Curriculum Vitae of Dr. Joe T. Sylve

Independent Digital Forensics and Cyber Security Researcher

joe.sylve@gmail.com

Personal Data

Born February 24, 1985 in Chalmette, LA. U.S. Citizen. Resident of New Orleans, LA

Education

- Ph.D. Engineering and Applied Science, Computer Science, University of New Orleans, 2017
  - Dissertation Title: Towards Real-Time Memory Forensics: Frameworks, Methods, and 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), Since 2011
  - License Number: 9445

Areas of Expertise

- Digital forensics, including investigative issues and expert testimony
- Research and Development
- Information Security
- Reverse engineering
- Memory analysis
- Operating systems internals
- File system internals

Current Affiliations

- Sole Proprietor, Bayou Bits Technologies, LLC, Since 2024
- Co-Organizer, DFIR Bayou Con, Since 2023
- External Advisory Board, UNO Department of Computer Science, Since 2022
- Developer, LiME Forensics, Open Source, Since 2010

Past Affiliations (Selected)

- Cellebrite / BlackBag Technologies, Inc, 2015-2024
  - Head of Computer Forensic Research (Cellebrite), 2021-2024
  - Director of Research and Development (BlackBag) , 2017-2021
  - Senior Research Developer (BlackBag), 2015-2017
- Adjunct Computer Science Faculty Louisiana State University, 2022 - 2023
- Adjunct Computer Science Faculty, University of New Orleans, 2017 - 2023
- Co-Founder and Managing Partner, 504ENSICS Labs, 2012-2015
- Senior Security Researcher, Digital Forensics Solutions, LLC, 2011-2012

- Graduate Research Assistant, Greater New Orleans Center for Information Assurance, Department of Computer Science, University of New Orleans, 2010-2011
- Organizing Committee, Digital Forensics Research Workshop, 2017-2022
- Technical Program Committee, Digital Forensics Research Workshop, 2014-2021
- Reviewer/Referee, *Journal of Digital Investigation (Elsevier), Computers and Security (Elsevier), IEEE Security & Privacy (IEEE), Journal of Forensic Sciences (AAFS), 2011-2021*
- Organizer, BSidesNOLA Conference, 2012-2020
- Organizer, NOLASec, 2011-2020
- Developer, Registry Decoder, Open Source, 2012
- Developer, DAMM - Differential Analysis of Malware in Memory, Open Source, 2013–2015
- Contributor, Volatility, Open Source, 2012-2014
- Member, FBI Infragard, 2014-2016

Journal and Conference Publications

- J. Sylve, V. Marziale, G. G. Richard III, "Modern Windows Hibernation File Analysis," *Journal of Digital Investigation,* Vol 20, 2017.
- J. Sylve, V. Marziale, G. G. Richard III, "Pool Tag Quick Scanning for Windows Memory Analysis," *Proceedings of the 2016 Digital Forensics Research Conference (DFRWS-EU),* March 2016, Lausanne, Switzerland.
- 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, 2011

Conference Presentations (Selected)

- “Revisiting the Linear Hash”’, DFRWS US 2020, Virtual, July 20, 2020
- “New Tools, Techniques, and Emerging Challenges in macOS Forensics”, The First Forensics Forum 2019, Birmingham, England, UK, November 13, 2019
- “The DFIR Practitioner's Guide to the Research & Development Process”, SANS Forensics & Incident Response Summit, Austin, TX, July 25, 2019
- “APFS Analysis: The Hard Parts”, The First Forensic Forum 2018, South Gloucestershire, England, UK, November 14, 2018
- “The Importance of APFS Snapshots in Investigations”, Techno Security, San Antonio, TX, September 18, 2018
- “Adding APFS Support to The Sleuthkit Framework”, DFRWS 2018, Providence, RI, July 18, 2018
- “Apple File System (APFS)”, DEX-XL Dutch Cybercrime Conference 2017, Arnhem, Netherlands, November 29, 2017
- “Towards Real-Time Memory Analysis”, DEX-XL Dutch Cybercrime Conference 2017, Arnhem, Netherlands, November 28, 2017
- “Apple Unified Logs”, DEX-XL Dutch Cybercrime Conference 2017, Arnhem, Netherlands, November 28, 2017
- “Memory Forensics: A Brief Introduction”, NSA/NSF/UNO GenCyber 2015, New Orleans LA, July 30, 2015
- “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 Incident Response Summit 2012, Austin TX, June 26, 2012
- “Android Mind Reading: Memory Acquisition and Analysis with DMD and Volatility”, ShmooCon 2012, Washington D.C., January 28, 2012

Other Recent Professional Activity (Selected)

- Workshop: “Building Digital Forensic Tools in Go”, DFRWS EU 2017, Überlingen, Germany, March 21, 2017
- Forensics Rodeo sub-committee member, DFRWS 2017, Austin, TX
- Workshop: “Building Digital Forensic Tools in Go”, DFRWS 2016, Seattle WA, August 7, 2016
- Invited talk on high performance memory analysis, Information Systems Audit and Control Association (ISACA), New Orleans Chapter, New Orleans, LA, March 10, 2016.
- Workshop: “Building Digital Forensic Tools in Go”, DFRWS 2015, Philadelphia PA, August 9, 2015
- Workshop: “Windows Forensics”, BSides Jackson 2012, Jackson MS, November 10, 2012
- Developed DFRWS Forensics Rodeo: “Android Memory Forensics”, DFRWS 2012, Washington D.C., August 7, 2012
- Invited talk on Android memory analysis, Information Systems Audit and Control Association (ISACA), New Orleans Chapter, New Orleans, LA, May 12, 2012.

Teaching

- Adjunct Instructor, Louisiana State University, 2022-2023
  - CSC 7360: Memory Forensics Research & Development
    - Fall 2023, Fall 2022
  - CSC 7700/4700: Network Operations & Defense, Spring 2023
  - CSC 4360: Malware Analysis and Reverse Engineering, Spring 2022
- Adjunct Instructor, University of New Orleans, 2017-2023
  - CSCI 4622/5622: Software Reverse Engineering
    - Fall 2023, Fall 2022, Fall 2021, Fall 2020, Spring 2019, Spring 2017
  - CSCI 4623/5623: Introduction to Computer Forensics
    - Spring 2022, Spring 2021, Spring 2020, Fall 2019, Fall 2017
  - CSCI 6625: Network Penetration Testing and Defense, Spring 2020
  - CSCI 4460/5460: Network Operations & Defense, Fall 2019
  - CSCI 4621/5621: Introduction to Computer Security, Fall 2018
  - CSCI 4402/5402: Operating System Security (Formerly OS II), Spring 2018
  - CSCI 4311/5311: Computer Networks and Telecommunications, Fall 2017
- Substitute Instructor, University of New Orleans, 2010-2016
  - CSCI 2467: System Programming Concepts
  - CSCI 4402: Principles of Operating Systems II
  - CSCI 4621: Computer Security
  - CSCI 4622/5622: Software Reverse Engineering
  - CSCI 4623/5623: Introduction to Computer Forensics
  - CSCI 6621: Advanced Computer Forensics
  - CSCI 6625: Network Penetration Testing and Defense
  - CSCI 6990: Memory Forensics
- McAfee Foundstone Instructor, 2013–2014
  - Foundstone Building Secure Software
  - Foundstone Writing Secure Code – ASP.net (C#)

Funded Research Grants

- **“**Instructional Materials Development: Reverse Engineering of Modern Malware”, National Security Agency, Co-PI, 2018, $119,225.00
- High-Level Differential Analysis of RAM for Analyzing Malware”, DARPA-PA-11-52: Cyber Fast Track (CFT), Co-PI, 2012, $106,773.20
- “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”, National Institute of Standards and Technology, Co-PI, 2012, $85,681.00
- “Forensic Capabilities for Embedded File Systems,” DARPA-PA-11-52: Cyber Fast Track (CFT), PI, 2012, $69,425.75
- “Platform Independent Secure Mobile Computing”, SPAWAR / Department of Defense, Graduate Researcher, 2010-2011, $270,550