Electronic Evidence
(It's Not What You Think)

Mark D. Rasch
MDRasch@Gmail.com
(301) 547-6925

Computer Forensics Defined

Computer Forensics can be defined simply, as a process of applying scientific and analytical techniques to computer Operating Systems and File Structures in determining the potential for Legal Evidence

Why is Evidence Important?

- In the legal world, Evidence is EVERYTHING
- Evidence is used to establish facts
- The Forensic Examiner is not biased

The Electronic Crime Scene

- Every case involves electronic evidence
- If there isn't electronic evidence, you haven't done your job
- Almost every document is electronic first
- Every crime potentially carries electronic evidence
- Cell phones, videos, surveillance, location, communications, search history, GPS, motive, opportunity, etc. are all on electronic records
- Public source information (Google searches, Google maps, Google view, public databases, social media)

EVERYTHING is Electronic

- Most paper originated in electronic form
- Reports, printouts, receipts, lab tests, other forensic reports were created, processed, or printed from a computer (often over a network). Thus errors that could be introduced from computers must be accounted for.
- Certain "physical" evidence is electronic – surveillance video, crime scene photographs, dashcam/bodycam, breathalyzer, radar and LiDar, interception, etc. If it was created, stored or processed by computer, it is digital evidence, and forensics may be required.
- What is a measurement and what is a report? Is an IP address hearsay?
- Law works by analogies – is a userid and password an ID or a key?

Key Takeaways for 2018

- It's rarely the computer anymore
- The phone is the computer
- The data is in the network
- The data is with third parties
- Cops rarely do the searching anymore
- The data is international

Key Takeaways for 1986

- We still need to have forensic processes to recover old data
- Particularly for “cold” cases
- Hardware issues
  - Floppy drives
  - JAZ or ZIP drives?
  - Diskpacks
- Software Issues
  - Updated or NON updated versions?
  - Forward or backward compatibility
- How do you do it forensically?

What Kinds of Cases Have Electronic Evidence?

- Every case has electronic evidence
- Cell tower or location data
- Alibi information
- Cell phone data
- Corroborating data
- 911 call (with location)

Digital Cameras (Traffic Cam, Surveillance Cams)

- If you want to place a person at a crime scene (or find the person who was at the crime scene) there are various places to look:
  - Cell tower “dump”
  - Collateral data (Yelp, Google, OpenTable, etc.)
  - Digital license plate readers (commercial and government)
  - Digital traffic cameras
  - Google maps and map history
  - Private or commercial surveillance cameras
  - Facial recognition
  - Social media (posted or tagged pictures)

The Digital Breadcrumbs

- Woke up, got out of bed, dragged a comb across my head…
- Digital alarm goes off, check email, check news
- Watch TV online, message friends
- Alexa, OK Google, Siri and digital thermostat and fitness tracker are watching and listening (and even Samsung TV)
- These can be remotely turned on, accessed and data retrieved
- OnStar or other services remotely turned on
- Webcams and microphones (including those in phones or watches) turned on
- Your devices are watching you (and reporting to others)

Primary and Metadata

- Primary data are things like the content of emails, files, folders, etc.
- Metadata is the data about that data – how and where it was created, when it was accessed, how it was transmitted
- BUT – it's not always clear which is which – example, userid and password to access email or bank account – data or metadata? Dial into bank VRU (Voice Response Unit) and type SSN – content or not?

Primary and Metadata

- Theory – expectation of privacy in data, no expectation of privacy in metadata
- Reality – metadata can tell more about user than the underlying data
- Who “owns” data and metadata?
- Katz analysis of data and metadata

Legal Difference Between Data and Metadata

- CONTENT information –
  - contents of e-mail,
  - contents of documents,
  - contents of communications –
  - require probable cause and warrant (mostly)
- PROVIDED that the subject has
  - a reasonable expectation of privacy in the content of that document/communication
  - Subjective privacy interest
  - Objectively reasonable

Legal Difference Between Data and Metadata

- Exceptions:
  - Express Waiver (you have no expectation of privacy OR your communications may be monitored)
  - Implied Waiver – you know that the communications may be monitored (for some purpose)
  - Waiver implied by dissemination? Social media, etc.
  - Consent by third party – e.g., employer, invited ear, carrier, apparent authority
  - Plain view
  - Exigent circumstances

Metadata

- Who OWNS the metadata?
- Smith v. Maryland, 442 US 735 (1979) – telephone toll records
  - Marshall/Brennan dissent – "Implicit in the concept of assumption of risk is some notion of choice. [U]nless a person is prepared to forgo use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance." … The prospect of unregulated governmental monitoring will undoubtedly prove disturbing even to those with nothing illicit to hide. Many individuals, including members of unpopular political organizations or journalists with confidential sources, may legitimately wish to avoid disclosure of their personal contacts. … Permitting governmental access to telephone records on less than probable cause may thus impede certain forms of political affiliation and journalistic endeavor that are the hallmark of a truly free society." *Smith v. Md.*, 442 U.S. 735 (1979).

Metadata

- United States v. Miller – bank records
  - *United States v. Miller*, 425 U.S. 435 (1976).
- Difference between records OF an individual/entity and records ABOUT an individual or entity

Metadata and Privacy

- US v. Jones – GPS Tracking device
  - *U.S. v. Jones*, 132 S.Ct. 945 (2012).
- Carpenter v. United States Dkt. No. 16-402– cell tower data
- Byrd v. United States, Dkt. No. 16-1371– rental car – ownership of "container" dictates privacy right in contents?
- *United States v. Choate*, 619 F.2d 21 (9th Cir. 1980).– mail cover
- NO warrant needed for metadata – subpoena or court order
  - Trap and trace
  - Pen register
  - Cell tower dump
  - Tracking device

Data about Data

- For communications
  - Info about sender – browser type and version
  - Operating system and version
  - Location and IP address
  - Traceroute and location of transmission
  - Communications software and version
  - Attachments and metadata (software and version)
- For Files
  - Location, creation, access dates
  - Modifications, collaborators, etc.
- For Networks
  - Access logs, modification logs, intrusion detection
  - Transmission, pathway, timing
  - IP address (static, dynamic, spoofed)

Where is the Evidence Located?

- Devices
  - Hardware, hard drives, RAM, dynamic memory, etc.
  - Storage
  - Backup, storage archival, cloud
  - Retrieve through EnCase or other tools
- Network
  - Network forensics
  - Remote forensics
- Cloud or Remote Services
- Third Party
  - ISP
  - Network Provider
  - Social Media

Where Do I Get The Evidence?

- Think globally – act locally
- Recreate the digital footprint
- Preserve first, obtain later
- Consider every place the data might be
- Think of devices that might store relevant data (e.g., event data recorder (EDR) in car, car GPS, smart home devices, wearables).
- Consider offsite data – third party and cloud

Search Warrants – Specificity and Procedure

- The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Search Warrants – Specificity and Procedure

- Several components
  - What is a "search?" What is a "seizure?" (are communications "seized?")
  - WHERE is the search conducted?
  - Search/Seize/then Search?
  - Scope of seizure – scope of search
  - Typically search for computer, determine computer is covered (covered records are on computer), then seize, THEN do minimization
- How do you do a search on cloud provider?
- Stored Communications Act

Stored Communications Act - Frankenwarrant

- SCA authorizes a SEARCH WARRANT to be served on an ISP if the warrant is issued by federal court or state court in compliance with state law
- The warrant is not "executed." Warrant is served on the ISP, email provider, etc.
- Can include a preservation order while obtaining a warrant so data is not deleted
- May include a gag order
- ISP then produces the records
- Question – sovereign immunity? Who executes the warrant?

New York v. Facebook

- In re 381 Search Warrants Directed to Facebook, Inc. – NY Court of Appeals 2015 NY Slip Op 06201 [132 AD3d 11] July 21, 2015
- Court issued 381 warrants directed at Facebook
- Sought subscriber information for disability fraud investigation
- Directed Facebook "to retrieve, enter, examine, copy, analyze, and . . . search [each] TARGET FACEBOOK ACCOUNT for profile information, contact and financial account information, groups, photos and videos posted, historical login information, and "[a]ny public or private messages."
- The warrants prohibited Facebook from notifying its subscribers or otherwise disclosing the existence or execution of the warrants, in order to prevent interference with the investigation

Facebook Search Warrant

- Warrant served on Facebook pursuant to SCA
- Facebook sought to challenge the warrant
- Court ruled that there is no procedure to challenge a search warrant, and that the SCA order is a warrant not a subpoena.
- The targets (account holders) could challenge the legality of the search but ONLY if they were ultimately prosecuted. Otherwise, they would never know about the existence of the warrant.

Gag Orders and Nondisclosure

- 18 U.S. Code § 2705 – typically give notice of SCA order (just like leaving copy of the warrant)
- Exception for "delayed" notice (90 day blocks)

  (A) endangering the life or physical safety of an individual;

  (B) flight from prosecution;

  (C) destruction of or tampering with evidence;

  (D) intimidation of potential witnesses; or

  (E) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

Gag Orders and Nondisclosure

- Must be a genuine showing of real probability of harm, not pro-forma
- Other states (e.g., MN) have gag orders by default
- So.. How do you assert privilege when you don't know about search?

How Do I Get The Evidence? (Compulsory Process)

- To target
  - Seizure – search incident to arrest. *Riley v. Cal.*, 134 S. Ct. 2473 (2014).
  - Consent
  - Grand Jury Subpoena
  - Search Warrant
  - Court Order
  - FISA Warrant
  - National Security Letter
  - Administrative Subpoena
  - Disclosure Order
  - Warrant exception (exigency, abandonment, etc.)
- To Third Party
  - Cloud provider
  - ISP
  - Social Network

Third Party Doctrine

- Derived from Smith v. Maryland 442 U.S. 735 (1979)
- You give up privacy when you entrust data (or metadata) to a third party

Third Party Doctrine

- Sotomayor concurrence in *Jones*

  "… it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers. Perhaps…some people may find the "tradeoff" of privacy for convenience "worthwhile," or come to accept this "diminution of privacy" as "inevitable," and perhaps not. I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year."

International Third Party

- What if the records are stored elsewhere?
- How do you get records in another country?
- International process of subpoenas
- Letters Rogatory
- Mutual Legal Assistance treaties (MLAT)
- How do you authenticate or admit into evidence?
- Forensics?

Rule 41 FR Crim P

- A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review. Fed. R. Evid. 41.

Rule 41 FR Crim P

- A magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if:
  - (A) the district where the media or information is located has been concealed through technological means; or
  - (B) in an investigation of a violation of 18 U.S.C. § 1030(a)(5), the media are protected computers that have been damaged without authorization and are located in five or more districts.

Ripley

- Remote kill switch
- Used by Uber internationally
- Immediately wiped the passwords of users in a specific country if texted
- Controlled by General Counsel in US
- If warrant executed, encrypted data could not be accessed
- Could include a fake welcome banner

No Knock Warrant

- Warrant typically requires service, notice, etc.
- No knock (black bag) warrants are the exception
- Warrants must typically be executed at a particular time of day and in a particular manner
- How does this apply to electronic warrants and non-geographic warrants?

Fuzzy Dunlop and Parallel Construction

- To avoid giving up sources, agency uses pretext for search
- Agency conducts unlawful internet search and finds data – or obtains from classified NSA intercept or other source
- Uses pretext like vehicle swerving within lane to establish probable cause (PC) to stop

Fuzzy Dunlop and Parallel Construction

- Judge and prosecutor may never be told true source of data and reason for search
- Example – DEA arranges for traffic accident involving suspect's vehicle (hit and run by DEA employee). During investigation of accident, police tell suspect to leave car with keys in it. Car is then "stolen" by another DEA agent, and searched.
- You won't know if you don't ask – motion for return of illegally seized property

Warrant/Subpoena/Order

- Multiple ways to collect evidence
- For content
  - Warrant
  - SCA order
  - Court order like warrant
  - FISA warrant
  - Consent
- For non-content
  - Subpoena duces tecum
  - Trap and trace
  - Other Court order
- Preservation Order

Location, Location, Location

- Location data may be critical in investigation, prosecution and defense
- How is it collected, where is it stored, and how is it retrieved and presented?
- Cell tower, Google Maps, third party apps, automatic license plate recognition (ALPR), webcams, IP addresses with geolocation, facial recognition, ancillary applications that rely on location to function

Stingrays and Dirtbags

- Warrant or court order required for tower dump
- Carpenter v. United States, Sup. Ct., No 16-402, argued Nov 29, 2017
- Cell tower data held by phone company – some compulsory process required
- Stingray acts as mobile cell tower – spoofing all phones in area to give up international mobile equipment identity (IMEI), number, and location
- Dirtbag (DRT) does same over wider location via airplane or drone
- Not clear if warrant is required to operate

RATs and NITs

- How do you get warrant or data when you don't know where server is?
- Jurisdictional limits of U.S. Courts
- How do you obtain data outside US?
- Playpen case – U.S. sought evidence of individuals downloading child porn from server outside U.S. through TOR software
- Obtained warrant from US Court to install SOMETHING onto server When server was visited, the SOMETHING (probably a Remote Access Terminal – RAT) or a NIT (Network Investigative Technique) beaconed the investigator with the true IP address of downloader – declared unlawful in Boston federal court in US v. Allain, 213 F. Supp. 3d 236 (D. Mass. 2016)

Digital Canaries

- How do you protect data in hands of third party?
- If YOUR data, you can third party encrypt
- If data ABOUT you, nondisclosure order with notice and opportunity to object, BUT
- What if party seeking evidence obtains gag order or simply “takes” data without knowledge of either party?

Digital Canaries

- Consider digital canaries – party holding data must certify under oath every month (or other time) that they have not disclosed or permitted disclosure of the data
- Failure to certify = notice of disclosure
- Can add liquidated damages provisions as well
- Balance of the equities

Encrypted Data

- Encrypted in whole or in part
- Encrypted end to end, point to point, in transmission, storage, archival or processing
- Whole disk encryption
- Session encryption
- Data level, network level, transport level encryption
- Multiparty or multifactor keys (Clipper chip redux)
- Encryption and expectation of privacy
  - Employee employer
  - Customer cloud provider

Compelled Decryption

- Fifth Amendment and self incrimination
- Act of production is testimonial
- Difference between biometric lock (fingerprint, face) and password or PIN
- Something you are (Shmerber) vs. something you know (Hubbel)
- Is password a key (not protected) or a statement (protected)
- The “going dark” problem

Who "Seizes" The Evidence?

- Who is first responder?
- How is electronic crime scene secured?
- Faraday cage
- *Riley v. Cal.*, 134 S. Ct. 2473 (2014). - search of cell phone incident to arrest
- Where data is third party (Facebook, LinkedIn, Google)
  - where is crime scene?
  - where is evidence?
  - who does minimization?
  - How do you apply Illinois v. Gates, 462 U.S. 213 (1983) (good faith)?
  - General warrant
  - Writ of Assistance

Jurisdiction and Venue

- Where is the search conducted?
- Does the court have authority to authorize the search in that location?
- Does the 4th Amendment apply to foreign searches?
- *Microsoft v. United States,* No. 17-2, argued Feb 27, 2018 (pending in Supreme Court) – location of company that stores the data?
- State court warrants for data outside the state? Outside the country?
- Letters rogatory and mutual assistance?

Basic Rules of Admissibility

- Relevance
- Authenticity
- Best Evidence
- Non-modification

What is an “Original?”

- What are you trying to prove?
- Where is the BEST evidence of what you are trying to prove?
- How will you authenticate it?
- How will you overcome hearsay objection?
- WHO will authenticate it?
- How will you demonstrate non-alteration (pre- and post-acquisition)?
- How will you present it in court?
- Special problems for contraband

Changes to Federal Rules of Evidence

- Rule 901 – Authentication
- In General. To satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is.
- (9) Evidence About a Process or System. Evidence describing a process or system and showing that it produces an accurate result.

New Rules –Rule 902

- Rule 902 – Evidence That Is Self-Authenticating
- The following items of evidence are self-authenticating; they require no extrinsic evidence of authenticity in order to be admitted:
  - (13) Certified Records Generated by an Electronic Process or System. A record generated by an electronic process or system that produces an accurate result, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12). The proponent must also meet the notice requirements of Rule 902(11).
- Effective January 1, 2018

Rule 901 (14)

- (14) Certified Data Copied from an Electronic Device, Storage Medium, or File.
  - Data copied from an electronic device, storage medium, or file, if authenticated by a process of digital identification, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12). The proponent also must meet the notice requirements of Rule 902(11).

Purpose of New Rules

- often a party goes to the expense of producing an authentication witness, and then the adversary either stipulates authenticity before the witness is called or fails to challenge the authentication testimony once it is presented.
- The amendment provides a procedure under which the parties can determine in advance of trial whether a real challenge to authenticity will be made, and can then plan accordingly.

Hash Values and Authentication

- data copied from electronic devices, storage media, and electronic files are ordinarily authenticated by "hash value." …
- If the hash values for the original and copy are the same, it is highly improbable that the original and copy are not identical.
- This amendment allows self-authentication by a certification of a qualified person that she checked the hash value of the proffered item and that it was identical to the original.

Imaging, Mirroring, or Copying

- What's the difference between
  - Imaging a drive
  - Mirroring a drive
  - Copying a file or directory
- How to apply these rules to servers, networks and fileshares
- How to apply these rules to the cloud and multitenant environments
- How to apply these rules to distributed data and encrypted databases

Chain of Custody (and Breaks)

- Purpose of Chain of Custody is to demonstrate non-alteration post acquisition
- Demonstrate who had access to data or media and how
- Best way – original, backup and working copy – as well as copy for defense
- But – break of chain of custody rarely fatal – if you can explain

Authenticity

- YHWH – I am what I am
- Or Popeye – I Yam Who I Yam
- Or FRE 901(a) To satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is
- It's simple (and insanely difficult)
  - I show you Exhibit x – what is it?
  - How do you know that's what it is?
  - Is it in substantially the same condition as it was when …?

Custodian of Records

- Most electronic evidence is admitted through some custodian
- Custodian MUST have some knowledge – but rarely enough

Custodian of Records

- Example – telephone toll record –
  - Custodian must demonstrate business records exception – regularly collected, regularly maintained, ordinary course of business – for reliability and hearsay exception – must have personal knowledge
  - BUT – does custodian really know how a phone record is created?
    - How does it go from cell phone to computer?
    - Cell phone to tower?
    - What computer collects the data?
    - What operating system, what program, what protocols?
    - How is it stored? Maintained?
    - Who has access to the records?
    - Fraud, hacking and errors

Hearsay (and Exceptions)

- Almost all electronic records are, or contain, hearsay
- Are data logs hearsay? Are they a “statement?”
- Business records for content
- What about metadata – is that a business record?

Delete Doesn't (and Restore Won't)

- Deleted files are likely recoverable
- Even at the network or cloud level
- Search for, demand, or subpoena deleted files!
- File allocation table (FAT) and restoration commands

The Trojan Defense

- If hackers can access and change data, they can add forensic files
- If you find malware on a machine, it creates possibility of remote access and insertion of programs
- Botnets and RATs impact forensic value of machine
- Inbound and Outbound log data must be secured

The Electronic Alibi

- How to establish
- How to defeat
- Difference between presence of device and presence of defendant or person
- BUT – people are generally wedded to their mobile devices
- Don’t forget wearables and Internet of Things (IoT) data
- Strava wearable fitness tracking and the DoD

How is Digital Evidence Processed?

- **Assessment**
  - Computer forensic examiners should assess digital evidence thoroughly with respect to the scope of the case to determine the course of action to take.
- **Acquisition**
  - Digital evidence, by its very nature, is fragile and can be altered, damaged, or destroyed by improper handling or examination. Examination is best conducted on a copy of the original evidence. The original evidence should be acquired in a manner that protects and preserves the integrity of the evidence.

How is Digital Evidence Processed?

- **Examination**
  - The purpose of the examination process is to extract and analyze digital evidence.
- **Extraction**
  - The recovery of data from its media. Analysis refers to the interpretation of the recovered data and putting it in a logical and useful format.
- **Documenting and Reporting**
  - Actions and observations should be documented throughout the forensic processing of evidence.

Be Prepared

- **Software licensing**
  - Ensure that all software used by the computer forensics unit is properly licensed by the agency or an individual assigned to the unit.
- **Resource commitment**
  - Establishing and operating a computer forensics unit may require significant allocation of financial resources and personnel. Many of the expenses are recurring and will have to be budgeted on a yearly basis. Resource allocation should include the type of facility that will house the unit, equipment used by examiners, software and hardware requirements, upgrades, training, and ongoing professional development and retention of examiners.

Be Prepared

- Training
  - It is important that computer forensics units maintain skilled, competent examiners. This can be accomplished by developing the skills of existing personnel or hiring individuals from specific disciplines.
  - Because of the dynamic nature of the field, a comprehensive ongoing training plan should be developed based on currently available training resources and should be considered in budget submissions
  - Consideration may also be given to mentor programs, on-the-job training, and other forms of career development

Reasons for a Forensic Analysis

- ID the perpetrator
- ID the method/vulnerability of the network that allowed the perpetrator to gain access into the system
- Conduct a damage assessment of the victimized network
- Preserve the evidence for Judicial action

Types of Forensic Requests

- Intrusion Analysis
- Damage Assessment
- Suspect Examination
- Tool Analysis
- Log File Analysis
- Evidence Search

Intrusion Analysis

- Who gained entry?
- What did they do?
- When did this happen?
- Where did they go?
- Why the chosen network?
- How did they do this?

Damage Assessment

- What was available for the intruder to see?
- What did he take?
- What did he leave behind?
- Where did he go?

File Recovery

- Deleted Files
- Hidden Files
- Slack Space
- Bad Blocks
- Steganography
- X-Drives
- New Technology File System (NTFS) Streams

More Information

Mark Rasch

MDRasch@gmail.com

301 547-6925