CES-35

Lab1 - Wireshark

Objetivo

Observar a sequência de trocas de mensagens entre duas entidades, investigando os detalhes da operação dos protocolos.

Você executará vários aplicativos de rede em diferentes cenários usando seu computador. Você observará os protocolos de rede em seu computador "em ação", interagindo e trocando mensagens com entidades de protocolo em execução em outro lugar na Internet.

Sniffers

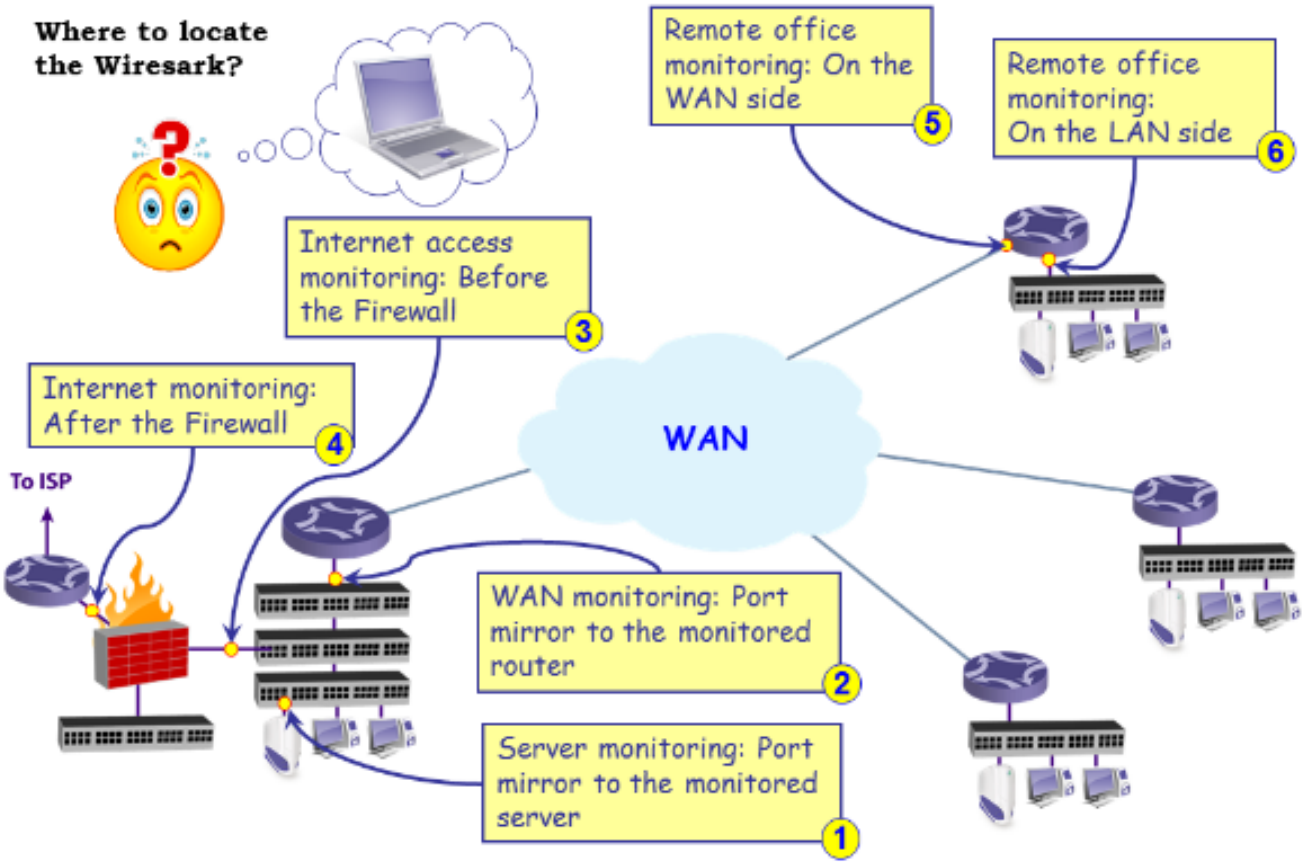
Farefajor de pacotes (sniffer): ferramenta básica para observar as mensagens trocadas entre entidades de protocolo em execução.

Um sniffer copia passivamente ("fareja") as mensagens enviadas e recebidas pelo computador; ele também exibirá o conteúdo dos vários campos de protocolo dessas mensagens capturadas.
Para esses laboratórios, usaremos o farejador de pacotes Wireshark um farejador de pacotes gratuito / shareware que roda em computadores Windows, Linux / Unix e Mac

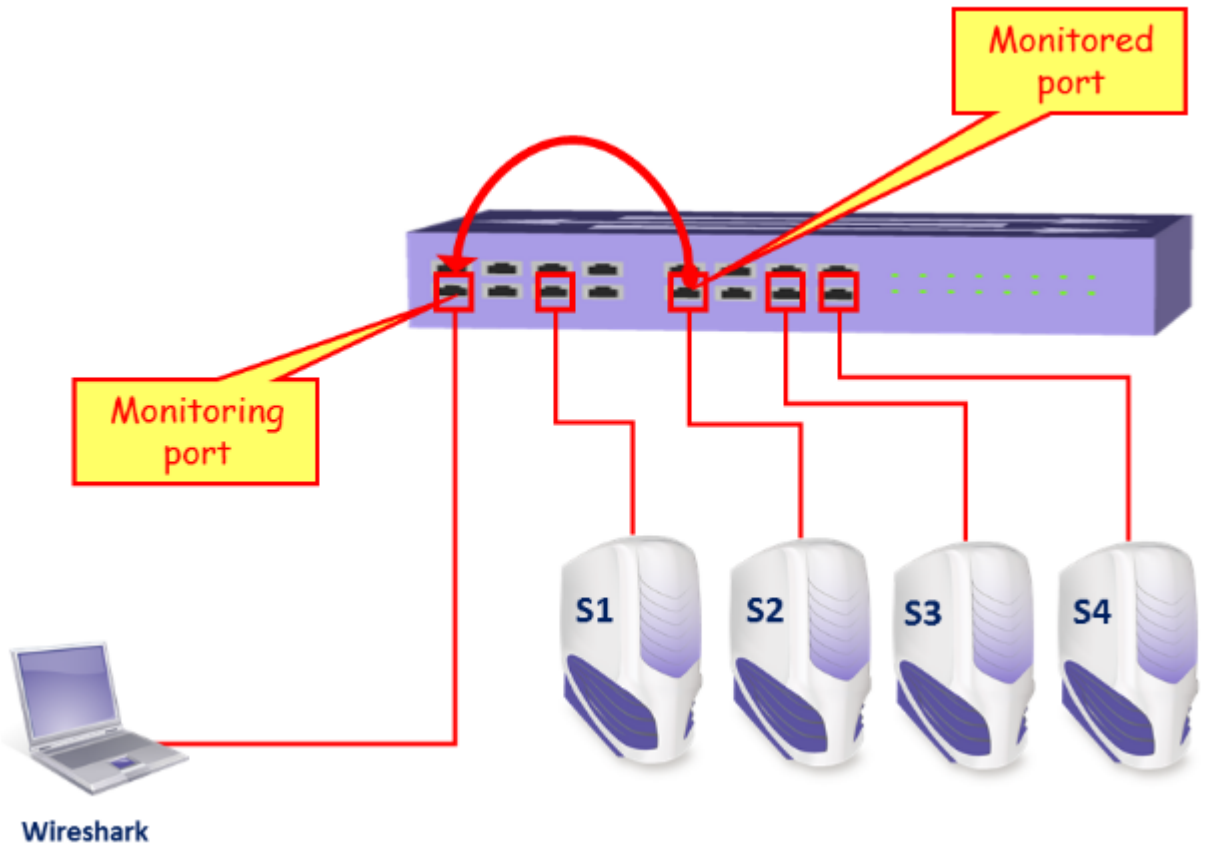
Para que serve?

- Compreender o funcionamento normal/anormal;
- Descobrir problemas da rede;
- Obter estatísticas da rede;
- Ensino;

Onde posicionar Sniffers?



Espelhando uma porta



Algumas perguntas

Does Wireshark affect network performance?

No. Wireshark is a listener, it doesn't generate traffic. However, if you set a switch on the system to duplicate all passing traffic to send to the Wireshark-monitored port then network traffic will be increased and performance could be impaired.

Is it illegal to use Wireshark on a public wifi?

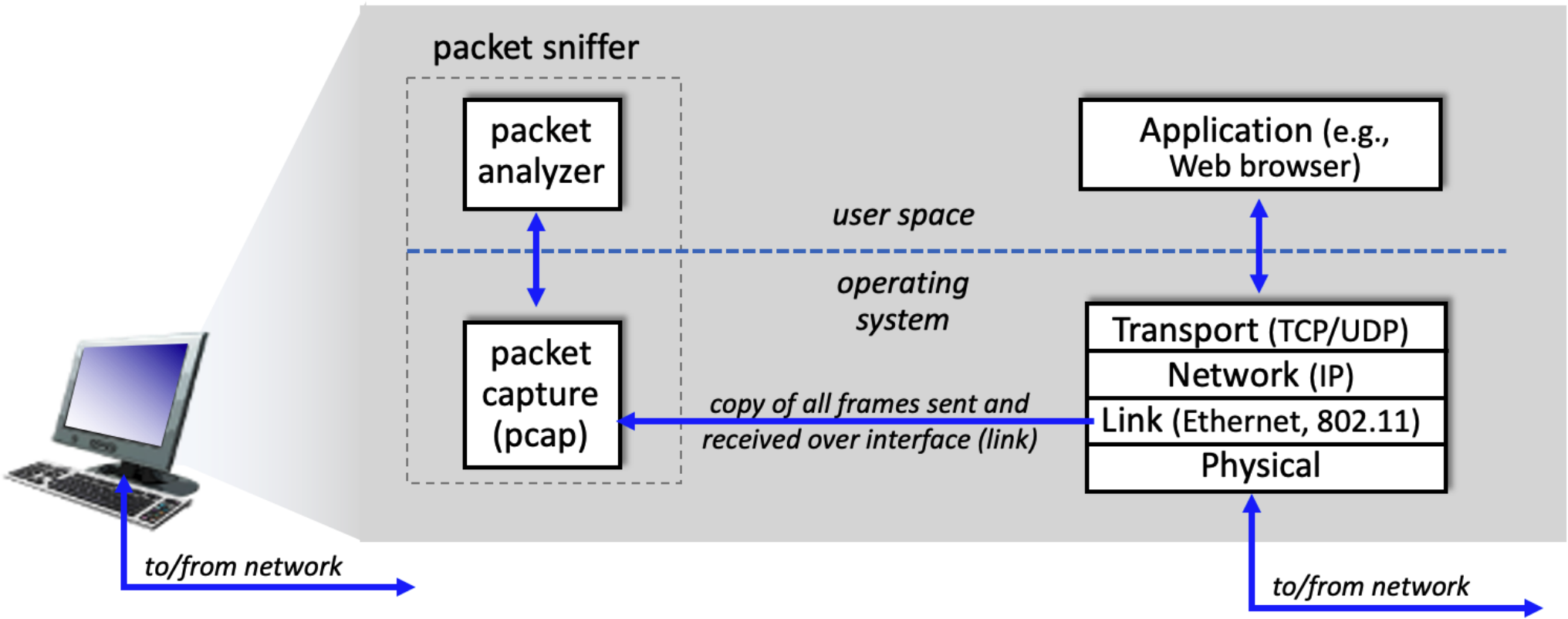
It is not illegal to use Wireshark anywhere, however, there are some illegal activities that can be facilitated by Wireshark. Think of Wireshark as being like a telescope. It is not illegal to look through the air with a telescope at passing cars, but it is illegal to use it to look through someone's window.

Limites

* What we can:
  - Capture packets
  - Watch smart statistics
  - Define filters – capture and display
  - Analyze problems

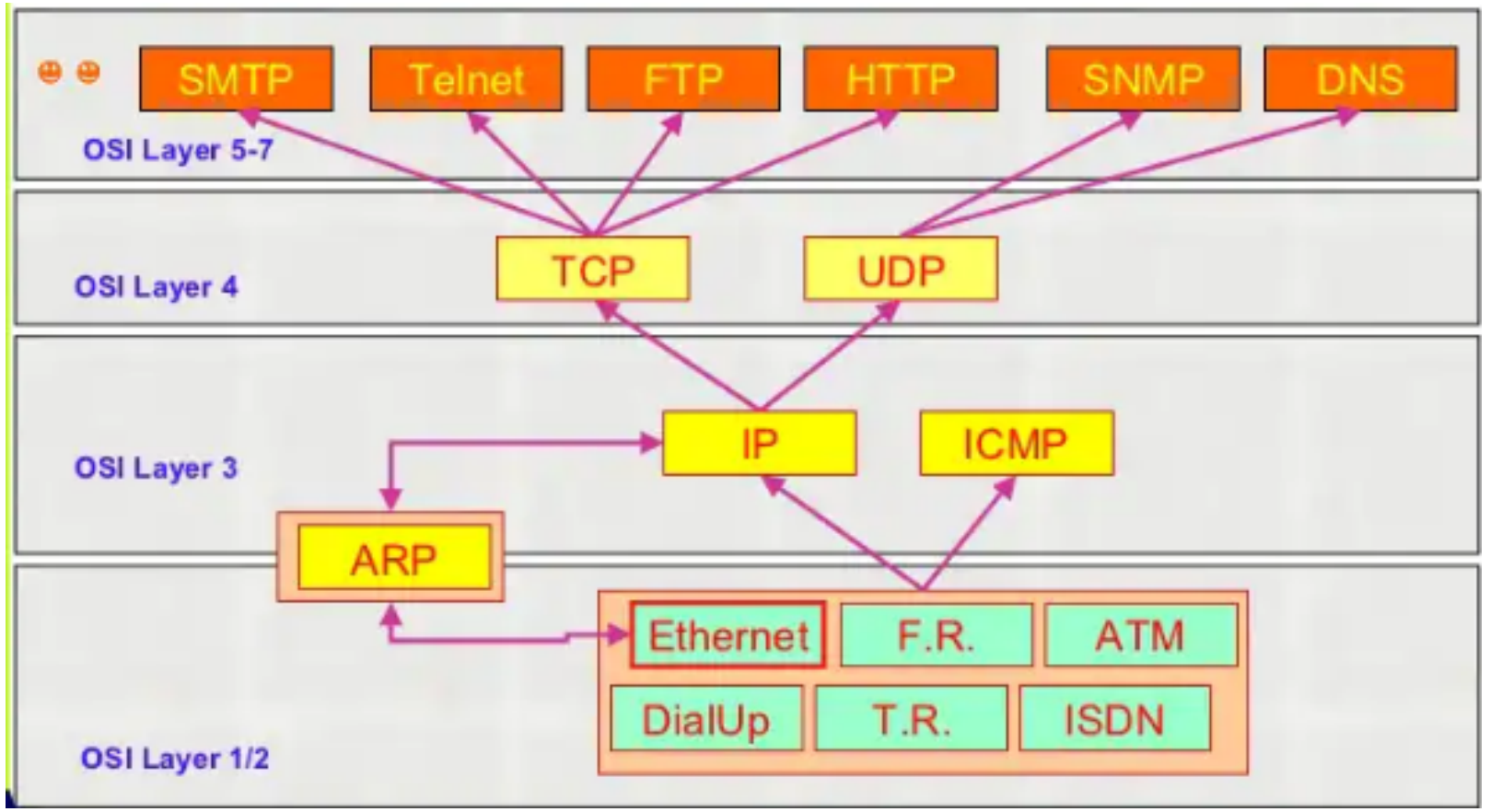
* What we cannot:
  - It is not and automatic tool
  - It is not suitable for long-term monitoring
  - It is not a “magic” tool

Estrutura de um sniffer

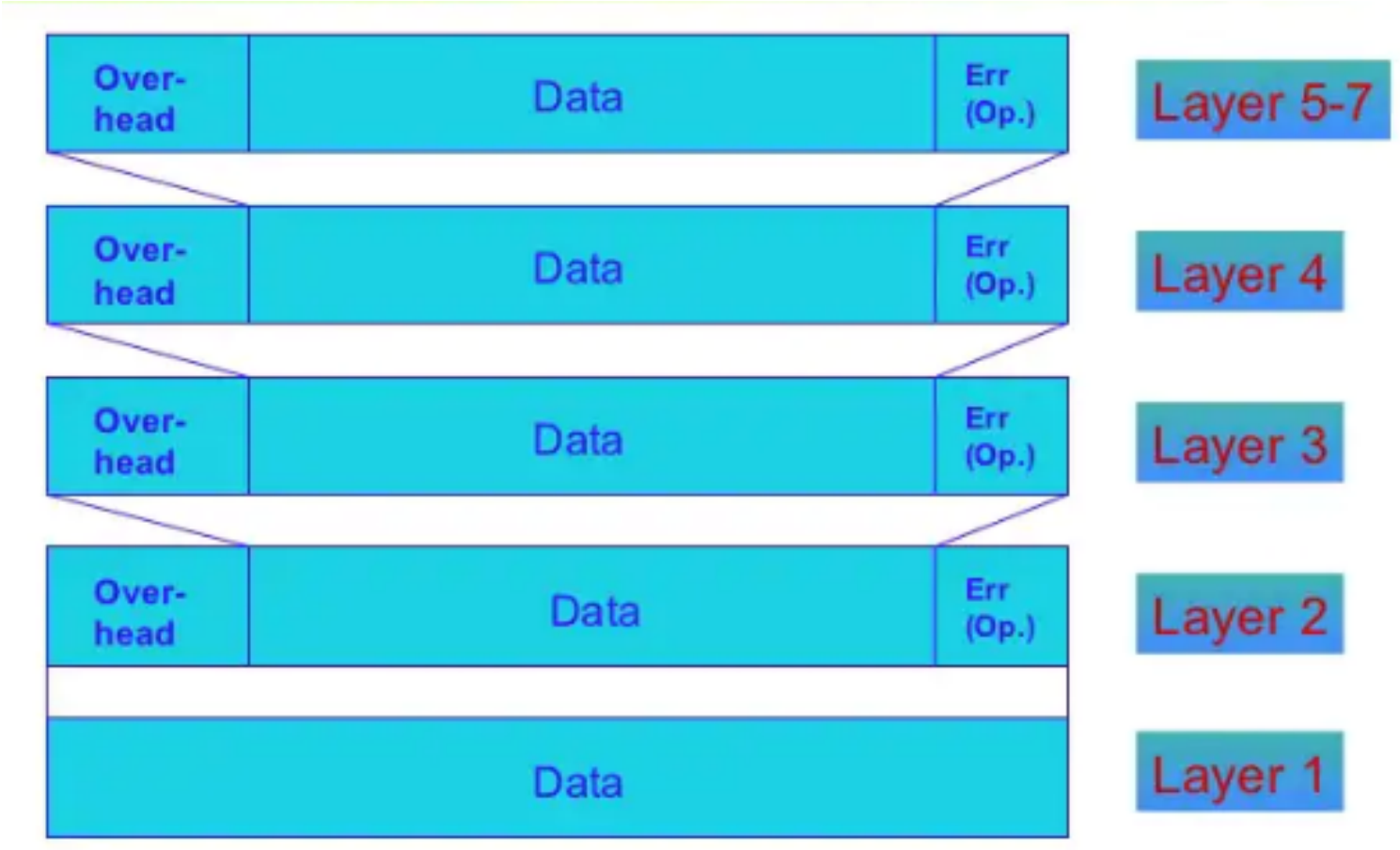


http://www.wireshark.org

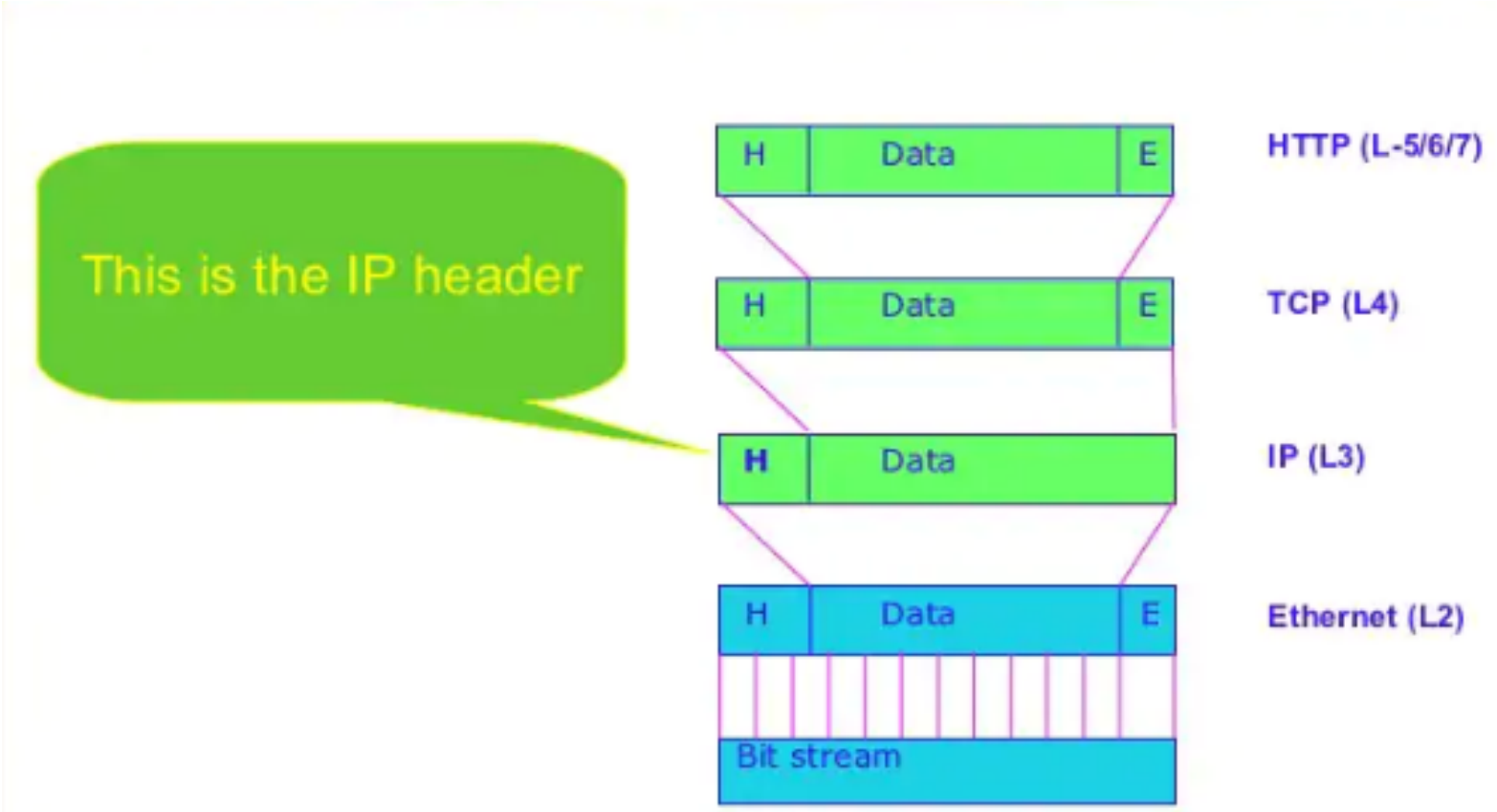
Lembrando das camadas...



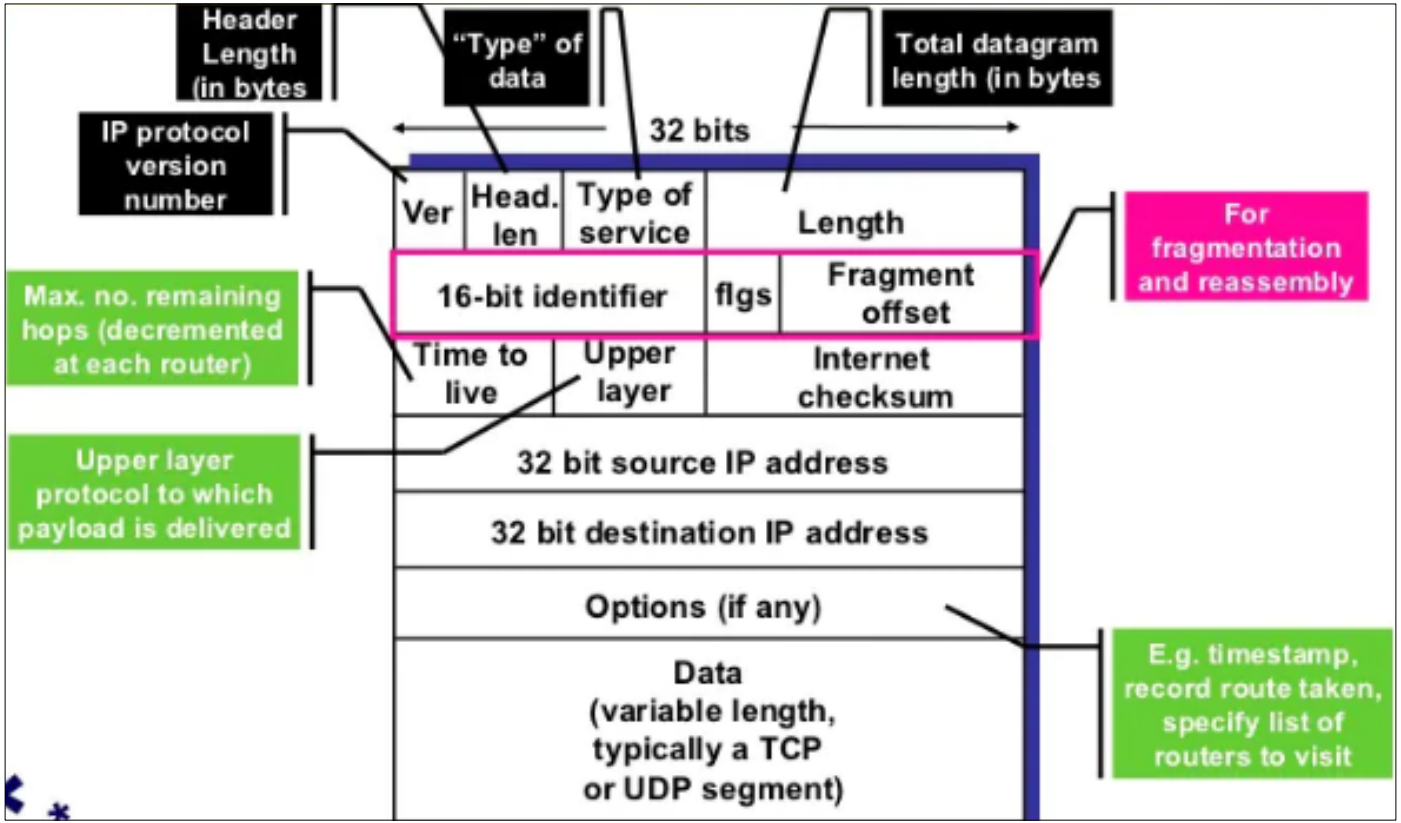
Estrutura de dados



Exemplo – Camada 3

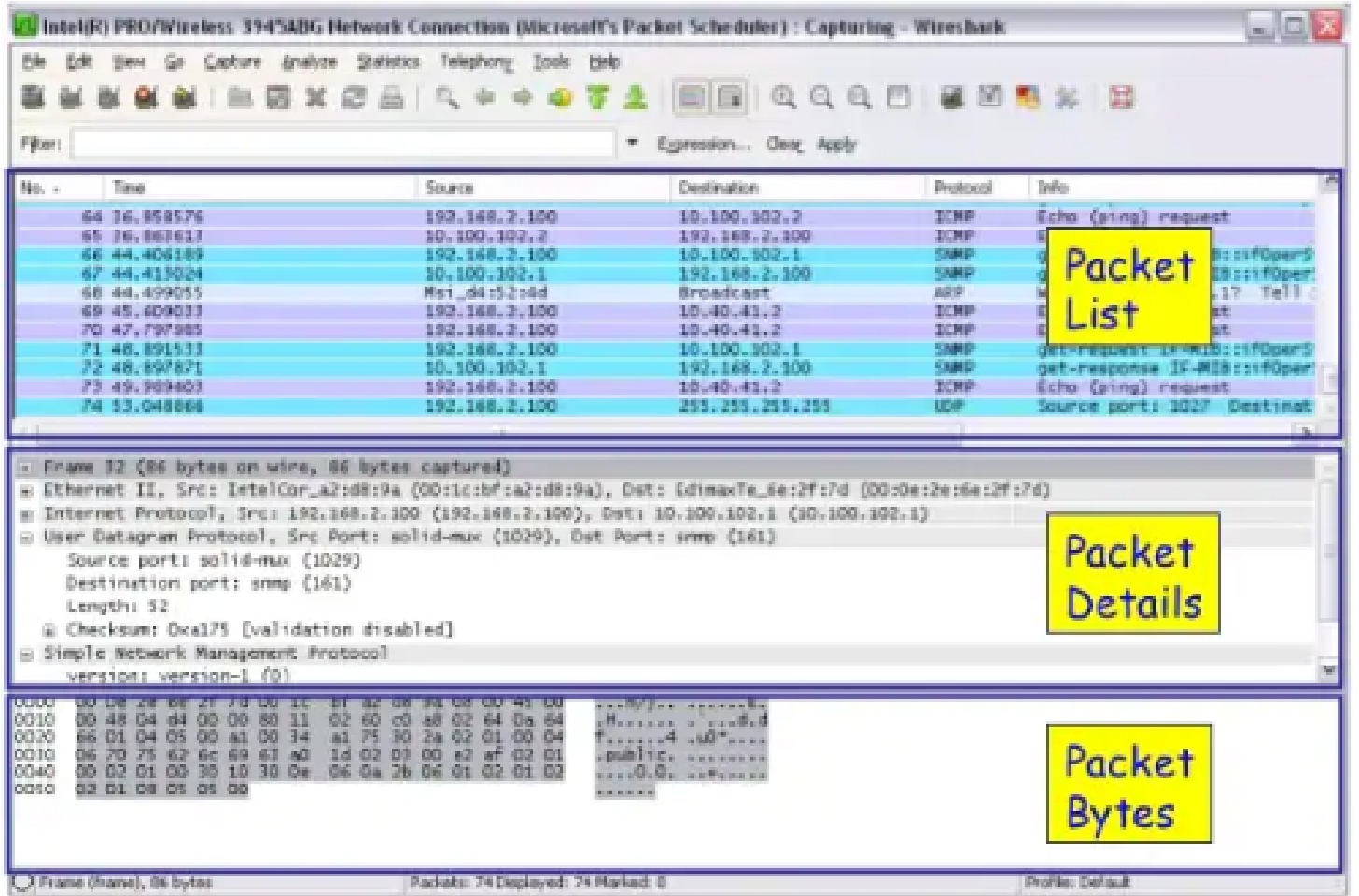


Exemplo – Cabeçalho IP




```
struct iphdr {
#if defined(__LITTLE_ENDIAN_BITFIELD)
        __u8    ihl:4,
                version:4;
#elif defined (__BIG_ENDIAN_BITFIELD)
        __u8    version:4,
                ihl:4;
#else
#error  "Please fix <asm/byteorder.h>"
#endif
        __u8    tos;
        __be16  tot_len;
        __be16  id;
        __be16  frag_off;
        __u8    ttl;
        __u8    protocol;
        __sum16 check;
        __be32  saddr;
        __be32  daddr;
        /*The options start here. */
};
```

Wireshark capturando



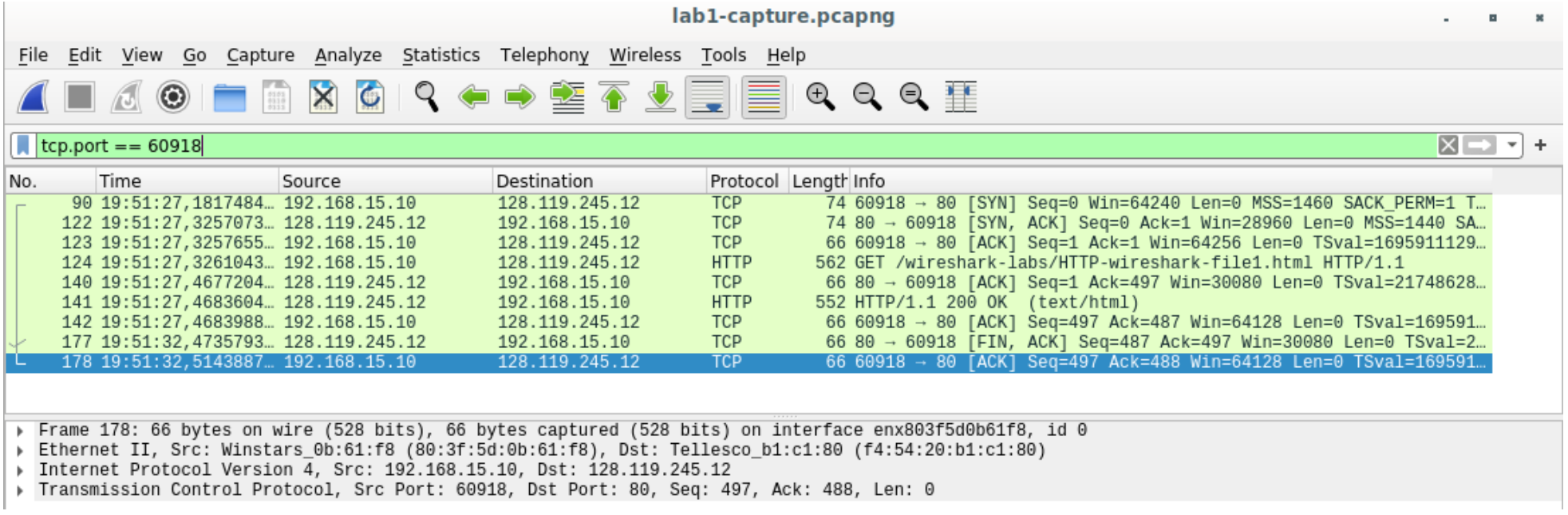
Wireshark – Packet list

Colunas:

- No - Represents a specific sequence number of the network packet. To classify a given packet, one can use this.
- Time - This is the time that a specific packet has been recorded.
- Source - This represents where we are getting the packets from. This is denoted as Internet Protocols (IP Addresses).
- Destination - This is used to represent the Internet Protocol(IP Address) where the packet is going.
- Protocol - This refers to the protocol of the data you have captured. This could be TCP, ARP etcetera
- Length- This is used to represent the size of the packet captured.
- Info - Additional information about the packet you have captured.

Wireshark – Filter

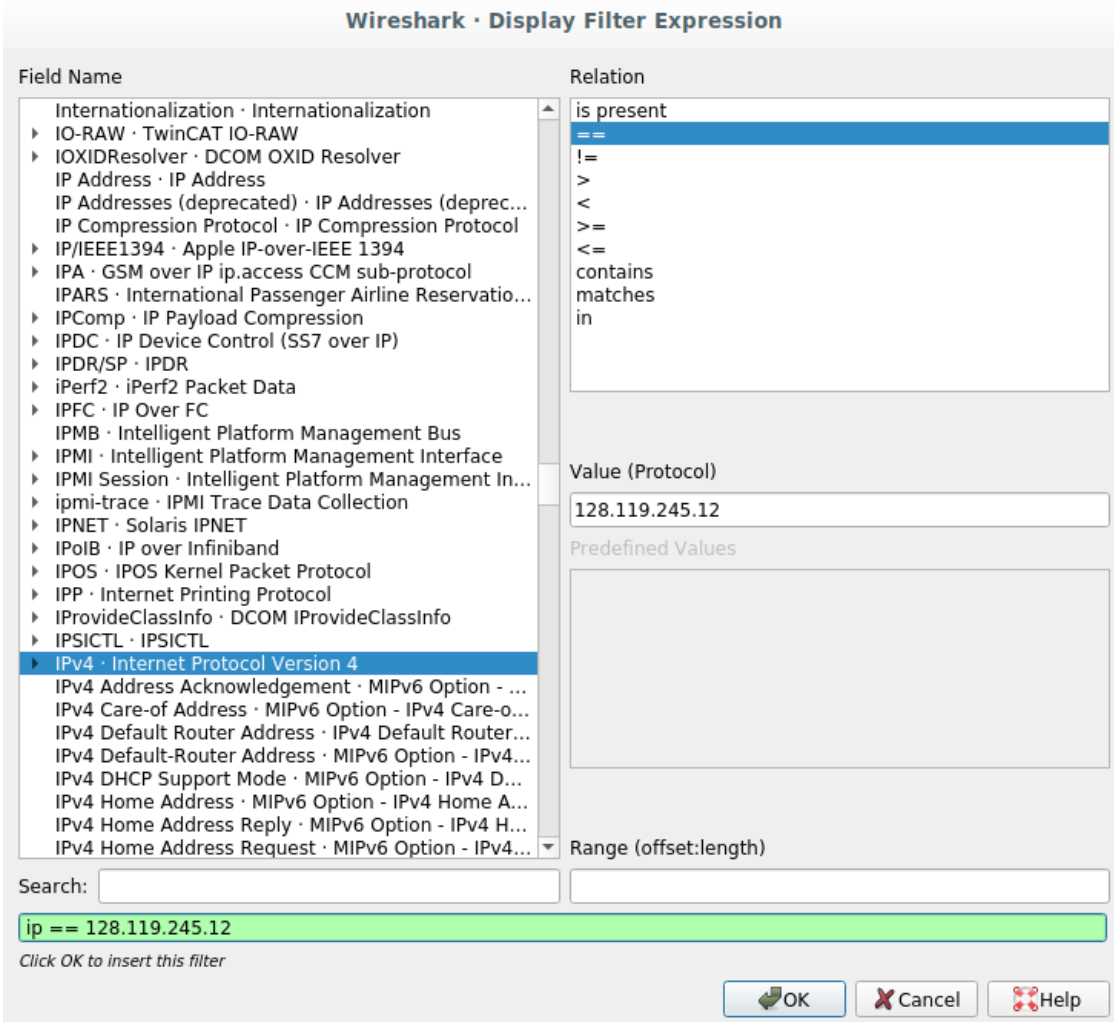
Existe uma sintaxe própria para filtrar os pacotes:



Wireshark – como construir o filtro

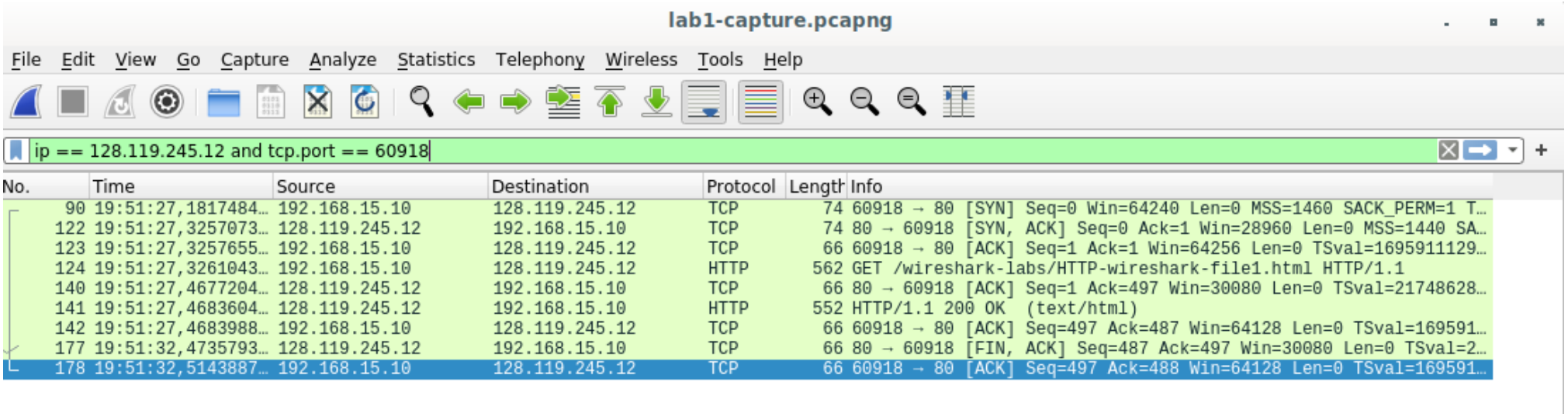
Analyze → Display Filter Expression → ipv4.
Escolha a opção de seu interesse, no meu caso o endereço do site do Kurose.

É possível compor condições para formar filtros mais completos e específicos.



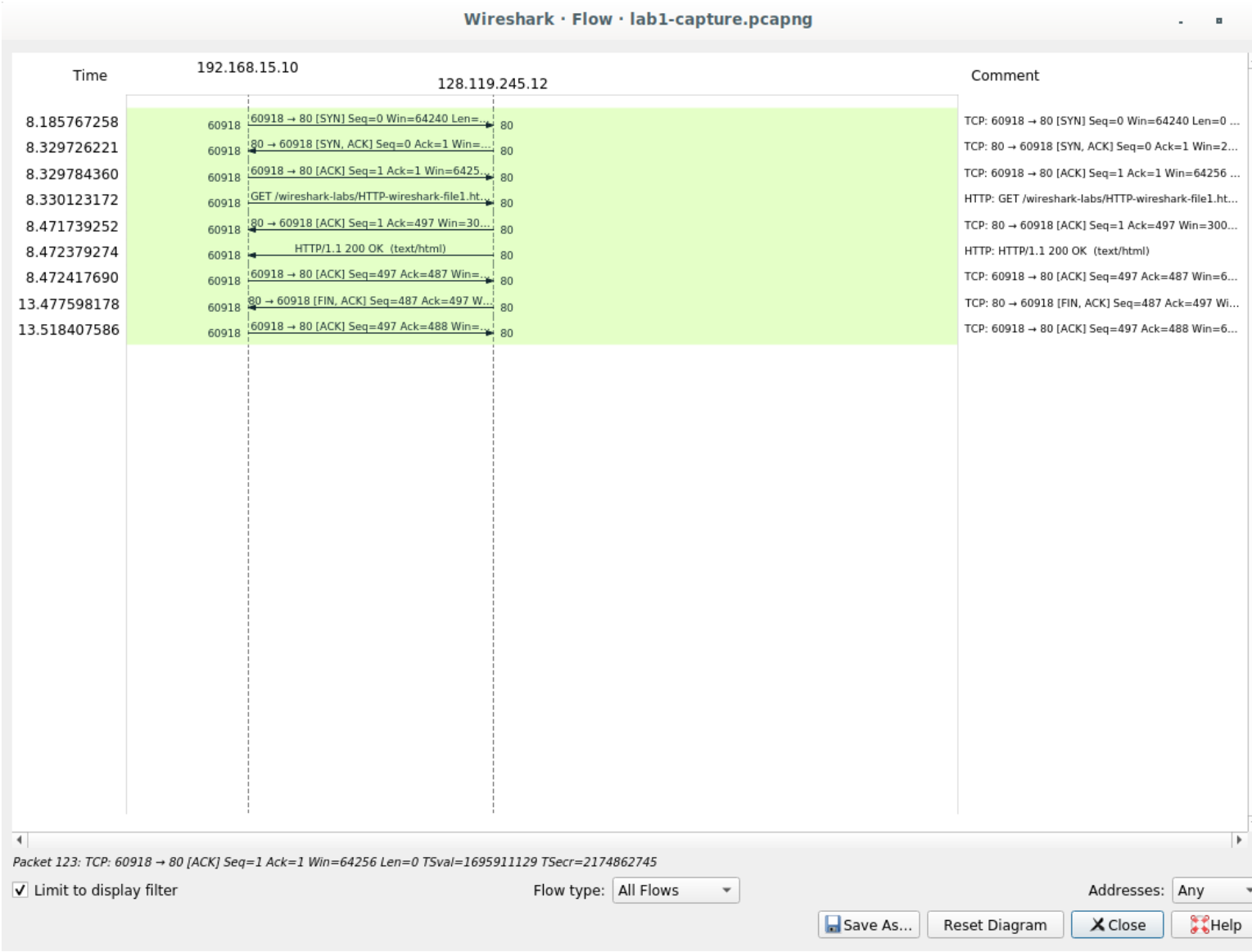
Wireshark – como construir o filtro

Filtro que seleciona IP e porta dos pacotes envolvidos com a transferência da página.



Wireshark FlowGraph

Em Statistics → FlowGraph clique em
Limit to display filter,
E verá os pacotes do fluxo selecionado no filtro.



Instalando o Wireshark

No site www.wireshark.org pode se fazer o download.

No Linux pode se instalar o pacote via comandos:

$sudo apt update
$sudo apt-get install wireshark
$sudo wireshark

Siga o roteiro e responda as perguntas.