MARYMAN®

INCIDENT RESPONSE · INVESTIGATIONS · DIGITAL FORENSICS

Evidence Can Change the Direction of a Case in a Heartbeat

2026 Estate Planning and
Trust Council of Long Beach

JOSEPH S. GREENFIELD, PH.D.

- President/Chief Forensic Examiner
- Associate Professor of Practice,
  University of Southern California
  - Developed the first cyber security program at USC (2009)
  - Developed a minor in computer & Digital Forensics (2012)
  - Co-created bachelor's degree in Intelligence and Cyber Operations
- Testified as a Digital Forensics Expert Witness in California, Federal, and International Courts

OVERVIEW

- How to establish scope of a cyber investigation
- What to expect in the digital forensic investigation
- How to make the most out of working with a digital forensic examiner
- What are some of the most common mistakes
- Tips for Fiduciaries
- Tales from the frontlines – don’t be a horror story!

What is Digital Forensics?

"Scientific acquisition, analysis, and preservation of data contained in electronic media."

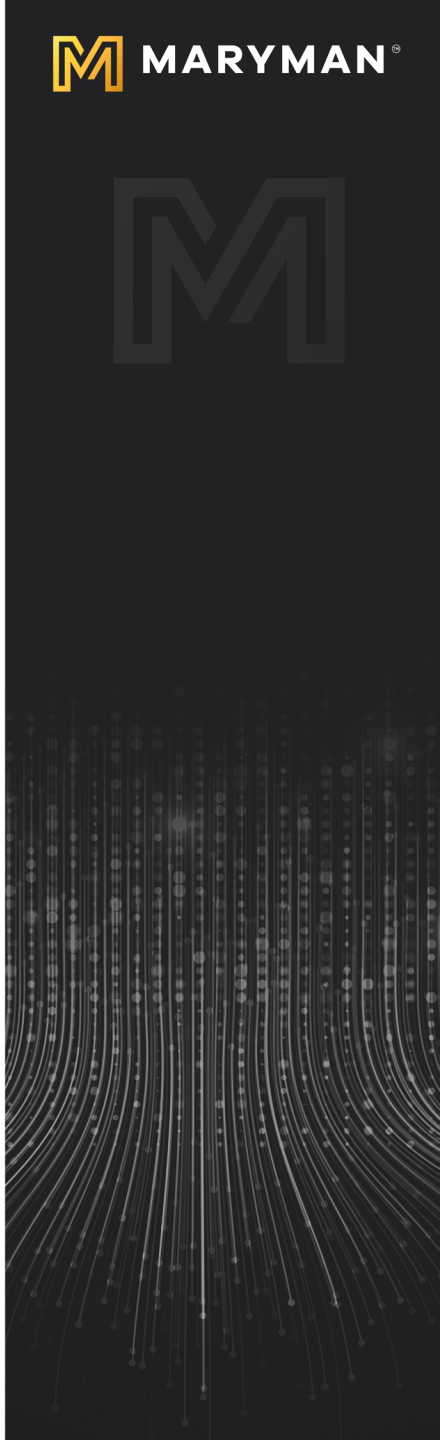
- We answer the Who, What, Where, When, and How
- Goals
  - **Preserve evidence** so it can be used **in a court of law**
  - Perform **scientifically valid** and **repeatable analysis** (Daubert and Frye)
- We use methodologies, procedures, tools, and techniques specific to digital forensics that can withstand scrutiny
- We provide truth of data in an increasingly artificial world

Digital Forensics: What Can We Find?

<u>Devices</u>
- Computers & Laptops
- Cell Phones
- Tablets
- Servers
- Cloud
- GPS
- Security Systems
- Smoking gun!

<u>Data</u>
- Deleted
- Hidden
- Obscured

<u>Digital fingerprints</u>
- Timestamps
- If data was deleted
- Who touched what
- Who changed what
- Is this thing real?



Digital Forensics – Typical Requests for Fiduciaries and Estate Matters

- Authenticating Email, Text Message, Document
- Recovering deleted emails and/or text messages
- Spyware on devices
- Compromised accounts (email, banking, etc.)
- Financial fraud
- Rebutting the opposition

When was the last time you had a trustee and/or beneficiary that did not own a cell phone, computer, laptop, email?

Planning For Digital Forensics

Finding the right firm and right fit

- IT should not be doing forensics or testifying
- Independent and free of conflicts
- Availability
- Experience
- Experience in testimony
- Empathy

When should you call?

- As soon as there is any suspicion of digital malfeasance

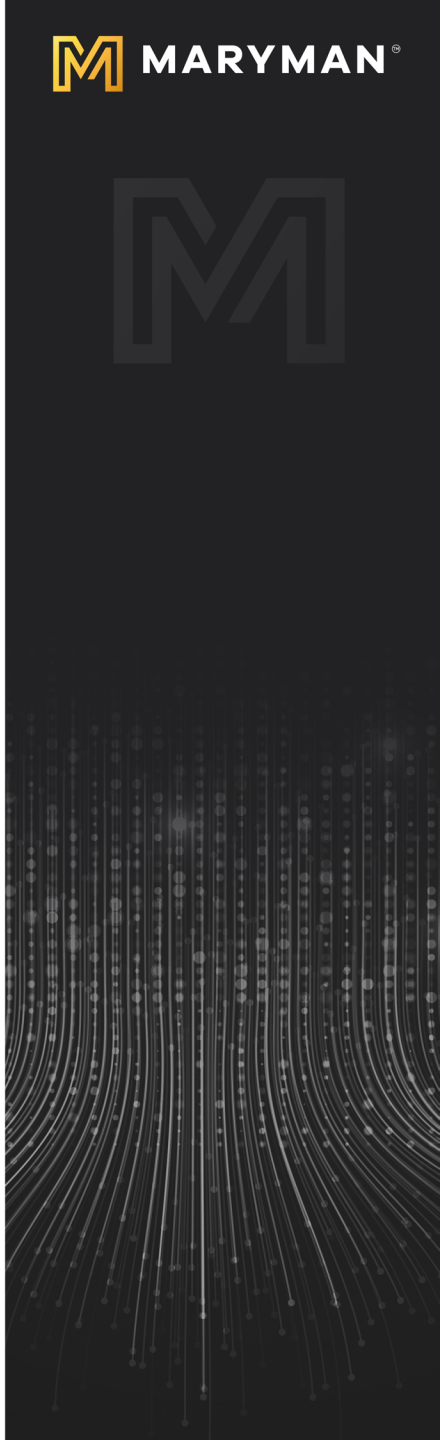
Preparing You and Involved Persons for Digital Forensics

Tell your client and their IT:

- Don’t delete anything
- Don’t change anything
- Stop using the device
- Don’t look for anything
- Step away from the keyboard! (if possible)
- Forensic preservation has its own timeline
- Estimates are just estimates
- Preservations can take between 24 – 48 hours

Email account and cloud account collection

- Admin access (business)
- Password(s)
- MFA coordination
- Tools for remote authentication
- Personal accounts have limited logging!



Digital Forensics – Scope and Analysis

Scope

- Extremely important for both analysis and eventual testimony
  - A skilled forensic examiner will establish and clarify the scope
  - Defining the scope will define the cost
  - If it is out of scope, it will not be examined and will not be subject to testimony
- Example scopes
  - Produce all messages to/from individuals between the following dates
  - Determine all files that were deleted between the following dates
  - Determine all word documents and PDFs that were viewed and edited
  - Determine if any files were copied to a USB device, especially during the following timeframe
  - Determine if malware/spyware was installed and by whom

Analysis

Digital forensic analysis can take days or weeks

- Depends on device(s) and scope

Common Mistakes and Challenges

Most common: We are given incorrect information

- Expectations are not clearly communicated
- Given the wrong device, file, email account, etc.
- Overly broad scope – distracts from the purpose of the investigation
- Find “all the bad stuff”
    - Overly broad is time consuming and often leads to much higher costs
- Asking to change evidence to help the client
- Asking to lie
- Asking to testify based on someone else’s examination (the client/IT)

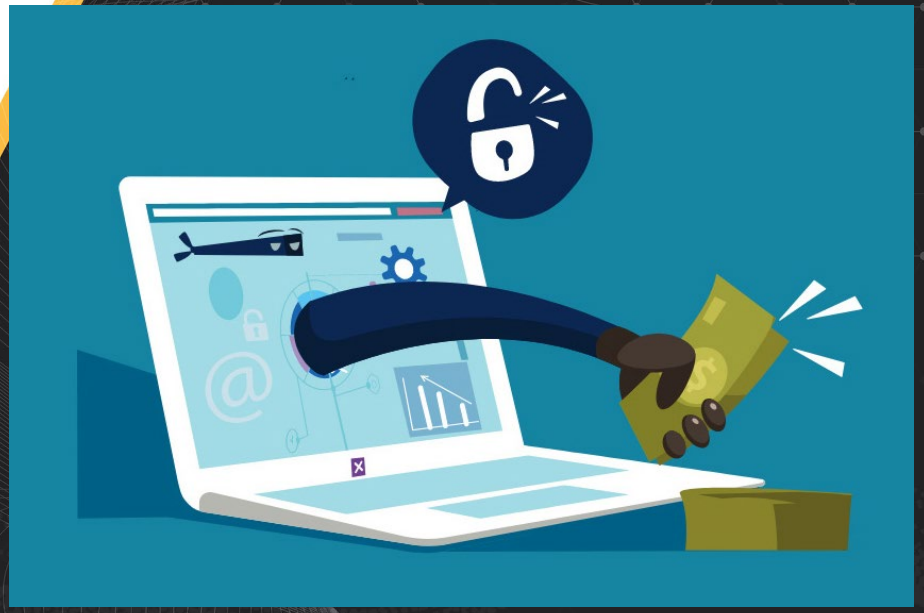
Tips For Fiduciaries

- Business Email Compromise / Wire Transfer Fraud
  - Single biggest concern for all individuals and businesses
  - Strongly recommend using a business email system (Google Workspace, Microsoft 365)
- DocuSign or other electronic signature systems
  - Verify electronic signatures!
  - DocuSign'ed documents have predictable metadata
- Emails can be spoofed
  - Simple to make an email appear to come from legitimate person
  - Forensics will want to review entire email, including the full email header
  - Talk to your IT about SPF, DKIM, and DMARC
- Multi-Factor Authentication (MFA) Everywhere!
  - Use authenticator app instead of text/SMS
- Use your enterprise password manager to store credentials
  - You probably need a copy of key personnel phone PINs, passcodes, break-glass passwords, etc.)

Tales From The Frontlines

Client lost over $30 million due to Business Email Compromise and Wire Transfer Fraud

- Bookkeeper went on vacation
- Backup personnel had their email accounts spammed for two weeks
- Bookkeeper came back from vacation, found entire investment account was drained
- What happened?!?
  - Assistant controller received phishing email – clicked the link, entered credentials
  - Hackers read emails for two weeks
  - Hackers sent fraudulently signed documents to the bank to add an authorized signer
  - Hackers spam-flooded client to hide the wire transfers
  - We empowered litigators towards a successful mediation with the bank – **90% recovery!**



Additional Topics

- Don’t forget about backups and logs!
  - iCloud, iTunes Backups, etc.?
  - IT backups?
  - If it has been deleted on the phone, it may still be on the computer
  - During litigation, inspection demands for opposing computer systems should include mobile backups, logs, etc.
- Don’t forget about cloud storage
  - Google Drive, iCloud, Dropbox, OneDrive, etc.
- Deleting a file leaves **evidence of deletion**, which can **violate a preservation/protection order**
  - The deletion is sometimes worse than the original data
- When was the last time you changed your passwords?
  - Are you using a password manager?

MARYMAN®

THANK YOU!

Joseph S. Greenfield, PhD.

President/Chief Forensic Examiner

310-738-8788

jgreenfield@maryman.com

www.maryman.com