रा.इ.सू.प्रौ.सं
NIELIT

राष्ट्रीय इलेक्ट्रॉनिकी एवं सूचना प्रौद्योगिकी संस्थान, रोपड़

National Institute of Electronics and Information Technology (NIELIT), Ropar

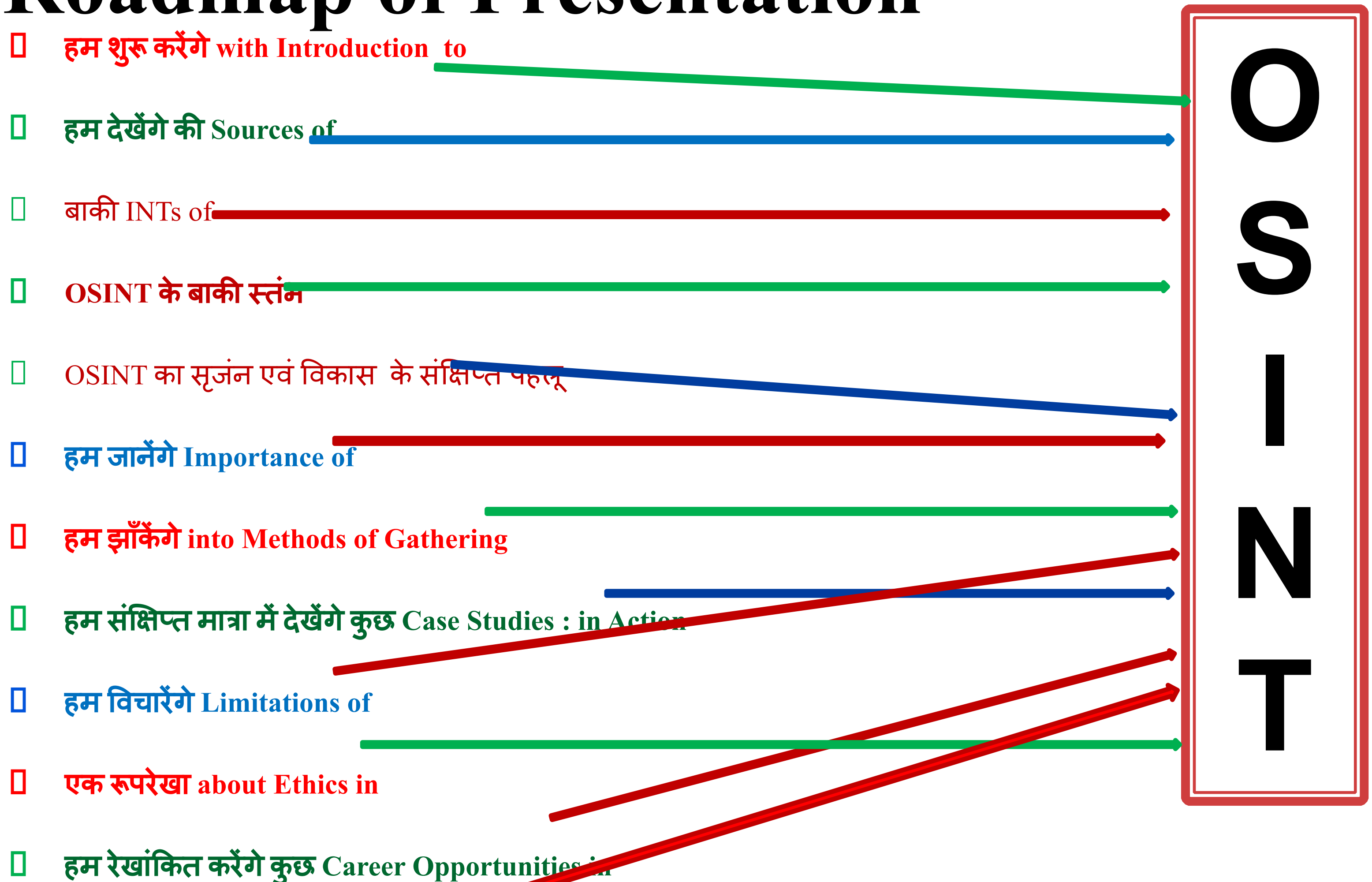
परदा उठाना Open Source Intelligence (OSINT) से

Open Source Intelligence (OSINT) Demystified

RAMINDER SINGH

SCIENTIST 'E', NIELIT ROPAR

Roadmap of Presentation



- हम शुरू करेंगे with Introduction to
- हम देखेंगे की Sources of
- बाकी INTs of
- OSINT के बाकी स्तंभ
- OSINT का सृजंन एवं विकास के संक्षिप्त पहलू
- हम जानेंगे Importance of
- हम झाँकेंगे into Methods of Gathering
- हम संक्षिप्त मात्रा में देखेंगे कुछ Case Studies : in Action
- हम विचारेंगे Limitations of
- एक रूपरेखा about Ethics in
- हम रेखांकित करेंगे कुछ Career Opportunities in

OSINT

हम आज की प्रस्तुति ख़त्म करेंगे एक

Cyber Security Slogan के साथ

Concept of OSINT

- Definition (परिभ|शा क्या है OSINT की?)
  refers to the collection and analysis of information from publicly available sources.

- What it includes? (क्या आता है इस में?)
  information from social media, news articles, websites, public records, and other online sources.

- Where it is used? (कहाँ होती है यह इस्तेमाल ?)
  is used by various entities for intelligence gathering, investigations, cybersecurity, and competitive analysis.

- Example of OSINT (OSINT का कोई उधारण)
  National Intelligence Grid (NATGRID) is in process of integrating data analytics, open source intelligence (OSINT) tool and web-based applications to offer a 360 degree solution for intelligence and law enforcement to authorised central and State agencies.

Other OSINTs

- Human Intelligence (HUMINT) -- is intelligence collection by human-to-human interaction.

- Signals Intelligence (SIGINT) -- employs interception of communications or messages done electronically COMINT (Communications Intelligence) & interception of Electric signals (for example, monitoring of radars) termed as ELINT (Electronic Intelligence).

- Geospatial Intelligence (GEOINT) -- visual representation of activities, analysis of images to extract information of intelligence called IMINT (Imagery Intelligence)

- Measurements & Signals Intelligence (MASINT) -- is scientific & technical information obtained by analysis of data (metric, angle, spatial, wavelength, time dependence, modulation, plasma, and hydro-magnetic) derived from technical sensors

Image Ref: https://www. wysiwygwebbuilder.com/

Text Reference Institutionalising Open Source Intelligence (OSINT) in India: An Analysis Amiy Krishna Himachal Pradesh National Law University, Shimla

OSINT के बाकी स्तंभ (remaining Pillars)

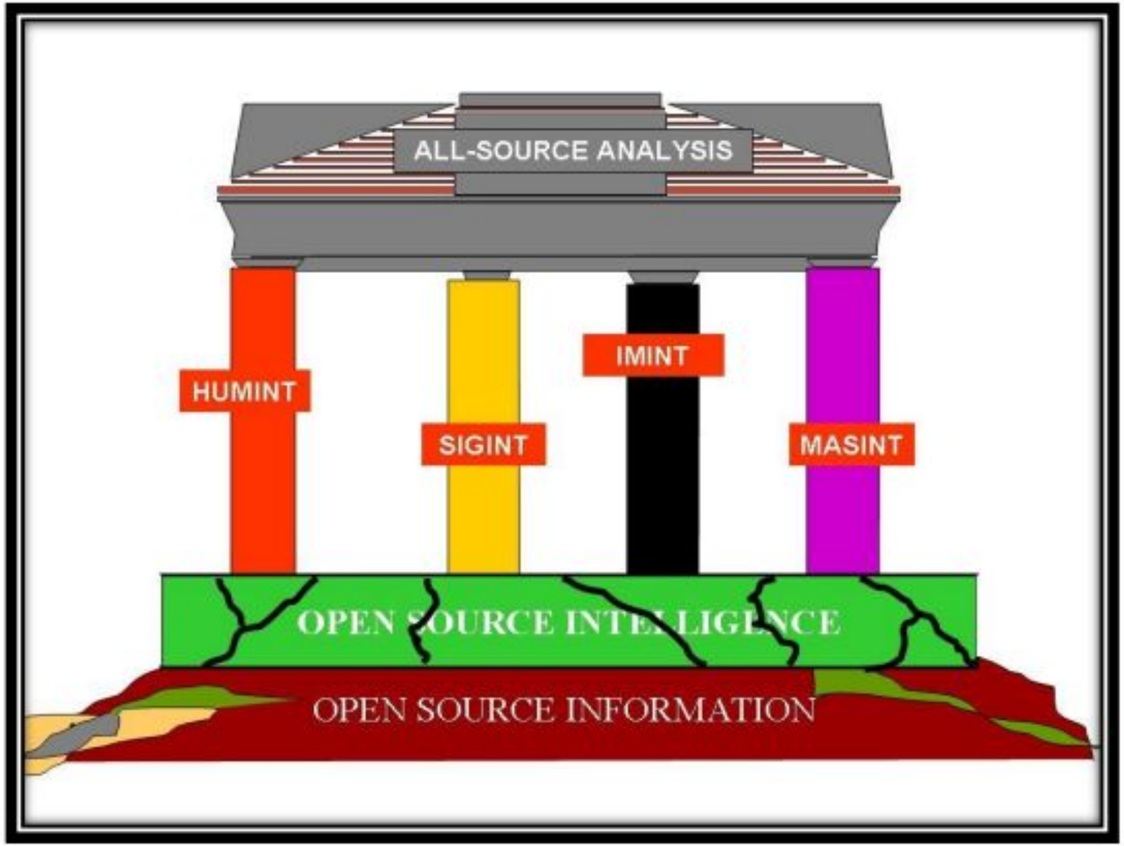


Image Reference Institutionalising Open Source Intelligence (OSINT) in India: An Analysis Amiy Krishna Himachal Pradesh National Law University, Shimla

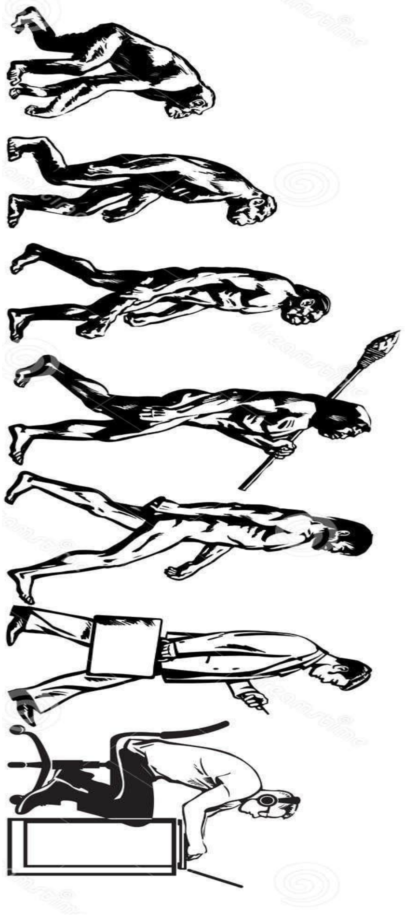
Evolution (सृजन) of OSINT and its brief (संक्षिप्त) Development (विकास)

Evolution of OSINT can be presented in three different phases:

- Pre-World War I blurred differences between open & secret sources
- post World War II till Cold War, intelligence experts realised importance of newspapers, radio & personal witness accounts.
- End of Cold War to present 'Revival of OSINT'. Internet & development of ICT

Major events for OSINT

- intelligence activities of US were carried out by e Office of Strategic Services (OSS) which was established in 1944 by William Donovan
- After Cold War, 'open to all' OSINT conference was organised by Robert David Steele. 600 participants from government and private sector, more than 40 countries



https://www.dreamstime.com/theory-evolution-man-theory-evolution-man-human-development-monkey-to-caveman-modern-businessmen-talking-image118185128

From where OSINT comes -- Publically Available information

- Websites: Information available on public websites, including news sites, social media platforms, government portals, and blogs.
- Online Communities: Forums, discussion boards, and social media groups where individuals share information and opinions.
- Public Records: Government records, court documents, property records, and business registrations that are accessible to the public.
- Open Data: Datasets released by governments, organizations, and researchers that can be freely accessed and analyzed.

Image Reference
https://www.sans.org/blog/what-is-open-source-intelligence/

From where OSINT comes -- Media Sources

- News Outlets: Newspapers, TV news channels, and online news platforms that provide up-to-date information on various topics.
- Broadcasts: Radio and TV broadcasts that can be monitored for intelligence gathering purposes.
- Podcasts: Audio programs covering a wide range of topics, including interviews, discussions, and analysis.
- Blogs and Opinion Pieces: Online articles and blog posts that offer insights and perspectives on different subjects.

Importance (महत्व) of OSINT

- provides access to a vast amount of publicly available information.

- It helps in understanding & analysing current events and trends.

- is crucial for conducting thorough research & making informed decisions.

By Whom OSINT is used (कौन इस्तेमाल करता है इसे)

- Government
- Law Enforcement
- Military
- Investigative journalists
- Human rights investigators
- Private Investigators
- Law firms
- Information Security
- Cyber Threat Intelligence
- Pen Testers
- Social Engineers

Image and tect Reference https://www.sans.org/blog/what-is-open-source-intelligence/

How OSINT is used ? (कैसे इस्तेमाल होता है ?)

Security and Intelligence

can be used to gather information on potential security threats, such as terrorist activity or cyberattacks. also be used for intelligence gathering on foreign governments, organizations, or individuals

Business & Market Research

used to gather information on competitors, industry trends, & consumer behaviour. can be used to inform business strategy & decision-making

Social Media Monitoring

Monitoring social media platforms such as Facebook, Twitter, Instagram, and LinkedIn to collect relevant information and insights.

Public Records Research

OSINT can be used by journalists to gather information on a range of topics, including politics, business, & crime. help to uncover stories & provide evidence for reporting.

Investigative Journalism:

Searching analysing public records, government databases, court filings, business registries, &property records, to uncover valuable intelligence.

Legal proceedings

OSINT can be used in legal proceedings to gather evidence or to conduct due diligence on potential witnesses or defendants.

https://www.sans.org/blog/what-is-open-source-intelligence/

OSINT Intelligence Cycle

- **Preparation** is when needs, requirements of request are assessed, such as determining objectives of tasking, identifying best sources to use to find information one is looking for.
- **Collection** collecting data information from as many relevant sources as possible.
- **Processing** collected data information are organized or collated.
- **Analysis and Production** interpretation of collected information to make sense of what was collected, i.e. identifying patterns or a timeline of travel history.
- **Dissemination** is presentation delivery of open-source findings, i.e. written reports, timelines, recommendations, etc. Answer questions for stakeholders

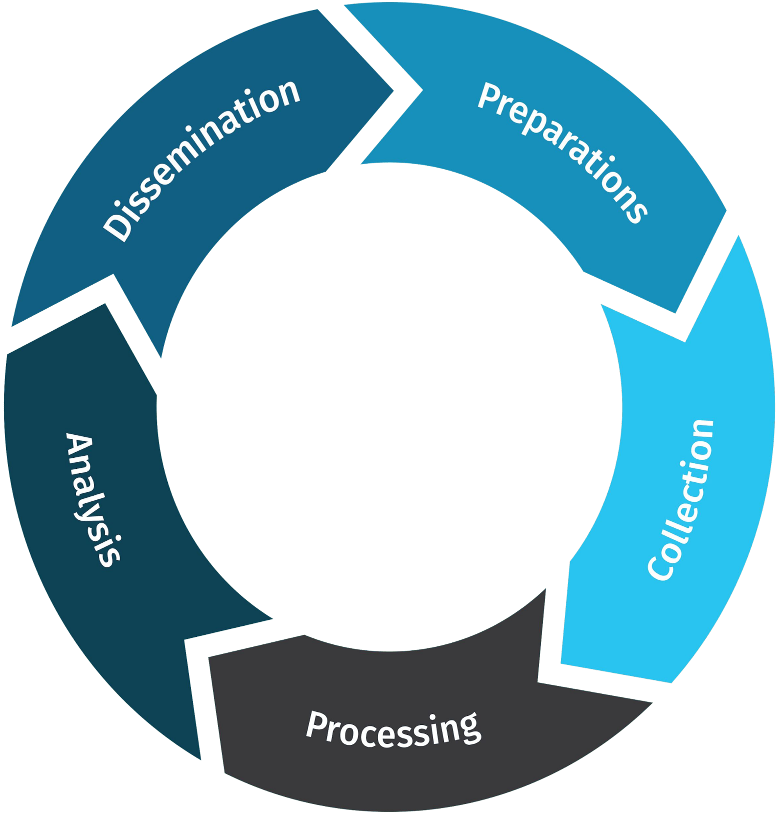


Image reference
https://www.sans.org/blog/what-is-open-source-intelligence/

OSINT Types (प्रकार)

Passive OSINT

- No engagement with the target
- Passively collecting from publicly available information
- Low risk of attribution

Active OSINT

- Engagement with the target
- May require special permission
- High risk of attribution

Image reference ***https://vietnamteachingjobs.com/active-vs-passive-learning/***

Advanteges (फायदे) of OSINT

Open-source intelligence (OSINT) is beneficial because it offers several advantages over other forms of intelligence collection.

Access to publicly available information: OSINT collects publicly available & legally accessible information. Organizations do not have to rely on classified or restricted sources of information, which can be costly & time-consuming to get.

Wide range of sources: gathered from a wide range of sources, including social media, news articles, government reports, & academic papers.

Timeliness: Because OSINT relies on publicly available information, it can be gathered quickly & in real time. Organizations or businesses can stay up-to-date on current events & emerging trends.

Cost-effective: than other forms of intelligence collection, such as human intelligence or signal intelligence. because OSINT relies on publicly available information & does not require specialized equipment or personnel.

https://www.sans.org/blog/what-is-open-source-intelligence/

OSINT techniques (तकनीकें)

uses range of techniques for collecting & analysing publicly available information. These are:

Search Engines -- Google, Bing, and Yahoo are valuable tools for gathering OSINT. using advanced search operators to find relevant information.

Social Media -- Twitter, Facebook, & LinkedIn valuable sources of OSINT. Monitoring & analysing: social media activity, analysts gain insight : trends, sentiment, & potential threats.

Public Records -- court documents, property records, & business filings: OSINT. Analysts gather information : individuals, organizations, & other entities.

News Sources -- newspapers, magazines, & online news outlets are valuable sources. Monitoring & analysing: news articles, analysts gain insight into current events, trends, & potential threats.

Web Scraping --. scraping data from multiple websites, analysts gather large amounts of relevant data in no time quickly & efficiently.

Data Analysis Tools-- Excel, Tableau, & R valuable for analysing large datasets. using these tools, analysts identify patterns, trends, & relationships in the data.

Image Reference
https://www.sans.org/blog/what-is-open-source-intelligence/

https://www.sans.org/blog/what-is-open-source-intelligence/

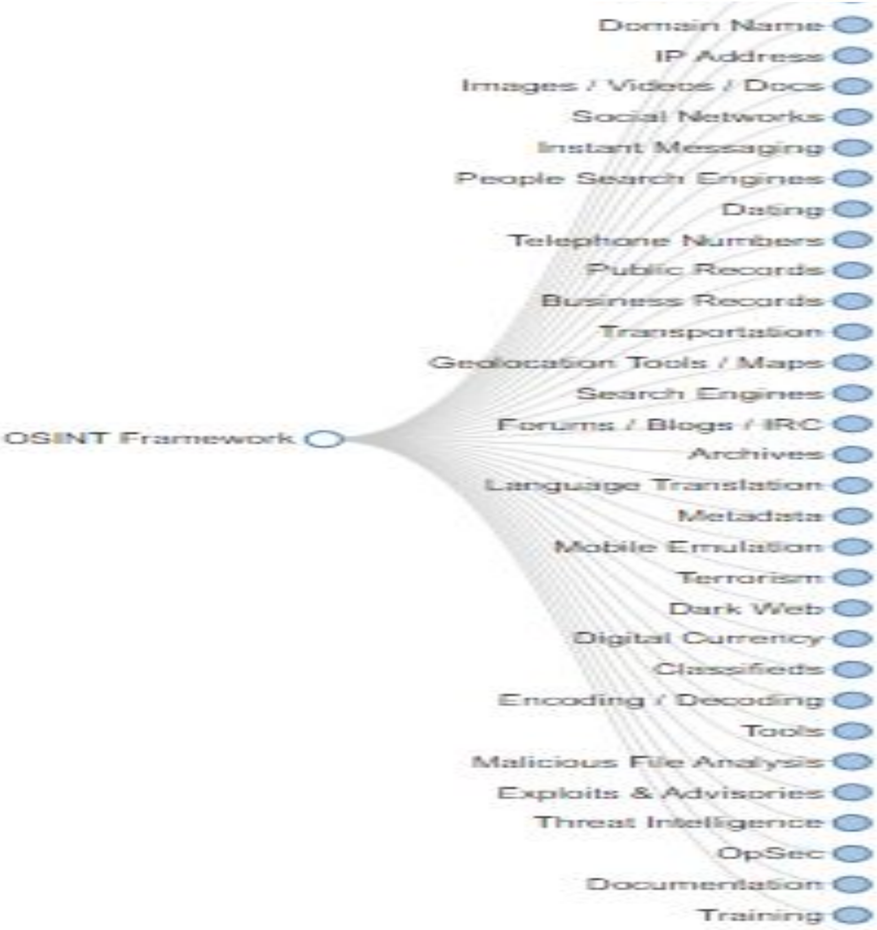
How is OSINT useful (मददगार) for organisation (संगठन)

used by a organizations, governments, businesses, & non-governmental organisations. useful in information gathering for a wide range of topics such as security threats, market research, & competitive intelligence.

- Support criminal investigations by providing background profiles on people & businesses
- Support human source assessments
- Support security/risk assessments
- Support decision making
- Assist with making associations between entities
- Provide situational awareness such as getting insight into current events

Live OSINT Framework (का चित्रन)

Website
https://osintframework.com/



Case Study examples : OSINT की कार्य कुशलता

- **Osint in Modern Warfare depicting Russian Ukraine war**

  Published in :January 21, 2023 | Expert Insights*Reference*

  https://www.synergiafoundation.org/insights/analyses-assessments / osint-modern-warfare

- **Balakot, China 'incursions' prove OSINT images are new threat for democracies and military *by LT.GEN H.S Panag (Retd,)***

  Published in:10 October, 2019 10:13 am IST

  https://theprint.in/opinion/balakot-china-incursions-osint-images-new-threat-democracies-military/303565/

- NATGRID developing centralised data platform using AI, OSINT for real time action against criminals

  Updated - April 26, 2023 at 08:51 PM. | New Delhi, April 26

  BY DALIP SINGH

  https://www.thehindubusinessline.com/news/natgrid-developing-centralised-data-platform-using-ai-osint-for-real-time-action-against-criminals/article66781491

How to begin (शुरुआत) OSINT

1. Fundamentals

- Understand basic principles & concepts of Open Source Intelligence (OSINT).
- Familiarize yourself with various sources of open source information available.
- Learn about different OSINT tools & techniques.

2. Develop Research Skills

- Enhance your online research skills to effectively gather information.
- Learn how to verify credibility &reliability of sources.
- Practice organizing & analysing large amounts of data.

Tools one may use (इस्तेमाल) in OSINT -Maltego

To start with here are some Open Source tools that one may use to gather information and learn about OSINT in a more practical oriented way.

Came into being in 2008, Maltego is one of the established OSINT tool.

It basically

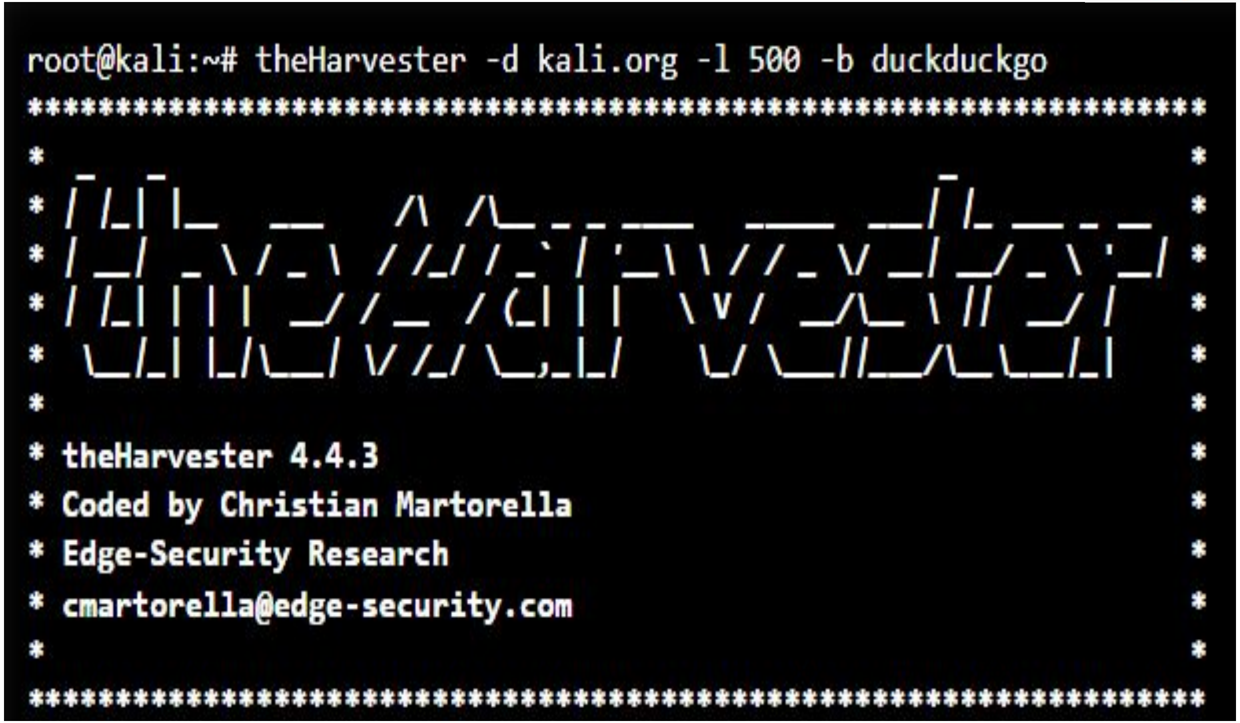
- monitors and map out links between entities,
- provides a visualisable output to user using it.

Very powerful when one wants to get information pertaining to cyber security aspects, especially identity of malwares.

Tools one may use (इस्तेमाल) in OSINT – The harvester

Another very powerful tool that is written in Python language is the theHarvester

- can be used to search Google, Bing, and PGP servers for e-mails, hosts, and subdomains.
- also search LinkedIn for user names.
- collects data from more than twenty mainstream search engines and websites, including Google, Bing, Yahoo.
- compiles whatever intelligence it can find on the public domain.

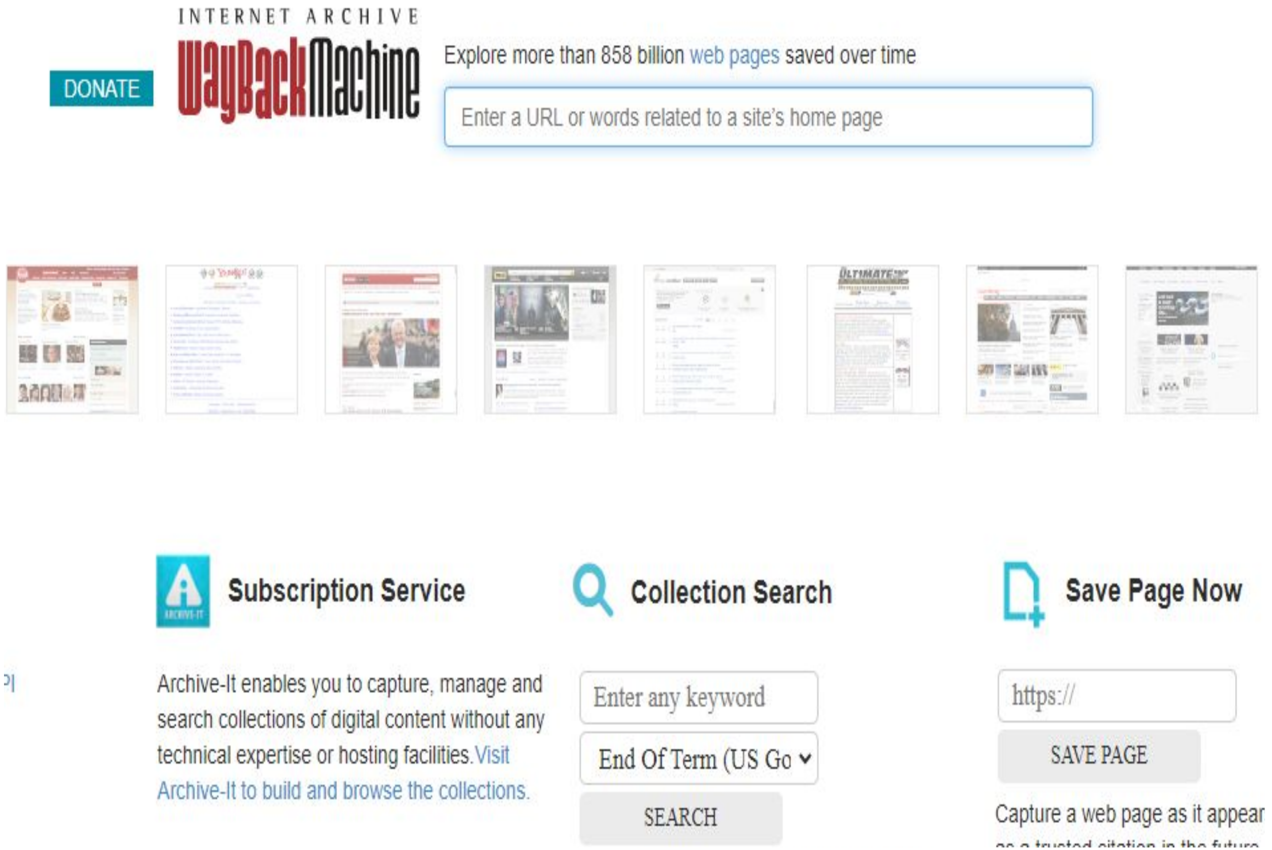


```
root@kali:~# theHarvester -d kali.org -l 500 -b duckduckgo
*******************************************************************
*  _   _                                            _             *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester 4.4.3                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************
```

Tools one may use (इस्तेमाल) in OSINT - Wayback Machine

https://archive.org/web/

- can be used to search Google, Bing, and PGP servers for e-mails, hosts, and subdomains.
- also search LinkedIn for user names.
- collects data from more than twenty mainstream search engines and websites, including Google, Bing, Yahoo, and Twitter,
- compiles whatever intelligence it can find on the public domain.



INTERNET ARCHIVE WaybackMachine

DONATE

Explore more than 858 billion web pages saved over time

Enter a URL or words related to a site's home page

Subscription Service

Archive-It enables you to capture, manage and search collections of digital content without any technical expertise or hosting facilities. Visit Archive-It to build and browse the collections.

Collection Search

Enter any keyword

End Of Term (US Go

SEARCH

Save Page Now

https://

SAVE PAGE

Capture a web page as it appear

Open Source Intelligence Limitations (की सीमायें)

- OSINT is not about what you find, but what you do with what you find

https://www.makeuseof.com/all-you-need-to-know-about-open-source-intelligence-osint/

1

Incomplete and limited information:

- **Open Source Intelligence relies on publicly available information, which may be incomplete or limited in scope.**

2

Lack of Context:

Open Source Intelligence often lacks the necessary context to fully understand the information collected, making it challenging to draw accurate conclusions.

3

Reliability and accuracy:

The accuracy and reliability of information obtained through Open Source Intelligence can vary, as it may be prone to misinformation or manipulation.

Open Source Intelligence Ethics (की आचार नीतियाँ)

What is Ethics?

- set of moral principles that govern a person's behaviour or conduct of an organization.
- involves distinguishing between right & wrong & making decisions based on ethical values.

Ethics in Open Source Intelligence

- ethics play a crucial role in ensuring responsible & legal use of information.
- considerations include respect for privacy, accuracy of information, & avoiding harm or exploitation.
- Adhering to ethical principles in Open Source Intelligence helps maintain trust, credibility, & professionalism.

An example of OSINT misuse in real world – A possibility

The 1997 released James Bond movie “Tomorrow Never Dies” is the best example where with the misuse of OSINT, two countries come close to the brink of war.

Tomorrow Never Dies

Career options (करियर की संभावनायें) in OSINT

Threat Intelligence Analyst

- play a crucial role in gathering & analysing OSINT data to provide insights & actionable intelligence to organizations.
- use advanced tools & techniques to collect, evaluate, & interpret information from various sources.

Certified Threat Intelligence Analyst
Cyber Secrurity | Network Security | IT Security | Cyber Security Audit

Digital Forensics Analysts

- specialize in examining digital devices & data to uncover evidence in legal cases or cybercrime investigations.
- employ OSINT techniques to gather information from online sources, analyse it, & present findings in a court of law.

Threat Intelligence Researcher

- focus on identifying & analysing potential threats to organizations.
- utilize OSINT tools & methods to monitor online platforms, social media, other sources to gather information about potential risks, vulnerabilities, & malicious activities.

OPERATIONAL THREAT INTELLIGENCE RESEARCH WITH OSINT

Today’s (आज का) Cyber Security Slogan(मंत्र)

फ़ेसबुक (Facebook) पर अपनी प्रोफाइल (Profile) को हमेशा रखें लॉक (lock), ताकि सोशियल मीडीया (Social media) पर बनी रहे हमेशा आपकी साख

Thank YOU all .

आप सबका बहुत आभार