SINGAPORE UNIVERSITY OF
TECHNOLOGY AND DESIGN

Established in collaboration with MIT

50.005 Computer System Engineering (Spring 2019)

NS Lab 3: Internet Domain Name System

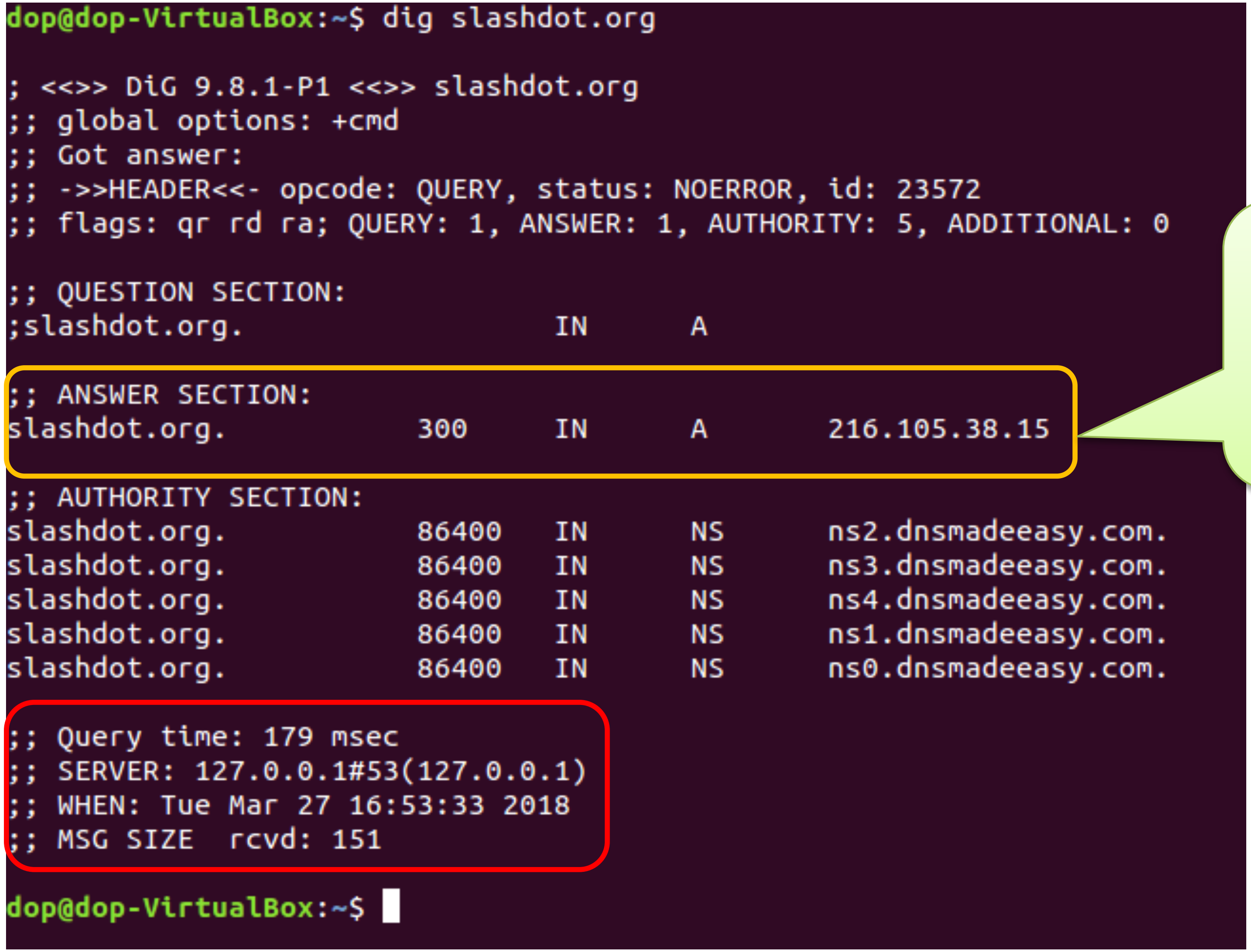
Objectives

1. Use **dig** to perform DNS queries (e.g. to look up an IP address)
2. Read and interpret **DNS records** of different types
3. Understand how a DNS query is resolved using **hierarchy and recursion**
4. Observe and understand the effect of **caching** on DNS lookup times
5. Use **Wireshark to trace** and read DNS packets sent to and from a machine

1. Exploring DNS using dig

- DIG - Domain Information Groper
  - commonly used for performing DNS lookups
  - Command: dig <host>
  - E.g. dig slashdot.org

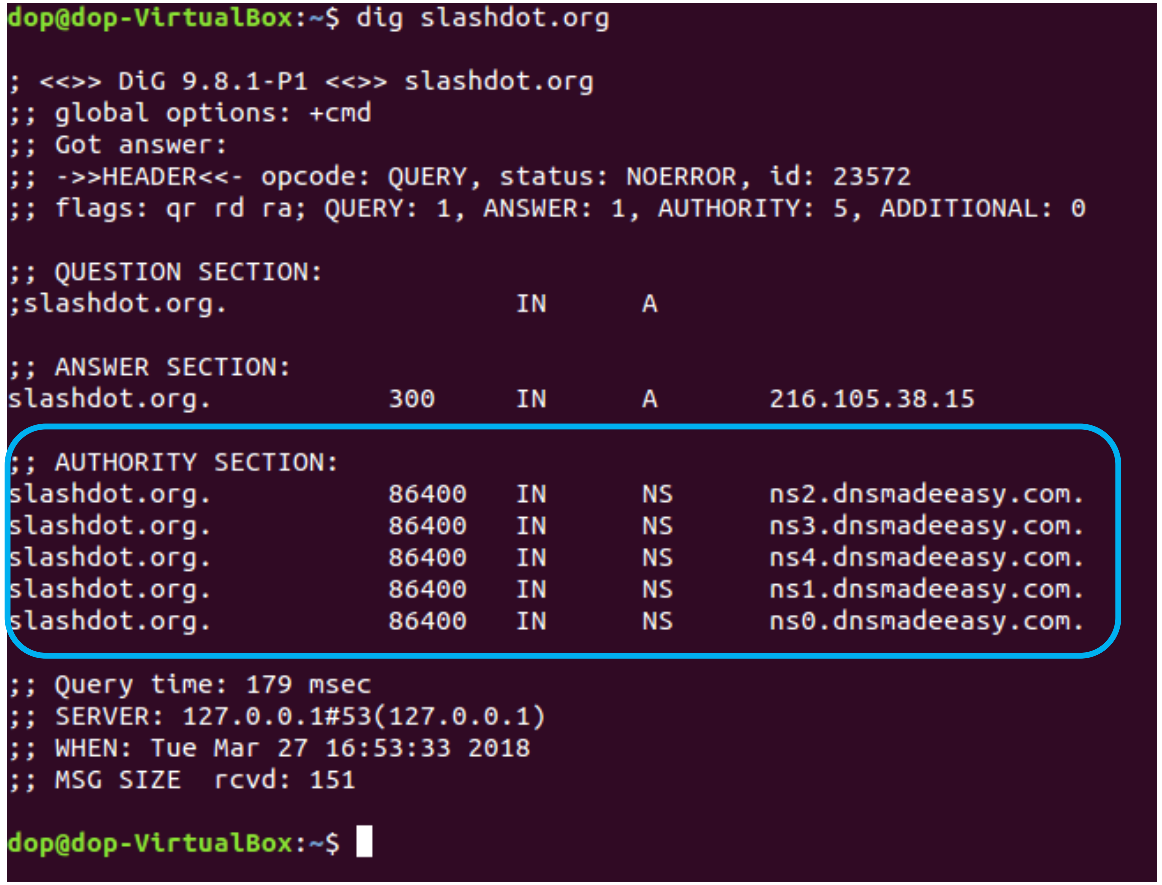
dig slashdot.org



```
dop@dop-VirtualBox:~$ dig slashdot.org

; <<>> DiG 9.8.1-P1 <<>> slashdot.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23572
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 5, ADDITIONAL: 0

;; QUESTION SECTION:
;slashdot.org.                  IN      A

;; ANSWER SECTION:
slashdot.org.           300     IN      A       216.105.38.15

;; AUTHORITY SECTION:
slashdot.org.           86400   IN      NS      ns2.dnsmadeeasy.com.
slashdot.org.           86400   IN      NS      ns3.dnsmadeeasy.com.
slashdot.org.           86400   IN      NS      ns4.dnsmadeeasy.com.
slashdot.org.           86400   IN      NS      ns1.dnsmadeeasy.com.
slashdot.org.           86400   IN      NS      ns0.dnsmadeeasy.com.

;; Query time: 179 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Tue Mar 27 16:53:33 2018
;; MSG SIZE  rcvd: 151

dop@dop-VirtualBox:~$ 
```

Server Name: slashdot.org
Expiry: 300 seconds
Class: IN
Type: A
Data: 216.105.38.15

authority section

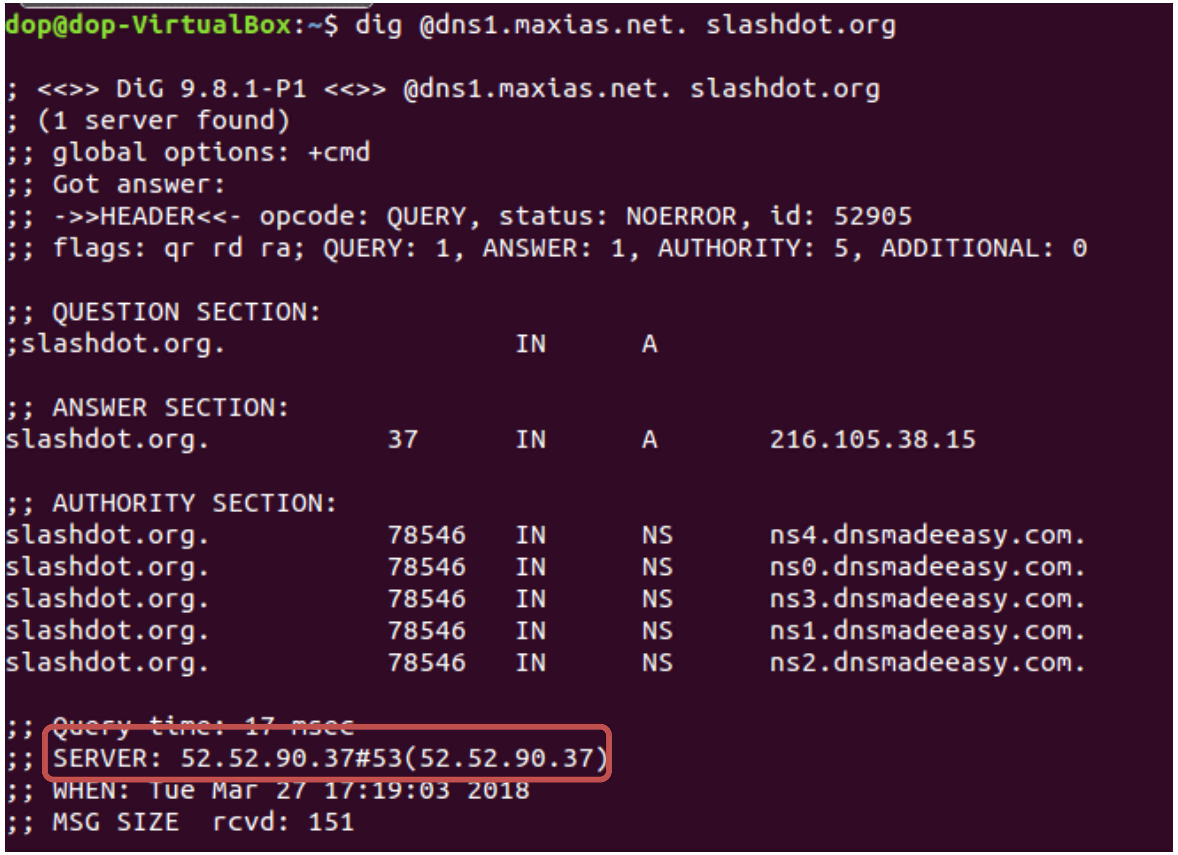


```
dop@dop-VirtualBox:~$ dig slashdot.org

; <<>> DiG 9.8.1-P1 <<>> slashdot.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23572
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 5, ADDITIONAL: 0

;; QUESTION SECTION:
;slashdot.org.                  IN      A

;; ANSWER SECTION:
slashdot.org.           300     IN      A       216.105.38.15

;; AUTHORITY SECTION:
slashdot.org.           86400   IN      NS      ns2.dnsmadeeasy.com.
slashdot.org.           86400   IN      NS      ns3.dnsmadeeasy.com.
slashdot.org.           86400   IN      NS      ns4.dnsmadeeasy.com.
slashdot.org.           86400   IN      NS      ns1.dnsmadeeasy.com.
slashdot.org.           86400   IN      NS      ns0.dnsmadeeasy.com.

;; Query time: 179 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Tue Mar 27 16:53:33 2018
;; MSG SIZE  rcvd: 151

dop@dop-VirtualBox:~$ 
```

- Type: NS
- Indicates the names of the DNS servers storing records for a particular domain
- Hosts: ns2.dnsmadeeasy.com., ns3.dnsmadeeasy.com., … are responsible for providing authoritative responses to names in the slashdot.org domain.

Query a specific server using the ‘@’

- Lookup using the DNS server dns1.maxias.net.
- Command: dig @dns1.maxias.net. slashdot.org



```
dop@dop-VirtualBox:~$ dig @dns1.maxias.net. slashdot.org

; <<>> DiG 9.8.1-P1 <<>> @dns1.maxias.net. slashdot.org
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52905
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 5, ADDITIONAL: 0

;; QUESTION SECTION:
;slashdot.org.                  IN      A

;; ANSWER SECTION:
slashdot.org.           37      IN      A       216.105.38.15

;; AUTHORITY SECTION:
slashdot.org.           78546   IN      NS      ns4.dnsmadeeasy.com.
slashdot.org.           78546   IN      NS      ns0.dnsmadeeasy.com.
slashdot.org.           78546   IN      NS      ns3.dnsmadeeasy.com.
slashdot.org.           78546   IN      NS      ns1.dnsmadeeasy.com.
slashdot.org.           78546   IN      NS      ns2.dnsmadeeasy.com.

;; Query time: 17 msec
;; SERVER: 52.52.90.37#53(52.52.90.37)
;; WHEN: Tue Mar 27 17:19:03 2018
;; MSG SIZE  rcvd: 151
```

Recursive search - dig

- Option : +norecurs

- dig @a.root-servers.net +norecurse redlab.lcs.mit.edu

```
; <<>> DiG 8.1 <<>> @a.root-servers.net +norecurse redlab.lcs.mit.edu
; (1 server found)
;; res options: init defnam dnsrch
;; got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 3, ADDITIONAL: 3
;; QUERY SECTION:
;;      redlab.lcs.mit.edu, type = A, class = IN

;; AUTHORITY SECTION:
MIT.EDU.                2D IN NS        BITSY.MIT.EDU.
MIT.EDU.                2D IN NS        STRAWB.MIT.EDU.
MIT.EDU.                2D IN NS        W20NS.MIT.EDU.

[output truncated]
```

- dig @bitsy.mit.edu +norecurse redlab.lcs.mit.edu

```
; <<>> DiG 8.1 <<>> @bitsy.mit.edu +norecurse redlab.lcs.mit.edu
; (1 server found)
;; res options: init defnam dnsrch
;; got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10
;; flags: qr ra; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 4
;; QUERY SECTION:
;;      redlab.lcs.mit.edu, type = A, class = IN

;; AUTHORITY SECTION:
LCS.MIT.EDU.            6H IN NS        MINTAKA.LCS.MIT.EDU.
LCS.MIT.EDU.            6H IN NS        OSSIPEE.LCS.MIT.EDU.
LCS.MIT.EDU.            6H IN NS        LAMPANG.LCS.MIT.EDU.
LCS.MIT.EDU.            6H IN NS        FEDEX.AI.MIT.EDU.

[output truncated]
```

…

Part 2: Tracing DNS using Wireshark

- Powerful tool used to capture packets sent over a network & analyse the content of the packets retrieved.
- Installation: sudo apt-get install wireshark
- Download "*dnsrealtrace.pcapng*" from eDimension.
  - contains a trace of the packets sent and received when a web page is downloaded from a web server over the SUTD network.
- Use the capture to answer questions in handout.

Deliverables

- Complete the activities and answer the questions in the handout.
- Submit a report containing your name, student ID and answers to eDimension.
- Due Date: **17 April, 2019 (23:59)**