✨1. INFORMATION GATHERING (RECONNAISSANCE)

Thursday, July 29, 2021 8:31 AM

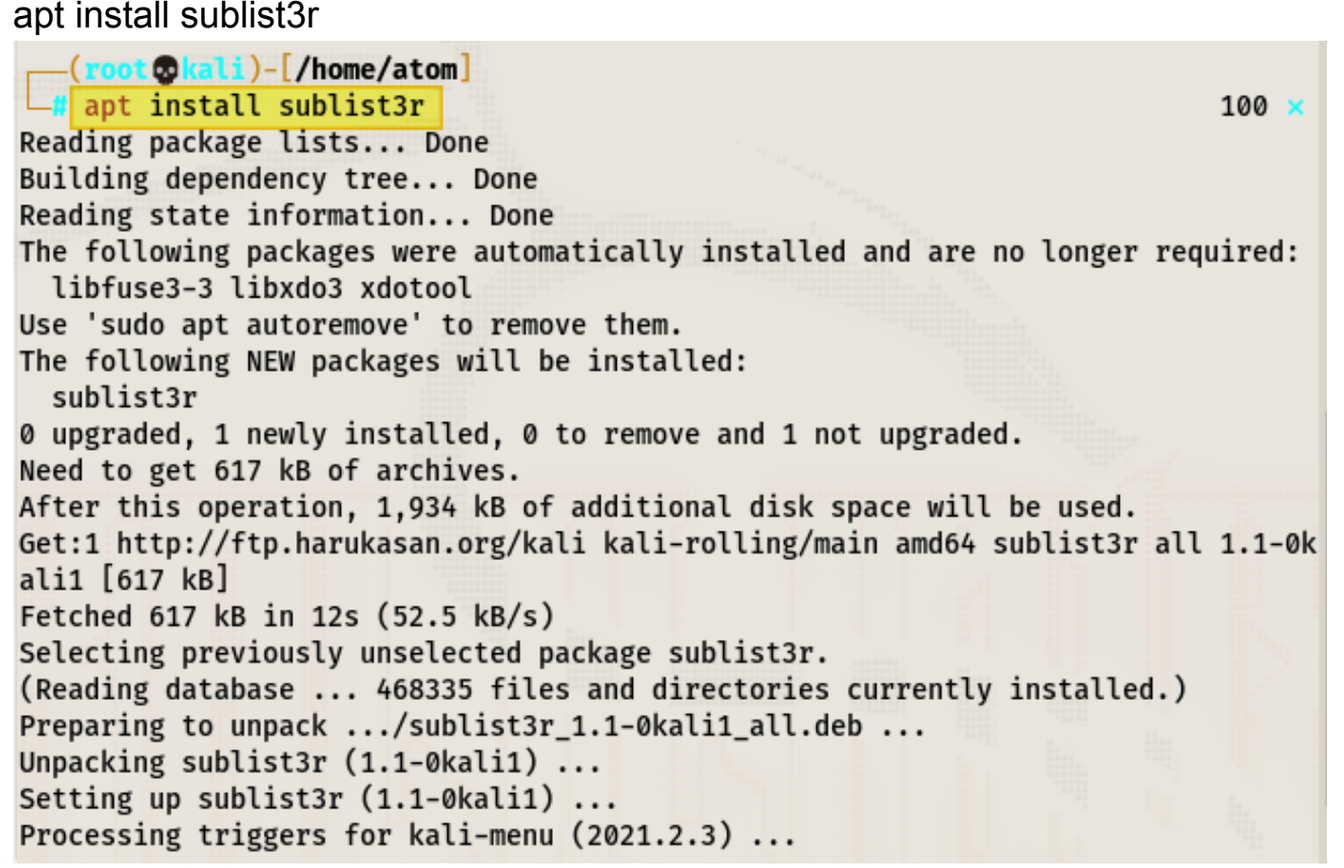
1. **PASSIVE RECONNAISSANCE**
   a. **PHYSICAL/SOCIAL**
      - LOCATION INFORMATION-
        - Satellite Images
        - Drones Recon
        - Building Layout (badge readers, break areas, security, fencing)
      - JOB INFORMATION-
        - Employees (names, job title, phone numbers, managers, etc.)
        - Pictures (badge photos, desk photos, computer photo, etc.)

   b. **WEB/HOST**
      - Target Validation-
        - WHOIS, nslookup, dnsrecon
      - Finding Subdomains-
        - Google Fu, dig, Nmap, Sublist3r, Bluto, crt.sh, etc.
      - Fingerprinting-
        - Nmap, Wappalyzer, Whatweb, BuiltWith, Netcat
      - Data Breacher-
        - HavelBeenPwned, Breach-Parse, WeLeakInfo

2. **IDENTIFYING OUR TARGET-**
   a. Search for domain emails and employees-
      i. http://hunter.io/search

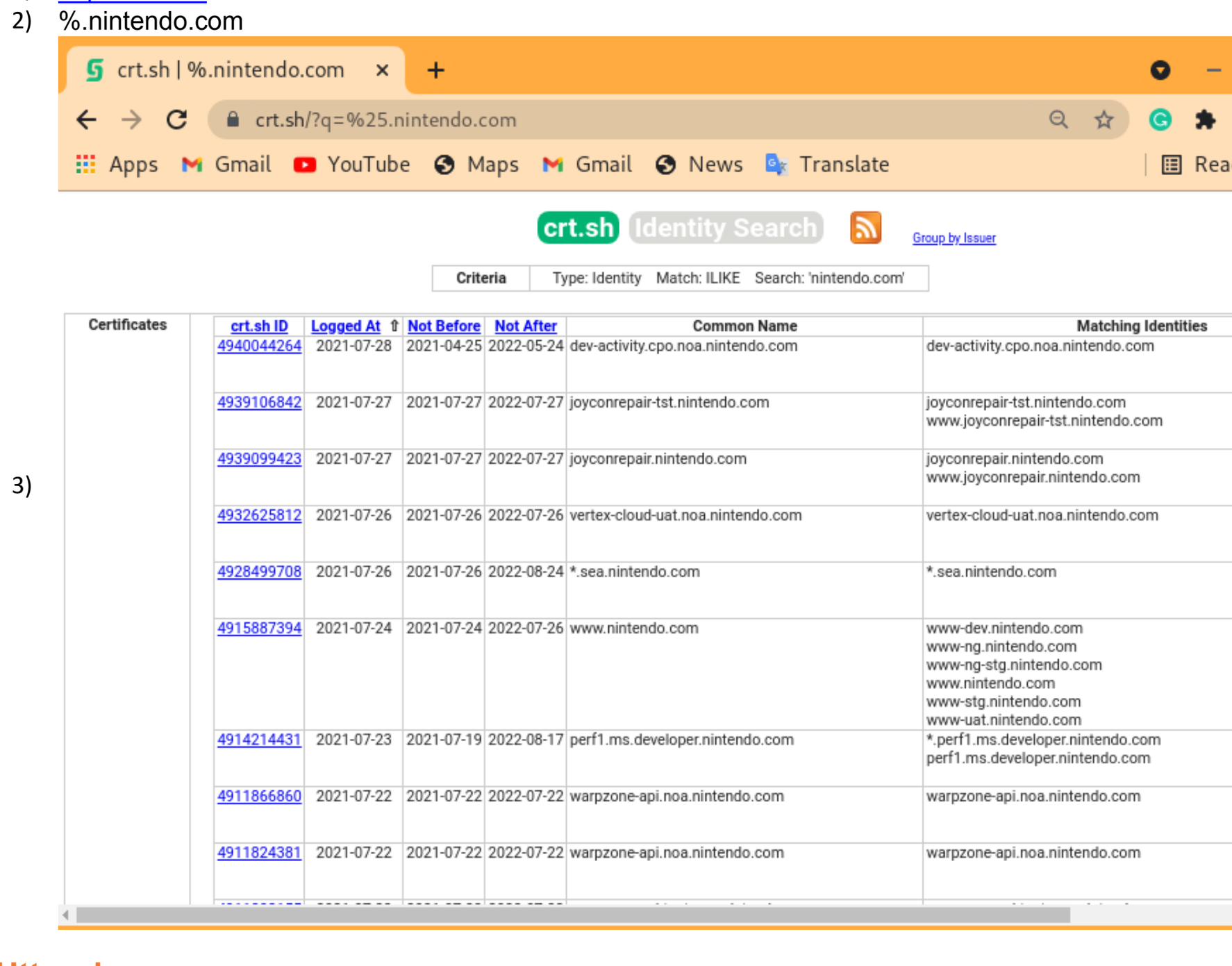
   b. Searching username and password in breaches-
      i. Searching for breaches in google
      ii. Use Breach-Parse

   c. Hunting Subdomains-
      i. **Sublist3r**
         1) apt install sublist3r
         2)

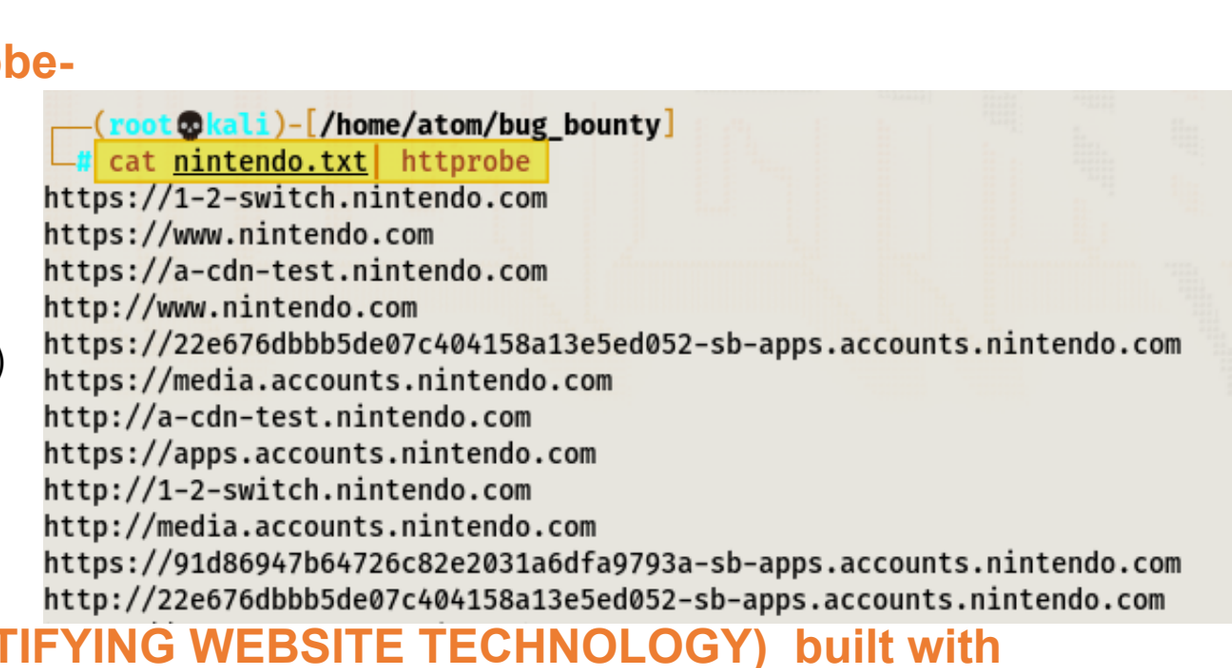


         3) sublist3r -d nintendo.com
         4)

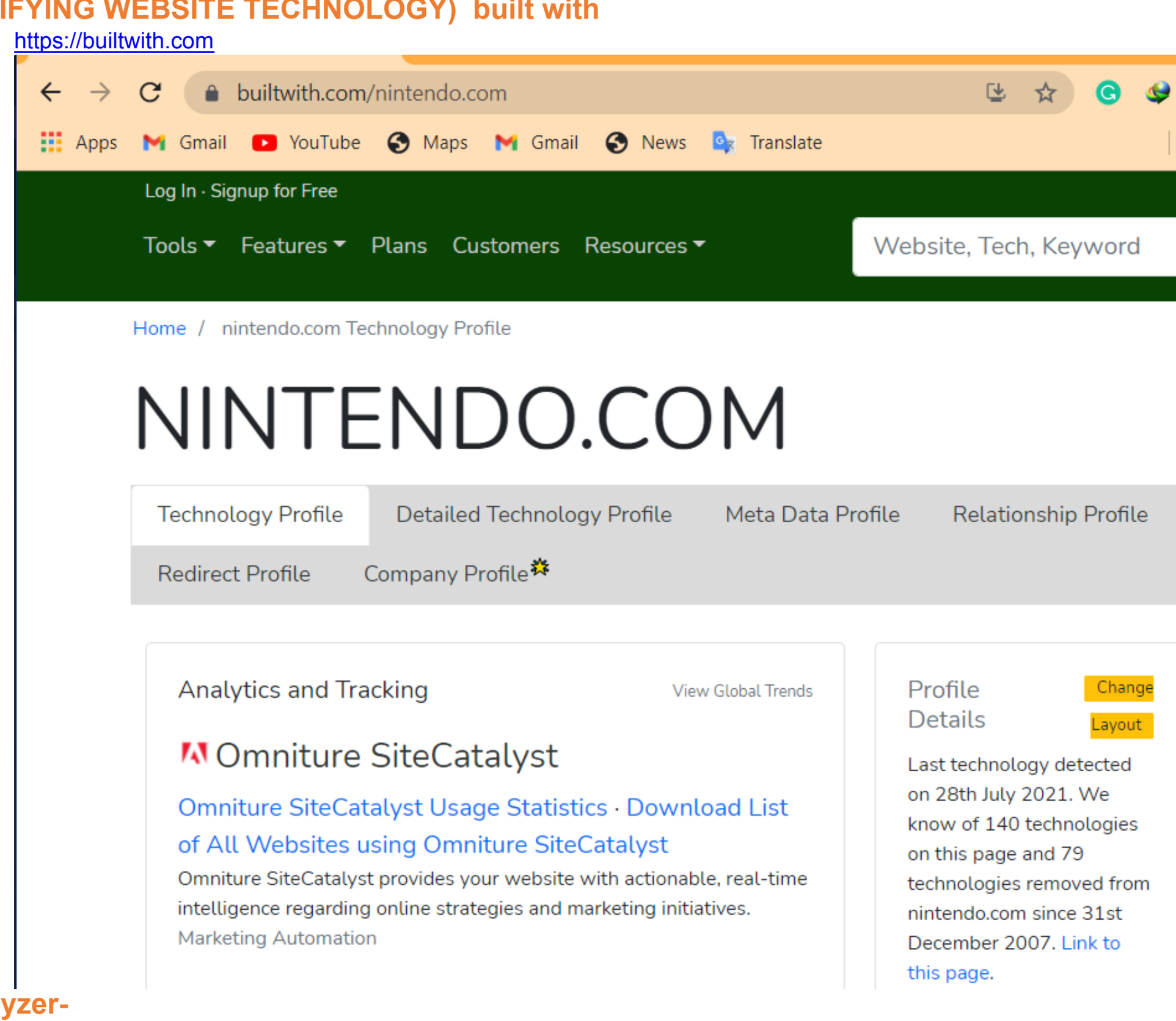
      ii. **crt.sh**
         1) https://crt.sh/
         2) %.nintendo.com
         3)



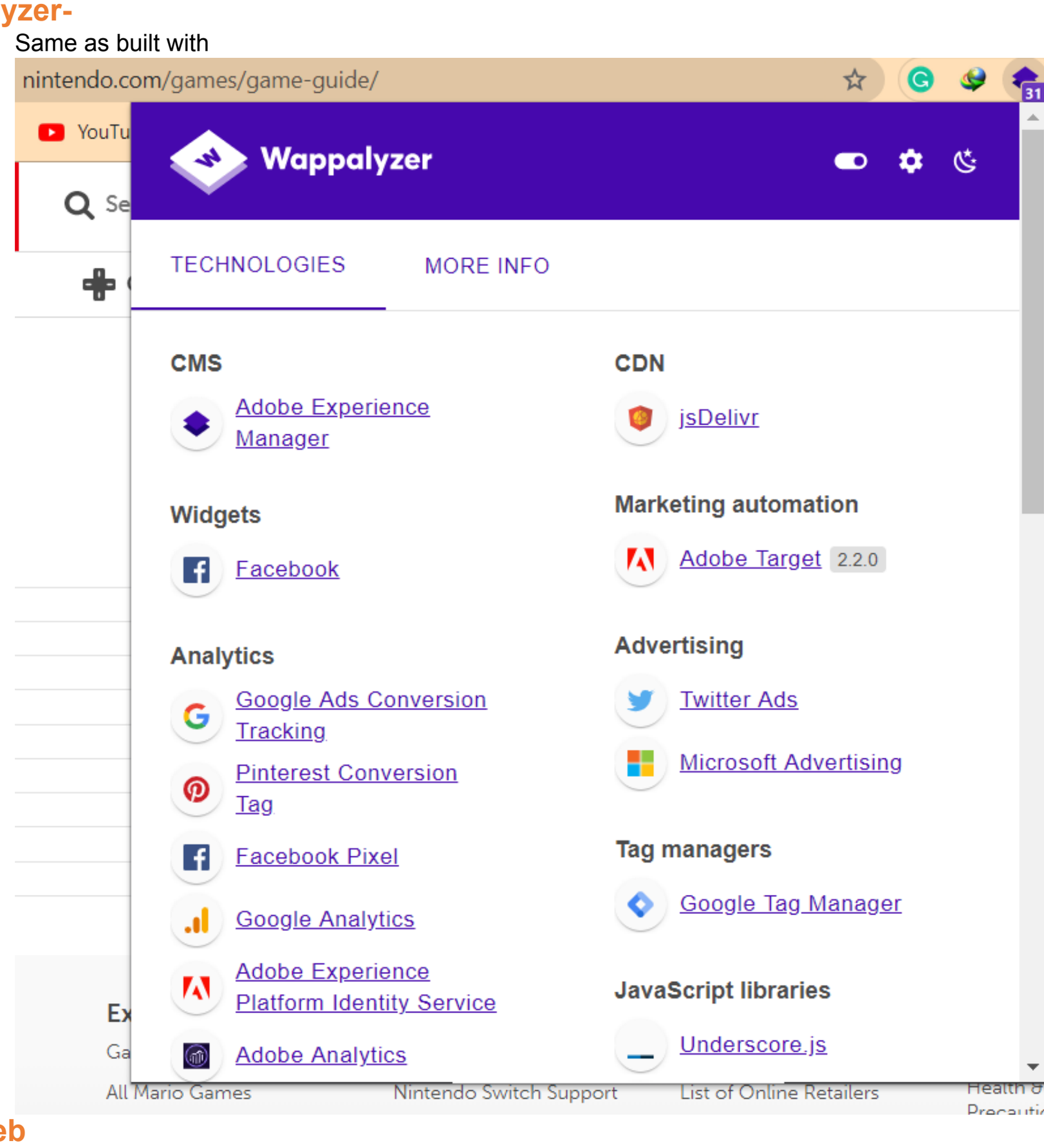
      iii. **Httprobe-**
         a)



      iv. **(IDENTIFYING WEBSITE TECHNOLOGY) built with**
         a) https://builtwith.com
         b)



      v. **wappalyzer-**
         a) Same as built with
         b)



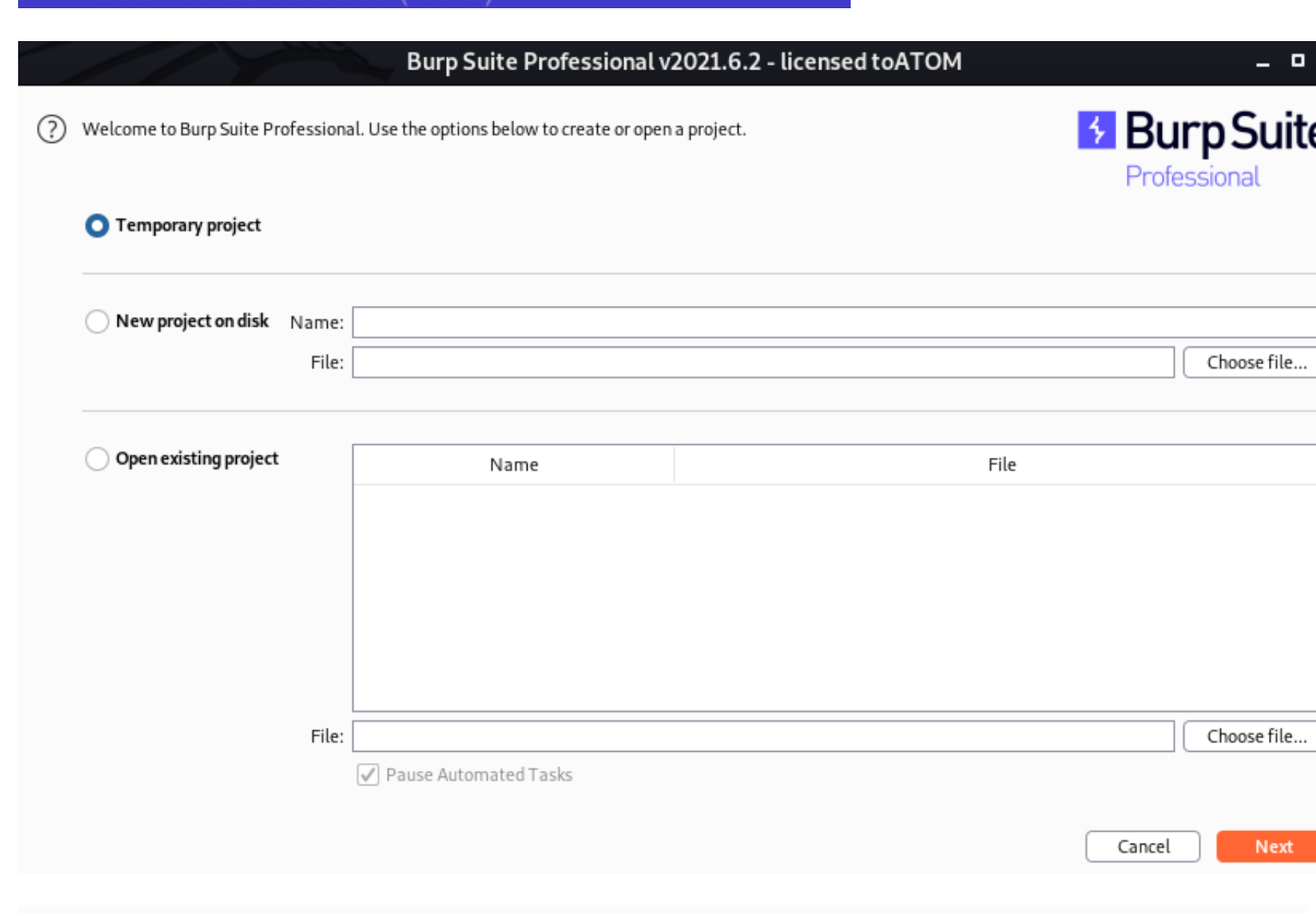
      vi. **whatweb**
         a)

      vii. **BURPSUITE-**

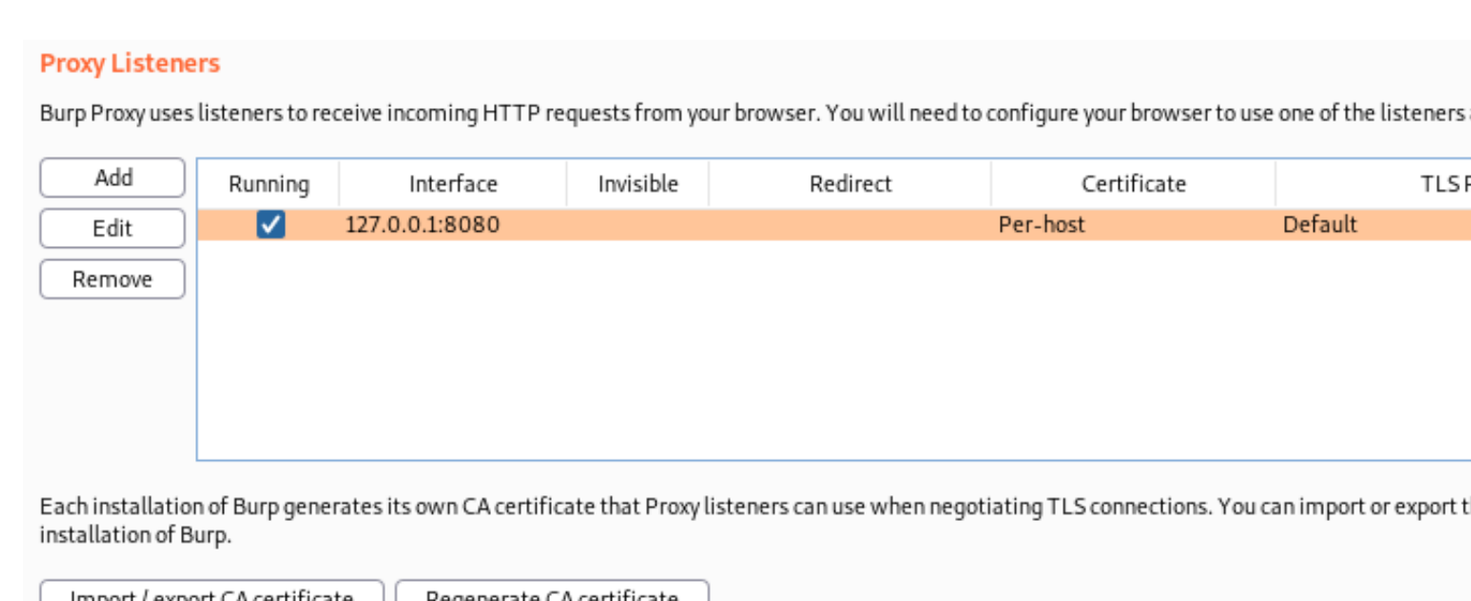
Burp Suite Professional

         a)

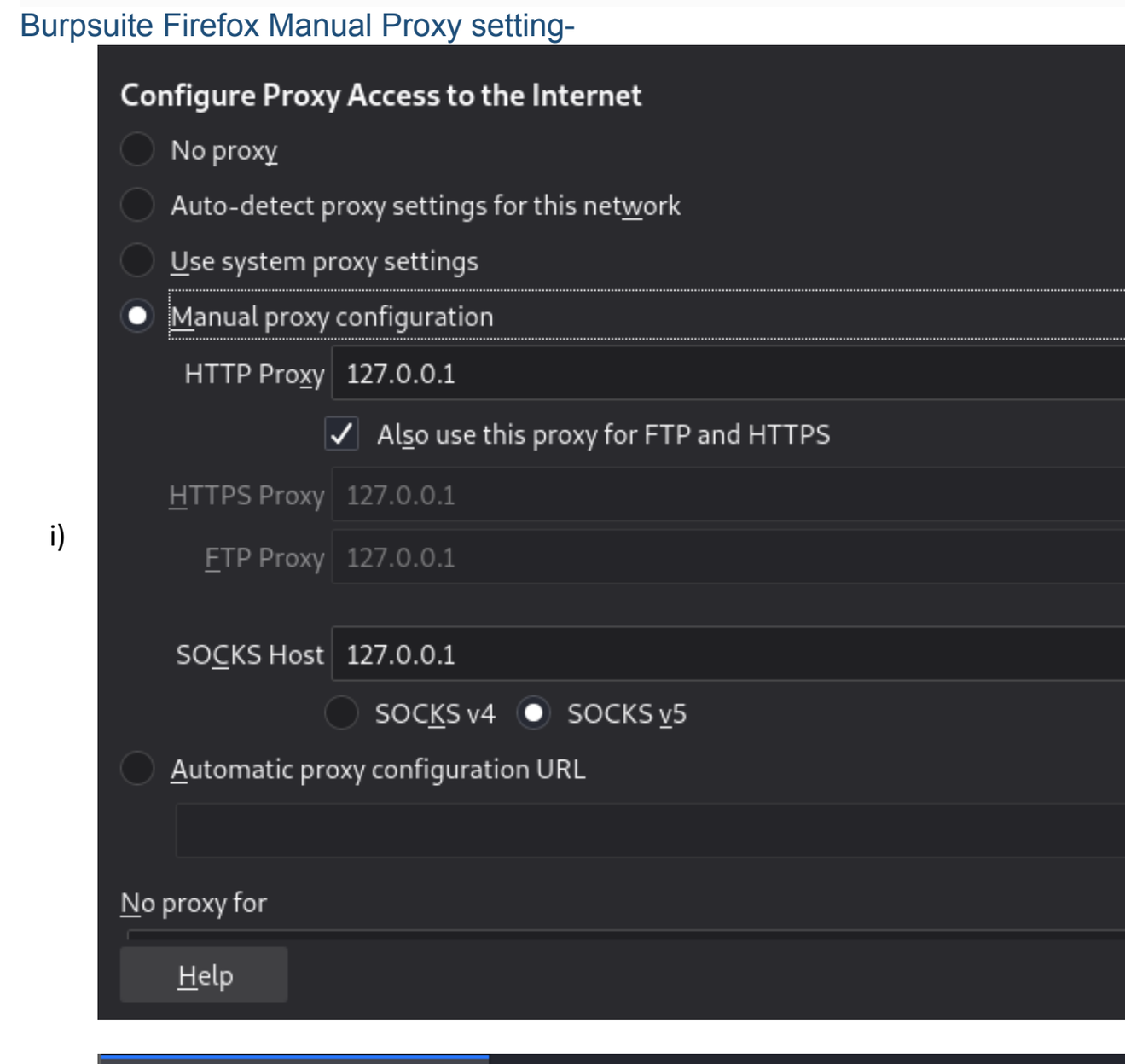
         b)



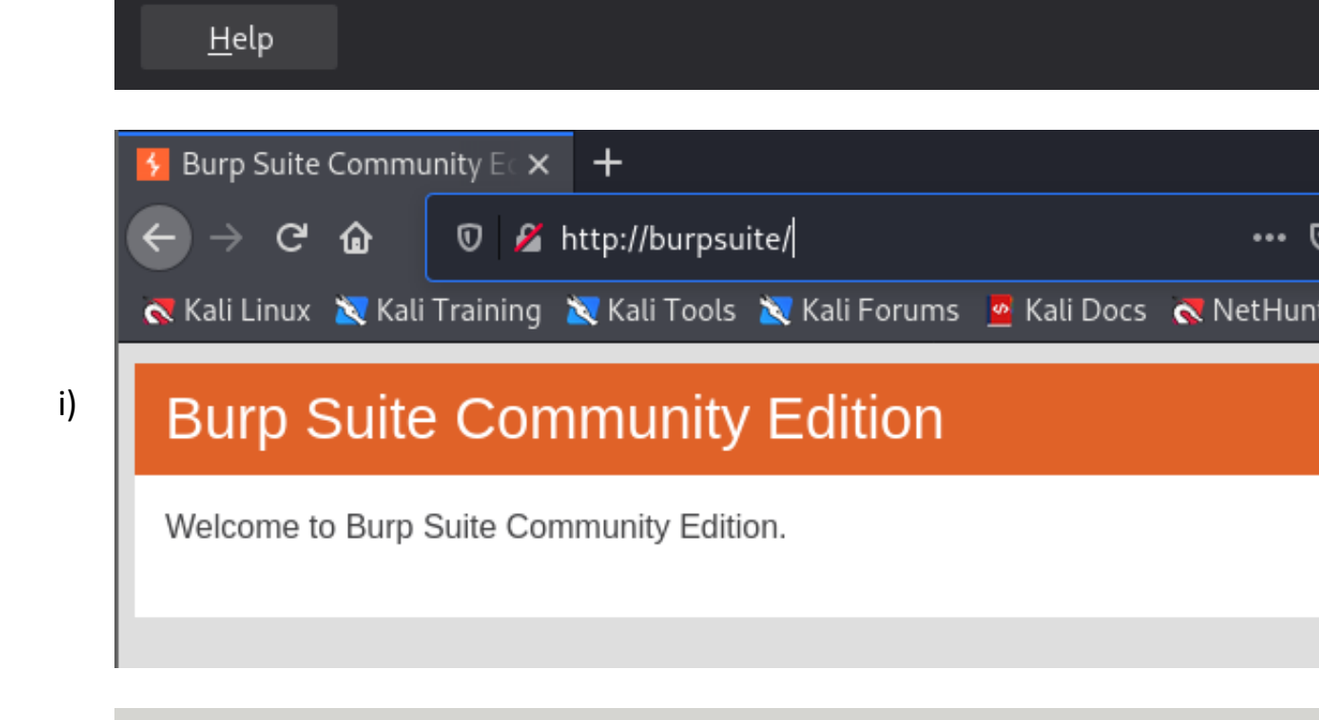
         c)



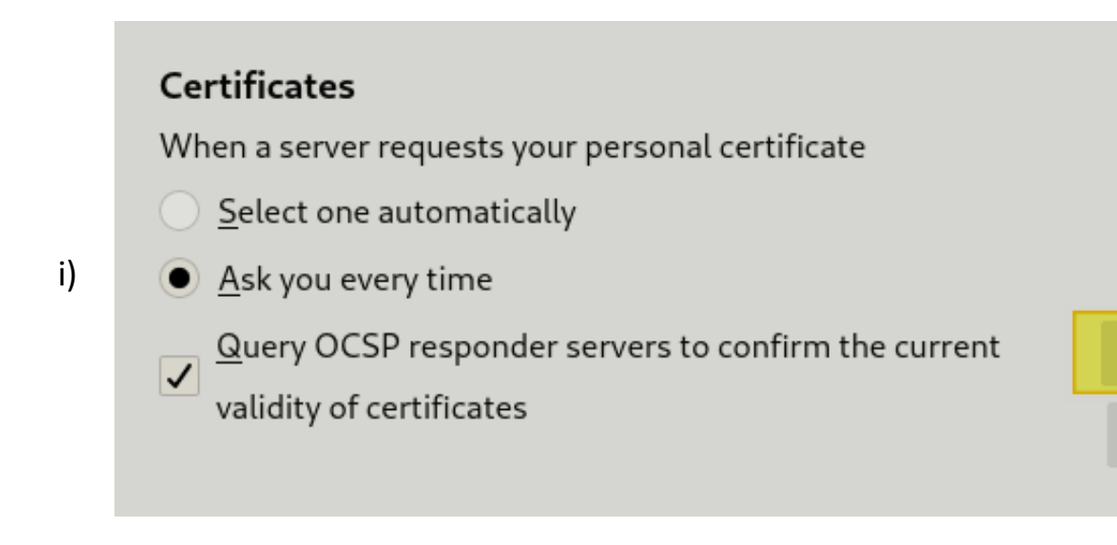
         d) Burpsuite Firefox Manual Proxy setting-
            i)



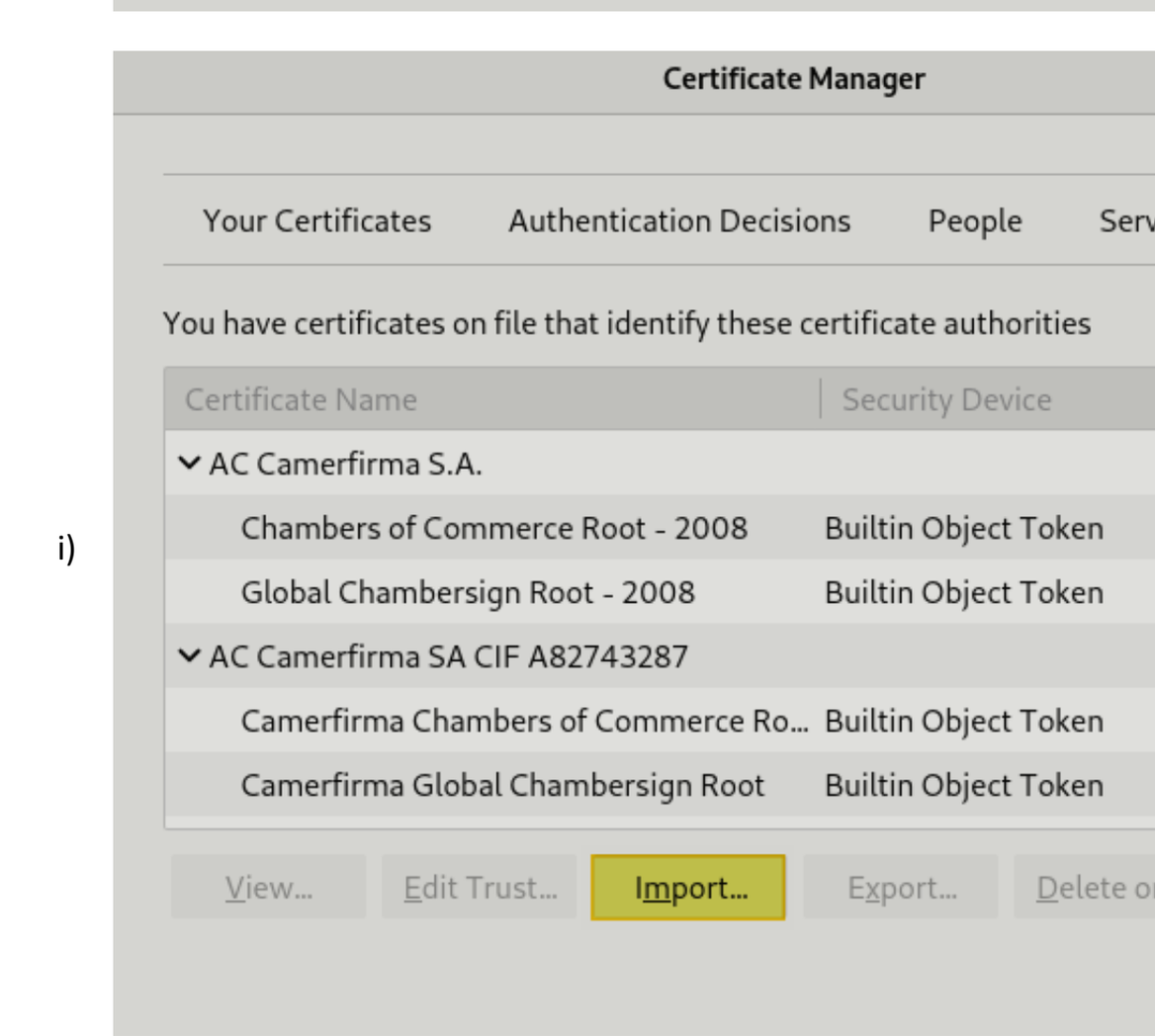
            i)



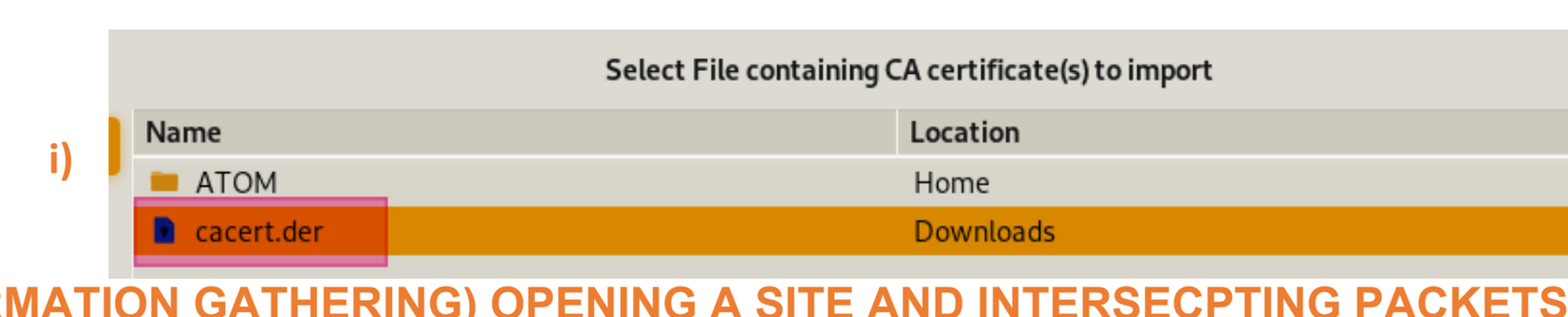
            i)



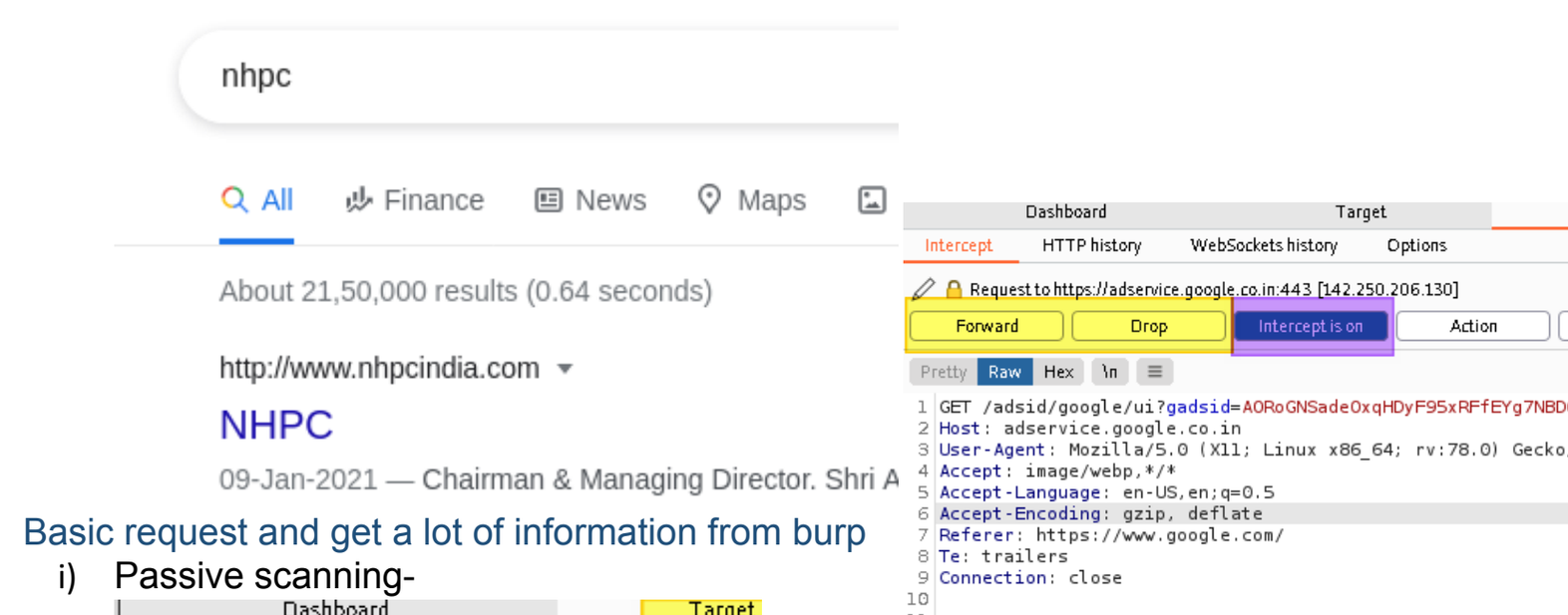
            i)



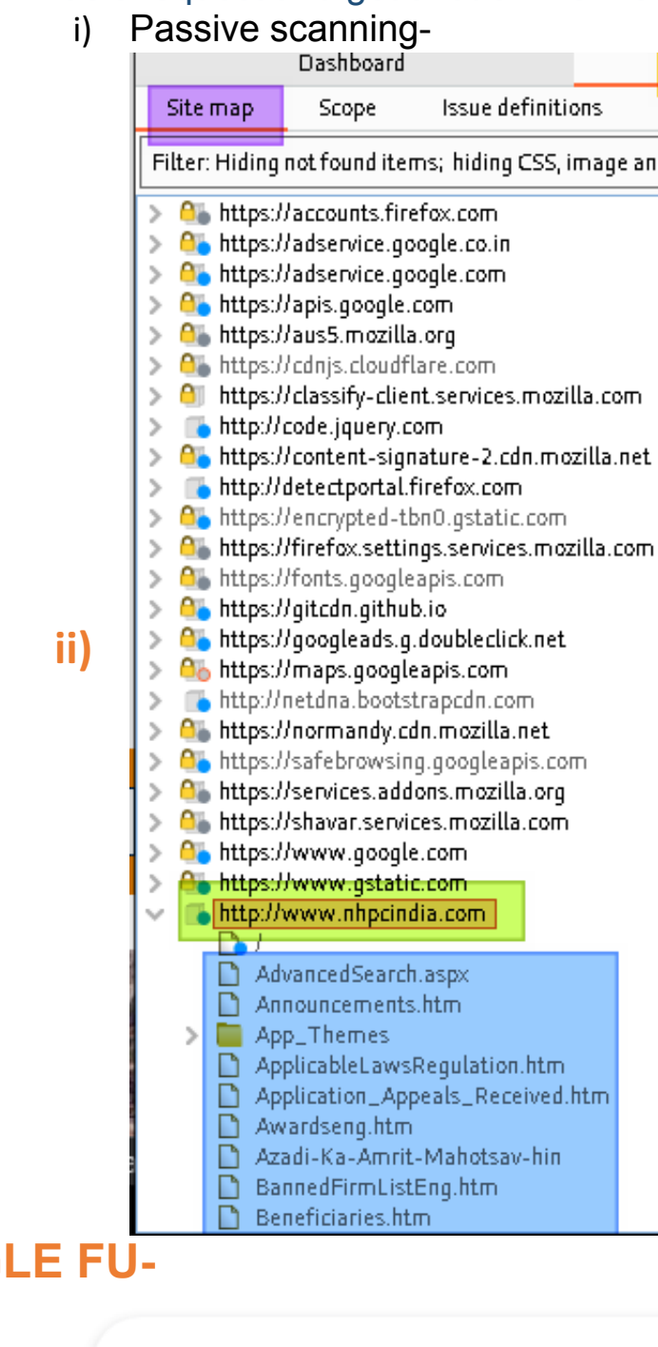
            i)



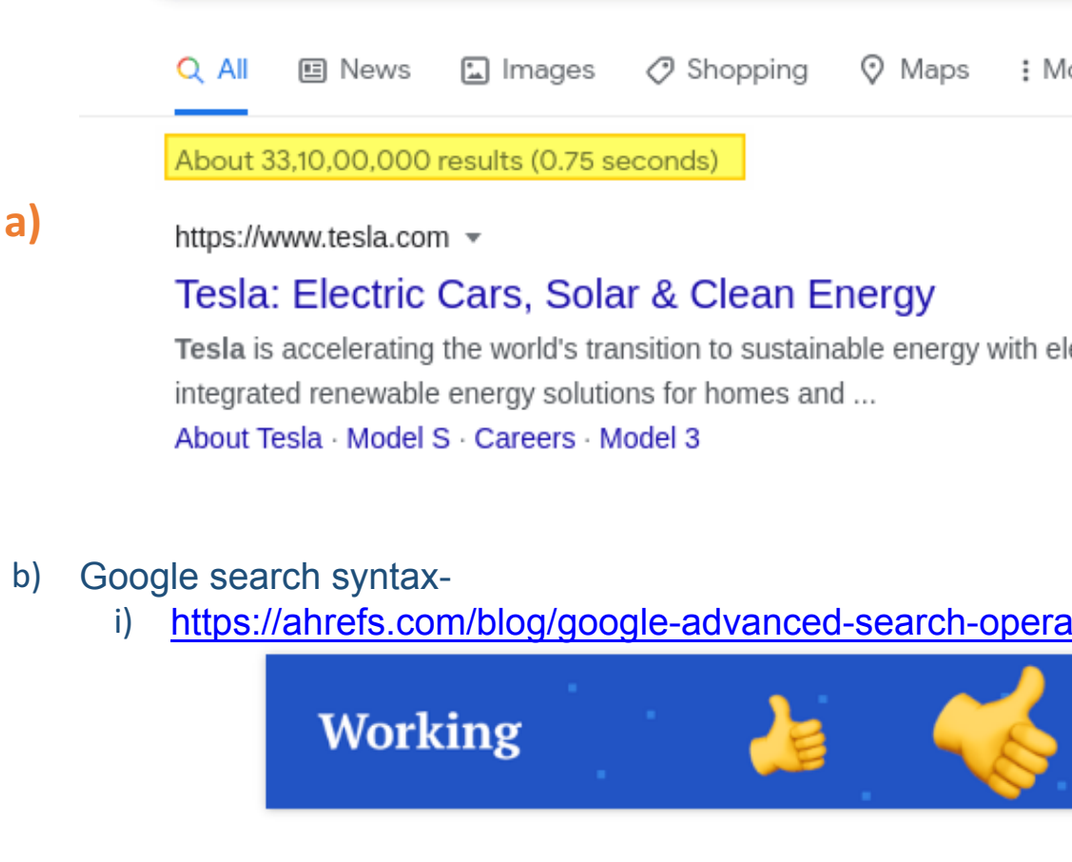
      viii. **(INFORMATION GATHERING) OPENING A SITE AND INTERSECPTING PACKETS-**



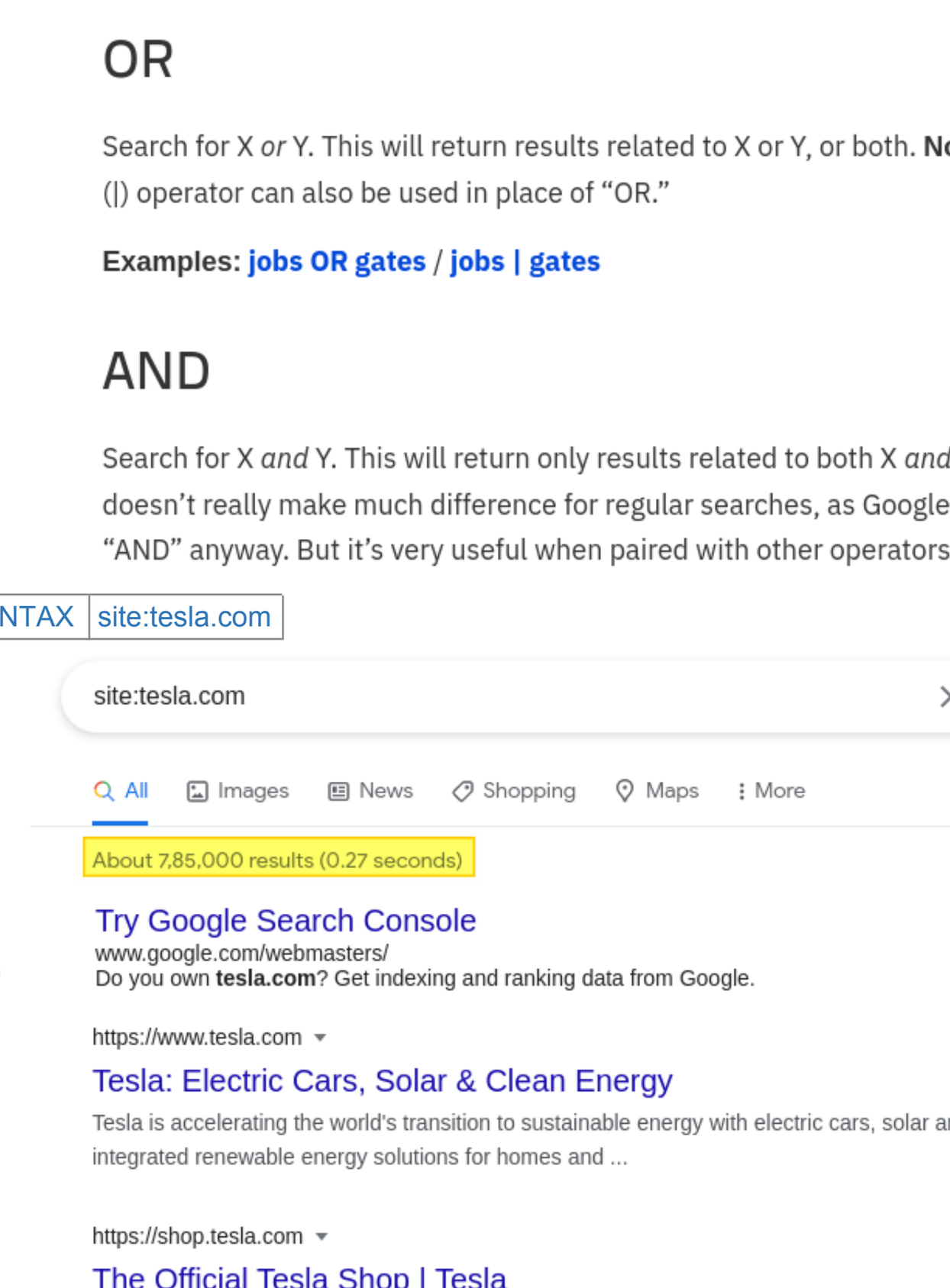
         a) Basic request and get a lot of information from burp
            i) Passive scanning-
            ii)



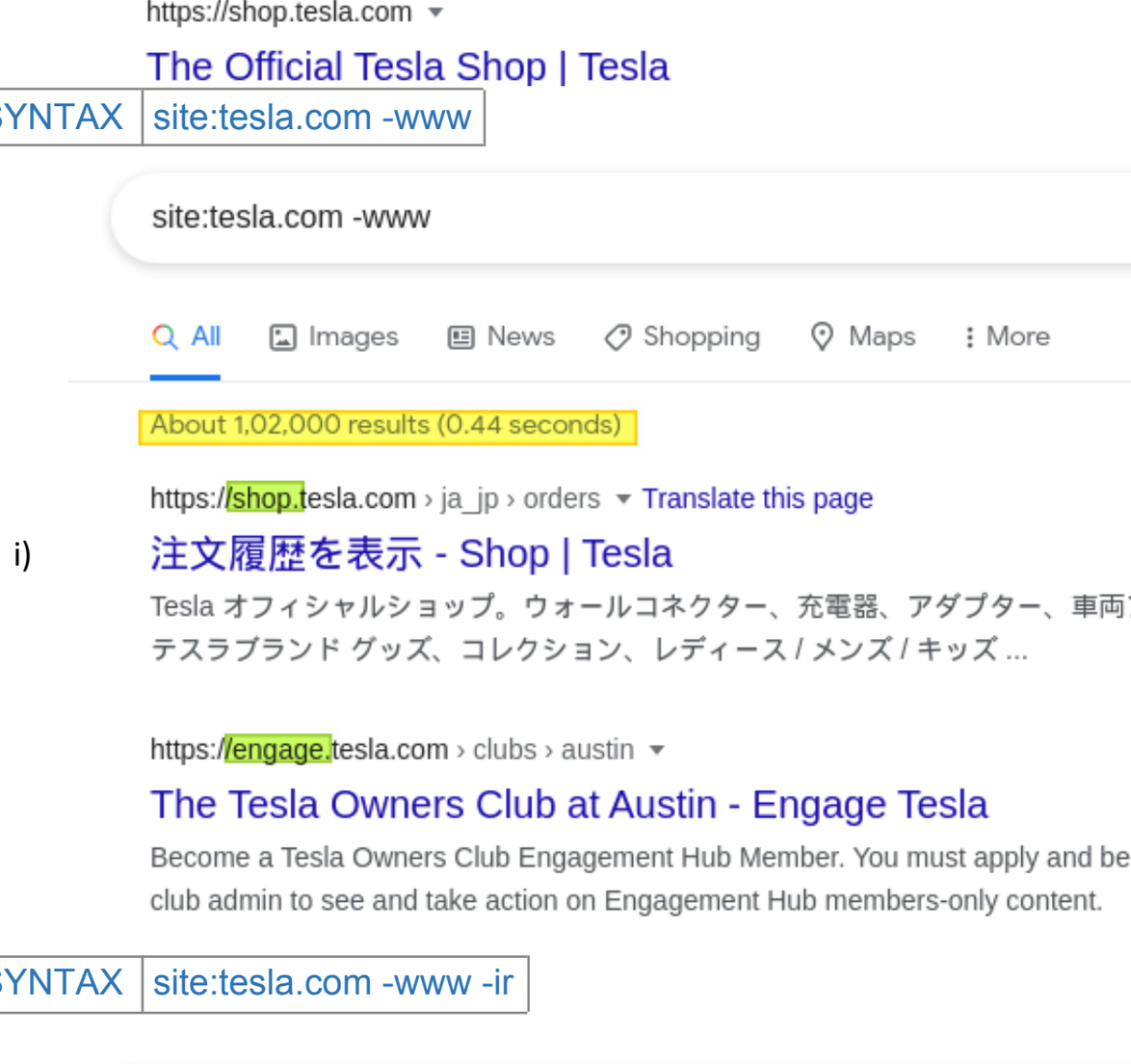
      ix. **GOOGLE FU-**
         a)



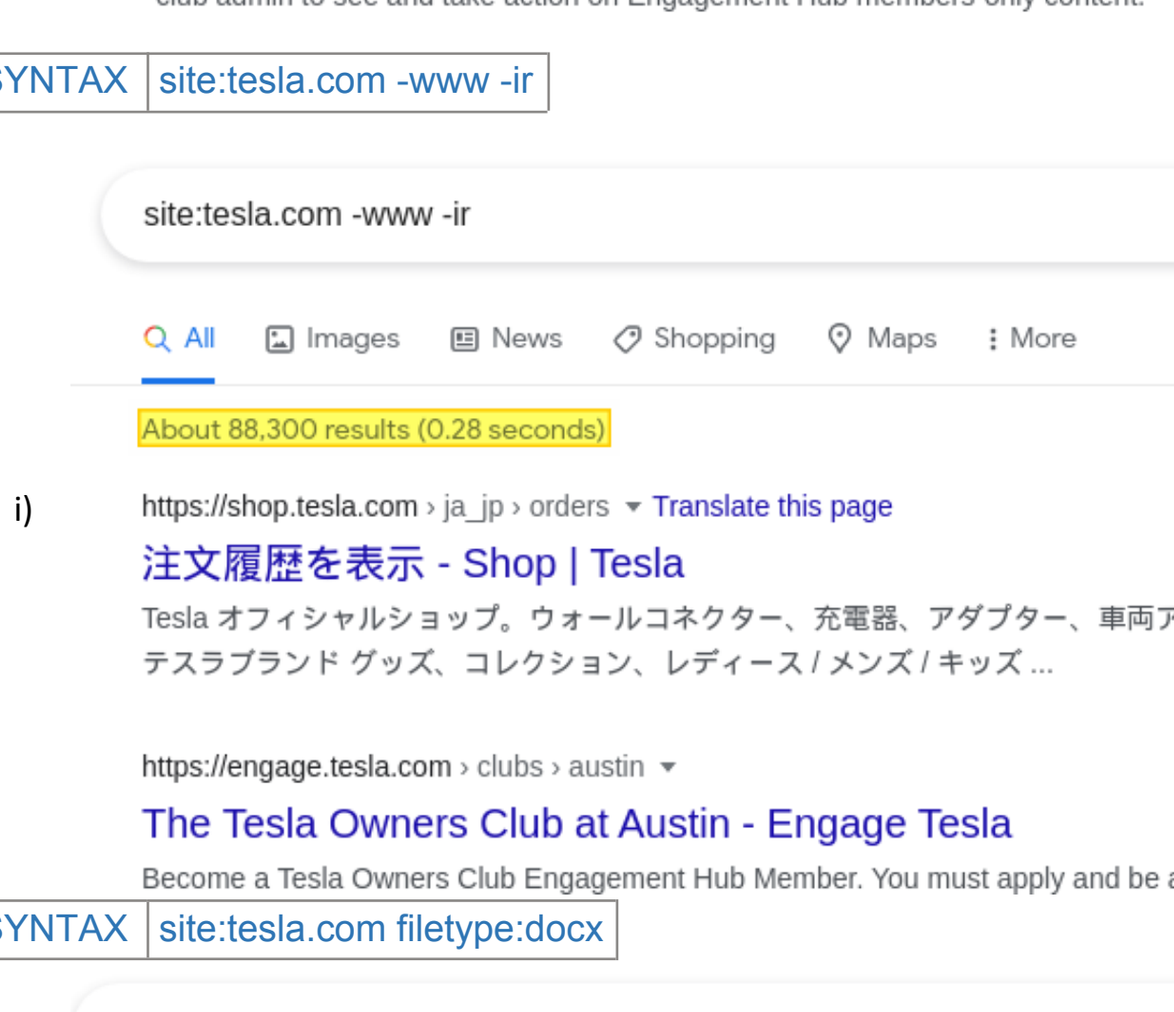
         b) Google search syntax-
            i) https://ahrefs.com/blog/google-advanced-search-operators/



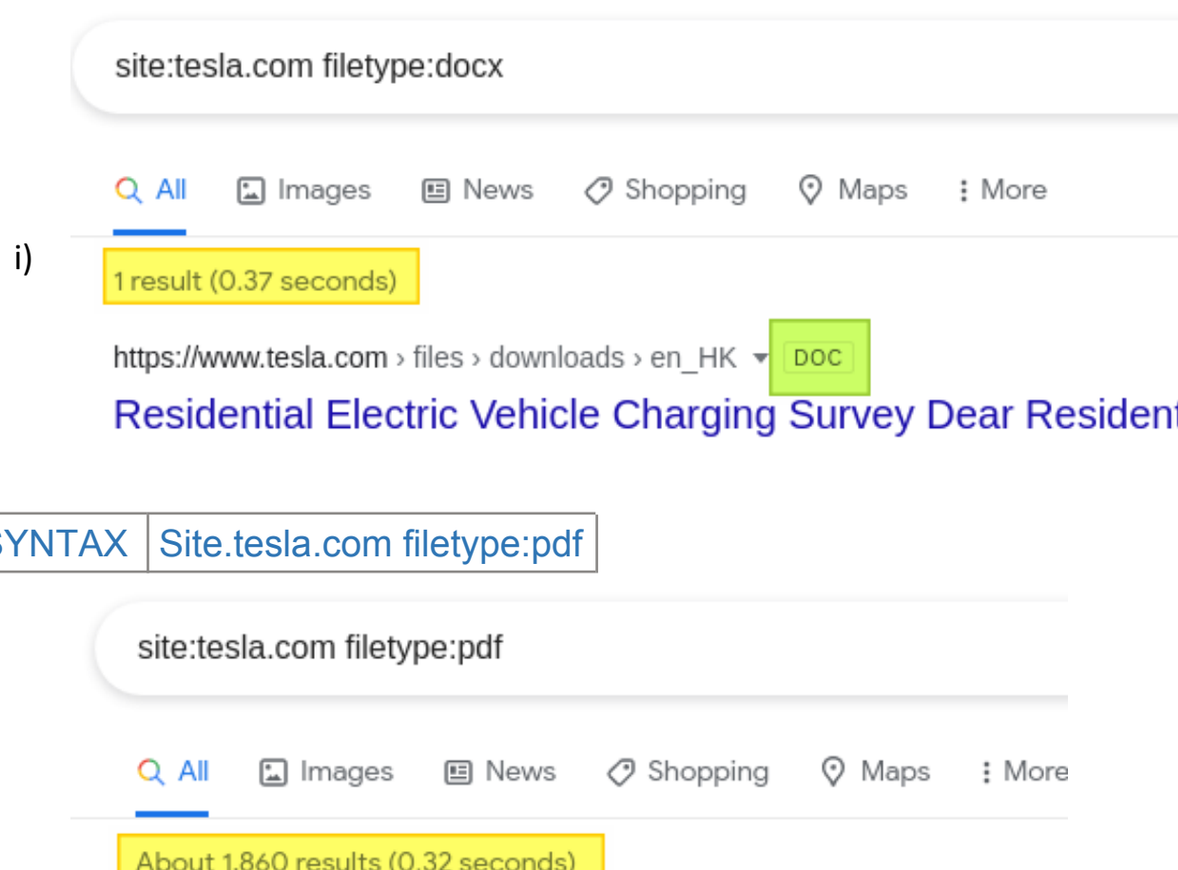
         c) SYNTAX site:tesla.com
            i)



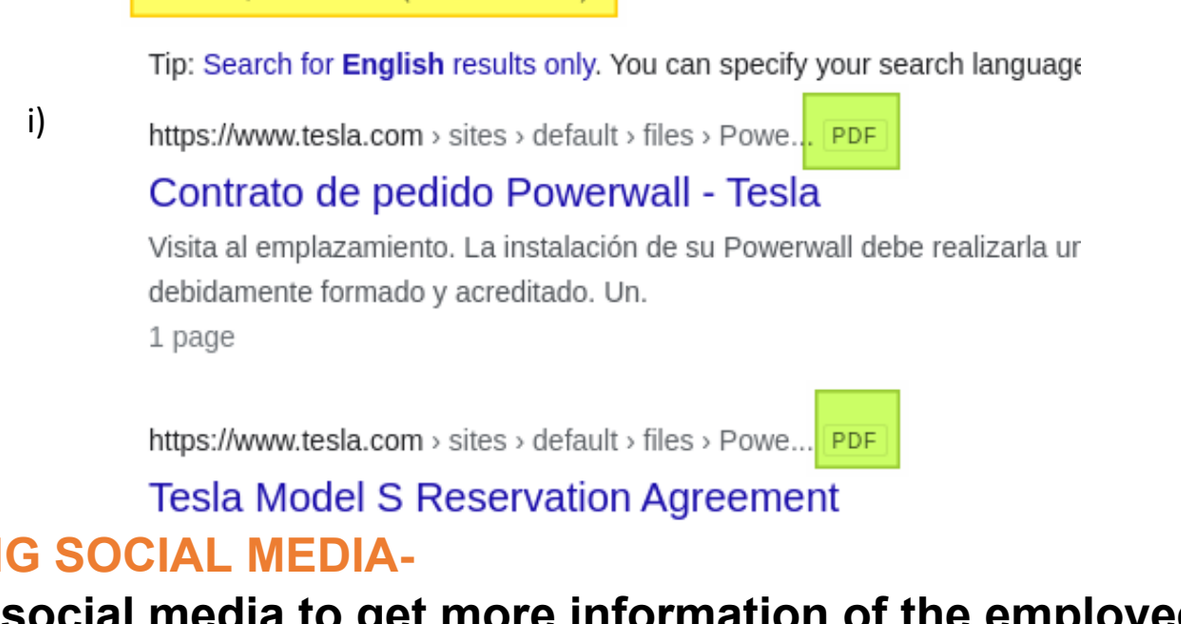
         d) SYNTAX site:tesla.com -www
            i)



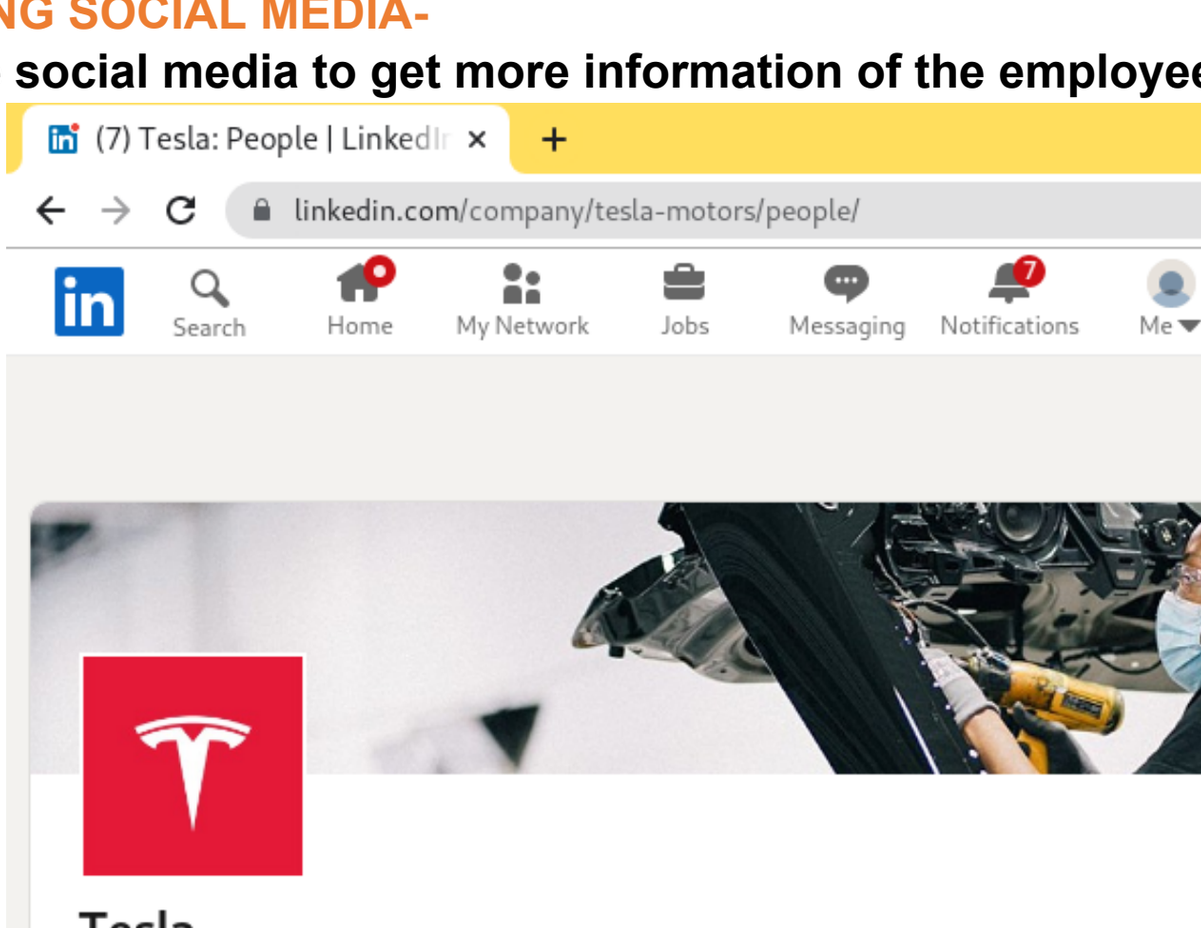
         e) SYNTAX site:tesla.com -www -ir
            i)



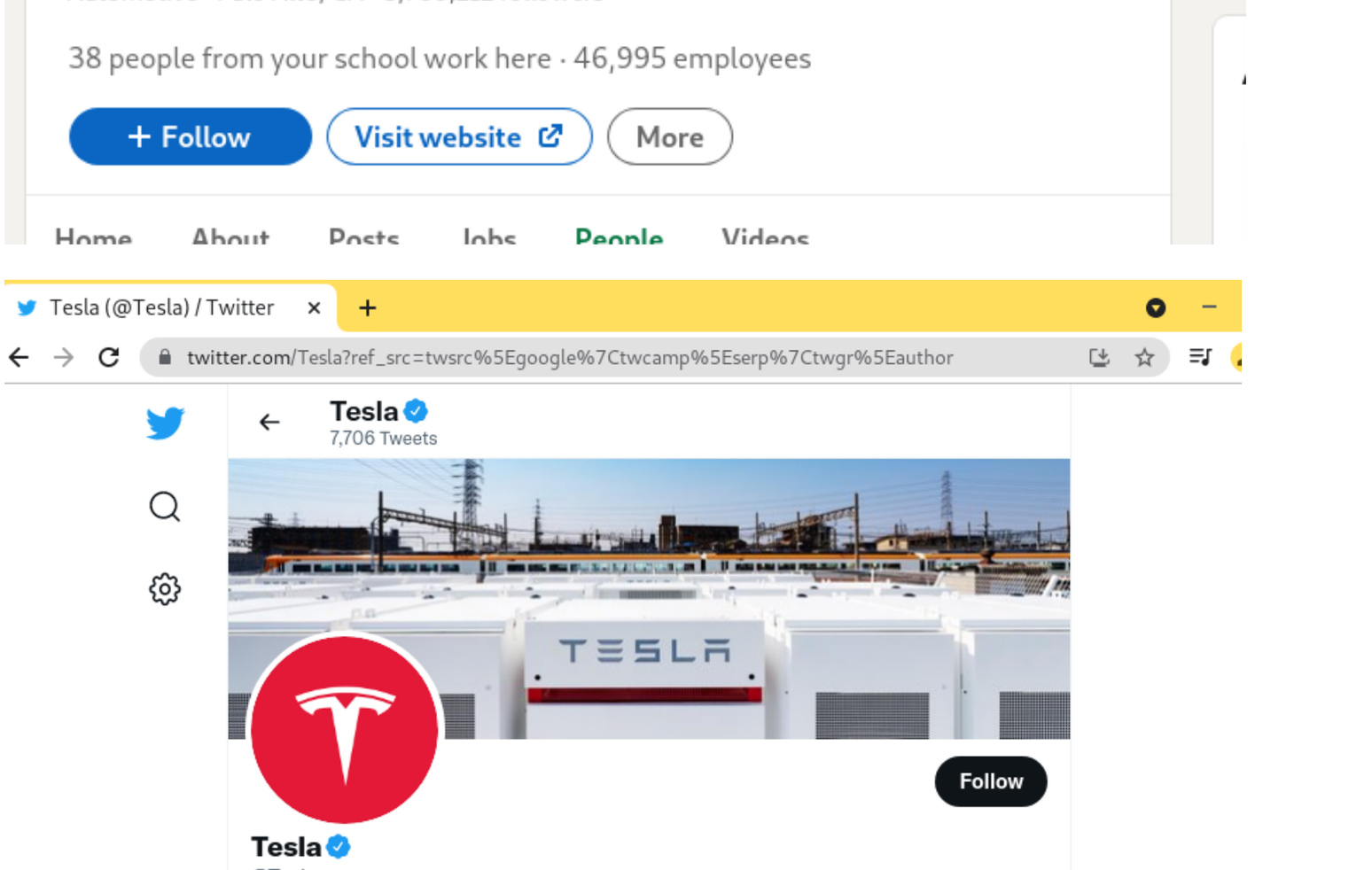
         f) SYNTAX site:tesla.com filetype:docx
            i)



         g) SYNTAX Site.tesla.com filetype:pdf
            i)



      x. **UTILIZING SOCIAL MEDIA-**
         1) **Use social media to get more information of the employees , network computer through image and videos**
            a)



            b)