PROGRAM MATERIALS
Program #3609
January 16, 2026

# The Evidence is Out There - Identifying, Preserving, and Presenting Digital Evidence

- Damon Hacker, MBA, CISA, CSXF, CMMC-RP-President-ArcherHall

Celesq® AttorneysEd Center
www.celesq.com

5301 North Federal Highway, Suite 150, Boca Raton, FL 33487
Phone 561-241-1919

# The Evidence is Out There – Identifying, Preserving, and Presenting Digital Evidence

Damon Hacker, MBA, CISA,
CSXF, CMMC-RP
President

ArcherHall
AIM HIGH

dhacker@archerhall.com
855.839.9084

ArcherHall
AIM HIGH

*Digital Forensics & eDiscovery experts serving attorneys in all 50 states*

- Cellphones
- Computers & Tablets
- External Hard Drives
- Smart Devices
- Emails & SMS
- Social Media Accounts
- Cloud Data
- Electronic Medical Records

Business Litigation

Employment Law

Schools and Higher-Ed

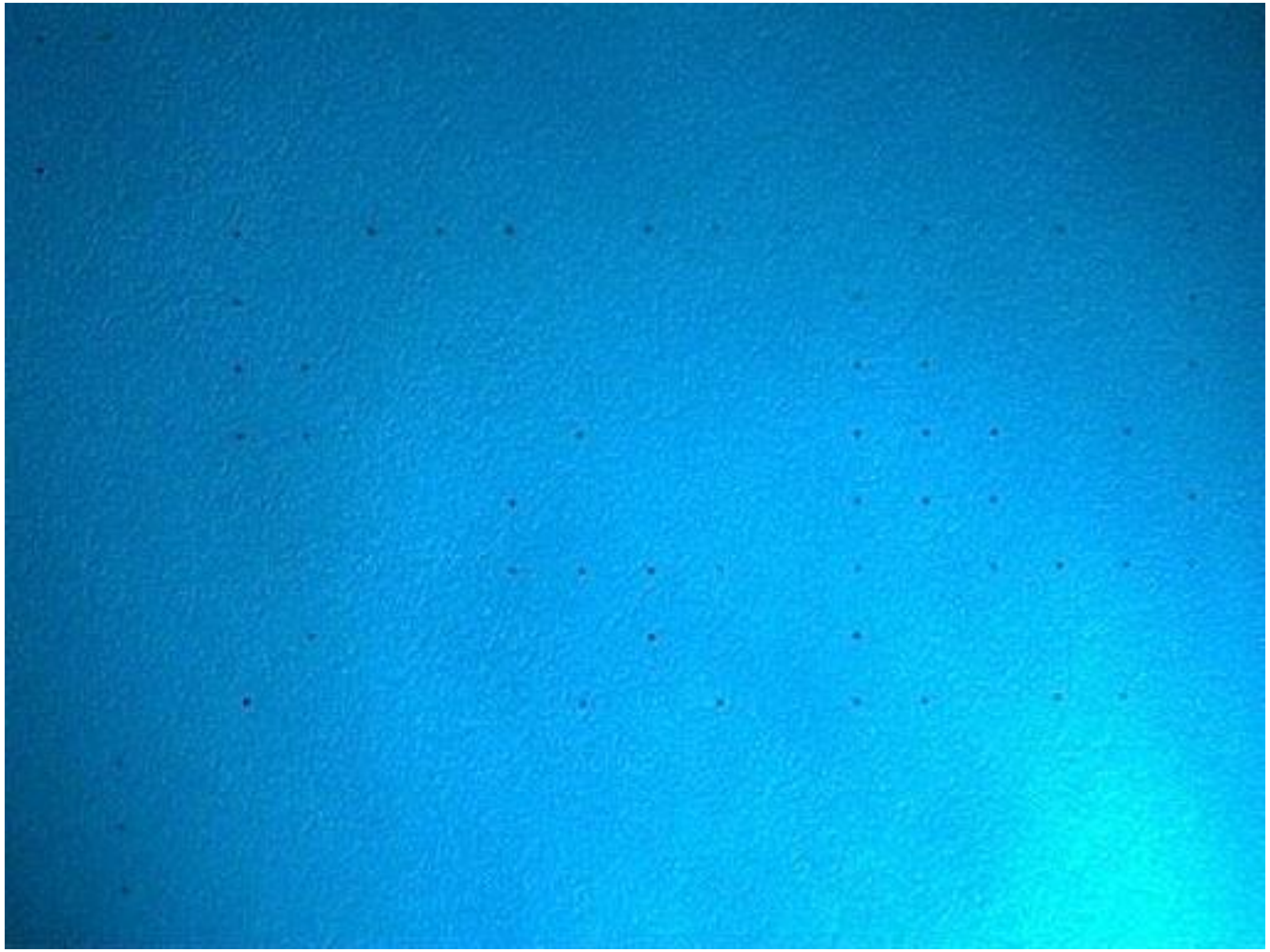
Medical Malpractice

IP Theft

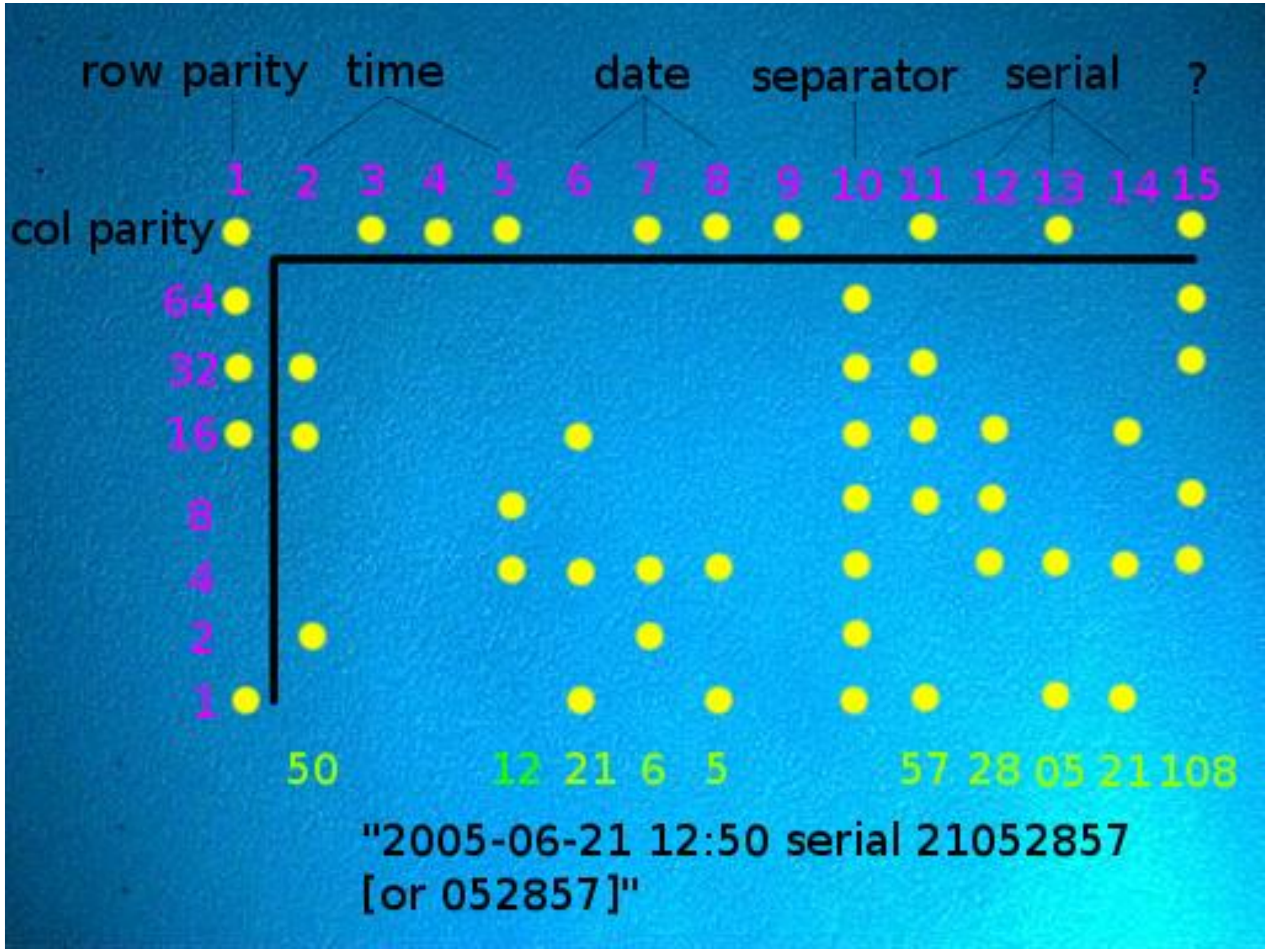
Bankruptcy

# Overview

- Introduction: Why Digital Evidence
- Dealing with Electronic Evidence
- Preservation, Preservation, Preservation
- Conjuring Up Evidence & What To Do About It
- Protocols in Dealing with Electronic Evidence
- Q&A



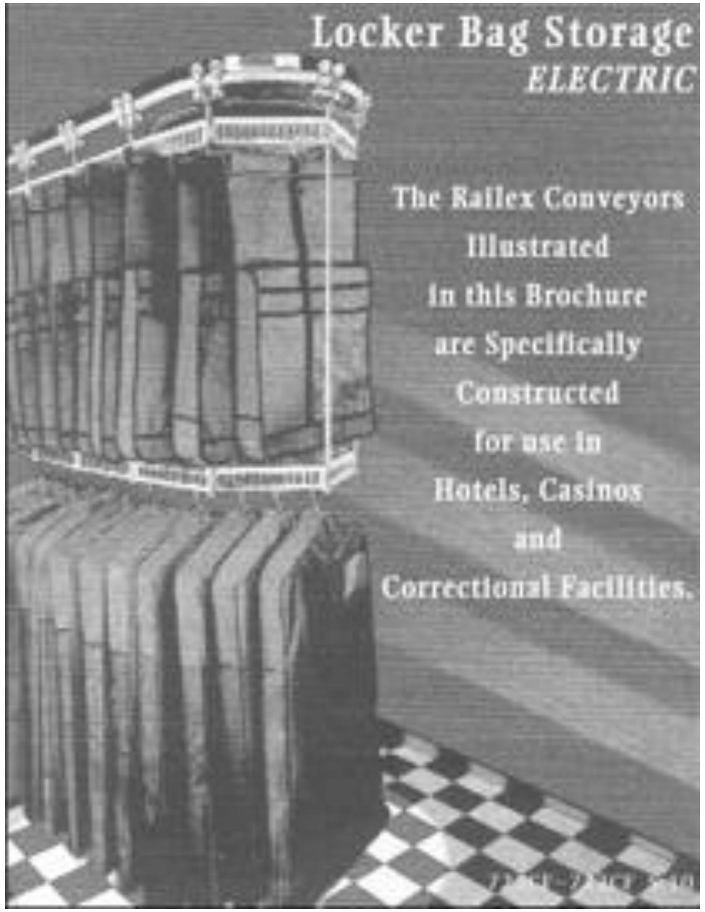
Xerox DocuColor 12 page, magnified 10x and photographed by the QX5 microscope under illumination from a Photon blue LED flashlight



"2005-06-21 12:50 serial 21052857
[or 052857]"

# Quick Case Study

- Wage/Hour Class Action
  - Non-Exempt classified as Exempt
  - Timeframe stretches back 3-4 years



Locker Bag Storage
*ELECTRIC*

The Railex Conveyors
Illustrated
in this Brochure
are Specifically
Constructed
for use in
Hotels, Casinos
and
Correctional Facilities.

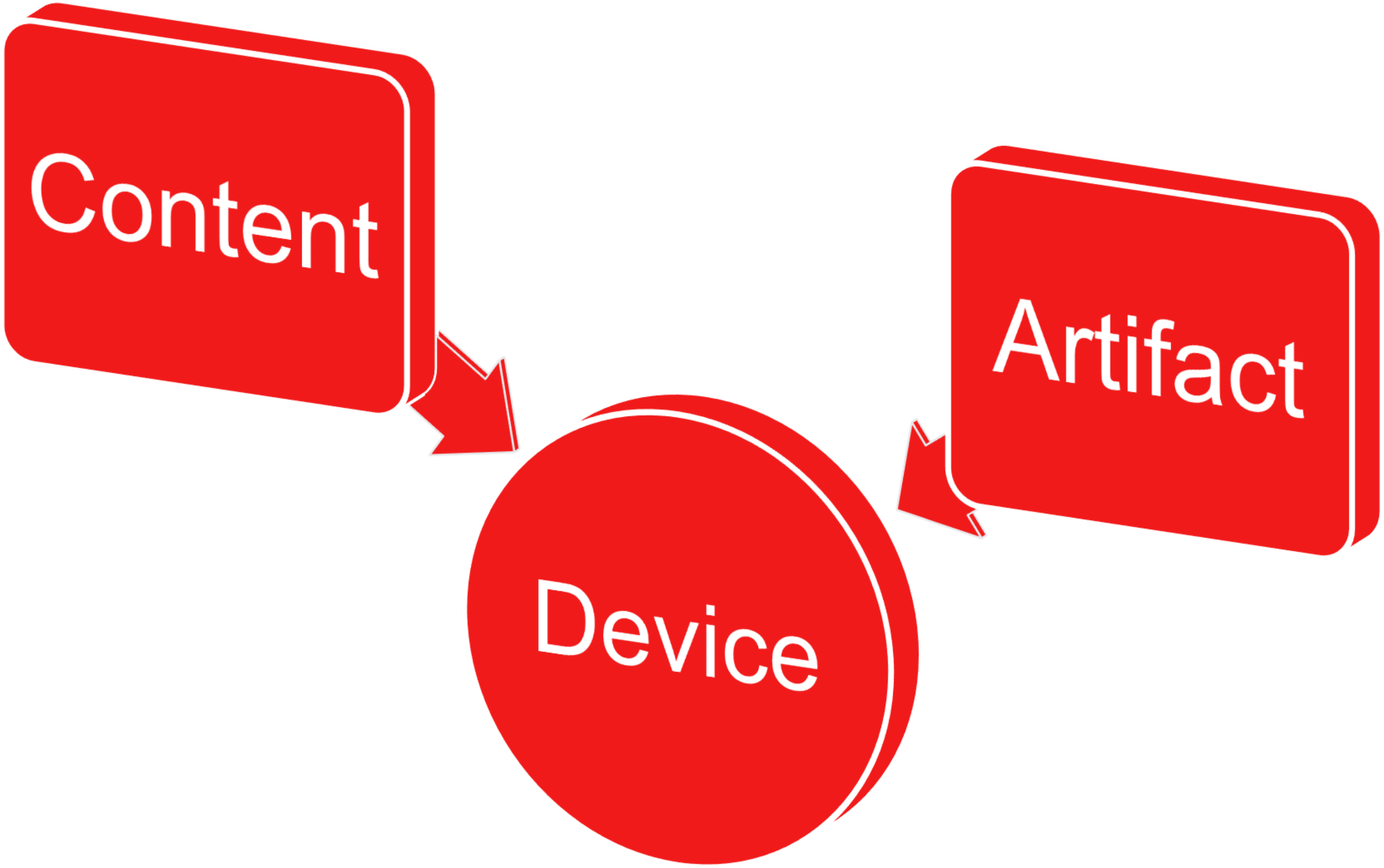
# Still Chasing Content?

- The OSHA Violation that Wasn’t
  - Terminated Employee
  - “Sweetening” the severance package
  - Wild accusations of wrongful acts by corporation

# Dealing with Electronic Evidence

# Locard’s Exchange Principle

In forensic science, Locard’s principle holds that the perpetrator of a crime will bring something into the crime scene ***and*** leave with something from it – both of which can be used as forensic evidence.



Content

Artifact

Device

# A Shift in Mindset

- Devices as Witnesses
  - Content (what someone “says”)
  - Artifact (outside corroboration / “witness”)
  - Simply record what’s going on
    - They don’t lie
      - Although you might need a translator (a GOOD one)
    - Capture significantly more than most people know about

# Dealing with Electronic Evidence

## E-Discovery

- “Managing large volumes”
- Content-centered
- Metadata
- Active Data

## Digital Forensics

- “Investigative”
- Content + Metadata + Artifacts
- Prove “How and What”
- Manipulation
- Deletion/Spoliation
- All Data
- Opinion

# What Digital Forensics Can and Cannot Do

# What You Can Expect

- Content
  - Keyword search for content/communication
    - Historical correspondence
    - Hidden information
    - Deleted information
    - Orphaned information
    - Encrypted information

- Correspondence
  - Memos
  - Emails
  - Instant messages
  - Faxes (yes, still used)
  - Deleted
  - Old and forgotten

- Business Records
  - Financial data
  - Assets
  - Calculations
  - PRIOR DRAFTS
  - DELETED DRAFTS
  - Projections

- Historical Website visited with pictures
- Logins to email and other accounts
- Maps, from Google, and other services
- Historical internet searches and those results

# What You Can Expect

- Conceptual Analysis (Artifact Analysis)
  - How the computer was used

    - IMs
    - E-mails
    - Web-based E-mails
    - Deletion activity
    - Wiping activity
    - Software installed
    - File Transfers (USB or cloud)
    - Attached hardware (mobile devices)
    - Other networks attached
    - Remote Access activity
    - Do we have the “Right” system?

# What You Can Expect

- Condition of evidence
  - Used by others
  - Formatted
  - Re-partitioned
  - Damaged
  - Wiped/Cleansed/Sanitized

# What Digital Forensics Can't Do

- Find evidence that isn't there
  - Never was on this evidence
  - May have been on this evidence but was overwritten
- Deal with Wrong Interpretations
  - Destroyed Server
  - Defragmenting destroyed data
- Prove the Negative (well, maybe)
- Answer the "Who was at the keyboard?" question
  - Some analysis will allow the answer to be inferred.

# What About the Cloud?

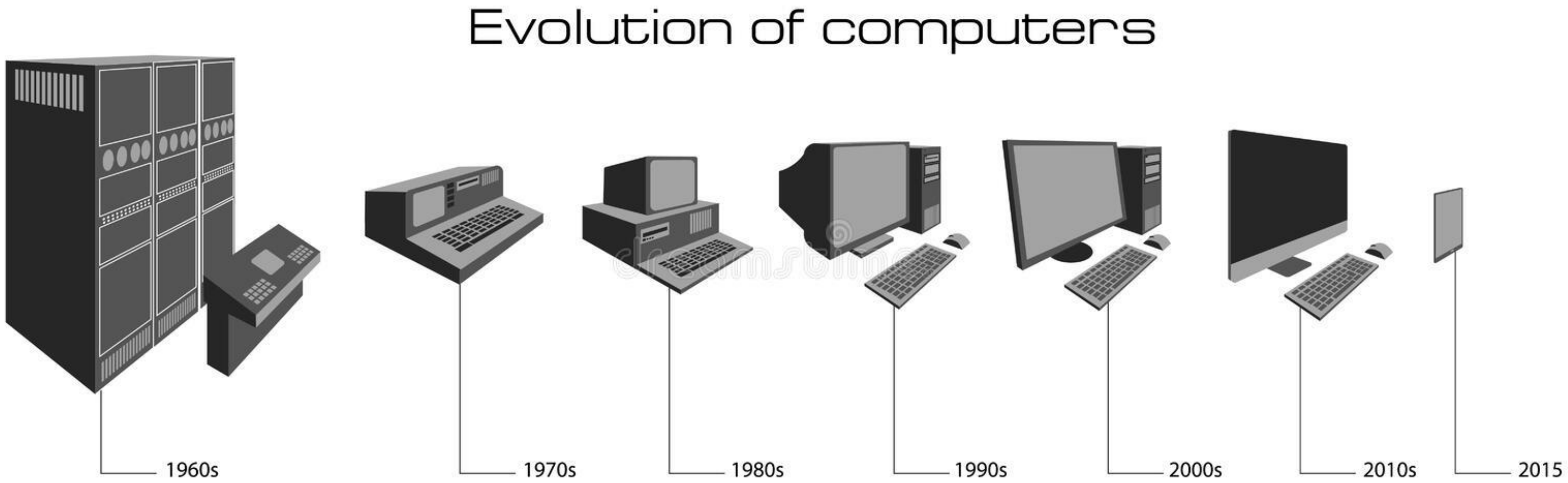
- Content vs Artifacts
  - How long do the artifacts last?
  - How long is deleted content available?
- Deleted data from…
  - Google
  - Outlook.com (including Hotmail)
  - Office 365
  - Cloud repositories

# Takeout Anyone?

- Google Takeout
  - Emails
  - Location data
  - Web history
  - Activity Logs
  - Maps

# How Computers Have Changed

- SSD and deleted data
- What is on the computer vs the cloud
- Encryption



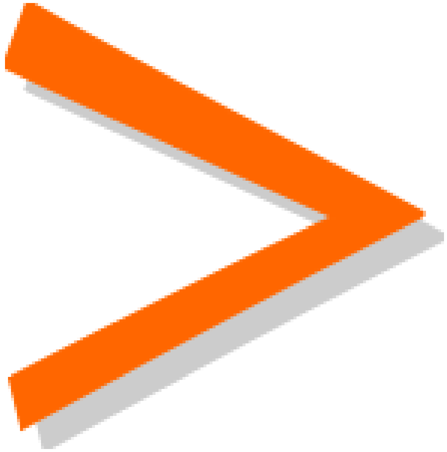
# Preservation

# Early Preservation is Critical

- Continued use of device may alter evidence
- New facts are learned, new theories emerge
  - Avoids having to revisit & re-interrupt
- Evidence doesn't "disappear"
  - Prevent claims of spoliation
  - Gain access to Best Evidence

# Preservation vs Search/Analysis

- Preservation does *not* mean search or analysis
- Can be performed completely independent of search/analysis protocol
- Duty to preserve is greater than duty to disclose



# Evidence Surrounds Us Everywhere

- ISP
- Router/Firewall
- IDS/IPS
- Managed Switches
- Servers
- Workstations
- Cell phones / tablets
- Other monitoring devices (alarm system)
- Log files
- GPS
- Cell Tower Data
- Syslog
- Dropbox
- Box
- Honeypots
- Virtual Machines and hosts
- Office 365
- Network Sniffers
- Backup tapes/disks
- Replication sites
- Disaster Recovery sites
- Digital Scale & other Measuring Devices
- RFID Data
- Gsuite and Takeout
- Video Surveillance
- Payment or other Registration Info

# Mobile Device Considerations

- Type of phone
- Type of data desired
  - Bad source for email
  - Need extensive location data?
  - Messages from Signal
  - Deleted data
- Cloud vs on the phone
- Filtering, privacy, etc.

# Preservation

- First & Foremost: Evidence Preservation
  - Admissibility in Court
  - Protection of All Parties Involved… even the investigator
  - Avoid Contamination/Spoliation of Evidence

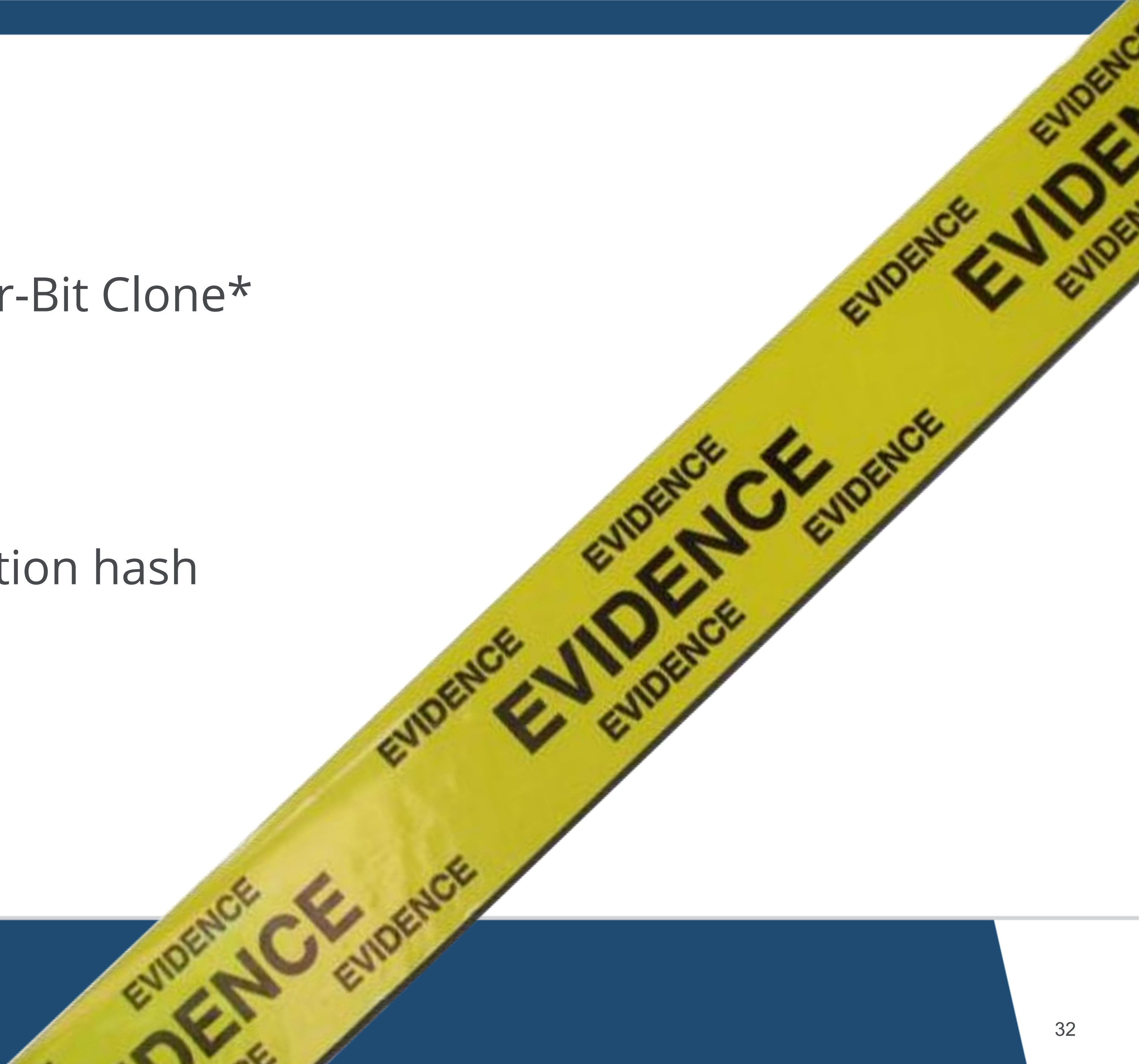
# Preservation

- Completeness
  - “The Whole Truth”
    - Used & Unused (Unallocated) Space
    - Active & Inactive Systems
    - Seemingly “Inaccessible” Systems & Media

# Preservation

- Methodology
  - Forensically-sound Bit-for-Bit Clone*
    - Copy, clone, mirror
  - Write-protect
  - Place on Sterile Media
  - MD5 or other authentication hash
  - Chain of Custody
  - Seal Evidence

*What about cell phones?

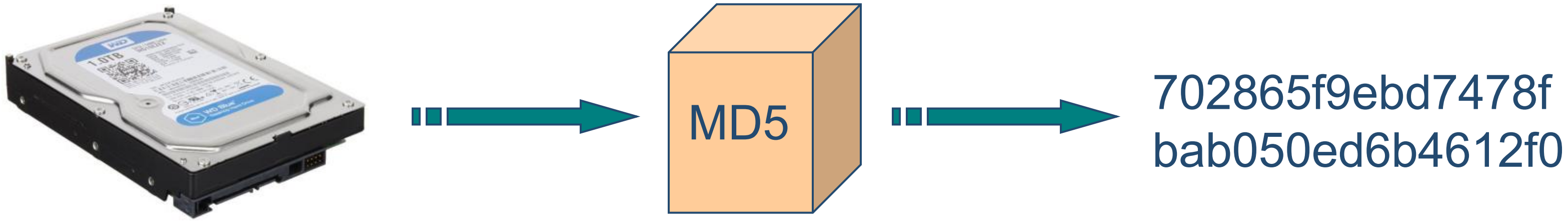


# Preservation

- Authenticate:
  - Prove “no change”
  - Prove Clones ARE the Same
- Method
  - MD5 Hash (digital fingerprint)
    - Industry-standard, industry-recognized
    - 128-bit
    - 1 in $1x10^{38}$ chance for deceiving
      - 100,000,000,000,000,000,000,000,000,000,000,000,000
      - DNA Evidence is 1 in $1x10^{9}$

# Authenticate

- Methodology
  - MD5 Hash – Digital Fingerprint
  - Prove nothing changed



MD5

702865f9ebd7478f
bab050ed6b4612f0

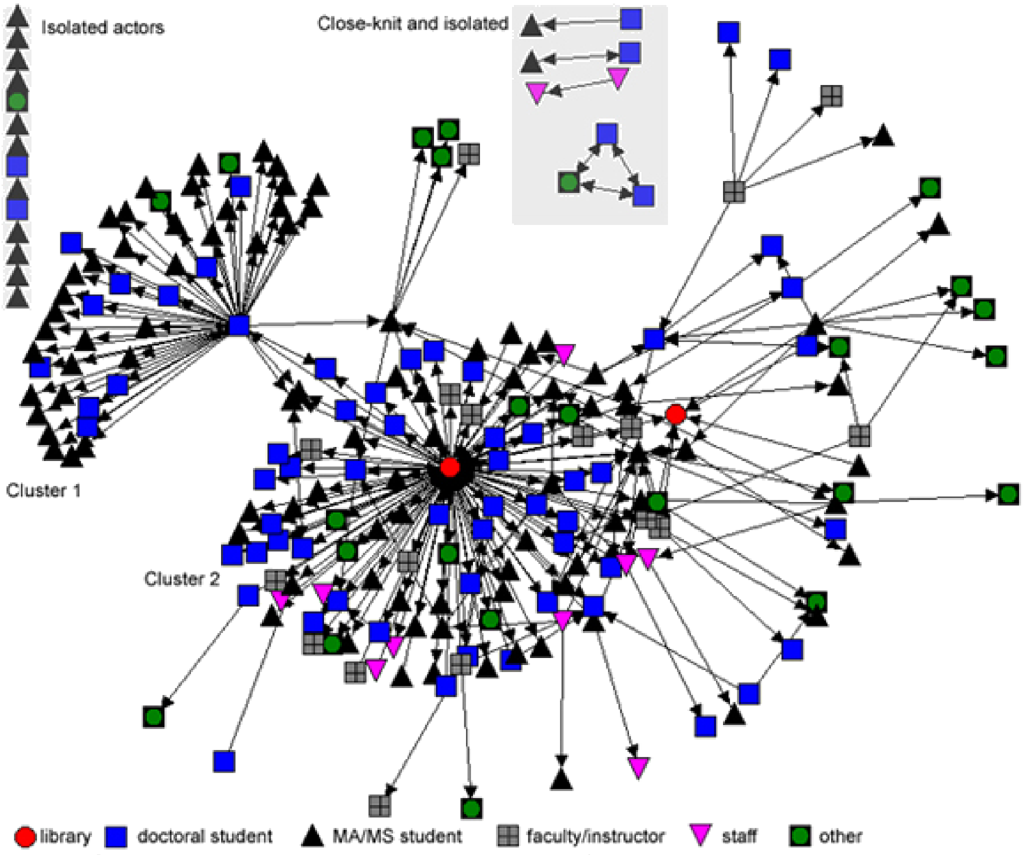
# Analysis: “Getting the Goods”

- Leave No Stone Unturned
  - Used (active) space
  - Unused (inactive/unallocated) space
  - Slack space
  - Deleted – partially, separation of metadata and content
  - Artifacts
  - Printed documents - sometimes
  - E-mail / IM / chat sessions
  - Internet History

# Analysis – Other Data?

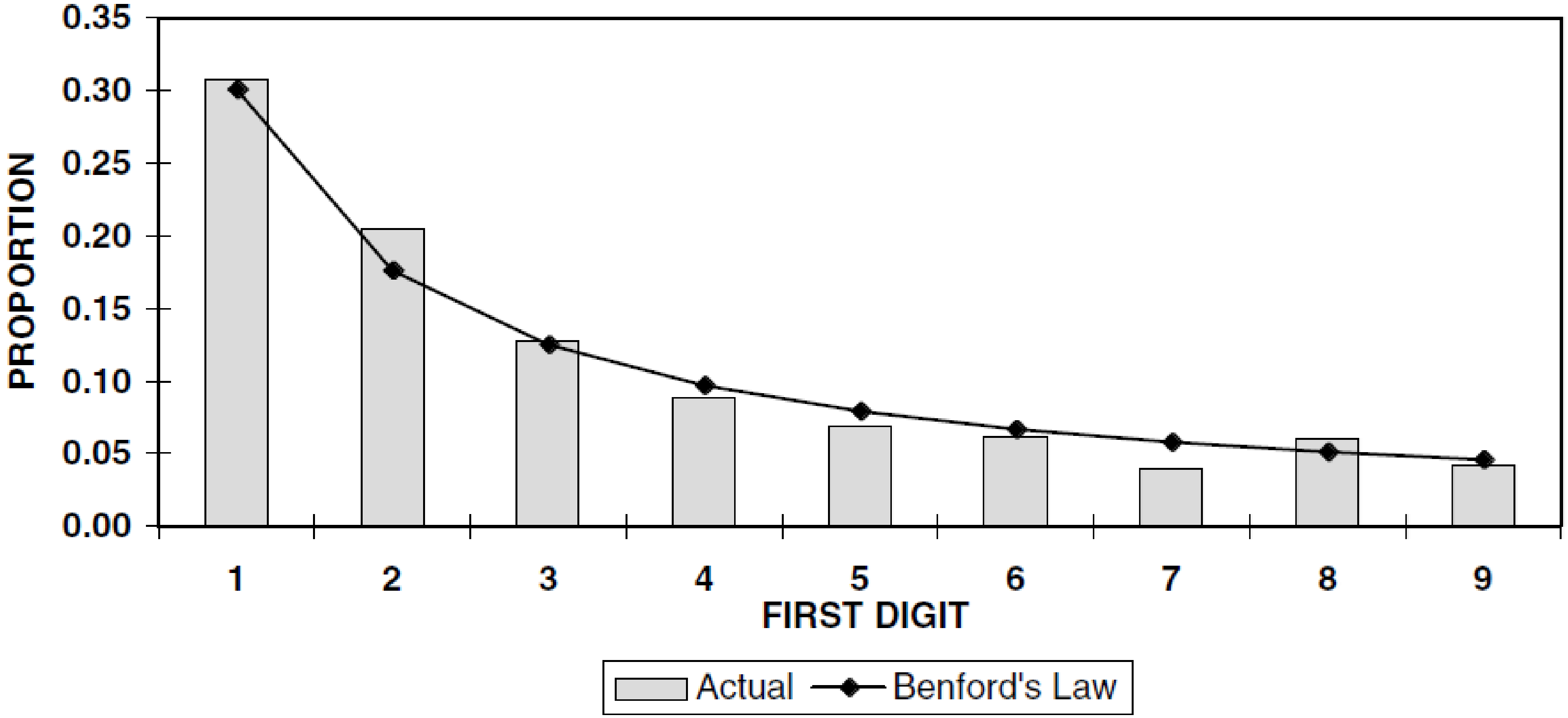
- USB drives used
- Files opened from those drives – names, locations and dates when opened
- Cloud services used

# Social Network Analysis

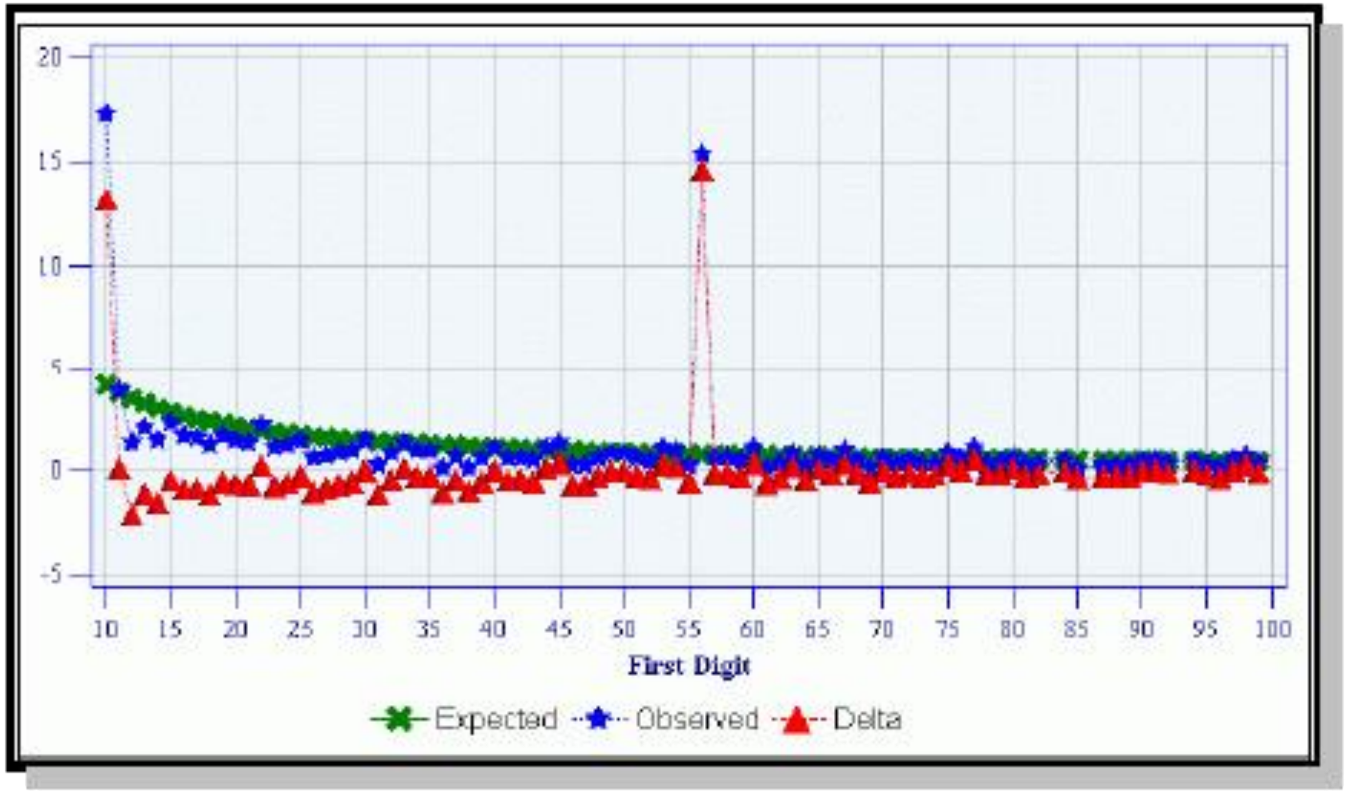


# Financial Analysis

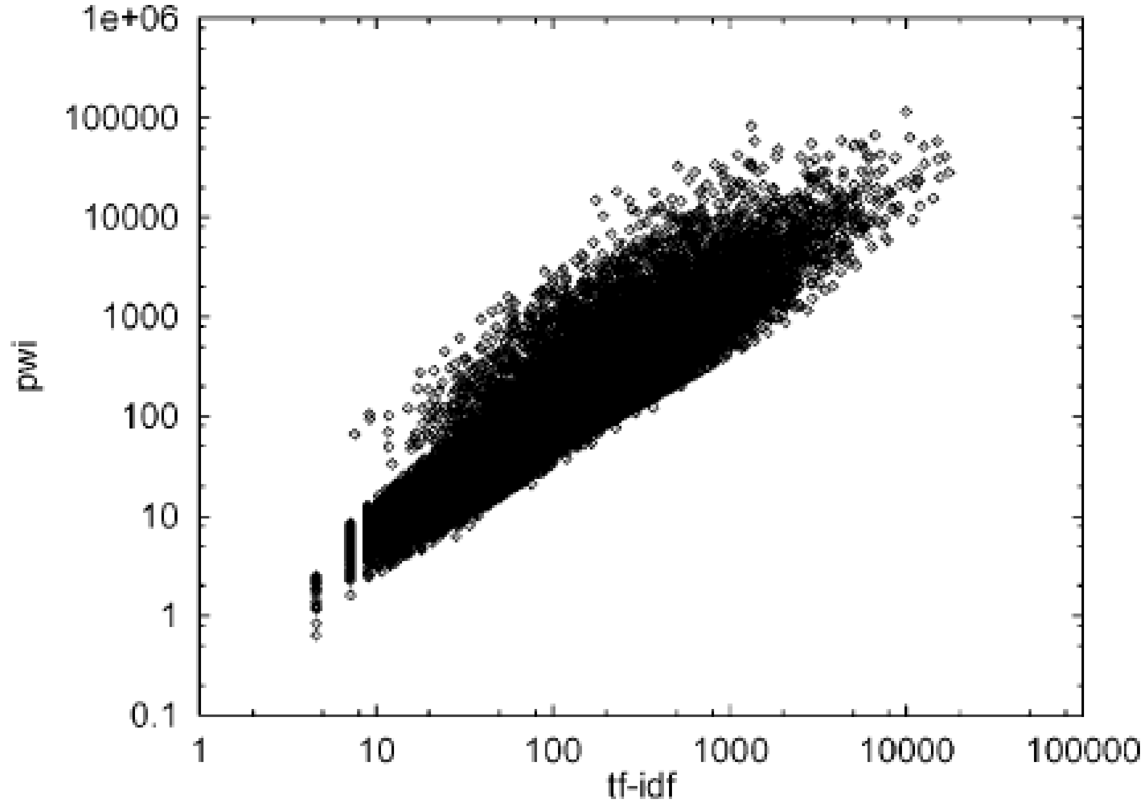
- Benford's Analysis



# Analysis


20
15
10
5
0
-5
10
15
20
25
30
35
40
45
50
55
60
65
70
75
80
85
90
95
100
First Digit
Expected
Observed
Delta

# TF/IDF - *Term Frequency over Inverse Document Frequency*



# Presentation

- Informal
  - Internal Investigations
  - Consulting Experts
- Formal
  - Preliminary Findings
  - Expert Report
  - Affidavits
  - Depositions
  - Expert Testimony
    - Voir Dire process
    - Withstand Daubert-Frye challenge

# Mobile Data Production

- Excel
  - Allows you to sort, filter, search, etc.
  - No balloons
  - Easy to redact
- PDF
  - Feature rich (pictures, balloons)
  - Tough to redact
- Cellebrite UFDR
  - Very flexible on export
  - Learning curve

# Mobile Data Production

- Produce just responsive messages?
- Produce entire conversation?
- Conversation in date range?
- 24 hours before and after message?

BATES' AUTOMATIC

**Numbering Machine.**

DIAL SETTING.

**Numbers Consecutively. Duplicates and Repeats.**

STEEL FIGURES!
PERFECT PRINTING!
ABSOLUTELY ACCURATE!

Indispensable for general office and factory use. *Systematizing and Labor-sav ing.*

**Sent on Ten Days Tria to Responsible Parties.**

Send for circulars. . . . . . .

**Bates Mfg. Co.**

EDISON BUILDING,

BROAD ST., N. Y.
U. S. A.

HIGHEST AWARD—
Medal and Diploma,
World's Fair.

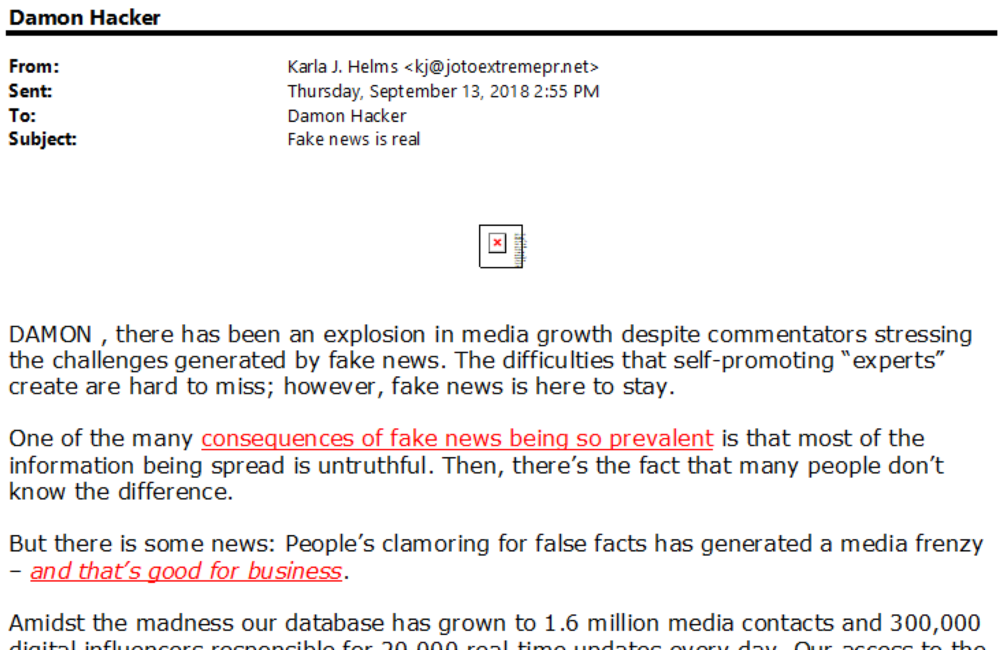
PRICE, FOUR WHEELS, $14

# Conjuring Evidence

…and what to do about it

# E-Mail

- A printout of an e-mail is *not* an e-mail



**Damon Hacker**

**From:** Karla J. Helms <kj@jotoextremepr.net>
**Sent:** Thursday, September 13, 2018 2:55 PM
**To:** Damon Hacker
**Subject:** Fake news is real

DAMON , there has been an explosion in media growth despite commentators stressing the challenges generated by fake news. The difficulties that self-promoting "experts" create are hard to miss; however, fake news is here to stay.

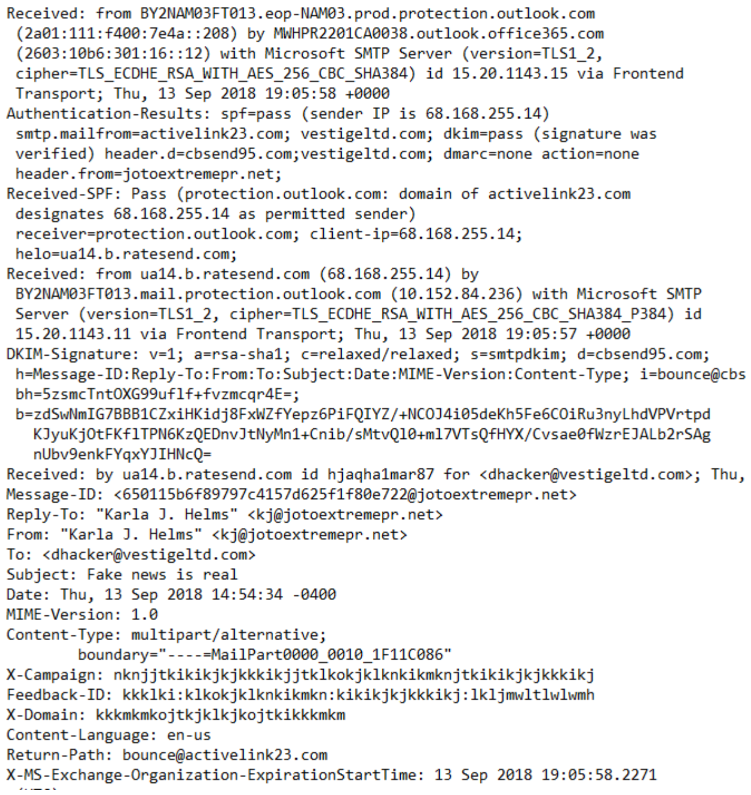
One of the many consequences of fake news being so prevalent is that most of the information being spread is untruthful. Then, there's the fact that many people don't know the difference.

But there is some news: People's clamoring for false facts has generated a media frenzy – *and that's good for business*.

Amidst the madness our database has grown to 1.6 million media contacts and 300,000 digital influencers responsible for 20,000 real-time updates every day. Our access to the

# E-Mail

- Under the Hood
  - IP Addresses
  - Travel Route
  - Authentication Details
  - Application Used
  - Diagnostic Info
  - Links & other Embedded Info
  - MAPI/IMAP & other Protocol Info



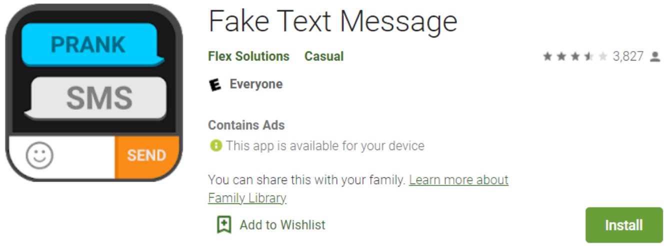
```
Received: from BY2NAM03FT013.eop-NAM03.prod.protection.outlook.com
 (2a01:111:f400:7e4a::208) by MWHPR2201CA0038.outlook.office365.com
 (2603:10b6:301:16::12) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384) id 15.20.1143.15 via Frontend
 Transport; Thu, 13 Sep 2018 19:05:58 +0000
Authentication-Results: spf=pass (sender IP is 68.168.255.14)
 smtp.mailfrom=activelink23.com; vestigeltd.com; dkim=pass (signature was
 verified) header.d=cbsend95.com;vestigeltd.com; dmarc=none action=none
 header.from=jotoextremepr.net;
Received-SPF: Pass (protection.outlook.com: domain of activelink23.com
 designates 68.168.255.14 as permitted sender)
 receiver=protection.outlook.com; client-ip=68.168.255.14;
 helo=ua14.b.ratesend.com;
Received: from ua14.b.ratesend.com (68.168.255.14) by
 BY2NAM03FT013.mail.protection.outlook.com (10.152.84.236) with Microsoft SMTP
 Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384) id
 15.20.1143.11 via Frontend Transport; Thu, 13 Sep 2018 19:05:57 +0000
DKIM-Signature: v=1; a=rsa-sha1; c=relaxed/relaxed; s=smtpdkim; d=cbsend95.com;
 h=Message-ID:Reply-To:From:To:Subject:Date:MIME-Version:Content-Type; i=bounce@cbs
 bh=5zsmcTntOXG99uflf+fvzmcqr4E=;
 b=zdSwNmIG7BBB1CZxiHKidj8FxWZfYepz6PiFQIYZ/+NCOJ4i05deKh5Fe6COiRu3nyLhdVPVrtpd
   KJyuKjOtFKflTPN6KzQEDnvJtNyMn1+Cnib/sMtvQ10+ml7VTsQfHYX/Cvsae0fWzrEJALb2rSAg
   nUbv9enkFYqxYJIHNcQ=
Received: by ua14.b.ratesend.com id hjaqha1mar87 for <dhacker@vestigeltd.com>; Thu,
Message-ID: <650115b6f89797c4157d625f1f80e722@jotoextremepr.net>
Reply-To: "Karla J. Helms" <kj@jotoextremepr.net>
From: "Karla J. Helms" <kj@jotoextremepr.net>
To: <dhacker@vestigeltd.com>
Subject: Fake news is real
Date: Thu, 13 Sep 2018 14:54:34 -0400
MIME-Version: 1.0
Content-Type: multipart/alternative;
        boundary="----=MailPart0000_0010_1F11C086"
X-Campaign: nknjjtkikikjkjkkkikjjtklkokjklknkikmknjtkikikjkjkkkikj
Feedback-ID: kkklki:klkokjklknkikmkn:kikikjkjkkkikj:lkljmwltlwlwmh
X-Domain: kkkmkmkojtkjklkjkojtkikkkmkm
Content-Language: en-us
Return-Path: bounce@activelink23.com
X-MS-Exchange-Organization-ExpirationStartTime: 13 Sep 2018 19:05:58.2271
```

# Screenshots vs Evidence

- Websites can easily produce screenshots
  - Customize phone model, carrier, battery life, etc.
- Altering contacts to fake messages
- Using fake message apps

# Conspicuous Texts

- Insurance matter
- Insured had helpful messages
- Messages were not on manager's phone
- Difficulty in getting access to phone
- Examination of database showed message origin



Fake Text Message

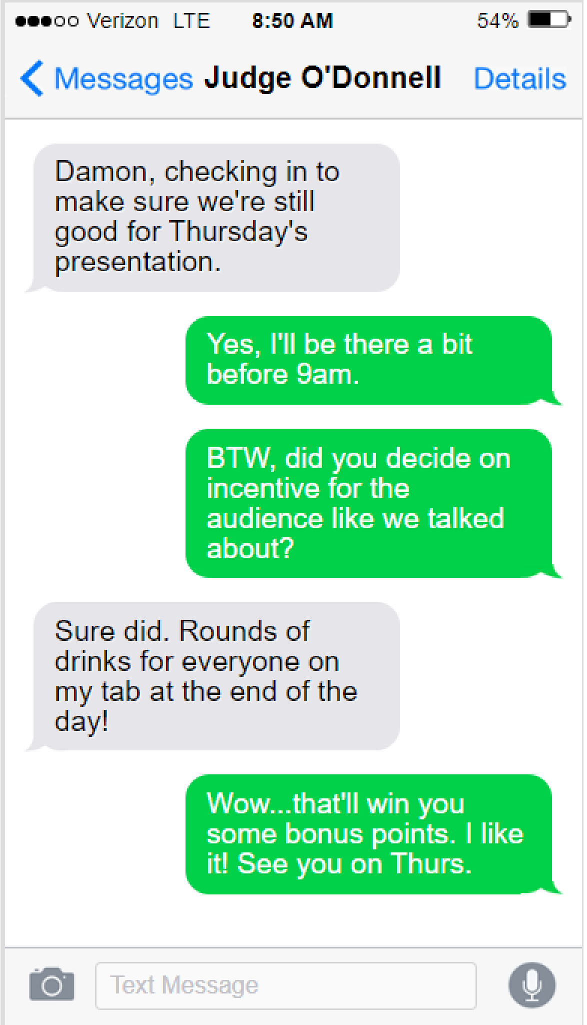
Flex Solutions Casual

Everyone

Contains Ads

This app is available for your device

You can share this with your family. Learn more about Family Library



Judge O'Donnell

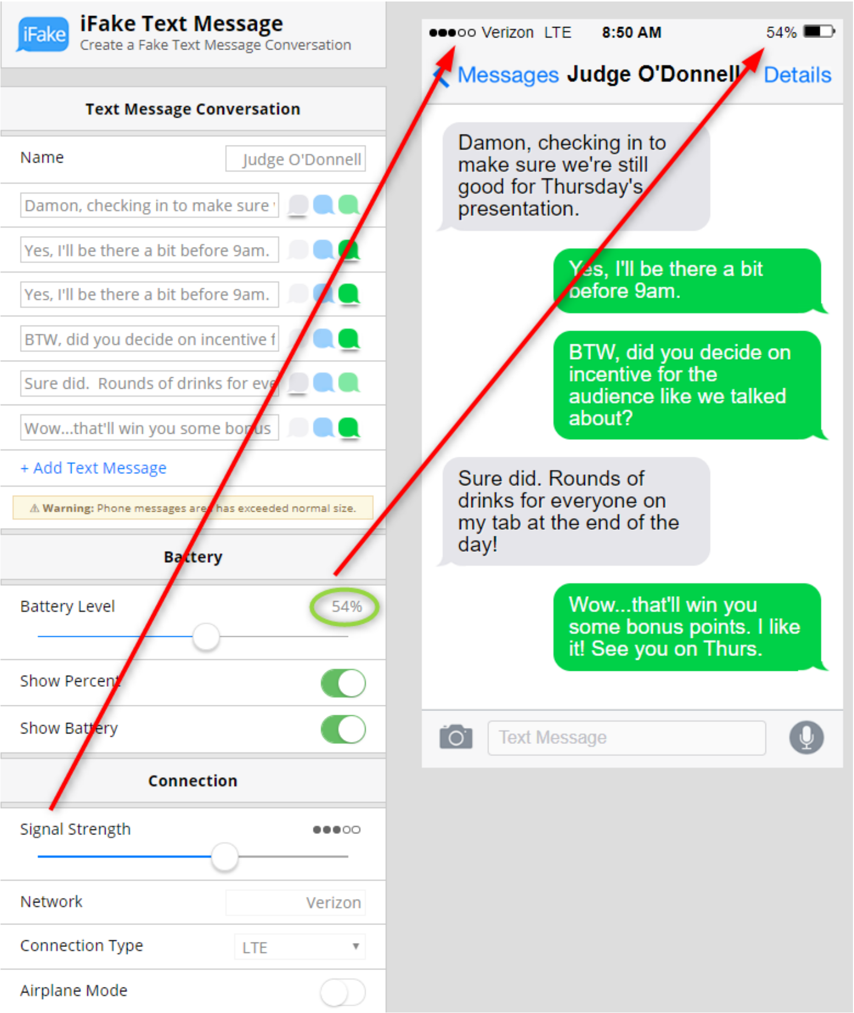
Damon, checking in to make sure we're still good for Thursday's presentation.

Yes, I'll be there a bit before 9am.

BTW, did you decide on incentive for the audience like we talked about?

Sure did. Rounds of drinks for everyone on my tab at the end of the day!

Wow...that'll win you some bonus points. I like it! See you on Thurs.



iFake Text Message
Create a Fake Text Message Conversation

**Text Message Conversation**

Name: Judge O'Donnell

- Damon, checking in to make sure '
- Yes, I'll be there a bit before 9am.
- Yes, I'll be there a bit before 9am.
- BTW, did you decide on incentive f
- Sure did.  Rounds of drinks for eve
- Wow...that'll win you some bonus

+ Add Text Message

⚠ **Warning:** Phone messages are has exceeded normal size.

**Battery**

Battery Level: 54%

Show Percent: ●

Show Battery: ●

**Connection**

Signal Strength: ●●●○○

Network: Verizon

Connection Type: LTE

Airplane Mode: ○

●●●○○ Verizon LTE 8:50 AM 54%

Messages **Judge O'Donnell** Details

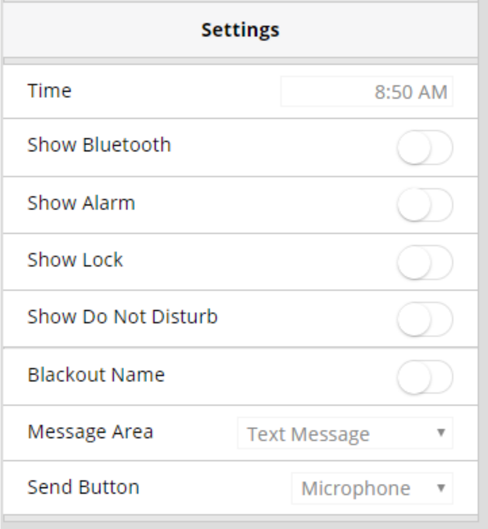
Damon, checking in to make sure we're still good for Thursday's presentation.

Yes, I'll be there a bit before 9am.

BTW, did you decide on incentive for the audience like we talked about?

Sure did. Rounds of drinks for everyone on my tab at the end of the day!

Wow...that'll win you some bonus points. I like it! See you on Thurs.



**Settings**

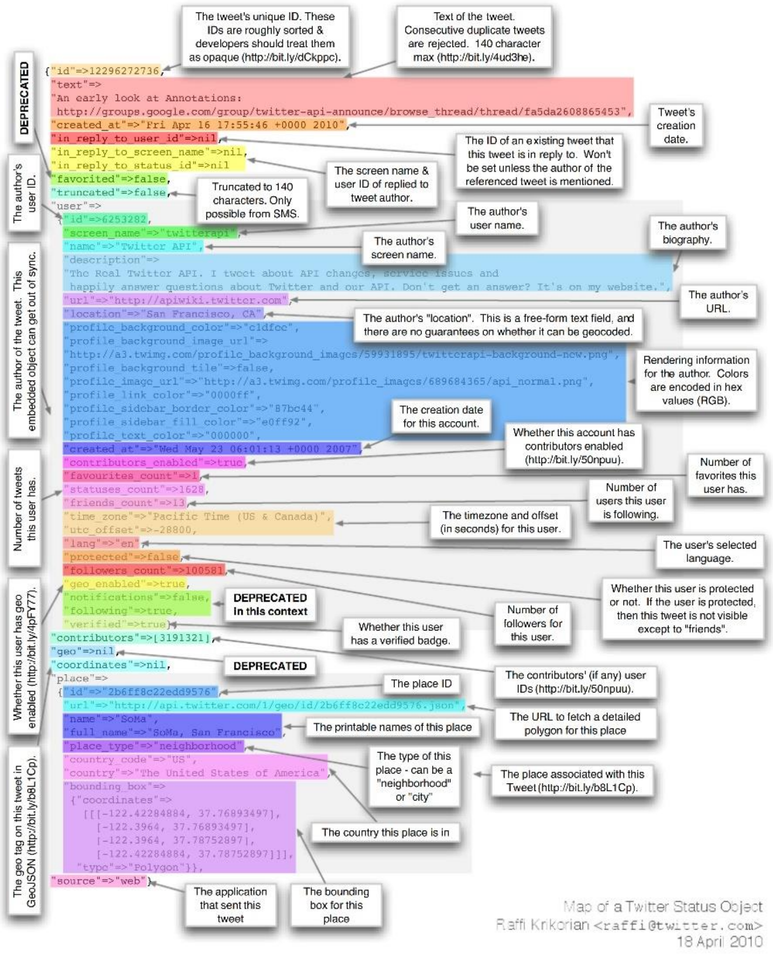
| | |
|---|---|
| Time | 8:50 AM |
| Show Bluetooth | ○ |
| Show Alarm | ○ |
| Show Lock | ○ |
| Show Do Not Disturb | ○ |
| Blackout Name | ○ |
| Message Area | Text Message |
| Send Button | Microphone |

# Twitter Math

- When does 280 not equal 280?

This message is 280 characters long. It is a demonstration to show the amount of data that can exist within a single Tweet. Short & Sweet! The preceding exclamation point is the old limit of 140 characters. Currently Tweets may contain 280 characters giving you more to play with

# Anatomy of a Tweet



```
{"id"=>12296272736,
 "text"=>
 "An early look at Annotations:
 http://groups.google.com/group/twitter-api-announce/browse_thread/thread/fa5da2608865453",
 "created_at"=>"Fri Apr 16 17:55:46 +0000 2010",
 "in_reply_to_user_id"=>nil,
 "in_reply_to_screen_name"=>nil,
 "in_reply_to_status_id"=>nil
 "favorited"=>false,
 "truncated"=>false,
 "user"=>
  {"id"=>6253282,
   "screen_name"=>"twitterapi",
   "name"=>"Twitter API",
   "description"=>
   "The Real Twitter API. I tweet about API changes, service issues and
    happily answer questions about Twitter and our API. Don't get an answer? It's on my website.",
   "url"=>"http://apiwiki.twitter.com",
   "location"=>"San Francisco, CA",
   "profile_background_color"=>"c1dfce",
   "profile_background_image_url"=>
   "http://a3.twimg.com/profile_background_images/59931895/twitterapi-background-new.png",
   "profile_background_tile"=>false,
   "profile_image_url"=>"http://a3.twimg.com/profile_images/689684365/api_normal.png",
   "profile_link_color"=>"0000ff",
   "profile_sidebar_border_color"=>"87bc44",
   "profile_sidebar_fill_color"=>"e0ff92",
   "profile_text_color"=>"000000",
   "created_at"=>"Wed May 23 06:01:13 +0000 2007",
   "contributors_enabled"=>true,
   "favourites_count"=>1,
   "statuses_count"=>1628,
   "friends_count"=>13,
   "time_zone"=>"Pacific Time (US & Canada)",
   "utc_offset"=>-28800,
   "lang"=>"en",
   "protected"=>false,
   "followers_count"=>100581,
   "geo_enabled"=>true,
   "notifications"=>false,
   "following"=>true,
   "verified"=>true},
 "contributors"=>[3191321],
 "geo"=>nil,
 "coordinates"=>nil,
 "place"=>
  {"id"=>"2b6ff8c22edd9576",
   "url"=>"http://api.twitter.com/1/geo/id/2b6ff8c22edd9576.json",
   "name"=>"SoMa",
   "full_name"=>"SoMa, San Francisco",
   "place_type"=>"neighborhood",
   "country_code"=>"US",
   "country"=>"The United States of America",
   "bounding_box"=>
    {"coordinates"=>
      [[[-122.42284884, 37.76893497],
        [-122.3964, 37.76893497],
        [-122.3964, 37.78752897],
        [-122.42284884, 37.78752897]]],
     "type"=>"Polygon"}},
 "source"=>"web"}
```

The tweet's unique ID. These IDs are roughly sorted & developers should treat them as opaque (http://bit.ly/dCkppc).

Text of the tweet. Consecutive duplicate tweets are rejected. 140 character max (http://bit.ly/4ud3he).

Tweet's creation date.

DEPRECATED

The ID of an existing tweet that this tweet is in reply to. Won't be set unless the author of the referenced tweet is mentioned.

The screen name & user ID of replied to tweet author.

Truncated to 140 characters. Only possible from SMS.

The author's user ID.

The author's user name.

The author's biography.

The author's screen name.

The author's URL.

The author's "location". This is a free-form text field, and there are no guarantees on whether it can be geocoded.

The author of the tweet. This embedded object can get out of sync.

Rendering information for the author. Colors are encoded in hex values (RGB).

The creation date for this account.

Whether this account has contributors enabled (http://bit.ly/50npuu).

Number of favorites this user has.

Number of users this user is following.

Number of tweets this user has.

The timezone and offset (in seconds) for this user.

The user's selected language.

Whether this user is protected or not. If the user is protected, then this tweet is not visible except to "friends".

DEPRECATED in this context

Number of followers for this user.

Whether this user has a verified badge.

Whether this user has geo enabled (http://bit.ly/4pFY77).

DEPRECATED

The contributors' (if any) user IDs (http://bit.ly/50npuu).

The place ID

The URL to fetch a detailed polygon for this place

The printable names of this place

The type of this place - can be a "neighborhood" or "city"

The place associated with this Tweet (http://bit.ly/b8L1Cp).

The country this place is in

The geo tag on this tweet in GeoJSON (http://bit.ly/b8L1Cp).

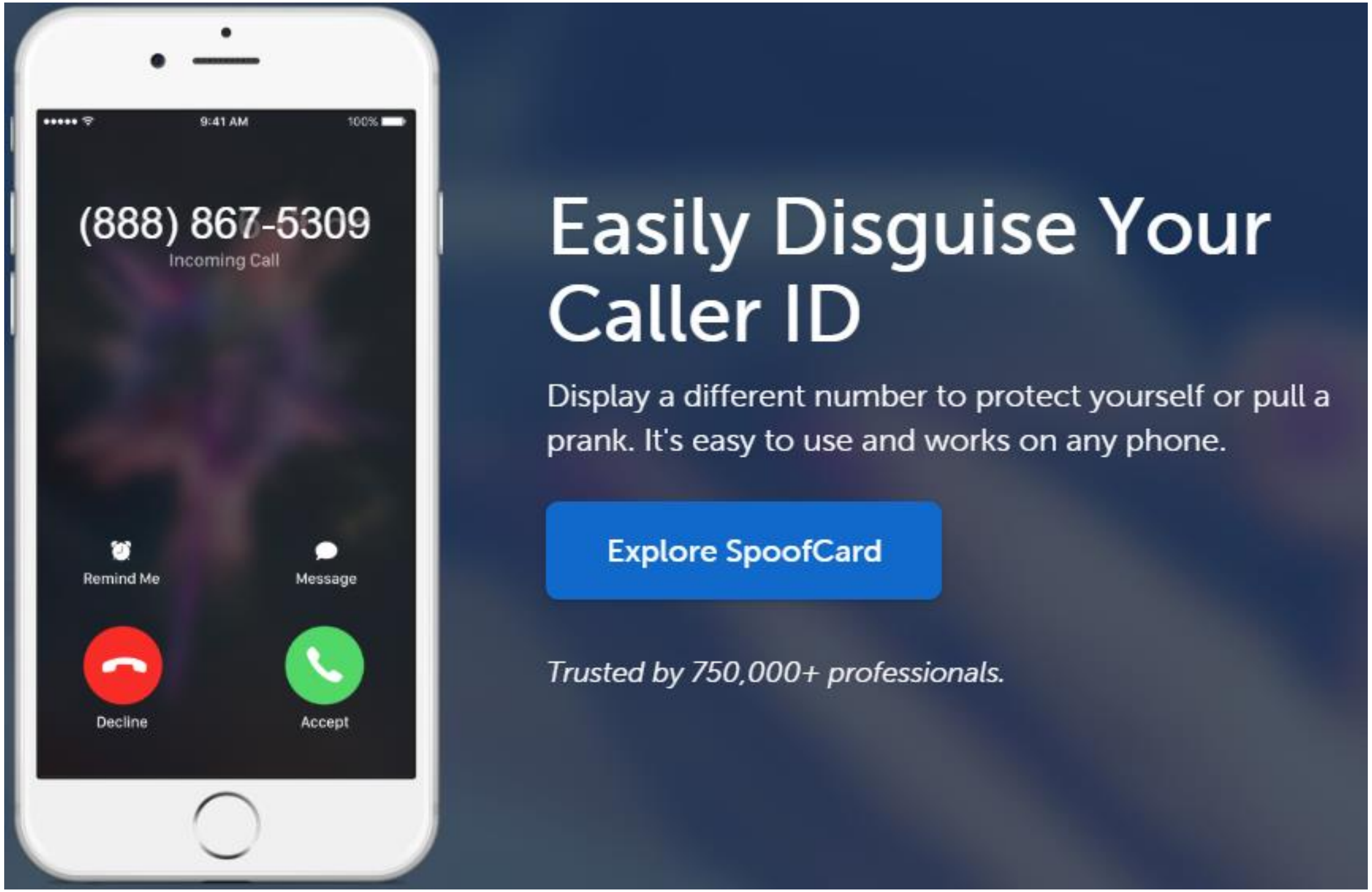
The application that sent this tweet

The bounding box for this place

Map of a Twitter Status Object
Raffi Krikorian <raffi@twitter.com>
18 April 2010

- Unique Tweet ID
- Screen name of user ID of reply
- Author's user name
- Author's screen name
- Author's location (free-form)
- Author's biography
- Creation date of account
- Timezone
- Number of users author is following
- Number of favorites this user has
- User's language
- Number of followers this user has
- Geolocation Info
- Application that sent the Tweet

*And probably more…*



# Easily Disguise Your Caller ID

Display a different number to protect yourself or pull a prank. It's easy to use and works on any phone.

*Trusted by 750,000+ professionals.*

# What to Do About It

- First:  Awareness
- Understand visual inspection is *unlikely* to reveal forgeries
- Recognize things may look differently based upon platform (Windows vs Mac, mobile vs. workstation), application (Outlook vs Outlook Express), etc.

# What to Do About It

- Recognize artifacts *likely* exist
- Insist on source documents
- Obtain “Best Evidence” – printouts are rarely it
- If in doubt, get a trained professional to assist

# Protocols for Handling ESI

# Protocol

- Make clear “Preservation is *not* search/analysis” & duty to preserve is greater than to produce
- Bifurcate data into:
  - Content
  - Artifacts

# Protocol

- Once processed, CONTENT goes back to Producing party for review, redaction & production
  - Creation of Privilege and Relevancy Log
- ARTIFACT analysis produced to both parties contemporaneously
  - Artifacts are not communication from an attorney,
  - Artifacts are not advice received from attorney,
  - No forms of privilege attach

# Protocol

- Protocol should include:
  - Reasonable Timeframe for review
  - Facility for *in camera* inspection
  - Privilege and Relevancy Log should require enough specificity
  - Consider "summary" of population turned over going to both sides
    - i.e.  On December 6, processor turned over to Producing party 6,430 items, broken down as:  X PDF, Y e-mails, Z Word documents, etc.

# Protocol

- Protocol should consider:
  - Production Form (native? PDF/TIFF?, inclusion of metadata?)
  - Compelled Disclosure clause

# Q&A

What else can I answer that we haven’t discussed?

# We’d love to hear from you!

Damon Hacker, MBA, CISA, CSXF, CMMC-RP
President

dhacker@archerhall.com
(855) 839-9084

ArcherHall
AIM HIGH