3.19. The "Packet Details" pane 3/23/16, 10:10 PM

3.19. The "Packet Details" pane

The packet details pane shows the current packet (selected in the "Packet List" pane) in a more detailed form.

Figure 3.17. The "Packet Details" pane

```
> Ethernet II, Src: Globalsc 00:3b:0a (f0:ad:4e:00:3b:0a), Dst: Vizio 14:8a:e1 (00:19:9d:14:8a:e1)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.21
> User Datagram Protocol, Src Port: 53 (53), Dst Port: 34036 (34036)

✓ Domain Name System (response)

     [Request In: 1]
     [Time: 0.055880000 seconds]
     Transaction ID: 0x403d
  > Flags: 0x8180 Standard query response, No error
     Ouestions: 1
     Answer RRs: 2
     Authority RRs: 8
     Additional RRs: 8
  > Queries
  > Answers
  > Authoritative nameservers
  > Additional records
```

This pane shows the protocols and protocol fields of the packet selected in the "Packet List" pane. The protocols and fields of the packet shown in a tree which can be expanded and collapsed.

There is a context menu (right mouse click) available. See details in <u>Figure 6.5, "Pop-up menu of the "Packet Details" pane"</u>.

Some protocol fields have special meanings.

- **Generated fields.** Wireshark itself will generate additional protocol information which isn't present in the captured data. This information is enclosed in square brackets ('[' and ']'). Generated information includes response times, TCP analysis, GeoIP information, and checksum validation.
- Links. If Wireshark detects a relationship to another packet in the capture file it will generate a link to that packet. Links are underlined and displayed in blue. If you double-clicked on a link Wireshark will jump to the corresponding packet.