Ghost Protocol – Snapchat as a Method of Surveillance

By:

Richard Matthews, Kieren Lovell and Matthew Sorell

From the proceedings of

The Digital Forensic Research Conference

DFRWS EU 2021

March 29 - April 1, 2021

Forensic Science International: Digital Investigation 36 (2021) 301112

Contents lists available at ScienceDirect

Forensic Science International: Digital Investigation

journal homepage: www.elsevier.com/locate/fsidi

Full Paper

Ghost protocol – Snapchat as a method of surveillance

Richard Matthews [a, *], Kieren Lovell [b], Matthew Sorell [a]

[a] University of Adelaide, School of Electrical and Electronic Engineering, Adelaide, Australia
[b] Tallinn University of Technology, School of Information Technologies: Department of Software Sciences, Tallinn, Estonia

ARTICLE INFO

Article history:
Available online 23 March 2021

Keywords:
Open source intelligence
Surveillance
Snapchat
Digital forensics

ABSTRACT

Social Networking Sites (SNS) are a rich source of open-source intelligence in the form of publicly available images, video and text. Privacy concerns have led to many sites removing metadata attached to multimedia on upload, effectively losing information of interest from intelligence perspectives. In this paper, we describe the exploitation of Snapchat's Snap Map (a web based portal to access media items uploaded to Snapchat's platform) as a surveillance tool to monitor the social unrest in Minneapolis - Saint Paul following the death of George Floyd, making specific use of the manner in which Snapchat presents Snaps on a publicly accessible map. We demonstrate how our technique can be used as a distributed surveillance system supplementing traditional CCTV footage where none would be available. We note a heavy reliance on trust is implied on the geolocation metadata and the resolution of the uploaded media. As a result, our process is vulnerable to database poisoning attacks. We therefore recommend that alternative forensic methods be used to verify and validate surveillance using our method.

1. Introduction

On May 28 2020 the hashtag “#minneapolisriots” was trending on the social network site (SNS) Twitter (Trend Calendar, 2020). Riots had broken out across Minneapolis - Saint Paul in response to the death of George Floyd. Users of SNSs were able to post visual media directly to public sites, allowing others to watch events unfold before their eyes, unbiased by the filter of broadcast media. Snapchat is just one of many such sites which enabled this to happen.

In June 2017 Snapchat updated their mobile application to introduce a new feature to allow users to upload curated media to a public “Snap Map“. The idea was that users could see other users on a live map and tap on a heatmap overlay to see where images and video were being uploaded in spots of activity. The media were quick to recognize the power of this tool when just two months later Hurricane Harvey struck the US states of Texas and Louisiana (Epstein, 2017). At the same time, images uploaded to Snapchat and distributed via Twitter showed President Trump misrepresenting crowds during a campaign stop. Media uploaded to the Snap Map showed the group was mainly made up of protestors (Hamby, 2017). Six months later, Snapchat would make this same feature available via a direct URL maps.snapchat.com available.

Snapchat has not been the only SNS used for such disclosures. In 2015, Russian military soldiers were located in Syria from geolocation-tagged photos posted to SNSs, including Instagram and Twitter. Such disclosure contradicted the political narrative of the time (Tsvetkova, 2015). Dating applications like Tinder and Grindr have also been used to geolocate individuals using triangulation (Frizell, 2014). At the end of 2013, in attempts to resolve the issue, Tinder downgrade the accuracy of the location feature to increments of 1 mile rather than 100 feet.

The prominence of SNSs being used to reveal hidden information has led to the following hypothesis: that Social Networking Sites can be used as a distributed surveillance system for the purposes of law enforcement and intelligence community. This hypothesis leads to the following questions:

- Can the SNS Snapchat be used as a distributed surveillance system?
- What method is required to easily extract media from Snapchat?
- How do we verify OSINT (Open Source Intelligence) media for surveillance purposes?

The next section discusses relevant work. Section 3 discusses the experimental design and methodology. Section 4 presents our results, the synthesis of information to form apparent conclusions

[*] Corresponding author.
E-mail address: publications@drmatthews.science (R. Matthews).

https://doi.org/10.1016/j.fsidi.2021.301112

and indicates future work. We conclude in Section 5 with a discussion of limitations.

2. Background

The definition of SNSs is given in the work of Boyd and Ellison (2007) as “web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system“. Graves et al. (2020) note that this differs to the definition of social media which focuses on user generated content, and Web 2.0 technologies specifically. We use the generic term SNS to describe both SNS and social media more broadly noting that Snapchat is consistent with the definition of SNSs given by Boyd and Ellison, excluding the ability to navigate the connections made by others in their network.

Mining digital evidence from SNSs is not new. Cusack and Alshaifi (2015) provided a case study of the proprietary tool *EnCase Forensic* to extract forensic artefacts from several test cases limited to accessed SNS URLs, web browser cache, local internet session artefacts created by interaction with SNS, and Facebook chat analysis. Their study further focused on Facebook, Twitter, Instagram, LinkedIn and Bayt.

To our knowledge, there has not been a technical assessment of Snapchat as a tool for surveillance. Snapchat has been evaluated as a method for sharing radiology didactics, exploiting the destructive capability of the image sharing SNS (Spieler et al., 2020). The results of the study suggested that Snapchat may be a viable method for diagnostics instead of using the traditional classroom mounted light boxes. Our study likewise explores similar “off-label” uses for the SNS. The previous work (Lovell and Heering, 2019) as seen in (Bay et al., 2020) introduced Snapchat as a method to track NATO maritime vessels. Eriksson et al. (2019) correctly identified that Snapchat's Snap Map can be scraped to extract user-generated content and location data; however, they excluded it from their study due to the inability to access a public API. In their study they explored the extraction of data from common SNSs as Twitter and Reddit for the purposes of facial recognition (Eriksson et al., 2019). The work of Jalal et al. (2019) documented a method of extracting images from Instagram posts using a scrape-by-location methodology and scrape-by-keyword. Similarly, in Mejova et al. (2015) a technique for extracting location data from Foursquare was documented to create a dataset of restaurant locations. This dataset was used to obtain images of food from Instagram using an Instagram specific API.

Sharma and De Choudhury (2015) have used the Instagram specific API to extract posts and images to document nutritional information on Instagram content. Fried et al. (2014) has been successful in obtaining information from Twitter to measure intrinsic population characteristics such as political leaning and geographical location. Huber et al. (2011) have also proposed a toolset which enables Facebook profile information and accompanying information to be captured in what is referred to as “social snapshots”. In all cases of successful scraping except Huber, authors relied upon public APIs. In our work, we do not rely upon open APIs and instead propose a bespoke and semi-manual method for content retrieval. This can be further automated through the reverse engineering of private APIs, but its description is left as the subject of a future paper.

3. Experimental design and method

We provide a method of digital media extraction from the SNS Snapchat before analysing if it is a suitable replacement for a CCTV system. To answer the question “Can Snapchat be used as a distributed surveillance system?” we first must characterize what a surveillance system is.

According to the Australia and New Zealand Police Recommendations for CCTV Systems (Electronic Evidence Specialists Advisory Group (EESAG), 2014), the desirable outcomes for law enforcement from a CCTV surveillance system can be broken down into six key areas. These are:

- identify facial features at entry, exit and transaction points in a business,
- read licence plate numbers,
- recognize clothing worn by persons of interest,
- monitor general activity in areas accessed by the public,
- an ability to track people moving through a site, and
- have a sufficient frame rate to track movement.

The media must also be easily extractable from the surveillance system and be obtainable in a format that is readable across systems. It is important to note that in this paper we are only concerned with the extraction of media and the analysis against the above framework.

As discussed by Jang and Kwak (2015) in Cusack and Alshaifi (2015) digital evidence must also be extracted while respecting the reasonable privacy of the individuals in question and without coercion or spoliation. Breaches of these principles may lead to the digital evidence being unacceptable for admission in addition to evaluation against the well established Daubert criteria.

To this end, an initial proof of concept study was performed using the built-in screen recording software in Apple iOS to determine if media could be easily extracted. The reasonable privacy of individuals was respected throughout the experimental design as only public media was recorded. This feasibility study showed that while media could successfully be obtained from Snapchat's Snap Map without notifying the user, it did not save any of the accompanying metadata leading to possible evidence spoilage.

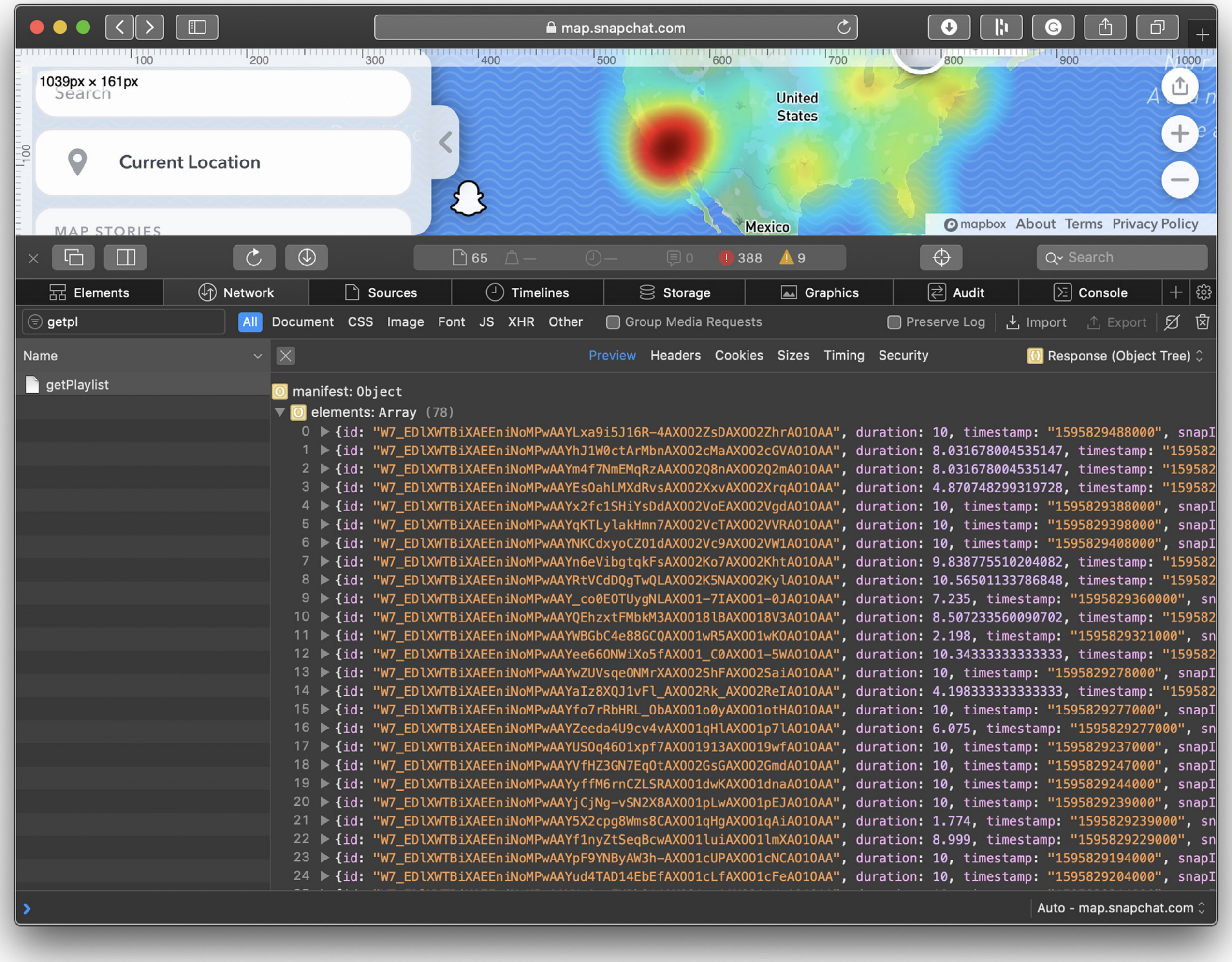
We then expanded our feasibility study to the web-hosted version of Snap Map. On the web version of Snap Map, it was observed that media was delivered as a response to a proprietary API using a POST query. By using a browser's development mode, we were able to view the answer to this POST query as an accompanying JSON objects (Fig. 1). These JSON objects contains metadata for the returned snaps. As a result, our method focused on the web version of the application to capture media from the Snap Map, where it is possible to view the JSON objects and record the accompanying metadata. While this does not prevent data spoilage of the metadata in the saved files, it does allow a copy of the metadata to be preserved in an additional text format. This prevents the spoilage of the metadata. Once again, only public media was recorded to maintain individuals' reasonable expectations of privacy.

3.1. *Process*

The location, collection, storage and analysis of media in this research was achieved as follows:

3.1.1. *Hotspot location*

Using Safari with developer mode enabled, navigate to maps.snapchat.com. Browse the map to find a location of interest referencing the heat map to find a location with media uploaded. This heat map is further discussed below.



```
manifest: Object
▼ elements: Array (78)
  0 ▶ {id: "W7_EDlXWTBiXAEEniNoMPwAAYLxa9i5J16R-4AX002ZsDAX002ZhrA010AA", duration: 10, timestamp: "1595829488000", snapI
  1 ▶ {id: "W7_EDlXWTBiXAEEniNoMPwAAYhJ1W0ctArMbnAX002cMaAX002cGVA010AA", duration: 8.031678004535147, timestamp: "159582
  2 ▶ {id: "W7_EDlXWTBiXAEEniNoMPwAAYm4f7NmEMqRzAAX002Q8nAX002Q2mA010AA", duration: 8.031678004535147, timestamp: "159582
  3 ▶ {id: "W7_EDlXWTBiXAEEniNoMPwAAYEsOahLMXdRvsAX002XxvAX002XrqA010AA", duration: 4.870748299319728, timestamp: "159582
  4 ▶ {id: "W7_EDlXWTBiXAEEniNoMPwAAYx2fc1SHiYsDdAX002VoEAX002VgdA010AA", duration: 10, timestamp: "1595829388000", snapI
  5 ▶ {id: "W7_EDlXWTBiXAEEniNoMPwAAYqKTLylakHmn7AX002VcTAX002VVRA010AA", duration: 10, timestamp: "1595829398000", snapI
  6 ▶ {id: "W7_EDlXWTBiXAEEniNoMPwAAYNKCdxyoCZ01dAX002Vc9AX002VW1A010AA", duration: 10, timestamp: "1595829408000", snapI
  7 ▶ {id: "W7_EDlXWTBiXAEEniNoMPwAAYn6eVibgtqkFsAX002Ko7AX002KhtA010AA", duration: 9.838775510204082, timestamp: "159582
  8 ▶ {id: "W7_EDlXWTBiXAEEniNoMPwAAYRtVCdDQgTwQLAX002K5NAX002KylA010AA", duration: 10.56501133786848, timestamp: "159582
  9 ▶ {id: "W7_EDlXWTBiXAEEniNoMPwAAY_co0EOTUygNLAX001-7IAX001-0JA010AA", duration: 7.235, timestamp: "1595829360000", sn
 10 ▶ {id: "W7_EDlXWTBiXAEEniNoMPwAAYQEhzxtFMbkM3AX0018lBAX0018V3A010AA", duration: 8.507233560090702, timestamp: "159582
 11 ▶ {id: "W7_EDlXWTBiXAEEniNoMPwAAYWBGbC4e88GCQAX001wR5AX001wKOA010AA", duration: 2.198, timestamp: "1595829321000", sn
 12 ▶ {id: "W7_EDlXWTBiXAEEniNoMPwAAYee66ONWiXo5fAX001_C0AX001-5WA010AA", duration: 10.34333333333333, timestamp: "159582
 13 ▶ {id: "W7_EDlXWTBiXAEEniNoMPwAAYwZUVsqeONMrXAX002ShFAX002SaiA010AA", duration: 10, timestamp: "1595829278000", snapI
 14 ▶ {id: "W7_EDlXWTBiXAEEniNoMPwAAYaIz8XQJ1vFl_AX002Rk_AX002ReIA010AA", duration: 4.198333333333333, timestamp: "159582
 15 ▶ {id: "W7_EDlXWTBiXAEEniNoMPwAAYfo7rRbHRL_ObAX001o0yAX001otHA010AA", duration: 10, timestamp: "1595829277000", snapI
 16 ▶ {id: "W7_EDlXWTBiXAEEniNoMPwAAYZeeda4U9cv4vAX001qHlAX001p7lA010AA", duration: 6.075, timestamp: "1595829277000", sn
 17 ▶ {id: "W7_EDlXWTBiXAEEniNoMPwAAYUSOq4601xpf7AX001913AX0019wfA010AA", duration: 10, timestamp: "1595829237000", snapI
 18 ▶ {id: "W7_EDlXWTBiXAEEniNoMPwAAYVfHZ3GN7Eq0tAX002GsGAX002GmdA010AA", duration: 10, timestamp: "1595829247000", snapI
 19 ▶ {id: "W7_EDlXWTBiXAEEniNoMPwAAYyffM6rnCZLSRAX001dwKAX001dnaA010AA", duration: 10, timestamp: "1595829244000", snapI
 20 ▶ {id: "W7_EDlXWTBiXAEEniNoMPwAAYjCjNg-vSN2X8AX001pLwAX001pEJA010AA", duration: 10, timestamp: "1595829239000", snapI
 21 ▶ {id: "W7_EDlXWTBiXAEEniNoMPwAAY5X2cpg8Wms8CAX001qHgAX001qAiA010AA", duration: 1.774, timestamp: "1595829239000", sn
 22 ▶ {id: "W7_EDlXWTBiXAEEniNoMPwAAYf1nyZtSeqBcwAX001luiAX001lmXA010AA", duration: 8.999, timestamp: "1595829229000", sn
 23 ▶ {id: "W7_EDlXWTBiXAEEniNoMPwAAYpF9YNByAW3h-AX001cUPAX001cNCA010AA", duration: 10, timestamp: "1595829194000", snapI
 24 ▶ {id: "W7_EDlXWTBiXAEEniNoMPwAAYud4TAD14EbEfAX001cLfAX001cFeA010AA", duration: 10, timestamp: "1595829204000", snapI
```

Fig. 1. The JSON objects represented as an object tree using Safari developer mode.

3.1.2. Media identification

Clicking on the location will cause a circle of differing radius to load up to a maximum of 80 snaps from the map. This radius is dependent on the level of map zoom. Clicking through the playlist, a video or image is located that is identified as being of interest. The URL at the top of the browser window will change for each new media that is loaded. This URL contains the metadata value 'SnapID'. This ID is noted. The remainder value in the URL is the location from which the request has been made, not the site from which the media has been uploaded.

3.1.3. Download

Using the developer mode, the network option is selected to display the web request using JavaScript 'getPlaylist'. This contains the JSON objects relevant to the media that has just been loaded in the browser from the map. The JSON objects are then referred to find the SnapID that was located in the browser. Within the JSON objects, a value is stored that contains the direct link to the server copy of the media. The media is then saved from the server and stored locally. As the media is directly accessed from the server and saved locally, a local copy is created which does not preserve the metadata. A copy of the JSON response for the 'getPlaylist' method is also saved to keep the accompanying metadata.

3.1.4. Storage

All media is saved to a folder which is backed up via push methods to a secure location. Extractions are saved with reference to date, time and location of the media extracted. Media is saved with the ID taken from the associated metadata tag as the file name. A further text file is saved, which contains the URL location to access the media directly. All data were then stored for later analysis.

3.2. Automation

In the course of our study, we have been able to further automate our process through the exploitation of developed scripts which rely on the private APIs indicated above. By using a POST method call, we are able to extract images through a scripted process simply by providing a set of co-ordinates consisting of latitude, longitude and download radius. We now discuss in detail the findings of this method when applied to (1) the study of the Twin City riots following the death of George Floyd and (2) during the policing of COVID restrictions in researchers' hometown of Adelaide, South Australia.

4. Results

To meet the needs of intelligence and policing requirements, the ANZPAA NIFS framework highlights six key areas that should be met to have an effective system. When read in conjunction with the intelligence cycle shown in Williams and Blum (2018) we see additional requirements around media extraction, and media availability to enable timely collection. We also note there are key findings that can be drawn from the JSON objects extracted from the SNS application itself. We now present these findings starting with a break down of the JSON objects followed by our framework analysis.

4.1. JSON objects

The exploitation of JSON objects using Safari developer mode is the enabling feature of our method. Similar results can be achieved in any modern internet browser. We believe this method has wider applications to be explored in future work. Consulting the raw JSON objects we see that Snapchat provides multiple metadata tags of interest to the forensic investigator. These fields are listed in Table 1.

4.2. Media extraction

The method proposed in Section 3 was applied during the period 28 to 31 May 2020, coinciding with the dates of the Twin City Riots following the death in custody of George Floyd. Over this time 2692 Snaps were extracted from the Snap Map comprising of 2600 MP4 videos and 92 JPEG images. The results of the media obtained is shown in Table 2.

Based on the result of nearly 2700 Snaps extracted in MP4 or JPEG format from the Snap Map over four days it is found that media can be easily extracted, and in a form that is easy to make readily viewable according to the framework we have adopted.

4.3. Media availability

To access images directly from the server, the URL contains an expiry EPOCH time, a key name and a key signature (Fig. 2). From Google documentation, it is noted that this is an example of a signed URL. “A signed URL is a URL that provides limited permission and time to make a request” (Google, c). We assume that this expiry time is the time that the image will no longer be made available from the server as the key will simply be rendered invalid. Comparing the extracted expiry time to the captured time noted in the metadata allowed an analysis of how long JPEG images are accessible from the server.

JPEG images (Fig. 3b) were found to have an expiry time hard-coded in the access URL (Fig. 2). This time ranged from 90 days and 7 s to 90 days, 45 min and 29 s. Both video media and JPEG images were found to use Google Cloud Storage XML API with the relevant expiration set for 90 days (Fig. 3). However, no evidence of deletion was found; instead, what was indicated was key expiry which rendered the media no longer accessible. It remains unknown if data can be recovered after this expiry date. Access cache control is set to 3600 s or 60 min which is consistent with our analysis finding the JPEG URL expiration time ranged. All times fell within this 3600 s allocation. As a result, it is determined that Snapchat has the necessary availability required for a surveillance system.

Videos are delivered by a different method which also uses a signed URL (Fig. 3a). The manner for providing video content is consistent with the V4 signing process within Google cloud (Google, b). In both cases, it was found that media was made accessible on the server through signed URLs for at least 90 days. Both methods utilize HTTP Headers and query strings (Fig. 3) based on the Google Cloud Storage XML API (Google, a) indicating that the previous process of parsing the signed URL may have been superseded and not cleaned up in the implementation of the current live production system.

Expiry times were found for Snapchat media from Snapchat Support (Snapchat, 0000) and are documented in Table 3.

The implication from these expiry times is that many users are under the impression that Snaps expire within 24 h. Snapchat states that “Deletion is our default” (Snapchat). Our research suggests that media may be stored much longer than the indicated deletion time. Through the use of expiring keys, media may be forensically recoverable from databases long after the proposed deletion time.

To further assess our results against the proposed frameworks, 3,00 media items were randomly selected from our extracted database of 2692. The results are shown in Table 4. Understanding error is important for any work in forensic science. Treating the data as a simple random sample, we can determine the standard error of our sample. Treating our sample as a non-finite population and using a 99% confidence level our standard error is calculated to be 2.89%.

From the analysis in Table 4 of the Twin City Riot case study it is clear that Snapchat has the potential to meet the following needs of a conventional surveillance system: ability to (1) identify faces, (2) identify clothing, (3) detect general activity and (4) track moving targets. Further evidence is required to determine the systems ability to track a target through a site of interest and to detect number plates. Facial identification is possible when high resolution media is obtained. This is similar to current CCTV trends. As a result, further study was conducted on the city of Adelaide to monitor night-life activity during the COVID restrictions between April to July of 2020. The same method was used as documented above to extract media items utilising the Snap Map. We do not report all media extracted but instead highlight cases that showcase the ability to identify faces, track users through a site and record number plates as these were the areas that required the most study.

4.4. Identifying faces

As with traditional CCTV setups, identifying faces depends on the quality of the image presented. Our results suggest facial recognition is capable using Snapchat's Snap Map but is heavily determined by the quality of the images saved on the map. This applies to manual methods using experienced CCTV examiners. Fully automated methods of facial recognition are beyond the scope of this paper. We suggest this as a future avenue for study. For the experienced CCTV examiner, it is likely a positive facial match would be able to be made from the media we were able to extract however, additional sources of information may be required in some instance especially for comparison. During our analysis of COVID restrictions we were able to successfully identify patrons in high traffic establishments allegedly failing to obey social distancing and other measures in place. These images were able to be passed onto local law enforcement for further investigation. The breaches were followed up with traditional policing methods including the use of CCTV and to our knowledge infringement notices were issued to non-compliant establishments.

4.5. Tracking through a site

Tracking a person through a site proves difficult due to the distributed nature of Snapchat. This does not mean it is impossible. During one incident, we were able to reverse engineer the timeline

Table 1
Metadata fields contained within the JSON Objects for Snapchat's Snap Map.

<table>
<tr><th>JSON Object</th><th>Type</th><th>Description</th></tr>
<tr><td>id</td><td>String</td><td>Unique string which identifies the object</td></tr>
<tr><td>duration</td><td>double</td><td>Length of video media types. Not present for image uploads.</td></tr>
<tr><td>timestamp</td><td>String</td><td>EPOCH time stamp.</td></tr>
<tr><td>snapInfo</td><td>Object</td><td>Container for below methods.</td></tr>
<tr><td>||.overlayText</td><td>String</td><td>Overlay text on media item added by Snapchat at upload.</td></tr>
<tr><td>||.publicMediaInfo.publicImageMediaInfo.mediaUrl</td><td>String</td><td>Image URL for image based post only</td></tr>
<tr><td>||.snapMediaType</td><td>String</td><td>Contains one of the following: SNAP_MEDIA_TYPE_VIDEO, SNAP_MEDIA_TYPE_VIDEO_NO_SOUND. Not present for image media uploads.</td></tr>
<tr><td>||.streamingMediaInfo</td><td>Object</td><td>Object containing below variables. Empty for image media type</td></tr>
<tr><td>||.||.mediaUrl</td><td>String</td><td>endingURL for video without edits by the Snapchat user. Empty for image media type</td></tr>
<tr><td>||.||.overlayUrl</td><td>String</td><td>endingURL for video with overlay text. Empty for image media type</td></tr>
<tr><td>||.||.prefixUrl</td><td>String</td><td>Location of media items. Combine with either mediaUrl, overlayUrl, previewUrl or previewWithOverlayUrl to obtain item. Empty for image media type</td></tr>
<tr><td>||.||.previewUrl</td><td>String</td><td>Preview image still from video. Empty for image media type</td></tr>
<tr><td>||.||.previewWithOverlayUrl</td><td>String</td><td>Preview image still from video with overlay. Empty for image media type</td></tr>
<tr><td>||.streamingThumbnailInfo</td><td>Object</td><td></td></tr>
<tr><td>||.||.infos</td><td>Object Array</td><td></td></tr>
<tr><td>||.||.infos[0] .IMAGE_THUMBNAIL_TYPE</td><td>String</td><td>contains “IMAGE_THUMBNAIL_TYPE”</td></tr>
<tr><td>||.||.infos[0] .thumbnailUrl</td><td>String</td><td>Full URL of jpeg.</td></tr>
<tr><td>||.||.infos[1] .VIDEO_THUMBNAIL_TYPE</td><td>String</td><td>Contains “VIDEO_THUMBNAIL_TYPE”, Empty for image media type</td></tr>
<tr><td>||.||.infos[1] .thumbnailUrl</td><td>String</td><td>Full URL of MP4. Empty for image media type</td></tr>
<tr><td>||.title</td><td>Object</td><td>Container to display the location information on the Snap when played.</td></tr>
<tr><td>||.||.fallback</td><td>String</td><td>Fallback location in English</td></tr>
<tr><td>||.||.strings</td><td>Array</td><td>10 in length ISO 639-1 Language codes and location. These are not always reported in constant order.</td></tr>
</table>

Table 2
Total extracted media by day.

	Extracted Media	Images	Videos
May 28	617	19	598
May 29	1434	39	1395
May 30	152	4	148
May 31	489	30	459
Total	2692	92	2600

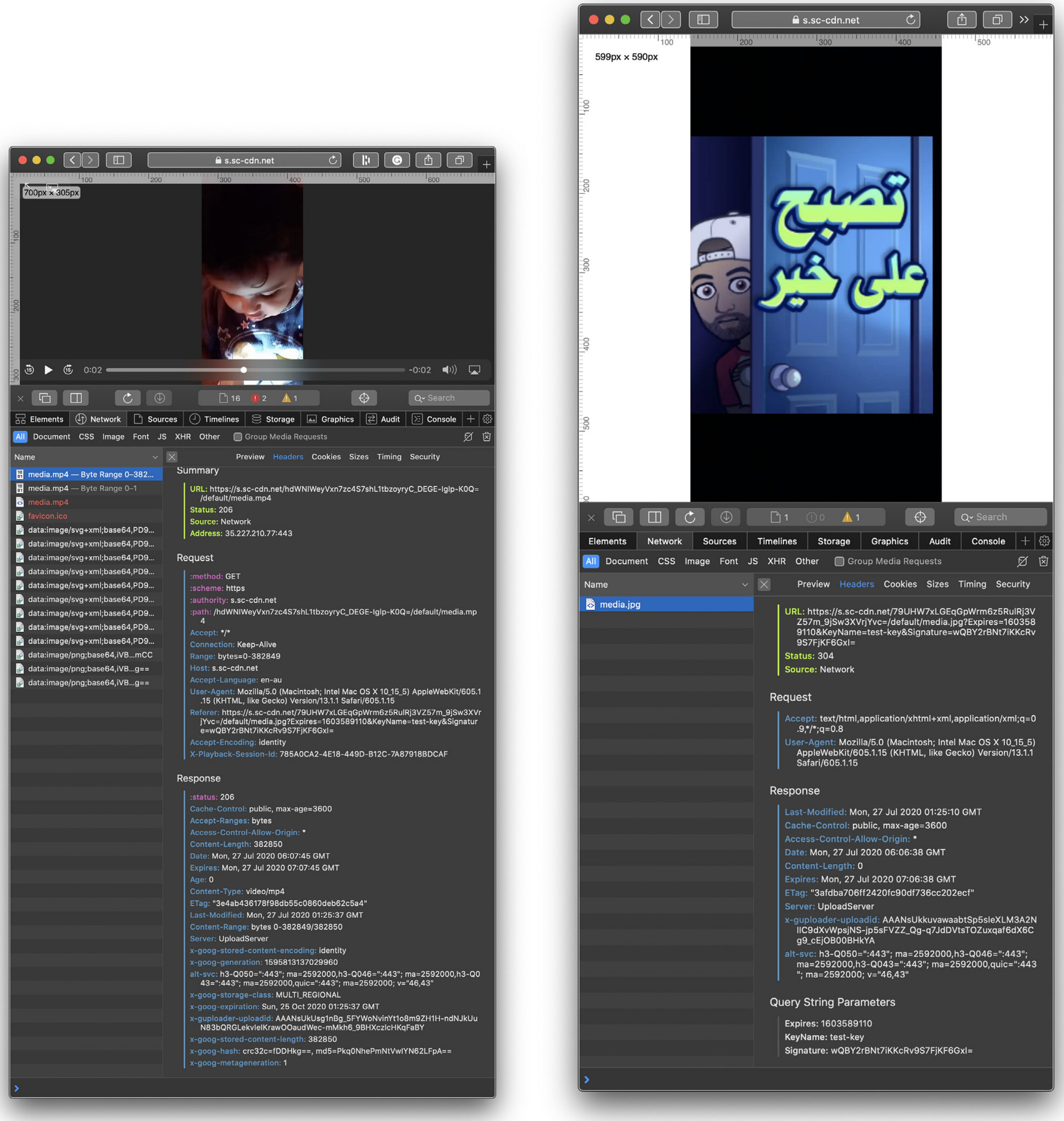
of a gentleman on a bucksnight due to multiple videos being taken at different places around Adelaide. We were able to note the time his group entered the city, had dinner, left the city and visited a bottle shop in the northern suburbs that evening. Through downloaded media from the public Snap Map we were able to trace the subjects movements through the wider metropolitan area of Adelaide, South Australia using nothing but visual comparison. Such a method easily lends itself to automation using machine learning and object recognition algorithms so long as a sufficiently accurate training set was provided.

4.6. *Reading number plates*

While the quality of media made it difficult to read licence plates this did not mean the task was impossible. In one such example we were able to extract a plate number from a vehicle we identified as https://s.sc-cdn.net/nad_nUCjCEd6HzZVFChgToQxk91QDYeGDRgAxcRIOfQ=/default/media.jpg?Expires=1598405853&KeyName=test-key&Signature=9fXICtku0iA7z4OkRGLxlRRrD9k=

ROOT URL Expiry Key Name Signature

Fig. 2. The Snapchat implementation of Google Cloud signed URLs for JPEG images.



```
media.mp4 — Byte Range 0–382...
media.mp4 — Byte Range 0–1
media.mp4
favicon.ico
data:image/svg+xml;base64,PD9...
data:image/svg+xml;base64,PD9...
data:image/svg+xml;base64,PD9...
data:image/svg+xml;base64,PD9...
data:image/svg+xml;base64,PD9...
data:image/svg+xml;base64,PD9...
data:image/svg+xml;base64,PD9...
data:image/svg+xml;base64,PD9...
data:image/svg+xml;base64,PD9...
data:image/png;base64,iVB...mCC
data:image/png;base64,iVB...g==
data:image/png;base64,iVB...g==

Summary
URL: https://s.sc-cdn.net/hdWNIWeyVxn7zc4S7shL1tbzoyryC_DEGE-Iglp-K0Q=
   /default/media.mp4
Status: 206
Source: Network
Address: 35.227.210.77:443

Request
:method: GET
:scheme: https
:authority: s.sc-cdn.net
:path: /hdWNIWeyVxn7zc4S7shL1tbzoyryC_DEGE-Iglp-K0Q=/default/media.mp
   4
Accept: */*
Connection: Keep-Alive
Range: bytes=0-382849
Host: s.sc-cdn.net
Accept-Language: en-au
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_5) AppleWebKit/605.1
   .15 (KHTML, like Gecko) Version/13.1.1 Safari/605.1.15
Referer: https://s.sc-cdn.net/79UHW7xLGEqGpWrm6z5RulRj3VZ57m_9jSw3XVr
   jYvc=/default/media.jpg?Expires=1603589110&KeyName=test-key&Signatur
   e=wQBY2rBNt7iKKcRv9S7FjKF6GxI=
Accept-Encoding: identity
X-Playback-Session-Id: 785A0CA2-4E18-449D-B12C-7A87918BDCAF

Response
:status: 206
Cache-Control: public, max-age=3600
Accept-Ranges: bytes
Access-Control-Allow-Origin: *
Content-Length: 382850
Date: Mon, 27 Jul 2020 06:07:45 GMT
Expires: Mon, 27 Jul 2020 07:07:45 GMT
Age: 0
Content-Type: video/mp4
ETag: "3e4ab436178f98db55c0860deb62c5a4"
Last-Modified: Mon, 27 Jul 2020 01:25:37 GMT
Content-Range: bytes 0-382849/382850
Server: UploadServer
x-goog-stored-content-encoding: identity
x-goog-generation: 1595813137029960
alt-svc: h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q0
   43=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43"
x-goog-storage-class: MULTI_REGIONAL
x-goog-expiration: Sun, 25 Oct 2020 01:25:37 GMT
x-guploader-uploadid: AAANsUkUsg1nBg_5FYWoNvinYt1o8m9ZH1H-ndNJkUu
   N83bQRGLekvIelKrawOOaudWec-mMkh6_9BHXczlcHKqFaBY
x-goog-stored-content-length: 382850
x-goog-hash: crc32c=fDDHkg==, md5=Pkq0NhePmNtVwIYN62LFpA==
x-goog-metageneration: 1
```

(a)

```
media.jpg

URL: https://s.sc-cdn.net/79UHW7xLGEqGpWrm6z5RulRj3V
   Z57m_9jSw3XVrjYvc=/default/media.jpg?Expires=160358
   9110&KeyName=test-key&Signature=wQBY2rBNt7iKKcRv
   9S7FjKF6GxI=
Status: 304
Source: Network

Request
Accept: text/html,application/xhtml+xml,application/xml;q=0
   .9,*/*;q=0.8
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_5)
   AppleWebKit/605.1.15 (KHTML, like Gecko) Version/13.1.1
   Safari/605.1.15

Response
Last-Modified: Mon, 27 Jul 2020 01:25:10 GMT
Cache-Control: public, max-age=3600
Access-Control-Allow-Origin: *
Date: Mon, 27 Jul 2020 06:06:38 GMT
Content-Length: 0
Expires: Mon, 27 Jul 2020 07:06:38 GMT
ETag: "3afdba706ff2420fc90df736cc202ecf"
Server: UploadServer
x-guploader-uploadid: AAANsUkkuvawaabtSp5sIeXLM3A2N
   IIC9dXvWpsjNS-jp5sFVZZ_Qg-q7JdDVtsTOZuxqaf6dX6C
   g9_cEjOB00BHkYA
alt-svc: h3-Q050=":443"; ma=2592000,h3-Q046=":443";
   ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443
   "; ma=2592000; v="46,43"

Query String Parameters
Expires: 1603589110
KeyName: test-key
Signature: wQBY2rBNt7iKKcRv9S7FjKF6GxI=
```

(b)

Fig. 3. The response received from a POST call to (a) deliver a video and (b) provide an image.

an all wheel drive Honda. Cross referencing the plate to the Minneapolis register via vincheck.info we were able to confirm the plate had been successfully read.

This shows that the system is capable of reading number plates,

Table 3
Snapchat deletion policy.

Snap Item	Deletion Time
After viewed by all recipients	Immediately
Unopened Snaps	30 days
Your Story	24 h
Custom Story	24 Hours
Our Story or public stories	24–48 h +
Location data from Map	40 Days

Table 4
Breakdown of images against surveillance framework.

Criteria	Number	%
Identify Faces	121	40.33
Identify Licence Plates	40	13.33
Identify Clothing	237	79.00
Detect General Activity	291	97.00
Track through a Site	5	1.67
Track Moving Targets	250	83.33
Reviewed	300	

where the quality of the images is sufficient. Given the current trends of smartphone cameras and mobile networks to see increasing quality, it is suspected that this capability will become increasingly commonplace within the next decade. Until then, consumer demand will be satisfied by compressed video which limits the opportunity to read number plates through the system.

5. Limitations

To further answer the question of reliability, we must consult the limitations of our methodology.

5.1. Resolution

The most obvious limitation of Snapchat being used as a distributed surveillance system is the resolution of media obtained off of the service. From our observations we note that this is affected by numerous factors including the quality of the imaging device as well as the compression employed by the system; both on device and on the SNS itself. However, as users increasingly demand high quality media we expect this limitation to resolve itself with time. This is in direct contrast to traditional CCTV systems where the system must be manually updated by the owner. Anecdotally, we are aware of the struggles banks have faced as early adopters of CCTV technology. As the technology has evolved over the last few decades we know the capabilities with respect to definition and resolution has increased significantly. However, many businesses struggle to justify the ongoing expense of updating these systems. As users update their phones typically every 12–24 months we expect a distributed surveillance system to maintain currency with optical resolutions. Indeed, internet network capabilities are also improving to support higher quality media with the advent of 5G networks. Should users of SNS demand higher quality media as a result of these technical innovations, Snapchat would be forced to increase the capabilities of their system to keep market share. Such innovations would in turn resolve the issues of resolution seen in this study.

5.2. Bias

As the dataset was taken during riots and protests, this may have biased our data set against faces being visible. The majority of footage which included people would capture backs rather than faces. Additionally, due to significant facial coverings being employed by people due to the outbreak of coronavirus, faces were mostly covered. To address this further studies were undertaken during the policing of coronavirus restrictions in Adelaide, South Australia.

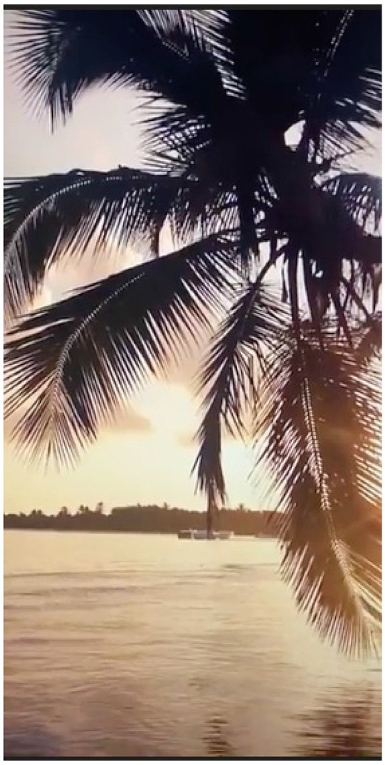


Fig. 4. This video was uploaded to the Snap Map in Adelaide South Australia in the middle of suburbia. There is no location which would correspond to the ocean scene seen. This is an example of disinformation and database poisoning.

As the data obtained in this study is still limited, caution must be given for any automated detection of offences being committed through the use of artificial intelligence or machine learning algorithms. There is a significant risk of over or under fitting.

5.3. Metadata

The map shows snap density corresponding to the number of Snaps uploaded in the location. Dark red corresponds to a high volume, blue is a low number or at least a minimum of one. This heat map scales on demand and is not useful to specify how many snaps have been uploaded in a set location.

When the Snap is uploaded to the map, it is done so with reference to the device location. This accompanying data is saved in the database of the application for recall when polled by the methods indicated above. Should this location data be incorrect at the time of upload, the database is effectively poisoned. This will cause the media to be located incorrectly on the map and render false results from visual analysis. During our investigations, it was noted that the metadata for the location of snaps uploaded to the map was incorrect during times of high volume traffic.

Additionally, an experiment was conducted where a computer screen playing an oasis video was recorded using Snapchat in a location where such an oasis did not exist. This video was then uploaded to the Snap Map without issue (Fig. 4). As a result, the site of the media content was inaccurately referenced to a new location unless observed to be a recording of an existing video.

To counter this issue, media metadata should be verified using traditional forensic methods. Specifically, we believe the analysis of conventional tools such as those which rely on physics, geometry, optics, sensor and pixel techniques in their application to media uploaded to Snapchat is now extended as an open area of future work (Farid, 2016).

5.4. Resources

From 1 June 2020 protests had spread across America and became difficult to monitor. People were asking for attention to be diverted towards different areas across the United States and the globe. By day 5 of the riots (2 June 2020), the behaviour of the protests that had swept across America had become a chaotic system making it increasingly hard to maintain focus on the system as a whole. A key finding, therefore, is to adequately resource this technique to avoid the risk of information explosion. Such methods could include automating the collection and processing stages of this forensic intelligence trace. Methods for exploiting and finally producing reports off of such intelligence are left to the reader.

In all instances, the media extracted from Snapchat's Snap Map provided a single point to pivot for further investigation. This reinforces the finding of Graves et al. (2020) from their analysis of court proceedings where digital evidence from SNSs are rarely used in isolation. Indeed, the processing and verification stage of the intelligence gathering cycle often will rely on open and closed sources of intelligence (Williams and Blum, 2018).

5.5. Technology

This paper has showcased conceptual work into the feasibility of a surveillance system being developed around social media such as Snapchat. While the concept has been proven valid, further work is required to ensure such a system can be developed. As such a system is only as beneficial as the data contained, a surveillance system would need to be built off of multiple sources of data. Snapchat's Snap Map is only one possible source of data to develop a system off of. Indeed, we see this approach in current offerings in the general OSINT marketplace with tools such as OSINT Combine's Nexus Xplore offering an ability to extract information from multiple SNS and catalogue it in a central system. The future of this space is not in the capability enhancement but in the education and adoption of law enforcement and security industries seeing the need to develop shared intelligence resources similar to marketing customer relationship management portals. Until such cross jurisdiction relationships are expanded and enforced, intelligence collection from tools such as Snap Map will be hampered in their effectiveness.

5.6. Availability

While our study has shown data can be extracted from Snapchat, we note that this explicitly requires the media to be uploaded to the platform in the first instance. Events which occur where there are insufficient users of the SNS are unlikely to be captured and uploaded to the service. The system explicitly relies on what users upload and from where they upload it. Likewise, fleeting events are also unlikely to be documented due to users insufficient reaction time. While CCTV is capable of capturing such events due to their permanent nature they suffer from lengthy planning and installation costs required to ensure adequate coverage of an area. We see media availability extracted from SNS complementing traditional CCTV in this manner and not acting as a replacement. Additionally, the current concept requires a reliance on the Snapchat API remaining the same or displaying greater transparency into the future.

6. Conclusion

We have proposed using the SNS Snapchat as a distributed surveillance system. We have explored the accessibility of media from the system and analysed standard policing requirements as identified in the Australia and New Zealand Police Recommendations for CCTV Systems. While our methodology meets many of these conditions proposed in the framework, it is noted that it is still significantly reliant on the interpretation of metadata. The need to verify images and video through traditional media forensic tools is recommended when relying on media for purposes of forensic investigation and intelligence gathering purposes. To effectively scale this method, automation is required to resolve the ongoing issues on information explosion as seen with open source intelligence. Snapchat should be considered by law enforcement and intelligence communities as a viable source for collection.

References

Bay, S., Batrla, M., Twetman, H., 2020. Camouflage for the digital domain. https://www.stratcomcoe.org/camouflage-digital-domain.

Boyd, D.M., Ellison, N.B., 2007. Social network sites: definition, history, and scholarship. J. Computer-Mediated Commun. 13, 210—230.

Cusack, B., Alshaifi, S., 2015. Mining social networking sites for digital evidence. Austr. Digital Forensics Confer. 15—21. https://doi.org/10.4225/75/57b3f23afb885.

Electronic Evidence Specialists Advisory Group (EESAG), 2014. Australia and New Zealand police recommendations for CCTV systems. https://web.archive.org/web/20180319163131/http://www.anzpaa.org.au/ArticleDocuments/220/AustraliaandNewZealandPoliceRecommendationsforCCTVSystems.pdf.aspx.

Epstein, K., 2017. Analysis | thanks to harvey, snapchat's map feature went from being kind of creepy to really useful. https://web.archive.org/web/20170901191540/https://www.washingtonpost.com/news/the-intersect/wp/2017/09/01/thanks-to-harvey-snapchats-map-went-from-being-really-creepy-to-really-useful/. (Accessed 28 July 2020).

Eriksson, P., Nordström, C., Troshin, A., 2019. Surveillance Using Facial Recognition and Social Media Data. Master's thesis. Uppsala Universitet.

Farid, H., 2016. Photo Forensics. MIT press. https://doi.org/10.7551/mitpress/10451.001.0001.

Fried, D., Surdeanu, M., Kobourov, S., Hingle, M., Bell, D., 2014. Analyzing the language of food on social media. In: 2014 IEEE International Conference on Big Data (Big Data). IEEE, pp. 778—783. https://doi.org/10.1109/BigData.2014.7004305.

Frizell, S., 2014. Tinder security flaw exposed users' locations | time. https://web.archive.org/web/20140307225523/https://time.com/8604/tinder-app-user-location-security-flaw/. (Accessed 29 July 2020).

a Google. Http headers and query string parameters for xml api | cloud storage. https://web.archive.org/web/20191123005515/https://cloud.google.com/storage/docs/xml-api/reference-headers. (Accessed 28 July 2020).

b Google. Signed urls | cloud storage | google cloud. https://web.archive.org/web/20200728012639/https://cloud.google.com/storage/docs/access-control/signed-urls. (Accessed 28 July 2020).

c Google. Signed urls and signed cookies overview | cloud cdn | google cloud. https://web.archive.org/web/20200728012627/https://cloud.google.com/cdn/docs/private-content. (Accessed 28 July 2020).

Graves, L., Glisson, W.B., Choo, K.K.R., 2020. Linkedlegal: investigating social media as evidence in courtrooms. Comput. Law Secur. Rep. 38, 105408. https://doi.org/10.1016/j.clsr.2020.105408. http://www.sciencedirect.com/science/article/pii/S0267364920300133.

Hamby, P., 2017. Watching Trump on Snapchat Map You Can Actually See How Far He Is from the Modest Crowd Gathered on the Street pic.twitter.Com/etzsw6-lizp. https://web.archive.org/web/20170830074128/https://twitter.com/peterhamby/status/902593369729376256. (Accessed 28 July 2020).

Huber, M., Mulazzani, M., Leithner, M., Schrittwieser, S., Wondracek, G., Weippl, E., 2011. Social snapshots: digital forensics for online social networks. In: Proceedings of the 27th Annual Computer Security Applications Conference, pp. 113—122. https://doi.org/10.1145/2076732.2076748.

Jalal, M., Wang, K., Jefferson, S., Zheng, Y., Nsoesie, E.O., Betke, M., 2019. Scraping social media photos posted in Kenya and elsewhere to detect and analyze food types. In: Proceedings of the 5th International Workshop on Multimedia Assisted Dietary Management. Association for Computing Machinery, New York, NY, USA, pp. 50—59. https://doi.org/10.1145/3347448.3357170, 10.1145/3347448.3357170.

Jang, Y.J., Kwak, J., 2015. Digital forensics investigation methodology applicable for social network services. Multimed. Tool. Appl. 74, 5029—5040. https://doi.org/10.1007/s11042-014-2061-8.

Lovell, K., Heering, D., 2019. Exercise neptune: maritime cybersecurity training using the navigational simulators. In: Proceedings of the 5th Interdisciplinary Cyber Research Conference 2019. Tallinn University of Technology, Tallinn, Estonia, pp. 34–37. https://old.taltech.ee/public/t/tarkvarateaduse-instituut/CRW_2019/mobile/index.html#p=36.

Mejova, Y., Haddadi, H., Noulas, A., Weber, I., 2015. Foodporn: obesity patterns in culinary interactions. In: Proceedings of the 5th International Conference on Digital Health 2015, pp. 51–58. https://doi.org/10.1145/2750511.2750524.

Sharma, S.S., De Choudhury, M., 2015. Measuring and characterizing nutritional information of food and ingestion content in instagram. In: Proceedings of the 24th International Conference on World Wide Web. Association for Computing Machinery, New York, NY, USA, pp. 115–116. https://doi.org/10.1145/2740908.2742754, 10.1145/2740908.2742754.

Snapchat. When are snaps chats deleted. https://app.cappture.cc/snapshots/1ead0715-efaf-69ba-b100-0ea9b2ae1df4. (Accessed 28 July 2020).

Spieler, B., Batte, C., Mackey, D., Henry, C., Danrad, R., Sabottke, C., Pirtle, C., Mussell, J., Wallace, E., 2020. Diagnosis in a snap: a pilot study using snapchat in radiologic didactics. Emerg. Radiol. https://doi.org/10.1007/s10140-020-01825-x, 10.1007/s10140-020-01825-x.

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 28 July 2020).

Tsvetkova, M., 2015. Russian soldiers geolocated by photos in multiple Syria locations, bloggers say. https://web.archive.org/web/20151111031342/http://www.reuters.com/article/2015/11/08/us-mideast-crisis-syria-russia-idUSKCN0SX0H820151108. (Accessed 28 July 2020).

Williams, H.J., Blum, I., 2018. Defining Second Generation Open Source Intelligence for the Defence Enterprise. RAND Corporation. https://doi.org/10.7249/RR1964.