DNSSEC

The shiny new cryptographically secured globally distributed database

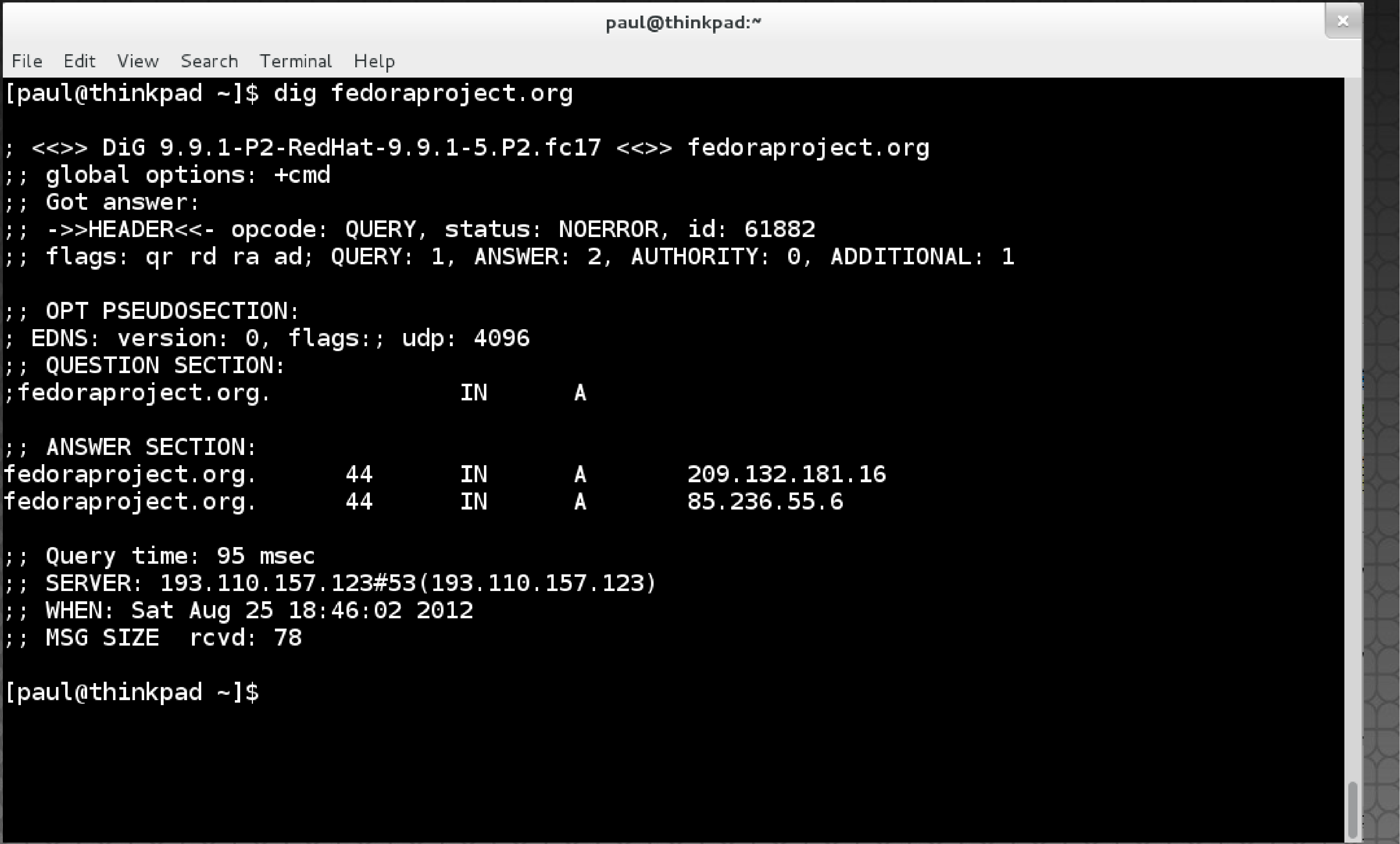
Presented by
Paul Wouters
seceng, Red Hat Inc.

Topics

- DNSSEC theory in 7 screen shots
- DNSSEC software: validating, signing
- Converting applications to use DNSSEC
- Using DNSSEC for non-DNS purposes
    - TLSA, SSHFP, IPSECKEY, <your crazy idea here>

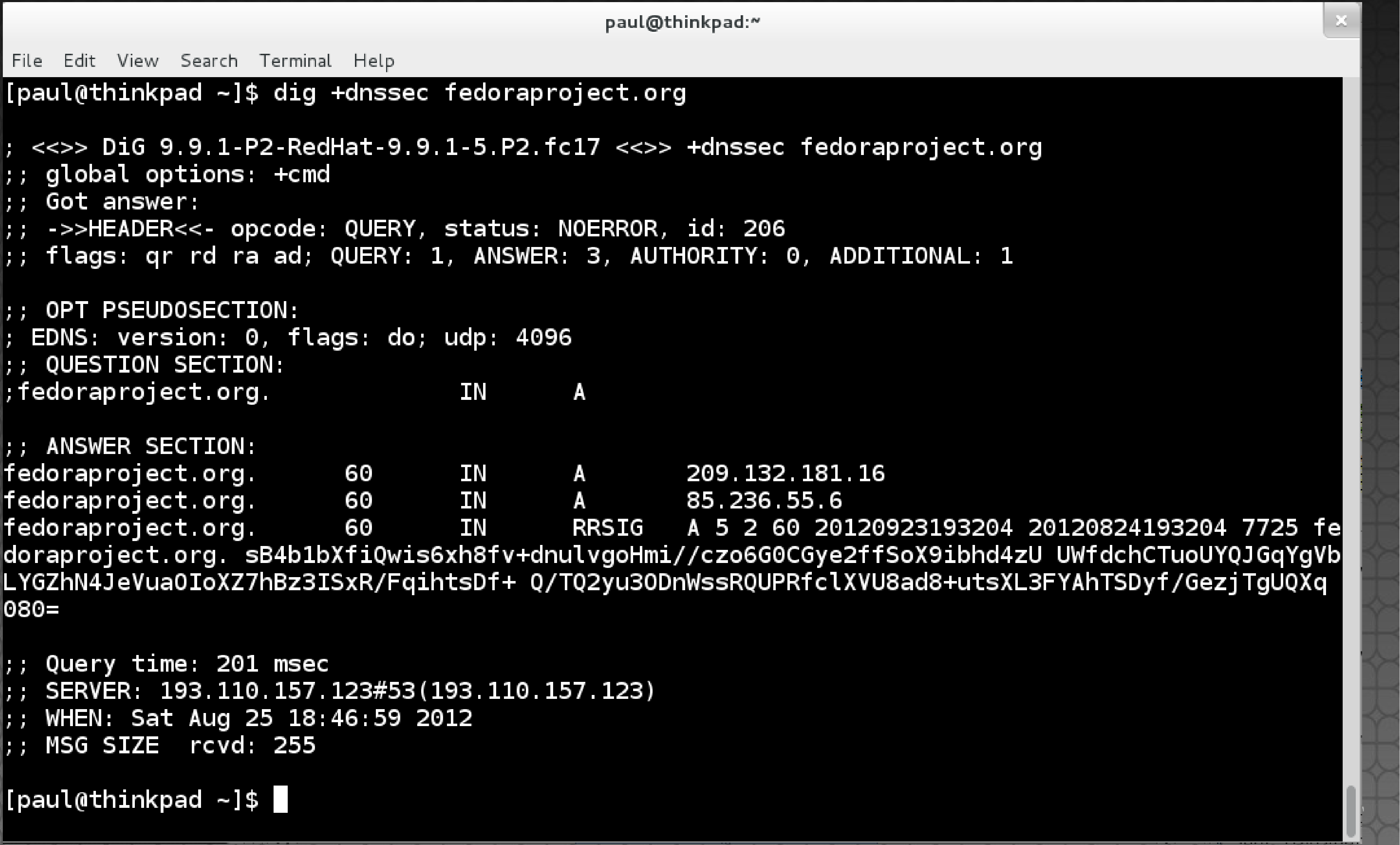
DNSSEC in 7 screen shots

Image a DNS RRset



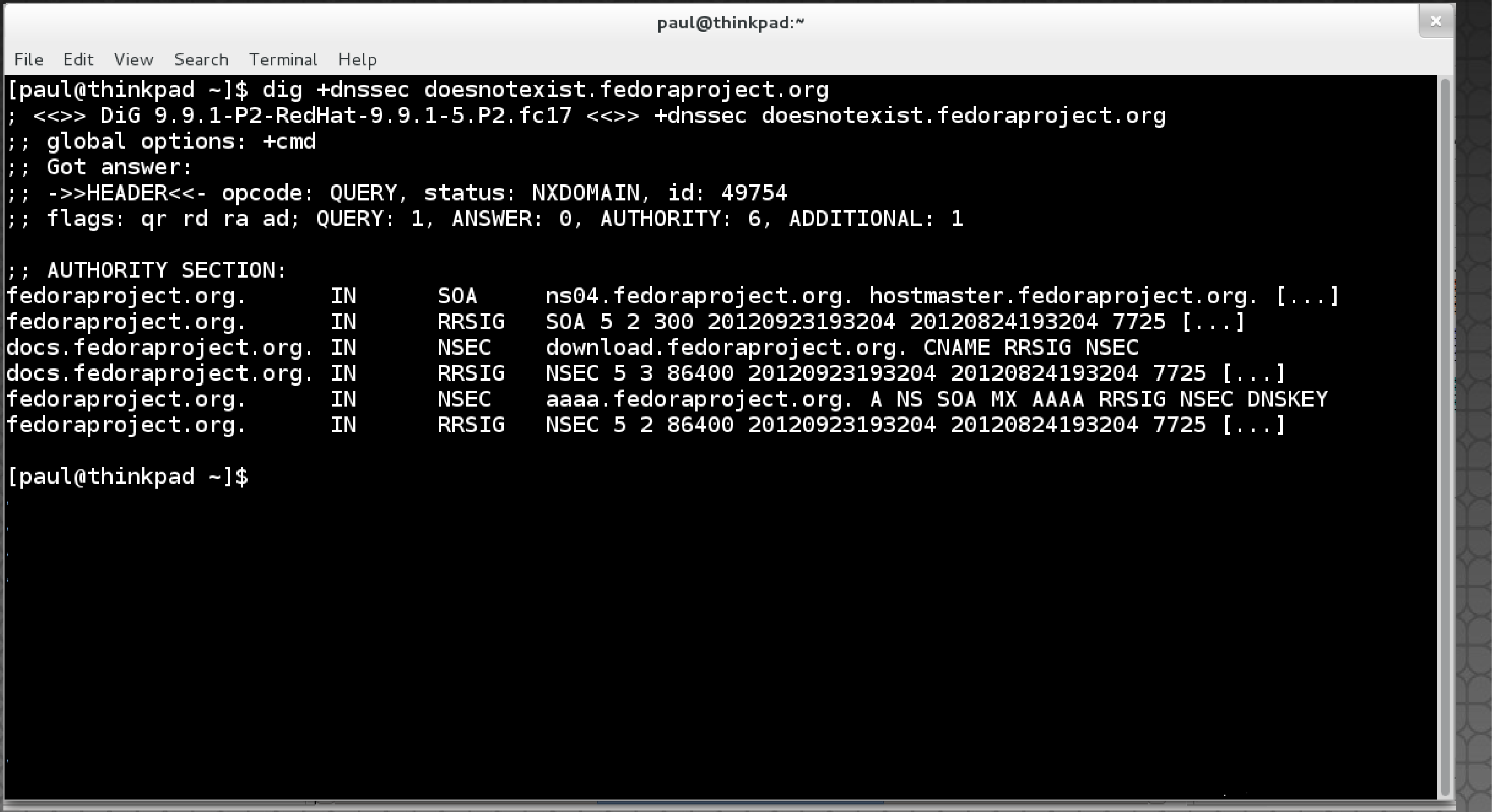
```
[paul@thinkpad ~]$ dig fedoraproject.org

; <<>> DiG 9.9.1-P2-RedHat-9.9.1-5.P2.fc17 <<>> fedoraproject.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61882
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;fedoraproject.org.             IN      A

;; ANSWER SECTION:
fedoraproject.org.      44      IN      A       209.132.181.16
fedoraproject.org.      44      IN      A       85.236.55.6

;; Query time: 95 msec
;; SERVER: 193.110.157.123#53(193.110.157.123)
;; WHEN: Sat Aug 25 18:46:02 2012
;; MSG SIZE  rcvd: 78

[paul@thinkpad ~]$
```

Add DNS signature record



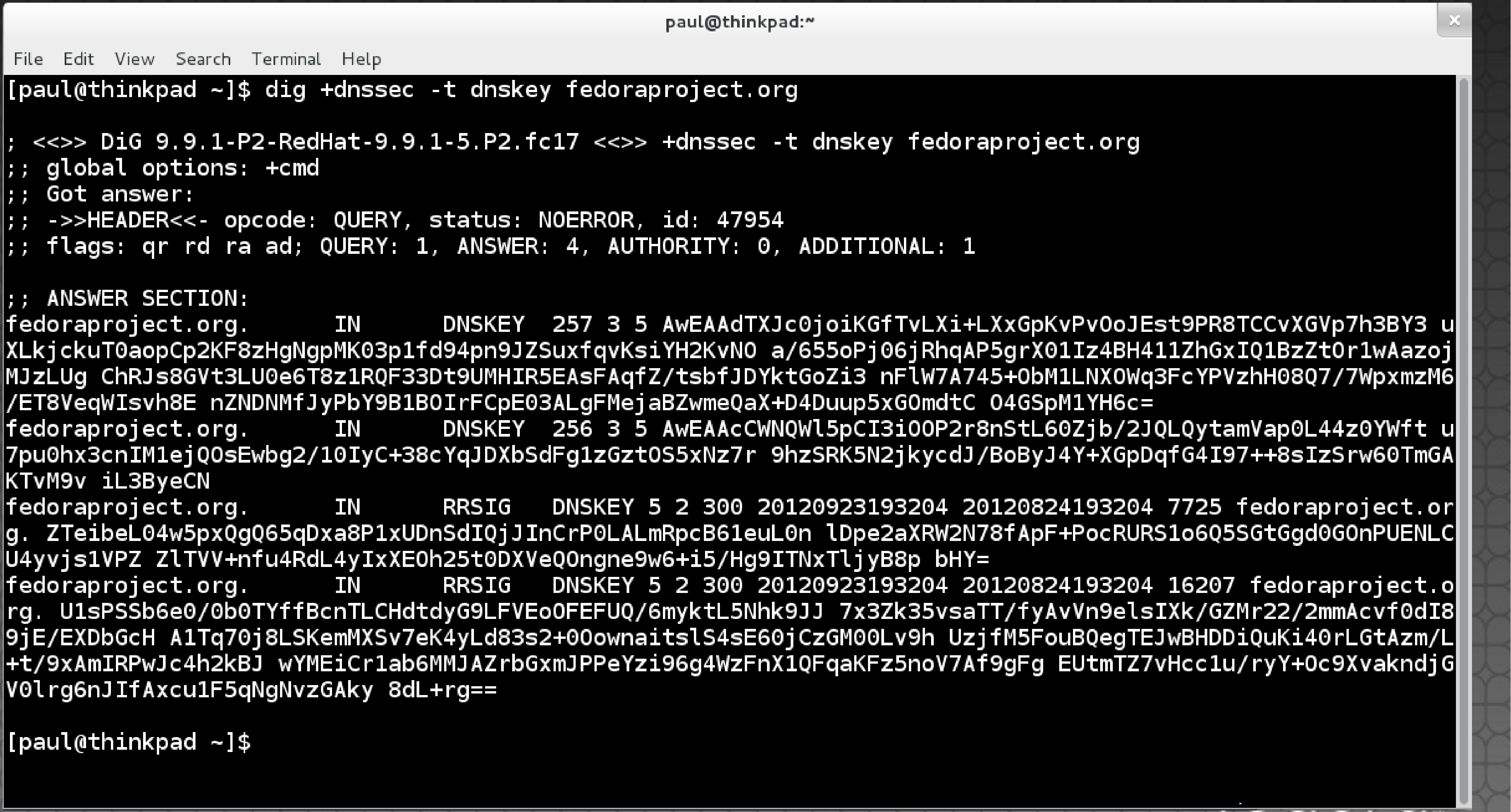
```
[paul@thinkpad ~]$ dig +dnssec fedoraproject.org

; <<>> DiG 9.9.1-P2-RedHat-9.9.1-5.P2.fc17 <<>> +dnssec fedoraproject.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 206
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
fedoraproject.org.      60      IN      A       209.132.181.16
fedoraproject.org.      60      IN      A       85.236.55.6
fedoraproject.org.      60      IN      RRSIG   A 5 2 60 20120923193204 20120824193204 7725 fe
doraproject.org. sB4b1bXfiQwis6xh8fv+dnulvgoHmi//czo6G0CGye2ffSoX9ibhd4zU UWfdchCTuoUYQJGqYgVb
LYGZhN4JeVuaOIoXZ7hBz3ISxR/FqihtsDf+ Q/TQ2yu3ODnWssRQUPRfclXVU8ad8+utsXL3FYAhTSDyf/GezjTgUQXq
080=

;; Query time: 201 msec
;; SERVER: 193.110.157.123#53(193.110.157.123)
;; WHEN: Sat Aug 25 18:46:59 2012
;; MSG SIZE  rcvd: 255

[paul@thinkpad ~]$ 
```

Also signature for NXDOMAIN



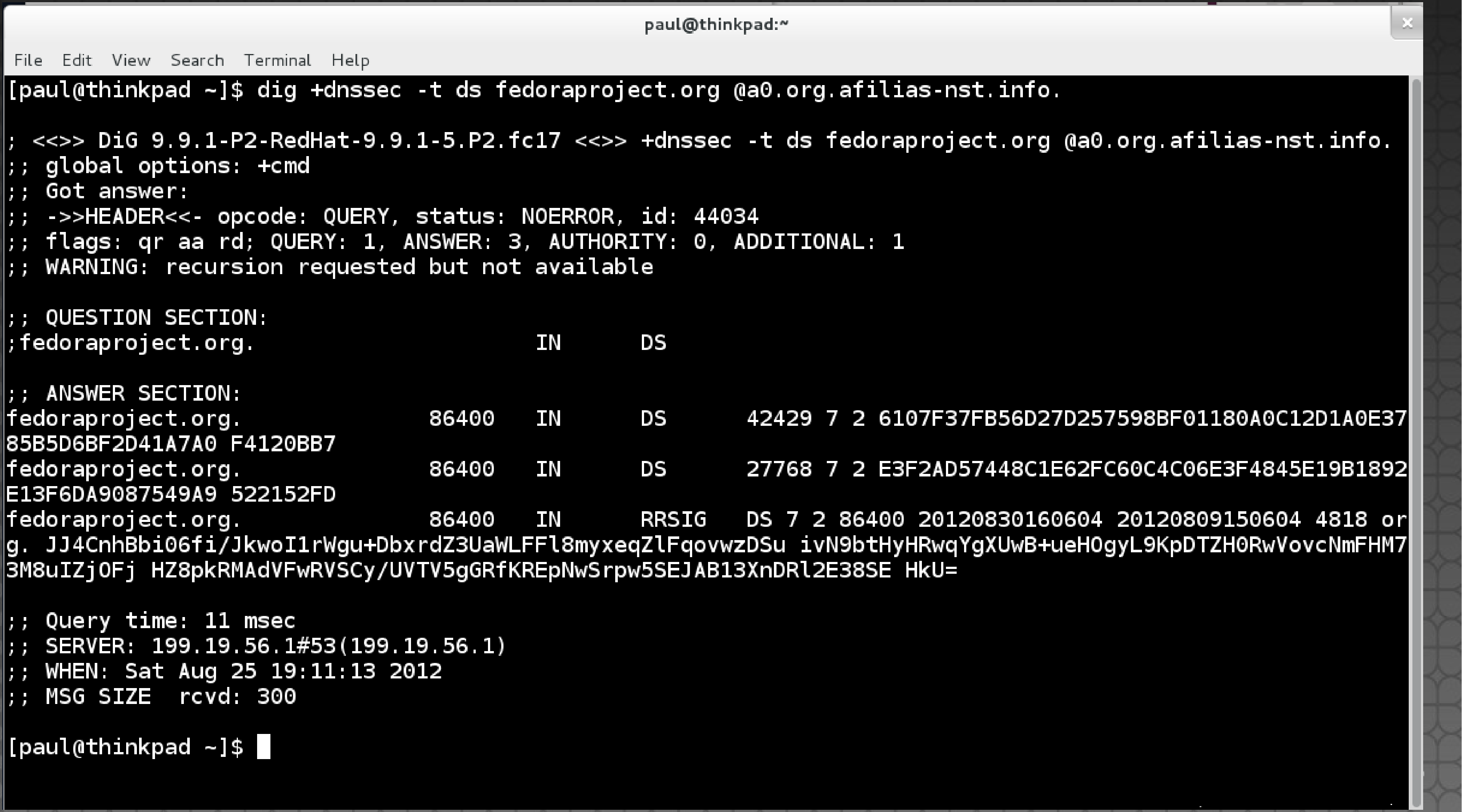
```
[paul@thinkpad ~]$ dig +dnssec doesnotexist.fedoraproject.org
; <<>> DiG 9.9.1-P2-RedHat-9.9.1-5.P2.fc17 <<>> +dnssec doesnotexist.fedoraproject.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 49754
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 6, ADDITIONAL: 1

;; AUTHORITY SECTION:
fedoraproject.org.      IN      SOA     ns04.fedoraproject.org. hostmaster.fedoraproject.org. [...]
fedoraproject.org.      IN      RRSIG   SOA 5 2 300 20120923193204 20120824193204 7725 [...]
docs.fedoraproject.org. IN      NSEC    download.fedoraproject.org. CNAME RRSIG NSEC
docs.fedoraproject.org. IN      RRSIG   NSEC 5 3 86400 20120923193204 20120824193204 7725 [...]
fedoraproject.org.      IN      NSEC    aaaa.fedoraproject.org. A NS SOA MX AAAA RRSIG NSEC DNSKEY
fedoraproject.org.      IN      RRSIG   NSEC 5 2 86400 20120923193204 20120824193204 7725 [...]

[paul@thinkpad ~]$
```

Publish the public key used in DNS



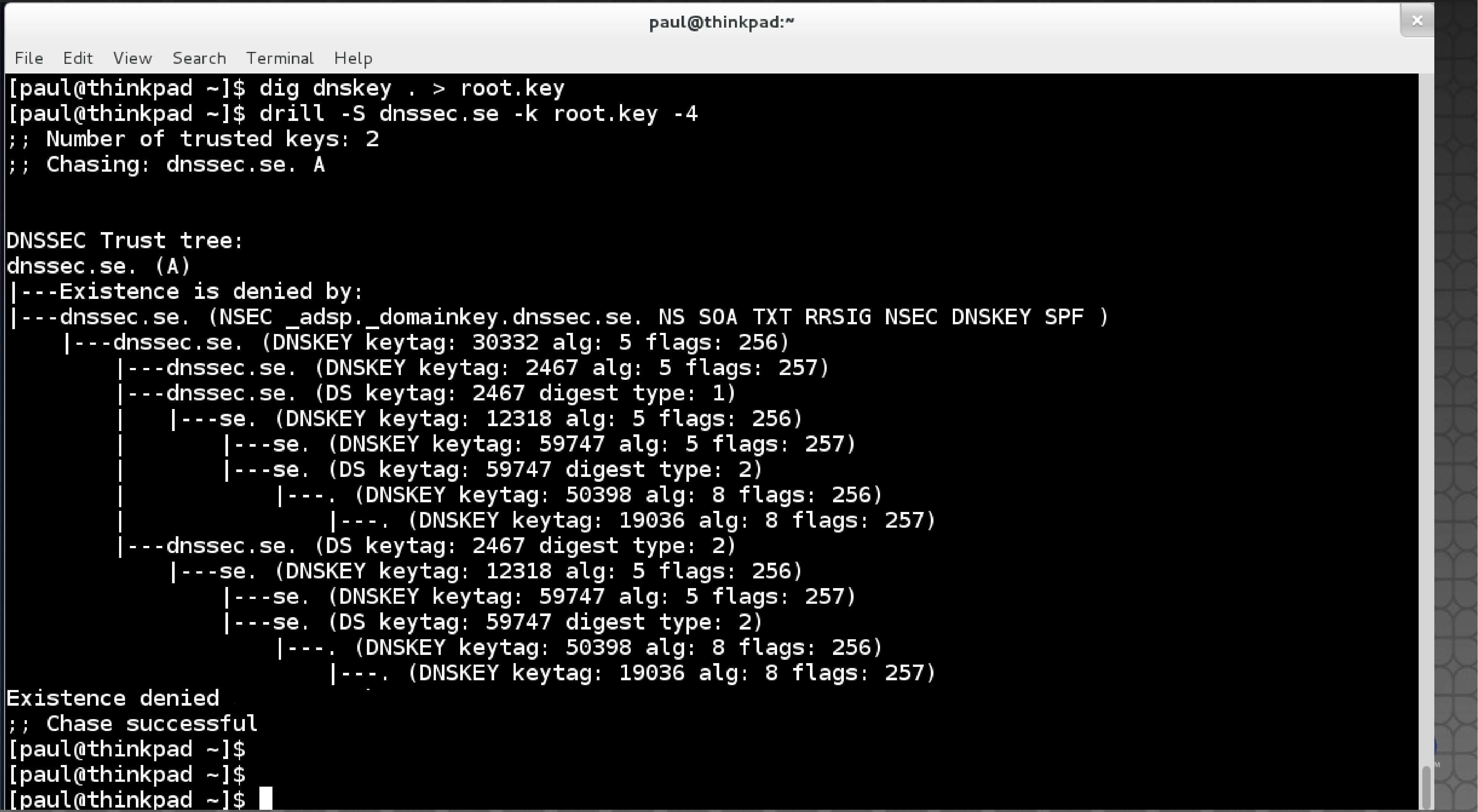
```
[paul@thinkpad ~]$ dig +dnssec -t dnskey fedoraproject.org

; <<>> DiG 9.9.1-P2-RedHat-9.9.1-5.P2.fc17 <<>> +dnssec -t dnskey fedoraproject.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47954
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; ANSWER SECTION:
fedoraproject.org.      IN      DNSKEY  257 3 5 AwEAAdTXJc0joiKGfTvLXi+LXxGpKvPvOoJEst9PR8TCCvXGVp7h3BY3 u
XLkjckuT0aopCp2KF8zHgNgpMK03p1fd94pn9JZSuxfqvKsiYH2KvNO a/655oPj06jRhqAP5grX01Iz4BH411ZhGxIQ1BzZtOr1wAazoj
MJzLUg ChRJs8GVt3LU0e6T8z1RQF33Dt9UMHIR5EAsFAqfZ/tsbfJDYktGoZi3 nFlW7A745+ObM1LNXOWq3FcYPVzhH08Q7/7WpxmzM6
/ET8VeqWIsvh8E nZNDNMfJyPbY9B1BOIrFCpE03ALgFMejaBZwmeQaX+D4Duup5xGOmdtC O4GSpM1YH6c=
fedoraproject.org.      IN      DNSKEY  256 3 5 AwEAAcCWNQWl5pCI3iOOP2r8nStL60Zjb/2JQLQytamVap0L44z0YWft u
7pu0hx3cnIM1ejQOsEwbg2/10IyC+38cYqJDXbSdFg1zGztOS5xNz7r 9hzSRK5N2jkycdJ/BoByJ4Y+XGpDqfG4I97++8sIzSrw60TmGA
KTvM9v iL3ByeCN
fedoraproject.org.      IN      RRSIG   DNSKEY 5 2 300 20120923193204 20120824193204 7725 fedoraproject.or
g. ZTeibeL04w5pxQgQ65qDxa8P1xUDnSdIQjJInCrP0LALmRpcB61euL0n lDpe2aXRW2N78fApF+PocRURS1o6Q5SGtGgd0GOnPUENLC
U4yvjs1VPZ ZlTVV+nfu4RdL4yIxXEOh25t0DXVeQOngne9w6+i5/Hg9ITNxTljyB8p bHY=
fedoraproject.org.      IN      RRSIG   DNSKEY 5 2 300 20120923193204 20120824193204 16207 fedoraproject.o
rg. U1sPSSb6e0/0b0TYffBcnTLCHdtdyG9LFVEoOFEFUQ/6myktL5Nhk9JJ 7x3Zk35vsaTT/fyAvVn9elsIXk/GZMr22/2mmAcvf0dI8
9jE/EXDbGcH A1Tq70j8LSKemMXSv7eK4yLd83s2+0OownaitslS4sE60jCzGM00Lv9h UzjfM5FouBQegTEJwBHDDiQuKi40rLGtAzm/L
+t/9xAmIRPwJc4h2kBJ wYMEiCr1ab6MMJAZrbGxmJPPeYzi96g4WzFnX1QFqaKFz5noV7Af9gFg EUtmTZ7vHcc1u/ryY+Oc9XvakndjG
V0lrg6nJIfAxcu1F5qNgNvzGAky 8dL+rg==

[paul@thinkpad ~]$
```

Hash of public key goes to parent



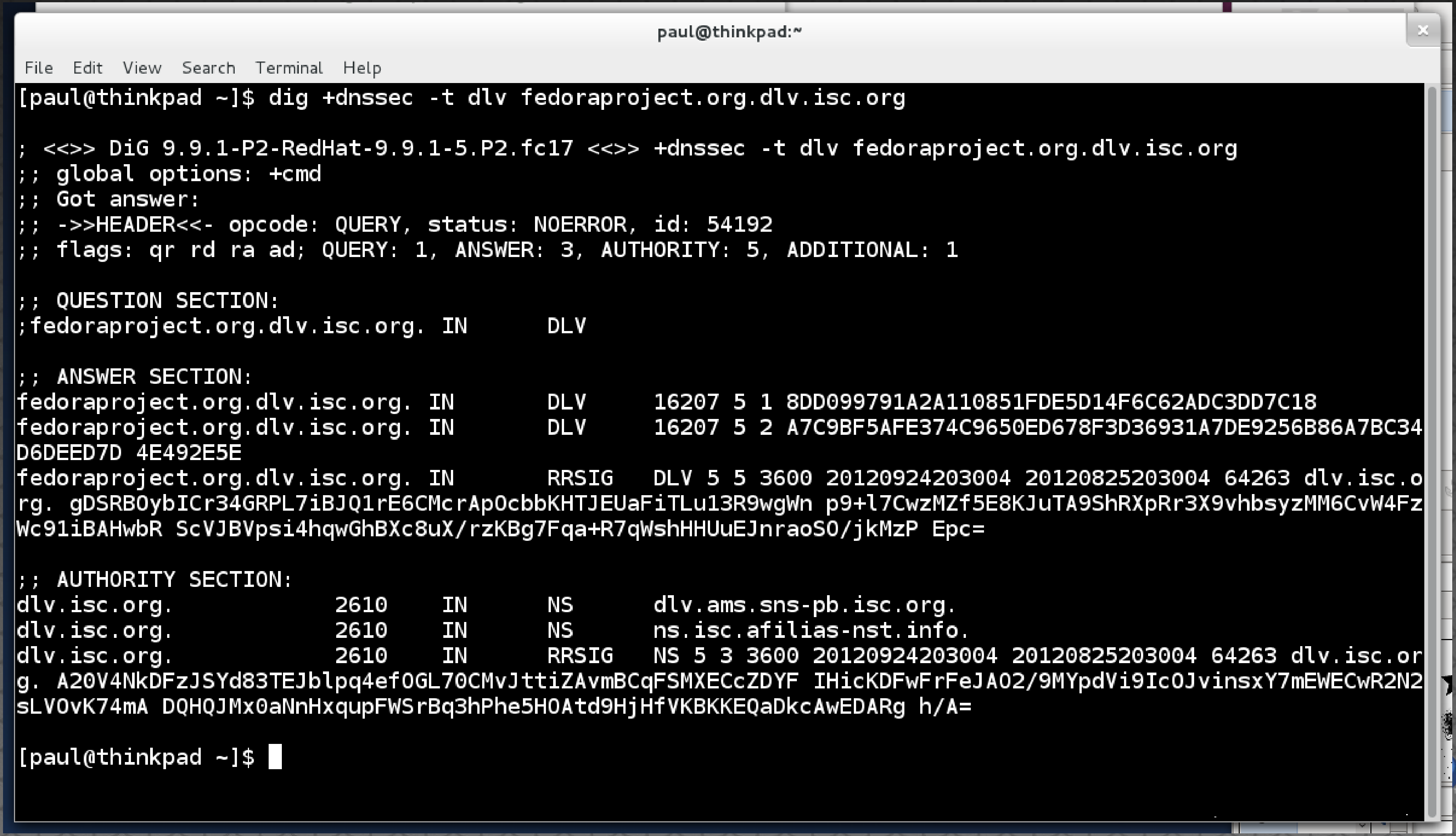
```
[paul@thinkpad ~]$ dig +dnssec -t ds fedoraproject.org @a0.org.afilias-nst.info.

; <<>> DiG 9.9.1-P2-RedHat-9.9.1-5.P2.fc17 <<>> +dnssec -t ds fedoraproject.org @a0.org.afilias-nst.info.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44034
;; flags: qr aa rd; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;fedoraproject.org.                     IN      DS

;; ANSWER SECTION:
fedoraproject.org.              86400   IN      DS      42429 7 2 6107F37FB56D27D257598BF01180A0C12D1A0E37
85B5D6BF2D41A7A0 F4120BB7
fedoraproject.org.              86400   IN      DS      27768 7 2 E3F2AD57448C1E62FC60C4C06E3F4845E19B1892
E13F6DA9087549A9 522152FD
fedoraproject.org.              86400   IN      RRSIG   DS 7 2 86400 20120830160604 20120809150604 4818 or
g. JJ4CnhBbi06fi/JkwoI1rWgu+DbxrdZ3UaWLFFl8myxeqZlFqovwzDSu ivN9btHyHRwqYgXUwB+ueHOgyL9KpDTZH0RwVovcNmFHM7
3M8uIZjOFj HZ8pkRMAdVFwRVSCy/UVTV5gGRfKREpNwSrpw5SEJAB13XnDRl2E38SE HkU=

;; Query time: 11 msec
;; SERVER: 199.19.56.1#53(199.19.56.1)
;; WHEN: Sat Aug 25 19:11:13 2012
;; MSG SIZE  rcvd: 300

[paul@thinkpad ~]$ █
```

Build DS -> DNSKEY trust chains



```
[paul@thinkpad ~]$ dig dnskey . > root.key
[paul@thinkpad ~]$ drill -S dnssec.se -k root.key -4
;; Number of trusted keys: 2
;; Chasing: dnssec.se. A


DNSSEC Trust tree:
dnssec.se. (A)
|---Existence is denied by:
|---dnssec.se. (NSEC _adsp._domainkey.dnssec.se. NS SOA TXT RRSIG NSEC DNSKEY SPF )
    |---dnssec.se. (DNSKEY keytag: 30332 alg: 5 flags: 256)
        |---dnssec.se. (DNSKEY keytag: 2467 alg: 5 flags: 257)
        |---dnssec.se. (DS keytag: 2467 digest type: 1)
        |   |---se. (DNSKEY keytag: 12318 alg: 5 flags: 256)
        |       |---se. (DNSKEY keytag: 59747 alg: 5 flags: 257)
        |       |---se. (DS keytag: 59747 digest type: 2)
        |           |---. (DNSKEY keytag: 50398 alg: 8 flags: 256)
        |               |---. (DNSKEY keytag: 19036 alg: 8 flags: 257)
        |---dnssec.se. (DS keytag: 2467 digest type: 2)
            |---se. (DNSKEY keytag: 12318 alg: 5 flags: 256)
                |---se. (DNSKEY keytag: 59747 alg: 5 flags: 257)
                |---se. (DS keytag: 59747 digest type: 2)
                    |---. (DNSKEY keytag: 50398 alg: 8 flags: 256)
                        |---. (DNSKEY keytag: 19036 alg: 8 flags: 257)
Existence denied
;; Chase successful
[paul@thinkpad ~]$
[paul@thinkpad ~]$
[paul@thinkpad ~]$
```

DNSSEC Lookaside Verification



```
[paul@thinkpad ~]$ dig +dnssec -t dlv fedoraproject.org.dlv.isc.org

; <<>> DiG 9.9.1-P2-RedHat-9.9.1-5.P2.fc17 <<>> +dnssec -t dlv fedoraproject.org.dlv.isc.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54192
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 3, AUTHORITY: 5, ADDITIONAL: 1

;; QUESTION SECTION:
;fedoraproject.org.dlv.isc.org. IN      DLV

;; ANSWER SECTION:
fedoraproject.org.dlv.isc.org. IN       DLV     16207 5 1 8DD099791A2A110851FDE5D14F6C62ADC3DD7C18
fedoraproject.org.dlv.isc.org. IN       DLV     16207 5 2 A7C9BF5AFE374C9650ED678F3D36931A7DE9256B86A7BC34
D6DEED7D 4E492E5E
fedoraproject.org.dlv.isc.org. IN       RRSIG   DLV 5 5 3600 20120924203004 20120825203004 64263 dlv.isc.o
rg. gDSRBOybICr34GRPL7iBJQ1rE6CMcrApOcbbKHTJEUaFiTLu13R9wgWn p9+l7CwzMZf5E8KJuTA9ShRXpRr3X9vhbsyzMM6CvW4Fz
Wc91iBAHwbR ScVJBVpsi4hqwGhBXc8uX/rzKBg7Fqa+R7qWshHHUuEJnraoSO/jkMzP Epc=

;; AUTHORITY SECTION:
dlv.isc.org.            2610    IN      NS      dlv.ams.sns-pb.isc.org.
dlv.isc.org.            2610    IN      NS      ns.isc.afilias-nst.info.
dlv.isc.org.            2610    IN      RRSIG   NS 5 3 3600 20120924203004 20120825203004 64263 dlv.isc.or
g. A20V4NkDFzJSYd83TEJblpq4efOGL70CMvJttiZAvmBCqFSMXECcZDYF IHicKDFwFrFeJAO2/9MYpdVi9IcOJvinsxY7mEWECwR2N2
sLVOvK74mA DQHQJMx0aNnHxqupFWSrBq3hPhe5HOAtd9HjHfVKBKKEQaDkcAwEDARg h/A=

[paul@thinkpad ~]$ █
```

DNSSEC states and bits

- Secure: validated from known trust anchor key
- Insecure: proven no trust anchor exists there
- Bogus: crypto failed,answer scrubbed (ServFail)
- Indeterminate: answers incomplete/missing

- Query using “dig +dnssec”
- Check dig output for “AD” - Authenticated Data
- Debug ServFail's using “dig +cd +dnssec”

DNSSEC in Linux distro's

- DNSSEC capable DNS resolvers
  - unbound (preferred for on the fly reconfiguration)
  - bind (named)
- DNSSEC capable DNS servers
  - All modern DNS servers (bind, nsd, powerdns)
- DNSSEC zone signers
  - opendnssec, dnssec-signzone (bind), pdns, dnssec-tools, ...
- DNSSEC utilities (dig, unbound-host, drill,..)
  - yum/apt-cache search dnssec

DNSSEC validation in Fedora / RHEL

- yum install unbound or yum install bind
- echo “nameserver 127.0.0.1” > /etc/resolv.conf
- No further configuration needed, DNSSEC enabled in default configuration since Fedora 15
- Don't actually do this on your laptop, as you depend on spoofed DNS every day!

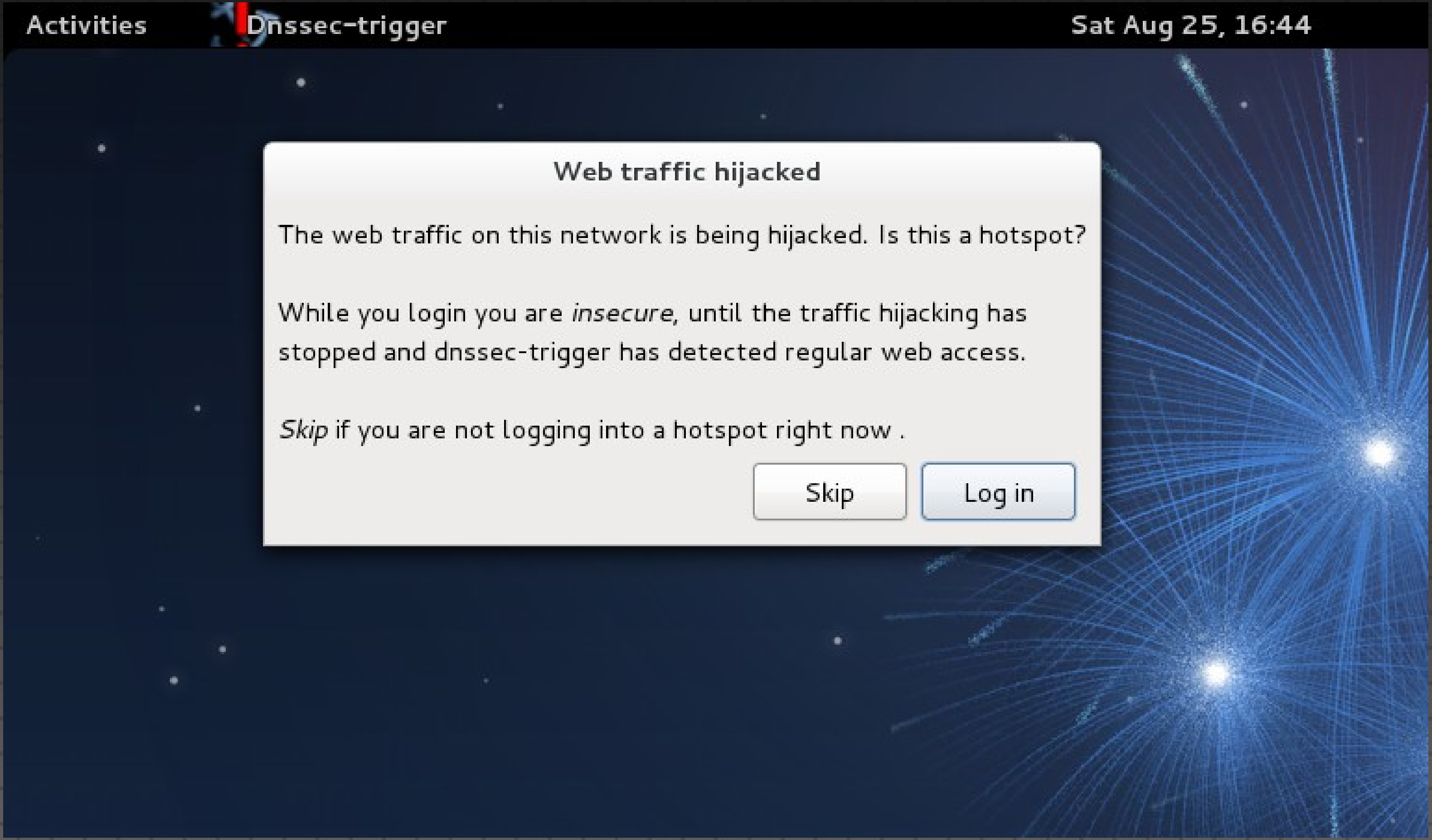
DNSSEC resolving issues

- DNSSEC too good – protects against
  - hotspot / captive portal
  - VPN – private views
  - opendns, NXDOMAIN squatting, dns rewriting
- Many applications mess with /etc/resolv.conf
- We need to address these issues all at once

DNSSEC and hotspots

- NetworkManager, unbound, dnssec-triggerd
- Run DNSSEC server locally: unbound
- dnssec-triggerd with NM hook to:
  - Detect hotspot via http://fp.org/static/hotspot.txt
  - use resolv.conf to temporarily bypass unbound
  - Launch browser to hotspot-nocache.fp.org
  - Detect payment / license agreement
  - Re-enable DNSSEC using unbound via resolv.conf

Hotspot detected



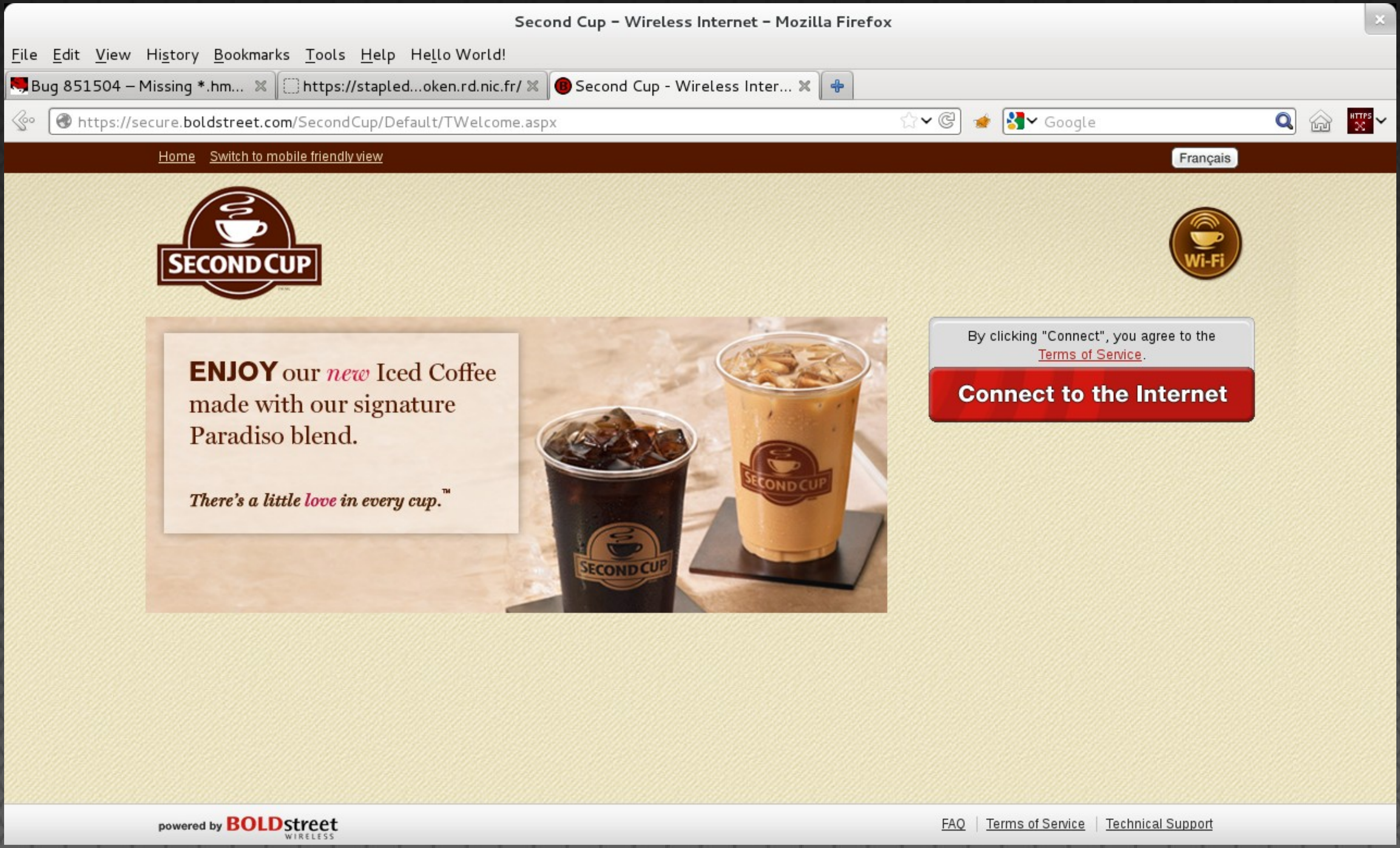
Web traffic hijacked

The web traffic on this network is being hijacked. Is this a hotspot?

While you login you are *insecure*, until the traffic hijacking has stopped and dnssec-trigger has detected regular web access.

Skip if you are not logging into a hotspot right now .

Login to hotspot



Second Cup – Wireless Internet – Mozilla Firefox

https://secure.boldstreet.com/SecondCup/Default/TWelcome.aspx

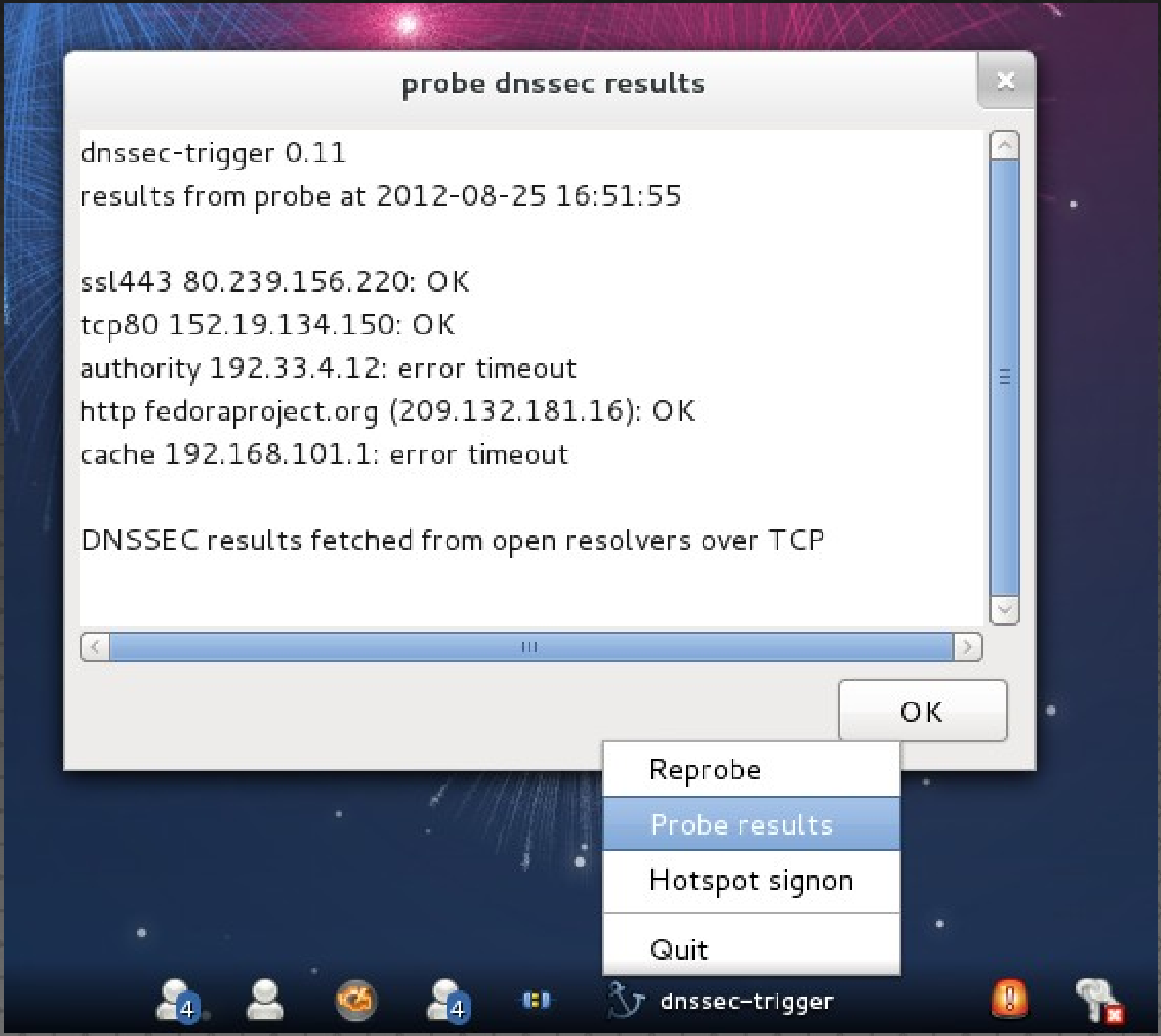
ENJOY our *new* Iced Coffee made with our signature Paradiso blend.

There's a little love in every cup.™

By clicking "Connect", you agree to the Terms of Service.

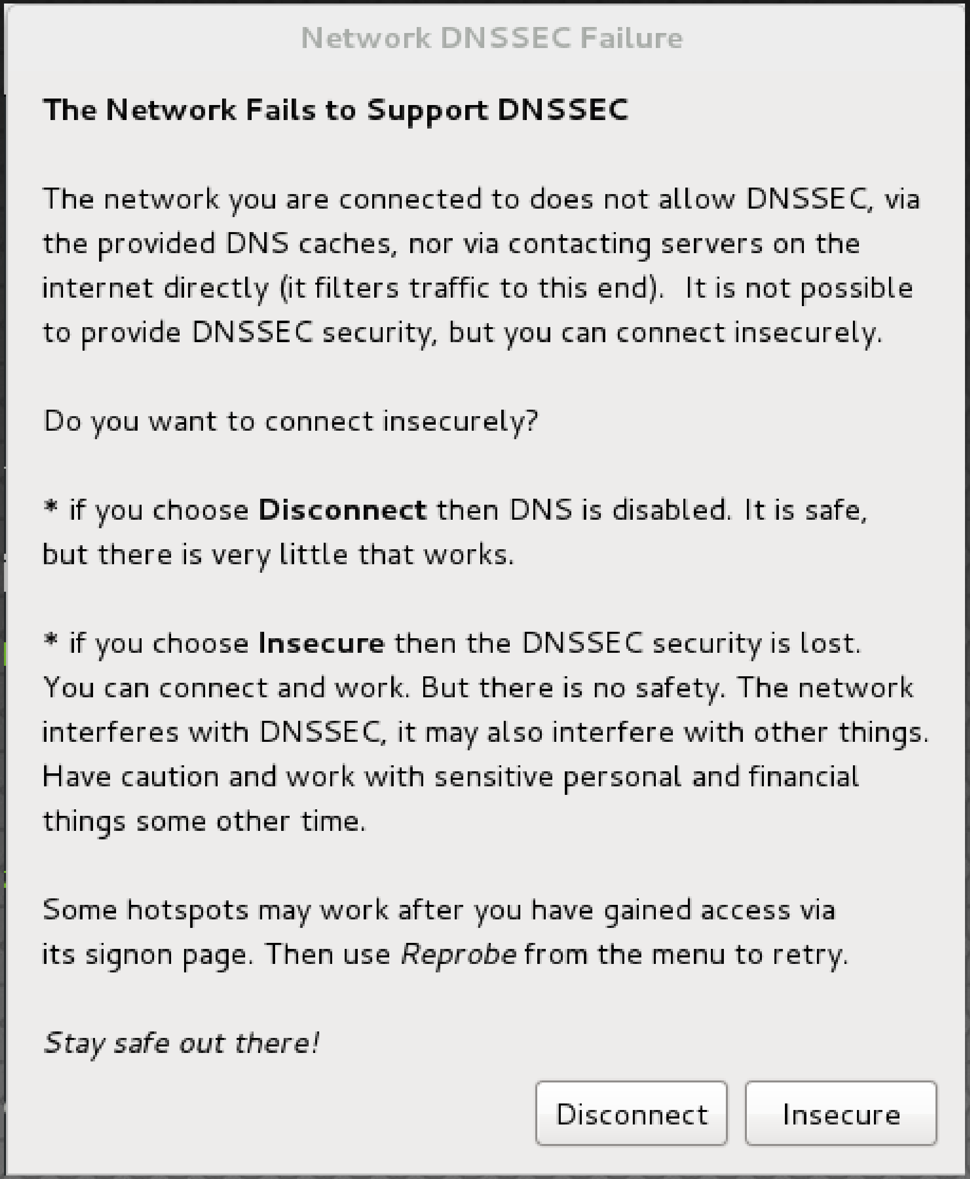
File
Edit
View
History
Bookmarks
Tools
Help
Hello World!
Bug 851504 – Missing *.hm...
https://stapled...oken.rd.nic.fr/
Second Cup - Wireless Inter...
Google
Home
Switch to mobile friendly view
Français
SECOND CUP
Wi-Fi
Connect to the Internet
powered by BOLDstreet WIRELESS
FAQ
Terms of Service
Technical Support

Fallback to DNS over TCP



```
dnssec-trigger 0.11
results from probe at 2012-08-25 16:51:55

ssl443 80.239.156.220: OK
tcp80 152.19.134.150: OK
authority 192.33.4.12: error timeout
http fedoraproject.org (209.132.181.16): OK
cache 192.168.101.1: error timeout

DNSSEC results fetched from open resolvers over TCP
```

Or worse: cache-only



The Network Fails to Support DNSSEC

The network you are connected to does not allow DNSSEC, via the provided DNS caches, nor via contacting servers on the internet directly (it filters traffic to this end). It is not possible to provide DNSSEC security, but you can connect insecurely.

Do you want to connect insecurely?

* if you choose **Disconnect** then DNS is disabled. It is safe, but there is very little that works.

* if you choose **Insecure** then the DNSSEC security is lost. You can connect and work. But there is no safety. The network interferes with DNSSEC, it may also interfere with other things. Have caution and work with sensitive personal and financial things some other time.

Some hotspots may work after you have gained access via its signon page. Then use *Reprobe* from the menu to retry.

Stay safe out there!

DNSSEC and VPNs

- Openswan reconfigures unbound on the fly
  - IPsec server sends XAUTH domain name and name server parameters to openswan client (i.e. “redhat.com”, 10.11.255.156)
  - Openswan informs unbound: “unbound-control forward_add redhat.com 10.11.255.156”
  - On termination, openswan issues “unbound-control forward_remove redhat.com” and “unbound-control flush_requestlist”

DNSSEC zone signing

- yum install opendnssec -y
- systemctl ods-enforcerd start
- systemctl ods-signerd start
- ods-ksmutil zone --add yourzone.com --input /var/named/yourzone.com --output /var/named/yourzone.com.signed
- ods-signer sign yourzone.zome
(updated named.conf, restart named, wait a few days, go to Registrar for DS, or dlv.isc.org to publish DLV)
- ods-ksmutil key ds-seen --zone yourzone.com \
    --keytag xxxxx

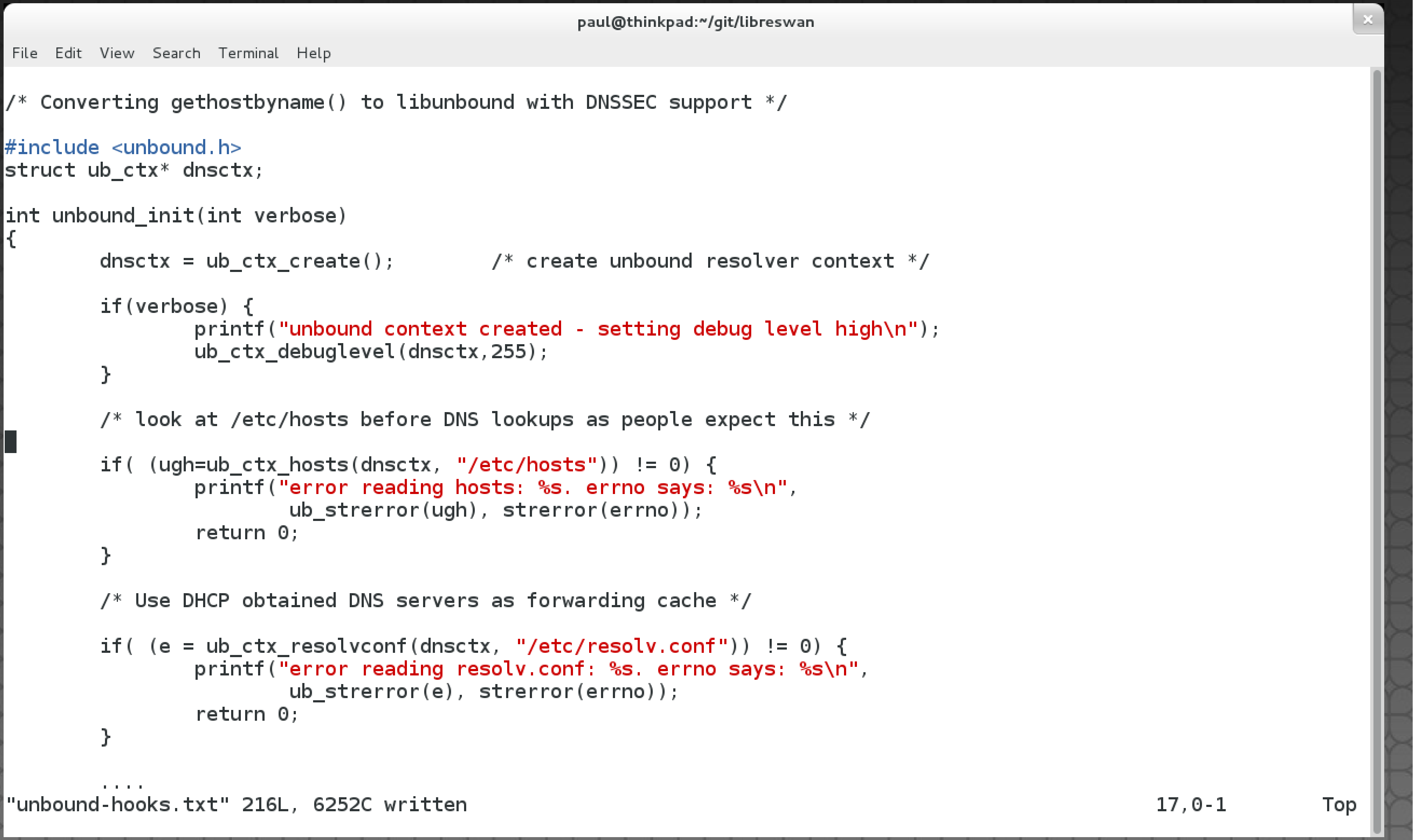
Convert code to use DNSSEC

- We will use libunbound as our API
- Find gethostbyname() calls (direct / indirect)

- Initialize a DNSSEC cache context
- Configure its behaviour to emulate POSIX
- Load DNSSEC trust anchor keys (root, DLV)

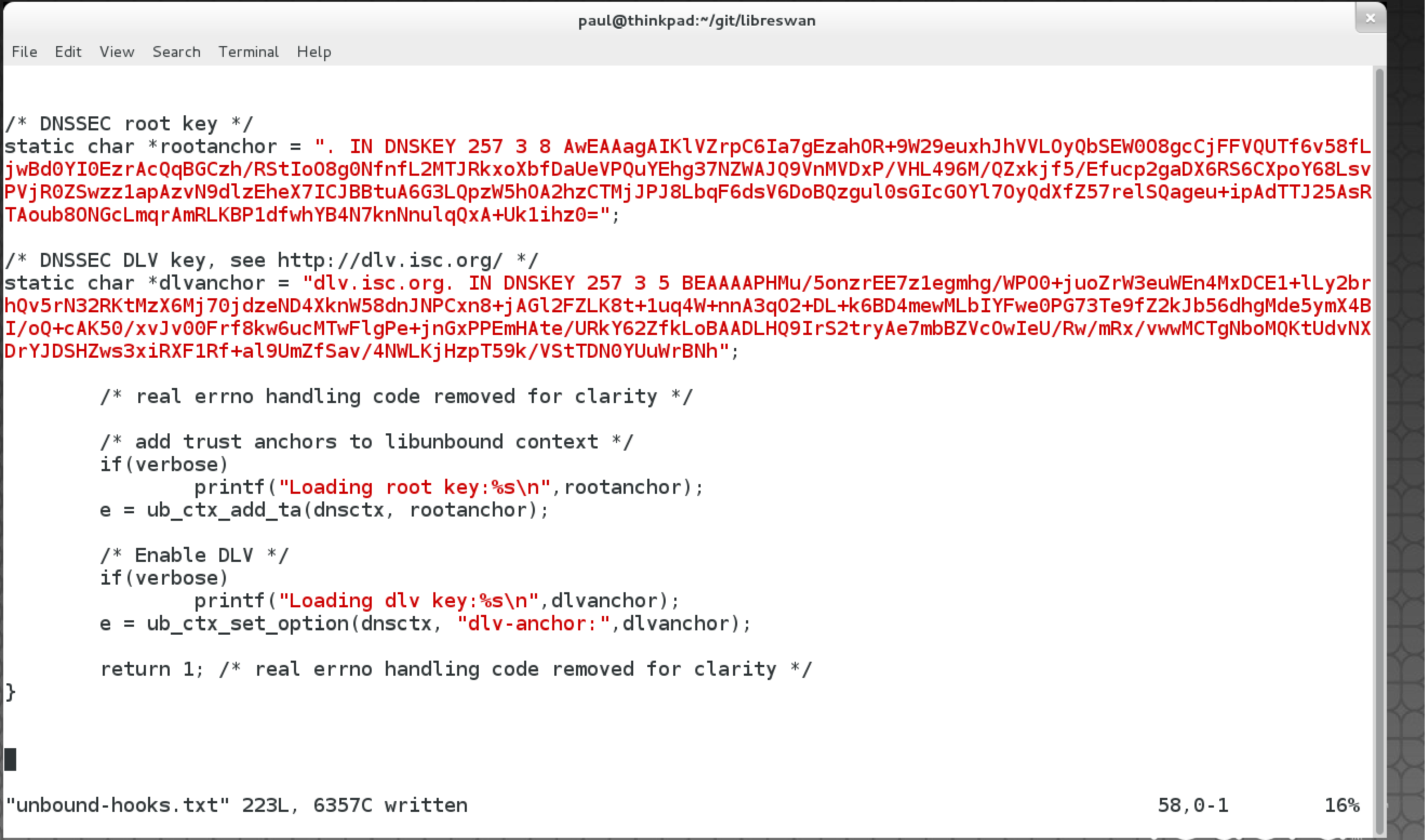
- Call ub_resolv() directly or via thread / callback
- Check return value for DNSSEC parameters

Code: initialize libunbound


paul@thinkpad:~/git/libreswan
File Edit View Search Terminal Help

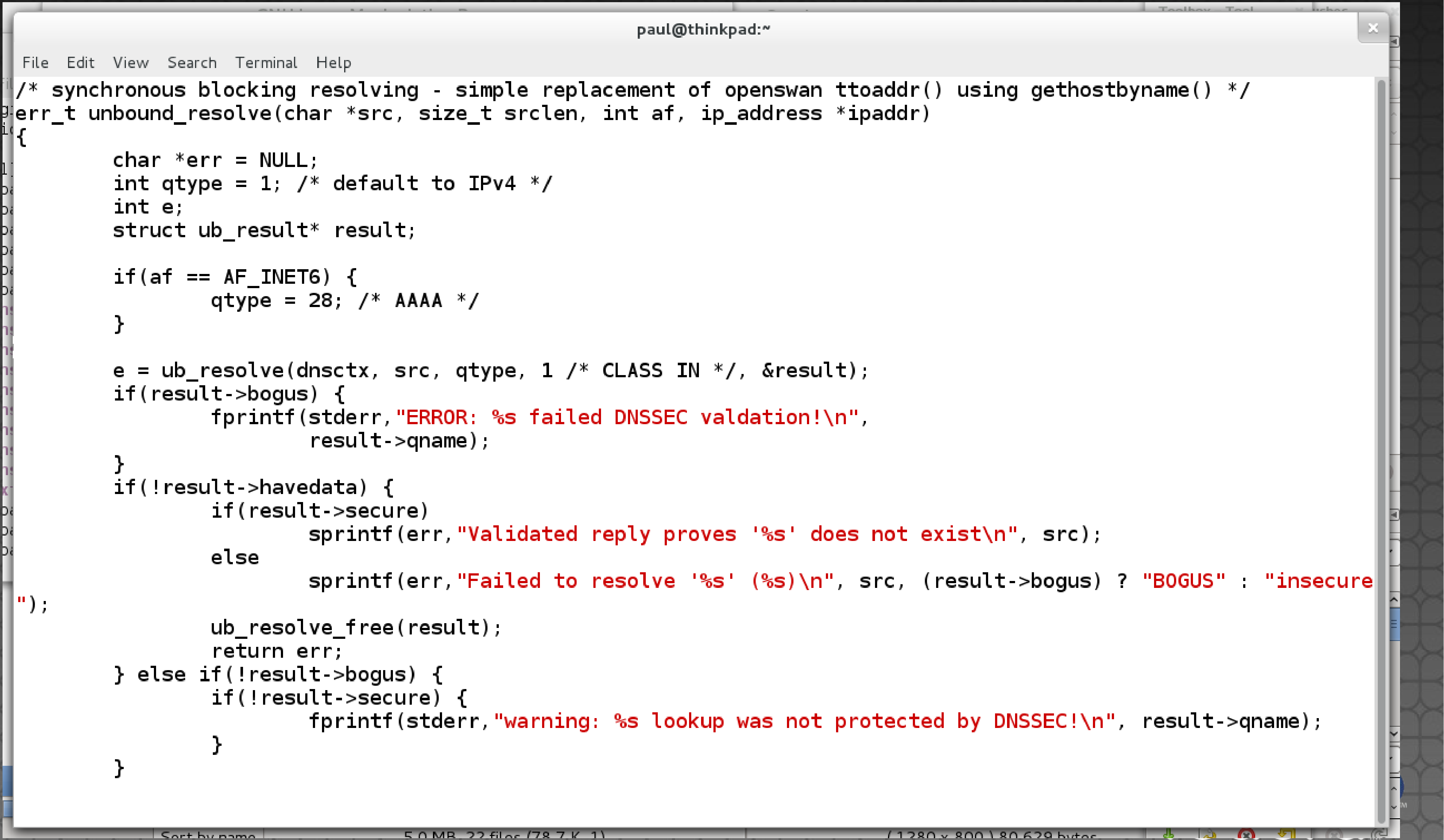
```
/* Converting gethostbyname() to libunbound with DNSSEC support */

#include <unbound.h>
struct ub_ctx* dnsctx;

int unbound_init(int verbose)
{
        dnsctx = ub_ctx_create();        /* create unbound resolver context */

        if(verbose) {
                printf("unbound context created - setting debug level high\n");
                ub_ctx_debuglevel(dnsctx,255);
        }

        /* look at /etc/hosts before DNS lookups as people expect this */

        if( (ugh=ub_ctx_hosts(dnsctx, "/etc/hosts")) != 0) {
                printf("error reading hosts: %s. errno says: %s\n",
                        ub_strerror(ugh), strerror(errno));
                return 0;
        }

        /* Use DHCP obtained DNS servers as forwarding cache */

        if( (e = ub_ctx_resolvconf(dnsctx, "/etc/resolv.conf")) != 0) {
                printf("error reading resolv.conf: %s. errno says: %s\n",
                        ub_strerror(e), strerror(errno));
                return 0;
        }

        ....
"unbound-hooks.txt" 216L, 6252C written                                                          17,0-1        Top
```

Add trusted DNSSEC keys


paul@thinkpad:~/git/libreswan
File Edit View Search Terminal Help

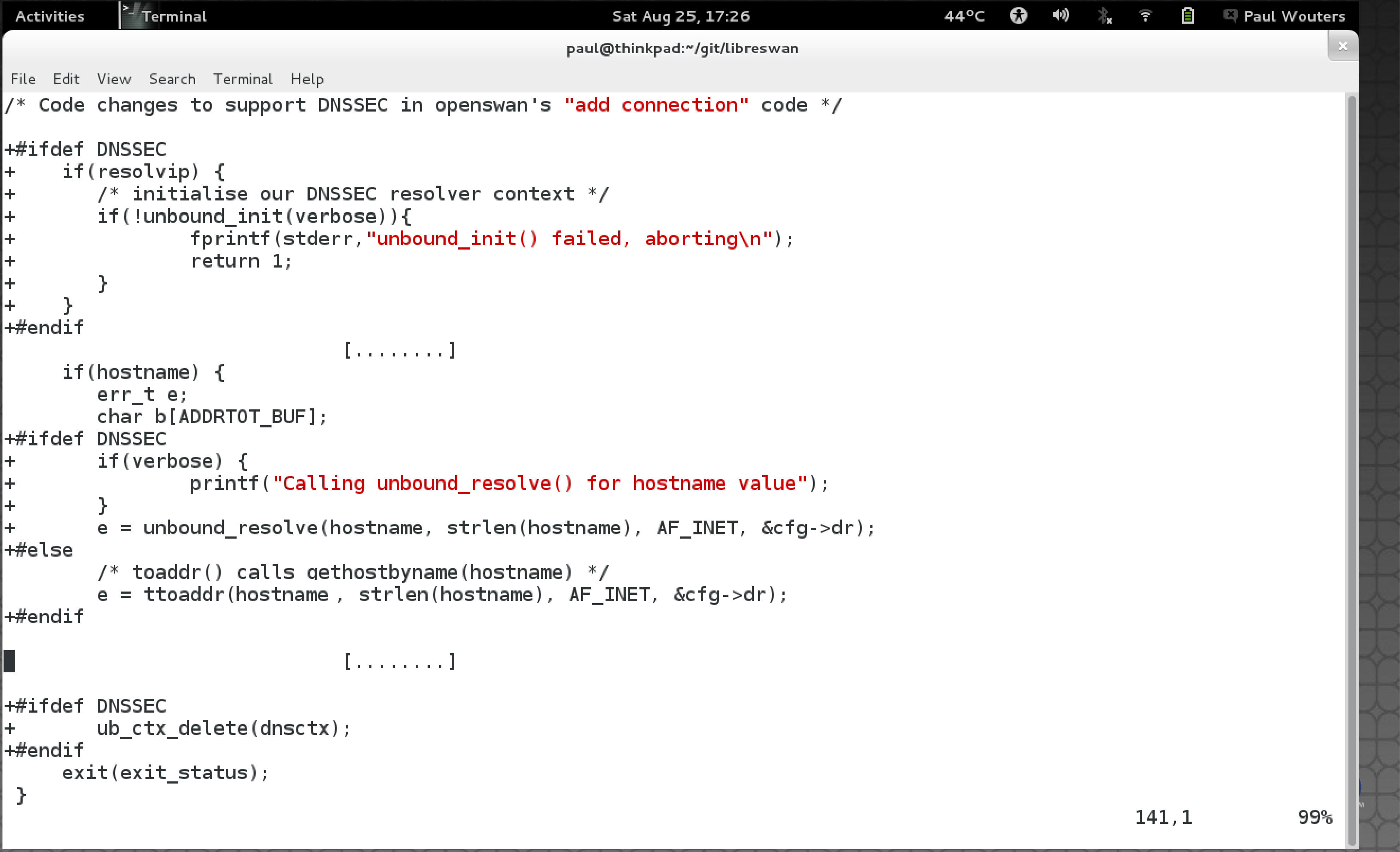
```
/* DNSSEC root key */
static char *rootanchor = ". IN DNSKEY 257 3 8 AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLOyQbSEW0O8gcCjFFVQUTf6v58fL
jwBd0YI0EzrAcQqBGCzh/RStIoO8g0NfnfL2MTJRkxoXbfDaUeVPQuYEhg37NZWAJQ9VnMVDxP/VHL496M/QZxkjf5/Efucp2gaDX6RS6CXpoY68Lsv
PVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LQpzW5hOA2hzCTMjJPJ8LbqF6dsV6DoBQzgul0sGIcGOYl7OyQdXfZ57relSQageu+ipAdTTJ25AsR
TAoub8ONGcLmqrAmRLKBP1dfwhYB4N7knNnulqQxA+Uk1ihz0=";

/* DNSSEC DLV key, see http://dlv.isc.org/ */
static char *dlvanchor = "dlv.isc.org. IN DNSKEY 257 3 5 BEAAAAPHMu/5onzrEE7z1egmhg/WPO0+juoZrW3euWEn4MxDCE1+lLy2br
hQv5rN32RKtMzX6Mj70jdzeND4XknW58dnJNPCxn8+jAGl2FZLK8t+1uq4W+nnA3qO2+DL+k6BD4mewMLbIYFwe0PG73Te9fZ2kJb56dhgMde5ymX4B
I/oQ+cAK50/xvJv00Frf8kw6ucMTwFlgPe+jnGxPPEmHAte/URkY62ZfkLoBAADLHQ9IrS2tryAe7mbBZVc0wIeU/Rw/mRx/vwwMCTgNboMQKtUdvNX
DrYJDSHZws3xiRXF1Rf+al9UmZfSav/4NWLKjHzpT59k/VStTDN0YUuWrBNh";

        /* real errno handling code removed for clarity */

        /* add trust anchors to libunbound context */
        if(verbose)
                printf("Loading root key:%s\n",rootanchor);
        e = ub_ctx_add_ta(dnsctx, rootanchor);

        /* Enable DLV */
        if(verbose)
                printf("Loading dlv key:%s\n",dlvanchor);
        e = ub_ctx_set_option(dnsctx, "dlv-anchor:",dlvanchor);

        return 1; /* real errno handling code removed for clarity */
}


"unbound-hooks.txt" 223L, 6357C written                                                        58,0-1        16%
```

Add DNSSEC resolve call



```
/* synchronous blocking resolving - simple replacement of openswan ttoaddr() using gethostbyname() */
err_t unbound_resolve(char *src, size_t srclen, int af, ip_address *ipaddr)
{
        char *err = NULL;
        int qtype = 1; /* default to IPv4 */
        int e;
        struct ub_result* result;

        if(af == AF_INET6) {
                qtype = 28; /* AAAA */
        }

        e = ub_resolve(dnsctx, src, qtype, 1 /* CLASS IN */, &result);
        if(result->bogus) {
                fprintf(stderr,"ERROR: %s failed DNSSEC valdation!\n",
                        result->qname);
        }
        if(!result->havedata) {
                if(result->secure)
                        sprintf(err,"Validated reply proves '%s' does not exist\n", src);
                else
                        sprintf(err,"Failed to resolve '%s' (%s)\n", src, (result->bogus) ? "BOGUS" : "insecure
");
                ub_resolve_free(result);
                return err;
        } else if(!result->bogus) {
                if(!result->secure) {
                        fprintf(stderr,"warning: %s lookup was not protected by DNSSEC!\n", result->qname);
                }
        }
```

replace gethostbyname()



```
/* Code changes to support DNSSEC in openswan's "add connection" code */

+#ifdef DNSSEC
+    if(resolvip) {
+       /* initialise our DNSSEC resolver context */
+       if(!unbound_init(verbose)){
+               fprintf(stderr,"unbound_init() failed, aborting\n");
+               return 1;
+       }
+    }
+#endif
                             [........]
     if(hostname) {
        err_t e;
        char b[ADDRTOT_BUF];
+#ifdef DNSSEC
+       if(verbose) {
+               printf("Calling unbound_resolve() for hostname value");
+       }
+       e = unbound_resolve(hostname, strlen(hostname), AF_INET, &cfg->dr);
+#else
        /* toaddr() calls gethostbyname(hostname) */
        e = ttoaddr(hostname , strlen(hostname), AF_INET, &cfg->dr);
+#endif

                             [........]

+#ifdef DNSSEC
+       ub_ctx_delete(dnsctx);
+#endif
     exit(exit_status);
 }
                                                                                                    141,1         99%
```

Achievement unlocked!

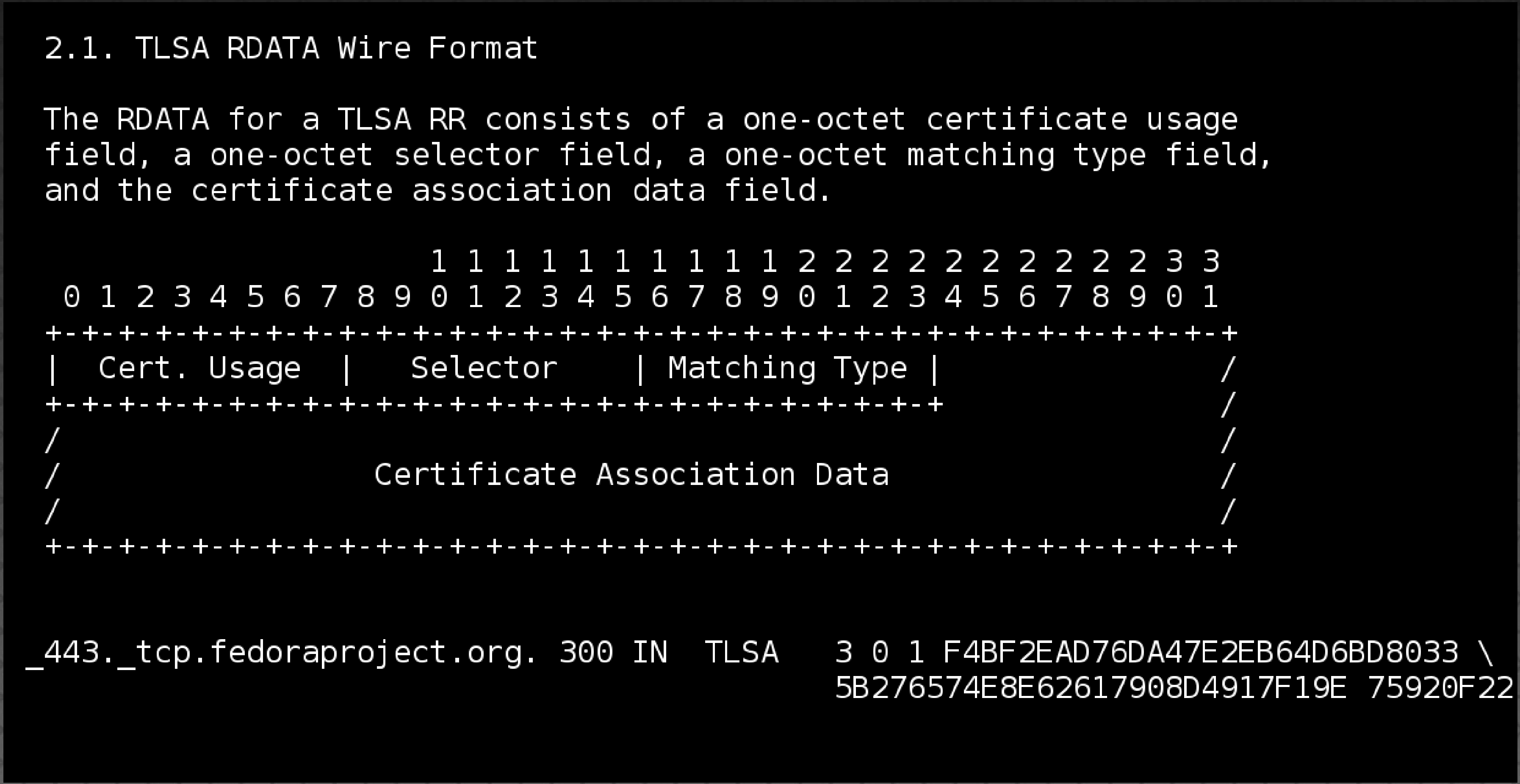
- Your zone is continuously signed and updated
- Your resolvers are deployed with DNSSEC
- You can handle necessary spoofed data from VPN and hotspots
- Your application is DNSSEC aware and protects against DNS spoofing and cache poisoning
- You can now use DNSSEC to securely publish **your own data**

non-DNS data use of DNSSEC

- TLSA – Store HTTPS certificates in DNS
- SSHFP – Store ssh known_hosts keys in DNS
- IPSECKEY – Store IPsec public RSA keys in DNS
- S/MIME – Store email public keys in DNS
- SMTP/TLSA – STARTSSL public keys in DNS

(first three are already described in RFCs, the last two are currently still drafts)

The TLSA record



```
 2.1. TLSA RDATA Wire Format

 The RDATA for a TLSA RR consists of a one-octet certificate usage
 field, a one-octet selector field, a one-octet matching type field,
 and the certificate association data field.

                      1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 2 3 3
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |  Cert. Usage  |   Selector    | Matching Type |               /
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+               /
 /                                                               /
 /                 Certificate Association Data                  /
 /                                                               /
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+


_443._tcp.fedoraproject.org. 300 IN  TLSA   3 0 1 F4BF2EAD76DA47E2EB64D6BD8033 \
                                            5B276574E8E62617908D4917F19E  75920F22
```

Other data suggestions

- PGP/GPG fingerprints in DNS ?
- OTR (IM) fingerprints in DNS ?
- File hashes in DNS ? (rpm, tripwire, IMA/EVM)
- SElinux policies via DNS ?
- Software Update Versions in DNS ?
- Distributed secure twitter-like publishing ?
  1. tweets.fp.org. IN TXT “#dnssec in @fedora is neat!”
  2. tweets.fp.org. IN TXT “#linuxcon people think I'm nuts”

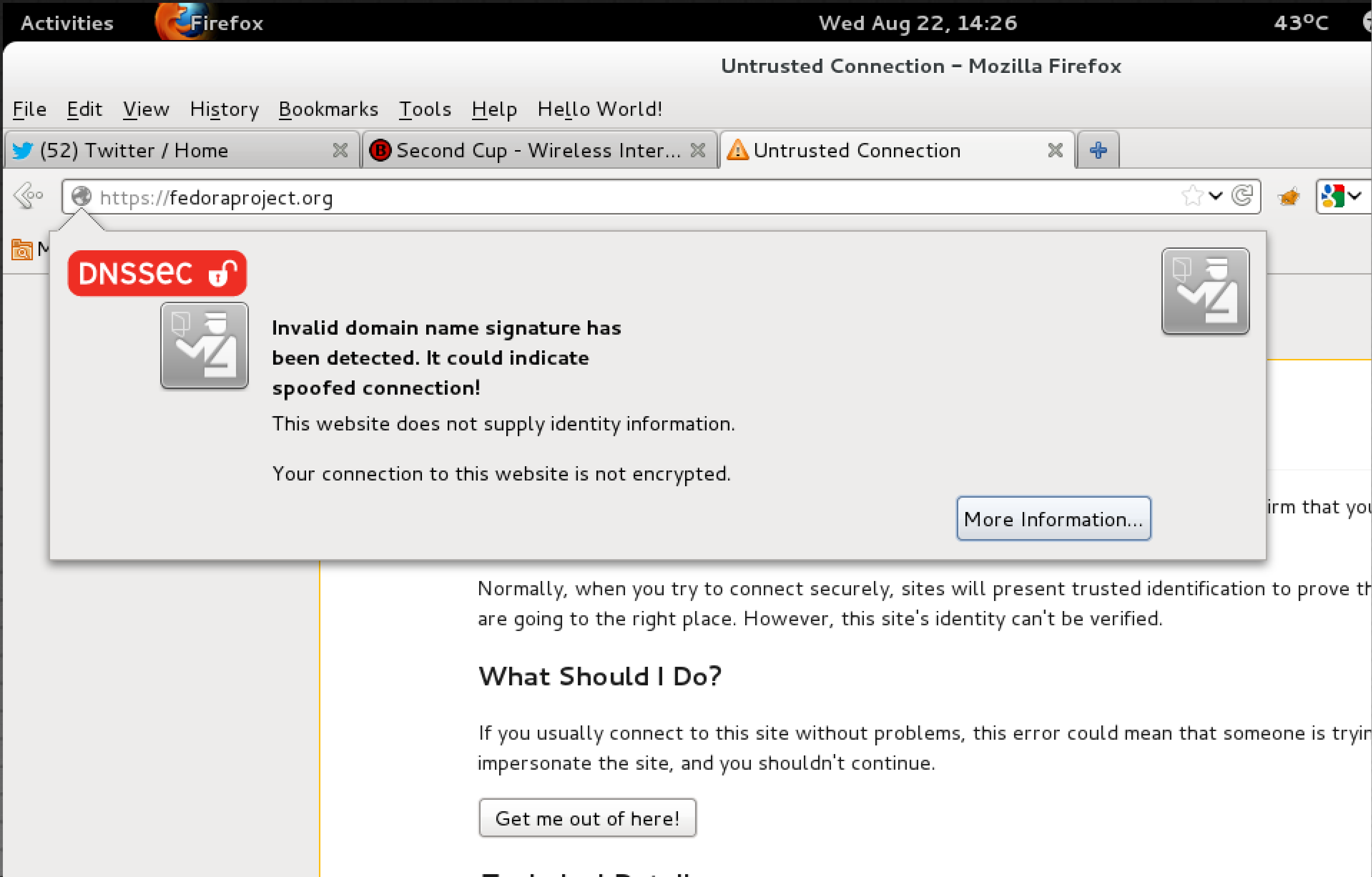
Offline DNSSEC chains

- My laptop stores DNSSEC hierarchy from the root (“.”) to itself (“pwouters.redhat.com”)
- Your laptop does same, from “.” to “johndoe.toronto.example.ca”
- Laptops can now authenticate each other offline via adhoc/bluetooth – no internet required as long as both have the root (“.”) key.

DNSSEC and Firefox

- addon: DNSSEC Validator (labs.nic.cz)
- addon: Extended Validator (os3sec.org)
- addon: DNSSEC / TLSA validator
  - people.redhat.com/pwouters/
- All proof of concept addons to push browser vendors for native integration

DNSSEC Validation



Activities
Firefox
Wed Aug 22, 14:26
43°C
Untrusted Connection – Mozilla Firefox
File Edit View History Bookmarks Tools Help Hello World!
(52) Twitter / Home
Second Cup - Wireless Inter...
Untrusted Connection
https://fedoraproject.org
DNSSEC

Invalid domain name signature has been detected. It could indicate spoofed connection!

This website does not supply identity information.

Your connection to this website is not encrypted.

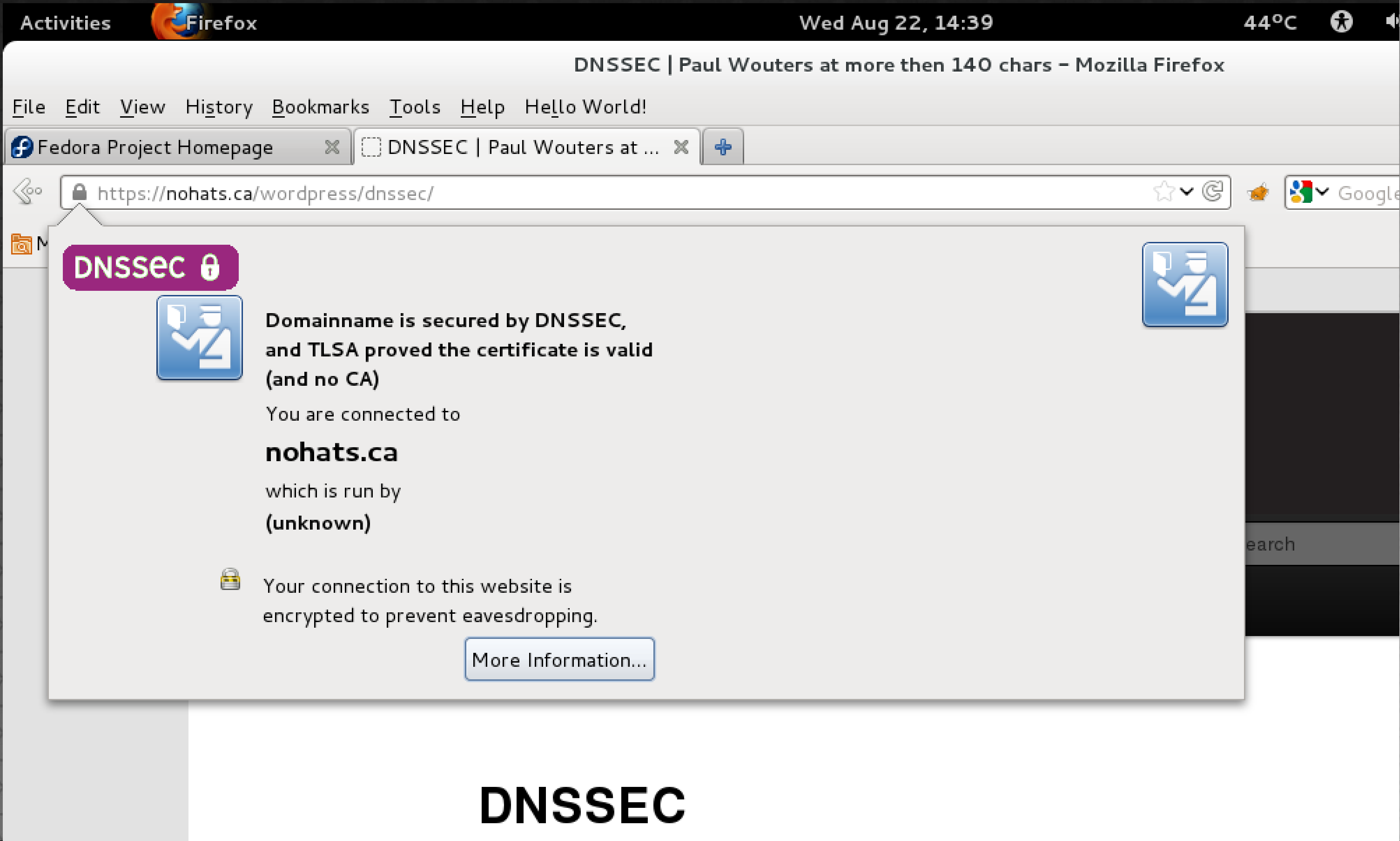
irm that you

Normally, when you try to connect securely, sites will present trusted identification to prove th are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is tryin impersonate the site, and you shouldn't continue.

TLSA / DNSSEC Validation



Activities
Firefox
Wed Aug 22, 14:39
44°C
DNSSEC | Paul Wouters at more then 140 chars - Mozilla Firefox
File Edit View History Bookmarks Tools Help Hello World!
Fedora Project Homepage
DNSSEC | Paul Wouters at ...
https://nohats.ca/wordpress/dnssec/
Google
DNSSEC

Domainname is secured by DNSSEC, and TLSA proved the certificate is valid (and no CA)

You are connected to

nohats.ca

which is run by

(unknown)

Your connection to this website is encrypted to prevent eavesdropping.

More Information...
earch
DNSSEC

Questions?

Ideas?

Contact:

pwouters@redhat.com

LetoAms on FreeNode, Twitter, etc

But djb says 'DNSSEC is evil'

- DNSSEC does not cause 51x amplification (numbers published by Dan Kaminsky and me)
- DNS privacy is more then just encryption
- DNScurve would destroy all DNS caches (causing much worse amplification)
- DNScurve causes CPU load on DNS auth servers (talk about Denial of Service attack)
- The OpenDNS business model is forging dns...
- **DJB is wrong – come talk to me afterwards**

But Moxie Marlinspike says 'DNSSEC and Verisign are evil'

- 200+ million domain names, can't store/verify
- X-Files was wrong, you need to trust someone
- Hierarchical trust or decentralized trust?

- “Peer to Peer” DNS cannot work, uniqueness requires enforcement, human-readability
- **Moxie is postponing the inevitable trust. come talk to me after the presentation**