Incident Report

DNS Service Unreachable Preventing Website Access

Prepared By: Adnan Khan

Role: Cybersecurity Student

Date: August 3, 2025

Contact: adnankprofesstional@gmail.com

1. Incident Summary

Users reported they were unable to access the website www.yummyrecipesforme.com. When trying to load the page, they received a "destination port unreachable" error. As a cybersecurity student, I investigated the issue to determine the root cause.

Using Wireshark, I captured network traffic while attempting to access the website. The analysis showed that the DNS service was unreachable, which prevented the domain name from being resolved to an IP address. Without this step, the browser cannot connect — making the website appear "down" even if it’s working.

2. Tools and Methods Used

Wireshark – To capture and analyze network packets
Command Prompt – To run network commands
nslookup – To test DNS resolution
netsh – To change DNS settings for testing
ipconfig /flushdns – To clear the local DNS cache

3. How I Reproduced the Issue

To simulate the problem, I followed these steps:

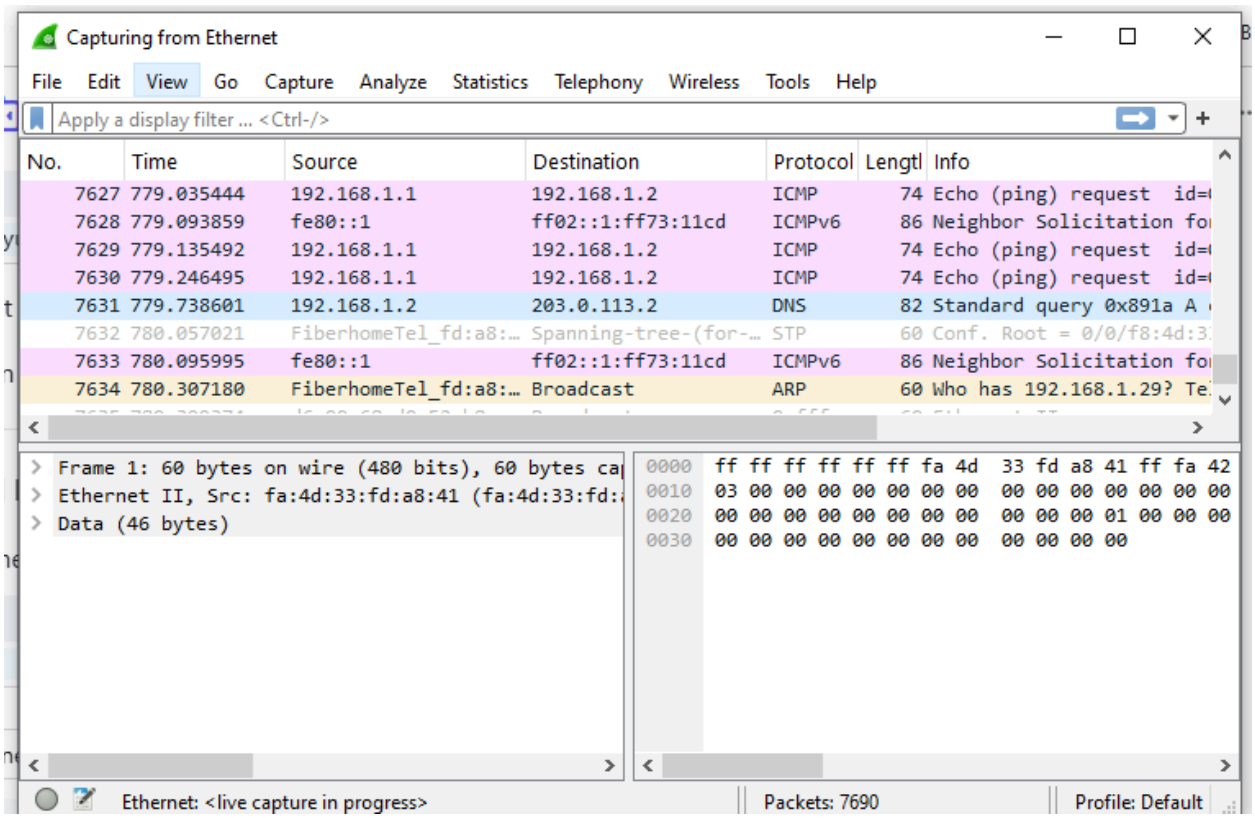
Changed DNS Server

I used this command to set a fake DNS server:

```
C:\Windows\system32>netsh interface show interface

Admin State    State          Type             Interface Name
-------------------------------------------------------------------------
Enabled        Connected      Dedicated        Ethernet


C:\Windows\system32>netsh interface ip set dns "Ethernet" static 203.0.113.2

The configured DNS server is incorrect or does not exist.
```

Started Wireshark Capture

Opened Wireshark and began capturing packets on my Wi-Fi interface.



nslookup www.yummyrecipesforme.com

This forces the system to ask the DNS server for the website's IP.

```
C:\Windows\system32>nslookup www.yummyrecipesforme.com
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  203.0.113.2

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Request to UnKnown timed-out

C:\Windows\system32>
```

Stopped Capture and Analyzed

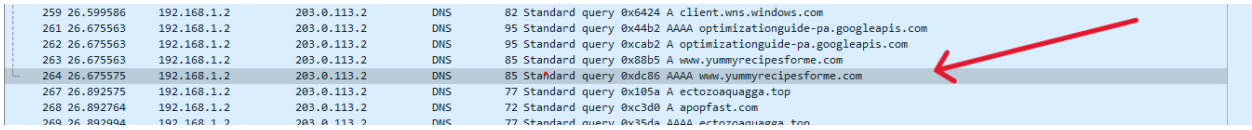
After 15 seconds, I stopped the capture and filtered for:
dns – to see the DNS query
icmp – to check for error messages

dns
dnsserver

No.		Source	Destination	Protocol	Length	Info
	642	192.168.1.2	203.0.113.2	DNS	85	Standard query 0xdc86 AAAA www.yummyrecipesforme.com
249	25.663642	192.168.1.2	203.0.113.2	DNS	95	Standard query 0x44b2 AAAA optimizationguide-pa.googleapis.com
250	25.663716	192.168.1.2	203.0.113.2	DNS	95	Standard query 0xcab2 A optimizationguide-pa.googleapis.com
258	26.599569	192.168.1.2	203.0.113.2	DNS	82	Standard query 0xc586 AAAA client.wns.windows.com
259	26.599586	192.168.1.2	203.0.113.2	DNS	82	Standard query 0x6424 A client.wns.windows.com
261	26.675563	192.168.1.2	203.0.113.2	DNS	95	Standard query 0x44b2 AAAA optimizationguide-pa.googleapis.com
262	26.675563	192.168.1.2	203.0.113.2	DNS	95	Standard query 0xcab2 A optimizationguide-pa.googleapis.com
263	26.675563	192.168.1.2	203.0.113.2	DNS	85	Standard query 0x88b5 A www.yummyrecipesforme.com
264	26.675575	192.168.1.2	203.0.113.2	DNS	85	Standard query 0xdc86 AAAA www.yummyrecipesforme.com
267	26.892575	192.168.1.2	203.0.113.2	DNS	77	Standard query 0x105a A ectozoaquagga.top
268	26.892764	192.168.1.2	203.0.113.2	DNS	72	Standard query 0xc3d0 A apopfast.com
269	26.892994	192.168.1.2	203.0.113.2	DNS	77	Standard query 0x35da AAAA ectozoaquagga.top
270	26.893077	192.168.1.2	203.0.113.2	DNS	72	Standard query 0x47b7 AAAA apopfast.com
278	27.104763	192.168.1.2	203.0.113.2	DNS	79	Standard query 0x348f AAAA clients4.google.com
279	27.105053	192.168.1.2	203.0.113.2	DNS	79	Standard query 0xa668 A clients4.google.com
280	27.105252	192.168.1.2	203.0.113.2	DNS	79	Standard query 0x01ae HTTPS clients4.google.com

4. Findings

A DNS query was sent to 203.0.113.2 using UDP port 53.



259	26.599586	192.168.1.2	203.0.113.2	DNS	82	Standard query 0x6424 A client.wns.windows.com
261	26.675563	192.168.1.2	203.0.113.2	DNS	95	Standard query 0x44b2 AAAA optimizationguide-pa.googleapis.com
262	26.675563	192.168.1.2	203.0.113.2	DNS	95	Standard query 0xcab2 A optimizationguide-pa.googleapis.com
263	26.675563	192.168.1.2	203.0.113.2	DNS	85	Standard query 0x88b5 A www.yummyrecipesforme.com
264	26.675575	192.168.1.2	203.0.113.2	DNS	85	Standard query 0xdc86 AAAA www.yummyrecipesforme.com
267	26.892575	192.168.1.2	203.0.113.2	DNS	77	Standard query 0x105a A ectozoaquagga.top
268	26.892764	192.168.1.2	203.0.113.2	DNS	72	Standard query 0xc3d0 A apopfast.com
269	26.892994	192.168.1.2	203.0.113.2	DNS	77	Standard query 0x35da AAAA ectozoaquagga.top

- No response came back from the DNS server.
- The nslookup command timed out.
- I checked for ICMP "Port unreachable" messages, but did not see one.
- This likely means the network dropped the packet silently, or the IP is completely unreachable.
- Even without an ICMP error, the lack of a DNS response confirms the service was not available.

5. Root Cause

The DNS server at 203.0.113.2 is unreachable. Since no service was listening or responding on UDP port 53, the domain www.yummyrecipesforme.com could not be resolved to an IP address.

This broke the first step in loading a website — DNS resolution — so users could not reach the site.

6. Affected Protocol and Service

- Affected Protocol: DNS (Domain Name System)
- Transport Protocol: UDP
- Port: 53
- Service Affected: DNS Resolution Service

Note: Even though ICMP is used to report errors, it was not the affected protocol — it was only expected to deliver an error message.

7. Recommendations

- Check DNS Server Status – Make sure the DNS service is running.
- Verify Port 53 – Ensure UDP port 53 is open and not blocked.
- Review Firewall Rules – Confirm no firewall is dropping DNS traffic.
- Use Backup DNS – Configure secondary DNS servers (like 8.8.8.8 or 1.1.1.1).
- Monitor for Outages – Use tools like nslookup or dig to test DNS health regularly.

8. Key Learnings

- DNS is a critical part of internet connectivity.
- A DNS failure can look like a website or internet outage.
- Wireshark helps identify where a connection is failing.
- Simulating failures builds real troubleshooting skills.
- Always check DNS first when users can’t access websites.

9. Conclusion

This investigation showed that the DNS service was unreachable, which stopped users from accessing the website. Even though the website might be online, without DNS, it cannot be found.

This lab helped me develop real-world skills in:

- Network troubleshooting
- Packet analysis with Wireshark
- Understanding TCP/IP protocols
- Writing cybersecurity incident reports