Task-6

1/09/2023

Vidit Sharma

21BCY10055

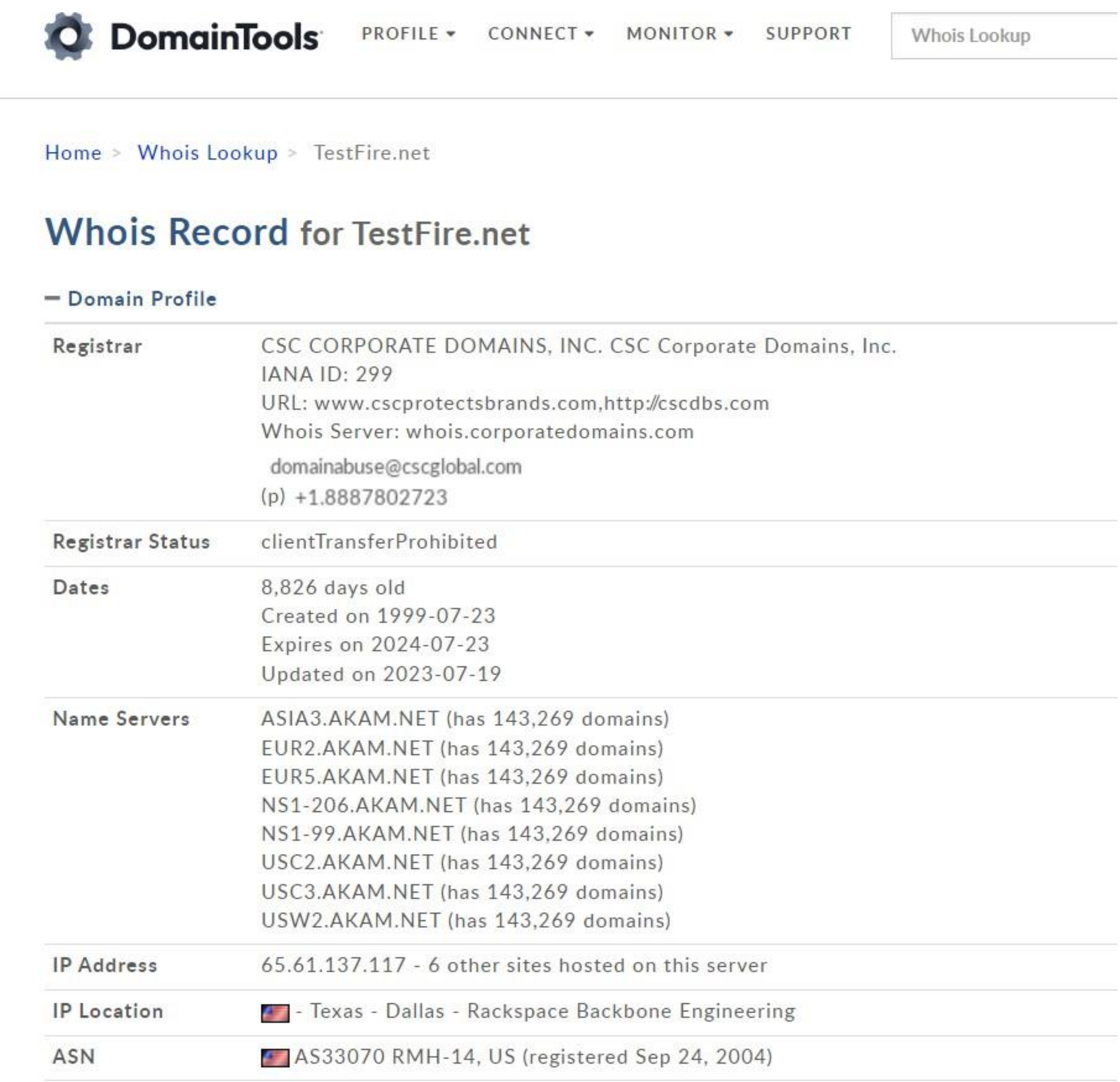
Information Gathering using OSINT framework-

OSINT (Open Source Intelligence) framework is a systematic approach used to gather, analyze, and interpret information from publicly available sources on the internet. It involves a combination of tools, techniques, and methodologies to collect data from social media, websites, forums, and other online platforms. OSINT framework helps individuals and organizations in various fields, including security, investigations, and research, to obtain valuable insights, identify trends, and assess potential threats or opportunities by leveraging publicly accessible information.

Conducting information gathering on a potentially vulnerable website using OSINT techniques requires careful planning and ethical considerations.

Vulnerable website URL - http://testfire.net/

Whois lookup is a valuable OSINT (Open-Source Intelligence) technique for gathering information about domain names and the organizations or individuals behind them.

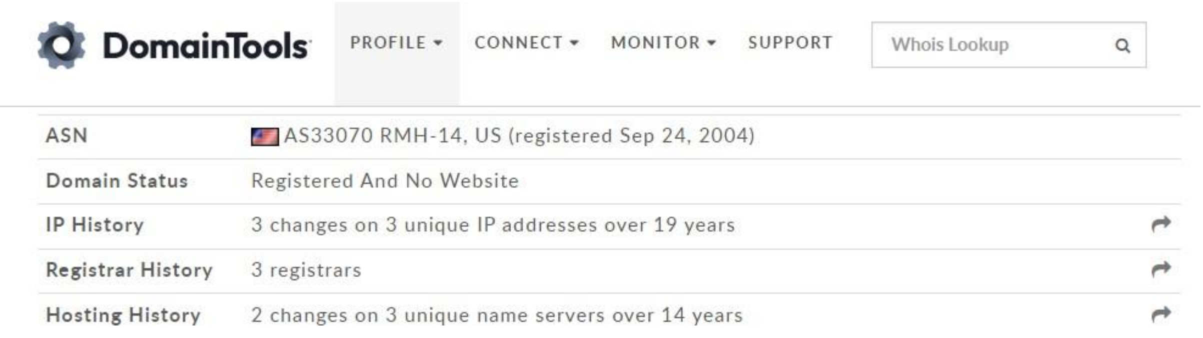


Home > Whois Lookup > TestFire.net

Whois Record for TestFire.net

— Domain Profile

Registrar	CSC CORPORATE DOMAINS, INC. CSC Corporate Domains, Inc. IANA ID: 299 URL: www.cscprotectsbrands.com,http://cscdbs.com Whois Server: whois.corporatedomains.com domainabuse@cscglobal.com (p) +1.8887802723
Registrar Status	clientTransferProhibited
Dates	8,826 days old Created on 1999-07-23 Expires on 2024-07-23 Updated on 2023-07-19
Name Servers	ASIA3.AKAM.NET (has 143,269 domains) EUR2.AKAM.NET (has 143,269 domains) EUR5.AKAM.NET (has 143,269 domains) NS1-206.AKAM.NET (has 143,269 domains) NS1-99.AKAM.NET (has 143,269 domains) USC2.AKAM.NET (has 143,269 domains) USC3.AKAM.NET (has 143,269 domains) USW2.AKAM.NET (has 143,269 domains)
IP Address	65.61.137.117 - 6 other sites hosted on this server
IP Location	- Texas - Dallas - Rackspace Backbone Engineering
ASN	AS33070 RMH-14, US (registered Sep 24, 2004)

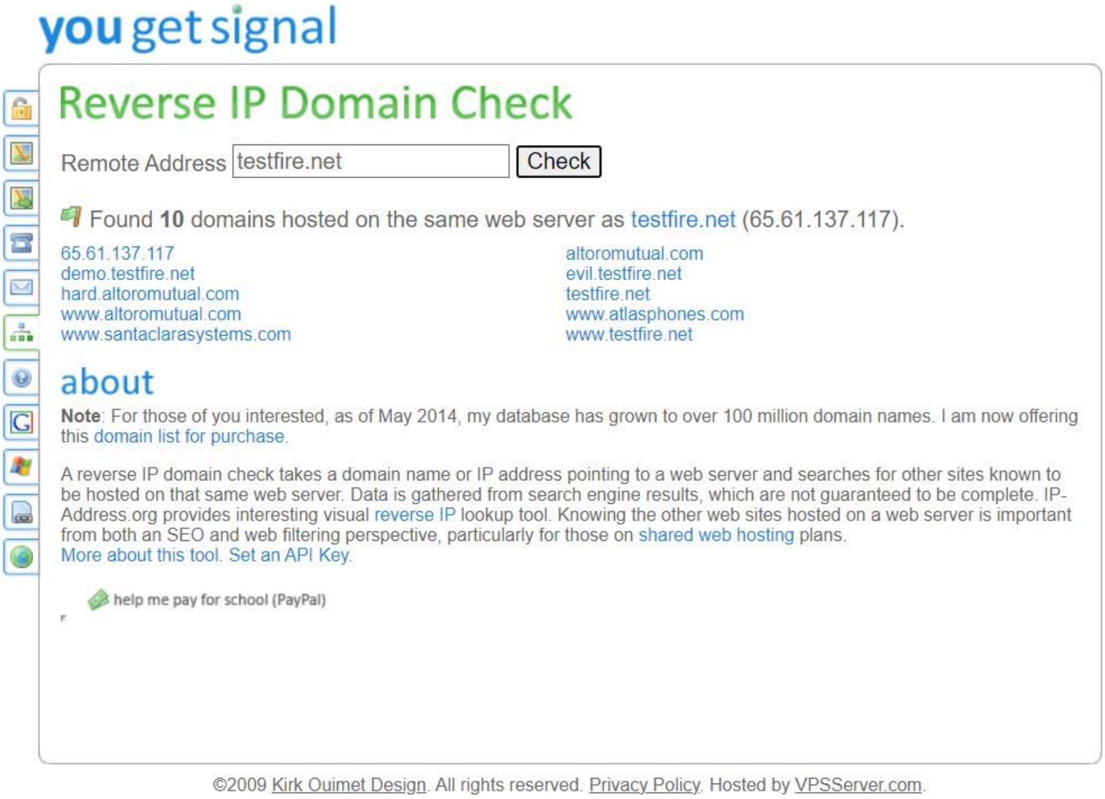


ASN	AS33070 RMH-14, US (registered Sep 24, 2004)
Domain Status	Registered And No Website
IP History	3 changes on 3 unique IP addresses over 19 years
Registrar History	3 registrars
Hosting History	2 changes on 3 unique name servers over 14 years

Information gathered from this website is as shown above.

Reverse IP domain check-

A reverse IP domain check is a technique used to find all the domain names hosted on a specific IP address or web server.



you get signal

Reverse IP Domain Check

Remote Address testfire.net Check

Found **10** domains hosted on the same web server as testfire.net (65.61.137.117).

65.61.137.117	altoromutual.com
demo.testfire.net	evil.testfire.net
hard.altoromutual.com	testfire.net
www.altoromutual.com	www.atlasphones.com
www.santaclarasystems.com	www.testfire.net

about

Note: For those of you interested, as of May 2014, my database has grown to over 100 million domain names. I am now offering this domain list for purchase.

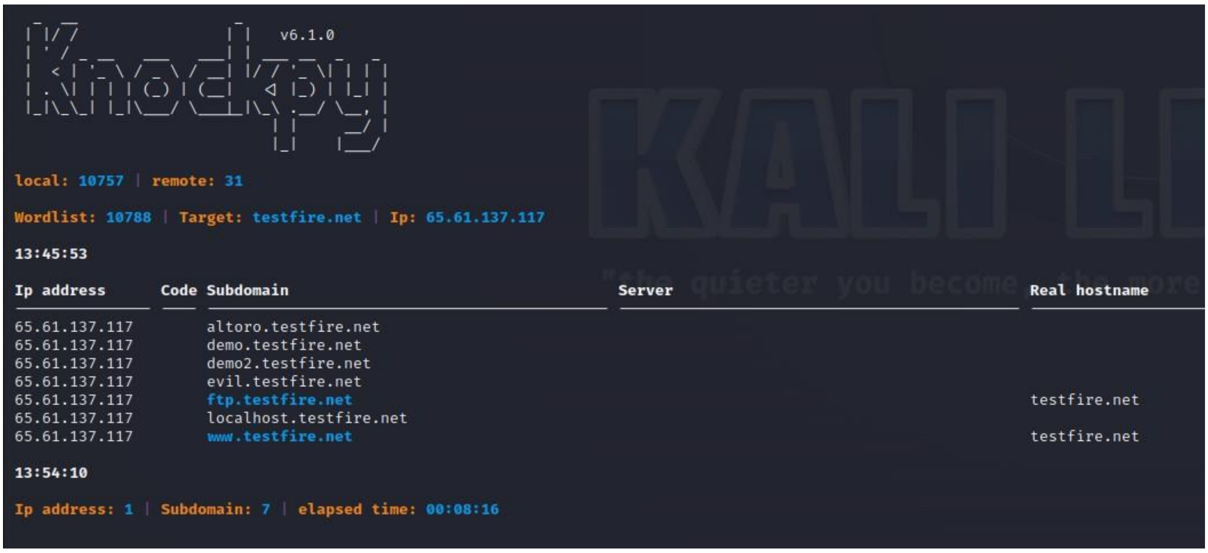
A reverse IP domain check takes a domain name or IP address pointing to a web server and searches for other sites known to be hosted on that same web server. Data is gathered from search engine results, which are not guaranteed to be complete. IP-Address.org provides interesting visual reverse IP lookup tool. Knowing the other web sites hosted on a web server is important from both an SEO and web filtering perspective, particularly for those on shared web hosting plans.
More about this tool. Set an API Key.

help me pay for school (PayPal)

©2009 Kirk Ouimet Design. All rights reserved. Privacy Policy. Hosted by VPSServer.com.

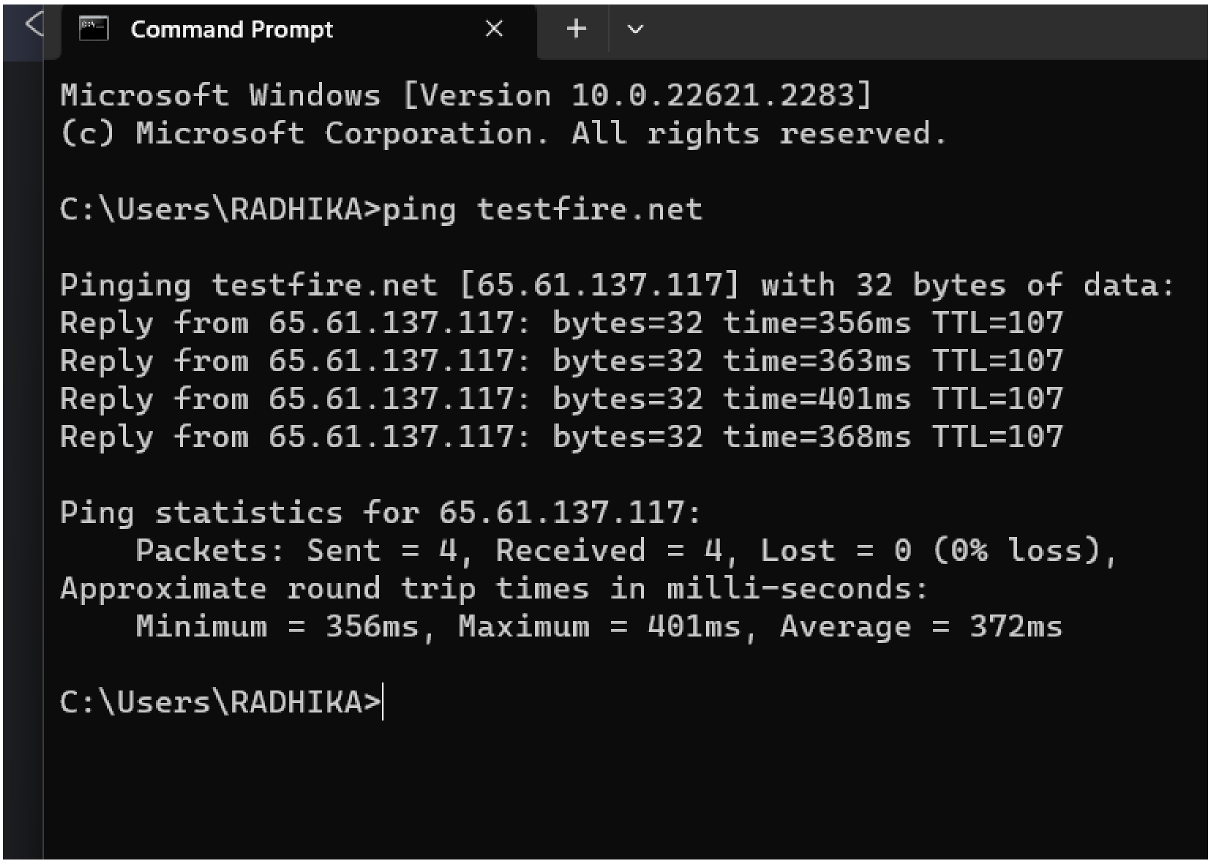
By checking the reverse IP it also give us idea that whether our target is hosted on shared web server or a dedicated web server.
I found 10 domains hosted on a same web server.

Next step is finding sub- domains of our target.



```
v6.1.0

local: 10757 | remote: 31

Wordlist: 10788 | Target: testfire.net | Ip: 65.61.137.117

13:45:53

Ip address       Code Subdomain                                      Server                                       Real hostname

65.61.137.117         altoro.testfire.net
65.61.137.117         demo.testfire.net
65.61.137.117         demo2.testfire.net
65.61.137.117         evil.testfire.net
65.61.137.117         ftp.testfire.net                                                                            testfire.net
65.61.137.117         localhost.testfire.net
65.61.137.117         www.testfire.net                                                                            testfire.net

13:54:10

Ip address: 1 | Subdomain: 7 | elapsed time: 00:08:16
```

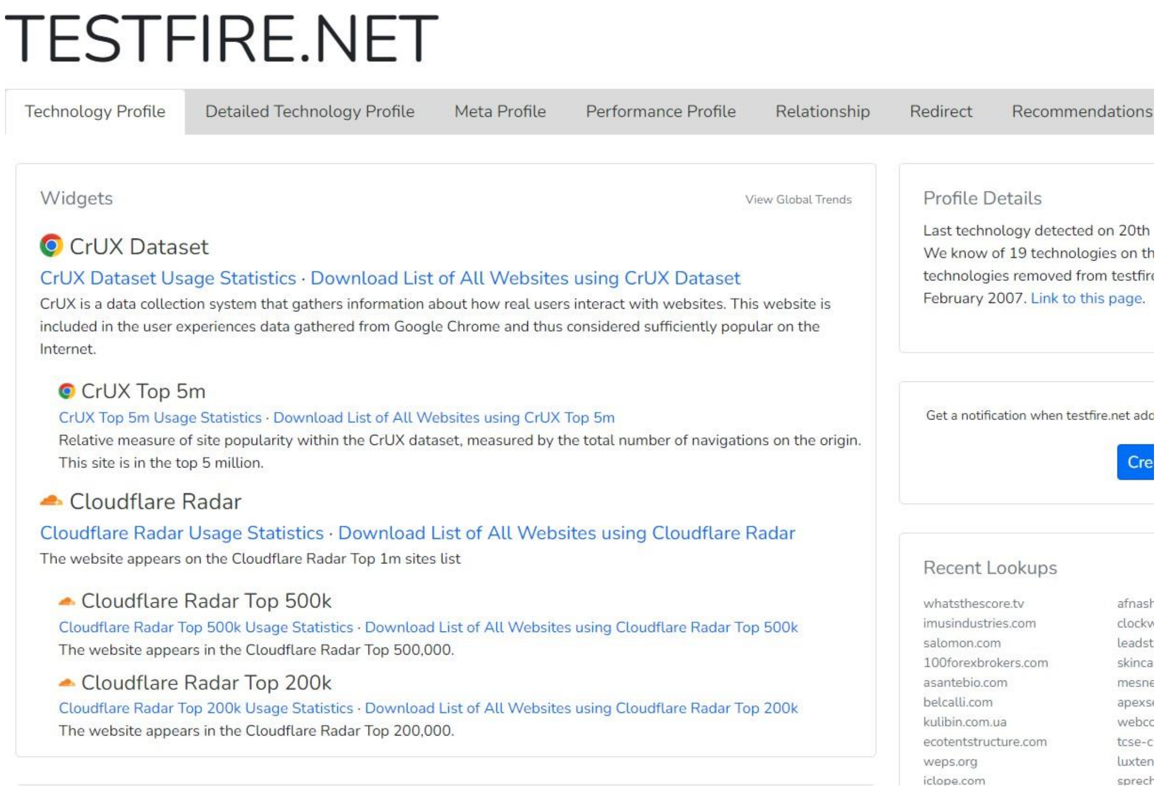
Now I will try to detect the operating system on which the website is hosted.



```
Microsoft Windows [Version 10.0.22621.2283]
(c) Microsoft Corporation. All rights reserved.

C:\Users\RADHIKA>ping testfire.net

Pinging testfire.net [65.61.137.117] with 32 bytes of data:
Reply from 65.61.137.117: bytes=32 time=356ms TTL=107
Reply from 65.61.137.117: bytes=32 time=363ms TTL=107
Reply from 65.61.137.117: bytes=32 time=401ms TTL=107
Reply from 65.61.137.117: bytes=32 time=368ms TTL=107

Ping statistics for 65.61.137.117:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 356ms, Maximum = 401ms, Average = 372ms

C:\Users\RADHIKA>
```

The TTL value is above 100 it means that the website is hosted on a windows server.

Last step is to find on which platform the website is hosted.



TESTFIRE.NET

Widgets

CrUX Dataset

CrUX Dataset Usage Statistics · Download List of All Websites using CrUX Dataset

CrUX is a data collection system that gathers information about how real users interact with websites. This website is included in the user experiences data gathered from Google Chrome and thus considered sufficiently popular on the Internet.

CrUX Top 5m

CrUX Top 5m Usage Statistics · Download List of All Websites using CrUX Top 5m

Relative measure of site popularity within the CrUX dataset, measured by the total number of navigations on the origin. This site is in the top 5 million.

Cloudflare Radar

Cloudflare Radar Usage Statistics · Download List of All Websites using Cloudflare Radar

The website appears on the Cloudflare Radar Top 1m sites list

Cloudflare Radar Top 500k

Cloudflare Radar Top 500k Usage Statistics · Download List of All Websites using Cloudflare Radar Top 500k

The website appears in the Cloudflare Radar Top 500,000.

Cloudflare Radar Top 200k

Cloudflare Radar Top 200k Usage Statistics · Download List of All Websites using Cloudflare Radar Top 200k

The website appears in the Cloudflare Radar Top 200,000.

Profile Details

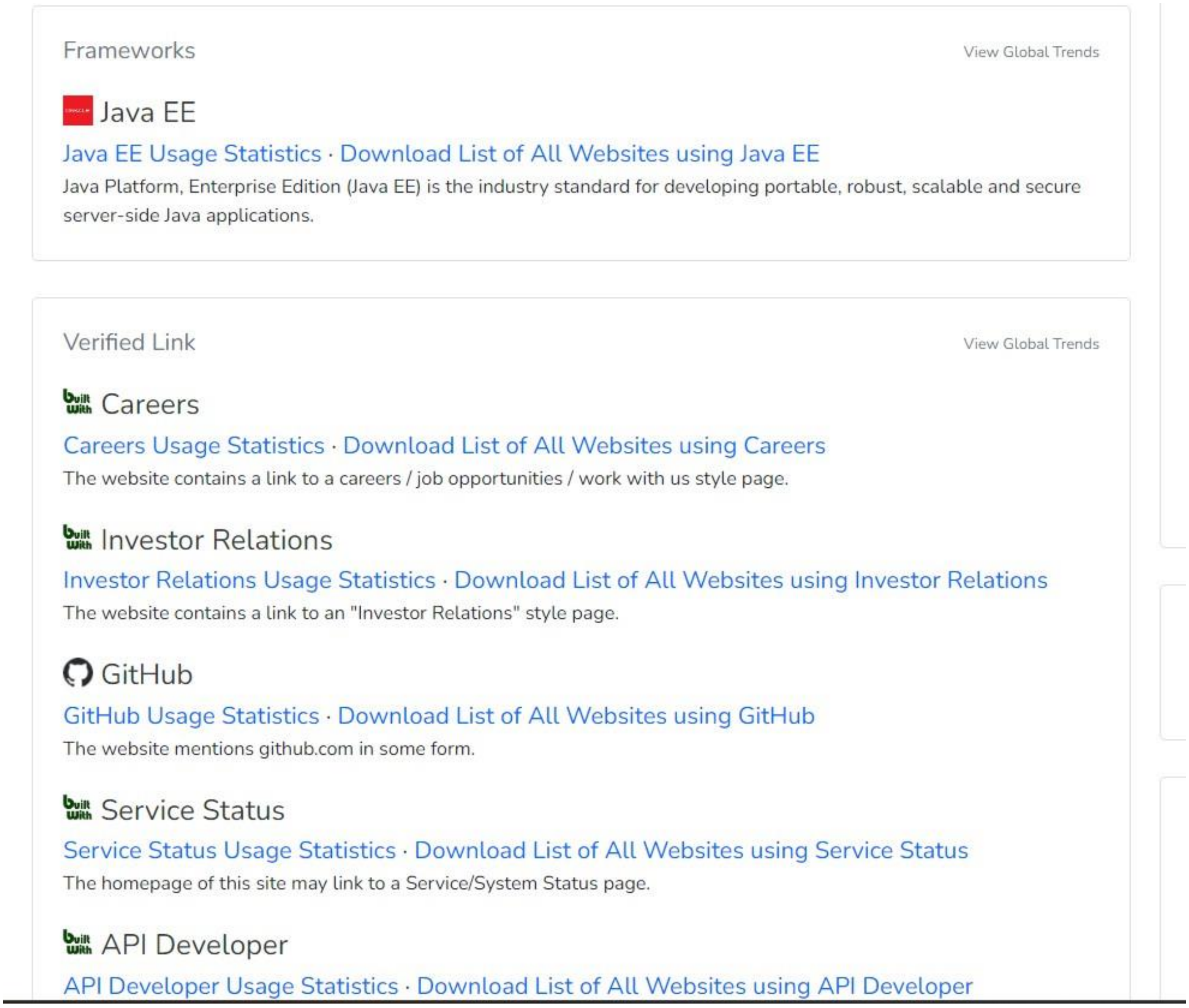
Last technology detected on 20th
We know of 19 technologies on th
technologies removed from testfir
February 2007. Link to this page.

Get a notification when testfire.net adc

Recent Lookups

whatsthescore.tv
imusindustries.com
salomon.com
100forexbrokers.com
asantebio.com
belcalli.com
kulibin.com.ua
ecotentstructure.com
weps.org
iclope.com

afnast
clockw
leadst
skinca
mesne
apexs
webcc
tcse-c
luxten
sprech



Frameworks

Java EE

Java EE Usage Statistics · Download List of All Websites using Java EE

Java Platform, Enterprise Edition (Java EE) is the industry standard for developing portable, robust, scalable and secure server-side Java applications.

Verified Link

Careers

Careers Usage Statistics · Download List of All Websites using Careers

The website contains a link to a careers / job opportunities / work with us style page.

Investor Relations

Investor Relations Usage Statistics · Download List of All Websites using Investor Relations

The website contains a link to an "Investor Relations" style page.

GitHub

GitHub Usage Statistics · Download List of All Websites using GitHub

The website mentions github.com in some form.

Service Status

Service Status Usage Statistics · Download List of All Websites using Service Status

The homepage of this site may link to a Service/System Status page.

API Developer

API Developer Usage Statistics · Download List of All Websites using API Developer

Name Server

View Global Trends

Akamai DNS

Akamai DNS Usage Statistics · Download List of All Websites using Akamai DNS

DNS services provided by Akamai.

Web Hosting Providers

View Global Trends

Rackspace

Rackspace Usage Statistics · Download List of All Websites using Rackspace

Fanatical Support web hosting from global hosting provider Rackspace, encompassing SliceHost.

US hosting · Dedicated Hosting

SSL Certificates

View Global Trends

Sectigo SSL

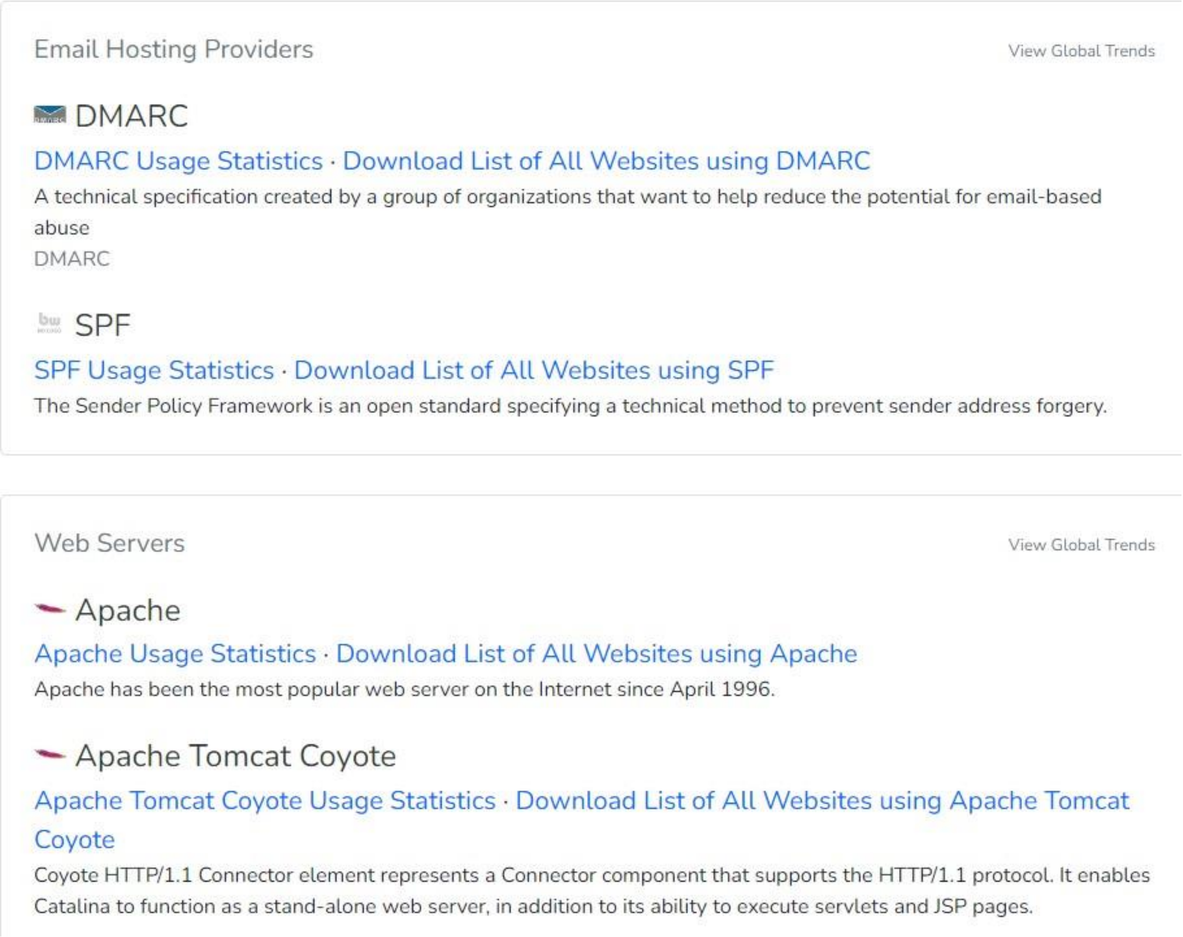
Sectigo SSL Usage Statistics · Download List of All Websites using Sectigo SSL

SSL from Sectigo formerly Comodo.

Sectigo Domain SSL

Sectigo Domain SSL Usage Statistics · Download List of All Websites using Sectigo Domain SSL

SSL registration with Sectigo (formerly Comodo CA).



Email Hosting Providers

View Global Trends

DMARC

DMARC Usage Statistics · Download List of All Websites using DMARC

A technical specification created by a group of organizations that want to help reduce the potential for email-based abuse

DMARC

SPF

SPF Usage Statistics · Download List of All Websites using SPF

The Sender Policy Framework is an open standard specifying a technical method to prevent sender address forgery.

Web Servers

View Global Trends

Apache

Apache Usage Statistics · Download List of All Websites using Apache

Apache has been the most popular web server on the Internet since April 1996.

Apache Tomcat Coyote

Apache Tomcat Coyote Usage Statistics · Download List of All Websites using Apache Tomcat Coyote

Coyote HTTP/1.1 Connector element represents a Connector component that supports the HTTP/1.1 protocol. It enables Catalina to function as a stand-alone web server, in addition to its ability to execute servlets and JSP pages.

It is hosted on Rackspace and JAVA EE is the framework.
I gathered the following information using Builtwith.