

ThreatQuotient



Censys Operation Guide

Version 1.0.0

Thursday, September 10, 2020

ThreatQuotient

11400 Commerce Park Dr., Suite 200
Reston, VA 20191

Support

Email: support@threatq.com

Web: support.threatq.com

Phone: 703.574.9893

Warning and Disclaimer

ThreatQuotient, Inc. provides this document “as is”, without representation or warranty of any kind, express or implied, including without limitation any warranty concerning the accuracy, adequacy, or completeness of such information contained herein. ThreatQuotient, Inc. does not assume responsibility for the use or inability to use the software product as a result of providing this information.

Copyright © 2020 ThreatQuotient, Inc.

All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

Last Updated: Thursday, September 10, 2020

Contents

Censys Operation Guide	1
Warning and Disclaimer	2
Contents	3
Versioning	4
Introduction	5
Installation	6
Configuration	7
Actions	8
submit_ip	9
submit_ip Mapping Table	36
submit_domain	38
submit_domain Mapping Table	107
submit_hash	111
submit_hash Mapping Table	128
Change Log	135

Versioning

- **Operation Version:** 1.0.0
- **Minimum ThreatQ Version:** 4.34.0

Introduction

The Censys operation enriches ingested ThreatQ system objects with context obtained from the Censys API.

The operation requires:

- a private or public Censys **API Key**
- the **username** associated with the API key

Installation

Perform the following steps to install the operation:



The same steps can be used to upgrade the operation to a new version.

1. Log into <https://marketplace.threatq.com/>.
2. Locate and download the **Censys Operation** file.
3. Navigate to your ThreatQ instance.
4. Click on the **Settings** icon and select **Operations Management**.
5. Click on the **Install Operation** button.
6. Upload the operation file using one of the following methods:
 - Drag and drop the file into the dialog box
 - Select **Click to Browse** to locate the operation file on your local machine



ThreatQ will inform you if the operation already exists on the platform and will require user confirmation before proceeding.

The operation will be added to your list of installed operations. You will still need to [configure and then enable](#) the operation.

Configuration



ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other feed-related credentials.

To Configure the operation:

1. Click on the **Settings** icon and select **Operations Management**
2. Locate the **Censys** operation and click on **Operation Settings**.
3. Enter the following parameters for the operation:

Parameter	Description
API Key	Your private or public Censys API key.
Username	The username associated to the API Key listed above.

4. Click on **Save Changes** then click on the toggle switch next to the operation name to enable the operation.

Actions

The operation offers the following actions:

Action	Description	Object Type	Object Subtype
submit_ip	Submits IP for analysis	Indicator	IP
submit_domain	Submits domain for analysis	Indicator	FQDN
submit_hash	Submits hash for analysis	Indicator	SHA-256

submit_ip

GET <https://censys.io/api/v1/view/ipv4> endpoint.

```
{
  "tags": [
    "http",
    "dns",
    "https"
  ],
  "53": {
    "dns": {
      "lookup": {
        "errors": false,
        "authorities": [],
        "support": true,
        "metadata": {},
        "questions": [
          {
            "type": "A",
            "name": "c.afekv.com"
          }
        ]
      }
    }
  }
}
```

```
    }
  ],
  "answers": [
    {
      "type": "A",
      "response": "192.150.186.1",
      "name": "c.afekv.com"
    },
    {
      "type": "A",
      "response": "108.162.217.121",
      "name": "c.afekv.com"
    }
  ],
  "additional": [],
  "open_resolver": true,
  "resolves_correctly": true
}
},
"protocols": [
```

```
"443/https",
"80/http",
"53/dns"
],
"ip": "1.1.1.1",
"443": {
  "https": {
    "dhe": {
      "support": false,
      "metadata": {}
    },
    "get": {
      "status_line": "200 OK",
      "title": "1.1.1.1 \u2014 The free app that makes your Internet faster.",
      "status_code": 200,
      "headers": {
        "server": "cloudflare",
        "content_type": "text/html",
        "strict_transport_security": "max-age=31536000",
        "connection": "keep-alive",
        "unknown": [
```

```
{
  "key": "date",
  "value": "Tue, 18 Aug 2020 23:39:19 GMT"
},
{
  "key": "x_amz_request_id",
  "value": "tx00000000000000ffce2e9-005f3c6466-1c564f2-default"
},
{
  "key": "cf_request_id",
  "value": "04a58a17630000fdd1aa91f200000001"
},
{
  "key": "served_in_seconds",
  "value": "0.006"
},
{
  "key": "cf_cache_status",
  "value": "HIT"
},
{
```

```

        "key": "expect_ct",
        "value": "max-age=604800, report-uri=\"https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct\""
    },
    {
        "key": "cf_ray",
        "value": "5c4f79389ceffdd1-ORD"
    }
],
"age": "577",
"expires": "Wed, 19 Aug 2020 03:39:19 GMT",
"cache_control": "public, max-age=14400",
"vary": "Accept-Encoding",
"last_modified": "Tue, 11 Aug 2020 23:37:52 GMT"
},
"body": "<!DOCTYPE html><html theme=\"light\" lang=\"en-US\" prefix=\"og:
http://ogp.me/ns#\"><meta charset=\"utf-8\"><title>1.1.1.1 \t(.....)</script></body></html>",
"metadata": {
    "description": "cloudflare",
    "product": "cloudflare"
},

```

```
    "body_sha256": "0e865861275bfdc96122506160fb63f684ed0e2fdf81cc3e5d62f14e5c6eb959"
  },
  "rsa_export": {
    "support": false,
    "metadata": {}
  },
  "tls": {
    "ocsp_stapling": false,
    "cipher_suite": {
      "name": "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
      "id": "0xC02B"
    },
    "certificate": {
      "parsed": {
        "signature_algorithm": {
          "oid": "1.2.840.10045.4.3.2",
          "name": "ECDSAWithSHA256"
        },
        "serial_number": "2393062632280249844899714234728687389",
        "issuer_dn": "C=US, O=DigiCert Inc, CN=DigiCert ECC Secure Server CA",
        "tbs_noct_fingerprint":
```

```
"c7f211619c7708951ad9a3c3f2513348193395d28a971a600befdd883eace9c8",
    "redacted": false,
    "tbs_fingerprint":
"292b9172703630cfe17212f4649ec512a64fcd5460093f54960c725ea0d76bce",
    "issuer": {
        "organization": [
            "DigiCert Inc"
        ],
        "country": [
            "US"
        ],
        "common_name": [
            "DigiCert ECC Secure Server CA"
        ]
    },
    "subject_dn": "C=US, ST=California, L=San Francisco, O=Cloudflare, Inc.,
CN=cloudflare-dns.com",
    "names": [
        "one.one.one.one",
        "1.1.1.1",
        "1.0.0.1",
```

```
        "162.159.46.1",
        "cloudflare-dns.com",
        "*.cloudflare-dns.com",
        "162.159.132.53",
        "162.159.36.1"
    ],
    "fingerprint_sha1": "6656840172b4fbbcd6d0a4a103491e93004d195f",
    "validation_level": "OV",
    "validity": {
        "start": "2019-01-28T00:00:00Z",
        "end": "2021-02-01T12:00:00Z",
        "length": 63547200
    },
    "version": 3,
    "fingerprint_md5": "308e8211296eafe71da7adbb0e56ccda",
    "spki_subject_fingerprint": "7ec099b644a732e5635c3f1a9955b368b-
c23522dde3a6b4f213b5eef7f60db1f",
    "subject_key_info": {
        "ecdsa_public_key": {
            "y": "bD1qyHe4y48uUFP99Bgmf2E37f/CvukLXbl+4d8c4nQ=",
            "b": "WsY12Ko6k+ez671VdpiGvGUdBrDMU7D2O848PifSYEs=",
```

```
        "n": "////////wAAAD/////////7zm+q2nF56E87nKwvxjJVE=",
        "length": 256,
        "gy": "T+NC4v4af5uO5+tKfA+eFivOM1drMV7Oy7ZAaDe/UfU=",
        "pub": "BMUgcIwgQlAoHn1EQXwweSk-
cY14dRJvF93E6K97SoqSxbD1qyHe4y48uUFP99Bgmf2E37f/CvukLXbl+4d8c4nQ=",
        "p": "////////wAAAAEAAAAAAAAAAAAAAAAAD/////////8=",
        "curve": "P-256",
        "x": "xSBwjCBCUCgefURBfDB5KRxjXh1Em8X3cTor3tKipLE=",
        "gx": "axfR8uEsQkf4vOblY6RA8ncDfYEt6zOg9KE5RdiYwpY="
    },
    "fingerprint_sha256": "57acde-
b3c847055c14102b077fbb95e7118cedd8f7b8c5c84bdfbfefea0bcfa35",
    "key_algorithm": {
        "name": "ECDSA"
    }
},
    "fingerprint_sha256": "b1910e0d8aa0d5de8e1f20c026d53ed9cf3d-
f0d72a866ecbdbfc8dfa650ed0bf",
    "extensions": {
        "key_usage": {
            "digital_signature": true,
```

```
        "value": 1
    },
    "crl_distribution_points": [
        "http://crl3.digicert.com/ssca-ecc-g1.crl",
        "http://crl4.digicert.com/ssca-ecc-g1.crl"
    ],
    "certificate_policies": [
        {
            "id": "2.16.840.1.114412.1.1",
            "cps": [
                "https://www.digicert.com/CPS"
            ]
        },
        {
            "id": "2.23.140.1.2.2"
        }
    ],
    "subject_key_id": "7095dc5ca38e6607dbcb8110c6abe7c3a8457fa0",
    "extended_key_usage": {
        "client_auth": true,
        "server_auth": true
    }
}
```

```
    },  
    "authority_key_id": "a39de61ff9da394fc06ee891cb95a5da31e20a9f",  
    "signed_certificate_timestamps": [  
      {  
        "timestamp": 1548690003,  
        "log_id": "pLkJkLQYWBSHuxOizGdwCjwlmAT5G9+443fNDsgN3BA=",  
        "version": 0,  
        "signature":  
"BAMARzBFAiEA5Z6D3jF7RZEbMt1bNHqL5NyCyrdNcem4FHTJZkExSLwCIHAJ9JRUo4h-  
sx5tnjow2SczIj+VGo9CcLm/RjvEZMZJK"  
      },  
      {  
        "timestamp": 1548690003,  
        "log_id": "h3W/5118+IxDmV+9827/Vo1HVjb/SrVgwbTq/16ggw8=",  
        "version": 0,  
        "signature":  
"BAMARjBEAiBQtJ9CTKHxqJfG/0InMXeQZX/6O8TrPwZNI/YXXOTe4wIgEKHGJxy/YjKk7RZIdL5krCCOTW4m-  
pDP9sgxF58JD0bw="  
      },  
      {  
        "timestamp": 1548690003,
```

```
        "log_id": "u9nfvB+KcbWTlCOXqpJ7RzhXlQqrUugakJZkNo4e0YU=",
        "version": 0,
        "signature": "BAMASDBGAiEAvc49MHM5m-
1LmtL+4vOow6IAIIVDJj6ZMn4vQj1NwHdECIQDj5KI/PT/mQXG+uTsApgp296WBXWGKI9szZgdj7/QEiQ=="
    }
],
"subject_alt_name": {
    "dns_names": [
        "cloudflare-dns.com",
        "*.cloudflare-dns.com",
        "one.one.one.one"
    ],
    "ip_addresses": [
        "1.1.1.1",
        "1.0.0.1",
        "162.159.132.53",
        "2606:4700:4700::1111",
        "2606:4700:4700::1001",
        "2606:4700:4700::64",
        "2606:4700:4700::6400",
        "162.159.36.1",
```

```
        "162.159.46.1"
      ]
    },
    "authority_info_access": {
      "ocsp_urls": [
        "http://ocsp.digicert.com"
      ],
      "issuer_urls": [
        "http://cacerts.digicert.com/DigiCertECCSecureServerCA.crt"
      ]
    },
    "basic_constraints": {
      "is_ca": false
    }
  },
  "signature": {
    "signature_algorithm": {
      "oid": "1.2.840.10045.4.3.2",
      "name": "ECDSAWithSHA256"
    },
    "self_signed": false,
```

```
        "valid": true,  
        "value": "MGUCMHs++oV9h0zLq/yN10b-  
sH3ZlaGvCemVRFavgGbBOW8kIewFeFjS1PtPdgaz258lVBQIxAM1H+Y3c9acnO+JYDrp-  
wuywROnD7Vm83xqSYmMk/0/nOXiAMEWM4ik9Aym2qpe7YmQ=="  
    },  
    "subject": {  
        "organization": [  
            "Cloudflare, Inc."  
        ],  
        "locality": [  
            "San Francisco"  
        ],  
        "common_name": [  
            "cloudflare-dns.com"  
        ],  
        "province": [  
            "California"  
        ],  
        "country": [  
            "US"  
        ]  
    }
```

```
    }
  }
},
"chain": [
  {
    "parsed": {
      "signature_algorithm": {
        "oid": "1.2.840.113549.1.1.12",
        "name": "SHA384WithRSA"
      },
      "serial_number": "14347142274732774646150233778247550482",
      "issuer_dn": "C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert
Global Root CA",
      "tbs_noct_fingerprint": "eb7525f88f0d9458f81a995019bf-
d34cb89ccdc957e7b0ef315f10f897638118",
      "validation_level": "unknown",
      "tbs_fingerprint": "eb7525f88f0d9458f81a995019bf-
d34cb89ccdc957e7b0ef315f10f897638118",
      "issuer": {
        "organization": [
          "DigiCert Inc"
        ]
      }
    }
  }
]
```

```
    ],
    "country": [
        "US"
    ],
    "organizational_unit": [
        "www.digicert.com"
    ],
    "common_name": [
        "DigiCert Global Root CA"
    ]
},
"subject_dn": "C=US, O=DigiCert Inc, CN=DigiCert ECC Secure Server
CA",

"fingerprint_sha1": "56ee7c270683162d83baeacc790e22471adaabe8",
"redacted": false,
"validity": {
    "start": "2013-03-08T12:00:00Z",
    "end": "2023-03-08T12:00:00Z",
    "length": 315532800
},
"version": 3,
```

```
        "fingerprint_md5": "c64ae88aeb2cb31198d70483212fb411",
        "spki_subject_fingerprint": "1eed935f0163c0979f-
d92440ea3660b2327ce1d00d04f73cfd3bd348519b0a23",
        "subject_key_info": {
            "ecdsa_public_key": {
                "y": "oOZ/WpIRl1Nv68DLP679Wz9HJOeaBy6Wvqgvu1cYr3Gk-
vXg6HuhbPGtkESvMNCuM",
                "b":
"szEvp+I+5+SYjgVr4/gtGRgdnG7+gUESAxQIj1ATh1rGVjmNii7RnSqFyO3T7Crv",
                "n": "//////////////////////////////////////////x2NNg-
fQ3Ld9YGg2ySLCneuzsGWrMxSlz",
                "length": 384,
                "gy": "NhfeSpYmLG9d-
npi/kpLcKfj0Hb0omhR86doxE7XwuMAKYLHOHX6BnXpDHXyQ6g5f",
                "pub":
"BOIIQup32CTeoCxx-
pBPOQJwjc-
qkCCg43PyE2uI1TFPbVkZVL85YCjXEexNjLp59e76Dm-
f1qSEZZTb+vAyz+u/Vs/RyTnmgculr6oL7tXGK9xpL14Oh7oWzxrZBErzDQrjA==",
                "p":
"//////////////////////////////////////////7/////AAAAAAAAAAD////////",
```

```
        "curve": "P-384",
        "x": "4ghC6n-
fYJN6gLGsKE85AnCNyqQIKDjc/ITa4jVMU9tWRlUvzlgKNcR7E2Munn17v",
        "gx":
"qofKIr6LBTeOscce8yCtdG4dO2KLp5uYWfdB4IJUKjhVAvJdv1UpbDpUXjhydgq3"
    },
    "fingerprint_sha256": "3d95cdde5440c-
bef2d04a9363b1e85ee32259f3af66339b0a9cdc99f27d7a02c",
    "key_algorithm": {
        "name": "ECDSA"
    }
},
    "fingerprint_sha256": "458446ba75d932e914f23c2b57b7d192ed-
dbc2181d958e1181ad5251747a1ee8",
    "extensions": {
        "key_usage": {
            "digital_signature": true,
            "certificate_sign": true,
            "crl_sign": true,
            "value": 97
        }
    },
```

```
"crl_distribution_points": [  
    "http://crl3.digicert.com/DigiCertGlobalRootCA.crl"  
],  
"certificate_policies": [  
    {  
        "id": "2.5.29.32.0",  
        "cps": [  
            "https://www.digicert.com/CPS"  
        ]  
    }  
],  
"subject_key_id": "a39de61ff9da394fc06ee891cb95a5da31e20a9f",  
"authority_key_id": "03de503556d14cbb66f0a3e21b1bc397b23dd155",  
"basic_constraints": {  
    "is_ca": true,  
    "max_path_len": 0  
},  
"authority_info_access": {  
    "ocsp_urls": [  
        "http://ocsp.digicert.com"  
    ]  
}
```

```
    }  
  },  
  "signature": {  
    "signature_algorithm": {  
      "oid": "1.2.840.113549.1.1.12",  
      "name": "SHA384WithRSA"  
    },  
    "self_signed": false,  
    "valid": true,  
    "value": "x4qqQ0vs-  
dMnFq9UfMDU2bphWe0isBWoue5pXJfMb/re-  
q22cx7a67M7nyn-  
Nk298EN-  
woASbM/nyatkYwg6B+IDir7ZjfIMOjSwiSnRUgt6gFQSjGUE9+NX9oqu0k8YfN5yJxmkhqWKvR7NlijLEEQdBrT7Ui20ruKBk-  
VxMxAwen-  
qYId0kueyctZIHrYPGxGr4d+Y1vhMPJ2SyQ7+D6XdW2wiHlEcU9V8or-  
6NoTIOPYPeWgHmFanYm-  
nZUMIAONPu56KGVkZqTZg+qZdM1uTX0c642yx-  
a8WG07I81XqiDgRNB0Rrz8HqE9q0nQRLyr8c7dfwhVDBWzWfdoCvSKbT9P5dw=="  
  },  
  "subject": {
```

```
        "organization": [
            "DigiCert Inc"
        ],
        "country": [
            "US"
        ],
        "common_name": [
            "DigiCert ECC Secure Server CA"
        ]
    }
}

},
"version": "TLSv1.2",
"validation": {
    "browser_trusted": true
},
"server_key_exchange": {
    "ecdh_params": {
        "curve_id": {
            "name": "secp256r1",
```

```
        "id": 23
      }
    },
    "metadata": {},
    "session_ticket": {
      "lifetime_hint": 64800,
      "length": 176
    },
    "signature": {
      "signature_algorithm": "ecdsa",
      "hash_algorithm": "sha256",
      "valid": true
    }
  },
  "dhe_export": {
    "support": false,
    "metadata": {}
  },
  "heartbleed": {
    "heartbeat_enabled": false,
```

```
        "heartbleed_vulnerable": false,
        "metadata": {}
    }
}
},
"ports": [
    80,
    443,
    53
],
"80": {
    "http": {
        "get": {
            "status_line": "200 OK",
            "title": "1.1.1.1 \u2014 The free app that makes your Internet faster.",
            "status_code": 200,
            "headers": {
                "server": "cloudflare",
                "content_type": "text/html",
                "strict_transport_security": "max-age=31536000",
                "connection": "keep-alive",
```

```
"unknown": [  
  {  
    "key": "cf_request_id",  
    "value": "04a318dfaf0000c55c97b39200000001"  
  },  
  {  
    "key": "served_in_seconds",  
    "value": "0.003"  
  },  
  {  
    "key": "cf_cache_status",  
    "value": "HIT"  
  },  
  {  
    "key": "cf_ray",  
    "value": "5c4b90df7dcbc55c-ORD"  
  },  
  {  
    "key": "date",  
    "value": "Tue, 18 Aug 2020 12:16:25 GMT"  
  },  
]
```

```
{
  {
    "key": "x_amz_request_id",
    "value": "tx0000000000000005e4068a-005f3bc4c2-1df2986-default"
  },
  {
    "key": "expect_ct",
    "value": "max-age=604800, report-uri=\"https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct\""
  }
],
"age": "471",
"expires": "Tue, 18 Aug 2020 16:16:25 GMT",
"cache_control": "public, max-age=14400",
"vary": "Accept-Encoding",
"last_modified": "Tue, 11 Aug 2020 23:37:52 GMT"
},
"body": "<!DOCTYPE html><html theme=\"light\" lang=\"en-US\" prefix=\"og:
http://ogp.me/ns#\"><meta charset=\"utf-8\"><title>1.1.1.1 \u2014 The free app that makes your
Internet faster.(.....)</script></body></html>",
"metadata": {
  "description": "cloudflare",
```

```
        "product": "cloudflare"
      },
      "body_sha256": "0e865861275bfdc96122506160fb63f684ed0e2fdf81cc3e5d62f14e5c6eb959"
    }
  },
  "autonomous_system": {
    "routed_prefix": "1.1.1.0/24",
    "path": [
      13335
    ],
    "asn": 13335,
    "description": "CLOUDFLARENET",
    "country_code": "US",
    "name": "CLOUDFLARENET",
    "rir": "unknown"
  },
  "updated_at": "2020-08-19T13:06:02+00:00",
  "location": {
    "latitude": -33.494,
    "longitude": 143.2104,
```

```
    "registered_country_code": "AU",  
    "country": "Australia",  
    "registered_country": "Australia",  
    "continent": "Oceania",  
    "timezone": "Australia/Sydney",  
    "country_code": "AU"  
  }  
}
```

submit_ip Mapping Table

ThreatQ provides the following default mapping for this operation action:

Provider Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples	Notes
.autonomous_system.name	Indicator.Attribute	Network	CLOUDFLARENET	N/A
.autonomous_system.routed_prefix	Indicator.Attribute	Routing	1.1.1.0/24	N/A
.autonomous_system.asn	Indicator.Attribute	ASN	13335	N/A
.tags	Indicator.Attribute	Tag	https	N/A
.25.smtp.starttls.metadata.product	Indicator.Attribute	SMTP Product	Postfix	N/A
.25.smtp.starttls.metadata.description	Indicator.Attribute	SMTP Product Description	Postfix	N/A
.25.smtp.starttls.banner	Indicator.Attribute	SMTP Banner	220 mx1.spbtv.com ESMTP Postfix	N/A
.587.smtp.starttls.metadata.product	Indicator.Attribute	SMTP Product	Postfix	N/A
.587.smtp.starttls.metadata.description	Indicator.Attribute	SMTP Product Description	Postfix	N/A
.587.smtp.starttls.banner	Indicator.Attribute	SMTP Banner	220 ps26.suite2.arena.ne.jp ESMTTP	N/A

Provider Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples	Notes
.53.dns.lookup.open_resolver	Indicator.Attribute	Open Resolution	True	N/A
.53.dns.lookup.resolves_correctly	Indicator.Attribute	Correct DNS Resolution	True	N/A
.53.dns.lookup.authorities.response	Indicator.Attribute	DNS Authority	g.root-servers.net	N/A
.protocols	Indicator.Attribute	Protocols	53/dns	N/A
.ports	Indicator.Attribute	Port	53	N/A
.location.country	Indicator.Attribute	Country	Australia	N/A
.location.country_code	Indicator.Attribute	Country Code	AU	N/A
.location.timezone	Indicator.Attribute	Timezone	Australia/Sydney	N/A

submit_domain

GET <https://censys.io/api/v1/view/websites> endpoint.

```
{
  "protocols": [
    "443/https_www",
    "443/https",
    "80/http_www",
    "25/smtp",
    "80/http"
  ],
  "updated_at": "2020-08-20T01:55:35+00:00",
  "tags": [
    "http",
    "smtp",
    "https"
  ],
  "25": {
    "smtp": {
      "starttls": {
        "metadata": {
          "product": "SMTP",
```

```
        "description": "Google SMTP",
        "manufacturer": "Google"
    },
    "ehlo": "250-mx.google.com at your service, [192.35.168.96]\\r\\n250-SIZE
157286400\\r\\n250-8BITMIME\\r\\n250-STARTTLS\\r\\n250-ENHANCEDSTATUSCODES\\r\\n250-PIPELINING\\r\\n250-
CHUNKING\\r\\n250 SMTPUTF8",
    "tls": {
        "version": "TLSv1.2",
        "certificate": {
            "parsed": {
                "version": 3,
                "fingerprint_md5": "f96d87fefff89b2d8adcd79ae7b7da50",
                "fingerprint_sha256": "06be8a7fe4736aaab32d5d-
d21de4d7874b344ddc6c018c5ce9f91a2922de3606",
                "validity": {
                    "end": "2020-10-07T08:33:07Z",
                    "length": 7257600,
                    "start": "2020-07-15T08:33:07Z"
                },
                "spki_subject_fingerprint": "643c23f-
b4e68b44af329ecdc1836173392b3d95c8b265683fa847011f023cd52",
```

```
"fingerprint_sha1": "98151355a11f39583d350517f7b67d2a27cb6060",
"redacted": false,
"signature_algorithm": {
  "name": "SHA256WithRSA",
  "oid": "1.2.840.113549.1.1.11"
},
"subject": {
  "common_name": [
    "mx.google.com"
  ],
  "country": [
    "US"
  ],
  "province": [
    "California"
  ],
  "organization": [
    "Google LLC"
  ],
  "locality": [
    "Mountain View"
  ]
}
```

```
    ]
  },
  "issuer": {
    "common_name": [
      "GTS CA 101"
    ],
    "country": [
      "US"
    ],
    "organization": [
      "Google Trust Services"
    ]
  },
  "tbs_fingerprint": "4d722c69e-
f680cbdf5b3fe7b0a866513c1c70c6d8a2a75418b25da7113a09fbb",
  "subject_dn": "C=US, ST=California, L=Mountain View, O=Google LLC,
CN=mx.google.com",
  "serial_number": "258996799351037845589150463252484693834",
  "issuer_dn": "C=US, O=Google Trust Services, CN=GTS CA 101",
  "validation_level": "OV",
  "names": [
```

```
"alt3.aspmx.l.google.com",  
"alt3.gmail-smtp-in.l.google.com",  
"alt4.gmail-smtp-in.l.google.com",  
"gmr-mx.google.com",  
"gmr-smtp-in.l.google.com",  
"aspmx.l.google.com",  
"alt1.aspmx.l.google.com",  
"alt1.gmail-smtp-in.l.google.com",  
"alt2.aspmx.l.google.com",  
"alt2.gmr-smtp-in.l.google.com",  
"alt3.gmr-smtp-in.l.google.com",  
"alt4.aspmx.l.google.com",  
"alt4.gmr-smtp-in.l.google.com",  
"aspmx3.googlemail.com",  
"aspmx4.googlemail.com",  
"mx3.smtp.goog",  
"mx.google.com",  
"alt1.gmr-smtp-in.l.google.com",  
"aspmx5.googlemail.com",  
"alt2.gmail-smtp-in.l.google.com",  
"aspmx2.googlemail.com",
```

```
        "gmail-smtp-in.l.google.com",
        "mx1.smtp.goog",
        "mx2.smtp.goog",
        "mx4.smtp.goog"
    ],
    "signature": {
        "valid": true,
        "value": "wRrD7RJm-
nXSm-
qDT3XKthz8NMhOg0wEvfJ8KYPlJJx07cPEF50-
leyeOyFyHAd-
pzfJ2Zs+/5/6i2WrxxRu8SjBqLyqWYC6cnkQoZUzZ2XWs6I-
vodxLf-
bwNd-
hX3mOwHIp30gvwUxb5ii/Rzx4u8JAySLZZ+0lWx-
sx032dS7SXm43BiBCXXv-
viM3eqZsXJPKQxfPLyqJhOV+hMDEB-
faj-
grWsIBHNBq0q53zRheCp-
mEjneDZ6NO/AWSZySZE5PBM7ao-
jMojveRbLijEvZ1CvvceYnc9a10Qqbmikfr7rw4WRzCykiqx24+WpvF1bj3nFHOJSHs4JAotdSjCxkI+aE1J1KVA=="
```

```
        "self_signed": false,
        "signature_algorithm": {
            "name": "SHA256WithRSA",
            "oid": "1.2.840.113549.1.1.11"
        }
    },
    "tbs_noct_fingerprint": "98bf-
b044142fb715371c22aafa47b52c819d825416eb82c351bcdd7e5c74e6d4",
    "subject_key_info": {
        "fingerprint_sha256": "03c27e15b-
c9dd74a6c0375644e552b0df292b2095f58eab86a1a0de3df576375",
        "key_algorithm": {
            "name": "ECDSA"
        },
        "ecdsa_public_key": {
            "n": "////////wAAAD/////////7zm+q2nF56E87nKwvxjJVE=",
            "gx": "axfR8uEsQkf4vOblY6RA8ncDfYEt6zOg9KE5RdiYwpY=",
            "p": "////////wAAAEAAAAAAAAAAAAAAAAAAD/////////8=",
            "gy": "T+NC4v4af5uO5+tKfA+eFivOMldrMV7Oy7ZAaDe/UfU=",
            "y": "encZbh6GY0H4BNVqkNdLbZz3VjFiaoeJCosjpDJCEdE=",
            "length": 256,
```

```
        "pub": "BMe-  
f5piAUQ6IGUo4x0skv6tQxZ8O9kmvh8anQnuZD4Z5encZbh6GY0H4BNVqkNdLbZz3VjFiaoeJCosjpDJCEdE=",  
        "b": "WsY12Ko6k+ez671VdpiGvGUdBrDMU7D2O848PifSYEs=",  
        "curve": "P-256",  
        "x": "x5/mmIBRDogZSjjHSyS/q1DFnw72Sa+HxqdCe5kPhnk="
```

```
    },  
    "extensions": {  
        "authority_info_access": {  
            "ocsp_urls": [  
                "http://ocsp.pki.goog/gts1o1core"  
            ],  
            "issuer_urls": [  
                "http://pki.goog/gsr2/GTS101.crt"  
            ]  
        },  
        "key_usage": {  
            "value": 1,  
            "digital_signature": true  
        },  
        "certificate_policies": [  
            {  
                "policy_identifier": "2.5.2.1",  
                "policy_qualifiers": [  
                    {  
                        "policy_qualifier": "c",  
                        "policy_qualifier_reason": "1"  
                    }  
                ]  
            }  
        ]  
    }  
}
```

```
{
  "id": "2.23.140.1.2.2"
},
{
  "id": "1.3.6.1.4.1.11129.2.5.3"
}
],
"extended_key_usage": {
  "server_auth": true
},
"subject_alt_name": {
  "dns_names": [
    "mx.google.com",
    "alt1.aspmx.l.google.com",
    "alt1.gmail-smtp-in.l.google.com",
    "alt1.gmr-smtp-in.l.google.com",
    "alt2.aspmx.l.google.com",
    "alt2.gmail-smtp-in.l.google.com",
    "alt2.gmr-smtp-in.l.google.com",
    "alt3.aspmx.l.google.com",
    "alt3.gmail-smtp-in.l.google.com",
```

```
        "alt3.gmr-smtp-in.l.google.com",
        "alt4.aspmx.l.google.com",
        "alt4.gmail-smtp-in.l.google.com",
        "alt4.gmr-smtp-in.l.google.com",
        "aspmx.l.google.com",
        "aspmx2.googlemail.com",
        "aspmx3.googlemail.com",
        "aspmx4.googlemail.com",
        "aspmx5.googlemail.com",
        "gmail-smtp-in.l.google.com",
        "gmr-mx.google.com",
        "gmr-smtp-in.l.google.com",
        "mx1.smtp.goog",
        "mx2.smtp.goog",
        "mx3.smtp.goog",
        "mx4.smtp.goog"
    ]
},
"authority_key_id": "98d1f86e10ebcf9bec609f18901ba0eb7d09fd2b",
"crl_distribution_points": [
    "http://crl.pki.goog/GTS101core.crl"
```

```
    ],
    "basic_constraints": {
        "is_ca": false
    },
    "subject_key_id": "31517f9fe7a880237e25e55e5e1a4d26d3284756",
    "signed_certificate_timestamps": [
        {
            "timestamp": 1594805589,
            "version": 0,
            "signature": "BAMASDBGAiEAvqvnQIP1Eao-
j598B9/xdjO4j2+1oKGJ2KS1mGxJB/a0CIQCWtLXGRx9u7Bs4l/X7C24brBSXIO6vvw4N5IanqGD/Nw==",
            "log_id": "xlKg7EjOs/yrFwmSxDqHQTMJ6ABlomJSQBujNioXxWU="
        },
        {
            "timestamp": 1594805589,
            "version": 0,
            "signature":
"BAMARzBFAiBCVIdRc4ff0PAbe2U0BBwlZQyINyImIDkG+UTZyWt4r-
gIhAMKPtNWMZJPAY1b/qiMxiPri1BUuPhsELa5wf3KITI0n",
            "log_id": "B7dcG+V9aP/xsMYdIxXHuuZXfFeUt2ruvGE6GmnTohw="
        }
    ]
}
```

```
    ]
  }
}
},
"chain": [
  {
    "parsed": {
      "version": 3,
      "fingerprint_md5": "dbb23c939236012e71d5f44dbc2acea0",
      "fingerprint_sha256": "95c074e35902a14-
abd9d19afb6e7f80e669ff8e2363270539d963613f04aaa21",
      "validity": {
        "end": "2021-12-15T00:00:42Z",
        "length": 142041600,
        "start": "2017-06-15T00:00:42Z"
      },
      "spki_subject_fingerprint": "6c9383467570b9fcf2e32d84-
fafbd22e82303d7a314dcd184a0face36bf51087",
      "fingerprint_sha1": "dfe2070c79e7ff36a925ffa327ffe3deecf8f9c2",
      "redacted": false,
      "signature_algorithm": {
```

```
        "name": "SHA256WithRSA",
        "oid": "1.2.840.113549.1.1.11"
    },
    "subject": {
        "common_name": [
            "GTS CA 101"
        ],
        "country": [
            "US"
        ],
        "organization": [
            "Google Trust Services"
        ]
    },
    "issuer": {
        "common_name": [
            "GlobalSign"
        ],
        "organizational_unit": [
            "GlobalSign Root CA - R2"
        ],
    },
```

```
        "organization": [  
            "GlobalSign"  
        ],  
    },  
    "tbs_fingerprint": "76802447a019931a3f004304c53f-  
dc6c1b2c378dc4be8f73b39fd9c969dfb445",  
    "subject_dn": "C=US, O=Google Trust Services, CN=GTS CA 101",  
    "serial_number": "149699596615803609916394524856",  
    "issuer_dn": "OU=GlobalSign Root CA - R2, O=GlobalSign, CN=-  
=GlobalSign",  
    "validation_level": "OV",  
    "signature": {  
        "valid": true,  
        "value": "GoA+Nn-  
n78y6pRjd9XlQWNa7HT-  
giZ/r3RNGk-  
mUmYHPQq6Scti9PEa-  
jvwRT2iWTHQr02fesqOqBY2ETUwgZQ+ll-  
toNFvh-  
sO9tvBCOIazpswWC9aJ9xju4tWDQH8NVU6YZZ/XteDSGU9YzJqPjY8q3MDxrm-
```

```
qepBCf5o8m-  
w/wJ4a2G6xzUr6Fb6T8McDO22PLRL6u3M4Tz-  
s3A2M1j6bykJYi8wWIRdAvKLWZu/axBVbzYm-  
qmwk-  
m5zLSDW5nIAJbELCQCZwMH56t2Dvqofx-  
s6BBcCFIZUSpxu6x6td0V7SvJCCosirSmIatj/9dSSVDQibet8q/7UK4v4ZUN80atnZz1yg==",  
    "self_signed": false,  
    "signature_algorithm": {  
        "name": "SHA256WithRSA",  
        "oid": "1.2.840.113549.1.1.11"  
    },  
    "tbs_noct_fingerprint": "76802447a019931a3f004304c53f-  
dc6c1b2c378dc4be8f73b39fd9c969dfb445",  
    "subject_key_info": {  
        "rsa_public_key": {  
            "length": 2048,  
            "exponent": 65537,  
            "modulus": "0BjPRdSLzdOc5EDv-  
frTdaSEbyc88jkx1uQ8xGYQ9n-
```

```
jwp71ANEJNvBYCAnyqgvRJLAuE9n1gWJP4wn-  
wt0d1WTHUv3TeGSghD2UawMw7IilA80a5gQSecLnYM53SDGHC3v0Rh-  
hZecjgyCoIxL/0iR/1C/nRGp-  
bTd-  
dQZrCvnkJjBfvGHRjYa+-  
fajP/Ype9SNnTfBRn3HXcLm-  
no+G14adC3EAW48THCOyT9GjN0+CPg7GsZi-  
hbG482kzQvb-  
s6RZYDiIO60ducaMp1Mb/LzZpKu83Txh15MVmO6BvY/iZEcgQAZO16yX6LnAWRKhSSUj5O1wNCyltGN8+aM9g9HNbSSsBw=="  
    },  
    "fingerprint_sha256": "6193e04d9f-  
b0a0d0820885b72c7d82c5078bcc1ff59b8d907024c149d81aca3b",  
    "key_algorithm": {  
        "name": "RSA"  
    },  
    "extensions": {  
        "authority_info_access": {  
            "ocsp_urls": [  
                "http://ocsp.pki.goog/gsr2"  
            ]  
        }  
    }  
}
```

```
    },
    "key_usage": {
      "crl_sign": true,
      "value": 97,
      "digital_signature": true,
      "certificate_sign": true
    },
    "certificate_policies": [
      {
        "cps": [
          "https://pki.goog/repository/"
        ],
        "id": "2.23.140.1.2.2"
      }
    ],
    "extended_key_usage": {
      "client_auth": true,
      "server_auth": true
    },
    "authority_key_id": "9be20757671c1ec06a06de59b49a2dd-
fdc19862e",
```

```
        "basic_constraints": {
            "is_ca": true,
            "max_path_len": 0
        },
        "crl_distribution_points": [
            "http://crl.pki.goog/gsr2/gsr2.crl"
        ],
        "subject_key_id": "98d1f86e10ebcf9bec609f18901ba0eb7d09fd2b"
    }
}

},
"signature": {
    "valid": true,
    "hash_algorithm": "sha256",
    "signature_algorithm": "ecdsa"
},
"ocsp_stapling": false,
"server_key_exchange": {
    "ecdh_params": {
        "curve_id": {
```

```
        "id": 23,
        "name": "secp256r1"
    }
}
},
"cipher_suite": {
    "id": "0xC02B",
    "name": "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256"
},
"validation": {
    "browser_trusted": true
}
},
"banner": "220 mx.google.com ESMTP u14si27940347jat.53 - gsmtip",
"starttls": "220 2.0.0 Ready to start TLS"
}
}
},
"80": {
    "http": {
        "get": {
```

```
"status_line": "200 OK",
"headers": {
  "x_frame_options": "SAMEORIGIN",
  "server": "gws",
  "content_type": "text/html; charset=UTF-8",
  "expires": "-1",
  "x_xss_protection": "0",
  "unknown": [
    {
      "value": "Wed, 19 Aug 2020 09:02:51 GMT",
      "key": "date"
    }
  ],
  "p3p": "CP=\\\"This is not a P3P policy! See g.co/p3phelp for more info.\\\"",
  "cache_control": "private, max-age=0"
},
"title": "Google",
"body": "<!doctype html><html itemscope=\\\"\\\" item-
type=\\\"http://schema.org/WebPage\\\" lang=\\\"en\\\"><meta content=\\\"Search the world's information,
including webpages, images, videos and more. Google has many special features to help you find
exactly what you're looking for.\\\" name=\\\"description\\\"></script></body></html>",
```

```
    "body_sha256": "576e5ee61b82c1426d-
c1ccf88da552619620fb0da0952d2e4f4f916b85dca9dc",
    "metadata": {
        "product": "Web Server",
        "description": "Google Web Server",
        "manufacturer": "Google"
    },
    "status_code": 200
}
},
"http_www": {
    "get": {
        "status_line": "200 OK",
        "headers": {
            "x_frame_options": "SAMEORIGIN",
            "server": "gws",
            "content_type": "text/html; charset=UTF-8",
            "expires": "-1",
            "x_xss_protection": "0",
            "unknown": [
                {
```

```
        "value": "Wed, 19 Aug 2020 12:02:51 GMT",
        "key": "date"
    }
],
    "p3p": "CP=\"This is not a P3P policy! See g.co/p3phelp for more info.\",
    "cache_control": "private, max-age=0"
},
    "title": "Google",
    "body": "<!doctype html><html itemscope=\"\" item-
type=\"http://schema.org/WebPage\" lang=\"en\"><meta content=\"Search the world's information,
including webpages, images, videos and more. Google has many special features to help you find
exactly what you're looking for.\" name=\"description\"><meta content=\"noodp\" name-
e=\"robots\"><meta content=\"text/html; (.....)</script></body></html>",
    "body_sha256": "d584a74ba21c20d3ealecbae8f0f931e26b51c-
c86c09fc687e9f66818f675a78",
    "metadata": {},
    "status_code": 200
}
},
    "443": {
```

```
"https_www": {
  "tls": {
    "version": "TLSv1.2",
    "certificate": {
      "parsed": {
        "version": 3,
        "fingerprint_md5": "afe7eaa32c7dff2935d6a68c98a02357",
        "fingerprint_sha256": "f45771f0874949fe10c72f569d7bca4a24c69b9b-
fc2f3011d8f25a5b4329ce01",
        "validity": {
          "end": "2020-10-07T08:29:16Z",
          "length": 7257600,
          "start": "2020-07-15T08:29:16Z"
        },
        "spki_subject_fingerprint": "50ba3e700ce-
f964b68d6190919412f89a630d1504e9d75149fc71c09211f7351",
        "fingerprint_sha1": "f8940f5dc69e48ab4ad8fa8393b053a12e7d4c54",
        "redacted": false,
        "signature_algorithm": {
          "name": "SHA256WithRSA",
          "oid": "1.2.840.113549.1.1.11"
```

```
    },  
    "subject": {  
      "common_name": [  
        "*.google.com"  
      ],  
      "country": [  
        "US"  
      ],  
      "province": [  
        "California"  
      ],  
      "organization": [  
        "Google LLC"  
      ],  
      "locality": [  
        "Mountain View"  
      ]  
    },  
    "issuer": {  
      "common_name": [  
        "GTS CA 101"  
      ]  
    }  
  }  
}
```

```
    ],  
    "country": [  
        "US"  
    ],  
    "organization": [  
        "Google Trust Services"  
    ]  
},  
"tbs_fingerprint": "0397ee-  
b84cf79244c13851135375593e52d66bc07427444a1ee1314fbaf6fe22",  
"subject_dn": "C=US, ST=California, L=Mountain View, O=Google LLC,  
CN=*.google.com",  
"serial_number": "3497534328382008347086678290465016940",  
"issuer_dn": "C=US, O=Google Trust Services, CN=GTS CA 101",  
"validation_level": "OV",  
"names": [  
    "*.g.co",  
    "*.google.com.ar",  
    "*.googlecnapps.cn",  
    "*.gkecnapps.cn",  
    "*.yt.be",
```

```
"gkecnapps.cn",  
"www.goo.gl",  
"youtu.be",  
"youtubeeducation.com",  
"*.google.com",  
"*.appengine.google.com",  
"*.cloud.google.com",  
"*.gcpcdn.gvt1.com",  
"*.google.ca",  
"*.google.com.co",  
"*.gvt2.com",  
"*.google.es",  
"*.google.pl",  
"*.youtubeeducation.com",  
"*.youtubekids.com",  
"developer.android.google.cn",  
"source.android.google.cn",  
"*.crowdsourcing.google.com",  
"*.google.co.jp",  
"*.google.hu",  
"*.google.nl",
```

```
"*.googleadapis.com",  
"ggpht.cn",  
"*.google.com.mx",  
"*.google.com.vn",  
"*.google.de",  
"*.google.fr",  
"*.gstaticcnapps.cn",  
"*.metric.gstatic.com",  
"*.url.google.com",  
"youtubekids.com",  
"*.android.com",  
"*.bdn.dev",  
"*.googlevideo.com",  
"google.com",  
"youtube.com",  
"*.google.co.uk",  
"*.google.it",  
"*.wear.gkecnapps.cn",  
"*.google.com.br",  
"*.gstatic.cn",  
"google-analytics.com",
```

```
"googlecnapps.cn",  
"urchin.com",  
"yt.be",  
"*.google.com.tr",  
"*.googleapis.cn",  
"*.googlecommerce.com",  
"*.youtube-nocookie.com",  
"*.gcp.gvt2.com",  
"*.google.cl",  
"googlecommerce.com",  
"*.google-analytics.com",  
"*.gstatic.com",  
"*.urchin.com",  
"android.com",  
"*.ggpht.cn",  
"*.google.com.au",  
"android.clients.google.com",  
"*.google.pt",  
"*.ytimg.com",  
"developers.android.google.cn",  
"goo.gl",
```

```
        "*.google.co.in",
        "*.gvt1.com",
        "*.youtube.com",
        "g.co"
    ],
    "signature": {
        "valid": true,
        "value": "yzIb5DCEiNDvsZowwZHKG6c8DK0Ob-
bX+Av9ekZyn-
VI+Qas67QgYvBShWqXwU7pjBqX2mQHa4c64rUir-
rblAA26TgPBV5RM2BrJCoX0zA5dTPOXAlZBCkCMm+Im9jfdZF5sa3HGHuUQE4DIt8zFhkzdVwOYUaaXuaH0f9n-
vq32Acve+P4ab2YSaSo4j1yc-
q4tKf4dJuSIDSXyUmH1m-
rPeToCikV2CFul/ZKu8b-
vqZpK2xjFbReHl4Aay+9jREHNH4dC+ZgFMSJ2qo4KGgAXzYo0tlezD5YDD+-
grm99ihmubmBlAbweJfAfPMxR07AFAb5oK/C4BU0BoDz+oFyo9skmw==",
        "self_signed": false,
        "signature_algorithm": {
            "name": "SHA256WithRSA",
            "oid": "1.2.840.113549.1.1.11"
        }
    }
}
```

```
    },
    "tbs_noct_fingerprint": "78f9b0162ef-
d1b50a6f08ecdcc6ad75ebe8658646036370b52fd895dafae451a",
    "subject_key_info": {
        "fingerprint_sha256": "e55134a3186f-
bba48c9ae323baa9f5fb1c8108e745bc8d2483ab48ed06da4911",
        "key_algorithm": {
            "name": "ECDSA"
        },
        "ecdsa_public_key": {
            "n": "////////wAAAD/////////7zm+q2nF56E87nKwvxjJVE=",
            "gx": "axfR8uEsQkf4vOblY6RA8ncDfYEt6zOg9KE5RdiYwpY=",
            "p": "////////wAAAEAAAAAAAAAAAAAAAAAAD//////////8=",
            "gy": "T+NC4v4af5uO5+tKfA+eFivOMldrMV7Oy7ZAaDe/UfU=",
            "y": "nvE/9EPQrWiNGF+XgwBk3RSWuHKoiO/d5Cqs/tVh88=",
            "length": 256,
            "pub": "BOKBMK+yIazADk2Iy94Zn9IlCu6Re-
fcurqTfUeYwzuiHnvE/9EPQrWiNGF+XgwBk3RSWuHKoiO/d5Cqs/tVh88=",
            "b": "WsY12Ko6k+ez671VdpiGvGUdBrDMU7D2O848PifSYEs=",
            "curve": "P-256",
            "x": "4oEwr7IhrMAOTYjL3hmf0iUK7pF59y6upN9R5jDO6Ic="
```

```
    }  
  },  
  "extensions": {  
    "authority_info_access": {  
      "ocsp_urls": [  
        "http://ocsp.pki.goog/gts1o1core"  
      ],  
      "issuer_urls": [  
        "http://pki.goog/gsr2/GTS1O1.crt"  
      ]  
    },  
    "key_usage": {  
      "value": 1,  
      "digital_signature": true  
    },  
    "certificate_policies": [  
      {  
        "id": "2.23.140.1.2.2"  
      },  
      {  
        "id": "1.3.6.1.4.1.11129.2.5.3"
```

```
    }  
  ],  
  "extended_key_usage": {  
    "server_auth": true  
  },  
  "subject_alt_name": {  
    "dns_names": [  
      "*.google.com",  
      "*.android.com",  
      "*.appengine.google.com",  
      "*.bdn.dev",  
      "*.cloud.google.com",  
      "*.crowdsource.google.com",  
      "*.g.co",  
      "*.gcp.gvt2.com",  
      "*.gcpcdn.gvt1.com",  
      "*.ggpht.cn",  
      "*.gkecnapps.cn",  
      "*.google-analytics.com",  
      "*.google.ca",  
      "*.google.cl",
```

```
"*.google.co.in",  
".google.co.jp",  
".google.co.uk",  
".google.com.ar",  
".google.com.au",  
".google.com.br",  
".google.com.co",  
".google.com.mx",  
".google.com.tr",  
".google.com.vn",  
".google.de",  
".google.es",  
".google.fr",  
".google.hu",  
".google.it",  
".google.nl",  
".google.pl",  
".google.pt",  
".googleapis.com",  
".googleapis.cn",  
".googlecnapps.cn",
```

```
"*.googlecommerce.com",  
"*.googlevideo.com",  
"*.gstatic.cn",  
"*.gstatic.com",  
"*.gstaticcnapps.cn",  
"*.gvt1.com",  
"*.gvt2.com",  
"*.metric.gstatic.com",  
"*.urchin.com",  
"*.url.google.com",  
"*.wear.gkecnapps.cn",  
"*.youtube-nocookie.com",  
"*.youtube.com",  
"*.youtubeeducation.com",  
"*.youtubekids.com",  
"*.yt.be",  
"*.yting.com",  
"android.clients.google.com",  
"android.com",  
"developer.android.google.cn",  
"developers.android.google.cn",
```

```
        "g.co",
        "ggpht.cn",
        "gkecnapps.cn",
        "goo.gl",
        "google-analytics.com",
        "google.com",
        "googlecnapps.cn",
        "googlecommerce.com",
        "source.android.google.cn",
        "urchin.com",
        "www.goo.gl",
        "youtu.be",
        "youtube.com",
        "youtubeeducation.com",
        "youtubekids.com",
        "yt.be"
    ]
},
"authority_key_id": "98d1f86e10ebcf9bec609f18901ba0eb7d09fd2b",
"crl_distribution_points": [
    "http://crl.pki.goog/GTS101core.crl"
```

```
    ],
    "basic_constraints": {
      "is_ca": false
    },
    "subject_key_id": "45efc0802d907461fcec25d7892f3f8b6d570eec",
    "signed_certificate_timestamps": [
      {
        "timestamp": 1594805363,
        "version": 0,
        "signature": "BAMASDBGAiEAlsUu2N-
prTTur/KX90fdYN/3Rp+UuuZIa5UJ8wzqRUboCIQDgK2gL9j/Xc7KAwfEMNd4lvGuglCP4BXgZtA6XCKnb0g==",
        "log_id": "5xLysDd+GmL7jskMYyTx6ns3y1YdESZb8+DzS/JBVG4="
      },
      {
        "timestamp": 1594805363,
        "version": 0,
        "signature": "BAMARjBEAiBBJIIfY7toc1ZLc9VD9HWuSQAfZH-
fofEMUh0iSyhV4I+gIgUodhyrGiOa5W2f+EEln4GoA5z9eOC7Rhq4pJZRlDF0M=",
        "log_id": "B7dcG+V9aP/xsMYdIxXHuuZXfFeUt2ruvGE6GmnTohw="
      }
    ]
  ]
```

```
    }  
  }  
},  
"chain": [  
  {  
    "parsed": {  
      "version": 3,  
      "fingerprint_md5": "dbb23c939236012e71d5f44dbc2acea0",  
      "fingerprint_sha256": "95c074e35902a14-  
abd9d19afb6e7f80e669ff8e2363270539d963613f04aaa21",  
      "validity": {  
        "end": "2021-12-15T00:00:42Z",  
        "length": 142041600,  
        "start": "2017-06-15T00:00:42Z"  
      },  
      "spki_subject_fingerprint": "6c9383467570b9fcf2e32d84-  
fafbd22e82303d7a314dcd184a0face36bf51087",  
      "fingerprint_sha1": "dfe2070c79e7ff36a925ffa327ffe3deecf8f9c2",  
      "redacted": false,  
      "signature_algorithm": {  
        "name": "SHA256WithRSA",
```

```
        "oid": "1.2.840.113549.1.1.11"
    },
    "subject": {
        "common_name": [
            "GTS CA 101"
        ],
        "country": [
            "US"
        ],
        "organization": [
            "Google Trust Services"
        ]
    },
    "issuer": {
        "common_name": [
            "GlobalSign"
        ],
        "organizational_unit": [
            "GlobalSign Root CA - R2"
        ],
        "organization": [
```

```
        "GlobalSign"
      ],
    },
    "tbs_fingerprint": "76802447a019931a3f004304c53f-
dc6c1b2c378dc4be8f73b39fd9c969dfb445",
    "subject_dn": "C=US, O=Google Trust Services, CN=GTS CA 101",
    "serial_number": "149699596615803609916394524856",
    "issuer_dn": "OU=GlobalSign Root CA - R2, O=GlobalSign, CN=-
=GlobalSign",
    "validation_level": "OV",
    "signature": {
      "valid": true,
      "value": "GoA+Nn-
n78y6pRjd9XlQWNa7HT-
giZ/r3RNGk-
mUmYHPQq6Scti9PEa-
jvwRT2iWTHQr02fesqOqBY2ETUwgZQ+ll-
toNFvh-
sO9tvBCOIazpswWC9aJ9xju4tWDQH8NVU6YZZ/XteDSGU9YzJqPjY8q3MDxrzm-
qepBCf5o8m-
```

```
w/wJ4a2G6xzUr6Fb6T8McDO22PLRL6u3M4Tz-  
s3A2M1j6bykJYi8wWIRdAvKLWZu/axBVbzYm-  
qmwk-  
m5zLSDW5nIAJbELCQCZwMH56t2Dvqofx-  
s6BBcCFIZUSpxu6x6td0V7SvJCCosirSmIatj/9dSSVDQibet8q/7UK4v4ZUN80atnZz1yg==",  
    "self_signed": false,  
    "signature_algorithm": {  
        "name": "SHA256WithRSA",  
        "oid": "1.2.840.113549.1.1.11"  
    },  
    "tbs_noct_fingerprint": "76802447a019931a3f004304c53f-  
dc6c1b2c378dc4be8f73b39fd9c969dfb445",  
    "subject_key_info": {  
        "rsa_public_key": {  
            "length": 2048,  
            "exponent": 65537,  
            "modulus": "0BjPRdSLzdOc5EDv-  
frTdaSEbyc88jKx1uQ8xGYQ9n-  
jwp71ANEJNvBYCAnyqgvRJLAuE9n1gWJP4wn-
```

```
wt0d1WTHUv3TeGSghD2UawMw7IilA80a5gQSecLnYM53SDGHC3v0Rh-  
hZecjgyCoIxL/0iR/1C/nRGp-  
bTd-  
dQZrCvnkJjBfvGHRjYa+-  
fajP/Ype9SNnTfBRn3HXcLm-  
no+G14adC3EAW48THCOyT9GjN0+CPg7GsZi-  
hbG482kzQvb-  
s6RZYDiIO60ducaMp1Mb/LzZpKu83Txh15MVmO6BvY/iZEcgQAZO16yX6LnAWRKhSSUj501wNCy1tGN8+aM9g9HNbSSsBw=="  
    },  
    "fingerprint_sha256": "6193e04d9f-  
b0a0d0820885b72c7d82c5078bcc1ff59b8d907024c149d81aca3b",  
    "key_algorithm": {  
      "name": "RSA"  
    }  
  },  
  "extensions": {  
    "authority_info_access": {  
      "ocsp_urls": [  
        "http://ocsp.pki.goog/gsr2"  
      ]  
    }  
  },
```

```
"key_usage": {
  "crl_sign": true,
  "value": 97,
  "digital_signature": true,
  "certificate_sign": true
},
"certificate_policies": [
  {
    "cps": [
      "https://pki.goog/repository/"
    ],
    "id": "2.23.140.1.2.2"
  }
],
"extended_key_usage": {
  "client_auth": true,
  "server_auth": true
},
"authority_key_id": "9be20757671c1ec06a06de59b49a2ddfdc19862e",
"basic_constraints": {
  "is_ca": true,
```

```
        "max_path_len": 0
      },
      "crl_distribution_points": [
        "http://crl.pki.goog/gsr2/gsr2.crl"
      ],
      "subject_key_id": "98d1f86e10ebcf9bec609f18901ba0eb7d09fd2b"
    }
  }
}
},
"session_ticket": {
  "length": 221,
  "lifetime_hint": 100800
},
"signature": {
  "valid": true,
  "hash_algorithm": "sha256",
  "signature_algorithm": "ecdsa"
},
"ocsp_stapling": false,
"metadata": {},
```

```
    "server_key_exchange": {
      "ecdh_params": {
        "curve_id": {
          "id": 23,
          "name": "secp256r1"
        }
      }
    },
    "cipher_suite": {
      "id": "0xC02B",
      "name": "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256"
    },
    "validation": {
      "matches_domain": true,
      "browser_trusted": true
    }
  },
  "https": {
    "get": {
      "status_line": "200 OK",
```

```
"headers": {
  "x_frame_options": "SAMEORIGIN",
  "server": "gws",
  "content_type": "text/html; charset=UTF-8",
  "alt_svc": "h3-29=\":443\"; ma=2592000,h3-27=\":443\"; ma=2592000,h3-T050-
0=\":443\"; ma=2592000,h3-Q050=\":443\"; ma=2592000,h3-Q046=\":443\"; ma=2592000,h3-Q043-
3=\":443\"; ma=2592000,quic=\":443\"; ma=2592000; v=\\\"46,43\\\"",
  "expires": "-1",
  "x_xss_protection": "0",
  "unknown": [
    {
      "value": "Tue, 18 Aug 2020 09:02:12 GMT",
      "key": "date"
    }
  ],
  "p3p": "CP=\\\"This is not a P3P policy! See g.co/p3phelp for more info.\\\"",
  "cache_control": "private, max-age=0"
},
"title": "Google",
"body": "<!doctype html><html itemscope=\\\"\\\" item-
type=\\\"http://schema.org/WebPage\\\" lang=\\\"en\\\"><meta content=\\\"Search the world's information,
```

including webpages, images, videos and more. Google has many special features to help you find exactly what you're looking for.\"(.....)</body></html>\",

```
    "body_sha256": "9d9150ed44a71019299938a479528fe-  
b328170a6e0ca61b5b73af21fd09734b5",  
    "metadata": {  
        "product": "Web Server",  
        "description": "Google Web Server",  
        "manufacturer": "Google"  
    },  
    "status_code": 200  
},  
"dhe": {  
    "support": false,  
    "metadata": {}  
},  
"dhe_export": {  
    "support": false,  
    "metadata": {}  
},  
"heartbleed": {  
    "metadata": {},
```

```
        "heartbleed_vulnerable": false,
        "heartbeat_enabled": false
    },
    "rsa_export": {
        "support": false,
        "metadata": {}
    },
    "tls": {
        "version": "TLSv1.2",
        "certificate": {
            "parsed": {
                "version": 3,
                "fingerprint_md5": "80fc9957756dd651bc46a128d96c0afc",
                "fingerprint_sha256": "00df652de98a1e8721c-
c8a20ab274ae741fe82510cd09f748cf0f8cadbf731cb",
                "validity": {
                    "end": "2020-11-03T08:53:40Z",
                    "length": 7257600,
                    "start": "2020-08-11T08:53:40Z"
                },
                "spki_subject_fingerprint":
```

```
"46f8a50e7f42cd9f464528212fe6610fa252b1479b134915b69f1efcb15ceb6d",
  "fingerprint_sha1": "cdcf6523dc03a889c9964950481f3ab9651b75b9",
  "redacted": false,
  "signature_algorithm": {
    "name": "SHA256WithRSA",
    "oid": "1.2.840.113549.1.1.11"
  },
  "subject": {
    "common_name": [
      "*.google.com"
    ],
    "country": [
      "US"
    ],
    "province": [
      "California"
    ],
    "organization": [
      "Google LLC"
    ],
    "locality": [
```

```
        "Mountain View"
    ],
},
"issuer": {
    "common_name": [
        "GTS CA 101"
    ],
    "country": [
        "US"
    ],
    "organization": [
        "Google Trust Services"
    ]
},
"tbs_fingerprint": "76f84653cde42673c0b6ecb-
dc07bffdec554fae3fdbcd27c24bd1b552ca312cb",
"subject_dn": "C=US, ST=California, L=Mountain View, O=Google LLC,
CN=*.google.com",
"serial_number": "278189548220930011386135995087617989858",
"issuer_dn": "C=US, O=Google Trust Services, CN=GTS CA 101",
"validation_level": "OV",
```

```
"names": [  
    "*.yting.com",  
    "android.clients.google.com",  
    "*.google.com.br",  
    "*.youtube.com",  
    "*.google.cl",  
    "*.google.de",  
    "*.google.nl",  
    "*.google.com",  
    "*.ggpht.cn",  
    "*.googlecommerce.com",  
    "*.gvt2.com",  
    "*.google.it",  
    "*.google.pt",  
    "*.google.com.tr",  
    "*.youtubeeducation.com",  
    "developer.android.google.cn",  
    "*.gkecnapps.cn",  
    "*.google.com.co",  
    "*.yt.be",  
    "developers.android.google.cn",
```

```
"*.google.ca",  
"*.google.com.ar",  
"*.gcp.gvt2.com",  
"*.google.com.au",  
"*.android.com",  
"*.crowdssource.google.com",  
"*.gstatic.com",  
"*.urchin.com",  
"*.google.hu",  
"*.googlecnapps.cn",  
"*.gstatic.cn",  
"*.gstaticcnapps.cn",  
"gkecnapps.cn",  
"google.com",  
"*.appengine.google.com",  
"*.gcpcdn.gvt1.com",  
"*.google.co.uk",  
"*.url.google.com",  
"g.co",  
"ggpht.cn",  
"googlecnapps.cn",
```

```
"youtube.com",  
"*.cloud.google.com",  
"*.g.co",  
"youtubeeducation.com",  
"google-analytics.com",  
"*.google.es",  
"*.googlevideo.com",  
"*.google.co.in",  
"*.youtubekids.com",  
"urchin.com",  
"*.google.com.vn",  
"*.googleapis.cn",  
"googlecommerce.com",  
"*.bdn.dev",  
"*.google.pl",  
"www.goo.gl",  
"youtu.be",  
"yt.be",  
"*.google.fr",  
"android.com",  
"*.youtube-nocookie.com",
```

```
        "goo.gl",
        "source.android.google.cn",
        "*.google.co.jp",
        "*.gvt1.com",
        "*.googleadapis.com",
        "*.metric.gstatic.com",
        "*.wear.gkecnapps.cn",
        "youtubekids.com",
        "*.google-analytics.com",
        "*.google.com.mx"
    ],
    "signature": {
        "valid": true,
        "value": "nTjC6jUw2LkYQwq3Gm3NWm-
cxNTe8m0bEZ0G2S1g+h-
m22pH8Ef5hMUesxxShMpjx0UeAhCvxjB4MJxD55Zq1AjBsLfGem2rtSLOHs-
gWUKYa1E0QMVcURkT2fBnI/VDpZVqgMCoT6WAiCEum-
rT96yn-
H7u77HakLMcTIKpsuUod/2DcCE0UqqZvOZSR8EcEK11sHztNvGHIAAQxvdVe-
fHEOFF2ozgREPx+CviHd0H2w-
```

```
cYqhOFaMqOVbEIOWn-
pPHygsJbNFN1cjLoEB/vNLvyC14Xc4H3LPjPCWTiAulvBLJJQ9nmggAgaEg7/9bs6da47V5awlyEAKzzmHGAmcNpX71Q=="
    "self_signed": false,
    "signature_algorithm": {
      "name": "SHA256WithRSA",
      "oid": "1.2.840.113549.1.1.11"
    }
  },
  "tbs_noct_fingerprint":
"8f977ff924e60c95449c6d158e0b764647e0a7c651780088bd03aa5ef33fa15f",
  "subject_key_info": {
    "fingerprint_sha256": "0a6f-
b0f123b24a114deaa9b6ec8a33c2141a04ed10b66c625a6fd6cd67c94269",
    "key_algorithm": {
      "name": "ECDSA"
    }
  },
  "ecdsa_public_key": {
    "n": "////////wAAAD/////////7zm+q2nF56E87nKwvxjJVE=",
    "gx": "axfR8uEsQkf4vOblY6RA8ncDfYEt6zOg9KE5RdiYwpY=",
    "p": "////////wAAAAEAAAAAAAAAAAAAAAAAD/////////8=",
    "gy": "T+NC4v4af5uO5+tKfA+eFivOM1drMV7Oy7ZAaDe/UfU=",
```

```
        "y": "UnzHoAW1cluuLzNNfWn13DMO+P+lRAJo5qjZACqnrS4=",
        "length": 256,
        "pub": "BBBi6xIe49OBCspU7MQn-
r9aBJ3rBB2O42R72xcWGNP5rUnzHoAW1cluuLzNNfWn13DMO+P+lRAJo5qjZACqnrS4=",
        "b": "WsY12Ko6k+ez671VdpiGvGUdBrDMU7D2O848PifSYEs=",
        "curve": "P-256",
        "x": "EGLrEh7j04EKylTsxCev1oEnesEHY7jZHvbFxYY0/ms="
    }
},
"extensions": {
    "authority_info_access": {
        "ocsp_urls": [
            "http://ocsp.pki.goog/gts1o1core"
        ],
        "issuer_urls": [
            "http://pki.goog/gsr2/GTS101.crt"
        ]
    },
    "key_usage": {
        "value": 1,
        "digital_signature": true
    }
}
```

```
    },  
    "certificate_policies": [  
      {  
        "id": "2.23.140.1.2.2"  
      },  
      {  
        "id": "1.3.6.1.4.1.11129.2.5.3"  
      }  
    ],  
    "extended_key_usage": {  
      "server_auth": true  
    },  
    "subject_alt_name": {  
      "dns_names": [  
        "*.google.com",  
        "*.android.com",  
        "*.appengine.google.com",  
        "*.bdn.dev",  
        "*.cloud.google.com",  
        "*.crowdsource.google.com",  
        "*.g.co",
```

```
"*.gcp.gvt2.com",  
"*.gcpcdn.gvt1.com",  
"*.ggpht.cn",  
"*.gkecnapps.cn",  
"*.google-analytics.com",  
"*.google.ca",  
"*.google.cl",  
"*.google.co.in",  
"*.google.co.jp",  
"*.google.co.uk",  
"*.google.com.ar",  
"*.google.com.au",  
"*.google.com.br",  
"*.google.com.co",  
"*.google.com.mx",  
"*.google.com.tr",  
"*.google.com.vn",  
"*.google.de",  
"*.google.es",  
"*.google.fr",  
"*.google.hu",
```

```
"*.google.it",  
"*.google.nl",  
"*.google.pl",  
"*.google.pt",  
"*.googleadapis.com",  
"*.googleapis.cn",  
"*.googlecnapps.cn",  
"*.googlecommerce.com",  
"*.googlevideo.com",  
"*.gstatic.cn",  
"*.gstatic.com",  
"*.gstaticcnapps.cn",  
"*.gvt1.com",  
"*.gvt2.com",  
"*.metric.gstatic.com",  
"*.urchin.com",  
"*.url.google.com",  
"*.wear.gkecnapps.cn",  
"*.youtube-nocookie.com",  
"*.youtube.com",  
"*.youtubeeducation.com",
```

```
"*.youtubekids.com",  
"* .yt.be",  
"* .yting.com",  
"android.clients.google.com",  
"android.com",  
"developer.android.google.cn",  
"developers.android.google.cn",  
"g.co",  
"ggpht.cn",  
"gkecnapps.cn",  
"goo.gl",  
"google-analytics.com",  
"google.com",  
"googlecnapps.cn",  
"googlecommerce.com",  
"source.android.google.cn",  
"urchin.com",  
"www.goo.gl",  
"youtu.be",  
"youtube.com",  
"youtubeeducation.com",
```

```
        "youtubekids.com",
        "yt.be"
    ],
    },
    "authority_key_id": "98d1f86e10ebcf9bec609f18901ba0eb7d09fd2b",
    "crl_distribution_points": [
        "http://crl.pki.goog/GTS101core.crl"
    ],
    "basic_constraints": {
        "is_ca": false
    },
    "subject_key_id": "163fb9ba67fc86a2141beb775a024c4205357676",
    "signed_certificate_timestamps": [
        {
            "timestamp": 1597139627,
            "version": 0,
            "signature": "BAMARjBEAh9JdXim9iJUP7+6wTluk-
vv90d4Y3VelaUFbRpTvwIQNAiEAmdKYmMBg+xBap3V+ufusaTpjuKHETTusq4FlqhZ2Gi4=",
            "log_id": "sh4FzIuizYogTodm+Su5iiUgZ2va+nDnsk1TLe+LkF4="
        },
        {
```

```
        "timestamp": 1597139627,
        "version": 0,
        "signature": "BAMASDBGAiEAu5BVfxOsRmj4h-
bNIq4sSbbRfD+ue0f0yhvXezKm3gRkCIQCJxHLjIt0N8ZbwSAT3Tt8H2pGTuMCITJGSsGDuFmsDGg==",
        "log_id": "Xqdz+d9WwOe1Nkh90EngMnqRmgYEOrIShBh1loFxRVg="
    }
]
}
}
},
"chain": [
    {
        "parsed": {
            "version": 3,
            "fingerprint_md5": "dbb23c939236012e71d5f44dbc2acea0",
            "fingerprint_sha256": "95c074e35902a14-
abd9d19afb6e7f80e669ff8e2363270539d963613f04aaa21",
            "validity": {
                "end": "2021-12-15T00:00:42Z",
                "length": 142041600,
                "start": "2017-06-15T00:00:42Z"
```

```
    },
    "spki_subject_fingerprint": "6c9383467570b9fcf2e32d84-
fafbd22e82303d7a314dcd184a0face36bf51087",
    "fingerprint_sha1": "dfe2070c79e7ff36a925ffa327ffe3deecf8f9c2",
    "redacted": false,
    "signature_algorithm": {
      "name": "SHA256WithRSA",
      "oid": "1.2.840.113549.1.1.11"
    },
    "subject": {
      "common_name": [
        "GTS CA 101"
      ],
      "country": [
        "US"
      ],
      "organization": [
        "Google Trust Services"
      ]
    },
    "issuer": {
```

```
        "common_name": [
            "GlobalSign"
        ],
        "organizational_unit": [
            "GlobalSign Root CA - R2"
        ],
        "organization": [
            "GlobalSign"
        ]
    },
    "tbs_fingerprint": "76802447a019931a3f004304c53f-
dc6c1b2c378dc4be8f73b39fd9c969dfb445",
    "subject_dn": "C=US, O=Google Trust Services, CN=GTS CA 101",
    "serial_number": "149699596615803609916394524856",
    "issuer_dn": "OU=GlobalSign Root CA - R2, O=GlobalSign, CN=-
=GlobalSign",
    "validation_level": "OV",
    "signature": {
        "valid": true,
        "value": "GoA+Nn-
```

```
n78y6pRjd9XlQWNa7HT-
giZ/r3RNGk-
mUmYHPQq6Scti9PEa-
jvwRT2iWTHQr02fesqOqBY2ETUwgZQ+ll-
toNFvh-
sO9tvBCOIazpswWC9aJ9xju4tWDQH8NVU6YZZ/XteDSGU9YzJqPjY8q3MDxrm-
qepBCf5o8m-
w/wJ4a2G6xzUr6Fb6T8McDO22PLRL6u3M4Tz-
s3A2Mlj6bykJYi8wWIRdAvKLWZu/axBVbzYm-
qmwk-
m5zLSDW5nIAJbELCQCZwMH56t2Dvqofx-
s6BBcCFIZUSpxu6x6td0V7SvJCCosirSmIatj/9dSSVDQibet8q/7UK4v4ZUN80atnZz1yg==",
    "self_signed": false,
    "signature_algorithm": {
        "name": "SHA256WithRSA",
        "oid": "1.2.840.113549.1.1.11"
    }
},
    "tbs_noct_fingerprint": "76802447a019931a3f004304c53f-
dc6c1b2c378dc4be8f73b39fd9c969dfb445",
    "subject_key_info": {
```

```
        "rsa_public_key": {
            "length": 2048,
            "exponent": 65537,
            "modulus": "0BjPRdSLzdOc5EDv-
frTdaSEbyc88jKx1uQ8xGYQ9n-
jwp71ANEJNvBYCAnyqgvRJLAuE9nlgWJP4wn-
wt0d1WTHUv3TeGSghD2UawMw7IilA80a5gQSecLnYM53SDGHC3v0Rh-
hZecjgyCoIxL/0iR/1C/nRGp-
bTd-
dQZrCvnkJjBfvGhMRjYa+-
fajP/Ype9SNnTfBRn3HXcLm-
no+G14adC3EAW48THCOyT9GjN0+CPg7GsZi-
hbG482kzQvb-
s6RZYDiIO60ducaMp1Mb/LzZpKu83Txh15MVmO6BvY/iZEcgQAZO16yX6LnAWRKhSSUj5O1wNCy1tGN8+aM9g9HNbSSsBw=="
        },
        "fingerprint_sha256": "6193e04d9f-
b0a0d0820885b72c7d82c5078bcc1ff59b8d907024c149d81aca3b",
        "key_algorithm": {
            "name": "RSA"
        }
    },
```

```
"extensions": {
  "authority_info_access": {
    "ocsp_urls": [
      "http://ocsp.pki.goog/gsr2"
    ]
  },
  "key_usage": {
    "crl_sign": true,
    "value": 97,
    "digital_signature": true,
    "certificate_sign": true
  },
  "certificate_policies": [
    {
      "cps": [
        "https://pki.goog/repository/"
      ],
      "id": "2.23.140.1.2.2"
    }
  ],
  "extended_key_usage": {
```

```
        "client_auth": true,  
        "server_auth": true  
    },  
    "authority_key_id": "9be20757671c1ec06a06de59b49a2ddfdc19862e",  
    "basic_constraints": {  
        "is_ca": true,  
        "max_path_len": 0  
    },  
    "crl_distribution_points": [  
        "http://crl.pki.goog/gsr2/gsr2.crl"  
    ],  
    "subject_key_id": "98d1f86e10ebcf9bec609f18901ba0eb7d09fd2b"  
    }  
}  
}  
},  
"session_ticket": {  
    "length": 221,  
    "lifetime_hint": 100800  
},  
"signature": {
```

```
        "valid": true,
        "hash_algorithm": "sha256",
        "signature_algorithm": "ecdsa"
    },
    "ocsp_stapling": false,
    "metadata": {},
    "server_key_exchange": {
        "ecdh_params": {
            "curve_id": {
                "id": 23,
                "name": "secp256r1"
            }
        }
    },
    "cipher_suite": {
        "id": "0xC02B",
        "name": "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256"
    },
    "validation": {
        "matches_domain": true,
        "browser_trusted": true
    }
}
```

```
        }  
      }  
    }  
  },  
  "ports": [  
    80,  
    25,  
    443  
  ],  
  "domain": "google.com",  
  "alexa_rank": 1  
}
```

submit_domain Mapping Table

ThreatQ provides the following default mapping for this operation action:

Provider Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples	Notes
.domain	Indicator.Attribute	Domain	google.com	N/A
.alexa_rank	Indicator.Attribute	Alexa Rank	1	N/A
.ports	Indicator.Attribute	Port	80	N/A
.tags	Indicator.Attribute	Tag	https	N/A
.443.https.dhe.support	Indicator.Attribute	DHE Support	False	N/A
.25.s-	Indicator	Country	US	N/A

Provider Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples	Notes
mtp.starttls.tls.certificate.parsed.subject.country	ator.Attribute			
.25.s-mtp.starttls.tls.certificate.parsed.subject.province	Indicator.Attribute	Province	California	N/A
.25.s-mtp.starttls.tls.certificate.parsed.subject.organization	Indicator.Attribute	Organization	Google LLC	N/A
.443.https_www.tls.certificate.parsed.fingerprint_md5	RelatedIndicator.Value	MD5	c9371e4e18b816db88f27027a7681297	N/A
.443.https_www.tls.certificate.parsed.fingerprint_sha1	RelatedIndicator.Value	SHA1	865b07e37a412b44e07e0c6ecb9f9592d25a587b	N/A
.443.https_www.tls.certificate.parsed.fingerprint_sha256	RelatedIndicator.Value	SHA256	61078460e957aab9670e1dee099cae-adc4d762cdfc970e8a7212795388eac16b	N/A

Provider Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples	Notes
.443.ht-tps.tls.certificate.parsed.fingerprint_md5	RelatedIndicator.Value	MD5	a37f996532a6e3af6ea8dc5e9d4d3c04	N/A
.443.ht-tps.tls.certificate.parsed.fingerprint_sha1	RelatedIndicator.Value	SHA1	8940a9f26d4bd34be7df10382a327f9eee751019	N/A
.443.ht-tps.tls.certificate.parsed.fingerprint_sha256	RelatedIndicator.Value	SHA256	ac366724a0b38d-d990a4d-f5cd5619f0566ec8433cd35d0ab9198262a6df6f914	N/A
.25.s-mtp.starttls.tls.certificate.parsed.fingerprint_md5	RelatedIndicator.Value	MD5	7f57f928901c4be91eb6f509e6b20b48	N/A
.25.s-mtp.starttls.tls.certificate.parsed.fingerprint_sha1	RelatedIndicator.Value	SHA1	b364c93387b384cdb56700cd4f531a0e554191fe	N/A
.25.s-	RelatedIn-	SHA256	8a4162886d72c19cac54839374ce60a34e5926213f9670-	N/A

Provider Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples	Notes
mtp.starttls.tls.certificate.parsed.fingerprint_sha256	indicator.Value		9a027007edf07d7a3b	
.443.https.get.body_sha256	RelatedIndicator.Value	SHA256	519297b8b1cd9b59afc757a29c-c60bd6414b38338baea390ceef8420328fd87a	N/A
.80.http.get.body_sha256	RelatedIndicator.Value	SHA256	1b73c184c7c70d4d14ce9310c70ff873e9788f4c-cf671d65865481e2431d1e1b	N/A
.80.http_www.get.body_sha256	RelatedIndicator.Value	SHA256	319abace3d-c8d06d4f6702d2b1574a3016cf45679c49564867f79cd61-57100c6	N/A

submit_hash

GET <https://censys.io/api/v1/view/certificates> endpoints.

```
{
  "parent_spki_subject_fingerprint": "917182d3cf4f6f2c8e08835fea12a01103241552aa9f8982265c944b-
cbd8eb08",
  "parsed": {
    "tbs_noct_fingerprint": "e72aab76606b549e3b-
d2d0581f87bb3923f8b4a341ffca5ead319a7fa52b9591",
    "subject_dn": "C=US, ST=CA, L=San Francisco, O=CloudFlare, Inc.,
CN=sni.cloudflaressl.com",
    "fingerprint_sha1": "b9ff848cde05e5402b4e5c0343af9f05bfdf0380",
    "fingerprint_sha256": "48177e03b47bdcb3b6ab28a92f8005b95302418cd5b9ede77a97eb918e4a2da2",
    "serial_number": "14102343226563625416190047971928015515",
    "validity": {
      "start": "2019-08-20T00:00:00Z",
      "length": 31579200,
      "end": "2020-08-19T12:00:00Z"
    },
    "redacted": false,
    "version": 3,
    "subject": {
```

```
    "country": [
      "US"
    ],
    "organization": [
      "CloudFlare, Inc."
    ],
    "province": [
      "CA"
    ],
    "locality": [
      "San Francisco"
    ],
    "common_name": [
      "sni.cloudflaressl.com"
    ]
  },
  "validation_level": "OV",
  "spki_subject_fingerprint": "ec56ae8a46a9e7f-
b40dda45dafd0da1a6522bdf0aed20896d0e6c9fc4627d456",
  "signature": {
    "value":
```

```
"MEUCIQDQDp-  
dmrF1SZP6W2x7z6x/iUGB7Ys0+GJgDWNai5hMPxAIgGz2o7r5pz3HYzfVlkgA0H2jpA4WzehfogrSGJEjQJk=",  
  "valid": false,  
  "signature_algorithm": {  
    "name": "ECDSA-SHA256",  
    "oid": "1.2.840.10045.4.3.2"  
  },  
  "self_signed": false  
,  
  "tbs_fingerprint": "f1c1693699592448ea5a2f515b5c2239f209cca2c5a7ee487f4aa03339ed8066",  
  "issuer": {  
    "country": [  
      "US"  
    ],  
    "organization": [  
      "CloudFlare, Inc."  
    ],  
    "province": [  
      "CA"  
    ],  
    "locality": [  

```

```
        "San Francisco"
    ],
    "common_name": [
        "CloudFlare Inc ECC CA-2"
    ]
},
"issuer_dn": "C=US, ST=CA, L=San Francisco, O=CloudFlare, Inc., CN=CloudFlare Inc ECC CA-2",
"subject_key_info": {
    "fingerprint_sha256":
    "e75136f8f368490b1698106cda55ff30218f4719ac0b228860ae30ad6e5a525a",
    "key_algorithm": {
        "name": "ECDSA"
    },
    "ecdsa_public_key": {
        "n": "////////wAAAD/////////7zm+q2nF56E87nKwvxjJVE=",
        "b": "WsY12Ko6k+ez671VdpiGvGUdBrDMU7D2O848PifSYEs=",
        "pub": "BAjivo7PatqPdeZM7tOyFloXyZtulBs-
gP01L+UboicUlmIWlyOulftT31FcbKLSMz7oUjKpy9iEQKXqbBPG9jhCw=",
        "gy": "T+NC4v4af5uO5+tKfA+eFivOMldrMV7Oy7ZAaDe/UfU=",
        "curve": "P-256",
```

```
      "x": "COK+js9q2o915kzu07IXWhfJm26UGyA/TUv5RuiJxTU=",
      "y": "mIWlyOULfT31FcbKLSMz7oUjKpy9iEQKXqbBPG9jhCw=",
      "p": "/////wAAAAEAAAAAAAAAAAAAAAAAD//////////8=",
      "length": 256,
      "gx": "axfR8uEsQkf4vOblY6RA8ncDfYEt6zOg9KE5RdiYwpY="
    }
  },
  "__expanded_names": [
    "cloudflaressl.com",
    "gq",
    "sni.cloudflaressl.com",
    "*.elpordistvest.gq",
    "com",
    "elpordistvest.gq"
  ],
  "extensions": {
    "extended_key_usage": {
      "server_auth": true,
      "client_auth": true
    },
    "ct_poison": true,
```

```
"authority_info_access": {
  "ocsp_urls": [
    "http://ocsp.digicert.com"
  ],
  "issuer_urls": [
    "http://cacerts.digicert.com/CloudFlareIncECCCA-2.crt"
  ]
},
"subject_key_id": "c71e81eafd799344b757d76a52d386ce1ad6bee4",
"basic_constraints": {
  "is_ca": false
},
"authority_key_id": "3e742d1fcf4575047e3fc0a2873e4c43835113c6",
"subject_alt_name": {
  "dns_names": [
    "elpordistvest.gq",
    "sni.cloudflaressl.com",
    "*.elpordistvest.gq"
  ]
},
"crl_distribution_points": [
```

```
        "http://crl3.digicert.com/CloudFlareIncECCCA2.crl",
        "http://crl4.digicert.com/CloudFlareIncECCCA2.crl"
    ],
    "certificate_policies": [
        {
            "id": "2.16.840.1.114412.1.1",
            "cps": [
                "https://www.digicert.com/CPS"
            ]
        },
        {
            "id": "2.23.140.1.2.2"
        }
    ],
    "key_usage": {
        "digital_signature": true,
        "value": 1
    }
},
"fingerprint_md5": "a1f788fc84c3c87682f28bf01995dd25",
"signature_algorithm": {
```

```
    "name": "ECDSA-SHA256",
    "oid": "1.2.840.10045.4.3.2"
  },
  "names": [
    "sni.cloudflaressl.com",
    "elpordistvest.gq",
    "*.elpordistvest.gq"
  ]
},
"validation": {
  "microsoft": {
    "type": "leaf",
    "was_valid": true,
    "valid": true,
    "parents": [
      "6172d7a1996cbef71a0182dd44b99e9c035742a9ebd0311aa73aa4733344c5a6"
    ],
    "in_revocation_set": false,
    "blacklisted": false,
    "trusted_path": true,
    "paths": [
```

```
[
  "48177e03b47bdc3b6ab28a92f8005b95302418cd5b9ede77a97eb918e4a2da2",
  "6172d7a1996cbef71a0182dd44b99e9c035742a9ebd0311aa73aa4733344c5a6",
  "16af57a9f676b0ab126095aa5ebadef22ab31119d644ac95cd4b93dbf3f26aeb"
],
"had_trusted_path": true,
"whitelisted": false
},
"apple": {
  "type": "leaf",
  "was_valid": true,
  "valid": true,
  "parents": [
    "6172d7a1996cbef71a0182dd44b99e9c035742a9ebd0311aa73aa4733344c5a6"
  ],
  "in_revocation_set": false,
  "blacklisted": false,
  "trusted_path": true,
  "paths": [
    [
```

```
        "48177e03b47bdc3b6ab28a92f8005b95302418cd5b9ede77a97eb918e4a2da2",
        "6172d7a1996cbef71a0182dd44b99e9c035742a9ebd0311aa73aa4733344c5a6",
        "16af57a9f676b0ab126095aa5ebadef22ab31119d644ac95cd4b93dbf3f26aeb"
    ]
],
"had_trusted_path": true,
"whitelisted": false
},
"google_ct_primary": {
    "type": "leaf",
    "was_valid": true,
    "valid": true,
    "parents": [
        "6172d7a1996cbef71a0182dd44b99e9c035742a9ebd0311aa73aa4733344c5a6"
    ],
    "in_revocation_set": false,
    "blacklisted": false,
    "trusted_path": true,
    "paths": [
        [
            "48177e03b47bdc3b6ab28a92f8005b95302418cd5b9ede77a97eb918e4a2da2",
```

```
        "6172d7a1996cbef71a0182dd44b99e9c035742a9ebd0311aa73aa4733344c5a6",
        "16af57a9f676b0ab126095aa5ebadef22ab31119d644ac95cd4b93dbf3f26aeb"
    ]
},
"had_trusted_path": true,
"whitelisted": false
},
"nss": {
    "type": "leaf",
    "was_valid": true,
    "valid": true,
    "parents": [
        "6172d7a1996cbef71a0182dd44b99e9c035742a9ebd0311aa73aa4733344c5a6"
    ],
    "in_revocation_set": false,
    "blacklisted": false,
    "trusted_path": true,
    "paths": [
        [
            "48177e03b47bdc3b6ab28a92f8005b95302418cd5b9ede77a97eb918e4a2da2",
            "6172d7a1996cbef71a0182dd44b99e9c035742a9ebd0311aa73aa4733344c5a6",
```

```
        "16af57a9f676b0ab126095aa5ebadef22ab31119d644ac95cd4b93dbf3f26aeb"
    ],
    "had_trusted_path": true,
    "whitelisted": false
}
},
"tags": [
    "unexpired",
    "leaf",
    "google-ct",
    "ov",
    "precert",
    "trusted",
    "ct"
],
"metadata": {
    "parse_status": "success",
    "updated_at": "2019-08-21T08:47:45",
    "parse_version": 0,
    "post_processed": false,
```

```
    "added_at": "2019-08-20T16:09:12+00:00",
    "source": "ct",
    "seen_in_scan": false
  },
  "parents": [],
  "precert": true,
  "raw": "MIID+zCCA6GgAwIBAgIQCp-
wDM+U18L7w4vW5yy2CmzAKBg-
gqhkJOPQQDAjBvMQswCQYDVQQGEwJVUzELMAkGA1UECBMCQ0ExFjAUBgNVBAcTDVNh-
biBGcmFuY2l2Y28xGTAXBgNVBAoTEENs-
b3VkRmx-
hcmUsIEluYy4xIDAeBgNVBAMTF0Ns-
b3VkRmx-
hcmUgSW5jIEVDQyBDQS0yMB4XDTE5MDgyMDAwMDAwMFoXDTEwMDgxOTEyMDAwMFow-
bTELMakGA1UEBhMCVVMxCzAJBgNVBAGTAkNBMRywFAYDVQQHEw1TYW4gRnJhb-
mNp-
c2NvMRk-
wFwYDVQQKExBDbG91ZEZsYXJlLCBJb-
mMuMR4wHAYDVQQDExVzb-
mkuY2xvdWRm-
```

bGFyZXNzbC5jb20wWTATBg-
qhkjOPQIBBg-
gqhkjOPQMBBwNCAAQI4r6Oz2ra-
j3XmTO7Tsh-
daF8mb-
bpQbID9NS/lG6InFNZiFp-
cj1JX099RXGy-
i0jM+6FIyqcvYhEC16m-
wTxvY4Qso4ICHzCCA-
swHwYDVR0jBBg-
wFoAUPnQtH89FdQR+P8Ci-
hz5MQ4NRE8YwHQYDVR0OBBYEFMce-
ger-
9eZNEt1fXaLLTh-
s4a1r7kMEYGA1UdEQQ/MD2CEGVscG9yZGlzdHZ1-
c3QuZ3GCFXNuaS5jbG91ZGZsYXJ1-
c3NsLmNvbYISKi5l-
bHBvcnRp-
c3R2ZXN0Lm-
dxMA4GA1UdDwEB/wQEAwIHgDAdBgNVHSUEFjAUBg-

grBgEFBQcDAQYIKwYBBQUHAWIweQYDVR0fBHIw-
cDA2oDSgMoYwaHR0cDovL2Ny-
bDMuZG1-
naWNl-
cnQuY29tL0Ns-
b3VkRmx-
hcmVJb-
mNFQ0NDQTIuY3JsMDagNKAy-
hjBodHRwOi8vY3JsNC5kaWd-
pY2Vy-
dC5jb20vQ2xvdWRGbgGFyZUluY0VDQ0NBMi5jcm-
wwTAYDVR0gBEUwQzA3BglghkgBhv1sAQEwKjAoBg-
grBgEFBQcCARYcaHR0cHM6Ly93d3cuZG1-
naWNl-
cnQuY29tL0NQZzAIBgZngQwBAGIwdgYIKwYBBQUHAQEEda-
jBoMCQGCCsGAQUFBzABh-
hhodHRwOi8vb2NzcC5kaWd-
pY2Vy-
dC5jb20wQAYIKwYBBQUHMAKGNH0dHA6Ly9jYWNl-
cnRzLmRpZ21jZXJ0LmNvbS9DbG91ZEZsYXJlSW5jRUNDQ0EtMi5jcnQwDAYDVR0TAQH/BAlwADATBgorBgEEAdZ5AgQDAQH/B-

```
AIFADAKBg-
gqhkjOPQQDAgNIADBFAiEA0A6XZqxdUmT+ltse8+s-
f4lBge2LNPhiYA1jQIuYTD8QCIBs9qO6+ac9x2M3lZZIANB9o6QOFs3oX6IK0hiRI0CSZ",
  "ct": {
    "google_pilot": {
      "index": 724548576,
      "ct_to_censys_at": "2019-08-20T16:09:11+00:00",
      "added_to_ct_at": "2019-08-20T16:07:48+00:00"
    },
    "google_skydiver": {
      "index": 233915306,
      "ct_to_censys_at": "2019-08-20T16:09:18+00:00",
      "added_to_ct_at": "2019-08-20T16:07:48+00:00"
    },
    "google_rocketeer": {
      "index": 791565396,
      "ct_to_censys_at": "2019-08-20T16:09:11+00:00",
      "added_to_ct_at": "2019-08-20T16:07:48+00:00"
    },
    "digicert_ct2": {
      "index": 59911836,
```

```
    "ct_to_censys_at": "2019-08-21T05:00:55+00:00",
    "added_to_ct_at": "2019-08-20T16:07:48+00:00"
  },
  "cloudflare_nimbus_2020": {
    "index": 55916960,
    "ct_to_censys_at": "2019-08-20T17:12:28+00:00",
    "added_to_ct_at": "2019-08-20T16:07:47+00:00"
  }
},
"zlint": {
  "version": 3,
  "errors_present": false,
  "notices_present": true,
  "lints": {
    "n_subject_common_name_included": true
  },
  "fatals_present": false,
  "warnings_present": false
}
}
```

submit_hash Mapping Table

ThreatQ provides the following default mapping for this operation action:

Provider Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples	Notes
.parsed.subject_dn	Indicator.Attribute	Subject Distinguished Name	CN=ssltest.dataou.com	N/A
.parsed.issuer_dn	Indicator.Attribute	Issuer Distinguished Name	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon	N/A
.parsed.serial_number	Indicator.Attribute	Serial Number	6266302516379758147141725893021220063	N/A
.parsed.validity.start	Indicator.Attribute	Validity Start	2019-08-20T00:00:00Z	N/A
.parsed.validity.end	Indicator.Attribute	Validity End	2020-09-20T12:00:00Z	N/A
.parsed.names	Indicator.Attribute	Name	ssltest.dataou.com	N/A
.parsed.signature.self_signed	Indicator.Attribute	Self Signed	False	N/A
.parsed.signature.valid	Indicator.Attribute	Valid Signature	False	N/A
.parsed.signature.signature_algorithm.name	Indicator.Attribute	Signature Algorithm Name	SHA256-RSA	N/A

Provider Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples	Notes
.parsed.signature.signature_algorithm.oid	Indicator.Attribute	Signature Algorithm OID	1.2.840.113549.1.1.11	N/A
.parsed.signature.value	Indicator.Attribute	Signature	1tpZxr7l0djmnm858oZitjn18Pe173583knMKXgoJcX4/RPNLqPLxlyBWkPnG3NtTT4h01q0fdgqIKfhlqqrq5C9X5pPOnJQHvQnR6qEtE1tRFxx48s1kah+SRYq0h2BzylCwwEGJ7n00reY3ABqKgsEabHSroneqzwSKliQEBdY4TU6Wq1m6WARoP6wEmoi/vrh5Url2g7l1OjXY4H9jYHQ2vLIqrhuwL/LVjvDcc5oQSU1/2ytqdNtSybunvgDUHcQZxvFva9qPn8vNt6MdVw33S+1UtA8hphFrcWzF91n2kzGme9HZIaBILosN+0s5YWciN/UGvbv1g9SWhg==	N/A
.parsed.extensions.subject_alt_name.dns_names	Indicator.Attribute	DNS Names	ssltest.dataou.com	N/A
.validation.apple.valid	Indicator.Attribute	Browser Trust Apple	True	N/A
.validation.microsoft.valid	Indicator.Attribute	Browser Trust Microsoft	True	N/A

Provider Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples	Notes
.validation.nss.valid	Indicator.Attribute	Browser Trust Mozilla NSS	True	N/A
.tags	Indicator.Attribute	Tag	unexpired	N/A
.parsed.subject.province	Indicator.Attribute	Province	CA	N/A
.parsed.subject.locality	Indicator.Attribute	Locality	San Francisco	N/A
.parsed.subject.country	Indicator.Attribute	Country	US	N/A
.parsed.subject.organizational_unit	Indicator.Attribute	Organizational Unity	GlobalSign Root CA - R2	N/A
.parsed.subject.common_name	Indicator.Attribute	Common Name	ssltest.datalou.com	N/A
.parsed.subject.organization	Indicator.Attribute	Organization	CloudFlare, Inc.	N/A
.parsed.subject_key_info.key_algorithm.name	Indicator.Attribute	Key Type	RSA	N/A
.parsed.subject_key_info.rsa_public_key.length	Indicator.Attribute	Key Length	2048	N/A

Provider Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples	Notes
.parsed.subject_key_info.rsa_public_key.modulus	Indicator.Attribute	Modulus	nZ8rTUK6LZIODfHP4MvjM9aU8dwKN+u9dlik 1K34wZYNC0++bHhgHU0IYg2kSpYps868qTQ OBTk1S16zD1FGCOvR+/10jm6Z9smDli/nMot5 ZJPdLFC0zjuPrsURzgOGqkiQuPpg8VS1RAen EvlaHR3+I2NstjeEtoSaR2Jg0vn7wayPjv38eW VbpWsFZeGOpsyXETvSw3nQWG3OhztkntuZM bq/mbimNKWdDPWBnK09G9Opo45RB0zSw2y Zf6/zOoo0aPJDgQP9yKPEKZPYI0FtOlcnCGP K81nN114vN+Kln1RLMSWr/tihl/zWvUsKQxmaq JY/EsHtWJr+sGlw==	N/A
.parsed.extensions.key_usage.key_encipherment	Indicator.Attribute	Key Encipherment	True	N/A
.parsed.extensions.key_usage.digital_signature	Indicator.Attribute	Digital Signature	True	N/A
.parsed.extensions.extended_key_usage.server_auth	Indicator.Attribute	Server Auth	True	N/A
.parsed.extensions.extended_key_usage.client_auth	Indicator.Attribute	Client Auth	True	N/A

Provider Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples	Notes
key_usage.client_auth				
.parsed.extensions.crl_distribution_points	Indicator.Attribute	CRL Paths	http://crl.sca1b.amazontrust.com/sca1b.crl	N/A
.parsed.extensions.certificate_policies	Indicator.Attribute	Policies	u'2.16.840.1.114412.1.2	N/A
.parsed.extensions.basic_constraints.is_ca	Indicator.Attribute	Constrains	False	N/A
.parsed.extensions.authority_info_access.ocsp_urls	Indicator.Attribute	AIA Paths OCSP	http://ocsp.sca1b.amazontrust.com	N/A
.parsed.extensions.authority_info_access.issuer_urls	Indicator.Attribute	AIA Paths Issuer	http://crt.sca1b.amazontrust.com/sca1b.crt	N/A
.ct.google_argon_2020.index	Indicator.Attribute	Certificate Transparency Argon	724442809	N/A
.ct.google_argon_2020.added_	Indicator.Attribute	Certificate	2019-08-20T14:01:42+00:00	N/A

Provider Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples	Notes
to_ct_at		Transparency Argon Date		
.ct.google_pilot.index	Indicator.Attribute	Certidicate Transparency Pilot	724442809	N/A
.ct.google_pilot.added_to_ct_at	Indicator.Attribute	Certidicate Transparency Pilot Date	2019-08-20T14:01:42+00:00	N/A
.ct.google_rocketeer.index	Indicator.Attribute	Certidicate Transparency Rocketeer	724442809	N/A
.ct.google_rocketeer.added_to_ct_at	Indicator.Attribute	Certidicate Transparency Rocketeer Date	2019-08-20T14:01:42+00:00	N/A
.metadata.added_at	Indicator.Attribute	Censys Metadata Added	2019-08-20T14:04:36+00:00	N/A

Provider Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples	Notes
		At		
.metadata.updated_at	Indicator.Attribute	Censys Metadata Updated At	2019-08-21T04:14:34	N/A
.metadata.source	Indicator.Attribute	Censys Metadata Source	ct	N/A
.parsed.fingerprint_md5	RelatedIndicator.Value	MD5	f3f5432ece3e477613aec1806d3f844b	N/A
.parsed.fingerprint_sha1	RelatedIndicator.Value	SHA1	21fb68a06ce0871ea1d5ad00dd278aa573af66f2	N/A
.parsed.fingerprint_sha256	RelatedIndicator.Value	SHA256	a40461051a6fd0e851ba3cc3e1901a30a9b747f55e982b733896c2f052de7a82	N/A
.parsed.subject_key_info.fingerprint_sha256	RelatedIndicator.Value	SHA256	7ec7fd2c4ca6f127905353ff3eff1a0e072e29431d5defd4f912b2972e2153c3	N/A

Change Log

- Version 1.0.0
 - Initial Release