

## **Cyber Security Essentials**

### **Lab 7 – Open-Source Intelligence (OSINT)**

#### **Task 1: OSINT**

Read and understand about OSINT. Write about OSINT in your own language.

The insight gained from processing and analysing public data sources such as broadcast TV and radio, social media, and websites is known as open-source intelligence (OSINT). Text, video, image, and audio data are available from these sources.

The analysis is based upon machine learning and deep neural network algorithms which enable the system to learn from the data to achieve and refine recognitions of patterns, trends, and relationships.

#### **Task 2: WHOIS**

Go to <https://www.whois.com/> and search for any website. See what all information you are getting about that domain.

Whois is a widely used Internet record listing that identifies who owns a domain and how to get in contact with them. The Internet Corporation for Assigned Names and Numbers (ICANN) regulates domain name registration and ownership.

Whois  
Identity for everyone

Enter Domain or IPWHOIS

DOMAINSWEBSITECLOUDHOSTINGSERVERSEMAILSECURITYWHOISUPPORTLOGIN

amazon.comUpdated 2 days agoInterested in similar domains?

Domain Information

Domain:

amazon.com

Registrar:

MarkMonitor Inc.

Registered On:

1994-11-01

Expires On:

2024-10-30

Updated On:

2019-05-07

Status:

clientDeleteProhibited  
clientTransferProhibited  
clientUpdateProhibited  
serverDeleteProhibited  
serverTransferProhibited  
serverUpdateProhibited

Name Servers:

ns1.p31.dynect.net  
ns2.p31.dynect.net  
ns3.p31.dynect.net  
ns4.p31.dynect.net  
pdns1.ultradns.net  
pdns6.ultradns.co.uk

amazonexpressjobs.co  
m

Buy Now

getamazon24.com

Buy Now

amazonexpressreviews.  
com

Buy Now

amazonexpressnews.co  
m

Buy Now

amazoninvest.net

Buy Now

amazonevents.net

Buy Now

Sale

Whois  
Identity for everyone

Enter Domain or IPWHOIS

DOMAINSWEBSITECLOUDHOSTINGSERVERSEMAILSECURITYWHOISUPPORTLOGIN

amazon.comUpdated 2 days agoInterested in similar domains?

Domain Information

Domain:

amazon.com

Registrar:

MarkMonitor Inc.

Registered On:

1994-11-01

Expires On:

2024-10-30

Updated On:

2019-05-07

Status:

clientDeleteProhibited  
clientTransferProhibited  
clientUpdateProhibited  
serverDeleteProhibited  
serverTransferProhibited  
serverUpdateProhibited

Name Servers:

ns1.p31.dynect.net  
ns2.p31.dynect.net  
ns3.p31.dynect.net  
ns4.p31.dynect.net  
pdns1.ultradns.net  
pdns6.ultradns.co.uk

amazonexpressjobs.co  
m

Buy Now

getamazon24.com

Buy Now

amazonexpressreviews.  
com

Buy Now

amazonexpressnews.co  
m

Buy Now

amazoninvest.net

Buy Now

amazonevents.net

Buy Now

Sale

Postal Code:

89507

Country:

US

Phone:

+1.2062664064

Fax:

+1.2062667010

Email:

hostmaster@amazon.com

Technical Contact

Name:

Hostmaster, Amazon Legal Dept.

Organization:

Amazon Technologies, Inc.

Street:

P.O. Box 8102

City:

Reno

State:

NV

Postal Code:

89507

Country:

US

Phone:

+1.2062664064

Fax:

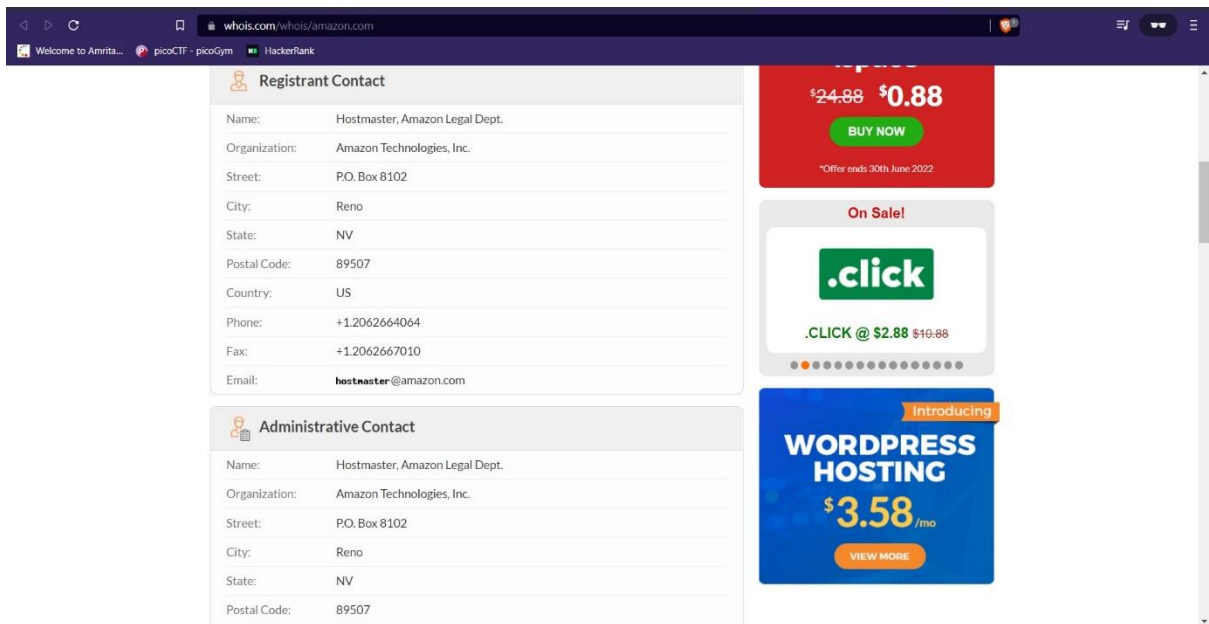
+1.2062667010

Email:

hostmaster@amazon.com

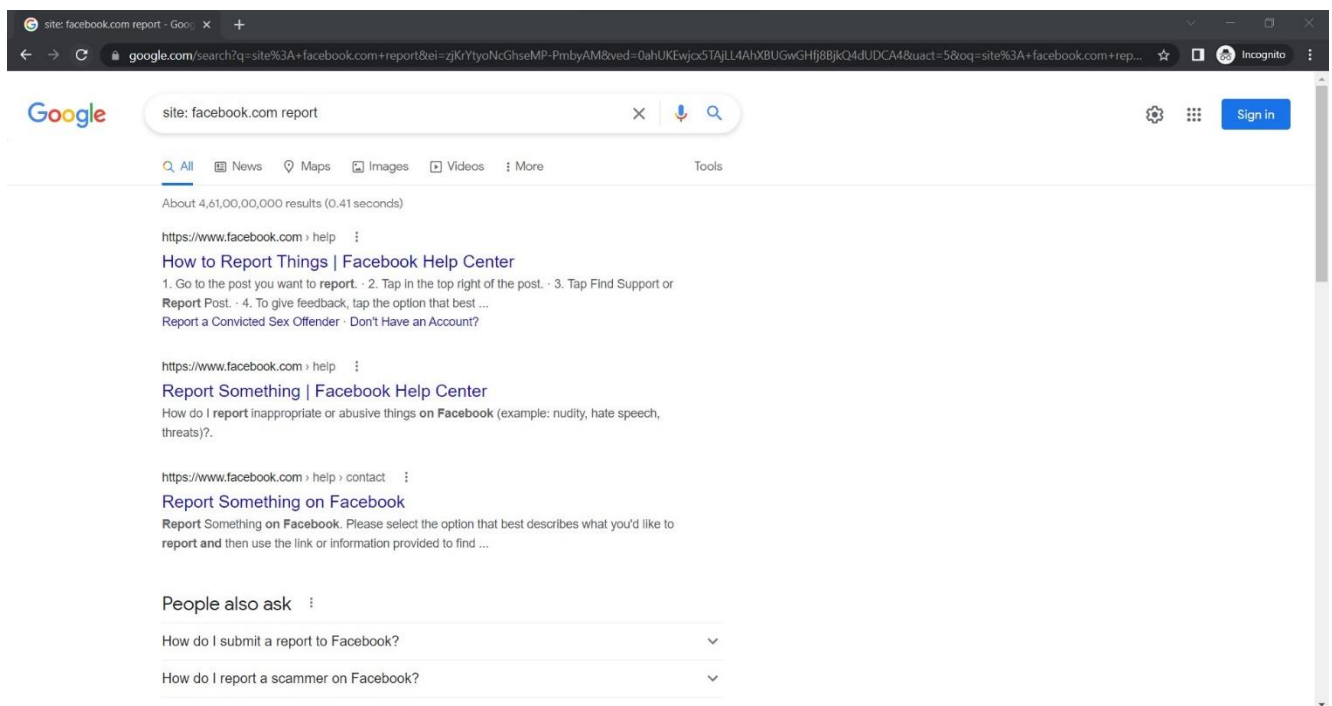
Raw Whois Data

Domain Name: amazon.com



### Task 3: Google Hacking

Read about google hacking and make a note on it. Use below commands after changing the website name and searched text 'report'. You can choose any website and text of your own.



link: facebook.com report - Google

google.com/search?q=link%3A+facebook.com+report&ei=7zKrYpfmB6OQseMPvs2w4Ac&ved=0ahUKEwjXmcXPjLL4AhUJSGwGHb4mDHwQ4dUDCA48uact=5&oq=link%3A+facebook.com...

link: facebook.com report

About 4,28,00,00,000 results (0.55 seconds)

<https://www.facebook.com/help/search?q=report+link>

### Report - Facebook Help Center

How to **Report** Things The best way to **report** abusive content or spam on Facebook is by using the **Report** link near the content itself. Below are some exa.

#### People also ask

- Where is the report link on Facebook?
- How do I submit a report to Facebook?
- How do I report a scammer on Facebook?
- Can you call Facebook to report a problem?

Feedback

<https://www.facebook.com/help/contact>

### Report Something on Facebook

**Report** Something on Facebook. Please select the option that best describes what you'd like to **report** and then use the link or information provided to find ...

<https://www.facebook.com/help>

filetype: pdf report - Google Search

google.com/search?q=filetype%3A+pdf+report&ei=CjOrYoHhOsmYseMP4NCqsA4&ved=0ahUKEwiBjujgLL4AhVJTgwGHwCoCuYQ4dUDCA48uact=5&oq=filetype%3A+pdf+report&gs\_lcp...

filetype: pdf report

About 26,60,00,000 results (0.44 seconds)

<https://www.appsheet.com/samples/Demo-of-templa...>

### Demo: Pdf Report - AppSheet

This app demonstrates formulas for generating a **PDF file**. It shows how to list information about the table, its children, and grandchildren.

<https://www.imi.europa.eu/call-documents/imi1/PDF>

### Final1 project report - Template

For the last **reporting** period: The following must be submitted as separate **PDF** files (originals should be sent by surface mail):

- Summary financial **report**, ...

24 pages

<http://www.africau.edu/images/default/sample/PDF>

### A Simple PDF File

A Simple **PDF File**. This is a small demonstration .pdf file - just for use in the Virtual Mechanics tutorials. More text. And more text. And more text.

2 pages

<https://www.sampletemplates.com/sample-report-in-pdf>

### FREE 40+ Sample Reports in PDF

218+ FREE **REPORT** Templates - Download Now Adobe **PDF**, Microsoft Word (DOC), Google Docs, Apple (MAC) Pages, Adobe Illustrator (AI) ...

intitle: certificate report - Google

google.com/search?q=intitle%3A+certificate+report&ei=STOrYuTYG9-aseMPk4OWwAo&ved=0ahUKEwikoc76jLL4AhVfTWwGHZOBbagQ4dUDCA4&uact=5&oq=intitle%3A+certificate+repo...

intitle: certificate report

About 10,40,000 results (0.54 seconds)

<https://www.india.gov.in/esic-form-certificate-entitlement...>

**ESIC form for certificate of entitlement - National Portal of India**

17-Sept-2020 — The Form-20 to Claim for Maternity Benefit after the death of an Insured Women leaving behind the child is available. The form is provided ...

**People also ask**

- How can I download ESIC certificate?
- How do I download entitlement certificate?
- How can I get ESIC form 37?
- What is ESIC certificate?

Feedback

<http://mi.nic.in>

**RNI**

Amendment of the format of Self-Declaration **Certificate** to be submitted by registered publications to RNI for authentication for import of Newsprint – reg.

[https://www.commoncriteriaportal.org/c0612\\_erpt](https://www.commoncriteriaportal.org/c0612_erpt) PDF

inurl: certificate report - Google

google.com/search?q=inurl%3A+certificate+report&ei=ejOrYtmGbmMseMPxYCvsAo&ved=0ahUKEwjajPuRjbl4AhU5RmwGHUXAC6YQ4dUDCA4&uact=5&oq=inurl%3A+certificate+report...

inurl: certificate report

About 6,88,000 results (0.38 seconds)

<https://dev.digicert.com/services-api/reports>

**Reports - API documentation - DigiCert**

**Reports.** This section includes the following endpoints: Request summary · Expiring **certificates** · Order **report**. About. DigiCert is the world's leading ...

[https://www.commoncriteriaportal.org/c0612\\_erpt](https://www.commoncriteriaportal.org/c0612_erpt) PDF

**Certification Report - Common Criteria**

by PP PP · 2018 — This **Certification Report** is to **report** the sponsor, Japan ID Connect with Secure. Authentication Promotional association as the developer of ...  
19 pages

**People also ask**

- How do I check a certificate?
- How do I check my SSL certificate?
- What is certificate in report?
- How do I view certificates in Linux?

Feedback

About 64,600 results (0.37 seconds)

https://hack.technoherder.com › google-hacking-aka-d...  
**Google Hacking aka Dorking - Techno Herder**  
inanchor:Certificate report to search for any pages whose anchor text includes the text "Certification" and have the text "report" anywhere on the page.

https://www.eccouncil.org  
**EC-Council: Certified Ethical Hacker | InfoSec Cyber Security ...**  
EC-Council is a global leader in InfoSec Cyber Security certification programs like Certified Ethical Hacker and Computer Hacking Forensic Investigator.

https://citationlabs.com › guides › link-prospector › adv...  
**Link Prospector Tool Guide - Advanced Searches - Citation Labs**  
In the second report, I searched for "freelance writing courses" and for "freelance writing certification." You can see just from the results that the ...

https://hackr.io › blog › google-dorks-cheat-sheet  
**Google Dorks Cheat Sheet 2022 [Free PDF] - Hackr.io**  
7 days ago — This Google Dorks cheat sheet covers everything you need to know about how to use the Google hacking technique to reach hidden search ...

https://moz.com › SEO Learning Center  
**Google Search Operators - Moz**

## Task 4: shodan and ipinfo

Go to <https://www.shodan.io/> and search for some website. See what all information you are getting from there. Select one IP from the result and search it on <https://ipinfo.io/> website.

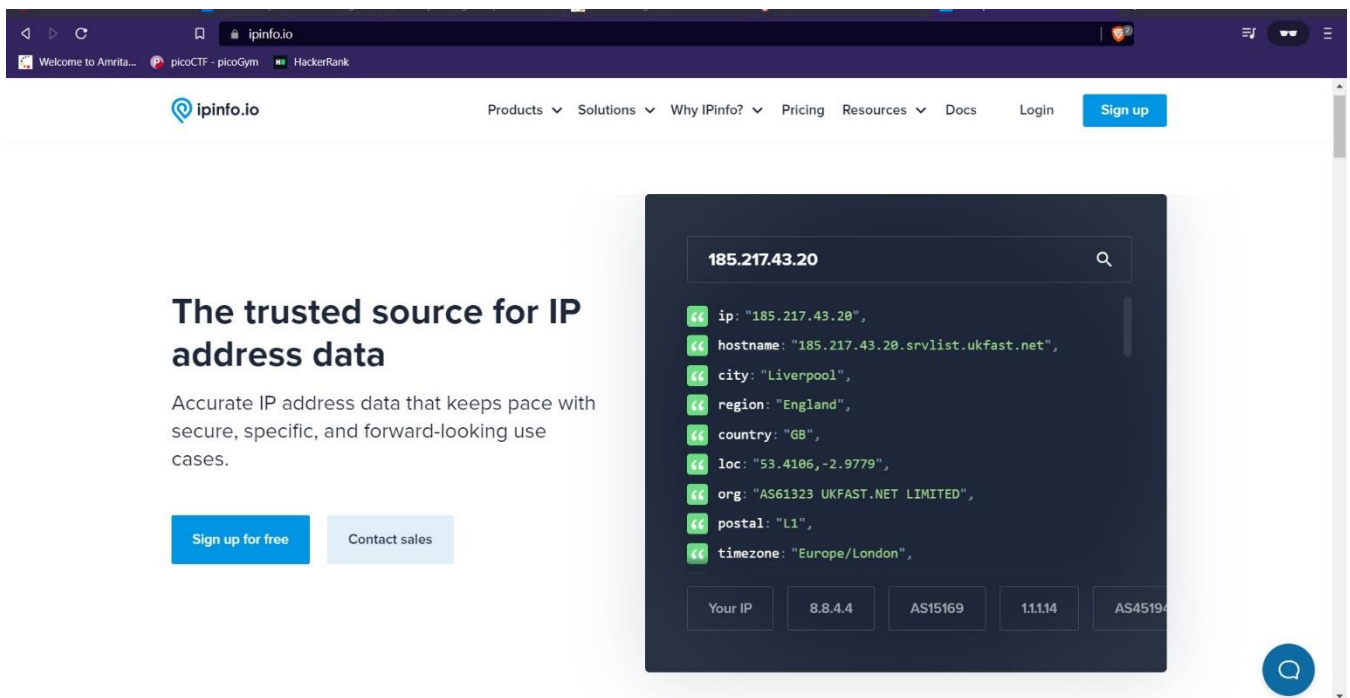
Shodan is a search engine that lets users search for various types of servers (webcams, routers, servers, etc.) connected to the internet using a variety of filters. Some have also described it as a search engine of service banners, which are metadata that the server sends back to the client.

The screenshot shows the Shodan search engine interface. The search query is 'facebook.com'. The results are displayed in a grid format. On the left, there are summary statistics: 'TOTAL RESULTS: 21,887', 'TOP COUNTRIES' (United States: 9,135, Germany: 3,230, United Kingdom: 1,087, Ireland: 1,039, Singapore: 797), and 'TOP PORTS' (443: 15,112, 80: 5,998, 8080: 236). The main results area shows three items:

- Document Moved**: A link to a document moved, with a timestamp of 2022-06-16T13:15:55.859751. It includes a list of domains: euromerics.be, www.nizoral.be, www.sereyts.be, www.stopluzen.be, www.futium.be, UKFAST.NET LIMITED, United Kingdom, Liverpool.
- SSL Certificate**: A link to an SSL certificate, with a timestamp of 2022-06-16T13:15:55.859751. It includes details: Issued By: GlobalSign RSA OV SSL CA 2018, Issued To: \*.eg.be, Issued To: \*.eg.be, Supported SSL Versions: TLSv1.2.
- Home - UWC Library Services**: A link to the UWC Library Services page, with a timestamp of 2022-06-16T13:14:05.359372. It includes details: 196.21.45.88, UWC.ac.za, University of the Western Cape, South Africa, Cape Town.

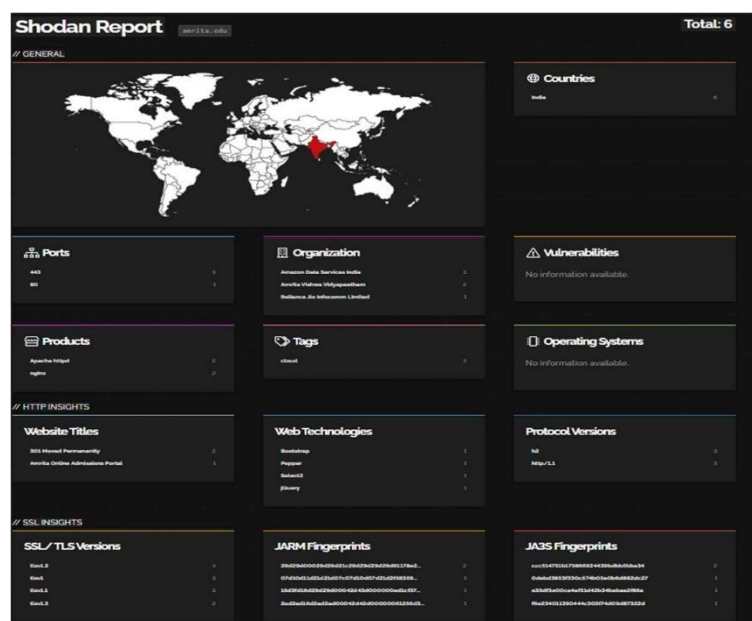
IPinfo is an industry-leading IP data provider specializing in IP to geolocation, ASN, IP to company, VPN detection, IP to carrier, IP ranges, and hosted domain data.





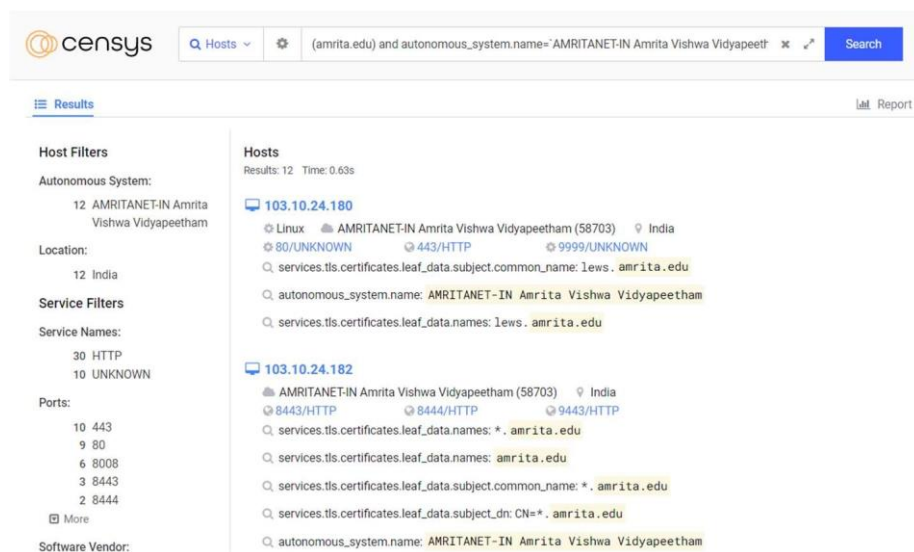
Task 5: Go through below website, search for any URL and document your finding.

Shodan is a search engine that allows users to search for different types of servers connected to the Internet using a variety of filters. Some have also described it as a service banner search engine, which is metadata that the server sends to the client.





Censys.io ([www.censys.io](http://www.censys.io)) is a web-based search platform for evaluating the attack surface for internet-connected devices. The tool can be used not only to identify Internet-connected and Internet of Things/Industrial Internet of Things (IoT/IIoT) assets, but also Internet-connected industrial control systems and platforms.

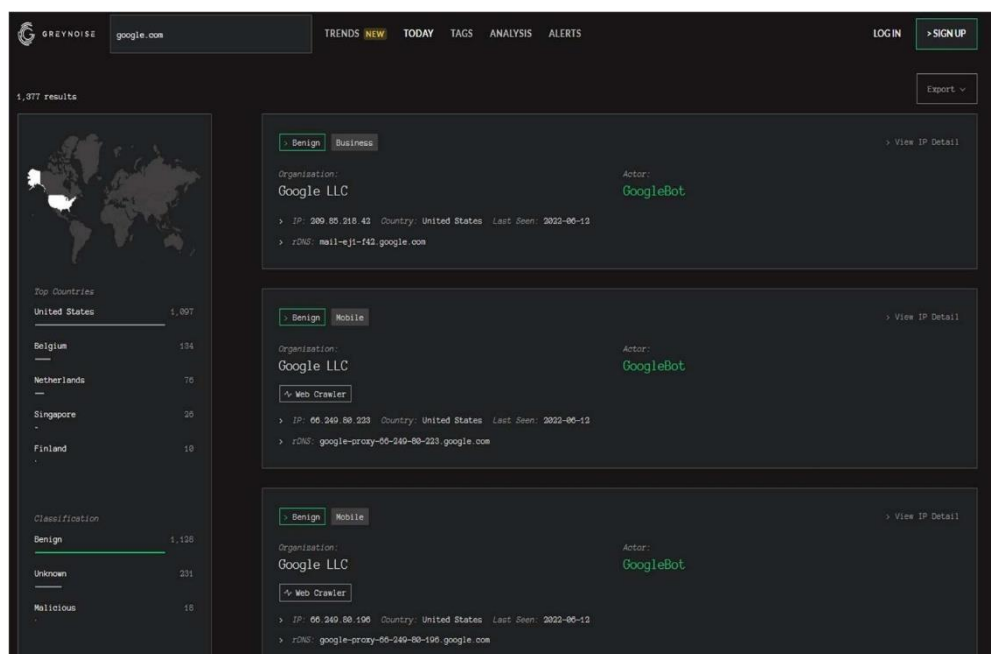


Hunter.io, aka Email Hunter, is an email hunter tool that helps marketers find the contact information associated with any domain. This is ideal for companies that use cold emailing as a way to fill their pipeline.

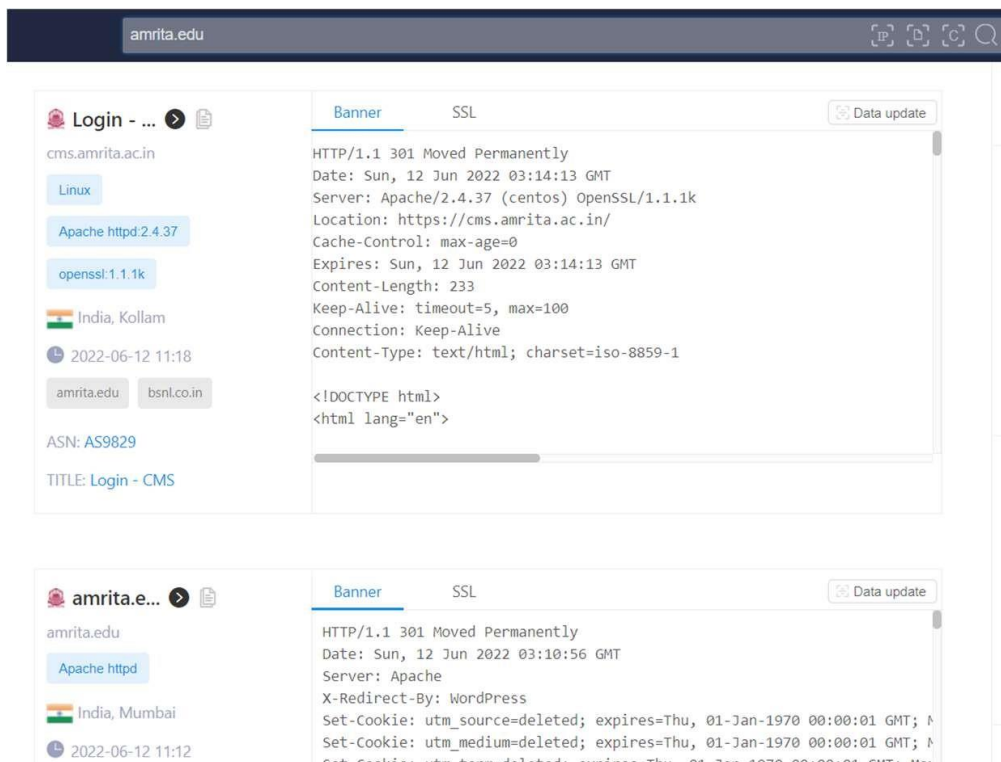
Most common pattern: {first}@amrita.edu	110 results
r hu@amrita.edu ✓	2 sources ▾
p ma@amrita.edu ●	9 sources ▾
k shna@amrita.edu ●	16 sources ▾
k en@amrita.edu ✓	5 sources ▾
v kat@amrita.edu ●	12 sources ▾

105 more results for amrita.edu. [Sign up](#) or [log in](#) to access the full results.

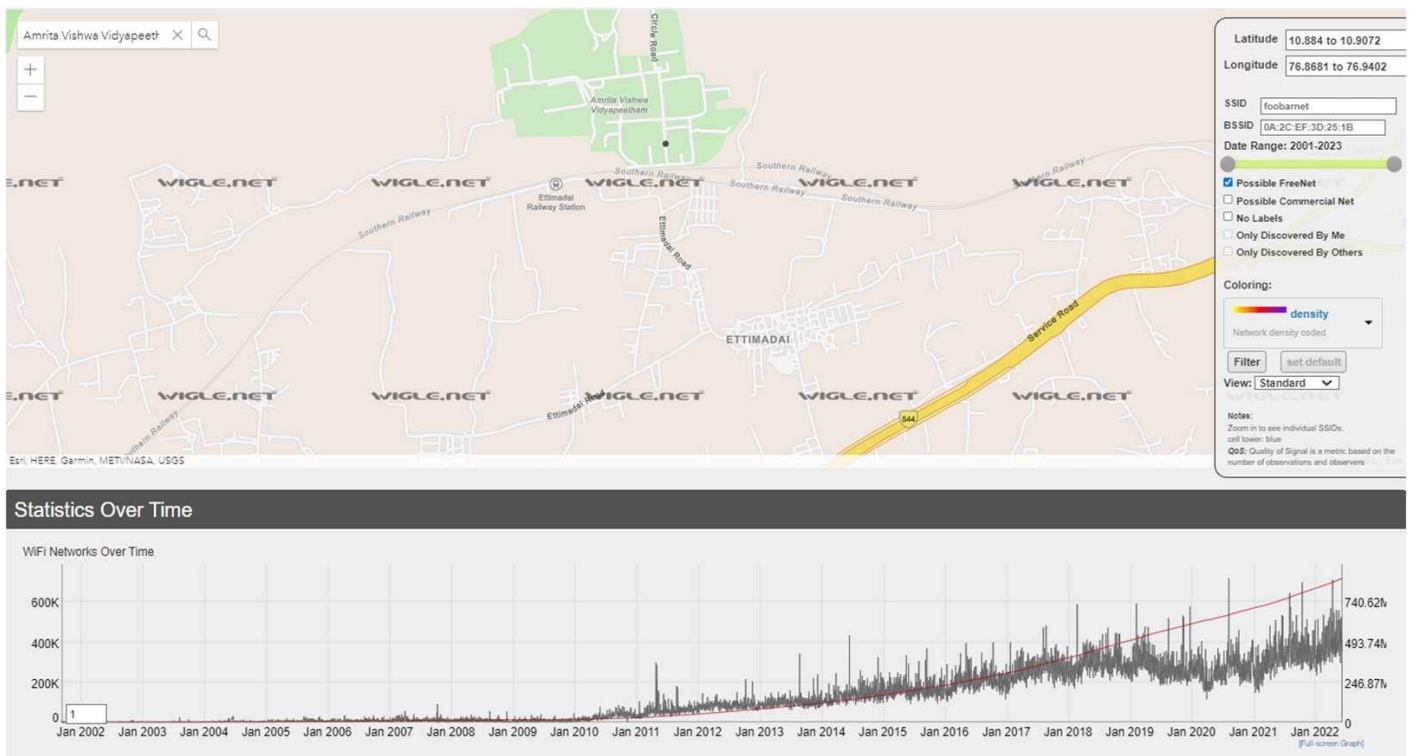
GreyNoise helps analysts spot events that aren't worth their attention. GreyNoise indicators are likely associated with opportunistic scanning of the web or broader enterprise services, not targeted threats.



ZoomEye is the world's leading provider of cyberspace mapping, China's first and world-famous cyberspace search engine powered by 404 Laboratory of Knownsec, and also a world-famous cyberspace search engine.



WiGLE is a website for collecting information about the different wireless hotspots 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.



PublicWWW is a digital marketing and affiliate marketing research tool that finds any alphanumeric snippet, signature or keyword in webpage HTML, JS and CSS code. PublicWWW is a useful tool for affiliate marketing and digital marketing research.

PublicWWW Examples Clusters Pricing Sign Up Log In

bootstrap.min.js Search

↑ Too many results? Try a phrase search with quotes: "bootstrap.min.js". Need more results? Try internal pages search.

query syntax

12736 web pages in 1.27 s. [URLs](#) [CSV](#) [CSV+snippets](#)

Rank	Url	Snippets
12 338	<a href="https://www.pizap.com/">https://www.pizap.com/</a>	--> <!-- JQuery and Bootstrap core js files --> <nd.js/1.3.0/respond.min.js></script> <[en hiv/3.7.0/html5shiv.js"></script> <script
15 183	<a href="https://www.limundo.com/">https://www.limundo.com/</a>	--> <!-- JQuery and Bootstrap --> <script type="t .com/plugins/jquery.min.js"></script> <scri ytics.com/analytics.js','ga'); ga('create'
15 573	<a href="https://mdbootstrap.com/">https://mdbootstrap.com/</a>	users.", "title": "md bootstrap cdn", "link": "https: some/5.15.3/css/all.min.css"> <title>MDB - st" href="/manifest.json"> <!-- Font Aweso

Pulsedive is a free analyst-centric threat intelligence platform that offers comprehensive, enriched threat intelligence from user submissions and threat intelligence feeds, equating to over 5 million IOCs searchable, completely free, at [pulsedive.com](https://pulsedive.com).

The screenshot shows the Pulsedive web interface. The top navigation bar includes links for Dashboard, Explore, Submit, API, and About, along with an Account dropdown and a search bar containing 'amrita.edu'. The left sidebar lists navigation options: Overview, Attributes, Threats, Feeds, Comments, Properties (with sub-items for dns and whois), and Linked Indicators (with sub-items for DNS, Mail Servers, and Name Servers). The main content area displays the domain 'amrita.edu' with a 'Very low risk' status and three indicators: 'SPF record present' and 'Linked IPs return PTR records'. A message at the top states: 'This indicator is not in our database. A passive scan was performed to fetch basic information quickly, without reaching out to the host.' Below the domain name, there are buttons for 'Copy Summary', 'Passive Scan', 'Active Scan', 'Submit', and 'Share'. The 'Highlights' section shows '#919707 on Cisco Umbrella top million' and '@ sysadmin@amrita.edu'. The 'Integrations' section lists VirusTotal, Shodan, and AbuseIPDB, all available in the 'Pro' plan. The 'Events' section shows the domain was updated on 2021-06-11 and expires on 2024-07-31.

Intelligence X is a search engine and data archive.

[Advanced](#)

Reposify is the new way organizations manage and protect their global network perimeter.

