Dr. Mohamed Elguindy
Cybercrime Expert, Faculty of Law, BUE, UNODC
Digital Expert, Public Prosecution Office

Applying Digital Forensics Methodology to Open Source Investigations of Counterterrorism

- **Correspondance:**
Dr. Mohamed Elguindy, Faculty of Law, BUE, Egypt.

- **E-mail:** mohamed.elgendy@bue.edu.eg

- **Citation:** Mohamed Elguindy, Applying Digital Forensics Methodology to Open Source Investigations in Counterterrorism, Journal of law and Emerging Technologies, Volume 1, Issue 1, 2021, (P.).11- 64

Applying Digital Forensics Methodology to Open Source Investigations of Counterterrorism

Dr. Mohamed Elguindy

Abstract

This research paper discusses the technical and legal aspects of open source intelligence (OSINT) as an investigation discipline in combating terrorism cases. Due to the proliferation of internet connectivity and the use of the Internet by terrorists, new mythologies and framework are needed to effectively identify, collect, preserve, and present the evidence related to such a serious crime. While there is no internationally agreed standard to apply on using OSINT for criminal investigations, the researcher proposes new framework that utilizes the application of digital forensics standards and methodologies in open source investigation to deliver admissible evidence in court of law.

Keywords: Open Source Investigations - Digital Forensics - open source intelligence (OSINT) - Counterterrorism - Criminal investigations

تطبيق منهجية الأدلة الجنائية الرقمية
على تحقيقات المصادر المفتوحة
في مكافحة الإرهاب

الدكتور/ محمد الجندي

الملخص

يتناول هذا البحث أهمية تحقيقات المصادر المفتوحة Open Source Investigations التي أصبحت تتمتع بأهمية كبيرة مؤخرًا بسبب الانتشار الكبير للمعلومات على الإنترنت وخصوصًا مع تطور مواقع التواصل الاجتماعي واستخدامها في العديد من العمليات الإجرامية؛ مما دعا الكثير من جهات إنفاذ القانون إلى استخدام أساليب تحقيقات المصادر المفتوحة باعتبارها وسيلة لجمع الأدلة الرقمية وتحليلها في القضايا الخطيرة كقضايا الإرهاب. وحتى الآن، لا يوجد لتحقيقات المصادر المفتوحة إطار معتمد أو معيار دولي فيما يتعلق بطريقة التعامل مع الأدلة والمعلومات المستمدة منها؛ لهذا يتناول هذا البحث كيفية تطبيق المعايير الدولية والمنهجية العلمية المتبعة في التحقيقات الجنائية الرقمية في كافة خطوات تحقيقات المصادر المفتوحة لضمان حجية وموثوقية الدليل المستمد من المصادر المفتوحة أمام المحاكم.

- الكلمات الرئيسية: تحقيقات المصادر المفتوحة – جمع وتحليل المعلومات من مصادر مفتوحة (OSINT) - الدليل الجنائي الرقمي - مكافحة الإرهاب - التحقيقات الجنائية.

Table of Contents

Introduction

The spread of the Internet and the rate at which technology is evolving, along with the fact that social networking is currently one of the most popular online activities, ensures that cybercrime is likely to increase at a rapid rate [(1)]. Around the world, organized crime gangs are using technology to coordinate and conduct crimes, posing several problems for law enforcement, forensic analysts, organizational security experts and members of the legal community[(2)].

In the Middle East, cybercrime has evolved rapidly over time as the Internet penetration rate in the region is outpacing the rest of the world with low digital literacy rate [(3)]. Additional reasons can be added to the rise of cybercrime in the region including but not limited to poor legislations, law enforcement capacity building, political problems, economic problems, and religious issues that sparked many troubles since the so-called Arab Spring in 2011. Since then, social networking sites usage has increased with different platforms being used in each country [(4)].

Although the aim of using social networking is to enable friends to communicate and socialize online, criminals and terrorists have identified vulnerabilities in social networks that they are exploiting because of the anonymity and abundance of freely available personal information that these social networks allow. The abundance of knowledge shared on social networks allows offenders to easily access and use relevant information to their benefit in committing crimes. For example, many terrorist incidents in the Middle East prove with no doubt that the Internet is the new battleground for

(1) NWC3. (2014). Retrieved May 27, 2020, from Bureau of Justice Assistance website: https://bja.ojp.gov/library/publications/national-white-collar-crime-center-annual-report-2013

(2) Taylor, R. W., Fritsch, E. J., & Liederbach, J. (2015). Digital crime and digital terrorism. Boston: Pearson.

(3) El-Guindy, M. (2008). Cybercrime in the Middle East. ISSA Journal, 6(6).

(4) Wonder, J. (2020, January 25). Digital Marketing Community. Retrieved May 27, 2020, from Digital Marketing Community website: https://www.digitalmarketingcommunity.com/researches/state-social-media-mena-region-2018-crowd-analyzer/

terrorists in gathering information, coordination of attacks, communications, recruitment, and fundraising [1].

The explosion of freely available information online is double-edged. While criminals and terrorists can use it against governments and civilians; on the other hand, governments and law enforcement departments can also use it to fight criminals. The Internet is "open" and "public" by design, thereby ensuring that a vast amount of information is available to anyone who has access to the Internet via a smartphone or computer [2]. Open Source Intelligence (OSINT) is publicly available information that has been obtained both legally and ethically. OSINT is one of the first forms of intelligence and originated well before the Internet came into existence at a time when information was gathered from newspapers, speeches, and radio. Its earliest records dated back to the Second World War.

Information available publicly is collected and exploited to generate intelligence for a specific target audience, such as military or law enforcement[3]. OSINT is also considered the lifeblood of intelligence [4]. It accounts for 70% to 80% of Intelligence sources for today's law enforcement departments in United States alone. The vast amount of available OSINT information is a challenge for many intelligence analysts as they have to traverse the ocean of information to locate what's relevant to them. Although OSINT techniques are useful in investigating cybercrime and already used by investigators and intelligence departments, there are currently no guidelines

[1] El-Guindy, M. (2014). Middle East Dilemma from the Caliphate to Open-source Jihad. Retrieved May 27, 2020, from Academia website: https://www.academia.edu/6432111/Middle_East_Dilemma_from_the_Caliphate_to_Open-Source_Jihad

[2] Appel, E. J. (2017). Internet Searches for Vetting, Investigations, and Open-Source Intelligence. https://doi.org/10.1201/b10523

[3] Pouchard, L. C., Dobson, J. D., & Trien, J. P. (2017). A Framework for the Systematic Collection of Open Source Intelligence. Retrieved May 27, 2020, from undefined website: https://www.semanticscholar.org/paper/A-Framework-for-the-Systematic-Collection-of-Open-Pouchard-Dobson/b655d9c157d0c76868cb-9620529f0217ae9a70a2

[4] Hulnick, A. S. (2010). The International Politics of Intelligence Sharingby James Igoe Walsh. Political Science Quarterly, 125(4), 715–716. https://doi.org/10.1002/j.1538-165x.2010.tb02080.x

or standard methodology in conducted OSINT investigations. Additionally, most investigators treat information gathered using OSINT techniques as supplementary than evidentiary.

This situation led to the proposed methodology to conduct OSINT investigation using digital forensics standards to allow for systematic gathering, analysing and presentation of the data in an acceptable and structured format in order to be admissible in court of law.

Literature Review

1. Cyberterrorism

The term "Cyberterrorism" is complex and combining two other terms "Cyber" which is referring to Cyberspace and "Terrorism". The term "Cyberterrorism" coined by Barry Collin, a senior research fellow at the Institute for Security and Intelligence in California in 1980s (1). However, Cyberterrorism as a term still lacks clear and widely accepted definition (2).

While there is no globally agreed definition to Cyberspace, there are accepted definitions that can be found and used in different scenarios. Cyberspace is considered the global domain in which information travels at different levels of the network consists of the physical, logical, data, and social layers (3). Cyberspace is also considered one of the most important terms in science fiction as it is originated in William Gibson's novel Neuromancer (4) in which he argues that Cyberspace has an anthropological dimension that is altering human experience with new perspectives.

[1] Arquilla, J., Ronfeldt, D. F., & States., U. (2001). Networks and netwars: the future of terror, crime, and militancy. Santa Monica, Ca: Rand.

[2] Conway, M. (2014). What is Cyberterrorism and How Real is the Threat? Cyber Behavior, 217–245. https://doi.org/10.4018/978-1-4666-5942-1.ch013

[3] Uche Mbanaso, & Eman Dandaura. (2015, June). The Cyberspace: Redefining A New World. Retrieved June 20, 2020, from ResearchGate website: https://www.researchgate.net/publication/280101879_The_Cyberspace_Redefining_A_New_World

[4] Gibson, W. (1984). Neuromancer. New York: Ace Science Fiction Books.

When it comes to cyberterrorism, there will be always confusion between cybercrime and cyberterrorism due to the lack of international definitions for both terms. An additional area of confusion is related to the distinction between the terrorist use of information technology and the Internet for facilitating their activities, and terrorism involving the use of internet, computer technology and cyberspace as a weapon or target for attacks.

It is important to differentiate between using the internet and cyberspace for terrorism purposes and using the internet and cyberspace as a weapon or target. True cyberterrorism deals with cyberspace and technology as a weapon or target with politically motivated violence against non-combatant targets. Cyberterrorism can be defined as(1):

“Cyberterrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.”

Dorothy E. Denning’s definition combines the cyberspace components used or targeted by act of terrorism as it is contained in Title 22 of the United States Code, Section 2656f(d). That statute contains the following definition(2):

“The term ‘terrorism’ means premeditated, politically motivated violence

(1) Dorothy E. Denning: Is Cyber Terror Next? (2001). Retrieved June 20, 2020, from Ssrc.org website: http://essays.ssrc.org/sept11/essays/denning.htm

(2) US Dep. of State Glossary: (2001). Retrieved June 20, 2020, from State.gov website: https://2001-2009.state.gov/s/ct/info/c16718.htm

perpetrated against non–combatant targets by sub–national groups or clandestine agents, usually intended to influence an audience."

1.1 Terrorist Use of the Internet

Due to the nature of terrorism in the Middle East, the researcher mainly focuses on the terrorists use of the internet to facilitate their attacks. Terrorism in its broader definition is not a new phenomenon in the region as it dates to the kingdom of Sargon of Akkad, Zealots against the Roman Empire, the Sicarii, and the Assassins [1]. Although terrorism is not based mainly on a specific ideology or religion, radical Islamic terrorism in the 21st century took a new turn due to many reasons. The latest call, which spread all over the world using the 21st century technologies to establish the so called "Caliphate" Islamic State of Iraq and Levant (ISIL) or Da'esh, is based on the old narrative that can be traced back to the old history of conflicts in the Islamic World.

By the end of the 20th century, terrorists started to use the internet to communicate and spread their message. Earliest examples included Al-jamāʻah al-Islamiyah in Egypt who started their own online presence using a very simple website in 1996, followed by other groups in Middle East such as Hamas, Armed Islamic Group in Algeria, Hezbollah in Lebanon, then Al-Qaeda's online media empire established after September 11, 2001.

In the 21st century, the Internet changed the equation of spreading ideas. Jihadists learned that propaganda is a must for success even if they do not win the war. It is a proven and true method of psychological warfare. In a letter to Mullah Mohamed Omar, Osama Bin laden said [2]: "It is obvious that the media war in this century is one of the strongest methods; in fact, its ratio may reach 90% of the total preparation for the battles"

[1] Amin Maalouf, & Harris, R. (1998). Samarkand. London: Abacus.

[2] AWAN, A. N. (2010, May 3). The Virtual Jihad – Combating Terrorism Center at West Point. Retrieved June 20, 2020, from Combating Terrorism Center at West Point website: https://www.ctc.usma.edu/the-virtual-jihad-an-increasingly-legitimate-form-of-warfare/

Jihadists have applied the lesson to harness mass media by sophisticated and adaptive uses of new media technologies and moved from physical space to cyberspace. After the collapse of the Taliban in November 2001, Al-Qaeda did not vanish but lost its haven in Afghanistan and became decentralized. Hamid Mir, Osama Bin Laden's biographer, watched "every second al Qaeda member carrying a laptop computer along with a Kalashnikov" as they prepared to scatter into hiding and exile. On the screens were photographs of September 11 hijacker Mohamed Atta. They wanted the ideology to remain and for new version of leaderless Al-Qaeda with no hierarchical order to emerge using new technologies and cyberspace[1].

In 2004, the National Intelligence Council (USA) published a report which discussed the global trends in 2020 [2]. One of the most important threats to the global security was the establishment of the so-called "Islamic State" or the Caliphate. Although the report considered this a fictional scenario, it stated that "Radical Islam will have a significant global impact…rallying disparate ethnic and national groups and perhaps even creating an authority that transcends national boundaries"

This fictional scenario provided an example of how a global movement fueled by radical religious identity could emerge. Under this scenario, a new Caliphate is proclaimed and manages to advance a powerful counter ideology that has widespread appeal. The report concluded that the Caliphate would not have to be entirely successful for it to present a serious challenge to international order. Subsequently, the information and communication revolution will amplify this call and fuel the clash between Western and Muslim worlds. Accordingly, a new generation of terrorists will appear and will start to attack different targets inside and outside the Muslim World.

[1] Baken, D. N., & Ioannis Mantzikos. (2015). Al Qaeda : the transformation of terrorism in the Middle East and North Africa. Santa Barbara, California: Praeger, An Imprint Of Ab-Clio, Llc.

[2] NIC. (2004). Mapping the Global Future. Retrieved June 20, 2020, from DNI website: https://www.dni.gov/files/documents/Global%20Trends_Mapping%20the%20Global%20Future%202020%20Project.pdf

Ironically, what was described in the NIC's report as a fictional scenario is now a reality with the presence of ISIS and other affiliated groups in the Middle East. With the help of cyberspace, the ideas of leaderless terrorists, lone wolves, open source Jihad and Islamic State become inevitable consequences. One of the most prominent figures in strategic Jihad, Abu Mus'ab al-Suri wrote this vision in a book entitled "The Call to Global Islamic Resistance". Although Al-Suri was a member of Muslim Brotherhood in Syria and influenced by the ideology of Sayyid Qutb, he did not believe in waging Jihad from top by replacing the rulers of Middle East countries [(1)].

In contrast, Al-Suri designed his own vision based on leaderless Jihad or individualized Jihad. He described his ideology and vision for "Future Salafi Jihadists" to establish the Islamic State in over 1600 pages published on the Internet in 2004 [(2)]. Al-Suri clearly described in his book that "Jihadists" need to understand the importance of Information Technology, Communications and Electronics especially those related to explosives. He wrote also that Information and Communications Technology (ICT), mass media, and the Internet are promising and should be used as a new medium to spread the ideology, gather information, and wage "Jihad". Furthermore, he noted that targeting critical facilities of ICT in "infidel" countries is vital for "Jihad" as it will shut down the entire country. That was the first "Jihadist" to talk about "Cyber Jihad". In his book, he stated that this guide is for "the third-generation mujahedeen", as he called them. The Jihadists who will form the new Al-Qaeda as an ideology and will utilize the Internet for self-learning, and then they will use this knowledge to wage Jihad in their home countries.

Those third generation Mujahedeen, as Al-Suri predicted, will replace Al-Qaeda. Consequently, their Jihad will be "leaderless" and waged by small groups rather than an organization. He believed that Al-Qaeda is not

[(1)] M W Zackie Masoud. (2015). An Analysis of Abu Mus'ab al-Suri's "Call to Global Islamic Resistance". Journal of Strategic Security, 6(1), 1–18. https://doi.org/10.5038/1944-0472.6.1.1

[(2)] Ibid

an organization; it is a call, a reference, a methodology. With the spread of such vision on the Internet, the ideology of "Jihad" as warfare or asymmetric terrorism became "open source" and inspired other terrorist groups in Middle East. Those small radical groups are challenging the security and existence of many Arab states and have even become transnational. These new generations of leaderless jihadists were recruited and radicalized through open source manuals spread on the Internet and social media networks. One of the most important examples is the Inspire magazine (1) published by AQAP (Al-Qaeda in in the Arabian Peninsula) in 2010 and edited by Samir Khan and Anwar Al-Awlaki; the latter became Bin laden of the Internet era. The legacy of Anwar Al-Awlaki still resonates to date, especially for lone wolves who attacked different targets in the Muslim World and in the West (2).

Following the so-called "Arab Spring" uprisings, Islamists tried to hijack the online narrative on social media to spread the idea of restoring the Caliphate. Al-Qaeda leader, Ayman Al-Zawahiri published online video and audio messages titled "the Islamic Spring" (3). In different messages, Al-Zawahiri focused on the importance of "Jihad" as the only way to restore the caliphate. He emphasized that the "Levant today is the hope of the Muslim Ummah," because it is the only "popular revolution" started during "the Arab Spring that followed the correct path," which requires both "Da'wah" and "Jihad" to establish the "rightly guided caliphate."

Although Al-Qaeda and like-minded jihadists call for the restoring of the Caliphate, they are opposing the ISIS version declared later by Baghdadi. This proves without a doubt that the old dispute over who will establish the

(1) Lemieux, A. F., Brachman, J. M., Levitt, J., & Wood, J. (2014). Inspire Magazine: A Critical Analysis of its Significance and Potential Impact Through the Lens of the Information, Motivation, and Behavioral Skills Model. Terrorism and Political Violence, 26(2), 354–371. https://doi.org/10.1080/09546553.2013.828604

(2) The Lessons of Anwar al-Awlaki. (2015, August 27). The New York Times. Retrieved from https://www.nytimes.com/2015/08/30/magazine/the-lessons-of-anwar-al-awlaki.html

(3) Holbrook, D. (2012). Al-Qaeda's Response to the Arab Spring on JSTOR. Retrieved June 20, 2020, from Jstor.org website: https://www.jstor.org/stable/26296891?seq=1#metadata_info_tab_contents

Caliphate still resonates and will pose serious threats to Middle East countries and their counterterrorism strategies [1].

In 2014, using sophisticated propaganda techniques, ISIS declared the return of "Khilafah" in their glossy magazine, DABIQ [2]. At the same time, ISIS published different ideas on establishing the Caliphate in their Rumiyah magazine which appeared in English language. The idea of the Islamic State is the heart of ISIS propaganda and is not only mentioned in magazines but in most video messages posted on social media to radicalize and recruit new jihadists from the West and from the Middle East. In 2014, ISIS media arm Al-I'tisam media presented the video message "Breaking of the borders" that declared the establishment of the Caliphate and removing the borders created by the Sykes–Picot Agreement [3].

This online propaganda mobilized youngsters who are sympathized with the idea of restoring the Caliphate to either immigrate to the land of Khilafah (Hijrah) or wage Jihad against "Infidels" in their home countries. The socio-psychological effects of social media and ISIS messages pose significant threats to Middle East countries who are struggling to decode these sophisticated messages to prevent radicalization of youth.

Accordingly, the availability of 21st century technologies in a region that has low technological competences combined with higher rates of unemployed youth, political, economic social and religious problems [4] will result in an uncertain future and a more volatile region.

[1] Holbrook, D. (2012). Al-Qaeda's Response to the Arab Spring on JSTOR. Retrieved June 20, 2020, from Jstor.org website: https://www.jstor.org/stable/26296891?seq=1#metadata_info_tab_contents

[2] Ingram, H. J. (2018). Islamic Stateis English-language Magazines, 2014-2017: Trends & Implications for CT-CVE Strategic Communications. Terrorism and Counter-Terrorism Studies. https://doi.org/10.19165/2018.1.03

[3] Weaver, M., & Tran, M. (2014, June 30). Isis announces Islamic caliphate in area straddling Iraq and Syria. Retrieved June 20, 2020, from the Guardian website: https://www.theguardian.com/world/2014/jun/30/isis-announces-islamic-caliphate-iraq-syria

[4] Nour, S. S. O. M. (2006). ICT Opportunities and Challenges for Development in the Arab Region. The New Economy in Development, 161–187. https://doi.org/10.1057/9780230287709_8

1.2 Social Media Terrorists

With the help of Twitter, Facebook, YouTube and other social media tools, global Jihadists can share their contribution of jihadi media, literature, videos, and graphic arts. These free and open tools allowed even non-jihadists to participate, engage and share their thoughts within the global jihadi environment. The emergence of open source jihad created what is called online "Jihadosphere", similar to Arabic "blogosphere" for activists (1).

The new generations of Jihadists are harnessing social media in propaganda, fundraising, recruitment, and communications as well as information gathering (2). They use social media to collect physical addresses, phone numbers, and private information related to the target, such as family members and their connections. This technique is widely used in Egypt by members of Muslim Brotherhood who are extensively using open-source tools to gather information on police officers (3).

Due to lack of cybersecurity awareness in law enforcement agencies in the region, many law enforcement personnel are using social media without protecting their privacy and even sharing their private photos and family connections which render them easy targets. A photo published on Facebook pages linked to Muslim Brotherhood groups asked followers to send the home address of one of the judges who prosecuted their friends and associates jailed for protesting after the ouster of the president, Muhammad Morsi, on July 3, 2013. A simple image search using Google will display many results for the same photo shared by Facebook and twitter users. Even If a police officer is not sharing anything private on his public profile, Jihadists are still able to

(1) Etling, B., Kelly, J., Faris, R., & Palfrey, J. (2010). Mapping the Arabic blogosphere: politics and dissent online. New Media & Society, 12(8), 1225–1243. https://doi.org/10.1177/1461444810385096

(2) FATF. (2015). Emerging Terrorist Financing Risks. Retrieved from https://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf

(3) Shima Galhoom. (2013, November 28). ميليشيات الجماعة تنتقم بحملات «تجريس وتشهير». Retrieved June 20, 2020, from Alwatan Newspaper website: https://www.elwatannews.com/news/details/363244

trick him using social engineering techniques. They easily create fake profiles for “pretty women”, “police officers with real data previously collected”, or anything of interest to the target, then request a friendship. If that will not work, they can try hacking techniques to gain access to his email address then to his account [1].

Unfortunately, after the so-called Arab Spring, vital data on law enforcement personnel are extensively published online and on social media networks such as Flickr [2] and Facebook which poses serious threats to police officers and even national security of most Middle East countries. One of the assassinations of a police officer in Egypt was carried out by the terrorist group Ansar Bayt Al-Maqdis exploited the online data available on social media [3]. In their statement of responsibility published on Jihadist forums, they urged anyone who has data on other officers to communicate with them using all available communication methods. Consequently, Muslim Brotherhood affiliated groups on Facebook revealed a list of police officers with their real names, phones and addresses as a call for vendetta. This evidence proves that Jihadists’ capabilities in using open-source information were much more powerful than those of law enforcement in Middle East at that time.

1.3 Open Source Terrorism

Open source information is vital for Jihadists as well as law enforcement if it is used properly in counterterrorism strategy. However, lack of an analytical mindset among law enforcement personnel in the region prevents many of them from catching online persons of interest or even understanding how terrorists operate in cyberspace. Terrorists have always used open source

[1] IBrahim Rashwan. (2015, October 3). “داعش” يخترق حساب ضابط شرطة بالبحيرة على “فـيس بوك”. Retrieved June 20, 2020, from Alwatan Newspaper website: https://www.elwatannews.com/news/details/812671

[2] Flickr. (2020, June 20). Retrieved June 20, 2020, from Flickr website: https://www.flickr.com/groups/piggipedia/pool/

[3] Lotfi Salman. (2013, December 29). بعد تأكيد مدير “رصد” عن قرب “الاغتيالات”.. “الإرهابية” تنشر قائمة ضباط “فض رابعة”. Retrieved June 20, 2020, from Alwatan News website: https://www.elwatannews.com/news/details/382568

intelligence since Al-Qaeda in Iraq during the era of Abu Mus'ab Al-Zarqawi, where they used Google Earth and GPS devices to pinpoint targets and to coordinate their attacks [1].

Google Earth, Bing maps and other techniques of gathering information are extensively used by terrorist groups in the Middle East. One obvious example is the latest group working in Egypt called "Hasm Group" [2]. Hasm was a new terrorist group that appeared in July 2016 and is responsible for a number of deadly attacks inside the country. The name "Hasm" is an acronym for a phrase in Arabic "Harakat Sawa'ed Masr" which means "The Movement of Egyptian Arms". The group claimed the assassination attempt on the deputy prosecutor general in September 2016 as well as the assassination attempt on leading Islamic cleric Ali Gom'a in August of the same year. They have presence on social media websites and have their own website with many information gathered from open sources. Their techniques of infiltrating into Cairo, capturing photos of their targets, and using Google Earth prove that this group has technical savvy members. They even host their website in different countries with a domain guarding service from other countries such as Iceland and Romania. Hasm affiliation is not known but it appears to be not being affiliated with any Salafi-jihadi groups as they use music inside their propaganda video. It is possible that they are linked to Muslim Brotherhood.

Liwaa al-Thawra (Revolution Brigade) was another new group working inside Egypt exploiting open source information and they were responsible for the attack on a checkpoint in the Nile Delta governorate, Al-Menoufiyah in August 2016 [3]. This group also claimed responsibility of the assassination of Brig. Gen. Adel Ragaei, commander of the Egyptian Army's Ninth Armored

[1] Cohen-Almagor, R. (2017). Jihad Online: How Do Terrorists Use the Internet? Retrieved June 20, 2020, from Ssrn.com website: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2878429

[2] Ahram Online. (2017). Egypt court declares militant group "Hasm" terrorist organisation - Politics - Egypt. Retrieved June 20, 2020, from Ahram Online website: http://english.ahram.org.eg/NewsContent/1/64/257982/Egypt/Politics-/Egypt-court-declares-militant-group-Hasm-terrorist.aspx

[3] Ahram Online. (2016). Two policemen killed in attack on checkpoint in Egypt's Menoufiya - Egypt. Retrieved June 20, 2020, from Ahram Online website: http://english.ahram.org.eg/News/239306.aspx

Division. This little-known group has its own website and they use the same online tactics of Hasm group. Their website is hosted outside Egypt and they have protected their domain registration with WhoisGuard, Inc in Panama. The group is believed to be linked directly to Muslim Brotherhood with many quotes from Sayyid Qutb on their website and social media accounts. Evidence that may link this group to Hasm and Muslim Brotherhood is the killing of Muslim Brotherhood leading figure Mohamed Kamal by Egyptian security forces [1]. According to the interior ministry, Kamal oversaw the Muslim Brotherhood's "armed wings" and their "cells." Liwaa al-Thawra terrorist group, in its statement claiming responsibility for Adel Ragaei's killing, announced that the murder was primarily in "retaliation for the killing of Mohamed Kamal" [2].

Open source intelligence is part of open source warfare theory [3] that makes it possible for small autonomous and leaderless groups to defeat much larger enemies. As mentioned earlier, Al-Qaeda started adopting this open source Jihad strategy since the first issue of Inspire Magazine [4], which includes bomb making techniques, security measures, guerrilla tactics, weapons training and other dangerous activities that do not require a lone wolf to travel in order to learn. Just a simple Google search is enough. Open source Jihad is a very important technique that requires much attention from law enforcement agencies in order to understand how those jihadists think.

One of the most infamous articles which appeared in Inspire magazine was devoted to building a bomb from readily available ingredients that will

[1] Ahram online. (2016). Ahram Online - Senior Brotherhood "armed wing" leader killed in shootout: Egypt's Interior Ministry. Retrieved June 20, 2020, from Ahram.org.eg website: http://english.ahram.org.eg/NewsPrint/245165.aspx

[2] Ahram Online. (2018). A look at Hasm and Lewaa Al-Thawra terror groups - Features - Egypt. Retrieved June 20, 2020, from Ahram Online website: http://english.ahram.org.eg/NewsContent/1/151/256787/Egypt/Features/A-look-at-Egypts-youngest-militant-groups-Hasm-and.aspx

[3] Charette, R. N. (2007). Full Page Reload. Retrieved from IEEE Spectrum: Technology, Engineering, and Science News website: https://spectrum.ieee.org/telecom/security/opensource-warfare

[4] Lemieux, A. F., Brachman, J. M., Levitt, J., & Wood, J. (2014). Inspire Magazine: A Critical Analysis of its Significance and Potential Impact Through the Lens of the Information, Motivation, and Behavioral Skills Model. Terrorism and Political Violence, 26(2), 354–371. https://doi.org/10.1080/09546553.2013.828604

not raise suspicion when purchased. The article was titled “Make a Bomb in the Kitchen of Your Mom: The AQ Chef” [1]. Most law enforcement agencies in MENA do not pay much attention to these types of manuals and guides; however, this article gained international attention after the April 2013 Boston Marathon bombing in which two brothers used the same recipe to create the pressure cooker-bombs [2]. Other tactics with different recipes were used in Egypt by Muslim brotherhood affiliated groups to build a bomb from simple things such as fireworks, nails, and razors. In addition to AQAP magazine, there are also many online resources in Arabic that teach jihadists how to build a simple bomb from simple ingredients such as gasoline, cement, children toys’ batteries, nails, and sulfuric acid.

Open source Jihad does not only pose threats to law enforcement and intelligence agencies but went further to attack critical targets such as the aviation industry. Terrorist organizations such as Al-Qaeda and ISIL have strong motivation in attacking the aviation industry due to the psychological effect of such attacks that may paralyze the transportation at national and international levels [3]. Although attacking airplanes is not new, it turns now to be more dangerous than ever before due to the simple recruitment and radicalization of jihadists using social media. In many cases, terrorist organizations tried to recruit personnel working in the aviation industry to aid or execute the attack [4].

In 2015, a Russian Airbus A321 plane was shot down on its way from the Sinai Peninsula to Saint Petersburg. Although final investigation reports are not published yet, Russia and other countries believed that it was a bomb

[1] Ibid

[2] Speckhard, A. (2013). The Boston Marathon Bombers on JSTOR. Retrieved June 20, 2020, from Jstor.org website: https://www.jstor.org/stable/26296940?seq=1#metadata_info_tab_contents

[3] Almasy, S. (2015, November 4). A look at past attempts to bomb airplanes. Retrieved June 20, 2020, from CNN website: https://edition.cnn.com/2015/11/04/world/airline-bombing-plots/

[4] ICT. (2016). Trends in Aviation Terrorism. Retrieved June 20, 2020, from Ict.org.il website: https://www.ict.org.il/Article/1757/trends-in-aviation-terrorism#gsc.tab=0

planted under one of the plane's seats. Shortly after the crash, ISIL claimed responsibility of the terror attack and said that it had been able to detect a security breach at the international airport in Sharm El-Sheikh [1]. At the end of January 2016, Reuters [2] published a report stating that an EgyptAir mechanic is suspected in the Russian plane crash, according to sources familiar with the matter. Ironically, smuggling a bomb into an airplane and bypassing the airport security was explained in detail in Inspire Magazine, issue 13 [3]. This issue is very important in regard to airport security and the aviation industry; it included also the profiles of the most infamous terrorists who attacked airplanes; Ramzi Yusuf, Umar Farouk and Richard Reid. In the chapter called OSJ "Opensource Jihad", AQ's kitchen introduced the hidden bomb. The chapter describes clearly how to breach airport security and how build a hidden bomb that can bring an airplane down with simple ingredients such as hydrogen peroxide, found in most pharmacies. Although no evidence of a successful carried out attack using the recent AQ manual, it is still applicable if combined with the instructions of bypassing airport security or even recruiting an employee to smuggle the bomb onboard.

Following the Russian airplane bombing, an explosion occurred on Daallo Airlines Flight 159, 20 minutes after it took off from Mogadishu. A subsequent investigation indicated that the explosion was caused by a bomb planted by Al-Shabaab terrorist group [4]. Later, Somali authorities stated at a news conference that security camera video recordings showed suspicious activity by two airport baggage handlers and by members of the airline's staff;

[1] Stewart, W. (2015, November 23). Russian plane crash: Bomb on tourist jet that crashed in Egypt "was placed under a seat." Retrieved June 20, 2020, from Evening Standard website: https://www.standard.co.uk/news/world/bomb-on-russian-tourist-jet-that-crashed-in-egypt-was-placed-under-a-seat-a3120741.html

[2] Reuters Editorial. (2016, January 29). Exclusive: EgyptAir mechanic suspected in Russian plane crash. Retrieved June 20, 2020, from U.S. website: https://www.reuters.com/article/us-egypt-crash-suspects-idUSKCN0V712V

[3] Rudner, M. (2016). (Electronic Jihad): The Internet as Al Qaedas Catalyst for Global Terror. Studies in Conflict & Terrorism, 40(1), 10–23. https://doi.org/10.1080/1057610x.2016.1157403

[4] Winsor, M. (2016, February 4). Somalia Daallo Airlines Explosion: Wheelchair Passenger Suspected As Suicide Bomber. Retrieved June 20, 2020, from International Business Times website: https://www.ibtimes.com/somalia-daallo-airlines-explosion-wheelchair-passenger-suspected-suicide-bomber-2294861

therefore, they detained the employees for questioning [1]. On May 30, 2016, a Somali military court sentenced 10 people it said were behind the attack and they were working in the airport at different jobs [2].

With the help of recruited employees in critical targets, social media radicalization, and open source manuals, open source jihad will be more dangerous than ever before. Cyberspace has become the new battleground for terrorists either used for facilitating their attacks or targeting critical infrastructure to spread fear. Consequently, investigators need to understand this new threat in order to fight back.

2. Digital Forensics

2.1 Definition

The first Digital Forensic Research Workshop (DFRWS) took place in the year 2001. The goal of the workshop was to bring together academics and digital forensic practitioners to form a group that would help define the discipline and recognize the challenges that lay ahead [3].

At the first DFRWS, digital forensics was formally defined as a science and described as "the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources" [4]. Digital forensics can also be defined as the identification, preservation and analysis of digital evidence while following a

[1] GeeskaAfrika. (2016, February 7). Somalia: Airport Staff, Airline Employees Detained Over Somali Plane Blast - Geeska Afrika Online. Retrieved June 20, 2020, from Geeskaafrika.com website: http://www.geeskaafrika.com/15400/somalia-airport-staff-airline-employees-detained-over-somali-plane-blast/

[2] Reuters. (2016, May 30). Somalia sentences two to life in prison for February airline blast - Business Insider. Retrieved June 20, 2020, from Business Insider website: https://www.businessinsider.com/r-somalia-sentences-two-to-life-in-prison-for-february-airline-blast-2016-5?IR=T

[3] Palmer, G. (2001). A Road Map for Digital Forensic Research. Retrieved from https://www.dfrws.org/sites/default/files/session-files/a_road_map_for_digital_forensic_research.pdf

[4] Ibid

sound methodology that will be legally accepted [1]. This means that forensic science is ultimately for use in a court of law. Forensic science provides an all-encompassing body of proven investigative techniques and methodologies that digital forensic investigators use when conducting a digital forensic investigation involving electronic evidence [2].

2.2 The Digital Forensics Process

The Digital forensics process encompasses the following categories [3]:

- Identification
- Preservation
- Collection
- Examination
- Analysis
- Presentation

The digital forensics process categories can be explained as follows[4]:

- Preparation: The first step is to create a plan to perform a digital forensic investigation and obtain all the required support documentation, forensic tools, and hardware before commencing with the actual investigation.
- Identification: This step identifies and surveys all possible sources of digital evidence. This includes obtaining evidence from all possible devices at the crime scene such as routers with built-in storage, mobile devices, and many others. This also pertains to evidence that can be obtained via Internet services accessed on these devices.

[1] Kim-Kwang Raymond Choo, & Dehghantanha, A. (2017). Contemporary digital forensic investigations of cloud and mobile applications. Amsterdam; Boston; Heidelberg; London; New York; Oxford; Paris; San Diego; San Francisco; Singapore; Sydney; Tokyo: Elsevier.

[2] Ibid

[3] Palmer, G. (2001). A Road Map for Digital Forensic Research. Retrieved from https://www.dfrws.org/sites/default/files/session-files/a_road_map_for_digital_forensic_research.pdf

[4] Casey, E. (2007). Handbook of computer crime investigation: forensic tools and technology. Amsterdam; London: Academic.

- Preservation: This step ensures that all possible changes to the digital evidence are prevented. This step also extends to the collection of the evidence.
- Examination and Analysis: This step involves searching and analysing the evidence and has been described as the "application of a scientific method and critical thinking" to be able to answer the fundamental questions of any investigation.
- Presentation: This step involves drafting a report of the investigation findings that will stand up to be admissible in court.

2.3 Digital Evidence

With the increase of internet and digital devices usage, it is likely that digital evidence is currently present in almost any crime [(1)].

Digital evidence is defined as any data that can establish that a crime has taken place or provide a link between a crime and the victim or the crime and the perpetrator [(2)]. The Scientific Working Group on Digital Evidence (SWGDE) defines digital evidence as any "information that is useful and of sufficient value that is either stored or transmitted in a digital form" [(3)].

When conducting a forensic investigation and reviewing the reliability and quality proof, it is imperative that the proof is correct and reliable due to the effect that the results can have on a person in a court. Digital forensic investigators must ensure that only specific forensically sound tools and techniques are used to maintain the integrity of the evidence and to ensure that the evidence is admissible in a court of law. The integrity of digital

[(1)] Jordaan, J. (2012). A Sample of digital forensic quality assurance in the South African criminal justice system. Retrieved June 4, 2020, from undefined website: https://www.semanticscholar.org/paper/A-Sample-of-digital-forensic-quality-assurance-in-Jordaan/a649b1238b3e265ff2f48bbd2e890e9495407df3

[(2)] Casey, E. (2007). Handbook of computer crime investigation: forensic tools and technology. Amsterdam; London: Academic.

[(3)] SWGDE - Documents. (2020). Retrieved June 4, 2020, from Swgde.org website: https://www.swgde.org/documents evidence must be ensured throughout the entire forensic investigation, and further asserts that hash sums should be calculated on the source evidence system and the evidence extracted. These are then to be compared to ensure authenticity and integrity of the evidence [1].

The key activity performed during a forensic investigation is the creation of a cryptographic hash. “A cryptographic hash function takes an arbitrary amount of data as an input and returns a fixed size string as output and the resulting value is a hash” [2]. Hashing usually takes place during the verification phase of the disk imagery process, as any modification, even to a single bit of data, will produce a completely different hash value. This means that a hash generated from the source drive can be compared to the hash of the forensic image and this confirms that the two items are exactly the same if the hashes match.

3. Open Source Intelligence

3.1 Definition

There are many definitions for Open Source Intelligence (OSINT); however, it is mainly the unclassified information that is being discovered, legally collected, categorized, and disseminated. OSINT described also as an intelligence gathering discipline that consists of collecting information from public or open sources and analyzing this information to produce valuable intelligence [3]. While OSINT is very valuable to policymakers, it is also cheaper source of intelligence [4]. According to the RAND study [5], OSINT

[1] Adelstein, F. (2006). Live forensics. Communications of the ACM, 49(2), 63. https ://doi.org/10.1145/1113034.1113070

[2] Altheide, C., & Carvey, H. A. (2011). Digital forensics with open source tools: using open source platform tools for performing computer forensics on target systems: Windows, Mac, Linux, UNIX, etc. Rockland, Mass.: Syngress; Oxford.

[3] Neri, F., Geraci, P., & Pettoni, M. (2011). Stalker: overcoming linguistic barriers in open source intelligence. International Journal of Networking and Virtual Organisations, 8(1/2), 37. https://doi.org/10.1504/ijnvo.2011.037160

[4] INTellingence: Open Source Intelligence — Central Intelligence Agency. (2010). Retrieved June 4, 2020, from Cia.gov website: https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/open-source-intelligence.html

[5] Williams, H. J., Williams, H. J., Blum, I., & Blum, I. (2018). Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise: Retrieved June 13, 2020, from Rand.org website: https://www.rand.org/pubs/research_reports/RR1964.html

is publicly available information that has been discovered, determined to be of intelligence value, and disseminated by a member of the IC (Intelligence Community). This is consistent with the U.S. definition in Section 931 of Public Law 109-163 that defines OSINT as “intelligence that is produced from publicly available information and is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement.” Open Source Information (OSIF) is merely unclassified data available to the public, while OSINT results from applying processing and exploiting the information to validate it as relevant, accurate, and actionable for use by the consumers [(1)].

It is important to distinguish between “open” and “free”. Being open means that everyone has the potential to see it in a lawful way. Furthermore, the information must be based on freely, widely available sources but open is not the same as free [(2)].

In the NATO OSINT Reader, they refer to a definition of open information from the Director of the Central Intelligence Directive:

“Open source information for purposes of this directive is publicly available information (i.e., any member of the public could lawfully obtain the information by request or observation), as well as other unclassified information that has limited public distribution or access. Open source information also includes any information that may be used in an unclassified context without compromising national security or intelligence sources and methods. If the information is not publicly available, certain legal requirements relating to collection, retention, and dissemination may apply.” [(3)]

Open Source Information is, according to this definition, “publicly available

[(1)] Ibid

[(2)] Babak Akhgar, P Saskia Bayerl, & Fraser Sampson. (2018). Open Source Intelligence Investigation From Strategy to Implementation. Cham Springer International Publishing Springer.

[(3)] NATO. (2002). NATO Open Source Intelligence Reader. Retrieved June 21, 2020, from Oss.net website: http://www.oss.net/dynamaster/file_archive/030201/254633082e785f8fe44f546bf5c9f1ed/NATO%20OSINT%20Reader%20FINAL%2011OCT02.pdf information”. The principle to be publicly available is if any member of the public could lawfully obtain the information by request or observation. It also defines unclassified information that is subject to limited public distribution or access, as well as information that can be used as open source information in an unclassified context without compromising national security. FBI also defines Open source intelligence as:

“...the intelligence discipline that pertains to intelligence produced from publicly available information that is collected, exploited, and disseminated in a timely matter to an appropriate audience for the purpose of addressing a specific intelligence requirement”. [1]

3.2 OSINT Sources

OSINT came into existence before the digital age and was connected to intelligence gathering from open sources of information, such as newspapers and public speeches, largely by the military, but also by other institutions with their own intelligence gathering agendas. As the Internet developed and made more and more unrestricted sources of information available, OSINT’s urgency increased exponentially [2]. OSINT can be applied to print or electronic formats, such as television, newspapers and more recently, for information available on the Internet. Intelligence analysts have been using OSINT to complement classified information for many years. Thanks to the ability of Internet browsing, search, indexing and search engines, the Internet has become a critical tool for every intelligence analyst. The majority of people have embraced the Internet and social networking sites, ensuring that certain personal life records are embedded in the public, semi-public and deep web of the Internet.

OSINT relies on the collection of various sources of information including

[1] Babak Akhgar, P Saskia Bayerl, & Fraser Sampson. (2018). Open Source Intelligence Investigation From Strategy to Implementation. Cham Springer International Publishing Springer.

[2] Ibid

Internet data such as gathering data from social media website. This intelligence is of value for national security, market research and market competitors. Facebook and Twitter are mined for law enforcement purposes, while online news channels are also monitored to detect and prevent terrorist activities[1].

3.3 OSINT Advantages and Values

OSINT has numerous advantages, including the fact that collecting information from open sources is usually less expensive and less risky compared with collecting information from other sources of intelligence. OSINT can offer insights into emerging trends like emerging political movements, new technologies, political events, and people's mass movements. It can also reduce the burden placed on classified intelligence collection by limiting information requests to only that which is not available nor accessible through OSINT resources [2].

The main problem facing intelligence analysts is the overload of information, with the volume of information publicly available. Most of the time there is no value to the available information and sifting through the mountains of available data becomes time- and resource-intensive. Intelligence analysts should use their proven classified intelligence methods to exploit OSINT, as this will provide them with an all-inclusive intelligent suite of products [3].

When it comes to the value of OSINT, the intelligence community is re-examining OSINT's value because it is freely accessible online. Some intelligence communities say one of the drawbacks of using OSINT is the slow development of analytical tools that allow analysts to analyze, collect and distribute large volumes of open source information. However, excluding

[1] Ibid

[2] Best, R. A., & Cumming, A. (2007). Open Source Intelligence (OSINT): Issues for Congress. United States: Library Of Congress Washington Dc Congressional Research Service.

[3] Robert David Steele. (2006). The Smart Nation Act: public intelligence in the public interest. Oakton, Va.: Oss, Inc.

information available on the Internet is equivalent to excluding the largest freely available data source, as the Internet enables trade, encourages, and promotes human interaction and provides entertainment [1].

OSINT can combine all available resources and expertise without security clearance and produce intelligence that can be shared with everyone. This is extremely valuable for early warning and law enforcement investigations. One downside of the free Internet information is that this information needs to be tested for its source and reliability [2]. Nowadays, information that is freely accessible on the Internet sometimes proves to have greater value in helping intelligence analysts understand the world than the findings of conventional cloak and dagger intelligence. Intelligence professionals agree that OSINT is useful and should therefore be collected and analyzed in the same way as classified intelligence is collected and analyzed [3].

Although many resources are available to OSINT, the intelligence communities need advanced tools to traverse the oceans with available information. Even though the Internet has provided intelligence analysts with search engines and translation apps, more advanced tools and methods are needed [4].

3.4 Verification of OSINT Sources

OSINT has always been available, but in the last few years it has received recognition and has been widely used. In addition, OSINT does not always have to be obtained openly; some information can be obtained discreetly. However, this intelligence must always be accurate, reliable, timely and

[1] Ibid

[2] Babak Akhgar, P Saskia Bayerl, & Fraser Sampson. (2018). Open Source Intelligence Investigation From Strategy to Implementation. Cham Springer International Publishing Springer.

[3] Best, R. A., & Cumming, A. (2007). Open Source Intelligence (OSINT): Issues for Congress. United States: Library Of Congress Washington Dc Congressional Research Service.

[4] Williams, H., & Blum, I. (2018). Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise. Retrieved from https://www.rand.org/content/dam/rand/pubs/research_reports/RR1900/RR1964/RAND_RR1964.pdf

verifiable [1]. OSINT is in the public domain and should not be confused with "publicly available," as certain obstacles to OSINT access are present. The obstacles are usually resources and the effort required to collect the OSINT. One of the methods that can be used to obtain more information from open sources is the covert operations. These techniques can be used to trick the suspect to accept friendship or relation with fake accounts created by Law Enforcement on Facebook and other social media websites [2].

The verification of an OSINT source can be done based on several factors [3]. These factors can be categorized as follows:

- Authority
- Accuracy
- Objectivity
- Timeliness
- Relevance

According to the study by University of Essex[4], the authority of a source depends on the credibility of the online account that published the information. Regarding the accuracy, how accurate is the source and whether it is verifiable or not. Objectivity is an important factor which determines if the source is biased or not. Time and date of the information published is another important factor that should be added and verified during investigating OSINT sources, and finally the relevance of the source.

[1] Gibson, S. (2020). Open source intelligence. Retrieved June 5, 2020, from The RUSI Journal website: https://www.tandfonline.com/doi/abs/10.1080/03071840408522297

[2] 2012 Law Enforcement Social Media | LexisNexis Risk Solutions. (2012). Retrieved June 5, 2020, from LexisNexis Risk Solutions website: https://risk.lexisnexis.com/insights-resources/white-paper/2012-law-enforcement-social-media

[3] Babak Akhgar, P Saskia Bayerl, & Fraser Sampson. (2018). Open Source Intelligence Investigation From Strategy to Implementation. Cham Springer International Publishing Springer.

[4] University of Essex. (2018b). Introductory Guide to Open Human Rights Centre Clinic. Retrieved from https://www1.essex.ac.uk/hrc/documents/Introductory_Guide_to_Open_Source_Inteligence_and_Digitial%20Verification.pdf

3.5 Legal Challenges of OSINT

There is no legal definition of what open or closed sources of information are. That does not mean this is an area of no legislation. Referring to NATO's definition of open sources of information, legal access is required [1]. When open information denotes lawful access, it means in practice that one can obtain the information without committing an offence. That does not mean that the information is provided and made open without any offence.

For example, Wikileaks is an organization that publishes classified information they receive from various sources that have either stolen information or broke into systems. This information is widely used by reporters [2]. Similarly, the Panama Papers were large quantities of supposed stolen information published on the internet by the law firm Mossack Fonseca in Panama [3]. For several countries, these records were primarily used by tax authorities to monitor properties that are suspected of being tax deprived. In other words, the original access to information may not be lawful but the individuals accessing this information after they were published online must be lawful.

A borderline between what is available and what comes from open sources can also be drawn. For most cases open sources are not the only knowledge source but are part of the overall picture. This applies whether it is a journalist, an intelligence officer or an investigator who collects information. The reason why it is important to distinguish between open and closed information is that one can freely refer to open information, irrespective of position, as it is available to everyone. In each case, however, a reference to closed sources must be taken into account.

Irrespective of whether the information comes from open or closed sources,

[1] NATO. (2001). NATO Open Source Intelligence Handbook. NATO. (Original work published 2001)

[2] WikiLeaks. (2019). Retrieved June 20, 2020, from Wikileaks.org website: https://wikileaks.org/

[3] ICIJ Offshore Leaks Database. (2020). Retrieved June 20, 2020, from Icij.org website: https://offshoreleaks.icij.org/

an investigator will have a limitation on collecting information from people. If a person has a blog in which he or she publishes information about his or her private life, the investigator will be able to follow his or her blog without infringing the privacy laws. In the case of any storage and use of personal data by the police, however, the Data Protection Rules apply irrespective of whether the data is collected from open or closed sources [1]. Investigators, therefore, should collect, store, and use personal data about citizens with a legal reason for their storage and use. Although there are no legal boundaries between the open and closed sources of information, the legal issues have a meaning that one must be aware of, both for accessing, storing, and using information, particularly for government agencies. When it comes to legal perspectives, it is important to distinguish between "open" and "free" as the two terms are not equal.

With the increase of cybercrime and cyberterrorism, there is also increase in the serious threats related to violating human rights. There has been long debate when it comes to using OSINT and protecting human rights, privacy, and data. For Internet users, the Council of Europe has produced a guide to clarify the existing understanding of human rights, particularly in this context. In relation to public authorities, it is expressly stated that any interference should not be arbitrary, pursue a legitimate objective pursuant to the European Convention on Human Rights (ECHR), such as the protection of national security or public order , public health or morals, and comply with human rights legislation [2]. Although investigators have certain investigatory powers, they have to consider legislation considering the balance between conditional rights and public or national security.

Police investigatory powers are established at national level and shall take

[1] Sunde, I. M. (2017). Cybercrime Law. Digital Forensics, 51–116. https://doi.org/10.1002/9781119262442.ch3

[2] ECHR. (2013). European Convention on Human Rights - Official texts, Convention and Protocols. Retrieved June 21, 2020, from Coe.int website: https://www.echr.coe.int/Pages/home.aspx?p=basictexts

into account specific national practices, policies, cultures and priorities. This is crucial, but in relation to investigating cybercrime, to which territorial boundaries are often irrelevant, the differences can be unhelpful and may provide frustrating obstacles. Many countries have extended the powers of investigators to investigate cybercrime and cyberterrorism which override normal perceptions of privacy and have met with opposition by human rights advocates. OSINT as a technique to investigate such crimes will not be different when used under investigatory powers of law enforcement authorities; however, certain obstacles may appear as what is legal in a country may be illegal in another country.

Based on the mentioned issues, legal matters surrounding OSINT investigations are uncertain in many areas due to the lack of a case law dealing specifically with these practices. However, investigators still need to understand certain issues related to conducting OSINT investigation from legal perspective. OSINT techniques often involve accessing and downloading materials which might be copyrighted and later used as evidence. This process may per se result in the commission of an offence. Other techniques in OSINT such as using fake profiles in communicating with a suspect or collecting specific information may fall into the category of an offense under the UK Computer Misuse Act 1990 (1). However, this will not be the case in other countries.

Privacy and Data protection is another legal dimension when it comes to OSINT investigations. Different privacy and data protection legislations are being used around the world; however, the EU has two main legislations which are the EU Data Protection Directive (2) and General Data Protection Regulation (GDPR) (3).

(1) HM Government. (2008). ARRANGEMENT OF SECTIONS Computer misuse offences. Retrieved from http://www.legislation.gov.uk/ukpga/1990/18/pdfs/ukpga_19900018_en.pdf

(2) EUR-Lex - 31995L0046 - EN - EUR-Lex. (2018). Retrieved June 21, 2020, from Europa.eu website: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046

(3) Ibid

Although these regulations can be applied when dealing with online information related to persons, there is currently no EU legislation covering data protection issues relating to police investigations in domestic situations. The GDPR for instance, deals with the processing of personal data for purposes of police and judicial cooperation but it applies to the data transmitted between Member States and provides minimum standards to be abided by. In 2016, the EU introduced the Police Directive to be added to the EU Data Protection Reform package [(1)]. The Directive deals with the processing of personal data for authorities responsible for preventing, investigating, detecting, and prosecuting crimes. It ensures that police forces can efficiently do their work using technological means while preserving the fundamental rights of citizens. The Directive is designed to be consistent with the (GDPR).

In the countries where United Nations Office on Drugs and Crime (UNODC) OSINT training was delivered, there were no laws regulating the protection of personal data during online investigations [(2)]. In 2018, Lebanon passed a special law for the Electronic Transactions and Personal Data; however, it does not explicitly regulate police investigation in relation to online data and is considered very weak legislation [(3)]. In Egypt, there is a Data Protection legislation issued in 2020[(4)]. In Iraq, there is no specific law or proposed draft legislation dealing with Data Protection at the time of writing this research.

4. Digital Forensics and Open Source Intelligence Methodology

Based on the UNODC training, the researcher developed a methodology

[(1)] Police Directive. (2020). Retrieved June 21, 2020, from European Data Protection Supervisor - European Data Protection Supervisor website: https://edps.europa.eu/data-protection/our-work/subjects/police-directive_en

[(2)] Greenleaf, G. (2017). Global Tables of Data Privacy Laws and Bills (5th Ed 2017). Retrieved June 21, 2020, from Ssrn.com website: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2992986

[(3)] State of Privacy Lebanon. (2019). Retrieved June 21, 2020, from Privacy International website: https://privacy-international.org/state-privacy/1081/state-privacy-lebanon#dataprotection

[(4)] Law No. 151 of 2020. (2020). Retrieved August 15, 2020, from International Trade Administration website: https://www.trade.gov/market-intelligence/egypt-data-protection to apply the standards and processes of digital forensics to open source intelligence in order to standardize the techniques used in investigating cybercrime.

A good process should ensure that the investigator does not skip steps in the investigation, and that the entire Chain of Custody is properly managed. To ensure a good process, the process needs to be based on a methodology. The methodology describes the phases to be reviewed and what is included in each phase so that, through the process, it can be used as a manual.

The methodology's purpose is to define a structured investigation to ensure that it remains forensically sound. The investigation may be considered forensically sound if it meets the principles, standards and processes of digital investigation that have been established. A methodology for digital evidence investigation must be based on digital forensics principles and common law enforcement and industry practices [1].

Open source information should be used as a basis both for ordinary investigations and intelligence-led investigations due to the large amount of information in open sources. Where the information is used as the basis for intelligence-led investigations, it will not necessarily be used in court as evidence. Nevertheless, it is important to maintain an Audit Trail so that decision-makers can rely on the information that the decision is based upon being correct. In case the information is to be used as evidence for prosecution, the authenticity and integrity of the evidence must be safeguarded in such a way that the value of the evidence cannot be questioned.

There are different models which present a methodological process for working with digital evidence. There are several Digital Forensic Investigation Process standards and guidelines such as ISO / IEC 27037 and NIST SP 800-

[1] Mckemmish, R. (1999). What is forensic computing? Canberra: Australian Institute Of Criminology.

86 lay out standards for digital evidence investigation [1]. Guidelines such as ACPO Guidelines IOCE Guidelines and the Electronic Evidence Guide (EEC) are also published with advise on how digital evidence is to be handled[2]. They will be both advisory standards and guidelines. That means evidence will not be automatically rejected because a given standard or guideline has been followed, but it is designed to ensure digital evidence is forensically sound.

The proposed methodology ensures that standards and guidelines should be used when applying OSINT techniques in cybercrime investigation based on digital forensics standards with additional steps that ensure the admissibility and forensically sound evidence. According to [3], there are important steps that should be followed when performing digital forensics as shown in Figure1.

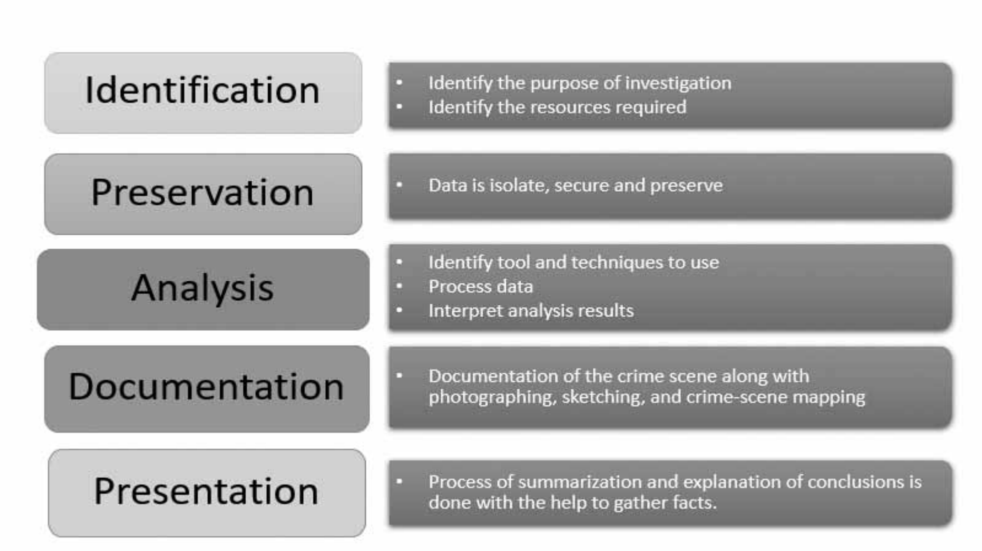

Identification
Identify the purpose of investigation
Identify the resources required
Preservation
Data is isolate, secure and preserve
Analysis
Identify tool and techniques to use
Process data
Interpret analysis results
Documentation
Documentation of the crime scene along with photographing, sketching, and crime-scene mapping
Presentation
Process of summarization and explanation of conclusions is done with the help to gather facts.

Figure 1. Digital Forensics Process

The National Institute of Standards and Technology (NIST) standard

[1] Beckett, J., & Slay, J. (2011). Scientific underpinnings and background to standards and accreditation in digital forensics. Digital Investigation, 8(2), 114–121. https://doi.org/10.1016/j.diin.2011.08.001

[2] Guttman, J. D. (2009). Introduction. Journal of Computer Security, 17(5), 515–515. https://doi.org/10.3233/jcs-2009-0396

[3] Casey, E. (2007). Handbook of computer crime investigation: forensic tools and technology. Amsterdam; London: Academic.

includes the following digital forensics steps as shown in Figure 2, which are used as approved guidelines in digital investigations [1].

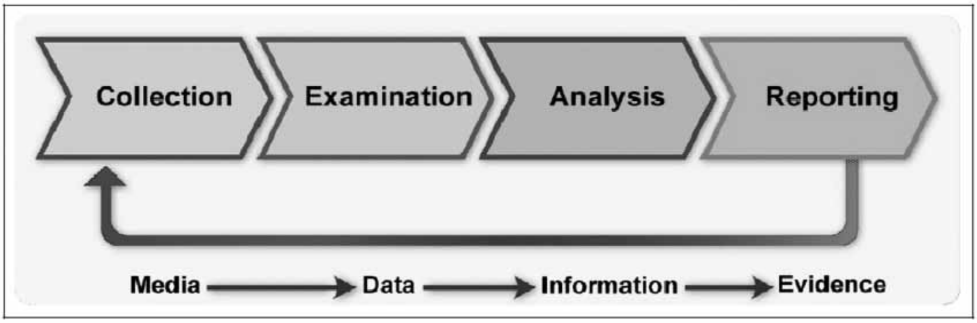


Figure 2. NIST Digital Forensics Process

The available standards in digital investigations can be used when performing OSINT techniques in digital investigations or in cybercrime investigations. However, there are some additional steps the researcher recommends that they should be added to the standards in order to produce a forensically sound OSINF that may be used as admissible evidence. These recommended steps are:

- Visualization of open source information gathered through OSINT techniques;
- Collaboration of more than one investigator to find relevant information or evidence in a case.

The proposed steps can be implemented in the mentioned standards and applied to all OSINT techniques in cybercrime investigation and even conventional crimes as shown in Figure 3.

[1] Widup, S. (2014). Computer forensics and digital investigation with Encase Forensic v7. New York: Mcgraw-Hill Education.

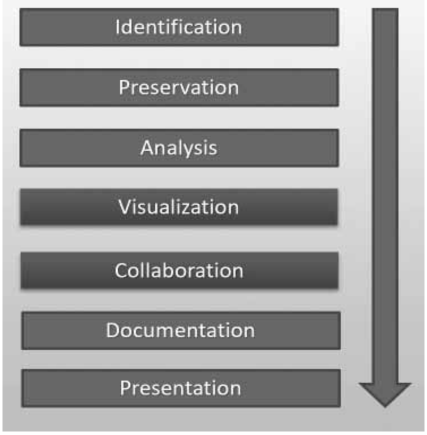


Figure 3. Proposed model to be used with OSINT investigations

4.2 Applying the new methodology

To introduce the new proposed methodology, the researcher used practical cases to explain how this model will be applied to OSINT techniques. During the UNODC training, real cases were introduced to the participants in order to be solved using OSINT techniques following the proposed methodology. The researcher prepared several cases in the form of Capture the Flag (CTF) competitions to encourage participants to find the real information on the internet and collaborate to connect the dots related to the proposed cases. Following are the steps used by the participants to solve the cases.

4.2.1 Identification

The first step is to identify persons of interest in the case to gather information using OSINT techniques. Information obtained may include potential associates, place and date of birth, any photographs of a key person, possible contact numbers, locations visited, marital status, current employer, previous employer, and a list of schools. There is also benefit in being able to recognize key individuals' interests, such as sports, hobbies, or social groups, as this information helps to build a profile of the person or persons of interest.

As members of social groups prefer to exchange information openly, photos of social activities attended by the participants are especially useful. However, before starting the search to identify persons of interests or other objects in the case, one must understand the structure of the data found online. Therefore, an online schema model [1] can be used to help investigators concentrate on the type of information and relations that can be gathered using OSINT techniques.

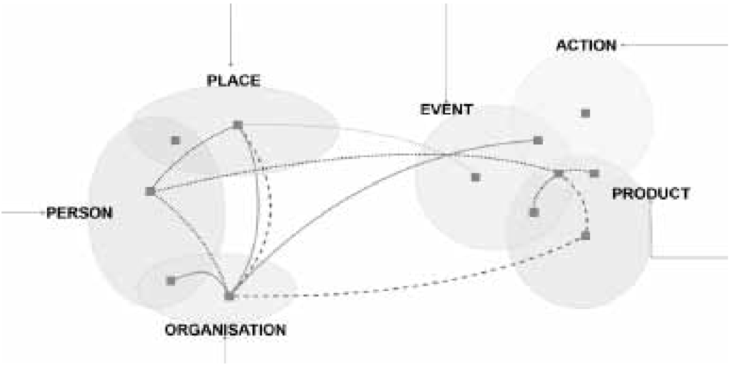


Figure 4. Entity relationship, OSINT Collection Schema (2)

Schema.org was funded by Google, Microsoft, Yahoo and Yandex. It is crucial to the development of a standardized model for repeatable performance and consistency with most other systems. Using the schema, investigators can search for a person's data, places, events, organizations, actions, and products. Identification will help an investigator to think where to find the information.

4.2.2 Collection / Preservation

There are many tools available to collect OSINF from online sources depending on the type of object. However, the collection of information should follow the proposed methodology to produce forensically sound evidence. It is essential that investigators always remain ethical and do not collect any

[1] Schemas. (2020). Retrieved June 12, 2020, from Schema.org website: https://schema.org/

[2] Chris. (2019, September 22). OSINT Collection Schema. Retrieved June 12, 2020, from OSINT Combine website: https://www.osintcombine.com/post/osint-collection-schema

evidence in a legally questionable manner, as this would make the evidence inadmissible in a court of law. Investigator must also be aware of not violating the terms and conditions of the various websites such as social media. The extraction of evidence from social media is most often a difficult task, and legal advice and assistance may be required to obtain evidence. Various laws governing privacy, access to information, electronic communication, and data transmission, to name a few, must also be fully understood and considered as evidence may be located in a foreign country.

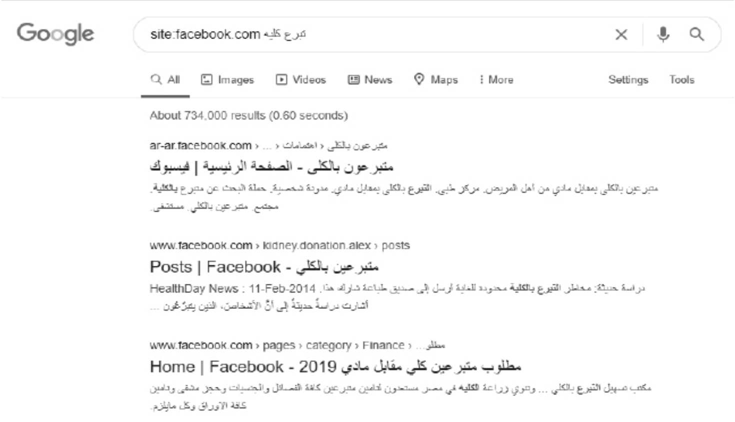
Preservation principle in digital forensics should be observed when collecting information from online sources. This ensures the least amount of change will be made to the data processed electronically and any inevitable changes can be compensated for and justified. In a situation where the evidence data is changed, the digital forensic investigator must document and be able to explain what changes have taken place and why [(1)].

Collection of open source information can be accomplished in variety of ways. Search engines are a good choice to start, especially Google and Yandex. Google is better when using advanced search operators and Yandex is a good choice if an investigator is looking for photos of person of interest [(2)] as the facial recognition algorithm in Yandex is way more advanced than Google reverse image search.

Social media websites such as Facebook include a wealth of information about targets due to its large user base and the dynamic nature of posted content. The Google search engine can be used to search within social media using advanced search operators: “site:facebook.com” as shown in figure 5.

[(1)] Mckemmish, R. (1999). What is forensic computing? Canberra: Australian Institute Of Criminology.

[(2)] Yandex.Images: search for images on the internet, search by image. (2011). Retrieved June 12, 2020, from Yandex website: https://yandex.com/images/



About 734,000 results (0.60 seconds)

ar-ar.facebook.com › ... › اهتمامات › متبرعون بالكلى

متبرعون بالكلى - الصفحة الرئيسية | فيسبوك

متبرعين بالكلى بمقابل مادي من أهل المريض. مركز طبي. التبرع بالكلى بمقابل مادي. مدونة شخصية. حملة البحث عن متبرع بالكلية.
مجتمع. متبرعين بالكلي. مستشفى.

www.facebook.com › kidney.donation.alex › posts

Posts | Facebook - متبرعين بالكلي

HealthDay News : 11-Feb-2014 .دراسة حديثة: مخاطر التبرع بالكلية محدودة للغاية أرسل إلى صديق طباعة شارك هذا
أشارت دراسةٌ حديثةٌ إلى أنّ الأشخاص، الذين يتبرّعون ...

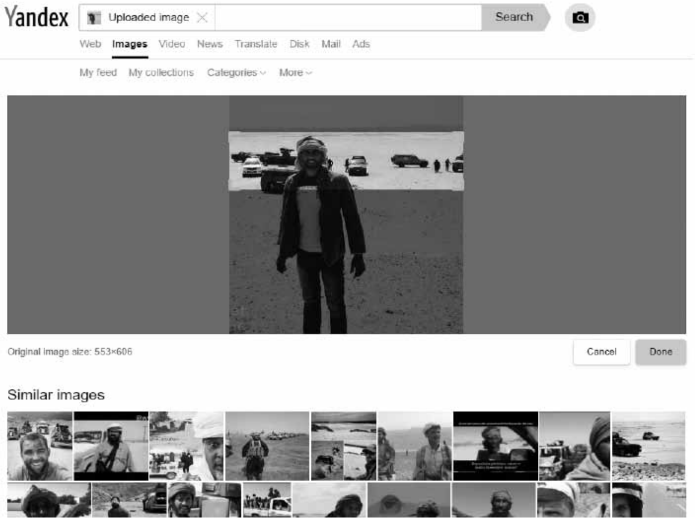
www.facebook.com › pages › category › Finance › ...مطلو

Home | Facebook - 2019 مطلوب متبرعين كلي مقابل مادي

مكتب تسهيل التبرع بالكلي ... وتنوي زراعة الكليه في مصر مستعدون لتامين متبرعين كافة الفصائل والجنسيات وحجز مشفى وتامين
كافة الاوراق وكل مايلزم.

Figure 5. Searching Facebook for people trading human organs in Arabic

Searching for individuals can be done using the Russian search engine, Yandex, either through advanced operators or reverse image search if the investigator has an image of the suspect as shown in figure 6.

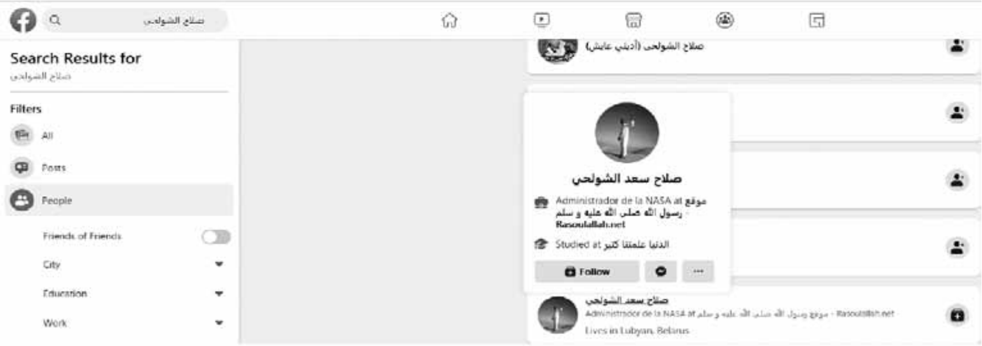


Original image size: 553×606

Similar images

Figure 6. Searching Yandex for suspect photos

When conducting a search on an individual using the first and last names of the individual, a web search using a web search engine such as Google and Yandex is advisable first. The returned search results should then be further investigated, as information made available from some of the web links gleaned from the web search could be useful and revealing. A further search can be done using social networking tools such as the LinkedIn and Facebook search facilities. There are many tools available that can be used to search within social media websites. But it is advisable to start searching using the search features available in these websites and look for the advanced search options. Sometimes, investigators will not be able to get more details from websites such as Facebook due to privacy options. In this case, it is advisable to search through some of the friends of the Facebook profile as there is a possibility that one of these Facebook profiles is not as secure and information about the individual may have been shared via friends' with unsecured Facebook profiles.



صلاح الشولحى (أدبني عايش)

صلاح سعد الشولحي

Administrador de la NASA at موقع رسول الله صلى الله عليه و سلم - Rasoulallah.net

Studied at الدنيا علمتنا كتير

صلاح سعد الشولحي

Administrador de la NASA at موقع رسول الله صلى الله عليه و سلم - Rasoulallah.net

Lives in Lubyan, Belarus

Figure 7. Facebook search feature (Searching for suspect in a case)

It is not possible now to go deeper in searching Facebook using the normal Facebook search as Facebook closed the Graph search; however, other techniques are still available to get more details from Facebook. Developers and OSINT practitioners are regularly delivering new tools, but it is not guaranteed to be working forever as well as previous tools used to collect data from social media, especially Facebook. Chrome extensions, for example are a good choice for investigators to collect and extract data from Facebook, LinkedIn, and other social media sites [1].

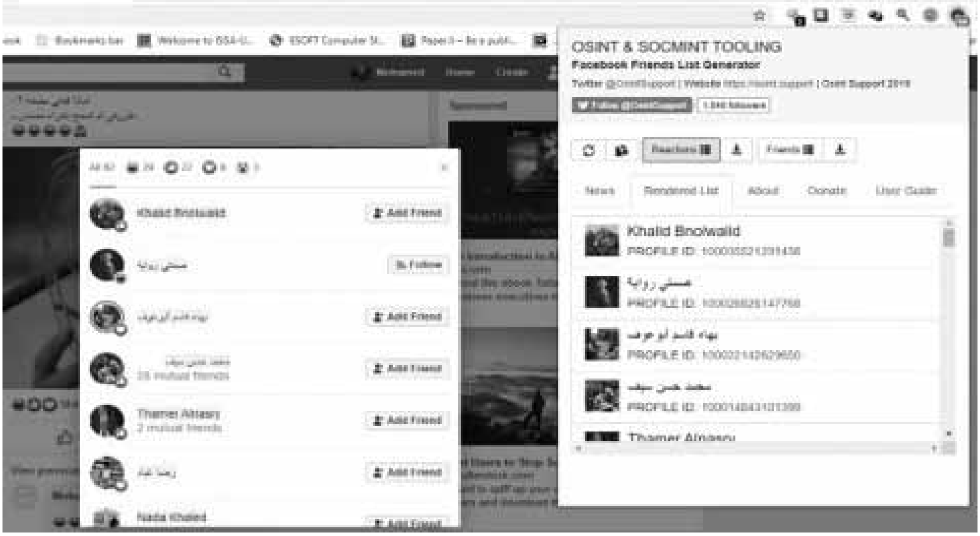


Figure 8. Facebook Friends List Generator (Chrome Extension)

When searching for persons' names, usernames, emails or online handlers, investigators can also use many tools available for free or with low fees. Using the same username or on-line alias across multiple social networking platforms is common practice for social media users. Once the screen name or online alias has been identified for an individual, an online search should be conducted using a web search engine or the online tool known as "NameChk" can be used in conjunction with the known online alias [2].

[1] Osint Support. (2020). Chrome Extensions. Retrieved June 12, 2020, from Osint Support website: https://osint.support/chrome-extensions/

[2] Namechk. (2020). Retrieved June 12, 2020, from Namechk.com website: https://namechk.com/

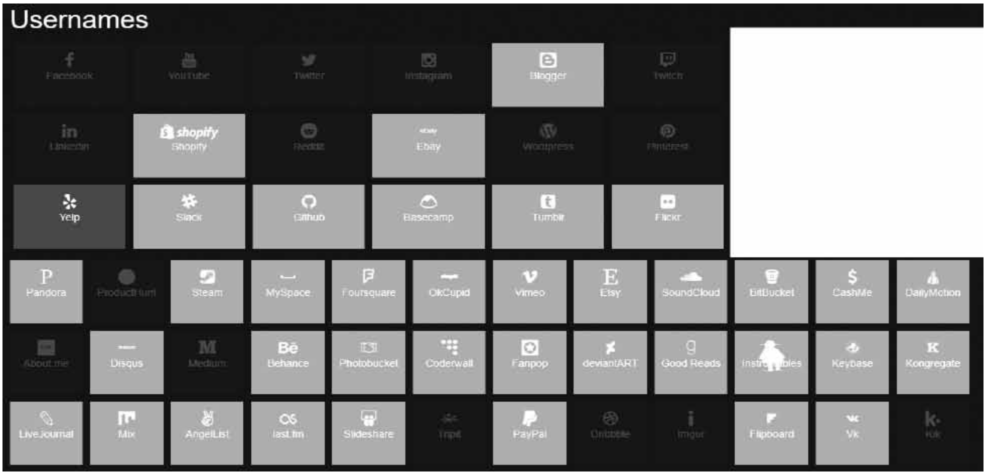


Figure 9. Finding usernames across different networks using Namechk tool

The “NameChk” web-based tool allows one to enter an online alias to see the availability of a particular online alias across different social networking sites. If the online alias is in use, the link can be selected and will be opened to the social networking site registered with that particular online alias, enabling the investigator to determine whether a site belongs to the person being searched. Another tool that is available to search for usernames, IP address and emails is SpiderFoot [1]. This tool makes it easy for investigator to automate the OSINT search across the internet sources in addition to providing a link analysis of the found results as shown in Figure 10 and Figure 11.

[1] SpiderFoot. (2020, March 30). Retrieved June 12, 2020, from SpiderFoot website: https://www.spiderfoot.net/

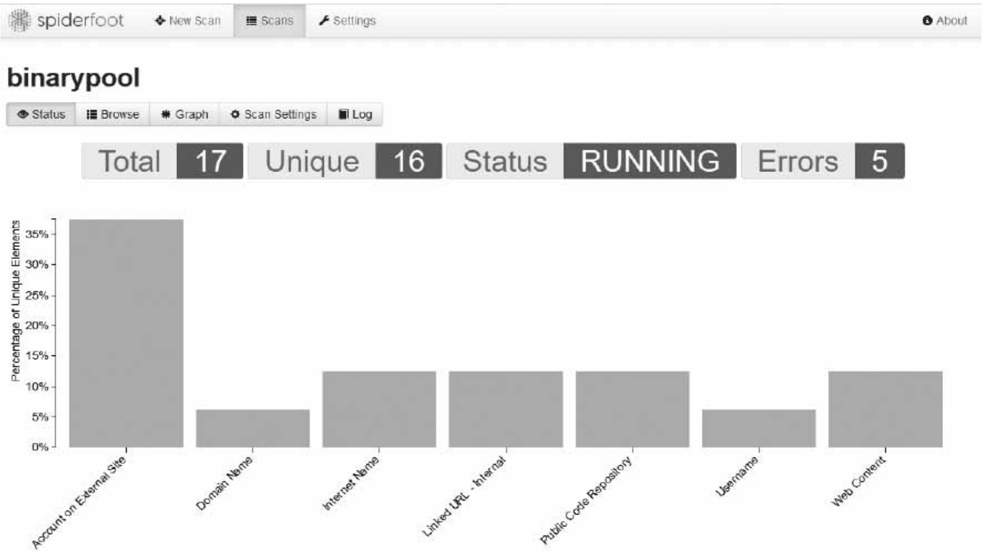


Figure 10. SpiderFoot running search for unique username

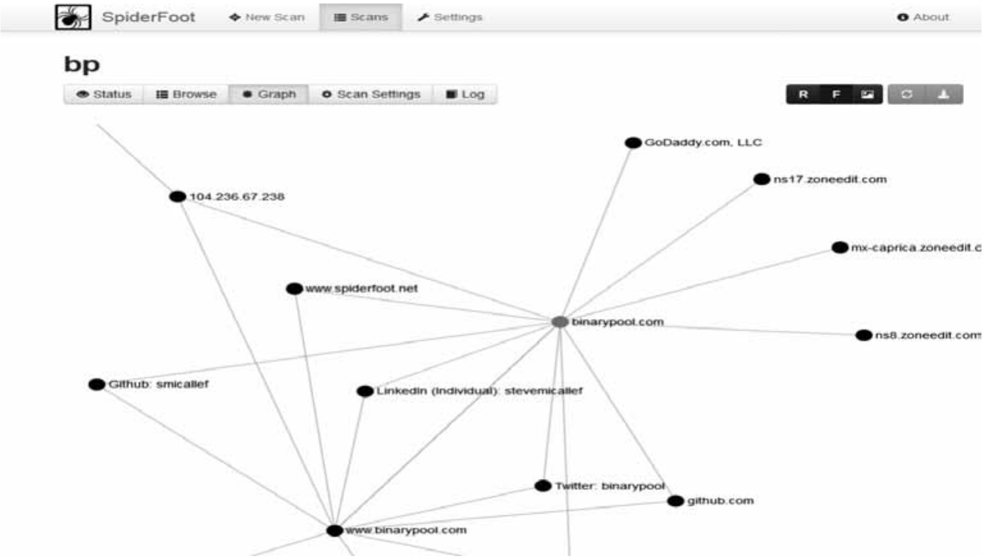


Figure 11. Graph tool in SpiderFoot which helps connect the dots

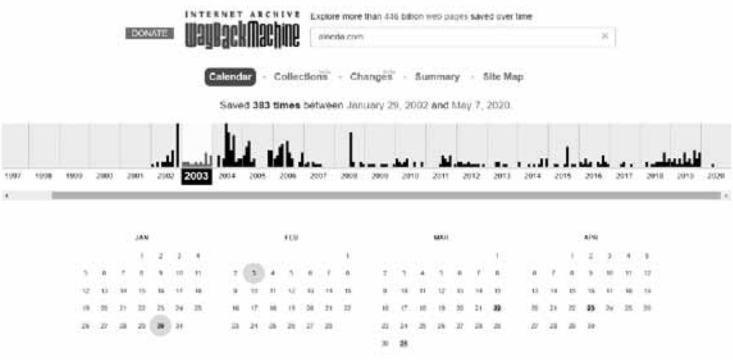
Although this automated OSINT tool is vital in searching for available online information, it is important that investigators pay attention to the false positive which can be found in the results. Findings from automated OSINT tools need to be treated with caution as it should be verified before considered accurate information in any case [1].

In the collection and preservation step, investigators may not find all information available using search engines and other tools that search in the surface web. Deeper web search is needed in this case. Deep web or invisible web includes data and information that is not indexed by search engines such as databases, deleted website copies and hidden links [2]. Collecting information from deleted websites or web pages is one example of finding information in the deep web.

Since 1996, the digital internet archiving tool known as the Wayback machine has built an internet archive and archived billions of web pages. The Internet archive contains web pages, films, audio, text, and software, enabling one to search for archived 1996 data. However, not all websites allow archiving; if the website does not allow the "robot.txt" protocol, the Wayback machine may not be able to archive the website. An example is Facebook which does not allow the robot.txt protocol to run without written permission on its site. However, if an investigator were to enter a website URL archived by the Wayback machine, he / she would be able to access the website as it appeared on each of the dates on which the Wayback machine initiated the website archiving. Figures 12 and 13 show and example for a deleted terrorist website called www.alneda.com with copies of its pages.

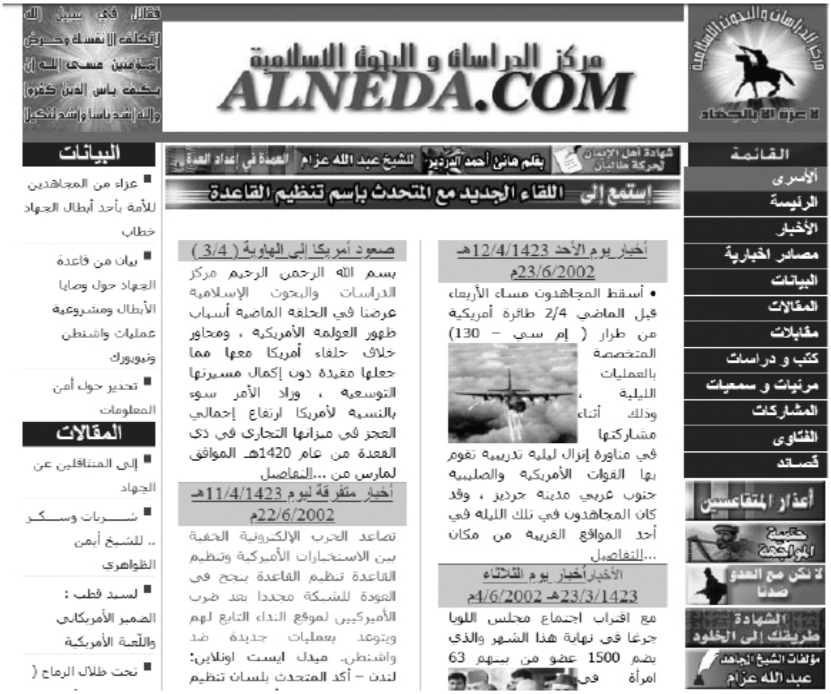
[1] Babak Akhgar, P Saskia Bayerl, & Fraser Sampson. (2018). Open Source Intelligence Investigation From Strategy to Implementation. Cham Springer International Publishing Springer.

[2] Doyle, E. (2020). The dark web. New York, Ny: Greenhaven Publishing.


INTERNET ARCHIVE
WaybackMachine
DONATE
Explore more than 446 billion web pages saved over time
alneda.com
Calendar · Collections · Changes · Summary · Site Map
2003
JAN
FEB
MAR
APR

Saved 383 times between January 29, 2002 and May 7, 2020.

Figure 12. Results of searching alneda.com website via Wayback machine



البيانات

■ عزاء من المجاهدين للأمة بأحد أبطال الجهاد خطاب

■ بيان من قاعدة الجهاد حول وصايا الأبطال ومشروعية عمليات واشنطن ونيويورك

■ تحذير حول أمن المعلومات

المقالات

■ إلى المتثاقلين عن الجهاد

■ شـــربات وســكـــر .. للشيخ أيمن الظواهري

■ لسيد قطب : الضمير الأمريكاني واللّعبة الأمريكية

■ تحت ظلال الرماح (

صعود أمريكا إلى الهاوية (3/4)

بسم الله الرحمن الرحيم مركز الدراسات والبحوث الإسلاميه عرضنا في الحلقه الماضيه أسباب ظهور العولمه الأمريكيه ، ومحاور خلاف حلفاء أمريكا معها مما جعلها مقيدة دون إكمال مسيرتها التوسعيه ، وزاد الأمر سوء بالنسبه لأمريكا ارتفاع إجمالي العجز في ميزانها التجارى في ذى القعدة من عام 1420هـ الموافق لمارس من ...التفاصيل

أخبار متفرقة ليوم 11/4/1423هـ 22/6/2002م

تصاعد الحرب الإلكترونية الخفية بين الاستخبارات الأميركية وتنظيم القاعدة تنظيم القاعدة ينجح في العودة للشبكة مجددا بعد ضرب الأميركيين لموقع النداء التابع لهم ويتوعد بعمليات جديدة ضد واشنطن. ميدل ايست اونلاين: لندن – أكد المتحدث بلسان تنظيم

أخبار يوم الأحد 12/4/1423هـ 23/6/2002م

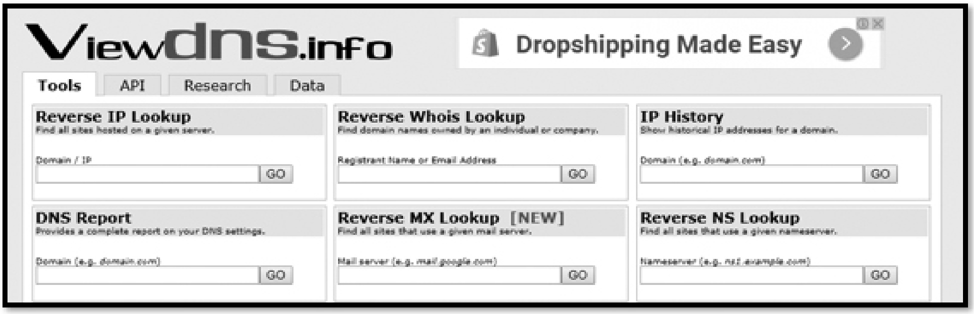
• أسقط المجاهدون مساء الأربعاء قبل الماضي 2/4 طائرة أمريكية من طراز (إم سي – 130) المتخصصة بالعمليات الليلية ، وذلك أثناء مشاركتها في مناورة إنزال ليليه تدريبيه تقوم بها القوات الأمريكيه والصليبيه جنوب غربي مدينه جرديز ، وقد كان المجاهدون في تلك الليله في أحد المواقع القريبه من مكان ...التفاصيل

الأخبارأخبار يوم الثلاثاء 23/3/1423هـ 4/6/2002م

مع اقتراب اجتماع مجلس اللويا جرغا فى نهاية هذا الشهر والذي يضم 1500 عضو من بينهم 63 امرأة في

Figure 13. Actual page copy from Wayback machine for alneda.com

According to the information needed, investigators can find many tools online to perform OSINT tasks. One of the valuable tools that can be used to investigate websites, IPs, emails, and many others is Viewdns.info as shown in Figure 14.



Reverse IP Lookup
Find all sites hosted on a given server.
Domain / IP

Reverse Whois Lookup
Find domain names owned by an individual or company.
Registrant Name or Email Address

IP History
Show historical IP addresses for a domain.
Domain (e.g. domain.com)

DNS Report
Provides a complete report on your DNS settings.
Domain (e.g. domain.com)

Reverse MX Lookup [NEW]
Find all sites that use a given mail server.
Mail server (e.g. mail.google.com)

Reverse NS Lookup
Find all sites that use a given nameserver.
Nameserver (e.g. ns1.example.com)

Figure 14. Viewdns.info tool

During the collection phase, investigators working on a terrorism case may find themselves limited when searching the surface web. Searching the deep web will be essential to find vital information about terrorist videos, materials and or traces. As mentioned earlier, the deep web can be searched using special web crawling techniques, advanced search engine queries, or searching specific sites such as the Wayback machine; however, dealing with the dark web is another challenge for investigators.

The term Dark Web is often confused with Deep Web. It should be clear that the terms are distinguished as there are three levels of the web [1]:

- Surface Web: Constitutes part of the web that is gathered and indexed by search engines such as Yahoo, Google, Bing or Yandex.
- Deep Web: Also known as the invisible web, it includes information that is not indexed by search engines. This information may not be hidden on purpose but may be available in protected, dynamic, and non-indexed databases or websites.
- Dark Web: Consists of several closed darknets providing restricted access to content which needs special software to connect to the peer-to-peer networks of this web. Dark web is part of the Deep Web and Tor network is one of the popular networks in the Dark Web as shown in Figure 15.

[1] Bartlett, J. (2016). The Dark Net. Random House Usa.

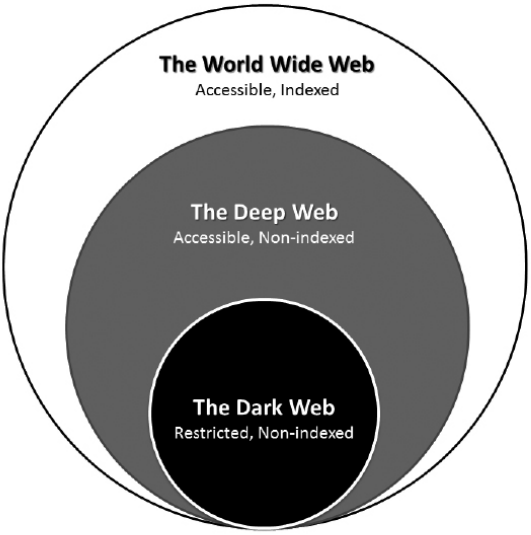


Figure 15. Surface vs Deep vs Dark Web

Unlike the surface and the deep web, the dark web offers anonymity and privacy options that make it harder for investigators to apprehend criminals who are using these networks. Therefore, law enforcement authorities (LEA) need to invest time and efforts investigating crimes committed on Dark Web. Tor and I2P networks are currently used by law enforcement authorities to search for illegal activities and criminals looking to hide their traces. However, the main challenges facing investigators in the dark web is to find the hidden nodes involved in illegal activities. Another challenge for investigators when dealing with dark web is there is no one search engines or database that includes all hidden services in the dark web; therefore, much effort and time are needed to identify the suspect using these technologies.

There are several OSINT tools that can be used to collect information for deep and dark webs. For example, a researcher proposed a tool called REAPER for automating the threat intelligence and OSINT processes. The primary objective was to find the distribution and source of where a credential dump first appeared in surface or dark web, while at the same time maintaining an in-depth study of the intelligence data that can be achieved by examining the criminal activities associated with it [1].

Another OSINT tool for collecting Dark Web data is TorBot [2], Which can be used to crawl and extract deep and dark web contents and provides visualization to represent the data in tree form.

There is a vast amount of relevant evidence available through OSINT; however, it can be challenging to obtain this information for digital forensic investigators who are only familiar with traditional digital forensics using evidence obtained from physical devices. It is always important to follow the preservation process in digital forensics framework to preserve the information that may be considered as evidence using video screen capturing when it is possible. Image screen shots are not reliable in many cases in court of law as it can be altered and modified easily.

4.2.3 Analysis

As in digital forensics, the analysis step is important in this OSINT methodology. Information and data gathered using OSINT techniques should be converted from machine data to a format that is understandable by humans.

When analysing information and evidence gathered using OSINT techniques, it is also important to check the accuracy and certainty of the evidence before using it in a case. Investigators need to make sure that the evidence is tamperproof and contains high level of assurance. Evidence needs also to be verified from multiple sources and not one source that could be admissible in court.

[1] Butler, B., Wardman, B., & Pratt, N. (2016). REAPER: an automated, scalable solution for mass credential harvesting and OSINT. 2016 APWG Symposium on Electronic Crime Research (ECrime). https://doi.org/10.1109/ecrime.2016.7487944

[2] Narayanan, P. S., Ani, R., & King, A. T. L. (2020). TorBot: Open Source Intelligence Tool for Dark Web. Lecture Notes in Networks and Systems, 187–195. https://doi.org/10.1007/978-981-15-0146-3_19

4.2.4 Visualization

Visualization is a very important step in OSINT techniques and can be used to link pieces of information together, reveal hidden links, draw timeline of events, and show valuable information to policymakers. Social networks, for example, contain a considerable amount of data and relationships. The number of people indirectly connected is an example of the type of valuable information a visualization tool can provide.

One of the valuable tools in visualizing OSINT data is Maltego. Maltego provides a mechanism for mining and gathering information using internet sources and provides useful tools for link analysis and visualization. Maltego includes search tools and transforms that enable investigators to search for people connections, social networks, companies, and various Internet infrastructures. It then graphically displays the search results. For example, if the evidence obtained during the processing and analysis stage can be used to determine an online alias, email address, or company name, this can be inserted into Maltego to perform a search. Figure 16 shows how Maltego gathers information about a terrorist website and draws graph of linked data easily.

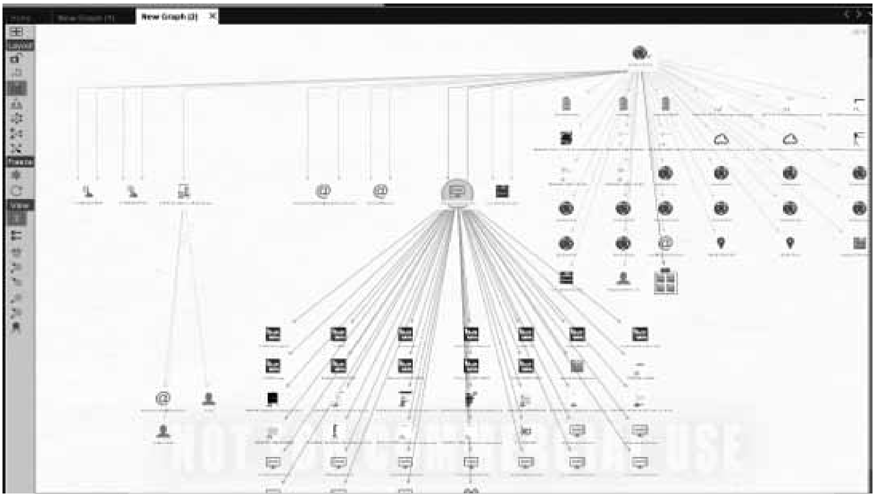


Figure 16. Maltego graph for terrorist website

There is different version of Maltego; the community edition which is free to be used by investigators with limited results and the paid version that can extract and gather more data from the internet than the community edition.

Maltego can also be used by investigators in analyzing and visualizing any other data that can be arranged in Excel sheets or CSV files such as CDR (Call-detail record). However, investigators need to be cautious when using Maltego in analysing and visualizing data in sensitive cases as Maltego connects the investigation machine to the internet and sends data to Maltego servers. There is another version of Maltego called CaseFile which is free and can be used only offline. This tool can be used to analyze and visualize data in cases that do not require gathering data from the internet. Investigators can try the other available tools according to many factors such as learning curve, budget, and nature of the case.

Another valuable tool in visualizing OSINT data, especially social network data is Ghephi. Gephi is an open-source network analysis and visualization software package written in Java on the NetBeans platform. It does not need access to the internet and therefore can be used safely in analyzing sensitive data. Investigating social network connections such as data extracted from Facebook and Twitter can be analyzed using Ghephi as shown in Figure 17.

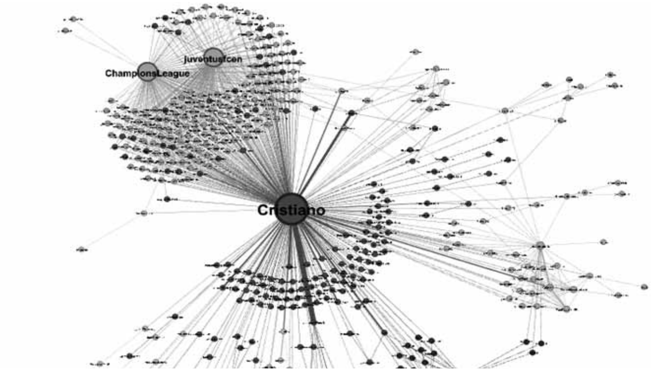


Figure 17. Analysing Twitter account connections using Ghephi

4.2.5 Collaboration

Collaboration is to work together in the investigation process. OSINT techniques require collaboration to solve complex cases. This step was conducted during the UNODC training using the Capture the Flag (CTF) methodology. Investigators need to separate the tasks among them to solve the case. Team leader for example was responsible for putting the plan, other team players were responsible for the information gathering phase, others were responsible for verification, analysis, and visualization of gathered information. Additional members of the team were responsible for double checking and documentation.

4.2.6 Documentation

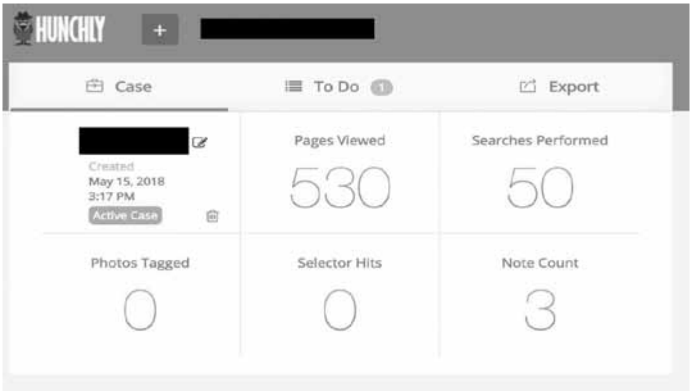
It is the responsibility of the investigator to document all actions and observations in the digital forensic research. All the documentation should be complete, accurate, factual, and comprehensive, resulting in a report being drawn up for the intended public. Writing reports is a vital skill although it is not easy for many investigators, especially when using OSINT techniques. Documentation is complementing all previous processes and should be followed with care to produce fine report that can be presented in a court of law. Integrity of evidence and the chain of custody should also be considered.

The researcher noticed the challenges that investigators were facing in documenting everything they are doing to solve the case. One of the most challenging steps is to maintain the integrity of evidence using hash values and making sure that every step is written clearly in addition to the actual evidence which is an overwhelming process.

Unfortunately, there are not many tools available to document the OSINT process and techniques and at the same time maintain the integrity of evidence and chain of custody. The standardization of this process for OSINT is also not present.

One of the valuable tools is Hunchly, which is intended for online investigations. The software is primarily designed for the use of law enforcement, academics, private investigators, cybersecurity experts and investigative journalists. Hunchly is a web capture tool which runs softly in the web browser and automatically records, documents, and annotates any website visited by investigators during the investigation. Investigators do not need to remember to take a screenshot, cut a URL and save documents while browsing with this tool.

The tool creates an audit trail of all the steps performed during investigations and automatically downloads and stores copies of reports, documents, and other materials locally. This greatly reduces the number of times investigator needs to stop and document the step. Hunchly also helps tag and categorize the content along the way [(1)].



[redacted]

[redacted]

Created
May 15, 2018
3:17 PM

Pages Viewed 530

Searches Performed 50

Photos Tagged 0

Selector Hits 0

Note Count 3

Figure 18. Hunchly case interface

Hunchly includes many valuable tools that assist the documentation process, to name but a few:

- Recording hash values for each evidence
- Export the data to CSV files

[(1)] Hunchly. (2017). Retrieved June 12, 2020, from Hunch.ly website: https://www.hunch.ly/

- Allow collaborations between more than one investigator
- Automatically produce final case report

4.2.7 Presentation

Presentation of evidence collected using OSINT techniques should follow the same process and standards in the digital forensics process presentation phase. Presentation in a court of law includes the final reports, charts, videos of evidence and should be presented by qualified expert witnesses. Presentations should not include technical jargon as judges and prosecutors will value more what they can see, touch, and understand. Visualization can also be used in the presentation step to simplify connections in complex cases such as organized crime rings and terrorism cases.

5. Conclusion and Future Work

5.1 Recommendation

The Internet explosion, the increase in the use of mobile devices, the growth of the user base of social network websites, and the need for Internet connections provide ample opportunities for cybercrime, making it essential for the traditional methodologies of digital forensic investigations to be updated to include evidence gathered through OSINT techniques.

Due to the volume of information publicly available on social media websites, using OSINT techniques will be valuable in investigating crimes committed online or any crime with evidence linked to cyberspace. This recommendation is supported also by researchers provided evidence on the importance of OSINT techniques in social media investigations[1].

[1] Taylor, M., Haggerty, J., Gresty, D., Almond, P., & Berry, T. (2014). Forensic investigation of social networking applications. Network Security, 2014(11), 9–16. https://doi.org/10.1016/s1353-4858(14)70112-6

OSINT tools and techniques were used successfully in solving many cases[1] either by law enforcement or investigative journalists around the world[2]. Therefore, it is recommended to standardize the process of OSINT methodology to provide admissible evidence in a court of law.

5.2 Future Research

The area of using OSINT techniques in cybercrime investigation, digital forensics and cybersecurity is very broad and needs much research. The Open source intelligence domain is expanding daily with more data available publicly online and therefore increasing the need to employ more advanced techniques to mine, collect and analyze this data by data scientists and using artificial intelligence algorithms. Law enforcement and other security departments continue to grapple with how to manage and fully exploit the current OSINT techniques known as second generation OSINT [3]. More research is needed concerning the future of the web and how information will be available in the new cyber-connected domains. The advancement of Web 3.0 (Semantic Web) will result in new technologies in publishing, exploiting, and analyzing of data. Machines and AI algorithms will play important role in the new generation of OSINT which considered the third generation of OSINT according to RAND corporation analysis [4]. Finally, international cooperation, public and private sector partnerships will be very important in shaping the new era of OSINT in near future which will be of value to law enforcement and intelligence community in fighting criminals and terrorists; however, more challenges will arise at the same time.

[1] bellingcat - the home of online investigations. (2021, January 29). Bellingcat. https://www.bellingcat.com/

[2] Cameroon atrocity: What happened after Africa Eye found who killed this woman. (2019, May 30). BBC News. https://www.bbc.com/news/av/world-africa-48432122

[3] Williams, H. J., Williams, H. J., Blum, I., & Blum, I. (2018). Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise: Retrieved June 13, 2020, from Rand.org website: https://www.rand.org/pubs/research_reports/RR1964.html

[4] Williams, H. J., Williams, H. J., Blum, I., & Blum, I. (2018). Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise: Retrieved June 13, 2020, from Rand.org website: https://www.rand.org/pubs/research_reports/RR1964.html