# «ІНСТИТУТ ПРИКЛАДНОГО СИСТЕМНОГО АНАЛІЗУ» НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ УКРАЇНИ «КПІ» КАФЕДРА МАТЕМАТИЧНИХ МЕТОДІВ СИСТЕМНОГО АНАЛІЗУ

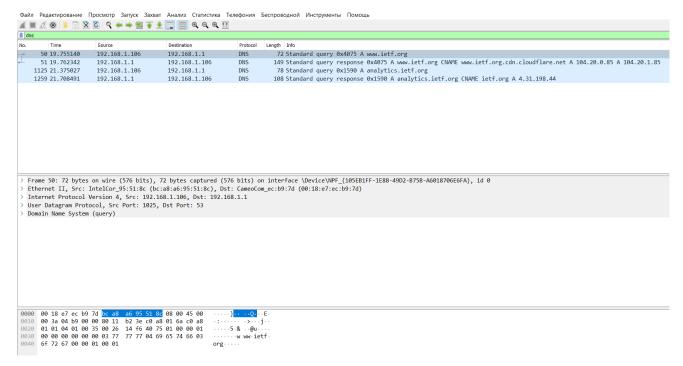
# Лабораторна робота №3 з курсу «Комп'ютерні мережі»

Виконала: студентка 3 курсу

групи КА 73

Собкович В.С.

Прийняв: Кухарєв С.О.



Frame 50: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface

\Device\NPF\_{105EB1FF-1E88-49D2-B75B-A6018706E6FA}, id 0

Ethernet II, Src: IntelCor\_95:51:8c (bc:a8:a6:95:51:8c), Dst: CameoCom\_ec:b9:7d (00:18:e7:ec:b9:7d)

Internet Protocol Version 4, Src: 192.168.1.106, Dst: 192.168.1.1

User Datagram Protocol, Src Port: 1025, Dst Port: 53

Domain Name System (query)

Transaction ID: 0x4075

Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

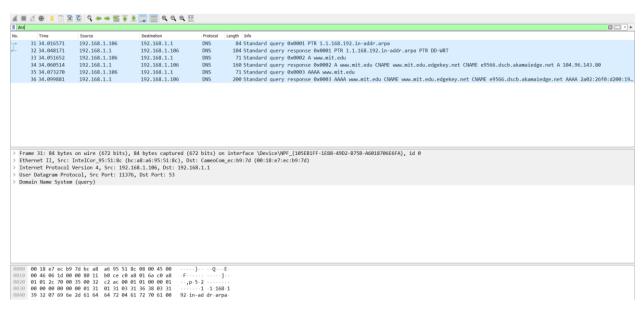
Queries

[Response In: 51]

// Термінал:

Значок Windows + R

Cmd

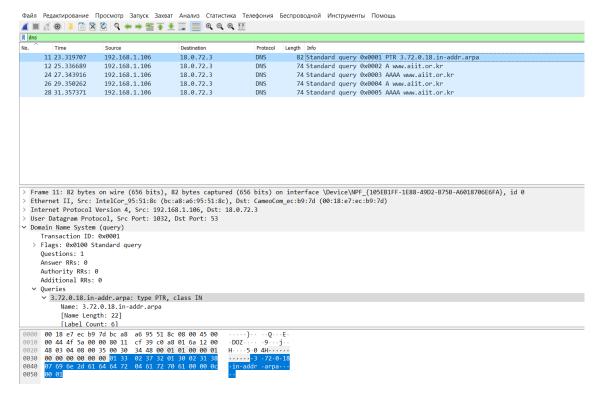


Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

38 27.681071 192.168.1.106 192.168.1.1 DNS 84 Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa 192.168.1.1 192.168.1.10 DNS 104 Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa PTR DD-MRT 40 27.688808 192.168.1.10 192.168.1.1 DNS 67 Standard query 0x000 pts mit.edu	dns			Bestesties	Protocol	80.1
- 39 27.683303 192.168.1.1 192.168.1.106 DNS 104 Standard query response 0x0001 PTR 1.1.168.192.in-addr.arpa PTR DD-WRT 40 27.688868 192.168.1.106 192.168.1.1 DNS 67 Standard query 0x0002 NS mit.edu	3.	Time	Source	Destination	Protocol	Length Info
40 27.688868 192.168.1.106 192.168.1.1 DNS 67 Standard query 0x0002 NS mit.edu	*	38 27.681071	192.168.1.106	192.168.1.1	DNS	
		39 27.683303	192.168.1.1	192.168.1.106	DNS	104 Standard query response 0x0001 PTR 1.1.168.192.in-addr.arpa PTR DD-WRT
41 27.697085 192.168.1.1 192.168.1.106 DNS 234 Standard guery response 0x0002 NS mit.edu NS ns1-37.akam.net NS use5.akam.net NS usw2.akam.net		40 27.688868	192.168.1.106	192.168.1.1	DNS	67 Standard query 0x0002 NS mit.edu
		41 27.697085	192.168.1.1	192.168.1.106	DNS	234 Standard query response 0x0002 NS mit.edu NS ns1-37.akam.net NS use5.akam.net NS usw2.akam.net NS asia1.akam.net NS eur5.akam.net NS.

- > Frame 38: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface \Device\WPF\_[105EBIFF-1E88-4902-875B-A6018706E6FA), id 0 
  > Ethernet II, Src: IntelCor\_95:51:8c (bc:a8:a6:95:51:8c), Dst: CameoCom\_ec:b9:7d (00:18:e7:ec:b9:7d) 
  > Internet Protocol Version 4, Src: 192.168.1.106, Dst: 192.168.1.1
  > User Datagram Protocol, Src Port: 11380, Dst Port: 53 
  > Domain Name System (query)

8888	00 18 e7 ec b9 7d bc a8 a6 95 51 8c 08 00	45 00 ·····}···Q··
	00 46 06 20 00 00 80 11 b0 cb c0 a8 01 6a	
0020	01 01 2c 74 00 35 00 32 c2 a8 00 01 01 00	00 01 ··,t-5-2 ····
0030	00 00 00 00 00 00 01 31 01 31 03 31 36 38	03 311 -1-16
0040	39 32 07 69 6e 2d 61 64 64 72 04 61 72 70	61 00 92 in-ad dr-ar
0050	00 0c 00 01	



## Теорія:

# Типи DNS записів

Записи DNS, або Ресурсні записи (англ. Resource Records, RR) — одиниці зберігання і передачі інформації в DNS.

Найбільш важливі типи DNS-записів:

- Запис А.
- Запис АААА.
- Запис СNAME.
- Запис МХ.
- Запис NS.
- ТХТ-запис.
- Запис PTR.
- Запис SOA.
- SRV-запис.

Запис А задає ІР-адреса хоста. За допомогою записів А виконується запит на перетворення імені домену в ІР-адресу.

Запис AAAA (IPv6 address record) зв'язує ім'я хоста з адресою протоколу IPv6. Наприклад, запит AAAA-запису на ім'я K.ROOT-SERVERS.NET поверне його IPv6 адреса — 2001:7fd::1

Запис типу CNAME (Canonical Name - Канонічне ім'я) дозволяють привласнювати хосту мнемонічні імена. Якщо DNS при зверненні до псевдоніму виявляє запис CNAME, що містить повне ім'я, DNS потім запитує повне ім'я домену.

Записи МХ містять визначення хоста системи обміну поштою для поштових повідомлень, що відправляються в цей домен. За допомогою записів цього типу і значень параметрів

конфігурації хостів системи обміну поштою в SMTP (Простий протокол передачі пошти) визначаються адреси хостів, які опрацьовують і перенаправляє пошту для цього домену. Кожному хосту системи обміну поштою повинна відповідати запис адреси хоста (A) в існуючій області.

Запис NS вказує відповідальний сервер для даного хоста.

Запис типу ТХТ зазвичай використовується для текстового опису доменного імені.

Запис РТК (pointer) або запис покажчика зв'язує IP хоста з його канонічним ім'ям. Наприклад, (на момент написання), для IP адреси 192.0.34.164: запит запису РТК 164.34.0.192.in-addr.arpa поверне його канонічне ім'я referrals.icann.org. З метою зменшення обсягу небажаної кореспонденції (спаму) багато серверів-одержувачі електронної пошти можуть перевіряти наявність РТК запису для хоста, з якого відбувається відправлення. У цьому випадку РТК запис для IP адреси повинна відповідати імені відправляючого поштового сервера, яким він представляється в процесі SMTP сесії.

Запис SOA (Start Of Authority) містить ім'я первинного DNS-сервера (Primary Name Server), адреса, необхідний для встановлення технічних контактів (Hostmaster), серійний номер (Serial number) різні значення таймерів (Refresh, Retry, Expire, Minimum TTL)

SRV-запис (server selection) вказує на сервери для сервісів, використовується, зокрема, для Jabber і Active Directory.

#### Контрольні запитання:

- 1. Знайдіть запит та відповідь DNS, який протокол вони використовують, UDP або TCP? Який номер цільового порта запиту DNS? Який номер вихідного порта відповіді DNS?
- UDP, Цільовий порт запиту –53, вихідний порт 1025;
  - 2. На який адрес IP був відправлений запит DNS? Чи є цей адрес адресом локального сервера DNS?
- 192.168.1.1, так;
  - 3. Проаналізуйте повідомлення із запитом DNS. Якого «Типу» цей запит? Чи вміщує цей запит деякі можливі компоненти «відповіді»?
- Типу A (Host address).Так, він вміщає тип та ім'я.
  - 4. Дослідіть повідомлення із відповіддю DNS. Яка кількість відповідей запропонована сервером? Що вміщує кожна з цих відповідей?
- Lds, Name, Type, Class, Time to live, Data length, Adress,
  - 5. Проаналізуйте повідомлення TCP SYN, яке відправила ваша робоча станція після отримання відповіді сервера DNS. Чи співпадає цільова IP адреса цього повідомлення з одною із відповідей сервера DNS?
- Ні, цільова IP адреса цього повідомлення 104.20.0.85, коли відповідь сервера DNS 192.168.1.106.
  - 6. Чи виконує ваша робоча станція нові запити DNS для отримання ресурсів, які

використовує документ, що отримав браузер?

Так;

- 7. Яким був цільовий порт повідомлення із запитом DNS? Яким був вихідний порт повідомлення із відповіддю DNS?
- Цільовий порт запиту 53, вихідний порт 1034;
  - 8. На яку IP-адресу був направлений запит DNS? Чи є ця адреса адресою вашого локального сервера DNS за замовчанням.
- 192.168.1.1 Так;
  - 9. Дослідіть повідомлення із запитом DNS. Якого «типу» був цей запит? Чи вміщує цей запит деякі можливі компоненти «відповіді»?
- Типу A (Host address). Hi;
  - 10. Дослідіть повідомлення із відповіддю DNS. Скільки записів із відповідями було запропоновано сервером? З чого складається кожна із цих відповідей?
- 3 відповіді. Name, Type, Class, Time to live, Data length, CNAME/Adress
  - 11. На яку IP-адресу був направлений запит DNS? Чи є ця адреса адресою вашого локального сервера DNS за замовчанням?
- 192.168.1.1, так.

1 відповідь;

- 12. Дослідіть повідомлення із запитом DNS. Якого «типу» був цей запит? Чи вміщує цей запит деякі можливі компоненти «відповіді»?
- Типу NS (authoritative Name Server). Hi;
  - 13. Дослідіть повідомлення із відповіддю DNS. Скільки записів із відповідями було запропоновано сервером? Які сервери DNS були запропоновані у відповіді? Сервери були запропоновані за допомогою доменного імені, адреси IP або й того й іншого?
- 8 штук(asia1.akam.net, eur5.akam.net, usw2.akam.net, ns1-37.akam.net, asia2.akam.net, ns1-
- 173.akam.net, use2.akam.net, use5.akam.net). Лише за допомогою доменного імені.
  - 14. На яку IP-адресу був направлений запит DNS? Чи є ця адреса адресою вашого локального сервера DNS за замовчанням? Якщо ні, то якому доменному імені відповідає ця IP-адреса?
- На 18.0.72.3, ця адреса не є адресою локального сервера DNS за замовчанням (bitsy.mit.edu)
  15. Дослідіть повідомлення із запитом DNS. Якого «типу» був цей запит? Чи вміщує цей запит деякі можливі компоненти «відповіді»?
- Типу A (Host address), типу AAAA (IPv6 Address) та типу PTR (domain name PoinTeR). Ні ; 16. Дослідіть повідомлення із відповіддю DNS. Скільки записів із відповідями було запропоновано сервером? З чого складається кожна з цих відповідей?

Name, Type, Class, Time to live, Data length, Adress

### Висновок:

В лабораторній роботі я ознайомилася з концепціями локальних сервер DNS; кешування DNSзаписів і повідомлень, а також з типами поля в записі DNS. Також, на превеликий подив, запис AAAA відноситься до типу DNS записів, а не пальчикових батарейок, як гадала раніше.