<https://www.maltego.com/downloads/>

Master link for all the documents:

<https://docs.maltego.com/support/home>

**Use this to understand the solution**

<https://docs.maltego.com/support/solutions/articles/15000008703-client-requirements>

**Introduction to Maltego**

<https://docs.maltego.com/support/solutions/articles/15000034121-introduction>

**Read the Uses cases from Maltego**

<https://docs.maltego.com/support/solutions/articles/15000012022-use-cases>

**🧠 Maltego Challenge Lab – Beginner Notes**

**🔍 What is Maltego?**

**Maltego** is a **graph-based OSINT tool** used to:

* Visualize relationships between people, domains, emails, IPs, social networks, etc.
* Perform deep-dive investigations on a person or organization.
* Map out cyber incidents or attacker infrastructure.

It uses **"Transforms"** (mini scripts) to pull public data from various sources.

**🎯 Lab Objective**

In a typical **Maltego Challenge Lab**, your goal is to:

* Track down a hacker, email, domain, or incident
* Map out relationships and evidence
* Use OSINT transforms to build the full picture

**🛠 Basic Concepts in Maltego**

| **Concept** | **What It Means** |
| --- | --- |
| **Entity** | An object like a person, domain, email, IP, phone number |
| **Transform** | A search query or action that finds more info |
| **Graph View** | A visual network of entities and their relationships |

**✅ Steps in Maltego Challenge Lab**

**Step 1: Start with a Seed (e.g., Domain or Email)**

* Example: example.com
* Add it to your graph

**Step 2: Run Transforms**

Right-click the entity and choose:

* DNS Transforms: to find A, MX, NS records
* WHOIS: get domain owner details
* Social Network Lookup
* Email Address Relationships
* IP Address info
* Pastebin leaks or breach data

**Step 3: Expand Network**

* Keep adding related entities
* Look for connections like:
  + Common email or phone numbers
  + Shared infrastructure (e.g. same IP for multiple domains)
  + Compromised assets

**Step 4: Analyze the Graph**

* Spot **central nodes** (e.g. reused email or common IP)
* See how entities are connected
* Identify attacker or target infrastructure

**Step 5: Report Your Findings**

Export:

* Screenshots of your graph
* CSV or Maltego case file (.mtgl)
* Notes explaining your path

**🧪 What You Might Explore**

| **Scenario** | **Goal** |
| --- | --- |
| Breach Investigation | Track email to domain to other leaks |
| APT Infrastructure | Link command-and-control (C2) domains/IPs |
| Fake Profiles | Map social connections of fake identity |
| Corporate Espionage | Link employees to leaked credentials or fake sites |

**🔐 Tips for Challenge Labs**

* Always **label your entities** clearly
* Don’t run too many transforms at once (it slows down or crashes)
* Use the **Casefile** mode for offline work
* Don’t trust all transforms blindly — some give outdated results
* Use **filters** to reduce noise and highlight valuable links

**🧠 Why Is Maltego Important?**

| **Reason** | **Benefit** |
| --- | --- |
| Visual OSINT | Easier to see hidden connections |
| Powerful integrations | Shodan, HaveIBeenPwned, Threat Intel, etc. |
| Threat hunting & IR | Spot threat actor infrastructure faster |
| Social engineering | Build real-world identity maps |
| Law enforcement use | Maltego is used globally in investigations |