



## *For Further Reading...*

This bibliography was created by the National Clearinghouse for Science, Technology and the Law to accompany the Crime Scene to Courtroom Forensics webinar *Electronic Evidence Essentials II: Data, Information and Knowledge*.  
**October 2019**

### **Books & Reports**

Andre Arnes, ed., Digital Forensics (Wiley 2017) <https://www.wiley.com/enus/Digital+Forensics-p-9781119262411>

ASTM International, Standard Terminology for Digital and Multimedia Evidence Examination (ASTM E2916-13) <https://www.astm.org/Standards/E2916.htm>

Eoghan Casey, Handbook of Digital Forensics and Investigation (Academic Press 2009) <https://www.elsevier.com/books/handbook-of-digital-forensics-and-investigation/casey/978-012-374267-4>

Eoghan Casey, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet (Academic Press 2011) <https://www.elsevier.com/books/digital-evidence-and-computer-crime/casey/978-0-08-092148-8>

Robert A. Cropf & Timothy C. Bagwell, eds., Ethical Issues and Citizen Rights in the Era of Digital Government Surveillance (2016) <https://www.igi-global.com/book/ethical-issues-citizen-rightsera/140979>

Larry E. Daniel & Lars E. Daniel, Digital Forensics for Legal Professionals: Understanding Digital Evidence from the Warrant to the Courtroom (Syngress 2015)

<https://www.elsevier.com/books/digital-forensics-for-legal-professionals/daniel/978-1-59749643-8>

Kim-Kwang Raymond Choo & Ali Dehghantanha, eds., *Contemporary Digital Forensic Investigations of Cloud and Mobile Applications* (Elsevier 2017)

<https://www.sciencedirect.com/science/book/9780128053034>

Anthony T. S. Ho & Shujun Li, eds., *Handbook of Digital Forensics of Multimedia Data and Devices* (Wiley 2015) <https://www.wiley.com/en-us/Handbook+of+Digital+Forensics+of+Multimedia+Data+and+Devices-p-9781118640500>

National Institute of Justice, *Forensic Examination of Digital Evidence: A Guide for Law Enforcement* (National Institute of Justice 2004) <https://www.ncjrs.gov/pdffiles1/nij/199408.pdf>

OSAC Task Group on Digital/Multimedia Science, *A Framework for Harmonizing Forensic Science Practices and Digital Multimedia Evidence*. (OSAC 2019)

[https://www.nist.gov/sites/default/files/documents/2018/01/10/osac\\_ts\\_0002.pdf](https://www.nist.gov/sites/default/files/documents/2018/01/10/osac_ts_0002.pdf)

George L. Paul, *Foundations of Digital Evidence* (ABA 2008)

<https://shop.americanbar.org/eBus/Store/ProductDetails.aspx?productId=215438>

John Sammons, *The Basics of Digital Forensics* (Syngress 2nd ed. 2014)

<https://www.elsevier.com/books/the-basics-of-digital-forensics/sammons/978-0-12-801635-0>

John Sammons, *Digital Forensics: Threatscape and Best Practices* (Syngress 2015)

<https://www.elsevier.com/books/digital-forensics/sammons/978-0-12-804526-8>

John Sammons & Lars Daniel, *Digital Forensics Trial Graphics: Teaching the Jury through Effective Use of Visuals* (Academic Press 2017)

<https://www.elsevier.com/books/digitalforensics-trial-graphics/sammons/978-0-12-803483-5>

## Articles

Michael Arnold, *iWITNESS: Collecting Data from Mobile Devices*, 40 LITIGATION 53 (Fall 2013)

[https://www.americanbar.org/publications/litigation\\_journal/2013-14/fall/collecting\\_data\\_mobile\\_devices.html](https://www.americanbar.org/publications/litigation_journal/2013-14/fall/collecting_data_mobile_devices.html)

Paige Bartholomew, *Seize First, Search Later: The Hunt for Digital Evidence*, 30 TOURO LAW REVIEW 1027 (2014)

<http://digitalcommons.tourolaw.edu/cgi/viewcontent.cgi?article=2570&context=lawreview>

Daniel B. Garrie & J. David Morrissy, *Digital Forensic Evidence in the Courtroom: Understanding Content and Quality*, 12 NORTHWESTERN JOURNAL OF TECHNOLOGY & INTELLECTUAL PROPERTY 121 (2014).  
<https://scholarlycommons.law.northwestern.edu/njtip/vol12/iss2/5>

Sean L. Harrington, *Collaborating with a Digital Forensics Expert: Ultimate Tag-Team or Disastrous Duo?*, 38 WILLIAM MITCHELL LAW REVIEW 353 (2011)  
<https://open.mitchellhamline.edu/wmlr/vol38/iss1/8>

Serge Jorgensen, *Convergence of Forensics, Ediscovery, Security, & Law*, 12 AVE MARIA LAW REVIEW 291 (2014) <https://avemarialaw-law-review.avemarialaw.edu/Content/articles/v12i2.Jorgensen.pdf>

J. Elizabeth McBath, *Trashing Our System of Justice? Overturning Jury Verdicts Where Evidence is Found in the Computer's Cache*, 39 AMERICAN JOURNAL OF CRIMINAL LAW 381 (2012)  
<http://ajclonline.org/the-journal>

Antonis Mouhtaropoulos, Chang-Tsun Li & Marthie Grobler, *Digital Forensic Readiness: Are We There Yet?*, 9 JOURNAL OF INTERNATIONAL COMMERCIAL LAW AND TECHNOLOGY 173 (2014)  
<http://www.jiclt.com/index.php/jiclt/article/view/213>

Sharon D. Nelson & John W. Simek, *Finding Wyatt Earp: Your Digital Forensics Expert*, 34 COMPUTER & INTERNET LAWYER 1 (March 2017)  
[https://senseient.com/wpcontent/uploads/CIL\\_0317\\_Nelson-c.pdf](https://senseient.com/wpcontent/uploads/CIL_0317_Nelson-c.pdf)

Kaitlyn R. O'Leary, *What the Founders Did Not See Coming: The Fourth Amendment, Digital Evidence, and the Plain View Doctrine*, 46 SUFFOLK UNIVERSITY LAW REVIEW 211 (2013)  
[http://suffolklawreview.org/wp-content/uploads/2013/02/OLeary\\_Note\\_PDF\\_Web.pdf](http://suffolklawreview.org/wp-content/uploads/2013/02/OLeary_Note_PDF_Web.pdf)

Jason T. Wright and Scott Wrobel, *Computer Forensics: Not Just for "Techies" Anymore*, 14 YOUNG LAWYER 3 (2010)  
[https://www.americanbar.org/content/dam/aba/publishing/young\\_lawyer/yld\\_tyl\\_july10\\_digital.authcheckdam.pdf](https://www.americanbar.org/content/dam/aba/publishing/young_lawyer/yld_tyl_july10_digital.authcheckdam.pdf)

## Webpages

NIST Digital Multimedia Evidence Scientific Committee & Subcommittees  
<https://www.nist.gov/topics/forensic-science/organization-scientific-area-committeesosac/digitalmultimedia-scientific>

Scientific Working Group on Digital Evidence <http://www.swgde.org>  
A Framework for Harmonizing Forensic Science Practices and Digital/Multimedia Evidence  
<https://www.nist.gov/news-events/news/2018/01/framework-harmonizing-forensic-sciencepractices-and-digitalmultimedia>

Validation of Forensic Tools & Software, A Quick Guide for the Digital Forensics Examiner  
<https://www.forensicmag.com/article/2011/03/validation-forensic-tools-and-software-quickguide-digital-forensic-examiner>

Asking & Answering the Right Questions About Mobile Forensics Methods  
[http://cellebriteusa.net/content/WP\\_LS.pdf](http://cellebriteusa.net/content/WP_LS.pdf)

ACPO Good Practice Guide for Digital Evidence [http://www.digital-detective.net/digital-forensics-documents/ACPO\\_Good\\_Practice\\_Guide\\_for\\_Digital\\_Evidence\\_v5.pdf](http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf)

Searching & Seizing Computers & Obtaining Electronic Evidence in Criminal Investigations  
<https://www.justice.gov/sites/default/files/criminalccips/legacy/2015/01/14/ssmanual2009.pdf>

NIST Computer Forensic Tool Testing Project <http://www.cftt.nist.gov/federated-testing.html>  
DOJ Digital Forensic Analysis Methodology Workflow  
[https://www.justice.gov/sites/default/files/criminalccips/legacy/2015/03/26/forensics\\_chart.pdf](https://www.justice.gov/sites/default/files/criminalccips/legacy/2015/03/26/forensics_chart.pdf)

ISO/IEC 27037:2012: Guidelines for Identification, Collection, Acquisition and Preservation Of Digital Evidence <https://www.iso.org/standard/44381.html>

ASTM Digital Evidence Active Standards  
<https://www.astm.org/COMMIT/SUBCOMMIT/E3012.htm>