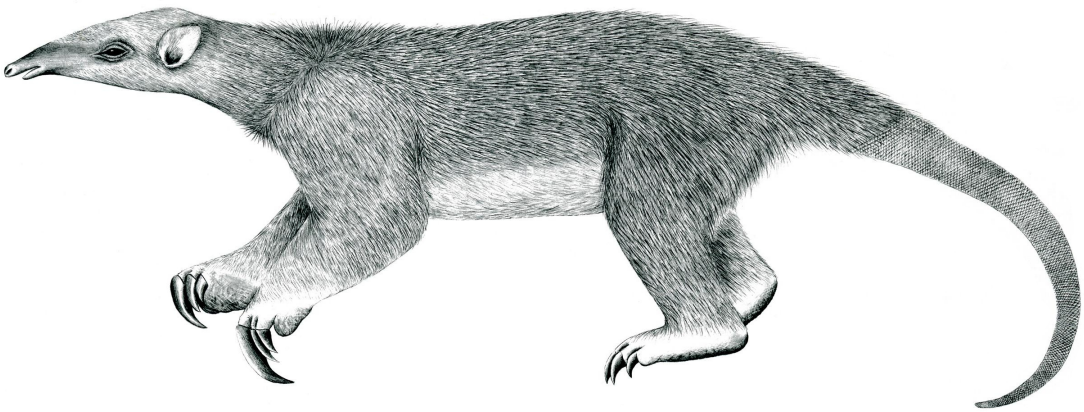
Tranalyzer2

dnsDecode

Domain Name System (DNS)



Tranalyzer Development Team

Contents

1 dnsDecode

1.1 Description

The dnsDecode plugin analyzes DNS traffic.

1.2 Configuration Flags

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

Name	Default	Description
DNS_MODE	4	0: Only aggregated header count info 1: +REQ records 2: +ANS records 3: +AUX records 4: +ADD records
DNS_HEXON	1	0: Hex output flags off 1: Hex output flags on
DNS_HDRMD	0	Header, OpCode, RetCode: 0: Bitfield 1: Numeric 2: String
DNS_AGGR	0	0: Full vectors 1: Aggregate records
DNS_TYPE	0	Q/A type format: 0: Numeric 1: String
DNS_QRECMAX	15	Max # of query records / flow
DNS_ARECMAX	20	Max # of answer records / flow
DNS_WHO	0	1: Output country and organization of DNS reply addresses
DNS_MAL_TEST	0	0: No tests for malware 1: Mal test @ flow terminated 2: Mal test @ L4Callback, pcad ops
DNS_MAL_TYPE	0	Malware type format: 0: code 1: string
The following additional flag is available in malsite.h:		
DNS_MAL_DOMAIN	1	0: Malsite IP address labeling mode 1: Malsite domain labeling mode, not implemented yet

DNS_MAL_TEST controls where the mal test is performed. Only in L4Callback enables a cooperation with pcaps, so that pcapd dumps all packets of a flow after the alarm was detected.

1.3 Flow File Output

The dnsDecode plugin outputs the following columns:

Column	Type	Description	Flags
dnsStat	H16	Status, warnings and errors	
dnsHdrOPField	H16	Header field of last packet in flow	
dnsHFlg_ OpC_ RetC	H8_ H16_ H16	Aggregated header flags, operational code and return code	DNS_HDRMD=0
dnsHFlg	H8	Aggregated header flags	DNS_HDRMD>0
dnsOpC	H16	Operational code	DNS_HDRMD=1
dnsOpN	S	Operational string	DNS_HDRMD=2
dnsRetC	H16	Return code	DNS_HDRMD=1
dnsRetN	S	Return string	DNS_HDRMD=2
dnsCntQu_ Asw_ Aux_ Add	R(U16_ U16_ U16_ U16)	# of question records, answer records, auxiliary records and additional records	
dnsAAAqF	F	DDOS DNS AAA / query factor	

If DNS_MODE>0, the following columns are displayed:

dnsTypeBF3_BF2_BF1_BF0	H8_H16_H16_H64	Type bitfields	DNS_HEXON=1
dnsQname	R(S)	Query name records	
dnsMalCnt	U32	Domain malware count	DNS_MAL_TEST>0 && DNS_MAL_DOMAIN=1
dnsMalType	R(S)	Domain malware type string	DNS_MAL_TEST>0 && DNS_MAL_DOMAIN=1&& DNS_MAL_TYPE=1&&
dnsMalCode	R(U32)	Domain malware code	DNS_MAL_TEST>0 && DNS_MAL_DOMAIN=1&& DNS_MAL_TYPE=0
dnsAname	R(S)	Answer name records	
dnsAPname	R(S)	Name CNAME entries	
dns4Aaddress	R(IP4)	Address entries IPv4	
dns4CC_Org	R(SC_S)	IPv4 country and organization	DNS_WHO=1
dns6Aaddress	R(IP6)	Address entries IPv6	
dns6CC_Org	R(SC_S)	IPv6 country and organization	DNS_WHO=1
dnsIPMalCode	R(H32)	IP malware code	DNS_MAL_TEST>0&& DNS_MAL_DOMAIN=0
dnsQType	R(U16)	Query record type entries	DNS_TYPE=0
dnsQTypeN	R(S)	Query record type names	DNS_TYPE=1
dnsQClass	R(U16)	Query record class entries	
dnsAType	R(U16)	Answer record type entries	DNS_TYPE=0
dnsATypeN	R(S)	Answer record type names	DNS_TYPE=1

Column	Type	Description	Flags
dnsAClass	R(U16)	Answer record class entries	
dnsATTL	R(U32)	Answer record TTL entries	
dnsMXpref	R(U16)	MX record preference entries	
dnsSRVprio	R(U16)	SRV record priority entries	
dnsSRVwgt	R(U16)	SRV record weight entries	
dnsSRVprt	R(U16)	SRV record port entries	
dnsOptStat	R(H32)	Option status	

1.3.1 dnsStat

The dnsStat column is to be interpreted as follows:

dnsStat	Description
2^0 (=0x0001)	DNS ports detected
2^1 (=0x0002)	NetBIOS DNS
2^2 (=0x0004)	DNS TCP aggregated fragmented content
2^3 (=0x0008)	DNS TCP fragmented content state
2^4 (=0x0010)	—
2^5 (=0x0020)	Warning: ANY: Zone all from a domain or cached server
2^6 (=0x0040)	Warning: Incremental DNS zone transfer detected
2^7 (=0x0080)	Warning: DNS zone transfer detected
2^8 (=0x0100)	Warning: DNS UDP length exceeded
2^9 (=0x0200)	Warning: following records ignored
2^{10} (=0x0400)	Warning: Max DNS query records exceeded... increase DNS_QRECMAX
2^{11} (=0x0800)	Warning: Max DNS answer records exceeded... increase DNS_ARECMAX
2^{12} (=0x1000)	Error: DNS record length error
2^{13} (=0x2000)	Error: Wrong DNS PTR detected
2^{14} (=0x4000)	Warning: DNS length undercut
2^{15} (=0x8000)	Error: UDP/TCP DNS header corrupt or TCP packets missing

1.3.2 dnsHdrOPField

From the 16 bit DNS header the QR bit and bit five to nine are extracted and mapped in their correct sequence into a byte as indicated below. It provides for a normal single packet exchange flow an accurate status of the DNS transfer. For a multiple packet exchange only the last packet is mapped into the variable. In that case the aggregated header state flags should be considered.

QR	Opcode	AA	TC	RD	RA	Z	AD	CD	Rcode
1	0000	1	0	1	1	1	0	0	0000

1.3.3 dnsHFlg_OpC_RetC

For multi-packet DNS flows e.g. via TCP the aggregated header state bit field describes the status of all packets in a flow. Thus, flows with certain client and server states can be easily identified and extracted during post-processing.

	dnsHFlg	Short	Description
2^7	(=0x01)	CD	Checking disabled
2^6	(=0x02)	AD	Authenticated data
2^5	(=0x04)	Z	Zone transfer
2^4	(=0x08)	RA	Recursive query support available
2^3	(=0x10)	RD	Recursion desired
2^2	(=0x20)	TC	Message truncated
2^1	(=0x40)	AA	Authoritative answer
2^0	(=0x80)	QR	0: Query / 1: Response

The four bit opcode field of the DNS header is mapped via [2^{opcode}] and an OR into a 16 bit field. Thus, the client can be monitored or anomalies easily identified. E.g. appearance of reserved bits might be an indication for a covert channel or malware operation.

	dnsOpC	Description
2^0	(=0x0001)	Standard query
2^1	(=0x0002)	Inverse query
2^2	(=0x0004)	Server status request
2^3	(=0x0008)	—
2^4	(=0x0010)	Notify
2^5	(=0x0020)	Update / Register (NetBIOS)
2^6	(=0x0040)	Release (NetBIOS)
2^7	(=0x0080)	Wait For Acknowledge (NetBIOS)
2^8	(=0x0100)	Refresh (NetBIOS)
2^9	(=0x0200)	reserved
2^{10}	(=0x0400)	reserved
2^{11}	(=0x0800)	reserved
2^{12}	(=0x1000)	reserved
2^{13}	(=0x2000)	reserved
2^{14}	(=0x4000)	reserved
2^{15}	(=0x8000)	reserved

The four bit rcode field of the DNS header is mapped via [2^{rcode}] and an OR into a 16 bit field. It provides valuable information about success of DNS queries and therefore facilitates the detection of failures, misconfigurations and malicious operations.

dnsRetC	Short	Description
2^0 (=0x0001)	No error	Request completed successfully
2^1 (=0x0002)	Format error	Name server unable to interpret query
2^2 (=0x0004)	Server failure	Name server unable to process query due to problem with name server
2^3 (=0x0008)	Name error	Authoritative name server only: Domain name in query does not exist
2^4 (=0x0010)	Not implemented	Name server does not support requested kind of query
2^4 (=0x0020)	Refused	Name server refuses to perform the specified operation for policy reasons
2^5 (=0x0040)	YXDomain	Name exists when it should not
2^6 (=0x0080)	YXRRSet	Resource record set exists when it should not
2^8 (=0x0100)	NXRRSet	Resource record set that should exist does not
2^9 (=0x0200)	NotAuth	Server not authoritative for zone
2^{10} (=0x0400)	NotZone	Name not contained in zone
2^{11} (=0x0800)	—	—
2^{12} (=0x1000)	—	—
2^{13} (=0x2000)	—	—
2^{14} (=0x4000)	—	—
2^{15} (=0x8000)	—	—

1.3.4 dnsTypeBF3_BF2_BF1_BF0

The 16 bit Type Code field is extracted from each DNS record and mapped via [2^{Typecode}] into a 64 bit fields. Gaps are avoided by additional higher bitfields defining higher codes.

dnsTypeBF3	Short	Description
2^0 (=0x01)	TA	DNSSEC Trust Authorities
2^1 (=0x02)	DLV	DNSSEC Lookaside Validation
2^2 (=0x04)	—	—
2^3 (=0x08)	—	—
2^4 (=0x10)	—	—
2^5 (=0x20)	—	—
2^6 (=0x40)	—	—
2^7 (=0x80)	—	—

dnsTypeBF2	Short	Description
2^0 (=0x0001)	TKEY	Transaction Key
2^1 (=0x0002)	TSIG	Transaction Signature
2^2 (=0x0004)	IXFR	Incremental transfer
2^3 (=0x0008)	AXFR	Transfer of an entire zone
2^4 (=0x0010)	MAILB	Mailbox-related RRs (MB, MG or MR)

dnsTypeBF2	Short	Description
2^5 (=0x0020)	MAILA	Mail agent RRs (OBSOLETE - see MX)
2^6 (=0x0040)	ZONEALL	Request for all records the server/cache has available
2^7 (=0x0080)	URI	URI
2^8 (=0x0100)	CAA	Certification Authority Restriction
2^9 (=0x0200)	—	—
2^{10} (=0x0400)	—	—
2^{11} (=0x0800)	—	—
2^{12} (=0x1000)	—	—
2^{13} (=0x2000)	—	—
2^{14} (=0x4000)	—	—
2^{15} (=0x8000)	—	—

dnsTypeBF1	Short	Description
2^0 (=0x0001)	SPF	
2^1 (=0x0002)	UINFO	
2^2 (=0x0004)	UID	
2^3 (=0x0008)	GID	
2^4 (=0x0010)	UNSPEC	
2^4 (=0x0020)	NID	
2^5 (=0x0040)	L32	
2^6 (=0x0080)	L64	
2^8 (=0x0100)	LP	
2^9 (=0x0200)	EUI48	EUI-48 address
2^{10} (=0x0400)	EUI64	EUI-48 address
2^{11} (=0x0800)	—	—
2^{12} (=0x1000)	—	—
2^{13} (=0x2000)	—	—
2^{14} (=0x4000)	—	—
2^{15} (=0x8000)	—	—

dnsTypeBF0	Short	Description
2^0 (=0x0000.0000.0000.0001)	—	—
2^1 (=0x0000.0000.0000.0002)	A	IPv4 address
2^2 (=0x0000.0000.0000.0004)	NS	Authoritative name server
2^3 (=0x0000.0000.0000.0008)	MD	Mail destination. Obsolete use MX instead
2^4 (=0x0000.0000.0000.0010)	MF	Mail forwarder. Obsolete use MX instead

dnsTypeBF0		Short	Description
2^{5}	(=0x0000.0000.0000.0020)	CNAME	Canonical name for an alias
2^{6}	(=0x0000.0000.0000.0040)	SOA	Marks the start of a zone of authority
2^{7}	(=0x0000.0000.0000.0080)	MB	Mailbox domain name
2^{8}	(=0x0000.0000.0000.0100)	MG	Mail group member
2^{9}	(=0x0000.0000.0000.0200)	MR	Mail rename domain name
2^{10}	(=0x0000.0000.0000.0400)	NULL	Null resource record
2^{11}	(=0x0000.0000.0000.0800)	WKS	Well known service description
2^{12}	(=0x0000.0000.0000.1000)	PTR	Domain name pointer
2^{13}	(=0x0000.0000.0000.2000)	HINFO	Host information
2^{14}	(=0x0000.0000.0000.4000)	MINFO	Mailbox or mail list information
2^{15}	(=0x0000.0000.0000.8000)	MX	Mail exchange
2^{16}	(=0x0000.0000.0001.0000)	TXT	Text strings
2^{17}	(=0x0000.0000.0002.0000)	—	Responsible Person
2^{18}	(=0x0000.0000.0004.0000)	AFSDB	AFS Data Base location
2^{19}	(=0x0000.0000.0008.0000)	X25	X.25 PSDN address
2^{20}	(=0x0000.0000.0010.0000)	ISDN	ISDN address
2^{21}	(=0x0000.0000.0020.0000)	RT	Route Through
2^{22}	(=0x0000.0000.0040.0000)	NSAP	NSAP address. NSAP style A record
2^{23}	(=0x0000.0000.0080.0000)	NSAP-PTR	—
2^{24}	(=0x0000.0000.0100.0000)	SIG	Security signature
2^{25}	(=0x0000.0000.0200.0000)	KEY	Security key
2^{26}	(=0x0000.0000.0400.0000)	PX	X.400 mail mapping information
2^{27}	(=0x0000.0000.0800.0000)	GPOS	Geographical Position
2^{28}	(=0x0000.0000.1000.0000)	AAAA	IPv6 Address
2^{29}	(=0x0000.0000.2000.0000)	LOC	Location Information
2^{30}	(=0x0000.0000.4000.0000)	NXT	Next Domain (obsolete)
2^{31}	(=0x0000.0000.8000.0000)	EID	Endpoint Identifier
2^{32}	(=0x0000.0001.0000.0000)	NIMLOC/NB	Nimrod Locator / NetBIOS general Name Service
2^{33}	(=0x0000.0002.0000.0000)	SRV/NBSTAT	Server Selection / NetBIOS NODE STATUS
2^{34}	(=0x0000.0004.0000.0000)	ATMA	ATM Address
2^{35}	(=0x0000.0008.0000.0000)	NAPTR	Naming Authority Pointer
2^{36}	(=0x0000.0010.0000.0000)	KX	Key Exchanger
2^{37}	(=0x0000.0020.0000.0000)	CERT	—
2^{38}	(=0x0000.0040.0000.0000)	A6	A6 (OBSOLETE - use AAAA)
2^{39}	(=0x0000.0080.0000.0000)	DNAME	—
2^{40}	(=0x0000.0100.0000.0000)	SINK	—
2^{41}	(=0x0000.0200.0000.0000)	OPT	—

	dnsTypeBF0	Short	Description
2^{42}	(=0x0000.0400.0000.0000)	APL	—
2^{43}	(=0x0000.0800.0000.0000)	DS	Delegation Signer
2^{44}	(=0x0000.1000.0000.0000)	SSHFP	SSH Key Fingerprint
2^{45}	(=0x0000.2000.0000.0000)	IPSECKEY	—
2^{46}	(=0x0000.4000.0000.0000)	RRSIG	—
2^{47}	(=0x0000.8000.0000.0000)	NSEC	NextSECure
2^{48}	(=0x0001.0000.0000.0000)	DNSKEY	—
2^{49}	(=0x0002.0000.0000.0000)	DHCID	DHCP identifier
2^{50}	(=0x0004.0000.0000.0000)	NSEC3	—
2^{51}	(=0x0008.0000.0000.0000)	NSEC3PARAM	—
2^{52}	(=0x0010.0000.0000.0000)	TLSA	—
2^{53}	(=0x0020.0000.0000.0000)	SMIMEA	S/MIME cert association
2^{54}	(=0x0040.0000.0000.0000)	—	
2^{55}	(=0x0080.0000.0000.0000)	HIP	Host Identity Protocol
2^{56}	(=0x0100.0000.0000.0000)	NINFO	—
2^{57}	(=0x0200.0000.0000.0000)	RKEY	—
2^{58}	(=0x0400.0000.0000.0000)	TALINK	Trust Anchor LINK
2^{59}	(=0x0800.0000.0000.0000)	CDS	Child DS
2^{60}	(=0x1000.0000.0000.0000)	CDNSKEY	DNSKEY(s) the Child wants reflected in DS
2^{61}	(=0x2000.0000.0000.0000)	OPENPGPKEY	OpenPGP Key
2^{62}	(=0x4000.0000.0000.0000)	CSYNC	Child-To-Parent Synchronization
2^{63}	(=0x8000.0000.0000.0000)	—	

1.4 Packet File Output

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

Column	Type	Description	Flags
dnsIPs	R(IP)	IP addresses (A/AAAA records)	DNS_WHO=0
dnsIPs_cntry_org	R(IP_S_S)	IP addresses, countries and organizations (A/AAAA records)	DNS_WHO=1
dnsStat	H16	Status, warnings and errors	
dnsHdr	H16	Header field of packet	DNS_HDRMD=0
dnsHFlg_OpC_RetC	H8_H16_H16	Aggregated header flags, operational and return codes	DNS_HDRMD=1
dnsHFlg_OpN_RetN	H8_S_S	Aggregated header flags, operational and return strings	DNS_HDRMD=2
dnsCntQu_	U16_	# of question records,	
Asw_	U16_	answer records,	
Aux_	U16_	auxiliary records and	
Add	U16	additional records	

1.5 Monitoring Output

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

Column	Type	Description	Flags
dnsPkts	U64	Number of DNS packets	
dnsQPkts	U64	Number of DNS Q packets	
dnsRPkts	U64	Number of DNS R packets	

1.6 Plugin Report Output

The following information is reported:

- Aggregated dnsStat
- Aggregated dnsHFlg, dnsOpC, dnsRetC
- Number of DNS packets
- Number of DNS Q packets
- Number of DNS R packets
- Number of alarms (DNS_MAL_TEST>0)

1.7 Example Output

The idea is that the string and integer array elements of question, answer, TTL and Type record entries match by column index so that easy script based mapping and post processing is possible. A sample output is shown below. Especially when large records are present the same name is printed several times which might degrade the readability. Therefore, a next version will have a multiple Aname suppressor switch, which should be off for script based post-processing.

Query name	Answer name	Answer address	TTL	Type
www.macromedia.com;	www.macromedia.com;www-mm.wip4.adobe.com	0.0.0.0;8.118.124.64	2787;4	5;1

1.8 TODO

- Compressed mode for DNS records