Certificate Transparency logs - search engines

https://crt.sh/

Certificate Transparency logs - search engines (cont)

https://censys.io/

By **driver_**
cheatography.com/driver/

Not published yet.
Last updated 14th July, 2017.

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

By **driver_**
cheatography.com/driver/

Not published yet.
Last updated 14th July, 2017.

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 ldns utilities

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

By **driver_**
cheatography.com/driver/

Not published yet.
Last updated 14th July, 2017.

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 insecu red -
ns.com
```

By **driver_**
cheatography.com/driver/

Not published yet.
Last updated 14th July, 2017.

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

Zone walking - NSEC3 - nsec3walker

```
$ ./collect insecu red ns.com > insecu red ns.com.co llect
```

Zone walking - NSEC3 - nsec3walker (cont)

```
$ ./unhash < insecu red ns.com.co llect > insecu red ns.com
.unhash
```

Installing nsec3walker on Ubuntu 16.04:

```
$ wget https: //d nsc urv e.o rg/
 nse c3w alk er- 201 012 23.t ar
.gz`

$ tar -xzf nsec3w alk er- 201 01
2 23.t ar.gz

$ cd nsec3w alk er- 201 01223

$ make
```

Calculating NSEC3 hash for a domain

$ ldns-nsec3-hash -t <iterations> -s <salt> <domain>

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 l
e.com
```

By **driver_**
cheatography.com/driver/

Not published yet.
Last updated 14th July, 2017.

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