Roll no:- T075

Sign:-

Name:- Chakradhar dwivedi

Practical no:- 1

Aim:- Use who is for Reconnaissance

* Reconnaissance

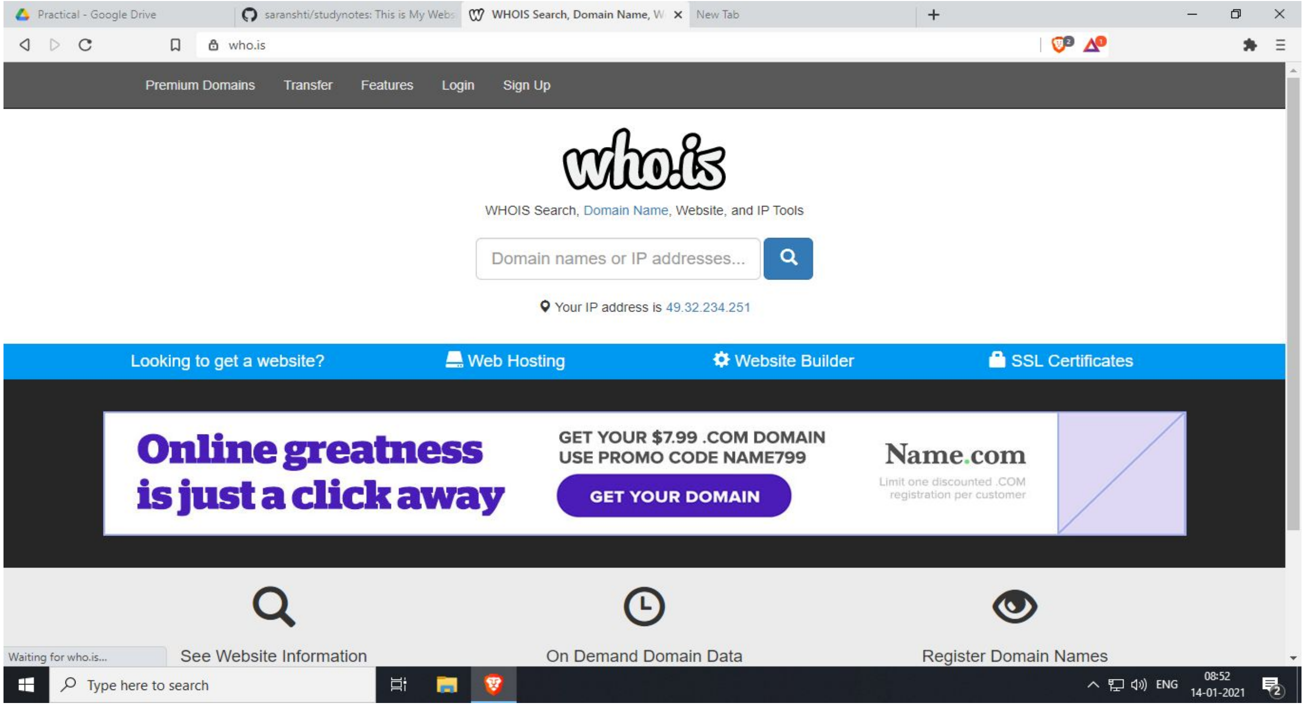
Information gathering & getting to known the target system is the first Process in ethical hacking Reconnaissance is a set of Processes and techniques (Foot printing) used to coverty discover and collect information about a target system During reconnaissance an ethical hacker attempts to gather on much information about a target system as possible following the seven steps listed below

(1) Gather initial information
(2) Determine the network range
(3) Identify active machines
(4) Discover open parts and access points
(5) Fingerprint the operating system
(6) Uncover services on parts
(7) Map the network

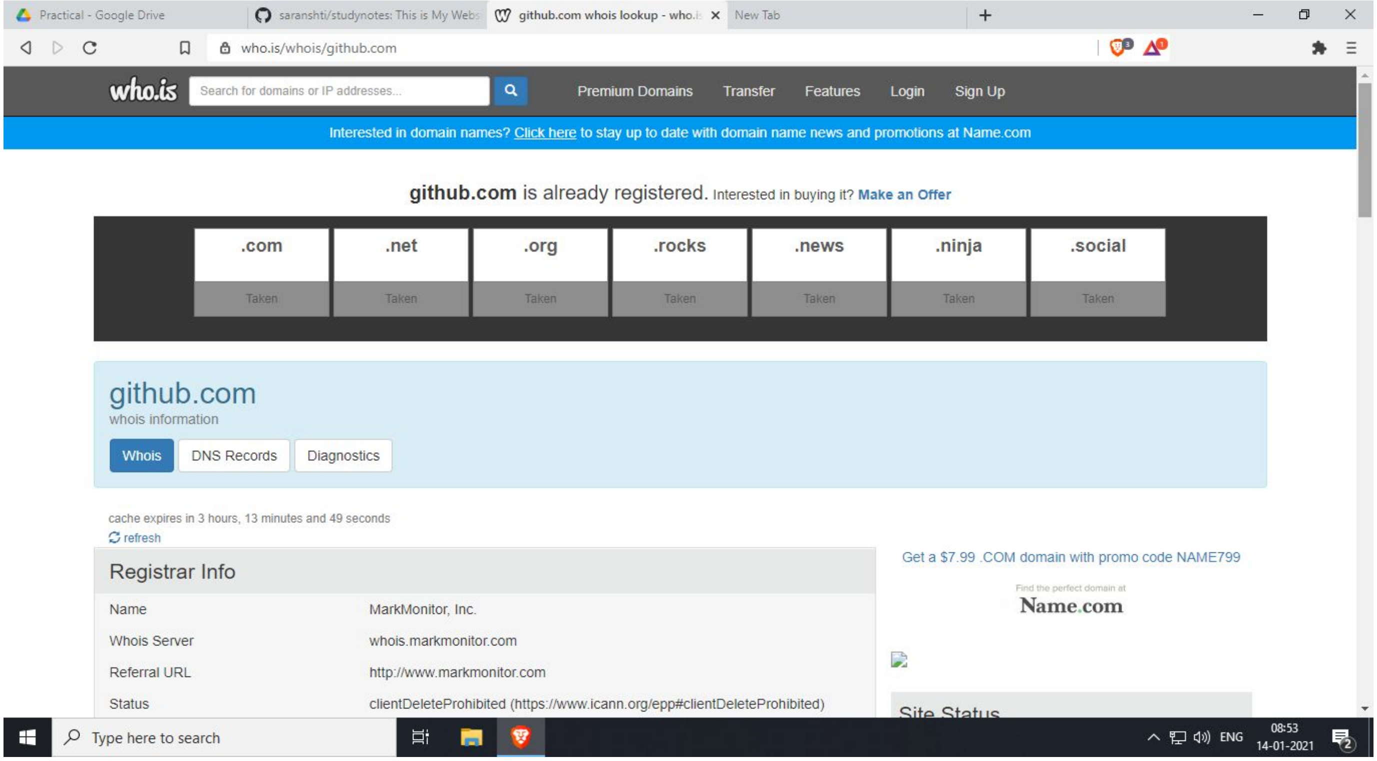
Practical No.1

Aim:- Use who.is for reconnaissance.

Step1: Open Browser and Search “who.is” and Open.


Practical - Google Drive
saranshti/studynotes: This is My Webs
WHOIS Search, Domain Name, W
New Tab
who.is
Premium Domains
Transfer
Features
Login
Sign Up
who.is
WHOIS Search, Domain Name, Website, and IP Tools
Domain names or IP addresses...
Your IP address is 49.32.234.251
Looking to get a website?
Web Hosting
Website Builder
SSL Certificates
Online greatness is just a click away
GET YOUR $7.99 .COM DOMAIN
USE PROMO CODE NAME799
GET YOUR DOMAIN
Name.com
Limit one discounted .COM registration per customer
See Website Information
On Demand Domain Data
Register Domain Names
Waiting for who.is...
Type here to search
ENG
08:52
14-01-2021

Step 2: Search the domain which you want to reconnaissance.


Practical - Google Drive
saranshti/studynotes: This is My Webs
github.com whois lookup - who.is
New Tab
who.is/whois/github.com
who.is
Search for domains or IP addresses...
Premium Domains
Transfer
Features
Login
Sign Up
Interested in domain names? Click here to stay up to date with domain name news and promotions at Name.com
.com Taken
.net Taken
.org Taken
.rocks Taken
.news Taken
.ninja Taken
.social Taken
Whois
DNS Records
Diagnostics
Get a $7.99 .COM domain with promo code NAME799
Find the perfect domain at Name.com
Site Status
Type here to search
ENG
08:53
14-01-2021

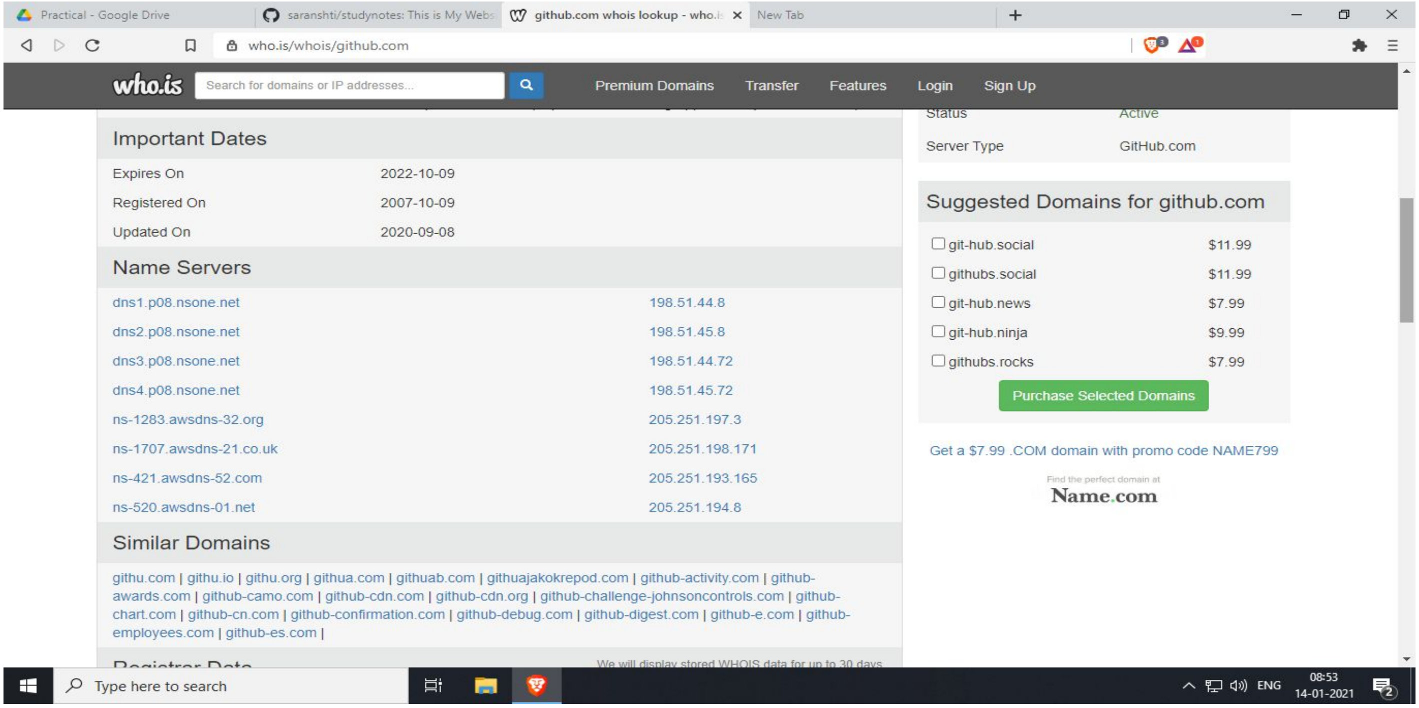
github.com is already registered. Interested in buying it? Make an Offer

github.com
whois information

cache expires in 3 hours, 13 minutes and 49 seconds
refresh

Registrar Info

Name	MarkMonitor, Inc.
Whois Server	whois.markmonitor.com
Referral URL	http://www.markmonitor.com
Status	clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)



Status	Active
Server Type	GitHub.com

Important Dates

Expires On	2022-10-09
Registered On	2007-10-09
Updated On	2020-09-08

Name Servers

dns1.p08.nsone.net	198.51.44.8
dns2.p08.nsone.net	198.51.45.8
dns3.p08.nsone.net	198.51.44.72
dns4.p08.nsone.net	198.51.45.72
ns-1283.awsdns-32.org	205.251.197.3
ns-1707.awsdns-21.co.uk	205.251.198.171
ns-421.awsdns-52.com	205.251.193.165
ns-520.awsdns-01.net	205.251.194.8

Similar Domains

githu.com | githu.io | githu.org | githua.com | githuab.com | githuajakokrepod.com | github-activity.com | github-awards.com | github-camo.com | github-cdn.com | github-cdn.org | github-challenge-johnsoncontrols.com | github-chart.com | github-cn.com | github-confirmation.com | github-debug.com | github-digest.com | github-e.com | github-employees.com | github-es.com |

Registrar Data

We will display stored WHOIS data for up to 30 days.

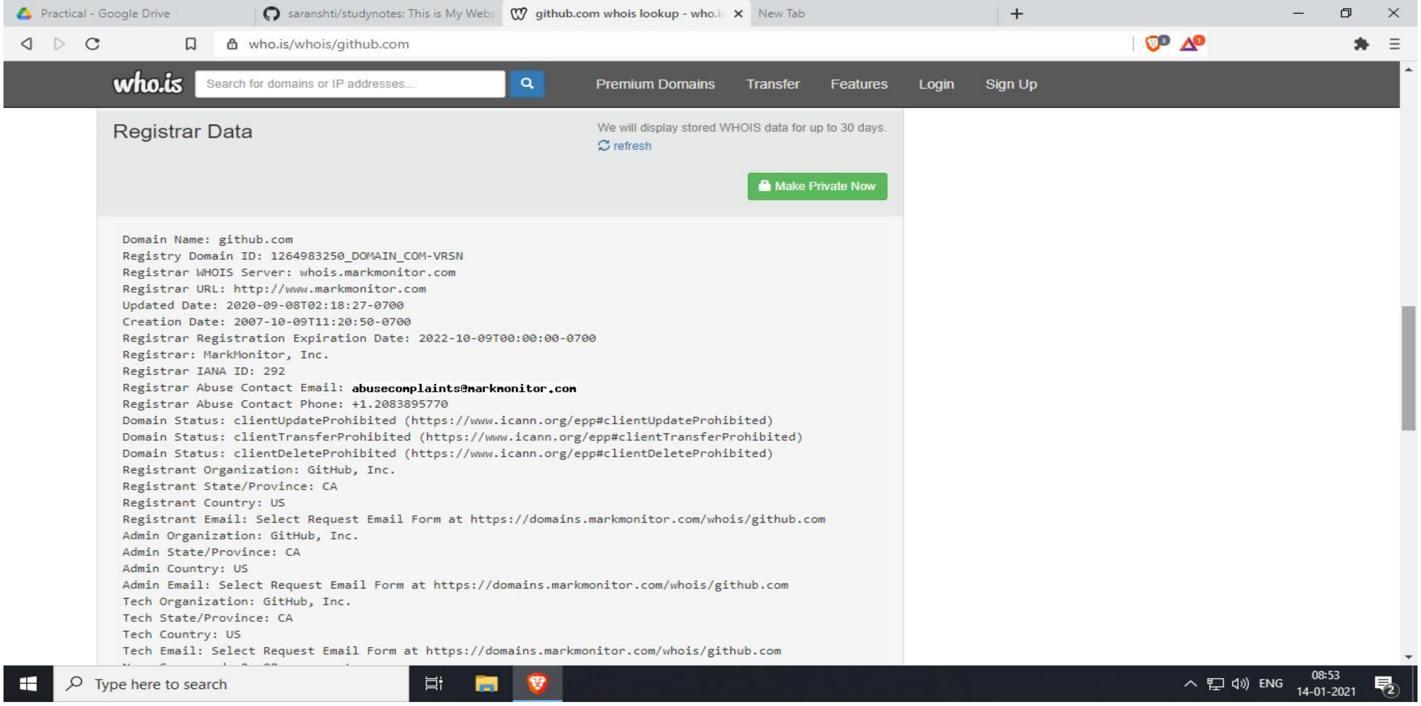
Suggested Domains for github.com

□ git-hub.social	$11.99
□ githubs.social	$11.99
□ git-hub.news	$7.99
□ git-hub.ninja	$9.99
□ githubs.rocks	$7.99

Purchase Selected Domains

Get a $7.99 .COM domain with promo code NAME799

Find the perfect domain at Name.com

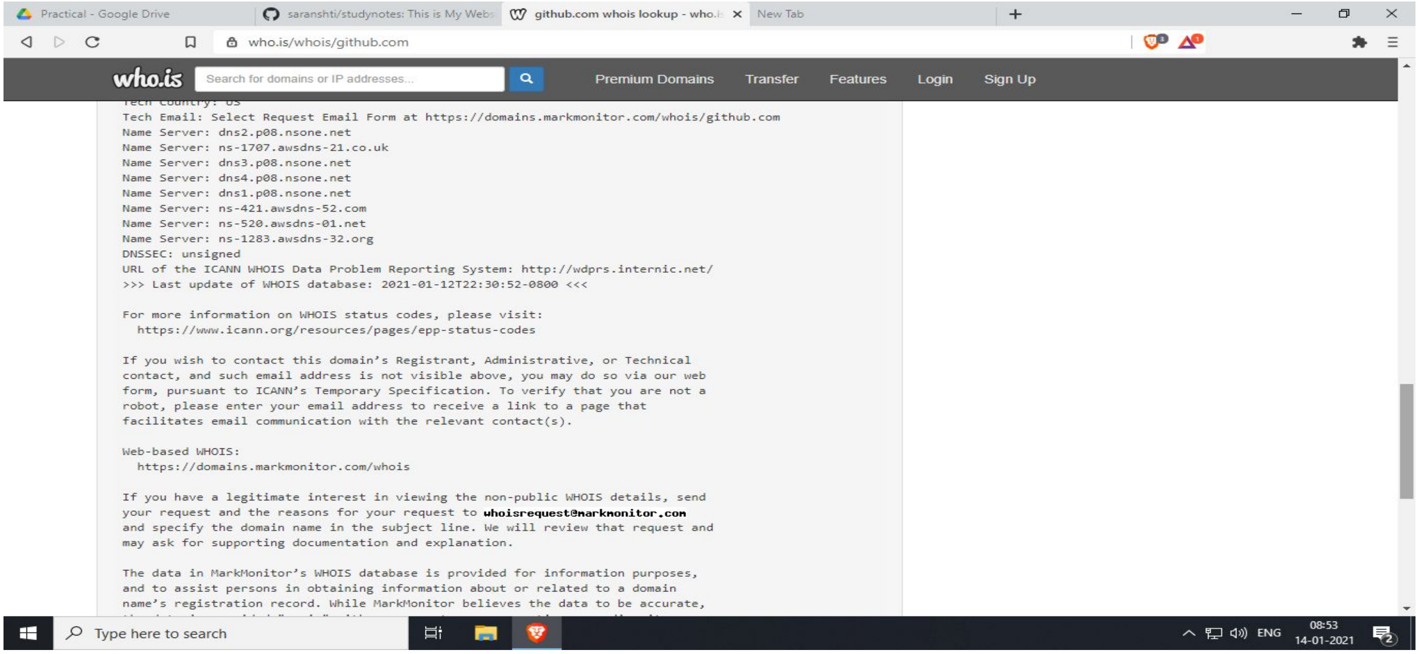


Registrar Data

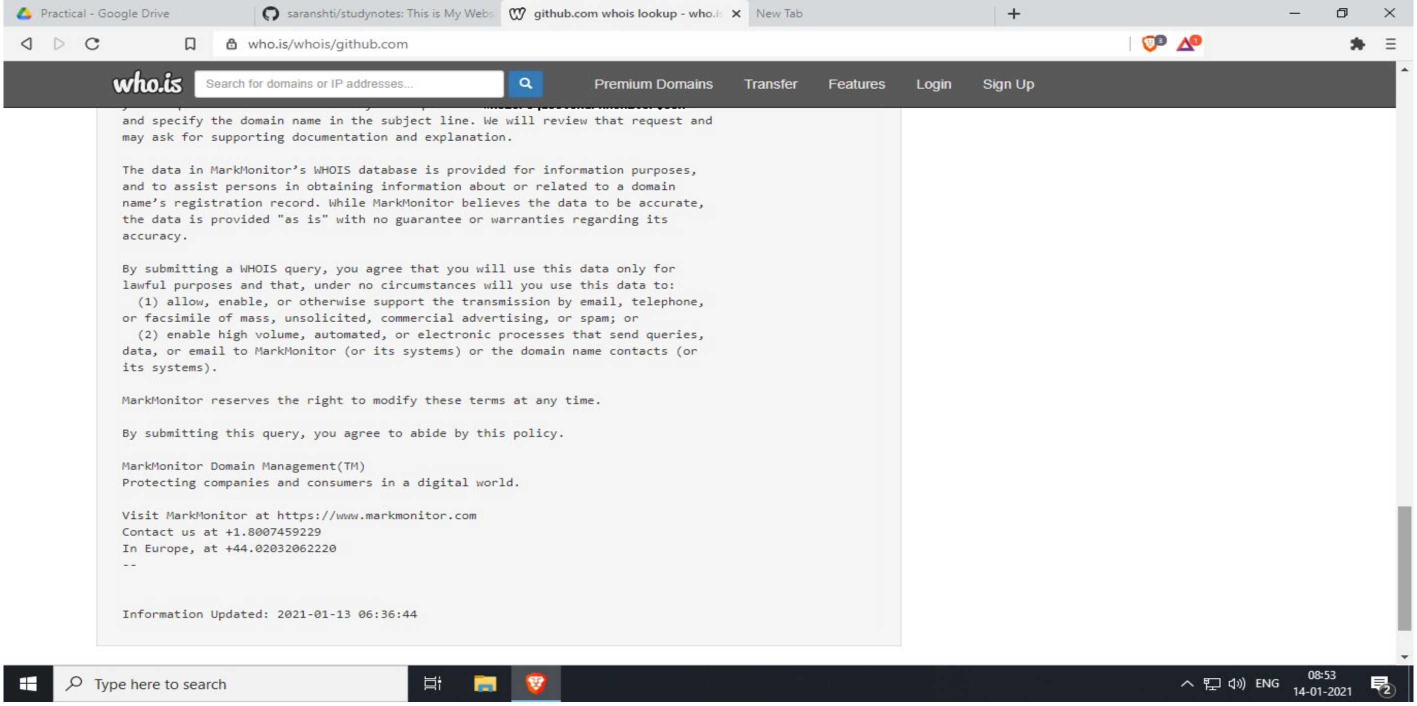
We will display stored WHOIS data for up to 30 days.
refresh

Make Private Now

```
Domain Name: github.com
Registry Domain ID: 1264983250_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2020-09-08T02:18:27-0700
Creation Date: 2007-10-09T11:20:50-0700
Registrar Registration Expiration Date: 2022-10-09T00:00:00-0700
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895770
Domain Status: clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)
Domain Status: clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited)
Domain Status: clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)
Registrant Organization: GitHub, Inc.
Registrant State/Province: CA
Registrant Country: US
Registrant Email: Select Request Email Form at https://domains.markmonitor.com/whois/github.com
Admin Organization: GitHub, Inc.
Admin State/Province: CA
Admin Country: US
Admin Email: Select Request Email Form at https://domains.markmonitor.com/whois/github.com
Tech Organization: GitHub, Inc.
Tech State/Province: CA
Tech Country: US
Tech Email: Select Request Email Form at https://domains.markmonitor.com/whois/github.com
```

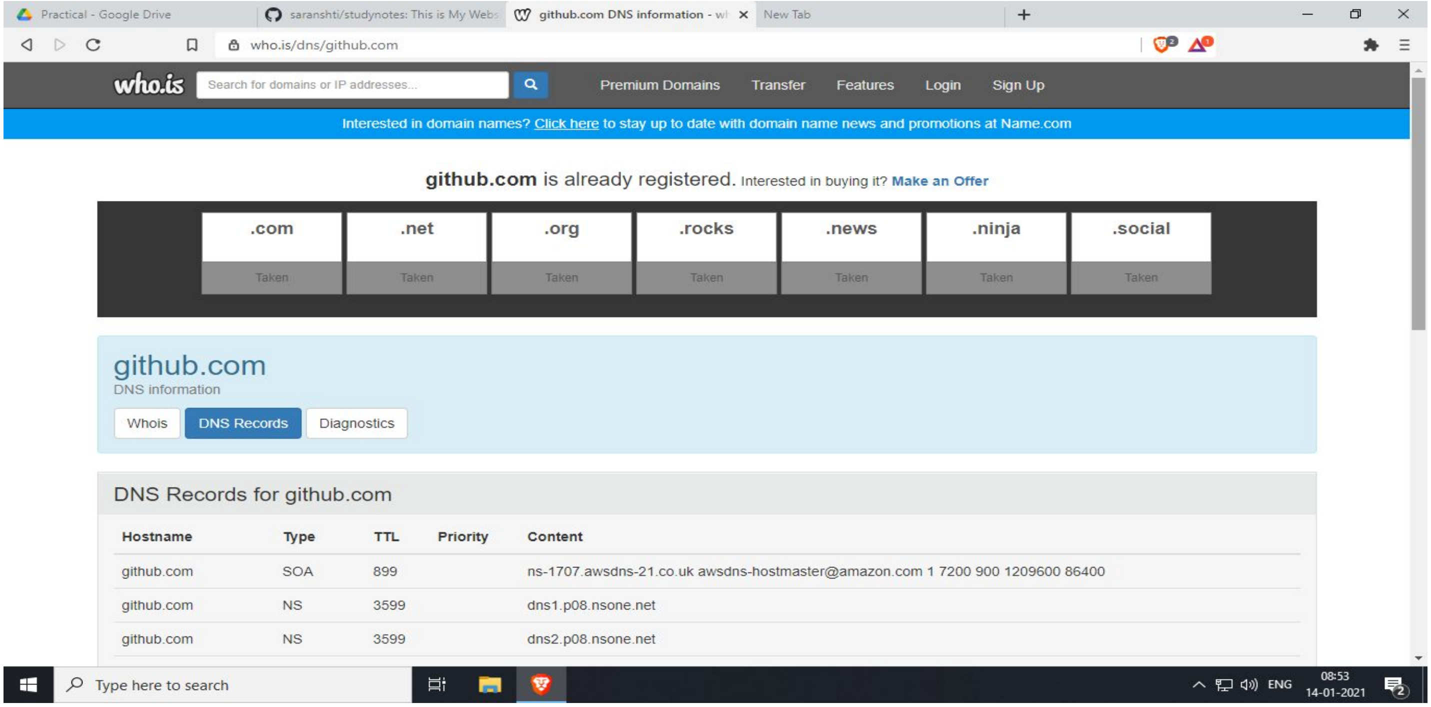


```
Tech Country: US
Tech Email: Select Request Email Form at https://domains.markmonitor.com/whois/github.com
Name Server: dns2.p08.nsone.net
Name Server: ns-1707.awsdns-21.co.uk
Name Server: dns3.p08.nsone.net
Name Server: dns4.p08.nsone.net
Name Server: dns1.p08.nsone.net
Name Server: ns-421.awsdns-52.com
Name Server: ns-520.awsdns-01.net
Name Server: ns-1283.awsdns-32.org
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2021-01-12T22:30:52-0800 <<<

For more information on WHOIS status codes, please visit:
  https://www.icann.org/resources/pages/epp-status-codes

If you wish to contact this domain's Registrant, Administrative, or Technical
contact, and such email address is not visible above, you may do so via our web
form, pursuant to ICANN's Temporary Specification. To verify that you are not a
robot, please enter your email address to receive a link to a page that
facilitates email communication with the relevant contact(s).

Web-based WHOIS:
  https://domains.markmonitor.com/whois

If you have a legitimate interest in viewing the non-public WHOIS details, send
your request and the reasons for your request to whoisrequest@markmonitor.com
and specify the domain name in the subject line. We will review that request and
may ask for supporting documentation and explanation.

The data in MarkMonitor's WHOIS database is provided for information purposes,
and to assist persons in obtaining information about or related to a domain
name's registration record. While MarkMonitor believes the data to be accurate,
```



```
and specify the domain name in the subject line. We will review that request and
may ask for supporting documentation and explanation.

The data in MarkMonitor's WHOIS database is provided for information purposes,
and to assist persons in obtaining information about or related to a domain
name's registration record. While MarkMonitor believes the data to be accurate,
the data is provided "as is" with no guarantee or warranties regarding its
accuracy.

By submitting a WHOIS query, you agree that you will use this data only for
lawful purposes and that, under no circumstances will you use this data to:
  (1) allow, enable, or otherwise support the transmission by email, telephone,
or facsimile of mass, unsolicited, commercial advertising, or spam; or
  (2) enable high volume, automated, or electronic processes that send queries,
data, or email to MarkMonitor (or its systems) or the domain name contacts (or
its systems).

MarkMonitor reserves the right to modify these terms at any time.

By submitting this query, you agree to abide by this policy.

MarkMonitor Domain Management(TM)
Protecting companies and consumers in a digital world.

Visit MarkMonitor at https://www.markmonitor.com
Contact us at +1.8007459229
In Europe, at +44.02032062220
--


Information Updated: 2021-01-13 06:36:44
```

Step 3: Go to the DNS Records Section.



Interested in domain names? Click here to stay up to date with domain name news and promotions at Name.com

github.com is already registered. Interested in buying it? **Make an Offer**

.com	.net	.org	.rocks	.news	.ninja	.social
Taken	Taken	Taken	Taken	Taken	Taken	Taken

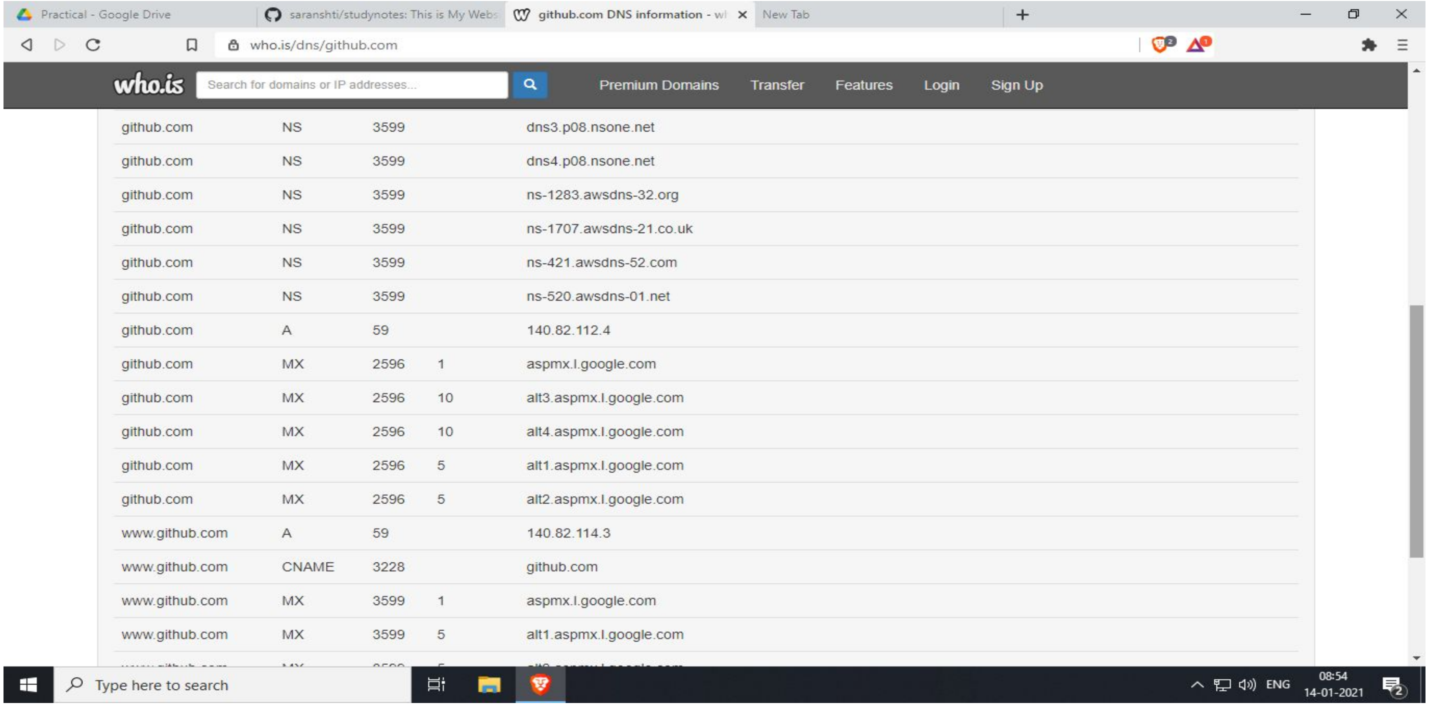
github.com

DNS information

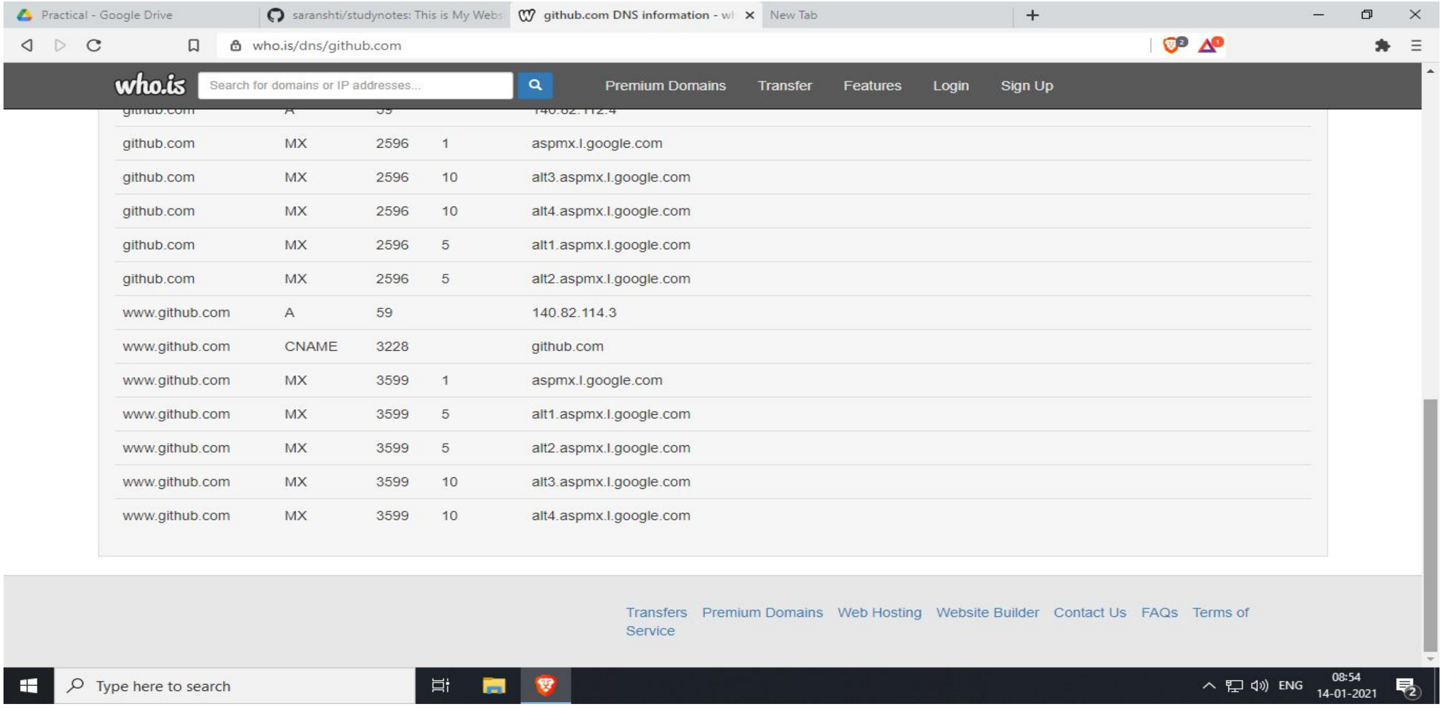
Whois | DNS Records | Diagnostics

DNS Records for github.com

Hostname	Type	TTL	Priority	Content
github.com	SOA	899		ns-1707.awsdns-21.co.uk awsdns-hostmaster@amazon.com 1 7200 900 1209600 86400
github.com	NS	3599		dns1.p08.nsone.net
github.com	NS	3599		dns2.p08.nsone.net



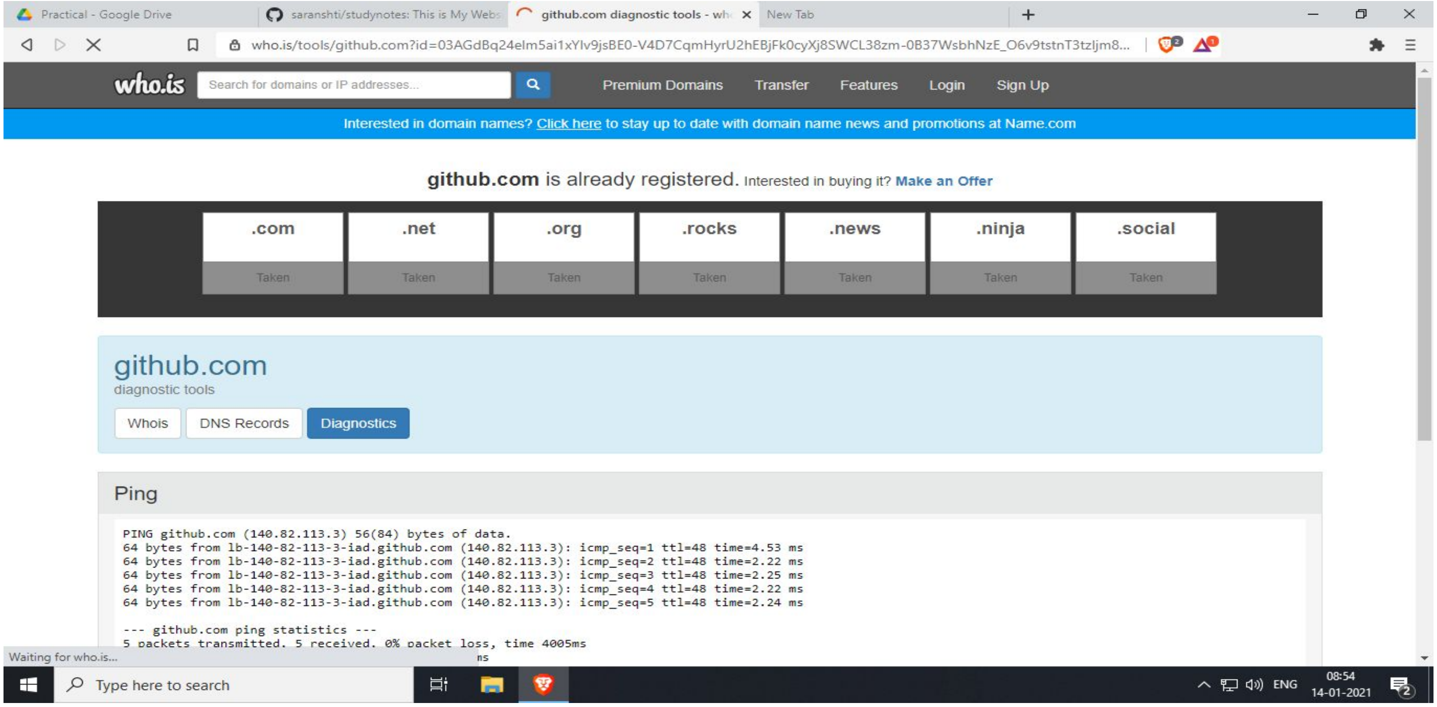
github.com	NS	3599		dns3.p08.nsone.net
github.com	NS	3599		dns4.p08.nsone.net
github.com	NS	3599		ns-1283.awsdns-32.org
github.com	NS	3599		ns-1707.awsdns-21.co.uk
github.com	NS	3599		ns-421.awsdns-52.com
github.com	NS	3599		ns-520.awsdns-01.net
github.com	A	59		140.82.112.4
github.com	MX	2596	1	aspmx.l.google.com
github.com	MX	2596	10	alt3.aspmx.l.google.com
github.com	MX	2596	10	alt4.aspmx.l.google.com
github.com	MX	2596	5	alt1.aspmx.l.google.com
github.com	MX	2596	5	alt2.aspmx.l.google.com
www.github.com	A	59		140.82.114.3
www.github.com	CNAME	3228		github.com
www.github.com	MX	3599	1	aspmx.l.google.com
www.github.com	MX	3599	5	alt1.aspmx.l.google.com



Practical - Google Drive
saranshti/studynotes: This is My Webs
github.com DNS information - wh
New Tab
who.is/dns/github.com
who.is
Search for domains or IP addresses...
Premium Domains
Transfer
Features
Login
Sign Up

github.com	A	59		140.82.112.4
github.com	MX	2596	1	aspmx.l.google.com
github.com	MX	2596	10	alt3.aspmx.l.google.com
github.com	MX	2596	10	alt4.aspmx.l.google.com
github.com	MX	2596	5	alt1.aspmx.l.google.com
github.com	MX	2596	5	alt2.aspmx.l.google.com
www.github.com	A	59		140.82.114.3
www.github.com	CNAME	3228		github.com
www.github.com	MX	3599	1	aspmx.l.google.com
www.github.com	MX	3599	5	alt1.aspmx.l.google.com
www.github.com	MX	3599	5	alt2.aspmx.l.google.com
www.github.com	MX	3599	10	alt3.aspmx.l.google.com
www.github.com	MX	3599	10	alt4.aspmx.l.google.com

Step 4: Go to the diagnostics Section.



Practical - Google Drive
saranshti/studynotes: This is My Webs
github.com diagnostic tools - wh
New Tab
who.is/tools/github.com?id=03AGdBq24elm5ai1xYlv9jsBE0-V4D7CqmHyrU2hEBjFk0cyXj8SWCL38zm-0B37WsbhNzE_O6v9tstnT3tzljm8...
who.is
Search for domains or IP addresses...
Premium Domains
Transfer
Features
Login
Sign Up

Interested in domain names? Click here to stay up to date with domain name news and promotions at Name.com

github.com is already registered. Interested in buying it? **Make an Offer**

.com	.net	.org	.rocks	.news	.ninja	.social
Taken	Taken	Taken	Taken	Taken	Taken	Taken

github.com

diagnostic tools

Whois
DNS Records
Diagnostics

Ping

```
PING github.com (140.82.113.3) 56(84) bytes of data.
64 bytes from lb-140-82-113-3-iad.github.com (140.82.113.3): icmp_seq=1 ttl=48 time=4.53 ms
64 bytes from lb-140-82-113-3-iad.github.com (140.82.113.3): icmp_seq=2 ttl=48 time=2.22 ms
64 bytes from lb-140-82-113-3-iad.github.com (140.82.113.3): icmp_seq=3 ttl=48 time=2.25 ms
64 bytes from lb-140-82-113-3-iad.github.com (140.82.113.3): icmp_seq=4 ttl=48 time=2.22 ms
64 bytes from lb-140-82-113-3-iad.github.com (140.82.113.3): icmp_seq=5 ttl=48 time=2.24 ms

--- github.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
```