

# IPInfo App for Splunk

App Version: 5.1.1

Author: Neel Shah - Greenace Consultants

Description: Installation and Configuration Document for IPInfo App for Splunk

Latest Update Date: 15<sup>th</sup> Dec, 2020

## Version Summary

Version	Change History
1.0.0	Initial Version
1.0.2	Added Screenshots and Web Installation Steps
1.0.3	Replace old dashboard screen with new
1.0.7	Bug Fixes, Color Issues
3.0.0	Support to Splunk 8.x and Python 3.x
	Internal Updates
3.4.9	New scripted lookup New ipinfobatch command
3.4.11	Bug Fixes and Compliance to Splunk App Inspect
3.5.3	Added Support for New Lookup Commands. <ul style="list-style-type: none"><li>- privacyinfolookup</li><li>- domaininfolookup</li><li>- rangesinfolookup</li></ul>
3.5.4	Bugfixes : Issues with ipinfolookup command
4.0.0	IPInfo not supported on Splunk 6.x and 7.x
4.0.9	Support for Proxy Settings
5.0.2	Support for Splunk Search Head Cluster
5.1.1	Merging ipinfolookup capability with original ipinfo command privacyinfolookup to now be privacyinfo domaininfolookup to now be domaininfo rangesinfolookup to now be rangesinfo

OS
Windows 10
Windows Server 2012
Windows Server 2016
RHEL 7
RHEL 8
UBUNTU 14
UBUNTU 16
UBUNTU 18
UBUNTU 20

## Supported Splunk

Splunk
Splunk 8.X

IPInfo App for Splunk provides an Integration between IPInfo API and Splunk. This app adds *ipinfo* command to Splunk, which uses IPINFO API engine to lookup information for a given IP

## Install the App

NOTE: There are multiple ways of deploying apps to Splunk environment, in this document we'll be referring installation via CLI (Command Line Interface)

### CASE1: SINGLE STAND ALONE MACHINE (CLI)

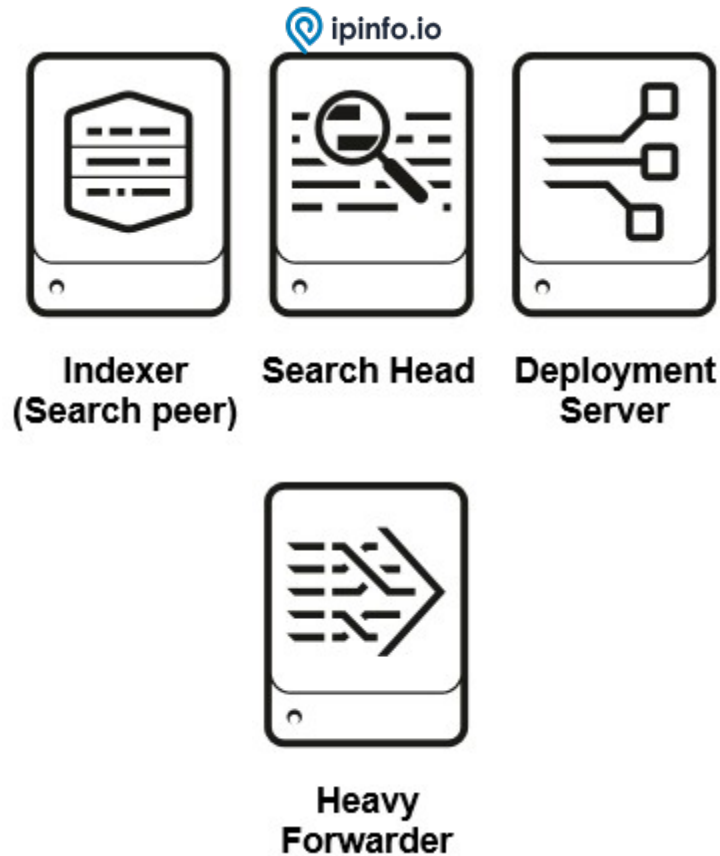
Single standalone Splunk Enterprise Installation on Windows/\*NIX



1. **Unzip ipinfo\_app.spl**
2. **Copy** the unzipped directory **ipinfo\_app** to **\$SPLUNK\_HOME/etc/apps/**
3. **Open CLI** and restart Splunk using **./splunk restart**

## CASE2: DISTRIBUTED ARCHITECTURE

Single Indexer Single Search head and Single forwarder (Heavy or Universal) and Deployment server



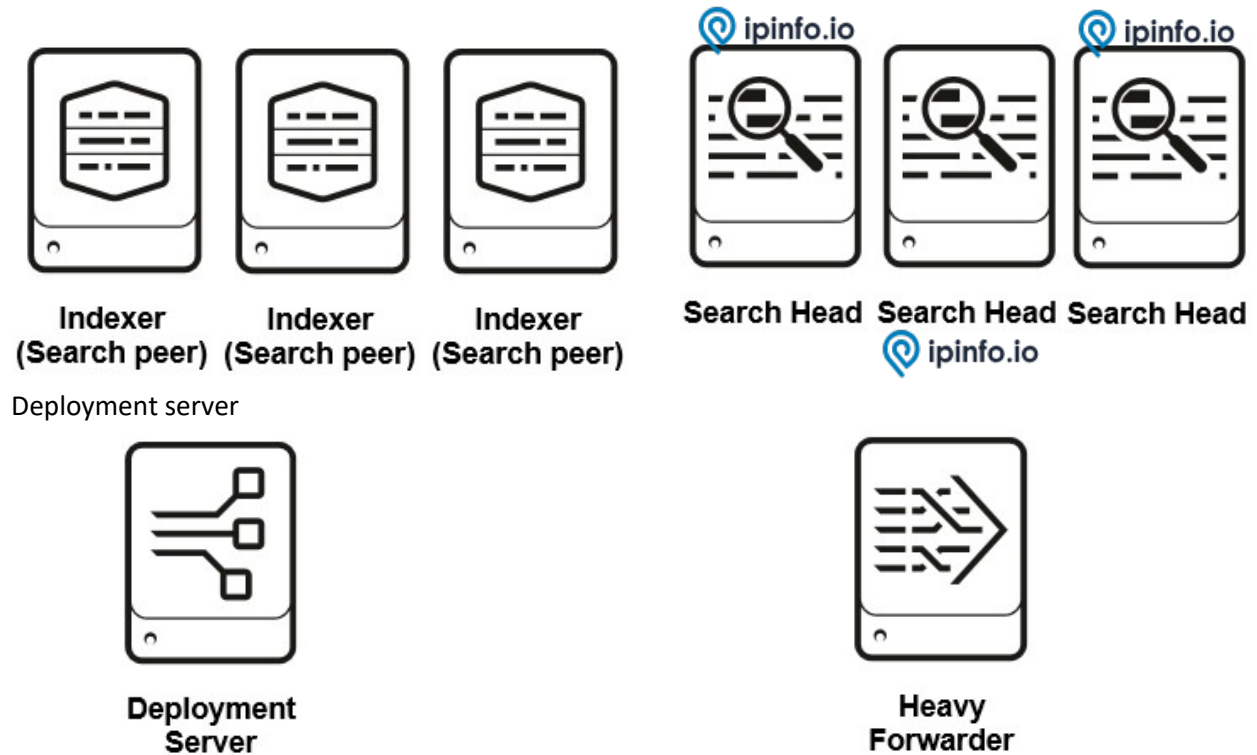
1. **Unzip ipinfo\_app.spl**
2. **Copy** the unzipped directory **ipinfo\_app** to deployment server in the following location  
**\$SPLUNK\_HOME/etc/deployment-apps/**
3. Add following to **serverclass.conf**

```
[serverClass:<SEARCHHEAD_SERVERCLASS>:app:< ipinfo_app > ]  
stateOnClient=enabled  
restartSplunkd=true
```

4. **Open CLI** deploy the apps using following command **./splunk reload deploy-server**

### CASE3: DISTRIBUTED ARCHITECTURE

Multiple non-clustered Indexers, Multiple non-clustered SearchHeads, Forwarder(Heavy or Universal) and



1. Unzip **ipinfo\_app.spl**
2. Copy the unzipped directory **ipinfo\_app** to deployment server in the following location  
**\$SPLUNK\_HOME/etc/deployment-apps/**
3. Add following to **serverclass.conf**

```
[serverClass:<SEARCHHEAD_SERVERCLASS>:app:< ipinfo_app >]
stateOnClient=enabled
restartSplunkd=true
```

4. Open CLI deploy the apps using following command **./splunk reload deploy-server**

## CASE4: DISTRIBUTED ARCHITECTURE

Single Site clustered Indexer, Clustered Search heads and Forwarder (Heavy or Universal).



1. **Unzip ipinfo\_app.spl**
2. **Copy ipinfo\_app** to Deployer server in the following location `$SPLUNK_HOME/etc/shcluster/apps/`
3. **Open CLI** on Deployer and deploy the app on Search Head Cluster using following command  
`./splunk apply shcluster-bundle -target <URI>:<management_port> -auth <username>:<password>`

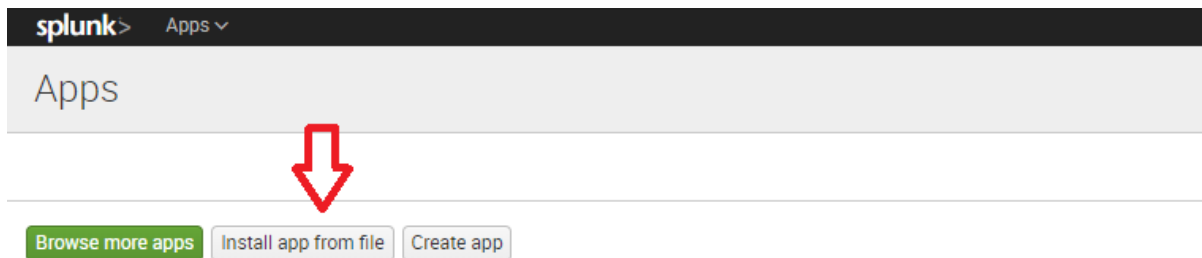


## CASE5: STANDALONE INSTALLATION (WEB)

1. On the Splunk Home Page, Click on “Manage Apps”



2. On the Manage Apps page, Click on “Install app from file”



3. Select path for IPINFO Splunk app and Click “Upload”

### Upload an app

If you have a .spl or .tar.gz app file to install, you can upload it using this form.

You can replace an existing app via the Splunk CLI. [Learn more.](#)

File

ipinfo\_app.tgz

☐ Upgrade app. Checking this will overwrite the app if it already exists.

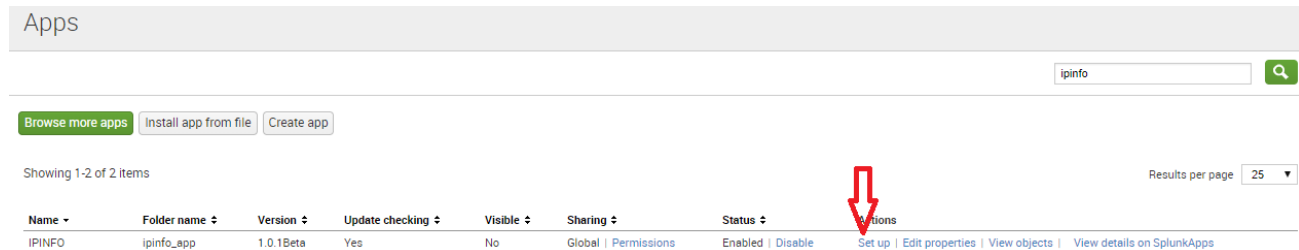
4. Splunk will prompt you to restart the machine, please restart

☒ **Restart Required**

You must restart Splunk Enterprise to complete update of this app.

## Configuration

1. After Installation and restart, login to the Splunk web and go to 'Manage Apps'
2. It will list out all the installed application and their configuration option.
3. Look for 'IPINFO' and click on the 'Set-Up' link to configure the add on.
- 4.



Apps

ipinfo

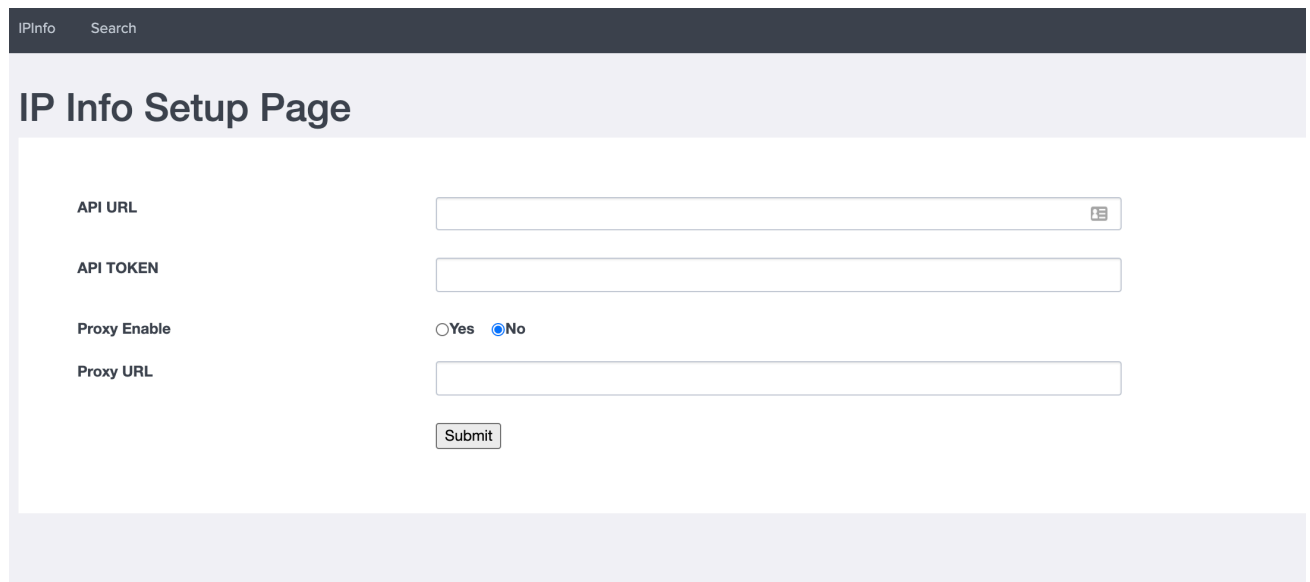
Browse more apps Install app from file Create app

Showing 1-2 of 2 items Results per page 25

Name	Folder name	Version	Update checking	Visible	Sharing	Status	Actions
IPINFO	ipinfo_app	1.0.1Beta	Yes	No	Global   Permissions	Enabled   Disable	Set up   Edit properties   View objects   View details on SplunkApps

## API Configuration

Just Enter your personalized authorization token, there is also link to purchase the token



IPInfo Search

### IP Info Setup Page

API URL

API TOKEN

Proxy Enable ☐ Yes ☒ No

Proxy URL

Submit

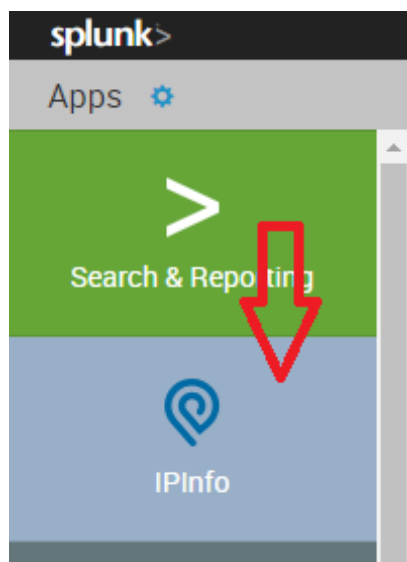
## CLI Configuration

Just update ip\_info\_setup.conf in \$SPLUNK\_HOME/etc/apps/ip\_info/local/

```
[api_configuration]  
api_url = https://ipinfo.io/  
token = <your token here>
```

and restart Splunk

## ACCESSING THE APP



## TEST COMMAND

-----IPInfo -----

```
| makeresults 1 | eval ip_add="1.186.41.179" | ipinfo ip_add | table ip, city, region, country, loc, postal, hostname
```

## Availability of Fields

- **Basic Subscription** - ip, city, region, country, loc, org, postal, hostname
- **Standard Subscription** - ip, city, region, country, loc, postal, hostname asn\_asn, asn\_name, asn\_domain, asn\_route, asn\_type
- **Pro Subscription** - ip, city, region, country, loc, postal, hostname asn\_asn, asn\_name, asn\_domain, asn\_route, asn\_type, company\_name, company\_domain, company\_type, carrier\_name, carrier\_mcc, carrier\_mnc

## ----- IPInfo Lookup -----

| makeresults | eval

ip="197.94.71.228,197.94.71.227,197.94.71.221,197.94.71.226,197.94.71.225,197.94.71.230" |  
makemv delim="," ip | mvexpand ip | ipinfolookup ip

IPInfo

Search

ipinfo.io

Save As

Close

New Search

| makeresults | eval ip="197.94.71.228,197.94.71.227,197.94.71.221,197.94.71.226,197.94.71.225,197.94.71.230" | makemv delim="," ip | mvexpand ip | lookup ipinfolookup ip

Last 24 hours

Q

✓ 6 results (7/12/20 9:00:00.000 PM to 7/13/20 9:50:17.000 PM)

No Event Sampling

Job

Smart Mode

Events

Patterns

Statistics (6)

Visualization

20 Per Page

Format

Preview

_time	asn	asn_asn	asn_domain	asn_name	asn_route	asn_type	carrier_mcc	carrier_mnc	carrier_name	city	company_domain	company_name	company_type	country	hostname	ip	loc
2020-07-13 21:58:17		Dimension Data (Pty) Ltd - Optinet	197.94.0.0/16	optinet.net	isp	Dimension Data (Pty) Ltd - Optinet				Cape Town	isp	optinet.net		ZA	197-94-71-228.hff.mweb.co.za	197.94.71.228	-33.9258,18.4232
2020-07-13 21:58:17		Dimension Data (Pty) Ltd - Optinet	197.94.0.0/16	optinet.net	isp	Dimension Data (Pty) Ltd - Optinet				Cape Town	isp	optinet.net		ZA	197-94-71-227.hff.mweb.co.za	197.94.71.227	-33.9258,18.4232
2020-07-13 21:58:17		Dimension Data (Pty) Ltd - Optinet	197.94.0.0/16	optinet.net	isp	Dimension Data (Pty) Ltd - Optinet				Cape Town	isp	optinet.net		ZA	197-94-71-221.hff.mweb.co.za	197.94.71.221	-33.9258,18.4232
2020-07-13 21:58:17		Dimension Data (Pty) Ltd - Optinet	197.94.0.0/16	optinet.net	isp	Dimension Data (Pty) Ltd - Optinet				Cape Town	isp	optinet.net		ZA	197-94-71-226.hff.mweb.co.za	197.94.71.226	-33.9258,18.4232
2020-07-13 21:58:17		Dimension Data (Pty) Ltd - Optinet	197.94.0.0/16	optinet.net	isp	Dimension Data (Pty) Ltd - Optinet				Cape Town	isp	optinet.net		ZA	197-94-71-225.hff.mweb.co.za	197.94.71.225	-33.9258,18.4232
2020-07-13 21:58:17		Dimension Data (Pty) Ltd - Optinet	197.94.0.0/16	optinet.net	isp	Dimension Data (Pty) Ltd - Optinet				Cape Town	isp	optinet.net		ZA	197-94-71-230.hff.mweb.co.za	197.94.71.230	-33.9258,18.4232

## ----- IPInfo Batch -----

| ipinfobatch ip="197.94.71.228,197.94.71.227,197.94.71.221 , 197.94.71.226,197.94.71.225 ,197.94.71.22"

New Search

Save As

Close

| ipinfobatch ip="197.94.71.228,197.94.71.227,197.94.71.221 , 197.94.71.226,197.94.71.225 ,197.94.71.22"

Last 24 hours

Q

✓ 6 results (7/12/20 7:00:00.000 PM to 7/13/20 7:29:56.000 PM) No Event Sampling

Job ▼

Smart Mode ▼

Events (0) Patterns Statistics (6) Visualization

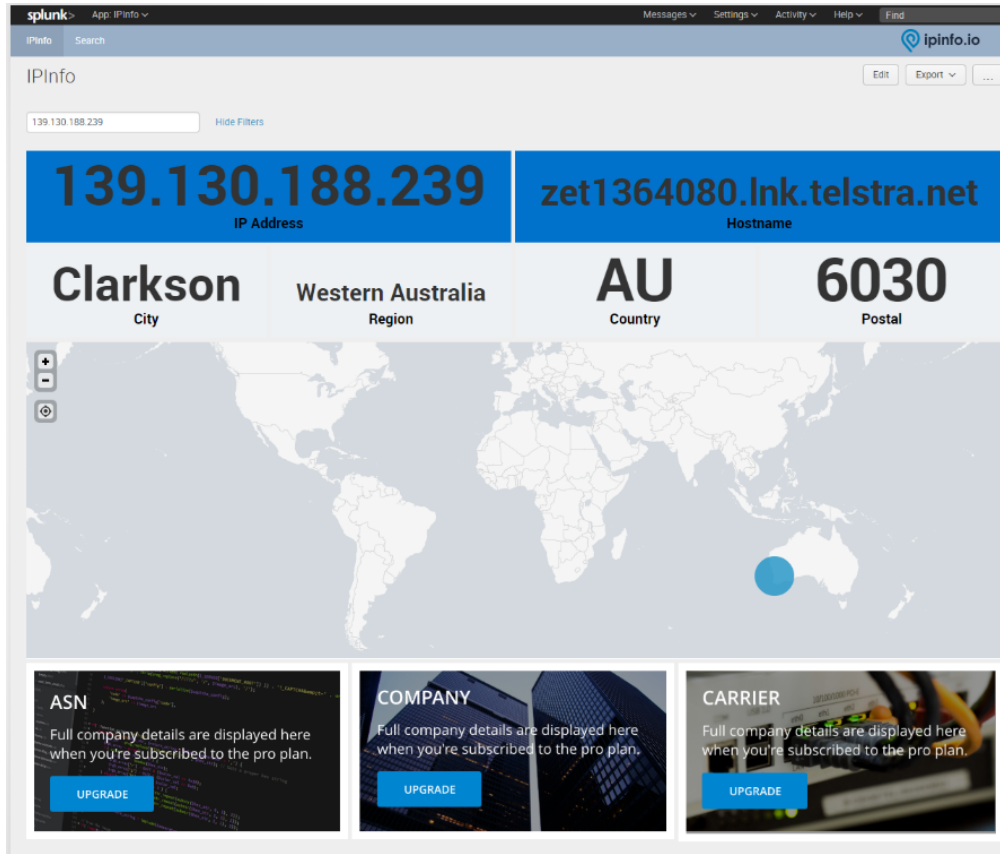
20 Per Page ▼

Format

Preview ▼

ip	hostname	city	region	country	loc	postal	timezone	asn	company	privacy
197.94.71.228	197-94-71-228.hff.mweb.co.za	Cape Town	Western Cape	ZA	-33.9258,18.4232	7945	Africa/Johannesburg	("asn":"AS18474","name":"Dimension Data (Pty) Ltd - Optinet","domain":"optinet.net","route":"197.94.0.0/16","type":"isp")	("name":"Dimension Data (Pty) Ltd - Optinet","domain":"optinet.net","type":"isp")	("vpn":false,"proxy":false,"tor"
197.94.71.22	197-94-71-22.hff.mweb.co.za	Cape Town	Western Cape	ZA	-33.9258,18.4232	7945	Africa/Johannesburg	("asn":"AS18474","name":"Dimension Data (Pty) Ltd - Optinet","domain":"optinet.net","route":"197.94.0.0/16","type":"isp")	("name":"Dimension Data (Pty) Ltd - Optinet","domain":"optinet.net","type":"isp")	("vpn":false,"proxy":false,"tor"
197.94.71.227	197-94-71-227.hff.mweb.co.za	Cape Town	Western Cape	ZA	-33.9258,18.4232	7945	Africa/Johannesburg	("asn":"AS18474","name":"Dimension Data (Pty) Ltd - Optinet","domain":"optinet.net","route":"197.94.0.0/16","type":"isp")	("name":"Dimension Data (Pty) Ltd - Optinet","domain":"optinet.net","type":"isp")	("vpn":false,"proxy":false,"tor"
197.94.71.226	197-94-71-226.hff.mweb.co.za	Cape Town	Western Cape	ZA	-33.9258,18.4232	7945	Africa/Johannesburg	("asn":"AS18474","name":"Dimension Data (Pty) Ltd - Optinet","domain":"optinet.net","route":"197.94.0.0/16","type":"isp")	("name":"Dimension Data (Pty) Ltd - Optinet","domain":"optinet.net","type":"isp")	("vpn":false,"proxy":false,"tor"
197.94.71.225	197-94-71-225.hff.mweb.co.za	Cape Town	Western Cape	ZA	-33.9258,18.4232	7945	Africa/Johannesburg	("asn":"AS18474","name":"Dimension Data (Pty) Ltd - Optinet","domain":"optinet.net","route":"197.94.0.0/16","type":"isp")	("name":"Dimension Data (Pty) Ltd - Optinet","domain":"optinet.net","type":"isp")	("vpn":false,"proxy":false,"tor"
197.94.71.221	197-94-71-221.hff.mweb.co.za	Cape Town	Western Cape	ZA	-33.9258,18.4232	7945	Africa/Johannesburg	("asn":"AS18474","name":"Dimension Data (Pty) Ltd - Optinet","domain":"optinet.net","route":"197.94.0.0/16","type":"isp")	("name":"Dimension Data (Pty) Ltd - Optinet","domain":"optinet.net","type":"isp")	("vpn":false,"proxy":false,"tor"

## IPINFO BASIC



The screenshot displays the IPInfo web application interface. At the top, there's a navigation bar with 'splunk' and 'App: IPInfo'. Below this is a search bar containing '139.130.188.239'. The main content area shows the IP address '139.130.188.239' and the hostname 'zet1364080.lnk.telstra.net'. Below these, it lists 'Clarkson' as the City, 'Western Australia' as the Region, 'AU' as the Country, and '6030' as the Postal code. A world map is shown with a blue dot indicating the location in Australia. At the bottom, there are three sections: 'ASN', 'COMPANY', and 'CARRIER', each with a placeholder image and a blue 'UPGRADE' button.

IP Address	Hostname
139.130.188.239	zet1364080.lnk.telstra.net

City	Region	Country	Postal
Clarkson	Western Australia	AU	6030

World Map showing location in Australia

ASN	COMPANY	CARRIER
Full company details are displayed here when you're subscribed to the pro plan.	Full company details are displayed here when you're subscribed to the pro plan.	Full company details are displayed here when you're subscribed to the pro plan.

[About](#) [Support](#) [File a Bug](#) [Documentation](#) [Privacy Policy](#)

[About](#) [Support](#) [File a Bug](#) [Documentation](#) [Privacy Policy](#)

## IPINFO PRO (NO CARRIER)

**splunk>** App IPInfo ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

---

IPInfo Search

---

IPInfo Edit Export ▾ ...

139.130.188.239 Hide Filters

<b>139.130.188.239</b>		<b>zet1364080.lnk.telstra.net</b>	
IP Address		Hostname	

<b>Clarkson</b>	<b>Western Australia</b>	<b>AU</b>	<b>6030</b>
City	Region	Country	Postal

ASN		COMPANY		CARRIER	
Key ▾	Value ▾	Key ▾	Value ▾	Key ▾	Value ▾
ASN	AS1221	NAME	Telstra Internet	NAME	N/A
NAME	Telstra Pty Ltd	DOMAIN	telstra.com.au	MCC	N/A
DOMAIN	telstra.net	TYPE	isp	MNC	N/A
ROUTE	139.130.0/16				
TYPE	isp				

About Support File a Bug Documentation Privacy Policy

© 2005-2018 Splunk Inc. All rights reserved.

## IPINFO PRO (WITH CARRIER)

splunk

App IPInfo

Messages

Settings

Activity

Help

Find

IPInfo

Search

ipinfo.io

Edit

Export

...

105.4.5.193

Hide Filters

105.4.5.193

IP Address

N/A

Hostname

Germiston

City

Gauteng

Region

ZA

Country

1401

Postal

ASN	COMPANY	CARRIER																												
<table> <tr> <th>Key</th> <th>Value</th> </tr> <tr> <td>ASN</td> <td>AS37158</td> </tr> <tr> <td>NAME</td> <td>Cell C (Pty) Ltd</td> </tr> <tr> <td>DOMAIN</td> <td>cellc.co.za</td> </tr> <tr> <td>ROUTE</td> <td>105.4.0.0/14</td> </tr> <tr> <td>TYPE</td> <td>isp</td> </tr> </table>	Key	Value	ASN	AS37158	NAME	Cell C (Pty) Ltd	DOMAIN	cellc.co.za	ROUTE	105.4.0.0/14	TYPE	isp	<table> <tr> <th>Key</th> <th>Value</th> </tr> <tr> <td>NAME</td> <td>NEOTEL GGSN2</td> </tr> <tr> <td>DOMAIN</td> <td>neotel.co.za</td> </tr> <tr> <td>TYPE</td> <td>isp</td> </tr> </table>	Key	Value	NAME	NEOTEL GGSN2	DOMAIN	neotel.co.za	TYPE	isp	<table> <tr> <th>Key</th> <th>Value</th> </tr> <tr> <td>NAME</td> <td>Cell C</td> </tr> <tr> <td>MCC</td> <td>655</td> </tr> <tr> <td>MNC</td> <td>7</td> </tr> </table>	Key	Value	NAME	Cell C	MCC	655	MNC	7
Key	Value																													
ASN	AS37158																													
NAME	Cell C (Pty) Ltd																													
DOMAIN	cellc.co.za																													
ROUTE	105.4.0.0/14																													
TYPE	isp																													
Key	Value																													
NAME	NEOTEL GGSN2																													
DOMAIN	neotel.co.za																													
TYPE	isp																													
Key	Value																													
NAME	Cell C																													
MCC	655																													
MNC	7																													

About

Support

File a Bug

Documentation

Privacy Policy

© 2005-2018 Splunk Inc. All rights reserved.



**splunk** App: IPInfo ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

---

IPInfo Search

105.4.5.193 Hide Filters

<b>105.4.5.193</b> <small>IP Address</small>		<b>N/A</b> <small>Hostname</small>	
<b>Germiston</b> <small>City</small>	<b>Gauteng</b> <small>Region</small>	<b>ZA</b> <small>Country</small>	<b>1401</b> <small>Postal</small>

A world map with a blue dot indicating the location of the IP address in South Africa.

ASN		COMPANY		CARRIER	
Key ▾	Value ▾	Key ▾	Value ▾	Key ▾	Value ▾
ASN	AS37168	NAME	NEOTEL GGSN2	NAME	Cell C
NAME	Cell C (Pty) Ltd	DOMAIN	neotel.co.za	MCC	655
DOMAIN	cellc.co.za	TYPE	isp	MNC	7
ROUTE	105.4.0.0/14				
TYPE	isp				

About Support File a Bug Documentation Privacy Policy

© 2005-2018 Splunk Inc. All rights reserved.

THANK YOU