

Technique	Forensic Techniques (e.g. DNA, Finger Printing)	Surveillance Techniques (Covert Human/ CCTV)
Explain/Describe the technique	Forensic investigators use a range of physical and biological techniques to collect evidence, including fingerprint analysis, trace evidence, fibres and threads, ballistics, and footwear impressions. These methods help reconstruct events and link individuals to crime scenes. One of the most effective techniques is DNA profiling, which identifies individuals by analysing their unique genetic code. DNA can be extracted from biological material such as blood, saliva, semen, hair, or skin cells, then compared to suspects, victims, or database records. Since each person's DNA is unique (except for identical twins), it is a highly reliable tool in forensic identification.	Surveillance is a key investigative technique used to monitor individuals, groups, or locations in order to prevent crime, gather intelligence, and support prosecutions. It can be carried out overtly or covertly. Overt surveillance is visible and obvious, such as CCTV in public areas, Automatic Number Plate Recognition (ANPR), police body-worn cameras, and drones monitoring large events. Covert surveillance is hidden and carried out without the subject's knowledge, including undercover officers infiltrating groups, covert human intelligence sources (CHIS), phone tapping, vehicle tracking, and listening devices. CCTV is the most widely used overt method in the UK, acting as both a deterrent and a source of visual evidence for prosecutions.
Types of Crime Where it Has Proved Useful (inc. violent crime, e crime and property crime)	DNA profiling has been invaluable in investigating serious crimes such as rape, sexual assault, and murder, where biological material is often left behind. It has also been used in burglary cases, where suspects may cut themselves or leave saliva or hair at the scene. Cold cases have particularly benefited from advances in DNA technology, as archived samples can be re-tested with modern, more sensitive methods to provide new leads or confirm earlier suspicions.	Surveillance has been particularly valuable in violent crime, such as assaults, murders, and terrorism, where CCTV footage and covert monitoring provide direct links to offenders. It is also effective in property crime, for example tracking burglars or stolen vehicles through ANPR and CCTV. In e-crime, surveillance of online activity and digital communications has been used to track cyber fraud, hacking, and terrorist networks, often through covert interception.
Situations it is most useful in and strengths: <i>Crime Scene, Laboratory, Police Station, Street?</i>	DNA profiling is most useful when samples are carefully collected from crime scenes and processed in controlled laboratory environments. Its strengths lie in its accuracy, reliability, and ability to exclude innocent suspects as well as identify perpetrators. Only a tiny biological sample is required, meaning even decades-old or degraded evidence can sometimes yield results. The technique can also confirm links between multiple crimes, identify unknown victims, or exonerate individuals who have been wrongly convicted.	Surveillance is most effective in public and high-risk areas. At a crime scene, CCTV may capture suspects entering or leaving. In the laboratory, footage and intercepted communications can be analysed forensically. In the police station, databases linked to ANPR and CCTV help officers build profiles of suspects. On the street, both overt and covert surveillance provide real-time monitoring of suspects. Its main strengths are deterrence, continuous coverage, the ability to track suspects across locations, and the provision of strong visual or audio evidence that can be persuasive in court.
Situations it is NOT useful in and limitations: <i>On a busy street. Where evidence is likely to be disturbed/ contaminated.</i>	Despite its strengths, DNA evidence has limitations. On busy streets or public areas, samples can be easily contaminated, transferred, or mixed with unrelated DNA. Low-quality or partial profiles may produce misleading matches, especially in large databases. In the laboratory, errors in handling or interpretation can compromise results. DNA analysis is also expensive, requires specialist expertise, and can take time, which limits its usefulness in fast-moving investigations. It is less relevant for cybercrime, where biological traces are unlikely to be present.	Surveillance has limitations. It is less useful in locations with blind spots or no camera coverage, or where images are of poor quality due to bad lighting, weather, or low resolution. Covert surveillance, such as phone tapping and vehicle tracking, requires strict legal authorisation under the Regulation of Investigatory Powers Act (RIPA), making it resource-intensive. Offenders can disguise themselves or avoid cameras, reducing effectiveness. In cybercrime, physical surveillance provides little benefit since offences often occur entirely online. There are also concerns over privacy, bias, and the potential misuse of surveillance technologies such as facial recognition.
Case Studies: Case studies where the techniques have been effective (or ineffective)	The power of DNA profiling was first demonstrated in the case of Colin Pitchfork (1987) , who became the first person convicted of murder through DNA evidence after samples linked him to two teenage girls' deaths in Leicestershire. However, DNA has also highlighted the risks of misinterpretation: However, the David Butler case (2005) revealed the dangers of relying on partial or low-quality DNA samples. Butler, a man with epilepsy and learning difficulties, was accused of murder after a partial DNA profile was found on a glove at the crime scene. Despite the weak and incomplete match, this became a central piece of evidence against him. Butler endured months in prison and a lengthy legal battle before he was cleared when it was shown that the DNA evidence was unreliable and could not safely implicate him. This case highlights the risk of wrongful accusations when DNA profiling is applied uncritically, showing that while the science is powerful, it must be interpreted with caution and in context.	Surveillance has played a central role in major cases. In the 7/7 London Bombings (2005), CCTV was essential in tracking the bombers' movements before and after the attacks, providing vital evidence for the investigation. More recently, the South Wales Police facial recognition trials highlighted both the potential and the risks of surveillance technology. While the system identified suspects, it also produced false positives, raising ethical and accuracy concerns. These examples show how powerful surveillance can be, but also why it must be used carefully and supported by other evidence.

Technique	Interview Techniques (Eyewitness/Experts)	Profiling Techniques
Explain/Describe the technique. <i>How is it executed?</i>	<p>Eyewitness Testimony (EWT) is evidence provided by people who directly observed a crime. Because memory is malleable, it is vulnerable to distortion from stress, bias, or poor questioning. Psychologists such as Elizabeth Loftus have shown that memory is reconstructive and can be influenced by wording or external information. To address these weaknesses, the Cognitive Interview (CI) was developed. This uses techniques such as reinstating the context (asking witnesses to recall what they saw, heard, or felt at the time), recalling events in different orders, and reporting from multiple perspectives. These methods aim to improve recall and reduce false or incomplete memories. Expert witnesses may also appear in court to interpret forensic evidence, explain psychological concepts such as false memory, or challenge unreliable testimony.</p>	<p>Offender profiling seeks to predict an offender's background, personality, and behaviour by analysing crime scene evidence. It is designed to narrow down suspects and guide police investigations when physical evidence is lacking. There are three main approaches:</p> <ol style="list-style-type: none"> 1. Top-down (typological profiling) – developed by the FBI, this categorises offenders as “organised” (planned crimes, careful crime scene management) or “disorganised” (chaotic, opportunistic behaviour). 2. Bottom-up (investigative psychology) – pioneered by David Canter in the UK, this relies on statistical analysis of crime scene data, patterns, and offender behaviour to build a picture. 3. Geographical profiling – developed by Kim Rossmo, this focuses on the spatial patterns of crimes to identify an offender's likely “base” or area of operation.
Types of Crime Where it Has Proved Useful (inc. violent crime, e crime and property crime)	<p>EWT is particularly useful in violent crime (e.g., assaults, robberies, and homicides) where witnesses are often present but physical evidence may be limited. It also plays a role in property crimes, such as burglaries or car thefts, where multiple witnesses may have seen offenders or suspicious activity. It is less directly useful in e-crimes, since these occur online without physical witnesses, though experts may still testify about digital methods or explain specialist forensic results to juries</p>	<p>Profiling is particularly effective in violent crimes such as serial murders, sexual assaults, and stalking, where offenders often display distinctive behavioural patterns. It is less useful in property crimes, such as opportunistic burglaries or thefts, which lack consistency, and in e-crimes, where offending takes place online without geographical or behavioural traces to analyse.</p>
Situations it is most useful in and strengths: <i>Crime Scene, Laboratory, Police Station, Street etc.?</i>	<p>EWT is valuable at different stages of the investigative process. At the crime scene or street, initial eyewitness accounts can provide immediate leads, such as suspect descriptions or vehicle details. In the police station, the Cognitive Interview helps extract more accurate memories and reduces the chance of contamination through poor questioning. In the courtroom, testimony provides a compelling narrative of events, which can be persuasive for juries and complement forensic or surveillance evidence. Its main strengths are that it sometimes provides the only available evidence, can be collected quickly, identifies suspects early, and when corroborated with other evidence, strongly supports a conviction</p>	<p>At the crime scene, profiling can highlight behavioural clues such as evidence of planning, choice of victim, or level of control used. In the police station, profiles help narrow suspect lists, link multiple offences, and allocate investigative resources more effectively. In terms of street-level policing, geographical profiling can predict where an offender is likely to operate next, helping to focus patrols. Profiling's main strengths are its ability to identify behavioural links between cases, highlight patterns that might otherwise be overlooked, and generate strong leads when combined with physical forensic evidence.</p>
Situations it is NOT useful in and limitations: <i>Contamination of evidence/inaccuracy of presentation of facts in court?</i>	<p>Despite its importance, EWT has major limitations. At the crime scene, witnesses under stress, fear, or trauma may misperceive or misremember events. In the police station, questioning techniques such as leading questions or suggestive language can distort memory. In court, juries may rely heavily on confident testimony, even though research shows confidence does not always match accuracy. More generally, eyewitnesses are vulnerable to cross-race bias, weapon-focus effect (attention drawn to a weapon rather than the offender's face), and post-event information from the media or other witnesses. Expert witnesses, while useful, can sometimes present flawed or exaggerated evidence, which risks misleading juries.</p>	<p>Profiling has limits. It is rarely useful in one-off or opportunistic crimes such as burglary or car theft, as there is little behavioural evidence to work with. It is ineffective in e-crime, where online activity leaves no physical crime scene. Profiling is also probabilistic, not definitive, meaning it suggests possibilities rather than certainties. Over-reliance can mislead investigations if assumptions are wrong. It requires skilled experts, large datasets, and detailed crime scene evidence to be reliable. In some cases, inaccurate profiling has led to wrongful accusations.</p>
Case Studies: Useful in/ not useful in	<p>Anthony Broadwater & Alice Sebold (1981) – Author Alice Sebold misidentified Anthony Broadwater as her attacker after a rape when she was a student. Although she failed to pick him in a police lineup, she later identified him in court, where he was the only Black man present. Combined with discredited hair analysis, this led to his wrongful conviction and 16 years in prison. He was exonerated in 2021 after a review found the evidence unreliable, highlighting how EWT can be distorted and contribute to serious miscarriages of justice. Ronald Cotton (1984) – Cotton was wrongly convicted of rape after the victim, Jennifer Thompson, confidently misidentified him in both a lineup and in court. Despite her certainty, DNA testing years later proved his innocence and identified the real perpetrator. Cotton spent over a decade in prison, showing how persuasive but inaccurate eyewitness testimony can be, and why forensic confirmation is vital before relying on EWT.</p>	<p>John Duffy (Railway Rapist, 1980s) – Psychologist David Canter used a bottom-up profiling approach to analyse crime scene behaviour and geography, correctly predicting Duffy's location, railway knowledge, and marital problems. His arrest showed how profiling can narrow suspect pools and provide valuable investigative leads. Colin Stagg (Rachel Nickell case, 1992) – Stagg was wrongly accused after police relied heavily on a psychological profile and a flawed undercover operation, despite no forensic evidence linking him to the murder. He was later cleared when DNA identified the real killer, Robert Napper, highlighting the dangers of over-reliance on profiling. Jack the Ripper (1888) – One of the earliest uses of profiling, with Dr. Thomas Bond suggesting the killer was a solitary man with possible anatomical knowledge. However, the vague profile did little to help investigations, showing the limitations of early profiling techniques.</p>

Technique	Other Techniques (choose one from main heading)
Explain/Describe the technique	Intelligence databases store and share information on offenders, suspects, vehicles, and criminal patterns. In the UK, key systems include the Police National Computer (PNC) , which holds details of arrests, cautions, convictions, and vehicle records, and the Police National Database (PND) , created after the Soham murders to allow forces nationwide to share intelligence. Local systems such as CRIMINT hold information on known criminals and protestors, while specialist databases have tracked gang affiliations (e.g., the Gangs Matrix, discontinued in 2022). Internationally, Interpol and Europol databases allow sharing of biometric and criminal intelligence across borders. These systems help link crimes, identify suspects, and safeguard the public.
Types of Crime Where it Has Proved Useful (inc. violent crime, e crime and property crime)	Intelligence databases have been especially valuable in tackling violent crimes , such as murders and gang-related assaults, where information on previous offences or networks can reveal links. They also play a key role in property crime , such as stolen vehicles or burglary, where patterns and suspect histories are logged and searchable. In e-crime , international databases managed by Europol and Interpol track cybercrime and fraud, allowing cross-border cooperation.
Explain the type of crime that it is useful in and strengths of this method:	Intelligence databases are most effective in serial or cross-jurisdictional crimes where suspects operate across different areas or police forces. They are particularly strong in safeguarding , as missing person alerts and offender histories can be shared instantly. Their strengths lie in centralising information, enabling links across cases that would otherwise go unnoticed, and supporting cooperation between local, national, and international agencies.
The type of crime it may NOT be useful in and limitations: One-off, police under public pressure etc.,	These databases are less useful for isolated, one-off crimes such as opportunistic thefts, where little prior intelligence exists. They can also be undermined by outdated or inaccurate entries, leading to wrongful suspicion. Concerns have been raised about bias and discrimination , for example with the Gangs Matrix disproportionately flagging young Black men. Data privacy issues, high running costs, and the potential for misuse further limit their reliability.
Case Studies:	The Soham murders (2002) exposed failures in intelligence-sharing when Ian Huntley, with prior sexual offence allegations, was able to work in a school; the Bichard Inquiry led to the creation of the Police National Database (PND) to prevent such gaps. By contrast, the Gangs Matrix (2012–2022) , designed to track suspected gang members after the London Riots, was scrapped for racial bias and human rights concerns, showing how databases can be both powerful and problematic. A positive example is the case of Joseph Kappen (2002) , where a partial match to his son on the National DNA Database led to Kappen’s exhumation and proved him guilty of three murders in 1973, making it the UK’s first familial DNA conviction and demonstrating the potential of databases to solve cold cases.

Key Terms:

Create a Mind Map for a potential answer for the question (**N.B.** – *Only use bullet points or you will **not be allowed to take this sheet into the exam!***)

This is the most 'point rich' question in the exam.

Use this space to create a mind map of your potential answer.

USE ONLY BULLET POINTS!