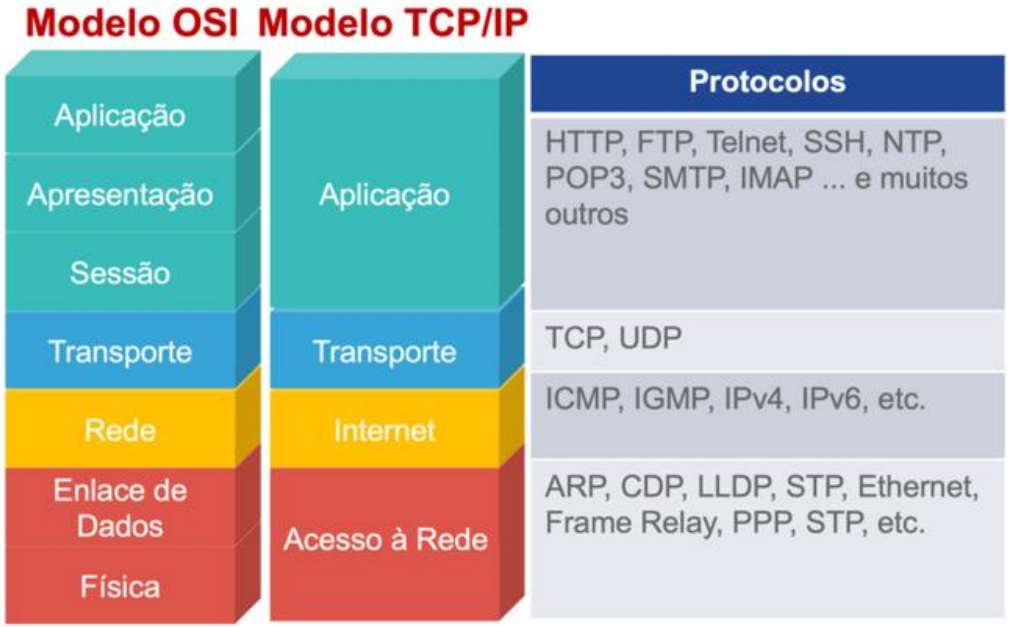
Professor: Ranyelson Neres Carvalho

Objetivo

- Capacitar os participantes a utilizarem o **Wireshark** para capturar, analisar e interpretar padrões de tráfego de rede, identificando possíveis anomalias e comportamentos suspeitos. A oficina abordará desde os conceitos básicos de redes até técnicas mais utilizadas para análise de tráfego.

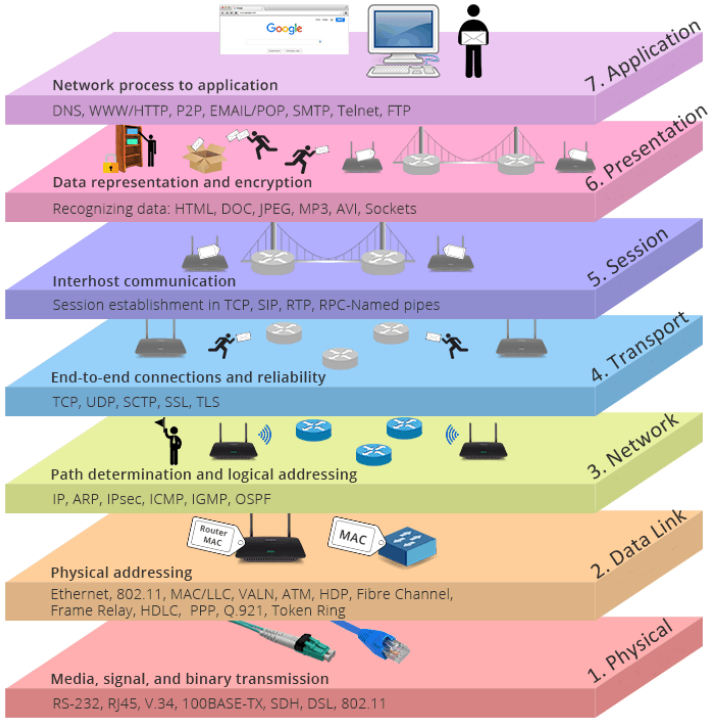
Conceitos fundamentais de redes

- **Modelo OSI e TCP-IP:**



Conceitos fundamentais de redes

- **Modelo OSI e TCP-IP:**



Conceitos fundamentais de redes

- **Pacotes:**
  - São unidades de dados que são transmitidas pela rede. Eles contêm tanto os dados que estão sendo enviados quanto informações de controle, como endereços de origem e destino, e são usados para garantir que a mensagem chegue corretamente ao seu destino;
  - Pacote é dividido em cabeçalho e dados (payload).

- **Endereços IP:**
  - É um identificador numérico atribuído a cada dispositivo conectado a uma rede de computadores que utiliza o Protocolo de Internet para comunicação;
  - IPv4 e IPv6.

- **Portas:**
  - As portas são identificadores numéricos usados para direcionar o tráfego de rede entre diferentes serviços ou aplicações em um dispositivo;
  - Portas bem conhecidas (0-1023): Usadas para serviços padrão como HTTP (porta 80), HTTPS (porta 443) e FTP (porta 21);
  - Portas registradas (1024-49151): Geralmente associadas a serviços ou aplicações específicas;
  - Portas dinâmicas (49152-65535): Usadas temporariamente por aplicativos para a comunicação.

Conceitos fundamentais de redes

- **Cabeçalhos de um pacote TCP e UDP**

Cabeçalho UDP

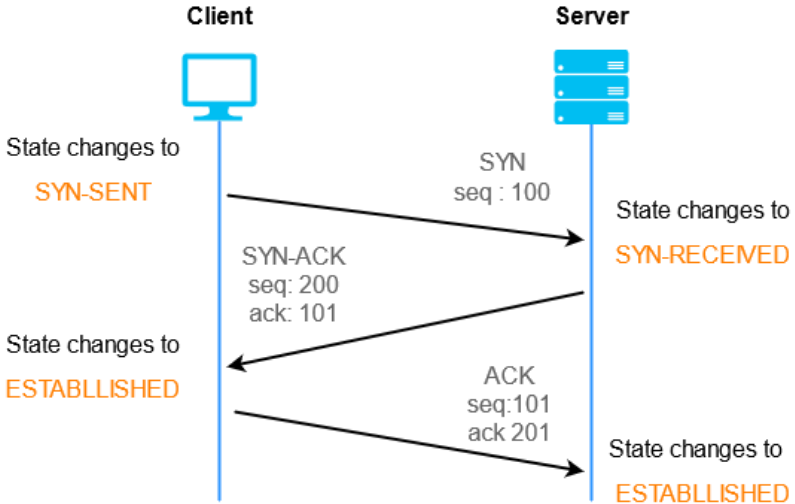
Número da porta de origem (16 bits)	Número da porta de destino (16 bits)
Comprimento total (16 bits)	Checksum (16 bits)

Cabeçalho do protocolo TCP

Endereço da porta de origem (16 bits)								Endereço da porta de destino (16 bits)
Número de Sequência (32 bits)								
Número de Confirmação (32 bits)								
HLEN (4 bits)	Reservado (6 bits)	URG	ACK	PSH	RST	SYN	FIN	Tamanho da janela (16 bits)
Checksum (16 bits)								Ponteiro de Urgência ou Urgent pointer (16 bits)
Opções e Preenchimento								

Conceitos fundamentais de redes

- **Three-Way Handshake (ou aperto de mão de três vias):**
- É o processo utilizado no Protocolo de Controle de Transmissão (TCP) para estabelecer uma conexão confiável entre dois dispositivos (cliente e servidor) na rede antes que os dados possam ser transmitidos.



Wireshark

- É uma ferramenta de código aberto amplamente utilizada para captura e análise de tráfego de rede. Ele permite que os usuários monitorem em tempo real o tráfego de uma rede local, capturando pacotes de dados que passam por interfaces de rede, como placas Ethernet ou Wi-Fi.
- Com o Wireshark, é possível inspecionar cada pacote capturado detalhadamente, verificando os cabeçalhos, protocolos e os dados transmitidos.