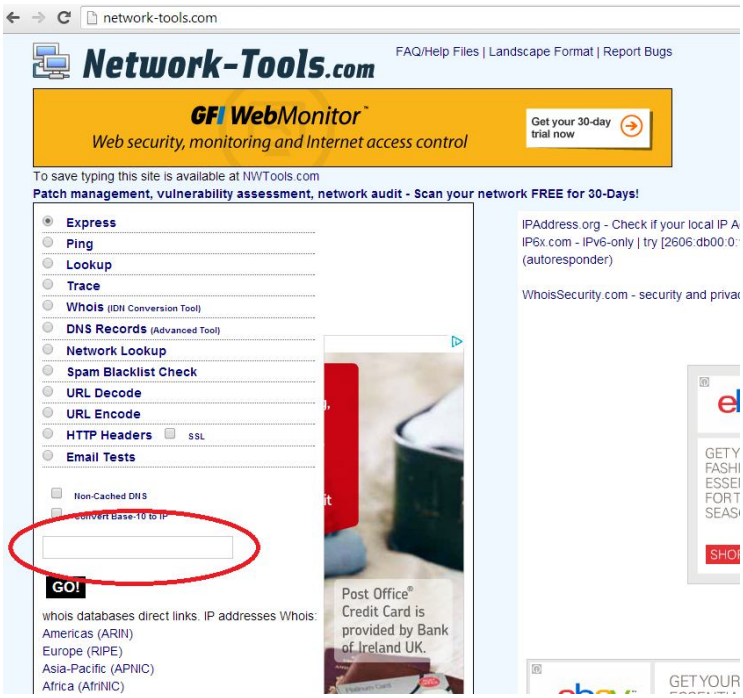
To find out all sorts of interesting things about a domain use the free tools at “network-tools.com”, enter the domain name in the search box on the right had side of the screen:



Then click “GO”, it will then display all the details about the domain. For our purpose we are only really interested in the first part, the ip address:

IPAddress.org - Check if your local IP Address can de detected | IPv6 connectivity tests: MyIP6.com - ipv6 or ipv4 |IP6x.com - IPv6-only | try [2606:db00:0:1::60] if your ipv6 DNS has no connectivity | Test ipv6 e-mail: test@ip6x.com(autoresponder)

WhoisSecurity.com - security and privacy of whois records | Privacy.net reviews the free KeePass password safe.

IP address: 198.38.82.127

Host name: aidpersonalinjury.com

Alias: aidpersonalinjury.com

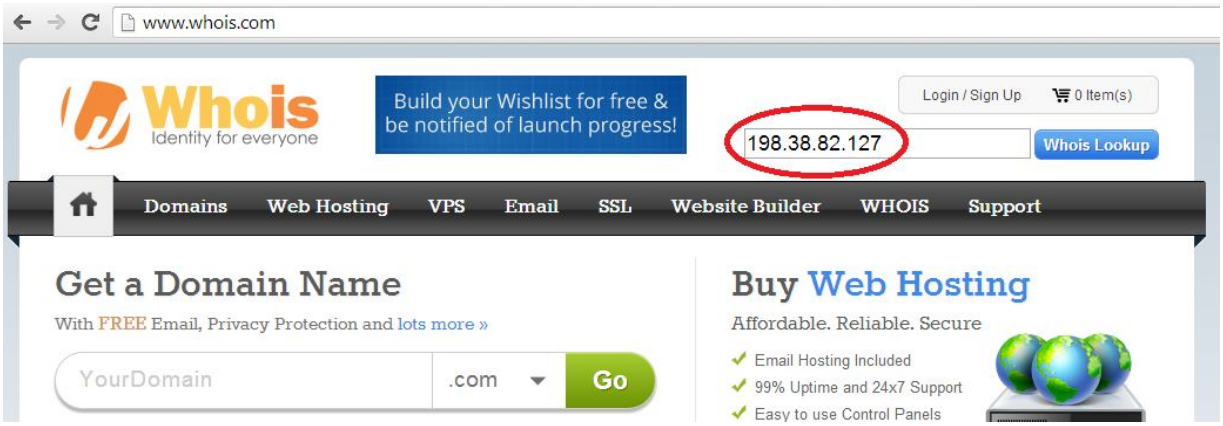
198.38.82.127 is from United States(US) in region North America

TraceRoute from Network-Tools.com to 198.38.82.127 [aidpersonalinjury.com]

Hop	(ms)	(ms)	(ms)	IP Address	Host name
1	1	0	0	206.123.64.46	-
2	0	0	0	64.124.196.225	xe-4-2-0.er2.dfw2.us.above.net
3	0	Timed out	2	206.223.118.61	equinix.tge9-3.ar1.dfw1.us.nlayer.net
4	1	3	1	69.31.63.184	ae1-70g.cr1.dfw1.us.nlayer.net
5	30	30	29	69.22.142.4	xe-0-2-1.cr1.ord1.us.nlayer.net
6	26	26	26	69.31.111.1	as23352.ae6-101.cr1.ord1.us.nlayer.net
7	27	26	26	204.93.204.73	ae11.cr1.ord6.us.scnet.net
8	26	27	62	204.93.204.53	ae3.ar8.ord6.us.scnet.net
9	26	26	26	204.93.205.62	as65401.ae2.ar8.ord6.us.scnet.net
10	27	27	27	198.38.82.127	mocha3011.mochahost.com

Trace complete

The IP address will tell us who and where the site is hosted, we can use the “whois” service to provide the details of where the site is hosted by supplying the ip address from above:



If you entered the name of the spam domain then it would only tell you the details about that domain, not who hosts it, just who registered it and you want to know who hosts it.

In our example, the details are:

Whois IP 198.38.82.127

Updated 46 minutes ago

```
#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/whois tou.html
#


#
# The following results may also be obtained via:
#
http://whois.arin.net/rest/nets;q=198.38.82.127?showDetails=true&showARIN=false&ext=netre
f2
#

NetRange:       198.38.80.0 - 198.38.95.255
CIDR:           198.38.80.0/20
OriginAS:       AS23352
NetName:        MOCAH-1
NetHandle:      NET-198-38-80-0-1
Parent:         NET-198-0-0-0-0
NetType:        Direct Allocation
RegDate:        2012-04-20
Updated:        2012-04-20
Ref:            http://whois.arin.net/rest/net/NET-198-38-80-0-1

OrgName:        Mochahost.com
OrgId:          ML-17
Address:        2880 Zanker Rd #203
City:           San Jose
StateProv:      CA
PostalCode:     95134
Country:        US
RegDate:        2011-05-25
Updated:        2013-07-03
Ref:            http://whois.arin.net/rest/org/ML-17
```

```
OrgTechHandle: MLADM-ARIN
OrgTechName:   ML-ADMIN
OrgTechPhone:  +1-408-351-0116
OrgTechEmail:  daves@mochahost.com
OrgTechRef:    http://whois.arin.net/rest/poc/MLADM-ARIN

OrgAbuseHandle: MLABU-ARIN
OrgAbuseName:   ML-ABUSE
OrgAbusePhone:  +1-408-351-0116
OrgAbuseEmail:  abuse@mochahost.com
OrgAbuseRef:    http://whois.arin.net/rest/poc/MLABU-ARIN

OrgTechHandle: MDG35-ARIN
OrgTechName:   Gams, Matthew D.
OrgTechPhone:  +1-920-232-9914
OrgTechEmail:  matthew.gams@xipher.net
OrgTechRef:    http://whois.arin.net/rest/poc/MDG35-ARIN


#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/whois_tou.html
#
```

What we are interested in is the "OrgAbuseEmail" field, in this case its abuse@mochahost.com, once you have that you can send them an email with the details of the spam that you received or the other contact method. For spam texts I use the following format to the emails that I send, quoting what the law states:

I received a text today which stated:

"£3154.31 is here waiting in your name, its compensation for the accident you had, for us to sent it out ASAP just fill out the form http://aidpersonalinjury.com"

Looking at the domain details the address resolves to:

```
IP address: 198.38.82.127
Host name: aidpersonalinjury.com
Alias: aidpersonalinjury.com
```

Which according to whois, is one of your ips:

Whois IP 198.38.82.127 Updated 1 second a

```
#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/whois_tou.html
#


#
# The following results may also be obtained via:
#
http://whois.arin.net/rest/nets;q=198.38.82.127?showDetails=true&showARIN=false&ext=netref2
#

NetRange:       198.38.80.0 - 198.38.95.255
CIDR:           198.38.80.0/20
OriginAS:       AS23352
```

```
NetName:        MOCAH-1
NetHandle:      NET-198-38-80-0-1
Parent:         NET-198-0-0-0-0
NetType:        Direct Allocation
RegDate:        2012-04-20
Updated:        2012-04-20
Ref:            http://whois.arin.net/rest/net/NET-198-38-80-0-1

OrgName:        Mochahost.com
OrgId:          ML-17
Address:        2880 Zanker Rd #203
City:           San Jose
StateProv:      CA
PostalCode:     95134
Country:        US
RegDate:        2011-05-25
Updated:        2013-07-03
Ref:            http://whois.arin.net/rest/org/ML-17
```

These types of text are illegal under UK law as can be seen from the communication officers website:

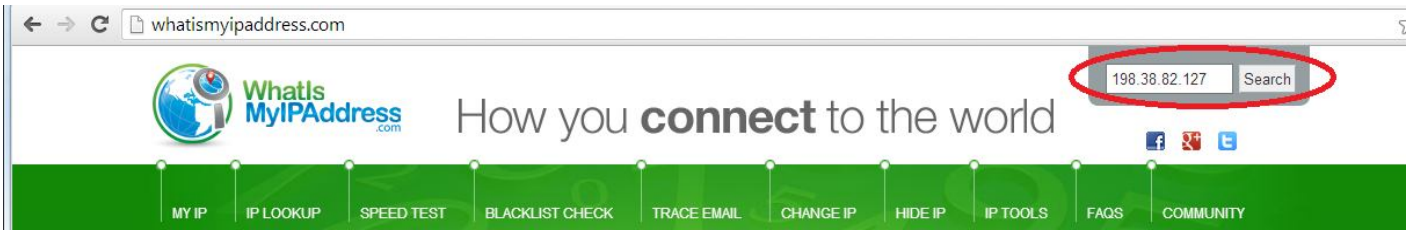
> ***What does the law say?***
> *The Privacy and Electronic Communications Regulations 2003 cover the way organisations send direct marketing by electronic means, including by text message (SMS).*
>
> *Organisations cannot send you marketing text messages you didn't agree to receive, unless:*
>
> - *the sender has obtained your details through a sale or negotiations for a sale;*
> - *the messages are about similar products or services offered by the sender; and*
> - *you were given an opportunity to refuse the texts when your details were collected and, if you did not refuse, you were given a simple way to opt out in all the text messages you received.*
> - *The Regulations do not cover marketing text messages sent to business numbers.*
>
> ***Are these messages illegal?***
> *The messages appear to breach the Privacy and Electronic Communications Regulations because they are being sent to individuals without prior consent and without identifying the sender. The messages also appear to breach other legislation and codes of practice.*

Looking at the website and had other similar texts and websites in the past they are people that collect peoples details and sell them to other oganisations, they gather these details as can be seen through texts that lie. Can you tell me what your policy is regarding these types of site and could you also provide me the company name of the person who owns the site so I can report them in the UK. They are using a whois privacy organisation so I cannot view the details, probably because they know that what they are doing is illegal.

Normally most ISPs are quite good and will do something about it, if not then just keep at it. In the past with smaller ISPs I have found that if you use the method above but to work out who their hosting company is and send the emails to them they tend to notice as the larger ISPs want to stop spam as much as we want spam stopped.

Also when contacting the ISPs don't be too nasty with your email, they don't know what their clients are up to and in some cases the ISP has acting on behalf of another ISP so it could be something they can't resolve initially, however they do tend to be helpful and will let you know who to contact.

Another useful site is whatismyipaddress.com, enter the ip address in the search field in the top right:



What is neat about this site as it will show you roughly where in the world the ip is hosted:

IP Details for 198.38.82.127

This information should not be used for emergency purposes, trying to find someone's exact physical address, or other purposes that would require 100% accuracy. Please read about geolocation accuracy for more information.

198.38.82.127 Lookup IP Address

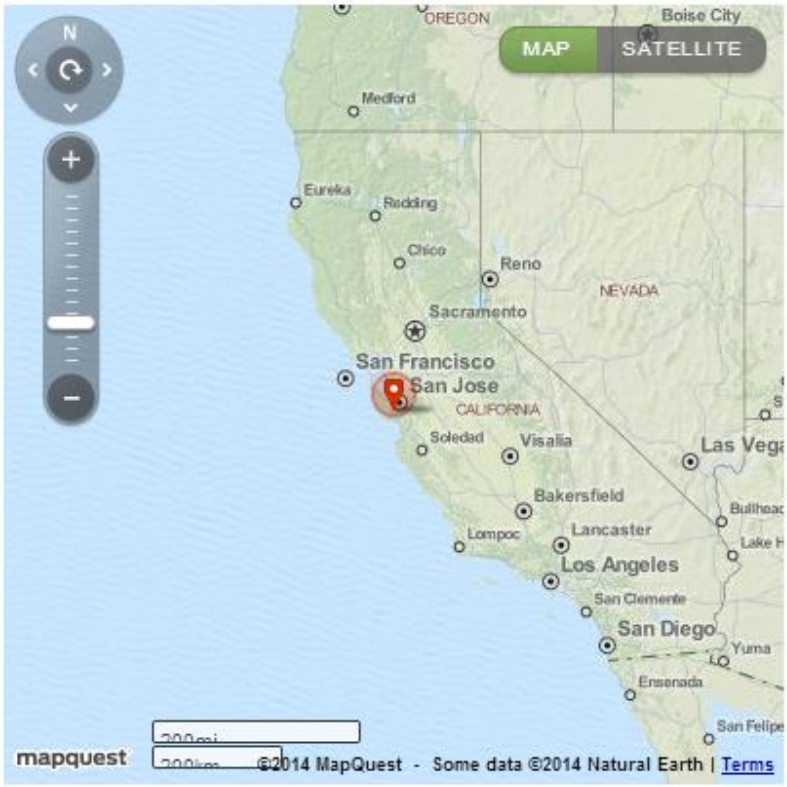
General IP Information

IP: 198.38.82.127
Decimal: 3324400255
Hostname: mocha3011.mochahost.com
ISP: Mochahost.com
Organization: Mochahost.com
Services: None detected
Type: Corporate
Assignment: Static IP
Blacklist: Blacklist Check

Geolocation Information

Country: United States
State/Region: California
City: San Jose
Latitude: 37.425 (37° 25′ 30.00″ N)
Longitude: -121.946 (121° 56′ 45.60″ W)
Area Code: 408
Postal Code: 95134

Geolocation Map



Neat hey?