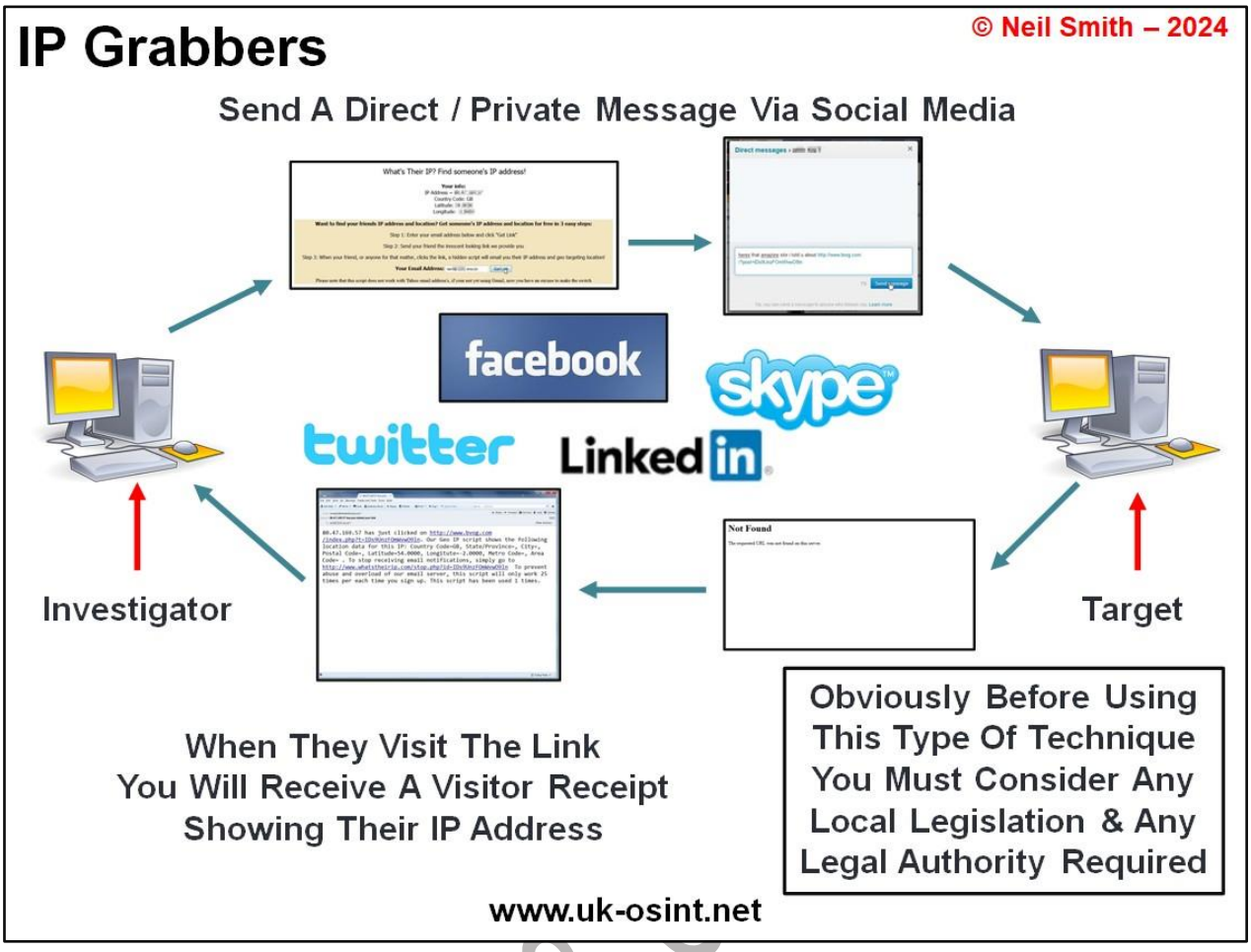


Sometimes as well as not having an Originating IP Address to investigate or research, you may also now have an email address either, so you can't send a Covert Tracking Email either.

However at times like these you may consider using an IP Grabber to get the IP Address of someone on-line, such as those on Facebook, Twitter or Skype etc.

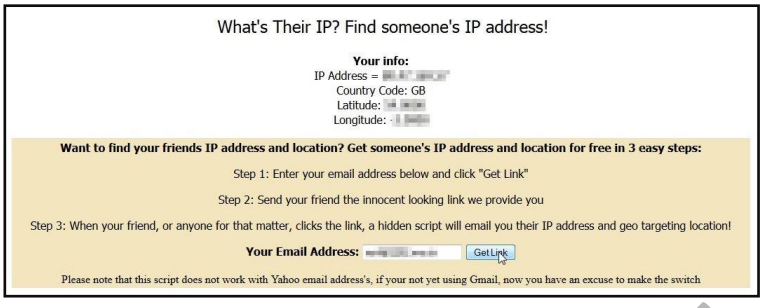
This may help locate the individual behind an online account but clearly may require some level of authorisation to use if you are within law enforcement.

There are a number of different IP Grabbers linked on the IP Grabbers page of our website at https://www.uk-osint.net/ipgrabbers.html.

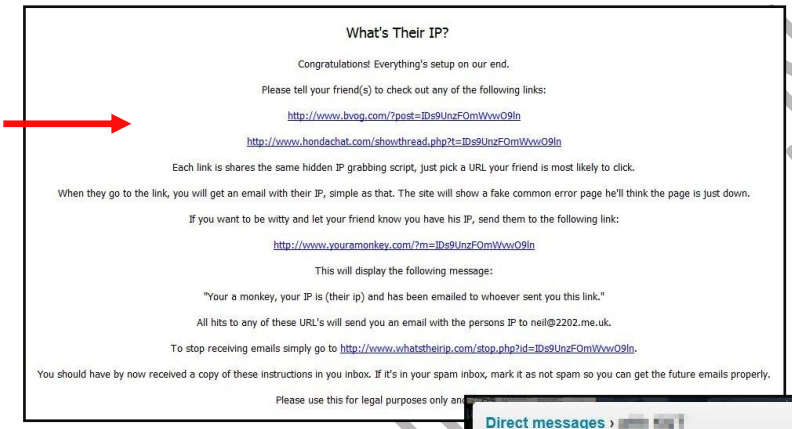
When you have identified an online account, such as with Facebook, Twitter or Skype etc., that you are interested in and when you have already engaged with that subject online, then you can send them a private message, which only they will see, with a link from an IP Grabber to get their IP Address if they visit the link.

So send a Private or Direct Message on Facebook & Twitter or a Text Message on Skype, as it must not be an open message which anyone else can see.

The following is an example of using an old, no longer available IP Grabber, to obtain and use a tracking link, is similar to how many of the other current online systems operate.

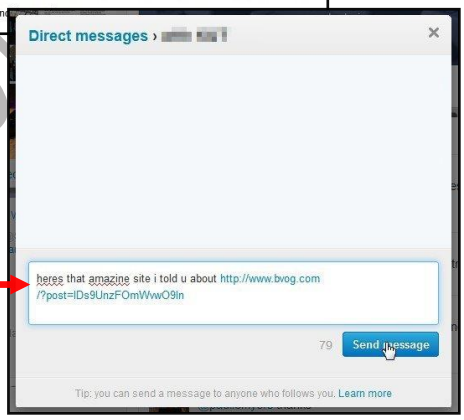


You can use a new email address to sign up and get the tracking link, picking one of the more covert tracking links, which directs the subject to an error page as opposed to a page saying that their IP Address has been logged.

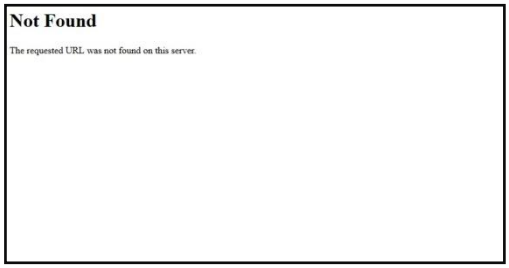


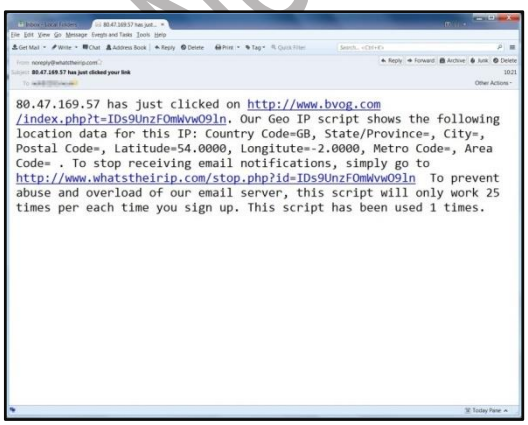
Now send this link in a message to the subject, either via a Private or Direct Message on Facebook & Twitter or a Text Message on Skype.

Make the message enticing by building up a relationship with the subject first, rather than arriving unexpected & looking like a spam message.



Then as soon as the subject clicks on the link and visits the page, which shouldn't necessarily raise any suspicion if done properly, you will then receive an email





with the IP Address of the subject who visited the page via the link. This IP Address can then be turned around in the same method as for "Covert Email Tracking".

Whilst all of these techniques work in theory, be they Tracing Email Headers, Covert Tracking Emails or IP Grabbers, obviously people can take steps to avoid detection by using a VPN / Proxy / Anonymiser, however;

- Whilst you can make changes to your settings to try to hide your actual IP Address, many people don't know how to and many just don't bother, just think of how easy most scam / spam emails are to trace

- Even if someone does know how to hide their actual IP Address, some email services don't let you sign on using a VPN / Proxy / Anonymiser and some that do are able to still identify your actual IP Address - try using a VPN / Proxy / Anonymiser and then visit https://ipleak.net/ to see your actual IP Address

- Whilst some email providers strip-out your originating IP Address from emails sent via their main website, some of these services keep in the originating IP Address when accessed via their app from a smartphone or tablet

- Sometimes people take precautions against giving their IP Address away as a Footprint whilst using their computer but will check their emails on their smartphone first, over which they may have less control

Think of these tools and techniques are a bit like taking fingerprints at a crime scene.

The police have been taking fingerprints at scenes of crime for over 100 years, so if there is a burglary you would expect the police to check for fingerprints, even though the burglar could easily have just worn gloves to avoid detection; but still every year many burglars are convicted because they left their fingerprints at a crime scene.

So these techniques can and do work but just not every time.