Dr. Lodovico Marziale
Managing Partner
504ENSICS, LLC
vico@504ensics.com

Education

Ph.D. in Computer Science, University of New Orleans, 2009.

Dissertation Topic: Advanced Techniques for Improving the Efficacy of Digital Forensics Investigations

M.S. in Computer Science, University of New Orleans, 2006.

B.S. in Finance, University of New Orleans, 2000.

GIAC Certified Digital Forensics Analyst (GCFA), 2009-Present.

Employment

Managing Partner, 504ENSICS, LLC, 2012-present.

Co-Founded a computer security firm offering custom research and development, digital forensics, incident response, and malware analysis services, network security audits/penetration tests, and training.

Senior Forensic Analyst, Digital Forensics Solutions, 2008 – 2012.

Performed digital forensic investigations, network penetration testing, incident response, training on digital forensics and general computer security, and research and development.

Visiting Assistant Professor, Department of Computer Science, University of New Orleans, Fall 2011.

Taught undergraduate and graduate-level classes in computer security and cryptography.

Research Assistant, Department of Computer Science, University of New Orleans, 2006-2009.

Conducted research on advanced topics in file carving, including porting of resource intensive code to run on GPUs, and In-Place file carving (see publications for details).

System Administrator, 2007– 2011, Network Security and System Administration Lab (NSSAL), University of New Orleans designated Center for Information Assurance Education.

Administered 50 seat lab designed for computer security and forensics classroom support and and research. Lab infrastructure included Solaris/NIS/NFS servers with a ZFS-clone-based virtual environment and Windows and Linux clients.

Desktop Support, Ochsner Health Plan, 2004-2006

Supported help desk by troubleshooting high complexity and high priority tickets. Handled new workstation rollouts. Managed migration from Windows 2000 – XP for ~500 user environment.

Funded Research Grants

"A Framework for Differential Analysis of Malware in RAM," DARPA-PA-11-52: Cyber Fast Track (CFT), PI, 2013, $106,773.60.

"Forensic Analysis of the OS X Spotlight Search Index," DARPA-PA-11-52: Cyber Fast Track (CFT), Co-PI, 2012, $135,534.60.

"Application-Level Memory Forensics for DALVIK," DARPA-PA-11-52: Cyber Fast Track (CFT), Co-PI, 2012, $137,145.60.

"Live Memory Analysis and Command Line Access Enhancement for Registry Decoder," NIST, Co-PI, 2012, $85,681.

"Automatically Generated Regular Expression-Based Signatures for File Carving," DARPA-PA-11-52: Cyber Fast Track (CFT), PI, 2012, $69,212.

"REGISTRY DECODER: Automatic Acquisition and Reporting of Relevant Microsoft Windows Registry Contents", National Institute of Justice, PI, 2010, $135, 635.

"CTISG: A Comprehensive Data Carving Architecture for Digital Forensics," National Science Foundation, Student Participant, 2006-2009, $260,697.

Publications

Books/Chapters

L. Marziale, S. Movva, G. G. Richard III, V. Roussev, L. Schwiebert,"Developing Massively Threaded Digital Forensics Tools Using Graphics Processing Units (GPUs) and Multicore CPUs", In Li, C.-T. (ed.), Handbook of Research on Computational Forensics, Digital Crime and Investigation: Methods and Solutions, IGI Global Publishing, 2010.

V. Roussev, G. G. Richard III, L. Marziale, "Classprints: Class-aware Similarity Hashes", In Ray, I., Shenoi, S. (eds.), Research Advances in Digital Forensics IV, Springer, 2008. ISBN: 9780387849263.

G.G. Richard III, V. Roussev, L. Marziale, "In-place File Carving", Research Advances in Digital Forensics III, Springer, 2007. ISBN: 9780387737416.

Selected Journal and Conference Publications

J. Sylve, A. Case, L. Marziale, G. G. Richard III, "Acquisition and Analysis of Volatile Memory from Android Devices," Journal of Digital Investigation, (8)3, 2012.

A. Case, L. Marziale, C. Neckar, G. G. Richard III, "Treasure and Tragedy in *kmem_cache* Mining for Live Forensics Investigation," *Proceedings of the 10th Annual Digital Forensics Research Workshop (DFRWS 2010)*, Portland, OR.

A. Case, L. Marziale, G. G. Richard III, "Dynamic Recreation of Kernel Data Structures for Live Forensics," *Proceedings of the 10th Annual Digital Forensics Research Workshop (DFRWS 2010)*, Portland, OR.

V. Roussev, L. Wang, G.G. Richard III, L. Marziale, "A Cloud Computing Platform for Large Scale Forensic Processing." *Proceedings of the Fifth Annual IFIP WG 11.9 International Conference on Digital Forensics*, 2009.

A. Case, A. Cristina, L. Marziale, G. G. Richard III, V. Roussev, "FACE: Automated Digital Evidence Discovery and Correlation," *Proceedings of the 8th Annual Digital Forensics Research Workshop (DFRWS 2008)*, Baltimore, MD.

V. Roussev, G.G. Richard III, L. Marziale, "Hash-based Classification of Data: Class-based Similarity Hashing," *Proceedings of the Fourth Annual IFIP WG 11.9 International Conference on Digital Forensics*, 2008.

L. Marziale, G.G. Richard III, V. Roussev, "Massive Threading: Using GPUs to Increase the Performance of Digital Forensics Tools," *Proceedings of the 7th Annual Digital Forensics Research Workshop (DFRWS 2007)*, Pittsburgh, PA.

V. Roussev, G.G. Richard III, L. Marziale, "Multi-Resolution Similarity Hashing," *Proceedings of the 7th Annual Digital Forensics Research Workshop (DFRWS 2007)*, Pittsburgh, PA.

G.G. Richard III, V. Roussev, L. Marziale, "Forensic Discovery Auditing of Digital Evidence Containers," *Journal of Digital Investigation*, (4)2, 2007.

G.G. Richard III, V. Roussev, L. Marziale, "In-place File Carving," *Proceedings of the Third Annual IFIP WG 11.9 International Conference on Digital Forensics*, 2007.

Conference Presentations

"Advanced Techniques for Registry Forensics: A Study of Three Scenarios," RSA Conference, San Francisco, CA, March 1, 2013.

"Advanced Registry Forensics with Registry Decoder," Security BSides Jackson, Jackson MS, November 10, 2012.

"Advanced Registry Forensics with Registry Decoder," Open Source Digital Forensics (OSDF) Conference, Washington D.C., October 3, 2012.

"Registry Decoder: Automated Acquisition and Investigation of the Windows Registry," DOD Cybercrime 2012, Atlanta GA, January 26, 2012.

"Automating Forensic Registry Analysis with Registry Decoder," BSidesDFW 2011: Advanced Persistent Texans, Dallas, TX, November 5, 2011.

"Dynamic Recreation of Kernel Data Structures for Live Forensics," 10th Annual DFRWS Conference, Portland, OR, August 2, 2010.

"FACE: Automated Digital Evidence Discovery and Correlation," 8th Annual Digital Forensics Research Workshop (DFRWS 2008), Baltimore, MD, August 12, 2008.

Workshops Conducted

"Basic Windows Forensics," Security BSides Jackson, Jackson MS, November 10, 2012.

"Advanced Registry Forensics with Registry Decoder," 12th Annul Digital Forensics Research Workshop (DFRWS), Washington D.C., August 8, 2012.

"Automating Forensic Registry Analysis with Registry Decoder," SANS Security East 2012 SANS @Night, New Orleans, LA, January 22, 2012.

Teaching

Assistant Professor, University of New Orleans, Fall 2011:

CSCI 4621/4621G: Computer Security

CSCI 6130: Data Encryption and Cryptology

Instructor, University of New Orleans, Spring 2009:

CSCI 3080: Ethics in the Computing Profession

Substitute Instructor, University of New Orleans, 2006-2009:

CSCI 4311: Computer Networks and Telecommunications

CSCI 4401: Principles of Operating System I

CSCI 4621: Computer Security

CSCI 4623: Introduction to Computer Forensics

CSCI 6621: Advanced Network Security and Forensics

Community Involvement

Organizer, NOLASec, 2012 – present.

NOLASec is a monthly meetup for information security and digital forensics students, researchers, and professionals featuring networking opportunities and talks on current topics in the field given by top experts.

Organizer, Security BSides NOLA Conference, 2012 – present.

BSides is a community-driven framework for hosting computer security conferences all over the world. In May, 2013, we successfully hosted the inaugural BSides in New Orleans.

Co-Developer, Scalpel, 2006 - present.

Scalpel is a free and open-source, fast file carver that reads a database of header and footer definitions and extracts matching files or data fragments from a set of image files or raw device files. Scalpel is filesystem-independent and will carve files from FATx, NTFS, ext2/3, HFS+, or raw partitions. It is useful for both digital forensics investigation and file recovery.

Co-Developer, Registry Decoder, 2010 – present.

Registry Decoder is a free and open-source tool that automates acquisition, analysis, and reporting of information found within the Windows Registry. Registry Decoder was released in September 2011 as an open source project and has since been downloaded over 10,000 times. It is used in many public and private forensic labs. Development of this tool was partially funded by the National Institute of Justice.

Member, Infragard, 2013 – present.

Infragard is a public-private partnership between the FBI and members of the private sector who are focused on intrusions and vulnerabilities affecting 18 critical infrastructures.

Member, Greater Mid-City Business Association, 2013 – present.

Member, New Orleans Chamber of Commerce, 2013 – present.