MIDDLESEX COUNTY DISTRICT ATTORNEY’S OFFICE

DIGITAL EVIDENCE LAB

Carl Schiller, Jeff Martin, Mel Ortiz
Kristen Noto, Lab Director

DIGITAL EVIDENCE LAB

- What is the MDAO Digital Evidence Lab?
  - A fully trained, fully staffed, digital forensics lab
  - Assist with the extraction and analysis of data from digital devices

DIGITAL EVIDENCE LAB

- Capabilities Overview
  - Search Warrant Assistance
  - Computer Forensics
  - Smart Phone Extraction & Analysis
  - DVR / NVR Surveillance Video Extraction & Analysis
  - Database Analysis

DIGITAL EVIDENCE LAB

- Search Warrant Assistance
  - Technical and Legal review of Search Warrant
  - Technical Assistance with serving SW
    - Technically sound data collection
    - On-site previews to narrow scope of evidence collection
    - Minimizes challenges at trial to law enforcement’s methods of preserving evidence

DIGITAL EVIDENCE LAB

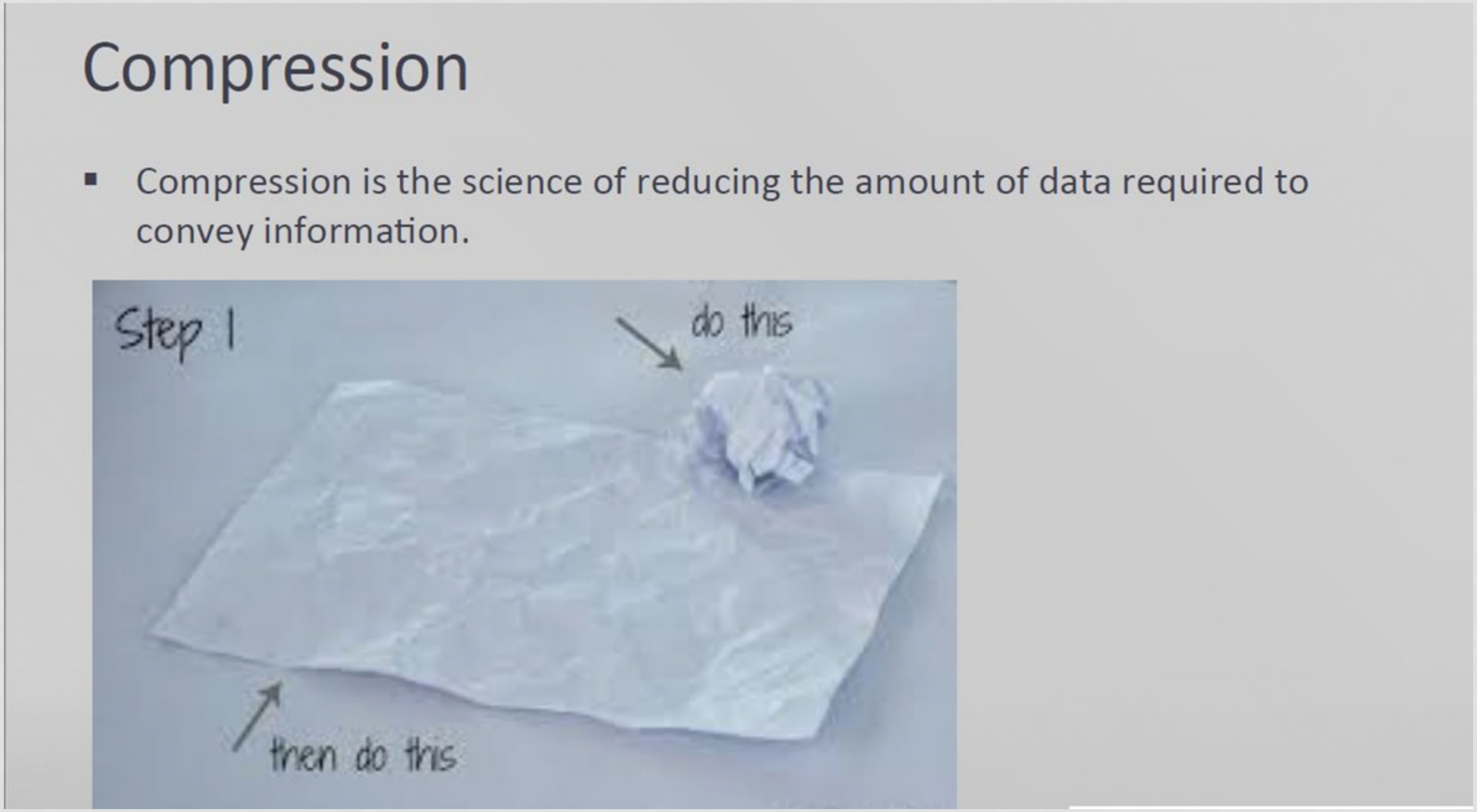
- Computer Forensics
  - PC / Mac
  - Linux Machines
  - Network Forensics
  - Internal and External Storage
  - Data Recovery
  - Memory (RAM) Capture

DIGITAL EVIDENCE LAB

- Surveillance Video / Cell Phone Video
  - CFVT (LEVA: Law Enforcement Video Association)
  - DVR's Overwrite Their Data!!!
  - Date/Timestamp Verification
  - Best Quality Video / Best Evidence (Video Compression)
  - On Scene Video Recovery / AVI vs. Native File

DIGITAL EVIDENCE LAB

- Surveillance Video / Cell Phone Video

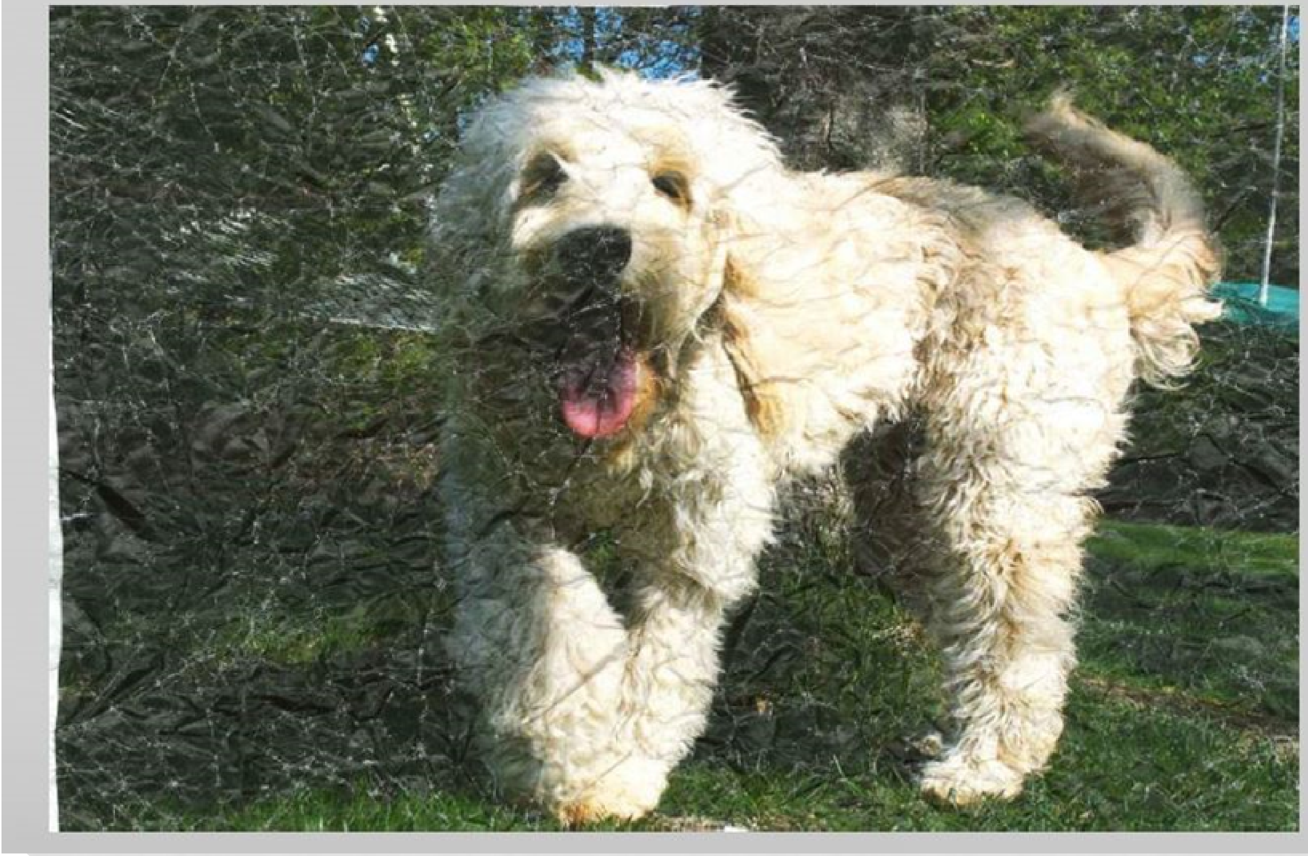


Compression

- Compression is the science of reducing the amount of data required to convey information.

Baxter - Uncompressed

Baxter – After Compression



DIGITAL EVIDENCE LAB

- Mobile Device Forensics
  - Cellebrite Certified Physical Analysts
  - Cellebrite UFED 4PC / Cellebrite Physical Analyzer
  - SQLite Database Analysis (Kik, Snapchat, Facebook Messenger)
  - Cloud Analysis
  - Common Issues with Mobile Devices

PASSWORDS AND ENCRYPTION

- *Technical Challenge: some devices that are password protected and/or encrypted are unable to be searched without those credentials*
- *COMMONWEALTH VS. GELFGATT*
  - The Court may compel a defendant to produce the passcode if the government can make a showing that it is a foregone conclusion the defendant knows the password/has the ability to decrypt.
- *Investigative solutions:*
  - *Ask the defendant if s/he knows the password.*
  - *Ask them to provide it!*
  - *Question witnesses who are likely to know- friends, spouses, scorned lovers…*
  - *Offer to unlock phones so the defendant can access numbers to make a post-arrest phone call*
  - *Observe the defendant manipulate the device, especially if they lock or unlock it.*
  - Ask for passwords in addition to the device unlock code (iTunes, iCloud, Google)
- PC/Laptops may contain mobile device backups (iTunes)
- Laptops with hardware encryption (TPM)

LIVE ANALYSIS

- Detect Encryption
- Extract Recovery Keys
  - Bitlocker
- Recover Credentials for Online Accounts
- Search base on hash values
  - NCMEC Reports
- Analysts should be part of the SW execution

CLOUD ANALYSIS

- Less data is stored on the physical device
- Consent form specific cloud analysis
- Magnet Axiom
  - Can parse cloud extractions

Partnerships

- The MDAO Digital Evidence Lab works closely with other state and federal agencies

Partnerships

- Office of the Attorney General Digital Forensics Lab
- FBI Computer Analysis Response Team (CART)
  - New England Regional Computer Forensics Lab (NE-RCFL)
  - Provide Middlesex County with FBI tools, training, and expertise.