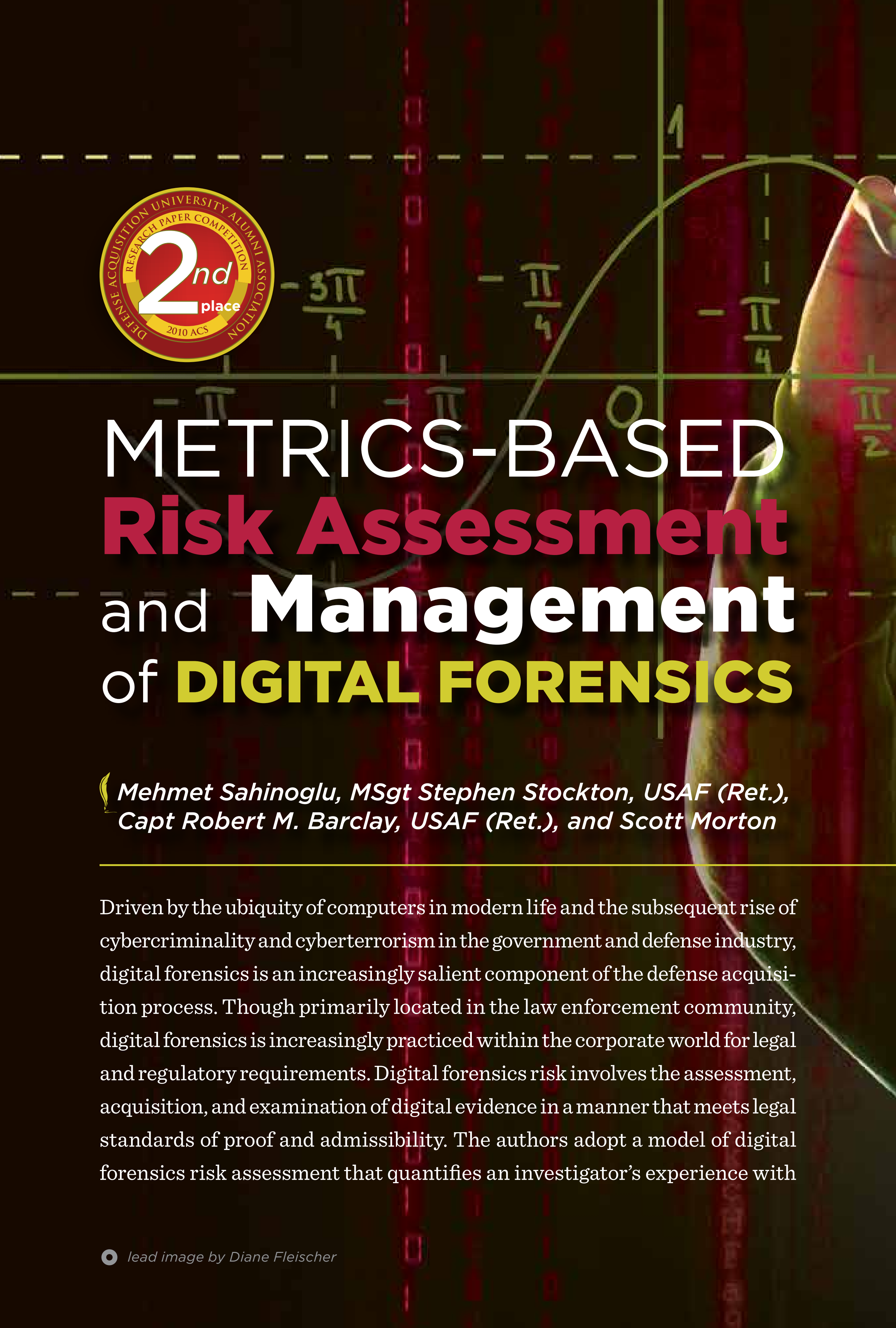


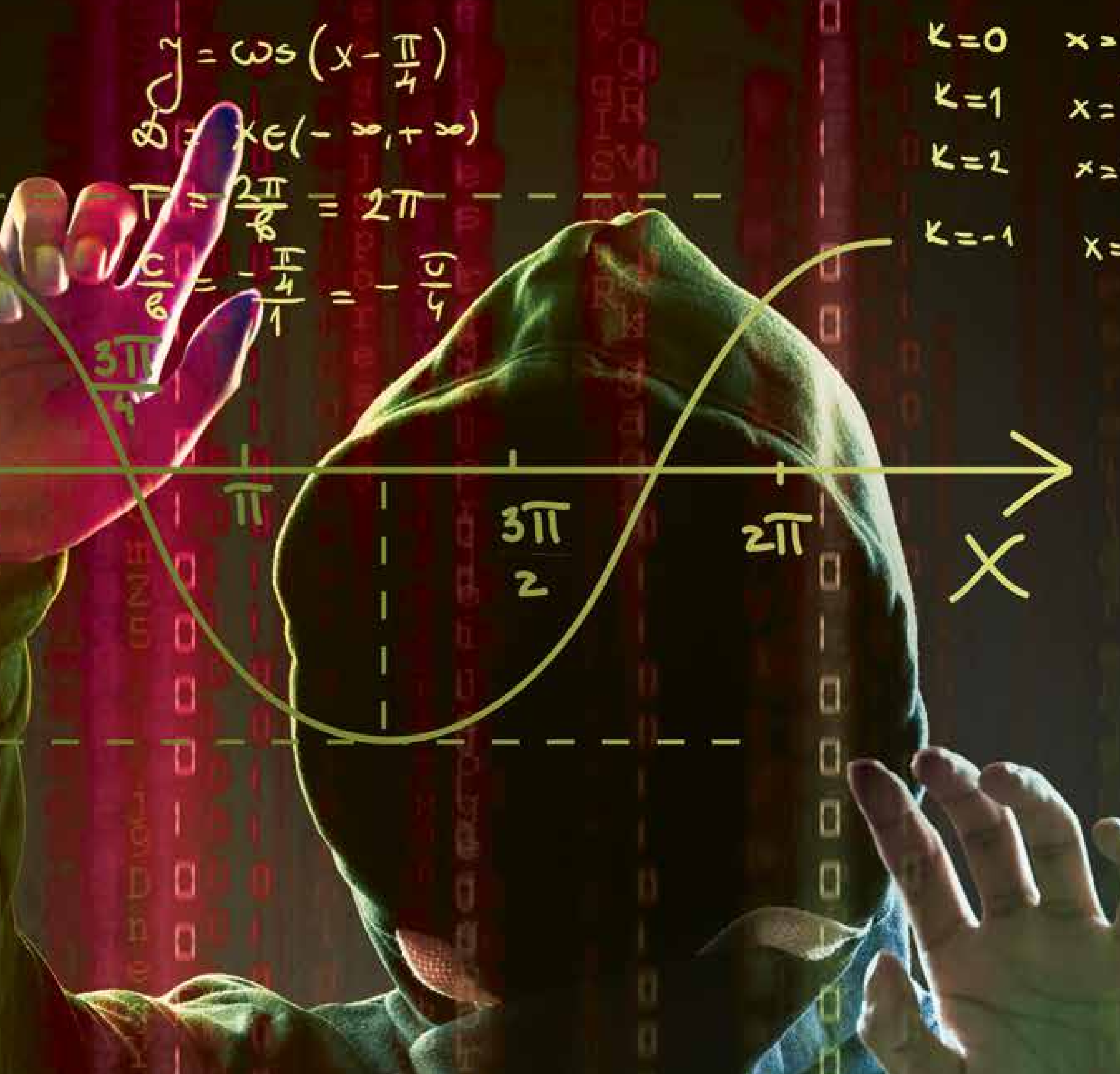
DEFENSE ACQUISITION UNIVERSITY ALUMNI ASSOCIATION
RESEARCH PAPER COMPETITION
2nd place
2010 ACS

METRICS-BASED Risk Assessment and Management of DIGITAL FORENSICS

Mehmet Sahinoglu, MSgt Stephen Stockton, USAF (Ret.), Capt Robert M. Barclay, USAF (Ret.), and Scott Morton

Driven by the ubiquity of computers in modern life and the subsequent rise of cybercriminality and cyberterrorism in the government and defense industry, digital forensics is an increasingly salient component of the defense acquisition process. Though primarily located in the law enforcement community, digital forensics is increasingly practiced within the corporate world for legal and regulatory requirements. Digital forensics risk involves the assessment, acquisition, and examination of digital evidence in a manner that meets legal standards of proof and admissibility. The authors adopt a model of digital forensics risk assessment that quantifies an investigator's experience with

lead image by Diane Fleischer

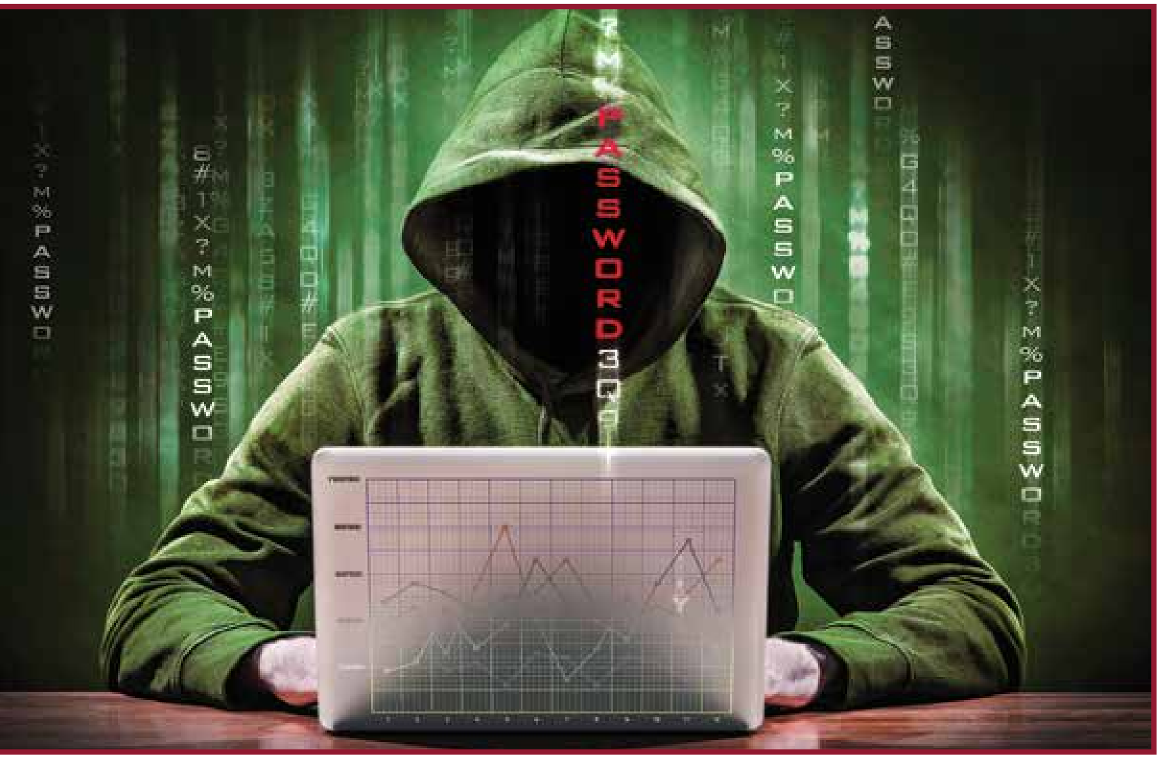


eight crucial aspects of the digital forensics process. This research adds the concept of quantifying through a designed risk meter algorithm to calculate digital forensics risk indices. Numerical and/or cognitive data were painstakingly collected to supply input parameters to calculate the quantitative risk index for the digital forensics process. Much needed risk management procedures and metrics are also appended.

Keywords: *Cyberterrorism, cybercriminality, risk meter*

Digital forensics is a topic that has been popularized by television programs such as *CSI.* Crime-solving glamour and drama aside, the reality is that the digital forensics process is a highly technical field that depends on the proper implementation of specific, well-accepted protocols and procedures. Inadequate forensic tools and technical examination, as well as lack of adherence to appropriate protocols and procedures, can result in evidence that does not meet legal standards of proof and admissibility. Digital forensics risk arises, for example, when personnel lack the proper tools to conduct investigations, fail to process evidentiary data properly, or do not follow accepted protocols and procedures.

Assessing and quantifying digital forensics risk is the goal of this article. To do so, the authors utilize a digital forensics risk meter, based on a series of questions designed to assess respondents' perceptions of digital forensics risk. Based on the responses, a digital forensics risk index will be calculated. Where this approach differs is that other approaches typically provide general guidance in the form of best practices, classification schemes or, at best, a checklist for digital forensics procedures, and do not provide quantitative tools (based on game theory) for risk management and mitigation. Examples of other such approaches follow:



- U.S. Department of Justice, *Forensic Examination of Digital Evidence: A Guide for Law Enforcement* (general guidelines and worksheets) (U.S. Department of Justice, 2004)
- *Error, Uncertainty, and Loss in Digital Evidence* (certainty levels) (Casey, 2002)
- *Cyber Criminal Activity Analysis Models using Markov Chain for Digital Forensics* (suspicion levels) (Kim & In, 2008)
- *Two-Dimensional Evidence Reliability Amplification Process Model for Digital Forensics* (evidence reliability) (Khatir, Hejazi, & Sneiders, 2008)
- *Building a Digital Forensic Laboratory: Establishing and Managing a Successful Facility* (checklist) (Jones & Valli, 2011)

One approach that does employ quantification, *Metrics for Network Forensics Conviction Evidence,* is confined to network forensics—mostly measuring severity impact—and does not provide mitigation advice (Amran, Phan, & Parish, 2009). In that research article, the authors show “how security metrics can be used to sustain a sense of credibility to network evidence gathered as an elaboration and extension to an embedded feature of Network Forensics Readiness (NFR).” They then propose “a procedure of evidence acquisition in network forensics ... then analyze a sample of a packet data in order to extract useful information as evidence through a formalized intuitive model, based on capturing adversarial behavior and layer analysis, ... apply the Common Vulnerability Scoring System—or CVSS metrics to show the severity of network attacks committed...”(p. 1).

The digital forensics risk meter presented in this article will provide objective, automated, dollar-based risk mitigation advice for interested parties such as investigators, administrators, and officers of the court to minimize digital forensics risk. Figure 1 represents a decision tree diagram to assess risk; Figure 2 (with the Advice column on the right extracted from Figure B-1, Appendix B) represents sample mitigation advice generated from the respondents’ inputs. This article will not only present a quantitative model, but will generate a prototype numerical index that facilitates appropriate protocols and procedures to ensure that legal standards of proof and admissibility are met.

FIGURE 1. DIGITAL FORENSICS RISK DIAGRAM

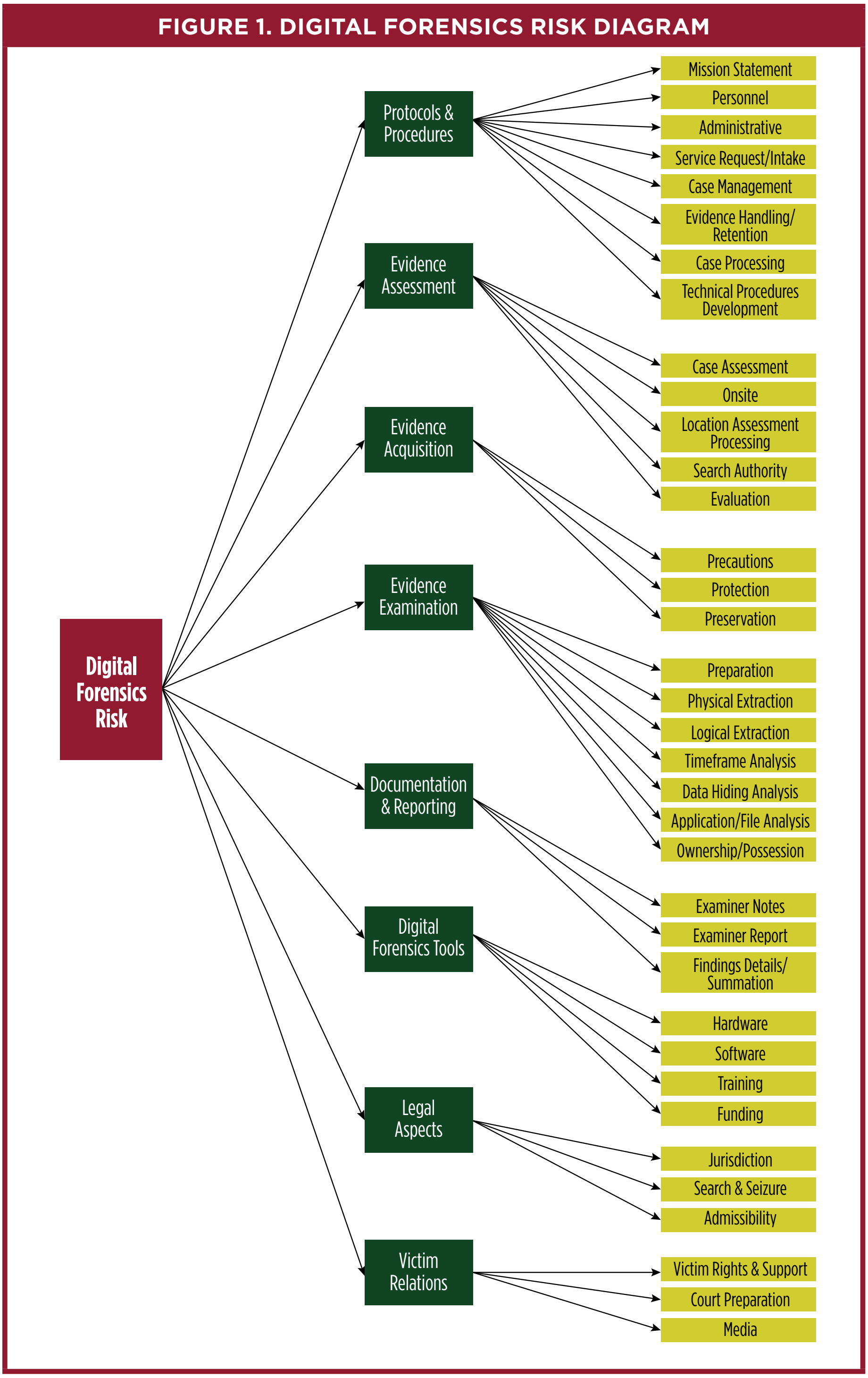


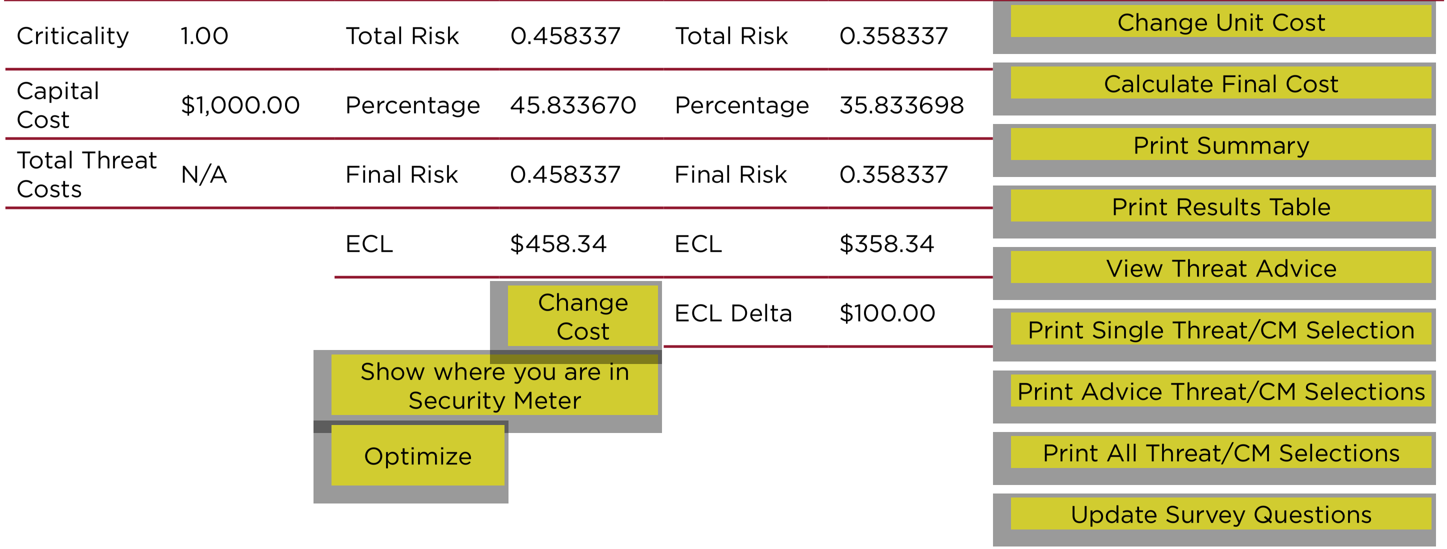
FIGURE 2. MEDIAN DIGITAL FORENSICS RISK METER RESULTS MITIGATED TO 35.83%

Vulnerab.	Threat	CM & LCM	Res. Risk	CM & LCM	Res. Risk	Change	Opt Cost	Unit Cost	Final Cost	Advice
0.220042	0.415771	0.325000		0.325000						
		0.675000	0.061754	0.675000	0.061754					
	0.237754	0.375000		0.375000						
		0.625000	0.032697	0.625000	0.032697					
	0.346476	0.550000		0.550000						
		0.450000	0.034308	0.450000	0.034308					
0.317111	0.559259	0.450000		0.721705		0.271705	$49.77			Increase the CM capacity for threat “Examiner Notes” for the vulnerability of “Documentation & Reporting” from 45.00% to 72.17% for an improvement of 27.17%
		0.550000	0.097541	0.278295	0.049355					
	0.440741	0.375000		0.375000						
		0.625000	0.087352	0.625000	0.087352					

FIGURE 2. MEDIAN DIGITAL FORENSICS RISK METER RESULTS MITIGATED TO 35.83%, CONTINUED

Vulnerab.	Threat	CM & LCM	Res. Risk	CM & LCM	Res. Risk	Change	Opt Cost	Unit Cost	Final Cost	Advice
0.462847	0.408269	0.725000		0.999195		0.274195	$50.23			Increase the CM capacity for threat “Victim Rights & Support” for the vulnerability of “Victim Relations” from 72.50% to 99.92% for an improvement of 27.42%
		0.275000	0.051966	0.000805	0.000152					
	0.250646	0.575000		0.575000						
		0.425000	0.049305	0.425000	0.049305					
	0.341085	0.725000		0.725000						
	0.275000	0.043414	0.275000	0.43414						
						Total Change	Total Cost	Break Even Cost	Total Final Cost	
						54.59%	$100.00	$1.83		

FIGURE 2. MEDIAN DIGITAL FORENSICS RISK METER RESULTS MITIGATED TO 35.83%, CONTINUED



Criticality	1.00	Total Risk	0.458337	Total Risk	0.358337
Capital Cost	$1,000.00	Percentage	45.833670	Percentage	35.833698
Total Threat Costs	N/A	Final Risk	0.458337	Final Risk	0.358337
		ECL	$458.34	ECL	$358.34
				ECL Delta	$100.00

Change Unit Cost
Calculate Final Cost
Print Summary
Print Results Table
View Threat Advice
Print Single Threat/CM Selection
Print Advice Threat/CM Selections
Print All Threat/CM Selections
Update Survey Questions
Change Cost
Show where you are in Security Meter
Optimize

Note. CM = Countermeasure; ECL = Expected Cost of Loss; LCM = Lack of Countermeasure; Opt = Optimize to; Res. Risk = Residual Risk; Vulnerab. = Vulnerability.

Vulnerabilities, Threats, and Countermeasures

Based on industry best practices guidelines, such as the U.S. Department of Justice (2004) *Forensic Examination of Digital Evidence: A Guide for Law Enforcement,* eight specific vulnerabilities are assessed:

1. Protocols and Procedures
2. Evidence Assessment
3. Evidence Acquisition
4. Evidence Examination
5. Documentation and Reporting
6. Digital Forensics Tools
7. Legal Aspects
8. Victim Relations

Within each vulnerability category, questions pertain to specific threats and countermeasures. For example, within the Evidence Acquisition vulnerability, respondents are asked questions regarding precautions, protection, and preservation threats and countermeasures. Within the Evidence Examination vulnerability, respondents are asked questions regarding preparation, physical extraction, logical extraction, timeframe analysis, data hiding analysis, application/file analysis, and ownership/possession threats and countermeasures. Within the digital forensics Tools vulnerability, respondents are asked questions regarding hardware, software, training, and funding threats and countermeasures. Figure 1 details these vulnerabilities and threats. The responses are then used to generate a quantitative Digital Forensics risk index.

Assessment Questions

Questions are designed to elicit responses regarding the perceived risk to proper Digital Forensics procedures, evidence handling/examination, admissibility, and other associated issues from particular threats, as well as the countermeasures the respondents may employ to counteract those threats. For example, in the Evidence Examination vulnerability, questions regarding the data hiding analysis threat include both threat and countermeasure questions. Threat questions would include:

- Do file headers not correspond to file extensions?
- Did the suspect encrypt or password-protect data?
- Are hidden messages present?
- Are host-protected areas (HPA) present?

Countermeasure questions would include:

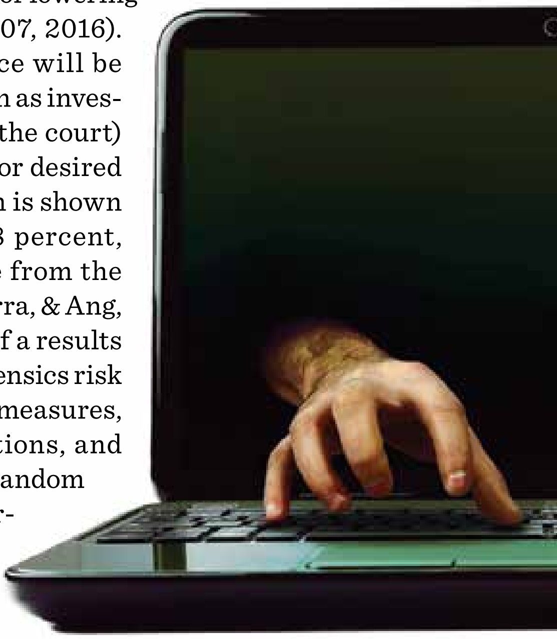
- Did the examiner correlate file headers to the corresponding file extensions to identify any mismatches that may indicate the user intentionally hid data?

- Did the examiner gain access to all password-protected, encrypted, and compressed files, which may indicate an attempt to conceal the data from unauthorized users?
- Did the examiner conduct a thorough stenographic analysis?
- Did the examiner gain access to HPAs that may indicate an attempt to conceal data?

Sample vulnerability (Evidence Acquisition) assessment questions employed in the digital forensics risk meter are found in Appendix A. Appendix A also clarifies and precludes confusion between Evidence Acquisition and materiel acquisition. The first proactive step in any digital forensic investigation is acquisition. The inherent problem with digital media is that it is readily modified just by accessing files. Working from a copy is one of the fundamental steps to making a forensic investigation auditable and acceptable to a court (Acquisition, n.d.).

Risk Calculation and Risk Management through Surveys

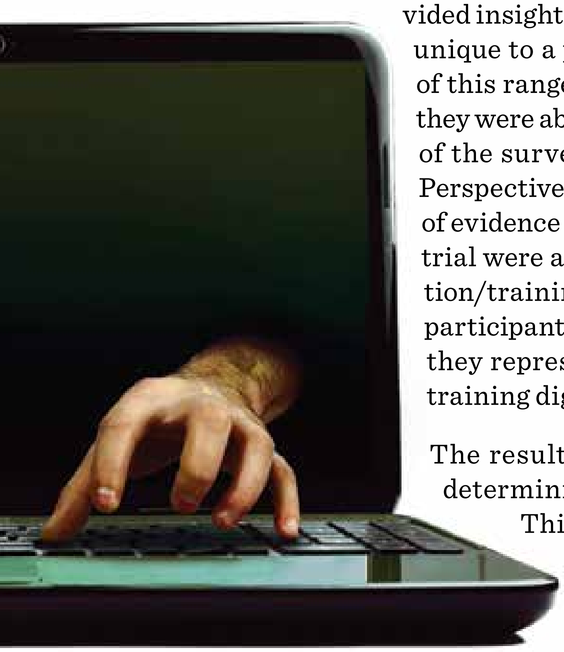
Based on their experience, the respondents answer yes or no to the survey questions. These responses are then used to calculate residual risk. Employing a game-theoretical mathematical approach, the calculated risk index is used to generate an optimization or lowering of risk to desired levels (Sahinoglu, 2007, 2016). A more detailed set of mitigation advice will be generated to show interested parties (such as investigators, administrators, and officers of the court) where risk can be reduced to optimized or desired levels. An example of such risk reduction is shown in Figure 2, from 45.8 percent to 35.8 percent, which represents the median response from the study participants (Sahinoglu, Cueva-Parra, & Ang, 2012). Figure 2 is an actual screenshot of a results table, representing the median digital forensics risk meter results displaying threat, countermeasures, residual risk indices, optimization options, and risk mitigation advice. For this study, a random sample of responses from 27 survey participants was analyzed; their residual



risk results are tabulated and presented in Appendix B. The survey portfolio used in this assessment and upon which this research article is based showed the complexity of the digital forensics field, encompassing tools, procedures, specific training, budget, and trial.

Digital forensics has two crucial phases (Appendix A). The first phase included all the forensics involved with the collection of data, while the second phase concerns defending the data collected, the means by which the data were collected, and chain of custody applied from the original collection until court (Sahinoglu, Stockton, Morton, Barclay, & Eryilmaz, 2014). The initial goal was to obtain survey input from local city leaders in Montgomery, Alabama. Although individuals from the Governor's Office, Montgomery Police Department, and District Attorney's office were willing to assist, our short timeframe and their busy schedules prevented their offices from providing input to the digital forensics survey. Fortunately, the authors had contacts at other law enforcement offices, which agreed to make personnel available for the survey and eventual follow-up. Eventually, three law enforcement offices and one special investigation/training organization participated and provided valuable input.

Our first objective was to explain the purpose of the survey and the potential value the combined results could offer each of the offices. At each location, participants included investigators, initial responders, digital forensics specialists, and legal experts (i.e., District Attorney Office personnel). The range of expertise of the participants was invaluable, as each provided insight into an aspect of the survey that is often unique to a position within a department. Because of this range of expertise, the authors are confident they were able to capture the three main components of the survey portion of the Risk-o-Meter (RoM). Perspectives from collection of evidence, packaging of evidence for trial, and presentation of evidence at trial were all given. Although the special investigation/training organization had many fewer survey participants, they did offer a unique perspective, as they represented an organization that focuses on training digital forensics experts for the military.



The results were then run for each participant, determining the Initial Repair Cost to Mitigate. This was determined by using a Criticality of 1.0, Equipment Cost of $0.0, and a

Production Cost of $1,000. The median of all results was determined and then optimized through the RoM to determine the best “bang for the buck” that would reduce the participant’s Total Residual Risk by 10 percent. The initial Total Residual Risk for the median participant was 45.8 percent, with an Expected Cost of Loss (ECL) of $458.34. Once optimized, the Total Risk was reduced to 35.8 percent, and the ECL was reduced by $100 to a total ECL of $358.34 (Figure 2). The first optimized solution was to increase the countermeasure (CM) capacity for the “Examiner Notes” threat for the Documentation and Reporting vulnerability from 45.0 percent to 72.17 percent, for an improvement of 27.17 percent. The second optimized solution was to increase the CM capacity for the “Victim Rights and Support” threat for the Victim Relations vulnerability from 72.50 percent to 99.92 percent, for an improvement of 27.42 percent.

Table B-2 in Appendix B depicts a set of constrained linear equations used within the body of the risk meter’s innovative second-stage software for the game-theoretic optimization necessary to create the Advice column (shown on the right in Figure 2). The Advice column’s original survey calculations are depicted in Figure B-1, which displays company ECSO8: 14th Ranked Overall Median Survey. This is followed by Figure B-2, which displays company OPD1’s Group Median Survey Taker’s Original Survey Outcome; while Figure B-3 displays company AUPD5’s Group Median Survey Taker’s Original Survey Outcome. In each case, the company representative seemed impressed with the results and noted the results for possible future implementation. One organization actually commented that they had already begun looking into increases in at least one CM that was identified by the optimization. Clearly, this episode validated the tool and its usefulness in their eyes.

Discussion and Conclusions

The advantages of conducting business on the Internet have been well documented. Conducting business online is frequently faster and cheaper than utilizing traditional methods. However, this comes with the digital forensics-related vulnerabilities and pertinent threats that tend to convert the positive advantages to clear disadvantages as a result of fraud and wrongdoing. With the advent of the Internet and burgeoning information systems, digital forensics has gained worldwide momentum. In every environment, the content of digital information relative to criminal undertakings and investigations alike has vastly increased, growing disproportionately to the capacities of state and local governments, as well as federal agencies and military components. The risk assessment, risk mitigation, or general risk management that involve planned investment policy in order of priority, with a sound and auditable, cost-effective approach, are missing links. The proposed digital forensics risk meter is an innovative initiative that provides a quantitative assessment of risk to the user as well as recommendations for mitigating that risk. This approach will be a highly useful tool to interested parties such as investigators, company or system administrators, and officers of the court seeking to minimize and thereby mitigate digital forensics risk by leveraging and introducing early, preventive CMs identified as an outcome of this dynamic closed-end survey.

> ***This approach will be a highly useful tool to interested parties such as investigators, company or system administrators, and officers of the court seeking to minimize and thereby mitigate digital forensics risk by leveraging and introducing early, preventive CMs identified as an outcome of this dynamic closed-end survey.***

Additional future research by the principal author will involve the addition of cloud computing concerns such as service provider cooperation and data accessibility, as well as the incorporation of new questions so as to better refine user responses and subsequent calculation of risk and mitigation recommendations. Minimization or mitigation of digital forensics risk will greatly facilitate the success of digital forensics investigations, ensuring that legal standards of proof and admissibility are ultimately met. The digital forensics risk meter tool provides the means to identify areas where risk can be minimized, as well as giving the objective, dollar-based mitigation advice to do just that. This aspect of objective quantifiable risk assessment and management will add to the trustworthiness of acquisition practices in terms of dependable Internet communications involving great quantities of materiel and their budgetary repercussions.

Limitations and Future Research

The limitations are obvious due to input data deficiency, but methods such as the one proposed in this article are a good way to start due to the objective, hands-off, automated, cost-effective treatment of the problem at hand. Sound assessment of digital forensics risk can result when information entered, from learned respondents, is as close to the truth as feasibly possible. The discussion that follows clarifies how this proposed work is directly relevant to acquisition reisk mitigation if applied appropriately within a system.

This research article is not focused on the usual law enforcement or digital-policing procedures, but is directed towards greater awareness for the in-house (e.g., acquisition community) workforce as they manage already existing risk assessment and risk management algorithms. By leveraging the countermeasures outlined in this article (in particular, the Advice column in Figure 2, which employs probability-estimation and game-theoretic risk computing), the authors anticipate that acquisition practitioners can better preclude future digital forensics breaches by taking timely CMs.

Law enforcement, in cooperation with the defense acquisition community, is increasingly becoming an important player in digital forensics, thereby lending increased scrutiny in this vital area. Law enforcement is more aware of evidence such as drug cartel activity and money laundering through all avenues such as export, import, and domestic acquisition activities. Even in homicide cases, much useful evidence can be deduced by using digital forensics information. In addition, digital forensics sciences not only can break a difficult case, but can do so quickly and inexpensively compared to police detectives' usual time-tested, but tedious practices. The proposed risk meter software and its algorithm can successfully lead the way toward navigating the stages of cost-effective risk assessment and management.

In conclusion, the best "bang for the buck" derives from simple usability and scientific objectivity.

References

Acquisition. (n.d.). In Wikibooks. Retrieved from https://en.wikibooks.org/wiki/Introduction_to_Digital_Forensics/Acquisition

Amran, A. R., Phan, R. C. W., & Parish, D. J. (2009). Metrics for network forensics conviction evidence. *Proceedings of the International Conference for Internet Technology and Secured Transactions (ICITST), Institute of Electrical and Electronics Engineers* (pp. 1–8), London, England. doi: 10.1109/ICITST.2009.5402640

Casey, E. (2002, Summer). Error, uncertainty, and loss in digital evidence. *International Journal of Digital Evidence, 1*(2). Retrieved from https://utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf

Jones, A., & Valli, C. (2011). *Building a digital forensic laboratory: Establishing and managing a successful facility*, Burlington, MA: Butterworth Heinemann & Syngress.

Khatir, M., Hejazi, S. M., & Sneiders, E. (2008). Two-dimensional evidence reliability amplification process model for Digital Forensics. *Proceedings of the IEEE Third International Annual Workshop on Digital Forensics and Incidents Analysis* (WDFIA 2008) (pp. 21–29), Malaga, Spain. doi: 10.1109/WDFIA.2008.11

Kim, D. H., & In, H. P. (2008). Cyber criminal activity analysis models using Markov chain for Digital Forensics. *Proceedings of the 2nd International Conference on Information Security and Assurance* (pp. 193–198), Busan, Korea. doi: 1109/ISA.2008.90

Sahinoglu, M. (2007). *Trustworthy computing: Analytical and quantitative engineering evaluation*. Hoboken, NJ: John Wiley.

Sahinoglu, M. (2016). *Cyber-risk informatics: Engineering evaluation with data science*. Hoboken, NJ: John Wiley.

Sahinoglu, M., Cueva-Parra, L., & Ang, D. (2012, May-June). Game-theoretic computing in risk analysis. *Wiley Interdisciplinary Reviews: Computational Statistics, 4*(3), 227–248. doi: 10.1002/wics.1205. Retrieved from http://authorservices.wiley.com/bauthor/onlineLibraryTPS.asp?DOI=10.1002/wics.1205&ArticleID=961931

Sahinoglu, M., Stockton, S., Morton, S., Barclay, R., & Eryilmaz, M. (2014, November 20). Assessing Digital Forensics risk: A metric survey approach. *Proceedings of the SDPS 2014 Malaysia, 19th International Conference on Transformative Science and Engineering, Business and Social Innovation*, Sarawak, Malaysia. Retrieved from https://www.researchgate.net/publication/268507819_ASSESSING_DIGITAL_FORENSICS_RISK_A_METRIC_SURVEY_APPROACH

U.S. Department of Justice. (2004). *Forensic examination of digital evidence: A guide for law enforcement*. Retrieved from https://www.ncjrs.gov/pdffiles1/nij/199408.pdf

Appendix A

Sample Vulnerability (Evidence Acquisition, Documentation and Reporting, and Victim Relations) Assessment Questions (in XML format) and Survey Template

```
<survey>
<vulnerability title= “Evidence Acquisition” level= “0”>
<vQuestion> Are special precautions not taken to preserve digital evidence?
</vQuestion>
<vQuestion> Was write protection not utilized to preserve and protect
original evidence? </vQuestion>
<vQuestion> Was digital evidence not secured in accordance with
departmental guidelines? </vQuestion>
<vQuestion> Was speed the primary concern when it came to acquiring
digital evidence? </vQuestion>

<threat title = “Precautions”>
<tQuestion> Was evidence on storage devices destroyed or altered?
</tQuestion>
<tQuestion> Was equipment damaged by static electricity and magnetic
fields? </tQuestion>
<tQuestion> Was the original internal configuration of storage devices and
hardware unnoted? </tQuestion>
<tQuestion> Were investigators unable to provide drive attributes?
</tQuestion>

<threat title = “Protection”>
<tQuestion> Was CMOS/BIOS information not captured? </tQuestion>
<tQuestion> Was the computer’s functionality and the forensic boot disk
not tested? </tQuestion>
<tQuestion> Did the forensic boot disk not boot? </tQuestion>
<tQuestion> Did the investigators not collect drive configuration information
from the CMOS/BIOS? </tQuestion>

<threat title = “Preservation”>
<tQuestion> Did the investigators not perform the acquisition using the
examiner’s system? </tQuestion>
<tQuestion> Was a RAID present in the subject system? </tQuestion>
<tQuestion> Was host-specific data not captured? </tQuestion>
<tQuestion> Was successful acquisition not verified? </tQuestion>

</threat>
</vulnerability>
</survey
```

DIGITAL FORENSICS RISK SURVEY

This survey has 8 main categories of vulnerabilities. Please identify the areas below where you have observed vulnerabilities while involved with digital forensics activities within your organization.

** A minimum of 2 categories must be chosen:*

Vulnerability Area		**Reference Page**
❑	Protocols & Procedures	Pages 1 & 2
❑	Evidence Assessment	Pages 3 & 4
❑	Evidence Acquisition	Page 5
❑	Evidence Examination	Pages 6 & 7
❑	Documentation & Reporting	Page 8
❑	Digital Forensics Tools	Page 9
❑	Legal Aspects	Page 10
❑	Victim Relations	Page 11

DIRECTIONS:

This Page:

- Select all vulnerability areas that apply
- Proceed to appropriate pages to complete survey for each vulnerability area

Survey Page(s):

Vulnerability

- Rate **Vulnerability** (0.1–10) with 10 being *most* vulnerable and 0.1 being *least* vulnerable
- Select all vulnerability statements that apply (*must choose at least one*)

Threat

- Rate **Threat** (0.1–10) with 10 being *greatest* threat and 0.1 being the *least* threat
- Using square check box, select all threat statements that apply to each threat category chosen (*must choose at least one*)

Countermeasure

- Rate associated **Countermeasure** for each threat category chosen above (0.1–10) with 0.1 being *least* effective and 10 being the *most* effective countermeasure
- Using square check box, select all countermeasure statements that apply (*must choose at least one*)

Rate (01.–10) if vulnerability applies

Vulnerability: Legal Aspects

- □ Legal authority for forensic examinations is unclear
- □ The extent of the authority to search is unstated
- □ Courtroom admissibility is not a prime consideration

Must select one (minimum) for each Vulnerability selected

Rate (0.1–10) for all Threats that apply

Threat: Jurisdiction	**Countermeasures**
□ There is conflicting jurisdiction	□ Jurisdiction is established among agencies prior to investigations
□ Multiple jurisdictions are often involved	□ Investigators and other officials from different areas coordinate and cooperate on cases
□ Potential evidentiary data are stored on the cloud or some other distant network resource	□ Court orders are obtained when requiring distant service providers to provide potentially evidentiary data
□ Cases often cross international borders	□ There are bilateral or multilateral agreements that facilitate cooperation with foreign law enforcement agencies

Threat: Search & Seizure	**Countermeasures**
□ Cases are often challenged for lack of probable cause	□ Forensic investigators unequivocally identify and articulate a probable cause necessary to obtain search warrants
□ On-site investigators often proceed without knowledge of a warrant	□ Search warrants are obtained prior to investigation on site
□ Investigators go beyond warrants originally used to assert search authority	□ New search warrants are obtained as new evidence is uncovered to avoid charges of “stale” warrants
□ The evidentiary chain of custody is often challenged	□ Full documentation of the evidentiary chain of custody is maintained throughout the investigation

Threat: Admissibility	**Countermeasures**
□ Digital evidence is sometimes changed by seizure	□ Strict measures are taken to ensure that when seizing digital evidence, the action does not change that evidence
□ Individuals besides forensic investigators access original digital evidence	□ Only forensically competent persons are allowed access to original digital evidence
□ Does activity related to cases come under legal/judicial review	□ All activities related to seizures, access, storage, or transfer of digital evidence are fully documented, preserved, and available for legal/judicial review
□ The state of evidence is often unknown prior to opening files	□ Evidence is “frozen” prior to opening the files

Must select one (minimum) Threat for each vulnerability selected

Appendix B

Respondent Results Tabulations

TABLE B-1. COMPANIES'/RESPONDENTS' (AFIT, AUPD, ECSO, OPD) SURVEY RESULTS FOR DIGITAL FORENSICS RISK METER STUDY

Survey Taker	Residual Risk %	Ranked Overall (Out of 27)	Remarks
AFIT1	52.47	6th	2nd out of 4 within AFIT
AFIT2	49.90	9th	3rd out of 4 within AFIT
AFIT3	52.71	5th	1st out of 4 within AFIT
AFIT4	47.64	10th	4th out of 4 within AFIT
AUPD1	31.15	26th	7th out of 7 within AUPD
AUPD2	39.67	20th	5th out of 7 within AUPD
AUPD3	50.02	8th	1st out of 7 within AUPD
AUPD4	36.98	21st	6th out of 7 within AUPD
AUPD5	44.59	16th ~ *Overall Average*	4th out of 7 within AUPD
AUPD6	46.06	13th	3rd out of 7 within AUPD
AUPD7	47.06	11th	2nd out of 7 within AUPD
ECSO1	51.80	7th	5th out of 9 within ECSO
ECSO2	46.66	12th	6th out of 9 within ECSO
ECSO3	56.94	2nd	2nd out of 9 within ECSO
ECSO4	57.67	1st	1st out of 9 within ECSO
ECSO5	54.87	3rd	3rd out of 9 within ECSO
ECSO6	41.36	19th	9th out of 9 within ECSO
ECSO7	54.84	4th	4th out of 9 within ECSO
ECSO8	45.83	14th *Overall Average*	7th out of 9 within ECSO
ECSO9	45.01	15th	8th out of 9 within ECSO
OPD1	35.00	23rd	4th out of 7 within OPD
OPD2	42.56	18th	2nd out of 7 within OPD
OPD3	44.35	17th	1st out of 7 within OPD
OPD4	33.39	25th	6th out of 7 within OPD
OPD5	28.23	27th	7th out of 7 within OPD
OPD6	34.39	24th	5th out of 7 within OPD
OPD7	36.41	22nd	3rd out of 7 within OPD

Note. Respondents are ranked within and overall, where Median is 45.83% (ECSO8) and Average is 44.73% (AUPD5: 44.49% is the closest respondent to 44.7%).

TABLE B-2. SET OF CONSTRAINED LINEAR EQUATIONS FOR TABLE B-1'S MEDIAN

Min COLLOSS (Column loss), s. t. (subject to):
$CM_{11} < 1$ **(1)**, $CM_{12} < 1$ **(2)**, $CM_{13} < 1$ **(3)**, $CM_{21} <1$ **(4)**, $CM_{22} <1$ **(5)**, $CM_{31} <1$ **(6)**,
$CM_{32} <1$ **(7)**, $CM_{33} <1$ **(8)**, COLLOSS <1 **(9)**

$CM_{11} > 0.675$ **(10)**, $CM_{12} > 0.475$ **(11)**, $CM_{13} > 0.725$ **(12)**,
$CM_{21} > 0.725$ **(13)**, $CM_{22} > 0.725$ **(14)**,
$CM_{31} > 0.675$ **(15)**, $CM_{32} > 0.675$ **(16)**, $CM_{33} > 0.675$ **(17)**,

$0.09148\ CM_{11}$ -1COLLOSS < 0 **(18)**, $0.05231\ CM_{12}$ -1COLLOSS < 0 **(19)**,
$0.07629\ CM_{13}$ -1COLLOSS < 0 **(20)**, $0.17734\ CM_{21}$ -1COLLOSS < 0 **(21)**,
$0.13966\ CM_{22}$ -1COLLOSS < 0 **(22)**, $0.18896\ CM_{31}$ - 1COLLOSS < 0 **(23)**,
$0.11601\ CM_{32}$ -1COLLOSS < 0 **(24)**, $0.15787\ CM_{33}$ -1COLLOSS < 0 **(25)**,

$0.09148\ CM_{11} + 0.05231\ CM_{12} + 0.07629\ CM_{13} + 0.17734\ CM_{21} + 0.13966\ CM_{22} +$
$0.18896\ CM_{31} + 0.11601\ CM_{32} + 0.15787\ CM_{33} > 1- 0.3583 = 1- 0.3583 = 0.6417$ **(26)**

Note. Used to attain a risk mitigated to 35.83% from an undesirable 45.83% inspired by Figure 2; where Total # Constraints = 3 * #Selected Threats + 2 = 3 * 8 + 2 = 24 + 2 = 26 along with Objective(Min).

FIGURE B-1. ECSO8: 14TH RANKED OVERALL MEDIAN SURVEY TAKER'S ORIGINAL SURVEY OUTCOME

VB	vb	Threat	threat	LCM	Risk	Post %	Post vb	>
Protocols and Procedures	0.220042	Personnel	0.415771	0.675000	0.061754	0.13		
		Administrative	0.237754	0.625000	0.032697	0.07		
		Service Request/Intake	0.346476	0.450000	0.034308	0.07	0.280926	!
Documentation and Reporting	0.317111	Examiner Notes	0.559259	0.550000	0.097541	0.21		
		Examiner Report	0.440741	0.625000	0.087352	0.19	0.403401	!
Victim Relations	0.462847	Victim Rights and Support	0.408269	0.275000	0.051966	0.11		
		Court Preparation	0.250646	0.425000	0.049305	0.11		
		Media	0.341085	0.275000	0.043414	0.09	0.315673	

Criticality	**1.00**
Capital Cost	**$1,000.00**
Total Threat Costs	**N/A**
Res-Risk* Criticality	**0.458337**
Total Res-Risk	**0.458337**
Expected Cost of Loss	**$458.34**
Cust. Guess Res-Risk	**0.50**

FIGURE B-2. OPD1: GROUP MEDIAN SURVEY TAKER'S ORIGINAL SURVEY OUTCOME

VB	vb	Threat	threat	LCM	Risk	Post %	Post vb	>
Evidence Assessment	0.309524	Onsite	0.585714	0.450000	0.081582	0.23		
		Evaluation	0.414286	0.450000	0.057704	0.16	0.397961	!
Digital Forensics Tools	0.247253	Software	0.422222	0.550000	0.057418	0.16		
		Training	0.577778	0.325000	0.046429	0.13	0.296705	!
Victim Relations	0.443223	Victim Rights and Support	0.438889	0.250000	0.048631	0.14		
		Court Preparation	0.258333	0.450000	0.051525	0.15		
		Media	0.302778	0.050000	0.006710	0.02	0.305333	
Criticality		**1.00**						
Capital Cost		**$1,000.00**						
Total Threat Costs		**N/A**						
Res-Risk* Criticality		**0.349998**						
Total Res-Risk		**0.349998**						
Expected Cost of Loss		**$350.00**						
Cust. Guess Res-Risk		**0.50**						

FIGURE B-3. AUPD5: GROUP MEDIAN SURVEY TAKER'S ORIGINAL SURVEY OUTCOME

VB	vb	Threat	threat	LCM	Risk	Post %	Post vb	>
Protocols and Procedures	0.162121	Administrative	0.225000	0.650000	0.23710	0.05		
		Service Request/Intake	0.285417	0.500000	0.023136	0.05		
		Case Management	0.214583	0.675000	0.023482	0.05		
		Case Processing	0.275000	0.675000	0.030094	0.07	0.225211	!
Evidence Examination	0.203030	Physical Extraction	0.500000	0.650000	0.065985	0.15		
		Data Hiding Analysis	0.500000	0.450000	0.045682	0.10	0.250428	!
Documentation and Reporting	0.219192	Examiner Notes	0.500000	0.450000	0.049318	0.11		
		Examiner Report	0.500000	0.625000	0.068497	0.15	0.264218	!
Legal Aspects	0.132323	Search and Seizure	1.000000	0.325000	0.043005	0.10	0.096445	
Victim Relations	0.283333	Victim Rights and Support	0.310096	0.275000	0.024162	0.05		
		Court Preparation	0.347556	0.225000	0.022157	0.05		
		Media	0.342348	0.275000	0.026675	0.06	0.163697	
Criticality		**1.00**						
Capital Cost		**$1,000.00**						
Total Threat Costs		**N/A**						
Res-Risk* Criticality		**0.445903**						
Total Res-Risk		**0.445903**						
Expected Cost of Loss		**$445.90**						
Cust. Guess Res-Risk		**0.50**						

Biographies

Dr. Mehmet Sahinoglu is the founding director of the Informatics Institute and Cybersystems and Information Security Graduate Program at Auburn University at Montgomery. Formerly the Eminent Scholar and Chair-Professor at Troy University's Computer Science Department, he holds a BS and MS in Electrical and Computer Engineering from Middle East Technical University-Ankara and University of Manchester Institute of Science and Technology, United Kingdom, respectively; and a PhD in Electrical and Computer Engineering and Statistics from Texas A&M, jointly. Dr. Sahinoglu conducts research in Cyber-Risk Informatics. He is the author of *Trustworthy Computing* (2007) and *Cyber-Risk Informatics: Engineering Evaluation with Data Science* (2016)—both with Wiley Interscience.

(E-mail address: msahinog@aum.edu)

MSgt Stephen Stockton, USAF (Ret.), has over 25 years in the IT field. He has developed, sustained, and operated military information systems. His experience includes application design, development, software lifecycle management, and software security. He has BS and MS degrees in Computer Science from Saint Leo University and Troy State University. He is currently enrolled in the Cybersystems and Information Security Master's Program at Auburn University at Montgomery. MSgt Stockton worked as a senior software engineer for General Dynamics after retiring from the USAF and now serves as an acquisition program manager at Maxwell-Gunter AFB.

(E-mail address: stephen.stockton.3@us.af.mil)

Capt Robert M. Barclay, USAF (Ret.), is currently a part-time research and teaching associate at Auburn University at Montgomery, and he is the IT security manager for the State of Alabama's Unified Judicial System, responsible for network security for the State Courts since 2009. He was previously employed by General Dynamics, and he was also employed by Troy State University at Montgomery for IT security and distance learning. He has 33 years of combined military and civilian service in IT security and related forensics experience. He holds a BS in Information Systems Management and is currently pursuing an MS in Cybersecurity, both from the University of Maryland.

(E-mail address: robert.barclay@alacourt.gov)

Mr. Scott Morton is a part-time research associate at Auburn University at Montgomery and adjunct professor on Cybersecurity and CS Programming at Troy University Montgomery campus and South University in Montgomery. He holds an MS in Computer Science with summa cum laude from Troy University Montgomery and a BA in International Relations from Johns Hopkins University. He currently researches Cybersystem Security Risk Assessment and Management.

(E-mail address: smorton1@aum.edu)