PDF File

CRIMES WITHOUT A CORPSE

UNIT OVERVIEW: This unit will introduce crimes without corpses. Some of these crimes include art forgery, currency forgery, music piracy, environmental crime, cyber crime, and questioned documents. Each individual crime will be discussed and the forensic approach to solving the crimes. The Student will build a **"Forensic Science Kit"** from the list of common materials provided.

DIRECTIONS: Read the unit material, look at the illustrations, access the suggested web sites, and complete the unit experiment. Answer the questions at the end of the unit.

FORENSIC SCIENCE KIT UNIT 16
• 6 different water-soluble black markers
• Scissors
• Coffee filters
• 6 clear plastic cups
• Clear adhesive or clear book binding tape (2-3 inches in width)
• Metric ruler
• Magnifying glass
• Stopwatch or clock with seconds indicated
• Paper

-

Key Terms		
art forgery	currency forgery	counterfeit
UV lights	music piracy	cyber crime
Cyber criminals	white-collar crime	computer
deleting	standards	requested standard
trademarks	oblique	freehand simulation
questioned document	over-writing	disguised writing
non-requested standards	watermark	indented writing
National Fraudulent Check File	ESDA	chemical fingerprinting
Bank Robbery Note File	FISH	
Anonymous Letter File	TLC	
microspectrophotometry		

Crimes without Corpses

The headlines are full of crimes of murder, but crimes without corpses are more prevalent. What do we mean by crimes without corpses? Those types of crimes might include art forgery, currency forgery, cyber crime, environmental crime, and document forgery. These types of crimes are dominated by greed, rather than anger and violence. These crimes are have sophisticated offenders and demand more inventive solutions by law enforcement and forensic investigators.

Art Forgery

Art forgery is not a common crime; however, it has been around for centuries and baffled investigators for almost as long. **Art forgery** is the crime of falsely making or altering artwork. In order to detect forgeries, art collectors and museum curators rely on forensic scientists to analyze works of art. Forensic scientists can analyze art work through various methods which will be discussed later.

Art forgers often study the works of the original artist so that they are able to learn about the country of origin, the pigments used (natural or artificial), and the artist's style. A tremendous amount of work goes into art forgery. The forger attempts to match the pigment composition and attempts to use the same brushstrokes as the original artist. Not all art forgeries are paintings. Some are other forms of media such as metals and ceramics. Ceramics are hard to copy because they are labor intensive to reproduce as well as difficult to obtain the clay from the same source as the original.

It always becomes necessary to undertake a careful scientific evaluation of the artwork before deciding on what and how the testing will be carried out. Forensic scientists use many methods to detect fakes. Some of the methods would include x-rays, analyzing fingerprints and palm prints left on a surface, UV light (black light), gas chromatography and gel electrophoresis. Each type of art object and forensic test presents its own challenges, but a thorough investigation can help to determine if the artwork is genuine or not. Just in recent years, it has become realistic to use forensic science testing and the availability of non-destructive techniques to analyze artwork and separate the original from the fraud.

One of the most well-known modern forgers was Tom Keating who claimed to have painted more than 2,000 works by great artists. However, it was not a forgery of one of the great artists, but that of a lesser-known English artist, that contributed to his arrest. In the question and answer section of this unit, you will have the opportunity to research some famous art forgeries and answer questions about them. Check out the following web site about art forgery:

https://www.futurelearn.com/courses/art-crime/0/steps/11884

Suggested readings on art forgery:

"Artful Dodgers" by Walter C. McCrone, The Sciences, January 2001

"Crime Science: How Investigators Use Science to Track Down the Bad Guys" by Vivien Bowers. Owl Books, 1997.

Currency Forgery

The crime of **currency forgery**, or counterfeiting, is as old as money itself. **Counterfeit** money describes an imitation (made with the intent to defraud) of coins, paper money, or evidence of governmental obligations. Throughout the centuries it has continued to be difficult to detect, and still continues to be so today. As forensic investigators improve their methods of detection and prevention, the criminals search for easier targets, e.g., credit card fraud, identity theft, music piracy, and trademark infringement.

Most counterfeiters are organized criminals who use multi-million-dollar printing plants to produce currency copies that are convincing to the general public. These people select their targets with careful planning. They seek currencies that have a wide international circulation, because these notes are quite easy to pass off outside the issuing country. Probably the most widely copied of all currencies is the U.S. dollar bill.

Counterfeit coins are not copied today to defraud banks, but to cheat coin collectors. This has become a big business.

In the past, banknotes were issued by having elaborate engraved designs that included hard-to-duplicate watermarking, sequential numbering, and even metal threads. Once high-quality printers became widely available, further steps were necessary to stop the forgers. Today's bank notes have new and improved safeguards to stop the forgery of currency. These safeguards include words that only appear when the note is heated by a copier lamp, color-changing ink that turns from green to black when the note is turned over, print that is only visible when viewed through a magnifying glass, machine readable bar codes, shimmering ink, and holograms. The look and feel of the bill, the watermark, and the security thread are the most reliable ways of verifying notes at the cash register which is the front line defense. Less reliable, but popular way of detecting fraud, is the UV light and iodine pens. These will detect florescent brighteners and starch, which are not used in genuine banknote paper. For more information on currency and currency forgeries, visit the following sites:

https://quizlet.com/69540596/forensics-counterfeit-flash-cards/

http://what-when-how.com/forensic-sciences/forgerycounterfeits/

To track down the currency forgers, investigators search for clues that are found in the paper type, printing techniques and the variety of ink used. All paper banknotes are now printed on high-quality stock that is impossible to mass duplicate economically. Substituted paper forms can be detected using a microscope, while **UV lights (ultraviolet)** can show the metal security threads in the true banknotes. X-rays are used to show watermarks and make them clearer. The laser and inkjet printers used to copy notes are easily detected when compared to the high quality methods used on the authentic banknotes. Chemical analysis of the ink can be traced back to the counterfeiters by suing a computer database that can match the characteristics of the ink.

Most criminal use of plastic cards such as credit cards and debit cards, involves fraud rather than counterfeiting; however, we will discuss it in this section of the unit. Card theft is becoming a big business with thieves. In most cases, the cards are stolen rather than copied. But being able to duplicate a card is not difficult, if the criminal gains access to genuine account details used to encode the magnetic stripe on the back. In fact, it is much easier to copy credit cards than it is to copy currency, due to the fact that there are so many different card designs. As long as the data contained in the magnetic strip is correct and the card looks like the real thing, a merchant will not suspect anything. When investigators look at these cards for fraud, they look for common identifying characteristics, such as defects used in the embossing process used to raise the numerals, details of the signature strip, the hologram, and the PVC overlays that cover the card's white core.

Copyrights and Trademarks

When we discuss crimes without corpses, we cannot forget about copyright and trademark infringement. Believe it or not, faked products make up an unbelievable one-tenth of all world trade. **Music piracy** is a huge problem for music companies. In fact, it is so huge that the federal government has enacted legislation to stop this crime. The government has committed to protecting musicians, songwriters, record labels, and the music they work so hard to create. Given the growing sophistication of today's music piracy trade, taking the profit out of crime is now more important than ever.

Some other types of copyright and trademark infringement include, but are not limited to, computer games, jewelry, and perfumes.

Cyber Crime

Cyber crime, or crime committed using the computer, is a big business in today's world. It includes :

- Software piracy – when computer programs are illegally reproduced and sold
- Hacking – unauthorized computer access and sabotage, either mischievously or maliciously
- Computer fraud – this deals with assets such as illegal bank transfers and credit card transactions
- Incidents of crime – the use of computers to commit crimes such as child pornography

In fact, criminals using the computer to perpetrate crimes are commonly referred to as **cyber criminals**. Cyber crime is often referred to as a **white-collar crime.** A white-collar crime is a nonviolent crime committed by an individual or a corporation that is a breech of trust, confidence, or duty. Because of the increase in computer crimes, it has become necessary for investigators to have a working knowledge of common computer-crime terms.

Because of our society's dependence on data, computers are now mainstreamed into our lives. The term **"computer"** extends beyond what we think of as desktops, laptops, and pocket computers. The term applies to anything containing a microprocessor. Even cell phones, fax machines, cameras, video recorders, even newer washing machines and clothes dryers – all contain chips to process and store data records. All of these are potential sources of evidence.

The majority of cyber crimes committed involve the use of conventional PC's. Deleting a file doesn't necessarily remove a file from a hard disk. **"Deleting"** simply changes the name of the file, in order to hide it from the user.

Computer criminals are more sophisticated these days, and are aware of the security loopholes, and use some sort of encryption and more secure deletion programs to hide incriminating data. The following list includes some common computer-crime terms and their meanings:

- Antivirus program – This is a program designed to detect a computer virus that has attached itself to a program on a disk or hard disk.
- Backdoor – This is a glitch in a computer system that will permit someone entry without a proper code or password.
- Browsing – This is the unauthorized examination of someone else's data after unlawful entry into computer files.
- Computer virus – A program is designed to attach itself to some other program and to attack and destroy the program.
- Data diddling – A procedure occasionally used by insiders. It involves placing false information into a computer.
- Fraud – As it relates to computer crimes, fraud is any use of trickery, deception, or falsification involving computers to obtain money, services, or property.
- Hacking – The illegal entry into a computer system, usually through a trial and error attempt. May also systematically use a random-digit programs, a modem, and an automatic caller.
- Impersonation – This is the unauthorized use of someone's identity, code, or password. This can also be associated with calling card or voice-mail frauds.
- Masquerading – This is also the unauthorized use of someone else's information.
- Picks – These programs are designed to break through or bypass security locks and safeguards.
- Program piracy – The unauthorized copying of commercial programming.

- Salami slice – The establishing of an account that is unauthorized in a company or bank computerized record system. Small amounts of money transfers go on unnoticed for long periods of time and eventually amount to large sums, or slices, of money.
- Superzapping – The use of repair, diagnosis, or maintenance programs to sidestep antitheft programs on a corporate computer system. Once inside, the superzapper is easily able to control the operation of the system.
- Trapdoor – A phenomenon similar to a backdoor. For the most part, trapdoors are intentionally left by a computer programmer so that they can gain entry, no matter what type of antitheft measures may be set up later.
- Trashing – The taking of information from discarded printouts, computer disks, or tapes. This is sometimes used in government or industrial espionage cases.
- Trojan horse – This is a hidden program that can lie dormant for a long amount of time until it is called up at a particular time or date occurs in the computer clock and calendar. This causes the Trojan horse to wake up. Sometime a Trojan horse will contain a computer virus. They can sometimes run specific program tasks or data manipulations.

When computer crimes are being investigated, employees or other persons help by providing information regarding the crime or possible suspects. An investigation begins at the lowest level of employees and will continue to the highest level of administration. Investigators have to remember that more than one person may be involved in cyber crime. Sometimes an audit or a repair order may bring the crime to the attention of authorities. The investigation starts with making a determination of which employees might have access to or reasons to become involved with computer crime. Evidence and records in computer crimes can be easily lost or destroyed, so investigators have to move cautiously throughout their search. The general principles of investigating cyber crime is similar to those for other crimes. The nature of the crime will determine if the crime falls under the local, state, or the federal level.

When a computer is seized as evidence, care must be undertaken to ensure that data is not lost. Many cyber criminals will booby-trap the computer. For example, touching a certain key on the keyboard, or even switching the computer on and off, could set the trap in motion and destroy evidence. If a cyber crime takes place in a large organization, an undercover operation may be set up. It is important to determine exactly what type of computer crime has been committed and if it was committed by an employee or someone from the outside. Some large companies and banks are reluctant to prosecute cyber criminals simply for the fact that it may damage their reputation.

Environmental Crimes

According to Gary Winston, Assistant State Attorney and head of the environmental crimes division of the Florida State Attorney's Office in Miami, "environmental crime is the crime of the future." With the modern methods of forensic detection we have today, it is easier than ever to track down criminals who pollute and destroy the natural environment. Laws help to protect our environment; however, all too often corruption can override concerns for the environment.

Analytical techniques can detect minute quantities of pollution in soil, air, and water. Pollution detection and control typically combine remote sensing with automated and manual testing. Detecting pollution is only half the challenge. To stop it, it must be traced back to a source, which

tends to be much more difficult. Sometimes, pollutants can be elusive, and much more difficult to track.

Environmental forensics uses investigative tools from fields as varied as chemistry, epidemiology, toxicology, biology, geology, history, and statistics. Forensics is rekindling the curiosity in environmental science. With the growth in this field, forensics is building techniques for identifying appropriate solutions into the diagnosis of a problem. Experts have established sources of pollutants and determined who is responsible. **Chemical fingerprinting** can be used to trace contaminants back to a source, especially with techniques for petroleum and lead contamination.

Environmental forensics has been referred to as a toolbox of techniques that lets you "think outside the box." Forensics helps you select the appropriate tests to acquire the appropriate data in order to make a more informed risk management decision. Environmental forensics has drawn the most attention to lawsuits where polluters pay for damages. Environmental forensics is currently also being used to determine potential liabilities. Before purchasing land with an industrial history, many companies are commissioning forensic assessments of sites before they buy, to see what legal and health risks may exist.

The field of environmental forensics is expected to grow, even on an international level. With the requirements of increasing environmental regulations and costlier litigation, this field is stepping up to meet the demand.

One of the most well-known cases of an oil spill is the 1989 *Exxon Valdez* oil spill. Even today, water samples with chemical fingerprinting are being used to see to what extent the *Valdez* petroleum is still affecting the marine life. To read more about this famous case, visit the following sites:

https://www.fisheries.noaa.gov/feature-story/lingering-oil-exxon-valdez-spill

Document Forgery

The writing habits we learned as young children are hard to shake off or disguise. We are used to holding a pen or pencil a certain way, shaping letters, and spacing lines and words. These qualities are what make handwriting such a useful diagnostic tool when it comes to questioned documents. This is the branch of forensics concerned with comparing and verifying ransom notes, forged contracts and wills, fake passports and ID, as well as other kinds of written and printed material – mostly found on paper. Whenever the source of authenticity of a document is in question, that document is deemed to be a **questioned document.**

When looking at handwriting, forensic document examiners look for individual characteristics that concentrate in four areas: form, line quality, arrangement, and content. When we think about the form of writing, you would consider the shape of individual letters, their slant, relative sizes, and how each is connected to the next. **Trademarks**, or the use of unusual characteristics, are also examined.

Also analyzed are similarities of punctuation, grammar, spelling, phrasing, and vocabulary. Examiners also work to:

- Determine if a document is authentic or if it was produced by the person who supposedly produced it

- Determine if a document was produced when it was supposed to have been produced
- Assess if a document has been altered in any way
- Compare handwriting, signatures, and typewritten or photocopied documents
- Expose damaged or obliterated writing

The forensic document examiners use all of their skills, experience, and several microscopic, photographic, and chemical analytic methods to solve these problems.

We already know that no two people write alike, even though their styles may be similar. A person's writing style is unique and is a result of unconscious automatic actions. A person doesn't think about how they write, but what they write. And you do not write the same way twice. Right now .... stop .... and write your signature ten times. Compare the results. Each signature is slightly different. Now, try holding the paper against the wall or using different writing instruments such as a pencil, pen, marker, etc. Your handwriting may be different each time, and also affected by your position and your writing utensil.

Our handwriting styles change as we age. Factors that can affect changes include disease or stroke, arthritis, fatigue, stress, impaired vision, hand or arm injuries, and intoxication with drugs or alcohol may dramatically change your handwriting.

A forensics handwriting examiner needs several **standards,** or writing samples, to get a feel for a person's writing style. If no usable **non-requested standards** (samples that already exist and are known to be authentic) are available, the examiner requests the suspect to provide a writing sample. This establishes a **requested standard.** Non-requested writings provide several advantages. The most important is that the samples reveal the writer's true writing habits and may reveal words and phrases that the writer frequently uses. A major disadvantage is that they must also be authenticated. If they can't be directly related to the writer, they do not have much value to the examiner.

A major advantage to requested writing samples is that no one questions their authenticity. The examiner watches the person write his or her name. They can even dictate what the individual writes, even a passage taken from a questioned document, so that the two samples can be compared. There are several disadvantages that accompany a requested writing sample. This causes some people to become nervous and causes them to concentrate too much on the writing process, which can lead to uncharacteristic changes. This makes the examination process much more difficult. A suspect may also try to disguise his or her handwriting style on purpose. A good way to get around this problem is to have the suspect write a good deal of material. It is easier to alter your style when writing short passages verses writing several pages.

When the examiner compares the samples between two handwritten documents, they look for similar points and points of differences while assessing the following features:

- Overall form – The size, shape, slant, proportion, and the beginning and ending strokes of the letters are part of the overall form.
- Line features – Writing speed, fluidity (how the writing flows), and the pressure used by the writing utensil provide hints about line features, as does the spacing between letters and words and how the letters are connected.
- Margins and formats – The width of margins, consistency of spacing, and the slant between lines fit into this category, which covers the overall form and layout of the writing.
- Content – Grammar, punctuation, and word choice all help point the examiner toward consistent errors, repeated phrases, and other clues that hint at a writer's ethnicity or level of education.

No single feature makes an accurate comparison, so examiners look for all these features when comparing documents. Based on findings, an examiner might say that the documents: absolutely match, match with a high probability, probably match, or do not match. Not every examination ends with an answer. On occasion they may say that they cannot make a determination based on the samples. Fortunately for the officials, most criminals aren't that clever. Many criminals misspell in the documents, and forensic examiners use these mistakes to their advantage.

The FBI maintains the **National Fraudulent Check File,** the **Bank Robbery Note File**, and the **Anonymous Letter File.** Examiners are able to compare documents in question with these files. High-tech files, like the **Forensic Information System for Handwriting (FISH)**, are also in existence. FISH contains scanned and digitalized documents that officials can compare with and stack up against other similar documents. Forensic document examiners visually check any matches. By double-checking samples, the possibility of mistakes is eliminated.

It is left up to a judge or jury if a document was altered or written by someone other than the stated author, for the purpose to defraud. Even the most talented forgers leave behind evidence of their efforts. Examiners don't just inspect with the naked eye, but also with the microscope. A common form of forgery is called **freehand simulation.** This is the attempt to copy a signature or handwriting sample, and tracing involves placing another document over an original signature and tracing its lines. An examiner can identify defects in the writing because of the unnatural feel of the forger. Perfectly matching another person's handwriting is not easy to do. Some common clues that give away forged writings include:

- Evidence of a previous drawing, which can include an underlying tracing of the words of signature
- Forger's tremors that indicate fine yet distinguishable markings or shakiness in the writing
- Uneven writing speed and pen pressure
- Hesitations
- Unusual pen lifts, where the forger continually checks his or her handiwork
- Patching and retouching, fixing or adding marks
- Blunt beginnings and endings

Another form of writing is called **disguised writing.** Disguised writing is a deception, where the writer attempts to disguise their handwriting. Many ransom notes are written this way.

Often times, forgers will try to remove, add, or change parts of written documents for a variety of reasons. Those reasons might be for financial gain and even to creating an alibi. Some alterations may be as small as changing a date or as complex as attempting to rewrite or erase signatures or

portions of documents. These changes are called erasures, obliterations, and alterations. Forensic investigators use the following investigative tools:

- A magnifying glass or a microscope used with **oblique** (angled) lighting that will uncover most erasures
- Ultraviolet or infrared light that may expose tiny fragments of erasers and ink that is stuck on the fibers of the paper
- Lycopodium powder, when dusted on the page, will cling to and expose tiny rubber particles and eraser fragments that remain after erasures

Being able to expose the erasure marks is important because even if the examiner can't see the original words or marks, they will at least know that someone altered the document, which may be proof of a crime and make documents null and void.

Sometimes criminals think they can destroy a document by burning it; however, many times there are enough fragments left over to identify the document. Handling charred pieces of paper is extremely difficult because they will crumble easily. The examiner can spray the paper with a solution of polyvinyl acetate in acetone in order to stiffen the paper and make handling easier. Next they treat the treated pages in a solution of alcohol, chloral hydrate, and glycerin and photograph them. They can also place the pages between two photographic plates and place them in a dark room for two weeks. They then develop the plates, which may reveal handwriting.

Often times, a forger will add words or marks to further alter the document. One of the most common ways is to change the amount of a check or date on a contract or will. These changes can be detected by looking for slight changes in the color of the ink, line thickness, pen pressure, and double lines.

Over-writing, is another way to forge. This is not done by erasing anything, but rather adding to or overwriting a part of the document. If the same type of ink is used both times, it can be very difficult to uncover. However, most forgers do not have access to the pen or ink that was originally used.

To the human eye, it may seem that two inks can be identical; however, under UV or infrared light, they may appear to be quite different. If lighting techniques do not provide any help in determining the forgery, the examiner may have to examine the chemical contents of the inks to show that they are quite different.

In the movies you have probably seen someone write a ransom note or threatening comments and then tear the page from a tablet. Underneath, indentations may be found that will expose the writing. The movement of a pen over a page will indent the page underneath along the path of the pen, creating what is called **indented writing.** On TV, they often use a pencil and rub the paper to expose the handwriting. Actually, this may destroy the evidence. On occasion, angling light over the paper will reveal indentations. When it does, a photograph is taken. A more sensitive method is the use of an **electrostatic detection apparatus (ESDA)**, which can often uncover indented writing several pages below the original page. The examiner, when using ESDA, will place a Mylar sheet over the page to protect it. They will then place both on a porous metal plate. A vacuum pulls the Mylar tightly against the page. Then an electric wand is passed over the sheet and the page producing

static electricity. The charge will be the greatest in the indentations. When black toner is poured or sprayed over the surface, similar to what is used in copy machines, it attaches itself to the surface in proportion to the degree of charge and reveals the indented writing.

On occasion, the forensic document examiner will need to determine if pages have been added to a document or if the document was actually created at a particular time. In these cases, the examiner may have to analyze the paper and ink that were used to create the document. Most types of paper are made of wood and cotton, and have chemical additives that will affect its opacity, color, brightness, strength, and durability.

- Coatings – improve the appearance and surface properties of the paper and may even make the paper better for copiers, printers, or even for writing
- Fillers – add color, strength, and surface texture
- Sizings – make the surface less porous to ink, so that writing and printing appear sharp and clear

The types and amounts of each of these additives will vary among manufacturers and paper types. Chemical testing will distinguish one type of paper and manufacturer from another. A **watermark** is another distinguishing characteristic. This is a translucent design on the paper that you can see by holding the page up to a light. By doing so, you can identify the manufacturer, the date of its production, and often for whom the paper was manufactured. Forgers have difficulty producing watermarks because with a true watermark, you will be able to spot it easier because there are fewer fibers than on the rest of the page. A forged mark is an added image that has a fiber density equal to the rest of the page. For more information about watermarking, visit these sites:

http://www.motherbedford.com/watermarks/Watermark1J.htm

http://research.microsoft.com/~hoppe/water.pdf

http://www.watermarks.info/indexi.htm

Often, the key to determining authenticity of a document lies in the ink that the writer used. Inks may appear to be identical physically, however, chemically they are very different. This distinction aids the identifier in determining if the same ink was used for each page or word and may even help determine if a particular ink even existed at the time the document was prepared.

There is one nondestructive method of ink comparison called **microspectrophotometry**. This process enables the examiner to accurately determine if the colors of the two inks match by comparing their light transmission, absorption, and reflective characteristics. Another method for comparing ink samples is **thin-layer chromotography (TLC)**, which is described below:

- Very small samples of the inked paper are punched from the written lines using a thin hollow needle.
- The tiny pieces of paper are placed in a test tube, and a solvent that dissolves the ink is added.

- A drop of the solvent solution, which now carries the ink, is placed on a paper strip along with drops of several known control inks.
- The strip is dried and then dipped into another solvent that migrates up the paper strip, dragging the inks along with it.

The respective size of the molecules will determine how far along the strip the inks will migrate. This process separates the inks into bands. If two different inks are used on the document, there will be different distinct bands. The U.S. Secret Service Forensics Services Division Questioned Document Branch maintains an extensive ink reference database which is located at the Ink Library. They maintain an extensive database of the TLC patterns of commercial inks. In recent years, more manufacturers have begun adding fluorescent-dye tags to their products so that identification is easier. The tags are changed annually so that forensics can more easily determine the year that the product was manufactured.

Other clues concerning the origin of a document other than pen and paper are left behind. Typewriters, printers, and copy machines can leave distinguishing marks on typed or copied papers. Typewriters are frequently used to write threatening letters, ransom, and extortion notes. If a typewriter has been used, the examiner tries to determine the make and model of the typewriter as well as matching up the note with a suspect typewriter, if there is one available. Of course, there is a database available with typefaces used in various models, both new and old. Recently, typewriters have given way to computers. Printers vary so little that distinguishing one from another is quite difficult. When searching typewritten documents, the examiner looks for misaligned or damaged letters, abnormal spacing before or after certain letters, and variations in the pressure applied to the page by some letters. They also look at the ribbon for additional information.

Copy machines duplicate images from one page to another through a complex series of events. Examiners can sometimes match a photocopied document to a particular copy machine because the mechanisms may leave marks on a page. The machine glass or camera lens may have scratches or defects that mark every page that it produces. Often these marks will appear on the photocopied page.

Document Authenticity Experiment

Experiment adapted from Forensics Teachers A-Z Resource Guide, Discovery Channel School.

Examiners use chromatography to match unknown substances with known substances. With the use of a mass spectrometer, a device that measures light absorption, examiners take chemical fingerprints. These fingerprints help examiners identify the substances. If they find an exact match, they try to locate the manufacturer.

This experiment uses chromatography to determine which ink was used to write a document. Paper chromatography is used to separate ink mixtures. Water carries the pigment up the paper by capillary action, an attractive force between the water molecules and the paper fibers. The ink separates into a rainbow pattern, but not all black inks leave the same patterns. Investigators may use individual color patterns to identify a particular brand of pen.

Materials:

- 6 different water-soluble black markers

- 7 precut strips of coffee-filter paper (cut into strips 10 x 3 cm each)
- 6 clear plastic cups
- Clear tape
- Metric ruler
- Magnifying glass
- Stopwatch or clock with seconds indicated
- Mystery document written with one of the 6 markers

Procedure:

1. Think about how examiners determine the authenticity of a document. What can you determine about the paper and the ink? Are there any identifying marks that are unique that could help determine the writer of the document? Could there be fingerprints on the paper? What kind of pen might have been used to write the document? What can you tell about the ink? Are all black inks the same? If the ink is a mixture of pigments, how can the pigments be separated?
2. Set out the six water-soluble black markers, plastic cups, tape, ruler, the precut coffee-filter strips, watch or clock, and magnifying glass. Make sure that you know which marker is used on which strip of paper.
3. Have a partner write a short document using one of the markers. The marker used by your partner should remain a secret until the end of the experiment. Without your knowledge, your partner should make a black dot three centimeters from the end of the coffee-filter strip and lower the strip into 2 cm of water so it doesn't reach the black dot. Your partner should show you the strip and tell you that this is a sample of the ink used in the document.
4. Make a black dot 3 cm from the end of each strip of coffee-filter paper. Fill each clear plastic cup with 2 cm of water. One at time, lower the strip so that it touches the water but doesn't reach the black dot.
5. Use your stopwatch or clock to determine how long it takes the pigments to separate on each strip of paper and move up. Measure the distance in cm.
6. Design a data table or graph to keep track of your results. Include space for each filter strip sample and important information about each pen (such as pen # 1, etc.).
7. Have your partner show you his/her strip that matches the document. Examine his/her strip against yours and make a match.
8. You will answer questions about your experiment in the unit question section.

Unit Extension

Explore the following forensic careers:

Document Examiner

Environmentalist

Computer Specialist

Conclusion

This unit introduced crimes without corpses. Topics of discussion included, art and currency forgery, music piracy, environmental crimes, cyber-crime, and questioned documents. These types of crimes are dominated by greed, rather than anger and violence. However, they continue to be

prevalent crimes within our society. Because these crimes are becoming more sophisticated, forensic examiners and investigators must implement more inventive solutions to crime solving.