

# Digital Network Intelligence [DNINT]

---

## WHOIS

---

- [WhoisFreaks](#)  
An API which allows you to search for WHOIS records by company name, owner name or keyword. Currently has over 430 million records dating as far back as 1986. Requires registration.
- [Whoisology](#)  
Search for WHOIS records and other data via domain name, email address or keyword. For enhanced results, a paid subscription is required.
- [DomainBigData](#)  
Find the registrant and other domains owned by the same person with their reverse WHOIS. Find domain history, domains on same IP, network owner and more.
- [GoFindWHOIS](#)  
A great online tool for locating information about a website or IP address. Offers WHOIS lookups, DNS records, IP tools, and other website enumeration tools. Created by [@netbootcamp](#), so be sure to follow them for updates.
- [Marcaria](#)  
Search WHOIS information in over 2,000 extensions including international ccTLDs and gTLDs.
- [IQ WHOIS](#)  
A great WHOIS search tool that offers downloadable databases, historical WHOIS records and more.

## Internet Protocol Addresses [IP]

---

- [IKnowWhatYouDownload](#)  
Search an IPv4 or IPv6 address and view the most recent torrents that have been downloaded or that the user is currently seeding.
- [AbuseIPDB](#)  
A database of abuse reports. Search an IP address and see if it has been included in any abuse reports, malicious activity reports, and spam campaigns.
- [Hurricane Electric BGP Toolkit](#)  
Contains loads of great networking tools.
- [BGPView](#)  
A BGP toolkit and ASN routing lookup tool that allows you to debug and investigate information about IP addresses, ASN, IXs, BGP, ISPs, prefixes and domain names.
- [InfoSniper](#)  
Provides detailed IP geo-location information.
- [IP Hub](#)  
An IP lookup tool featuring proxy and VPN detection. A free API is also available. Requires a paid subscription for best results.
- [IP Quality Score](#)  
A collection of fraud detection tools including proxy and VPN detection, bot detection, email validation, and lots of other tools. Offers many free tools. Requires a paid subscription to be able to use everything.
- [IP Teoh](#)  
Simple tool that provides basic information about an IP address. Geo-location, ISP, and

proxy/VPN/TOR node detection.

- [CentralOps](#)  
A great collection of various networking tools. Ping, traceroute, WHOIS, nslookup, domain dossier and so on.
- [IP-Neighbors](#)  
Find neighboring websites, hostnames, and domains. Get an idea who runs a host, the hosting density, and neighboring hosts
- [NetworksDB](#)  
Contains information about the public IPv4 and IPv6 addresses, networks and domains owned by companies and organizations across the world along with city-level IP geolocation data and autonomous system information. Also offers a free API.
- [PeeringDB](#)  
A user-maintained database of networks. Provides a wealth of interconnection data.
- [Robtex](#)  
Gathers public information about IP numbers, domain names, host names, autonomous systems, routes, etc. It then indexes the data in a big database and provides free access to the data.
- [IntelX IP Address Search](#)  
A great IP address search tool offered by IntelX.

## Domain Name System [DNS] Records

---

- [PTArchive](#)  
Search for historical reverse DNS records. Currently has over 230 billion records retrieved from 2008 to now.
- [PassiveDNS](#)  
Search for DNS records via domain name.
- [IntoDNS](#)  
Checks the health and configuration of DNS and mail servers.
- [ViewDNS Info](#)  
Allows users to gather a large amount of data about a given website or IP address.
- [DNSlytics](#)  
Offers loads of great tools such as DNS, MX, WHOIS and SPF lookups along with multiple reverse search tools.
- [dnstwister](#)  
The anti-phishing domain name search engine and DNS monitoring service, Search a domain name and this tool will show you related domain names that could potentially be used for phishing campaigns.
- [DMNS](#)  
Domains App makes it easy to see domains availability across extensions and notifies you about any WHOIS or DNS changes.
- [DomainCodex](#)  
Research domain information and all associated data, including records, IP addresses, page metadata, location and much more. Has over 315 million indexed domains.
- [IntelX Domain Search](#)  
A great domain search engine offered by IntelX.

## Website Analysis

---

# Enumeration

- [Wappalyzer](#)  
Discover what software versions are running on any website.
- [BuiltWith](#)  
Find out what technology a website is running.
- [w3techs](#)  
See which technologies a website is running, such as CMS, programming language, web server and hosting provider.
- [HackerTarget](#)  
Find virtual hosts, server info and IP address reputation of a server or IP address. Gather IP address intelligence including hosting provider, ASN, netblock and IP geolocation.
- [NetCraft Site Report](#)  
Find out the infrastructure and technologies used by any site.
- [Hexometer](#)  
Check out the technologies that are being used on any website.
- [LargerIO](#)  
Uncovers the technologies used on websites.
- [CMLabs](#)  
List the websites that use a particular technology, with email addresses and phone numbers. Use this to find new leads, market analysis and competitor research.
- [AnalyzeID](#)  
Helps locate websites that have the same owner. Checks for matching email, Facebook app ID and nameservers. Search by URL.
- [Pulsedive](#)  
Enter a URL and receive information such as threat intelligence reports, port scans, IP details, additional URLs, subdomains and other IOCs.
- [MMHDAN](#)  
Calculate a fingerprint of a website. Things like HTML, Favicon, Certificates in SHA1, SHA256, MD5 and MMH3. Lets you create links to quickly search in various IoT search engines.
- [Snyk Vulnerability Scanner](#)  
Performs a basic passive vulnerability scan on a website. Detects outdated technologies, insecure HTTP headers, XSS and more.
- [CookieServe](#)  
Enter the URL of a website and find out what cookies are being used and understand their purpose.
- [Reverse Google AdSense](#)  
Locate domains with the same Google AdSense ID.
- [Lookyloo Web Forensics Tool](#)  
Captures websites and let you analyze and investigate them.
- [The Favicon Finder](#)  
A free online service to finding icons on websites. Just enter in a target URL.
- [SOCRadar Deep Web Report](#)  
Search a domain and get a simple report of the companies exposure. Requires a paid subscription to view full reports.
- [Well-Known.dev](#)  
Search well-known resources, phrases, and terms served by ad sites across the web.
- [AdsByDomain](#)  
Scan a domain and visualize that domains ads.
- [StylifyMe](#)  
A great tool for analyzing the style characteristics of a particular website.

## Web Page Monitoring

- [FollowthatPage](#)  
A change detection and notification service that sends you an email when your favorite web pages have changed.
- [WatchThatPage](#)  
A service that enables you to automatically collect new information from any web page. Select which pages to monitor, and this will find which pages have changed, and collect all the new content for you.
- [VisualPing](#)  
Enter a URL that you would like to monitor, then enter an email address and this will send you emails everytime that page changes.
- [Carbon Dating The Web](#)  
Predict the birthday of any web page.
- [GemiusAudience](#)  
Provides knowledge and information for online publishers, investors, media agencies and advertisers to make the right decisions.  
For example you can find, in the listed countries, how many some visitors or users a website has.

## Uniform Resource Locators [URL] Redirects and Backlinks

---

- [RedirectDetective](#)  
A free URL redirection checker that allows you to see the complete path a redirected URL goes through.
- [WhereGoes](#)  
Allows you to do a full trace of URL redirects.
- [SpyOffers](#)  
A tool for tracking and recording the redirection paths of a URL.
- [SEO Spyglass Backlink Checker](#)  
Allows you to find out how many sites are linking to a certain web page. Requires registration to view full results.
- [Backlinks Analyzer](#)  
See how many sites link to a web page.
- [SpyFu](#)  
Displays website information and metrics, SEO analytics, backlinks and more by searching a URL.
- [CheckShortURL](#)  
Easily expand URLs from most URL shortening services such as t.co, goo.gl, bit.ly, amzn.to, tinyurl.com, ow.ly,youtu.be and more.
- [URLScan](#)  
Scan URLs for any malicious activity.
- [OpenLinkProfiler](#)  
A free link research tool that enables you to check the backlinks of any website. Enter a domain name in the search box and click the 'Get backlink data' button to get an immediate link analysis.
- [Short Link Verification Cheatsheet](#)  
A list of techniques to verify links from many URL shortening services. Created by [@SIENT\\_pl](#).  
Archived [here \(Wayback\)](#) and [here \(archive.today\)](#).

## Wireless Fidelity [WiFi]

---

- [WiGLE](#)  
The Wireless Geographic Logging Engine is a website for collecting crowd-sourced wardriving information about the different wireless networks and cell towers around the world. Users can register on the website and upload hotspot data like GPS coordinates, SSID, MAC address and the encryption type used on the hotspots discovered. Great way to get an address from a Wi-Fi SSID.
- [Mylnikov API](#)  
A free API that allows you to get latitude and longitude by Wi-Fi BSSID or MAC address.
- [OpenWiFi](#)  
API and database. The project seems idle since 2018 but the service is still online.
- [3WiFi](#)  
Similar to Wigle, this is a interactive, crowd-sourced map of wireless access points.
- [RadioCells](#)  
A community project to collect information on cell tower and Wi-Fi base stations and plot them on a map. The project itself was founded in 2009.
- [OpenWiFiMap](#)  
Database and map for free network Wi-Fi access points from all over the world.
- [WiMan](#)  
Helps find all the free Wi-Fi hotspots available per destination and elsewhere in the world.
- [WiFiSpace](#)  
Find open free and public Wi-Fi hotspots practically anywhere in the world.
- [WiFi Map](#)  
Another site that shows you publicly open Wi-Fi networks by location. They also offer a mobile app.
- [BT WiFi](#)  
The UK's biggest Wi-Fi hotspot network. Over 5 million available hotspots nation wide.
- [OpenWiFiSpots](#)  
Search for free open wireless networks worldwide.
- [Airport WiFi](#)  
Provides WiFi passwords from airports and lounges around the world.

## Media Access Control [MAC]

---

- [MAC Address Lookup](#)  
Lookup any MAC address and view the manufacturers name.
- [MAC and OUI Lookup](#)  
Displays the name of the company that manufactured a network card. You can also do a reverse lookup and find the MAC addresses registered by a company.
- [MAC Lookup](#)  
Another tool that provides information about any MAC address.
- [MAC Address Search](#)  
Yep, it's another MAC address search tool.

## User Agents

---

- [User Agent Parser](#)  
Lookup a browser user-agent and view details about it such as software versions, OS types, and more.
- [UA Parser](#)  
A simple tool that displays your current user agent strings.

## Internet of Things [IoT] Search

---

## Device Discovery

- [Shodan](#)  
A search engine that lets the user find specific types of computers and IoT devices connected to the internet using a variety of filters.
- [Censys](#)  
The search engine for finding internet devices, like computers, servers, and other smart devices.
- [ZoomEye](#)  
Another search engine which is used mostly to see open devices that are vulnerable and most often used by pentesters to test or exploit their vulnerabilities over the internet. Zoomeye lets user find specific connected network devices.
- [Thingful](#)  
A search engine for the internet of things (IoT), providing a unique geographical index of connected objects around the world, including energy, radiation, weather, and air quality devices as well as seismographs, iBeacons, ships, aircraft and even animal trackers.
- [GreyNoise](#)  
Collects, analyzes, and labels mass internet scan and attack activity into a feed of Anti-Threat Intelligence (ATI).
- [Natlas](#)  
This is described as a "collection of nmaps". Catalogs things like open ports and software versions.
- [ONYPHE](#)  
A cyber defense search engine for open-source and cyber threat intelligence data. Collected by crawling various sources available on the Internet and active internet scanning.
- [FOFA](#)  
FOFA is a cyberspace search engine. It help customers find IP assets quickly. Essentially a clone of Shodan.
- [LeakIX](#)  
Search engine indexing open ports on the internet. It focuses on listing the databases and table names and keeps an history of every successful connection.
- [BinaryEdge](#)  
Focuses on acquiring, analyzing and classifying internet wide data by combining efforts in the areas of cybersecurity, data science and machine learning. Requires registration.

## CCTV and Webcams

- [EarthCam](#)  
A searchable global network of live streaming webcam feeds.
- [WebCamTaxi](#)  
Directory of open webcams organized by country and location.
- [OpenTopia](#)  
Catalogues live webcams that have been found via search engines. Allows you to view camera feeds plotted on a map.
- [Insecam](#)  
Live cameras directory. Claims to be the world's biggest directory of online surveillance security camera feeds. Searchable by location or camera manufacturer.
- [The Webcam Network](#)  
A large directory of open CCTV and webcams, organized by location.
- [Windy Webcams](#)  
A large open webcam directory. Formally known as "Lookr".

- [WebcamMap](#)  
A directory or open IP cameras plotted on a map.
- [SkylineWebcams](#)  
View live webcam feeds from around the world. Sorted by country.
- [AirportWebcams](#)  
Directory of webcams from various airports and runways from around the world.
- [KrooozCams](#)  
Another large directory or open IP cameras.
- [London Traffic Cams](#)  
Live feeds of traffic cameras in London, England.
- [London Traffic Cams 30 Day Archive](#)  
A 30-day archive of traffic camera footage from London, England.
- [Fisgonia](#)  
Directory of open IP cameras plotted on a map. Website is in Spanish.
- [List of Unsecured IP Cameras](#)  
A great article that describes the most common types of IP cameras that are exposed online. Also provides a list of default credentials for common IP cameras.
- [IPVM Camera Calculator](#)  
Calculate the field of view, layout and design of a CCTV camera network.
- [CamVista](#)  
A directory of open IP cameras. Appears to be outdated, but still worth mentioning.
- [Deckchair](#)  
A directory of live camera feeds organized by location.
- [Surveillance Under Surveillance](#)  
Shows you cameras and guards almost everywhere. You can see where they are located and, if the information is available, what type they are, the area they observe, or other interesting facts.
- [Ukraine Live Cams](#)  
A large collection of live and real-time webcams in Ukraine plotted on 3D map.

## Attack Maps

---

- [Bitdefender Threat Map](#)  
A cyber threat and cyber-attack map that displays information in real-time.
- [Kaspersky Cyberthreat Map](#)  
Displays cyber-attacks in real-time with very pretty animations.
- [Digital Attack Map](#)  
A map that displays distributed denial-of-service (DDoS) attacks in real-time.
- [FireEye Cyber Threat Map](#)  
Shows on-going cyber threats and cyber-attacks in real-time.
- [LookingGlass Threat Map](#)  
Shows attacks and infections for known malware in real-time.
- [CheckPoint Live Cyber Treat Map](#)  
Displays real-time malware infections, phishing attacks and exploitation on a map.
- [Talos Intelligence Reputation Center](#)  
Claims to be the world's most comprehensive real-time threat detection network. Includes an interactive map.
- [Spamhaus Live Botnet Threat Map](#)  
A live map of botnet activity, zombies and C2 servers.
- [Imperva Threat Attack Map](#)  
Real-time view of on-going cyber attacks.

- [Talos Intelligence Cyber Attack Map](#)  
A live map that shows the top spam and malware distributors.
- [ThreatButt](#)  
A real-time cyber attack map. By far the most 1337 looking attack map out there.
- [Akamai Attack Visualizations](#)  
This real-time visualization shows the phishing, malware, and command & control threats that Akamai is blocking (for customers) through its Intelligent Platform and its unprecedented insights into DNS and IP traffic.
- [Fortinet Threat Map](#)  
Interactive map that displays statistics of active cyber attacks in real-time.
- [Sophos Threat Intelligence](#)  
A static threat tracking map. All data comes from SophosLabs monitoring and malware research activities. Map is not in real-time.
- [NetScout Omnis Threat Map](#)  
Displays DDoS attacks observed globally in real-time as well as other statistics such as size, type, sources, destinations, time span and more.
- [SonicWall Worldwide Attacks](#)  
Provides a graphical view of worldwide attacks over the last 24 hours. It shows which countries are being attacked and where the attack originates. This interactive map shows not only malware attacks, but ransomware, encrypted traffic, intrusion attempts, and spam/phishing attacks. Also included are attack site statistics for the past 24 hours.

## Public Buckets

---

- [Public Buckets](#)  
Find public AWS and Azure buckets and documents via keyword.
- [GreyHatWarfare Bucket Search](#)  
A great tool that lists open AWS S3 buckets and helps you search for interesting files. Requires registration for limited free use. Requires a paid subscription to access advanced features.

## Exploits and Proof of Concept [PoC]

---

- [ExploitDB](#)  
An archive of exploits, vulnerabilities, shellcode, 0days, security articles, whitepapers and more. Ran by Offensive Security.
- [GHDB](#)  
The Google Hacking Data Base is an index of search queries (we call them dorks) used to find publicly available information, intended for pentesters and security researchers.
- [MITRE CVE](#)  
The mission of the CVE program is to identify, define, and catalog publicly disclosed cyber-security vulnerabilities.
- [NIST NVD](#)  
The U.S. government repository of standards based vulnerability management data represented using the Security Content Automation Protocol (SCAP). Enables automation of vulnerability management, security measurement, and compliance. The NVD includes databases of security checklist references, security-related software flaws, misconfigurations, product names, and impact metrics.
- [CVE Details](#)  
You can browse for vendors, products and versions and view CVE entries, vulnerabilities, related to them. You can view statistics about vendors, products and versions of products. Vulnerability data is updated daily using NVD feeds.



- [VulDB](#)  
A vulnerability database documenting and explaining security vulnerabilities, threats, and exploits since 1970.
- [CVE Trends](#)  
Crowdsourced CVE intelligence and trends.
- [0day.today](#)  
A database and marketplace for both public and 0day exploits.
- [RouterPwn](#)  
An outdated database of router exploits.
- [Vulners](#)  
Claims to be the largest correlated database of vulnerabilities and exploits.

## Advanced Persistent Threats [APTs]

---

- [MITRE ATT&CK Groups](#)  
Great collection of known APT groups that are currently in operation as well as groups that are no longer active.
- [\[XLSX\] APT Groups and Operations](#)  
A large list of known APTs that is organized by country of operation. Archived copies available [here \(Wayback\)](#). Offline copy available [here \(AnonFiles\)](#).
- [\[IMAGE\] APT Operation Groups](#)  
A collection of infographics that display the various known and currently active cyber operation groups per country. Archived [here \(Wayback\)](#) and [here \(archive.today\)](#).

## Malware and Malware Analysis

---

- [vx-underground](#)  
The best source for malware samples available on the internet. They also have large archives of various whitepapers, zines and other interesting things.
- [Malware Traffic Analysis](#)  
A source if pcap files and malware samples. Since the summer of 2013, this site has published over 2,000 blog entries about malicious network traffic. Almost every post on this site includes pcap files and/or malware samples.
- [DarkFeed](#)  
A live feed of malicious indicators of compromise (IOCs). Including domains, URLs, hashes, and IP addresses.
- [Malpedia](#)  
The primary goal of Malpedia is to provide a resource for rapid identification and actionable context when investigating malware.
- [Abuse.ch](#)  
A research project at the Bern University of Applied Sciences (BFH). Home of some great projects such as MalwareBazaar, botnet C&C trackers, SSL blacklists and more.
- [URLHaus](#)  
A project from abuse.ch with the goal of sharing malicious URLs that are being used for malware distribution.
- [FireHOL IP Lists](#)  
This site analyses all available security IP Feeds, mainly related to on-line attacks, on-line service abuse, malwares, botnets, command and control servers and other cybercrime activities.
- [Ransom-DB](#)  
Provides ransomware tracking in real-time, tracking ransomware groups and their victims.

- [RansomWatch](#)  
A constantly updated database that tracks ransomware operators.

## Personal Connection Profiling

---

- [GRC SheildsUP](#)  
Great tool for profiling your internet connection and router for exposure, potential vulnerabilities, and open ports. These are the results you want to see; [\[IMAGE\] SheildsUP TruStealth](#), [\(Wayback\)](#), [\(archive.today\)](#).
- [IPLeak](#)  
See what information you are giving away while browsing the internet. IP addresses, DNS leaks, WebRTC leaks, fingerprints and user-agent.
- [BrowserLeaks](#)  
Here you will find a gallery of security testing tools that will show you what kind of personal data can be leaked, and how to protect yourself from it.
- [DNS Leak Test](#)  
A simple tool to check for DNS leakage.
- [WebKay](#)  
A demonstration of all the data your browser knows about you. All this data can be accessed by any website without asking you.
- [PrivacyTests](#)  
An open-source list of web browser privacy tests.
- [Trackography](#)  
Find out who is tracking you when you are reading your favorite news online.

## Browser Extension Resources

---

- [CRXcavator](#)  
Automatically scans browser extension stores every 3 hours and produces a quantified risk score for each extension. Catalogs extensions for Chrome, Firefox and Edge.
- [Crx4Chrome](#)  
A catalogue of Chrome extensions. Allows you to download older versions and view related metadata about an extension.
- [Firefox Legacy Collector Dump](#)  
A large archive of legacy Firefox browser extensions.
- [ca-archive](#)  
Another catalogue of classic Firefox add-ons created before WebExtensions apocalypse.

## Other Tools

---

- [Domains-Index](#)  
An index of registered domains, sorted by TLD. Allows you to download lists of registered TLDs in .csv format. Requires registration and a paid subscription. However, some TLD lists are free.
- [ZoneFiles](#)  
Another index of registered domains sorted by TLDs. Updated daily. Requires paid subscription and registration to access their datasets.
- [Zone-H](#)  
An Internet security portal containing original IT security news, digital warfare news, geopolitics, proprietary and general advisories, analyses, forums, and a large archive of website defacements.
- [Default Router Settings](#)  
A list of default settings and login credentials for over 2,000 routers.

- [OpenSezMe](#)  
Contains over 6,000 default credentials for routers and other IoT devices.
- [Browserling](#)  
Allows you view a website in a different browser online. For example, a Mac user can test a website to see how it acts in Internet Explorer, without having to install a VM.
- [ISP Quick List](#)  
A free database that lists ISPs for wireless, broadband, DSL, ADSL, cable, etc. Organized by country.
- [ISP Today](#)  
A worldwide database of internet service providers.
- [Wikipedia - Lists of Internet Service Providers by Country](#) ([WikiLess](#))  
Lists of ISPs organized by country.
- [API Guesser](#)  
Enter the API key or token to find out which service it can be used by.