Understanding Digital Forensics

Adam Blevins, Hamilton Clermont Cooperative
Damon Hacker, Vestige Digital Investigations
Ryan LaFlamme, Ennis Britton Co., L.P.A.

OSBA leads the way to educational excellence by serving Ohio's public school board members and the diverse districts they represent through superior service, unwavering advocacy and creative solutions.

Investigating Denial of Service (DoS) Attacks

A Denial of Service attack is an actions designed to disrupt the target system's ability to provide services.

A common DoS attack generates a flood of data, overwhelming the system or network so that it cannot respond to legitimate requests.

Investigating Denial of Service (DoS) Attacks

One of the first steps in any investigation is to identify individuals who have information relating to the incident. Such individuals may include-

- Network admins/users
- Employees, current or former
- Internet Service Providers
- Consultants
- Human resources

Investigating Denial of Service (DoS) Attacks

What are right questions to ask?

- What is the nature of the attack
- What hosts where involved (internal and external)
- When did the incident occur
- Was there personal information or other data loss
- Has the intrusion event been resolved

Investigating Denial of Service (DoS) Attacks

When gathering data it is important to ensure the logs are maintained and protect the integrity of the data.

- Server log rotation may overwrite data so time is important to ensure the data is available
- Log files may be very large and required post processing to locate the attack.
- Protect integrity of logs records with cryptographic methods to ensure they are not modified

Investigating Denial of Service (DoS) Attacks

Firewall logs and other gateway appliances will include valuable information that will be required for law enforcement and future mitigation.

- Source and destination IP Address of hosts
- Ports used during the attack
- Number of connection attempts
- Date and time of the attack

Investigating Denial of Service (DoS) Attacks

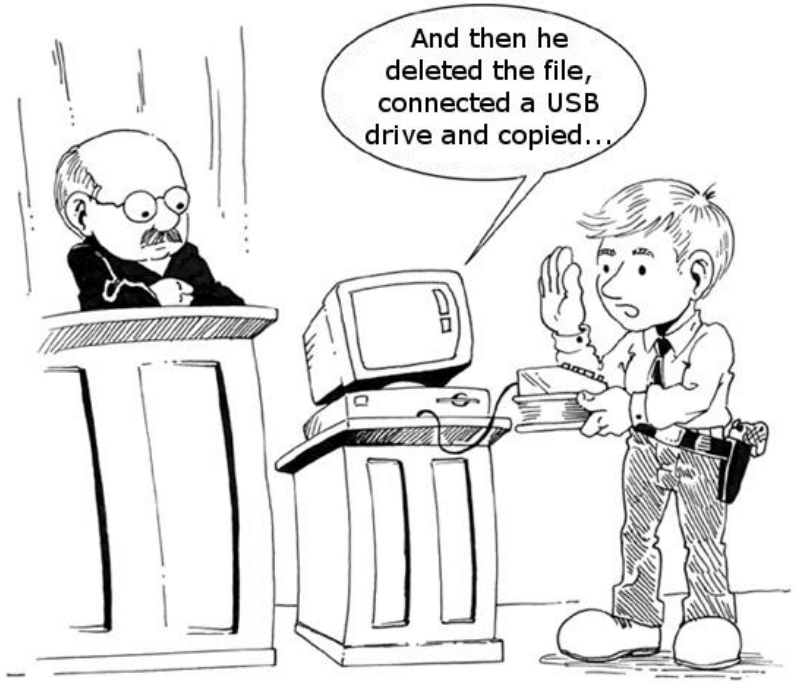
It is also important to preserve logs in all other systems that may include information on the attacks. Such devices may include-

- Firewalls
- IPS/IDS systems
- Routers
- Servers
- Web Filters
- Servers and host systems

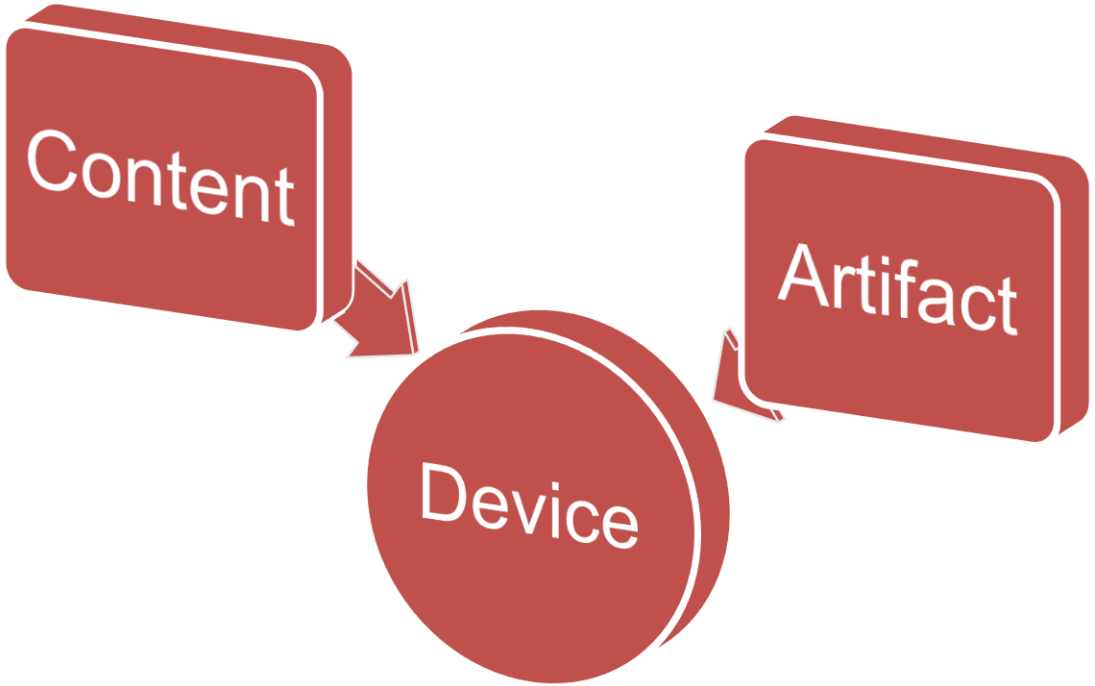
Melding Legal & Technology

- Devices as Witnesses
- How digital evidence is used
- Framework You Need to Know:
  - Identify
  - Preserve
  - Avoid Misinterpretations

Devices as Witnesses



Devices as Witnesses



How Digital Evidence is Used

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

- Correspondence
  - Memos
  - Emails
  - Instant messages
  - Faxes
  - Deleted
  - Old and forgotten

- Business Records
  - Financial data
  - Assets
  - Calculations
  - PRIOR DRAFTS
  - DELETED DRAFTS
  - Projections
  - Everything you could imagine

- Every Website visited
- All pictures from those websites
- Every Website from popups and popunders
- All maps, from Mapquest or Google Maps for example

- Every INTERNET SEARCH
  & the Search Results

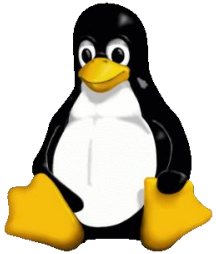
Preservation

Authentication

Analysis

Presentation

Identify the Devices

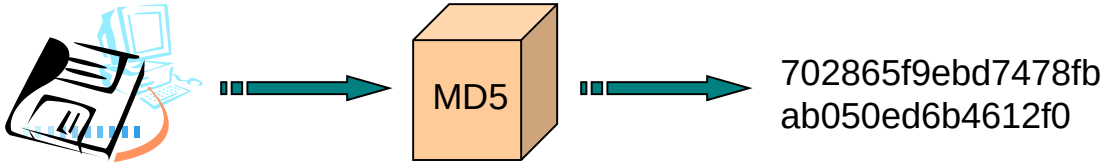


Preservation

- 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

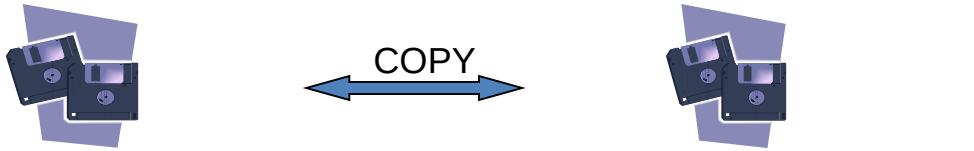
Authenticate

- Our Methodology
  - MD5 Hash –
    Digital Fingerprint



Authenticate

- Prove copies (working) are the same



702865f9ebd7478fbab050ed6b4612f0

702865f9ebd7478fbab050ed6b4612f0

Authenticate

- Prove nothing has changed

702865f9ebd7478fbab050ed6b4612f0

702865f9ebd7478fbab050ed6b4612f0

Analysis: “Getting the Goods”

- Leave No Stone Unturned
  - Content, including Deleted
  - Artifacts
  - Printed documents
  - E-mail / IM / chat sessions
  - Internet History
  - Hiding Activity
  - Temporal Analysis
  - Software and Hardware Installed & Uninstalled
  - Nefarious Activity (Wiping, Booby Traps, Encryption)

E-Discovery Foundations

- The Civil Rules have been amended over the years to address electronically stored information.
- Pursuant to Civ. R. 34, any party may serve discovery requests on any other party:
  - (1) to inspect and copy any designated documents or electronically stored information….stored in any medium from which information can be obtained that are in the possession, custody, or control of the party upon whom the request is served;
  - (2) to inspect and copy, test, or sample any tangible things that are in the possession, custody, or control of the party upon whom the request is served;
  - (3) to enter upon designated land or other property in the possession or control of the party upon whom the request is served for the purpose of inspection and measuring, surveying, photographing, testing, or sampling the property or any designated object or operation on the property.

Limitations on E-Discovery

- Civ. R. 26(B)(4) provides a framework through which a recipient of a discovery request for electronically stored information may object if such request imposes an undue burden.

- Undue burden may be overcome if good cause is shown, which is determined according to the following:

  (a) whether the discovery sought is unreasonably cumulative or duplicative;

  (b) whether the information sought can be obtained from some other source that is less burdensome, or less expensive;

  (c) whether the party seeking discovery has had ample opportunity by discovery in the action to obtain the information sought; and

  (d) whether the burden or expense of the proposed discovery outweighs the likely benefit, taking into account the relative importance in the case of the issues on which electronic discovery is sought, the amount in controversy, the parties' resources, and the importance of the proposed discovery in resolving the issues.

Limitations on E-Discovery

- Privacy Laws:

- **Family Educational Rights and Privacy Act (FERPA) 20 U.S.C. 1232g; 34 CFR Part 99**
  - This Federal law prohibits the disclosure of educational records accept under certain circumstances, one of which is a lawfully issued subpoena.

  - A parent or eligible student must provide written consent before a school or school district discloses a student's education records, unless one of the exceptions to FERPA's general consent rule applies.

  - FERPA only protects educational records which are defined as records which are:
    - 1) Directly related to a student.

    - 2) Maintained by an educational agency/institution or by a party acting on behalf of the educational agency/institution

Limitations on E-Discovery

- FERPA Subpoena Process:
- A public records request is not a good vehicle for obtaining student records due to privacy laws such as FERPA.
- If a school district receives a lawfully issued subpoena for education records, it must inform the parent of each child for whom educational records must be disclosed that a subpoena has been received and to give the parents an opportunity to seek a protective order. The school district itself may seek a protective order to seal the educational records from public view.
- A court or an "issuing agency" with a law enforcement purpose can order that the contents of the subpoena not be disclosed. This enables the school district to comply with the subpoena without notifying the parents.
- The rules for when a school district may release educational records without prior written consent are contained in 34 CFR Part 99.31.

Limitations on E-Discovery

- Ohio Privacy Laws:
- Ohio has its own statute protecting the confidentiality of student records.
- R.C. 3319.321 provides that “No person shall release, or permit access to, personally identifiable information other than directory information concerning any student attending a public school, for purposes other than:
  - Administrative use;
  - Missing Child Investigations;
  - Certain juvenile court orders;
  - Required reports of violations of offenses contained in R.C. 3313.662

Limitations on E-Discovery

- Ohio Privacy Laws: 3319.321
- “Personally Identifiable Information is not defined in the statute but there are some other statutes in the Revised Code which contain a definition for personal information.”
- RC 1349.19: "Personal information" means an individual's name, consisting of the individual's first name or first initial and last name, in combination with and linked to any one or more of the following data elements, when the data elements are not encrypted, redacted, or altered by any method or technology in such a manner that the data elements are unreadable:
  - Social security number;
  - Driver's license number or state identification card number;
  - Account number or credit or debit card number, in combination with and linked to any required security code, access code, or password that would permit access to an individual's financial account.

Limitations on E-Discovery

- Ohio Privacy Laws: 3319.321
- “Personally Identifiable Information is not defined in the statute but there are some other statutes in the Revised Code which contain a definition for personal information.”
- R.C. 1347: “Personal information" means any information that describes anything about a person, or that indicates actions done by or to a person, or that indicates that a person possesses certain personal characteristics, and that contains, and can be retrieved from a system by, a name, identifying number, symbol, or other identifier assigned to a person.
- However, because a definition is not provided in 3319.321, school districts interpret the meaning of personally identifiable information broadly in favor of protecting confidentiality.

Public Records

- Ohio's Public Records laws treat electronic records essentially the same as any other medium. (R.C. 149.43)
- School District's and municipalities have moved towards digital storage of records but there are still paper files around to be searched or inspected.
- Emails, databases, spreadsheets, invoices, purchase orders, policies, personnel records, etc. in a digital form are subject to retention and disclosure the same as any hardcopy record.
- Records are to be organized and retained in accordance with the content rather than the medium. All school districts have a records retention policy which sets forth the time periods for which particular records will be kept. Some records are required to be kept by law while others must be maintained in accordance with their legal, historical, financial or administrative value.

Public Records

- Persons requesting electronic records through a public records request may demand that the records be conveyed electronically.

- The public records laws allow for the public entity to charge for the actual cost of copies produced. This is typically does not occur with electronic transmission of records since the transmission cost is so low or difficult to determine. However, public entities may charge to place the records on a CD or DVD or for the actual cost of hardcopies provided. Further, with regard to database extractions, there may be charges for the actual costs of extraction, including where a public entity uses a private contractor to do the extraction. *See, State ex rel. Gibbs v. Concord Twp. Trustees, 152 Ohio App.3d 387, 2003-Ohio-1586, ¶ 31 (11th Dist.); State ex rel. Gambill v. Opperman, 135 Ohio St.3d 298, 2013-Ohio-761, ¶ 29*

- Records are to be provided within a “reasonable time”

- Denials of public records requests must be supported by legal references. This may give you something to latch on to. The requestor can always revise a denied request so a denial may not be the end of the road. The more specific the request, the harder to deny.

Public Records

- **How to make your request more successful:**
- Be specific! A public records request is not a discovery request. “Any and all records pertaining in any way to my client” will likely be denied.
- Provide sufficient search criteria so that your request is not too overbroad or vague to be fulfilled.
- Provide specific search terms with a date range. If you are looking for emails provide the parties between whom you would like the emails if possible. Describe the content you are seeking, e.g. “Emails between the Board members and the Superintendent concerning _____ between August 31 and December 31.”
- Be sure that you are requesting records and not simply making requests for information. Public entities have no obligation to respond to such requests.
- If your initial request is denied, and you disagree or think a record may exist, don’t simply resubmit the same request as it will likely be denied or ignored. Modify the request to be more specific if possible or otherwise address the reasons for the denial.

Thank you!

Ohio School Boards Association

@OHschoolboards

Visit our website at: www.ohioschoolboards.org