

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**Український державний університет науки і технологій**

Кафедра «Комп’ютерні інформаційні технології»

**Лабораторна робота №2  
з дисципліни «Безпека програм та даних»**

**на тему:**

**«**Проведення розвідки на основі відкритих джерел.»

Виконав:

студент гр. ПЗ2011

Кулик С.В.

Прийняв:

доц. Жеваго О. О.

Дніпро, 2023

**Тема.** Проведення розвідки на основі відкритих джерел.

**Мета.** Ознайомитись з основними інструментами проведення розвідки на основі

відкритих джерел.

**Завдання**

1. Оберіть організацію, яка, на вашу думку, заслуговує на вашу увагу. Це може бути навчальний заклад, комерційна компанія або, неприбуткова організація.

2. В адресному рядку браузера перейдіть за адресою {site}/robots.txt. Проаналізуйте вміст файлу. Зробіть висновки про наявність "прихованих" директорій.

3. Перейдіть за адресою http://www.google.com. Задайте пошукові запити, наприклад:

▪ site:{site} filetype:docx confidential

▪ site:{site} filetype:doc secret

▪ site:{site} inurl:admin

▪ site:{site} filetype:sql

▪ site:{site} intext: "Access denied"

Проаналізуйте логіку запитів і отримані дані. Побудуйте свої запити.

4. Перейдіть за адресою <https://www.tutorialspoint.com/google_hacking_tests.htm>. Перевірте вебресурс обраної для аналізу організації.

5. Перейдіть за адресою <https://www.exploit-db.com/google-hacking-database>. Оберіть 3 запити, та перевірте вебресурс обраної для аналізу організації.

6. Виконайте збір інформації про організацію. Знайдіть:

* сайт;
* ip адресу (ping);
* інформацію про DNS (nslookup);
* хостінг (ip2location);
* операційну систему - використовуйте інструмент Netcraft;
* визначте правила формування поштових облікових записів, наприклад використовуючи Web Data Extractor;
* знайдіть документи з розширенням PDF на домені організації;
* посилання на сторінку входу.

7. За допомогою Wireshark знайдіть всі GET запити на головній сторінці, та проаналізуйте їх.

Для збору інформації обов’язково повинні бути використані наступні інструменти:

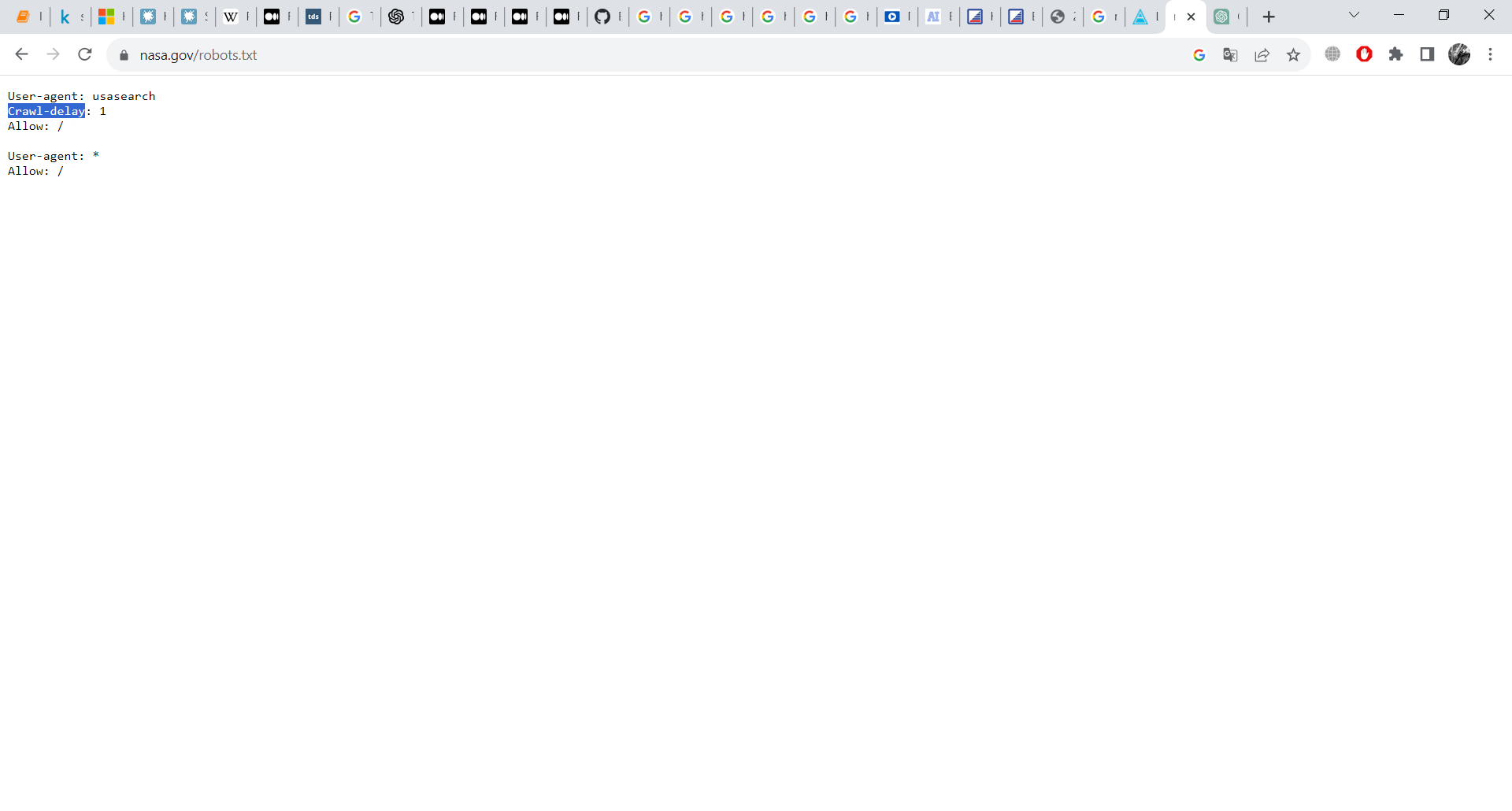
* ping;
* nslookup;
* https://who.is — щоб отримати детальну інформацію про доменне ім'я;
* Wireshark — для перехоплення пакетів.

**Індивідуальне завдання**

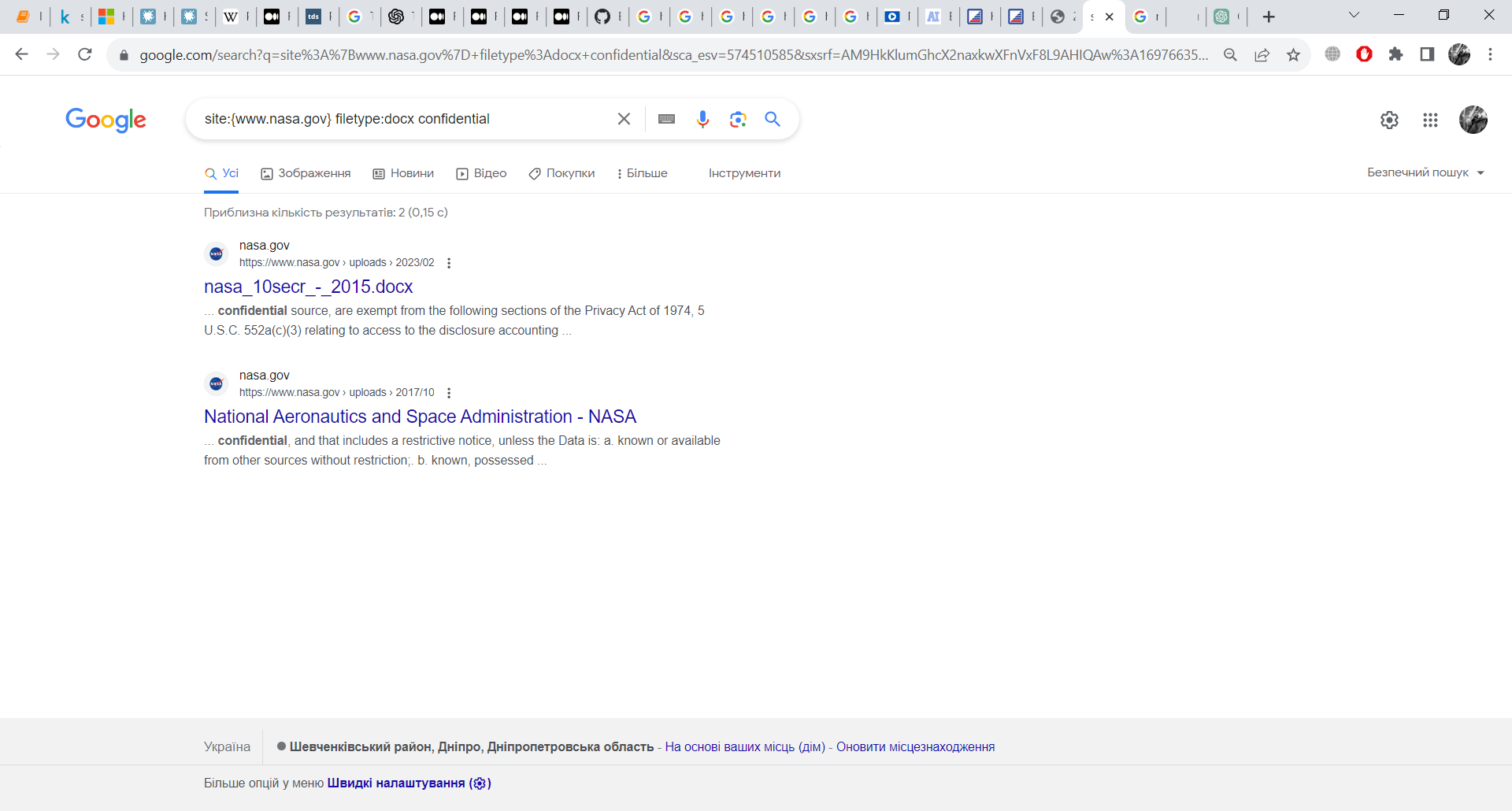
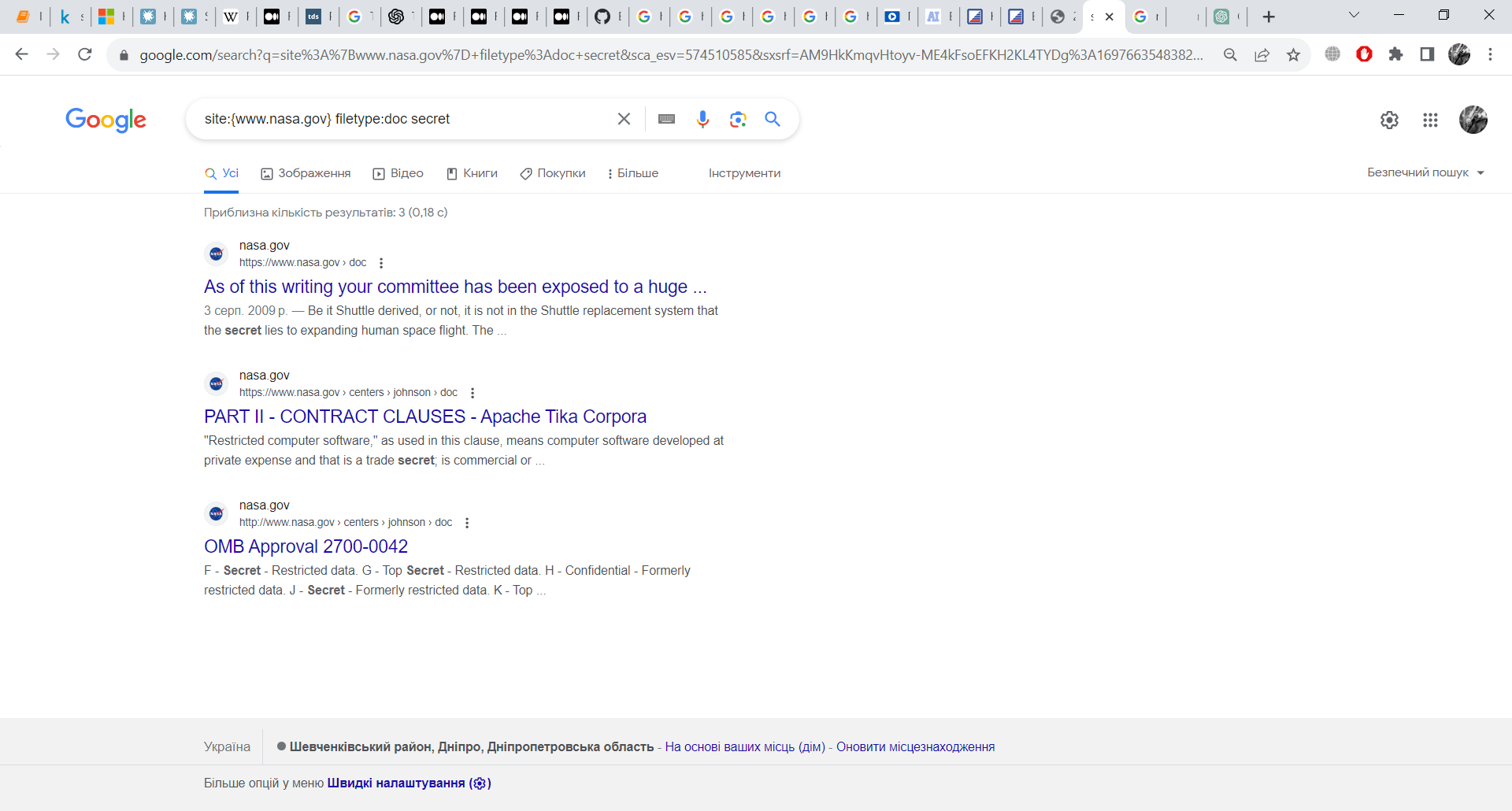
Сайт для аналізу - <https://www.nasa.gov/>

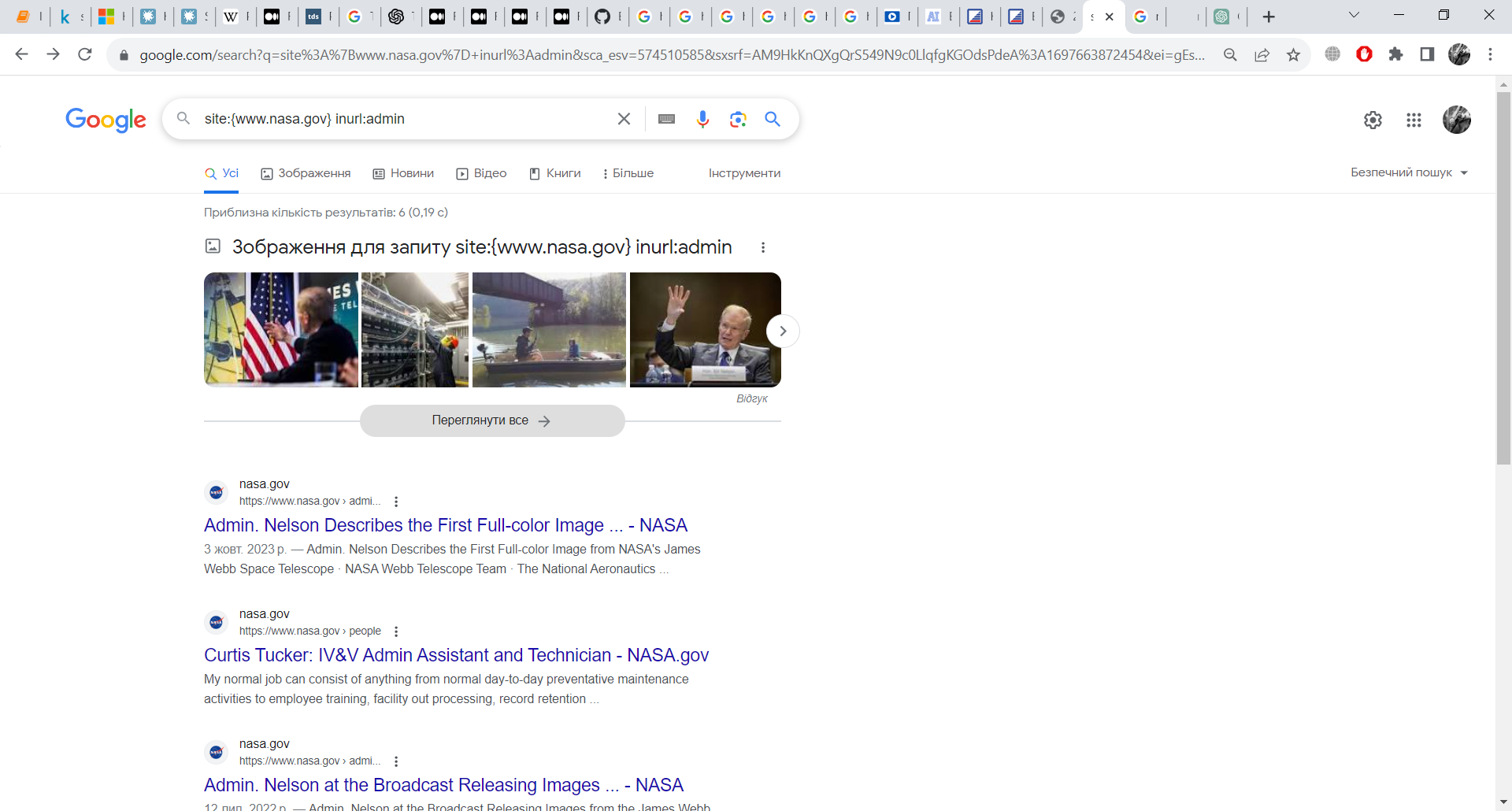
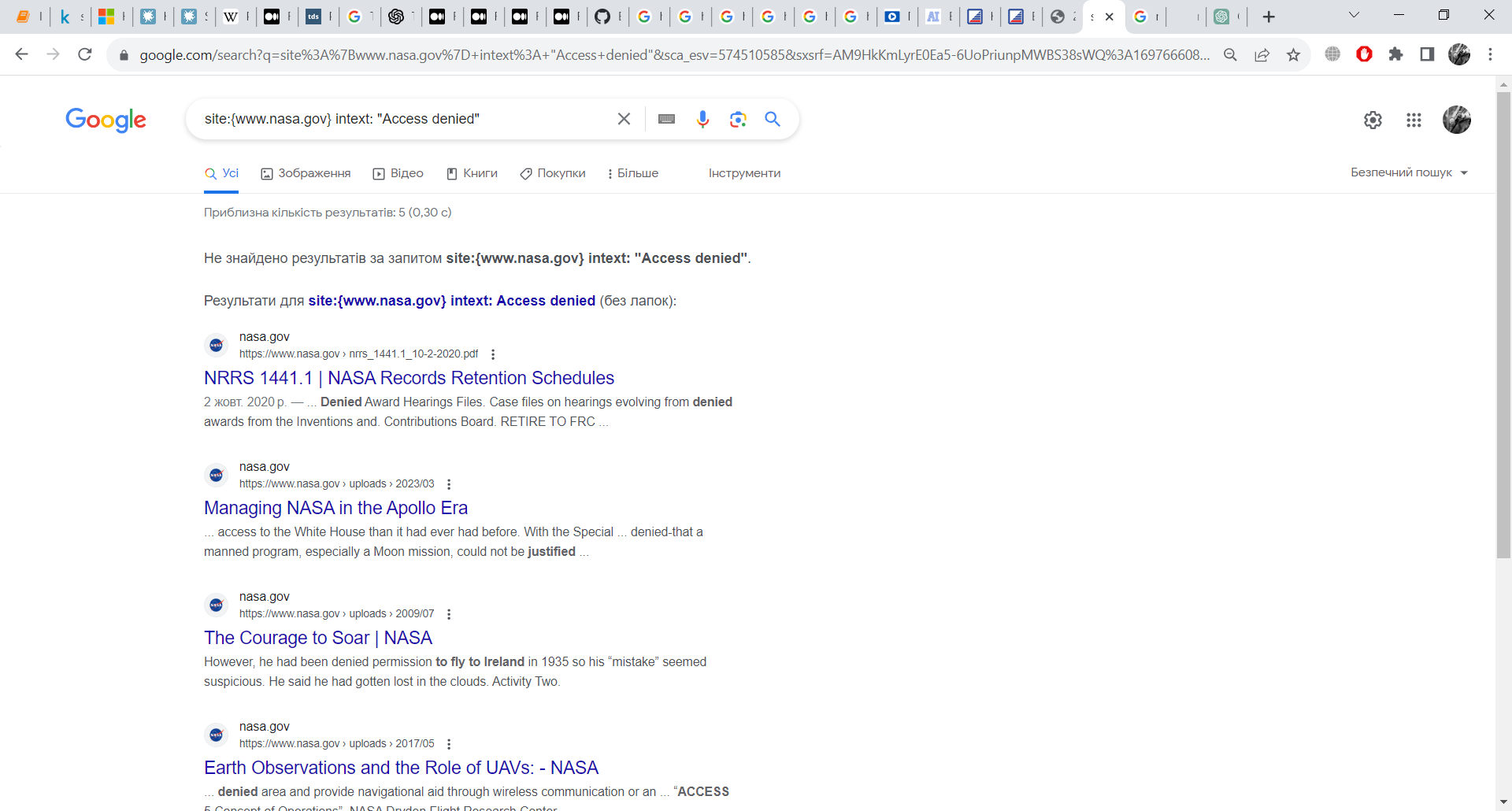
**Опис дій по збору інформації**

1. Аналіз файлу robots.txt показує, що в ньому нема прихованих папок, а також встановлено час переходу між сторінками в 1 секунду.



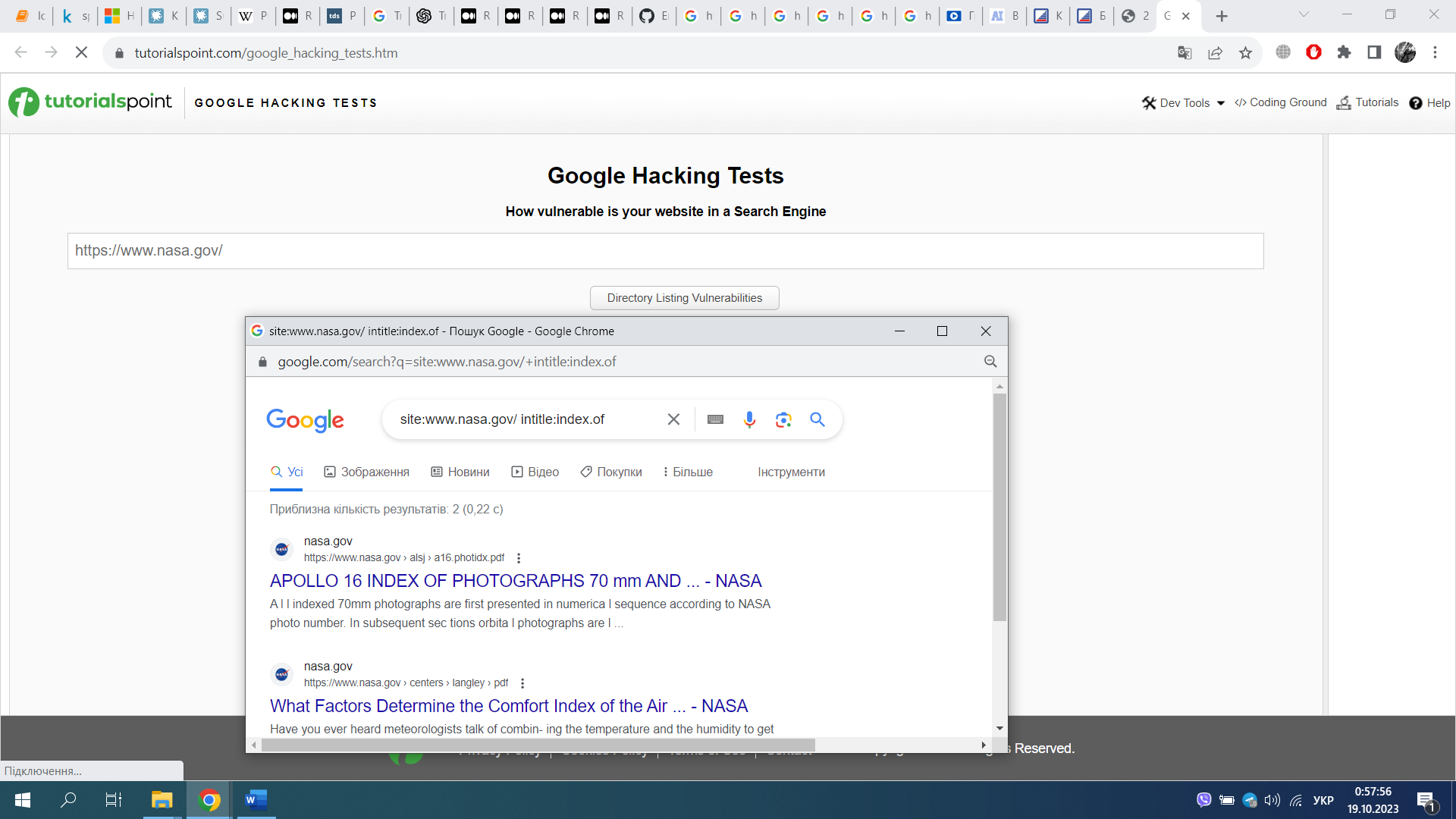
1. Аналіз за допомогою пошукових запитів.

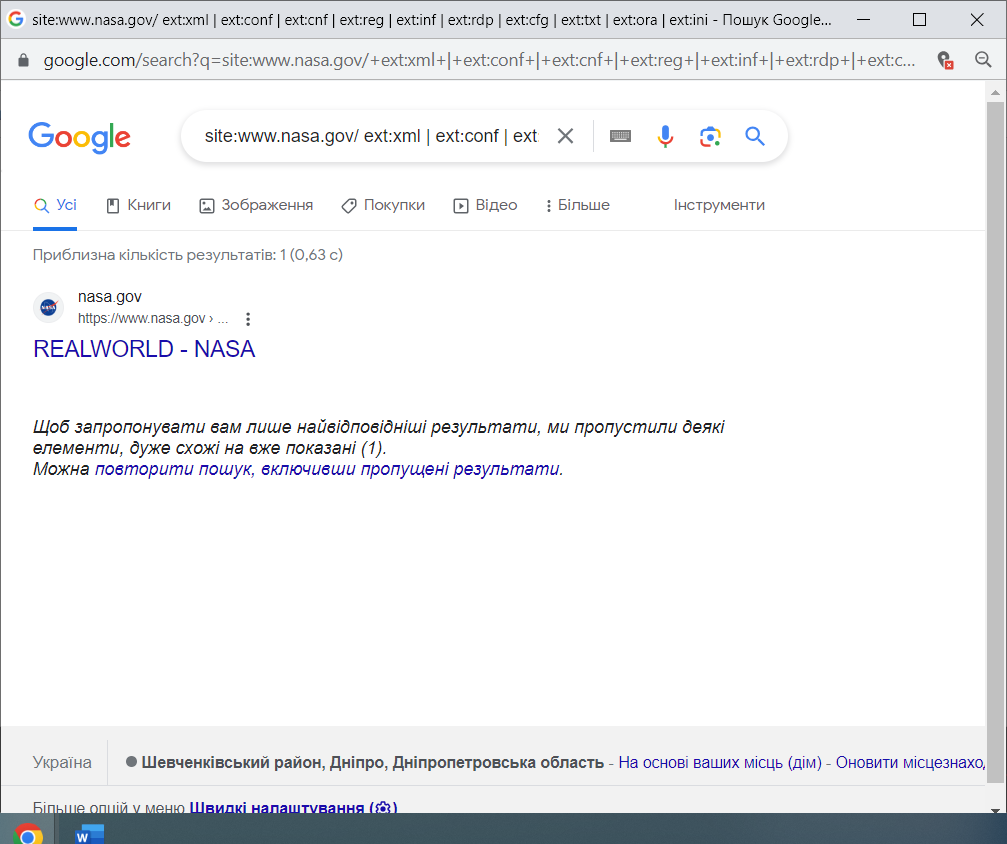
 

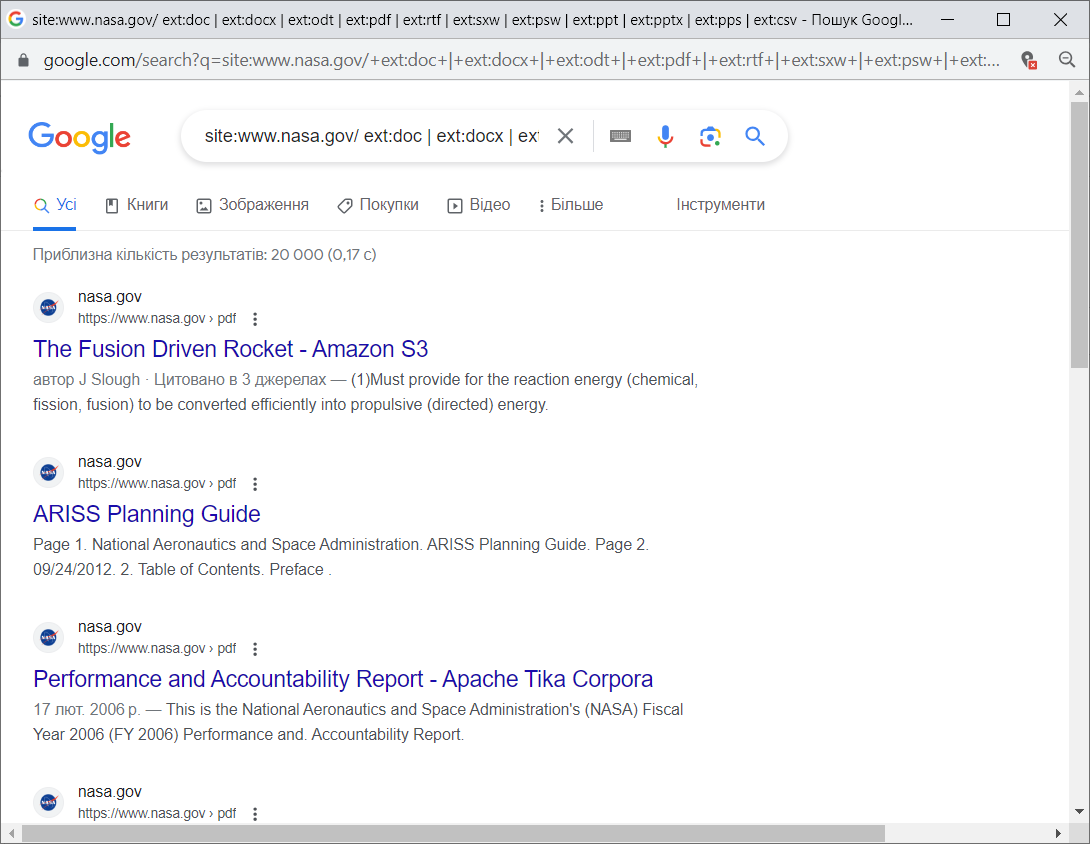
 

Дослідивши дані файли можна знайти багато цікавої інформації.

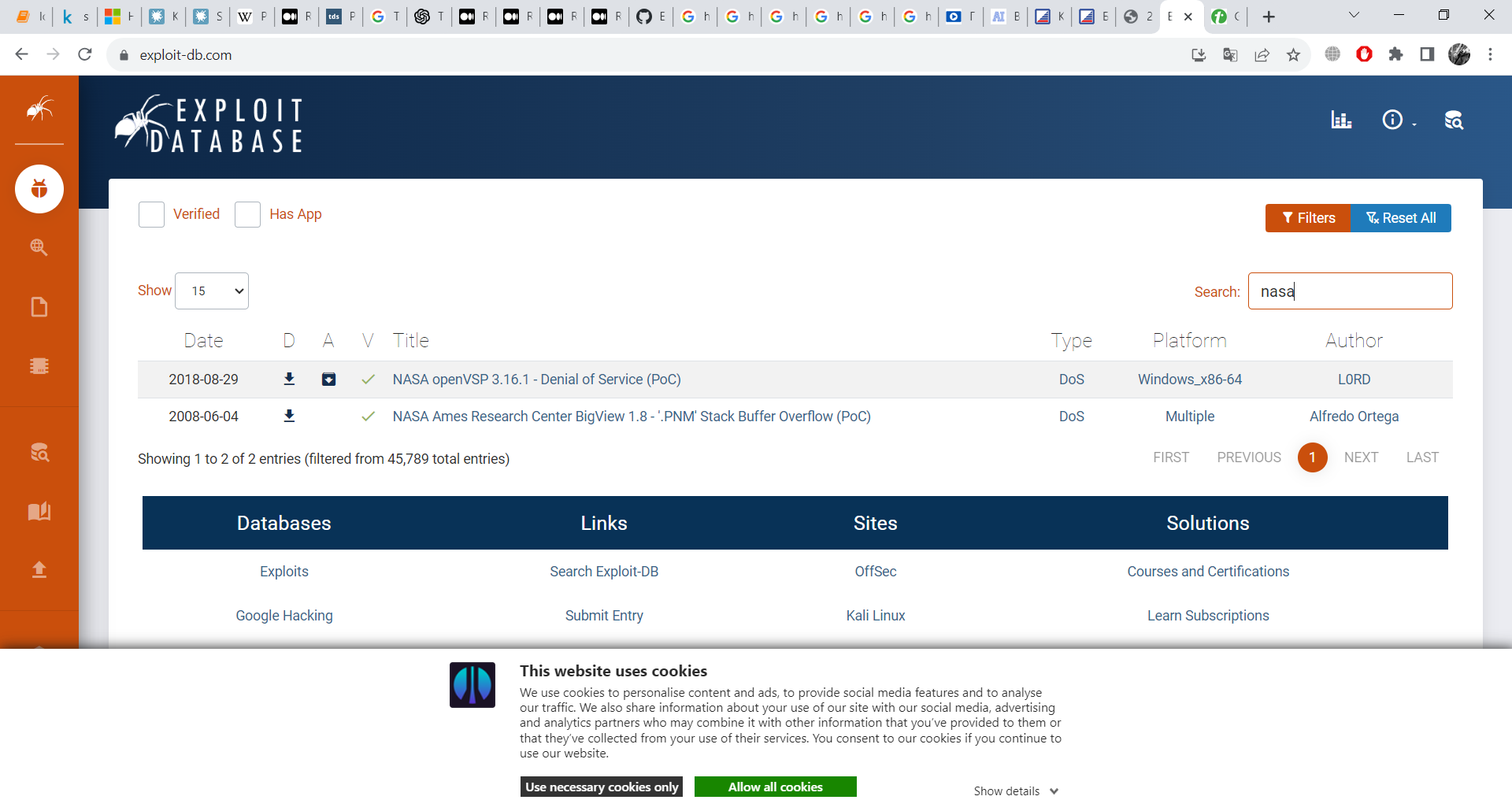
1. Результати перевірки обраної організації <https://www.nasa.gov/> за допомогою <https://www.tutorialspoint.com/google_hacking_tests.htm>



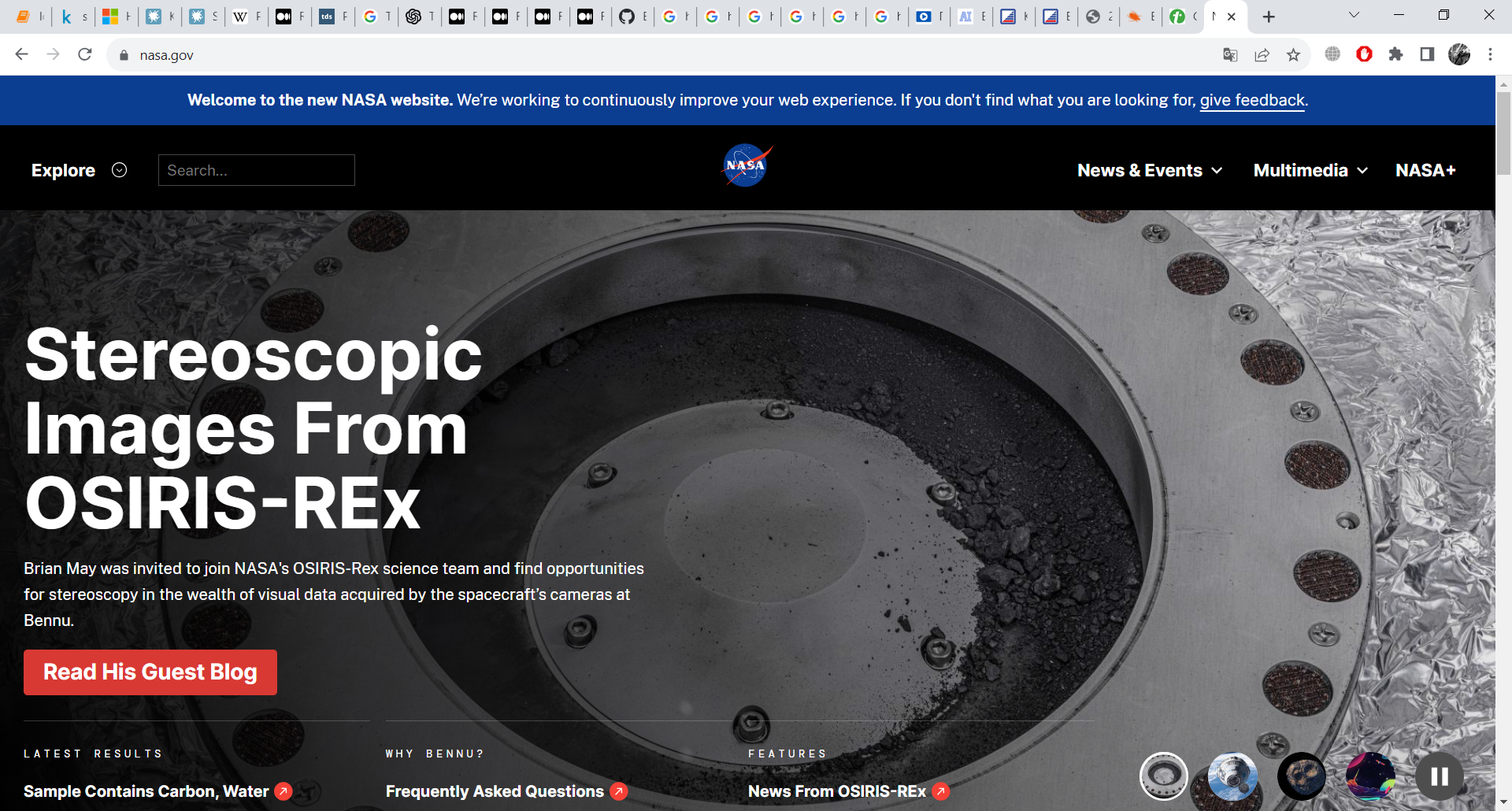


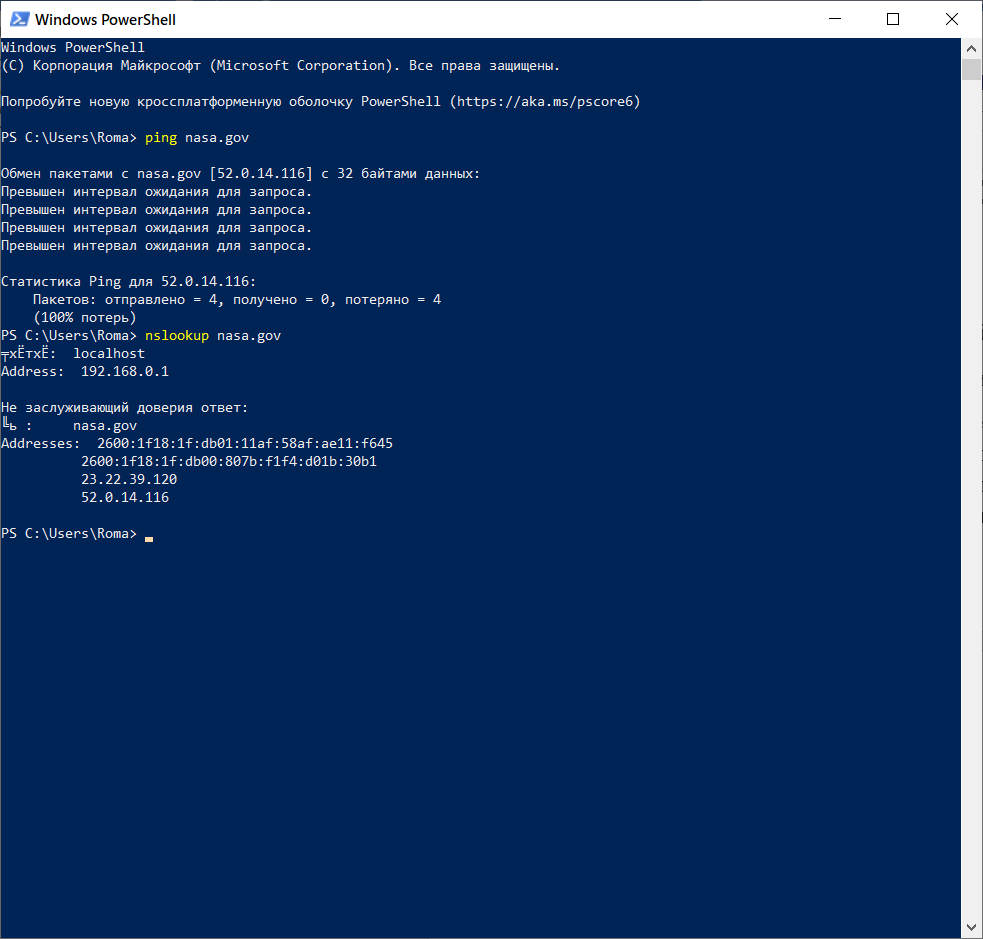


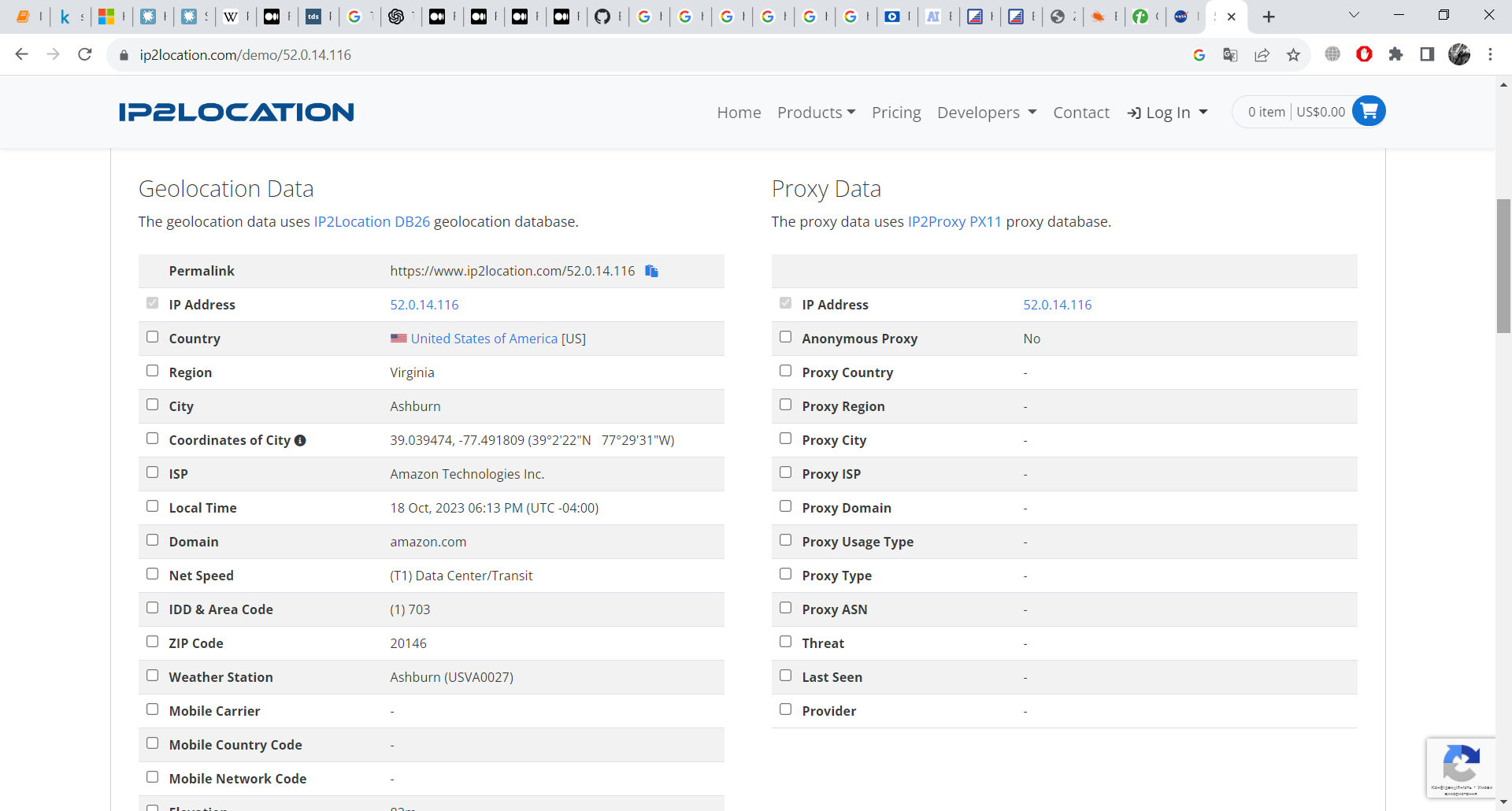
1. Результати перевірки обраної організації <https://www.nasa.gov/> за допомогою <https://www.exploit-db.com/google-hacking-database>



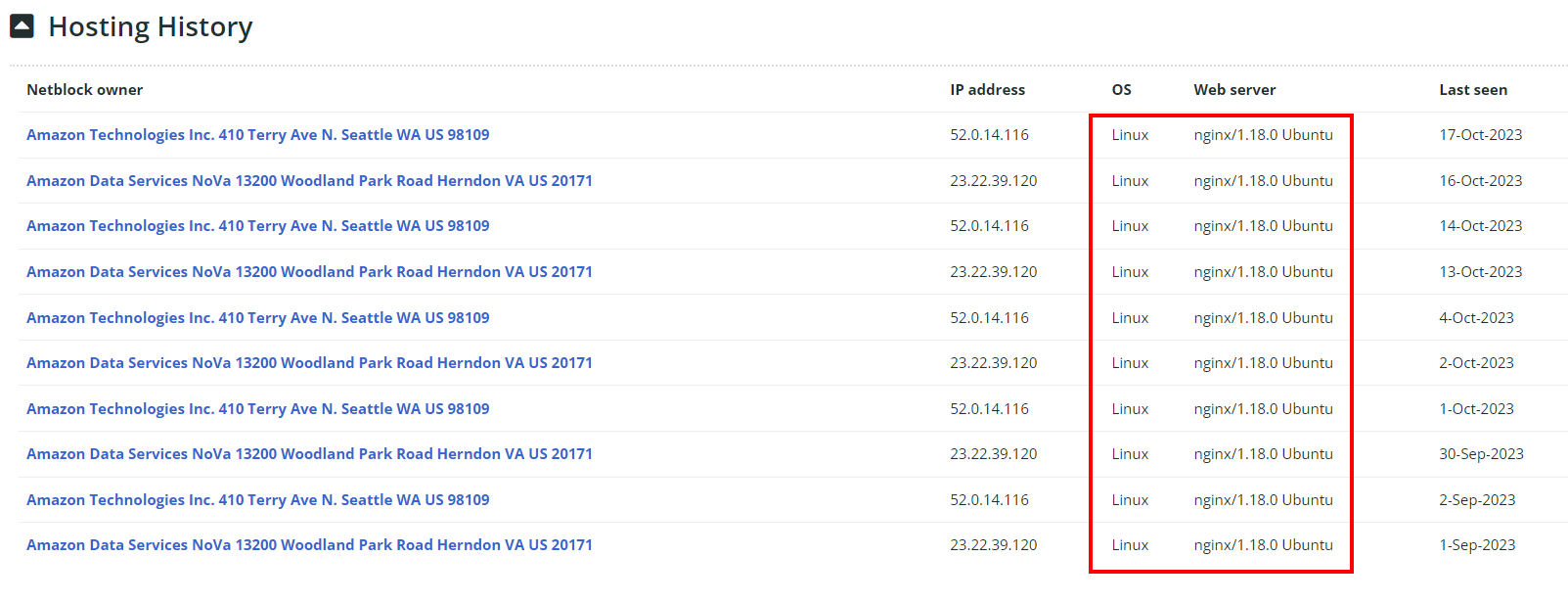
1. Збір інформації про організацію:
   * Сайт:



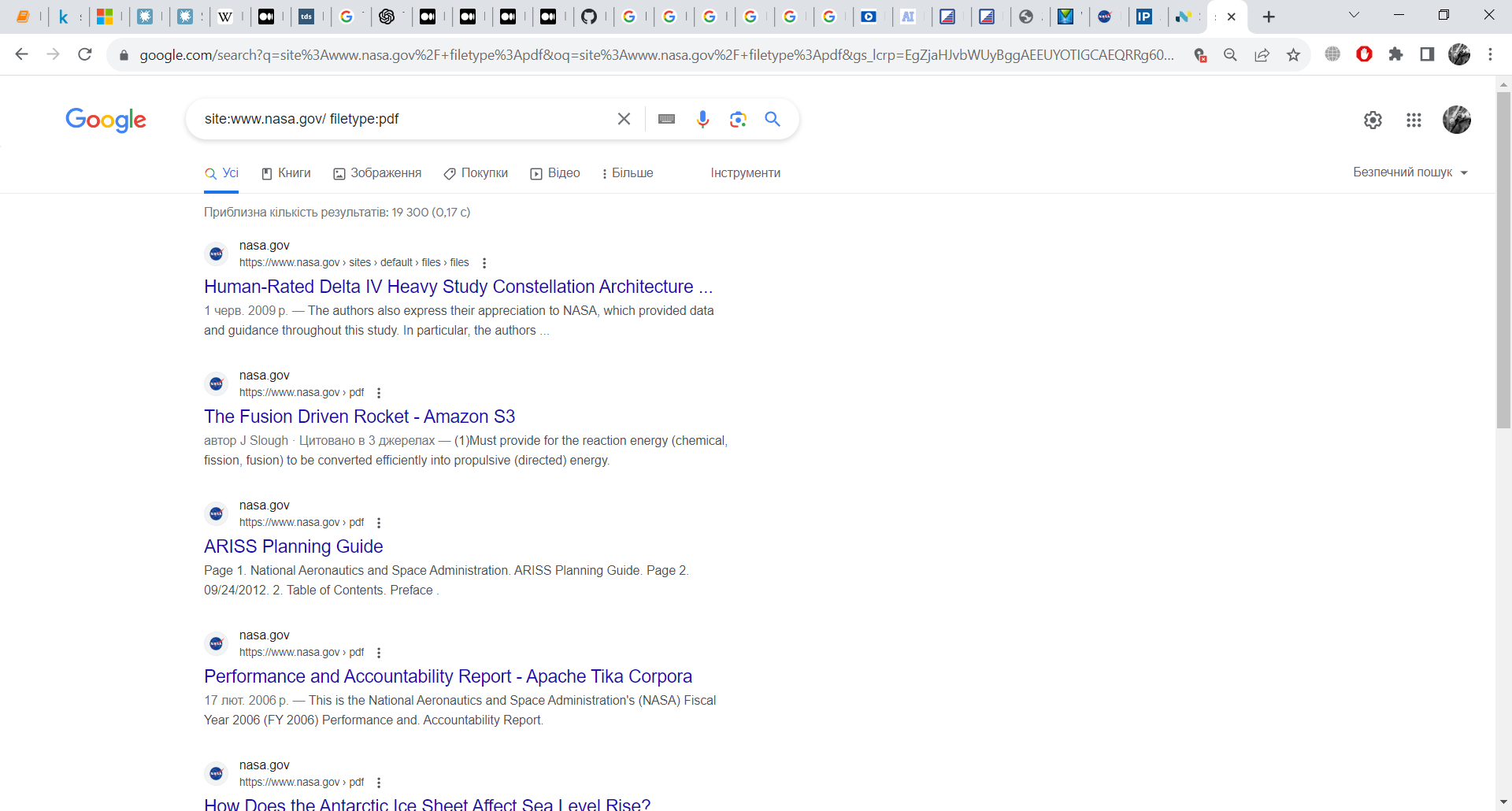
* ip адреса: 52.0.14.116
* Інформація про DNS: 
* Адреса за ip-адресом:



* Операційна система:

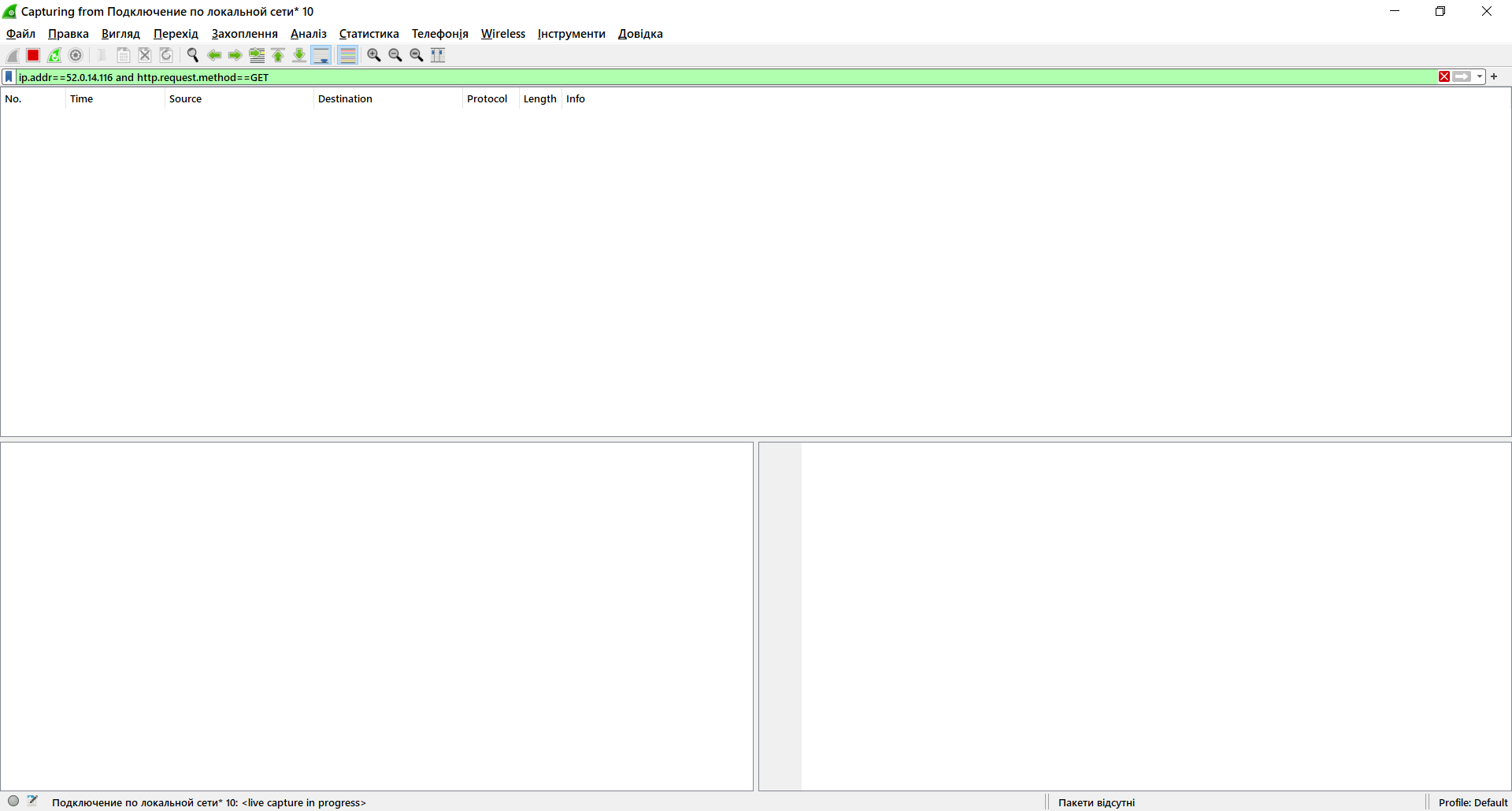


* Знайти файли з розширенням .pdf:



1. Пошук всіх GET запитів на головній сторінці за допомогою Wireshark.

ip.addr==52.0.14.116 and http.request.method==GET



**Висновки**

Проведена розвідка на основі відкритих джерел підкреслює важливість доступності інформації в Інтернеті для розвідки. За допомогою різноманітних інструментів, таких як веб-скрапінг та аналіз соціальних мереж, можна отримати різноманітну інформацію. Проте, важливо бути обережними і критично оцінювати джерела, оскільки інформація може бути недостовірною. Дотримання законодавства і етичних стандартів є обов'язковим. Постійне вдосконалення навичок є необхідним у зв'язку з технологічним розвитком.