

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>

en1 368

Pause
Remove

+ New Session

⚙ Preferences

Protocol	Source	Destination	Length
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

ipv4.fragmentOffset Fragment Offset 66

ipv4.flags.reserved Reserved 82

ipv4.flags.moreFragments More Fragments 02

ipv4.flags.doNotFragment Don't Fragment 28

ipv4.flags Flags 66

ipv4.dst Destination IP Address 64

ipv4.checksum Header Checksum 64

Destination 28.37.37.15.15.50

Source bc:5c:4c:0e:1a:2c

EtherType 2048 IPv4

Payload 94 bytes

IPv4 [TCP] 162.125.34.129 -> 192.168.2.102

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

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