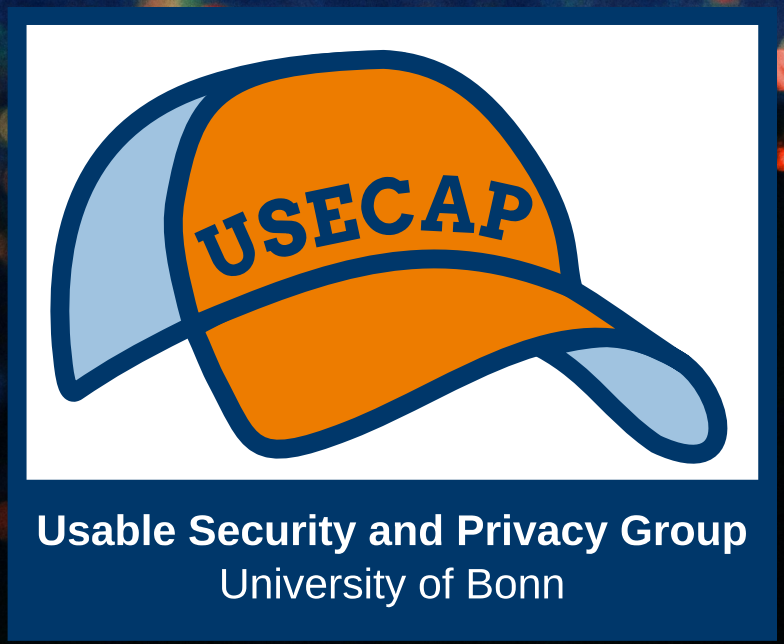
Certificate Transparency Observatory

Karoline Busse, Christian Tiefenau



Certificate Transparency

- RFC 6962 by Laurie, Langley, Käsper
- Public, verfifiable logging of SSL/TLS certificates
- Fast detection of misissued Certificates and (possibly) rogue CAs

Current State of CT

- 13 Logs, ~15 Mio certificates logged
- Some query interfaces for log data available

crt.sh CA ID	5

CA Name/Key

```
Subject:
    commonName                = GeoTrust Global CA
    organizationName          = GeoTrust Inc.
    countryName               = US
Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
        Public-Key: (2048 bit)
        Modulus:
            00:da:cc:18:63:30:fd:f4:17:23:1a:56:7e:5b:df:
            3c:6c:38:e4:71:b7:78:91:d4:bc:a1:d8:4c:f8:a8:
            43:b6:03:e9:4d:21:07:08:88:da:58:2f:66:39:29:
            bd:05:78:8b:9d:38:e8:05:b7:6a:7e:71:a4:e6:c4:
            60:a6:b0:ef:80:e4:89:28:0f:9e:25:d6:ed:83:f3:
            ad:a6:91:c7:98:c9:42:18:35:14:9d:ad:98:46:92:
            2e:4f:ca:f1:87:43:c1:16:95:57:2d:50:ef:89:2d:
            80:7a:57:ad:f2:ee:5f:6b:d2:00:8d:b9:14:f8:14:
            15:35:d9:c0:46:a3:7b:72:c8:91:bf:c9:55:2b:cd:
            d0:97:3e:9c:26:64:cc:df:ce:83:19:71:ca:4e:e6:
            d4:d5:7b:a9:19:cd:55:de:c8:ec:d2:5e:38:53:e5:
            5c:4f:8c:2d:fe:50:23:36:fc:66:e6:cb:8e:a4:39:
            19:00:b7:95:02:39:91:0b:0e:fe:38:2e:d1:1d:05:
            9a:f6:4d:3e:6f:0f:07:1d:af:2c:1e:8f:60:39:e2:
            fa:36:53:13:39:d4:5e:26:2b:db:3d:a8:14:bd:32:
            eb:18:03:28:52:04:71:e5:ab:33:3d:e1:38:bb:07:
            36:84:62:9c:79:ea:16:30:f4:5f:c0:2b:e8:71:6b:
            e4:f9
        Exponent: 65537 (0x10001)
```

Certificates

Not Before	Not After	Issuer Name
2002-05-21	2018-08-21	C=US, O=Equifax, OU=Equifax Secure Certificate Authority
2002-05-21	2018-08-21	C=US, O=Equifax, OU=Equifax Secure Certificate Authority
2002-05-21	2022-05-21	C=US, O=GeoTrust Inc., CN=GeoTrust Global CA

Issued Certificates

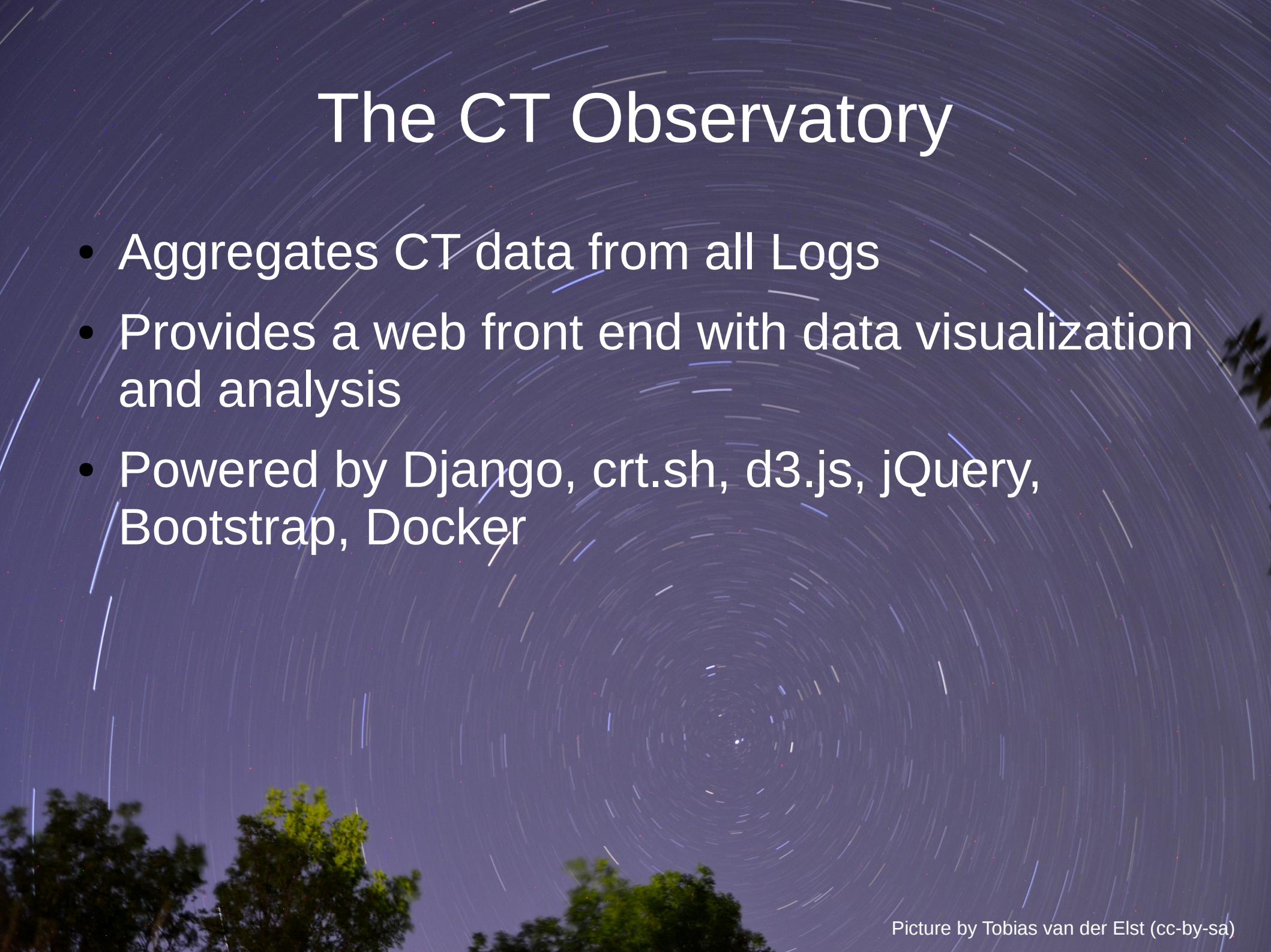
Select search type: IDENTITY

Enter search term: (% = wildcard)

Search options:

The CT Observatory

- Aggregates CT data from all Logs
- Provides a web front end with data visualization and analysis
- Powered by Django, crt.sh, d3.js, jQuery, Bootstrap, Docker



Welcome to the CT Observatory!

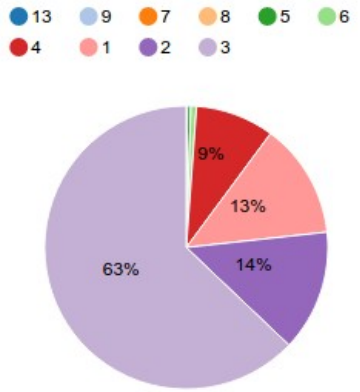
15580517 Certificates

A total of 15580517 certificates from 10 logs have been collected and observed by this observatory.

8124258	active
7456259	expired
0	revoked
0	misissued

Number of occurrences in logs

This chart shows the number of occurrences of a certificate in all monitored logs.



15423 Certificate Authorities

A total of 15423 CAs are observed.

0	correctly operating
0	show interesting behaviour

10 Logs

A total of 10 logs are being observed. The biggest log holds 14278450 certificates and the smallest log holds 1062 certificates.

Log	Entries
Google Pilot log	14276616
Google Aviator log	13375477
Google Rocketeer log	12500994
Certly.IO log	1496779
Symantec log	342234
DigiCert Log Server	291281
Izenpe log	74373
WoSign log	17043
Venafi log	15900
Symantec VEGA log	1063

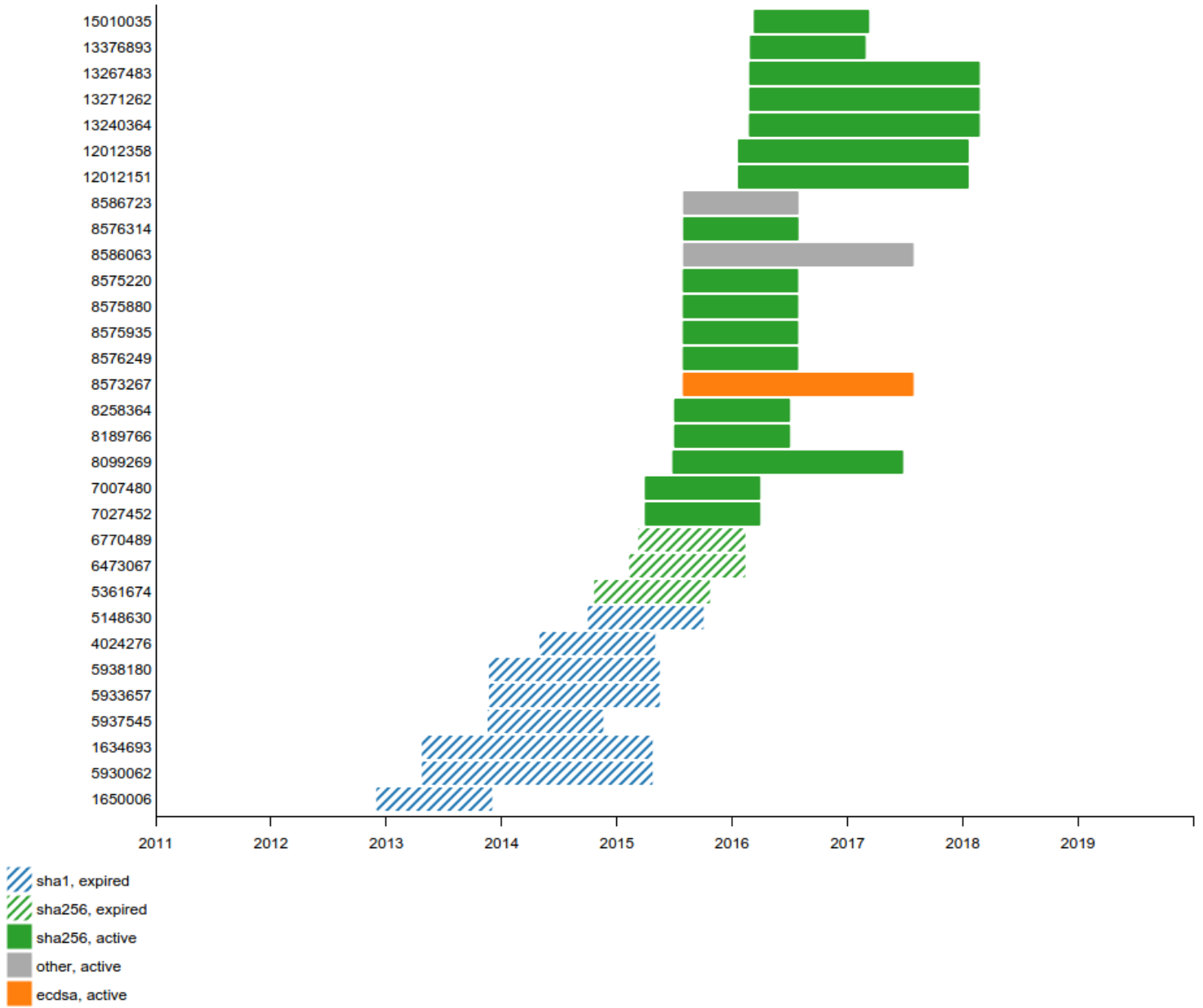
Most frequent signature algorithms

notBefore, per month

Timeline

Back up to the top

Order by notBefore notAfter length



signature_algorithm
sha256WithRSAEncryption

notBefore
2015-11-03 00:00:00

notAfter
2018-11-28 12:00:00

has_expired
False

digest_md5
68:42:3D:55:EA:27:D0:B4:FD:A1:87:8F:CA:B7:A1:EB

digest_sha1
25:09:FB:22:F7:67:1A:EA:2D:0A:28:AE:80:51:6F:39:0D:E0:CA:21

certificate_identity

Information from certificate_identity:

dNSName
example.com

dNSName
example.edu

dNSName
example.net

dNSName
example.org

organizationName
Internet Corporation for Assigned Names and Numbers

organizationalUnitName
Technology

dNSName
www.example.com

dNSName
www.example.edu

dNSName
www.example.net

commonName
www.example.org

dNSName
www.example.org

This certificate has been issued by DigiCert SHA2 High Assurance Server CA.

List all certificates with CN=www.example.org.

Issuer

Information about the **issuer** directly from the certificate:

C
US

O
DigiCert Inc

OU
www.digicert.com

CN
DigiCert SHA2 High Assurance Server CA

Subject

Information about the **subject** directly from the certificate:

C
US

ST
California

L
Los Angeles

O
Internet Corporation for Assigned Names and Numbers

OU
Technology

CN
www.example.org

Tree

Future Work

- Data Mining/Big Data Analysis to detect “interesting events“, e.g.
  - Switching a CA
  - Switching to weaker crypto
  - New extensions
- In-depth analysis of historical certificate data
- Provide better service for domain administrators

The CT Observatory

Soon at https://ct-observatory.org
https://github.com/USECAP/ct-infrastructure
{busse, tiefenau}@cs.uni-bonn.de