

Skill Development Program

Open Source Intelligence (OSINT)

Presented By:
Mohamed Feroz Khan D

Guided By:
Ramaguru Radhakrishnan



Disclaimer

- Most of the tools used here are free and open source.
- All the information that we gather and analyze are from publicly available sources.
- While OSINT is also used by hackers, OSINT in itself is generally not illegal, we are not exploiting systems or people to obtain our information.
- We (the presenters or TIFAC-CORE in Cyber Security or Amrita Vishwa Vidyapeetham) are not responsible for any misuse of the information and/or techniques demonstrated.
- Before performing searches please verify with your College, University, State, Country, Workplace Laws and Rules.



What is OSINT?

- Open source intelligence (OSINT) is data collected from publicly available sources to be used in an intelligence context. It is not related to open source software or public intelligence.
- OSINT sources can be divided into different categories of information flow:
 1. Media
 2. Internet
 3. Public government data
 4. Professional and academic publications
 5. Commercial data

What can we find with OSINT

- Email addresses
- Phone numbers
- Addresses
- Identities
- Background checks
- Social media accounts
- Criminal records
- Scams
- and More



Who uses OSINT?

- Law enforcement
- Security professionals
- Malicious hackers
- Businesses
- Investigators
- Journalists
- Common Citizens



By piecing the information together we can build a bigger picture

- We gather and analyze data on our target
- That data can lead to other users that interact with our target
- By collecting information we can ultimately build a broader picture of what we are looking for.

Example :

1. Any social media platform
2. Data breach dump
3. Users real identity & location

Employers checking on social media

Employers may use OSINT to monitor social media activity related to their company or its employees.

KFC worker fired after Facebook photos show her licking potatoes

Worker who snapped photos also fired

Published On: Feb 21 2013 07:10:19 AM EST

A A A Print Email Send Recommend 33 +1 0 Tweet 4 Pin It



Facebook

What is a Sock Puppet?

- Also can be referred to as a burner account
- This is an account that we can use that is not associated to us in any way
- Use a fake name, location , job, image etc.

Why do we need a sock puppet account ?

- Depending on who we are investigating and they may dox us with our own information.
- We may spook the targets if they know we are viewing their page or draw suspicion.

Additional consideration

- Always use your account in your OSINT VM
- If you run a VPN Facebook may flag your account
- Using TOR is a good option



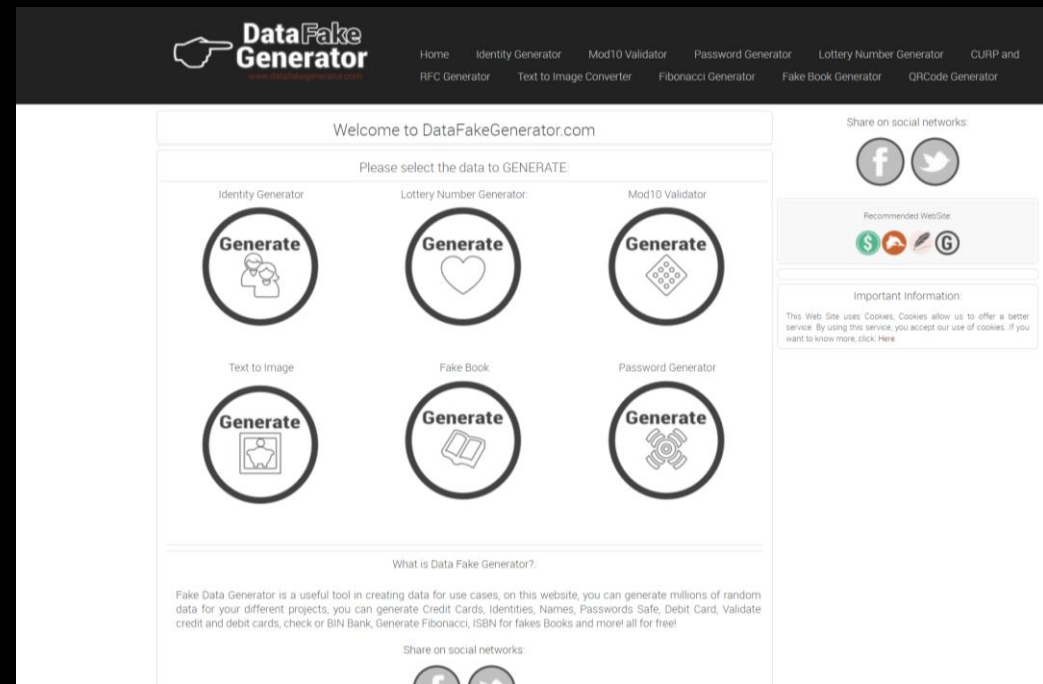
Sock Puppet

The tools need to create a sock puppet accounts are

- This person does not exist
- Fake data generator



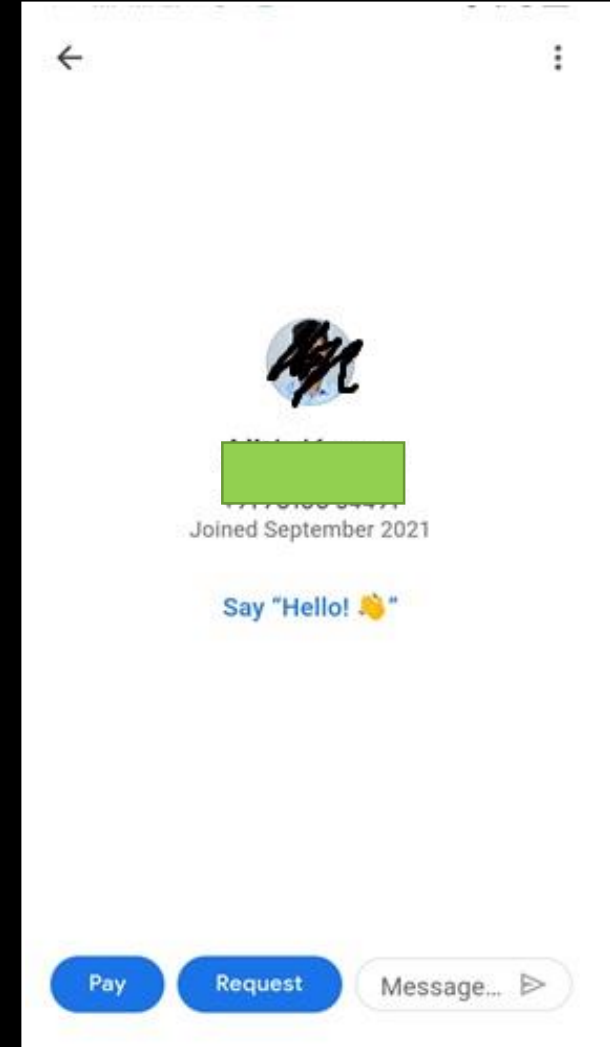
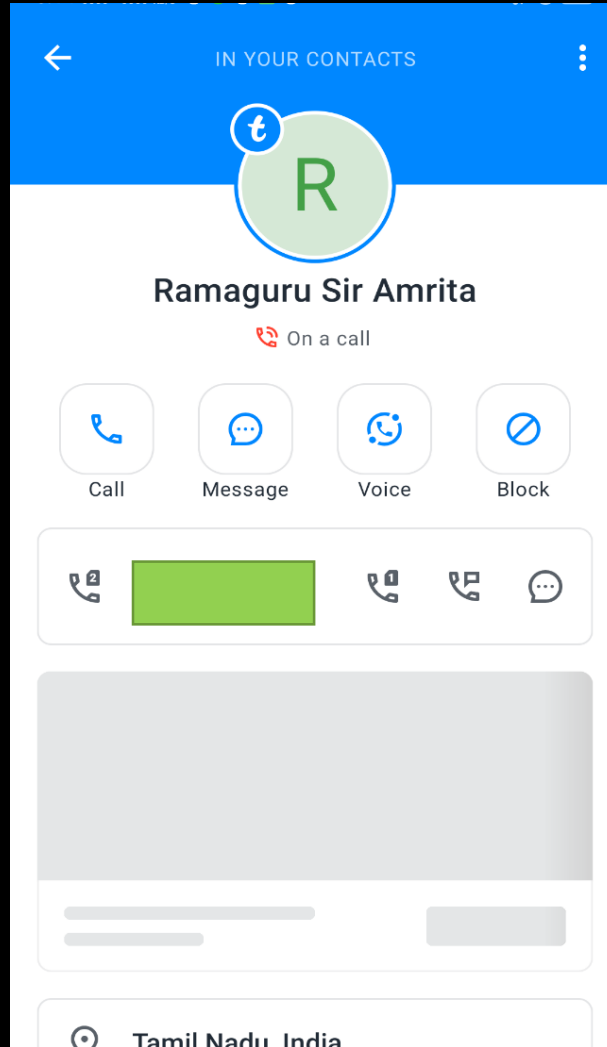
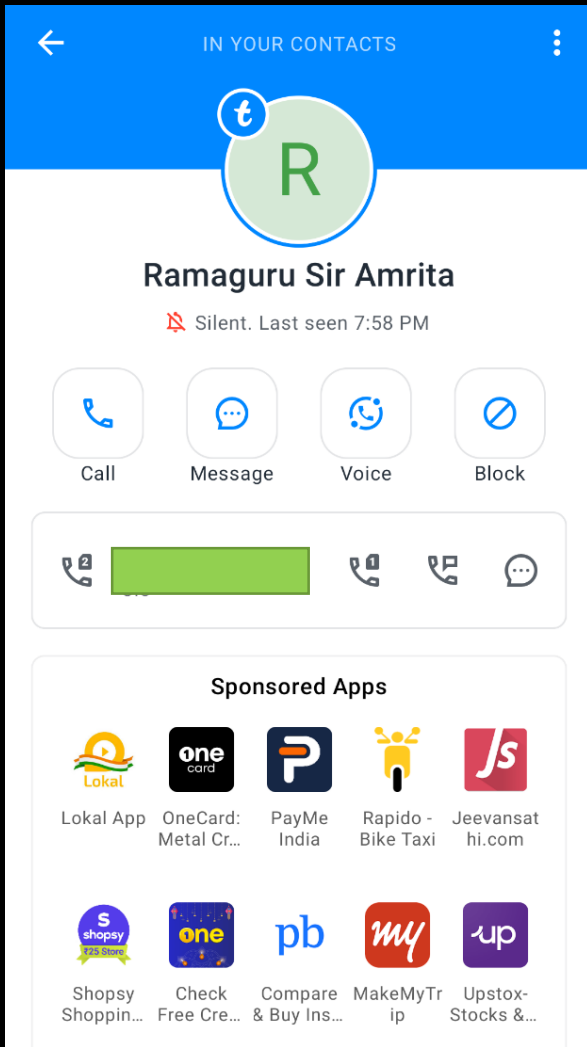
Imagined by a GAN (generative adversarial network)
StyleGAN2 (Dec 2019) - Karras et al. and Nvidia
Don't panic. Learn how it works [1] [2] [3]
Code for training your own [original] [simple] [light]
Art • Cats • Horses • Chemicals • Contact me
Another | Sponsor



Google Advanced Operators

- “ramaxxxx@gmail.com” - It will search exact keyword that we want
- cache:facebook.com/udemy - The target post was deleted its cache would be with the google
- Password filetype:xls - Used to search the passwords which are available with google
- site: www.facebook.com elon musk - In the particular site it will search
- phonebook:bill gates - Find someones phone number available in google
- Camera \$400 - Search for a price of a product
- Camera \$50..\$400 – Search within a range of amount we enter
- loc:"india" facebook - Find news from a certain location in Google News

Google Pay and Truecaller OSINT



Search Yellow Directory

[SearchYellowDirectory.com](#)

[White Pages](#)[Yellow Books](#)[Reverse Phone](#)[List of Countries](#)

Japanese Phone Numbers

Location for 81-75-xxxxxx is Kyoto. Find major cities, area codes, how to call between Japanese cities and countries abroad.

International Directories
[All Area Codes USA, Canada](#)

Japan Reverse Lookup

[Home](#) / [Reverse Phone](#) / [Japan](#) / [Kyoto Phone Number](#)

Phone number in Kyoto, Japan: +81 - 75 - 2571131

Country: Japan

Country code: 81

Area Code 75: Kyoto

Capital of Japan: Tokyo

Local Time: 11/05/2022 00:36:38 AM

Time Zone: Japan Standard Time (JST)

[Japan Yellow Pages and Email Address Lookup](#)

[Major area codes in Japan](#)

Mobile codes for Japan: [70](#), [80](#), [90](#)

+81-75-2571131 Japan reverse phone lookup

81-75-2571131 phone number **Location:** Kyoto

How to call Japan from:

International Calling Codes - How to Call to and from Japan

from India landline: 00 + **81** + area code + 4-to-8-digit local number

from India mobile: +**81** + mobile code + 4-to-8-digit local

Tinfoleak

Tinfoleak is a website which gives the information about the people from twitter

TINFOLEAK

WEB INTERFACE

SEARCH FOR LEAKSABOUTPRIVACY POLICY

SEARCH FOR LEAKS

Get the report in your inbox.


Note: e-mail address is exclusively for the purpose of sending you an e-mail with the URL to the dossier requested. No spam. No third parties.
Note 2: you report may take a while to arrive to you. It requires processing and there are more requests enqueued. Be patient. Resending your request several times won't accelerate it.

@elonmusk

sayikir916@dm tubes.com

Verification expired. Check the checkbox again.


☐ I'm not a robot

hCAPTCHA
Privacy - Terms

Send

<BACK TO LIST

DeleteSource

info@tinfoleak.com

Date:
04-11-2022 21:15:18

Subject: tinfoLeak.com

Your requested Tweeter report

by tinfoLeak.com


You requested a report for elonmusk @ tinfoleak.com to be sent to: sayikir916@dm tubes.com
The IP of the requester is: 14.139.187.130


The URL to check your report is this: <https://tinfoleak.com/reports2/elonmusk.html>

@VAguileraDiaz
Tinfoleak.com

vaguilera@lsecauditors.comInternet Security Auditors

Account Created at: 06/02/2009





Elon Musk

Twitter Complaint Hotline Operator
Followers: 113,996,589 | Following: 127 |
Likes: 14990
Tweets: 20,028 (4.09 tweets/day)

Verified: True

Twitter ID: 44196397

URL:

Location: Hell

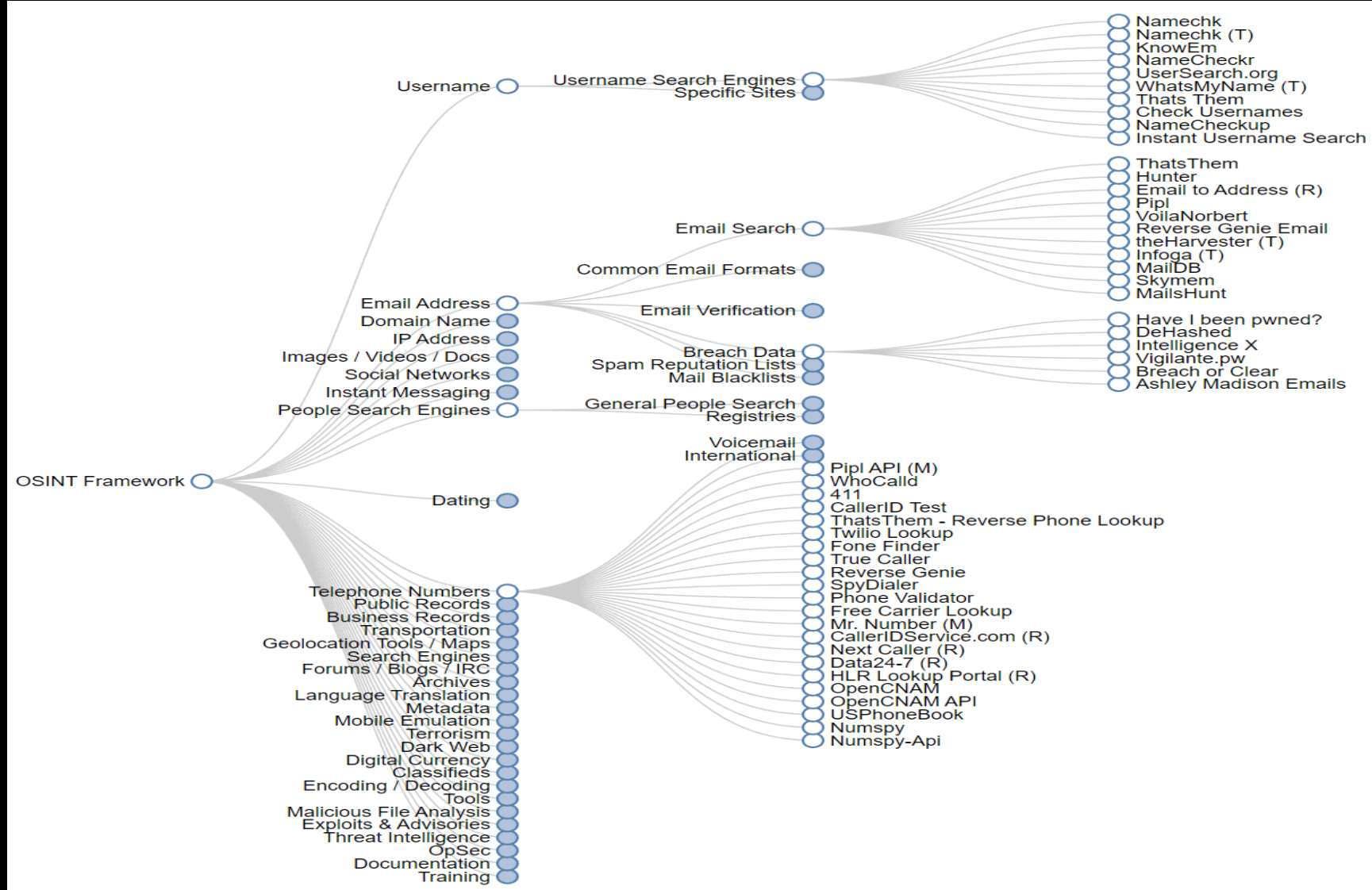
Time Zone: None

Geo enabled: False

Listed count: 100751

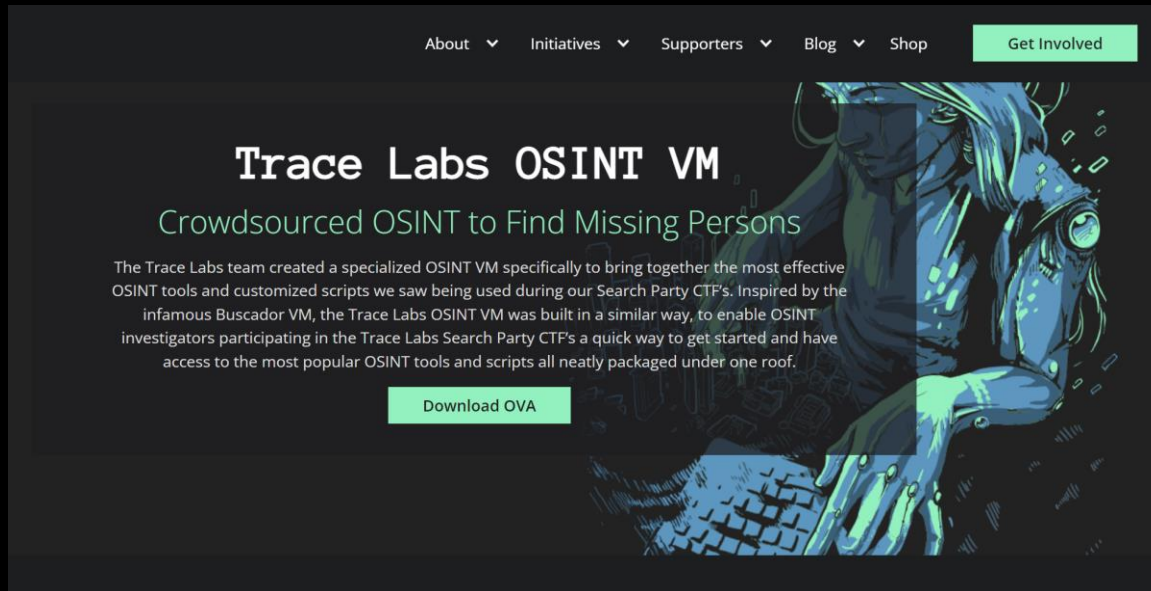
Language: None

OSINT Framework



OSINT Operating System

- Trace Labs OSINT VM
- CSI Linux



The screenshot shows the homepage of the Trace Labs OSINT VM. The navigation bar includes links for About, Initiatives, Supporters, Blog, Shop, and a prominent 'Get Involved' button. The main heading is 'Trace Labs OSINT VM' with the subtitle 'Crowdsourced OSINT to Find Missing Persons'. A paragraph describes the VM as a specialized tool for digital forensics, inspired by the Buscador VM. A 'Download OVA' button is located at the bottom of the main content area. The background features a stylized illustration of a person with a cybernetic eye and a keyboard.

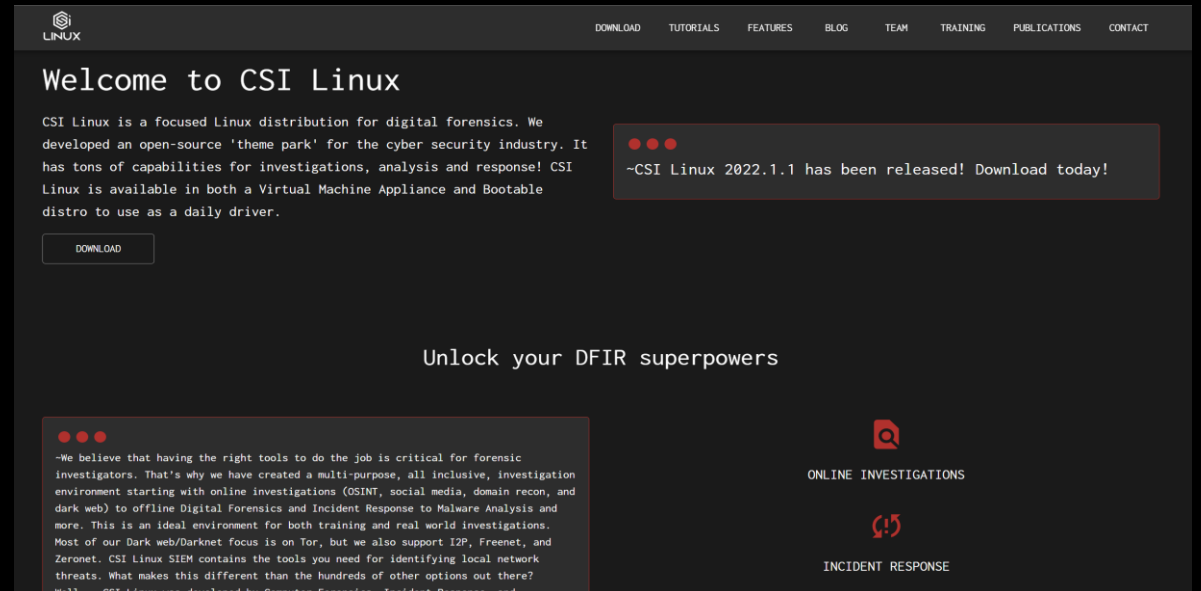
About ▾ Initiatives ▾ Supporters ▾ Blog ▾ Shop [Get Involved](#)

Trace Labs OSINT VM

Crowdsourced OSINT to Find Missing Persons

The Trace Labs team created a specialized OSINT VM specifically to bring together the most effective OSINT tools and customized scripts we saw being used during our Search Party CTF's. Inspired by the infamous Buscador VM, the Trace Labs OSINT VM was built in a similar way, to enable OSINT investigators participating in the Trace Labs Search Party CTF's a quick way to get started and have access to the most popular OSINT tools and scripts all neatly packaged under one roof.

[Download OVA](#)



The screenshot shows the homepage of the CSI Linux website. The navigation bar includes links for Download, Tutorials, Features, Blog, Team, Training, Publications, and Contact. The main heading is 'Welcome to CSI Linux'. A paragraph describes CSI Linux as a focused Linux distribution for digital forensics. A 'Download' button is located below the text. A red alert box at the top right states: '~CSI Linux 2022.1.1 has been released! Download today!'. The section 'Unlock your DFIR superpowers' features a quote about the importance of having the right tools for forensic investigations. On the right, there are two icons: a magnifying glass for 'ONLINE INVESTIGATIONS' and a speech bubble for 'INCIDENT RESPONSE'.

[Download](#) [Tutorials](#) [Features](#) [Blog](#) [Team](#) [Training](#) [Publications](#) [Contact](#)

Welcome to CSI Linux

CSI Linux is a focused Linux distribution for digital forensics. We developed an open-source 'theme park' for the cyber security industry. It has tons of capabilities for investigations, analysis and response! CSI Linux is available in both a Virtual Machine Appliance and Bootable distro to use as a daily driver.

[Download](#)

~CSI Linux 2022.1.1 has been released! Download today!

Unlock your DFIR superpowers

~We believe that having the right tools to do the job is critical for forensic investigators. That's why we have created a multi-purpose, all inclusive, investigation environment starting with online investigations (OSINT, social media, domain recon, and dark web) to offline Digital Forensics and Incident Response to Malware Analysis and more. This is an ideal environment for both training and real world investigations. Most of our Dark web/Darknet focus is on Tor, but we also support I2P, Freenet, and Zeronet. CSI Linux SIEM contains the tools you need for identifying local network threats. What makes this different than the hundreds of other options out there? Well... CSI Linux was developed by Computer Forensics, Incident Response, and...

[ONLINE INVESTIGATIONS](#)

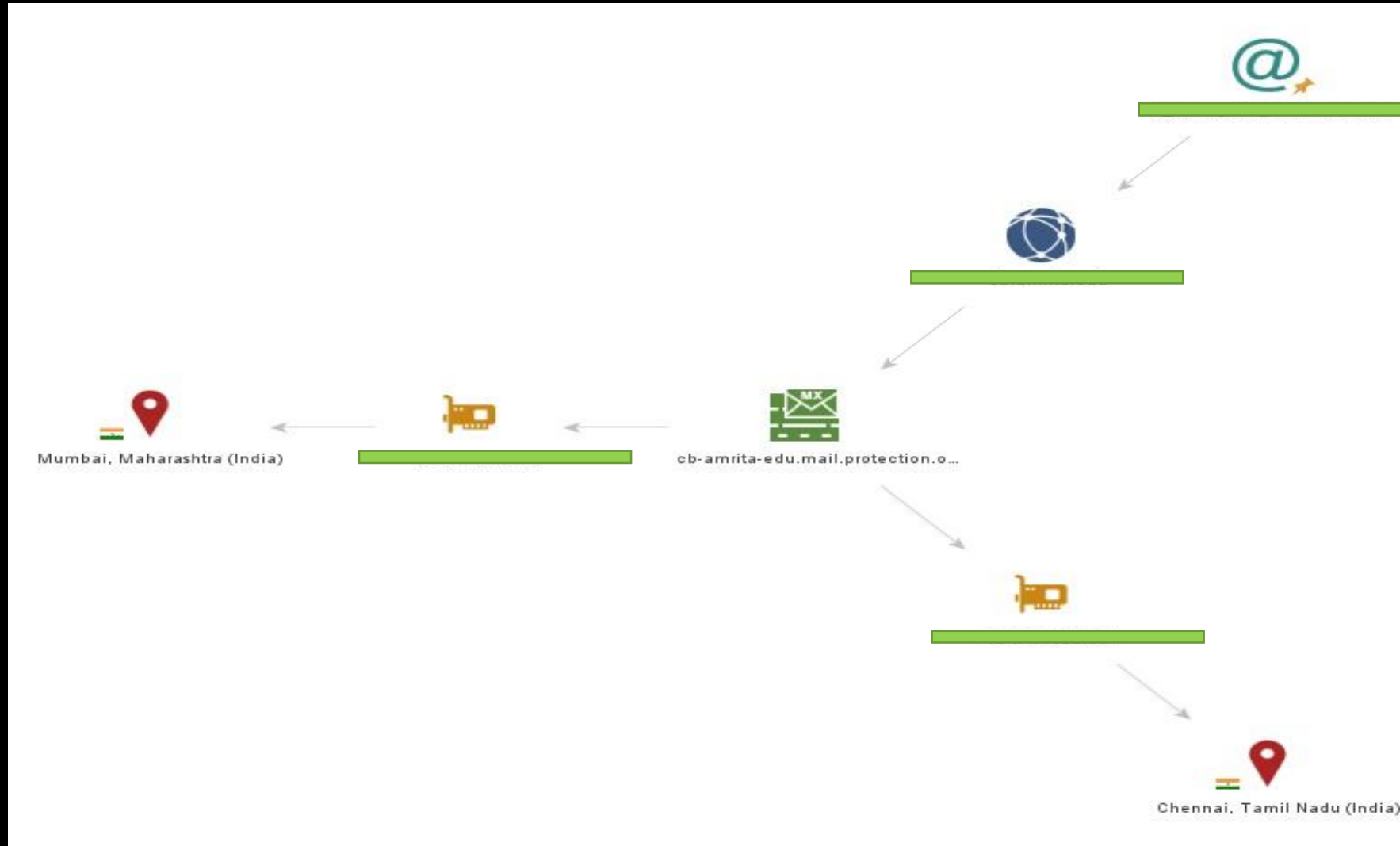
[INCIDENT RESPONSE](#)

Maltego

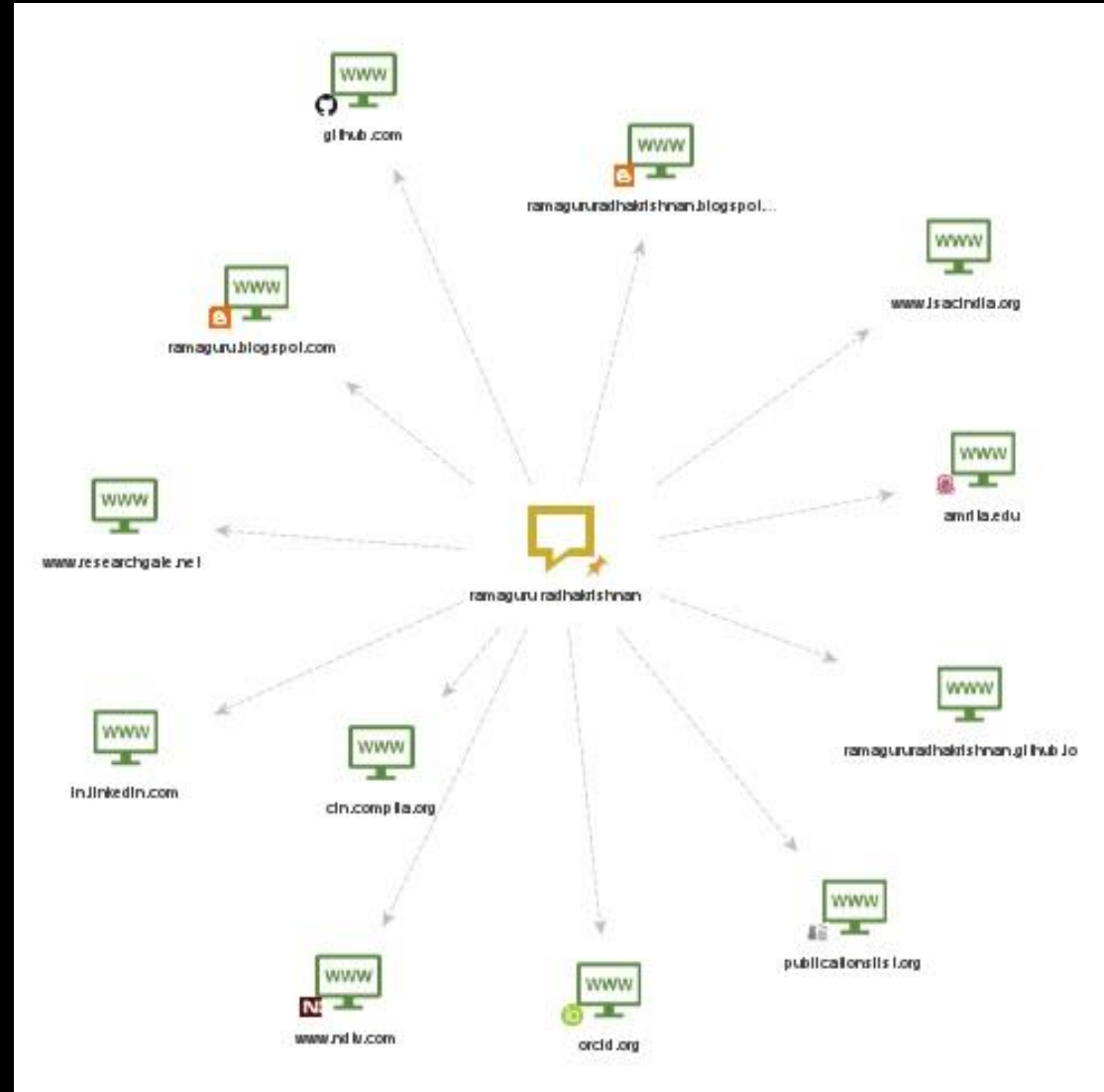
- Open-source intelligence and forensics, developed by Paterva, South Africa.
- Graphical link analysis tool for gathering and connecting information for investigative tasks.
- Java application that runs on Windows, Mac and Linux.



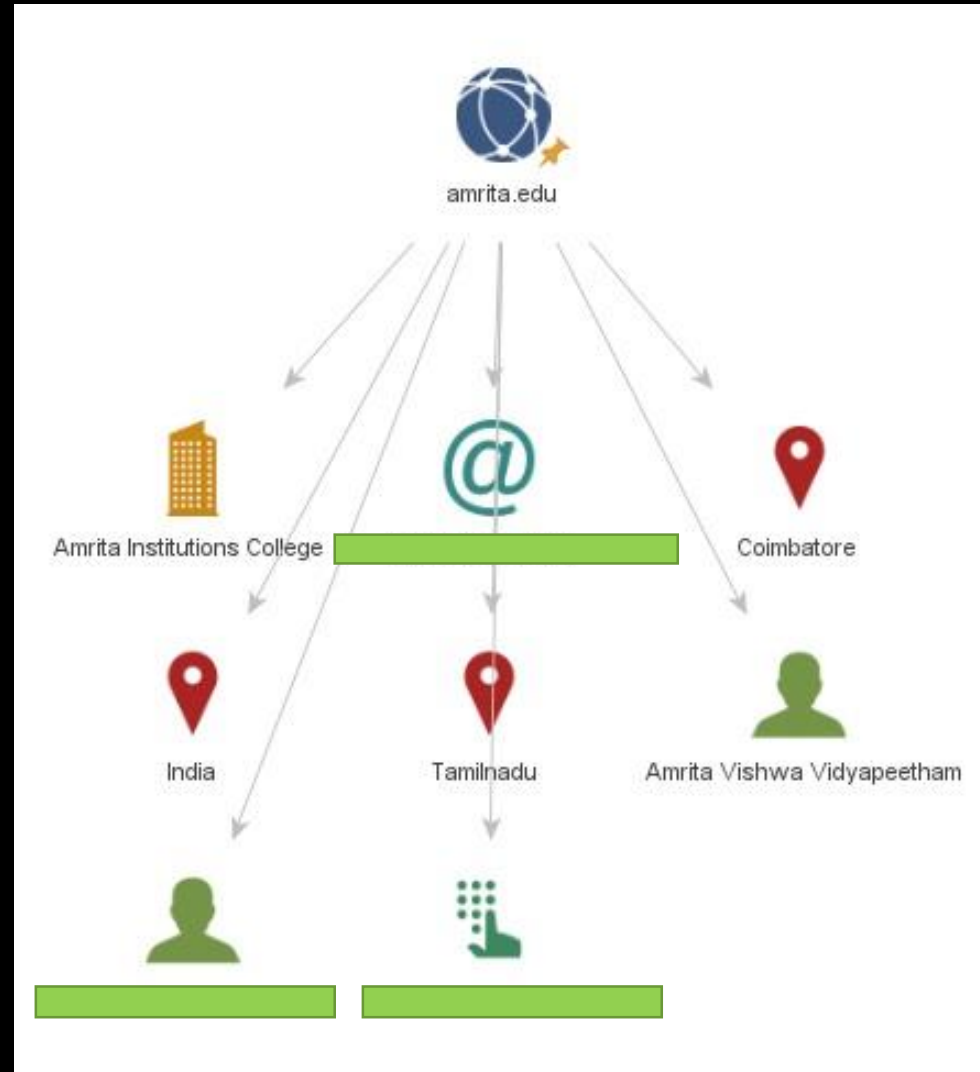
Example 1: Email based Search



Example 2: Name based Search



Example 3: Whois Record



Thank You for listening
patiently

Any Doubts?