NETCAP Overview v0.3.9

> Documentation: docs.netcap.io

LayerEncoders

Name	NumFields	Fields
TCP	23	Timestamp, SrcPort, DstPort, SeqNum, AckNum, DataOffset, FIN, SYN, RST, PSH, ACK, URG, ECE, CWR, NS, Window, Checksum, Urgent, Padding, Options, PayloadEntropy, PayloadSize, Payload
UDP	8	Timestamp, SrcPort, DstPort, Length, Checksum, PayloadEntropy, PayloadSize, Payload
IPv4	17	Timestamp, Version, IHL, TOS, Length, Id, Flags, FragOffset, TTL, Protocol, Checksum, SrcIP, DstIP, Padding, Options, PayloadEntropy, PayloadSize
IPv6	12	Timestamp, Version, TrafficClass, FlowLabel, Length, NextHeader, HopLimit, SrcIP, DstIP, PayloadEntropy, PayloadSize, HopByHop
DHCPv4	16	Timestamp, Operation, HardwareType, HardwareLen, HardwareOpts, Xid, Secs, Flags, ClientIP, YourClientIP, NextServerIP, RelayAgentIP, ClientHWAddr, ServerName, File, Options
DHCPv6	7	Timestamp, MsgType, HopCount, LinkAddr, PeerAddr, TransactionID, Options
ICMPv4	5	Timestamp, TypeCode, Checksum, Id, Seq
ICMPv6	3	Timestamp, TypeCode, Checksum
ICMPv6Echo	3	Timestamp, Identifier, SeqNumber
ICMPv6NeighborSolicitation	3	Timestamp, TargetAddress, Options
ICMPv6RouterSolicitation	2	Timestamp, Options
DNS	18	Timestamp, ID, QR, OpCode, AA, TC, RD, RA, Z, ResponseCode, QDCount, ANCount, NSCount, ARCount, Questions, Answers, Authorities, Additionals
ARP	10	Timestamp, AddrType, Protocol, HwAddressSize, ProtAddressSize, Operation, SrcHwAddress, SrcProtAddress, DstHwAddress, DstProtAddress
Ethernet	6	Timestamp, SrcMAC, DstMAC, EthernetType, PayloadEntropy, PayloadSize
Dot1Q	5	Timestamp, Priority, DropEligible, VLANIdentifier, Type
Dot11	14	Timestamp, Type, Proto, Flags, DurationID, Address1, Address2, Address3, Address4, SequenceNumber, FragmentNumber, Checksum, QOS, HTControl
NTP	15	Timestamp, LeapIndicator, Version, Mode, Stratum, Poll, Precision, RootDelay, RootDispersion, ReferenceID, ReferenceTimestamp, OriginTimestamp, ReceiveTimestamp, TransmitTimestamp, ExtensionBytes
SIP	7	Timestamp, Version, Method, Headers, IsResponse, ResponseCode, ResponseStatus
IGMP	13	Timestamp, Type, MaxResponseTime, Checksum, GroupAddress, SupressRouterProcessing, RobustnessValue, IntervalTime, SourceAddresses, NumberOfGroupRecords, NumberOfSources, GroupRecords, Version
LLC	6	Timestamp, DSAP, IG, SSAP, CR, Control
IPv6HopByHop	2	Timestamp, Options

SCTP	5	Timestamp, SrcPort, DstPort, VerificationTag, Checksum
SNAP	3	Timestamp, OrganizationalCode, Type
LinkLayerDiscovery	5	Timestamp, ChassisID, PortID, TTL, Values
ICMPv6NeighborAdvertisement	4	Timestamp, Flags, TargetAddress, Options
ICMPv6RouterAdvertisement	7	Timestamp, HopLimit, Flags, RouterLifetime, ReachableTime, RetransTimer, Options
EthernetCTP	2	Timestamp, SkipCount
EthernetCTPReply	4	Timestamp, Function, ReceiptNumber, Data
LinkLayerDiscoveryInfo	8	Timestamp, PortDescription, SysName, SysDescription, SysCapabilities, MgmtAddress, OrgTLVs, Unknown
IPSecAH	5	Timestamp, Reserved, SPI, Seq, AuthenticationData
IPSecESP	4	Timestamp, SPI, Seq, LenEncrypted
Geneve	8	Timestamp, Version, OptionsLength, OAMPacket, CriticalOption, Protocol, VNI, Options
IPv6Fragment	7	Timestamp, NextHeader, Reserved1, FragmentOffset, Reserved2, MoreFragments, Identification
VXLAN	7	Timestamp, ValidIDFlag, VNI, GBPExtension, GBPDontLearn, GBPApplied, GBPGroupPolicyID
USB	20	Timestamp, ID, EventType, TransferType, Direction, EndpointNumber, DeviceAddress, BusID, TimestampSec, TimestampUsec, Setup, Data, Status, UrbLength, UrbDataLength, UrbInterval, UrbStartFrame, UrbCopyOfTransferFlags, IsoNumDesc, Payload
LCM	9	Timestamp, Magic, SequenceNumber, PayloadSize, FragmentOffset, FragmentNumber, TotalFragments, ChannelName, Fragmented
MPLS	5	Timestamp, Label, TrafficClass, StackBottom, TTL
ModbusTCP	6	Timestamp, TransactionIdentifier, ProtocolIdentifier, Length, UnitIdentifier, Payload
OSPF	14	Timestamp, Version, Type, PacketLength, RouterID, AreaID, Checksum, AuType, Authentication, LSAs, LSU, LSR, DbDesc, HelloV2
OSPF	14	Timestamp, Version, Type, PacketLength, RouterID, AreaID, Checksum, Instance, Reserved, Hello, DbDesc, LSR, LSU, LSAs
BFD	17	Timestamp, Version, Diagnostic, State, Poll, Final, ControlPlaneIndependent, AuthPresent, Demand, Multipoint, DetectMultiplier, MyDiscriminator, YourDiscriminator, DesiredMinTxInterval, RequiredMinRxInterval, RequiredMinEchoRxInterval, AuthHeader
GRE	17	Timestamp, ChecksumPresent, RoutingPresent, KeyPresent, SeqPresent, StrictSourceRoute, AckPresent, RecursionControl, Flags, Version, Protocol, Checksum, Offset, Key, Seq, Ack, Routing
FDDI	5	Timestamp, FrameControl, Priority, SrcMAC, DstMAC
EAP	6	Timestamp, Code, Id, Length, Type, TypeData
VRRP	10	Timestamp, Version, Type, VirtualRtrID, Priority, CountIPAddr, AuthType, AdverInt, Checksum, IPAdresses
EAPOL	4	Timestamp, Version, Type, Length

EAPOLKey	22	Timestamp, KeyDescriptorType, KeyDescriptorVersion, KeyType, KeyIndex, Install, KeyACK, KeyMIC, Secure, MICError, Request, HasEncryptedKeyData, SMKMessage, KeyLength, ReplayCounter, Nonce, IV, RSC, ID, MIC, KeyDataLength, EncryptedKeyData
CiscoDiscovery	5	Timestamp, Version, TTL, Checksum, Values
CiscoDiscoveryInfo	27	Timestamp, CDPHello, DeviceID, Addresses, PortID, Capabilities, Version, Platform, IPPrefixes, VTPDomain, NativeVLAN, FullDuplex, VLANReply, VLANQuery, PowerConsumption, MTU, ExtendedTrust, UntrustedCOS, SysName, SysOID, MgmtAddresses, Location, PowerRequest, PowerAvailable, SparePairPoe, EnergyWise, Unknown
USBRequestBlockSetup	6	Timestamp, RequestType, Request, Value, Index, Length
NortelDiscovery	7	Timestamp, IPAddress, SegmentID, Chassis, Backplane, State, NumLinks

CustomEncoders

Name	NumFields	Fields
TLS	27	Timestamp, Type, Version, MessageLen, HandshakeType, HandshakeLen, HandshakeVersion, Random, SessionIDLen, SessionID, CipherSuiteLen, ExtensionLen, SNI, OSCP, CipherSuites, CompressMethods, SignatureAlgs, SupportedGroups, SupportedPoints, ALPNs, Ja3, SrcIP, DstIP, SrcMAC, DstMAC, SrcPort, DstPort
LinkFlow	9	TimestampFirst, TimestampLast, Proto, SourceMAC, DstMAC, TotalSize, NumPackets, UID, Duration
NetworkFlow	9	TimestampFirst, TimestampLast, Proto, SrcIP, DstIP, TotalSize, NumPackets, UID, Duration
TransportFlow	9	TimestampFirst, TimestampLast, Proto, SrcPort, DstPort, TotalSize, NumPackets, UID, Duration
HTTP	14	Timestamp, Proto, Method, Host, UserAgent, Referer, ReqCookies, ReqContentLength, URL, ResContentLength, ContentType, StatusCode, SrcIP, DstIP
Flow	17	TimestampFirst, LinkProto, NetworkProto, TransportProto, ApplicationProto, SrcMAC, DstMAC, SrcIP, SrcPort, DstIP, DstPort, TotalSize, AppPayloadSize, NumPackets, UID, Duration, TimestampLast
Connection	17	TimestampFirst, LinkProto, NetworkProto, TransportProto, ApplicationProto, SrcMAC, DstMAC, SrcIP, SrcPort, DstIP, DstPort, TotalSize, AppPayloadSize, NumPackets, UID, Duration, TimestampLast