Evaluation and test of various tools for OSINT- based Snapchat Investigation

Length: 15,153 words

Due:

Abstract

The paper aims to investigate the Snapchat Application as the open-source Tool available to gather the information or data of the users. The Application provides a platform for the users to enjoy entertainment while posting their media, including pictures and videos. There are OSCINT tools available that are considered open-source have information for the users so that they can get access to the data of other users and can be used for different purposes. The paper will include the analysis of Snapchat tools to investigate whether the snap chat application is safe or secure for the users or not. In this regard, the paper will analyze the different tools such as a snap map and snap lion to hack the users' data. Hence, the paper showed that the Snapchat application is not authentic and secure for the users for both illegal and legal purposes. Therefore, it needs to have better management and the Application developers to ensure the safe use of the Application.

Table of Contents

Chapter 1: Introduction

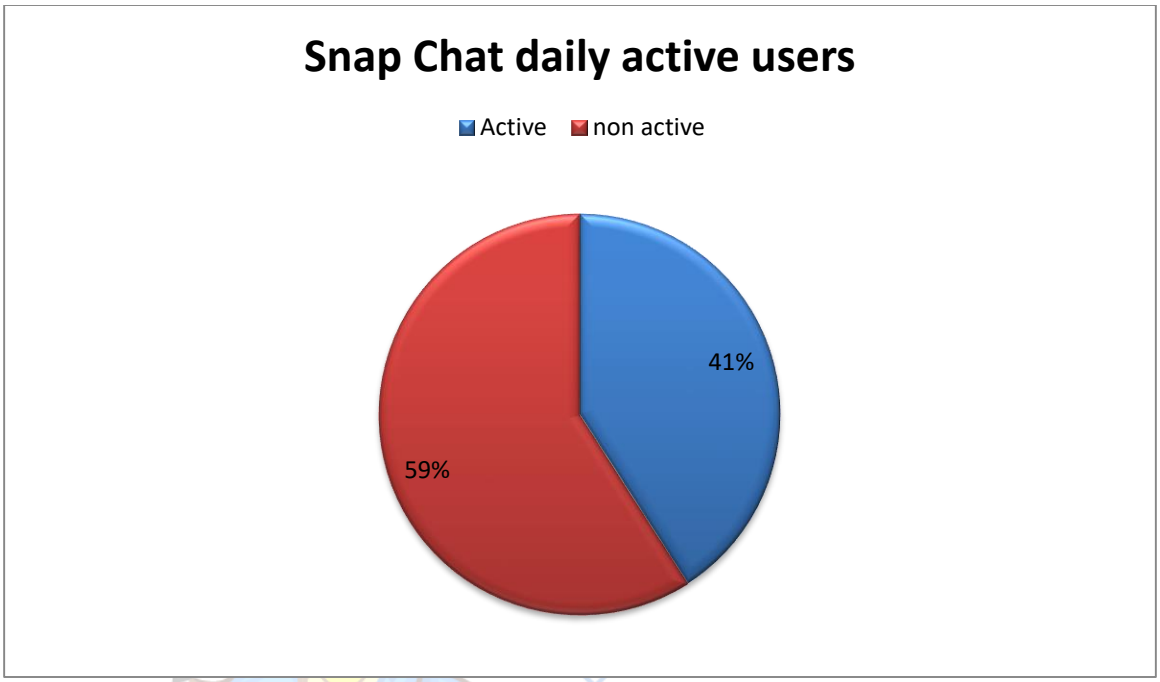
Background

Snapchat is a popular social media application to be proven to have little use as an OSINT resource (Evangelista et al., 2020). Open-source Intelligence is known as the practice of collecting information from publicly published or publicly available resources. The operations are practiced by IT Security Pros, state-sanctioned intelligence operatives, and malicious hackers use these Advanced Techniques. In the lies and search through the major haystack of visible data through social media to find access. They are looking to gain some purpose or achieve a goal.

However, OSINT tools are considered open sources. Rather, they are defined as the public nature of information being analyzed. Therefore, in many ways, it gives the mirror image of operational security OPSEC to be the security process for any organization or Department to protect public data for them or with some purpose. It is to analyze to understand and reveal the damage to the truth. Also, IT security departments are increasingly moving towards Performing OSINT operations and tools for the organizations to understand and ensure operational security.

OSINT History – Spycraft to Information Technology

During the 1980s, intelligent services and Military operations shifted some data and information gathering activities (Wiradarma and Sasmita, 2019). Through social media to try to gain the Advisory some mail, or understand the phones to discover the secrets related to different personalities. Therefore, efforts were put to look after useful information. It was freely and readily available on the officially published websites or other resources.



(Snapchat Demographic Stats: How Many People Use Snapchat in 2022?, 2022)

At that time, the world was changing. And with the use of social media, they had the scene that they could go for plenty of sources such as publicly available databases newspapers, which contained useful Information interesting Information. Specifically, someone is connected to the Internet or through social media. Consequently, the idea of OSINT was originally designed to refer to the spycraft kind.

Meanwhile, a similar technique is applied to cyber security. Therefore, most organizations have a public-facing infrastructure and vast infrastructure with Spain or many networks. There are technologies and hosting service is available. Therefore, information can be stored, the workers with the employee-owned BYOD devices. Also, there are cloud-based devices available like webcams and other hidden resources for having the code of active applications and programs available. There is staff in many companies that seldom know where to have the real asset in the organization, whether public or not. Companies also have control over several additional assets. Indirectly, such is the accounts over social media because there is a piece of potential information or data available that could be dangerous if it is in the wrong hands.

Problem statement

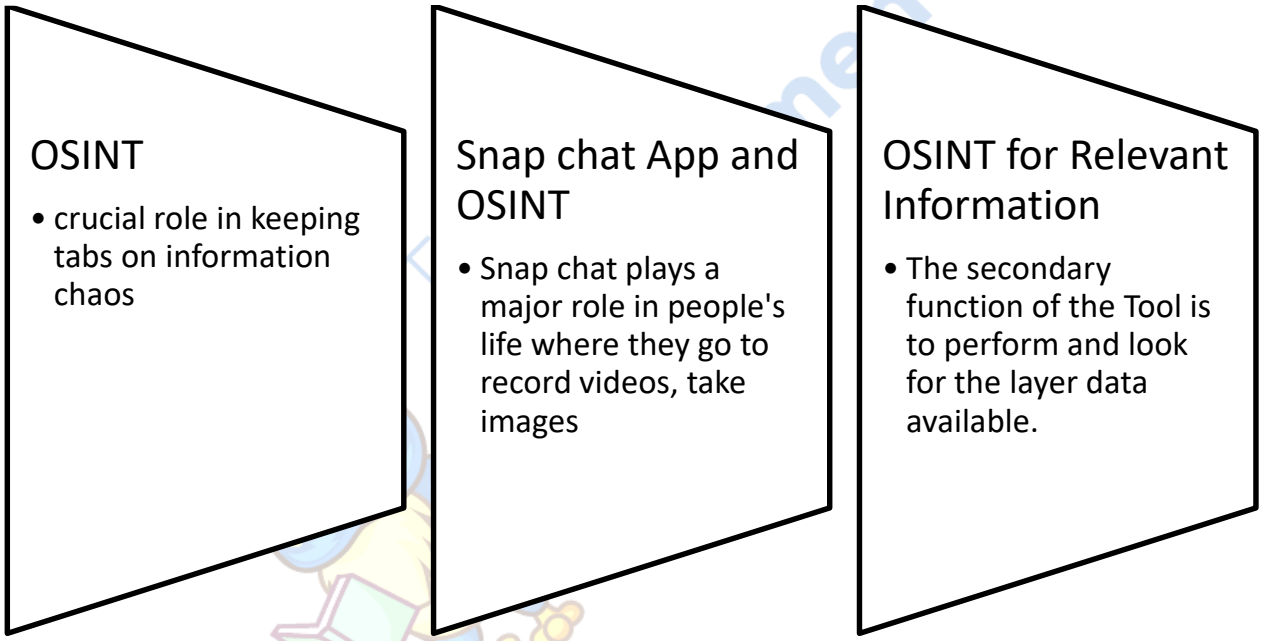
- How can Snapchat better guard against the risk of a hacker gaining access to its important information and that of its users?
- Which OSINT technologies and approaches can be used to gain access to Snapchat's most important data?
- Is the snap map a safe platform for users?

Objectives

- To investigate how Snapchat's open-source information might be utilized for nefarious reasons by hackers.
- To research and analyze OSINT-based tools for Snapchat investigation using a snap map and snaplion

Importance of OSINT for Applications and Websites

OSINT plays a crucial role in keeping tabs on information chaos. The Department needs to have three important tasks because many OSINT tools are developed to assist. Those needs are related to the organization. Most of the tools of OSINT serve all three functions, and they can be operated in Excel or other formats.



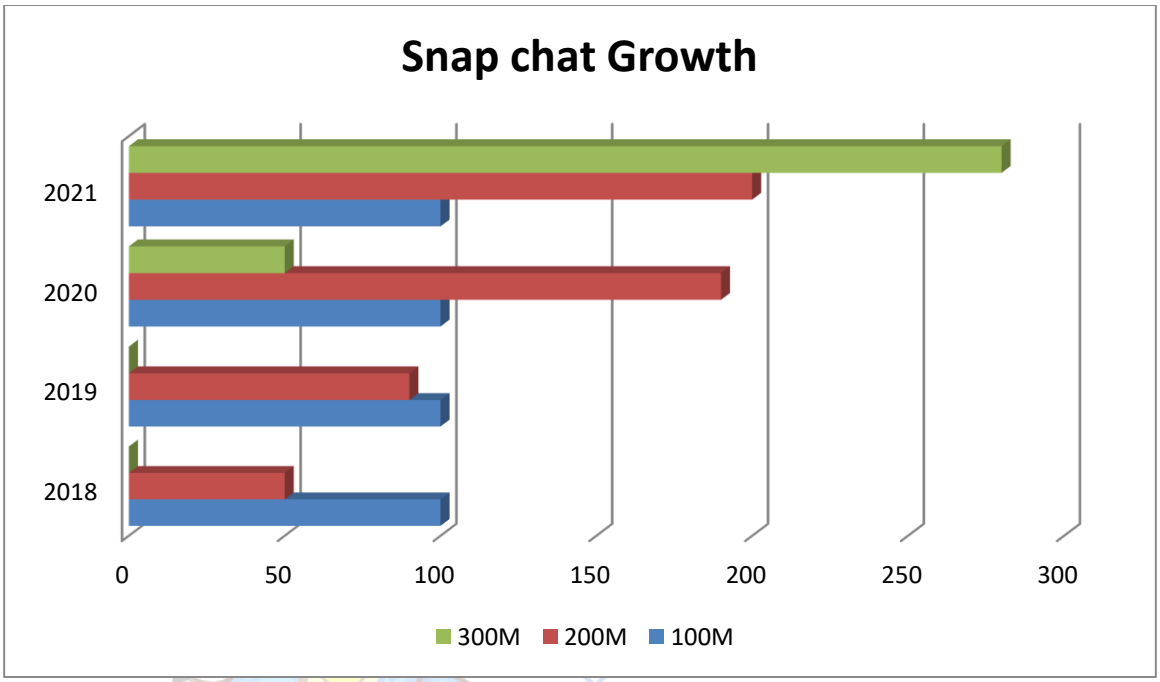
Snap chat application gained popularity just after its introduction among the users. It became an entertainment tool or purpose for people to enjoy file sharing their photos and videos over the social media platform. However, it is an abject provided to have the platform for entertainment, but it was not secure from the organization and the perspective of the organization. The developer of the application could not give authentic reliability and information to the users. So it was with the evidence that there was data availability, even after the deletion of the data of the snap chat users.

Similarly, Snapchat went to for the recognition of many of the employees or workers working behind the application, including developers, to get the data access of the other users and then use them for their purposes. So, the purpose of personal use can be legal and illegal there for both. The sides are riskier for the users who use the synaptic application to gain more popularity among the users if it moves towards the secure option for the users.

It is only possible if the developers have major access to the application. They allow users to go for the entertainment, which provides them with a secure platform, rather than having the riskier platform to share their most sensitive data, such as images and videos.

Public-Facing Assets

The most important function is helping Information Technology teams discover public-facing assets. And what information possesses on their social media accounts. There is a potential attack on the Services surface. Therefore, it is important to discover public Assets in general people. Rather, there is penetration testing on the platform. And the main job is to record the data. Someone could publicly find and use it for hiking or other wrong meals.



(Snapchat Demographic Stats: How Many People Use Snapchat in 2022?, 2022)

Snap chat App and OSINT

Snap chat plays a major role in people's life where they go to record videos, take images, and share those images publicly over social media or the Internet (Lemay, Doleck, and Bazelais, 2017). Similarly, snap chat also offers maps, and if someone is using Chrome, there is an option available on the right side to save the data in a very easy manner. It also gives information or a similar object where the information is not publicly available but private.

But, with the use of these tools, those data can be hacked by people because the Tool is available for people to gather information through different search engines. The major use of the Tool is to gather than formation for research purposes and other security reasons, but there are other people or users for the means of hacking or other wrongs.

OSINT for Relevant Information

The secondary function of the Tool is to perform and look for the layer data available. Companies, such as social media, locations, or other domains might define the network organization. Conclusion: there has been a lot of bringing information and technology logo assets of the organization, and they are merged with lots of acquisitions. And they have a function that is very useful for them, given the extreme development and popularity of social media. There is an analysis of the company's parameter for sensitive data, which is probably helpful for any group to use for their purposes.

Through the OSINT tool, the company can improve cyber security and help discover data or information regarding the company's workers. Any hacker or attacker can exploit information Technology assets and other confidential data. For some wrong means, the data can be used. Therefore, discovering data first and then hiding or removing it. It is the better step finishing, and denial of services attack can be reduced if the data is timely removed by the organization.

Common OSINT TOOLS

Following are the commonly found open source tools available to gather data or information about the users.

Maltego

Maltego is specialized in uncovering the relationship between a company's people domain and the information publicly accessible over social media or on the Internet. It is known for having some erroneous amount of information or data and plotting the data in very easy-to-read graphs and charts. The Tool ensures that the graphs have up to 10,000 points. Therefore maltego programs or Tool works by automating the searching of data resources publicly available by different users. Users or individuals can click on one button and execute their multiple queries, known as a program's transform action.

Mitaka

Mitaka is a Tool available over Chrome extension or Firefox Add-on. It has six Dozen search engines for different IP addresses, URLs, domains. Bitcoin wallet addresses, ASNs, and various indicators of compromise from browser or web browser available the extension saves. The actions are the shortcuts of various online databases with a click; for those who prefer a focused

alternative, extension more limited set sputnik. There is also the availability of this Tool to have the data analysis.

Spiderfoot

Spiderfoot is the Tool that is recognized to integrate various data resources and understand IP addresses, domains subdomains, email addresses, ASN surnames of phone numbers, and usernames. It also includes BTC addresses available on GitHub in consequence, spider photo. It comes in a command-line interface and an embedded webserver to have a web-based GUI. The Application itself has over 200 modules. So it is to make it ideal for red teaming reconsider activities. Is it to analyze more data about the Target or Identity or their organization and wish to have an expose on the Internet to have the data for your analysis or some purpose?

Spyse

Spyse is described there is complete Internet as its registry. It is the better gear for cyber security professionals or the organization. It relies on the project, such as intelligence and the spider mentioned above the foot, and the data available on the website o the associated server. They are owners and IoT. It's the Tool through which the spices engine examines the data to give any security risk to the different entities. There is a free plan available for the developers of the applications to build the Application using spice API and then go for the paid subscription and have the exes of the information required.

BuiltWith

Built with is the Tool for the popular websites that are built or develop the different tech stacks and other platforms are available with power, different websites, built with have the detection, whether the website is using Joomla, WordPress or Drupal for the further details of what the website built with? The generalist data include libraries or JavaScript such as JQuery or bootstraps website is using. Furthermore, Services provides a list of installed applications plugged in on the website. Also, the server information is to Framework the analytics and the data or information Tracking available.

Therefore built with is used to reconsiderIan's purpose, combined with the website. A security scanner such as WPScan and database API has common security vulnerabilities that can have a major impact on our website for those looking to mend. This Tool is suitable to provide a more

focused output that is concise and meaningful both analyzer and built with is used that suits better to analyze the data of the website.

Intelligence X

Intelligent X is known there is an archival service and search engine to have a historical version of web pages (Hollenbaugh, 2019). They're also entirely to data set available that is otherwise removed from the website due to some objections or legal reasoning. Although the Tool is giving sounds similar to information, it is a way back machine for security reasons, so it can be used whether the data is deleted or not.

Snapchat – Tools (OSINT)

The following are known as top tools used for OSINT, where they are specialized and different from one another. There is different Tool in need of the organization or the individual to use in different ways, specifically for a Snap chat to have the security of the data such as images, videos, or locations. Theron addition, there has been sharing publicly or

Tools	Link
addmeContacts	http://add-me-contacts.com/
AddMeSnaps	https://www.addmesnaps.com/
ChatToday	https://chattoday.com/
Dizkover	https://www.dizkover.com/
Gebruikersnamen: Snapchat	https://gebruikersnamen.nl/winkel/
GhostCodes	https://www.ghostcodes.com/
Listchats	https://www.listchats.com/
OSINT Combine: Snapchat MultiViewer	https://www.osintcombine.com/snapchat-multi-viewer
snapdex	https://ghostdex.app/

Snap Map	https://map.snapchat.com/
Snapchat-mapscraper	https://github.com/nemec/snapchat-map-scraper
Snapmap-dl	https://github.com/sdushantha/snapmap-dl
Snap Nickname	https://snapnickname.com/
Snap Political Ads Library	https://www.snap.com/en-GB/political-ads
SnapStory	https://github.com/sdushantha/SnapStory
Snapyfox	https://snapyfox.com/
Social Finder	https://socialfinder.app/

These are some popular tools used for the analysis and data information available for security reasons the organizations t Somehow, the information is also used by the wrong means, or the hackers where can use the information to hit the data or mislead the information. Similarly, Snapchat is an application with videos, images, and Maps or locations of people. These images, videos, and locations are publicly or privately available. It can be accessible by using the OSINT tool. Therefore, the Tool's availability is meaningful for the intelligence purpose, but it can be used incorrectly to gather data and use it for personal reasons.

There is a need to understand and analyze the risk associated with the use of OSINT. It reveals the privacy of the user of Snapchat. Nobody wishes to have such information from a third party. But the use of the OSINT tool is essential for accessing the resources available over the Internet. Even if the information is unable to get from Google or other search engines, the OSINT tool helps get better results for data availability.

Chapter 2: Literature review

OSINT and Snap Chat

On May 28, 2020, there was a hashtag trending"#minneapolisriots" on Twitter, on which is the social network side riot loads broke down across the hashtag (Trend Calendar, 2020). Saint Paul responded to the death of George if Lord also used social networks. It made the media directly onto the public side. It allowed others to watch events, have unbiased information, and filter broadcast media. Therefore, Snapchat is just one of the OSINT examples to happen (Tabatabaei and Wells,2016).

There is no doubt that snap chat is the Tool or the app that gives the options to keep security. It is to hide the data in terms of photos or location. But it cannot be said that snap chat is the most secure platform for people not to risk data leakage. Once there are open sources, there is available through the open sources OSINT to detect the data and use it for any purpose (Gong, Cho, and Lee, 2018). The publicly available Data would be better for users searching for free data availability. Also, the data is easy to access for any account relevant to searching for different means.

Consequences of OSINT (Open source intelligence)

OSCINT has been the platform as an open-source for the public to gather data. Ultimately it encourages the public to be part of the network where data or information is available. Snap chat is based on secure options for the users. However, there are many flaws as well in the Application. Open-source intelligence collects information from different sources or applications(Matthews, Lovell, and Sorell, 2021). These sources possess the value of having open-source data. It means there is an available source where the user has selected the information to be available publicly.

Consequently, the data is available through the sources such as Google or other applications. The search engine gives the platform to search for any open source information with no data encrypted. OSCINT is primarily effective for law enforcement, national security, and business intelligence. Similarly, the function is to go for the analysis and search of non-sensitive data. It is to answer the unclassified or proprietary intelligence requirements of the task or the organization.

Many individuals use the information. Thus, OSCINT possesses the media platform to be used for useful information. There is a media category where newspapers, radio, and television are sources to gather information or data. Internet is another category where data is available through different search engines. Similarly, public government data is also available for intelligence use. There are government publications and other sources. Through the Internet, there are search engines, and also, there are man applications such as Twitter, Facebook, and snap chat(Gong, Cho, and Lee, 2018).

Snap Chat Privacy Settings

Soon after the application is used, the encryption on both photos and videos and the platform and application is considered the more secure and safe period form for the users (Andrén and Heurlin, 2020). However, the messages of the snap chat application or not encrypted. It does not mean that the whole information of the user is available over the snap chat application. But, somewhere, it reveals that this application is giving a clue that the information with regard to the messages of the users aris

It does not disclose the people's sensitive information while sharing their photos and capturing videos. But on the other side, there is no such type of end corruption present or available for the messages or the text. They share. It is also difficult to truly identify what happened. So to the messages over Snapchat. Once the server of the Snapchat is on, there is an option for the users to get the excess of those messages ((Reed, 2022).

It shows how insecure the snap chat platform or application is to work on. Similarly, snap chat is working for entertainment purposes, but it does not show any concern for the users' privacy. On the contrary, it is revealed in the privacy settings for not having such authority over encrypted messages or information of the users, so they feel confident enough using the application.

There is privacy available over Snapchat; the settings tune does not allow or let people find out the mobile number as we're there for the settings option, whether to go for this Snapchat account (Lao, Mao, and Sy, 2018). Using the mobile number or not for the users who don't want to share their mobile numbers have the Privacy option in the application to go for the hide information of a mobile showing their numbers. Similarly, if people are concerned about privacy, they can turn

off this option or feature, and they can use their option for those people or share their number with those they want to share.

There is a purpose of the settings in Snapchat, the developer kept in mind, to give the security and privacy settings. So the users can avoid the unknown flood of people and then have a better experience of using the application. In the meantime, it is also the option of two Factor authentication present over Snapchat (Villaespesa and Wowkowych, 2020). Similarly, two-factor authentication requires to have the additional updated information or data regarding the user. So to go for the excess of this option, besides the password. It means that once a new device has the excess of the account, it will receive a code via text. So it is done with a mobile phone. Then after the verification in the account, it can be logged to access the data or share the media such as pictures and videos, adding this additional step of getting the authentication done or through the snap chat.

It is more difficult for people, as well, to access their accounts because their passwords can be cracked by other people as well (Perea El Khalifa, 2021). And if they get the excess for the mobile Phone in any circumstances such as at home or with other family members, they can go for the excess of the account. Therefore, it cannot be said that the use of the Snapchat application is so secure for the users to use it with the major purpose of having the most secure and private form of entertainment purpose.

It is not a secure platform for sharing sensitive data such as images or videos, also due to the non-encrypted services. It is also not secure and safe to have the messages over Snapchat. The messages can also be shared with other people if they know how to access the OSCINT open source platforms available.

Snap Chat - Hackers Access

Snap chat gives images of the person using social media or snap chat. And the information is available through the open-source intelligence agencies also go for the open resource intelligence to track equipment events such as people and weapons systems. There are targets of Interest, but hackers work against the Nation's Pride (Velten and Arif, 2016). Therefore those hackers use open source intelligence to identify technical data of the humans and go for social engineering

attacks. The security team is deployed to go for the Strategies and techniques to find the backing weaknesses in the system.

And, therefore intelligent people engineers are hired and information technology systems. Those officers who work there night to close the weaknesses to understand whether the weaknesses are a lie and where there is a need to work on those images of the country or the nation as a whole. For any country, it is of great importance to have the security of information of the client. Once there is no such security, the data can be accessed through the open-source (Pastor-Galindo et al., 2020). It can have a major influence on people's minds because they will be afraid of getting hacked for their open data source. Intelligence helps the security teams on the greater level being compromised and the issues in the system event.

Issues are once highlighted in the system, then they can pick the issues data easily, and they can go for the security of the data. But, their applications, such as Snap chat availability, give access to the people who were specifically hackers to access the data (Piwek and Joinson, 2016). And use it for the wrong means can harm people's minds can disturb them. Also, it can have a major impact on the goodwill and reputation of the company's management. Because once the company has weaker information technology, without a doubt, then it will lose most of its shareholders or clients.

They will not trust the security system of the company. So, it is essential to go for Snapchat to have precious information. But, on the other side, it has been the priority of the cyber security teams to work on the fair use of information.

Workers of Snapchat – SnapLion Tool for hacking

Snapchat Application went into popularity, and it gained major information about the users were relying on it for entertainment purposes Snapchat. Snapchat is the platform for users who share their media in terms of images and videos, and they move on towards a better experience. Also, it includes the location of the media, including images and videos. Similarly, there are employees involved in managing the data of the users. Therefore, the information and data are available to give them better Services.

It was analyzed and highlighted in 2014 that users of Snapchat are complaining about the attack on their data or bullying by the users who have the information of the credentials of the users of

the Snapchat application(Reed, 2022). At the time, the company did not talk about any of the actions because it was not highlighted that company employees were involved. It was done in 2016 and 2017, where employees were highlighted(Reed, 2022). Legal action was taken against the employees. They go for the tools was used by the workers who had the authorized access to the data, Snap Lion, and get the information such as phone number, location, and media of the users. It was done by doing the wrong justifications and using the data.

The workers used the data to attack the accounts. It was to read the users' messages and then bully them based on their chatting or the images/videos they shared. They were having with other people. It was also done based on the media, including images and video. They were sharing with their friends and other members, and the employees were then using those media information, pictures, or videos(Villaespesa and Wowkowych, 2020). It was to give access to the third party as well. Use them to attack the users. Also, the workers had the credentials or login information to get access and then bullied them whenever they needed it.

Security Level of Snap Chat

However, there is a security level for the snap chat users. But it is not encrypted for the images of the users. Users do not go for the authenticity of the security. Data or information is available through the commercial category for the people or the agencies (Velten and Arif, 2016). They can use data for their purpose and can even misuse the data. Once the data is misused, it can be hectic for the users to trust the Application or the platform. Companies are working hard to secure the data of the users. It is to build their trust. But some people misuse it, and for this reason, IT departments are working hard to keep data secure.

The snap messages are encrypted for the snap chat where no one can see the text. But referencing the pictures or images, then the data is not secured. It possesses flaws in the system. Even the users go for hidden or private data, not publicly making it available. But on the other hand, the data is available through many search options. The data can be gathered from different applications for misuse purposes.

In June 2017, The Social Network site SNS or Application, Snapchat, went for an updated mobile Application to introduce new features and allow users to upload curated media to the public availability of Snap live Map (García, 2021). Some users might analyze and see that other

users have the Live Map, and they can tap on the heat map overlay to understand where the images are. And videos uploaded in support of the activities or operations. Unfortunately, the Media was too quick to organize or recognize the power of the Application within the two months, and hurricane Harvey Struck the American state of Texas and Louisiana.

Similarly, image is uploaded to Snapchat, and those images are distributed via Twitter. For example, President Trump misrepresented the crowds during his campaign stop. Thus, media was uploaded. The image is to snap. The map showed a group of people mainly made up of protesters. Six months later, Snapchat has made similar features available via the direct URL of maps snapchat.map.com(Tabatabaei and Wells,2016). Snapchat did it because Snapchat is not only the social network site to go for the disclosure of the data or information of the people. But in 2015, Russian military soldiers were located in Syria from geolocation tagged photos posted to Social Network sites (Matthews, Lovell, and Sorell, 2021). It includes Twitter and Instagram as well.

So, disclosure was contradicted, and there was a political narrative because the data disclosure was there to the public regarding the political parties. There are applications such as Tinder and Grinder. And Tinder was also used to go for the geolocation of the individual. So, I used a net triangulation, and at the end of 2013, an attempt was made to resolve the issue because Tinder was downgraded (Courrier, 2021). It was to maximize the efficiency and accuracy of location features to move for the increment of 1 mile, rather than having the 100 foot to give with information of IT data. The prominence of a social network site is used to reveal important information following the helper of social media. Networking sites distributed surveillance systems for intelligence and law enforcement.

The definition of a social network site is given in the different works to understand that web-based services permit individuals to construct the availability of public or semi-public profiles within a system or the boundary (Kalpakiset al., 2016). However, it cannot accumulate the list of the users who can share the connection and transfer the connections or make the information available within the system. In this manner, it was focused on differences in the definition of social media. That has a great focus on user-generated content and also Web 2.0 Technologies. Specifically, the information generated from The Social Network site to understand both social network sites and social media more largely.

It is to note that Snapchat is consistent, and it is defining a social network site to give the ability to navigate different connections (Hayden, 2019). Mining digital evidence is not new for the Social Network side. Therefore there is a case study of proprietary. It has forensic artifacts and goes for the major test cases, limiting access to social network sites, URLs, local internet sessions, etc. Web browser cache has the direction of the social network sites with Facebook and other websites and applications such as Twitter, LinkedIn, Instagram, or Snapchat (Gibson, 2016). These give the knowledge that there has been—no technical assessment for Snapchat, which is a tool for service.

Snapchat is evaluated to share pictures and images to The Social Network site (Wells, and Gibson, 2017). The result is understandable in many research and studies and the synapse. It is a viable method to diagnose instead of using the traditional classroom-mounted lightbox. Therefore, the explosion of level can be used on Social Network sites, and it can be seen in the previous work of the studies that the method to track net to a maritime is also identified through the Map of the Snapchat. Therefore, it can be scraped extracted, the user-generated location or data; can also be excluded from the study.

It can exercise because the general public should not access such data (MÂNDRAȘ, 2017). Once the general public access such sensitive data, it can be dangerous for any country to show it and analyze it for misuse. For example, there is data available Over the Social Network site, such as a snap search to go for it. The president of the political leader or an actor or celebrity is going to the conference or other meetings. But, before security reasons, there was no such availability of the exact location of these personalities (García, 2021).

How OSINT affects Access to Sensitive Information

And also they are other issues that are related to the defense of the country. Once those issues are addressed, the country's defense cannot give the exact location or how it is. They are going to cope with those issues. But, of course, no one would share these strategic planning on the border or inside the country to understand how these strategies are being made (Perea El Khalifa,2021). And they are fighting and coping with those. Issues, once they are fighting with those issues. Then, the people can understand that the military is adopting these strategies is or other people there. For social network sites, there are open resources, and once open resources are there. They

can go for the exercise of the information of the different personalities of the people or even though organization their wish to have.

But it is not safe and secure for the country's internal matters to share such data, which is more sensitive (Chitkaraet al., 2020). And to make people understand the activities and what they will do in the strategies here to fight with the other people of the country. There are enemies related to the celebrities, or people are there, it can be any misfortunate or unwanted situation arise to cope with such situations? It is important to go for the analysis of many of the resources. Openly available source over the Social Network sites, such as Snapchat, keeping in consideration (Mercado, 2009) there has been studies that show that the data is not available for public use. The public is using the information or the data for personal use.

But on the other side, it is important to understand that sensitive data is not available. There might be many studies on the military as well. There can be research on military equipment (Williams and Blum, 2014). But once the research is done, people can find the general data over the Internet or on open Sources. But on the other side, people or the general public cannot find the sensitive Data because they delete or edit the database to own the necessity to be secured. And not to be shared with the general public to go for better research and methodologies, rather than sharing publicly and getting negatively affected by all enemies.

Sharma and De Choudhury (2015) analyzed the study on Instagram to demonstrate the data available for the images or pictures for the public. Of course, the information would not be extracted in terms of hidden or private. Rather the information was extracted that was general and available for the public. Fried et al. (2014) successfully went for the information collection from Twitter for geographical location and public learning. It probably demonstrates and states that such information is available through OSINT open-source (Benes,2013). But, on the other side, there is information that is not available to the general public. However, many researchers have gone for the data collection, but it is about the available information.

OSINT – Publicly Available Platforms

Open source is intelligence from publicly available material or information (Hribar, Podbregar, and Ivanuša, 2014). Most intelligence experts go for the definition of OSINT because it is for public consumption. It is the information that is accessible without the specialist tool or app.

However, it included sources only available to the subscribed people, such as journals or newspapers. The content is available for authorized people and subscribers to have the information.

They include the information gathered for the mass media internet specialist journals for Photos, research, and geospatial information or sources used in the investigation for any case studies. Therefore, it is not only to get the jungle information regarding celebrities or other people or other techniques used to use the useful information through open-source intelligence (Pastor-Galindo et al., 2020).

Useful Information Access Sources

The government can go for the important newspaper information or have a major impact on its performance. People have open sources that are highly effective for their information or knowledge. They gained information about the fashion of forgetting the major information. After World War two forces were implemented (Hulnick, 2010), it was analyzed that there should be information available for the public to get information and have knowledge about the world or the country. It will be beneficial for the general public to have open sources to get the information for general knowledge. Ready, Snapchat is known as a popular platform, and it is challenging to use Snapchat for investigation purposes (Benes, 2013).

Specifically, when one needs a mobile phone to go for a little deeper information, the website, Snapchat, offers to go for a website for extensive information through OSINT. Snapchat can be used with Open Source intelligence, which can be beneficial. The website of Snapchat is available mostly for mobile either, which can gain information. Also, in the Snapchat, Live Map. It is important to go for the exact date or the time. It was uploaded, for example, on Snapchat, go for the date and time, the content of the pictures uploaded by the user (Gong, Cho, and Lee, 2018). It gives deep information regarding the users of the uploaded content. Similarly is an app chat live map. It goes for a better display of these in-app J2 codes as well.

The code is a QR code, which can be scared through the mobile phone application, and it can direct to the Profile, which has contained outside Snapchat, and these contained might be the paid content order. They contain the advertisement for the use of the account. With the open-source website, Snapchat codes are available, which can instantly be used to visit the website

(Shipp and Fried, 2014). and outside Snapchat as well. So it is to expose and get the available information.

Snapchat Application gives a major experience to users through smartphones or mobile phones. It is ready to use for investigation purposes. There are resources available, but few resources have the best option for the research or investigation. However, the software can use the information. These are the Android or tablet-supported programs or software. So they can be used if there is any issue running. Snapchat on Android, and then this can go for a better experience. Better. Once the software is uninstalled, it can work efficiently, a better way to use Snapchat. It gives the option to go for and have the better space. If one has the space in a mobile phone or disc, it can go for Snapchat through the software (Poltash, 2012).

However, it is also essential to understand that searching for e numbers is easy to get information through a Snapchat acc. It is to go for this simple. In addition, the number from the phone contacts, either available on the smartphone or emulator, then sink the accounts with Snapchat. If it matches, then the user name will appear on the screen. The person on the phone is using Snapchat and is not added, and the user of Snapchat wants to analyze and search for the friends available on Snapchat. Then the phone number option can help them sink all the accounts and go for the open-source information available to search for friends or the circle in the phone directory. And then understand that which person is available on Snapchat from all the contacts.

There is a need to also realize open-source intelligence available for Snapchat. But on the other side, it is essential to keep in mind that if one searches for the other person's number or Profile, the person will be suggested to the friends. The name would be up here because the person has been searching through the phone number from the open-source Indulgence availability on Snapchat or the software using Open Source. It is also important to understand that usernames are also available on the mobile Application simply by inputting the user name in the search bar. Once there is a user name in the search bar. Then if there are any Profiles with that username, they will give definite results. The results will be obvious, and they can give the Profile of the search to username or person.

Open-source intelligence gives the platform to search and analyze the available information (Pastor-Galindo et al., 2020). But on the other side, there is little probability that the person who

is added to the list of the user can have the information that the person is searching for and having such activities through the search engine. However, it will not be shown in detail step-by-step, but they can go for the magnifying glass icon. Therefore, open-source intelligence can get the open data or information available for friends or other people or wherever needed. But on the other side, it is essential to realize that the information is available. But, it will also give us the information of the person searching the app's data.

Open source has great importance and the lives of people and other organizations. This is because open-source intelligence gives the available information, and therefore there are many applications available where there is information, such as LinkedIn, Facebook, Twitter, and Snapchat (Utz, Muscanell, and Khalid, 2015). However, there is information available that has been allowed by the user, the person who has a profile over the Internet. Therefore, those who write the articles or content pieces allowed the content available on the different search engines such as Google to get the result. And read the articles on the information available information.

It is good for the people moving towards the study purpose when it is not always about having information regarding the celebrities or other people. Organizations search for information, for example, people who use Snapchat (Gong, Cho, and Lee, 2018). And one of the people can use Snapchat and move towards the job interview. Then, the management can go search of the person over social media with the help of open-source intelligence wants the data gathered for the candidate. It will be easier to go for the maximum potential data and then get the data according to the needs and demands of the personality and the person's behavior through the post. Once the person is suitable for the job, then he or she can be hired on an easy basis.

Chapter 3: Methodology

The methodology will be based on the qualitative approach. Hence, secondary data is to be taken as tools for Snapchat. Similarly, there will be data collection from the different articles. There are peer-reviewed articles to analyze those articles for the tools that have been used to determine the results. In this regard, the research design will be based on identifying the Framework to go for the different tools used to analyze the data regarding Snapchat. There is a need to understand that the methodology will focus on the users' privacy using the platform while uploading the other information; the tools are used together.

Analysis of Snapchat tools

The information is available is open source for different users or readers. Also, this information or even the data can be utilized for some wrong means that can be harmful. Therefore, there are different tools available for Snapchat based on those tools. The research design will be analyzed to understand how these tools are formulated for the open-source information available for the users who can use the information for both positive and negative purposes (Schwarz and Creutzburg, 2021). Similarly, peer-reviewed articles were published on tools for Snapchat or open-source availability.

- They will determine how the different researchers have gone through the different methodologies to analyze the different tools.
- It is to ensure that the results give the authenticity to go for the analysis of the security of the users' information over the social media who are using the platform such as Snapchat for entertainment purposes.

The comparison compares the articles for the various OSCINT Snapchat tools present in the Snapchat data to determine whether these tools are important to implement. And they get the result desired result that the users want to have while maintaining their account over Snapchat.

Plan Execution

There will be a plan execution, where the Snapchat accounts will be analyzed through the different tags. There will be keywords that should be used to understand tools that can be utilized for any person who will search for the information available over Snapchat. Also, it will be utilized in a manner that can give huge information to the users while having different tools, such

as the Snapchat map. Or other search engines where they can get the data such as information or photos of the users or the people available over the platform of Snapchat.

The research technique will be there for different types. And the research technique will be used to combine the content analysis of the different peer-reviewed articles to understand how the researchers have found the Snapchat tools to be used together with the information or the users' data. Similarly, there is a security option available for the people because it is the open-source information available to search, and they can save the data wherever it is available. Meanwhile, the research will be based on using the theory to develop the concept.

Grounded Theory and Peer-Reviewed Articles

The theory will be based on the Grounded Theory approach to go for the different OSINT or open-source tools and techniques for the synapse chat to analyze them and then get the further results that are essential to understand how the research is going to get the results for understanding the tools that are essential for the search.

- The research determines the effective tools available for the users compared to their data to be secured.
- It is to analyze the data of the users. It's secure enough to be available over the Snapchat application, or their data is riskier on Snapchat. It can be accessed through an open-source tool or technique used by any user or person.

Once the tools are identified, it will be easier to understand which tools are the. For example, the most frequently used is open source by the user of the people available over the social media to gather the information from the Snapchat appellate Forum. Similarly, it will be analyzed through the content analysis of the peer-reviewed articles and the tools information available to the standard that people are getting the information from the synaptic yet. Similarly, whether the users' information is secure enough due to the availability of the open-source or the tools and techniques the people are using together with the information will be analyzed. And likewise, after this analysis, the research will use the technique to compare the tools.

And the frequent use of the users of the different tools is to again evaluate how the users are using the different tools and the tools that are frequently used compared to the other tools. But, in the meantime, there will be an analysis of the peer-reviewed articles. And, also the comparison

of the articles will be there to understand the point of the researcher where the researcher reviews different methodologies. And get the results to understand how the researchers perceive the snap chat to be the most secure platform. Or to be the open-source platform that can be accessed by anyone who can get the information or who wishes to have the data or the information of any person who has the account.

Ground theory analysis or approach will evaluate the real-time information available (Courrier, 2021). It is regarding the Snapchat tools to gather the information or data from the Application or the platform. Similarly, the ground theory review is based on evaluating the real-time data, which will be available through the peer-review. The articles are to analyze the data and then compare them based on their analysis and methodologies used by the researchers. It will give the imager sign to the research to go for the better quality.

There will be authenticity and reliability of the research because there will be an analysis of the tools and techniques for the OSINT. But on the other side, there will be an analysis and comparison of the peer-reviewed articles. Different researchers have gone through the different results for the use of the open-source tools and techniques together with the information to understand whether they are secure for the users.

SnapLion Tool

Snap chat application got its success and popularity among the users for sharing their media such as images or videos online platform, or with people or friends. There are options available to go for the privacy of the data or deletion of the data within the specified period. The application users went for the installation of Snapchat and used it for entertainment purposes. TheApplication was popular, but it was highlighted that the Snapchat application had a major problem with using the Application for users (Zuleanand Şercan, 2018). The major problem was included for the staff members of the Snap chat workers who were involved in the regulation of the accounts to see whether the users were getting a better experience.

The workers of Snapchat had authorized access to the accounts, a login, or credentials of the users of Snap chat applications (McKenzie, Keßler, and Andris, 2019).unfortunately, with the use of credentials

The workers of the Snap chat application are started fishing attacks and scamming the accounts. It was 2014 year when the Application faced a major concern for the security of the people. The users did not have the security or privacy for their email addresses, phone numbers, locations, and other personal information(Reed, 2022). The workers were unjustified in attending to the credentials of the users. They were getting the login information of the users of the Snapchat application, and they were using the login information to get excess personal data or information to use for the unjustified purpose. It was done in 2014 and continued till 2017. It was the year 2019 when they came.

Company management took a series of steps to analyze the workers and understand the workers are there to use the data. But, unfortunately, they are wrong means, and they are not giving better services to the people or others. They are bullying people, taking their data, and getting the information for the wrong means and purposes.

Over time, it became possible for the company's CEO to understand that workers were not doing their job properly. However, not all the workers were involved in this act of phishing and scamming of the personal accounts of the people of users of the snap chat. But some users were using the users' information, and we're not getting the proper data for the services. They were taking on the users based on their messages or the images they were taking. The workers were mostly the new or appointed workers of the company who were getting personal information.

Workers started reading messages, email addresses, and the users' media. They were getting the media and using it to bully the users and attack their data. The application users felt the account logged in without their permission, and it became the hacking by Snapchat own employees. And it was done for some purposes. However, the company still does not know how many of the accounts were hacked by the workers and where the data was used after getting the useful information of the users. But it became a legal matter for the company to get its reputation back and then take legal action against those.

Employees were using the people's data illegally. They were using it for some purpose, to share the data with other parties, or they were themselves harassing and attacking the users. The workers used the snapLion Tool to get access to the data. However, they were authorized for the services and not to access the users' accounts to damage the reputation and trust of the users.

Analysis

The study takes the web-hosted version of snap chat map. The web version of Snapchat Map is taken to observe. The Media was delivered to respond to a proprietary API using POST Query. So, there is a development model of the browser, which is enabled to answer the POSTquery and accompany the JSON object. The object in the snap map has metadata for the returned snaps. Therefore the method is focused on the web version to use applications and capture the media. The snap map makes it possible to get all objects and then record the objects while accompanying metadata.

It does not prevent the data from spoiling the metadata and moving towards API files. Also, it does not permit a copy of the metadata for the additional text format. It stops the spoilage of metadata. And again, the public Media is only recorded to maintain these enabled expectations of privacy of the user. The process includes the following steps to understand the Tool to be used to analyze the privacy of Snapchat.

With developer mode with a safari, it navigates Maps.Snapchat.com and then browses. The map is of Interest; while referencing the heat map and gate, the media uploaded, the heat Mabel is taken. And thus, it is discussed below.

While there is click on the location to go for it, the circle of radius, and then upload the maximum of 80 snaps present on the map. The radius depends on the level of map Zoom. Therefore while clicking through the plate list, there are images or videos. That is located to identify is being interested. The URL is present at the top of the browser window that is changed. If on New Media, when the New Media is loaded, the URL contains the metadata, which has the value id/snapsId.The ID is noted, and the remainder is in the present URL. URL denotes the location, which is the request that has been made. It is not the site from the Media that is uploaded. Rather. It is the ID used to give it the value or location.

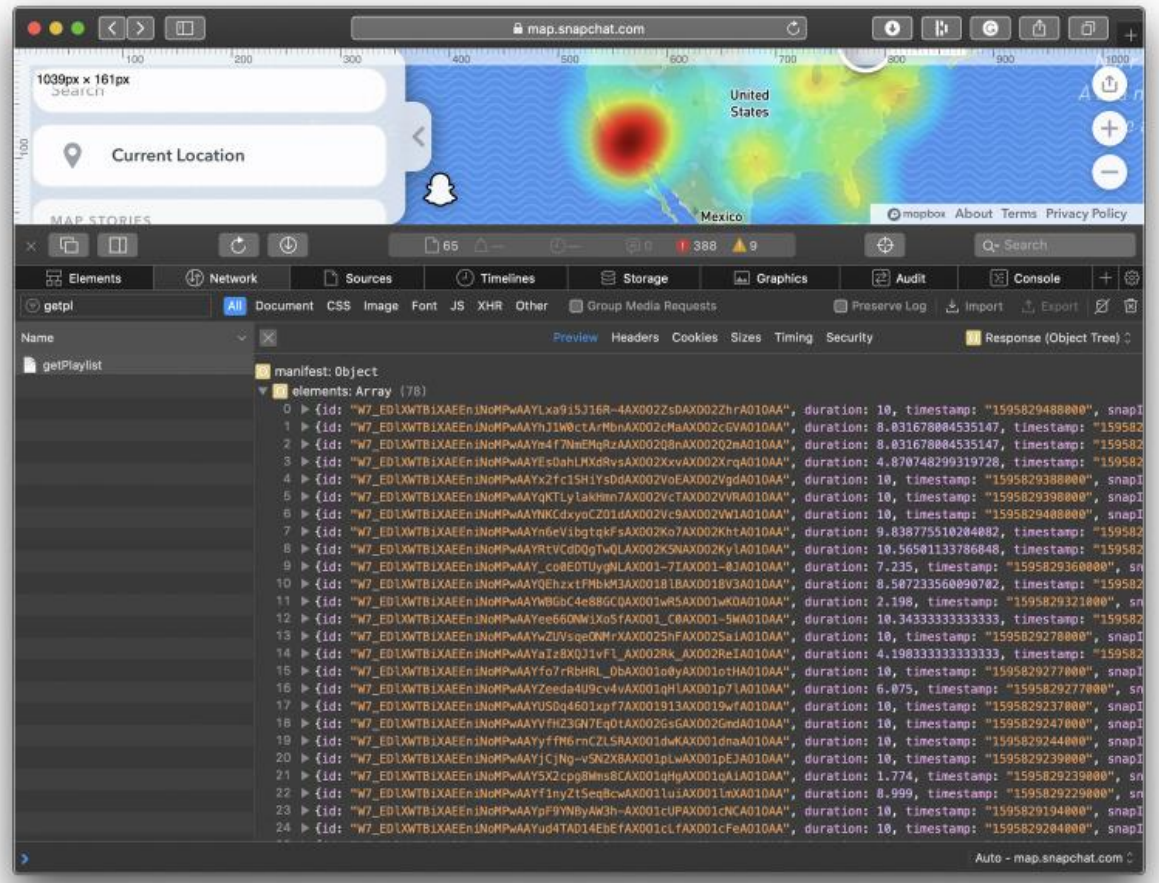


Figure. 1. Using Safari developer mode, The JSON objects are represented as an object tree

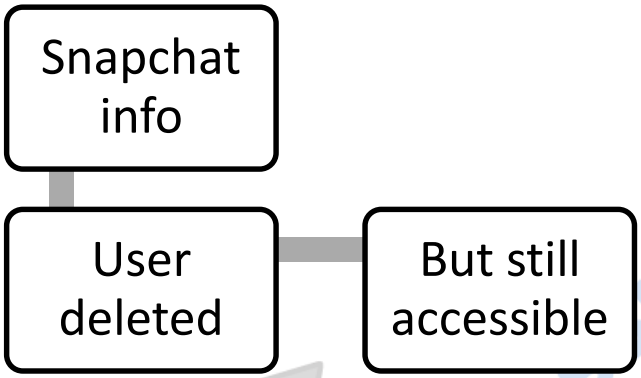
With the developer mood, a Network option is available to display the web request while using gate playlist JavaScript. It is a JSON in objects relevant to the media images or video loaded in the browser using the map. The JSON objects are known to find the server present on the browser within the objects of Json; there is a value stored, and it has the link to the server copy of picture images or videos. The Media is saved from the server, and it is present on the local server stored for the further use of the users or to download. The media can be accessed directly from the server because it is saved locally and created copy.

The javascript does not have any preserved ones of metadata. A copy of a JSON response to having the JavaScript get playlist method to keep the accompanying metadata saved. Likewise, there is a process through which automate. There is a developed script present for the exploitation. It relies on the private APIs indicated above while using post method calls. It is

easy to extract media through the scripted. So it is simply required a POST method call to provide a set of coordinates based on longitude, latitude and download a radius. If it is essential to go for the method and then understand where the media of Snapchat is locally present, download it.

It is present in this scenario, which shows that these adapted data can be downloaded, and the map gives the location where the user's data is available on the local network. A local network allows permission to download the media, whether it is an image or video of the user. It shows that the browser seeks permits to go for the download of the media, which is the security question on the use of the sin objective, where the availability of the URL is the major.

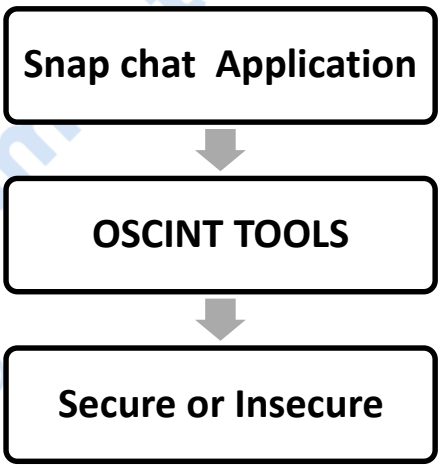
The major key resource for the people or the user is to get the data. Also, there is Media availability on Google or documentation because once there is a signed URL provides permission. However, it takes time to go for the request, and it also has an expiry time when the Media is no longer available.



But it gives the accessibility of the JPEG images and his from the server and gets the data, which is in user for the users. There are ghost protocols available for Snapchat (Chitkara, et al., 2020). The Tool is essential for people to get the data on Snapchat. There is an expiry time as well. For many of the users, it is to go for the deletion of the data on an automatic basis. And there is an expiry time for a snap map for Media or the images. It gets deleted after 24 hours, and data can be secured. However, the research is done where it has been analyzed. While using the Snap chat, that deletion is the default in the Snap chat.

Instead, the synaptic data stores the data for too much time longer than it has defined for 24 hours. It shows that there is deletion time. But the media does not get deleted within 24 hours;

instead, with the use of Snap chat. It takes a lot of time to delete the data automatically once. The data is there on the Snap chat. It is stored for a longer period, and it can be used or downloaded from the available.



OSCINT tools such as Ghost Protocol are used to access the data and download it. With expiring keys, the Snapchat data can be forensic and recovered if it is present in the database needed after the proposed deletion period. The data is available for the synapse that users, no matter the users delete the data or do not go the use the data, are present on Snapchat. The further assessment of the result gives the proposed Framework that there are available items that can be extracted from the database of Snapchat.

The results give an error in the Snapchat user where the data is not deleted. According to the deletion time, it should be deleted after 24 hours. Rather it takes a lot of time to delete the data. Moreover, even the data is not permanently deleted; when required, the data can be used with foreign sake, demand. Therefore, it is obvious that data is not secured and can be present.

Tracking the location or media of a person through the site gives a clue that it is difficult to go for the distributed nature of Snapchat. It is impossible to have security while using Snapchat because tools can recover the password. Or even the location or the media of the person. During the incident, it is obvious that the people or people are available. And these weren't Tool for the use of Snapchat.

They can go for the extraction of multiple media videos from different places. It is important to note that there is a need to understand that the public could access the snap maps. Snap map is available where the media can be downloaded or the objects can be traced because there is no deletion period for these Snapchats.

The snap map denotes a density corresponding to the number of snaps uploaded in the given location. A dark red correspondence gives to the high volume of the use. Similarly, there is a blue, which is lower in number, and the least minimum number, which gives the lower use of the

location, the heat map scale. Yield is given to understand and use to specify the synapse that has been uploaded by the users in the settle equations or the places. Similarly, it gives a chance to the users to use the location so that they can access the information of the people, which is publicly available on the server, and access the person.

And it gives a clue that it is clear that snaps have the scent tools or the ghost protocols that can use the browsers or the websites that can access their data. However, Snapchat goes for the claim that data is not stored, and once the users go for the option of deletion of the data after 24 hours, then it will not be present (Villaespesa, and Wowkowych, 2020). And it will be deleted. It has been observed using the Snapchat app thatthe data is available after 24 hours, even if there is an analysis that shows that the data is available. The data shows that it can be accessed by any users who have access to the website and understand how to access publicly available data over the server.

Even the data is available for the forensic, use whenever needed the Snap or uploaded on the map, and they are the users using the reference device location. The device's location is there where people put their media, whether it is an image or a video, or a place where they are standing at that time. This accompanying data is moved in the database and is saved in the Application database, which the different methods can recall. There are Ghost Protocol or other methods to extract the location passwords or even the media to access the users' data.

These locations are used, and their location can be incorrect because the location used to win the Media is uploaded, and the database can be poisoned. Because it gives the different locations where people go for and upload their media. It calls the media to be located in the wrong way because there is a map, which can also give false results. Therefore, the users, even, can get it. The fake visual analysis goes for the investigation and the metadata is available on the synapse location. And once the map is incorrect, it can give false information. The map can be incorrect with the reason for the high volume of traffic because the majority of the people are using Snapchat and uploading their pictures.

Therefore, the different locations are the online detection of the location. They may get to the wrong location and move towards that. The experiment also gives that the computer screen plays a major role. While recording the video from the computer screen, there is an unknown location

with the snap chat tool. Because if someone captured the video for Snapchat using the Application of. But there is a video captured from the screen of the computer or the laptop, and then obviously, it can fake the other users.

They are moving towards the required location where the video is available, and then it will give them a fake quick visual analysis because it will not be present there. And the uploaded video will be from a different location because it is present on the computer or laptop for any other user or even in the user who is uploading the video. Maybe the owner of the video or the picture is not being captured eight the location to the Send video or the picture is being uploaded on Snapchat. So it gives that media content is also fake.

They are fake when the information is not correctly included. Applications are available for the people using the Application while presenting in their location to capture the video or the picture. But on the other side, there can be a curator reference for the video or the picture. Once they are captured from the laptop screen of a computer screen because they are recorded videos or listing videos already present on the laptop, even the person can capture the online video of the person or the location present on the laptop. But once again, it will give the fake location because the location will be captured for the user who is using Snapchat and giving the video recording or the picture uploaded on the location.

The location will be specified for the user using Snapchat on the mobile phone, not where the aerial video is recorded(Seidl, et al., 2015). Or the picture has been captured. So it gives that glue, even for those who are moving towards the capture of the videos on Snapchat, and does not give the Authority or security of getting the right video location or the time.

Therefore media metadata is verified while using the method that these people rely on the media, availability over the website rather than having the correct location. Therefore, the people using the snap chat will have their location on their mobile phones. This is because they are using the media and uploading Snapchat pictures.

It mentions Oscint tools can be used to get the data of Snapchat users. Different tools are available over the Internet to access the users' data. The paper has used the snap map to get the person's location who has shared media. It is the location detection of the person using the snap map. Similarly, a snap map also has stored media for a longer period. However, the app has

declared deletion time for media. But it does not work. There is no such check and balance from a snap chat application to control the media. The Media plays a major role where users are interested in getting other people's media. The snap map is the major Tool used to take other people's data.

Therefore the data over Snapchat is not secured. Snap chat is the Application where users save their media or captures using the camera. But the Media is stored for longer than the declared period. Users can delete the data at their end. But the data can be accessed easily from open-source sites. The sites are available to get the data of the users even it is deleted. Likewise, the data can be misused. The use of the scent Tool clarifies the data of snap chat can be hacked from open sources(Reed, 2022). There are open sources such as a snap map or ghost protocol to get the data. Thus the data can be misused after hacking from the tools available over the Internet.

The open-source sites give permit the users to access the media available. The availability of the media from the applications is the major reason behind the hacking of data. The data can be misused as it is easily available. The major reason the data is available is for the applications. The applications have not taken serious steps to move toward the data availability of the users. The application developers must keep in mind the deletion of data permanently when asked. Instead, the data is available for anytime access by a third party. It denotes the tools are there to access the data. Also, the data access is harmful to the people who use the Application. For example, Snapchat is widely used, but the data is available even after deleting it after tools.

Case-based Analysis Snap map and Snap Lion

Snap chat map gives access to Media even after the deletion period

A study has been done on the use of snap chat applications regarding privacy and security of the data. The data includes images and videos to be included in Snapchat, which the users of the Application share. In this regard, the paper went on at the collection of Secondary data and understood what tools are included in the Snapchat application that the users use. Andsimilarly, this Snapchat application is also available and based on the number of users who are increasing over time to use the Application and share their images and videos.

Similarly, the paper went on Snap chat Map, which is available for the users to include their images and video of images and videos, including the location of the person where he or she is taking the image or making the videos. On the other hand, it is included in the image or video.

The paper emphasized the security and privacy of the user's data of a snap chat application, giving authority to the users of Snapchat. And they go for the deletion of the data within a specified period of 24 hours or more. But it has been found in the study that data remains there in the snap chat application. Even the user deletes the data. After 24 hours, Snapchat does not delete the users' data, including images and pictures.

Rather Snapchat saves the data, and it has been found to share the data with many other users or third parties. There are open sources available for Snapchat. The open sources for the Snapchat application or the one that gives access to the people do search for media such as images and videos of the people or the user. They wish to see it and break the privacy of the users, where the users have selected for the deletion of the data. But data is not deleted.

Instead, the data is present there in the option to be viewed by any individual or the user; the third party involvement in this Snapchat application is done through the Tool or a Snapchat map. The Snapchat Map allows a user to search for the images for the users they are looking for. In the meantime, they can save the data and even get the location of the person taking the image or making the video at that time. Therefore it reveals the privacy of the users who are using the Snap chat application for entertainment purposes. But on the other side, they are data not secured by any means.

And there is an individual or the user knows how to use the tools, Such as Snap chat Map or other tools that can steal the data. Or they can steal the user's information on the individual who is present over Snapchat and sharing with the media. So the paper went on the use of safari developer mode to go for the object tree and understand how the third party extracts the data, or the users who go for the use of the data for searching, the information or the data of the person they are looking for. Similarly, there is a network option for them to go ching through the URL of Snapchat, map through the browser, and they get the media in terms of images or videos for their personal use as

There is a huge reason behind it: the error in the Application for not deleting. Being at the data on a timely basis is the developers in the snap chat application. They have instructed the users to delete their data if they want to within 24 hours. But on the other side, the programming has been done, where the data is not deleted. Instead, the data is available there for any third-party use.

Snap chat data is not Authentic for Investigation

The analysis and investigation for the study reveal that there is no such stronger privacy or security for the users' data. Rather, the user can access the data through the Snapchat application while using the Application URL through the online platform. Similarly, there is open-source information available for the users to go for the excess of the data; users can access the data for any purpose. They can also download it for their purposes. There are open-source tools available is, such as Ghost Protocol. It gives the data up to the users to go for the data downloading.

Snap chat is not secure and authentic

Snapchat is not a secure platform for users. There is access to the data of users. They can even recover the data the user of Snapchat deletes. There are Snapchat keys that move towards the data which is expired. But still, it is available in the information center of Snapchat for forensic investigation. Even Snapchat allows giving the data or information of the users to a third party through the database where the data has been deleted during the deletion period by the users. But it is available for the users, no matter what they have deleted. The use of the data database permits forensic investigation. Other third-party people who use the data for the wrong means can also represent the data on Snapchat (Seidl, et al., 2015).

The analysis also gave the idea that a database does not go for the deletion of data, and ghost protocols allow it to go for the exes and get the location on the other side. There is also density in this matter, where users go for making or taking pictures making videos through the other objects.

For example, if users go for making videos through laptops or the television platform, it will give you the location of the person making the video. They are in the area, but the video will not present the area or where it was made, or the video was captured in the other area. But the user is making the video through the television screen or the laptop screen. And then, it will show the location of the person who is making the video rather than giving the exact location of the video where the video the captured or made by the people.

The users who go for the investigation purposes, such as forensic investigation to get some information regarding the person's location or to get the information or data of the individual, were using Snapchat for a new legal purpose. It is not authentic to go for this Snapchat investigation because the users again make the video take the picture in any other location. Snapchat allows the users to take the location where the mobile or the Application is present. It is not the location that belongs to the video or the image of where it relates to.

Therefore, the analysis is done for investigation purposes, which is not sure to give the exact or authentic results regarding the person's location. Therefore, the device's location where it is used to make the picture can be detected. But it cannot be detected that the accompanying data is present at the exact location of the image or the picture. Even the personal gain or take the picture from a laptop computer or television screen. And therefore, it will represent that the picture has been taken where the application user on mobile is present.

Rather, it is not giving the exact location of the picture where it was at a cane. So the mobile investigation or Snapchat to get the information on the person's location is not authentic by any means. It will give the data or the result, which is based on the device's location and not the location of the media in an exact way.

Snap chat map and SnapLion tools make Snap chat insecure Application

In the year 2019, a breach of the snap chat data occurred, where the workers of Snapchat were spying on different users to view their location data, messages, and more before this. There were attacks two around 55,000 Snap chat Login credit credentials. It is a phishing attack in 2017 for data security is concerned (Paulsen, 2021). Snapchat Application breached the security of the users, and in 2019 on the higher level where it went on the security incidents(Reed, 2022). It was where the employees were abusing the users and were working.

Workers were viewing the regular users of the Snap chat. They were also reviewing their messages and even were getting the location of the people. The Snapchat employees or workers were also available in the Application. So they had access to any of the count of the people. And this became the major reason why the people over workers of the synapse. They, too, were having the excesses of the location or the people's information, and they were using that information for other, wrong means for purposes.

Similarly, there were exes of the data information, including email, addresses, phone numbers, and the other personal information of the users. So therefore, there was a tool involved to go for the object user's information from Snapchat Map. But along with this, there was the Tool involved, which was snapped lion, which is present internally for the workers as well to design. And it is to go for access to the data or information of the users present on the Snapchat application. So it was done initially to design, to go for the law enforcement requests. And then include the court orders and gate the authorized employees to get the users' data and do not use it for personal means.

Over time, the employees used the data for spamming and then tracked the users to analyze their activities. Even the workers were doing harmful activities. For example, workers were bullying the users using the snap chat application. However, former workers who came out could understand that there were workers with them, who were using the people's information, or users on the Snapchat application. It is not good for the reputation of the organization workers with the authorization were using these tools.

SnapLion is to get the reasons and justify why they had access, but they were not using the information. But it was the data that was available to the company and management to see that

workers had access to the accounts of the users. And they were opening the accounts of the users to get their locations, email addresses, phone numbers, and other useful information to use for the wrong means, which is unjustified. In any manner, it was not clear how much or what number of accounts existed inappropriately. Butsome consequences had a greater impact on other users of Snapchat.

The snap chat application is the most insecure. There were unauthorized activities by the workers. They have authorized access to the accounts or tools that can be used to get the location and date of the users. And those activities began at the time, and it was not known yet how many accounts were hacked. And what the data was used and for what purpose; therefore, it was named the phishing attack on the Snapchat accounts.

Results

the paper analyzed two tools for the snap chat investigation to be safe and secure for the users. In this regard, the tools used were named Snapchat, Map, and snapLion. These tools were used to understand how Snapchat is not giving a safe and pain secure platform whether Snapchat is giving a safe and secure platform for the users to use for their entertainment purpose.

Snapchat Application is Not Safe and Authentic

Snapchat Application is not safe and secure for the users to upload their media, including images and videos, over the Internet. Therefore, an analysis is done in the paper to investigate whether Snapchat is good for the users to upload their data or personal images or videos for entertainment purposes. The analysis for the paper has revealed that many people are using a snap map to access the media, including images and videos, even after the deletion period. Therefore, the application developers have revealed the option of deleting data after the specified period, such as 24 hours. Still, the snap chat does not go for the deletion of data even after a specified period.

However, the period is specified, but the snap chat keeps the data available for other individuals who can access the data through the recorded location of the people. The paper has emphasized the use of the data because users' data is personal data in it can be used. It is for any wrong means as to where snap Map is the Application or the option where the individuals can access the data while having the location of the people. Whenever the Snapchat map is used, then it can be analyzed that the person is using the particular location and he or she is standing there.

Therefore, it reveals the person's privacy, and it gives the results of not being safe and secure for the users or the people who take pictures and upload the videos. On the other side, the paper has also emphasized the use of fake locations. Therefore, for investigation purposes, snap chat goes for any of the investigations of the users who can be involved in any of the crimes. However, Snapchat cannot give them authentic or exact results. Because for the people taking pictures from the laptop or television screen. They cannot show the exact location. Rather, the Application will show the location where the person is available and taking the pictures or making the video.

On the other side, the exact, genuine location of the image or video will not be specified in the uploaded image or video as a whole, the media by the Snapchat users. Therefore, the Application

is not authentic or safe for the investigation purposes for any legal action to be taken against any of the person or individual using the image or video. Similarly, Snapchat uses the snaplion by the workers of the synaptic. The paper has investigated and allies how the workers of Snapchat have used the data from the year 2014 and onwards to use the data of the users and use it for the wrong means (Seidl, et al., 2015).

The employees of Snapchat have been taking the messages of the individuals, and they have been harassing the individuals and using the data for their means. Therefore, it was investigated that the workers were using the users' media to use them for harassment or other illegal means. Taking into consideration, it also reveals that Snapchat uses an application that is not safe and authentic for the users to upload their media over there. Similarly, Snapchat is not authentic because the management of Snapchat is not that efficient in controlling the employee's actions against the customers.

Once the consumers or users are dissatisfied, they know that their data, which is personal data and sensitive, is being used by the employee. Then they would never allow the Application to be installed on their mobile phones. It shows that Snapchat use can be harmful or dangerous for the users because it is not safe from both workers' perspectives.

There have been workers who use the data for their wrong or illegal means and for the Snap Chat Map, which gives the exact location of the people and media, even after the deletion of the data (Seidl et al., 2015). Both the tools reveal the use of snap chat is not authentic and safe for the users. It does not give Authority to the users to save their data and does not give authentic information to the users. Thus, the paper does not support the most authentic Snapchat application for the users.

OSCINT Tools of Snapchat Gives access to unauthorized people

The research came out of the major Tool to be included in the paper, the Snap lion and snap map. And it gave the major direct access to the workers who were using the data for the unjustified. They give the information to other people. Snapchat employees had major data access. The Department even could not recognize the activities they were doing there. The CEO of snap chat then analyzed the incident. Several employees were involved in spamming and taking the users'

data activities. The incident was then reported in 2017 to the FBI for further investigation (Villaespesa and Wowkowych, 2020).

It was done to analyze how employees used the tools for the unfair means together or to capture the people's or the users' data using the Snap chat application. And what has impacted the accounts of the people while getting their data. Thus, snap chat application is not a secure and safe platform for the users. The data or the information is not secured to share. There is no such privacy of the data from the workers. However, there have been major steps taken, but there is a lack in the performance of the data to provide timely security to the users. Similarly, OSCINT tools provide the major platform to the users or the third party to access the data and use it for unfair purposes.

Conclusion

Snapchat is considered a popular platform on Social Media as an application for entertainment purposes. There is open-source intelligence available where the data is present or publicly available, publicly available data. Or even the published data is available resources for the individual or users who can use them for different purposes. There are different purposes for the individuals who gather the data from open source intelligence to further investigate the data or to further use the data for their means.

Both the means are there. The purpose can be legal or illegal. They all have open-source tools available where public information can be gathered and used somehow. The paper analyzed different synaptic chat application tools to understand what tools are represented together with the users' information in this manner. The paper chooses to go for the two tools of Snapchat map and Snaplion.

It has been found that the use of snap chat applications is not secure for the users due to private see settings a The privacy settings do not give the option to go for the privacy of the shared information such as messages. It is not just about moving toward the most sensitive information by sharing videos—images over social media or applications. But on the other side, it is also about having non-encrypted messages. It shows the most sensitive information present over the social media platform using the snap chat application. Once one can read the messages of any user, then it can be very risky to use the data for any illegal purpose as well.

Therefore it has been found that the Snapchat application is not a secure application to share information, including both messages and media, since the application developer has not been available to give authentic and stronger privacy to the users so that they can confidently use the application without having any risk in mind.

There is no denying that Snapchat is the most popular application and is still being used by users. There are privacy and Security Options available. But, the literature revealed that even having the 2-step Verification about the factor of password can also be taken from the use of any of the sources, and there is no such privacy.

There is the availability of the code so that the code can be received via mobile text. And then, that code can be used for any illegal purposes. If any of the people get access to the person's mobile phone, having the application of Snapchat. The developers must consider going for better application use rather than relying on the privacy settings, which are no more considered the safest settings for people. Once they click on the privacy setting for not sharing their mobile number, or the data, their messages and media pictures are safe and secure. Instead, the media and the most sensitive information through. The message is not secure because it is not encrypted in information over the Snapchat application.

It is to go for the analysis and understand the safety and security of the users who have been using this inept application. In this regard, the paper went on to a long discussion on the literature and understood that there is the use of the snap chat data by the third party or the individual. So, for both legal and illegal purposes, the major outcome of the paper was done by the snap Map, where the map was used for the available location or data of the individuals or users who use the snap chat application for entertainment purposes. There is an option to delete the data about the Snapchat application that possesses the data for a while.

Therefore, it was analyzed that the third party can exist the data without permission, which will be publicly available. But open-source intelligence is not available on any of the other platforms. Rather, the individual who can use the open sources can gather the data and locate the person who is uploading the media, including images and videos. On the other side, the paper went on the analyze workers of Snapchat who used the tool snap map as data for the users. Therefore, Snapchat workers have the information of users to access the accounts of the users the Snapchat. In conclusion, snap chat possesses the tools that can be used to steal users' privacy. Therefore, it is unsafe, and the company should make it safe and secure.

This is to maintain better services for the users of the applications, rather than hack the information and use it for illegal means and access to an account. It is also for the other crime investigation purpose to provide the data to the legal authorities. Whenever they want to go for the analysis of the location of some of the people to investigate or move towards the legal means. Therefore, the paper understood that the snap chat workers used the people's data. It was for personal uses rather than having better use of the data to provide better services.

It revealed that open intelligence sources had affected the major security of the people's sensitive information collected and used by individual parties such as workers and other people. Therefore, the Snapchat tool is not a safe and secure platform for users. It is not safe. And secure platform for both legal and illegal users because they cannot get useful information to access and understand for their use.

Recommendations

Snapchat is a platform for entertainment purposes (Andrén and Heurlin, 2020). Many users appreciate using the Application for their media or sharing pictures and videos. Thus, there is a need to build a platform that gains the users' trust. Once the users are satisfied, it can gain higher productivity and profitability. There are many applications available, and due to higher competition, it is required to go for better options for the users to make them loyal to the use of Snapchat.

The paper results reveal that the use of snap chat is not safe and secure for individuals. For example, it is not safe to share the locations and permit workers to access the users' personal information (Bayer et al., 2016). Furthermore, users cannot delete their data permanently, and the data get stored for a longer period even after the deletion of the data.

- Snap chat management must consider the audit of the workers to analyze their performance and watch if they are using the information of the users for the illegal purpose
- Management must think about the developers of the application to perform well to raise the confidence of the users. However, many people are using the snap chat for entertainment. But still, they are unaware of or neglect the privacy or security of the application while knowing that the Snapchat application is not a secure application to use it.
- The management shouldn't neglect the development of the application, with better privacy settings, for the users to share their information through the messages with other users. The information shared by the medium of the message should be encrypted, and the users must have then access to their accounts rather than any third party can access

their account. Also, there should be two-way verification instead of having good, just text messaging and mobile phone.

- There should be e-mail verification so that users should verify their access to the account. And the system does not allow any third party to access the account or with the mayor use of code through the text message over sim or mobile phone.
- Management must introduce the developers who give a secure platform for the users to use with more confidence
- The major problem Snapchat application have the security issue. The users' data is not secure, and even it is not authentic to use for legal or investigation purposes. Therefore, the management would go for these steps to make the data secure and then save the data for the users.
- Similarly, The management should decide to secure the data use of the users by the workers. They should be several workers who can access the data of the users. And not all the workers must have access. It will give the huge privilege to the management to have confidence in the security of the user's data. So Snapchat possesses are the most sensitive information of the people to share pictures and videos.
- Management should introduce a new marketing strategy that highlights the secure platform for the users of the Application where their data will be end-to-end encrypted and will not be shared with anyone
- Any complaint from any user should be responded to in a while and also solve their issues at the earliest
- The tools for the access of the data should be analyzed, and then steps should be taken to ensure the safety and data of the users should be secured. The analysis of the tools gives the Authority to the management to analyze whether the developers should have the changes in the Application to make sure the better use of the Application or the user should go for the major changes for the security of the data. It gave me the confidence that the users should rely on the Application and use the platform without hindrance.

References

Andrén, O. and Heurlin, A., 2020. Snapchat Spectacles 2.0: Shakey or Secure.

Backlinko. 2022. *Snapchat Demographic Stats: How Many People Use Snapchat in 2022?*. [online] Available at: <https://backlinko.com/snapchat-users> [Accessed 19 February 2022].

Bayer, J.B., Ellison, N.B., Schoenebeck, S.Y. and Falk, E.B., 2016. Sharing the small moments: ephemeral social interaction on Snapchat. *Information, Communication & Society*, *19*(7), pp.956-977.

Benes, L., 2013. OSINT, new technologies, education: Expanding opportunities and threats. A new paradigm. *Journal of Strategic Security*, *6*(3), pp.22-37.

Bossetta, M., 2018. The digital architectures of social media: Comparing political campaigning on Facebook, Twitter, Instagram, and Snapchat in the 2016 US election. *Journalism & mass communication quarterly*, *95*(2), pp.471-496.

Charteris, J., Gregory, S. and Masters, Y., 2014. Snapchat'selfies': The case of disappearing data. *Rhetoric and Reality: Critical perspectives on educational technology. Proceedings of ascilite Dunedin 2014*.

Chitkara, A., Singh, D., Gupta, A. and Varshney, G., 2020, January. IntelliSpect: Personal Information Search Tool. In *2020 International Conference on Information Networking (ICOIN)* (pp. 556-561). IEEE.

Choi, T.R. and Sung, Y., 2018. Instagram versus Snapchat: Self-expression and privacy concern on social media. *Telematics and informatics*, *35*(8), pp.2289-2298.

Connelly, L. and Osborne, N., 2017, July. Exploring risk, privacy and the impact of social media usage with undergraduates. In *Proceedings of the European Conference on Social Media* (Vol. 4, pp. 72-80).

Courrier, S., 2021. Pourquoi l'Open Source Intelligence (OSINT) est une corde à ajouter à son arc. *I2D-Information, donnees documents*, (1), pp.52-55.

Evangelista, J.R.G., Sassi, R.J., Romero, M. and Napolitano, D., 2020. Systematic literature review to investigate the Application of open source intelligence (osint) with artificial intelligence. *Journal of Applied Security Research*, pp.1-25.

García, F.J.C., 2021. Private Investigation and Open Source INTelligence (OSINT). In *Cybersecurity Threats with New Perspectives*. IntechOpen.

Gibson, H., 2016. Acquisition and preparation of data for OSINT investigations. In *Open Source Intelligence Investigation* (pp. 69-93). Springer, Cham.

Gong, S., Cho, J. and Lee, C., 2018. A reliability comparison method for OSINT validity analysis. *IEEE Transactions on Industrial Informatics*, *14*(12), pp.5428-5435.

Hayden, M.E., 2019. Guide to Open Source Intelligence (OSINT).

Hollenbaugh, E.E., 2019. Privacy management among social media natives: An exploratory study of Facebook and Snapchat. *Social Media+ Society*, *5*(3), p.2056305119855144.

Hribar, G., Podbregar, I. and Ivanuša, T., 2014. OSINT: a "grey zone"?. *International Journal of Intelligence and CounterIntelligence*, *27*(3), pp.529-549.

Hulnick, A.S., 2010. The dilemma of open sources intelligence: Is OSINT really intelligence?. In *The Oxford handbook of national security intelligence*.

Kalpakis, G., Tsikrika, T., Cunningham, N., Iliou, C., Vrochidis, S., Middleton, J. and Kompatsiaris, I., 2016. OSINT and the Dark Web. In *Open Source Intelligence Investigation* (pp. 111-132). Springer, Cham.

Karthika, S., Bhalaji, N., Chithra, S., Harikarthick, N.S. and Bhattacharya, D., 2021. NoRegINT—A Tool for Performing OSINT and Analysis from Social Media. In *Inventive Computation and Information Technologies* (pp. 971-980). Springer, Singapore.

Konstantinidis, A., Chatzimilioudis, G., Zeinalipour-Yazti, D., Mpeis, P., Pelekis, N. and Theodoridis, Y., 2015. Privacy-preserving indoor localization on smartphones. *IEEE Transactions on Knowledge and Data Engineering*, *27*(11), pp.3042-3055.

Lao, C., Mao, C. and Sy, A., 2018. Security Analysis on Snapchat.

Lemay, D.J., Doleck, T. and Bazelais, P., 2017. "Passion and concern for privacy" as factors affecting snapchat use: A situated perspective on technology acceptance. *Computers in Human Behavior*, *75*, pp.264-271.

Li, C., Hay, M., Miklau, G. and Wang, Y., 2014. A data-and workload-aware algorithm for range queries under differential privacy. *arXiv preprint arXiv:1410.0265*.

MÂNDRAȘ, L.P., 2018. Social media și OSINT. *INFOSFERA-Revista de studii de securitate si Informații pentru Apărare*, *10*(4), pp.33-40.

Matthews, R., Lovell, K. and Sorell, M., 2021. Ghost protocol–Snapchat as a method of surveillance. *Forensic Science International: Digital Investigation*, *36*, p.301112.

McKenzie, G., Keßler, C. and Andris, C., 2019. Geospatial privacy and security. *Journal of spatial information science*, (19), pp.53-55.

Mercado, S.C., 2009. Sailing the Sea of OSINT in the Information Age. *Secret Intell Reader*, *78*.

Pastor-Galindo, J., Nespoli, P., Mármol, F.G. and Pérez, G.M., 2020. The not

Paulsen, J.E., 2021. AI, Trustworthiness, and the Digital Dirty Harry Problem. *Nordic Journal of Studies in Policing*, *8*(2), pp.1-19.

Perea El Khalifi, D., 2021. Social media and open source intelligence (OSINT) in Andalusian local governments: the cases of Instagram and Twitter.

Piwek, L. and Joinson, A., 2016. "What do they snapchat about?" Patterns of use in time-limited instant messaging service. *Computers in human behavior*, *54*, pp.358-367.

Poltash, N.A., 2012. Snapchat and sexting: A snapshot of baring your bare essentials. *Rich. JL & Tech.*, *19*, p.1.

Rakower, L.H., 2011. Blurred line: zooming in on Google Street View and the global right to privacy. *Brook. J. Int'l L.*, *37*, p.317.

Ramphul, K. and Mejias, S.G., 2018. Is" Snapchat Dysmorphia" a real issue?. *Cureus*, *10*(3).

Reed, C., 2022. *Snapchat Data Breaches: Full Timeline Through 2021*. [online] Firewall Times. Available at: <https://firewalltimes.com/snapchat-data-breach-timeline/> [Accessed 15 January 2022].

Revell, Q., Smith, T. and Stacey, R., 2016. Tools for OSINT-Based Investigations. In *Open Source Intelligence Investigation* (pp. 153-165). Springer, Cham.

Sambhe, N., Varma, P., Adlakhiya, A., Mahakalkar, A., Nakade, N. and Lakhe, R., 2021. USING OSINT TO GATHER INFORMATION ABOUT A USER FROM MULTIPLE SOCIAL NETWORKS. *INFORMATION TECHNOLOGY IN INDUSTRY*, *9*(2), pp.207-211.

Schwarz, K. and Creutzburg, R., 2021. Design of Professional Laboratory Exercises for Effective State-of-the-Art OSINT Investigation Tools-Part 1: RiskIQ Passive-Total. *Electronic imaging*, *2021*(3), pp.43-1.

Schwarz, K., Schwarz, F. and Creutzburg, R., 2020. Conception and implementation of professional laboratory exercises in the field of open source intelligence (OSINT). *Electronic Imaging*, *2020*(3), pp.278-1.

Seidl, D.E., Paulus, G., Jankowski, P. and Regenfelder, M., 2015. Spatial obfuscation methods for privacy protection of household-level data. *Applied Geography*, *63*, pp.253-263.

Sharma, S.S. and De Choudhury, M., 2015, May. Measuring and characterising nutritional information of food and ingestion content in instagram. In *Proceedings of the 24th International Conference on World Wide Web* (pp. 115-116).

Shipp, A.J. and Fried, Y. eds., 2014. *Time and work, Volume 1: How time impacts individuals*. Psychology Press.

Soffer, O., 2016. The oral paradigm and Snapchat. *Social Media+ Society*, *2*(3), p.2056305116666306.

Stutzman, F.D., Gross, R. and Acquisti, A., 2013. Silent listeners: The evolution of privacy and disclosure on Facebook. *Journal of privacy and confidentiality*, *4*(2), p.2.

Tabatabaei, F. and Wells, D., 2016. OSINT in the Context of Cyber-Security. *Open source intelligence investigation*, pp.213-231.

Trend Calendar, 2020. Trending Words on 28th May, 2020. *Trend Calendar*. https:// us.trend-calendar.com/trend/2020-05-28.htmlviahttps://app.cappture.cc/ snapshots/1ead0778-82a6-6ae0-8bfa-0ea9b2ae1df4. (Accessed 20 Dec 2021)

Truelove, V., Freeman, J. and Davey, J., 2019. "I Snapchat and Drive!" A mixed methods approach examining snapchat use while driving and deterrent perceptions among young adults. *Accident Analysis & Prevention*, *131*, pp.146-156.

Utz, S., Muscanell, N. and Khalid, C., 2015. Snapchat elicits more jealousy than Facebook: A comparison of Snapchat and Facebook use. *Cyberpsychology, Behavior, and Social Networking*, *18*(3), pp.141-146.

Vaterlaus, J.M., Barnett, K., Roche, C. and Young, J.A., 2016. "Snapchat is more personal": An exploratory study on Snapchat behaviors and young adult interpersonal relationships. *Computers in Human Behavior*, *62*, pp.594-601.

Velten, J.C. and Arif, R., 2016. The influence of snapchat on interpersonal relationship development and human communication. *The Journal of Social Media in Society*, *5*(2), pp.5-43.

Velten, J.C., Arif, R. and Moehring, D., 2017. Managing disclosure through social media: How Snapchat is shaking boundaries of privacy perceptions. *The Journal of Social Media in Society*, *6*(1), pp.220-250.

Villaespesa, E. and Wowkowych, S., 2020. Ephemeral storytelling with social media: Snapchat and Instagram stories at the Brooklyn Museum. *Social Media+ Society*, *6*(1), p.2056305119898776.

Wang, J., Zhu, R., Liu, S. and Cai, Z., 2018. Node location privacy protection based on differentially private grids in industrial wireless sensor networks. *Sensors*, *18*(2), p.410.

Wells, D. and Gibson, H., 2017. OSINT from a UK perspective: Considerations from the law enforcement and military domains. *Proceedings Estonian Academy of Security Sciences, 16: From Research to Security Union*, *16*, pp.84-113.

Williams, H.J. and Blum, I., 2018. *Defining second generation open source intelligence (OSINT) for the defense enterprise*. RAND Corporation Santa Monica United States.

Wiradarma, A.A.B.A. and Sasmita, G.M.A., 2019. IT Risk Management Based on ISO 31000 and OWASP Framework using OSINT at the Information Gathering Stage (Case Study: X Company). *International Journal of Computer Network and Information Security*, *11*(12), p.17.

Zulean, M. and Şercan, E., 2018. Democratic control of Romanian intelligence after three decades: quis custodiet ipsos custodes?. *Defense & Security Analysis*, *34*(4), pp.365-384.