

ยินดีต้อนรับสู่

CYBER SECURITY WORKSHOP



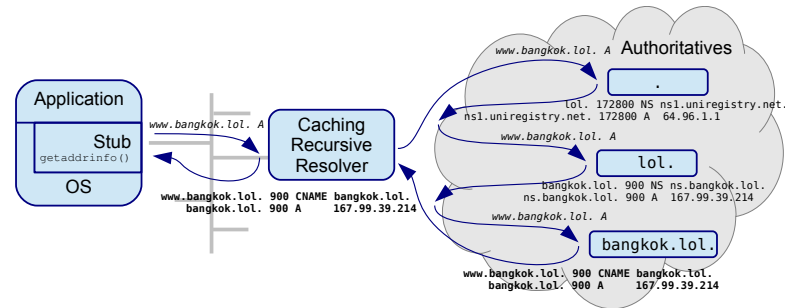
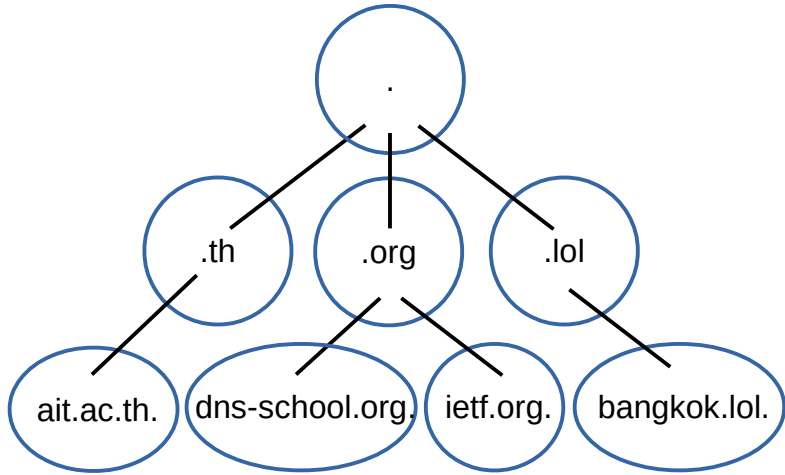
Basics part 2

Bangkok
8-9 May 2019

The material in these slides is based on Karst Koymans' CIA
course material, see: <https://www.os3.nl/2020-2021/courses/cia/start>

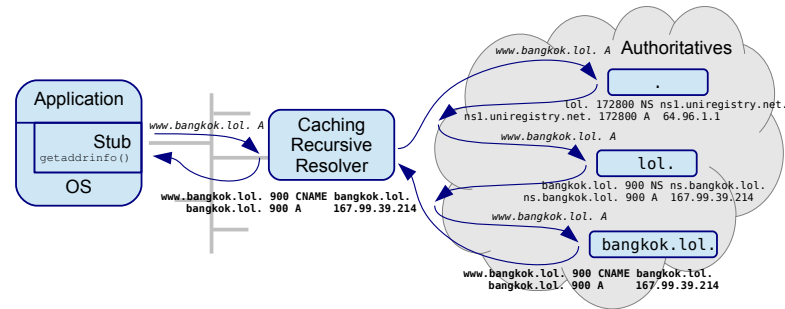
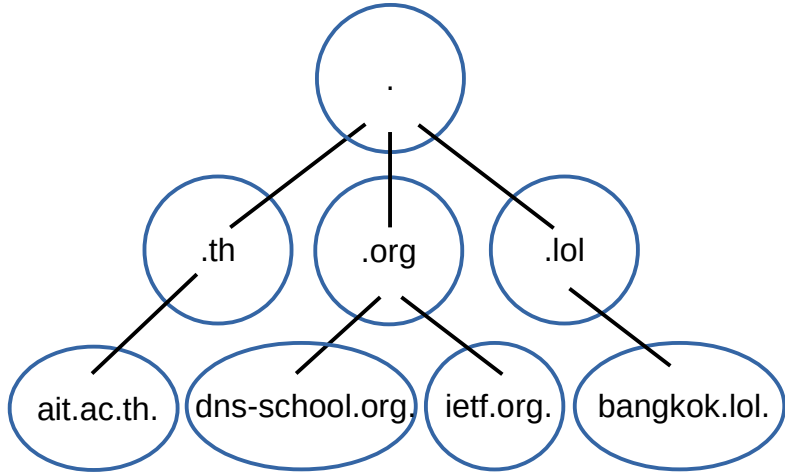
Concepts

- **Domain Name Space**
 - Organised as a (domain name) tree
- **Resource Records**
 - The actual DNS data
- **Resolvers**
 - Send queries to name servers
- **Name Servers**
 - Send responses to resolvers (Server)



Concepts

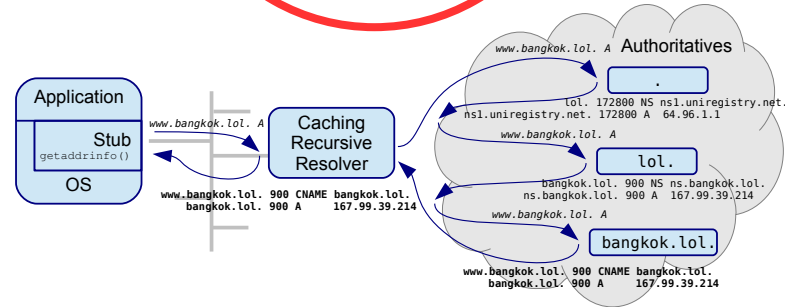
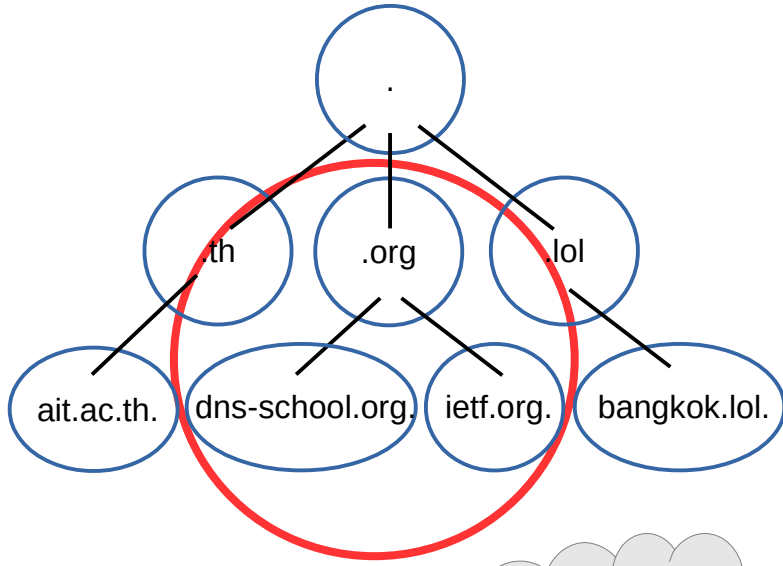
- **Label**
 - lol
 - the name between the dots
 - root label is empty! “”
- **Domain name**
 - bangkok.lol
 - A sequence of labels
 - **Fully Qualified Domain Name (fqdn)**
 - bangkok.lol.
 - Relative Domain Name
 - res-0
 - res-0.do



Concepts

- **Domain**

- A domain name together with all domain names below



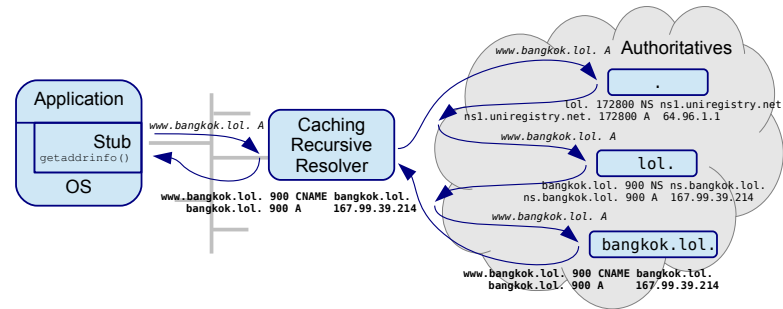
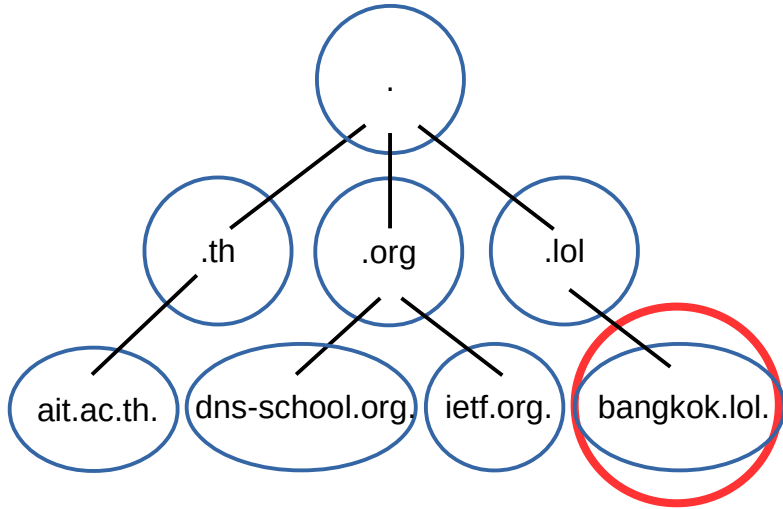
Concepts

- **Domain**

- A domain name together with all domain names below

- **Zone**

- Organization unit of Authoritative Information



Apex → bangkok.lol.
ns.bangkok.lol.
www.bangkok.lol.

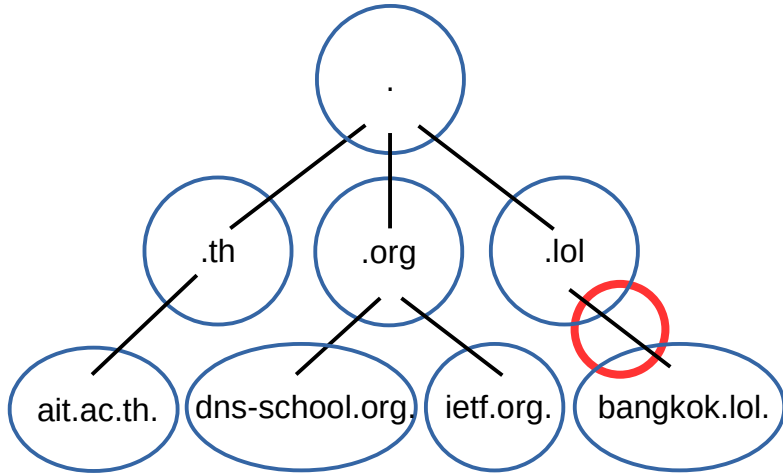
Concepts

- **Domain**

- A domain name together with all domain names below

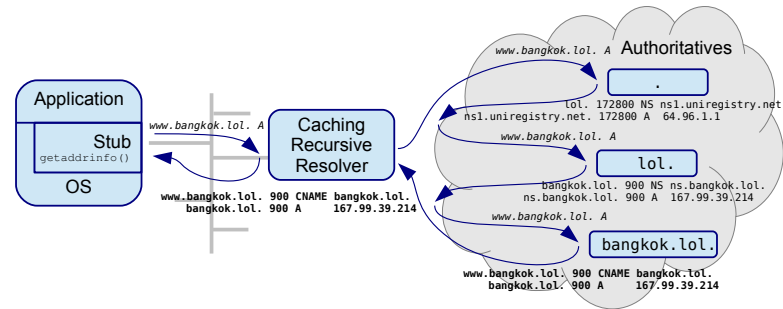
- **Zone**

- Organization unit of Authoritative Information



- **Delegation**

- Delegation of authority via **Referral** at the **Zone Cut** from a **Parent** to a **Child**



Resource Records (RRs)

- Owner
 - bangkok.lol.
- TTL
- Class
 - IN, CH, HS
- Type
 - A, AAAA, CNAME, etc...
- Resource data (RDATA)
 - depends on type

```
$ drill bangkok.lol A
;; ->>HEADER<<- opcode: QUERY, rcode: NOERROR, id: 1
;; flags: qr rd ra ; QUERY: 1, ANSWER: 1, AUTHORITY:
;; QUESTION SECTION:
;; bangkok.lol. IN A

;; ANSWER SECTION:
bangkok.lol. 900IN A 167.99.39.214

;; Query time: 4 msec
;; SERVER: 2001:980:2283:fe::1
;; WHEN: Sun May 5 13:23:10 2019
;; MSG SIZE rcvd: 45
```

Resource Record Set (RRset)

- A set of RRs with same
 - Owner name
 - Class
 - Typebut with different
 - RDATA

```
$ drill bangkok.lol NS
;; ->>HEADER<- opcode: QUERY, rcode: NOERROR, id: 4
;; flags: qr rd ra ; QUERY: 1, ANSWER: 2, AUTHORITY:
;; QUESTION SECTION:
;; bangkok.lol. IN NS

;; ANSWER SECTION:
bangkok.lol. 900 IN NS ns.bangkok.lol.
bangkok.lol. 900 IN NS ns.nlnetlabs.nl.

;; Query time: 4 msec
;; SERVER: fd88:10d2:853e:10::1
;; WHEN: Sun May 5 13:34:44 2019
;; MSG SIZE rcvd: 75
```


A record

- Name → IPv4 address
- Can be more than 1

```
$ drill thnic.co.th
;; ->>HEADER<<- opcode: QUERY, rcode: NOERROR, id: 4
;; flags: qr rd ra ; QUERY: 1, ANSWER: 2, AUTHORITY:
;; QUESTION SECTION:
;; thnic.co.th.  IN  A

;; ANSWER SECTION:
thnic.co.th.  3600    IN  A   52.76.117.40
thnic.co.th.  3600    IN  A   61.19.242.184

;; Query time: 777 msec
;; SERVER: 2001:980:2283:fe::1
;; WHEN: Sun May  5 13:59:20 2019
;; MSG SIZE  rcvd: 61
```

AAAA record

- Name → IPv6 address
- a.k.a. Quad-A
- Common to be > 1

```
$ drill bangkok.lol AAAA
;; ->>HEADER<- opcode: QUERY, rcode: NOERROR, id: 5
;; flags: qr rd ra ; QUERY: 1, ANSWER: 1, AUTHORITY:
;; QUESTION SECTION:
;; bangkok.lol. IN AAAA

;; ANSWER SECTION:
bangkok.lol. 857 IN AAAA 2a03:b0c0:2:d0::df0:3001

;; Query time: 2 msec
;; SERVER: 192.168.1.1
;; WHEN: Sun May 5 13:46:11 2019
;; MSG SIZE rcvd: 57
```

CNAME record

- Name → Canonical Name
- **No other RRs at the same Owner!**
 - Maybe ANAME
- No subdomains
 - Use DNAME for that

```
$ drill www.bangkok.lol A
;; ->>HEADER<- opcode: QUERY, rcode: NOERROR, id: 3
;; flags: qr rd ra ; QUERY: 1, ANSWER: 2, AUTHORITY:
;; QUESTION SECTION:
;; www.bangkok.lol. IN A

;; ANSWER SECTION:
www.bangkok.lol. 900 IN CNAME bangkok.lol.
bangkok.lol. 622 IN A 167.99.39.214

;; Query time: 100 msec
;; SERVER: fd88:10d2:853e:10::1
;; WHEN: Sun May 5 13:49:33 2019
;; MSG SIZE rcvd: 63
```

PTR record

- Address → Domain name

- Why is that useful?

- Troubleshooting
(ping / traceroute)
- Logging
- Forward Confirmed
Reverse DNS

- IPv6 has long PTRs

- 1.0.0.3.0.f.d.0.0.0.0.0.0.0.0.0.0.d.0.0.2.0.0.0.0.c.0.b.3.0.a.2.ip6.arpa. PTR (teacher.do.dns-schoolorg.)

```
$ drill -x 61.19.242.184
;; ->>HEADER<<- opcode: QUERY, rcode: NOERROR, id: 6
;; flags: qr rd ra ; QUERY: 1, ANSWER: 1, AUTHORITY:
;; QUESTION SECTION:
;; 184.242.19.61.in-addr.arpa. IN PTR

;; ANSWER SECTION:
184.242.19.61.in-addr.arpa. 3600 IN PTR (
    www-rr.thnic.co.th. )

;; Query time: 2691 msec
;; SERVER: 2001:980:2283:fe::1
;; WHEN: Sun May 5 13:59:36 2019
;; MSG SIZE rcvd: 76
```

MX record

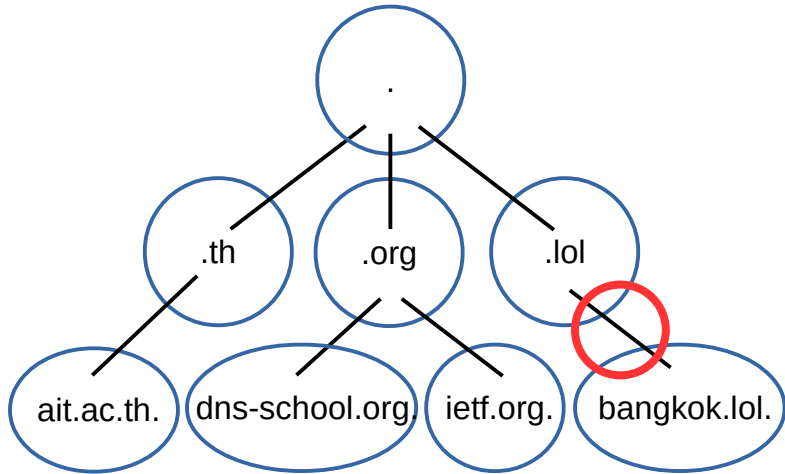
- Mail Exchange
- 1st RDATA field
 - Priority
- 2nd RDATA field
 - SMTP server for the domain

```
$ drill mail.in.th MX
;; ->>HEADER<<- opcode: QUERY, rcode: NOERROR, id: 1
;; flags: qr rd ra ; QUERY: 1, ANSWER: 7, AUTHORITY:
;; QUESTION SECTION:
;; mail.in.th.      IN      MX

;; ANSWER SECTION:
mail.in.th.      3592 IN      MX      1 aspmx.l.google.com.
mail.in.th.      3592 IN      MX      5 alt1.aspmx.l.google.com.
mail.in.th.      3592 IN      MX      5 alt2.aspmx.l.google.com.
mail.in.th.      3592 IN      MX      10 aspmx2.googlemail.com.
mail.in.th.      3592 IN      MX      10 aspmx3.googlemail.com.
mail.in.th.      3592 IN      MX      10 aspmx4.googlemail.com.
mail.in.th.      3592 IN      MX      10 aspmx5.googlemail.com.
```

NS record

- **Name Server**
 - Delegates Authority
 - Make DNS Decentralized
- In both Parent & Child!



```
$ drill @64.96.1.1 bangkok.lol NS
;; ->HEADER<- opcode: QUERY, rcode: NOERROR, id:
;; flags: qr rd ; QUERY: 1, ANSWER: 0, AUTHORITY:
;; QUESTION SECTION:
;; bangkok.lol. IN NS

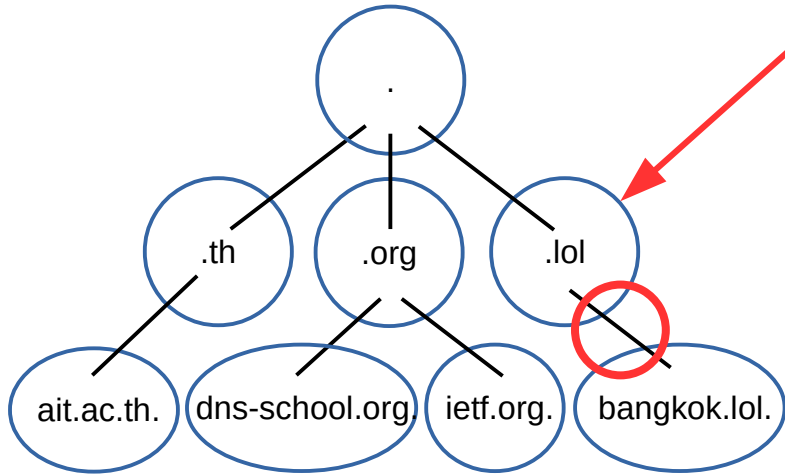
;; ANSWER SECTION:

;; AUTHORITY SECTION:
bangkok.lol. 900 IN NS ns.bangkok.lol.
bangkok.lol. 900 IN NS ns.nlnetlabs.nl.

;; ADDITIONAL SECTION:
ns.bangkok.lol. 900 IN A 167.99.39.214
ns.bangkok.lol. 900 IN AAAA ...
```

NS record

- Name Server
- **Glue**
 - “in bailiwick”
 - Not authoritative



```
$ drill @64.96.1.1 bangkok.lol NS
;; ->HEADER<- opcode: QUERY, rcode: NOERROR, id:
;; flags: qr rd ; QUERY: 1, ANSWER: 0, AUTHORITY:
;; QUESTION SECTION:
;; bangkok.lol. IN NS

;; ANSWER SECTION:

;; AUTHORITY SECTION:
bangkok.lol. 900 IN NS ns.bangkok.lol.
bangkok.lol. 900 IN NS ns.nlnetlabs.nl.

;; ADDITIONAL SECTION:
ns.bangkok.lol. 900 IN A 167.99.39.214
ns.bangkok.lol. 900 IN AAAA ...
```

SOA record

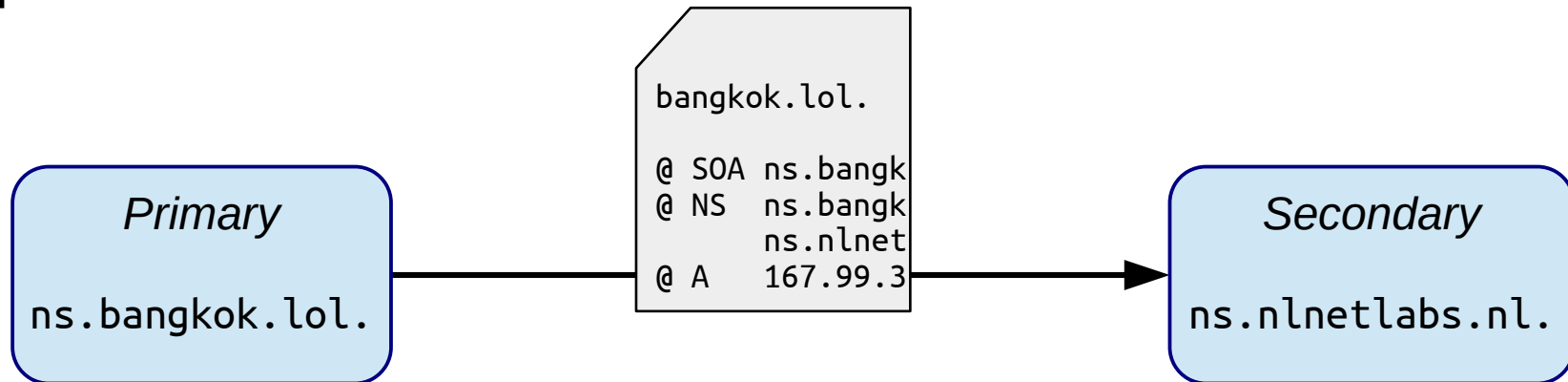
- **Start Of Authority**
- Administrates zone parameters
 - Primary server
 - Email address
 - Version of Zone
 - Control Plane parameters for *secondary servers*

```
;; ->>HEADER<<- opcode: QUERY, rcode: NOERROR, id: 1
;; flags: qr rd ra ; QUERY: 1, ANSWER: 1, AUTHORITY:
;; QUESTION SECTION:
;; bangkok.lol. IN SOA

;; ANSWER SECTION:
bangkok.lol. 0 IN SOA ns.bangkok.lol. (
                sysadm.nlnet.nl.
                2019050418 ; serial
                28800      ; refresh (8 hours)
                14400      ; retry (4 hours)
                604800     ; expire (1 week)
                86400      ; minimum (1 day)
                )
```


Name server types

- Master – Primary
- Hidden Master
- Secondary
- Stealth
- Slave



Zone file

\$ORIGIN bangkok.lol.

\$TTL 900

```
@    IN    SOA ns sysadm.nlnet.nl. (  
      2019050418 ; serial  
      28800      ; refresh (8 hours)  
      14400      ; retry (4 hours)  
      604800     ; expire (1 week)  
      86400      ; minimum (1 day)  
      )
```

```
      IN    NS     ns
```

```
      IN    NS     ns.nlnetlabs.nl.
```

```
ns   IN    AAAA  2a03:b0c0:2:d0::df0:3001
```

```
      IN    A      167.99.39.214
```

```
@    IN    AAAA  2a03:b0c0:2:d0::df0:3001
```

```
      IN    A      167.99.39.214
```

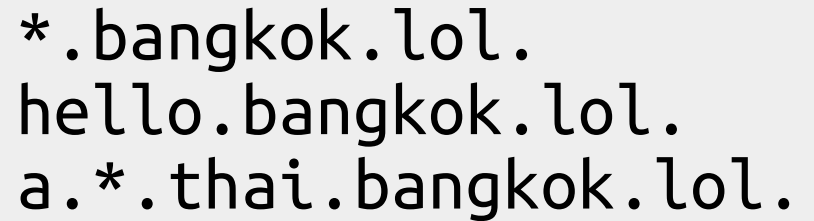
```
www  IN    CNAME  @
```

Wildcard records

- RR that can be used for all matching query names
- Leftmost label is '*'
- **Only** matches when wildcard label is directly below longest match

Wildcard records

- welcome.bangkok.lol.
 - Wildcard match
- hello.bangkok.lol.
 - **No** wildcard match
- welcome.hello.bangkok.lol.
 - **No** wildcard match
- something.thai.bangkok.lol.
 - Wildcard match on *.thai.bangkok.lol. (ENT)



```
*.bangkok.lol.  
hello.bangkok.lol.  
a.*.thai.bangkok.lol.
```

Lab time!



- Hands on: <http://bangkok.lol/>
- 2. Set up an Authoritative Name Server