

Multiple Documents

Part	Description
1	Main Document
2	Exhibit A - 3/24/16 Letter from defense counsel
3	Exhibit B - 3/28/16 Email to defense counsel
4	Exhibit C - 4/15/16 Letter from defense counsel

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OHIO
EASTERN DIVISION

UNITED STATES OF AMERICA,) CASE NO.: 1:15-CR-00275
Plaintiff,)
v.) JUDGE DAN AARON POLSTER
JOHN CLEMENTS,)
Defendant.) GOVERNMENT'S MOTION FOR 30-
) DAY EXTENSION FOR INDEPENDENT
) TESTING BY DIGITAL, INC.

Now comes the United States of America, through its counsel, Carole S. Rendon, Acting United States Attorney, and Brian McDonough, Assistant United States Attorney, and respectfully moves this Court for a 30-day extension for independent expert Digital, Inc. to test the software in this case. Digital should have the independent testing completed within 30 days. Additional information is in the attached memorandum.

Respectfully submitted,

CAROLE S. RENDON
United States Attorney

By: /s/ Brian M. McDonough
Brian M. McDonough (OH: 0072954)
Assistant United States Attorney
United States Court House
801 West Superior Avenue, Suite 400
Cleveland, OH 44113
(216) 622-3965
(216) 522-2403 (facsimile)
Brian.McDonough@usdoj.gov

MEMORANDUM

I. Introduction

After reviewing Defendant's Motion to Suppress or, in the Alternative, Motion to Reconsider Defendant's Motion to Compel Discovery (Doc #: [22]), the Court held a teleconference on March 17, 2016, with Assistant United States Attorney Brian McDonough for the government and Attorney Eric Nemechek for Defendant to discuss the Motion. As a result, the parties agreed to confer and agree upon an independent person/entity to test the Shareaza LE software used in this case to determine if the software allows the user to access any part of a computer that is not otherwise publicly available -- and to do so within 30 days from today. As such, the Court denied the motion to suppress as premature.

From March 17th through March 24th counsel have researched independent experts/entities to perform the software testing in this case. On March 24th, defense counsel suggested Robert Young of Johnson-Laird, Inc. See Exhibit A. On Friday, March 25th, government counsel emailed defense counsel and wrote that the undersigned would research Mr. Young and update defense counsel. See Exhibit B. On March 28th, the undersigned telephoned defense counsel and informed him that Mr. Young's credibility had been called in to question in U.S. v. Lofthouse, where his testimony had been stricken. See Exhibit B. The government suggested Cigital, Inc. ("Cigital") as an independent expert. See Exhibit B. On the March 28th, government counsel emailed defense counsel with Cigital's website: <http://www.cigital.com>. To date, defense counsel has not objected to Cigital as the independent expert. Eighteen days later, on Friday, April 15th, defense counsel suggested that as an alternative to Robert Young, Dr. Marcus Rogers be selected as an independent expert. See Exhibit C. Given that the defense has

never objected to Digital, the government proposes that Digital perform the independent testing in this case under the analysis listed below.

II. Digital's Independent Testing of the Law Enforcement Software Used in This Case

Digital has its principal place of business at 21351 Ridgetop Circle, Suite 400, Dulles, Virginia, 20166. Digital can review the software source code and related scripts originally based on the LimeWire peer-to-peer networking protocols to automate searching for users distributing child pornography on the Gnutella network. Digital will review any changes made to LimeWire by the law enforcement software to determine whether it simply queries/gathers publicly known information, or whether it exploits vulnerabilities in the LimeWire based source code or supporting protocols to access Gnutella clients to gain access to information that may not be normally available.

Digital proposes the following analysis:

- Obtain LimeWire source code from a public repository, build it and ensure that it installs and runs. Document default file sharing settings in LimeWire.
- Obtain source code for the law enforcement software based on LimeWire, build it and ensure that it installs and runs.
- Determine which LimeWire files were added/deleted/modified by the law enforcement software using the following approaches:
 - Perform directory listings to determine which files have been added or deleted.
 - Generate a cryptographic hash of each file in both source trees. Determine which files have changed by looking at which files have different cryptographic hashes in the two source trees.

- For files that exist in both source trees, perform a ‘diff’ on both versions of the file to determine which ones have been modified. This will provide yet another mechanism to determine if any files have changed, and will also provide details about the exact changes that have been made by the law enforcement software.
- Analyze the list of changes gathered using the above techniques and manually review the relevant code to determine if or how LimeWire’s functionality has been altered.
- If, after performing the above steps, it appears that the law enforcement software only looks for normal information, Digital will run the version that was built earlier and ensure that it is capable of finding the types of information and/or files that the law enforcement software claims its tool can find (e.g. images in default directories). This is done to validate that law enforcement software provided source code executes queries and processes responses as expected.
- Run the law enforcement software, as well as unmodified LimeWire (the versions built earlier), and analyze network traffic generated by the two pieces of software. This is done to ensure that law enforcement software is not sending any traffic that could perform operations that LimeWire would never perform.

Using the above techniques, Digital will attempt to determine whether the following assertions are true:

- The law enforcement software does not exploit a vulnerability in any software.
- The law enforcement software does not misuse the protocols on the Gnutella network to do things that it was not intended to do.

- The law enforcement software does not change any configuration options in other users' software to extract information that would normally not be publicly available (e.g. it does not make other users' software share private parts of their filesystems).

III. Conclusion

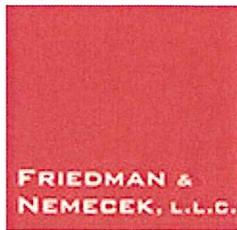
For the reasons stated above, the government moves this Court for a 30-day extension for independent expert Digital, Inc. to test the law enforcement software in this case.

CERTIFICATE OF SERVICE

I hereby certify that on this 18th day of April 2016, a copy of the foregoing document was filed electronically. Notice of this filing will be sent to all parties by operation of the Court's electronic filing system. All other parties will be served by regular U.S. Mail. Parties may access this filing through the Court's system.

/s/ Brian M. McDonough

Brian M. McDonough
Assistant U.S. Attorney



THE IMG CENTER
1360 EAST 9TH STREET, SUITE 650
CLEVELAND, OHIO 44114
TELEPHONE 216.928.7700
WWW.FANLEGAL.COM

Eric C. Nemecek, Esq.
ecn@fanlegal.com

March 24, 2016

SENT VIA EMAIL TO: Brian.McDonough@usdoj.gov

Brian M. McDonough, Esq.
Assistant U.S. Attorney
801 W. Superior Ave., Ste. 400
Cleveland, OH 44113

Re: *United States of America v. John Clements*
Case No. 1:15-cr-00275-DAP

Mr. McDonough:

I hope this letter finds you well. In an effort to comply with the Court's March 17th Order, I have been attempting to identify potential candidates to conduct an independent forensic examination of the Shareaza LE software. To that end, I have identified Robert Young, of Johnson-Laird, Inc., as being an expert who is highly qualified and independent from the parties or proceedings in this case. Mr. Young's qualifications and firm information can be found at <https://www.jli.com/people.htm>.

I have not contacted Mr. Young directly regarding this case or the independent examination ordered by the Court. However, I am certainly willing to discuss the matter with Mr. Young if you believe that he is an acceptable candidate. As such, please contact me at your earliest convenience to discuss this matter in greater detail, including your position regarding Mr. Young conducting the independent forensic examination of the Shareaza LE software in this case.

Thank you in advance for your prompt attention to this request. I look forward to speaking with you soon.

Very truly yours,

Eric C. Nemecek

cc: file

McDonough, Brian (USAOHN)

From: McDonough, Brian (USAOHN)
Sent: Monday, March 28, 2016 5:03 PM
To: 'Eric Nemecek'
Subject: RE: US v Clements

Eric,

As we discussed today, based on Robert Young's testimony being stricken in the Lofthouse case, the government proposes that Digital conduct the independent testing in this case. More information about Digital is available on its website: <https://www.digital.com/>

Thanks,

Brian M. McDonough
Assistant United States Attorney
Northern District of Ohio
United States Court House
801 West Superior Avenue
Suite 400
Cleveland, Ohio 44113
Telephone: (216) 622-3965
Cell: (216) 701-1586
Fax: (216) 522-8355
E-mail: Brian.McDonough@usdoj.gov

From: Eric Nemecek [mailto:ecn@fanlegal.com]
Sent: Monday, March 28, 2016 4:19 PM
To: McDonough, Brian (USAOHN)
Subject: RE: US v Clements

I should be free in about 10 minutes if that works for you. Cell or office are fine.

Thanks,

Eric C. Nemecek, Esq.

Friedman & Nemecek, L.L.C.
The IMG Center
1360 E. 9th Street, Suite 650
Cleveland, Ohio 44114
P: 216.928.7700
E: ecn@fanlegal.com



Friedman & Nemecek, L.L.C. - Confidential Communication

This transmission contains confidential information intended only for the addressee(s) and may also be privileged and/or subject to attorney work-product protection. If you are not the intended recipient, any use, dissemination, distribution, or copying of this document or its contents is strictly prohibited. If you receive this message in error, please contact the sender immediately either by return E-mail or by telephone at (216) 928-7700. Thank You.

From: McDonough, Brian (USAOHN) [<mailto:Brian.McDonough@usdoj.gov>]
Sent: Monday, March 28, 2016 4:04 PM
To: Eric Nemecek
Subject: RE: US v Clements

That works. Are you free now?

Brian M. McDonough
Assistant United States Attorney
Northern District of Ohio
United States Court House
801 West Superior Avenue
Suite 400
Cleveland, Ohio 44113
Telephone: (216) 622-3965
Cell: (216) 701-1586
Fax: (216) 522-8355
E-mail: Brian.McDonough@usdoj.gov

From: Eric Nemecek [<mailto:ecn@fanlegal.com>]
Sent: Friday, March 25, 2016 4:54 PM
To: McDonough, Brian (USAOHN)
Subject: RE: US v Clements

Ok. I have a 1:00 meeting on Monday, but I should be done around 3:30 or so. Any time after that should be fine. Have a good weekend.

Thanks,

Eric C. Nemecek, Esq.

Friedman & Nemecek, L.L.C.
The IMG Center
1360 E. 9th Street, Suite 650
Cleveland, Ohio 44114
P: 216.928.7700
E: ecn@fanlegal.com



Friedman & Nemecek, L.L.C. - Confidential Communication

This transmission contains confidential information intended only for the addressee(s) and may also be privileged and/or subject to attorney work-product protection. If you are not the intended recipient, any use, dissemination, distribution, or copying of this document or its contents is strictly prohibited. If you receive this message in error, please contact the sender immediately either by return E-mail or by telephone at (216) 928-7700. Thank You.

From: McDonough, Brian (USAOHN) [<mailto:Brian.McDonough@usdoj.gov>]

Sent: Friday, March 25, 2016 2:54 PM

To: Eric Nemecek

Subject: RE: US v Clements

Eric,

Thanks for the email and letter. I will review it. Let's talk on Monday afternoon.

Thanks,

Brian M. McDonough
Assistant United States Attorney
Northern District of Ohio
United States Court House
801 West Superior Avenue
Suite 400
Cleveland, Ohio 44113

Telephone: (216) 622-3965

Cell: (216) 701-1586

Fax: (216) 522-8355

E-mail: Brian.McDonough@usdoj.gov

From: Eric Nemecek [<mailto:ecn@fanlegal.com>]

Sent: Thursday, March 24, 2016 6:15 PM

To: McDonough, Brian (USAOHN)

Subject: US v Clements

Brian,

I hope all is well. Please see the attached letter in reference to the testing of the Shareaza LE software.

Thanks,

Eric C. Nemecek, Esq.

Friedman & Nemecek, L.L.C.

The IMG Center

1360 E. 9th Street, Suite 650

Cleveland, Ohio 44114

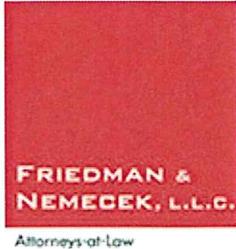
P: 216.928.7700

E: ecn@fanlegal.com



Friedman & Nemecek, L.L.C. - Confidential Communication

This transmission contains confidential information intended only for the addressee(s) and may also be privileged and/or subject to attorney work-product protection. If you are not the intended recipient, any use, dissemination, distribution, or copying of this document or its contents is strictly prohibited. If you receive this message in error, please contact the sender immediately either by return E-mail or by telephone at (216) 928-7700. Thank You.



THE IMG CENTER
1360 EAST 9TH STREET, SUITE 650
CLEVELAND, OHIO 44114
TELEPHONE 216.928.7700
WWW.FANLEGAL.COM

Eric C. Nemecek, Esq.
ecn@fanlegal.com

April 15, 2016

SENT VIA EMAIL TO: Brian.McDonough@usdoj.gov

Brian M. McDonough, Esq.
Assistant U.S. Attorney
801 W. Superior Ave., Ste. 400
Cleveland, OH 44113

Re: *Independent Testing of Shareaza LE Software in Clements*

Mr. McDonough:

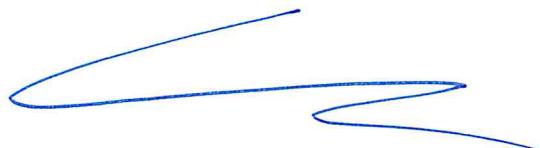
I hope this letter finds you well. Since you expressed concerns regarding Mr. Young performing the independent examination of the Shareaza LE software in this case, I have been trying to identify alternative and disinterested experts to assist with the software analysis. To that end, I have identified Dr. Marcus ("Marc") Rogers as a potential expert witness to perform the testing in this case. Dr. Rogers is the head of cyber forensics at Purdue University. In addition to working in the private sector, Dr. Rogers is also involved with forensic training for a number of law enforcement agencies throughout the United States, including the N.S.A. I am including a copy of Dr. Rogers' CV with this letter for your review.

I recently sent an email to Dr. Rogers with general information about this matter: namely, the fact that this was a child pornography case and that the Court has issued an Order authorizing independent testing of the propriety law enforcement software used during the undercover investigative stage. Apart from these general issues, I have not discussed any substantive information regarding the issues, arguments or underlying case facts, nor have I provided him with the case name/caption or the specific software herein at issue. Dr. Rogers sent me an email yesterday evening and expressed his interest in assisting with the independent testing in this case. He indicated that his first availability to discuss the specific issues in the case, including the independent testing, would be on Monday, April 18th, in the afternoon. If Dr. Rogers is an acceptable candidate, I can schedule a teleconference for a time next week that is mutually convenient for all parties.

Also, in light of the thirty (30) day deadline set forth in the Judge's Order, it might be a good idea to contact the Court to advise them that we are still in the process of selecting an expert witness. Looking ahead, we will also need to determine the specific parameters and procedures for the testing process.

Thank you in advance for your prompt attention to this request. I look forward to speaking with you soon.

Very truly yours,

A handwritten signature in blue ink, appearing to read "Eric C. Nemecek, Esq."

Eric C. Nemecek, Esq.

*cc: file
Enclosure(s)*

Marcus K. Rogers

4710 N 225 W Phone: (765) 560-3290
West Lafayette, IN 47907-2039 Email: rogersmk@icloud.com
URL: <http://www.cyberforensics.purdue.edu>
Citizenship: Canadian Status: Permanent Resident – Green card

Education:

- | | |
|------|---|
| 2001 | Ph.D. Psychology , Forensic Psychology, University of Manitoba |
| 1997 | Diploma, Telecommunications and Internet Fraud investigations , Canadian Police College, Ottawa. |
| 1996 | Diploma, Electronic Search and Seizure , Canadian Police College, Ottawa |
| 1995 | M.A. Psychology , Personality, University of Manitoba |
| 1986 | Diploma, Law Enforcement , Winnipeg Police Academy, Winnipeg |
| 1986 | B.A. Psychology/Criminology , University of Manitoba |

Appointments:

- | | |
|--------------|---|
| 2015-Present | Department Head, Computer & Information Technology, Purdue Polytechnic Institute, Purdue University. |
| 2014-2015 | Interim Department Head, Computer & Information Technology, College of Technology, Purdue University. |
| 2014-2015 | Visiting Endowed McDevitt Chair in Computer Science, LeMoyne College. |
| 2014-Present | Director Cyber Forensics & Security Program, College of Technology, Purdue University. |
| 2013-Present | Senior Cyber Forensics Advisor – DOJ International Criminal Investigative Training Assistance Program (ICITAP). |
| 2013-2014 | Associate Department Head, Computer & Information Technology |
| 2012-Present | Departmental Chair – PhD Committee. |
| 2011 | Special Investigator – Prosecutor’s Office Tippecanoe County (Sworn Law Enforcement). |
| 2010 | Chair: College of Technology Faculty Grievance Committee, Purdue University. |
| 2009 | Chair: College of Technology Faculty Grievance Committee, Purdue University. |
| 2008 | Chair: College of Technology Faculty Grievance Committee, Purdue University. |
| 2007-Present | Professor: Department of Computer and Information Technology, College of Technology, Purdue University. Faculty Lead: Cyber Forensics Program. |

2004-2006	Associate Professor: Department of Computer and Information Technology, College of Technology, Purdue University. Faculty Lead: Cyber Forensics Program.
2003-2004	Courtesy Appointment – Assistant Professor: Purdue University, School of Technology, Computer Technology Department

Honors and Awards:

2014	Visiting McDevitt Endowed Chair in Computer Science – LeMoyne
2014	AAFS Digital & Multimedia Sciences Section Outstanding Case Study Award
2013	AAFS Digital & Multimedia Sciences Section Outstanding Research Award
2012	Pillar of CERIAS
2012	Fellow American Academy of Forensic Sciences
2009	Fellow of CERIAS
2009	Paul H. Chapman Award, Foundation for Improvement of Justice
2008	University Faculty Scholar
2007	International Association of Chiefs of Police -iXP Excellence in Technology Award (Collaboration with Indiana State Police)
2006	Lafayette Police Department Award/commendation
2006	Outstanding Non-tenured Faculty Award: Computer Technology
2005	Outstanding Non-tenured Faculty Award: Computer Technology
2005	Best Research Poster: School of Technology Faculty Convocation
2005	West Coast Security Conference 2005 - Best Presenter
2003	Industry and Technology Canada, Education and Internet Innovators Award-Manitoba
2002	Industry and Technology Canada, Education and Internet Innovators Award-Manitoba.
2001	West Coast Security Conference 2001- Best Presenter
1997	Winnipeg Police Association Scholarship
1996	University of Manitoba Doctoral Fellowship (declined)
1996	Winnipeg Police Association Scholarship
1995	Winnipeg Police Association Scholarship

Professional Association Memberships:

- American Academy of Forensic Sciences (AAFS) Digital & Multimedia Sciences (DMS) – Section Secretary
- INFRAGARD - FBI
- ASTM - International
- American Bar Association - Associate (ABA) – Science and Technology Law
- Past - Scientific Working Group on Digital Evidence (SWGDE)
- American Association of University Professors (AAUP)
- Computer Forensic Educator's Working Group (CFEWG)
- American Psychological Association (APA)
- High Tech Crime Network (HTCN)
- American Psychology-Law Society (APLS)
- Certified Information Systems Security Professional (CISSP)

Committees:

- NIST OSAC Digital Evidence, 2014
- Chair NIST OSCAC Digital Evidence Education Sub-Committee, 2014
- General Chair: ICST Conference on Digital Forensics & Cyber Crime, Purdue, 2012
- Co-Chair Technical Committee: ICST Conference on Digital Forensics & Cyber Crime, Dublin Ireland, 2011
- Technical Program Committee: Security and Forensics in Communication Systems (IEEE SFCS 2012).
- Scientific Program Committee: International Conference on Information and Telecommunication Technologies in Forensics (ICTinForensics 2011), Salvador, Bahia, Brazil
- Program Committee ACM SAC, 2011
- Scientific Program Committee, ICST Conference on Digital Forensics & Cyber Crime, Abu Dhabi, 2010
- Digital Forensics Certification Board - Past Chair, Certification Committee (DFCB)
- American Academy of Forensic Science (AAFS) – Digital Evidence - Chair, Planning Committee
- Common Digital Evidence Format Working Group (CDEF)
- (ISC)2 SCCP Quality Control and Review Committee
- International Chair – (ISC)2 Common Body of Knowledge Review Committee – Law Compliance and Investigation Domain
- Digital Forensics Research Workshop
- Member – Scientific Working Group on Digital Evidence
- SC Magazine International Awards Committee – International Judge
- Committee Member – Electronic Crime Partnership Initiative (ECPI) NIJ
- IFIP Working Group on Digital Evidence Section 11.9
- Technical Program Committee – International Conference on Digital Forensics & Cyber Crime
- Scientific Approaches in Digital Forensic Engineering: Program Committee

Editorial Boards:

- Editor - Cybercrime Department IEEE Security & Privacy
- Editorial Advisory Board - Security, Privacy, and Digital Forensics in the Cloud: Wiley
- Board Member - Scholarena Journal of Forensic Science
- Board Member – Journal of Forensic Investigation (Avens)
- Associate Editor - Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Heidelberg, Germany: Springer-Verlag Science & Business.
- Associate Editor - Journal of Digital Forensics, Security and Law
- Consulting Editor – Cyber Safety “the Series” (Chelsea House)
- Former Editor-in-Chief - Journal of Digital Forensic Practice (Taylor & Francis)
- Former member -Editorial Advisory Board – Encyclopedia of Forensic Sciences (Elsevier)

- Former Co-Editor-in -Chief – Encyclopedia of Information Assurance (Auerbach)
- Editorial Advisory Board – Information Assurance and Security Ethics in Complex Systems: Interdisciplinary Perspectives (IGI Global)
- Editorial Board – International Journal of Digital Evidence
- Editorial Board – International Journal of Cyber Crimes and Criminal Justice
- Editorial Advisory Board – SC Magazine
- Editorial Board – Information Security Journal: ISC2 Journal
- Editorial Board – Computers and Security

Advisory Boards:

- Chair Advisory Committee - Digital Forensics Certification Board
- Consortium of Digital Forensic Specialists (CDFS) (Past member)
- Digital Forensics Certification Board (Past member)
- University of Colorado Denver, National Center for Media Forensics
- University of Winnipeg, Department of Continuing Education, Information Security Program (Past member)
- Purdue Employees Federal Credit Union (PEFCU) Supervisory Board
- Champlain College, Masters in Computer Forensics (Dept. of Business Administration) (past member)
- Defiance College Cyber Forensics Program (past member)

Reviewer:

- External Reviewer – British Columbia Institute of Technology (BCIT) Forensic Sciences Program
- University College Dublin
- Rhode Island Research Alliance
- International Conference on Politics and Information Systems
- IEEE Transactions on Information Forensics & Security
- Swiss National Science Foundation – Expert Reviewer
- Kentucky Engineering & Science Foundation
- Information Security Journal
- Cambridge University Press
- Thompson Publications – Technical Reviewer
- Digital Forensics Research Workshop (DFRWS)
- Wiley & Sons, Encyclopedia of Information Security
- U.S. Civilian Research & Development Foundation (CRDF)
- Maryland Technology Development Corporation (TEDCO)
- NIST, Incident Response Guide SP-800 series.
- NIST, Computer Forensics Guide SP-800 series.
- Handbook of Information Security, Bidgoli, H. (Ed.). Wiley & Sons
- National Institute of Justice (NIJ): Curriculum Guidelines for Digital Forensics
- National Institute of Justice (NIJ): White Collar & Cyber Crime Grants Education
- Pearson Education
- Elsevier
- SUNY Buffalo NSA SFS Program – external reviewer
- Qatar National Research Fund

Certifications:

- AccessData Certified Examiner (ACE)
- Notary State of Indiana
- Digital Forensics Certified Practitioner – Founder Level, Digital Forensics Certification Board
- FTK Vista Forensics, Access Data
- Cyber Cop 102 – Automated Forensic Tools (AFT), National White Collar Crime Center
- Certified Computer Crime Investigator – Advanced (CCCI), High Tech Crime Network
- Certified Information System Security Professional (CISSP), ISC²
- Basic Data Recovery and Analysis (BDRA), National White Collar Crime Center
- Advanced Data Recovery and Analysis (ADRA), National White Collar Crime Center
- Access Data Boot Camp

Teaching Experience:

2013	Digital Forensics for Law Enforcement – 5 Day Training (Zagreb, Croatia)
2013	Basic Mac Forensics for Law Enforcement – 3 Day Training (Purdue)
2013	Digital Evidence Triage – 3 Day training seminar (Purdue)
2012	Advanced Mac Forensics for Law Enforcement – 3 Day training seminar (Albany , NY)
2011	Digital Evidence Triage – Law Enforcement Training – 3 Day Training Seminar (St. Louis)
2010	Introduction to Mac Forensics for Law Enforcement – 3 Day training seminar (Purdue)
2010	Advanced Mac Forensics for Law Enforcement – 3 Day training seminar (Purdue)
2010	Introduction to Mac Forensics for Law Enforcement – 3 Day training seminar (Albany, New York)
2009	Digital Evidence Triage - Financial Services Training – 3 Day Training Seminar (Purdue)
2009	Digital Evidence Triage – Law Enforcement Training – 3 Day Training Seminar (Purdue)
2009	Digital Evidence Triage – Law Enforcement Training – 3 Day Training Seminar (Vermont)

- 2009 Digital Evidence Triage – Law Enforcement Training – 3 Day Training Seminar (Boston)
- 2009 Digital Evidence Triage – Law Enforcement Training – 3 Day Training Seminar.
- 2008 Cyber Forensics Triage – DOJ US Attorney's Office, Los Angeles – 3 Day Training seminar.
- 2008 *Digital Evidence Management* – (ISC)2 Secure Baltimore – 1 Day Baltimore, MD.
- 2008 Introduction to Mac Forensics for Law Enforcement – 3 Day training seminar.
- 2007 LE Digital Investigations Boot Camp – Purdue, 3 Day Law Enforcement Training.
- 2007 Emerging Trends in Digital Investigations – Purdue, 1 Day Law Enforcement Training.
- 2007 Digital Evidence Management and Handling, Management and practitioners training (ISC)2 – 1 Day Chicago, IL.
- 2006 Digital Evidence Management and Handling, Social Engineering, Management and practitioners training (ISC)2. University of Tokyo – 1 Day Los Angeles, CA.
- 2006 Digital Evidence Management and Handling, Management and practitioners training (ISC)2 – 1 Day Boston, MA.
- 2005 Digital Evidence Management and Handling, Management and practitioners training (ISC)2 – 1 Day Durham, NC.
- 2005 Digital Evidence Management and Handling, Management and practitioners training (ISC)2 – 1 day Austin Texas.
- 2005 Fast Computer Forensics Triage (NW3C & Indiana State Police) – 3 Day training for LE investigators, Purdue.
- 2005-Present College of Technology, Computer Technology Department, Purdue University – Basic Computer Forensics, Advanced Research Topics in Cyber forensics.
- 2004 Email Forensics, Law Enforcement Training (NW3C & Indiana State Police) – 1 day training for LE investigators, Indianapolis, IN.
- 2004 Computer Forensics First Responder Course, Law Enforcement Training (NW3C & Indiana State Police) – 3 day LE training course, Purdue.
- 2004 Information Assurance Education Graduate Certificate Program (Purdue University) – Advanced topics in Information Assurance; cyber-criminalistics.

- 2004 DND ISSO Conference – 2 Day, Network Safeguards and Counter Measures. Cornwall Ontario.
- 2004 School of Technology, Computer Technology Department, Purdue University-Introduction to Computer Forensics.
- 2003 DnD ISSO Conference - 3 Day Incident Response and Evidence Management course. Cornwall Ontario.
- 2003 Information Assurance Education Graduate Certificate Program (Purdue University) – Advanced topics in Information Assurance; cyber-criminalistics.
- 2002 North American Air Defense (NORAD) - Incident Response Methodology course.
- 2002-2003 University of Winnipeg - Continuing Education, Course Design and teaching of 4 core courses: Introduction to Information Security, Cryptography & Encryption, Network & Remote Access concepts (Firewalls, VPN, IDS), Incident Response & Forensic Friendly Procedures.
- 2000-2002 University of Manitoba- Introduction to Psychology: Continuing Education High-school Pilot Program, full term Regular Session.
- 2000 University of Winnipeg- Psychology of the Computer Criminal: Guest Lecturer: Fall Semester.
1996. BC Justice Institute-Computer and Information Security: Computer Crime and Investigations: Winnipeg Police College
- 1993 University of Manitoba- Teaching Assistant: Environmental Psychology
- 1992 University of Manitoba- Teaching Assistant: Stress

Research, Service, and Consulting Experience:

- 2007- Present Professor of Cyber Forensics. Computer & Information Technology Department, Purdue University.
- 2004–2006 Associate Professor of Cyber Forensics. Computer Technology Department, Purdue University.
- 2003-Present Research Scientist -Cyber Forensics. Center for Education and Research in Information Assurance and Security (CERIAS), Purdue University.
- 2002 Principal Researcher, Information Assurance & Security. Internet Innovation Centre, Faculty of Engineering, University of Manitoba.
- 2002 SANS, Development and authoring of the Social Engineering component of the SANS Core Essentials Information Security training certification

course

2001. Ph.D. Thesis: A Social Learning Theory and Moral Disengagement Analysis of Criminal Computer Behavior: An Exploratory Study.
- 2001 ISC², Development and authoring of the Forensics-Incident Response component of the Certified Information Systems Security Professional review course.
- 1997-99 Consultant, several international banks (confidentiality and non-disclosure agreements in effect) E-commerce and Network Security.
1997. Consultant, BC Justice Institute and BC Institute of Technology Forensic Sciences Program.
- 1995 M.A. Thesis: Understanding Police Burnout: A Salutogenic Approach
- 1993-2001 Board Member, AGASSIZ Institute for Conflict Studies, University of Manitoba.
- 1991 Honors Thesis: Accuracy of Eyewitness Testimony

Employment:

2010 –Present MKR Forensics LLC

President and CEO, Digital evidence and digital crime scene analysis, examination and expert testimony.

2004-Present

(Faculty) Computer & Information Technology Department, College of Technology, Purdue University.

2003-present Purdue University

Research Scientist, Center for Education and Research in Information Assurance and Security (CERIAS).

2002-2003 University of Manitoba

Principal Researcher, Information Assurance & Security, Internet Innovation Centre, Faculty of Engineering, University of Manitoba. Conduct research on the human/societal interaction with technology, emphasis on deviant computer behaviors, and cyber-terrorism.

2002-2003 University of Winnipeg

Lecturer and course design, Continuing Education, Network Security Diploma program

2000 –2002 Deloitte & Touche LLP

Director Forensic Computing and Secure eBusiness, Duties: Leader of the Manitoba Office for E-Business Security, National Director-Lead SeB Forensic Computing services. IT security consulting, network security reviews, intrusion and penetration

testing, risk analysis, policy development, security awareness and security assurance programs, PKI, forensic data analysis, and research.

2001 University of Manitoba

Lecturer, Department of Psychology University of Manitoba, Winnipeg, Canada.

Teaching introductory psychology.

2000-2010 ISC2 (CISSP)

Lead Instructor for the ISC2 Certified Information Systems Security Professional (CISSP) review and preparation course. Member of the QA team for SSCP Designation.

1999-2000 EDS Systemhouse

Senior Security Technical Architect, Duties: Coordinator and lead security architect for the Canadian Information Security Practice. IT security consulting, network security reviews, intrusion and penetration testing, risk analysis, policy development, security awareness and security assurance programs, PKI, and security research.

1999 Director Information Protection Center Province of Manitoba

Chief Security Officer for the Province. Duties included supervising staff, network security reviews, intrusion and penetration testing, risk analysis, policy development, security awareness and security assurance programs, PKI, security research, response escalation and incident investigation. Member of the Architecture Review Board for the Province

1998-99 SHL Systemhouse

Senior Security Technical Architect, Duties: Coordinator and lead security architect for the Canadian Information Security Practice. IT security consulting, network security reviews, intrusion and penetration testing, risk analysis, policy development, security awareness and security assurance programs, PKI, and security research.

1997-98 Vancouver Stock Exchange

Technology Information Security Officer, Duties: risk analysis, policy development, security awareness training and education, intrusion testing, enterprise wide information security monitoring, security consulting on project development, project management, application testing and evaluation, EDP system auditing.

1986-98 Winnipeg Police Service

Lead Detective Commercial Crime, Computer/Technological Crimes Unit. Promoted to Detective. Duties: develop the Computer/Technological Crimes Unit, investigate computer related frauds, child pornography, corporate espionage, software piracy, credit card frauds, network attacks, and act as a consultant to other municipal and federal law enforcement agencies, and legislators.

Expert Witness Status

- US Federal Court (Criminal) - Indiana
- US Federal Court (Criminal) – Kentucky
- Illinois State Court (Criminal)
- Federal Court (Criminal) - Canada

Amicus Curiae Briefs:

United States v. Andrus, F.3d (10th Cir. 2007). BRIEF OF AMICI CURIAE COMPUTER FORENSICS RESEARCHERS AND SCIENTISTS IN SUPPORT OF APPELLANT AND REVERSAL OF THE DENIAL OF THE MOTION TO SUPPRESS

Publications:

Gupta, S., & Rogers, M. (2014). Exploring forensic implications of the fusion drive. *The Journal of Digital Forensics, Security, and Law*, 9 (2), 145-154.

Rogers, M. & Seigfried-Spellar, K. (2014). Using internet artifacts to profile a child pornography suspect. *Journal of Digital Forensics Security and Law*, 9 (1), 57-66.

Rogers, M. (2014). Modern-day Robin Hood or moral disengagement: Understanding the justification for criminal computer activity. In K. Seigfried-Spellar & M. Lanier (Eds), *Essential Readings in Cybercrime Theory and Practice* (pp. 147-152). San Diego, CA: Cognella.

Rogers, M. (2014). Cybercriminal taxonomies. In K. Seigfried-Spellar & M. Lanier (Eds), *Essential Readings in Cybercrime Theory and Practice* (pp. 31-42). San Diego, CA: Cognella.

Seigfried-Spellar, K. & Rogers, M. (2013). Does deviant pornography use follow a Guttman-Like progression? *Computers and Human Behavior*, 29 (2013), 1997-2003.

Gladyshev & M. Rogers (Eds.). (2012) *Digital Forensics and Cyber Crime*, Third International ICST Conference, ICDF2C 2011, Dublin, Ireland, October 26-28, 2011, Revised Selected Papers. Heidelberg, Germany: Springer-Verlag Science & Business.

Levendoski, M., Datar, T., & Rogers, M. (2012). Yahoo! Messenger forensics on Windows Vista and Windows 7. In P. Gladyshev & M. Rogers (Eds), *Digital Forensics and Cyber Crime*, Third International ICST Conference, ICDF2C 2011, Dublin, Ireland, October 26-28, 2011, Revised Selected Papers (pp. 172-179). Heidelberg, Germany: Springer-Verlag Science & Business.

Cho, G. & Rogers, M. (2012). Finding forensic information on creating a folder in \$LogFile of NTFS. In P. Gladyshev & M. Rogers (Eds), *Digital Forensics and Cyber Crime*, Third International ICST Conference, ICDF2C 2011, Dublin, Ireland, October 26-28, 2011, Revised Selected Papers (pp. 211-225). Heidelberg, Germany: Springer-Verlag Science & Business.

Katz, E., Mislan, R., Rogers, M., & Smith, A. (2012). Results of field testing mobile phone shielding devices. In P. Gladyshev & M. Rogers (Eds), *Digital Forensics and Cyber Crime*, Third International ICST Conference, ICDF2C 2011, Dublin, Ireland, October 26-28, 2011, Revised Selected Papers (pp. 47-61). Heidelberg, Germany: Springer-Verlag Science & Business.

Seigfried-Spellar, K., Bertoline, G., & Rogers, M. (2012). Internet child pornography, U.S. sentencing guidelines, and the role of Internet Service Providers. In P. Gladyshev & M.

Rogers (Eds) Digital Forensics and Cyber Crime, Third International ICST Conference, ICDF2C 2011, Dublin, Ireland, October 26-28, 2011, Revised Selected Papers (pp. 17-32). Heidelberg, Germany: Springer-Verlag Science & Business.

Pfleeger, S., Rogers, M., Bashir, M., Caine, K., Caputo, D., Losavio, M. & Stolfo, S. (2012). Does profiling make us more secure? *Privacy & Security: IEEE*. 10(4), 10-15.

Rogers, M. K., & Seigfried-Spellar, K. C. (2011). Internet child pornography: Legal issues and investigative tactics. In T Holt (Ed.), *Crime On-Line: Correlates, Causes, and Context*. Durham, NC: Carolina Academic Press.

Seigfried-Spellar, K., Lovely, R., & Rogers, M. (2011, February). Personality assessment of self-reported Internet child pornography consumers using Bandura's theory of reciprocal determinism. In K. Jaishankar (Ed.), *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior*. Boca Raton, FL: CRC Press.

Seigfried-Spellar, K. & Rogers, M. (2010, May 11). Low neuroticism and high hedonistic traits for female Internet child pornography consumers. *Cyberpsychology, Behavior, and Social Networking*. Advance online publication. doi: 10.1089/cyber.2009.0212

Rogers, M. & Smith, J. (2010). Computer forensics for the forensic audio professional. Proceedings, AES 39 International Conference, Copenhagen, Denmark, June 17-19th, 2010.

Gao, Y., Cao, T., & Rogers, M. (2010). Reconstructing executable files: A robust address translation approach. IET Information Security.

Bagilli, I., Mohan, A. & Rogers, M. (2010). SMIRK: SMS management and information retrieval kit. In Goel (Ed.), *Digital Forensics and Cyber Crime* (pp. 33-42). Heidelberg, Germany: Springer-Verlag Computer Science.

Rogers, M. (2010). The psyche of cyber criminals: A psycho-social perspective. In Ghosh & Turrini (Eds.) *Cybercrimes: A Multidisciplinary Perspective* (pp. 217 – 235). Heidelberg, Germany: Springer-Verlag Law Division.

Rogers, M. (2010). Legal, regulations, investigations and compliance. In Tipton (Ed.). *Official (ISC)2 Guide to the CISSP CBK*, 2nd edition (pp. 503-538). Danvers, MA: CRC Press.

Liles, S., Hoebich, M, & Rogers, M. (2010). Legal issues in cyber forensics: Issues confronting the discipline. In Peterson & Shenoi (Eds.), *Advances in digital forensics V*. Boston: Springer, (pp. 267-276).

Bagilli, I. & Rogers, M. (2009). Self-reported cyber crime: An analysis on the effects of anonymity and pre-employment integrity. *International Journal on Cyber Criminology*, 3 (2), 552-568.

Rogers, M. & Seigfried-Spellar , K. (2009). The Future of Digital Forensics: Merging Behavioral Sciences and Digital Evidence. (Position Paper). Indo-US Conference on Cybersecurity, Cybercrime and Cyberforensics, Kochi India (August 20-21, 2009).

- Rogers, M. & Hacker, T. (2009). Digital Evidence and Cloud Computing – Position Paper, ARO Workshop on Digital Forensics. Washington, DC.
- Rogers, M. & Leshney, S. (2009). Virtualization and digital investigations. In Tipton & Krause (Eds.), Information Security Management Handbook 6th Edition, vol 3, (pp. 347-363). Boca Raton, FL: CRC Press.
- Seigfried, K., Lovely, R., & Rogers, M. (2008). *Self-reported Internet child pornography users: A psychological analysis*. International Journal of Cyber Criminology, 2(1), 286-297.
- Scarborough, K.E., Rogers, M., Frakes, K., & San Martin, C. (2008). Digital evidence. In F. Schmallegger & M. Pittaro (Eds.), *Crimes of the Internet* (pp. 477-488). Upper Saddle River, NJ: Pearson Prentice Hall.
- Rogers, M. (2008). Cyber forensics and home land security. In Voeller (Ed.), *Wiley Handbook of Science and Technology for Homeland Security*. New Jersey: Wiley & Sons.
- Rigby, S. & Rogers, M. (2008). The general digital forensics model. Proceedings of the ADFSL 2008 Conference on Digital Forensics, Security and Law, Oklahoma City, April 23-25, 2008.
- Rigby, S., Dark, M., Ekstrom, J. & Rogers, M. (2008). Measuring conceptual understanding: A case study. Proceedings of the 9th ACM SIGITE Conference on Information Technology Education, Cincinnati, OH, 11-16.
- Choudhury, A., Rogers, M., Gillam, W. & Watson, K. (2008). A novel skin tone detection algorithm for contraband image analysis. Proceedings of the Third International workshop on Systematic Approaches to Digital Forensic Engineering. Berkley, CA, May 22, 2008, 3 – 9.
- Rogers, M. (2008). The future of digital evidence: Introduction to virtualization. NW3C Informant.
- Rogers, M. (2008). Frequently Asked Questions on Cyber Crime. Milano, Italy: Polimetrica.
- Kiley, M., Dankner, S. & Rogers, M. (2008). Forensics significance of instant messaging artifacts. In Ray & Shenoi (Eds.), *Advances in digital forensics IV* (pp. 129-138). Boston: Springer.
- Rogers, M. (2008). Enterprise incident response and digital evidence. In Tipton & Krause. (Eds.). *Information Security Management Handbook 6th Edition Volume 2* (pp. 391 - 403). New York: Auerbach.
- Rogers, M. (2008). Cyber forensics and home land security. In Voeller (Ed.), *Wiley Handbook of Science and Technology for Homeland Security*. New Jersey: Wiley & Sons.
- Rogers, M. (2007). Legal, regulations, compliance and investigations. In Tipton & Henry (Eds.), *Official (ISC)2 Guide to the CISSP CBK* (pp. 683-717). New York: Auerbach.
- Rogers, M. (2007). The role of computer crime investigators in counter terrorism and

intelligence gathering. *NW3C Informant*, 3(1), 28.

Baggili, I., Mislan, R., & Rogers, M. (2007). Mobile phone forensics tool testing: A database driven approach. *International Journal of Digital Evidence*, Fall 2007.

Rigby, S., Dark, M., Ekstrom, J., & Rogers, M. (October 2007). Preparing IAS Graduates to Recognize and Manage Complexity. *Proceedings of the 2007 SIGITE Annual Conference*, October 18-20, 2007, Sandestin, FL.

Rogers, M. (2007). Social engineering: The human factor in information assurance. In Tipton & Krause. (Eds.). *Information Security Management Handbook 6th Edition Volume 1* (pp. 2897 - 2910). New York: Auerbach.

Kiley, M., Shinbara, T., & Rogers, M. (2007). iPod forensics update. *International Journal of Digital Evidence*, Spring 2007, 6(1).

Rogers, M., Scarborough, K., Frakes, K., & San Martin, C. (2007). National, state & local law enforcement digital evidence survey: Perceptions of prosecutors' and judges' knowledge and willingness to deal with digital evidence. In Craiger & Shenoi (Eds.), *Advances in Digital Forensics III* (pp. 41-52). Boston: Springer

Brinson, A., Robinson, A., & Rogers, M. (2006). A cyber forensics ontology: Creating a new approach to studying cyber forensics. *Proceedings of the Digital Forensics Research Workshop 2006*, 3S (2006), 37-43.

Gupta, M., Hoeschele, M., & Rogers, M. (2006). Hidden disk areas: HPA and DCO. *International Journal of Digital Evidence*, Fall 2006, 5(1).

Rogers, M. (2006). Law compliance and investigation. In Tipton & Henry (Eds.). *The Official CISSP Study Guide*. New York: Auerbach.

Rogers, M., Seigfreid, K., & Tidke, K. (2006). Self-reported Computer Criminal Behavior: A Psychological Analysis. *Proceedings of the Digital Forensics Research Workshop 2006*, August 14-16th, 2006, Lafayette, Indiana, (pp. 116-120).

Rogers, M., Goldman, J., Mislan, R., Wedge, T. & Debrota, S. (2006). Fast cyber forensics triage process model. *Journal of Digital Forensics, Security and Law*, 1(2), 19-37.

Rogers, M. & Scarborough, K. (2006). Cyber crime. *Encyclopedia of Police Science 3rd Edition*. London: Routledge.

Bebe, N., Kessler, G., & Rogers, M. (2006). Book review: Computer evidence: Collection & preservation. *Journal of Digital Forensic Practice*, 1.

Carrier, B., Casey, E., Garfinkel, S., Kornblum, J., Hosmer, C., Rogers, M., & Turner, P. (2006). Standardizing digital evidence storage. *Communications of the ACM*, February, 2006, 49(2), 67-68.

Losavio, M., Adams, J., & Rogers, M. (2006). Gap analysis: Judicial experience and perception of electronic evidence. *Journal of Digital Forensic Practice*, 1. (pp. 13-17).

Ksander, S., Gillam, B., & Rogers, M. (2006). Product review: Ultrablock forensic card reader. *Journal of Digital Forensic Practice*, 1.

Scarborough, K. & Rogers, M. (2006). Information security. *Encyclopedia of Police Science 3rd Edition*. London: Routledge.

Scarborough, K. & Rogers, M. (2006). Computer technology. *Encyclopedia of Police Science 3rd Edition*. London: Routledge.

Rogers, M. (2006). The development of a meaningful hacker taxonomy: A two dimensional approach. *Digital Investigations*, 3, 97-102.

Rogers, M., Smoak, N., Lui, J. (2006). Self-reported criminal computer behavior: A big-5, moral choice and manipulative exploitive behavior analysis. *Journal of Deviant Behavior*, 27, 3, 245-268.

Rogers, M. (2006). DCSA: Applied digital crime scene analysis. In Tipton & Krause. (Eds.). *Information Security Management Handbook 5th Edition Volume 3* (pp. 601-614). New York: Auerbach

Rogers, M. (2006). The information technology insider risk In H. Bigdoli (Ed.), *Information Security Handbook, Vol 3*. (pp. 3-17). New York, NY: John Wiley & Sons, Inc.

Rogers, M. (2005). Cyber forensics program partnership. *National White Collar Crime Center Informant*, 1(2), 26/40.

Marsico, C. & Rogers, M. (2005). Applied iPod Forensics. *International Journal of Digital Evidence*, Fall 2005, 4,2.

Rogers, M. (2005). The insider threat: Debunking the “wagon wheel” approach to information security. *Security Wire Digest*, Vol 7. No. 17, March 3, 2005.

Hoeschele, M. & Rogers, M. (2005). Detecting social engineering. In Pollitt & Shenoi (Eds.). *Advances in Digital Forensics* (pp. 67-77). New York: Springer.

Meyers, M. & Rogers, M. (2005). Digital forensics: Meeting the challenges of scientific evidence. In Pollitt & Shenoi (Eds.). *Advances in Digital Forensics* (pp. 43-50). New York: Springer.

Meyers, M. & Rogers, M. (2004). Computer forensics: The need for standardization and certification within the U.S. court systems. *International Journal of Digital Evidence*, Fall 2004, 3(2).

Carney, M. & Rogers, M. (2004). The trojan made me do it: A first step in statistical based event reconstruction. *International Journal of Digital Evidence*, Spring 2004, 2,4.

Rogers, M. & Ogloff, J. (2004). A comparative analysis of Canadian computer and general criminals. *Canadian Journal of Police & Security Services*, 1, 366-376.

Rogers, M. & Seigfried, K. (2004). The future of computer forensics: A needs analysis survey. *Computers and Security*, 23, 1, 12-16.

- Rogers, M. (2003). Law investigation and ethics. In Tipton & Berti (Eds). *2003 CBK review course*. Dunedin: SMT.
- Rogers, M. (2003). Computer forensics: Science or fad. *Security Wire Digest*, 5(55), July 24.
- Rogers, M. (2003). Understanding deviant computer behavior: A moral development and personality trait approach. *Canadian Psychological Association Abstracts, Summer 2003*.
- Rogers, M. (2003). The role of criminal profiling in computer forensic investigations. *Computers & Security*, 22(4) 292-298.
- Rogers, M. (2003). The psychology of cyber-terrorism. In Silke & Merari (Eds.). *Terrorists, Victims and Society: Psychological Perspectives on Terrorism and Its Consequences* (pp. 75-92). London: Wiley and Sons.
- Rogers, M., & Berti, J. (2001). Social engineering: The forgotten risk. In Tipton & Krause. (Eds.). *Information Security Management. Handbook, 4th Edition, Volume 3* (pp. 51-63). New York: Auerbach.
- Rogers, M. (2000). The need for a balanced approach to security. *CIPS Newsletter*, Winnipeg Manitoba, December.
- Rogers, M. (2000). Fight back against electronic attackers. *Retail Advisor, Summer Edition*. Deloitte and Touche.
- Rogers, M. (2000). The need for information security in today's wired world. *CIPS Newsletter*, Edmonton Alberta, March.
- Rogers, M. (2000). The need for information security in today's wired world (re-print). *CIPS Newsletter*, Winnipeg Manitoba, June.
- Rogers, M. (2000). *Modern day robin hood or moral disengagement: Understanding the justification for illegal computer activity*. Available: <http://www.infowar.com>.
- Rogers, M. (1999). *The psychology of hackers: The need for a new taxonomy*. Available: <http://www.infowar.com>.
- Rogers, M. (1999). Organized computer crime and more sophisticated security controls: Which came first the chicken or the egg? Available: <http://www.infowar.com>.

Conference Presentations:

Datar, T., Cole, K. & Rogers, M. (2014). Awareness of Scam-E-Mail: An Exploratory Research Study. Conference on Digital Forensics, Security and Law (May, Richmond Virginia) – No proceedings. (Best Student paper Award)

Seigfried-SPELLAR, K. & Rogers, M. (2014). *Using Internet Artifacts to Profile a Child Pornography Suspect*. Conference on Digital Forensics, Security and Law (May, Richmond Virginia) – No proceedings.

Sitarz, R. & Rogers, M. (2014). *Internet Addiction to Child Pornography*. Conference on Digital Forensics, Security and Law (May, Richmond Virginia) – No proceedings. (Best Student Paper Award).

Rogers, M. & Nguyen. C. (2013). Zeus Stealth BoT: Case Study. American Academy of Forensic Sciences Annual Meeting (Feb, Washington, DC) – no proceedings.

Rogers, M. (2012). Guest Panelist - Recapturing Our Youth (kids at risk of becoming hackers). Department of Homeland Security (DHS) - SRI International Infosec Technology Transition Council (ITTC) (Nov., Menlo Park, CA) – no proceedings.

Rogers, M. (2012). The Role of Digital Forensics in the Justice System. 10th Annual Crown Defence Conference (Sept., Winnipeg, Canada) – no proceedings.

Rogers, M. (2012). Applied behavior analysis: Its role in the digital investigation. AIDE 2012 Conference (May, Huntington, WV) – no proceedings.

Rogers, M. & Winkworth, R. (2012). Disposable cell phone analysis: TracHac. American Academy of Forensic Sciences Annual Meeting (Feb, Atlanta, GA) – no proceedings.

Rogers, M. & Seigfried-Spellar, K. (2012). Applied predictive modeling: The role of behavioral sciences in digital forensics. American Academy of Forensic Sciences Annual Meeting (Feb, Atlanta, GA) – no proceedings.

Craiger, P. & Rogers, M. (2012). Scientific validation of digital forensic tools: A case study. American Academy of Forensic Sciences Annual Meeting (Feb, Atlanta, GA) – no proceedings.

Rogers, M. (2011). Current issues in digital forensics. Appalachian Institute for Digital Evidence 2011 Conference, (July, Marshall University, VA) – no proceedings.

Rogers, M. & Seigfried, K. (2011). Development of an Offender Classification Based Investigative Protocol for Use with Online Consumers of Child Pornography Cases: An Information Technology and Behavioral Sciences Approach. American Academy of Forensic Sciences Annual Meeting (Feb, Chicago, IL) - no proceedings.

Seigfried, K. & Rogers, M. (2011). Exploring the Progression of Non-deviant and Deviant Pornography Use By Age of Onset and Sex. American Academy of Forensic Sciences Annual Meeting (Feb, Chicago, IL) - no proceedings.

Rogers, M. (2010). Digital evidence. Association of Inspectors General Spring Conference, May 12-14th, 2010, Indianapolis, Indiana.

Strzempka, K., Katz, E., Rogers, M., & Huff, P. (2010). Forensic analysis of a VISTA 64 hard drive. American Academy of Forensic Sciences Annual Meeting (Feb, Seattle, Wa) – no proceedings.

Seigfried-Spellar, K. & Rogers, M. (2010). Psychological assessments and attitudes toward deviant computer behavior. American Academy of Forensic Sciences Annual Meeting (Feb, Seattle, Wa) – no proceedings.

Baggili, A., Mohan, A., & Rogers, M. (2009). SMIRK - SMS Management and Information Retrieval Kit. International Conference on Digital Forensics & Cyber Crime, Albany, NY (Sept 30 - Oct. 2, 2009).

Baggili, A., Mohan, A., & Rogers, M. (2009). SMIRK - SMS Management and Information Retrieval Kit. Mobile Forensics World 09, (May 30th, 2009, Chicago, IL).

Liles, S., Hoebich, M, & Rogers, M. (2009). Legal issues in cyber forensics: Issues confronting the discipline. IFIP Working Group on Digital Forensics 11.9, Jan 25th, 2009, Orlando Florida.

Rogers, M. (2008). It's all about the technology; isn't it? *(ISC)2 e-symposium*, September, 23, 2008 – web conference.

Rigby, S., Dark, M., Ekstrom, J. & Rogers, M. (2008). Measuring conceptual understanding: A case study. SIGITE'08, October 16-18, 2008, Cincinnati, Ohio.

Seigfried, K. & Rogers, M. (2008). Self-reported female consumers of Internet child pornography: A psychological analysis. International Association of Forensic Science's 18th Triennial Meeting (July, New Orleans).

Choudhury, A., Rogers, M., Gillam, W. & Watson, K. (2008). A novel skin tone detection algorithm for contraband image analysis American Academy of Forensic Sciences Annual Meeting (Feb, Washington DC) – no proceedings.

Rogers, M. (2007). Digital forensics pedagogy. DFWG – FBI RCFL Conference, Louisville, Kentucky, (June 18-20th, 2007).

Rogers, M. (2007). Dealing with social engineering: Tips and techniques. ISC West Security Conference. (March, Las Vegas, NV).

Scarborough, K., Rogers, M., & Frakes, K. (2007). Digital Evidence Training – Current Status in the CJS. Academy of Criminal Justice Sciences Annual Meeting. (March, Seattle, WA).

Rogers, M. (2007). Digital Evidence practitioner standards: Issues and possible solutions. American Academy of Forensic Sciences Annual Meeting (Feb, San Antonio, TX).

Rogers, M. & Scarborough, K. *The Role of Cyber Forensics in the War on Terrorism*. First Nordic-American Symposium on Public Safety. Copenhagen, Denmark, Oct 10-12, 2006.

Losavio, M., Wilson, D., Elmaghriby, A., Graham, J., Srinivasan, S., Elder, D., & Rogers, M. (2006). Working Between Disciplines – Issues in Building the Digital Forensics Bridge From Computer Science to Judicial Science *Digital Forensics Research Workshop, August 14-16th, 2006, Lafayette, Indiana*.

- Rogers, M., Goldman, J., Mislan, R., Wedge, T., & Debrota, S. (2006). Computer Forensics Fast Triage Process Model (CFFTPM). Association for *Digital Forensics Security & Law Conference*, April 20 , 2006, Las Vegas, NV.
- Rogers, M., & Scarborough, K. (2006). National digital evidence survey. American Academy of Forensic Sciences (AAFS), National Conference, February 23rd, 2006, Seattle, WA.
- Rogers, M. (2005). Persistence of electronic documents: The forensic importance. *Circuit Judges Judicial College*, October 18th, 2005, Covington, KY.
- Rogers, M. & Losavio, M. (2005). Legal and certification issues – Moderators. *Digital Forensics Research Workshop*, August, 18th, 2005, New Orleans, LA.
- Gillam, B. & Rogers, M. (2005). File Hound: A forensics tool for first responders. *Digital Forensics Research Workshop*, August, 18th, 2005, New Orleans, LA.
- Rogers, M. (2005). Psychology and Computer Crime. *NIJ Research and Evaluation Conference*, July 18th, 2005, Washington, DC.
- Rogers, M. (2005). Psychological profiling and computer forensics: Locard's principle in the digital world. E-Crime and Computer Evidence. March 29th, 2005. Monaco.
- Hoeschele. M. & Rogers, M. (2005). Detecting social engineering. *International Conference on Digital Forensics, Feb 13-16, 2005, Orlando Florida: IFIP-11*.
- Marsico, C. & Rogers, M. (2005). iPod forensics. *International Conference on Digital Forensics, Feb 13-16, 2005, Orlando Florida: IFIP-11*.
- Meyers, M. & Rogers, M. (2005). Digital forensics: Meeting the challenges of scientific evidence. *International Conference on Digital Forensics, Feb 13-16, 2005, Orlando Florida: IFIP-11*
- Rogers, M. & Goldman, J (2004). National cyber forensics center. *Paper Presented at the NW3C Economic Crimes Summit*, Indianapolis, IN, March 2004.
- Rogers, M. (2004). Cyber-profiling. *Paper Presented at the NW3C Economic Crimes Summit*, Indianapolis, IN, March 2004.
- Rogers, M. (2002). Profiling computer criminals & malicious code writers? *Paper Presented at the ASIS Cybercrime 2002 Summit*, Arlington, VA, February 2002
- Rogers, M. (2001). Social engineering; The forgotten risk. *Paper Presented at the West Coast Security Conference 2001*, Vancouver, BC, November 2001.
- Rogers, M. (2000). The psychology of hackers: The criminal insider. *Paper Presented at the SANS Institute*, Monterey, California, June 2000.
- Rogers, M. (2000). The future of information security/assurance. *Paper Presented at the ISACA Conference*, Winnipeg, May 2000.
- Rogers, M. (1999). Psychological profiling of hackers. *Paper Presented at the Computer Security Institute (CSI) NetSec 99 Conference*, St. Louis, Missouri, June 1999.

Rogers, M. (1999). The psychology of hackers: A new taxonomy. *Paper Presented at the RSA World Security Conference*, San Jose, California, Feb 1999.

Rogers, M. (1998) The psychology of hackers. *Paper Presented ISSA Conference*, Sacramento, California, October 1998.

Keynote Addresses

- 2013 Keynote: Indiana State Wide Association Security IT fall meeting 2013, Oct 24, 2013, Indianapolis IN.
- 2012 Keynote: Norwegian Information Security Conference, Nov. 19-21st, 2012, Bodo, Norway.
- 2012 ISSA/Infragard Chicago Information Security Conference, August 2nd, 2012, Chicago IL.
- 2012 Keynote: HighTech Crime Investigators Association, Conference, April 11th, 2012 St. Paul Minnesota.
- 2011 Keynote: International ICST Conference on Digital Forensics & Cyber Crime (ICDF2C) Oct. 28th, 2011, Dublin, Ireland.
- 2011 ISSA Indiana/Kentucky InfoSec 2011 Conference, Cyber Forensics – what you should know. Sept, 2011, Louisville, Kentucky,
- 2011 Keynote: Norwich University Master of Information Security & Assurance (MISA) Program Residency Presentations and Workshop, June 13th, 2011, Northfield Vermont, USA.
- 2010 Keynote: International ICST Conference on Digital Forensics & Cyber Crime (ICDF2C) Oct. 5, 2010, Abu Dhabi, UAE.
- 2010 Keynote: ADFSL Conference, May 20th, 2010, St. Paul Minnesota
- 2009 Keynote: Seoul Korea. September, 2009: International Symposium on Cyber Crime Response
- 2009 Keynote: Chicago Con, May 9th, 2009: The Evolution of Social Engineering.
- 2007 Keynote: iSociety – Annual Conference Calumet Indiana
- 2007 Keynote: Association of Certified Fraud Investigators – Annual Fraud Seminar, Winnipeg Canada – evolution of digital evidence.
- 2007 Keynote: ACM-SAC 2007 Korea: Cyber Forensics
- 2005 Keynote Speaker: Security Leadership Conference Chicago: *Social Engineering, the Human Factor in Information Assurance*.
- 2003 Keynote Speaker: HIPAA of Indiana Annual Conference, Indianapolis Indiana. *Through the looking glass: Alice in HIPAA land*.
- 2003 Keynote Speaker: Jack Henry Society of Midwest Indiana, Indianapolis Indiana. *Information security*.

Invited Addresses and Colloquia:

- 2013 Invited Speaker - Counter-Crime Technology Investigation Symposium, Tokyo Japan.
- 2013 Invited Speaker – Eurasian Regional Cooperative For Forensic Science Development, Kiev, UA
- 2013 Invited Speaker – Indiana CPA Fraud Conference, Indianapolis, IN.

2012	Invited Speaker – US Embassy, Rule of Law in South East Europe. Zagreb, Croatia.
2010	Invited Panelist – American Academy of Psychiatry and the Law – 41 st Annual Meeting, Tucson Arizona
2010	Invited Panelist – Workshops on Interdisciplinary Studies in Security and Privacy (WISSP): Abu Dhabi, UAE.
2010	Invited Speaker - The 2010 Purdue Student Pugwash Midwest Regional Conference – Purdue University
2009	Invited Speaker – (ISC)2 Chicago: Digital Evidence Management
2009	Featured Speaker – (ISC)2 San Antonio: Digital Evidence Management
2008	Invited Speaker – Indiana Public Defenders Conference: Cyber Forensics, What a computer expert can do for you.
2008	Guest Lecturer – IUPUI Forensics Sciences – Cyber Forensics
2008	Invited Speaker – Ontario Provincial Strategy to Protect Children from Sexual Abuse and Exploitation on the Internet Multi-disciplinary Conference, London Ontario: Digital Evidence Triage
2008	Invited Panelist – Workshop on Interdisciplinary Studies in Security and Privacy, September 26 th , 2008, Polytechnic Institute of NYU, Brooklyn, New York.
2008	Digital evidence Management and Handling Secure Atlanta -Atlanta Georgia
2007	Invited Panelist – NW3C Economic Crime Summit 2007, Crystal City: LE and Academia
2007	Featured Speaker – (ISC)2 Minneapolis: <i>Digital Evidence Management</i>
2007	Invited Speaker: Purdue ITaP Copyright Colloquium, Purdue West Lafayette
2007	Invited Speaker, Korea University, Seoul Korea
2007	Invited Speaker, Korean Information Security Agency, Seoul Korea
2007	Invited Speaker, Electronics & Technology Research Institute, Daejeon Korea
2007	Invited Speaker – NIJ Research Conference 2007, Crystal City, DC – Filehound – Contraband Images investigative tool.
2006	Invited Address: NW3C Economic Crime Summit 2006 – Rhode Island: Cyber forensics and Counter Terrorism.
2006	Featured Speaker: IEEE SIG Calumet: <i>Digital Evidence Management</i>
2006	Featured Speaker: (ISC)2 Indianapolis: <i>Enterprise IR and Digital Evidence Management</i>
2006	Featured Speaker: Chase Law School, Northern Kentucky
2006	Featured Speaker: Kentucky Bar Association Annual Conference
2006	Featured Speaker: University of Louisville Information Security Seminar
2005	Featured Speaker: (ISC)2 San Jose Conference: <i>Social Engineering</i> .
2005	Invited Address: Lockheed Martin San Diego: <i>Anti-forensics</i> .
2004	Featured Speaker: (ISC)2 Indianapolis Conference: <i>Social Engineering: The Forgotten Information Assurance Risk</i>
2004	Featured Speaker: (ISC)2 Chicago Conference: <i>Social Engineering: The Forgotten Information Assurance Risk</i>
2004	Featured Speaker: (ISC)2 Toronto Conference: <i>Social Engineering: The Forgotten Information Assurance Risk</i>
2004	Featured Speaker: (ISC)2 Washington Conference: <i>Social Engineering: The Forgotten Information Assurance Risk</i>
2004	Panelist: CERIAS Information Security Symposium: <i>Cyber Terrorism</i>
2004	Panelist/Moderator: CERIAS Information Security Symposium: <i>Cyber Forensics</i>

2004	Invited Speaker: Computer Forensic Educators Working Group, Orlando Florida. <i>Current state of cyber forensics.</i>
2004	Invited Speaker: NSF, Washington DC. <i>Computer Forensics.</i>
2003	ISSA Indiana/Kentucky InfoSec 2003 Conference, Louisville, Kentucky. <i>The current state of digital forensics.</i>
2003	HIPAA Working Group of Indiana, Indianapolis Indiana. <i>HIPAA and Risk Management</i>
2003	Invited Speaker: MISA, University of Manitoba, Winnipeg Manitoba. <i>The risk of wireless LANs.</i>
2003	Invited Speaker: Business Innovation & Growth Conference, Winnipeg Manitoba. <i>Identity theft.</i>
2003	Invited Speaker Digitized Conference, Winnipeg Manitoba. <i>The psychology of hackers.</i>
2002	Invited Speaker: Business Innovation & Growth Conference, Winnipeg Manitoba. <i>The psychology of hackers.</i>
2002	Invited Speaker: CIPS Conference, Winnipeg Manitoba. <i>The psychology of hackers.</i>
2002	Invited Speaker: Digitized Conference, Winnipeg Manitoba. <i>The nature of computer crime.</i>
2001	Invited Speaker: Manitoba Parole and Probation Annual General Meeting Winnipeg Manitoba, Canada. <i>Technology related crimes.</i>

Workshop Presentation:

Rogers, M. (2012). Advanced Mac Forensics, NY State Police, June 2012, Albany NY.

Rogers, M. (2011). Evidence Analytics. Intel Corp, Dec 1st, 2011. Hillsboro, OR.

Rogers, M. & Katz, E. (2011, Sept). Digital Evidence Triage. St. Louis, MO.

Rogers, M. (2011, July). The Psychology of Cyber Adversaries: Panel Member. Sandia National Labs, NM.

Rogers, M. (2011, July). Digital Evidence and Cyber Warfare. Sandia National Labs, NM.

Rogers, M. (2011). Digital Evidence Triage Workshop. Norwich University, June 14th, 2011.

Rogers, M. (2010). Psychology of Cyber Terrorism. INTEL WRT continuing Education Program, Sept 23rd, 2010.

Rogers, M. (2010). Digital Evidence Management and Handling. Association of Credit Union Auditors National Conference, June 15-18, 2010, Minneapolis, MN.

Rogers, M. & Goldman, J. (2010). Digital Evidence Triage Workshop for Auditors. ISACA International Conference, Cancun Mexico, June 5-6th, 2010.

Seigfried-Spellman, K**. & Rogers, M. (2009). The Role of Profiling in Cyber Crimes Investigations. Indo-US Conference on Cybersecurity, Cybercrime and Cyberforensics, Kochi India (August 20-21, 2009).

Rogers, M. & Seigfried-Spellar, K. (2009, July). Investigating Online Consumers of Child Pornography. 1st Annual ACM Northeast Digital Forensics Exchange, New York: NY. Workshop Presentation.

Workshop Attended (no presentation):

- 2012 – National Institute of Justice/RTI International – How to be an Expert Witness (Online)
- 2010 – National Institute of Justice/RTI International – Expert Testimony 1 (Online)
- 2010 – National Institute of Justice/RTI International – Offender Profiling: Psychology Contributions to Behavioral Crime Scene Analysis (Online)
- 2009 – American Academy of Sciences (Computer Science and Telecommunications Board). July 21-22nd, 2009, Washington DC, Usability Security and Privacy.