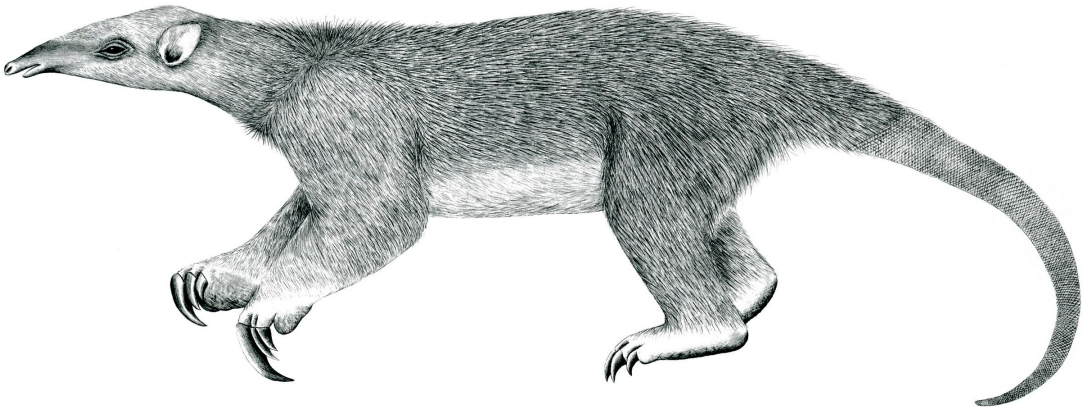
Tranalyzer2

icmpDecode

Internet Control Message Protocol (ICMP)



Tranalyzer Development Team

Contents

1 icmpDecode

1.1 Description

The icmpDecode plugin analyzes ICMP and ICMPv6 traffic. It generates global and flow based statistics.

1.2 Configuration Flags

The following flags can be used to control the output of the plugin:

Name	Default	Description	Flags
ICMP_TC_MD	0	Type/code representation: 0: bitfield, 1: explicit array of type code, 2: type code statistics [NOT IMPLEMENTED YET]	
ICMP_NUM	10	Number of type and code information	ICMP_TC_MD=1
ICMP_FDCORR	1	Flow direction correction	
ICMP_PARENT	0	Resolve the parent flow	
ICMP_STATFILE	0	Print ICMP statistics in a separate file	
ICMP_NOCODE	"-"	Symbol to use to represent the absence of a code	

1.2.1 Environment Variable Configuration Flags

The following configuration flags can also be configured with environment variables (ENVCNTRL>0):

- ICMP_NOCODE
- ICMP_SUFFIX

1.3 Flow File Output

The icmpDecode plugin outputs the following columns:

Column	Type	Description	Flags
icmpStat	H8	Status	
icmpTCcnt	U8	Type/Code count	
icmpBFType_Code	H32_H16	Aggregated type (<32) and code bitfield	ICMP_TC_MD=0&& IPV6_ACTIVATE=0
icmpBFTypH_TypL_Code	H32_H32_H16	Aggr. type H(>128), L(<32) and code bitfield	ICMP_TC_MD=0&& IPV6_ACTIVATE=1
icmpType_Code	R(U8_U8)	Type and code fields	ICMP_TC_MD=1
icmpTmGtw	H32	Time/gateway	
icmpEchoSuccRatio	F	Echo reply/request success ratio	
icmpPFindex	U64	Parent flowIndex	ICMP_PARENT=1

1.3.1 icmpStat

The `icmpStat` column is to be interpreted as follows:

	icmpStat	Description
2^0	(=0x01)	Flow is ICMP
2^1	(=0x02)	—
2^2	(=0x04)	—
2^3	(=0x08)	—
2^4	(=0x10)	WANG2 Microsoft bandwidth test
2^5	(=0x20)	ICMP ECHO Seq Num abnormal increment
2^6	(=0x40)	Embedded LOKI covert channel
2^7	(=0x80)	Embedded SSH covert channel

1.3.2 icmpBFType_Code

For **ICMP (IPv4)**, the `icmpBFType_Code` column is to be interpreted as follows:

	icmpBFType	Description
2^0	(=0x00000001)	Echo Reply
2^1	(=0x00000002)	—
2^2	(=0x00000004)	—
2^3	(=0x00000008)	Destination Unreachable
2^4	(=0x00000010)	Source Quench
2^5	(=0x00000020)	Redirect (change route)
2^6	(=0x00000040)	Alternate Host Address (Deprecated)
2^7	(=0x00000080)	—
2^8	(=0x00000100)	Echo Request
2^9	(=0x00000200)	Router Advisement
2^{10}	(=0x00000400)	Router Selection
2^{11}	(=0x00000800)	Time Exceeded
2^{12}	(=0x00001000)	Parameter Problem
2^{13}	(=0x00002000)	Timestamp Request
2^{14}	(=0x00004000)	Timestamp Reply
2^{15}	(=0x00008000)	Information Request
2^{16}	(=0x00010000)	Information Reply
2^{17}	(=0x00020000)	Address Mask Request
2^{18}	(=0x00040000)	Address Mask Reply
2^{19}	(=0x00080000)	Reserved (for Security)
2^{20}	(=0x00100000)	Experimental

icmpBFType	Description
2^{21} (=0x00200000)	Experimental
2^{22} (=0x00400000)	Experimental
2^{23} (=0x00800000)	Experimental
2^{24} (=0x01000000)	Experimental
2^{25} (=0x02000000)	Experimental
2^{26} (=0x04000000)	Experimental
2^{27} (=0x08000000)	Experimental
2^{28} (=0x10000000)	Experimental
2^{29} (=0x20000000)	Experimental
2^{30} (=0x40000000)	Traceroute
2^{31} (=0x80000000)	Datagram Conversion Error (Deprecated)

The `icmpCode` for **Destination Unreachable** (`0x00000008`) is to be interpreted as follows:

icmpBFCode	Description
2^{0} (=0x0001)	Network Unreachable
2^{1} (=0x0002)	Host Unreachable
2^{2} (=0x0004)	Protocol Unreachable
2^{3} (=0x0008)	Port Unreachable
2^{4} (=0x0010)	Fragmentation Needed/DF set
2^{5} (=0x0020)	Source Route failed
2^{6} (=0x0040)	Destination Network unknown
2^{7} (=0x0080)	Destination Host unknown
2^{8} (=0x0100)	Src host isolated
2^{9} (=0x0200)	Dest net administratively prohibited
2^{10} (=0x0400)	Dest host administratively prohibited
2^{11} (=0x0800)	Dest net unreachable for type of service
2^{12} (=0x1000)	Dest host unreachable for type of service
2^{13} (=0x2000)	Communication administratively prohibited
2^{14} (=0x4000)	Precedence violation
2^{15} (=0x8000)	Precedence cut off

For **ICMPv6 (IPv6)**, the `icmpBFType_Code` column is to be interpreted as follows:

icmpType	Description
0	Reserved
1	Destination Unreachable
2	Packet Too Big
3	Time Exceeded
4	Parameter Problem
100	Private experimentation
101	Private experimentation
102–126	Unassigned
127	Reserved for expansion of ICMPv6 error messages
128	Echo Request
129	Echo Reply
130	Multicast Listener Query
131	Multicast Listener Report
132	Multicast Listener Done
133	Router Solicitation
134	Router Advertisement
135	Neighbor Solicitation
136	Neighbor Advertisement
137	Redirect Message
138	Router Renumbering
139	ICMP Node Information Query
140	ICMP Node Information Response
141	Inverse Neighbor Discovery Solicitation
142	Inverse Neighbor Discovery Advertisement
143	Version 2 Multicast Listener Report
144	Home Agent Address Discovery Request
145	Home Agent Address Discovery Reply
146	Mobile Prefix Solicitation
147	Mobile Prefix Advertisement
148	Certification Path Solicitation
149	Certification Path Advertisement
150	ICMP messages utilized by experimental mobility protocols such as Seamoby
151	Multicast Router Advertisement
152	Multicast Router Solicitation
153	Multicast Router Termination
154	FMIPv6 Messages
155	RPL Control Message
156	ILNPv6 Locator Update Message
157	Duplicate Address Request
158	Duplicate Address Confirmation
159	MPL Control Message
160–199	Unassigned
200	Private experimentation
201	Private experimentation
255	Reserved for expansion of ICMPv6 informational messages

The `icmpCode` for **Destination Unreachable (1)** are:

	icmpCode	Description
2^0	(=0x0001)	No route to destination
2^1	(=0x0002)	Communication with destination administratively prohibited
2^2	(=0x0004)	Beyond scope of source address
2^3	(=0x0008)	Address unreachable
2^4	(=0x0010)	Port unreachable
2^5	(=0x0020)	Source address failed ingress/egress policy
2^6	(=0x0040)	Reject route to destination
2^7	(=0x0080)	Error in Source Routing Header

The `icmpCode` for **Time Exceeded (3)** are:

	icmpCode	Description
2^0	(=0x0001)	Hop limit exceeded in transit
2^1	(=0x0002)	Fragment reassembly time exceeded

The icmpCode for **Parameter Problem (4)** are:

	icmpCode	Description
2^0	(=0x0001)	Erroneous header field encountered
2^1	(=0x0002)	Unrecognized Next Header type encountered
2^2	(=0x0004)	Unrecognized IPv6 option encountered
2^3	(=0x0008)	IPv6 First Fragment has incomplete IPv6 Header Chain

The icmpCode for **Router Renumbering (138)** are:

	icmpCode	Description
2^0	(=0x0001)	Router Renumbering Command
2^1	(=0x0002)	Router Renumbering Result
	255	Sequence Number Reset

The icmpCode for **ICMP Node Information Query (139)** are:

	icmpCode	Description
2^0	(=0x0001)	The Data field contains an IPv6 address which is the Subject of this Query
2^1	(=0x0002)	The Data field contains a name which is the Subject of this Query, or is empty, as in the case of a NOOP
2^3	(=0x0004)	The Data field contains an IPv4 address which is the Subject of this Query

The icmpCode for **ICMP Node Information Response (140)** are:

	icmpCode	Description
2^0	(=0x0001)	A successful reply. The Reply Data field may or may not be empty
2^1	(=0x0002)	The Responder refuses to supply the answer. The Reply Data field will be empty
2^2	(=0x0004)	The Qtype of the Query is unknown to the Responder. The Reply Data field will be empty

1.4 Packet File Output

In packet mode (-s option), the icmpDecode plugin outputs the following columns:

Column	Type	Description	Flags
icmpStat	H8	Status	
icmpType	U8	Message type	
icmpCode	U8	Message code	
icmpID	H16	Identifier	
icmpSeq	H16	Sequence number	
icmpPFindex	U64	Parent flowIndex	ICMP_PARENT=1

1.5 Monitoring Output

In monitoring mode, the icmpDecode plugin outputs the following columns:

Column	Type	Description	Flags
icmpPkts	U64	Number of ICMP/ICMPv6 packets	
icmpEchoReq	U64	Number of ICMP/ICMPv6 echo request packets	
icmpEchoRep	U64	Number of ICMP/ICMPv6 echo reply packets	

1.6 Plugin Report Output

The following information is reported:

- Aggregated icmpStat
- Number of ICMP/ICMPv6 echo request packets
- Number of ICMP/ICMPv6 echo reply packets
- ICMP/ICMPv6 echo reply / request ratio

1.7 Additional Output

The icmpDecode plugin outputs absolute and relative statistics in the PREFIX_icmpStats.txt file. Note that the default suffix of "_icmpStats.txt" can be changed by editing the ICMP_SUFFIX flag.

The output is as follows (IPV6_ACTIVATE=0||IPV6_ACTIVATE=2):

Type	Code	Description
ICMP_ECHOREQUEST	--	Echo request
ICMP_ECHOREPLY	--	Echo reply to an echo request
ICMP_SOURCE_QUENCH	--	Source quenches
ICMP_TRACEROUTE	--	Traceroute packets
ICMP_DEST_UNREACH	ICMP_NET_UNREACH	Network unreachable
ICMP_DEST_UNREACH	ICMP_HOST_UNREACH	Host unreachable
ICMP_DEST_UNREACH	ICMP_PROT_UNREACH	Protocol unreachable
ICMP_DEST_UNREACH	ICMP_PORT_UNREACH	Port unreachable
ICMP_DEST_UNREACH	ICMP_FRAG_NEEDED	Fragmentation needed
ICMP_DEST_UNREACH	ICMP_SR_FAILED	Source route failed
ICMP_DEST_UNREACH	ICMP_NET_UNKNOWN	Network unknown
ICMP_DEST_UNREACH	ICMP_HOST_UNKNOWN	Host unknown
ICMP_DEST_UNREACH	ICMP_HOST_ISOLATED	Host is isolated
ICMP_DEST_UNREACH	ICMP_NET_ANO	Network annotation
ICMP_DEST_UNREACH	ICMP_HOST_ANO	Host annotation
ICMP_DEST_UNREACH	ICMP_NET_UNR_TOS	Unreachable type of network service
ICMP_DEST_UNREACH	ICMP_HOST_UNR_TOS	Unreachable type of host service
ICMP_DEST_UNREACH	ICMP_PKT_FILTERED	Dropped by a filtering device
ICMP_DEST_UNREACH	ICMP_PREC_VIOLATION	Precedence violation

Type	Code	Description
ICMP_DEST_UNREACH	ICMP_PREC_CUTOFF	Precedence cut off
ICMP_REDIRECT	ICMP_REDIR_NET	Network redirection
ICMP_REDIRECT	ICMP_REDIR_HOST	Host redirection
ICMP_REDIRECT	ICMP_REDIR_NETTOS	Network type of service
ICMP_REDIRECT	ICMP_REDIR_HOSTTOS	Host type of service
ICMP_TIME_EXCEEDED	ICMP_EXC_TTL	TTL exceeded in Transit
ICMP_TIME_EXCEEDED	ICMP_EXC_FRAGTIME	Fragment Reassembly Time Exceeded

If IPV6_ACTIVATE>0, then the output becomes:

Type	Code	Description
ICMP6_ECHOREQUEST	--	Echo request
ICMP6_ECHOREPLY	--	Echo reply to an echo request
ICMP6_PKT_TOO_BIG	--	Packet too big
ICMP6_DEST_UNREACH	ICMP6_NO_ROUTE	No route to destination
ICMP6_DEST_UNREACH	ICMP6_COMM_PROHIBIT	Communication with destination prohibited
ICMP6_DEST_UNREACH	ICMP6_BEYOND_SCOPE	Beyond scope of source address
ICMP6_DEST_UNREACH	ICMP6_ADDR_UNREACH	Address unreachable
ICMP6_DEST_UNREACH	ICMP6_PORT_UNREACH	Port unreachable
ICMP6_DEST_UNREACH	ICMP6_SR_FAILED	Source route failed
ICMP6_DEST_UNREACH	ICMP6_REJECT	Reject source to destination
ICMP6_DEST_UNREACH	ICMP6_ERROR_HDR	Error in Source Routing Header
ICMP6_TIME_EXCEEDED	ICMP6_EXC_HOPS	Hop limit exceeded in transit
ICMP6_TIME_EXCEEDED	ICMP6_EXC_FRAGTIME	Fragment reassembly time exceeded
ICMP6_PARAM_PROBLEM	ICMP6_ERR_HDR	Erroneous header field
ICMP6_PARAM_PROBLEM	ICMP6_UNRECO_NEXT_HDR	Unrecognized Next Header type
ICMP6_PARAM_PROBLEM	ICMP6_UNRECO_IP6_OPT	Unrecognized IPv6 option
ICMP6_MCAST_QUERY	--	Multicast Listener Query
ICMP6_MCAST_REP	--	Multicast Listener Report
ICMP6_MCAST_DONE	--	Multicast Listener Done
ICMP6_RTER_SOLICIT	--	Router Solicitation
ICMP6_RTER_ADVERT	--	Router Advertisement
ICMP6_NBOR_SOLICIT	--	Neighbor Solicitation
ICMP6_NBOR_ADVERT	--	Neighbor Advertisement
ICMP6_REDIRECT_MSG	--	Redirect Message
ICMP6_RTER_RENUM	ICMP6_RR_CMD (0)	Router Renumbering Command
ICMP6_RTER_RENUM	ICMP6_RR_RES (1)	Router Renumbering Result
ICMP6_RTER_RENUM	ICMP6_RR_RST (255)	Router Renum.: Sequence Number Reset
ICMP6_NODE_INFO_QUERY	ICMP6_NIQ_IP6 (0)	Node Info. Query: contains an IPv6 address
ICMP6_NODE_INFO_QUERY	ICMP6_NIQ_NAME (1)	Contains a name or is empty (NOOP)
ICMP6_NODE_INFO_QUERY	ICMP6_NIQ_IP4 (2)	Contains an IPv4 address
ICMP6_NODE_INFO_RESP	ICMP6_NIR_SUCC (0)	Node Info. Response: Successful reply
ICMP6_NODE_INFO_RESP	ICMP6_NIR_DENIED (1)	Responder refuses to answer
ICMP6_NODE_INFO_RESP	ICMP6_NIR_UNKN (2)	Qtype of the query unknown
ICMP6_INV_NBOR_DSM	--	Inverse Neighbor Discovery Solicitation Msg

Type	Code	Description
ICMP6_INV_NBOR_DAM	--	Inverse Neighbor Disc. Advertisement Msg
ICMP6_MLD2	--	Version 2 Multicast Listener Report
ICMP6_ADDR_DISC_REQ	--	Home Agent Address Discovery Request Msg
ICMP6_ADDR_DISC_REP	--	Home Agent Address Discovery Reply Msg
ICMP6_MOB_PREF_SOL	--	Mobile Prefix Solicitation
ICMP6_MOB_PREF_ADV	--	Mobile Prefix Advertisement
ICMP6_CERT_PATH_SOL	--	Certification Path Solicitation Message
ICMP6_CERT_PATH_ADV	--	Certification Path Advertisement Message
ICMP6_EXP_MOBI	--	Experimental mobility protocols
ICMP6_MRD_ADV	--	Multicast Router Advertisement
ICMP6_MRD_SOL	--	Multicast Router Solicitation
ICMP6_MRD_TERM	--	Multicast Router Termination
ICMP6_FMIPV6	--	FMIPv6 Messages
ICMP6_RPL_CTRL	--	RPL Control Message
ICMP6_ILNP_LOC_UP	--	ILNPv6 Locator Update Message
ICMP6_DUP_ADDR_REQ	--	Duplicate Address Request
ICMP6_DUP_ADDR_CONF	--	Duplicate Address Confirmation

1.8 Post-Processing

1.8.1 icmpX

The `icmpX` script extracts all ICMP flows and their parents (flows which caused the ICMP message) from a flow file. Run `./icmpX --help` for more information.

1.8.2 protStat

The `protStat` script can be used to sort the `PREFIX_icmpStats.txt` file for the most or least occurring types and codes. It can output the top or bottom *N* protocols or only those with at least a given percentage:

- list all the options: `protStat --help`
- for better readability, use `protStat` with `tcol`: `protStat ... | tcol`
- sorted list of types (by packets):

```
protStat PREFIX_icmpStats.txt
```

- top 10 ICMP types and codes (by packets):

```
protStat PREFIX_icmpStats.txt -n 10 -icmp
```

- bottom 5 ICMPv6 types and codes (by packets):

```
protStat PREFIX_icmpStats.txt -n -5 -icmpv6
```

- ICMP and ICMPv6 types and codes with packets percentage greater than 20%:

```
protStat PREFIX_icmpStats.txt -p 20
```

- ICMP and ICMPv6 types and codes with packets percentage smaller than 5%:

```
protStat PREFIX_icmpStats.txt -p -5
```