

1  
2 [Encrypted Internet  
3 Traffic Classification  
4 Using a Supervised  
5 Spiking Neural Network]  
6  
7  
8  
9  
10

11 < Felipe Castro  
12 11796909 >  
13  
14

}

# Conteúdo da 'Apresentação' {

## 01 Contexto Geral

< Ideia geral do problema e como o artigo se propôs a resolver >

## 02 Projeto do Experimento

< Conjunto de dados, pré-processamento e medidas de avaliação >

## 03 Resultados

< O que foi prometido, o que foi realizado e discussões sobre >

## 04 Planejamento

< Quais serão os próximos passos e quando serão desenvolvidos >

}

```
1 01 {  
2  
3
```

```
4  
5 [Contexto Geral]  
6  
7
```

```
8 < Ideia geral do problema e como o  
9 artigo se propôs a resolver >  
10  
11
```

```
12 }  
13  
14
```

```
1  Resumo; {
```

```
2  
3  
4      <p O artigo "Encrypted Internet Traffic  
5      Classification using a Supervised Spiking  
6      Neural Network" trata do uso de Spiking Neural  
7      Networks (SNNs) para classificar tráfego de  
8      internet criptografado. A ideia principal é  
9      identificar o tipo de tráfego (como streaming,  
10     chat em redes sociais, chamadas VoIP, etc.)  
11     sem precisar descriptografá-lo. >
```

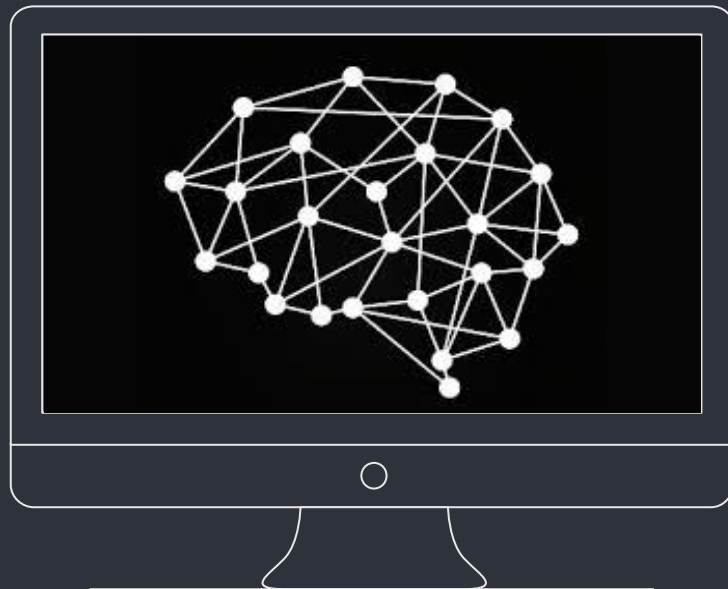
```
12     </p>
```

```
13  
14 }
```

# Spiking Neural Networks {

Diferente das redes neurais convencionais, que usam operações matemáticas contínuas, as SNNs processam dados através de picos de ativação (spikes), simulando neurônios biológicos.

}



Fonte da imagem: pngtree.com

# Como Funciona a 'Rede'? {

## Entrada



$$I_i^{(\ell)}[t+1] = \alpha I_i^{(\ell)}[t] + \sum w_{ij}^{(\ell)}[t] S_j^{(\ell)}[t]$$

## Memória do Neurônio



$$U_i^{(\ell)}[t+1] = \beta U_i^{(\ell)}[t] + I_i^{(\ell)}[t] - S_i^{(\ell)}[t]$$

## Função de Ativação



$$S_i^{(\ell)}[t] \equiv \Phi(U_i^{(\ell)}[t] - u)$$

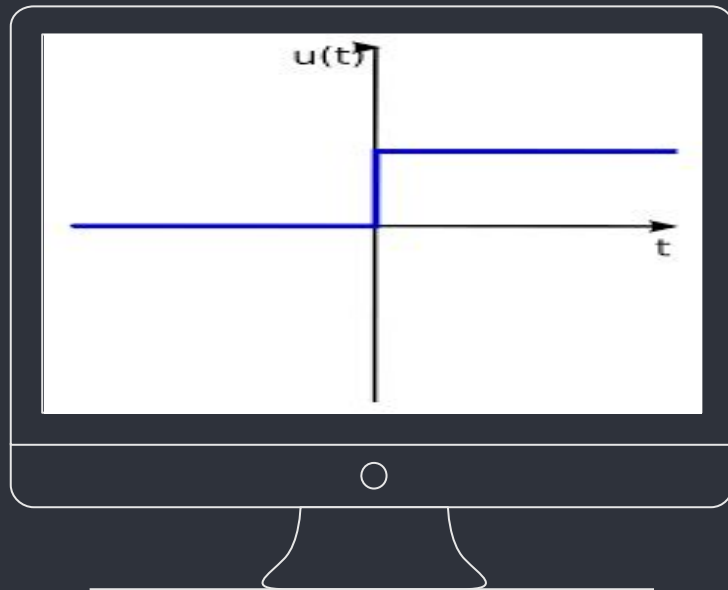
}

# Surrogate Backpropagation

{

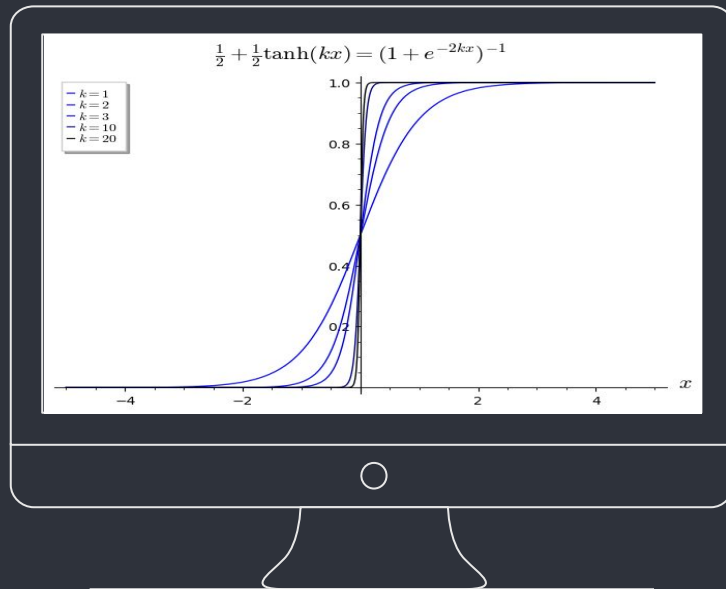
Como a função de ativação (step-function) não é diferenciável, precisamos fazer uso de uma função substituta para calcular o gradiente durante a backpropagation.

}



# Surrogate Backpropagation

Como a função de ativação (step-function) não é diferenciável, precisamos fazer uso de uma função substituta para calcular o gradiente durante a backpropagation.





1  
2 02 {  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14

## [Projeto do Experimento]

< Conjunto de dados, pré-processamento  
e medidas de avaliação >

}

# Estrutura do 'Experimento' {

## Pré-processamento



< Leitura dos PCAPs,  
seleção de features  
e divisão dos fluxos  
>

## Separação dos dados



< Separação do  
conjunto de dados  
entre categorias e  
depois entre treino,  
validação e teste >

## Treinamento



< Treinamento  
iterativo por meio  
de épocas >

## Avaliação



< Avaliação por meio  
de medidas de acerto  
e visualizações do  
comportamento da  
rede >

}

## 2016 ISCX VPN-nonVPN Traffic Dataset {



< Conjunto de dados comumente utilizado para pesquisas em classificação de tráfego de rede, especialmente para diferenciar tráfego VPN de tráfego não VPN. >

}

## ISCX-Tor2016 Dataset {



< Conjunto de dados desenvolvido para auxiliar na pesquisa de detecção e classificação de tráfego da rede Tor, que é projetada para anonimizar a comunicação na Internet. >

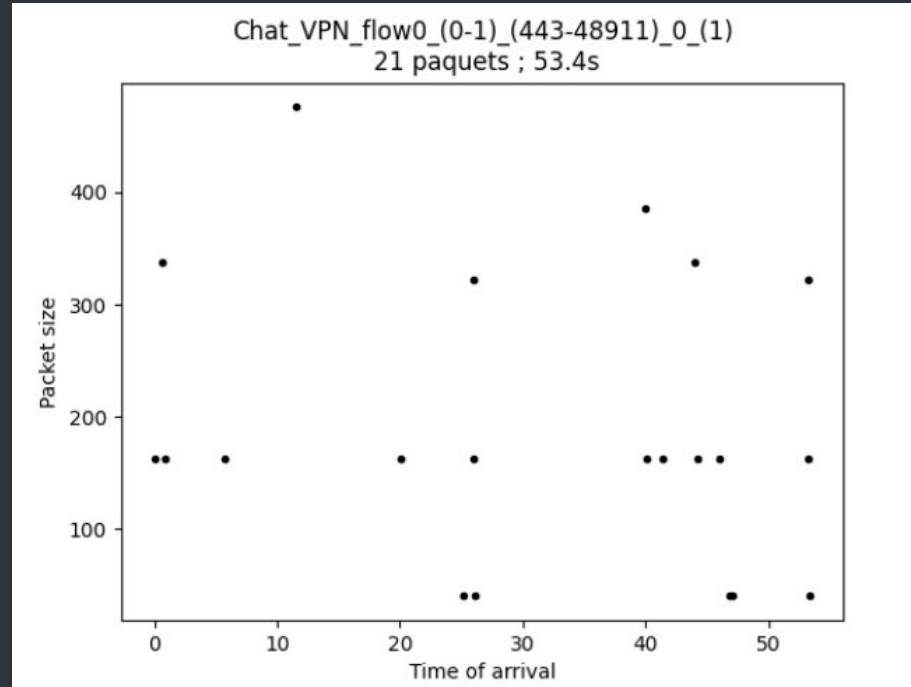
}

# Leitura dos 'PCAPs' {

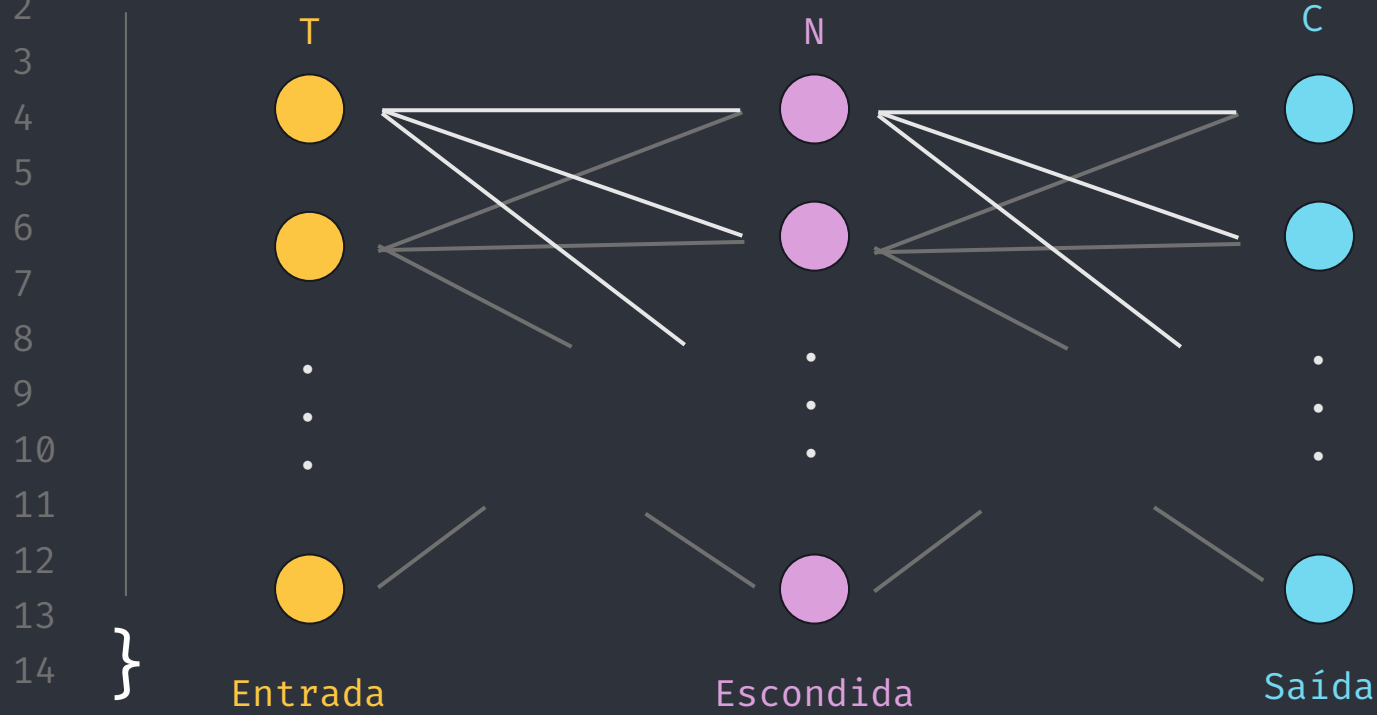
	timestamp	IP_version	IP_ihl	IP_tos	IP_len	IP_id	IP_flags	IP_frag	IP_ttl	IP_proto	IP_checksum	IP_src
0	1433356821.839550	4	5	0	162	20629	DF	0	107	6	53743	205.188.12.91
1	1433356821.839658	4	5	0	40	52142	DF	0	64	6	33360	10.8.8.178
2	1433356822.479111	4	5	0	338	21179	DF	0	107	6	53017	205.188.12.91
3	1433356822.479913	4	5	0	40	52143	DF	0	64	6	33359	10.8.8.178
4	1433356822.680985	4	5	0	162	21344	DF	0	107	6	53028	205.188.12.91

IP_dst	IP_options	TCP_sport	TCP_dport	TCP_seq	TCP_ack	TCP_dataofs	TCP_reserved
10.8.8.178	[]	443.0	48911.0	3.987076e+09	2.730303e+09	5.0	0.0
205.188.12.91	[]	48911.0	443.0	2.730303e+09	3.987076e+09	5.0	0.0
10.8.8.178	[]	443.0	48911.0	3.987076e+09	2.730303e+09	5.0	0.0
205.188.12.91	[]	48911.0	443.0	2.730303e+09	3.987077e+09	5.0	0.0
10.8.8.178	[]	443.0	48911.0	3.987077e+09	2.730303e+09	5.0	0.0

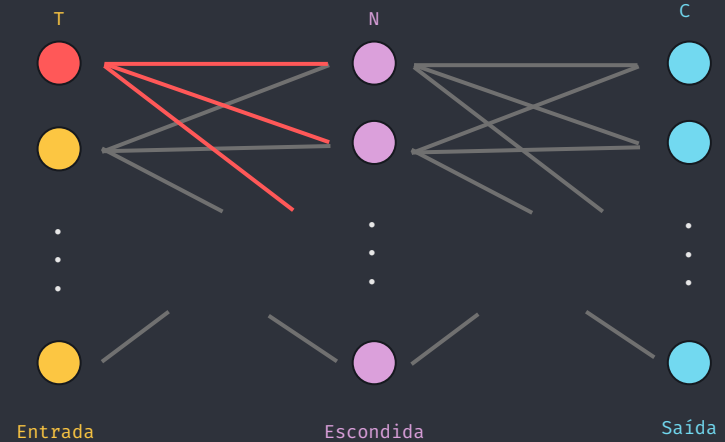
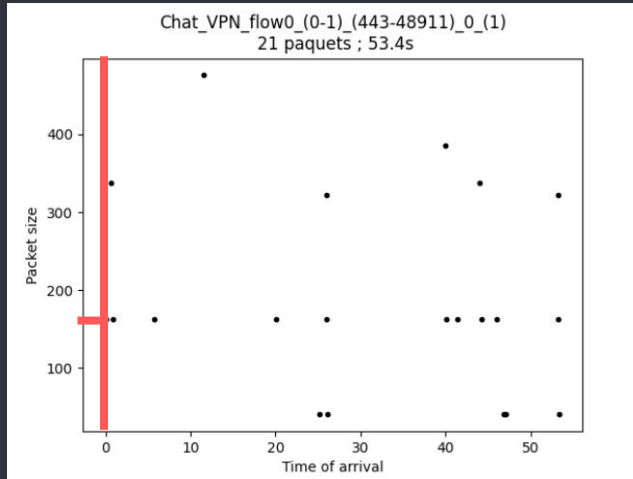
# Tratamento dos 'PCAPs' {



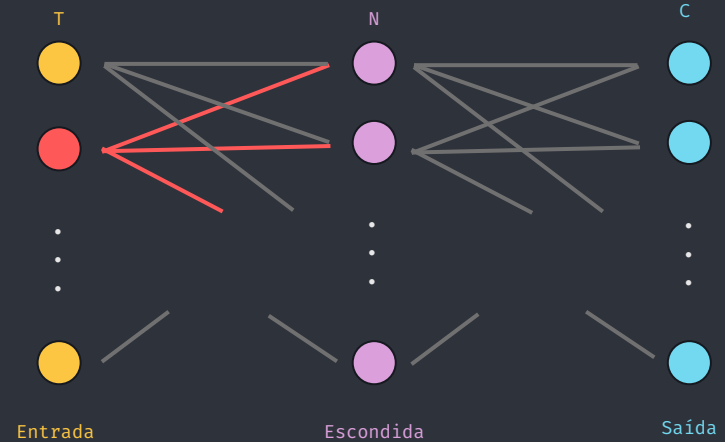
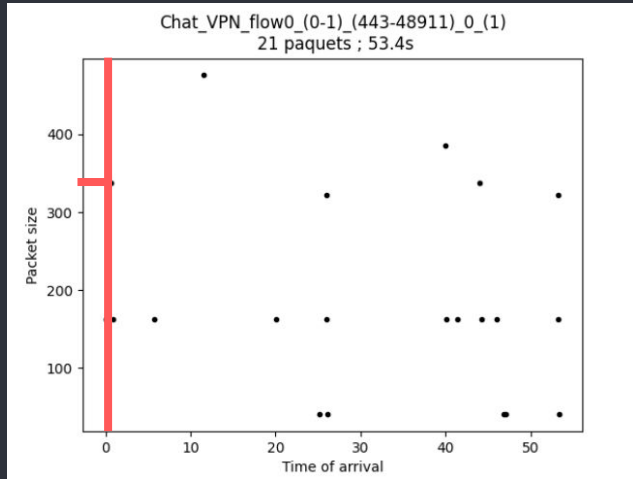
# Arquitetura da Rede; {



# Arquitetura da Rede; {



# Arquitetura da Rede; {





```
1 03 {  
2  
3  
4
```

```
5 [Resultados]  
6  
7
```

```
8 < 0 que foi prometido, o que foi  
9 realizado e discussões sobre >  
10  
11
```

```
12 }  
13  
14
```

# Avaliação; {

## Acurácia



< Medida geral de quanto o modelo acerta >

## Revocação



< Capacidade do modelo de não deixar de retornar a classe correta, evitando falsos negativos >

## Precisão



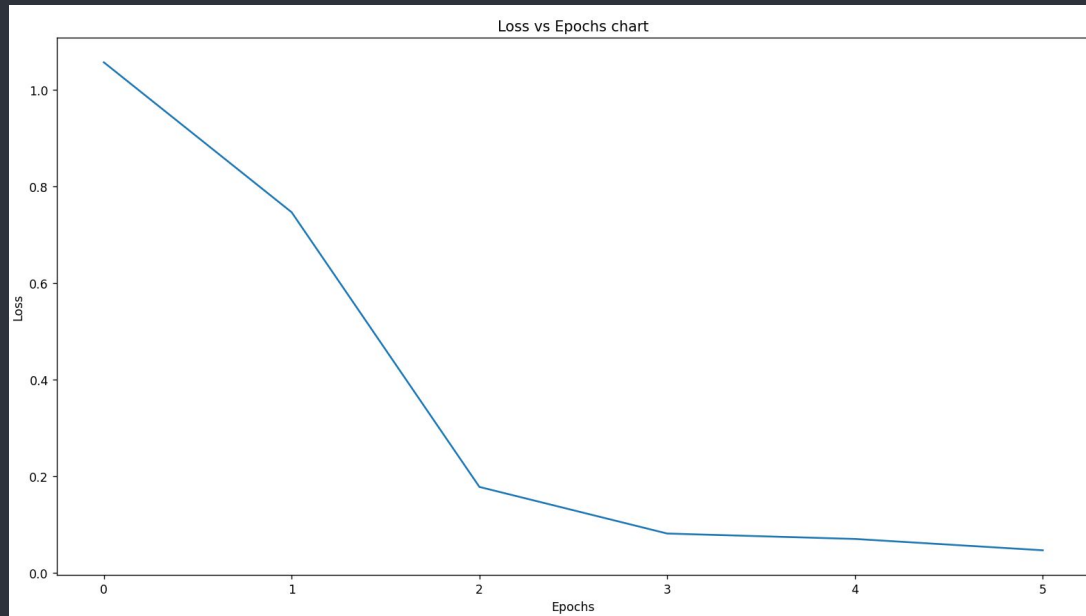
< Medida de quanto o modelo retorna a classe correta com maior especificidade, evitando falsos positivos >

}

```
1  Avaliação; {  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14 }
```

```
VOIP : Re = 99.7% ; Pr = 99.4% ; Ac = 99.2%  
File Transfer : Re = 81.8% ; Pr = 81.8% ; Ac = 98.9%  
Chat : Re = 95.6% ; Pr = 97.7% ; Ac = 99.2%
```

```
1  Avaliação; {  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14 }
```



1 Avaliação; {

2

3

4

5

6

7

8

9

10

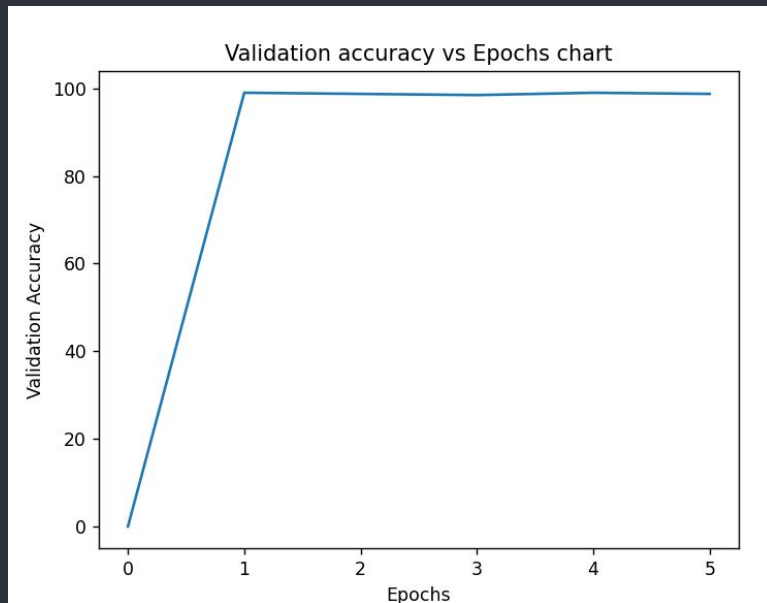
11

12

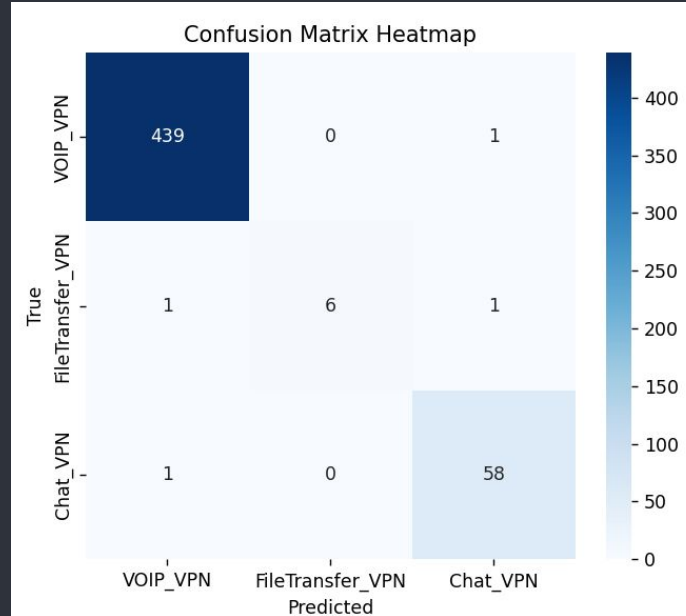
13

14

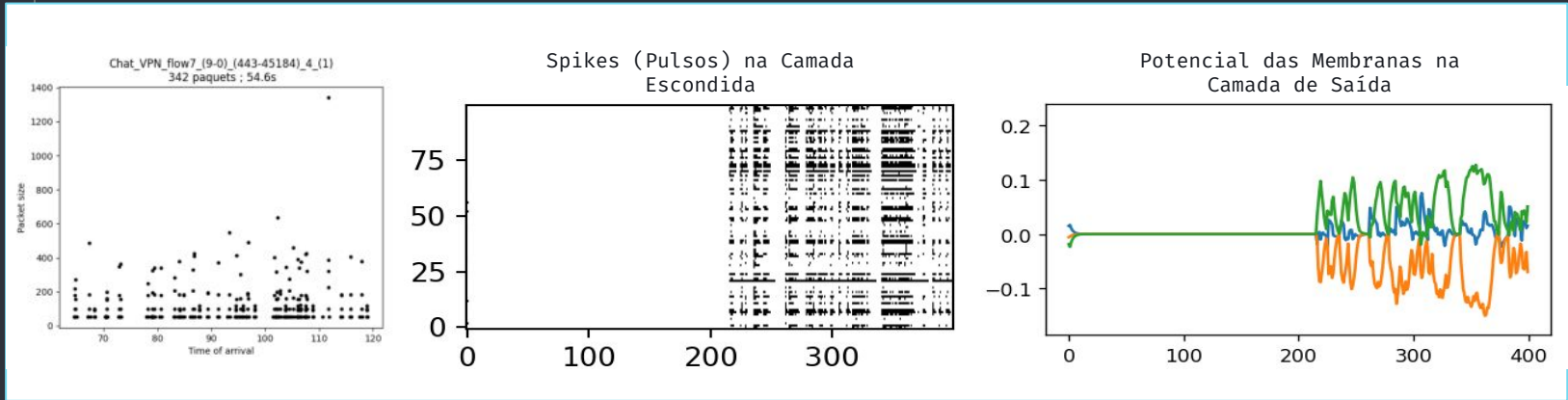
}



# Avaliação; {

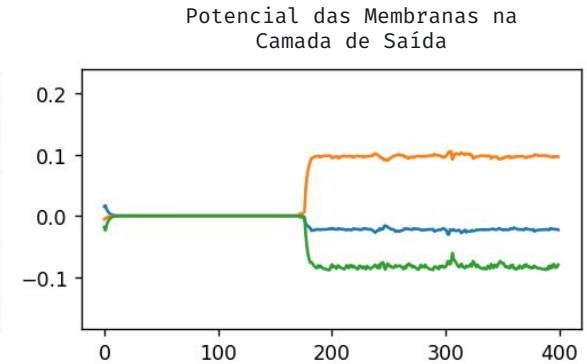
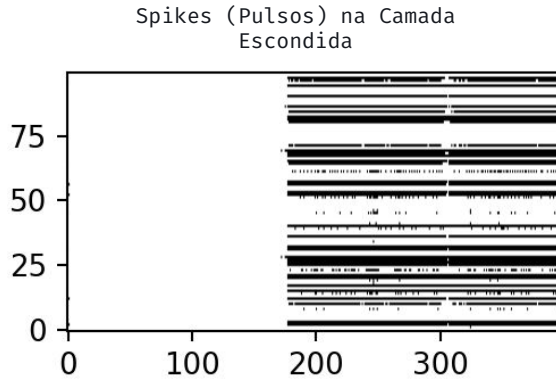
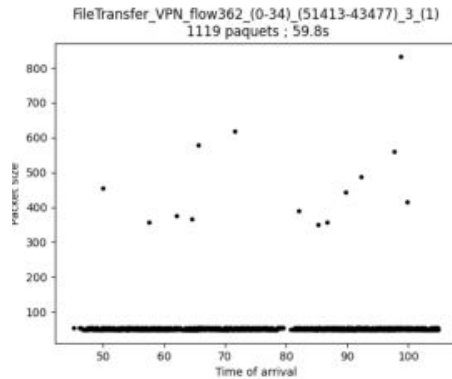


# Avaliação (CHAT); {



}

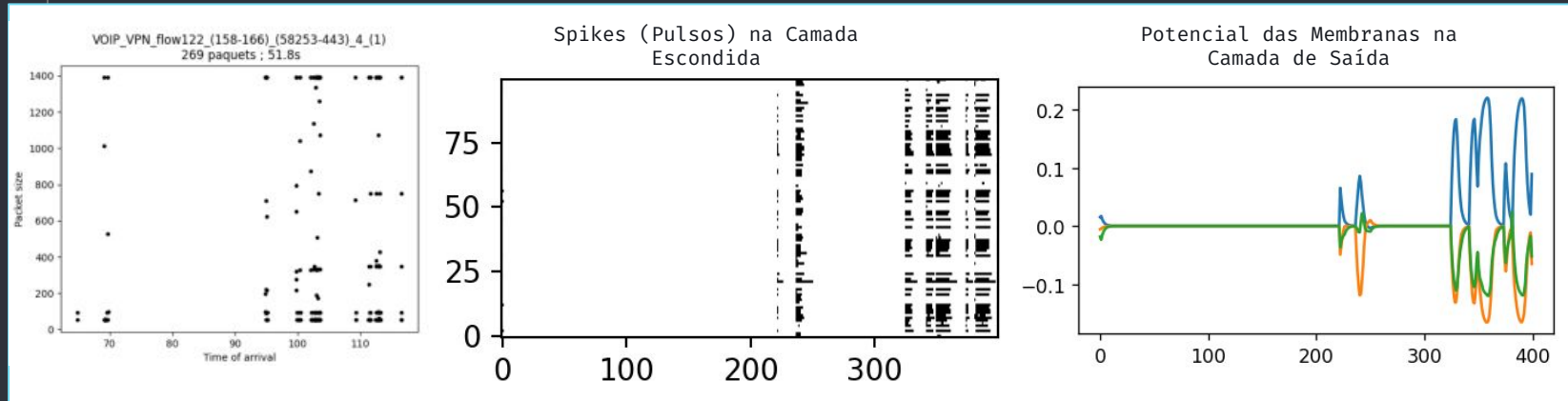
# Avaliação (FILE\_TRANSFER); {



}



# Avaliação (VoIP); {



```
1
2
3
4 0 que eu pretendo
5 fazer? {
6
7
8
9
10
11
12
13
14 }
```

< Meu objetivo é **reproduzir as técnicas** utilizadas nesse estudo e aplicá-las a um **novo conjunto de dados dentro do mesmo domínio**, explorando sua eficácia em diferentes cenários. Algumas bases de dados que considereei incluem:

**CIC-Darknet2020:** Focado em tráfego da Darknet, incluindo comunicações anônimas. >



Fonte da imagem: istockphoto.com






04 {

[Planejamento]

< Quais serão os próximos passos  
e quando serão desenvolvidos >

}

# Planejamento {Esperado}

	Maio	Junho
Reproduzir com Conjunto de Dados Completo		
Obter e Tratar Dados do Novo Experimento		
Implementação e Execução com Novos Dados		
Análise dos Resultados		
Preparação da apresentação		

# Referência do Artigo {

Ali Rasteh, Florian Delpech, Carlos Aguilar-Melchor, Romain Zimmer, Saeed Bagheri Shouraki, Timothée Masquelier,

Encrypted internet traffic classification using a supervised spiking neural network,

**Neurocomputing:**

- \* Volume 503,
- \* 2022,
- \* Pages 272-282,
- \* ISSN 0925-2312,

DOI:

- \* <https://doi.org/10.1016/j.neucom.2022.06.055>.

}

thanks.c

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14

```
Muito {  
Obrigado;  
|  
}
```

