GORDON P. ERSPAMER (CA SBN 83364)
GErspamer@mofo.com
EUGENE ILLOVSKY (CA SBN 117892)
EIllovksy@mofo.com
STACEY M. SPRENKEL (CA SBN 241689)
SSprenkel@mofo.com
MORRISON & FOERSTER LLP
425 Market Street
San Francisco, California 94105-2482
Telephone: 415.268.7000
Facsimile: 415.268.7522

Attorneys for Plaintiffs
Vietnam Veterans of America; Swords to Plowshares: Veterans Rights Organization; Bruce Price; Franklin D. Rochelle; Larry Meirow; Eric P. Muth; David C. Dufrane; Tim Michael Josephs; and William Blazinski

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

VIETNAM VETERANS OF AMERICA, *et al.*,

Plaintiffs,

v.

CENTRAL INTELLIGENCE AGENCY, *et al.*,

Defendants.

Case No. CV 09-0037-CW

DECLARATION OF JOHN FREDERICK ASHLEY ADDRESSING RETREIVABILITY OF DATA ON MAGNETIC TAPES

Complaint filed January 7, 2009

I, John Frederick Ashley, declare as follows:

1. I serve as the Executive Vice President at Encore Discovery Solutions (EDS), 1225 Eye Street N.W., Suite 500, Washington, DC 20005 (www.encorediscovery.com). EDS, which specializes in computer forensics and the recovery of digital data, maintains one of the largest corporate computer forensics laboratories in the United States. I currently lead the electronic discovery consulting, computer forensics, and data analytics groups.

A. GENERAL BACKGROUND AND QUALIFICATIONS

2. From 1997 - 2000, I was the head of the Greater Manchester (U.K.) Police Department's Computer Examination Unit, which at the time was the largest criminal computer forensics unit in Europe. I was responsible for all computer examinations in Manchester, England, North Wales, and the Isle of Man. I also conducted and supervised electronic retrieval projects in other jurisdictions and advised prosecutors on issues involving electronic evidence collection.

3. I have presented to the Houses of Parliament and taught courses on computer evidence recovery at Bramshill Police Staff College, the British Computer Society, and various universities, including the American University in Washington D.C.

4. Most recently, I was the Chief Executive Officer of Ashley Litigation Counseling and previously the National Practice Leader and Executive Vice President for consulting and computer forensics at First Advantage Litigation Counseling.

5. Since 1989, I have qualified and testified as an expert in the fields of computer forensics and electronic discovery on approximately eighty occasions in Federal and State courts throughout the United States as well as in Europe. In at least ten of those instances, I testified specifically regarding the retrieval of data from back-up tapes and spoliation of electronic evidence.

6. My *curriculum vitae*, which is annexed hereto as Exhibit "A", provides more details about my professional background and experience, including the details of my experience as an expert consultant and witness in matters related to computer forensics.

B. COMPUTER FORENSICS

7. Computer forensics refers to a branch of digital forensic science pertaining to legal evidence found in computers and digital storage media. The goal of computer forensics is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing, and presenting facts and opinions about the information.

8. Computer based evidence is primarily recovered from magnetic media, usually hard drives, removable media, or tape. Magnetic media are designed to retain their information for long periods without change, typically many years or decades, unless their contents are overwritten with new data. Accordingly, computer data can exist in a recoverable form that is capable of yielding admissible, relevant, and probative evidence for many years after it has been created.

9. There are different options for retrieving the data discussed in Paragraph 8. These include reproducing the hardware/software configurations used originally to store the data on magnetic tapes or, in the absence of the original software, by converting the data files to a format capable of being interacted with on a different or more modern computer system.

10. The methods explained in Paragraph 7 will, in most instances, result in the recovery of the data at issue. The probability of recovery is enhanced by the existence of duplicate copies of the magnetic tapes on other types of media.

C. SCOPE

11. I was retained in this matter to opine on the retrievability of data stored on "magnetic tapes." My understanding is that Defendants used these magnetic tapes as storage devices in the 1970s and presently claim that the data is irretrievable by currently available technology.

D. OVERALL CONCLUSION

12. In my opinion, based on my experience and on my review of the materials described below, a suitably qualified and equipped company can be identified that would be capable of retrieving the electronic data from the magnetic tapes in question.

E. RETRIEVABILITY OF THE FILES STORED ON THE MAGNETIC TAPES

13. With respect to this matter, I received from counsel and reviewed the document referred to as the "Manifest", VET001_009230 - VET001_009235. This document appears to be a list of the contents of 11 boxes which references a number of magnetic tapes, including duplicates. I received from counsel and reviewed an index to the "Partial Printout", VET102_000518 - VET102_000537, which Defendants have represented they believe is a partial listing of the contents of those tapes, and I reviewed similar appearing documents produced in conjunction with the Partial Printout, VET102_000001 – VET102_000020; VET102_000129 – VET102_000148; and VET102_0000356 – VET102_000395. I also reviewed part of the CIA administrative record, VET020-000196-VET020-000199, a recent Request for Information ("RFI") issued by the Defendant U.S. Department of Defense ("DOD"), which is attached hereto as Exhibit B, and photographs of the particular magnetic tapes. Prior to my review I signed the Protective Order acknowledgement form issued by this Court.

14. Based on that documentation, the DOD is in possession of both original magnetic tapes and a series of duplicate magnetic tapes that appear to contain Edgewood-related data of files saved to tapes in the early 1970's.

15. I have been informed that the CIA and DOD, through its counsel, allege that unidentified declassification personnel from each agency cannot access, read, or convert that data to a readable form.

16. I was advised by counsel concerning the meet-and-confer ordered by the Court regarding the magnetic tapes issue, and I have been informed that the DOD has declined to answer any questions regarding the hardware or software used in the creation of those tapes or the specific details of any previous attempts to access, read, or convert the data. I have been informed that Defendants have since informed Plaintiffs that they have asked internal agencies such as Department of the Army's Medical Research and Material Command ("MRMC"), and the Defense Technical Information Center ("DTIC") and the Defense Logistics Agency ("DLA") as well as two external agencies, Battelle Memorial Institute and UNISYS as to whether they possessed capability to convert or review the magnetic tapes. I understand that Defendants have

neither provided any specific details of these requests or responses beyond stating that these organizations did not possess the requisite hardware to perform the conversion nor have they made any showing that these agencies are qualified in data retrieval or data restoration. See paragraph 32 below.

17. My review of the Partial Printout and Manifest provided by plaintiffs indicates that the magnetic tapes were used in connection with a UNIVAC 1108 computer system, that FORTRAN was used to compile output from that system, that the data management system from System Development Corporation called ADEPT was used, and that the storage transmittal documents refer to data output from the Edgewood database(s) as SYMOUTS.

18. UNIVAC 1108 was a 36-bit mainframe, multi-processor, computer system introduced in 1964 by Sperry Rand that used integrated circuits and transistorized electronics. Approximately 296 processors were ultimately sold to the government and other customers.

19. FORTRAN is a general-purpose programming language developed by IBM in the 1950s for scientific and engineering applications with the first FORTRAN compiler being delivered in 1957. It is still widely in use today.

20. ADEPT (Advanced Development Prototype) is a comprehensive information-processing system implemented at System Development Corporation ("SDC") in the late 1960s. It was used with mainframe computers to manage, share and control sharing of data by users throughout the lifecycle of the data. The system included programs that allow the user to describe entries in a database, load them onto a machine, ask questions about them, perform calculations on them, have them presented for analysis, obtain hard-copy reports, and update and maintain the database. It is not clear whether Defendants retained or archived the ADEPT system so that it is available today.

21. I understand that System Development Corporation ("SDC"), the developer of ADEPT, was formed as a spinoff of System Development Division of the RAND Corporation in 1957 for the purpose of working in the public interest on research, development, and application of information technology and the system sciences associated with computers. Its main customer

was the U.S. military and it was acquired by the Borroughs Corporation in 1980 based upon SDC's expertise and experience in systems engineering capability.

22. Assuming that: (a) the partial printout corresponds to the magnetic tapes; (b) the original tapes or the corresponding duplicate tapes are in good condition and not corrupt, the probability of which is increased by the existence of duplicate tapes; and (c) the tapes were constructed using a UNIVAC 1108 computer system, FORTRAN programming language, and ADEPT software, in my expert opinion, the content of the magnetic tapes can be accessed today.

F. PRIOR CONVERSION EFFORTS OF DATA FILES

23. My review of a November 1, 1973 Memorandum at VET001_009236 indicates that the data files were also sent to OJCS, which I understand is the acronym for the CIA Office of Joint Computer Service.

24. It appears from the documents I was provided that the OJCS converted some of these software programs for use on its own OJCS hardware and was in the process of converting the file management functions from ADEPT to GIMS II, when that work was suspended in 1973. The memorandum does not indicate what type of hardware was used. It is not clear whether Defendants' counsel has attempted to search OJCS records storage within DOD for copies of the converted data.

25. The memorandum indicates that the GIMS II system OJCS conversion of transfer of the data files was suspended and not completed, but OJCS had concluded that it was feasible to convert the files to hardware and the GIMS II data management system and that work had started on the project.

26. It would be helpful to confirm if the DOD still has these files in a semi-converted state and whether it still uses the GIMS II data management system or software.

27. This memorandum further supports my conclusion detailed in Paragraph 12 that the data on the magnetic tapes is capable of being accessed as the OJCS was successful in beginning to convert certain programs and files from the UNIVAC/ADEPT platform to OJCS hardware and software in 1973.

G. RELATION OF PARTIAL PRINTOUT TO SUBSTANCE ON THE MAGNETIC TAPES

28. My review of VET001_009235 of the Manifest indicates that the Tapes in Box #10 contain GULF output files and other final databases, as well as DEFINE, COMPOSE, and SHOW routines, which presumably resulted in data printouts of selected data.

29. GULF, specifically identified on the Manifest, is System Development Corporation's designation for an output of a file as it physically exists on disk. DEFINE, COMPOSE and SHOW are in all reasonable probability routines built into the ADEPT system. In my experience DEFINE would detail the report or printout which is needed from the database, COMPOSE would detail the query that will be run against the database and SHOW would detail the result(s) of the query or series of queries being run.

30. Some of the entries on the Manifest were redacted. For example, on page 5 at VET001_009235, which is submitted with this declaration, the following passage appears: "GULF of Edgewood and [redacted] final data bases, as well as DEFINE, COMPOSE, and SHOW routines." It would be helpful to know what information has been redacted from the "Manifest" as that information may assist in enabling or insuring access to the data stored on the tapes.

31. Examination of the material which I was provided, detailed in Paragraph 13 above, indicates that the partial printouts may be the result of querying databases and printing the results. The format or construction of those queries is unknown. The documents appear to provide various information related to fields in the database which identify the names, service numbers, volunteer numbers, test substances and doses, and other information concerning participants in the Edgewood testing program, including details relating to some of the individual plaintiffs. In all reasonable probability there is other relevant data stored on the magnetic tapes than is reflected in the partial printouts.

H. INFORMATION THAT WOULD BE HELPFUL TO FURTHER ASSESS THE RETRIEVAL OF THE INFORMATION ON THE MAGNETIC TAPES

32. In order to make a definitive conclusion about whether the information or files on the magnetic tapes can be retrieved, answers to the following questions would be necessary or helpful:

a) Was the UNIVAC 1108 computer system and ADEPT system the origin for the data stored on the magnetic tapes?

b) If the hardware and software discussed in subparagraph a) were not the origin, what is the make and model of the computer system and the make and version of the software used to create the magnetic tapes?

c) What are the make, model, and size of the backup tapes?

d) What tape drive was used to create the magnetic tapes?

e) What other systems, if any, were used to create the magnetic tapes?

f) Is the type of hardware and software used to create the magnetic tapes still in the possession or control of the Defendants or from any other government agency?

g) What employees, active or retired, still exist that have worked with the equipment used to write the data to the magnetic tapes?

h) What attempts have been made to consult with or involve the employees or unit that first created the magnetic tapes or that provided the electronic files from Edgewood?

i) What are the specific details discussed in Paragraph 16 regarding the attempts to access, read, or convert the tapes?

j) What are the technological capabilities of the sources the government consulted to attempt to access, read, or convert the magnetic tapes?

k) What is the current format of the magnetic tapes?

l) In what location have the tapes been stored?

m) In what condition have the magnetic tapes and duplicates been stored?

n) Have the tapes been rewound on a certain frequency?

o) Is there any external labeling on the tapes? If so, what do those labels contain?

33. I understand that Plaintiffs' counsel has asked the Defendants' counsel for this information in a meet and confer session, and that all of their queries have been refused thus far.

34. It would be helpful to have access to inspect the tapes in order to make a determination regarding access and conversion. I understand that defendants have claimed that the files contained on the magnetic tapes were classified as "secret" at the time the magnetic tapes were originally created in approximately 1973-1974, and that no declassification review has yet been conducted. Thus, because the tapes themselves are not alleged to be classified, but rather it is the content or data on the tapes to which the government still claims classification based on an original determination made 38 years ago, I would recommend that the Court allow inspection of the magnetic tapes by Plaintiffs' representative to facilitate the access of the data, which would not infringe any claimed privilege to the information on the tapes.

35. I have been informed that the DOD has publicized a Request for Information ("RFI") located at https://www.fbo.gov/index?s=opportunity&mode=form&tab=core&id=dd35b20789a9d4d9312005e5588d8d71&_cview=0 for "digitizing old magnetic tapes." The RFI is "not a request for proposals (RFP), and is not to be construed as a commitment by the government to issue a solicitation or ultimately award a contract. [It] is for planning and market research purposes only." The RFI "seeks to identify responsible potential sources and obtain information regarding price, delivery time, and capabilities."[1]

[1] Annexed hereto as Exhibit B is a true and correct copy of the RFI, which states: "This is a Sources Sought/Request for Information (RFI) only. This Sources Sought, in accordance with FAR 15.201(e), is not a request for proposals (RFP), and is not to be construed as a commitment by the government to issue a solicitation or ultimately award a contract. This is for planning and market research purposes only and shall not be considered as an obligation on the part of the Government to acquire any products or services. Responses will not be considered as proposals, nor will any award be made as a result. Responses will not be returned.

(Footnote continues on next page.)

36. In my expert opinion, because there is insufficient information provided in the RFI, including a complete lack of answers to the questions enumerated in Paragraph 32, no technician would be able to properly respond to the RFI or credibly assess the effort required to retrieve the data stored on the tapes

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct and that this Declaration was executed on this 13th day of December, 2011.

/s/ John Frederick Ashley
John Frederick Ashley

(Footnote continued from previous page.)

Washington Headquarters Services (WHS) / Acquisition Directorate (AD), seeks to identify responsible potential sources and obtain information regarding price, delivery time, and capabilities for those sources who can provide one or a combination of the following:

1. Digitized onto searchable PDF documents and saved to either a CD or DVD six (6) UNIVAC 1108 system magnetic reels of tape, or

2. Digitized onto unsearchable PDF documents and saved to either a CD or DVD six (6) UNIVAC 1108 system magnetic reels of tape, or

3. Printed copies (read and transcribed) of the six (6) UNIVAC 1108 system magnetic reels of tape onto paper preferably sized 11x18 but no smaller than 8.5x11.

Additional information about the tapes:

The six (6) UNIVAC 1108 system magnetic reels of tape were created in March 1972.

Submittal Information:

Interested parties may submit a capability statement, no more than five (5) pages, for your company, your teammates and/or subcontractors. This information should include an estimate on price, an estimate on how long it would take to deliver the requested information, the way you can deliver the information (1, 2, 3 or any combination thereof) your Facility Business Clearance (none, Secret, Top Secret), and the business size standard for North American Industry Classification Systems NAICS Code 518210. Please include company name, company address, and Cage Code. Also, please indicate if you, your teammates and/or subcontractors fall under any of the categories listed by the Small Business Administration, i.e. Women Owned Small Business.

Attestation Pursuant to General Order 45, section X.B

I hereby attest that I have on file all holograph signatures for any signatures indicated by a "conformed" signature (/S/) within this efiled document.

/s/ Gordon P. Erspamer
Gordon P. Erspamer

EXHIBIT A

Curriculum Vitae
John F. Ashley

Name:	John F. Ashley
Address:	Epiq Systems
	1225 Eye Street, N.W. Suite 500, Washington, DC 20005
Telephone:	202.556.0041
E-mail	JAshley@EpiqSystems.com

Professional Experience

Apr 2011 – Present	**Epiq Systems. EVP, Consulting and Forensics**
Jul 2010 – Apr 2011	**Encore Discovery Solutions, EVP, Consulting and Forensics**
Sep 2009 – Jul 2010	**Ashley Litigation Consulting, Chief Executive Officer**
Nov 2008 – Aug 2009	**First Advantage Litigation Consulting, National Practice Leader**
Jan 2006 – Oct 2008	**First Advantage Litigation Consulting, EVP, Electronic Evidence**
Apr 2004 - Dec 2005	**First Advantage CoreFacts, Chief Technology Officer**
Jan 2001 - Apr 2004	**CoreFacts, Chief Technology Officer**
Jul 2000 - Dec 2000	**CoreFacts Resources, Director, Electronic Evidence**

Responsible for designing, equipping and supervising one of the largest corporate computer forensics laboratories on the East Coast. Forensic computer hardware configured to optimize leading forensic software.

Case Studies

- Representation of plaintiff corporation in a contractual dispute with federal government requiring the restoration of 40 back-up tapes held on three different types of magnetic media, containing the Emails and user created data of a staff of 160 persons. The data had been created over a 30-month period and total data size was 183 gigabytes. Three Email packages, MS Outlook, Netscape and ccMail were successfully investigated.
- Defense representation in a software trade secrets dispute requiring the capture of 14 terabytes of data within a 45-day period, without interrupting client's workflow. Data from 320 NT workstations, 90 NT laptops and 15 servers was forensically captured. In excess of 300 search terms were run across the encapsulated data, all relevant Email folders and electronic documents were hosted on secure web servers and reviewed by more than 50 attorneys throughout the US.
- Plaintiff representation in a breach of fiduciary duty, contract, trade secret and misappropriation of confidential information case requiring the capture of data from five NT laptops and the restoration of six months backup of Email data for five former employees.
- Plaintiff representation in a financial mismanagement case requiring the imaging and investigation of 71 laptop drives.

1998 - July 2000 Greater Manchester Police, Computer Examination Unit, Unit Head

- Responsible for forensic data retrieval from all computers used in crime, covering a population of 3.5 million people.
- Managed workload increase from 153 cases in 1997 to 263 cases in 1999.
- Designed and installed Microsoft NT4 networks of investigation machines.
- Given additional responsibility for the forensic examination of all computers seized in North Wales and the Isle of Man.
- Wide experience of covert intrusion investigations involving imaging, monitoring and surveillance techniques.
- Employed on a consultative basis to manage the establishment of a number of computer forensics units for a variety of UK police forces.
- Provided vulnerability advice to various public bodies.
- Considerable fraud investigation experience involving the majority of accountancy software packages.
- Advised and assisted in technical interviews of computer skilled offenders on many occasions.

1996 - 1998 Greater Manchester Police, Computer Examination Unit, Senior Forensic Investigator

- Managed the accreditation of the Unit to the internationally accepted ISO 9002 standard.
- Designed and Installed a Novell network of investigation machines.
- Interviewed, appointed and trained forensic investigation detectives.

1989 - 1996 Greater Manchester Police, Obscene Publications Unit, Supervisor / Investigator

- The first police officer in the UK to investigate computer pornography.
- Responsible for data retrieval from pornographers' and pedophiles' computer systems.
- Investigated all forms of technical crime involving computers: hacking, cracking, virus writing, phreaking, mobile phone cloning and credit card duplication.
- Lead investigator in a number of international obscenity and pedophile cases.

Expert Witness Testimony

- Expert witness in the investigation and prosecution of Dr. Harold Shipman for the murder of 15 patients. Testified in relation to 12 of the 15 victims regarding the forensic investigation of a complex computer network that revealed back dated and falsely inserted records leading to the identification of victims who were subsequently exhumed. Provided 500 exhibits and 120 witness statements relating to the suspicious deaths of patients. Shipman found guilty on all counts.
  Filmed and interviewed in the UK, by Ed Bradley, for CBS's 60 Minutes regarding the computer forensics skills deployed in this case. The program screened in January and June 2001.
  Filmed and interviewed in the UK, by The Learning Channel regarding the computer forensics skills deployed in this case. The program first screened in the US in March 2001.
- Expert witness for the prosecution in a trial involving the large-scale theft of hard drives from Quantum. Performed a forensic financial analysis of the suspect's corporate server accounting packages. Investigation revealed a wide distribution network throughout Europe. Testified in Wolverhampton Crown Court over a five-day period. All five defendants found guilty.
- Expert witness for the prosecution in a trial involving the theft of corporate computers throughout the north of England. Conducted forensic analysis of residual data found on a large number of re-formatted stolen hard disk drives assisted in identifying the original owners of recovered computer equipment. Testified in Manchester Crown Court over a five-day period. Defendant found guilty.
- Expert witness for the prosecution in a trial involving the running of an electronic bulletin board system that was the UK gateway to an international network involved in the worldwide electronic distribution of obscene material. Testified in Maidstone Crown Court. Two defendants found guilty.
- Expert witness for the prosecution in a trial involving the blackmail of 17 individuals. Forensic examination of a word processing system revealed systematic threat letters held in hidden and limbo files. Testified at Manchester Crown Court. Two defendants found guilty.
- Expert witness for the prosecution in a trial involving international disk based distribution of obscene material. Testified at Swindon Crown Court. Defendant found guilty.
- Expert witness for the prosecution in a North Wales case involving distribution of pedophilic material via the Internet. Forensic examination of a computer hard drive refuted defense testimony that an unknown person had used Back Orifice 2000 and Netbus to gain control of the defendant's machine.

Notable Cases

- On behalf of the Securities and Futures Authority, assisted Guernsey Police and a team of forensic accountants, in the forensic on-site imaging and investigation of two computer networks comprising a total of 22 machines in relation to the Sumitomo Corporation $2.6 billion copper fraud.
- On behalf of the FBI, carried out UK Home Office authorized house searches relating to the recovery of computer related data from laptops and other storage media in the possession of two Libyan males suspected of involvement in the bombing of US Embassies in Africa.
- On behalf of the Isle of Man Police, investigated a laptop computer that had been surrendered by the user who had found that he was being anonymously blackmailed via Email. Forensic examination uncovered evidence that the user had gained employment within the IT section of a major offshore bank and had accessed customer's private identification information, which was then provided to a criminal group in Belgium. This group had subsequently blackmailed him via an Email service provider in Texas when he had refused to assist them further with their criminal activity.
- In conjunction with the US Customs and Postal Service, forensically investigated the electronic contents of 18 hard drives used in Denmark to run two pedophile electronic bulletin board systems. Recovered evidence led to the identification of individuals who had downloaded pedophilia in the US and the UK.
- Forensic examination of two encrypted hard drives found evidence that led to the simultaneous worldwide arrest of 120 pedophiles. Many of the individuals involved were exchanging digital images of their actual abuse of children via secure web servers. One of which was known as Wonderland and was located in Boston, Massachusetts.
- Forensic examination of a suspect's computer revealed 35 live viruses and plans to infect viruses in a number of UK corporations. Further analysis revealed the breach of a US based grocery company's customer credit card database, where customer credit card details had been posted on bulletin boards and used by group members for international communication. This led to the simultaneous arrest of five individuals who were collectively known as ArcV, a high profile virus-writing group.
- Forensic examination of a re-formatted hard drive revealed more than 100 fraudulent Internet credit card purchase transactions and the distribution network for the illegally purchased goods.
- On behalf of New Scotland Yard gained access to a number of electronic bulletin boards that were distributing pedophilia. Subsequently provided evidence and assistance to their technical experts and the Metropolitan Police Computer Crime Unit.

Speaking Engagements

- Appeared on a number of television and radio programs in the UK in relation to computer forensics and communications investigation work.
- Profiled on British weekly prime time show "The Cook Report" regarding techniques used in identifying English users of a Danish pedophile Internet bulletin board.
- Lectured on Computer Forensics at Merseyside Police Training College.
- Lectured on Computer Crime at Bramshill Police Staff College.
- Guest speaker at the British Computer Society.
- Lectured on Computer Pornography at the University of Central Lancashire.
- Lectured on Computer Crime at the University of Manchester Institute of Science and Technology.
- Consultant to the Association of Chief Police Officer's Working Group into Computer Pornography.
- Presentations given at the Houses of Parliament and in Manchester to the Home Affairs Select Committee that led to amendments to UK law in relation to the sentencing of child offenders and the creation of a new offence in relation to electronic pseudo photographs.
- Lectured on Computer Forensics to the F3 Forum, a group comprising the majority of UK law enforcement and corporate computer forensic experts.
- Lectured on Computer Forensics at the American University, Washington D.C.
- Lectured on Computer Fraud to the Virginia Society of Certified Public Accountants.

Education

- Educated at Sir John Deane's Grammar School, Northwich, Cheshire graduating in 1969 with Certificates in Mathematics, English Language, Geography and French.
- Jul 1969 - Jan 1971 Cheshire Constabulary Police Cadet graduate.
- Jan - Apr 1971 Police Training Center Constable graduate.
- Oct 1977 examination qualification to the rank of Sergeant.
- Oct 1980 examination qualification to the rank of Inspector.
- Nov 1989 - Dec 1993 in force computer investigation training with ongoing IS specialized support.
- 1990 - 1994 various UK based data retrieval and network training seminars.
- 1995 Computer Forensics software and hardware training provided by Computer Forensics Ltd.
- 1996 Advanced Computer Forensics software and hardware training provided by Computer Forensics Ltd.
- 1996 Computer Forensics software and hardware training provided by Authentec Data Recovery specialists.
- 1997 Advanced Computer Forensics techniques software and hardware training provided by Vogon International Ltd.
- 1998 Data Networks and Communications training seminars provided by CLC.
- Computer Forensics experiential learning throughout the period 1989 - 2010.

US Expert Deposition and Testimony

December 2000, selected as an independent computer forensics expert by the United States District Court for the eastern District of Virginia, Alexandria Division, to assist in an intellectual property dispute that centered on verifying the electronic time and date stamp information of the plaintiff's software prototypes and supporting electronic presentations. Subsequently deposed at length by the plaintiff's attorney. Four days into trial, the case settled at the plaintiff's request, a day prior to my scheduled testimony.
Dr. Bradley S. Fordham v. OneSoft Corporation, et al.,
Civil Action No. 00-1078-A (Eastern District of Virginia)

June 2001, testified and cross-examined as the defendant's computer forensics expert, before the judicial court of Harris County, Texas, in support of a defendant corporation's motion to mirror image and investigate the plaintiff's electronic storage devices. Motion granted.
Gyrodata Inc. v. Baker Hughes Inc. and Baker Hughes Inteq.,
Cause No. 2000-40391 (Harris County, Texas 127th Judicial District)

August 2001, United States District Court for the Eastern District of Virginia, deposed as the plaintiff's computer forensics expert in a multi defendant unsolicited bulk email litigation. I provided expert opinion based on my analysis of more than 125,000 member complaints.
AOL v. Netvision Audiotext, dba Cyber Entertainment Network, et al.,
Civil Action No. 99-1186-A (Eastern District of Virginia)

September 2001, testified and cross-examined as the defendant's computer forensics expert, before the judicial court of Harris County, Texas, in support of a defendant corporation's rebuttal of a motion alleging spoliation of electronic evidence.
Gyrodata Inc. v. Baker Hughes Inc. and Baker Hughes Inteq.,
Cause No. 2000-40391 (Harris County, Texas 127th Judicial District)

October 2001, United States District Court for the Eastern District of Virginia, deposed as the defendants' and counter-plaintiffs' computer forensics expert in a breach of contract, breach of fiduciary duty, theft of trade secrets and violation of the Electronic Communications Privacy Act litigation.
Beyond Technology Corp. v. WebMethods, Inc., and K. Alyssa Berg,
Civil Action No. 01-655-A (Eastern District of Virginia)

October 2001, 53rd District Court of Travis County, Texas, deposed as the plaintiff's computer forensics expert in an employee solicitation and theft of trade secrets case.
Advanced Fibre Communications v. Calix Networks, Inc. and Tony Roach,
Cause No.GN102712 (53rd District Court of Travis County, Texas)

June 2002, United States District Court for the Middle District of Florida, Fort Myers Division, deposed as the defendants' and counter-plaintiffs' computer forensics expert in a defamation and tortious interference with business relationships litigation.
Gary Van Meer, and Palm Harbor Medical, Inc. v. Stryker Sales Corp.,
Civil Action No. 2:00-CV-454-FTM-29D (Middle District of Florida)

June 2002, testified and cross-examined as a computer forensics expert, before the United States District Court for the Middle District of Florida, Fort Myers Division, in support of defendants' and counter-plaintiffs' motion alleging spoliation of electronic evidence.
Gary Van Meer, and Palm Harbor Medical, Inc. v. Stryker Sales Corp.,
Civil Action No. 2:00-CV-454-FTM-29D (Middle District of Florida)

September 2002, testified and cross-examined as the plaintiff's computer forensics expert, before the United States District Court for the Southern District of Florida, Miami Division, in support of plaintiff's motion for contempt alleging spoliation of electronic evidence and support of plaintiff's rebuttal of defendant's motion to dismiss preliminary injunction and temporary restraining order.
Plaintiff's motion for contempt upheld, with the defendant being ordered to pay all of the plaintiff's attorney's and expert's fees which were incurred during the investigation and presentation of the contempt motion.
Four Seasons Hotels and Resorts B.V., Four Seasons Hotels (Barbados) Limited,
Four Seasons Hotels Limited, and Four Seasons Caracas, C.A. v. Consorcio Barr, S.A.,
and Carlos L. Barrera,
Case No. 01-4572 CIV-MOORE

October 2002, United States District Court for the Eastern District of Virginia, deposed as the plaintiff's computer forensics expert in a litigation concerning unsolicited bulk email. I provided expert opinion concerning the persons responsible for the transmission of tens of millions of unsolicited bulk commercial emails.
Verizon Internet Services, Inc. v. Alan Ralsky, et al.,
Civil Action No. 01-0432-A (Eastern District of Virginia)

October 2002, testified as the defendant's computer forensics expert, before the United States District Court for the Middle District of Florida, Fort Myers Division, in response to plaintiffs' motion alleging spoliation of electronic evidence.
Gary Van Meer, and Palm Harbor Medical, Inc. v. Stryker Sales Corp.,
Civil Action No. 2:00-CV-454-FTM-29D (Middle District of Florida)

November 2002, testified and cross-examined as the defendant's computer forensics expert, before the United States District Court for the Middle District of Florida, Fort Myers Division, in rebuttal of plaintiffs' computer forensics expert's evidence supporting a motion alleging spoliation of electronic evidence.
Gary Van Meer, and Palm Harbor Medical, Inc. v. Stryker Sales Corp.,
Civil Action No. 2:00-CV-454-FTM-29D (Middle District of Florida)

January 2003, testified and cross-examined, at trial, as plaintiff's computer forensics expert, before the United States District Court for the Southern District of Florida, Miami Division. Testimony encompassed Computer Fraud and Abuse, Electronic Communication Interception, and Trade Secret Theft.
Four Seasons Hotels and Resorts B.V., Four Seasons Hotels (Barbados) Limited, Four Seasons Hotels Limited, and Four Seasons Caracas, C.A. v. Consorcio Barr, S.A., and Carlos L. Barrera,
Case No. 01-4572 CIV-MOORE

January 2003, rebuttal testimony and cross-examination, at trial, as plaintiff's computer forensics expert, before the United States District Court for the Southern District of Florida, Miami Division. Testimony encompassed Computer Fraud and Abuse, Electronic Communication Interception, and Trade Secret Theft.
Rebuttal testimony proved that one of the defendant's key electronic exhibits was not original, but had been fabricated in an attempt to deceive the court.
Final Judgement issued May 9, 2003 awarded plaintiffs $4,877,600.00 in damages.
Four Seasons Hotels and Resorts B.V., Four Seasons Hotels (Barbados) Limited, Four Seasons Hotels Limited, and Four Seasons Caracas, C.A. v. Consorcio Barr, S.A., and Carlos L. Barrera,
Case No. 01-4572 CIV-MOORE

May 2003, United States District Court for the District of Columbia, deposed as the defendant's computer forensics expert in a litigation alleging racial bias and discrimination.
Provided testimony in relation to the alteration, fabrication and authentication of email.
The plaintiff withdrew his allegations a short time later and the case settled.
Timothy Dean and Michelle Dean v. Starwood Hotels & Resorts Worldwide Inc., d/b/a The St. Regis Washington by Starwood Hotels and Resorts,
Civil Action No. 1:02CV00867

July 2003, testified and cross-examined, at trial, as plaintiff's computer forensics expert, before the United States District Court for the Eastern District of Virginia, Alexandria Division. Testimony encompassed tortious interference with business relationships, breach of contract, civil conspiracy and spoliation of data.
Plaintiff's awarded in excess of $565,000 in damages.
CACI Dynamic Systems, Inc. v. Delphinus Engineering, Inc., and James R. Everitt, Jr.,
Civil Action No. 02-1454-A

January 2004, testified and cross-examined, in arbitration, as claimant's computer forensics expert, before an Arbitration Tribunal of the American Arbitration Association in Charleston, South Carolina. Testimony encompassed tortious interference with business relationships, breach of contract and spoliation of data. Arbitrator subsequently awarded claimant $10,567,478 and reimbursement of claimant's arbitration costs.
CACI Dynamic Systems, Inc. v. V. Allen Spicer,
AAA Case No. 16 160 00725 02

March 2004, United States District Court for the Southern District of New York, deposed as the defendant's computer forensics expert in a litigation alleging unfair dismissal. Provided testimony in relation to the creation and authentication of a document produced in paper form by the plaintiff.
Michelle Bell v. Davis & Partners, LLC and Wolf Management & Leasing, LLC,
Civil Action No. 03CV4175

November 2004, testified and cross-examined as plaintiff's computer forensics expert, at a Preliminary Injunction Hearing, before the United States District Court for the District of Maryland, Northern Division. Testimony encompassed the defendants' co-ordinated use of data destruction utilities to prevent the discovery of the plaintiff's stolen source code and proprietary information.
Bowe Bell + Howell Company v. Document Services Inc., and Albert M. Harris et al.,
Civil Action No. 043418

November 2004, testified and cross-examined as plaintiff's computer forensics expert, in rebuttal to counter defendants' testimony and provide pattern analysis to show the extent of defendants' data destruction efforts, at a Preliminary Injunction Hearing, before the United States District Court for the District of Maryland, Northern Division.
The Judge granted the plaintiff broad injunctive relief and found that the defendants had intentionally destroyed relevant documents and indicated that an adverse inference instruction will likely be given to the jury as a sanction.
Bowe Bell + Howell Company v. Document Services Inc., and Albert M. Harris et al.,
Civil Action No. 043418

March 2005, provided testimony, in arbitration, as respondent's computer forensics expert, before an Arbitration Tribunal of the American Arbitration Association in Philadelphia, Pennsylvania. Testimony encompassed the restoration of Lotus Notes e-mail and attachments from multiple back-up tapes.
Boston Power Group v. Alstom Power, Inc.,
AAA Case No. 14-Y-110-01410-03

March 2005, testified and cross-examined as plaintiff's computer forensics expert, at a Preliminary Injunction Hearing, before the United States District Court for the Eastern District of Michigan, Southern Division. Testimony encompassed the defendants' theft of trade secrets and proprietary information and the defendants' spoliation of evidence.
The Judge granted the plaintiff broad injunctive relief and scheduled a spoliation hearing for April 2005.
Henkel Corporation v. Charles K. Cox and Chemtool Corporation,
Civil Action No. 050735

April 2005, United States District Court for the Eastern District of Michigan, Southern Division, deposed as the plaintiff's computer forensics expert. Testimony encompassed the defendants' theft of trade secrets, proprietary information and spoliation of evidence.
Henkel Corporation v. Charles K. Cox and Chemtool Corporation,
Civil Action No. 050735

November 2005, United States District Court for the Southern District of Indiana, Indianapolis Division, testified as the defendants' and counter-plaintiffs' computer forensics expert in a motion hearing concerning the recovery of deleted email. Parties agreed that I be the expert, appointed as an officer of the court, to oversee the retrieval of deleted email from a number of desktop and laptop computers and a Blackberry device.
Roy O. Ball and Norman W. Bernstein v. Versar, Inc.,
Cause No. IP01-C-0531-H/K

April 2006, United States District Court for the Northern District of California. Appeared as the plaintiffs electronic discovery and computer forensics expert in a securities litigation discovery conference. Assisted in technical discussions concerning electronic discovery, including the identification of backup tapes and the database production format of reviewed data.
JDS Uniphase Corporation Securities Litigation,
C-02-1486 CW (EDL)

May 2006, United States District Court for the Northern District of California. Appeared as the plaintiffs electronic discovery and computer forensics expert in a securities litigation discovery conference. Assisted in technical discussions concerning electronic discovery, including the restoration of backup tapes and the production of certain filetypes in native format.
JDS Uniphase Corporation Securities Litigation,
C-02-1486 CW (EDL)

June 2006, United States District Court for the Northern District of California. Appeared as the plaintiffs electronic discovery and computer forensics expert in a securities litigation discovery conference. Assisted in technical discussions concerning electronic discovery, including the production of metadata from departmental shared servers and the preservation of indices for multiplexed backup tapes.
JDS Uniphase Corporation Securities Litigation,
C-02-1486 CW (EDL)

September 2006, United States District Court for the Eastern District of Pennsylvania, deposed as the plaintiff's computer forensics expert. Testimony encompassed the defendants' theft of trade secrets, theft of proprietary information and spoliation of evidence.
DeCODE Genetics, Inc., v. Dr. Hakon Hakonarson et al.,
Civil Action No. 06-CV-3461

September 2006, United States District Court for the Eastern District of Pennsylvania, testified as the plaintiff's computer forensics expert in a Preliminary Injunction Hearing. Testimony encompassed the defendants' theft of trade secrets, theft of proprietary information and spoliation of evidence.
DeCODE Genetics, Inc., v. Dr. Hakon Hakonarson et al.,
Civil Action No. 06-CV-3461

November 2006, United States District Court for the Eastern District of Pennsylvania, testified as the plaintiff's computer forensics expert in a Preliminary Injunction Hearing. Testified in rebuttal of defendants' and opposing expert's testimony. Testimony encompassed the defendants' theft of trade secrets, theft of proprietary information and spoliation of evidence.
DeCODE Genetics, Inc., v. Dr. Hakon Hakonarson et al.,
Civil Action No. 06-CV-3461

April 2007, United States District Court for the District of Idaho, deposed as the defendants' computer forensics expert. Testimony encompassed the plaintiff's destruction of data, internet activity, none production of a large external removable media device, theft of proprietary information and spoliation of evidence.
Peter Wachtell v. Capital One Financial Corporation and Capital One Services Inc.,
Civil Action No. 03-267-S-MHW

August 2007, Circuit Court for Baltimore County, deposed as the defendants' computer forensics expert. Testimony encompassed the retrieval of previously deleted deeds of trust and analysis of embedded and attaching metadata.
Patrice Saylor v. Glenna Hass, et al.,
Case No. 03-C-06-005226

September 2007, Circuit Court of Arlington County, testified as the plaintiff's computer forensics expert at a spoliation of evidence hearing. Testimony encompassed the defendants' non preservation and non production of electronic devices for analysis.
CACI, Inc v. Robert Donovan et al.,
Case No. 06-1289

July 2008, United States District Court for the District of Delaware. Computer forensics and electronic discovery declarant for defendants. Declaration encompassed the plaintiffs electronic discovery production and document retention.
Advanced Micro Devices Inc. and AMD International Sales & Service, Ltd., v.
Intel Corporation and Intel Kabushiki Kaisha,
Civil Action No. 05-441 (JJF)

August 2008, United States District Court for the District of Delaware. Computer forensics and electronic discovery declarant for defendants. Declaration encompassed rebuttal of the plaintiffs electronic discovery production and document retention response to my July, 2008 declaration.
Advanced Micro Devices Inc. and AMD International Sales & Service, Ltd., v.
Intel Corporation and Intel Kabushiki Kaisha,
Civil Action No. 05-441 (JJF)

January 2009, United States District Court for the District of Delaware. Computer forensics and electronic discovery declarant for defendants. Declaration submitted to update the Court on the progress of the defendants investigation of the plaintiffs electronic discovery production.

Advanced Micro Devices Inc. and AMD International Sales & Service, Ltd., v.
Intel Corporation and Intel Kabushiki Kaisha,
Civil Action No. 05-441 (JJF)

February 2009, Circuit Court for Baltimore County, testified as the defendants' computer forensics expert. Testimony encompassed the retrieval of previously deleted deeds of trust and analysis of embedded and attaching metadata.
Patrice Saylor v. Glenna Hass, et al.,
Case No. 03-C-06-005226

April 2009, Superior Court of the State of California, County of Santa Clara, deposed as the plaintiff's computer forensics and electronic discovery expert. Testimony encompassed the defendants' theft of trade secrets and theft of proprietary and confidential information.
Jasmine Networks, Inc. v. Marvell Semiconductor, Inc. et al.,
Case No. 1-01-CV801411

November 2010, testified and cross-examined, as defendant's computer forensics and electronic discovery expert, before the United States District Court for the Eastern District of Virginia, Richmond Division. Testimony encompassed alleged spoliation of data.
E. I. du Pont de Nemours and Co. v. Kolon Industries, Inc.
Civil Action No. 3:09CV00058

February 2011, testified and cross-examined, as defendant's computer forensics and electronic discovery expert, before the United States District Court for the Eastern District of Virginia, Richmond Division. Testimony encompassed alleged spoliation of data and restoration of recovered deleted email.
E. I. du Pont de Nemours and Co. v. Kolon Industries, Inc.
Civil Action No. 3:09CV00058

July, 2011, American Arbitration Association, New York, New York, deposed as the claimant's computer forensic and electronic discovery expert. Testimony encompassed the global misappropriation of market data, the breach of subscription and redistribution agreements and the destruction of DACS permissions records.
BGCantor Market Data, L.P., Cantor Fitzgerald & Co., and Cantor Fitzgerald Securities v. Tullett Prebon Information (C.I.) Ltd. F/K/A Tullett Financial Information (C.I.) Ltd.
Case No. 50 148 T 00737 10

August, 2011, American Arbitration Association, New York, New York, testified as the claimant's computer forensic and electronic discovery expert. Testimony encompassed the global misappropriation of market data, the breach of subscription and redistribution agreements and the destruction of DACS permissions records.
BGCantor Market Data, L.P., Cantor Fitzgerald & Co., and Cantor Fitzgerald Securities v. Tullett Prebon Information (C.I.) Ltd. F/K/A Tullett Financial Information (C.I.) Ltd.
Case No. 50 148 T 00737 10

August 2011, testified and cross-examined, as defendant's computer forensics and electronic discovery expert, before the United States District Court for the Eastern District of Virginia, Richmond Division. Testimony encompassed the timing and method of acquiring alleged trade secrets.
E. I. du Pont de Nemours and Co. v. Kolon Industries, Inc.
Civil Action No. 3:09CV00058

EXHIBIT B

Digitizing old magnetic tapes

Solicitation Number: RFI-UNIVAC1108Tapes
Agency: Other Defense Agencies
Office: Washington Headquarters Services
Location: WHS, Acquisition Directorate

Note: There have been modifications to this notice. You are currently viewing the original synopsis. To view the most recent m
click here

Solicitation Number: RFI-UNIVAC1108Tapes

Notice Type: Sources Sought

Synopsis:
Added: Oct 31, 2011 12:55 pm

This is a Sources Sought/Request for Information (RFI) only. This Sources Sought, in accordance with FAR 15.201(e),is not a request for proposals (RFP), and is not to be construed as a commitment by the government to issue a solicitation or ultimately award a contract. This is for planning and market research purposes only and shall not be considered as an obligation on the part of the Government to acquire any products or services. Responses will not be considered as proposals, nor will any award be made as a result. Responses will not be returned.

Washington Headquarters Services (WHS) / Acquisition Directorate (AD), seeks to identify responsible potential sources and obtain information regarding price, delivery time, and capabilities for those sources who can provide one or a combination of the following:

1. Digitized onto searchable PDF documents and saved to either a CD or DVD six (6) UNIVAC 1108 system magnetic reels of tape, or

2. Digitized onto unsearchable PDF documents and saved to either a CD or DVD six (6) UNIVAC 1108 system magnetic reels of tape, or

Processin
Services

3. Printed copies (read and transcribed) of the six (6) UNIVAC 1108 system magnetic reels of tape onto paper preferably sized 11x18 but no smaller than 8.5x11.

Additional information about the tapes:

The six (6) UNIVAC 1108 system magnetic reels of tape were created in March 1972.

Submittal Information:

Interested parties may submit a capability statement, no more than five (5) pages, for your company, your teammates and/or subcontractors. This information should include an estimate on price, an estimate on how long it would take to deliver the requested information, the way you can deliver the information (1, 2, 3 or any combination thereof) your Facility Business Clearance (none, Secret, Top Secret), and the business size standard for North American Industry Classification Systems NAICS Code 518210. Please include company name, company address, and Cage Code. Also, please indicate if you, your teammates and/or subcontractors fall under any of the categories listed by the Small Business Administration, i.e. Women Owned Small Business.

Please consult the list of document viewers if you cannot open a file.

RFI

Type: Other (Draft RFPs/RFIs, Responses to Questions, etc..)
Posted Date: October 31, 2011

RFI - Digitizing magnetic tapes.pdf (6.10 Kb)
Description: PDF description of RFI/Sources Sought

Contracting Office Address:
Rosslyn Plaza North, Suite 12063
1155 Defense Pentagon
Washington, District of Columbia 20301-1155
United States

Primary Point of Contact.:
Meghan Morgan
meghan.morgan@whs.mil
Phone: 703-545-1159

Return To Opportunities List

For Help: Federal Service Desk Accessibility