Lab 5: Gathering Target Information - Footprinting and Social Engineering

Part 1: Explore Google Hacking:

"Google hacking" refers to the practice of using Google or other search engines' advanced functionalities to better gather information about a target organization. We demonstrate this on The New York Times using various different google filters.

Figure 1: Normal Google Search For "New York Times"

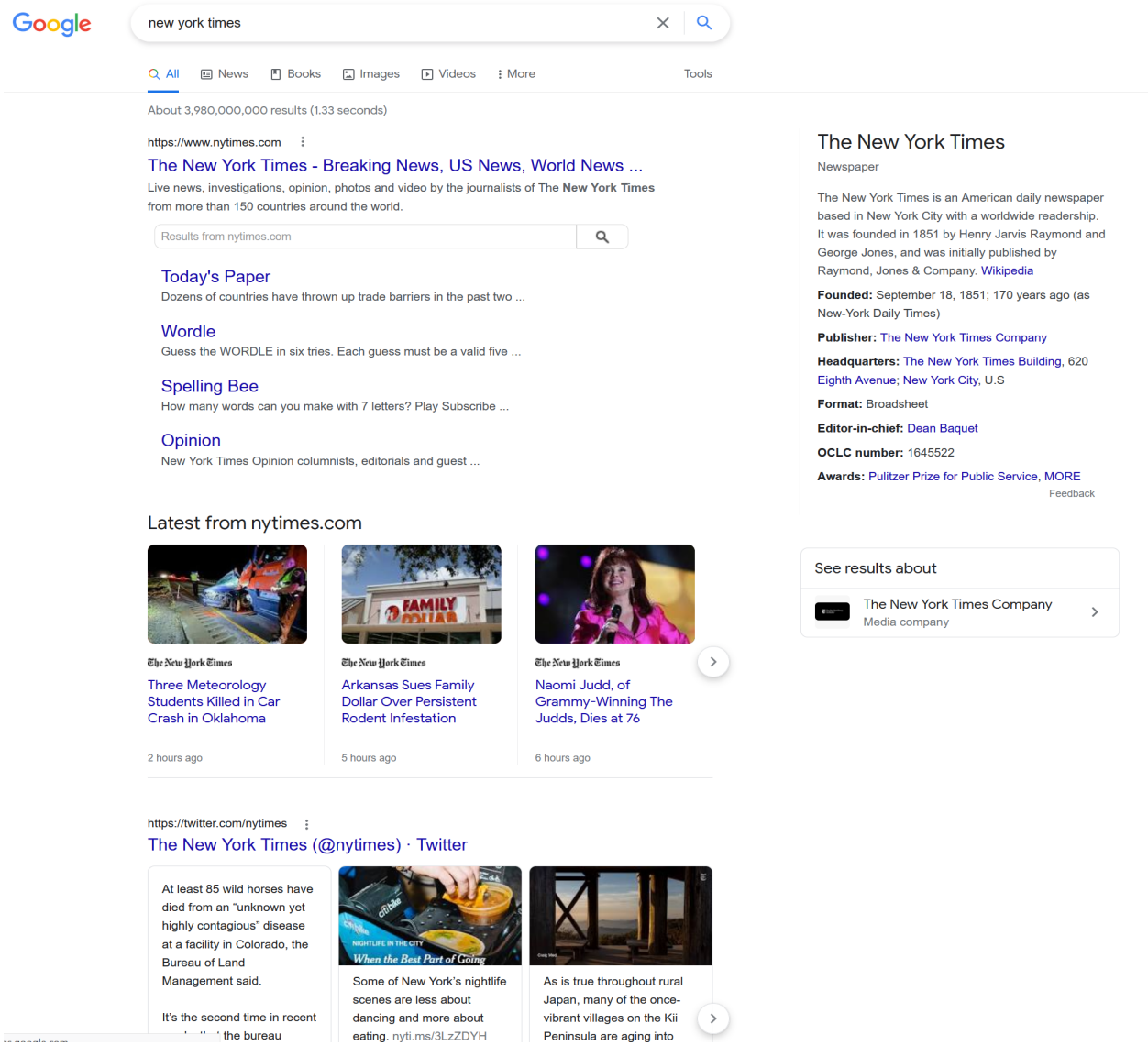


Figure 2: Applying The site: Filter

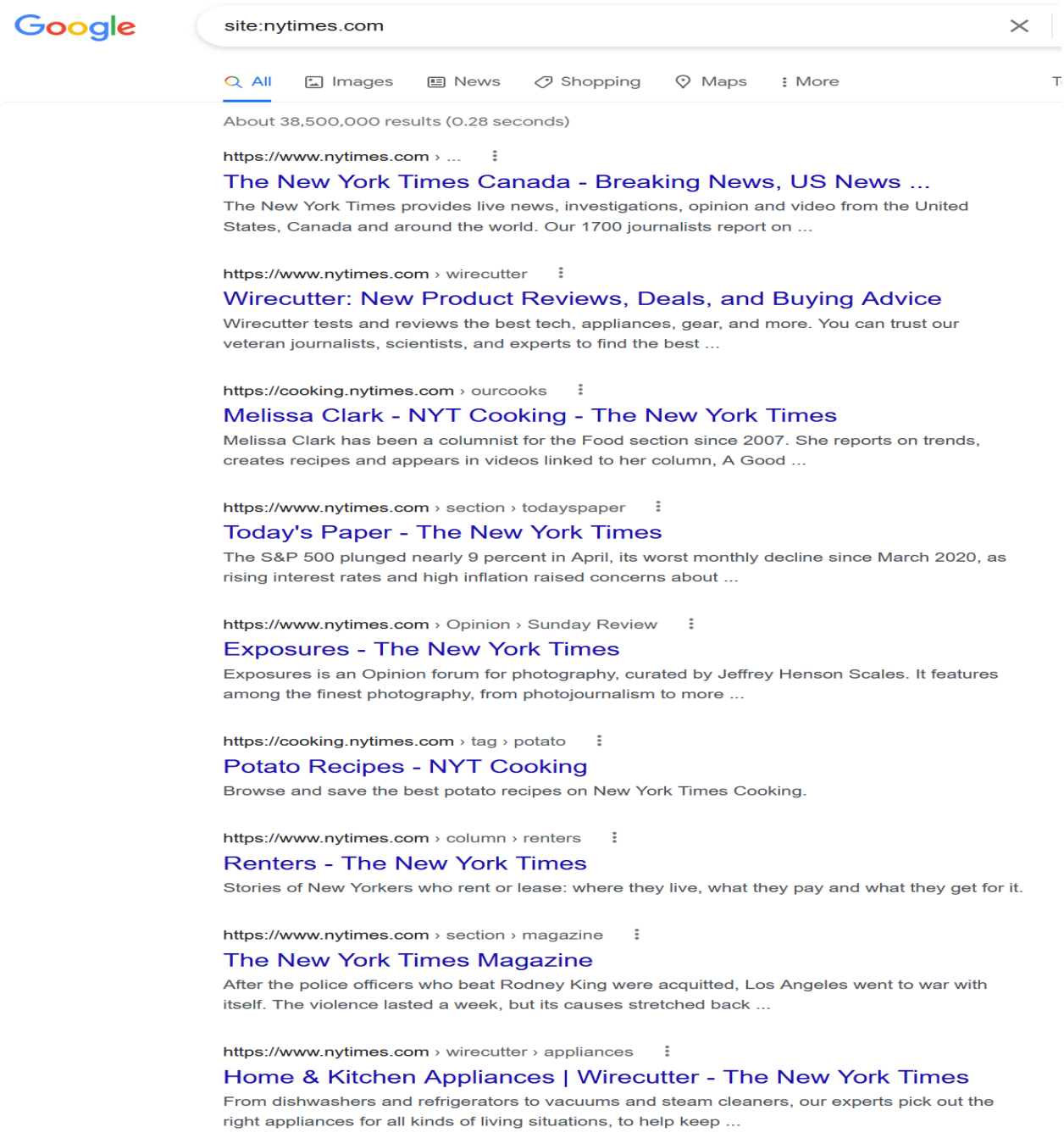


Figure 3: Applying The inurl: Filter

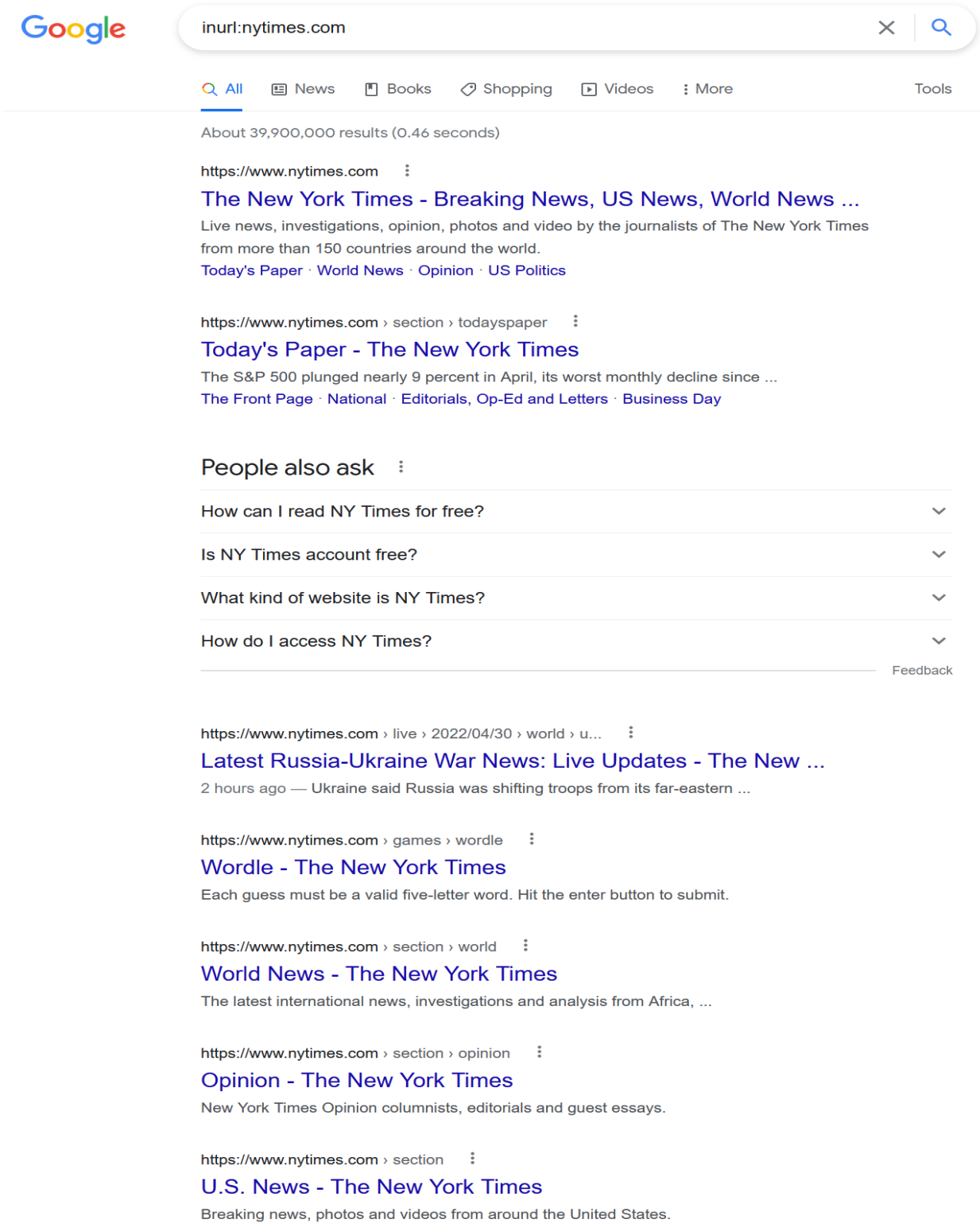


Figure 4: Applying The link: Filter

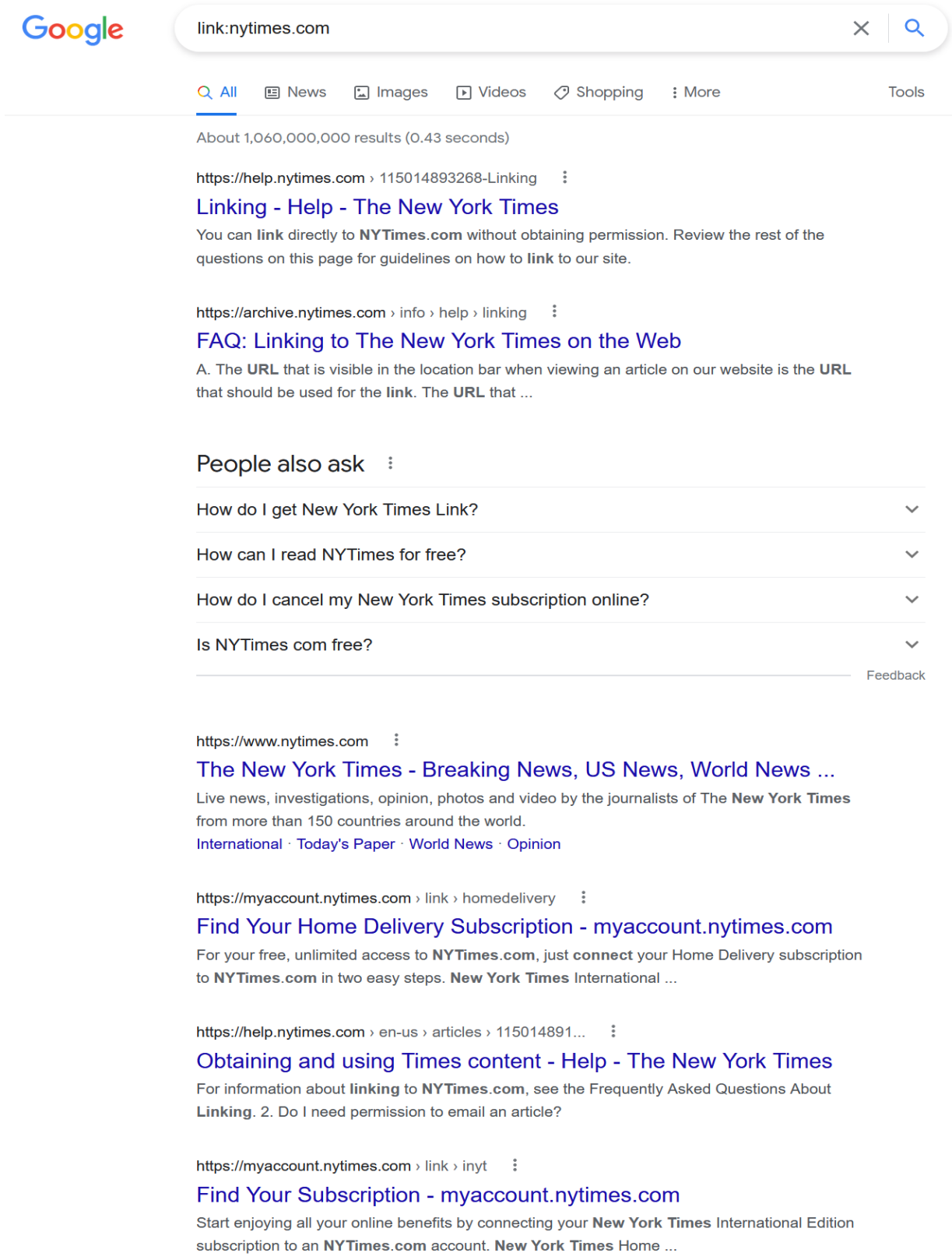


Figure 5: Applying The related: Filter

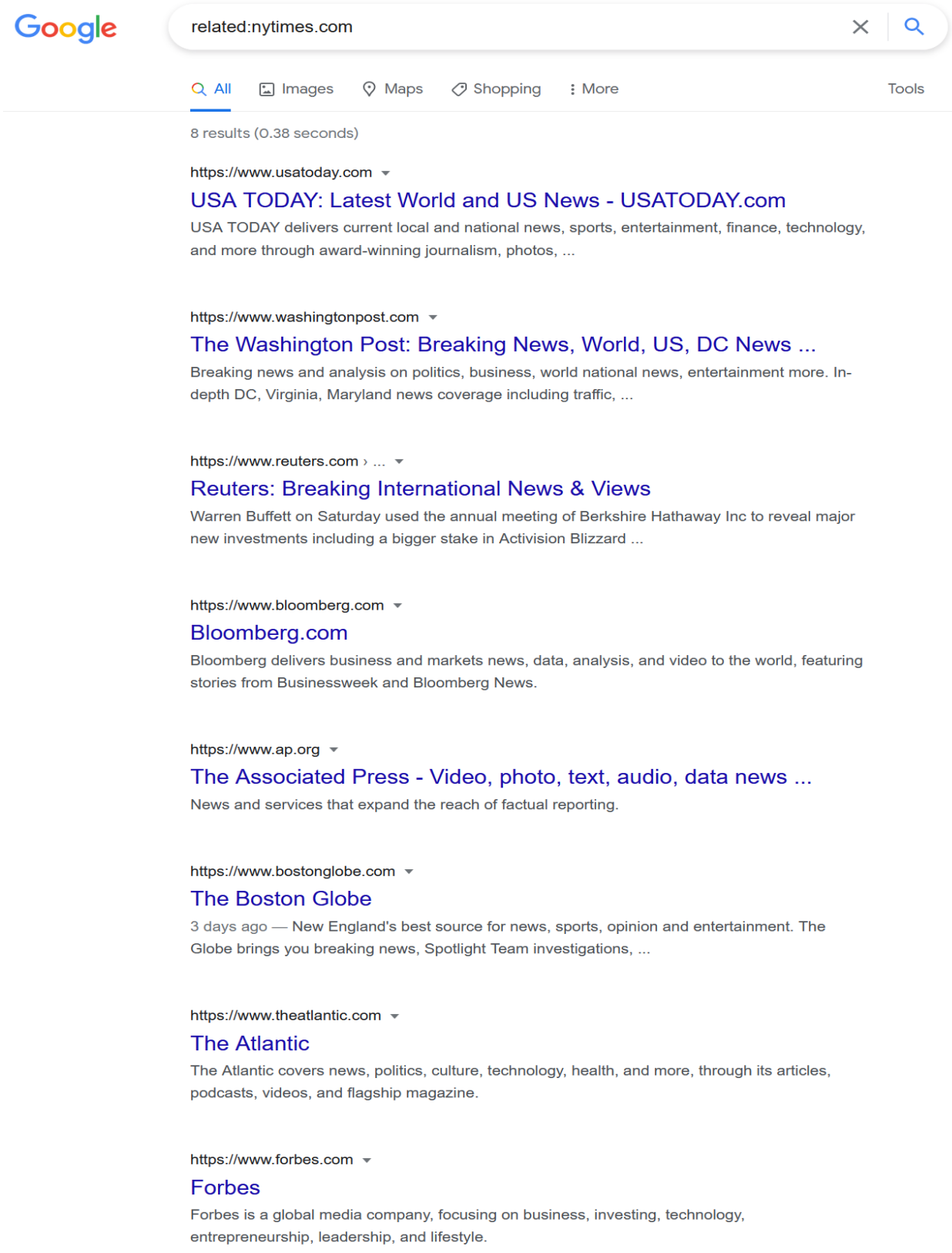
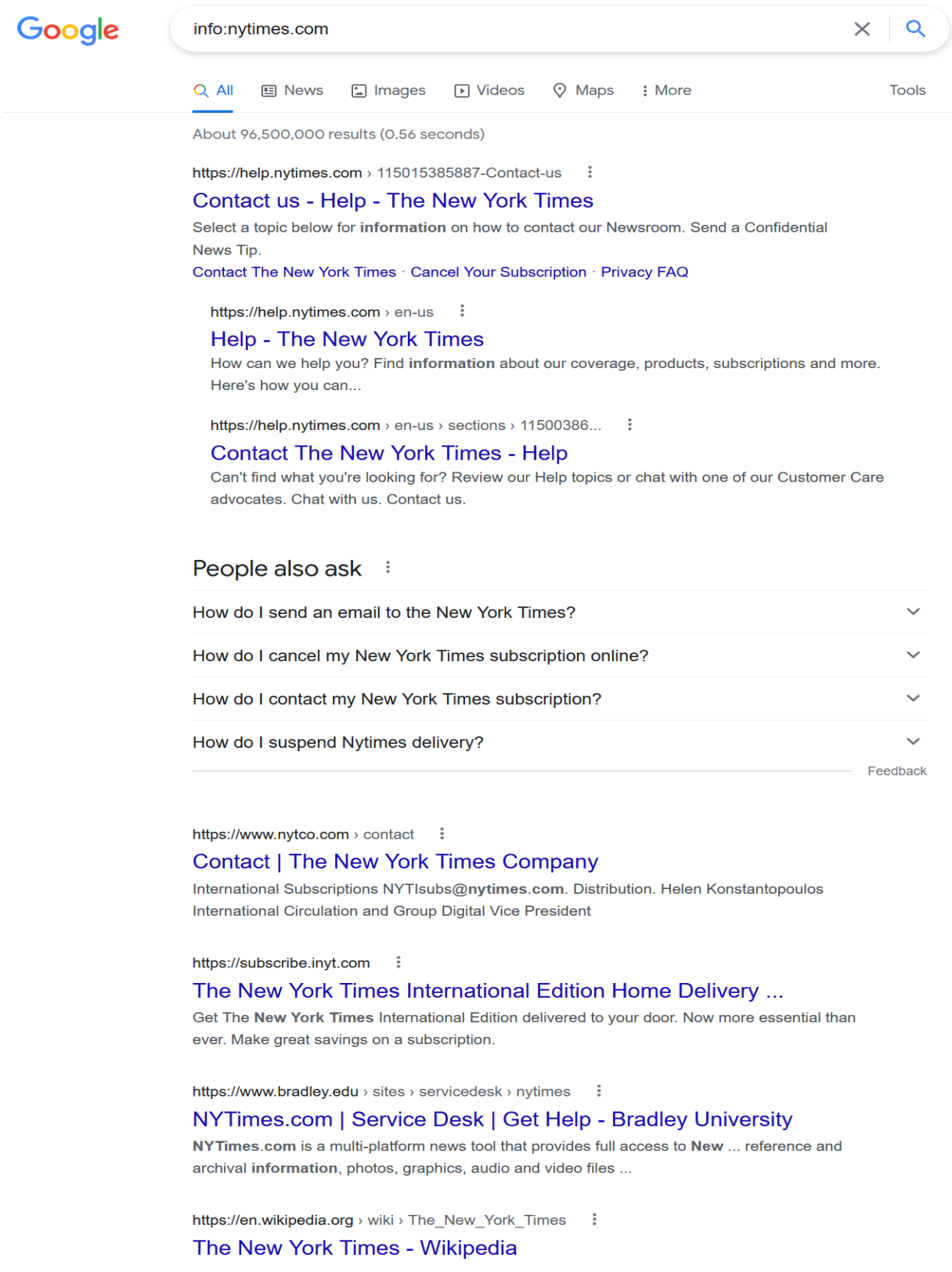


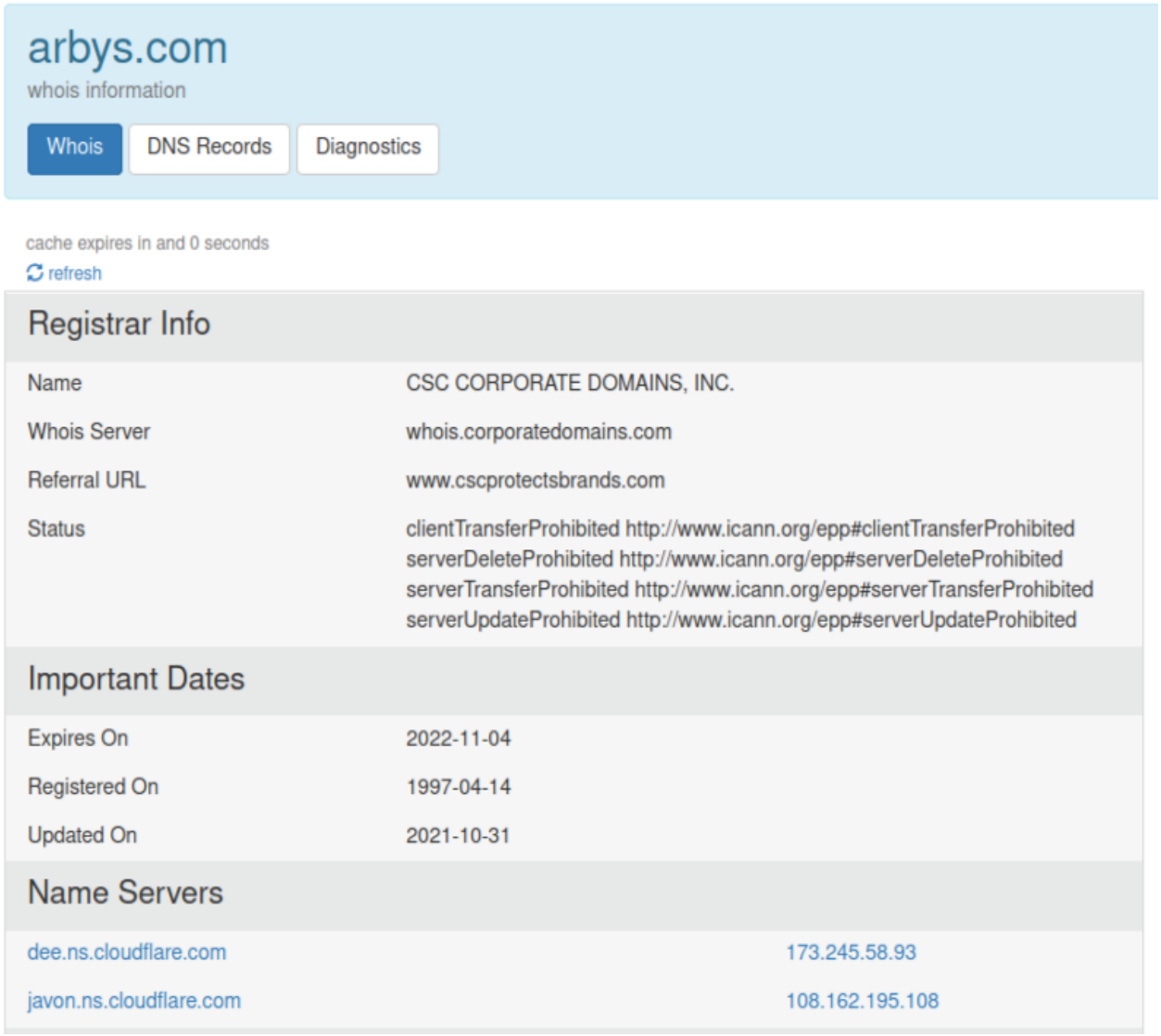
Figure 6: Applying The info: Filter



Part 2: Explore the WHOIS Database:

The WHOIS database is another valuable resource for organizational footprinting and reconnaissance operations. It acts as a basic DNS lookup service that an attacker can use to gather the IP addresses of the organization they wish to attack or defend. The screenshots below show the results of using the WHOIS database to look up our target organization Arbys.

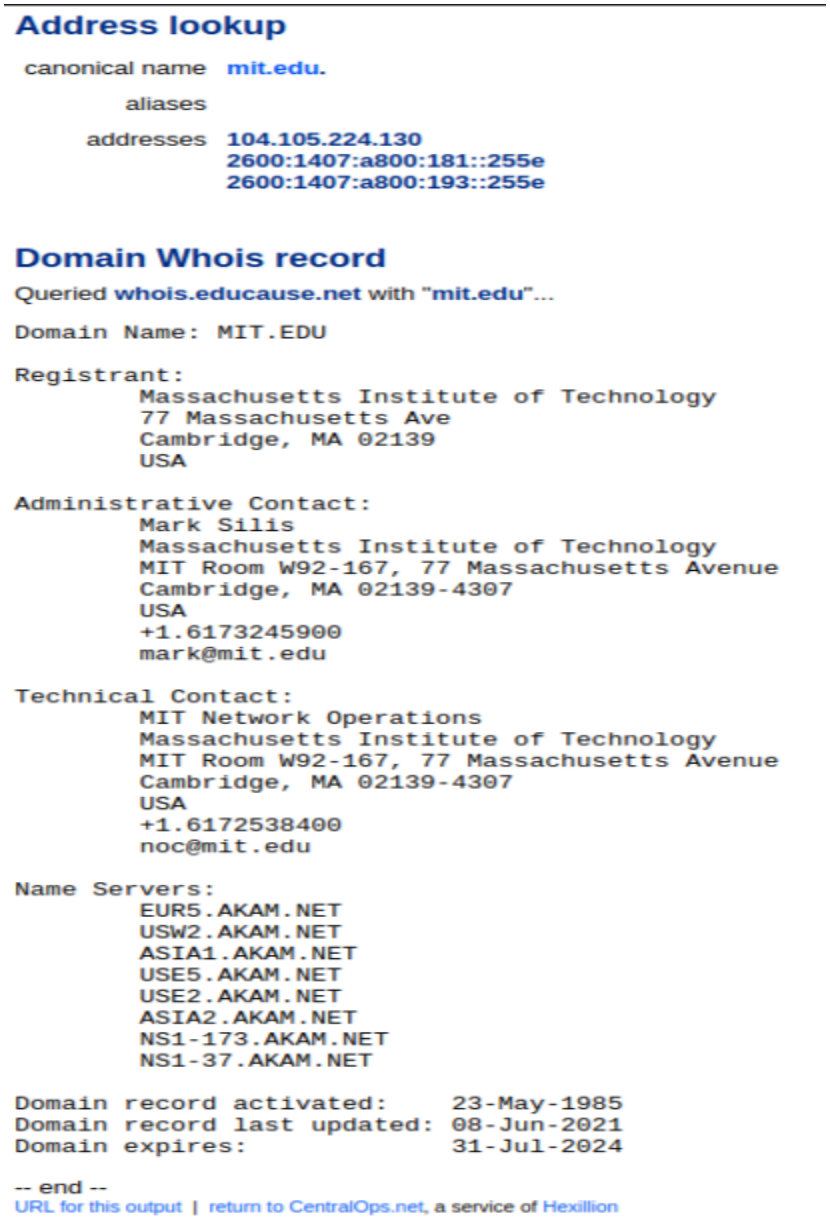
Figure 7: WHOIS Arbys



Part 4: Using Domain Dossier WHOIS Function

CentralOps is an alternative to the WHOIS lookup done in the Kali VM. The information displayed by centralops is generally much more verbose, as the figures below demonstrate.

Figure 8: Domain Dossier of MIT:



Address lookup

canonical name mit.edu.
aliases
addresses 104.105.224.130
2600:1407:a800:181::255e
2600:1407:a800:193::255e

Domain Whois record

Queried whois.educause.net with "mit.edu"...

```
Domain Name: MIT.EDU

Registrant:
        Massachusetts Institute of Technology
        77 Massachusetts Ave
        Cambridge, MA 02139
        USA

Administrative Contact:
        Mark Silis
        Massachusetts Institute of Technology
        MIT Room W92-167, 77 Massachusetts Avenue
        Cambridge, MA 02139-4307
        USA
        +1.6173245900
        mark@mit.edu

Technical Contact:
        MIT Network Operations
        Massachusetts Institute of Technology
        MIT Room W92-167, 77 Massachusetts Avenue
        Cambridge, MA 02139-4307
        USA
        +1.6172538400
        noc@mit.edu

Name Servers:
        EUR5.AKAM.NET
        USW2.AKAM.NET
        ASIA1.AKAM.NET
        USE5.AKAM.NET
        USE2.AKAM.NET
        ASIA2.AKAM.NET
        NS1-173.AKAM.NET
        NS1-37.AKAM.NET

Domain record activated:    23-May-1985
Domain record last updated: 08-Jun-2021
Domain expires:             31-Jul-2024
```

-- end --
URL for this output | return to CentralOps.net, a service of Hexillion

Figure 9: Domain Dossier of Arbys

Address lookup

canonical name www.arbys.com.

aliases

addresses 104.18.33.167
172.64.154.89
2606:4700:4400::6812:21a7
2606:4700:4400::ac40:9a59

Domain Whois record

Queried whois.internic.net with "dom Arbys.com"...

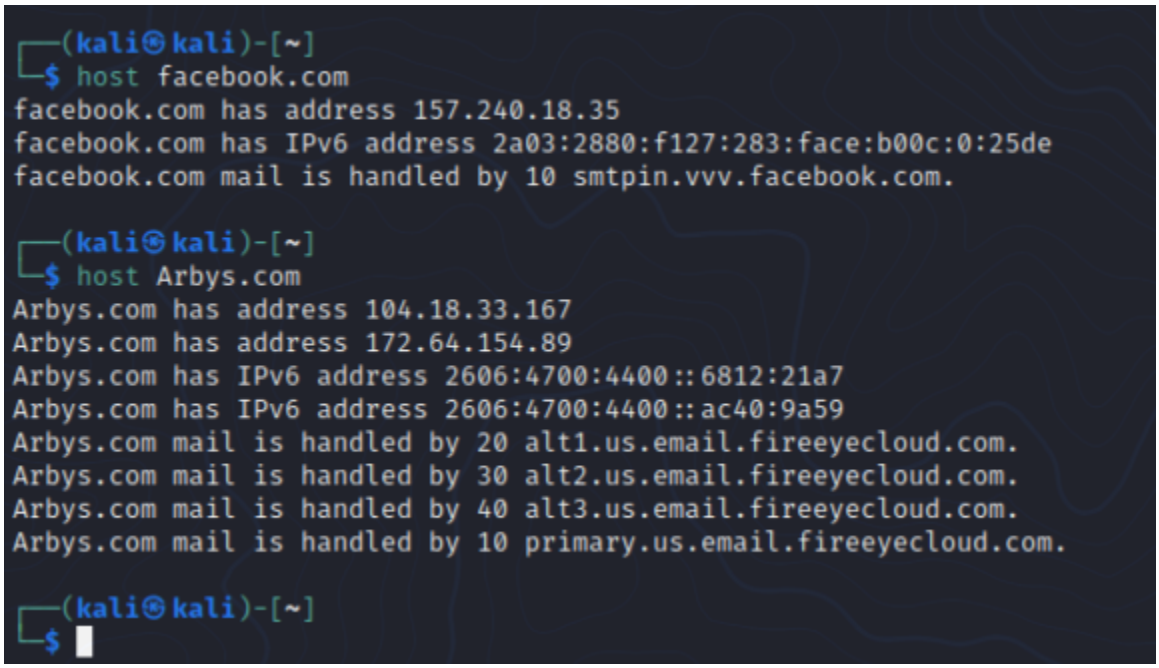
```
   Domain Name: ARBYS.COM
   Registry Domain ID: 3167276_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.corporatedomains.com
   Registrar URL: http://cscdbs.com
   Updated Date: 2021-10-31T05:10:35Z
   Creation Date: 1997-04-14T04:00:00Z
   Registry Expiry Date: 2022-11-04T18:59:49Z
   Registrar: CSC Corporate Domains, Inc.
   Registrar IANA ID: 299
   Registrar Abuse Contact Email: domainabuse@cscglobal.com
   Registrar Abuse Contact Phone: 8887802723
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
   Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
   Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
   Name Server: DEE.NS.CLOUDFLARE.COM
   Name Server: JAVON.NS.CLOUDFLARE.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2022-05-01T05:18:19Z <<<
```

Queried whois.corporatedomains.com with "Arbys.com"...

Part 5: DNS Reconnaissance

The host utility built into our Kali VM can be used for dns lookup purposes, as shown in the screenshots below. Hackers can use the DNS footprint of organizations to determine what subdomains to attack/which subdomains of an organization are vulnerable to attack.

Figure 10: Using host For DNS Lookup



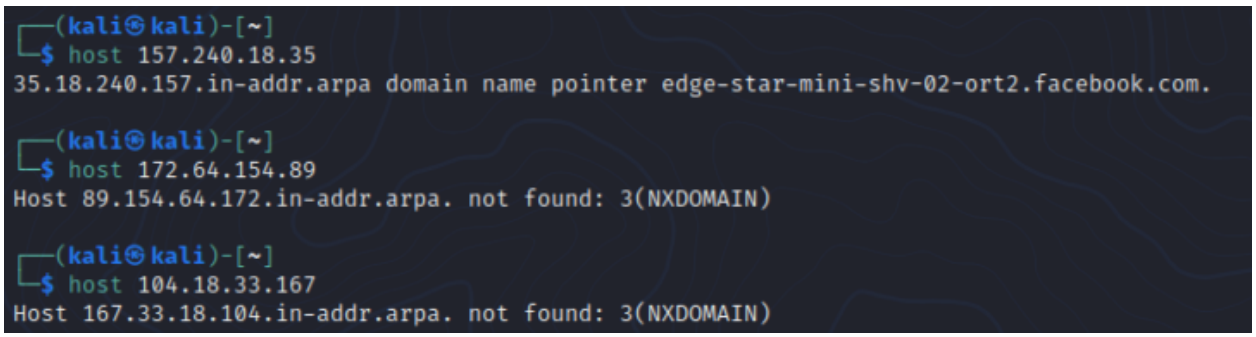
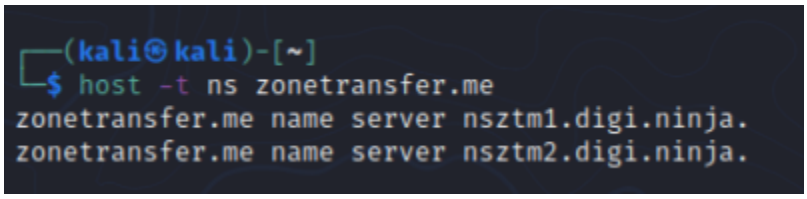
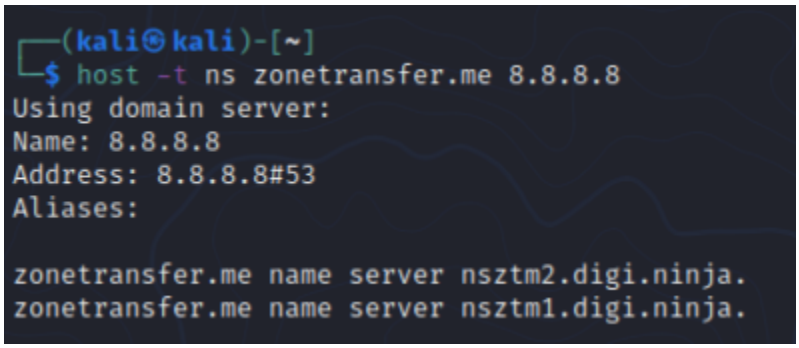


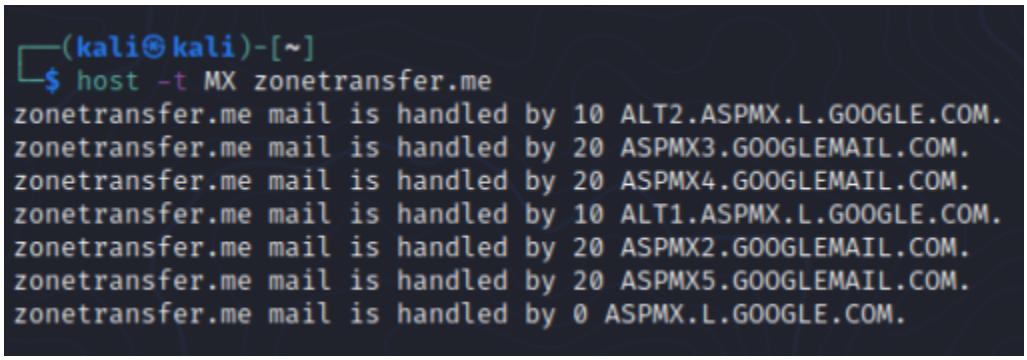
Figure 11: DNS servers for zonetransfer.me

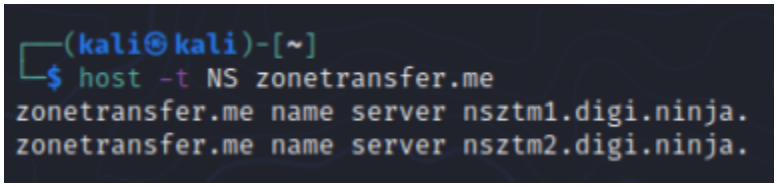


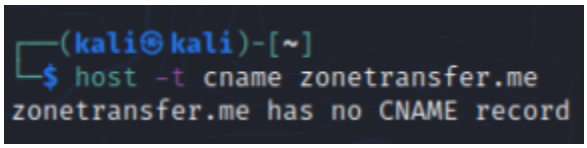


Using the default DNS server

Figure 12: Using host to view DNS records







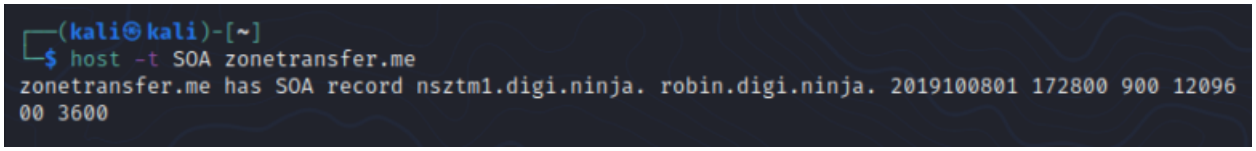
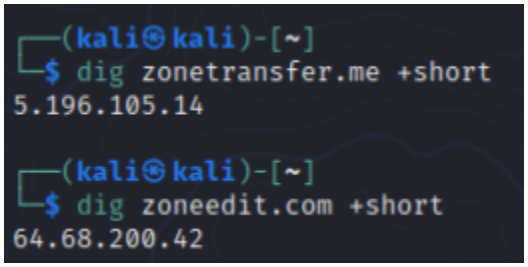
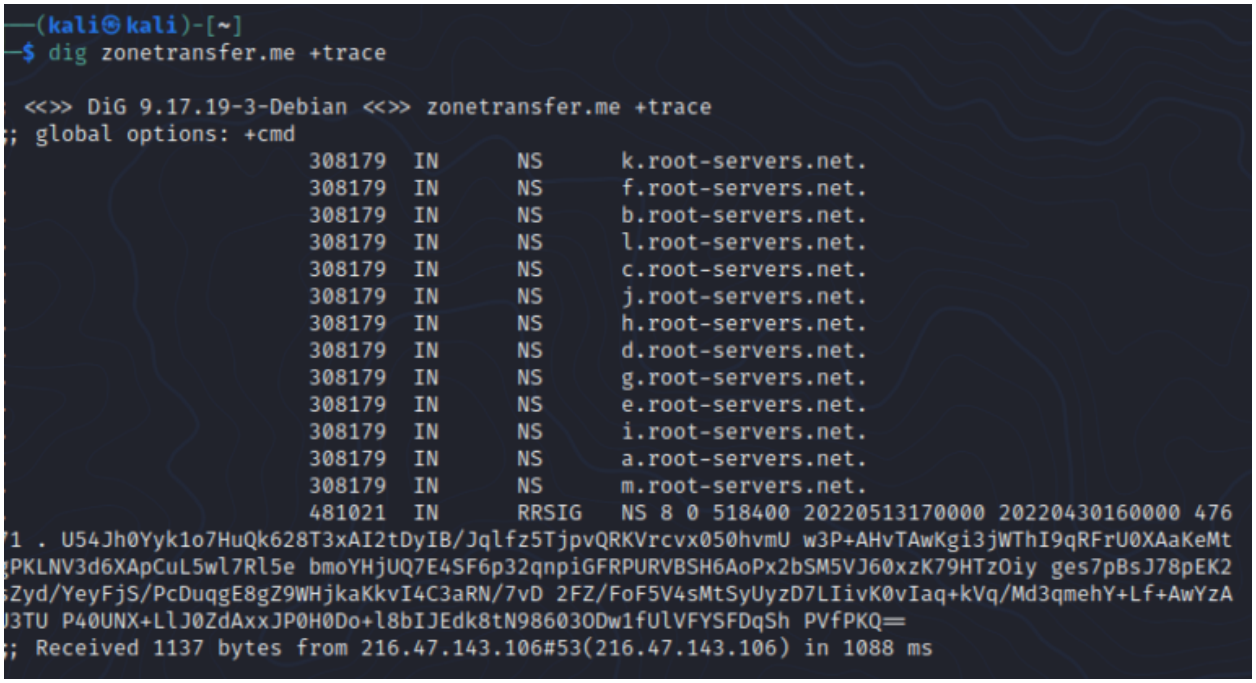


Figure 13: Using dig for DNS lookup and Tracing





Part 6: Collecting Information With TheHarvester

TheHarvester is a widely used command line utility employed by ethical hackers to footpring an organization along with “Google Hacking” and DNS reconnaissance. TheHarverster is particularly good at crawling the web for various bits of information regarding a target. And can be configured with a wide variety of command line flags to suit almost any application.

Figure 14: Using TheHarvester to Find Interesting URLs In the iit Domain

Figure 15: List of hosts in the Domain

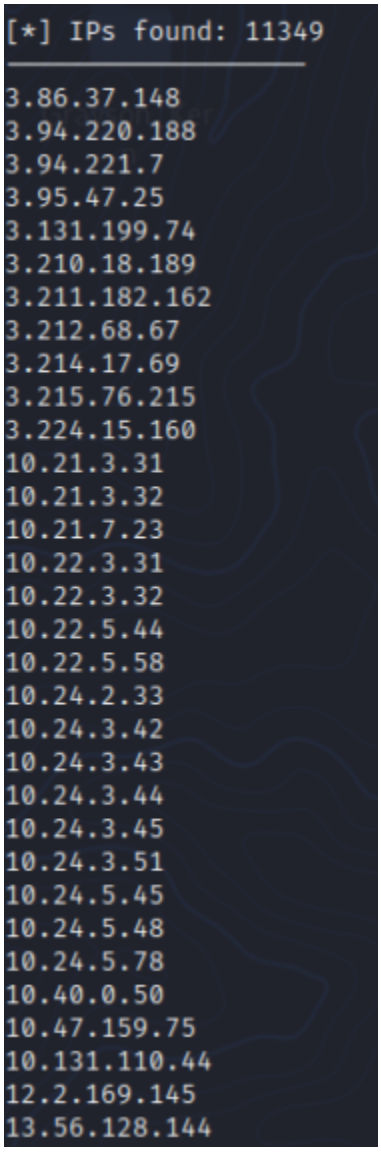


Figure 16: Configuring TheHarvster With Command Line Flags