### decodedns

指定したパケットをDNSプロトコルに基づいて解析し、出力します。

#### 構文

decodedns

#### 説明

出力されるフィールドは以下の通りです。

* **additionals**: その他関連レコード（配列）
* **answers**: DNSサーバーの応答メッセージ原文（配列）
* **authorities**: 権限のあるDNSサーバーに関する情報（配列）
* **bytes**: DNS応答ペイロードのサイズ（整数）
* **direction**: トランザクションの方向（文字列）
* c->s: クライアントからのリクエスト
* s->c: サーバーからのレスポンス
* **domain**: クエリ対象のドメインアドレス（文字列）
* **dst\_ip**: DNSトランザクションの宛先IPアドレス。通常はDNSサーバーのアドレス（IPアドレス）
* **dst\_port**: DNSトランザクションの宛先ポート（整数）
* **flags**: DNSヘッダーフラグ。参照: [https://www.iana.org/assignments/dns-parameters/dns-parameters.xhtml#dns-parameters-12](https://www.iana.org/assignments/dns-parameters/dns-parameters.xhtml)
* **ip**: ドメインアドレスに関連付けられたIPアドレス（IPアドレス）
* **src\_ip**: DNSトランザクションの送信元IPアドレス（IPアドレス）
* **src\_port**: DNSトランザクションの送信元ポート（整数）
* **status**: クエリ実行結果（エラーがある場合はエラーメッセージを表示）
* FORMAT\_ERROR: クエリ内容に誤りがあり、サーバーで処理できない
* NAME\_ERROR: クエリされたドメインアドレスが存在しない
* NO\_ERROR: エラーなし
* NOT\_IMPLEMENTED: DNSサーバーが要求されたクエリをサポートしていない
* REFUSED: DNSサーバーによる応答拒否
* SERVER\_FAILURE: サーバーエラーによりクエリを処理できない
* **txid**: DNSトランザクションID（16進数文字列）
* **type**: DNSレコードタイプ（A, AAAA, CNAME, MX, NS, PTR, SOA, SRV, TXT）。参照: [https://www.iana.org/assignments/dns-parameters/dns-parameters.xhtml#dns-parameters-4](https://www.iana.org/assignments/dns-parameters/dns-parameters.xhtml)。

#### 使用例

任意のPCAPファイルからDNS通信のみを抽出

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

#### 互換性

decodednsコマンドは、ENT #2309 2019-11-27\_10-43バージョン以降でサポートされています。