

05

Mão à obra: Analisando tráfego com o Wireshark

Iremos agora verificar o que um usuário mal intencionado poderá fazer para analisar protocolos que estão passando na rede.

- Abra o Wireshark, que deve ter sido instalado junto com o GNS3.
- Escolha a placa de rede de seu computador.
- No filtro, coloque o protocolo `HTTP`.

The screenshot shows the Wireshark interface with the following details:

- File menu:** Wi-Fi, File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help.
- Toolbar:** Standard icons for opening files, capturing, analyzing, and saving.
- Packet List:** Shows 42 captured packets. The first few are highlighted in blue, indicating they are selected. The columns are: No., Time, Source, Destination, Protocol, Length, and Info.
- Selected Packet:** The first selected packet (No. 36) is highlighted in blue. The Info column shows: "215 M-SEARCH * HTTP/1.1". The details pane below shows the raw hex and ASCII data for this packet.
- Details pane:** Shows the raw hex and ASCII representation of the selected packet.
- Bottom status bar:** "Packets: 753 - Displayed: 42 (5.6%)" and "Profile: Default".

- Como fizemos no vídeo, abra um site que utilize o protocolo `HTTP`, por exemplo o [blog da Alura](http://blog.alura.com.br/) (<http://blog.alura.com.br/>).
- Volte para o Wireshark e procure pela requisição `GET`.

Tente encontrar na análise mais detalhada, informações da página acessada. Qual o resultado?