

We are OSINTCurio.us



BROWSER, OPSEC, OSINT

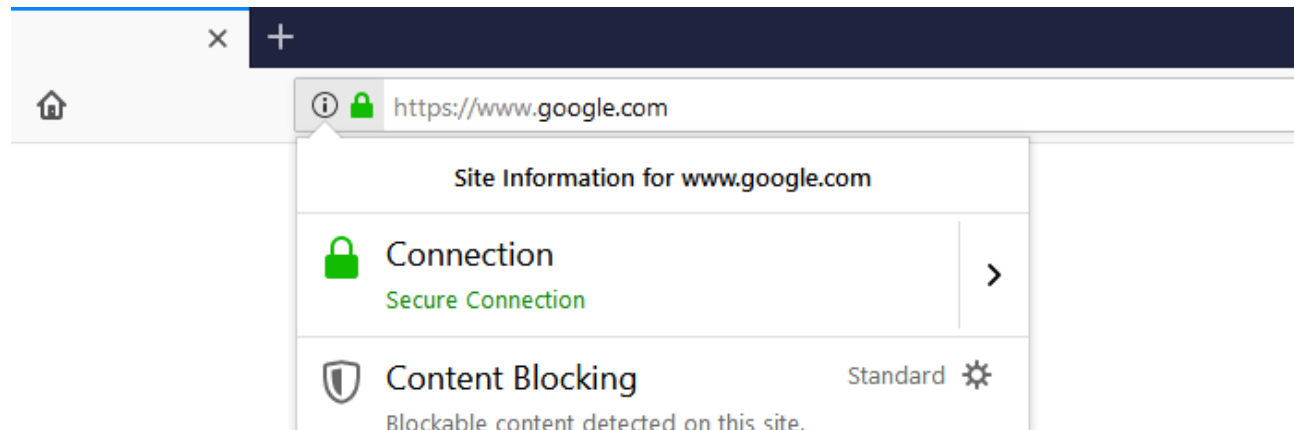
Certificates: The OSINT Gift that Keeps on Giving...



What are certificates?

Everybody on the internet uses certificates, or public key certificates, whether you are aware of it or not. Certificates are documents that can provide proof of an identity, for instance a web server that is claiming its identity to your browser. These public keys can be used for encrypting data that is sent via, for instance, a connection over HTTPS but they are

also used for proving that the server you are reaching is the same server that is listed in the certificate. When a certificate checks out and the connection is encrypted, you are usually served a little green lock in your browser nowadays.



The famous green lock, telling the user that according to what the browser is able to check, this server is serving a correct certificate and your browser established a secure connection

If a different server on a different URL would serve your browser the same certificate, your browser will show a warning that the connection can't be trusted, warning you that the identity of the server in question might be incorrect. Since certificates are provided by a certificate authority and usually have checks in place to prove identities, this is an extra layer of security used to secure communication and mitigate against other types of fraud.

What is certificate transparency?

Certificate transparency was developed after the certificate authority **DigiNotar was compromised** in 2011. During the time that DigiNotar was compromised, there were 531 certificates issued for several different domains, among them some high profile companies like Google, Microsoft, and Yahoo! There was a need to check the certificates that were issued by the Certificate Authorities (CA), so people decided to publicly share the new certificates that were issued by a CA. By sharing all the logs publicly, companies, CAs, and browser would be able to check for the validity of the issued certificates and block whatever was deemed necessary.

What can you find inside certificates?

A certificate that is used on the internet has a fixed set of fields that are described in the **X.509 standard**. There are multiple interesting fields, but some of the more interesting ones are:

Serial Number	A unique identifier for the certificate
Subject Common Name	The URI of the server it was assigned to

Subject organizationName	The company it was issued to
X509v3 Subject Alternative Names	Other URI's or server names that can use this certificate

Some of these fields can be used to find more information on a target. Whether you are performing a red team assignment, a security assessment or need to find company related information for an investigation, it can be used for all these purposes. Let's have a look at each of these fields to see what we can do with it.

Common Name

By searching for the domain name within the certificates in tools like **Shodan.io** or **Censys.io**, it is not uncommon to find multiple servers that use the same certificate. One reason is that a lot of companies use 'wildcard certificates', in which multiple different servers or websites can use the same certificate, as long as they are hosted within the same domain. This is possible by stating in the 'Subject Name' that a certificate is usable by all the sub domains of that domain it is issued to.

They do that by using a wildcard “*” character like this example:
*.whatsapp.com.

To query this in Shodan, you first have to create an account, because the queries use what are called ‘filters’ and everything that goes a bit deeper than a simple IP address is done by filters. Good news, even the free account is good enough to do all the things that follow. After creating an account, simply go to <https://shodan.io> and fill in the following in the search field or [click here](#) to go there directly:

```
ssl: "*.whatsapp.com"
```

Shodan doesn’t have a lot of options to search for specific pieces of information within a certificate, so the domain names will have to be queried via the basic “ssl” filter. To query the same in Censys, go to <https://censys.io/certificates> and fill in the following or [click here](#) to go there directly:

```
parsed.names: "*.whatsapp.com"
```

What is returned is a list of servers that presented a certificate that is valid for anything in regards to **'*.whatsapp.com'**. Since Censys also shows expired certificates by default, you can select the option 'unexpired' in the list with tags, or manually extend the query like this or [click here](#) to open it:

```
(parsed.names: "*.whatsapp.com") AND tags.raw: "unexpired"
```



15


sted

Certificates


Page: 1/1 Results: 23 Time: 92ms


 **C=US, ST=California, L=Menlo Park, O=Facebook, Inc., CN=*.whatsapp.com**


 DigiCert SHA2 High Assurance Server CA


 2018-03-22 – 2019-03-27


 *.whatsapp.com, whatsapp.com


 parsed.names: *.whatsapp.com

 **C=US, ST=CA, L=Menlo Park, O=Facebook, Inc., CN=*.whatsapp.com**


 DigiCert SHA2 High Assurance Server CA


 2018-08-21 – 2019-11-27


 *.whatsapp.com, whatsapp.com


 parsed.names: *.whatsapp.com


 **C=US, ST=California, L=Santa Clara, O=WhatsApp, Inc., CN=*.whatsapp.com**


 DigiCert Baltimore CA-2 G2

 2016-06-16 – 2019-09-09

 *.whatsapp.com, whatsapp.com

 parsed.names: *.whatsapp.com

 **C=US, ST=CA, L=Menlo Park, O=Facebook, Inc., CN=*.whatsapp.com**

 DigiCert SHA2 High Assurance Server CA

Serial Number & Fingerprint

Every certificate is unique also has a serial number and can have specific fingerprints (in SHA256, SHA1, and/or MD5 hash formats). When a certificate is found, it is also possible to pivot from there and query sites like **crt.sh**, **Shodan** or **Censys** for websites that use this particular certificate. Let's have a look at a certificate used by the domain snappytv.com. The latest certificate when writing this article was found here: **<https://crt.sh/?id=950002587>**

It has the following properties:

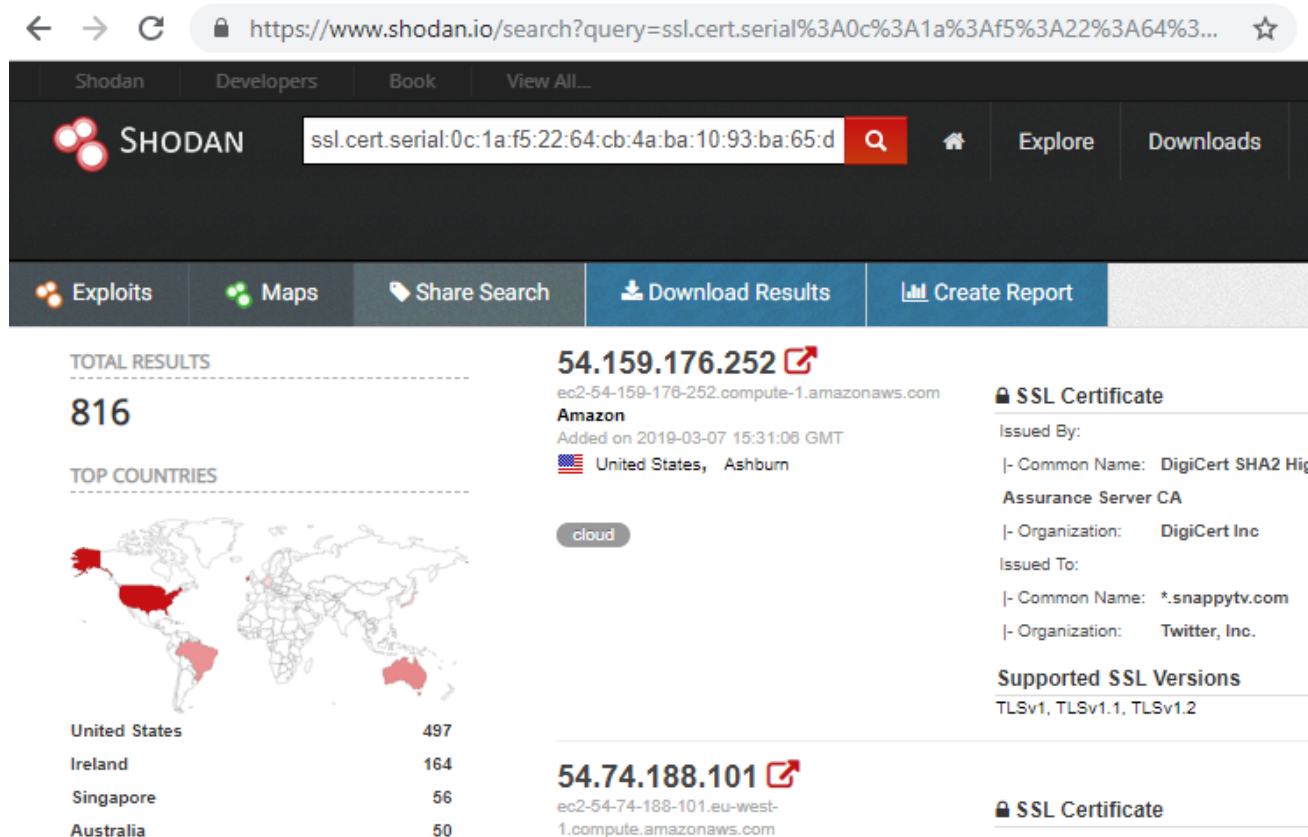
Serial number:

0c:1a:f5:22:64:cb:4a:ba:10:93:ba:65:d1:df:94:c3

Fingerprint in SHA256:

648DD11860F72F5CB9A273CCA4E1A4400F5F4472AD3068D12601A73EF13151D4

We can find related servers by feeding the serial number into Shodan, by using with the '**ssl.cert.serial**' directive:



If we want to do the same in Censys to find out what is in that data set and filter out all the certificates that are not valid anymore, we can query in two different ways. The first one is to query by using the serial number, like we did in Shodan. There's only one caveat, you need to convert the long hexadecimal serial number to a decimal format before using it in Censys. After that, it can be found via the query, that leads to the same certificate (or [click here](#)):

```
parsed.serial_number: 16090707583045581948353732816307983555
```

The second option is to use the ‘fingerprint’ that we found. The query to run is as follows (or go there directly via [this link](#)):

```
parsed.fingerprint_sha256: 648DD11860F72F5CB9A273CCA4E1A4400F5
```

When looking at the certificate alone, you might also wonder whether you can see which servers are using that certificate, or maybe whether they are located in multiple countries. In Censys the easiest way to do that is click on the ‘explore’ button on the top right and select the option ‘IPv4 Hosts’ which will give back a list of servers that are using or have been using this particular certificate.

*.snappytv.com

Certificate

Trust

CT

ZLint

PEM

Raw Data

Explore

Basic Information

Subject DN

C=US, ST=California, L=San Francisco, O=Twitter, Inc., OU=Twitter Security, CN=*.snappytv.com

Issuer DN

C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 High Assurance Server CA

Serial

16090707583045581948353732816307983555

Validity

2018-10-19 00:00:00 to 2020-01-16 12:00:00 (454 days, 12:00:00)

Names

*.snappytv.com

snappytv.com

Fingerprint

SHA-256

648dd11860f72f5cb9a273cca4e1a4400f5f4472ad3068d12601a73ef13151d4

SHA-1

ee079f772f56f11db1c4000eb31c87da1c5a7c2c

MD5

b099779c5455a557a188dc7cecc31858

Public Key

Key Type

2048-bit RSA, e = 65,537

STRONG

Modulus

f5:fd:ea:1f:c4:1f:2c:96:64:8f:a5:8c:b1:2a:76:55:fb:e1:55:07:

Related Certificates

Certificates with the same identity (key + subject)

Certificates with the same public key

Certificates with the same serial number

Certificates with the same names

Certificate Transparency

Associated Pre-Certificates

CA Hierarchy

What's using this certificate?

Popular Websites

IPv4 Hosts

External Services

AWS Certlint

crt.sh

Subject Alternative Name

Besides the URL or server name a certificate was assigned to, it is possible to use a certificate for multiple domain names. It is common to see other domain names pop-up in the lists with 'Alternative Names', therefore giving you a pivot point for further investigations. If the certificate is also used for internal communication it is even possible that internal server and domain names show up here. This can give an even better insight into the internal infrastructure of a company, helping

with the recon stage in (for instance) a penetration test, or even find different businesses that are connected to the target.

A good example of it can be seen in **this certificate** that was issued for the domain 'ssl.ui.ptlogin2.imqq.com', where different domains can be seen that seem to lead to a login service for different environments:

```
-----
Subject DN  C=CN, ST=guangdong, L=shenzhen, O=Shenzhen Tencent Computer Systems Company
             Limited, CN=ssl.ui.ptlogin2.imqq.com
-----
Issuer DN   C=BE, O=GlobalSign nv-sa, CN=GlobalSign Organization Validation CA - SHA256 - G2
-----
Serial      13680230631489361611024544079
-----
Validity    2018-08-24 10:05:29 to 2019-08-25 10:05:29 (366 days, 0:00:00)
-----
Names       login.imqq.com
             login.myapp.com
             login.qcloud.com
             login.qzone.com
             login.weiyun.com
             ssl.ptlogin2.imqq.com
             ssl.ptlogin2.myapp.com
             ssl.ptlogin2.qcloud.com
-----
```

And while this is valid certificate with valid domain names, there sometimes are cases where one starts wondering what the reason was for a specific certificate. Here is an example of a certificate that very well may have been used to decrypt traffic by impersonating SSL traffic from Facebook, Google, Twitter and YouTube:

login.dpmptsp.local

Certificate PEM

Raw Data Explore

Basic Information

Subject DN

C=ID, ST=Jawa Barat, L=Pemkab Bogor, O=dpmptsp, OU=IT, CN=login.dpmptsp.local, emailAddress=admin@dpmptsp.go.id

Issuer DN

C=ID, ST=Jawa Barat, L=Kabupaten Bogor, O=DPMPPTSP, OU=IT, CN=login.dpmptsp.local, emailAddress=admin@dpmptsp.go.id

Serial

14109352335678035848

Validity

2017-07-16 06:59:05 to 2027-07-14 06:59:05 (3650 days, 0:00:00)

Names

192.168.1.254
192.168.2.254
192.168.3.254
dpmptsp.local
facebook.com
google.com
login.dpmptsp.local
twitter.com
youtube.com

Browser Trust

Apple

Untrusted

Microsoft

Untrusted

Mozilla NSS

Untrusted

Key Usage and Constraints

Key Usage

Digital Signature, Key Encipherment

Ext. Key Usage

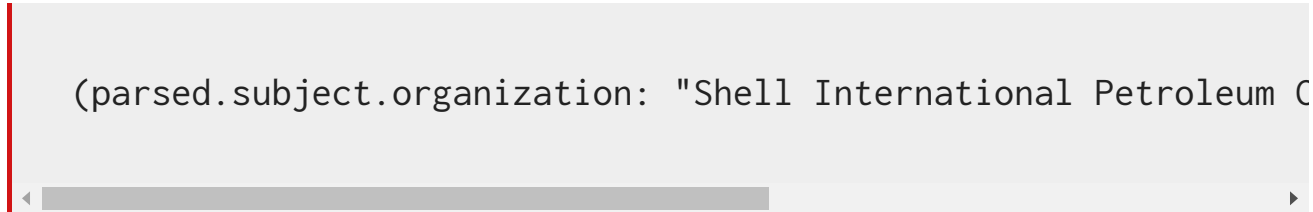
Client Auth, Server Auth

Organization Name

If we are looking into a specific company within Censys, we can query a specific field that contains the organization's name. Let's say we would like to find out what certificates are registered by the Shell company. We can do a very quick query on anything that has the name Shell in it by feeding Censys the following line (or **click**):

```
parsed.subject.organization: Shell
```

That returns more than 4000 results, but by searching within certificates that are assigned to the domain shell.com we find that the actual organization names are a bit longer, for instance “Shell Oil Company”, or the very formal sounding (**click**):

A screenshot of a search result in a light gray box. It shows a single line of text: (parsed.subject.organization: "Shell International Petroleum C. Below the text is a horizontal scrollbar with a gray track and a white slider, indicating the text is scrollable. A red vertical line is on the left side of the box.

```
(parsed.subject.organization: "Shell International Petroleum C
```

Running that query we find a bit more than 120 certificates that were requested by that particular company name. By going over the different organizations with the name ‘Shell’ it is possible to find more businesses and domains that are leading back to this mother company. And when there are multiple companies we are interested in, we can combine them into one **larger query** too.

Querying on Location

Since the location of an IP address is not always accurate and a lot of websites are in the cloud, querying for certificates that were issued by a specific company in a specific city is another possibility. Here we have to

be a bit more creative with our filters. Let's say we want to query the following information:

- A business dealing with 'finance'
- Located within New York
- Only currently active certificates
-

The query in Censys for that contains three parts. The first part is the word 'finance', followed by the operator AND to include the next part, which is the location. After that we have the last part, the previously seen 'unexpired' tag, that results in the following query (or [click here](#)):

```
finance AND (parsed.subject.locality: New York) AND tags.raw:
```

And the result is a list of 352 certificates that are matching our query indeed show websites that are dealing with finances that are supposedly within the New York area:

Q Certificates

finance AND (parsed.subject.locality: New York) AND tags.raw: "unexpired"

Results

Report

Certificates

Page: 1/15 Results: 352 Time: 594ms

C=US, ST=New York, L=New York, O=Weil, Gotshal & Manges LLP, CN=business-finance-restructuring.weil.com

DigiCert SHA2 High Assurance Server CA

2017-05-22 – 2020-06-25

business-finance-restructuring.weil.com

parsed.subject.locality: New York

C=US, ST=New York, L=New York, O=New York State Housing Finance Agency, CN=*.sonymaexpress.org

DigiCert SHA2 Secure Server CA

2019-02-21 – 2020-05-15

*.sonymaexpress.org, sonymaexpress.org

tags: unexpired

jurisdictionCountry=US, jurisdictionStateOrProvince=New York, businessCategory=Private Organization, serialNumber=303621, C=US, ST=New York, L=New York, O=Commercial Finance Association, Inc., CN=www.cfa.com

Starfield Secure Certificate Authority - G2

2017-11-15 – 2019-11-15

cfa.com, www.cfa.com

tags: unexpired

businessCategory=Government Entity, jurisdictionCountry=US, jurisdictionStateOrProvince=New York,

More Information

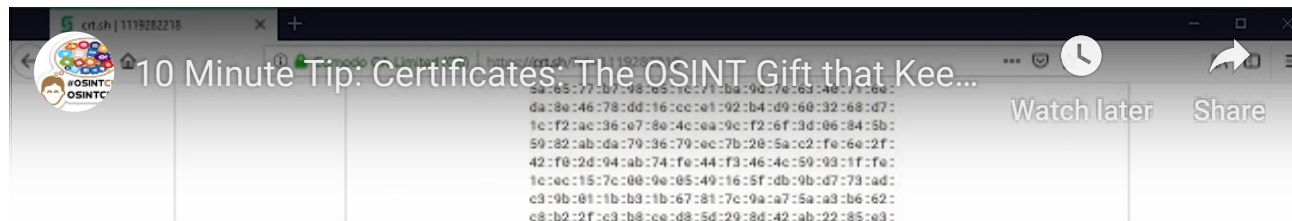
Shodan and **Censys** can provide a lot of information when it comes to domain names and certificates. But the real strength is in the information that can be found inside them and how they are used to

pivot on organizations, locations, web servers et cetera. The only thing you need is a free account on either of them. With Censys there is a limit of 250 queries a month, but that can already help you out on the first steps in this world.

For information on what fields there are within Shodan, you can visit this **blog article** about the features that are available. For Censys there isn't a ready made list with fields. But Censys will help you with an auto-fill feature while you are typing, making it a bit easier to get queries right the first time.

And besides that, I was recommended the book '**Hack The World with OSINT**' by Chris Kubecka. I haven't read it myself yet, but this book goes into detail when it comes to using Censys for OSINT purposes. Because there is a lot more to find out there than what is hidden in certificates.

Sector035 made a 10 Minute Tip video of this blog post's content that can be watched below, or directly on our YouTube channel.



Related



Muting the Twitter algorithm and using basic search operators for better OSINT research

IN "BROWSER"



How to search effectively and efficiently - Part I: basic principles, tips and tricks for OSINT

IN "BROWSER"



Dial cURL for Content

IN "OSINT"

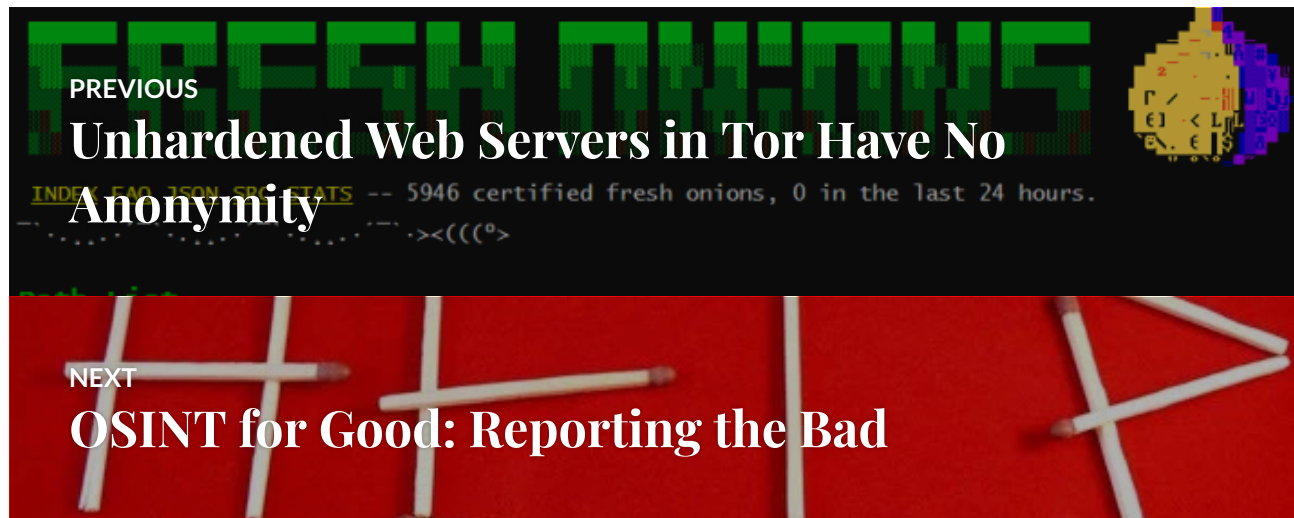
One thought on “Certificates: The OSINT Gift that Keeps on Giving...”

Pingback: **Website Attribution Without WhoIs – Reverse IP Lookups (Part 2) – NixIntel**

Leave a Reply

Enter your comment here...

This site uses Akismet to reduce spam. [Learn how your comment data is processed.](#)





Creative Commons License



All content on this site is
licensed under a **Creative Commons**
Attribution-ShareAlike 4.0
International License.