Лабораторна робота № 17
ДОСЛІДЖЕННЯ РОБОТИ DNS У ОС WINDOWS

Мета заняття: ознайомитися з особливостями функціонування системи DNS з використанням локальних інструментів ОС Windows та веб-інтерфейсу.

Теоретичні відомості

Система доменних імен (DNS) перетворює доменні імена на IP-адреси, які браузери використовують для завантаження інтернет-сторінок. Кожен пристрій, підключений до Інтернету, має власну IP-адресу, яка використовується іншими пристроями для визначення його місцезнаходження. Сервери DNS дозволяють людям вводити звичайні слова у своїх браузерах, наприклад, google.com, без необхідності відстежувати IP-адреси для кожного веб-сайту.

DNS-сервер

DNS-сервер - це комп'ютер з базою даних, що містить публічні IP-адреси, пов'язані з назвами веб-сайтів, на які веде IP-адреса користувача. DNS діє як телефонна книга в Інтернеті. Щоразу, коли люди вводять доменні імена в адресний рядок веб-браузерів, DNS знаходить потрібну IP-адресу. IP-адреса сайту - це те, що скеровує пристрій у потрібне місце для доступу до даних сайту.

Після того, як DNS-сервер знаходить правильну IP-адресу, браузери беруть цю адресу і використовують її для надсилання даних на периферійні сервери мережі доставки контенту (CDN) або вихідні сервери. Після цього користувач отримує доступ до інформації на веб-сайті. DNS-сервер починає процес з пошуку відповідної IP-адреси для уніфікованого локатора ресурсів (URL) веб-сайту.

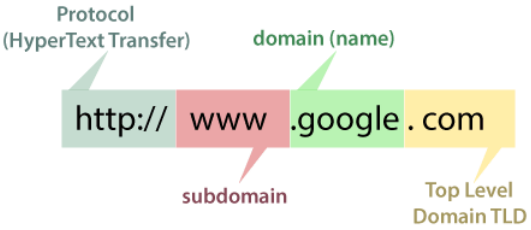

Рис. 1. Структура імен DNS

У звичайному DNS-запиті URL-адреса, яку вводить користувач, повинна пройти через чотири сервери, щоб отримати IP-адресу. Ці чотири сервери співпрацюють один з одним, щоб отримати правильну IP-адресу для клієнта, і вони включають в себе:

Функціонування DNS

Рекурсор DNS: Рекурсор DNS, який також називають DNS-розпізнавачем, отримує запит від DNS-клієнта. Потім він зв'язується з іншими DNS-серверами, щоб знайти потрібну IP-адресу. Після отримання запиту від клієнта він сам діє як клієнт. При цьому він робить запити, які надсилаються іншим трьом DNS-серверам: кореневим серверам імен, серверам імен домену верхнього рівня (TLD) і авторитетним серверам імен.

Кореневі сервери імен: Кореневий сервер імен призначений для кореневої зони DNS в Інтернеті. Його завдання - відповідати на запити, що надсилаються на нього щодо записів у кореневій зоні. Він відповідає на запити, надсилаючи назад список авторитетних серверів імен, які відповідають відповідному домену верхнього рівня. Спочатку кореневим серверам імен давали доменні імена, що відображали організації, які ними керували. У цих історичних назвах можна побачити справжніх великих гравців у розвитку Інтернету: ISI, NASA, військові США та інші. Деякі з серверів все ще знаходяться під управлінням урядових установ або військових США, де для їх захисту можуть бути застосовані додаткові заходи безпеки. Однак для зручності всі кореневі сервери імен тепер мають алфавітні "літерні імена" в спеціальному домені "root-servers.net".

Сервери імен доменів верхнього рівня або Сервери імен TLD (top-level domain): Сервер імен TLD зберігає IP-адресу домену другого рівня, що міститься в імені TLD. Потім він звільняє IP-адресу веб-сайту та надсилає запит на сервер імен домену.

Авторитетні сервери імен: Авторитетний сервер імен - це те, що дає вам реальну відповідь на ваш DNS-запит. Існує два типи авторитетних серверів імен: головний сервер або первинний сервер імен і підлеглий сервер або вторинний сервер імен. Головний сервер зберігає оригінальні копії записів зони, тоді як підлеглий сервер є точною копією головного сервера. Він розподіляє навантаження на DNS-сервер і виконує роль резервного, якщо головний сервер виходить з ладу.

Авторитетні сервери імен зберігають інформацію про записи DNS. Рекурсивний сервер виступає в ролі посередника, розташованого між авторитетним сервером і кінцевим користувачем. Щоб дістатися до сервера імен, рекурсивний сервер повинен "рекурсивно" пройти по дереву DNS, щоб отримати доступ до записів домену.

Авторитетний DNS-сервер

Використовуючи аналогію з телефонною книгою, уявіть собі IP-адресу як номер телефону, а ім'я людини - як URL-адресу веб-сайту. Авторитетні DNS-сервери мають копію "телефонної книги", яка пов'язує ці IP-адреси з відповідними доменними іменами. Вони надають відповіді на запити, надіслані рекурсивними серверами імен DNS, надаючи інформацію про те, де можна знайти певні веб-сайти. Надані відповіді містять IP-адреси доменів, задіяних у запиті.

Авторитетні DNS-сервери відповідають за певні регіони, такі як країна, організація або місцевість. Незалежно від того, який регіон він обслуговує, авторитетний DNS-сервер виконує дві важливі функції. По-перше, сервер зберігає списки доменних імен та IP-адрес, які їм відповідають. Потім він відповідає на запити від рекурсивного DNS-сервера щодо IP-адреси, яка відповідає доменному імені.

Після того, як рекурсивний DNS-сервер отримує відповідь, він надсилає цю інформацію назад на комп'ютер, який її запитував. Комп'ютер використовує цю інформацію для підключення до IP-адреси, і користувач отримує доступ до веб-сайту.

Рекурсивний DNS-сервер

Після того, як користувач вводить URL-адресу у своєму веб-браузері, ця URL-адреса передається рекурсивному DNS-серверу. Потім рекурсивний DNS-сервер перевіряє свою кеш-пам'ять, щоб побачити, чи вже зберігається IP-адреса для URL-адреси. Якщо інформація про IP-адресу вже існує, рекурсивний DNS-сервер надсилає IP-адресу браузеру. Після цього користувач зможе побачити веб-сайт, для якого він ввів URL-адресу.

З іншого боку, якщо рекурсивний DNS-сервер не знайде IP-адресу під час пошуку у своїй пам'яті, він продовжить процес отримання IP-адреси для користувача. Наступним кроком рекурсивного DNS-сервера є зберігання IP-адреси протягом певного періоду часу. Цей період часу визначається власником домену за допомогою параметра, який називається "час життя" (TTL).

Кешування DNS-браузера

Операційна система (ОС), яка використовується на вашому пристрої, зберігає записи ресурсів DNS за допомогою кешування. Кешування запобігає надмірності, коли хтось намагається зайти на сайт. Це, в свою чергу, зменшує час, необхідний для того, щоб потрапити на сайт. Якщо пристрій, який ви використовуєте, нещодавно заходив на сторінку, до якої він намагається отримати доступ, IP-адреса може бути надана кешем. Таким чином, запит до веб-сайту може бути виконаний без залучення DNS-сервера.

Таким чином, кеш DNS допомагає спростити процес пошуку DNS, який в іншому випадку був би необхідний для зв'язування доменного імені з IP-адресою. Це робить процес доступу до веб-сайту набагато швидшим.

Зберігання даних сервера імен DNS

Однією з найважливіших функцій, яку виконують сервери імен, є зберігання даних про імена. Кожен DNS-сервер є, по суті, різновидом сервера баз даних. База даних містить багато видів інформації про субдомени та окремі пристрої в межах домену або зони, за які відповідає сервер. У DNS записи бази даних, які містять

цю інформацію про імена, називаються записами ресурсів (RR). З кожним вузлом у зоні пов'язаний певний набір RR-записів.

Кожен вузол може мати різну кількість записів, залежно від типу вузла і того, яка інформація для нього зберігається. Записи ресурсів додаються, змінюються або видаляються, коли змінюється інформація DNS, адміністраторами, які вносять зміни в текстові основні файли на комп'ютері сервера. Потім ці файли зчитуються в пам'ять програмним забезпеченням DNS-сервера, аналізуються (інтерпретуються) і перетворюються в двійкову форму. Після цього вони готові до використання для вирішення запитів на імена DNS та інших запитів.

Основні стандарти DNS, RFC 1034 і 1035, визначили ряд типів записів про ресурси. З часом цей список змінювався, оскільки в наступних стандартах створювалися нові типи RR, а використання інших змінювалося. Як і інші параметри Інтернету, в DNS насправді існує кілька десятків визначених типів RR, але лише деякі з них широко використовуються; інші вже застаріли, використовуються для спеціальних цілей або є "експериментальними" за своєю природою.

Таблиця 1

Загальні типи записів про ресурси

Значення типу RR	RR Текстовий код	Тип RR	Опис
1	A	Address	Містить 32-бітну IP-адресу. Це основа DNS, оскільки саме тут зберігається адреса вузла для цілей дозволу імен.
2	NS	Name Server	Вказує ім'я сервера імен DNS, який є авторитетним для зони. Кожна зона повинна мати принаймні один запис NS, який вказує на її основний сервер імен, і це ім'я також повинно мати дійсний запис A (адреса).
5	CNAME	Canonical Name	Цей запис ресурсу використовується для визначення псевдонімів, які вказують на справжнє ім'я вузла. Запис CNAME забезпечує відповідність між цим псевдонімом

			і "канонічним" (справжнім) іменем вузла. Запис ресурсу CNAME зазвичай використовується для приховування змін у внутрішній структурі DNS від зовнішніх користувачів, дозволяючи їм використовувати незмінний псевдонім, в той час як внутрішні імена змінюються відповідно до потреб організації. Для прикладу див. розділ про дозвіл імен.
6	SOA	Start Of Authority	Запис ресурсу SOA використовується для позначення початку DNS-зони та надання важливої інформації про неї. Кожна зона повинна мати рівно один запис SOA, який містить такі дані, як назва зони, ім'я її основного (головного) авторитетного сервера, а також технічні дані, такі як адреса електронної пошти її адміністратора та параметри частоти оновлення підлеглих (вторинних) серверів імен.
12	PTR	Pointer	Надає вказівник на інше місце у просторі імен. Ці записи найбільш відомі завдяки їх використанню у зворотному дозволі через домен IN-ADDR.ARPA.
15	MX	Mail Exchange	Вказує розташування (ім'я пристрою), яке відповідає за обробку електронної пошти, надісланої на домен.
16	TXT	Text String	Дозволяє зберігати довільний додатковий текст, пов'язаний з доменом.

Всі ці записи ресурсів використовуються різними способами для визначення зон і пристроїв у них, а потім дозволяють вирішувати імена та виконувати інші функції.

Огляд локальних інструментів ОС Windows та веб-інтерфейсів

Для дослідження DNS можуть використовуватися як локальні інструменти, вбудовані у ОС Windows, так і сторонні застосунки або веб-інструменти.

Спочатку розглянемо специфіку роботи з локальними інструментами.

Доменом, який буде розглядатися як приклад, було обрано cisco.com.

ipconfig – це команда розширеного аналізу System Service Tools (SST), призначена для відображення всіх поточних мережевих з'єднань, класу TCP/IP, інформації про DHCP та DNS.

Використовується дана команда зазвичай з командного рядка, проте також при необхідності її можна відкрити, перейшовши за адресою C:\WINDOWS\system32, і запустити exe-файл "ipconfig.exe" або використавши командлет PowerShell.

Щоб отримати список усіх записів DNS, які кешуються на комп'ютері, потрібно відкрити консоль і ввести команду **ipconfig /displaydns**. Вона покаже ім'я DNS записів, IP-адресу та додаткову інформацію.

```
C:\Users\Andrii>ipconfig /displaydns

Windows IP Configuration

    cisco.com
    ----------------------------------------
    Record Name . . . . . : cisco.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 498
    Data Length . . . . . : 4
    Section . . . . . : Answer
    A (Host) Record . . . : 72.163.4.185


    Record Name . . . . . : j.gtld-servers.net
    Record Type . . . . . : 1
    Time To Live  . . . . : 498
    Data Length . . . . . : 4
    Section . . . . . : Additional
    A (Host) Record . . . : 192.48.79.30


    Record Name . . . . . : k.gtld-servers.net
    Record Type . . . . . : 1
    Time To Live  . . . . : 498
    Data Length . . . . . : 4
    Section . . . . . : Additional
```

Рис. 2. Використання локальних утиліт

Для їх очищення, використовується команда **ipconfig /flushdns**. Якщо після використання команди, все пройшло успішно, в результаті буде виведене повідомлення про те, що " Кеш dns resolver успішно очищено"

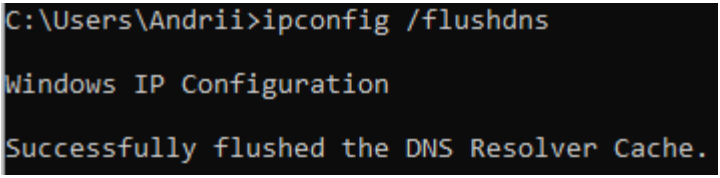

Рис. 3. Використання локальних утиліт

Одразу після використання цієї команди і переходу на певний веб-сайт, комп'ютер повторно надсилає DNS-запит для цього сайту. Проте сайт може не додатися до списку локального DNS кешу одразу через певні особливості оновлення кешу. Однак зазвичай з часом кеш DNS автоматично оновлюється з актуальною інформацією.

Команда ipconfig обмежена в можливостях. Наприклад, з її допомогою є неможливий пошук запису DNS.

nslookup – утиліта, що надає користувачеві інтерфейс командного рядка для звернення до системи DNS (простіше кажучи, DNS-клієнт). Вона також дозволяє користувачам отримувати інформацію про доменні імена та IP-адреси з інфраструктури DNS.

Щоб відобразити основну інформацію про домен, потрібно ввести команду nslookup і назву домену:

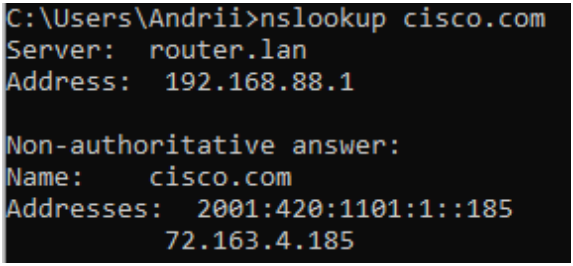

Рис. 4. Використання локальних утиліт

У цьому прикладі показано записи "A" для домену. Локальний DNS-сервер повертає свою адресу разом з інформацією про шуканий домен. Проте ця відповідь вважається неавторитетною, оскільки вона надається локальним DNS, а не DNS, пов'язаним з доменом.

Щоб вказати тип запиту, потрібно безпосередньо після директиви nslookup і перед доменним ім’ям вказати опцію -type= і додати бажаний варіант. Наприклад, щоб переглянути сервери імен для домену, використовується -type=ns. У наступному прикладі показано інформацію про сервери імен для cisco.com.

```
C:\Users\Andrii>nslookup -type=ns cisco.com
Server:  router.lan
Address:  192.168.88.1

Non-authoritative answer:
cisco.com       nameserver = ns3.cisco.com
cisco.com       nameserver = ns2.cisco.com
cisco.com       nameserver = ns1.cisco.com

cisco.com       nameserver = ns2.cisco.com
cisco.com       nameserver = ns1.cisco.com
cisco.com       nameserver = ns3.cisco.com
```

Рис. 5. Використання локальних утиліт

Щоб перевірити попередні неавторитетні результати на іншому DNS-сервері, потрібно додати ім'я сервера в кінець команди. У цьому прикладі запитується IP-адреса cisco.com безпосередньо з сервера імен Вікіпедії. Відповідь містить авторитетну відповідь для цього домену.

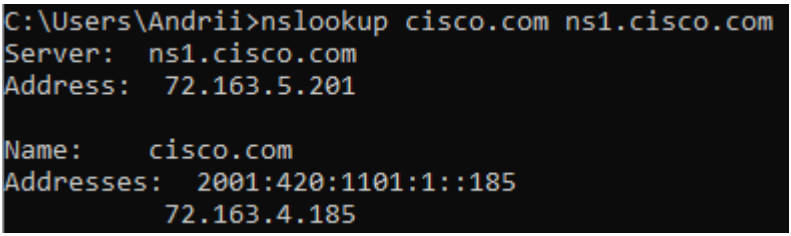

Рис. 6. Використання локальних утиліт

Для налагодження інформації з nslookup використовується прапорець -debug. У режимі налагодження відображаються запити, надіслані до DNS-сервера, а також відповіді, отримані у відповідь.

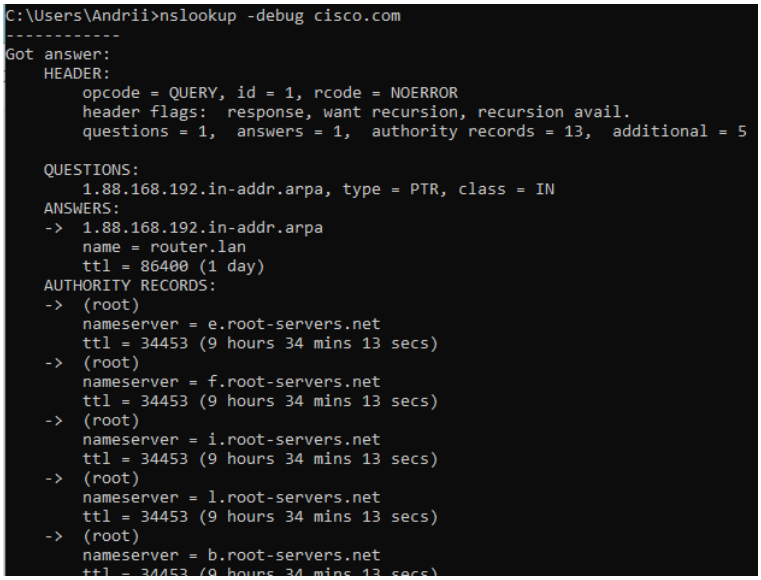

Рис. 7. Використання локальних утиліт

Також для аналізу даних DNS використовуються веб-сервіси. З їх допомогою можна отримати аналогічну та навіть більш детальну інформацію.

Whois.com – сервіс, що пропонує широкий спектр продуктів і послуг таких як реєстрація доменів, веб-хостинг, надання конструкторів веб-сайтів, комплексних пакетів хостингу електронної пошти та SSL-сертифікатів.

Проте в даному випадку, корисним є отримання інформації щодо окремих доменів та контактів зв'язку з ними.

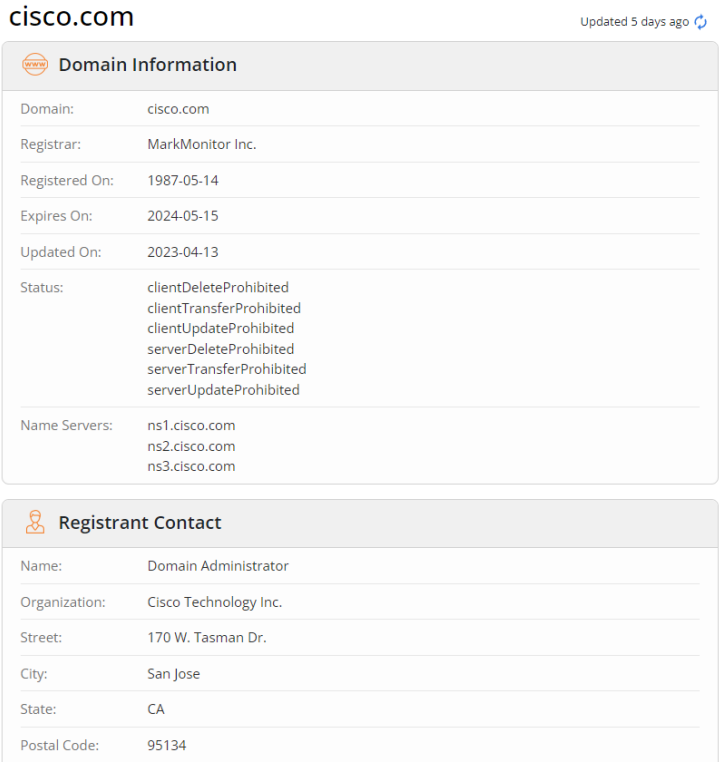

Рис. 8. Використання whois.com

NsLookup.io – це веб-клієнт DNS, який запитує DNS-записи для заданого доменного імені. Він дозволяє переглядати всі записи DNS для веб-сайту. Він надає ту саму інформацію, що й інструменти командного рядка, такі як dig і nslookup, але використовує для цього веб-браузер.

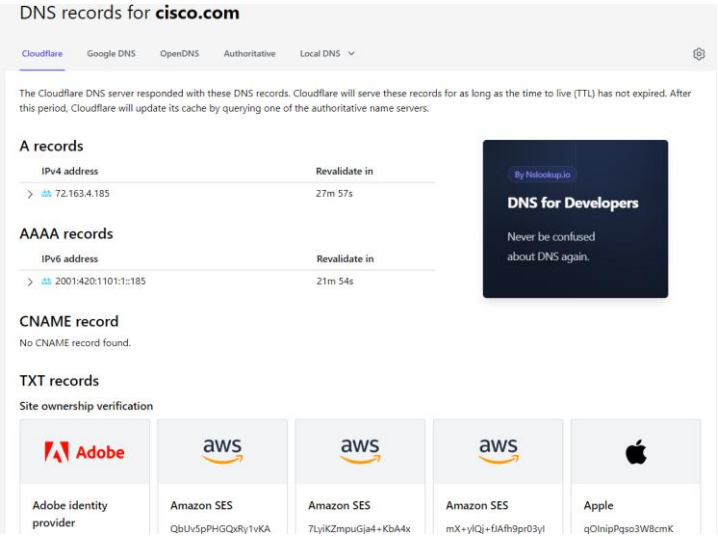

Рис. 9. Використання nslookup.io

CentralOps.net – сайт, що є колекцією інтернет-утиліт, розроблених компанією Hexillion.

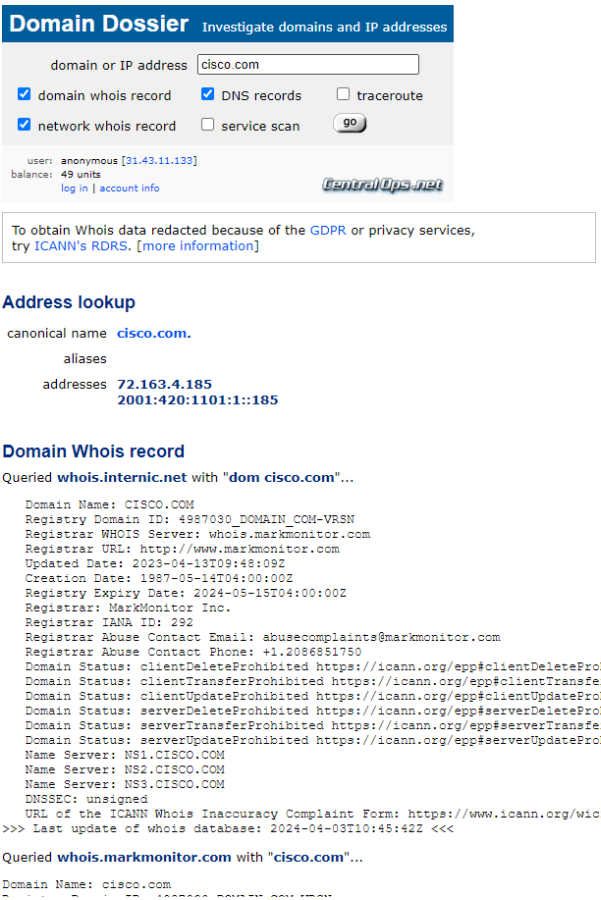

Рис. 10. Використання centralops.net

DNSdumpster.com – це безкоштовний інструмент для дослідження доменів, який може виявити хости, пов'язані з доменом.

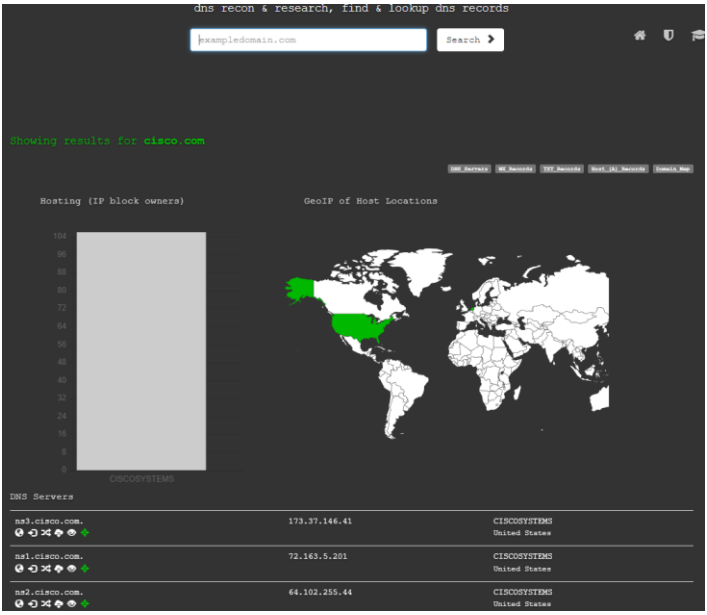

Рис. 11. Використання dnsdumpster.com

WolframAlpha.com – база знань і набір обчислювальних алгоритмів. У даному сервісі також можна отримати статистичну інформацію щодо доменів та піддоменів.

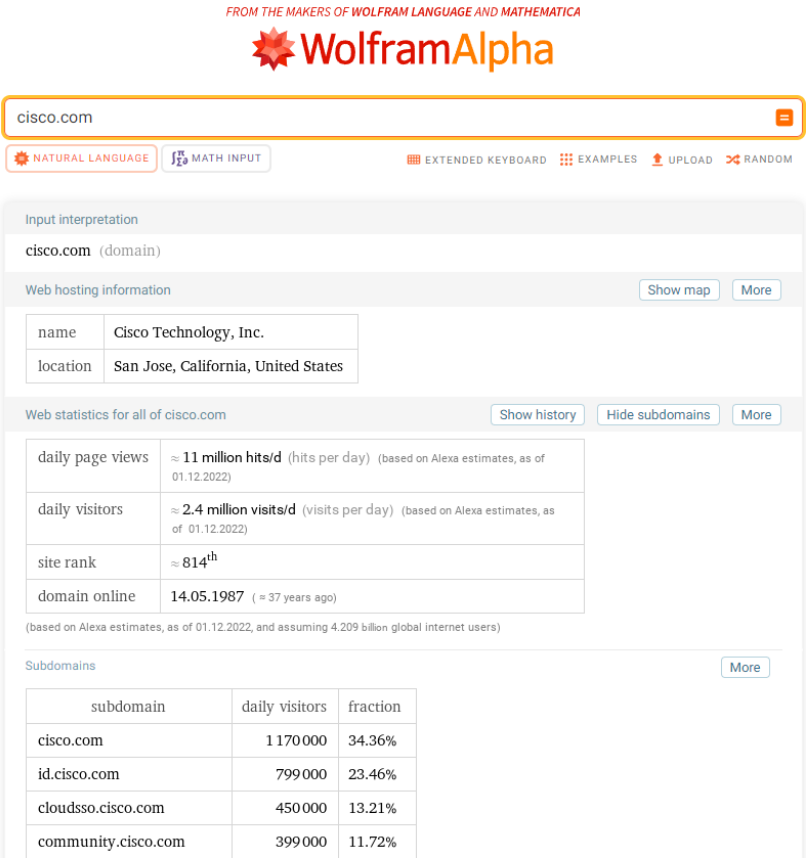

Рис. 12. Використання wolframalpha.com

Завдання на лабораторну роботу

1. Дослідити роботу локального інструменту ipconfig з ключами. Очистити DNS-кеш на комп'ютері, спробувати перевірити зв'язкок з доменом cisco.com та перевірити зміни локального кешу DNS.

2. Дослідити роботу локального інструменту nslookup. Отримати авторитетну відповідь від серверу домену, отриманого у таблиці 2. Виконати запит debug.

Таблиця 2

Варіант	Домен	Варіант	Домен
1	google.com	18	microsoft.com
2	lifecell.ua	19	mikrotik.com
3	digitalocean.com	20	rozetka.ua
4	amazon.com	21	booking.com
5	juniper.net	22	reddit.com
6	github.com	23	spotify.com
7	stackoverflow.com	24	yahoo.com
8	lenovo.com	25	vodafone.ua
9	instagram.com	26	fortinet.com
10	signal.org	27	facebook.com
11	nytimes.com	28	ibm.com
12	linkedin.com	29	bing.com
13	zte.com.cn	30	ukr.net
14	ebay.com	31	zoom.us
15	apple.com	32	wordpress.org
16	gov.ua	33	netflix.com
17	twitter.com	34	huawei.com

3. Отримати інформацію щодо домену та заповнити таблиці 3, 4, 5.

Таблиця 3

Ім’я домену	
Адреса IPv4	
Адреса IPv6	
Піддомени	
Організація	
Адреса органцізації	
Електронна пошта	
Телефон	
Дата створення домену	

Таблиця 4

Name Server	Адреса IPv4	Адреса IPv6

Таблиця 5

SOA data		Revalidate in
Start of authority		
Email		
Serial		
Refresh		
Retry		
Expire		
Negative cache TTL		

Контрольні питання

1. Як працює DNS?
2. Яким чином розподілена служба DNS?
3. Які існують основні типи серверів DNS? Які завдання вони виконуюють?
4. Скільки існує кореневих серверів? Які їх IP-адреси?
5. Які найбільш важливі типи DNS-записів? Для чого вони використовуються?
6. Як переглянути DNS-кеш на Windows?
7. Як отримати авторитетну відповідь під час використання утиліти nslookup?