

# Revisiting Risk Sensitive Digital Evidence Collection

Erin E. Kenneally[1]  
erin@sdsc.edu

Christopher L. T. Brown[2]  
clbrown@techpathways.com

## Abstract

Over the past decade or so, well-understood procedures and methodologies have evolved within computer forensics digital evidence collection that emphasized disk imaging procedures. In their paper Risk Sensitive Digital Evidence Collection [3], the authors posit that the current methodology which focuses on collecting entire bit-stream images of original evidence disk could increase legal and financial risks. The authors go on to state that the rapidly increasing and changing volume of data within corporate network information systems and personal computers is driving the need to revisit current evidence collection methodologies. No assertion is made in the foundation paper that current methodologies are no longer valid; moreover it is presented that in some situations selective evidence extraction could be accomplished while still ensuring reliability, completeness, accuracy, and verifiability of computer disk evidence.

Risk Sensitive Digital Evidence Collection was presented in three sections with the first section framing the debate and change drivers for a risk-sensitive approach to digital evidence collection. Section 2 outlined the current methods of evidence collection along with a cost-benefit analysis. Section 3 described the methodology components of the risk-sensitive approach to collection, and then concludes with a legal and resource risk assessment of this approach.

This paper will revisit the original abstract methodology framework proposal highlighting the work to be done for successful evaluation and peer review.

## 1. Balancing the Risk: Refining Collection Methods Without Compromising Forensic Principles

Modifying current digital forensic techniques - identification, acquisition, preservation, analysis and presentation - in response to changing contexts does not necessarily mean that results are less reliable for forensic proof purposes. This paper specifically addresses the risks of insisting on bit-stream imaging methodology in large volume (e.g. greater than 200 GB), time-sensitive, and network based contexts. Correspondingly, this paper explores a methodology that balances the risks of selective imaging so that evidentiary reliability can be attained in concert with resource sensitivities. The hallmark of this risk-sensitive methodology is the filtering and reduction of data collection at the front-end acquisition stage, rather than wholesale collection and filtering of data at the back-end examination stage. As such, the goal of reduced legal risk and economic burden is attainable.

A primary risk associated with the current bit-stream imaging process can be gauged by cost metrics- time and resources. Both costs are becoming unmanageable in civil and criminal proceedings, exacting a toll on victims and investigators alike. This derives from the fact that the context within which we are applying our forensic tools and methodology has changed. Computer forensic autopsies are no longer performed on single machines with small data storage capacities. Rather, the scope for potential evidence has expanded to networks of interconnected

computers, each with vast storage capacities containing potential artifacts of legal relevance. This challenges our conceptual and technical ability to erect electronic crime scene tape. Thus, cost pressures must be managed by interpreting and applying traditional standards in parallel with this evolving context.

Specifically, the traditional legal standards of “reasonableness” must continue to shape the application of technology to evidentiary standards. Reasonableness is most often evaluated in terms of the time and resource costs described earlier. Just as it would be unreasonable to expect that investigators cordon-off an entire building, mercury fulminate hundreds of offices for latent fingerprints, and seize every file cabinet during the course of a robbery scene investigation, it is similarly unreasonable to expect the analogous situation in the electronic crime scene even though there is conceivably trace evidence of the crime beyond what was searched and seized. The reasonableness standard takes into account cost and capabilities, and does not require perfection. In this digital forensic setting, factors driving cost include large volume data sets and complicated data accessibility (e.g. network environments).

One risk of remaining steadfast to bit-stream acquisition amidst this emerging resource tug-of-war is the ultimate imperilment to evidentiary reliability- the outright failure to collect digital evidence. It is one issue if this failure can be ascribed to incompetence or mistake, yet quite another when it results from a conscious choice based on insufficient processing resources. The question has become whether forensic professionals will continue to force an ineffective strategy on a changing opponent, or, adapt the strategy to better control against the opponent. The opponent here is the time and resource cost variables, exacerbated by relatively static evidentiary reliability requirements. The strategy here is the methodology chosen to meet evidentiary standards.

## **2. Responding to Change: Risk Sensitive Evidence Collection Methodology**

The proposed Risk Sensitive Evidence Collection Methodology [3] calls for selective artifact extraction during the initial collection phase of the computer forensics process. This methodology can be performed on dead systems using standard connections to the target computer systems such as directly attached IDE converter cables or client/server disk redirection software allowing selective artifact extraction to a forensics collection platform. While selective artifacts of interest can be identified and extracted from a dead system, one of the greatest advantages of this methodology is its ability to allow live system evidence identification and selective extraction while allowing the original systems to continue normal operations. This methodology involves a pre-acquisition evidence search and filtering for purposes of minimizing the collection of irrelevant data, which in the traditional bit-stream methodology occurs post-acquisition during the laboratory examination phase.

Two critical components of the proposed methodology are: (1) live searching and simultaneous identification of evidence, and (2) selective extraction of low-level evidence supporting artifacts from the digital media.

Preliminary high-level methodology requirements are focused on the way in which the collection data connection is made, how the connection is secured and how the data is read, copied and interpreted.

A. Data Connection: It is a well accepted principle within the relevant computer forensics community that in the interests of ensuring evidentiary integrity, software should not be installed on the evidence system. Likewise, this principle serves IT utility goals of minimizing intrusiveness and performance conflicts.

B. Data Integrity: Data integrity goes hand-in-hand with the risk-sensitive evidence collection methodology given the evidentiary demands of reliability, completeness, accuracy, and verifiability.

C. Data Representation: The client application performing live evidence search, identification and extraction should accomplish sector reads of data provided by the remote server agent and reconstruct the data for search and extraction in a read-only approach without changing source metadata. In this client-server analogy note that the remote server agent is an agent running on the potential evidence platform and the client is the imaging, analysis, or extraction platform. Additionally, this client-server methodology does not apply exclusively to network based imaging and analysis but can also apply to isolated direct connections such as USB (Universal Serial Bus), network crossover and parallel port connection types.

(a) File Data Unit: The file data unit will include the contents of the entire file, excluding any data contained in file slack space in the ending cluster. File slack can be defined as non-file-related data contained in the final unused section of last cluster of a file's total allocated clusters.

File storage on disks: Understanding that files stored on a computer hard disk can be of varying size depending on their contents is straight forward. However, the file storage in a file system may be less clear. Hard disk storage allocated for files in DOS and Windows file systems is allocated in fixed length storage areas called clusters. The fixed length attribute of these storage clusters almost guarantees that there will be some area in the final cluster a file resides which is not used by the file. This area is referred to as "file slack". While the data contained in file slack could be of value, the data is rarely related to the file assigned to the cluster. One of the best analogies explaining file slack is that of a video tape. It is helpful to recall a 60 minute video tape in a VCR which contains a 60 minute television program. If that same tape was used to record a 45 minute news program, the tape would contain the new program, but also include 15 minutes of the originally recorded program at the end. While the 15 minutes of "tape slack" in this case may have value, its relevance to the new 45 minute program is only by way of storage location rather than substantive content.

If file slack space is required because it is believed to have relevance to the file being extracted, additional corresponding sector/cluster data unit should be extracted. These additional artifacts

will allow investigators to show a complete map of the file's location on disk and its relationship to file slack.

(b) Sector Data Unit: The sector data unit will include the complete contents of an identified sector in binary and/or ASCII representation.

(c) Mandatory Supporting Artifacts: Each file data unit should be indexed with file metadata including original sector locations of the file on the disk, file hash value in MD5, SHA1 or other suitable hashing algorithm, and file MAC (last modified, accessed, created) times if available. Each sector data unit should be indexed with a hash value provided using a suitable cryptographic algorithm such as MD5 and SHA1. Additional supporting artifacts for the evidence disk should include Disk Manufacture, Disk ID, Disk Geometry, Disk Label and Disk Feature Set if available.

File system artifacts should include any file system meta files such as the MFT (Master File Table) in Windows NTFS. This type of Meta file describes how file systems on disk are organized and used by the higher level operating system, file tables and a complete file system index including any timestamps and file size information. This index should also include any recoverable deleted files.

(d) Identity and Access Control Artifacts: Identity management and object level access control, based on the identity of system users is an important (and often critical) factor in network operating environments. Sometimes managed by a complex array of directories such as LDAP (lightweight directory access protocol), file security identification descriptors and remote access control servers, identity management artifacts can exist in many places throughout a network. Collection of identity management artifacts which clearly indicate specific user's rights as well as access permissions to individual objects is essential and should be considered mandatory. Collection of logs indicating access to systems based on remote access servers can be considered supplemental, although the authors recommend they be mandatory. It is important to note that while identity management and access control are discussed here in the context of network operating environments, they can be present in stand alone operating systems such as LINUX and Windows XP.

(e) Supplemental Supporting Artifacts: For each operating system and environment unique artifacts will be present which may add corroborative weight to mandatory artifacts collected. For example, for all Windows 9x and above, supplemental artifacts may include Windows event log files, registry and other compound files such as databases. The identity of supplemental supporting artifacts would be determined based upon the specific case, operating system and the systems specific environment. Investigators' selection of supplemental artifacts should be aided by a set of templates and/or decision trees. For each of these supplemental files the file data unit's mandatory supporting artifacts should also be collected.

(f) Templates: Each operating system and environment will contain a unique set of artifacts (mandatory and supplemental) which assist in investigations. In some cases each artifact will be specific such as the "Master File Table located in the available partition cluster" in a Windows NTFS -formatted disk. In other cases an artifact will be more general such as

“Database Files” as a generic descriptor for database files (e.g. database.mdb). It is recommended that templates describing mandatory and supplemental artifacts be collected for each group of operating systems. These templates could further be refined to specify artifacts and their location for each specific operating system versions and environments. Practical and proven development of these templates is essential for investigator success and acceptance of this methodology.

By identifying specific mandatory and supplemental supporting artifacts the risk-sensitive evidence collection methodology attempts to eliminate the collection of non-relevant data. Non-relevant data is normally filtered out during the static, laboratory-based digital forensics analysis process. Thus, by shifting the filtering of non-relevant data to the collection phase, costs (time and resources) associated with acquisition and examination are reduced.

Insofar as this paper champions an evolved collection methodology, more granular templates describing technical specifications are needed. The identification of mandatory and supporting artifacts for common digital search and seizure contexts is an effort requiring further research and process control. The authors encourage subsequent development and evaluation of this proposed methodology by the digital forensic community. Further research towards the formalization of Risk Sensitive Digital Evidence Collection should include:

- I. The creation of formal protocol for artifact identification (platform agnostic)
- II. Creation of standards-based XML schema to support protocol (the templates)
- III. Creation of formal RSEC templates and use procedures
- IV. Development of sample applications
- V. Published test results from a single platform test and evaluation using prototype templates and environment

Once the process and templates are clearly defined, the Risk Sensitive Evidence Collection Methodology can become a valuable addition to the computer forensics investigators tool set. It is important to highlight that the Risk Sensitive Evidence Collection Methodology is an additional methodology to be implemented in a suitable situation that would benefit stakeholders. In cases where collection of entire disk in a bit-stream fashion under current forensics methodologies remains reasonable, the existing methodology should continue to be used.

### **3. Addressing the Legal Risks of the Evolved Collection Methodology**

#### **A. Fourth Amendment Protection Against Unreasonable Searches and Seizures.**

One notable risk of adhering to legacy bit-stream methodology is a mounting of 4th Amendment challenges and violations. This is likely to take the form of challenges to search warrants and subsequent elimination of evidence in the worst cases, and search warrant drafting difficulties in the best cases. Specifically, adherence to legacy dogma that “everything” must be requested, search warrants may be invalidated on their face if their scope overreaches the 4<sup>th</sup> Amendment standards of narrowness, particularity, and reasonableness.

Alternatively, even if a warrant for electronic evidence is scoped and issued properly, the execution of search and seizure procedures may violate the warrant. Specifically, insistence on bit-stream imaging of all data could amount to the equivalent of electronic bulldozing, attendant by a high risk of collecting irrelevant, proprietary, privileged and/or privacy-protected data. This virtual scooping can threaten to pollute the admissibility of the entire corpus of the search and seizure. As judges authorize the execution of search warrants to be conducted in increasingly less time, forensic investigators need to have a community-vetted methodology that avoids intimation of ad hoc search procedures yet is responsive to time constraints imposed by legal orders.

## **B. Due Process Constitutional Protections**

One major legal underpinning likely to be raised by opponents of the evolved method is based on the constitutionally guaranteed access to evidence under the Due Process clause of the 5th and 14th Amendments.<sup>1</sup> This fundamental standard of fairness has been interpreted to oblige the government to afford criminal defendants a meaningful opportunity to present a complete defense. It also imposes a duty on the government to preserve and disclose “material exculpatory” evidence for use by the defense.<sup>2</sup> Furthermore, the government's failure to preserve material exculpatory evidence violates the criminal defendant's rights regardless of whether the government acted in good or bad faith.<sup>3</sup> *Arizona v. Youngblood*, a seminal case articulating the test for fairness, further requires that the defendant demonstrate the police acted in bad faith in failing to preserve the evidence when the evidence sought by the defense is not "material exculpatory" evidence but is potentially useful to the defense.<sup>4</sup> Also, a defendant's failure to request material exonerative evidence does not relieve the government from disclosing it.<sup>5</sup>

To be sure, there is no single interpretation of “bad faith”, and no court has rendered an opinion in the specific facts suggested herein. However, bad faith has been found in cases where it is clear that evidence has been deliberately destroyed or hidden<sup>6</sup>, and in certain instances when LE deviates from standard operating procedures for handling evidence.<sup>7</sup> However, courts will consider whether LE is acting in good faith based on an accepted methodology and/or the nature of the data at hand. Given that there is no case on point which has interpreted bad faith in the context of either the traditional or proposed methodology, the duty to preserve electronic data might best be gauged by asking whether LE is constitutionally bound to “find” all relevant evidence, including exonerative electronic information? What is LE's duty to collect and preserve digital evidence? To what extent must LE exhaust or even pursue the search for digital evidence?

*Youngblood* clarified that the right to due process is limited and opined that the Court has been unwilling to "impos[e] on the police an undifferentiated and absolute duty to retain and to preserve all material that might be of conceivable evidentiary significance in a particular prosecution."<sup>8</sup> A showing that the evidence might have exonerated the defendant is not enough. In order to be considered "material exculpatory evidence", the evidence must both have apparent exculpatory value before it was destroyed, and there must have been no other reasonable means to obtain comparable evidence by other reasonably available means.<sup>9</sup>

Relying on *Trombetta's* test for fairness, Risk-Sensitive approach relies upon the accuracy of the collection and testing process to help establish the reliability of the methodology, thus supporting an inference that the missing data lacked significant exculpatory value.<sup>10</sup> Furthermore, the Risk Sensitive Methodology draws upon case law that supports collection procedures where the process/results cannot be recreated after the fact. It is further predicated on the predominant legal standard of "reasonableness" which is determined in light of the peculiar circumstance and context of each case.

Bad faith can be measured by LE's control over the potential evidence. To be sure, it is difficult to predict the exonerative value of evidence that does not currently exist because it was either never collected or has been destroyed, discarded, or lost. A key distinction lies in whether the government has control over the quality and quantity of what is collected and preserved, versus situations where investigators are at the mercy of what is left behind, analogous to a microscopic remnant of blood or partial latent fingerprint. LE is only required to preserve evidence under its control and unless the challenger can show bad faith by LE, failure to preserve potentially useful evidence does not violate due process.<sup>11</sup>

The suggested Risk Sensitive model does not facilitate ignorance of potentially exculpatory evidence, and in fact, is designed to reflect and embed collection of artifacts with highly probable evidence based on the practical experience and laboratory testing of forensic practitioners. In this way, investigators can avoid the digital equivalent of failing to interview witnesses, conscious disregard for contrary hypotheses, or indifference to relevant evidence.

### **C. Evidentiary Reliability**

The purpose of measuring the reliability of this methodology is to reduce the uncertainty about the contribution made by the technique, not to prove the contribution that was made. In other words, the point is not to prove a negative- that this methodology did not miss exculpatory evidence- because that sets up a strawman for any attempt to gain legal groundswell for this methodology.

An anticipated legal objection to this Risk Sensitive Methodology is that it fails to provide complete, verifiable, and/or accurate results, thus inviting authenticity or reliability challenges and threatening evidence admissibility or relative weight in a legal proceeding.

The standard for reliability is invoked if the data collected via the methodology is the basis for expert testimony.<sup>12</sup> In cases where evidence gathered via this methodology is being presented as substantive, and not the basis for expert testimony, reliability proof is moot and any challenges would go to the weight of the evidence, as is the case with the evidence derived from the traditional methodology. In situations where the *Daubert* standard is invoked, reliability challenges based on lack of testing, peer review, known and error rate, general acceptance are merely based on the immaturity of the Risk Sensitive approach as opposed to substantive dissonance among the relevant forensic community. Thus, as this methodology is tested and deployed in amongst practitioners, the outcome of a *Daubert* scrutiny will become apparent and ripe for reliability determinations. Furthermore, it is helpful to note that even the traditional,

"established" bit-stream methodology is subject to the very same challenges based on the non-exhaustive factors elicited in *Daubert*.

The standard for authentication is that there is a 'reasonable likelihood that the evidence is what it purports to be'. Under this standard, courts have generally not been receptive to such claims in the absence of specific evidence of alteration. Therefore, the offeror of evidence is not required to rule out all possibilities inconsistent with authenticity. This means that the Risk Sensitive methodology need not produce results that are 100% complete, accurate and verifiable in order to meet admissibility standards. Also, data authentication may not necessarily be precluded by the use of examination software that alters non-essential data but had no significant effect on the substantive data.<sup>13</sup>

Regarding authenticity based on completeness, to be sure, it is impossible to verify the existence/or lack thereof of evidence in a dynamic environment since the parameters of the digital crime scene can be quite difficult to define. The Risk Sensitive method does not freeze time for the entire corpus of the digital crime scene, only selective portions. Nevertheless, for those selected pieces of data, the same court-vetted hashing techniques used in traditional methodology to ensure evidence integrity is employed to authenticate that what was originally captured is the same as what is being presented in court. Furthermore, courts have upheld evidence as meeting the authentication threshold in situations where the accuracy of the testing on the uncollected evidence was sufficient to infer lack of exculpatory value.<sup>14</sup>

In response to challenges to Best Evidence requirements, copies and duplicates are deemed to have satisfied this standard if they are shown to "reflect the data accurately." The question of how accuracy is established can be inferred from courts' acceptance of hashing technique verification as discussed earlier.<sup>15</sup> Therefore, selective collection challenges can be thwarted by reliance on hash verification, no different than how challenges to the traditional methodology are countered.

#### **D. Upholding Forensic Principles**

The Risk Sensitive method is based on the same core forensic principles which the traditional methodology seeks to uphold.<sup>16</sup> These include:

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.<sup>17</sup>

As applied to the Risk Sensitive methodology, it is apparent that this approach does not run afoul of the principles espoused therein.

While the courts will ultimately opine on the reliability of a methodology, digital forensics practitioners should not wait for the adjudicative process to define appropriate methodologies. First, most reported computer forensics cases come from trial courts and have little precedential value. Second, since few computer forensics cases get appealed, there is not much guidance to be gained from courts of appeals. Even when such cases are appealed, appellate review is a deferential standard, so most of the methodology determinations will remain at the trial court level. Finally, decisions that are reported generally involve cases at the far end of the spectrum, thus arguably offering dubious guidance to those methodologies generated from mainstream activities.

#### **4. Conclusion**

While the current and proposed evidence collection methodologies appear contradictory, they are both derived from the same principled evidentiary basis. Significant differences include the overall quantity of data initially collected, and the bifurcated search methodology involving both pre- and post acquisition identification of evidence based on relevancy determinations. Completeness must not be adjudged by the relative quantitative differences between the two methodologies. Rather, completeness should continue to be measured by the legal standards of reasonableness and relevance. The advantage of collecting everything is that the search for relevant evidence can be prolonged and extended or revisited if supported by proper legal process. However, the costs associated with acquiring “all” data, in comparison to the costs of taking a risk-sensitive approach, strongly advocate for adoption of this revised methodology.

Analogizing to the familiar physical crime scene scenario, the traditional methodology would call for the equivalent of mercury fulminating and photographing the entire building and objects residing for purposes of capturing any and all relevant evidence during a felony investigation. The impracticality and unreasonableness of that approach reinforces acceptance of physical forensic methodologies where the forensic investigator must make real time evidence identification and acquisition decisions based on resource practicalities and crime context. This reality is becoming more favorable in the digital forensics arena, where the deluge of digital artifacts is precluding wholesale seizure of digital buildings.

The challenges lie in gaining general acceptance from the relevant community, which will lead to the development of tools and the training to allow investigators to identify and collect relevant digital data reducing the overall risk of oversight. This groundswell, de facto acceptance of what is occurring in practice must also be formalized by endorsement from authoritative bodies within the digital forensics practitioner community. 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 the mere possibility that exculpatory evidence was not acquired enough to support a due process challenge.

Insofar as this paper champions an evolved collection methodology, more granular templates describing technical implementations are needed. The identification of mandatory and

supporting artifacts for common digital search and seizure contexts is an effort requiring further research and process control. The authors encourage subsequent development and evaluation of these templates by the digital forensic community.

Current tools and techniques are evolving in step with environmental pressures and forensic needs to offer the capability to conduct Risk Sensitive Evidence Collection. Distributed search tools offering faster evidence and relating artifact selection are emerging which should help mitigate trained investigator apprehension to selective evidence collection.

## ENDNOTES

[1] Erin Kenneally, M.F.S., J.D. is a licensed Attorney who holds Juris Doctorate and Master of Forensic Sciences degrees. Ms. Kenneally consults, researches, publishes, and speaks on prevailing and forthcoming issues at the crossroads of information technology and the law. This includes evidentiary, procedural, and policy implications related to digital forensics, information security and privacy technology. She has lectured and helped coordinate training conferences for officers of the court, law enforcement, and industry professionals concerned with digital evidence and information forensics. She is a Cyber Forensics Analyst at the San Diego Supercomputer Center, liaises and holds leadership positions with the Computer and Technology Computer High Tech Task Force (CATCH) and the Global Privacy and Information Quality Working Group, and provides thought leadership to numerous private and government advisory committees engaged in information technology law issues.

[2] Christopher L. T. Brown, CISSP is the Founder and CTO of Technology Pathways, LLC a provider of Security Products and Services for Corporate, Legal and Government communities. Mr. Brown is the chief architect of the Technology Pathways ProDiscover family of security products. Prior to his position with Technology Pathways Mr. Brown has served in key positions at several companies including GlobalApp, Inc., CompuVision, Inc., and StoragePoint, Inc. Mr. Brown teaches network security and computer forensics at the University of California at San Diego and has written numerous books on Windows, the Internet and forensics. Mr. Brown's most recent book "Computer Evidence: Collection and Preservation" is published by Charles River Media. Mr. Brown retired from a career with the U.S. Navy where he managed a team of 80 technicians working in the area of Information Warfare and Network Operations. He holds numerous career certifications from UCSD, (ISC)2, Microsoft, CISCO, CompTIA and CITRIX.

[3] Risk Sensitive Digital Evidence Collection, Erin E. Kenneally, Christopher L.T. Brown, Digital Investigations Journal Volume 2 Issue 2, Elsevier, August, 2005

[4]

---

<sup>1</sup>See, *California v. Trombetta*, 467 U.S. 479, 485 (1984); see also, *United States v. Valenzuela-Bernal*, 458 U.S. 858, 867 (1982)>.

<sup>2</sup><See *United States v. Agurs*, 427 U.S. 97, 49 L. Ed. 2d 342, 96 S. Ct. 2392 (1976); *Brady v. Maryland*, 373 U.S. 83, 10 L. Ed. 2d 215, 83 S. Ct. 1194 (1963)>.

<sup>3</sup> *Arizona v. Youngblood*, 488 U.S. At 57.

<sup>4</sup> *Youngblood*, 488 U.S. At 57-58.

<sup>5</sup> *United States v. Bagley*, 473 U.S. 667 (1985).

<sup>6</sup> See *McCune v. City of Grand Rapids*, 842 F.2d 903, 907 (6th Cir. 1988)>; where procedures have been engineered that were likely to produce misleading evidence (*Youngblood*, 488 U.S. At 58).

<sup>7</sup>In both *Killian* and *Trombetta*, the Court noted good faith and established conventions: "In failing to preserve breath samples for respondents, the officers here were acting 'in good faith and in accord with their normal

---

practice." *California v. Trombetta*, 467 U.S. 479, 488 (quoting *Killian v. United States*, 368 U.S. 231, 242 (1961)). In *Colorado v. Bertine*, in approving an inventory search, the Court thought it significant that there had been "no showing that the police, who were following standard procedures, acted in bad faith or for the sole purpose of investigation." 479 U.S. 367, 372 (1987). See also *United States v. Watkins*, 188 F.3d 520 (10th Cir. 1999) (finding no bad faith where the defense failed to support its argument that the agent's destruction of witness interview notes violated DEA policy because it offered no proof of that policy at trial).>

8 *Youngblood*, 488 U.S. at 58

9 *Trombetta*, 467 U.S. At 489.

10 *Id.*, the Court noted that categorical evidence of the accuracy of the testing process- the Intoxilyzer's measurement of samples, could supply the missing predicate. Since that machine was highly accurate, was periodically and frequently checked for malfunction, and had rare false positives that were caused by known interferences that could be investigated and disproved in a particular case, the Court found that the evidence of test results was highly reliable and thereby concluded that the missing breath samples lacked significant exculpatory value.

11 *State v. Yates*, 64 Wn. App. 345, 351, 824 P.2d 519 (citing *State v. Starka*, 116 Wn.2d 859, 884, 810 P.2d 888 (1991)), review denied, 119 Wn.2d 1017 (1992).

12 Technical expert opinion is admissible if it is based on sufficient facts/data, is the result of reliable principles and methods, and the expert has applied the principles and methods reliably. See, Fed. R. Evid. 702 (as amended); *Daubert v. Merrell Dow Pharmaceuticals*, 509 U.S. 579 (1993), the foremost case establishing guidelines for the Federal standard for expert testimony reliability; and, *Kumho Tire Co., Ltd., v. Carmichael*, 526 U.S. 137 (1999), which extended *Daubert* to technical areas other than those considered strictly scientific.

13 See, National Institute of Justice Computer Crime and Intellectual Property Section, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations (July 2002) available at <<http://www.cybercrime.gov/searching.html#A>>.

14 See, FN 31 and accompanying text.

15 See, *State v. Cook*, 149 Ohio App. 3d 422, 2002 Ohio 4812, 777 N.E.2d 882, (Ohio Ct. App., Montgomery County Sept. 13, 2002).

<sup>16</sup>The IOCE was formed in 1995. In December 1997, the G8 High Tech Crime Sub-Group tasked IOCE to develop international standards for the exchange of digital evidence. By November 1999, the first product was ratified by IOCE. During 2000, the IOCE proposal was substantially accepted. See, Report on Digital Evidence, 13th INTERPOL Forensic Science Symposium, Lyon, France, October 16-19 2001, available at <<http://www.interpol.int/Public/Forensic/IFSS/meeting13/Reviews/Digital.pdf>>

<sup>17</sup> These principles were recommended by the G8 as developed by IOCE. See, International Organization on Computer Evidence (IOCE) First Responders Guide Template (December, 2000), available at <<http://ncfs.org/documents/ioce2000/reports/firstResponders.pdf>>; see also, IOCE Principles and Definitions, available at <<http://ncfs.org/documents/ioce2002/reports/principlesDefinitions.pdf>>