MIT World Peace University

Vulnerability Identification and Penetration Testing
Third Year B. Tech, Semester 6

CSI: Cyber Crime Investigation Manual

Manual Version 1

Prepared By

Parth Zarekar

March 3, 2024

Contents

1 Recovery of Hacking Instagram Accounts

2 Recovery of Hacked Facebook Accounts

3 Telegram Investigation

telemetr.io can be used for Investigation related to telegram channels which were involved inn the crime. Telemetr helps give a profile of the channel including the real subscriber and the grown of the channel over periodic timeframes.

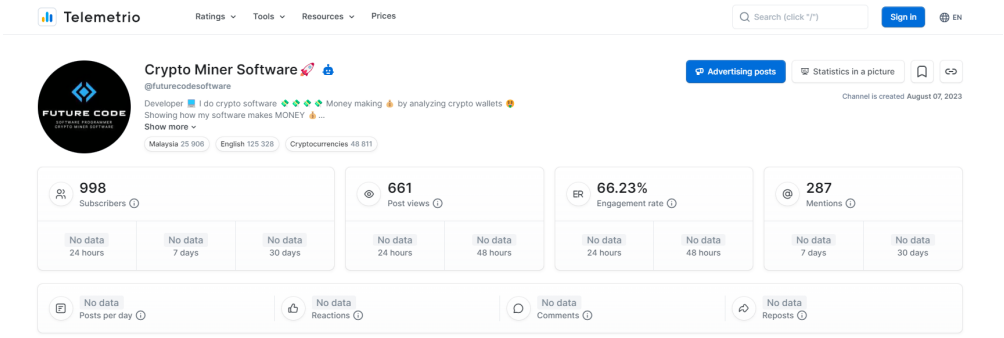

Figure 1: Telemetr.io

TOOLS url: https://telemetr.io/en

4 Investigation of Fraud Website

4.1 Website registration details investigation

A WHOIS lookup is a process used in website investigation to gather information about domain registration. This information can be used to identify the owner of the domain, the domain registrar, and the domain's registration and expiration dates. WHOIS lookups can also provide information about the domain's name servers, the domain's status, and the domain's contact information.

- **Name server:** The DNS (domain name System) servers that are authoritative for the domain
- **Status of the domain:** Whether the domain is active, expired, on hold, etc.
- **ownership Verification:** It helps verify the legitimacy of a website by confirming the details provided byt during the domain registration process.
- **Contact Information:** It provides contact details of the domain owner, which can be useful for reaching out in case of legal or technical issues.
- **Domain History:** By looking at the registration and expiration dates, you can get an idea of how long a website has been in existence.
- **Name Server information:** This can be relevant for understanding the hosting infrastructure of a website.

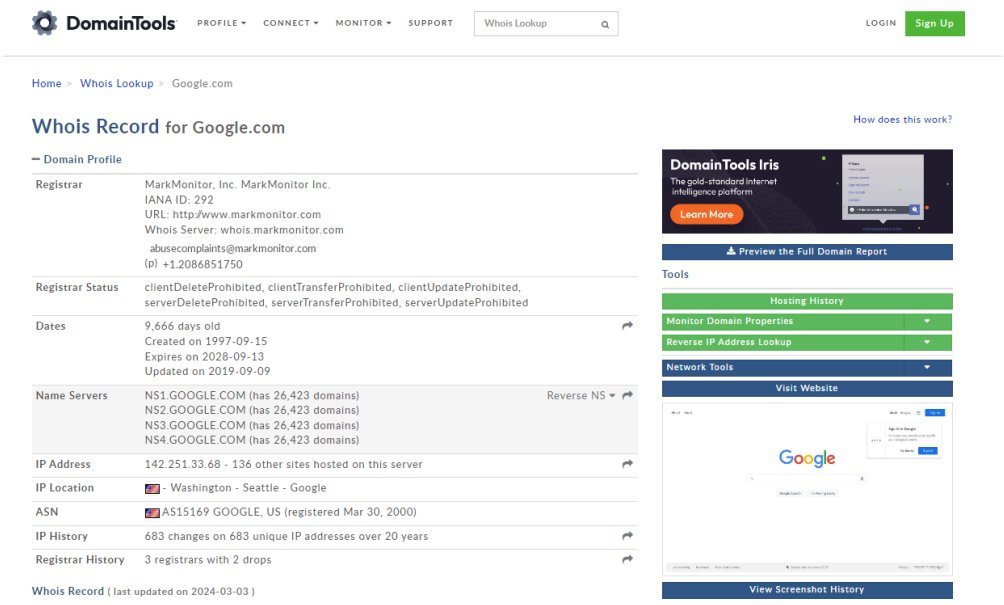

Figure 2: WHOIS Lookup

TOOLS url:

- https://whois.domaintools.com/
- https://www.whois.com/

4.2 Website History Investigation

Wayback Machine is a digital archive of the World Wide Web and other information on the Internet. It allows the user to go back in time and see what a website looked like in the past. It is a great tool for website investigation as it can help you understand the history of a website, including how it has evolved over time, what content has been added or removed, and how the website has been used by different people. Information gather from the wayback machine are:

- **Archived Versions of the Website:** The primary function of the Wayback Machine is to provide access to historical snapshots of websites. Users can enter a URL and view different version of a webpage captured at various points in time.
- **Website Changes overtime:** By navigating through different snapshots, you can observe how a website has evolved, see design changes, and track the addition or removal of content.
- **Availability Status:** You can determine if a website was accessible and archived on specific dates. This is particularly useful for Investigating the historical Availability of a site.

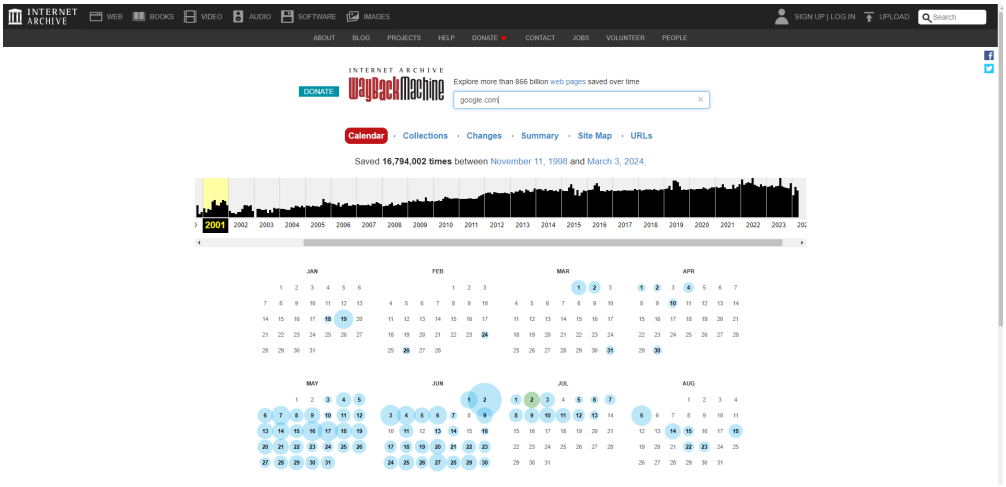

Figure 3: Wayback Machine

TOOLS url:

- https://archive.org/web/

5 Investigation For Phishing and Fraudulent websites

Scam Advisor is a Valuable online tool for Investigating the legitimacy of websites, particularly those suspected of phishing or fraudulent activities. Users can simply visit the scam Advisor website, input the URL of the website in question, and receive a comprehensive report. The report includes a scam score indicating the risk level, a trust score for evaluating reliability, and details on domain age, popularity, and ownership. Users can delve into server location, user reviews, and contact information to assess the website's credibility. Scam Advisor empowers individuals to make informed decisions about the trustworthiness of websites, contributing to a safer online environment.

5.1 Step1:

Visit the Scam Advisor website and enter the URL of the website you want to investigate. scamadvisor.com