Transporting & Storing Digital Evidence

- 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.
  - CFAS detectives will check out the equipment for forensic examination
  - If the RCFL is going to conduct the computer examination, all items must STILL be logged through the LMPD Property Room.
Who Can Assist with Digital Evidence?

- Within LMPD:
  - Computer Forensics and Analysis Squad
  - Video Forensic Analysis Squad
  - Crime Scene Unit: Collects evidence at crime scenes, including digital devices.
    - Collected digital devices may also need to be processed for other types of evidence, such as DNA, or latent prints.
Who Can Assist with Digital Evidence?

- KY Regional Computer Forensics Laboratory
  - http://www.krcfl.org/
- 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 - Minimum 48 hours advance notice
    - Duplication, Storage and Preservation of Electronic Equipment and other Digital Evidence
    - Prompt, Accurate, and Impartial Examinations of Digitally Stored Evidence
    - Courtroom Testimony
Who Conducts the Exam?

- Generally, all forensic computer examinations will take place at the Regional Computer Forensics Laboratory (RCFL).
  - [http://www.krcfl.org/](http://www.krcfl.org/)
    - Download Service Request form
Who Conducts the Exam?

- 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”)
Homework

- Don't worry... this isn't graded, and you don't need to turn anything in, it's just a good resource for you:
  - [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
Contact Information

- 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
Questions?
NUMBER TWO
Hey,

Congrats on the promo!

Can't think of a more deserving person!

I'd say Kevin Lamkin is the best choice, especially since he just got re-certified.

I go back Oct. 14 to sign, but will have already started V-ing out around Oct. 10!!

Woo Hoo!

GT

Detective G.T. Craig
Louisville Metro Police Dept.
633 W Jefferson St.
Louisville, KY 40202
502-574-7747 - Office
502-379-0272 - Cell

Sent from my Nextel BlackBerry

---

From: Chambers, Donnie R
Sent: Wednesday, August 24, 2011 02:29 PM
To: Craig, Glenn
Subject: Your Replacement for DEI

Hey Short Timer, who do you suggest we develop to teach your topics?
**KENTUCKY LAW ENFORCEMENT COUNCIL**

**FUNDERBURK BUILDING, 521 LANCASTER AVENUE**  
**RICHMOND, KENTUCKY 40475-3102**  
**(859) 622-6218**  
**FAX No. (859) 622-5943**  
**DOCJT.KLEC@ky.gov**

**CURRICULUM DEVELOPMENT FORM**

**Digital Evidence for Investigators**  
**CURRICULUM TITLE**

<table>
<thead>
<tr>
<th>COURSE NUMBER</th>
<th>COURSE HOURS</th>
</tr>
</thead>
<tbody>
<tr>
<td>32</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DETECTIVES GLENN CRAIG AND DAN JACKMAN</th>
<th>LMPD</th>
</tr>
</thead>
<tbody>
<tr>
<td>COMPLETED BY (NAME)</td>
<td>AFFILIATION/ORGANIZATION</td>
</tr>
</tbody>
</table>

**Status of Course:**  
**RECERTIFICATION WITH CHANGES**

<table>
<thead>
<tr>
<th>Approval Date:</th>
<th>Effective Date:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Name the KLEC approved training school presenting the training course:

**Louisville Metro Police Training Academy**  
**Name of School**

**2911 Taylor Boulevard**  
**Louisville, KY 40208**  
**Address of School**

Signature of Chief Administrator of KLEC certified training school submitting curriculum for approval.

**Major Kevin Greenwood, Training Commander**  
**Printed Name, Title**
CURRICULUM DEVELOPMENT FORM

Class Level: Basic

Method of Testing: Written Examination

Course Description: This course is an awareness level training on digital evidence recognition, preservation and documentation for use in criminal investigations. Contemporary issues in digital data storage and transmission will be considered in light of their impact on criminal investigations.

Prerequisites: None

Risk Level: Low
Fitness Level: Low

INDICATE HOW THE NEED FOR THIS CURRICULUM WAS IDENTIFIED

<table>
<thead>
<tr>
<th>Job Task Analysis</th>
<th>Training Needs Assessment</th>
<th>Course Critiques</th>
<th>Legal Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Other (Explain)

Attach Schedule, Objectives and Bibliography

For KLEC Purposes Only

<table>
<thead>
<tr>
<th>Skills</th>
<th>Human</th>
<th>Conceptual</th>
</tr>
</thead>
</table>
# Digital Evidence for Investigators

<table>
<thead>
<tr>
<th>Time</th>
<th>Monday</th>
<th>Tuesday</th>
<th>Wednesday</th>
<th>Thursday</th>
<th>Friday</th>
</tr>
</thead>
<tbody>
<tr>
<td>8:00</td>
<td>Internet Information</td>
<td>Social Networking</td>
<td>Information Gathering</td>
<td>Practical Exercises/Examination</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2 hours</td>
<td>3 hours</td>
<td>3 hours</td>
<td>7.5 hours</td>
<td></td>
</tr>
<tr>
<td>9:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10:00</td>
<td>Recognizing Digital Evidence</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11:00</td>
<td>2 hours</td>
<td>Documenting Crime Scenes</td>
<td>Cell Phone Examinations</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 hour</td>
<td>1 hour</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12:00</td>
<td>LUNCH</td>
<td>LUNCH</td>
<td>LUNCH</td>
<td>LUNCH</td>
<td>LUNCH</td>
</tr>
<tr>
<td>1:00</td>
<td>Physical Evidence Preservation</td>
<td>Electronic Evidence</td>
<td>Enhancing Criminal Investigations</td>
<td>Practical Exercises</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1 hour</td>
<td>4 hours</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2:00</td>
<td>Virtual Evidence Preservation</td>
<td>Practicals</td>
<td>4 hours</td>
<td></td>
<td>(Con't)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4 hours</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
1.0 **Internet Information**

During this course of instruction the learner will be able to:

1.1 Given reference materials, list the stages of evolution of the internet.
1.2 Identify the key components of a computer.
1.3 Given an example of an IP address, identify the owner of the IP address.
1.4 Given an example of a domain name, identify the country of origin of the domain name.
1.5 Given reference materials, define the term browser.
1.6 Given reference materials, define the term hacker.
1.7 Given reference materials, define the phrase "google it".
1.8 Given reference materials, define the term virus.
1.9 Given reference materials, define the term SPAM.
1.10 Given reference materials, define the term encryption.
1.11 List obstacles faced by investigators during internet investigations.

Bibliography: #1, #2, #3

2.0 **Recognizing Digital Evidence**

During this course of instruction the learner will be able to:

2.1 Name the types of investigations which typically involve digital evidence.
2.2 Recognize and identify different types of digital evidence.
2.3 List the initial steps to address digital evidence in an investigation.
2.4 Identify the support units and agencies available to LMPD investigators to assist with digital evidence.

Bibliography: #4, #5, #6

3.0 **Physical Evidence Preservation**

During this course of instruction the learner will be able to:

3.1 Identify issues related to preserving physical network evidence.
3.2 Identify issues related to preserving volatile evidence.
3.3 Evaluate the importance of properly documenting digital evidence prior to a search.
3.4 Evaluate the importance of documenting digital evidence after a search.
3.5 Given a piece of electronic evidence, identify the proper method for transporting the evidence to a secure facility.

Bibliography: #4, #5, #6

4.0 Virtual Evidence Preservation

During this course of instruction the learner will be able to:

4.1 Demonstrate the proper method for capturing real time electronic evidence from the internet.
4.2 Demonstrate the proper method for preserving real time electronic evidence for presentation in a court.
4.3 Given an example of a computer file listing, evaluate the scope of the search that is legally permitted for the given listing.
4.4 Given reference materials, identify the official custodian of records at a given internet company.
4.5 Given an example of an email or IP address, compose a error free preservation letter, utilizing acceptable terminology and format, to the proper internet company representative of the given internet company.
4.6 Given reference materials, accurately complete a Grand Jury Subpoena Request Form.
4.7 Given an example of an internet account, accurately compose a search warrant completely detailing all items to be seized.

Bibliography: #7, #8

5.0 Social Networking

During this course of instruction the learner will be able to:

5.1 Without reference, create an undercover profile on a social networking website.
5.2 Navigate through various user’s profiles within a social networking site.
5.3 Given an example of an email address, locate the associated social networking profile on the internet.
5.4 Given an example of a social networking profile, generate a map showing the relationship between the given profile and other profiles on the social networking.

6.0 Documenting Crime Scenes
During this course of instruction the learner will be able to:

6.1 Given a mock search situation, properly document the aspects of the computer crime scene.

6.2 Identify issues related to documenting evidence from wireless devices.

6.3 Identify issues related to documenting a computer crimes scene that are necessary for court.

Bibliography: #7, #8, #9, #10, #11

7.0 Electronic Evidence Practical Exercise

During this course of instruction the learner will be able to:

7.1 During a practical exercise, demonstrate the proper identification of electronic evidence.

7.2 During a practical exercise, demonstrate the proper seizure of electronic evidence.

7.3 During a practical exercise, demonstrate the proper documentation of electronic evidence.

7.4 During a practical exercise, demonstrate the proper transportation of electronic evidence.

Bibliography: #4, #5, #6

8.0 Information Gathering

During this course of instruction the learner will be able to:

8.1 Identify and utilize the functions of the Kentucky State Police Fusion Center.

8.2 Identify and utilize the functions of the E-Warrants system of the Kentucky Administrative Office of the Courts.

8.3 Register for the Justice Exchange program.

8.4 Identify and utilize the functions of the Justice Exchange program.

Bibliography: #20, #21, #22, #23, #24
9.0 Cell Phone Examinations (Cell Phone Investigations Kiosk-CPIK)

During this course of instruction the learner will be able to:

9.1 Identify components of the CPIK system.
9.2 Utilize the proper protocol to access the CPIK system.
9.3 Utilize the CPIK system to extract evidence from a given cell phone.
9.4 Utilize the CPIK system to extract evidence from a given palm device.
9.5 Utilize the CPIK system to extract evidence from a given blackberry device.
9.6 Create a final report of evidence extracted from a device using the CPIK system.

10.0 Enhancing Criminal Investigations

During this course of instruction the learner will be able to:

10.1 Compare and contrast the differences between the various versions of the Arbitrator in-car mobile video systems currently in use in patrol vehicles.
10.2 Identify operational issues associated with the Arbitrator in-car mobile video systems.

Bibliography: #13, #14, #15, #16, #17, #18, #19

11.0 Practical Exercises/Examination

During this course of instruction the learner will be able to:

11.1 Evaluate officer safety concerns at crime scenes which may involve digital evidence.
11.2 Evaluate evidentiary safety concerns at crime scenes which may involve digital evidence.
11.3 During a practical exercise at a physical mock crime scene, identify potential sources of digital evidence.
11.4 During a practical exercise involving an online site, identify potential sources of digital evidence.

11.5 During a practical exercise, preserve, label and transport digital evidence in a manner that maintains the admissibility of the evidence in a criminal court proceeding.

Bibliography: #4, #5, #6

12.0 Course Critique

During this course of instruction, the learner will be able to

12.1 Complete a critique of the course for use by instructors to evaluate the effectiveness of the course.
Bibliography:


7. Internet Crimes Against Children—Undercover Investigations, Department of Justice, Columbus, OH, February 2007.

8. SEARCH—Advanced Responders: Search and Seizure of Small Office/Home Office Networks.


