User Guide

Iris Investigate

October 2024

DomainTools

In this Document

Get Started **3**
- Access 3
- APIs 3

Begin Your Investigation **3**
- Searching 3
- Viewing Results in the Web Interface 4
- Advanced Search Filters 5
- Pivoting on Search Results 5
- Navigating with Search History 8
- The Product Menu 10
- Tagging Domains 11

Collaboration **12**
- Groups 12
- Search Hashes 12
- Sharing Investigations 13
- Reporting 14
- Export Pivot Engine Results 14
- Manually Trigger Updates to Web-Related Data 14

Data Panels **15**
- Domain Profile Data Panel 15
- Domain History Data Panel 16
- Screenshot History Data Panel 17
- Stats Data Panel 17
- Visualization Data Panel 18
- Passive DNS (pDNS) Data Panel 18
- IP Profile Data Panel 20
- IP Tools Data Panel 20
- SSL Profile Data Panel 20
- Whois History Data Panel 21

Settings **21**
- Pivot Engine Settings 21

Reference **22**
- Domain Risk Score Ranges 22
- Guided Search 22
- Match Operations Available in Advanced Search 23

Pivot Engine Table Columns (Fields)..... 23
Search Reference..... 25
SSL Certificate Collection Criteria..... 33
Iris Query Quotas and Duplicate Queries..... 34

Get Started

Access Iris Investigate at iris.domaintools.com/investigate/.

Access

Access is provisioned in your DomainTools Enterprise account. Contact enterprisesupport@domaintools.com for help.

APIs

The Iris Investigate API and the DomainTools API suite are documented in our OpenAPI specifications on SwaggerHub, and in our API documentation.

Begin Your Investigation

When you begin a search, Iris Investigate automatically starts your investigation. Investigations are containers that organize a collection of search queries and results, search trails, data pivots, notes, and more. The Collaborate section explains how to share and export investigations.

Searching

Perform your first search from the DomainTools Research page, the Iris Investigate landing page, or from within the app.

Begin searches with any of the accepted search parameters, and Iris Investigate will guess which type of data you provided: for example, it will interpret `4.2.2.2` as an IP address and `domaintools.com` as a domain name. (The Iris Investigate UI accepts 'de-fanged' values for

IP and host addresses such as `example[.]tld` and `4[.]2.2.2`.) Include shortcodes in your query string to specify the data type, and pass these codes from non-DomainTools applications in the API.

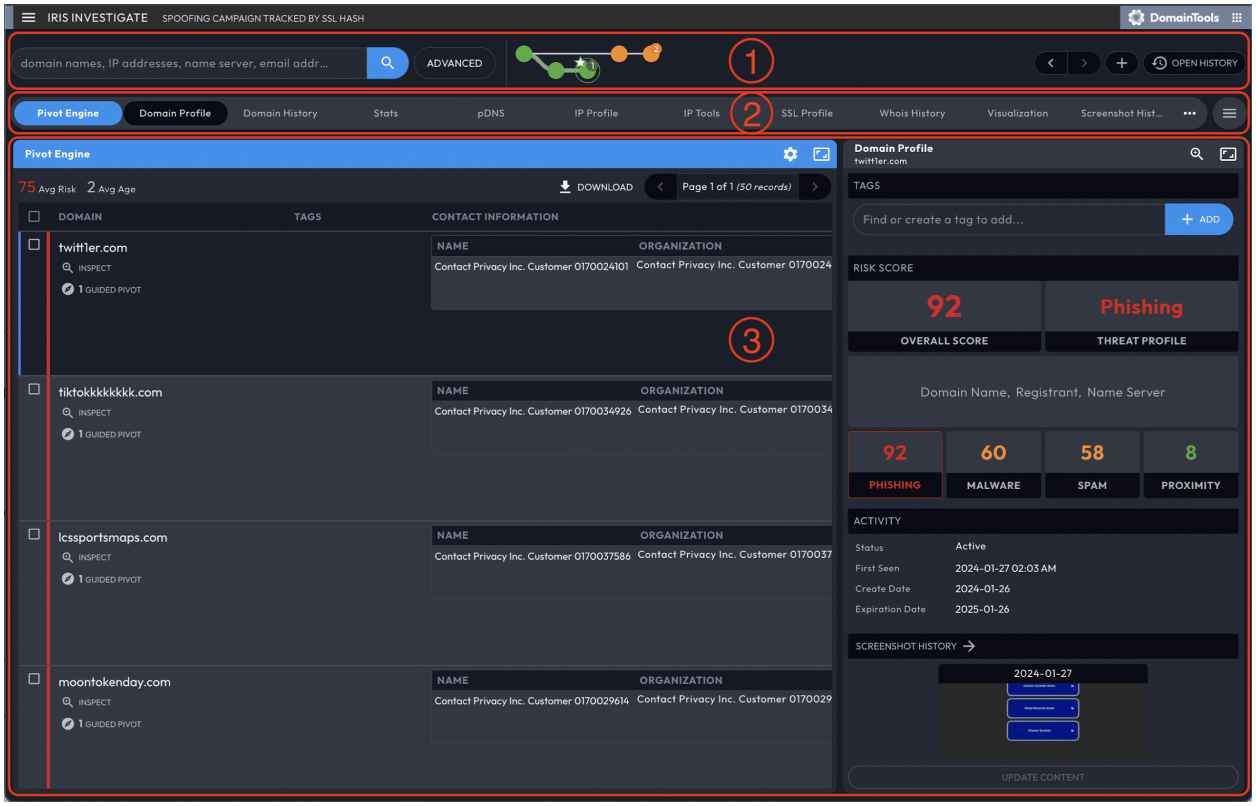
Apex Domains in Search

An apex domain, also known as root domain, is the highest hierarchical level in a registered domain's namespace. For example, in the domain `example.com`, `example.com` is the apex domain, while `www.example.com` is a subdomain

Viewing Results in the Web Interface

Your search will bring you to the Iris Investigate web interface, the interface you will start at if you have made a recent search or if you are continuing an investigation. Start interacting with your search results with three major components of the Iris Investigate web interface:

1. The **Search Area**, including a navigable 'breadcrumb' investigation graph.
2. The **Panel Navigation, Tabs, and Selector**, for navigating and re-ordering Data Panels.
3. The **Results Panel**, which begins with the Pivot Engine in the leftmost spot.



Review the results of your search query in the Pivot Engine panel:

- If Iris provides a single domain for your search, it populates the Data Panels with information for that domain.
- If your search query returns multiple domains, Iris lists multiple entries in the Pivot Engine, and populates the remaining Data Panels with the domain you select.

The Data Panels remain populated with the selected domain's information while you create new branches, or perform searches with no results. This means that the active domain will remain populated in the Data Panels until you select a different domain.

Advanced Search Filters

Filter or expand your results through the Advanced button next to the search box. Add additional filters with logical `AND` (narrow results) and `OR` (expand results) operators. Each filter can use a match rule available for its specific data type (see the Search Parameters section in the Reference, below).

Drag/drop values from the Pivot Engine into the (opened) Advanced Search pane to quickly build an advanced search based on values in the Pivot Engine.

Iris Investigate supports a maximum of 1024 filters per advanced search.

Pivoting on Search Results

The concept of a “pivot” is fundamental to many investigations—that is, given a starting point, discover connections to one or more related items. For example, if your starting point is a domain lookup, a common pivot is on the email address of the registrant of the domain. This pivot shows all of the other domains in the DomainTools database that are connected to that email address. Many datapoints serve as pivots—IP addresses, registrant names, name servers, etc. Most data types shown in Iris Investigate can function as pivot points.

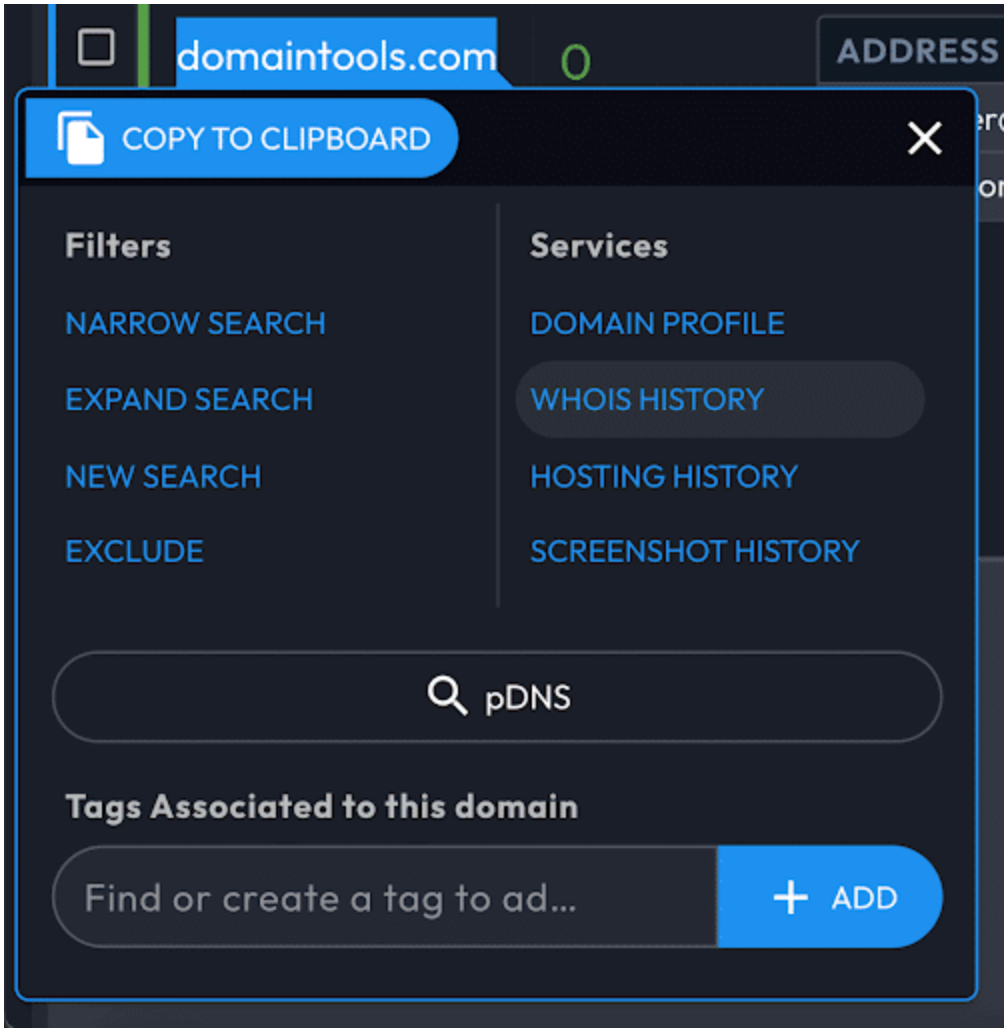
Execute advanced searches directly from your search results by pivoting on specific data points. Pivots advance your investigation by modifying your search with data you select from your search results.

In addition to listing your search results, the Pivot Engine aggregates search results, displaying key data points which can be pivoted on or explored further in the relevant associated data panel.

Right-clicking on a data point brings up the Operations Menu, which pivots on or (with many data types) further inspects the data.

Pivoting with the Operations Menu

By right-clicking a data point, the Operations Menu lets you narrow or expand your search with the data point's string, start a new search, or exclude results containing that string. These operations mirror what is available in the advanced search panel. For example, `Expand Search` will use your new search term to create an `OR` search with your previous query. Trigger an `OR` search with your original and means that the new search will be a logical `AND` of your original query and additional queries.



Previewing and Inspecting Results with the Operations Menu

In addition to the filter controls for pivots, the Operations Menu offers preview and inspection information, depending on the type of data you select.

When you select a domain, the Operations Menu links to domain-specific information across multiple Data Panels.

When you select a non-domain field (e.g. IP address, contact information), the Operations Menu will display:

- The number of domains that share that value.

- The option to list and further investigate those domains from a side panel (for guided pivots).
- A link to investigate the data point in the pDNS panel
- The Domain Risk Score.

The Operations Menu will also display information specific to the type of field selected. For example, if you right click an IP it shows `IP Profile`, `Ping`, `Traceroute`, and `PTR`. A SSL field provides a link to the SSL Profile.

Guided Pivots

Iris Investigate highlights any field that can pivot to 500 or fewer domains, a range that typically indicates a useful investigation target. Often, the smaller the number of pivots, the more useful the connection to another domain may be. For each of the Guided Pivots, the average risk of the associated domains is shown as a quick indicator of severity.

Configure the threshold or disabled Guided Pivots in settings, accessible from the Product Menu or the settings icon on the top left of the Pivot Engine.

Domain Risk Score

The Domain Risk Score predicts how likely a domain is to be malicious, often before it is weaponized. Read more about the Domain Risk Score in the User Guide and Technical Brief. The score comes from the strongest scoring of two distinct algorithms: Proximity and Threat Profile.

Proximity evaluates the likelihood a domain may be part of an attack by analyzing how closely connected it is to other known-bad domains. Threat Profile leverages machine learning to model how closely a domain's intrinsic properties resemble others used for spam, phishing, or malware. The highest score from either spam, phishing, or malware becomes the Threat Profile score.

Consult the Domain Risk Score Ranges in the Appendix, below.

Navigating with Search History

Each time you pivot on your results, Iris Investigate moves your investigation forward to a new node in your Search History. Each new node connects to its originating node with a line/edge.

Toggle fullscreen mode with h. For a complete list of Iris Investigate UI keyboard shortcuts, consult the Reference section.

The search history graph is coded with details about each search node. For example, green nodes indicate your active investigation path, orange nodes indicate searches outside of your active investigation path, and the blue 'document' icon nodes indicate passive DNS results. Consult the Reference section for all Search History indicators.

Return to any point in your investigation by selecting the node, and Iris Investigate will load your Pivot Engine and Data Panels for that query. Continue with new pivots, and Iris will create a new branch of nodes.

Create a new, empty history branch by selecting the + button near the top right corner of the Pivot Engine. Your next query will be the root node of the new branch (note how this feature can aid in organizing your investigation). Start a new branch with the current node as the root. To do this, select `Manage History > New History Branch > Start it with the Current Search`.

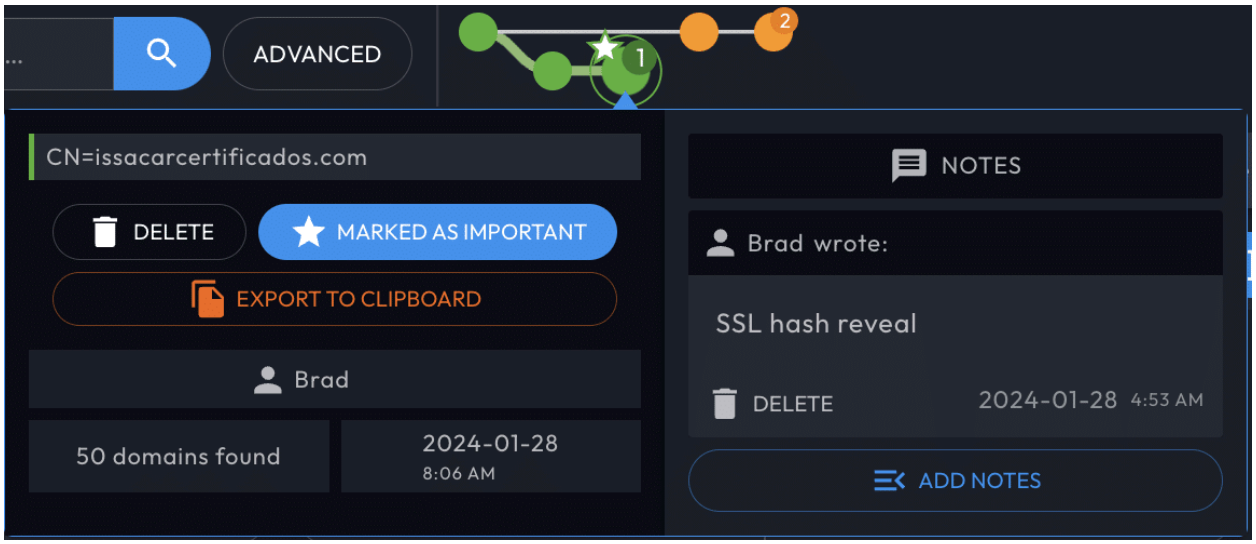
Once you delete a node or a branch, it cannot be recovered.

Annotating in Search History with the Search Node Drawer

Hovering over a search node invokes the search node drawer, which can:

- Highlight nodes with the Mark as Important button.

- Export this node's search hash to the clipboard.
- Review and add Search Notes.

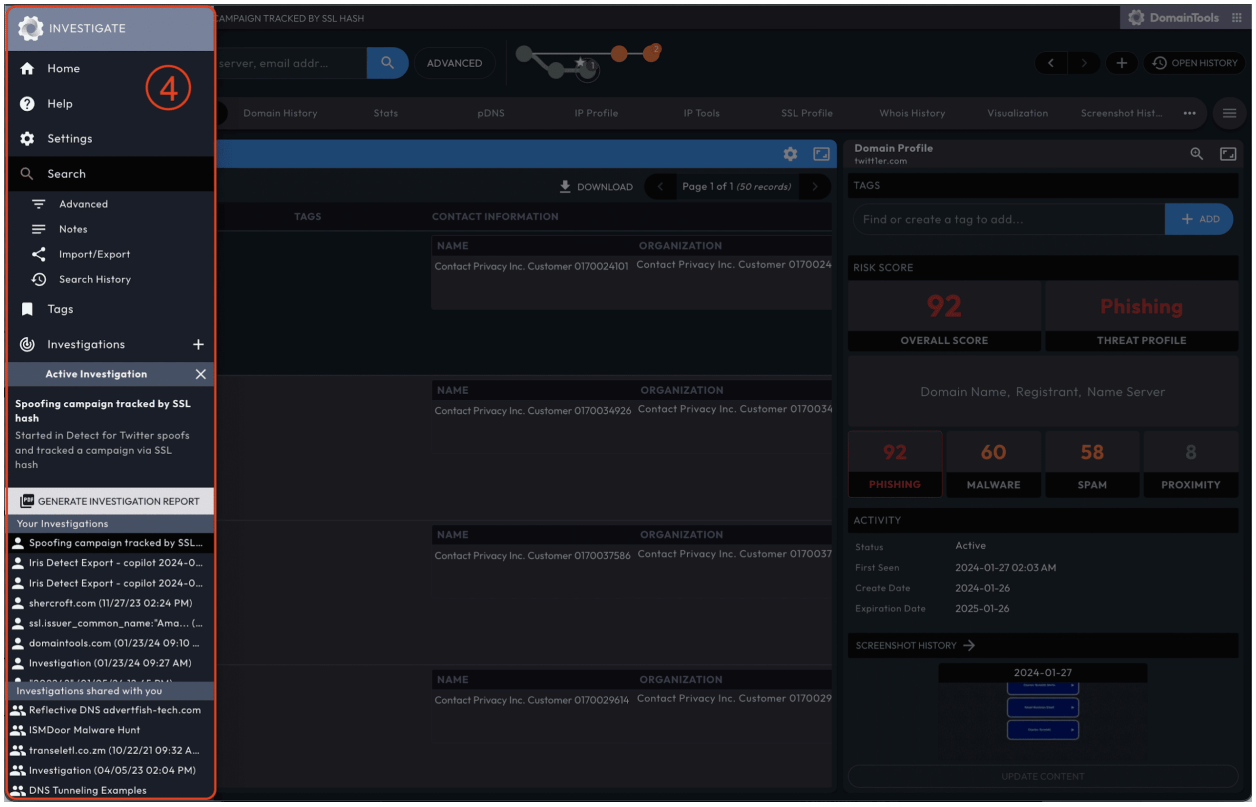


When notes exist for a node, a number on the node indicates how many notes it has. The search nodes in your investigation history also indicate (with a number bubble) the Search Notes count, as well as the nodes Marked as Important.

Enter an IP address, domain name, or email address in your notes, and Iris Investigate enables Operations Menus to search or filter directly from the notes.

The Product Menu

Create or open investigations, start an ad-hoc search, adjust the layout, or return to the home page from the navigation column. Click “Iris Investigate” in the upper left corner to open it.



The Product Menu contains the Settings menu.

Tagging Domains

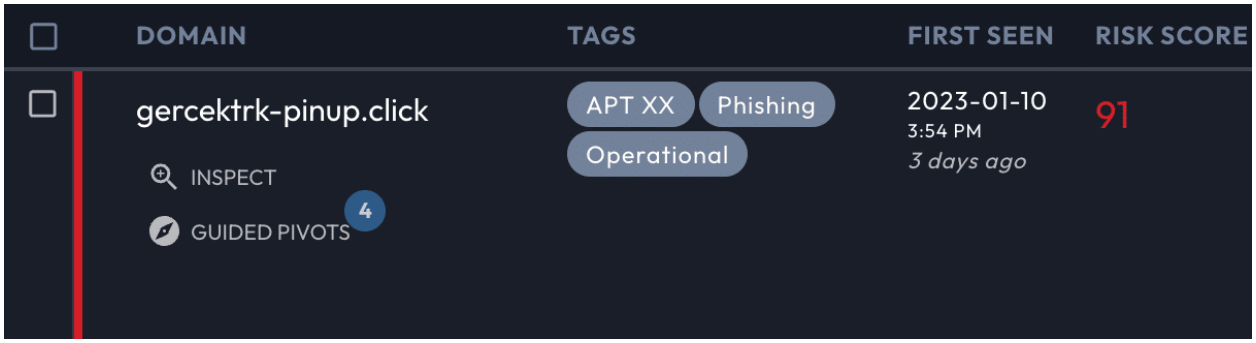
Tags attach to domains, include an editable description field, and can be modified with the Iris by the Iris APIs. Edit, search, and filter by tag. The Tag Manager displays all the domains associated with a single tag, across your group.

Tags can be applied to these and other use cases:

- Attribution labeling
- Threat profile type
- Operational status
- Inclusion in a specific case
- Triage or other status
- Programmatic decision-making

In addition to the API, access tags through the following sections of the Iris Investigate UI:

- The Pivot Engine lets you modify tags from one or multiple domains by selecting the domains and the Tag button (you can also export tags).
- The Operations Menu, when opened from a domain, allows you to edit tags for that domain.
- The Tag Manager (accessible from the Product Menu) displays all tags from your investigations. It also includes tags used in your group: consult the Collaborating section, below.
- The Stats Data Panel visualizes tags.



Sharing Tags and Tagged Results

Your tags are automatically shared with other users in your group. Your investigations are private by default, but can also be shared to your group.

If you export a Search Hash to a user outside of your group, your tags will not be visible.

Collaboration

Groups

A Group consists of the other Iris Investigate users at your company.

Search Hashes

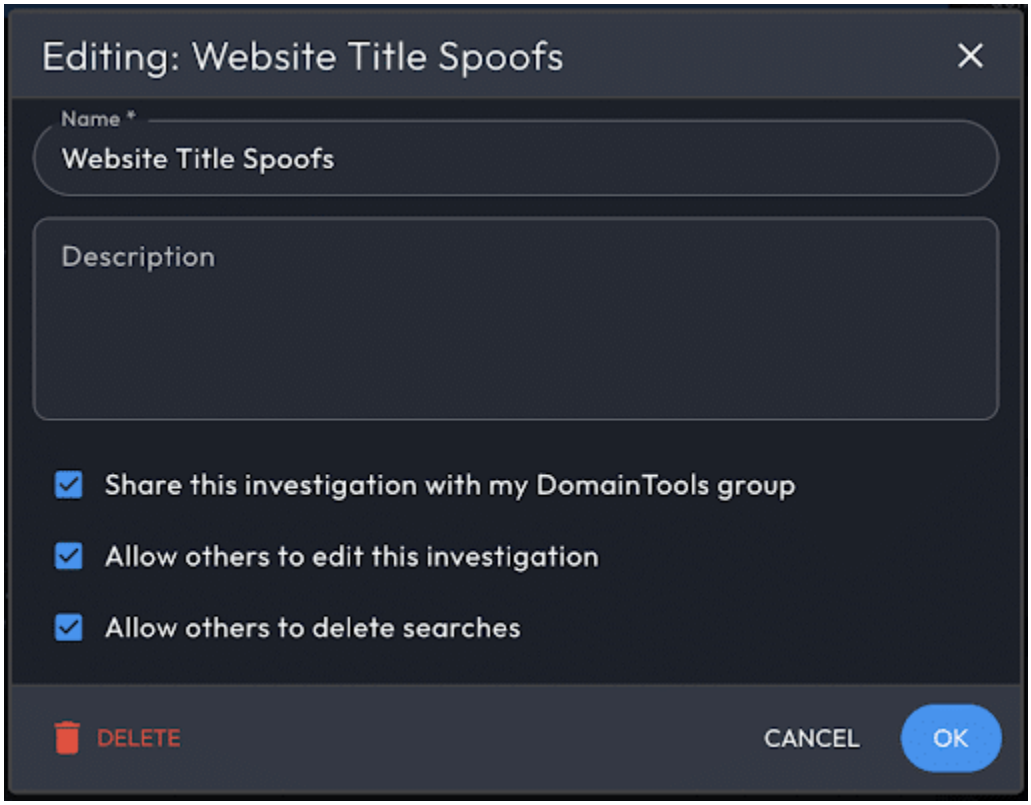
Search Hashes will share a specific search to anyone with Iris Investigate, including people outside of your group. Search hashes reproduce search terms, but do not include tags or other

investigation-specific information. Search hashes can also be used by the Investigate API to query for the results of an advanced search first created through the Investigate web interface.

Sharing Investigations

By default, investigations are private to the originating user.

Share your investigations from the Product Menu by hovering over your active investigation, and then selecting `Edit Investigation`. Three access levels are available for your group members: `view`, `add branches`, and `delete branches`.



When another user creates a new search node in your shared investigation, that node will appear in Search History with a sharing icon, and trigger a browser notification.

When an investigation is shared with you, the investigation will appear in your investigation list in the Product Menu, grouped under the heading `Investigations shared with you`.

If you unshare an investigation, the investigation disappears for other group members.

Reporting

The `Generate Investigation Report` button in the Product Menu creates a PDF containing the following information:

- Title and description.
- Investigation path in tabular form, and including search notes.
- Pivot Engine data in tabular form, with columns matching your Pivot Engine Panel columns. For search results numbering over 500, the report will include the page of Pivot Engine results that are displayed at the time of generation.
- Statistics, via the Stats Data Panel.
- Visualizations, generated from the current appearance of the Visualization Data Panel (large result sets may not display well in this format; download high-res images from the Visualization Data Panel directly).

Reports are generated from the viewpoint of the current selected node in your investigation. For a report of the full investigation, select the final node before generating the report. The Stats, Visualization, and Pivot Engine Data Panels must be displayed in the investigation UI in order for their contents to be included in the report.

Export Pivot Engine Results

Export your full Pivot Engine table at any time by selecting the DOWNLOAD button next to page navigation near the top of the Pivot Engine Data Panel, and selecting the format (CSV, STIX 1.2, or STIX 2.0).

Fields containing multiple values have repeated columns in order to maintain a single value per table element.

Manually Trigger Updates to Web-Related Data

Multiple Iris Investigate data panels contain web-related data that is gathered via web crawler.

By default, the web crawler will gather data upon the first discovery of a domain. If a domain has a domain risk score of 70 or above, the web crawler will automatically gather data every 3 months. If the user group uses Iris Detect to watch a domain, the web crawler will gather data every day.

To update web-related data at a cadence outside of our default settings, it is possible to trigger the web crawler to gather web-related data for a domain or group of domains. Select the `update content` button in the relevant data panels (Pivot Engine, Screenshot History, Domain Profile, SSL Profile) to trigger the web-crawler to gather fresh web-related data including:

- Screenshot
- Website title
- Website response code
- Redirect domain
- Server type
- Website trackers
- Aspects of the SSL certificate

Data Panels

Iris Investigate uses Data Panels to present domain information in containers.

Navigate Data Panels with the Data Panel Tabs, and select which Data Panels are visible through the 'hamburger' menu on the far right of the ribbon.

Data Panels can be resized with the 'resize' icon on the far right of the Data Panel's title ribbon. Most panels have settings options, accessible through the settings icon in the panel's title bar. Context-appropriate Data Panels can be invoked from the Operations Menu and Pivot Engine, as well as from within Data Panels.

Domain Profile Data Panel

The Domain Profile Data Panel serves as a snapshot of all domain related data in one data panel. It is especially useful for getting an overview of the domain-related data, and choosing the next data panel to review for your investigation.

The Domain Profile panel shows the following information:

- Domain name
- Domain Risk Score
- Screenshot

- Recent Passive DNS resolutions
- Dates: First Seen date/time, Whois Create Date, Expiration Date
- Email address(es)
- Registrant Organization
- Registrar
- Registrar Status
- Name Servers
- IP addresses
- IP location
- ASN
- Whois History summary
- Website title and server type
- “Raw” Whois record

Domain History Data Panel

Domain History shows how a domain has evolved over time. It replaces the legacy Hosting History service, covering many more fields and covering all domains tracked by DomainTools.

The tracked data elements include:

Data Element	**Description**
Status	When a domain is seen as newly active by DomainTools, or when a domain becomes inactive
Whois data	Create/expiration dates, registrar and registrant names, contact emails, and more
DNS data	Results of daily DNS resolutions for A, NS, MX and SOA active resolutions
Web content	Website title, response code, server type, trackers, and more
Screenshots	The date/time when a new screenshot is captured
SSL Certificate updates	The SHA 1 hash, validity dates, Issuer Common Name, and up to the first 5 Subject Alt Names

Each data element is tracked for differential changes, and records are generated when a value in a tracked field changes. The newly added element is shaded green and also has a short vertical bar. Unchanged elements have no special formatting.

Filter the list by primary and secondary categories in the Domain History: Fields Settings menu, accessible through the gear icon on the left of the Domain History panel title bar. Show and hide the new subset of your results by toggling in the `Field` button, located in the panel's column rows.

Domain History versus Historical pDNS and WHOIS Data

Domain History is available for over 98% of active domains, and for all domains created since 2021. For some domains, additional historical information is available in the legacy Hosting History Data Panel Panel (via the Investigate UX), and in our 20+ years of records in the WHOIS History Data Panel.

Screenshot History Data Panel

The Screenshot History data panel provides an index of dates for which DomainTools has an archived screenshot for the domain. If Screenshot History is empty, select the `Update Content` button to queue the web crawler to gather an updated screenshot for the domain (typically available within five minutes, and up to 24 hours).

When multiple historical screenshots are available, browse through them using `<` or `>`.

Stats Data Panel

The Stats Data Panel shows the number of occurrences of datapoints within the displayed results set, and can help you understand the level of connection of the domains in your pivot engine. In some cases, such as date fields and domain risk score, domains in the result set are grouped in sets, rather than by individual values.

Each of the data types is represented graphically (a map for IP country and pie charts for all others), organized in a table.

In the settings menu within the Stats Panel, under `Sorting`, guided pivots can be ordered first.

Stats aggregates data for the first 2,500 records in the results set.

Visualization Data Panel

The Visualization Data Panel is a visual representation of connections between domains in the Pivot Engine. It depicts domains as blue nodes; the color-coding for the others can be seen in the legend in the upper left. A domain can either be a larger or normal sized dot. The larger dots represent domains with high domain risk scores of 70 or higher. The legend also shows how many instances there are for each field in the graph. Select Edit Fields to choose up to 4 fields (plus domain) to view.

Double-clicking a domain or IP address node makes it the current domain and populates all domain-centric panels. When you hover over a node on the graph, that node and those directly connected to it are highlighted. Zoom in and out on the graph, and drag an item in the Force layout in order to put the most interesting data in the center.

The `Link Degree` slider in the lower-right lets you filter out data that either have too many or too few connections.

Node Inspector

Use the `Node Inspector` on the right of the panel to view the values for each of the fields. It is possible to search for a specific value or filter by field, and perform guided pivots.

This is a great way to see a list of all the different values used by the domains in the pivot engine for a specific field (data point).

Passive DNS (pDNS) Data Panel

Passive DNS (pDNS) shows current and past domain to IP resolutions, as well as date stamps bracketing and relative dates, for when a given resolution was observed.

Query pDNS data from a search, or as a pivot with the Operations Menu. The pDNS data in Iris Investigate include the following record types:

Record Type	Description
A	IPv4 resolutions for domains and subdomains/hostnames (by default, the pDNS panel shows A records only)
AAAA	IPv6 resolutions for domains and subdomains
NS	Name server
SOA	Start Of Authority email addresses and name servers
MX	Mail server host names and IP addresses
CNAME	Alias records mapping one hostname to another
TXT	Optional catch-all record that may contain arbitrary descriptive information

Apex Domains

The pDNS Panel supports searching by apex domain, subdomain, or both. Consult the note in Searching for a definition of apex domain.

Query vs Response

pDNS data is available from the query and response 'directions':

- The query direction, also known as `rrname`, shows historical results for when the domain was queried and IP addresses were returned.
- The response direction, also known as `rdata`, shows historical results for when the IP or IP CIDR range was queried and domain(s) were returned.

The response direction often yields fewer or no records This is because in DNS A records, domain is the query and the IP address is the response. If you enter a domain with the toggle set to response, or an IP address with the toggle set to query, if no results appear, try flipping the toggle and re-running the search.

Send Results to Pivot Engine

Send pDNS results to the Pivot Engine by selecting Send domain results to pivot engine. You can modify or restart your search with pivots.

IP Profile Data Panel

IP Profile is analogous to the Domain Profile panel. It provides key datapoints as well as the raw Whois record for the IP address. Pivot on the IP itself in order to modify or begin a search on that address.

In most places where an IP address is displayed across Iris Investigate, a magnifying glass icon appears just to the right of the address. Selecting the icon will bring up the IP Inspect view, which is a fast way to view the IP Profile and IP Tools data for an IP address without losing your place in the UX.

IP Tools Data Panel

The IP Tools panel provides three tools to investigate IP address information:

- **Ping** generally tells you whether the IP address is reachable. When you trigger a ping through the interface, the ping originates from DomainTools and includes no record of your involvement.
- **Traceroute** gives insights into the hosting, routing, and reachability of the IP address. As with Ping, when you trigger a traceroute through the interface, it originates from DomainTools and includes no record of your involvement.
- **PTR**, the DNS Pointer (PTR) record, is commonly used as a form of Reverse DNS lookup. It shows the CNAME of the IP address, which tells you about the actual owner of the address (often a hosting provider) but not necessarily about the domains that may be hosted on that address.

SSL Profile Data Panel

The SSL Profile panel provides SSL certificate details, including additional potential pivots. When DomainTools finds more than one certificate on a domain, Iris Investigate shows the certificates in separate tabs. For additional information on DomainTools collection and validation processes, consult the SSL Certificate Collection reference section.

The additional pivots from an SSL/TLS certificate are found in the `Extensions -> Subject Alt Name` section, from which you can open the Operations Menu. To examine all the domains covered by a certificate, use the `ADD TO FILTERS` button.

Note that when using the `contain` operator for SSL Alt Names, the search term must exactly match any substring resulting from the domain being split by dots. For example, in `example.domain.com`, matches would be generated from `example`, `domain`, and `com`.

Whois History Data Panel

The Whois History Data Panel shows, by default, the current Whois record for the domain, with a vertical timeline of earlier dates for which DomainTools has a historical Whois record.

View changes to Whois records with three methods: `Side by Side` and `Inline` highlight the differing rows in the Whois record, while `Raw records` show the two records together.

Unique emails are listed for pivoting with the Operations Menu.

Settings

The Settings panel is located within the Product Menu.

Pivot Engine Settings

Guided Pivots Settings

Configure guided pivot ranges for each available data type.

Historical Search Settings

In addition to current records, Iris Investigate can find historical records matching email address and registrant information queries. Specifically, the three query types supported are `email address`, `registrant`, and `Whois record contains`. By default, historical search is enabled.

Per-search override: on an individual search, enable or disable historical queries on the three supported fields. To override, open `Advanced search`, select the history icon, and re-run your query.

Historical searching can return domains that do not match your query. The reason for this is that at some time in the domain's history, it did match the query. To see the record(s) where the domain matched the query, select `See Historical Matches`. This opens Whois History to the most recent record that matched your search term.

Active and Inactive Domains: Iris Investigate will indicate when a domain is inactive with an icon near the domain name in Pivot Engine, and in the Status column. To be marked inactive, the domain must no longer resolve in DNS. Because there can be unusual cases in which registered domains do not resolve, or where unregistered domains do resolve, both conditions (not registered, not delegated) must be true for the domain to be marked inactive.

Reference

Domain Risk Score Ranges

Consult our Domain Risk Score User Guide.

Guided Search

Guided search inputs are accepted in the Iris Investigate search area, and by passing the guided search parameters to Iris Investigate via a URL. Guided search parameters and accepted operators are specified in this appendix below.

For example, searching Iris Investigate for `209242` to locate domains on the Autonomous System Number (ASN) `ASN209242` will return results for the string `209242`, including user accounts and email addresses.

However, the search string `ip.asn:"209242"` will instruct Iris Investigate to search only ASNs.

These two searches can also be accomplished with a URL query parameter. A generic search for `209242` is constructed as:

```
https://iris.domaintools.com/investigate/search/?q="209242"
```

A guided search for `ASN209242`, however, is written as:

https://iris.domaintools.com/investigate/search/?q=ip.asn:"209242"

Match Operations Available in Advanced Search

- Begins With
- Matches
- Exactly Matches (case sensitive)
- Does Not Match
- Does Not Exactly Match (case insensitive)
- Contains (matches if any term in the query is found)
- Contains All
- Does Not Contain
- Does Not Contain All
- Ends With
- Greater Than
- Greater Than or Equal To
- Matches (“Equal To” for quantitative fields)
- Equal To or Less Than
- Less Than
- Exactly

Pivot Engine Table Columns (Fields)

By default, the table includes all fields:

- Domain
- Status (active or inactive)
- Tags
- Domain Lifecycle First Seen (when DomainTools first became aware of the current Domain Lifecycle)
- Domain Risk Score
- Email (registrant email)
- Email domain
- Contact Information (registrant, admin, tech, billing, SOA, etc.)
- Registrant

- Registrant Organization
- Registrar
- Registrar Status
- Create Date
- Expiration Date
- Name Server
- IP (Address, ISP, ASN, Country)
- Trackers – the following web trackers are gathered with screenshots:
    - Google Adsense
    - Google Universal Analytics
    - Google Analytics 4
    - Google Tag Manager
    - Baidu
    - Facebook
    - Hotjar
    - Matomo
    - Statcounter
    - Yandex
- Rank
- Website Response
- Website Title
- Server Type
- Redirect
- Redirect Domain
- MX (Mail Exchanger) Information
- SSL certificate Hash
- SSL certificate Organization
- SSL certificate Subject Alt Names
- SSL Certificate Issuer
- TLD (to enable sorting/filtering by TLD in large result sets)

Search Reference

Search Tips and Guidance

- Filters that match more than 100M domains will not return results and prevent any subsequent filters from matching. (If possible, place these last in any advanced query so they have less of a set of domains to filter)
- Values in a Whois record are tokenized in our data storage and so these filters cannot match on substring values. Whole terms must be used.
- This means for Date/Time etc.. fields in Whois it is not possible to match on the Date value alone, the entire Date/Time will be required to match.
- The following list of English Stop words are automatically excluded from matching: a, an, and, are, as, at, be, but, by, for, if, in, into, is, it, no, not, of, on, or, such, that, the, their, then, there, these, they, this, to, was, will, with.
- Special characters are used to delimit search terms and separate for tokenizing. Some special characters will not split terms, these are: +._\@,:-
- All other non-letter or digit characters (besides special character and UTF-8 byte sequences) will split terms.
- The “@" symbol in email addresses is a special signal to allow "@domain.ext" searches.
- Trailing special characters are ignored.
- The wildcard `*` matches zero or more characters, and the wildcard `?` matches exactly one character.

`Matches` and `Exactly Matches`

The `Matches` filter performs a standard search on text fields, while the `Exactly Matches` filter ensures precise matching.

The `Matches` surfaces records that contain all the analyzed tokens of the searched value in the analyzed tokens stored for the requested field-value. Filtering for `this is an-example text.value` will surface records that contain all of these tokens: [`this`, `is`, `an`, `example`, `text.value`]. The ordering of the searched tokens will not impact the results.

The `Exactly Matches` filter surfaces records that contain exactly the same searched value, without analysis. Filtering for `this is an-example text.value` will surface records with that exact string (`"this is an-example text.value"`).

`Contains` and `Contains All`

The `Contains` and `Contains All` filters perform standard searches on text fields. `Contains All` ensures that all tokens are present, while `Contains` ensures that at least one of them is present.

The `contains` filter looks for records that contain at least one of the tokens of the searched value. Filtering for `this is an-example text.value` will surface records that contain at least one of the following tokens: [`this`, `is`, `an`, `example`, `text.value`].

The `Contains All` filter looks for records that contain all the tokens of the searched value in the requested field-value. Filtering for `this is an-example text.value` will surface records that contain all of the following tokens: [`this`, `is`, `an`, `example`, `text.value`]. The ordering of the searched tokens will not impact the results.

Parameters, Inputs, Operators, and Shortcodes

Field	Historical Toggle	Shortcode	Options									
Adsense	-	ad	Does Not Match	Exists	Matches							
Baidu Analytics	-	-	Does Not Match	Exists	Does Not Exist	Matches						
Contact Country Code	-	cons.cc	Begins With	Does Not Match	Exists	Matches						
Contact Name	-	cons.nm	Begins With	Contains	Contains All	Does Not Contain	Does Not Contain All	Does Not Exactly Match	Exactly Matches	Exists		
Contact Phone	-	cons.ph	Begins With	Does Not Match	Exists	Matches						
Contact Street	-	cons.str	Begins With	Contains	Contains All	Does Not Contain	Does Not Contain All	Does Not Exactly Match	Exactly Matches	Exists		
Create Date	-	cre	Does Not Match	Greater Than	Greater Than or Equal To	Less Than	Less Than or Equal To	Matches	Within			
Domain	-	domain	Begins With	Contains	Does Not Contain	Does Not Match	Ends With	Exists	In	Matches	Not In	
Email	Yes	em	Begins With	Does Not Match	Exists	In	Matches	Not In				
Email - Admin	-	empa	Begins With	Does Not Match	Exists	Matches						
Email - Billing	-	empb	Begins With	Does Not Match	Exists	Matches						

Field	Historical Toggle	Shortcode	Options									
Email - DNS/SOA	-	ema	Begins With	Does Not Match	Exists	Matches						
Email - Registrant	-	empr	Begins With	Does Not Match	Exists	Matches						
Email - Technical	-	empt	Begins With	Does Not Match	Exists	Matches						
Email - Whois	-	emw	Begins With	Does Not Match	Exists	Matches						
Email Domain	-	emd	Begins With	Does Not Match	Exists	In	Matches	Not In				
Expiration Date	-	exp	Greater Than	Greater Than or Equal To	Less Than	Less Than or Equal To	Matches	Within				
Facebook (Meta Pixel)	-	-	Does Not Match	Exists	Does Not Exist	Matches						
First Seen	-	current_lifecycle_first_seen	Greater Than	Greater Than or Equal To	Less Than	Less Than or Equal To	Matches	Within				
Google Analytics	-	ga	Does Not Match	Exists	Does Not Exist	Matches						
Google Analytics 4	-	-	Does Not Match	Exists	Does Not Exist	Matches						
Google Tag Manager	-	-	Does Not Match	Exists	Does Not Exist	Matches						
Hotjar	-	-	Does Not Match	Exists	Does Not Exist	Matches						

Field	Historical Toggle	Shortcode	Options									
IP	-	ip.ip	Does Not Match	Greater Than	Greater Than or Equal To	In	Less Than	Less Than or Equal To	Matches	Not In		
IP ASN	-	ip.asn	Does Not Match	Greater Than	Greater Than or Equal To	Less Than	Less Than or Equal To	Matches				
IP Country Code	-	ip.cc	Begins With	Does Not Match	Exists	Matches						
ISP IP Information	-	ip.isp	Contains	Contains All	Does Not Contain	Does Not Contain All	Does Not Exactly Match	Exactly Matches	Exists			
MX Server	-	mx.mx	Begins With	Does Not Match	Exists	Matches						
MX Server Domain	-	mx.mxd	Begins With	Does Not Match	Exists	Matches						
MX Server IP	-	mx.mip	Does Not Match	Greater Than	Greater Than or Equal To	In	Less Than	Less Than or Equal To	Matches	Not In		
Matomo	-	-	Does Not Match	Exists	Does Not Exist	Matches						
Name Server	-	ns.ns	Does Not Match	Exists	Matches							
Name Server Domain	-	ns.nsd	Begins With	Does Not Match	Exists	Matches						
Name Server IP	-	ns.nip	Does Not Match	Greater Than	Greater Than or Equal To	In	Less Than	Less Than or Equal To	Matches	Not In		

Field	Historical Toggle	Shortcode	Options									
Rank	-	popularity_rank	Does Not Match	Greater Than	Greater Than or Equal To	Less Than	Less Than or Equal To	Matches				
Redirect Domain	-	rdd	Begins With	Does Not Match	Exists	Matches						
Registrant	Yes	r_n	Begins With	Contains	Contains All	Does Not Contain	Does Not Contain All	Does Not Exactly Match	Does Not Match	Exactly Matches	Exists	Matches
Registrant Organisation	-	r_o	Begins With	Contains	Contains All	Does Not Contain	Does Not Contain All	Does Not Exactly Match	Does Not Match	Exactly Matches	Exists	Matches
Registrar	-	reg	Begins With	Contains	Contains All	Does Not Contain	Does Not Contain All	Does Not Exactly Match	Does Not Match	Exactly Matches	Exists	Matches
Risk Score	-	cr	Does Not Match	Greater Than	Greater Than or Equal To	Less Than	Less Than or Equal To	Matches				
SSL Alt Names	-	ssl.alt_names	Begins With	Contains	Does Not Contain	Does Not Match	Exists	Matches				
SSL Duration (days)	-	ssl.duration	Does Not Match	Greater Than	Greater Than or Equal To	Less Than	Less Than or Equal To	Matches				
SSL Email	-	ssl.em	Begins With	Does Not Match	Exists	Matches						
SSL Hash	-	ssl.sh	Begins With	Does Not Match	Exists	Matches						
SSL Issuer Common Name	-	ssl.issuer_common_name	Begins With	Contains	Does Not Contain	Does Not Match	Ends With	Matches				

Field	Historical Toggle	Shortcode	Options									
SSL Not After Date	-	ssl.not_after	Does Not Match	Greater Than	Greater Than or Equal To	Less Than	Less Than or Equal To	Matches	Within			
SSL Not Before Date	-	ssl.not_before	Does Not Match	Greater Than	Greater Than or Equal To	Less Than	Less Than or Equal To	Matches	Within			
SSL Subject	-	ssl.s	Begins With	Does Not Match	Exists	Matches						
SSL Subject Common Name	-	ssl.common_name	Begins With	Contains	Does Not Contain	Does Not Match	Ends With	Matches				
SSL Subject Org Name	-	ssl.so	Begins With	Contains	Contains All	Does Not Contain	Does Not Contain All	Does Not Exactly Match	Does Not Match	Exactly Matches	Exists	Matches
Server Type	-	server_type	Begins With	Contains	Contains All	Does Not Contain	Does Not Contain All	Does Not Exactly Match	Does Not Match	Exactly Matches	Exists	Matches
Statcounter - Project Codes	-	-	Does Not Match	Exists	Does Not Exist	Matches						
Statcounter - Security Codes	-	-	Does Not Match	Exists	Does Not Exist	Matches						
Status	-	active	Matches									
TLD	-	tld	Begins With	Does Not Match	Exists	In	Matches	Not In				
Tags	-	tags	Contains	Contains All	Does Not Contain	Does Not Contain All						

Field	Historical Toggle	Shortcode	Options									
Website Title	-	title	Begins With	Contains	Contains All	Does Not Contain	Does Not Contain All	Does Not Exactly Match	Does Not Match	Exactly Matches	Exists	Matches
Whois Record	Yes	whois	Contains	Contains All								
Yandex Metrica	-	-	Does Not Match	Exists	Does Not Exist	Matches						

SSL Certificate Collection Criteria

Collecting SSL Cert data

DomainTools employs three separate methods to gather certificate data:

1. Certificate Transparency Log Certificates
    a. DomainTools constantly monitors industry-known certificate transparency logs to find newly published certificates. These are collected in parallel with our web crawler and active collection sources and won't replace certificates gathered through the other methods.
2. Web Crawler
    a. When gathering web-related data on a domain, the web crawler also attempts to collect a certificate from both the apex domain and www subdomain.
    b. This certificate can replace the certificate gathered through active collection if it is more recent.
3. Active certificate crawls
    a. We attempt to gather certificates for domains identified by DomainTools on a weekly basis.
    b. Found certificates will replace the certificate gathered through web crawl if it is more recent.

Certificate Validation

- For certificates gathered in the weekly crawl, we check that the requested hostname is in either the cert's Common Name or Subject Alt Names fields. If the hostname is not present, the certificate is not collected.
- Certificates are gathered regardless of the trustworthiness of the issuing Certificate Authority so the broadest set of certificates is available for analysis.
- All certificates are gathered, even when their validity dates are outside of the gathering date.
- There is no support for certificate revocation in current certificate processing. .
- The quality and security of the checked server's SSL/TLS configuration is not checked: a server may have a valid certificate, but still have a weak SSL/TLS configuration.

For example, consider the self-signed certificates from the SSL Organization "Internet Widgits Pty Ltd".

The certs are self-signed, and cannot be trusted publicly, but are still collected and returned by Iris Investigate. Some may find certificates of this sort to be useful indicators, notwithstanding their non-public-trust status.

Iris Query Quotas and Duplicate Queries

Quotas are measured at the group level, and reset each month. Queries consume your Iris Investigate quota in the following ways.

Pivot Engine Queries in the Iris Investigate UI

The following activities do consume your quota:

- Executing an omnisearch (from `landing` or `search` pages) that returns results;
- Executing an advanced search that returns results;
- Sending a result to the Pivot Engine (including the `narrow`, `expand`, `new`, and `exclude` functions);
- Revisiting a search node >30 days since it was created;
- Loading new pages in the Pivot Engine;
- Sorting Pivot Engine results.

The following activities are considered **duplicate queries** and do not consume your quota:

- The query contains identical filter, sorting, and page parameters;
- The query matches the attributes of a query made that counted toward the quota within <30 days.

Passive DNS (pDNS) Queries in the Iris Investigate UI

The following activities do consume your quota:

- Executing a search query that returns results (from either the search field, or popovers throughout the UI);
- Executing/triggering the `load more` (i.e., infinite scroll) function in search results;
- Revisiting a search node >30 days since it was created.

The following activities are considered **duplicate queries** and do not consume your quota:

- The query contains identical filter, sorting, and page parameters;

- The query matches the attributes of a query that counted toward the quota within 30 days.

Queries in the Iris Investigate API

The following activities do consume your quota:

- Executing a query;
- Loading additional pages of results.

The following activities are considered **duplicate queries** and do not consume your quota:

- Identical queries made <1 hour of a previous query that counted against your quota.