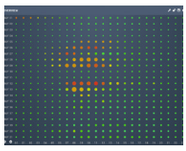
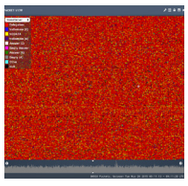
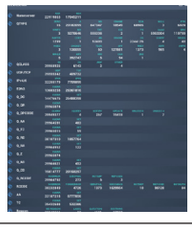
turing
by NOMINET

Decoding DNS data

Technical datasheet

Traffic graphs

The *turing by Nominet* UI provides access to the data collected through a set of traffic graphs. These can be selected by the user and displayed alone or together.

Graph type		Description	Variants	Data displayed	Options
Overview		Visualisation overview of DNS traffic	n/a	Volume of traffic and ratio of NXDOMAIN / NOERROR responses	Select start date; set scope to 1, 7, 14, 21 days or to 2 years; select multiple hour or day blocks within this
Traffic		Graphs which plot query volume broken down by a given datatype against time	General	Total; Timeout; Reason	Include or exclude any data item; change resolution; zoom in /out or pan on time period
			Transport	Layer 3 Protocol (IPv4 or IPv6) Layer 4 Protocol (UDP or TCP) EDNS	
			Query	OPCODE and RCODE; AA, TC, RD, RA, CD, AD, QR and Z bits QTYPE QCLASS (IN, CH, ANY or “other) EDNS DO bit	
			QTYPE	All QTYPES can be displayed; the following preset defaults have been defined: ADDRESS; INFRA; DNSSEC; UNEXPECTED	
			RESPONSE	RCODE; AA and TC bits; ANCOUNT	
Packet view		Graph of individual packet/ response pairs	n/a	Each query/response pair for the given time period coloured by a variety of different metrics, e.g.: Response types: Delegation; NXDOMAIN (C); NODATA; NXDOMAIN (N); Answer (C); Empty Answer; Answer (A); Empty (A); Other; Null Zoom into individual packet level data	Include/exclude any of the types; Navigate between packets; Order by time, source IP, QNAME See top source IPs and QNAMES See fine-grained time series
Traffic profiling		Lists of top 100 queries	Query names	Top 100 Domain names; count of queries for each of these	Group by QNAME, label, TLD, SLD, 3LD, 4LD Sort by query volume or alphabetic domain name
			Source IPs	Top 100 source IP addresses; count of queries for each of these; ASN; description; country code	Group by Address, ASN, subnet, country code Sort by query volume or IP address
Breakdown		Query volumes for various parameters	n/a	Nameserver; QTYPE; QCLASS; UDP/TCP; IPv4/6; EDNS; Q_DO; Q_QR; Q_OPCODE; Q_AA; Q_TC; Q_RD; Q_RA; Q_Z; Q_AD; Q_CD; Q_RCODE; RCODE; AA; TC; Reason; ANCOUNT; Timeout; Burst	None

Data selection

The data displayed in the traffic graphs can be restricted by choosing the following attributes as appropriate in each graph:

Time period	For overview: select start date; set scope to 1, 7, 14, 21 days or to 2 years; select hour or day blocks within this. All other graphs can have time periods from 1 second upwards. (The packet view will shorten the period in an attempt to limit the number of packets shown to 100,000.)		
Query and Transport	Name server QNAME, with optional sub-domain QTYPE QCLASS Source IP with optional sub-domain Transport (TCP, IPv6, EDNS & DO bit) Reason AN+, TO, BUSRT	Request flags	QR; AA; TC; RD; RA; Z; AD; CD OPCODE RCODE
		Response flags	AA; TC RCODE

Performance

Data capture	*turing* can capture in excess of 200k queries per second per Collector instance. There is minimal performance impact from data capture on the DNS Servers themselves. *turing* can alternatively be configured to sniff the data straight from a tap port on a switch.
Lag (seconds)	All data gets synchronised 10 seconds after every minute from the Collector to the Aggregator, so there is at most 70 seconds delay between capture and availability for real-time analysis. Real time alerting is something that can be done at the Collectors, which see the traffic as it comes by.

Interface

Human computer interface	Keyboard/mouse Touch enabled interface
Application front-end	HTML5 web application
Data collection method	pcap to sniff DNS packets “from the wire”
API available?	Yes[1]
API type	RESTful interface; JSON over HTTP[1]

System requirements

Hardware	Collector	The Collector component can be installed on: • Either each DNS Server to be monitored; • Or on a separate server using port mirror to capture the DNS traffic We recommend servers should be configured with a minimum of 4GB RAM. For very high DNS traffic volumes (over 200 KQps) we recommend use of SSDs in the server on which the Collector component is installed. Storage capacity required will depend on traffic volumes and the final configuration of *turing*.
	Aggregator	A dedicated physical or virtualised server should be provided for the Aggregator. The requirements for number of CPU cores, RAM, and storage type and capacity depend on traffic volumes and desired performance
Software	Collector	• 64-bit Linux (RHEL 6 or later or FreeBSD 10.1 or later recommended) • CGI host e.g. Apache
	Aggregator	• Java SE7.0 and above • MySQL 5.1.73 or later
	UI	• Web server e.g. Apache

[1]This is supplied as a beta version for release v1.0. Customers wishing to use the API in this version should be aware that later versions may implement it in a different way and changes may need to be made to any code written