

Certificate Transparency logs - search engines

<https://crt.sh/>

Certificate Transparency logs - search engines (cont)

<https://censys.io/>

C

By [driver_](#)
cheatography.com/driver/

Not published yet.
Last updated 14th July, 2017.
Page 1 of 100.

Sponsored by **CrosswordCheats.com**
Learn to solve cryptic crosswords!
<http://crosswordcheats.com>

Certificate Transparency logs - search engines (cont)

<https://google.com/transparencyreport/https/ct/>

Extracting sub-domains from Rapid7 FDNS dataset

```
$ zcat <dataset_name> | jq -r 'if (.name | test("\\.example\\.com$")) then .name else empty end'
```

Extracting sub-domains from Rapid7 FDNS dataset (cont)

```
$ zcat 201702_04- fdn s.j son.gz |  
mpty end'
```

Rapid7 · Forward DNS dataset

https://scans.io/study/sonar.fdns_v2

C

By [driver_](#)
cheatography.com/driver/

Not published yet.
Last updated 14th July, 2017.
Page 2 of 100.

Sponsored by [CrosswordCheats.com](#)
Learn to solve cryptic crosswords!
<http://crosswordcheats.com>

Zone walking - NSEC

```
$ ldns-walk @<nameserver> <domain>
```

Zone walking - NSEC (cont)

```
$ ldns-walk @ns1.i nse cur edn s.c  
ns.com
```

Installing Idns utilities

```
$ sudo apt-get install ldnsutils  
# On Ubuntu /Debian  
$ yum install ldns # On Redhat /  
CentOS
```

C

By [driver_](#)
cheatography.com/driver/

Not published yet.
Last updated 14th July, 2017.
Page 3 of 100.

Sponsored by **CrosswordCheats.com**
Learn to solve cryptic crosswords!
<http://crosswordcheats.com>

Zone transfer

```
$ dig AXFR @<nameserver> <domain>
```

Zone transfer (cont)

```
$ dig AXFR @ns1.i nse cur edn s.com insecur ed -  
ns.com
```



By [driver_](#)
cheatography.com/driver/

Not published yet.
Last updated 14th July, 2017.
Page 4 of 100.

Sponsored by CrosswordCheats.com
Learn to solve cryptic crosswords!
<http://crosswordcheats.com>

Zone walking - NSEC3 - nsec3walker

```
$ ./collect_insecu red ns.com > insecurednhash $minsecu red ns.com.co lllect
llect
```

Zone walking - NSEC3 - nsec3walker (cont)

```
.unhash
```

Installing nsec3walker on Ubuntu 16.04:

```
$ wget https://dnscurv.eo rg/
nsec3walker-20101223.tar
.gz`

$ tar -xzf nsec3walker-20101
223.tar.gz

$ cd nsec3walker-20101223

$ make
```

Calculating NSEC3 hash for a domain

```
$ dns-nsec3-hash -t <iterations> -s <salt>
<domain>
```



By [driver_](#)
cheatography.com/driver/

Not published yet.
Last updated 14th July, 2017.
Page 5 of 100.

Sponsored by CrosswordCheats.com
Learn to solve cryptic crosswords!
<http://crosswordcheats.com>

Calculating NSEC3 hash for a domain (cont)

```
$ ldns-n sec 3-hash -t 10 -s 1A2B3C 4D5E6F myzone.ex amp 1  
e.com
```



By [driver_](#)
cheatography.com/driver/

Not published yet.
Last updated 14th July, 2017.
Page 6 of 100.

Sponsored by CrosswordCheats.com
Learn to solve cryptic crosswords!
<http://crosswordcheats.com>