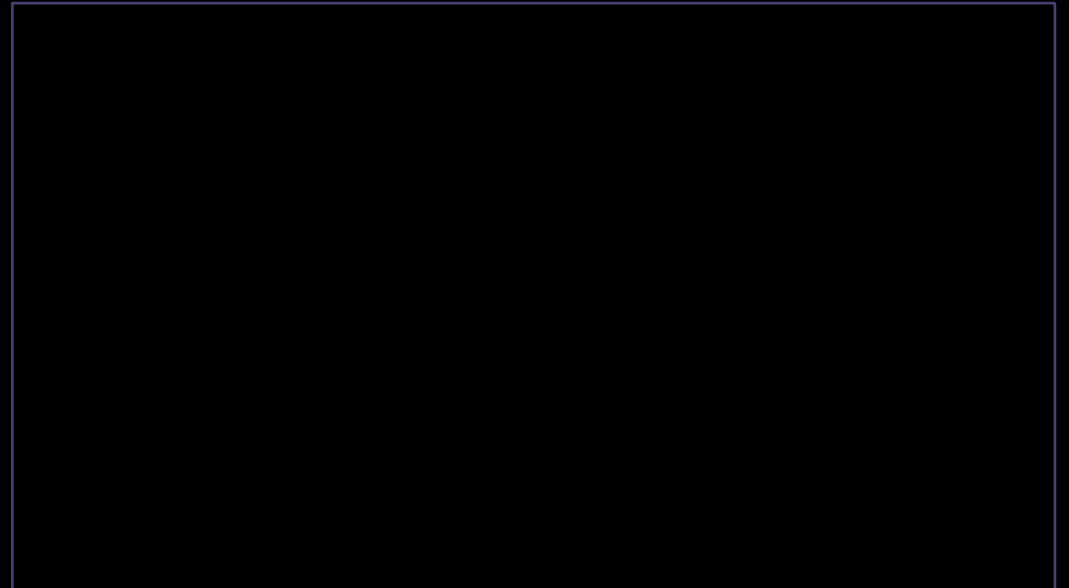




Prime

CCS-A

Entendendo os
Protocolos TCP/IP

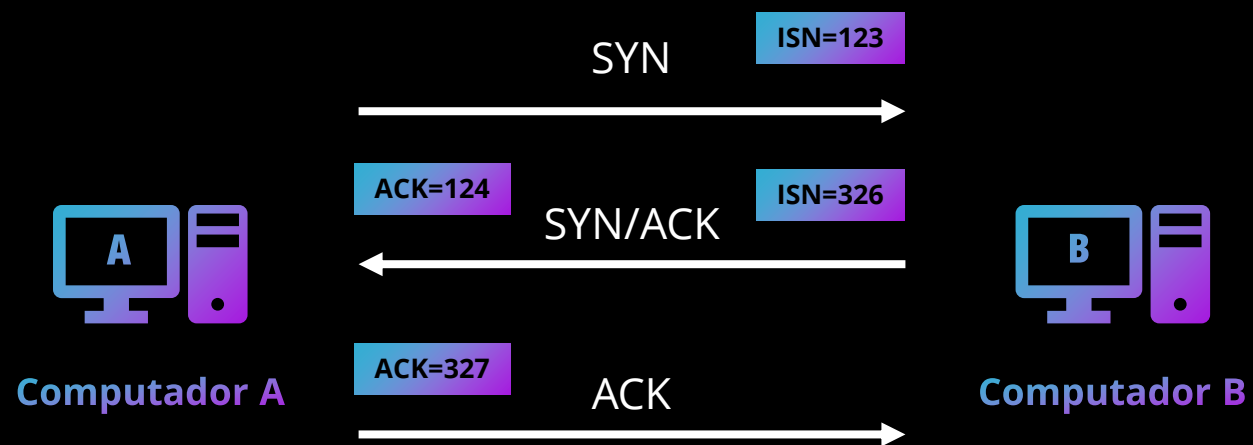


Protocolo de Controle de Transmissão (TCP)

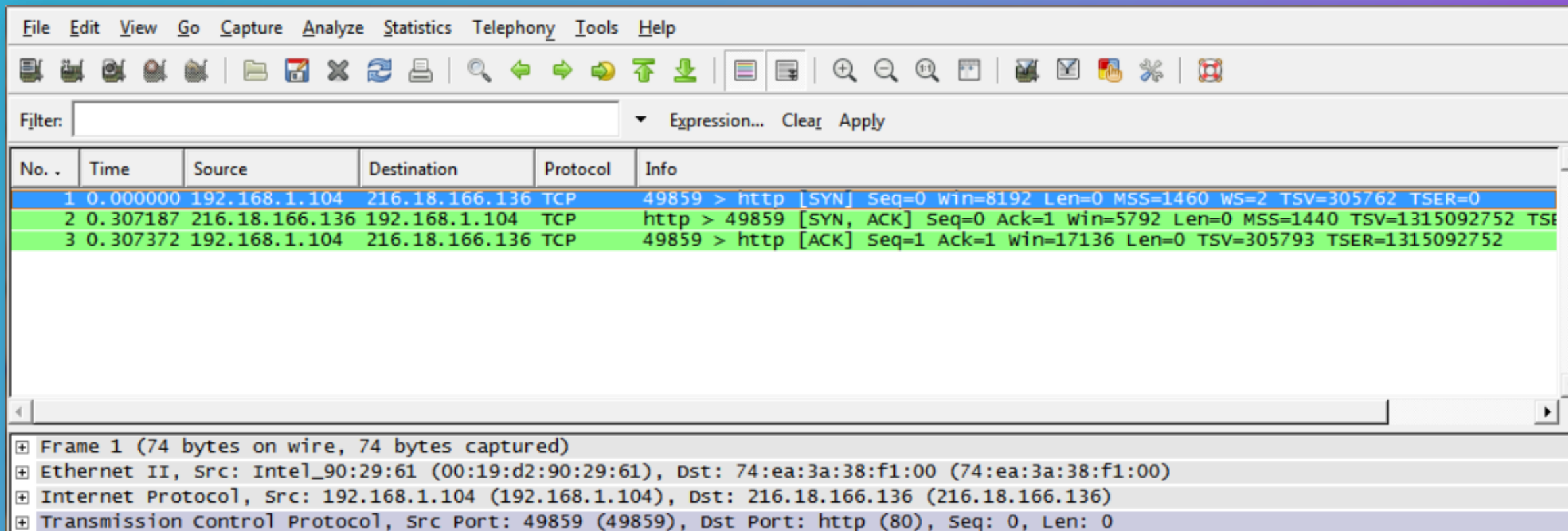
- Comunicação orientada à conexão e garante a entrega confiável.
- Retransmite quaisquer dados perdidos ou corrompidos.
- Necessário em aplicativos que precisam de transporte confiável.
- Exige confirmação do recebimento dos dados.
 - ▶ ACKs Acknowledgement (Reconhecimento);
 - ▶ Gerando sobrecarga, diferente do UDP;
 - ▶ Mas garantindo entrega.
- Utiliza números de sequência e números de confirmação.
 - ▶ Número de sequência - Número atribuído a cada parte dos dados enviados;
 - ▶ Número de confirmação - Número de sequência original da mensagem da resposta.



Handshake de Três Vias TCP



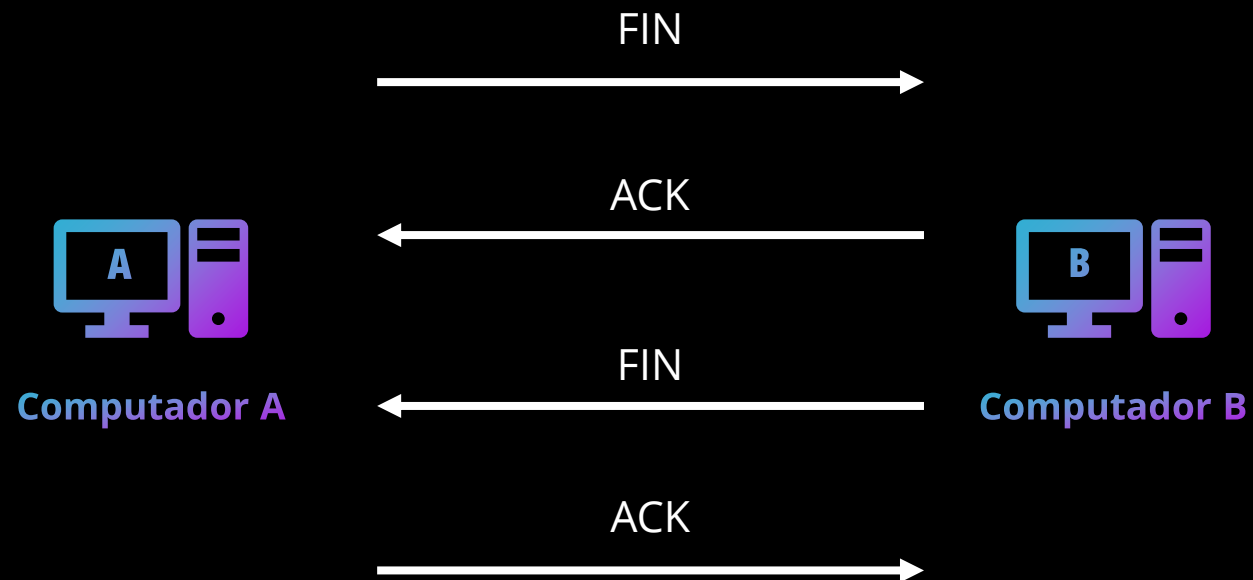
Three Way Handshake Wireshark



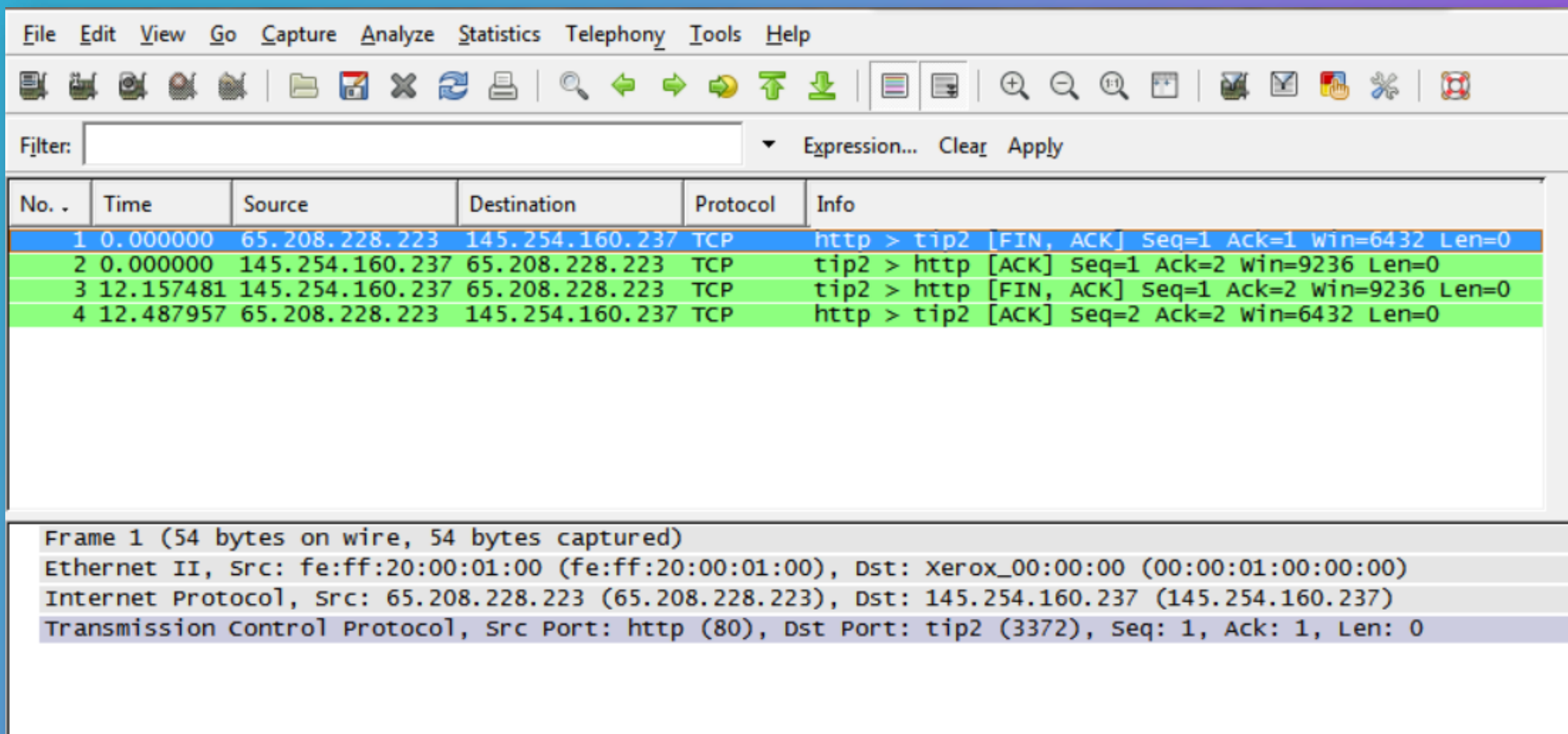
No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.104	216.18.166.136	TCP	49859 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=2 TSV=305762 TSER=0
2	0.307187	216.18.166.136	192.168.1.104	TCP	http > 49859 [SYN, ACK] Seq=0 Ack=1 win=5792 Len=0 MSS=1440 TSV=1315092752 TSER=0
3	0.307372	192.168.1.104	216.18.166.136	TCP	49859 > http [ACK] Seq=1 Ack=1 win=17136 Len=0 TSV=305793 TSER=1315092752

Frame 1 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: Intel_90:29:61 (00:19:d2:90:29:61), Dst: 74:ea:3a:38:f1:00 (74:ea:3a:38:f1:00)
Internet Protocol, Src: 192.168.1.104 (192.168.1.104), Dst: 216.18.166.136 (216.18.166.136)
Transmission Control Protocol, Src Port: 49859 (49859), Dst Port: http (80), Seq: 0, Len: 0

Desconectando-se (educadamente) de uma Sessão TCP



Finalizando Conexão Wireshark



File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: Expression... Clear Apply

No. .	Time	Source	Destination	Protocol	Info
1	0.000000	65.208.228.223	145.254.160.237	TCP	http > tip2 [FIN, ACK] Seq=1 Ack=1 win=6432 Len=0
2	0.000000	145.254.160.237	65.208.228.223	TCP	tip2 > http [ACK] Seq=1 Ack=2 win=9236 Len=0
3	12.157481	145.254.160.237	65.208.228.223	TCP	tip2 > http [FIN, ACK] Seq=1 Ack=2 win=9236 Len=0
4	12.487957	65.208.228.223	145.254.160.237	TCP	http > tip2 [ACK] Seq=2 Ack=2 win=6432 Len=0

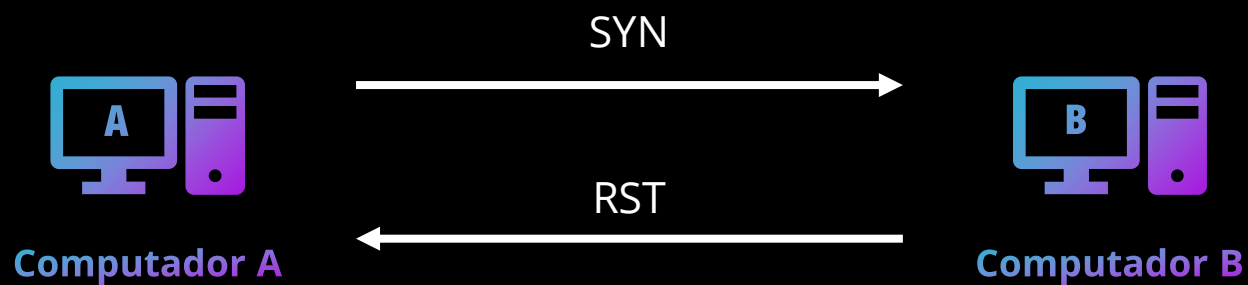
Frame 1 (54 bytes on wire, 54 bytes captured)

Ethernet II, Src: fe:ff:20:00:01:00 (fe:ff:20:00:01:00), Dst: xerox_00:00:00 (00:00:01:00:00:00)

Internet Protocol, Src: 65.208.228.223 (65.208.228.223), Dst: 145.254.160.237 (145.254.160.237)

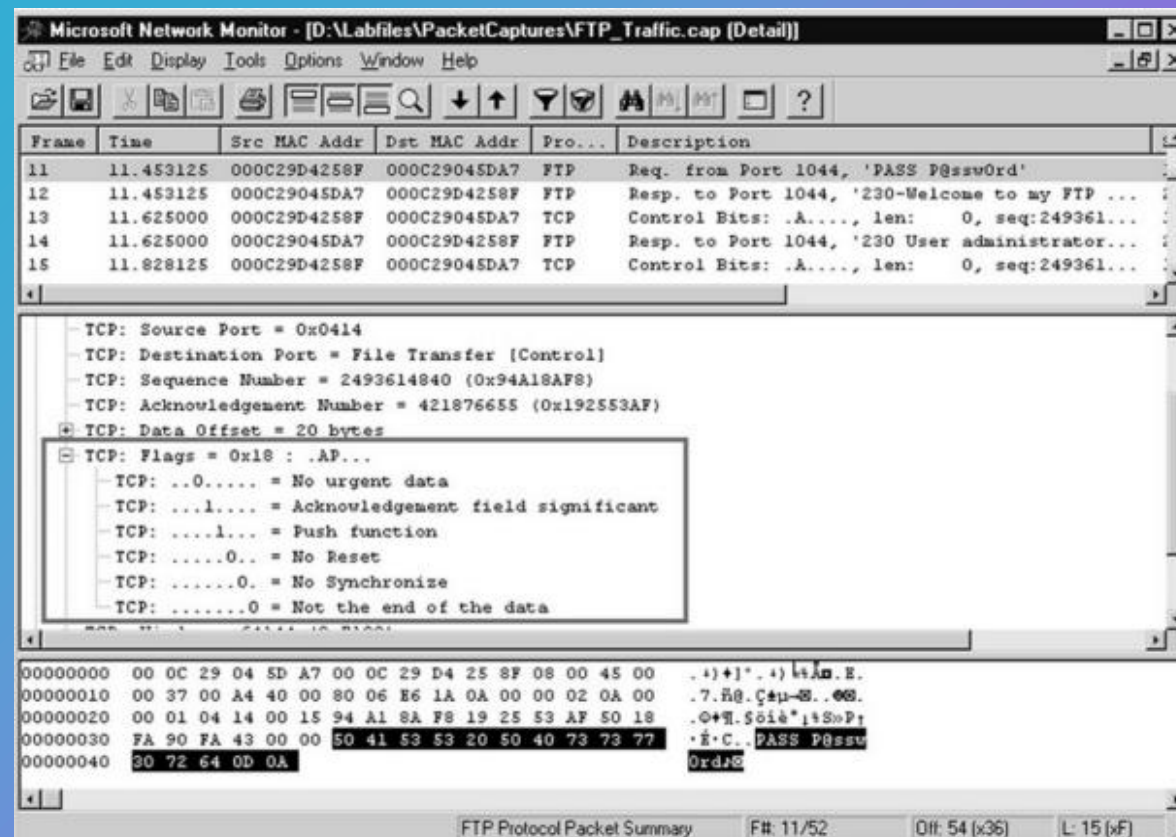
Transmission Control Protocol, Src Port: http (80), Dst Port: tip2 (3372), Seq: 1, Ack: 1, Len: 0

Desconectando-se (indelicadamente) de uma Sessão TCP



Sinalizadores TCP

- ▶ SYN;
- ▶ ACK;
- ▶ PSH;
- ▶ URG;
- ▶ FIN;
- ▶ RST.



Portas TCP

— **Porta** - Endereço exclusivo atribuído ao aplicativo.

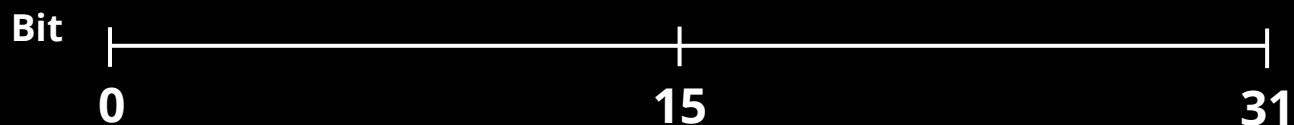
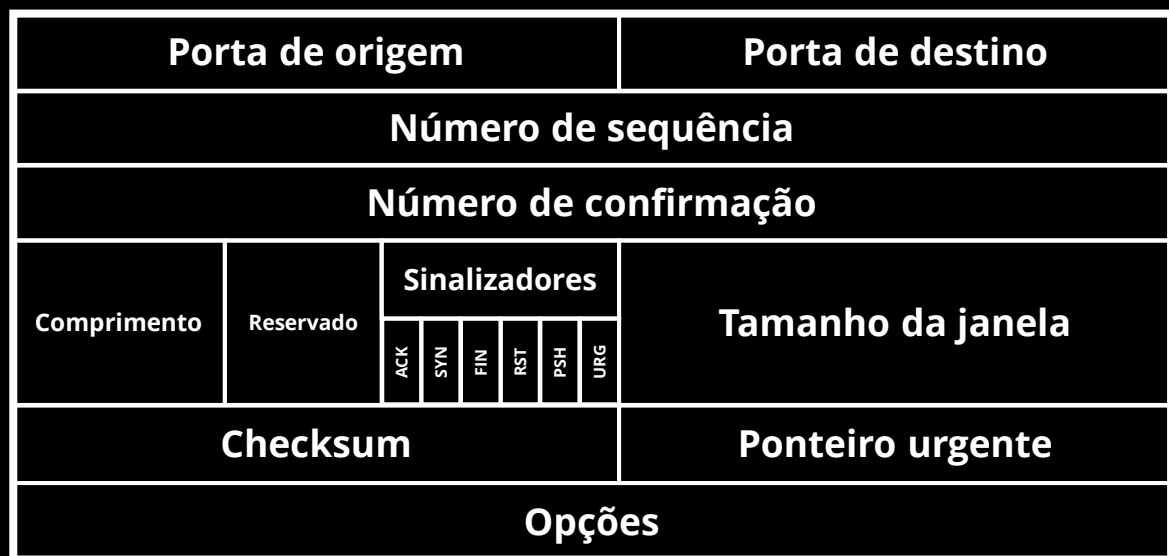
- ▶ **Porta 20 – FTP Data** - Porta para enviar dados para um cliente;
- ▶ **Porta 21 – FTP Control** - Porta que envia arquivos para um servidor;
- ▶ **Porta 22 – SSH** - Porta para criptografar comunicação de acesso remoto. É usado comumente como um substituto da Porta 23/Telnet;
- ▶ **Porta 23 – Telnet** - Porta usada para conectar de forma remota a um sistema, servidor ou roteador;
- ▶ **Porta 25 – SMTP** - Porta para enviar e-mail na Internet;

Portas TCP

— **Porta** - Endereço exclusivo atribuído ao aplicativo.

- ▶ **Porta 53 - DNS** - Porta para transferências de zona DNS;
- ▶ **Porta 80 - HTTP** - Protocolo de Internet para acessar sites da web via navegador.
- ▶ **Porta 110 - POP3** - Porta que é também o protocolo para ler e-mails;
- ▶ **Porta 139 - NetBIOS** - Porta utilizada para estabelecer uma conexão entre dois sistemas para comunicação NetBIOS;
- ▶ **Porta 143 - IMAP** - Porta usada via IMAP, um novo protocolo de Internet para ler e-mail;
- ▶ **Porta 443 - HTTPS** - Porta para tráfego seguro na web;
- ▶ **Porta 3389 - RDP** - Porta para administração remota de um sistema Windows.

Cabeçalho TCP



User Datagram Protocol (UDP)

— Usado por aplicativos que não se preocupam em garantir que os dados cheguem ao sistema de destino.



- ▶ **Porta 53 – DNS** - Consultas DNS;
- ▶ **Porta 67 e 68 – DHCP** - Serviço DHCP e solicitações de clientes;
- ▶ **Porta 69 – TFTP** - Download de arquivos sem solicitar autenticação;
- ▶ **Porta 137 e 138 – NetBIOS** - Serviço de nome e datagrama
- ▶ **Porta 161 – SNMP** - Protocolo Simples de Gerenciamento de Rede (SNMP).

Cabeçalho UDP

Porta de origem	Porta de destino
Comprimento	Checksum

Bit

0 15 31

Protocolo de Internet (IP)

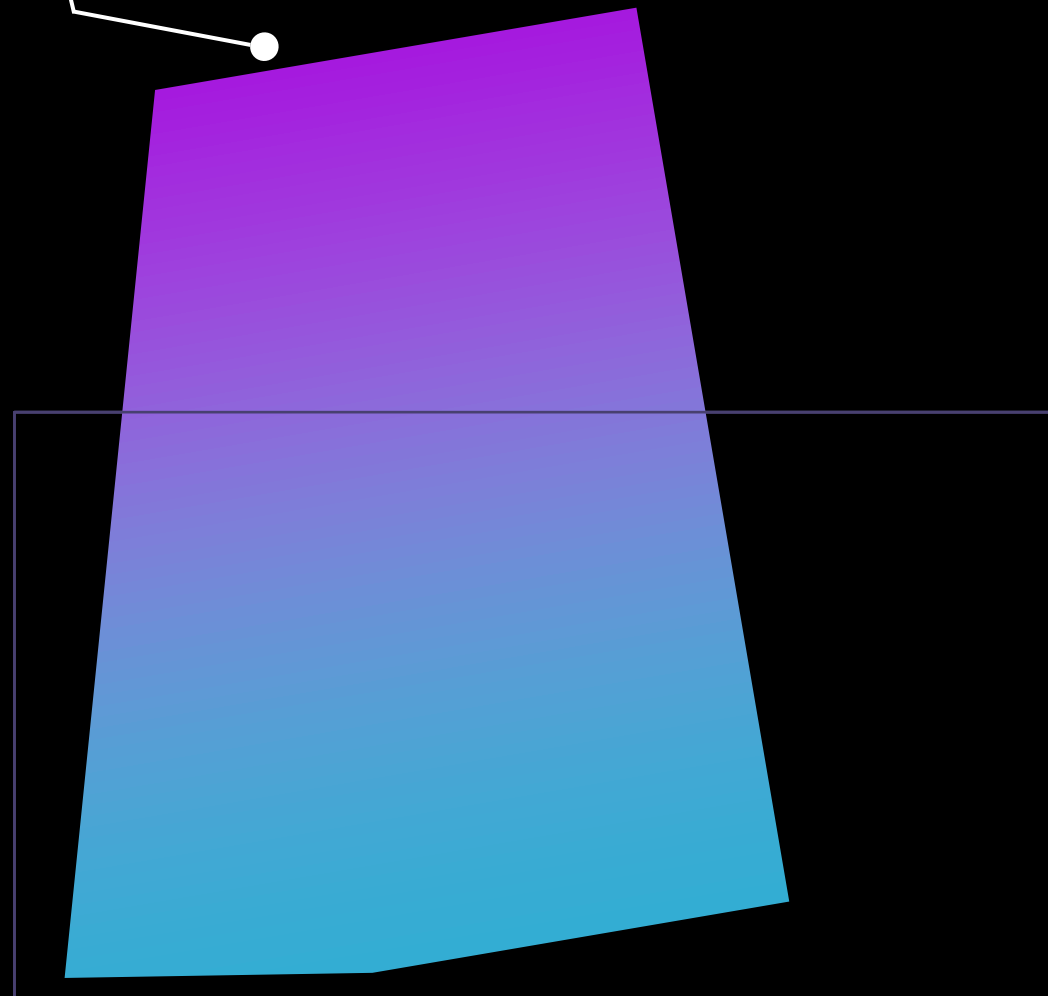


- ▶ Fornece entrega de pacotes para protocolos superiores no modelo.
- ▶ "Melhor esforço", ou seja, não confiável.
- ▶ Não garante a entrega;
- ▶ Simplesmente envia os dados.
- ▶ Endereçamento e roteamento lógico do TCP/IP.

Cabeçalho IP

Versão	Comprimento do cabeçalho	Tipo de serviço	Comprimento total	
Identificação			Sinalizadores de IP	Deslocamento de fragmento
Tempo de vida (TTL)	Protocolo		Checksum de cabeçalho	
Endereço de origem				
Endereço de destino				
Opções IP				

Bit 0 15 31



Internet Control Message Protocol (ICMP)

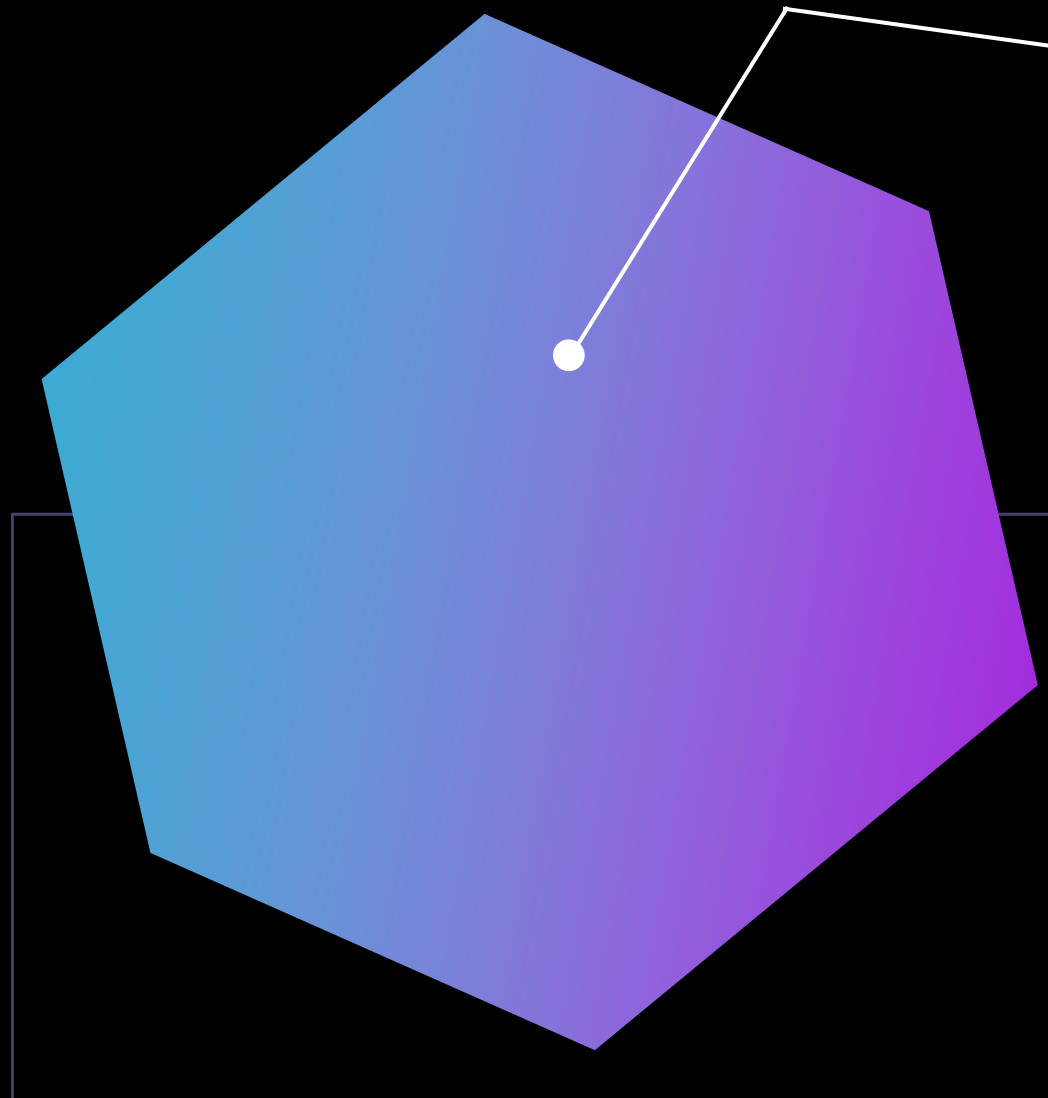
— Permite que os sistemas em TCP/IP compartilhem informações de status e erros.



— **Ping** – Envio de solicitações de eco ICMP.

— **Tracert** – Rastreia o caminho para o host.

- ▶ Envia solicitações de eco ICMP para um endereço IP enquanto incrementa o TTL no cabeçalho IP.

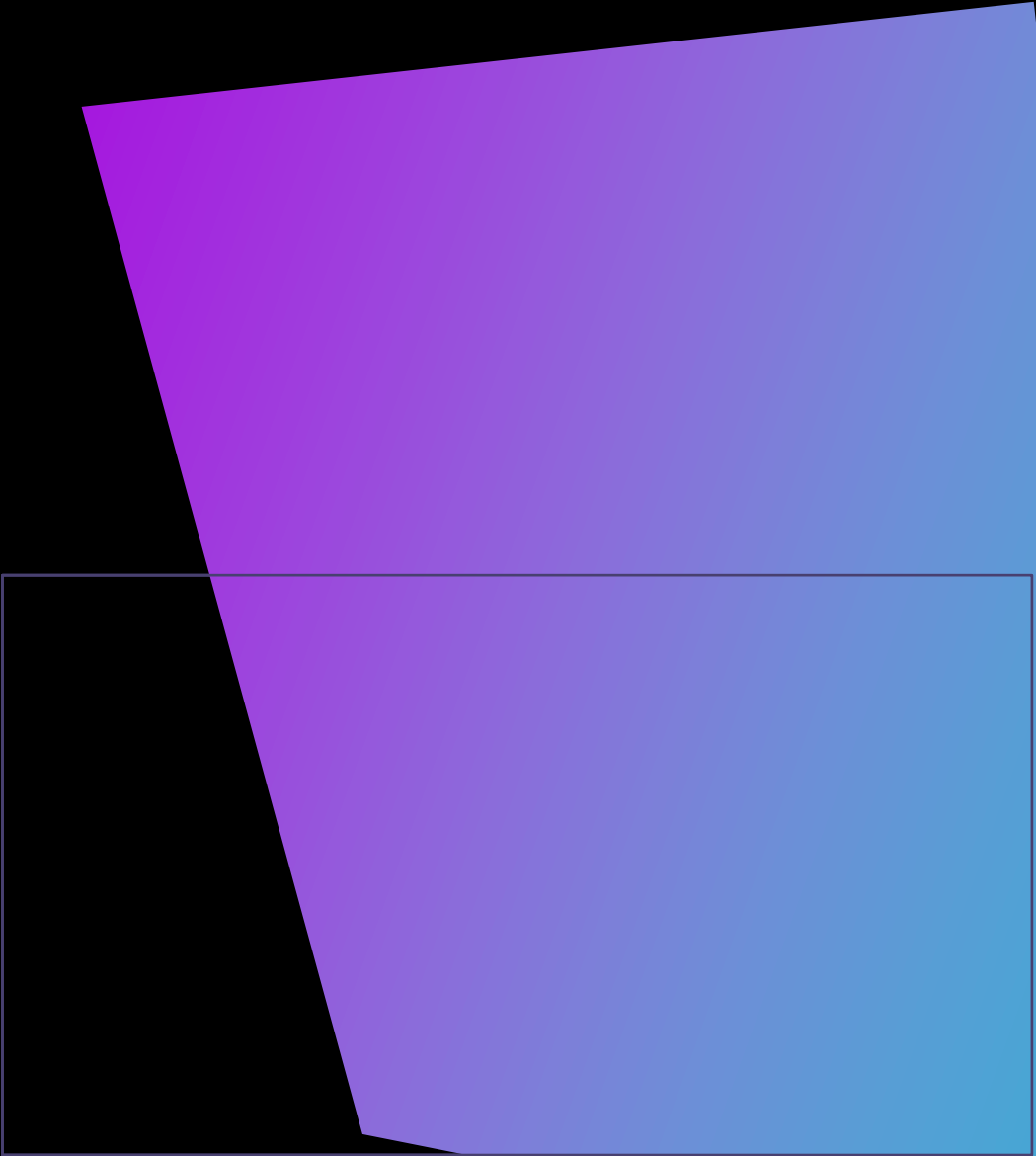
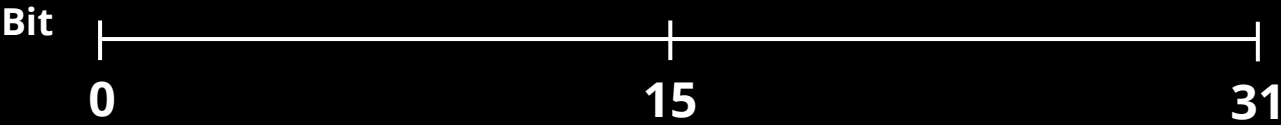


Tipos e Códigos de ICMP

— Não usa portas, mas tipos e códigos.

Tipo	Código	Descrição
0 - Echo Reply	0	Mensagem de "echo reply"
3 - Destino Inalcançável	0	Rede de destino inalcançável
	1	Host de destino inalcançável
	2	Protocolo de destino inalcançável
	3	Porta de destino inalcançável
8 - Solicitação de eco	0	Mensagem de solicitação de eco

Cabeçalho ICMP



Protocolo de Resolução de Endereço (ARP)

- Fornece resolução de endereço lógico para endereço físico em uma rede TCP/IP.
- Todos os sistemas na rede local enxergam a mensagem e o sistema que possui o endereço IP para o qual o ARP está procurando respostas.
- Todos os sistemas mantêm caches ARP que incluem mapeamentos de endereço IP para endereço físico.

OBRIGADO !

ENTENDENDO OS PROTOCOLOS TCP - IP