

Open Source Intelligence (OSINT)



“Known Unknowns”



- “There are known knowns, things we know that we know; and there are known unknowns, things that we know we don’t know. But there are also unknown unknowns, things we do not know we don’t know”
- *Donald Rumsfeld, A Memoir*



Open Source Intelligence (OSINT) defined

“Open-source intelligence (OSINT) is an intelligence that is produced from publicly available information and is collected, exploited and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement”

US Department of Defence

“Ninety percent of intelligence comes from open sources. The other ten percent, the clandestine work is just more dramatic. The real intelligence hero is Sherlock Holmes not James Bond”

Lieutenant General Sam Wilson, former Director, Defence Intelligence Agency.



OSINT & Data Protection

- Lawfulness , fairness and transparency.
- What you collect for one purpose cannot be used for another incompatible purpose.
- Data minimisation, collect as much as necessary or as little as possible.
- Accuracy- ensure the data is good quality
- Storage limitations, retain no longer than needed.
- Integrity and confidentiality. You cannot public disclose what you have collected about an individual.
- Accountability you must be able to demonstrate the reasons for collecting the data.
- Notification every data subject should be notified.(Unless restrictions apply)



Open Source Data (OSD)

Generic data from a primary source. Satellite images, telephone call data, metadata, datasets, survey data, photographs, audio or video recordings.

Open Source Information (OSINF)

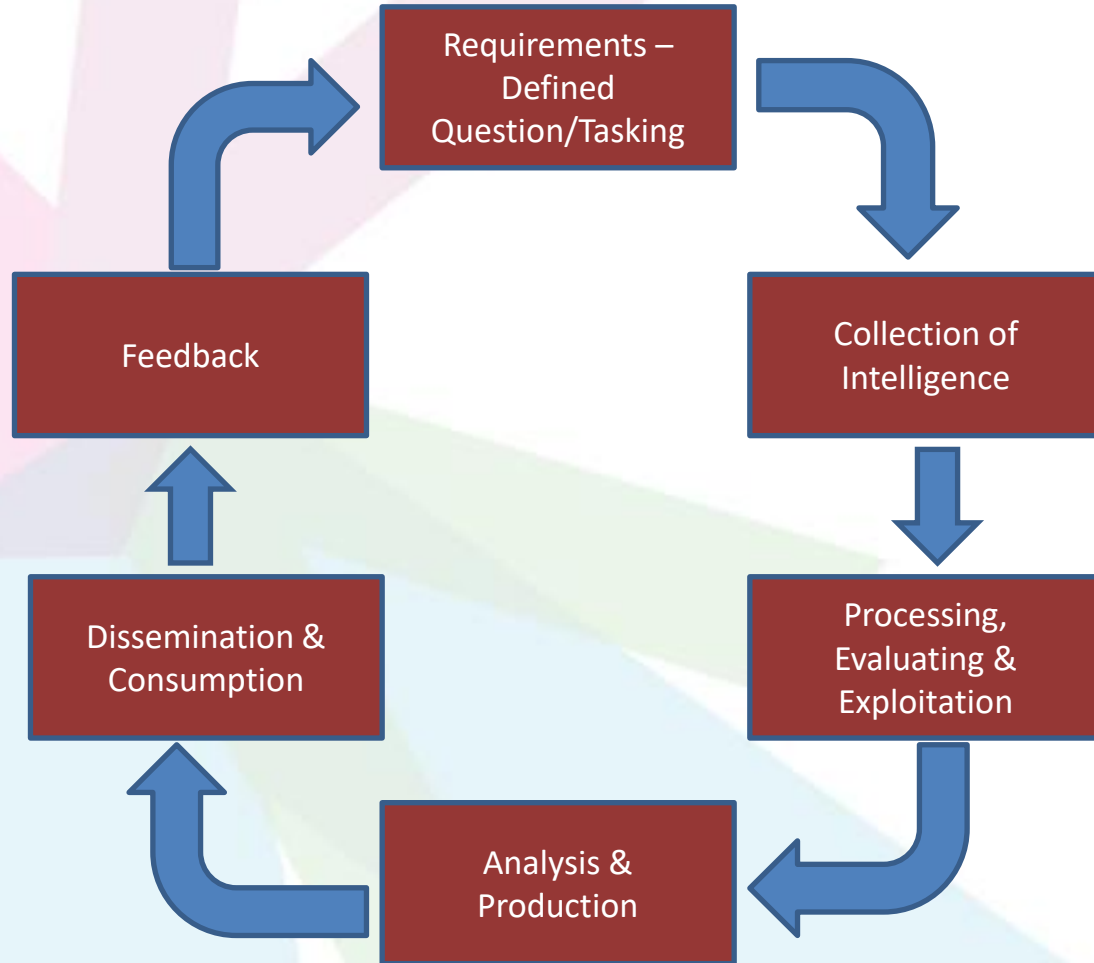
Generic data from a secondary source. Books, articles, dissertations, artworks and interviews,

Open Source Intelligence (OSINT)

Information that has been discovered, filtered and designed to meet a specific purpose. The output of open source material processing.

Validate Open Source Intelligence (OSD)

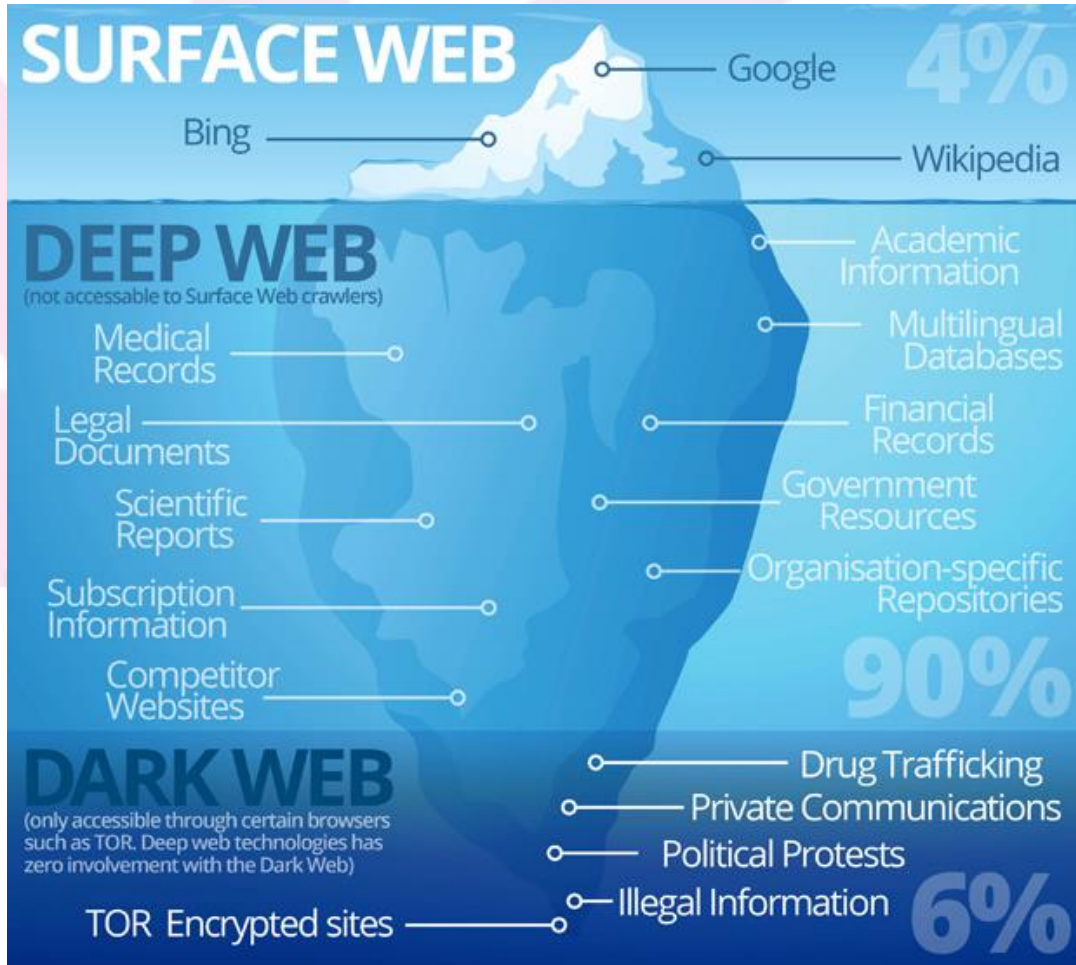
OSINT with a degree of certainty. Data that has been verified from a reputable source





Using the internet safely







Staying safe online

```
Command Prompt

C:\>ipconfig /all

Windows IP Configuration

Host Name . . . . . : DC01
Primary Dns Suffix . . . . . : Prohut.net
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : Prohut.net

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . : 
Description . . . . . : Intel(R) 82574L Gigabit Network Connection
Physical Address. . . . . : 00-0C-29-C9-64-81
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
IPv4 Address. . . . . : 192.168.1.10(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
DNS Servers . . . . . : 192.168.1.10
NetBIOS over Tcpip. . . . . : Enabled

Tunnel adapter isatap.{3C381FB8-0BCB-4801-920D-582078C06860}:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : 
Description . . . . . : Microsoft ISATAP Adapter
Physical Address. . . . . : 00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes

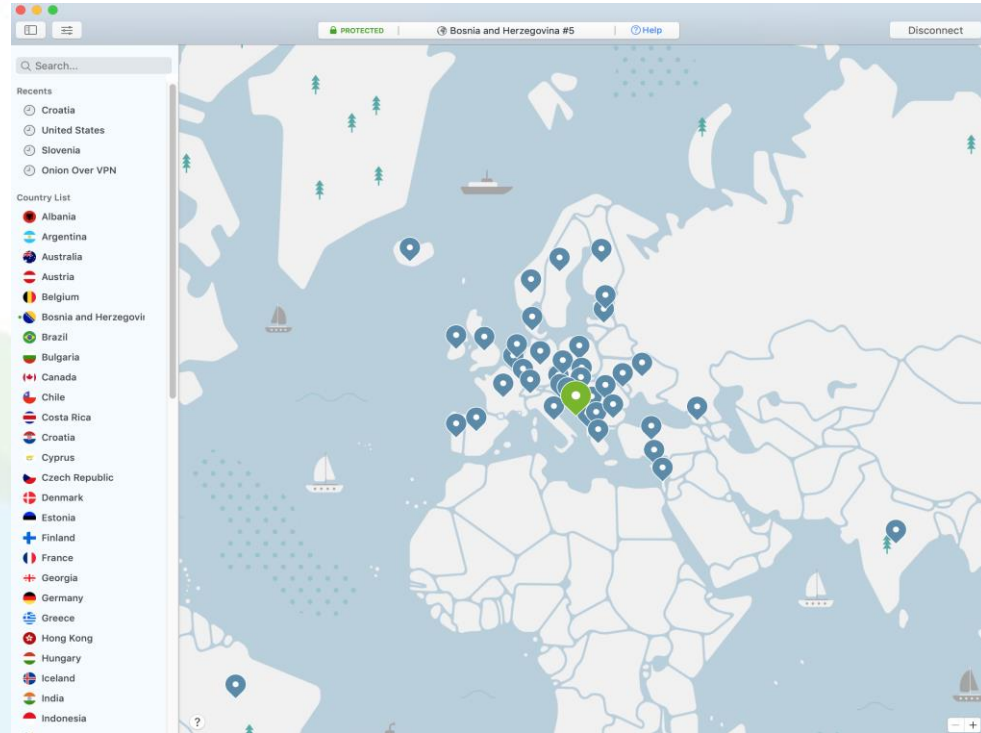
C:\>
```

- IP Address is the unique address of a device that identifies itself on a network and is assigned by your internet service provider (ISP).
- Static IP Address –
Using the same IP all the time.
- Dynamic IP Address –
A new IP is assigned by ISP each time you connect to the internet by using Dynamic Host Configuration Protocol (DHCP)



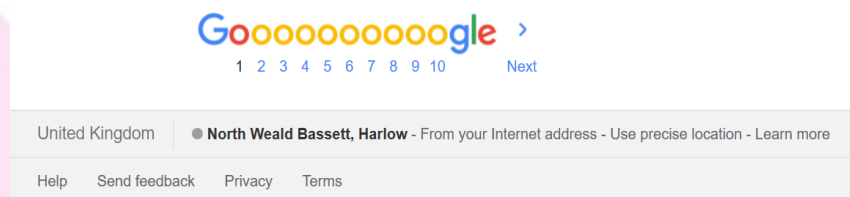
Virtual Private Network (VPN)

- Access remote sites while assuring confidentiality of sensitive data
- Gives user anonymous IP address
- User appears to be in a different location avoiding censorship
- Share files privately

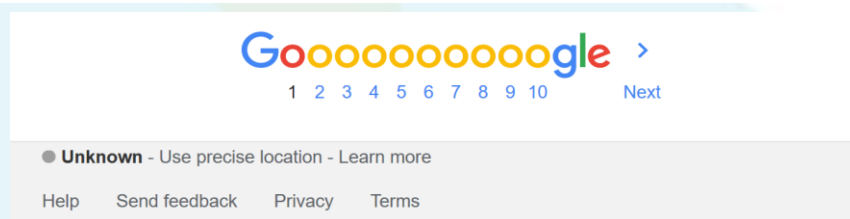
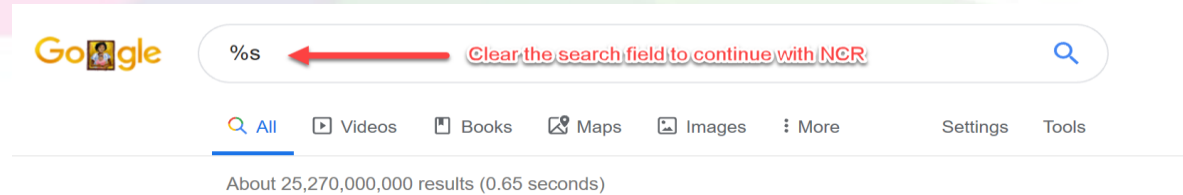




Searching Google -No Country Recognition



https://www.google.com/search?q=%s&pws=0&gl=us&gws_rd=cr





Searching Effectively

- Ask the right question.
- Define your topic as succinctly as possible
- Who? What? Where? When? How? Why?
- List keywords (Between 4 and 8). The average is 1.5 this is not enough



Enforced Term Operators

- Account Number – 9,810,000,000
- Account Number and sort code – 358,000,000
- “Account Number” – 28,600,000
- “Account Number” “sort code” – 1,070,000
- “Account Number” AND “sort code” – 987,000
- “Account Number” AND “Sort Code” AND Barclays – 95,900
- “Account Number” AND “sort code” AND “Barclays Bank” – 66,200
- “Account Number” AND “sort code” AND “Barclays Bank” AND London – 29,100
- “Account Number” AND “sort code” AND “Barclays Bank” AND Bosnia – 1,580
- “Account Number” AND “sort code” AND “Barclays Bank” AND Sarajevo – 713
- “Account Number” AND “sort code” AND “Barclays Bank” AND Sarajevo filetype:pdf - 11
- “Account Number” AND “sort code” AND “Barclays Bank” AND Sarajevo AND Rahma filetype:pdf - 1



Anonymous Search Engines

- <https://www.startpage.com/>
- <https://www.lukol.com/>
- <https://www.mozbot.com/>
- <https://peekier.com/>
- <https://www.searchencrypt.com/>
- <https://search.disconnect.me/>
- <https://www.discretesearch.com/>
- <https://duckduckgo.com/>
- <https://www.oscobo.com/>
- <http://yippy.com/>

Create a 'NEW' identity...



Fake Name Generator generates random names and information that you can use to create false profiles within Social Media. <http://namegenerators.org/fake-name-generator/>
<https://en.namefake.com/>

You do not want to use your personal account for your business purpose. <https://www.fakemail.net/>

Generate an email address that you can use to receive confirmation requests or to send anonymous emails to a subject or entity. <https://emailfake.com/>

If you have a Gmail account, then you can receive alias emails into your genuine inbox. This is called the "Gmail dot Trick."

If your email is johnsmith@gmail.com, you own all dotted versions of your address:

- john.smith@gmail.com
- jo.hn.sm.ith@gmail.com
- j.o.h.n.s.m.i.t.h@gmail.com

Need a face to put to your fake account.

Pictures on a profile are important to get right. <https://generated.photos/faces>





The Darkweb

Negative

- Drug dealing
- Arms dealing
- False documents
- Hackers, ransomware other security exploits
- Terrorist organisations
- Illegal gambling and betting
- Sale of stolen information – corporate secrets, credit card and banking details
- Counterfeit items

Positive

- Human rights activists
- Journalists
- Whistleblowers
- Privacy advocates
- Law enforcement
- Individuals and governments for the exchange of secret / sensitive information.
- Open source intelligence
- Monitoring of forums and blogs



Fictional Case Study



You have been provided a photograph of a male wearing a blue suit and asked to create a subject profile. You are not told any more information.

What are your actions?

Assume nothing

Believe nobody

Check everything

Google Reverse Image Searching - Location



Tracing Assets



