Lista De Exercícios #02: Extraindo Informações TCP-DUMP

Nos anos 80, Van Jacobson, Steve McCanne e outros desenvolveram o *TCPDUMP* – uma ferramenta de captura de tráfego de rede. A própria ferramenta é capaz de decodificar o tráfego e apresentá-lo em maneira legível aos usuários. Mas também pode gravá-lo em formato binário, para leitura e análise posterior.

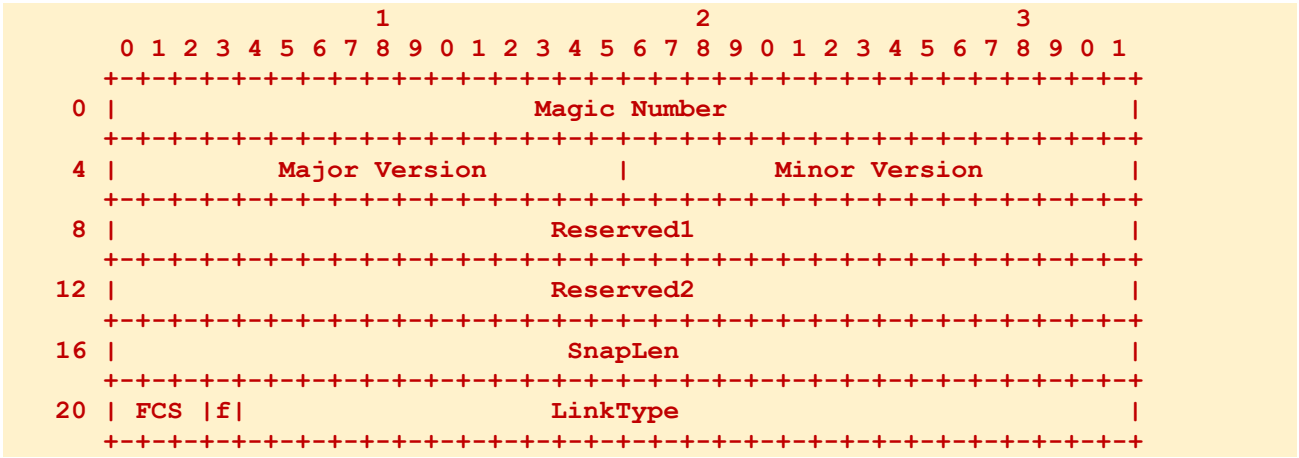
Para gravar o tráfego no *TCPDUMP* use o comando

```
tcpdump -w nomeArquivo.cap
```

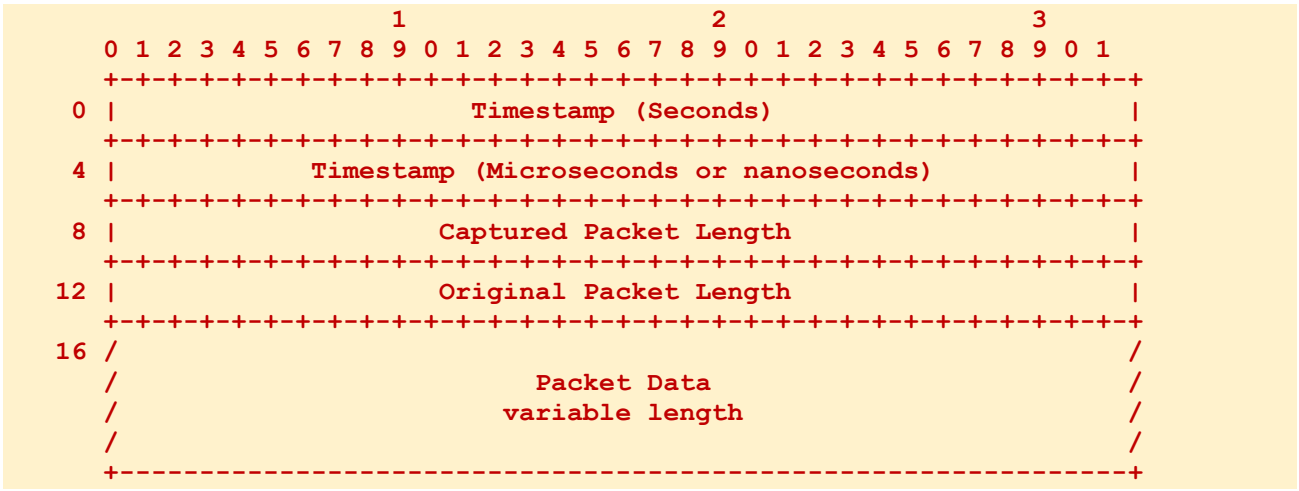
O formato do arquivo gravado é:

```
+-------------------+---------+---------+---------+----
|  cabecalhoArquivo | pacote1 | pacote2 | pacote3 | ...
+-------------------+---------+---------+---------+----
```

O formado cabeçalho do arquivo é:



E o formato de cada pacote que segue o cabeçalho do arquivo é:



Explicações para o significado de cada um dos campos nas figuras anteriores, bem como informações adicionais, podem ser encontradas em:

https://tools.ietf.org/id/draft-gharris-opsawg-pcap-00.html

Desenvolva um programa que leia um arquivo capturado pelo *tcpdump* (alguns exemplos estão disponibilizados no *assignment* do Github Classroom) e responda:

a) Mostre o conteúdo de cada um dos campos nos *headers* dos pacotes IP capturados (vide https://pt.wikipedia.org/wiki/Protocolo_de_Internet);

b) Em que momento inicia/termina a captura de pacotes?

c) Qual o tamanho do maior TCP pacote capturado?

d) Há pacotes que não foram salvos nas suas totalidades? Quantos?

e) Qual o tamanho médio dos pacotes UDP capturados?

f) Qual o par de IP com maior tráfego entre eles?

g) Com quantos outros IPs o IP da interface capturada interagiu?

ATENÇÃO:

NÃO é permitido usar bibliotecas não nativamente incorporadas ao Python