# EXHIBIT A

# APPLICATION FOR SEARCH WARRANT
G.L. c. 276, §§ 1-7

TRIAL COURT OF MASSACHUSETTS

NAME OF APPLICANT: KEVIN M. CHRISTOPHER

NEWTON — COURT DEPARTMENT

MIDDLESEX — DIVISION

POSITION OF APPLICANT: DETECTIVE

SEARCH WARRANT DOCKET NUMBER: 0912 SW 03

I, the undersigned **APPLICANT**, being duly sworn, depose and say that:

1. I have the following information based upon the attached affidavit(s), consisting of a total of 17 pages, which is (are) incorporated herein by reference.

2. Based upon this information, there is **PROBABLE CAUSE** to believe that the property described below:

- ☐ has been stolen, embezzled, or obtained by false pretenses.
- ☒ is intended for use or has been used as the means of committing a crime.
- ☐ has been concealed to prevent a crime from being discovered.
- ☐ is unlawfully possessed or concealed for an unlawful purpose.
- ☒ is evidence of a crime or is evidence of criminal activity.
- ☐ other *(specify)*_____

3. I am seeking the issuance of a warrant to search for the following property *(describe the property to be searched for as particularly as possible)*:
DELL COMPUTER W/ WHITE COVER AND GRAY TRIM, ALL OBJECTS CAPABLE OF STORING DIGITAL DATA IN ANY FORM, INCLUDING BUT NOT LIMITED TO CENTRAL PROCESSING UNITS, OPTICAL SCANNERS, DIGITAL CAMERAS, MODEMS, ROUTERS, MEMORY STICKS, THUMB OR USB DRIVES, FIREWALLS, TAPES, ZIP DRIVE DISKS, DIGITAL VIDEO DISKS, PRINTERS OPERATING SYSTEMS, APPLICATION PROGRAM DISKS, SOFTWARE, HARDWARE, CD-ROMS, COMPUTER ACCESS CODES, PASSWORDS AND/OR PROTOCOLS, ALL MANUELS, BOOKS, BROCHURES, ALL EVIDENCE OF

4. Based upon this information, there is also probable cause to believe that the property may be found *(check as many as apply)*:
- ☒ at *(identify the exact location or description of the place(s) to be searched)*:
[redacted]

which is occupied by and/or in the possession of: RICCARDO F CALIXTE

- ☒ on the person or in the possession of *(identify any specific person(s) to be searched)*:
RICCARDO F. CALIXTE
- ☐ on any person present who may be found to have such property in his or her possession or under his or her control or to whom such property may have been delivered.

**THEREFORE,** I respectfully request that the court issue a Warrant and order of seizure, authorizing the search of the above described place(s) and person(s), if any, to be searched, and directing that such property or evidence or any part thereof, if found, be seized and brought before the court, together with such other and further relief that the court may deem proper.

I ☐ have previously submitted the same application.
I ☒ have **not** previously submitted the same application.

PRINTED NAME OF APPLICANT: DET KEVIN M. CHRISTOPHER

SIGNED UNDER THE PENALTIES OF PERJURY:
x DET. K. Christopher #174
Signature of Applicant

SWORN AND SUBSCRIBED TO BEFORE
x Catherine M. Coyle
Signature of Justice, Clerk-Magistrate or Assistant Clerk

3-30-09
DATE

COMMONWEALTH OF MASSACHUSETTS

MIDDLESEX, SS TRIAL COURT

NEWTON DIVISION DISTRICT COURT DEPT

---

# APPLICATION AND AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

---

**(M.G.L., Ch. 276, ss. 1 to 7; St. 1964, C. 557)**

I, Kevin M. Christopher, being duly sworn, hereby depose and say that:

1) CLASSIFICATION OF SEARCH. Based upon the information contained or referenced herein, there is PROBABLE CAUSE to believe that the property described below:

- ☐ has been stolen, embezzled, or obtained by false pretenses.
- [X] is intended for use or has been used as the means of committing a crime.
- ☐ has been concealed to prevent a crime from being discovered.
- ☐ is unlawfully possessed or concealed for an unlawful purpose.
- [X] is evidence of a crime or is evidence of criminal activity.
- ☐ as otherwise specified:

2) DESCRIPTION OF ITEMS TO BE SEARCHED FOR AND SEIZED.

a. I am seeking the issuance of a warrant to SEIZE the following property:

(1) All objects capable of storing digital data in any form, including but not limited to central processing units ("CPUs"), optical scanners, digital cameras, modems, routers, memory sticks, thumb or USB drivers, firewalls, tapes, zip drive disks, digital video disks ("DVDs"), and computerized printers (which objects, as a whole, shall be referred to herein as the "Computer System").

(2) All of the Computer System's documentation, including but



KMC

not limited to:

(a) Operating System and Application programming disks, software, hardware, CD-ROMs, etcetera;

(b) Manuals, books, or brochures pertaining to computer programs and/or applications;

(c) Manuals, books, or brochures pertaining to an Internet Service Provider(s).

(3) Computer access codes, passwords and/or protocols.

(4) All evidence of ownership of, access to, and/or control over the Computer System on Sunday, March 01, 2009 at approximately 1959 hrs and Saturday, March 07, 2009 at approximately 1812 hrs.

b. And to transport the Computer System to a secure location and, there, to EXAMINE said Computer System for the following evidence:

(1) All of the Computer System's documentation, including but not limited to:

(a) Operating System and Application programming disks, software, hardware, CD-ROMs, etcetera;

(b) Manuals, books, or brochures pertaining to computer programs and/or applications;

(c) Manuals, books, or brochures pertaining to an Internet Service Provider(s).

(2) Computer access codes, passwords and/or protocols.

(3) All evidence of ownership of, access to, and/or control over the Computer System on Sunday, March 01, 2009 at approximately 1959 hrs and Saturday, March 07, 2009 at approximately 1812 hrs.

3) DESCRIPTION OF THE PLACE TO BE SEARCHED. Based upon the information contained or referenced herein, there is also probable cause to believe that the property may be found at:

a. The residence of [redacted] in



KM

Chestnut Hill, Massachusetts, being more fully described as follows:

1. [redacted] is a multi dwelling complex which contains 41 units in which 154 students and 2 staff members reside.
2. The front entrance is located just off of Commonwealth Ave and it is labeled [redacted] above the front entrance doors.
3. There are several (7) entrances in the rear of the structure which are located directly on the campus.
4. The exterior of the building is constructed with a light beige/yellow brick, with brown doors & windows with copper gutters, down spouts and copper flashing. The roof is a multicolored slate roof.
5. Upon entering the front entrance doors you step into a glass foyer and pass through another set of glass doors which leads into a larger foyer. Directly in front there is a set of blue stairs which lead down one flight to the second floor (blue vinyl) (10 steps to a landing and then another 4 steps down). Directly in front of the stairs there is a concierge desk, take a right and proceed down the hallway, there is an elevator to the right and a conference room directly opposite, continued past a lounge on your left and through another door (at which time the floor becomes a multi-colored tile floor – beige, blue & pink). Upon passing through this door [redacted] is directly on your right, continue down the hallway (constructed of cinder blocks painted beige) and [redacted] is the next door on your right. There is only one entrance to [redacted].
6. [redacted] has a blue door with a silver kick-plate. There is a maroon room marker above the door inscribed [redacted]. In addition there is a handmade orange construction paper door tag with a green construction paper tri-circular shape

(similar to Mickey Mouse) with the names; Chris, Ryan, Jeffrey and Ricardo and [redacted] written on it.

7. Which is occupied by and/or in possession of Riccardo F. Calixte (herein referred to as "the premises");

4) BASIS OF PROBABLE CAUSE. The basis of my belief that probable cause exists justifying this search warrant is as follows:

a. On 01/27/09 Officer Eng filed a report regarding two Boston College students who were having domestic issues. The reporting party was identified as [redacted] and the other student was identified as Riccardo F. Calixte. The roommate issues are being addressed by Residential Life staff at this time. [redacted] also advised Officer Eng that Mr. Calixte is involved in some computer hacking incidents. [redacted] advised Officer Eng that Mr. Calixte has changed grades for other students by accessing the Boston College computer system. Mr. Calixte is also reported to be an employee of the Information Technology department here at Boston College. It should be noted that [redacted] is not only a named witness to these allegations but also a reliable witness in another investigation which he brought to our attention.

b. On 01/28/09 I met with [redacted] to discuss these allegations further. At this time he advised me of the following. Mr. Calixte is a computer science major who is considered a master of the trade amongst his peers. He is also employed by the Boston College I.T. department. [redacted] stated that he was aware of Mr. Calixte's reputation as a "hacker" prior to him being assigned into his room. [redacted] stated that Mr. Calixte has a Dell computer with a white cover and gray trim, a couple of external hard drives and other media devices which he owns and/or uses. [redacted] stated that it is not uncommon for Mr. Calixte to appear with unknown laptop computers which he says are given to him by Boston College for field testing or he is "fixing" for other students. Mr. Calixte was also a suspect in a stolen Boston College laptop computer

report I investigated previously. [redacted] reported that Mr. Calixte uses two different operating systems to hide his illegal activities. One is the regular B.C. operating system and the other is a black screen with white font which he uses prompt commands on. This computer has three log on fields and it is reported that Mr. Calixte uses the nicknames "enigma" and "Bootleg enigma". [redacted] reported to me that he has observed Mr. Calixte hack into the B.C. grading system that is used by professors to change grades for students, he has "fixed" computers so that they cannot be scanned by any system for detection of illegal downloads and illegal internet use, "jail breaks" cell phones, possibly stolen ones, for people so that the phones can be used on networks other than they are meant for and downloaded program software against the licensing agreement for free. [redacted] also advised me that Mr. Calixte has a cache of approximately 200+ illegally downloaded movies as well as music from the internet. [redacted] also stated that Mr. Calixte has personally implicated himself in illegal activity to him on previous occasions.

c. [redacted] told me that since his problems with Mr. Calixte his brand new computer has crashed and he suspects that Mr. Calixte is responsible. Mr. Calixte has access into [redacted]'s computer as he set it up for him when they were friends and he knows the password. The computer has been looked at by several experts and none of them can resolve the problem.

d. [redacted] has also recently been the victim of a mass e-mailing to the Boston College community in which he is reported to be gay and coming out of the closet. A gay web site profile was also created in [redacted]'s name and was attached to the e-mails. The use of a Boston College list server was used to accomplish this. The e-mails were sent via g-mail and yahoo. I have sent compliance/preservation letters to all of the required sites and subpoena request letters for information regarding these e-mails.



KMD

e. I was later contacted by the Boston College Director of Security for I.T, Mr. David Escalante and he advised me that he was contacted by a non-police Administrator who is working with [redacted] due to the stress he has encountered as a result of these e-mails. The Administrator asked him to look into the origin of the e-mails and he did. Mr. Escalante advised me that the suspect e-mails were traced back to Mr. Calixte.

f. Mr. Escalante told me the following:

(a) On two occasions web-based email accounts (gmail and yahoo mail) were used to send email to a mailing list at BC. The yahoo message included the IP address of the client used to send the message. This IP was 136.167.207.174 – indicating the sender was on the BC campus, and was using a wired connection in Gabelli residence hall.

(b) Records from the network registration system show that the computer was registered as a guest (rather than the usual student or faculty/staff). The registration system also contained the following additional information:

| | |
|---|---|
| Hardware Address: | 00:23:38:BE:38:24 |
| Computer Name | bootleg-laptop |
| Operating System | Unix Linux |
| Email Address | smaikopt@ctst.org |
| IP Lease Start Time | Saturday, March 7, 2009 17:44:12 |
| IP Lease End Time | Sunday, March 8, 2009 4:38:58 |

c) Searching the history of the registration system for additional uses of the computer name "bootleg-laptop" reveals that was used on August 24, 2008 by a computer registered to Riccardo F. Calixte.

d) The content of the email sent to the BC mailing list included a screen shot of a web page hosted on www.adam4adam.com. This website allows people to create a personal profile that others can view. The screenshot was of a fake profile for the victim of the email. Examination of network logs showed that the IP address used to send the email had not been to visit www.adam4adam.com.



KW

Reviewing network DNS logs for the five days prior to the initial email, we found one computer in Gabelli that had been to www.adam4adam.com. Looking this IP address and time in the network registration system returned the following information:

| | |
|---|---|
| Name: | Riccardo F. Calixte |
| Hardware Address: | 00:19:B9:4D:31:3E |
| Computer Name: | calixtri-ubuntu |
| Operating System: | Unix Linux |
| IP Lease Start Time: | February 27, 2009 2:47:39 |
| IP Lease End Time: | Sunday, March 1, 2009 20:08:46 |

e) Calixte had previously registered another computer on the network with the same name as the computer used to send the email message.

f) A computer he registered on the network by Mr. Calixte made frequent accesses to www.adam4adam.com in the two days leading up to the email. This was the only computer in that dorm to access www.adam4adam.com in five days prior to the email.

g) The machine Mr. Calixte registered on the network, and the machine used to send the email message both run the Ubuntu Linux operating system. This is an uncommon operating system on the BC network. In the five days prior to the incident only two users in Gabelli hall had computers running Ubuntu Linux.

g. I know from my training and experience as both a cyber crime investigator and as a lay person acquainted with online chatting, emailing, shopping, and other miscellaneous online activity, people who use computers and regularly go online to various websites, often must enter information known as "user names," or log-in screen names, as well as passwords, in order to access certain things on their computers and on various online websites. Often, people will use the same user name and password in various locations, simply because it is easier to remember one password that will work for so many purposes/places. I also know that people will store their passwords electronically on their computers, on printouts, in

telephone/address books, on sticky notes, in filing cabinets, and in handwritten notes.

h. Your affiant believes and has probable cause to believe that the evidence that I seek permission to search for (consisting of the above-referenced computer system, computer data files, and other specified property, which all are directly associated with the above-stated facts and which all constitute evidence of the crime of "Obtaining computer services by Fraud or Misrepresentation" under Massachusetts General Law, Chapter 266, Section 120F and "Unauthorized access to a computer System" under Massachusetts General Law, Chapter 266, Section 120F.) are believed to be located in the premises and in the computer(s) at the premises.

(5) Affiant's Experience, Education, Training & Study

a. I am a Police Detective for the Boston College Police Department ("BCPD"), assigned as a criminal investigator. I have been a Police Officer with the Boston College Police Department for approximately sixteen years. Prior to my employment with "BCPD" I was employed for approximately five years as a Federal Law Enforcement Ranger with the United States Department of the Interior assigned to their Law Enforcement Division at Boston National Historic Park in Boston Massachusetts.

b. I graduated from a full time Municipal Massachusetts Criminal Justice Training Council Police Academy in Canton, Ma. as well as a Seasonal Federal Law Enforcement Academy in Franklin, NC.

c. I have attended numerous other classes and training seminars sponsored by the Massachusetts Criminal Justice Training Council, various police departments, private agencies and the Middlesex County District Attorneys Office. Over the course of my career I have been involved in the investigation and prosecution of numerous serious crimes including; Narcotic Investigations, Computer crimes, Identity Theft, Identity Fraud, Attempted Murder and other crimes against people and property. I have

been an Affiant on previous Search Warrants and have executed approximately ten search warrants during my career.

(6) Reasonable Inferences Based Upon Investigative Experience:

I spoke to Sergeant Matthew G. Murphy of the Massachusetts State Police. Sergeant Murphy told me that:

a. In July 2007, Sergeant Murphy was assigned to the Middlesex District Attorney's Office and currently holds that assignment. In July 1997, Sergeant Murphy was assigned as an investigator in what was then called the High Tech and Computer Crimes Division of the Attorney General's Office, Sergeant Murphy has testified in both Superior and District Courts throughout the Commonwealth. In the course of Sergeant Murphy official duties as a police officer, he has interviewed many defendants, suspects and witnesses. Furthermore, Sergeant Murphy has made in excess of one hundred (100) arrests for a variety of criminal offenses.

b. Sergeant Murphy attended and graduated from the Massachusetts State Police Academy, where he received extensive training in criminal investigation. In addition to his public service experience, Sergeant Murphy also has additional knowledge in the area of corporate information security. Since 1997, Sergeant Murphy has been a member of the HTCIA (High Technology Crime Investigation Association), an international association whose membership includes corporate security specialists and federal and local law enforcement officers concentrating in the area of high technology crime. The HTCIA also provides training on various issues and areas related to high technology crimes, which Sergeant Murphy has attended.

Sergeant Murphy has been to a number of training seminars and conferences, the focus of which has been high technology related crimes and include the following:

ii. November 1997 Training conference on the subject of *Internet Child Pornography* sponsored by the National Association of Attorney General's Criminal Law Committee held in New York,

NY.

iii. April 1998 Training conference on the subject of *Computer Crime Scene Search & Seizure, Search Warrants & Legal Issues* sponsored by the HTCIA.

iv. February 1998 Training seminar on the subject of *Wireless Fraud* sponsored by the Cellular Telecommunications Industry Association.

v. March 1998 Training conference on the subject of *Investigative Sources of Information* presented by National White Collar Crime Center and LEXIS-NEXIS.

vi. September 1998 "CyberCop 101": Training course on the subject of *Computer Search & Seizure* sponsored by the National White Collar Crime Center and held at the FBI Academy in Quantico, VA.

vii. April 1999 Training seminar on the subject of *Legal and Technical Issues involved with Intellectual Property and E-Commerce* sponsored by the New Hampshire Business Committee for the Arts.

viii. August 1999 "Forensic Computer Science": Training course on the subject of C*omputer Forensics* given by New Technologies, Inc. and held at its facility in Gresham, OR.

ix. December 1999 Training seminar on the subject of basic computer investigations given by the National Infrastructure Protection Center held at the FBI AcadeSergeant Murphy in Quantico, VA.

x. May 2000 "IACIS" training course where Sergeant Murphy became a Certified Electronic Evidence Collection Specialist by the International Association of Computer Investigative Specialists.

xi. February 2001 "EnCase" training course where Sergeant Murphy completed 32 hours of *Intermediate Training in Computer*



KM

*Forensics.*

xii. June 2001 "Networks and Networking for Agents" and "System Security and Exploitation" courses instructed by Sytex, Inc.

xiii. February 2003 "Advanced Data Recovery and Analysis" sponsored by the National White Collar Crime Center.

xiv. June 2003 "Advanced EnCase" training course where Sergeant Murphy completed 32 hours of *Advanced Training in Computer Forensics.*

xv. June 2004- "EnCase" training course where Sergeant Murphy completed 32 hours of Expert Series of Professional Development and Training, *Internet and E-mail Examinations.*

xvi. April 2005 obtained the EnCase Certified Examiner (EnCE) Certification. The EnCE certifies both public and private sector professionals in the use of Guidance Software's EnCase computer forensic software. EnCE certification acknowledges that professionals has mastered computer investigation methodology as well as the use of EnCase during complex computer examinations.

xvii. December 2005- "*Advanced Responders – Search and Seizure of SOHO Networks*" training course sponsored by SEARCH (the National Consortium for Justice Information and Statistics) where Sergeant Murphy completed 24 hours of search and seizure of small office and home office wireless systems.

xviii. December 2006 – "Child Sexual Exploitation Investigations" training course sponsored by the Department of Justice Office of the Juvenile Justice and Delinquency Prevention and Fox Valley Technical College where Sergeant Murphy completed 36 hours of training in Child Sexual Exploitation Investigations.

xix. October 2007 - "EnCase" training course where Sergeant Murphy completed 32 hours of Expert Series of Professional Development and Training, *Advanced Internet Examinations.*

xx. Also, several training seminars and conferences on the subject of *Child Exploitation and Child Pornography Over the Internet* sponsored by the FBI and the Massachusetts State Police.

xxi. Also, several trainings on the subject of *Internet Crimes Against Children* sponsored by the Massachusetts State Police Internet Crimes Against Children Task Force, specifically Captain Thomas Kerle and Sergeant Steven DelNegro.

c. Sergeant Murphy has been a computer crime instructor for the Massachusetts Criminal Justice Training Council and the Cyber Protection Program of the Middlesex County District Attorney's Office, which provides training for law enforcement officers throughout the Commonwealth. Moreover, Sergeant Murphy has participated in dozens of criminal investigations related to high technology crimes conducted by the Massachusetts Office of the Attorney General, the United States Customs Service, the Federal Bureau of Investigation, District Attorney Offices throughout the Commonwealth, and various local police departments; these investigations include over a hundred investigations of dissemination of child pornography over the Internet. He has assisted in the service of multiple search warrants relative to the search and seizure of high technology devices.

Sergeant Murphy also told me that:

d. *The Ability to "Undelete" Files.* When most computers store data, the operating software tells the CPU to assign the data a "file" name (usually a pre-existing file name if it exists, or a name selected (inputted via keyboard) by the user) and sends the data to a storage medium, typically either the "hard drive" of the computer, the floppy drive, or some other peripheral storage device such as a zip drive, tape drive, or writable compact disk (WCD). In order to manage the inventory of all stored files, many operating systems also maintain a "File Allocation Table" (FAT) which tells the CPU where all data is stored. The names (and actual locations of the data on the hard drive or other storage medium) are

recorded in the FAT each time a "file" is saved, accessed, modified, transferred or otherwise affected. When a file is "deleted" by a user, the computer does not in fact remove its data from the designated storage medium, but, instead, alters the FAT to indicate that the space previously consumed by that "deleted" data is now available to be overwritten with new data if necessary. Typically, space that is consumed by "deleted" data is not overwritten until all other unconsumed space is first written to or consumed (although this factor may be affected by the type of the computer system and the use of certain operating software). This fact is important in law enforcement since it means that so-called "deleted" files or data are, in fact, often still present on the computer's storage medium (i.e. floppy disk, hard drive, tape drive, etc.) and can be (and have been) recovered months, years, and even decades after their deletion if the integrity of the computer system is maintained. In my experience, it is not at all uncommon to be able to "undelete" deleted files or data years after their deletion date. As the capacity of computers to store data rises each year, the likelihood that previously "deleted" data has not yet been overwritten and is still recoverable also rises concurrently. The result is that evidence of a crime, stored in a computer system, may be recovered even after the passage of significant periods of time and, in some instances, even after a deliberate attempt to destroy it.

e. *The Automated Creation of "Associated" Files.* In the vast majority of computer systems, each time a file is received, transferred, modified, altered, or otherwise affected, the computer will make some form of a notation or record of that event either in a "log" of activity or by creating or modifying (at or about the same moment in time) a file "associated" with the computer data file which witnessed the activity. For example, when files are received in most IBM-compatible systems using Microsoft Explorer as a software application to navigate the Internet, the file is loaded into a "Temporary Internet" directory and/or "cache" files, and the Internet address of the source of the file is logged or recorded into the



KW

"navigation" directories and files of Microsoft Explorer. At the same time, if a computer system contacts an Internet website, the website itself will transmit a "cookie" which is a short computer code which (using Microsoft Explorer as an example) is logged or recorded in the "Cookies" directory of the Internet browsing software. A "cookie" is a computer code logged into a receiving computer for future reference the next time that computer system contacts the website. The use of cookies enables the website administrators/owners to know if that computer system has previously visited the website before. Generally speaking, these cookie and cache files are computer data files which are "associated" with the computer data file containing the image or data being downloaded (that is transmitted) from the Internet to a computer accessing a website on the Internet. Just as a card index system may be created to catalog a limitless number of features relative to the contents of a filing cabinet, so too may "associated" computer data files be created for a wide variety of software applications relative to other computer data files (and not just merely Internet communication and browsing). This recording and logging feature is not limited to IBM-compatible computers, but applies to various computer systems and computer programs although the name for the storage locations (e.g. "cache" or "cookie" file) may change depending on the computer system and the computer software. Through a careful and thorough analysis of files, which are in any way "associated" with a file of evidentiary significance, it is possible to:

i. Identify where a computer system has "gone" or "visited" on the Internet;
ii. Where certain evidentiary computer data files were taken from the Internet;
iii. Who was at the keyboard at or around the time that certain computer data files of evidentiary significance were created, modified, printed or deleted (e.g. the downloading of images from a child pornography

Internet site might be immediately followed by a visit to the website of an employer); and

iv. When the computer activity occurred.

g. *Computer data storage size.* Today, computers are capable of storing vast quantities of data. Using printed text as an example, most commercially available computers today could easily store on their hard drives thousands and thousands of pages of text. If a computer uses additional storage media (e.g. floppy disks, tape drive tapes, zip drives, writable CDS, magneto optical drives, optical drives, etc.), the capacity for storage becomes limitless.

h. *Encryption, Booby-traps, Hiding or Disguising Files.* Today, computers are also capable of disguising or hiding data to hinder or to prohibit its detection. Computers are capable of encrypting data so as to make it un-retrievable by the average computer user. The Hi-Tech & Computer Crimes Division is in possession of computer software which is available to law enforcement and which will assist in breaking some forms of encryption, but the use of such software can be time consuming, depending upon the amount of data stored and the complexity of the encryptions. Attempting to decrypt data is an extremely time and equipment intensive process, requiring a laboratory environment to be done effectively. Some users will purposefully rename files with otherwise innocuous file names to deter curiosity seekers and others. Similarly, computer users may also "booby-trap" their computers or password protect their computer systems in an attempt to hide their activities and prevent the collection of evidence against them.

i. *Data Files Are Easily Transferred* Transferring data files between computers or onto storage devices such as disks is a simple task that takes little time. As such, once a file is on one computer at a given location – particularly a home -- I believe that there is probable cause to believe that it could be moved to any storage device or other computer at that same location.

j. *Request for Off-Premise Searching.* For the foregoing reasons, I request to search for the above identified Computer System and to transfer it to a secured law enforcement location where its contents may be forensically examined in a manner best suited for the retrieval and preservation of all evidence.

k. *Request to Allow Civilian Computer Expert to Execute Search of Computer System under Supervision by a Sworn Law Enforcement Officer.* I wish to employ the assistance of a civilian investigator working in the Cyber Enforcement Unit (i.e., the computer forensics laboratory) of the Cyber Protection Program located at the Middlesex District Attorney's Office. A computer search requires the assistance of a qualified computer forensic specialist to execute the search of the computer system and to draw off the knowledge of these individuals during the search of the computer system. Sergeant Murphy is a detective in the CEU where he supervises Melissa Marino, a civilian investigator who, like Sergeant Murphy, has specialized training and experience in the field of digital data recovery and analysis. Their special expertise in searching computerized data/components will aid us in properly and adequately obtaining and examining the sought after information. I therefore request authorization for Digital Evidence Investigator Melissa Marino to participate in the entire search that is the subject of this warrant application.

l. I am aware that the forensic analysis of a computer may extend beyond the customary seven-day return period, and will require the assistance of a qualified forensic computer analyst. Therefore, I request permission for a forensic computer analyst to assist in the examination of the laptop. An initial return of service will be filed within seven days, and complete results of the forensic analysis of the computer will be provided to defense counsel during the pretrial discovery process.