

Web技術を利用したモダンな
パケットアナライザの開発

Dripcap による
次世代のパケット解析

梶本 論 (株式会社PTP)

<https://github.com/dripcap/dripcap>

The screenshot displays the Dripcap application interface. On the left, a sidebar shows a session named 'en1' with 368 packets, and buttons for 'Pause', 'Remove', 'New Session', and 'Preferences'. The main panel is divided into two sections. The top section lists network sessions with columns for protocol, source/destination IP and port, and packet count. The bottom section shows a detailed view of a selected TCP packet (108th packet in the session).

Session List:

Protocol	Source IP:Port -> Destination IP:Port	Count
TCP	172.217.25.195:443 -> 192.168.2.102:59738 ...	66
UDP	192.168.2.100:54108 -> 239.255.255.250:19...	216
TCP	192.168.2.102:59757 -> 162.125.34.129:443 ...	146
TCP	192.168.2.102:59757 -> 162.125.34.129:443 ...	393
TCP	162.125.34.129:443 -> 192.168.2.102:59757 ...	66
TCP	162.125.34.129:443 -> 192.168.2.102:59757 ...	66
TCP	162.125.34.129:443 -> 192.168.2.102:59757 ...	108
TCP	192.168.2.102:59757 -> 162.125.34.129:443 ...	66
TCP	192.168.2.102:57410 -> 54.169.159.150:443 ...	128
TCP	192.168.2.102:59702 -> 82.145.223.181:443 ...	54

Packet Details (TCP 162.125.34.129:443 -> 192.168.2.102:59757):

- Version 4
- Internet Header Length 5
- Type of service 0
- Total Length 94
- Identification 9951
- Flags 2 Don't Fragment
- Fragment Offset 64
- TTL 51
- Protocol 6 TCP
- Header Checksum 39086
- Source IP Address 162.125.34.129

Packet Structure (Hex/ASCII):

Offset	Hex	ASCII
28	37 37 15 13 3d bc 5c 4c 0e	(7 7 . . = . \ L .
32	1a 2c 08 00 45 00 00 5e 26 df	. , . . E . . ^ & .
40	00 33 06 98 ae a2 7d 22 81	@ . 3 . . . } " .
48	c0 a8 02 66 01 bb e9 6d 92 63	. . . f . . m . c
56	42 31 cd df b5 55 80 18 00 45	B 1 . . . U . . . E
64	ff 8c 00 00 01 01 08 0a 80 7c	
72	b7 40 3b 8b 19 5a 17 03 03 00	. @ ; . . Z
80	25 5a ef b4 d4 3e 2b 44 0e eb	% Z . . . > + D . .
88	bf eb 24 d9 bf 31 2d 8d 8a b5	. . \$. . 1 - . . .
96	70 86 6c 37 6c a8 d7 02 ae b4	p . l 7 l
104	4d 0b 7a 9d 72 9b 7b fb	M . z . r . { .

Dripcap はネットワーク上の通信データを簡単に可視化することができるツールです。
今までにない柔軟な拡張性で、ネットワークのデバッグを支援します。



WebUI

HTML / CSS / JavaScript で
GUI を自由に構築



JavaScript-friendly

ECMAScript 6 で
パケットの解析機能を拡張



パッケージシステム

1-Click で npm に登録した
プラグインをインストール



マルチコアに最適化

複数の JavaScript スレッドで
パケットを並列処理



クロスプラットフォーム

macOS / Linux / Windows
に標準で対応



オープンソース

すべてのソースコードを
MIT ライセンスで公開