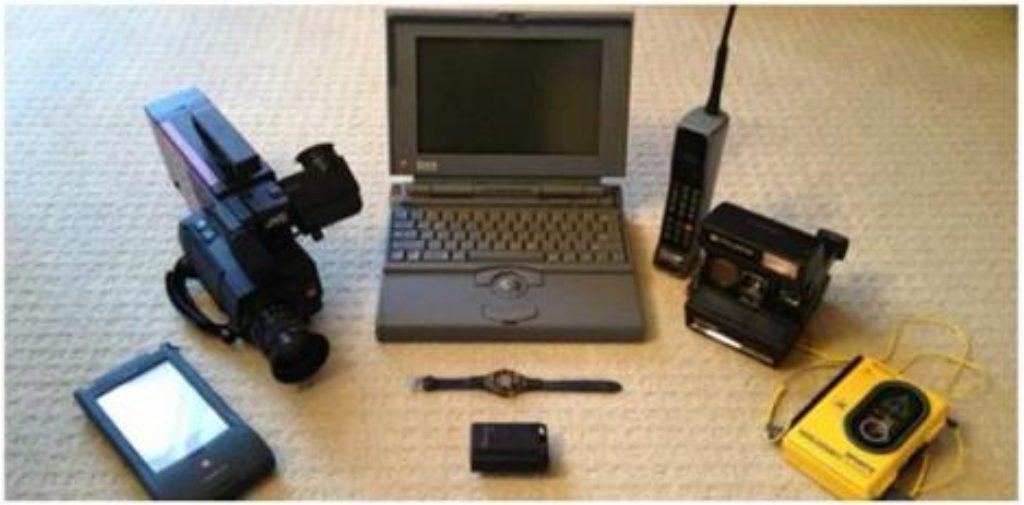
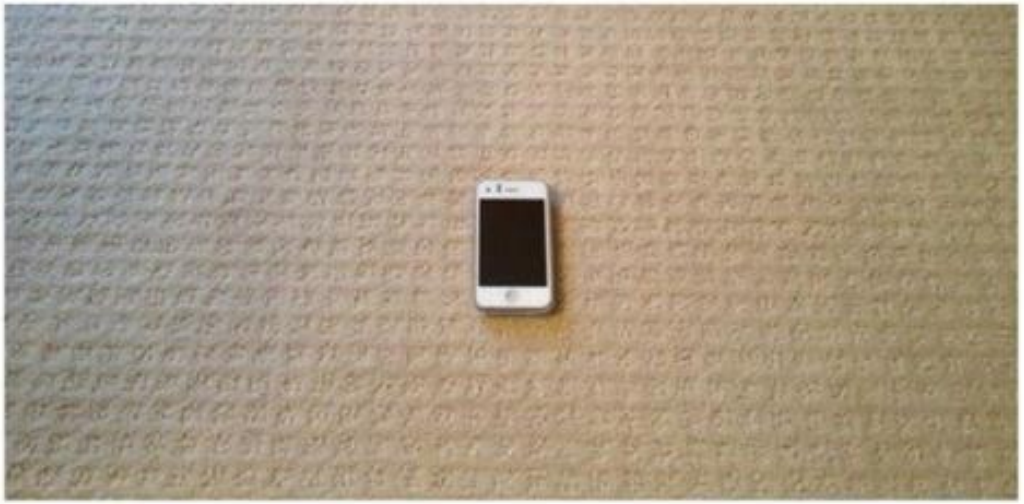
Best Practice in Responding To Cyber Threats

Robert Morgester
Senior Assistant Attorney General
Robert.Morgester@doj.ca.gov

Then and Now
1996 / 2016





Relearning Old Lessons

- 1996 / 2016 needs
  - Training
  - Investigative resources
  - Forensic resources
    - Address these needs separately
- 1996 / 2016 problems
  - Victims
    - Identification, Reporting / Notification

Training

- Develop in-house programs
- Identify non-profit or government trainers
  - SEARCH.org; NAAG; NWC3
- Leverage private vendors
- Train your agents and prosecutors

Investigative Resource

- You already have the right agents
- Create vertical prosecution teams
- Subject Matter Expert support
  - Child exploitation agents
  - Local
  - On-line
    - https://www.hightechcrimecops.org/
    - DigitalDA
    - CDAA eCrime / eEvidence Community
      - http://sidebars.cdaa.org/new-item4

Forensic Resource

- No substitute for a good interview
- Doing more with less
  - Copies of digital evidence; anything goes
  - Triage forensics
  - Leveraging office resources
  - Contractors
  - College / University
- Starting a commune
  - Bringing your examiners together

Victim Issues

- Identification
  - Finding them
- Reporting & Notification
  - Mandate for data breaches

Current Cal. DOJ Programs

- Privacy Enforcement and Protection Unit
  - http://oag.ca.gov/privacy
- eCrime Unit
  - http://oag.ca.gov/ecrime
- Cal. Cyber Crime Center
  - https://oag.ca.gov/c4
- Digital Evidence Training Program
  - http://oag.ca.gov/cci-subject-areas/d-digital-evidence