### decodesflow

sFLow 패킷을 디코딩합니다.

#### 문법

decodesflow

#### 설명

출력하는 필드는 다음과 같습니다.

* **agent\_addr**: 에이전트의 IP 주소
* **agent\_id**: 에이전트 식별자
* **counters**: **sampling\_type**이 counters일 때 다음과 같은 맵 형태 정보를 출력
* **admin\_status**: 관리자 포트 활성화 여부(true, false)
* **if\_direction** (0: 알 수 없음, 1: Full-duplex, 2: Half-duplex, 3: 수신, 4: 송신)
* **if\_index**: 인터페이스 식별자
* **if\_speed**: 연결 링크 bps
* **if\_type**: 이더넷은 6, 그 외 번호는 IANA가 할당한 인터페이스 타입 표준 번호 참조: <https://ietf.org/assignments/ianaiftype-mib/ianaiftype-mib>("IANAifType ::= TEXTUAL-CONVENTION", "SYNTAX INTEGER" 섹션)
* **in\_bcast\_pkts**: 받은 브로드캐스트 패킷 개수
* **in\_discards**: 받은 패킷 중 버려진 개수
* **in\_errors**: 받은 패킷 중 오류가 있는 패킷 개수
* **in\_mcast\_pkts**: 받은 멀티캐스트 패킷 개수
* **in\_octets**: 받은 용량(bytes)
* **in\_ucast\_pkts**: 받은 유니캐스트 패킷 개수
* **in\_unknown\_protos**: 받은 패킷 중에서 프로토콜을 알 수 없는 패킷 개수
* **oper\_status**: 실제 링크 활성화 여부(true, false)
* **out\_bcast\_pkts**: 보낸 브로드캐스트 패킷 개수
* **out\_discards**: 보낼 패킷 중에서 버려진 개수
* **out\_errors**: 보낼 패킷 중에서 오류가 있는 패킷 개수
* **out\_mcast\_pkts**: 보낸 멀티캐스트 패킷 개수
* **out\_octets**: 보낸 용량(bytes)
* **out\_ucast\_pkts**: 보낸 유니캐스트 패킷 개수
* **promisc\_mode**: 모든 패킷 수신 활성화 여부(true, false)
* **drops**: 성능 부족으로 손실된 패킷 개수. **sampling\_type**이 flow일 때 정보를 출력
* **dst\_ip**: 목적지 IP 주소. 일반적으로 sFlow 수집 서버의 주소를 표시.
* **dst\_port**: 목적지 포트 번호
* **flow**: **sampling\_rate**에 따라 무작위로 샘플링한 패킷
* **flow\_seq**: **src\_id**별로 샘플을 생성할 때마다 1씩 증가
* **flows**: **sampling\_type**이 flow일 때 샘플링한 플로우 데이터 정보를 출력
* **frame\_length**: 샘플링 하기 전 패킷의 길이(bytes)
* **header**: 이더넷 헤더 옥텟 바이트 스트림
* **protocol**: 연결 계층 프로토콜(예: ethernet)
* **stripped**: 연결 계층 헤더 옥텟을 추출하기 전에 패킷에서 제거된 옥텟 개수
* **input\_if\_index**: **sampling\_type**이 flow일 때 받은 인터페이스 식별자 정보를 출력
* **output\_if\_index**: **sampling\_type**이 flow일 때 보낸 인터페이스 식별자 정보를 출력
* **protocol**: 전송 계층 프로토콜(udp)
* **sample\_pool**: 샘플링 대상 원본 개수. **sampling\_type**이 flow일 때 정보를 출력
* **sample\_type**: 샘플링 종류
* **sampling\_rate**: 샘플링 비율. 지정된 패킷 개수 중에서 1개 추출. **sampling\_type**이 flow일 때 정보를 출력
* **src\_id**: 인터페이스 식별 번호
* **src\_id\_type**: RFC 2613에 정의된 인터페이스 타입(0: ifIndex, 1: smonVlanDataSource, 2: entPhysicalEntry). 관련 내용은 RFC 2613, "Remote Network Monitoring MIB Extensions for Switched Networks Version 1.0"에서 3.1.1 DataSource Objects 참조: <https://tools.ietf.org/html/rfc2613>
* **src\_ip**: 출발지 IP 주소. 일반적으로 sFlow 에이전트의 주소를 표시.
* **src\_port**: 출발지 포트 번호
* **uptime**: 에이전트의 부팅 후 가동 시간
* **ver**: sflow 버전(버전 5만 지원)

#### 사용 예

pcapfile /opt/logpresso/sonar/sflow.cap | decodesflow