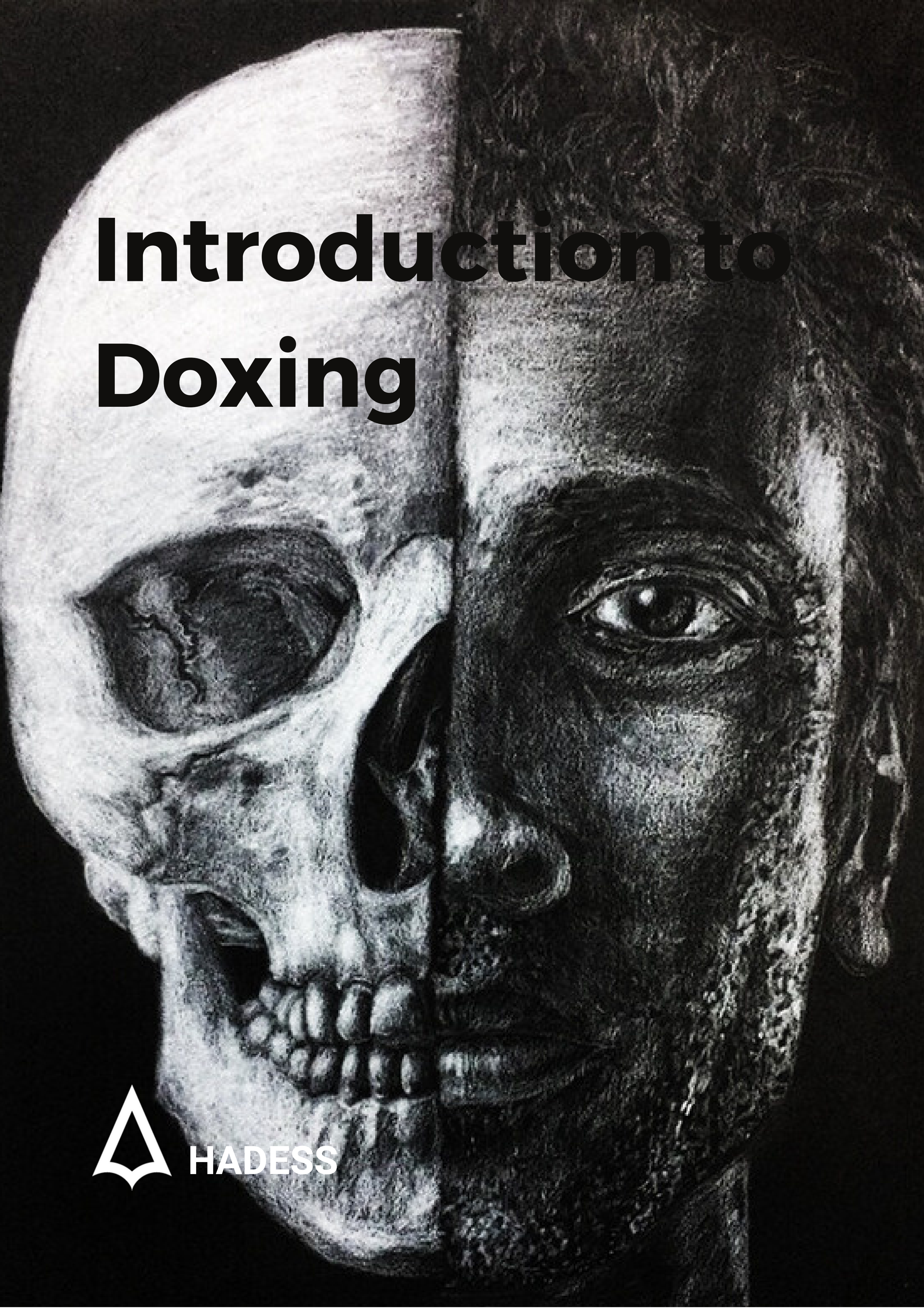
# Introduction to Doxing



HADESS

# FOREWARD

This document  is about Osint methods for information gathering with example person which made by hadess cybersecurity company.
All of these data comes from various origins such as: website, social media and leaks.

# EXECUTIVE SUMMARY

OSINT stands for Open Source Intelligence, it's the OSINT full form, and is one of the key aspects in understanding the cybersecurity that rules the Internet these days.

OSINT examples include:

- Asking questions on any search engine.
- Research public forums on how to fix your computer.
- Watch a youtube video on how to make a birthday cake.

Doxing (also seen as 'doxxing'), an abbreviation for "Dropping Documents", is a type of cyberattack where the attacker steals the victim's personal information and leaks it onto the internet.

- Real name / last name
- Email address
- Phone number
- Social media profiles
- Address or location
- Employer
- Bank account or credit card information

# Table of Contents

# OSINT

OSINT stands for Open Source Intelligence, it's the OSINT full form, and is one of the key aspects in understanding the cybersecurity that rules the Internet these days.

The term OSINT comes from many decades ago, in fact, US military agencies started using the term OSINT in the late 1980's as they were re-evaluating the nature of information requirements in tactical levels under battlefields. Then in 1992, the Intelligence Reorganization Act determined the main goals of intel gathering included key concepts like:

- Must be objective intelligence free of bias
- Data must be available on public and non-public sources

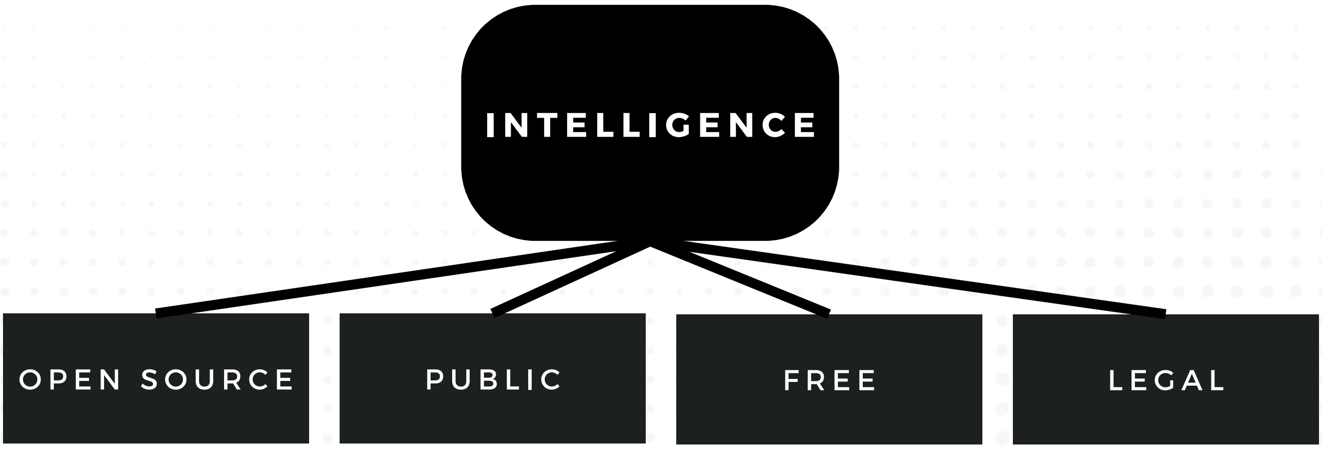
While the concept of OSINT has evolved since then, as it does not include the non-public sources, the concept originates from that time.

Open source intelligence (OSINT) is information collected from public sources such as those available on the Internet, although the term isn't strictly limited to the internet, but rather means all publicly available sources.

"OS" (from OSINT) means Open Source. In this case, it is not related to the famous open source movement, but to any publicly available source where the user can obtain the information in their intelligence data collection.

The key word behind OSINT concept is information, and most importantly, information that can be obtained for free. It doesn't matter if it is located inside newspapers, blogs, web pages, tweets, social media cards, images, podcasts, or videos as long as it is public, free and legal.

With the right information in your hands, you can get a great advantage over your competition, or speed up any company/people investigation you are in charge of.



INTELLIGENCE

OPEN SOURCE

PUBLIC

FREE

LEGAL

# OSINT Examples

With the right information in your hands, you can get a great advantage over your competition, or speed up any company/people investigation you are in charge of.

But OSINT is even simpler, you know; many of us associate OSINT to cyber war, cyber attacks, cybersecurity, etc. And while those things are a part of it, OSINT is much more explicit and uncomplicated.

OSINT examples include:

- Asking questions on any search engine.
- Research public forums on how to fix your computer.
- Watch a youtube video on how to make a birthday cake.

As you see, you don't need to be a hacker to use OSINT in your daily life: you're already using it, you just might have not known it.

However, since we are focused on modern OSINT for the cybersecurity fields, we will now take a look at how your company or project can benefit from it.

## Active Osint

- Direct contact with the target
- More reliable results
- High risk of detection
- Example: port scanning

## Passive Osint

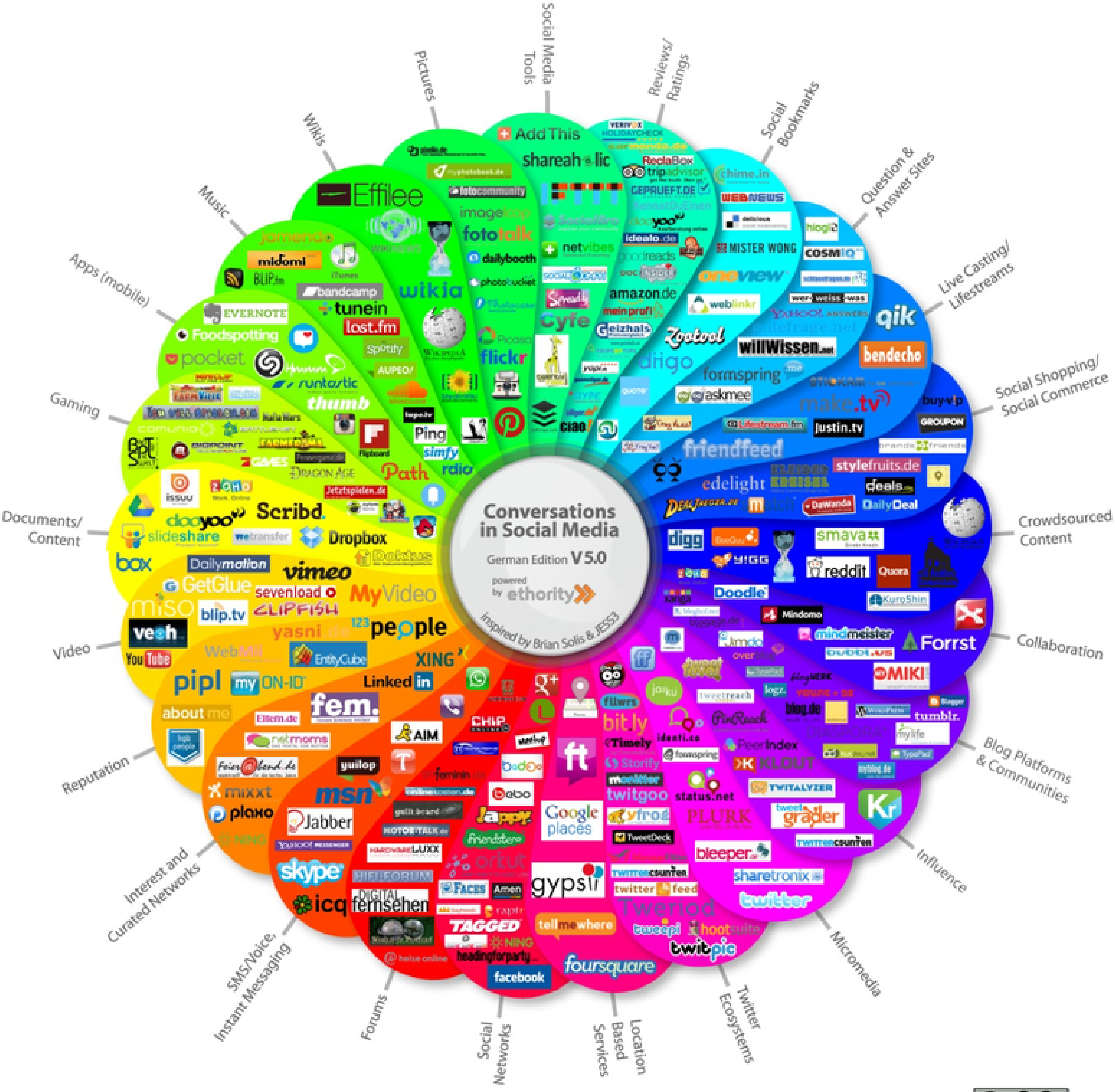
- Contact based on third-party services
- May include false positives and noise
- Low risk of detection
- Example: Security APIs

# OSINT Examples

Let's take a look into the most popular OSINT techniques used in cybersecurity:

| No | Methods |
|---|---|
| 1 | Collect employee full names, job roles, as well as the software they use. |
| 2 | Review and monitor search engine information from Google, Bing, Yahoo, and others. |
| 3 | Monitoring personal and corporate blogs, as well as review user activity on digital forums. |
| 4 | Identify all social networks used by the target user or company. |
| 5 | Review content available on social networks like Facebook, Twitter, Google Plus, or Linkedin. |
| 6 | Access old cached data from Google – often reveals interesting information. |
| 7 | Identify mobile phone numbers, as well as mail addresses from social networks, or Google results. |
| 8 | Search for photographs and videos on common social photo sharing sites, such as Flickr, Google Photos, etc. |
| 9 | Use Google Maps and other open satellite imagery sources to retrieve images of users' geographic location. |
| 10 | Never forget about the all-powerful OSINT Framework by Justin Nordine, which can be a great source of inspiration for any OSINT investigation |

# OSINT Examples



Conversations in Social Media – Version 5.0 – 09.2012 by ethority | http://social-media-prisma.ethority.de | http://www.twitter.com/ethority | Contact us for updates: prisma@ethority.de

# What is Doxing?

Doxing (also seen as ‘doxxing’), an abbreviation for “Dropping Documents”, is a type of cyberattack where the attacker steals the victim’s personal information and leaks it onto the internet.

Usually, the goal of doxing is to harass or shun the victim in some way.

And unfortunately, doxing is more common than you’d think. All sorts of people get doxed. It doesn’t matter whether you’re a celebrity or just an Average Joe.

In order to avoid doxing, it’s very important to be careful with the type of information you put up on the internet.

What Information Do Hackers Need for Doxing?

Doxing (also seen as ‘doxxing’), an abbreviation for “Dropping Documents”, is a type of cyberattack where the attacker steals the victim’s personal information and leaks it onto the internet.

For a doxing attack, hackers usually look for information such as:

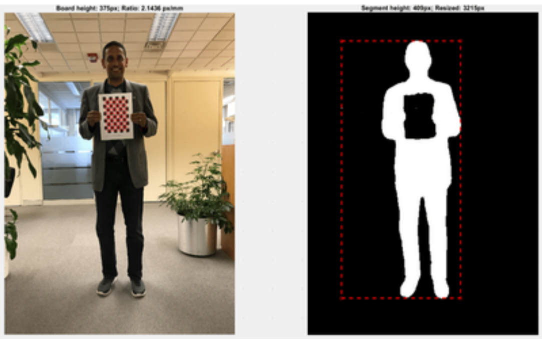
- Real name / last name
- Email address
- Phone number
- Social media profiles
- Address or location
- Employer
- Bank account or credit card information

# Reza Golzar Doxing for fun and ~~profit~~

THIS DOCUMENT IS MEANT TO BE USED FOR EDUCATIONAL PURPOSES ONLY.

# Reza Golzar Doxing

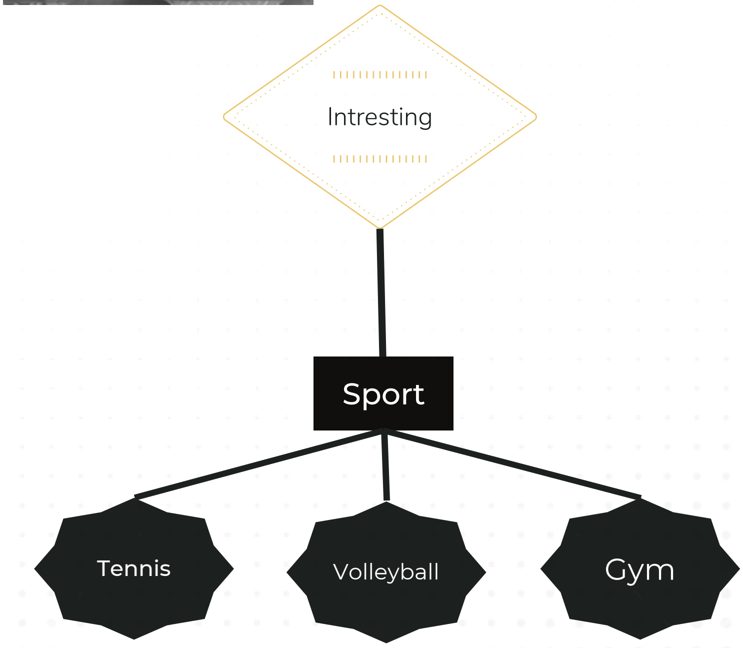
- Find name & family with google image reverse search:
- https://images.google.com/
- Name & Family: Mohammad Reza Golzar
- Find Weight & Height & Age with AI:


Board height: 375px; Ratio: 2.1436 px/mm
Segment height: 409px; Resized: 321px

- Weight: 84Kg-87Kg
- Height: 5' 10" (1.77 m)
- Birthday: March 21, 1977

# Reza Golzar Doxing

● Interesting Sport



●

Intresting

Sport

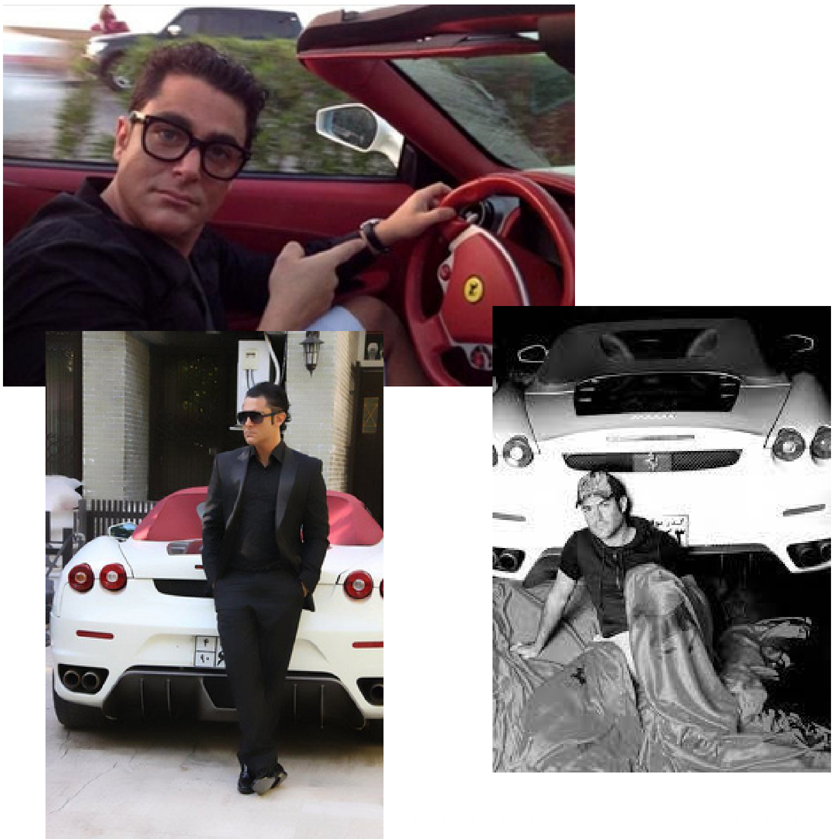
Tennis

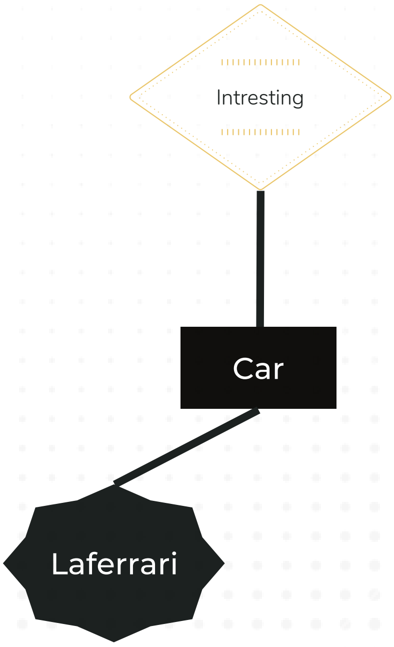
Volleyball

Gym

# Reza Golzar Doxing

- Interesting Car



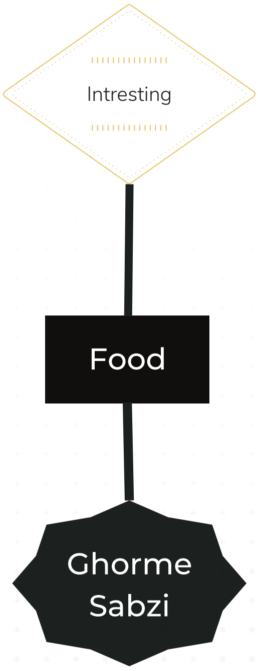


Intresting

Car

Laferrari

● Interesting Food



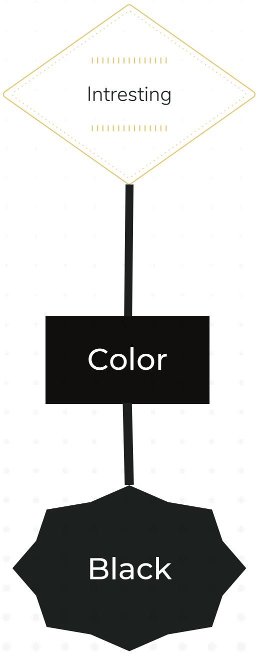
Intresting

Food

Ghorme Sabzi

# Reza Golzar Doxing

- Interesting Color

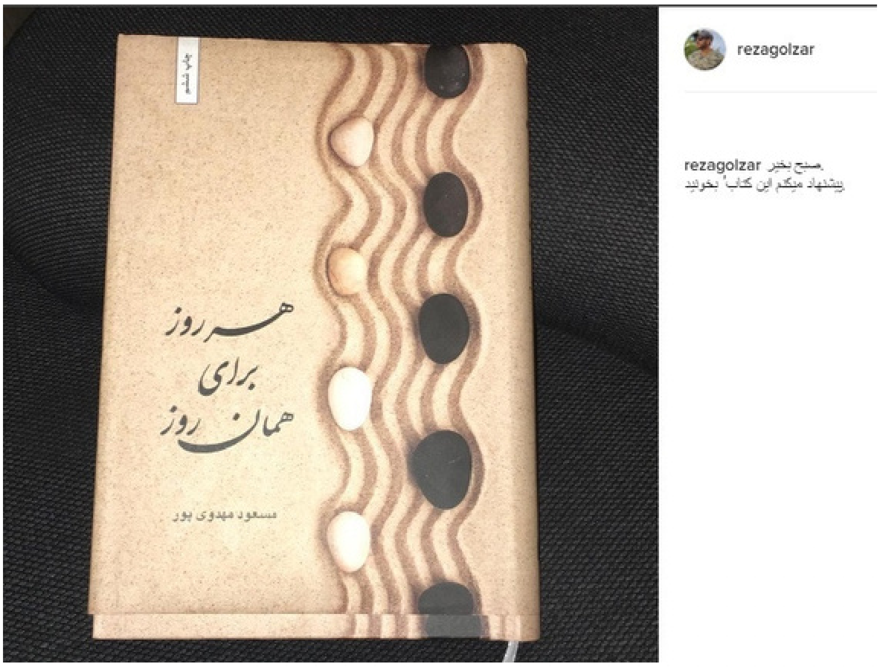


Intresting

Color

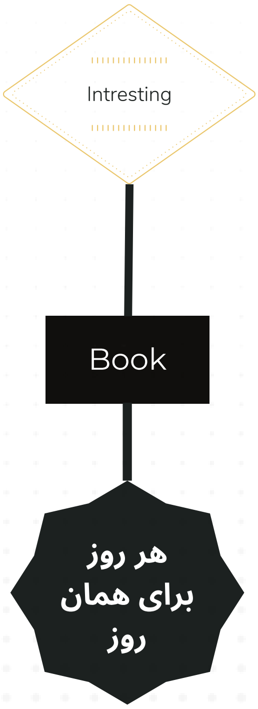
Black

● Interesting Book



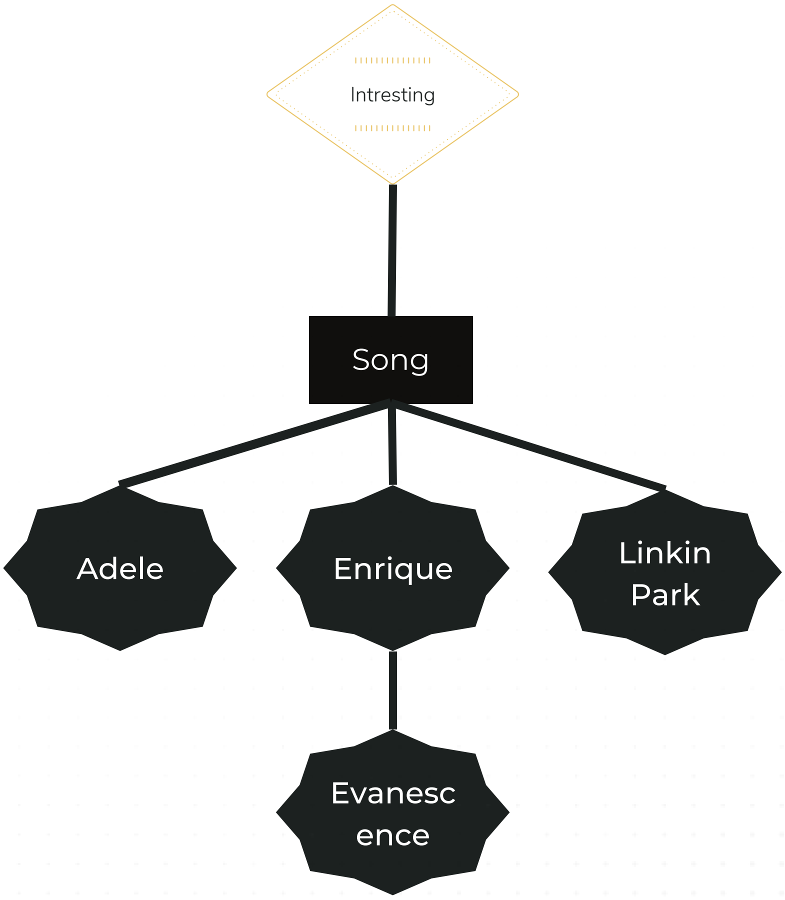
rezagolzar

rezagolzar صبح بخیر.
پیشنهاد میکنم این کتاب' بخوانید



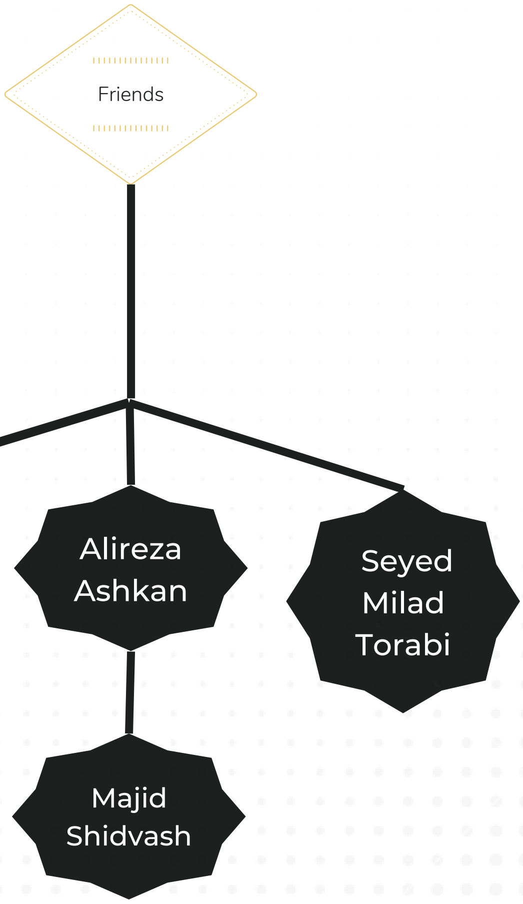
# Reza Golzar Doxing

- 🔴 Interesting Song
- Find Similar Song with AI
- spotalike.com
- https://melobytes.com/en/app/ai_image2song
- 🟢 Enrique, Adele, Linkin Park, Evanescence



# Reza Golzar Doxing

Some Friends



Friends

Mahdi Hejrati

Alireza Ashkan

Seyed Milad Torabi

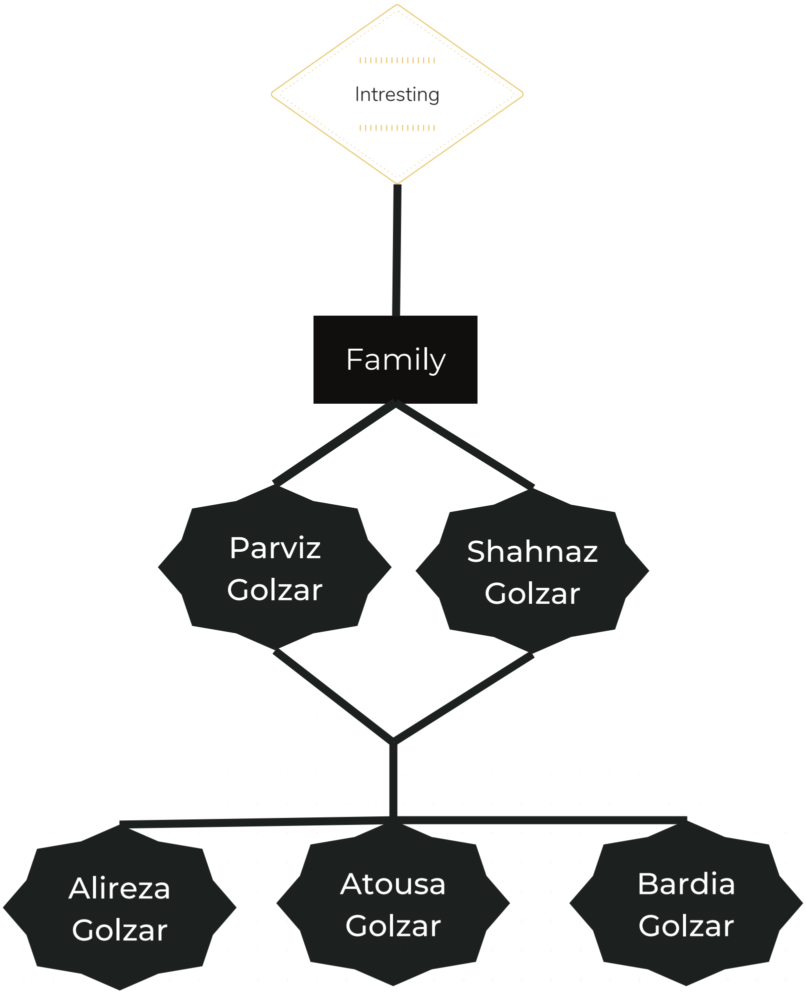
Majid Shidvash

# Reza Golzar Doxing

- Family

Wiki & familysearch

-

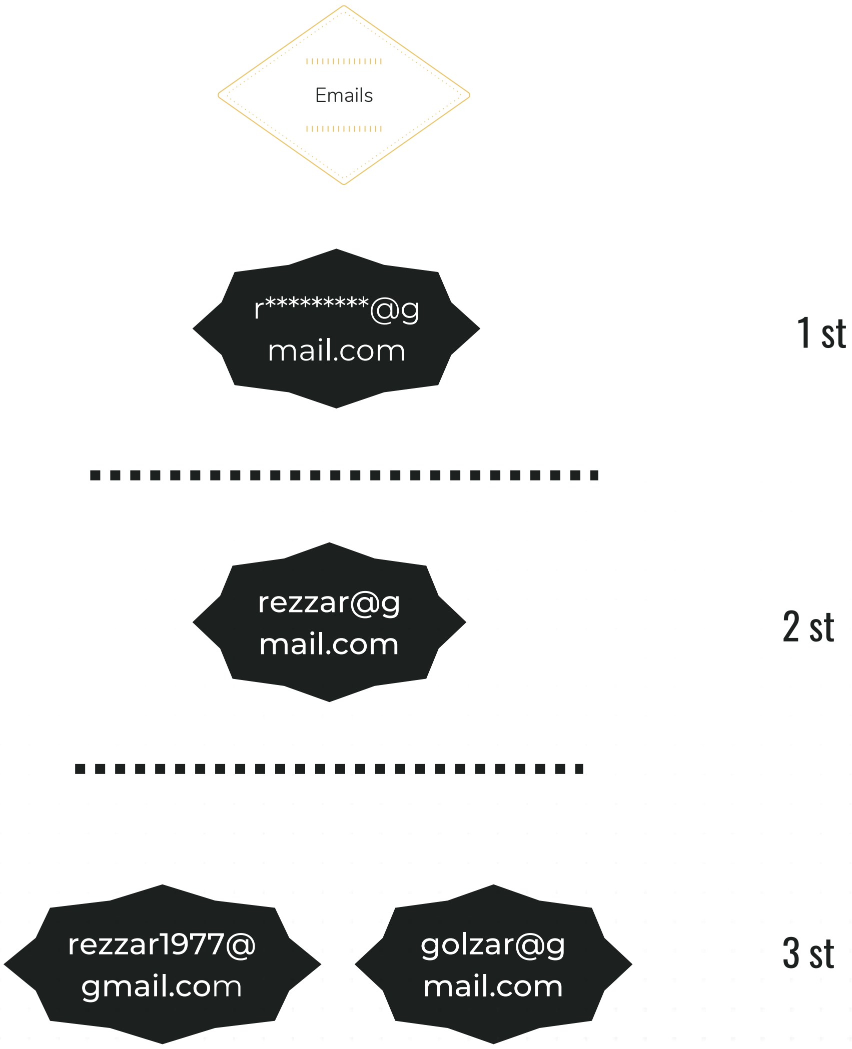


# Reza Golzar Doxing

● Emails

Domain Whoise & Leaks & Wayback

●



Emails

r*********@gmail.com

1 st

rezzar@gmail.com

2 st

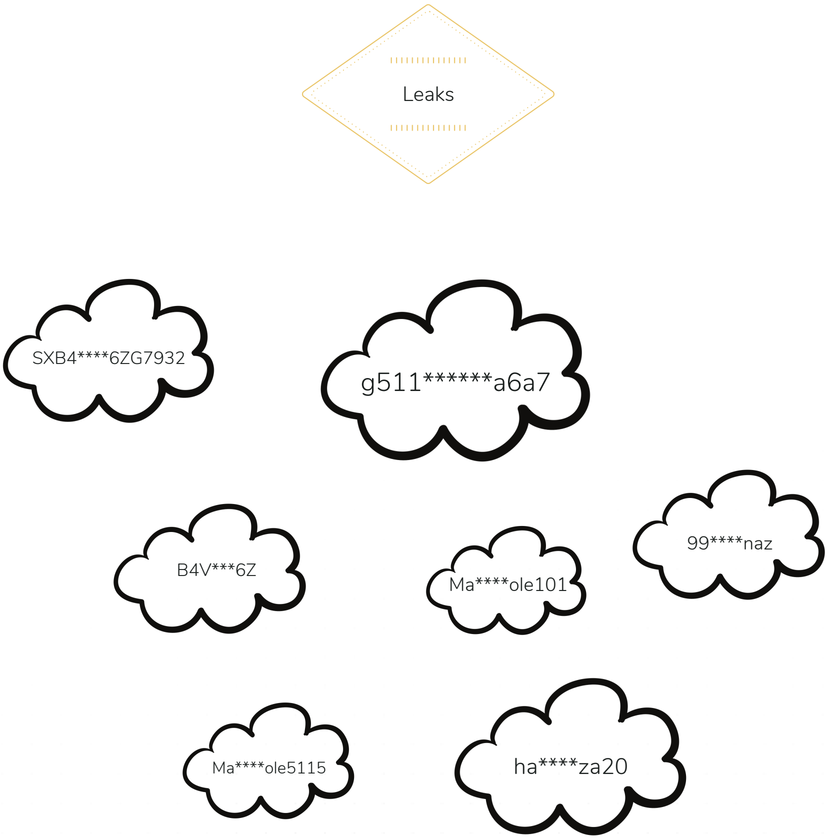
rezzar1977@gmail.com

golzar@gmail.com

3 st

# Reza Golzar Doxing

- Passwords
- Leaks



Leaks

SXB4****6ZG7932

g511*******a6a7

B4V***6Z

Ma****ole101

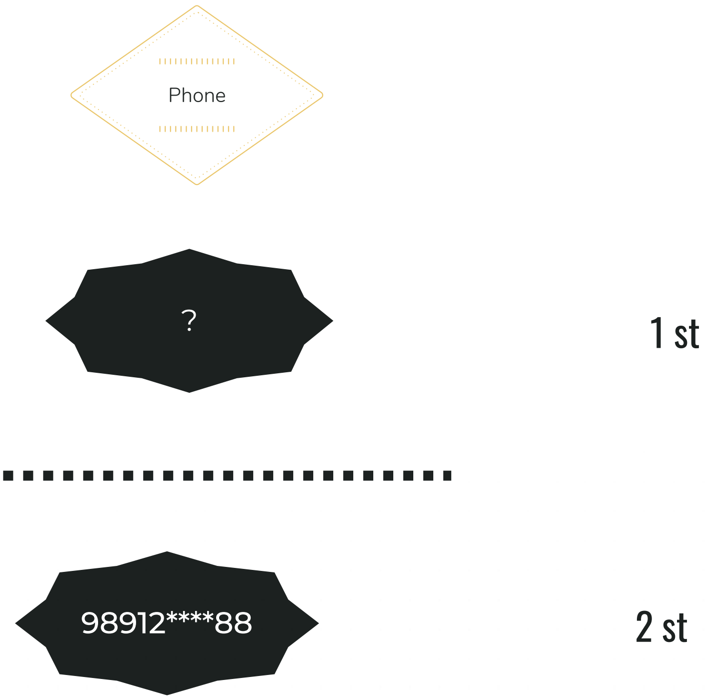
99****naz

Ma****ole5115

ha****za20

# Reza Golzar Doxing

- 🟥 Phone
- Domain Whoise & Leaks & Wayback
- 🟩



Phone

?

1 st

98912****88

2 st

# Reza Golzar Doxing

● Card

Leaks & Wayback

●

Card

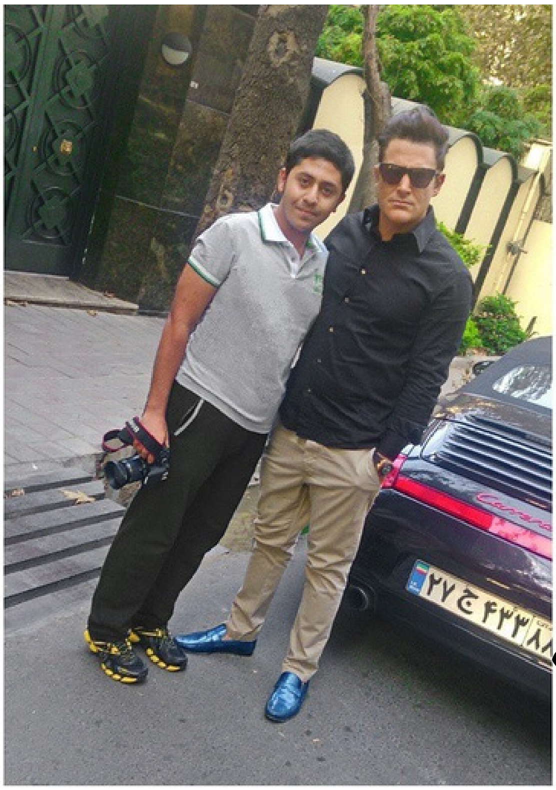
6104********9074

1 st

# Reza Golzar Doxing

- Cars
- Images with AI
-

Cars

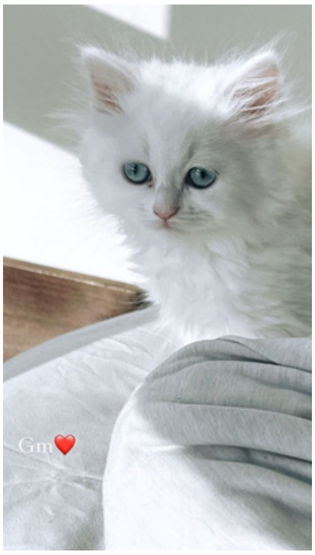


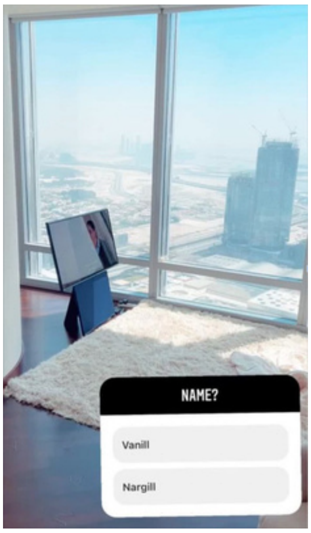
۲۷ ج ۴۳۳ ایران ۸۸

# Reza Golzar Doxing

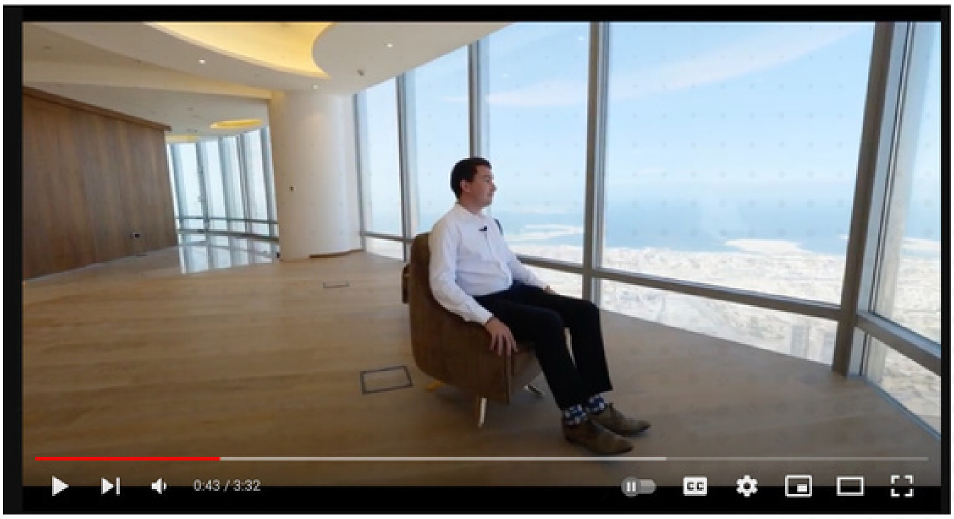
- 🔴 Home(s)
- Images Location with Geo
- 🟢

Home(s)





The Corporate Suites at Burj Khalifa



# Resources

- securitytrails.com

# Hadess
# Products and Services

→ ## ThirdEye | Attack Surface Intelligence

Find your company leakage and monitor attack vector.

→ ## Red Teaming Operation | PROTECTION PRO

Fully assess your organization’s threat detection and response capabilities with a simulated cyber-attack.

# About **Hadess**

Savior of your Business to combat cyber threats
Hadess performs offensive cybersecurity services through infrastructures and software that include vulnerability analysis, scenario attack planning, and implementation of custom integrated preventive projects. We organized our activities around the prevention of corporate, industrial, and laboratory cyber threats.

## Contact Us

To request additional information about Hadess's services, please fill out the form below. A Hadess representative will contact you shortly.

**Website:**

www.hadess.io

**Email:**

Marketing@hadess.io

**Phone No.**

+989362181112

**Company No.**

982128427515

hadess_security

HADESS

www.hadess.io