Quick Start Guide

DomainTools

Iris Investigate

Part 1: Concept Overview

Security analysts and threat hunters have a tough—and important—job. Defenders must make threat assessment and response decisions related to known or suspected attacks, often under time pressure and with very high stakes. When examining domain names or IP addresses implicated in suspicious or malicious activity, two fundamental questions are always on a security team's mind: **Who is attacking me? What is the extent and nature of their infrastructure?**

Other investigators often seek information about individuals or organizations, and the domain space can be particularly illuminating for this, showing relationships such as parent/child companies, business diversity, etc.

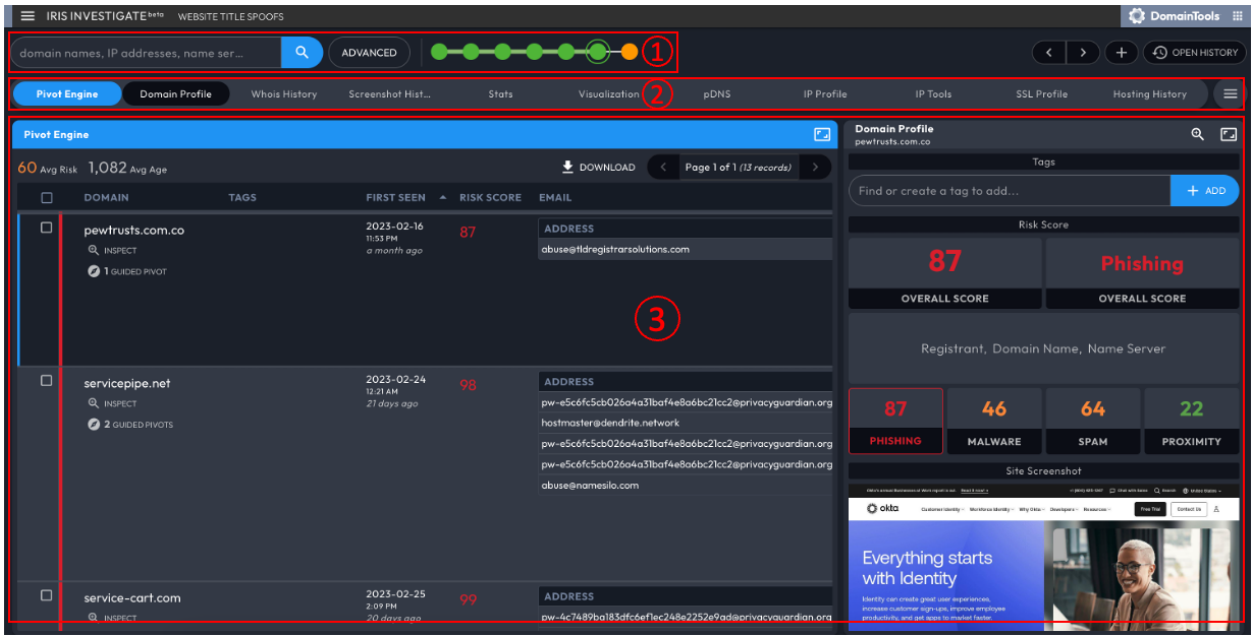
A SaaS offering designed to help quickly develop reliable answers to such questions, **DomainTools Iris Investigate** unites the world's largest domain profile data store and passive DNS data from Farsight Security DNSDB and other top-tier providers with query tools that complement and enhance natural investigative workflows. Iris Investigate's design is heavily influenced by close work with some of the world's best cyber intelligence investigators, to understand and respect their workflows, objectives, and operating constraints.

Part 2: Interface Description

When you receive this guide, you should already have been granted access to Iris Investigate. You can reach the interface at https://iris.domaintools.com/investigate
Once you have logged in to Iris Investigate, the initial landing page displays a search box that allows you to begin your investigation from some of the most common entry points:

- Domain name (single or list)
- Hostname
- Domain registrant name (person or organization)
- Registrant email
- IP address (single or list) or range

Most of your work in Iris Investigate will be conducted in a screen that looks similar to the below:



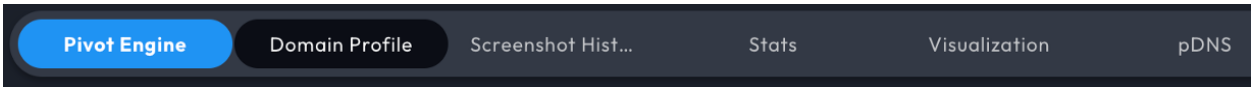
The interface has three main sections:

1. **Search and Search History:** The Search box is where you enter queries to the tool. You can click “Advanced” (next to the search box) to build more complex, nuanced searches, and you can click “Back” to go to the immediately preceding search.Search History display records a “breadcrumb trail” of your queries and pivots. It can help you retrace your steps, explore different branches of inquiry, and create a record of the steps that led you to a particular conclusion.
2. **Panel Ribbon:** Choose a data panel to view.
3. **Data Panels Arena:** This is where you conduct your investigation by working your way through searches, filters, and pivots. Each Data Panel has a specific purpose and set of information that it displays.

NOTE: The above screenshot depicts the interface in Dark Mode. You can select light or dark themes by clicking the three-bar menu in the upper left, choosing Settings, and clicking the “Themes” tab.

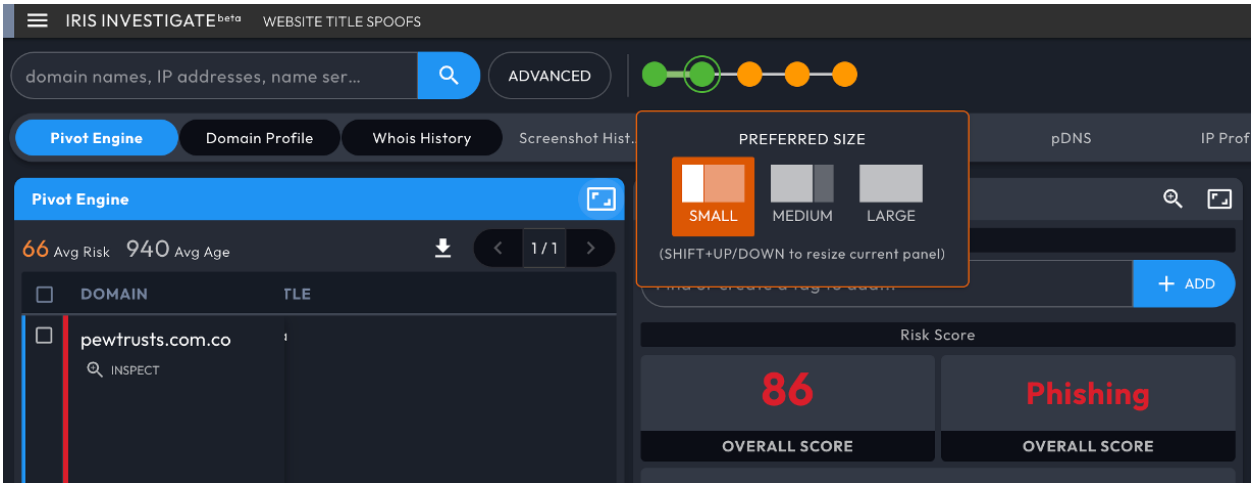
Arranging the Data Panels

Ordering Panels: The Panel Ribbon is below the search and history; it lists each panel name horizontally. You have flexibility to control the ordering of all the panels except for Pivot Engine, which is anchored on the far left. To change the order, from the Panel Bar, drag and drop a panel’s title to the desired new position.



Example: moving Visualization next to Pivot Engine

Panel Sizing: Each data panel can be configured to display as small, medium, or large. To make adjustments, click the sizing icon in the right side of the panel title box.



Or if you place your cursor between panels, the size selector will appear and you can adjust panel sizing from there. You can also double-click on the panel title box to change the size.

Note that the active panel (typically on the far left with the panel title box highlighted in blue) is given priority to display its preferred size. Any remaining screen area shows additional panels but those panels may not reflect their preferred size in order to ensure the active panel fully displays.

A few details on how panel sizing works: The goal is to use as much of the available screen as possible to show data. The panel on the far left is considered the “active” panel; it is highlighted in blue and given priority for display. As you move across panels, if the far-left one is any size except large, the remaining screen space will display adjacent panels to the right. If you have a large monitor, you can get quite a number of panels displayed side-by-side if you wish.

Pivoting on Datapoints

One of the fundamental goals of investigators using Iris Investigate is to discover and map connections between entities, which in turn helps them understand adversaries and their infrastructure, or business organizational structures. To this end, most of the data points (email addresses, IP addresses, name servers, etc) identified in Iris Investigate can serve as pivot points, helping the user discover other domains or IPs that are connected to the selected datapoints.

The Operations Menus that appear when you right-click (or CTRL-click) a datapoint enable the following:

- **Narrow Search:** filter the results set to show only those domains that match the selected term
- **Expand Search:** find all other domains in the DomainTools database that match the selected term and add them to current results
- **New Search:** find all other domains that match the term and present them (only) as a new results set
- **Exclude:** exclude all domains that match the selected term
- **pDNS (for domains or IP addresses):** examine passive DNS records related to the domain or the IP address

The number of domains matching the selection, which is shown in the Operations Menu, **gives a good hint as to whether the pivot will be fruitful**:

For example, abuse@wildwestdomains.com, which is a privacy email associated with millions of domains, won't help investigators find meaningful connections in most cases. On the other hand, ***a unique, personal email address*** *is a very strong indication of connection among domains.*

Data Panels

Pivot Engine: A table view of search results with sortable columns. You can choose the fields (columns) to display in the table from the Columns control in the navigation bar. **Many of the datapoints in the Pivot Engine are right-clickable links**, which invoke a menu of options for further exploration.

pDNS: A table showing passive DNS records for domains or IP addresses. The data populates in three ways: by searching on a domain or IP in the main search box; as a pivot from a domain; as a pivot from an IP address. You can also enter a hostname (e.g. hostname.example.com) in the main search box to see passive DNS records for that hostname, and domain profile information for the domain itself.

Visualization: A graphical view of search results, represented as nodes on the chart. This can often be a useful way to discover and understand relationships among domains, IPs, and more. As with the datapoints in the Pivot Engine, the nodes in the visual graph are right-clickable to modify the search.

Stats (for searches with at least two domains): A summary of key datapoints for the set of domains, showing the number of domains that share each datapoint. This can be a quick way to spot patterns of ownership, hosting, and other information.

Domain Profile and IP Profile: Each of these panels gives an at-a-glance view of information about the domain or IP address, respectively. When your search results in more than one domain, these panels are empty until you select a domain or IP address in the Pivot Engine table.

Whois History and Hosting History: Whois History shows a timeline for Whois records for the domain. The interface also allows you to compare adjacent records to spot changes. Hosting History gives details on IP addresses, domain registrars, and name servers associated with a domain. Each of those data types is right-clickable to enable a search pivot or gain more insight about it.

IP Tools: Ping and Traceroute networking tools as well as the DNS PTR (pointer) record for the IP address.

SAVED INVESTIGATIONS

Iris Investigate automatically records your investigative steps, with a default investigation name based on the search term with which you began the investigation. You can rename the investigation and provide a description of it. You can also delete investigations. *(Note: deleted investigations cannot be recovered!)*

Part 3: Sample Investigations

To help you explore Iris Investigate, below are two sample investigations, taken from actual historical cases. For simplicity, the steps below only involve a few of the data panels. Feel free to explore the others, as well.

> ***Note:*** *because many of the domains in these examples are tied to actual cybercrime, this guide always "defangs" the domain names by placing square brackets around the dot, e.g. example[.]com, to prevent your accidentally visiting a dangerous domain. Iris Investigate ignores the brackets, so you can paste or type the domains into the search box as they are.*

Example 1: Bank Phishing Investigation

Phishing has been implicated in many major data breaches. If a security team identifies a known or suspected phish, they can often learn important information about the phisher by discovering and examining connected infrastructure. That information can help them defend against the phisher, cooperate with law enforcement, monitor the attacker, etc. The first domain in this example was actually part of a phishing email received by a bank.

Preparation:

1. Log in to Iris Investigate at https://iris.domaintools.com/investigate
2. Begin at the Home screen (which is the default upon logging in)

Investigation sequence:

3. **Type or paste the phishing domain**, **goeoglledoc[.]com, into the search box**
4. Notice that the Pivot Engine data panel shows the information that DomainTools has about this domain, arranged across the table in a single row. Notice, too, that the Domain Profile panel gives a summary of the domain, including the "raw" Whois record and a screenshot thumbnail.
5. From the Pivot Engine data panel, find the Registrant name, **Reginald C. Rodman**. **Right-click this name**, and from the resulting menu, **click "Expand Search."** Iris Investigate now shows all domains that share this registrant name.
6. Notice the themes evident in the domain names, particularly the misspellings of bank names and shared document resources. **Consider what this tells an investigator**:
   a. This registrant has a clear pattern of targeting financial institutions (misspellings of bank names)
   b. These domains look like part of a coordinated phishing campaign: the misspelled domain names are meant to lure unsuspecting users into clicking them, either by mimicking a real institution or by appearing to be a shared file/document resource.
7. **Double-click Visualization** in the tabs at the bottom of the screen. This maximizes the Visualization data panel. In the list of fields, **use the controls to show the four fields of Registrant, IP, Email, and Create Date**.
8. Notice that the create dates show particular "hotspots" of domain registration activity. This could further help an investigator pinpoint possible timeframes to look for evidence of the phishing campaign. The visual graph also helps make relationships among entities very easy to grasp.
9. If desired, **you could continue the investigation** by pivoting on any of the email addresses

shown as nodes in the graph. Remember that right-clicking the nodes brings up a menu that shows how many domains DomainTools knows about that share that datapoint.

10. Notice, in the navigation bar on the left side of the screen, that **Iris Investigate has automatically created an investigation for you**. You will later be able to re-visit this investigation, with all of its steps recorded in Search History. You can also delete the investigation if you wish—just keep in mind that once deleted, it can't be recovered.

From the above, you can see how, within just a few minutes, an investigator can learn a great deal about the context of the initial phishing domain, and can orient defenses properly against this threat.

Example 2: "Volatile Cedar" APT Investigation

"Advanced Persistent Threat," or APT, is common parlance for threat actors and/or the tools they use to attack high-value targets. This investigation focuses on a group that Check Point, a network security company, called "Volatile Cedar" in an excellent report they produced. Check Point picked the name based on their attribution of the activity to Lebanon.

In this sample investigation, you will see how DomainTools historical data can help uncover the identities of threat actors who use domain registration privacy services to conceal their identities.

Investigation sequence:

1. From the Navigation bar on the left, **click Start New Investigation.** Note that you can give the investigation a name and/or a description if you wish. (You may need to expand the Navigation bar by clicking the arrow at the bottom-left of the screen)
2. In the search box, **type or paste dotnetexplorer[.]info**
3. In the Pivot Engine (or the Domain Profile) data panel, notice that this domain is registered with Whois privacy, obscuring any details about the domain's registrant.
4. From the tabs at the bottom of the screen, **double-click Whois History**
5. Notice the timeline on the left part of the screen. Privacy-protected records are denoted by an icon (eye with a slash over it)
6. **Click the date 2014-12-05**, which does not have this icon
7. Notice the "raw" Whois record in the gray box in the center-right part of the screen. You can see in this record that the registrant of the domain gave an address in Beirut, before putting the domain under private registration
8. **Bonus: Look at Screenshot History, and click "See all."** The screenshots are very similar, which tends to reinforce that it was the same registrant who operated this domain under open registration and under privacy (as opposed to the domain dropping and being picked up by a different person/organization)

This sequence demonstrates a method that DomainTools customers use regularly to learn more about domains that are cloaked in Whois privacy.

Appendix: Additional Resources

The following links may be helpful as background or for additional details about Iris Investigate:

Iris Investigate User Guide
Iris Investigate Product Page
About DomainTools