

Haris Hamidovic, CIA, ISMS IA, is chief information security officer at Microcredit Foundation EKI Sarajevo, Bosnia and Herzegovina. Prior to his current assignment, Hamidovic served as IT specialist in the NATO-led Stabilization Force (SFOR) in Bosnia and Herzegovina. He is the author of four books and more than 60 articles for business and IT-related publications. Hamidovic is a certified information technology expert appointed by the Federal Ministry of Justice of Bosnia and Herzegovina and the Federal Ministry of Physical Planning of Bosnia and Herzegovina.

The Relevance of IT in Criminal Investigations An Introduction to Expert Testimony

As a result of increasing interconnectivity, information systems and networks are now exposed to a growing number and a wider variety of threats and vulnerabilities.¹

Given that threats posed to organizations by cybercrimes have increased faster than potential victims—or cybersecurity professionals—can cope with them,² an increase in requests for IT expert testimony is expected.

The main activity of the court in a criminal proceeding and the main goal of the criminal procedure is the determination of facts necessary to decide the disputed matters.³ Judges cannot be expected to be knowledgeable on other issues than the law, and in particular, they are not expected to have any specialized knowledge on any technical subject matter. The judge is expected to have the same general knowledge of issues as any common citizen.⁴

Given that judges do not have the necessary technical expertise required to establish all relevant facts and make a final decision, the court invites an expert to provide insight to establish the necessary facts. Numerous and extensive analysis of case law shows that expertise has become almost a regular part of criminal procedures, but lack of it is also the most common reason for delays and overall inefficiency of criminal procedures.⁵ Expert testimony is subject to the rules of criminal procedure, but also must be conducted under the rules of the expert's specific professional subject area.

The main objective of this article is to point out some of the specifics and problems of expert testimony in the field of IT. To do so, the article presents a general process of expert testimony in criminal proceedings, using the Bosnia and Herzegovina perspective as an example, which can be applied internationally.

THE CONCEPT OF EXPERTISE

Expertise is a process in which—under orders of the prosecutor or court and in compliance with the conditions prescribed by law—experts, in

accordance with the rules of their field of science, technical knowledge, skills or artistic orientation, examine objects of testimony and subsequently provide their expert findings and opinion.⁶

An expert is not required if the court can understand and evaluate the evidence without help from those with specialized knowledge and understanding of a subject area.

Experts may also be engaged by defendants and their counsel. The task of the experts, engaged by one of the parties, is to oversee the expertise rendered on behalf of other parties and to safeguard the rights and position of their party.⁷

EXPERT TESTIMONY PROCESS⁸

The expert testimony process generally has three phases:

- **Introductory**—Provides a preparation for the operational phase. The expert is first introduced to the legal standards governing expert testimony. The criminal case and the expertise task are then presented to the expert. The material to be the subject of the expert analysis and any supporting documentation are provided to the expert. The subject of the evaluation and the questions that need to be answered are introduced to the expert.
- **Operational**—Expert testimony is directly performed in the operational phase. It is conducted by the expert by applying methods and means in accordance with his/her profession and adhering to the requirements of the prosecutor or the court.
- **Concluding**—The expert, based on his/her evaluation, gives an opinion. The expert witness presents findings and opinion, and worksheets, sketches and notes to the authority that ordered the expertise.

The opinion of the expert may be given before the court in the form of a categorical or a hypothetical conclusion. When giving a categorical conclusion, the expert is confident in the merits of his/her findings, while in a hypothetical conclusion, the expert presents just an assumption—a version



Do you have something to say about this article?

Visit the *Journal* pages of the ISACA web site (www.isaca.org/journal), find the article, and choose the Comments tab to share your thoughts.

of the controversial circumstances (subject of expertise). Ideally, the expert is always able to present before the court a categorical opinion about the existence of disputed facts; however, sometimes an expert is not able to offer a categorical conclusion, but only a probable (hypothetical) one.

The expert gives the findings and opinions on his/her free belief, which is based solely on special knowledge, examination results and expert assessment. How and what methods should be used for testing must be determined by the expert. Other participants in the proceedings should not affect the expert.

Evaluation has to be performed solely on the evidence presented to the expert by the prosecutor or the court. If the expert determines that, for the opinions and findings, it is necessary to get new evidence and obtain new items, the expert can make the suggestion to the prosecutor or the court to obtain the additional material needed.

Expert testimony is subject, just as any other evidence, to free judicial evaluation. In assessing the testimony of expert witnesses, the court should always look through the prism of the procedural provisions and rules of the profession for which it engaged the expert.

SCIENTIFIC EVIDENCE

Application of scientific knowledge in specific circumstances is the essence of expertise. The scientific component of the expertise conclusion is crucial for the value of expert testimony in criminal proceedings.⁹

Four criteria, developed in the case of *Daubert v. Merrell Dow Pharmaceuticals Inc.*,¹⁰ for the admissibility and validity of scientific evidence almost always apply to digital forensics in US federal cases and most international cases.¹¹ The test of scientific evidence includes four basic issues:

1. Can the theory or technique be tested (has it been)?
2. Is there a high, known or potential rate of error; are there standards controlling the technique's operation; and are the standards being maintained?
3. Has the theory or technique been subjected to peer review and publication?
4. Does the theory or technique hold "general acceptance" within the relevant scientific community?

IT EXPERT TESTIMONY

Given that the number of criminal offenses related to cybercrime is increasing,¹² an increase in requests for IT expert testimony is also expected.

In many respects, IT evidence is just like any other evidence; however, the following characteristics warrant special consideration:¹³

- **Design**—Computer systems will only create and retain electronic records if specifically designed to do so.
- **Volume**—The large volume of electronic records causes difficulties with storage and prolongs the discovery of a specific electronic record.
- **Commingling**—Electronic records that relate to a specific wrongdoing are mixed with unrelated electronic records.
- **Copying**—Electronic copies can be immediately and perfectly copied; after which, it is difficult—and, in some cases, impossible—to identify the original from the copy. In other cases, a purported copy may be deliberately or accidentally different from the original, and, hence, evidentially questionable.
- **Volatility**—Electronic records can be immediately and deliberately or accidentally altered and expunged.
- **Automation**—Electronic records may be automatically altered or deleted.

Given the ubiquity of digital evidence, it is the rare crime that does not have some associated data stored and transmitted using computer systems. Despite its prevalence, few people are well versed in the evidentiary, technical and legal issues related to digital evidence, and as a result, digital evidence is often overlooked, collected incorrectly or analyzed ineffectively.¹⁴

CONCLUSION

The most effective way to prevent unauthorized access to information systems and data is the introduction and development of effective security measures; however, a comprehensive response must include the threat and use of measures of criminal law. Criminal prohibition of unauthorized access will give extra protection to information systems and data.

Forms of computer crime are characterized by great diversity. Given that judges do not possess the technical expertise necessary to establish all relevant facts regarding cybercrime, the court invites experts to provide expertise to establish the necessary facts.

Application of scientific knowledge in specific circumstances is the essence of expertise. The scientific component of the expert conclusion is crucial for the value of expert testimony in criminal proceedings. To increase the quality and probative value of expert testimony, it is necessary to standardize all of the important stages of expertise.

ENDNOTES

- ¹ Organisation for Economic Co-operation and Development (OECD), *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*, 2002
- ² Deloitte, *Cyber crime: A Clear and Present Danger*, 2010
- ³ Council of Europe, European Commission, "Commentary on the Criminal Procedure of Bosnia and Herzegovina," 2005
- ⁴ United Nations Mission in Bosnia Herzegovina (UNMIBH), "The Testimony of Expert Witnesses: Use and Misuse of Expert Testimony—Program Evaluation of the Judicial System," 2000
- ⁵ *Op cit*, Council of Europe 2005
- ⁶ "Law of Criminal Procedure of Bosnia and Herzegovina," *Official Gazette of Bosnia and Herzegovina*, No. 36, 21 November 2003
- ⁷ *Op cit*, Council of Europe 2005
- ⁸ *Ibid*.
- ⁹ *Op cit*, Council of Europe 2005
- ¹⁰ *Daubert v. Merrell Dow Pharmaceuticals Inc.* (1993) 509 U.S. 579, 113 S.Ct. 2786, 125 L.Ed.2d 469
- ¹¹ Cohen, Fred; *Challenges to Digital Forensic Evidence*, Fred Cohen & Associates, 2008
- ¹² US Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Deloitte, "2010 CyberSecurity Watch Survey," CSO, January 2010
- ¹³ Standards Australia, HB 171-2003, *Guidelines for the Management of IT Evidence*, 2003
- ¹⁴ Eoghan, Casey; *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*, 2nd Edition, Academic Press, 2004

The *ISACA Journal* is published by ISACA. Membership in the association, a voluntary organization serving IT governance professionals, entitles one to receive an annual subscription to the *ISACA Journal*.

Opinions expressed in the *ISACA Journal* represent the views of the authors and advertisers. They may differ from policies and official statements of ISACA and/or the IT Governance Institute® and their committees, and from opinions endorsed by authors' employers, or the editors of this *Journal*. *ISACA Journal* does not attest to the originality of authors' content.

© 2011 ISACA. All rights reserved.

Instructors are permitted to photocopy isolated articles for noncommercial classroom use without fee. For other copying, reprint or republication, permission must be obtained in writing from the association. Where necessary, permission is granted by the copyright owners for those registered with the Copyright Clearance Center (CCC), 27 Congress St., Salem, MA 01970, to photocopy articles owned by ISACA, for a flat fee of US \$2.50 per article plus 25¢ per page. Send payment to the CCC stating the ISSN (1526-7407), date, volume, and first and last page number of each article. Copying for other than personal use or internal reference, or of articles or columns not owned by the association without express permission of the association or the copyright owner is expressly prohibited.

www.isaca.org