October 4, 2011

William E. Sharp
ACLU of Kentucky
315 Guthrie Street
Suite 300
Louisville, Kentucky 40202-3820

Re: Open Records Request

Dear Mr. Sharp:

This is in response to your open records request. You requested copies of any and all books, papers, documents, memoranda, or other materials pertaining to the Cell Phone Investigations Kiosk (“CPIK”). This request includes, but is not limited to the following:

1. Handouts, manuals, PowerPoint presentations, or other training materials for use in the “Digital Evidence for Investigators” program identified in the Curriculum Development Form prepared by Major Kevin Greenwood, Training Commander.

Please find enclosed 52 pages responsive to this request.

2. Correspondence, whether written or electronic, sent by Detectives Glen Craig and/or Dan Jackman regarding the “Digital Evidence for Investigators” program.

Please find enclosed 11 pages responsive to this request.

3. LMPD policies and/or procedures governing the use of CPIK.

Please be advised there are no records responsive to this request. There are no LMPD policies governing the use of Cell Phone Investigations Kiosk.


Please be advised this request is too broad and non-specific to provide a response. There are 1,168 sworn and 345 civilian personnel. If you can provide any specific information, LMPD can process your request.
There are a total of 63 pages responsive to your request. There is a fee due of $6.30 for copies $2.07 for mailing costs for a total fee due the Louisville Metro Police Department in the amount of $8.37. Please reference ORR#11-1001 when you send the fee. If I can be of assistance on this or any other matter, please contact me.

Sincerely,

By: Sharon L. King, Paralegal
Louisville Metro Police Department
Media/Public Information Office
633 West Jefferson Street
Louisville, KY 40202
sharon.king@louisvilleky.gov
Telephone: 502-574-7697
Fax: 502-574-7680

RCW/slk

ORR – 11-1001

cc: Chief Robert C. White
NUMBER ONE
LESSON PLAN

Recognizing and Responding to Digital Evidence

Course Number

February 28, 2011
COURSE NAME: Digital Evidence for Investigators

TITLE: Recognizing and Responding to Digital Evidence

CLASS LEVEL: Officer of Any Rank

OBJECTIVES: At the end of the session, the student will be able to:

- Name the types of investigations which *typically* involve digital evidence
- Recognize and identify different types of digital evidence
- List the steps to address digital evidence in an investigation
- Identify the support units and agencies available to LMPD investigators to assist with digital evidence

METHOD OF INSTRUCTION: Lecture/Facilitation

METHOD OF TESTING: Practical Exercises

TRAINING AIDS: Computer with Projector, DVD Player, Handouts

REFERENCES:

- National Institute of Justice “Guide to Electronic Crime Investigation”
- LMPD SOP 8.36.7

COMPLETED BY: Glenn T. Craig

DATE: February 23, 2011

REVISIONS BY:
INTRODUCTION

Recognizing and Responding to Digital Evidence

This block of instruction is intended to familiarize you with the different (typical) types of digital evidence you may encounter in your investigations.

We’ll be talking about some technical information, but not to worry, you will learn how to approach digital evidence without the need to memorize or understand all of the technical aspects.

I want to give you a little history regarding computer forensics within the Louisville Metro Police Department. As a preface, I was formerly a Louisville Police Department (the old “City”) detective prior to merger. As a result, you may hear me refer to “we”, or “us” in regards to the groundwork that was laid to facilitate an in-house squad devoted to computer forensics. This certainly isn’t intended to slight the Jefferson County Police, as they were making some progress of their own regarding electronic evidence around the same time as LPD.

In the late 1990s, a good friend of mine, Detective Mike Turley (Ret.), was assigned to the White Collar Crime Squad. Mike was an excellent investigator of high-dollar financial crimes. In those types of cases, the investigator literally followed the “paper trail”, by scouring the financial records of the victim (typically a financial institution) to ascertain where the money went missing, how much was stolen, and who was responsible. Typically, this involved a large amount
LEC
(Cont): of paper documents and it was common to be faced with going through banker boxes or file cabinets full of records.

In an event that would eventually be a catalyst to develop a squad capable of in-house computer forensics, Mike was assigned an embezzlement case involving a local financial institution. When he met with the security personnel and requested the financial records (as usual, he was expecting many paper documents), he was led to a room with a computer set up as a server. The security person nodded to the server and said, “There they are”.

Mike would later say that he was a little embarrassed to admit to the bank security person that the Louisville Police was not equipped to handle electronic evidence.

As a result, Mike spearheaded an effort to convince the administration of LPD to take a hard look at forming a squad to process electronic evidence in support of criminal investigations. During the interim, Detective Kevin Lamkin (also of the White Collar Crime Squad) began processing electronic evidence with limited resources available at the time.

After about a year of writing policy and securing funding, the Computer Forensics and Analysis Squad went online in January, 2001. The rest, as they say, is history.

Time: 4 Minutes
PRESENTATION

PP2: Course Objectives: The student will be able to:

1. Name the types of investigations which typically involve digital evidence
2. Recognize and identify different types of digital evidence
3. List the steps to address digital evidence in an investigation
4. Identify the support units and agencies available to LMPD investigators to assist with digital evidence

PP3: This course will NOT:

Attempt to turn you into a Forensic Computer Examiner

But rather instruct you how to properly obtain electronic evidence to maintain integrity for court proceedings.

PP4: Law Enforcement and Digital Evidence

QTC: How often will an investigation involve digital evidence?

AR: 79% of Americans have either or desktop or laptop computer at home
74% of adults have Internet access at home
65% of adults use a high-speed Internet service at home (1)

Any investigation could potentially involve electronic evidence.

PP5: Law Enforcement and Digital Evidence (Cont)
LEC: This article caught my eye in the paper a few years ago. The story was written as basically a slam to Kentucky, as if to say our state is backwards because 32% of Kentucky homes still don’t have computers. (This number is probably even lower now.)

I looked at that number another way: if 32% of Kentucky homes don’t have a computer, then roughly two-thirds of all Kentucky homes DO have at least one computer!

Consider all the runs law enforcement agencies make to households all over the state in a year; about 66% of those homes have a computer, and thus perhaps vital electronic evidence relating to the crime being investigated.

PP6: Law Enforcement and Digital Evidence (Cont)

LEC: Louisville Metro Government currently has in use approximately 5000 client computers, and 300 servers. Even Metro employees not working in technical positions still use this technology for timekeeping, email communications and other intranet usage, and are creating potential electronic evidence when the computers are used for illegal purposes, or used in a way which violates Metro computer usage policies.

QTC/ PP7: What is Computer Forensics?

AR: 1. Obtaining electronic evidence from computers
2. Obtaining electronic evidence from cell phones
3. Obtaining evidence from providers, such as cell phone companies or internet providers.
LEC: “Forensics” in the context of “Computer Forensics” simply refers to the process of creating an exact copy of the original media in such a way that the original remains unchanged, and the copy is verifiable as an exact duplicate of the original.

Sometimes, mistakenly, referred to as a “Mirror Image”

The computer examiner will never simply “dig around” on the original suspect computer by turning it on and searching, as that is actually changing data (evidence) on the original evidence.

Instead, the “forensic image” is searched for the pertinent evidence, leaving the original evidence intact.

This forensic image must be verifiable as an “exact duplicate” of the original for court purposes. That means every single “1”, and every single “0” must be accounted for, and appear in the same order and places as on the original.

PP8: Hardware “Write-Blocking” device prevents data from being written to the source media. Essentially a one-way valve, in that data flows from the original media to the forensic image, but data is NEVER written or changed on the original.
Typical CFAS Case Workflow

Ideally, CFAS will be contacted by the investigator at that time he or she recognizes the case they’re working may involve digital evidence.

Typically, the initial assistance from CFAS will come on the form of simple advice, or assisting in drafting the search warrant to ensure the proper language is included which authorizes the “forensic examination” of seized items.

When the time comes to serve the search warrant at the target location, a CFAS detective will assist in securing and transporting the evidence to the Property Room, if requested.

In most residential or small business scenarios, it will likely be possible for the personnel on scene to complete the takedown of the computer(s), and transporting to the Property Room. Guidance can often be given via telephone from CFAS to the on-site investigator on proper procedures.

CFAS will check out evidence from the Property Room for forensic analysis, and return evidence when processing is complete.

Finally, if necessary, the CFAS detective will testify in court proceedings to how the electronic evidence was obtained, and examined.

TIME: 20 Minutes
Some "typical" types of investigations where electronic evidence can be expected:

- Child pornography – possession and trafficking
- Fraud related offenses, especially e-commerce and Identity Theft
- Electronic surveillance – video and/or audio (e.g. bank video of robbery)
- Internet Social Networking sites as a vehicle for harassment or other criminal offenses

It is crucial that the investigator recognize that electronic evidence *may* exist in ANY investigation! Don’t assume that there won’t be a potential for valuable electronic evidence when conducting a "non computer crime" investigation.

AFQ

TIME: 25 Minutes
What is Digital Evidence?

Computers
Cell phones
GPS devices
Records from cell companies or internet providers

According to the National Institute of Justice “Guide to Electronic Crime Investigation”:

Digital evidence is information and data of value to an investigation that is stored on, received, or transmitted by an electronic device.

First responders should remember that items capable of containing digital evidence may also harbor physical evidence such as DNA, fingerprints, or other trace evidence. Physical evidence should be preserved for appropriate examination.

Volatile vs. Non-Volatile Electronic Evidence

Volatile Electronic Evidence: Data which is lost when power is removed from the device (or power is shut down).

RAM (Random Access Memory), data stored in RAM is lost upon shutdown of a computer, such as information displayed on the screen that hasn’t been saved to a file, or sent to a temporary cache.
LEC
(Cont): There are methods to capture and retain volatile data during the evidence collection, but prior intelligence is necessary to facilitate this type of collection.

The type of investigation may dictate the necessity of obtaining volatile evidence. “How many rocks does it take to make a pile?”

You may be able to accomplish same thing with a photograph of the computer screen contents prior to shutdown such as child porn on suspect’s screen at time of search warrant entry.

PP14: Volatile vs. Non-Volatile Electronic Evidence (Cont)

LEC: Non-Volatile Electronic Evidence: Data which is not lost when power is removed from device or power is turned off.

This includes data which has been written to the hard disk, or other non-volatile media, such as flash media or CD/DVD disc.

If a computer/device is powered on at time of seizure, it’s still a good idea to take a photo of the screen display.

AFQ

TIME: 35 Minutes
I Anticipate Electronic Evidence in My Investigation, Now What?

Gather as much intelligence as possible regarding the type of digital evidence you believe you may encounter.

If target is a business setting, is there a cooperative System Administrator available? A business system may need to be forensically imaged or previewed onsite, leaving the system operational during and after the acquisition.

Contact a CFAS Detective for assistance in drafting the Search Warrant, if necessary.

Proper language in original warrant will authorize examination to take place on seized electronic items: “...submit seized items to electronic forensic examination” in Personal Property to Wit section.
I Anticipate Electronic Evidence in My Investigation, Now What? (Cont)

Designate personnel responsible for securing electronic evidence during warrant service.

Allow ONLY designated personnel to handle electronic evidence. (Police-proof scene!)

Be sure to plan ahead BEFORE executing search warrant to ensure everyone knows his/her responsibilities.

Transport evidence to Property Room.

Handle with Care!

Prepare and submit Service Request to appropriate unit.

AFQ

TIME: 45 Minutes
(BREAK)
Serving the Search Warrant

Officer Safety:
Notice the emphasis on the slide on “Officer Safety”.

It is imperative to prevent complacency when serving these types of warrants. Never assume that the target is just a “passive computer geek”!

Computer-literate criminals may possess other technical skills, such as explosives or weapons proficiency.

Serving the Search Warrant (Cont)

Make SAFE but QUICK entry!

Use pre-designated officer(s) responsible for securing computer(s). This is also to protect the evidence from untrained officers that may try to help by searching the computer because “they’re good with computers”.

Allow NO ONE to access computers, except CFAS detectives or specially trained officer(s). Obviously, don’t accept any offer of “help” from the suspect(s) to “get into” the computer. If the suspect is being cooperative, by all means ask them for any passwords for the computer, and write those down.

Log and prepare seized items for transport at the direction of the CFAS detectives or designee. Enter the information from electronic devices on the search warrant log just as in any other search warrant scene. Be sure to include model numbers and names, and serial numbers.
Video – Seizing Electronic Evidence

Note on video: The video recommends “pulling the plug” on stand-alone computers that are on. DISREGARD THIS!

The accepted practice in this situation is to simply perform a “graceful shutdown” of the computer, documenting the time/date the shutdown is initiated and completed.

Should the computer take an unusually long time to complete this process, pulling the plug is a last resort.

“How to Seize, Package, Transport, and Store Computer Evidence”

The video is approximately 18 minutes in length, and discusses the proper methods of seizing and transporting electronic evidence.

Once again, a special note regarding computers that are powered on at the time of a search warrant: the video recommends “pulling the plug” from the back of the computer in this circumstance. DISREGARD THIS!

TIME: 90 Minutes
PP20: Transporting and Storing Digital Evidence

LEC: Transport computer (the box itself) in rear floorboard, with front seat pushed back to secure. Do NOT place computer equipment or media in trunk!

Secure any loose media and manuals in boxes for transport.

Log all items into LMPD Property Room, and CFAS detectives will check out the equipment for forensic examination.

If the RCFL is to conduct the computer examination, all items must STILL be logged through the LMPD Property Room.

OBJ #4/PP21: Who Can Assist with Digital Evidence?

LEC: There are several resources available within LMPD to assist you with digital evidence.

As noted previously, the Computer Forensics and Analysis Squad is available to assist in drafting electronic evidence search warrants, serving those warrants, and processing the electronic evidence.

The Video Forensic Analysis Squad also deals with digital surveillance video on a daily basis. This squad will assist in retrieving both analog and digital video evidence, as well as processing video for use in ATL bulletins and court presentation.
Remember that any devices capable of containing digital evidence may also yield other types of crucial evidence, such as DNA or latent prints.

**PP22:** Who Can Assist with Digital Evidence? (Cont)

**LEC:** The Kentucky Regional Computer Forensics Laboratory (RCFL) is located at the University of Louisville Shelby Campus. Det. Kevin Lamkin is assigned full-time at the RCFL, and Det. Chris Bowman divides his time equally between the Video squad office at LMPD HQ, and the RCFL facility.

**RCFL Services:**

Any law enforcement agency with jurisdiction in Kentucky may request assistance (at no cost to them) with the following activities:

**Pre-Seizure Consultation**

**On-Site Seizure and Collection** – Must have a minimum of 48 hours advance notice. This service would be used in those instances where it’s necessary to image the suspect computer(s) onsite, such as a business network.

**Duplication, Storage and Preservation of Electronic Equipment and other Digital Evidence**

**Prompt, Accurate, and Impartial Examinations of Digitally Stored Evidence**

**Courtroom Testimony**

**TIME: 100 Minutes**
Who Conducts the Exam?

Generally, all forensic computer examinations will take place at the Regional Computer Forensics Laboratory (RCFL).

The RCFL is equipped with multiple forensic examiners and equipment, and will provide the most expedited service for processing of digital evidence.

The Service Request form for submitting items to the RCFL for examination is available at: http://www.krcfl.org.

Who Conducts the Exam? (Cont)

LMPD S.O.P. 8.36.7:

Where it is not an emergency situation, the evidence may be taken to the Kentucky Regional Computer Forensics Lab (KRCFL) only after it has been entered into the Property Room as evidence. The KRCFL is a full service forensics laboratory and training center devoted entirely to the examination of digital evidence in support of criminal investigations. They will support investigations into the following crimes:
Terrorism
Child Pornography
Homicide
Violent Crime
Internet Crime
Theft or Destruction of Intellectual Property
Fraud
Cell phone exams (self-serve “kiosk”)

**PP25:** Homework

**LEC:** Don’t worry! This assignment isn’t graded, and you don’t have to turn anything in. This is simply a good resource to use for reference:

[www.justice.gov/criminal/cybercrime/ssmanual/](http://www.justice.gov/criminal/cybercrime/ssmanual/)

Department of Justice manual on Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations

**TIME:** 110 Minutes
PP26: Contact Information

LEC: Det. Glenn Craig:
Cell: 502-379-0272
Office: 502-574-7747

Det. Kevin Lamkin
Cell: 502-817-0843
Office (RCFL): 502-852-4461

Det. Chris Bowman
Cell: 502-439-3842
FINAL REVIEW

QTC: Name some “typical” investigations you’d expect to involve digital evidence.

AR: Child Pornography
Fraud Investigations
Investigations involving online Social networking sites
Video surveillance stored digitally

ANY investigation potentially involves some type of digital evidence!

QTC: Name some different types of digital evidence, or items which may contain digital evidence.

AR: Cell phones
Computers
PDA (personal data assistants)
Online records (such as IP logs, or electronic communications)
Volatile data
Non-volatile data
QTC: List the general steps in addressing digital evidence

AR: Gather intelligence

Contact CFAS for assistance with warrant, if necessary

Pre-plan for serving search warrant; designate personnel to secure electronic evidence

Transport to Property Room

Submit Service Request form

QTC: What support units are available within LMPD to assist with digital evidence?

AR: Computer Forensics and Analysis Squad
Video Forensic Analysis Squad

QTC: Name an outside resource available to assist with digital evidence.

AR: Regional Computer Forensics Lab (RCFL)

AFQ

TIME: 115 Minutes
CONCLUDING STATEMENT

We’ve covered quite of bit of information in this block, including some technical information.

You probably won’t remember all of it, and that’s OK.

Just remember to contact one of the support squads as soon as you recognize your investigation may involve digital evidence so that they may assist you in the proper handling of that evidence.

TIME: 120 Minutes
TRAINING AIDS

Computer and projector

Video: “How to Seize, Package, Transport and Store Computer Evidence”

DVD Player

Handouts of PowerPoint outline