### decodedns

Decodes the DNS request and response packets.

#### Syntax

decodedns

#### Description

The output fields are as follows:

* **additionals**: Other additional records (array)
* **answers**: Answer resource records from the DNS server (array)
* **authorities**: Information of authoritative DNS servers (array)
* **bytes**: Size (integer) of the DNS payload
* **direction**: Direction of the transaction (string)
* c->s: Request from the client
* s->c: Response from the server
* **domain**: Domain address to be queried (string)
* **dst\_ip**: Destination IP address of the DNS transaction (IP address)
* **dst\_port**: Destination port of the DNS transaction (integer)
* **flags**: DNS header flag. Refer to: [https://www.iana.org/assignments/dns-parameters/dns-parameters.xhtml#dns-parameters-12](https://www.iana.org/assignments/dns-parameters/dns-parameters.xhtml)
* **ip**: IP address connected to the domain address (IP address)
* **src\_ip**: Source IP address of the DNS transaction (IP address)
* **src\_port**: Source port of the DNS transaction (integer)
* **status**: Query result. If there is an error, an error message is displayed.
* FORMAT\_ERROR: The DNS server could not interpret the request.
* NAME\_ERROR: The domain name in the request does not exist.
* NO\_ERROR: No error.
* NOT\_IMPLEMENTED: The DNS server does not support the type of request.
* REFUSED: The DNS server refused the request.
* SERVER\_FAILURE: The DNS server was unable to process the request due to an internal server error.
* **txid**: DNS transaction ID (hexadecimal string)
* **type**: DNS record type (strings such as A, AAAA, CNAME, MX, NS, PTR, SOA, SRV, TXT). Refer to: [https://www.iana.org/assignments/dns-parameters/dns-parameters.xhtml#dns-parameters-4](https://www.iana.org/assignments/dns-parameters/dns-parameters.xhtml)

#### Usage

Decode DNS packets from a pcap file.

pcapfile /opt/logpresso/pcap/abnormal\_traffic.pcap | decodedns