

# FOOTPRINTING ON Thirdwheel.com.np



FOOTPRINTING

**REPORT ON FOOTPRINTING**

**Thirdwheel.com.np**

**DATE 27, NOV, 2021**

**Charchit Subedi**

## Contents

|                               |   |
|-------------------------------|---|
| Introduction.....             | 2 |
| Basic Info .....              | 2 |
| Basic Component.....          | 3 |
| Network.....                  | 3 |
| TYPES OF FOOTPRINTING .....   | 4 |
| Types of foot printing: ..... | 4 |
| □ ACTIVE.....                 | 4 |
| □ PASSIVE .....               | 4 |
| ACTIVE FOOTPRINTING:.....     | 4 |
| Whois .....                   | 5 |
| AQUATONE .....                | 5 |
| SUBLIST3R.....                | 6 |
| KNOCKPY .....                 | 7 |
| PASSIVE .....                 | 8 |
| Conclusion .....              | 9 |
| 1. Domain Name .....          | 9 |
| 2. Sub Domains.....           | 9 |
| 3. Ip Address .....           | 9 |
| 4. Name Server.....           | 9 |
| 5. Mail Server.....           | 9 |
| 6. Contacts.....              | 9 |
| 9. Telephone Numbers.....     | 9 |
| 10. Host .....                | 9 |

## **T** Introduction

Third Wheel is established on 2018 A.D with a mission to help general public by providing them two wheeler services in a convenient and reliable way through mobile app. Initially, started with just regular servicing, we are now adding up services like emergency services, blue book renew, bike accessories etc. As time went on, we have been adding additional features in our app and providing other additional services which may be helpful for people in their daily life.

### **How it Works?**

#### **Pick Up**

Your precious time shouldn't be consumed for your two-wheeler maintenance. Either from home or office or even on your way, Third wheel users are hassle-free. One small buzz on your mobile app and Third wheel assistance are right there.

#### **Servicing**

We have experts of automobile to deliver excellence at your doorsteps. Reliable maintenance, reasonable price, quality assurance and customized care. Maintaining your Bike and timely servicing is our responsibility.

#### **Delivery**

So where do you want your bike to be delivered? When do you need your bike? Third wheel ensures timely delivery of quality services, you will never be disappointed.

### **Basic Info**

|                               |                                                              |
|-------------------------------|--------------------------------------------------------------|
| <b>Domain Name:</b>           | thirdwheel.com.np                                            |
| <b>IP Address :</b>           | 202.51.74.39                                                 |
| <b>IP Location :</b>          | Province 3 – Kathmandu – communication and communicate nepal |
| <b>First registered date:</b> | 2018-08-03 12:53:44                                          |
| <b>Last updated date:</b>     | 2020-01-21 11:09:54                                          |
| <b>Primary name server:</b>   | ns1.thirdwheel.com.np                                        |
| <b>Secondary name server:</b> | ns2.thirdwheel.com.np                                        |
| <b>Registrant Email:</b>      | thirdwheelnepal@gmail.com                                    |
| <b>Contact person:</b>        | Arun Kumar Raut                                              |
| <b>Company name:</b>          | third wheel pvt. ltd.                                        |
| <b>Administrative Email :</b> | thirdwheelnepal@gmail.com                                    |
| <b>Telephone:</b>             | 01-621553                                                    |
| <b>Address:</b>               | Lokanthali - 1, Madhayapur Thimi                             |

## Basic Component

- **Widgets:** Facebook , OWL Carousel
- **Programming languages:** PHP 7.4.20
- **Analytics:** Facebook Pixel 2.9.48, google analytics
- **JavaScript frameworks:** Angular JS 1.4.4 , RequireJS 2.1.14sqdp1
- **Web frameworks:** Laravel
  - **Web Server :** Apache 2.4.6
  - **Web Server extensions :** OpenSSL 1.0.2k
  - **Operating System :** CentOS
  - **Hosting Panels :** cPanel
  - **UI Frameworks :** Bootstrap 4.3.1 , Animate.css
  - **Live chat :** Facebook Chat Plugin 2.12
- **Miscellaneous:** Popper 1.14.7
- **Javascript libraries:** core-js 3.1.3 , loadsh 4.8.2 , SweetAlert2 , YUI 2.9.0 , jQuery

## Network

- **Site** <https://www.thirdwheel.com.np>
  - **unique hosts:**
    1. 202.51.74.39 dev.thirdwheel.com.np
    2. 202.51.74.39 ns2.thirdwheel.com.np
    3. 202.51.74.39 ns1.thirdwheel.com.np
    4. 202.51.74.39 www.thirdwheel.com.np
  - **Found Subdomain :** 9
    - www.thirdwheel.com.np
    - cpanel.thirdwheel.com.np
    - dev.thirdwheel.com.np
    - www.dev.thirdwheel.com.np
    - mail.thirdwheel.com.np
    - srv.thirdwheel.com.np
    - www.srv.thirdwheel.com.np
    - webdisk.thirdwheel.com.np
    - webmail.thirdwheel.com.np

**Found Subnets :** - 202.51.74.0-255 : 6 host

- **IP ADDRESS :** 202.51.74.39

## **TYPES OF FOOTPRINTING**

Footprinting is the initial step of an assault on data frameworks where an aggressor gathers data about an objective organization for distinguishing different ways of interfering into the framework. Utilizing this, we can track down various freedoms to infiltrate and evaluate the objective association's organization.

### **Types of foot printing:**

□ **ACTIVE**

□ **PASSIVE**

### **ACTIVE FOOTPRINTING:**

This includes gathering data about the objective with direct connection. In this sort of footprinting, the objective might perceive the continuous data gathering process, as we just collaborate with the objective organization.

Dynamic Footprinting strategies include:

1. Questioning distributed name servers of the objective
2. Removing metadata of distributed reports and records
3. Taking a great deal of site data utilizing different kinds of reflecting and web spidering devices
4. Social event data through email following
5. Performing Whois query
6. Removing DNS data
7. Performing traceroute investigation
8. Performing social designing

The significant objectives of footprinting consolidate gathering the association information, centralized server information, and progressive information of the person in question. By coordinating footprinting across different association levels, we can obtain valuable information, for instance, network blocks, express IP addresses, agent nuances, and so on such information can help the organization interlopers in getting to private data or performing various kinds of hacks on the goal association.

## Whois

Whois is an Internet administration and convention that queries and shows data relating to an area name from stores of space name enlistment centers around the world. Whois administration is a free Internet administration that empowers a client to look through a particular area name's accessibility and, for the situation that it's enrolled, the allotted substance/individual to whom it is enlisted. Whois was first considered in 1982 as an upgrade to the Nickname convention that was created by ARPANET.

### **WHOIS search results**

|                        |                                  |
|------------------------|----------------------------------|
| Domain Name:           | thirdwheel.com.np                |
| First registered date: | 2018-08-03 12:53:44              |
| Last updated date:     | 2020-01-21 11:09:54              |
| Primary name server:   | ns1.thirdwheel.com.np            |
| Secondary name server: | ns2.thirdwheel.com.np            |
| Registrant Email:      | thirdwheelnepal@gmail.com        |
| Contact person:        | Arun Kumar Raut                  |
| Company name:          | third wheel pvt. ltd.            |
| Administrative Email : | thirdwheelnepal@gmail.com        |
| Telephone:             | 01621553                         |
| Address:               | Lokanthali - 1, Madhayapur Thimi |

In this whois we can get the IP ADDRESS, Doiman name, SUB-Domain and other information.

## AQUATONE

AQUATONE is a bunch of instruments utilized for performing surveillance, checking, and revelation o area names. AQUATONE can find subdomains on a given objective area utilizing OSINT source and the most well-known space savage power strategy. Subsequent to finding the subdomain, the AQUATONE instrument can filter the space for standard web ports and HTTP headers data. HTML bodies and depictions can be gathered and considered as the report to investigate the assault climate rapidly.

```

  _____
 / _ _ \   / _ _ \   / _ _ \   / _ _ \
/_/_/    /_/_/    /_/_/    /_/_/
discover v0.5.0 - by @michenriksen

Identifying nameservers for thirdwheel.com.np... Done
Using nameservers:

- 202.51.74.39
- 202.51.74.39

Checking for wildcard DNS... Done

Running collector: Certificate Search... Done (3 hosts)
Running collector: HackerTarget... Done (5 hosts)
Running collector: Google Transparency Report... Done (3 hosts)
Running collector: Dictionary... Done (8210 hosts)
Running collector: Censys... Skipped
-> Key 'censys_secret' has not been set
Running collector: Riddler... Skipped
-> Key 'riddler_username' has not been set
Running collector: Wayback Machine... Done (2 hosts)
Running collector: PublicWWW... Done (0 hosts)
Running collector: PTRArchive... Error
-> PTRArchive returned unexpected response code: 502
Running collector: Threat Crowd... Done (2 hosts)
Running collector: DNSDB... Timed out
Running collector: Netcraft... Done (0 hosts)
Running collector: PassiveTotal... Skipped
-> Key 'passivetotal_key' has not been set
Running collector: VirusTotal... Skipped
-> Key 'virustotal' has not been set
Running collector: Shodan... Skipped
-> Key 'shodan' has not been set

Resolving 8211 unique hosts...
202.51.74.39 dev.thirdwheel.com.np
202.51.74.39 ns1.thirdwheel.com.np
202.51.74.39 ns2.thirdwheel.com.np
202.51.74.39 thirdwheel.com.np
202.51.74.39 www.dev.thirdwheel.com.np
202.51.74.39 www.thirdwheel.com.np

Found subnets:

- 202.51.74.0-255 : 6 hosts

Wrote 6 hosts to:

- file:///home/saugat/aquatone/thirdwheel.com.np/hosts.txt
- file:///home/saugat/aquatone/thirdwheel.com.np/hosts.json

```

In this above screenshot we can find the identifying name server and also we can check the domain host. In this aquatone we can found subnet, and resolving unique hosts.

## **SUBLIT3R**

Sublister is a device planned in python and utilizations OSINT to count subdomains of sites. It helps pen-analyzers in gathering and assembling subdomains for an area which is their objective. To get the exact outcomes, sublilster utilizes many web crawlers like Google, Yahoo, and so on and even apparatuses like Netcraft, Virustotal, and so forth.

```
(saugat@kali) - [~/Desktop/Sublist3r]
$ python3 sublist3r.py -d thirdwheel.com.np

          _____
         /  _  _  \
        /  /  \  \
       /  /    \  \
      /  /      \  \
     /  /        \  \
    /  /          \  \
   /  /            \  \
  /  /              \  \
 /  /                \  \
/  /                  \  \
\  \                  /  /
 \  \                /  /
  \  \              /  /
   \  \            /  /
    \  \          /  /
     \  \        /  /
      \  \      /  /
       \  \    /  /
        \  \  /  /
         \  \/_/

# Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for thirdwheel.com.np
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
[-] Total Unique Subdomains Found: 9
www.thirdwheel.com.np
cpanel.thirdwheel.com.np
dev.thirdwheel.com.np
www.dev.thirdwheel.com.np
mail.thirdwheel.com.np
srv.thirdwheel.com.np
www.srv.thirdwheel.com.np
webdisk.thirdwheel.com.np
webmail.thirdwheel.com.np

(saugat@kali) - [~/Desktop/Sublist3r]
$
```

In the above screenshot the tool name is Sublist3r where we can Enumerating subdomains and also used to find unique subdomain.



## KNOCKPY

Thump is an apparatus written in Python and is intended to identify subdomains in an objective space through a wordlist.

```
(saugat@kali) - [~/Desktop/knock]
$ python3 knockpy.py thirdwheel.com.np

v5.2.0

local: 10757 | google: 0 | duckduckgo: 3 | virustotal: 0
Wordlist: 10760 | Target: thirdwheel.com.np | Ip: 202.51.74.39
00:55:11

Ip address      Code Subdomain      Server      Real hostname
-----
202.51.74.39    200 dev.thirdwheel.com.np  Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips
202.51.74.39    200 ns2.thirdwheel.com.np  Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips
202.51.74.39    200 ns1.thirdwheel.com.np  Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips
202.51.74.39    www.thirdwheel.com.np

00:56:12
Ip address: 1 | Subdomain: 4 | elapsed time: 00:01:01

(saugat@kali) - [~/Desktop/knock]
$
```

We can find world list of domain and IP addresses, code, subdomain, servers, and real hostname.

## PASSIVE

This includes gathering data about the objective without direct connection. It is a kind of footprinting gathering that is essentially valuable when there is a necessity that the data gathering exercises are not to be identified by the objective isn't shipped off the objective association from a host or from mysterious has or benefits over the Internet. We can simply accumulate the recorded and set aside information about the objective using web crawlers, interpersonal interaction sites, and so on and some website and tools are used to footprinting for this report are given below:

- ❑ **Wappalyzer** : <https://www.wappalyzer.com/lookup/thirdwheel.com.np>
- ❑ **Spyse**: <https://spyse.com/search?query=thirdwheel.com.np&target=domain>
- . **Shodan.io** : <https://www.shodan.io/host/202.51.74.39>

Domain ▾

thirdwheel.com.np

+ Add Search Parameter

Results

5 results

**thirdwheel.com.np** 302 CRITICAL

Title: Third Wheel || Online Bike/Scooter Servicing

Final url: <https://thirdwheel.com.np/>

Alexa rank: 3023940

Issuer Org: Let's Encrypt

Scanned on 2021-08-30

DNS Records SSL/TLS

A: 202.51.74.39 - AS23647 - Communications & Communicate Nepal Pvt L... [Expand \(9\)](#)

MX: mx2.zoho.com

MX: mx3.zoho.com

MX: mx.zoho.com

PHP 7.4.16 Apache 2.4.6 CentOS OpenSSL 1.0.2

In this above picture same as we can insert the IP or Domain and we can all the need that we need for footprinting and gather the information.

## Conclusion

This report of footprinting was made only for the instructive reason to get the data about THIRDWHEEL.COM.NP All the examination was directed in a way that reenacted a noxious entertainer with the objectives of acquiring the data like:

1. Domain Name
2. Sub Domains
3. Ip Address
4. Name Server
5. Mail Server
6. Contacts
7. Telephone Numbers
- 8.Host

These objectives of get-together the data by Footprinting were met. All the necessary data are accumulated in the degree of access that an overall web client would have assembled. The data required are assembled from above source and devices as followed recorded previously.



