ЛАБОРАТОРНА РОБОТА № 16
ДОСЛІДЖЕННЯ СЛУЖБИ ДОМЕННИХ ІМЕН DNS ТА АНАЛІЗ МЕРЕЖНОГО ТРАФІКУ ЗА ДОПОМОГОЮ АНАЛІЗАТОРА ПРОТОКОЛІВ WIRESHARK

Мета заняття: ознайомитися з призначенням, ієрархічною структурою та принципами функціонування служби доменних імен DNS; вивчити основні типи ресурсних записів та порядок розв'язання доменних імен; ознайомитися із сучасними протоколами захищеного транспортування DNS-запитів (DoT, DoH, DoQ) та технологією DNSSEC; отримати практичні навички використання команд діагностики DNS в ОС Windows (**nslookup**, **Resolve-DnsName**, **ipconfig**) та аналізатора протоколів **Wireshark** для дослідження інкапсуляції повідомлень і діагностики роботи служби імен.

1. ТЕОРЕТИЧНІ ВІДОМОСТІ

Призначення та структура служби DNS

Система доменних імен (Domain Name System, DNS) – це розподілена ієрархічна служба, яка забезпечує перетворення зручних для сприйняття людиною символьних імен вузлів у мережні адреси та у зворотному напрямку. Саме DNS дозволяє користувачеві звертатися до ресурсу за іменем **www.cisco.com**, а не за адресою 72.163.4.185 чи 2001:420:1101:1::185.

Простір імен DNS має деревоподібну структуру. Корінь простору позначається крапкою «.», нижче розташовані домени першого рівня (Top Level Domain, TLD): загальні (com, org, net, edu), національні (ua, pl, de) та нові (tech, online). Кожен домен може містити піддомени нижчого рівня. Повне ім'я вузла, записане від вузла до кореня, називають повним доменним іменем (Fully Qualified Domain Name, FQDN). Структуру простору імен наведено на рис. 1.

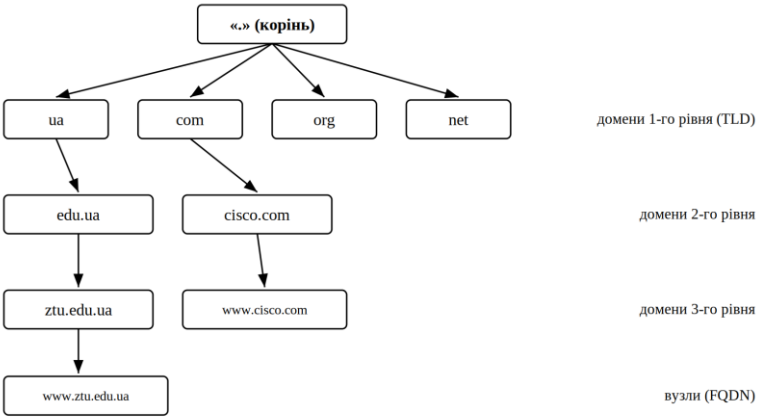


Рис. 1. Ієрархічна структура простору доменних імен

Частину простору імен, за адміністрування якої відповідає окрема організація, називають **зоною**. Відомості зони зберігаються на авторитетних (authoritative) серверах імен. Передавання відповідальності за піддомен іншому серверу називають **делегуванням**. Кореневу зону обслуговують 13 іменованих кореневих серверів (від a.root-servers.net до m.root-servers.net), фізично реалізованих сотнями anycast-екземплярів по всьому світу.

Ресурсні записи DNS

Дані зони зберігаються у вигляді ресурсних записів (Resource Record, RR). Кожен запис має ім’я, клас (для мереж TCP/IP – IN), тип, значення та час життя TTL (Time To Live), який визначає, скільки секунд відповідь дозволено зберігати у кеші. Основні типи ресурсних записів наведено у табл. 1.

Таблиця 1

Основні типи ресурсних записів DNS

Тип	Призначення	Приклад значення
A	IPv4-адреса вузла	93.184.216.34
AAAA	IPv6-адреса вузла	2606:2800:21f:cb07::1
CNAME	Канонічне ім’я (псевдонім)	www → e2867.dsca.akamaiedge.net
MX	Поштовий сервер домену та його пріоритет	10 alln-mx-01.cisco.com
NS	Авторитетний сервер зони	ns1.cisco.com
SOA	Початковий запис зони: первинний сервер, пошта адміністратора, серійний номер, таймери	ns1.cisco.com. admin.cisco.com. 2026090101
PTR	Зворотне перетворення адреси в ім’я (зона in-addr.arpa, ip6.arpa)	1.1.1.1.in-addr.arpa → one.one.one.one
TXT	Довільний текст; використовується для SPF, DKIM, DMARC, підтвердження прав на домен	v=spf1 include:_spf.google.com ~all
SRV	Розташування служби: протокол, порт, пріоритет, вага	_sip._tcp 10 60 5060 sip.example.com
CAA	Перелік центрів сертифікації, яким дозволено видавати сертифікати для домену	0 issue "letsencrypt.org"

Порядок розв’язання доменного імені

Програмний компонент вузла, який формує DNS-запити, називають **stub resolver** (у Windows його функції виконує служба DNS Client). Він надсилає **рекурсивний** запит до налаштованого рекурсивного сервера (резолвера), отриманого вручну або за протоколом DHCP. Резолвер, у свою чергу, виконує послідовність **ітеративних** запитів до кореневого сервера, сервера зони TLD та авторитетних серверів, доки не отримає остаточну відповідь (рис. 2).

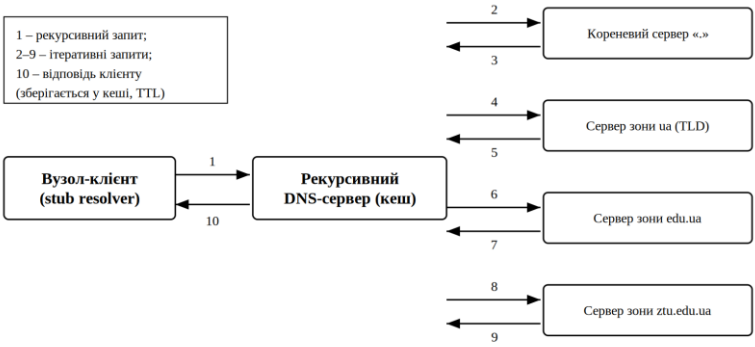


Рис. 2. Порядок розв'язання доменного імені

Отриману відповідь резолвер зберігає у кеші протягом часу TTL, тому наступні запити виконуються значно швидше. Кешуються і негативні відповіді (RFC 2308): якщо імені не існує, сервер повертає код відповіді NXDOMAIN, який також кешується на час, визначений у записі SOA. Окрім кешу резолвера, власний кеш має й операційна система вузла.

Повідомлення DNS складається із заголовка (ідентифікатор транзакції, прапорці, лічильники записів) та секцій запитання (Queries), відповіді (Answers), повноважень (Authority) і додаткових відомостей (Additional). Серед прапорців найважливіші: **QR** (запит або відповідь), **RD** (бажана рекурсія), **RA** (рекурсія доступна), **AA** (авторитетна відповідь), **AD** (дані перевірено засобами DNSSEC) та код відповіді **RCODE** (0 – NOERROR, 2 – SERVFAIL, 3 – NXDOMAIN).

Транспортування та захист DNS-трафіку

Класично DNS використовує протокол UDP, порт 53 (так званий Do53). Якщо відповідь не вміщується у дейтаграму або виконується передавання зони, застосовується TCP, порт 53. Розширення EDNS(0) (RFC 6891) дозволяє узгодити більший розмір повідомлення та передавати додаткові параметри. Оскільки класичний DNS не захищений, розроблено низку протоколів захищеного транспортування та перевірки достовірності даних (табл. 2).

Таблиця 2

Протоколи транспортування та захисту DNS

Протокол	Транспорт і порт	Стандарт	Особливості
Do53	UDP/TCP, порт 53	RFC 1034, 1035	Дані передаються у відкритому вигляді
DoT	TLS over TCP, порт 853	RFC 7858	Шифрування; трафік легко ідентифікувати за портом
DoH	HTTPS, порт 443	RFC 8484	Запити не відрізняються від звичайного веб-трафіку
DoQ	QUIC, порт 853/UDP	RFC 9250	Менші затримки, захист від блокування за портом
ODoH	HTTPS через проксі	RFC 9230	Розділення відомостей про клієнта і про запит
DNSSEC	Do53 та інші	RFC 4033–4035	Цифровий підпис записів (RRSIG, DNSKEY, DS, NSEC)

Технологія **DNSSEC** не приховує вміст запитів, а забезпечує перевірку цілісності та походження відповіді за допомогою ланцюжка довіри від кореневої зони. Якщо резолвер перевірив підписи, у відповіді встановлюється прапорець **AD**. Шифровані протоколи DoT, DoH і DoQ, навпаки, приховують вміст запиту від спостерігача, але не гарантують достовірності даних – тому їх застосовують спільно з DNSSEC.

Сучасні ОС підтримують шифрований DNS вбудованими засобами: в ОС Windows 11 DoH налаштовується у властивостях мережного адаптера («Параметри DNS-сервера → Шифрування DNS»), у Linux – у systemd-resolved, у більшості браузерів DoH вмикається незалежно від налаштувань ОС. Наслідком є те, що на мережному рівні DNS-запити перестають бути видимими у вигляді відкритих повідомлень на порту 53.

Публічні рекурсивні DNS-сервери

Окрім серверів оператора зв’язку та власних серверів організації, широко використовуються публічні рекурсивні сервери. Вони відрізняються політикою фільтрації, збереженням журналів та підтримкою захищених протоколів (табл. 3). Адреси публічних серверів станом на жовтень 2026 р. наведено за даними офіційної документації відповідних служб.

Таблиця 3

Публічні рекурсивні DNS-сервери

Служба	IPv4	IPv6	DoT / DoH / DoQ	DNSSEC
Cloudflare	1.1.1.1, 1.0.0.1	2606:4700:4700::1111	+ / + / +	+
Google Public DNS	8.8.8.8, 8.8.4.4	2001:4860:4860::8888	+ / + / –	+
Quad9	9.9.9.9, 149.112.112.112	2620:fe::fe	+ / + / +	+
OpenDNS	208.67.222.222, 208.67.220.220	2620:119:35::35	+ / + / –	–
AdGuard DNS	94.140.14.14, 94.140.15.15	2a10:50c0::ad1:ff	+ / + / +	+
Mullvad DNS	194.242.2.2	2a07:e340::2	+ / + / –	+
DNS4EU (ЄС)	86.54.11.100, 86.54.11.1	2a13:1001::86:54:11:100	+ / + / –	+

Для служби DNS4EU адреса 86.54.11.100 відповідає резолверу без фільтрації, а 86.54.11.1 – резолверу із блокуванням шкідливих доменів.

Команди діагностики DNS в ОС Windows

Основним інструментом діагностики служби імен залишається команда **nslookup**, яка працює у двох режимах: неінтерактивному (ім’я та сервер задаються у рядку запуску) та інтерактивному (команди вводяться після запуску). Синтаксис команди:

nslookup [-опція] [ім’я | -] [сервер]

Основні параметри та команди інтерактивного режиму наведено у табл. 4.

Таблиця 4

Основні параметри команди nslookup

Параметр (команда)	Призначення
set type=A | AAAA | MX | NS | SOA | TXT | PTR | CAA | SRV | ANY	Задання типу ресурсного запису, який запитується
set debug | set d2	Виведення детального (повного) вмісту повідомлень DNS
set timeout=N	Час очікування відповіді, с
set retry=N	Кількість повторних спроб
set port=N	Порт сервера імен (за замовчуванням 53)
set recurse | set norecurse	Запит з рекурсією або без неї
server IP | lserver IP	Перехід до іншого сервера імен
ls -d домен	Спроба передавання зони (зазвичай заборонено)
exit	Вихід з інтерактивного режиму

У середовищі Windows PowerShell доступні сучасніші командлети модуля DnsClient. На відміну від **nslookup**, який звертається до сервера імен напряму та не використовує кеш служби DNS Client, командлет **Resolve-DnsName** працює через клієнтську службу ОС, тому його результати відповідають тому, що насправді отримують застосунки. Основні командлети наведено у табл. 5.

Таблиця 5

Команди Windows PowerShell для роботи з DNS

Команда	Призначення
Resolve-DnsName -Name ім'я -Type тип -Server адреса	Виконання DNS-запиту заданого типу до заданого сервера
Resolve-DnsName -Name ім'я -DnssecOk	Запит із запитом даних DNSSEC (RRSIG)
Resolve-DnsName -Name ім'я -CacheOnly	Пошук лише у кеші клієнта
Get-DnsClientServerAddress	Перелік серверів імен, налаштованих на інтерфейсах
Get-DnsClientCache	Перегляд вмісту кешу служби DNS Client
Clear-DnsClientCache	Очищення кешу служби DNS Client
Get-DnsClientDohServerAddress	Перелік відомих клієнту серверів DoH
Test-NetConnection -Port 853 -ComputerName адреса	Перевірка доступності порту (наприклад, DoT)

Класичні команди **ipconfig /displaydns** та **ipconfig /flushdns** виводять і очищають кеш перетворювача імен. В ОС Linux аналогічні функції виконують команди **dig**, **host**, **nslookup** та **resolvectl query**.

Аналізатор протоколів Wireshark

Wireshark – це вільний аналізатор мережних протоколів (сніфер), який перехоплює кадри на обраному мережному інтерфейсі та декодує їх відповідно до рівнів моделі TCP/IP. Станом на жовтень 2026 р. підтримуваними є гілки 4.6.x (поточна) та 4.4.x (попередня). Вікно програми містить три основні панелі: перелік перехоплених кадрів, детальний розбір обраного кадру за рівнями та шістнадцятковий дамп (рис. 3).

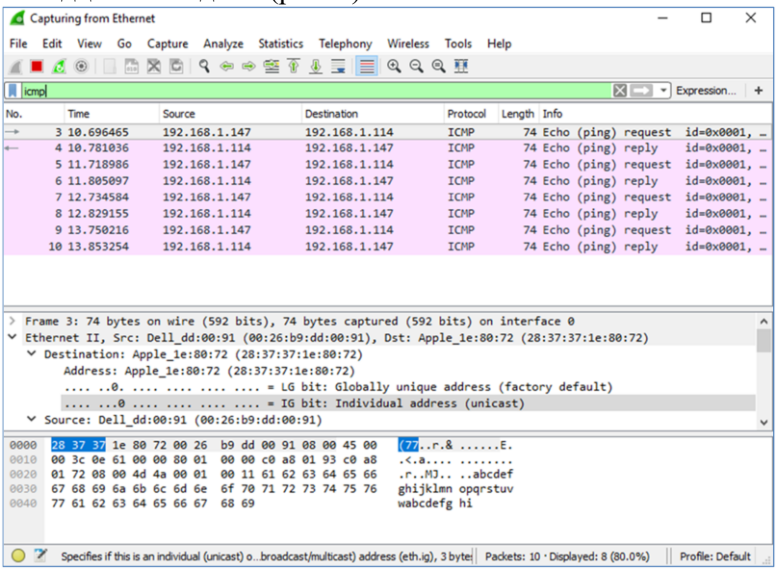


Рис. 3. Вікно аналізатора протоколів Wireshark

У Wireshark розрізняють два типи фільтрів. **Фільтр захоплення** (capture filter) задається до початку перехоплення синтаксисом BPF (наприклад, port 53) і зменшує обсяг збережених даних. **Фільтр відображення** (display filter) застосовується до вже перехоплених даних і використовує власний синтаксис Wireshark

(наприклад, dns.qry.type == 1). Основні фільтри відображення для аналізу DNS наведено у табл. 6.

Таблиця 6

Основні фільтри відображення Wireshark для аналізу DNS

Фільтр	Призначення
dns	Усі повідомлення протоколу DNS
dns.flags.response == 0 | == 1	Лише запити | лише відповіді
dns.qry.name == "ztu.edu.ua"	Запити щодо конкретного імені
dns.qry.type == 1 | 28 | 15 | 2	Запити типу A | AAAA | MX | NS
dns.flags.rcode != 0	Відповіді з помилкою (NXDOMAIN, SERVFAIL тощо)
dns.time > 0.1	Відповіді, отримані довше ніж за 100 мс
dns.resp.ttl < 300	Відповіді з малим часом життя запису
dns.flags.authoritative == 1	Авторитетні відповіді
udp.port == 53 | tcp.port == 853	Трафік Do53 | трафік DoT
mdns | llmnr	Службові протоколи розв'язання імен у локальній мережі

Корисними є також засоби **Statistics → DNS** (узагальнена статистика запитів і відповідей), **Statistics → Conversations** та команда контекстного меню **Follow → UDP Stream**. Поле **dns.time** обчислюється самим аналізатором як інтервал між запитом і відповіддю.

Особливості сучасної інфраструктури DNS

Під час виконання роботи слід враховувати особливості, характерні для сучасних мереж:

– великі сервіси використовують мережі доставки вмісту (CDN) та технологію anycast, тому для одного й того самого імені різні резолвери повертають різні IP-адреси;

– ім'я часто є псевдонімом (CNAME) і розв'язується через ланцюжок із кількох імен;

– значення TTL для таких записів становить десятки секунд, що дозволяє швидко змінювати маршрути доставки вмісту;

– у кадрах, адресованих у зовнішні мережі, MAC-адресою отримувача є адреса маршрутизатора (основного шлюзу), а не віддаленого вузла, оскільки MAC-адреси діють лише в межах широкомовного домену;

– ім’я вузла, до якого звертається браузер, може бути видимим у полі SNI повідомлення TLS Client Hello; механізм Encrypted Client Hello (ECH) приховує і це поле.

2. ЗАВДАННЯ НА ЛАБОРАТОРНУ РОБОТУ

Вихідні дані для виконання роботи визначаються за номером варіанта **N**, який відповідає номеру студента у списку групи (табл. 7–9). Усі результати наводяться у звіті у вигляді заповнених таблиць 10–14 та копій екрана.

Таблиця 7

Доменні імена для дослідження

№ вар.	Домен 1	Домен 2	Домен 3
1	ztu.edu.ua	rfc-editor.org	netflix.com
2	kpi.ua	wikipedia.org	europa.eu
3	knu.ua	mozilla.org	un.org
4	lpnu.ua	debian.org	nasa.gov
5	nure.ua	ubuntu.com	cern.ch
6	chnu.edu.ua	kernel.org	arxiv.org
7	cisco.com	github.com	bbc.co.uk
8	wireshark.org	cloudflare.com	ukr.net
9	ietf.org	google.com	rozetka.com.ua
10	iana.org	microsoft.com	novaposhta.ua
11	icann.org	apple.com	diia.gov.ua
12	rfc-editor.org	amazon.com	suspilne.media
13	wikipedia.org	netflix.com	dou.ua
14	mozilla.org	europa.eu	ztu.edu.ua
15	debian.org	un.org	kpi.ua
16	ubuntu.com	nasa.gov	knu.ua
17	kernel.org	cern.ch	lpnu.ua
18	github.com	arxiv.org	nure.ua
19	cloudflare.com	bbc.co.uk	chnu.edu.ua
20	google.com	ukr.net	cisco.com
21	microsoft.com	rozetka.com.ua	wireshark.org
22	apple.com	novaposhta.ua	ietf.org
23	amazon.com	diia.gov.ua	iana.org
24	netflix.com	suspilne.media	icann.org
25	europa.eu	dou.ua	rfc-editor.org
26	un.org	ztu.edu.ua	wikipedia.org
27	nasa.gov	kpi.ua	mozilla.org
28	cern.ch	knu.ua	debian.org
29	arxiv.org	lpnu.ua	ubuntu.com
30	bbc.co.uk	nure.ua	kernel.org

Таблиця 8

Сервери імен та типи ресурсних записів

№ вар.	DNS 1	DNS 2	Типи записів
1	1.1.1.1 (Cloudflare)	194.242.2.2 (Mullvad DNS)	A, AAAA, MX
2	8.8.8.8 (Google Public DNS)	86.54.11.100 (DNS4EU (без фільтрації))	AAAA, NS, TXT
3	9.9.9.9 (Quad9)	86.54.11.1 (DNS4EU (захищений))	A, AAAA, SOA
4	208.67.222.222 (OpenDNS)	1.0.0.1 (Cloudflare (альт.))	A, AAAA, NS
5	94.140.14.14 (AdGuard DNS)	8.8.4.4 (Google Public DNS (альт.))	A, CNAME, CAA
6	194.242.2.2 (Mullvad DNS)	149.112.112.112 (Quad9 (альт.))	A, NS, CAA
7	86.54.11.100 (DNS4EU (без фільтрації))	208.67.220.220 (OpenDNS (альт.))	A, MX, TXT
8	86.54.11.1 (DNS4EU (захищений))	1.1.1.1 (Cloudflare)	A, AAAA, TXT
9	1.0.0.1 (Cloudflare (альт.))	8.8.8.8 (Google Public DNS)	AAAA, MX, TXT
10	8.8.4.4 (Google Public DNS (альт.))	9.9.9.9 (Quad9)	AAAA, CNAME, MX
11	149.112.112.112 (Quad9 (альт.))	208.67.222.222 (OpenDNS)	A, SOA, CAA
12	208.67.220.220 (OpenDNS (альт.))	94.140.14.14 (AdGuard DNS)	A, CNAME, NS
13	1.1.1.1 (Cloudflare)	194.242.2.2 (Mullvad DNS)	A, NS, SOA
14	8.8.8.8 (Google Public DNS)	86.54.11.100 (DNS4EU (без фільтрації))	AAAA, MX, NS
15	9.9.9.9 (Quad9)	86.54.11.1 (DNS4EU (захищений))	AAAA, CAA, TXT
16	208.67.222.222 (OpenDNS)	1.0.0.1 (Cloudflare (альт.))	A, AAAA, CAA
17	94.140.14.14 (AdGuard DNS)	8.8.4.4 (Google Public DNS (альт.))	A, TXT, CAA
18	194.242.2.2 (Mullvad DNS)	149.112.112.112 (Quad9 (альт.))	A, MX, NS
19	86.54.11.100 (DNS4EU (без фільтрації))	208.67.220.220 (OpenDNS (альт.))	A, MX, SOA
20	86.54.11.1 (DNS4EU (захищений))	1.1.1.1 (Cloudflare)	AAAA, SOA, TXT
21	1.0.0.1 (Cloudflare (альт.))	8.8.8.8 (Google Public DNS)	A, AAAA, MX
22	8.8.4.4 (Google Public DNS (альт.))	9.9.9.9 (Quad9)	AAAA, NS, TXT
23	149.112.112.112 (Quad9 (альт.))	208.67.222.222 (OpenDNS)	A, AAAA, SOA
24	208.67.220.220 (OpenDNS (альт.))	94.140.14.14 (AdGuard DNS)	A, AAAA, NS
25	1.1.1.1 (Cloudflare)	194.242.2.2 (Mullvad DNS)	A, CNAME, CAA
26	8.8.8.8 (Google Public DNS)	86.54.11.100 (DNS4EU (без фільтрації))	A, NS, CAA

№ вар.	DNS 1	DNS 2	Типи записів
27	9.9.9.9 (Quad9)	86.54.11.1 (DNS4EU (захищений))	A, MX, TXT
28	208.67.222.222 (OpenDNS)	1.0.0.1 (Cloudflare (альт.))	A, AAAA, TXT
29	94.140.14.14 (AdGuard DNS)	8.8.4.4 (Google Public DNS (альт.))	AAAA, MX, TXT
30	194.242.2.2 (Mullvad DNS)	149.112.112.112 (Quad9 (альт.))	AAAA, CNAME, MX

Таблиця 9

Фільтри аналізатора Wireshark

№ вар.	Фільтр захоплення	Фільтр відображення 1	Фільтр відображення 2
1	port 53	dns	dns.flags.response == 1
2	udp port 53	dns.qry.type == 1	dns.time > 0.05
3	port 53 or port 853	dns.qry.type == 28	dns.flags.rcode != 0
4	host 208.67.222.222	dns && ip.addr == 208.67.222.222	dns.resp.ttl < 300
5	port 53 or icmp	dns.qry.name contains "nure.ua"	dns.flags.recdesired == 1
6	udp port 53 or udp port 5353	udp.port == 53	dns.count.answers > 1
7	port 53	dns.qry.type == 15	dns.flags.authoritative == 1
8	udp port 53	mdns || llmnr	dns.qry.name contains "cloudflare.com"
9	port 53 or port 853	dns.qry.type == 2	dns.time > 0.1
10	host 8.8.4.4	icmp || dns	dns.flags.response == 0
11	port 53 or icmp	dns	dns.flags.response == 1
12	udp port 53 or udp port 5353	dns.qry.type == 1	dns.time > 0.05
13	port 53	dns.qry.type == 28	dns.flags.rcode != 0
14	udp port 53	dns && ip.addr == 8.8.8.8	dns.resp.ttl < 300
15	port 53 or port 853	dns.qry.name contains "debian.org"	dns.flags.recdesired == 1
16	host 208.67.222.222	udp.port == 53	dns.count.answers > 1
17	port 53 or icmp	dns.qry.type == 15	dns.flags.authoritative == 1
18	udp port 53 or udp port 5353	mdns || llmnr	dns.qry.name contains "arxiv.org"
19	port 53	dns.qry.type == 2	dns.time > 0.1
20	udp port 53	icmp || dns	dns.flags.response == 0
21	port 53 or port 853	dns	dns.flags.response == 1
22	host 8.8.4.4	dns.qry.type == 1	dns.time > 0.05
23	port 53 or icmp	dns.qry.type == 28	dns.flags.rcode != 0
24	udp port 53 or udp port 5353	dns && ip.addr == 208.67.220.220	dns.resp.ttl < 300
25	port 53	dns.qry.name contains "europa.eu"	dns.flags.recdesired == 1

№ вар.	Фільтр захоплення	Фільтр відображення 1	Фільтр відображення 2
26	udp port 53	udp.port == 53	dns.count.answers > 1
27	port 53 or port 853	dns.qry.type == 15	dns.flags.authoritative == 1
28	host 208.67.222.222	mdns || llmnr	dns.qry.name contains "knu.ua"
29	port 53 or icmp	dns.qry.type == 2	dns.time > 0.1
30	udp port 53 or udp port 5353	icmp || dns	dns.flags.response == 0

1. Визначити мережні параметри робочої станції та параметри служби DNS: назву вузла, IP-адресу, маску підмережі, основний шлюз, перелік серверів імен, стан шифрування DNS. Використати команди:

```
ipconfig /all
Get-DnsClientServerAddress
Get-DnsClientDohServerAddress
```

Результати навести у вигляді табл. 10.

2. Дослідити кеш служби DNS Client: вивести його вміст, визначити кілька записів із зазначенням TTL, після чого очистити кеш і переконатися у результаті:

```
ipconfig /displaydns | more
Get-DnsClientCache | Select-Object Entry, RecordType,
TimeToLive
Clear-DnsClientCache
```

3. Для кожного з трьох доменів свого варіанта (табл. 7) виконати перевірку зв'язку командою **ping** та отримати записи типу A і AAAA на обох DNS свого варіанта (табл. 8). Приклад послідовності команд:

```
ping -4 домен
ping -6 домен
nslookup домен dns1
Resolve-DnsName -Name домен -Type AAAA -Server dns2
```

Результати навести у вигляді табл. 11. Пояснити, чому IP-адреси, отримані від різних DNS, можуть відрізнятися.

4. Для кожного домену свого варіанта отримати ресурсні записи тих типів, які зазначено у табл. 8. Застосувати інтерактивний режим nslookup та командлет Resolve-DnsName:

```
nslookup
> server dns1
> set type=MX
> домен
> exit
Resolve-DnsName -Name домен -Type MX -Server dns1
```

Результати навести у вигляді табл. 12. Для запису SOA пояснити призначення його полів, для MX – правило вибору поштового сервера, для CAA – призначення обмеження.

5. Порівняти роботу двох DNS свого варіанта: час відповіді, значення TTL, наявність ознаки авторитетності, наявність прапорця AD (DNSSEC), відмінності у відповідях для одного й того самого імені. Для перевірки DNSSEC використати:

```
Resolve-DnsName -Name домен -Type A -Server dns1 -
DnssecOk
```

Результати навести у вигляді табл. 13.

6. Виконати перехоплення трафіку в аналізаторі Wireshark із фільтром захоплення свого варіанта (табл. 9). Під час перехоплення очистити кеш і повторно виконати запити з п. 3. Застосувати по черзі обидва фільтри відображення свого варіанта. Для одного запиту і відповідної йому відповіді визначити: ідентифікатор транзакції, прапорці RD, RA, AA, AD, код відповіді, кількість записів у секціях, значення dns.time, порт джерела та отримувача, MAC- та IP-адреси відправника й отримувача. Результати навести у вигляді табл. 14.
7. Порівняти кадр локального обміну (ping до вузла своєї мережі) та кадр звернення до зовнішнього вузла. Пояснити, чому MAC-адреса отримувача у другому випадку не є MAC-адресою віддаленого вузла.
8. Дослідити службовий трафік розв'язання імен у локальній мережі: застосувати фільтри **mdns** та **llmnr**, визначити адреси призначення та номери портів цих протоколів, пояснити їх призначення.
9. Дослідити шифрований DNS: увімкнути DoH у параметрах мережного адаптера (або в браузері), повторити запити та проаналізувати трафік за фільтрами **tcp.port == 853** і **tls**. Пояснити, які відомості залишаються доступними спостерігачеві, а які – ні.
10. Виконати зворотне перетворення (запит PTR) для однієї з IP-адрес, отриманих у п. 3, та пояснити отриманий результат:

```
nslookup -type=PTR адреса dns1
Resolve-DnsName -Name адреса -Type PTR
```

Таблиця 10

Параметри робочої станції та служби DNS

№ з/п	Параметр	Значення
1	Мережна назва вузла	
2	IP-адреса / маска підмережі	
3	Основний шлюз	
4	Фізична (MAC) адреса інтерфейсу	
5	Сервери імен, отримані від DHCP	
6	Стан шифрування DNS (DoH)	
7	Кількість записів у кеші до очищення	

Таблиця 11

Результати розв’язання доменних імен

Домен	DNS	Запис A	Запис AAAA	TTL, с	Час, мс

Таблиця 12

Ресурсні записи доменів варіанта

Домен	Тип запису	Значення (скорочено)	TTL, с

Таблиця 13

Порівняння роботи DNS

Показник	DNS 1	DNS 2
Середній час відповіді, мс		
Значення TTL у відповіді, с		
Ознака авторитетності (AA)		
Прапорець AD (DNSSEC)		
Відмінності у складі відповіді		
Висновок щодо застосування		

Таблиця 14

Результати аналізу повідомлень DNS у Wireshark

Показник	Запит	Відповідь
Номер кадру		
Ідентифікатор транзакції		
Прапорці RD / RA / AA / AD		
Код відповіді (RCODE)		
Кількість записів Answers / Authority		
Порт джерела / отримувача		
IP-адреси джерела / отримувача		
MAC-адреси джерела / отримувача		
Час відповіді dns.time, с		

ЗВІТ ПОВИНЕН МІСТИТИ

1. Титульний аркуш, тему та мету роботи.
2. Номер варіанта та вихідні дані варіанта: три доменні імена, адреси двох DNS, типи ресурсних записів, фільтри захоплення та відображення (табл. 7–9).
3. Заповнену табл. 10 з мережними параметрами робочої станції та параметрами служби DNS.
4. Заповнені табл. 11 і 12 з результатами розв’язання доменних імен та отриманими ресурсними записами, а також текст використаних команд.
5. Заповнену табл. 13 з порівнянням роботи двох DNS.
6. Заповнену табл. 14 та копії екрана вікна Wireshark із застосованими фільтрами варіанта, на яких видно запит і відповідь DNS та розбір кадру за рівнями.
7. Копію екрана з результатами дослідження службових протоколів mDNS / LLMNR та шифрованого DNS (DoH), а також пояснення, які відомості доступні спостерігачеві у кожному випадку.
8. Результат зворотного перетворення (запит PTR) з поясненням.

9. Висновки, у яких зазначити: від чого залежить час розв'язання імені; чому відповіді різних DNS відрізняються; яку роль відіграє TTL та кешування; які загрози усуває DNSSEC, а які – шифровані протоколи DoT/DoH/DoQ; які відомості про роботу користувача можна отримати, аналізуючи лише DNS-трафік.

КОНТРОЛЬНІ ПИТАННЯ

1. Призначення та ієрархічна структура служби доменних імен DNS. Поняття зони та делегування.
2. Основні типи ресурсних записів DNS та їх призначення.
3. Порядок розв'язання доменного імені. Рекурсивні та ітеративні запити.
4. Кешування у DNS. Призначення параметра TTL та негативне кешування.
5. Структура повідомлення DNS. Призначення прапорців QR, RD, RA, AA, AD та кодів відповіді.
6. Транспортні протоколи DNS. У яких випадках застосовується TCP, порт 53?
7. Протоколи захищеного транспортування DNS: DoT, DoH, DoQ. Їх відмінності та порти.
8. Технологія DNSSEC: призначення, основні типи записів, ознака перевірених даних.
9. Команди діагностики DNS в ОС Windows. Відмінності між nslookup і Resolve-DnsName.
10. Аналізатор Wireshark: фільтри захоплення та фільтри відображення, основні фільтри для аналізу DNS-трафіку. Чому в кадрах до віддалених вузлів MAC-адресою отримувача є адреса маршрутизатора?