DARTFORD BOROUGH COUNCIL - POLICY FOR INTERROGATING SOCIAL MEDIA FOR INVESTIGATIVE PURPOSES

1. INTRODUCTION

- 1.1 Open-source Intelligence or OSINT refers to a broad array of information and sources that are generally available (whether on payment or otherwise), including information obtained from internet (social networking) sites, books, media, newspapers, radio, television, journals, TV, newswires, newsgroups, mapping, imagery photographs, commercial subscription databases and other library data.
- 1.2 Social networking sites and OSINT contain a wealth of information, intelligence and evidence about suspects, victims, witnesses, members of organised crime groups and other aspects of criminal and anti-social activity.
- 1.3 Social networking Twitter, Facebook and LinkedIn to name but a few have opened up numerous opportunities and is a key component to profiling the subject of an investigation. The pool of information (postings, videos, photos etc.) about each individual can form a distinctive social signature.
- 1.4 Social networking evidence can be a valuable addition to an investigation, but it has to be gathered in a way that will hold up in court. Once the access to social networking information has been secured, simply due to public accessibility, evidence must be gathered in a way that is legal and useful. Collecting evidence from social networking sites has the potential to impact on individual's rights to privacy and may therefore require authorisation under the Regulation of Investigatory Powers Act 2000 (see section 3 below).
- 1.5 This Policy sets the framework by which officers may utilise OSINT, social media and video sharing sites when conducting investigations into alleged offences and aims to ensure the minimum standards that must be adopted by all officers in order to maintain the integrity of any evidence gained so as not to compromise:
 - the hardware/software infrastructure of the Council's computer systems;
 - investigative tactics;
 - on-going and future Council investigations;
 - the personal safety of individuals; and
 - reputational risks to the Council;
 - breach of RIPA reportable to IPCO¹ and possible disciplinary issues.

This Policy also ensures that investigations are done lawfully and correctly so as not to interfere with an individual's human rights and with due consideration of relevant legislation, including:

the Human Rights Act 1998;
the Data Protection Legislation ²
Computer Misuse Act 1990

¹ Investigatory Powers Commissioner's Office

²Data Protection Act 2018 and UK GDPR (derived from the General Data Protection Regulation (EU) 2016/679)

 the Regulation of Investigatory Powers Act 2000, together with the published codes of practice from the Home Office, IPCO and the Information Commissioner's Office; Chapter 30 of the Criminal Procedure and Investigations Act 1996 (Section 23(1)) Code of Practice); PACE 1984 Protection of Freedoms Act 2012 – regulation of CCTV and other surveillance camera technology & Surveillance Camera Commissioner + Codes of Practice.
1.6 This Policy should be read in conjunction with the Council's Policy Statement - Regulation of Investigatory Powers Act 2000 (RIPA) (as amended). Remember to complete the 'Application for authorisation to conduct an OVERT investigation' (on the intranet).
2. WHAT IS MEANT BY 'SOCIAL MEDIA'
2.1 Social media can take many forms. However, there are some facets, which will be common to all forms of social media.
Social media will always be a web-based service that allows individuals and/or businesses to construct a public or semi-public profile. Beyond this, social media can be very diverse, but will often have some, or all, of the following characteristics;
 the ability to show a list of other users with whom they share a connection; often termed "friends" or "followers", the ability to view and browse lists of connections and those made by others within the system; hosting capabilities allowing users to post audio, photographs and/or video content that is viewable by others.
2.2 Social media can include community based web sites (see Appendix 6 – Social Networking Sites), online discussions forums, chatrooms and other online social spaces. Current examples of the most popular forms of social media and therefore the most likely to be of use when conducting investigations into alleged offences, include;
 □ Facebook □ Twitter □ YouTube □ Vine □ Instagram □ LinkedIn □ Pinterest □ Google+ □ TumbIr □ Reddit □ Flickr
2.3 Social media interrogations involve the detailed analysis of an organisation's or

- individual's social media accounts. They are commonly used to provide information relevant to an investigation, court case or background checks.
- Interrogations can be critical in providing admissible evidence in civil and criminal matters, pre-employee screenings or internal investigations involving current or former

employees. This can be due to the need to ascertain specific evidence in relation to potentially fraudulent activity, data theft, gross misconduct, identifying those responsible for environmentally damaging fly-tipping, benefit fraud, or selling alcohol or tobacco to minors.

- 2.5 By its very nature, social media accumulates a sizable amount of information about a person's life, from daily routines to specific events. Accessibility on mobile devices can also mean that a person's precise location at a given time, may also be recorded whenever they interact with a form of social media on their devices.
- 2.6 Although social media is a useful tool when investigating alleged offences with a view to bringing a prosecution, there is a danger that its use can be abused, which would have an adverse effect, damaging potential prosecutions and even leave the Council open to complaints or criminal charges itself.

3. HUMAN RIGHTS & REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

- 3.1 Whilst the use of social media to investigate is not automatically considered covert surveillance, its misuse when conducting investigations can mean that it crosses over into the realms of covert and/or targeted surveillance, even when that misuse is inadvertent, therefore becoming unauthorised surveillance and breaching a person's right to privacy under Article 8 of the European Convention on Human Rights.
- 3.2 There is a significant amount of information on an individual's social media pages. This information might be relevant to an investigation being undertaken by the Council. However, unguided research into the sites of suspect offenders could fall within the remit of RIPA and therefore require a *directed surveillance authorisation*, prior to the undertaking of an investigation. See the RIPA (Regulation of Investigatory Powers) Policy Statement.
- 3.3 Where a website or social media account requires a minimal level of interaction, such as sending or receiving a friend request before access is permitted, this may not in itself amount to establishing a relationship. Equally, the use of electronic gestures such as "like" or "follow" to react to information posted by others online would not in itself constitute forming a relationship. However, it should be borne in mind that entering a social media site or responding on these terms, may lead to further interaction with other users and a *CHIS authorisation* should be obtained if it is intended for an officer or a CHIS to engage in such interaction to obtain, provide access to or disclose information³, without disclosing their identity.
- 3.4 Officers embarking on any form of investigatory action should always do so with RIPA in mind. Whilst RIPA will not always be relevant to every investigation, it is vital that officers involved in investigative practices regularly review their conduct with respect to investigatory actions. Any investigation is capable of evolving from being one that does not require a RIPA authorisation, to one that does, at any point. Instances of repeated and/or regular monitoring of social media accounts, as opposed to one-off viewing, may require a RIPA authorisation.

Intelligence provides a link to evidence. Evidence of whatever type must be both relevant and admissible. Evidence is relevant if it logically goes to proving or disproving some fact at issue in the prosecution. It is admissible if it relates to the facts

³ Refer to paragraphs 4.29 to 4.35 of the <u>Covert Human Intelligence Sources Code of practice</u> (December 2022) for details on where a CHIS authorisation may be available for online activity, including the need to carry out a risk assessment RIPA/Policy For Interrogating Social Media For Investigative Purposes 7 March 2023

in issue, or to circumstances that make those facts probable or improbable and has been properly obtained.

- 3.5 Even if surveillance without a RIPA authorisation is not illegal, if a RIPA authorisation is not obtained, the surveillance carried out will not have the protection that RIPA affords and may mean it is rendered inadmissible.
- 3.6 If reasonable steps have been taken to inform the public or particular individuals that their social media account(s) is being monitored, this can be regarded as **OVERT** and a directed surveillance authorisation will not normally be required. **Officers must at all times use their department's allocated social media account** (see section 12 below).

4. PRIVACY SETTINGS & PRIVATE INFORMATION

4.1 **Expectation of privacy** is a key issue and must be given proper consideration. A decision will hinge on whether the users of the particular site have a reasonable expectation of it. Users normally have the choice whether to make their profile and associated postings/blogs available for public view or to restrict access to 'friends' only. Many users may assume that the 'default' settings deliver reasonable privacy, so may not specifically set their requirement, but still 'expect' privacy of access to their content. Similarly, 'friends' variations on settings can impact on others' privacy. Much depends on the way the hosting site is programmed (or on original philosophy of the provider).

It is therefore recognised that the account 'settings' may not always fully reflect the end-users expectation of privacy. It is however reasonable to conclude that postings on 'walls' or 'blogs' on a social networking site to which the author has applied no privacy settings to, are likely to be considered to be within the public domain (see section 4.2. below).

4.2 **Private Information** - when a person's activities take place in public, covert surveillance of that person's activities in public may still result in the obtaining of private information. This is likely to be the case where that person has a reasonable expectation of privacy, even though acting in public and where a record is being made by a public authority of that person's activities for future consideration or analysis.

These considerations are also likely to arise if several records relating to one subject are to be analysed together in order to establish, for example, a pattern of behaviour, lifestyle etc., or if one or more pieces of information (whether or not in the public domain) are covertly obtained for purposes of making a permanent record on that person or for subsequent data processing to generate further information. In such circumstances, the totality of information gleaned may constitute private information even if individual records do not.

- 4.3 It does not always follow that users who do not restrict access have totally forfeited their right to privacy or that covert research of their profiles could not amount to directed surveillance. Where means of restricting access to the information have been put in place, the author has a clear expectation of privacy and so the use of measures to circumvent access controls is capable of amounting to surveillance and may require authority under RIPA.
- 4.4 Depending on the nature of the online platform, there may be a reduced expectation of privacy where information relating to a person or group of people is made openly available within the public domain (see Appendix 1 Is the information on Facebook private or public?).

- 4.5 Where information about an individual is placed on a publicly accessible database, for example the telephone directory or Companies House, which is commonly used and known to be accessible to all, individuals are unlikely to have any reasonable expectation of privacy over the monitoring by public authorities of that information.
- 4.6 Individuals who post information on social media networks and other websites whose purpose is to communicate messages to a wide audience are also less likely to hold a reasonable expectation of privacy in relation to that information.
- 4.7 Where privacy settings are available, but not applied, the data may be considered 'open source' or publicly available (i.e. there is a reduced expectation of privacy).

Example: Where a person publishes content on a public profile, they allow everyone, including those not on that particular social media platform, to access and use that information whilst also allowing it to be associated with them. In practice, this means that photographs, video content or any other relevant information posted by individuals and businesses to a public profile on any given social media platform can be viewed, recorded and ultimately used as evidence against them should the matter end in legal proceedings, subject to the usual rules of evidence.

- 4.8 Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person's activities in public may still result in the obtaining of private information. This is likely to be the case where that person has a reasonable expectation of privacy even though acting in public and where a record is being made by the Council of that person's activities for future consideration or analysis. Surveillance of publicly accessible areas of the internet should be treated in a similar way, recognising that there may be an expectation of privacy over information, which is on the internet, particularly where accessing information on social media websites. This is because the intention when making such information available was not for it to be used for a covert purpose such as investigative activity. This is regardless of whether a user of a website or social media platform has sought to protect such information by restricting its access by activating privacy settings.
- 4.9 Whether the Council interferes with a person's private life includes a consideration of the nature of the Council's activity in relation to that information. Simple *reconnaissance* of such sites (i.e. preliminary examination with a view to establishing whether the site or its contents are of interest) is unlikely to interfere with a person's reasonably held expectation of privacy and therefore is not likely to require a directed surveillance authorisation.

General observation duties do not require a RIPA authorisation, whether covert or overt. Such general observation duties frequently form part of the Council's legislative functions, as opposed to the pre-planned surveillance of a specific person or group of people. General observation duties may include monitoring of publicly accessible areas of the internet in circumstances where it is not part of a specific investigation or operation.

However, where officers are systematically collecting and recording information about a particular person or group, a directed surveillance RIPA authorisation should be considered. These considerations apply regardless of when the information was shared online.

Example: Council officers monitoring publicly accessible information on social media websites, using a general search term (such as the name of a particular event they are monitoring), would not normally require a directed surveillance authorisation. However, if they were seeking information relating to a particular individual or group of individuals, for example, by using the search term "group x" (even where the true

identity of those individuals is not known) this may require authorisation. This is because use of such a specific search term indicates that the information is being gathered as part of a specific investigation or operation, particularly in circumstances where information is recorded and stored for future use.

Personal information obtained through general observation, is subject to the Data Protection Legislation.

- 4.10 Officers must ensure compliance with the Data Protection Act 2018 principles and UK GDPR. The social media interrogation must be legitimate under the Data Protection Legislation. This means it must be reasonable, lawful and appropriate. Obtaining information for one purpose, cannot later be used for a completely different purpose. Check whether the way the planned interrogation of social media provides a 'lawful basis' for processing data under the UK GDPR. If sensitive (i.e. 'special category') data is likely to be collected this means extra conditions must be met under the UK GDPR see the Analysis of Social Media for Investigations Privacy Notice. A Data Protection Impact Assessment (DPIA) must be carried out with reference to the lawful bases and legal gateways (see section 10 below).
- 4.11 Where officers intend to access a social media or other online account to which they have been given access with the consent of the owner, they will still need to consider whether the account(s) may contain information about others who have not given their consent. If there is a likelihood of obtaining private information about others, the need for a directed surveillance authorisation should be considered, particularly (though not exclusively), where it is intended to monitor the account going forward.
- 4.12 When considering what is available on an individual's public social media profile, officers investigating an offence, or potential offence, should always keep in mind what relevance it has to that investigation. Only information that is relevant to the investigation and goes some way toward proving the offence, should be gathered. If there is any doubt as to whether something is relevant, then advice should be sought from Legal Services.

5. CONDUCTING INVESTIGATIONS/RESEARCH OVER THE INTERNET

- 5.1 Internet Service Providers maintain a record of IP addresses and the sites visited. Websites may record IP addresses as well as other details about the computer used including the browser, operating system, and computer name. Records are often kept of the time and date of each visit in addition to the sites the visitor came from and went to. Websites can install cookies on to a computer in order to identify the user, should they return to that site, or another site that subscribes to the same cookie monitoring service.
- 5.2 Any activity carried out over the internet leaves a trace or footprint that can identify the device used and, in some instances, the individual carrying out that activity. Officers engaged in investigation and/or research over the internet must take precautions to protect the security of themselves and of the Council's computer systems.
- 5.3 Only Level 1 Overt Open Source Intelligence/Research and Level 2 Advanced Open Source Investigation/Research (see the levels below) should be carried out on devices that are attributable to the Council. For any other type of covert investigation/research, where the investigator would not wish those being investigated to be aware of the investigation or of Council interest, equipment must be used which cannot be attributed to the Council or any individual member of staff.

A computer or laptop cannot be made totally 'non-attributable', as there is a risk of detection through connection to the IP address. However, the use of a Council allocated iPad or similar device, connected to its mobile network (not to wifi), would be 'non-attributable'.

A non-Council identity (email address), would need to be used on the 'non-attributable' device - an email address that identifies (or risks identifying) the user should not be used – instead, use a random email address e.g. golden.sunsets@gmail.com.

Non-attributable devices must never be used for personal use.

5.4 Departments must ensure that a 'non-attributable' device is kept in a secure environment and that there are strict procedures in place to regulate and audit its use. Records must be kept of sites visited and information gathered in a locally held log/register. The criteria detailed in the following levels should be seen as a minimum requirement to carry out operational activity on the internet.

If the iPad is a 10.1-inch model or smaller, a free version of MS Word can be used to store and maintain documents on the iPad.

5.5 Staff carrying out any type of investigation/research over the internet must be appropriately trained (see section 11 below).

Level 1 - Overt Open Source Investigation/Research

- conducting research overtly across publicly accessible search areas of the internet such
 as map viewing, street views, local authority sites, auction sites or any publicly available
 website in cases where there is no requirement to register details to gain access;
- must not be used for any covert investigation;
- as the research activity is considered overt, there is no requirement for any RIPA authorisation;
- no senior officer advance authorisation required but officers must adhere to relevant Council Data Protection Legislation policies/procedures and IT Security Policy;
- must be conducted on Council computers.

Level 2 – Overt Advanced Open Source Investigation/Research

- research across publicly accessible search areas of the internet, such as search engines, people search sites and social network sites;
- registration required to gain access;
- the research is not intended to remain covert and may become known to the subject;
- no senior officer advance authorisation required, unless convert surveillance is intended;
- active consideration should be given to a RIPA authorisation on a case-by-case basis;
- sterile profile accounts [a profile in the true name of the officer, but is not their active profile
 and is entirely sterile of their personal information] must be used to log onto sites requiring
 registration (see section 5.6 below);
- any interaction with the subject must not be covert and there must be no interaction with a subject beyond that which is entirely necessary for the immediate purposes. Be aware that befriending subjects, poking, writing on walls or joining groups is likely to require a RIPA directed surveillance authorisation) unless it is explicit that the profile is that of an officer:
- must be conducted using Council computers;

 must be able to evidentially capture and store information, as these records would need to be available for inspection/audit in any subsequent internal/external investigation.

Level 3 - Covert Advanced Open Source Investigation/Research

- research across publicly accessible search areas of the internet such as search engines, people search sites and social network sites requiring registration to gain access;
- research is intended to remain covert and is not intended to become known to the subject;
- RIPA authorisation procedure referred to in xxx MUST be followed;
- false persona profile accounts [a profile created in a false name to protect the officer's true identity becoming known to the subject] must be used to log onto sites requiring registration (see section 5.6 below);
- there must be no interaction with subjects no befriending subjects, writing on walls or joining discussions;
- must be able to evidentially capture and store, as these records would need to be available for inspection/audit in any subsequent internal/external investigation
- only non-attributable computers to be used.
- 5.6 **Sterile & /False Persona Profile Accounts** Under no circumstances will officers use their own personal or anyone else's social networking profile to conduct work related research, regardless of whether the investigation is of an overt or covert nature.
 - sterile profile accounts must be created with the true details of the officer making enquiries and must be registered using their Council email address;
 - false persona profile accounts must only be used for covert investigations and must be undertaken using a non-attributable computer.

No false persona account must be set up without prior authority, in consultation with the Data Protection Officer. If an officer needs to establish a false persona account on line account (for example an email address) that does not identify themselves as a Council employee, then this requires authorising by their senior manager. Authority need not be under RIPA unless the activity that is then undertaken is covert surveillance.

5.7 **Trawling** - Using the internet to research publicly available information is an important element of modern intelligence collection. Using key words to search information across the internet and in websites that have not been subject to any security controls or personal restrictions by the authors, can be effective at identifying emerging threats. Although the activity may be covert, this open trawling may not acquire private information and may not therefore require RIPA authorisation.

Continual and targeted examination of data in this way may increase the likelihood of private information being obtained from others and therefore, consideration should be given to obtaining a directed surveillance authorisation. Each case needs to be considered in isolation, as all social media sites are different. If no access controls are applied (i.e. open data for all to view), then there is no expectation of privacy. Therefore, a RIPA authorisation for directed surveillance would not necessarily be needed, if no access controls were in place. However, as indicated above, all sites are different and individual consideration should be given.

A false persona profile account may be required if a covert account is needed to search any sites. However, it would be unusual to need such a profile account, unless access controls were on a site.

5.8 Covertly Breaching Access Controls - Social media sites encourage members to establish in-built security controls to restrict the level of private information that is on display.

For example, Facebook provides security levels that a member can set to allow only accepted 'friends' to be able to view the private information of the member.

To gain access to this information covertly, an officer would need to use a false persona profile account to register with Facebook, create a profile and then send a request to the subject to become their friend. Therefore, if a subject's account access is restricted, which needs the officer to covertly breach those access controls, then a directed surveillance authorisation is required. This authorisation is sufficient so long as the intention of the officer is to only monitor the contents of the site that they have accessed.

For example, using Facebook, an officer 'bumps' to the subject with the hope that the subject accepts their request without any challenge or exchange on line. Once accepted (without challenge) the officer only remains inactive as a 'friend' on the subject's profile, which enables them to view the content of the site. This activity would be considered as covert and likely to obtain private information (as access to it is restricted). In this example, only a directed surveillance authorisation should be applied for. A false persona profile account would be required to log onto Facebook.

A CHIS authorisation may be required when using an internal trading organisation in circumstances when a covert relationship is likely to be formed. However, the use of disguised purchaser details in a single overt electronic purchase is not likely to require a CHIS authorisation because no relationship is usually established at this stage.

6. WHAT IS PERMITTED UNDER THIS POLICY

using different platforms to gather information that are publicly available (see section
9 below);
using information <i>posted on a public profile</i> without a RIPA authorisation;
using social media for surveillance with a RIPA authorisation, where the investigation
is unusual and/or is likely to capture confidential information and the risks to privacy
have been assessed as being proportionate and justified.

Officers must at all times prevent their own identities becoming compromised while doing their investigations or research.

7. WHAT IS NOT PERMITTED UNDER THIS POLICY?

Where an individual under investigation has set their social media account to private, s should not attempt to circumvent those settings under any circumstances. Such its would include, but are not limited to;
sending 'friend' or 'follow requests to the individual;
setting up or using bogus social media profiles in an attempt to gain access to the
individual's private profile (unless this has been authorised by a senior manager and supported by a RIPA authorisation);
contacting the individual through any form of instant messaging or chat function
requesting access or information;
asking family, friends, colleagues or any other third party to gain access on their behalf,
or otherwise using the social media accounts of such people to gain access;
covert monitoring through social media without a directed surveillance authorisation
(see section 3.2 above);
establishing a covert relationship through social media without a CHIS authorisation (see section 3.3 above); or
ISPE SECTION A A MOOVEL OF

any other method, which relies on the use of subterfuge or deception.

Officers should keep in mind that simply using profiles belonging to others, or indeed fake profiles, in order to carry out investigations does not provide them with any form of true anonymity. The location and identity of an officer carrying out a search can be easily traced through tracking of IP addresses and other electronic identifying markers.

- 7.2 Whilst one-off visits, or otherwise infrequent visits spread out over time, cannot be considered 'directed surveillance' for the purposes of RIPA, repeated or frequent visits may cross over into becoming 'directed surveillance' requiring RIPA authorisation. A person's social media profile should not, for example, be routinely monitored on a daily or weekly basis in search of updates, as this will require a RIPA authorisation, the absence of which is an offence.
- 7.3 Regardless of whether the social media profile belonging to a suspected offender is set to public or private, it should only ever be used for the purposes of evidence gathering. Interaction or conversation of any kind should be avoided at all costs, and at no stage should officers seek to make contact with the individual through the medium of social media. Any contact may lead to accusations of harassment or, where a level of deception is employed by Officers, entrapment, either of which would be detrimental and potentially fatal to any future prosecution.

8. CAPTURING EVIDENCE (MAINTAINING RECORDS) (see Appendix 2 – Evidence)

- 8.1 Once content available from an individual's social media profile has been identified as being relevant to the investigation being undertaken, it needs to be recorded and captured for the purposes of producing as evidence at any potential prosecution. Depending on the nature of the evidence, there are a number of ways in which this may be done:
- where evidence takes the form of a readable or otherwise observable content, such as text, status updates or photographs, it is acceptable for this to be copied directly from the site, or captured via a screenshot, onto a hard drive or some other form of storage device, and subsequently printed to a hard copy. The hard copy evidence should then be exhibited to a suitably prepared witness statement in the normal way;
- where evidence takes the form of audio or video content, then efforts should be made to download that content onto a hard drive or some other form of storage device such as a CD or DVD. Those CDs and/or DVDs should then be exhibited to a suitably prepared witness statement in the normal way. Any difficulties in downloading this kind of evidence should be brought to the attention of the IT Section who will be able to assist in capturing it.
- 8.2 When capturing evidence from an individual's public social media profile, steps should be taken to ensure that all relevant aspects of that evidence are recorded effectively. For example, when taking a screenshot of a person's social media profile, officers should make sure that the time and date are visible on the screenshot in order to prove when the evidence was captured. Likewise, if the evidence being captured is a specific status update or post published on the suspected offender's profile, steps should be taken to make a screenshot. Without this information, the effectiveness of the evidence is potentially lost as it may not be admissible in court.
- 8.3 Due to the nature of social media, there is a significant risk of collateral damage in the form of other, innocent parties' information being inadvertently captured alongside that of the suspected offender's. When capturing evidence from a social media profile, steps should be taken to minimise this collateral damage, either before capturing the evidence, or RIPA/Policy For Interrogating Social Media For Investigative Purposes 7 March 2023

subsequently through redaction. This might be particularly prevalent on social media profiles promoting certain events, where users are encouraged to interact with each other by posting messages or on photographs where other users may be making comments.

8.4 Officers will have regard to Chapter 30 of the Criminal Procedure and Investigations Act 1996 (Section 23(1)) Code of Practice, with regard to the manner in which they record, retain and reveal to the prosecutor, material obtained in a criminal investigation and which may be relevant to the investigation and related matters.

Where recorded material (in any form or media) is obtained during the course of an investigation which might be relevant to an investigation, or another investigation, or to pending or future civil or criminal proceedings, then it should not be destroyed, but retained in accordance with the requirements of the Council's Data Retention & Disposal Policy & Schedule and the Criminal Procedures and Investigations Act 1996 (i.e. consider using the evidence obtained in a sensitive unused material schedule⁴) and any other legal requirements.

- 9. OTHER INFORMATION TECHNOLOGY TOOLS AVAILABLE FOR INVESTIGATIVE PURPOSES (see Appendix 3 Internet Research Websites, Appendix 4 Search Engines, Appendix 5 Search Engines Tutorial and Appendix 7 Images Videos GPS)
- 9.1 Whilst social media can be a useful and fruitful means of investigating offences and potential offences, it is by no means the only tool available within the realm of Information Technology. A vast array of other, mostly web-based tools are also at the disposal of those conducting investigations. For example, where there is a website advertising the services of a local business and there is evidence that this business is engaging in illegal activity, there are IT tools available that can track who is responsible for setting up that website, and so can be a good starting point when trying to link potential offenders to the offending business.
- 9.2 There are a series of specialist search tools available, which offer options to the online investigator, especially as these tend to excel in searching social media. Some of these search tools have their own unique strengths, whether it is looking at photos, finding user profiles or even establishing geo-social footprints collectively they provide a powerful toolkit to the online investigator (see Appendix 3 Internet Research Websites and Appendix 4-Search Engines).

10. DATA PROTECTION LEGISLATION

- 10.1 Officers must undertake a Data Privacy Impact Assessment before undertaking surveillance. This is best done in writing and should, among other things, consider whether the surveillance is necessary and proportionate.
- 10.2 Personal data processed by the Council is subject to the Data Protection Legislation. Personal data should be retained and destroyed in accordance with the requirements of the Council's Data Retention & Disposal Policy & Schedule. Due to the nature of social media, it is important to remember that when information produced as a hard copy is destroyed, that all digital copies of that evidence is likewise destroyed.
- 10.3 Providing accessible information to individuals about the use of their personal information is a key element of their legal right to transparency as set out in the Data Protection Legislation. As a data controller, the Council has a duty to explain via a *privacy notice*, how it processes personal information that is within its control and its lawful bases for processing

⁴ Crown Prosecution Service- Disclosure Manual RIPA/Policy For Interrogating Social Media For Investigative Purposes 7 March 2023

10.4 Before starting a covert investigation or following the gathering of 'intelligence' for the purposes of a prosecution, in addition to the relevant RIPA authorisation for a covert investigation, officers must, in consultation with the Data Protection Officer:

	complete	a Data	Privacy	Impact	Assessment;
--	----------	--------	---------	--------	-------------

 ensure that their service specific privacy notice explains how personal information is being processed and the lawful bases for such processing.

11. TRAINING

Officers from the following departments have been trained⁵ to use the internet and world wide web (open source – freely available data) more effectively for research and investigation, including the use of jargon, surface search, deep web search, social media investigations (search, networking and monitoring tools), technologies, how to identify sources of evidence and protecting IDs online:

- Community Safety Unit;
- Environmental Health;
- Fraud;
- · Housing Services;
- HR:
- · Legal Services;
- Planning Services.

12. ALLOCATION OF SOCIAL MEDIA ACCOUNTS

The Communications team will, on the request of a relevant manager, set up sterile profile accounts for officers who have been trained (see section 11 above). Managers are responsible for ensuring compliance with this Policy. False profile accounts will be set up in exceptional circumstances, following advance consultation with the Data Protection Officer.

13. REVIEW

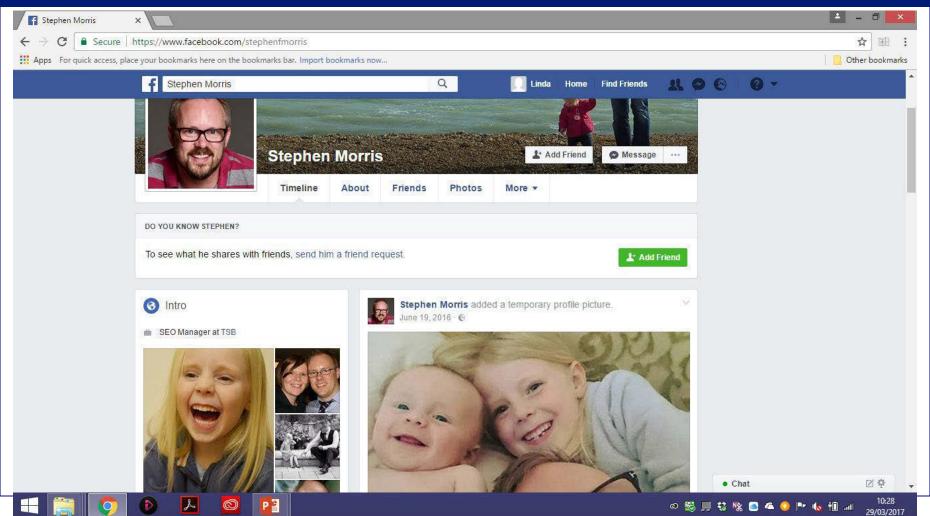
This Policy will be reviewed periodically and in line with the <u>Policy Statement - Regulation of Investigatory Powers Act 2000 (RIPA) (as amended)</u> to ensure that both Policies remain current and compliant with relevant legal requirements and best practice guidance.

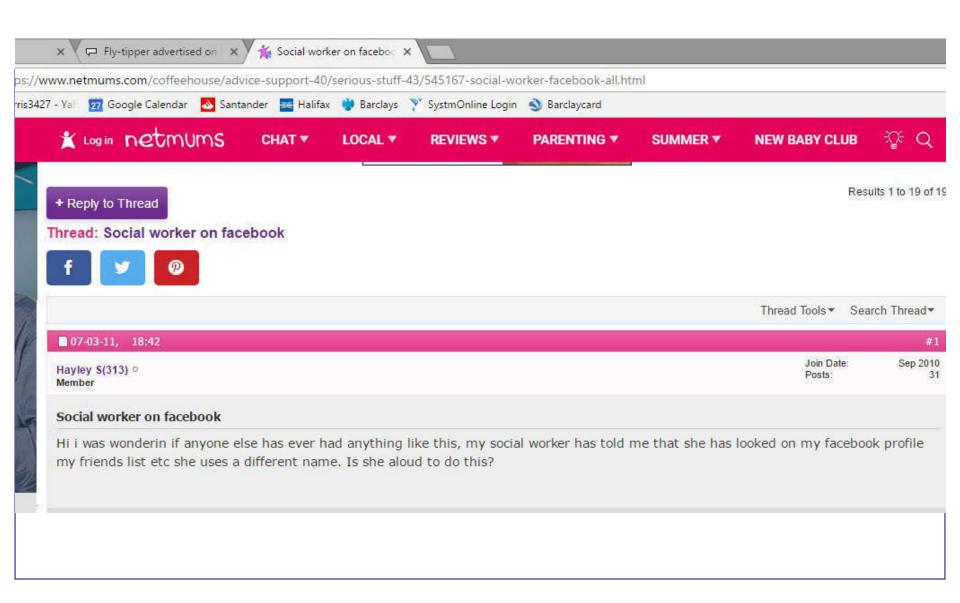
14. EQUALITY IMPACT ASSESSMENT

This Policy has been assessed with regard to an Equality Impact Assessment. The assessment has been graded as having a low potential impact, as the proposals in this Policy would have no potential or actual differential impact on grounds of race, ethnicity, nationality, gender, transgender, disability, age, religion or belief or sexual orientation.

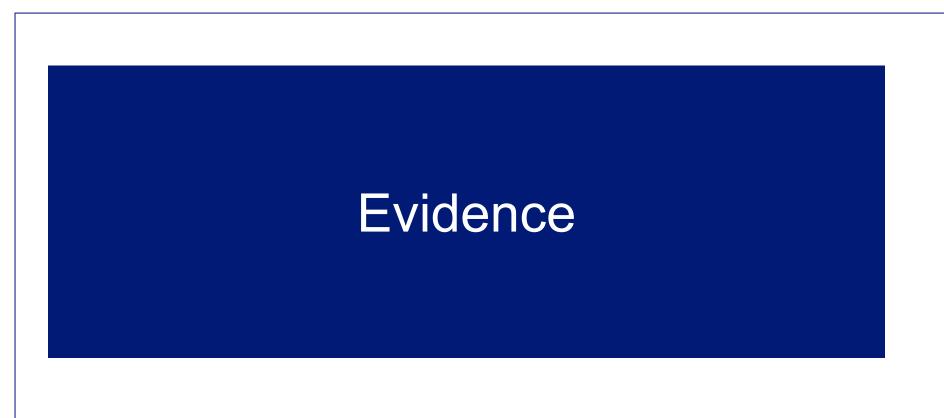
⁵ 28 October 2019

Is the information on Facebook private or public?





www.actnow.org.uk



- First original no corruption of data
- Properties of electronic objects
- Capture and secure original
- Working copy (mirror image)
- Note keeping and record of process used
- Secure storage
- WORM CD/DVD
- Secure partition on hard server

- Training of personnel
- Creation of procedural note and policy
- Completion of audit log/form
- Pocket Note Book entry
- Section 9 Witness Statement

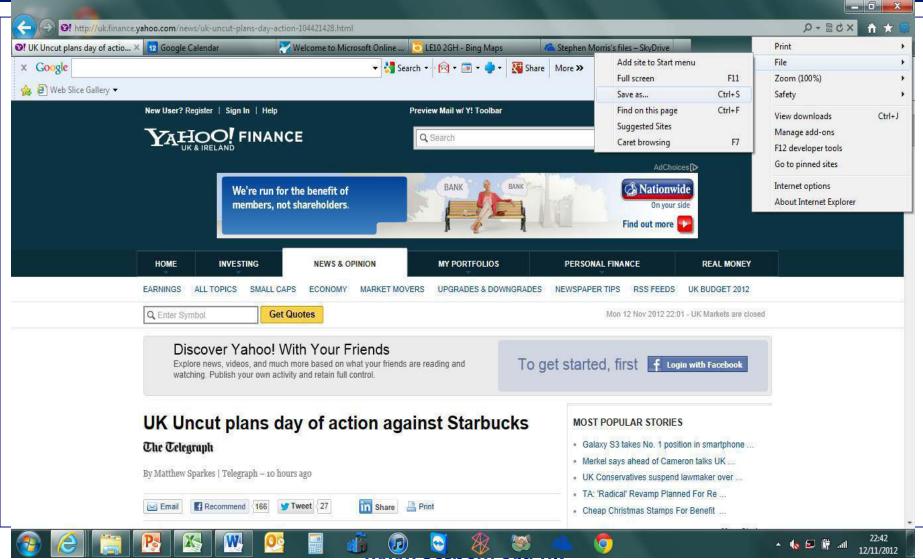
- Audit Trail
 - CPIA record, retain, reveal (Defence tactics relating to investigators capturing evidence)
- Print Screen into Word Document
- Temporary Internet Files (caches),
 Cookies

- Accurate Record of our activity required
- Video of screen activity
- Hypercam, BBSoft etc
- Kept with evidence (exhibits)

Hypercam http://www.hyperionics.com/hc/



Webpage capture



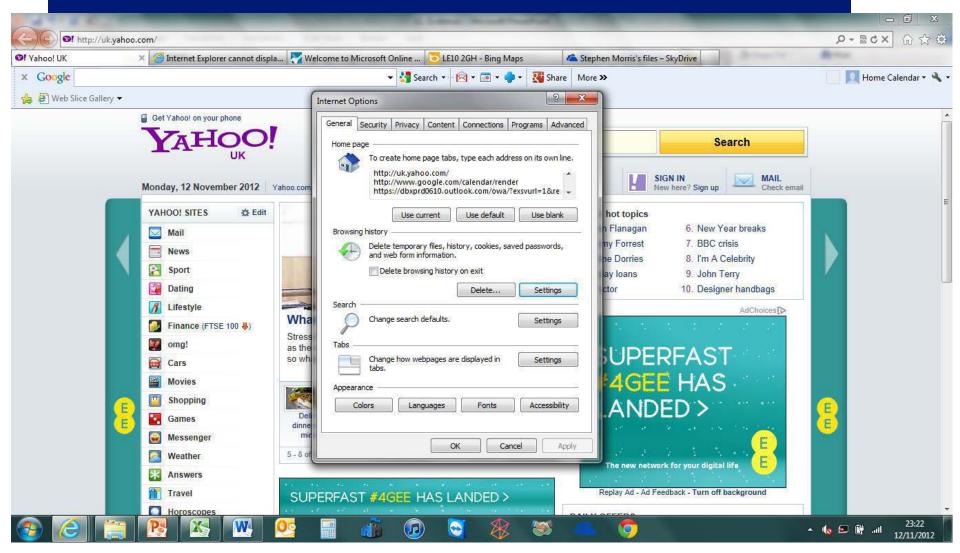
Web Site Capture



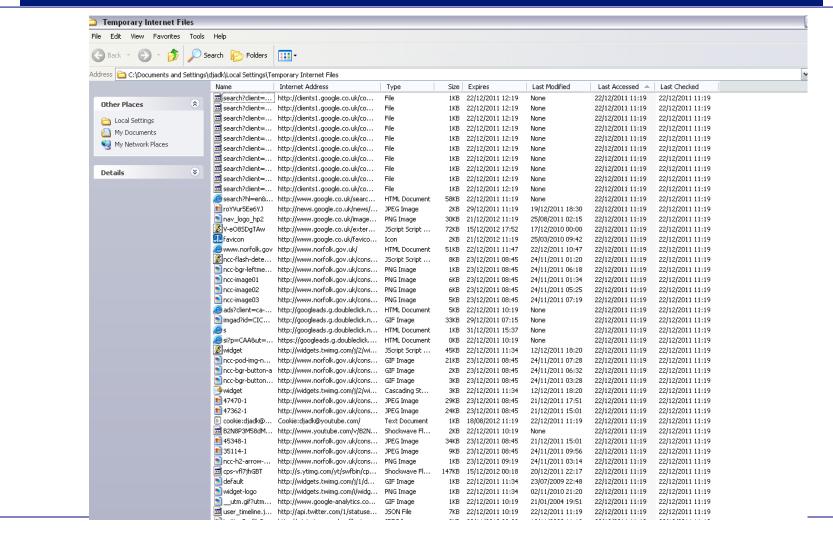
Browsing history — Audit trail

- When using a computer on the internet, information is exchanged between your computer and the servers that host the WebPages that you are viewing. These are commonly referred to as 'Temporary Internet Files' and 'Cookies'.
- Temporary Internet files are downloaded for each web page. HyperText Markup Language (html) is the predominant language for making these web pages.
- They are saved to the Temporary Internet Files folder, creating a 'cache' of the web page on your computer's hard disk.

Browsing history — Audit trail



Browsing history — Audit trail



Internet Research Websites

01 November 2019

Search Engines

https://www.google.co.uk/ (or com)

https://www.bing.com/

https://www.yandex.com/

http://www.dogpile.com/

https://duckduckgo.com/

http://www.webcrawler.com/

https://uk.search.yahoo.com/

http://www.searchenginecolossus.com/

Comments

- Search engines are real-time directories of what has been cached from the internet by software – Many types of search engine, searching specific subjects across the internet
- Skill required to reduce number of 'hits' Boolean logic
- Search engines on small individual websites and larger ones such as ebay, flickr, etc.
- Advanced search facilities and filters semantics
- Exact words and phrases Predictive text, caches Regional search engines

Phone numbers

http://www.magsys.co.uk

http://static.ofcom.org.uk/static/numbering/

http://whocallsme.com (and other tele-pest blogs)

https://www.truecaller.com/

https://www.whatsapp.com/

http://www.saynoto0870.com/

Comments

- Search exact numbers in search engines (speech marks)
- Consider different formats of number posted on a site that might have been cached
- 08 numbers require geographical exchange numbers further information to search

Website details

https://www.nominet.uk/

http://whois.domaintools.com/

http://centralops.net/co/

Comments

• Lots of technical data available

- Associated accounts (domains etc)
- Opportunities for further enquiries payment information etc
- Complete history from RIPE
- For a small fee complete history of domain 'ownership'

Old Website Caches

http://archive.org/web/ Waybackmachine

http://www.webarchive.org.uk/

Comments

- Enter website address (domain name) into search box
- Outlook style calendar for current year appears with cached dates in blue background
- Hover over a date and the exact time and date of cache appears
- Click on a highlighted date and the old webpage/site appears revealing images, names, contact details, phone numbers email addresses – all researchable

People Searching - Social Networking Sites

https://pipl.com/

http://www.yasni.co.uk (or com)

https://www.yandex.com/

http://www.dogpile.co.uk/

https://www.facebook.com/help/community/question/?id=10203187384877484

https://www.facebook.com/help/460711197281324/

https://twitter.com/search-advanced?lang=en-gb

https://www.linkedin.com/help/linkedin/answer/302

https://inteltechniques.com/menu.html

http://osintframework.com/

https://www.bellingcat.com/

https://namechk.com/

https://usersearch.org/

https://www.peekyou.com/

https://pikdo.net/

http://sometag.org

http://www.192.com

Comments

- Lots of information! Judge carefully the source and the information provided
- Different sites, different settings
- Potential privacy and Human Rights and RIPA issues and authorisation may be required for some activity

- There is private information on most profiles and it does require consideration of why looking at it, and necessity and proportionality of extent of intrusion balanced with what being dealt with
- Guidance, Your organisation policy if required obtain legal advice (but don't be afraid
 to consider and use this as a research opportunity) Every set of circumstances needs to
 be considered on it's own merits

Businesses

https://beta.companieshouse.gov.uk/

https://opencorporates.com/

https://www.endole.co.uk/products/company-search/

https://www.duedil.com/

https://www.arachnys.com/solutions/investigator

https://star.worldbank.org/content/beneficial-ownership-quides

Comments

- The source of data is Companies House, however researching the site can be time consuming and for some data require registration
- Many websites provide the same data in more accessible and easily read format
- Searches by postcode, address, through Google etc often return 'hits' through these sites.
- Again, consider reliability and if to be used as evidence or to cause some definitive action, consider obtaining it directly from Companies House

Property

http://www.zoopla.co.uk

http://www.rightmove.co.uk/

http://www.landregisteronline.gov.uk/

http://www.landregistry.gov.uk/property info/phs/

http://www.192.com/

https://www.elra.eu/facts-sheets/land-registries-cadastres-in-europe/2-land-registry-and-the-cadaster/

Comments

- Lots of information about current and old property listings
- Photographs, prices, and often tagging data in photographs which might real other information such as names, email addresses, phone numbers
- 192.com is a pay site free searches provide very random, sketchy results
- Elra.eu is official EU central point of contact for enquiries with EU land registries

Blogs

http://www.blogsearchengine.org/

https://www.searchblogspot.com/

http://www.lycos.com/

Comments

• Lots of different blogs search engines – normally focused on particular subjects

Postcode

http://www.royalmail.com

http://www.postcodeanywhere.co.uk/demos/address-finder/

Comments

 Open source royal mail site to check addresses within a post code, or find post code for an address

Images videos GPS (EXIF Data)

https://www.google.com/imghp?hl=EN

https://www.bing.com/

https://www.tineye.com/ (reverse image search)

https://www.gps-coordinates.org/

www.pic2map.com

https://www.flickr.com/ (search by tagging, location, user, geo-tagging etc)

https://www.google.co.uk/intl/en uk/earth/

http://www.findexif.com

http://fotoforensics.com

http://exif.regex.info/exif.cgi

http://www.geograph.org.uk/

Comments

- Search images by their properties, tagging data, geo-tagging data etc
- Search images to find them on other websites
- Search by location, user, etc
- Identifies user details, account user names, and lots more which can then be researched through Google etc to link to other online activity
- Consider facial recognition and machine learning technologies

Vehicles

https://www.mycarcheck.com/

https://www.gov.uk/request-information-from-dvla

https://ownvehicle.askmid.com/

https://www.vehicleenguiry.service.gov.uk/Default.aspx

https://www.gov.uk/check-mot-status

https://cazana.com/uk

Comments

- DVLA will provide registered keeper information if requested and reasons are in line with their disclosure regime
- Other site provide vehicle make, model and colour from registered number
- Askmid provides information about current insurance status
- Other sites provide other vehicle history upon payment but beware, some promise lots but take your money and deliver little

Organisations

http://www.the-sia.org.uk/home/licensing/register/register.htm (door supervisors etc)

http://www.gassaferegister.co.uk/

http://www.gmc-uk.org (doctors)

http://www.legalhub.co.uk Bar Council register

http://www.gla.gov.uk Gangmasters Licensing Authority

Comments

 A few examples – when researching people and their business or private activities, consider what organisations they might be registered with. The websites of these organisations often provide publicly available personal information

ebay

http://www.ebay.co.uk/sch/ebayadvsearch/

http://pages.ebay.co.uk/help/search/search-commands.html

https://www.ecopsapp.com/

Comments

- Using advanced search facilities on ebay, and with practice you should be able to find information about anything being sold, and information about sellers
- E-cops provides a professional ebay search and statement at a cost

•

Financial

http://findsortcodes.co.uk/#

http://www.postcodeanywhere.co.uk/demos/bank-validator/

https://europa.eu/youreurope/business/taxation/vat/check-vat-number-vies/index en.htm

https://www.bindb.com/bin-database.html

http://www.binbase.com/search.html

http://www.equifax.co.uk - http://www.experian.coml

https://www.trustonline.org.uk/

https://www.gov.uk/search-bankruptcy-insolvency-register

https://www.insolvencydirect.bis.gov.uk/eiir/

Comments

• A number of resources that provide bank and other financial services informationipts etc

Identity documents checker sites

https://www.consilium.europa.eu/prado/en/search-by-document-country.html

https://www.keesingtechnologies.com/reference-database/id-documents/

Comments

- Consilium Europa provides free on-line information about EU identity documents such as passports, visas, identity cards, some driving licences, and other forms of ID
- Keesing is internationally recognised and provides support for all worldwide travel documents. Publishes bulletins, guidance and online support. Subscription required

Maps

https://www.google.com/maps

https://www.openstreetmap.org

https://yandex.com/maps/

https://liveuamap.com/

Comments

- Extensive and detailed, providing a variety of views, and photographs of street views
- Beware Streetview and satellite images might be quite old

Evidence Capture

http://www.hyperionics.com Hypercam Hypersnap

http://www.httrack.com

https://www.flashbackrecorder.com/

http://getfireshot.com/

http://camstudio.org/

http://discover.techsmith.com/camtasia-screen-recording/

http://osirtbrowser.com/

Comments

• National and organisational procedures must be followed

- ▶ Software 'spiders' or 'robots'
- Crawl across web-pages and documents not securely protected
- Capture meta data meta tags values/ratings
- Feed into servers (caches)
- Algorithms (formulas) for analysis and search results

- Different types present results in different order. What do you think might influence this process
- Different levels of penetration and frequency
- Some focus on particular parts of the internet
- Beware caches when viewing results
- Beware predictive text leading to narrow parameters

- Return results think we want
- Google.com Google.co.uk Google.ie Google.fr
- Temporary internet folder

- https://www.google.co.uk/ (or com)
- https://www.bing.com/
- https://www.yandex.com/
- http://www.dogpile.com/
- https://duckduckgo.com/
- http://www.webcrawler.com/
- https://yippy.com/
- https://uk.search.yahoo.com/
- http://www.searchenginecolossus.com/

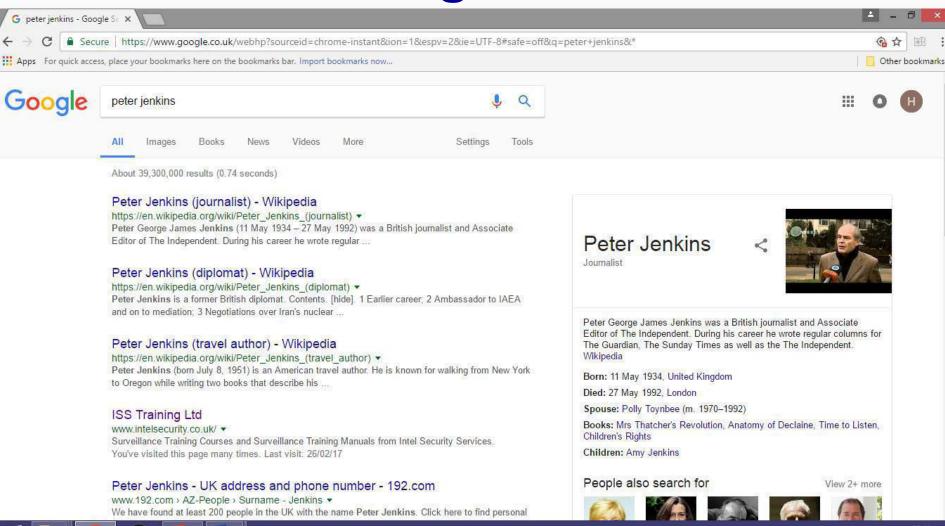
Search Engines – Advanced Search Table page 10 of Manual

Tools

When?

Operators

- Exact word or phrase
- All of these words
- One or more of these words
- None of these words
- Region
- Related (related:www.intelsecurity.co.uk)
- Linked (link:www.intelsecurity.co.uk)
- Site (site:www.intelsecurity.co.uk)









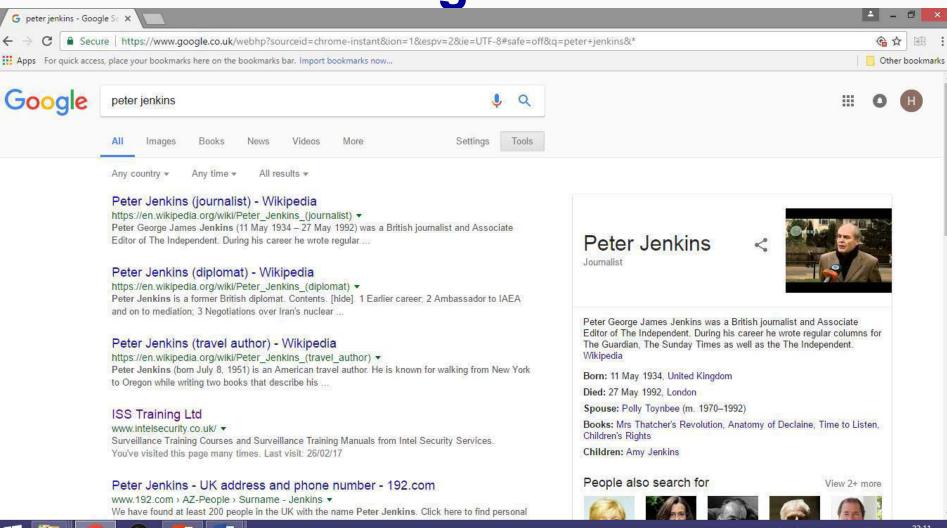








12/03/2017













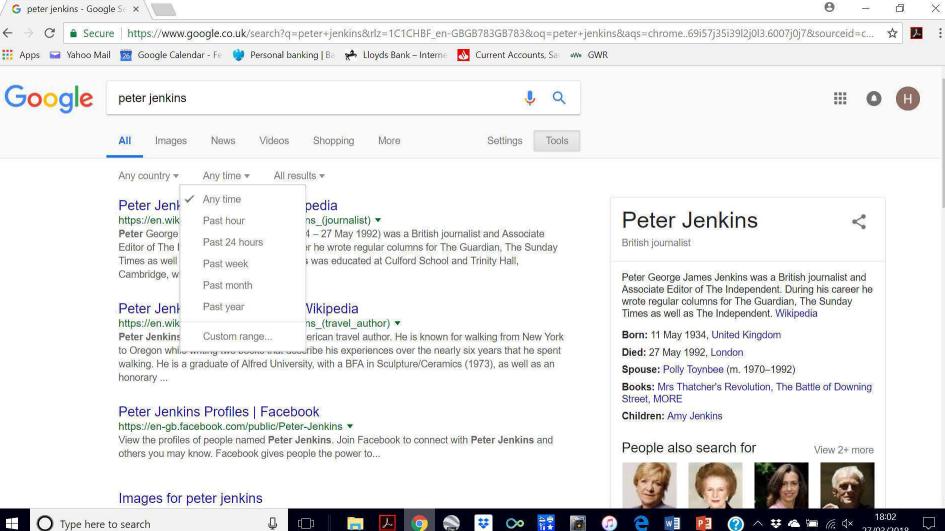


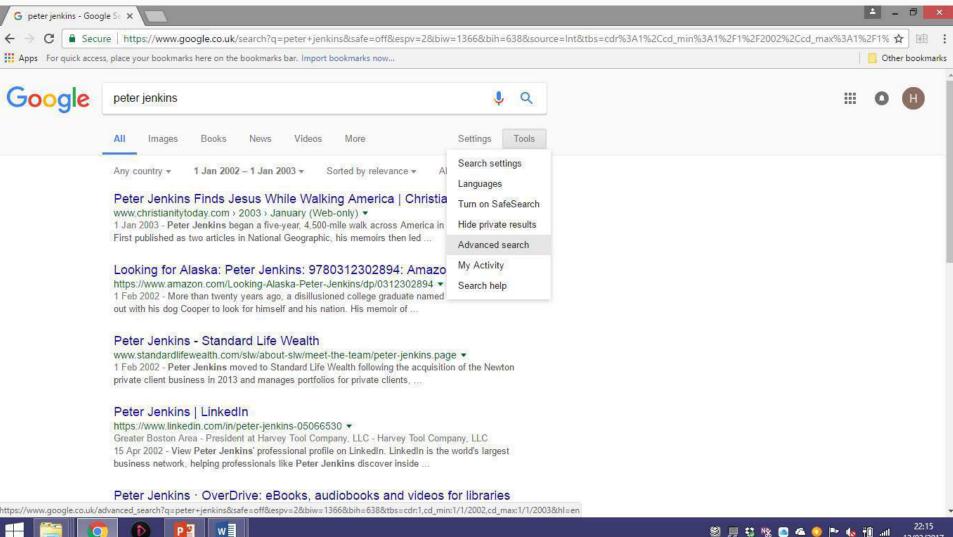


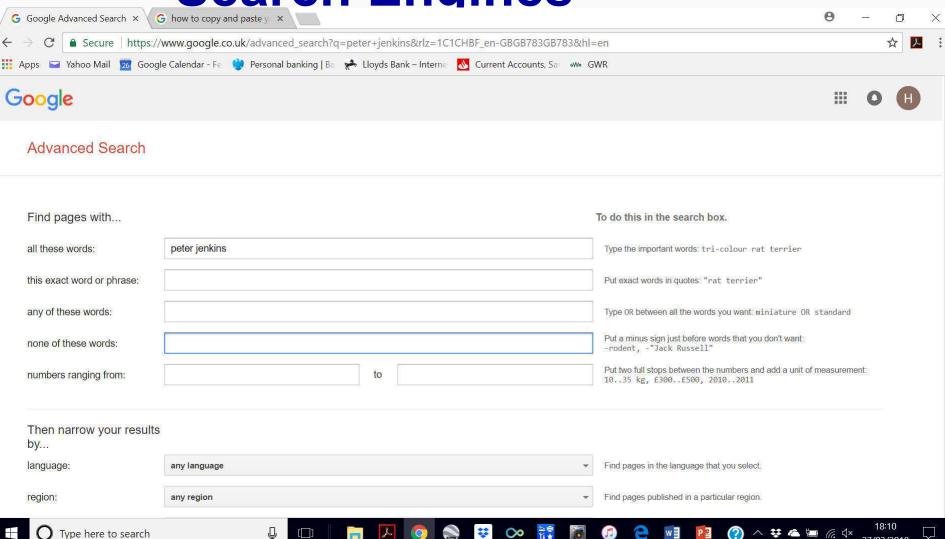


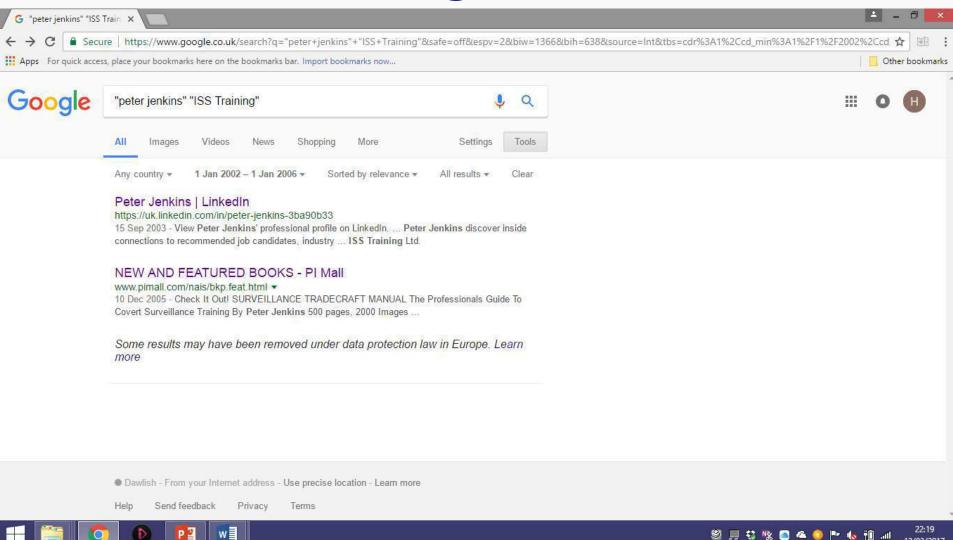




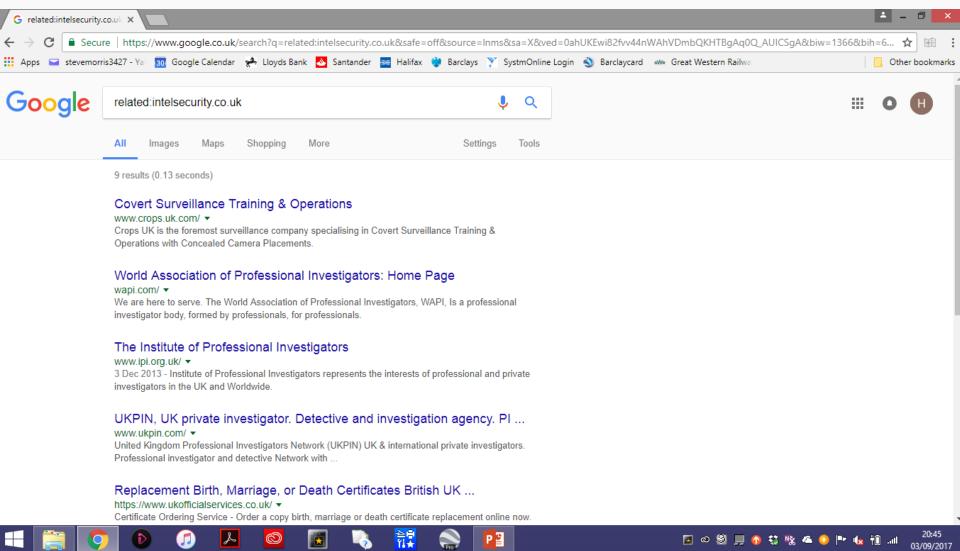




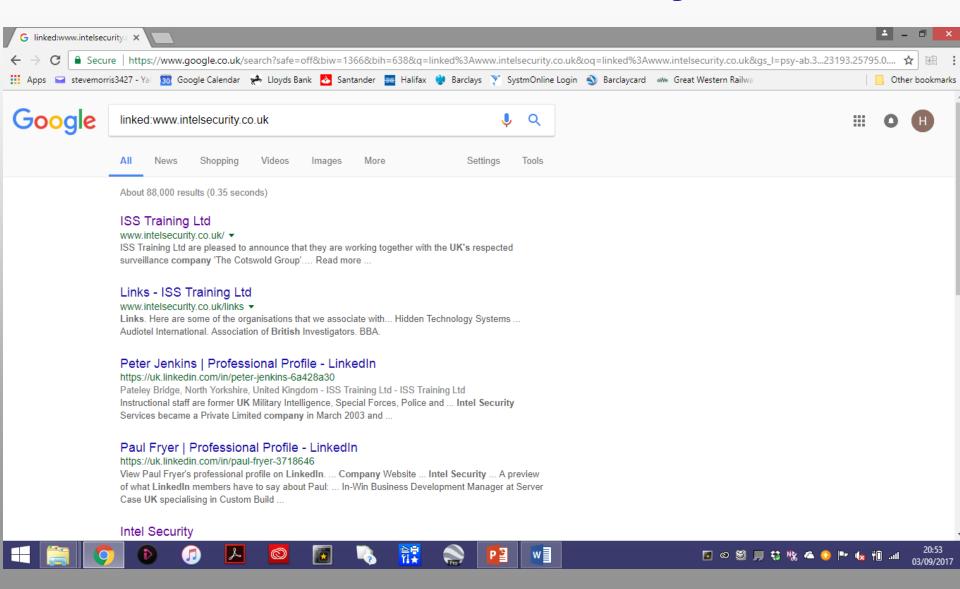




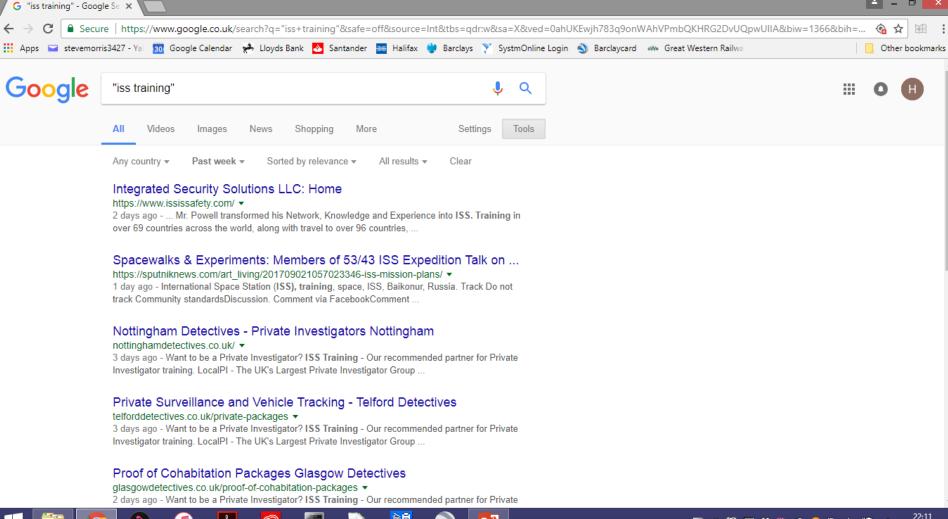
related:intelsecurity.co.uk



linked:www.intelsecurity.co.uk



Recent Cache searching – low meta data value caches































- Advanced Search Techniques
- Reducing the Number of 'Hits'
- Boolean Logic
- "exact numbers or words"
- -word "phrase or collection of words"

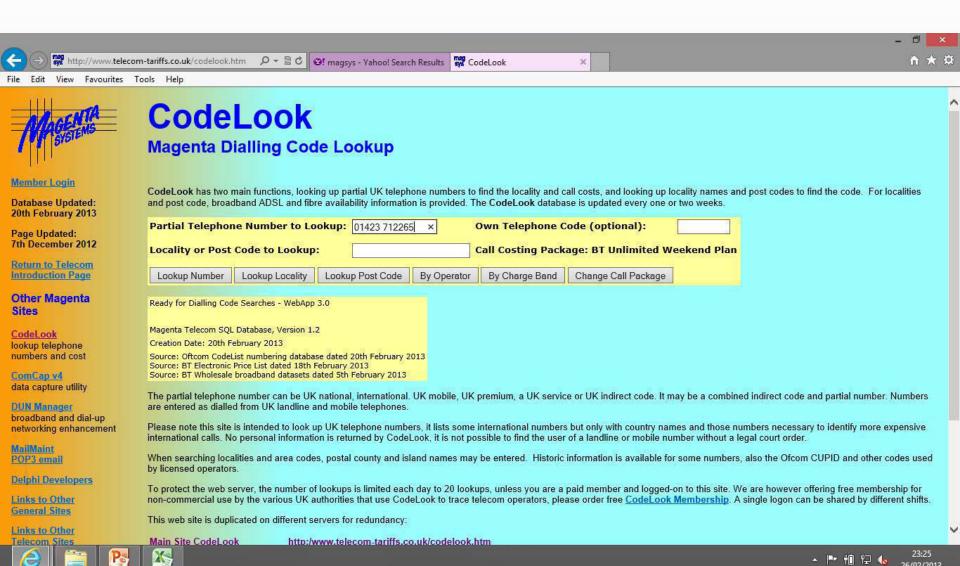
- Use Several Search Engines different results
- Be careful that advanced search does not 'tip out' results e.g. Region - Ireland might remove universal American sites used extensively in Ireland
- Different search engines for different subject areas

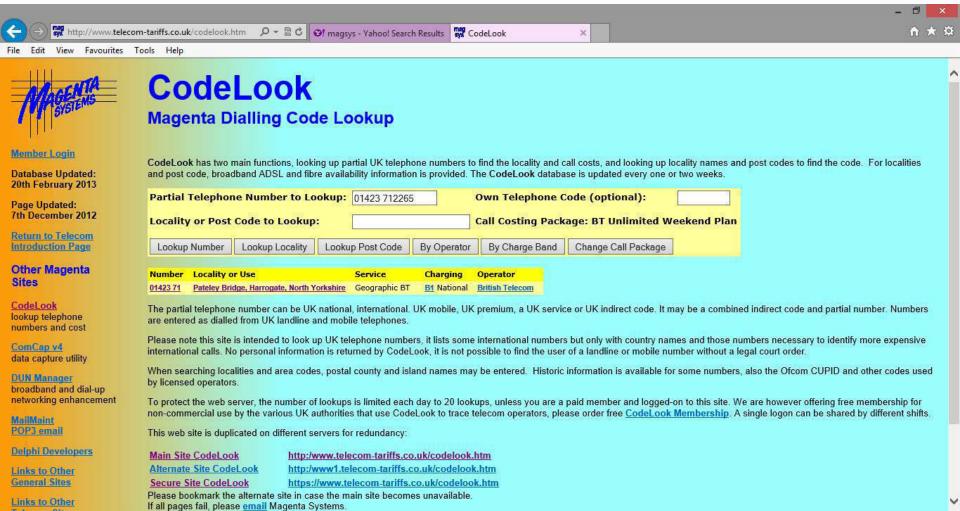
Searching Phone Nos.

- Enter "07988 123456"
- ▶ Enter "07988123456" (searches precise details)
- But what other formats might have been used?
- +44 (0) 7988 123456 and more

08 Numbers

- Virtual numbers
- Attached to geographic exchanges and numbers
- 'say no to 0870'
- Identify
 - geographic location
 - other account/business information
 - other numbers to research

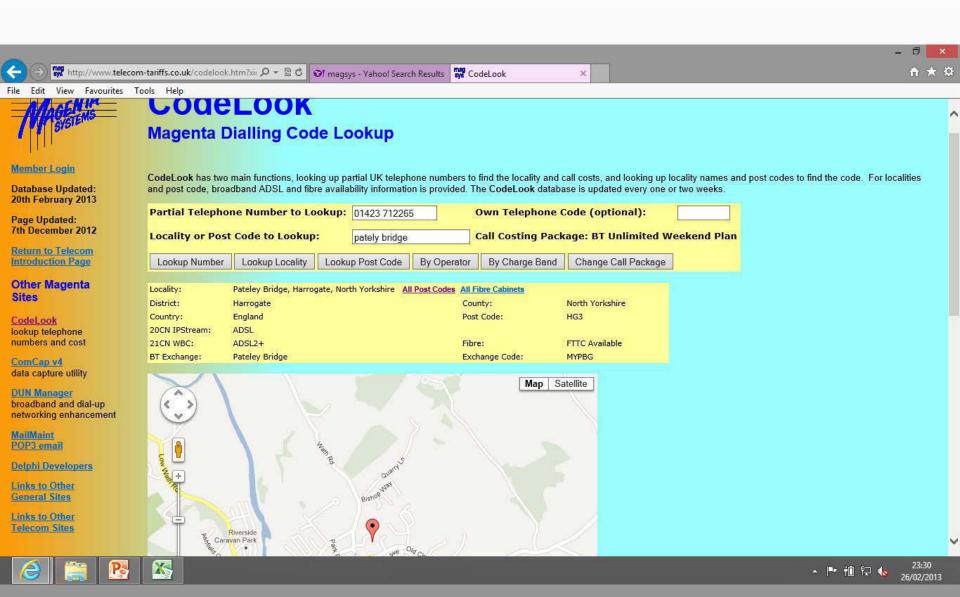


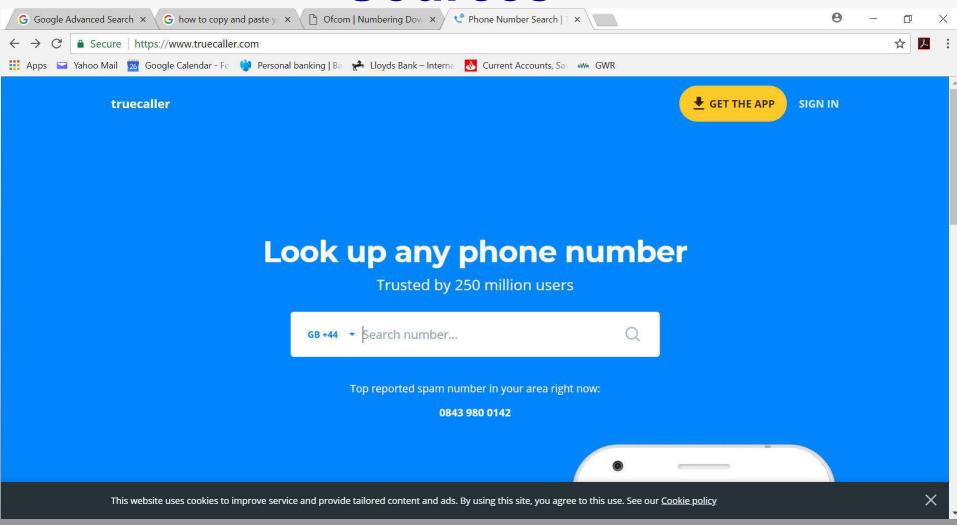


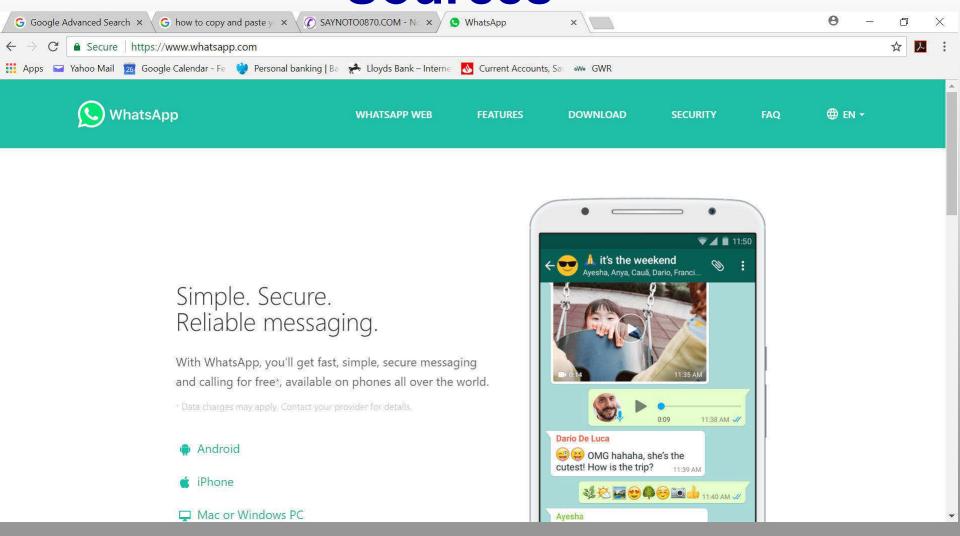
🔺 📭 前 🖫 👠

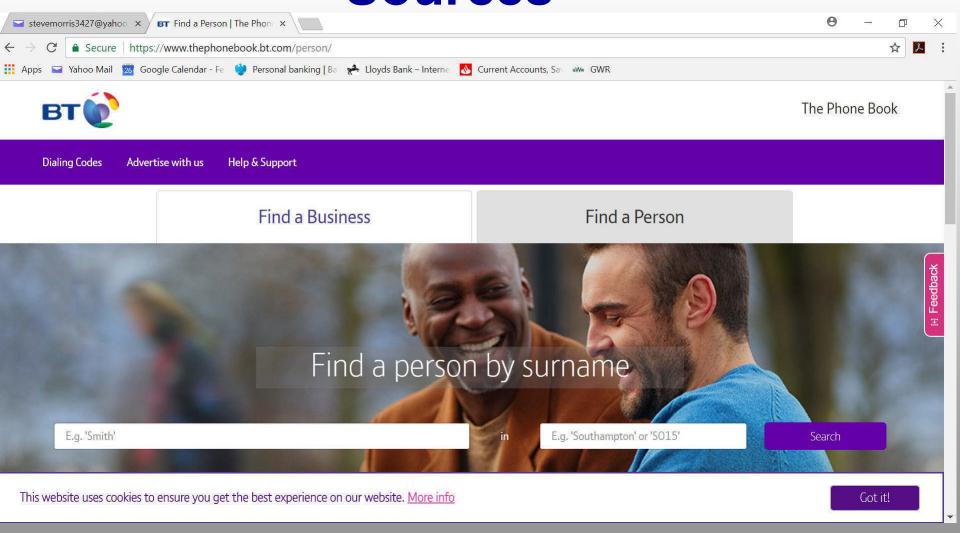
26/02/2013

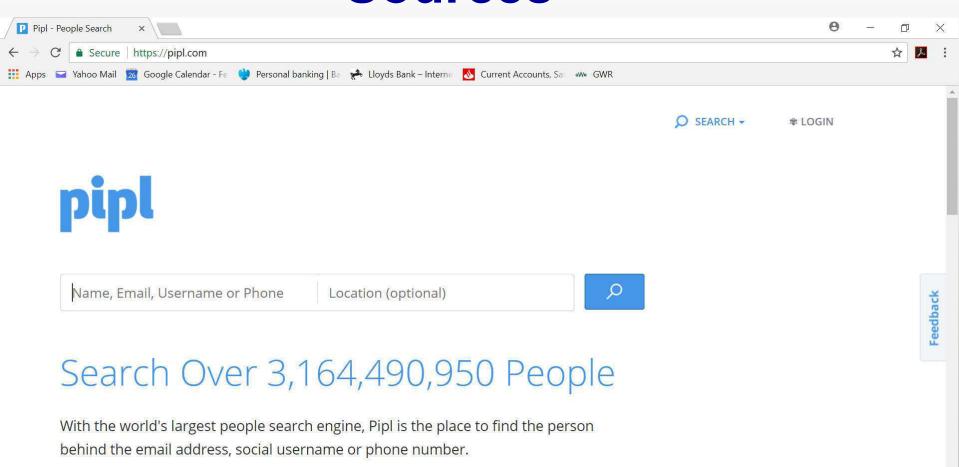
elecom Sites











Intelligence or Evidence?

- Is our product evidence?
- Or is it intelligence that provides a link to evidence?
- How can we prevent others identifying the intelligence and methods of investigation?
- Sensitive method of investigation
- ▶ CPIA

Introduction

Search engines are real-time directories of information (metadata) that has been cached from the internet by software. The software consists of 'robots' or 'spiders', that crawl across websites and documents that do not prevent their access. They cache (capture), and store these webpages.

The web page content is 'valued', using a number of analytical tools and values, and also algorithms set to the values required by that particular search engine.

Some search engines focus on particular parts of the internet.

Because of the individually programmed analytical tools and algorithms, different search engines might research the same places on the internet, but return results in a very different order. – there have been allegations of 'fixing' the results, and in some instances these have been found to be true. Given the marketing power of search engines and the ability to route users through particular areas of the internet, the opportunity for financial gains are enormous, and therefore the likelihood that it is "fixed" is high in relation to some topics to be researched.

A competent website designer will be able to increase meta data, links and associations, raising the profile of the site and it's position in the 'hits' returned in response to a search. One mare point of interest is that an uncontrolled search of a common word or series of words will return results on Google listed in the millions. Although there are many results, this figure is broadly based on how many times the site has been 'crawled' and cached by the spiders and kept a cache.

So let's do the maths! If the name Adele appeared on just one webpage in ten places, and the 'spiders' crawled the webpage just once per day for, and that one webpage existed since the year 2000, we have the following calculation -

10(words on webpage) x 365(days per year) x 16(number of years to end of year 2016) = 58,400

A search for the word 'Adele' on 9th March 2017 returned '179,000,000' results, but it is now easy to see how many repeated visits to the same webpage over a period of time

can easily produce vast numbers of 'results'. Many pages with many references to Adele, and not just the singer Adele will produce many hits in a very short period of time So – there aren't 179,000,000 webpages found, but 179,000,000 caches or captures of the word – albeit it might be many of the same!

Harnessing the power of a search engine

As a researcher of the internet it is not important to know how a search engine works, although it might assist when interpreting results provided, but it is important to understand how to use the search engine effectively. Search engine technology in various forms is used by most search facilities on the internet, including social media, commercial sites, government and other sites. Even the administrator of a relatively small website van install a Goole 'widget' to enable searching of the site. Therefore the random use of search engine tools might focus your search on that site.

Searching

To facilitate this training session Google will be used, but there are many other search engines that you should consider. Remember, Google is a large commercial search engine with vast software reaching across the internet on a very regular basis, which will inevitably return vast results. Some other more obscure search engines will only search particular parts of the internet, with relatively less powerful search facilities, not very efficiently and not regularly visiting the same webpages, but useful because there focus results in less 'noise' (noise is a term used for all the information that might bury that which you are searching for).

A few basics

When searching, think about the terms and words likely to be used by the entities or their associates, and use these rather than using only your own official or organisational terminology

Often persons trying to remain relatively anonymous or untraceable will not be found through their correct name or details. However if you find an address or other related data, remove the name or details you are researching, or search using this other criteria. It might reveal other related businesses or persons, or even your subject using a different

identity, and research of these other entities might reveal the information that you are seeking about your subject.

Simple example – Search of *Stephen Morris Post Code B32 4DJ* might not reveal anything about Stephen Morris, but just a search of *B32 4DJ* might reveal other persons and details of businesses at that location. Research of these persons or businesses might reveal links to your subject, and go on to reveal information about that person that you are seeking.

The Google search you are likely to use in the UK will be defaulted to Google.com or Google.co.uk. Because of where you are, Google will return results it assumes you are interested in (UK, European and American), you don't see much for Peru, or Iceland, or maybe Japan – but these regions or countries have the internet! So when researching a particular topic, consider the country or region and in the Google search box type Google with the suffix for that country. Up will come Google Fr. Google.fr is the French version of Google. Searching for a French person or place on this search engine will return results for the person or place in France rather than buildings or places in the UK named after that entity in France.

Spelling - Google's spell checker automatically uses the most common spelling of a given word, whether or not you spell it correctly. T will provide you with results using its own spelling but provide you with the opportunity to see results for your spelling. Check which you want and use that option. Upper and lower case letters are the same in Google. A search for Heinz Baked Beans is the same as a search for heinz baked beans

Beware of caches!

Earlier we said that the results returned by Google are the cache results. During the training you will see how to identify the time and date and reveal that cached page. Provided everything goes well (you have a good, consistent internet connection, the web page still exists, and no data packets are misplaced in transfer), a click on that link will most probably take you to that page. However, any number connection of problems might result in you visiting the cache, which might be several days old. Clearly this is not necessarily how the webpage looks real time. So best practice is that if you identify something you intend to use as evidence about the page as it is now, view the website details in the URL box on your web browser, and go directly to this link via the URL,

missing out the search engine. This will mean that you can be sure the webpage you are viewing is 'real time', and then you should capture the information/evidence.

Advanced search and search operators.

In common with other search engines, Google has advanced search facilities, operators, and tools. Understanding these capabilities, and using variations on words, and phrases together with adjustments to the operators and tools will reduce the number of worthless results, and focus the search effectively. There is no science to this, but practice will improve your skills.

In common with many search engines, Google constantly changes it's appearance and interface. If you have difficulty finding the features detailed below, use the Google 'help' search and type in the facility you are looking for.

At the time of producing this tutorial, the search facilities can be found as follows.

Type in the initial Google search box broadly what you are looking for. This will provide a view which consists of results, a further search box, below which are the opportunities to search videos, shopping, images. Also a tab named 'tools' – clicking on this tab will reveal further operators to focus the search such as country or specific dates or ranges of dates. Also, in the top right hand corner will be a 'cog' Clicking on this cog opens a dialogue box and one of the facilities listed here is 'advanced search'. Click on advanced search and this reveals many search operators to fine tune your search.

Many of these search tools can be used by the experienced researcher just within the basic Google search box using a variety of symbols and punctuations.

There now follows a list of the various search facilities. Remember, adjusting them in isolation is not what is required, but tweaking and adjusting them as you get particular results is the way to success.

Search engine tools and operators

Symbol	How to use it
66	Putting a phrase or series of numbers such as a phone number in speech marks will return results for that specific word or phrase "0121 423 5983" will return all of the exact matches for that exact number rather than all of the 0121 numbers, or obscure part numbers or delivery codes which contain that set of numbers
-	When you put a minus sign in front of a word it removes results with that word in it them. So if you were looking for Steve Davis, but not the snooker player, using <i>steve davis –snooker</i> in the search box removes the results that include the word snooker. Multiple words phrases and operators can be used in conjunction with each other.
*	Use an asterisk as a wildcard for a term or word you are unsure of. Example: "a * saved is a * earned"
@	Find social tags Example: @searcher
OR	Find pages that might use one of several words. Example: waste OR rubbish OR removal OR clearance
#	Find popular hashtags for trending topics Example: #brexit
site:	Search and get results from certain sites or domains. Examples: Gov.uk or Ebay.co.uk
related:	Find websites and blogs (and sometimes social media posts) that are similar to a web address you are interested in. Example: related:Travelodge.co.uk
linked:	Find websites and blogs (and sometimes social media posts) Google has identified as linked in some way to a web address you are interested in Example: linked: thesurveillancegroup.com
info:	Get information about a web address, including the cached version of the page, similar pages, and pages that link to the site.

	Example: info:google.com
cache:	See what a page looks like the last time Google visited the site. Example: cache:bbc.co.uk

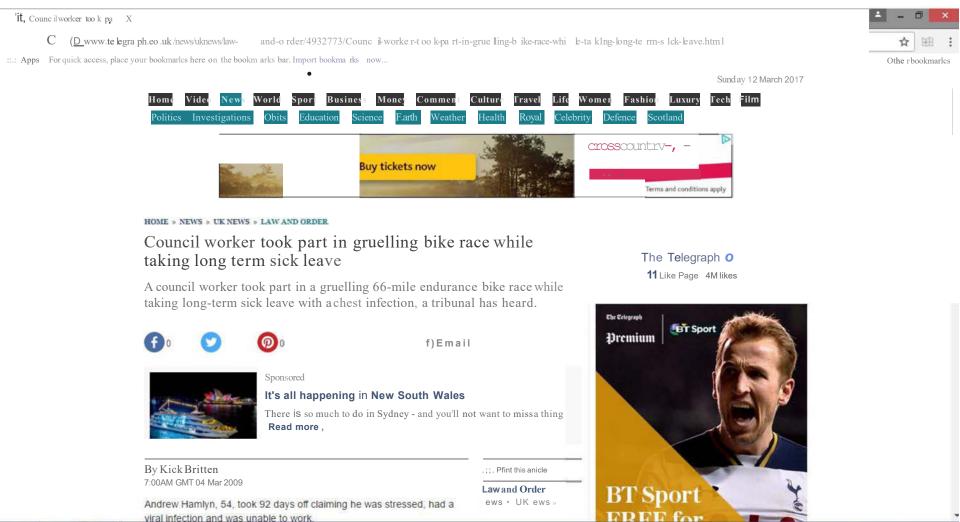
When you search using operators or punctuation marks, don't add any spaces between the operator and your search terms.

Remember – the key to success is to adjust your various search criteria to focus upon what you are searching for. If you discover obscure or uncommon terminology for the entity you are searching, try using this with one or two other unique terms you have. And use more than one search engine

Social Networking Sites

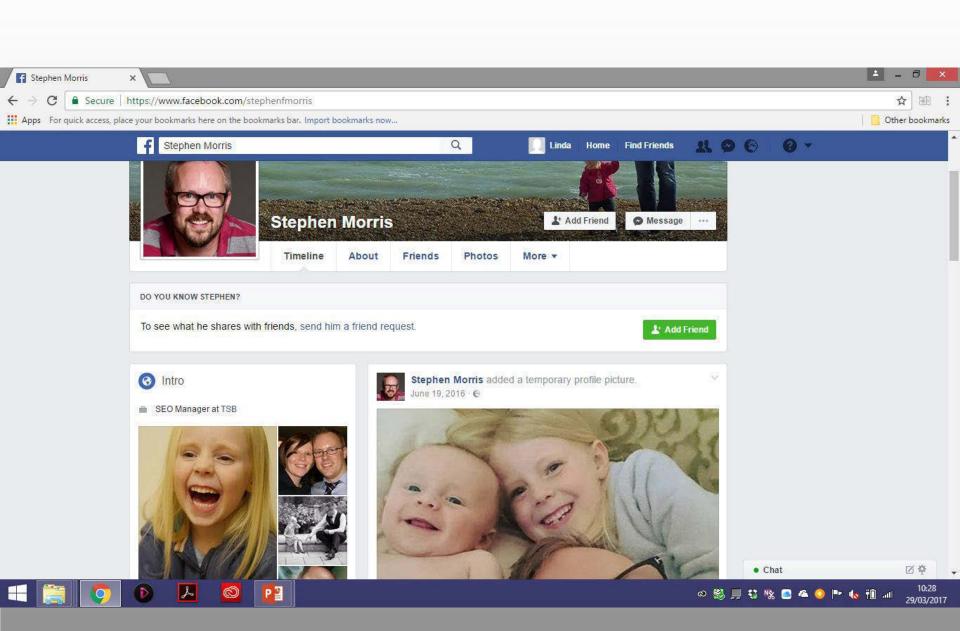
Facebook



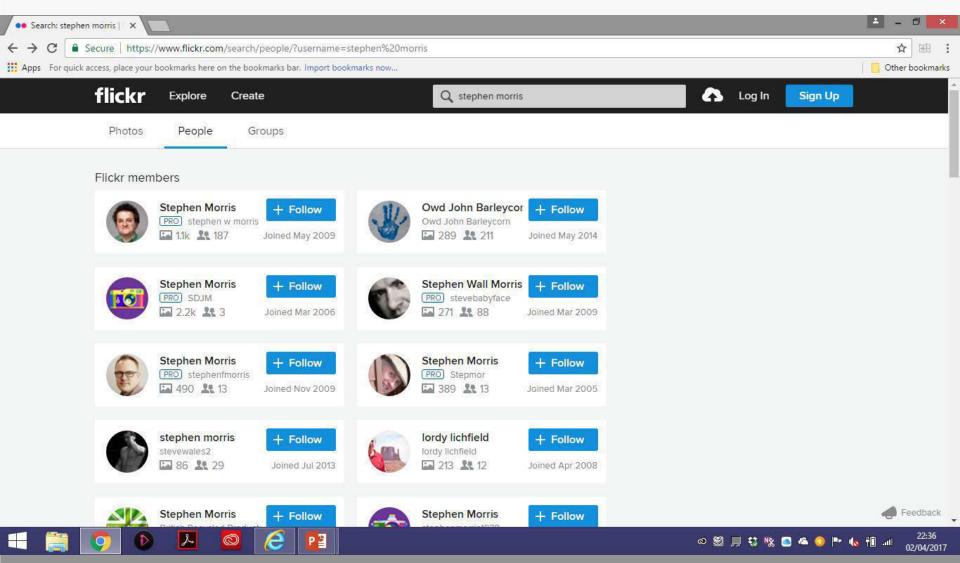


lin. 🔐 🌏 🕶 🔕 🐉 🕃 📃 👺

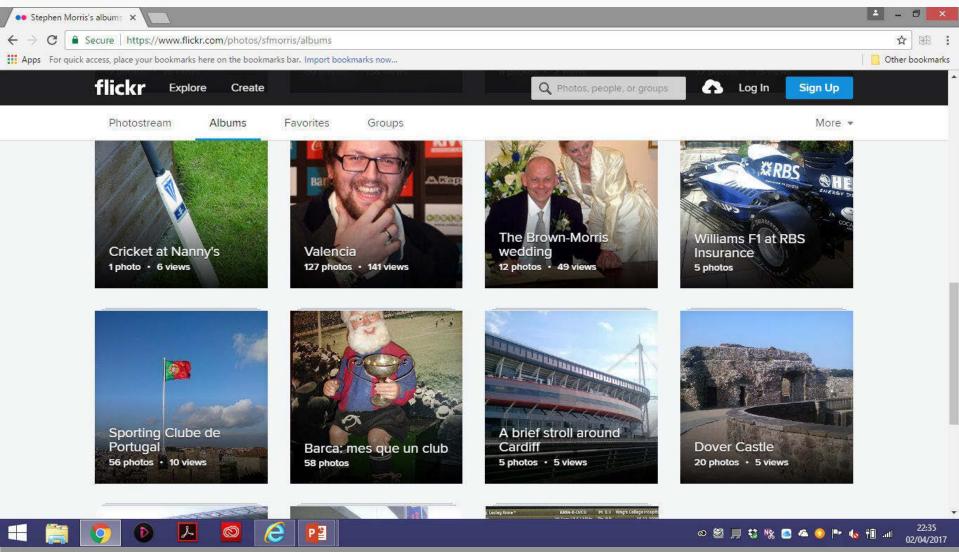
12/03/2017



Search Google images with image from Facebook – find flickr account



Images on flickr contain Exif data – location date time device etc.



SNS Specific Search Sites

https://pipl.com/

http://www.yasni.co.uk (or com)

https://www.yandex.com/

https://www.facebook.com/help/community/question/

https://www.facebook.com/help/

https://twitter.com/search-advanced?lang=en-gb

https://www.linkedin.com/help/linkedin/answer/302

https://inteltechniques.com/menu.html

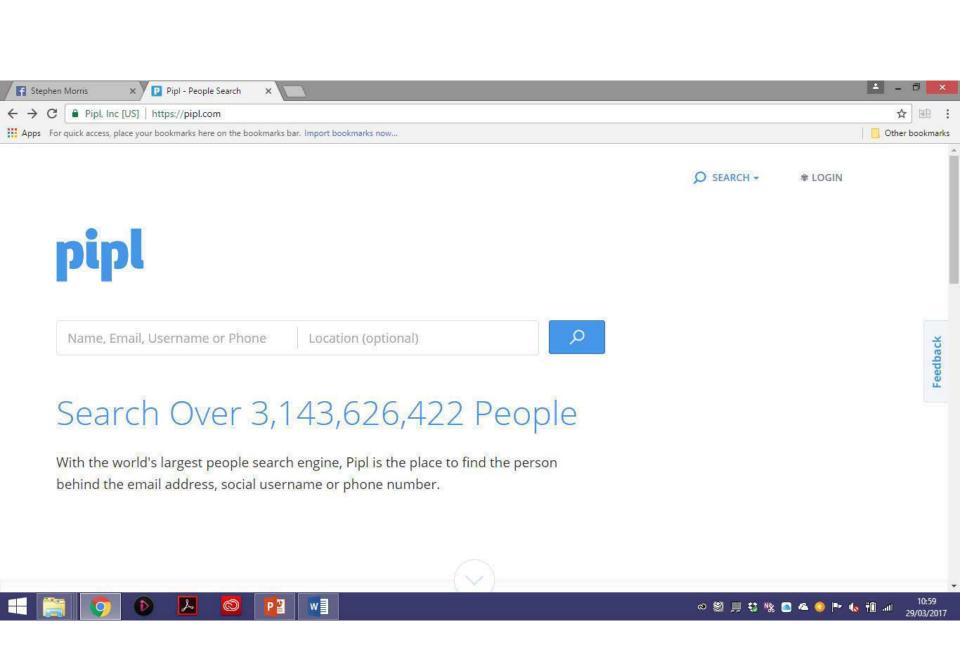
http://osintframework.com/

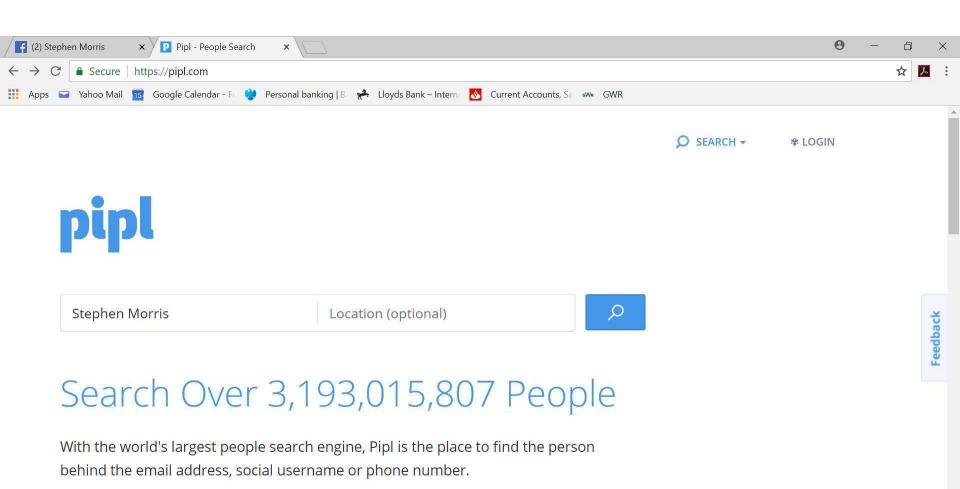
https://namechk.com/

http://www.192.com

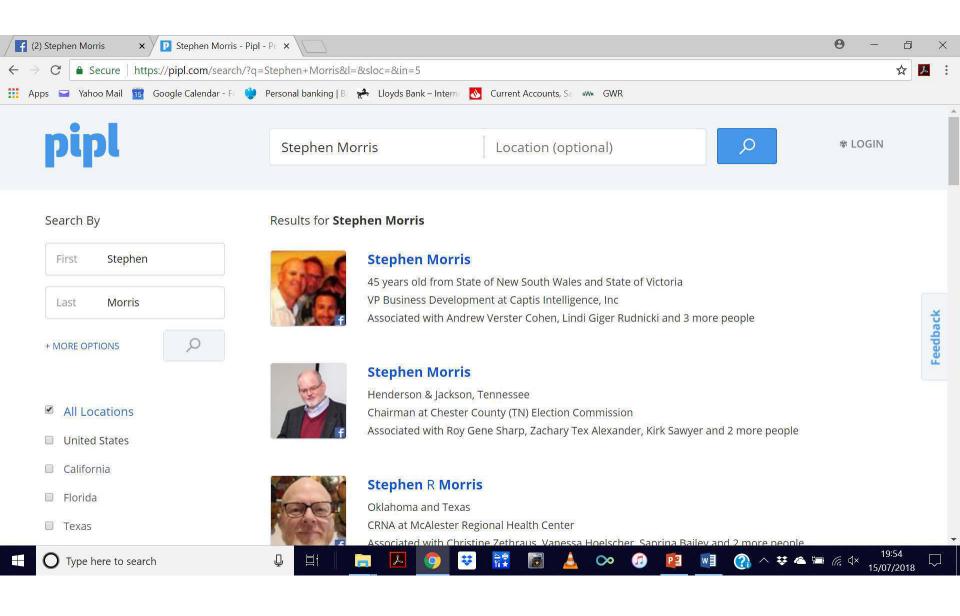
https://sometag.org/ https://pikdo.net/?hl=en

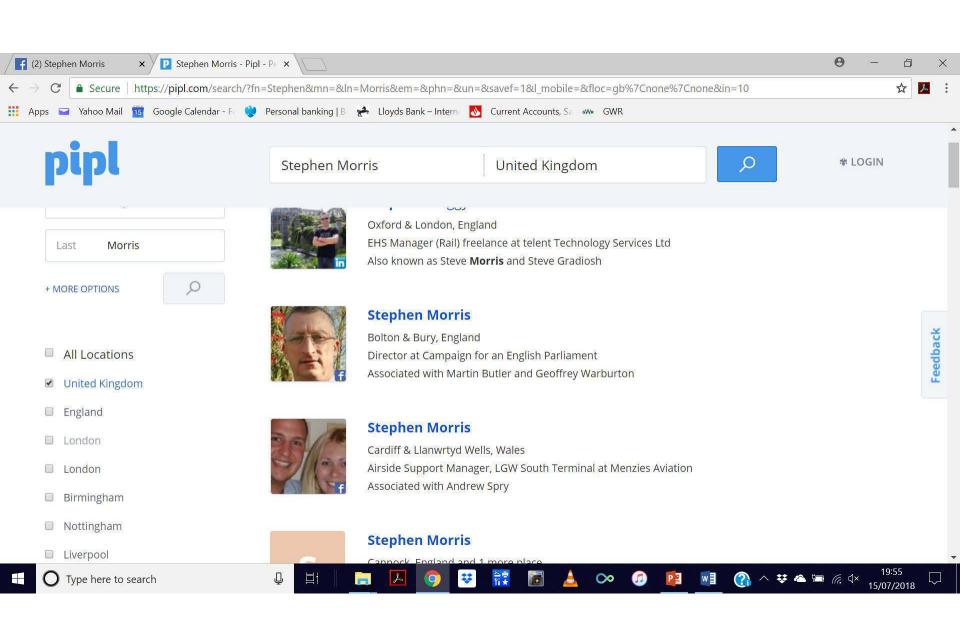
http://www.dogpile.co.uk/

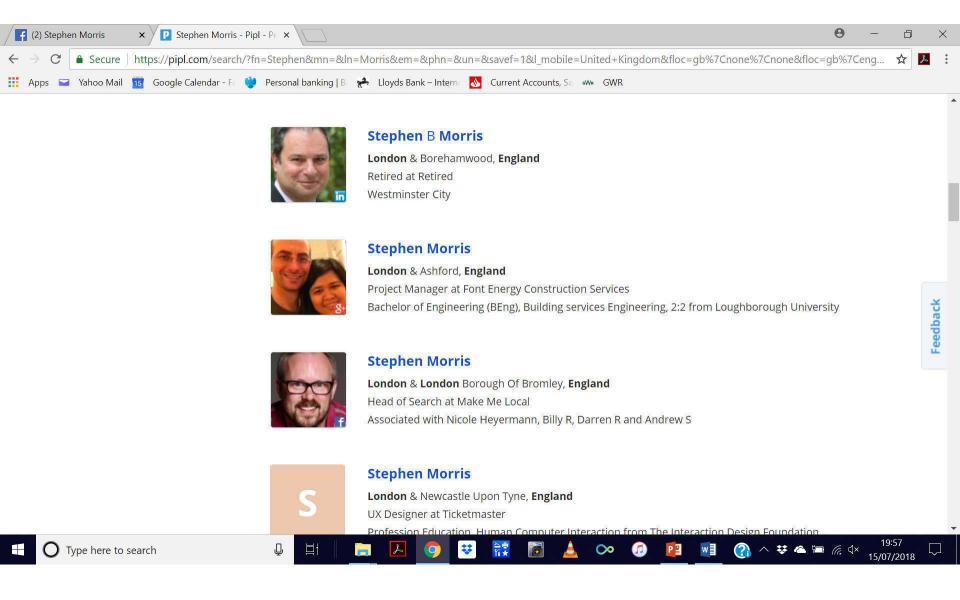


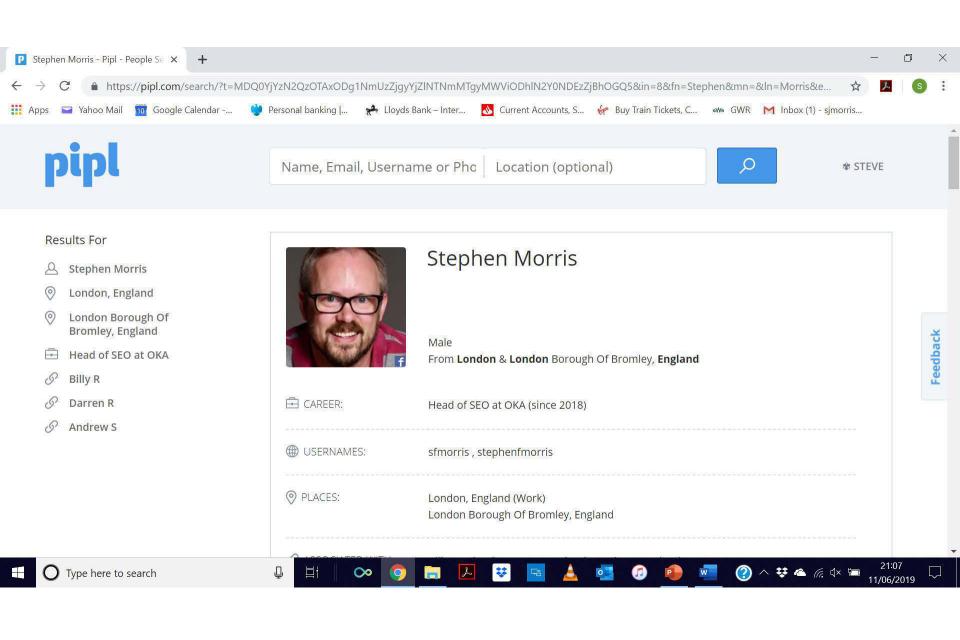


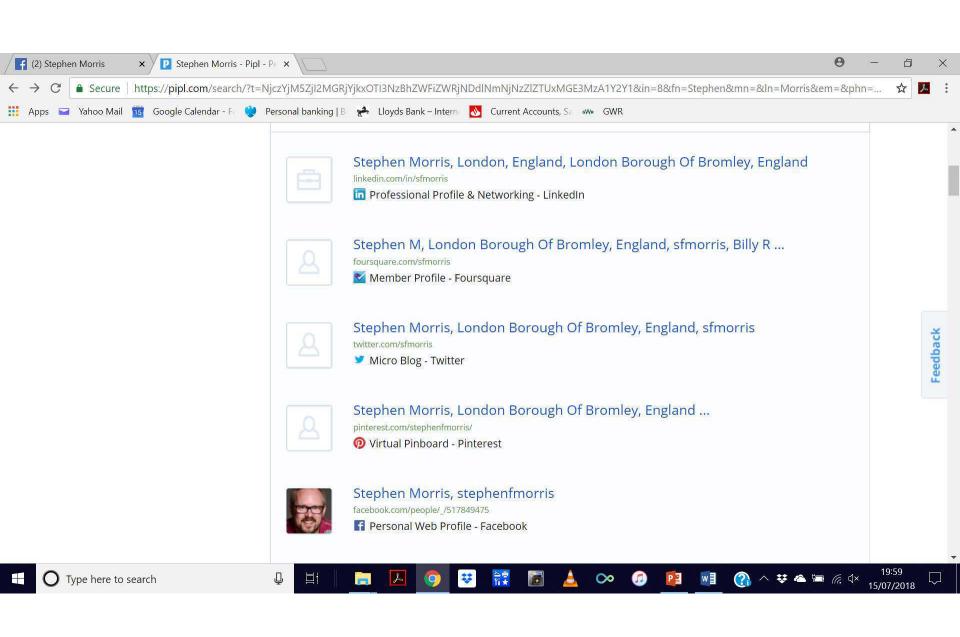
Type here to search

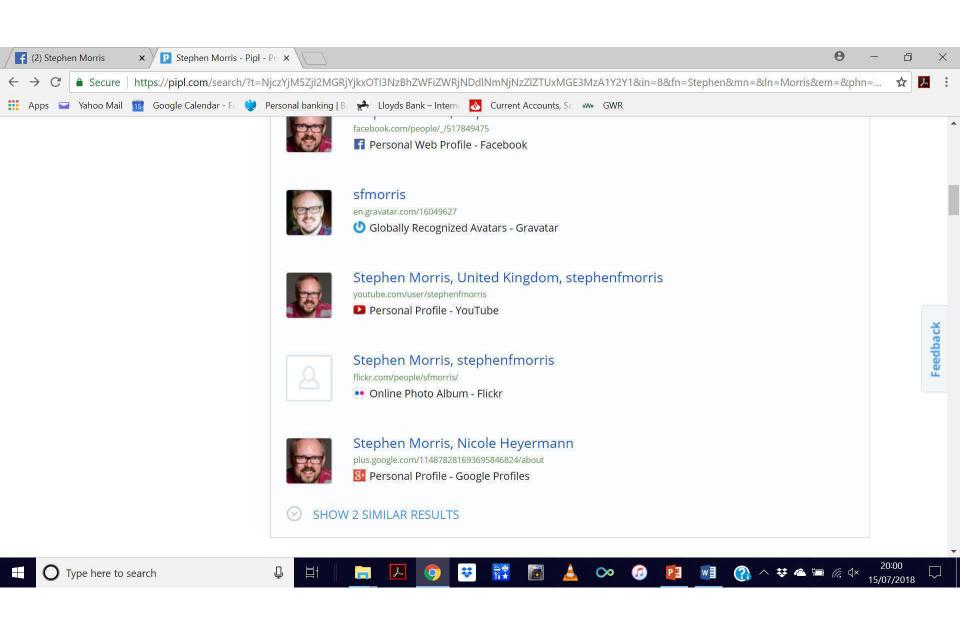


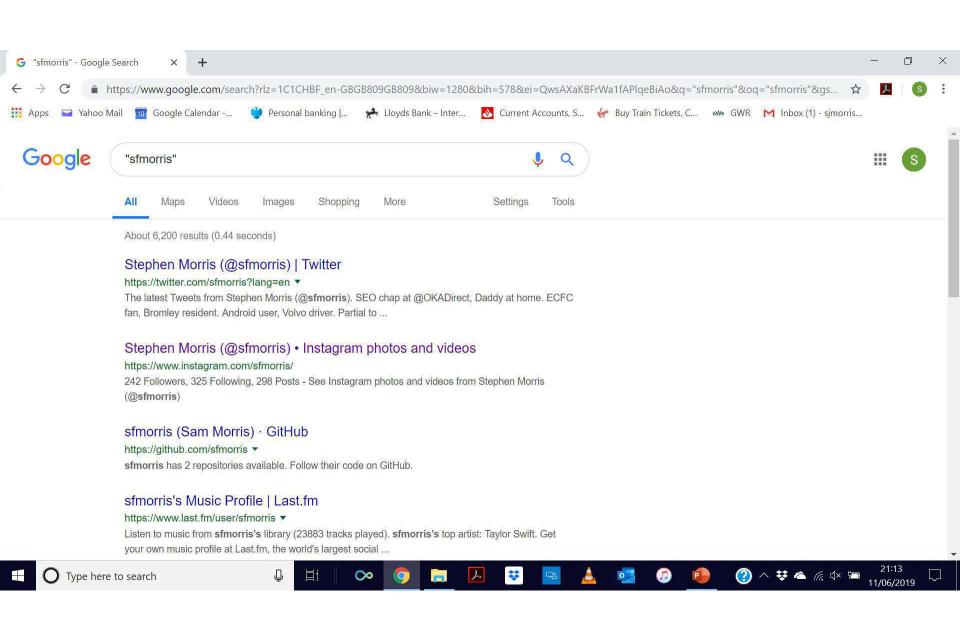


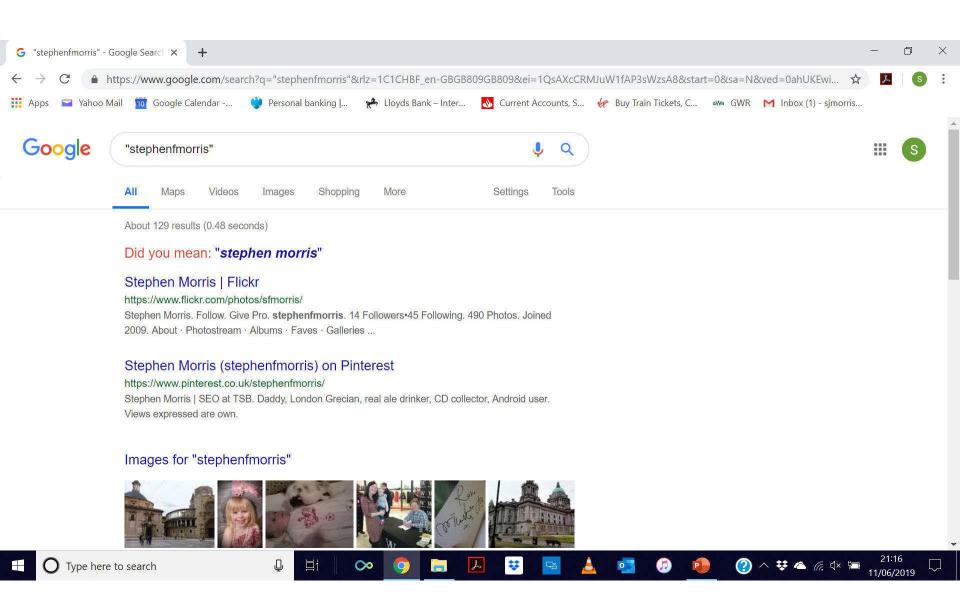


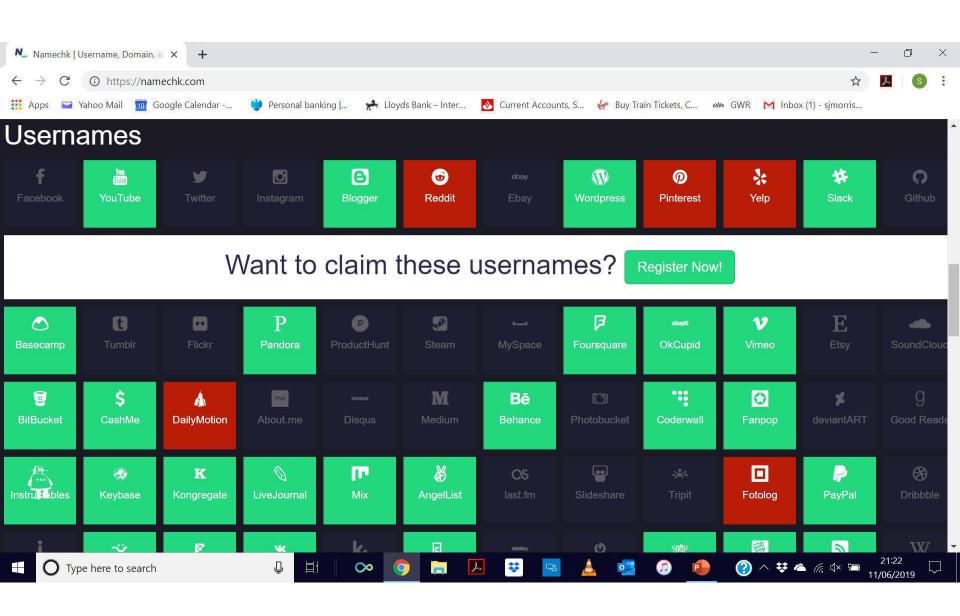


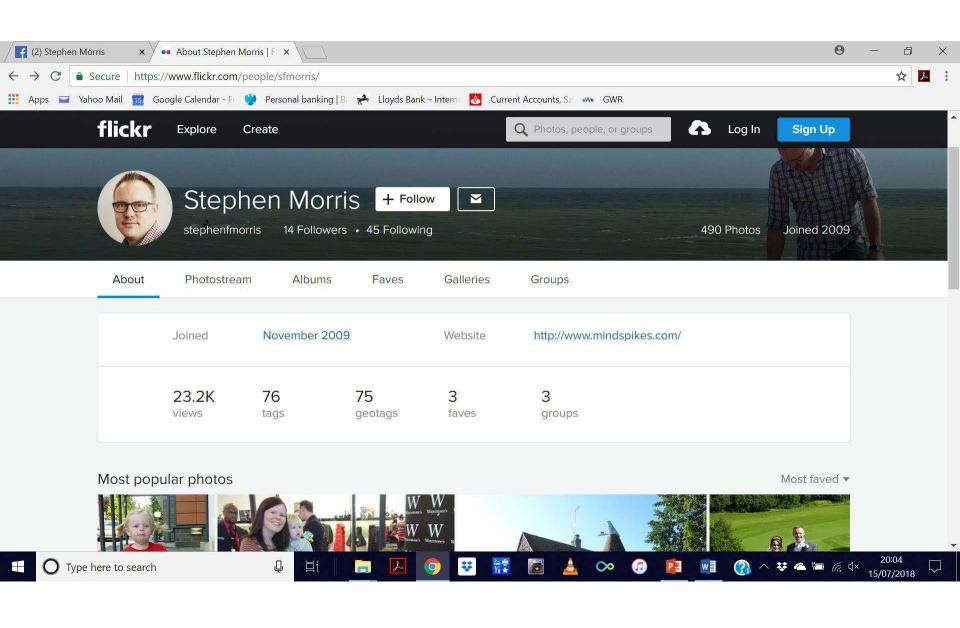


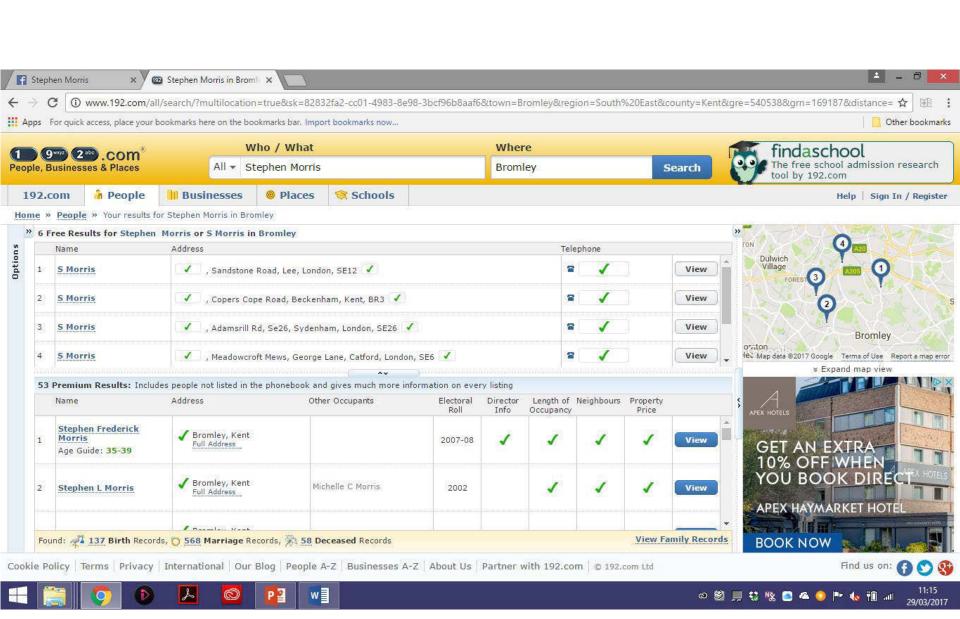




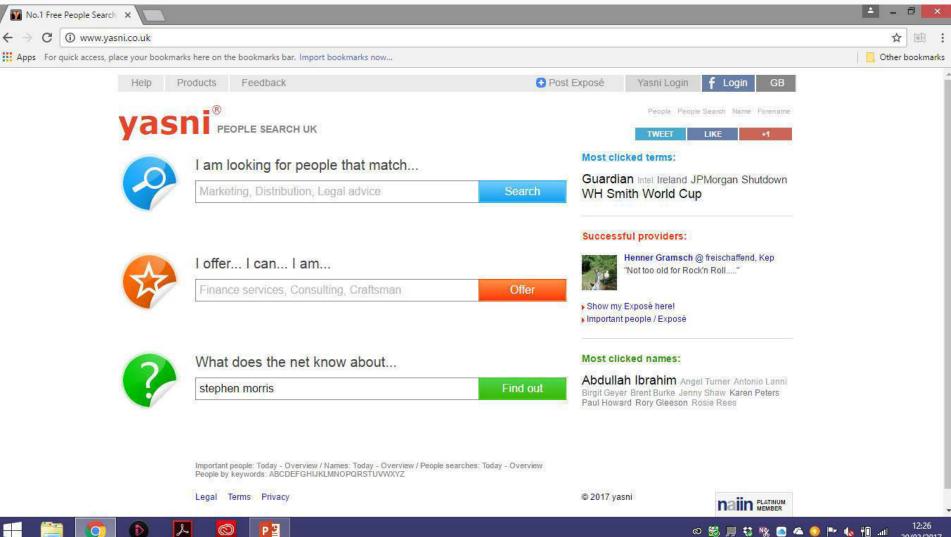






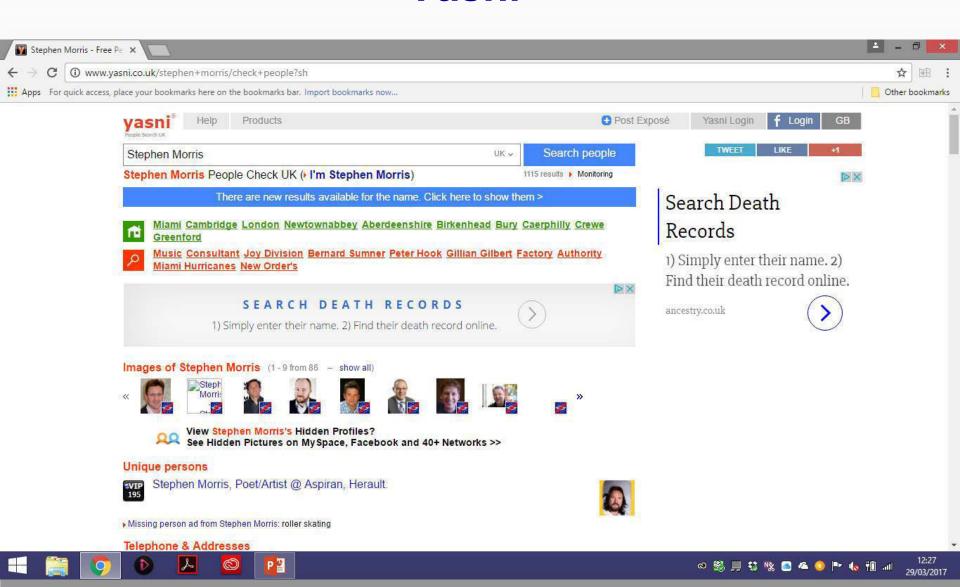


Yasni

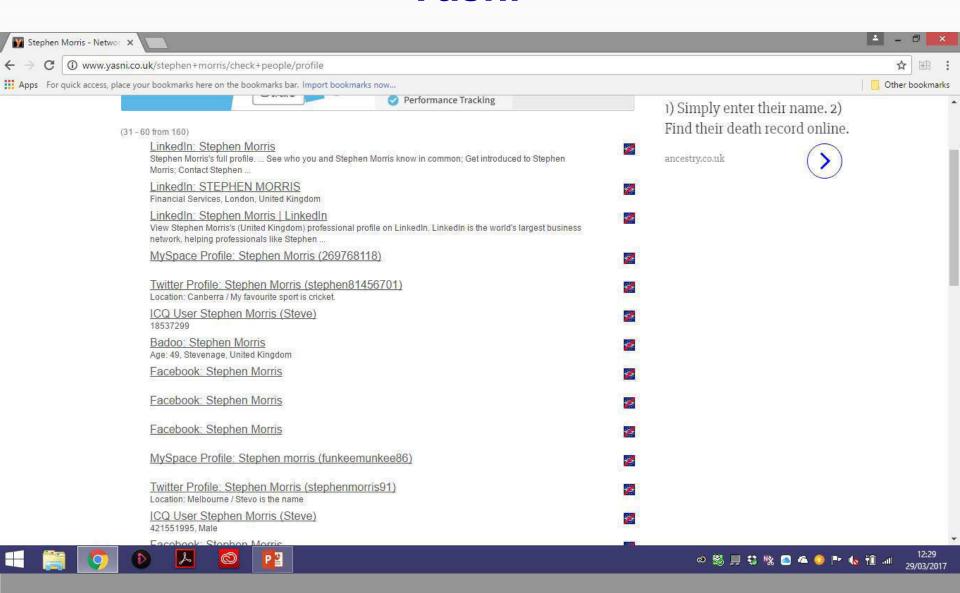




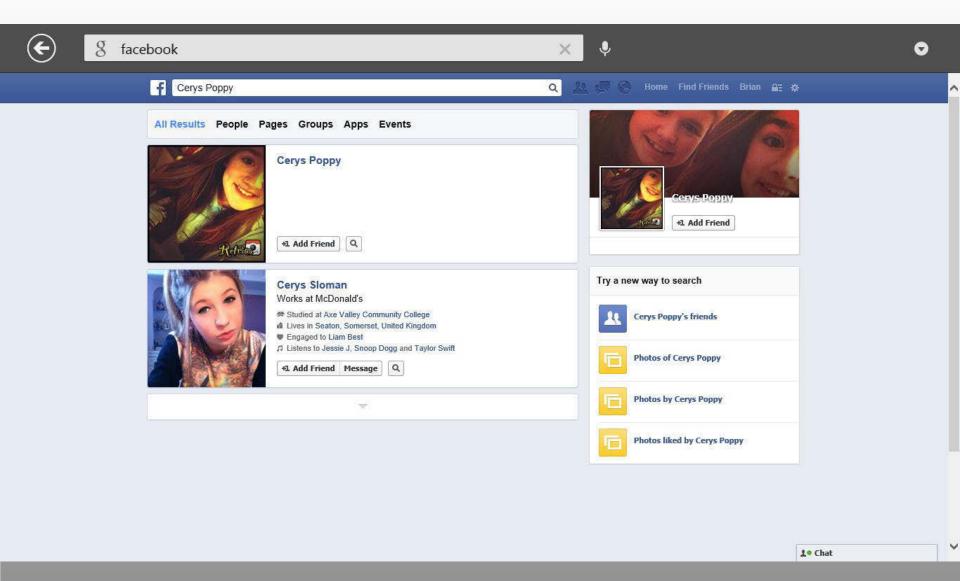
Yasni



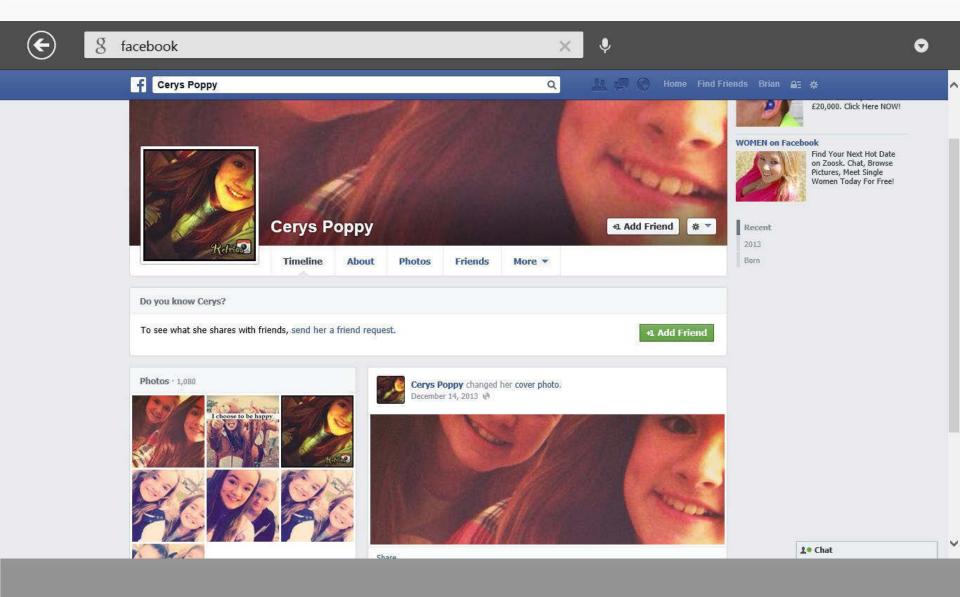
Yasni



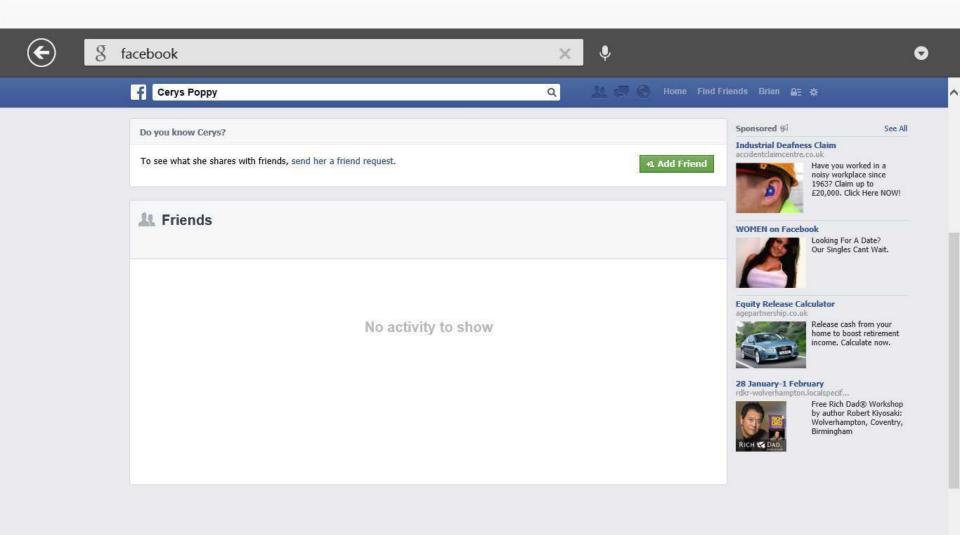
Facebook



Facebook

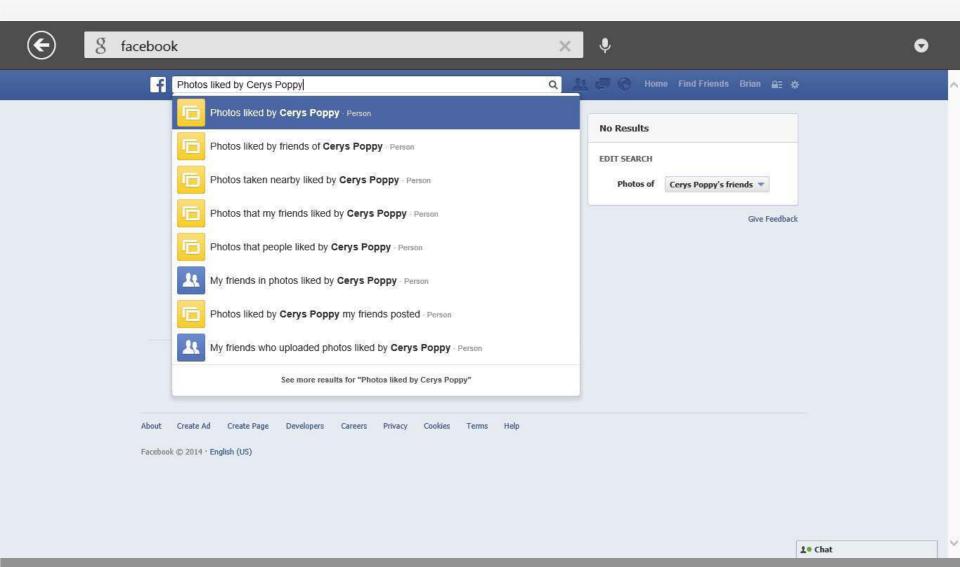


Facebook – Cerys Poppy friends - private

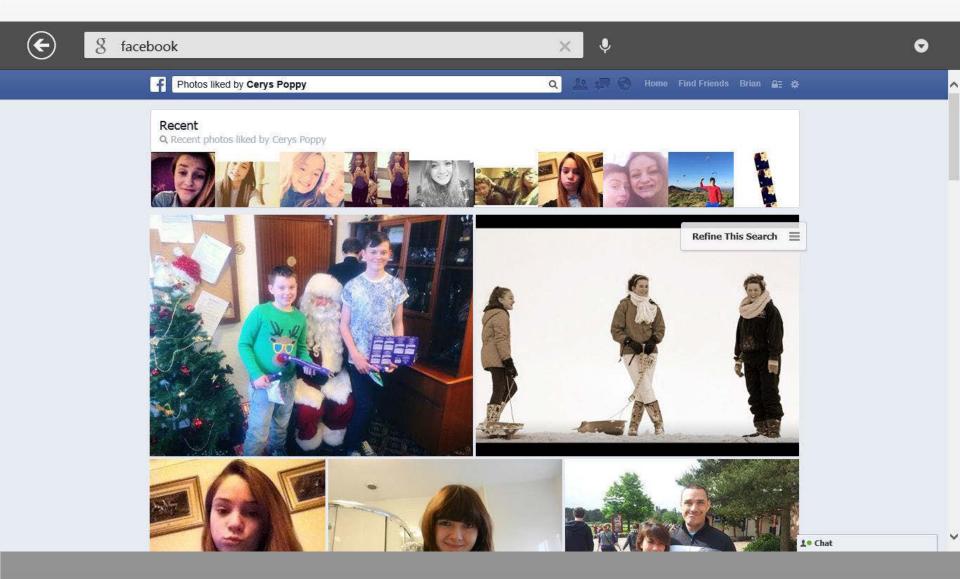


10 Chat

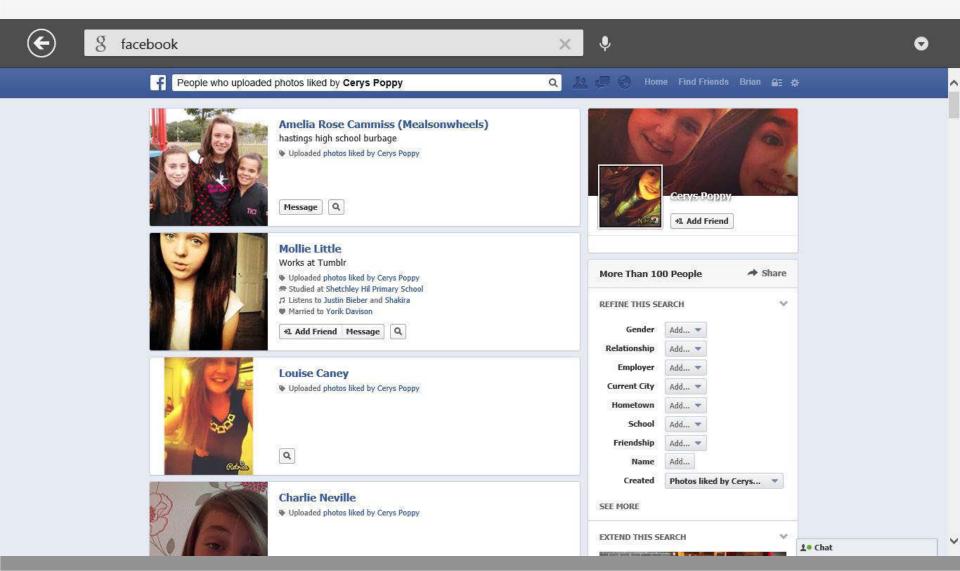
Facebook – search commands - Graphsearch



Facebook – photos liked by Cerys Poppy



Facebook – profile that uploaded these photos – Friends!!



Facebook Searching - Graphsearch

Facebook uses pages and some regular search engine type search criteria as well as other algorithms and settings
Graphsearch
Home page – settings – language settings – language

english us

Facebook Searching

Type all of exactly what you want to search Look for hints as you type Maybe go for final choice on list provided Photos of Photos by Photos liked by Photos commented on by Photos of friends Photos by's friends Friends of etc. etc. Useful to be on an associated profile to ensure a link

Let's get more personal!

Find information set at private through profile settings

Be specific when searching for information relating to people – the Facebook search box finds all photos or all posts or groups for everyone named Stephen Morris

But what if we could find information precisely relating to our specific Stephen Morris, or a business.

Let's get more personal!

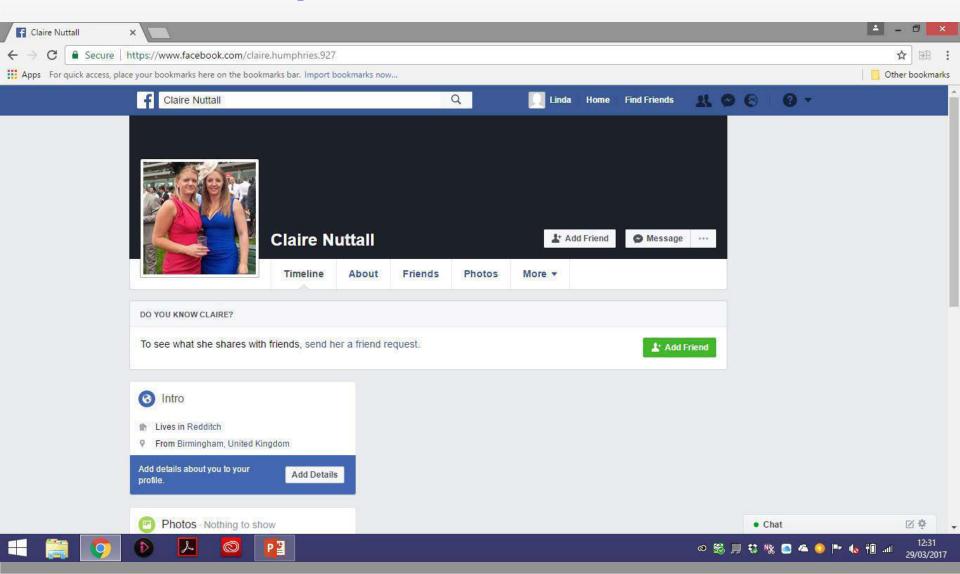
If you have a Facebook profile, you can lock **your door** to the information you know exists

However, you can't lock other doors or corridors across Facebook. Your posts, comments, photos etc etc may be available through other routes

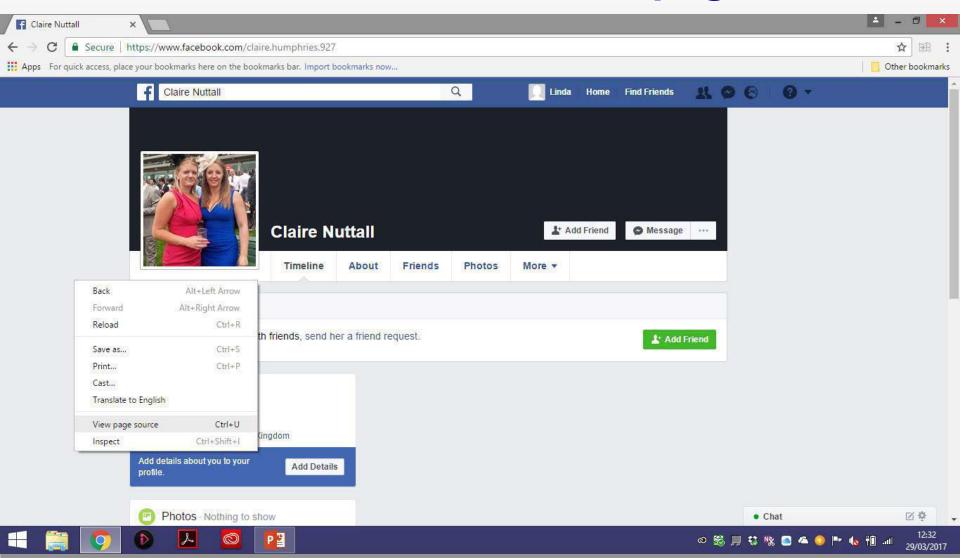
Also, whilst Facebook may (and it is a big may) apply the security you demand through the Facebook search box – there is another way in.

- The URL search bar of your web browser

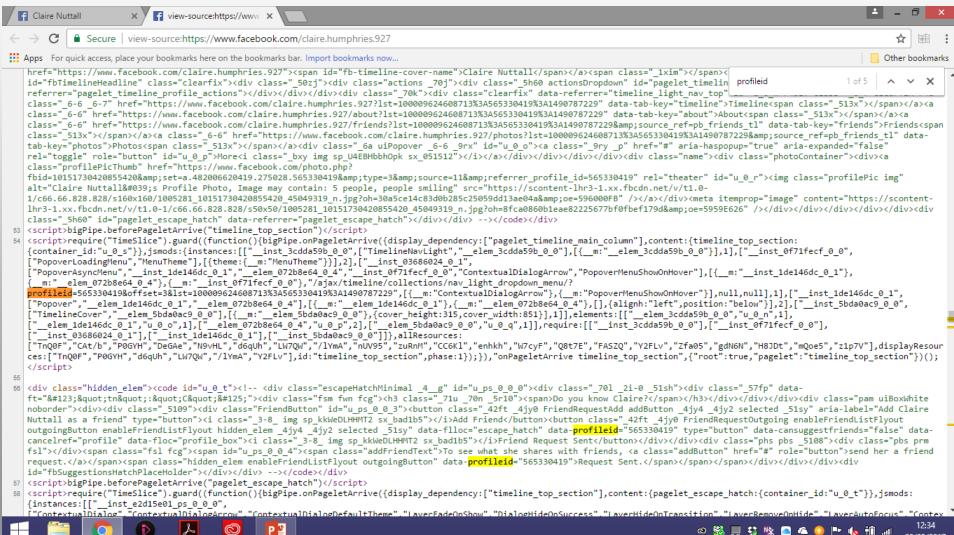
This profile is completely locked down – no friends, photos etc to show



Find the Facebook Profile ID – right click on a blank area. Then click 'View page source'

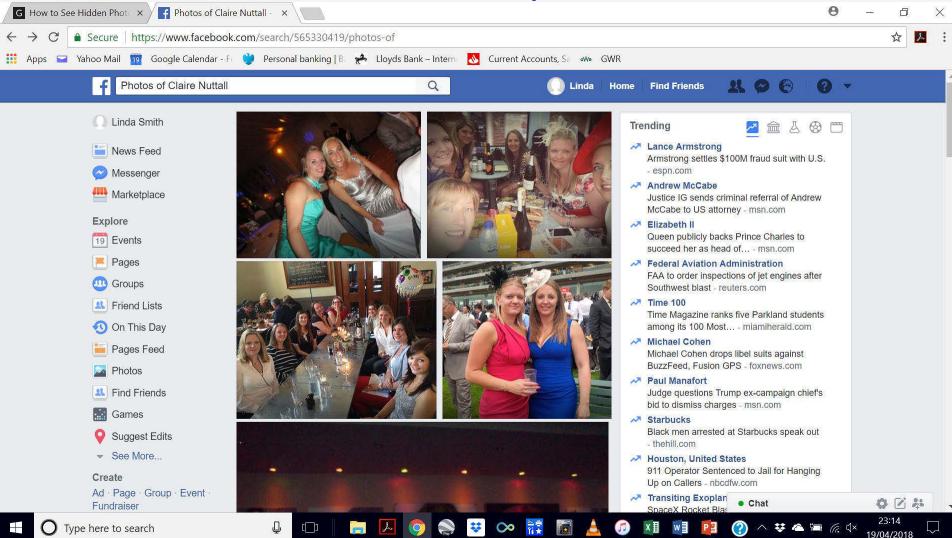


Ctr–F opens a search box – type profileid - then profile ID is 565330419





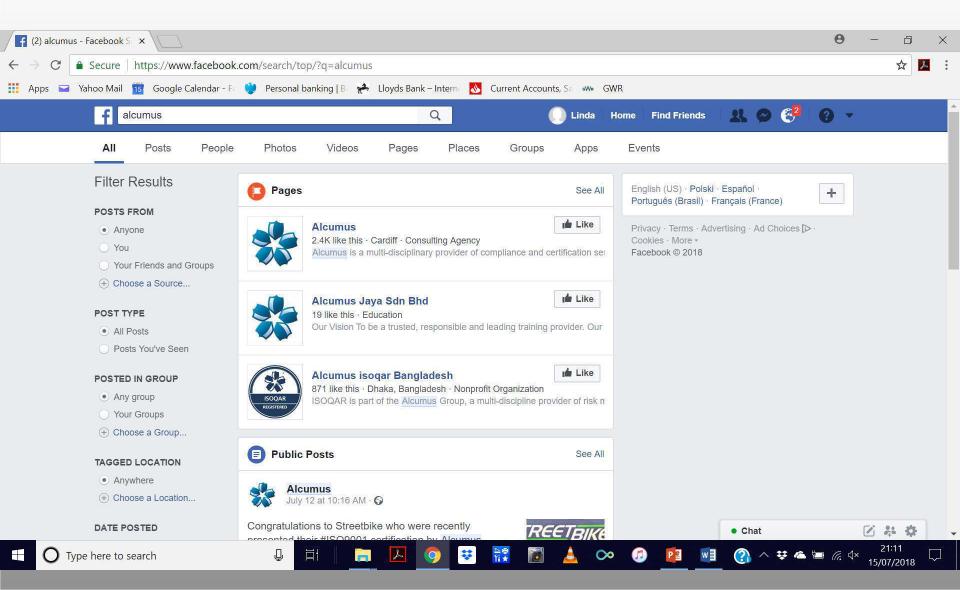
https://www.facebook.com/search/565330419/photos-of *Profiles – comments – places – husband (location and address)*



What about businesses – or even anything that is not a personal profile?

Using the URL browser we can search specific terms on Facebook and also use keywords to find what we are looking for

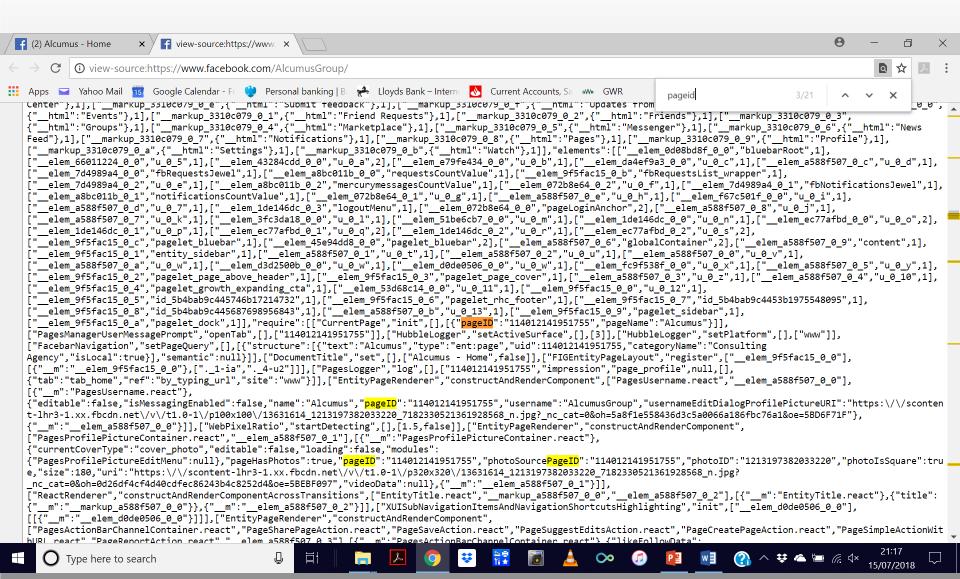
Lets research Alcumus – Type a search in the facebook search box



Employees and other activity not visible directly from here, so – view page source

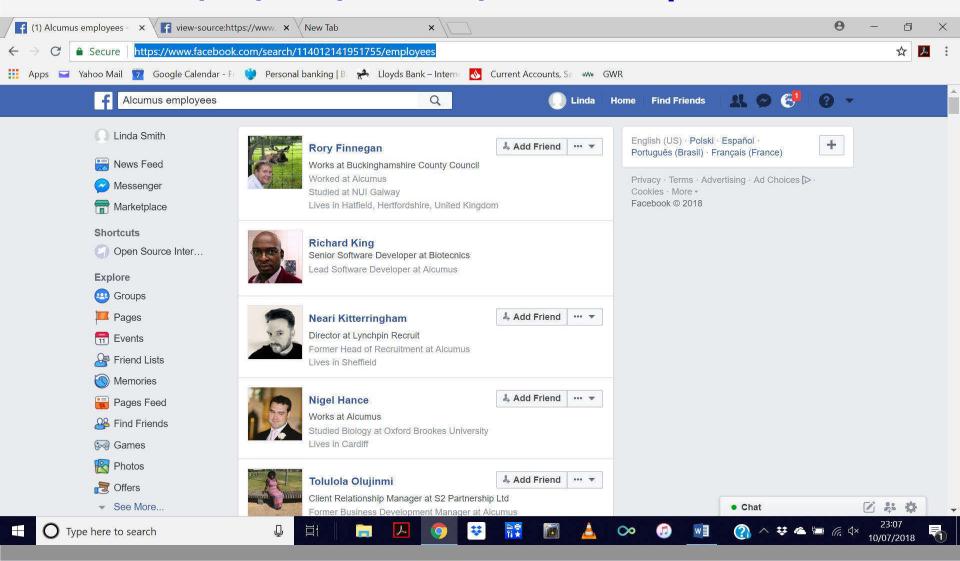


This is not a profile – it is a page So the command is pageid

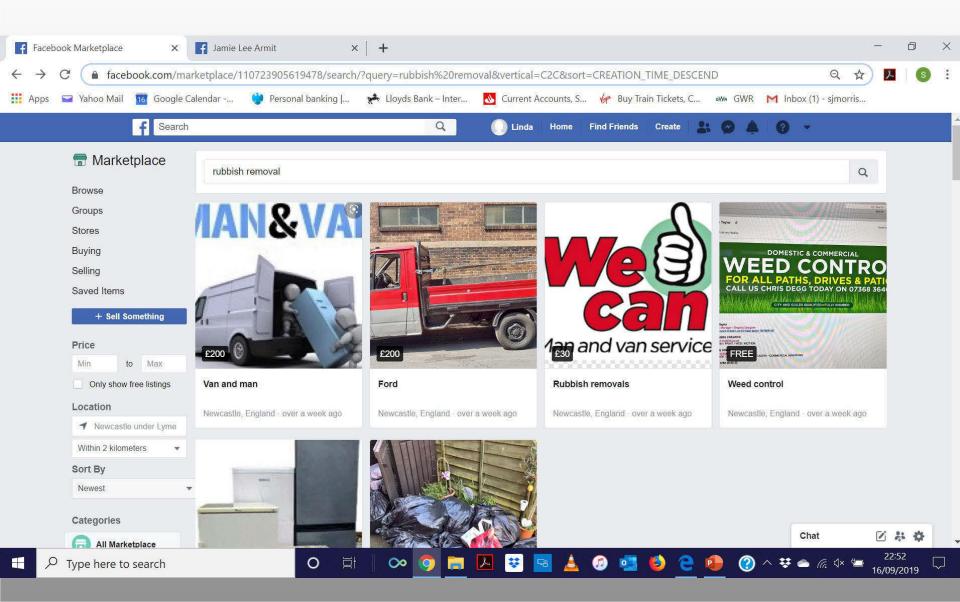


https://www.facebook.com/search/114012141951755/employees

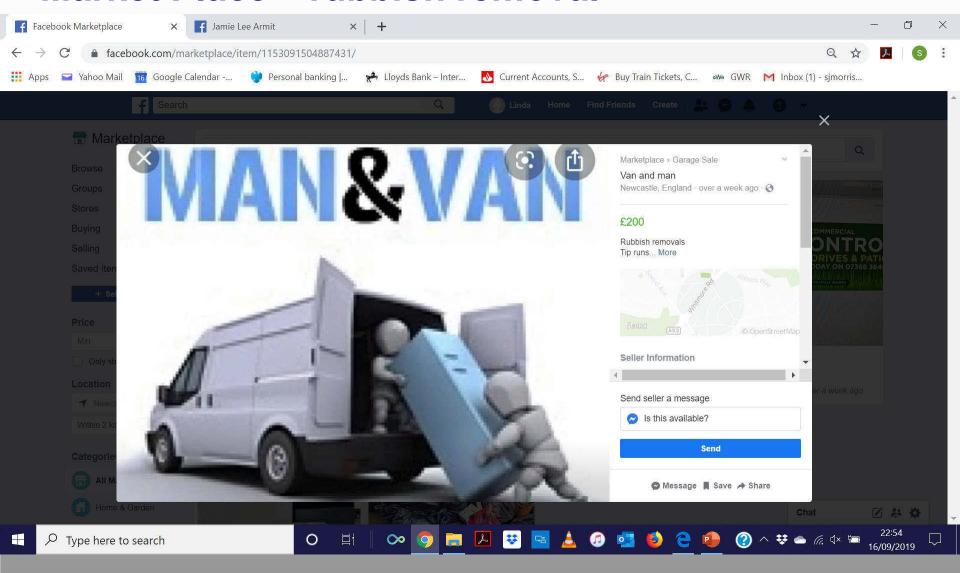
about 135 people - personal profiles and personal data



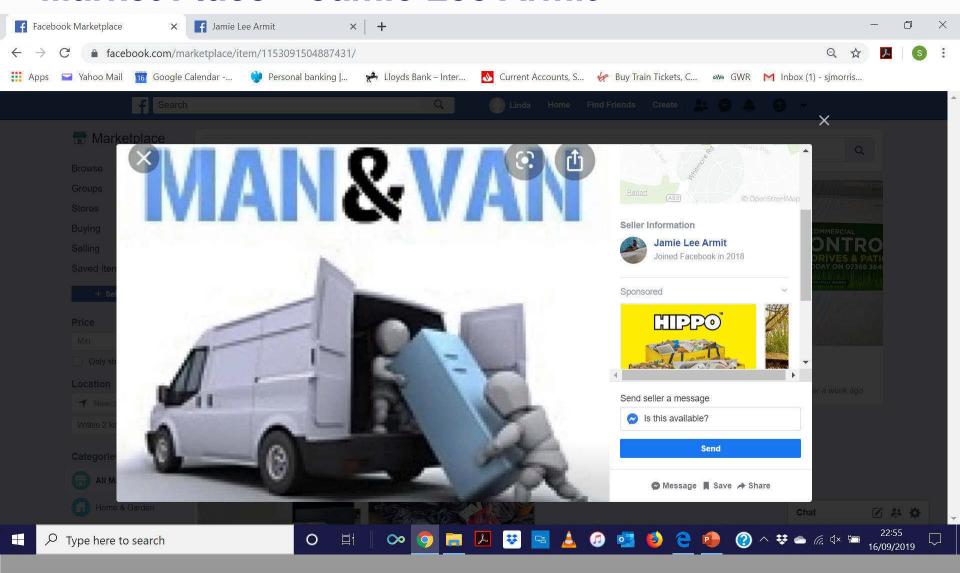
Market Place - rubbish removal



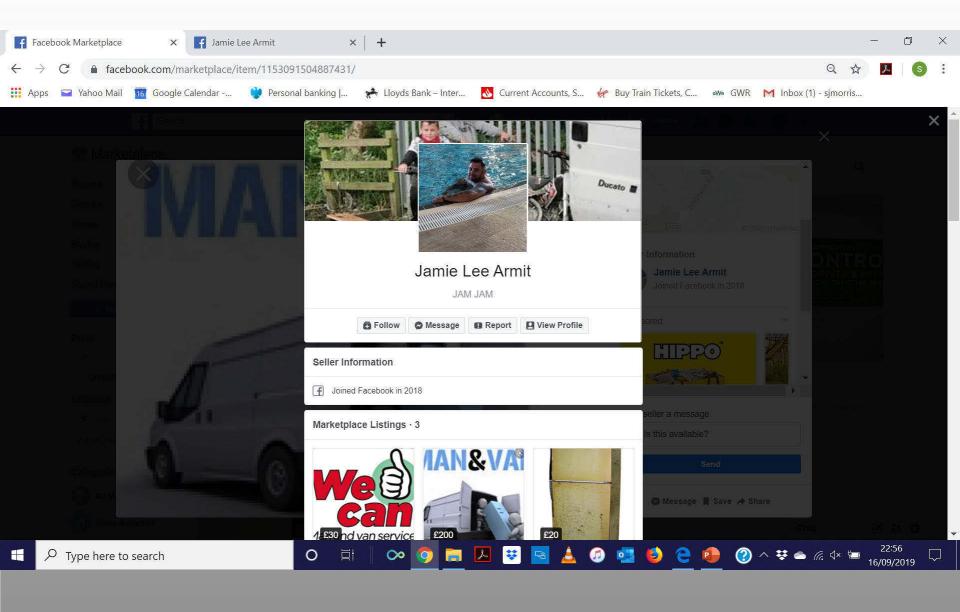
Market Place - rubbish removal



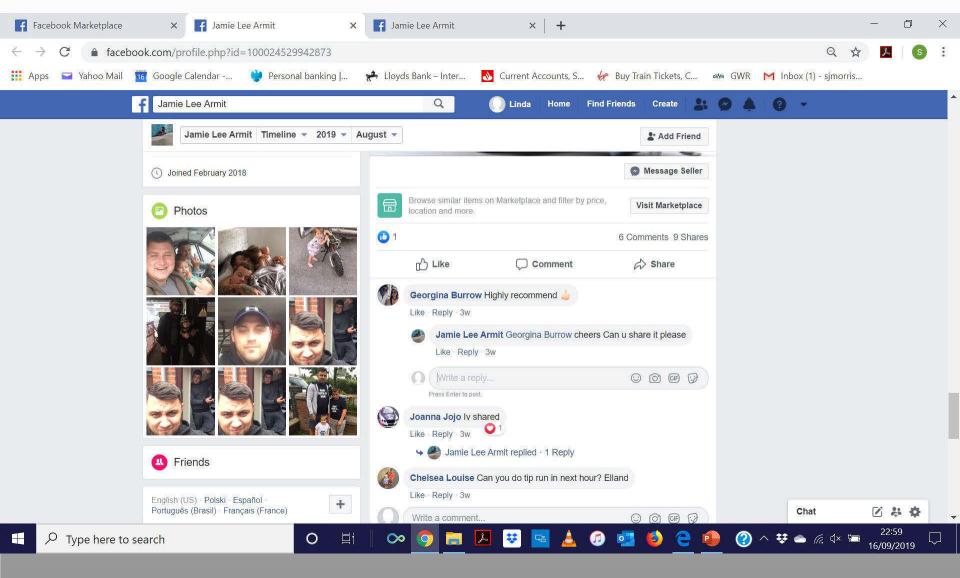
Market Place – Jamie Lee Armit



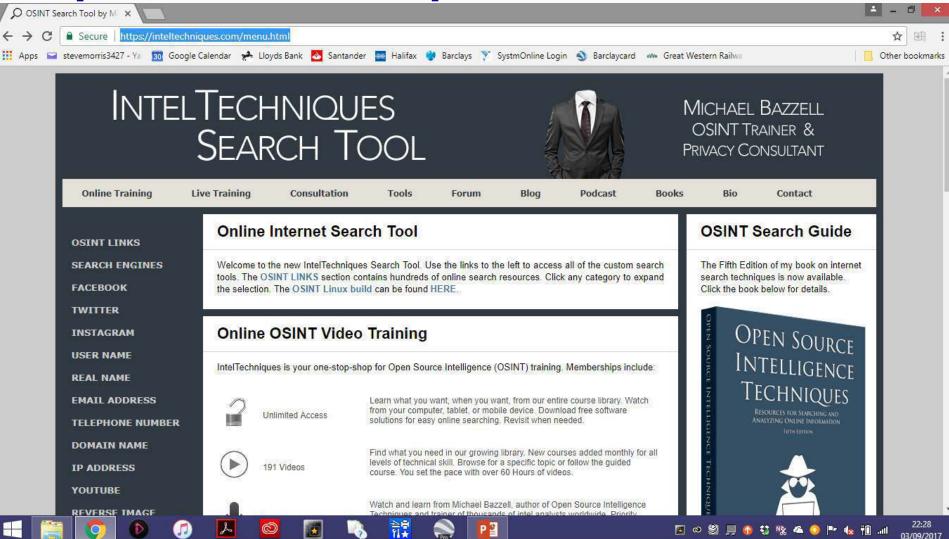
Market Place – Jamie Lee Armit



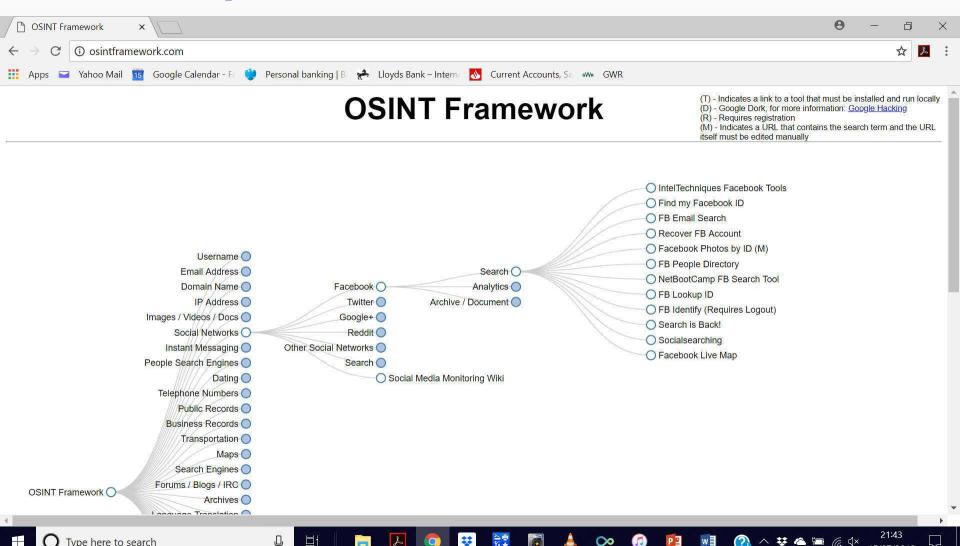
Personal Profile - Jamie Lee Armit



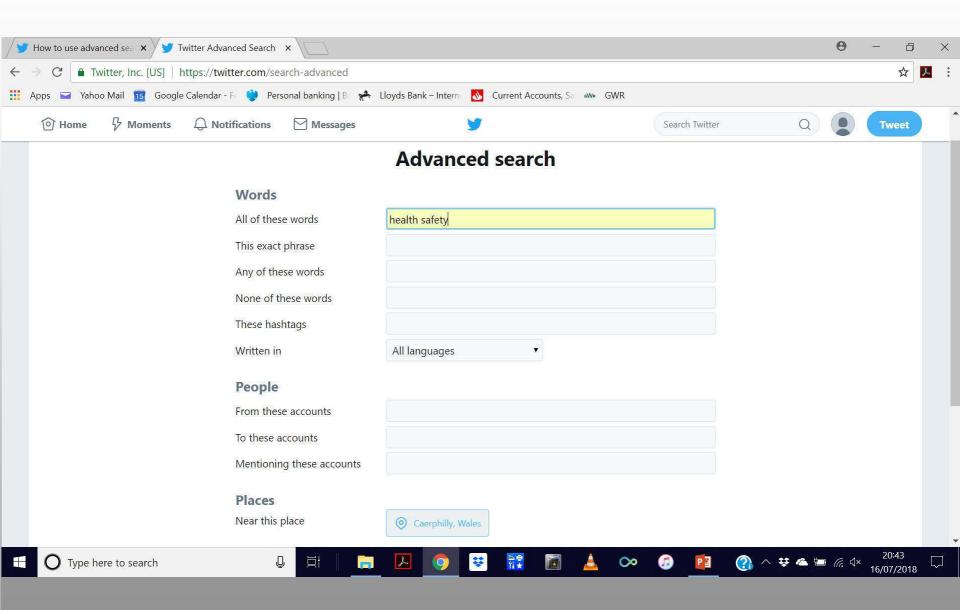
https://inteltechniques.com/menu.html



http://osintframework.com/



Twitter - Click ADVANCED SEARCH - enter data



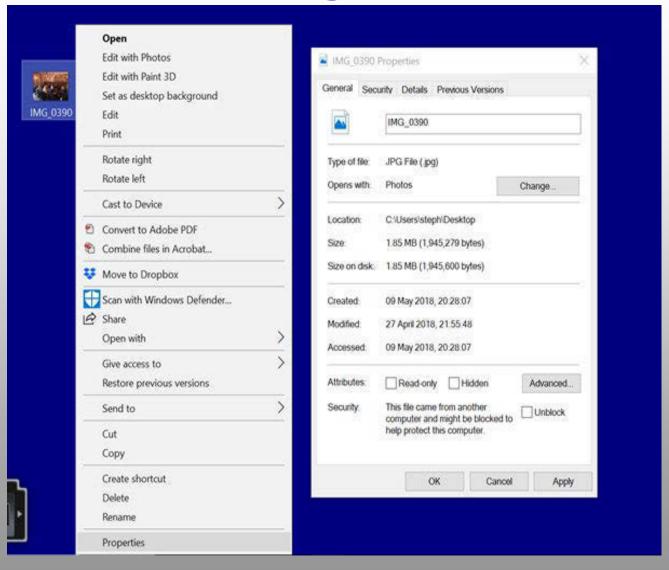
Next steps

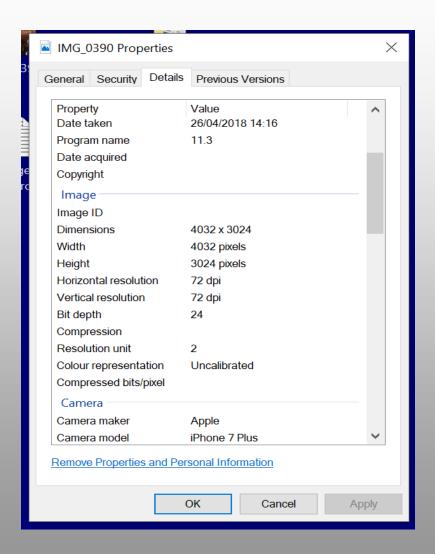
- Obtain an email address
- Open accounts/profiles
- Adjust your settings
- Will need a mobile number for authentication

First - Terminology

- JPEG, TIFF, GIF, PNG, Raw
- Metadata
- EXIF
- GPS Co-ordinates (percentages or degrees)
- Facial recognition
- Machine learning
- Processing software (adobe elements etc)

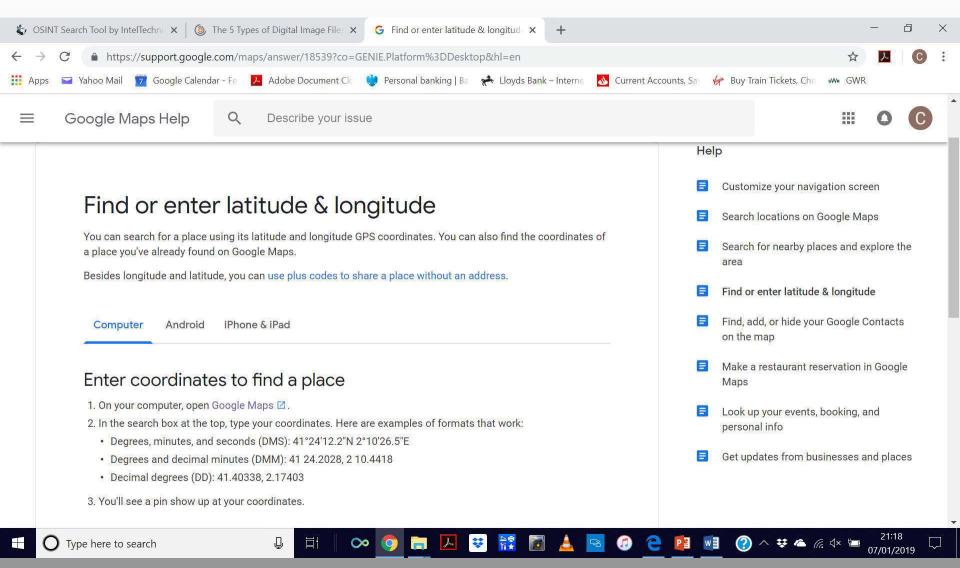




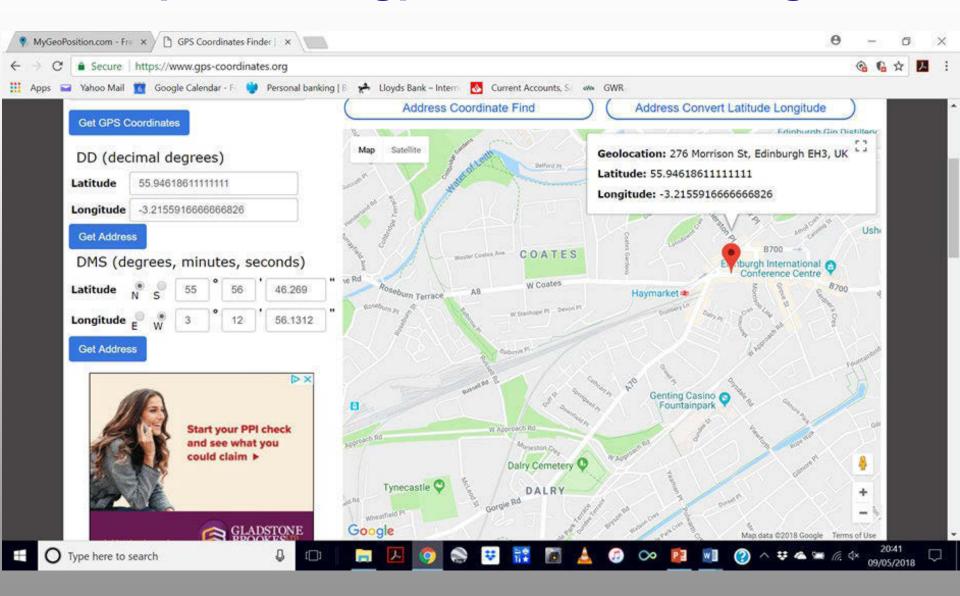


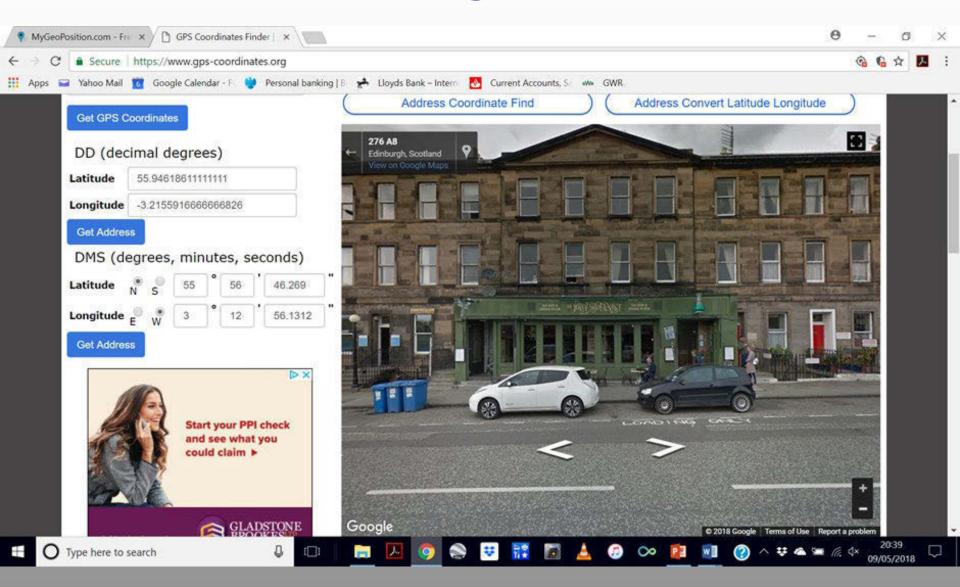


Google maps help

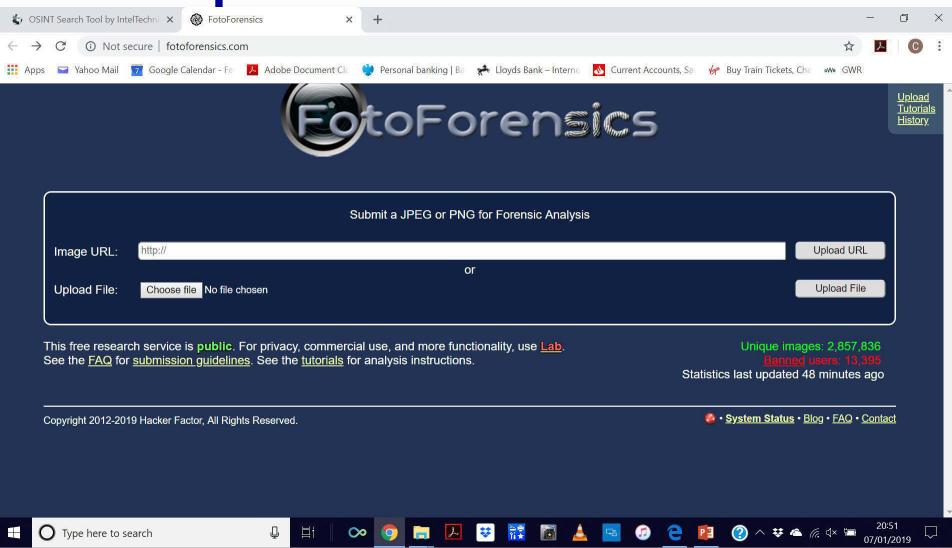


https://www.gps-coordinates.org/

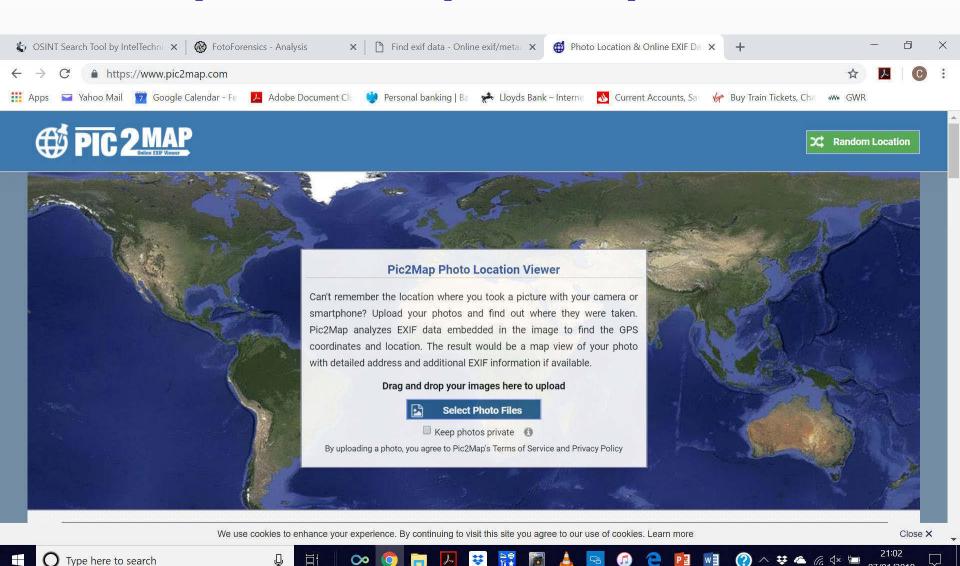




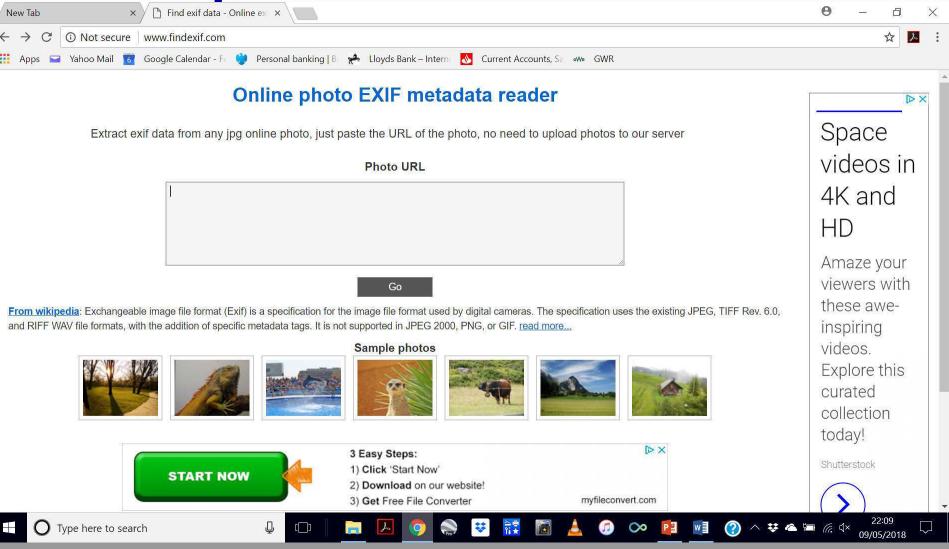
http://fotoforensics.com/



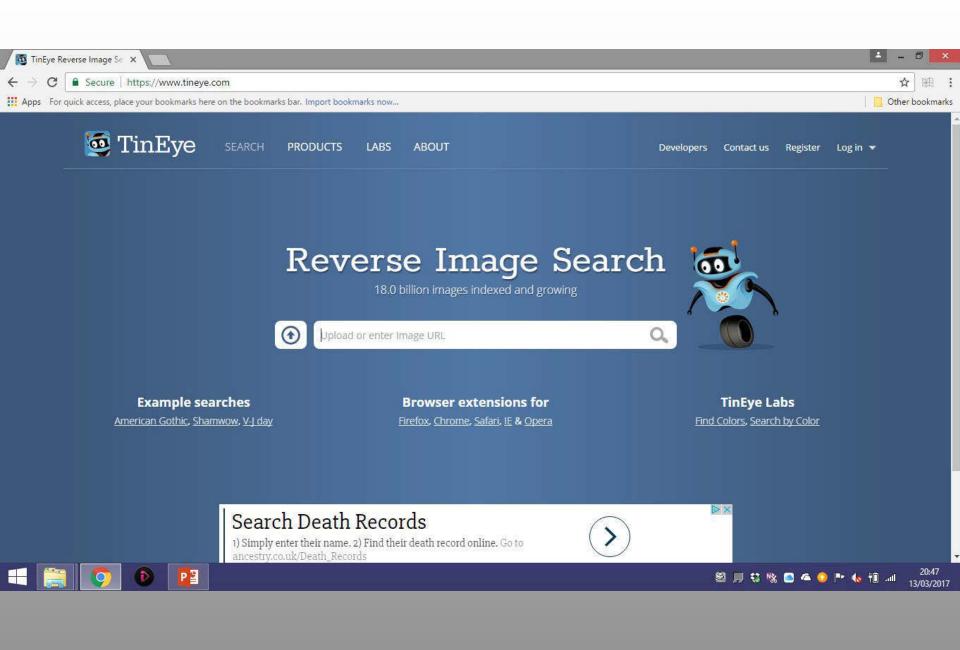
https://www.pic2map.com/

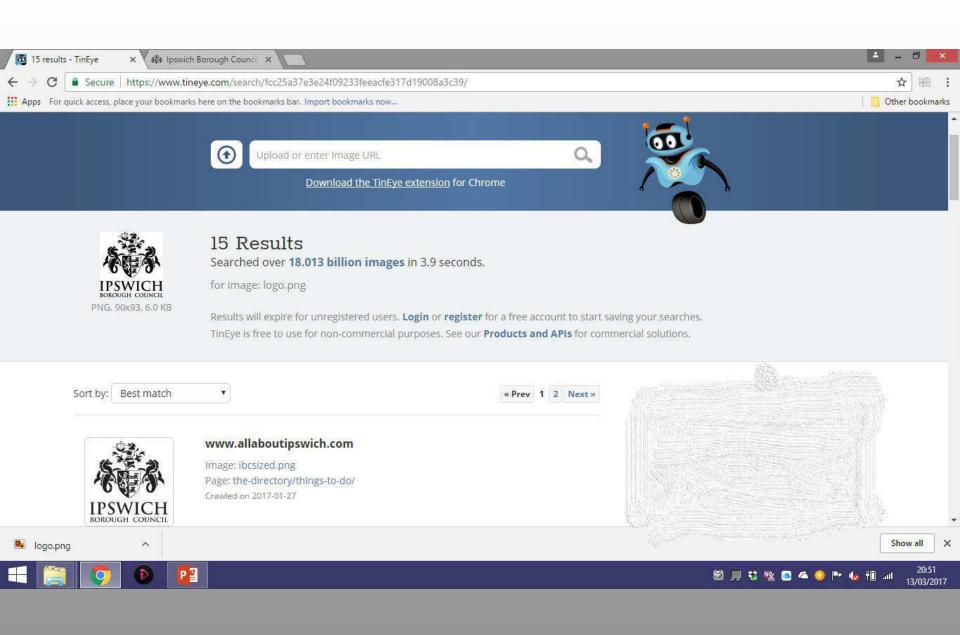


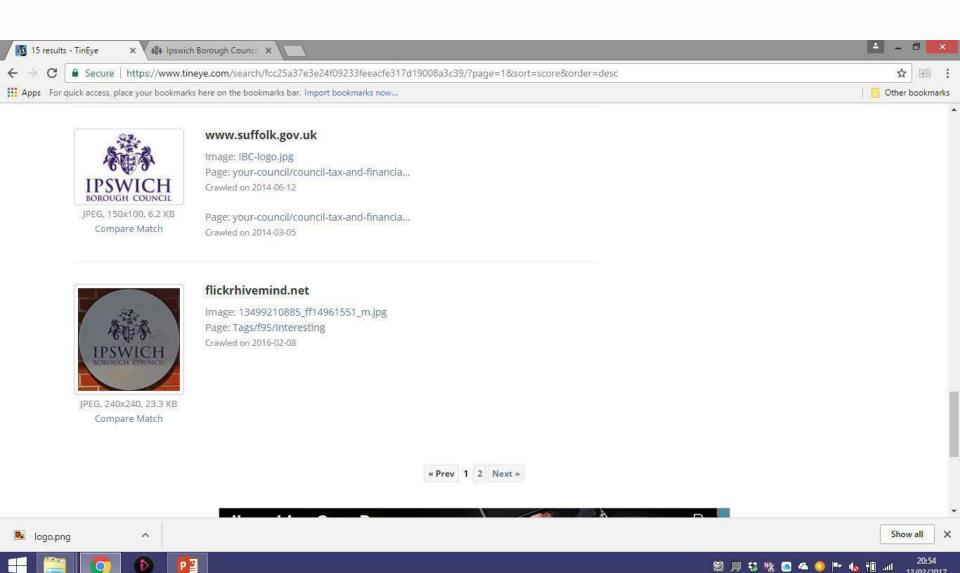
http://www.findexif.com/



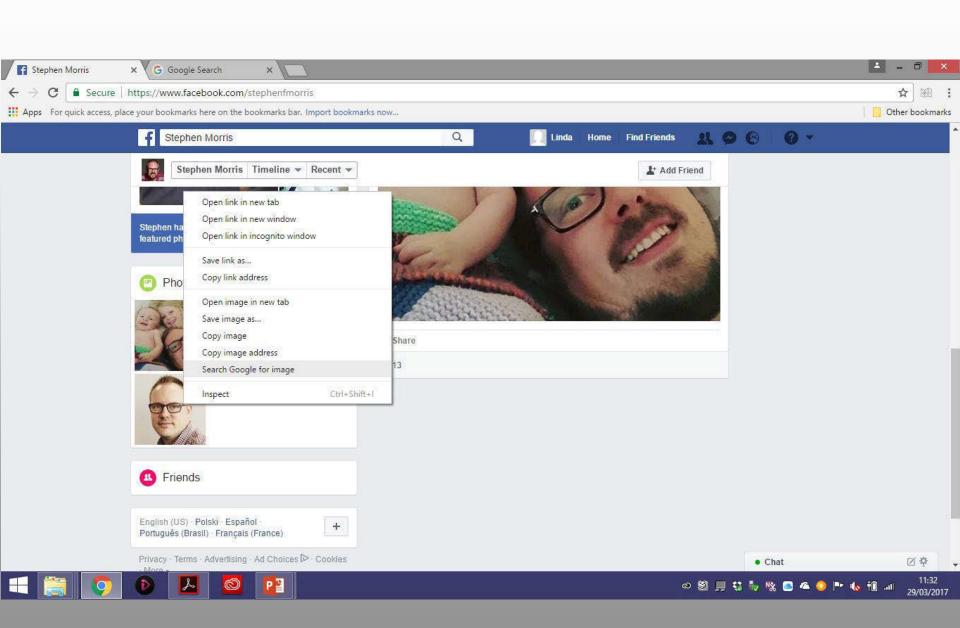








13/03/2017





Report images

Pages that include matching images

Bromley SEO Event - September 2015 - Shine Search



shinesearch.co.uk/blog/bromley-seo/ ▼ 400 × 400 - 11 Sep 2015 - September 10th 2015 marked the first proper meeting of 3 current or former SEO professionals in our local town of Bromley, South East London ...

UEFA 5 star stadium certification | Five stars. Posh stadium... | Flickr



https://www.flickr.com/photos/sfmorris/4179342448 48 × 48 - Five stars. Posh stadium, this Camp Nou.

Nou Estadi Castalia | Home of Club Deportivo Castellón. | Stephen ...



https://www.flickr.com/photos/sfmorris/4387809955 48 × 48 - 20 Feb 2010 - Home of Club Deportivo Castellón.

Bonka Bones | Bones and a cup of Bonka. | Stephen Morris | Flickr



https://www.flickr.com/photos/sfmorris/4178579237 48 × 48 - Bones and a cup of Bonka.

Camp Nou dugouts | Well protected, these. Alex Ferguson woul... | Flickr



https://www.flickr.com/photos/sfmorris/4179352326 48 × 48 - Well protected, these. Alex Ferguson would be happy.

















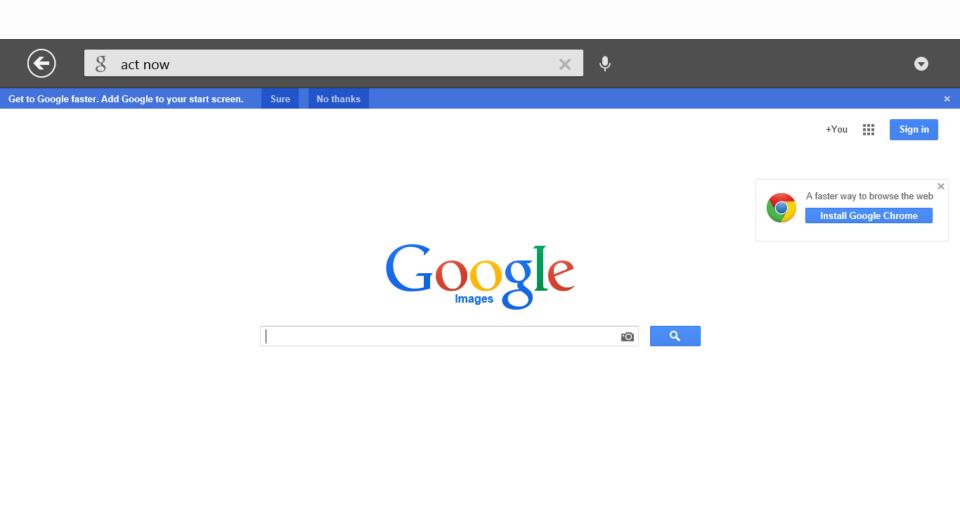












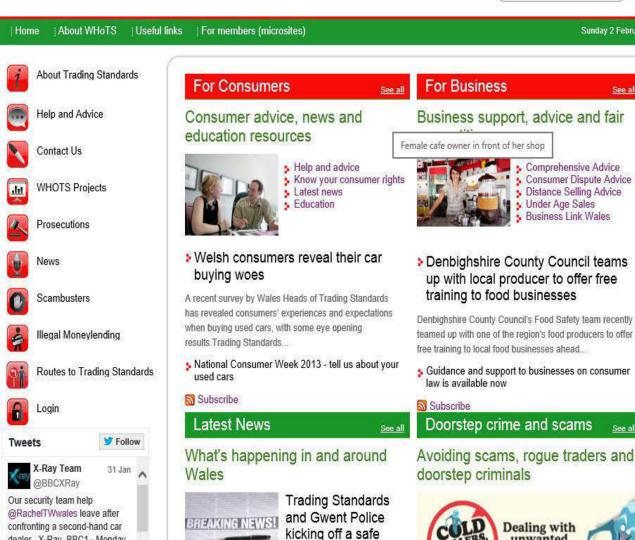
Advertising Business About New Privacy & Terms Settings Google.co.uk





Sunday 2 February 2014

See all









unwanted



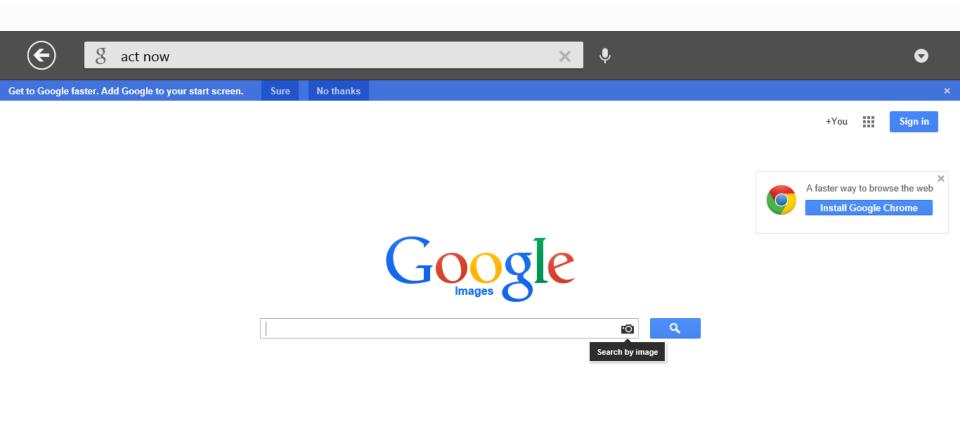
See all



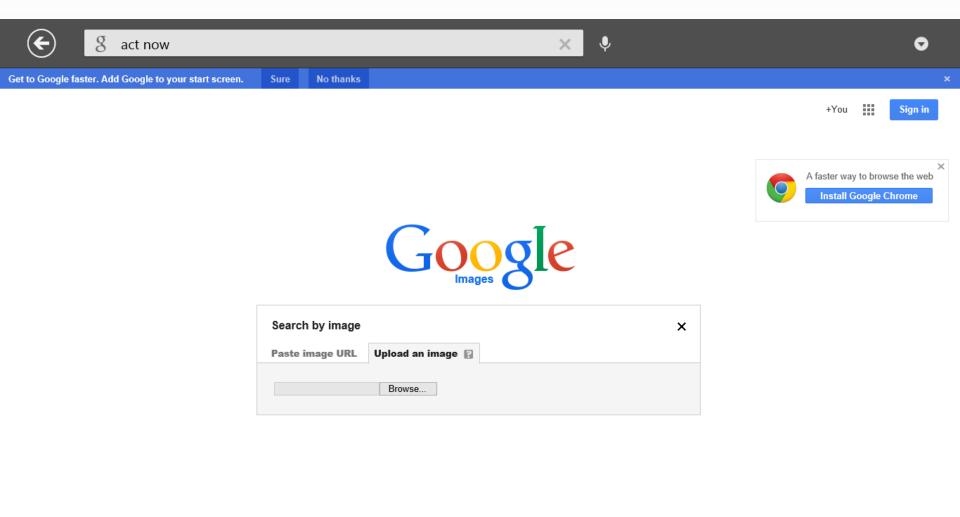




dealer. X-Ray, BBC1 - Monday



Advertising Business About New Privacy & Terms Settings Google.co.uk



New Privacy & Terms

Settings

Google.co.uk

About

Business

Advertising

Small businesses are normally privately owned corporations, partnerships, or sole proprietorships. What constitutes "small" in terms of government support and ...

Visually similar images - Report images



Pages that include matching images

How Congress Can Boost Small Business in 2014 - US News and ...



www.usnews.com > News -

620 × 413 - Dec 17, 2013 - Business advocates are hoping the proposed budget deal will provide funding and stability to small businesses in 2014. If your New Year's ...

Small Business | The Fiscal Times



www.thefiscaltimes.com > Life + Money > Career Economics > 146 × 82 - Get small business news and articles about startups, entrepreneurs and more with The Fiscal Times.

Small Business Financial Development Corporation Of Orange County



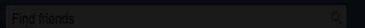
sbfdoc.com/ •
950 × 360 - The Small Business Disaster Loan Guarantee Program helps agriculture-related enterprises and other small businesses obtain financing needed to recover ...

Small Business Saturday: AmEx Marketing Ploy? | The Fiscal Times



www.thefiscaltimes.com > Business + Economy •

592 × 333 - Nov 30, 2013 - American Express's Small Business Saturday campaign is an obvious win for Main Street, but is the company's own bottom-line boost getting in ...







Karen Upton

7 September 2013 · 🚱

Share

2 people like this.



Alison Davies This is fantastic! ! Where is this?

9 May 2014 at 08:31

Sponsored 🛒

Create Advert



Adobe Creative Cloud

creative.adobe.com

Save 40%. All new apps & training in the latest release of Creative Cloud. Join now.

























https://www.google.com/search?tbs=sbi:AMhZZiuOR4QxBkCkuVvfsWv4Fb48fc6rfRagBHGBwcLIF8vkfHTOuGyuUg-kTdlqxisQUJjdztzrjRYwKK1Khygiw6RzW4WsWQr9Seerlt





Image size: 960 × 720

Find other sizes of this image: All sizes - Medium

Best guess for this image: european castles

List of castles in Europe - Wikipedia, the free encyclopedia

en.wikipedia.org/wiki/List_of_castles_in_Europe -Below are lists of castles in Europe, organized by country: Sovereign states[edit]. Charlottenburg Palace, Berlin, Germany. Windsor Castle, England, United ...

European - Exploring Castles

www.exploring-castles.com/european castles.html • European Castles have caused wars; inspired fairytales; and defined entire nations. Europe is the birthplace of the castle, and is home to the vast majority of ...

Visually similar images

Report images









































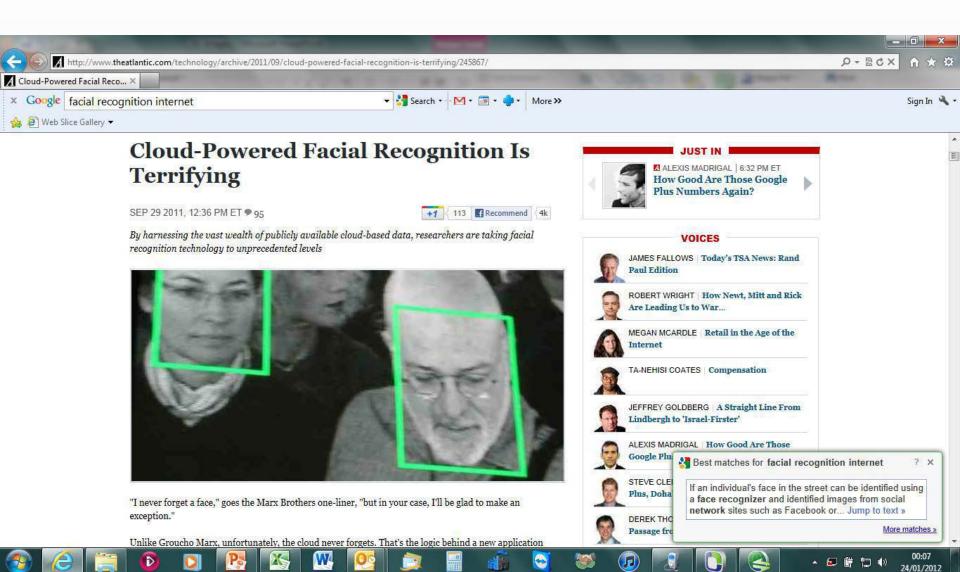


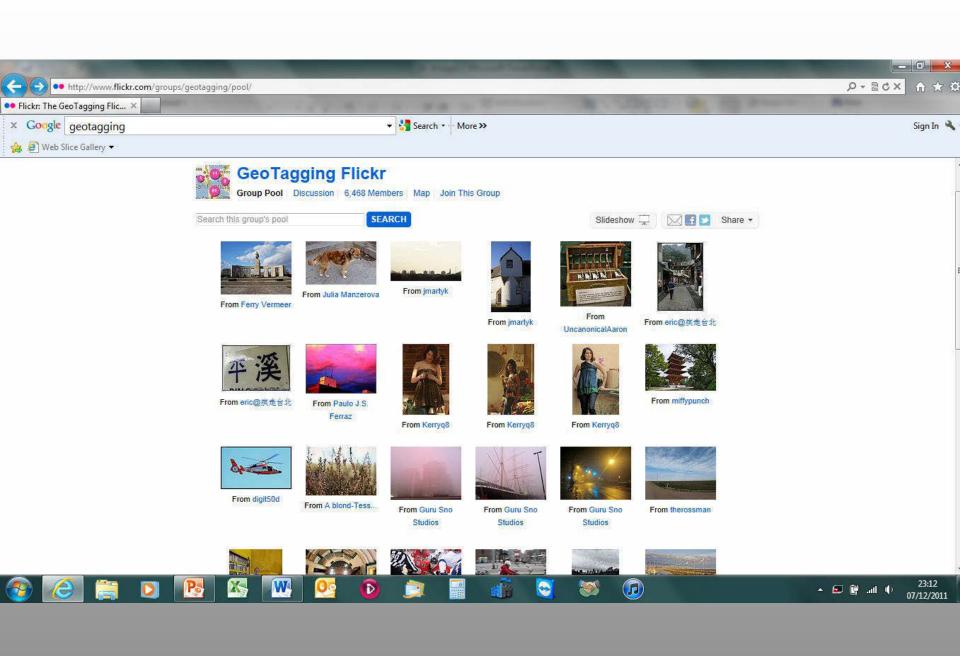


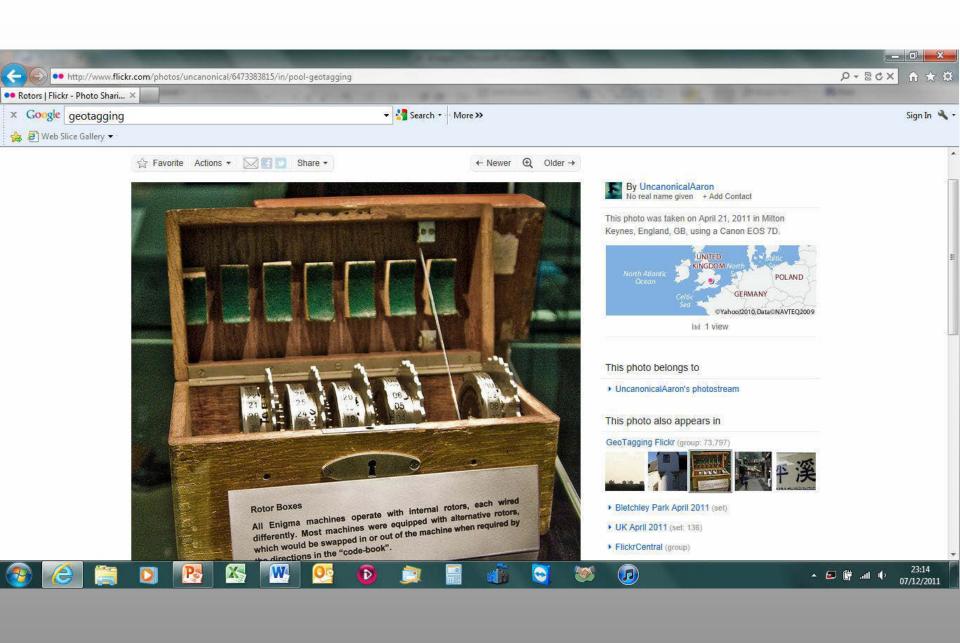


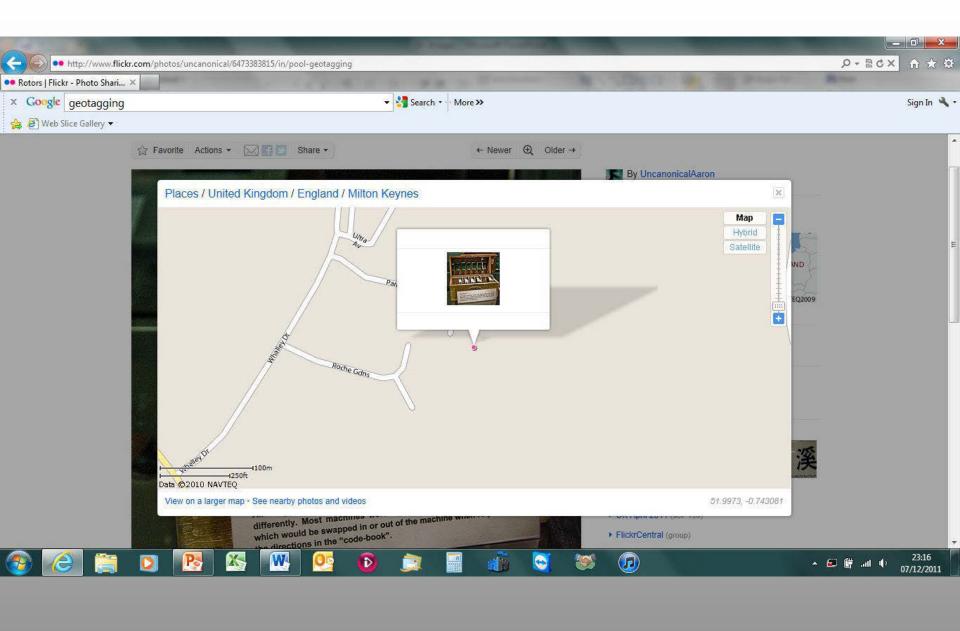
Facial Recognition

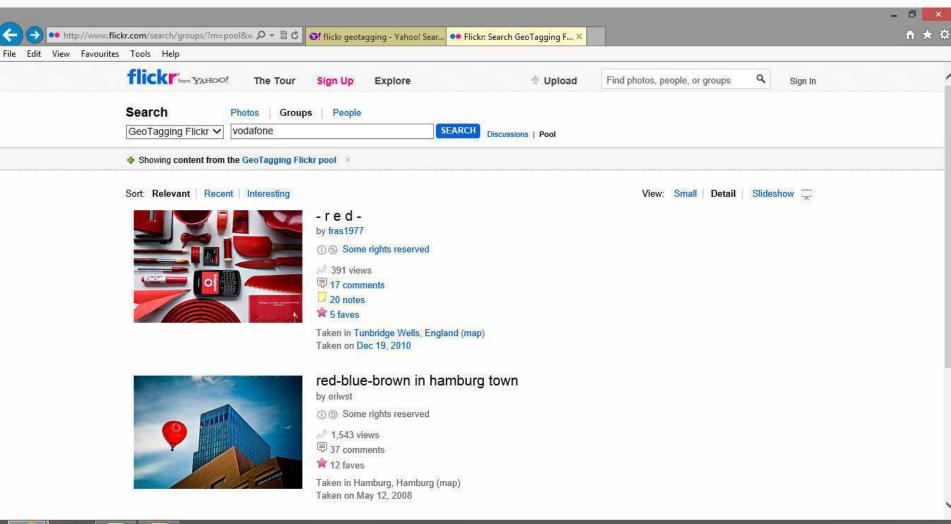
- Facebook facial recognition system scans pictures you're tagged in
- KFC store in China lets customers pay with facial recognition
- Rail passengers could be charged for journeys by iris scan
- Facebook is looking for your face in photos you don't even know exist
- Facial recognition technology is being used by companies such as Tesco, Google and Facebook, and it has huge potential for security. Concerned? It may be too late to opt out...
- Chinese police use facial recognition technology to send jaywalkers instant fines by text



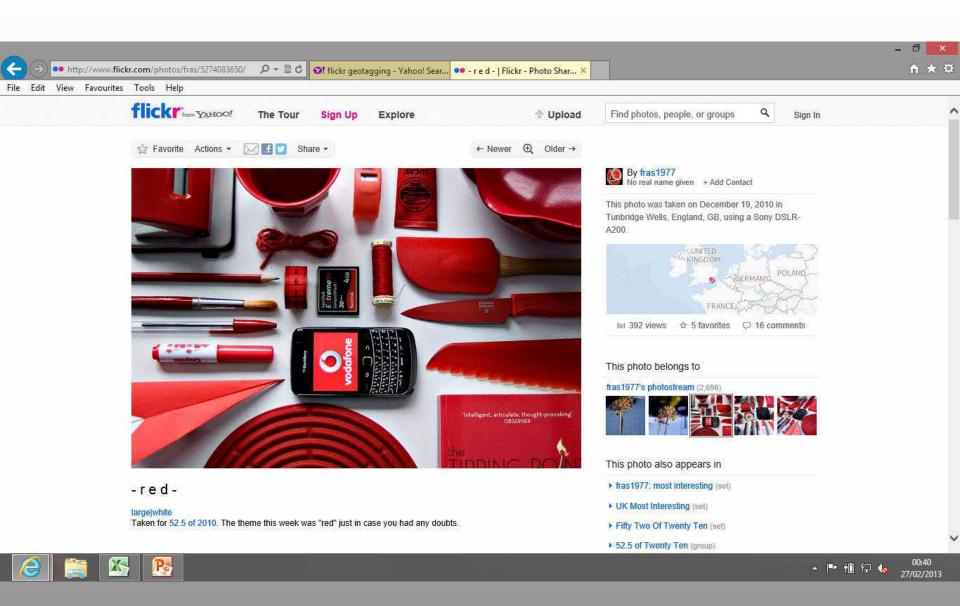


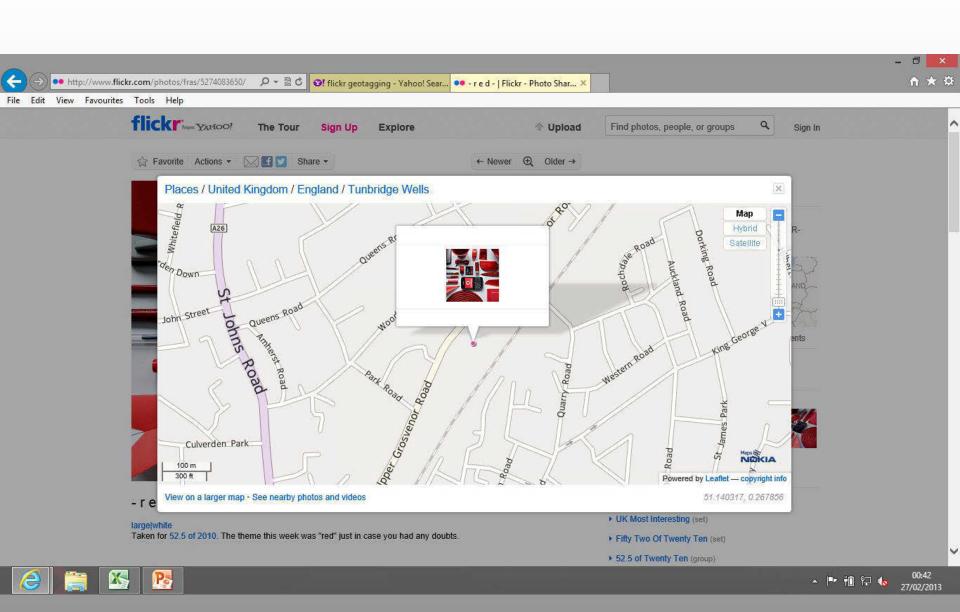


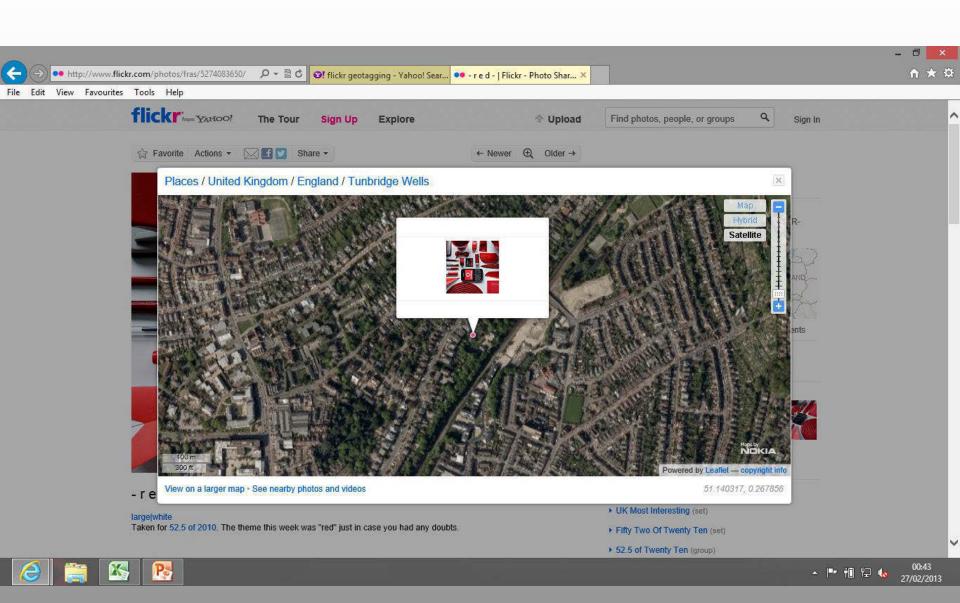












Videos

 On original site uploaded to – which might be a blog or membership page or other social media with the associated links

- Might be a link from your site such as Facebook to the site of origin
- Uploaded directly to a website not normally origin details

Videos

To find original site link (URL)

- Hover mouse of video whilst not playing and it might appear – if not, start the video to force it to link to the site of origin, then hover mouse of playing video
- Right click and follow instructions (copy link address) (show video URL)
- The URL might be published adjacent to the video

Intelligence or Evidence?

- Is our product evidence?
- Or is it intelligence that provides a link to evidence?
- How can we prevent others identifying the intelligence and methods of investigation?
- Sensitive method of investigation
- **CPIA**