DNS analysis

In this experiment, you investigate the DNS protocol characteristics by using the software *dig*. This experiment should be performed in your machine which must have Internet connectivity. The command dig is a tool for querying DNS nameservers for information about host addresses, mail exchanges, nameservers, and related information.

Installing Dig

The tool dig can be found in many operational systems, including Windows, Linux (Unix) or Macintosh OS X operating system. You can find instructions to install it on your system as follows:

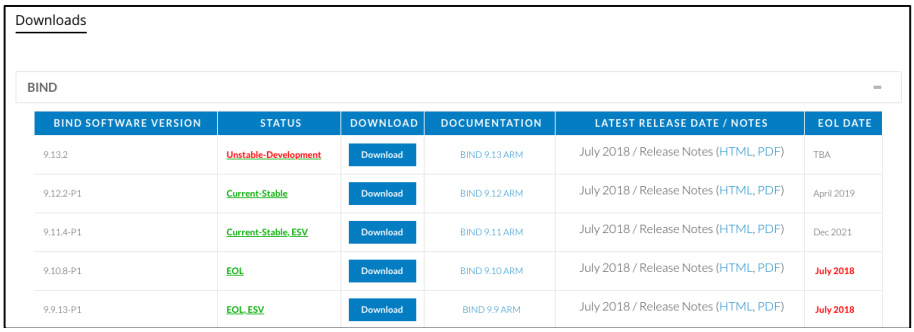
Installing on Linux (Ubuntu/Debian)

```
apt-get install dnsutils
```

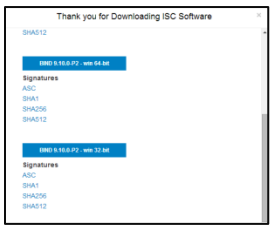
Installing on Windows

Download from https://www.isc.org/downloads/

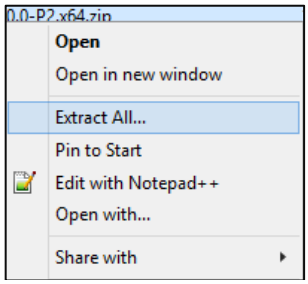
Under the BIND heading, click the download button of the "Current-stable" release.



Select your version (32-bit, 64-bit)



Right click on the download, select "Extract All…" and extract the package to your chosen location. You can use as location "C:\Program Files".




```
$ cd "C:\Program Files\BIND9.XXXX"
$ dig utwente.nl
```

Running Dig

Once you're in the terminal, you're ready to start asking DIG for DNS queries. The basic dig command will follow the syntax:

```
$ dig name @server type
```

dig	invokes the utility
name	is the host you are looking for information about (e.g. utwente.nl)
@server	allows you to query the name from a different location (e.g. 8.8.8.8 for Google's resolver)
type	is an optional field that allows you to have DIG locate a specific record type (e.g. A, AAAA, CNAME, MX, TXT, etc.)

A	It specifies IP address (IPv4) for given host.
AAAA	It specifies IP address (IPv6) for given host.
CNAME	The records are used for creating aliases of domain names.
MX	It specifies a mail exchange server for a DNS domain name.
NS	It specifies an authoritative name server for given host.
TXT	The text record can hold arbitrary non-formatted text string.

Example:

The below command request for your DNS server the IP address associated with the name **utwente.nl**. The output contains a lot of details that in the first moment is not critical for our laboratory.

```
$ dig  utwente.nl

; <<>> DiG 9.10.6 <<>> utwente.nl
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17424
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1452
;; QUESTION SECTION:
;utwente.nl.                    IN      A

;; ANSWER SECTION:
utwente.nl.             1787    IN      A       130.89.3.249

;; Query time: 5 msec
;; SERVER: 1.1.1.1#53(1.1.1.1)
;; WHEN: Tue Aug 28 11:45:33 CEST 2018
;; MSG SIZE  rcvd: 55
```

query details and options

question section

answer section

1. Find the IPv6 address (AAAA) of the name "**utwente.nl**".
2. Find all the mail servers (MX) of the domain name "**utwente.nl**".
3. Find all the name servers of the domain "**utwente.nl**".
4. Execute the following command and describe all the DNS requests. Use the Wireshark to identify the number of DNS requests sent to get the result.

   $ dig +trace **utwente.nl** +nodnssec

5. You can use dig to check the DNSSEC signature of a domain. Describe how you can use dig for that and present the output for the domain "**utwente.nl**". How can you identify that this signature is valid? Compare the output using "www.dnssec-failed.org" (hint: status).