
pyonyphe Documentation

Release 1.0

Sebastien Larinier

May 18, 2022

Contents

1	Introduction	3
2	Examples	5
2.1	Search Information on an IP	5
3	API Reference	15
3.1	onyphe	15
	Python Module Index	17
	Index	19

This is the official Python wrapper around both the Onyphe REST API.

CHAPTER 1

Introduction

tutorial

2.1 Search Information on an IP

```
#!/usr/bin/env python
# onyphe_ip.py
#
# Author: Sebastien Larinier

import onyphe

API_KEY = "YOUR_API_KEY"
ip = sys.argv[1]
#Input validation
if len(sys.argv) == 1:
    print('Usage: %s ' % sys.argv[0])
    sys.exit(1)
try:
    # Setup the ap
    api = onyphe.Onyphe(API_KEY)
    # Perform the search
    result = api.summary_ip(ip)
    print(json.dumps(result))
except Exception as e:
    print('Error: %s' % e)
    sys.exit(1)
```

```
{'count': 32,
'error': 0,
'myip': '176.169.140.4',
'results': [{'@category': 'geoloc',
 '@timestamp': '2017-12-01T12:32:23.000Z',
 '@type': 'ip',
 'asn': 'AS15169',
```

(continues on next page)

(continued from previous page)

```

'city': '',
'country': 'US',
'country_name': 'United States',
'geolocation': '37.7510,-97.8220',
'ip': '8.8.8.8',
'ipv6': 'false',
'latitude': '37.7510',
'longitude': '-97.8220',
'organization': 'Google LLC',
'subnet': '8.8.0.0/19'},
{'@category': 'inetnum',
 '@timestamp': '1970-01-01T00:00:00.000Z',
 '@type': 'ip',
 'country': 'US',
 'information': ['Undisclosed'],
 'netname': 'Undisclosed',
 'seen_date': '1970-01-01',
 'source': 'Undisclosed',
 'subnet': 'Undisclosed'},
{'@category': 'pastries',
 '@timestamp': '2017-12-01T10:56:10.000Z',
 '@type': 'pastebin',
 'domain': ['discordapp.com', 'boards.net', '1blu.de', 'google.com'],
 'hostname': ['station.boards.net',
 'rv1898.1blu.de',
 'google-public-dns-a.google.com'],
 'ip': ['104.16.59.5',
 '104.16.20.142',
 '104.16.22.142',
 '104.16.23.142',
 '178.254.7.216',
 '104.16.19.142',
 '104.16.21.142',
 '104.16.58.5',
 '8.8.8.8'],
 'key': 'CSWkvpgt',
 'seen_date': '2017-12-01'},
{'@category': 'pastries',
 '@timestamp': '2017-12-01T10:12:19.000Z',
 '@type': 'pastebin',
 'domain': ['google.com'],
 'hostname': ['google-public-dns-a.google.com',
 'google-public-dns-b.google.com'],
 'ip': ['8.8.8.8',
 '255.0.0.0',
 '192.168.160.1',
 '192.168.52.128',
 '8.8.4.4',
 '192.168.52.0',
 '255.255.255.0',
 '255.255.255.255',
 '192.168.52.255',
 '127.0.0.1',
 'fe80::20c:29ff:feal:d692'],
 'key': 'rqDDrRaz',
 'seen_date': '2017-12-01'},
{'@category': 'pastries',

```

(continues on next page)

(continued from previous page)

```
'@timestamp': '2017-12-01T05:52:59.000Z',
'@type': 'pastebin',
'domain': ['raspbrian.org',
'google.com',
'githubusercontent.com',
'com.br',
'abuse.ch',
'hosts-file.net',
'malwaredomains.com',
'gt500.org',
'sysctl.org',
'amazonaws.com',
'ovh.net',
'co.uk',
'amazon.com'],
'hostname': ['zeustracker.abuse.ch',
'gist.githubusercontent.com',
'5-153-225-231.no-reverse-dns-set.bytemark.co.uk',
'210-29.amazon.com',
'raw.githubusercontent.com',
'mirror1.malwaredomains.com',
'bots.ovh.net',
'206-80.amazon.com',
's3.amazonaws.com',
'ec2-107-22-171-143.compute-1.amazonaws.com',
'gt500.org',
'google-public-dns-a.google.com',
'www.raspbian.org',
'186.216.161.195.user.vctelecom.com.br',
'166-22.amazon.com',
'google-public-dns-b.google.com'],
'ip': ['213.186.34.12',
'72.21.206.80',
'8.8.4.4',
'192.168.1.1',
'151.101.194.49',
'151.101.0.133',
'151.101.2.49',
'151.101.192.133',
'8.8.8.8',
'139.146.167.25',
'fe80::f15e:521c:71bb:4eb4',
'151.101.128.133',
'127.0.0.1',
'151.101.64.133',
'52.216.20.75',
'207.171.166.22',
'2001:41c9:1:3ce:0:0:1:10',
'151.101.66.49',
'74.63.222.170',
'151.101.130.49',
'186.216.161.195',
'192.168.1.10',
'72.21.210.29',
'5.153.225.231',
'107.22.171.143'],
'key': 'leyBGtdu',
```

(continues on next page)

(continued from previous page)

```

'seen_date': '2017-12-01'},
{'@category': 'pastries',
 '@timestamp': '2017-11-30T20:03:27.000Z',
 '@type': 'pastebin',
 'domain': ['google.com'],
 'hostname': ['google-public-dns-a.google.com'],
 'ip': ['fe80::441a:a7ff:fef4:8540',
 'fe80::42:fdff:fe89:f73e',
 'fe80::c8a9:2fff:fe24:5054',
 'fe80::14c5:5aff:fe58:212d',
 '192.168.1.254',
 '192.168.122.255',
 '255.255.255.0',
 'fe80::42:90ff:feb8:b5b0',
 '172.27.0.1',
 'fe80::e8b7:62ff:fe85:c537',
 '8.8.8.8',
 '172.21.0.1',
 'fe80::4c28:c4ff:fe34:846a',
 '192.168.1.0',
 '192.168.122.1',
 'fe80::42:caff:fe92:297b',
 '172.18.0.1',
 '172.20.0.1',
 'fe80::42:d2ff:fef2:fd9c',
 'fe80::f07a:3dff:fe06:a2cf',
 '172.22.0.1',
 '192.168.2.0',
 '192.168.1.111',
 '127.0.0.1',
 '172.30.0.1',
 '192.168.2.1',
 'fe80::5055:7fff:fe6e:71ed',
 'fe80::dach:8aff:fe7e:b00e',
 '192.168.1.255',
 '172.19.0.1',
 'fe80::7cb6:9dff:fe57:ffcc',
 'fe80::f41f:d4ff:fe3c:5a89',
 '172.17.0.1',
 '172.26.0.1',
 'fe80::42:40ff:fe01:23c5',
 '192.168.2.255'],
 'key': 'wdSRXk2y',
 'seen_date': '2017-11-30'},
{'@category': 'pastries',
 '@timestamp': '2017-11-30T19:24:26.000Z',
 '@type': 'pastebin',
 'domain': ['as48707.pl', 'google.com'],
 'hostname': ['google-public-dns-a.google.com',
 'ip-212-91-7-33.as48707.pl',
 'ip-212-91-6-58.as48707.pl'],
 'ip': ['8.8.8.8', '212.91.6.58', '212.91.7.33'],
 'key': 'TNbTeVXY',
 'seen_date': '2017-11-30'},
{'@category': 'pastries',
 '@timestamp': '2017-11-30T19:08:48.000Z',
 '@type': 'pastebin',

```

(continues on next page)

(continued from previous page)

```

'domain': ['google.com'],
'hostname': ['google-public-dns-a.google.com'],
'ip': ['8.8.8.8'],
'key': '0MjevuY6',
'seen_date': '2017-11-30'},
{'@category': 'pastries',
 '@timestamp': '2017-11-30T18:58:23.000Z',
 '@type': 'pastebin',
 'domain': ['google.com', 'github.com'],
 'hostname': ['1b-192-30-253-113-iad.github.com',
 'google-public-dns-a.google.com',
 '1b-192-30-253-112-iad.github.com'],
 'ip': ['8.8.8.8', '192.30.253.112', '192.30.253.113'],
 'key': '0wUc90E1',
 'seen_date': '2017-11-30'},
{'@category': 'pastries',
 '@timestamp': '2017-11-30T14:46:07.000Z',
 '@type': 'pastebin',
 'domain': ['lwn.net', 'google.com'],
 'hostname': ['google-public-dns-a.google.com', 'prod.lwn.net'],
 'ip': ['45.33.94.129',
 '255.255.255.255',
 '10.0.0.1',
 '2600:3c03:0:0:f03c:91ff:fe61:5c5b',
 '8.8.8.8',
 'fe80::ce51:67bd:73e8:fe63'],
 'key': '6jFXSW0s',
 'seen_date': '2017-11-30'},
{'@category': 'pastries',
 '@timestamp': '2017-11-30T14:29:21.000Z',
 '@type': 'pastebin',
 'domain': ['google.com'],
 'hostname': ['google-public-dns-a.google.com'],
 'ip': ['8.8.8.8', '127.0.0.1'],
 'key': 'T2UFRFRFW',
 'seen_date': '2017-11-30'},
{'@category': 'pastries',
 '@timestamp': '2017-11-30T14:01:17.000Z',
 '@type': 'pastebin',
 'domain': ['google.com'],
 'hostname': ['google-public-dns-a.google.com'],
 'ip': ['10.0.0.1', '255.255.255.255', '8.8.8.8'],
 'key': 'RaYZP25y',
 'seen_date': '2017-11-30'},
{'@category': 'synscan',
 '@timestamp': '2017-11-26T23:47:45.000Z',
 '@type': 'port-53',
 'asn': 'AS15169',
 'country': 'US',
 'ip': '8.8.8.8',
 'location': '37.7510,-97.8220',
 'organization': 'Google LLC',
 'os': 'Linux',
 'port': '53',
 'seen_date': '2017-11-26'},
{'@category': 'synscan',
 '@timestamp': '2017-11-26T22:47:46.000Z',

```

(continues on next page)

(continued from previous page)

```

'@type': 'port-53',
'asn': 'AS15169',
'country': 'US',
'ip': '8.8.8.8',
'location': '37.7510,-97.8220',
'organization': 'Google LLC',
'os': 'Linux',
'port': '53',
'seen_date': '2017-11-26'},
{'@category': 'synscan',
 '@timestamp': '2017-11-26T22:47:42.000Z',
 '@type': 'port-53',
 'asn': 'AS15169',
 'country': 'US',
 'ip': '8.8.8.8',
 'location': '37.7510,-97.8220',
 'organization': 'Google LLC',
 'os': 'Linux',
 'port': '53',
 'seen_date': '2017-11-26'},
{'@category': 'synscan',
 '@timestamp': '2017-11-26T22:47:31.000Z',
 '@type': 'port-53',
 'asn': 'AS15169',
 'country': 'US',
 'ip': '8.8.8.8',
 'location': '37.7510,-97.8220',
 'organization': 'Google LLC',
 'os': 'Linux',
 'port': '53',
 'seen_date': '2017-11-26'},
{'@category': 'synscan',
 '@timestamp': '2017-11-26T22:47:31.000Z',
 '@type': 'port-53',
 'asn': 'AS15169',
 'country': 'US',
 'ip': '8.8.8.8',
 'location': '37.7510,-97.8220',
 'organization': 'Google LLC',
 'os': 'Linux',
 'port': '53',
 'seen_date': '2017-11-26'},
{'@category': 'synscan',
 '@timestamp': '2017-11-26T22:47:26.000Z',
 '@type': 'port-53',
 'asn': 'AS15169',
 'country': 'US',
 'ip': '8.8.8.8',
 'location': '37.7510,-97.8220',
 'organization': 'Google LLC',
 'os': 'Linux',
 'port': '53',
 'seen_date': '2017-11-26'},
{'@category': 'synscan',
 '@timestamp': '2017-11-26T22:47:24.000Z',
 '@type': 'port-53',
 'asn': 'AS15169',

```

(continues on next page)

(continued from previous page)

```

'country': 'US',
'ip': '8.8.8.8',
'location': '37.7510,-97.8220',
'organization': 'Google LLC',
'os': 'Linux',
'port': '53',
'seen_date': '2017-11-26'},
{'@category': 'synscan',
 '@timestamp': '2017-11-26T22:47:20.000Z',
 '@type': 'port-53',
 'asn': 'AS15169',
 'country': 'US',
 'ip': '8.8.8.8',
 'location': '37.7510,-97.8220',
 'organization': 'Google LLC',
 'os': 'Linux',
 'port': '53',
 'seen_date': '2017-11-26'},
{'@category': 'synscan',
 '@timestamp': '2017-11-26T22:47:20.000Z',
 '@type': 'port-53',
 'asn': 'AS15169',
 'country': 'US',
 'ip': '8.8.8.8',
 'location': '37.7510,-97.8220',
 'organization': 'Google LLC',
 'os': 'Linux',
 'port': '53',
 'seen_date': '2017-11-26'},
{'@category': 'synscan',
 '@timestamp': '2017-11-26T22:47:17.000Z',
 '@type': 'port-53',
 'asn': 'AS15169',
 'country': 'US',
 'ip': '8.8.8.8',
 'location': '37.7510,-97.8220',
 'organization': 'Google LLC',
 'os': 'Linux',
 'port': '53',
 'seen_date': '2017-11-26'},
{'@category': 'resolver',
 '@timestamp': '2017-11-26T14:37:09.000Z',
 '@type': 'forward',
 'domain': 'better-than.tv',
 'forward': 'area61.better-than.tv',
 'ip': '8.8.8.8',
 'ipv6': 0,
 'seen_date': '2017-11-26'},
{'@category': 'resolver',
 '@timestamp': '2017-11-25T15:19:42.000Z',
 '@type': 'reverse',
 'domain': 'google.com',
 'ip': '8.8.8.8',
 'ipv6': 0,
 'reverse': 'google-public-dns-a.google.com',
 'seen_date': '2017-11-25'},
{'@category': 'resolver',

```

(continues on next page)

(continued from previous page)

```

'@timestamp': '2017-11-21T21:38:10.000Z',
'@type': 'reverse',
'domain': 'google.com',
'ip': '8.8.8.8',
'ipv6': 0,
'reverse': 'google-public-dns-a.google.com',
'seen_date': '2017-11-21'},
{'@category': 'resolver',
 '@timestamp': '2017-11-20T03:34:43.000Z',
 '@type': 'forward',
 'domain': 'apa.at',
 'forward': 'apasfwl.apa.at',
 'ip': '8.8.8.8',
 'ipv6': 0,
 'seen_date': '2017-11-20'},
{'@category': 'resolver',
 '@timestamp': '2017-11-18T14:44:02.000Z',
 '@type': 'reverse',
 'domain': 'google.com',
 'ip': '8.8.8.8',
 'ipv6': 0,
 'reverse': 'google-public-dns-a.google.com',
 'seen_date': '2017-11-18'},
{'@category': 'resolver',
 '@timestamp': '2017-11-16T17:31:34.000Z',
 '@type': 'reverse',
 'domain': 'google.com',
 'ip': '8.8.8.8',
 'ipv6': 0,
 'reverse': 'google-public-dns-a.google.com',
 'seen_date': '2017-11-16'},
{'@category': 'resolver',
 '@timestamp': '2017-11-15T21:13:31.000Z',
 '@type': 'reverse',
 'domain': 'google.com',
 'ip': '8.8.8.8',
 'ipv6': 0,
 'reverse': 'google-public-dns-a.google.com',
 'seen_date': '2017-11-15'},
{'@category': 'resolver',
 '@timestamp': '2017-11-14T17:22:21.000Z',
 '@type': 'forward',
 'domain': 'bot.nu',
 'forward': 'bot.nu',
 'ip': '8.8.8.8',
 'ipv6': 0,
 'seen_date': '2017-11-14'},
{'@category': 'resolver',
 '@timestamp': '2017-11-14T04:58:21.000Z',
 '@type': 'reverse',
 'domain': 'google.com',
 'ip': '8.8.8.8',
 'ipv6': 0,
 'reverse': 'google-public-dns-a.google.com',
 'seen_date': '2017-11-14'},
{'@category': 'resolver',
 '@timestamp': '2017-11-13T18:45:27.000Z',

```

(continues on next page)

(continued from previous page)

```
'@type': 'reverse',
'domain': 'google.com',
'ip': '8.8.8.8',
'ipv6': 0,
'reverse': 'google-public-dns-a.google.com',
'seen_date': '2017-11-13'}],
'status': 'ok',
'took': '0.098',
'total': 1481}
```


3.1 onyphe

3.1.1 Exceptions

O

onyphe, [15](#)

O

onyphe (*module*), 15