Joe Sylve
Managing Partner
504ENSICS Labs
joe@504ensics.com

Education

Ph.D. Engineering and Applied Science, Computer Science, University of New Orleans, (Expected 2015)

Dissertation Topic: High Performance Memory Analysis

M.S. Computer Science, University of New Orleans, 2011

Thesis Title: "Android Memory Capture and Applications for Security and Privacy"

B.S. Computer Science, University of New Orleans, 2010

GIAC Certified Digital Forensics Investigator (CGFA), 2011 – present

License Number: 9445

Employment

Managing Partner & Co-Founder, 504ENSICS Labs, 2012 - present

Senior Security Researcher, Digital Forensics Solutions, LLC, 2011 – 2012

Research Assistant, Greater New Orleans Center for Information Assurance, Department of Computer Science, University of New Orleans, 2010-2011

Director, Camp Stanislaus, 2009-2011

Systems Engineer, Crescent City Technologies, 2008 – 2009

Projects Group Student Worker Manager, University Computing Center, University of New Orleans, 2004-2008

Research Interests

Digital Forensics, Network Security, Mobile Forensics, Linux Operating System Internals, Kernel Exploitation, Embedded File System Internals, Volatile Memory Analysis

Selected Journal and Conference Publications

J. Sylve, A. Case, L. Marziale, G.G. Richard III, "Acquisition and analysis of volatile memory from android devices." *Digital Investigation*, 2012

Open Source Projects

Registry Inspector, 2013 - present

Dalvik Inspector, 2013 - present

Volatility, 2012 - present

Registry Decoder, 2012

libFATES – Filesystem Analysis Toolkit for Embedded Systems, 2012

LiME Forensics – Linux Memory Extractor, 2010 – present

Funded Grants

"High-Level Differential Analysis of RAM for Analyzing Malware", DARPA CFT, Co-PI, 2012, $106,773.20

"Forensic Analysis of the OS X Spotlight Search Index", DARPA CFT, Co-PI, 2012, $135,534.60

"Application-Level Memory Forensics for DALVIK", DARPA CFT, Co-PI, 2012, $137,145.60

"Live Memory Analysis and Command Line Access Enhancement for Registry Decoder", NIST, Co-PI, 2012, $85,681.00

"Forensic Capabilities for Embedded File Systems," DARPA CFT, PI, 2012, $69,425.75

"Platform Independent Secure Mobile Computing", SPAWAR, Graduate Researcher, 2010-2011, $270,550

Conference Presentations

"Next Generation TCP/IP Stack Deep Dive", Open Memory Forensics Workshop (OMFW) 2014, Herndon VA, November 4, 2014

"Spotlight Inspector", Blackhat USA Arsenal 2014, Las Vegas NV, Aug, 6, 2014

"Dalvik Memory Analysis and a Call to ARMs", Open Memory Forensics Workshop (OMFW) 2013, Chantilly VA, November 4, 2013

"Dalvik Inspector", Blackhat USA Arsenal 2013, Las Vegas NV, July 31 – Aug 1, 2013

"Datalore: Android Memory Analysis. Where No Tool Has Gone Before", Open Memory Forensics Workshop (OMFW) 2012, Chantilly VA, October 2, 2012

"The Insider Threat in Your Pocket: What you should know about mobile security", FBI Cyber Awareness Meeting 2012, New Orleans, LA, September 19, 2012

"LiME Forensics 1.1", Blackhat Arsenal 2012, Las Vegas NV, July 25-26, 2012

"Android Memory Acquisition and Analysis with LiME and Volatility", SANS Forensics and Incidence Response Summit 2012, Austin TX, June 26, 2012

"Android Mind Reading: Memory Acquisition and Analysis DMD and Volatility", ShmooCon 2012, Washington D.C., January 28, 2012

Workshops Conducted

"Windows Forensics", BSides Jackson 2012, Jackson MS, November 10, 2012

"DFRWS Forensics Rodeo: Android Memory Forensics", DFRWS 2012, Washington D.C., August 7, 2012

Teaching

McAfee Foundstone Instructor, 2013 – 2014:

Foundstone Building Secure Software

Foundstone Writing Secure Code – ASP.net (C#)

Substitute Instructor, University of New Orleans, 2010-Present:

CSCI 2467: System Programming Concepts

CSCI 4402: Principles of Operating Systems II

CSCI 4621: Computer Security

CSCI 4623: Introduction to Computer Forensics

CSCI 6621: Advanced Computer Forensics

CSCI 6990: Reverse Engineering Malware

CSCI 6990: Memory 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.

Member, Infragard, 2014 – 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.

Program Committee, Digital Forensics Research Workshop (DFRWS), 2014-present.

DFRWS is a non-profit, volunteer organization dedicated to the sharing of knowledge and ideas about digital forensics research. DFRWS organizes an annual conference and sponsors technical working groups and annual challenges to help drive the direction of research and development.

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

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