**EXPERIMENT 3**

**FINGERPRINTING**

Types of Fingerprinting

* Website Fingerprinting
* Competitive Intelligence
* WHOIS Fingerprinting
* Fingerprinting using advanced Google hacking techniques
* Email Fingerprinting
* DNS Fingerprinting
* Network Fingerprinting

**Whois footprinting**

WHOIS (pronounced as the phrase who is) is a query and response protocol and whois footprinting is a method for glance information about ownership of a domain name as following:

Domain name details

Contact details contain phone no. and email address of the owner

Registration date for the domain name

Expire date for the domain name

Domain name servers

**Whois Lookup**

It is broadly used in support of querying databases that store the registered users or assignees of an Internet resource, such as a domain name, an IP address block, or an autonomous system, but is also used for a wider range of other information. The protocol stores and delivers database content in a human-readable format.

Browse given URL [http://whois.domaintools.com/](https://whois.domaintools.com/)in browser and type any domain name.

For example: let’s search pentestlab.in

Now you can see it has created a whois record for pentestlab.in where it contains details like email address, IP, registrant Org. From the given record, anyone can guess that this domain has some connection to raj chandel. The attacker needs to perform footprinting on raj chandel taking help from the previous article.

There is so many other tools use for whois footprinting for example:

Caller IP

Whois Analyzer pro

Whois lookup multiple addresses

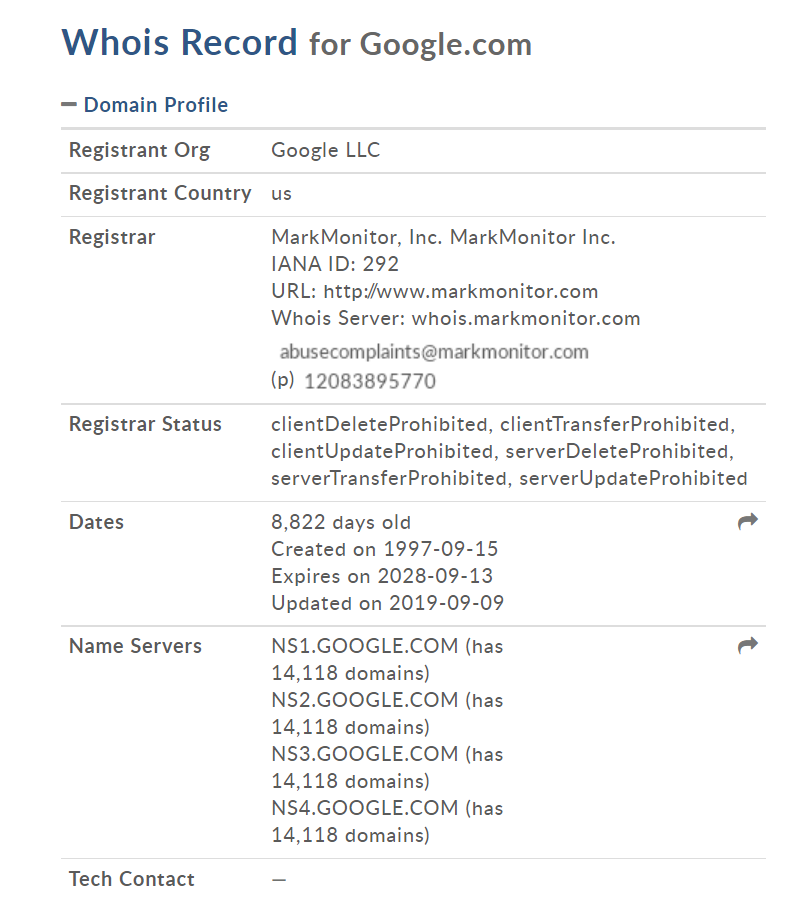


Figure 3.1

**DNS Footprinting**

The attacker performs DNS footprinting in order to enumerate DNS record details and type of servers. There is 10 type of DNS record which provide important information related to the target location.

* A/AAAA
* SVR
* NS
* TXT
* MX
* CNAME
* SOA
* RP
* PTR
* HINFO

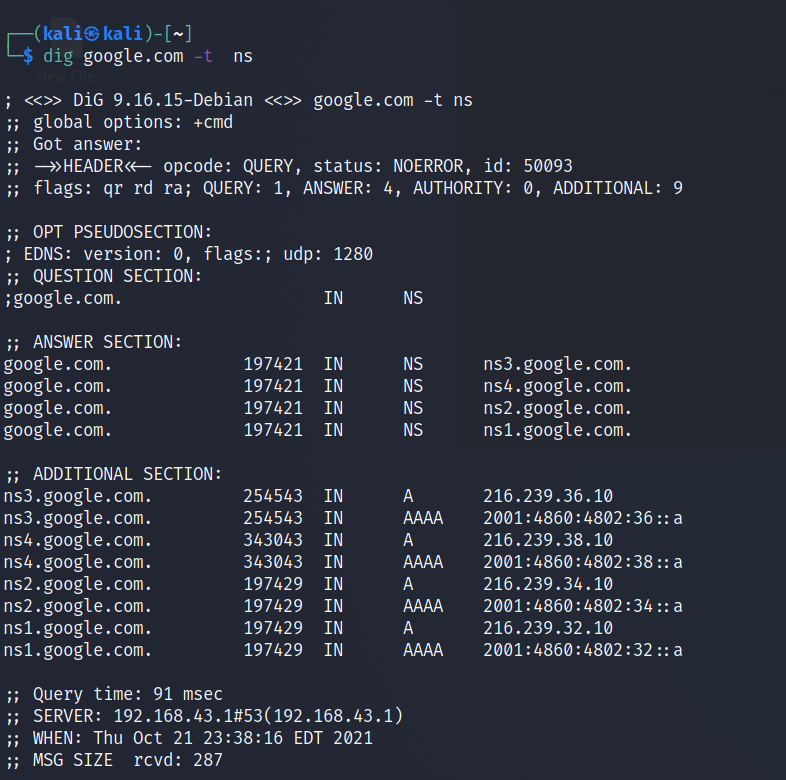


Figure 3.2

**Domain Dossier**:

it is an online tool use for complete DNS footprinting as well as whois footprinting.

There are so many online tools use for DNS footprinting, using domain dossier we will check for DNS records of penetstlab.in, select the check box for DNS records and traceroute and then click on go.

You can observe that the data which we received from whois lookup and from domain dossier is the same to some extent. It has given email ID and moreover details of DNS records TXT, SOA, NS, MX, A and PTR.

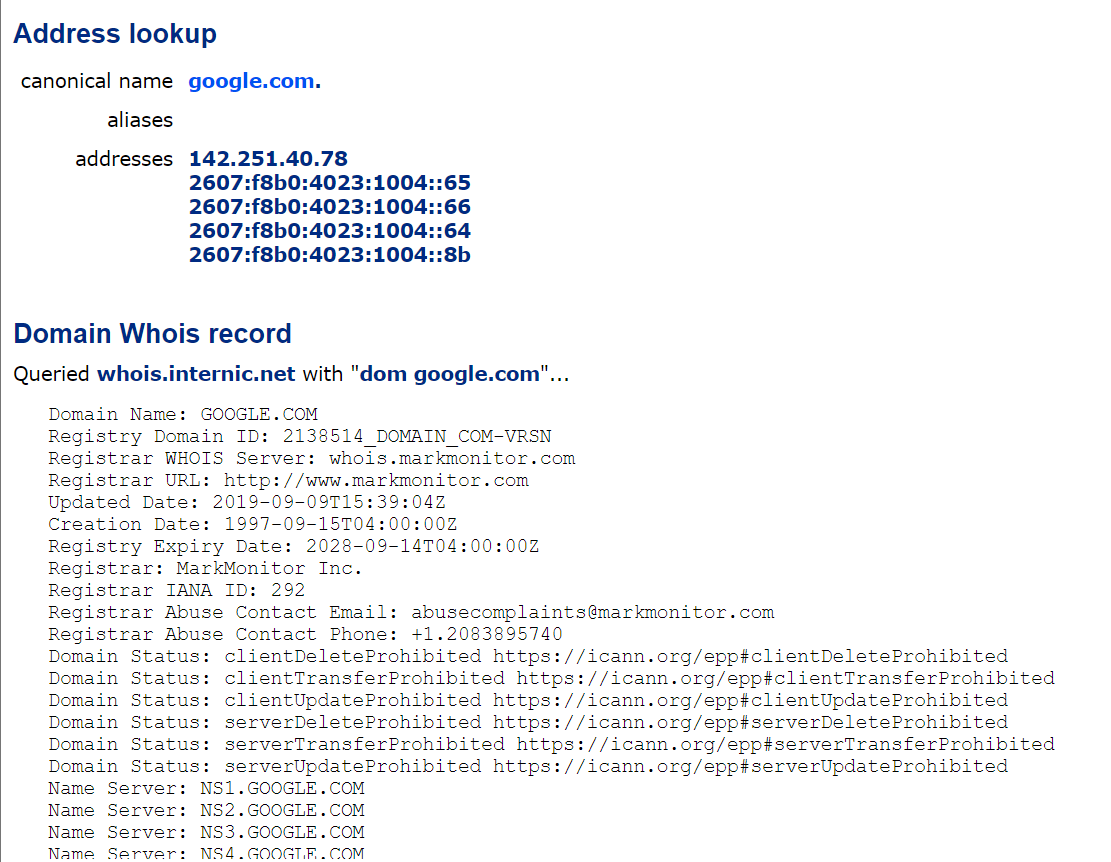
.3

Figure 3.3

**DNS Dumpster**:

 it is also an online use for DNS footprinting.

DNSdumpster.com is a FREE domain research tool that can discover hosts related to a domain. Enumerate a domain and pull back up to 40K subdomains, results are available in an XLS for easy reference.

Repeating the same process for pentestlab.in, it will search for its DNS record. From the given screenshot, you can observe we have received the same details as above. More it will create a copy as an output file in from XLS.

You get signal: it is also an online tool used for DNS footprinting as well as for Network fingerpprinting

A reverse IP domain check takes a domain name or IP address pointing to a web server and searches for other sites known to be hosted on that same web server. Data is gathered from search engine results, which are not guaranteed to be complete

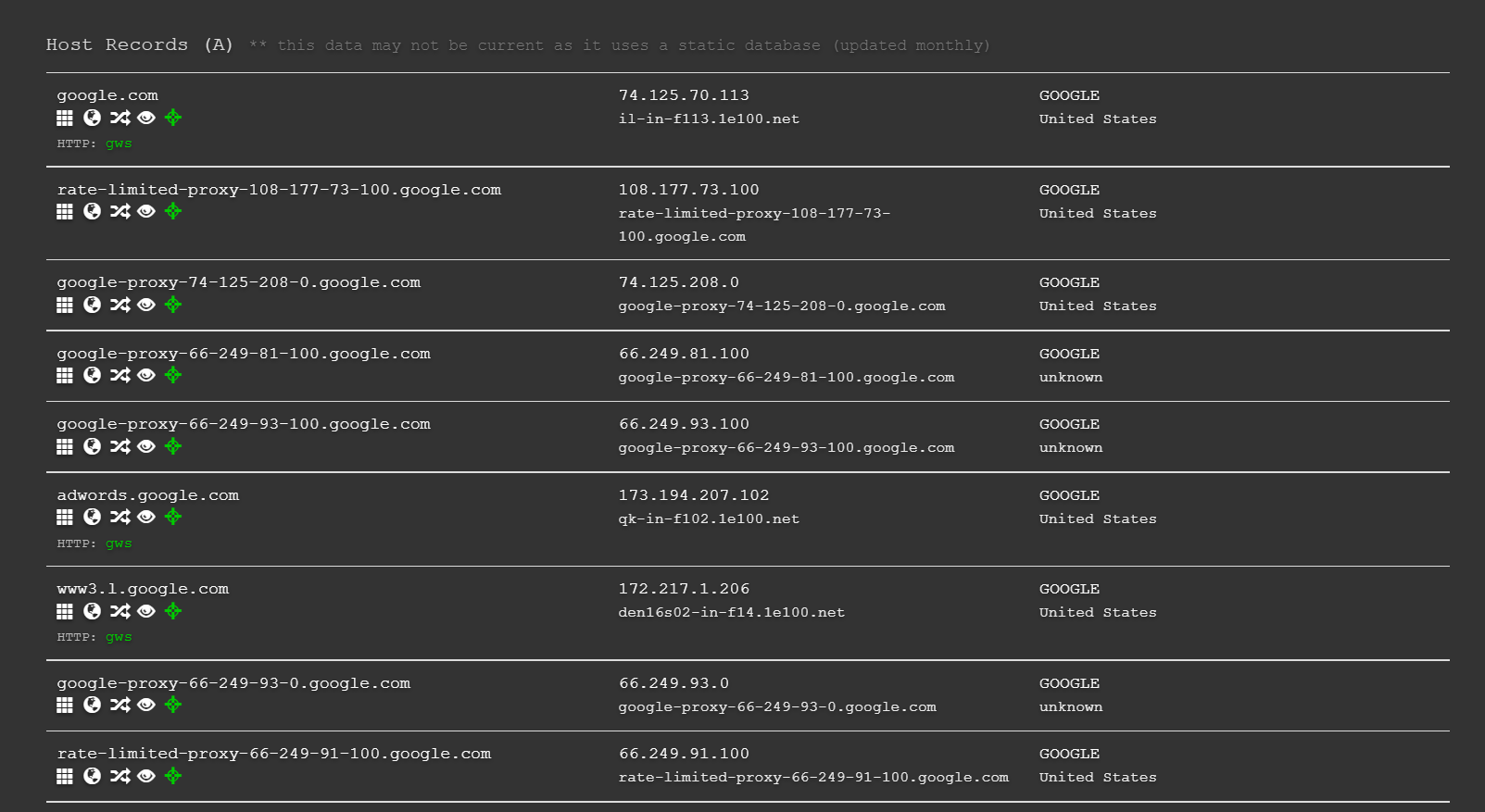


Figure 3.4

Hence we get the IP 72.125.70.113 for pentestlab.inmoreover it dumped the name of 14 other domain which is hosted on the same web server.

**Website Fingerprinting**

It is a technique used for extracting the details related to the website as following

Archived description of the website

Content management system and framework

Script and platform of the website and web server

**Web crawling**

Extract metadata and contact details from the website

Website and web page monitoring and analyser

**Archive.org**:

It is an online tool use for visiting the archived version of any website.

Archive.org has search option as way back machine which is like a time machine for any website. It contains entire information from past till present scenario of any website either their layout or content everything related to the website is present inside. In simple words, it contains the history of any website.

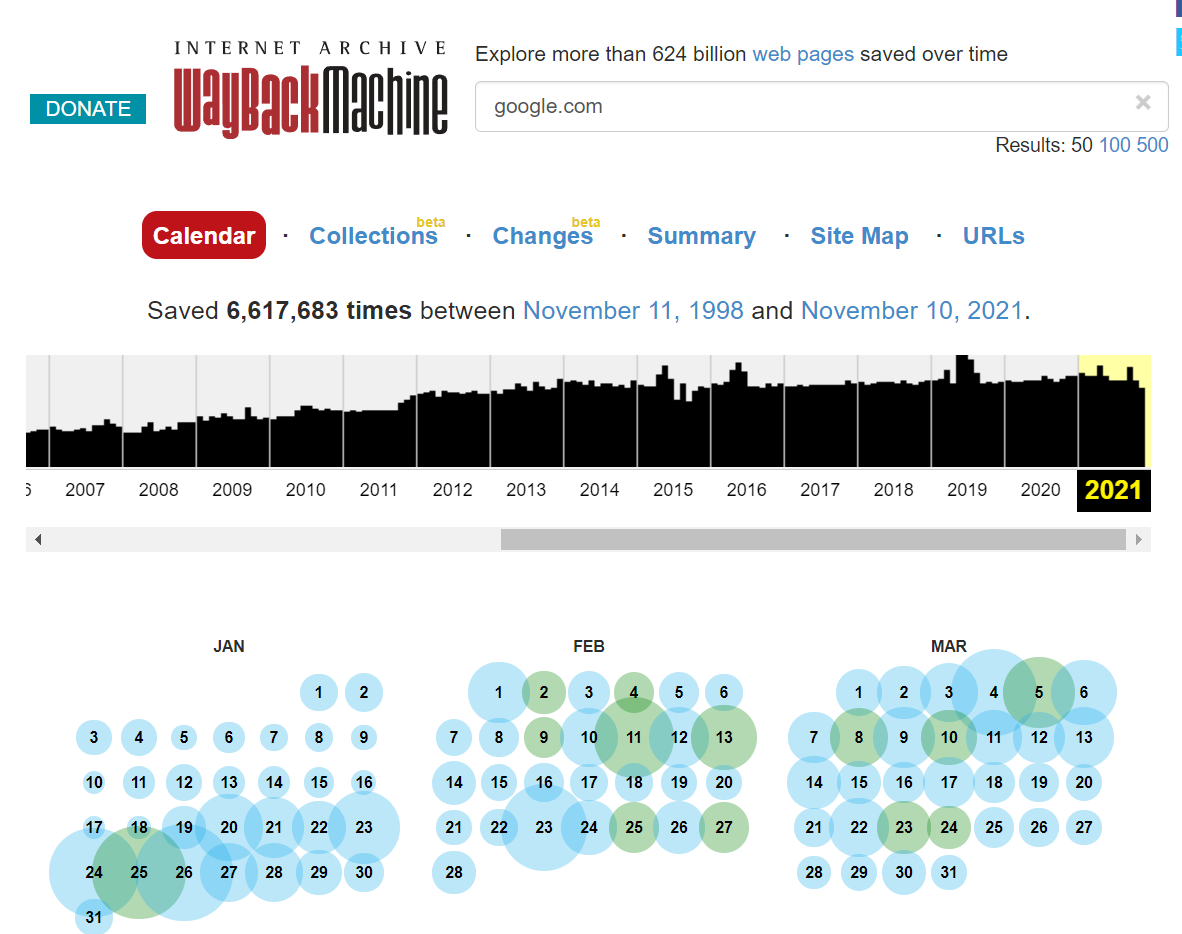


Figure 3.5

**Built With**:

 It is an online tool used for detecting techniques and framework involved inside running website.

BuiltWith.com technology tracking includes widgets, analytics, frameworks, content management systems, advertisers, content delivery networks, web standards, and web servers to name some of the technology categories.

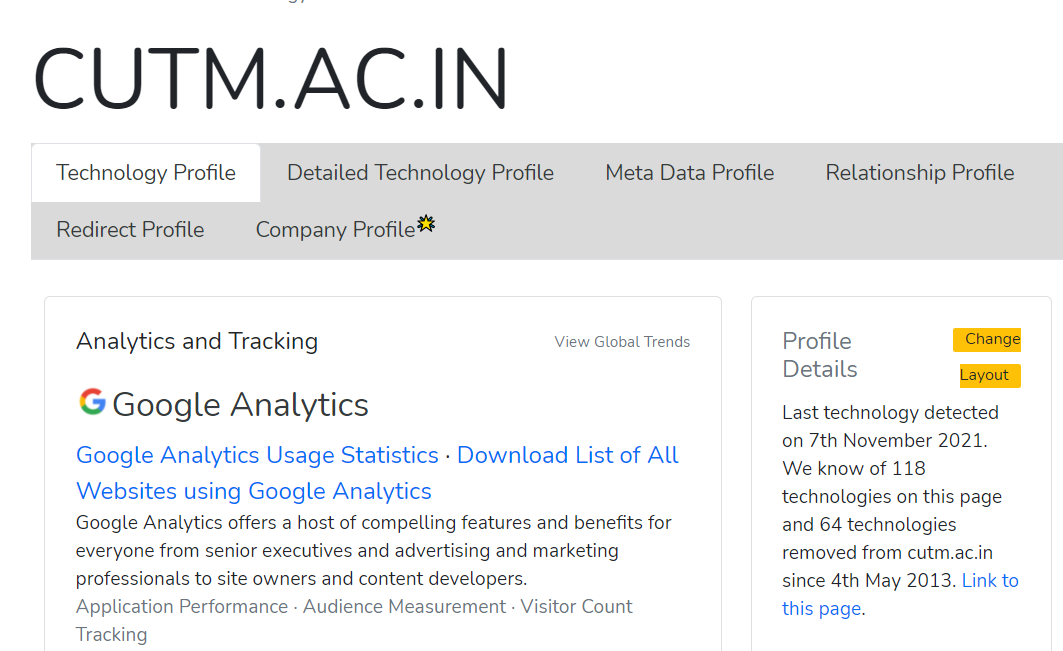


Figure 3.6

**Whatweb**

Whatweb can identify all sorts of information about a live website, like Platform, CMS platform, Type of Script, Google Analytics, Web server Platform, and IP address Country. A pentester can use this tool as both a recon tool & vulnerability scanner.

Open the terminal in Kali Linux and type following command

whatweb “any website url”

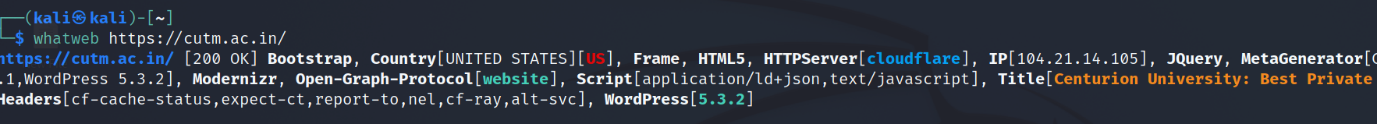


Figure 3.7

**Web crawling**

is a free and open-source Web crawler and offline browser, developed by Xavier Roche

It allows you to download a World Wide Web site from the Internet to a local directory, building recursively all directories, getting HTML, images, and other files from the server to your computer. HTTrack arranges the original site’s relative link-structure.

 Give target URL for copy the web site as “any website url” which starts downloading the website.

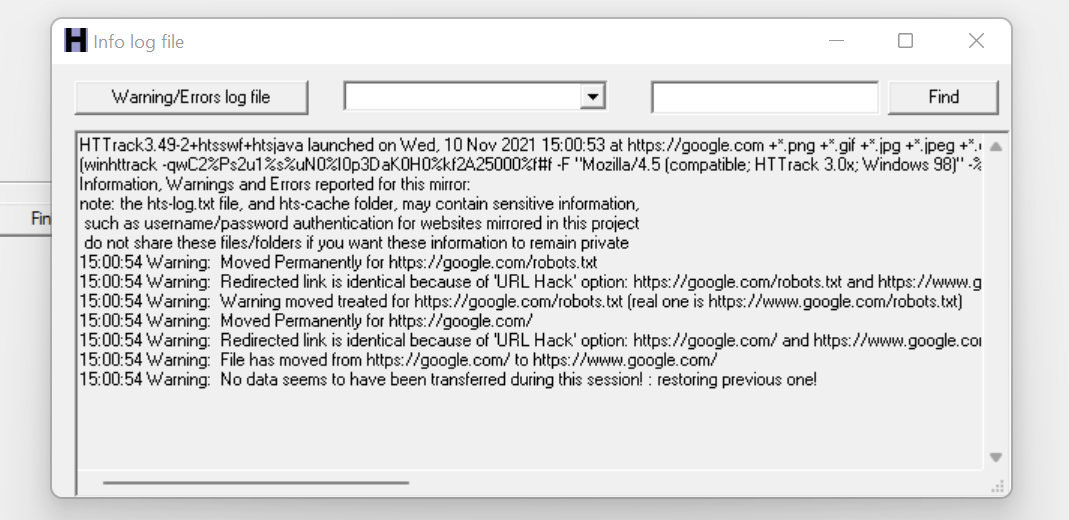


Figure 3.8

**Web Data Extractor**

Web Data Extractor Pro is a web scraping tool specifically designed for mass-gathering of various data types. It can harvest URLs, phone and fax numbers, email addresses, as well as meta tag information and body text. A special feature of WDE Pro is custom extraction of structured data.

Start new project Type target URL as ignitetechnologies.in and select folder to save the output and click on ok.

Now, this tool will extract metadata, email contact no. and etc from inside the target URL.

From given screenshot, you can see it found 40 meta tags1 email 84-phone number from ignitetechnologies.in website.

Similarly, the other tool use as web data extractor:

**Web spider**

**Competitive Intelligence**

**Website-Watcher** is a powerful yet simple website-monitoring tool, perfectly suited to the beginner and advanced user alike.  You can download it from here.

Using the new tab and enter the target URL which starts monitoring the target website.

For example, I enter the URL for monitoring this website.

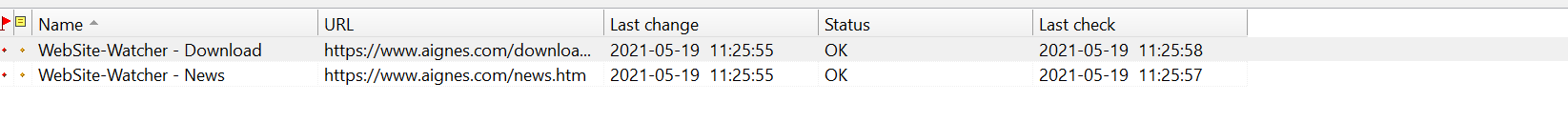


Figure 3.9

**Result:** Different types of fingerprinting was learnt.