

DomainTools Iris

Investigative Power from the Leader in Domain and DNS Threat Intelligence



10 Billion+
Current and Historical
Whois Records



4.5 Billion+
IP Address
Change Events



1.8 Billion+
Registrar
Change Events



3 Billion+
Name Server
Change Events



580 Million+
Screenshots

Get Decisive Intelligence, Fast

The Internet can be a great place to hide. There are over 300 million domain names, over 4 billion IP addresses and many more nameservers, hostnames and email addresses within the infrastructure of DNS. Criminals make use of all of these resources to attack their targets, moving often and hiding in plain sight behind Whois privacy and shared hosting environments.

Within this context, threat intelligence analysts and incident response professionals must make critical decisions about proper defenses or countermoves. They need reliable information quickly, and must arm themselves with the best tools and data in order to expose threat infrastructure and defeat criminal networks. Fortunately, they have a potent new tool in the fight—**DomainTools Iris**.

Iris is a proprietary threat intelligence and investigation platform that combines enterprise-grade domain and DNS-based intelligence with an intuitive web interface, helping security teams quickly and efficiently investigate potential cybercrime and cyberespionage.

The screenshot displays the DomainTools Iris interface with several key components:

- Pivot Engine:** A table listing domains with associated metrics like AdSense, Alexa, Risk Score, and IP information.

Domain	AdSense	Alexa	Risk Score	IP
1domaintools.com			45.23	185.53.179.13
advertising-info			30.03	64.74.223.46
airtonizer.com			19.96	208.73.211.164
antiblock.com			19.96	185.53.179.13
arch3d.com			30.1	8.5.1.45
autigliantours.com			38.52	185.53.179.20
- Visualization:** A network graph showing relationships between domains, registrars, and IP addresses.
- Domain Profile (domaintools.com):**
 - IP Address History:** 85 changes on 29 unique IP addresses over 8 years.
 - Registrar History:** 4 registrars.
 - Name Server History:** 6 changes on 6 unique name servers over 11 years.
 - Whois Record:**

```


Domain Name: DOMAINTOOLS.COM
Registrar: DOMAIN ID: 1471312_DOMAIN_COM-VALE
Registrar WHOIS Server: whois.eonm.com
Registrar URL: www.eonm.com
Updated Date: 2014-07-24T11:07:33.000
Creation Date: 1994-08-02T04:00:00.000
Registrar Registration Expiration Date: 2017-08-01T04:00:00.000
Registrar: EONM, LLC
Registrar IANA ID: 48
Domain Status: clientTransferProhibited https://www.icann.org/epp/1
Registrar WHOIS ID:
Registrar Name: DOMAIN ADMINISTRATOR
Registrar Organization: DOMAINTOOLS, LLC
Registrar Street: 2211 350 AVENUE
Registrar State: WASHINGTON
Registrar City: SEATTLE
Registrar State/Province: WA
          
```
- Stats:**
 - IP Country Code (8 values):**

UNITED STATES	192
SWITZERLAND	20
GERMANY	14
CAYMAN ISLANDS	4
UNITED KINGDOM	4
LUXEMBOURG	2
AUSTRIA	2
AUSTRALIA	1
 - IP (88 values):** (List of IP addresses)
- Screenshot History:** A gallery of website screenshots.

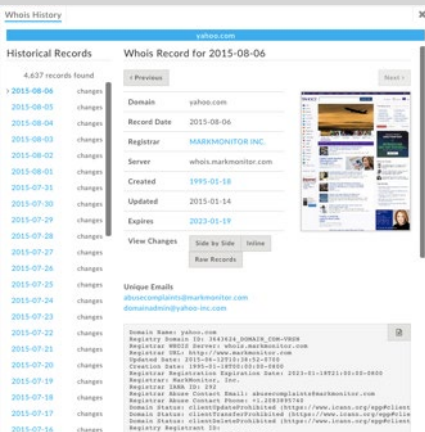
Benefits

- **Better Data Gives You Better Answers**—Put the world’s largest database of domain profile information to work for you and avoid the blind spots that come with inferior data sources.
- **Designed By Investigators, For Investigators**—DomainTools works with some of the best cybercrime investigators in the world. Iris was purpose-built for their best practices and methodologies and democratizes threat intelligence by bringing this power to a much broader spectrum of organizations.
- **Changes the Economics of Attribution**—The expense of hiring external expertise or assigning internal resources to adversary analysis has always been prohibitive. DomainTools Iris changes the equation, enabling high-confidence profiling and attribution at costs far below traditional means.
- **Provides Visibility Beyond the Firewall**—Simply identifying malicious domains and IP addresses doesn’t protect organizations against the extended networks operated by threat actors. DomainTools Iris gives organizations the ability to create forensic maps of criminal activity to triage threat indicators, assess risk, and prevent future attacks.

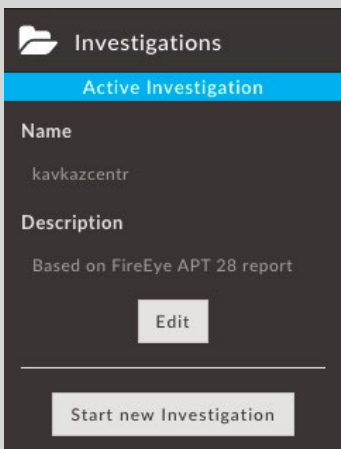
Key Features



Visualization shows the relationships among entities



Whois History lets you go back in time



Create and revisit saved investigations

Who Uses DomainTools?

The largest organizations in the world across all major verticals, including:

- Banking and Finance
- Healthcare
- Energy and Utilities
- Government
- Technology

Try it Out

DomainTools Iris is a premium research tool. If you would like to experience the power of Iris, please email sales@domaintools.com or call 206-838-9020.