### decodedns

PCAP 파일에서 DNS 쿼리 내용을 디코딩해 보여줍니다. 패킷 단위로 디코딩하려면 pcapdecode 명령을 이용하십시오.

#### 문법

decodedns

#### 설명

출력하는 필드는 다음과 같습니다.

* **additionals**: 기타 관련 레코드(배열)
* **answers**: DNS 서버의 응답 메시지 원본(배열)
* **authorities**: 권한있는 DNS 서버에 관한 정보(배열)
* **bytes**: DNS 응답 페이로드의 크기(정수)
* **direction**: 트랜잭션 방향(문자열)
* c->s: 클라이언트의 요청
* s->c: 서버의 응답
* **domain**: 질의 대상 도메인 주소(문자열)
* **dst\_ip**: DNS 트랜잭션의 목적지 IP 주소. 일반적으로 DNS 서버의 주소(IP 주소)
* **dst\_port**: DNS 트랜잭션의 목적지 포트(정수)
* **flags**: DNS 헤더 플래그. 참조: [https://www.iana.org/assignments/dns-parameters/dns-parameters.xhtml#dns-parameters-12](https://www.iana.org/assignments/dns-parameters/dns-parameters.xhtml)
* **ip**: 도메인 주소와 연결된 IP 주소(IP 주소)
* **src\_ip**: DNS 트랜잭션의 출발지 IP 주소(IP 주소)
* **src\_port**: DNS 트랜잭션의 출발지 포트(정수)
* **status**: 쿼리 실행 결과(오류가 있으면 오류 메시지 표시)
* FORMAT\_ERROR: 질의 내용에 오류가 있어 서버가 처리할 수 없음
* NAME\_ERROR: 질의한 도메인 주소가 존재하지 않음
* NO\_ERROR: 오류 없음
* NOT\_IMPLEMENTED: DNS 서버가 요청한 질의를 지원하지 않음
* REFUSED: DNS 서버의 응답 거부
* SERVER\_FAILURE: 서버 오류로 질의를 처리할 수 없음
* **txid**: DNS 트랜잭션 ID(16진수 문자열)
* **type**: DNS 레코드 타입(A, AAAA, CNAME, MX, NS, PTR, SOA, SRV, TXT). 참조: [https://www.iana.org/assignments/dns-parameters/dns-parameters.xhtml#dns-parameters-4](https://www.iana.org/assignments/dns-parameters/dns-parameters.xhtml).

#### 사용 예

임의의 PCAP 파일에서 DNS 통신만 디코딩

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

#### 호환성

decodedns 명령어는 ENT #2309 2019-11-27\_10-43 버전부터 지원합니다.