You'll need to either log in or join PostDesk in order to contribute to this discussion.
Your contribution will be posted straight after.

- Log In
- Join

Contact PostDesk

Close

Your Name

First Last

Email *

Telephone Number

Skype Username

Callback?

I'd like a call back

Your Reason For Getting In Touch

Select Reason

Whatever your query is, we will be in touch within a few hours. We do not share your email address or add it to a database.

Submit

We recommend you connect with Facebook to read, discuss and debate this article on PostDesk

Connect with Facebook
(http://ec1capital.com)

PostDesk (http://www.postdesk.com)

/

Tech (http://www.postdesk.com/tech)

/

Culture (http://www.postdesk.com/tech/culture)

For in-depth tech / culture news, analysis, discussion and debate

We recommend you connect with Facebook to read, discuss and debate this article on PostDesk

- Log In with Facebook
- Don't have Facebook? Log In or create an account manually.

- Continue without logging in

Interview with a private investigator on 'Open Source Intelligence': How everything you do can be tracked easily, and legally, using the Internet

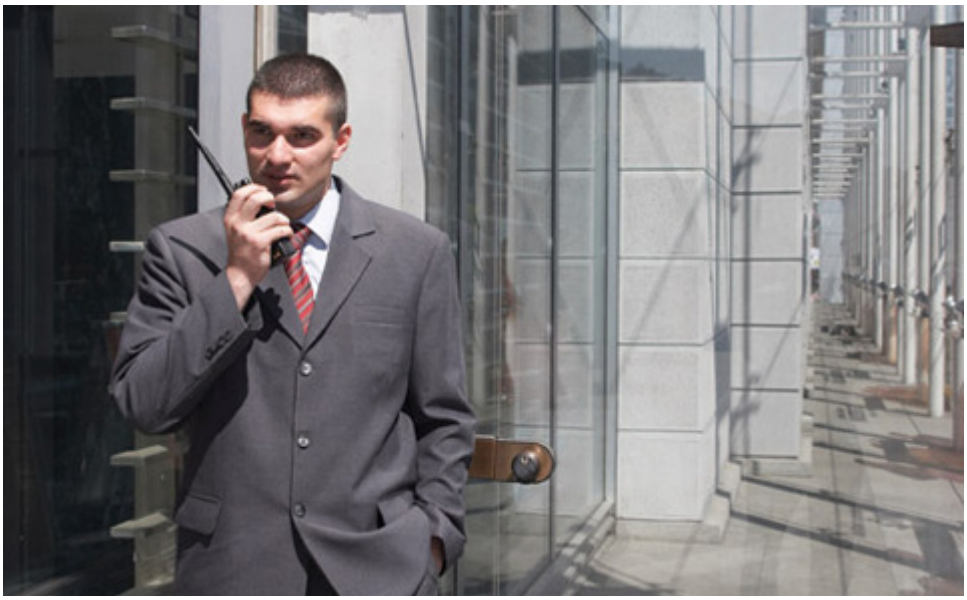
We interviewed Neil Smith, an investigative researcher and Open Source Intelligence trainer. He's also the man behind uk-osint.net – a resource for OSINT. He provides OSINT training for law enforcement, and for private investigators and journalists.

Email Article

Close

Firstname Lastname thought you might be interested in this article on PostDesk: http://postdesk.com/article-title

Send



Neil started out by giving us a basic definition of Open Source Intelligence. He described how it is "…any unclassified information, in any medium, that is generally available to the public, even if its distribution is limited or only available upon payment. Basically information, which anyone can legally access, so not things that only the police or solicitors can access."

We put a number of questions concerning OSINT to him – here are his responses in their entirety.

Neil Smith's website - uk-osint.net – is a valuable resource for OSINT. He also provides OSINT training for law enforcement, and for private investigators and journalists.

What are the most common misconceptions with regard to Open Source Intelligence?

Most people think that Open Source Intelligence (OSINT) is of no value and is just what is reported in the press or just what people put on Facebook but they are so wrong.

- Most fraud trials will involve company documents supplied by Companies House, which is OSINT.
- If you are doing asset tracing then you use Land Registry records, which is OSINT.
- If you are trying to prove family connections between people, then you use records of births, death & marriages, which is OSINT.

Yes we still use what is reported in the press and what people put on their social networking accounts but there are so many sources it's hard to pigeon hole it into just a few words.

Duedil is a British startup founded by Damian Kimmelman. Launched in April 2011, Duedil is the largest database of free company financials in the world, aggrigating over 30 billion data points including information in the Companies House database

What kinds of applications are there for Open Source Intelligence?

It take it by applications you mean different types of software or websites, (I know it's a blatant plug) but my website at www.uk-osint.net lists literally hundreds of useful websites and software. I have a few personal

favourites like findmypast.com for genealogy records, tracesmart.co.uk for electoral roll information, duedil.com for free company & director information in the UK & Eire and creepy for twitter.

How important is open-source intelligence to journalists?

I am writing these answers whilst listening to the Leveson Inquiry, so I would say OSINT is vital to investigative journalists as it offers the possibility of legally gain access to really useful information. I have found crucial bits on evidence on-line that has helped in many criminal and civil cases. If you don't try OSINT techniques then you don't know what you are missing out on.

What role does open source intelligence play in law enforcement?

Whatever you are investigating, whether it is as a journalist or as a police officer or local authority fraud investigator then you could possibly find information on-line that will help your enquiries or give you a greater understanding of your subject.

In the fight against terrorism or organised crime where so called grey figures (who have no history with the police) are used in one way or another, then OSINT is likely to be the only way you can find out about them.

What did open source intelligence involve before the Internet came about?

Basically many of the OSINT resources have been available for many decades, even well before the internet but the internet has meant you can access them all easily on-line rather than having to visit individual offices and companies up and down the country to gather individual bits of information.

Think back many years ago and people would have access to a credit reference agency on a dedicated computer that did nothing else but now all the credit reference agencies are accessed on-line and are just another website.

We no longer have to make visits to a local registry office or planning office as all of their details are now on-line. We are no longer restricted to just making local enquiries, now you can access the world.

Neil Smith tells us how private investigators still end up having to go out to speak to people and to follow people of interest on foot or in a car.

How has the role of the private investigator changed over the years as the internet has rapidly developed over the past few years – especially with the rise of social networks like Facebook, Twitter and similar services? Will the role of investigators on foot become less important over time?

Most private investigators still end up having to go out to speak to people and to follow people of interest on foot or in a car. The internet and OSINT has enabled private investigators, just like journalists and police officers, to have a greater knowledge of an area or an individual before going out.

I am lucky that I don't leave the office and haven't for about 8 years but I regularly supply information to investigators so they have photographs of individuals and know of the likely places someone will be travelling to before they start following them.

More people than ever claim to be 'investigators'. Has being an investigator become 'easier', or more accessible as a result of the Internet?

Lots of people claim to be an investigator but I wouldn't class them all as such. I write a blog but it doesn't make me a journalist. If you are not an inquisitive person then you are never going to be a good investigator, be it a private one, a journalist or even in law enforcement, all of whom I help train.

What are the best tools for the on-line investigator – and what are those most frequently overlooked by even a fairly experienced investigator?

There are loads of good tools and I have mentioned a few already, one that most people forget is friendsreunited.com. Just because it's not currently that popular in comparison 10yrs ago or to Facebook now, don't forget it still has really useful details on millions and millions of people in the UK and further afield.

Neil Smith tells us how friendsreunited.com is one tool that many investigators overlook - just because it's not currently as popular as Facebook is now, it still contains useful details on millions and millions of people in the UK and further afield.

What is the best way for an investigator to identify relevant, reliable sources from the vast amount of publicly available information on the Internet?

If you are starting out then try to find information on yourself and your friends and family. Think how can you locate information that you already know about them, now try to find the same information on other people you don't know but who you are interested in.

Does social engineering ever play a role in open source intelligence?

Again it depends what you mean by Social Engineering. I don't manipulate information or people I just harvest the information that I can locate about them. Obviously what people do with that information is another question but I tend to only work for people I already know.

How much does open source intelligence rely on a lack of privacy awareness by the majority of people (and the businesses they run) – or even an element of naivety (in that they don't take issue with disclosing large amounts of personal information on-line)?

A lot of time I am able to access quite personal information on sites like Facebook and photographs because people do not know what they are doing and have poor security; however on-line it isn't just about what you do, it's also about what your friends and family do. They may put lots of personal information about you on-line and that is out of your control, so lots of time there is very little you can do.

In what ways can intelligence be gleaned from social media? ...and when it comes to social media – does having a 'locked down' and fully private Facebook and/or Twitter account mean a private investigator could never access that users photographs, posts and friends lists?

Going back to my previous answer if you know what you are doing you can legally access lots of content from a Facebook account that the subject thinks has good "Friend Only" privacy settings. The same goes for Twitter. A lot of the time it is nothing special, it is just a matter of knowing how these sites work and knowing how you can work around them. I can't & wouldn't create software that bypasses any level of security, I'm just not that technical. But I do spend hour looking at some of these websites, looking for ways to access information and occasionally you find a new useful technique.

What are the on-line advanced searching techniques would a private investigator use?

Most of the time you just have to use the basic things that most kids already know about but if no-one has ever shown you these things then how are you expected to know about them.

Not everyone spends their lives on-line or even likes going on-line but it's hard to be an investigator nowadays if you don't get on with computers. Saying that I still have a client who writes to me and whom I have to fax my reports to.

What are the legal issues that face the private investigator or investigative journalist using open source intelligence techniques on-line?

If you only use legal techniques to obtain information that anyone else can access then really you don't have too many legal issues to worry about but obviously you should always be aware of the Data Protection Act and the Human Rights Act.

"If you only use legal techniques to obtain information that anyone else can access then really you don't have too many legal issues to worry about but obviously you should always be aware of the Data Protection Act and the Human Rights Act."

What do you foresee future developments to be across open source intelligence and the whole intelligence sector?

When I started training these OSINT techniques in around 2003 we used a lot of American examples and American databases. Now all the examples we use are UK based and there are hundreds of really useful UK databases and more and more useful things are being made available on-line all the time.

What are the best resources for those interested in perusing open source intelligence skills further, learning techniques and finding useful tools?

When I first started learning these things I went over to America to do some courses run by Brian Ingram (www.cispi.net) and with Kevin Ripa (www.computerpi.com) who are both just brilliant people to learn from and to know. Then after a few years of using OSINT Techniques at work for my enquiries I was approached by a training company to take over their OSINT training course in 2003 and have been doing all my own material for my own company since around 2008.

I have also been running my website at www.uk-osint.net for a few years to help people access useful OSINT resources.

I like to think my courses are both good in content and good value. As I am actually using these techniques daily then I like to think I can explain how & why we use them and can change the course to incorporate any new techniques and new sites.

There are some people who teach OSINT courses but who have never actually used any of them outside of the training room and you can see that the techniques and material is very out of date.

Obviously there are a few other good people out there to learn from but I've spent more than an hour writing these answers so I'm not going to name anyone else (other than Brian & Kevin who are top guys).

Can you tell us more about your business – what kind of training you offer, as well as who can benefit from it?

My business has two strands, my research enquiries and my training.

I have a number of clients that send me details of people or companies that they want to know all about, people they want to trace or assets that people may have. This could be from other investigators, insurers, from other companies or even from the government occasionally. I don't work for members of the public for a number of reasons. I also only work for people I already know so don't ask me to do any work for you.

The training is mostly for law enforcement but I also training other investigators and journalists.

I am running a 3day course in Bristol on the 2nd – 4th of April and will be doing another one in London in the autumn. People can always contact me for details.