**2CEIT78PE8 : FCL**

**Name:** Jinal Sojitra

**Enrollment No. :** 19012021081

**Subject:** FCL Practical 1 to 3

**Class:** CEIT-A

**2CEIT78PE8: FCL**

**Practical: 1**

**Aim: OSINT Framework**

**OSINT Framework:**

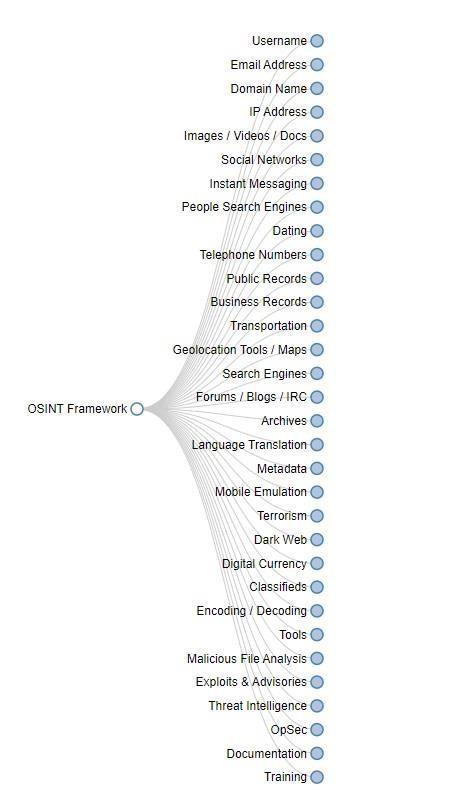
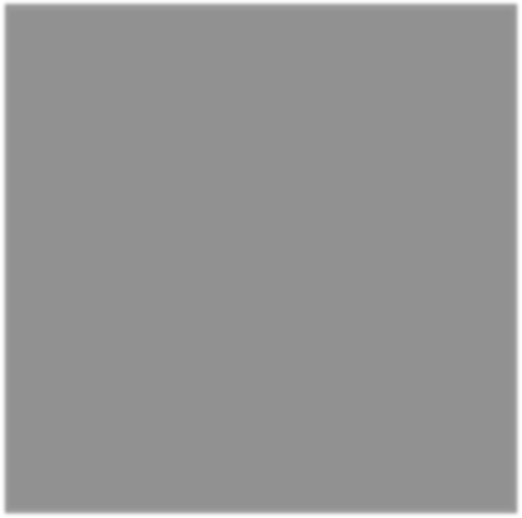
The OSINT framework is a cybersecurity structure that consists of a collection of OSINT technologies that may be used to find information about a target more quickly and easily. It is a web-based platform that allows you to browse several OSINT tools on various themes and goals based on your requirements. The OSINT framework focuses on acquiring data through open-source tools and resources. It can also be easily browsed by looking at the OSINT tree and it provides an excellent classification of all existing intel sources.**OSINT Framework Classification**

The OSINT Framework can be accessed from the website: https://osintframework.com/ On the right top corner of the screen, you can find indicators for some of the listed tools. (T) — Indicates a link to a tool that must be installed and run locally

(D) — Google Dork (or Google Hacking) (R) — Requires registration

(M) — Indicates a URL that contains the search term and the URL itself must be edited manually

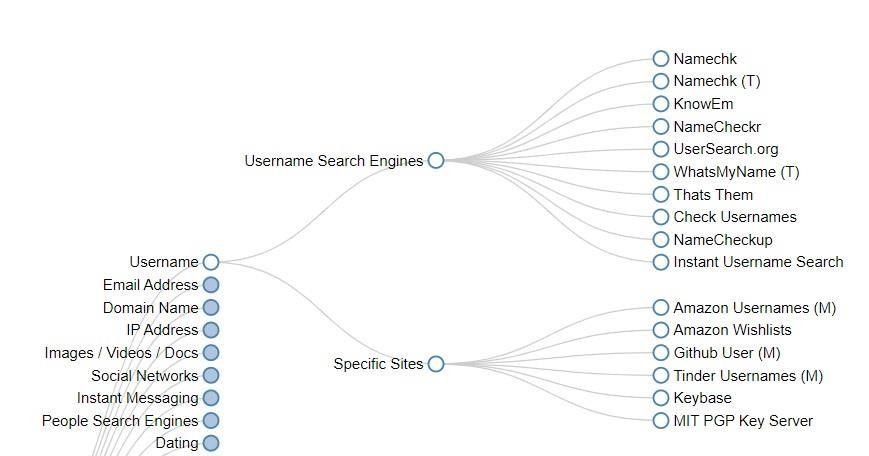
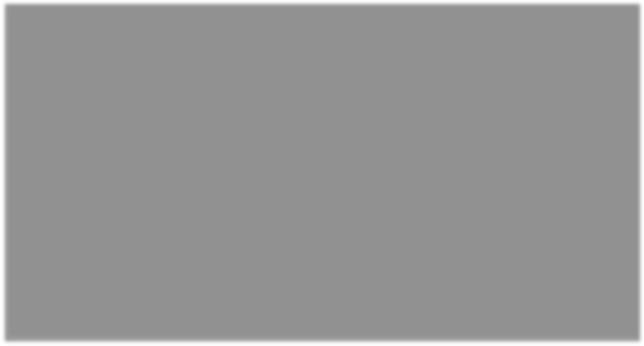
**Below you can find an OSINT tree :**



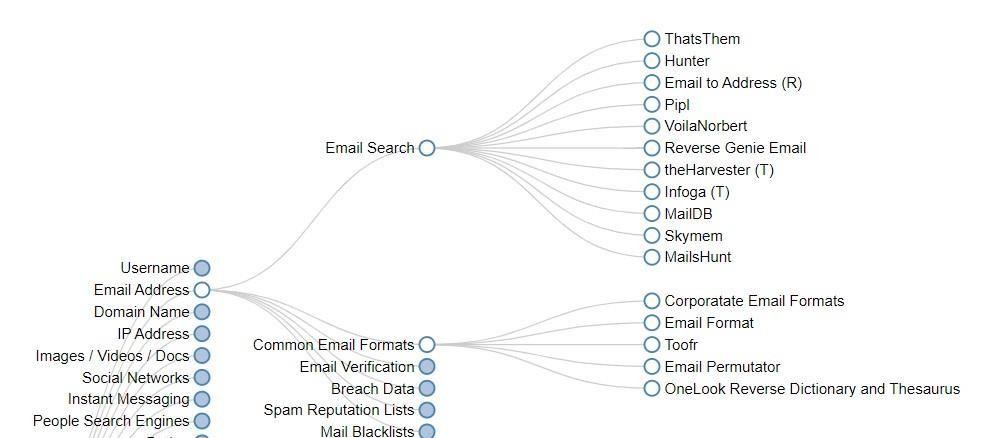
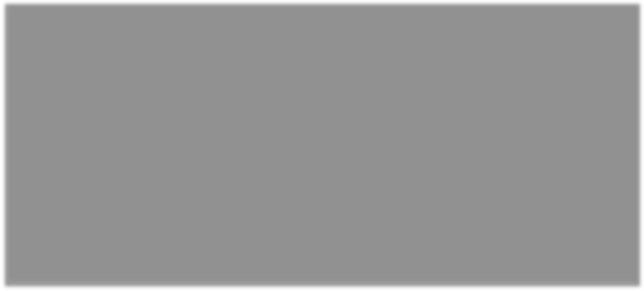
**19012021081: Jinal Sojitra**

**2CEIT78PE8:FCL**

**Username:**



**Email Address OSINT:**



**When you are searching for a breached email address, then you can find many links to useful resources such as**

Have I been pwned? Intelligence X Vigilante.pw

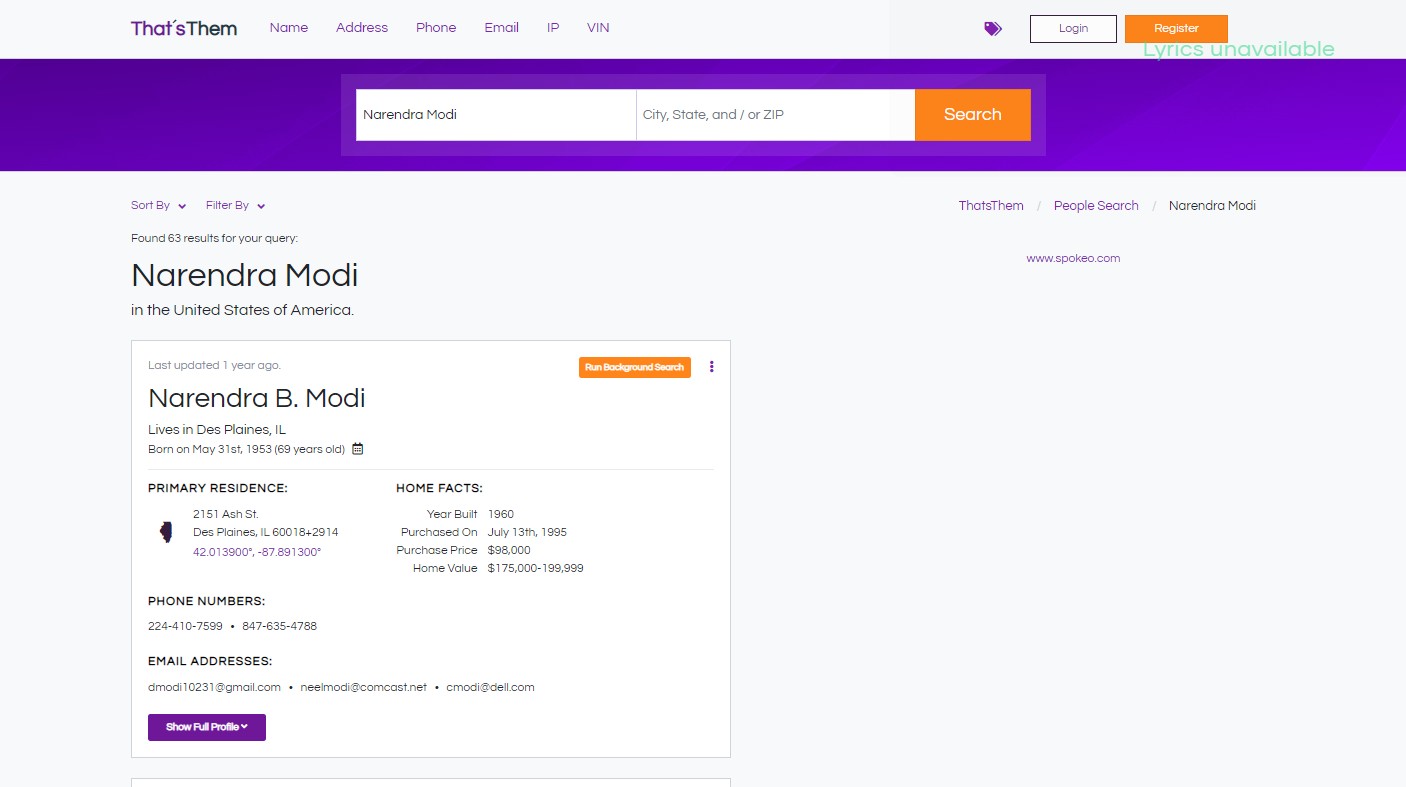
Asley Madison Email , etc.

**19012021081: Jinal Sojitra**

**2CEIT78PE8:FCL**

**Like all the functionally available OSINT frameworks.**

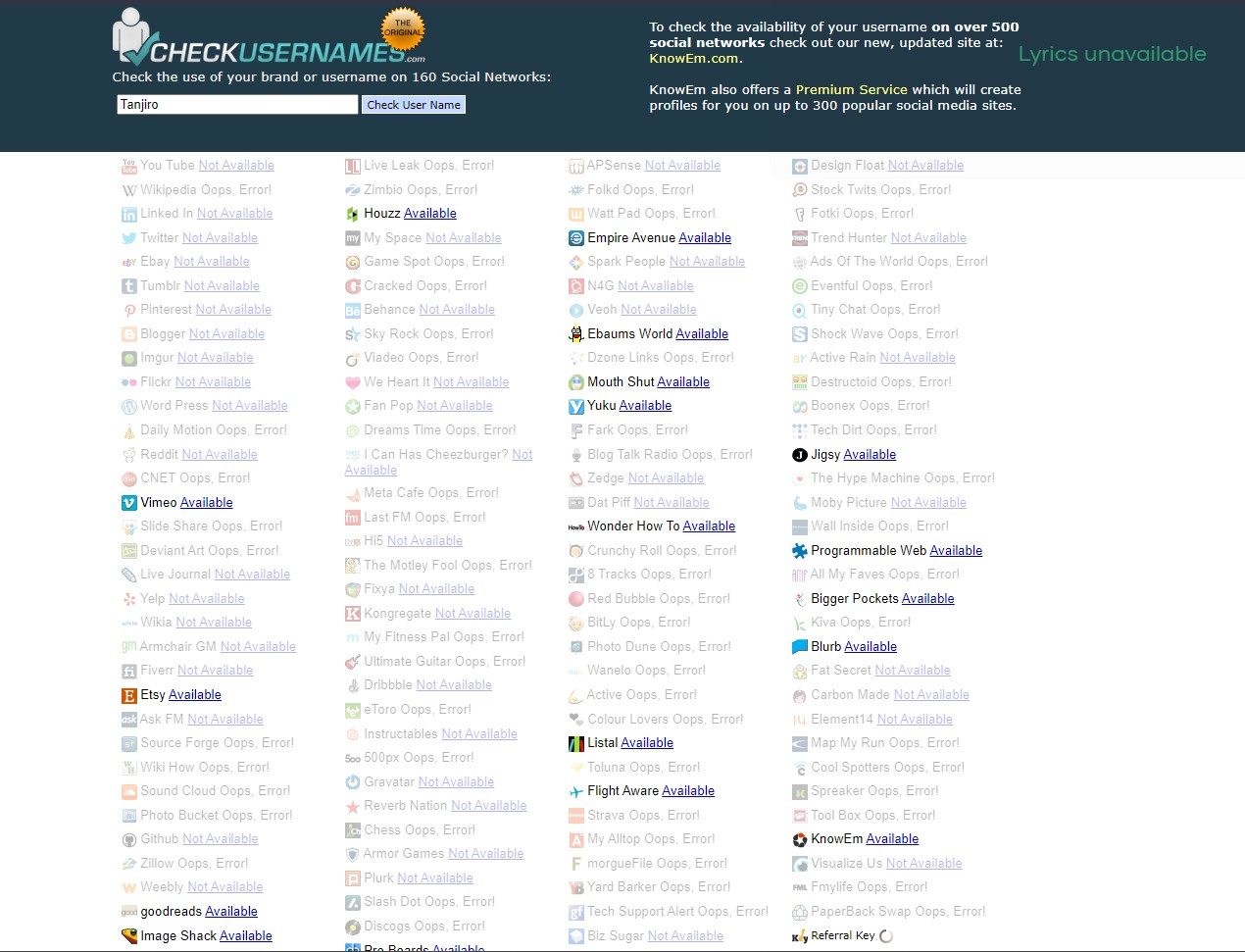
**1. Username search in OSINT with functionality thatsthem.com so the output is:**



**19012021081: Jinal Sojitra**

**2CEIT78PE8:FCL**

**2. Also in other usernames functionality use and check usernames available on social media sites** [**CheckUsernames - SocialMedia Username Search by KnowEm:**](https://checkusernames.com/)

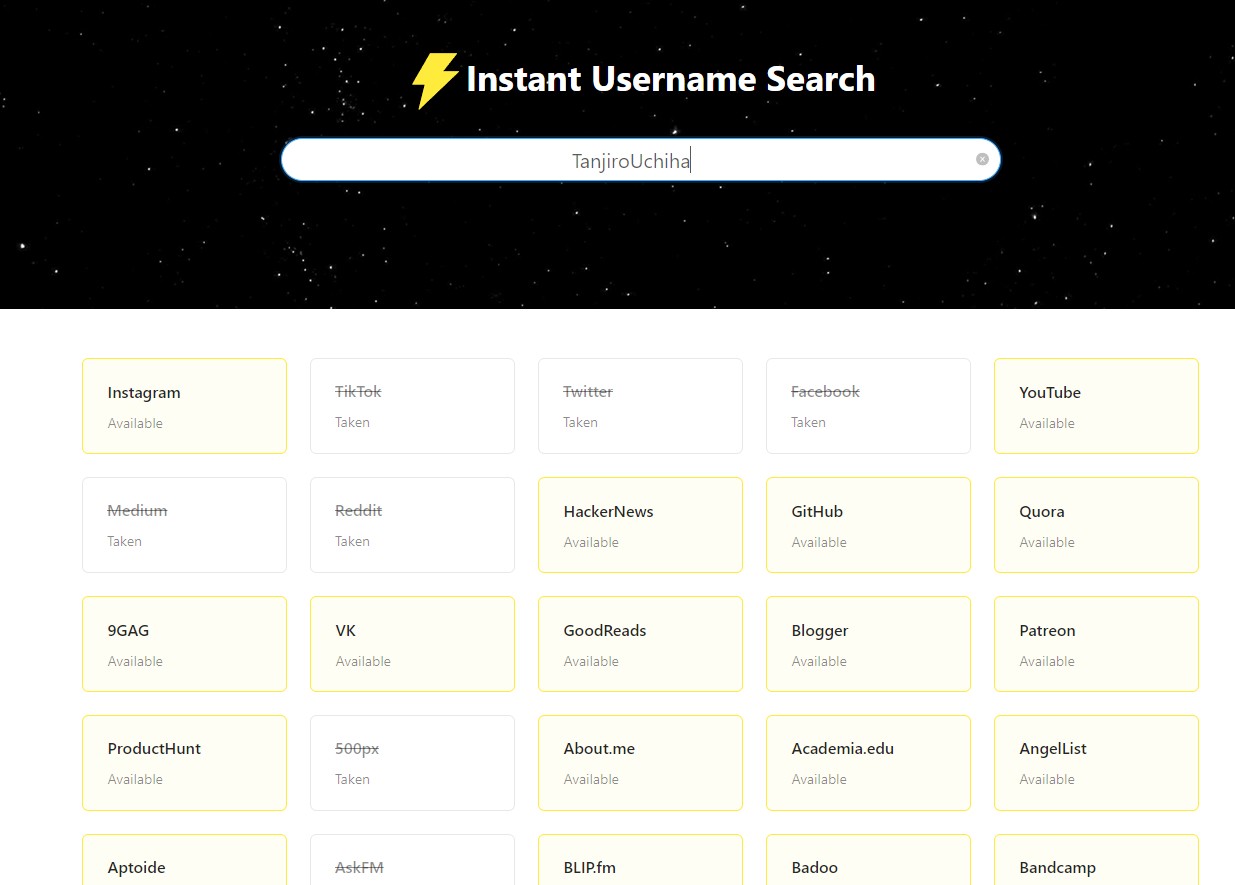


**19012021081: Jinal Sojitra**

**2CEIT78PE8:FCL**

**3. Use this site also for search usernames** [**Instant UsernameSearcht**](https://instantusername.com/%23/)**o available in**

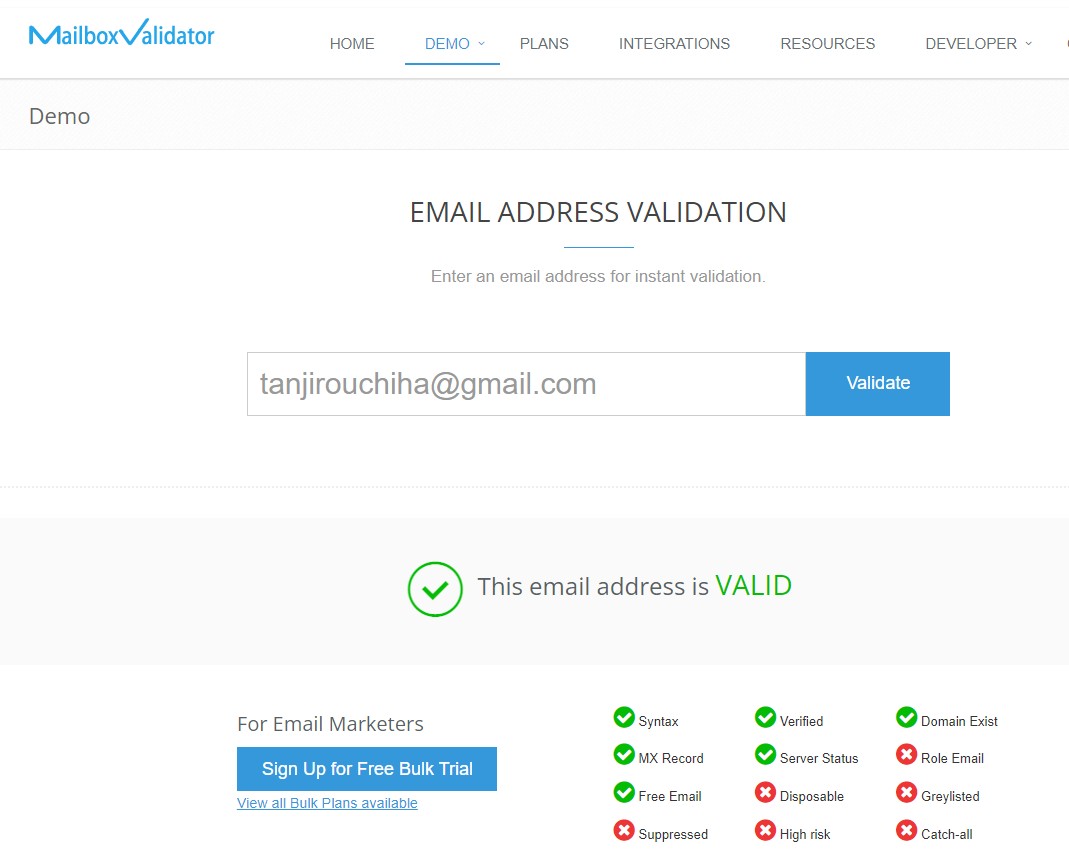
**social media**



**19012021081: Jinal Sojitra**

**2CEIT78PE8:FCL**

**4. Email Verification: this site is used to verify the correct email address or not:** [**Free Email Address Validation | MailboxValidator**](https://www.mailboxvalidator.com/demo)

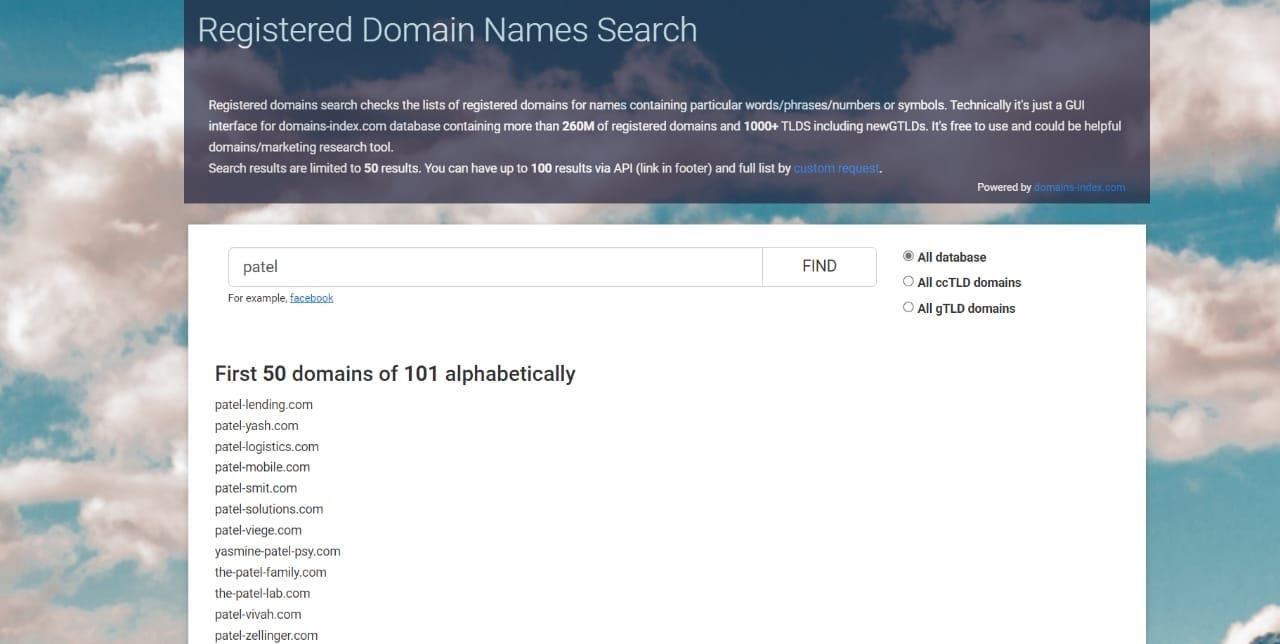
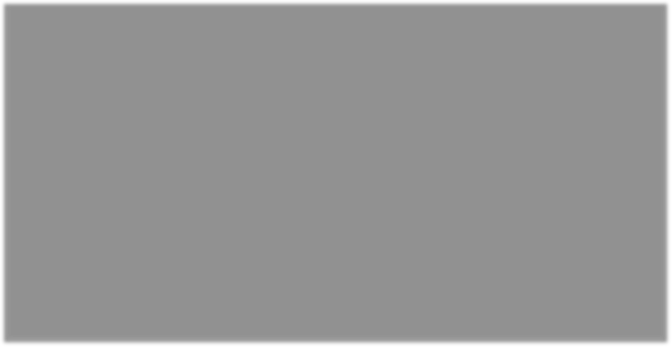


**19012021081: Jinal Sojitra**

**2CEIT78PE8:FCL**

**5. Registered Domain Names Search:**

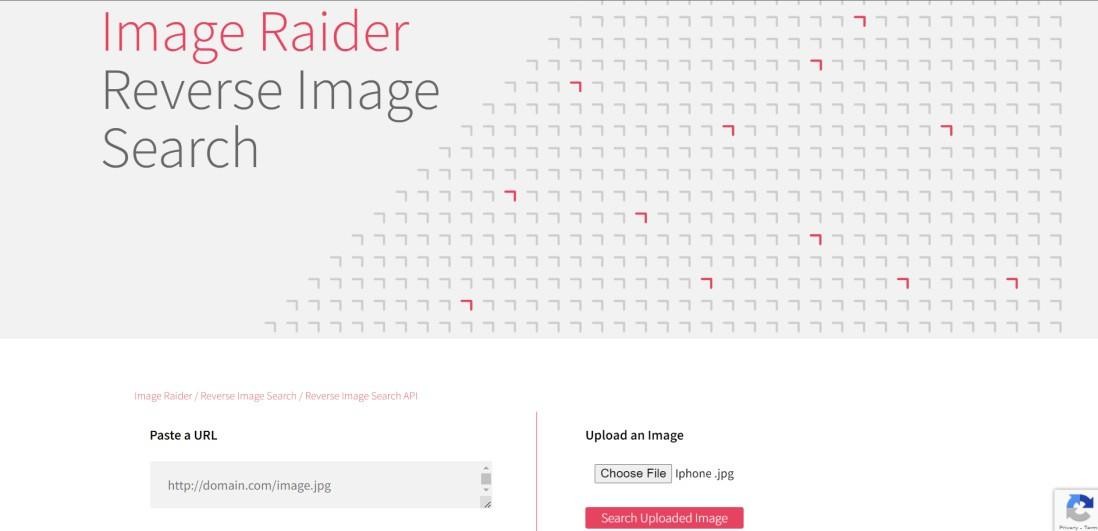
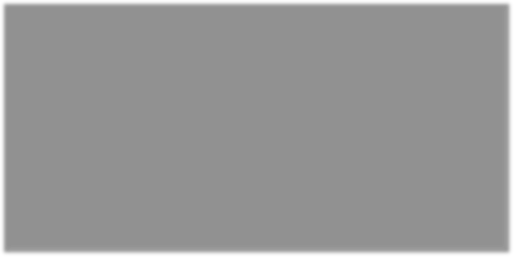
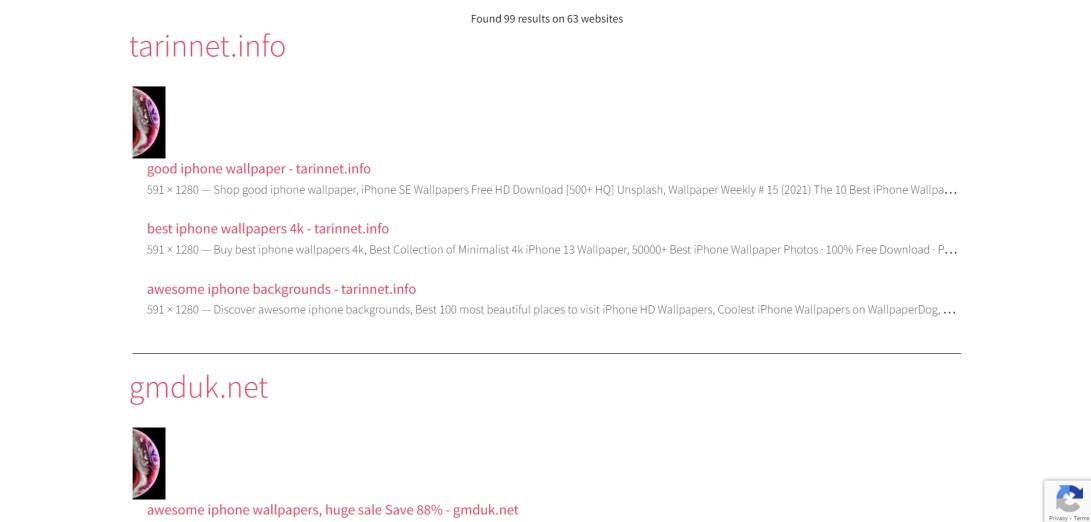
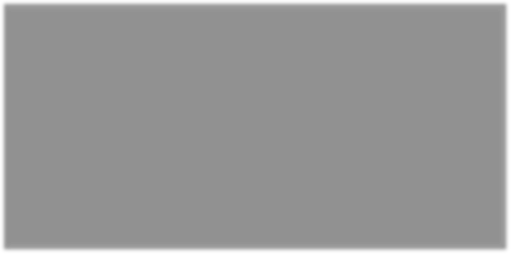
Registered domains search checks the lists of registered domains for names containing particular words/phrases/numbers or symbols. Technically it's just a GUI interface for the domains-index.com database containing more than 260M of registered domains and 1000+ TLDs including new TLDs. It's free to use and could be a helpful domains/marketing research tool.



**19012021081: Jinal Sojitra**

**2CEIT78PE8:FCL**

**6. Search images using Image Raider functionality:**



**7. Archive.is**

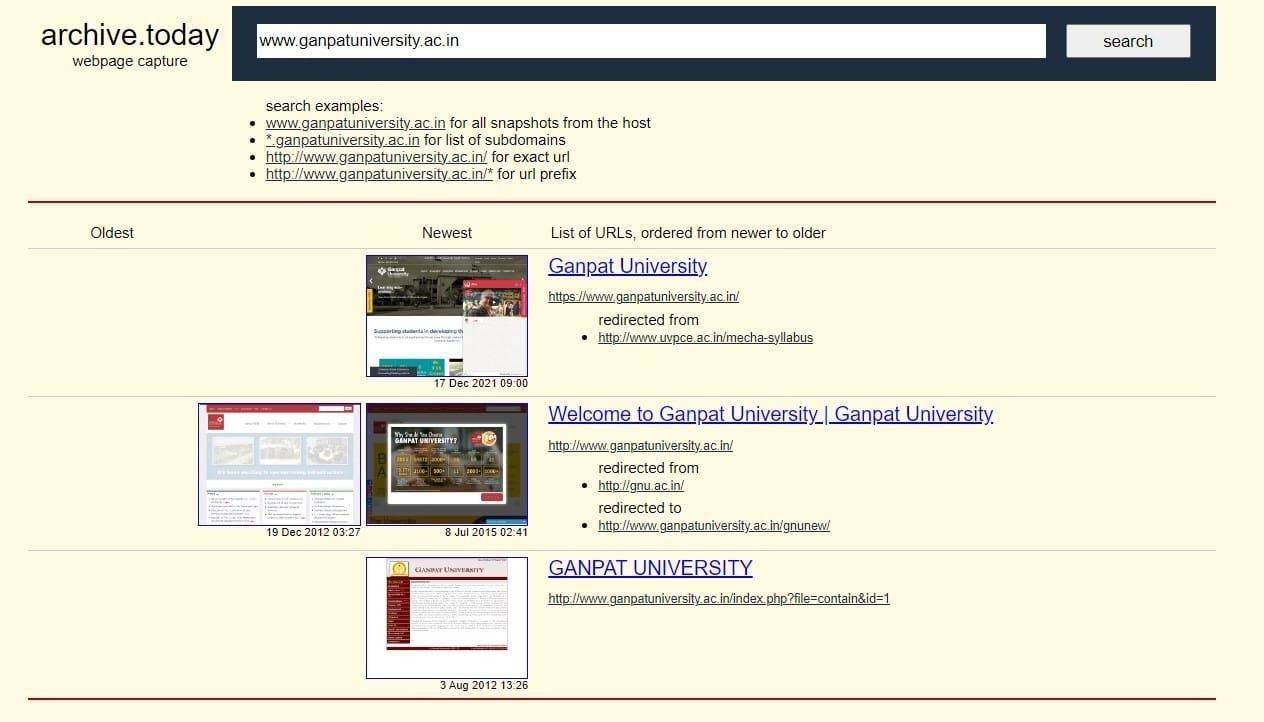
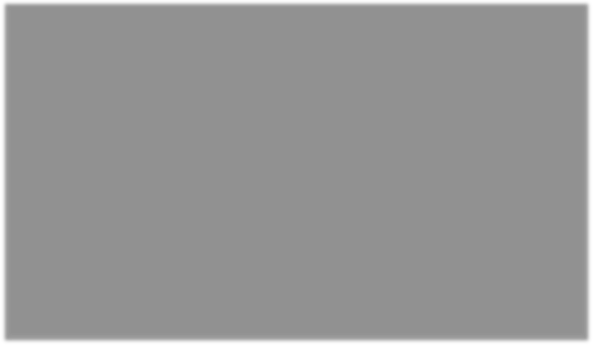
Archive.is today a time capsule for web pages

It takes a 'snapshot' of a webpage that will always be online even if the original page disappears? It saves text and a graphical copy of the page for better accuracy and provides a short and reliable link

to an unalterable record of any web page.

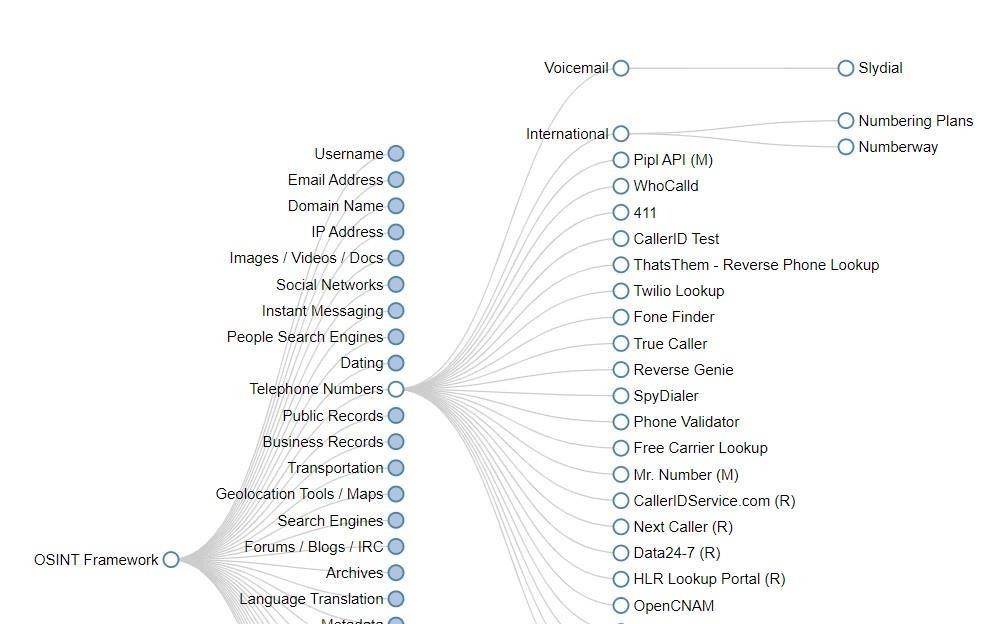
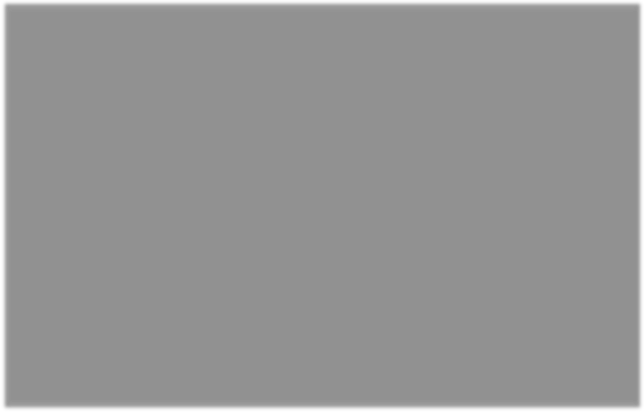
**19012021081: Jinal Sojitra**

**2CEIT78PE8:FCL**



**8. Phone Numbers OSINT**

Do you want to identify phone numbers? Don’t worry, the OSINT framework contains a whole bunch of tracking tools that allow you to identify an incoming call. These tools are shown in the below picture.



**19012021081: Jinal Sojitra**

**2CEIT78PE8:FCL**

**Practical: 2**

**Aim: Deep Web Monitoring**

Dark web monitoring services are growing in popularity. Password managers offer these services, among many other features that make them a must-have for any privacy-conscious individual. Heck, dark web monitoring is so crucial that even credit monitoring firms and identity theft protection and monitoring companies are now offering it to sweeten their packages.

But what is dark web monitoring? How does dark web monitoring work? And why is it important?

**What Is the Dark Web?**

Before we delve into what dark web monitoring actually is, it makes sense to lay some foundations about the critical term in play–the dark web. What exactly is the dark web?

To understand the dark web, we have to zoom out to the more extensive internet. The internet is defined as a

global network of interconnected devices. It can be categorized into three broad categories: the surface web, the deep web, and the dark web.

The surface web is the part of the internet that most people use daily; its content is indexed by search engines like Google Search, Bing, and DuckDuckGo. The deep web contains sensitive information about people and organizations like email addresses, phone numbers, etc. This information is not indexed and is hence inaccessible via search engines.

On the other hand, the dark web is a network of anonymous websites and forums hidden in the deep web. To access the dark web, you need specialized software.

Dark web monitoring is the process of scouring these hard-to-find anonymized websites on the deep web searching for leaked personal or business credentials, like email addresses, bank account details, credit card numbers, etc. The whole process is often automated.

When your email address, phone number, or other Personally Identifiable Information (PII) is found on the dark web, you’re alerted to partake in preventive measures to protect yourself. These measures could include changing your passwords if they've been leaked, replacing your credit or debit card, etc.

Typically, dark web monitoring tools scan for individual information like email addresses, phone number,

social security numbers, credit card numbers, bank account numbers, and passport numbers on the dark web.

Stolen or leaked information is usually traded on dark web websites and forums, sometimes given away for free. All of this leaked information is hidden from everyday internet users on the dark web; it's hard to tell if any of your personal information has been leaked or breached.

Of course, that's unless one of the companies that hold your data tells you about it. The truth of the matter is, most companies stay silent if they’ve been affected by a data breach or leak to protect their reputation and revenue, despite data breach reports being commonplace on security websites these days.

But you don't have to worry about the dark web so much, as dark web monitoring tools and services will help

do the heavy lifting for you.

Picture this: you get an email from your dark web monitoring tool telling you that it found one of your credentials on the dark web. It's logical to ask yourself how your credentials ended up on the darknet in the first place.

**19012021081: Jinal Sojitra**

**2CEIT78PE8:FCL**

If your information is found on the dark web, it’s evident that someone must have accessed it without permission. Commonly, criminals steal information by accessing companies’ database systems and then leak contents or sell it online.

This is referred to as a data breach or data leak, depending on how it happened.

But data breaches and leaks are just two examples of how hackers can steal your information. There are other ways hackers can get hold of your data, like through malware, phishing, and ATM/gas skimmers.

**How Do Dark Web Monitoring Tools Work?**

Dark web monitoring tools, which include scrapers, crawlers, and scanners, scour hundreds, if not thousands, of dark web websites per day looking for your personal information. They often scour dark websites that are dedicated to trading stolen information.

Scrapers download publicly available data on dark web websites or forums trading personal information, then analyze the data to find a match.

Suppose some of your PII is found. In that case, you are then notified to take the necessary measures to

protect yourself.

**Do You Need Dark Web Monitoring?**

Because the dark web is hidden from the regular internet user and its shabby history, it’s essential to know if your information is out there. Criminals can use your information to commit any of the vast arrays of identity theft crimes (using stolen identities to commit fraud, primarily for financial gain).

Consequently, you need to know about data leaks and breaches because it's nearly impossible to shield yourself from future attacks if you don't.

Dark web monitoring tools keep you informed so you can take action to limit, or, better, entirely avoid the

resultant problems like account takeover, identity theft, financial fraud, and others.

If you’re keen on protecting yourself, these monitoring services will give you some form of leverage to better prepare for the worst.

**Do Dark Web Monitoring Tools Work?**

Before you go to spend your hard-earned cash on any of the identity theft and monitoring services that also promise dark web monitoring, you should know if it works in the first place.

The fact is, they do, but there are significant limitations that make these tools not as efficient as you might be told to believe.

The effectiveness of a dark web monitoring tool is tightly tied to how long it takes to find these stolen credentials. And that solely depends on when your information is publicly revealed on the dark web. In other words, if your information is being sold on the dark web, these tools won't access it. And you won't know if your data is out there.

Chances are, by the time stolen data is given away for free on the dark web, someone has already tried to use it in nefarious ways.

Knowing of data breaches earlier is always better, and thus more responsibility is often in the hands of

companies that hold your details.

**19012021081: Jinal Sojitra**

**2CEIT78PE8:FCL**

**Tor Browser:**

Tor (short for “The Onion Router”) is a completely free, open-source browser that helps you surf the internet anonymously. It erases your browsing history automatically with every session and encrypts all your traffic. It also lets you access the dark web — the hidden and un-indexed websites on the internet. Because of its ability to let you access the world wide web freely, some countries block Tor entirely.

Originally, the Tor network was developed by the U.S. Navy to enable anonymous online communication for military organizations. In 2006, the military dropped the project, which has since been handled by a non- profit.

These days, the Tor Project mainly focuses its attention on its browser and the development of a few other privacy tools, which we’ll touch on later.

**The Tor browser and the dark web**

Pirated content iconThe Tor browser is the only browser that lets you visit the dark web. The dark web generally features websites that you can’t access through a normal search engine or via a conventional browser. You also need to know the exact web address to visit a dark website.

The dark web is home to unregulated websites, which means you can find anything from pirated movies to black markets, illegal drugs, and child porn on there.

As such, we don’t advise visiting the dark web unless you know what you’re doing. We also have a dedicated guide for information about the Dark Web.

**19012021081: Jinal Sojitra**

**2CEIT78PE8:FCL**

**Practical: 3**

**Aim: Tracing/Tracking Fake Accounts on Social Media**

**What are Fake Social Media Accounts?**

Fake social media accounts are profiles that are either not associated with a real person or are created with an actual person’s personal information without their consent. These accounts are usually called imposter accounts or sock puppet accounts. The latter is mainly used to describe accounts run by people to praise themselves and criticize others.

**Scammers create fake social media accounts for various reasons, including**

To impersonate you or others

To extort money from your followers through scams (usually by pretending that the original owner of the account is in trouble and needs donations)

To harass people online

To spread false information – usually political – and hate speech

To leave false reviews or complaints about brands and their products/services

To destroy a person’s reputation

Most, if not all, of the major social media platforms (i.e. Facebook, Twitter, Instagram, LinkedIn, Pinterest, YouTube, and Snapchat) are plagued with fake accounts. Even some minor platforms (Quora, Tumblr, etc.) and dating apps have fraudsters pretending to be other people.

**Profile Picture**

Fake accounts often use avatars and symbols as their profile images, instead of photos. And when they do use actual human photos, they are usually low resolution. Low-res pictures can be a red flag when the account purportedly belongs to a public figure or celebrity.

To be sure whether the account is fake or not, run the profile picture through search engines like Google Image Search to see if the image is linked to another account or has appeared somewhere else on the internet.

**Photo Forensics:**

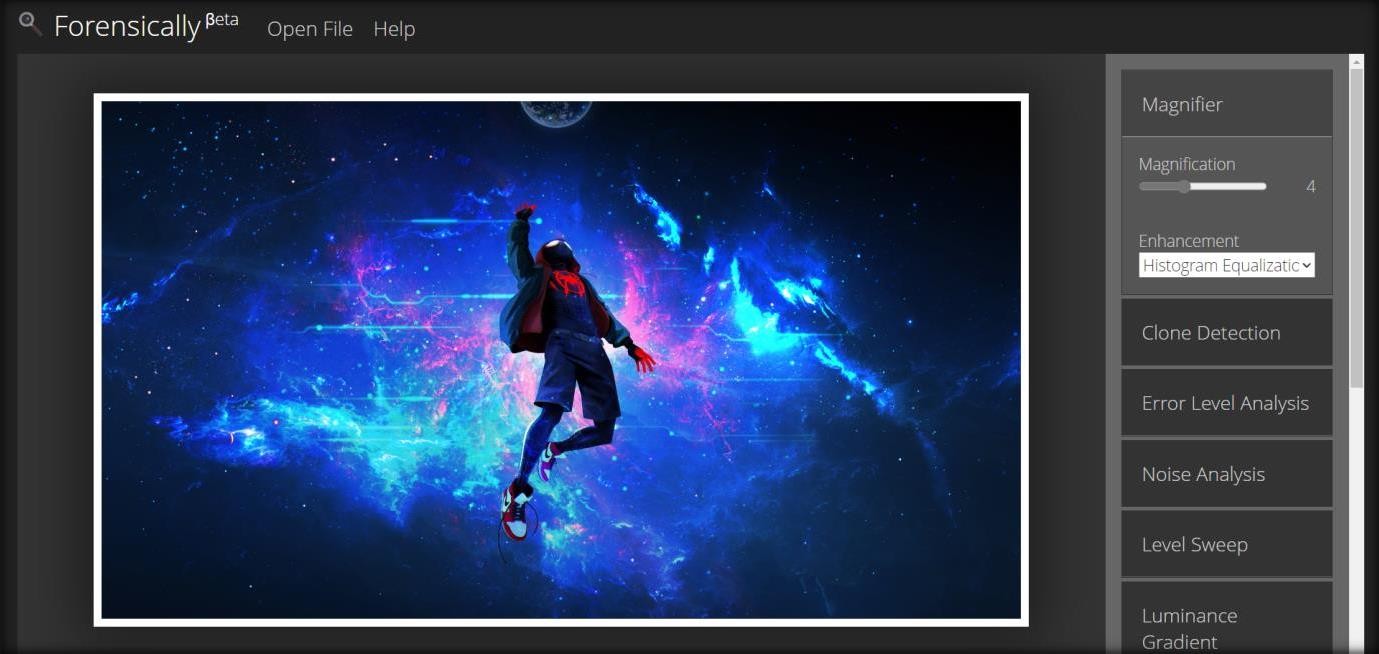
Photographs have been doctored since photography was invented. Dictators have erased people from photographs and from history. Politicians have manipulated photos for short-term political gain. Altering photographs in the predigital era required time-consuming darkroom work. Today, powerful and low-cost digital technology makes it relatively easy to alter digital images, and the resulting fakes are difficult to detect. The field of photo forensics—pioneered in Hany Farid's lab at Dartmouth College—restores some trust to photography. In this book, Farid describes techniques that can be used to authenticate photos. He provides the intuition and background as well as the mathematical and algorithmic details needed to

understand, implement, and utilize a variety of photo forensic techniques.

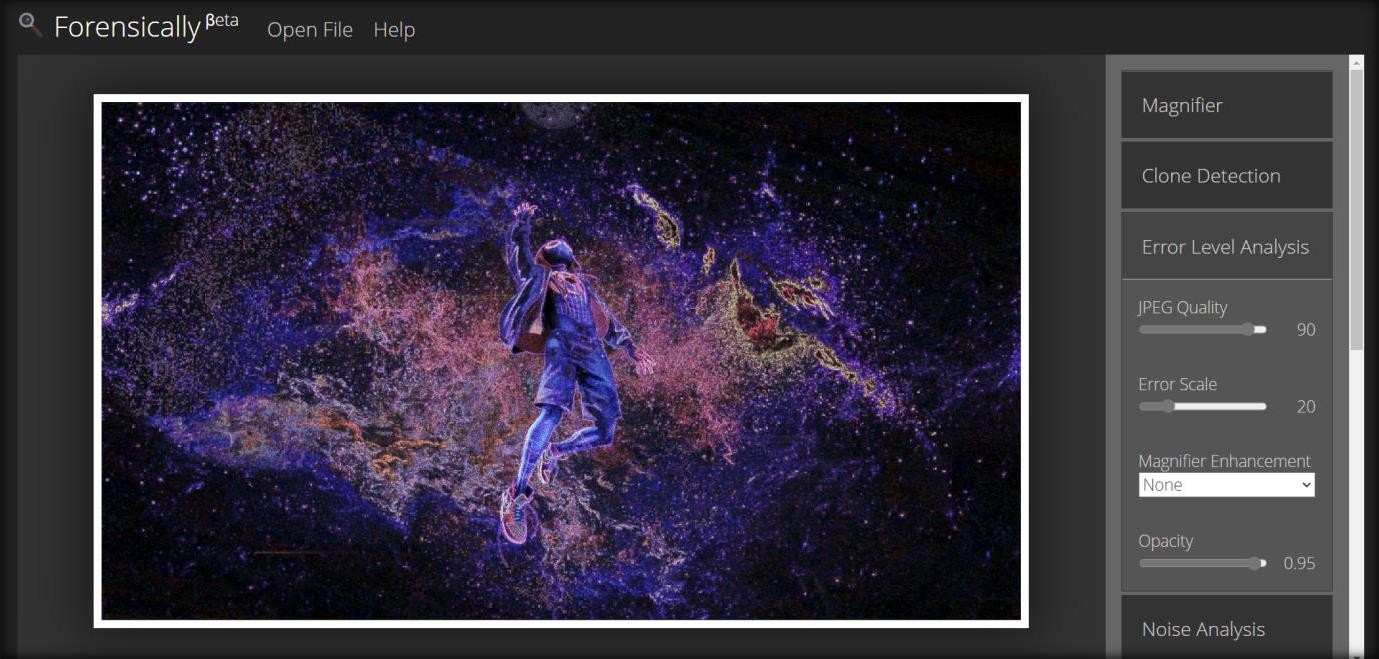
**19012021081: Jinal Sojitra**

**2CEIT78PE8:FCL**

[**Forensically, free online photo forensics tools - 29a.ch**](https://29a.ch/photo-forensics/#forensic-magnifier)



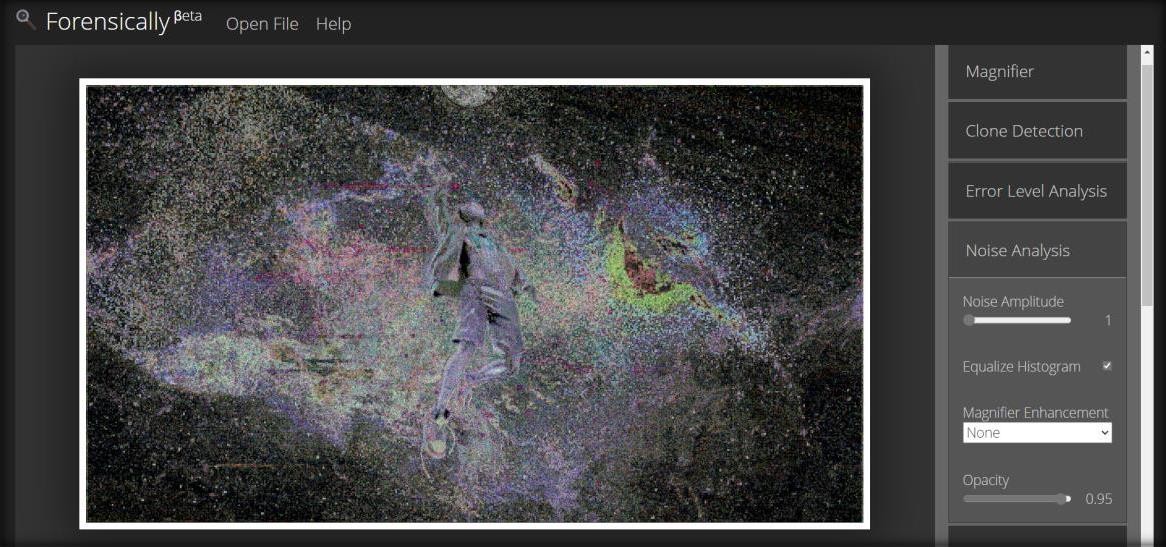
**Error Level Analysis:**



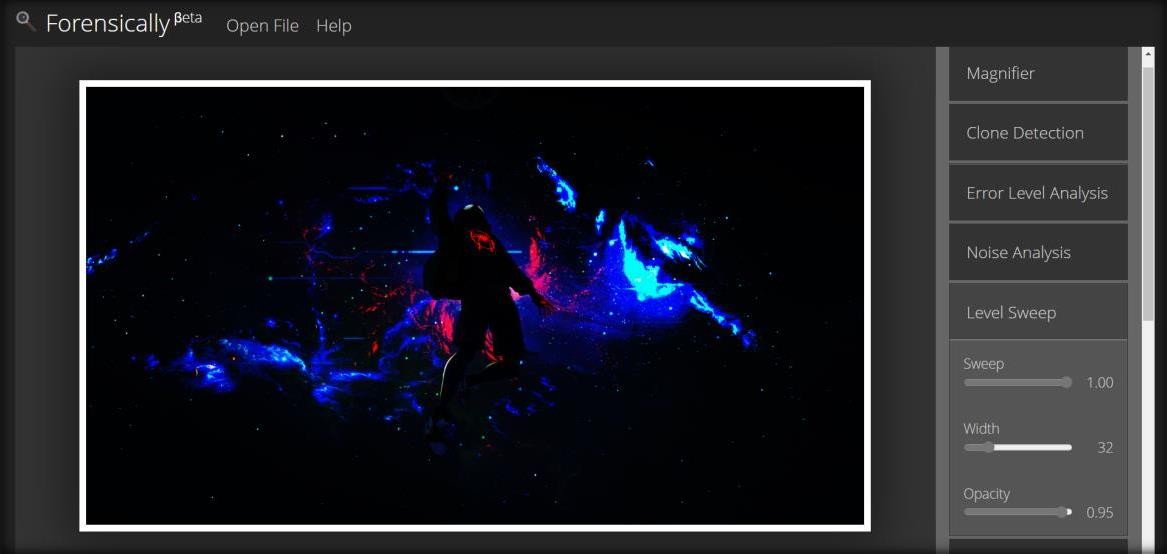
**19012021081: Jinal Sojitra**

**2CEIT78PE8:FCL**

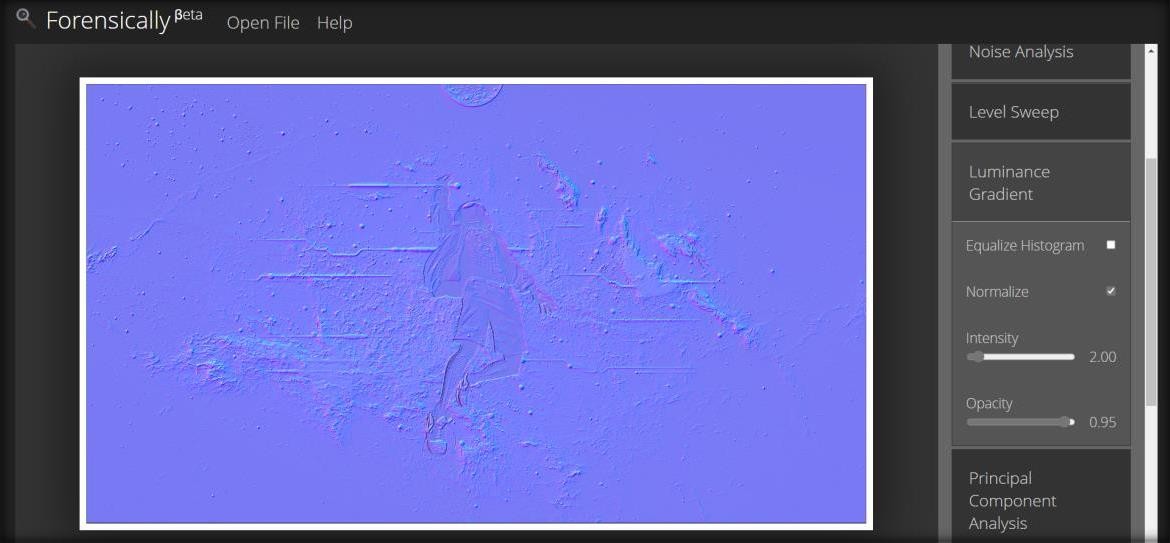
**Noise Analysis:**



**Level Sweep:**



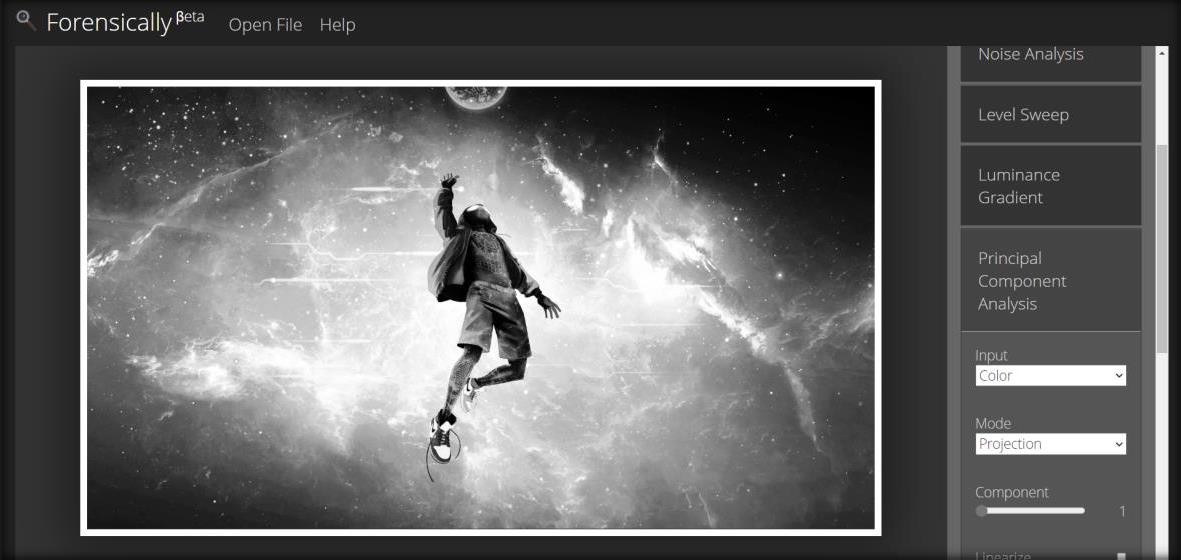
**Luminance Gradient:**



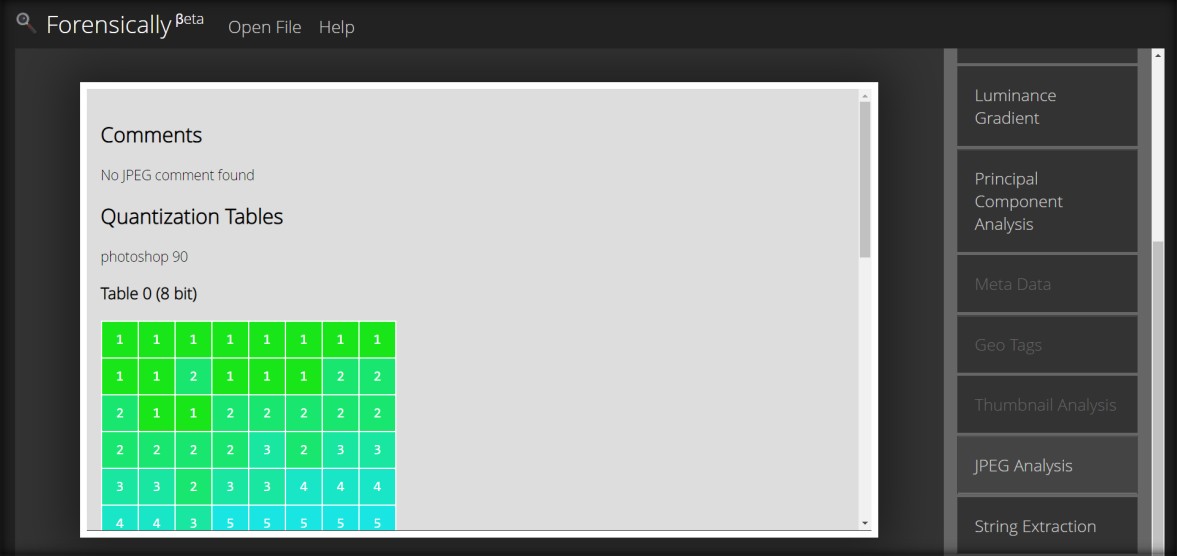
**19012021081: Jinal Sojitra**

**2CEIT78PE8:FCL**

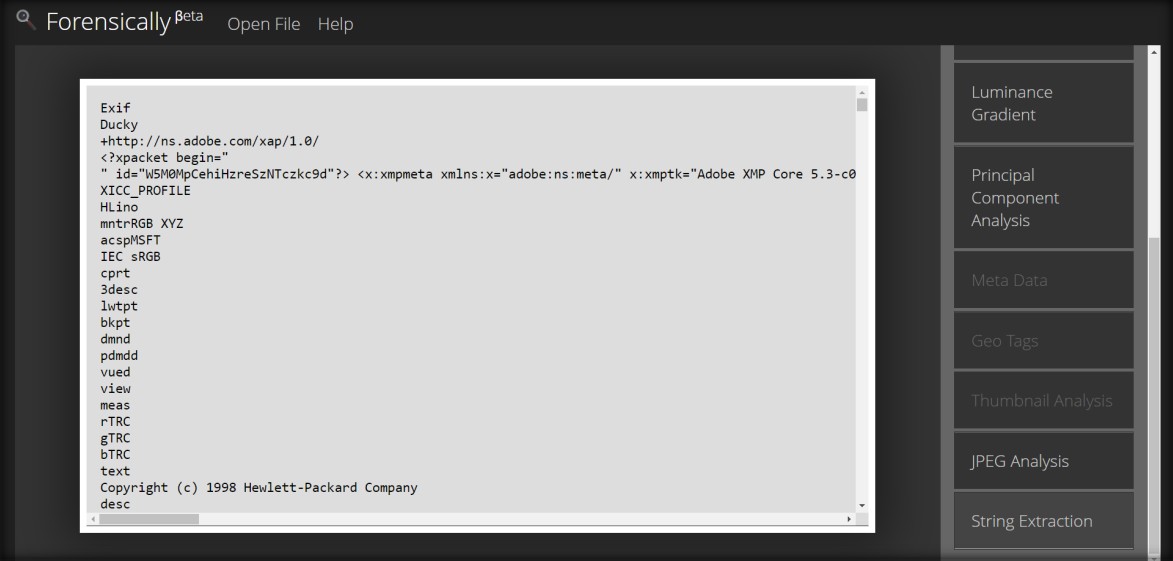
**Principal Component Analysis:**



**JPEG Analysis:**



**String Extraction of the image:**



**19012021081: Jinal Sojitra**