Задачи по 4-й лабораторной

A. Утилита nslookup

IP-адрес сайта www.aabi.info

```
(base) margarita@margarita-HP-Pavilion-Laptop-15-cs0xxx:~$ nslookup www.aabi.info
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   www.aabi.info
Address: 101.231.81.172

(base) margarita@margarita-HP-Pavilion-Laptop-15-cs0xxx:~$
```

С поиском авторитетного DNS-сервера на линуксе у меня возникла какая-то проблема, ничего не выводится :(

```
(base) margarita@margarita-HP-Pavilion-Laptop-15-cs0xxx:~$ nslookup -type=NS  www.harvard.edu
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
www.harvard.edu canonical name = pantheon-systems.map.fastly.net.

Authoritative answers can be found from:

(base) margarita@margarita-HP-Pavilion-Laptop-15-cs0xxx:~$
```

Я попросила человека с Windows ввести команду у себя. Получилось, что авторитетный DNS-сервер для гарвардского университета - это ns1.fastly.net, но как на линукс это сделать, не смогла найти

```
C:\Users\Lenovo>nslookup -type=NS  www.harvard.edu
╤xËтxË:  UnKnown
Address:  192.168.0.1

Не заслуживающий доверия ответ:
www.harvard.edu canonical name = pantheon-systems.map.fastly.net

fastly.net
        primary name server = ns1.fastly.net
        responsible mail addr = hostmaster.fastly.com
        serial  = 2017052201
        refresh = 3600 (1 hour)
        retry   = 600 (10 mins)
        expire  = 604800 (7 days)
        default TTL = 30 (30 secs)
```

Несколько IP-адресов имеет, например www.google.com

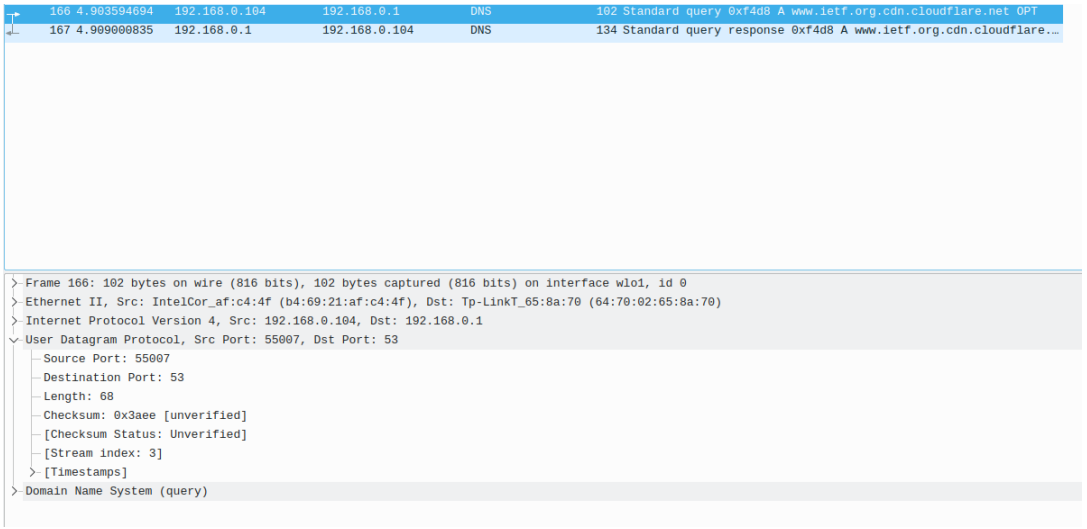
```
(base) margarita@margarita-HP-Pavilion-Laptop-15-cs0xxx:~$ nslookup www.google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   www.google.com
Address: 173.194.222.105
Name:   www.google.com
Address: 173.194.222.99
Name:   www.google.com
Address: 173.194.222.147
Name:   www.google.com
Address: 173.194.222.106
Name:   www.google.com
Address: 173.194.222.103
Name:   www.google.com
Address: 173.194.222.104
Name:   www.google.com
Address: 2a00:1450:4010:c0b::69
Name:   www.google.com
Address: 2a00:1450:4010:c0b::63
Name:   www.google.com
Address: 2a00:1450:4010:c0b::6a
Name:   www.google.com
Address: 2a00:1450:4010:c0b::93

(base) margarita@margarita-HP-Pavilion-Laptop-15-cs0xxx:~$
```

Веб-сервер www.spbu.ru имеет один IP-адрес

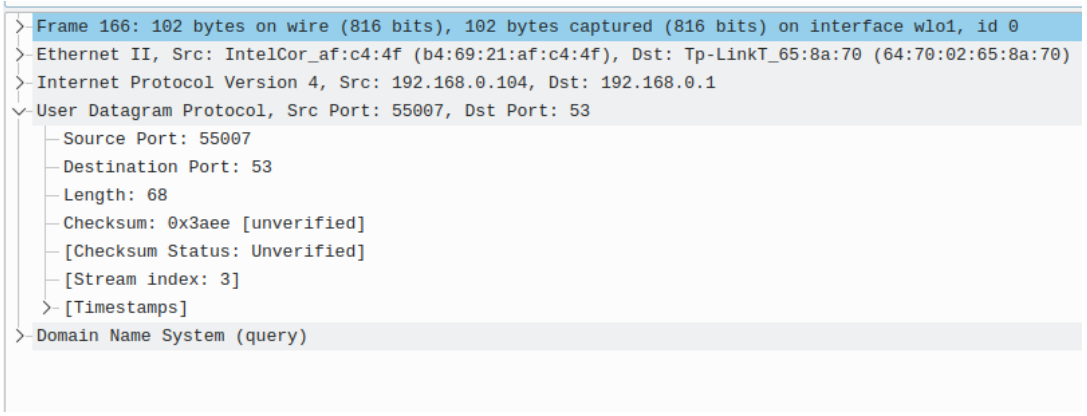
```
(base) margarita@margarita-HP-Pavilion-Laptop-15-cs0xxx:~$ nslookup www.spbu.ru
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
www.spbu.ru     canonical name = spbu.ru.
Name:   spbu.ru
Address: 195.239.37.91

(base) margarita@margarita-HP-Pavilion-Laptop-15-cs0xxx:~$
```

Б. DNS-трассировка www.ietf.org

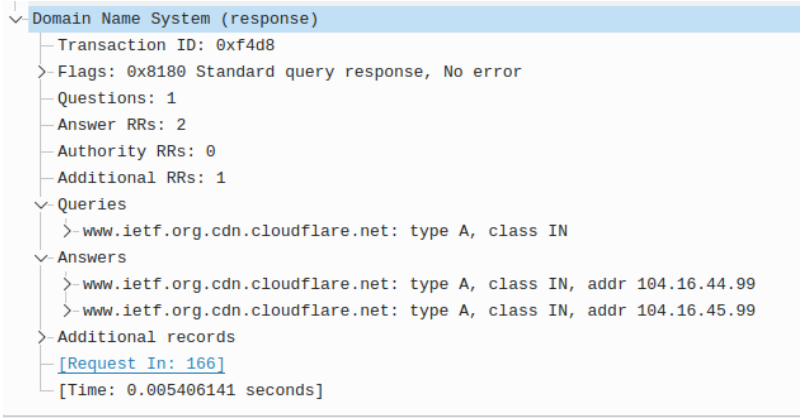
Используется транспортный протокол UDP (User Datagram Protocol)



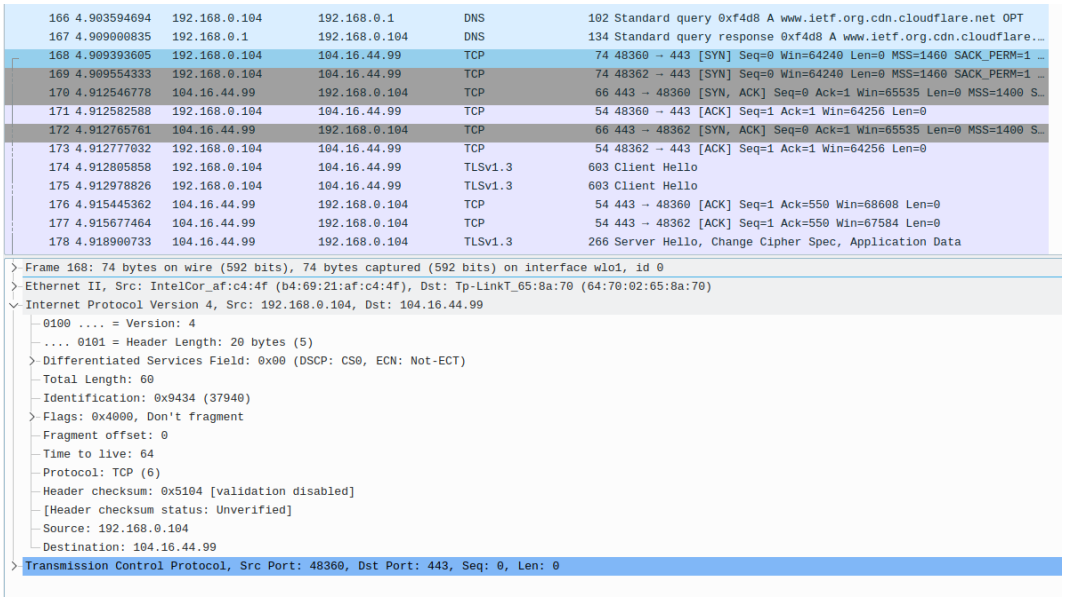
Порт назначения у запроса DNS - 53.



Запрос был отправлен на IP-адрес 192.168.0.1, DNS-адрес у меня такой же.
Запрашивается запись типа A (type A), ответов в запросе нет.
Пришло 2 ответа - 2 IP-адреса сервера:



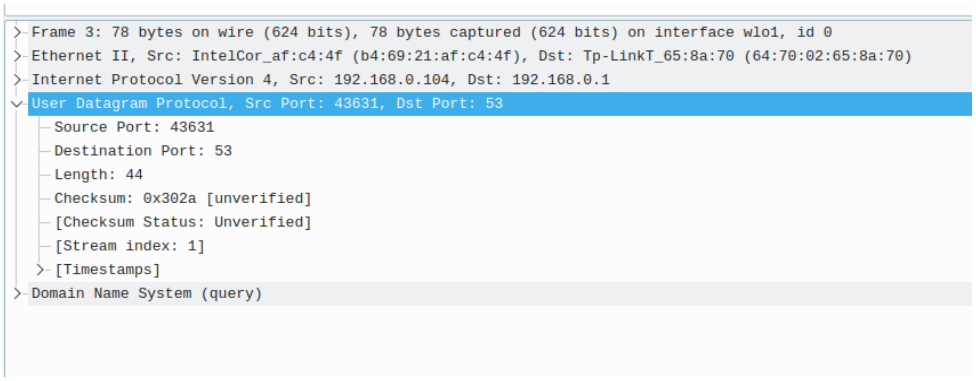
IP-адрес назначения TCP-пакета с флагом SYN совпадает с одним из IP-адресов, полученным в ответном сообщении (104.16.44.99)

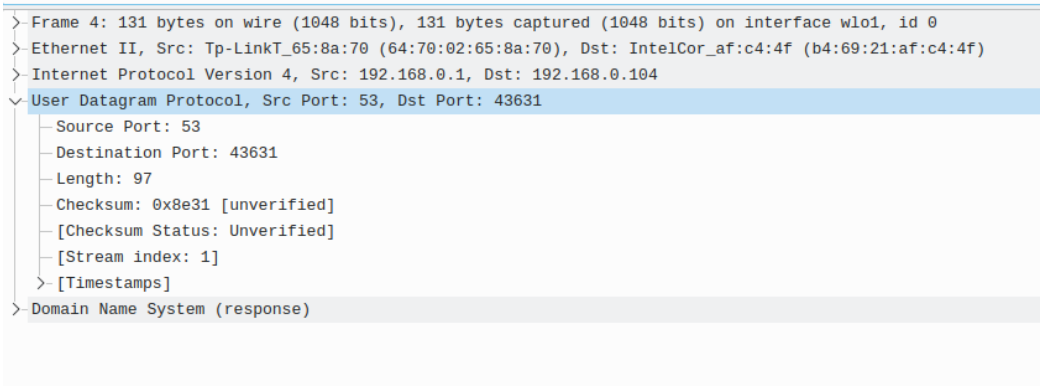


Да, потом отправляется еще 2 DNS-запроса.

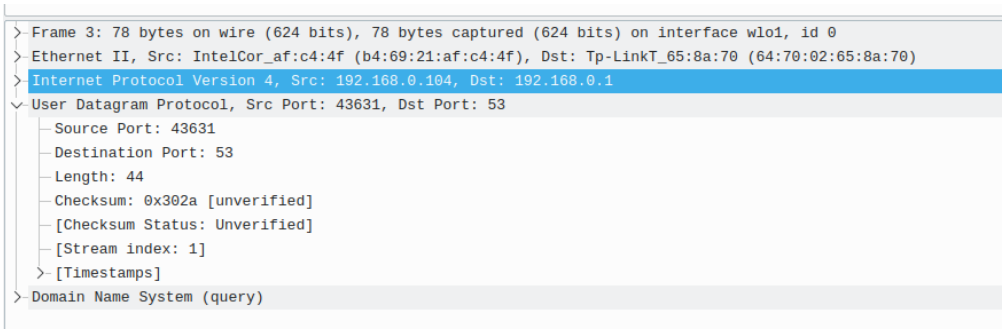
B. DNS-трассировка www.spbu.ru

Порт назначения и источника - 53.

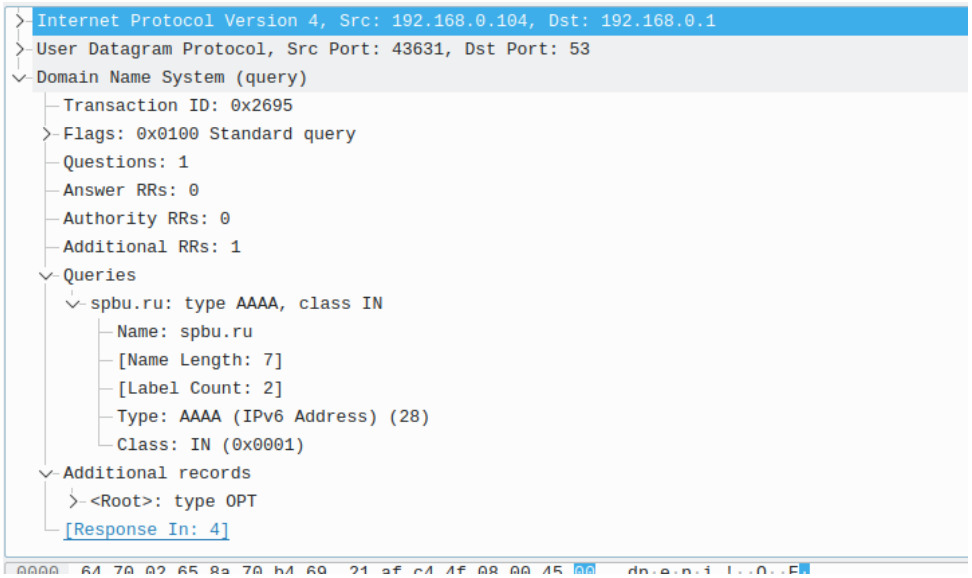




Запрос был отправлен на IP-адрес 192.168.0.1, что совпадает с адресом локального DNS-сервера.



Запрашивается запись типа AAAA, ответов не содержится



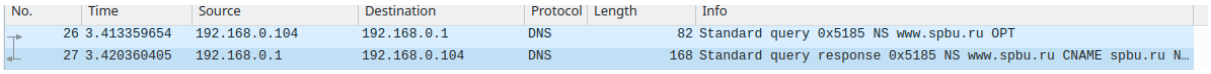
Приходит один ответ, каноническое имя CNAME

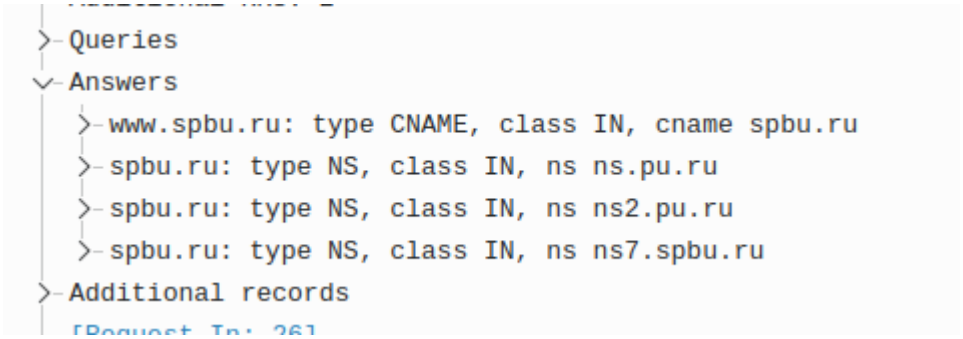
Г. DNS-трассировка nslookup –type=NS

Запрос был отправлен на IP-адрес 192.168.0.1, что все так же совпадает с адресом локального DNS-сервера.

В этот раз запрашиваются данные типа NS, ответов нет.

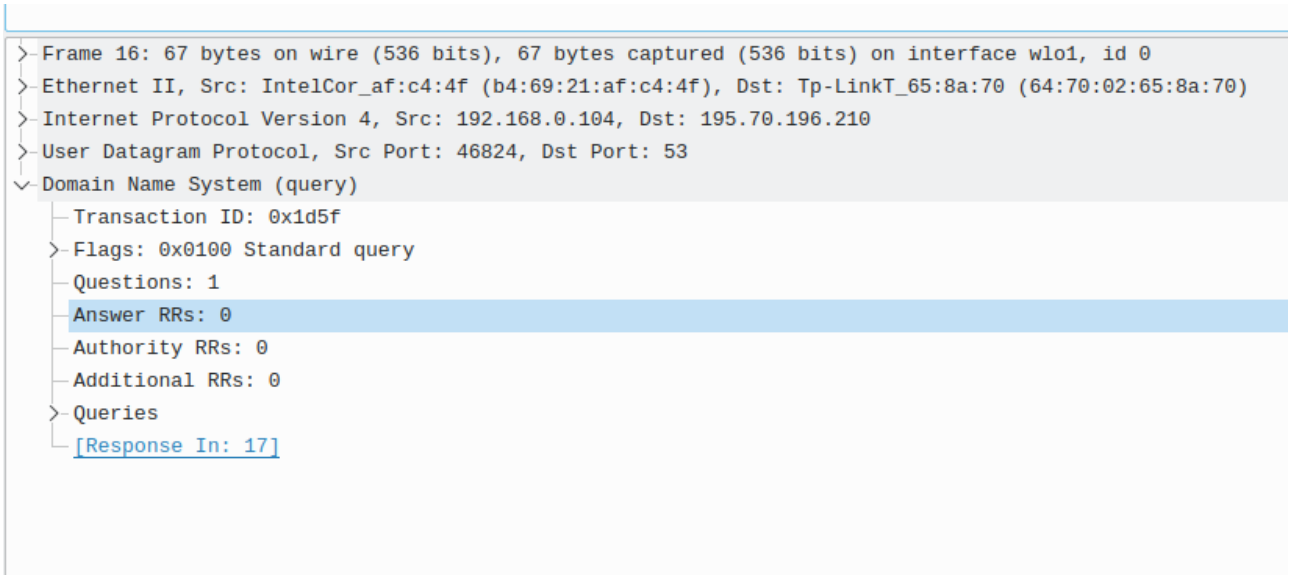
В ответе содержатся имена трех серверов: ns2.pu.ru, ns.pu.ru, ns7.pu.ru, а адресов там нет.



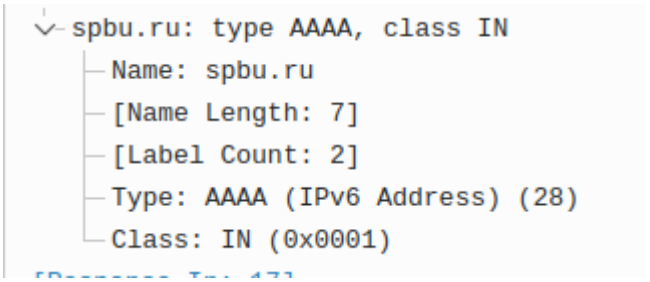


Д. DNS-трассировка nslookup www.spbu.ru ns2.pu.ru

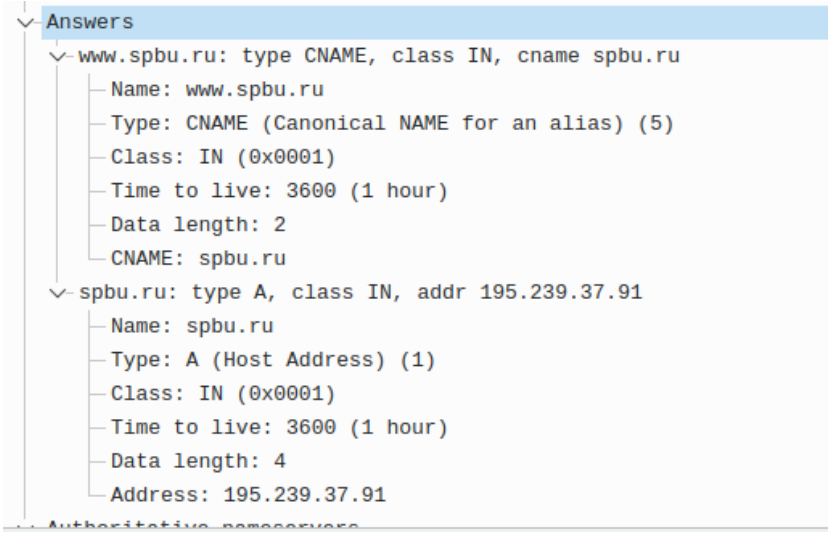
Последний запрос был отправлен на 195.70.196.210. Он принадлежит spbu.ru



Запрашивается тип AAAA, ответов нет.



В последнем ответов не было, а в предпоследнем нашлись два:



E. Сервисы whois

(ссылка на источник https://support.google.com/domains/answer/3288171?hl=ru)
WHOIS – это база данных, в которой хранятся сведения о доменах. В ней можно найти следующую информацию:

- контактные данные регистранта, администратора и технических специалистов;
- сведения о спонсирующем регистраторе;
- дату создания и обновления домена, а также срок его регистрации;
- DNS-серверы и статус домена.

Будем использовать сервис https://www.reg.ru/whois/

Информация реестра

Домен	WILDBERRIES.RU
Сервер DNS	ns1.wildberries.ru. 194.1.214.8
Сервер DNS	ns2.wildberries.ru. 91.230.107.70
Сервер DNS	ns3.wildberries.ru. 62.109.12.21
Состояние	зарегистрирован, делегирован, проверен
Администратор домена	Частное лицо «Private Person»
Регистратор	RU-CENTER-RU
Связь с администратором	— Форма обратной связи с администратором — Обратиться через услугу «Доменный брокер»
Дата регистрации	2004-03-30T20:00:00Z
Дата окончания регистрации	2023-03-30T21:00:00Z
Преимущественное продление до	2023-05-01
Источник	TCI

```
(base) margarita@margarita-HP-Pavilion-Laptop-15-cs0xxx:~$ nslookup www.wildberries.ru 192.168.0.1
Server:         192.168.0.1
Address:        192.168.0.1#53

Non-authoritative answer:
Name:   www.wildberries.ru
Address: 185.138.253.1
Name:   www.wildberries.ru
Address: 185.138.254.1
Name:   www.wildberries.ru
Address: 185.138.252.1
```

```
(base) margarita@margarita-HP-Pavilion-Laptop-15-cs0xxx:~$ nslookup www.wildberries.ru 194.1.214.8
Server:         194.1.214.8
Address:        194.1.214.8#53

Name:   www.wildberries.ru
Address: 185.138.254.1
Name:   www.wildberries.ru
Address: 185.138.253.1
Name:   www.wildberries.ru
Address: 185.138.252.1

(base) margarita@margarita-HP-Pavilion-Laptop-15-cs0xxx:~$
```

```
(base) margarita@margarita-HP-Pavilion-Laptop-15-cs0xxx:~$ nslookup www.wildberries.ru 91.230.107.70
Server:         91.230.107.70
Address:        91.230.107.70#53

Name:   www.wildberries.ru
Address: 185.138.252.1
Name:   www.wildberries.ru
Address: 185.138.254.1
Name:   www.wildberries.ru
Address: 185.138.253.1

(base) margarita@margarita-HP-Pavilion-Laptop-15-cs0xxx:~$
```