Lab 6: Perform Whois footprinting

Lab Scenario

During the footprinting process, gathering information on the target IP address and domain obtained during previous information gathering steps is important. As a professional ethical hacker or penetration tester, you should be able to perform Whois footprinting on the target; this method provides target domain information such as the owner, its registrar, registration details, name server, contact information, etc. Using this information, you can create a map of the organization’s network, perform social engineering attacks, and obtain internal details of the network.

Lab Objectives

- Perform Whois lookup using DomainTools

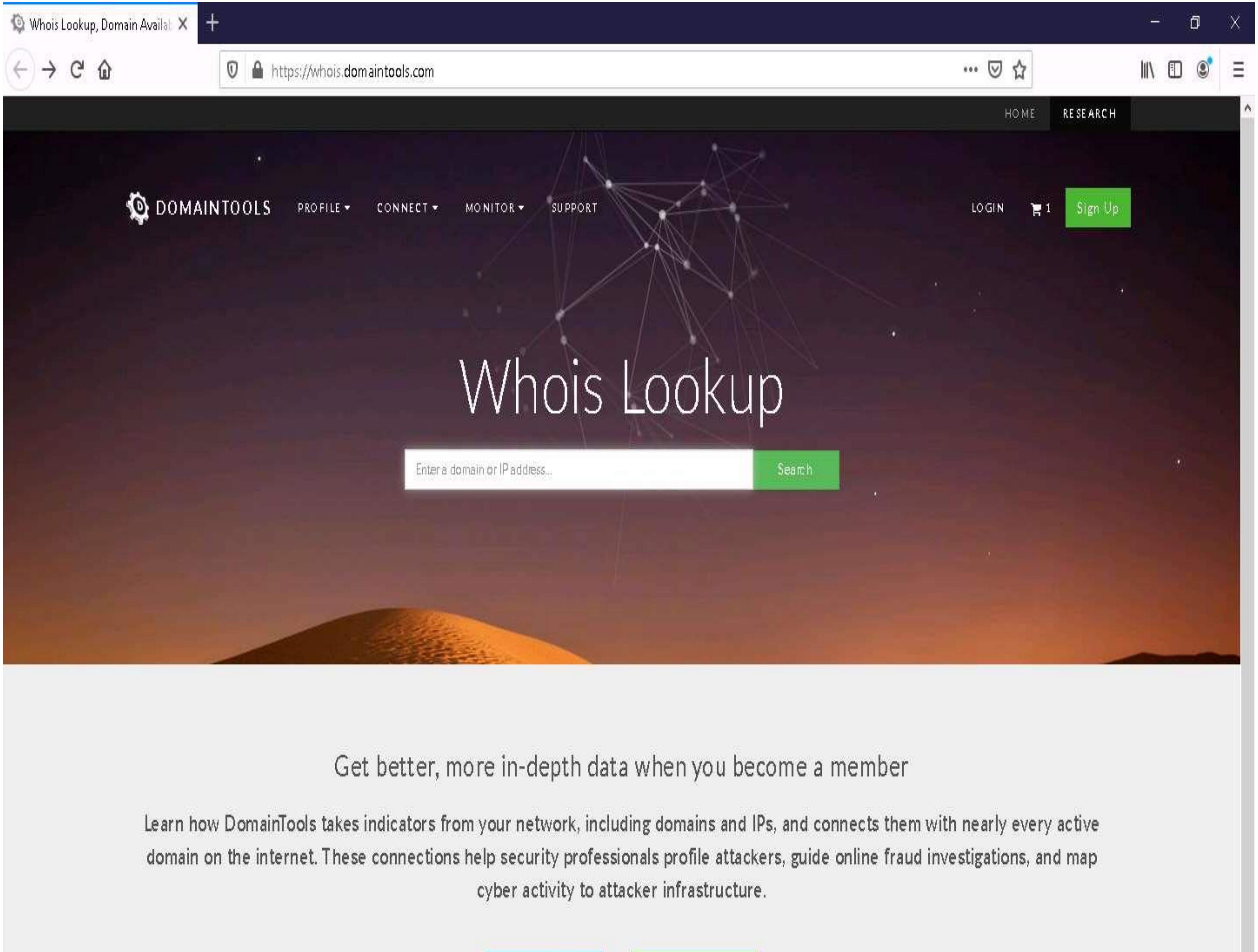
Overview of Whois Footprinting

This lab focuses on how to perform a Whois lookup and analyze the results. Whois is a query and response protocol used for 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. This protocol listens to requests on port 43 (TCP). Regional Internet Registries (RIRs) maintain Whois databases, and contains the personal information of domain owners. For each resource, the Whois database provides text records with information about the resource itself and relevant information of assignees, registrants, and administrative information (creation and expiration dates).

Task 1: Perform Whois Lookup using DomainTools

Here, we will gather target information by performing Whois lookup using DomainTools.

1. □ Open any web browser (here, **Mozilla Firefox**). In the address bar of the browser place your mouse cursor, click http://whois.domaintools.com and press **Enter**. The Whois Lookup website appears, as shown in the screenshot.



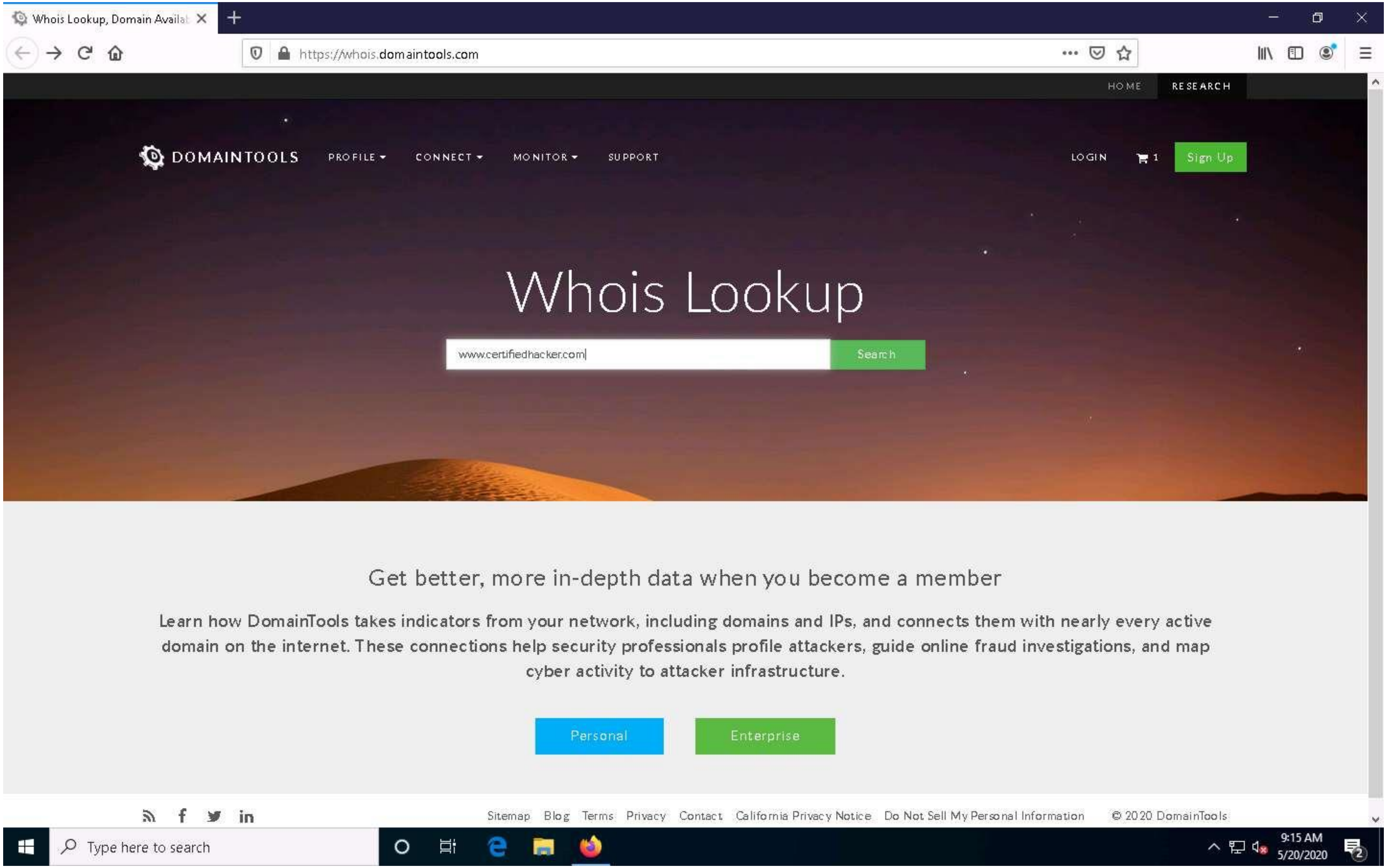
Whois Lookup, Domain Availal
https://whois.domaintools.com
HOME
RESEARCH
DOMAINTOOLS
PROFILE ▾
CONNECT ▾
MONITOR ▾
SUPPORT
LOGIN
1
Sign Up
Enter a domain or IP address...
Search

Whois Lookup

Get better, more in-depth data when you become a member

Learn how DomainTools takes indicators from your network, including domains and IPs, and connects them with nearly every active domain on the internet. These connections help security professionals profile attackers, guide online fraud investigations, and map cyber activity to attacker infrastructure.

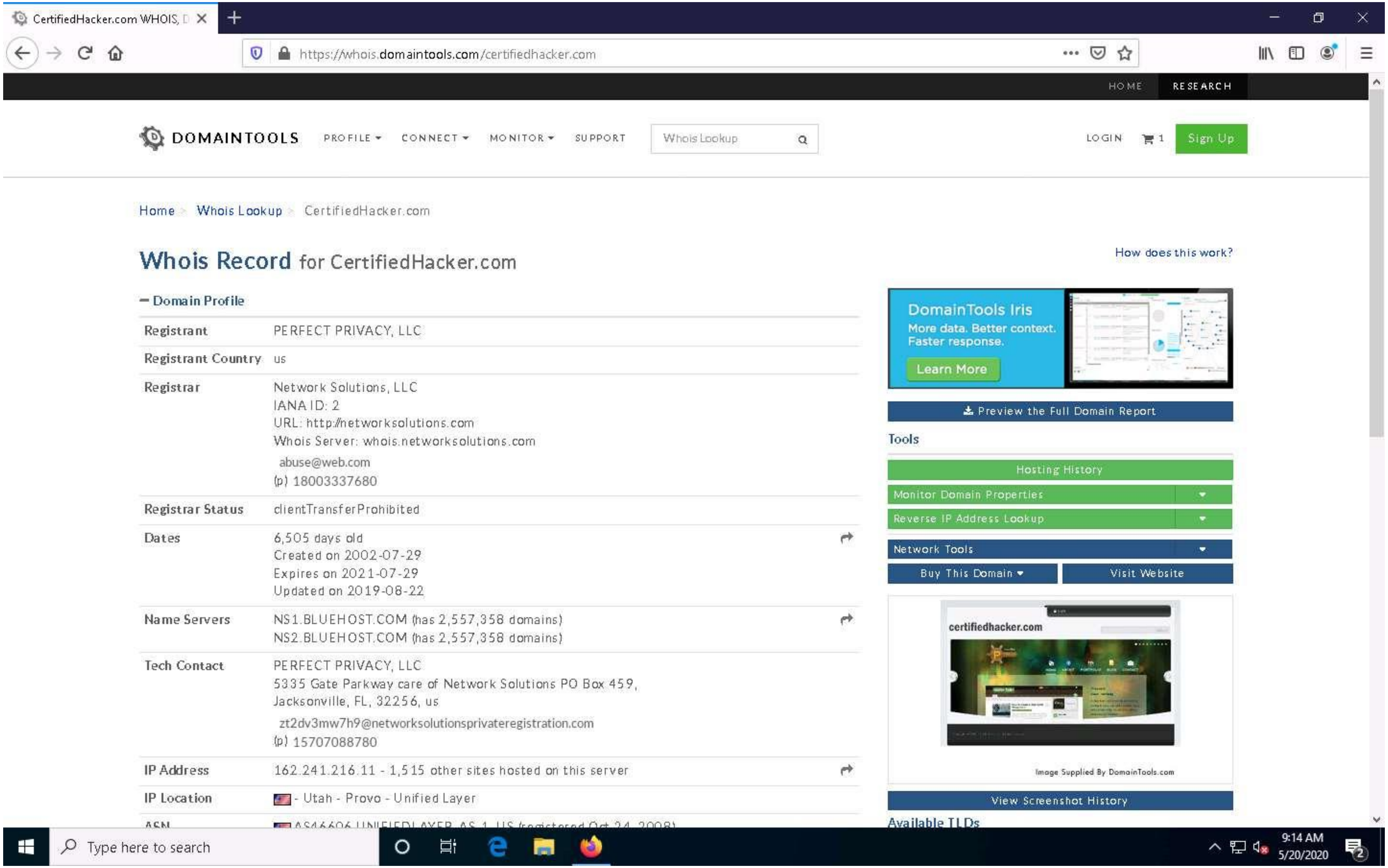
2. □ Now, in the **Enter a domain or IP address...** search bar, type **www.certifiedhacker.com** and click **Search**.



Get better, more in-depth data when you become a member

Learn how DomainTools takes indicators from your network, including domains and IPs, and connects them with nearly every active domain on the internet. These connections help security professionals profile attackers, guide online fraud investigations, and map cyber activity to attacker infrastructure.

3. □ This search result reveals the details associated with the URL entered, **www.certifiedhacker.com**, which includes organizational details such as registration details, name servers, IP address, location, etc., as shown in the screenshots.

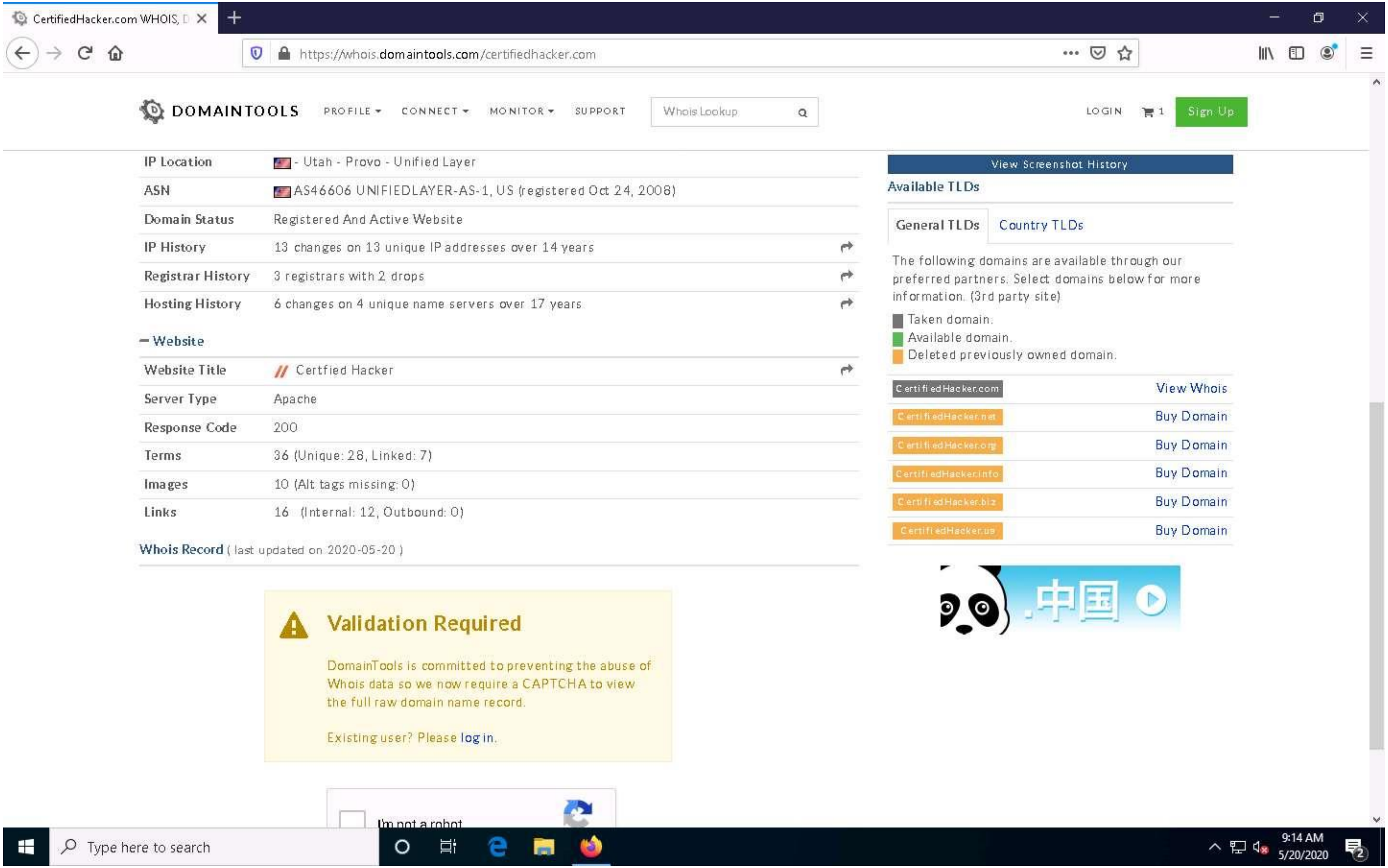


CertifiedHacker.com WHOIS, D
https://whois.domaintools.com/certifiedhacker.com
HOME
RESEARCH
DOMAINTOOLS
PROFILE
CONNECT
MONITOR
SUPPORT
Whois Lookup
LOGIN
1
Sign Up
Home > Whois Lookup > CertifiedHacker.com
How does this work?
DomainTools Iris
More data. Better context. Faster response.
Learn More
Preview the Full Domain Report
Tools
Hosting History
Monitor Domain Properties
Reverse IP Address Lookup
Network Tools
Buy This Domain
Visit Website
certifiedhacker.com
Image Supplied By DomainTools.com
View Screenshot History
Available TLDs
Type here to search
9:14 AM
5/20/2020

Whois Record for CertifiedHacker.com

− Domain Profile

Registrant	PERFECT PRIVACY, LLC
Registrant Country	us
Registrar	Network Solutions, LLC IANA ID: 2 URL: http://networksolutions.com Whois Server: whois.networksolutions.com abuse@web.com (p) 18003337680
Registrar Status	clientTransferProhibited
Dates	6,505 days old Created on 2002-07-29 Expires on 2021-07-29 Updated on 2019-08-22
Name Servers	NS1.BLUEHOST.COM (has 2,557,358 domains) NS2.BLUEHOST.COM (has 2,557,358 domains)
Tech Contact	PERFECT PRIVACY, LLC 5335 Gate Parkway care of Network Solutions PO Box 459, Jacksonville, FL, 32256, us zt2dv3mw7h9@networksolutionsprivateregistration.com (p) 15707088780
IP Address	162.241.216.11 - 1,515 other sites hosted on this server
IP Location	- Utah - Provo - Unified Layer
ASN	AS46606 UNIFIEDLAYER-AS-1 - US (registered Oct 24, 2008)



IP Location	- Utah - Provo - Unified Layer
ASN	AS46606 UNIFIEDLAYER-AS-1, US (registered Oct 24, 2008)
Domain Status	Registered And Active Website
IP History	13 changes on 13 unique IP addresses over 14 years
Registrar History	3 registrars with 2 drops
Hosting History	6 changes on 4 unique name servers over 17 years

— Website

Website Title	Certfied Hacker
Server Type	Apache
Response Code	200
Terms	36 (Unique: 28, Linked: 7)
Images	10 (Alt tags missing: 0)
Links	16 (Internal: 12, Outbound: 0)

Whois Record (last updated on 2020-05-20)

Validation Required

DomainTools is committed to preventing the abuse of Whois data so we now require a CAPTCHA to view the full raw domain name record.

Existing user? Please log in.

□ I'm not a robot

View Screenshot History

Available TLDs

General TLDs | Country TLDs

The following domains are available through our preferred partners. Select domains below for more information. (3rd party site)

■ Taken domain.
🟩 Available domain.
🟧 Deleted previously owned domain.

CertifiedHacker.com	View Whois
CertifiedHacker.net	Buy Domain
CertifiedHacker.org	Buy Domain
CertifiedHacker.info	Buy Domain
CertifiedHacker.biz	Buy Domain
CertifiedHacker.us	Buy Domain

4. □ This concludes the demonstration of gathering information about a target organization by performing the Whois lookup using DomainTools.

5. □ You can also use other Whois lookup tools such as **SmartWhois** (https://www.tamos.com), **Batch IP Converter** (http://www.sabsoft.com), etc. to extract additional target Whois information.
6. □ Close all open windows and document all the acquired information.