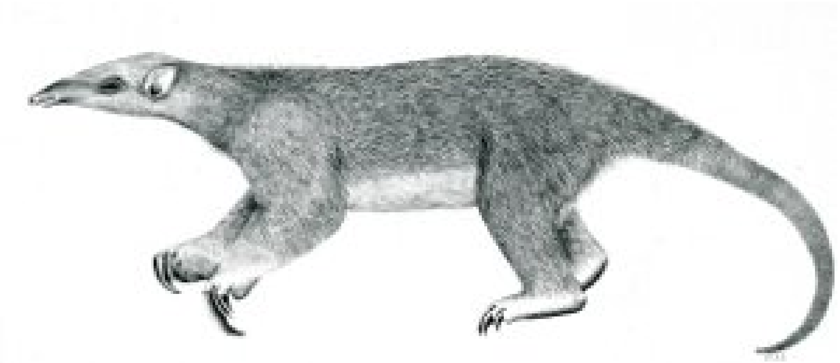
Tranalyzer2

tcpFlags

tcpFlags



Tranalyzer Development Team

Contents

1 tcpFlags

1.1 Description

The tcpFlags plugin contains IP and TCP header information encountered during the lifetime of a flow.

1.2 Configuration Flags

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

Name	Default	Description
SPKTMD_SEQACKREL	0	Seq/Ack Numbers 0: absolute, 1: relative (-s option)
RTT_ESTIMATE	1	Whether (1) or not (0) to estimate Round trip time
IPCHECKSUM	2	0: No checksums calculation 1: Calculation of L3 (IP) Header Checksum 2: L3/L4 (TCP, UDP, ICMP, IGMP, ...) Checksum
WINDOWSIZE	1	Whether (1) or not (0) to output TCP window size parameters
SEQ_ACK_NUM	1	Whether (1) or not (0) to output Sequence/Acknowledge Number features
FRAG_ANALYZE	1	Whether (1) or not (0) to enable fragmentation analysis
NAT_BT_EST	1	Whether (1) or not (0) to estimate NAT boot time
SCAN_DETECTOR	1	Whether (1) or not (0) to enable scan flow detector
WINMIN	1	Minimal window size defining a healthy communication, below packets are counted

1.2.1 WINMIN

WINMIN default 1 setting selects all packets/flow where communication came to a halt due to receiver buffer overflow. Literally the number of window size 0 packets to the sender are then counted. WINMIN can be set to any value defining a healthy communication, which depends on the network and application.

1.3 Flow File Output

The tcpFlags plugin outputs the following columns:

Column	Type	Description	Flags
tcpFStat	H16	Status	
ipMindIPID	U16	IP minimum delta IP ID	
ipMaxdIPID	U16	IP maximum delta IP ID	
ipMinTTL	U8	IP minimum TTL	
ipMaxTTL	U8	IP maximum TTL	
ipTTLChg	U8	IP TTL Change Count	
ipTOS	H8	IP Type of Service	
ipFlags	H16	IP aggregated flags	
ipOptCnt	U16	IP options count	IPV6_ACTIVATE=0
ipOptCpCl_Num	H8_H32	IP aggregated options, copy-class and number	IPV6_ACTIVATE=0
ip6OptCntHH_D	U16_U16	IPv6 aggregated hop by hop dest. option counts	IPV6_ACTIVATE=1

Column	Type	Description	Flags
ip6OptHH_D	H32_H32	IPv6 hop by hop destination options	IPV6_ACTIVATE=1
tcpPSeqCnt	U16	TCP packet sequence count	SEQ_ACK_NUM=1
tcpSeqSntBytes	U64	TCP sent seq diff bytes	SEQ_ACK_NUM=1
tcpSeqFaultCnt	U16	TCP sequence number fault count	SEQ_ACK_NUM=1
tcpPAckCnt	U16	TCP packet ack count	SEQ_ACK_NUM=1
tcpFlwLssAckRcvdBytes	U64	TCP flawless ack received bytes	SEQ_ACK_NUM=1
tcpAckFaultCnt	U16	TCP ack number fault count	SEQ_ACK_NUM=1
tcpInitWinSz	U32	TCP initial effective window size	WINDOWSIZE=1
tcpAveWinSz	F	TCP average effective window size	WINDOWSIZE=1
tcpMinWinSz	U32	TCP minimum effective window size	WINDOWSIZE=1
tcpMaxWinSz	U32	TCP maximum effective window size	WINDOWSIZE=1
tcpWinSzDwnCnt	U16	TCP effective window size change down count	WINDOWSIZE=1
tcpWinSzUpCnt	U16	TCP effective window size change up count	WINDOWSIZE=1
tcpWinSzChgDirCnt	U16	TCP effective window size direction change count	WINDOWSIZE=1
tcpWinSzThRt	F	TCP packet count ratio below window size WINMIN	WINDOWSIZE=1
tcpFlags	H8	TCP aggregated protocol flags (CWR, ACK, PSH, RST, SYN, FIN)	
tcpAnomaly	H16	TCP aggregated header anomaly flags	
tcpOptPktCnt	U16	TCP options packet count	
tcpOptCnt	U16	TCP options count	
tcpOptions	H32	TCP aggregated options	
tcpMSS	U16	TCP Maximum Segment Length	
tcpWS	U8	TCP Window Scale	
tcpTmS	U32	TCP Time Stamp	NAT_BT_EST=1
tcpTmER	U32	TCP Time Echo Reply	NAT_BT_EST=1
tcpEcI	F	TCP Estimated counter increment	NAT_BT_EST=1
tcpBtm	TS	TCP Estimated Boot time	NAT_BT_EST=1
tcpSSASAATrip	F	(A) TCP Trip Time SYN, SYN-ACK, (B) TCP Trip Time SYN-ACK, ACK	RTT_ESTIMATE=1
tcpRTTAckTripMin	F	TCP Ack Trip Minimum	RTT_ESTIMATE=1
tcpRTTAckTripMax	F	TCP Ack Trip Maximum	RTT_ESTIMATE=1
tcpRTTAckTripAve	F	TCP Ack Trip Average	RTT_ESTIMATE=1
tcpRTTAckTripJitAve	F	TCP Ack Trip Jitter Average	RTT_ESTIMATE=1
tcpRTTSseqAA	F	(A) TCP Round Trip Time SYN, SYN-ACK, ACK (B) TCP Round Trip Time ACK-ACK RTT	RTT_ESTIMATE=1 RTT_ESTIMATE=1
tcpRTTAckJitAve	F	TCP Ack Round trip average Jitter	RTT_ESTIMATE=1

1.3.1 tcpFStat

The tcpFStat column is to be interpreted as follows:

tcpFStat	Description
0x0001	Packet no good for interdistance assessment
0x0002	Scan detected in flow
0x0004	Successful scan detected in flow
0x0008	Timestamp option decreasing
0x0010	TCP option init
0x0020	ACK packet loss state machine init
0x0040	Window state machine initialized
0x0080	Window state machine count up/down
0x0100	L4 checksum calculation if present
0x0200	UDP-Lite checksum coverage error

1.3.2 ipFlags

The ipFlags column is to be interpreted as follows:

ipFlags	Description
0x0001	IP options corrupt
0x0002	IPv4 packets out of order
0x0004	IPv4 ID roll over
0x0008	IP fragment below minimum
0x0010	IP fragment out of range
0x0020	More Fragment bit
0x0040	IPv4: Dont Fragment bit IPv6: reserve bit
0x0080	Reserve bit

ipFlags	Description
0x0100	Fragmentation position error
0x0200	Fragmentation sequence error
0x0400	L3 checksum error
0x0800	L4 checksum error
0x1000	L3 header length snapped
0x2000	Packet interdistance = 0
0x4000	Packet interdistance < 0
0x8000	TCP SYN flag with L7 content

1.3.3 ipOptCpCl_Num

The aggregated IP options are coded as a bit field in hexadecimal notation where the bit position denotes the IP options type according to following format: [$2^{\text{Copy-Class}}$]_[2^{Number}]. If the field reads: 0x10_0x00100000 in an ICMP message it is a 0x94 = 148 router alert.
Refer to RFC for decoding the bitfield: http://www.iana.org/assignments/ip-parameters.

1.3.4 tcpFlags

The tcpFlags column is to be interpreted as follows:

tcpFlags	Flag	Description
2^0 (=0x01)	FIN	No more data, finish connection
2^1 (=0x02)	SYN	Synchronize sequence numbers
2^2 (=0x04)	RST	Reset connection
2^3 (=0x08)	PSH	Push data
2^4 (=0x10)	ACK	Acknowledgement field value valid

tcpFlags	Flag	Description
2^5 (=0x20)	URG	Urgent pointer valid
2^6 (=0x40)	ECE	ECN-Echo
2^7 (=0x80)	CWR	Congestion Window Reduced flag is set

1.3.5 tcpAnomaly

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

tcpAnomaly	Description
`0x0001`	FIN-ACK flag
`0x0002`	SYN-ACK flag
`0x0004`	RST-ACK flag
`0x0008`	SYN-FIN flag, scan or malicious packet
`0x0010`	SYN-FIN-RST flag, potential malicious scan packet or channel
`0x0020`	FIN-RST flag, abnormal flow termination
`0x0040`	Null flag, potential NULL scan packet, or malicious channel
`0x0080`	XMas flag, potential Xmas scan packet, or malicious channel
`0x0100`	L4 option field corrupt or not acquired
`0x0200`	SYN retransmission
`0x0400`	Sequence Number retry
`0x0800`	Sequence Number out of order
`0x1000`	Sequence mess in flow order due to pcap packet loss
`0x2000`	Sequence number jump forward
`0x4000`	ACK number out of order
`0x8000`	Duplicate ACK

1.3.6 tcpOptions

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

tcpOptions	Description
2^0 (=`0x00000001`)	End of Option List
2^1 (=`0x00000002`)	No-Operation
2^2 (=`0x00000004`)	Maximum Segment Size
2^3 (=`0x00000008`)	Window Scale
2^4 (=`0x00000010`)	SACK Permitted
2^5 (=`0x00000020`)	SACK
2^6 (=`0x00000040`)	Echo (obsoleted by option 8)
2^7 (=`0x00000080`)	Echo Reply (obsoleted by option 8)
2^8 (=`0x00000100`)	Timestamps
2^9 (=`0x00000200`)	Partial Order Connection Permitted (obsolete)
2^{10} (=`0x00000400`)	Partial Order Service Profile (obsolete)
2^{11} (=`0x00000800`)	CC (obsolete)
2^{12} (=`0x00001000`)	CC.NEW (obsolete)
2^{13} (=`0x00002000`)	CC.ECHO (obsolete)
2^{14} (=`0x00004000`)	TCP Alternate Checksum Request (obsolete)
2^{15} (=`0x00008000`)	TCP Alternate Checksum Data (obsolete)

tcpOptions	Description
2^{16} (=0x00010000)	Skeeter
2^{17} (=0x00020000)	Bubba
2^{18} (=0x00040000)	Trailer Checksum Option
2^{19} (=0x00080000)	MD5 Signature Option (obsoleted by option 29)
2^{20} (=0x00100000)	SCPS Capabilities
2^{21} (=0x00200000)	Selective Negative Acknowledgements
2^{22} (=0x00400000)	Record Boundaries
2^{23} (=0x00800000)	Corruption experienced
2^{24} (=0x01000000)	SNAP
2^{25} (=0x02000000)	Unassigned (released 2000-12-18)
2^{26} (=0x04000000)	TCP Compression Filter
2^{27} (=0x08000000)	Quick-Start Response
2^{28} (=0x10000000)	User Timeout Option (also, other known unauthorized use)
2^{29} (=0x20000000)	TCP Authentication Option (TCP-AO)
2^{30} (=0x40000000)	Multipath TCP (MPTCP)
2^{31} (=0x80000000)	all options > 31

1.4 Packet File Output

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

Column	Description	Flags
ipTOS	IP Type of Service	
ipID	IP ID	
ipIDDiff	IP ID diff	
ipFrag	IP fragment	
ipTTL	IP TTL	
ipHdrChkSum	IP header checksum	
ipCalChkSum	IP header computed checksum	
l4HdrChkSum	Layer 4 header checksum	
l4CalChkSum	Layer 4 header computed checksum	
ipFlags	IP flags	
ipOptLen	IP options length	
ipOpts	IP options	
seq	Sequence number	
ack	Acknowledgement number	
seqDiff	Sequence number diff	SEQ_ACK_NUM=1
ackDiff	Acknowledgement number diff	SEQ_ACK_NUM=1
seqPktLen	Sequence packet length	SEQ_ACK_NUM=1
ackPktLen	Acknowledgement packet length	SEQ_ACK_NUM=1
tcpFStat	TCP aggregated protocol flags (CWR, ACK, PSH, RST, SYN, FIN)	

Column	Description	Flags
tcpFlags	Flags	
tcpAnomaly	TCP aggregated header anomaly flags	
tcpWin	TCP window size	
tcpOptLen	TCP options length	
tcpOpts	TCP options	

1.5 Plugin Report Output

The aggregated ipFlags, tcpAnomaly and tcpWinSzThRt are reported.

1.6 References

- http://www.iana.org/assignments/ip-parameters
- http://www.iana.org/assignments/tcp-parameters/tcp-parameters.xml