Donald E. Vilfer, J.D., CFE, ACE

Professional:

Vilfer & Associates, Inc., dba Califorensics 2002-present. President of Firm that emphasizes fact-finding and computer forensics in support of complex litigation or referral for prosecution. Representative clients include law firms, state and local government, pharmaceutical companies, aircraft manufacturers, financial institutions and school districts. Cases have included investigation of fraud, theft of intellectual property, computer crimes and forensics, employee misconduct, sexual harassment, environmental litigation and defense of complex fraud. Extensive experience in obtaining and analyzing computer forensic evidence. Experience as an expert witness and court-approved expert.

Perry-Smith LLP, 2001-2002, Senior Director, Litigation Support and Investigative Services Group. Led the Litigation Support and Investigative Services practice area for Sacramento's largest regional accounting firm. Supported attorneys in civil and criminal litigation involving clients from a variety of sectors, including manufacturing, aerospace, banking, education, real estate and government.

Federal Bureau of Investigation, 1986-2001.

1996-2001, Supervisory Special Agent for the White Collar Crime and Computer Crimes Squad. Conducted and oversaw the investigation of white collar crime and computer crimes. Achieved successful prosecutions in the areas of Securities Fraud, Bank Fraud, Embezzlement, Intellectual Property Rights, Computer Crimes and Bankruptcy Fraud. Oversaw the largest Intellectual Property Rights case in the FBI. Supervised the FBI Computer Forensics Team (CART). Supervised a successful international investigation of a series of computer intrusions into financial institutions, resulting in the arrest and conviction of those involved.

1994-1996, Supervisory Special Agent for the Rapid Start Team. At FBI Headquarters, Washington D.C., managed a team of professionals responsible for the on-site management of major cases and crisis worldwide on over 50 cases at venues from the White House to the Oklahoma City bombing command post. Led a project to develop an automated litigation support package for complex white-collar cases.

1986-1994, Special Agent. While assigned as Special Agent, Washington D.C. field office, conducted an investigation of an international multi-billion dollar bank fraud (BCCI). Oversaw a team of agents and financial analysts responsible for gathering relevant evidence and tracing proceeds. Conducted investigation and asset tracking throughout the US, England, the Cayman Islands and Abu Dhabi.

As Assistant Division Counsel, provided legal advice and instruction in criminal, civil, and employment law areas. Reviewed affidavits for search warrants and court orders.

Delaware Ohio County Prosecuting Attorney's Office, 1986. Prosecuted criminal cases and successfully briefed and argued an appeal.

Donald E. Vilfer, J.D., CFE, ACE
(continued)

Education:

Bachelor of Science, Criminal Justice/Pre-Law, Bowling Green State University, 1982.

Ohio State University College of Law, Juris Doctorate, 1986.

Specialized Training:

Access Certified Examiner (ACE) certification for Computer Forensics and Decryption.

Four months training at the FBI Academy, including courses in White Collar Crime.

50 Hour Certified Fraud Examination course, including investigation, computer crime, law and accounting.

Advanced White-Collar Crime courses during tenure with the FBI.

One week Computer Crimes course for FBI Supervisors.

Advanced Computer Forensics training.

Network Forensics and Cell Phone Forensics training.

FBI Computer Security class.

FBI class for Supervisory Special Agents over Computer Crimes investigations.

Continuing Legal Education Instructor, *Computer Forensics for Attorneys.*

Frequent guest and consultant to media on crime and computer forensics matters.

Legal Instructor for the National Business Institute.

FBI Instructor for International Law Enforcement Training Academy in Budapest

Affiliations:

Member of the Ohio Bar (inactive status).
Certified Fraud Examiner (CFE).
Access Certified Examiner (ACE).
Member of the California Association of Licensed Investigators.
Associate Member of the Sacramento County Bar Association.

Califorensics

2281 Lava Ridge Court, Suite 130
Roseville, CA 95661
TEL: (916) 789-1602
FAX: (916) 789-1609

September 30, 2010

Mitchell Baker, Esq.
1543 Champa St, Suite 400
Denver, CO 80202

Re: *U.S. v. Harper*
Report of Findings Related to CILC

Dear Mr. Baker:

You asked us to use the forensic images produced in discovery to recreate and analyze your client's software product, Case Investigative Lifecycle (CILC), as it was when the Federal Bureau of Investigation (FBI) executed a search warrant and imaged the computers used by the defendants.

In conducting our analysis, we performed the below enumerated procedures:

- We received forensic images of the computers imaged by the FBI in 2005 and reviewed the drives for general contents and computer names.
- We determined through discussions with you the devices most likely to contain relevant program files.
- We used the forensic images to boot in a virtual environment the defendant's computers as they existed at the time of the search warrant.
- We examined the various components of the CILC software as it existed on the computers and servers at the time the FBI executed its search warrant.
- We reviewed the current version of the software.

Upon performing these procedures, we developed the findings set forth in this report, which include the following:

1. The CILC software did not appear to be "vaporware" but included a large amount of complex coding that would have required significant development.
2. The CILC software was functional at the time of the search warrant.
3. The software contained many notable features, making it a functional product for the intended consumer.

4. A market for software that has the functionality of CILC exists.

Findings

1. The CILC software did not appear to be "vaporware" but included a large amount of complex coding that would have required significant development.

The CILC software does not appear to be "vaporware." In other words, it does not appear as though the developers created fake programs that were not usable or that they did not intend to continue to develop. On the servers on which the CILC program was developed, we observed a large amount of source code as well as Microsoft Visual Studio, a software development suite, evidencing that development efforts were taking place on these servers.

We also observed software products that could be used as the backend, or the underlying components for a program, which is consistent with the program the defendants were developing. These software products include an Oracle database installation that could support the data structures required to drive a case management database, an Apache web server capable of driving a website that could operate as a front end, or user interface to that database and Perl, a scripting language that would assist in the generation of web pages.

Additionally, we observed installation binaries on these servers. When the server component of the CILC product was installed on our test machine, the installation program prompted for the locations of the following software packages: Oracle, Apache, Perl and CesarFTP. These are likely components that would be required to run the case management system developed by the defendants.

2. The CILC software was functional at the time of the search warrant.

We were able to fully install a server and client for CILC on one of our test machines. However, upon running the CILC client after installation, we were prompted with the message "Error initializing your security key." We did not have access to a working product key and were not able to continue to test the 2005 client-server version of the product. We did successfully run CILC Basic, a standalone version of the CILC software found on the forensic image named bbirpq1ddimage, which was from the computer named IRPSOLDSK002.

We tested the product by booting the computer image on which it was found as a virtual machine and then launching the program and using it much like the intended user would use the product. We opened an existing case and entered data concerning the fictional investigation. The data entered included information about initial investigation and follow-up. We verified that the program saved this information and that it was viewable when the program was again opened. We also verified that the previously entered information was retrievable within the program using the "Find" feature within the CILC program. We also verified that the size of the case file grew with each entry of data and upon saving of the case.

Throughout the use of the program, we found no feature that did not appear to function as intended. The timeline search did not return results for all of the points in time entered into the case, but only drew upon manually entered timeline points from the Lead Sheet section. This is how the software apparently was intended to function, but limits the analysis capabilities of the software. While we used the software as an intended end-user would use the software, it is possible other features could have performance issues we did not detect. With no item found to have such an issue, and dozens of features working without fault, we are able to conclude the software was functional at the time the search warrant was executed.

3. The software contained many notable features, making it a functional product for the intended consumer.

We evaluated both the software as it existed at the time of execution of search warrant and the software as it exists in 2010. The CILC Basic software described above was evaluated for whether it was a functional product for law enforcement, the intended consumer. The software as it existed at the time of the search, had the capability to track a wealth of information about investigations. The program allowed for gathering information about crime scenes, manpower assignments, arrests, notifications, vehicles, weapons, evidence, searches and other relevant data. The program allowed for the addition of photos and other files. The Follow-up tab within the program allowed for assigning and tracking leads in the investigation and information regarding interviews. The Prosecution Phase tab allows for the tracking of witness and District Attorney information, exhibits and discovery. It appears this portion of the program could be used by investigator or prosecutor.

The CILC Basic program from 2005 was a functional product for the intended consumer in that it would facilitate an investigator tracking many important details during an investigation. Such a tool is invaluable to the investigator working complex investigations with many witnesses, items of evidence and details to track and cross-reference. The program includes reminders concerning the recommended procedures during various phases of investigation—helpful to even the most experienced investigators. The CILC Basic version of the program appears best suited for individual investigators or small agencies, with all of the data apparently being written to the case file. A single investigator could use the program to track information on his or her own investigations. A small agency could place the case file on a server and access it to open, edit and save from individual networked computers. In our testing, the search feature did not search across multiple cases and could thus limit the program's usefulness to larger agencies that need to search across all investigations for cases assigned to investigators or suspect/witness names. Presumably, the client-server version of the software as it existed in 2005 would have offered the same functionality we observed in CILC Basic, but with data stored in a central database, more likely searchable by multiple users across multiple cases. As detailed below, the current enterprise version of the CILC program we did review offered this sort of functionality as well as additional analysis capabilities.

The 2010 version of the software was also reviewed by us. We reviewed the software by first receiving a demonstration of the software from the developers and then requesting they perform various actions at our direction and under our supervision while noting the results. The tasks were designed to test the usefulness of the software as well as the design and architecture of the current client-server version of CILC. We found that this software had many of the same features described above in the CILC Basic program with many enhancements to the design or architecture of the program. For example, the program was web-based, using standard web browsers to access the data from a central database. This is far more common today than in 2005 and would be a welcome feature to inexperienced users. The program also does not store data locally, a welcome security feature given the mobility of computers in most agencies.

We observed that the current version of the CILC enterprise software appeared to be able to integrate with a variety of databases, making it likely more attractive to a wider variety of agencies who might seek to integrate it with their current databases (Oracle, SQL etc). Another welcome feature is the customizable nature of the program, allowing agencies to have their particular data needs addressed in the client interface. The program included built-in link analysis capabilities to analyze data entered across multiple fields. The program also included an electronic case file, allowing for centralized storage and tracking of all documents associated with the case. This case file could be located within an agency's network storage or inside the database. The version also included a feature to require supervisor approval for various tasks or submissions to the database.

The version of the client-server software reviewed by us was associated with a SQL database. We directed the developers to enter data into the fields of the program and then verified that the data was truly written to the database and not simply displayed on the screen or stored in a flat file. Using MySQL, we verified that the SQL database did in fact contain the newly entered data.

4. A market for software that has the functionality of CILC exists.

It has long been a challenge of law enforcement to effectively manage data related to investigations. Gone are the days of paper reports and only physical files within departments. All agencies now rely on digital data to track information about their cases. There are many companies that create and market software for this purpose to law enforcement. These companies often boast of being able to manage information from "Dispatch through Prosecution" and it appears the CILC software strives to similarly manage information throughout the criminal justice pipeline. No one software application would meet the needs of all agencies, but the functionality that we observed in our review of the CILC software would undoubtedly be of interest to many law enforcement agencies.

Sincerely,

Don Vilfer
Califorensics