Kevin V. Bluml, GCFA, GCFE, EnCE, CPP

CURRICULUM VITAE

Kevin V. Bluml, GCFA, GCFE, EnCE, CPP

Employment

Optiv Security; Minnesota
Consultant – Enterprise Incident Management, November, 2015 – May, 2020

- Computer Forensics and Incident Response
- Perform forensic analysis of computers and related storage devices using a variety of forensic software products
- Perform on-site Incident Response and forensic imaging and data captures of computers and related media

Evolver Inc., Reston, VA
Forensic Examiner, 2013-2019
Performed Computer Forensics Examinations as a contractor for the FDIC.

- Work was performed as needed as part of a FDIC insured bank's closing or take-over by the FDIC.
- Preserve evidence for use in any ongoing or future investigation related to the specific bank's issues that caused the FDIC to become involved.
- Position required a Public Trust clearance.

United Health Group Inc.; Minnetonka, MN
Corporate Security Investigator, 2004 – 2013

- Primary Computer Forensic Investigator for Corporation
- Fraud investigator
- Duties include all types of fraud investigations, credit card fraud, misuse of corporate assets including computer, telephone and network activity
- Investigate all forms of electronic data

Kroll Ontrack, Inc.; Eden Prairie, Minnesota.
Senior Forensic Engineer, 1998 – 2004

- Responsible for conducting sound computer forensic analysis and maintaining strict media chain of custody using protocols and procedures in line with established state and federal guidelines and company policies.
- Acquire and preserve computer media in either a lab setting or through onsite data capture or seizure. This involves creating byte-by-byte forensic copies of original media for legal and investigative purposes.
- Perform data recovery, including both file and email recovery, on electronic media to be analyzed during the course of a computer forensic investigation.
- Interact with Project Management to provide the highest quality of output in order to meet the customer's desired outcomes. This includes interaction with Managers, Case Managers, and Electronic Discovery Consultants.
- Conduct investigations involving analysis of electronic media. Example analysis conducted includes but is not limited to:
    - Searches for evidence of financial fraud and theft of trade secrets on computer media from desktops, laptops, and server platforms.
    - Searches for evidence of reformatting, dates of reformatting, and utilities used to wipe or copy data from electronic media
    - Locating evidence of improper removal, duplication, destruction, or transmission of e-mail messages or files.
- Provide expert testimony and investigative support as needed on various projects.
- Position included a DOD Secret Security Clearance.

Experience With Computer Forensics Examinations

Onsite Data Captures
- Over 300

Multi-Drive Analysis Projects
- Over 250

Drive Examinations
- Over 3500

Testimony – Expert Witness
- Depositions
- Court – State and Federal

Experience With The Following Computer Forensics Auditing Tools

Computer Forensics Tools (Software)

- Guidance Software - EnCase® Forensic, Enterprise, E-Discovery
- X-Ways Software Technology AG - X-Ways Forensics, WinHex
- Paraben Corporation - Email Examiner, Network Email Examiner, P2 Commander
- Agile Risk Management - F-Response
- SubRosaSoft.com - MacForensicsLab
- Forward Discovery - Raptor
- e-fense - Helix
- AccessData – FTK, DNA, PRTK
- Nuix - ProofFinder
- WetStone - Gargoyle
- Digital Detective - NetAnalysis
- Magnet Forensics - Internet Evidence Finder, Axiom
- ASR Data - SMART for Linux
- Windows PowerShell

Investigative/Analysis Tools for Examining:

- EXCHANGE
- OFFICE 365/MICROSOFT 365 EMAIL AND AUDIT LOGS
- LOTUS NOTES
- DOS
- WINDOWS
- NETWARE
- MACINTOSH
- LINUX/UNIX

Experience In The Following Operating System Structures

MS DOS
WINDOWS '95, 98, 2000, ME, XP, 2003, Vista, Windows 7, 10
WINDOWS NT 3.5.1 & 4.0
MACINTOSH
UNIX
LINUX
WINNT/2000, 2003, 2008 SERVER
WIN NT NTFS, GPT
FAT 12, FAT 16, FAT 32, & exFAT
HFS, HFS +
EXT3, EXT4

Experience In The Following Hardware and Media Types

FLOPPY DISKETTES
DISK DRIVES
MAGNETIC TAPES & OPTICAL MEDIA
REMOVABLE MEDIA (FLOPPY DISKS, ZIP DISKS, JAZZ DISKS, OPTICAL, CD/DVD ROM, SMART MEDIA, FLASH MEMORY AND MEMORY MEDIA CARDS)
DESKTOPS
LAPTOPS
CELL PHONES
TABLETS
USB & FIREWIRE DRIVES
OPTICAL CARTRIDGES
IDE DISK DRIVES
SCSI DISK DRIVES
USB EXTERNAL DEVICES
PERSONAL DATA ASSISTANTS (PDA'S)
SERVERS
RAID ARRAYS
DRIVE INTERVALS
DIGITAL DESIGN – CMOS/TTL INTEGRATED CIRCUITS
ANALOG DESIGN
STEPPER MOTORS
TELEPHONE SWITCHING SYSTEMS

Experience In The Following Programming/Assembly Languages

C
C++
FORTRAN
BASIC
PERL
PYTHON
VISUAL BASIC 5
DEC PDP8

PDP11/23
INTEL 8080/8085
CRAY-APML & CAL
SCRIPT/ BATCH INTERPRETERS: IBM EXEC & REXX;UNIX SHELL (C, BOURNE)
HTML/JAVA
ASSEMBLER (INTEL)
ENSCRIPT
WINDOWS POWERSHELL

Representative Project Experience

- A consortium of news media outlets, searching for potential election fraud, requested complete forensic analysis on Florida Secretary of State Katherine Harris' office computers. With portable server, mirror imaged 4 hard drives onsite. Conducted full forensic analysis of data readily accessible and recovered deleted data. Analyzed drive for partial or overwritten files. Completed analysis in approximately 20 hours. Searched across all data for documents containing 91 key words within certain date limitations. Produced specific data for clients on 48 CD's. Participated in press conferences and conference calls to explain the data.
  See: Barstow, David. "Data Permanently Erased from Florida Computers." *The New York Times.* 8 Aug. 2001.; Lauer, Nancy Cook. "Experts Access Harris' Computers." *Tallahassee Democrat Newspaper.* 2 Aug. 2001; Mollman, Steve. "Digging for Computer Dirt." *Salon.* 22 April 2002.
- Analyzed images from nine hard drives. Prepared detailed expert report for presentation in Federal Court. Case involved former employee hacking into company's system after departure. Involved analyzing drives from both the company and the suspected hacker. Based in large part on Kroll Ontrack's assistance, client was given a directed verdict. Case was presented for possible Federal criminal prosecution and the report was forwarded to the Federal prosecutor's office. Have been requested by the Federal Prosecutor's office to assist in further analysis and likely testimony in the criminal case.
- Assisted client by reviewing opposing party's expert testimony. Provided testimony and documentation to refute opposing party's expert opinions. This computer forensics consultation, among other things, helped the client to reach a favorable, six-figure verdict.
- Aid in planning case strategy, forming deposition and interrogatory questions, and evaluating opposing party's electronic evidence.
- Worked in cooperation with US and Cuban governments to assist in examining several computers that were involved in an international child kidnapping case. Traveled to Cuba to exchange data with Cuban authorities for their prosecution of the offending party.
- Traveled to Grand Cayman to image and analyze approximately 35 computers involved in a construction project dispute. Analysis showed that the majority, if not all of the computers were reformatted in the week prior to arrival. Data recovery efforts were successful in producing a large majority of the original data that was on the computers prior to the reformatting and reinstall of the Operating Systems.

Education

Kroll Ontrack, Inc.: On-the-job training in Kroll Ontrack data recovery technology, 1998-2004

Normandale Community College; Bloomington, Minnesota: Law Enforcement Program, 1989 – 1992.

Kevin V. Bluml, GCFA, GCFE, EnCE, CPP

Certifications

GIAC® Certified Forensic Analyst (GCFA) – February, 2020 – Present

GIAC® Certified Forensic Examiner (GCFE) – December, 2016 – Present

EnCase® Certified Examiner (EnCE) - June 2005 - Present

Microsoft Certified Professional (MCP) - 2000/2001

Certified Protection Professional (CPP) – 1993 - Present

Continuing Education and Training

SANS FOR508 - Advanced Incident Response, Threat Hunting, and Digital Forensics – November, 2019 – February, 2020

Taught SANS FOR500 - Windows Forensics – May-July 2018

SANS Blue Team Summit - April, 2018

SANS FOR408 – Windows Forensics Analysis Training – August, 2016

EnFuse (formerly CIAC) National Conference – May 2016

Minnesota IAFCI Annual Conference – October, 2014

Minnesota HTCIA Conference – April, 2014

Minnesota IAFCI Annual Conference – October, 2013

FACT Annual Conference – September, 2013

EnCase® V4 E-Discovery, Online training - February, 2013

EnCase® V7 Computer Forensics II, Online training - January, 2013

EnCase® V7 Computer Forensics I, Online training - November, 2012

Windows Registry Analysis – October, 2012

Minnesota IAFCI Annual Conference – October, 2012

EnCase® V7 Transition – Chicago, IL – August 2012

FACT Annual Conference – November, 2011

Minnesota IAFCI Annual Conference – October, 2011

ASIS National Security Conference – October, 2010

FACT Annual Conference – September, 2010

EnCase® Enscript Programming – Sterling, VA – April, 2010

EnCase® Advanced Computer Forensics – Pasadena, CA – March, 2010

EnCase® eDiscovery v3, Houston, Texas – January, 20010

EnCase® Enterprise v6 Examinations, Chicago, Illinois – November, 2009

EnCase® Network Intrusion Investigations, Houston, Texas – July, 2009

EnCase® Advanced Internet Examinations, Chicago, Illinois – June, 2009

EnCase® Examination of NTFS File Systems, Chicago. Illinois – May, 2009

FACT Annual Conference – October, 2008

Minnesota IAFCI Annual Conference – October, 2007

Minnesota HTCIA Conference – May, 2007

Secure 360 Conference – May, 2006

FACT Annual Conference – October, 2005

Minnesota HTCIA Conference – May, 2005

Expert Witness Training Course, William Mitchell Law School, St. Paul, Minnesota – November 13, 2003.

Computer Forensics Summit, Kroll Ontrack Inc., 3 Days – November 2003.

EnCase® Advanced Computer Forensics Course, Houston, Texas - October, 2003.

SMART - Next Generation Linux Forensics Course - 2003

ASIS National Security Conference – 2001

ASIS Pacific Rim Conference - 2001

Implementing and Supporting Microsoft Windows NT Server 4.0 in the Enterprise - 2000

ASIS National Security Conference - 2000

FACT Annual Conference – 1999

Minnesota Institute of Legal Education (MILE) - Expert Witnesses - 1999

DOS/Windows Operating system internals - 1998

Visual Basic 5 - 1998

Implementing and Supporting Microsoft Windows NT Workstation 4.0 - 1998

Implementing and Supporting Microsoft Windows NT Server 4.0 - 1998

Professional Organizations

Member, National and State chapter of American Society for Industrial Security (ASIS)
Past Member, National Information Technology Security Council (ASIS)

Member, Minnesota Chapter Infragard FBI and private sector partnership

Member, National and State chapter of Association of Certified Fraud Examiners (ACFE)

Member, National and State chapter of International Association of Financial Crimes Investigators (IAFCI)
Vice President, MN Chapter (IAFCI) 2012-2014

Past Member, Forensic Association of Computer Technologists (FACT) – Group no longer active

Past Member, National and State Chapters, High Technology Crime Investigation Association (HTCIA)
Treasurer, MN Chapter (HTCIA) 2014

Past Member and Former Director, Midwest Electronic Crime Investigators Association (MECIA) – since dissolved

Testimony

- *State of Minnesota v. Laura Scholz, Court File No. 27-CR-14-6136 – State of Minnesota District Court, County of Hennepin, Fourth Judicial District* – Court testimony, April 24, 2015, qualified as an expert witness. Testimony was mainly focused on the failure of the State to properly preserve electronic evidence and the difficulties and results caused by the delay in review.
- *American Lafrance Corp. v. Elite Power Prods.Corp.*, Case # 03-CV-119- Deposition testimony over two days – April 22, 2005 and May 20, 2005 – Case involved intentional date manipulation and data manipulation as well as attempted evidence spoliation
- *American Lafrance Corp. v. Elite Power Prods.Corp.*, Case # 03-CV-119-Testimony, Hearing held on April 16, 2004 – Circuit Court for Shawano, Wisconsin. Case involved disk alteration, date manipulation and evidence spoliation. Analysis showed that AutoCAD drawings had been modified and that the times and dates were manipulated in an attempt to have drawings appear to have been made years earlier than when they were actually done. Also determined that there was attempted evidence destruction within the 10 day time period before the hearing. Files on the original media had been deleted between the original production and the analysis of the original media on the date of the hearing. Preliminary injunction granted in part based upon the electronic evidence that was presented.
- *Breneisen v. Motorola, Inc.*, Case # 02-CV-02799-Deposition, March 12, 2004 – United States District Court for Northern District of Illinois, Eastern Division. Case involved searching for electronic copies of emails that existed on paper only and attempting to document the authenticity of them. Also documented the amount of data that was likely overwritten or destroyed due to the continued use. Case further involved detailed

analysis and comparisons of various email programs and their output. Finally, the case entailed analyzing data from four hard drives, three copies of the same hard drives that the defendant had imaged a month earlier, and a backup tape of the server that contained the emails for two of the three parties being investigated.

- *In re Gemstar Development Corp. Patent Litig*., Case # 02-MC-18-EA(J) -Deposition, October 22, 2003 – United States District Court for Northern District of Georgia (Discovery handled in Northern District of Oklahoma). Case involved two hard drives – the second one was not initially sent in until a recent file system create date was noticed on the first drive. Client then discovered that there was a second hard drive that had not been turned over to them. The second hard drive had evidence of having been dropped. Performed standard recovery and produced the data via EDV.
- *Coin Acceptors, Inc. v. Lejeune*, Ct. File # C-2003-90918 IJ – Deposition, August 26, 2003 – Expert Testimony, September 4, 2003 - Circuit Court for Anne Arundel County, Maryland. Case involved recovering deleted data from ex-employee's hard drive, comparing it to data from a CD-ROM that was turned over during discovery, and showing that the data on the CD-ROM had been on the drive and deleted prior to the drive being returned to the company.
- *Travelocity.com v. Josephs and Orbitz*, *LLC,* Ct. File # 03 CH 8280 - Deposition - Circuit Court of Cook County, Illinois (County Department, Chancery Division) August 7, 2003. Case involved theft of trade secrets; provided testimony related to the installation of a Zip drive two days before employee's departure.
- *Kelly v. Kelly,* Case # 142-8-02 LEDM - Court Testimony - Vermont District & Family Court - Hyde Park, VT - June 26, 2003. Divorce case involving locating and validating Internet based email messages.
- *In re Request for Removal of Matthes,* City of Prescott Common Council – testimony before council meeting – Prescott, Wisconsin – February 26, 2003. Case involved allegations of inappropriate use of city computer by city employee.
- *State v. Tripp,* Case # CR72448, Circuit Court, Buchanan County, MO – Deposition – Eden Prairie, MN – February 20, 2003. Murder case, involving computer evidence and use of wiping utility on computer hard drives.
- *McKibbins v. International Business Machines,* Case # CV99-04465 CBM (AJWx) – Court Testimony – Federal Court – Los Angeles, CA - February 28, 2002, Evidentiary Hearing Motion In Limine. Case involved offensive emails that Kroll Ontrack recovered from backup tapes. Testified about processes and authenticity.
- *Jackson v. Microsoft Corporation,* Case # C01-775P*,* Court Testimony – Federal Court - Seattle, WA – December 13, 2001. Qualified as an expert witness.
- *NMS Services, Inc., v. The Hartford Fire Ins. Co.,* Case # 01-667-A – Deposition – Baltimore, MD – November 6, 2001.
- *Langeslag v. KYMN, Inc.*, Case # C1-99-892 - Deposition - Minneapolis, MN - April 16, 2001.
- *Curtiss v. Pierce* –Trial Testimony - Hastings (Dakota County), MN - November 2, 2000. Qualified as an expert witness.
- *Pinnacle Real Estate Tax Services Inc v. Chicago Title & Trust*, Case #160604 - Deposition - McLean, VA - August 4, 1999.
- *Med-Link Technologies Inc v. Ashish Kupoor/Sita Kupoor* - Deposition - Florham Park, NJ - July 1, 1999.
- *Emerson v. Nims* - Deposition - Minneapolis, MN - June 22, 1999.
- *International Ass'n of Machinists & Aerospace Workers v. Northwest Airlines, Inc.*, Case # 112772 & 124600 Arbitration - St. Paul, MN - October 19, 1998.

Technical/Professional Presentations

ASIS National Conference; Dallas, TX - October 2010.

Twin Cities Chapter of Association of Certified Fraud Examiners – August 2009

Minnesota Chapter of International Association of Financial Crimes Investigators – April 2008

Minnesota chapter of HTCIA 1st annual conference, Brooklyn Park, MN – September 2002.

ASIS Conference on International Security Management; Amsterdam, The Netherlands – April 2002.

ASIS National Conference; San Antonio, TX - October 2001.

ASIS Pacific Rim Conference; Honolulu, HI - March 2001.

FBI Infragard seminar; St. Paul, MN - March 2001.

3M Cyberincident response team; St. Paul, MN - February 2001.

ASIS National Conference; Orlando, FL - September 2000.

ARMA/PRISM International's 1999 Joint Symposium; Las Vegas, NV - December 1999.

New Jersey CPAs; East Brunswick, New Jersey - October 1999.

AICPA Conference; Washington, DC - September 1999.

National Defender Investigator Association, 1999 Midwest Regional Conference; Minneapolis, MN - September 1999.

Joint Conference of HTCIA and ISSA; Boston, MA - June 1999.

ASIS Computer Security Seminar; Los Angeles, CA - April 1999.