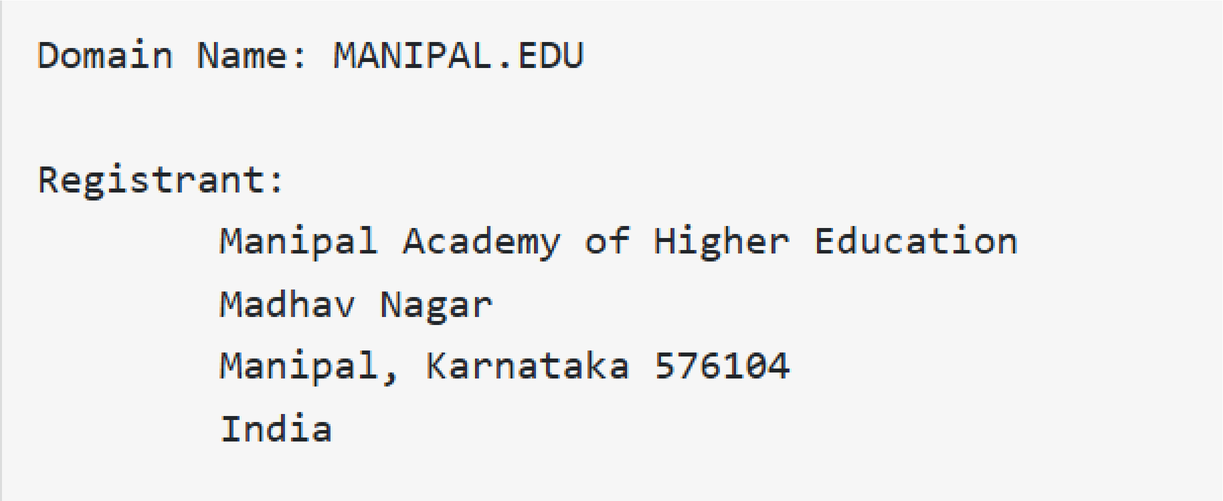
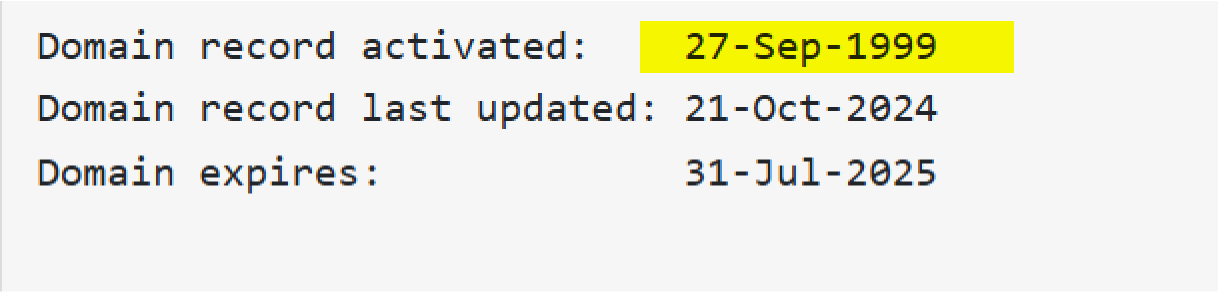
LAB 6

Who is the domain registrar of www.manipal.edu?



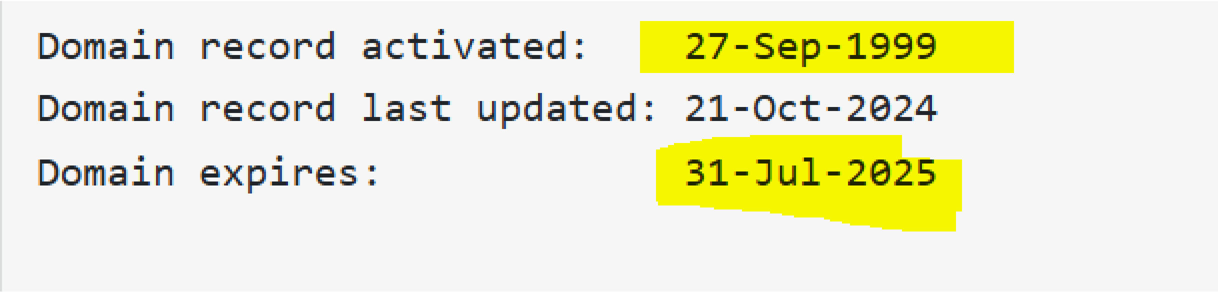
```
Domain Name: MANIPAL.EDU

Registrant:
        Manipal Academy of Higher Education
        Madhav Nagar
        Manipal, Karnataka 576104
        India
```

What is the domain creation date?



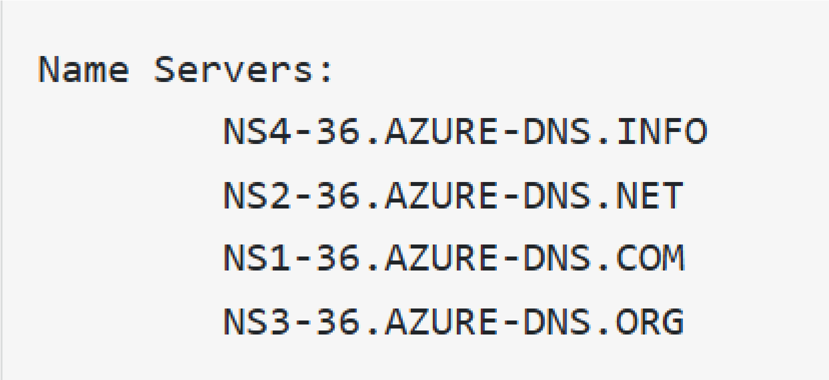
```
Domain record activated:    27-Sep-1999
Domain record last updated: 21-Oct-2024
Domain expires:             31-Jul-2025
```

What is the expiration date of the domain?



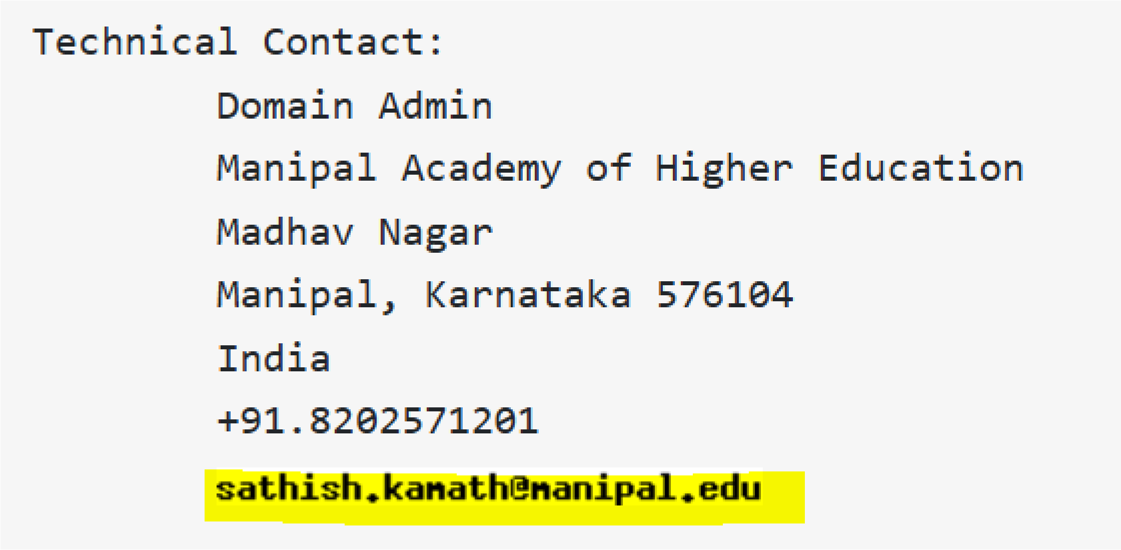
```
Domain record activated:    27-Sep-1999
Domain record last updated: 21-Oct-2024
Domain expires:             31-Jul-2025
```

Identify the name servers associated with the domain.



```
Name Servers:
          NS4-36.AZURE-DNS.INFO
          NS2-36.AZURE-DNS.NET
          NS1-36.AZURE-DNS.COM
          NS3-36.AZURE-DNS.ORG
```

Is there any contact email provided for administrative or technical support?

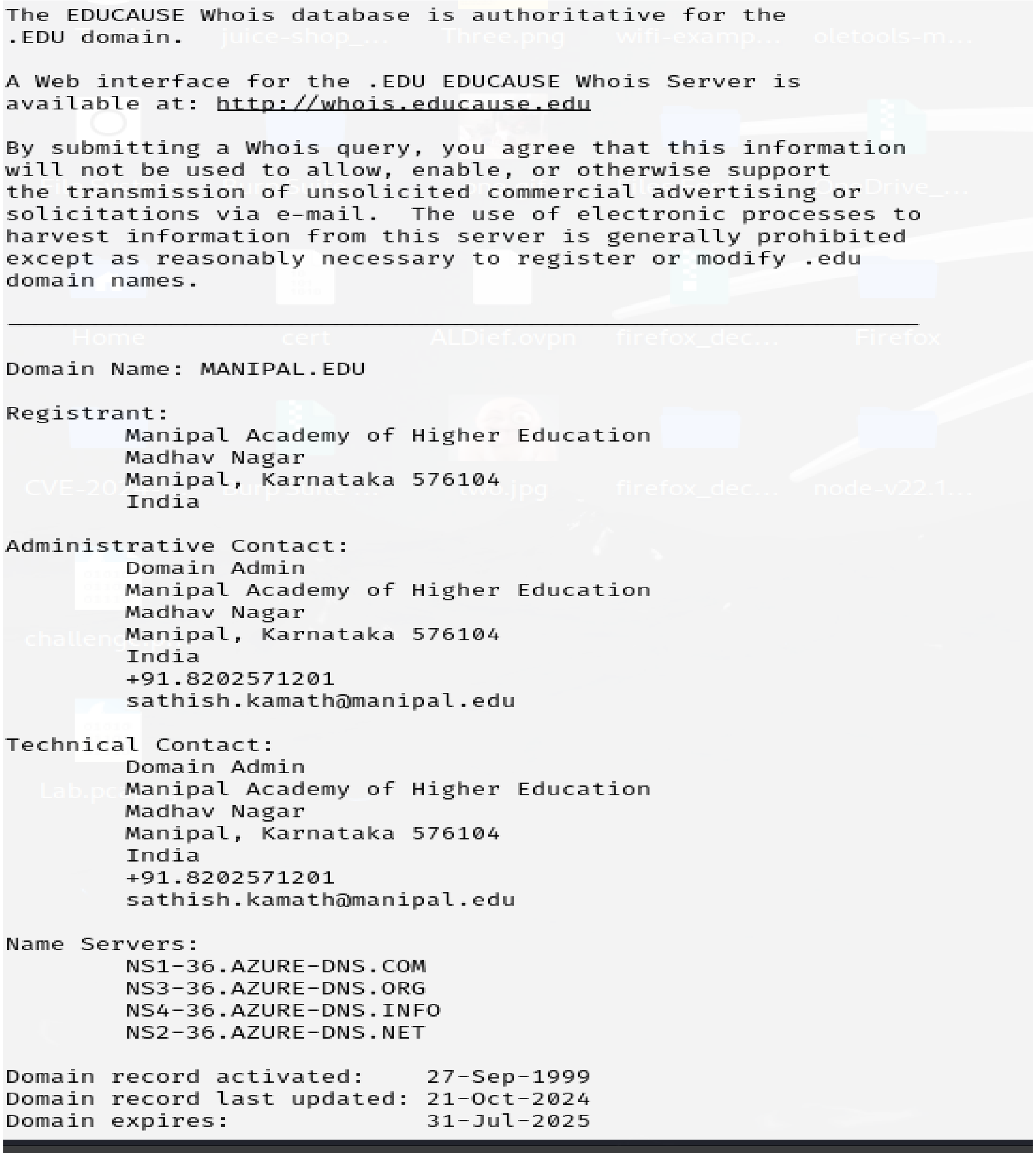


```
Technical Contact:
          Domain Admin
          Manipal Academy of Higher Education
          Madhav Nagar
          Manipal, Karnataka 576104
          India
          +91.8202571201
          sathish.kamath@manipal.edu
```

What country is the domain registered in?

India

Run a WHOIS query for example.com and check if the registrant's details (name, address, email) are visible.



```
The EDUCAUSE Whois database is authoritative for the
.EDU domain.

A Web interface for the .EDU EDUCAUSE Whois Server is
available at: http://whois.educause.edu

By submitting a Whois query, you agree that this information
will not be used to allow, enable, or otherwise support
the transmission of unsolicited commercial advertising or
solicitations via e-mail.  The use of electronic processes to
harvest information from this server is generally prohibited
except as reasonably necessary to register or modify .edu
domain names.

-------------------------------------------------------------

Domain Name: MANIPAL.EDU

Registrant:
        Manipal Academy of Higher Education
        Madhav Nagar
        Manipal, Karnataka 576104
        India

Administrative Contact:
        Domain Admin
        Manipal Academy of Higher Education
        Madhav Nagar
        Manipal, Karnataka 576104
        India
        +91.8202571201
        sathish.kamath@manipal.edu

Technical Contact:
        Domain Admin
        Manipal Academy of Higher Education
        Madhav Nagar
        Manipal, Karnataka 576104
        India
        +91.8202571201
        sathish.kamath@manipal.edu

Name Servers:
        NS1-36.AZURE-DNS.COM
        NS3-36.AZURE-DNS.ORG
        NS4-36.AZURE-DNS.INFO
        NS2-36.AZURE-DNS.NET

Domain record activated:    27-Sep-1999
Domain record last updated: 21-Oct-2024
Domain expires:             31-Jul-2025
```

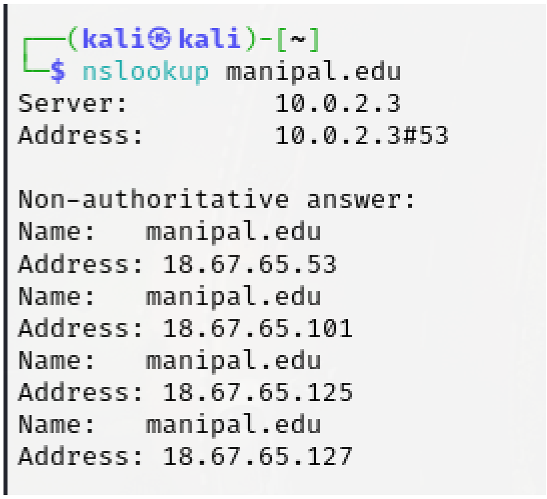
If privacy protection is enabled, what information is displayed instead of actual owner details?

Address, technical person and his contact details

What are the security implications of exposing or hiding data?

Exposing the data will lead to phishing attacks, brute force attacks and social engineering attacks . Hiding the data we make full stop for all of these by, we cannot verify the legitimacy of the website.

Look for Name Server (NS) records and associated domains.



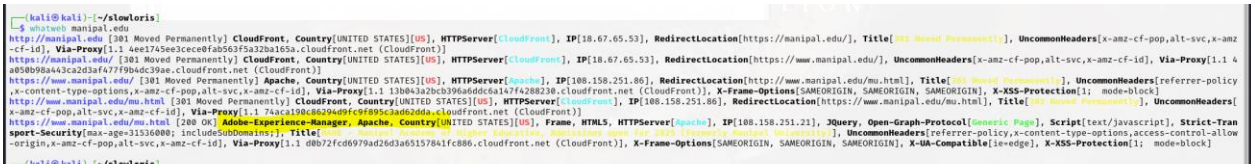
```
┌──(kali㉿kali)-[~]
└─$ nslookup manipal.edu
Server:         10.0.2.3
Address:        10.0.2.3#53

Non-authoritative answer:
Name:   manipal.edu
Address: 18.67.65.53
Name:   manipal.edu
Address: 18.67.65.101
Name:   manipal.edu
Address: 18.67.65.125
Name:   manipal.edu
Address: 18.67.65.127
```

what are the different methods to find the subdomain using both passive and active methods

for passive method we can use google dorking where for active method we can use gobuster, ffuf etc

Identify CMS (WordPress, Joomla, etc.) and frameworks used.

Here manipal.edu using Adobe Experience manager



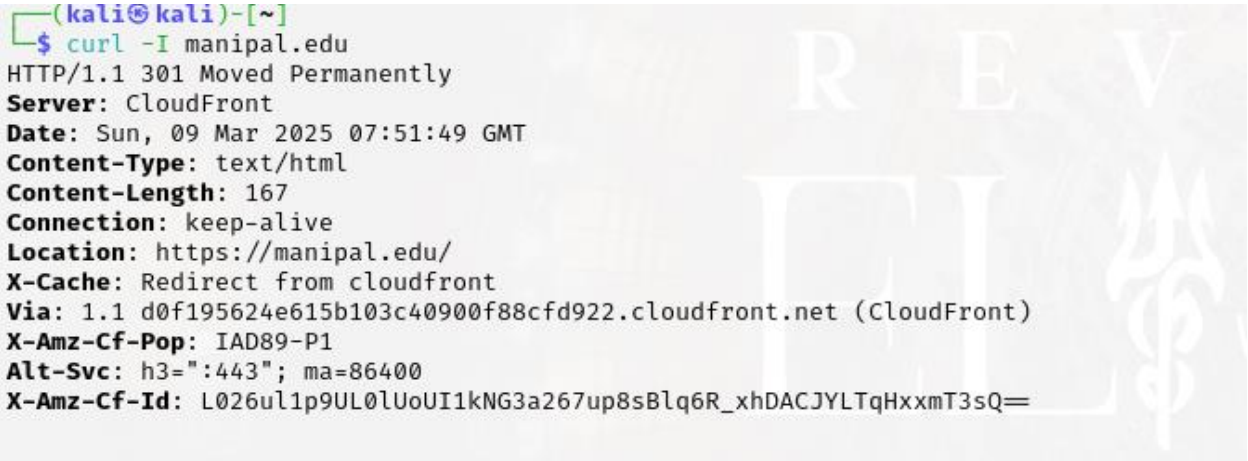
```
┌──(kali㉿kali)-[~/slowloris]
└─$ whatweb manipal.edu
http://manipal.edu [301 Moved Permanently] CloudFront, Country[UNITED STATES][US], HTTPServer[CloudFront], IP[18.67.65.53], RedirectLocation[https://manipal.edu/], Title[301 Moved Permanently], UncommonHeaders[x-amz-cf-pop,alt-svc,x-amz
-cf-id], Via-Proxy[1.1 4ee1745ee3cece0fab563f5a32ba165a.cloudfront.net (CloudFront)]
https://manipal.edu/ [301 Moved Permanently] CloudFront, Country[UNITED STATES][US], HTTPServer[CloudFront], IP[18.67.65.53], RedirectLocation[https://www.manipal.edu/], UncommonHeaders[x-amz-cf-pop,alt-svc,x-amz-cf-id], Via-Proxy[1.1 4
a050b98a443ca2d3af477f9b4dc39ae.cloudfront.net (CloudFront)]
https://www.manipal.edu/ [301 Moved Permanently] Apache, Country[UNITED STATES][US], HTTPServer[Apache], IP[108.158.251.86], RedirectLocation[http://www.manipal.edu/mu.html], Title[301 Moved Permanently], UncommonHeaders[referrer-policy
,x-content-type-options,x-amz-cf-pop,alt-svc,x-amz-cf-id], Via-Proxy[1.1 13b043a2bcb396a6ddc6a147f4288230.cloudfront.net (CloudFront)], X-Frame-Options[SAMEORIGIN, SAMEORIGIN, SAMEORIGIN], X-XSS-Protection[1;  mode=block]
http://www.manipal.edu/mu.html [301 Moved Permanently] CloudFront, Country[UNITED STATES][US], HTTPServer[CloudFront], IP[108.158.251.86], RedirectLocation[https://www.manipal.edu/mu.html], Title[301 Moved Permanently], UncommonHeaders[
x-amz-cf-pop,alt-svc,x-amz-cf-id], Via-Proxy[1.1 74aca190c86294d9fc9f895c3ad62dda.cloudfront.net (CloudFront)]
https://www.manipal.edu/mu.html [200 OK] Adobe-Experience-Manager, Apache, Country[UNITED STATES][US], Frame, HTML5, HTTPServer[Apache], IP[108.158.251.21], JQuery, Open-Graph-Protocol[Generic Page], Script[text/javascript], Strict-Tran
sport-Security[max-age=31536000; includeSubDomains;], Title[MAHE - Manipal Academy of Higher Education, Admissions open for 2025 (formerly Manipal University)], UncommonHeaders[referrer-policy,x-content-type-options,access-control-allow
-origin,x-amz-cf-pop,alt-svc,x-amz-cf-id], Via-Proxy[1.1 d0b72fcd6979ad26d3a65157841fc886.cloudfront.net (CloudFront)], X-Frame-Options[SAMEORIGIN, SAMEORIGIN, SAMEORIGIN], X-UA-Compatible[ie=edge], X-XSS-Protection[1;  mode=block]

┌──(kali㉿kali)-[~/slowloris]
```

compare whatweb and wappalyzer

whatweb is a command line tool where are wapplyzer is a browser extension

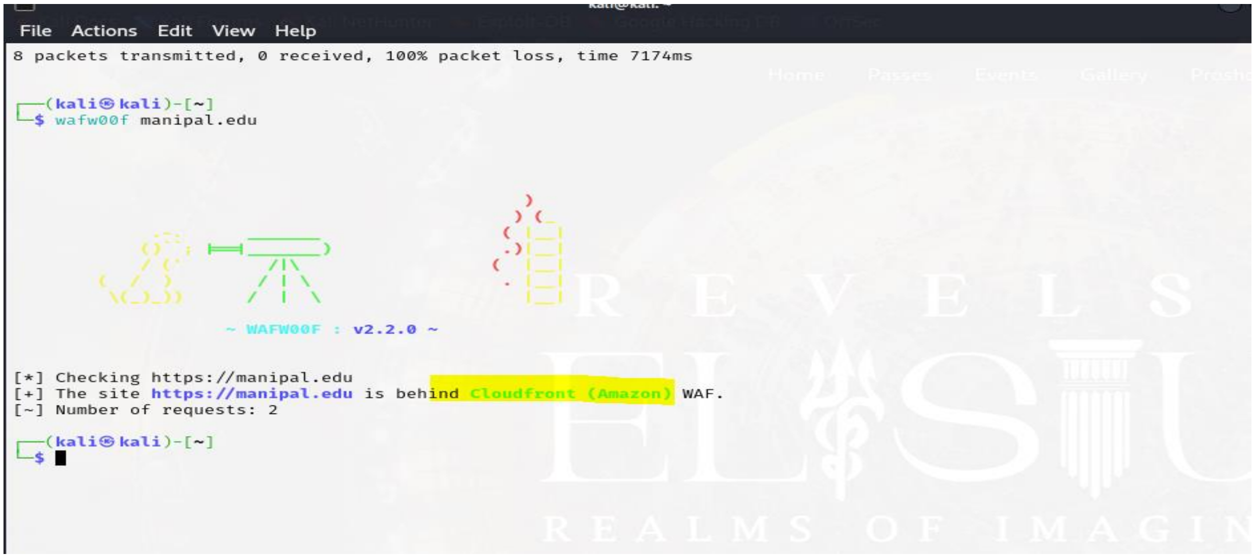
Fetch the HTTP Header (Many methods are available). Identify the tools used to find HTTP Header details

the tool use here is curl -I manipal.edu



```
┌──(kali㉿kali)-[~]
└─$ curl -I manipal.edu
HTTP/1.1 301 Moved Permanently
Server: CloudFront
Date: Sun, 09 Mar 2025 07:51:49 GMT
Content-Type: text/html
Content-Length: 167
Connection: keep-alive
Location: https://manipal.edu/
X-Cache: Redirect from cloudfront
Via: 1.1 d0f195624e615b103c40900f88cfd922.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: IAD89-P1
Alt-Svc: h3=":443"; ma=86400
X-Amz-Cf-Id: L026ul1p9UL0lUoUI1kNG3a267up8sBlq6R_xhDACJYLTqHxxmT3sQ==
```

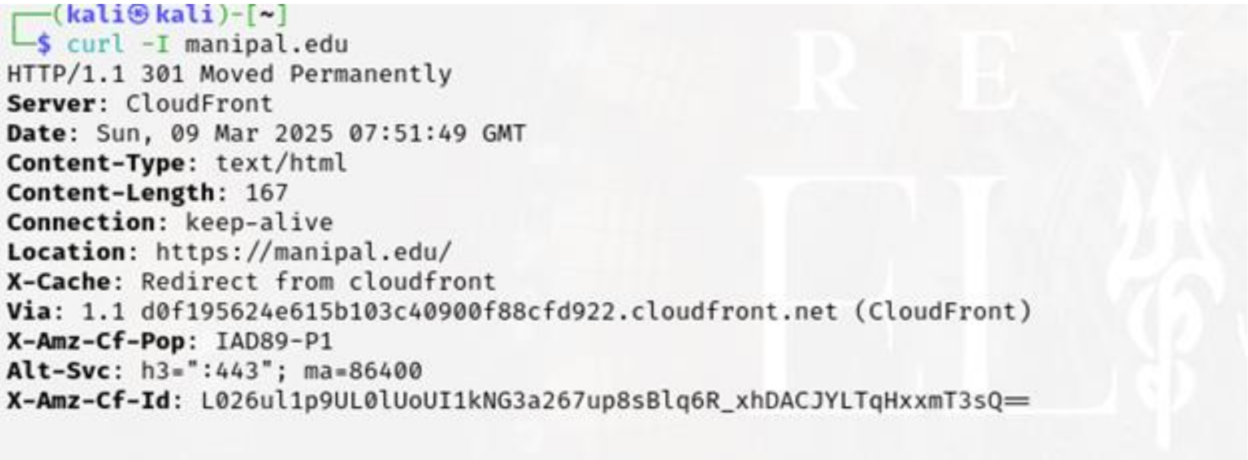
Check whether domain have firewall installed or not



```
8 packets transmitted, 0 received, 100% packet loss, time 7174ms

┌──(kali㉿kali)-[~]
└─$ wafw00f manipal.edu

                ~ WAFW00F : v2.2.0 ~

[*] Checking https://manipal.edu
[+] The site https://manipal.edu is behind Cloudfront (Amazon) WAF.
[~] Number of requests: 2

┌──(kali㉿kali)-[~]
└─$ █
```

do they have load balancer

By analyzing http header we can see that there is a record via
here manipal website is using cloudfront



```
┌──(kali㉿kali)-[~]
└─$ curl -I manipal.edu
HTTP/1.1 301 Moved Permanently
Server: CloudFront
Date: Sun, 09 Mar 2025 07:51:49 GMT
Content-Type: text/html
Content-Length: 167
Connection: keep-alive
Location: https://manipal.edu/
X-Cache: Redirect from cloudfront
Via: 1.1 d0f195624e615b103c40900f88cfd922.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: IAD89-P1
Alt-Svc: h3=":443"; ma=86400
X-Amz-Cf-Id: L026ul1p9UL0lUoUI1kNG3a267up8sBlq6R_xhDACJYLTqHxxmT3sQ==
```