PRACTICAL: 3

AIM:

Footprinting is the process of accumulating data regarding a specific network environment, usually for the purpose of finding ways to intrude into the environment. Footprinting can reveal system vulnerabilities and improve the ease with which they can be exploited. It is also known as reconnaissance. Study practical approach to implement Footprinting: Gathering Target Information by making use of the following tools: Recon-ng, Maltego ,OSRFramework , BillCipher , and OSINT Framework.

THEORY:

Footprinting and Reconnaissance:

Reconnaissance and footprinting are two essential processes in any security assessment .They can help a corporation develop a security posture strategy and detect potential risks.

The practise of locating and evaluating the security hazards inherent within an organisation is known as network footprinting. Similar to reconnaissance, it entails learning as much as you can about the target, including information that might not be easily accessible online. The security posture of the organisation may then be profiled using this data, and any possible weak areas can be found. In the aftermath of a hack or data breach, it may be used as proof. A business may more readily demonstrate that it followed all essential steps to safeguard its data by keeping an accurate record of its security posture.

Footprinting is a part of reconnaissance, a more thorough strategy. Reconnaissance is the stage of ethical hacking where you learn about the target system. This data may comprise everything from network architecture to employee contact information. Locating as many possible attack routes as is practicable is the goal of reconnaissance.

Recon-ng:

On GitHub, there is a free and open-source programme called recon-ng. The most fundamental and effective reconnaissance instrument, Open-Source Intelligence (OSINT), is the foundation of Recon-ng. Contextual assistance and command completion are only a couple of the useful features offered by the interactive interface.

Features-

- Recon-ng is a free and open-source utility, so you can download and use it without spending any money.
- Recon-ng is a comprehensive collection of modules for information collecting. You can use so many of its components to acquire information.
- Recon-ng functions as a website/web application scanner.
- simplest and most effective tools

Maltego:

Maltego is an open source information collecting and graphical link analysis tool for tasks related to conducting investigations. Operating systems for Windows, Macs, and Linux are all compatible with the Java application Maltego. Many different types of people utilise Maltego, such as security experts, forensic detectives, investigative journalists, and researchers. It will provide you with timely information mining, easily understandable information depiction, and information gathering.

Features-

- Information from scattered data sources can be easily gathered.
- Create a graph that automatically connects and combines all the data.
- Investigate relationships in your data visually.

OSR Framework:

The OSRFramework is the most often used method for acquiring information about an organization's target domain or employee from open-source or publicly accessible sources. This technique is mostly used by malicious hackers in attacks like phishing and social engineering. On the plus side, though, we can use this OSINT technique to comprehend the scope and become accustomed to our target area.

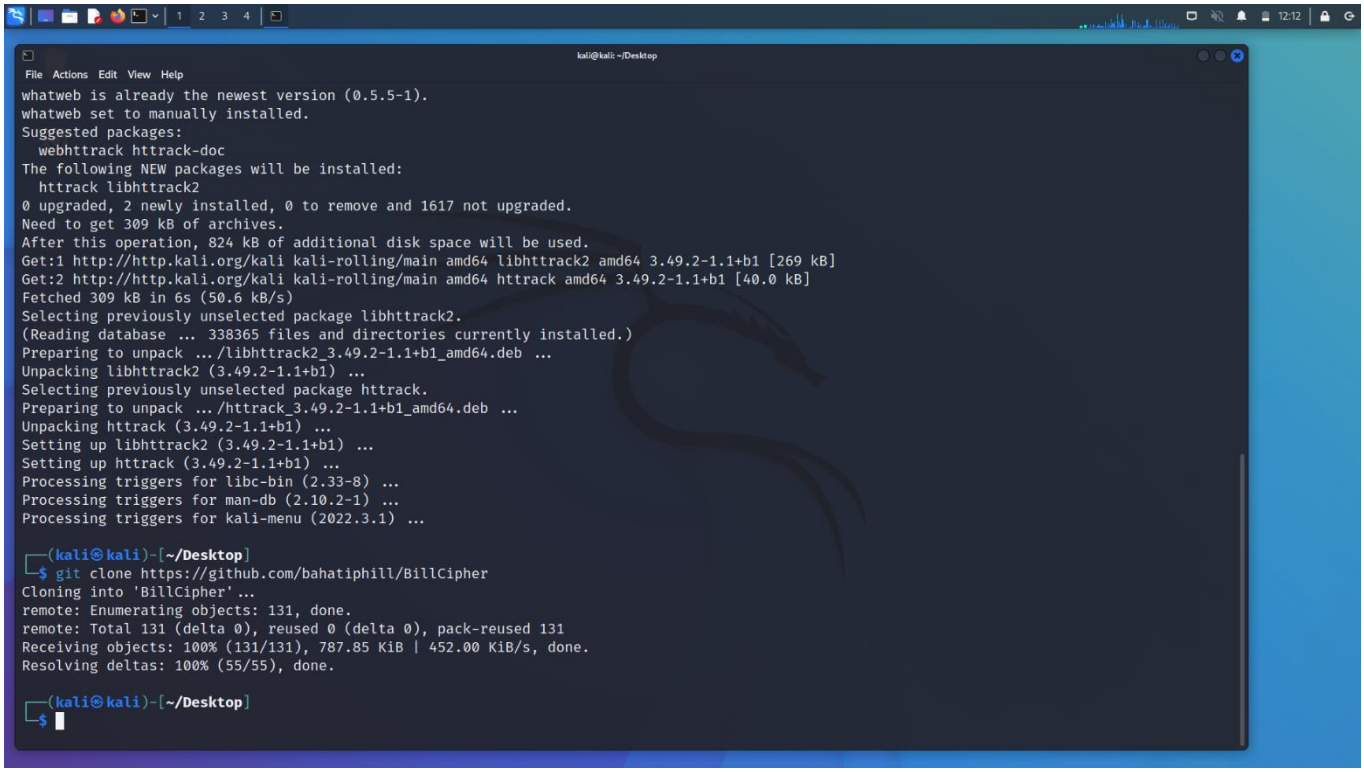
BillCipher:

The most popular technique for obtaining data from open-source or publicly available sources on a target domain or employee of a business is the OSRFramework. Malicious hackers mostly employ this tactic in social engineering and phishing assaults. On the bright side, we may utilise this OSINT method to comprehend the extent and become acquainted with our target region.

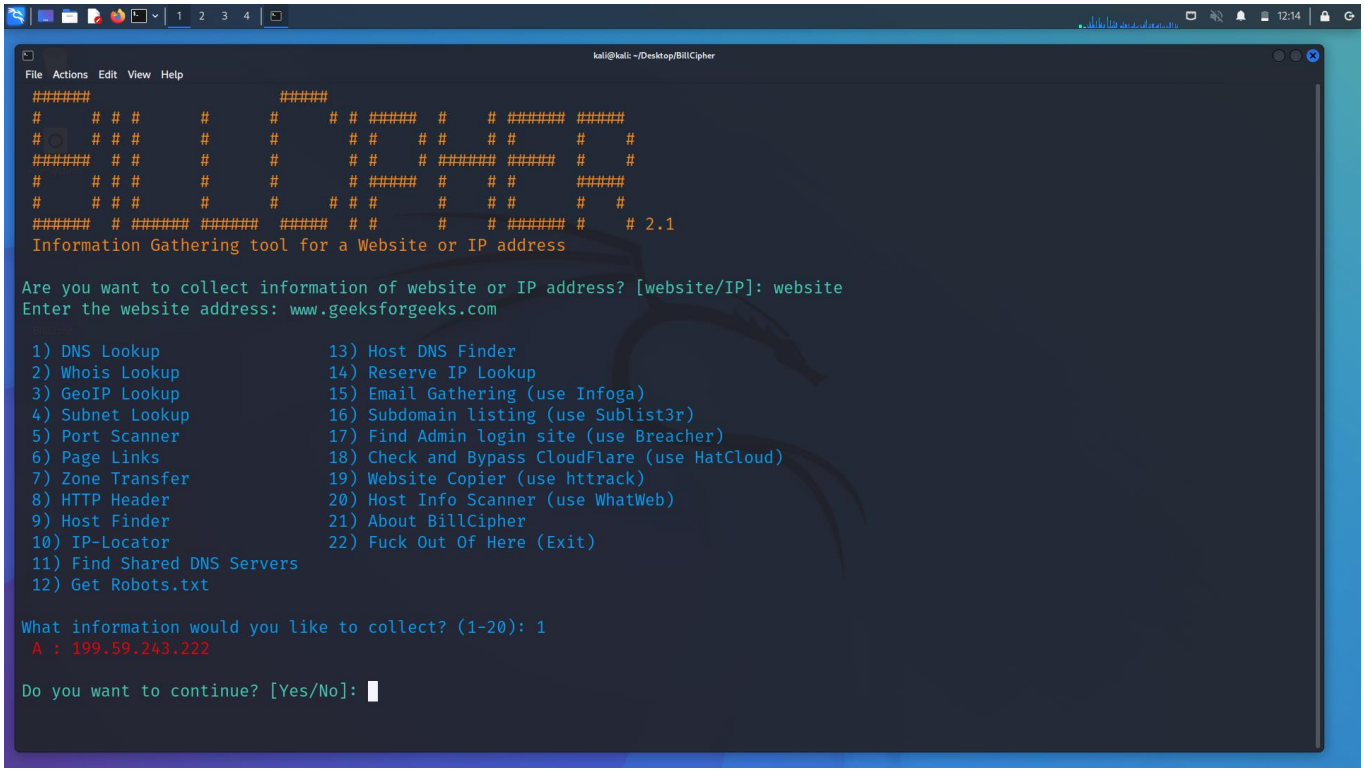
OSINT Framework:

Open-source intelligence, or OSINT, is any information about a person or organisation that has been legally gathered from unpaid, public sources. Data that may be accessible in a range of media types is also included in OSINT. Even while we typically think of information as text-based, it may also be in the form of pictures, movies, webinars, lectures, and conferences.

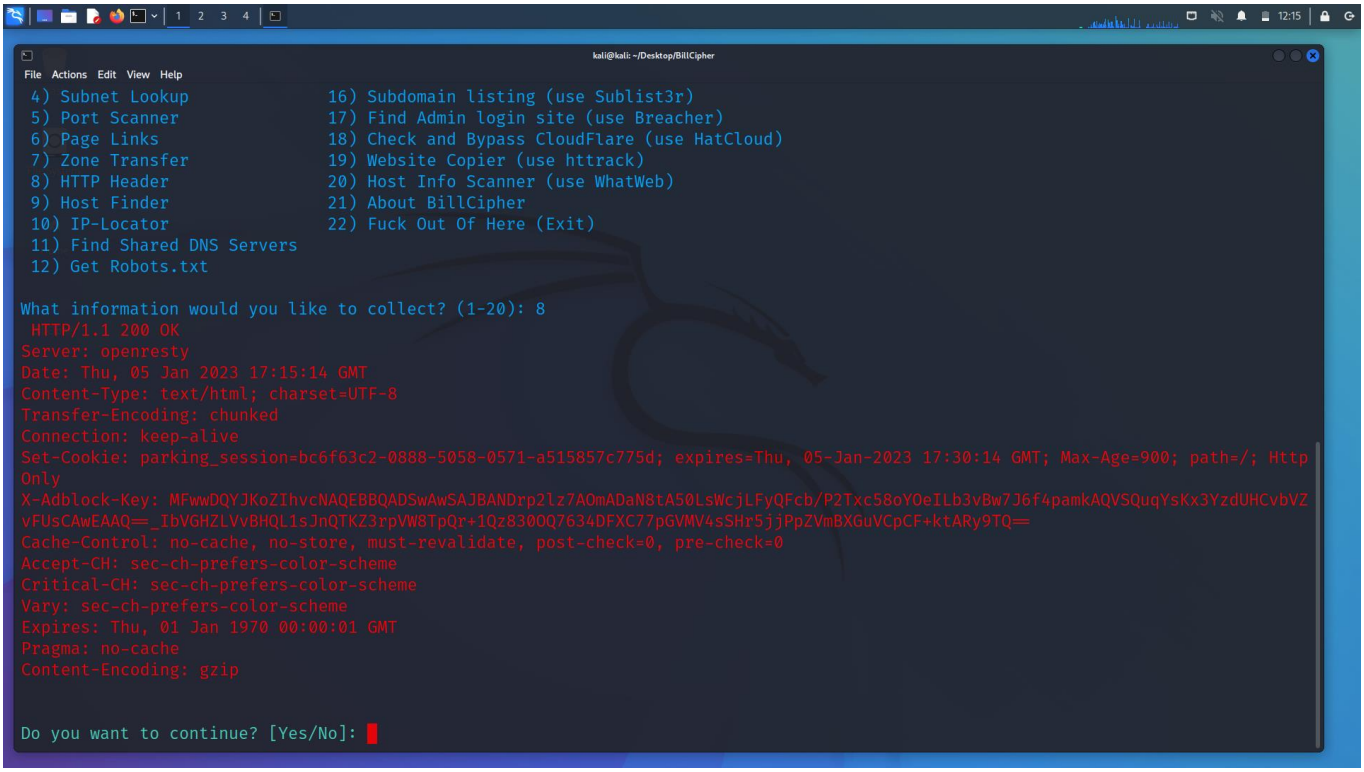
OUTPUT:



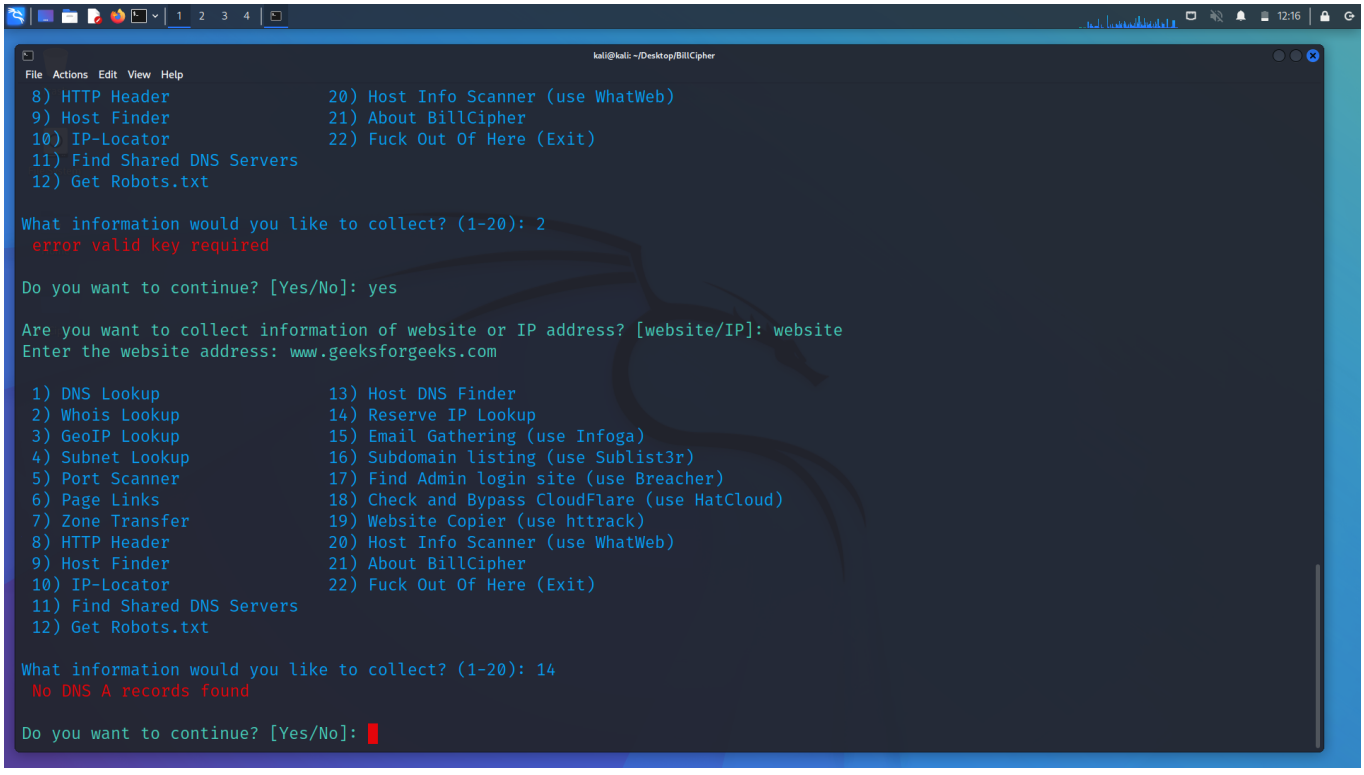
Created a file in Desktop and added dependencies and git clone



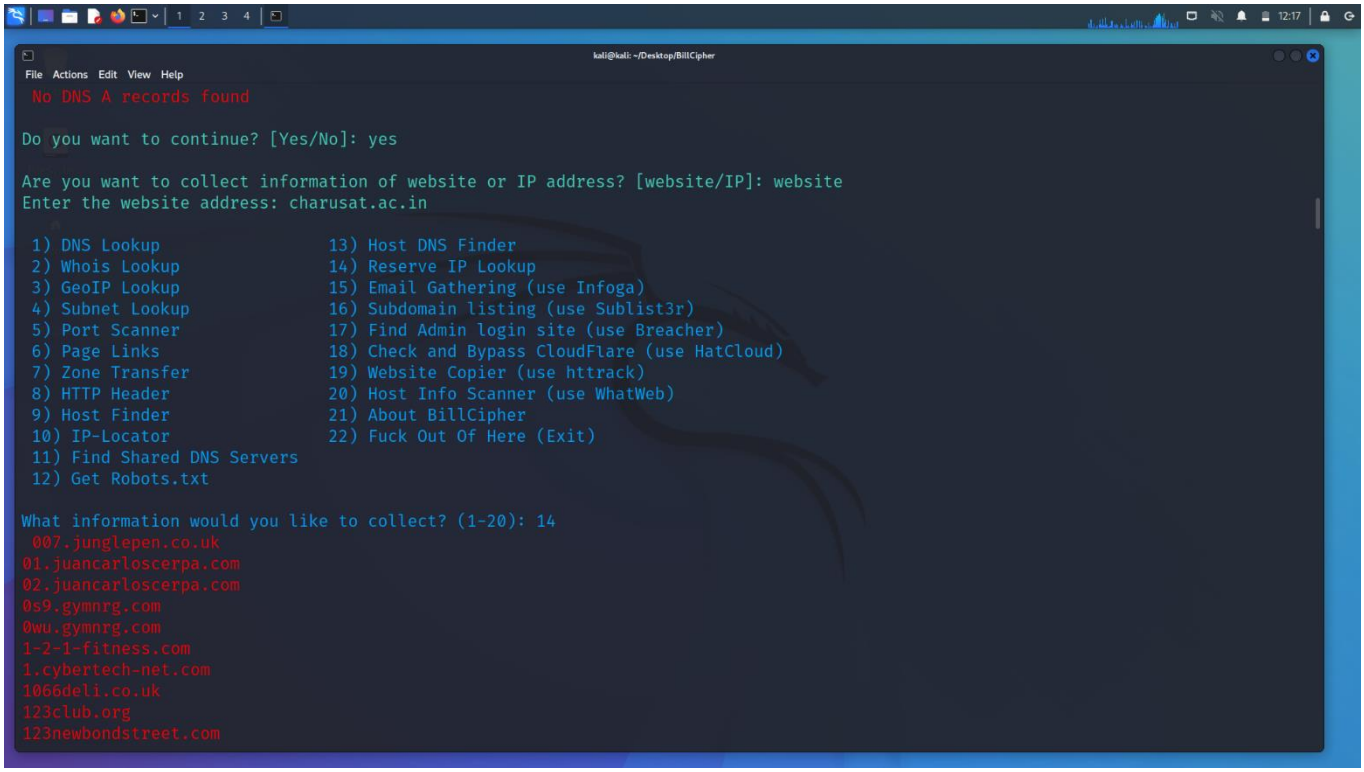
DNS lookup command for geeksforgeeks



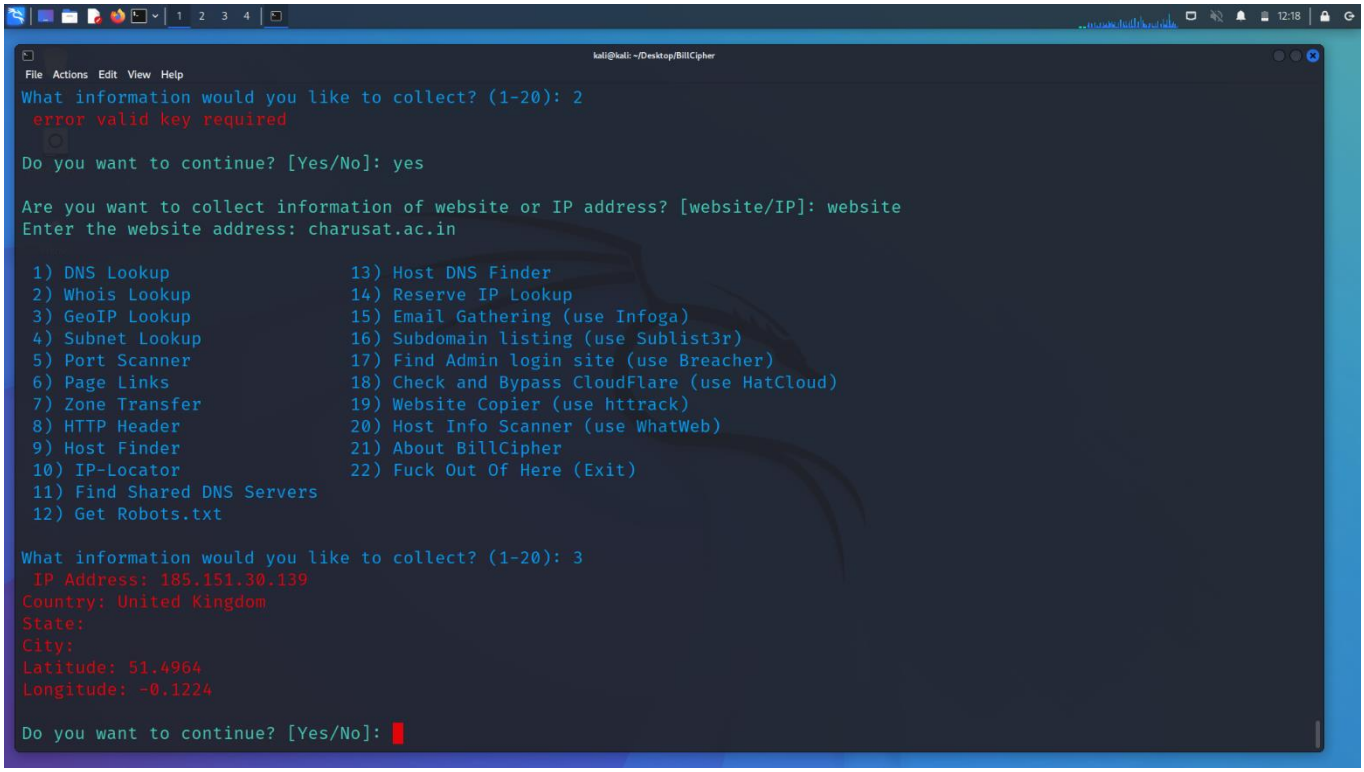
HTTP Header for geeksforgeeks



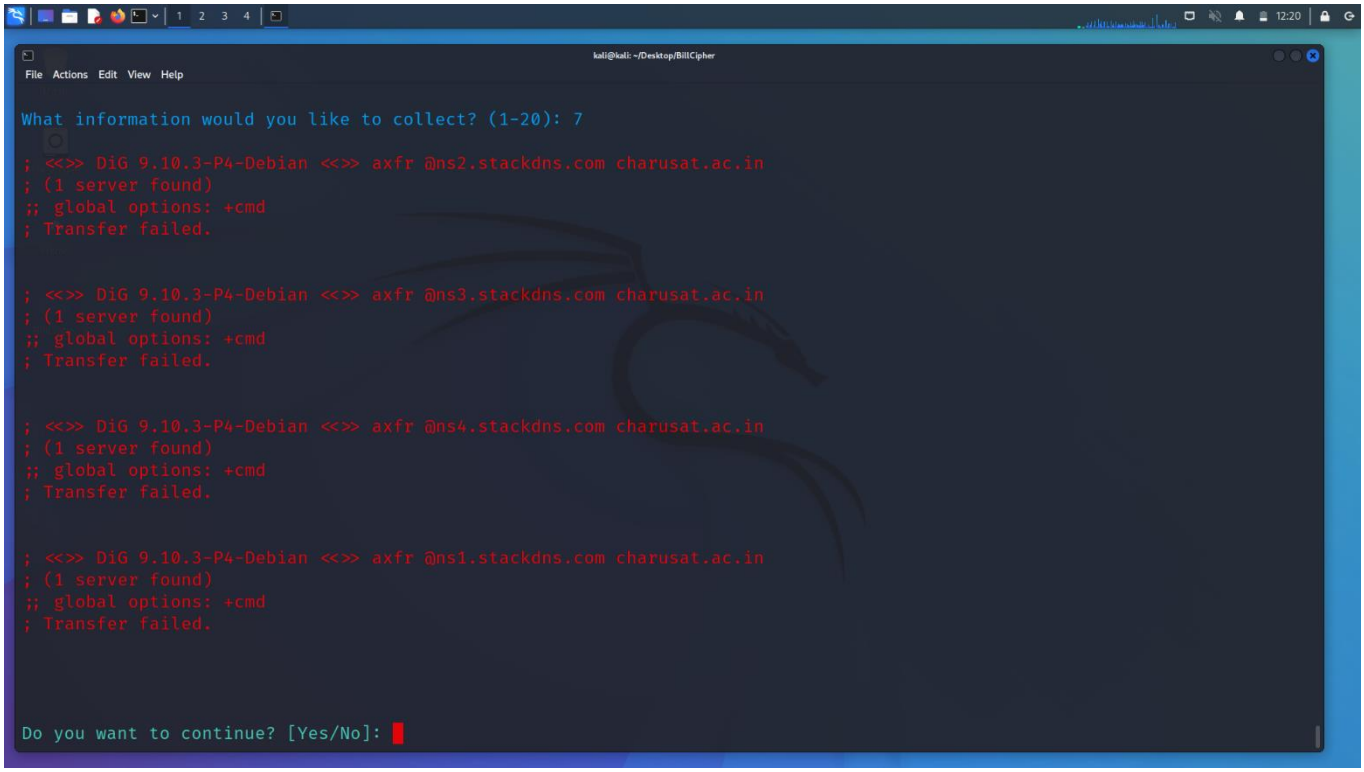
Reserve IP lookup :- no DNS found as it is secure website



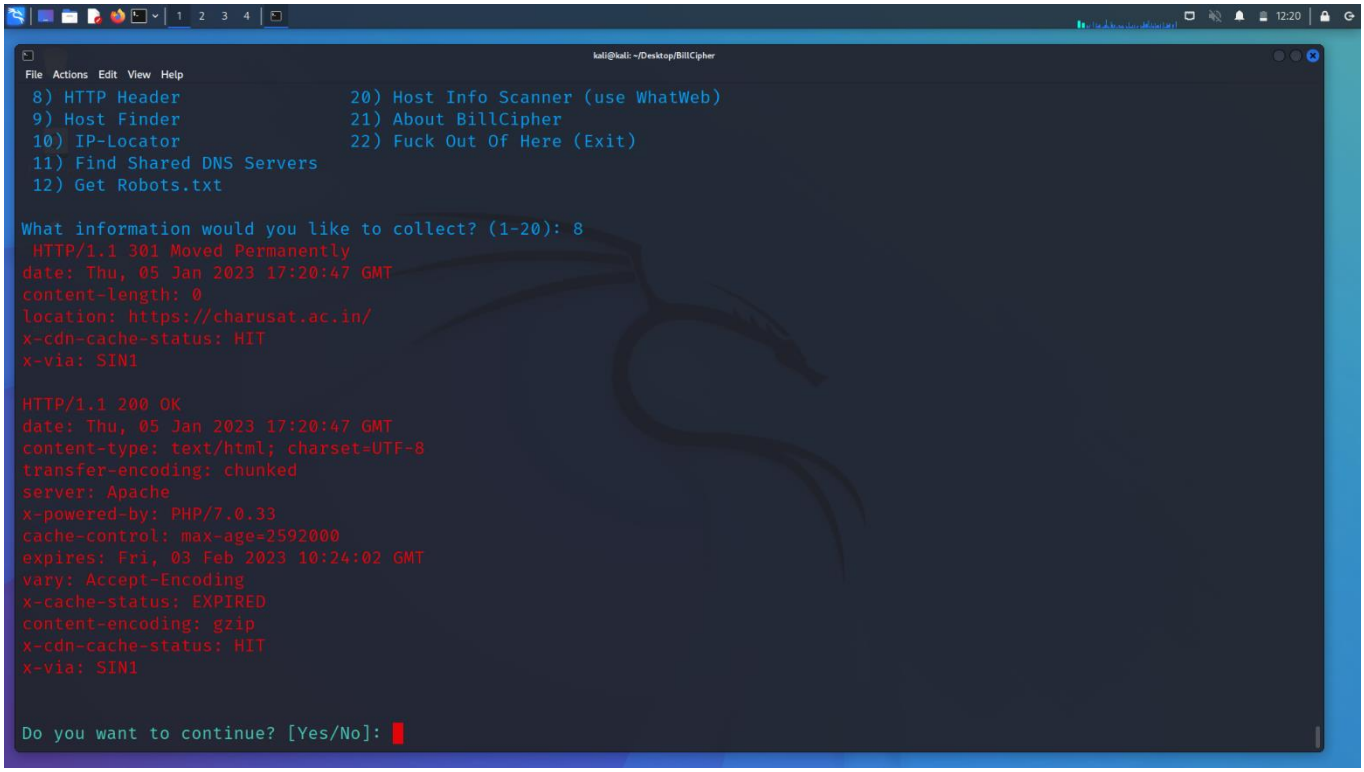
Same as above but use for charusat.ac.in



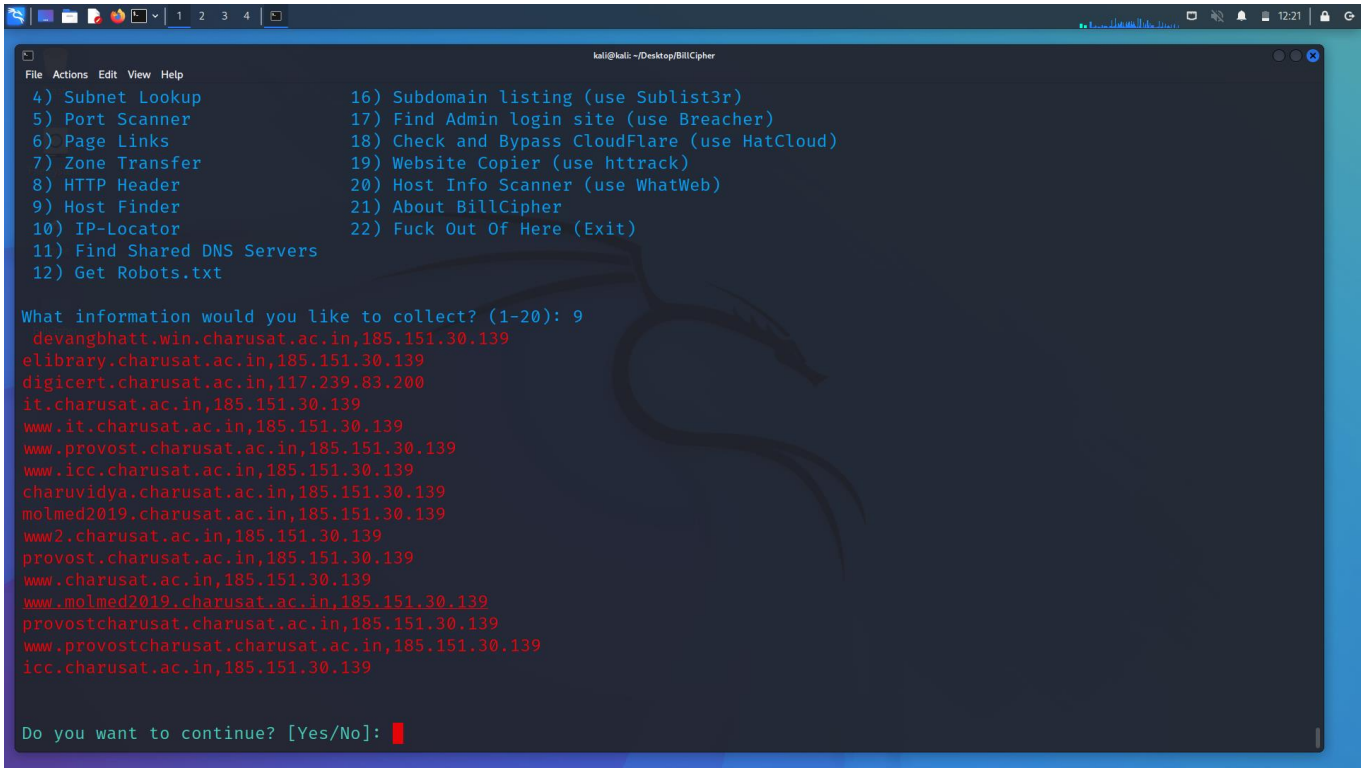
GeoIp lookup of charusat.ac.in



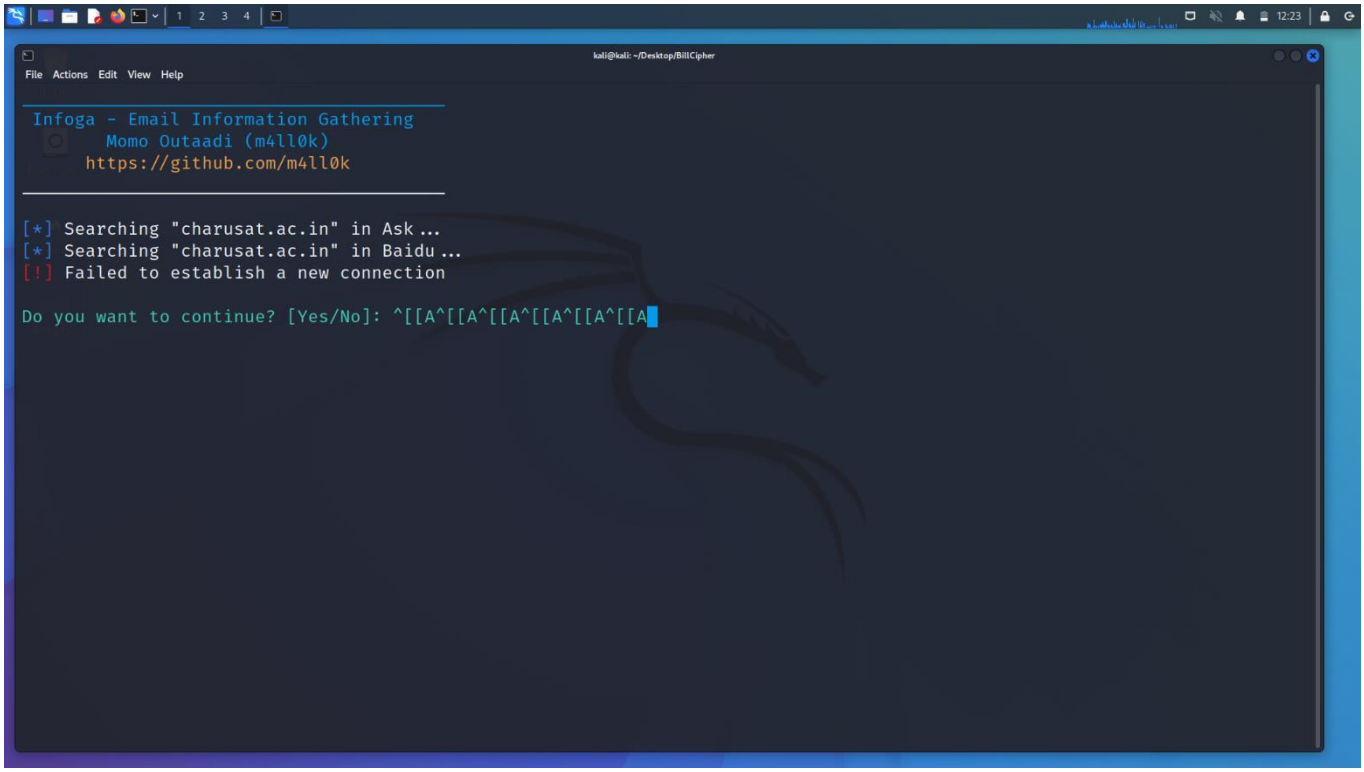
About zone transfer information



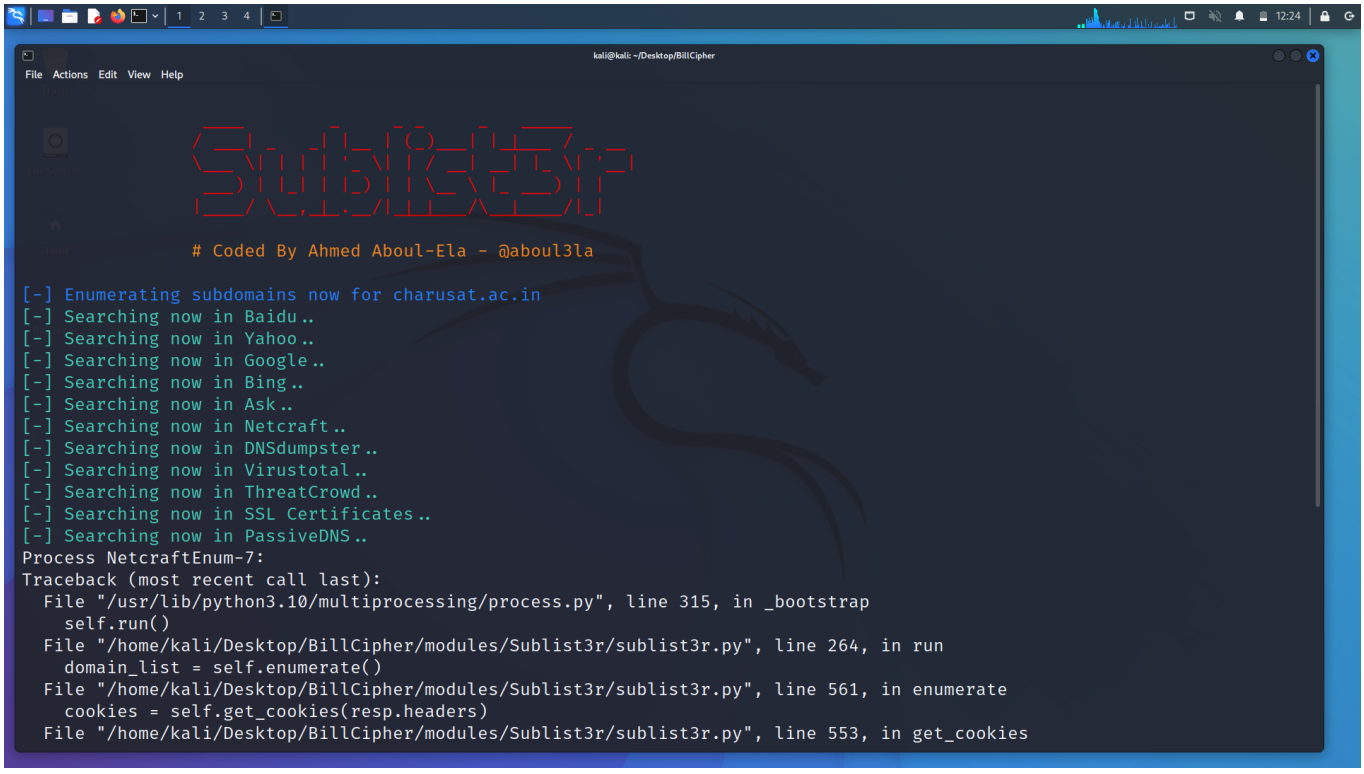
HTTP header info for charusat.ac.in



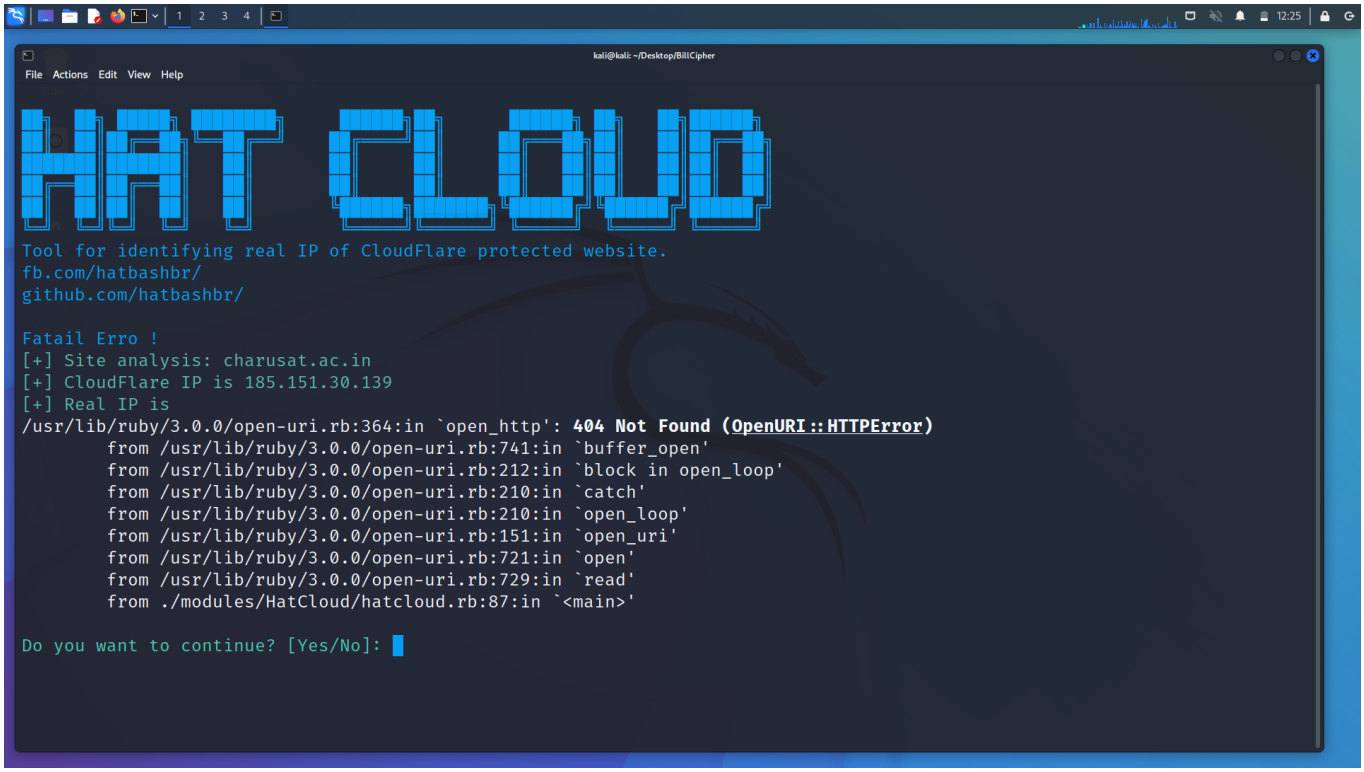
Host finder for charusat.ac.in



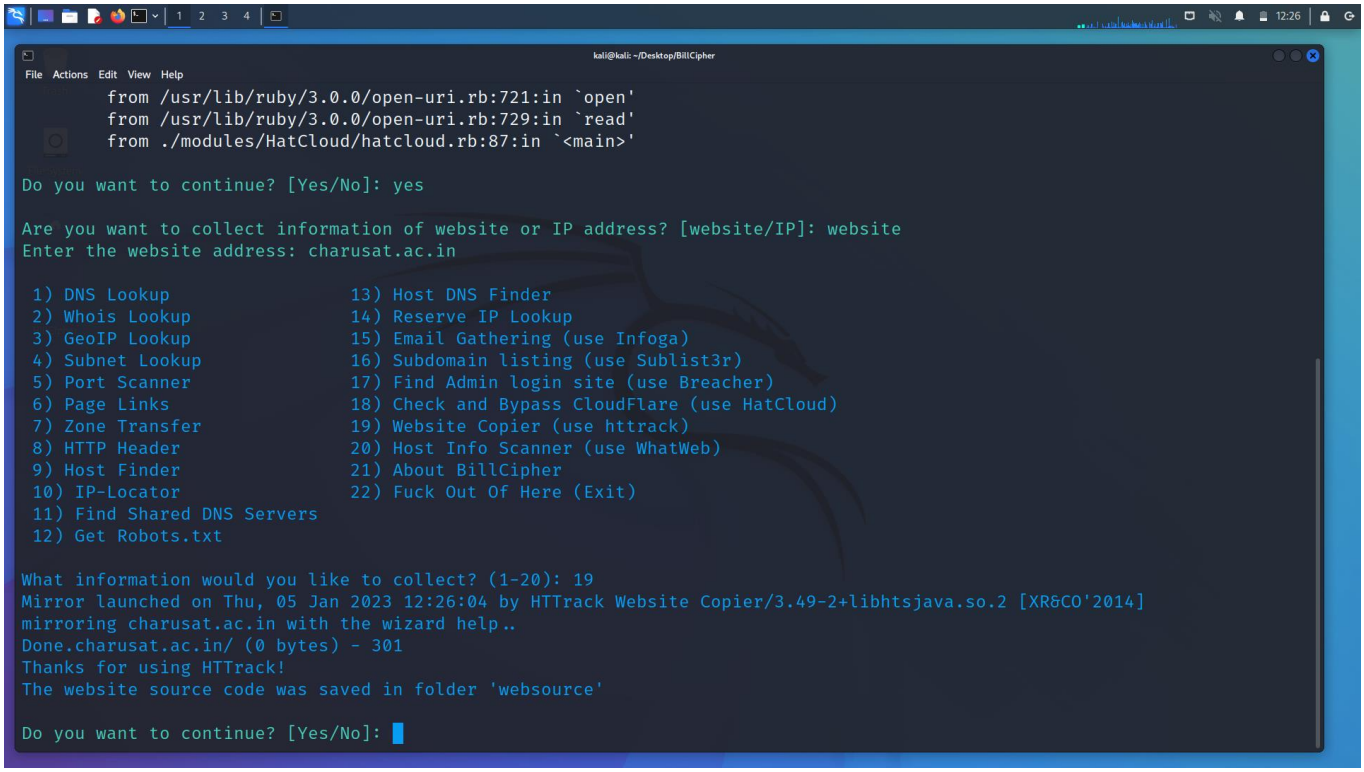
E-mail gathering for charusat.ac.in



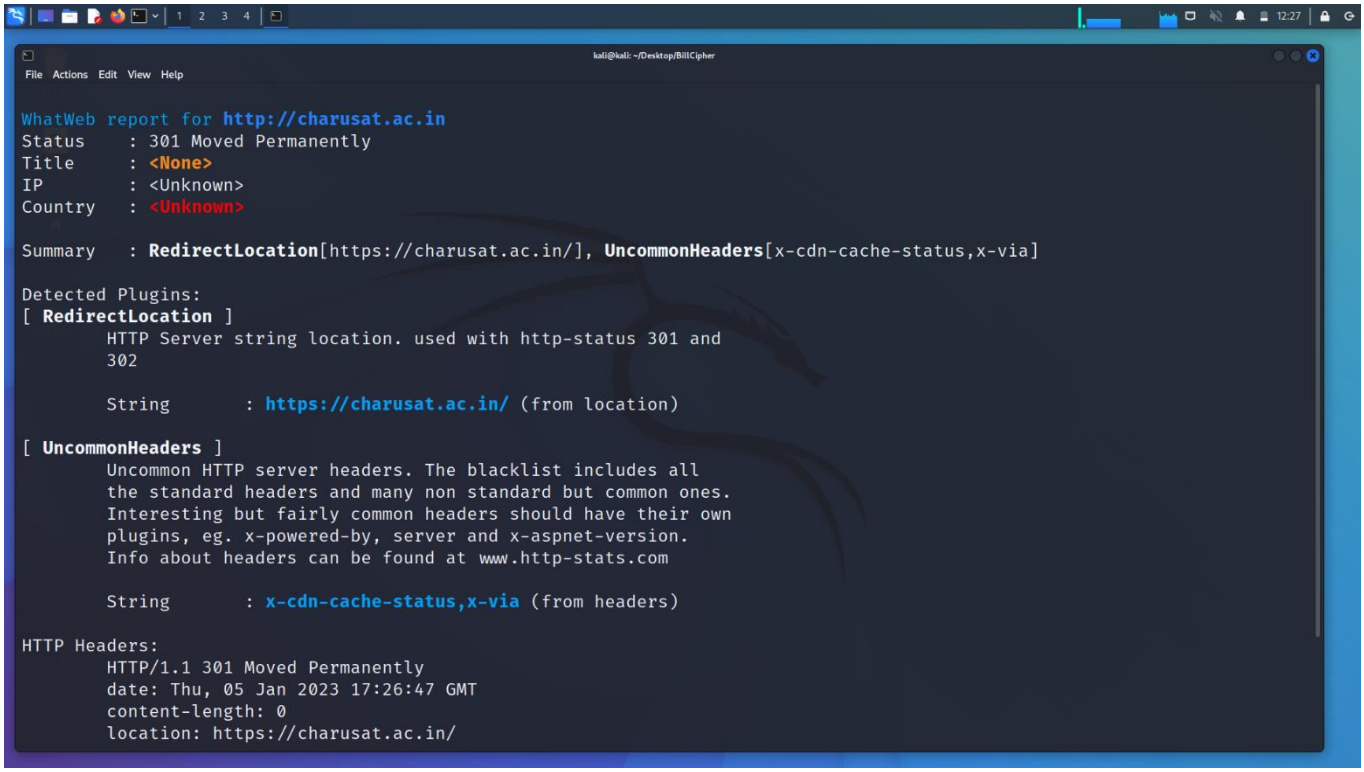
Subdomain listing for charusat.ac.in



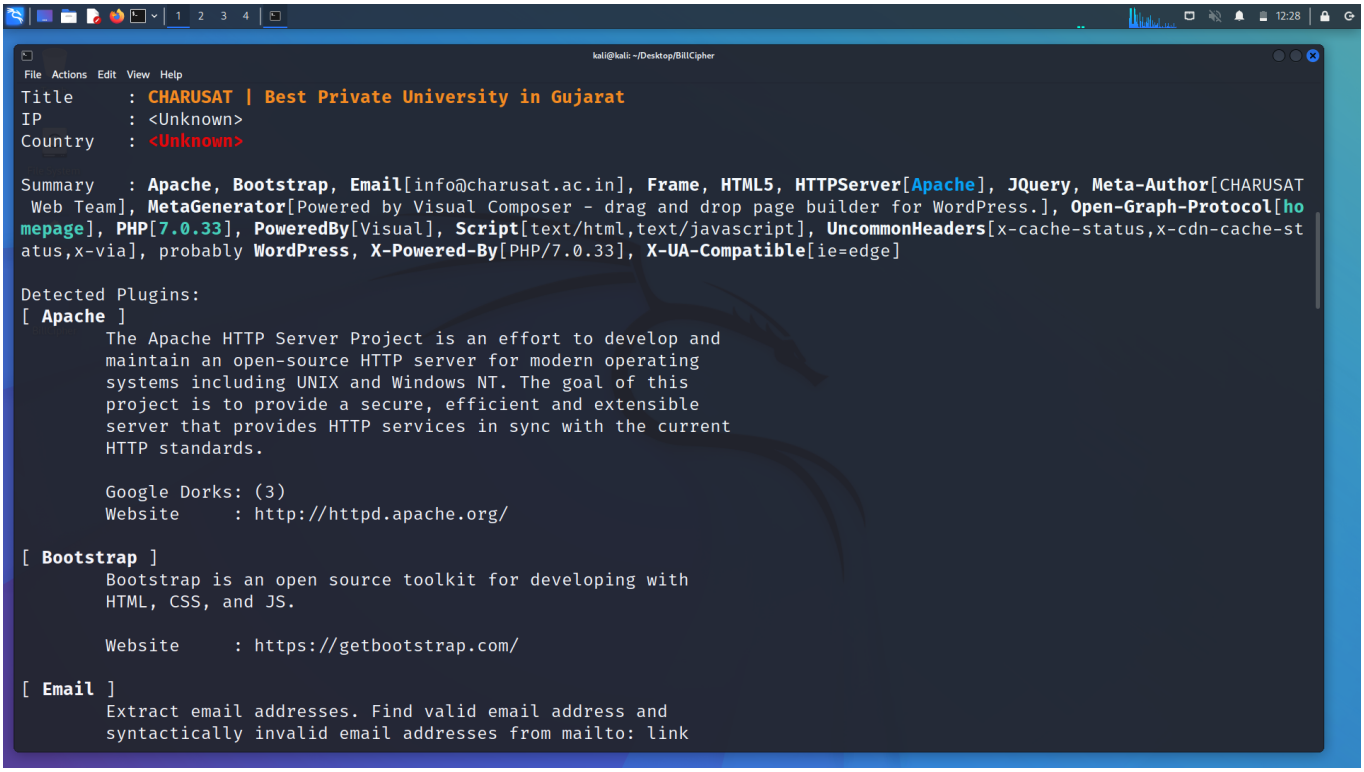
It will check and bypass cloudflare



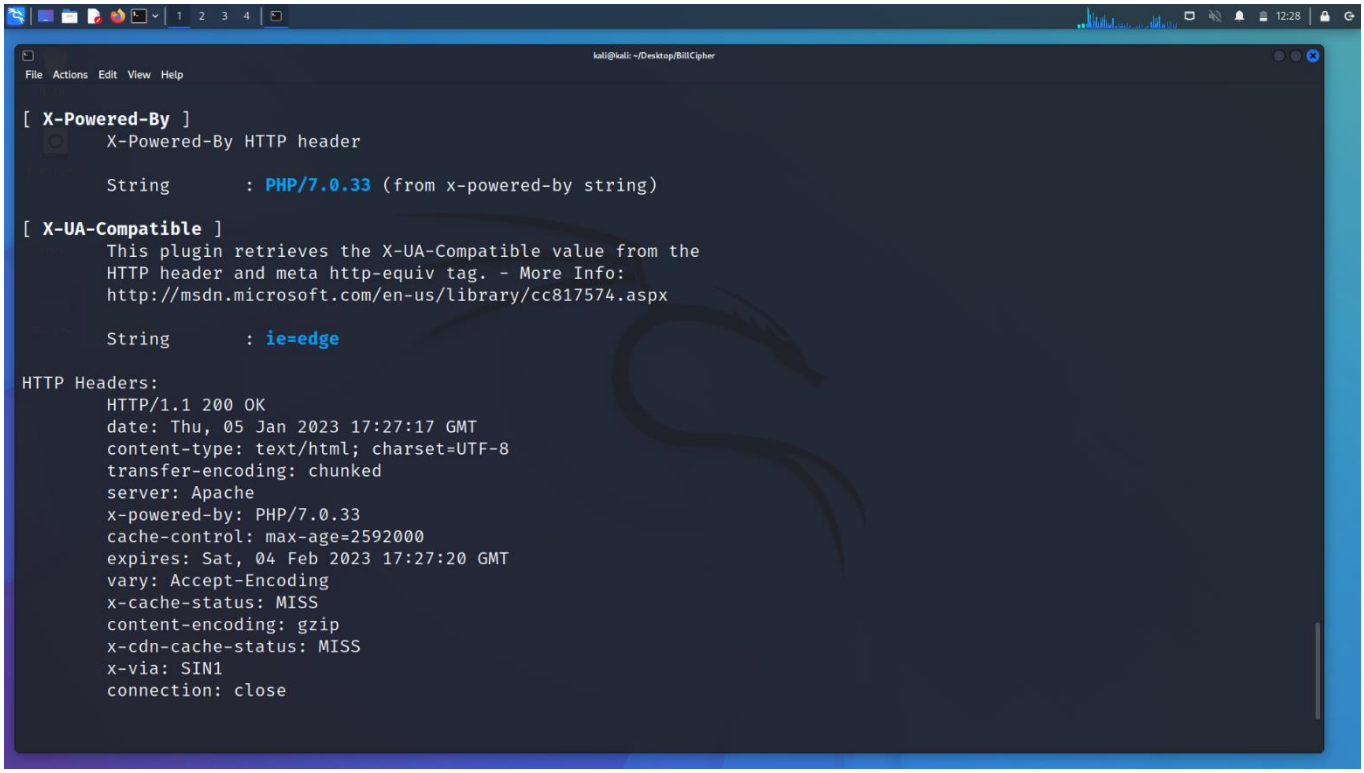
Website copier for charusat.ac.in



Host info scanner 1.1



Host info scanner 1.2



Host info scanner 1.3

LATEST APPLICATIONS:

- Students or new graduates can use and apply to test their websites.
- Also to find the loopholes in several websites of clients .
- Also used in several smalls bug bounties programs for security purposes.

LEARNING OUTCOME:

This practical helped me better understand footprinting and how attackers may employ it to get information about our devices. We also studied software that may help us get information like an email address or the IP address of a website, among other things. You should be aware that some of these tools can be used maliciously.

REFERENCES:

1. About footprinting and reconnaissance:

https://www.eccouncil.org/cybersecurityexchange/ethical-hacking/basics-footprintingreconnaissance

2. Recon-ng: https://www.geeksforgeeks.org/recon-ng-installation-on-kali-linux/

3. Maltego: https://www.maltego.com/

4. OSR Framework: https://www.kali.org/tools/osrframework/

5. BillCipher: https://github.com/bahatiphill/BillCipher

6. OSI Framework:

https://www.asktheeu.org/en/request/5762/response/18627/attach/8/9.OSINT%20Documentation.pdf

7. Lab Module: https://www.youtube.com/watch?v=JWF3bkUclQE