Spoofs, Fakes, and Manipulation: The Challenge of Validating Messages and Social Media Content on Mobile Phones

Lars Daniel EnCE, CCPA, CCO, CTNS, CTA, CIPTS, CWA
Practice Leader - Digital Forensics at Envista Forensics
919-621-9335 / lars.daniel@envistaforensics.com

We would all like to believe that when we view a photo, the contents therein are a true and accurate representation of what they purport to be. Unfortunately, this is not always the case. We are all aware of software tools that allow for manipulating photos to create convincingly real fakes. Sometimes, these fakes are so convincing that veracity cannot be determined by examining the picture alone with the naked eye.

This has been true with photos for a long time and is true today with videos using deep fake technology. Software applications are widely available that allow a person to manipulate video or audio in order to make it appear that he or she is saying something that they never said. Like with the Reface App[i], where a person's face can be replaced with another's. It seems that the technology has advanced to the point where anyone can create a very convincing fake video of events and do so using an application on his or her phone. The individual need not have any special expertise in creating videos, all they need is the software.

Making fake photos and videos is relatively simple but making faked and spoofed social media and messaging content is even easier.

Additionally, a person can alter or fake text message communications, and someone can do it with a low level of technical sophistication and relative ease.

In mobile device forensics, the best method to collect the evidence from a phone is performed by utilizing cell phone forensics software and hardware. Before we cover the problems with verifying pictures and screenshots of social media content and text messages, it is pertinent to have a high-level overview of how data is collected.

The forensic acquisition process encompasses all the methods and procedures utilized to collect digital evidence. This collection process can take many forms with mobile phones and the data from mobile devices can reside in numerous locations. With mobile phones, the data extraction methods used are determined by multiple factors, including the cell phone's make, model, operating system version, and physical damage, to name a few.

How Mobile Phone Forensic Tools Verify Evidence

When a forensic acquisition is performed on a computer hard drive, a bit-for-bit duplicate of the data is created. In other words, all the data contained on the hard drive, including existing data, deleted data, and unallocated space, are collected in a forensic image file. This forensic image file is exactly like the data contained on the computer hard drive. However, a forensic acquisition of a mobile device is different, as it almost always has to be powered on.

The forensic data collection process from the mobile device is better called a "forensics extraction," as data is extracted from the device instead of a perfect bit-for-bit copy of the evidence item. With the mobile phone powered on, the forensic software cannot access some areas of data. However, that inaccessible data is usually of little to no value evidentiarily.

Following the forensic copying comes the hashing process. A mathematical algorithm is run against the copied data, producing a unique hash value. This hash value can be thought of as a digital fingerprint, uniquely identifying the copied evidence exactly as it exists at that point in time.

Preemptively raising the question, “Why bother hashing the forensic copy of a cell phone if it is not exactly the same as the original evidence like a computer?” Well, suppose you made a forensic copy of a phone today and hashed it, and sometime later an opposing attorney claimed you manipulated data. In that case, you could go back to the original forensic copy to prove you did not.

> *But what happens when the evidence is collected from a cell phone using screenshots or pictures? Since there is no mathematical algorithm or any other kind of forensic verification, how do we know that the messages or social media content are real?*

Manual Examinations

To have confidence in the evidence gathered from mobile phones without forensic software and hardware begins with a correctly performed manual examination. A physical acquisition is the best option with mobile phone forensics, followed by a logical or filesystem acquisition. Manual examinations should be utilized as a last resort when other forensic acquisition methods are not possible. The risk of changing or deleting evidence on a mobile phone is significantly increased when performing a manual examination because it introduces a higher potential for human error.

A manual examination of a cell phone involves an examiner manipulating the mobile phone to the different areas of information, such as text messages or call history, and taking pictures of the screen with a camera. A correctly performed manual examination will reduce the risks of modifying the original evidence. Therefore, a manual examination is a viable option when acquiring cell phone evidence with correct procedures and thorough documentation.

The quality of a manual cell phone examination depends on the competency of the examiner. For example, suppose proper procedures and detailed documentation are not part of the manual examination. In that case, it can call into question whether or not the evidence was properly preserved and if tampering, intended or otherwise, occurred during the examination of the cell phone.

Pictures only tell part of the story. What happened during the time between the individual pictures being taken? Pictures alone do not provide any real verification that the phone evidence has not been altered. A video camera running continuously throughout the manual examination process, with no breaks, pauses, or edits, is the only method for evidence verification in the absence of a mathematical hash value. The video should begin before the phone is powered up. At the end of the examination, the phone should be powered down in view of the camera.

In my experience, it is uncommon for forensic examiners to properly follow best practices and protocols when it comes to manual examinations. A video recording rarely accompanies the photos of the mobile phone contents.

Why It Matters: Fakes Are Spoofs Are Real and On The Rise

Social Media Fakes

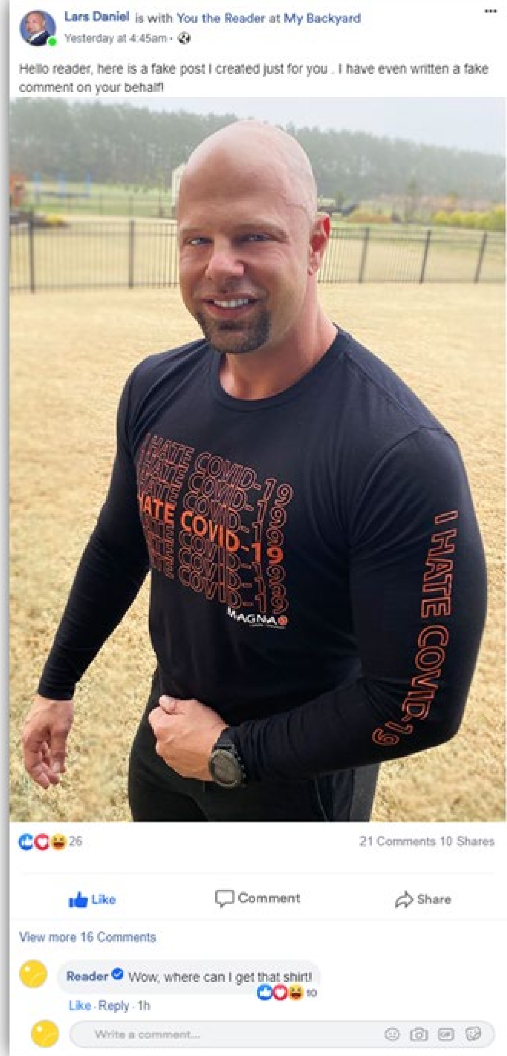
The pervasiveness of social media in our culture and the frequency at which users access these platforms to communicate, share, and consume content have broadened and deepen the amount of courtroom evidence. However, social media evidence has one particular vulnerability, the ability to be altered or forged.

It does not take a high degree of technical capability or access to special software to create fake social media posts. Anyone can find websites that allow you to make fake social media posts and messages that look real, indistinguishable from authentic content.

For example, here are posts I made between myself and you, the reader, as a means of illustration. In addition, I can create fake posts and messages for all major social media platforms. The following faked social media messages and posts were created using a web-based application that is both simple to use and free.[ii]

Facebook

The time, date, location, content, comments, reactions, and chat messages contained in these photos are all fake.



Lars Daniel is with You the Reader at My Backyard

Yesterday at 4:45am ·

Hello reader, here is a fake post I created just for you . I have even written a fake comment on your behalf!

26

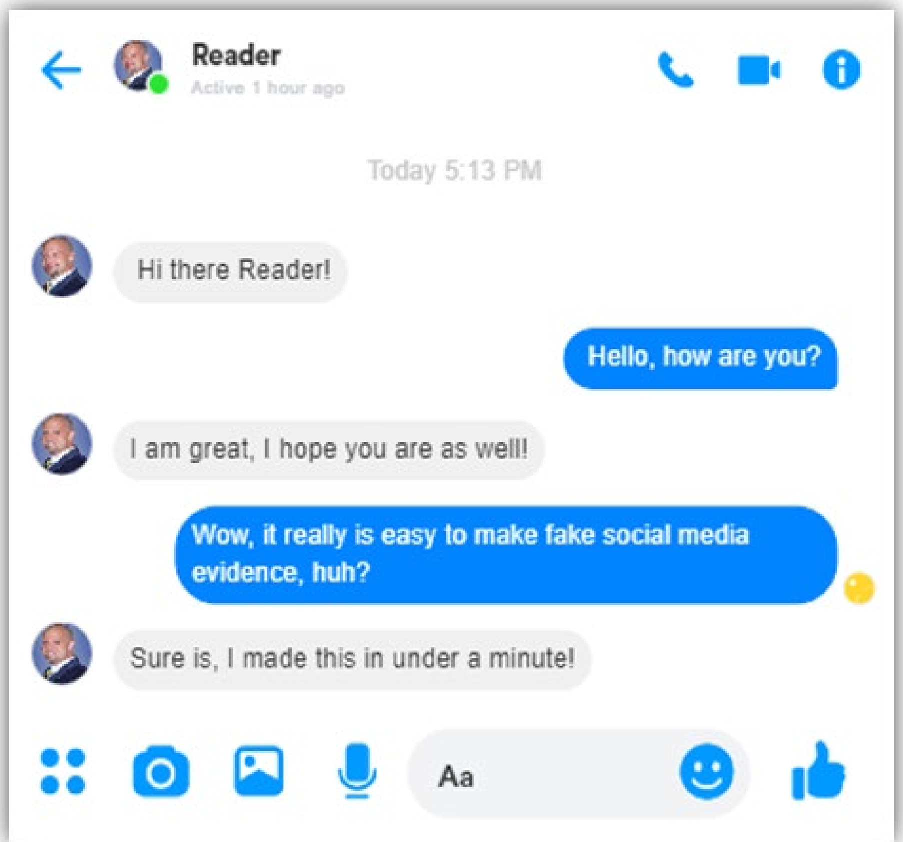
21 Comments 10 Shares

View more 16 Comments

Reader Wow, where can I get that shirt!

10

Like · Reply · 1h



Reader
Active 1 hour ago

Today 5:13 PM

Hi there Reader!

Hello, how are you?

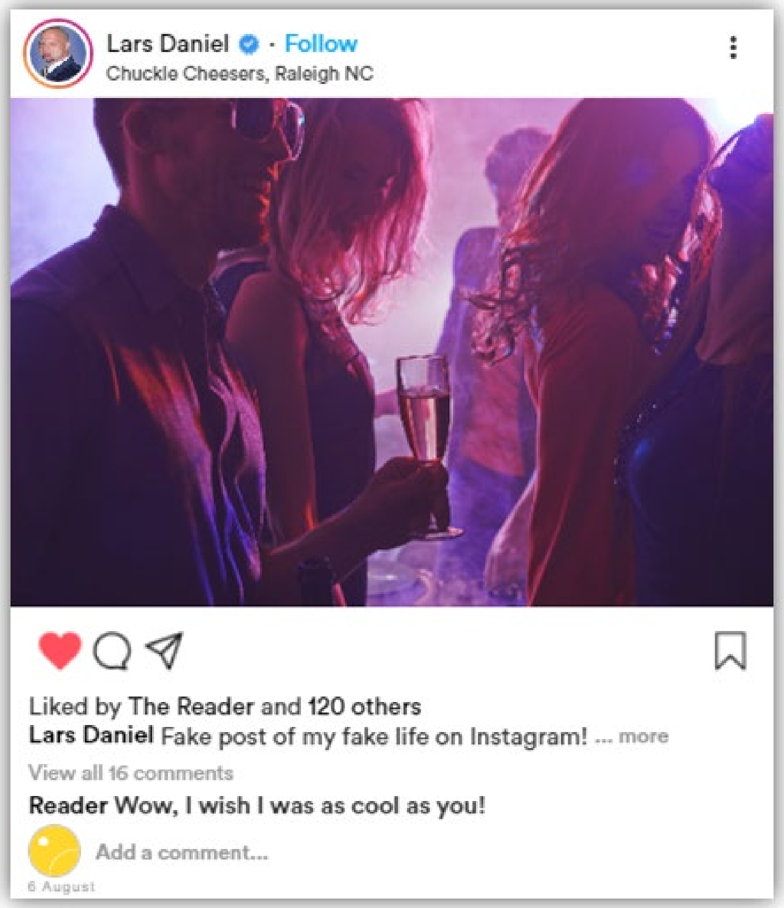
I am great, I hope you are as well!

Wow, it really is easy to make fake social media evidence, huh?

Sure is, I made this in under a minute!

Instagram

The account, blue check showing that I am a verified user, location, photo, content, comments, reactions, and chat communications are all fake.



Lars Daniel

Chuckle Cheesers, Raleigh NC

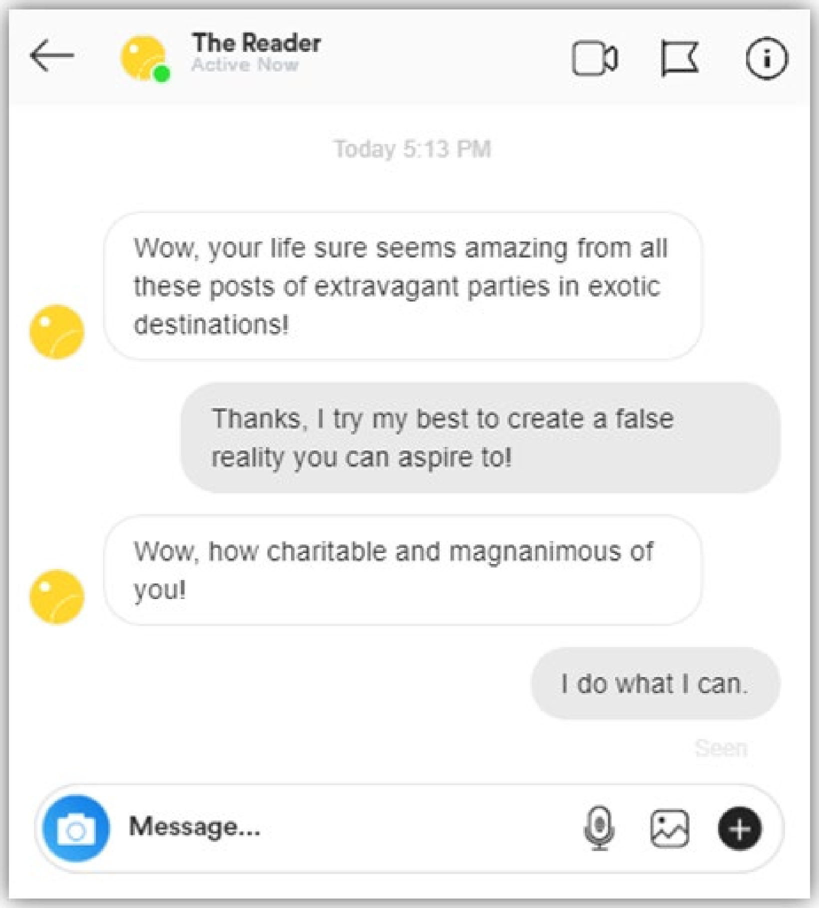
Liked by The Reader and 120 others

Lars Daniel Fake post of my fake life on Instagram! ... more

View all 16 comments

Reader Wow, I wish I was as cool as you!

6 August



Today 5:13 PM

Wow, your life sure seems amazing from all these posts of extravagant parties in exotic destinations!

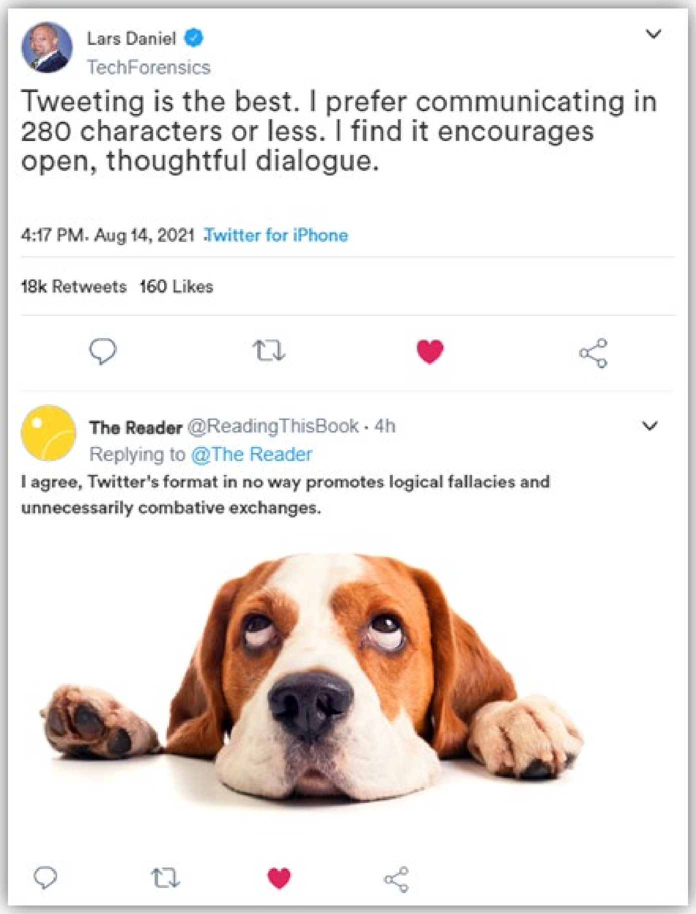
Thanks, I try my best to create a false reality you can aspire to!

Wow, how charitable and magnanimous of you!

I do what I can.

Twitter

The account, tweets, time, retweets, likes, comments, and chats communications are fake.



Lars Daniel
TechForensics

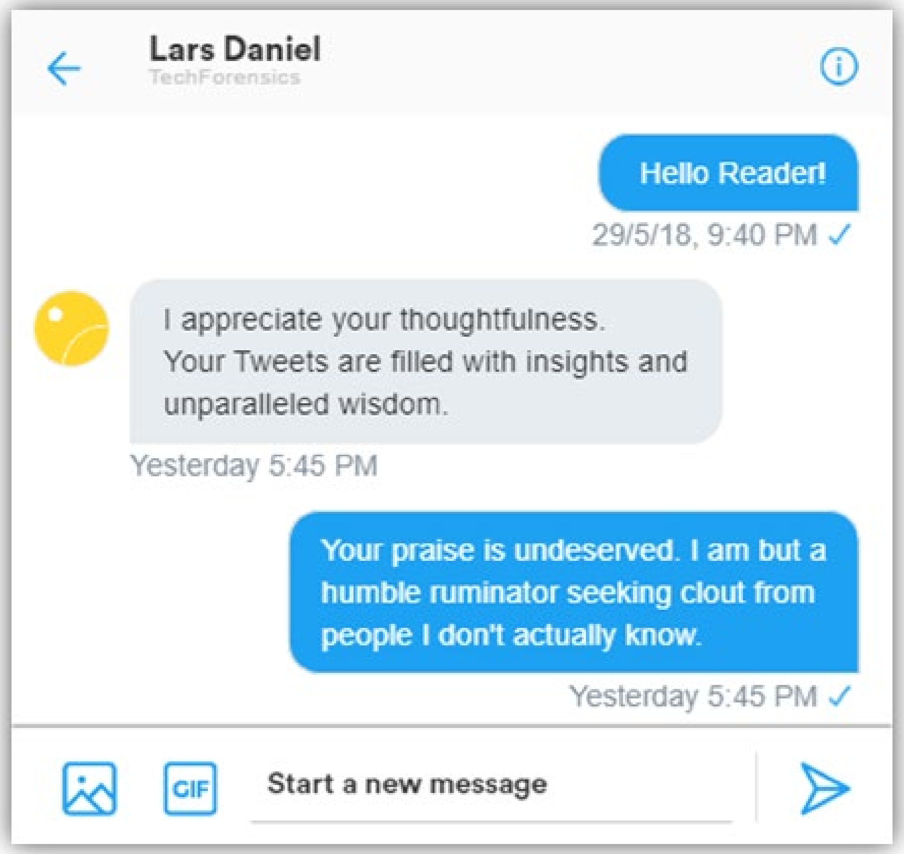
Tweeting is the best. I prefer communicating in 280 characters or less. I find it encourages open, thoughtful dialogue.

4:17 PM. Aug 14, 2021 Twitter for iPhone

18k Retweets 160 Likes

The Reader @ReadingThisBook · 4h
Replying to @The Reader

I agree, Twitter's format in no way promotes logical fallacies and unnecessarily combative exchanges.



Lars Daniel

TechForensics

Hello Reader!

29/5/18, 9:40 PM ✓

I appreciate your thoughtfulness. Your Tweets are filled with insights and unparalleled wisdom.

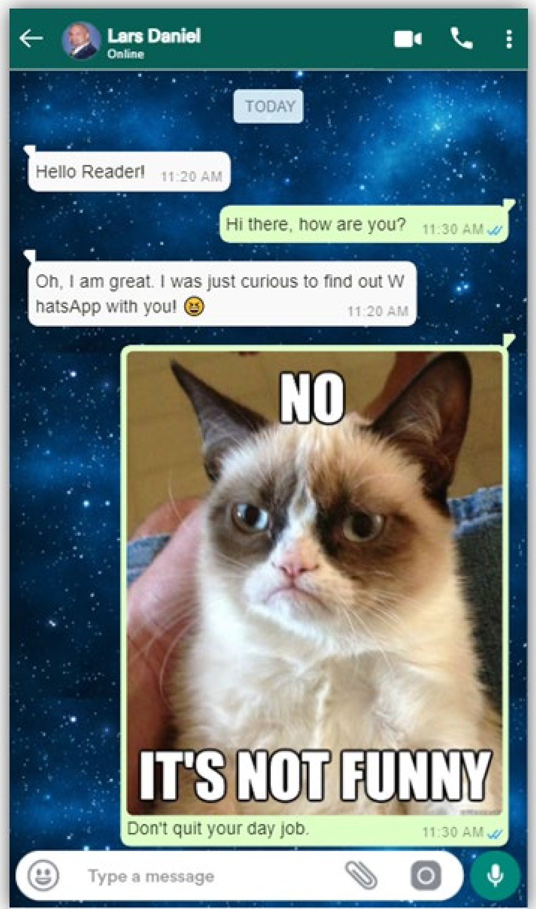
Yesterday 5:45 PM

Your praise is undeserved. I am but a humble ruminator seeking clout from people I don't actually know.

Yesterday 5:45 PM ✓

WhatsApp

The account, name, status, content, photo, and time are all fake.



Hello Reader! 11:20 AM

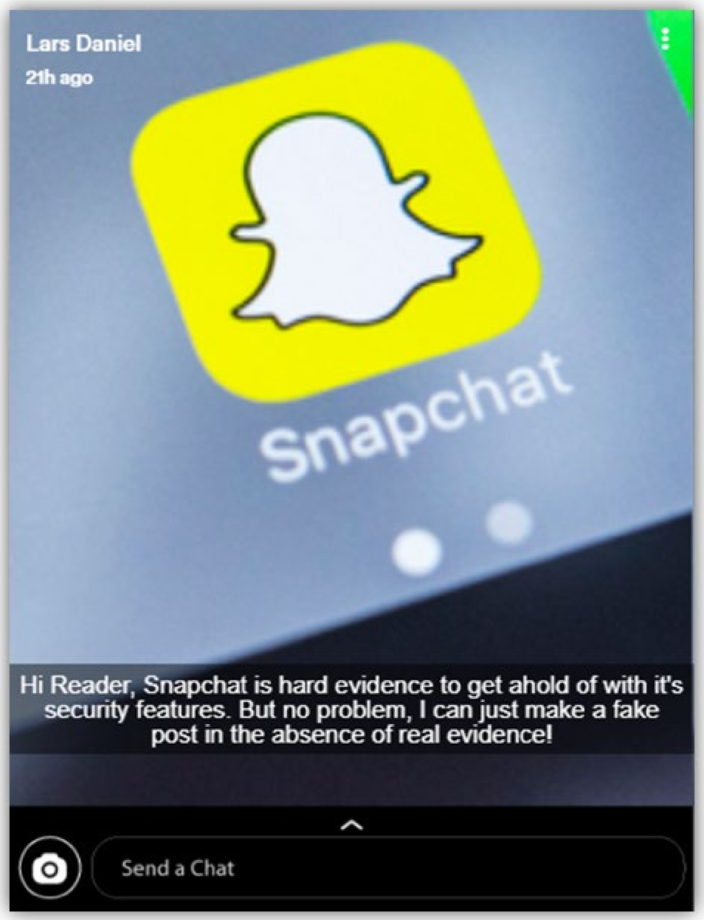
Hi there, how are you? 11:30 AM

Oh, I am great. I was just curious to find out W hatsApp with you! 😆 11:20 AM

Don't quit your day job. 11:30 AM

Snapchat

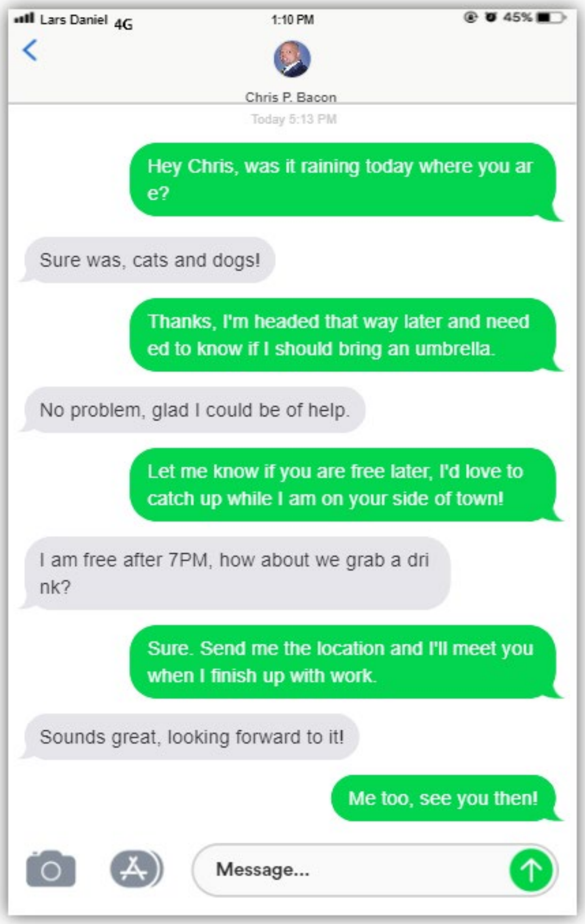
The image, text, time, name, account, and content are all fake



Hi Reader, Snapchat is hard evidence to get ahold of with it's security features. But no problem, I can just make a fake post in the absence of real evidence!

Texting

The account, contact, connection, name, content, time, icons, battery, and cellular service bars are all fake.



Hey Chris, was it raining today where you ar e?

Sure was, cats and dogs!

Thanks, I'm headed that way later and need ed to know if I should bring an umbrella.

No problem, glad I could be of help.

Let me know if you are free later, I'd love to catch up while I am on your side of town!

I am free after 7PM, how about we grab a dri nk?

Sure. Send me the location and I'll meet you when I finish up with work.

Sounds great, looking forward to it!

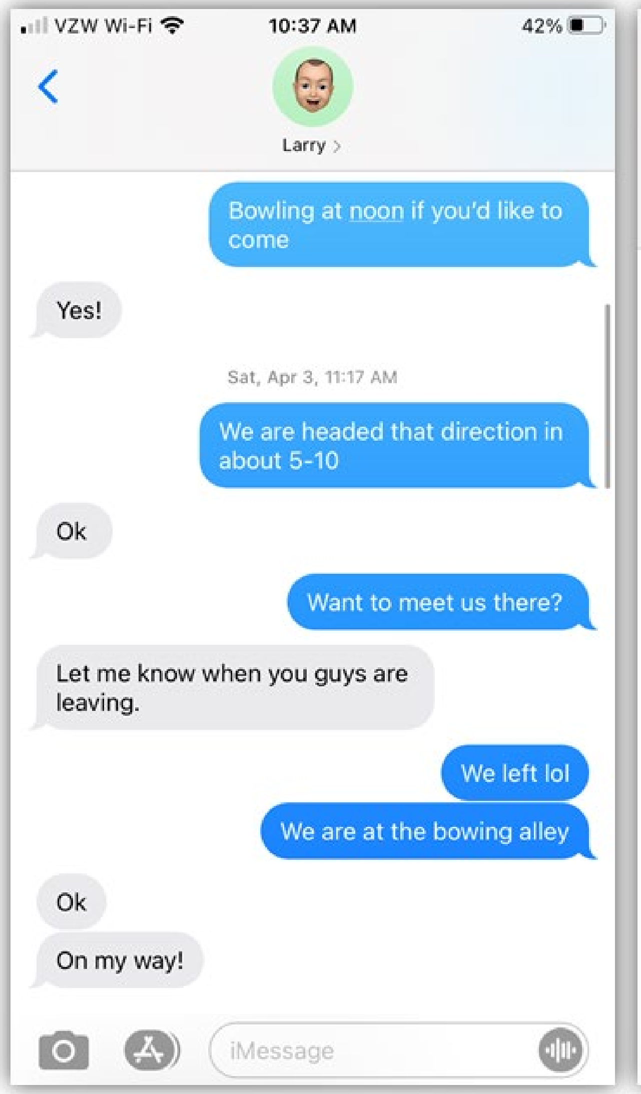
Me too, see you then!

Spoofs and Fakes: Just the Phone

Creating fake messaging application communications on a cell phone doesn't require any outside tools, like the web-based application from the previous section. Instead, a user can make a fake with just the phone that they have in their hands that looks the same as a screenshot or photo provided as evidence.

Name Change

Screenshots of a text message conversation cannot verify the actual identity of a person alone. This is because the contact name can be changed at any time and the phone numbers of the sender or recipient are not recorded in the actual conversation itself in any way. For example, a person could change the contact on their phone named "Larry" to "David" by only editing the contact information, then take the pictures of the conversations to provide as evidence. All the messages sent between the person and Larry would appear to be between the person and David.



Bowling at noon if you'd like to come

Yes!

Sat, Apr 3, 11:17 AM

We are headed that direction in about 5-10

Ok

Want to meet us there?

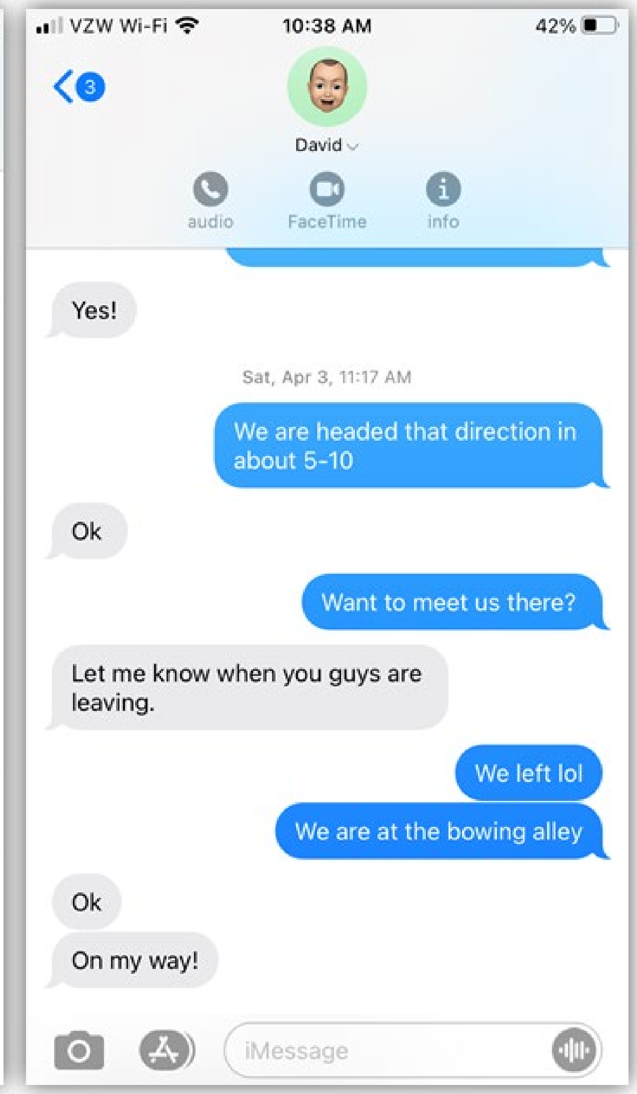
Let me know when you guys are leaving.

We left lol

We are at the bowing alley

Ok

On my way!



Yes!

Sat, Apr 3, 11:17 AM

We are headed that direction in about 5-10

Ok

Want to meet us there?

Let me know when you guys are leaving.

We left lol

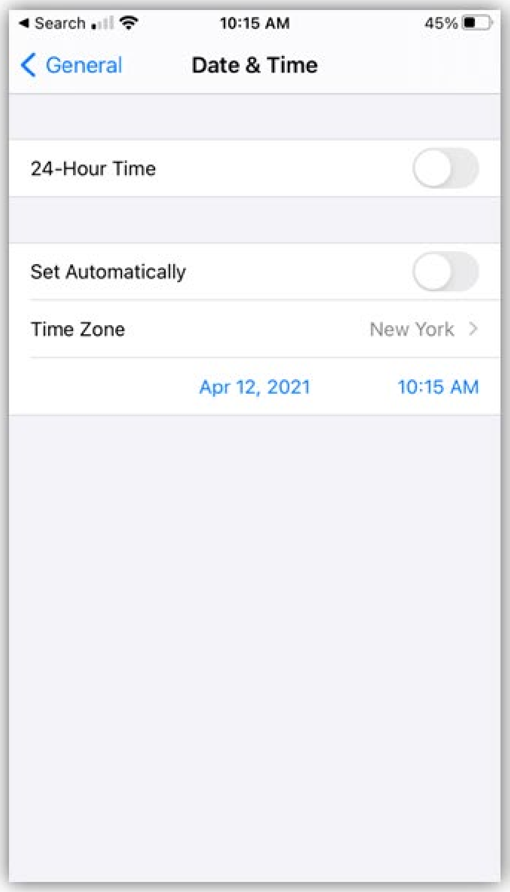
We are at the bowing alley

Ok

On my way!

Time Travel – Back Dating

It is possible to backdate an iPhone and to create text messages with fake dates and times. This can be done by going to the "Settings" application, selecting "General" from the menu, and then selecting "Date & Time." Next, from the "Date & Time" menu, turn off "Set Automatically." From there, click the menu option "Set Date & Time," and now the date and time can be set to anything. I can then send a text message that will show any date and time I select.

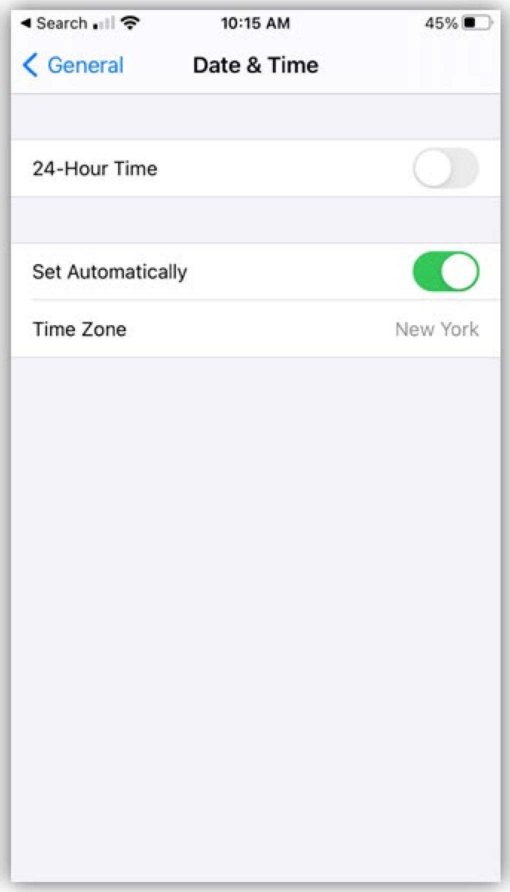


24-Hour Time ○

Set Automatically ○

Time Zone New York

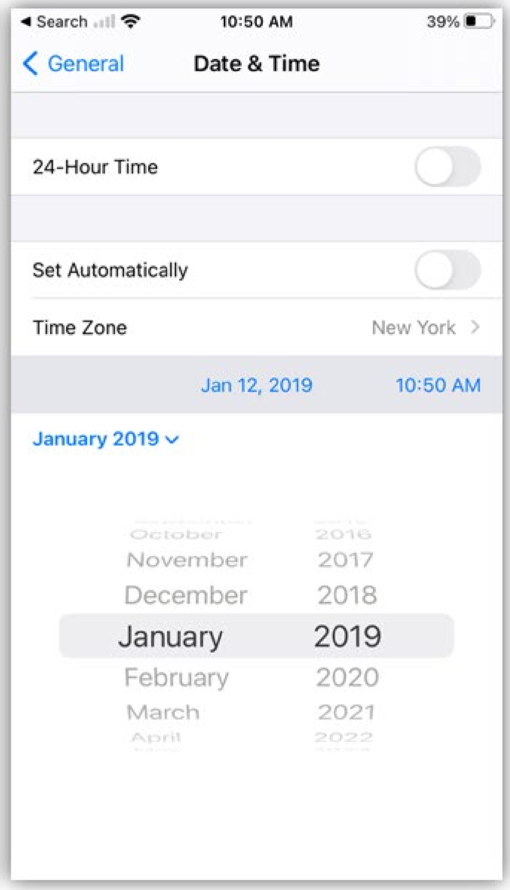
Apr 12, 2021 10:15 AM



24-Hour Time ○

Set Automatically ●

Time Zone New York



24-Hour Time ○

Set Automatically ○

Time Zone New York

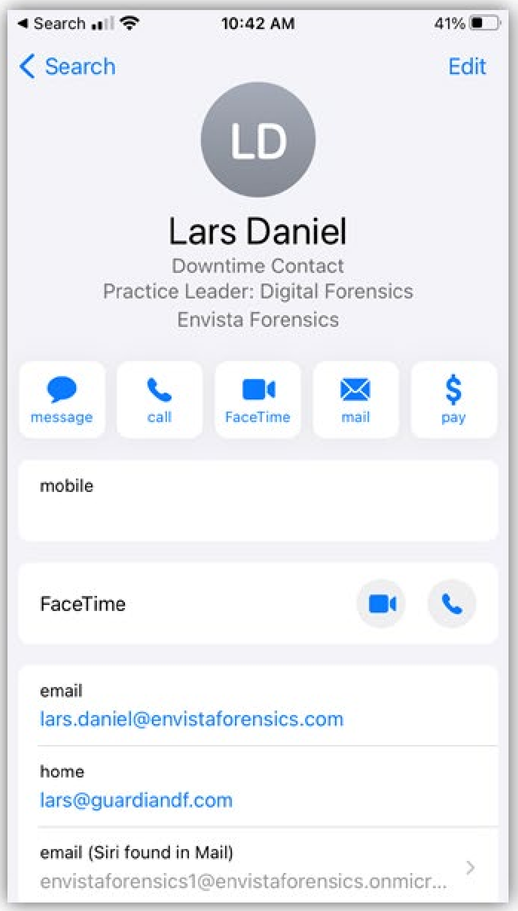
Jan 12, 2019 10:50 AM

January 2019

Talking to Myself – iMessage

Using only an iPhone, you can create a contact that uses your email address for iMessage communication. You then make a different contact on the phone that uses your cell phone number. While both the email and cell phone number are associated with you, you can have a conversation with yourself by naming them differently on the phone.

Couple this with the ability to backdate an iPhone, and it's possible to create months' or even years' worth of messages between two parties in an afternoon whom you can name anything you want and the screenshots would look exactly the same as a real message conversation.



◂ Search 10:42 AM 41%

< Search Edit

LD

Lars Daniel

Downtime Contact
Practice Leader: Digital Forensics
Envista Forensics

message call FaceTime mail pay

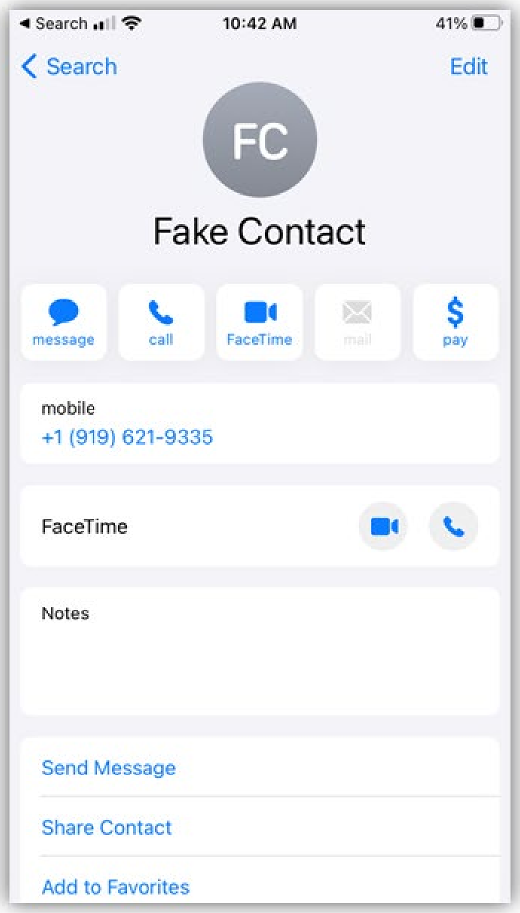
mobile

FaceTime

email
lars.daniel@envistaforensics.com

home
lars@guardiandf.com

email (Siri found in Mail)
envistaforensics1@envistaforensics.onmicr...



◂ Search 10:42 AM 41%

< Search Edit

FC

Fake Contact

message call FaceTime mail pay

mobile
+1 (919) 621-9335

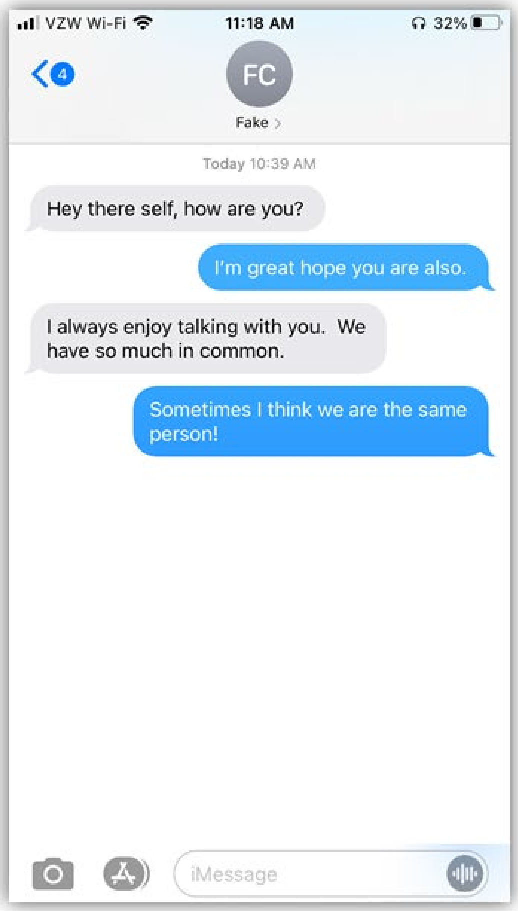
FaceTime

Notes

Send Message

Share Contact

Add to Favorites



VZW Wi-Fi 11:18 AM 32%

< 4

FC

Fake >

Today 10:39 AM

Hey there self, how are you?

I'm great hope you are also.

I always enjoy talking with you. We have so much in common.

Sometimes I think we are the same person!

iMessage

When in Doubt Challenge the Evidence

When performing a manual examination, there are two critical components. One, the phone needs to be isolated from cellular and wireless networks. If you're looking at photos of text messages and see that there are Wi-Fi or cellular bars, you know that the phone was not isolated from the networks. Isolation of the device itself is achieved by eliminating all forms of data transmission, including the cellular network, Bluetooth, wireless networks (Wi-Fi), and infrared connections. By isolating the phone from all networks, the mobile phone is prevented from receiving any new data that would cause other data to be deleted, or worse, overwritten. The goal is to preserve the evidence as a snapshot in time of exactly how the evidence existed when it was received into custody.

Isolation

Did they Use a Faraday Bag?

A Faraday bag blocks any signals that a cell phone might pick up by blocking electrical fields and radio frequencies. A microwave uses this same technology, utilizing a Faraday cage to contain the magnetron's radio frequency within the cooking chamber. A cell phone can also be isolated from networks by wrapping the phone in a radio frequency shielding cloth and placing it into Airplane Mode.

Airplane Mode

After a digital forensic examiner has placed the phone into a Faraday bag or other device to ensure that the phone cannot receive any data, it is acceptable to put it into Airplane Mode. Once this is done, the phone can be removed for the duration of the examination. However, there is one caveat to this. The examiner must ensure that the phone is placed in Airplane Mode and that wireless functionality is turned off. You have likely experienced this in real life when flying. Even though you must turn off your cellular service while on an airplane, you can still access the Internet and transmit data using Wi-Fi; both wireless and cellular connectivity must be turned off for device isolation.

Video Verification

The other critical component, as previously discussed, is the continuous video footage of the examination of the cell phone, using photos of the contents, such as text messages or emails, for verification. Documentation from the National Institute of Standards and Technology (NIST) is an excellent resource for cross-examining experts or whoever documented messages via photo or screenshot.

In the following short example, we will utilize NIST documentation as exhibits to show the need for video verification. We will assume that no video was taken during the manual examination for the purpose of our example.

Cross-Examination Example: Video Verification

Q: Are you familiar with the National Institute of Standards and Technology (NIST)?

A: Yes

Q: Would you consider NIST to be a reliable source for information concerning cell phone forensics?

A: Yes

Q: Would you consider NIST to be an authority in the digital forensics community on how digital evidence should be handled?

A: Yes

INTRODUCE EXHIBIT: *NIST Special Publication 800-101 Revision 1 Guidelines on Mobile Device Forensics*

Q: Please read the second to last paragraph on page 51.

A: "Invariably, not all relevant data viewable on a mobile device using the available menus may be acquired and decoded through a logical acquisition. Manually scrutinizing the contents via the device interface menus while video recording the process not only allows such items to be captured and reported but also confirms that the contents reported by the tool are consistent with observable data. Manual extraction must always be done with care, preserving the integrity of the device in case further, more elaborate acquisitions are necessary."

Q: What exactly is a manual examination of a cell phone?

A: A manual examination is where you take pictures of the contents from the phone, such as pictures of the text messages or emails.

Q: And that is what NIST is talking about in that paragraph, is that correct?

A: yes

Q: Did you video record your manual examination?

A: No

Q: Is there a reason you chose not to videotape the examination?

A: I didn't think I needed to since I was documenting the text messages with photos.

Q: Since the examination was not video recorded, can you prove if any of the text messages on the phone were deleted **UNINTENTIONALLY** during the manual examination?

A: No

Q: Since the examination was not video recorded, is there any way you can prove if any of the text messages on the phone were deleted **INTENTIONALLY** during the manual examination?

A: No

Q: Since the examination was not video recorded, is there any way you can prove if any of the text messages on the phone were modified **UNINTENTIONALLY** during the manual examination?

A: No

Q: Since the examination was not video recorded, is there any way you can prove if the text messages on the phone were modified **INTENTIONALLY** during the manual examination?

A: No

Q: Since the examination was not video recorded, is there any way you can prove if the text messages on the phone were created **UNINTENTIONALLY** during the manual examination?

A: No

Q: Since the examination was not video recorded, is there any way you can prove if the text messages on the phone were created **INTENTIONALLY** during the manual examination?

A: No

Q: If you had video recorded your examination, you could provide proof that there was no intentional or unintentional manipulation of the cell phone. Is that correct?

A: Yes

Conclusion

It is not hard to imagine this line of questioning expanded and enhanced by an attorney being a long and arduous experience for the witness. All because they skipped a simple step of video recording the process of their examination. Having testified as an expert witness on evidence verification and the authenticity of photos or screenshots of text messages, I can tell you that this is a common scenario.

Often basic forensic procedures are not followed in manual examinations. Mobile phones are not isolated from networks, exposing them to data manipulation and deletion. Manual examinations are not recorded, leaving the trier of fact with only the word of the examiner instead of verifiable proof in the form of a video recording. We all walk around with a video camera in our pocket. Beyond extreme circumstances, there is no excuse for an improperly performed manual examination, and if your encounter one in your case, it can be challenged from a forensic perspective.

[i] Reface. Face swap videos

[ii] Zeoob | Generate Instagram, TikTok, Snapchat, Twitter, Facebook Chats & Posts with comments to offer your students some variety in dealing with storytelling.