NETCAP Overview v0.5

> Documentation: docs.netcap.io

LayerEncoders

Name	NumFields	Fields
TCP	25	Timestamp, SrcPort, DstPort, SeqNum, AckNum, DataOffset, FIN, SYN, RST, PSH, ACK, URG, ECE, CWR, NS, Window, Checksum, Urgent, Padding, Options, PayloadEntropy, PayloadSize, Payload, SrcIP, DstIP
UDP	10	Timestamp, SrcPort, DstPort, Length, Checksum, PayloadEntropy, PayloadSize, Payload, SrcIP, DstIP
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	20	Timestamp, Operation, HardwareType, HardwareLen, HardwareOpts, Xid, Secs, Flags, ClientIP, YourClientIP, NextServerIP, RelayAgentIP, ClientHWAddr, ServerName, File, Options, SrcIP, DstIP, SrcPort, DstPort
DHCPv6	11	Timestamp, MsgType, HopCount, LinkAddr, PeerAddr, TransactionID, Options, SrcIP, DstIP, SrcPort, DstPort
ICMPv4	7	Timestamp, TypeCode, Checksum, Id, Seq, SrcIP, DstIP
ICMPv6	5	Timestamp, TypeCode, Checksum, SrcIP, DstIP
ICMPv6Echo	5	Timestamp, Identifier, SeqNumber, SrcIP, DstIP
ICMPv6NeighborSolicitation	5	Timestamp, TargetAddress, Options, SrcIP, DstIP
ICMPv6RouterSolicitation	4	Timestamp, Options, SrcIP, DstIP
DNS	22	Timestamp, ID, QR, OpCode, AA, TC, RD, RA, Z, ResponseCode, QDCount, ANCount, NSCount, ARCount, Questions, Answers, Authorities, Additionals, SrcIP, DstIP, SrcPort, DstPort
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	19	Timestamp, LeapIndicator, Version, Mode, Stratum, Poll, Precision, RootDelay, RootDispersion, ReferenceID, ReferenceTimestamp, OriginTimestamp, ReceiveTimestamp, TransmitTimestamp, ExtensionBytes, SrcIP, DstIP, SrcPort, DstPort
SIP	11	Timestamp, Version, Method, Headers, IsResponse, ResponseCode, ResponseStatus, SrcIP, DstIP, SrcPort, DstPort
IGMP	15	Timestamp, Type, MaxResponseTime, Checksum, GroupAddress, SupressRouterProcessing, RobustnessValue, IntervalTime, SourceAddresses, NumberOfGroupRecords, NumberOfSources, GroupRecords, Version, SrcIP, DstIP

LLC	6	Timestamp, DSAP, IG, SSAP, CR, Control
IPv6HopByHop	4	Timestamp, Options, SrcIP, DstIP
SCTP	7	Timestamp, SrcPort, DstPort, VerificationTag, Checksum, SrcIP, DstIP
SNAP	3	Timestamp, OrganizationalCode, Type
LinkLayerDiscovery	5	Timestamp, ChassisID, PortID, TTL, Values
ICMPv6NeighborAdvertisement	6	Timestamp, Flags, TargetAddress, Options, SrcIP, DstIP
ICMPv6RouterAdvertisement	9	Timestamp, HopLimit, Flags, RouterLifetime, ReachableTime, RetransTimer, Options, SrcIP, DstIP
EthernetCTP	2	Timestamp, SkipCount
EthernetCTPReply	4	Timestamp, Function, ReceiptNumber, Data
LinkLayerDiscoveryInfo	8	Timestamp, PortDescription, SysName, SysDescription, SysCapabilities, MgmtAddress, OrgTLVs, Unknown
IPSecAH	7	Timestamp, Reserved, SPI, Seq, AuthenticationData, SrcIP, DstIP
IPSecESP	6	Timestamp, SPI, Seq, LenEncrypted, SrcIP, DstIP
Geneve	12	Timestamp, Version, OptionsLength, OAMPacket, CriticalOption, Protocol, VNI, Options, SrcIP, DstIP, SrcPort, DstPort
IPv6Fragment	9	Timestamp, NextHeader, Reserved1, FragmentOffset, Reserved2, MoreFragments, Identification, SrcIP, DstIP
VXLAN	9	Timestamp, ValidIDFlag, VNI, GBPExtension, GBPDontLearn, GBPApplied, GBPGroupPolicyID, SrcIP, DstIP
USB	20	Timestamp, ID, EventType, TransferType, Direction, EndpointNumber, DeviceAddress, BusID, TimestampSec, TimestampUsec, Setup, Data, Status, UrbLength, UrbDataLength, UrbInterval, UrbStartFrame, UrbCopyOfTransferFlags, IsoNumDesc, Payload
LCM	13	Timestamp, Magic, SequenceNumber, PayloadSize, FragmentOffset, FragmentNumber, TotalFragments, ChannelName, Fragmented, SrcIP, DstIP, SrcPort, DstPort
MPLS	7	Timestamp, Label, TrafficClass, StackBottom, TTL, SrcIP, DstIP
Modbus	12	Timestamp, TransactionID, ProtocolID, Length, UnitID, Payload, Exception, FunctionCode, SrcIP, DstIP, SrcPort, DstPort
OSPF	16	Timestamp, Version, Type, PacketLength, RouterID, AreaID, Checksum, AuType, Authentication, LSAs, LSU, LSR, DbDesc, HelloV2, SrcIP, DstIP
OSPF	16	Timestamp, Version, Type, PacketLength, RouterID, AreaID, Checksum, Instance, Reserved, Hello, DbDesc, LSR, LSU, LSAs, SrcIP, DstIP
BFD	21	Timestamp, Version, Diagnostic, State, Poll, Final, ControlPlaneIndependent, AuthPresent, Demand, Multipoint, DetectMultiplier, MyDiscriminator, YourDiscriminator, DesiredMinTxInterval, RequiredMinRxInterval, RequiredMinEchoRxInterval, AuthHeader, SrcIP, DstIP, SrcPort, DstPort
GRE	21	Timestamp, ChecksumPresent, RoutingPresent, KeyPresent, SeqPresent, StrictSourceRoute, AckPresent, RecursionControl, Flags, Version, Protocol, Checksum, Offset, Key, Seq, Ack, Routing, SrcIP, DstIP, SrcPort, DstPort
FDDI	5	Timestamp, FrameControl, Priority, SrcMAC, DstMAC
EAP	6	Timestamp, Code, Id, Length, Type, TypeData

VRRP	12	Timestamp, Version, Type, VirtualRtrID, Priority, CountIPAddr, AuthType, AdverInt, Checksum, IPAdresses, SrcIP, DstIP
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
CIP	12	Timestamp, Response, ServiceID, ClassID, InstanceID, Status, AdditionalStatus, Data, SrcIP, DstIP, SrcPort, DstPort
Ethernet/IP	12	Timestamp, Command, Length, SessionHandle, Status, SenderContext, Options, CommandSpecific, SrcIP, DstIP, SrcPort, DstPort
SMTP	9	Timestamp, IsEncrypted, IsResponse, ResponseLines, Command, SrcIP, DstIP, SrcPort, DstPort
Diameter	13	Timestamp, Version, Flags, MessageLen, CommandCode, ApplicationID, HopByHopID, EndToEndID, AVPs, SrcIP, DstIP, SrcPort, DstPort

CustomEncoders

Name	NumFields	Fields
TLSClientHello	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
TLSServerHello	27	Timestamp, Version, Random, SessionID, CipherSuite, CompressionMethod, NextProtoNeg, NextProtos, OCSPStapling, TicketSupported, SecureRenegotiationSupported, SecureRenegotiation, AlpnProtocol, Ems, SupportedVersion, SelectedIdentityPresent, SelectedIdentity, Cookie, SelectedGroup, Extensions, SrcIP, DstIP, SrcMAC, DstMAC, SrcPort, DstPort, Ja3S
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	18	Timestamp, Proto, Method, Host, UserAgent, Referer, ReqCookies, ResCookies, ReqContentLength, URL, ResContentLength, ContentType, StatusCode, SrcIP, DstIP, ReqContentEncoding, ResContentEncoding, ServerName
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
DeviceProfile	7	Timestamp, MacAddr, DeviceManufacturer, NumDeviceIPs, NumContacts, NumPackets, Bytes
File	10	Timestamp, AddrType, Protocol, HwAddressSize, ProtAddressSize, Operation, SrcHwAddress, SrcProtAddress, DstHwAddress, DstProtAddress
POP3	7	Timestamp, Client, Server, AuthToken, User, Pass, NumMails