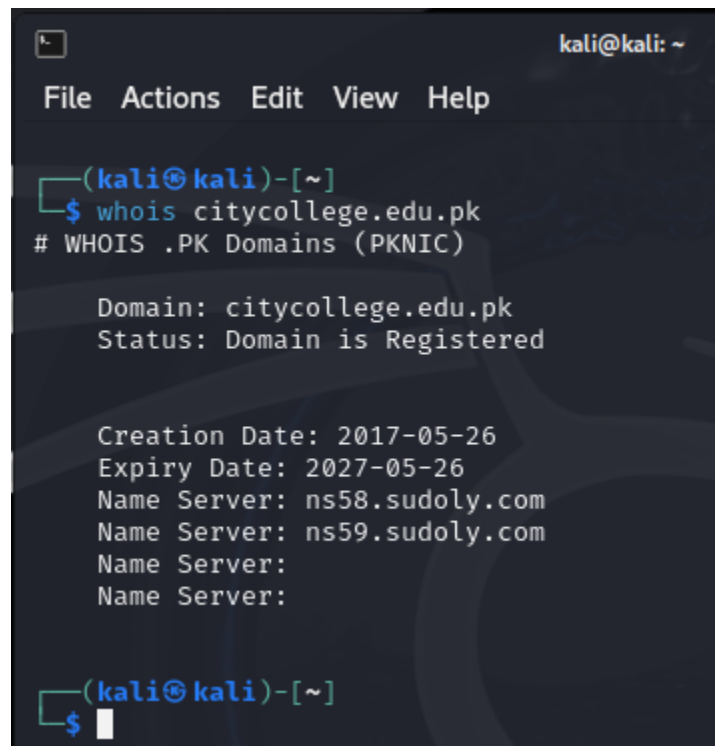


# Email and Domain Information Gathering

Information Gathering is the process of collecting essential data about the target domain or network. Information can be of various types, like subdomains of the target domain, DNS Information, Port Information, etc.

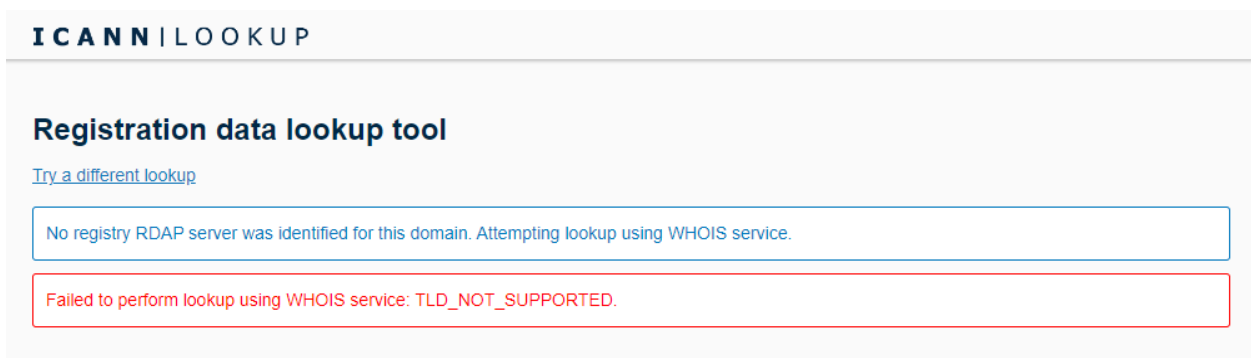
**Example:**

1. **WHOIS Lookup:**  
By using Commands:



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ whois citycollege.edu.pk  
# WHOIS .PK Domains (PKNIC)  
  
Domain: citycollege.edu.pk  
Status: Domain is Registered  
  
Creation Date: 2017-05-26  
Expiry Date: 2027-05-26  
Name Server: ns58.sudoly.com  
Name Server: ns59.sudoly.com  
Name Server:  
Name Server:  
(kali@kali)-[~]  
$
```

**By Using Website:**



**ICANN | LOOKUP**

---

**Registration data lookup tool**

[Try a different lookup](#)

No registry RDAP server was identified for this domain. Attempting lookup using WHOIS service.

Failed to perform lookup using WHOIS service: TLD\_NOT\_SUPPORTED.

## DNS Records Analysis:

Cmd: dig citycollege.edu.pk MX

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ dig citycollege.edu.pk MX  
  
; <<>> DiG 9.19.21-1+b1-Debian <<>> citycollege.edu.pk MX  
;; global options: +cmd  
;; Got answer:  
;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 60875  
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1  
  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags:; udp: 1232  
;; QUESTION SECTION:  
;citycollege.edu.pk.          IN      MX  
  
;; ANSWER SECTION:  
citycollege.edu.pk.          14400   IN      MX      0 citycollege.edu.pk.  
  
;; Query time: 324 msec  
;; SERVER: 100.64.100.1#53(100.64.100.1) (UDP)  
;; WHEN: Fri Jul 26 03:48:58 EDT 2024  
;; MSG SIZE rcvd: 63  
  
(kali@kali)-[~]
```

Cmd: nslookup -type=TXT Citycollege.edu.pk

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ nslookup -type=TXT citycollege.edu.pk  
Server:          100.64.100.1  
Address:         100.64.100.1#53  
  
Non-authoritative answer:  
citycollege.edu.pk      text = "v=spf1 ip4:209.172.2.100 +a +mx +ip4:149.56.18.177 ~all"  
  
Authoritative answers can be found from:  
  
(kali@kali)-[~]  
$
```

Website: [MXToolbox.com](http://MXToolbox.com)

[a:citycollege.edu.pk](https://citycollege.edu.pk)
Find Problems
↻ a

Type	Domain Name	IP Address	TTL
A	citycollege.edu.pk	209.172.2.100 OrangeHost (AS19053)	4 hrs

	Test	Result
✓	DNS Record Published	DNS Record found

[dns check](#)
[mx lookup](#)
[dmarc lookup](#)
[spf lookup](#)
[dns propagation](#)

Reported by [ns59.sudoly.com](#) on 7/26/2024 at 2:54:31 AM (UTC -5), [just for you.](#)

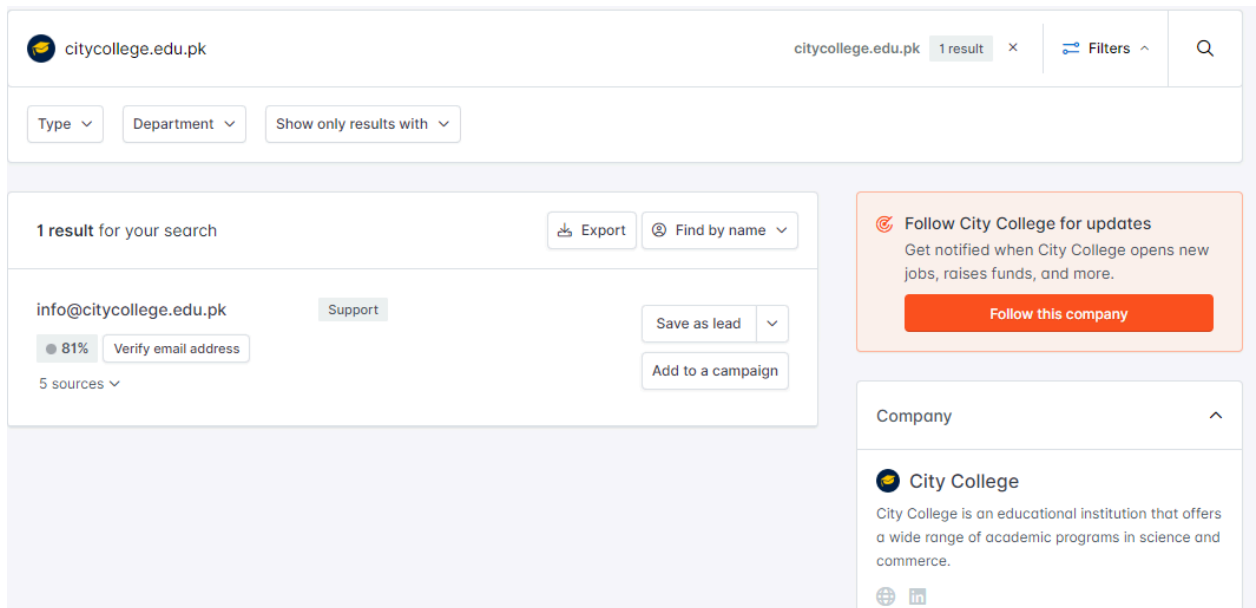
[Transcript](#)

### Email Address Search:

Cmd: theHarvester -d citycollege.edu.pk -b google

[illegible]

Website: Hunter.io



## Metadata Analysis:

Metadata analysis can be a useful tool in ethical hacking because it can help investigators understand what happened during a cyberattack. Metadata is data that describes other data, such as comments, timestamps, and file paths. It can be found in many digital artifacts, including files, emails, databases, and other proprietary data sets.

## Document Metadata Extraction:

Tools/Webbsites:

**exiftool pass.txt**

```
(kali@kali)-[~]
$ cd Desktop

(kali@kali)-[~/Desktop]
$ exiftool pass.txt
ExifTool Version Number      : 12.76
File Name                    : pass.txt
Directory                    : .
File Size                    : 109 bytes
File Modification Date/Time   : 2024:07:05 12:17:49-04:00
File Access Date/Time        : 2024:07:05 12:18:18-04:00
File Inode Change Date/Time   : 2024:07:05 12:17:49-04:00
File Permissions              : -rw-rw-r--
File Type                    : TXT
File Type Extension          : txt
MIME Type                    : text/plain
MIME Encoding                : us-ascii
Newlines                     : Unix LF
Line Count                   : 1
Word Count                   : 1

(kali@kali)-[~/Desktop]
```

## Online Metadata Analysis

Website: [Get-Metadata2.go.com](https://get-metadata2.go.com)

fiverr.json	
image_width	1361
image_height	711
bit_depth	8
color_type	RGB with Alpha
compression	Deflate/Inflate
filter	Adaptive
interlace	Noninterlaced
srgb_rendering	Perceptual
gamma	2.2
pixels_per_unit_x	3779
pixels_per_unit_y	3779
pixel_units	meters
image_size	1361x711
megapixels	0.968
category	image
raw_header	89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52 00 00 05 51 00 00 02 C7 08 06 00 00 00 87 78 02 03 00 00 00 01 73 52 47 42 00 AE CE 1C E9 00 00 00 04 67 41 4D 41 00 00 B1 8F 0B FC 61 05 00 00 00 09 70 48 59 73 00 00 0E C3 00 00 0E C3 01 C7 6F A8 64 00 00 F4 E3 49 44 41 54 78 5E EC DD 0B 7C 15 E5 9D FF 71 FF DD ED BF F7 FB 75 2F B6 DD DE EF 17 DB DD 6D BB ED AE B6 2B F4 2F 6E 0B B8