Forensic Digital & Multimedia Sciences
Forensic Digital & Multimedia Sciences
The Proceedings of the American Academy of Forensic Sciences is an official publication of the American Academy of Forensic Sciences (AAFS) and includes various areas of the forensic sciences such as pathology, toxicology, physical anthropology, psychiatry, odontology, jurisprudence, criminalistics, questioned documents, digital sciences, engineering sciences and other disciplines. The proceedings herein are from the Digital & Multimedia Sciences section for the years 2009 to 2011.

As with the Proceedings in which these abstracts were originally published, there is no implication or assertion that the AAFS, any of its sections, or any member of the AAFS have verified the statements and/or conclusions of the abstracts. The views expressed in this publication are not those of the AAFS or individual members. In short, the data and opinions appearing in the abstracts are the responsibility of the individual authors alone.

All contents copyright 2009-2011 by the AAFS. Unless stated otherwise, noncommercial reproduction of material contained herein is permitted by the AAFS provided that the copying is faithful to the original. No other reproduction of any form may be done without prior written permission from the AAFS. Printed in the United States of America.
Preface

The American Academy of Forensic Sciences (AAFS) is a multi-disciplinary professional organization created and maintained to provide leadership in the application of science to the legal system. A premier forensic science organization, its specific objectives are to promote professionalism, integrity, competency and education, and to foster scientific research, improvements in the practice of forensic science, and collaboration within the many fields of forensic science.

For sixty-three years, since its founding in 1948, the AAFS has served a distinguished and diverse membership. It comprises eleven different sections representing the broad range of expertise and interest of its members, now numbering over 6200. Included among them are physicians, attorneys, dentists, toxicologists, physical anthropologists, document examiners, psychiatrists, physicists, engineers, criminalists, educators, and digital evidence specialists. Representing all fifty US states, all ten Canadian provinces and 61 other countries from all corners of the world, AAFS members actively practice forensic science. In many cases, AAFS members also teach and conduct research in the field, producing hundreds of refereed publications and books.
The editors express gratitude to the past and present AAFS leadership, especially to the AAFS staff headed by Executive Director Anne Warren, to the AAFS Presidents since 1949 and to our section’s directors and chair persons.

### Academy Presidents

<table>
<thead>
<tr>
<th>Name</th>
<th>Term</th>
<th>Name</th>
<th>Term</th>
<th>Name</th>
<th>Term</th>
</tr>
</thead>
<tbody>
<tr>
<td>Douglas H. Ubelaker, PhD</td>
<td>2011-12</td>
<td>June K. Jones, MS</td>
<td>1979-80</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Joseph P. Bono, MA</td>
<td>2010-11</td>
<td>Kurt M. Dubowski, PhD</td>
<td>1978-79</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thomas L. Bohan, PhD, JD</td>
<td>2009-10</td>
<td>B. Edward Whittaker, BS</td>
<td>1977-78</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Carol E. Henderson, JD</td>
<td>2008-09</td>
<td>James T. Weston, MD</td>
<td>1976-77</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bruce A. Goldberger, PhD</td>
<td>2007-08</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>James G. Young, MD</td>
<td>2006-07</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Edmund R. Donoghue, MD</td>
<td>2005-06</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ronald L. Singer, MS</td>
<td>2004-05</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kenneth E. Melson, JD</td>
<td>2003-04</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Graham R. Jones, PhD</td>
<td>2002-03</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mary Fran Ernst, BLS</td>
<td>2001-02</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>John D. McDowell, DDS, MS</td>
<td>2000-01</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Patricia J. McFeeley, MD</td>
<td>1999-00</td>
<td>Maier I. Tuchler, MD</td>
<td>1968-69</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Richard Rosner, MD</td>
<td>1996-97</td>
<td>Robert B. Forney, PhD</td>
<td>1965-66</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Haskell M. Pitluck, JD</td>
<td>1995-96</td>
<td>Dwight M. Palmer, MD</td>
<td>1964-65</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Steven C. Batterman, PhD</td>
<td>1994-95</td>
<td>Oliver C. Schroeder, Jr., JD</td>
<td>1963-64</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enrico N. Togneri, BA</td>
<td>1993-94</td>
<td>Milton Helpern, MD</td>
<td>1962-63</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Homer R. Campbell, Jr., DDS</td>
<td>1991-92</td>
<td>Russel S. Fisher, MD</td>
<td>1960-61</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ellis R. Kerley, PhD.</td>
<td>1990-91</td>
<td>Ordway Hilton, MA</td>
<td>1959-60</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Richard C. Froede, MD</td>
<td>1989-90</td>
<td>John F. Williams, BS</td>
<td>1958-59</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Richard S. Frank, BS</td>
<td>1988-89</td>
<td>Val B. Satterfield, MD</td>
<td>1957-58</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yale H. Caplan, PhD.</td>
<td>1987-88</td>
<td>Alan R. Moritz</td>
<td>1956-57</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Don Harper Mills, JD, MD</td>
<td>1986-87</td>
<td>Fred E. Inbau, BS, LLB,</td>
<td>1955-56</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maureen Casey Owens, AB</td>
<td>1984-85</td>
<td>Louis P. Regan, MD, LLB</td>
<td>1953-54</td>
<td></td>
<td></td>
</tr>
<tr>
<td>George E. Gantner, MD</td>
<td>1983-84</td>
<td>R.N. Harger, PhD</td>
<td>1952-53</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Anthony Longhetti, BA</td>
<td>1982-83</td>
<td>S.A. Levinson, MD, PhD</td>
<td>1951-52</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Joseph H. Davis, MD</td>
<td>1981-82</td>
<td>R.B.H. Gradwohl, MD</td>
<td>1949-51</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Digital and Multimedia Sciences
Board of Directors Representatives and Chairs

<table>
<thead>
<tr>
<th>Year</th>
<th>Director</th>
<th>Chair</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011-2012</td>
<td>Zeno J. Geradts, PhD</td>
<td>David W. Baker, MFS</td>
</tr>
<tr>
<td>2010-2011</td>
<td>Zeno J. Geradts, PhD</td>
<td>David W. Baker, MFS</td>
</tr>
<tr>
<td>2009-2010</td>
<td>Carrie M. Whitcomb, MSFS</td>
<td>Zeno J. Geradts, PhD</td>
</tr>
<tr>
<td>2008-2009</td>
<td>Carrie M. Whitcomb, MSFS</td>
<td>Zeno J. Geradts, PhD</td>
</tr>
</tbody>
</table>

Our heartfelt thanks to the Academy Staff for managing the proceedings process that results in the highest standards of quality including Sonya Bynoe, Publications & Website Coordinator; Debbie Crockett, Finance Manager; Sondra Doolittle, Meetings & Exposition Manager; Phyllis Gilliam, Receptionist; Salena Grant, Assistant Meetings Manager; Cheryl Hunter, Membership Coordinator; Nancy Jackson, Director of Development & Accreditation; Tracie McCray, Accounting Assistant; Christie Vigil, Membership Assistant; and Kimberly Wrasse, Executive Assistant.

This further acknowledges the excellent work of all our Digital and Multimedia Sciences authors and colleagues worldwide who are willing to share their work for education.

Carrie M. Whitcomb, MSFS
Zeno J. Geradts, PhD
David W. Baker, MFS

Prepared by:
Laura L. Liptai, PhD
Engineering Sciences

1 The Executive Committee of The American Academy of Forensic Sciences has directed Laura Liptai, Ph.D. of the Engineering Sciences Section to prepare this volume for publication.
Table of Contents

Index of Title by Year
2011 ..................................................................................................................................................................Index 1
2010 ..................................................................................................................................................................Index 3
2009 ..................................................................................................................................................................Index 5

Index by Presenting Author .....................................................................................................................Index 7

Proceedings by Year
2011 ............................................................................................................................................................................... 1
2010 ............................................................................................................................................................................ 12
2009 ............................................................................................................................................................................ 25
# Index of Title by Year

<table>
<thead>
<tr>
<th>Year</th>
<th>Title</th>
<th>Authors</th>
<th>Affiliations</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011</td>
<td>The Digital Forensics Certification Board (2009-2010): Activities and Certifications</td>
<td>Carrie M. Whitcomb, MSFS*, National Center for Forensic Science, 12354 Research Parkway, University of Central Florida, PO Box 162367, Orlando, FL 32816-2367</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Communicating Results: The Digital Forensic Report</td>
<td>Mark Pollitt, MS*, Daytona State College, 1200 West International Speedway Boulevard, Daytona Beach, FL 32114</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Development of an Offender Classification Based Investigative Protocol for Use With Online Consumers of Child Pornography Cases: An Information, Technology, and Behavioral Sciences Approach</td>
<td>Kathryn C. Seigfried-Spellar, MA, 401 North Grant Street, Knoy Hall of Technology, West Lafayette, IN 47907; and Marcus Rogers, PhD*, 401 North Grant Street, West Lafayette, IN 47907</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Exploring the Progression of Nondeviant and Deviant Pornography Use By Age of Onset and Sex</td>
<td>Marcus Rogers, PhD, 401 North Grant Street, West Lafayette, IN 47907; and Kathryn C. Seigfried-Spellar, MA*, 401 North Grant Street, Knoy Hall of Technology, West Lafayette, IN 47907</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>An Approach for the Detection of the Illicit Use of Legitimate Network Access Credentials by an Intruder</td>
<td>Christopher W. Day, BS*, 2 South Biscayne Boulevard, Suite 2800, Miami, FL 33131</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Finding Light After Dark: Low Light Photography for Forensic Investigators</td>
<td>Francesca M. Daher, BA*, Harris County Institute of Forensic Sciences, Imaging Department, 1885 Old Spanish Trail, Houston, TX 77027; Dustin C. Hatfield, BA, Harris County Medical Examiner’s Office, 1885 Old Spanish Trail, Houston, TX 77054; and Desmond R. Bostick, and Andre Santos, BA, Harris County Institute of Forensic Sciences, 1885 Old Spanish Trail, Houston, TX 77054</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Preventing a Rush to Judgment: Application of Computer Forensics in Data Breach Cases</td>
<td>Jason M. Paroff, JD*, Kroll Ontrack, 1 Harmon Meadow Boulevard, Suite 225, Secaucus, NJ 07094; Stephen D. Baird, MS, Kroll Ontrack, 1166 Avenue of the Americas, 23rd Floor, New York, NY 10036; and Alan E. Brill*, MBA, Kroll Ontrack, 1 Harmon Meadow Boulevard, Suite 225, Secaucus, NJ 07094</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Camera-to-Subject Distance and Facial Comparison Examinations</td>
<td>Richard W. Vorder Bruegge, PhD*, Federal Bureau of Investigation, OTD-DES, Building 27958A, Pod E, Quantico, VA 22135</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Imaging the Unseen with Digital UV/IR Technology: Preliminary Bruising and Tattoo Studies</td>
<td>Stephanie L. Hoffman, MSFS*, 27811 Northbrook Avenue, Canyon Country, CA 91351; and Wilson T. Sullivan, MPA, Chaminade University of Honolulu, 3140 Waialae Avenue, Honolulu, HI 96813-1578</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td></td>
<td>A Review On Automatic Footwear Retrieval Systems From Crime Scene Shoe Marks</td>
<td>Federico Cervelli, PhD*, Via Valerio 10, Trieste, 34100, ITALY; Francesca Dardi, BS, and Sergio Carrato, PhD, Univeristy of Trieste, Via Valerio 10, Trieste, 34100, ITALY</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Preliminary Assessment of Discrimination of Twins in Photographs Based on Facial Blemishes</td>
<td>Nisha Srinivas, MS*, Matthew Pruitt, BA, Gaurav Aggarwal, PhD, and Patrick J. Flynn, PhD, University of Notre Dame, Department of Computer Science and Engineering, South Bend, IN 46556;and Richard W. Vorder Bruegge, PhD, Federal Bureau of Investigations, OTD-DES, Building 27958A, Pod E, Quantico, VA 22135</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>Title</td>
<td>Authors</td>
<td>Page</td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
<td>------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The Reduction of False Negative Errors in Fuzzy Hashing</td>
<td>Matthew G. Nolan, BS*, 1702 Byrd Street, Baltimore, MD 21230; and Michael J. Salyards, PhD*, 45 High Street, Sharpsburg, GA 30277</td>
<td>7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Computer Forensic Bitmaps and Visualization for Data Identification</td>
<td>Shane A. Macaulay*, Security Objectives Corporation, 1100 Dexter Avenue North, Suite 100, Seattle, WA 33487</td>
<td>7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Facial Comparison Using 3D Techniques</td>
<td>Arnout C. Ruifrok, PhD*, Netherlands Forensic Institute, Laan van Ypenburg 6, Den Haag, 2497 GB, NETHERLANDS; Chris van Dam, MSc, and Robin T.A. van Rootzeler, MSc, University of Twente, Hallenweg 15, Enschede, 7522 NH, NETHERLANDS</td>
<td>8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Removing JPEG Artifacts in Skin Images for Forensic Analysis</td>
<td>Chaoying Tang, MEng*, Nanyang Technological University, Forensics and Security Lab, NSI-05-01A, School of Computer Engineering, 50 Nanyang Avenue, 639798, SINGAPORE; Adams W. K. Kong, PhD*, Nanyang Technological University, Blk N4, 50 Nanyang Avenue, 639798, SINGAPORE; and Noah Craft, MD, PhD, DTM&amp;H, University of California at Los Angeles School of Medicine, LA Biomedical Research Institute, at Harbor-UCLA Medical Center, 1000 West Carson Street, Torrance, CA 90502</td>
<td>8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Conversion of AVI “txts” Stream Data to Adobe® Premiere® Pro Title Files</td>
<td>Douglas S. Lacey, BS*, DL Technology LLC., 4 Averil Court, Fredericksburg, VA 22406; and Bruce E. Koenig, MFS, BEK TEK LLC., 12115 Sangsters Court, Clifton, VA 20124-1947</td>
<td>9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recovering Multimedia From File Fragments</td>
<td>Michael Piper, BA*, United States Secret Service, 950 H Street, Northwest, Suite 4200 - FSD, Washington, DC 20223</td>
<td>9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Quantifying Phase Changes in Audio Authenticity Examinations</td>
<td>David J. Snyder, BS*, William L. Hinton, BS*, Andrew Galotti, BS*, and Kenneth Marr, MS*, Federal Bureau of Investigation, Engineering Research Facility, Building 27958A, Quantico, VA 22135</td>
<td>10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Camera Identification in Large Databases of Images</td>
<td>Zeno J. Geradts, PhD*, Netherlands Forensic Institute, Ministry of Justice, Laan van Ypenburg 6, Den Haag, SH 2497 GB, NETHERLANDS; and Wiger Van Houten, MS, Netherlands Forensic Institute, Laan van Ypenburg 6, Den haag, NETHERLANDS</td>
<td>10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Macintosh® Forensics: A Crash Course</td>
<td>Gavin W. Manes, PhD*, Avansic: E-Discovery and Digital Forensics, 401 South Boston Avenue, Suite 1701, Tulsa, OK 74103</td>
<td>11</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Macintosh® PList Files: Hidden Information for Digital Forensics Investigators</td>
<td>Gavin W. Manes, PhD*, Avansic - Digital Forensics, 401 South Boston Avenue, Suite 1701, Tulsa, OK 74103</td>
<td>11</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Title</td>
<td>Authors</td>
<td>Page</td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------</td>
<td>------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Using Reports, Peer Review, and Administrative Reviews to Teach and Maintain Quality in Digital Forensics</td>
<td>Mark Pollitt, MS*, University of Central Florida, PO Box 162367, Orlando, FL 32816-2367</td>
<td>12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Quantifying Error Rates of File Type Classification Methods</td>
<td>Vassil Roussev, PhD*, University of New Orleans, Computer Science, 2000 Lakeshore Drive, 311 Mathematics Building, New Orleans, LA 70148</td>
<td>12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Psychological Assessments and Attitudes Toward Deviant Computer Behaviors</td>
<td>Marc Rogers, PhD*, 401 North Grant Street, West Lafayette, IN 47907; and Kathryn C. Seigfried-Spellar, MA*, 401 North Grant Street, Knoy Hall of Technology, West Lafayette, IN 47907</td>
<td>12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lessons Learned From Teaching a Distance- Delivered Incident Response Course</td>
<td>J. Philip Craiger, PhD, University of Central Florida, Department of Engineering Technology, University of Central Florida, Orlando, FL 32816; Paul K. Burke, BS, Northeastern University, Boston, MA 02115; and Mark Pollitt, MS*, University of Central Florida, University of Central Florida, PO Box 162367, Orlando, FL 32816-2367</td>
<td>14</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recovering Deleted Evidence From Mobile Devices</td>
<td>Eoghan Casey, MA*, 3014 Abell Avenue, Baltimore, MD 21218</td>
<td>14</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Solid State Drive Technology and Applied Digital Forensics</td>
<td>John J. O’Brien, MA*, United States Army, Cyber Counterintelligence Activity, 4553 Llewellyn Avenue, Fort Meade, MD 20755; and Sean P. O’Brien, BS*, Defense Computer Forensic Laboratory, 911 Elkridge Landing Road, Linticum, MD 21090</td>
<td>15</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mobile Device (Cell Phone/PDA/GPS) Data Extraction Tool Classification System</td>
<td>Samuel I. Brothers, BBA*, 7501 Boston Boulevard, Room 113, Springfield, VA 22153</td>
<td>15</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exploiting Metadata to Recover Multimedia From 3GP Fragment</td>
<td>Michael Piper, BA*, United States Secret Service, 950 H Street, Northwest, Suite 4200 - FSD, Washington, DC 20223</td>
<td>16</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Video File Recovery and Playback of Partly Erased Videofiles</td>
<td>Zeno J. Geradts, PhD*, and Rikkert Zoun, MS, Netherlands Forensic Institute, Ministry of Justice, Laan van Ypenburg 6, Den Haag, 2497 GB, NETHERLANDS</td>
<td>16</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Calibration and Validation of Videographic Visibility Presentations</td>
<td>Thomas Ayres, PhD*, 101 Kensington Road, Kensington, CA 94707</td>
<td>17</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Utility of Quantization Tables for Digital Image Authentication</td>
<td>Amanda E. Broyles, MAM, Federal Bureau of Investigation, Building 27958A, Quantico, VA 22135; and Richard W. Vorder Bruegge, PhD*, Federal Bureau of Investigation, OTD-FAVIAU, Building 27958A, Pod E, Quantico, VA 22135</td>
<td>17</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identification of Cameras With Photo Response Non-Uniformity (PRNU) in Large Databases</td>
<td>Zeno J. Geradts, PhD*; and Wiger Van Houten, MS, Netherlands Forensic Institute, Ministry of Justice, Laan van Ypenburg 6, Den Haag, 2497 GB, NETHERLANDS</td>
<td>18</td>
<td></td>
<td></td>
</tr>
<tr>
<td>An Alternative Method for ENF Data Analysis</td>
<td>William L. Hinton, BS*, Kenneth Marr, MS*, and David J. Snyder, BS*, Federal Bureau of Investigation, Engineering Research Facility, Building 27958A, Quantico, VA 22135</td>
<td>18</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Building a Database of Electric Network Frequency Variations for Use in Digital Media Authenticity</td>
<td>Jeffrey M. Smith, MS*, National Center for Media Forensics, 1800 Grant Street, Suite 230, Denver, CO 80210</td>
<td>19</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Index 3
<table>
<thead>
<tr>
<th>Title</th>
<th>Authors</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Digital Forensics Certification Board: Its History and Future</td>
<td>Carrie M. Whitcomb, MSFS*, National Center for Forensic Science, University of Central Florida, PO Box 162367, Orlando, FL 32816-2367; Zeno J. Geradts, PhD*, Netherlands Forensic Institute, Ministry of Justice, Laan van Ypenburg 6, Den Haag, 2497GB, NETHERLANDS; Robert T. Lee, MBA*, Mandiant, 675 North Washington Street, Suite 210, Alexandria, VA 22314; Marcus Rogers, PhD*, 401 North Grant Street, West Lafayette, IN 47907, and Eoghan Casey, MA*, 1101 East 33rd Street, Suite C301, Baltimore, MD 21218</td>
<td>20</td>
</tr>
<tr>
<td>Changes in Approach for Scalability in Digital Forensic Analysis Emphasizing Distributed, Collaborative, and Automated Techniques</td>
<td>Brian Roux, MS*, 701 Poydras Street, Suite 150P, New Orleans, LA 70065</td>
<td>20</td>
</tr>
<tr>
<td>Forensic Data Extraction in Computer Child Pornography Investigations</td>
<td>Sigurd Murphy, BA*, Defense Computer Forensic Laboratory, Linthicum, MD; Donald P. Flynn, JD, Defense Cyber Crime Center, DC3, Linthicum, MD; Thomas J. McAleer, Defense Computer Forensic Laboratory, Linthicum, MD; Andrew Medico, BS, Defense Cyber Crime Institute, Linthicum, MD; Daniel Raygoza, Defense Computer Forensic Laboratory, Linthicum, MD; and Michael J. Salyards, PhD*, U.S. Army Criminal Investigations Laboratory, 4930 North 31st Street, Forest Park, GA 30297</td>
<td>21</td>
</tr>
<tr>
<td>Challenges for Digital Forensic Acquisition on Virtualization and Cloud Computing Platforms</td>
<td>Christopher W. Day, BS*, Terremark Worldwide, Incorporated, 2 South Biscayne Boulevard, Suite 2800, Miami, FL 33131</td>
<td>21</td>
</tr>
<tr>
<td>Virtualizing the Computer Forensic Examination Platform</td>
<td>Brian D. Nunamaker, BS*, Drug Enforcement Administration, 10555 Furnace Road, Lorton, VA 2205</td>
<td>21</td>
</tr>
<tr>
<td>Tips &amp; Tricks for the Analysis and Harvesting of Data From Macintosh Computers</td>
<td>Jessica J. Reust Smith, MFS*, Stroz Friedberg, LLC, 1150 Connecticut Avenue, Northwest, Suite 200, Washington, DC 20036</td>
<td>22</td>
</tr>
<tr>
<td>A Baseline for XP Boot Changes</td>
<td>Benjamin R. Livelsberger, BA*, National Institute of Standards &amp; Technology, 100 Bureau Drive Stop 8970, Gaithersburg, MD 20899-8970</td>
<td>22</td>
</tr>
<tr>
<td>A Forensic Analysis of a Vista 64 Hard Drive</td>
<td>Marc Rogers, PhD, 401 North Grant Street, West Lafayette, IN 47907; Katie Strempek, BS*, 3708 Sweet Valley Lane, Apartment A1, Lafayette, IN 47909; and Eric Katz, BS*, 2099 Malibu Drive, West Lafayette, IN 47906</td>
<td>23</td>
</tr>
<tr>
<td>Testing Tools to Erase Hard Drives for Reuse</td>
<td>James R. Lyle, PhD*, and Craig Russell, MS, National Institute of Standards &amp; Technology, 100 Bureau Drive Stop 8970, Gaithersburg, MD</td>
<td>23</td>
</tr>
<tr>
<td>Indication of CD Burning by Detailed Examination of SMFT: A Case Review</td>
<td>Douglas Elrick, BA*, Digital Intelligence, 17165 West Glendale Drive, New Berlin, WI 53066</td>
<td>23</td>
</tr>
<tr>
<td>The Application of Known Sample Searching to Digital Forensics</td>
<td>Name and address removed at author's request.</td>
<td>24</td>
</tr>
<tr>
<td>Reliability of Computer Forensic Tools: Application of Chain of Custody Principles</td>
<td>Daniel Ayers, MSc*, and Ricard Kelly, forensic-validation.com, PO Box 97651, Manukau City, Auckland, 2241, NEW ZEALAND</td>
<td>24</td>
</tr>
<tr>
<td>Title</td>
<td>Authors</td>
<td>Pages</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>Evidence From Explosives Correlated With Digital Evidence Examinations</td>
<td>Carrie M. Whitcomb, MSFS*, National Center for Forensic Science, c/o University of Central FL, PO Box 162367, Orlando, FL 32816-2367</td>
<td>25</td>
</tr>
<tr>
<td>Standardization of Digital Forensic Research Techniques</td>
<td>Carey R. Murphey, PhD*, White Oak Labs, 5121 Valerie Street, Bellaire, TX 77401</td>
<td>25</td>
</tr>
<tr>
<td>Understanding the Costs of Conducting Computer Forensic Examinations</td>
<td>Douglas G. Elrick, BA*, Digital Intelligence, 17165 West Glendale Drive, New Berlin, WI 53151</td>
<td>25</td>
</tr>
<tr>
<td>A Case Study: Overcoming Anti-Forensic Methods Used on External Storage Drives</td>
<td>Michael Andrew*, CyberSecurity Institute, 21816 132nd Street Southeast, Monroe, WA 98272; and Steven Hailey, CyberSecurity Institute, 17716 Trombley Road, Snohomish, WA 98290</td>
<td>26</td>
</tr>
<tr>
<td>A Virtual Architecture for Digital Forensic Tool Validation</td>
<td>J. Philip Craiger, PhD*, Chris Marberry, BS, Greg Dorn, BS, and Scott Conrad, BS, National Center for Forensic Science, University of Central Florida, PO Box 162367, Orlando, FL 32816-2367</td>
<td>27</td>
</tr>
<tr>
<td>Smart Unpacking: Methods for Characterization and Extraction of Embedded Content</td>
<td>Benjamin Long, BBA*, NIST, 100 Bureau Drive, Stop 8970, Gaithersburg, MD 20899</td>
<td>27</td>
</tr>
<tr>
<td>Fixed Size and Variable Size Block Hashes for File Identification</td>
<td>Douglas R. White, MS*, 4225 Angell Road, Taneytown, MD 21787-2601</td>
<td>28</td>
</tr>
<tr>
<td>Applying Advanced Search Techniques to Digital Forensics</td>
<td>Brian D. Carrier, PhD*, Basis Technology, One Alewife Center, Cambridge, MA 02140</td>
<td>28</td>
</tr>
<tr>
<td>Computer Forensic Tool Testing Strategies</td>
<td>James R. Lyle, PhD*, National Institute of Standards and Technology, 100 Bureau Drive, Mail Stop 8970, Gaithersburg, MD 20899</td>
<td>28</td>
</tr>
<tr>
<td>An Odyssey Into Lesser Known Regions of Embedded Metadata in Microsoft File Formats</td>
<td>Eoghan Casey, MA*, ONKC LLC, 3014 Abell Avenue, Baltimore, MD 21218</td>
<td>29</td>
</tr>
<tr>
<td>Supporting Cyber Crime Investigation With the UAB Spam Data Mine</td>
<td>Chengcui Zhang, PhD*, CH 127, 1530 3rd Avenue South, Birmingham, AL 35294; Chun Wei, MS, Wei-Bang Chen, MS, Richa Tiwari, MS, and Xin Chen, PhD, CH 128, 1530 3rd Avenue South, Birmingham, AL 35294; and Gary Warner, BS, CH 100, 1530 3rd Avenue South, Birmingham, AL 35294</td>
<td>29</td>
</tr>
<tr>
<td>The Impact of Multicore CPUs and Graphics Processing Units (GPUs) on Digital Forensics Tool Design</td>
<td>Golden G. Richard III, PhD*, Department of Computer Science, University of New Orleans, New Orleans, LA 70148</td>
<td>29</td>
</tr>
<tr>
<td>Digital Media Players — Recent Research and a Cautionary Tale</td>
<td>Jessica Reust Smith, MFS*, Stroz Friedberg, LLC, 1150 Connecticut Avenue Northwest, Suite 200, Washington DC, 20036; Thomas Owley, MD, 1747 West Roosevelt Road, Chicago, IL 60608; Edward Zawadzki, DO, 144 West 12th Street, New York, NY 10021; Soyna Owley, MD, 1500 Waters Place, 10011, Bronx, NY 10461; and Stephen B. Billick, MD, 11 East 68th Street, Suite 1B, New York, NY 10065-4955</td>
<td>30</td>
</tr>
<tr>
<td>Using Computational Forensic Linguistics to Screen Pedophilic Communications</td>
<td>Carole E. Chaski, PhD*, Institute for Linguistic Evidence, 25100 Trinity Drive, Georgetown, DE 19947-6585; and Raye Croghan, BS, ALIAS Technology, LLC, 25100 Trinity Drive, Georgetown, DE 19947-6585</td>
<td>30</td>
</tr>
<tr>
<td>Forensic Analysis of Forensic Analysis of Spyware/Monitoring Software</td>
<td>Don L. Lewis*, Lakewood Police Department, 445 South Allison Parkway, Lakewood, CO 80226</td>
<td>31</td>
</tr>
<tr>
<td>Title</td>
<td>Authors</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Application of Natural Language Processing to the Digital Forensic Process</td>
<td>Mark Pollitt, MS*, University of Central Florida, PO Box 162367, Orlando, FL 32816-2367; and Anne Diekema, PhD, Center for Natural Language Processing, Syracuse University, 335 Hinds Hall, Syracuse, NY 13244</td>
<td>31</td>
</tr>
<tr>
<td>Testing of Image Quality of In-Car Video Systems</td>
<td>Herbert L. Blitz, MBA*, and Jerry Jeffers, MS, Institute for Forensic Imaging, 338 South Arlington Avenue, Suite 111, Indianapolis, IN 46219</td>
<td>31</td>
</tr>
<tr>
<td>Examining Photo Response Non-Uniformity for the Comparison of Cameras</td>
<td>Zeno J. Geradts, PhD*, Maarten van der Mark, BS, and Wiger Van Houten, MS, Netherlands Forensic Institute, Ministry of Justice, Laan van Ypenburg 6, Den Haag, 2497 GB, NETHERLANDS</td>
<td>33</td>
</tr>
<tr>
<td>Determination of Time of Recording With Electric Network Frequency (ENF)</td>
<td>Maarten Huijbrechtse, BS, and Zeno J. Geradts, PhD*, Netherlands Forensic Institute, Ministry of Justice, Laan van Ypenburg 6, Den Haag, 2497 GB, NETHERLANDS</td>
<td>33</td>
</tr>
<tr>
<td>Car Speed From CCTV Images</td>
<td>Bart Hoogeboom, MS*, and Ivo Alberink, PhD, Netherlands Forensic Institute, Laan van Ypenburg 6, Den Haag, 2497 GB, NETHERLANDS</td>
<td>34</td>
</tr>
<tr>
<td>3-Dimensional Analysis of Video Footage</td>
<td>Gerda Edelman, and Jurrien Bijhold, PhD*, Netherlands Forensic Institute, Laan van Ypenburg 6, 2497 GB, Den Haag, 2497GB, NETHERLANDS</td>
<td>34</td>
</tr>
<tr>
<td>Quantifying Measurement Variation and Evidential Value When Performing Body Height Estimations in Digital Images</td>
<td>Ivo Alberink, PhD*, Bart Hoogeboom, MS, and Annabel Bolck, PhD, Netherlands Forensic Institute, Laan van Ypenburg 6, Den Haag, 2497 GB, NETHERLANDS</td>
<td>34</td>
</tr>
<tr>
<td>A Morphological Classification of Eyebrows to Aid in Forensic Facial Comparisons</td>
<td>Matthew E. Graves, MFS*, Carl R. Kriigel, BS, and Cristy B. Pruitt, MFS, U.S. Army Criminal Investigation Laboratory, 4930 North 31st Street, Forest Park, GA 30297</td>
<td>36</td>
</tr>
<tr>
<td>The Persistence of Image Files on Digital Camera Memory Cards</td>
<td>Brian J. Gestring, MS*, Cedar Crest College, 100 College Drive, Forensic Science Program, Allentown, PA 18104</td>
<td>37</td>
</tr>
<tr>
<td>The Virtual Digital Forensics Laboratory</td>
<td>Mark R. McCoy, EdD*, University of Central Oklahoma, Forensic Science Institute, 100 North University, Edmond, OK 73034</td>
<td>37</td>
</tr>
<tr>
<td>Author by Last Name</td>
<td>Title</td>
<td>Page</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Alberink, Ivo PhD*, Bart Hoogeboom, MS, and Annabel Bolck, PhD, Netherlands Forensic Institute, Laan van Ypenburg 6, Den Haag, 2497 GB, NETHERLANDS</td>
<td>Quantifying Measurement Variation and Evidential Value When Performing Body Height Estimations in Digital Images</td>
<td>34</td>
</tr>
<tr>
<td>Andrew*, Michael CyberSecurity Institute, 21816 132nd Street Southeast, Monroe, WA 98272; and Steven Hailey, CyberSecurity Institute, 17716 Trombley Road, Snohomish, WA 98290</td>
<td>A Case Study: Overcoming Anti-Forensic Methods Used on External Storage Drives</td>
<td>26</td>
</tr>
<tr>
<td>Ayers, Daniel MSc*, and Ricard Kelly, forensic-validation.com, PO Box 97651, Manukau City, Auckland, 2241, NEW ZEALAND</td>
<td>Reliability of Computer Forensic Tools: Application of Chain of Custody Principles</td>
<td>24</td>
</tr>
<tr>
<td>Ayres, Thomas PhD*, 101 Kensington Road, Kensington, CA 94707</td>
<td>Calibration and Validation of Videographic Visibility Presentations</td>
<td>17</td>
</tr>
<tr>
<td>Blitzer, Herbert L. MBA*, and Jerry Jeffers, MS, Institute for Forensic Imaging, 338 South Arlington Avenue, Suite 111, Indianapolis, IN 46219</td>
<td>Testing of Image Quality of In-Car Video Systems</td>
<td>31</td>
</tr>
<tr>
<td>Brothers, Samuel I. BBA*, 7501 Boston Boulevard, Room 113, Springfield, VA 22153</td>
<td>Mobile Device (Cell Phone/PDA/GPS) Data Extraction Tool Classification System</td>
<td>15</td>
</tr>
<tr>
<td>Broyles, Amanda E. MAM, Federal Bureau of Investigation, Building 27958A, Quantico, VA 22133; and Richard W. Vorder Bruegge, PhD*, Federal Bureau of Investigation, OTD-FAVIAU, Building 27958A, Pod E, Quantico, VA 22133</td>
<td>Utility of Quantization Tables for Digital Image Authentication</td>
<td>17</td>
</tr>
<tr>
<td>Carrier, Brian D. PhD*, Basis Technology, One Alewife Center, Cambridge, MA 02140</td>
<td>Applying Advanced Search Techniques to Digital Forensics</td>
<td>28</td>
</tr>
<tr>
<td>Casey, Eoghan MA*, 3014 Abell Avenue, Baltimore, MD 21218</td>
<td>Recovering Deleted Evidence From Mobile Devices</td>
<td>14</td>
</tr>
<tr>
<td>Casey, Eoghan MA*, ONKC LLC, 3014 Abell Avenue, Baltimore, MD 21218</td>
<td>An Odyssey Into Lesser Known Regions of Embedded Metadata in Microsoft File Formats</td>
<td>29</td>
</tr>
<tr>
<td>Cervelli, Federico PhD*, Via Valerio 10, Trieste, 34100, ITALY; Francesca Dardi, BS, and Sergio Carrato, PhD, University of Trieste, Via Valerio 10, Trieste, 34100, ITALY</td>
<td>A Review On Automatic Footwear Retrieval Systems From Crime Scene Shoe Marks</td>
<td>5</td>
</tr>
<tr>
<td>Authors</td>
<td>Title</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Chaski, Carole E. PhD*, Institute for Linguistic Evidence, 25100 Trinity Drive, Georgetown, DE 19947-6585; and Raye Croghan, BS, ALIAS Technology, LLC, 25100 Trinity Drive, Georgetown, DE 19947-6585</td>
<td>Using Computational Forensic Linguistics to Screen Pedophilic Communications</td>
<td>30</td>
</tr>
<tr>
<td>Craiger, J. Philip PhD*, Chris Marberry, BS, Greg Dorn, BS, and Scott Conrad, BS, National Center for Forensic Science, University of Central Florida, PO Box 162367, Orlando, FL 32816-2367</td>
<td>A Virtual Architecture for Digital Forensic Tool Validation</td>
<td>27</td>
</tr>
<tr>
<td>Craiger, J. Philip PhD, University of Central Florida, Department of Engineering Technology, University of Central Florida, Orlando, FL 32816; Paul K. Burke, BS, Northeastern University, Boston, MA 02115; and Mark Pollitt, MS*, University of Central Florida, University of Central Florida, PO Box 162367, Orlando, FL 32816-2367</td>
<td>Lessons Learned From Teaching a Distance-Delivered Incident Response Course</td>
<td>14</td>
</tr>
<tr>
<td>Daher, Francesca M. BA*, Harris County Institute of Forensic Sciences, Imaging Department, 1885 Old Spanish Trail, Houston, TX 77027; Dustin C. Hatfield, BA, Harris County Medical Examiner’s Office, 1885 Old Spanish Trail, Houston, TX 77054; and Desmond R. Bostick, and Andre Santos, BA, Harris County Institute of Forensic Sciences, 1885 Old Spanish Trail, Houston, TX 77054</td>
<td>Finding Light After Dark: Low Light Photography for Forensic Investigators</td>
<td>3</td>
</tr>
<tr>
<td>Day, Christopher W. BS*, 2 South Biscayne Boulevard, Suite 2800, Miami, FL 33131</td>
<td>An Approach for the Detection of the Illicit Use of Legitimate Network Access Credentials by an Intruder</td>
<td>3</td>
</tr>
<tr>
<td>Day, Christopher W. BS*, Terremark Worldwide, Incorporated, 2 South Biscayne Boulevard, Suite 2800, Miami, FL 33131</td>
<td>Challenges for Digital Forensic Acquisition on Virtualization and Cloud Computing Platforms</td>
<td>21</td>
</tr>
<tr>
<td>Edelman, Gerda and Jurrien Bijhold, PhD*, Netherlands Forensic Institute, Laan van Ypenburg 6, 2497 GB, Den Haag, 2497GB, NETHERLANDS</td>
<td>3-Dimensional Analysis of Video Footage</td>
<td>34</td>
</tr>
<tr>
<td>Elrick, Douglas BA*, Digital Intelligence, 17165 West Glendale Drive, New Berlin, WI 53066</td>
<td>Indication of CD Burning by Detailed Examination of $MFT: A Case Review</td>
<td>23</td>
</tr>
<tr>
<td>Elrick, Douglas G. BA*, Digital Intelligence, 17165 West Glendale Drive, New Berlin, WI 53151</td>
<td>Understanding the Costs of Conducting Computer Forensic Examinations</td>
<td>25</td>
</tr>
<tr>
<td>Gerardts, Zeno J. PhD*, and Rikkert Zoun, MS, Netherlands Forensic Institute, Ministry of Justice, Laan van Ypenburg 6, Den Haag, 2497 GB, NETHERLANDS</td>
<td>Video File Recovery and Playback of Partly Erased Videofiles</td>
<td>16</td>
</tr>
<tr>
<td>Title</td>
<td>Page</td>
<td></td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------</td>
<td></td>
</tr>
<tr>
<td>Examining Photo Response Non-Uniformity for the Comparison of Cameras</td>
<td>33</td>
<td></td>
</tr>
<tr>
<td>Camera Identification in Large Databases of Images</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>Identification of Cameras With Photo Response Non-Uniformity (PRNU) in Large Databases</td>
<td>18</td>
<td></td>
</tr>
<tr>
<td>The Persistence of Image Files on Digital Camera Memory Cards</td>
<td>37</td>
<td></td>
</tr>
<tr>
<td>A Morphological Classification of Eyebrows to Aid in Forensic Facial Comparisons</td>
<td>36</td>
<td></td>
</tr>
<tr>
<td>An Alternative Method for ENF Data Analysis</td>
<td>18</td>
<td></td>
</tr>
<tr>
<td>Imaging the Unseen with Digital UV/IR Technology: Preliminary Bruising and Tattoo Studies</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>Car Speed From CCTV Images</td>
<td>34</td>
<td></td>
</tr>
<tr>
<td>Determination of Time of Recording With Electric Network Frequency (ENF)</td>
<td>33</td>
<td></td>
</tr>
<tr>
<td>Conversion of AVI “txts” Stream Data to Adobe® Premiere® Pro Title Files</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>Forensic Analysis of Forensic Analysis of Spyware/Monitoring Software</td>
<td>31</td>
<td></td>
</tr>
<tr>
<td>Name and address removed at author's request.</td>
<td>The Application of Known Sample Searching to Digital Forensics</td>
<td>24</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------------------------------------------------------</td>
<td>-----</td>
</tr>
<tr>
<td>Murphy, Sigurd BA*, Defense Computer Forensic Laboratory, Linthicum, MD; Donald P. Flynn, JD, Defense Cyber Crime Center, DC3, Linthicum, MD; Thomas J. McAlveer, Defense Computer Forensic Laboratory, Linthicum, MD; Andrew Medico, BS, Defense Cyber Crime Institute, Linthicum, MD; Daniel Raygoza, Defense Computer Forensic Laboratory, Linthicum, MD ; and Michael J. Salyards, PhD*, U.S. Army Criminal Investigations Laboratory, 4930 North 31st Street, Forest Park, GA 30297</td>
<td>Forensic Data Extraction in Computer Child Pornography Investigations</td>
<td>21</td>
</tr>
<tr>
<td>McCoy, Mark R. EdD*, University of Central Oklahoma, Forensic Science Institute, 100 North University, Edmond, OK 73034</td>
<td>The Virtual Digital Forensics Laboratory</td>
<td>37</td>
</tr>
<tr>
<td>Manes, Gavin W. PhD*, Avansic: Digital Forensics, 401 South Boston Avenue, Suite 1701, Tulsa, OK 74103</td>
<td>Macintosh® Forensics: A Crash Course</td>
<td>11</td>
</tr>
<tr>
<td>Manes, Gavin W. PhD*, and Craig Russell, MS, National Institute of Standards &amp; Technology, 100 Bureau Drive Stop 8970, Gaithersburg, MD</td>
<td>Testing Tools to Erase Hard Drives for Reuse</td>
<td>23</td>
</tr>
<tr>
<td>Lyle, James R. PhD*, National Institute of Standards and Technology, 100 Bureau Drive, Mail Stop 8970, Gaithersburg, MD 20899</td>
<td>Computer Forensic Tool Testing Strategies</td>
<td>28</td>
</tr>
<tr>
<td>Macaulay*, Shane A. Security Objectives Corporation, 1100 Dexter Avenue North, Suite 100, Seattle, WA 33487</td>
<td>Computer Forensic Bitmaps and Visualization for Data Identification</td>
<td>7</td>
</tr>
<tr>
<td>Macintosh® PList Files: Hidden Information for Digital Forensics Investigators</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Author(s)</td>
<td>Title</td>
<td>Page</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Nolan, Matthew G. BS*, 1702 Byrd Street, Baltimore, MD 21230; and</td>
<td>The Reduction of False Negative Errors in Fuzzy Hashing</td>
<td>7</td>
</tr>
<tr>
<td>Michael J. Salyards, PhD*, 45 High Street, Sharpsburg, GA 30277</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nunamaker, Brian D. BS*, Drug Enforcement Administration, 10555</td>
<td>Virtualizing the Computer Forensic Examination Platform</td>
<td>21</td>
</tr>
<tr>
<td>Furnace Road, Lorton, VA 22405</td>
<td></td>
<td></td>
</tr>
<tr>
<td>O’Brien, John J. MA*, United States Army, Cyber Counterintelligence</td>
<td>Solid State Drive Technology and Applied Digital Forensics</td>
<td>15</td>
</tr>
<tr>
<td>Activity, 4553 Llewelyn Avenue, Fort Meade, MD 20755; and Sean P.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>O’Brien, BS*, Defense Computer Forensic Laboratory, 911 Elkhart Landing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Road, Linthicum, MD 21090</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Paroff, Jason M. JD*, Kroll Ontrack, 1 Harmon Meadow Boulevard, Suite</td>
<td>Preventing a Rush to Judgment: Application of Computer Forensics in</td>
<td>3</td>
</tr>
<tr>
<td>225, Secaucus, NJ 07094; Stephen D. Baird, MS, Kroll Ontrack, 1166</td>
<td>Data Breach Cases</td>
<td></td>
</tr>
<tr>
<td>Avenue of the Americas, 23rd Floor, New York, NY 10036; and Alan E.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Brill*, MBA, Kroll Ontrack, 1 Harmon Meadow Boulevard, Suite 225,</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Secaucus, NJ 07094</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Piper, Michael BA*, United States Secret Service, 950 H Street,</td>
<td>Recovering Multimedia From File Fragments</td>
<td>9</td>
</tr>
<tr>
<td>Northwest, Suite 4200 - FSD, Washington, DC 20223</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Piper, Michael BA*, United States Secret Service, 950 H Street,</td>
<td>Exploiting Metadata to Recover Multimedia From 3GP Fragment</td>
<td>16</td>
</tr>
<tr>
<td>Northwest, Suite 4200 - FSD, Washington, DC 20223</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pollitt, Mark MS*, Daytona State College, 1200 West International</td>
<td>Communicating Results: The Digital Forensic Report</td>
<td>1</td>
</tr>
<tr>
<td>Speedway Boulevard, Daytona Beach, FL 32114</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pollitt, Mark MS*, University of Central Florida, PO Box 162367,</td>
<td>Using Reports, Peer Review, and Administrative Reviews to Teach and</td>
<td>12</td>
</tr>
<tr>
<td>Orlando, FL 32816-2367</td>
<td>Maintain Quality in Digital Forensics</td>
<td></td>
</tr>
<tr>
<td>Pollitt, Mark MS*, University of Central Florida, PO Box 162367,</td>
<td>Application of Natural Language Processing to the Digital Forensic</td>
<td>31</td>
</tr>
<tr>
<td>Orlando, FL 32816-2367; and Anne Diekema, PhD, Center for Natural</td>
<td>Process</td>
<td></td>
</tr>
<tr>
<td>Language Processing, Syracuse University, 335 Hinds Hall, Syracuse,</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NY 13244</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reust Smith, Jessica J. MFS*, Stroz Friedberg, LLC, 1150 Connecticut</td>
<td>Tips &amp; Tricks for the Analysis and Harvesting of Data From</td>
<td>22</td>
</tr>
<tr>
<td>Avenue, Northwest, Suite 200, Washington, DC 20036</td>
<td>Macintosh Computers</td>
<td></td>
</tr>
<tr>
<td>Authors</td>
<td>Title</td>
<td>Page</td>
</tr>
<tr>
<td>---------</td>
<td>-------</td>
<td>------</td>
</tr>
<tr>
<td>Reust Smith, Jessica MFS*, Stroz Friedberg, LLC, 1150 Connecticut Avenue Northwest, Suite 200, Washington DC, 20036; Thomas Owley, MD, 1747 West Roosevelt Road, Chicago, IL 60608; Edward Zawadzki, DO, 144 West 12th Street, New York, NY 10021; Soyna Owley, MD, 1500 Waters Place, 10011, Bronx, NY 10461; and Stephen B. Billick, MD, 11 East 68th Street, Suite 1B, New York, NY 10065-4955</td>
<td>Digital Media Players — Recent Research and a Cautionary Tale</td>
<td>30</td>
</tr>
<tr>
<td>Richard III, Golden G. PhD*, Department of Computer Science, University of New Orleans, New Orleans, LA 70148</td>
<td>The Impact of Multicore CPUs and Graphics Processing Units (GPUs) on Digital Forensics Tool Design</td>
<td>29</td>
</tr>
<tr>
<td>Rogers, Marc PhD*, 401 North Grant Street, West Lafayette, IN 47907; and Kathryn C. Seigfried-Spellar, MA*, 401 North Grant Street, Knoy Hall of Technology, West Lafayette, IN 47907</td>
<td>Psychological Assessments and Attitudes Toward Deviant Computer Behaviors</td>
<td>12</td>
</tr>
<tr>
<td>Rogers, Marc PhD, 401 North Grant Street, West Lafayette, IN 47907; Katie Strzempka, BS*, 3708 Sweet Valley Lane, Apartment A1, Lafayette, IN 47909; and Eric Katz, BS*, 2099 Malibu Drive, West Lafayette, IN 47906</td>
<td>A Forensic Analysis of a Vista 64 Hard Drive</td>
<td>23</td>
</tr>
<tr>
<td>Rogers, Marcus PhD, 401 North Grant Street, West Lafayette, IN 47907; and Kathryn C. Seigfried-Spellar, MA*, 401 North Grant Street, Knoy Hall of Technology, West Lafayette, IN 47907</td>
<td>Exploring the Progression of Nondeviant and Deviant Pornography Use By Age of Onset and Sex</td>
<td>2</td>
</tr>
<tr>
<td>Roussev, Vassil PhD*, University of New Orleans, Computer Science, 2000 Lakeshore Drive, 311 Mathematics Building, New Orleans, LA 70148</td>
<td>Quantifying Error Rates of File Type Classification Methods</td>
<td>12</td>
</tr>
<tr>
<td>Roux, Brian MS*, 701 Poydras Street, Suite 150P, New Orleans, LA 70065</td>
<td>Changes in Approach for Scalability in Digital Forensic Analysis Emphasizing Distributed, Collaborative, and Automated Techniques</td>
<td>20</td>
</tr>
<tr>
<td>Ruifrok, Arnout C. PhD*, Netherlands Forensic Institute, Laan van Ypenburg 6, Den Haag, 2497 GB, NETHERLANDS; Chris van Dam, MSc, and Robin T.A. van Rootselaer, MSc, University of Twente, Hallenweg 15, Enschede, 7522 NH, NETHERLANDS</td>
<td>Facial Comparison Using 3D Techniques</td>
<td>8</td>
</tr>
<tr>
<td>Seigfried-Spellar, Kathryn C. MA, 401 North Grant Street, Knoy Hall of Technology, West Lafayette, IN 47907; and Marcus Rogers, PhD*, 401 North Grant Street, West Lafayette, IN 47907</td>
<td>Development of an Offender Classification Based Investigative Protocol for Use With Online Consumers of Child Pornography Cases: An Information, Technology, and Behavioral Sciences Approach</td>
<td>1</td>
</tr>
</tbody>
</table>

Index 12
<table>
<thead>
<tr>
<th>Name</th>
<th>Affiliation</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smith, Jeffrey M. MSc*</td>
<td>National Center for Media Forensics, 1800 Grant Street, Suite 230, Denver, CO 80210</td>
<td>Building a Database of Electric Network Frequency Variations for Use in Digital Media Authenticity</td>
<td>19</td>
</tr>
<tr>
<td>Snyder, David J. BS*</td>
<td>William L. Hinton, BS*, Andrew Galotti, BS*, and Kenneth Marr, MS*</td>
<td>Quantifying Phase Changes in Audio Authenticity Examinations</td>
<td>10</td>
</tr>
<tr>
<td>Srinivas, Nisha MS*</td>
<td>Matthew Pruitt, BA, Gaurav Aggarwal, PhD, and Patrick J. Flynn, PhD, University of Notre Dame, Department of Computer Science and Engineering, South Bend, IN 46556; and Richard W. Vorder Bruegge, PhD, Federal Bureau of Investigations, OTD-DES, Building 27958A, Pod E, Quantico, VA 22135</td>
<td>Preliminary Assessment of Discrimination of Twins in Photographs Based on Facial Blemishes</td>
<td>6</td>
</tr>
<tr>
<td>Tang, Chaoying MEng*</td>
<td>Nanyang Technological University, Forensics and Security Lab, NS1-03-01A, School of Computer Engineering, 50 Nanyang Avenue, 639798, SINGAPORE; Adams W. K. Kong, PhD*, Nanyang Technological University, Blk N4, 50 Nanyang Avenue, 639798, SINGAPORE; and Noah Craft, MD, PhD, DTM&amp;H, University of California at Los Angeles School of Medicine, LA Biomedical Research Institute, at Harbor-UCLA Medical Center, 1000 West Carson Street, Torrance, CA 90502</td>
<td>Removing JPEG Artifacts in Skin Images for Forensic Analysis</td>
<td>8</td>
</tr>
<tr>
<td>Vorder Bruegge, Richard W. PhD*</td>
<td>Federal Bureau of Investigation, OTD-DES, Building 27958A, Pod E, Quantico, VA 22135</td>
<td>Camera-to-Subject Distance and Facial Comparison Examinations</td>
<td>4</td>
</tr>
<tr>
<td>Whitcomb, Carrie M. MSFS*</td>
<td>National Center for Forensic Science, 12354 Research Parkway, University of Central Florida, PO Box 162367, Orlando, FL 32816-2367</td>
<td>The Digital Forensics Certification Board (2009-2010): Activities and Certifications</td>
<td>1</td>
</tr>
<tr>
<td>Whitcomb, Carrie M. MSFS*</td>
<td>National Center for Forensic Science, c/o University of Central FL, PO Box 162367, Orlando, FL 32816-2367</td>
<td>Evidence From Explosives Correlated With Digital Evidence Examinations</td>
<td>25</td>
</tr>
<tr>
<td>Author(s)</td>
<td>Title</td>
<td>Page</td>
<td></td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
<td>------</td>
<td></td>
</tr>
<tr>
<td>Whitcomb, Carrie M. MSFS*, National Center for Forensic Science, University of Central Florida, PO Box 162367, Orlando, FL 32816-2367; Zeno J. Geradts, PhD*, Netherlands Forensic Institute, Ministry of Justice, Laan van Ypenburg 6, Den Haag, 2497GB, NETHERLANDS; Robert T. Lee, MBA*, Mandiant, 675 North Washington Street, Suite 210, Alexandria, VA 22314; Marcus Rogers, PhD*, 401 North Grant Street, West Lafayette, IN 47907, and Eoghan Casey, MA*, 1101 East 33rd Street, Suite C301, Baltimore, MD 21218</td>
<td>The Digital Forensics Certification Board: Its History and Future</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>White, Douglas R. MS*, 4225 Angell Road, Taneytown, MD 21787-2601</td>
<td>Fixed Size and Variable Size Block Hashes for File Identification</td>
<td>28</td>
<td></td>
</tr>
<tr>
<td>Zhang, Chengcui PhD*, CH 127, 1530 3rd Avenue South, Birmingham, AL 35294; Chun Wei, MS, Wei-Bang Chen, MS, Richa Tiwari, MS, and Xin Chen, PhD, CH 128, 1530 3rd Avenue South, Birmingham, AL 35294; and Gary Warner, BS, CH 100, 1530 3rd Avenue South, Birmingham, AL 35294</td>
<td>Supporting Cyber Crime Investigation With the UAB Spam Data Mine</td>
<td>29</td>
<td></td>
</tr>
</tbody>
</table>
After attending this presentation, attendees will be persuaded to review the process and will be ready to go for the Phase II with the automated system.

This presentation will impact the forensic science community by promoting trust and confidence in the digital forensics profession by providing an objective and validated certification process which will help the maturation of digital forensics as a science.

The Digital Forensics Certification Board (DFCB) will have a great impact due to its launching at the right time, being weeks after the initial National Academy of Sciences report in 2009. Certification for digital practitioners is imperative. The DFCB is a professional certification requiring a clean background review.

The Digital Forensic Certification Board was created to develop a professional certification process for digital evidence. After numerous meetings with digital evidence practitioners and various agencies, digital certification has finally come to pass. The process was begun at www.dfcb.org with the first application taken on February 9, 2009 and ended in September 16, 2009. Sam Guttman, retired as the Assistant Inspector General for Investigations for Postal OIG, volunteered to be President of the DFCB.

DFCB developed a “Founders” process for those who have had over five years of experience in the field of digital forensics. Accreditation of our certification process was planned via the Forensic Specialty Accreditation Board (FSAB). The founders were given a registration that could substantiate their experience, education, training, publications, positions held, testimonies given, their background and other relevant activities. Each founder must have scored 100 points on the application form to qualify. They wrote 15 questions in the domains of their expertise each with four incorrect answers and one correct answer. These questions became part of the collection of questions that have been sorted and verified. There were 600 viable questions that resulted from the founders group that will be validated when the next round of applicants begin the electronic version of the application process. There were 130 founders that successfully completed the certification process.

The DFCB started Certification Phase II from June 14th thru July 31st, 2010 and developed an automated application online. The application for Phase II had the following criteria:

- Score a minimum number of points on the Assessment Scoring Sheet and provide supporting documentation
- Meet and continue to comply with the DFCB Code of Ethics and Standards
- Pass a background review
- Develop 15 usable test questions with multiple choice answers. Applicants shall author questions and answers following the instructions posted on the DFCB website
- Take a non-score test sampling from questions developed by the founders. Instructions for developing multiple choice questions are available on the website.

The next phase will focus on the development, validation, and delivery of DFCB Certification tests.

This project was supported by NIJ Grant.

Carrie M. Whitcomb, MSFS*, National Center for Forensic Science, 12354 Research Parkway, University of Central Florida, PO Box 162367, Orlando, FL 32816-2367
for deriving pertinent data that can be used as evidence to either prosecute or exonerate those people charged with this type of criminal offense. Anecdotal and research based evidence indicates that law enforcement spends an increasing amount of their limited resources (both time and personnel) dealing with cases involving online child pornography. It has also been speculated that technology innovations such as the Internet, webcams, and social networks have greatly assisted child pornographers with their criminal craft.

Whether the rate of child pornography is increasing or not has been the topic of very heated debate. What is not debatable is the technical difficulty that arises when investigating this type of criminal activity. This difficulty has been correlated with the increased size of available storage devices and the falling cost to consumers. The days of simply looking at every sector on a storage device for possible evidence is no longer practical and in some cases not technically feasible within a reasonable time frame. What is required are more tactical and focused approaches to investigating large amounts of data. These approaches or process models need to be informed by research that studies the personality and motivational characteristics of the offenders in question.

The presentation will introduce an offender characteristics based investigative protocol that assists investigators looking for digital evidence. The protocol combines advances in the behavioral analysis of online consumers of child pornography with common locations of digital evidence found on computing system. Previous behavioral characteristics based models, such as Lanning (2001) and Krone (2004) were modified to take into account the security precautions commonly implemented by these offenders. The Rogers-Seigfried model identifies common types and locations of digital evidence available to investigators based on the classification of the offender. The process model advocates treating the computing system as a digital crime scene analogous to the physical crime scene where context and evidence proximity (both physical/virtual and temporal) are important considerations.

The model also leverages the constraints and default behaviors built into the various operating systems, file systems and applications based on usability and human computer interaction standards. These constraints limit the potential virtual space that must be examined by investigators looking to identify and understand the context of any digital evidence.

The proposed model has been used successfully in several investigations involving online child pornography. The presentation will present a brief case study to illustrate the concepts introduced. Limitations of the model and suggestions for future research will also be discussed.

Evidence, Pedophilia, Investigations

B4 Exploring the Progression of Nondeviant and Deviant Pornography Use By Age of Onset and Sex

Marcus Rogers, PhD, 401 North Grant Street, West Lafayette, IN 47907; and Kathryn C. Seigfried-Spellar, MA*, 401 North Grant Street, Knoy Hall of Technology, West Lafayette, IN 47907

After attending this presentation, attendees will be presented with the results of an empirical study assessing the difference in age of onset for engaging in various forms of nondeviant and deviant pornography and the progression of pornography use between men and women. In addition, attendees will learn whether there is a progression of increased risk for engaging in nondeviant to deviant forms of pornography based on age of onset.

This presentation will impact the forensic science community by adding to the body of knowledge examining the age of onset for consuming various forms of nondeviant and deviant pornography.

Although seemingly counterintuitive, research indicates the collections of child pornography users not only contain sexualized images of children, but other genres of pornography both deviant and socially acceptable in nature (c.f., Quayle & Taylor, 2002; Quayle & Taylor, 2003).1,2 In fact, interviews with child pornography users have suggested that some offenders move “through a variety of pornographies, each time accessing more extreme material” (Quayle & Taylor, 2002, p. 343)3 as a result of desensitization or appetite satiation, which lead to collecting and discovering other forms of deviant pornography (Quayle & Taylor, 2003).2 Also, some consumers stated they downloaded the images simply because they were available and accessible, making the behaviors primarily a result of compulsion rather than a specific sexual interest in children (Basbaum, 2010).1

Some child pornography consumers exhibit a complex array of sexual interests, which may be representative of a more general level of paraphilic tendencies rather than a specific sexual interest in children. In a study conducted by Endrass et al. (2009),4 the collection of images from 231 men charged with child pornography use also revealed other types of deviant pornography. Specifically, nearly 60% of the sample collected child pornography and at least one other type of deviant pornography, such as bestiality, excrement, or sadism, with at least one out of three offenders collecting three or more types of deviant pornography (Endrass et al., 2009).4 This research suggests the majority of Internet child pornography users are collecting a wider range of deviant pornography, which may reflect a general level of sexual deviance rather than a specific paraphilia, such as pedophilia. In other words, some child pornography consumers may be dissidents within the normal population who exhibit a wider range of sexual interests.

Although case studies exist, few empirical research studies have assessed the question of whether individuals who use nondeviant forms of pornography (e.g., adult pornography) are at a greater risk for consuming deviant forms of pornography (e.g., animal and child pornography). The current study adds to this body of knowledge by examining the age of onset for consuming various forms of nondeviant and deviant pornography. Specifically, the present project will explore at what age individuals first knowingly searched for, downloaded, and exchanged/shared the following pornography genres: adult-only, animal (bestiality), and child pornography. By examining the interrelations among the self-reported age and pornography use variables, the goal is to provide a better understanding of how nondeviant pornography use either facilitates or accelerates the probability of engaging in more deviant forms of pornography.

The first goal of this study is to determine whether or not the age of onset is a risk factor for engaging in deviant pornography. In other words, are individuals who engage in nondeviant pornography use at an earlier age more likely to engage in deviant forms of pornography use compared to late onset users? The second goal of this study is to determine whether or not the age of onset for nondeviant and deviant pornography differs by sex (male, female). Finally, the third goal of this study will explore the frequency of pornography use by collapsing the respondents into pornography categories: none, adult-only, animal-only, child-only, adult-animal, adult-child, animal-child, and adult-child-animal. This will assess whether self-reported child pornography users are more likely to self-report adult and animal pornography behaviors compared to the other categories of users.

Results and future implications of the study’s findings will be discussed.

References:

After attending this presentation, attendees will understand a typical Persistent External Targeted Threat (PETT) attack and one of the most common follow-on modes of persistence utilizing stolen, but valid, network access credentials. Previously, PETTs were most commonly observed in government agencies but are now becoming more prevalent in the private sector as demonstrated by the so-called “Aurora” attacks against Google in January of 2010. A common result of a PETT attack is the compromise of valid user and system administrator credentials that are then subsequently used by the adversary to continue to access the victim network via VPN, RDP, Enterprise Portals, or other remote access platforms. Due to the fact that the credentials used by the intruder are valid access credentials, the intruder is simply “logging in” and no longer required to utilize an exploit or some other form of “hacking” to continue to intrude into the network. This form of intrusion is difficult to differentiate from legitimate user access and hence challenging to detect.

This presentation will impact the forensic science community by providing practitioners with awareness of this form of illicit activity as well as network and system observables to detect it in networks of interest. Given that one of the primary results of a PETT attack is sensitive data exfiltration, it is important for investigators to know how to identify the patterns and observables that the malicious misuse of valid network access credentials leave behind in the forensic record. Finally, a new, free, extensible, open-source tool will be introduced to help investigators process many common log file types to highlight the observable patterns of the above-mentioned malicious misuse of valid network credentials.

After attending this presentation, attendees will learn techniques used by night shift scene investigators in a medical examiner setting to photographically document decedents and places of death in low light situations.

This presentation will impact the forensic science community by providing information on photography training initiatives used in a medical examiner setting for advanced photography techniques to enhance scene investigations.

While the burden of photographic documentation may fall on a professional forensic photographer for some fortunate agencies, many non-photographers in the forensic community find themselves struggling to take high-quality photographs, especially in low light situations. Since many forensic scenes occur at night or in low light situations, the use of these techniques can prove to be very useful to the forensic community as a whole.

---

**B5 An Approach for the Detection of the Illicit Use of Legitimate Network Access Credentials by an Intruder**

Christopher W. Day, BS*, 2 South Biscayne Boulevard, Suite 2800, Miami, FL 33131

After attending this presentation, attendees will understand how the pressures on corporate and governmental managers who believe that their organization has been the target of a successful breach of sensitive personal or health-care data can lead to jumping to conclusions that, in fact, a suspected breach is a real one. This can result in the notification of thousands of people, informing them that they have been victims of an incident that, in fact, never occurred. The application of computer forensics often provides the best way of determining whether an actual incident occurred and whether that incident meets the varied criteria for victim notification under the 47 United States State laws, plus applicable United States and international federal laws and regulations.

This presentation will impact the forensic science community by demonstrating that through the use of digital forensics, companies can avoid needless large outlays for notification and remediation cost if it can be shown with forensic accuracy that an incident did not occur (or that it is different in scope than assumed) and avoid the creation of unnecessary anxiety on the part of persons who would be concerned about identity theft when, in fact, their data was not at risk.

When an organization has reason to believe it has suffered a breach of sensitive personal or health-care information, there are literally dozens of state and federal laws and regulations that may, depending on the nature of the data compromised, and the home jurisdiction of the individuals involved, require specific notification of affected individuals as well as governmental entities. These notifications are often tied to tight timelines in the law, but it has been found that with proper project control and forensic discipline, an investigation can be carried out within the allotted time frames that can provide management (and usually counsel) with the best information available to support their decision making process. Recent surveys indicate that the cost to an organization of a data breach can exceed $20 per victim simply for notification and basic remediation assistance, so breaches of as little as 50,000 records can quickly result in a million dollar unplanned expense. This is, of course, in addition to what can be substantial costs related to reputational damage, and the potential costs of litigation, or added regulatory oversight that can result from reported cases of data loss – even where it is later found that the event did not actually occur.

The forensic work has the added benefit, in many cases, of providing valuable insights into exactly what happened, the vector through which an incident originated, and sometimes information about the perpetrators. It is not unusual to be able to provide some assurance that an incident has been stopped and that there is not a continuing leakage of sensitive data.

A series of case studies based on the team’s work that will demonstrate actual situations in which computer forensics proved that an incident did not occur, or that it was less severe than had been assumed will be provided.

---

**B6 Preventing a Rush to Judgment: Application of Computer Forensics in Data Breach Cases**

Jason M. Paroff, JD*, Kroll Ontrack, 1 Harmon Meadow Boulevard, Suite 225, Secaucus, NJ 07094; Stephen D. Baird, MS, Kroll Ontrack, 1166 Avenue of the Americas, 23rd Floor, New York, NY 10036; and Alan E. Brill*, MBA, Kroll Ontrack, 1 Harmon Meadow Boulevard, Suite 225, Secaucus, NJ 07094

After attending this presentation, attendees will understand how the pressures on corporate and governmental managers who believe that their organization has been the target of a successful breach of sensitive personal or health-care data can lead to jumping to conclusions that, in fact, a suspected breach is a real one. This can result in the notification of thousands of people, informing them that they have been victims of an incident that, in fact, never occurred. The application of computer forensics often provides the best way of determining whether an actual incident occurred and whether that incident meets the varied criteria for victim notification under the 47 United States State laws, plus applicable United States and international federal laws and regulations.

This presentation will impact the forensic science community by demonstrating that through the use of digital forensics, companies can avoid needless large outlays for notification and remediation cost if it can be shown with forensic accuracy that an incident did not occur (or that it is different in scope than assumed) and avoid the creation of unnecessary anxiety on the part of persons who would be concerned about identity theft when, in fact, their data was not at risk.

When an organization has reason to believe it has suffered a breach of sensitive personal or health-care information, there are literally dozens of state and federal laws and regulations that may, depending on the nature of the data compromised, and the home jurisdiction of the individuals involved, require specific notification of affected individuals as well as governmental entities. These notifications are often tied to tight timelines in the law, but it has been found that with proper project control and forensic discipline, an investigation can be carried out within the allotted time frames that can provide management (and usually counsel) with the best information available to support their decision making process. Recent surveys indicate that the cost to an organization of a data breach can exceed $20 per victim simply for notification and basic remediation assistance, so breaches of as little as 50,000 records can quickly result in a million dollar unplanned expense. This is, of course, in addition to what can be substantial costs related to reputational damage, and the potential costs of litigation, or added regulatory oversight that can result from reported cases of data loss – even where it is later found that the event did not actually occur.

The forensic work has the added benefit, in many cases, of providing valuable insights into exactly what happened, the vector through which an incident originated, and sometimes information about the perpetrators. It is not unusual to be able to provide some assurance that an incident has been stopped and that there is not a continuing leakage of sensitive data.

A series of case studies based on the team’s work that will demonstrate actual situations in which computer forensics proved that an incident did not occur, or that it was less severe than had been assumed will be provided.

---

**References**


Untrained or inexperienced photographers often face several challenges when it comes to low light photography. These challenges are most commonly associated with the limitations of a mounted flash unit. By removing or disabling the flash unit and manipulating the camera settings, an apparent daylight photograph can be achieved. These types of photographs can add valuable information to an investigation or serve as a permanent visual record of the scene prior to evidence being removed for processing.

While inexpensive point and shoot cameras appear to be a simple solution for investigators lacking photography experience, these cameras often fail to produce the desired results. These cameras often have severe limitations and pre-fixed settings which can prevent the photographer from achieving the desired exposure. For these reasons, SLR cameras are recommended for most typical forensic photography situations and required for low light situations. This presentation is designed to show how previously untrained investigators are now using these SLR cameras and manual camera settings to perform the advanced photographic techniques used to document scenes in low light situations.

Once a basic understanding of camera operation is established, investigators should be entrusted with SLR cameras capable of long exposures and tripod mounting. Through training the investigative staff is allowed to experiment with manual camera settings, tripods, and SLR cameras under the direct supervision and instruction of a trained forensic photographer. By learning how shutter speed and aperture affect the exposure, investigators can begin to use the minimal available light to illuminate the scene beyond what is visible with the naked eye. The investigators begin to understand the limitations of a traditional flash and how street lamps, headlights, and even flashlights can provide the needed light to capture the entire scene.

With proper equipment, training, and practice, scene investigators have achieved outstanding results with time exposures and “painting with light.” These valuable tools provide the quality of photographs needed for proper scene documentation and, therefore, the transfer of all available and potentially crucial scene information onto the forensic pathologist or other investigative agencies.

The result of these training initiatives is demonstrated in the photographs themselves by comparison of traditional methods to these more advanced techniques. The discussion will encourage agencies to enhance their use of photographic documentation and training across multiple disciplines as well as provide examples of how this has been accomplished in our agency.

Photography, Low Light, Investigations

B8 Imaging the Unseen with Digital UV/IR Technology: Preliminary Bruising and Tattoo Studies

Stephanie L. Hoffman, MSFS*, 27811 Northbrook Avenue, Canyon Country, CA 91351; and Wilson T. Sullivan, MPA, Chaminade University of Honolulu, 3140 Waiulae Avenue, Honolulu, HI 96813-1578

After attending this presentation, attendees will learn about the electromagnetic spectrum and its relevance to visible, ultraviolet, and infrared digital photography. This presentation will also cover the documentation of visible, ultraviolet, and infrared radiation and their effects on different items of evidence as they transmit (remove), reflect (lighten), and/or absorb (darken) with each type of radiation, with digital single lens reflex (SLR) camera systems. Camera/lighting settings and equipment will also be suggested for specific types of evidence. In particular, the preliminary research results on revealing/documenting both fresh and healed bruising and removing/darkening tattoos with ultraviolet (UV) and infrared (IR) radiation will be discussed. These preliminary research findings aim to highlight the possible evidentiary results that can be obtained through the use of these techniques, and how easily they can be accomplished with a UV/IR modified digital SLR camera. Successful results were obtained with each tattoo and bruise tested; of particular note is a case where the bruise was revealed seven months after it had disappeared from human sight. It is clear that both of the referenced techniques have yielded results proving they could be of great use at investigative stages with identifications and abuse cases.

This presentation and the research proposed within it will impact the forensic science community by demonstrating: (1) the need for the everyday use of both visible and ultraviolet/infrared (UV/IR) photography in forensic cases; (2) the ease with which these techniques can be accomplished via digital photography; and, (3) the impacts possible at various stages in the criminal justice process which can be achieved by revealing and documenting evidence that often goes unnoticed.

The potential of ultraviolet/infrared (UV/IR) photography to aid in investigations has yet to be fully realized and utilized by the forensic community. Past film based methodologies for this type of photography were difficult, unpredictable, inconsistent and/or expensive, resulting in its limited use. However, the once popular film based camera systems are being replaced by digital equivalents, and as such, it is time these old film methodologies were reevaluated as potential tools with the new digital single lens reflex (SLR) camera systems. UV/IR photography no longer needs to be thought of as difficult, unpredictable, inconsistent, and/or expensive since digital camera systems offer a framework to make these techniques and applications a more feasible option. This research demonstrates the need for the standard use of both visible and UV/IR digital photography in forensic cases by identifying the possible unique evidentiary items these techniques can now provide for identifications and abuse cases; as well as the ease with which these techniques can now be accomplished through digital means. The speed with which such results can now be obtained and distributed has the potential to greatly impact and expedite cases at both the investigative and prosecutorial stages.

Infrared, Ultraviolet, Photography

B9 Camera-to-Subject Distance and Facial Comparison Examinations

Richard W. Vorder Bruegge, PhD*, Federal Bureau of Investigation, OTD-DES, Building 27958A, Pod E, Quantico, VA 22135

After attending this presentation, attendees will learn how to calculate the subject-to-camera distance necessary to achieve an orthographic projection for the face over the region extending from the nose to the ears, as well as the implications of this result for individuals and agencies involved in the capture and analysis of facial images, particularly when using measurements of facial features for comparison analysis.

This presentation will impact the forensic science community by informing it of a technical issue relating to forensic facial comparison that could lead to multiple false exclusions of subjects.

Forensic facial comparison examinations often incorporate a combination of morphological and anthropometric analyses.1 Recent efforts have begun to rigorously assess the utility of anthropological landmarks2,3 and morphological features4 as objective, measurable characteristics of faces that can be used for comparison analysis. It is anticipated that forensic facial comparison analyses in the future will incorporate a more explicit determination of the size and shape, relative or otherwise, of specific features of the face and head than has been done in the past. Such features include the eyes, nose, mouth, and ears.

While many key facial features used in forensic comparison (as well as in facial recognition applications) are practically co-planar (e.g., eyes and mouth), the nose and ears are distinctly out of the facial plane. As a result, they are prone to perspective distortion and the relative size of these features will vary with camera position relative to the subject.

* Presenting Author
The degree to which this effect impacts the accuracy of automated facial recognition (FR) algorithms and systems has not been reported. Since the ears are not considered by most FR algorithms, any distortions to them can be expected to have a negligible effect on the automated portion of the system. However, practical experience has shown that human reviewers of FR system output frequently focus on the ears and nose to quickly sort through a candidate list. As a result, distortions in ear and nose can negatively impact the overall effectiveness of a human-computer FR system.

The effect of perspective on facial images is well established in the photographic and forensic communities. An analysis of anthropological landmarks on several subjects included in the MAGNA database demonstrated the degree of measurement errors that ensue for different camera-to-subject distances. In particular, measurements of features associated with the ears were shown to be especially prone to perspective error. This result was not unexpected, given the fact that the ears are the most remote part of the face and head that is visible in a frontal image.

Under ideal conditions, 2-dimensional images of the face and head (photographs or video images) would be acquired in a way that perspective distortions were removed, and measurements taken from the photograph would accurately reflect the true physical measurements – so long as those measurements were taken in a plane parallel to the plane of the camera sensor. Images which depict three-dimensional objects with no perspective distortion, such as architectural drawings, are referred to as being in orthographic projection and they reflect a situation in which all rays of light reflected off a subject enter the camera lens parallel to one another.

Existing guidance for the acquisition of frontal photographs (e.g., ANSI/NIST-ITL 1-2007) describes a typical camera to subject distance of 1.5- to 2.5-meters. In this paper, it will be demonstrated that this distance is sufficient to generate a correct perspective projection of the face and ears when a frontal photograph is acquired to meet resolution requirements for SAP Levels 40 and above. Instead, a distance of approximately 70-meters would be necessary to achieve orthographic projection for a facial image that incorporates the entire region from the nose to the ears at SAP Level 40 (approximately 200-pixels between the pupils), while a distance of approximately 125-meters is necessary for SAP Level 50 (approximately 600-pixels between the pupils). Such distances are impractical in virtually every controlled capture (e.g., enrollment) scenario. As a result, facial comparison practitioners must actively incorporate anticipated perspective effects into their analyses. Likewise, any other forensic or biometric application that incorporates the nose and ear as components must take this effect into account. This particularly applies to anyone who would use photo-anthropometry alone as a basis for inclusion or exclusion of a subject.

It is important to note that human beings are not accustomed to viewing each other in orthographic projection, but in perspective projection. Under such conditions, a photograph depicting a subject in an orthographic projection could lead to an improper exclusion by a screener. As a result, the requirements of manual screening and forensic analysis may be somewhat at odds with one another.

References:

B10 A Review On Automatic Footwear Retrieval Systems From Crime Scene Shoe Marks

Federico Cervelli, PhD*, Via Valerio 10, Trieste, 34100, ITALY; Francesca Dardi, BS, and Sergio Carrato, PhD, University of Trieste, Via Valerio 10, Trieste, 34100, ITALY

After attending this presentation, attendees will have a clear understanding of the state of the art systems for the automatic retrieval of the footwear that left the shoe mark found at the crime scene and will gain a basic understanding of automatic “one to one” comparison techniques between the shoe mark and the suspect’s footwear.

This presentation will impact the forensic science community by providing knowledge of state of art automatic footwear retrieval systems, developed to help forensic scientists in finding the shoe that left the mark at the crime scene.

The activities performed during the crime scene analysis are of paramount importance for the investigation. The crime scene expert is in charge of the detailed documentation of the crime scene status, as well as the search for fingerprints, shoe prints, biological fluids, chemicals, firearms ammunition, and the collection of the items pertaining the crime for a later and deeper analysis in the laboratory.

In particular, shoe marks play a key role to understand the crime and can help investigators gain precious information: when there is no suspect or few elements are available, knowing the make and model of the shoe sole that left the shoe mark on the scene can point a path, while, on the other hand, if there is a known suspect, his or her shoes can be compared to the shoe mark found on the crime scene to evaluate his or her involvement in the criminal act.

Two different approaches can be followed in order to find the make and the model of the shoe which produced the shoe mark on the crime scene: (1) a forensic shoe print expert analyzes the shoe mark and looks for the corresponding shoe on electronic and paper catalogs; and (2) a footwear retrieval system is queried with the crime scene shoe mark, and the results of the query are then analyzed by the expert.

Some semi-automatic systems have been proposed and face the problem: shoe prints are classified by a human expert which describes them with a series of geometric patterns. This work will guide the audience through the systems proposed in literature, starting from the very first work to current algorithms. Fourier based systems, fractals based systems, invariant moments systems, and feature based systems will be shown and their working principles will be explained in all relevant details to guarantee their understanding. A comparison among
the different approaches will be made showing the advantages and disadvantages of each method under a forensic point of view.

Results of the performance of some of the most successful methods will be presented, both on synthetic and on real shoe marks, showing the difference between ideal and practical performance from the perspective of the forensic expert in the need to choose among one of the available approaches.

The presentation will end with a brief overview on automatic method to compare the shoe mark with the suspect’s footwear.

The audience will be aware of the advantages and disadvantages of the current state of the art on automatic footwear retrieval systems.

Shoe Mark, Automatic Retrieval System, Footwear

B11 Preliminary Assessment of Discrimination of Twins in Photographs Based on Facial Blemishes

Nisha Srinivas, MS*, Matthew Pruitt, BA, Gaurav Aggarwal, PhD, and Patrick J. Flynn, PhD, University of Notre Dame, Department of Computer Science and Engineering, South Bend, IN 46556; and Richard W Vorder Bruegge, PhD, Federal Bureau of Investigations, OTD-DES, Building 27958A, Pod E, Quantico, VA 22135

After attending this presentation, attendees will be aware of efforts to utilize facial blemishes as a potential means of identification in photographs.

This presentation will impact the forensic science community by exposing them to current research efforts to establish a statistical basis to support the Digital and Multimedia Sciences (DMS) discipline of forensic facial comparisons – a critical aspect of all forensic disciplines in light of the National Academy of Science report. Attendees should recognize a need to develop a deeper understanding of this and other emerging forensic disciplines within DMS and consider their applicability to their forensic laboratory.

Digital cameras capable of recording both still images and videos are ubiquitous in our society. Likewise, video surveillance through the use of closed-circuit television systems is becoming more prevalent. Frequently, law enforcement or intelligence agencies have a requirement to identify subjects depicted in those photographs and videos. The growing interest in both facial recognition and facial identification led the Federal Bureau of Investigations to create the Facial Identification Scientific Working Group (FISWG) in 2009. The mission of FISWG is to develop consensus standards, guidelines, and best practices for the discipline of image-based comparisons of human features, primarily face, as well as to provide recommendations for research and development activities necessary to advance the state of the science in this field.1

As background, FISWG defines facial recognition as “[t]he automated searching of a facial image in a biometric database (one-to-many), typically resulting in a group of facial images ranked by computer-evaluated similarity,” while facial identification is defined as “[t]he manual examination of the differences and similarities between two facial images or a live subject and a facial image (one-to-one) for the purpose of determining if they represent the same person.”2 In a practical sense, (automated) facial recognition systems generate candidate lists which must then be evaluated by a human reviewer performing facial identification.

While there has been extensive research conducted in facial recognition and, to a lesser extent, facial identification within both academic and industrial settings, this research has not yet converged to a single consensus set of standards of practice comparable to fields such as DNA analysis or fingerprint analysis, nor has a statistical basis for identification or exclusion been established. As a result, fully automated face recognition has not yet achieved a level of reliability and repeatability that make it suitable for use as a means of identification in the court room. Likewise, while the manual comparison process of facial identification has been accepted for expert testimony in multiple United States federal and state courts, it is lacking in a statistical basis from which conclusions may be drawn.

One attempt to address the statistical basis for human identification from facial images is the Magna Study.3,4 In this large scale study involving over 3,000 subjects, it was determined that a meta-analysis of anthropometric measures of landmarks common to all human faces is not sufficient to discriminate between individuals. Put another way, this study found that the geometric distribution of a large set of landmarks common to all human faces (e.g., corners of the eyes and mouth) is not sufficiently unique to allow one to individualize a subject. Additional work remains to be performed on the Magna data to determine to what degree individuals might be segmented into individual classes based on the distribution of these landmarks. However, the Magna result indicates that facial features other than common landmarks will be necessary to support classification to groups smaller than 1% of the population.

Facial blemishes, such as freckles or moles, are currently considered to be the best candidates for these features, as they are presumed to be comparable to friction ridge minutiae.

Incorporation of facial blemishes as features has already been shown to improve automated face recognition software.5 The current effort to be described in this presentation would extend the utilization of such features for automatic face recognition, but will also have applicability to the forensic use of facial identification. More specifically, the current effort is intended to assess the ability to discriminate between identical and fraternal twins based solely on the distribution of facial blemishes. The hypothesis to be tested is that the distribution of blemishes on one twin’s face will differ from the distribution of blemishes on the other’s face. A secondary hypothesis to be tested is that the distribution of blemishes on any given face is random.

Data supporting this effort has already been collected for approximately 100 pairs of twins in 2009 at the Twins Days convention, held annually in August in the town of Twinsburg, Ohio. An additional collection is planned for 2010. For this analysis, each facial image will be processed using a face detection algorithm based on the work of Viola and Jones6 that returns the bounds of a candidate face.

An Active Shape Model, first developed by Cootes et al.,7 is fit to the face’s bounding region, yielding a set of face feature locations that correspond to anthropometrically or photometrically significant points. Combinations of these points define one or more face-centered coordinate systems, providing a normalized basis for feature location. After normalization, blemishes will be identified using an automated extraction technique based on an approach first developed by Park and Jain.8 Once blemishes have been marked, their distribution will then be determined for each subject and comparisons performed between subjects – not just within twin pairs, but across the entire population of subjects.

References:


* Presenting Author
Presenting Author

PDF of a sum of bytes is the convolution of the two uniform size. The principle that allows this to occur is that bytes can be treated as triggering a hash are considerably worse than those of a smaller block that this modulus would be hit as the odds of a larger block size would set off to create a hash character when the rolling sum modulus hashes to block sizes. This was done by keeping a third counter which or not it was actually a derivative of another file. An examiner would probably need to look at the file to determine whether match and one would expect the match score to drop to a number where suddenly falling to zero. After some investigation, it was found that this relatively good matching distances. This problem would occur a relatively significant amount of the time as the length of a fuzzy hash is between 33 and 64 characters. Originally, while this is occurring, another hash is being created that is appended to the original to allow for comparisons of files with block sizes that were either 50% or 200% of the original.

This brought about a relatively serious false negative rate as the block sizes changed for specific files that were just on the edge between two different block sizes. For files of this type, fuzzy hashing is unable to match files that were ~50% of the size of the original or greater than 200% of the size of the original for certain cases. In testing, this proved to be troublesome as the file was still very similar to the original, but due to the intolerance of differences in block sizes there would be no match.

This would occur a relatively significant amount of the time as the length of a fuzzy hash is between 33 and 64 characters, but the distribution is uniform, meaning that these tail conditions are just as likely to occur as the more generally tolerant conditions of a hash around 48 characters which can be appended to either way and still achieve relatively good matching distances.

During testing, it was observed that the match scores reported back were generally linearly dropping to a range around 40-50 and then suddenly falling to zero. After some investigation, it was found that this had to do with the block sizes being incompatible. This generally seemed counterintuitive as a large portion of the file was still a perfect match and one would expect the match score to drop to a number where an examiner would probably need to look at the file to determine whether or not it was actually a derivative of another file.

The solution to this problem was to expand the tolerance of the hashes to block sizes. This was done by keeping a third counter which would set off to create a hash character when the rolling sum modulus four times the original block size was equal to one less than that number.

This could lead to some questioning as to how one could be sure that this modulus would be hit as the odds of a larger block size triggering a hash are considerably worse than those of a smaller block size. The principle that allows this to occur is that bytes can be treated as something close to independent uniform distributions from 0-255. The PDF of a sum of bytes is the convolution of the two uniform distributions, which in statistical terms forms a Gaussian curve about twice the average. Some simple math can show that discrete Gaussian modulus of the block size creates a uniform distribution from 0-(block size-1), meaning that it is simply a negative binomial distribution that repeats itself each time it ends.

Knowing that the statistics approach the expected value the longer they continue, it was safe to assume that in almost all cases (for non trivial files) that the third hash would be between 8 and 16 characters which is enough information to reliably trigger a match. Producing a fourth hash though, would max out at eight characters, and since the algorithm requires more than seven consecutive characters to be the same for any match to be declared, as well as the tendency for the values that are effected in the hash to change with relatively little data added, only an exact match of the file could be found, and only if that file happened to be one of the 20% of files that happened to have an 8 byte hash.

When using this third hash appended to the first two, false error rates were on average halved, but they became much more useful in the sense of appearing more like what you would expect a human to be able to detect. It is easy for the human brain to determine visually that a file is 40% identical to another and he/she will then wonder why the hash fails to accurately classify this homology. Using the old method, files would (on average) fall off when there was a 37.5% match, but now this level of accuracy has been doubled allowing files to match down to an 18.75% match. This level of matching allows for the limitation to become the actual algorithm to match files rather than the generation of hashes.

The tradeoff for this would be an expected increase in processing time as the program is now computing three hashes instead of two. There is a very slight increase in processing time due to the fact that the extra hashes only provide new code when they are invoking their own encoding of data which is one-sixth as often as the original two pieces of the hash are invoked. This combined with the fact that there is only one extra operation per cycle which does not get invoked this allows for the increase in execution time to be only 10%.

Digital Forensics, Fuzzy Hashing, Error Rate

B13 Computer Forensic Bitmaps and Visualization for Data Identification

Shane A. Macaulay*, Security Objectives Corporation, 1100 Dexter Avenue North, Suite 100, Seattle, WA 33487

After attending this presentation, attendees will understand some of the principles of visualization techniques which can be applied to data identification.

This presentation will impact the forensic science community by discussing the components used to generate bitmaps from opaque data regions. Attendees will be presented visualized examples from several public data sources and understand how these can be applied toward forensic methods and tools.

These images are generated fundamentally by using variable block hashing combined with advanced search techniques (akin to an overlay network of a distributed hash table) and guaranteed binary clone detection.

Using established cryptographic algorithms, or “digital fingerprints”, with scaled variable size, applied to an opaque data region, illustrates a domain of knowledge when extrapolated against what is currently known in an existing database. Database seed material would typically be data from sources such as National Institute of Standards and Technologies (NIST) National Software Reference Library (NSRL), or other similar collections.

Bitmap generation applications can be used for coverage analysis, isolation of unknown or new artifacts and also data recovery. Data
of frame rates, resolution and amount of movement of a person on the
between variability of reconstructed 3D models; determine the influence
uncalibrated multi-frame video material this collaborative project aims
generate a dense 3D model based on shape and texture but are
pose and lighting conditions resulting in easy and quick binary
 advantages and disadvantages. Shape from Silhouettes is robust against
the use of Morphable Models. Each of these techniques has its own
information in the multiple frames.

Verification 3D."

Although biometric techniques exist for facial comparison using
image material, these techniques only show acceptable performance
when using full frontal images of good quality in a controlled
environment. As soon as the quality of the image material is gets below
ISO 19794 requirements, the performance of the current biometric
systems quickly deteriorates. As it is extremely rare that surveillance
video footage material complies with the ISO 19794 requirements,
automated biometric systems in practice are useless for forensic
casework.

Current forensic facial comparison techniques using un-calibrated
CCTV footage are based on visual comparison by human operators using
2D images. Forensic experts take only one or a few frames from a video
on which they base a facial comparison with images or reconstructed
video footage of a suspect. During this process, potentially valuable
information from unused sub-optimal frames is discarded.

To improve the use of the available image information and to
develop techniques to determine the evidential value of the surveillance
video, the Netherlands Forensic Institute started a collaborative project
with the University of Twente, The Netherlands, titled “Person
Verification 3D.”

Using a multi-frame approach, more of the available information
can be used. In contrast to 2D image comparison, 3D model comparison
is more reliable, because it doesn’t suffer from changes in lighting
conditions and/or pose. It also offers the possibility to combine the
information in the multiple frames.

The main three techniques to reconstruct 3D facial models from 2D
video footage are Structure from Motion, Shape from Silhouettes, and
the use of Morphable Models. Each of these techniques has its own
advantages and disadvantages. Shape from Silhouettes is robust against
pose and lighting conditions resulting in easy and quick binary
comparison for fitting but a PCA shape model is needed for accurate
reconstruction. Structure from Motion is robust against lighting
conditions but results in a relative sparse model. Morphable Models
generate a dense 3D model based on shape and texture but are
computationally expensive.

In evaluating existing techniques for building 3D face models from
uncalibrated multi-frame video material this collaborative project aims
to combine the complementary techniques to: determine the within and
between variability of reconstructed 3D models; determine the influence
of frame rates, resolution and amount of movement of a person on the
accuracy of a 3D model; compare the constructed 3D models with 2D
and 3D reference material; and to quantify the evidential value of the
available footage in terms of a Bayesian likelihood framework.

An overview of existing biometric techniques, visual comparison of
CCTV footage, the techniques used to construct 3D models, the progress
of the project, and initial results using CCTV footage of varying quality
will be presented.

B15 Removing JPEG Artifacts in Skin Images
for Forensic Analysis

Chaoyang Tang, MEng*, Nanyang Technological University, Forensics
and Security Lab, NSI-05-01A, School of Computer Engineering, 50
Nanyang Avenue, 639798, SINGAPORE; Adams W. K. Kong, PhD*,
Nanyang Technological University, Bld N4, 50 Nanyang Avenue,
639798, SINGAPORE; and Noah Craft, MD, PhD, DTM&H, University
of California at Los Angeles School of Medicine, LA Biomedical
Research Institute, at Harbor-UCLA Medical Center, 1000 West Carson
Street, Torrance, CA 90502

After attending this presentation, attendees will understand a new
method which removes blocking artifacts in JPEG-compressed skin
images for forensic analysis.

This presentation will impact the forensic science community by
providing a useful method to remove blocking artifacts in JPEG-
compressed skin images. With this technique, biometric traits in
evidence images can be used for criminal and victim identification
reliably.

Recent technological advances have allowed for a proliferation of
digital media. This media can be used as evidence in legal cases and
hints for investigation. Increasing capability of processing this media for
criminal and victim identification is becoming an important task. In
some cases (e.g., child pornography and masked gunman), faces of
criminals or victims cannot be seen, because they are covered or
obstructed. Biometric traits on/in the skin (e.g., skin marks and veins)
become important features for identification. Dr. Craft and Dr. Kong
were recruited by the United States Department of Justice as expert
witnesses for a legal case, United States v. Michael Joseph Pepe (2008),
which involved sexual acts with seven pre-teen girls in Cambodia. Dr.
Craft was required to identify skin marks in digital images (evidence
images) collected from a crime scene and skin marks of the suspect, Mr.
Pepe, for verification, because the face of the criminal in the evidence
images could not be observed. Unfortunately, Dr. Craft’s expert opinion
was challenged, partially because of blocking artifacts in the evidence
images.

Using biometric traits in/on the skin for criminal and victim
identification highly depends on quality of evidence images because of
the size of these traits. Evidence images, taken by consumer cameras,
are always compressed by the JPEG algorithm. Blocking artifacts are a
well known problem caused by this algorithm. As a result, vein patterns
can be broken and skin marks can be blurred, or even totally removed,
especially under high compression ratios. Although many methods have
been proposed to remove blocking artifacts, none are developed
specifically for skin images. In fact, they make the situation even worse,
because they generally smooth images, including the traits, to alleviate
blocking artifacts.

This presentation introduces a new algorithm to remove blocking
artifacts in skin images. This algorithm formulates skin image
deblocking as an estimation problem and embeds statistical information
of skin images into a maximum a posteriori (MAP) model to perform the
estimation. A statistical analysis is carried out on a skin image database
to obtain a cumulative distribution function (CDF) of difference between

* Presenting Author
two neighboring pixel values. Because intensity values usually do not change abruptly in a skin image, the CDF of the database and that of a testing image are quite similar. However, the JPEG algorithm removes high frequency information and changes the original CDF. This phenomenon is more serious in the $U$ and $V$ components, because of the down-sampling process and because of the even larger quantization parameters in the JPEG algorithm. The proposed algorithm uses the CDF of the database as a target to modify a compressed image. A potential function is designed based on the difference between the CDF of the database and that of the compressed image. In this way it connects the MAP model and the statistical information from the skin image database. The gradient descent method is utilized to minimize the potential function.

The proposed algorithm has two novel characteristics: first, it exploits the prior knowledge of skin images extensively; and, secondly, it guarantees that the resultant and compressed images have the same quantized Discrete Cosine Transform (DCT) coefficients, which cannot be achieved by most other methods. The performance of the algorithm was evaluated on 762 skin images with different compression ratios, and compared with four other deblocking methods. Both subjective and objective evaluations demonstrated that the results from the proposed algorithm were more close to the original images. It not only removed blocking artifacts, but also recovered skin features. The out-performance was more obvious when the compression ratio increased. From the resultant images, vein patterns and skin marks can be extracted efficiently for forensic analysis.

Child Pornography, Vein Pattern, Skin Mark

B16 Conversion of AVI “txts” Stream Data to Adobe® Premiere® Pro Title Files

Douglas S. Lacey, BS*, DL Technology LLC., 4 Averil Court, Fredericksburg, VA 22406; and Bruce E. Koenig, MFS, BEK TEK LLC., 12115 Sangsters Court, Clifton, VA 20124-1947

After attending this presentation, attendees will understand how to identify and extract text or caption data embedded in an Audio Video Interleave (AVI) multimedia container format file. Once extracted, this information can then be converted into Adobe® Premiere® Pro title files, which can then be used in conjunction with the imported video/audio information.

This presentation will impact the forensic science community by allowing video examiners to more comprehensively review a video/audio recording contained in an AVI file. The embedded text information, which may be overlooked, can prove to be vitally important in establishing an accurate timeline of events.

AVI files may contain video, audio, and/or text data, multiplexed and indexed as separate data streams (“vids,” “auds,” and “txts,” respectively) within a single container file. Multimedia software such as Windows Media Player allows for playback of both the recorded video and audio information and, through an optional setting, enables the user to display the embedded text or caption data, if present. Typically, this text data is displayed by the software outside of the video playback area, and not as an overlay of the recorded visual information.

With AVI files produced by digital video recorders (DVRs), embedded text information typically consists of corresponding date and time information for the captured images/audio, an assigned name for the particular camera view, and/or other identifying information. Date and time information may also be “burned” into the visual data, but the embedded information sometimes provides additional detail. For example, a video frame may have a “burned” time of “09:55:44,” and an embedded time of “09:55:44.197,” thereby providing timing information out to the millisecond. Unfortunately, when AVI files with embedded text data are imported into non-linear video editing software such as Adobe® Premiere® Pro for more detailed review, the embedded text information is no longer accessible and is unable to be displayed.

Through detailed analysis of an AVI file’s structure and index, the locations of the embedded “txts” stream data entries can be determined, and accordingly, they can be extracted into a separate data file. By creation of a template Adobe® Premiere® Pro title file, separate title screens can then be produced for each extracted text entry. These title screens can then be imported into Adobe® Premiere® Pro and overlaid on their respective video frames, allowing for a more detailed analysis of the recording. Batch processes can be used to expedite the location, extraction, and conversion steps.

Two case examples in which they produced automated scripts for the location, extraction, and conversion of embedded “txts” stream data into Adobe® Premiere® Pro title files will be presented. These title files were then used to establish accurate timelines of the depicted events, to find discontinuities in the original recording processes, and to provide additional information which was not readily apparent from analysis of only the video and audio data.

While this presentation concentrates on the use of Adobe® Premiere® Pro, the methodology and steps which will be discussed may be applicable to other non-linear video editing programs, which feature title screens or a similar ability to overlay text information on a video file.

Digital Video, Embedded Text, Metadata

B17 Recovering Multimedia From File Fragments

Michael Piper, BA*, United States Secret Service, 950 H Street, Northwest, Suite 4200 - FSD, Washington, DC 20223

After attending this presentation, attendees will gain an understanding of how multimedia files, commonly used in cell phones, are structured and how that structure can be exploited to recover the audio and video contents of fragmented files.

This presentation will impact the forensic science community by bridging the gap between the computer forensics and multimedia forensics disciplines by demonstrating a methodology for recovering the multimedia payload within damaged or partially recovered files.

Cell phone forensic examinations are performed everyday to recover existing and deleted data. Reviewing file fragments can be problematic depending on the type of data contained within the file and the scheme used to encode it. ASCII text characters have a direct representation in digital data and can be interpreted easily. Multimedia information (audio and video) is more complex. Audio and video encoders exploit human perception to reduce data redundancy. This results in algorithms that are highly complex and have many variable options. Knowing the state of these variables can distinguish streaming multimedia from gibberish.

In this case study, fragments of two deleted files recovered from separate cell phones will be examined – a 3GP file and an MP4 file. In each case, an exemplar file was provided from the phone. Attempts to play these fragments directly were not successful, but suggested that information was present. Successful decoding of the multimedia payload required understanding the file specifications of the data involved, exploiting the exemplar files to form assumptions that reduced the unknown variables, and exploiting existing metadata to calculate the missing metadata. Once sufficient metadata was reconstructed, a standard multimedia viewer could be used to play the recordings.

Multimedia, File Fragments, Recovery
B18 Quantifying Phase Changes in Audio Authenticity Examinations

David J. Snyder, BS*, William L. Hinton, BS*, Andrew Galotti, BS*, and Kenneth Marr, MS*, Federal Bureau of Investigation, Engineering Research Facility, Building 27958A, Quantico, VA 22135

The goal of this presentation is to present testing results of manual and automatic methods for detecting phase changes in forensic audio recordings when conducting audio authenticity examinations.

This presentation will impact the digital and multimedia forensic science community by defining the limitations of using phase change as an analysis tool in audio authenticity examinations. Phase changes by themselves may not provide insight as to whether an event is an alteration or not, but shows promise as a method to correlate multiple events. If the accuracy of detecting phase changes is unreliable, this will also impact the value of it being used as potential method for forensic audio authentication.

Hypothesis: To determine whether a phase change in a forensic audio recording can accurately be identified as an alteration or edit and develop criteria or parameters classifying the event as such.

Synopsis: A series of test recordings that include various digital and analog formats, which are both altered and unaltered with discrete reference tones recorded at various amplitudes will be used to test manual and automatic methods for a change in phase. Testing results provide answers to the question: Is a phase change in an audio file synonymous with alterations?

The use of changes in phase is not a new analysis method for forensic audio authenticity examinations. Interest in expanding its role to detecting edits in digital recordings has increased in the last several years. Several concerns accompany this increased interest. Automatic detection of phase shifts can help speed a cumbersome time-consuming process of manually locating events, but accuracy and the thresholds of such detection methods are not widely known. Even if events are detected accurately there is not any specific criteria to determine whether the phase shift is the result of an alteration or naturally occurring event during the time of recording.

Test recordings will be produced to include reference tones at various amplitudes to determine if changing the amplitude of the reference tone will directly impact the accuracy of automatic phase detection systems. The test recordings will also contain a range of naturally occurring events and files with various alterations. The use of several common digital formats that represent the type of audio being received for examination and the method in which they are recorded may show that some formats may not maintain phase. An automatic detection system may falsely identify phase changes that may be inherent to the recording process, format, or recording environment and not necessarily the result of an edit or alteration. It may also identify phase changes where they do not exist or not identify them at all. Being able to accurately account for the number of phase changes detected or not detected is important.

The second part of this presentation will attempt to clarify what a phase change means to the authenticity of an audio recording. Even if the detection of phase changes is accurate, what correlation does a phase change have to an alteration or edit? Examination of known events may help correlate phase changes caused by edits or naturally occurring ones. Criteria for establishing which phase changes are the result of an alteration and which ones are not is lacking. This problem is similar to identifying events as pause or voice-activated for analog recorders. Both of these events are caused by stopping the transport of the recorder without disengaging the record and erase heads. A pause event is generally associated with a potential alteration, whereas a voice-activated event is generally not. Often the events are identified through testing the operation of the analog recorder; these methods do not translate to digital recorders.

Statement: Phase changes by themselves may not provide insight as to whether an event is an alteration or not, but shows promise as a method to correlate multiple events. If the accuracy of detecting phase changes is unreliable, this will also impact the value of it being used as potential method for forensic audio authentication.

Audio, Authenticity, Data Analysis

B19 Camera Identification in Large Databases of Images

Zeno J. Geradts, PhD*, Netherlands Forensic Institute, Ministry of Justice, Laan van Ypenburg 6, Den Haag, SH 2497 GB, NETHERLANDS; and Wiger Van Houten, MS, Netherlands Forensic Institute, Laan van Ypenburg 6, Den haag, NETHERLANDS

After attending this presentation, attendees will be informed on different methods for camera identification, ranging from pixel defects to PRNU in digital cameras. Limitations and possibilities are discussed.

This presentation will impact the forensic science community by demonstrating the possibilities for extracting evidence from larger databases of images, such as child pornography and allow examiners to link cases to each other.

A digital camera consists of many electronic components. After the image has been formed on the image sensor, the image information will pass through all of the components before the final data file is written to flash memory. Each step in this process may add random noise to the image. Even during the image formation process itself, a noise-like pattern from the sensor may be introduced in the image. This noise-like pattern is a small but measurable systematic contribution to the signal, and is called the Photo Response Non Uniformity (PRNU) pattern. The visibility of this signal is limited and may be a small difference depending on the intensity of the signal. In practice, this means that well illuminated images will result in a better extraction of this signal compared to when the image is dark. Extraction of these patterns is done with complex filters, such as wavelet filtering.

The PRNU pattern itself can be determined from the image and it preferably is done with images with no discernible textures (flat field image, for example from a grey surface). In the past, the influence of strong compression was examined, and it appeared as though it was still possible to extract the PRNU pattern; however, it initially turned out to be more complicated than once thought. The examining of the PRNU pattern for forensic use is well researched by Jessica Fridrich and others.

There is a standard working procedure for the examination of PRNU in casework. The examiner will compare the retrieved pattern with one or more images. It will also be determined if the pattern is specific for the sensor (i.e., device characteristic) and determine the influence of possible class characteristic signals in this signal (i.e., brand or model characteristic). For this reason, at least three, and preferably ten cameras of the same make and model were used to validate the method for PRNU comparison.

In practice, it is not always possible to have the camera for casework; however, it is possible to determine if a set of images have been made with the same camera or different cameras based on the PRNU pattern. By comparing the pattern from a questioned image with the pattern from a set of reference images made with a suspect camera, it can be determined whether the questioned image was produced with the suspect camera or not. This works when the image is authentic, but fails when the image underwent any spatial transformations (e.g., rotation, shearing, resizing) because the “fingerprint” is desynchronized, unless the same transformations are applied to the reference material. It is also possible to alter the image such that the PRNU pattern is filtered out, although this is complicated and time consuming.

Other techniques for camera identification also exist, mainly based on statistical features. However, these approaches often involve time
consuming feature extraction and SVM training and only work on the classification level.

With this research, the influence of aging of cameras was also examined. This research also showed that matching based on a PRNU pattern within a two-year time frame for different models and brands of cameras was still successful. Also heating the cameras to 50°C, and freezing to -20°C, did not significantly alter the PRNU pattern within the tested cameras.

The use of large image databases, such as child pornography and other databases of relevant images will require significant processing power. For these, it is important to have a better pre-selection, based on other information, such as quantization tables of images which can be extracted instantly. The results of the examination based on images that were downloaded from online photo websites are demonstrated, and groups of cameras between the different images are found. For a good comparison, it is important to have the most original images, to know exactly what kind of operations have been conducted on the image. Since in casework the ground truth may not be known, it is important to draw conclusions based on a Bayesian framework.

PRNU, Camera Identification, Image Comparison

**B20  Macintosh® Forensics: A Crash Course**

Gavin W. Manes, PhD*, Avansic - Digital Forensics, 401 South Boston Avenue, Suite 1701, Tulsa, OK 74103

The goals of this presentation are to discuss: (1) data preservation and forensic collection from a Macintosh® system; (2) forensics investigation of a Macintosh® system; (3) differences between Windows™ and Macintosh® systems related to forensic collection and investigation; and, (4) additional challenges of the Macintosh® based on file system structure, file formats, and caches.

This presentation will impact the forensic science community by providing the basic tools and techniques to forensically acquire Macintosh® computers. Participants will also be aware of the complexities and difficulties of Mac computers vs. Windows™.

Most investigators spend their time an energy learning and keeping up with the latest tools and techniques for Windows™ investigators. However, the steadily increasing market share of Mac OSX means that most investigators will find themselves in a position to examine these systems. This presentation will give forensic investigator with little knowledge of the Mac OSX platform the basic knowledge necessary to acquire and analyze one of these systems.

The first step in any digital forensics investigation is to imaging evidence drives. However, Apple® has made it very difficult to work with hardware components, meaning that this seemingly simple task can become a complicated operation. A brief overview will be given of how to “crack the cases” for some of these machines and retrieve hard drives for imaging. Alternative means of acquiring images will be discussed, particularly when hardware, time, or other circumstances require that clever techniques be employed. Solutions presented will include the well-known “Firewire Target Mode” workaround, as well as instructions in using common Live CDs for imaging Apple® computers.

Once the basics of acquisition have been covered, a basic overview of the of the Mac OSX file system will be provided. The basic challenges to investigators will be described, the tools used to address those challenges, and the differences in the ways that each of those tools approaches the problems. Interpretation of HFS+ MAC times and unusual file types that have significant evidentiary value will be discussed. Other important evidence caches include information related to such user activity as web browsing, file usage, iPod and iPhone usage.

Working with Macintosh® computers is an increasingly necessary tool in the forensic investigator’s arsenal. But the Macintosh operating system has proved a very unique beast with its own set of challenges, requiring a body of specialized knowledge to tackle it effectively. The goal of this presentation is to familiarize the investigator with many of these basic problems and arm them with the some of the tools needed to level the playing field.

Digital Forensics, Data Preservation, Investigation

**B21  Macintosh® PList Files: Hidden Information for Digital Forensics Investigators**

Gavin W. Manes, PhD*, Avansic - Digital Forensics, 401 South Boston Avenue, Suite 1701, Tulsa, OK 74103

The goals of this presentation are to: (1) educate the audience about forensically relevant information contained within Macintosh® Plist files; (2) discuss the basic structure, functions, and location of Plist files; and (3) provide the audience with tools and information to appropriately interpret Plist files (particularly those who have digital forensics experience).

This presentation will impact the forensic science community by arming attendees with techniques and information in order to retrieve forensically relevant information from Macintosh® Plist files.

Although extremely common in system running Mac OSX and devices such as the Apple® iPhone and iPad, the structures of Apple® plist files remain mysterious to many forensic investigators. This creates an obstacle for many investigators tackling OSX systems, since plist files contain valuable information relevant to forensic investigations. Further complicating the issue, graphical interfaces for handling with these files are confusing and primitive at best.

An in-depth overview of the Apple® plist format in all of its incarnations, including the “binary,” “XML,” and “ASCII,” or “old-fashioned” formats will be given. Furthermore, information will be provided to help decode other formats an investigator may consider “unusual” that are sometimes seen stored in plist files relevant to forensic investigations. These include formats such as the “alias records,” which can be found storing potentially useful information about files that may exist in different locations across a system.

Finally, tips to efficiently process and analyze these files when encountered in the field using several readily available tools will be provided. The structure of commonly examined plist files will be discussed, along with important practical examples for handling some of the more complex structures.

This will give investigators inexperienced with this aspect of Mac OSX investigations a deep and informative look at what challenges might be normally encounter in the field.

Digital Forensics, Investigation, Computers

* Presenting Author
B1 Using Reports, Peer Review, and Administrative Reviews to Teach and Maintain Quality in Digital Forensics

Mark Pollitt, MS*, University of Central Florida, PO Box 162367, Orlando, FL 32816-2367

After attending this presentation, attendees will understand how to integrate a functional and managerial approach to teaching and implementing forensic report writing, peer review, and administrative reviews for digital forensic examiners in both traditional and non-traditional settings.

This presentation will impact the forensic science community by providing digital forensic examiners, their managers, and educators with a model that can be adapted to provide training, education, and process improvement in forensic report writing.

Arguably, forensic reports are the single most important document created in forensic science. These documents represent the culmination of the examiner’s work and are the foundation for the legal use of the results of the examination. The quality of the written report is critical for the examiner’s testimony and her professional reputation. The examiner’s organization is likewise heavily invested in the report, as it “represents” the quality of the entire laboratory and the work of all examiners employed by the organization.

One of the traditional approaches to maintaining the quality of the forensic reports is to conduct reviews of the finished products by both peers and administrators. This process has long been accepted as a best practice by forensics managers and accrediting bodies. It is a process that has been followed for years.

It is therefore ironic that managers and examiners are often frustrated with the report writing and review process. Many managers will complain about the writing abilities of their examiners, but are seemingly unable to teach report writing skills effectively. Further, forensic customers such as investigators, lawyers, and jurists are sometimes critical of the reports provided by examiners. In the digital forensic discipline, this is especially difficult, as the methodologies are complex, the results are often voluminous, and the border between the investigative and the forensic can be fuzzy.

This paper will describe a methodology that has been developed in training both students of forensic science and practicing forensic examiners. The approach will combine a functional and a management approach. The former is focused on defining the structure of the forensic report based upon the forensic objectives and the requirements of the Federal Rules of Evidence. Since an effective peer or administrative review must have an objective standard or “measuring stick” against which to evaluate the report, the development of metrics for this purpose will be discussed. Since there are a great number of digital forensic practitioners who do not operate in traditional laboratories with the ready availability of peers and knowledgeable administrators, this presentation will discuss how reviews can be implemented in non-traditional settings.

Since the goals of peer and administrative reviews are a continuous process improvement, these approaches have application in academic, as well as, initial and recurrent examiner training. The author will discuss his observations of the effectiveness of this approach in training examiners as well as educating students.

Forensic Reports, Quality Management, Peer Review

B2 Quantifying Error Rates of File Type Classification Methods

Vassil Roussev, PhD*, University of New Orleans, Computer Science, 2000 Lakeshore Drive, 311 Mathematics Building, New Orleans, LA 70148

After attending this presentation, attendees will gain an appreciation of the limitations of current file type classification techniques. Attendees will also gain a methodological insight on how to critically examine published work and will learn of new techniques and tools that aid their work.

This presentation will impact the forensic science community by demonstrating how to practically approach the problem of “examining validation and expelling incompetence” for an important area in the field. It is believed that this basic approach readily extends beyond the specific area and has much wider methodological implications.

The problem of identifying the file type of a sample of data arises as part of basic digital forensic processing, such as data recovery and reconstruction, as well as network forensics. Looking ahead, its importance is expected to grow further with the adoption of forensics triage and statistical sampling techniques, which will be increasingly needed to deal (in part) with the rapid growth of target data.

This presentation will discuss both methodological issues not addressed by current work and provide a case study to illustrate the points. Specifically, it will be argued that the current formulation of the file type classification problem is inherently flawed for large classes of file types, such as pdf and doc/docx, and cannot possibly yield informative error rate estimates. Therefore, the problem is re-formulated as two separate problems—primary data format classification and compound data format classification that are independent of each other.

It is also argued that existing studies have been flawed both methodologically and statistically, as the volume of data studied is woefully inadequate to draw any reliable conclusions. This presentation will demonstrate that for some popular storage formats, such as deflate-coded data, the problem of classifying it cannot be based on current statistical approaches and a deeper, specialized analysis, including expectations of the content of the uncompressed data, is a hard requirement.

Finally, a case study will be discussed in which classification techniques were evaluated for some popular primary data formats, such as jpeg and mp3, and quantify their reliability as a function of the sample size. The reliability of compound format detection for pdf and zip/docx formats will be evaluated and a new analytic technique will be demonstrated that can distinguish deflate-compressed data from other types of high-entropy data.

Digital Forensics, Error Rate Estimation, File Type Classification

B3 Psychological Assessments and Attitudes Toward Deviant Computer Behaviors

Marc Rogers, PhD*, 401 North Grant Street, West Lafayette, IN 47907; and Kathryn C. Seigfried-Spellar, MA*, 401 North Grant Street, Knoy Hall of Technology, West Lafayette, IN 47907

The goals of this presentation are to explore whether deviant computer behavior is part of a larger syndrome of deviance. This presentation will examine whether the personality profiles of those
committing deviant computer behaviors are similar to the profiles obtained from those who engage in more general deviance; will examine a potentially unique correlation of deviant computer behavior — Asperger's syndrome; will validate psychometric instruments for use with the "hacker" sub-culture, and to assist digital evidence investigators.

This presentation will impact the forensic science community by providing information related those individuals who are involved in criminal computer behavior.

Surveys indicate that there is an increasing risk of computer intrusion, computer crime and attacks on personal and business information. Computer criminality is a serious problem that affects individuals, businesses, and our nation’s security. In 2008, the Computer Security Institute (CSI) released the findings from their Computer Crime and Security Survey. The survey consisted of 521 respondents, who reported an average cost per financial fraud incident of $500,000. Forty four percent of the respondents also reported that they were victims of insider abuse and twenty-seven percent reported being the victim of targeted attacks. Despite these figures, most work in this area is aimed at devising approaches to protect computer information; very little research has been aimed at understanding why and who commits these criminal acts. The current research adds to this small body of knowledge by examining the motives and characteristics and those involved in deviant computer behavior.

The current study has four specific goals. The first goal is to explore whether deviant computer behavior is part of a larger syndrome of deviance. Much research has shown that non-computer-related delinquent/criminal activities, substance use, and early/risky sexual behavior are typically seen in the same individuals and can be considered part of a larger syndrome of deviance. The first goal of the present project is to ascertain how strongly related deviant computer behavior is to these other markers of deviance. This is achieved by examining the interrelations among measures of delinquency/crime, substance use, early/risky sexual behavior, and deviant computer behavior.

Second, personality profiles are examined to determine whether those committing deviant computer behaviors are similar to the profiles obtained from those who engage in more general deviance. Several meta-analyses have demonstrated that interpersonal antagonism (i.e., lack of empathy, oppositionality, grandiosity, and selfishness) and problems with impulse control are the most consistent personality correlation of a variety of antisocial and deviant behavior. Thus, the second goal of the present study is to compare the personality correlation of deviant computer behavior to what is known about the personality correlations of crime/delinquency, substance use, and early/risky sexual behavior. This goal is achieved by correlating the degree of deviant computer behavior with indicators of five broad-band personality factors derived from basic research on personality and widely-used in studies of deviant behavior. The five factor model employed consists of five broad traits: Neuroticism (vs. emotional stability), Extraversion (vs. introversion), Openness (vs. closedness) to experience, Agreeableness (vs. antagonism), and Conscientiousness/Constraint (vs. lack of constraint).

The third goal is to examine a potentially unique correlation of deviant computer behavior—Asperger’s syndrome. Within the past decade, questions are emerging regarding the possibility of there being a link between computer criminality and a disorder known as Asperger syndrome. Unfortunately, this question has not received the attention from empirical and scientific research that it deserves and demands; no research has been conducted on whether or not there is a relationship between hacking and Asperger syndrome. As computer criminals begin to face our judicial system, the possibility of a link between criminal behavior and this disorder is extremely important, for it could become a legal defense or mitigating factor in a criminal case. In addition, “a diagnosis could alter sentencing . . . [by] assessing the degree of criminal intent.” Due to the lack of research, understanding the true relationship between computer criminals and Asperger syndrome needs to be addressed. Therefore, the goal of the current study is to conduct an extensive comparison and exploration of the relation between computer criminality and Asperger syndrome. This comparison will involve examining relations between a self-reported measure of symptoms of Asperger’s syndrome and measures of computer-related deviance.

The fourth objective is to further validate certain psychometric instruments for use with the “hacker” sub-culture. These instruments have been developed and/or used in previous studies.

Results and future implications of the study’s findings will be discussed.

References:

B4 Cloud Computing and Electronic Discovery: Challenges in Collection of Large Scale Digital Evidence With Internet-Based Storage, Applications, and Infrastructure

Alan E. Brill, MBA*, Kroll Ontrack, One Harmon Meadow Boulevard, Suite 225, Secaucus, NJ 07094; and R.J. Straight, JD*, Kroll Ontrack, Inc., 1166 Avenue of the Americas, New York, NY 10036

After attending this presentation, attendees will understand how the evolution of information processing from traditional storage systems to distributed cloud computing has impacted electronic discovery. Many organizations have transitioned from storing data on its premises to so-called “cloud computing” environments in which data, applications or infrastructure is in remotely dedicated or shared locations accessed through the internet. The increasing reliance on cloud computing has a significant impact on planning and performing electronic discovery in civil actions.

This presentation will impact the forensic science community by reviewing the increasing challenges to the collection of large-scale digital evidence in civil cases caused by the evolving use of internet-based remote computation, storage and infrastructure - commonly known as “Cloud Computing” services.

As more and more organizations make use of various forms of so-called cloud computing (Software as a Service, Internet-based storage, Infrastructure on Demand, etc.) traditional approaches to the collection of information subject to discovery in civil cases will present challenges of increasing complexity to the forensic science community. Ready or not, this is happening, and this presentation will help with an understanding of the challenge and approaches to evolving solutions.

* Presenting Author
In the United States, the Federal Rules of Civil Procedure and similar rules in other countries recognize that various forms of electronically stored information can be vital in civil litigation. But as the technology of the internet has evolved, organizations are processing and storing data not only in their own data centers, but in shared facilities, virtual systems, and increasingly, in storage and processing facilities accessible over the internet.

This presentation will show how these so-called “cloud computing” services affect the process of electronic discovery, from identifying where and how information relevant to the litigation is stored, to how it can be collected from remote sources in a forensically acceptable manner.

Electronic discovery can involve thousands — or even millions of documents. Such volumes, particularly where the data may be in many places and in many forms represents an evolving threat to the ability of the forensic science to keep up with the evolution of information processing.

Electronic Discovery, Cloud Computing, Civil Litigation

B5 Lessons Learned From Teaching a Distance-Delivered Incident Response Course

J. Philip Craiger, PhD, University of Central Florida, Department of Engineering Technology, University of Central Florida, Orlando, FL 32816; Paul K. Burke, BS, Northeastern University, Boston, MA 02115; and Mark Pollitt, MSc, University of Central Florida, University of Central Florida, PO Box 162367, Orlando, FL 32816-2367

The goals of this presentation are to: a) discuss the specific incident response knowledge and skills students are expected to demonstrate; b) compare and contrast the two modes of access, discussing advantages and disadvantages of both methods; and c) discuss a third method under investigation that involves virtualization software running on a server that is accessible over the internet.

This presentation will impact the forensic science community by providing educators and trainers with alternative methods of delivering hands-on, computer-based forensic projects and assignments that require a deal of realism.

Universities are increasing the number of online (distance) courses offered in order to reduce space requirements while allowing increased enrollment, both of which generate more revenue. Experience has taught us that there are courses that do not easily translate into an online format, particularly those that require students to complete hands-on assignments under quasi-realistic conditions in a physical computer lab. Over the last several years, the authors have taught graduate and undergraduate versions of a course in Incident Response that requires students to assimilate concepts from the fields of computer/network forensics and computer/network security. In this course, students learn to identify and address factors related to computer incidents, such as: malware, hacker reconnaissance and exploits, insider access, social engineering, log file interpretation, and combining digital “evidence” to draw conclusions and make recommendations. The capstone project for this course requires students to manage a quasi-realistic ‘live computer incident’ where an external unauthorized user (hacker) has gained access to a ‘privileged account’ and attempts to control the server. Students must investigate the incident on a live, running server, which runs contrary to the “traditional” computer forensics process (pull-the-plug, create a forensic duplicate of the media, perform a forensic examination on the duplicate), but is a situation they may encounter under real-world circumstances.

This is a fairly simple assignment to create and manage provided it is run within a computer lab where a professor can supervise students as they are sitting at a computer terminal working on the problem. The same assignment run under an online class, however, creates issues for both professor and students, including: a) ensuring students can access the server from a distance; b) ensuring students do not cheat; c) ensuring students have sufficient knowledge for the assignment, and; d) providing students sufficient access rights to conduct the investigation, while ensuring they cannot change or delete any important assignment or system files on the server.

Over the years two modes of student access to the ‘victimized’ server were used for the capstone assignment. In the first two-class run, a Linux server was created that was ‘self hacked,’ leaving both obvious and non-obvious signs of unauthorized access and behavior. Each student was provided with an account, and students accessed the server over the Internet using SSH (a secure tunneling protocol). In the second two-class run, virtualization software was used to create a Linux virtual machine that was again ‘self hacked.’ The running virtual machine was then ‘suspended,’ which wrote the state of the running system (i.e., contents of memory, running processes, etc.) to disk. The suspended virtual machine was compressed (zipped) and the compressed file uploaded to the course website. Students could then download the file, uncompress, and run it within the virtualization software running on their own computer.

Incident Response, Online Learning, Distance-Based Learning

B6 Recovering Deleted Evidence From Mobile Devices

Eoghan Casey, MA*, 3014 Abell Avenue, Baltimore, MD 21218

After attending this presentation, attendees will gain an understanding of how to recover deleted evidence from mobile devices and will learn how this evidence has been used in actual cases. Practitioners will learn about the forensic challenges and advantages associated with mobile devices. Researchers will learn about areas that require further exploration to advance the field of mobile device forensics.

This presentation will impact the forensic science community by expressing how the growing number of mobile devices can contain digital evidence, including cell phones, smart phones, and satellite navigation systems. Although some deleted data may be recoverable from these devices, the process can be technically difficult and physically destructive. This presentation presents various approaches to extracting and interpreting deleted data from non-volatile memory on mobile devices and discusses the forensic implications of each approach.

Mobile devices present significant forensic opportunities and challenges. Their ever-increasing prevalence, functionality, and storage capacity make them valuable sources of evidence. Evidence on these devices can include incriminating communications, illegal materials, location-based information, passwords, and other personal data. However, the complexity and variety of mobile devices make it difficult to develop standardized forensic methods for recovering deleted data from non-volatile memory of these systems. Current tools and techniques available to forensic practitioners and researchers for acquiring and examining data from embedded systems are limited to specific model devices and, under most circumstances, not all of the data can be retrieved due to proprietary hardware and software.

To ensure that important evidence on mobile devices is not overlooked, it is important for practitioners in digital forensics to be aware of the potential for recovering deleted data from mobile devices and how this evidence can be useful in an investigation. Digital forensic researchers also need to be aware of the unsolved challenges relating to extraction and interpretation of deleted data from non-volatile memory on mobile devices. This presentation covers various approaches to obtaining and analyzing deleted data from mobile devices, including file system examination and chip extraction. The forensic implications of each approach are discussed, and case examples and research are presented to demonstrate and emphasize key points.

Mobile Device Forensics, Cell Phone Forensics, Digital Evidence

* Presenting Author
**B7  Kernel-Independent Tools for Deep, Live Digital Forensic Investigation**

Golden G. Richard III, PhD*, University of New Orleans, Department of Computer Science, New Orleans, LA 70148

After attending this presentation, attendees will understand the importance of developing kernel-independent, deep analysis tools to support live digital forensic investigations. Existing live forensics tools either perform shallow analysis, relying on the target’s operating system to retrieve data of evidentiary value, or target specific operating system and kernel versions. This limits their usefulness for investigating machines in the wild. This presentation discusses ongoing research in developing deep analysis tools for live forensics, which automatically adapt to different operating system and kernel versions.

This presentation will impact the forensic science community by discussing methods for designing portable live forensics tools that are applicable to a wide range of forensic targets. This work is important because manually developing support for the large number of operating system and kernel versions now widely deployed is impractical.

A number of factors have contributed to an increasing interest in live forensics, where the machine under investigation continues to run while forensic evidence is collected. These factors include a huge increase in the size of forensic targets, increasing case backlogs as more criminal activity involves the use of computer systems, and the need to turn around cases very rapidly to counter acts of terrorism or other criminal activity where lives or property may be in imminent danger. In addition, a live investigation may reveal a substantial amount of volatile evidence that would be lost if only a traditional “pull the plug” investigation were performed. This volatile evidence includes lists of running processes, network connections, data fragments such as chat or email messages, and keying material for drive encryption. All of this volatile information can be crucial in expediting processing of a case, by providing critical contextual information that supplements traditional analysis, such as processing disk images.

Early live forensics efforts typically involved running a number of statically linked binaries on the forensic target (e.g., ls, ps, lsmod, lsof, etc. under Linux) and capturing the output of these commands for later analysis. A physical memory dump might also be captured, but analysis of the physical memory dump was often limited to simple string searches. Recently, research into deeper, advanced techniques has substantially increased the capabilities of live investigation. Physical memory dumps can now be analyzed to reconstruct models of the current and historical states of a live system under investigation. This kind of analysis relies on deep understanding of data structures in the running operating system kernel to extract evidence pertinent to an investigation.

A key problem in developing tools for deeply analyzing live systems is that the format of key kernel structures changes across versions of the installed operating system. This is a problem for both Microsoft Windows and for Linux. For Microsoft operating systems, support is required for Windows NT, 2000, XP, Vista, Windows 7, and the various server offerings, with patch levels (e.g., XP with SP2) introducing even more diversity. For Linux, the problem is much more severe, because official kernel versions are released much more frequently and a large installed base of each version may be present. Furthermore, different distributions, such as Ubuntu, Red Hat, SUSE, etc. may introduce distribution-specific modifications to the kernel. Finally, since the Linux kernel is open source, individual users can modify and install custom versions of the kernel. Linux kernel structures that must be analyzed for deep, live forensics therefore change quite frequently and constantly manually updating tools to support new kernel variants is essentially an impossible task.

Automatic model key kernel data structures, such as process descriptors and process memory maps, regardless of kernel version will be presented. The techniques rely on on-the-spot disassembly of important kernel routines, with pattern matching applied to the resulting disassemblies, to discern the structure of kernel data. This is basically an automatic, on-the-spot reverse engineering effort against important kernel components. A description of the techniques and the live forensics tools built using these techniques will be provided in the presentation. The tools use both list-walking approaches as well as data carving techniques to discover both current (e.g., processes now running, currently open network connections) and historical (e.g., terminated processes, closed network connections) volatile evidence.

**Digital Forensics, Live Forensics, Linux**

---

**B8  Solid State Drive Technology and Applied Digital Forensics**

John J. O’Brien, MA*, United States Army, Cyber Counterintelligence Activity, 4553 Llewellyn Avenue, Fort Meade, MD 20755; and Sean P. O’Brien, BS*, Defense Computer Forensic Laboratory, 911 Elledge Landing Road, Linthicum, MD 21090

After attending this presentation, attendees will understand some principles of digital forensic methodologies when solid state drives are examined; will understand what the differences are compared to traditional rotating media; and will understand what new concepts may be put into operation and which old ones still work.

Solid state drives are becoming more commonplace. This new “old” technology is finding its way into the notebook computer market as well as enterprise systems, and it is important for forensic practitioners to be ready when they first encounter such a drive. This presentation will impact the forensic science community by preparing practitioners for when the first solid state drive hits a forensic lab.

The purpose of this presentation is to learn about the newest solid state drives and the forensic methodologies that may be applied to these technologies and to specifically answer the question: “What unique issues and challenges do solid state drives present to digital forensics?” A solid-state drive (SSD) is a data storage device that uses solid-state memory to store persistent data. Data on the SSD is interpreted by the installed Operating System (OS) and File System (FS) which presents the data to the user. High Proficiency SATA SSDs are being built in both a 2.5” and 1.8” form factors in capacities from 64-300GB. There are two different types of SSD technologies; the SLC (single level cell), and the MLC (multi-level cell) design. MLC doubles the capacity of flash memory by interpreting four digital states in the signal stored in a single cell – instead of the traditional (binary) two digital states. The forensic techniques for the SSDs may differ from those for traditional rotating media. Areas that will be discussed are: forensic tools for working with SSDs, the Flash File System (FSD), the translation and magic that occurs within the chip sets on the SSD to provide the data to the OS and FS for operations, the Host Protected Area (HPA), residual data, wear leveling rules, data streams, data carving, and recovering deleted file data.

**Solid State, Digital Forensics, Computers**

---

**B9  Mobile Device (Cell Phone/PDA/GPS) Data Extraction Tool Classification System**

Samuel J. Brothers, BBA*, 7501 Boston Boulevard, Room 113, Springfield, VA 22153

After attending this presentation, attendees will be able to categorize any mobile device acquisition tool in a systematic classification system. In addition, an overview of all currently available commercial tools for cell phone data extraction will be discussed.

This presentation will impact the forensic science community by providing a common framework for a digital device data extraction tool classification system for the entire digital forensics community.

**Solid State, Digital Forensics, Computers**

---

* Presenting Author
Our world today has been saturated with inexpensive digital devices. These digital devices are used to stay in contact with friends, (e.g., phone calls and text messages) and to help find our way (e.g., GPS devices). These digital devices have become ubiquitous in our society.

Criminals use these devices to aid them in committing crimes, including the use of GPS devices for human and narcotics smuggling to the use of cell phone text messaging to coordinate attacks and communicate orders in organized crime. These devices contain a wealth of information and intelligence for investigators of crimes.

The field of digital device forensics is in its infancy at this time. The digital forensics community needs a framework (common baseline of understanding) for the classification and understanding of the plethora of tools released into the commercial marketplace in the last five years. A lot of false advertising has occurred, and many practitioners in this field are yearning for an understanding of how these tools work.

It is also critical that the practitioners understand how these tools will impact their evidence collection process. This presentation will “peel back the curtain” to allow attendees to see what is going on “behind the scenes” of these tools. Also presented is a framework and classification system for these tools to provide a better understanding for digital forensics practitioners.

**Digital, Forensics, Classification**

## B11 Video File Recovery and Playback of Partly Erased Videofiles

Zeno J. Geradts, PhD*, and Rikkert Zoun, MS, Netherlands Forensic Institute, Ministry of Justice, Laan van IJpengbu 6, Den Haag, 2497 GB, NETHERLANDS

After attending this presentation, attendees will have an understanding of methods of repairing video files in forensic casework.

This presentation will impact the forensic science community by presenting an open source approach for the analysis of image and video files. The use of in digital video is rapidly increasing. Analog CCTV systems are replaced by digital systems, digital cameras are increasingly popular and affordable, many mobile phones now come equipped with a camera, and high-bandwidth internet allows home users to share their recordings and download video material in larger quantities than ever before. When digital video content is an important part of case evidence, such as in cases of recorded child pornography or other recordable crimes, finding every last bit of video data and making it viewable can be crucial to the investigation.

This is not always as easy as simply searching the data carriers using regular operating system functionality. Deleted files can usually be found with typical forensic software, if they are not yet overwritten and still reside intact on an undamaged data carrier. In some cases, however, the deleted video files may be partly overwritten or file systems may be damaged, leaving the investigator only with fragments of files.

Recognizing such fragments and rebuilding them to valid files that can be viewed using video playback software requires thorough knowledge of file format specifications and laborious manual data editing. Many digital forensic investigators lack the time to get into such details.

Netherlands Forensic Institute developed Defraser (Digital Evidence Fragment Search & Rescue), an open source software tool to help the investigator by searching for video file fragments and analyzing their integrity. It allows drag-and-drop combining of video file elements to create playable video files. The tool is plug-in-based, allowing users to store and share their knowledge of particular file formats by programming their own plug-ins.

The product can be downloaded including sourcecode from http://sourceforge.net/projects/defraser. This tool was developed open source, so that other people can write plug-ins, and also if other software engineers would like to review the code, this possibility exists, since it is not a black box approach. It can also be implemented in other products, since it is written under BSD license. Also other users with proposals for changes can submit these changes, and they will be implemented.

Within defraser, plug-ins for MPEG-1, 2 & 4, 3GPP/QuickTime/MP4 and AVI are implemented, and new plug-ins

---

* Presenting Author
are developed based on casework. The user can also develop their own plug-ins with .net and C#. Examples are provided as reference.

The defraser tool could be developed further, with more plug-ins for other image and video file formats such as JPEG, ASF, FLV and Matroska. Forensic logging: trace results to source evidence files (using hash), and tools to automate the analysis. The tool can be used on large images of unknown data, to extract relevant video data. Since the tools also tries to visualize partly erased video, false hits might occur, and further analysis is necessary. In this presentation some examples will be presented in casework where repair was necessary, and this tool was useful for analysis.

**Defraser, Video Streams, Recovery**

**B12 Calibration and Validation of Videographic Visibility Presentations**

**Thomas Ayres, PhD*, 101 Kensington Road, Kensington, CA 94707**

The goal of this presentation is to review the history and current status of calibration and validation techniques for forensic visibility presentations. Attendees will learn what steps can be taken to ensure a technically defensible approach to capturing and presenting scene visibility tests, as well as, the results of a study that can support the use of such tests.

This presentation will impact the forensic science community by presenting details of the findings as well as recommendations for forensic applications of videographic visibility tests. These results add to the technical foundation for introduction of such images in courtroom settings.

In order to capture and demonstrate visibility of crucial aspects of an accident scene or reenactment for forensic purposes, there must be some means of ensuring that the final image corresponds in a known way to the original viewing conditions. Careful photographic or videographic capture, e.g. from a known position of interest and with lighting similar to the time of the incident, is an essential first step, but it is also necessary to have a procedure for calibrating and validating the image.

Throughout the past several decades, there have been two primary approaches used for such calibration and validation. One involves direct comparison of an image with the scene itself; the use of Polaroid® photos for this purpose has largely given way to viewing static video images on a monitor. In this approach, one or more viewers compare what they see in the scene ahead to what is visible in the photos or monitor, and select photos or adjust the images to match crucial aspects of scene visibility. The other common approach involves the use of stimuli introduced into the scene, generally contrast charts; viewers record their observations of the charts at the scene, and then later select or adjust final images to provide the same level of chart visibility as at the scene.

Further validation of the final images can be obtained by comparing what a group of viewers detect and notice in the scene to what they detect and notice in the images. In forensic applications, it is usually not practical to have more than a few people involved in a site visibility test. This presentation will describe a study conducted specifically to determine the success of current videographic calibration and validation techniques. Test subjects were brought to view a night roadway scene that had been calibrated by adjustment of the monitor at the scene and validated based on observations of a contrast test chart. Comparison of scene and videographic visibility results demonstrated the utility of the techniques.

Details of the findings as well as recommendations for forensic applications of videographic visibility tests will be presented. These results add to the technical foundation for introduction of such images in courtroom settings.

**Visibility, Videography, Contrast Detection**

**B13 Utility of Quantization Tables for Digital Image Authentication**

**Amanda E. Broyles, MAM, Federal Bureau of Investigation, Building 27958A, Quantico, VA 22135; and Richard W. Vorder Bruegge, PhD*, Federal Bureau of Investigation, OTD-FAVIAU, Building 27958A, Pod E, Quantico, VA 22135**

After attending this presentation, attendees will understand what a JPEG quantization table is, how they differ among manufacturers, and how this information can be used in image authentication examinations. This presentation will impact the forensic science community by reinforcing the value of metadata analysis in digital image authentication and providing another avenue through which claims of image manipulation can be addressed.

The process of digital image authentication usually incorporates an assessment of the metadata contained within the digital image file. This can include information on the make and model of the camera used to take a picture, as well as other information such as date and time or camera settings like shutter speed, aperture, or image size (in pixels). This type of metadata often serves to provide circumstantial evidence regarding the source of a questioned image. For example, if image files depicting child pornography are found on a suspect’s computer and the files contain metadata indicating the same make and model as the camera found next to the computer, then this provides compelling evidence that the camera was used to record those image files. Likewise, if the time and date indicated in the metadata correspond to a time when the suspect had access to the camera and victim, this provides additional circumstantial evidence. The mere presence of camera metadata in a digital image file is often cited as support for the authenticity of the file and the scene depicted therein.

However, because there is the potential that such metadata can be falsified (or “spoofed”), the value of such analysis in these cases may be limited, depending upon the specific type of metadata in question. For example, it is a relatively straightforward process to manually modify the time and date metadata using a hex editor, while leaving no trace of this modification. On the other hand, other types of metadata may be very difficult to falsify. This paper addresses one such type of metadata – JPEG quantization tables.

Quantization tables are used to define the amount of compression an image file will undergo when subjected to JPEG compression. A quantization table includes a total of 192 values, broken out into three sets of 64 values. The first set affects the luminance of the image, while the second and third sets affect the chrominance. When a digital camera user selects an image quality setting such as “Fine,” “Normal,” or “Basic,” they are typically selecting a specific quantization table that has been predefined by the camera manufacturer. In some cases, the manufacturer will also use a different quantization table for images of different size (or resolution). Based on an analysis of approximately 200 cameras, Farid suggested that the quantization table could be used to narrow the source of an image to a small subset of camera makes and models. Subsequently, after examining 1,000,000 images, Farid identified a total of 10,153 combinations (“classes”) of camera make, model, resolution, and quantization table. The fact that a given camera make and model can generate files of the same size with different quantization tables typically reflects variations in the quality setting. Therefore, in order to completely spoof a digital camera image, the manipulated file must also include the correct quantization table.

The work described in this paper extends the analysis of quantization tables contained in digital images to the “thumbnail”
images included within many digital image files. “Thumbnail” images are reduced size versions of images that are used for ease of display either on a camera monitor or within a computer browser. They are complete digital image files in and of themselves, so they can have their own quantization tables. As a result, digital camera image files can have more than one set of quantization tables—one for the thumbnail and one for the full size image. The quantization tables for the full size image and the thumbnail image usually are different, which means that any spoofing attempt must utilize two quantization tables, making it more difficult.

Further complicating spoofing attempts is the fact that one cannot simply modify the quantization tables using a hex editor, since this can result in dramatic modifications to the image quality. Likewise, commercially available image processing applications such as Adobe® Photoshop® will typically utilize a small set of quantization tables that differ from those of camera manufacturers, meaning that any manipulated image will have to be reprocessed outside of Photoshop® to create a falsified quantization table if the proper quantization tables are to be generated. Finally, additional properties of thumbnail images generated by digital cameras as opposed to image processing will be described, such as size, orientation, and framing.

References:

Digital Image Authentication, Digital & Multimedia Sciences, Image Manipulation Detection

B14 Identification of Cameras With Photo Response Non-Uniformity (PRNU) in Large Databases

Zeno J. Geradts, PhD*; and Wiger Van Houten, MS, Netherlands Forensic Institute, Ministry of Justice, Laan van IJenburg 6, Den Haag, 2497 GB, NETHERLANDS

After attending this presentation, attendees will be aware of the possibilities of linking a certain image to a specific camera in larger databases.

This presentation will impact the forensic science community by discussing validation of techniques in large scale databases.

Photo Response Non-Uniformity pattern is a unique sensor noise pattern that is present in all the images and videos produced by a camera, as it originates from intrinsic sensor properties.

This sensor noise pattern acts as a fingerprint, and this fingerprint essentially represents the deviation of each pixel with respect to the average pixel response at uniform illumination. This noise pattern is a stable pattern, which makes it a good candidate for linking a certain image to a certain camera. In each case validation is needed to determine if the patterns are really random, which means the creation of flat field images from at least ten cameras of the same make and model. Flat field images are images taken from a gray surface where no edges are visible.

Indeed, large scale testing on photo cameras has shown that it is possible (with low false acceptance and false rejection rates, or a high likelihood ratio) to identify the source camera based on the patterns that were extracted from images. In general, the amount of compression present in photos is much less severe than what is encountered in videos, especially if they originate from webcams or mobile phones.

The compression effectively acts as a low-pass filter, thus removing or attenuating the PRNU pattern. Another problem is that these devices have in general a much lower resolution and visual inspection already signifies the high amount of compression artifacts present. On the other hand, multiple frames are available from which an average noise pattern can be calculated, which alleviates some of these problems.

Also, these low-cost devices may have a stronger PRNU pattern compared to full size digital cameras, which adds to the feasibility of identification. Previously seen in small scale tests that under certain conditions it is also possible to correctly identify the source video camera, even for heavily compressed webcam videos obtained from YouTube. It is expected that these low quality webcam videos behave similar to videos shot with mobile phones, and hence may also be very useful in a forensic context.

For testing PRNU on larger databases a framework for comparison has been developed, which is open source and can be downloaded from http://sourceforge.net/projects/prnucmpare/.

One of the problems encountered with these low quality cameras is that these compression artifacts (seen as square DCT blocks in the extracted patterns) cause high correlations to occur between unrelated cameras. This stresses the need for large scale testing. However, large scale tests are tedious to perform, mainly due to the low calculation times needed for extracting the noise pattern from the videos, and the lack of online video databases with known source (similar to Flickr for photos). With the advent of an online pattern database, there is hope to overcome both these problems. This allows larger scale testing, and hopefully the ability to make predictions about the reliability of the method applied to these low resolution cameras in practice.

In forensic reports, the error rates of the method are also considered, and will conclude within the Bayesian approach.

Photo Response Non-Uniformity, Likelihood Ratio, Camera Identification

B15 An Alternative Method for ENF Data Analysis

William L. Hinton, BS*, Kenneth Marr, MS*, and David J. Snyder, BS*, Federal Bureau of Investigation, Engineering Research Facility, Building 27958A, Quantico, VA 22135

After attending this presentation, attendees will understand current ENF (Electric Network Frequency) analysis techniques for use in the area of digital and multimedia evidence (DME). ENF analysis attempts to detect, analyze, and evaluate embedded power line information that occasionally is recorded on analog and digital recordings. An alternative method to record ENF data will be presented and assessed for accuracy and suitability.

This presentation will impact the forensic science community, especially the sub-disciplines of forensic audio, video, and image analysis, by showing an alternative method available for ENF analysis. Cautions concerning the resolution and accuracy of ENF analysis will provide the DME practitioner with important Daubert and Frye testimony information.

Hypothesis: An alternative method to evaluate ENF (Electric Network Frequency) data can be accomplished using single-purpose power logger instruments.

Synopsis: Single-purpose power logger instruments were used to compile archive ENF data in the Eastern Interconnect grid of the United States. Comparison of simultaneous power logger and audio recordings showed that pattern matches depend on the resolution selected of the data.

Forensic audio examiners are evaluating the suitability of using ENF information that is occasionally embedded on analog and digital recordings. The goal of the analysis is to match the ENF pattern of
embedded power line information found on evidence recordings to the ENF patterns archived from electric power grids. Potential shortcomings in data resolution, database collection and custody, and the searchability of ENF databases have not yet been resolved. This paper presents an alternative method to collect, store and evaluate ENF data in the eastern grid of the United States.

In the past, power line information (50/60 Hz hum and harmonics) on evidence recordings has been used in audio signal analysis and authenticity examinations. This information can assist audio examiners to correct the speed of recordings and to indicate areas of possible recording alterations when an interruption in the power line hum is detected. The analysis of ENF information using pattern matching is a recent focus in forensic audio research. ENF analysis attempts to match the power line hum pattern on evidence recordings to a hum pattern archived in databases of previously recorded electric grid information. This paper describes the results of test recordings to collect ENF data in Virginia (the eastern interconnect grid of the United States) using stand-alone, single-purpose instruments, AEMC Power Quality Loggers, Model PQL 120. This type of instrument measures and stores the electric power information directly with a frequency resolution of 0.01 Hertz. Power Loggers are plugged directly into wall sockets and sample electric grid parameters, including voltage, current, frequency, and power.

This paper describes the characteristics of Power Loggers and their suitability for analyzing ENF grid information. Test data indicates that there is a distinct trade-off between data accuracy and pattern matching. At the highest resolution of test data gathered, the data from multiple loggers in the same building indicates differences in simultaneous recordings. This result is contrary to previous ENF test results which claim that simultaneous ENF recordings on the same electric grid always match. Data was recorded simultaneously on three power loggers during an audio recording on which ENF power line hum was intentionally recorded. The first comparison analysis evaluated the power logger data resolution needed to uniquely identify a known recorded interval with the same pattern in the power logger database. The test results indicate that multiple pattern matches can occur as the data quality is reduced.

Tests were then conducted with simultaneous power logger recordings and known audio recordings that have 60 Hz induced interference coupled into the audio recording. Comparison analysis was made of the power logger data with the known audio recording. Additional tests were conducted which compared the Logger data with intentionally altered known audio recordings. The results indicate that a trade-off must be made between desired resolution and successful matches of ENF patterns. This evaluation to detect known interruptions in audio recordings is an ultimate goal of ENF analysis. Test results indicate that power line interruptions can be made without detection. In addition, the power logger data will be used to calculate this method’s ‘error rate’ for Daubert hearing purposes.

These results indicate data incompatibility can exist between power line hum information derived from audio evidence and that archived using data collection methods not designed for the analysis of power line hum information. Another result of this analysis is highlighting the importance of conditioning the data. Successful ENF analysis to date has used traditional data conditioning techniques (resampling and filtering) in order to have compatible data patterns for analysis. This data conditioning can have unknown effects for ENF data analysis.

Audio, ENF, Data Analysis

B16 Building a Database of Electric Network Frequency Variations for Use in Digital Media Authenticity

Jeffrey M. Smith, MSc*, National Center for Media Forensics, 1800 Grant Street, Suite 230, Denver, CO 80210

After attending this presentation, attendees will become familiar with the fundamental principles behind utilizing the variations in the Electric Network Frequency to authenticate digital recordings and the approach the National Center for Media Forensics has taken to create a database of ENF variations for the Western United States.

This presentation will impact the forensic science community by providing an overview of a new technique in authenticating digital audio and discussing the current research on this subject underway at the National Center for Media Forensics.

There is great need for research in the area of forensic media authentication with regards to digital audio. Tools used in authenticating analog tapes do not apply in the digital domain where sophisticated criminals are capable of seamlessly editing evidence. One proposed tool that is currently undergoing a fair amount of research and has been presented in European courts is the extraction of the Electric Network Frequency (ENF) component of a digital recording in order to authenticate it and perhaps even obtain a time-stamp. When this tool is successful, a forensic investigator is capable of locating edits, identifying the broad geographical area in which a recording was made, accurately assessing the date and time a recording was made, whether the recording is an original or copy, or if it is the result of two audio files being combined or mixed together.

However, for this application to reach its potential, a database of Electric Network Frequency variations for each grid must be available. For the United States, these grids include one for the Western United States, one for the Eastern United States, and one for Texas. It is possible for one to obtain this information from the local power company but for this data to be readily available and easily analyzed, a custom database must be recording ENF variations twenty four hours a day, seven days a week, three hundred and sixty five days a year. The National Center for Media Forensics is currently maintaining a database covering ENF variations for the Western United States and has plans to implement databases in other parts of the country as well. The analysis of this database involves generating a low sample rate waveform from data collected directly from a power outlet. This waveform can then be spectrally analyzed for pseudo-random variations and compared to field recordings exhibiting a strong ENF component.

In this presentation examples will be shown to demonstrate the application as well as proposed methods regarding its use. Following this brief introduction, elaboration on current research trends including those at the National Center for Media Forensics where a database of the distributed power grid covering the western United States is collecting data twenty four hours a day for potential use in media authentication and time stamping recordings of unknown origin. A review of relevant literature that relates to this topic will be given in addition to proposed areas in need of research. A scenario in which recordings originating in either the continental United States or Canada can be authenticated and/or time stamped for use in forensic applications will be described. This involves at least one database in each of the three grids covering these countries. In addition to establishing these databases, refinement in techniques regarding ENF extraction, analysis, and comparison must be undertaken in order for this tool to reach its full potential.

Audio Forensics, Digital Media Authentication, Electric Network Frequency

Audio, ENF, Data Analysis
The Digital Forensics Certification Board: Its History and Future

Carrie M. Whitcomb, MSFS*, National Center for Forensic Science, University of Central Florida, PO Box 162367, Orlando, FL 32816-2567; Zeno J. Geradts, PhD*, Netherlands Forensic Institute, Ministry of Justice, Laan van Veenenburg 6, Den Haag, 2497GB, NETHERLANDS; Robert T. Lee, MBA*, Mandiant, 675 North Washington Street, Suite 210, Alexandria, VA 22314; Marcus Rogers, PhD*, 401 North Grant Street, West Lafayette, IN 47907, and Eoghan Casey, MA*, 1101 East 33rd Street, Suite C301, Baltimore, MD 21218

After attending the presentation, attendees will understand the evolution of the Digital Forensic Certification Board (DFCB), become aware of the application process, will understand the value of professional certification, and will understand it is community driven.

This presentation will impact the forensic science community by discussing how the Digital Forensic Certification Board was able to respond immediately to one area that the National Sciences Academy February 2009 Report’s found lacking, which was the need for certification programs. The DFCB launched their certification program for digital forensics practitioners and managers on March 2, 2009.

Professional certifications in digital forensics are something the community has needed for years and it is now a reality. The Digital Forensics Certification Board (DFCB) professional certifications are truly independent and community driven. The DFCB certification program was developed with National Institute of Justice (NIJ) funding. The terms for the development of this certification program by consensus were followed. The DFCB will eventually be applying for recognition by the Forensic Specialties Accreditation Board (FSAB), which is currently recognized by the American Academy of Forensic Sciences.

There are (2) types of forensic certifications offered: Digital Forensic Certified Practitioner (DFCP) and the Digital Forensic Certified Associate (DFCA). The Founders process offers those, who have been active for years in the digital forensic discipline the opportunity to become certified by demonstrating expertise and experience. Once the Founders process concludes, those seeking certification will be required to sit for a comprehensive exam.

DFCB, Professional, Certification

Changes in Approach for Scalability in Digital Forensic Analysis Emphasizing Distributed, Collaborative, and Automated Techniques

Brian Roux, MS*, 701 Poydras Street, Suite 150P, New Orleans, LA 70065

After attending this presentation, attendees will understand the difficulties currently faced in digital forensics, the mounting problem increasing storage capacities pose for the field, the failings inherent in current generation digital forensic tools’ approach to analysis, the necessity of adopting a collaborative and staged approach to analysis, and see an example of how a new such approach can be implemented to address these problems.

This presentation will impact the forensic science community by proposing a more scalable architecture for digital forensic analysis and exposing failings in current generation practices as they relate to time constrained scenarios.

Digital forensics is traditionally performed using “dead” analysis where storage devices are imaged for later processing while the device is in an off state. Modern digital forensics is moving toward the employment of “live” analysis techniques for memory capture, among other things, prior to power off or solely live techniques in cases where systems cannot be powered down. The former approach requires extensive time for thorough analysis and the later requires highly skilled individuals able to deal with unexpected situations arising from live analysis where malicious content could be triggered. Both practices require finite resources: time and expertise.

In a criminal setting the expanding need for immediate triaging of devices is beginning to be articulated as backlogs expand. In England, for example, the Association of Chief Police Officers is searching for a system to act as a “digital breathalyser” to deal with evidence backlogs approaching two years in some areas. The United States has had a number of high profile cases dealing with laptop searches at border crossings with the methodologies exposed painting a haphazard picture of their practices.

Modern digital forensic tools, both commercial and open source, employ a single user paradigm wherein the evidence, once acquired, is worked on in an individual workstation context. The prevailing approaches are also pointed toward analysis in the lab rather than in the field. This design fails to apply modern advances in distributed and high performance computing to speed analysis, and is overly reliant on static features rather than allowing for dynamic insertion of automated processes into the analysis.

Reconstruction of the forensic process is proposed as a staged approach using a pipelined system for the automated portion of analysis. The proposed process treats forensic data as a server centered, rather than workstation centered, resource. By centralizing control over the forensic data, information can be used by multiple systems in tandem. In the example presented, a triage stage takes files from the loaded disk image and distributes them to processing nodes which push the read data through an expandable pipeline of automated processes including file hashing, text extraction, indexing, file type identification, etc. Experimental results show a significant decrease in processing time versus the traditional single station approach.

This distributed approach also allows for node specialization for dealing with proprietary data types requiring specialized or in-depth second pass processing such as extracting individual emails from email stores or performing cross analysis of multiple systems for similarities. Post-triage stages can continue using automated processing while making previous stage data available for one or more analysts to examine allowing preliminary reports to be generated before the data is completely processed. Likewise, limited preliminary analysis can be performed in the field during acquisition or initial inspection with that information integrated with the triage stage.

An initial overview will be presented of the prototype “Black Friar” framework which implements the staged approach to forensic analysis with performance results. Results will be followed by examination of the future development road map as an implementation of the staged forensic approach with special emphasis placed on the flexibility open source frameworks for forensics provide for analysts to integrate new tools into the process. After becoming “production ready” Black Friar will be available as an open source digital forensic tool.

It is recommended attendees be familiar with current generation digital forensic practices, have a working knowledge of file systems and common file types, and some understanding of distributed computing, distributed file systems, and general concepts in high performance computing.

Digital Forensic Analysis, Distributed Processing, Digital Forensic Frameworks
B19 Forensic Data Extraction in Computer Child Pornography Investigations

Sigurd Murphy, BA*, Defense Computer Forensic Laboratory, Linthicum, MD; Donald P. Flynn, JD, Defense Cyber Crime Center, DC3, Linthicum, MD; Thomas J. McAleer, Defense Computer Forensic Laboratory, Linthicum, MD; Andrew Medico, BS, Defense Cyber Crime Institute, Linthicum, MD; Daniel Raygoza, Defense Computer Forensic Laboratory, Linthicum, MD; and Michael J. Salyards, PhD*, U.S. Army Criminal Investigations Laboratory, 4930 North 31st Street, Forest Park, GA 30297

After attending this presentation, attendees will understand the unique technical, legal, and investigative challenges in child pornography investigations, learn about the key forensic steps in conducting an automated examination, and understand the importance of a user-friendly display.

This presentation will impact the forensic science community by explaining how forensic data extraction is a powerful tool that could revolutionize the way digital evidence is examined primarily in child pornography investigations and possibly in other types of offenses.

This presentation will describe a new and powerful model for examining digital evidence in child pornography examinations. Child pornography introduces three challenges. First, anecdotal reports from local, state, and federal laboratories show that the sheer numbers of cases and volume of media associated with child pornography overwhelms most digital evidence laboratories. Second, computer forensic examiners are often asked to make determinations outside of their expertise like medical determinations (especially about the age of children in digital images) and legal determinations about whether the content of a picture of document contains pornographic material. Finally, examiners are burdened with lab requests that ask for “all information about all files.” These types of examinations can take 3-9 months to complete, and often contain detail that is neither understood nor used by customers in the investigative and legal communities.

Forensic Data Extraction (FDE) was designed to meet these challenges and consists of four key elements. First, a robust extraction tool uses commercially available forensic software tool to search cases for images, videos, Peer-to-Peer file sharing logs, email messages, internet chat logs, and web browser history. The tool searches both allocated files and unallocated space, and automatically looks inside compressed files. Operating system and application files are eliminated using the NIST NSRL. This step is performed in a highly efficient machine-driven manner that was designed to be run in a massively parallel operation.

Second, all of the recovered files are stored in a database with their associated metadata (original path, size, last modified time, etc). MD5 hashes are computed for each recovered file so that files can be matched against lists of known child pornography files. Images and videos not found in the known files list are ranked by an algorithm that judges human (flesh) content. In addition, thumbnails of videos are generated after skipping past opening title/credit screens so the investigator can easily see a preview of the content of the video.

Third, a highly robust and user-friendly front end allows for easy viewing, sorting, and classification of the files by the investigative, medical, and legal communities. Known child pornography files and files that are known to be transferred via peer-to-peer (P2P) software are grouped together and highlighted. The remaining images are sorted by human content rating so that the investigator can view more likely files first. This front is delivered inside of a mini virtual machine to facilitate support for the largest possible set of customer machine configurations.

Finally, a follow-up mechanism allows the customer to quickly and securely request that a follow-on examination be conducted in a manner that they control. This technique marries files selected by customers with the back-end database to allow for timely follow-up examinations on files of interest.

This model results in dramatic increases in productivity and timeliness while simultaneously allowing the customer to maintain an increased amount of control over their casework. Unexpected benefits include increased guilty pleas, identification of additional victims and acceptance of the customer front end by the judicial community. Details will be presented about how FDE works, statistics showing the effects on productivity and some noteworthy case examples.

Digital Evidence, Computer Forensics, Child Pornography

B20 Challenges for Digital Forensic Acquisition on Virtualization and Cloud Computing Platforms

Christopher W. Day, BS*, Terremark Worldwide, Incorporated, 2 South Biscayne Boulevard, Suite 2800, Miami, FL 33131

After attending this presentation, attendees will understand the issues involved with acquiring digital evidence from virtualization systems such as VMware and Xen-based systems, as well as so-called “cloud computing” platforms that rely on these technologies to provide organizations and users with highly-scalable and distributed computing capabilities. Attendees will learn how virtualization systems work and the particular challenges they pose to the forensic investigator. In addition attendees will learn about the most common types of cloud computing platforms and how each introduces additional challenges for the investigator above and beyond those presented by virtualization technologies.

This presentation will impact the forensic science community by providing practitioners with a primer for these increasingly common but to many practitioners, still mysterious, technologies and platforms that they will likely be asked to perform forensics acquisitions and investigations on in the near future. This presentation will also present some practical techniques and procedures practitioners can utilize in their work with these systems.

Given the theme of this year’s conference, it seems fitting to examine the technology of virtualization and one of the primary emerging applications of this technology, cloud computing, and the challenges these will present to digital forensic investigators now and in the near future. Various estimates and projections point to an increasing use of cloud computing platforms now and in the near future, some indicating as much as 30% of corporate information processing will take place on some form of cloud platform by 2011. In any case, forensic investigators will need to have an understanding of the technologies involved, the different types of cloud platforms likely to be encountered and what acquisition and investigation challenges they are likely to encounter. Most importantly, investigators must have an established, tested, and accepted methodology for performing evidence acquisitions and investigations on these platforms. One methodology the author is working on in conjunction with the FBI will be presented as an example.

Digital Forensics, Virtualization, Cloud Computing

B21 Virtualizing the Computer Forensic Examination Platform

Brian D. Nunamaker, BS*, Drug Enforcement Administration, 10555 Furnace Road, Lorton, VA 22405

After attending this presentation, attendees will learn how to implement a virtualized examination platform to conduct computer forensic examinations. Attendees will also have a greater knowledge of the advantages and disadvantages of this configuration.

This presentation will impact the forensic science community by showing how a computer forensics laboratory implemented a virtualized...
B22  A Baseline for XP Boot Changes

Benjamin R. Livelsberger, BA*, National Institute of Standards & Technology, 100 Bureau Drive Stop 8970, Gaithersburg, MD 20899-8970

After attending this presentation, attendees will become familiar with a baseline of what changes take place to the volumes of a Windows XP system on boot.

This presentation will impact the forensic science community by discussing how an accidental boot to a computer's host operating system is a serious error for a forensic investigator, but understanding the changes that occur when a system boots can mitigate resulting damage.

The behavior of the Windows XP SP2 operating system installed to a FAT32 volume was studied. The operating system was installed and the research was done in an isolated environment. No additional programs were installed, but "user files" were copied to two secondary volumes. Over the course of five boot cycles, before and after images were made of the system. The images were then compared for differing sectors and differences were analyzed using the Sleuth Kit digital investigation tools.

Over the course of five boots and shutdowns of a generic Windows XP system little or no change was made to the secondary volumes, but an average of close to 13,900 sectors changed on the system's boot volume. Changes occurred in each of the boot volume’s reserved, FAT, and data areas. On each cycle the reserved area’s FS Info sector changed and for each cycle between two and five sectors of the FAT 0 table and between two and five sectors of the FAT1 table changed.

Between 12,501 and 14,827 sectors changed in the data area on each boot. Most of these sectors represented changes to allocated file content. On average, the content of 34 system files changed with the range being 32 - 36 files. A core set of 31 files had content change in each of the five boot cycles. 96% of the changes to file content were to the PAGEFILE.SYS and SYSTEM files (the page file size was 2GB). In general, sectors weren’t de-allocated, but on each boot a small number of previously unallocated sectors (averaging around 170, but ranging from 20 to 633) did become allocated.

In the boot volume’s data area, in addition to changes to file content and to allocation status, a small number of sectors containing directory entries (file metadata) differed after each boot cycle. For one of the boot cycles, the access times for 497 entries changed, but for the remaining four cycles no access times were altered. Changes to write date and time values were more consistent. On average 54 directory entries had their write date and time values updated with a range of 52 to 55 directory entries. A core set of 51 of those directory entries changed consistently in each of the five boot cycles. Four to seven entries consistently had their size values changed. A set of four of these entries had their size values altered in every cycle and on each cycle eight new directory entries were created.

Having an understanding of the nature of how a system changes on boot and having a baseline for those changes allows the investigator to begin and to defend the examination of an inadvertently booted system.

Boot, Filesystem, FAT32

B23 Tips & Tricks for the Analysis and Harvesting of Data From Macintosh Computers

Jessica J. Reust Smith, MFS*, Stroz Friedberg, LLC, 1150 Connecticut Avenue, Northwest, Suite 200, Washington, DC 20036

The goal of this presentation is to show attendees what they can do to avoid some of the forensic pitfalls caused by the occasional foray into the forensic analysis of Macintosh computers. In addition, attendees will learn forensic examination techniques for extracting valuable evidence from Macintosh computers, drawn from both applied research and actual investigations.

This presentation will impact the forensic science community by describing tips and tricks for digital forensic examiners when approaching both the forensic analysis of Macintosh computers in investigations and the harvesting of data for counsel review and discovery obligations.

As the market share of Macintosh computers rises, they are turning up in increasing numbers in forensic investigations of both civil and criminal manners. However, when compared to their PC counterparts, Macintosh computers usually present additional challenges to the digital forensic examiner due to the nature of their file system and operating system and the analysis tools available.

There are a number of different software programs available to facilitate the examination of Macintosh computers, and it is important for the examiner to understand the strengths and weaknesses of the tools...
they use so as not to overlook important evidence or data. This presentation will show attendees what they can do to avoid some of the forensic pitfalls caused by the occasional foray into the forensic analysis of Macintosh computers. In addition, attendees will learn forensic examination techniques for extracting valuable evidence from Macintosh computers, drawn from both applied research and actual investigations.

**Macintosh Computers, E-Discovery, Digital Forensics**

**B24 A Forensic Analysis of a Vista 64 Hard Drive**

Marc Rogers, PhD, 401 North Grant Street, West Lafayette, IN 47907; Katie Strzempka, BS*, 3708 Sweet Valley Lane, Apartment A1, Lafayette, IN 47909; and Eric Katz, BS*, 2099 Malibu Drive, West Lafayette, IN 47906

After attending this presentation, attendees will have the tools and knowledge necessary to view evidence and other data stored in Microsoft Vista's Shadow Volumes.

This presentation will impact the forensic science community by communicating one potential way of analyzing Vista Shadow copies and viewing a Vista 64-bit hard drive using a virtual machine.

Sixty-four bit processing may be revolutionary for computing, but can create a hassle for computer investigators. This is especially true in departments without the funding to afford a new 64 bit PC. Criminals rarely face the same limitations. Vista tries to help its users by offering a function called Shadow Copy that creates restore points to recover files as they were. Shadow Copy is a wonderful tool, but in some Vista versions, such as Home Premium, the user has no access to the Shadow Copy. For investigators this means that the Shadow Copy is there and files may be present in it, but there is no easy way to access or restore from it. What happens when an investigator must look at a Vista 64 bit machine and restore the Shadow Copy volume and all that is available are 32 bit computers?

The case discussed in this paper addresses these exact issues. Illegal images were known to be on the suspect's hard drive, but were inaccessible. Several methods were utilized to access the files within the shadow volume and the combination of some of these methods proved to be successful and forensically sound.

**Vista, Shadow Copy, 64 Bit**

**B25 Indication of CD Burning by Detailed Examination of SMFT: A Case Review**

Douglas Elrick, BA*, Digital Intelligence, 17165 West Glendale Drive, New Berlin, WI 53066

After attending this presentation, attendees will be able to examine a Windows based computer or evidence that files have been burned to an optical disc.

This presentation will impact the forensic science community by providing new sources of potential evidence in digital investigations.

One of most common case scenarios in computer forensics is one in which an employee leaves a company and is suspected of taking intellectual property to a competitor. Examiners are routinely asked to analyze the work computer and look for file activity prior to the employee’s departure, what external storage devices have been attached, what files have been attached to emails, and if any files have been burned to a CD or DVD disc. The first three requests are fairly straightforward to complete but the detection of files that have been burned to disc has been difficult to determine. Thousands of files and gigabytes of proprietary information can be absconded with few methods for detection.

In a recent case, several hundred documents were found to have been last accessed just prior to the employee leaving. Not all the files in a particular subfolder were accessed which suggests a selective process and not an automated routine. Further examination revealed that the NTFS entry modified date and time was also updated within seconds of the last accessed time. Test burning of files through Windows XP SP2 revealed similar date and time results with the last accessed date and time and the entry modified date and time.

Through a detailed examination of the SMFT, clues are revealed indicating that files have been burned using the Windows operating system. Testing has shown that this detection can be accomplished for Windows XP through Windows 7 beta. A thorough understanding of the SMFT record structure including file attributes, record headers and record slack is needed for recognition of these indicators.

This presentation will demonstrate the artifacts left behind by which the Windows CD Burning process. While the evidence found is not conclusive that particular files and folders have been stored on optical disc, the artifacts found will provide strong indicators.

**CD-Burning, MFT, File Attributes**

**B26 Testing Tools to Erase Hard Drives for Reuse**

James R. Lyle, PhD*, and Craig Russell, MS, National Institute of Standards & Technology, 100 Bureau Drive Stop 8970, Gaithersburg, MD

After attending this presentation, attendees will be made aware of some of the issues used in testing computer forensic tools used to erase hard drives before reuse of the hard drive.

The presentation will impact the forensic science community by increasing awareness in the community of the tool behaviors and limitations likely to be encountered when using tools to prepare digital media for reuse between cases.

The Computer Forensics Tool Testing (CFTT) project at the National Institute of Standards and Technology develops methodologies for testing computer forensic tools. A methodology for testing tools was developed that erases entire hard drives. Digital media used in the processing and analysis of digital data is often reused between cases. Good practice dictates that the reused media is completely erased between cases so that data from one case does not get mixed in with another case. Test methodologies have been developed to examine the behavior of drive wiping tools. By using this methodology an investigator should have confidence that the tool used to prepare storage disk drives for forensic reuse are in fact wiped of any remnants of earlier investigations.

The core requirement for a tool is the removal of all accessible data on the hard drive. At a minimum all visible sectors should be overwritten with new data that is forensically benign. Some tools may adhere to a policy that ignores hidden sectors (Host Protected Area (HPA) or Device Configuration Overlay (DCO) with the justification that as long as the hidden area is in place it is inaccessible and not likely to cause a problem. Other tools remove hidden areas and then overwrite the formerly hidden data.

An important feature, sometimes overlooked by tools, is the erase instruction built in to recent hard drives. ATA drives that implement the SECURE ERASE instruction can overwrite an entire hard drive with a single command. Our test methodology provides for testing tools that use either multiple WRITE commands or the SECURE ERASE command. There are several advantages to using the SECURE ERASE command; these include faster performance and the erasure of data from failed sectors. Sometimes a hard drive removes a failing sector from normal use and substitutes a new sector from a spare sector pool. The SECURE ERASE command can access the failed sector and remove any data that is present.

**For Reuse**
B27 The Application of Known Sample Searching to Digital Forensics

Name and address removed at author's request.

After attending this presentation, attendees will gain an understanding of the potential benefits and challenges of applying known sample searching to the field of digital forensics.

This presentation will impact the forensic science community by discussing how the application of known sample searching to digital forensics can allow examiners to search for and identify thousands of potentially important artifacts, including artifacts which examiners may not otherwise recognize. It will also assist examiners in confirming the origin of artifacts identified during investigations, and in more precisely understanding the activity that led to the creation of specific artifacts. Finally, the presentation may aid in generating interest, debate, and additional work in the application of known sample search techniques to digital forensics.

Digital Forensics, Software Testing, Media Erasure

B28 Reliability of Computer Forensic Tools: Application of Chain of Custody Principles

After attending this presentation, attendees will understand limitations of the reliability of current computer forensic tools, protocols, and results. Attendees will then be able to consider what modifications to their computer forensic analysis protocols may be required, and will be better informed as to the types of validation tests that should be carried out on computer forensic tools and results.

This presentation will impact the forensic science community by encouraging the forensic community to require that tool vendors improve their products to better account for how data is handled and how computations are performed. These factors will in turn improve the reliability of computer forensic evidence presented in court.

"Chain of Custody" protocols are widely used to establish that a physical exhibit uplifted from a crime scene is the same exhibit produced in court and that the exhibit has not been tampered with in any way. The chain of custody comprises every person responsible for handling the exhibit, from the person who collected it through to the person producing the exhibit in court. Each person must be able to give evidence as to whom (or where) they obtained the exhibit, to whom the exhibit was relinquished, what happened to the exhibit whilst in their custody, and what steps were taken to ensure the integrity of the exhibit was preserved.

Computers, hard drives, and other electronic media are physical exhibits for which the chain of custody must be maintained in the usual way. However, when computer forensic analysis tools are used to examine electronic evidence the traditional chain of custody protocols may not be adequate to establish that analysis results presented in court are reliable and have not been subject to tampering.

This presentation demonstrates how inadvertent errors and deliberate tampering can adversely affect the reliability of widely used computer forensic tools in ways that may not be easily detected. The problem is illustrated using a recent case study involving multiple flaws in a widely used computer forensic tool.

Current practice and tools do not effectively address the problem are illustrated. It is argued that, with current tools and practices, the chain of custody in respect of computer forensic analysis results is often broken. It will be proposed that the issue could be addressed by adapting traditional chain of custody protocols to provide assurance over the internal processes employed by tools to read, interpret and display data.

The concept of judicial notice, the Daubert test and statutory provisions as to reliability of evidence are briefly discussed in the context of computer forensic tools.

Computer, Reliability, Validation
B1 Evidence From Explosives Correlated With Digital Evidence Examinations

Carrie M. Whitcomb, MSFS®, National Center for Forensic Science, c/o University of Central FL, PO Box 162367, Orlando, FL 32816-2367

After attending this presentation, attendees will see how high explosives create large amounts of evidence in small fragments and the manner in which the explosive scene is triaged can have a correlation with the large amounts of data in digital evidence coming into laboratories for processing.

This presentation will impact the forensic community by showing that it is all about process. Forensic processes come and go as new evidence evolves. The theory of certain processes can be applicable to various diverse forms of evidence that seem to have nothing in common. However, the desired outcomes are the same, find the most probative evidence as quickly as possible.

When I participated in the evidence collection and processing post-blast scenes resulting from an Improvised Explosive Device (IED) for the U.S. Postal Inspection Service, it was the rule that “everything” within the scene would be brought to the laboratory for examination. The vast majority of IEDs encountered utilized low explosives. The fragments were large and the damage to the environment varied. However, when an IED utilizing a high explosive detonates, the volume of debris from the environment of the crime scene is tremendous. A new approach for evidence collection and the redefining of “everything” are necessary.

Bombing scenes are very much like hard drives; bomb scenes are divided into grids and hard drives are divided into sectors. Each grid and each sector are evaluated to determine the presence of environmental debris and the presence of evidence. The solution for the high explosives crime scenes processing may be a clue to working a large digital evidence case with terabytes of data. Stay tuned!

Digital Evidence, Large Volumes, Processes

B2 Standardization of Digital Forensic Research Techniques

Carey R. Murphey, PhD®, White Oak Labs, 5121 Valerie Street, Bellaire, TX 77401

After attending this presentation, attendees will have increased insight into the challenges regarding standardization of emerging techniques and protocols in the field of digital forensics and will be better able to evaluate various ways in which the research community might have greater impact on standard operating procedures used by labs or investigators.

This presentation will impact the forensic science community by identifying, clarifying, and analyzing issues observed in the process of translating published techniques into adopted standard operating procedures in digital forensics.

This presentation explores the challenges of taking a technique from peer-review and publication to use in standard operating procedures by labs and investigators. Also discussed are the various constraints related to the age of the field, vendor support, and the standardization and certifications processes that are intended, in part, to directly support widespread adoption of good practices.

A case study involving forensic examination of Windows® logs is used for illustrative purposes. Despite the combination of a peer-reviewed, published protocol and a freely available software tool that facilitates implementation of the protocol, the recommended approach appears to have had quite limited adoption in the form of standard operating procedures. This was unexpected and indicates additional requirements that appear to significantly impact adoption of good practices in digital forensic labs. Peer-review, freely available tools, and even standardization of good practices might have enhanced impact on adopted standard operating procedures if additional requirements of digital forensics labs are met.

Ultimately this presentation addresses the question, what can one do to encourage regional digital forensic labs or individual investigators to adopt peer-reviewed techniques for digital forensics? Peer-review of a protocol may be valuable support for satisfying Daubert challenges, but it is only one of a number of requirements that labs may face in order to adopt a protocol into its standard operating procedures. Many digital forensic labs have a strong reliance on commercial software tools, such that availability of a tool that supports the protocol is an important consideration for incorporating the protocol into standard operating procedures. In some ways, this may be inherent to digital forensics due to rapidly emerging information technology and aspects of commercial software tool development. Software tools can help satisfy requirements for reliability, reproducibility or uniform accuracy. In this opinion, even the combination of peer-review of a protocol together with a freely available software tool may still have quite limited impact. This can be seen in the contrast between the reliance on commercial tools in many labs compared with the more limited adoption of open source tools. Some labs may be reluctant to codify a standard procedure without associated commercial vendor support. This suggests that peer-review, tools, and even standardization efforts may have a significantly enhanced impact if additional requirements are met.

Digital Forensics, Standard Operating Procedures, Requirements

B3 Understanding the Costs of Conducting Computer Forensic Examinations

Douglas G. Elrick, BA®, Digital Intelligence, 17165 West Glendale Drive, New Berlin, WI 53151

After attending this presentation, attendees will be able to accurately evaluate, compute, and budget the needed costs of digital forensic examiners. Whether starting a new unit or expanding an existing one, costs can be effectively estimated.

This presentation will impact the forensic community by providing managers and directors an introduction to the computer technology and practices of this forensic discipline, a guide for budgeting and planning to adequately equipment, and examples of the types of cases examiners will face.

Attendees of this presentation will learn about real costs associated with computer forensic examinations and will come away with an understanding and appreciation for the necessary types hardware, software, facilities, and training requirements for this newly recognized scientific discipline. A comparison of the commonly used forensic applications and hardware will be given. This will be helpful in the purchasing and budgetary development process for both managers and experienced practitioners.
Costs for conducting computer forensic examinations can be broken down into four main categories; hardware, software, facilities, and training. While these categories are similar in other forensic disciplines, the need for continuing updates is more apparent and pronounced in the computer field. Typical hardware and software startup costs requirements based upon a two-person section will range between $30,000 and $100,000. This presentation will highlight this range and describe the factors involved in the cost differentiations. Specific software programs and hardware devices will be addressed in a manner to present a perspective and comparison of the many features. A listing of what is considered “industry standard” applications based upon functionality will be provided along with a variety of lesser known and often less expensive or free alternatives. What must also be factored into the overall cost will be the need for annual updates of licenses and hardware changes. Many of the current forensic software packages are offering (some are requiring) annual subscription services for their products in order to receive updates and fixes. Hardware lifecycles are running approximately three years before upgrades are necessary. New types of storage media is a big reason for required upgrades. For example, when new interfaces to hard drives or new flash media types are developed the forensic workstation must be capable of connecting to it. This can often be accomplished through relatively inexpensive adapters. In other circumstances, it may require complete upgrades to the internal components of the computer. Approximately $10,000 a year may be necessary to cover these updates.

With regard to the facilities needed for digital forensics, while the data collection and inventory of the physical components of the submitted evidence are done in a traditional laboratory environment with the ability to address any chemical or biological contamination, the forensic computer analysis is typically accomplished at a desk location. The desk location should still be a part of the laboratory with all of its security and controls, but should be in an isolated place. Due to the nature of the data displayed, which is often child pornography, the examination should be conducted in an area where viewing is limited to the examiner and not to any passerby. The examination may also require considerable concentration and the work area should allow for minimal distraction.

Unlike most other forensic disciplines where the methods of analysis and identification are continually improving but the evidence itself has remained the same, with computer information the form of the evidence is consistently changing and evolving. This frequent change necessitates updated training. Continuing education is essential in order for examiners to stay abreast of new technologies and methodologies. Software and hardware providers offer regularly scheduled training updates and there are several computer forensic associations that provide methodology training each year. For state and local law enforcement grant-funded training opportunities are available. A minimum number of hours should be twenty hours per year, per examiner, as this meets the educational requirements of several industry certifications. This would provide the most basic of updates. A preferred number would be 80 hours, budgeted at $20,000 a year for two examiners.

Managers and directors who are not familiar with the computer technology and practices of this forensic discipline will have a guide for budgeting and planning to adequately equip and provide for the types of cases examiners will face. Experienced examiners will be presented with an analysis of commonly used programs, hardware and training options.

Computer Forensics, Budget, Costs

---

Michael Andrew*, CyberSecurity Institute, 21816 132nd Street Southeast, Monroe, WA 98272; and Steven Hailey, CyberSecurity Institute, 17716 Trombley Road, Snohomish, WA 98290

This presentation is based on a case study involving theft of proprietary data and efforts to conceal the offense. After attending this presentation, attendees will be able to identify and overcome certain efforts made to mislead and frustrate forensic analysis of file system activities on external storage drives.

This presentation will impact the digital forensic science community by providing analysts a methodology and practical technique that will assist in accurate analysis of data stored on external hard drives.

There are three primary learning objectives for this presentation: (1) facilitate analysis of external storage drives that have been used with a computer running a Microsoft Windows operating system that utilizes the NTFS file system, (2) identify and interpret certain data artifacts recorded on an external storage drive by the operating system, and (3) utilize these artifacts and overcome anti-forensic methods, assisting in the accurate analysis of file creation, deleting, copying, and moving processes.

This case study outlines a methodology that can be used to detect the manipulation of creation date and time stamps associated with files copied to an external storage drive. The case study also presents a process that can be used to track the movement of files to and from an external drive without reliance on recovery of latent data, (i.e., relevant file data and meta-data), or access to records located on the computer system that was used to copy the files onto the external drive.

This case concerning a large quantity of proprietary data that was downloaded to an external USB storage drive by employees, prior to departing a company. Analysis of records located in the USBSTOR sub-key on computers at the company revealed the date that the external drive was connected and used to copy the proprietary data.

In response to a court order, the defendants presented an external USB hard drive for analysis. The defendants refused to make available any computers that had been used to access the surrendered USB drive. They maintained they had never copied the proprietary data onto their personal computers and that their personal data was always kept separate from the downloaded data.

Analysis of the USB storage drive revealed the presence of proprietary files with creation date and time stamps that appeared to correlate with the connection records recovered from the USBSTOR sub-key on the company computers. However, further analysis revealed that the date and time had been manipulated at least three times during file creation processes, indicating multiple attempts to mislead and frustrate the analysis. The deception was discovered through analysis of artifacts on the USB drive that were generated as part of the System Restore function used by certain Microsoft Windows operating systems. Consequently, analysis was able to show that the presented drive was doctored in an attempt to make it appear as though it was the drive used to originally download proprietary data at the company.

In response to an inspection, the defendants also revealed that other relevant proprietary data had once been present on the drive, despite the claims of the defendants. The analysis was able to track the movement of these undisclosed files onto and off of the USB drive, demonstrating that the defendants had misrepresented their actions regarding the proprietary data and their compliance with the order of the court.

This case study is centered on a situation that presents significant challenges to an analyst; an external storage device is presented for analysis and the analyst does not have access to the computer that created the data on the storage device. The analyst cannot inspect records on the connected system to check if the file creation and file access date and time stamps for data on the storage device - derived from the system time.

---

* Presenting Author
set on the connected computer - have been manipulated. The methodology used in this case will be beneficial to the analyst in these types of situations, and can provide independent verification of activities surrounding the data on an external storage drive or device.

**Anti-Forensics, Storage Drive, Time-Stamp**

---

**B5 A Virtual Architecture for Digital Forensic Tool Validation**

J. Philip Craiger, PhD*, Chris Marberry, BS, Greg Dorn, BS, and Scott Conrad, BS, National Center for Forensic Science, University of Central Florida, PO Box 162367, Orlando, FL 32816-2367

After attending this presentation, attendees will have an overview of virtual systems, tool validation, and how the two can be combined to create a powerful testing architecture.

This presentation will impact the forensic community by demonstrating how crucial it is that examiners validate their tools. This talk will provide examiners with the necessary information for them to create a comprehensive architecture for tool validation.

The evolving nature of computer software is fast paced and constantly changing. However, no software is perfect and anomalies can present themselves; bugs can be introduced with new features, or as an unintended consequence of a bug fix. This is, unfortunately, the reality of computer software and as a result of this it is vital for computer forensic examiners to validate the forensic tools they use and to ensure that the tool’s results are accurate. A simple way to validate a tool is to compare a tool’s calculated value against a previously known value, such as a one-way cryptographic hash value of a drive, volume, or even a file. Another is to “triangulate” results by testing the same function of several different programs against the same medium to see if they produce the same results.

While evaluating digital forensic proficiency tests it was noted several examiner’s test results differed from our “validated answers.” (The validated answers were obtained by triangulating results from several different forensic suites and different versions of these suites). Of interest was determining whether these discrepancies were due to error user, forensic suite error, or some other unanticipated anomaly (e.g., bad hardware).

In order to test these hypotheses a virtual architecture was developed that allows the separation of the influences of different forensic suites, different versions of the suites, and operating systems in order to identify the possible source of these errors. A typical validation methodology would involve dedicating several computers to running different forensic suites (separate computers would be used so as not to contaminate the results by installing and/or running two forensic suites on the same computer). This methodology results in significant duplicated time and effort for every single instance of forensic suite that requires validation. Disk imaging has simplified this process to a degree, by allowing a “baseline” image to be created and kept, but it is still undesirable in terms of required storage space and the amount of time required. Virtualization technologies, however, allow a significant portion of this process to be streamlined, in terms of both required disk space and time spent. One important feature that virtualization allows are snapshots: a complete save of the current state of a running computer, such as any installed programs or an active running program. The ability to freely and quickly move between snapshots is immensely beneficial as this allows a user to move between different versions of software in only a few minutes instead of waiting for whole disk images to be applied back to the hard drive or having to re-install everything from scratch.

The use of virtualization has greatly improved the process of the internal result validation for the competency test. Not only has using this functionality saved time, but this is all derived from a single feature of virtualization technologies. Decreasing the time spent performing the necessary yet time consuming tasks is something that can benefit any laboratory or practitioner. Virtualization also has many other features that are desirable to the forensic community, such as creating self-contained (air-gapped) investigative virtual machines, and completely standardized hardware that does not change even if you move the virtual machine to different physical computers. These and many other features of virtualization should be sufficient reason to investigate the use of these technologies in any digital forensic environment.

**Virtual System, Tool Testing, Tool Validation**

---

**B6 Smart Unpacking: Methods for Characterization and Extraction of Embedded Content**

Benjamin Long, BBA*, NIST, 100 Bureau Drive, Stop 8970, Gaithersburg, MD 20899

After attending this presentation, attendees will learn about the theoretical and practical frameworks, being developed for the NSRL, to characterize, extract, and measure embedded digital objects using mathematically-based techniques.

This presentation will impact the forensic community by presenting frameworks for addressing the content analysis, data extraction, and measurement of these embedded digital objects.

This work presupposes that digital content can be characterized and classified according to mathematical properties and structures. Discussed is ongoing work as well as how this can form a foundation for validation and measurement of the structures discovered.

This talk describes what Smart Unpacking Research is with respect to the National Software Reference Library (NSRL) project. The NSRL is a project of the National Institute of Standards and Technology (NIST) for collecting and providing identifying information about known files. The NSRL project’s goal is to unpack as many files as possible. This research was originally conceived for addressing a particular scenario that occurs frequently in NSRL operations – the need to extract files from compound files (files containing other files) that have no corresponding off-the-shelf unpacker. In addition to this primary scenario, the results of this work may be applied in more general ways. The unpacking methods being developed in this ongoing research are derived by means of modeling the patterns in relevant files using mathematical and other modeling techniques. The objective of this talk is to present the current status of this work and its more general relevance to related problems in the computer forensics domain.

Specifically, this work uses Pattern Theory to develop high quality models for patterns of interest in files, file formats, as well as specific types of content. These models describe how certain patterns are formed and allow us to develop algorithms and techniques for recognizing patterns in certain types of files, file formats, and file content. These algorithms are then implemented using a software framework of parsers to extract files. The parsing framework may also provide measurements to help assess the completeness and quality of such file-extraction operations both for these derived unpackers, as well as, for off-the-shelf unpackers.

Also discusses are how such techniques might be applied to other challenges of general relevance in computer forensics. Generalized versions of this work will be most relevant to one of two tasks: (1) improving understanding of file format and content, as well as, (2) enhanced file carving techniques to extract digital objects out of their digital context.

The focus of the current work is not to reveal the content or structure in encrypted or compressed patterns, but simply to identify data.
that might contain embedded compressed or encrypted information. Once identified, such data can be extracted as objects for further processing (e.g., decompression or decryption).

**Mathematical Content Analysis, Data Measurement, Content Validation**

**B7 Fixed Size and Variable Size Block Hashes for File Identification**

*Douglas R. White, MS*, 4225 Angell Road, Taneytown, MD 21787-2601

After attending this presentation, attendees will understand some of the principles of identification of files during investigations of computer systems based on cryptographic hashes of files and partial files.

This presentation will impact the forensic community by introducing the rigor of cryptographic digital file identification at a granular level, which supports statistical identification of objects.

Use of cryptographic hashes or “digital fingerprints” to automatically identify files is absolute when applied to a file as a whole, where the file is unambiguously categorized. When dealing with morphing digital objects, such sorting leaves many files to be dealt with by manual review.

Block hashing is a method of applying the cryptographic algorithms to smaller-than-file size portions of the suspect data. Previous work used cryptographic hashes to “fingerprint” portions of data files, which assist investigators in identification of modified and partially deleted suspect data. Such cryptographic hashes cannot be used to identify similarities between data.

In this case study, cryptographic hashes and “spamsum” fingerprints of corresponding variable sized blocks are computed. The aggregation of the block hash values allows statistical probabilities of identification of suspect files, taking the dynamic nature of digital objects into consideration. The association of a cryptographic hash with spamsum combines positive file identification with a method of identifying similar file content. With this information, investigators can identify portions of uncataloged files which are similar to portions of known, cataloged files.

Examples of practical applications of this technique will be presented. Files from 90 computer systems within one organization were processed. Examples of installation of common software applications can be identified, despite installation modifications. Identification of shared documents can be identified, including edit changes. This work addresses the use of simple anti-forensics methods to defeat automated file identification.

**Cryptography Hash, File Identification, Block Hash**

**B8 Computer Forensic Tool Testing Strategies**

*James R. Lyle, PhD*, National Institute of Standards and Technology, 100 Bureau Drive, Mall Stop 8970, Gaithersburg, MD 20899

After attending this presentation, attendees will become aware of some of the strategies used by the Computer Forensics Tool Testing (CFTT) project at the National Institute of Standards and Technology (NIST) for testing computer forensic tools used in the acquisition of digital evidence.

This presentation will impact the forensic community by increasing awareness that the impact tool test strategies have on the ability of tool testing to reveal anomalies in tool behavior.

The Computer Forensics Tool Testing (CFTT) project at the National Institute of Standards and Technology develops methodologies for testing computer forensic tools. The developed test methodologies to several tools in the areas of disk imaging and write blocking have been applied and test strategies for testing storage erasing, deleted file recovery, and string searching are being developed. A test strategy should cover all tool features and also give the tool opportunities to fail in easily detectable ways.

For example, good forensic practice is to start by writing zeros to any pieces of media that would be used in an examination of digital data. However, one common way for a tool to fail is to place information in the wrong location. If a block of zeros is transposed with another block of zeros the switch is undetectable. A better practice for media initialization during testing is to write unique content to each disk sector. This has the advantage that out of place data is easy to recognize. If the unique data also includes the original location of each sector then knowing the original location may be helpful in characterization of the tool behavior.

Disk imaging involves acquiring an image of either a physical hard drive or a disk partition, also called a logical drive. A disk imaging tool functions by reading each sector from the drive to be examined and creating either an image file or a clone of the original on a similar device. An image file contains all of the information to exactly reconstitute the original hard drive. While an image file may be stored as a bit for bit copy of the original, it is usually compressed in some way to save space.

Write Blocking is used to protect original digital data from modification during acquisition or preliminary inspection in order to determine relevance to an investigation.

Storage erasing, as considered by CFTT, is for storage device reuse within an organization rather than for disposal or transfer to a destination outside the organization.

This presentation examines selected test cases and test procedures used by the CFTT project to demonstrate the kinds of tool errors that can be revealed by each strategy.

**Digital, Tool Testing, Software**

**B9 Applying Advanced Search Techniques to Digital Forensics**

*Brian D. Carrier, PhD*, Basis Technology, One Alewife Center, Cambridge, MA 02140

After attending this presentation, attendees will have a better understanding of what search techniques exist, but are not yet being applied to digital forensics. Attendees will see an example of how these techniques can be applied to digital forensics tools.

This presentation will impact the forensic science community by discussing and talking about how research advances in other fields (namely information retrieval) can be applied to digital forensics to help an investigator more quickly locate evidence.

Keyword searching is common in a digital investigation, but primitive methods are currently being used. Keywords are entered and a list of files with the keyword is given. The files could be listed by file name, by the order the search tool found them in, or something else. It is similar to searching the web 10 years ago. There have been many advances in search techniques that could be applied to digital investigations to help find evidence more quickly. Examples of advances include faceted search, clustering search results by topic, generating automated summaries of documents, and improved ranking. These techniques would allow the investigator to more quickly review search results and ignore the false positives. This presentation will provide an overview of these technologies and demonstrate how they can be used in an investigation.

**Digital Evidence, Search, Analysis Tools**

* Presenting Author
B10  An Odyssey Into Lesser Known Regions of Embedded Metadata in Microsoft File Formats

Eoghan Casey, MA*, ONKC LLC, 3014 Abell Avenue, Baltimore, MD 21218

After attending this presentation, attendees will understand how to find previously unknown metadata embedded in digital files that can be critical to an investigation.

This presentation will impact the forensic community by showing forensic examiners, at a practical level, how to uncover lesser-known metadata in digital files. At a higher level, this presentation demonstrates the limitations of file format documentation, existing forensic tools, and the importance of conducting methodical experiments and tests in digital forensics. Furthermore, to bring this process into the realm of science, the methodology used in all three cases is formalized to help forensic examiners repeat the process in other contexts and apply it to other file formats.

A few bytes buried in a digital file can contain crucial details in a case, like remnants of activities that contradict suspect statements, or incriminating text from prior versions of an e-mail. The main challenge for forensic examiners is that the most useful embedded metadata can be buried the deepest. Conversely, the fact that this information is difficult to locate means that it is harder to alter or destroy, and may persist despite the best efforts of the subject in an investigation.

Three cases are presented that made use of lesser known metadata in Microsoft file formats: Word, Excel, and Outlook. The embedded data used in these investigations is poorly documented. Furthermore, forensic tools are ineffective at extracting this information. This presentation guides attendees through an odyssey into Microsoft file formats, using a combination of research and experimentation to uncover important clues embedded (and in one instance encoded) within a file. Digital Evidence, Embedded Metadata, Digital File Formats

B11  The Impact of Multicore CPUs and Graphics Processing Units (GPUs) on Digital Forensics Tool Design

Golden G. Richard III, PhD*, Department of Computer Science, University of New Orleans, New Orleans, LA 70148

After attending this presentation, attendees will understand the role that multicore CPUs and Graphics Processing Units (GPUs) can play in substantially increasing the performance of tools that process digital evidence. The motivation for “massively threaded” tool designs that support both multicore CPUs and GPUs will be discussed and both the possibilities and limitations of this approach to speeding up digital forensics processing will be covered.

This presentation will impact the forensic community by exposing mechanisms for substantially increasing the performance of digital forensics tools on commodity hardware, with little or no additional hardware expenses, albeit with increased effort on the part of tool developers. This work is important because higher performance tools are critical to deal with the increasing size of investigative targets.

Since the size and complexity of digital forensics targets continues to grow, with commodity disk sizes now exceeding 1TB, it is crucial that tool developers increase the performance of tools that process digital evidence. This is important both to ensure that cases can be processed rapidly to provide timely results and to avoid aggravating the persistent problem of case backlogs. Good tool design plays an important role in rapid evidence processing, but single-threaded designs that process evidence using only a single CPU cannot be scaled up to deal with ever-increasing target sizes. Therefore, alternative mechanisms must be considered, including more effective use of available computing resources, such as multicore CPUs and high-performance Graphics Processing Units (GPUs). Modern CPUs now commonly use multiple compute cores with lowered clock speeds (e.g., the Intel Core2Duo) in favor of single-core designs with high clock speeds (e.g., the Pentium 4 series and earlier). There has also been a major architectural shift in GPU designs, with modern GPUs providing hundreds of (relatively) general purpose processors instead of very specialized graphics processors. Since most current-generation tools are single threaded, they are generally unable to take advantage of the compute resources offered by multicore CPUs and GPUs. The transition to simple multithreading in tools to fully utilize multicore CPUs is a first (and easier) step in the right direction. But in this presentation it will be argued that new massively threaded digital forensics tool designs are needed and the role that GPUs can play should be carefully considered. Modern GPUs are essentially “supercomputers on a card” and with careful programming can yield very significant performance improvements for a variety of problems. But the associated programming issues are non-trivial and care must be exercised in dividing work between the host CPU and GPUs for maximal performance gains.

Results of some recent efforts to port digital forensics operations to GPUs and multicore CPUs to increase tool performance will be presented. The focus will be on file carving, with performance results comparing single-threaded designs, simple multithreading on multicore CPUs, and GPU implementations presented. Digital Forensics, Graphics Processing Units, High Performance Computing

B12  Supporting Cyber Crime Investigation With the UAB Spam Data Mine

Chengcui Zhang, PhD*, CH 127, 1530 3rd Avenue South, Birmingham, AL 35294; Chun Wei, MS, Wei-Bang Chen, MS, Richa Tiwari, MS, and Xin Chen, PhD, CH 128, 1530 3rd Avenue South, Birmingham, AL 35294; and Gary Warner, BS, CH 100, 1530 3rd Avenue South, Birmingham, AL 35294:

After attending this presentation, attendees will understand how cybercrime investigations can be assisted and how additional evidence of guilt can be gathered through queries to the UAB Spam Data Mine. The UAB Spam Data Mine gathers millions of email messages together into a relational database which supports rich queries as well as complex data analysis to reveal non-intuitive relationships between the cybercrime events to be identified. Online for more than a year, the Data Mine has been successfully used to merge multiple phishing cases against several brands into single cases, and to provide additional data used in the sentencing portions of cases to prove dates and durations of criminal activity in several cases in multiple countries.

The Spam Data Mine will be explained, including the sources for the millions of emails, and the method of parsing, analyzing, and clustering the data. How the Data Mine has been used successfully as the starting point of a successful Malware Investigation will be demonstrated, proving that multiple seemingly unrelated malware attacks were actually a single attack aimed at stealing financial account information through keystroke logging of compromised computers, and leading to identification and arrest of involved perpetrators. In many cases, the Spam Data Mine was able to rapidly conclude that a malware attack was underway, even when the anti-virus products had not yet been updated to provide signatures to detect the emerging malware.

In the second part of this presentation, also discussed is how spam campaigns which use “image-based” spam can be successfully clustered into their appropriate campaigns, even when the images are obscured to
prevent successful optical character recognition (OCR). A unique approach to separating complex images into several layers for deeper analysis and matching will be explained. A case study will be presented where image analysis was able to identify many spam messages all related to the same “Stock Market Pump and Dump” campaigns which will be used to illustrate the possibilities that Image-based clustering of emails can achieve to assist Law Enforcement. The ability to rapidly identify whether a new spam message is part of an existing criminal operation or is something new will be illustrated.

While the computer science aspects of data mining and image processing techniques will be discussed in some detail, many examples of the types of complex law enforcement queries that can be supported by the UAB Spam Data Mine will be provided. Illustrations of appropriate ways to use these new capabilities in support of investigative efforts will be discussed for many scenarios.

**Computer Forensics, Spam, Spam Images**

**B13 Digital Media Players — Recent Research and a Cautionary Tale**

Jessica Reust Smith, MFS*, Stroz Friedberg, LLC, 1150 Connecticut Avenue Northwest, Suite 200, Washington DC, 20036; Thomas Owley, MD, 1747 West Roosevelt Road, Chicago, IL 60608; Edward Zawadzki, DO, 144 West 12th Street, New York, NY 10021; Soyina Owley, MD, 1500 Waters Place, 10011, Bronx, NY 10461; and Stephen B. Billick, MD, 11 East 68th Street, Suite 1B, New York, NY 10065-4955

After attending this presentation, attendees will gain knowledge of recent research and analysis performed on digital media players, with a specific emphasis on Apple iPod™ devices and the analysis of metadata for generating timelines and determining user activity.

This presentation will impact the forensic community by serving as a cautionary tale and reminder about the challenges involved when preserving, storing, and analyzing devices as dynamic as digital media players.

Digital media players are fast becoming as ubiquitous as cell phones, and are turning up in increasing numbers in forensic investigations of both civil and criminal matters. A jogger is raped and her digital media player is missing. A suspect is arrested with a digital media player in his possession. What can examination of this device do to help determine the guilt or innocence of the suspect? An employee is accused of industrial espionage. A digital media player is turned over for examination. Could this device have been used in the commission of this crime? What evidence can be extracted from the digital media player to help build a timeline of the commission of the alleged offense?

Digital media players vary greatly both between and within manufacturers. For example, since the introduction of the Apple iPod™, only seven years ago, there have been 15 different hardware versions released. Even within each version there are differences resulting from firmware updates, file system formats, and syncing methods. All of these possible combinations result in unique behaviors that can impact the conclusions that can be drawn from forensic analysis. What happens when the battery dies while it is stored in your evidence room? What are the forensic consequences of playing a song or simply the passage of time? Can you verify the MD5 hash of your forensic duplicate with the original evidence if you allow it to sync with your forensic workstation?

When performing forensic tool/methodology testing and evaluation, your ability to duplicate the hardware, firmware, file system, and syncing environment can significantly impact your results. For this reason, relying on the published results of other forensic researchers without performing sufficient verification may not be wise. When building a timeline of the user activities it is important to have, among other things, an in-depth knowledge of both the file system on which the activity took place and the applications that are involved in the activity.

Metadata that can be used in timeline generation is stored, both on the device and within the software application data store used for syncing (most frequently iTunes™). What are the implications on your forensic examination for a two year old device that has been sync’d with each new version of syncing software as they were released? Can you rely on the metadata for each digital media file to be consistent?

Attendees of this presentation will learn forensic examination techniques for extracting valuable evidence from digital media players, drawn from both applied research and actual investigations. This presentation will also show a forensic examiner what they can do to avoid some of the forensic pitfalls caused by the fast changing digital media player environment.

**ipod, Timeline Generation, Metadata Analysis**

**B14 Using Computational Forensic Linguistics to Screen Pedophilic Communications**

Carole E. Chaski, PhD*, Institute for Linguistic Evidence, 25100 Trinity Drive, Georgetown, DE 19947-6585; and Raye Croghan, BS, ALIAS Technology, LLC, 25100 Trinity Drive, Georgetown, DE 19947-6585

After attending this presentation, attendees will understand a validated computational forensic linguistic method for assessing two communication types, threats and pedophilic grooming, in order to screen for pedophilic communications.

This presentation will impact the forensic and legal communities by delivering a method to discover early warning evidence of threatening and grooming behavior that results in child endangerment, abduction, and sexual assault.

Most adults experience threats and pedophilic grooming communications after the fact, when emotional or physical harm has been inflicted. Children, by virtue of their age, are even less likely to be able to accurately evaluate these covert communication types. Lack of exposure to such communications means that most of us are not able to recognize these communication types for what they are, even if we recognize that something is not right in the situation. Yet the ability to recognize and accurately classify different types of problematic texts has obvious survivability, as well as, investigative value in evaluating recidivism potential for convicted and repeat offenders. Computational Forensic Linguistics provides objective, intelligent classification for these rarely-experienced and very problematic text types.

As a branch of natural language engineering, Computational Forensic Linguistics quantifies specific linguistic features in text and dialog, and then subjects this quantification to statistical analysis for classification of documents into forensically-significant categories. ALIAS, Automated Linguistic Identification and Assessment System (Chaski 2005, 2007, 1997) is a computational forensic linguistic program with components for authorship, witness statement relatedness, and other forensically-significant questions. In this presentation, two components of ALIAS, ThreatAssess and PREText are discussed.

ALIAS ThreatAssess provides a very rapid (milliseconds) assessment of a text to determine if it is classified as a real threat or not. Using a database of real threat letters which have been involved in investigation or litigation and the Chaski Writing Sample Database of simulated threat letters, apologies, love letters, complaints, and angry letters as comparison texts, a cross-validated statistical model for classifying texts has been developed. Like the threat text type, each comparison text type has an interpersonal and emotional communicative purpose and therefore represents a good foil. Each new text fed into ThreatAssess is classified as either a real threat or a comparison type based on the statistical model whose accuracy is at least 92% with a maximum of 100%.

Built on ALIAS ThreatAssess, ALIAS PREText, or PREditor Text, provides a very rapid assessment of a text and/or a chat dialog to

* Presenting Author
determine if it is classified as sexual predatory grooming or not. ALIAS PREText was developed using several different types of pedophilic communications: (1) pedophile to pedophile, (2) pedophile to victim, (3) pro-pedophile activism, (4) risky communications, and (5) defensive pedophile communications. Pedophile to pedophile data includes personal interactions between pedophiles dating back to 1996 as associated with pedophile participation in special interest pro-pedophile only membership groups where electronic communications took place through email, forums, and electronic chat. Pedophile to victim data includes grooming tactics captured between a pedophile and a child or an adult informant posing as a child where the pedophile acted on the chat by appearing physically to meet the minor victim. Many of these chats have been used in court as part of the conviction process. Pro-pedophile activism data includes known pro-pedophile activism web sites, blog articles, papers and letters promoting the pedophilia cause in defense of perceived persecution by society. Risky communication data includes electronic interaction between adults curious about pedophilic tendencies and the normalization of the perversion by the pedophile community and recruitment of new pro-pedophile member tactics. Defensive pedophile communication data includes electronic communications among pedophiles with convictions and/or admitted activities and attraction to minors despite severe penalties, including overt/covert threats against countries and persons illegalizing child pornography and persons engaged in prosecution or anti-pedophile activism.

PREText implements a statistical model of these different communication types, providing a score based on an empirically-derived threshold. ALIAS PREText’s objective, quantitative, statistically-validated scoring can be used to develop techniques and training in pedophilic cybercrime investigations, to provide cloaking for investigators, and to present scientific evidence to judges and juries about communications which are, fortunately, unlikely to have been experienced firsthand by the triers of fact.

Pedophile Communications, Forensic Linguistics, Predatory Grooming

B15 Application of Natural Language Processing to the Digital Forensic Process

Mark Pollitt, MS*, University of Central Florida, PO Box 162367, Orlando, FL 32816-2367; and Anne Diekema, PhD, Center for Natural Language Processing, Syracuse University, 335 Hinds Hall, Syracuse, NY 13244

After attending this presentation, attendees will understand the level structure of natural language processing, the corresponding levels of abstraction and access in digital forensics, and how the two taxonomies are related.

This presentation will impact the forensic community by introducing the digital forensic community to the theories and approaches utilized in the natural language processing community.

Since the second World War, computer scientists and others have struggled to find computational methods to translate, understand, and mimic human communications. What has evolved is an interdisciplinary approach known collectively as natural language processing (NLP). The literature in this community includes the notion of “levels of language” which describe the different ways in which “text” in the broadest sense communicates meaning. These include: phonology, morphology, lexical, syntactic, semantic, discourse, and pragmatic.

The digital forensic community faces a somewhat similar problem in that meaning is stored on computers at a number of different levels. The context and therefore the meaning of any particular data, from a digital forensic perspective, can be altered by the various levels of access/abstraction including the physical media, operating system, file system, application, and content. The metadata from each of these layers provide additional context that shapes the meaning of the data.

This presentation will provide a brief overview of the history of NLP, an explanation of the NLP levels of language, a review of the digital forensic levels of access/abstraction, discuss the similarities of these two processes and map their correspondence with the goal of identifying NLP techniques and methodologies that can be applied to digital forensics.

Natural Language Processing, Digital Evidence, Digital Forensics

B16 Forensic Analysis of Forensic Analysis of Spyware/Monitoring Software

Don L. Lewis*, Lakewood Police Department, 445 South Allison Parkway, Lakewood, CO 80226

After attending this presentation, attendees will be familiar with the challenges presented by the covert nature of spyware/monitoring software. An approach to identify and recover the application and its data files will be presented.

This presentation will impact the forensic community by exploring how the monitoring software, SpectorPro, is designed to be invisible to the computer user in order to avoid detection, but this results in a significant challenge for forensic examination.

Spyware/Monitoring software is marketed to consumers and businesses to monitor activities of children or employees. It is designed to be invisible to the computer user in order to avoid detection, but this results in a significant challenge for forensic examination. This presentation is the result of a case study and research in how to identify and examine spyware/monitoring software.

There are also monitoring emailer applications which monitor and email the user activity to the person monitoring an individual. Emailers have some advantages for the forensic examiner, because they send emails that are easily found in an examination. These emails appear in an unencrypted format and are easily viewed and documented. This presentation only deals with the spyware/monitoring application, which is more difficult to identify, process and examine.

Spyware, Covert Installation, Monitoring Software

B17 Testing of Image Quality of In-Car Video Systems

Herbert L. Blitzer, MBA*, and Jerry Jeffers, MS, Institute for Forensic Imaging, 338 South Arlington Avenue, Suite 111, Indianapolis, IN 46219

After attending this presentation, attendees will gain knowledge on how in-car digital video systems are to be tested in the future and how this might affect forensic video analyses.

This presentation will impact the forensic community by showing that the use of in-car digital video is expected to continue growing and that the IACP has promulgated requirements that departments can utilize in the acquisition of systems. The result is expected to be an increase in the quality and some degree of predictability of performance of these systems. This will have an impact on how forensic video analysts interpret their findings in the future. It will help anticipate what sized objects might be reproduced, what colors might be reliable, and how movements can be interpreted.

The use of in-car video systems in police and other emergency vehicles is growing rapidly. Unfortunately, there are many aspects that are important to a successful system and guidelines for these systems are just emerging. Some of these aspects deal with: physical properties, electrical properties, system integration properties, and image quality.
Setting requirements for image quality is very difficult and a set of properties has been selected for use at this time. This paper will deal with those properties, how they are measured, and what performance details they cover.

Over the past few years, a team lead by the International Association of Chiefs of Police (IACP) has been working to determine the physical layouts that are involved in in-car video recording and they have set some basic indications of the types of objects that should be resolvable. They have measured the lighting conditions that might be encountered and the colors that might appear in scenes. They also have indications of the movements of interest in a typical scenario. The testing routines are based on these findings.

The properties measured are static resolution, dynamic modulation, dynamic range, aspect ratio, and color fidelity. Static resolution is measured both vertically and horizontally using targets that are consistent with the objects of interest at a typical scene. Bar charts are used and the test is designed to show if the system can reproduce a certain standard or not. It is a pass fail test and not an engineering measurement. Dynamic modulation started out as a test of resolution of a moving target, but testing has shown that what is really being measured is the degree of modulation an image maintains as the target moves faster and faster. This turns out to depend on the sensitivity of the light levels, sensor and the shutter speeds of the camera. Hence, this property is now referred to as modulation of a dynamic target. The system’s compression routines can have a significant impact on these results. Dynamic range is measured using a luminometer with a 10,000:1 test target. The system’s monotonic response above noise threshold point and below the saturation point is examined. Most of the cameras were in the range of about 100:1, which is a bit short of the range found in a number of typical scenes. Comparisons to digital still cameras are shown for context. To measure color fidelity, a Macbeth Corporation Color Checker is used along with 5,000° Kelvin lamps. Frames are then taken from the video as an officer would when analyzing a recording is sampled. The CIE/Lab values for the primary colors and gray level patches are measured and individually compared to the correct values for those patches. Then a figure of merit is calculated based on the mean square error calculation.

The result of measuring a number of cameras, each with its respective software, is shown. As a general rule, the analog cameras are better at dynamic modulation, but worse in the other respects. The high definition cameras are very good at color fidelity and static resolution, but sensitive to light levels when examining dynamic modulation. Dynamic range measurements are comparable across all the cameras tested, and all are marginal relative to the application requirement. All are low relative to the range that can be achieved with digital still cameras.

The testing described in this paper is the basis for the image quality portions of the current IACP, in-car digital video specification. These may change as new technology is developed and as practical experience under the current regime is recorded. For example, there was discussion of moving color test targets, but this in not measured in the current specification.

In-Car Video, Forensic Video, Testing

B18 A Subjective Video Quality Test Method for the Assessment of Recorded Surveillance Video

Mark A. McFarland, ME*, U.S. Department of Commerce, NTIA/ITST, 325 Broadway, Boulder, CO 80305

After attending this presentation, attendees will learn of a new test method developed by the National Telecommunications and Information Administration (NTIA) that is suitable for assessing the subjective video quality of surveillance (and other task-based) video.

Attendees will also understand the unique problems associated with assessing the quality of surveillance video and why extant testing recommendations on subjective video quality assessment (developed by the International Telecommunication Union (ITU)), cannot be applied to the surveillance video testing.

This presentation will impact the forensic science community by giving the forensic video community a standardized method to assess the quality of surveillance video. Law enforcement organizations have noted problems arising from low quality surveillance video and have been developing guidelines that aim to improve the quality of surveillance video; yet no method exists that can be used to measure this quality. The test method described in this presentation provides a new testing method, which may be used to measure the subjective video quality of surveillance (and other task-based) video.

The quality of surveillance video impacts our law enforcement communities, courts, and the public. Poor surveillance video quality could result in critical evidence being dismissed and criminals remaining at large or being set free.

The quality of surveillance video is of major importance to the law enforcement community. Quality is defined as the minimum acceptable levels of impairments that make it possible for law enforcement to utilize the recorded surveillance video to do its job and identify images in the video that are pertinent to an investigation and use those images to help identify, apprehend, and prosecute criminals. Once a crime is committed, the surveillance video may become critical evidence for the purpose of identifying what happened and who and what was involved in the crime. The surveillance video helps law enforcement piece together the events, objects, and individuals related to the crime and apprehend and prosecute the suspect(s). The surveillance video is essential evidence in many criminal cases.

Low quality surveillance video is a problem for the law enforcement community because it impedes its ability to do its job. Low quality recordings do not give law enforcement the level of detail needed to identify a suspect or an object or to piece together the events of a crime. Many groups have been looking at improving this quality. The National Telecommunications and Information Administration’s (NTIA) Institute for Telecommunications Sciences (ITS) has undertaken research in this area. Part of this research resulted in the development of a subjective video quality test method suitable to measure a video analyst’s assessment of that quality.

Methods for subjective video quality testing have been proposed by the International Telecommunication Union (ITU), the Motion Pictures Expert Group (MPEG), military image quality researchers, and others over the previous decades. The method described in this abstract synthesizes recommendations of these groups, along with recommendations by law enforcement video analysts, and proposes a new test method which enables the subjective quality of surveillance video to be measured in a standardized manner.

The unique problems associated with assessing the quality of surveillance video are presented. Reasons why extant testing recommendations on subjective video quality assessment (developed by the ITU) cannot be applied to the surveillance video testing are also discussed.

This test method will benefit the law enforcement community and video quality researchers because it provides a standardized method to assess the effectiveness of guidelines and recommendations which were developed to improve the quality of surveillance video. This method has been presented to the International Telecommunication Union (ITU), and is currently a draft recommendation by the ITU’s Study Group 9.

Surveillance Video Quality, Subjective Video Quality, Video Quality Assessment
B19  Examining Photo Response Non-Uniformity for the Comparison of Cameras

Zeno J. Geradts, PhD*, Maarten van der Mark, BS, and Wiger Van Houten, MS, Netherlands Forensic Institute, Ministry of Justice, Laan van Ypenburg 6, Den Haag, 2497 GB, NETHERLANDS

After attending this presentation, attendees will learn what conclusions can be drawn from Photo Response Non-Uniformity, how to validate the method, and methods for examination and practical software.

This presentation will impact the forensic community by providing practical methods of validation and some statistical background for determining if images are made with the same camera.

Camera identification, based on pixel artifacts, has been widely known in forensic science for over a decade. Currently, sensors (CMOS/CCD) are manufactured with no pixel defects, and the Photo Response Non-Uniformity (PRNU) can be used as a comparison measure for a specific camera. The PRNU is a measure to identify cameras based on the slight variations between pixels which is characteristic for a camera and claimed not to vary in time.

For practical use in forensic science, it is important to validate the results and also the causes of the PRNU. This paper aims to answer two questions:

- Is there a practical method for measuring PRNU?
- What are the causes of PRNU and statistics behind it?

In the past a Matlab-script for reading the PRNU was developed for low resolution cameras. Since it is not easy to use on a wide scale, it was converted to Java coupled with a database of cameras. The goal of this application is to help forensic researchers and others to determine the source of a digital photographic image. To achieve this goal both the digital image(s) and the suspected source camera is needed. It is also necessary to have several other digital cameras available, preferably of the same brand and model to compare the results. This application works by extracting an average Photo Response Non-Uniformity pattern, a form of chip specific noise, from the images of interest. The correlation between the PRNU and reference patterns from several cameras is calculated. The reference pattern that has the highest correlation is most likely to be the source camera for the image of interest.

The following steps are taken during the extraction process of the PRNU:

- Blocks of pixels are averaged to reduce jpeg artifacts.
- A convolution with a small Gaussian filter is performed.
- The filtered image is subtracted from the original to get the filtered noise.
- The image edges are set to zero (convolution causes errors near the edges).
- Multiple PRNU patterns are averaged to one pattern.
- The PRNU patterns can be stored in a database and a hit list will appear with a ranking. When using this program it is important to validate the results by using several same type cameras to know how random the pattern is. The software for this database is named PRNU Compare and available from www.sourceforge.net.

Within this research an attempt is made to find a statistical measure to objectively qualify the value of the evidence, by dividing the probability density functions under two hypothesis. Based on the correlation found between the PRNU pattern extracted from the questioned image and the flat fields from the suspect’s camera a Bayesian conclusion could be drawn. The results are convincing, since the correlation between two images having the same origin is much higher than when this is not the case. Due to the large amounts of test data needed to reliably estimate the density functions, it is not a practical approach. A few alternative approaches are mentioned, which may be useful for continued research on solving this issue.

Different methods for concluding the results are discussed as well as future research within the European Network of Excellence FIDIS (www.fidis.net), where an attempt is made to link cameras based on PRNU, (e.g., YouTube).

B20  Determination of Time of Recording With Electric Network Frequency (ENF)

Maarten Huijbrechtse, BS, and Zeno J. Geradts, PhD*, Netherlands Forensic Institute, Ministry of Justice, Laan van Ypenburg 6, Den Haag, 2497 GB, NETHERLANDS

After attending this presentation, attendees will gain knowledge of how Electric Network Frequency assists in determining the authenticity of a recording, tampering, the time of recording utilizing ENF, how to collect ENF, and validation of results with statistical background.

This presentation will impact the forensic community by giving an overview of the current status of ENF-research, tests to validate the results, and to use a Bayesian approach for conclusions.

In casework, sometimes there are doubts regarding the authenticity of a recording. Has a crime been committed at a certain time, when for example someone recorded it with a video camera on a phone? There can be time stamps on the recording; however, sometimes there is also the signal of the electricity network available on the recording.

The European network has 50 Hz as mail frequency, whereas the U.S. network has 60 Hz. However, it is known from various research studies, for example by Grigoras, that over time, the frequency is not constant, but fluctuates around 50 Hz in a presumably random way. At each point in time, the fluctuation is the same throughout the entire network.

It is also known that a digital audio recording can contain the ENF signal if it has been recorded with mains powered equipment (Grigoras). Further, according to Kajstura et al., it is possible to detect the ENF signal in a recording made with battery-powered equipment.

Grigoras and Kajstura et al. have shown that it is possible to verify or falsify a questioned time of recording by comparing the ENF signal from the recording with a database of the ENF fluctuation. The natural follow-up question is: Can we use the ENF signal from a digital audio recording to determine its (unknown) time of recording? Our research aims at answering this question.

A database was created of the ENF fluctuation that was recorded from September 2005 to February, 2007 (with some interruptions). This database is reported to differ less than 2 mHz from frequency measurements by the Swiss ETRANS company.

This database is used to test the randomness of the ENF fluctuation. This was completed by computing typical correlation coefficients (r) and root-mean-squared differences (e) for two separate pieces of equal length from the database. With r close to 1 and e close to 0, the pieces are determined to be (almost) identical. Ideally, this only happens when the two pieces are in fact not separate ones, but the same ones.

Furthermore, ENF fluctuation were collected for a month. During this collection process, several audio recordings were made both in uncompressed (.WAV) and compressed (.MP3) format. By matching the ENF signal from these recordings with the collected ENF fluctuation, testing to determine whether r and e are significantly closer to 1 and 0 respectively than the typical values found from the database was conducted, and thus whether a recording can be uniquely positioned in time.

Future research could be aimed at determining with which network a certain recording has been made. The difference for example between the American network (60 Hz) and the European network (50 Hz) might be obvious. A recording can also be made with a generator, which could also have certain ENF patterns. Future research within this field could...
also include checking for patterns derived from ENF for example in the images of video streams or other sources.

For forensic research it would be necessary to have ENF databases from electricity networks that are not connected and accessible to other forensic scientists. A java applet for acquisition has been developed for the acquisition. A challenge is to have a reliable signal from the different networks in the world, in which different laboratories in the world can acquire data from the different networks. When large ENF databases from different networks are available, it is possible to compare the databases, which helps in determining authenticity of a recording in forensic science. Also in the forensic conclusion of the report it becomes possible to conclude in a Bayesian approach, since statistics are available from these database, and conclusions drawn are more objective.

ENF, Electric Network Frequency, Audio

**B21 Car Speed From CCTV Images**

*Bart Hoogeboom, MS*, and Ivo Alberink, PhD, Netherlands Forensic Institute, Laan van Ipenburg 6, Den Haag, 2497 GB, NETHERLANDS

After attending this presentation, attendees will understand some principles of how to cope with measurement errors when performing the calculation of speed of a car from CCTV images and how to gain insight in the measurement errors.

This presentation will impact the forensic community by providing a better understanding of measurement errors in speed calculations from CCTV footage.

In forensic investigation, on a regular basis the question arises whether the speed of a car shown in a video can be determined. The video is usually obtained from a Closed Circuit Television (CCTV) system containing time lapse, black & white, or color recording.

The speed of the questioned car is calculated by measuring the path of the car between two images and calculating the time difference between the two images given the time by the CCTV system. To measure the path of the car between two images a three dimensional computer model from the road and characteristic points may be used. The model can be looked upon from the same perspective as the questioned images, and with the computer model projected on the questioned images the position of the car can be determined. As for every measurement in real life, there will be a difference between measured and real path, so measured paths, and time intervals accordingly, are always estimates for actual values. In this case study, two different situations are discussed: in the first case a car was recorded by two different cameras from the same CCTV system; in the second case a car was recorded by just one camera from a CCTV system. Those two different situations have been approached with different methods for gaining insight into the estimation errors.

In the first method, referred to as the stationary method, the errors made in the path and the time estimation are separated. To measure the path between two images from the two different cameras, a similar car was positioned at the scene of crime, at the position as can be seen in the questioned images. For this, the cameras that took the original video footage were repositioned using the questioned images. For both cameras, the positioning of the car was repeated by different operators, thus producing a variation around an average position per image. The different positions were measured using a land surveying device, and from the resulting drawing the paths between the positions were calculated. For the timing two clocks were started and recorded by the first camera. After this, without stopping the clocks, one clock was moved to the second camera and recorded. The recorded videos of the clocks were used to observe the difference in given time intervals by the CCTV system and the clocks. The variation in the observed errors of these time intervals and their paths were used to estimate a confidence interval for the calculated speed.

In the second method, referred to as the dynamic method, the estimation of the error made in the speed calculation is directly performed. Validation recordings from the same type of car, traveling with known speed along the path that was traveled by the car in the questioned video were made. For this, the same recording equipment was used as for the questioned video. These validation recordings of the car were made at different speeds, chosen around the estimated speed of the car in the questioned video. From the validation recordings the speed of the car was derived in the same way as for the questioned video. The difference between the calculated speed and the known speed was used to calculate the variation around the average difference. This variation was used to estimate a 95% confidence interval for the calculated speed.

CCTV, Photogrammetry, Statistics

**B22 3-Dimensional Analysis of Video Footage**

*Gerda Edelman, and Jurrien Bijhold, PhD*, Netherlands Forensic Institute, Laan van Ipenburg 6, Den Haag, 2497GB, NETHERLANDS

After attending this presentation, attendees will be familiar with methods for 3-D visualization based on video footage. This presentation will impact the forensic community by giving new insights on 3-D visualization based on video.

Video footage from CCTV, phonecams, etc. can be used to track, trace, and identify perpetrators. However, with the growing number of video recording devices, the amount of information increases rapidly. This makes it necessary to improve the process of capturing, converting, synchronizing, viewing, and analyzing video files. Surveillance images could be used more effectively with the help of 3-dimensional models of the scenes that are visible in the surveillance images.

First, virtual camera views in 3-D models can help to design a camera plan with an optimal coverage of the areas under surveillance. When these virtual camera views are matched with the real camera views, it becomes possible to estimate the position and speed of people and cars that are visible in the real video images.

With such information, it can be predicted when a person or car might show up in another camera. At the Netherlands Forensic Institute a project is being carried out to reconstruct all movements of people and cars before, during, and after a big incident from analysis of all available video footage.

In this presentation, a brief description of the project is given. Forensic aspects of the interpretation of video footage are demonstrated with video footage from a police investigation and a 3-D model of an urban area. The models are used as a tool for documenting observations in the video, combining these observations with other information sources, and for testing and documenting hypotheses on relations between events in different cameras.

3-D, CCTV, Video Footage

**B23 Quantifying Measurement Variation and Evidential Value When Performing Body Height Estimations in Digital Images**

*Ivo Alberink, PhD*, Bart Hoogeboom, MS, and Annabel Bolck, PhD, Netherlands Forensic Institute, Laan van Ipenburg 6, Den Haag, 2497 GB, NETHERLANDS

After attending this presentation, attendees will understand principles of how to cope with measurement errors when performing

* Presenting Author
body height measurements in images and how to quantify eventual evidential value.

In forensic practice, height estimations on perpetrators visible in video footage from surveillance cameras are regularly requested. The approach to this at the Netherlands Forensic Institute is the following: the crime scene is visited with a number of test persons. A Closed Circuit Television (CCTV) or camera image is selected in which the perpetrator is standing more or less in upright position. The test persons are positioned at the same location and in front of the same camera as the perpetrator on the original footage in as much as possible the same pose. This procedure is called a reconstruction and yields validation readings that allow to correct interpretation of height estimates of the perpetrator.

On the basis of 2-D photographs and fixed location points, a 3-D model of the scene of the crime is created. Using common points of the 3-D model and the camera view on the questioned image, the location and orientation of the camera is determined, and the 3-D model is projected such that it has the same perspective as the camera images. Next, investigators perform height measurements on the test persons and the perpetrator by placing cylinders over the bodies in the 3-D model, from feet to head. The height of the cylinders approximates the actual height of the test persons and perpetrator, reduced by the loss in height by the pose of the perpetrator. Variation between actual and measured heights of the test persons and the perpetrator is introduced by factors like creation of the 3-D model, finding of camera orientation and focal length, presence of lens distortion, pose of the perpetrator in the chosen image, presence and height of head- and footwear, interpretation of head and feet in the images by investigators. This variation may be decomposed into a systematic and a random part. By measuring reference objects in the image, like measuring sticks, an estimate of the systematic error by variation in the modeling of the crime scene can be made. Systematic error by varying height loss because of pose cannot be estimated directly. In practice (casework), systematic errors amount to several centimeters and vary from case to case. Since variation introduced by head- and footwear cannot be removed without extra knowledge, height measurements are usually of the test persons and the perpetrator including head and footwear.

The goal is to answer the following two questions:

1. On the basis of the measurements, how can probability statements be given (confidence intervals) on the actual height of the perpetrator?
2. In case there is a suspect: what is the evidential value, in terms of a Likelihood Ratio, of eventual resemblance of suspect’s and perpetrator’s height?

These questions have not received much attention in the literature, which has focused more on technical methods than validation. Using normal approximations and the observed variation on test persons, a method is described for obtaining confidence intervals for the height, including head- and footwear, of the perpetrator. Since the number of test persons is usually limited, the result is in terms of the Student-t distribution. In addition, an expression is obtained for the Likelihood Ratio, measuring the strength of evidence of resemblance of the actual height of a suspect and the measured height of the perpetrator. This depends both on the rarity of the estimated perpetrator’s height and on its closeness to the suspect’s height. The analysis of validation measurements described in the current paper does not depend on the method used and holds up as well if measurements are made on the basis of projective geometry (vanishing points).

Evidential Value, Body Height Estimation, Confidence intervals

---

**B24 Face Recognition on CCTV Material Using a Biometric System: Limitations and Opportunities**

Arnout C. Ruifrok, PhD*, Netherlands Forensic Institute, Laan van IJsendorp 6, Den Haag, 2497 GB, NETHERLANDS

After attending this presentation, attendees will have a better insight in the limitations and possibilities of automated biometric systems for facial identification using CCTV material.

This presentation will impact the forensic community by qualifying some of the claims made by facial recognition systems.

Biometric face recognition is still advocated as a good option for person identification and detection of people on watch lists. However, the current state of the art in face recognition is mostly not sufficient for forensic applications. Although some of the techniques reach reasonably high levels of recognition under controlled circumstances with frontal face images, of course, surveillance images hardly ever capture a suspect frontal face, with good lighting conditions, and a neutral facial expression. Also sharpness and resolution are, in general, far from optimal. Of interest to the forensic use of biometric systems is knowledge about the reliability of the matching results, even under imperfect conditions.

The performance of face recognition software was studied using surveillance images from six different analog cameras and camera-positions. The surveillance material was recorded at 4CIF (704x576 pixels) at 12 frames per second. Volunteers were asked to walk along a predefined path and stop walking and look left and right at 4 positions. The frontal-most images at each position were selected for the analysis. Verification match results were used to construct receiver-operator curves (ROC), and the Equal Error Rate (EER), error rate at the setting resulting in equal rates of false accepts and false rejects was used as performance criteria.

When using good quality controlled lighting and frontal pose images, an EER of 1.5% can be reached using automated face recognition software. However, when using passport-type but less controlled entrance-card images, the EER increased to 9%. Even with cameras at eye-height and fully zoomed-in the EER increased to 24-30% at distances of 1.5-3.5 m. When the subjects were wearing a baseball cap, EER increased 4-10% compared to bare-headed images. Images from a teller-machine like camera position performed relatively well. These images resulted in an EER of 16% with people looking into the camera, but performance dropped to an EER of 37% when people looked straight ahead, when a database of high quality controlled frontal images was used. However, when a database with images from a similar low position camera was used, the EER improved to 19% for the teller-machine images with people looking straight ahead and to 9% when people looked straight into the camera. At almost all camera positions the use of a reference database with images from the same camera position outperformed the use of full frontal images as reference database. This indicates that full frontal images are not always the best reference set for automated face recognition. Preferably images from the same camera and position should be used.

The absolute match-values generated by the recognition software should be viewed with care, as low quality images compared to a low quality database resulted in high match-values for matching as well as mismatching images, with high EER values as consequence. The data even suggests that the mismatch-values of an image with a database of images of a similar quality may be predictive of the EER of the system. This means that the evidential value of an image may be predicted by the mismatch value with images of similar quality, providing the opportunity to establish the evidential value of the CCTV image without suspect information.

Facial Recognition, CCTV Images, Biometrics

---

* Presenting Author
B25  A Morphological Classification of Eyebrows to Aid in Forensic Facial Comparisons

Matthew E. Graves, MFS*, Carl R. Krügel, BS, and Cristy B. Pruitt, MFS, U.S. Army Criminal Investigation Laboratory, 4930 North 31st Street, Forest Park, GA 30297

After attending this presentation, attendees will learn about a facial identification study that supports photographic comparisons as a part of image analysis. In facial identification research, there is very little information pertaining to the uniqueness of eyebrow features to be used in support of facial identification. The basis for conclusions reached through photographic comparison lies in the detection of correspondence or discordance of subject features. At the end of the presentation, the attendees will understand how eyebrow features can be used to support forensic facial comparisons and image analysis examinations. After attending this presentation, attendees will also understand the three main methodologies for forensic facial comparisons. Eyebrow classification based on morphological characteristics for facial comparisons will also be discussed. In addition, the various aspects of the eyebrow that were visualized to create a classification system will be presented along with the results of classifying 112 sets of eyebrows. Finally, further research possibilities in this area will be suggested.

This presentation will impact the forensic community by providing a methodology for the examination of eyebrows when performing forensic facial comparisons or identifications.

The goal of this study was to photograph approximately 100 individuals and then perform side-by-side photographic comparisons to determine if the eyebrow contained individual characteristics to suggest they are unique. In order to evaluate the uniqueness of eyebrows and the morphological characteristics they possess, it was necessary to develop a database of facial images for examination. For this project, 112 individuals volunteered to be photographed. Each photograph was categorized according to general shape, arch height and size (the width of the eyebrow in this instance). While grouping the images, the number of subsets containing distinct characteristics made it rare if any two eyebrows fell into the same category, and many other features were observed that could prove beneficial in determining eyebrow uniqueness. Therefore, the various characteristics were arranged into a table listing each category and an eyebrow classification. The observable features were then assigned a numerical value within each group.

After evaluating each of the 112 photographs and a total of 224 eyebrows, a spreadsheet containing the classification of each image was compiled. Based on the “Eyebrow Classification Table” developed, there were a total of 17 areas examined to aid in classifying each individual’s eyebrows. The spreadsheet depicts that from the 112 individuals who were studied in this project, no two sets of eyebrows classified the same way. Upon analyzing the results obtained from this study, eyebrows appear to be an area that, when adequately examined, may prove valuable as a piece of the puzzle for facial identifications. Since no two individuals’ eyebrows were found to be similar in this study, the utilization of a classification system should aid examiners in developing a universal terminology and methodology for the evaluation of eyebrows for individualization.

While all of the classifications of the eyebrows of 112 individuals in this study were found to be unique, there is still much research that must be completed in order to more thoroughly evaluate this method for use as a facial comparison tool. Future research on this topic may include studies on intra-assessor agreement, photographic variables, the effects of facial expressions on eyebrow characteristics, changes in eyebrows over time, and numerous other possibilities.

Overall, the eyebrow area appears to be a region of the face that is distinguishable between individuals. While eyebrow identification cannot and should not be used as a stand-alone source of individualization, when used in conjunction with other methods of facial comparison, it could prove to be extremely useful. The classification system developed may prove beneficial as a starting point for an examiner attempting to identify an individual from a photograph. In the future, it may be possible to create charts and overlays of standards depicting what constitutes various shapes and sizes of eyebrows. Through training, experience, and with the help of exemplar images depicting various characteristics, examiners throughout the forensic science community will become more accustomed to the examination of eyebrows when performing forensic facial comparisons.

Morphology, Classification, Facial Identification

B26  Future Tools for Forensic Digital Audio Analysis

Kenneth Marr, MS*, David J. Snyder III, BS*, and William L. Hinton, BS*, Federal Bureau of Investigation - FAVIAU, ERF - Building 27958A, Quantico, VA 22135

After attending this presentation, attendees will understand the changing nature of forensic audio tools and analysis. In addition, attendees will realize that Digital and Multimedia sub-disciplines will have an increasing share of common training, forensic tools, and examination requirements.

This presentation will impact the forensic community, especially the sub-disciplines of computer forensics, forensic audio, video, and image analysis, by showing that interdisciplinary communication and cooperation concerning training and forensic tools are vital and will significantly improve future examinations.

The toolbox for the forensic audio examiner of the future will contain an increasing number of computer forensic methods. A timeline is presented which details the accelerating pace of forensic audio technology and tool development. Current practitioners will recognize many tools and methods which, although important and considered cutting-edge when first developed, have been shelved for more accurate and applicable tools of today. These historical changes highlight the trend that new tools require not only additional qualifications and certifications but also more technical training for audio examiners. Computer hardware and software analysis, and automated technology will demand higher levels of education and technical degrees in order to explain examination results and implications of the findings to a jury in the courtroom. Issues of tool validation, calibration, and technical applicability are new hurdles that will become more prevalent and necessary when examination results are presented to more and more sophisticated courtroom judges and juries.

Training, qualifications, and laboratory accreditation will become more and more aligned with the field of computer forensics. With the incorporation of forensic audio as part of the Digital and Multimedia Sciences discipline, it is clear that a significant amount of computer forensics training is also needed for many aspects of forensic audio analysis. Only after a significant level of computer-related topics will the training divorce into separate “tracks” for the sub-disciplines of forensic audio, video, and image analysis.

Laboratory accreditation will become more prevalent and expected for both large and small forensic laboratories. This trend may cause a number of smaller facilities to stop forensic audio examinations due to the overhead costs of quality assurance programs, accreditation documentation (e.g., SOP’s), ongoing technical requirements, and maintenance costs of both hardware and software tools.

Enhancement of audio recordings now utilizes some powerful new techniques and methods which were not available in the past. New data processing techniques allow an examiner to view an entire audio file visually to identify areas of clipping or distortion, silence, abrupt changes in environment, and background noise levels, etc. The examiner

* Presenting Author
can then select and apply filtering techniques to the recording in a batch process which usually takes far less time than traditional aural review and filtering in real time. The future holds the likelihood that more sophisticated audio enhancement tools will allow examiners to be even more effective in less time than at any point in the past.

Nowhere has the shift in expectations involved in forensic audio been more profound than in audio authenticity examinations. Many traditional techniques are simply not applicable to today’s digital audio authenticity issues. These include magnetic development and physical inspection of analog evidence tapes. Newly designed methods to authenticate recorded files and identify any alterations have been implemented for some law enforcement digital recorders.

Other aspects of forensic audio analysis will also require specialized examination tools. These tools will apply to many aspects of forensic audio including enhancement, authenticity, voice comparison, automated gunshot detection and analysis, and possibly web-based voice surfing capabilities.

It is proposed that the development of any forensic analysis tool of the future must incorporate independent testing, validation, and certification of those tools. The forensic tool validation process must be timely and applicable. Some larger accredited laboratories already have established testing and validation procedures for new tools. Some of the necessary steps in this process include: (1) identification of potential new forensic tools, (2) researching the capabilities and credibility of the manufacturers or source of the new tools, (3) testing the functions and features of the new tools, comparing results to previous tools and to other standard audio discipline techniques, (4) validation of the new tool’s functions by an objective testing facility, and (5) certification and documentation of the new tool for use in forensic audio analysis.

An example for a digital audio authentication method designed for forensic examiners in the battlefield is the audio enhancement tool Avid Pro Tools®. This tool has been shown to be effective in the courtroom near real-time. It allows the examiner to apply various effects to the audio file, enhancing the signal-to-noise ratio, removing noise, and improving the clarity of the audio.

A computer forensics lab must be able to keep pace with the technology it analyzes, and it must allow investigators secure remote access to forensic tools. Virtualized hosts and virtualized storage, along with strong network encryption, allow organizations the flexibility for multiple investigators to collaborate using the same evidence, while using as many virtual forensic workstations as needed, with a storage system that can scale to hundreds of terabytes.

Virtualization technology is the abstract layer that resides between what is presented and the physical hardware. There are three core virtualized technologies needed to create a virtual lab environment: virtual private networks, virtual machines, and virtualized storage. A fourth (non-virtualized) component, two-factor identity management technologies, is also needed to create a secure and confidential lab environment. This technology can be applied to existing computer forensic labs to create a complete virtualized layer that still meets rigid ASCLD (American Society of Crime Laboratory Directors) requirements.

Digital Forensics, Virtual Digital Forensics, Virtual Lab

B28 The Persistence of Image Files on Digital Camera Memory Cards

Brian J. Gestring, MS*, Cedar Crest College, 100 College Drive, Forensic Science Program, Allentown, PA 18104

After attending this presentation, attendees will learn that it is possible to recover image files from digital camera memory cards after they have been erased and the card reformatted. A number of experiments will be described that illustrate how easy it is to recover these images with commercially available software. Mechanisms will also be discussed which prevent image recovery.

This presentation will impact the forensic community by demonstrating how standard operating procedures (SOPs) are essential for implementing a successful digital imaging platform. This presentation will alert users to the persistence of image files on digital camera memory cards and demonstrate how to effectively clear these cards. This information should be incorporated into any agencies SOP.

The dramatic improvement in digital imaging technology has led to growing acceptance of digital photography by both the law enforcement and forensic community. As the cost of a good single lens reflex (SLR) style camera continues to drop and the image quality for these digital SLRs (dSLRs) continues to increase, many agencies have elected to replace their traditional film applications with digital photography.

One fundamental difference encountered when switching from film to a digital platform involves the mechanism in which the images are initially recorded. With traditional film, the image is recorded as either a negative or positive (e.g., slide film) image. Since both of these are tangible, it is easier to physically and mentally keep track of them. With digital photography, images are recorded onto memory storage devices in the camera. Once these images are transferred from the card, the cards are cleared and reused again. Often users will utilize the “delete all” or “format card” feature on the camera to clear the cards in between uses. After either of these processes, no images will be visible on the card with either the camera or an external device. Unfortunately, this does not mean that the images are permanently deleted. There are a number of commercially available softwares that are very good at recovering image files from digital camera memory cards. Since the security of images taken for forensic science or other law enforcement applications is paramount, it is important to realize that even “empty” cards may contain images.

To evaluate the parameters where image files can be recovered, experiments were devised using a Nikon D200 dSLR with a 60 mm Micro Nikor lens and a new 2 GB 133 speed CompactFlash™ card. The
camera was set to ISO 100, auto white balance, and the quality was set to Raw + JPEG (large). Exposure was set manually based upon the TTL lens meter and was set to $f\ 3.2$ and $1/60$ for all the exposures. PowerPoint was used to make slides with the experiment title, name, and sequential numbering. Each slide was then photographed with the D200 mounted on a tripod.

For the first experiment 99 images were recorded to fill the card. The images were saved onto an external hard drive and then the “delete all” feature on the camera was used to clear the card. The card appeared blank when evaluated through the camera or a computer. Commercially available image recovery software was then used to analyze the deleted card and recover any possible images. All of the RAW and JPEG images were recovered with no loss in resolution.

Without the aid of the image recovery software, the “deleted card” still appeared blank. The card was then reformatted on the same digital camera. Again, the card appeared blank to the camera or a computer. Using the image recovery software, all of the RAW and JPEG images were recovered from the deleted and now reformatted card with no loss in resolution. This same card was then reformatted an additional six times. After each reformating, all of the original images were recovered with no loss in resolution.

In the second experiment 51 new images were recorded onto the deleted and reformatted card. The original images were stored onto an external hard drive and then the images were cleared from the camera using the “delete all” feature. All of the images from experiment 2 (RAW & JPEG) were recovered with the image recovery software as well as the last 46 RAW and JPEG images from experiment 1. There was no loss of resolution in any of the images.

A number of additional experiments were performed that fully evaluated the ability of the image recovery software to recover images off of cards thought to be empty. For those familiar with computers, it might not be surprising that deleted files can be recovered. Since the outward appearance of digital cameras still resembles that of their film ancestors, the fact that digital cameras are actually computers is often overlooked. Experiments such as these are necessary to define best practices and create standard operating procedures for digital photography.

Digital Photography, Memory Cards, Image Recovery