NETWORK SECURITY PRACTICES – ATTACK AND DEFENSE

DNS Security

DNS Basics

- Domain Name Service
- Translate between domain names and IP addresses
  - E.g., bs2.to ↔ 140.113.168.8
  - Domain names are human-friendly
  - IP addresses keep changing
  - Phonebook (104)
- One of the fundamental component of the Internet
  - What you rely on everyday
  - web, mail, FTP, SSH, IM, Skype, updates, …
- Invented by Paul Mockapetris at USC in 1983
- BIND by Berkeley in early 1980s
- UDP or TCP (port 53)

Hierarchical Name Space

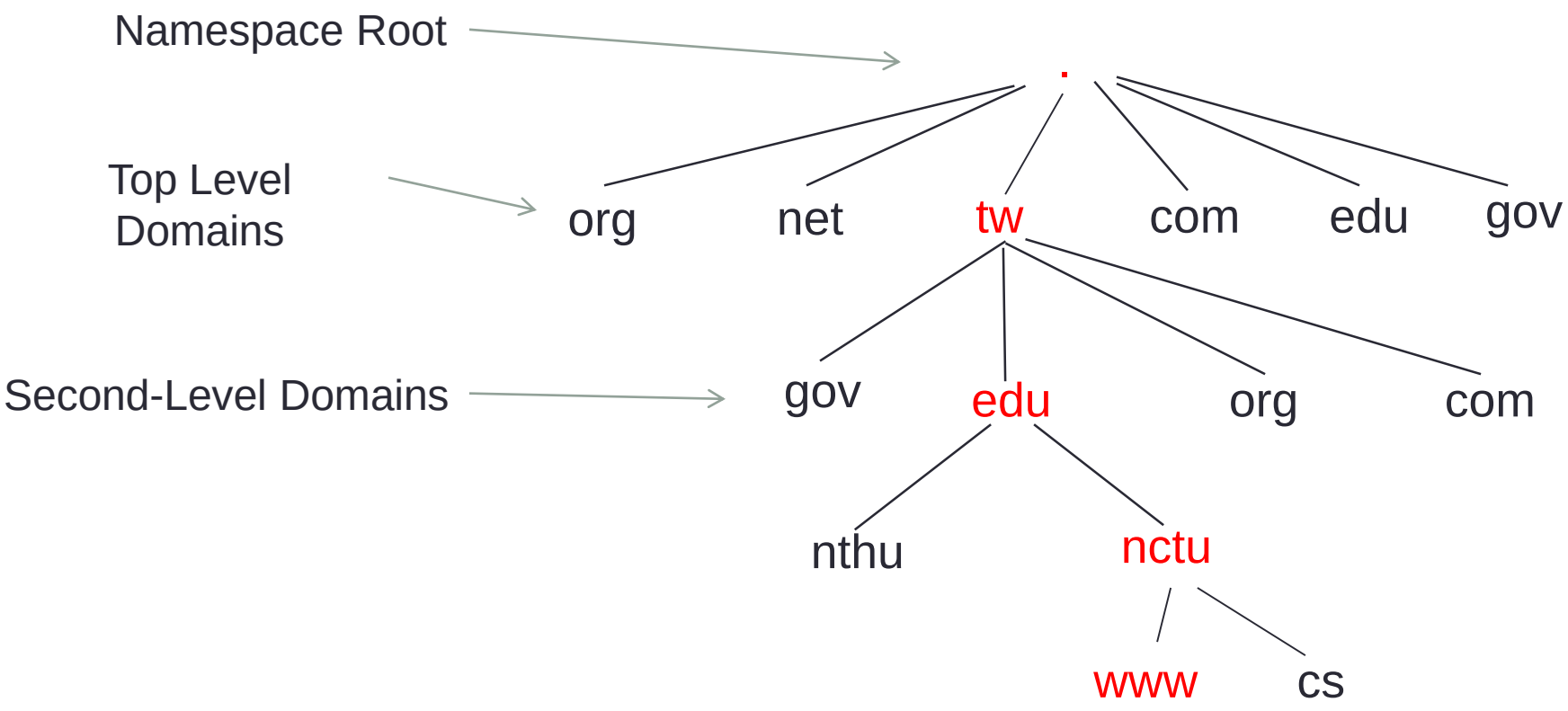
Host name

(sub) domain name

bsd1.cs.nctu.edu.tw.

Fully qualified domain name (FQDN)

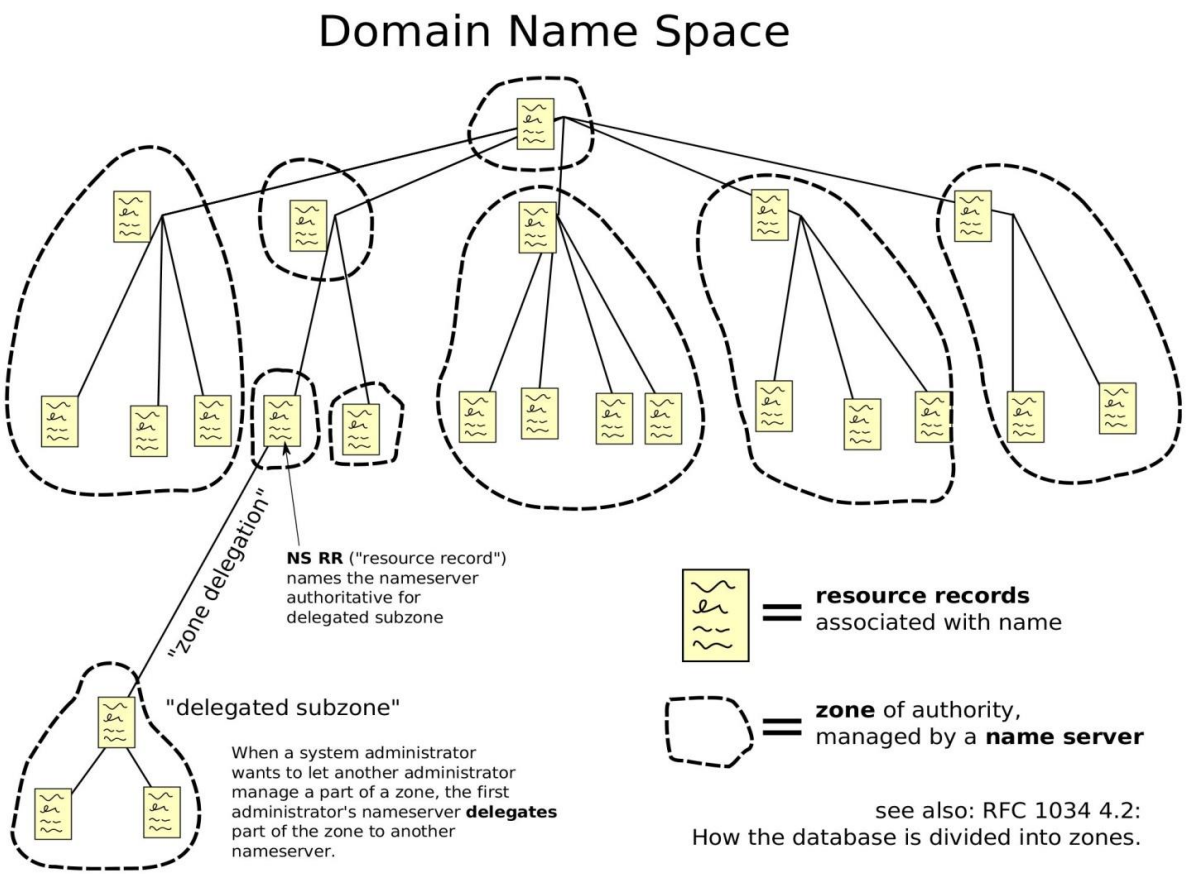
Hierarchical Name Space



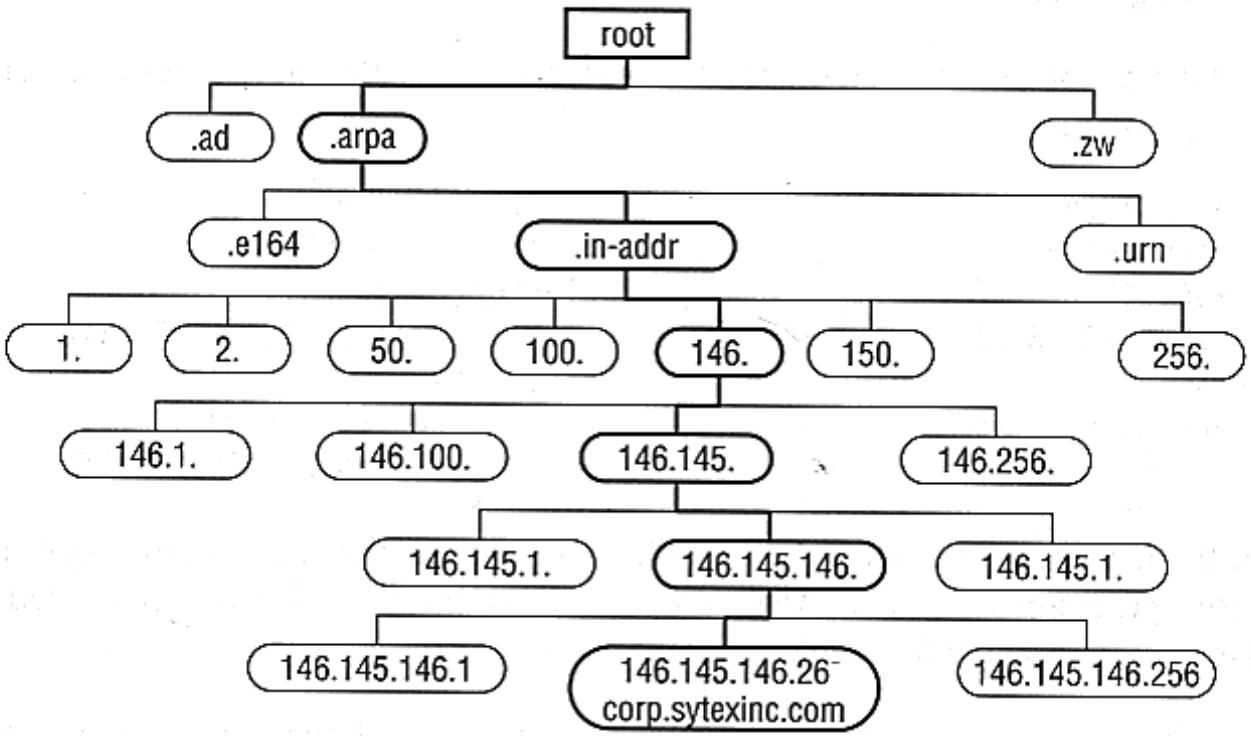
Domain Name Space

- The name space is divided into *zones* (or *domains*)
- A DNS zone consists of a collection of connected nodes authoritatively served by an *authoritative nameserver*.
  - A single nameserver (e.g. BIND) can host several zones

Domain Name Space

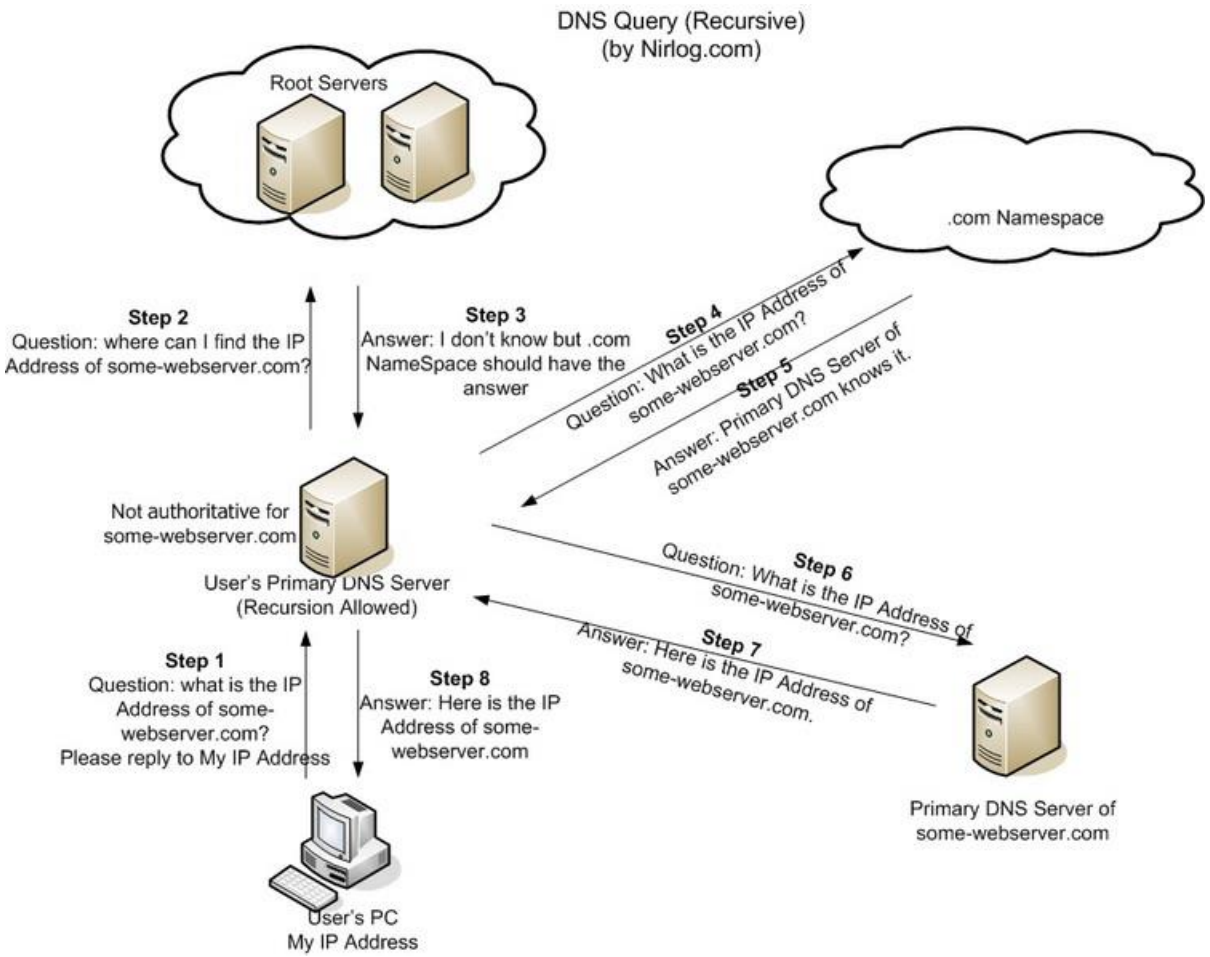


Reverse DNS Lookup



(from Network Security by Eric Cole)

DNS Query → Resolve → Response



DNS Query → Resolve → Response

- The client sends a query to the server containing
  - A specified DNS domain name, stated as a fully qualified domain name (FQDN)
  - A specified query type, which specifies a resource record by type (A, MX,…)
  - A specified class for the DNS domain name (usually ‘IN’ the internet class)

root@cloud:~

```
[root@cloud ~]# dig cs.nctu.edu.tw

; <<>> DiG 9.3.6-P1-RedHat-9.3.6-4.P1.el5_4.2 <<>> cs.nctu.edu.tw
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1096
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;cs.nctu.edu.tw.                        IN      A

;; ANSWER SECTION:
cs.nctu.edu.tw.         1523    IN      A       140.113.235.111

;; AUTHORITY SECTION:
cs.nctu.edu.tw.         2668    IN      NS      dns2.cs.nctu.edu.tw.
cs.nctu.edu.tw.         2668    IN      NS      dns.cs.nctu.edu.tw.

;; ADDITIONAL SECTION:
dns.cs.nctu.edu.tw.     2668    IN      A       140.113.235.107
dns2.cs.nctu.edu.tw.    2924    IN      A       140.113.235.103

;; Query time: 1 msec
;; SERVER: 140.113.1.1#53(140.113.1.1)
;; WHEN: Thu Mar 18 15:17:28 2010
;; MSG SIZE  rcvd: 117
```

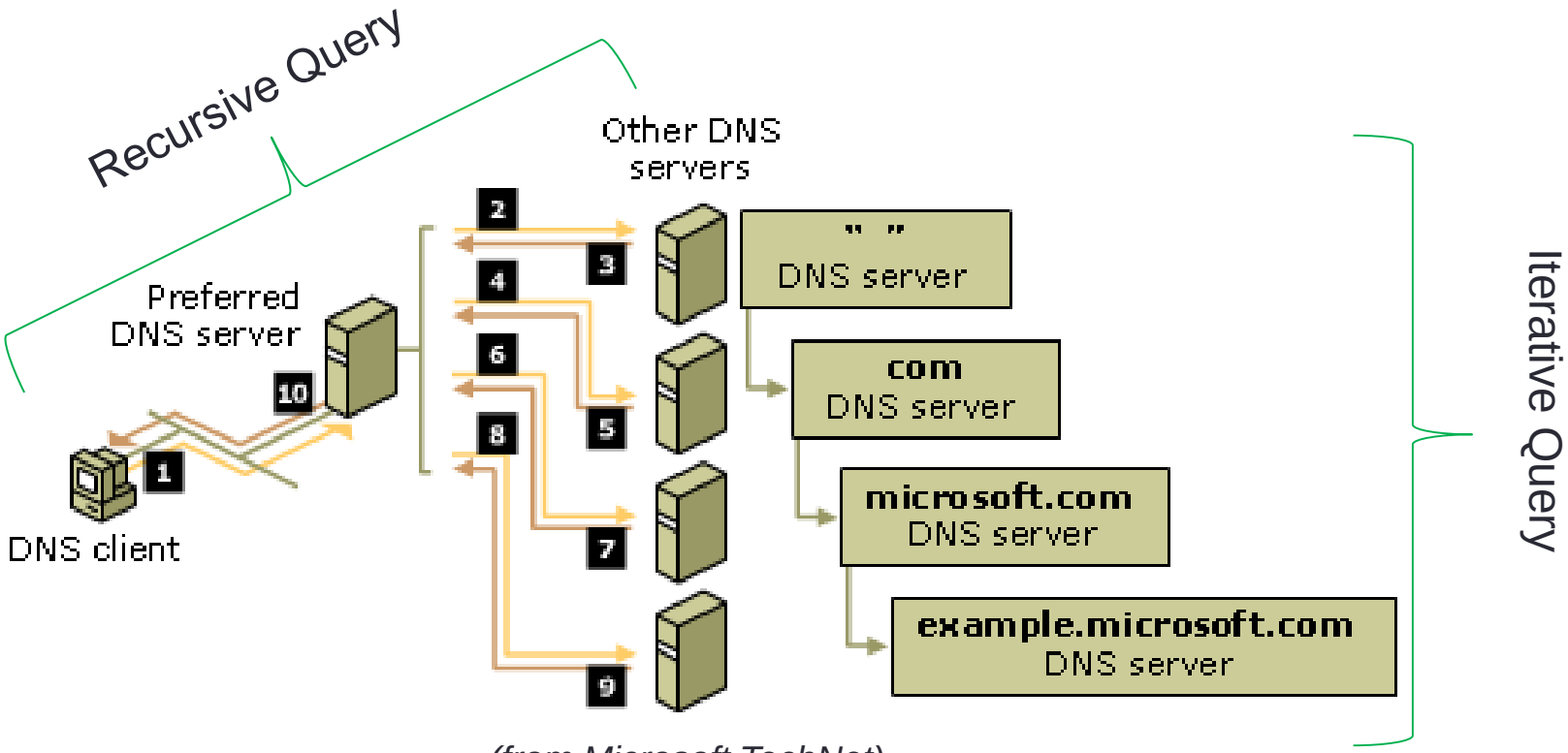
```
[root@cloud cgi-bin]# nslookup 140.113.235.111
Server:         140.113.1.1
Address:        140.113.1.1#53

Non-authoritative answer:
111.235.113.140.in-addr.arpa    name = cswproxy.cs.nctu.edu.tw.

Authoritative answers can be found from:
235.113.140.in-addr.arpa        nameserver = dns2.cs.nctu.edu.tw.
235.113.140.in-addr.arpa        nameserver = dns.cs.nctu.edu.tw.
dns.cs.nctu.edu.tw      internet address = 140.113.235.107
dns2.cs.nctu.edu.tw     internet address = 140.113.235.103

[root@cloud cgi-bin]#
```

```
[root@cloud ~]# dig cs.nctu.edu.tw MX

; <<>> DiG 9.3.6-P1-RedHat-9.3.6-4.P1.el5_4.2 <<>> cs.nctu.edu.tw MX
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9313
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 2, ADDITIONAL: 5

;; QUESTION SECTION:
;cs.nctu.edu.tw.                        IN      MX

;; ANSWER SECTION:
cs.nctu.edu.tw.         1684    IN      MX      5 csmx1.cs.nctu.edu.tw.
cs.nctu.edu.tw.         1684    IN      MX      5 csmx2.cs.nctu.edu.tw.
cs.nctu.edu.tw.         1684    IN      MX      10 csmx3.cs.nctu.edu.tw.

;; AUTHORITY SECTION:
cs.nctu.edu.tw.         2097    IN      NS      dns.cs.nctu.edu.tw.
cs.nctu.edu.tw.         2097    IN      NS      dns2.cs.nctu.edu.tw.

;; ADDITIONAL SECTION:
csmx1.cs.nctu.edu.tw.   574     IN      A       140.113.235.104
csmx2.cs.nctu.edu.tw.   3552    IN      A       140.113.235.105
csmx3.cs.nctu.edu.tw.   3185    IN      A       140.113.235.119
dns.cs.nctu.edu.tw.     2097    IN      A       140.113.235.107
dns2.cs.nctu.edu.tw.    3051    IN      A       140.113.235.103

;; Query time: 1 msec
;; SERVER: 140.113.1.1#53(140.113.1.1)
;; WHEN: Thu Mar 18 15:26:59 2010
;; MSG SIZE  rcvd: 215

[root@cloud ~]#
```

DNS Query → Resolve → Response

- The client-side DNS service can answer the query locally using cached information from a previous query
- A DNS server can its own cache to answer a query
- The DNS can query the other DNS server on behalf of the client
  - A *recursive* DNS query from the client's perspective
- The client can query additional DNS servers
  - An *iterative* DNS query from the client's perspective
  - A DNS server can also query additional DNS servers iteratively

DNS Query → Resolve → Response



(from Microsoft TechNet)

DNS Query → Resolve → Response

- An *authoritative answer* from a server with direct authority for the queried name
- A *positive answer*
  - Possibly the server uses the cached information
- A *referral answer* containing the other DNS servers to contact with (recursion is not supported)
- A *negative answer* if
  - An authoritative server reported that the queried name does not exist in the DNS namespace
  - An authoritative server reported that the queried name exists but no records of the specified type exist for that name

DNS Query → Resolve → Response

root@solid:~

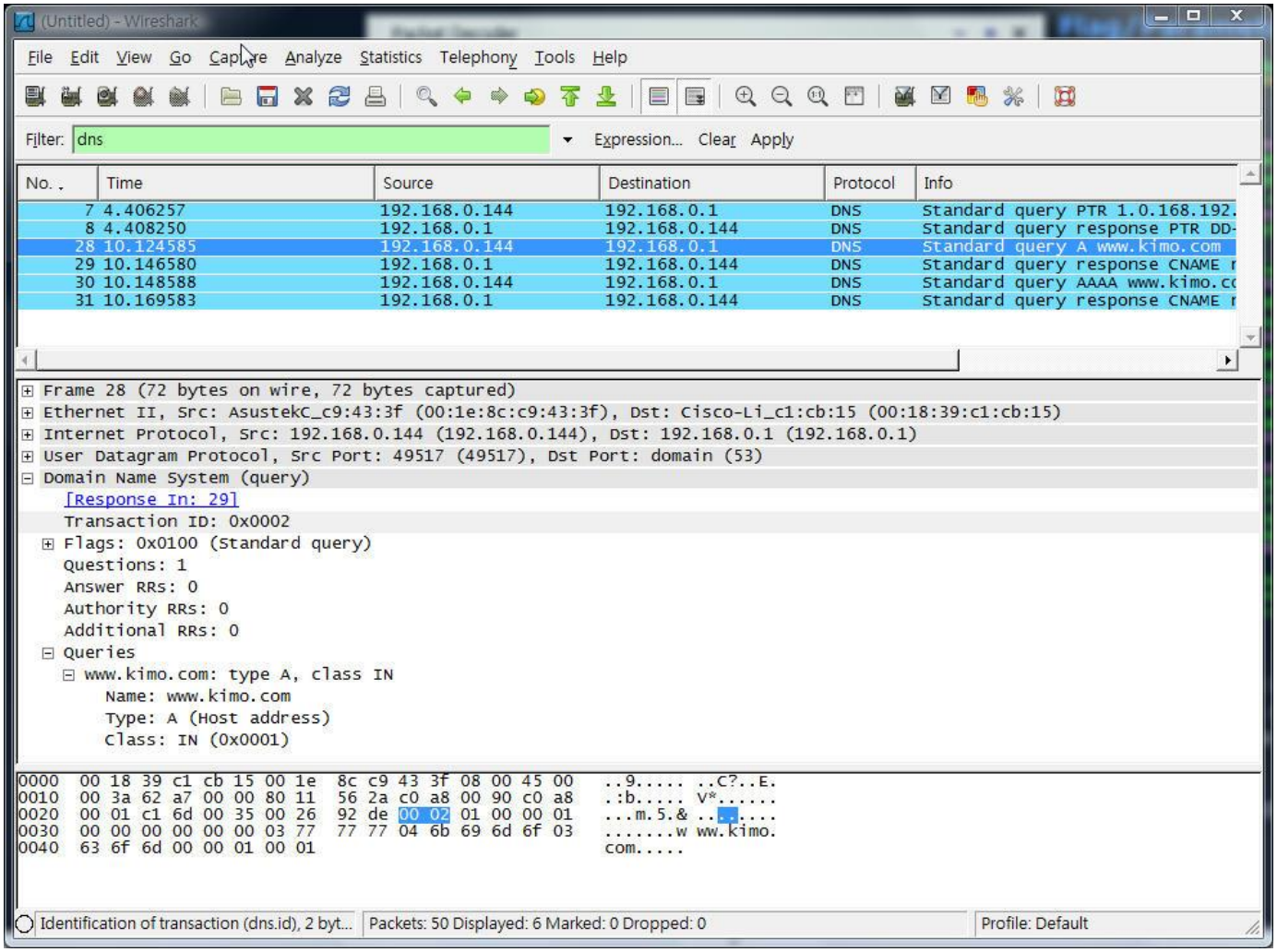
```
[root@solid ~]# nslookup - dns.cs.nctu.edu.tw
> www.cs.nctu.edu.tw
Server:         dns.cs.nctu.edu.tw
Address:        140.113.235.107#53

Name:   www.cs.nctu.edu.tw
Address: 140.113.235.47
>
> www.nctu.edu.tw
Server:         dns.cs.nctu.edu.tw
Address:        140.113.235.107#53

Non-authoritative answer:
Name:   www.nctu.edu.tw
Address: 140.114.60.211
Name:   www.nctu.edu.tw
Address: 140.113.40.35
Name:   www.nctu.edu.tw
Address: 140.113.40.36
>
```

DNS Resolve and Response Unfolded

```
[root@sense ~]# dig www.cs.nctu.edu.tw +trace

; <<>> DiG 9.3.6-P1-RedHat-9.3.6-4.P1.el5 <<>> www.cs.nctu.edu.tw +trace
;; global options:  printcmd
.                       58271   IN      NS      A.ROOT-SERVERS.NET.
.                       58271   IN      NS      B.ROOT-SERVERS.NET.
.                       58271   IN      NS      C.ROOT-SERVERS.NET.
.                       58271   IN      NS      D.ROOT-SERVERS.NET.
.                       58271   IN      NS      E.ROOT-SERVERS.NET.
.                       58271   IN      NS      F.ROOT-SERVERS.NET.
.                       58271   IN      NS      G.ROOT-SERVERS.NET.
.                       58271   IN      NS      H.ROOT-SERVERS.NET.
.                       58271   IN      NS      I.ROOT-SERVERS.NET.
.                       58271   IN      NS      J.ROOT-SERVERS.NET.
.                       58271   IN      NS      K.ROOT-SERVERS.NET.
.                       58271   IN      NS      L.ROOT-SERVERS.NET.
.                       58271   IN      NS      M.ROOT-SERVERS.NET.
;; Received 468 bytes from 140.113.1.1#53(140.113.1.1) in 1 ms

tw.                     172800  IN      NS      e.dns.tw.
tw.                     172800  IN      NS      d.dns.tw.
tw.                     172800  IN      NS      g.dns.tw.
tw.                     172800  IN      NS      c.dns.tw.
tw.                     172800  IN      NS      ns.twnic.net.
tw.                     172800  IN      NS      a.dns.tw.
tw.                     172800  IN      NS      b.dns.tw.
tw.                     172800  IN      NS      h.dns.tw.
tw.                     172800  IN      NS      f.dns.tw.
;; Received 478 bytes from 198.41.0.4#53(A.ROOT-SERVERS.NET) in 136 ms
```

```
edu.tw.                 86400   IN      NS      moestar.edu.tw.
edu.tw.                 86400   IN      NS      a.twnic.net.tw.
edu.tw.                 86400   IN      NS      b.twnic.net.tw.
edu.tw.                 86400   IN      NS      c.twnic.net.tw.
edu.tw.                 86400   IN      NS      d.twnic.net.tw.
edu.tw.                 86400   IN      NS      moevax.edu.tw.
edu.tw.                 86400   IN      NS      moemoon.edu.tw.
;; Received 371 bytes from 211.79.207.26#53(e.dns.tw) in 5 ms

nctu.edu.tw.            518400  IN      NS      ns2.nctu.edu.tw.
nctu.edu.tw.            518400  IN      NS      ns.nctu.edu.tw.
nctu.edu.tw.            518400  IN      NS      ns1.nchc.org.tw.
;; Received 130 bytes from 192.83.166.9#53(a.twnic.net.tw) in 2 ms

cs.nctu.edu.tw.         3600    IN      NS      dns.cs.nctu.edu.tw.
cs.nctu.edu.tw.         3600    IN      NS      dns2.cs.nctu.edu.tw.
;; Received 105 bytes from 140.113.6.2#53(ns2.nctu.edu.tw) in 0 ms

www.cs.nctu.edu.tw.     60      IN      A       140.113.235.47
cs.nctu.edu.tw.         3600    IN      NS      dns.cs.nctu.edu.tw.
cs.nctu.edu.tw.         3600    IN      NS      dns2.cs.nctu.edu.tw.
;; Received 121 bytes from 140.113.235.107#53(dns.cs.nctu.edu.tw) in 0 ms

[root@sense ~]#
```

DNS Query Packet



DNS Response Packet

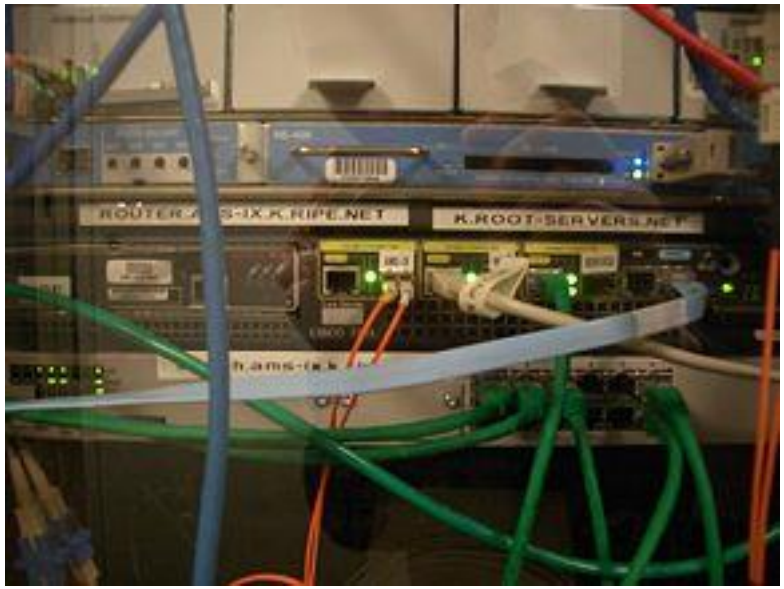
```
⊞ Internet Protocol, Src: 192.168.0.1 (192.168.0.1), Dst: 192.168.0.144 (192.168.0.144)
⊞ User Datagram Protocol, Src Port: domain (53), Dst Port: 49517 (49517)
⊟ Domain Name System (response)
    [Request In: 28]
    [Time: 0.021995000 seconds]
    Transaction ID: 0x0002
  ⊞ Flags: 0x8180 (Standard query response, No error)
    Questions: 1
    Answer RRs: 5
    Authority RRs: 8
    Additional RRs: 8
  ⊟ Queries
    ⊞ www.kimo.com: type A, class IN
  ⊟ Answers
    ⊞ www.kimo.com: type CNAME, class IN, cname rc.tpe.yahoo.com
    ⊞ rc.tpe.yahoo.com: type CNAME, class IN, cname tw.rc.yahoo.com
    ⊞ tw.rc.yahoo.com: type CNAME, class IN, cname w2.rd.tw.g1.b.yahoo.com
    ⊞ w2.rd.tw.g1.b.yahoo.com: type CNAME, class IN, cname tw1-w2.rd.tw.g1.b.yahoo.com
    ⊞ tw1-w2.rd.tw.g1.b.yahoo.com: type A, class IN, addr 119.160.246.23
  ⊟ Authoritative nameservers
    ⊞ g1.b.yahoo.com: type NS, class IN, ns yf4.yahoo.com
    ⊞ g1.b.yahoo.com: type NS, class IN, ns yf3.yahoo.com
    ⊞ g1.b.yahoo.com: type NS, class IN, ns yf2.yahoo.com
    ⊞ g1.b.yahoo.com: type NS, class IN, ns yf8.yahoo.com
    ⊞ g1.b.yahoo.com: type NS, class IN, ns yf6.yahoo.com
    ⊞ g1.b.yahoo.com: type NS, class IN, ns yf7.yahoo.com
    ⊞ g1.b.yahoo.com: type NS, class IN, ns yf5.yahoo.com
    ⊞ g1.b.yahoo.com: type NS, class IN, ns yf1.yahoo.com
  ⊟ Additional records
    ⊞ yf1.yahoo.com: type A, class IN, addr 68.142.254.15
    ⊞ yf2.yahoo.com: type A, class IN, addr 68.180.130.15
    ⊞ yf3.yahoo.com: type A, class IN, addr 203.212.162.166
    ⊞ yf4.yahoo.com: type A, class IN, addr 202.86.6.92
    ⊞ yf5.yahoo.com: type A, class IN, addr 124.108.95.11

00a0  74 77 31 2d 77 32 c0 5c  c0 75 00 01 00 01 00 00   tw1-w2.\ .u......
```

Important for later discussion of DNS attacks

DNS Root Servers

- Answer requests for records in the root zone
- Answer other requests returning a list of the designated *authoritative* name servers for the appropriate *top-level domain* (TLD)

- There are 13 root servers
- 9 of them operate in multiple geographical locations and use *anycast* for increased performance and fault-tolerance



DNS Root Servers

Letter	IPv4 address	IPv6 address	Old name	Operator	Location	Software
A	198.41.0.4	2001:503:BA3E::2:30	ns.internic.net	VeriSign	distributed using anycast	BIND
B	192.228.79.201	2001:478:65::53 (not in root zone yet)	ns1.isi.edu	USC-ISI	Marina Del Rey, California, U.S.	BIND
C	192.33.4.12		c.psi.net	Cogent Communications	distributed using anycast	BIND
D	128.8.10.90		terp.umd.edu	University of Maryland	College Park, Maryland, U.S.	BIND
E	192.203.230.10		ns.nasa.gov	NASA	Mountain View, California, U.S.	BIND
F	192.5.5.241	2001:500:2f::f	ns.isc.org	Internet Systems Consortium	distributed using anycast	BIND 9[3]
G	192.112.36.4		ns.nic.ddn.mil	Defense Information Systems Agency	distributed using anycast	BIND
H	128.63.2.53	2001:500:1::803f:235	aos.arl.army.mil	U.S. Army Research Lab	Aberdeen Proving Ground, Maryland, U.S.	NSD
I	192.36.148.17	2001:7fe::53 (testing, not in root zone yet)	nic.nordu.net	Autonomica	distributed using anycast	BIND
J	192.58.128.30	2001:503:C27::2:30		VeriSign	distributed using anycast	BIND
K	193.0.14.129	2001:7fd::1		RIPE NCC	distributed using anycast	NSD[4]
L	199.7.83.42 (since November 2007; originally was 198.32.64.12)[5]	2001:500:3::42		ICANN	distributed using anycast	NSD[6]
M	202.12.27.33	2001:dc3::35		WIDE Project	distributed using anycast	BIND

DNS Root Servers

```
[root@solid ~]# dig

; <<>> DiG 9.6.1-P3-RedHat-9.6.1-10.P3.fc11 <<>>
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61492
;; flags: qr rd ra; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 14

;; QUESTION SECTION:
;.                              IN      NS

;; ANSWER SECTION:
.                       143100  IN      NS      I.ROOT-SERVERS.NET.
.                       143100  IN      NS      J.ROOT-SERVERS.NET.
.                       143100  IN      NS      K.ROOT-SERVERS.NET.
.                       143100  IN      NS      L.ROOT-SERVERS.NET.
.                       143100  IN      NS      M.ROOT-SERVERS.NET.
.                       143100  IN      NS      A.ROOT-SERVERS.NET.
.                       143100  IN      NS      B.ROOT-SERVERS.NET.
.                       143100  IN      NS      C.ROOT-SERVERS.NET.
.                       143100  IN      NS      D.ROOT-SERVERS.NET.
.                       143100  IN      NS      E.ROOT-SERVERS.NET.
.                       143100  IN      NS      F.ROOT-SERVERS.NET.
.                       143100  IN      NS      G.ROOT-SERVERS.NET.
.                       143100  IN      NS      H.ROOT-SERVERS.NET.

;; ADDITIONAL SECTION:
A.ROOT-SERVERS.NET.     587648  IN      A       198.41.0.4
A.ROOT-SERVERS.NET.     587648  IN      AAAA    2001:503:ba3e::2:30
B.ROOT-SERVERS.NET.     603804  IN      A       192.228.79.201
C.ROOT-SERVERS.NET.     603027  IN      A       192.33.4.12
D.ROOT-SERVERS.NET.     597388  IN      A       128.8.10.90
E.ROOT-SERVERS.NET.     602132  IN      A       192.203.230.10
F.ROOT-SERVERS.NET.     603804  IN      A       192.5.5.241
F.ROOT-SERVERS.NET.     603804  IN      AAAA    2001:500:2f::f
G.ROOT-SERVERS.NET.     604577  IN      A       192.112.36.4
H.ROOT-SERVERS.NET.     603027  IN      A       128.63.2.53
H.ROOT-SERVERS.NET.     603027  IN      AAAA    2001:500:1::803f:235
I.ROOT-SERVERS.NET.     603804  IN      A       192.36.148.17
J.ROOT-SERVERS.NET.     604577  IN      A       192.58.128.30
J.ROOT-SERVERS.NET.     604577  IN      AAAA    2001:503:c27::2:30

;; Query time: 1 msec
;; SERVER: 140.113.1.1#53(140.113.1.1)
;; WHEN: Thu Mar  4 22:05:32 2010
;; MSG SIZE  rcvd: 500

[root@solid ~]#
```

DNS Root Servers

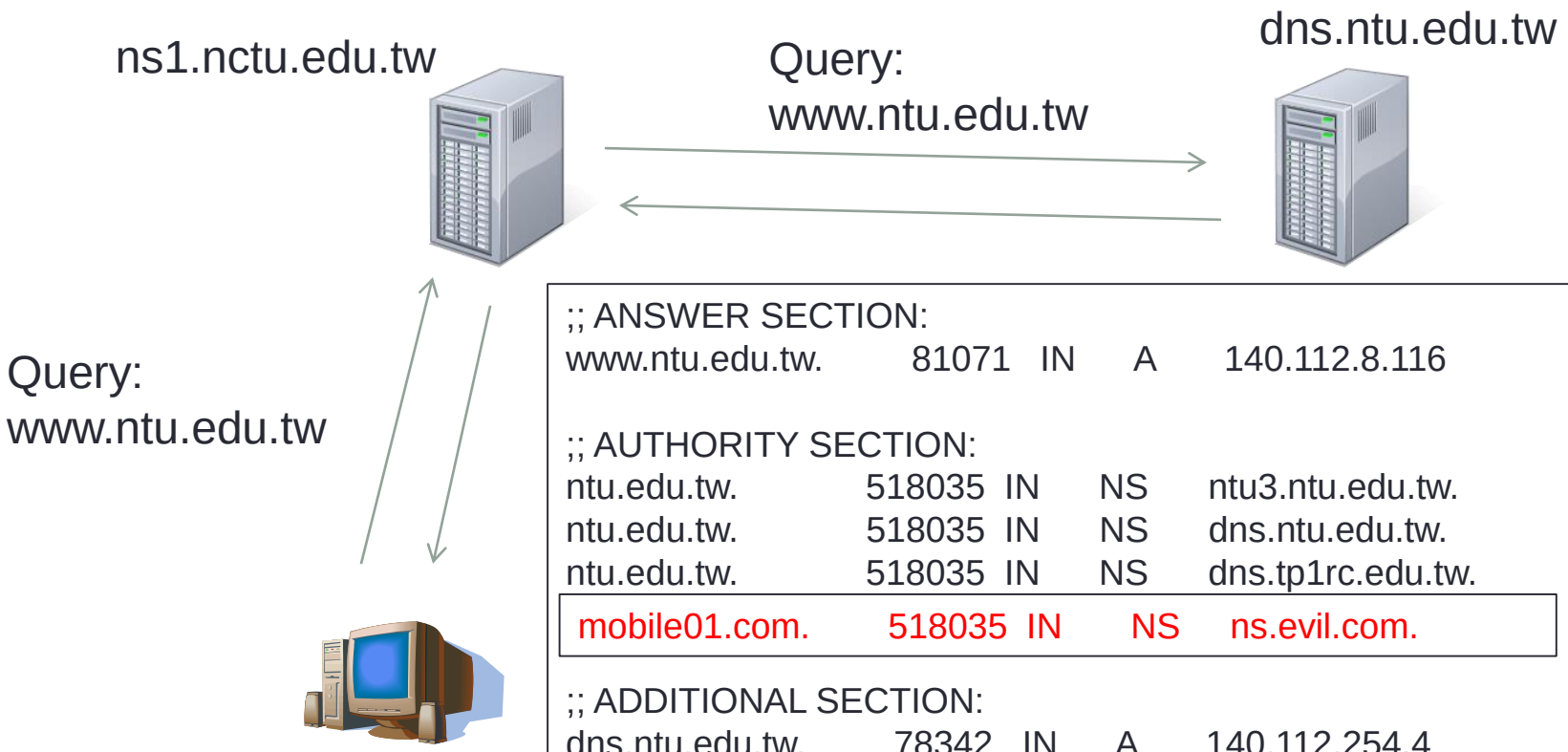
Inherent DNS Vulnerabilities

- Lack of authentication to back “trusts”
  - Users/hosts typically trust the host-address mapping provided by DNS
  - DNS resolvers trust responses received after sending out queries
- Responses can include DNS information not directly related to the query
- The use of cache
- It is easy to fake DNS responses

DNS cache poisoning (Vulnerability 1)

- First concept by Chris Schuba at Purdue in 1993
  - http://ftp.cerias.purdue.edu/pub/papers/christoph-schuba/schuba-DNS-msthesis.pdf
- DNS resource records (see RFC 1034)
  - An “A” record supplies a host IP address
  - A “NS” record supplies name server for domain
- Example
  - mobile01.com NS ns.evil.net /delegate to mobile01 nameserver
  - ns.evil.net A 1.2.3.4 / address for mobile01 nameserver
- Result
  - Look up mobile01 through cache goes to 1.2.3.4

DNS cache poisoning (baseline)




```
;; ANSWER SECTION:
www.ntu.edu.tw.        81071   IN     A      140.112.8.116

;; AUTHORITY SECTION:
ntu.edu.tw.            518035  IN     NS     ntu3.ntu.edu.tw.
ntu.edu.tw.            518035  IN     NS     dns.ntu.edu.tw.
ntu.edu.tw.            518035  IN     NS     dns.tp1rc.edu.tw.
mobile01.com.          518035  IN     NS     ns.evil.com.

;; ADDITIONAL SECTION:
dns.ntu.edu.tw.        78342   IN     A      140.112.254.4
dns.tp1rc.edu.tw.      166018  IN     A      163.28.16.10
dns3.twaren.net.       1581    IN     A      211.79.61.47
ns.evil.com.           80000   IN     A      1.2.3.4
```

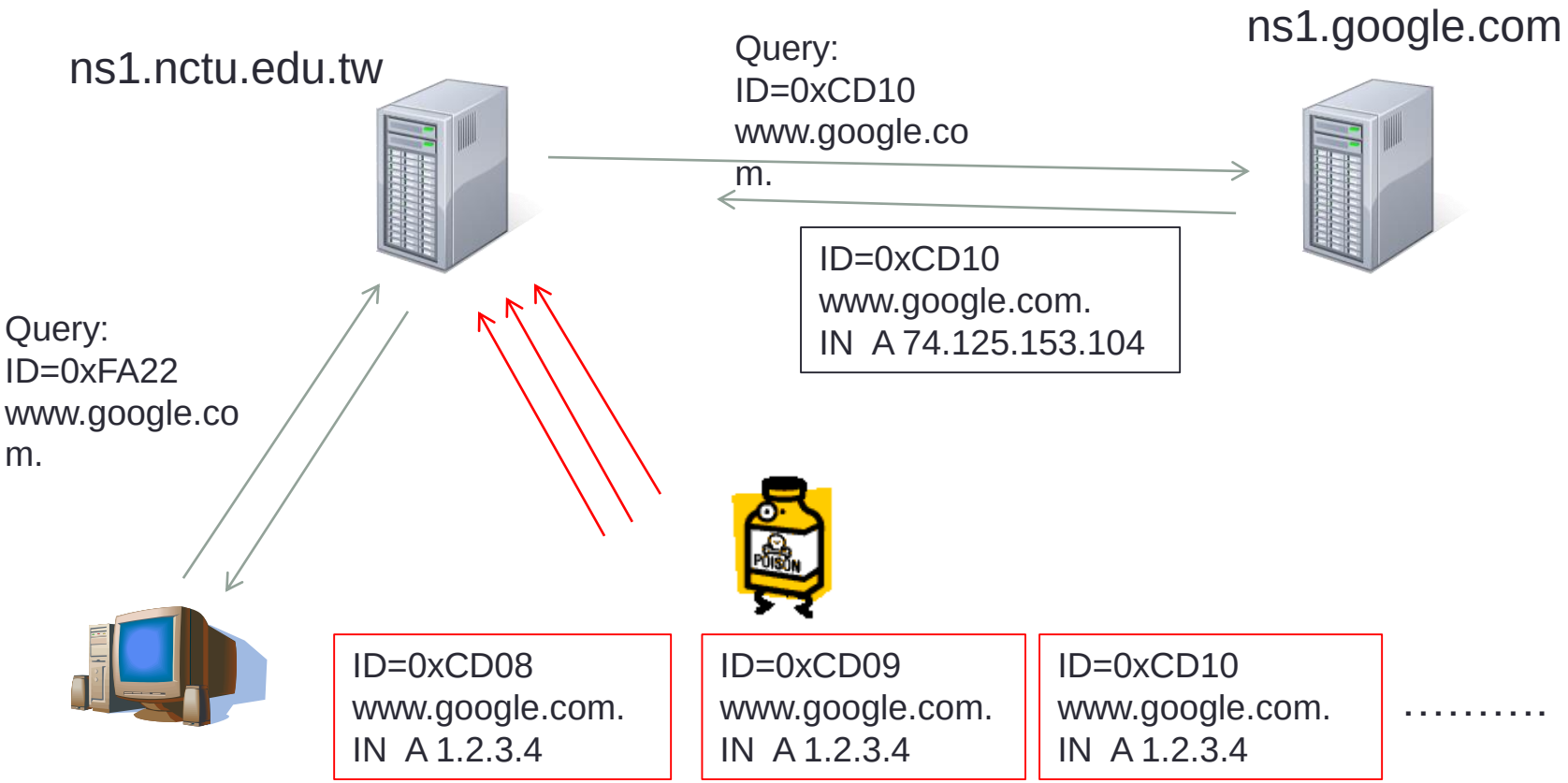
The Bailiwicks Defense

- The bailiwick system prevents foo.com from declaring anything about com, or some other TLD, or www.google.com
- In bailiwicks
  - The *root* servers can return any record
  - The *com* servers can return any record for *com*
  - The *google.com* servers can return any record for *google.com*

DNS cache poisoning (fake response)

- You don’t need an evil nameserver to poison a target victim nameserver
- Respond before the real nameserver
  - An attacker can guess when a DNS cache entry times out and a query has been sent, and provide a fake response.
  - The fake response will be accepted only when its 16-bit transaction ID matches the query
  - CERT reported in 1997 that BIND uses sequential transaction ID and is easily predicted
    - fixed by using random transaction IDs

DNS cache poisoning (faked response)



Guess the ID

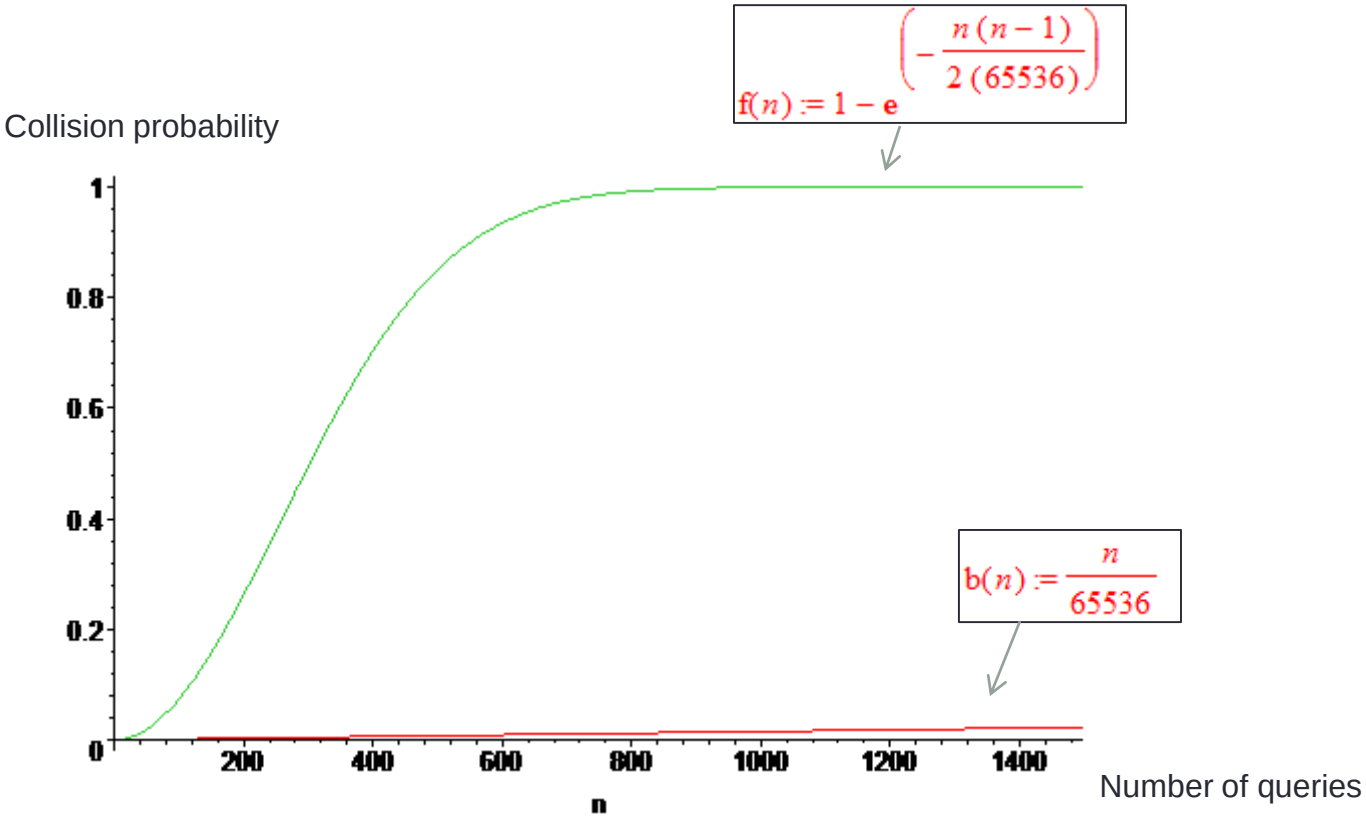
- Early versions of DNS servers deterministically increment the ID field
- Vulnerabilities were discovered in the random ID generation
  - Weak random number generator
  - The attacker is able to predict the ID if knowing several IDs in previous transactions
- Birthday attack
  - Force the resolver to send many identical queries, with different IDs, at the same time
  - Increase the probability of making a correct guess

DNS cache poisoning (birthday attack through a flurry of requests)

- Improve the chance of responding before the real nameserver (discovered by Vagner Sacramento in 2002)
  - Have many (say hundreds of) clients send the same DNS request to the name server
  - Send hundreds of reply with random transaction IDs at the same time
  - Due to the Birthday Paradox, the success probability can be close to 1

Birthday Attack

It's been reported that success on hitting the right QID can be commonly achieved in 10 seconds.



Summary of DNS Poisoning so far

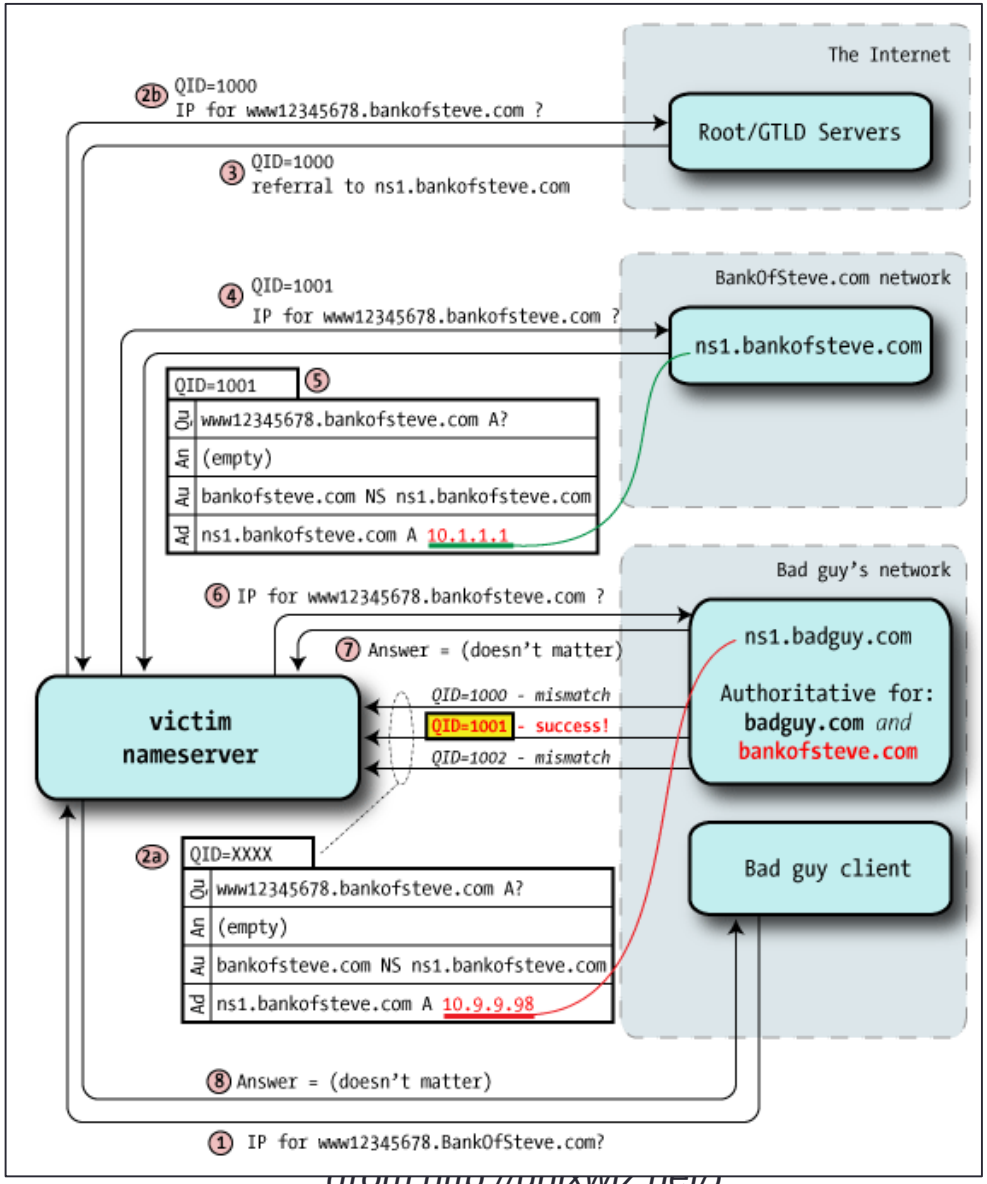
- So far, we know that
  - You can poison an ‘A’ record on a victim ns
    - Put ‘www.google.com. A 1.2.3.4’ on ns1.nctu
    - Users in NCTU can still access other Google services (www.gmail.com , maps.google.com, picasa.google.com,…)
  - You can poison a ‘NS’ record on a victim ns
    - Put ‘mobile01.com NS ns.evil.com’ on ns1.nctu
    - With Bailiwick defense, you can only do this following a query to the mobile01.com domain
- Furthermore, you need to race against the legitimate responses and wait for TTL to expire
  - Practically not so devastating

Kaminsky-Style Poisoning

- In the summer of 2008, Dan Kaminsky discovered a new way to poison DNS
  - It poisons the whole domain
  - It defeats Bailiwick defense
  - Very devastating
  - Followed by world-wide DNS server patches

Kaminsky-Style Poisoning

- You want to poison the *bankofsteve.com* domain
- Send query for *www12345678.bankofsteve.com* (something unlikely to exist in the victim ns' cache)
- Spoof responses to the victim that delegates the DNS query to a ns controlled by *badguy.com*
- The spoofed response can contain the real bankofsteve.com nameserver's FQDN so that it will pass bailiwick check
- The glued record 'ns1.bankofsteve.com A 10.9.9.98' points to the IP address of *badguy.com*'s ns
- To the victim, the bad guy owns *bankofsteve.com* domain



(from http://unixwiz.net/)

Kaminsky-Style Poisoning

- The bad guy no longer needs to wait for TTL
  - 1.google.com, 2.google.com, 3.google.com, ..4.google.com,…
- To the victim, a bad guy who wins the race for "123.google.com" owns the whole google.com domain
- The malicious response
  - google.com NS ns1.google.com
  - ns1.google.com A 6.6.6.6

  OR
  - google.com NS ns.badguy.com

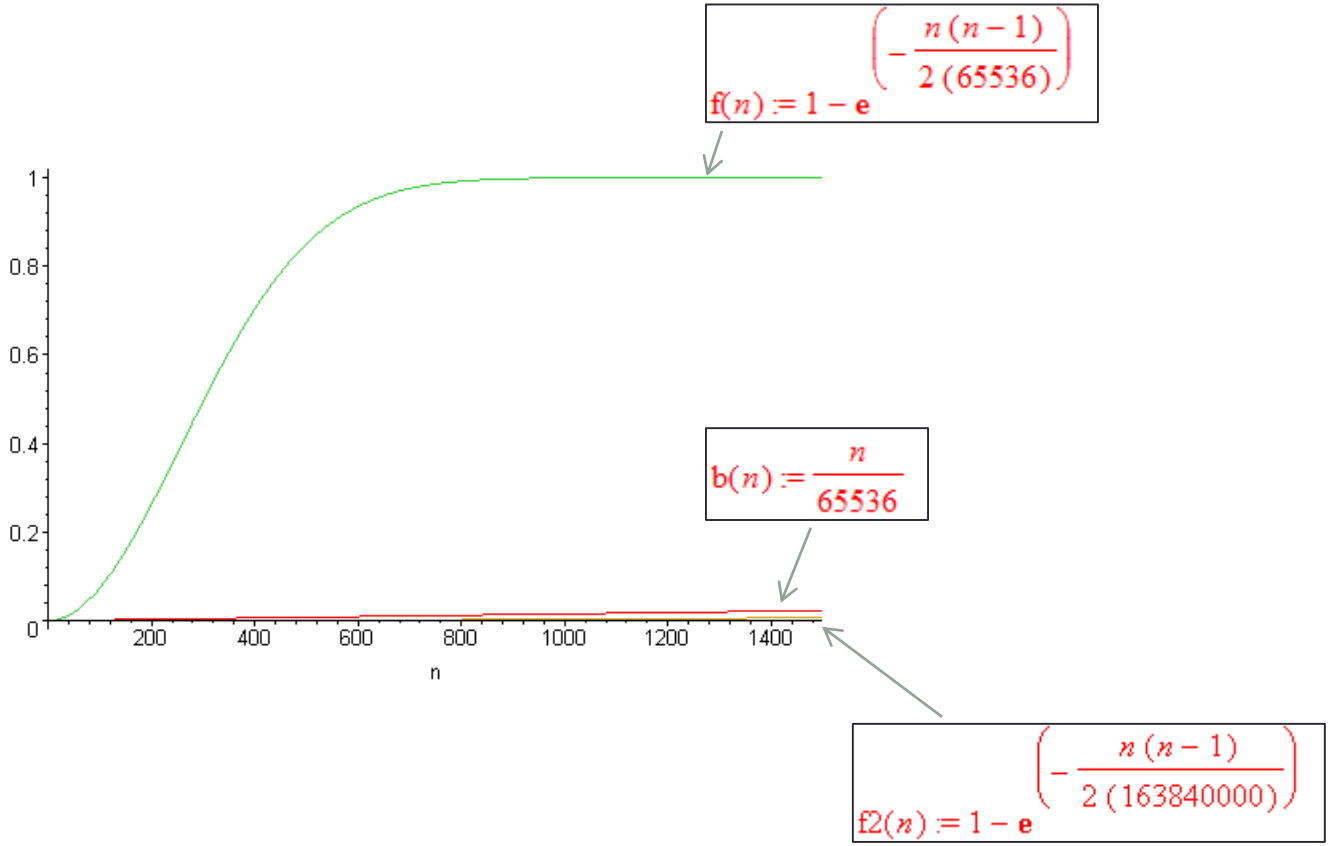
The Defense

- What is supposed to prevent DNS poisoning?
  - Bailiwick
  - (Real random) Query ID
    - 16-bit random number
    - The real server knows the number, because it was contained in the query
    - The bad guy has to guess
  - TTL
    - If you've got the correct working record in the cache, the attacker can't touch it
    - However, if you've got the poisoned record, this actually hurts
- Flurry of queries (birthday attack) defeats the query ID
- The use of non-existing FQDNs in Kaminsky attack defeats the TTL and Bailiwick. It also amplifies the efficiency in birthday attack.

Defense for (Kaminsky-Style) DNS Poisoning

- All attacks depend on hitting the right QID value, which is only 16 bit long
- Can we increase it?
  - It will break the existing DNS deployment
- Instead, use source-port randomization on the DNS server
  - Originally, DNS server always uses port 53 as src port for sending queries and received responses
  - Use a random src port number for each outgoing query and its corresponding response
  - Microsoft's patched DNS server pre-allocates 2500 UDP ports for this
    - $2^{16}*2500 = 163840000$ combinations to guess

Birthday Attack Again



Future of DNS

- The patch following the Kaminsky attack is practically effective
  - What else defense can you think of?
- Port address translation on firewalls can de-randomize the source port randomization
- Theoretically, one can still poison the current DNS system
- Data origin authentication and data integrity are the two fundamental issues of current DNS

Future of DNS

- DNSSEC
  - Build PKI based protection into DNS
  - Resource record is digitally signed
- IPv6
  - Comes with encryption and authentication
  - Alleviates threats from spoofed packets

```
nlnetlabs.nl.  IN  SOA (soa-parameters)
; The zone key
nlnetlabs.nl.  IN  DNSKEY LabsKey
nlnetlabs.nl.  IN  RRSIG(SOA)Labskey
; The (self) signature of the zone key
nlnetlabs.nl.  IN  RRSIG(DNSKEY)Labskey
nlnetlabs.nl.  IN  NS open.nlnetlabs.nl.
nlnetlabs.nl.  IN  RRSIG(NS)LabsKey
```

DNSSEC

42 28.781528	fe80::688c:a7c9:d791:	ff02::c	SSDP	M-SEARCH * HTTP/1.1
43 30.058664	Buffalo_2e:5b:8e	Spanning-tree-(for-br	STP	Conf. Root = 32768/0/00:16:01:2e:5b:8e Cost = 0 Port = 0x8001
44 30.984010	192.168.0.103	192.168.0.1	DNS	Standard query A iis.se
45 31.621175	192.168.0.1	192.168.0.103	DNS	Standard query response A 212.247.7.218 RRSIG
46 32.058254	Buffalo_2e:5b:8e	Spanning-tree-(for-br	STP	Conf. Root = 32768/0/00:16:01:2e:5b:8e Cost = 0 Port = 0x8001
47 32.779610	fe80::688c:a7c9:d791:	ff02::c	SSDP	M-SEARCH * HTTP/1.1
48 34.057206	Buffalo_2e:5b:8e	Spanning-tree-(for-br	STP	
49 35.778155	fe80::688c:a7c9:d791:	ff02::c	SSDP	
50 35.983716	CadmusCo_5e:3b:79	Cisco-Li_c1:cb:15	ARP	
51 35.984348	Cisco-Li_c1:cb:15	CadmusCo_5e:3b:79	ARP	
52 36.055674	Buffalo_2e:5b:8e	Spanning-tree-(for-br	STP	

```
▷ Queries
▽ Answers
  ▷ iis.se: type A, class IN, addr 212.247.7.218
  ▽ iis.se: type RRSIG, class IN
      Name: iis.se
      Type: RRSIG (RR signature)
      Class: IN (0x0001)
      Time to live: 1 minute
      Data length: 154
      Type covered: A (Host address)
      Algorithm: RSA/SHA1
      Labels: 2
      Original TTL: 1 minute
      Signature expiration: Mar 26, 2011 17:10:01.000000000
      Time signed: Mar 16, 2011 17:10:01.000000000
      Id of signing key(footprint): 42734
      Signer's name: iis.se
      Signature
▽ Authoritative nameservers
  ▷ iis.se: type NS, class IN, ns ns2.nic.se
  ▷ iis.se: type NS, class IN, ns ns.nic.se
  ▷ iis.se: type NS, class IN, ns ns3.nic.se
  ▷ iis.se: type RRSIG, class IN
```

```
050  07 da c0 0c 00 2e 00 01  00 00 00 3c 00 9a 00 01   ........ ...<....
060  05 02 00 00 00 3c 4d 8d  ad 69 4d 80 7e 69 a6 ee   .....<M. .iM.~i..
070  03 69 69 73 02 73 65 00  30 4e c6 79 82 25 bc 51   .iis.se. 0N.y.%.Q
080  3a e4 a9 17 f2 57 72 7c  80 00 23 8d 99 ad ca a0   :....Wr| ..#.....
090  33 5d 8c 8c 49 03 f4 ee  eb c1 01 78 ab 4c a0 d4   3]..I... ...x.L..
0a0  cf 9e ca 2e 42 ef f1 3b  c4 59 52 bf 84 f8 2e 05   ....B..; .YR.....
0b0  9f e2 80 ac 96 00 45 08  44 78 73 ba e8 33 64 2c   ......E. Dxs..3d,
```

Hank@Blueberry:/home/Hank

File Edit View Terminal Help

```
[root@Blueberry Hank]# dig +dnssec iis.se.

; <<>> DiG 9.7.1-P2-RedHat-9.7.1-2.P2.fc13 <<>> +dnssec iis.se.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 13603
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 4, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 1280
;; QUESTION SECTION:
;iis.se.                        IN      A

;; ANSWER SECTION:
iis.se.                 60      IN      A       212.247.7.218
iis.se.                 60      IN      RRSIG   A 5 2 60 20110326091001 20110316
091001 42734 iis.se. ME7GeYIlvFE65KkX8ldyfIAAI42ZrcqgM12MjEkD9O7rwQF4q0yg1M+e yi
5C7/E7xFlSv4T4LgWf4oCslgBFCER4c7roM2QsouQFk/4tBvJeqSfz 6+3DCjYtDb7YPTVYXpS8MurQ2
QuZfIZStPr55isePa06Z13SWpte8zIi GAM=

;; AUTHORITY SECTION:
iis.se.                 3600    IN      NS      ns2.nic.se.
iis.se.                 3600    IN      NS      ns.nic.se.
iis.se.                 3600    IN      NS      ns3.nic.se.
iis.se.                 3600    IN      RRSIG   NS 5 2 3600 20110326091001 20110
316091001 42734 iis.se. lSpoFTTrFO589hg8c1vcw4PsKxComA+UY99Zt70M46DaXVQQv/9I+JLs
 btZ8JCBtRsCYwvb5VSkG7gfXTK7lmuJXegi6f98NNSYOJlKkdT3n+Qig NFcAySETCuxD5RpG2xH5Qs
1A9s6iEX9vqm0jSo6XOwhbEDBnjlaXgRiw L08=

;; Query time: 641 msec
;; SERVER: 192.168.0.1#53(192.168.0.1)
;; WHEN: Thu Mar 17 20:29:03 2011
;; MSG SIZE  rcvd: 440

[root@Blueberry Hank]# dig +dnssec iis.se.
```

DNSSEC

- Authoritative server can provide digital signatures for resource record set (RRset).
  - Verify by public Keys (Zone Signing Key and Key Signing Key)
  - But how to verify the public keys?
- Validating resolver verifies the signatures to authenticate a DNSSEC response
  - Typically, a recursive resolver (e.g. 140.113.1.1 on NCTU campus) will act as the validating resolver
  - Typically, the DNS client (the stub resolver) at the end-point is non-validating
  - Connection between end-point and the validating resolver can be secured by IPSec

DNSSEC

```
[Hank@IP-167-145 ~]$ dig +dnssec +multiline  iis.se.

; <<>> DiG 9.7.1-P2-RedHat-9.7.1-2.P2.fc13 <<>> +dnssec +multiline iis.se.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18493
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 4, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;iis.se.                        IN A

;; ANSWER SECTION:
iis.se.                 60 IN A 212.247.7.218
iis.se.                 60 IN RRSIG A 5 2 60 20110319100001 (
                                20110309100001 42734 iis.se.
                                J2sy+w6ZJLuzlfoiVwMhAdtKGhjFERX3RzGtqWM7P5CA
                                XaE33dCnBzTJ+dCbinrq7ePIbNlfvwG3i+/aNA2MZ+Td
                                mQ7aEsbYmRN3w9GI7uPUd6Vx/AIU2Xso+/5Z07TmbRXq
                                mtaTGbtABhkz/SPNYXlkLwT0Z5L1di8gLXFUUxI= )

;; AUTHORITY SECTION:
iis.se.                 3600 IN NS ns.nic.se.
iis.se.                 3600 IN NS ns3.nic.se.
iis.se.                 3600 IN NS ns2.nic.se.
iis.se.                 3600 IN RRSIG NS 5 2 3600 20110319100001 (
                                20110309100001 42734 iis.se.
                                AGSQiCRsFJoqkMUG/a1rJOh+irhcvdQPWviQu2ltladq
                                LybPblNORhVyQ9WEsouZmmj7cjWam/Evdi7Nnz5D94XL
                                pG6avBJdaPit6OSHwOvfKs2djKh0/kj0ecsP9rnRK2jJ
                                cjgZIMlD88VbxLKyOc9a0P4KhxH7xxAObejnrPw= )

;; Query time: 335 msec
;; SERVER: 140.113.1.1#53(140.113.1.1)
;; WHEN: Mon Mar 14 12:09:21 2011
;; MSG SIZE  rcvd: 440

[Hank@IP-167-145 ~]$
```

Non-validating resolver

```
[Hank@IP-167-145 ~]$ dig +dnssec +multiline @149.20.64.20  iis.se.

; <<>> DiG 9.7.1-P2-RedHat-9.7.1-2.P2.fc13 <<>> +dnssec +multiline @149.20.64.20 iis.se.
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6381
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 4, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;iis.se.                        IN A

;; ANSWER SECTION:
iis.se.                 60 IN A 212.247.7.218
iis.se.                 60 IN RRSIG A 5 2 60 20110319100001 (
                                20110309100001 42734 iis.se.
                                J2sy+w6ZJLuzlfoiVwMhAdtKGhjFERX3RzGtqWM7P5CA
                                XaE33dCnBzTJ+dCbinrq7ePIbNlfvwG3i+/aNA2MZ+Td
                                mQ7aEsbYmRN3w9GI7uPUd6Vx/AIU2Xso+/5Z07TmbRXq
                                mtaTGbtABhkz/SPNYXlkLwT0Z5L1di8gLXFUUxI= )

;; AUTHORITY SECTION:
iis.se.                 3351 IN NS ns.nic.se.
iis.se.                 3351 IN NS ns2.nic.se.
iis.se.                 3351 IN NS ns3.nic.se.
iis.se.                 3351 IN RRSIG NS 5 2 3600 20110319100001 (
                                20110309100001 42734 iis.se.
                                AGSQiCRsFJoqkMUG/a1rJOh+irhcvdQPWviQu2ltladq
                                LybPblNORhVyQ9WEsouZmmj7cjWam/Evdi7Nnz5D94XL
                                pG6avBJdaPit6OSHwOvfKs2djKh0/kj0ecsP9rnRK2jJ
                                cjgZIMlD88VbxLKyOc9a0P4KhxH7xxAObejnrPw= )

;; Query time: 837 msec
;; SERVER: 149.20.64.20#53(149.20.64.20)
;; WHEN: Mon Mar 14 12:11:51 2011
;; MSG SIZE  rcvd: 440

[Hank@IP-167-145 ~]$
```

Validating resolver

DNSSEC Chain of Trust

org. Zone

KSK_{org} DNSKEY
ZSK_{org} DNSKEY + $RRSIG_{KSKorg}$
isc.org. DS Tag_$KSK_{isc.org}$ + $RRSIG_{ZSKorg}$

isc.org. Zone

$KSK_{isc.org}$ DNSKEY
$ZSK_{isc.org}$ DNSKEY + $RRSIG_{KSKisc.org}$
www.isc.org. A + $RRSIG_{ZSKisc.org}$

DNSKEY (Root ZSK, KSK)

29	3.121117	192.168.0.103	192.168.0.1	DNS	Standard query DNSKEY <Root>
30	3.142509	192.168.0.1	192.168.0.103	DNS	Standard query response DNSKEY DNSKEY
31	3.855560	202.39.43.198	192.168.0.144	HTTP	Continuation or non-HTTP traffic

```
▷ Flags: 0x8180 (Standard query response, No error)
  Questions: 1
  Answer RRs: 2
  Authority RRs: 0
  Additional RRs: 0
▷ Queries
▽ Answers
  ▽ <Root>: type DNSKEY, class IN
      Name: <Root>
      Type: DNSKEY (DNS public key)
      Class: IN (0x0001)
      Time to live: 1 day, 22 hours, 48 minutes, 27 seconds
      Data length: 264
    ▽ Flags: 0x0101
        .... ...1 .... .... = This is the zone key for the specified zone
        .... .... 0... .... = Key is not revoked
        .... .... .... ...1 = Key is a Key Signing Key
      Protocol: 3
      Algorithm: Unknown (0x08)
      Key id: 19036
      Public key
  ▽ <Root>: type DNSKEY, class IN
      Name: <Root>
      Type: DNSKEY (DNS public key)
      Class: IN (0x0001)
      Time to live: 1 day, 22 hours, 48 minutes, 27 seconds
      Data length: 136
    ▽ Flags: 0x0100
        .... ...1 .... .... = This is the zone key for the specified zone
        .... .... 0... .... = Key is not revoked
        .... .... .... ...0 = Key is a Zone Signing Key
      Protocol: 3
      Algorithm: Unknown (0x08)
      Key id: 21639
      Public key
```

Hank@Blueberry:/home/Hank

File Edit View Terminal Help

```
[root@Blueberry Hank]# dig . DNSKEY +multiline

; <<>> DiG 9.7.1-P2-RedHat-9.7.1-2.P2.fc13 <<>> . DNSKEY +multiline
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 35969
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;.                      IN DNSKEY

;; ANSWER SECTION:
.                       168507 IN DNSKEY 257 3 8 (
                                AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLOyQ
                                bSEW0O8gcCjFFVQUTf6v58fLjwBd0YI0EzrAcQqBGCzh
                                /RStIoO8g0NfnfL2MTJRkxoXbfDaUeVPQuYEhg37NZWA
                                JQ9VnMVDxP/VHL496M/QZxkjf5/Efucp2gaDX6RS6CXp
                                oY68LsvPVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3
                                LQpzW5hOA2hzCTMjJPJ8LbqF6dsV6DoBQzgul0sGIcGO
                                Yl7OyQdXfZ57relSQageu+ipAdTTJ25AsRTAoub8ONGc
                                LmqrAmRLKBP1dfwhYB4N7knNnulqQxA+Uk1ihz0=
                                ) ; key id = 19036
.                       168507 IN DNSKEY 256 3 8 (
                                AwEAAb5gVAzK59YHDxf/DnswfO1RmbRZ6W16JfhFecfI
                                +EUHRXPWlXDi47t2FHaKyMMEROapL5SZ8HiCzl05lORZ
                                GGdN37WY7fkv55rs+kwHdVRSrQdl81fUnEspt67IIgaj
                                3SrGyZqgzyixNk/8oT3yEfKDycTeJy4chKPt0JegWrjL
                                ) ; key id = 21639

;; Query time: 23 msec
;; SERVER: 192.168.0.1#53(192.168.0.1)
;; WHEN: Thu Mar 17 22:29:14 2011
;; MSG SIZE  rcvd: 439

[root@Blueberry Hank]#
```

DNS beyond 512bytes – EDNS0

1 0.000000	192.168.0.103	192.168.0.1	DNS	Standard query A www.whitehouse.gov
2 0.372227	192.168.0.1	192.168.0.103	DNS	Standard query response CNAME www.whitehouse.gov.edgesuite.net RRSIG

```
        Time to live: 30 minutes
        Data length: 6
        Name server: n2h.akamai.net
    ▽ h.akamai.net: type NS, class IN, ns n0h.akamai.net
        Name: h.akamai.net
        Type: NS (Authoritative name server)
        Class: IN (0x0001)
        Time to live: 30 minutes
        Data length: 6
        Name server: n0h.akamai.net
  ▽ Additional records
    ▽ <Root>: type OPT
        Name: <Root>
        Type: OPT (EDNS0 option)
        UDP payload size: 1280
        Higher bits in extended RCODE: 0x0
        EDNS0 version: 0
      ▽ Z: 0x8000
          Bit 0 (DO bit): 1 (Accepts DNSSEC security RRs)
          Bits 1-15: 0x0 (reserved)
        Data length: 0
```

```
1b0  12 00 02 00 01 00 00 07  08 00 06 03 6e 34 68 c1   ........ ....n4h.
1c0  14 c1 12 00 02 00 01 00  00 07 08 00 06 03 6e 37   ........ ......n7
1d0  68 c1 14 c1 12 00 02 00  01 00 00 07 08 00 06 03   h....... ........
1e0  6e 38 68 c1 14 c1 12 00  02 00 01 00 00 07 08 00   n8h..... ........
1f0  06 03 6e 32 68 c1 14 c1  12 00 02 00 01 00 00 07   ..n2h... ........
200  08 00 06 03 6e 30 68 c1  14 00 00 29 05 00 00 00   ....n0h. ...)....
210  80 00 00 00                                         ....
```

) Response Type (dns.resp.type), 2 b... Packets: 2 Displayed: 2 Marked: 0 Dropped: 0

Hank@Blueberry:/tmp/p1

File Edit View Terminal Help

```
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20610
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 9, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 1280
;; QUESTION SECTION:
;www.whitehouse.gov.    IN A

;; ANSWER SECTION:
www.whitehouse.gov.     3600 IN CNAME www.whitehouse.gov.edgesuite.net.
www.whitehouse.gov.     3600 IN RRSIG CNAME 7 3 3600 20110321101947 (
                                20110318091947 3302 whitehouse.gov.
                                xam1iCbw2XQdak7M19CN3x6hYavvD2ZKJpU9NX6ZdhfF
                                Q02tCMHrN1gtsZ3wWH9glH2UKEMrQs4+orlHW9nkN3hC
                                pCVwt3aNjjGgrnLi0Qttupedv/7OKGCNtgpeyphZSMIj
                                hzTcUF2SdN95tnoxoB24yyaa1dldv/8JxmLCo14= )
www.whitehouse.gov.edgesuite.net. 900 IN CNAME a1128.h.akamai.net.
a1128.h.akamai.net.     20 IN A 198.173.160.17
a1128.h.akamai.net.     20 IN A 198.173.160.49

;; AUTHORITY SECTION:
h.akamai.net.           1800 IN NS n5h.akamai.net.
h.akamai.net.           1800 IN NS n1h.akamai.net.
h.akamai.net.           1800 IN NS n6h.akamai.net.
h.akamai.net.           1800 IN NS n3h.akamai.net.
h.akamai.net.           1800 IN NS n4h.akamai.net.
h.akamai.net.           1800 IN NS n7h.akamai.net.
h.akamai.net.           1800 IN NS n8h.akamai.net.
h.akamai.net.           1800 IN NS n2h.akamai.net.
```

DNS Over TCP – ENDS0

Hank@Blueberry:/tmp/p1

File Edit View Terminal Help

```
[root@Blueberry p1]# dig  gov. DNSKEY
;; Truncated, retrying in TCP mode.

; <<>> DiG 9.7.1-P2-RedHat-9.7.1-2.P2.fc13 <<>> gov. DNSKEY
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17884
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;gov.                            IN      DNSKEY

;; ANSWER SECTION:
gov.                    65831   IN      DNSKEY  256 3 7 AQOzN7RchHtjxjNavn3AYMNYRK4YTPv9hONG2y+43/zApQh3KHZQo3l1 rprk9K
eRWD1PxtUltA40w8ANrui+YQd30Io1Jn0fEG9KVDtZWQXaXWXr lNw1eP93xIG71RALot9X22a845cNqwrhqCe0ke8BcATNDMBKw35NnRV2 AWP9AxsaUJd
AK51qXDve5PPqgzPUR2wUCytdLBLU3n4MjLizR/GyqIXw vUCSBfW5S+7Mco1l1vJPI7Sdepays3MaRgvjA8x1UOuqaNeWkWDnbJUM owlUWgKDdRFZ9G3L
rUev3XXxmrMarK0sN6zm4zxLdbxtZkKQzCywWZ+h Ku30WRGN
gov.                    65831   IN      DNSKEY  256 3 7 AQPfjKZ6za5oNBsA+pyN49NNoqR45FvK6+dcto5//bRwZTHtSbf7b/tI eGwggV
8p4ULebkF9JuYcEcWVlSHfUMJVA6z9MHZ/rH585lPvM2jSNFVh 21iVpNce4RH3DxsXf38tb+YrJk+kMj8VhxPRe5gMsYZ3U3/L13c3HKjh X1CLYhTlJYD
4jX9AOl5Sc7qv6FaYLfjtjsieBcShp6e8A8za7l8FVCLn cTDFPOnokeDMpPwwcXVcbfKBd7LN8lcBq4neW81ORZIzQI9GurabpU4w uVdRG6yixeJgncmK
d+ttjfJVB5QmFtSqyJ7LTrHkMxR/Mg/bc93FZ/7g sEhoqkcD
gov.                    65831   IN      DNSKEY  256 3 7 BQEAAAABvSN63WSZXqKpkUlpHZjtvhZqgTTXwS+ayt8E/0AuuXvEuFOk UzUqyU
ahwSdhbds2aLWJK4Gg7Z0huM/hAnqgvMxpRgY9wyJ0oh5UuO3X pAChAEups6ufY7M/+16lHpkbjQgw45o3t/AOFrxhjAUOA4PR21P7Jmko fhMFmnhLnro
u9fK+704kr/5uq19xZ1nClCZd+Awtt7mgArePJ0k6HDbS cXY9hjr6uwKwbx8Dji+nCajkxBHatAFLz8G0z0lCN3VSnMSrw7U+nNpL zUBcGB8oYAyHV2Mo
xQFPm8z+b8fZemT5kXftn/XdEbS4qrG48czluD56 ESUSQ+z9p4AGLw==
gov.                    65831   IN      DNSKEY  257 3 7 AQO7tpGcHVEdeAwk47cj6Tuc3dvAUktIQ1vMu8mGtGYQ8F6vSOgViE0t mzPtVF
rV9E6kY1jLYCh+oKPWn7efpQVMkqc+2b9ECYk/81fA4Vb0BfyY KKhiW7T1uNX4rC03JZa2u8iOHwqq4BRVplksFXCGn47i2Sosa5KuqCNB qUA0oyPTEbx
kyNo3Q6l8ZcscILqbvWZ0BJKaLCTtj08Nj35LTqd/XVoE Obp48A21Pqyi6Kiblh9H6NoLtqhlvP5+8AujtINJ+sTUQZYgqt9iFQp2 AH4HvyJdw8Vkr1QR
hhshq6RgRidnOvTIWZKoe4QHQrvmOfW245zv+22I uu5rYpcl

;; Query time: 70 msec
;; SERVER: 192.168.0.1#53(192.168.0.1)
;; WHEN: Fri Mar 18 22:54:32 2011
;; MSG SIZE  rcvd: 1121

[root@Blueberry p1]#
```

DNS Over TCP – ENDS0

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.0.103	192.168.0.1	DNS	Standard query DNSKEY gov
2	0.022376	192.168.0.1	192.168.0.103	DNS	Standard query response DNSKEY
3	0.023432	192.168.0.103	192.168.0.1	TCP	58718 > domain [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=42637285 TSER
4	0.024752	192.168.0.1	192.168.0.103	TCP	domain > 58718 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 TSV=64
5	0.024825	192.168.0.103	192.168.0.1	TCP	58718 > domain [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSV=42637286 TSER=64
6	0.025099	192.168.0.103	192.168.0.1	DNS	Standard query DNSKEY gov
7	0.032455	192.168.0.1	192.168.0.103	TCP	domain > 58718 [ACK] Seq=1 Ack=24 Win=5792 Len=0 TSV=6446332 TSER=42
8	0.091587	192.168.0.1	192.168.0.103	TCP	[TCP segment of a reassembled PDU]
9	0.091685	192.168.0.103	192.168.0.1	TCP	58718 > domain [ACK] Seq=24 Ack=2 Win=5888 Len=0 TSV=42637353 TSER=6
10	0.092877	192.168.0.1	192.168.0.103	DNS	Standard query response DNSKEY DNSKEY DNSKEY DNSKEY
11	0.092899	192.168.0.103	192.168.0.1	TCP	58718 > domain [ACK] Seq=24 Ack=1124 Win=8192 Len=0 TSV=42637355 TSE
12	0.095749	192.168.0.103	192.168.0.1	TCP	58718 > domain [FIN, ACK] Seq=24 Ack=1124 Win=8192 Len=0 TSV=4263735
13	0.096860	192.168.0.1	192.168.0.103	TCP	domain > 58718 [FIN, ACK] Seq=1124 Ack=25 Win=5792 Len=0 TSV=6446338

```
    Type: DNSKEY (DNS public key)
    Class: IN (0x0001)
    Time to live: 20 hours, 25 minutes, 47 seconds
    Data length: 262
  ▽ Flags: 0x0101
      .... ...1 .... .... = This is the zone key for the specified zone
      .... .... 0... .... = Key is not revoked
      .... .... .... ...1 = Key is a Key Signing Key
    Protocol: 3
    Algorithm: RSA/SHA1 + NSEC3/SHA1
    Key id: 53138
    Public key
```

```
0000  08 00 27 5e 3b 79 00 18  39 c1 cb 15 08 00 45 00   ..'^;y.. 9.....E.
0010  01 43 00 00 40 00 40 11  b7 f1 c0 a8 00 01 c0 a8   .C..@.@. ........
0020  00 67 00 35 c1 ad 01 2f  6d c3 02 21 83 80 00 01   .g.5.../ m..!....
0030  00 01 00 00 00 00 03 67  6f 76 00 00 30 00 01 c0   .......g ov..0...
0040  0c 00 30 00 01 00 01 1f  4b 01 06 01 01 03 07 01   ..0..... K.......
0050  03 bb b6 91 9c 1d 51 1d  78 0c 24 e3 b7 23 e9 3b   ......Q. x.$..#.;
0060  9c dd db c0 52 4b 48 43  5b cc bb c9 86 b4 66 10   ....RKHC [.....f.
0070  f0 5e af 48 e8 15 88 4d  2d 9b 33 ed 54 5a d5 f4   .^.H...M -.3.TZ..
```

DNS Over TCP

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.0.103	140.113.235.107	TCP	36443 > domain [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=1462080 TSER=0 WS=7
2	0.018092	140.113.235.107	192.168.0.103	TCP	domain > 36443 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1452 WS=1 TSV=1291658924
3	0.018189	192.168.0.103	140.113.235.107	TCP	36443 > domain [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSV=1462099 TSER=1291658924
4	0.018661	192.168.0.103	140.113.235.107	DNS	Standard query A www.facebook.com
5	0.041815	140.113.235.107	192.168.0.103	DNS	Standard query response A 69.63.181.11
6	0.042053	192.168.0.103	140.113.235.107	TCP	36443 > domain [ACK] Seq=37 Ack=123 Win=5888 Len=0 TSV=1462123 TSER=1291658947
7	0.044141	192.168.0.103	140.113.235.107	TCP	36443 > domain [FIN, ACK] Seq=37 Ack=123 Win=5888 Len=0 TSV=1462125 TSER=1291658947
8	0.061407	140.113.235.107	192.168.0.103	TCP	domain > 36443 [ACK] Seq=123 Ack=38 Win=66240 Len=0 TSV=1291658967 TSER=1462125
9	0.063757	140.113.235.107	192.168.0.103	TCP	domain > 36443 [FIN, ACK] Seq=123 Ack=38 Win=66240 Len=0 TSV=1291658967 TSER=146212
10	0.063832	192.168.0.103	140.113.235.107	TCP	36443 > domain [ACK] Seq=38 Ack=124 Win=5888 Len=0 TSV=1462145 TSER=1291658967

```
▷ Frame 5 (188 bytes on wire, 188 bytes captured)
▷ Ethernet II, Src: Cisco-Li_c1:cb:15 (00:18:39:c1:cb:15), Dst: CadmusCo_5e:3b:79 (08:00:27:5e:3b:79)
▷ Internet Protocol, Src: 140.113.235.107 (140.113.235.107), Dst: 192.168.0.103 (192.168.0.103)
▷ Transmission Control Protocol, Src Port: domain (53), Dst Port: 36443 (36443), Seq: 1, Ack: 37, Len: 122
▽ Domain Name System (response)
    [Request In: 4]
    [Time: 0.023154000 seconds]
    Length: 120
    Transaction ID: 0x79ac
  ▷ Flags: 0x8180 (Standard query response, No error)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 2
    Additional RRs: 2
  ▷ Queries
  ▽ Answers
    ▽ www.facebook.com: type A, class IN, addr 69.63.181.11
        Name: www.facebook.com
        Type: A (Host address)
        Class: IN (0x0001)
        Time to live: 4 seconds
        Data length: 4
        Addr: 69.63.181.11
  ▽ Authoritative nameservers
    ▽ www.facebook.com: type NS, class IN, ns glb2.facebook.com
        Name: www.facebook.com
        Type: NS (Authoritative name server)

0000  08 00 27 5e 3b 79 00 18  39 c1 cb 15 08 00 45 00   ..'^;y.. 9..
0010  00 ae f0 ea 40 00 37 06  19 73 8c 71 eb 6b c0 a8   ....@.7. .s.
0020  00 67 00 35 8e 5b 67 1a  a5 7f 8e 8a 90 c6 80 18   .g.5.[g. ...
0030  81 60 50 1c 00 00 01 01  08 0a 4c fd 26 c3 00 16   .`P..... ..L
```

File: "/tmp/wireshark_XXXXAD7AtO Packets: 10 Displayed: 10 Marked: 0 Drop

```
Hank@Blueberry:/home/Hank
File  Edit  View  Terminal  Help
[root@Blueberry Hank]# dig  www.facebook.com. @dns.cs.nctu.edu.tw   +tcp

; <<>> DiG 9.7.1-P2-RedHat-9.7.1-2.P2.fc13 <<>> www.facebook.com. @dns.cs.nctu.edu.tw +tcp
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 31148
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;www.facebook.com.              IN      A

;; ANSWER SECTION:
www.facebook.com.       4       IN      A       69.63.181.11

;; AUTHORITY SECTION:
www.facebook.com.       8968    IN      NS      glb2.facebook.com.
www.facebook.com.       8968    IN      NS      glb1.facebook.com.

;; ADDITIONAL SECTION:
glb1.facebook.com.      1261    IN      A       69.171.239.10
glb2.facebook.com.      1261    IN      A       69.171.255.10

;; Query time: 25 msec
;; SERVER: 140.113.235.107#53(140.113.235.107)
;; WHEN: Thu Mar 17 20:53:56 2011
;; MSG SIZE  rcvd: 120

[root@Blueberry Hank]#
```

DNSSEC Zone enumeration issue

```
[Hank@IP-167-145 ~]$ dig +dnssec +multiline @149.20.64.20  pighead.iis.se.

; <<>> DiG 9.7.1-P2-RedHat-9.7.1-2.P2.fc13 <<>> +dnssec +multiline @149.20.64.20 pighead.iis.se.
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 144
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 6, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;pighead.iis.se.                IN A

;; AUTHORITY SECTION:
iis.se.                 3600 IN SOA ns.nic.se. hostmaster.iis.se. (
                                1299668401 ; serial
                                10800      ; refresh (3 hours)
                                3600       ; retry (1 hour)
                                1814400    ; expire (3 weeks)
                                14400      ; minimum (4 hours)
                                )
iis.se.                 3600 IN RRSIG SOA 5 2 3600 20110319100001 (
                                20110309100001 42734 iis.se.
                                nc2eofMP5fQHjAM/liyTO08riekIsMa/XUdEtrQmQgn2
                                UtzlVqRlIHlJPPc2W/fpSi8MCo06WAo4e5myV74D4Noe
                                QaFg16tRYWmx4aGkpPIW3HY8nY/wMp4nHnaQZ4g7F06d
                                BQdn9E8F2QkNWmodb3E1CdfmRKy6Ud33B2d+63k= )
iis.se.                 3600 IN RRSIG NSEC 5 2 14400 20110319100001 (
                                20110309100001 42734 iis.se.
                                jQ+wpfgv3KJ0BUrWAOGVB7V23/Grvzm5P+MCDfZOK0N6
                                ealNpbGAQw0k+YeXsN+eMflMd2VPXi3AeMy9VW6ueI9n
                                eQBm/JLHtYilfnQWt7yq+8zTd5ylatQy06naeBuF/wjA
                                UKt3vdIQZoYxVCmPXI432KQDvRqdvG8G3MWjE2c= )
iis.se.                 3600 IN NSEC 2010.iis.se. A NS SOA MX TXT AAAA RRSIG NSEC DNSKEY
packages.iis.se.        3600 IN RRSIG NSEC 5 3 14400 20110319100001 (
                                20110309100001 42734 iis.se.
                                UUfe8jMK5kj672Z0LGR86yftbXgetUmrlLUVu5GekoXC
                                /WaQvWCSmQF2RE2JVtJUkv/64jP2Zb/+cFpdKImiY4Y8
                                uTx6hPLNjPlvebaseI+XLdbAUjIAkK9r+w742rfaDXJE
                                3IZLOilUb9mwjSBn/rigWvd6CiI8vkZA/qnjVH8= )
packages.iis.se.        3600 IN NSEC pingdom.iis.se. CNAME RRSIG NSEC

;; Query time: 970 msec
;; SERVER: 149.20.64.20#53(149.20.64.20)
;; WHEN: Mon Mar 14 12:20:55 2011
```

```
[Hank@IP-167-145 ~]$ nslookup packages.iis.se
Server:         140.113.1.1
Address:        140.113.1.1#53

Non-authoritative answer:
packages.iis.se canonical name = spiffy.iis.se.
Name:   spiffy.iis.se
Address: 212.247.204.146

[Hank@IP-167-145 ~]$ nslookup pingdom.iis.se
Server:         140.113.1.1
Address:        140.113.1.1#53

Non-authoritative answer:
Name:   pingdom.iis.se
Address: 194.17.45.54

[Hank@IP-167-145 ~]$ nslook up 2010.iis.se
bash: nslook: command not found
[Hank@IP-167-145 ~]$ nslookup 2010.iis.se
Server:         140.113.1.1
Address:        140.113.1.1#53

Non-authoritative answer:
2010.iis.se     canonical name = more.prod.iis.se.
Name:   more.prod.iis.se
Address: 212.247.7.218

[Hank@IP-167-145 ~]$
```

DNSSEC NSEC3

eth0 (src

File Edit View Go Capture Analyze Statistics

Filter:

No.	Time	Source
5	0.549381	192.168.0.
6	0.549772	192.168.0.
7	0.551095	192.168.0.
8	1.139370	192.168.0.
9	1.139433	192.168.0.

```
    Original TTL: 1 day
    Signature expiration: Mar 23, 2011 1
    Time signed: Mar 18, 2011 18:00:25.0
    Id of signing key(footprint): 47602
    Signer's name: gov
    Signature
  ▽ 578et16s7ltnsq1t0amm21gl20oj5g76.gov:
    Name: 578et16s7ltnsq1t0amm21gl20oj5g
    Type: NSEC3 (Next secured hash)
    Class: IN (0x0001)
    Time to live: 3 hours
    Data length: 41
    Hash algorithm: SHA-1 (1)
  ▷ NSEC3 flags: 0
    NSEC3 iterations: 8
    Salt length: 6
    Salt value: 4C44934802D3
    Hash length: 20
```

```
02d0  00 32 00 01 00 00 2a 30  00 29 01 00 00
02e0  44 93 48 02 d3 14 29 dc  67 7e 11 43 66
02f0  f0 5a 55 1e f2 63 f2 56  5a de 00 07 22
0300  00 02 90 20 38 38 72 6d  37 71 67 66 32
0310  74 73 61 62 31 67 76 69  76 32 63 65 67
0320  37 62 30 61 c1 c7 00 2e  00 01 00 00 2a
0330  00 32 07 02 00 01 51 80  4d 89 c4 b9 4d
```

Frame (141 bytes) | Reassembled TCP (1524 bytes)

Salt value (dns.nsec3.salt_value), ... | Packets: 16 D

Hank@Blueberry:/tmp/p1

File Edit View Terminal Help

```
                                )
gov.                    10800 IN RRSIG SOA 7 1 86400 20110323100025 (
                                20110318100025 47602 gov.
                                X7OFs4h4+krTRzM3lnktdp336VuhB3Rf2OIqwfsu4pdl
                                w25dy6sNOw6xFok55AcS7hv9MxlRTp7lTvBiTLraEU+u
                                PckI52QgM6isH/KmN28EBM87DyjHE/CHUcu6CgwoatU0
                                mnX82W9pGGY01MjjhIKIf9nzHGTCkVDcJx1itGZPQSlK
                                6YAKKb2mpjJCHjoBal4b9l16dy5BilfS5mMt0t3sE6Pt
                                eeX8PyYxkZGPMDA4Z+7nZq74P5RJr5SWQUMXlZeVmlln
                                XCrwU4BUbXqNw6G4okLLeyiQEQYCtVpJ63Tcw7h4cutN
                                ukwopEhXS0JSQ/23kB6eCwq6yD/cInlJyw== )
578et16s7ltnsq1t0amm21gl20oj5g76.gov. 10800 IN RRSIG NSEC3 7 2 86400 20110323100025 (
                                20110318100025 47602 gov.
                                AiTj6iUFUrciJSMgz6SsfOcIXOxB5TOLYdGH2KMub+hL
                                PRiDO2t+dbbay+LHPcYa55L5DHtqy/MMQaVxK4kR6y0p
                                UCbulMP2aY87DAX+kCEqMkMiRleWCFFVWS0kOcAnsGcy
                                NbBuEVlOF9ANofPKwfdB1k5D1UIUyE0nGvT/JMwEtU+2
                                p40nKAOdzrCeFvKTyojXDwGuh37fqPjTmwYIOSIYt0b8
                                hVp9/usHrsfwGXa3426ro4xTnL1an0+vC7F+7Sn/pepO
                                nYRoZIfvmNkQ8kUVVNmdpZ6/fgymwC1Jnr5tIjqvhUjb
                                1f2IaQSQ/i3FdTrxEiKO86r+UJzPnAOkOA== )
578et16s7ltnsq1t0amm21gl20oj5g76.gov. 10800 IN NSEC3 1 0 8 4C44934802D3 57E6EVGH8DJ675MRU1D5A7NICFP5CMMU NS SOA RR
88rm7qgf26i8tsab1gviv2cegacf7b0a.gov. 10800 IN RRSIG NSEC3 7 2 86400 20110323100025 (
                                20110318100025 47602 gov.
                                WlfpPDkgQnQKwzcdZw4KOLari+GdUjqG6v+Hkjg2BecP
                                OsY9dJPxxaFQuUtuQLh6eze5LueO/r4ekFVX6RuGkwWw
                                MY3SrcMZBiHXaMb/4wt0gINLqBqHKGSFKRlwjN4S8Xvl
                                /bxGd1VjRSoNCzyxBaOxDVsEjieVq+w2czne/eFaf9Tx
                                JEP6x8k9gxLpL5uekSMj1ENcF1tX+QgClJ/KaK/LuGY2
                                abvBlEf5h5xshkoEKwHbnVVtl+EXw96mZBmSPlhrODu2
                                xQZSIva0jJ6SrLJr4hdjhVoT7pqaOWQP9IBv8+xAILwx
                                x0dOxthcokg50ooaiL0RMHf2QGa57AE6Lg== )
88rm7qgf26i8tsab1gviv2cegacf7b0a.gov. 10800 IN NSEC3 1 0 8 4C44934802D3 892OJMPA5JSSGH11KT2GQ5DFCK6JDG55 NS
ka690fnatniqid78pvjh8b29tb4p3bio.gov. 10800 IN RRSIG NSEC3 7 2 86400 20110323100025 (
                                20110318100025 47602 gov.
                                ko1z1tpi3vavMbf6VP59VS9A2PDLX8MgCVHeDoIXGPGT
                                Ei3nsjtxn4QnNt1m9gp86ul+fG5zxZAT922w4UxCYMWd
                                ypVrwLxpaRtnBBNs1jmLPZIs+kf4Ot/V77B9aDZ3RluG
                                3MmBWQt6sRa2W/1/VZ8hIuyjxvGkVpmoEtl41f+qC+u+
                                0ftnJQSHxYqkCNzsK7fjN261owBGCbdD8Gp1aAvZYz3H
                                q7Kz0HixAfeHm0Ko28EFm0UqKL57nzlz/UZyQANLGs7q
                                6C5JvubNC2rgeibpv81vfFZGbZb4u09JJl7B9glTxluR
                                jZoMfgbzk+HjMgziKg3OPmM3HZiYJ0+YzA== )
ka690fnatniqid78pvjh8b29tb4p3bio.gov. 10800 IN NSEC3 1 0 8 4C44934802D3 KAQQHVAHKG9ML8UTC9QCOV5L8GDCL1PT NS

;; Query time: 593 msec
;; SERVER: 192.168.0.1#53(192.168.0.1)
;; WHEN: Fri Mar 18 23:06:17 2011
;; MSG SIZE  rcvd: 1522

[root@Blueberry p1]#
```

DNSSEC Status on TLD domains

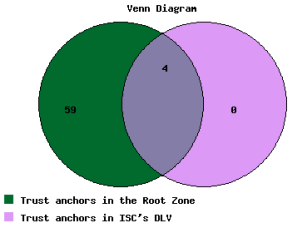
- http://stats.research.icann.org/dns/tld_report/

TLD DNSSEC Report (2011-03-17)

[archive] [latest]

Summary

- 306 TLDs in the root zone in total
- 69 TLDs are signed;
- 63 TLDs have trust anchors published as DS records in the root zone;
- 4 TLDs have trust anchors published in the ISC DLV Repository.



TLD	Sig
ac.	NO
ad.	NO
ae.	NO
aero.	NO
af.	NO
ag.	YES
ai.	NO
al.	NO
am.	YES
an.	NO
ao.	NO
aq.	NO
ar.	NO
arpa.	YES
as.	NO
asia.	YES
at.	NO

TLD DNSSEC Report (2014-10-21 00:02:12)

[archive] [latest]

Summary

- 734 TLDs in the root zone in total
- 552 TLDs are signed;
- 544 TLDs have trust anchors published as DS records in the root zone;
- 6 TLDs have trust anchors published in the ISC DLV Repository.