[Course | SkillFactory](https://apps.skillfactory.ru/learning/course/course-v1:SKILLFACTORY+hack_pentest+2020/block-v1:SKILLFACTORY+hack_pentest+2020+type@sequential+block@5b7ad135e0cd47fa8778348d17fd2b89/block-v1:SKILLFACTORY+hack_pentest+2020+type@vertical+block@076685b731984aea8c505117f530e56b)

* Модуль 35. Активный и пассивный сбор информации

**35.6. Практика**

## **Задачи**

**1**

1. **Найдите поддомены *skillfactory.ru*, которые имеют веб-страницу.**

**2**

1. **Определите, на каком конструкте построен сайт skillfactory.ru, используя любые инструменты, позволяющие анализировать трафик, приложите скриншот и пояснение.**

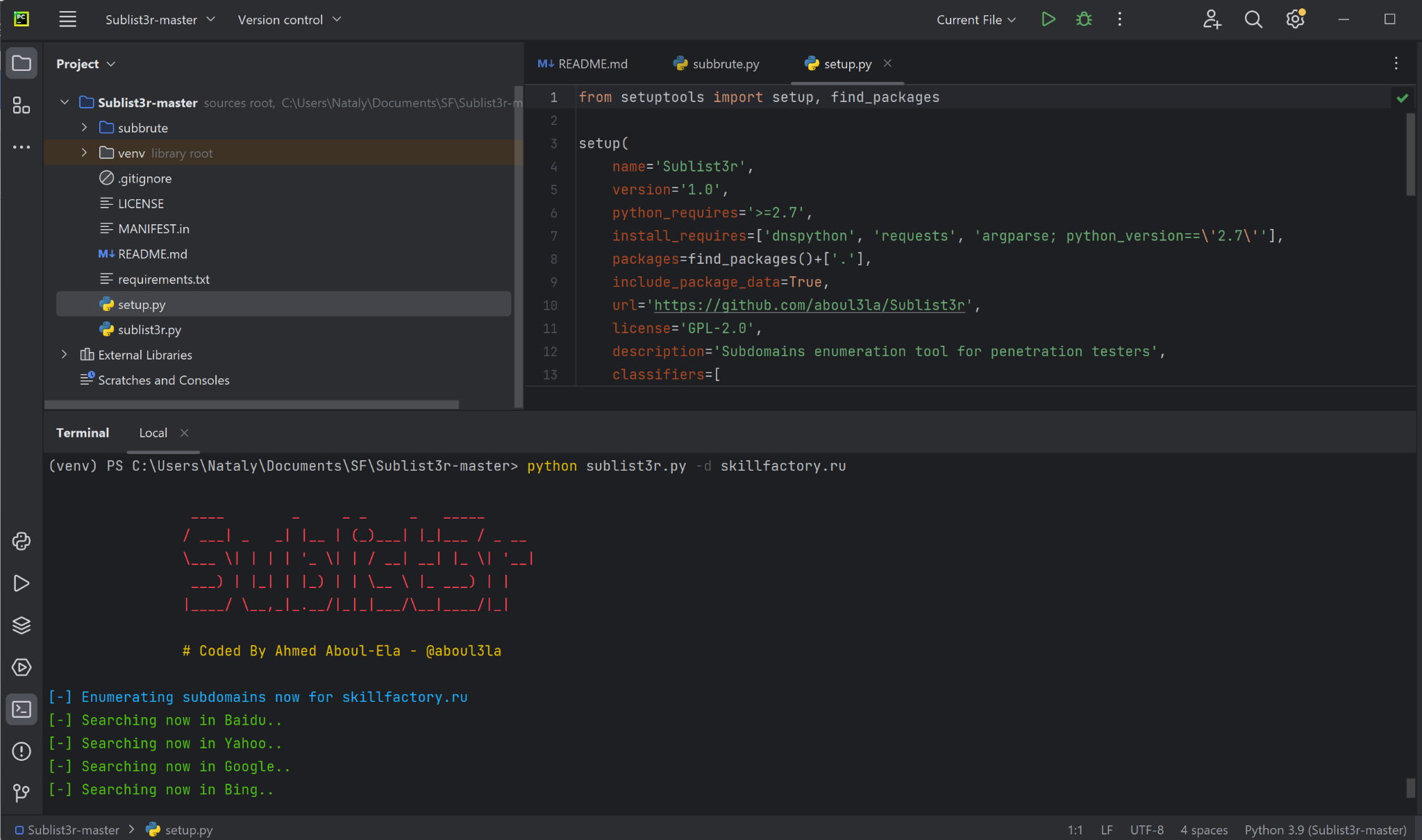
**3**

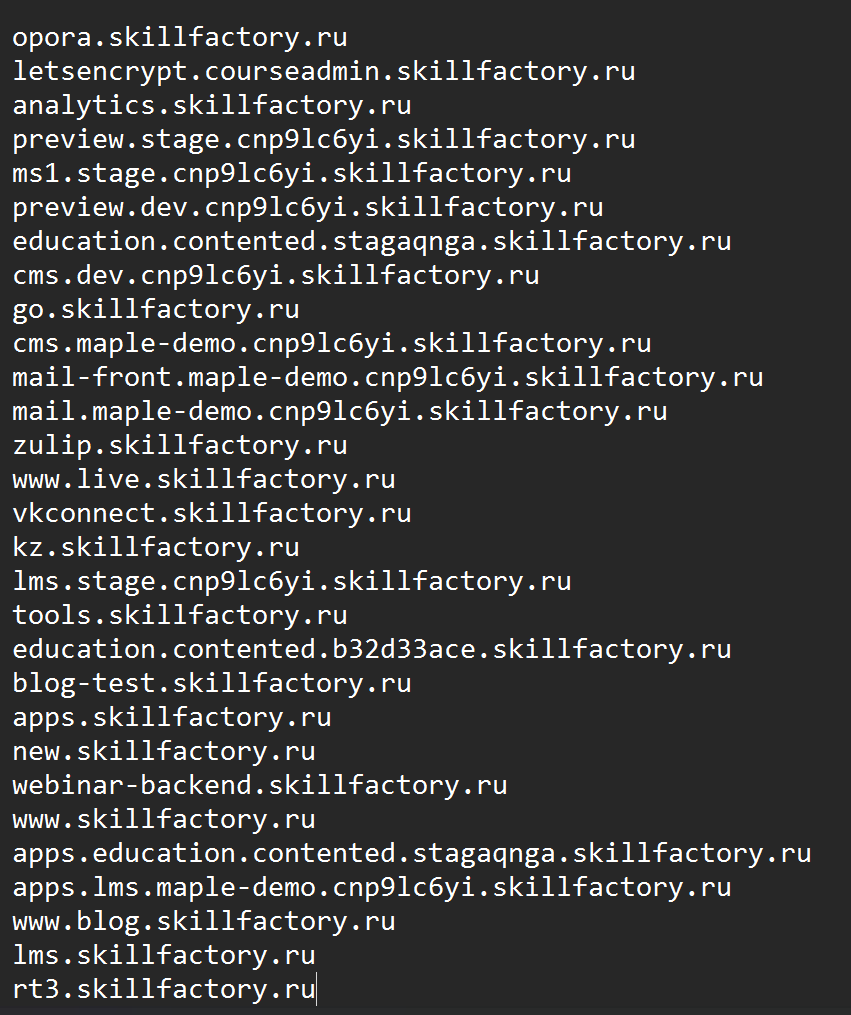
1. **Используя *Censys.io*, найдите точное количество хостов с открытым 445 портом и баннером *SMB 1.0* по России. В ответе напишите количество и как можно использовать эту информацию.**

## Решение

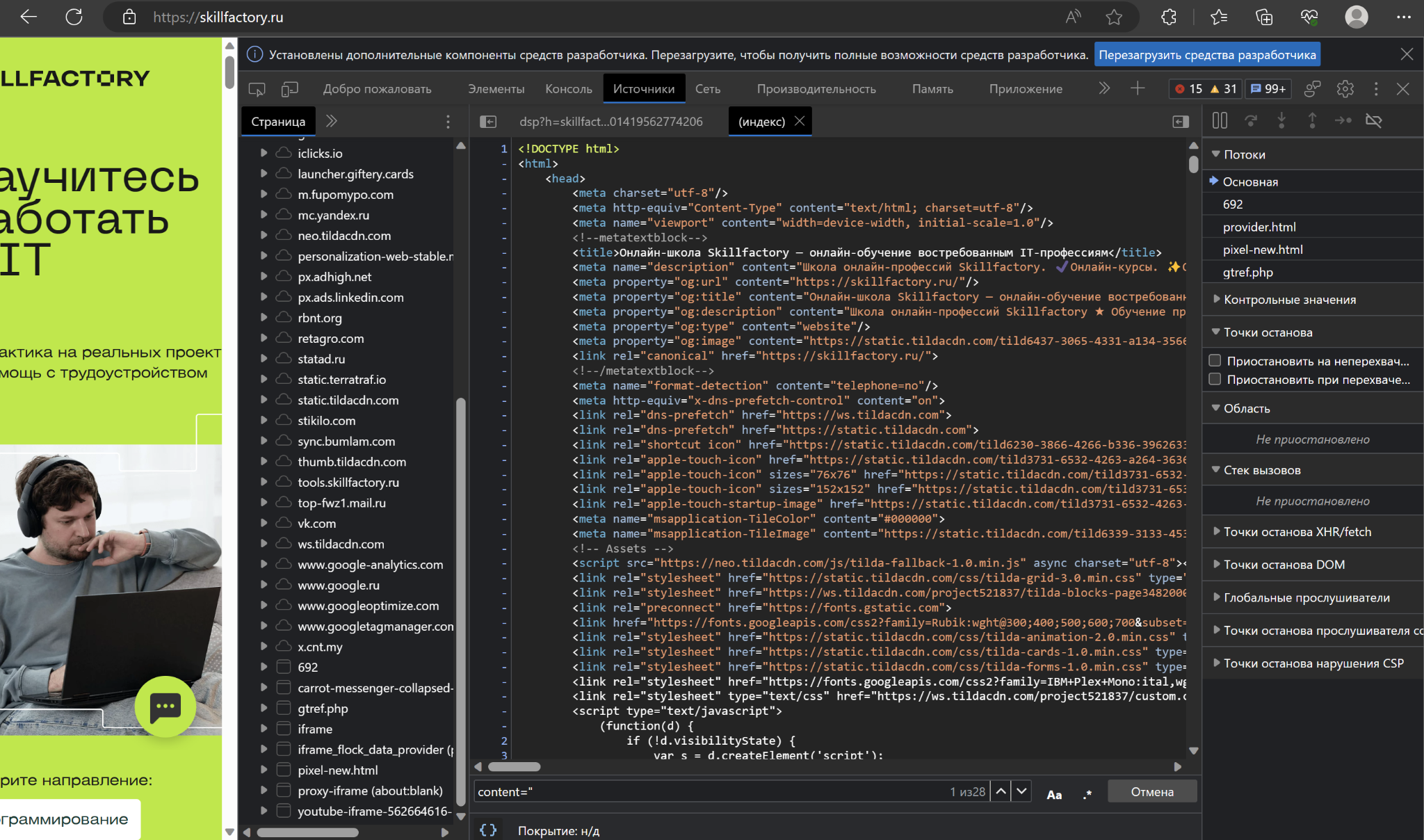
1. **Использую** [**GitHub - aboul3la/Sublist3r: Fast subdomains enumeration tool for penetration testers**](https://github.com/aboul3la/Sublist3r)

Для поиска поддоменов *skillfactory.ru напишу команду* ***python sublist3r.py -d skillfactory.ru***

****

****

1. **Можно использовать DevTools. Посмотреть в тегах <meta> атрибуты и видно очень частое использование слова “tilda”. Делаю вывод - cms сделан на Tilda.**

****