### pcapreplay

指定したPCAP送受信デバイスを通じて、PCAPファイルに保存された通信を再現します。このコマンドの実行には管理者権限が必要です。受信したトラフィックをIPSやネットワーク通信解析装置のモニターポートへ送信する方式で応用できます。

#### 構文

pcapreplay device="DEVICE\_NAME" [pps=INT]

必須パラメータ

**device="DEVICE\_NAME"**

[system pcapdevices](https://docs.logpresso.comnull)コマンドで識別されたデバイスの中から、通信パケットを再現するネットワークインターフェースを指定します。インターフェースは**name**で識別されるデバイス名を指定してください。

オプションパラメータ

**pps=INT**

パケット送信速度をPPS（packets per second）単位で指定します。

#### 説明

このコマンドを動作させるには、ログプレッソ・ソナーを運用するシステムにlibpcapやwinpcapなどのドライバーがインストールされており、ログプレッソ・ソナープロセスがネットワークインターフェースに対してRAW I/Oを管理者権限で利用できる必要があります。

本コマンドは、受信したトラフィックをIPSやネットワークトラフィック解析装置のモニターポートへ送信する用途に適用できます。

テーブルに保存されたパケットデータを再現する場合は、[table](https://docs.logpresso.comnull)コマンドにorder=ascオプションを適用し、パケットを元の時系列順に並べ替えてください。

#### 使用例

直近5分間にtapped\_trafficテーブルへ保存されたレコードから**payload**フィールドを抽出し、PCAP送受信デバイスenp0s3から1,302,083pps（約1Gbps相当）の速度でトラフィックを送信

table order=asc duration=5m tapped\_traffic | fields payload | pcapreplay device="enp0s3" pps=1302083