Exercise 1: Explore DNS records (Not marked, No need to submit)

DNS servers use different record types for different purposes. For each type of DNS record, there is an associated type of DNS query. Check the following page ( <https://en.wikipedia.org/wiki/List_of_DNS_record_types>) and find out what the following resource record types are used for:

* A
* Returns a 32-bit [IPv4](https://en.wikipedia.org/wiki/IPv4) address, most commonly used to map [hostnames](https://en.wikipedia.org/wiki/Hostname) to an IP address of the host, but it is also used for [DNSBLs](https://en.wikipedia.org/wiki/DNSBL), storing [subnet masks](https://en.wikipedia.org/wiki/Subnet_mask) in [RFC 1101](https://tools.ietf.org/html/rfc1101), etc.
* 返回32位[IPv4](https://en.wikipedia.org/wiki/IPv4" \o "IPv4的)地址，最常用于将[主机名](https://en.wikipedia.org/wiki/Hostname)映射到[主机](https://en.wikipedia.org/wiki/Hostname)的IP地址，但它也用于[DNSBL](https://en.wikipedia.org/wiki/DNSBL)，在[RFC 1101中](https://tools.ietf.org/html/rfc1101)存储[子网掩码](https://en.wikipedia.org/wiki/Subnet_mask)等。
* CNAME

Alias of one name to another: the DNS lookup will continue by retrying the lookup with the new name.

一个名称与另一个名称的别名：DNS查找将通过使用新名称重试查找来继续。

* MX

Maps a domain name to a list of [message transfer agents](https://en.wikipedia.org/wiki/Message_transfer_agent) for that domain

映射一个域名的列表，[邮件传输代理](https://en.wikipedia.org/wiki/Message_transfer_agent" \o "邮件传输代理)为该域

* NS

Delegates a [DNS zone](https://en.wikipedia.org/wiki/DNS_zone) to use the given [authoritative name servers](https://en.wikipedia.org/wiki/Authoritative_name_server)

委派[DNS区域](https://en.wikipedia.org/wiki/DNS_zone)以使用给定的[权威名称服务器](https://en.wikipedia.org/wiki/Authoritative_name_server)

* PTR  
  Pointer to a [canonical name](https://en.wikipedia.org/wiki/Canonical_name). Unlike a CNAME, DNS processing stops and just the name is returned. The most common use is for implementing [reverse DNS lookups](https://en.wikipedia.org/wiki/Reverse_DNS_lookup), but other uses include such things as [DNS-SD](https://en.wikipedia.org/wiki/Zero_configuration_networking#Apple's_protocol:_Multicast_DNS/DNS-SD).

指向[规范名称的](https://en.wikipedia.org/wiki/Canonical_name)指针。与CNAME不同，DNS处理停止，只返回名称。最常见的用途是实现[反向DNS查找](https://en.wikipedia.org/wiki/Reverse_DNS_lookup)，但其他用途包括[DNS-SD等](https://en.wikipedia.org/wiki/Zero_configuration_networking#Apple's_protocol:_Multicast_DNS/DNS-SD)。

* SOA

Specifies *authoritative* information about a [DNS zone](https://en.wikipedia.org/wiki/DNS_zone), including the primary name server, the email of the domain administrator, the domain serial number, and several timers relating to refreshing the zone.

指定有关[DNS区域的](https://en.wikipedia.org/wiki/DNS_zone)*权威*信息，包括主名称服务器，域管理员的电子邮件，域序列号以及与刷新区域相关的多个计时器。

Exercise 2: Tracing DNS with Wireshark (Not marked, No need to submit)

For this particular experiment download the dns trace file: [dns-etheral-trace-2](https://webcms3.cse.unsw.edu.au/COMP3331/18s2/resources/17305).

Step 1: Open an xterm and run Wireshark.

Step 2: Load the trace file *dns-ethereal-trace-2*by using the *File*pull down menu, choosing *Open*and selecting the appropriate trace file. This file captures the sequence of messages exchanged between a host and its default DNS server while using the *nslookup*(this tool is similar to the *dig*tool that we used earlier in the lab) utility for obtaining the canonical name (type A record) of [www.mit.edu](http://www.mit.edu/). The IP address of the default DNS server for the host is 128.238.29.22. Now filter out all non-DNS packets by typing “dns” (without quotes) in the filter field. Also click the right arrow for DNS in the packet-header detail window. Now focus on the **last two DNS messages**from the 6 listed and answer the following questions:

Question 1: What transport layer protocol is being used by the DNS messages?

UDP

Question 2: What is the source and destination port for the DNS query message and the corresponding response?

Source Port: 3742

Destination Port: 53

[Response In: 20]

Question 3: To what IP address is the DNS query message sent? Is this the same as the default local DNS server?

Source: 128.238.38.160

Destination: 128.238.29.22

Yes

Question 4: How many “questions” are contained in the DNS query message? What “Type” of DNS queries are they? Does the query message also contain any “answers”?

Questions: 1

www.mit.edu: type A, class IN

No

Question 5: Examine the DNS response message. Provide details of the contents of the “Answers”, “Authority” and “Additional Information” fields. What can you infer from these?

www.mit.edu: type A, class IN, addr 18.7.22.83

mit.edu: type NS, class IN, ns BITSY.mit.edu

mit.edu: type NS, class IN, ns STRAWB.mit.edu

mit.edu: type NS, class IN, ns W20NS.mit.edu

BITSY.mit.edu: type A, class IN, addr 18.72.0.3

STRAWB.mit.edu: type A, class IN, addr 18.71.0.151

W20NS.mit.edu: type A, class IN, addr 18.70.0.160