COMPUTING & ICT—Year 09 Knowledge Organiser: Digital Forensics

Summary

School student Maria has gone missing. Over a series of 7 lessons, students need to look at metadata, location data, Instagram and messages from Maria's phone that she has left at home. Students look at a series of witness statements and search Maria's bedroom for clues as to where Maria could be.

This unit also has an escape room style activity of the crime scene where Maria is found (alive).

The unit covers e-safety and the signs of grooming. It also covers brute force attacks, VPNs, Cookies, Internet history and deleting files from hard drive, giving students a good insight into how our own personal data is tracked online and on our personal devices.

What is Digital Forensics?

- An area of forensic science that focuses on identifying, acquiring, processing, analysing and reporting on stored data electronically.
- Where a form of computer system is specifically investigated
- Electronic evidence is a component of almost all criminal activities and digital forensics support is crucial for law enforcement investigations.
- Electronic evidence can be collected from a wide array of sources, such as computers, smartphones, remote storage, unmanned aerial systems, shipborne equipment, and more.
- Electronic evidence can be collected from a wide array of sources, such as computers, smartphones, remote storage, unmanned aerial systems, shipborne equipment, and more.

Why is this unit important?

- Learning about digital forensics opens up a fascinating world where you can be a digital detective, protect people's information, and solve puzzles that help make the digital world safer for everyone.
- Also, it's a lot of fun and can lead to some awesome career opportunities in the future!

Digital Forensics Analyst Job Role

- **Investigate Cybercrimes**: Examine computers, mobile devices, and networks to find evidence of cybercrimes.
- **Recover Deleted Data**: Use specialized tools to recover deleted or hidden files and data.
- **Analyze Digital Evidence**: Look through digital files, emails, and internet history to uncover crucial information.
- **Stay Updated**: Keep up-to-date with the latest digital forensics tools, techniques, and cyber threats.
- **Pays between £35,000 to £50,000 per year**, depending on experience and location.

Key Vocabulary

Analysis	A detailed examination of the elements or structure of something.
Brute Force Attack	A brute force attack is a hacking method that uses trial and error to crack passwords, login credentials, and encryption keys.
Chain of Custody	The term Chain of Custody refers to the chronological documentation associated with the evidence. This records the paper trail, custody, transfer, analysis and disposal of the evidence.
Chronological	Following the order in which they occurred. "the entries are in chronological order"
Digital Forensics	Digital forensics is the process of uncovering and interpreting electronic data. It is the process of identifying, preserving, analysing, and documenting digital evidence.
IP Address	A unique string of characters that identifies each computer using the Internet Protocol to communicate over a network i.e. 123.23.46.232
MAC Address	A MAC address is the unique identifier that is assigned by the manufacturer to a piece of network hardware.
Metadata	Metadata is data about data - it allows a computer to construct an image.

How can digital artefacts be explored and analysed to reveal information about a person?
How do we protect ourselves against unwanted attention online?