Risk Sensitive Digital Evidence Collection

By

Erin Kenneally and Christopher Brown

Presented At

The Digital Forensic Research Conference

DFRWS 2005 USA New Orleans, LA (Aug 17th - 19th)

Realizing - Risk Sensitive Evidence Collection

Digital Forensic
Research Workshop
2005

Purpose of this Presentation

- Call to Action → Realizing proposed RSEC methodology
  - Kenneally, Brown, "Risk Sensitive Digital Evidence Collection", Digital Investigation (Summer 2005)
  - Posits that current methodologies which focus on collecting entire bit-stream images of original evidence disk are increasing legal and financial risks

Presenters

- **Erin Kenneally, M.F.S., J.D.** - Forensic Analyst at the San Diego Supercomputer Center, liaises and holds leadership positions with the Computer and Technology Computer High Tech Task Force (CATCH) and High Technology Computer Investigation Association (HTCIA)

- **Christopher L. T. Brown, CISSP** - Founder and CTO of Technology Pathways, LLC, Lead architect of the ProDiscover family of computer forensics products

Agenda

- frame the debate and change drivers for a risk sensitive approach to digital evidence collection.
- current methods of evidence collection along with a cost-benefit analysis.
- describes the methodology requirements of the risk sensitive approach to collection,
- legal and resource risk assessment of this approach.

Balancing the Risk:
Refining Collection Methodology Without Compromising Forensic Principles

Methodology & Tool Evolution

- Forensic techniques must be evaluated when:
  - dynamic variables
    - data volume
    - business environment
    - legal restrictions

    …converge to impede the goal of producing verifiable results.

Modification

- Modifying current digital forensic techniques
  - identification
  - acquisition
  - preservation
  - Analysis
  - presentation

… in response to changing contexts does not necessarily mean that results are less reliable for forensic proof purposes.

Contexts

- Addresses the risks of Insisting on bitstream imaging:
    - Large and/or dispersed volumes (200 GB and above)
    - Time-sensitive
    - Network based S&S

Current Process: Primary Risk

- **Cost Metrics**
  - Time
  - Resources

- **Both costs are becoming unmanageable**
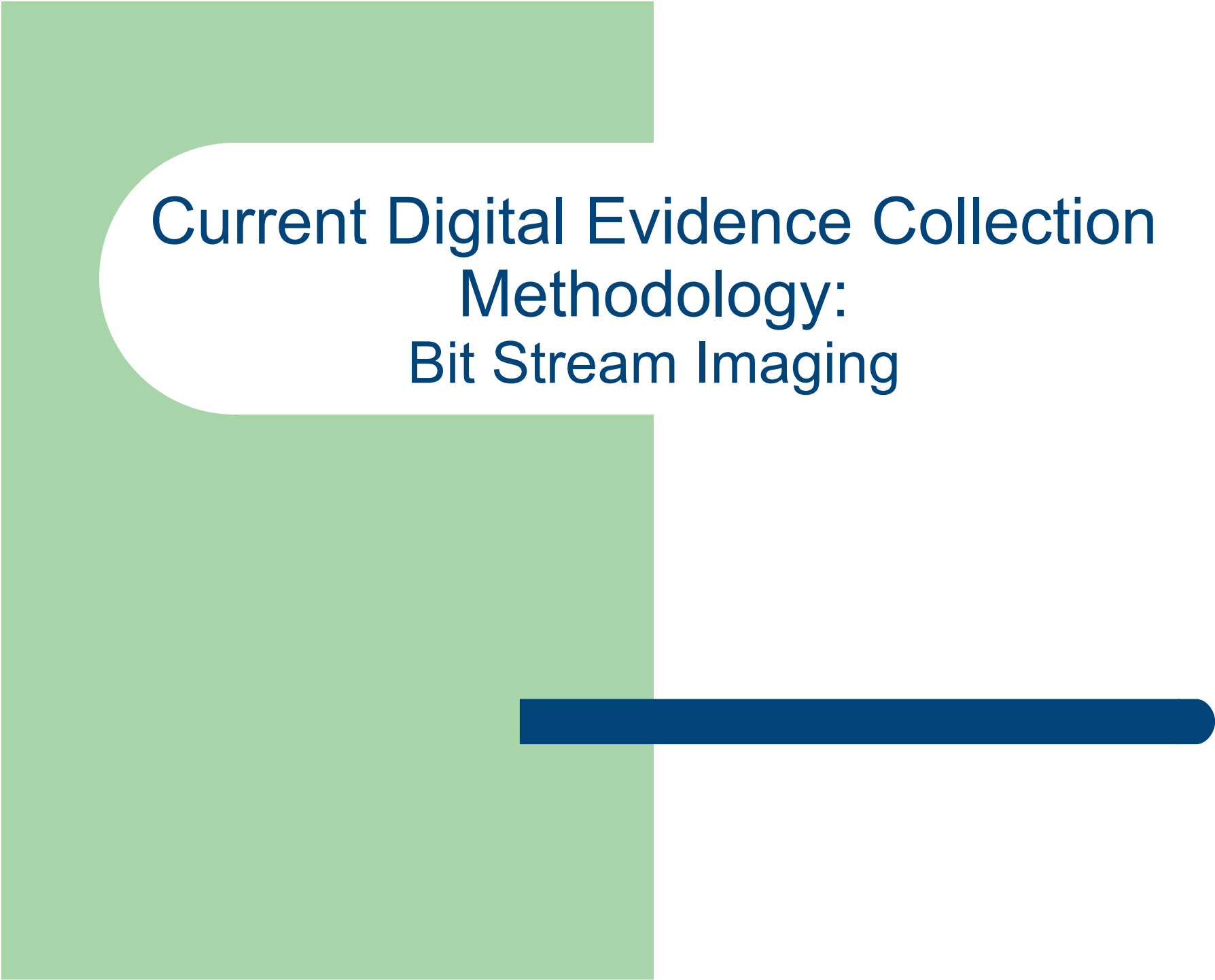
Computer forensic autopsies

- Past:
  - Single systems with single small capacity disks

- Today:
  - Multiple Systems with multiple large capacity disks, network storage, and encrypted volumes

Reasonableness

- Cost factors must be managed
    - Legal standards of "reasonableness"
    - Weigh cost & capabilities
    - Does not require perfection

Net Requirement

- Revised computer data evidence collection methodology is needed which:
  - Balances time and resource cost
  - Meets evidentiary demands of
    - Reliability
    - Completeness
    - Accuracy
    - Verifiability

Current Digital Evidence Collection Methodology:
Bit Stream Imaging

Collect Now Analyze Later

- Nature of digital evidence drives desire to collect Everything now and analyze later

- Also helps counter opponent's challenges that LE is deliberately hiding exculpatory evidence.

Analysis

- All analysis can be performed on the *image* thus protecting the original evidence disk

   Note that extensive time is spent during analysis for filtering of non-relevant data

Responding to Change:
Risk Sensitive Evidence Collection Methodology

Proposed Abstract Methodology

- The Risk Sensitive Evidence Collection Methodology:
  - Does not negate the use of current methodologies when use is reasonable and warranted
  - Is proposed for use when the situation warrants
  - Propels and makes explicit the high-level framework … template and implementation tasks TBD
  - Requires formalization & proof of concept in a controlled environment

The Methodology

- The Risk Sensitive Evidence Collection Methodology calls for:
    - On-scene artifact/evidence identification
    - Selective artifact/evidence extraction
    - From live or dead systems

Greatest benefits are realized when used on live systems allowing the original systems to continue operating as usual

Critical Concepts

- Pre-searching and subsequent identification of evidence/artifacts (n/a…but complementary to research proposed thusfar)

- RSEC addresses selective extraction of
  - evidence/artifacts identified by pre-search
  - low-level evidence supporting artifacts defined by RSEC Templates as mandatory or supplemental

Live Search and Identification

- Critical Concepts (see paper detail)
  - Data Connection
  - Data Integrity
  - Data Representation

Selective Evidence Extraction

- Based on investigator identification of evidence based on pre-search results:
    - Keyword match
    - Hash comparison
    - Visual inspection

Selective Extraction Format

- Identification steps will result in the need to extract data in (one or both):
  - File Data Unit
    - Contents of file as seen by native operating environment
  - Sector Data Unit
    - Binary and/or ASCII representation

Mandatory Supporting Artifacts (1)

- **General Evidence Media Artifacts:**
  - Disk/media manufacture, ID, geometry, label and true feature set if available

- **File Data Unit (for each):**
  - Metadata
  - Original sector locations
  - File hash value in MD5 or SHA1,
  - MAC (last modified, accessed, created)

Mandatory Supporting Artifacts (2)

- File System Artifacts:
  - Any file system meta files such as the MFT (Master File Table) in Windows NTFS
  - File tables / File system index including any time stamps and file size information
  - Index should include any recoverable deleted files
- Identity and Access Control Artifacts:
  - File security identification descriptors and remote access control servers, identity management

Supplemental Supporting Artifacts

- Include operating system specific artifacts such as:
    - Windows event log files
    - Registry (all files to reconstruct)
    - Other compound files such as databases (access, oracle and from email servers)
- Artifact Identification & Selection
    - Aided by the creation of templates

Sample Template

Mandatory		
Master File Table	First Sector of Partition	If volume is formatted NTFS
Ntuser.dat	\Documents and Settings\<User>	
Security Event Log SecEvent.Evt	%System%/System32/Config/	
System Event Log SysEvent.Evt	%System%/System32/Config/	

[Example Artifact Template for Windows 2000 Operating System]

What's Not Collected

- Non-relevant data
- Data normally filtered out during the analysis of a collected image
- Essentially RSEC is a shifting of *filtering* from analysis to collection
- Overall time needed for collection and analysis are reduced

A lot of work to do:

- Create formal protocol for artifact identification (platform agnostic)
    - Creation of standards-based XML schema to support protocol (the templates)
    - Create formal RSEC template creation and use procedures
- Develop sample applications
- Choose a single platform to test and evaluate templates in prototype environment
- Publish tests results for peer review

Risk Assessment:
The Costs and Benefits of Risk Sensitive Forensic Methodology

Legal Benefits (1)

- <u>4th Amendment</u> challenges and violations
  - Standard: narrow, particular, reasonable
  - Search warrant drafting ---> invalidation --> evidence elimination
  - "any/all data related to X" ripe for overreaching in network context
- Methodology is responsive to <u>more granular</u> precision

Potential Costs

- Due Process Challenges – LE Duty to Collect

  - Fairness tests
    - Gov't duty to preserve "material exculpatory" evidence <Brady, Agurs>
    - Bad faith if potentially useful <Youngblood>
      - Application: no precedent in this context, but analogize
        - No DP violation when LE fail to preserve breath samples in accordance w/ normal practice <California v. Trombetta>
        - DP violation when clothing material to misidentification defense destroyed <US v. Mclure>

Legal Benefits (2)

- Sensitive to <u>Due Process</u> requirements
  - Ask the right <u>question</u>: **whether LE is constitutionally bound to "find" all relevant evidence, including exonerative electronic information?**
  - **DP imposes no affirmative duty upon the state to use the best available technology <Youngblood>**
  - **LE only required to preserve evidence under its <u>control</u>, absent bad faith failure to preserve potentially useful evidence no violate DP <St. v. Yates>**
  - **Selective acquisition via transparent methodology elicits knowledge, control, duty**

Legal Benefits (2)

- (Con't) Sensitive to DP
  - <u>Standard</u> is not 'proving a negative', rather, that methodology reduces uncertainty of technique
    - Accuracy of collection and testing establish reliability --> inference that 'uncollected' data lack significant exculpatory value
- **Lack of legal guidance favors a <u>practitioner-based</u>, thought-leadership approach**

Scope of LE Duty

- Risk Sensitive Model : LE is not actively "creating" evidence , but rather, is passively serving as bailor of existing evidence

- *Case law supports collection procedures where the process/results cannot be recreated after the fact.*

- Accuracy and consistency of methodology counter challenges

Potential Costs

- 1. <u>Principles-based challenge:</u>
  - Accuracy, completeness, verifiability, reliability challenges
  - Affect admissibility/weight

Legal Benefits (3)

- **Risk-Sensitive <u>Upholds Forensic Principles</u>**

  1. When dealing with digital evidence, all of the general forensic and procedural principles must be applied.

  2. Upon seizing digital evidence, actions taken should not change that evidence.

  3. When it is necessary for a person to access original digital evidence, that person should be trained for the purpose.

  4. All activity relating to the seizure, access, storage or transfer of digital evidence must be fully documented, preserved and available for review.

  5. An Individual is responsible for all actions taken with respect to digital evidence whilst the digital evidence is in their possession.

  6. Any agency, which is responsible for seizing, accessing, storing or transferring digital evidence is responsible for compliance with these principles.

Legal Benefits (4)

- **Where do we turn in absence of precedent on point?**

  -->Analogy: <u>e-Discovery Model</u>

  - **Evidentiary obligations of Preservation Duty
    &
    Risk Sensitive Evidence Collection**

    - **e-Discovery standards derived from same context (resource pressures, reliability requirments)**

    - **e-Discovery principles promoted in Risk Sensitive Evidence Collection Methodology**

Legal Benefits (4) *(Model Principles, con't)*

- **(1) <u>Cost-benefit framework</u>**

    a. **<Zubulake>- define scope of discovery limits** to   **minimize cost and balance fairness**
    - accessible, inaccessible labels
    b. **<u>FRCP</u>- construed and administered to "to secure the just, speedy, and inexpensive determination of every action**
    c. **<u>FRE</u> construed with business in mind**
    d. **<u>Search warrant</u> scope narrowness**

Legal Benefits () (Model Principles, con't)

- **(1) Cost-benefit framework**

    e. <u>Sedona Principles</u>

    "When balancing the cost, burden, and need for electronic data and documents, courts and parties should apply the balancing standard embodied in embodied in Fed. R. Civ. P. 26(b)(2) and its state law equivalents, which requires considering the technological feasibility and realistic costs of preserving, retrieving, producing and reviewing electronic data, as well as the nature of the litigation and the amount in controversy."

Legal Benefits (5) (Model Principles,con't)

- **(2) Reasonableness**
  - **a. FRCP (proposed)**
    - **- no duty to retrieve data not reasonably accessible**
  - **b. <Zubulake>**
    - **"Must a corporation, upon recognizing the threat of litigation, preserve every shred of paper, every email or electronic document, and every backup tape? The answer is clearly, 'no."**
  - **c. Sedona Principles**
    - *"..unreasonable to expect parties to take every conceivable step to preserve all potentially relevant data."* **- deference to reasonable sampling, searching, and selection criteria that determines what is ultimately collected**

Legal Benefits (5) (Model Principles,con't)

-
    (3) <u>Flexible Methodology</u>
    - procedures should be responsive to
        -- particulars of evidence
        -- issues of case
        -- technologies involved

CONCLUSION

The Same, Only Different

- Current v. Risk-Sensitive evidence collection-different methodologies but SAME principles
  - Reasonableness
  - Forensic principles
- Formalizing a methodology to do what is often already done in practice benefits all

Challenges

- Tools to support RSEC are emerging (DFRWS 05')

- Methodology template should capture the domain knowledge for evidence acquisition in complex and large data environment.

Remember

- Just as the mere possibility that something could have happened is not, in and of itself, enough to establish reasonable doubt in a criminal trial, so too is <u>the mere possibility that exculpatory evidence was not acquired enough to support a due process challenge</u>

References

- Kenneally, Brown, "Risk Sensitive Digital Evidence Collection", Digital Investigation (Summer 2005).

- The NIST Disk Imaging Tool Specification 3.1.6 describes technical details of recommended processes uses in bit-stream imaging.

- *California v. Trombetta*, 467 U.S. 479, 485 (1984)

- *United States v. Valenzuela-Bernal*, 458 U.S. 858, 867 (1982)

- *United States v. Agurs*, 427 U.S. 97, 49 L. Ed. 2d 342, 96 S. Ct. 2392 (1976)

References (2)

- *Brady v. Maryland*, 373 U.S. 83, 10 L. Ed. 2d 215, 83 S. Ct. 1194 (1963)
- *Arizona v. Youngblood*, 488 U.S. At 57
- *People v. Eagen*, 892 P.2d 426, 428-29 (Colo. Ct. App. 1994)
- *State v. Yates*, 64 Wn. App. 345, 351, 824 P.2d 519
- *Commonwealth v. Small*, 741 A.2d 666 (Pa. 1999)
- *United States v. Bagley*, 473 U.S. 667 (1985)
- *McCune v. City of Grand Rapids*, 842 F.2d 903, 907 (6th Cir. 1988)

Thank You!

- Questions?
- Don't forget the feedback sheets