OSINT Case Study: Anonymized Example

Case Summary:

This report demonstrates a simulated OSINT (Open Source Intelligence) operation for educational purposes. All identifying data has been anonymized.

Objective:

To showcase how basic OSINT techniques using publicly available tools can identify general information about a device, location, and user activity.

Methodology:

1. A shortened URL was created using a tracking service (e.g., Grabify).

2. The link was shared with a consenting friend.

3. Upon clicking, metadata was captured including IP address, device type, browser info, and ISP.

4. IP geolocation tools were used to determine an approximate city location.

5. Public map services (e.g., Google Maps) were used to explore surrounding geography.

6. No personally identifiable information (PII) was collected, retained, or shared.

Findings (Anonymized):

- Device: Android 7.0, Samsung Galaxy Device

- Browser: Chrome Mobile, via Instagram in-app browser

- IP Address: 49.xxx.xxx.xxx (anonymized)

- Approximate Location: City Z, Country Y

- ISP: Major Telecom Provider

- GPS Coordinates: Lat 30.xxxx, Long 78.xxxx (approx. 2km radius)

OSINT Case Study: Anonymized Example

Ethical Considerations:

[OK] Consent obtained prior to the test

[OK] All data anonymized post-capture

[OK] No data shared outside this educational context

[OK] Target individual was informed after test and offered digital privacy tips

Conclusion:

This exercise highlights how trivially accessible tools can produce significant insights. It's a reminder to be mindful of link tracking, app permissions, and VPN usage.

DISCLAIMER: This report is strictly for educational use. Do not replicate without informed consent and ethical guidelines.

Generated on: 2025-07-11 18:31:54