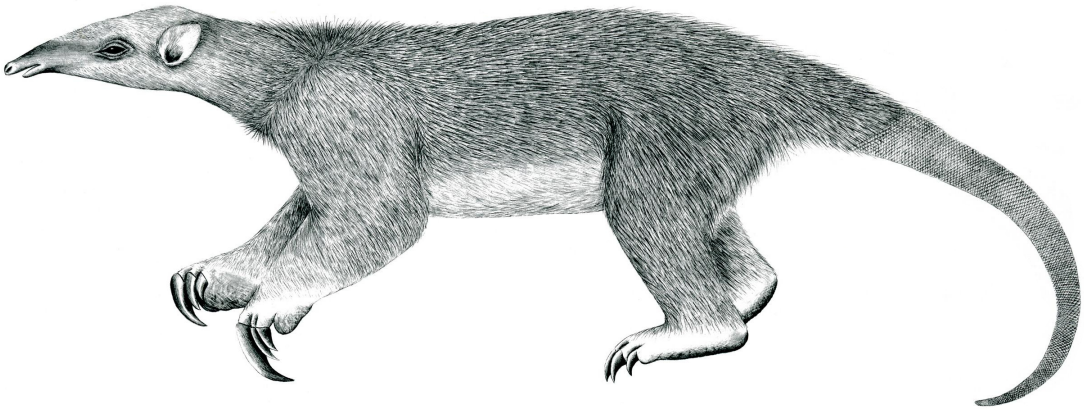
Tranalyzer2

tcpFlags

IP and TCP flags



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	Flags
IPTOS	0	IPv4 ToS / IPv6 Class representation: 0: IP ToS hex 1: DSCP_ECN decimal 2: Precedence(1-7)_ECN decimal	
RTT_ESTIMATE	1	Estimate Round trip time	
IPCHECKSUM	2	0: No checksums calculation 1: Calculation of L3 (IP) header checksum 2: Calculation of L3 (IP) and L4 (TCP, UDP, . . .) checksum	
WINDOWSIZE	1	Output TCP window size parameters	
WINMIN	1	Min. window size threshold defining a healthy communication (only packets below the threshold are counted)	
SEQ_ACK_NUM	1	Output Sequence/Acknowledge number features	
FRAG_ANALYZE	1	Enable fragmentation analysis	
NAT_BT_EST	1	Estimate NAT boot time	
SCAN_DETECTOR	1	Enable scan flow detector	
MPTCP	1	Enable MPTCP dissection	
TCPJA4T	1	Output JA4T/JA4TS fingerprints	
JA4TOPTMX	20	Maximal options stored in flow	TCPJA4T=1
TCPFLGCNT	1	TCP flags counts	
SPKTMD_SEQACKREL	0	SEQ/ACK numbers representation (-s option): 0: absolute 1: relative	SEQ_ACK_NUM=1
SPKTMD_SEQACKHEX	0	SEQ/ACK numbers representation (-s option): 0: uint32_t 1: hex32	SEQ_ACK_NUM=1

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 (ToS)	IPTOS=0
ipToSDscp_ecn	U8_U8	IP ToS: DSCP and ECN	IPTOS=1
ipToSPrec_ecn	U8_U8	IP ToS: Precedence and ECN	IPTOS=2
ipFlags	H16	IP aggregated flags	
ipOptCnt	U16	IP options count	IPV6_ACTIVATE=0|2
ipOptCpCl_Num	H8_H32	IP aggregated options, copy-class and number	IPV6_ACTIVATE=0|2
ip6OptCntHH_D	U16_U16	IPv6 aggregated Hop-by-Hop dest. option counts	IPV6_ACTIVATE>0
ip6OptHH_D	H32_H32	IPv6 Hop-by-Hop destination options	IPV6_ACTIVATE>0
tcpISeqN	U32	TCP initial sequence number	SEQ_ACK_NUM=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
tcpBFlgtMx	U32	TCP max bytes in flight	SEQ_ACK_NUM=1
tcpInitWinSz	U32	TCP initial effective window size	WINDOWSIZE=1
tcpAvgWinSz	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	H16	TCP aggregated protocol flags (FIN, SYN, RST, PSH, ACK, URG, ECE, CWR)	
tcpAnomaly	H16	TCP aggregated header anomaly flags	
tcpCntF_S_R_P_A_ U_E_C_FA_SA_ RA_N_SF_SFR_ RF_X	16xU16	TCP flags counts: FIN, SYN, RST, PSH, ACK, URG, ECE, CWR, FIN-ACK, SYN-ACK, RST-ACK, none, SYN-FIN, SYN-FIN-RST RST-FIN, Xmas (FIN-PSH-URG)	TCPFLGCNT=1
tcpJA4T	SC	TCP JA4T/JA4TS fingerprint	TCPJA4T=1

Column	Type	Description	Flags
tcpOptPktCnt	U16	TCP options packet count	
tcpOptCnt	U16	TCP options count	
tcpOptions	H32	TCP aggregated options	
tcpMSS	U16	TCP maximum segment size	
tcpWS	U16	TCP window scale factor	
tcpMPTBF	H16	MPTCP type bitfield	MPTCP=1
tcpMPF	H8	MPTCP flags	MPTCP=1
tcpMPAID	U8	MPTCP address ID	MPTCP=1
tcpMPDSSF	H8	MPTCP DSS flags	MPTCP=1
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
tcpUtm	D	TCP estimated up time	NAT_BT_EST=1
tcpBtm	TS	TCP estimated boot time	NAT_BT_EST=1
tcpSSASAATrip	F	TCP trip time: A flow: SYN, SYN-ACK B flow: SYN-ACK, ACK	RTT_ESTIMATE=1
tcpRTTAckTripMin	F	TCP ACK trip minimum	RTT_ESTIMATE=1
tcpRTTAckTripMax	F	TCP ACK trip maximum	RTT_ESTIMATE=1
tcpRTTAckTripAvg	F	TCP ACK trip average	RTT_ESTIMATE=1
tcpRTTAckTripJitAvg	F	TCP ACK trip jitter average	RTT_ESTIMATE=1
tcpRTTSseqAA	F	TCP round trip time: A flow: SYN, SYN-ACK, ACK B flow: ACK-ACK	RTT_ESTIMATE=1
tcpRTTAckJitAvg	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 good for inter-distance assessment
0x0002	TCP option init
0x0004	Timestamp option decreasing
0x0008	L4 option field corrupt or not acquired
0x0010	Window state-machine initialized
0x0020	Window update
0x0040	Win 0 probe
0x0080	Win 0 probe ACK
0x0100	Min Window detected

tcpFStat	Description
0x0200	WS used
0x0400	Window Receiver full
0x0800	Window state-machine count up(1)/down(0)
0x1000	L4 Checksum calculation if present
0x2000	UDPLITE Checksum coverage error
0x4000	TCP Selective ACK Option
0x8000	MPTCP detected

1.3.2 ipToS

The ipToS column is to be interpreted as follows:

ipToS	Description
0x01	ECN0: enable ECN when requested by incoming connections, and also request ECN on outgoing connection attempts
0x02	ECN1: (default) enable ECN when requested by incoming connections, but do not request ECN on outgoing connections
0x04	Precedence 0
0x08	Precedence 1
0x10	Precedence 2
0x20	Precedence 3: Class Sel 0
0x40	Precedence 4: Class Sel 1
0x80	Precedence 5: Class Sel 2

1.3.3 ipToS precedence description

The precedence in ipToS, Mode 0-2 is defined by the following table according to RFC 2474:

DSCP	Hex Md 0 Values	Dec Md 1-2 Values	Precedence: Description
CS0	0x00	0	Best Effort
LE	0x01	1	—
CS1	0x20,0x28,0x30,0x38	8, 10, 12, 14	1: Priority
CS2	0x40,0x48,0x50,0x58	16, 18, 20, 22	2: Immediate
CS3	0x60,0x68,0x70,0x78	24, 26, 28, 30	3: Flash - mainly used for voice signaling
CS4	0x80,0x88,0x90,0x98	32, 34, 36, 38	4: Flash Override
CS5	0xa0,0xb8	40, 46	5: Critical - mainly used for voice RTP
CS6	0xc0	48	6: Internetwork Control
CS7	0xe0	56	7: Network Control

1.3.4 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: Don't 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	Length in L3/4 header < actual L3/4 length
0x2000	Length in UDP/UDP-Lite header $\neq$ actual UDP/UDP-Lite length
0x4000	Packet inter-distance = 0
0x8000	Packet inter-distance < 0

1.3.5 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.

1.3.6 tcpFlags

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

	tcpFlags	Description
2^0	(=0x0001)	FIN: No more data, finish connection
2^1	(=0x0002)	SYN: Synchronize sequence numbers
2^2	(=0x0004)	RST: Reset connection
2^3	(=0x0008)	PSH: Push data
2^4	(=0x0010)	ACK: Acknowledgement field value valid
2^5	(=0x0020)	URG: Urgent pointer valid
2^6	(=0x0040)	ECE: ECN-Echo
2^7	(=0x0080)	CWR: Congestion Window Reduced flag is set
2^8	(=0x0100)	FIN-ACK: Acknowledgment of FIN
2^9	(=0x0200)	SYN-ACK: Acknowledgment of SYN
2^{10}	(=0x0400)	RST-ACK: Acknowledgment of RST
2^{11}	(=0x0800)	Potential NULL scan packet or malicious channel
2^{12}	(=0x1000)	SYN-FIN flag: potential scan packet or malicious packet
2^{13}	(=0x2000)	SYN-FIN-RST flag: potential scan packet or malicious channel
2^{14}	(=0x4000)	FIN-RST flag: abnormal flow termination

	tcpFlags	Description
2^{15}	(=0x8000)	Potential Xmas scan packet (FIN-PSH-URG) or malicious channel

1.3.7 tcpAnomaly

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

tcpAnomaly	Description
0x0001	SYN retransmission
0x0002	SEQ retransmission
0x0004	SEQ fast retransmission
0x0008	Duplicate ACK
0x0010	TCP Keep-Alive
0x0020	TCP Keep-Alive ACK
0x0040	Sequence number out-of-order
0x0080	Sequence mess in flow order due to pcap packet loss
0x0100	ACK for unseen packet
0x0200	Previous packet not captured
0x0100	-
0x0200	-
0x1000	Scan detected in flow
0x2000	Successful Scan detected in flow
0x4000	SYN flag with L7 content
0x8000	-

1.3.8 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)

	tcpOptions	Description
2^{13}	(=0x00002000)	CC.ECHO (obsolete)
2^{14}	(=0x00004000)	TCP Alternate Checksum Request (obsolete)
2^{15}	(=0x00008000)	TCP Alternate Checksum Data (obsolete)
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

1.3.9 tcpMPTBF

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

	tcpMPTBF	Description
2^0	(=0x0001)	TCP_MP_CAPABLE
2^1	(=0x0002)	TCP_MP_JOIN
2^2	(=0x0004)	TCP_MP_DSS
2^3	(=0x0008)	TCP_MP_ADD_ADDR
2^4	(=0x0010)	TCP_MP_REM_ADDR
2^5	(=0x0020)	TCP_MP_PRIO
2^6	(=0x0040)	TCP_MP_FAIL
2^7	(=0x0080)	TCP_MP_FSTCLS
2^{15}	(=0x8000)	TCP_MP_PRIV

1.4 Packet File Output

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

Column	Type	Description	Flags
ipToS	H8	IP Type of Service (ToS)	IPTOS=0
ipToSDcsp_ecn	U8_U8	IP ToS: Precedence and ECN	IPTOS=1
ipToSPrec_ecn	H8	IP ToS: DSCP and ECN	IPTOS=2
ipID	U16	IP ID	
ipIDDiff	I32	IP ID diff	
ipFrag	H16	IP fragment	
ipTTL	U8	IP TTL	
ipHdrChkSum	H16	IP header checksum	
ipCalChkSum	H16	IP header computed checksum	
l4HdrChkSum	H16	Layer 4 header checksum	
l4CalChkSum	H16	Layer 4 header computed checksum	
ipFlags	H16	IP flags	
ip6HHOptLen	I16	IPv6 Hop-by-Hop options length	IPV6_ACTIVATE>0
ip6HHOpts	R(H8)	IPv6 Hop-by-Hop options	IPV6_ACTIVATE>0
ip6DOptLen	I16	IPv6 Destination options length	IPV6_ACTIVATE>0
ip6DOpts	R(H8)	IPv6 Destination options	IPV6_ACTIVATE>0
ipOptLen	I16	IPv4 options length	IPV6_ACTIVATE=0|2
ipOpts	R(H8)	IPv4 options	IPV6_ACTIVATE=0|2
seq	U32/H32	Sequence number	SEQ_ACK_NUM=1
ack	U32/H32	Acknowledgement number	SEQ_ACK_NUM=1
seqMax	U32/H32	Sequence number max	SEQ_ACK_NUM=1
seqDiff	I32	Sequence number diff	SEQ_ACK_NUM=1
ackDiff	I32	Acknowledgement number diff	SEQ_ACK_NUM=1
seqLen	U32	Sequence length	SEQ_ACK_NUM=1
ackLen	U32	Acknowledgement length	SEQ_ACK_NUM=1
seqFlowLen	I64	Sequence flow length	SEQ_ACK_NUM=1
ackFlowLen	I64	Acknowledgement flow length	SEQ_ACK_NUM=1
tcpMLen	I64	Aggregated valid bytes transmitted so far	SEQ_ACK_NUM=1
tcpBFlgt	U32	Number of bytes in flight (not acknowledge)	SEQ_ACK_NUM=1
tcpFStat	H16	TCP aggregated protocol flags + combinations (CWR, ACK, PSH, RST, SYN, FIN, ...)	
tcpFlags	H16	Flags	
tcpAnomaly	H16	TCP aggregated header anomaly flags	
tcpWin	U32	TCP window size	
tcpWS	U16	TCP window scale factor	
tcpMSS	U16	TCP maximum segment size	
tcpTmS	U32	TCP time stamp	NAT_BT_EST=1
tcpTmER	U32	TCP time echo reply	NAT_BT_EST=1
tcpMPTyp	U16	MPTCP type	MPTCP=1
tcpMPF	H8	MPTCP flags	MPTCP=1
tcpMPAID	U8	MPTCP address ID	MPTCP=1
tcpMPDSSF	H8	MPTCP DSS flags	MPTCP=1
tcpOptLen	I32	TCP options length	
tcpOpts	R(H8)	TCP options	

1.5 Monitoring Output

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

Column	Type	Description	Flags
tcpScan	U64	Number of TCP scans attempted	
tcpSuccScan	U64	Number of TCP scans successful	
tcpSynRetries	U64	Number of TCP SYN retries	
tcpSeqRetries	U64	Number of TCP seq retries	

1.6 Plugin Report Output

The following information is reported:

- Aggregated ipFlags
- Aggregated tcpFlags
- Aggregated tcpAnomaly
- Aggregated ipToS
- Number of TCP scans attempted, successful
- Number of TCP SYN retries, seq retries
- Number of WinSz below WINMIN

1.7 References

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