Forensic Science International: Reports 8 (2023) 100346



Contents lists available at ScienceDirect

Forensic Science International: Reports

journal homepage: www.sciencedirect.com/journal/forensic-science-international-reports



Digital Forensics

# Identifying fake vs. real communication records: A case study



Graeme Horsman [1]

*Cranfield Forensic Institute Cranfield University, United Kingdom*

ARTICLE INFO

*Keywords:*
Digital forensics
Communication records
Messages
Investigation
Law enforcement

ABSTRACT

Records of communication often play an important role in many criminal inquiries giving insight into existing and alleged relationships. The forensic analysis of digital devices can provide such information, however in some cases, screen captured records may be all that is available. In these instances, it is necessary to evaluate the authenticity of this information given the availability of free to use communication record mockup services that can be used to create realistic looking, but fictitious communication records. This work seeks to ascertain whether freely available communication record mockup services pose a threat to law enforcement officers in terms of not being able to distinguish a communication record mockup from a genuine communication record screen capture. An evaluation of communication record mockup services for creating WhatsApp, iMessage and Twitter mockups are identified and their ability to create realistic communication record mockups is evaluated. The results of these tests are provided and discussed, and 41 communication record mockups are supplied forming one of the first datasets to support those conducting communication record authenticity checks.

## 1. Introduction

Records of communication are often relevant to many criminal inquiries [1] as they provide information about, and insight into existing and alleged relationships. We may think of communication records (CRs) as call logs and SMS messages, however social media platforms and web services have now diversified the ways in which individuals can liaise. While this has led to many positive societal impacts, consequently, such platforms have also been used to bully, troll, virtual mob, distribute unlawful content and to maliciously converse [2]. Those tasked with investigating such incidents may seek to rely upon the content that any communications between parties contain in order to progress their inquiries, and in some cases, the records themselves may constitute an offence. Given the impact that CRs can have on an investigation and all parties involved, it is important that their authenticity is validated [3] and whilst this may seem obvious, this should be done in all cases in order to determine that any record of a 'communication event' is real and that they can be relied upon. However, in some cases the possibility of 'non-authentic' communication records may not even be considered.

In some cases, CRs can be acquired through the forensic acquisition and examination of an individual's digital device. Alternatively, service providers may be contacted in order to acquire and review any logs they maintain in regards to how specific accounts have behaved on their platforms [4]. Both these methods can provide metadata that can be used to support the authentication of the sending/receiving of information between parties, however, in some cases law enforcement officers may receive records of communication through more informal methods. This can often include parties subject to an inquiry supplying 'screen captures' (a screen capture (sometimes referred to as a screenshot) 'is a photo capture of what you currently see on the screen of your device' [3]) of messages which they consider to be of relevance [5–9]. Olliers Solicitors [10] state that 'screenshots of digital messages are regularly served as evidence in criminal cases [11], usually to support allegations like harassment and malicious communications'. In turn, police forces advise potential victims to consider screen capturing content to preserve evidence of communications [7–9].

Where screen captures are provided, determining the legitimacy of the CR is arguably more difficult given the ease in which they can be faked [12]. This is arguably of concern given that screen captures of CRs, particularly showing text messages are reported as a relatively common occurrence in investigations [13], and in some cases the need to even check may be overlooked. Whilst at first glance, any concerns around the screen captured CRs may seem trivial, there are a number of freely available web-based and application services that can be used to create 'communication record mockups' (CRMs) which can be found via simple web searches [13]. A CRM is a false CR, constructed in a way that attempts to make it look realistic. A CRM service typically seeks to allow

*E-mail address:* graeme.horsman@cranfield.ac.uk.
[1] ORCID: 0000-0002-0685-0650

https://doi.org/10.1016/j.fsir.2023.100346
Received 15 July 2023; Received in revised form 16 November 2023; Accepted 18 November 2023
Available online 1 December 2023
2665-9107/© 2023 Published by Elsevier B.V. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).




**Fig. 1.** The master CR created in WhatsApp version 2.23.5.78 on iOS.

users to construct fake conversations, and then place these into a mock user interface of the application or service they are trying to recreate - i.e. a user could create a CRM of a Whatsapp chat. It should be noted that many CRM services highlight that their use should be limited to 'pranks' (see for example 'WhatsApp Fake Chat' at https://www.fakewhats.com/generator), however, their use can be deployed in more malicious circumstances.

When screen captured CRs are supplied, often an evaluation of their authenticity may be limited to visual checks as any underlying metadata may not be available. Arguably, this potentially increases the chance of any law enforcement officer failing to detect a fake. This work seeks to ascertain whether freely available CRM services pose a threat to law enforcement officers in terms of not being able to distinguish a CRM from a genuine CR screen capture. An evaluation of CRM services for creating Whatsapp, iMessage and Twitter mockups are identified and their ability to create realistic CRMs is evaluated. The results of these tests are provided and discussed, and 41 CRMs are supplied forming one of the first datasets to support those conducting CRM authenticity checks.

## 2. Screen captured communication records

From a forensic perspective, the analysis of any device that has sent/received any communication provides arguably greater reassurance of

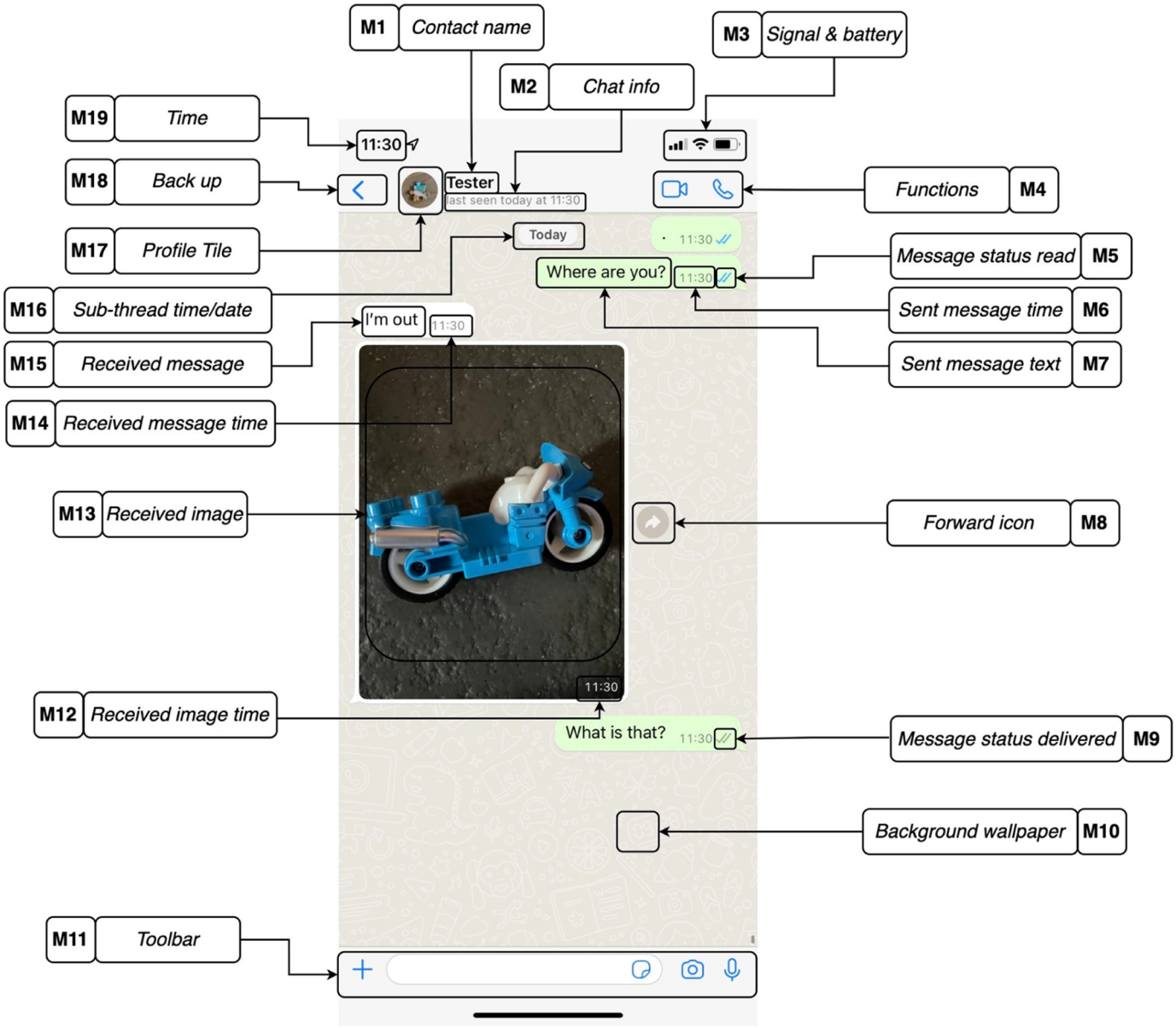



**Fig. 2.** WhatsApp CR markup on iOS showing 19 'marks' for authentication.

**Table 1**
iOS CRMs and the results of a visual authenticity evaluation.

| *Type* | *Source* | *Screen Capture ID* | *M1* | *M2* | *M3* | *M4* | *M5* | *M6* | *M7* | *M8* | *M9* | *M10* | *M11* | *M12* | *M13* | *M14* | *M15* | *M16* | *M17* | *M18* | *M19* | *Total Score* | *Percentage Match* | *Percentage Match (excluding OS artefacts)* |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Web | https://www.fakewhats.com/generator | W1 | 0.5 | 0.5 | 0.5 | 0 | 1 | 1 | 0.5 | 0 | 1 | 0.5 | 0.5 | 0 | 1 | 0.5 | 1 | 0 | 0.5 | 0.5 | 0.5 | 10 | 52.63% | 52.94% |
| Web | https://fakedetail.com/fake-whatsapp-chat-generator | W2 | 1 | 0.5 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 0.5 | 1 | 1 | 1 | 1 | 1 | 0.5 | 1 | 1 | 0 | 14.5 | 76.32% | 85.29% |
| Web | https://fakeinfo.net/fake-whatsapp-chat-generator | W3 | 0.5 | 0.5 | 0.5 | 1 | 1 | 1 | 1 | 0 | 1 | 0.5 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 0.5 | 12.5 | 65.79% | 67.65% |
| Web | https://zeoob.com/generate-whatsapp-chat/ | W4 | 1 | 0.5 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 0.5 | 1 | 1 | 1 | 1 | 1 | 0.5 | 1 | 1 | 0 | 14.5 | 76.32% | 85.29% |
| Web | https://www.wofox.com/ui-editing-tools/whatsapp-chat-mockup | W5 | 1 | 0.5 | 0 | 0.5 | 1 | 1 | 1 | 0 | 1 | 0.5 | 1 | 0.5 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 13 | 68.42% | 76.47% |
| Web | https://dizwa.com/simulators/generate-whatsapp-chat/ | W6 | 0.5 | 0.5 | 0 | 1 | 1 | 0.5 | 0.5 | 0 | 1 | 0.5 | 1 | 0.5 | 1 | 0.5 | 0.5 | 0.5 | 0.5 | 0.5 | 0 | 10.5 | 55.26% | 61.76% |
| App iOS | Fake W-Prank Funny App V1.2 | W7 | 0.5 | 0.5 | 0 | 0.5 | 1 | 1 | 0.5 | 0 | 0 | 0.5 | 0.5 | 1 | 1 | 1 | 0.5 | 0 | 0.5 | 0.5 | 0 | 9.5 | 50.00% | 55.88% |
| App iOS | WhatsUp Prank Chat | W8 | 0.5 | 0 | 0 | 0.5 | 0 | 0.5 | 1 | 0 | 0 | 0.5 | 0.5 | 1 | 1 | 1 | 1 | 0 | 0.5 | 0.5 | 0 | 8.5 | 44.74% | 50.00% |
| App iOS | Prank | W9 | 0.5 | 0 | 0 | 0.5 | 1 | 0 | 1 | 0 | 0 | 0 | 0.5 | 1 | 1 | 1 | 1 | 0 | 0.5 | 0.5 | 0 | 8.5 | 44.74% | 50.00% |




**Fig. 3.** Service 'https://www.fakewhats.com/generator' - W1.

the legitimacy of any communication alleged to have taken place. However, there are circumstances when achieving this may not be possible and the provision of a screen capture may be the only viable option. An individual may screen capture a CR where the prolonged existence of it cannot be guaranteed, or where other parties may be in a position to delete/edit it at any point [7]. Examples include messaging services that allow those who send a message but have the option to subsequently delete it for all parties subject to a conversation at any point (a feature offered by Whatsapp), or if content has been placed on a social media network [14,15]. In addition, in some cases it may not be viable for law enforcement to obtain a device where a CR is stored and




**Fig. 4.** Service 'https://fakedetail.com/fake-whatsapp-chat-generator' - W2.




**Fig. 5.** Service 'https://fakeinfo.net/fake-whatsapp-chat-generator' - W3.

acquire it using forensic methods as a device owner may not wish to provide access to it, or in the case of victim specific offences, there may be a reluctance to take the phone out of their possession for a period of time [10].

Determining the authenticity of a screen captured CR can be difficult, where if the original screen capture file can be accessed, internal file metadata may offer some limited information about the origin of it and how it was taken [13]. However, depending on how a law enforcement official received the screen capture file, such internal metadata may have been removed or altered either by the sender, or the service used to transfer the file. In some cases, when screen captured CRs are received, authenticity checks can be limited to a visual inspection.

### 2.1. *Visual authentication*

It is important to detect CRMs as soon as possible in the investigatory process in order to prevent wrongful allegations from persisting and to prevent time and resources being wasted. In relation to incidents involving relevant CRs, disputes may arise between parties as to the contents of any communications sent, or that communications have even been sent at all. In some cases, addressing this issue may be straightforward, where digital records of any communication thread may be acquired from a relevant party's device, or a communication service provider. However, in others, CRs may be deleted by either party (for example, maintaining any message/communication may cause distress to a party so they delete it) or the device used to facilitate communication may no longer be available for interrogation. In such cases, inquiries may be limited to screen captures of relevant CRs. Where screen captured CRs are supplied, determining their authenticity can be limited to a visual inspection of the elements within it, yet to undertake this process first requires acknowledgment of the need to do this and that the generation of fake CRs is a possibility. In addition, under the pressures of their role, law enforcement officers may find themselves needing to make decisions on the validity of such information quickly, limiting the




**Fig. 6.** Service 'https://zeoob.com/generate-whatsapp-chat/' - W4.




**Fig. 7.** Service 'https://www.wofox.com/ui-editing-tools/whatsapp-chat-mockup' - W5.

depth of any review of the CR screen capture. Finally, conducting a successful review requires understanding the characteristics of real communication platform interfaces and being able to determine when such traits are not present in any given CR screen capture. This presents a challenge for two reasons, first, the number of platforms that communication can take place on meaning a wide range of differing interfaces, and second, the intricacies involved in determining when a CRM may have failed to accurately recreate the communication platform interface.

## 3. Methodology

This work provides an evaluation of three CRM services in order to try and address whether they pose a risk to law enforcement in regards to being able to detect fake CRs. These services include Whatsapp, iMessage and Twitter. The following methodological steps have been taken.

1. A master CR for each service has been produced on a test device containing some of the core communication actions (sent and received messages etc.) and a screen capture created.
2. Following a review of the master CR, a markup of it is then created to identify 'marks' within the interface that could be used to authenticate a potential fake CR screen capture. These marks include artefacts in the service's graphical user interface which appear as standard (for example, standard patterns wallpaper that a service uses, or validation 'ticks' seen with WhatsApp messages).
3. Freely available CRM services are identified and a fake CR which attempts to match the appropriate content within the master CR is created using each service.
4. A visual authenticity evaluation using the 'marks' flagged in the master CR markup is undertaken for each CRM service in order to identify how each service compares when attempting to create a realistic looking fake CR screen capture.




**Fig. 8.** Service 'https://dizwa.com/simulators/generate-whatsapp-chat/' - W6.

a. This work justifies a visual inspection based approach as this may be found to be the only way that law enforcement officers can authenticate CR screen captures they receive or see.
b. Each CRM service screen capture will be evaluated against the master CR markup and scores given as follows:

i. 1 point will be given if the CRM service can accurately (to the eye) create a mark that correctly represents the same region or artefact in the legitimate service.

1. This includes a combination of factors including colour, size, type and location.

i. 0 points will be awarded if the CRM service is unable to create a mark that is present in the legitimate service.
ii. 0.5 points will be awarded if the CRM service fails to accurately (to the eye) create a mark that correctly represents the same region or artefact in the legitimate service, but it is present in some shape or form.




**Fig. 9.** Service 'Fake W-Prank Funny App V1.2' - W7.

*To note:- It is recognised that visual inspections of this type an element of subjectivity in terms of making scoring decisions, therefore so far as possible the same principles have been applied in every case. All images and scores are available for inspection.

CRM services were identified via the Google search engine, Apple's App Store and Google's Play Store, using the search terms '*fake <service> chat creator*', '*fake <service> message*' and '*fake <service> post*'.

To start the analysis, WhatsApp is evaluated first.

### 3.1. WhatsApp

WhatsApp is reported to have 'approximately two billion monthly active users' and be the most popular messaging App available [16]. As result, it is argued that where CRs are pertinent to an inquiry, the WhatsApp platform may likely be encountered by investigative teams. At the time of this work, WhatsApp version 2.23.5.78 on iOS and version 2.23.4.79 on Android were evaluated. Whilst WhatsApp does offer their

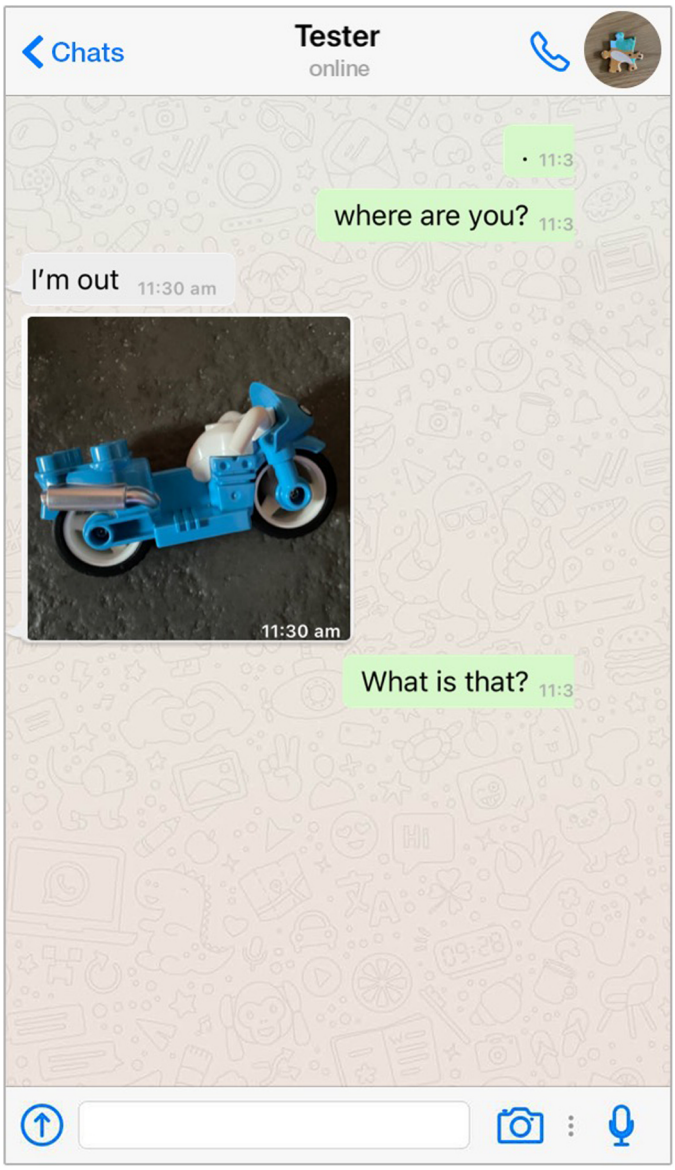



**Fig. 10.** Service 'WhatsUp Prank Chat' - W8.

users the ability to configure their messaging interface with bespoke backgrounds, given the potentially infinite number of possible configurations, this work has opted to maintain the default visual interface presented to the user when the application is first installed on both iOS and Android.

### 3.1.1. *WhatsApp iOS CRMs*

Shown in Fig. 1, a master CR has been created using WhatsApp's default visual setup. The conversation has been configured to be with a contact named 'Tester' and their avatar image has been set. Three messages are sent, and two received - one of which being an image.

From an analysis of the master CR shown in Fig. 1, a markup has been created that highlights 19 'marks' within a real WhatsApp CR screen capture that could be used to conduct a visual authentication of any WhatsApp CR screen capture they receive. These 19 marks are as follows:

M1:- Contact name, font and colour.
M2:- Chat information, font and colour.
M3:- Signal & battery symbols.
M4:- Video & audio call functions.




**Fig. 11.** Service 'Prank' - W9.

M5:- Message status 'read' symbol and colour.
M6:- Sent message time, font and colour.
M7:- Sent message text, font and colour.
M8:- Forward icon
M9:- Message status 'delivered' symbol and colour.
M10:- Background wallpaper.
M11:- Message toolbar and icons.
M12:- Received image time.
M13:- Received image.
M14:- Received message time.

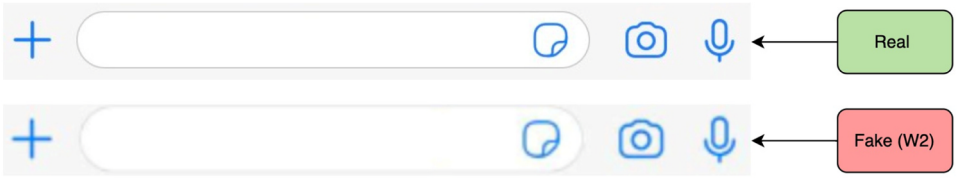



**Fig. 12.** A comparison of a real message toolbar (mark M11) and a fake one (shown from screen capture W2).

M15:- Received message.
M16:- Sub-thread time/date.
M17:- Contact avatar.
M18:- Backup icon.
M19:- Time.

All 19 identifying marks for WhatsApp are shown in Fig. 2:

Searches conducted via Google, and on the AppStore and PlayStore led to the identification of nine CRM services (noted in Section 3.1.2) and attempts were made to recreate this CR using CRM services.

*3.1.2. Results*

Table 1 provides the results of a visual authenticity evaluation of CRMs created by nine CRM services where the source of each CRM service is noted (either URL or App name) and each screen capture is provided an identifier (W#). Each service was used to create a CRM that visually matches the master CR shown in Fig. 1 as closely as possible using the service's settings and capabilities. Once created, the author conducted a visual authenticity evaluation to assess each of the 19 marks in the original master CR against each CRM service's ability to replicate these in any generated fake CR. As part of this evaluation, the scoring methodology set out in Section 3 was applied, and the results are shown in Table 1.




**Fig. 13.** The master CR created in WhatsApp version 2.23.4.79 on Android.

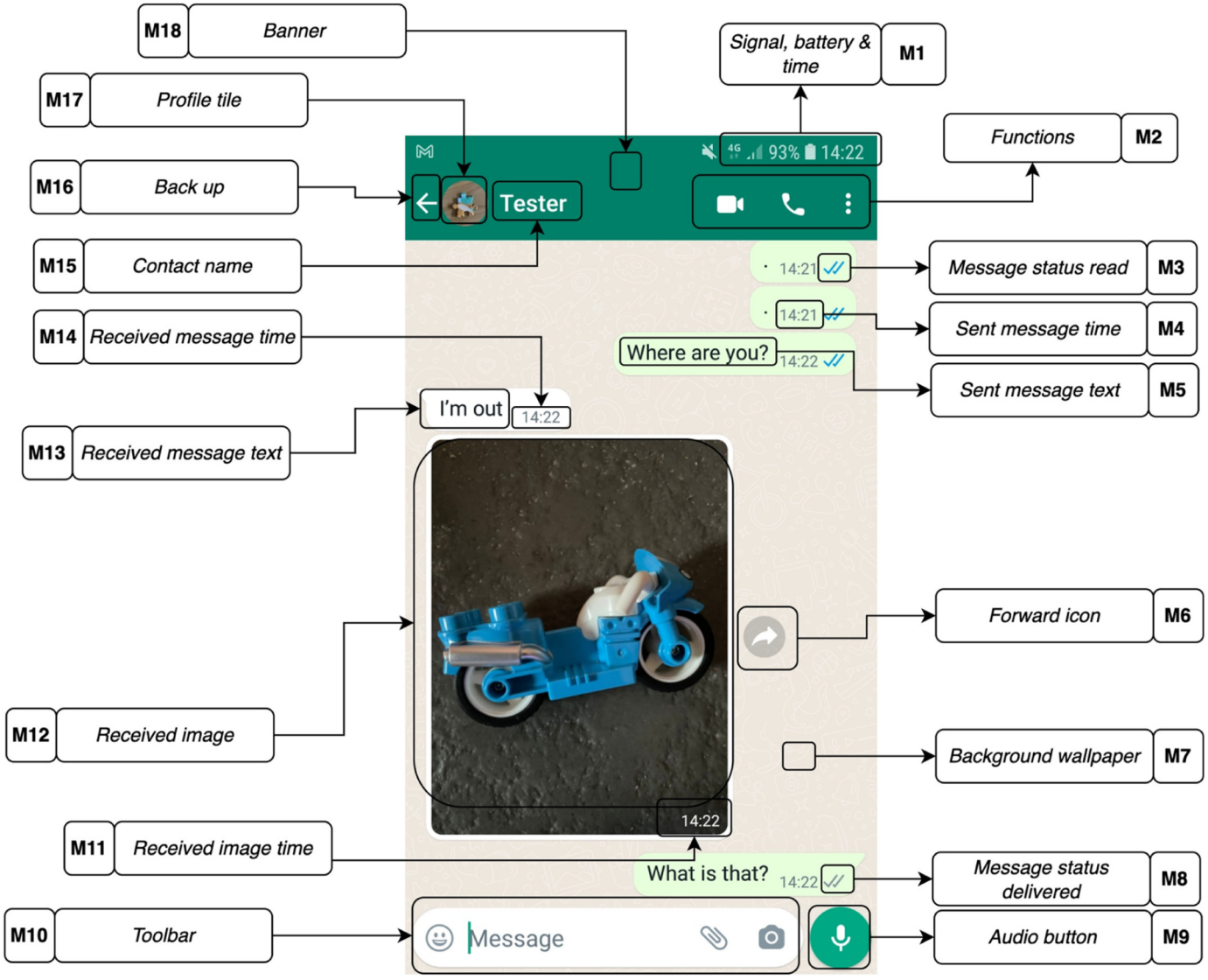



**Fig. 14.** WhatsApp CR markup on Android showing 18 'marks' for authentication.

**Table 2**
Android CRMs and the results of a visual authenticity evaluation.

| *Type* | *Source* | *Screen Capture ID* | *M1* | *M2* | *M3* | *M4* | *M5* | *M6* | *M7* | *M8* | *M9* | *M10* | *M11* | *M12* | *M13* | *M14* | *M15* | *M16* | *M17* | *M18* | *Total Score* | *Percentage match* | *Percentage Match (excluding OS artefacts)* |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Web | https://www.fakechatapp.com/ | W1_Android | 0 | 0.5 | 1 | 1 | 0.5 | 0 | 0.5 | 1 | 0 | 0.5 | 1 | 1 | 0.5 | 1 | 0.5 | 0 | 0.5 | 0 | 9.5 | 52.78% | 55.88% |
| Web | https://fakedetail.com/fake-whatsapp-chat-generator | W2_Android | 0 | 1 | 1 | 1 | 1 | 0 | 0.5 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 0.5 | 1 | 1 | 1 | 14 | 77.78% | 82.35% |
| Web | https://fakeinfo.net/fake-whatsapp-chat-generator | W3_Android | 0.5 | 1 | 1 | 1 | 1 | 0 | 0.5 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 0.5 | 1 | 1 | 1 | 13.5 | 75% | 76.47% |
| Web | https://zeoob.com/generate-whatsapp-chat/ | W4_Android | 0 | 1 | 1 | 1 | 1 | 0 | 0.5 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0.5 | 1 | 1 | 1 | 15 | 83.33% | 88.24% |
| Web | https://www.oflox.com/demo/wpfake/index.php | W5_Android | 0.5 | 1 | 1 | 1 | 1 | 0 | 0.5 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0.5 | 1 | 1 | 1 | 12.5 | 69.44% | 70.59% |
| Web | https://www.wofox.com/ui-editing-tools/whatsapp-chat-mockup | W6_Android | 0 | 1 | 1 | 1 | 1 | 0 | 0.5 | 1 | 1 | 0.5 | 1 | 1 | 1 | 1 | 0.5 | 1 | 1 | 1 | 14.5 | 80.56% | 85.29% |
| Web | https://www.fakewhatsapchat.com/ | W7_Android | 0.5 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 0.5 | 0 | 0 | 1 | 1 | 0.5 | 1 | 1 | 1 | 11.5 | 63.89% | 64.71% |
| Web | https://dizwa.com/simulators/generate-whatsapp-chat/ | W8_Android | 0 | 1 | 1 | 1 | 0.5 | 0 | 0.5 | 1 | 1 | 1 | 1 | 1 | 0.5 | 1 | 0.5 | 1 | 0.5 | 1 | 13.5 | 75% | 79.41% |
| Web | https://pranx.com/chat-screenshot/ | W9_Android | 0.5 | 0 | 0 | 0 | 0.5 | 0 | 0 | 0 | 0 | 0.5 | 0 | 1 | 0.5 | 0 | 0 | 1 | 0 | 1 | 5 | 27.78% | 26.47% |
| App iOS | Whatspoof fake chat | W10_Android | 0.5 | 0.5 | 0.5 | 0.5 | 0.5 | 0 | 0.5 | 0 | 0 | 0.5 | 0.5 | 1 | 0.5 | 0.5 | 0.5 | 0.5 | 0.5 | 1 | 8.5 | 47.22% | 50.00% |
| App Android | Fake Chat Whats Mock Text Prank | W11_Android | 0.5 | 1 | 1 | 1 | 1 | 1 | 0.5 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0.5 | 1 | 1 | 1 | 16.5 | 91.67% | 94.12% |
| App Android | Fake Chat Maker - WhatsMessage | W12_Android | 0.5 | 1 | 1 | 1 | 1 | 0 | 0.5 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0.5 | 1 | 1 | 1 | 15.5 | 86.11% | 88.24% |
| App Android | WhatsFake - Fake Chat Maker | W13_Android | 0.5 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0.5 | 1 | 1 | 1 | 16 | 88.89% | 91.18% |
| App Android | Fake Whatsp Chat, Call, Status | W14_Android | 0.5 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0.5 | 1 | 1 | 1 | 17 | 94.44% | 97.01% |




**Fig. 15.** Service 'https://www.fakechatapp.com/' -W1_Android.




**Fig. 16.** Service 'https://fakedetail.com/fake-whatsapp-chat-generator' -W2_Android.

As it is possible for users to crop any CRMs so that operating specific artefacts (battery icons, network provider names etc.) are excluded, an additional percentage match score for each service has been provided which excludes matching for operating specific artefacts.

All CRM service screen captures (W1-W9) are provided in Figs. 3–11.

### 3.1.3. *Discussion*

The first important point to note is that no CRM services are capable of accurately and completely recreating the master CR noted in Fig. 1, therefore in all cases, there are potentially elements that are available that visually indicate that a screen capture is fake. It is important to stress that this is a 'potential' as there are elements that could be cropped out of a screen capture through cropping that may remove the chance to raise suspicions. For example, a user may crop a screen capture so that the elements M3 (signal and battery icons), M11 (message toolbar) and M19 (system time) are not present, and suspicions may not be raised as these parts of the capture do not contain any of the conversation - likely to be the main part of interest to law enforcement. However, specifically in regards to M3 and M19, only two of their services were able to partially replicate these elements (with a score of 0.5). All services made an attempt to replicate M11, however only 5 were considered to be effective (scoring 1).

The web services 'https://fakedetail.com/fake-whatsapp-chat-generator' and 'https://zeoob.com/generate-whatsapp-chat/' were considered to produce the most realistic CRMs with a joint percentage match score of 76.32%. In contrast, the applications 'WhatsUp Prank Chat' and 'Prank' were considered to produce the least visually authentic CR screen captures, jointly scoring 44.74%.

### 3.1.4. **Important - the visual authenticity evaluation process*

It is important to note that the visual authenticity evaluation that has




**Fig. 17.** Service 'https://fakeinfo.net/fake-whatsapp-chat-generator' - W3_Android.




**Fig. 18.** Service 'https://zeoob.com/generate-whatsapp-chat/' - W4_Android.

taken place, does so with an element of flexibility and leniency. To explain what is meant by this, we must consider the operational environment that visual authenticity checks are likely to be conducted in, where law enforcement officers are under pressure and often subject to time pressures. Therefore it is suggested that the level of visual scrutiny that is likely to be applied by officers (particularly if they do not realise the potential for screen captures to be fakes) may be lower than in laboratory environments where officers might be briefed specifically to detect fake records. It is that scenario that this work wants to consider here, as it attempts to evaluate the risk of fake CR screen captures being considered real. Therefore a strict visual evaluation may be considered unrealistic in terms of what may be being faced in real life.

To provide an example, consider Fig. 12 which shows a comparison of a real message toolbar (mark M11) and a fake one (shown from screen capture W2). As part of the visual authenticity evaluation process, this was considered to be a mark that was correctly replicated by the CRM service (scoring 1 point), yet when considered in isolation and outside of the full image, it is arguably clearer that the two images are not matching. For instance, the fake screen capture is less sharp, and variances in colour are clearly visible. However, it is considered that the faked toolbar is close enough in likeness that law enforcement officers that are under pressure may consider it to be legitimate. For this reason, similar levels of leniency and flexibility are applied during the visual authenticity evaluation process so that the threat posed by CRM services can be considered in the context of an operational environment. This approach is taken with all visual authenticity evaluation processes undertaken in this work.

### 3.2. *WhatsApp Android CRMs*

As with iOS shown in Fig. 1, a master CR has been created using WhatsApp's default visual setup on Android version 2.23.4.79. The conversation has been configured to be with a person named 'Tester' and their avatar image has been set. Four messages are sent, and two received - one of which being an image. This is shown in Fig. 13.

From an analysis of the master CR shown in Fig. 13, a markup has been created that highlights 18 'marks' within a real WhatsApp CR




**Fig. 19.** Service 'https://www.oflox.com/demo/wpfake/index.php' - W5_Android.




**Fig. 20.** Service 'https://www.wofox.com/ui-editing-tools/whatsapp-chat-mockup' - W6_Android.

screen capture that could be used to conduct a visual authentication of any WhatsApp CR screen capture they receive from an Android platform. These 18 marks are as follows and are shown visually in Fig. 14:

M1:- Signal, battery and time symbols.
M2:- Video & audio call functions.
M3:- Message status 'read' symbol and colour.
M4:- Sent message time, font and colour.
M5:- Sent message text, font and colour.
M6:- Forward icon
M7:- Background wallpaper.
M8:- Message status 'delivered' symbol and colour.
M9:- Audio button symbol and colour.
M10:- Message toolbar and icons.
M11:- Received image time.
M12:- Received image.
M13:- Received message.
M14:- Received message time.
M15:- Contact name.
M16:- Backup icon.
M17:- Contact avatar.
M18:- Banner

Searches conducted via Google, and on the AppStore and PlayStore led to the identification of 14 CRM services (noted in Section 3.1.2) and attempts were made to recreate this CR using CRM services.

### 3.2.1. *Results*

As with iOS, Table 2 provides the results of a visual authenticity evaluation of CRMs created by the 14 CRM services where the source of each CRM service is noted (either URL or App name) and each screen capture is provided an identifier (W#_Android). Each service was used to create a CRM that visually matches the master CR shown in Fig. 13 as closely as possible using the service's settings and capabilities. Once created, the author conducted a visual authenticity evaluation to assess each of the 18 marks in the original master CR against each CRM service's ability to replicate these in any generated fake CR. As part of this

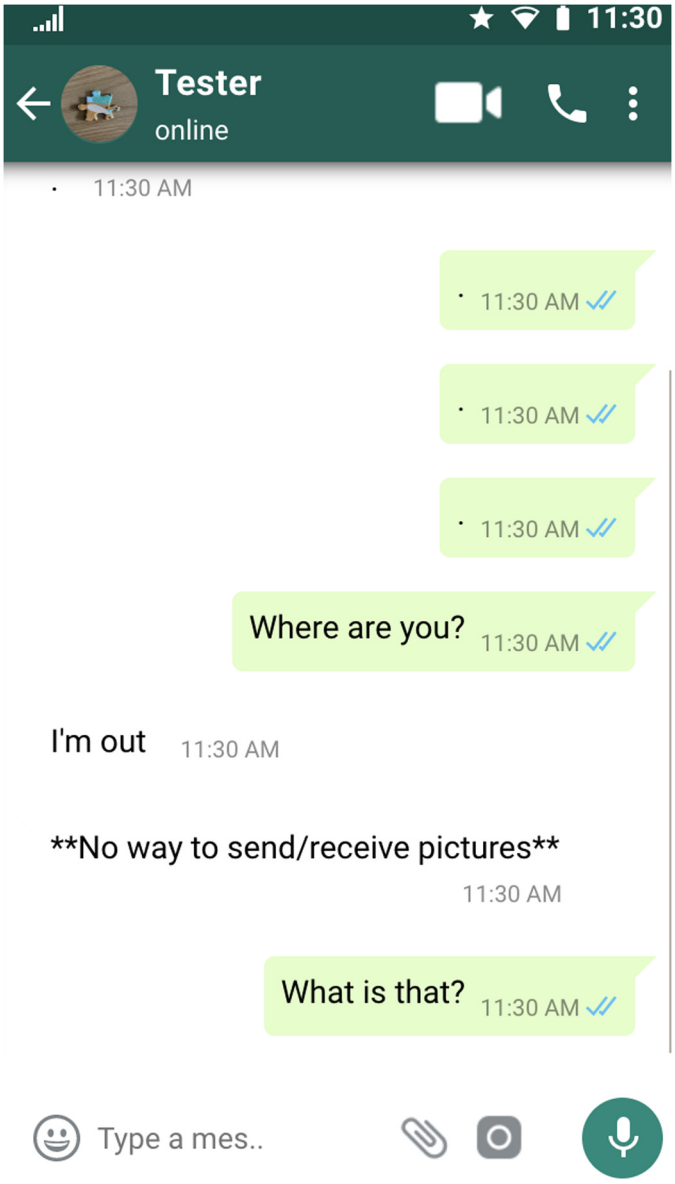



**Fig. 21.** Service 'https://www.fakewhatsapchat.com/' - W7_Android.




**Fig. 22.** Service 'https://dizwa.com/simulators/generate-whatsapp-chat/' - W8_Android.

evaluation, the scoring methodology set out in Section 3 was applied, and the results are shown in Table 2.

As it is possible for users to crop any CRMs so that operating specific artefacts (battery icons, network provider names etc.) are excluded, an additional percentage match score for each service has been provided which excludes matching for operating specific artefacts.

All 14 CRM service screen captures (W1_Android - W14_Android) are provided in Figs. 15–28.

### 3.2.2. *Discussion*

As with the replication of WhatsApp on iOS, none of the 14 CRM services were considered capable of replicating WhatsApp on Android with 100% accuracy (shown in Fig. 13) in accordance with this work's visual authenticity evaluation principles. The Android application '*Fake Whatsp Chat, Call, Status*' was considered to produce the most realistic CRM with a percentage match score of 94.44%. In contrast, the web service 'https://pranx.com/chat-screenshot/' was considered to produce the least visually authentic CR screen capture, scoring 27.78%.

In some cases, the CRM services provided difficulty in creating a chronological conversation, see for example W14_Android, where once timestamps are manually set on each message, their ordering is difficult to control (shown in this screen capture as receiving a message, before any are sent). Therefore in screen captures that show out of sync conversations, it is due to difficulties in organising the order of messages. The implications of this are that anyone trying to mock-up a conversation would need to ensure that messages are set with timestamps that are minutes apart to allow for a correct flow of conversation.

## 3.3. *WhatsApp concluding points*

The WhatsApp CRM services are considered to provide a mix of quality in terms of their ability to produce CRM screen captures, however through trial and error, it is viable for an individual to identify free services that can produce near accurate mock ups. It is also important to note that these services tend to fail in the replication of minor details contained within the WhatsApp interface (such as battery/settings info and artefact position/colour). In most cases, replication of the general




**Fig. 23.** Service 'https://pranx.com/chat-screenshot/' - W9_Android.




**Fig. 24.** Service 'Whatspoof fake chat' - W10_Android.

substance of what would be expected in a WhatsApp CR (i.e. the conversation/messages) is achieved. As a result, it is suggested that the danger of failing to detect a fake CR lies with a law enforcement officer focusing on the communication substance of a CR screen capture, but not looking beyond it for markers of 'fakeness'. In most cases, a CRM screen capture can be identified via an analysis of the background wallpaper shown in the screen capture as this appears to be difficult for services to replicate. However, WhatsApp does allow users to change their wallpaper, therefore in some cases, it may not be possible to rely on this as a mark of fakeness. In addition, some CRM services do offer the ability for users to upload a bespoke background for their screen capture, however due to the potential endless configuration possibilities, this was not explored.

If we arbitrarily consider CRM services to be effective if they can replicate 75% of the marks identified in both of the master images for iOS and Android, then there are two effective services available for iOS CRMs and eight for Android CRMs.

## 4. iOS Message

On iOS devices, users have the ability to send messages via standard




**Fig. 25.** Service 'Fake Chat Whats Mock Text Prank' - W11_Android.

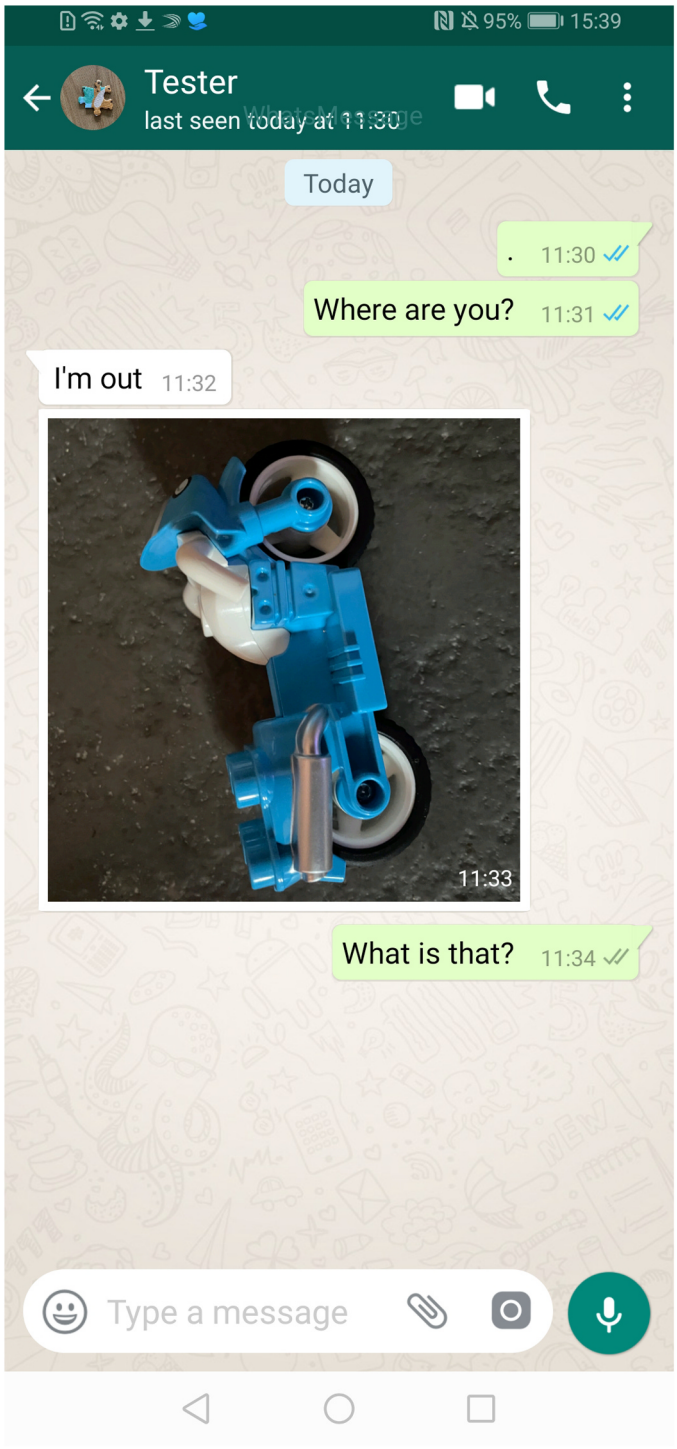



**Fig. 26.** Service 'Fake Chat Maker - WhatsMessage' - W12_Android.

SMS/MMS and Apple's iMessage service. In contrast to standard SMS/MMSmessages, iMessage are typically sent to another iPhone, iPad, iPod touch or Mac over Wi-Fi or mobile data networks [17]. On the iOS messaging interface, iMessages are displayed in blue speech bubbles, distinguishing them from standard SMS/MMS which are displayed in green speech bubbles. Fig. 29 shows a master CR record created for Messages showing a conversation has been configured to be with a person named 'Tester'. Two messages are sent, one of which being an image and two are received.

From an analysis of the master CR shown in Fig. 29, a markup has been created that highlights 11 'marks' within a real iMessage CR screen capture that could be used to conduct a visual authentication of any iMessage CR screen capture received. These 11 marks are as follows and are shown visually in Fig. 30:

M1:- Banner
M2:- Signal, battery and time symbols.
M3:- Sent message text in green bubble.
M4:- Background wallpaper
M5:- Feature toolbar.
M6:- Message toolbar and icons.
M7:- Sent image.




**Fig. 27.** Service 'WhatsFake - Fake Chat Maker' - W13_Android.




**Fig. 28.** Service 'Fake Whatsp Chat, Call, Status' - W14_Android.

M8:- Received message grey bubble.
M9:- Thread metadata.
M10:- Contact name & tile.
M11:- Time.

Searches conducted via Google, and on the AppStore led to the identification of 8 CRM services (noted in Section 4.1) and attempts were made to recreate the CR shown in Fig. 29 using these CRM services.

### 4.1. Results

Table 3 provides the results of a visual authenticity evaluation of CRMs created by the 8 CRM services where the source of each CRM service is noted (either URL or App name) and each screen capture is provided an identifier (iMes#). Each service was used to create a CRM that visually matches the master CR shown in Fig. 29 as closely as possible using the service's settings and capabilities. Once created, the author conducted a visual authenticity evaluation to assess each of the 11 marks in the original master CR against each CRM service's ability to




**Fig. 29.** The master CR created for iMessage on iOS 16.1.1.

replicate these in any generated fake CR. As part of this evaluation, the scoring methodology set out in Section 3 was applied, and the results are shown in Table 3.

As it is possible for users to crop any CRMs so that operating specific artefacts (battery icons, network provider names etc.) are excluded, an additional percentage match score for each service has been provided which excludes matching for operating specific artefacts.

All 8 CRM service screen captures (iMes1-iMes8) are provided in Figs. 31–38.

Of the 8 services used, none were considered to be able to fully create an authentic mockup inline with the master CR shown in Fig. 29. The iOS application 'FakeChat - Prank SMS Creator' was considered to produce the most realistic CRM with a percentage match score of 86.36%. In contrast, the web service 'http://ifaketext.com/' was considered to produce the least visually authentic CR screen capture, scoring 27.27%.

## 5. Twitter

Twitter is reported to have around 237.8 million monetizable daily active users for the second quarter of 2022, and whilst this falls short of the reported 2 billion users platforms like Facebook and YouTube maintain, the platforms still appeals to a large audience [18]. In addition, there have been a number of reported criminal incidents that have taken place on this platform requiring lawful investigation [19] and studies have indicated concern over the spread of disinformation [20] and fake news [21]. In contrast to the direct messaging services considered in Section 3 and 4, consideration of 'mock status' styled communication is considered here in the form of Tweets made on Twitter.

Fig. 39 shows a master CR record created for a Tweet made from an account named 'Tester' with the handle '@tester6596′. The message '*This is my very first tweet! Yes!*' is posted, with the time and date shown and 1 view.

From an analysis of the master CR shown in Fig. 39, a markup has been created that highlights 9 'marks' within a real Tweet CR screen capture that could be used to conduct a visual authentication of any Tweet CR screen capture received. These 9 marks are as follows and are shown visually in Fig. 40.

M1:- Profile picture.
M2:- Account name.
M3:- Account handle.
M4:- 'More' option.
M5:- Tweet interaction options.
M6:- Analytics label.
M7:- View count.
M8:- Time and Date.
M9:- Tweet contents.

Searches conducted via Google led to the identification of 10 CRM services (noted in Section 5.1) and attempts were made to recreate the CR shown in Fig. 39 using these CRM services.

### 5.1. Results

Table 4 provides the results of a visual authenticity evaluation of CRMs created by the 10 CRM services where the source of each CRM service is noted (either URL or App name) and each screen capture is provided an identifier (T#). Each service was used to create a CRM that visually matches the master CR shown in Fig. 39 as closely as possible using the service's settings and capabilities. Once created, the author conducted a visual authenticity evaluation to assess each of the 9 marks in the original master CR against each CRM service's ability to replicate these in any generated fake CR. As part of this evaluation, the scoring methodology set out in Section 3 was applied, and the results are shown in Table 4.

All 10 CRM service screen captures (T1-T10) are provided in Figs. 41–50.

Of the 10 services used, none were considered to be able to fully create an authentic mockup inline with the master CR shown in Fig. 39. The services 'https://sweary.com/fake-tweet-generator/', 'https://www.tucktools.com/spoof-tweet/' and 'https://shashiirk.github.io/fake-tweet-generator/' were considered to produce the most realistic CRM with percentage match scores of 83.33%. In contrast, the web service 'https://simitator.com/generator/twitter/tweet' was considered to produce the least visually authentic CR screen capture, scoring 50%.

In regards to the effectiveness of Twitter CRMs, subtle differences in structure and layout could not be completely replicated. For example, in

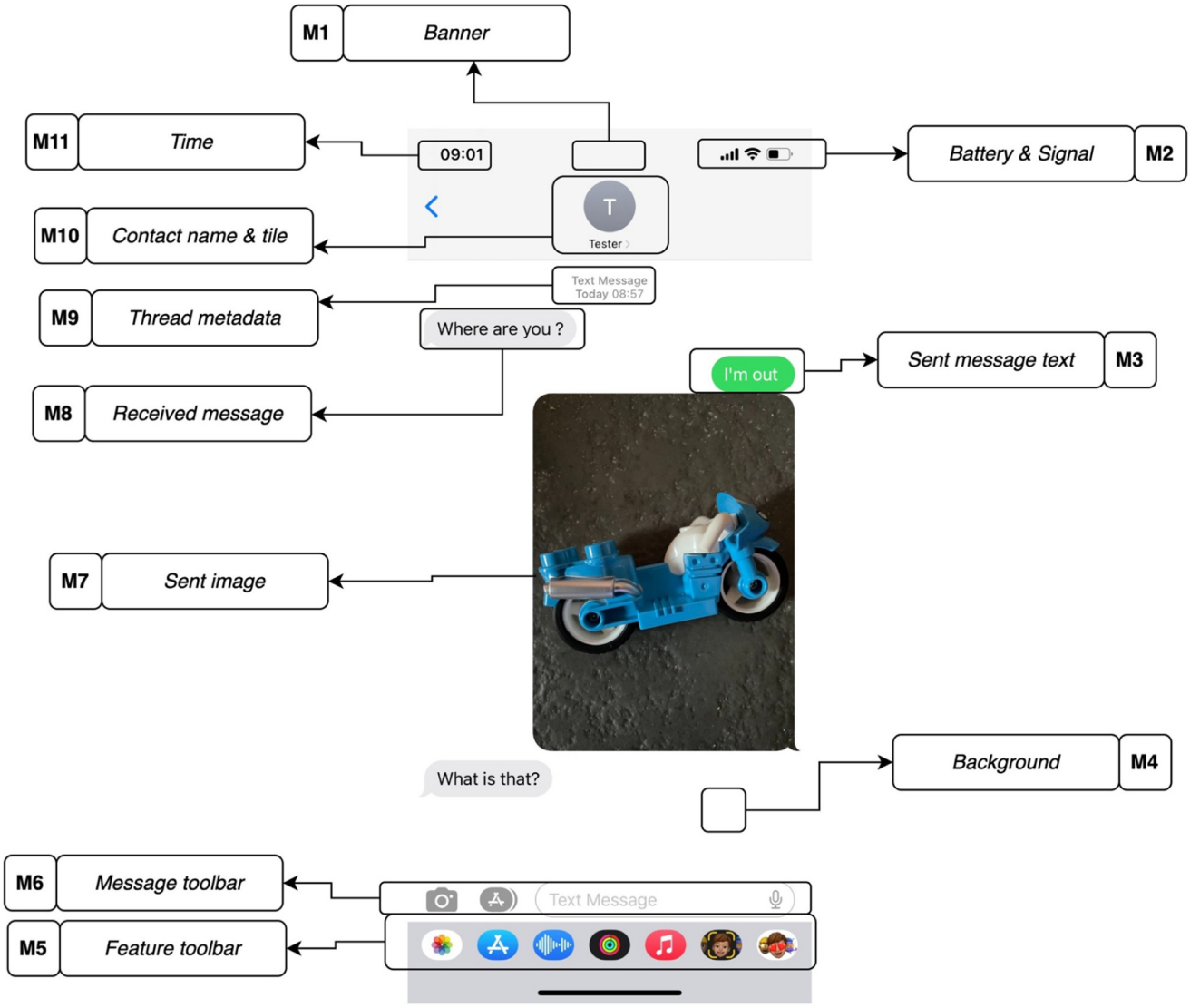



**Fig. 30.** iMessage CR markup showing 15 'marks' for authentication.

regards to service T2, the date represented could only be displayed as 'Apr 06′, where Twitter represents single days as 'Apr 6′ (Mark M8 in Fig. 40). Similarly, no service could reproduce a view count, where in many cases this was mocked up by extending the date and time text field. The implications of this like with the inability to 'bold' the view count number. Further, the replication of the Tweet interaction options (mark M5) is not correctly and completely replicated in 50% of the test cases (see for example T3 with a different 'share' icon being used in comparison with the master CR in Fig. 39).

## 6. Conclusions

This work has examined the use of CRM services for creating fake screen captures of CRs for the services Whatsapp, iOS Messages and Tweets made on Twitter. A total of 41 services have been examined, available online and on the PlayStore and AppStore. The intention was to evaluate whether CRM services pose a realistic threat to law enforcement officers in terms of being able to distinguish a CRM from a genuine CR screen capture. The results show that in no cases, could any CRM service completely mimic the traits of a genuine CR screen capture. Whilst this may suggest that no such threat exists, the following points of note are raised.

1. It should be considered that when under pressure, visual authenticity checks may be conducted quickly meaning there is likely a lower standard of evaluation. Therefore whilst it may seem like some of the visual differences noted in the work may seem obvious, where there is no genuine image to cross-evaluate a CR screen capture against, such differences may not be identified.
2. Arguably, interfaces that are complex are more difficult to replicate as it is likely that there are more 'marks' that need to be effectively copied. Such logic would suggest that services may find it more difficult to replicate the WhatsApp interface on iOS (with 19 marks) and Android (with 18 marks), rather than a Tweet (with 9 marks) or Messages on iOS (with 11 marks). However, the data did not suggest this was the case. Services replicating WhatsApp on Android were found to have an average percentage match across all services of 72.42%, with services replicating WhatsApp on iOS having an average percentage match across all services of 59.36%. In contrast, services replicating Tweets maintained an average percentage match across all services of 68.89% and for Messages on iOS, an average percentage match across all services of 53.98% was achieved.
3. Cropping screen captures may pose an issue when it comes to the detection of authenticity. In many cases across all services, the replication of some redundant interface components was not

**Table 3**
iOS Messages and the results of a visual authenticity evaluation.

| *Type* | *Source* | Screen Capture ID | *M1* | *M2* | *M3* | *M4* | *M5* | *M6* | *M7* | *M8* | *M9* | *M10* | *M11* | Total Score | Percentage Match | Percentage Match (excluding OS artefacts) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Web | http://iphonefaketext.com/ | IMes1 | 0.5 | 0.5 | 0.5 | 1 | 0 | 0.5 | 0.5 | 1 | 0.5 | 0.5 | 0.5 | 6 | 54.54% | 55.56% |
| Web | https://ifaketextmessage.com/ | IMes2 | 0.5 | 0.5 | 1 | 1 | 0 | 0.5 | 0 | 1 | 0 | 0.5 | 0.5 | 5.5 | 50% | 50.00% |
| Web | https://www.fakeimess.com/generator | IMes3 | 0.5 | 0.5 | 0.5 | 1 | 0 | 0.5 | 0.5 | 0.5 | 0 | 0.5 | 0.5 | 5 | 45.45% | 44.44% |
| Web | https://fakedetail.com/fake-iphone-text-messenger-generator | IMes4 | 0.5 | 0.5 | 1 | 1 | 0 | 0.5 | 0 | 1 | 1 | 0.5 | 0.5 | 6.5 | 59.09% | 61.11% |
| Web | http://ios.foxsash.com/ | IMes5 | 0.5 | 0.5 | 0.5 | 1 | 0 | 0.5 | 0.5 | 0.5 | 0.5 | 0.5 | 0.5 | 5.5 | 50% | 50.00% |
| Web | http://ifaketext.com/ | IMes6 | 0 | 0.5 | 0.5 | 0 | 0 | 0.5 | 0 | 0.5 | 0 | 0.5 | 0.5 | 3 | 27.27% | 22.22% |
| Web | https://zeoob.com/generate-iphone-chat/ | IMes7 | 0.5 | 0.5 | 1 | 1 | 0 | 0.5 | 0.5 | 1 | 0.5 | 0.5 | 0.5 | 6.5 | 59.09% | 61.11% |
| App iOS | FakeChat - Prank SMS Creator | IMes8 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 0.5 | 1 | 9.5 | 86.36% | 83.33% |




**Fig. 31.** Service 'http://iphonefaketext.com/' - iMes1.

effectively achieved. Take for example mark M5 for Messages on iOS where no CRM services could replicate the feature toolbar from the original Messages interface. However, to avoid this issue, a user could simply crop their mock screen capture in order to remove these regions of the interface so that it would not be possible to tell that they were not present. Cropping out interface elements like battery and signal signs, times and messages bars would circumvent the issue that many CRM services have with effectively replicating them.

It is argued that it is important to maintain a record of those services in existence which can cause challenges for determining the authenticity of CRs and how they are developing. The images provided in this work provides a starting dataset of CRM service capabilities and to offer a resource for authenticity checks to take place. It should also be noted that visual checks should not always be considered effective for authenticity checking and whilst it is acknowledged in some cases that it may be necessary, determining the presence of CRs through the examination of a device or records provided by a service provided should always be considered more reliable.




**Fig. 32.** Service 'https://ifaketextmessage.com/' - iMes2.




**Fig. 33.** Service 'https://www.fakeimess.com/generator' - iMes3.




**Fig. 34.** Service 'https://fakedetail.com/fake-iphone-text-messenger-generator' - iMes4.




**Fig. 35.** Service 'http://ios.foxsash.com/' - iMes5.




**Fig. 36.** Service 'http://ifaketext.com/' - iMes6.




**Fig. 37.** Service 'https://zeoob.com/generate-iphone-chat/' - iMes7.




**Fig. 38.** Service 'FakeChat - Prank SMS Creator ' - iMes8.




**Fig. 39.** The master Twitter CR created using a web browser.

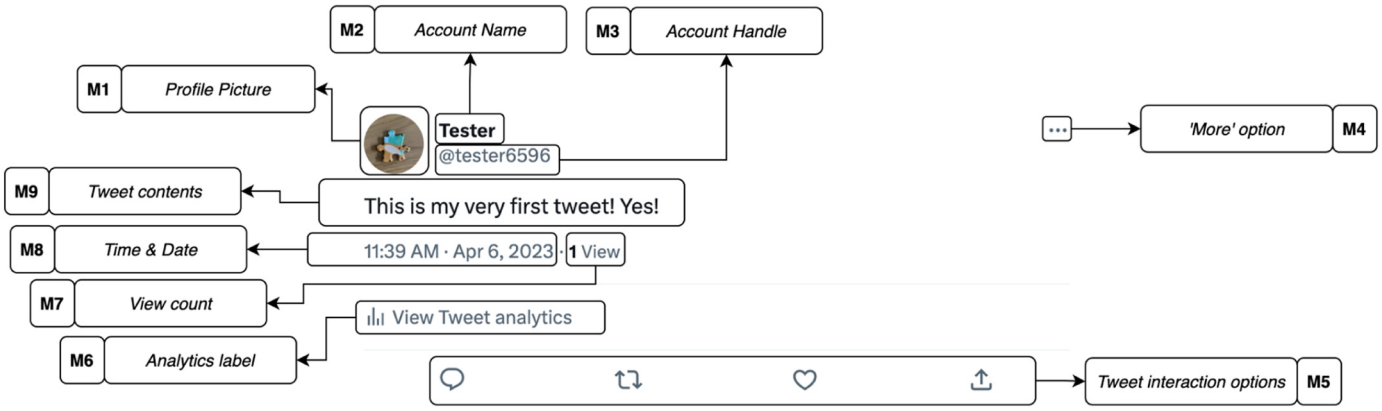



**Fig. 40.** Twitter CR markup showing 9 'marks' for authentication.

**Table 4**
Tweets and the results of a visual authenticity evaluation.

| *Type* | *Course* | *Screen Capture ID* | *M1* | *M2* | *M3* | *M4* | *M5* | *M6* | *M7* | *M8* | *M9* | *Total Score* | *Percentage Match* |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Web | https://www.tweetgen.com/create/tweet.html | T1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 7 | 77.78% |
| Web | https://codebeautify.org/fake-tweet-generator | T2 | 1 | 1 | 1 | 0 | 0.5 | 0 | 0.5 | 0.5 | 1 | 5.5 | 61.11% |
| Web | https://zeoob.com/fake-tweet-generator/ | T3 | 1 | 1 | 1 | 0 | 0.5 | 0 | 0.5 | 0.5 | 1 | 5.5 | 61.11% |
| Web | https://shashiirk.github.io/fake-tweet-generator/ | T4 | 1 | 1 | 1 | 1 | 1 | 0 | 0.5 | 1 | 1 | 7.5 | 83.33% |
| Web | https://www.prankmenot.com/?twitter_tweet | T5 | 0.5 | 1 | 1 | 0 | 0.5 | 0 | 0.5 | 0.5 | 1 | 5 | 55.56% |
| Web | https://www.tucktools.com/spoof-tweet/ | T6 | 1 | 1 | 1 | 1 | 1 | 0 | 0.5 | 1 | 1 | 7.5 | 83.33% |
| Web | https://simitator.com/generator/twitter/tweet | T7 | 0.5 | 1 | 1 | 0 | 0.5 | 0 | 0.5 | 0.5 | 0.5 | 4.5 | 50% |
| Web | https://dizwa.com/simulators/generate-twitter-tweet/?utm_content=cmp-true | T8 | 1 | 0.5 | 0.5 | 0.5 | 0.5 | 0 | 0.5 | 0.5 | 1 | 5 | 55.56% |
| Web | https://sweary.com/fake-tweet-generator/ | T9 | 1 | 1 | 1 | 1 | 1 | 0 | 0.5 | 1 | 1 | 7.5 | 83.33% |
| Web | https://ovdss.com/apps/tweet-generator | T10 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 7 | 77.78% |




**Fig. 41.** Service 'https://www.tweetgen.com/create/tweet.html' - T1.




**Fig. 42.** Service 'https://codebeautify.org/fake-tweet-generator' - T2.




**Fig. 43.** Service 'https://zeoob.com/fake-tweet-generator/' - T3.




**Fig. 44.** Service 'https://shashiirk.github.io/fake-tweet-generator/' - T4.

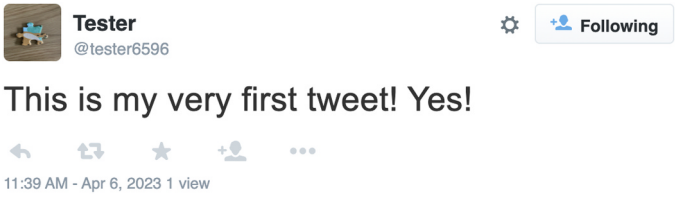



**Fig. 45.** Service 'https://www.prankmenot.com/?twitter_tweet' - T5.




**Fig. 46.** Service 'https://www.tucktools.com/spoof-tweet/' - T6.




**Fig. 47.** Service 'https://simitator.com/generator/twitter/tweet' - T7.




**Fig. 48.** Service 'https://dizwa.com/simulators/generate-twitter-tweet/?utm_content=cmp-true' - T8.




**Fig. 49.** Service 'https://sweary.com/fake-tweet-generator/ ' - T9.




**Fig. 50.** Service 'https://ovdss.com/apps/tweet-generator' - T10.

## CRediT authorship contribution statement

**Horsman Graeme:** Conceptualization, Data curation, Formal analysis, Investigation, Methodology, Project administration, Writing – original draft, Writing – review & editing.

## Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

## References


[1] Gov.uk (2012) 'Communications data – the facts' Available at: ⟨https://www.gov.uk/government/news/communications-data-the-facts⟩ (Accessed: 17 March 2023).

[2] House of Lords Communications Committee (2014) 'Communications Committee - First Report Social media and criminal offences- CHAPTER 2: SOCIAL MEDIA AND THE LAW' Available at: ⟨https://publications.parliament.uk/pa/ld201415/ldselect/ldcomuni/37/3704.htm⟩ (Accessed: 17 March 2023).

[3] BC Society of Transition Houses (2021) 'How to Save and Print a Screenshot' Available at: ⟨https://bcsth.ca/wp-content/uploads/2021/03/B.-How-to-Save-and-Print-a-Screenshot-for-Evidence_FINAL_24Feb2021.pdf⟩ (Accessed: 27 March 2023).

[4] College of Policing (2023) 'Communications data investigation' Available at: ⟨https://www.college.police.uk/career-learning/learning/courses/communications-data-investigation⟩ (Accessed: 19 April 2023).

[5] Citizens Advice Scotland (2023) 'If your intimate photos or videos are shared without your consent' Available at: ⟨https://www.citizensadvice.org.uk/scotland/law-and-courts/society-s/privacy-and-media-s/if-your-intimate-photos-or-videos-are-shared-without-your-consent/⟩ (Accessed: 28 March 2023).

[6] Crown Prosecution Service (2023) 'Social Media and other Electronic Communications' Available at: ⟨https://www.cps.gov.uk/legal-guidance/social-media-and-other-electronic-communications⟩ (Accessed: 17 March 2023).

[7] Lancashire Constabulary, (2023) 'Someone I know has sent me a rude / offensive message on social media, what can I do about it?' Available at: ⟨https://www.lancashire.police.uk/faqs/online-safety/someone-i-know-has-sent-me-a-rude-offensive-message-on-social-media-what-can-i-do-about-it/⟩ (Accessed: 17 March 2023).

[8] Metropolitan Police (2023) 'I'm being harassed by someone on social media. What can I do?' Available at: ⟨https://www.met.police.uk/advice/advice-and-information/har/harassment-on-social-media/⟩ (Accessed: 28 March 2023).

[9] Police Scotland (2023) 'Sextortion' Available at: ⟨https://www.scotland.police.uk/advice-and-information/internet-safety/sextortion/⟩ (Accessed: 27 March 2023).

[10] Olliers Solicitors (2023) 'Can screenshots be relied upon as evidence?' Available at: ⟨https://www.olliers.com/news/can-screenshots-be-relied-on-as-evidence/⟩ (Accessed: 28 March 2023).

[11] Gill, Jim (2022) 'When it Comes to Using Screenshots as Evidence, It's All About Authentication' Available at: ⟨https://www.jdsupra.com/legalnews/when-it-comes-to-using-screenshots-as-2429321/⟩ (Accessed: 17 March 2023).

[12] Cloudnine (2023) 'eDiscovery Daily Blog' Available at: ⟨https://cloudnine.com/ediscoverydaily/production/authenticating-communication-screenshots/⟩ (Accessed: 27 March 2023).

[13] Finch, Ian (n.d.) 'How to Spot Falsified Evidence in Mobile Device Screenshots' Available at: ⟨https://www.vestigeltd.com/resources/articles/how-to-spot-falsified-evidence-in-mobile-device-screenshots/⟩ (Accessed: 28 March 2023).

[14] BBC News (2018) 'Woman guilty of 'racist' Snap Dogg rap lyric Instagram post' Available at: ⟨https://www.bbc.co.uk/news/uk-england-merseyside-43816921⟩ (Accessed: 28 March 2023).

[15] Antoniou, Nicola and Scarlett, Eleanore. (2022) 'Social media in court: your tweets could be used as evidence against you' Available at: ⟨https://theconversation.com/social-media-in-court-your-tweets-could-be-used-as-evidence-against-you-97739⟩ (Accessed: 28 March 2023).

[16] Statista (2022) 'WhatsApp - Statistics & Facts' Available at: ⟨https://www.statista.com/topics/2018/whatsapp/#topicOverview⟩ (Accessed: 27 March 2023).

[17] Apple (2021) 'https://support.apple.com/en-gb/HT207006′ Available at: ⟨https://support.apple.com/en-gb/HT207006⟩ (Accessed: 28 March 2023).

[18] Statista (2023) 'Twitter - Statistics & Facts' Available at: ⟨https://www.statista.com/topics/737/twitter/#topicOverview⟩ (Accessed: 6 April 2023).

[19] G. Horsman, K. Ginty, P. Cranner, Identifying offenders on Twitter: a law enforcement practitioner guide, Digit. Investig. 23 (2017) 63–74.

[20] Knight Foundation (2018) 'How much "fake news" can we identify on Twitter?' Available at: ⟨https://knightfoundation.org/features/misinfo/⟩ (Accessed: 6 April 2023).

[21] C.S. Atodiresei, A. Tănăselea, A. Iftene, Identifying fake news and fake users on Twitter, Procedia Comput. Sci. 126 (2018) 451–461.



https://dspace.org/

# Identifying fake vs. real communication records: a case study

**Horsman, Graeme**

**2023-12**
Elsevier
https://doi.org/10.1016/j.fsir.2023.100346
Horsman G. (2023) Identifying fake vs. real communication records: a case study. Forensic Science International: Reports, Volume 8, December 2023, Article number 100346

Downloaded from a DSpace repository. https://dspace.org/