10.2 Victims and suspects

A lot can be learnt from a body. Its features and proportions help forensic scientists to identify it and marks on it can suggest the cause of death. Likewise, forensic science can provide investigators with the evidence they need to successfully identify and convict those who committed the crime.

INQUIRY science 4 fun

Teeth impressions

Can you be identified from your teeth?

Collect this ...

- 'jelly' lollies such as jelly frogs or snakes (one per student)

Do this ...

1. Carefully bite *once* into the jelly lolly. If possible, bite right through it.
2. Compare the teeth impression with your actual teeth. Did it have the same number?

Record this ...

Describe any differences between your teeth impression and your actual teeth.

Explain how teeth impressions might be used to solve a crime.

Autopsy

A corpse will be sent from the crime scene to the coroner's office where forensic pathologists perform an **autopsy**. This is done to:

- confirm the identity of a 'known' body or to find out who an 'unknown' body is
- determine or confirm the cause of death.

The main steps in an autopsy are shown in Figure 10.2.1.

Identifying bodies

Visual confirmation of a body is often impossible if it has been in a fire or explosion or has been in the water or bush for some time. Identification is even more difficult if there is nothing to link the body with its surroundings. Investigators must then try to match it with descriptions and photos of missing people on police files. If the person has been missing for a long time, then the task is even harder. The information on the database will then be inaccurate.

To aid identification, pathologists carrying out the autopsy will:

- take fingerprints where possible from the body. These can then be compared with fingerprints on police files or those found around the house or apartment where the person thought to be the victim lived
- inspect any remaining tissue for identifying marks such as birthmarks, tattoos and scars. These can then be compared with marks seen on the likely victim in family photos or on the database of missing persons
- take samples or photos of clothing and jewellery. These can then be compared with those worn by the likely victim when last seen alive
- extract DNA from any remaining tissue and compare it with DNA collected from the clothing, toothbrush or hairbrush of the likely victim. If the person has been missing for a long time, then their home is likely to have been cleaned out, leaving none of their DNA. Their direct relatives will have similar DNA and so comparison may need to be with them.

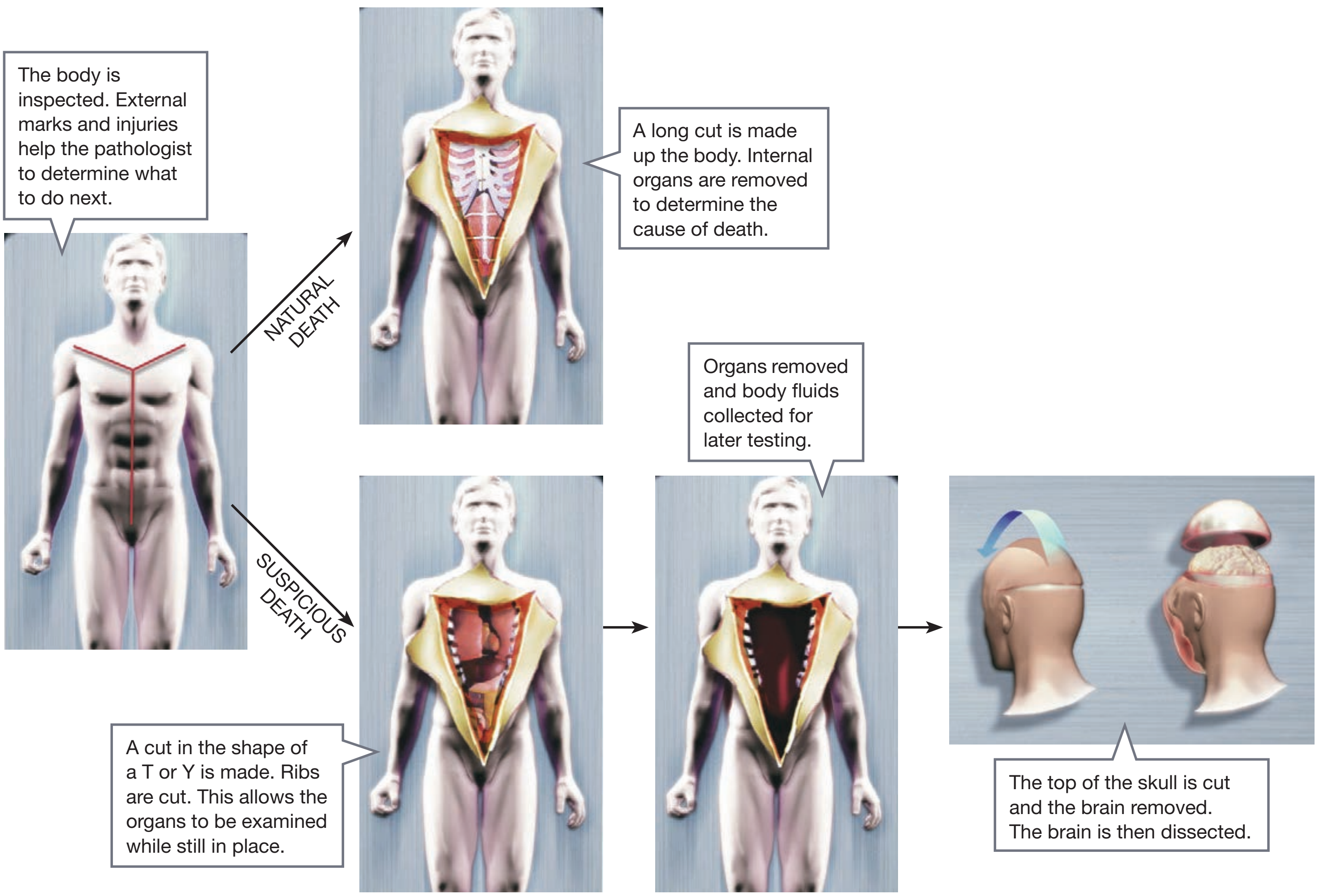


Figure 10.2.1 An autopsy is a systematic dissection of a corpse. The exact order and degree of dissection depends on whether the victim is thought to have died naturally or from foul play.

Identifying skeletons

DNA deteriorates with time, especially when exposed to intense heat. There might even be no tissue left on the skeleton to analyse on corpses that were not discovered for a long time. Investigators then compare the medical and dental records of the likely victim with the injuries and dental work found on the skeleton. Badly broken bones commonly have pins, plates and screws inserted in them (like those in Figure 10.2.2) to help them repair. Finding these in a skeleton can confirm its identity, as can replacement hips or knees.

Figure 10.2.2 This artificial knee and the pegs used to fix it to the bones are clearly visible on an X-ray. They would quickly confirm the identity of a body.

SciFile

Anthropometry

Alphonse Bertillon became chief of criminal investigation for the Paris police after he developed a way of identifying people from their body proportions. His system (called **anthropometry** or the **Bertillon system**) was widely used from 1882 to 1905 until a twin brother was incorrectly jailed!

Jewellery, belt buckles and buttons left on the skeleton will also give an idea of the victim's sex and age. Their style changes every 10 years or so and will also suggest roughly when the person died.

If none of this if possible, then the age and sex of the corpse can be determined from the size and density of large bones such as the pelvis, skull and femur (the main bone of the leg). Figure 10.2.3 shows a forensic scientist taking some of these measurements.

1 p344

Figure 10.2.3 Measurements of a skeleton can provide information about the sex and age of the victim.

10.3

Cause of death

A forensic pathologist must determine whether death was natural or caused by someone or something else. Each cause of death such as shooting, stabbing and drowning leaves its tell-tale signs.

Shooting

Bullets may still be in a body or may have exited and lodged in furniture or walls nearby. This allows the path of the bullet to be determined. Shotguns shower a victim with multiple pellets. A single wound suggests that the shotgun was close while a scattering of wounds like those in Figure 10.2.4 suggests that the victim was shot from a distance. If there are burn marks from the exploding gunpowder this would indicate that the gun was shot from close range.

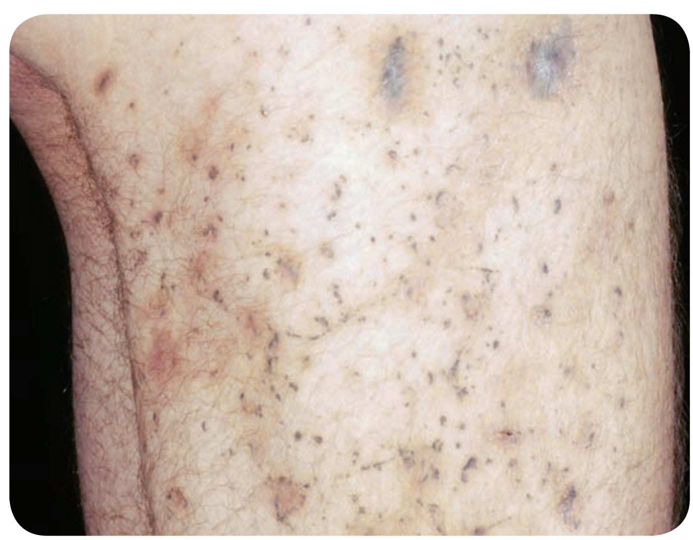


Figure 10.2.4 These wounds are from the pellets of a shotgun. They are spread out, indicating that the shooter was some distance from the victim. If the shooter was close, then the individual wounds would join to form one large wound.

Wounds

Knives leave their own tool marks on the body. For example, the wound produced by a straight-edged knife is different from one with a serrated edge. The depth of the wound gives an idea of the force used in the attack, and its angle suggests the direction of the attack. (Sometimes the angle will even suggest that it was not an attack at all but a horrible accident.) Where the wounds are located also provides information about the attacker. Wounds on the right side of the chest, for example, suggest that the attacker was left-handed. Wounds on the right of the back suggest the attacker was right-handed.

Bruises like those in Figure 10.2.5 indicate that a blunt object was used as the weapon.

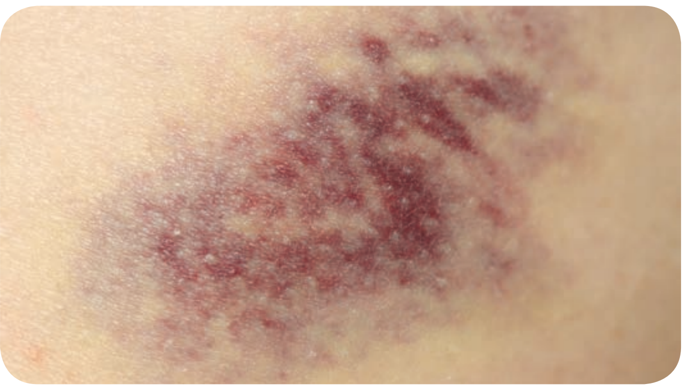


Figure 10.2.5 Skin bruises badly if punched, kicked or hit. The skin won't be pierced but it might split and bones underneath are likely to fracture.

Drowning

Water will be in the lungs and stomach of a victim who has drowned. This water will contain **diatoms**. These are small single-celled organisms that are partly made of silica, a very hard material that forms a variety of shapes. Some are shown in Figure 10.2.6. Each creek, lake or dam has different-shaped diatoms and their shape can pinpoint the location of a drowning and whether the body was shifted after death.

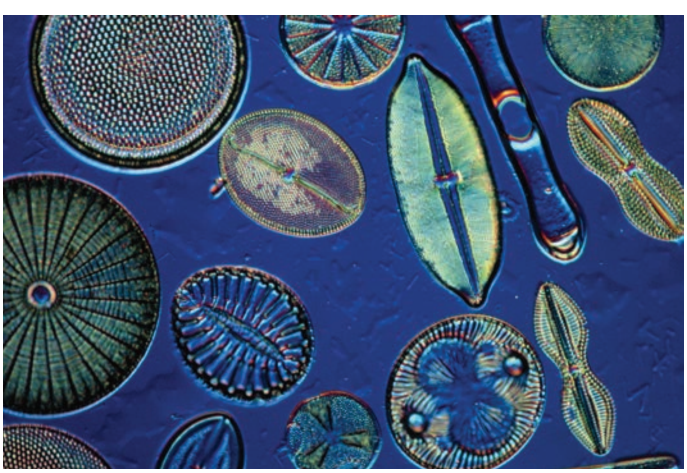


Figure 10.2.6 Diatoms come in an amazing variety of shapes, as this scanning electron microscope (SEM) image shows. The characteristic shapes of diatoms can point to where a drowning occurred.

Identifying suspects

Photographs

Photographs are excellent for proving identity and are used in passports, driver's licences and student identification cards. They are not as useful for identifying suspects. This is because:

- the only photos police have will be those who have already been found guilty of previous crimes. First offenders won't yet have their photos on file
- an eyewitness needs to sift through hundreds of photographs. This exposure can lead to **retroactive interference**, a process in which eyewitnesses involuntarily merge images in their memory to form a 'suspect' who looks nothing like the person who committed the crime.

Identikit

Sketched portraits have long been used as a method of identification. At first these sketches were drawn by professional artists from descriptions from eyewitnesses. However, the quality of these portraits depended as much on the ability of the artist as it did on the accuracy of the eyewitness account.

Identikit became widely used after 1959. It used sets of pre-drawn facial features (eyes, mouth, chin shape etc.) that slotted together to form a portrait. Identikit had many advantages over artist-drawn portraits. It:

- allowed a realistic image to be constructed at any police station
- did not depend on the ability or availability of an artist
- allowed various combinations of features to be tried to trigger the memory of the eyewitness.

Figure 10.2.7 Computer software allows realistic images of suspects to be produced by dragging across different facial features from its database of images.

Today, police use computerised versions of Identikit like the one shown in Figure 10.2.7. The computer-composite images are fast, can be digitally enhanced to make them even more realistic and can be three-dimensional. Some are incredibly accurate, like the one in Figure 10.2.8 on page 338.

2 p345

Figure 10.2.8 This computer-generated Identikit image of a criminal helped to catch him in 2005. It shows a remarkable similarity to the real man.

Home-grown FACE

SciFile

In 1989, Australia was the first country to produce a coloured computerised version of Identikit. Called FACE, it allowed police to take laptop computers to the crime scene and immediately identify criminals. FACE helped to identify the three men who had set off explosives in the 2002 terrorist bombing in Bali.

Proving the suspect was there

For a prosecution to be successful, police need to be able to prove that a suspect was at the scene of a crime. This can be done in a number of ways, including:

- electronic tracking
- fingerprints
- DNA.

Electronic tracking

Security cameras and **CCTV** (closed circuit TV) are now common in shopping centres, banks, train stations and airports, outside nightclubs and even in city streets and lanes. Video from these can prove that a suspect was at the scene at the time of the crime. They may even show the suspect carrying out the crime.

Biometric facial recognition technologies that allow a CCTV to scan a crowd and identify known offenders are now being trialled. Most of these techniques compare the positions of points on the face with those of known criminals. Figure 10.2.9 shows how it's done.

When switched on, your mobile phone can enable your phone company to locate you to within 10–50 metres. This allows police to track suspects (and victims) and gives an easy way of proving that the suspect was close to the scene at the time the crime happened.

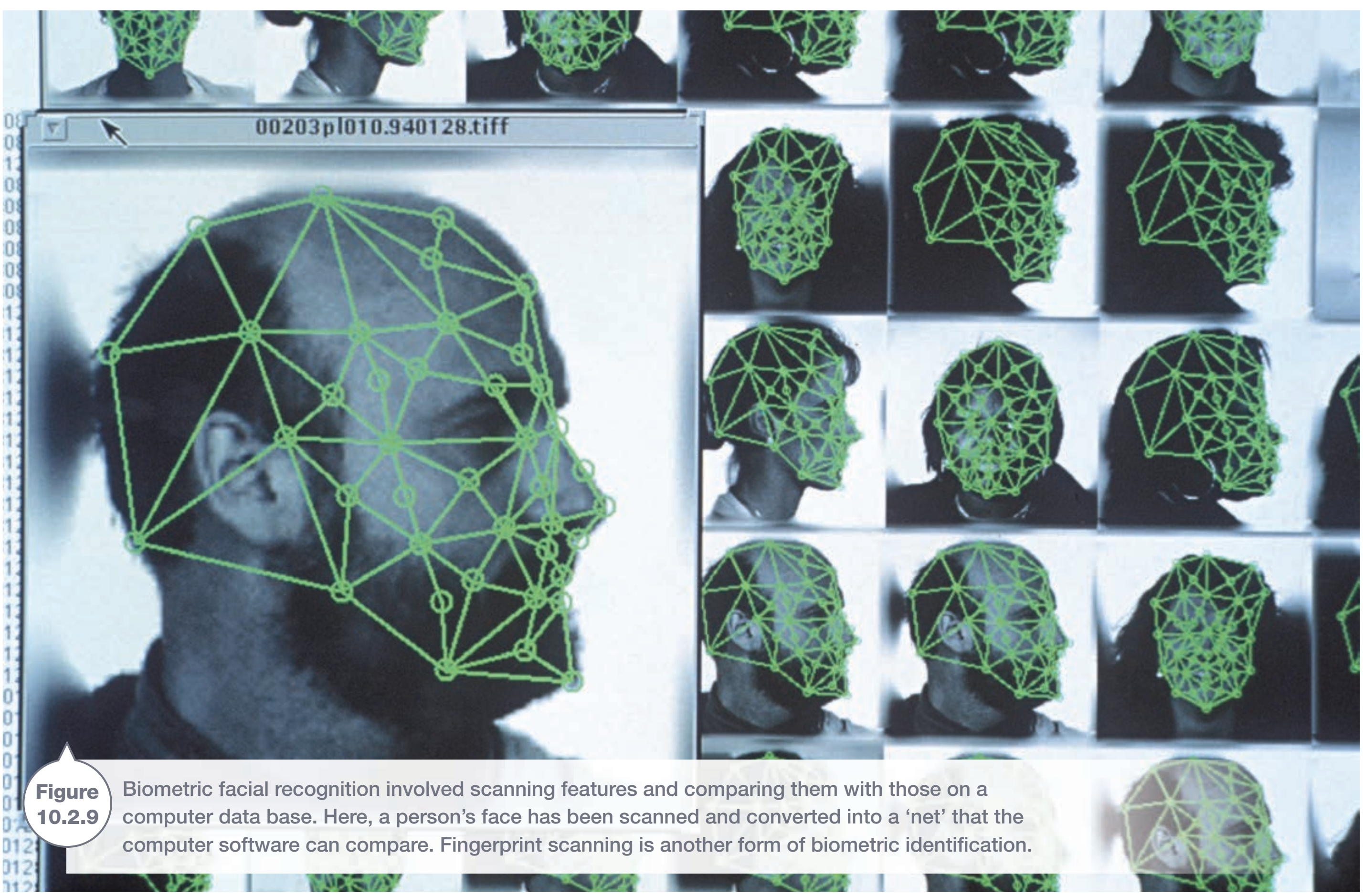


Figure 10.2.9 Biometric facial recognition involved scanning features and comparing them with those on a computer data base. Here, a person's face has been scanned and converted into a 'net' that the computer software can compare. Fingerprint scanning is another form of biometric identification.

Photos or video of unlawful behaviour sometimes ends up on social networking sites. Once there, it can be used as evidence in court. For example, in 2009, police used a video posted on Facebook to convict a 20-year-old Victorian man of hoon (dangerous) driving. His $21 000 Ford Falcon utility was confiscated, his licence was disqualified for 18 months and he was fined $2000.

SciFile

Warning, warning!

Some police districts in the United Kingdom have been trialling CCTV cameras that speak! Police watch the cameras at all times and use small speakers to warn people who are misbehaving that they are being watched.

SKILL BUILDER

Taking fingerprints

Good fingerprints can end up being smudged or with too much or too little ink. To take a good fingerprint, follow these steps.

1. Roll your thumb across the damp surface of the inkpad.
2. As Figure 10.2.10 shows, roll it *once* across white paper.
3. If the print is smudged or has too much ink, then *do not* get more ink but 'dry' your thumb by rolling out more prints of it.

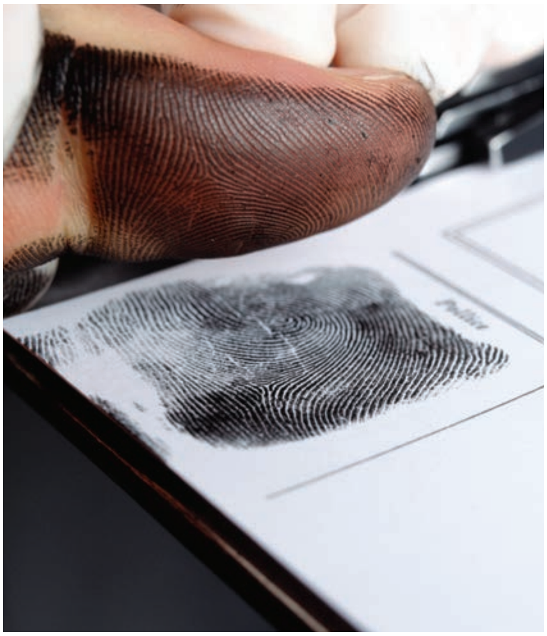


Figure 10.2.10 Roll your finger and don't squash it.

INQUIRY science 4 fun

Taking fingerprints

Can you take good fingerprints?

Yes

Collect this …

- ink pad
- white paper
- scissors
- glue or sticky tape

Do this …

1. Refer to the Skillbuilder and follow its steps to produce two good thumbprints.
2. Repeat with another finger.
3. Cut out the best two images of your thumb and two of your finger.
4. Paste one of each into your workbook, writing your name above them.
5. Swap the others with someone else in the class. Paste theirs in your workbook too, writing their name above theirs.
6. Construct a tally of the different types of fingerprints in your class. From this tally, identify which type is:
   a. most common
   b. least common.

Record this …

Describe the fingerprints you produced. Are they loops, arches, whorls or composites?

Explain what you think your results suggest about finding suspects based on their fingerprints.

Fingerprints

No two sets of fingerprints from different people have ever been found to be the same. This makes fingerprints an excellent method of identifying suspects or proving that they were at the scene of a crime. The patterns that fingerprints form can be classified as **loops**, **whorls**, **arches** or **composites**. These are shown in Figure 10.2.11 on page 340.

Before computers, fingerprints were unlikely to be stored outside the state or country of the suspect. Also, manual comparison of fingerprints was difficult since it is slow and prone to mistakes. For these reasons, some criminals were able to move about undetected, committing crimes as they went. Computers have overcome most of these problems by storing, sharing, comparing and matching fingerprints across different states and countries.

SciFile

Same but different

Identical twins do not have identical fingerprints. However, their fingerprints do share more similarities than found between non-twin brothers and sisters.

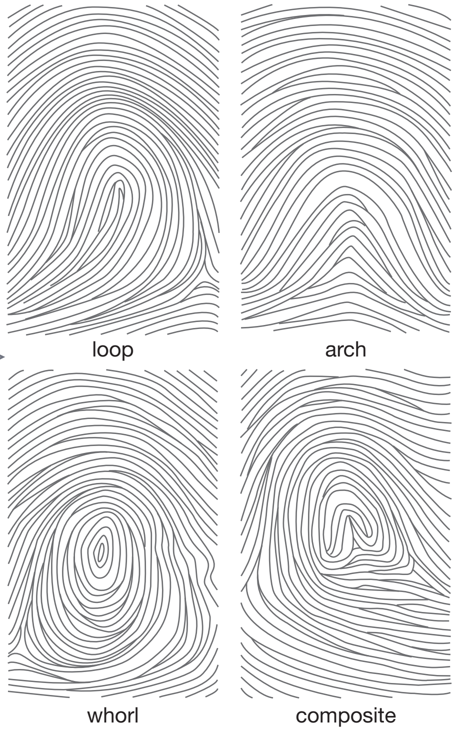


Figure 10.2.11

The four basic fingerprint types: loops, whorls, arches and composites. About 60–65% of all fingerprints are loops, about 35% are whorls and 5% are arches. Composite fingerprints are even more uncommon.

DNA profiling

DNA can be extracted from even the tiniest samples of flesh, blood, hair, saliva or semen left at a crime scene. For example, a knife used in an attack will contain the DNA of the victim in blood on its blade and the DNA of their attacker in sweat and oils on its handle. Everyone has different DNA and everyone's DNA produces a different autoradiogram. One is shown in Figure 10.2.12. An **autoradiogram** is produced by chopping up DNA and then separating its fragments. This process is called **gel electrophoresis**, and is shown in Figure 10.2.13. Computer programs then run matches against DNA on police databases.

Finding a suspect's DNA at a crime scene is proof that they were there at some time. However, it does not suggest when they were there or for what reason.

3 p345
10.4

Figure 10.2.12

An autoradiogram codes DNA as a series of black bars. If the pattern of the bars in a suspect matches those from a crime scene, then it proves they were there at some time.

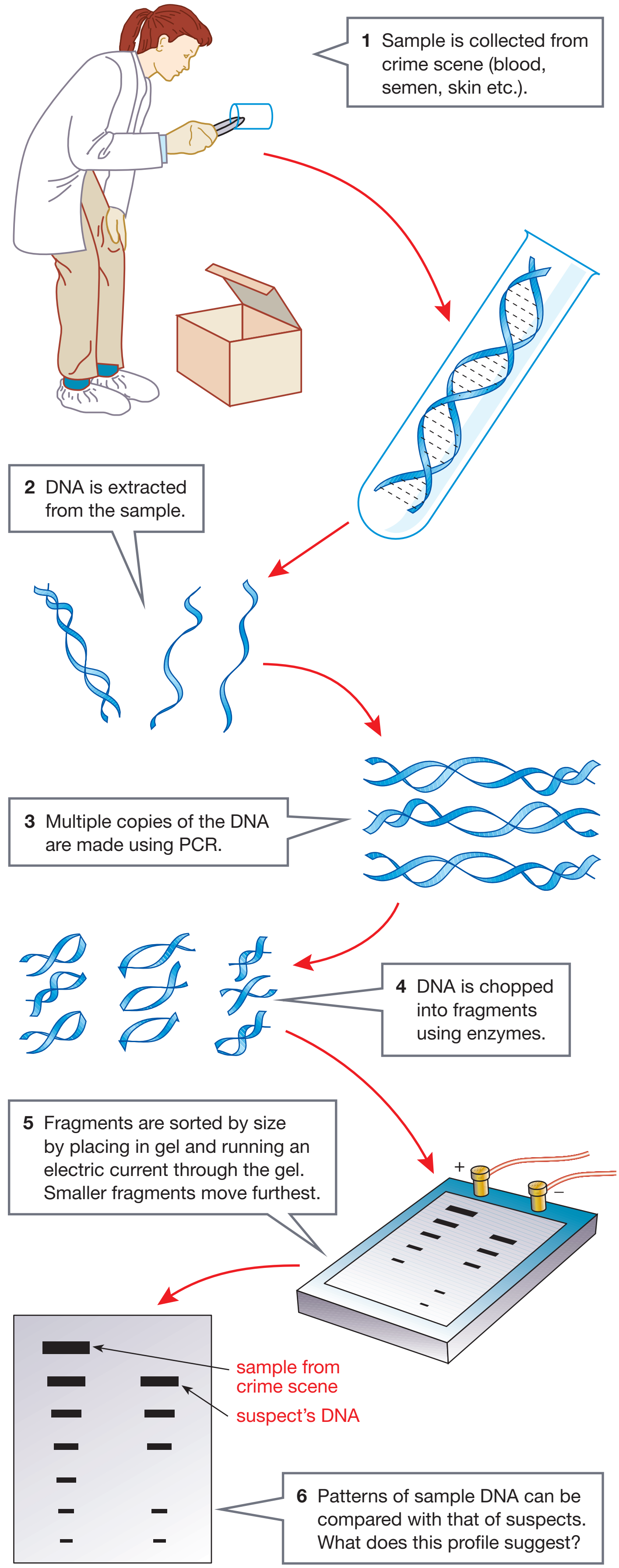


Figure 10.2.13

DNA from a crime scene is extracted, copied, chopped and then separated using gel electrophoresis. The end result is an autoradiogram.

SCIENCE AS A HUMAN ENDEAVOUR

Use and influence of science

New poisons

Figure 10.2.14 Dioxins failed to kill Victor Yushchenko in 2004 but he still bears the scars of the assassination attempt. These two photos were taken 5 months apart.

There is a long history of using poisons for assassinations (political murders). Assassins in ancient Rome commonly used poisons to kill opponents. Poisonous mushrooms killed the Roman emperor Claudius, and his successor Nero used cyanide to kill relatives who threatened his power. Family dinners were simply murder!

Since ancient Roman times antinomy, arsenic, lead, mercury and thallium have all been used to kill. However, the symptoms of these poisons are now so well known that doctors quickly realise that they are not dealing with simple illness. Police quickly realise that an attempted assassination has taken place. For these reasons, assassins have recently used some very different poisons.

Ricin

Ricin is a poison extracted from castor beans that is about 200 times more deadly than cyanide. Its symptoms are similar to natural diseases and vary depending on whether it has been eaten, injected or breathed in. There is no test that will confirm its presence and there is no known antidote (cure).

In most cases, ricin has been detected before it had a chance to poison anyone. For example, ricin was found in mail sent to the White House in 2003. Ricin was used in the bizarre assassination of Georgi Markov in 1978 in London (UK). Markov had defected (escaped) from communist Bulgaria seven years earlier and wrote anti-communist books and plays. Markov collapsed after being 'accidentally' jabbed in the leg by a passerby with the tip of an umbrella. It probably looked like the one shown in Figure 10.2.15. Markov died three days later. An autopsy found in his calf a tiny metallic pellet that had been drilled out and which contained traces of ricin. It seems that the umbrella was a specially designed gun and the passerby an assassin. There was a similar, failed, assassination attempt ten days earlier in Paris on another Bulgarian defector, Vladimir Kostov. The KGB (the Soviet secret police) is thought to have been behind both incidents.

10.5

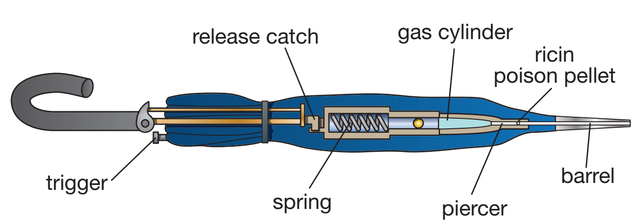


Figure 10.2.15 An artist's impression of the umbrella 'gun' used to shoot Georgi Markov in 1978.

Dioxins

Dioxins are poisonous chemicals that are present in tiny quantities in cigarette smoke, plastics and some industrial wastes. In 2004, assassins used dioxins in an attempt to kill Victor Yushchenko while he was campaigning to become President of the Ukraine. He suddenly fell ill with suspected food poisoning. Five days later he developed lesions and ulcers on his face, chest and stomach and throughout his digestive tract. Blood tests showed extremely high levels of dioxins in his blood. He survived, eventually won the election and became president in 2005. Figure 10.2.14 on page 341 shows him before and after being poisoned.

Radioactive poisons

Radioactive materials are incredibly dangerous and exposure to them is usually accidental or highly controlled. For example, radiotherapy uses controlled doses to kill cancerous cells. However, the radioactive element **polonium-210** was used to kill Alexander Litvinenko (Figure 10.2.16) in London in 2006. Litvinenko once worked for the KGB but had defected to the United Kingdom. There he was highly critical of the Russian government, and its then-president Vladimir Putin. Litvinenko fell seriously ill soon after meeting with two ex-KGB officers for lunch. Polonium-210 was found in his urine and 3 weeks later he was dead. No-one is sure how Litvinenko was poisoned but investigators are certain that it was deliberate. This is because polonium emits **alpha rays**, a type of nuclear radiation that is easily blocked. If exposure was accidental, then his clothes and skin would have stopped it entering his body.

A nuclear reactor is needed to produce radioactive materials such as polonium-210, probably putting the murder well beyond the normal assassin and organised crime. It is thought that only a government or secret service would be able to access such materials.

In 2007, the United Kingdom charged Andre Lugovoy with the murder of Litvinenko. He was one of the ex-KGB officers who had lunch with Litvinenko the day he fell ill. Russia has refused to extradite (release) him for trial.

Figure 10.2.16 Alexander Litvinenko before and after he was poisoned with polonium-210. Polonium emits radioactivity in the form of alpha rays. Traces of polonium-210 were found in his urine, the restaurant where he ate, his home, his office, a hotel and two aircraft he travelled on.

10.2 Unit review

Remembering

1 **State** two pieces of evidence that might suggest a murder happened well away from where a body is found.

2 **State** how accurately authorities can locate you using the signal from your mobile phone.

Understanding

3 **Explain** how a belt buckle or buttons on a skeleton can help in determining the sex of a long-dead murder victim and when the murder may have happened.

4 It's much easier to confirm the identity of a body found in a burnt-out house than one found in the bush. **Explain** why.

5 **Explain** what DNA found at a crime scene:
- a tells police
- b doesn't tell police.

6 Hairbrushes and toothbrushes are often taken by forensic investigators. **Explain** why they would take them from the:
- a home of a missing person
- b homes of their blood relatives.

7 **Explain** how investigators determine if a shotgun blast came from close or far away.

8 **Explain** how Facebook led to the confiscation of a Ford Falcon utility in 2009.

9 **Explain** why Alexander Litvinenko's exposure to polonium-210 could not have been an accident.

Applying

10 **Use** Figure 10.2.17 to **identify** the origin of:
- a trace evidence 1
- b trace evidence 2.

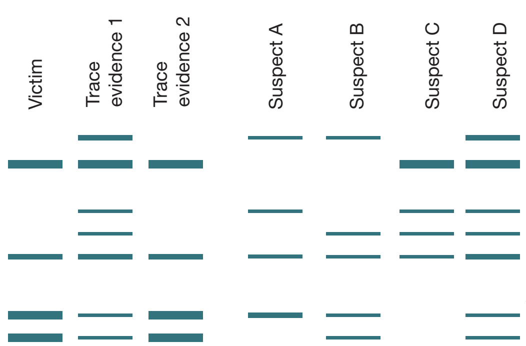


Figure 10.2.17

11 **Identify** what type of murder weapon was used if:
- a there is a clear entry and exit hole on the body
- b there is a 'peppering' of wounds
- c the person was complaining of stomach problems before they died.

Evaluating

12 **Propose** reasons why CCTV cameras are commonly located in:
- a large shops
- b banks
- c petrol stations.

13 Facial recognition software will eventually allow CCTV to track people, whether they are known offenders or innocent people going about their daily business. **Evaluate** whether this is fair and give your opinion on whether it should be allowed.

14 **Propose** how a mobile phone can be used to fake an alibi, suggesting that suspect was well away from a crime scene when they were really there.

15 Some people argue that YouTube has encouraged young people to undertake very dangerous activities, like those found in films such as *Jackass*.
- a **Propose** reasons why YouTube might be able to do this when earlier technologies did not.
- b **Assess** whether it is a good idea to upload a video of a dangerous activity onto YouTube.

16 Doctors first thought that victims of ricin, dioxin and polonium poisoning had simply eaten something that had 'gone off'. **Propose** the advantages this gives an assassin.

Creating

17 **Construct** or trace diagrams to contrast whorls, loops and arches.

Inquiring

1 Perform an interactive autopsy on an artificial human by searching for a *virtual autopsy* site on the internet.

2 Use the following as key words to search the internet to find forensic games to play.
- Identikit games
- fingerprint games
- DNA fingerprint or DNA matching games

3 DNA has sometimes led to the wrong person being found guilty. Research the case of Farah Jama and outline what went wrong.

4 Research cases in which DNA has proven that protected species of whales have sometimes ended up as sushi.

5 At one time, the law didn't require evidence to prove the guilt of a suspect. Investigate what trial by ordeal was and how it was used in law.

10.2 Practical activities

1 Measuring the body

Anthropometry is the measurement of the human body.

Purpose

To determine whether anthropometry accurately predicts height.

Materials

- dressmakers' tape measure or string and metre ruler
- access to skeleton (or photo of skeleton)
- calculator

Procedure

1 Use Figure 10.2.19 to locate the femur, noting where the bone begins and ends.

2 In pairs, use the tape measure to determine the length of each other's femur. Alternatively, mark the length on the string and then use the ruler to measure its length. Record its length in a table like that shown below.

3 Measure your actual height and that of your partner (in centimetres). Record the height in the table.

4 In a similar way, measure the femur on the skeleton and its overall height, recording each measurement in the table.

Results

1 In your workbook, construct a table like that shown below for all your results:

	Length of femur (cm)	Actual height (cm)	Calculated height (cm)
Me			
My prac partner			
Skeleton (male)			
Skeleton (female)			

2 Anthropometry uses the following mathematical formulas to predict the height of a person based on the length of their femur:

For males:

predicted height (cm) = femur length × 2.38 + 69.089

For females:

predicted height (cm) = femur length × 2.317 + 61.412

Use these formulas to calculate your predicted height and that of your partner.

3 Assume the skeleton was male. Use its femur length to calculate its likely height.

4 Repeat the calculation, but this time assume the skeleton was female.

Discussion

1 **Compare** your actual height with the height predicted by the formula.

2 **Assess** how accurate the formula was.

3 **Compare** the actual height of the skeleton or poster-skeleton with the predicted heights for males and females.

4 **Use** this information to **identify** the skeleton as male or female.

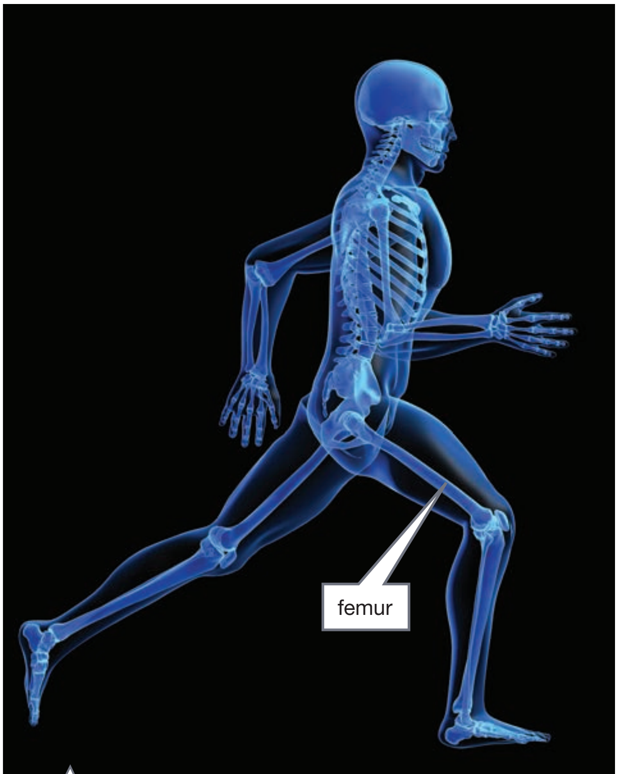


Figure 10.2.18 The femur is sometimes known as the thigh bone. It goes from your hip to your knee.

2 Identikit

Purpose

To construct an Identikit.

Materials

- access to digital camera (tripod optional)
- access to computer and printer
- access to photocopier
- A4 paper
- scissors or Stanley knife
- sticky tape or glue

SAFETY

Be extremely careful with a Stanley knife. Always cut against a hard surface. Retract its blade when not in use.

Procedure

1. Set up a corner in which each person in the class is to have their photo taken. Ensure that:
   - the corner is bright
   - it has a plain background
   - it has a seat
   - the tripod is set 1–2 metres from the seat. If you do not have a tripod, then mark the spot from which the photos are to be taken.
2. Photograph each person in the class. Zoom the lens in or out to ensure that their face (including hair) takes up most of the screen on the digital camera.
3. Print out all the photos in black and white, either individually or in groups of two or four photos per A4 sheet. Photocopy all the photos so that every 4–6 students have a complete set. Cut each photo into sections as shown in Figure 10.2.19. Use features from different people to construct different and imaginary faces.

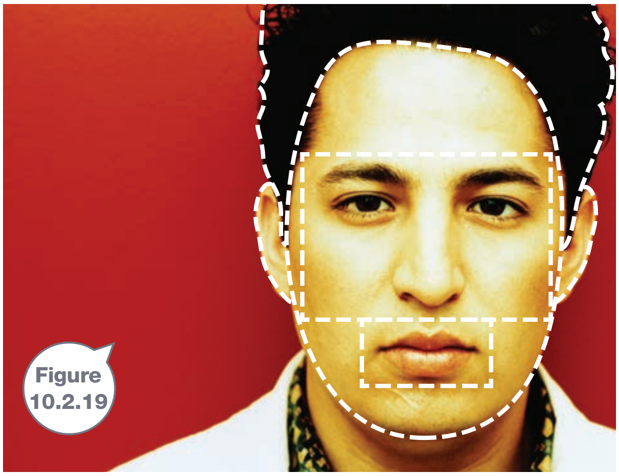


Figure 10.2.19

4. Alternatively, use an appropriate program on your computer to cut, paste and edit parts of different people to form imaginary faces.

Results

When you have a face that 'works', stick it onto a fresh sheet of A4 paper. Alternatively, save and print one of your digital faces.

Discussion

1. **Assess** how realistic the faces were that you constructed.
2. **Assess** whether any of them looks like someone in your school. By coincidence, they often do!
3. **Identify** what other features you would need to construct images of everyone in your school.

3 Gel electrophoresis

Purpose

To use gel electrophoresis to separate dyes.

Materials

- rectangular plastic container (such as a margarine or takeaway food container)
- hard plastic (such as that found in ice-cream containers)
- aluminium foil
- scissors
- power pack
- 2 electric leads with alligator clips
- food dyes (blue, red, green and yellow)
- felt-tip pens (blue, red, green and yellow)
- filter paper
- hotplate or Bunsen burner, tripod, bench mat and gauze mat
- 0.1% sodium hydrogen carbonate buffer solution (0.2 g sodium hydrogen carbonate in 200 mL water)

SAFETY

Tie long hair back.

Turn Bunsen burner flame to yellow or off when not in use.

All chemicals, including sodium hydrogen carbonate should be considered to be toxic.

Gel electrophorsis continued on next page

Gel electrophorsis continued

- 1% agar (1 g agar in 100 mL sodium hydrogen carbonate buffer solution)
- cling wrap

Procedure

1 Cut the plastic container down so that its walls are about 3 cm high.

2 Cut the hard plastic to form a comb that fits across the plastic container with two ‘prongs’ holding it in place. There should be about 6–8 teeth in the comb. Trim the teeth so that they don’t touch the container bottom. It should look like that shown in Figure 10.2.20.

3 Cut off aluminium foil to form two strips about 5 × 8 cm in size.

4 Fold the foil over the ends of the plastic container. The strips should cover the ends and should reach the bottom inside the container.

5 Heat the 1% agar until it boils then let it cool.

6 Meanwhile, prepare samples of food dye or felt-tip pens. To do this, paint or draw 1 cm diameter spots of different colours onto filter paper.

7 Pour agar gel into the plastic container until it reaches a depth of 1 cm.

8 Place the comb across the container, about 2 cm from one end. The agar gel should reach just below the top of the comb’s teeth.

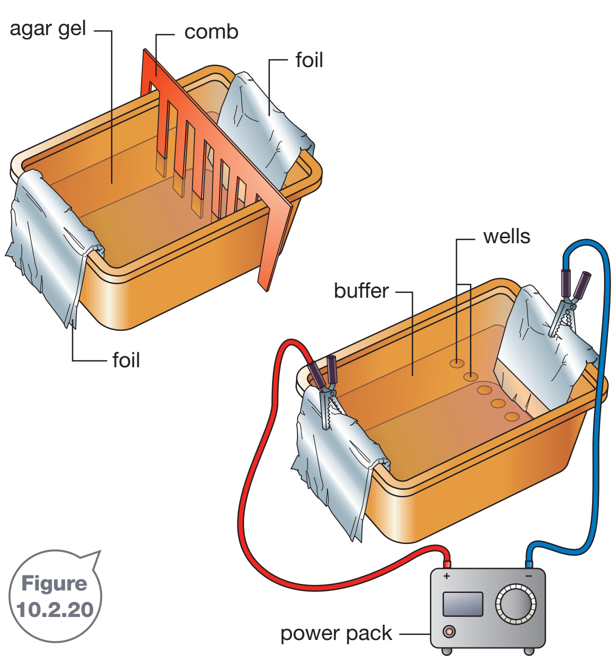


Figure 10.2.20

9 Leave the gel to set. This should take about 15 minutes or it can be covered in plastic cling wrap and left overnight in the refrigerator.

10 When the gel is set, carefully remove the comb.

11 For each of the colours prepared in step 6, cut rectangular strips small enough to fit in the ‘wells’ left behind when the plastic comb was removed.

12 Insert a strip in each of the wells.

13 Carefully pour about 100 mL buffer solution over the gel so that it is completely covered.

14 Connect the aluminium strip to the negative terminal of the power pack and the positive terminal to the other strip. Set the power pack to 4.5 V.

15 Keep the power pack on for about 45 minutes or until colours have obviously separated.

Results

Measure how far each of the colours moved (in mm) down the gel. Record your measurements in a table like that below.

Sample	Distance colour moved (mm)
Blue food dye	
Blue pen	
Red food dye	
Red pen	
Green food dye	
Green pen	
Yellow food dye	
Yellow pen	

Discussion

1 The voltage causes the dye particles to move towards the positive terminal. Small particles move the furthest, while large particles move more slowly. **Use** this information to **list** the samples in order from smallest to largest particles.

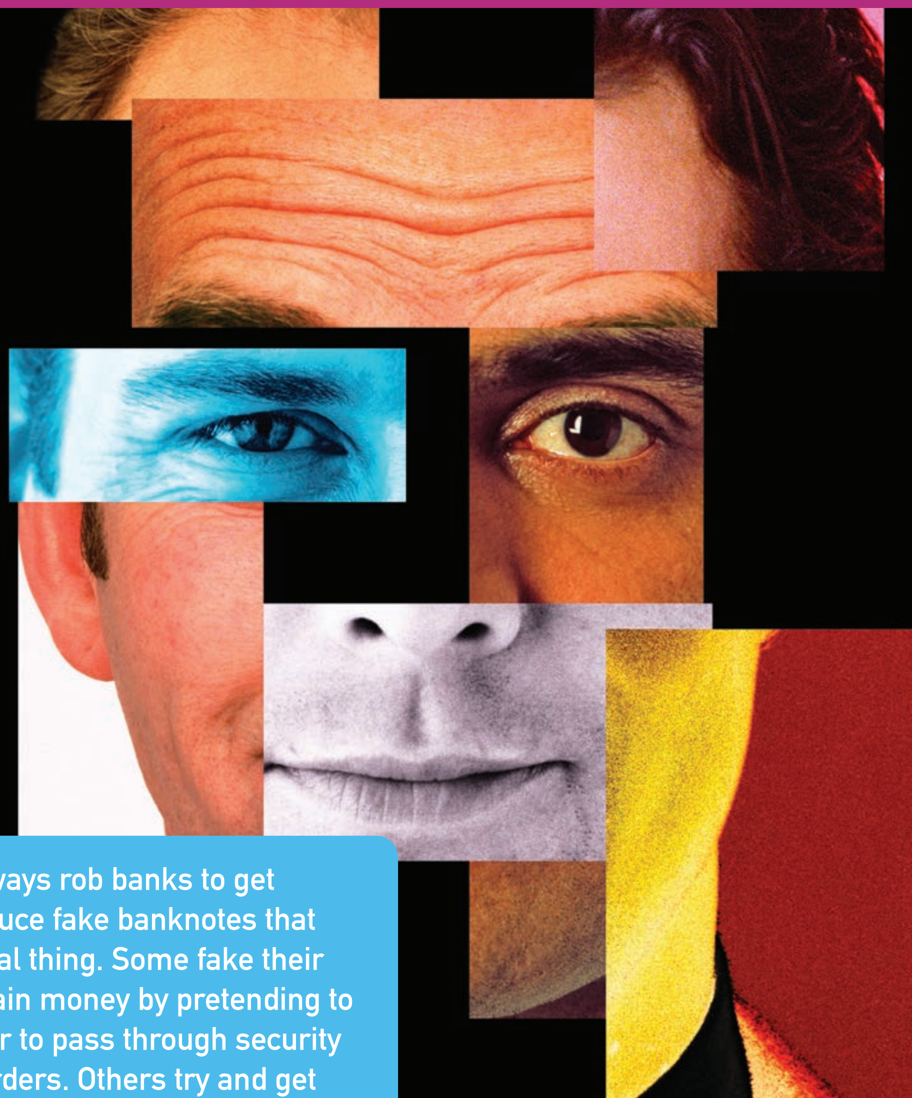
2 **Compare** the size of the particles of the same colour dye and pen (for example, compare the red food dye with the red pen).

3 **Propose** whether the dye particles are charged positive or negative.

4 **Justify** your answer.

5 **Compare** the results obtained here with an autoradiogram like that shown in Figure 10.2.12 on page 340.

10.3 Fakes and extortion



Criminals don't always rob banks to get money. Some produce fake banknotes that can pass for the real thing. Some fake their own identity to obtain money by pretending to be someone else or to pass through security at international borders. Others try and get money by threatening. Forensics provides ways of detecting what and who is fake and who is making threats.

False identities

Knowing the true identity of a person is vital whenever they:

- cross an international border
- claim money from the government (such as Centrelink), institutions (such as banks, insurance companies) or individuals (such as the inheritance from a will)
- gain access to high-security institutions (such as bank vaults, military installations and biochemical laboratories)
- gain access to sensitive files (such as those held by hospitals, state and federal police, espionage (spy) organisations such as ASIO or ASIS).

Identity fraud is when someone pretends to be someone else. It costs Australia billions of dollars each year and so increasingly complex methods are being used to stop it.

Documents proving identity

Passports, driver's licences and credit cards are easy ways of proving your identity. All these documents have features to ensure they are secure and cannot be used by anyone but their 'owners':

- Passports once had photos pasted into them but this proved too easy to change or replace. Modern passports (and driver's licences) contain scanned images that are difficult to alter.
- Passports now have an electronic chip in their centre page that contains the name, sex, nationality, date of birth and a digital version of the passport-holder's photograph. This chip is activated when scanned and its details can be checked against the passport's front page. These 'chipped' passports are known as **ePassports** and Australia was one of the first countries in the world to introduce them. The 'chip' symbol in Figure 10.3.1 on page 348 indicates that the document is an ePassport.

- Modern credit and identity cards usually include features such as holograms (like the ones in Figure 10.3.2) that make them difficult to reproduce. Credit cards also include magnetic strips and chips that contain the customer's details and a personal identification number (PIN). Signatures are easily forged while only the true owner of the card should know its PIN.

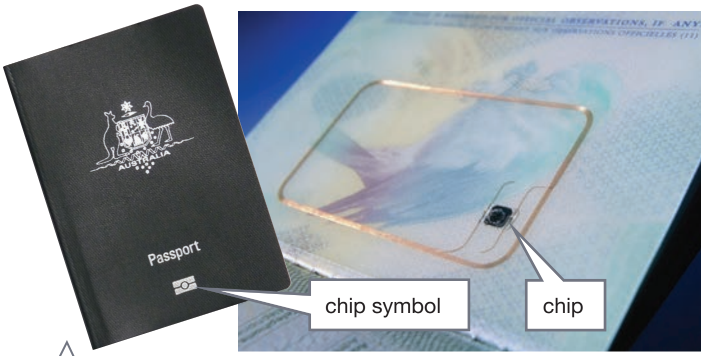


Figure 10.3.1 ePassports carry a chip that contains all your information and a digital version of your photo.

Mission very possible!

In 2009, two well-dressed men entered an expensive jewellery store in London (UK) and left with £40 million ($78 million) of watches, rings, bracelets and necklaces. Although their images were recorded by CCTV cameras, it is thought that they were wearing rubber masks like those used in *Mission: Impossible*!

SciFile

Figure 10.3.2 Credit cards and identity cards commonly have holograms that make them more difficult to fake.

Biometric facial recognition

Most people identify you by your face. Biometric facial recognition software allows a computer to do this too. It measures the position of your facial features and compares them with those of photographs on file. International airports around Australia and many airports overseas have special self-service gates (**Smartgates**) that photograph travellers and identify them with the digital photo on the chip in their ePassports. You can see a Smartgate in Figure 10.3.3.

Figure 10.3.3 Smartgates scan your face and use biometric recognition software to match it with the image in your ePassport.

Want chips with that?

In 2004, microchips were implanted under the skin of important lawmakers in Mexico that give them (and only them) access to computer files containing sensitive information on criminal activity. Some European nightclubs now give VIP access and service to members who are implanted with microchips containing their personal details.

SciFile

Fingerprint scans

Most countries have increased their border security since the terrorist attacks of 11 September 2001 (commonly known as '9/11'). For example, all visitors entering and leaving the USA via its international airports have their fingerprints scanned. These are then checked against files of known terrorists. Also, scanned fingerprints and whole handprints are also increasingly being used to sign in and out of work and as a 'key' to access computers, secure facilities or bank accounts (Figure 10.3.4). Access is only gained if the match is positive.

Figure 10.3.4 Fingerprint scanners are now used in some shops and banks overseas to match prints with customers' banking details. Money is then directly debited from their account.

Iris and retina identification

The **iris** is the coloured ring of muscle in the eye that controls the size of the pupil. As Figure 10.3.5 shows, its patterns and colouring are incredibly complex. Each person has unique iris patterns and each eye has a different pattern. For these reasons, the iris provides a far better method of identification than a fingerprint. It is also impossible to fake—the iris contains 266 identifiable features and constantly moves, whereas a fake eye remains static.

The **retina** is at the rear of the eye and its pattern of blood vessels is even better than the iris as proof of identity. Although more difficult to obtain, retina scans are more accurate than iris scans.

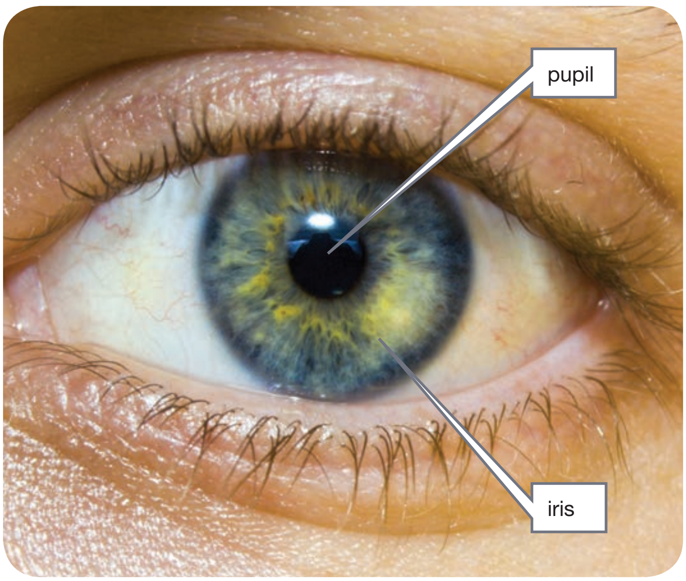


Figure 10.3.5 The iris gives the eye its colour. It has 266 identifiable features and it does not change with age. This makes it an accurate way of identifying someone.

Forgery

Counterfeit (fake) banknotes are relatively rare because real notes include special features that make them difficult to reproduce. Some of these features are shown in Figure 10.3.6 on page 350.

Australia was the first to use **polymer film** (plastic) notes. They are harder to counterfeit and last four or five times longer than paper ones—while a paper \$5 note had an average life of about 6 months, a plastic one lasts more than 3 years.

Organised crime groups are usually the only ones with sufficient money to purchase the technology, materials and skills needed to produce realistic counterfeit banknotes.

Realistic counterfeit banknotes are difficult to detect by shop assistants and bank tellers unless they know what to look for. It might be the feel of the paper used, its colours or its serial number. (Real banknotes all carry different serial numbers, whereas counterfeits usually have the same serial number.) Unfortunately, these differences may only become apparent after many fake notes have already been passed off as real.

SciFile

Obviously fake!

The USA has never had a \$1 million banknote. However, this did not stop Alexander D. Smith from trying to pass this fake one as a real note in 2007!

INQUIRY science 4 fun

Inspecting banknotes

Can you find the anticounterfeit features on a banknote?

Yes

Collect this …

- banknote (it doesn't need to be Australian)
- magnifying glass or stereomicroscope
- ultraviolet (UV) light (optional)

Do this …

1. Carefully inspect the banknote. Take note of the features shown in Figure 10.3.6 on page 350.
2. Use the magnifying glass or stereomicroscope to find microprinting and the UV light for fluorescing inks.

Record this …

Describe what you found.

Explain how these features stop counterfeiting.

SciFile

Drug money

In many large cities in the USA, up to 93% of the banknotes have been found to have traces of the illegal drug cocaine on them. Perhaps in the future, fake US banknotes will be detected because they have no traces of cocaine!

Intaglio printing
A raised form of printing that can be felt with your fingers

Australian banknotes have their portraits, denomination number and the word *Australia* in intaglio printing.

Material
Paper banknotes are printed on special paper with its own characteristic feel.

Australian banknotes are printed on polymer film (plastic). They last longer than paper notes and are harder to counterfeit.

Optically active devices
Images that are holographic (producing multicolour effects) or clear

All Australian banknotes have an image of a seven-pointed star that is only complete when held up to the light.

Figure 10.3.6 One side of an Australian $10 note, highlighting the features that make it near-impossible to counterfeit.

Australian banknotes use a second optical device. The $10 note has a windmill while the $50 note has a lyrebird.

Microprinting
Very small printed details such as sentences and initials that cannot be reproduced by a colour printer or photocopier. A magnifying glass is needed to read it.

The $10 note has the poem 'The Man from Snowy River' on its front. The Australian $5 note has an early version of 'Advance Australia Fair' on its back.

Not shown
Metal band: This is often inside the layer of the paper and can be felt and seen under backlighting.
Water mark: Hidden images in paper notes that are only seen when the note is held up to the light. The $50 note has the Australian coat of arms.
Serial numbers: Prominent letters and/or numbers on one or both sides of the note. Each number is different. Counterfeit notes often all have the same serial number. The $10 note has two serial numbers on one side, each in a different font.
Fluorescing inks: These inks glow under ultraviolet light. Parts of the serial number of the $10 note fluoresce (glow).

Fake documents and extortion

Criminals sometimes use fake signatures and documents to gain access to inheritances and insurance policies and to commit business fraud. They sometimes also use **extortion** (threats and blackmail) to get what they want. Forensics can help to determine:

- if a signature or document is real
- who wrote a threatening letter or email or who posted offending material on the internet.

Handwriting

Everyone's handwriting has characteristic features that can be used to identify who wrote or signed a document. Some of these features are shown in Figure 10.3.7.

INQUIRY science 4 fun

Fake signatures

Can you fake someone's signature?

Yes

Collect this ...

- pen
- paper (preferably lined)

Do this ...

1. Write your signature on a piece of paper.
2. Swap signatures with another classmate and then try and reproduce their signature.
3. Take particular notice of the features shown in Figures 10.3.7 and 10.3.8.

Record this ...

Describe what happened.
Explain why you think signatures are difficult to forge.

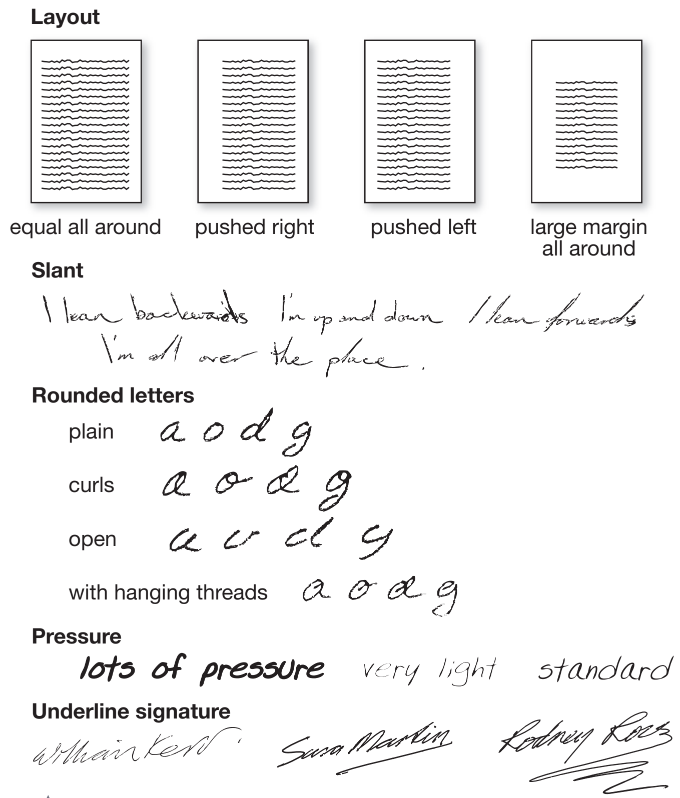


Figure 10.3.7 Handwriting changes with a person's age, but its basic features do not.

You can alter your handwriting but the way you construct each letter tends to remain the same. For example, Figure 10.3.8 shows different ways to construct the letter E.

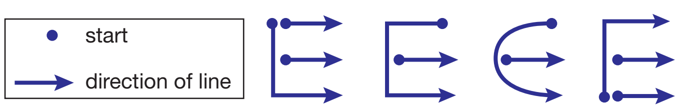


Figure 10.3.8 How do you construct the letter E?

Papers and inks

Papers differ in their texture, absorbencies, the presence of watermarks and weight (often referred to as grams per square metre or GSM). All these characteristics affect the way an ink spreads and is absorbed and the way each individual letter appears.

Inks differ too. For example, different black inks contain different combinations of colours: some black inks contain blue while others have brown in them. **Chromatography** uses a solvent such as water or alcohol to dissolve and separate an ink into its component pigments. This is what has happened in Figure 10.3.9. In this way, the ink used to forge a signature or letter or to write or print a threat can be matched with a suspect's pen or printer.

1 p353 2 p353 3 p354 10.6

Electronic documents

Everything you do on a computer is recorded on your computer hard drive in **binary code**, using the numbers 0 and 1. When you delete a file, all you delete is the way you access it. The original coding and information is still there. This means that every document, email, Twitter or Facebook entry will still be there, to be retrieved if and when needed by forensics investigators.

SciFile

Blackbox

The operation of most modern cars is controlled by computers, which also store information such as the car's speed, braking pressure and steering. All this information can be downloaded after an accident and might soon be used by police to charge drivers and allow insurance companies to reject insurance claims.

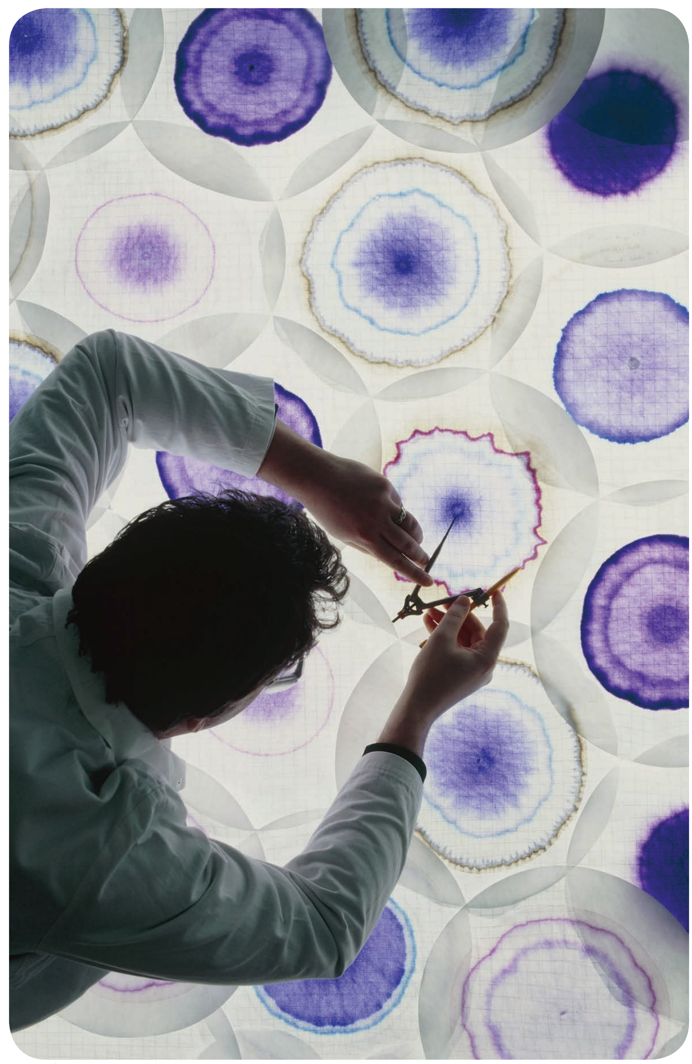


Figure 10.3.9 Chromatography separates pigments and dyes and produces strips or rings of colours. Here a forensic scientist is investigating the pigments used to make up different brands of black ink.

10.3 Unit review

Remembering

1 People fake their identity for many reasons. **List** reasons that are connected to:
- **a** money
- **b** security
- **c** information.

2 **State** where these are in the eye.
- **a** the iris
- **b** the retina

3 **State** how many features can be identified in an iris.

4 **Recall** the features used in Australian banknotes by matching the following features with their descriptions.

a intaglio	**i** holograms and windows
b fluoresce	**ii** tiny printed text
c micropринting	**iii** raised text
d optically active devices	**iv** glow

5 **List** features that might alert someone that a banknote is fake.

6 **Name** the process by which the ink of a pen is separated.

Understanding

7 **Explain** the advantages of ePassports over 'normal' passports.

8 **Explain** why microchips are inserted under the skin of:
- **a** Mexican lawmakers
- **b** some nightclub patrons.

9 Old-style driver's licences were slips of paper with no photo. **Predict** some of the problems this caused.

Applying

10 **Identify** the pen used to write a threatening letter from the results shown in Figure 10.3.10 of a chromatography experiment. Note that each strip was left in the solvent for a different time.

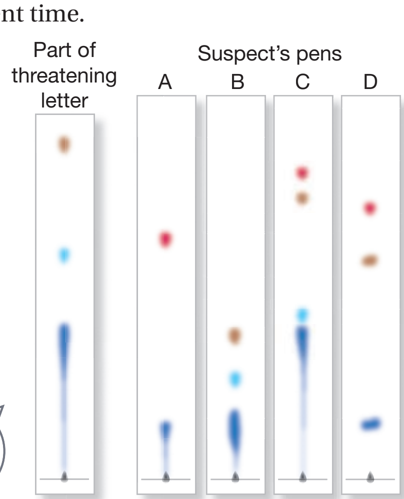


Figure 10.3.10

Analysing

11 **Compare** iris and retina identification with fingerprinting.

12 Write each letter of the alphabet in capitals, and **analyse** how you constructed them. Add arrows, similar to Figure 10.3.8 on page 351, showing how each letter was constructed.

Evaluating

13 Many cats and dogs have microchips inserted under their skin and a tattoo in their ear. **Propose** reasons why.

14 Imagine a future where everyone has microchips inserted under their skin at birth.
- **a** **List** as many advantages as you can think of.
- **b** **List** as many disadvantages as you can think of.
- **c** Based on your lists, **assess** whether implanting everyone with microchips is a good idea or not.
- **d** **Justify** your choice.

Creating

15 **Construct** a simple sentence and write it in four very different handwriting styles.

Inquiring

1 Research what Note Printing Australia (NPA) is and where it is located.

2 Research which other countries use polymer or plastic banknotes.

3 Investigate the so-called 'Hitler Diaries' and explain how they were eventually found to be fake.

4 Search the internet for videos showing chromatography separating dyes.

5 Use the key term *fake bank notes* to research a group of criminals that was printing counterfeit notes. Find:
- the country the criminals were operating in
- when they were operating
- how much fake money is thought to have been passed as real
- how the fakes were discovered.

10.3 Practical activities

1 Chromatography

Purpose

To use chromatography to determine which pen wrote a threatening letter.

Materials

- at least three different coloured biros or felt-tipped pens
- pencil
- 250 mL or larger beaker
- filter paper strips
- methylated spirits
- icy-pole stick
- paperclips

SAFETY

Methylated spirits is flammable so keep it away from naked flames or sparks.

Procedure

1. On one end of a filter strip, write in pencil the brand name or colour of a pen you are about to test.
2. Use a pen to draw a large dot about 1.5 cm from the other end of the filter strip.
3. Repeat with the other pens and colours, using a separate piece of filter paper for each.
4. Add about 1 cm of methylated spirits to the beaker.
5. Attach the filter strips to the icy-pole stick with paperclips and arrange as shown in Figure 10.3.11.
6. Leave the strips to soak up the methylated spirits for 20–30 minutes.
7. Unclip the strips and allow to them to dry.

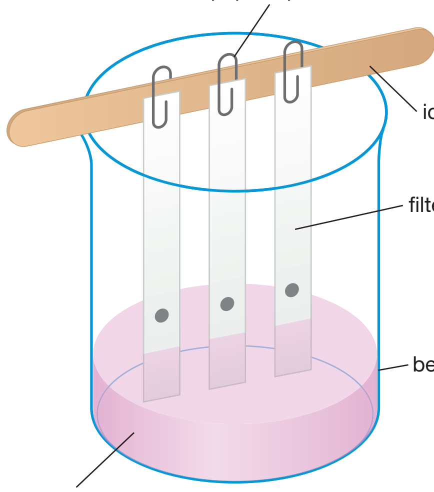


Figure 10.3.11

Results

List the colours that are mixed together to make up each ink.

Discussion

1. **Describe** what the methylated spirits did to the inks.
2. If you had two pens of the same colour but different brands, **compare** the colours that made up each ink.
3. **Explain** how chromatography could be used to determine who wrote a threatening letter.

2 Smartie colours

Purpose

To design a way of separating the different food dyes present in the coloured shells of Smarties®.

Materials

- Smarties of different colours
- materials as chosen by students

Procedure

The food dyes used in Smarties tend to 'run' when they get wet. Use this information to design a way of separating the colours present in the coloured candy shells of Smarties. Once you have written your procedure, have your teacher check it before attempting your experiment.

Results

1. Construct a diagram showing your experimental set-up.
2. Construct diagrams showing your results.

Discussion

List the colours used to form the different food dyes that colour the candy shells of Smarties.

3 Reading a burnt note

Purpose
To retrieve messages written on a note that has been burnt.

Materials
- ballpoint pen (not a felt pen)
- sheet of paper
- sheet of greaseproof paper
- bench mat or metal tray
- long barbecue matches
- spray bottle containing a mix of 1:3 parts glycerine and water

SAFETY
Do not spray the mixture near people.

Procedure
1. Use the ballpoint pen to write a long message or a list of words on the paper.
2. Lightly scrunch up the note. Don't scrunch it too much or too tightly.
3. Place the scrunched paper on the bench mat or in the metal tray.
4. Set fire to the paper and allow it to burn. *Do not* blow on the paper. It doesn't matter if the flame goes out.
5. When the flame has died out, *carefully* transfer the burnt paper onto the greaseproof paper. Try not to disturb the ashes.
6. Gently spray the burnt paper with the glycerine/water mix until it is wet.
7. Carefully smooth the paper back and look for your writing.
8. Repeat the experiment but try different colours and makes of pens.

Results
On another clean sheet of paper, write down what you can see on the burnt note.

Discussion
1. The ink in ballpoint pens contains dyes, some metal and solvents that evaporate, allowing the ink to dry. **Use** this information to **identify** what is probably left behind on the note.
2. **Propose** a reason for the glycerine/water mix.
3. **List** the problems in this experiment that could make it impossible to read the message on the note after burning.
4. **Explain** how this method could be used to prove that a criminal has been practising forged signatures.
5. **Create** a scenario (story) in which a criminal might be writing notes and then destroying them.

Chapter review 10

Remembering

1 **Name** a major event that caused border security to be increased in many countries.

2 Australia uses plastic instead of paper for its banknotes. **State** two reasons why.

3 **List** the information included in the chip in an ePassport.

Understanding

4 **Define** the terms:
- a homicide
- b arson
- c ballistics
- d corpse
- e anthropometry
- f assassination
- g counterfeit
- h fluoresce.

5 Nothing is moved from a crime scene until it is marked and photographed. **Explain** why.

6 **Explain** why DNA is considered to be the 'ultimate' fingerprint.

7 **Explain** what retroactive interference is and how it can make identification unreliable.

8 **Describe** what happens when you delete something from your computer.

Applying

9 **Identify** places around your house where investigators would be likely to find large quantities of your DNA.

10 **Calculate** roughly how long a body has been dead for if its temperature is:
- a 35°C
- b 29°C
- c 17°C.

Analysing

11 **Contrast** physical evidence with trace evidence.

12 **Classify** the fingerprints in Figure 10.4.1 as arch, loop, whorl or composite.

Evaluating

13 A body has been found a long way from water. An autopsy showed that the person had drowned.
- a **Propose** what evidence would have been found to show that the person had drowned.
- b **Propose** a way investigators could find out where the person drowned.

14 A male body is found in the bush. There is a band tattooed around his right arm and a large dark birthmark down the right side of his face. He is wearing a leather jacket and his driver's licence is in its pocket. X-rays show that he has pins in his left ankle and fillings in his back teeth. **Assess** each of these pieces of evidence and **rank** them from most useful to least useful for identifying the body.

15 Ricin could be considered to be the 'ideal' poison for an assassin. **Propose** a reason why.

16 **Propose** what information managers might look for in a chip under the skin of patrons coming into their nightclubs.

17 Imagine a scheme in which everyone in Australia had their DNA taken and their DNA autoradiograms stored on government databases or on identity cards.
- a **Propose** a list of advantages and disadvantages of such a scheme.
- b **Assess** whether or not you would support a scheme like this.

Creating

18 **Use** the following ten key terms to **construct** a visual summary of the information presented in this chapter.

crime scene
physical evidence
trace evidence
corpse
diatoms
DNA
fibres
victim
suspect
drowning

10.7

Figure 10.4.1

a 
b 
c 
d 

Thinking scientifically

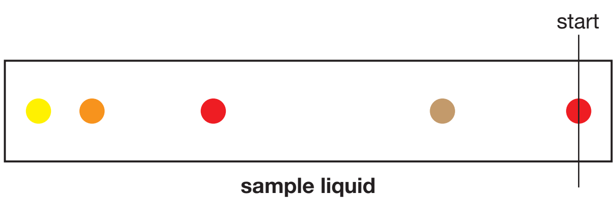
Q1 In a laboratory, forensic scientists are attempting to reproduce the wounds of a stabbing attack. To do this they use a kitchen knife to quickly stab a piece of beef bought from the butcher. Which is the most likely result from this experiment?

A A flattening of the tissues
B A shallow cut across the tissues
C A deep, rectangular hole
D A deep, circular hole

Q2 A corpse is found face up in a multistorey carpark in the inner city. In the autopsy, evidence is found that indicates that the corpse was murdered elsewhere. Which of the following pieces of evidence does *not* indicate this?

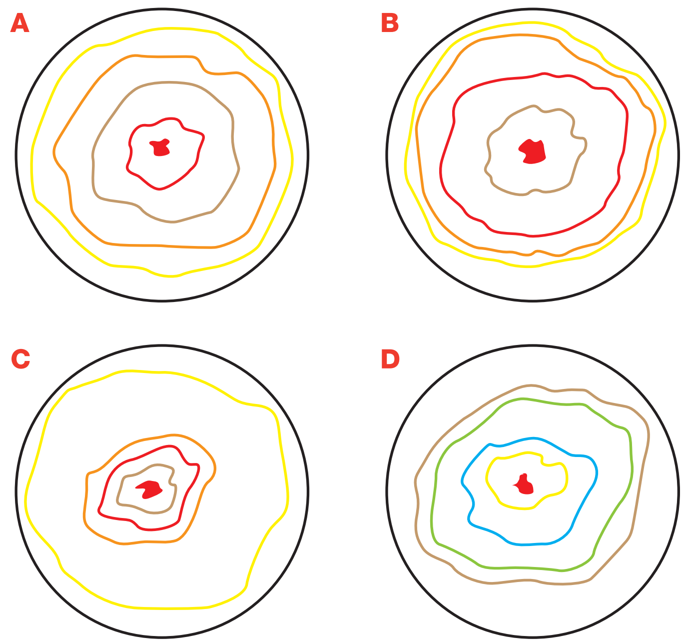
A Diatoms are found in the lungs of the corpse.
B DNA from someone else was found on the clothing of the corpse.
C Fresh pollen from dandelion flowers is found throughout the clothing of the corpse.
D Blood has pooled (collected) across the belly and chest of the corpse.

Q3 A splash of red liquid has been found on clothing belonging to the main suspect of a murder. Chromatography was used to separate the colours that made up the splash. It produced a strip of filter paper as shown below.



At the murder scene was a pool of spilt red drink. Chromatography was used to test this sample and other samples of red drinks (samples A, B, C, D). Samples of the different drinks were placed in the centre of a circle of filter paper.

Identify which sample matched the liquid found on the suspect.



The following information applies to questions 4–6. Various samples of DNA were found at a crime scene. A part of their DNA autoradiograms are shown below.

Q4 Identify which DNA autoradiogram A–D came from the victim.

Q5 Identify the person A–D who had never been at the crime scene.

Q6 Identify the suspect(s) in the case.

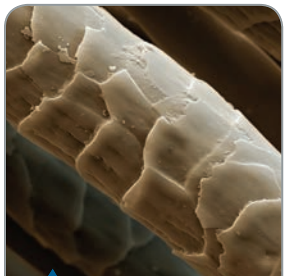
Glossary

Unit 10.1

Arson: deliberate lighting of a fire

Ballistics: the study of guns and ammunition

Circumstantial evidence: evidence that points to a suspect but doesn't prove they are guilty



Fibres

Core body temperature: 37°C for a healthy human

Corpse: dead body

Crime scene unit (CSU): specialists who collect and bag evidence

DNA: deoxyribonucleic acid

Fibres: strands of material such as hair, wool or polyester

Fingerprints: patterns of ridges and grooves on the fingers and toes

Homicide: murder or manslaughter of another human

Impressions: track marks

Impressions

Negative impression: an impression formed by material gathering in recesses, such as the grooves in a tyre or shoe

Non-porous: doesn't absorb liquids such as body oils

Pathology: the study of disease and cause of death

Physical evidence: large pieces of evidence

Porous: absorbs body oils

Positive impression: an exact image, such as the pattern of a shoe or a tyre

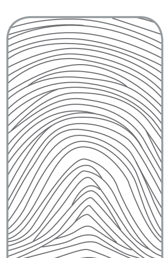
Tool mark: characteristic mark left by a tool

Toxicology: the study of the effects of poisons and chemicals on the body

Trace evidence: microscopic evidence such as fibres or DNA

Unit 10.2

Alpha rays: form of nuclear radiation



Arches

Anthropometry: study of body size and proportions

Arches: a form of fingerprint in the shape of arches

Assassination: political murder

Autopsy: dissection of a body to determine cause of death

Autoradiogram: identifying pattern that represents DNA patterning

Bertillon system: a form of anthropometry in which body size and proportions are measured

Biometric facial recognition: when a face is scanned and computer-matched with stored images of faces

Identikit

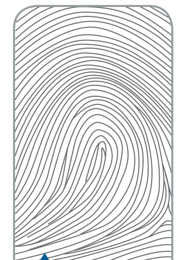
CCTV: closed circuit TV

Composite: a form of fingerprint

Diatoms: microscopic organisms found in water, each with a different shape

Dioxins: a form of poison

Gel electrophoresis: a process in which DNA is cut then analysed to produce an autoradiogram



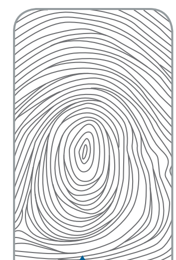
Loops

Identikit: form of identification in which facial features are slotted together

Loops: a form of fingerprint in the shape of loops

Polonium-210: radioactive material, used once as a poison

Retroactive interference: changes in the memory of an eyewitness after looking at other images



Whorls

Ricin: a form of poison

Whorls: a form of fingerprint in the shape of whorls

Unit 10.3

Binary code: the way a computer stores information: 0 and 1

Fluoresce

Chromatography: the use of solvents to separate colours of ink and other materials

Counterfeit: fake (usually refers to a banknote)

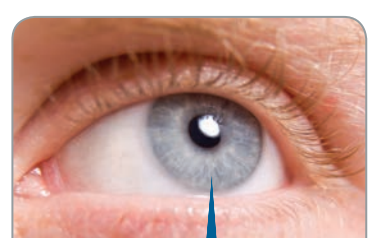
ePassport: a passport that includes a chip recording personal information

Extortion: threats and blackmail

Fluoresce: shining due to special light (e.g. UV)

Identity fraud: pretending to be someone else

Intaglio: raised printing



Iris

Iris: coloured ring of muscle in the eye that controls the size of the pupil

Polymer film: plastic used to make banknotes

Retina: back of the eye

Smartgate: gate that electronically reads ePassports