Intelligence Collection For Investigations

Intro to OSINT & Reconnaissance

Have you done OSINT research before?

You've conducted recon if you've:

- Unmasked a catfish or stalker online
- Found someone's social media information from a phone number
- Searched through relationships between a user and their friends to learn about them
- Found information about a target from photos posted publicly
- Looked at cached versions of websites offline
- Used custom search variables in google searches like "" or limiting by date
- Searched through city or government databases to find information
- Done a reverse google image search

Asking Answerable Questions

Research is the process of discovering information someone else already knows. Through asking narrowly defined, answerable questions, we can make our investigations efficient and successful.

In order for an investigation to be successful, it is critical that you ask craft answerable questions before starting your research. Which of these is answerable?

Does Brazil have a better music scene than Norway?

What is the most important tech startup in Norway?

How many drug related offenses make up arrests in Oslo?

Are public officials more corrupt in Sweden or Norway?

Open ended questions are difficult to answer and lend themselves more to opinions. Due to how much information is available online, you will waste hours digging through speculative, low quality information.

Distill Investigations Into Answerable Questions

Let’s take an unanswerable question and convert it into answerable ones.

Are public officials more corrupt in Sweden or Norway?

- How many charges of crimes public corruption were prosecuted between 2009 and 2019 in Norway and Sweden?
- Who is a prosecutor, police source, or expert on corruption in Norway and Sweden I can interview and quote?
- What books or research can I consult on public corruption in both countries?
- How is public corruption investigated in each country, and what organization is responsible for it?

These questions can be answered. It’s critical that before you begin, you extract the most answerable questions from your overall investigation.

Researching Answerable Questions

After extracting your answerable questions, the next important step is to determine the scope of your investigation. Before starting, you should know how much information you need to answer your question.

Who owned the company that was recently fined for unsafe labor practices?
Look through business registration records in the state to identify the owner on registration documents

What experts on corruption can I speak to in Norway and Sweden?
Find recent press articles about corruption and note which experts they interviewed, contact the agencies they are affiliated with.

How do I contact a person at a company who doesn't list their email address publicly?
Scrape company email addresses, discover the format the company uses for email addresses, and apply the format to the name of the person you wish to contact.

Break down these questions into answerable ones:

Is cybercrime the biggest threat to businesses?
How serious is gun violence in Norway?
How do I contact someone about security at Equifax?

Different Types of Intelligence Collection

What is the difference between gathering information from active and passive recon?

Passive collection is preferred and almost always used to start, because it will not alert the target to the investigation.

Navigating to a website or looking up the information of who owns it from a third party will not likely alert a target to your presence. In passive recon, we minimize any interaction with the target network that could raise any red flags. Because of this, OSINT is the preferred way for hackers and researchers to conduct recon.

Active collection discovers information directly from interactions with the target, and increases the likelihood of detection. This may blow the investigators cover, depending on what you're investigating. We can use tools like ping, nmap, nikto, and traceroute to learn technical information about the target networks directly, and even through direct contact trick a subject into clicking an advanced web tracking link.

Some more types of recon - HUMINT

HUMINT - Most good investigators can rely on social engineering and soft skills to learn information that would be challenging or impossible to find with OSINT. Human intelligence is the art of creating information-bearing relationships with carefully chosen sources. This can be as simple as an attractive sales agent buying coffee for a receptionist each time they visit the company, or as extreme as overtly pressuring a source.

There are many ways to make someone who hates you still give you information. OSINT can be used to convince people you know so much about their company already that any secrets they have are worthless. By creating the illusion you already know everything about the company, a target is less likely to hold back.

Some more types of recon - SIGINT

SIGINT is the branch of intelligence that studies signals for information. This can be as simple as observing the wireless traffic in an area to determine when people come and go, or as elaborate as planting a device to record the wireless traffic of a target network to capture passwords.

Signals intelligence often requires proximity to a target, but can learn a lot even through passive means. Through signals intelligence, we can determine things like GPS location by the signal strength of nearby wireless networks, which computers are connected to which wireless networks, and silently footprint the technology in a geographic area.

A researcher signing up for a tour of a facility could walk the floor with an Android phone running a wireless sniffer, identifying every device present including the unique MAC address of employees smartphones and personal devices. This allows for tracking the proximity of those devices later. The most useful data learned in SIGINT investigations is often who was present in a location or what networks a target has permission to access.

Open Source Intelligence - An Ocean Of Data

- OSINT is a branch of both the military and civilian intelligence services, but also a core part of business intelligence.
- The majority of the information available online is not accessible through google, meaning a google search can only skim the surface.
- Most information is found in databases or can be accessed through API's
- Most business or government functions generate data and papertrails
- People contribute tons of information about themselves on social media sites, and the data can be accessed via API's
- Vast pools of data can be mined, analyzed, and sorted to look for relationships that wouldn't be immediately obvious to a human researcher

C2055837 STARBUCKS U.S. BRANDS CORPORATION

Registration Date:	09/18/1997
Jurisdiction:	CALIFORNIA
Entity Type:	DOMESTIC STOCK
Status:	MERGED OUT
Agent for Service of Process:	**CORPORATION SERVICE COMPANY WHICH WILL DO BUSINESS IN CALIFORNIA AS CSC - LAWYERS INCORPORATING SERVICE (C1592199)** To find the most current California registered Corporate Agent for Service of Process address and authorized employee(s) information, click the link above and then select the most current 1505 Certificate.
Entity Address:	533 AIRPORT BLVD., SUITE 400 BURLINGAME CA 94010
Entity Mailing Address:	533 AIRPORT BLVD., SUITE 400 BURLINGAME CA 94010

Document Type	File Date	PDF
MERGER	02/17/2004	
MERGER	01/14/2004	
SI-NO CHANGE	07/28/2003	
SI-COMPLETE	10/14/1997	Image unavailable. Please request paper copy.
REGISTRATION	09/18/1997	Image unavailable. Please request paper copy.

The Intelligence Cycle

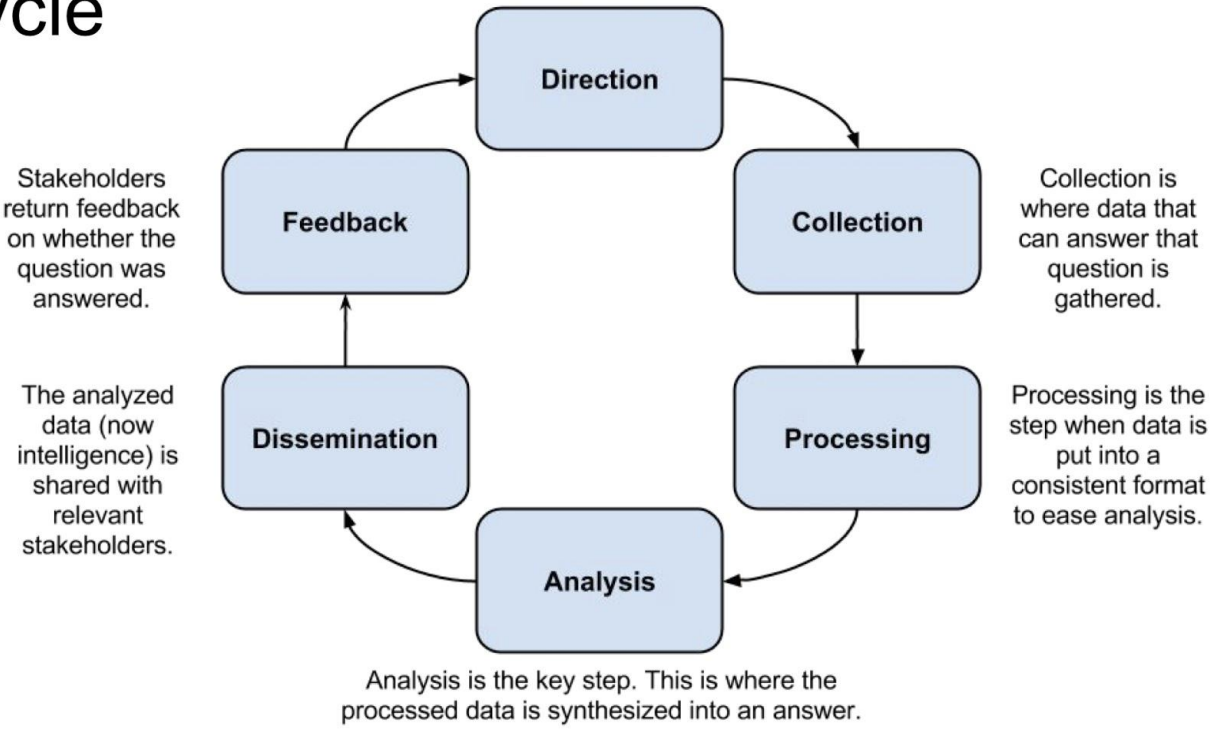
To begin an intelligence investigation, we have to ask an answerable question.

Good questions:

- What server technology does scientology.org use?
- Has anyone working at The Guardian had their passwords compromised in a major breach?

Bad questions:

- Is Goodwill more secure than CVS?
- Should Equifax fire their CEO?



Source: thebridgesummit.co

The purpose of intelligence gathering is to refine raw data into insight and understanding through answering questions in an investigation

Data is not intelligence

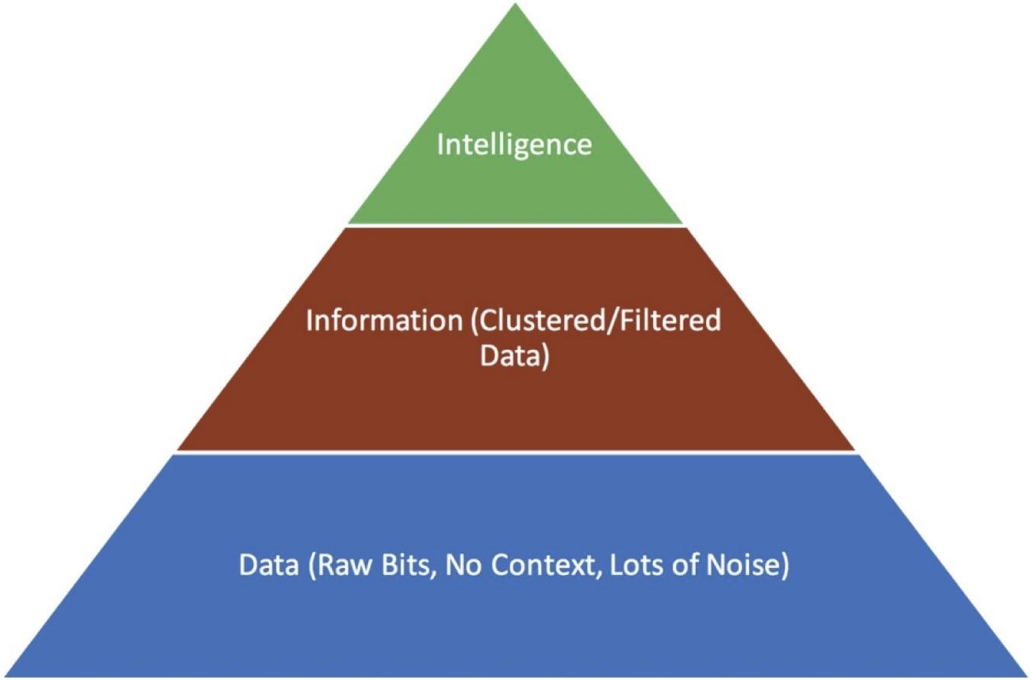
The goal of an investigation with Maltego is to refine raw data into intelligence

Through gathering data to build a complete picture of the question we are trying to answer, we can arrive at very specific conclusions.

Through representing data in a Maltego graph, we can see patterns through link analysis

Link analysis is a type of knowledge discovery. It is an iterative and user-interactive process used to spot, attempt to analyze, and clearly visualize patterns in datasets.

Feeding bad or irrelevant data into link analysis makes it useless



What is Maltego?

Maltego is a canvas onto which you can place data, and then use algorithms called “Transforms” to mine related data

It takes care of the process of data import, processing, transformation, analysis, and visualization with a single click

Pulls from vast API’s of data to be able to search for patterns and clearly display them

Commercial partners develop Transforms for investigators, police, military, and intelligence agencies

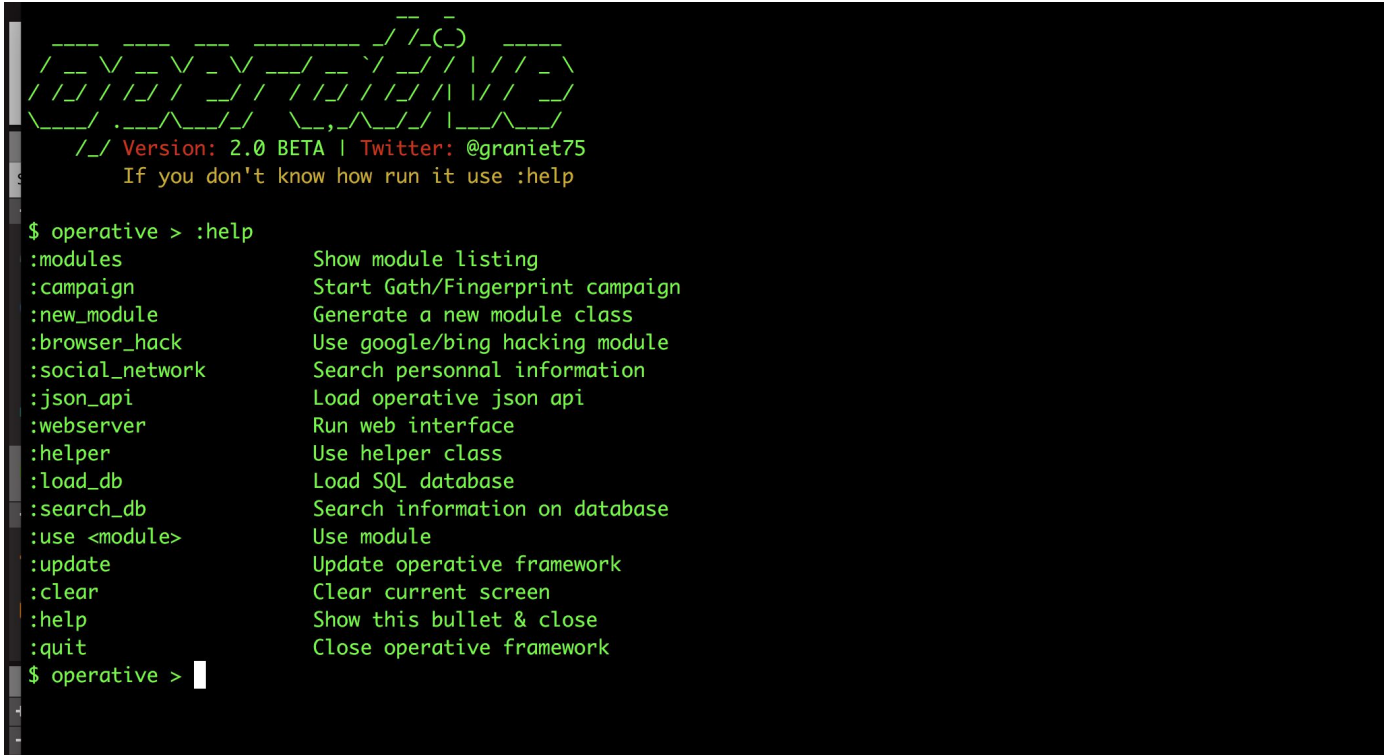
Particular focus on social media and technical infrastructure, tracking of people, organizations, and physical hardware

Basic OSINT - Data Scrapers

Whois queries - Find information on websites
The Harvester - Search for email addresses to contact and track hard to find people - https://github.com/laramies/theHarvester
The OSINT Framework - Web interface for access to many common OSINT tools

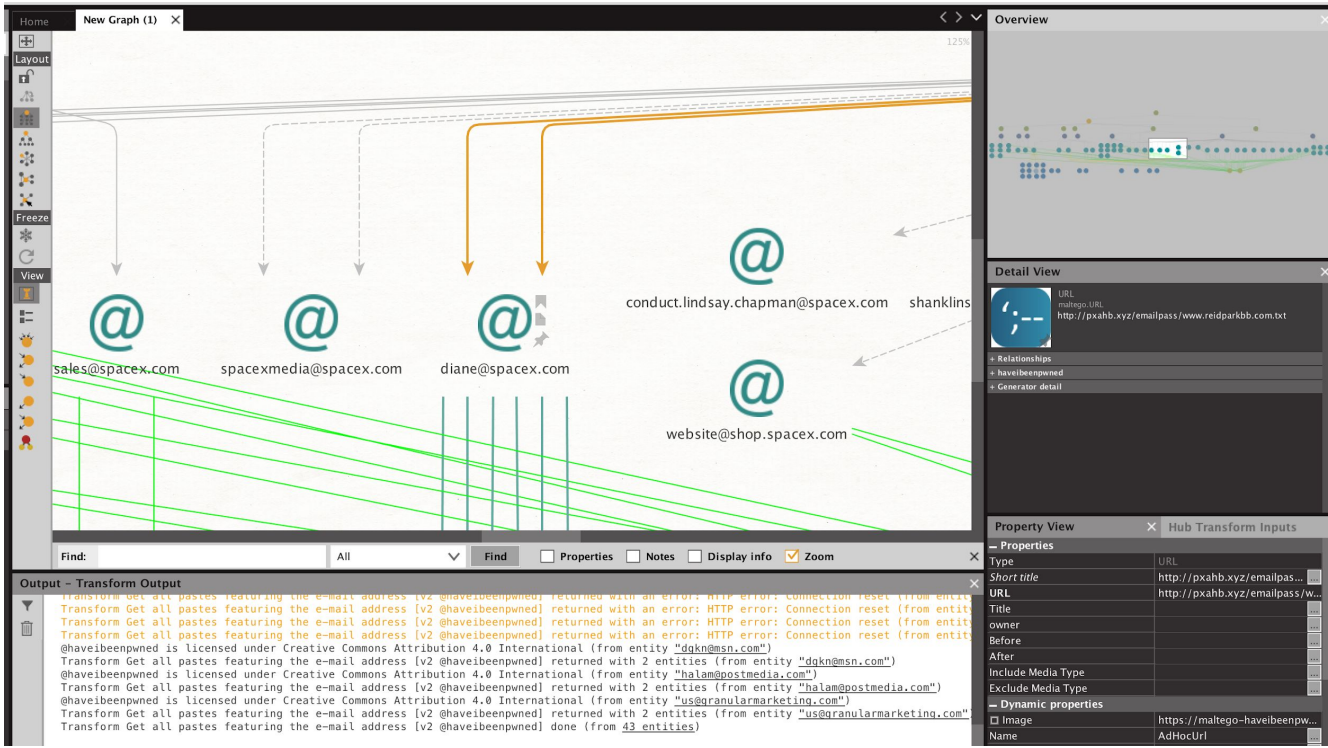
Beginner OSINT - The Operative Framework

Find the email address of a owner of a website, then search for other websites they own.
Find the default passwords of devices you encounter



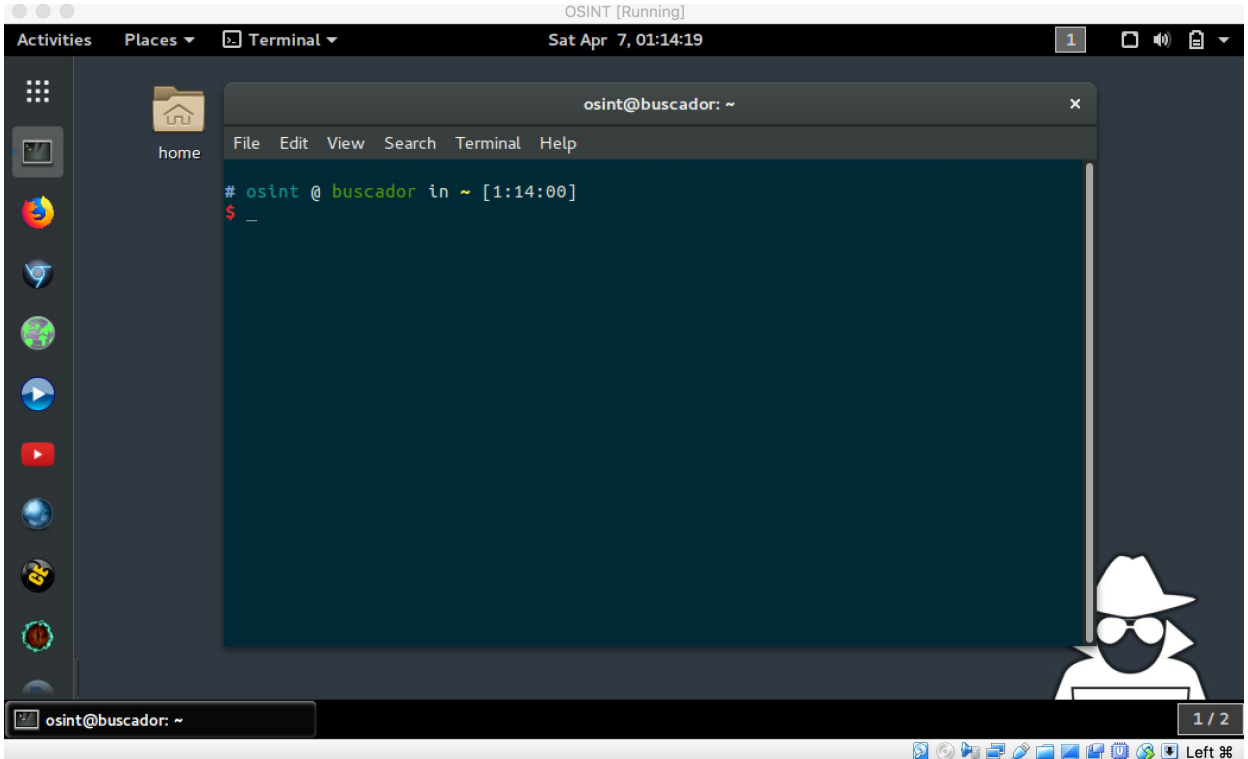
Intermediate OSINT - Maltego

- Link secretive organizations with tracking codes
- Identify other websites on the same server
- Profile technology a website or service uses
- Profile a user on social media and look for links
- Track a user across the internet
- Identify key members of organizations



Advanced OSINT - Buscador OS

Entire linux OS dedicated to OSINT



Questions to research -

Target: **SpaceX -** Aerospace company

Investigation Objective: **What is the procedure for SpaceX to work with an outside company, and who is in charge?.**

Target: **Smith & Wesson** - Firearms manufacturer.

Investigation objective: **How many lawsuits has Smith & Wesson faced in the past 5 years?**

Target: **Priceline.com** - Organization convicted of interfering in US politics and investigations

Investigation objective: **What internal files has Priceline.com left public?**

We can come back to these after we learn some more tools!

Reading and more lecture

Reading:

Email Scraping to find target email addresses -
https://null-byte.wonderhowto.com/how-to/scrape-target-email-addresses-with-theharvester-0176307/

Target fingerprinting with the Operative Framework -
https://null-byte.wonderhowto.com/how-to/recon-research-person-organization-using-operative-framework-0176323/

How to conduct an OSINT investigation with Maltego -
https://null-byte.wonderhowto.com/how-to/video-use-maltego-research-mine-data-like-analyst-0180985/

Lecture:

Maltego - Cyber Weapons Lab - Research like an OSINT Analyst
https://youtu.be/46st98FUf8s?list=PLs3nCuKxkfjCIld1RJU67ToVRWCYznvXn

Extra Credit:

Spiderfoot - https://null-byte.wonderhowto.com/how-to/use-spiderfoot-for-osint-gathering-0180063/