
ネットワーク
解析ソフトの開発

目次

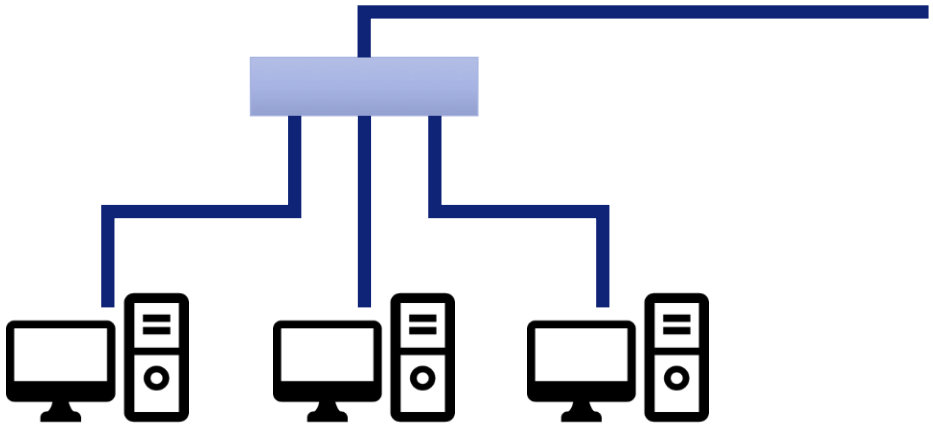
Pcap-qt

- ソフトウェアの概要
- 各機能説明
- ソフトウェアの今後の課題
- 感想と考察

ネットワークアナライザとは？

Pcap-qt

- ネットワークに流れるパケットを解析するソフトウェア
- トラブルシューティングに使われる
- ネットワークの流れがわかる！



要件と仕様

Pcap-qt

要件

・Linuxで稼働する

・ソフトウェアで提供する

・データを見やすく表示する

・DBへ暗号化し保存する

・ソフトウェアの利用制限がある

仕様

CentOS7 (x86_64)

C++とQtによる開発

パケット一覧・グラフ・リアルタイム可視化

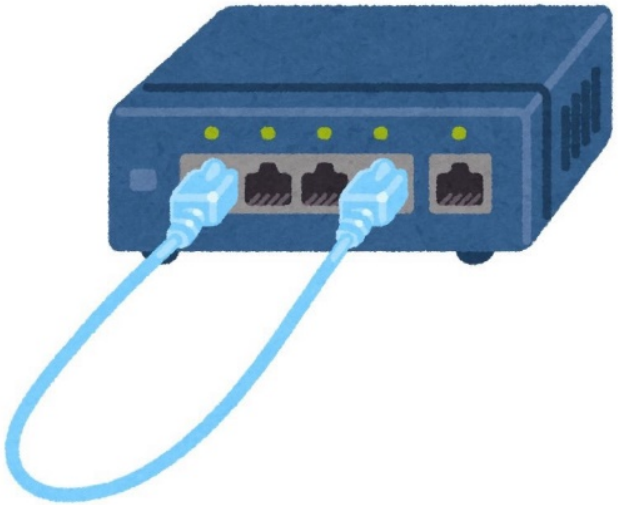
ログを暗号化して保存

管理者権限で使用可能

動作環境

Pcap-qt

- CentOS7 (64bit)
- Libpcap (1.5.3で動作確認)
- Qt (5.7/5.8で動作確認)
- MariaDB (10.1.3以降)
- データベース容量500MB（30日分のデータ格納可能）

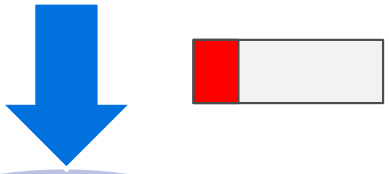


システム全体構成

Pcap-qt

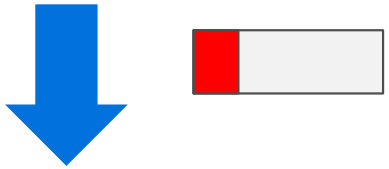
① デバイスを取得し，ユーザが選択する
② カーネルがパケットを取得する
③ libpcapがカーネルからユーザ
　プログラムへパケットをコピーする
③ パケットを解析する
④ パケットデータと
　ネットワーク統計をGUI表示する

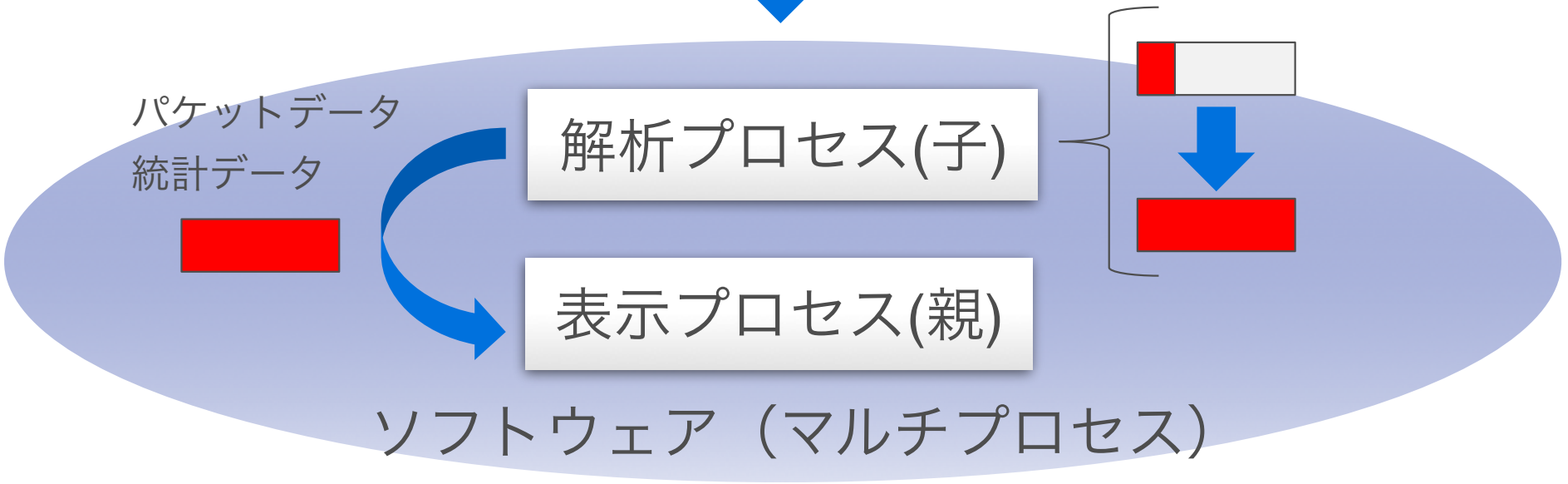
デバイス
（IEEE802.3仕様）



パケット
（ARP，IPv4）

Linux カーネル





システム全体構成

Pcap-qt

3つのプログラムを作成した
マルチプロセスで実行する

pcap-device

① デバイスを取得し，ユーザ
が選択する

pcap-capture

② カーネルがパケットを取得する
③ libpcapがカーネルからユーザ
プログラムへパケットをコピーする
③ パケットを解析する

pcap-qt

④ パケットデータと
ネットワーク統計をGUI表示する

ソフトウェア名

Pcap-qt

パケットの速度とフレームワークQtを意識した

スピード感のあるロゴの採用

パケットキャプチャ

Pcap-qt

キャプチャ可能なデータリンク

- IEEE802.3仕様

解析可能なプロトコル

- ARP
- IPv4
- TCP
- UDP
- ICMP
- DNS

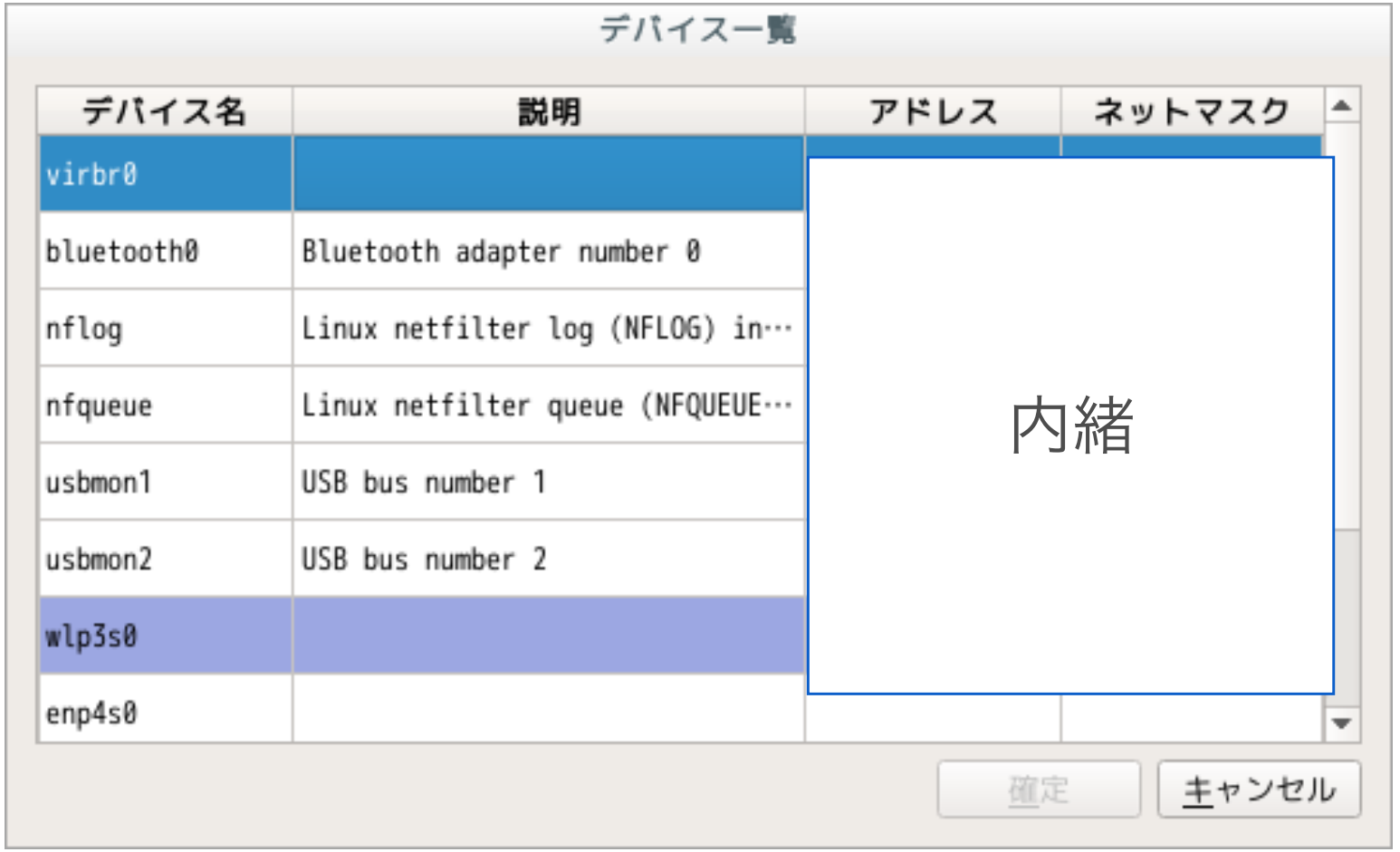
識別可能なプロトコル

- HTTP(S)
- FTP
- Telnet
- SSH
- DHCP
- NTP

デバイス選択

Pcap-qt

パケットキャプチャする**デバイス**を選択する



pcap-deviceから取得

メインフレーム（パケット一覧）

Pcap-qt

解析したパケットを表示する

エラーの有無・**プロトコル**ごとに色分け

pcap-captureから取得

メインフレーム（パケット詳細）

Pcap-qt

パケットの情報を詳しく表示する

IEEE802.3

IPv4

UDP

DNS

パケット詳細

```
パケットID [34]
[IEEE80
[IPv4]
 > IPパケット長 :62(ヘッダ :20)バイト
 > 識別子 + フラグメントオフセット :14251 + 16384 (0x37ab + 0x4000)
 > サービスタイプ :0x0
 > 生存時間(TTL) :64
 > ヘッダチェックサム :0x7d3b (エラーなし)
 > 送信元IPアドレス
 > 宛先IPアドレス :
[UDP] [10943] -> [53(DNS)] データグラム長:42
 > 送信元ポート番号 :10943
 > 宛先ポート番号 :53
 > チェックサム :0xb795 (エラーなし)
[DNS] id=40276:[問い合わせ(QUERY)] 再帰可能
 > Rcode :0(エラーなし)
 > 問い合わせ数 :1, 回答数 :0, オーソリティ数 :0, 追加情報数 :0
 > 質問          :mtalk.google.com, QType = 0x0001(A), QClass =
0x0001(IN)
```

DNSメッセージ

メインフレーム（生パケットデータ）

Pcap-qt

実際にネットワークを流れている
データを16進数で表示する

DNSメッセージ

パケットのフィルタリング

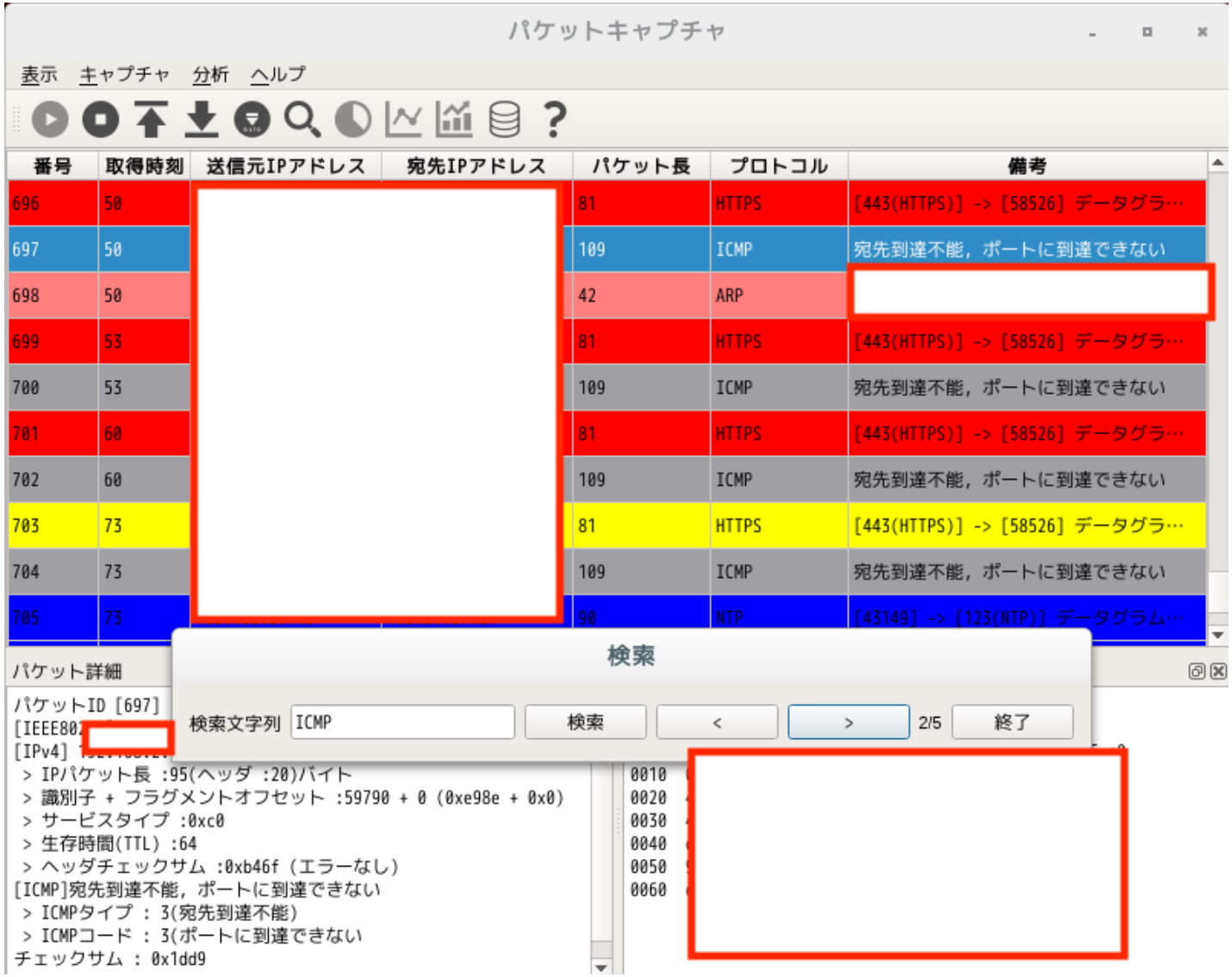
Pcap-qt

簡単なUIで，キャプチャするパケットを**絞り込む**

パケットの検索

Pcap-qt

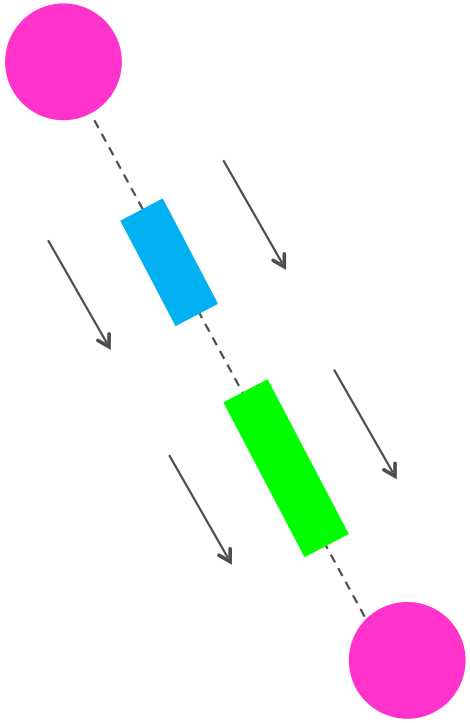
気になるパケットデータを**検索**する



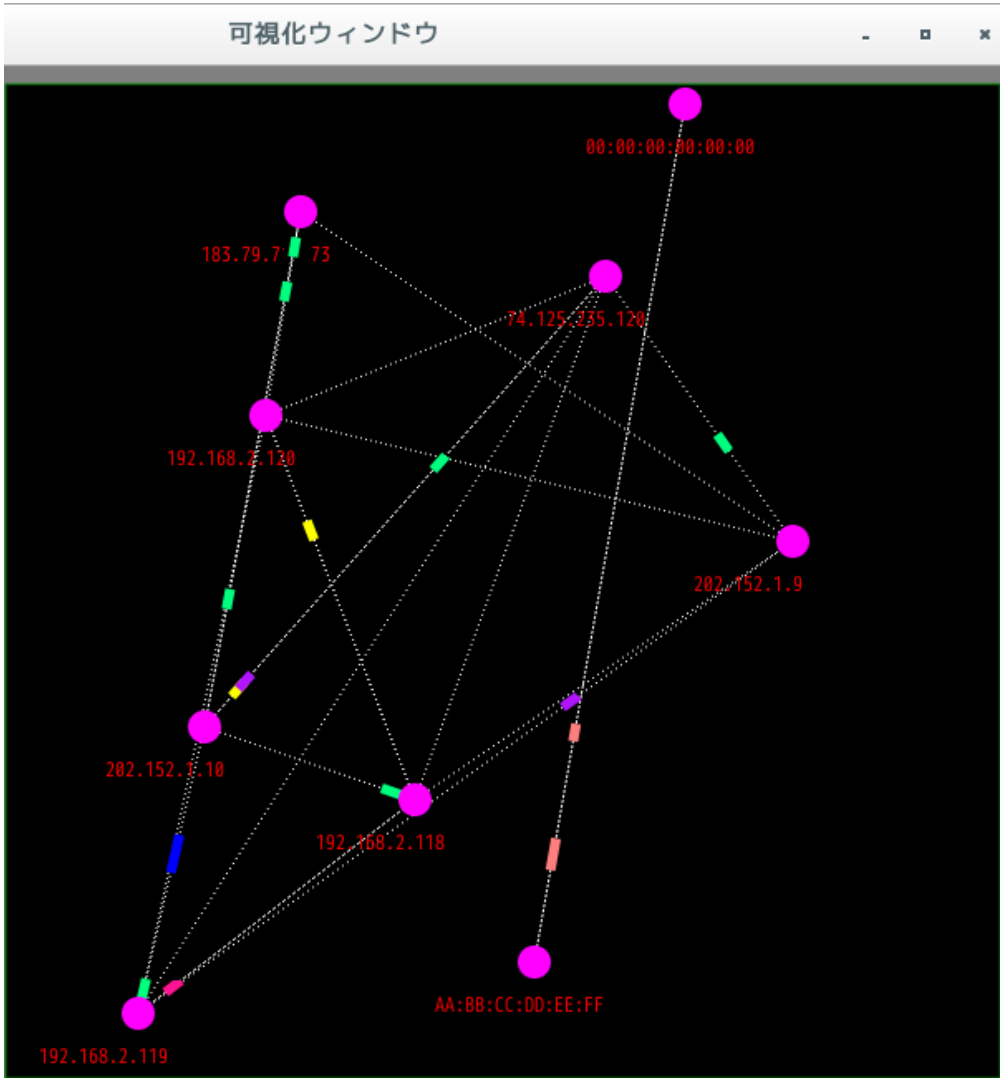
パケットの可視化

Pcap-qt

アニメーションでネットワークの流れを理解する



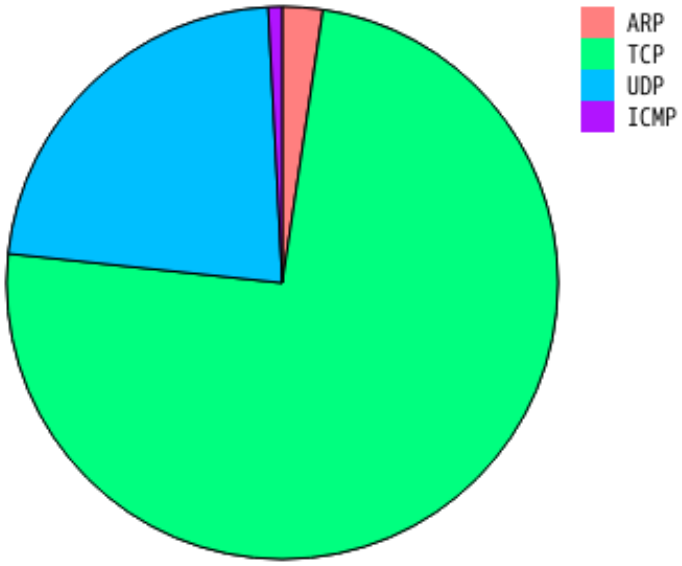
パケットが動く！

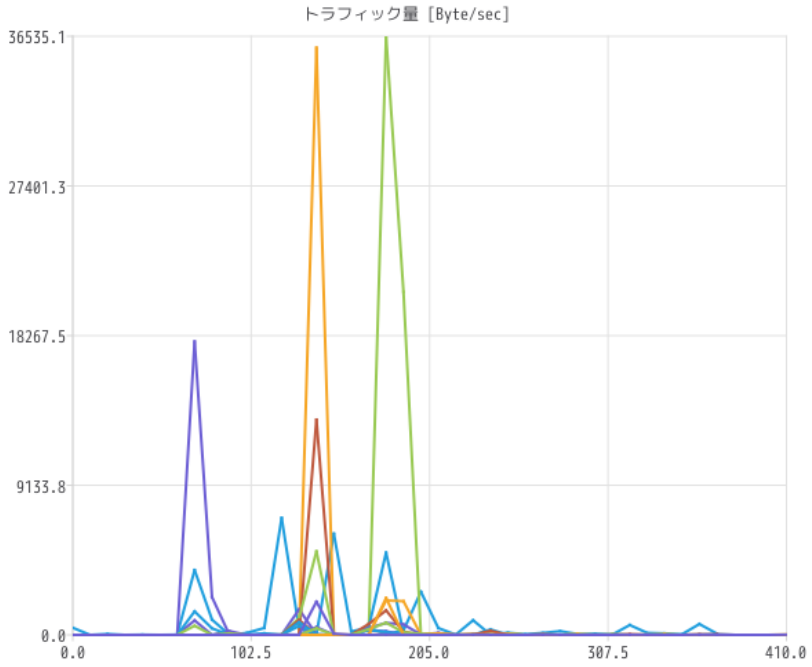


ネットワーク統計

Pcap-qt

- プロトコル統計
- トラフィック量統計

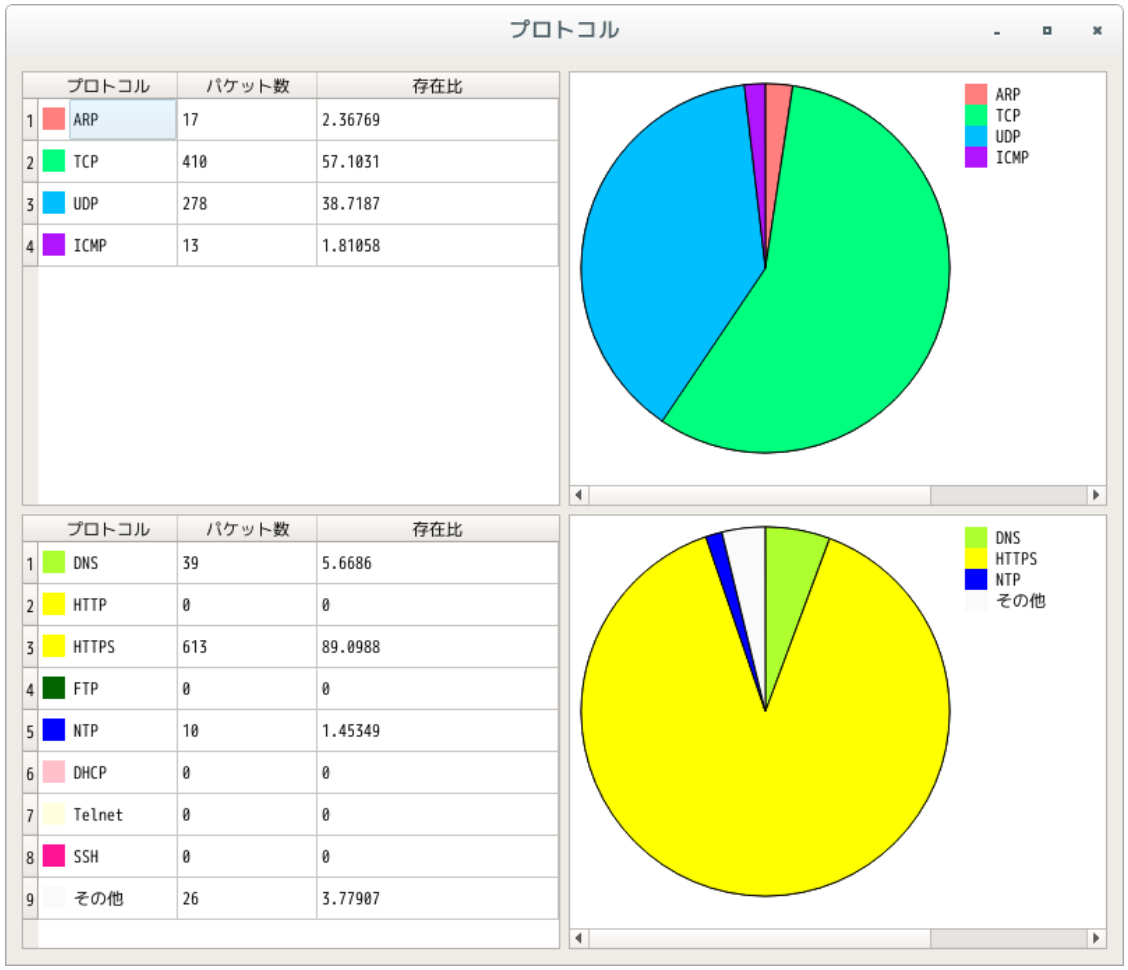




統計（プロトコル）

Pcap-qt

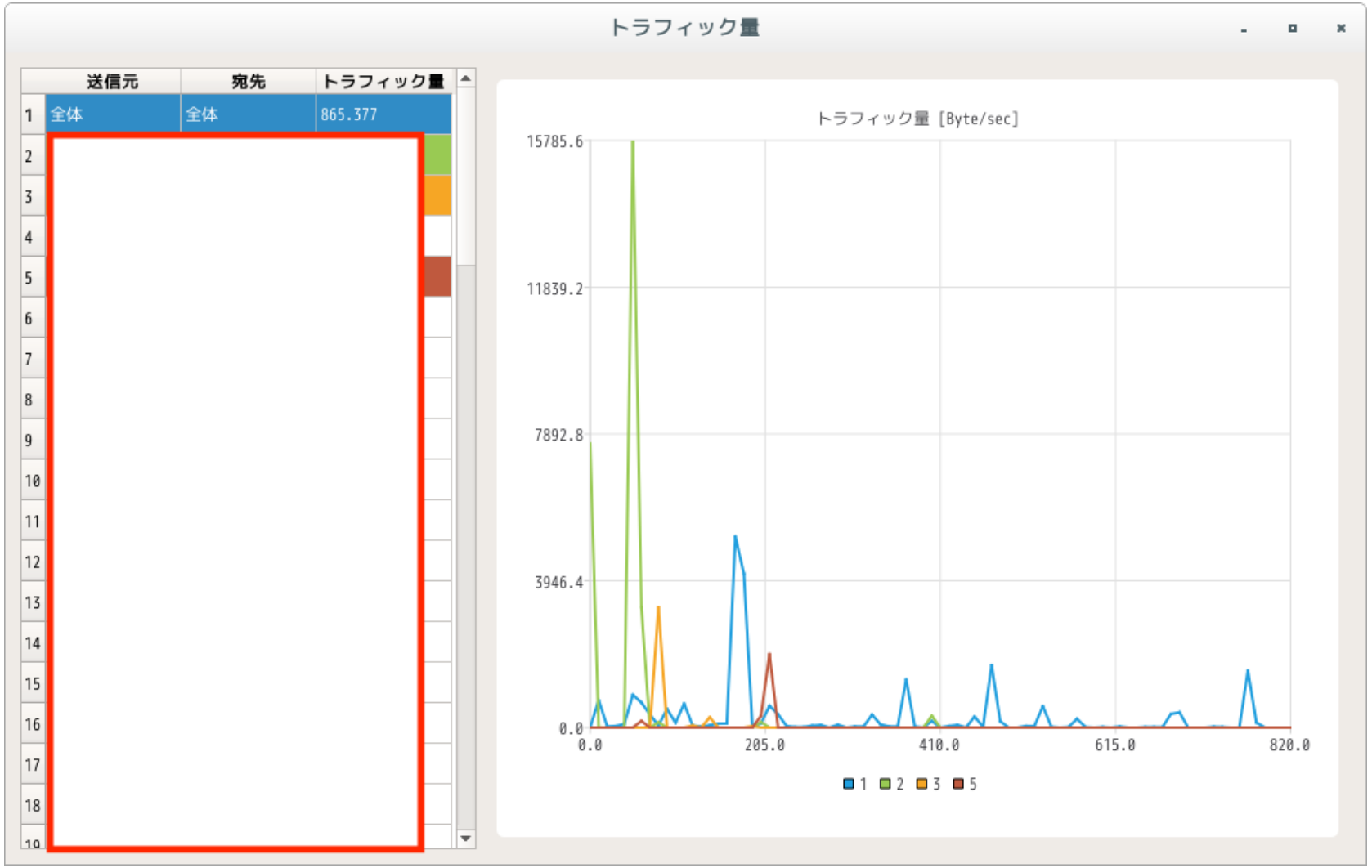
各プロトコルの割合を**円グラフ**で表示する



統計（トラフィック量）

Pcap-qt

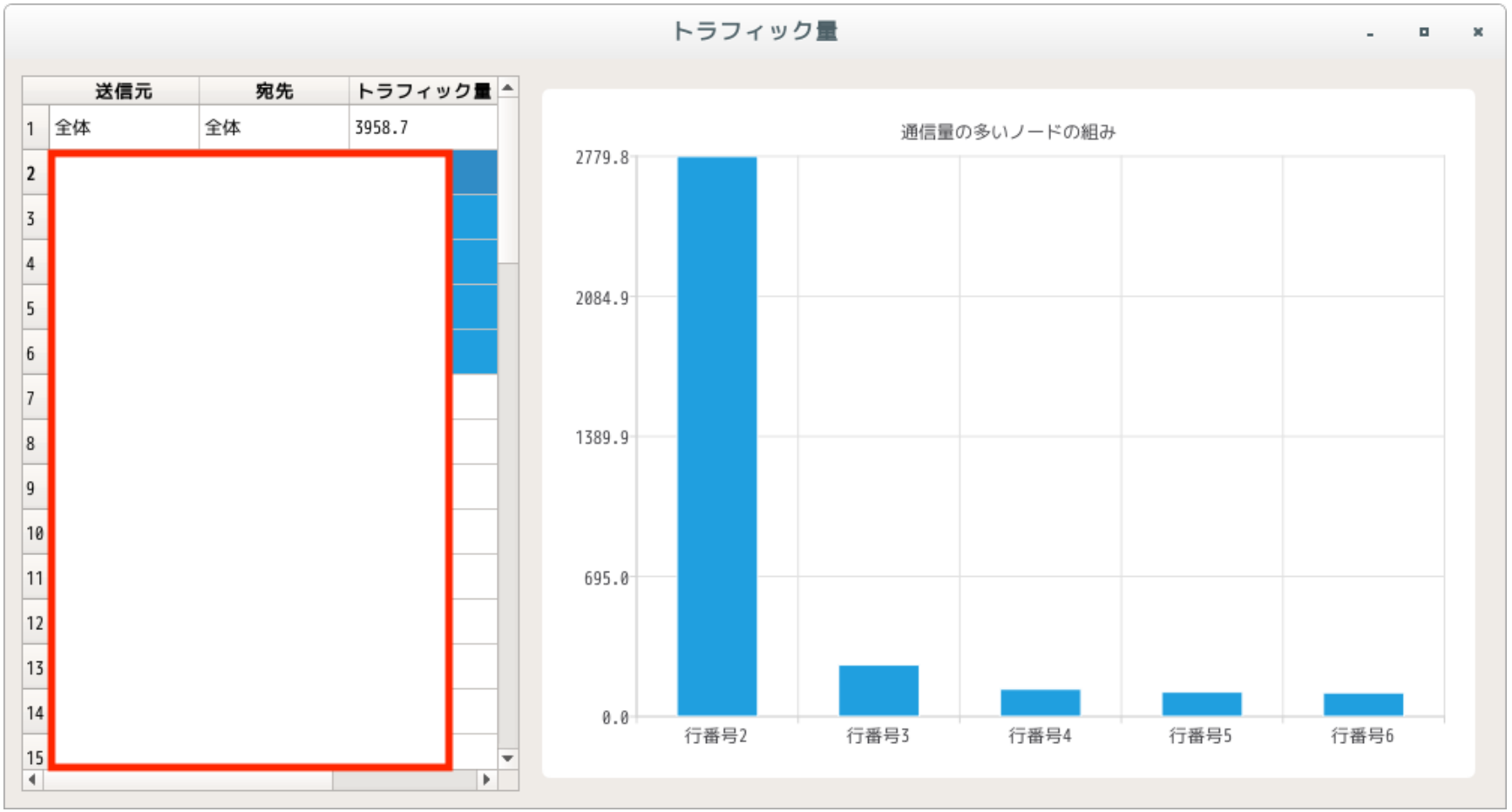
ノード間のトラフィック量を**折れ線グラフ**で表示する



統計（通信）

Pcap-qt

通信量の多い通信を**棒グラフ**で表示する

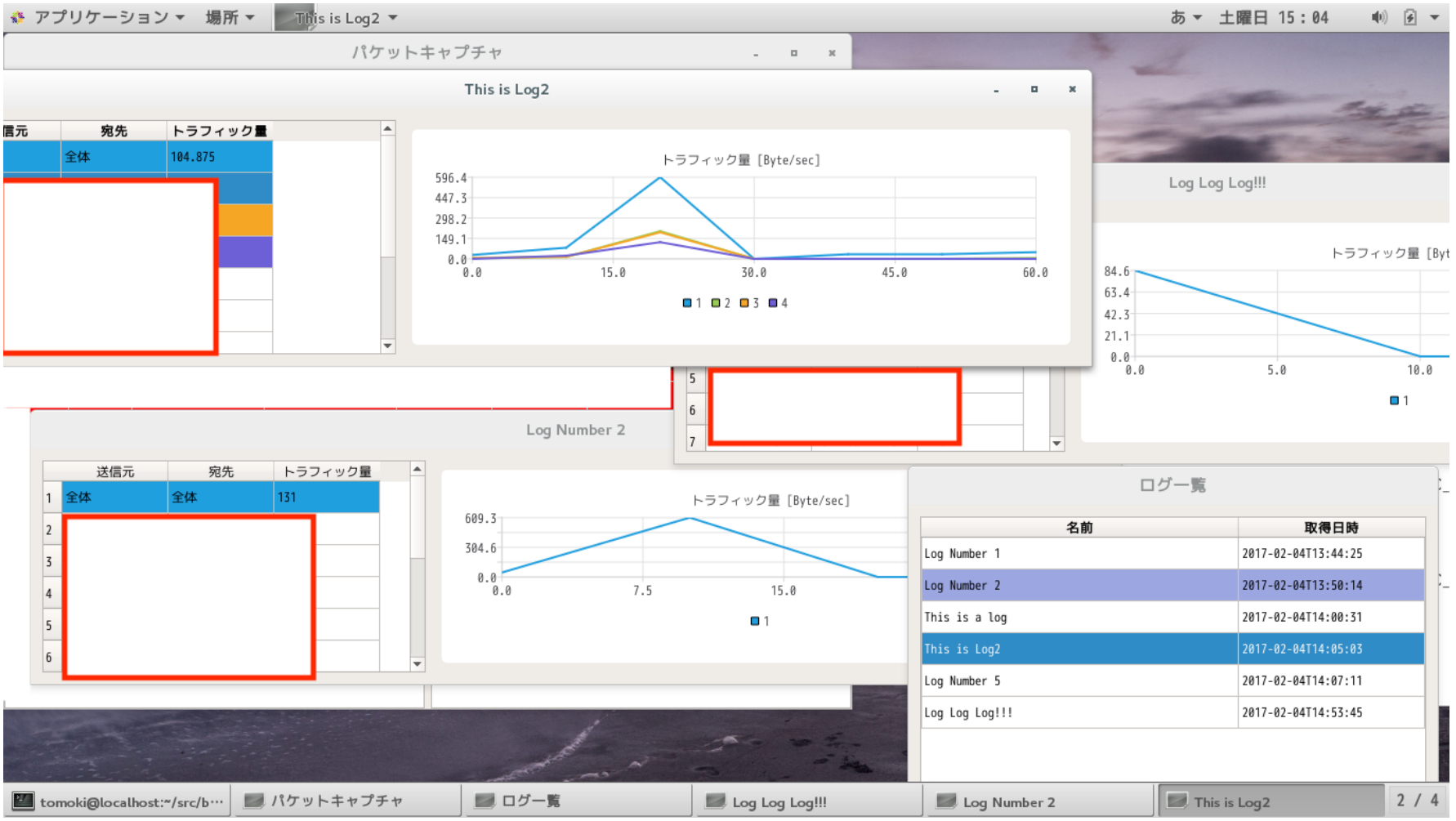


データ管理（ログ）

Pcap-qt

過去30件までのネットワーク統計をデータベースに保存可能

データベース内で**暗号化**する



ソフトウェアの今後の展望

Pcap-qt

・メモリ占有による重い動作を改善する

・データベースをより効率的に設計する

・扱えるプロトコル/データリンクの数を増やす

・可視化ウィンドウを高機能にする

・折れ線グラフのスケールを動的に変化させる

Pcap-qt

おしまい