

# OSINT - SSL/TLS Certificates.

<https://crt.sh/>

## crt.sh Certificate Search

Enter an **Identity** (Domain Name, Organization Name, etc),  
a **Certificate Fingerprint** (SHA-1 or SHA-256) or a **crt.sh ID**:

**Search**

[Advanced...](#)

<a href="#">crt.sh ID</a>	<a href="#">Logged At</a> ⓘ	<a href="#">Not Before</a>	<a href="#">Not After</a>	
<a href="#">3144337544</a>	2020-07-26	2011-07-10	2013-07-09	*.google.com
<a href="#">2381394777</a>	2020-01-27	2011-07-13	2012-07-13	*.mail.google.com
<a href="#">2380986199</a>	2020-01-26	2011-02-16	2012-02-16	*.mail.google.com
<a href="#">2380850988</a>	2020-01-26	2012-02-29	2013-02-28	onex.wifi.google.com
<a href="#">2380841885</a>	2020-01-26	2011-07-13	2012-07-13	accounts.google.com
<a href="#">2380681291</a>	2020-01-26	2013-11-22	2013-11-24	hosted-id.google.com
<a href="#">2380579544</a>	2020-01-26	2011-05-11	2012-05-11	accounts.google.com
<a href="#">2379825238</a>	2020-01-26	2011-05-11	2012-05-11	adwords.google.com

<https://google.com/>

-site:abcd.com site:\*.abcd.com

dnsrecon:

```
(kali㉿kali)-[/usr/share/dnsrecon]
$ dnsrecon -t brt -d unec.edu.az -D /usr/share/dnsrecon/namelist.txt
[*] Using the dictionary file: /usr/share/dnsrecon/namelist.txt (provided by
user)
[*] brt: Performing host and subdomain brute force against unec.edu.az ...
```

```
[*] brt: Performing host and subdomain brute force against unec.edu.az ...
[+] A bm.unec.edu.az [204.178.200.200]
[+] A digital.unec.edu.az [204.178.200.200]
[+] A engineering.unec.edu.az [204.178.200.200]
[+] A extern.unec.edu.az [204.178.200.200]
[+] A forum.unec.edu.az [204.178.200.200]
[+] A library.unec.edu.az [204.178.200.200]
[+] A mail.unec.edu.az [204.178.200.200]
[+] A new.unec.edu.az [204.178.200.200]
```