Online Investigation: Using the Internet for Investigative Policing Practice

Steve Elers

Introduction

Digital technology continues to advance with devices such as smart phones, tablet devices and personal computers containing a growing number of features and applications that facilitate both interpersonal and mass communication. The internet has become an important part of global culture in the 21st century (Witkowski, 2002) and provides additional options for how messages are generated and received (Day, 2013). This rapid development of technology has impacted upon how law enforcement agencies collate digital evidence (Nelson, Phillips & Steuart, 2010). The training of police officers in the use of digital and online investigative techniques appears to be restricted to police officers in specialised units. The purpose of this paper is to present some examples of basic online investigative tools which utilise freely available methods that are accessible to anyone with an internet connection. The methods that are discussed below may assist police officers with their investigations. This paper is an introductory guide and serves as an *approach* as opposed to a rule book or manual. By understanding an *approach* to online tools, it becomes easier to extrapolate suitable methods of inquiry when required. This paper does not cover techniques which gain unauthorised access to data in a system or any other activities that would require a court order or warrant to execute. Further, it is important to note that the process or procedures in gathering digital evidence has a direct influence on the outcome of an investigation (Yusoff, Ismail & Hassan, 2011). Therefore it is recommended that the methods explained in this paper are rigorously documented if used in an investigation and that advice from specialists is sought during all stages of the investigation.

Digital Images

The cliché of "a picture is worth a thousand words" is certainly applicable to a criminal investigation. Digital imaging has surpassed traditional photography due to the increase in ownership of mobile phones, digital cameras and other digital devices which feature image capturing capabilities. One advantage of digital imaging for an investigator is the exchangeable image file format (EXIF) data which is automatically embedded in digital images by most mobile phones, digital cameras and other digital devices. EXIF is a type of metadata (Nelson et al., 2010) which can determine what make, model and type of camera was used, but more importantly it can ascertain the location, date and time of where and when the image was taken. In some instances it is merely a matter of viewing the properties of the image to determine the make, model and other information.

To establish the location of where a digital image was taken, there are multiple free EXIF readers/viewers online which will detail the metadata including the global position system (GPS) coordinates. The GPS coordinates can be entered into digital mapping applications such as Google Maps which will pinpoint the approximate location of where the digital image was taken. Some EXIF readers will simultaneously display a map of the approximate location as it presents the metadata. This tool can be useful when attempting to ascertain locations of interest. While this method has its advantages, the predominant social networking sites such as Facebook and Twitter remove EXIF data from digital images.

Further, if the digital image has been altered or enhanced by software or applications such as Photoshop then the EXIF data is often removed. The EXIF data can also be manipulated to give false metadata. Despite the possibilities of EXIF data being removed or altered, digital images that are captured directly from the device i.e. seized mobile phone or emailed directly from the device will most likely contain the EXIF data unless the device settings were changed. Thus, it is worthwhile to scan digital images with an EXIF reader/viewer. The entire process takes only a few seconds.

Another digital image tool that can assist an investigation is Google images. This is located at www.google.com/images Click on the camera icon in the search bar then click on "Upload an image". This tool will compare your digital image with others on the web. If the exact image is online, Google may be able to locate it. It can be used in cases of identity fraud whereby an individual uses a random photograph of an unrelated person sourced online. Digital images of individuals are often used to lure unsuspecting targets in dating scams or the infamous "Nigerian scams". The website www.tineye.com also does the same task. A website called www.facesaerch.com (purposely spelt incorrectly) searches the internet for facial images. This functions similarly to a standard Google image search, albeit for faces.

Websites

To determine the owner (registrant) of a particular website and to ascertain his/her contact details, a quick search of the WHOIS database directory of domain names will most likely provide the information. The Internet Corporation for Assigned Names and Numbers (ICANN) requires registries and registrars to "collect and display technical information and contact details for all registrants" (Burshtein, 2005, p. 77). There are various entry points on the internet to access a WHOIS database directory to query domain registrant details; an easy to remember website is: **www.who.is** This site enables a search to be conducted using only a website domain (name). A search will return the registrant's name, address, phone number and email address. Some registrars offer a service to anonymise details by providing their own details instead of the actual registrant which will result in the required information not being available.

Another worthwhile online instrument for websites is the Internet Archive's Wayback Machine https://archive.org/web/ This is essentially a repository of webpages that have been archived since as far back as 1996 (AlNoamany, Weigle & Nelson, 2013).

A search engine technology called Alexa Crawl scans the worldwide web and periodically takes snapshots of websites which are then permanently archived (Howell, 2006). By visiting the Internet Archive's Wayback Machine, a website can be viewed in previous versions despite whether or not the website has been updated or removed completely by the owner.

This tool will prove to be a goldmine for sociologists, anthropologists and political analysts in years to come (Denev, 2012).

For investigators, the archived repository can be of assistance when online content has been removed or modified (Howell, 2006), or the website no longer exists. According to Andersen (2013), data captures from the Internet Archive's Wayback Machine have been used in federal court cases in the United States. The Internet Archive's Wayback Machine may not necessarily capture historical records of all websites, particularly if the website owner has utilised technology to prevent web crawling (Andersen, 2013). Google also permits viewing of cached pages but has limitations such as not being able to view multiple captures of the one page.

The website **www.copyscape.com** scans the internet for plagiarised web content. This interface allows a user to simply enter a webpage address, and results will appear of other websites that have identical content. For instance, this can be used to track the viral nature of certain information that is relevant to an inquiry, or merely establishing links between two or more individuals. Like the other online tools mentioned in this paper, other alternatives exist in the worldwide web that should also be explored.

Google Commands for Data Mining

From personal interaction with police officers and academics (both staff and students) I have noticed that many do not know how to drive Google correctly in order to find the relevant information that is hidden among the plethora of online data. Police investigators and academic researchers have similar goals, to systematically collect and interpret information in order to gain understanding. Google commands, or Google operators, use advanced search methods which enable a user to refine a search "by limiting the index by web location, content type, and various search metadata" (Spencer, 2011, p. 7).

Google commands are essentially a method of inputting search queries with advanced functions in order to locate the most relevant information. Google, like Yahoo, is a searchable database of websites and other online content which are obtained from a type of software called web crawlers or spiders that methodically scan the worldwide web by following links from one page to another (Taylor, 2010). Table 1 demonstrates three Google commands.

Google Command	Function
site:	The **site:** command instructs Google to search specific websites/ domain names/domain extensions. For example: **site:nz** Results only from .nz websites (New Zealand) **site:au** Results only from .au websites (Australia) **site:police.wa.gov.au** Results only from the WA Police website. **site:nzherald.co.nz** Results only from the NZ Herald news site. **IMPORTANT –** There is no space between site: and the domain. Each country has their own domain extensions i.e. .nz, .au etc. For a full list enter "country domain extensions" into Google.
filetype:	The **filetype:** command instructs Google to return results with a specified file format. For example: **filetype:pdf** Results only in PDF format. **filetype:doc** Results only in Microsoft Word format. **filetype:xls** Results only in Excel spreadsheets. **filetype:ppt** Results only in PowerPoint. **IMPORTANT –** There is no dot or space between filetype: and the format abbreviation.
link:	The **link:** command instructs Google to return website pages that link to a specific website. For example: **link:police.wa.gov.au** Returns websites that have linked to the WA Police website. **IMPORTANT –** There is no space between link: and the domain.
For a full list of Google commands visit: **http://www.searchcommands.com/google/**	

Table 1

The use of Google commands for an investigation requires innovative thinking dependent upon the information you are attempting to locate. Hackers have used Google commands to exploit vulnerabilities on servers for a number of years (Wong, 2005). The approach or mindset of using Google commands will generate interesting results. For example, the **link:** command in conjunction with the Facebook address of a particular gang returned results of individuals and websites that had links to the gang's Facebook site. Google commands is a very useful data mining tool but proficiency is required to maximise the search function benefits. I recommend readers undertake their own study about Google commands and become familiar with it.

Social Media

It is fast becoming a necessity for police to monitor social media communications as the information that is generated from social media networks can impact upon tactical policing decisions and provide a plethora of intelligence for analysis. It is interesting to note that some people willingly post comments and photographs of criminal behaviour. The observation of potential out-of-control parties, social disorder, activism activities and many other concerns are valid reasons for police to be actively involved in monitoring social media. The New Zealand Police have used a paid software package called Signal which monitors social media posts (New Zealand Police, 2012). I have not had the opportunity to evaluate this software but similar monitoring technology is freely available online. Twitter searches can be conducted on **https://twitter.com/search-home** It would be advisable to take advantage of Twitter's "operators" and "advanced search" tips which is located on the same page. The website **www.socialmention.com** searches not only Twitter, but also Facebook and several other social media networks in "real-time".

To search older Twitter posts, **www.topsy.com** is able to search older tweets which are no longer available from the Twitter interface.

Google Alerts is a recommended tool to stay up to date with information you would like to follow.

By registering for free at **www.google.com/alerts**, Google will email a notification to the user whenever a keyword appears online that you have designated to track. For example, if I sign up to Google Alerts and enter “Mike’s Outlaw Motorcycle Club” as an alert; whenever “Mike’s Outlaw Motorcycle Club” appears on news sites, blogs, discussions and other content, Google will immediately email me with the direct links. A similar tool is **www.mention.com** but is limited to just one keyword or search term under their free plan.

To learn more about the use and monitoring of social media for policing, the IACP Center for Social Media website is highly recommended as it contains a corpus of resources and information about the topic for law enforcement agencies. The IACP Center for Social Media website is **www.iacpsocialmedia.org**

Applications for Frontline Duties

The New Zealand Police recently circulated iPhones and iPads to frontline police in order to “do their job better and faster” (New Zealand Police, 2013). The rationale behind this distribution was to allow instant remote access to the national police computer in order to conduct background checks on persons of interests, victims, vehicles and so forth. There are a number of free applications that can provide frontline police with a range of utilities at their immediate disposal. One such application is Google Translate which is available as a free download for both Apple and Android. This tool currently supports translation between 80 languages and allows the user to “speak, type, write or take a picture to translate” (Google, 2014). The Asian population is rapidly growing in New Zealand, with almost one in every four Aucklanders being Asian (Collins, 2013). This handy application can assist to remove communication barriers between police and non-English speakers and provide frontline officers with an immediate translator on the spot. Given that there are approximately one million Android applications available for download in Google Play and a similar number in Apple’s App Store (Elgazzar, Ejaz & Hassanein, 2013), there should be an abundance of relevant applications that are useful for policing. I encourage frontline officers to spend some time to familiarise themselves with such applications.

Conclusion

This paper has presented some basic online investigative tools that may assist police in the function of their duties. The examples that were presented are just a small representation of the many free online tools that are available in the growing internet technology sphere. As technology is constantly improving, some of these tools may become obsolete. Thus, it is important to maintain an active interest and maintain skills in this area. I recommend that police organisations incorporate training in online technology for investigation purposes to all police officers from recruits to existing staff. It should be mandatory for all police officers attached to an inquiry or investigation unit to receive training in this area in order to further enhance their investigative skills.

About the Author

Steve Elers is a Vice-Chancellor’s Doctoral Scholarship recipient at the Auckland University of Technology where he is undertaking a PhD in communication studies. A former police officer (Western Australia Police), he has a master degree in public relations.

References

ALNoamany, Y., Weigle, M. C., Nelson, M. L. (2013). Access patterns for robots and humans in web archives. Retrieved from http://arxiv-web3.library.cornell.edu/pdf/1309.4009.pdf

Andersen, H. (2013). A website owner’s practical guide to the Wayback Machine. *Journal on Telecommunications and High Technology Law, 11,* 251-277. Retrieved from http://www.jthtl.org/content/articles/V11I1/JTHTLv11i1_Andersen.PDF

Burshtein, S. (2005). Whazup with the WHOIS? *Canadian Journal of Law and Technology, 4*(1), 77-81.

Collins, S. (2013, December 4). Census 2013: Our changing nation. *The New Zealand Herald.* Retrieved from http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11166490

Day, S. (2013). Self-disclosure on Facebook: How much do we really reveal? *Journal of Applied Computing and Information Technology, 17*(1).

Denev, D. (2012). *Models and methods for web archive crawling* (Doctoral thesis, Saarland University, Saarbrucken, Germany). Retrieved from http://www.mpi-inf.mpg.de/~ddenev/phd-thesis.pdf

Elgazzar, K., Ejaz, A., & Hassanein, H. S. (2013). AppaaS: Offering mobile applications as a cloud service. *Journal of Internet Services and Applications, 4*(17). Retrieved from http://www.jisajournal.com/content/pdf/1869-0238-4-17.pdf

Google. (2014). Google Translate. Retrieved from https://play.google.com/store/apps/details?id=com.google.android.apps.translate

Howell, B. A. (2006). Proving web history: How to use the internet archive. *Journal of Internet Law, 9*(8), 3-9.

Nelson, B., Phillips, A., & Steuart, C. (2010). *Guide to computer forensics and investigations* (4th ed.). Boston, MA: Cengage Learning.

New Zealand Police. (2012). Electronic eyes and ears flag risks. Retrieved from http://www.tenone.police.govt.nz/tenone/December12National2.htm

New Zealand Police. (2013). Mobility rollout concludes policing excellence implementation (plus picture). Retrieved from http://www.police.govt.nz/news/release/35461

Reading, A. (2009). Mobile witnessing: Ethics and the camera phone in the ‘war on terror’. *Globalizations, 6*(1), 61-76. doi:10.1080/14747730802692435

Spencer, S. (2011). *Google power search.* Sebastopol, CA: O’Reilly Media, Inc.

Taylor, G. (2010). What makes Google tick? Economic Review, 28(2), 16-19.

Wong, L. W. (2005). Information gathering using google. Retrieved from http://igneous.scis.ecu.edu.au/proceedings/2005/forensics/wong.pdf

Witkowski, J. (2002). Can juries really believe what they see? New foundational requirements for the authentication of digital images. *Journal of Law & Policy, 10,* 267-294. Retrieved from https://law.wustl.edu/Journal/10/index.html

Yusoff, Y., Ismail, R., & Hassan, Z. (2011). Common phases of computer forensics investigation models. *International Journal of Computer Science & Information Technology, 3*(3), 17-31. doi:10.5121/ijcsit.2011.3302