

The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes options like Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for packet capture and analysis. The main window is divided into three panes: the packet list, packet details, and packet bytes.

The packet list pane shows a list of captured packets. The first 16 packets are displayed, with columns for Time, Source, Destination, Protocol, Length, and Info. The packets are as follows:

Time	Source	Destination	Protocol	Length	Info
7 0.021264250	127.0.0.1	127.0.0.1	TCP	66	45930 →
8 0.021273042	127.0.0.1	127.0.0.1	HTTP	324	HTTP/1.1
9 0.021275000	127.0.0.1	127.0.0.1	TCP	66	45930 →
10 0.023060208	127.0.0.1	127.0.0.1	TCP	66	80 → 459
11 0.026094833	127.0.0.1	127.0.0.1	TCP	66	45930 →
12 0.026128667	127.0.0.1	127.0.0.1	TCP	66	80 → 459
13 12.980775548	127.0.0.1	127.0.0.1	DNS	81	Standard
14 12.980906173	127.0.0.1	127.0.0.1	ICMP	109	Destinat
15 12.980929631	127.0.0.1	127.0.0.1	DNS	81	Standard
16 12.980935006	127.0.0.1	127.0.0.1	ICMP	109	Destinat

The packet details pane shows the structure of the selected packet (packet 14). It includes the following fields:

- Ethernet II, Src: 00:00:00:00:00:00 (00:00:00:00:00:00), Dst: 00:00:00:00:00:00 (00:00:00:00:00:00)
- Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
- Transmission Control Protocol, Src Port: 45930, Dst Port: 80

The packet bytes pane shows the raw data of the selected packet in hexadecimal and ASCII format. The data is as follows:

```

0000  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0010  00 3c 2a 97 40 00 40 06 12 23 7f 00 00 00 00 00
0020  00 01 b3 6a 00 50 1f ba 15 ad 00 00 00 00 00 00
0030  82 00 fe 30 00 00 02 04 ff d7 04 02 08 00 00 00
0040  01 48 00 00 00 00 01 03 03 07
  
```

The status bar at the bottom of the interface shows the file name "wireshark_loFOD3J2.pcapng", the number of packets "Packets: 172", the number of displayed packets "Displayed: 172 (100.0%)", and the profile "Profile: Default".

```
* syslog_514_udp - started (PID 8055)
* discard_9_udp - started (PID 8063)
* ntp_123_udp - started (PID 8052)
* quotd_17_udp - started (PID 8065)
* dummy_1_udp - started (PID 8069)
* daytime_13_udp - started (PID 8059)
* dummy_1_tcp - started (PID 8068)
* discard_9_tcp - started (PID 8062)
* pop3_110_tcp - started (PID 8046)
* daytime_13_tcp - started (PID 8058)
* time_37_tcp - started (PID 8056)
* chargen_19_udp - started (PID 8067)
* time_37_udp - started (PID 8057)
* ident_113_tcp - started (PID 8054)
* chargen_19_tcp - started (PID 8066)
* ftp_21_tcp - started (PID 8048)
* echo_7_udp - started (PID 8061)
* pop3s_995_tcp - started (PID 8047)
* finger_79_tcp - started (PID 8053)
* tftp_69_udp - started (PID 8050)
* quotd_17_tcp - started (PID 8064)
* echo_7_tcp - started (PID 8060)
* https_443_tcp - started (PID 8043)
* ftps_990_tcp - started (PID 8049)
done.
Simulation running.
```