FRAUD DETECTION, INVESTIGATION, & RESOLUTION: FINISHING THE JOB
WHAT CAN A FORENSIC LAB DO FOR YOUR WHITE-COLLAR INVESTIGATION?

All of the “CSI” stuff on TV is not just used to solve violent TV crimes. See how real-world forensics can help you investigate and prove your white-collar or fraud case in both civil and criminal court. This session will provide a foundation for recognizing evidence that should be forensically examined, handling and transporting such evidence, and knowing what testing is available once the evidence is secured.

HUGO A. HOLLAND, JR., J.D., CFE
Assistant District Attorney
First Judicial District
Shreveport, LA

Hugo Holland worked his way through college and law school as a deputy sheriff in Baton Rouge, earning a Bachelor of Criminal Justice in 1985 and a Juris Doctor in 1988 from Louisiana State University.

Upon being admitted to the Louisiana Bar, Mr. Holland was commissioned an Assistant District Attorney in Louisiana’s 35th Judicial District. Two years later he moved to Shreveport where he became an Assistant District Attorney in 1991.

During the course of his prosecutorial career, Mr. Holland has handled more than one hundred jury trials, hundreds of grand jury investigations, and conducted or supervised thousands of felony investigations. He is a special Assistant District Attorney in several jurisdictions in Louisiana, handling high-profile sex, homicide, and public corruption cases around the state, one of which was recently highlighted by CBS News’ 48 Hours.

Mr. Holland currently teaches advanced criminal courses, including advanced investigative techniques, at numerous police academies throughout Louisiana, and regularly instructs prosecutors on various topics in almost a dozen states and at the National College of District Attorneys. He also teaches for the Louisiana Judicial College, the training arm for Louisiana judges, and for the Louisiana’s Legislative Auditor.

Mr. Holland is a past-President of the Assistant District Attorneys section of the Louisiana District Attorneys Association, and has been a member of the Board of Directors of that organization for nearly a decade. On behalf of Louisiana’s District Attorneys he is very active in the legislature, drafting and successfully guiding numerous pieces of legislation through the process, testifying numerous times before various legislative committees.

He is a member of the bars of Louisiana, Texas, numerous federal courts, the Louisiana District Attorneys Association, the National District Attorneys Association, and various local
and regional organizations relating to law enforcement, including the Louisiana Attorney General’s Internet Crimes Against Children Task Force, for which he is the legal advisor.

Among other outside activities, Hugo Holland is a licensed pilot and a Major in the United States Civil Air Patrol. He is also a reserve police officer in Bossier City, Louisiana, where he rides a regular patrol shift on a weekly basis.
I. Forensic laboratories usually have 7 divisions
   a. Trace evidence—hair, fabric, dust, fiber, and skeletal remains
   b. Chemistry—test samples of blood and urine for alcohol, drugs, and poisoning. Chemistry sets are also used in the analysis of synthetic materials such medicines, dyes, and stains. Specialists in the area of chemistry also rely on gas chromatographs, mass spectrometers, and microscopes to identify chemicals.
   c. Serology—specializes in the identification and analysis of bloodstains and other bodily fluids, as well as DNA sequencing. The most common of the DNA tests, the polymerase chain reaction, is now able to be performed in small laboratories, thanks to advancements in this area; however, the analysis of mitochondrial DNA is still only performed in large forensic laboratories.
   d. Materials—identify and analyze metals, paints, ceramics, soil, and wood in an attempt to trace a crime back to a possible suspect. The biology unit is in charge of analyzing all biological evidence, such seeds and plants.
   e. Firearms/tool marks—tests weapons to see which weapon made the mark on an object or wounded or killed a person. To be able to carry out these tests, firearms specialists study the used bullet cartridges and use shooting baths to fire weapons, identify the bullet marks, and establish the firing distance.
   f. Photography—documents crime scene or other evidence. Processing resources and dark room services allow specialists in the area of photography to analyze photographs and bring the evidence to light; also used to document materials and firearms/tool mark testing.
**WHAT CAN A FORENSIC LAB DO FOR YOUR WHITE-COLLAR INVESTIGATION?**

<table>
<thead>
<tr>
<th>NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>g. Others—large labs also have arson and explosives experts as well as specialists in software, computer data, files, documents, audios, and video recordings. The units available in different labs will vary from one to the other; however, the need for certain analyses and the budget of each lab determines the availability of the departments—including computer forensics. <em>Often includes forensic document examination and fingerprint identification.</em></td>
</tr>
</tbody>
</table>

II. Anatomy of a white-collar investigation

a. Document/evidence collection  
b. Observation  
c. Interview  
d. Forensics plays a part in the first step of any white-collar or fraud investigation  

III. Document examination  

a. Identification of handwriting and signatures—handwriting identification is a comparison study requiring authenticated specimens of known handwriting from the individual(s) concerned. These are closely compared to the handwriting characteristics exhibited by the questioned writing in order to determine authorship. *Like must be compared to like: printing to printing and cursive to cursive, with comparable letters, letter combinations, words, and numerals.*  
b. Identification of a document as a forgery—generally broken into several categories  
   i. No attempt made by the forger to imitate the genuine signature of the person purportedly signing the document  
   ii. Attempt to imitate genuine signature by some method of tracing of a model signature  
   iii. Freehand attempt to simulate the genuine signature from a model  
   iv. Purported signer is fictitious
WHAT CAN A FORENSIC LAB DO FOR YOUR WHITE-COLLAR INVESTIGATION?

v. Entire document is fictitious

vi. “Cut and paste” where genuine signature, or copy, is transferred from some authentic source to a fraudulent document

c. Identification of typewriters, check writers, photocopies, and computer printers

d. Detection of alterations, additions, deletions, or substitutions—performed to detect whether a portion of a document has been altered, some portion rendered not readily visible, or some text added. If an obliteration/alteration is identified, then the method is determined and described, and if possible the text of the obliterated entry deciphered. Instruments such as a Video Spectral Comparator (VSC) assist in this study. The VSC allows the examiner to examine the document through infrared illumination using an infrared sensitive CCD camera as a detector. The image is examined by viewing on a monitor, and digital image processing through a computer. This is very useful in ink differentiation.

e. Identification and deciphering of indented writing—an imprint that may be left on the underlying pages when the top sheet of paper is written upon. This impression of the writing is influenced by pen pressure and thickness of the paper. Indented writing is very useful as a form of connecting evidence, such as tying a robbery note to a writing pad recovered from a suspect. Classically, indented writing was identified and deciphered by means of low angle oblique light and photography. More recently, an instrument known as an Electrostatic Detection Apparatus, or ESDA, is used to produce a visual image of the indented writing on transparency film. This procedure is non-destructive and rather undetectable.
WHAT CAN A FORENSIC LAB DO FOR YOUR WHITE-COLLAR INVESTIGATION?

| f. | Comparisons of inks and identification of type of writing instrument |
| g. | Qualifications of a forensic document examiner |
|    | i. Examiner must have a sound basic education through the baccalaureate degree. The typical training period is two years of study and practical experience in an established questioned-documents laboratory where the examiner trainee studies the basic literature, completes study projects, becomes familiar with the role of forensic sciences in general and questioned documents in particular as they relate to the legal system. |
|    | ii. It should be understood that questioned documents is a valid and legitimate field of study as a discipline in forensic examinations and identification. It is not to be confused with “graphologists” or “grapho-analysts” who claim the ability to assess personality traits of a person from their handwriting. Whether the claim is valid or not, the association of these individuals with handwriting has caused some of them to claim sufficient expertise to determine whether or not a signature is genuine. |

IV. DNA analysis

| a. | DNA inherited from our parents |
| b. | Present in all nucleated cells—meaning almost every cell in the body. Commonly found in blood, semen, saliva, mucous, and any other bodily fluid |
| c. | Unique between individuals—except for identical twins |
| d. | Unchanged by age, environment, physical condition, or illness |
| e. | Usually NOT left by dead dermal cells |
**WHAT CAN A FORENSIC LAB DO FOR YOUR WHITE-COLLAR INVESTIGATION?**

- Taking a known DNA sample by buccal swab—there are 3,000,000,000,000 cells in the human body and only about 100 are needed to obtain a DNA profile

- What if the target will not provide a sample?
  - Coffee mugs
  - Drinking cups
  - Soda cans and bottles
  - Cigarette butts

- Where can DNA be found in a white-collar investigation?
  - Computer keyboard and mouse
  - TV remote control
  - Clothing
  - Telephone keypad and handset
  - Stamps and envelopes
  - Documents
  - Generally anything that a person has touched

- Obtaining the “unknown” DNA swab
  - Every kit manufacturer sells sterile swabs
  - If the sample is dry, one drop of distilled water should be used on the swab
  - Art, not science, as to where to obtain the swab

- Storage of materials with suspected DNA

- Chain of custody concerns

**V. Fingerprints**

- No two are alike, even for identical twins
- Left by salts, oils, etc. in the ridges of the skin on fingers, palms, toes, and soles of the feet, and also sometimes the oils from the forehead left on the fingers after touching the face
- **INVERSE** relationship between porosity of surface and the chance prints will be obtained

---

**NOTES**
d. This is NOT CSI—we can’t get a fingerprint off an ice cube

e. Within the last 15 years it has gotten easier to obtain prints from documents due to various fuming methods

f. Latent prints
   i. Inadvertently left behind by a person handling items
   ii. Will degrade over time, especially if exposed to the elements
   iii. In the CJ system, prints found at about 10% of crime scenes, and USABLE prints found in about 30% of the scenes where prints are found—thus only about 1 in 30 crime scenes has usable prints
   iv. Usable v. unusable

VI. Handling and processing documentary evidence
   a. Storage—always store documents in a cool, dry place, in an envelope, NEVER in plastic as DNA is biodegradable if left wet
   b. Handling—use gloves—basic rubber gloves as used in hospitals
   c. Pre-treatment documentation
      i. Photocopy document
      ii. Photograph document
      iii. Scan in TIFF or RAW format 600 dpi minimum—crop to actual size to reduce file size
      iv. Save the image in at least two locations—one of which should be a CD or DVD with all the case documents
   d. Document processing
      i. Iodine fuming—if documents intercepted in transit, this is the best fuming method as it leaves little trace after a short period of time
      ii. Ninhydrin fuming
**WHAT CAN A FORENSIC LAB DO FOR YOUR WHITE-COLLAR INVESTIGATION?**

1. Superglue, lightbulb, small dish, metal clip, enclosure
2. Does NOT cause ink runs, even if using submersion method
   iii. If prints are located, it usually requires special photographic equipment, at least specialty lenses, to properly document the prints
   1. Macro-photography—refers to a finished photograph of a subject at greater than life size
   2. Special lenses required

e. Forensic document examiners comparing handwriting should only handle evidence AFTER processing for prints and DNA

f. Chain of custody is not always necessary:

**NOTES**

VII. Forensic computer analysis
   a. A branch of digital forensic science pertaining to legal evidence found in computers and digital storage media
   b. 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
   c. Although it is most often associated with the investigation of a wide variety of computer crimes, computer forensics may also be used in civil proceedings. The discipline involves similar techniques and principles to data recovery, but with additional guidelines and practices designed to create a legal audit trail.
   d. In civil cases, the organization’s policies and procedures must be carefully followed.
Corporations often have incident response plans that you should follow. Even with civil cases, keep in mind that federal and state laws related to search and seizure may come into play. The case may become a legal matter, especially if it’s related to fraud, security breaches, or privacy infringements.

i. In both criminal and civil cases, evidence must be:
   1. Legally obtained—adhere to the instructions in the search warrant or incident response plan.
   2. Complete—don’t leave behind computer evidence just because you think it might exonerate the suspect, even if you think the suspect is an awful person.
   3. Reliable—the evidence must be untainted. It should remain unchanged from its original. Following careful procedures will help you ensure that fragile computer evidence doesn't get altered, deleted, enlarged, or changed in any way. Maintaining the chain of custody will also ensure that evidence remains reliable.
   4. Authentic—it has to be the real thing, not a fake.
   5. Believable—a jury and a judge (or corporate managers and auditors) need to understand and accept the evidence. Sometimes this is challenging with highly technical, computer evidence.

e. Recognizing computer evidence—computer technology shows up in all sorts of places these days. Evaluate the scene for possible places that digital evidence can reside, including:
   i. Computers
**WHAT CAN A FORENSIC LAB DO FOR YOUR WHITE-COLLAR INVESTIGATION?**

<table>
<thead>
<tr>
<th>ii.</th>
<th>External hard drives</th>
</tr>
</thead>
<tbody>
<tr>
<td>iii.</td>
<td>CDs and DVDs</td>
</tr>
<tr>
<td>iv.</td>
<td>Thumb drives</td>
</tr>
<tr>
<td>v.</td>
<td>Floppy disks</td>
</tr>
<tr>
<td>vi.</td>
<td>Cell phones</td>
</tr>
<tr>
<td>vii.</td>
<td>Voice over IP phones</td>
</tr>
<tr>
<td>viii.</td>
<td>Answering machines</td>
</tr>
<tr>
<td>ix.</td>
<td>iPods</td>
</tr>
<tr>
<td>x.</td>
<td>Electronic game devices</td>
</tr>
<tr>
<td>xi.</td>
<td>Digital video recorders (Tivo)</td>
</tr>
<tr>
<td>xii.</td>
<td>Digital cameras</td>
</tr>
<tr>
<td>xiii.</td>
<td>PDAs</td>
</tr>
<tr>
<td>xiv.</td>
<td>GPSs</td>
</tr>
<tr>
<td>xv.</td>
<td>Routers</td>
</tr>
<tr>
<td>xvi.</td>
<td>Switches</td>
</tr>
<tr>
<td>xvii.</td>
<td>Wireless access points</td>
</tr>
<tr>
<td>xviii.</td>
<td>Servers</td>
</tr>
<tr>
<td>xix.</td>
<td>Fax machines</td>
</tr>
<tr>
<td>xx.</td>
<td>Printers that buffer files</td>
</tr>
<tr>
<td>xxi.</td>
<td>Photo copiers that buffer files</td>
</tr>
<tr>
<td>xxii.</td>
<td>Scanners that buffer files</td>
</tr>
</tbody>
</table>

**f. “Pulling the Plug”**

| i. | Two schools of thoughts on initial discovery of computer evidence—“pulling the plug” to completely power down the device or attempting to obtain volatile information in RAM before powering down |
| ii. | Safest method is to simply “pull the plug” |
| iii. | This results in loss of RAM information but: |
| l. | Any script the suspect has written that should execute upon shut-down doesn't get a chance to run. (Suspects sometimes write scripts that tell the computer to delete incriminating files when a user selects Shut Down from the Start menu.) |
## WHAT CAN A FORENSIC LAB DO FOR YOUR WHITE-COLLAR INVESTIGATION?

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2. Temporary word-processing and other interim files remain on the hard drive, whereas they might get deleted if the software applications shut down more gracefully. (Microsoft Office and other software applications write temporary files to the hard drive as the user works on documents. The files get deleted when the application is shut down in the normal way.)</td>
<td></td>
</tr>
<tr>
<td>iv. Peripherals should be “tagged and bagged” as well, including cables</td>
<td></td>
</tr>
<tr>
<td>g. The actual forensic analysis</td>
<td></td>
</tr>
<tr>
<td>i. Drives and other media are always “imaged” and the work performed on the “image” only</td>
<td></td>
</tr>
<tr>
<td>ii. HASH values assure authenticity</td>
<td></td>
</tr>
<tr>
<td>iii. EnCase is currently the “gold standard” but there are others</td>
<td></td>
</tr>
<tr>
<td>iv. Cell phones present a different problem</td>
<td></td>
</tr>
<tr>
<td>1. Multiple brands require multiple interface cables, multiple software readers</td>
<td></td>
</tr>
<tr>
<td>2. Bypassing user-created passwords requires yet additional software</td>
<td></td>
</tr>
<tr>
<td>4. If seized when “on,” do NOT turn it “off.” If seized when “off,” do NOT turn it “on.”</td>
<td></td>
</tr>
<tr>
<td>v. Regardless of the type of digital evidence, it requires not only the appropriate software but also a person trained and certified in its use before digital evidence seized in a case may be introduced in court</td>
<td></td>
</tr>
</tbody>
</table>

## NOTES

VIII. Firearms/tool mark impressions
a. A tool mark is defined as any impression, cut, gouge, or abrasion caused by a tool coming into contact with another object.

b. Certainly includes, for example, a firing pin striking the primer on a firearm.

c. Also includes such things as screw drivers, bolt cutters, car bumpers, letter openers, tires, shoes.

IX. Choosing a private forensic laboratory

a. Each will specialize in some area of forensics, such as computer forensics or DNA.

b. Choose one that specializes, not necessarily one that does everything—jack of all trades, master of none.

c. Ask that the lab provide a list of technicians who have qualified in court, the areas in which they have qualified, and the CV of each technician they may have working on your case.

d. Geography is everything, at least in relation to court appearances. If you can choose a lab within 150 miles or one across the country, choose the closest one. Paying travel time and expenses for an expert is VERY costly.

e. Your local police department or sheriff’s office is likely to have technicians qualified in fingerprint examination, computer forensics, macro photography, and tool mark impressions that work “part time” on private cases. These folks are likely already qualified in court as experts as well.