INFORMATION GATHERING REPORT

**ON**

**“www.utest.com”**

**Submitted to:**

**Ms. Tripti Misra**

**Assistant Professor(SS)**

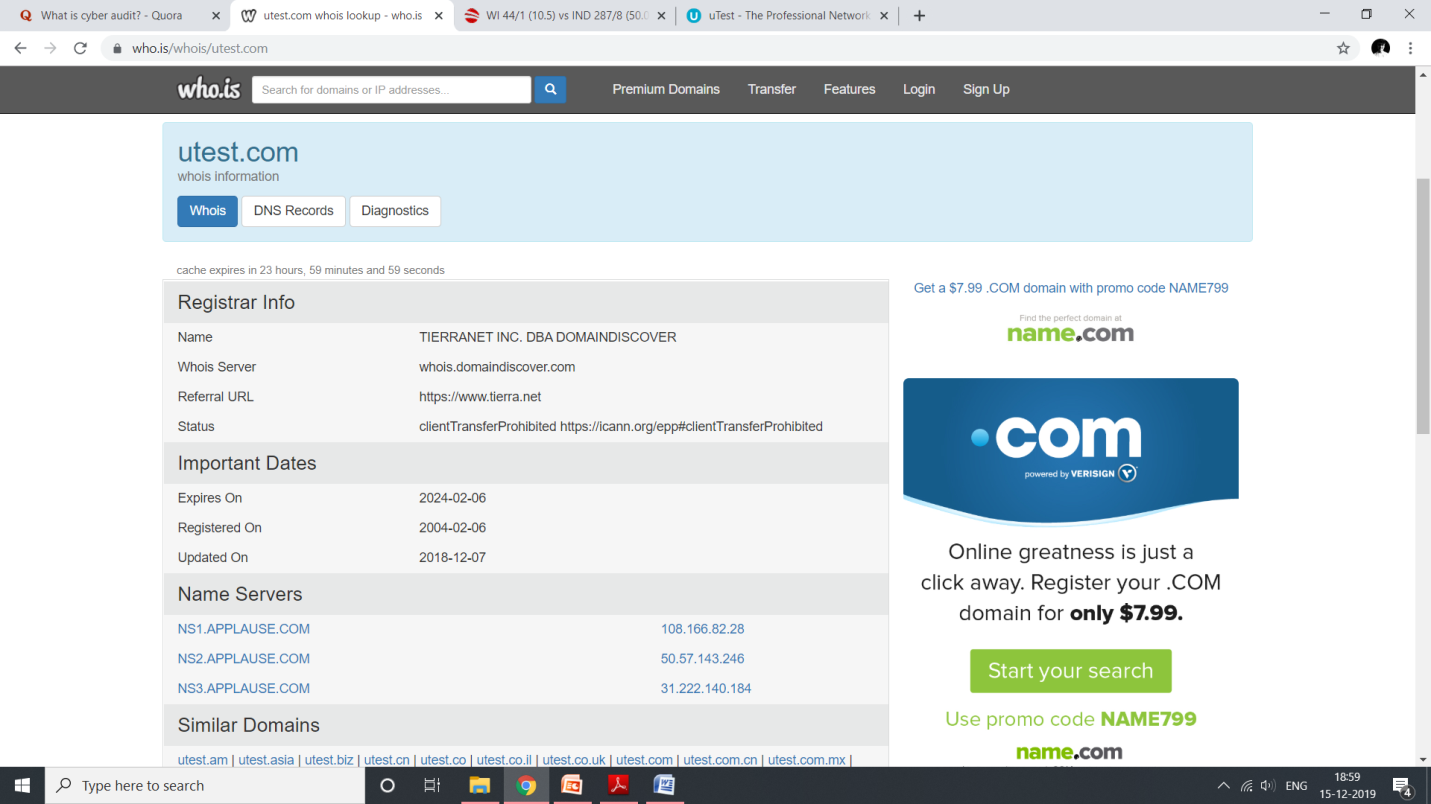
**Department of Systemics**

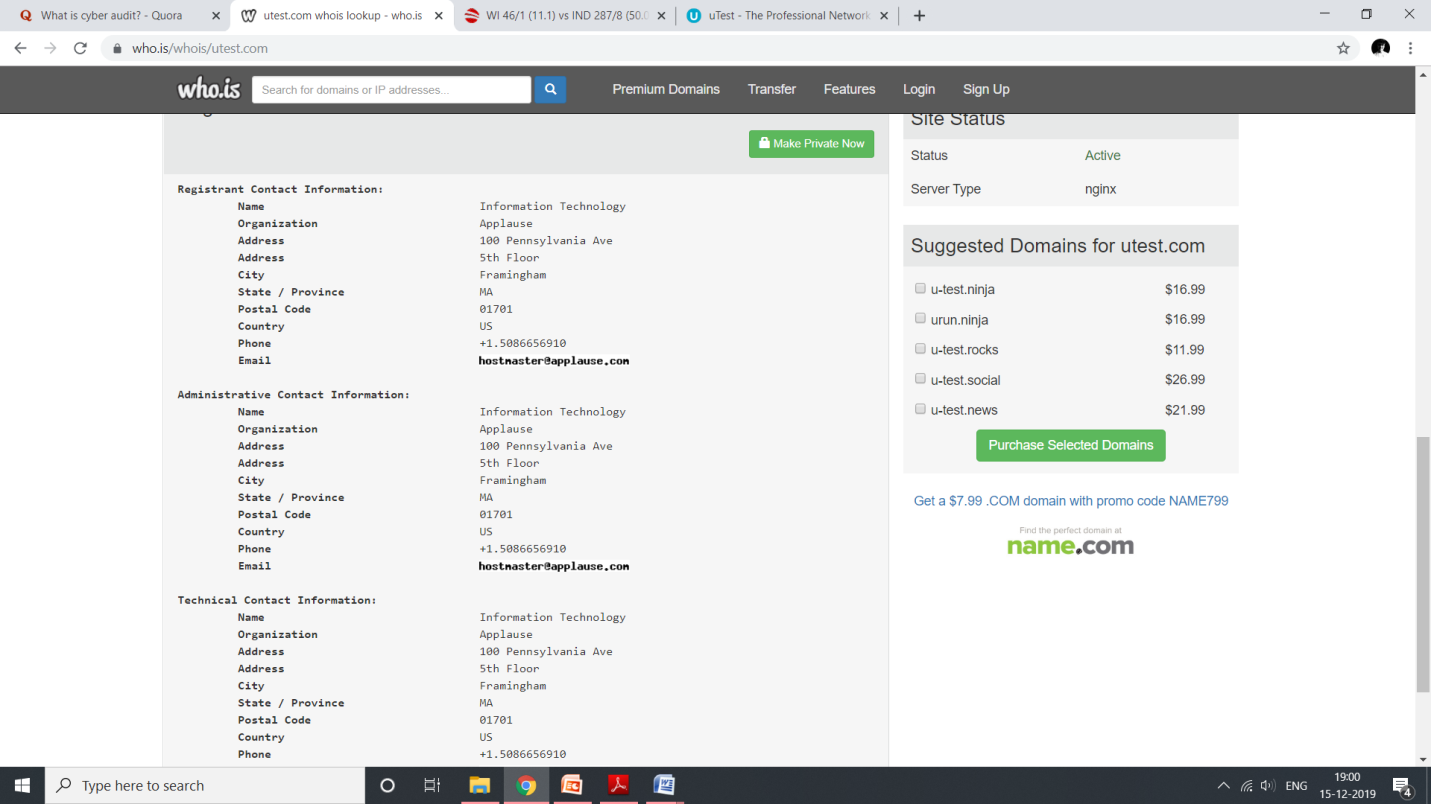
Student Name**: OJASVI SINGH CHAUHAN**

Roll No**: R134218111**

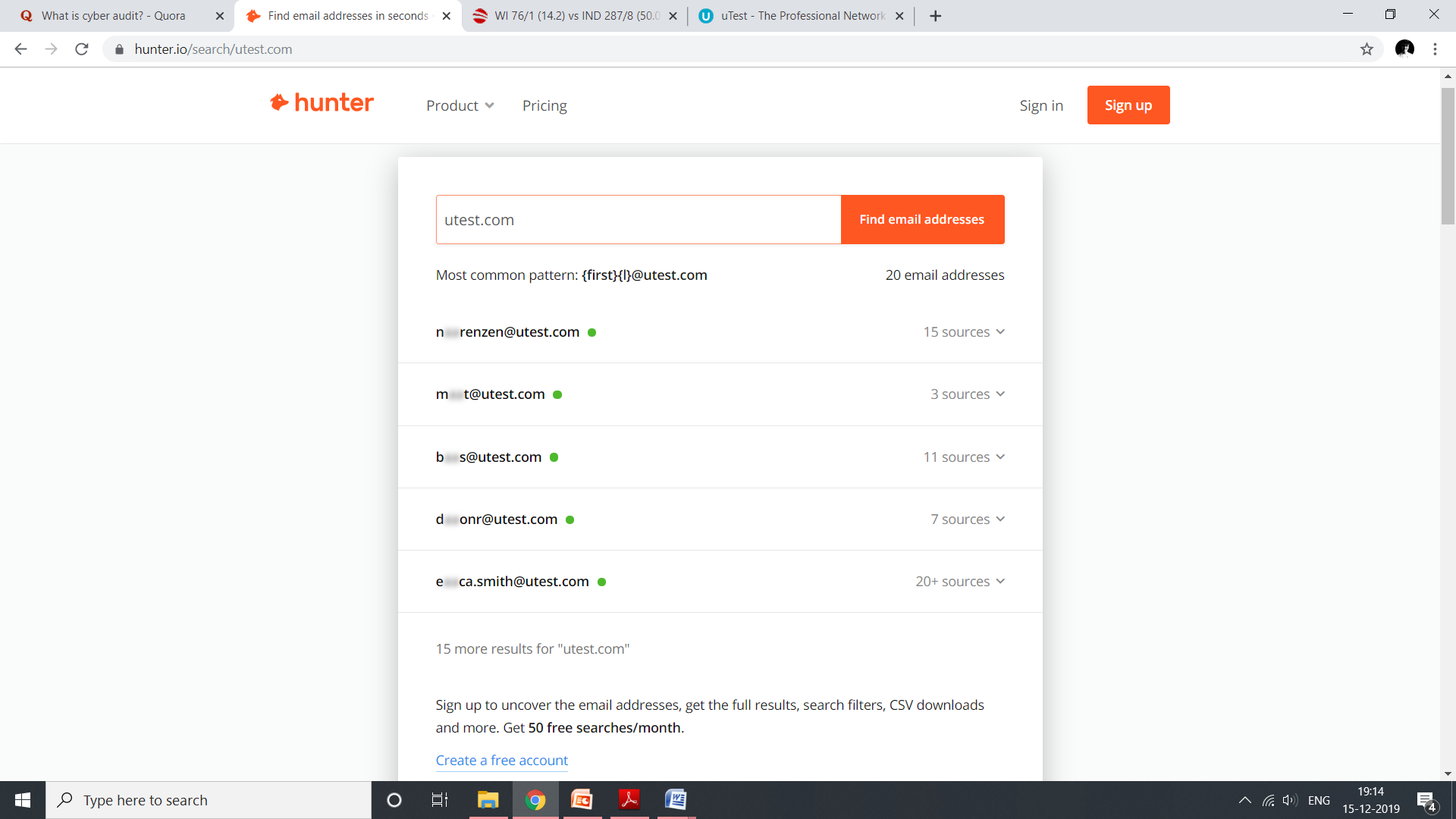
SAP ID**: 500068394**

1. **Who.is** : It is a website by which we can perform searching on its whois database, look up domain and IP owner information, and we can check out dozens of other statistics. We can get all the data we need about a domain and everything associated with that domain anytime with a single search.

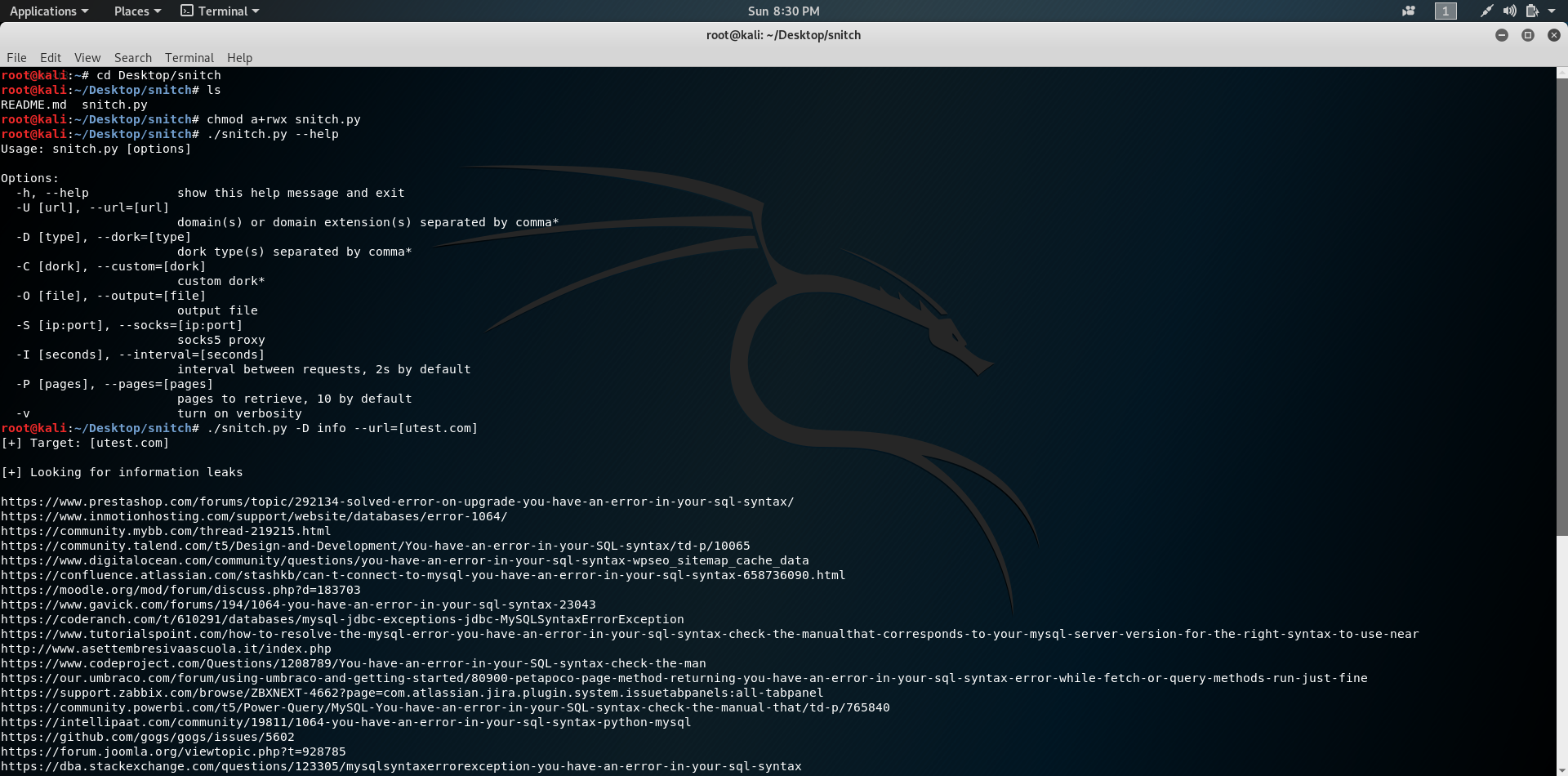




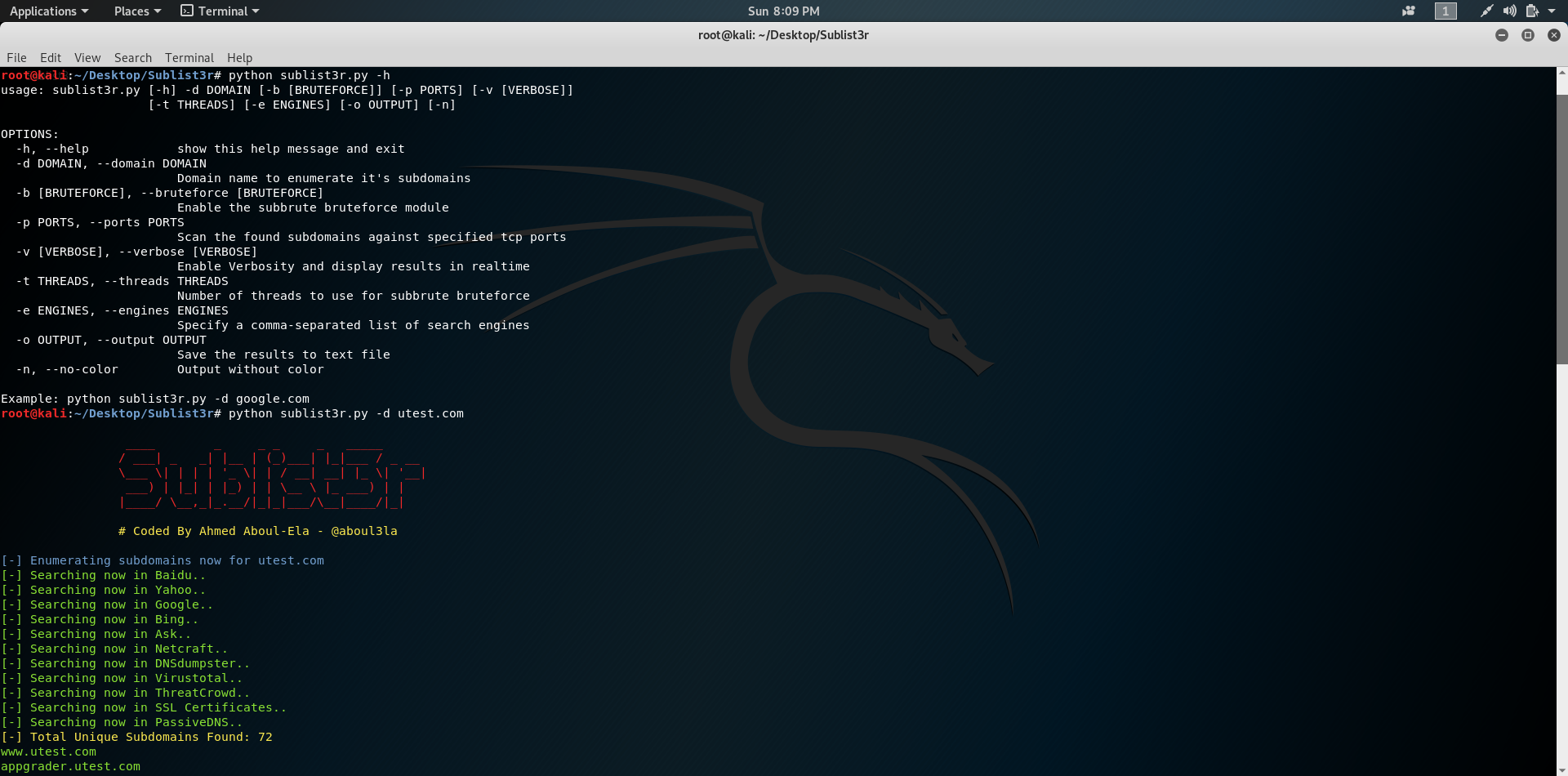
1. **Hunter.io** : We can get the email addresses behind any website. Its Domain Search lists all the people working in a company with their name and **email address** found on the web. With 200+ million email addresses indexed, effective search filters and scoring, it's the most powerful email-finding tool ever created.

.

1. **Snitch**: It is a tool which automates information gathering process for specified domain. Using build-in dork categories, this tool helps gather specified information domain which can be found using web search engines. It can be quite useful in early phases of pentest.

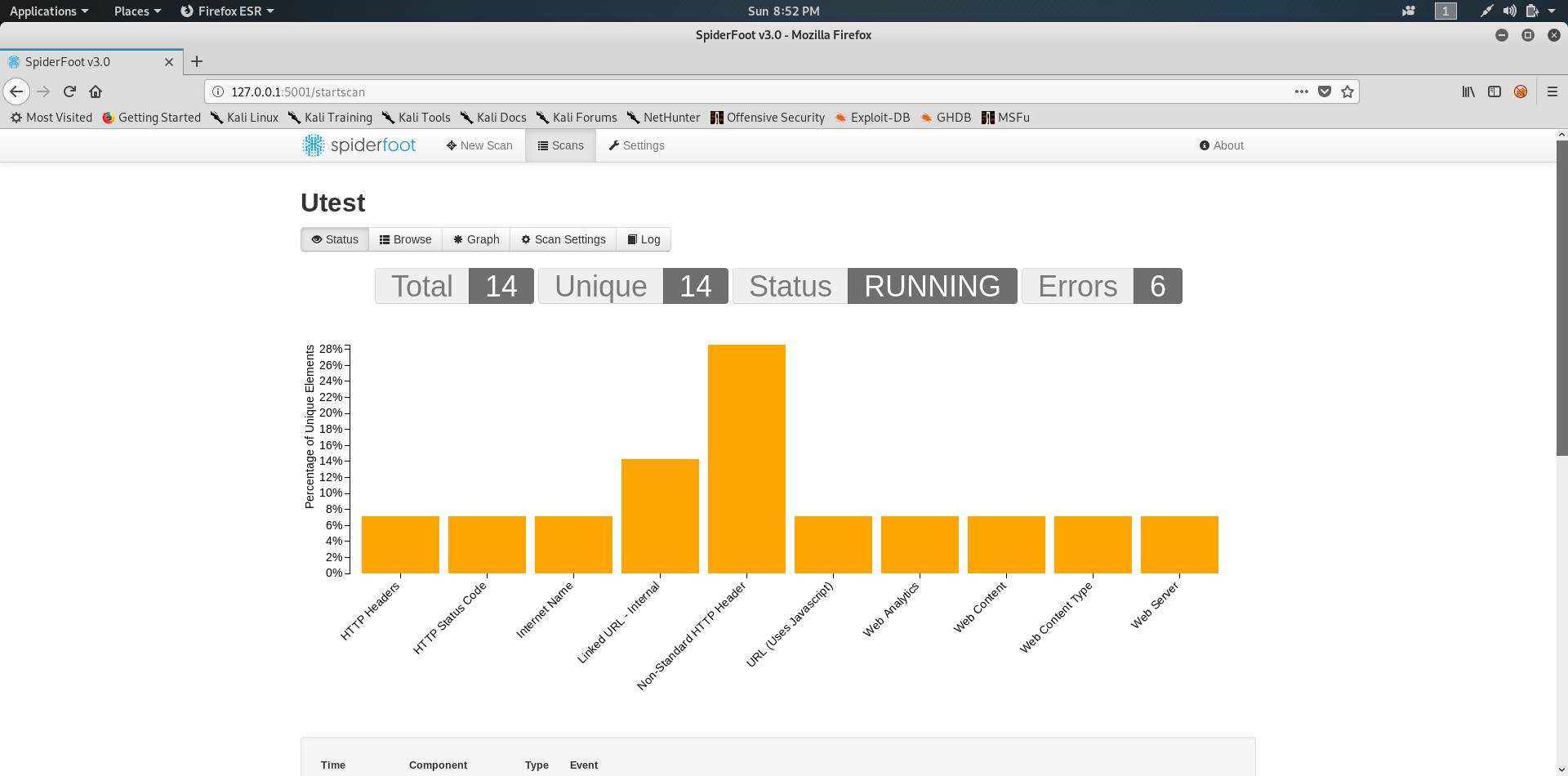


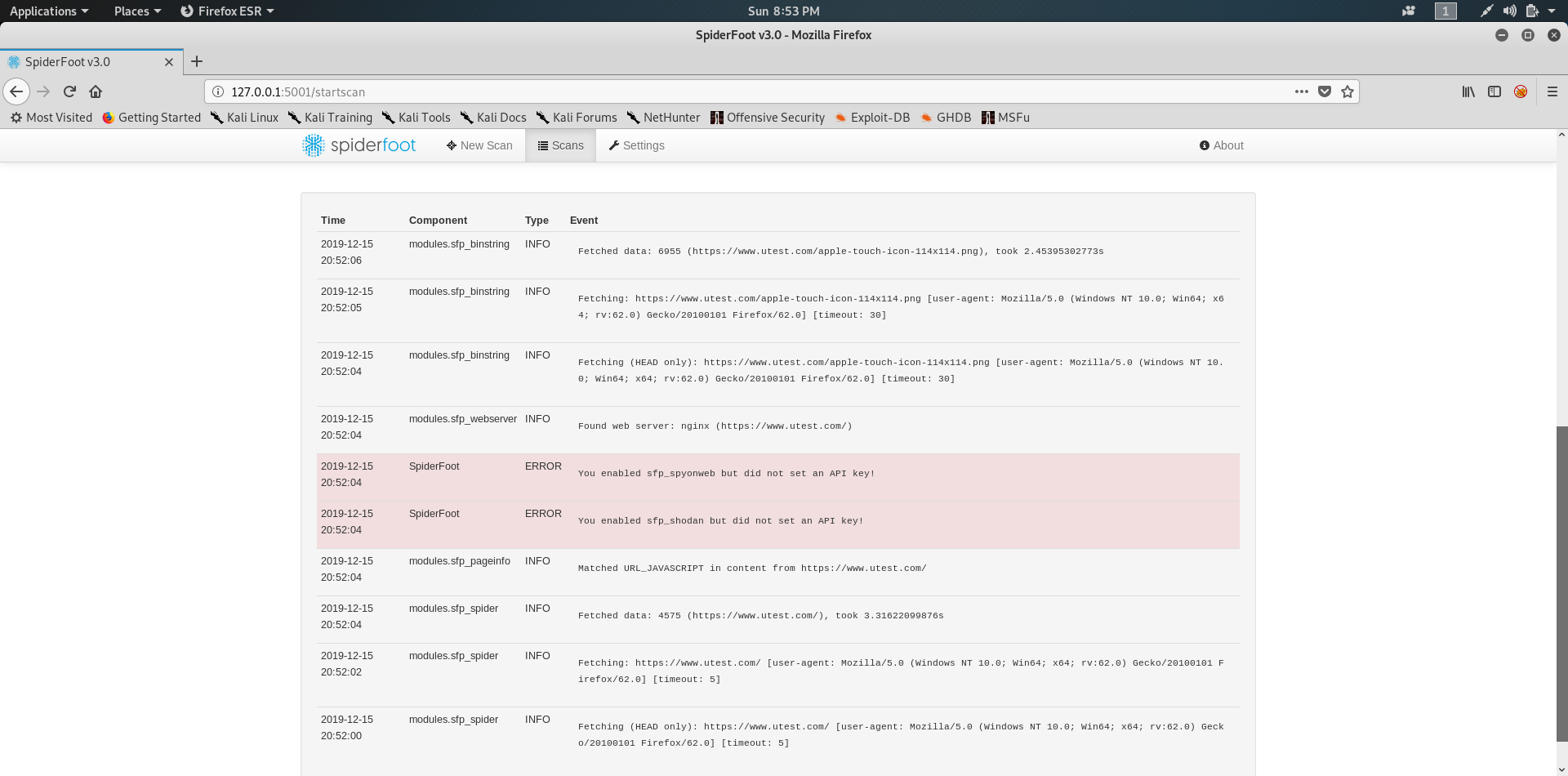
1. **Sublist3r** is a python tool designed to enumerate subdomains of websites using OSINT. It helps penetration testers and bug hunters collect and gather subdomains for the domain they are targeting. Sublist3r enumerates subdomains using many search engines such as Google, Yahoo, Bing, Baidu and Ask. Sublist3r also enumerates subdomains using Netcraft, Virustotal, ThreatCrowd, DNSdumpster and ReverseDNS.



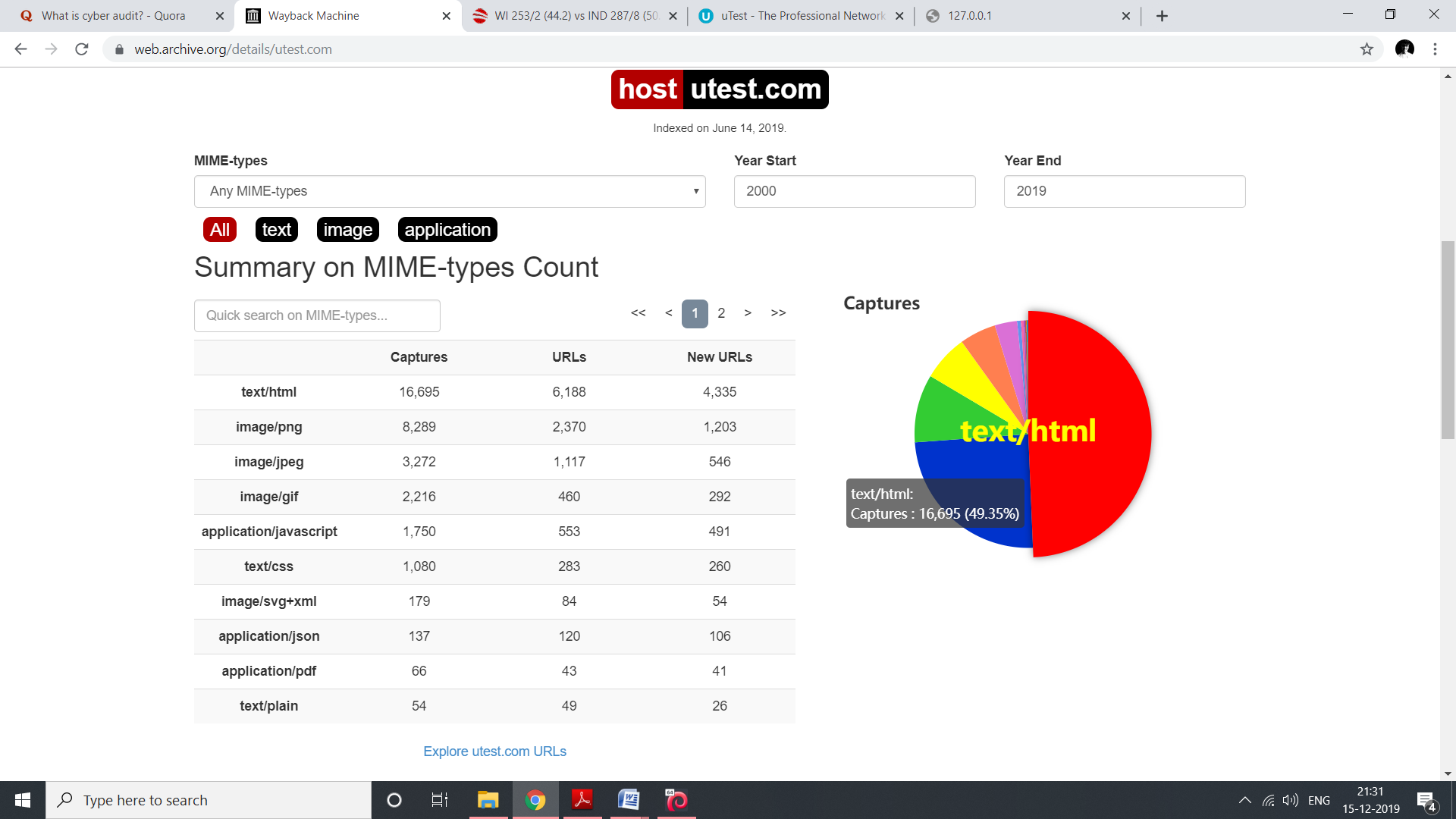
1. **SpiderFoot:** It is an open source intelligence (OSINT) automation tool. Its goal is to automate the process of gathering intelligence about a given target, which may be an IP address, domain name, hostname, network subnet, ASN, e-mail address or person's name.







1. **Wayback Machine** : The Internet Archive, a 501(c)(3) non-profit, is building a digital library of Internet sites and other cultural artifacts in digital form. Like a paper library, they provide free access to researchers, historians, scholars, the print disabled, and the general public. Their mission is to provide Universal Access to All Knowledge.



1. **RBL Lookup**: It is a browser based RBL tool. It is used for discovering if an IP address is on any of the more popular real-time blackhole lists that is checked by the website. To perform a RBL lookup on a domain name, we just type directly into the RBL search box below.

