

- In verde sono evidenziati i MAC address (in particolare i MAC address sono le stringhe esadecimali fra le parentesi tonde).
- In rosso è evidenziato il contenuto della richiesta.
- La principale differenza fra le due modalità è evidenziata invece in giallo nello screen HTTPS, in quanto presente solo lì. Si tratta dell'encrypted alert, elemento presente nella comunicazione HTTPS e assente nella comunicazione HTTP. Il protocollo HTTPS infatti, al contrario di HTTP, è un protocollo sicuro e cifrato.

The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Help, and various tool icons. The main window is divided into three panes: Packet List, Packet Details, and Packet Bytes.

- Packet List:** Shows a list of captured packets. Packet 11, an HTTP GET request, is highlighted with a red box. The list includes columns for No., Time, Source, Destination, Protocol, and Length.
- Packet Details:** Provides a hierarchical view of the selected packet's structure. For the HTTP GET request, it shows the Request Line, Headers, and Body. The 'Hypertext Transfer Protocol' section is expanded, showing the request line and various headers.
- Packet Bytes:** Displays the raw data of the packet in hexadecimal and ASCII. The data is organized into columns representing different parts of the packet.

The interface also shows a status bar at the bottom indicating the current capture source as 'Ethernet (eth0, 14 bytes)' and the packet count as 'Packets: 23 (100.0%)'.