Project 3: Domain Name System Analysis

CS513: Computer Networks

Javier Vela Tambo
jvela@wpi.edu

October 9, 2025

All the code developed for this assignment is available at the following GitHub repository: `https://github.com/javiervela/dns_analysis`. The codebase includes a Python library wrapping the `dig` CLI tool, as well as scripts to perform the analysis and generate the tables included in this report.

1 Basic DNS Operations

For the first exercise, a series of DNS queries were performed for the domain `unizar.es`, which belongs to the University of Zaragoza in Spain. The results of these queries are summarized in Table 1. The university's web server is hosted on a single dedicated server (`master.unizar.es`) with the IP address `155.210.11.203`. The domain uses multiple authoritative DNS servers and for email services, the domain relies on two mail exchange servers provided by a third-party service.

Table 1: DNS records for `unizar.es`

Domain	IP Address	ADNS	Web	Mail
unizar.es	155.210.11.203	chico.rediris.es	master.unizar.es	mxa-006a4e02.gslb.pphosted.com
		ns2.unizar.es		mxb-006a4e02.gslb.pphosted.com
		ns.unizar.es		
		ns3.unizar.es		
		sun.rediris.es		

2 Internet Infrastructure for Organization Domain

The list of universities and colleges analyzed in this section was obtained by sampling 100 entries from the `Colleges.csv` dataset, available at `https://web.cs.wpi.edu/~cew/share/Colleges.csv`. Only institutions for which valid DNS records were found for all three categories were included in the final analysis, totaling 53 universities.

The detailed DNS infrastructure for each of the selected universities and colleges is presented in Table 2. The table includes the domain name, the authoritative DNS servers (ADNS), web servers, and mail servers, along with the number of servers for each service. For clarity, the tables list only the domain name of the first server record for each service provider (ADNS, web, and mail), rather than the full server hostnames. The table shows a diverse range of service providers used by these institutions. Some universities host their web services on platforms like Squarespace, while many rely on Outlook and Google for email services. The use of cloud-based DNS services such as Cloudflare and AWS is also prevalent.

Table 2: DNS infrastructure for selected universities and colleges

Domain	ADNS	No.	Web	No.	Mail	No.
acba.edu	bluehost.com	2	squarespace.com	1	google.com	3
achs.edu	awsdns-39.com	4	achs.edu	1	google.com	7
aimtinc.com	ui-dns.de	4	squarespace.com	1	ionos.com	2
avedainstituteprovo.c	domaincontrol.com	2	avedainstituteprovo.c	1	secureserver.net	2
belrea.edu	domaincontrol.com	2	belrea.edu	1	outlook.com	1
bmdpark.com	domaincontrol.com	2	bmdpark.com	1	outlook.com	1
boisebible.edu	dreamhost.com	3	multiscreensite.com	1	outlook.com	1
brittanyacademy.edu	cloudflare.com	2	brittanyacademy.edu	1	outlook.com	1
byts.edu	cloudflare.com	2	wixdns.net	1	google.com	5
byuh.edu	byuh.edu	3	psdops.com	1	outlook.com	1
ccac.edu	akam.net	6	omniweb.cloud	1	outlook.com	1
centrahealth.com	azure-dns.net	4	edgekey.net	1	pphosted.com	2
cheyney.edu	azure-dns.info	4	cheyney.edu	1	cheyney.edu	2
cims.edu	domaincontrol.com	2	cims.edu	1	google.com	5
clackamas.edu	dnsmadeeasy.com	5	clackamas.edu	1	outlook.com	1
clarendoncollege.edu	cloudflare.com	2	omniweb.cloud	1	mimecast.com	2
collegeofthedesert.edu	collegeofthedesert.edu	3	omniweb.cloud	1	outlook.com	1
conemaugh.org	gcd-dns.com	2	azurefd.net	1	mimecast.com	2
dcmoboces.com	stier.org	4	apptegy.net	1	GOOGLE.com	5
deltastate.edu	deltastate.edu	2	deltastate.edu	1	deltastate.edu	2
empire.edu	empire.edu	3	empire.edu	1	mimecast.com	2
flcc.edu	suny.edu	6	cloudfront.net	1	outlook.com	1
gotoccsi.org	domaincontrol.com	2	gotoccsi.org	1	googlemail.com	5
hairschoolomaha.com	squarespacedns.com	8	squarespace.com	1	outlook.com	1
hptc.edu	onenet.net	2	squarespace.com	1	barracudanetworks.c	2
infinitycollege.edu	domaincontrol.com	2	infinitycollege.edu	1	outlook.com	1
jacksonville-college.edu	esc7.net	6	jacksonvillecollege.ed	1	google.com	5
kcu.edu	kcu.edu	7	kcu.edu	1	GOOGLEMAIL.COI	5
kdstudio.com	worldnic.com	2	kdstudio.com	1	inmotionhosting.com	1
kokomobeautyschool.	domaincontrol.com	2	squarespace.com	1	kokomobeautyschool.	1
lccc.wy.edu	wyo.gov	6	wy.edu	1	outlook.com	1
liaschorrinstitute.com	dns-parking.com	2	liaschorrinstitute.com	1	titan.email	2
maryville.edu	awsdns-06.net	4	pantheonsite.io	1	barracudanetworks.c	2

Domain	ADNS	No.	Web	No.	Mail	No.
mayvillestate.edu	ndus.edu	5	mayvillestate.edu	1	outlook.com	1
msbbcs.edu	dnsmadeeasy.com	4	msbbcs.edu	1	mxthunder.com	4
nptiflorida.edu	cloudflare.com	2	nptiflorida.edu	1	nptiflorida.edu	3
nv.edu	ct.gov	2	nv.edu	1	outlook.com	1
ohiochristian.edu	cloudflare.com	2	azurefd.net	1	outlook.com	1
pillar.edu	cloudflare.com	2	webflow.com	1	outlook.com	1
pmi.edu	easydns.com	4	wpenginepowered.co	1	pmi.edu	2
sf.edu	azure-dns.net	4	wpeproxy.com	1	outlook.com	1
slchc.edu	dns-parking.com	2	slchc.edu	1	outlook.com	1
sscc.edu	oar.net	2	sscc.edu	1	outlook.com	1
swmich.edu	cloudflare.com	2	terminalfour.net	1	google.com	5
tooeletech.edu	nsone.net	4	tooeletech.edu	1	sophos.com	2
trevecca.edu	azure-dns.org	4	hubspot.net	1	outlook.com	1
ultimatetouchbarber	namecheaphosting.co	2	ultimatetouchbarber	1	ultimatetouchbarber	1
und.edu	ndus.edu	5	und.edu	1	outlook.com	1
usao.edu	onenet.net	2	usao.edu	1	outlook.com	1
vbc.edu	bluehost.com	2	vbc.edu	1	google.com	5
washingtonbarbercoll	microsoftonline.com	4	ludicrous.cloud	1	outlook.com	1
winonah.net	winonah.net	2	winonah.net	1	winonah.net	1
woodbury.edu	azure-dns.org	4	wpeproxy.com	1	pphosted.com	2

.com

Table 3 summarizes the percentage of universities that provide their own infrastructure for each service. It is observed that only a small fraction of institutions manage their own authoritative DNS servers (11.32%) and mail servers (13.21%), while a majority (50.94%) host their web services independently.

Table 3: Percentage of universities providing their own infrastructure for each service

ADNS	Web	Mail
11.32%	50.94%	13.21%

Table 4 lists the top five providers for each service category, along with the number and percentage of universities using each provider. DomainControl.com and Cloudflare are the most common choices for authoritative DNS services, while Squarespace is the leading provider for web hosting. Outlook.com dominates the email service category. For some providers, such as Google and Microsoft, multiple domain names are used for their services. In these cases, the most representative domain name has been selected.

Table 4: Top 5 Providers for ADNS, Web, and Mail Services

ADNS	No. (%)	Web	No. (%)	Mail	No. (%)
domaincontrol.com	7 (13.5%)	squarespace.com	5 (9.6%)	outlook.com	23 (44.2%)
cloudflare.com	7 (13.5%)	omniweb.cloud	3 (5.8%)	google.com	10 (19.2%)
azure.microsoft.com	5 (9.6%)	azure.microsoft.com	2 (3.8%)	mimecast.com	3 (5.8%)
bluehost.com	2 (3.8%)	wpeproxy.com	2 (3.8%)	pphosted.com	2 (3.8%)
aws.amazon.com	2 (3.8%)	—	—	barracudanetworks.com	2 (3.8%)

Finally, Table 5 provides statistics on the number of servers used per service across the analyzed universities. The number of authoritative DNS servers ranges from 2 to 8, with a mean of 3.25 servers. Web services are typically hosted on a single server, while mail services vary more widely, with a maximum of 7 servers and a mean of 2.11.

Table 5: Statistics for Number of Servers per Service

Statistic	ADNS	Web	Mail
Min	2	1	1
Max	8	1	7
Mean	3.25	1.00	2.11
Median	2	1	1

3 Local DNS Servers

On my system, the default Local DNS server (LDNS) is `192.168.1.1`, which is the IP address of my home router. The router acts as a DNS forwarder, relaying queries from local devices to the DNS servers provided by Spectrum, my Internet Service Provider (ISP).

Initially, I selected eighteen different LDNS servers for analysis from the suggested list at `https://gist.github.com/mutin-sa/5dcbd35ee436eb629db7872581093bc5`. However, these public DNS servers returned an error to the `+norecurse` queries, likely due to restrictions imposed by the server administrators trying to avoid *DNS cache snooping* attacks.

After further investigation, I identified eleven LDNS servers that responded correctly to the `+norecurse` queries. These servers correspond to Internet Service Providers (ISPs) and are distributed across various geographic locations, including providers in the USA and Spain. Table 6 shows the chosen LDNS servers' IPs, their hostnames, and the measured Round-Trip Time (RTT) in milliseconds for DNS queries to `wpi.edu`. In order to accurately measure the RTT, the queries were performed with the `+norecurse` option.

Table 6: LDNS Response Times

LDNS IP	Hostname	RTT (ms)
64.233.207.16	dns1.wideopenwest.com	41
209.18.47.62	dns-cac-lb-02.charter.com	44
64.233.207.2	dns2.wideopenwest.com	44
71.10.216.1	rns01.charter.com	45
64.233.217.3	try11-dns2.try.wideopenwest.com	47
64.233.217.2	try11-dns1.try.wideopenwest.com	49
71.10.216.2	rns02.charter.com	52
209.18.47.61	dns-cac-lb-01.charter.com	62
212.230.255.129	ns1.xtratelecom.es	137
212.230.255.1	ns2.xtratelecom.es	138
84.236.142.130	—	152

4 Learning from DNS Caches

In this section, I have used the previously selected LDNS servers (see Table 6) to analyze the DNS cache behavior for a list of popular domains. I have selected 8 domains with variable popularity related to technology and social media. Initially, I considered including university domains, but they resulted in very few cache hits, likely due to their lower popularity compared to more popular domains.

Table 7 shows the Authoritative TTL (ATTL) values for these domains, which range from 60 seconds (Facebook) to 172800 seconds (Zoom). To obtain the ATTL values, I first retrieved the authoritative DNS servers for each domain and then queried each ADNS server directly.

Table 7: Authoritative TTLs (ATTLs) for Popular Domains

Hostname	ATTL
google.com	300
youtube.com	300
microsoft.com	3600
facebook.com	60
github.com	900
slack.com	3600
zoom.us	172800
canva.com	300

To measure the popularity of each domain, I performed a DNS query for each domain using each LDNS server, repeating the process every 5 minutes from October 7, 2025, at 9:52 AM to October 7, 2025, at 12:38 PM (a total of 33 samples). Each query was performed with the `+norecurse` option to ensure that the LDNS server would only respond from its cache. If the LDNS server did not have a cached entry for the domain, it would not return anything, which I counted as a cache miss. If a response was returned, it was counted as a cache hit.

Figure 1 shows a heatmap representing the percentage of cache hits for each LDNS server and domain combination. The results show that more popular domains like `google.com` and `youtube.com` have higher cache hit rates across most LDNS servers, while less popular domains like `canva.com` and `zoom.us` have lower hit rates. Notably, there is a significant variation in cache hit rates among different LDNS servers, indicating that the user base and query patterns of each ISP can greatly influence DNS cache performance.

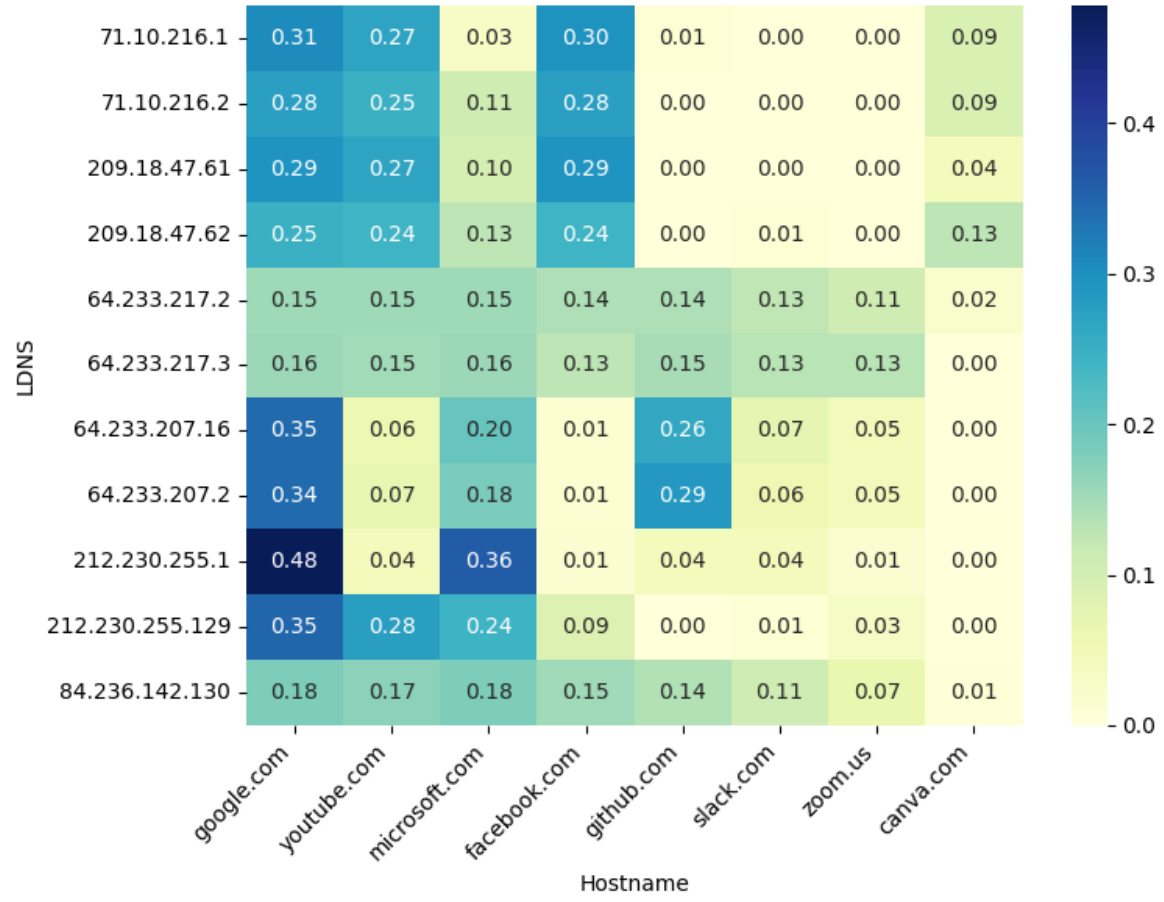

Figure 1: Heatmap of Percentage of LDNS Hits

5 DNS as an Internet Measurement Platform

For the last portion of the project, I measured an estimation of the RTT between the LDNS servers listed in Table 6 and the authoritative DNS servers (ADNS) for each of the eight popular domains listed in Table 7.

To estimate the RTT between each LDNS and the ADNS for the selected domains, I used the query time reported by the `dig` command. For each LDNS, I queried a non-existent subdomain of each target domain, both with and without the `+norecurse` option. The `+norecurse` query measures the response time from the LDNS cache alone, while the standard query forces the LDNS to contact the ADNS. The difference between these two times approximates the RTT between the LDNS and the ADNS, since the invented subdomain ensures a cache miss and triggers recursion.

Figure 2 shows a heatmap of the estimated RTT values between each LDNS and ADNS combination. The results indicate significant variability in RTTs, with some LDNS servers experiencing much higher latencies to certain ADNS servers. Additionally, there are negative RTT values in some cases, which likely result from measurement inaccuracies or network conditions that cause the `+norecurse` query to take longer than the recursive query. These anomalies highlight the challenges of using DNS queries for precise latency measurements.

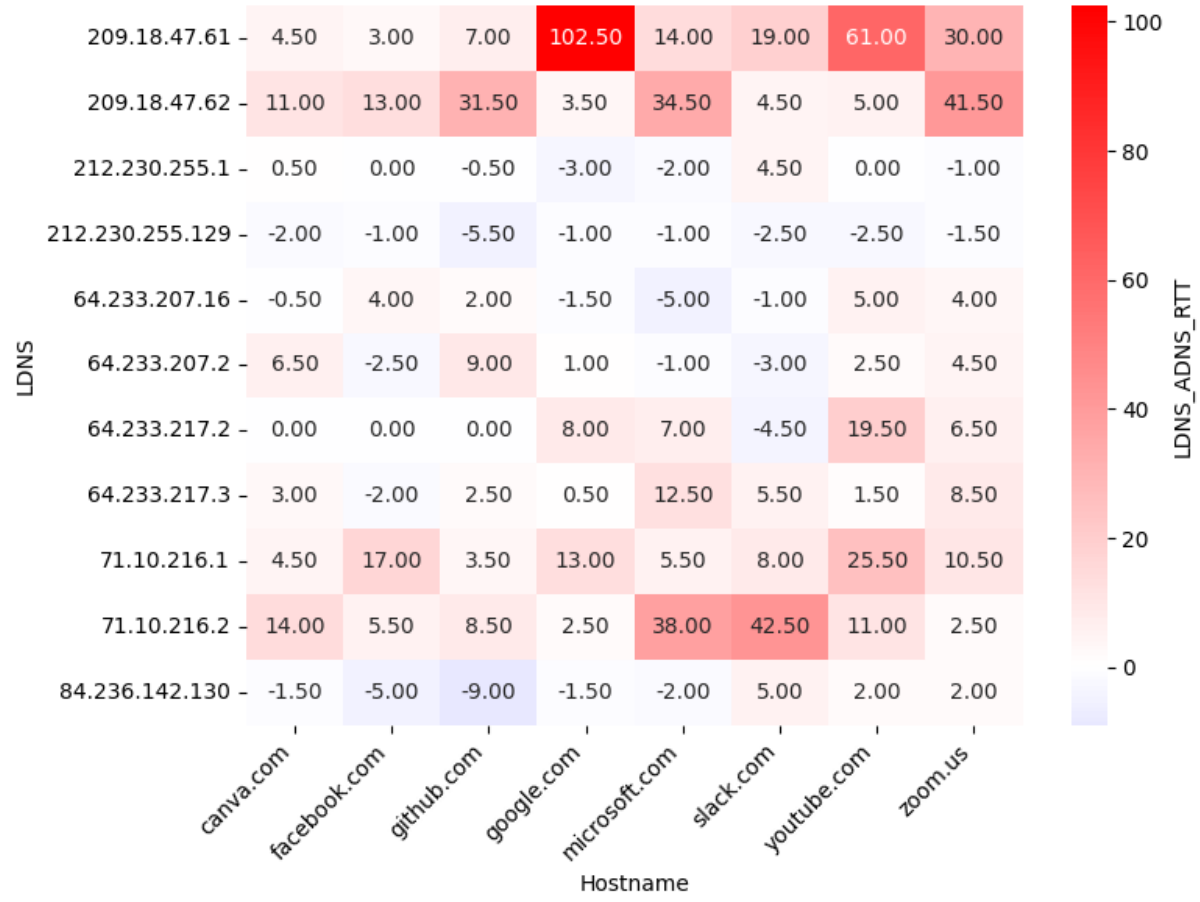

Figure 2: Heatmap of Estimated RTT between LDNS and ADNS

Tables 8 and 9 summarize the total estimated RTTs. Table 8 shows the total RTT for each LDNS summed across all ADNS, while Table 9 presents the total RTT for each domain summed across all LDNS. The LDNS with the highest total RTT is `209.18.47.61`. The domain with the highest total RTT is `youtube.com`. Conversely, the LDNS with the lowest total RTT is `212.230.255.129`. The domain with the lowest total RTT is `canva.com`. Negative total RTT values in these tables further indicate potential measurement errors or anomalies.

Table 8: Estimated Total RTT Between Each LDNS and ADNS (Summed Across All ADNS)

LDNS IP	Estimated Total RTT (ms)
209.18.47.61	**241.0**
209.18.47.62	144.5
212.230.255.1	-1.5
212.230.255.129	**-17.0**
64.233.207.16	7.0
64.233.207.2	17.0
64.233.217.2	36.5
64.233.217.3	32.0
71.10.216.1	87.5
71.10.216.2	124.5
84.236.142.130	-10.0

Table 9: Estimated Total RTT Between LDNS and ADNS for Each Domain (Summed Across All LDNS)

Domain	Estimated Total RTT (ms)
canva.com	**40.0**
facebook.com	32.0
github.com	49.0
google.com	124.0
microsoft.com	100.5
slack.com	78.0
youtube.com	**130.5**
zoom.us	107.5