Aula prática 1

Monitoria InfraCom 2020.3

Josenildo Vicente (jva)

Objetivo

Fazer experimentos

- Traceroute
- Ping
- Wireshark
- Telnet
  - HTTP
  - SMTP (Email)
- DNS
  - NSLOOKUP

VPN

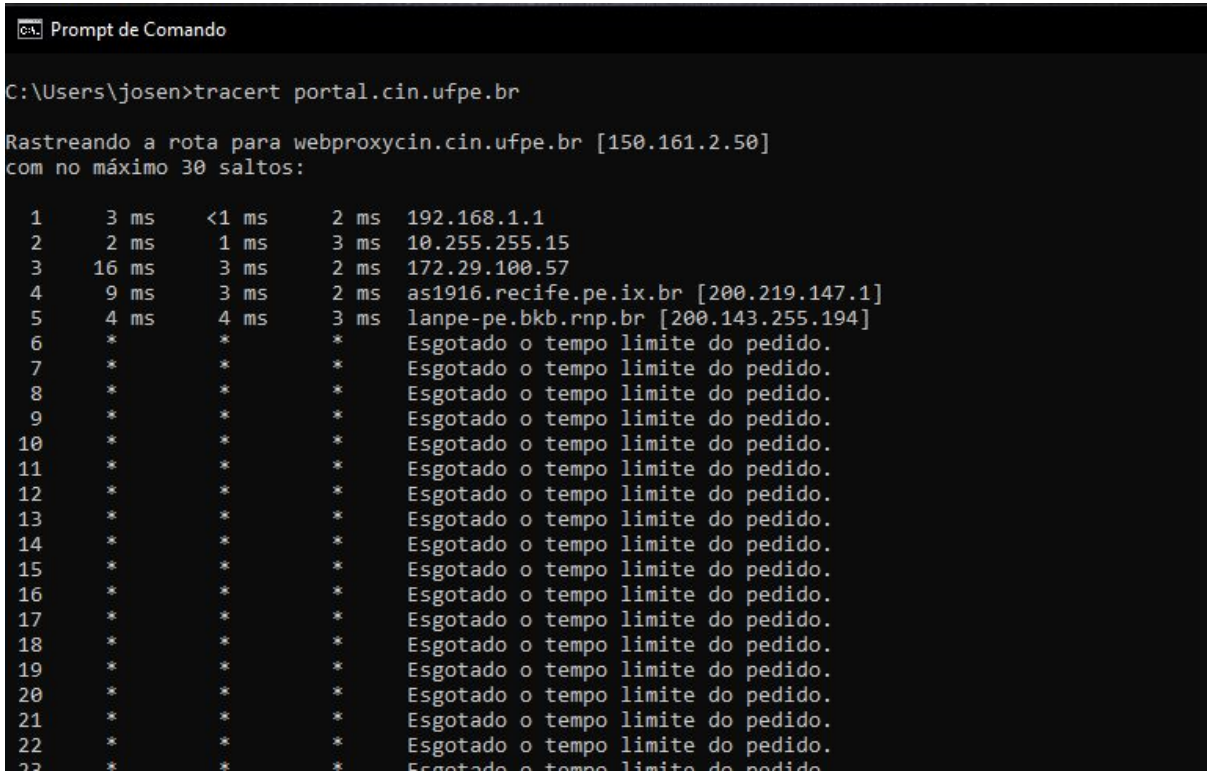
https://sites.google.com/cin.ufpe.br/coordenacao-de-infraestrutura/rede/vpn

Traceroute

É uma ferramenta que permite descobrir o caminho que é feito pelos pacotes desde sua origem até o destino.

traceroute [domínio ou ip] (Ubuntu)

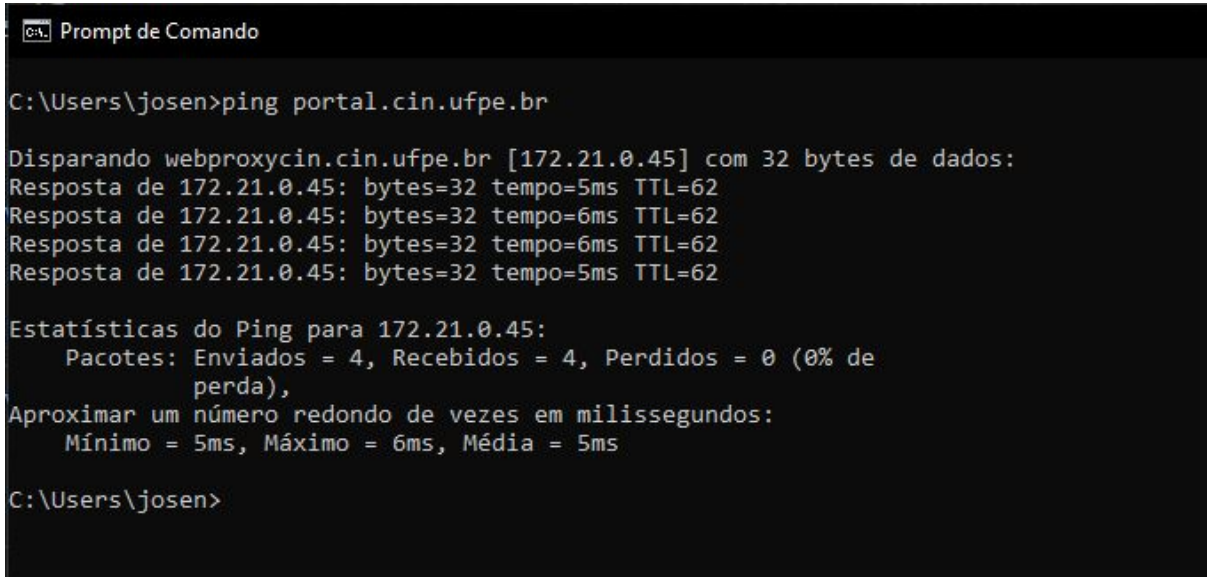
tracert [domínio ou ip] (Windows)



Ping

Comando usado para medir o tempo de envio e resposta de um pacote de dados a outro computador/servidor.

ping [domínio ou ip]



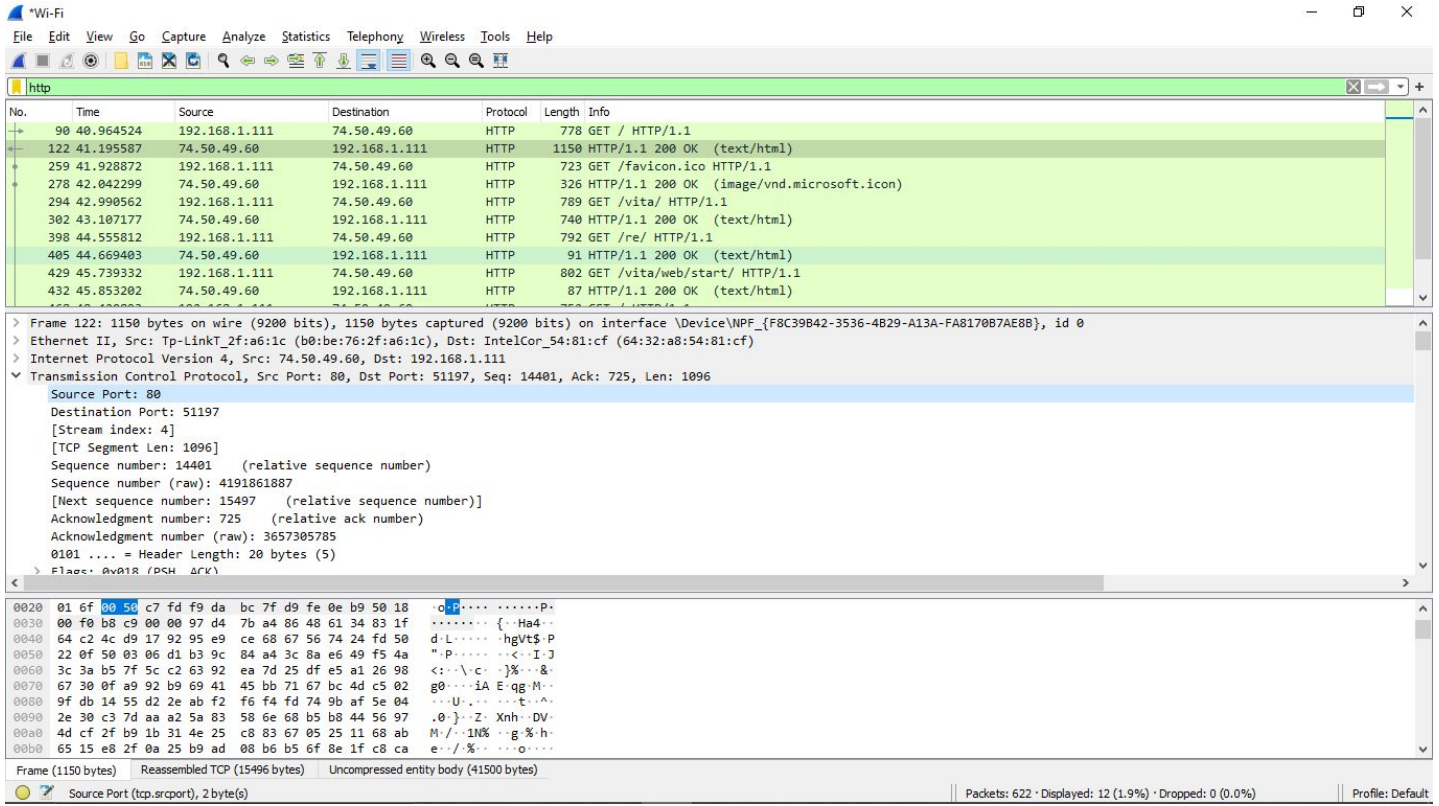
Wireshark

É um sniffer, ele captura o tráfego endereçado/destinado à placa de rede local

Tem a possibilidade de utilizar filtros detalhados

https://www.wireshark.org/

Wireshark


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
90 40.964524 192.168.1.111 74.50.49.60 HTTP 778 GET / HTTP/1.1
122 41.195587 74.50.49.60 192.168.1.111 HTTP 1150 HTTP/1.1 200 OK (text/html)
259 41.928872 192.168.1.111 74.50.49.60 HTTP 723 GET /favicon.ico HTTP/1.1
278 42.042299 74.50.49.60 192.168.1.111 HTTP 326 HTTP/1.1 200 OK (image/vnd.microsoft.icon)
294 42.990562 192.168.1.111 74.50.49.60 HTTP 789 GET /vita/ HTTP/1.1
302 43.107177 74.50.49.60 192.168.1.111 HTTP 740 HTTP/1.1 200 OK (text/html)
398 44.555812 192.168.1.111 74.50.49.60 HTTP 792 GET /re/ HTTP/1.1
405 44.669403 74.50.49.60 192.168.1.111 HTTP 91 HTTP/1.1 200 OK (text/html)
429 45.739332 192.168.1.111 74.50.49.60 HTTP 802 GET /vita/web/start/ HTTP/1.1
432 45.853202 74.50.49.60 192.168.1.111 HTTP 87 HTTP/1.1 200 OK (text/html)
Frame 122: 1150 bytes on wire (9200 bits), 1150 bytes captured (9200 bits) on interface \Device\NPF_{F8C39B42-3536-4B29-A13A-FA8170B7AE8B}, id 0
Ethernet II, Src: Tp-LinkT_2f:a6:1c (b0:be:76:2f:a6:1c), Dst: IntelCor_54:81:cf (64:32:a8:54:81:cf)
Internet Protocol Version 4, Src: 74.50.49.60, Dst: 192.168.1.111
Transmission Control Protocol, Src Port: 80, Dst Port: 51197, Seq: 14401, Ack: 725, Len: 1096
Source Port: 80
Destination Port: 51197
[Stream index: 4]
[TCP Segment Len: 1096]
Sequence number: 14401 (relative sequence number)
Sequence number (raw): 4191861887
[Next sequence number: 15497 (relative sequence number)]
Acknowledgment number: 725 (relative ack number)
Acknowledgment number (raw): 3657305785
0101 .... = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
0020 01 6f 00 50 c7 fd f9 da bc 7f d9 fe 0e b9 50 18
0030 00 f0 b8 c9 00 00 97 d4 7b a4 86 48 61 34 83 1f
0040 64 c2 4c d9 17 92 95 e9 ce 68 67 56 74 24 fd 50
0050 22 0f 50 03 06 d1 b3 9c 84 a4 3c 8a e6 49 f5 4a
0060 3c 3a b5 7f 5c c2 63 92 ea 7d 25 df e5 a1 26 98
0070 67 30 0f a9 92 b9 69 41 45 bb 71 67 bc 4d c5 02
0080 9f db 14 55 d2 2e ab f2 f6 f4 fd 74 9b af 5e 04
0090 2e 30 c3 7d aa a2 5a 83 58 6e 68 b5 b8 44 56 97
00a0 4d cf 2f b9 1b 31 4e 25 c8 83 67 05 25 11 68 ab
00b0 65 15 e8 2f 0a 25 b9 ad 08 b6 b5 6f 8e 1f c8 ca
Frame (1150 bytes)
Reassembled TCP (15496 bytes)
Uncompressed entity body (41500 bytes)
Source Port (tcp.srcport), 2 byte(s)
Packets: 622 · Displayed: 12 (1.9%) · Dropped: 0 (0.0%)
Profile: Default

Telnet

Protocolo cliente-servidor usado para permitir a comunicação entre computadores ligados numa rede, baseado em TCP.

Permite o acesso remoto.

Não possui criptografia.

Para ativar o telnet: link

Telnet

HTTP

- Protocolo de transferência de hipertexto.
- Protocolo base da web, viabiliza a obtenção de objetos(páginas, imagens...)
- Usa o TCP como transportador
- Utiliza porta 80 como padrão

Métodos do HTTP

Alguns métodos do HTTP 1.1:

GET: busca um objeto definido por uma URL requisição

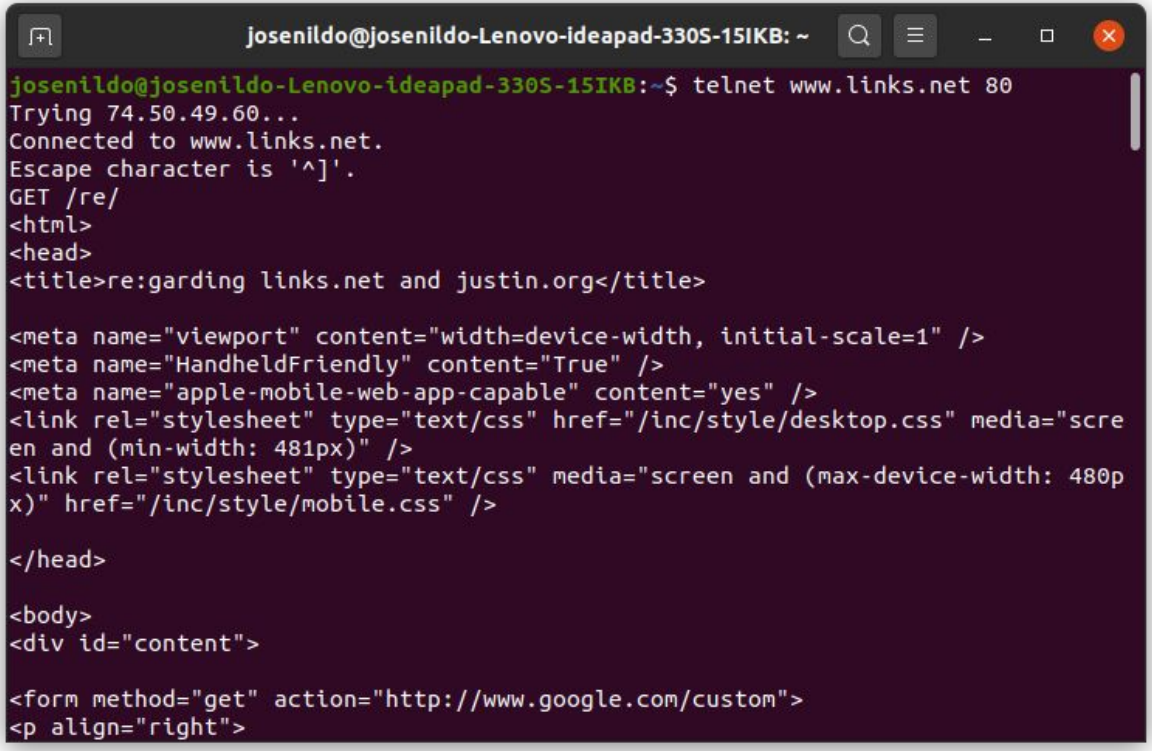
PUT: indica que os dados no corpo da consulta devem ser armazenados na URL especificada

POST: envia dados para serem processados pelo servidor no corpo da mensagem

HEAD: Similar ao método GET, mas retorna somente o cabeçalho da resposta do servidor

DELETE: apaga o arquivo especificado na URL

Exemplo de requisição HTTP



Alguns códigos de resposta

200 OK - conexão estabelecida e objeto requisitado encontrado

301 Moved Permanently - indica que houve um redirecionamento permanente. E, no campo Location do Head, está a nova localidade, o registro com a URL antiga deve ser alterado para a nova

304 Not Modified - usado quando o cliente utiliza cache, indicando que o objeto solicitado não foi alterado

404 Not Found - indica que o recurso não foi encontrado

403 - acesso negado

lista de códigos de estados http

Telnet

SMTP

- Usa TCP para transferência confiável e direta de mensagem de e-mail do cliente para o servidor
- Usa a porta 25

Experimento SMTP, envio de e-mail

telnet mail.cin.ufpe.br 25

HELO cin.ufpe.br

MAIL FROM:<seu email(Cln)>

RCPT TO:<email receptor(Cln)>

DATA

From: <seu email>

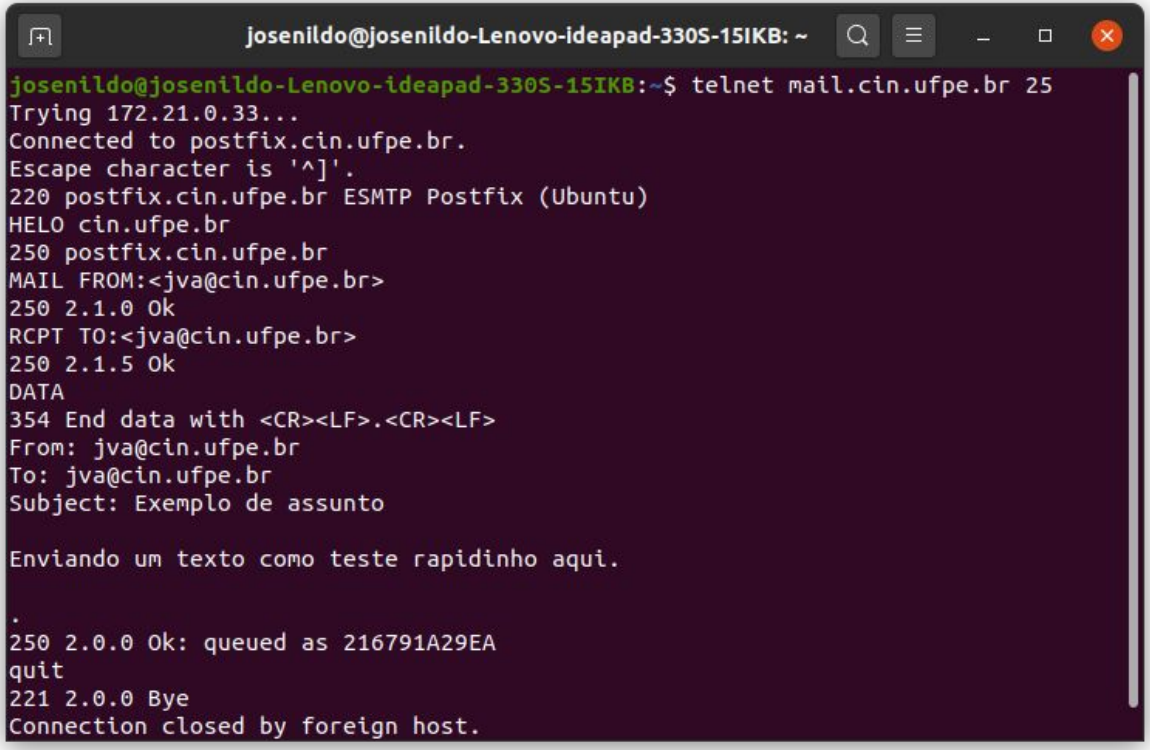
To: <email receptor>

Subject: Assunto

Conteúdo

.

Exemplo


josenildo@josenildo-Lenovo-ideapad-330S-15IKB: ~
josenildo@josenildo-Lenovo-ideapad-330S-15IKB:~$ telnet mail.cin.ufpe.br 25
Trying 172.21.0.33...
Connected to postfix.cin.ufpe.br.
Escape character is '^]'.
220 postfix.cin.ufpe.br ESMTP Postfix (Ubuntu)
HELO cin.ufpe.br
250 postfix.cin.ufpe.br
MAIL FROM:<jva@cin.ufpe.br>
250 2.1.0 Ok
RCPT TO:<jva@cin.ufpe.br>
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
From: jva@cin.ufpe.br
To: jva@cin.ufpe.br
Subject: Exemplo de assunto
Enviando um texto como teste rapidinho aqui.
.
250 2.0.0 Ok: queued as 216791A29EA
quit
221 2.0.0 Bye
Connection closed by foreign host.

Exercício

Envie um email pelo terminal para jva@cin.ufpe.br

Coloque no assunto: [Exercicio de monitoria 1 InfraCom] - seu nome

No corpo da mensagem coloque seu nome completo e login

DNS

Sistema de nomes de domínios

Banco de dados distribuído entre servidores hierárquicos

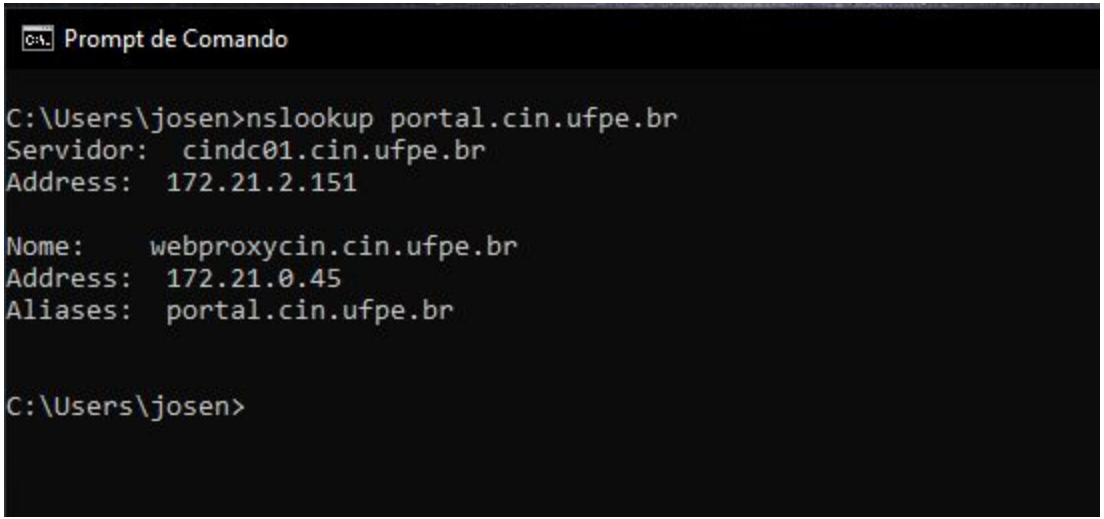
São os responsáveis por localizar e traduzir para números IP os endereços ‘nominais’ que digitamos nos navegadores

NSLOOKUP

Ferramenta utilizada para obter informações sobre registros de DNS de um determinado domínio, host ou IP

comando: nslookup [domínio]

NSLOOKUP


Prompt de Comando
C:\Users\josen>nslookup portal.cin.ufpe.br
Servidor: cindc01.cin.ufpe.br
Address: 172.21.2.151
Nome: webproxycin.cin.ufpe.br
Address: 172.21.0.45
Aliases: portal.cin.ufpe.br
C:\Users\josen>

WHOIS

Repositório público que reúne os dados de todos os domínios registrados no mundo.

https://registro.br/tecnologia/ferramentas/whois/