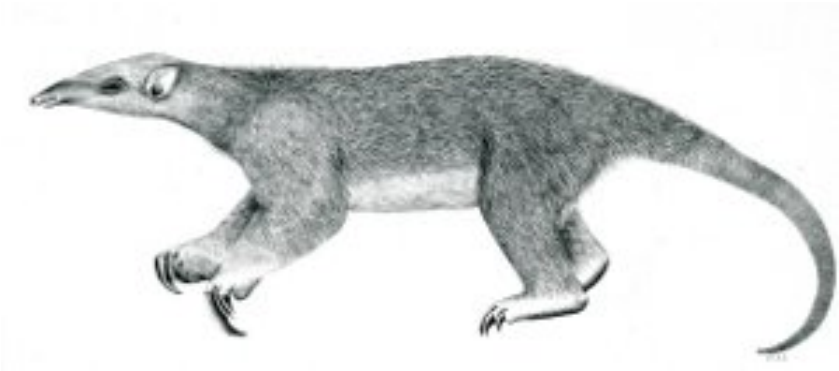
Tranalyzer2

dnsDecode

Domain Name System (DNS)



Tranalyzer Development Team

Contents

1 dnsDecode

1.1 Description

This plugin produces DNS header and content information encountered during the lifetime of a flow. The idea is to identify DNS header and payload features using flow parameters in order to extract information about applications or users. The DNS plugin requires no dependencies and produces only output to the flow file. User defined compiler switches in *dnsDecode.h, malsite.h* produce optimized code for the specific application.

1.2 Configuration Flags

The flow based output and the extracted information can be controlled by switches and constants listed in the table below. The most important one is `DNS_MODE` which controls the amount of information in the flow file. `DNS_AGGR` controls the aggregation of duplicate names and values. The last three limit the amount of memory allocated for flow based DNS record storage. The default values revealed reasonable performance in practise.

Name	Default	Description	Flags
`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_REQA`	0	0: full vectors, 1: Aggregate request records	
`DNS_ANSA`	0	0: full vectors, 1: Aggregate answer records	
`DNS_QRECMAX`	15	Max # of query records / flow	
`DNS_ARECMAX`	20	Max # of answer records / flow	
`MAL_TEST`	0	1: activate blacklist malware test mode (IPv4 only)	
`MAL_TYPE`	0	1: Type string; 0: Code	
The following additional flag is available in `malsite.h`:			
`MAL_DOMAIN`	1	0: malsite ip address labeling mode 1: malsite domain labeling mode	

1.3 Flow File Output

The default settings will result in 11 tab separated columns in the flow file where the items in column 6-11 are sequences of strings containing DNS record name, address entries and specific DNS entry information such as Type or TTL separated by semicolons. The idea is that the array elements of strings of the different columns correspond to each other so that easy script based post processing is possible. The different output modes controlled by `DNS_MODE` provide an incremental method from a high speed compressed representation to a full human readable representation.

Column	Type	Description	Flags
dnsStat	H16	Status, warnings and errors	
dnsHdriOPField	H16	Header field of last packet in flow	
DnsStat_	H8_	Aggregated header status,	

Column	Type	Description	Flags
OpC_	H16_	opcode and	
RetC	H16	return code	
dnsCntQu_	R:U16_	# of question records	
Asw_	U16_	# answer records	
Aux_	U16_	# of auxiliary records	
Add	U16	# additional records	
dnsAAAqF	F	DDOS DNS AAA / Query factor	
dnsTypeBF3_BF2_BF1_BF0	H8_H16_H16_H64	Type bitfields	DNS_MODE > 0
dnsQname	RS	Query Name records	DNS_MODE > 1
dnsMalType	RS	Domain Malware Type String	MAL_TEST=1 && MAL_TYPE=1 && MAL_DOMAIN=1
dnsMalCode	RH32	Domain Malware code	MAL_TEST=1 && MAL_TYPE=0 && MAL_DOMAIN=1
dnsAname	RS	Answer Name records	
dnsAPname	RS	Name CNAME entries	
dns4Aaddress	RIP4	Address entries IPv4	
dns6Aaddress	RIP6	Address entries IPv6	
dnsIPMalCode	RH32	IP Malware code	MAL_TEST=1 && MAL_DOMAIN=0
dnsAType	RU16	Answer record Type entries	
dnsAClass	RU16	Answer record Class entries	
dnsATTL	RU32	Answer record TTL entries	
dnsMXpref	RU16	MX record preference entries	
dnsSRVprio	RU16	SRV record priority entries	
dnsSRVwgt	RU16	SRV record weight entries	
dnsOptStat	RU32	option status	
dnsOptCodeOwn	RU16	option code owner	

1.3.1 dnsStat

The DNS status bit field listed below provides an efficient method to post process flow data files in order to detect incidents during flow processing.

dnsStat	Type	Description
2^0 (=0x0001)	DNS_PRTDT	DNS ports detected
2^1 (=0x0002)	DNS_NBIOS	NetBios DNS
2^2 (=0x0004)	DNS_FRAGA	DNS TCP aggregated fragmented content
2^3 (=0x0008)	DNS_FRAGS	DNS TCP fragmented content state
2^4 (=0x0010)	DNS_FTRUNC	Warning: Name truncated
2^5 (=0x0020)	DNS_ANY	Warning: ANY: Zone all from a domain or cached server
2^6 (=0x0040)	DNS_IZTRANS	Warning: Incremental DNS zone transfer detected
2^7 (=0x0080)	DNS_ZTRANS	Warning: DNS zone transfer detected

dnsStat	Type	Description
2^8 (=0x0100)	DNS_WRNULN	Warning: DNS UDP Length exceeded
2^9 (=0x0200)	DNS_WRNIGN	Warning: following Records ignored
2^{10} (=0x0400)	DNS_WRNDEX	Warning: Max DNS name records exceeded
2^{11} (=0x0800)	DNS_WRNAEX	Warning: Max address records exceeded
2^{12} (=0x1000)	DNS_ERRLEN	Error: DNS record length error
2^{13} (=0x2000)	DNS_ERRPTR	Error: Wrong DNS PTR detected
2^{14} (=0x4000)	DNS_WRNMLN	Warning: DNS length undercut
2^{15} (=0x8000)	DNS_ERRCRPT	Error: UDP/TCP DNS Header corrupt or TCP packets missing

1.3.2 dnsHdriOPField

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 dnsHStat_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.

dnsHStat	Short	Description
2^7 (=0x01)	CD	Checking Disabled
2^6 (=0x02)	AD	Authenticated Data
2^5 (=0x04)	Z	Zero
2^4 (=0x08)	RA	Recursion Available
2^3 (=0x10)	RD	Recursion Desired
2^2 (=0x20)	TC	Truncated
2^1 (=0x40)	AA	Authoritative Answer
2^0 (=0x80)	QR	Query / 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)	QUERY, Standard query
2^1 (=0x0002)	IQUERY, Inverse query
2^2 (=0x0004)	STATUS, Server status request
2^3 (=0x0008)	—
2^4 (=0x0010)	Notify

dnsOpC	Description
2^4 (=0x0020)	Update
2^5 (=0x0040)	reserved
2^6 (=0x0080)	reserved
2^8 (=0x0100)	reserved
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	RR Set Exists when it should not
2^8 (=0x0100)	NXRRSet	RR 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)	—	—

dnsTypeBF3	Short	Description
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)
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
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	—
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

dnsTypeBF0	Short	Description
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 Plugin Report Output

The following information is reported:

- Number of DNS IPv4/6 packets
- Number of DNS IPv4/6 Q,R packets
- Aggregated status flags (dnsStat)
- Number of alarms (MAL_TEST)

1.5 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

1.6 TODO

- Compressed mode for DNS records