Fundamentos de Redes

Objectives

- Basic study of FTP, DNS; and HTTP.

FTP

1. In a Linux terminal, access a FTP server (forcing IPv4) and download a file:

```
ftp -4 speedtest.tele2.net
```

Use *anonymous* as login name, with no password.
List all files in root, download file *2MB.zip* from the server, and quit:

```
ls
get 2MB.zip
quit
```

>> Based on the captured packets, identify and analyze the TCP sessions (including sequence and acknowledge numbers and flags).
>> Analyze the exchanged FTP commands.
Note: Wireshark packet decoding (by default) uses relative TCP sequence numbers, i.e., the first packet TCP sequence number is always shown as zero and all following sequence numbers are adjusted accordingly. In reality, the first sequence number is not zero.

DNS

2. Start a Wireshark capture and in a Linux terminal perform multiple DNS queries:

```
nslookup www.up.pt
nslookup google.com
nslookup -q=AAAA www.up.pt
nslookup -q=MX www.up.pt
```

>> Analyze the captured DNS packets.
Note: Is no packets appear, means that the local DNS cache already contain the query result. Test with other domain names.

HTTP

3.1. Start a Wireshark capture for HTTP packets. With a browser access the following URL:

```
www.ua.pt
```

>> Analyze the format of a GET HTTP message.
>> What's the purpose of the 200 HTTP response?

3.2. In a Linux terminal, with the curl application, get the HTTP contents of the following URL:

```
curl http://www.cgd.pt
curl http://www.bpi.pt
curl http://www.bancobpi.pt
```

>> What's the purpose of the 302 HTTP response?
Note: if *curl* is not found, install it: `sudo apt install curl`

3.3. In a Linux terminal, with the curl application, get the HTTP contents of the following URL:

```
curl http://www.ua.pt/erro1
```

>> What's the purpose of the 404 HTTP response?

3.4. In a Linux terminal send a POST HTTP message with the curl application:

```
curl -d "param1=value1&param2=value2" -X POST http://wwww.sapo.pt
```

>> Analyze the format of a POST HTTP message.