Atividade Avaliativa #02: TCP-DUMP

Observações:

1. Os programas deverão ser desenvolvidos em linguagem PYTHON;
2. Em todas as questões serão cobradas a criação de funções pelo aluno e o uso de exceções. Esses pontos serão critérios avaliativos, ou seja, o não uso implica em decréscimo na nota em cada questão não implementada utilizando tais recursos.

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

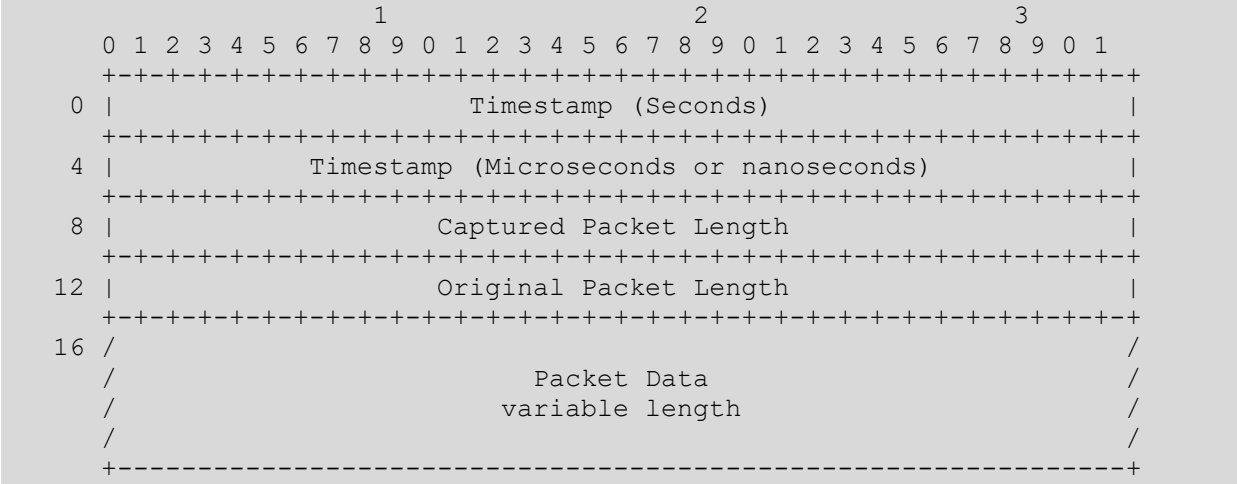
   Para gravar o tráfego no tcpdump use o comando *tcpdump -w nomeArquivo.cap*. O formato do arquivo gravado é:

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

   O formado cabeçalho do arquivo é:

```
                     1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
0 |                          Magic Number                         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
4 |          Major Version        |         Minor Version         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
8 |                           Reserved1                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
12|                           Reserved2                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
16|                            SnapLen                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
20| FCS |f|                   LinkType                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

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 Moodle) 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

Você deve entregar somente o programa (com comentários).