Science-
Digital Forensics

We're living in an increasingly digital world which means that the 'bad guys' also have access to lots of digital devices that can help them to commit crimes. Whether that is part of a cyber security hack or using a burner phone as part of an organised crime gang; they create digital artefacts every day through their interactions with computers, mobile phones and other digital objects. Forensics have had to try and keep one step ahead of the game in order to gather, analyse and present digital evidence in order for it to be used in a court of law to convict the criminals.

When you think of forensics, what's the first thing that comes to mind? Your views are probably shaped by what you've seen on television programmes with people dressed in white, carrying bags of tools and investigating crime scenes in scary looking places. But forensic science is all about using science to help with legal matters and these next two activities are going to focus on Digital Forensics specifically. This is the area of forensics in which professionals analyse data from computers or other forms of digital media. It includes lots of areas such as computer forensics, network forensics, mobile phone forensics, image & video forensics and database forensics. It has become really important and it's all been brought about by the introduction of new technology.

Activity One will show you how easy it can be for criminals to collect data about someone from their online presence, and for Activity Two you will become the digital forensics investigator, looking for any evidence of criminal action!

If you would like the answers to the activities, please email _____ stating your school and key stage.

- Know or know of https://tinyurl.com/2vrjbwtu
- The Phisherman https://tinyurl.com/55kb3cma
- Cyber activities to create https://tinyurl.com/ytx38uh3
- Malware https://tinyurl.com/mv5v687y
- Games and activities https://tinyurl.com/3s5pj3am
- Staying safe online https://tinyurl.com/bpa72sd9

- A career in security – are you up for the challenge? https://tinyurl.com/25yka4fu
- Cyber aware https://tinyurl.com/22r3yte5

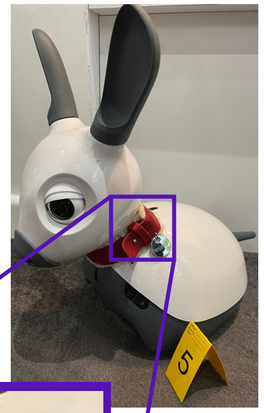
- 'Tech We Can' lesson packs https://tinyurl.com/4wkjkf6w
- Cyber Security practical resources for schools https://tinyurl.com/36pjhjdb
- CyberFirst overview https://tinyurl.com/bdabazj5
- Helping parents keep their children safe online https://tinyurl.com/5ykxm2yp
- Back to school online safety guides https://tinyurl.com/3hvf9zwj

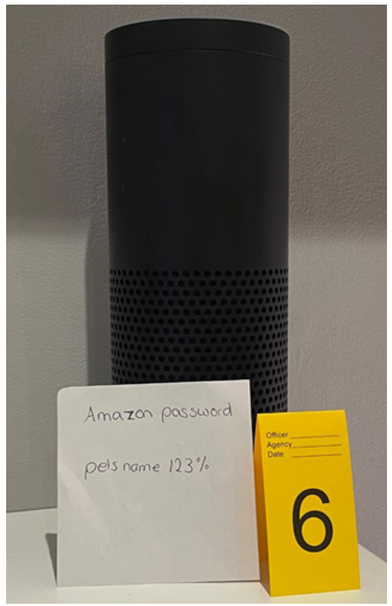
Forensics

For this activity you will need to carefully watch the BT video on the Digital Forensics page. When watching, what do you notice? Can you spot some clues in the background?

The living room in the video is a digital crime scene, littered with pieces of information that may be clues to help solve this activity. Each piece of information that has been identified with a crime scene marker can be used to build a bigger picture of who you are, or even used to by criminals to log in to your online accounts.

The items can be seen in the video, but we've included some close-ups on this page so you can look in more detail.





Activity 1
Forensics

A friend of yours has recently setup an Instagram account and has asked you to test how secure it is by trying to login without being told their login information.

You have seen the following bits of information (images on page 3) recently posted in the background of their social media pictures.

You obviously know your friend's name, but it has asked for their birthday?

A: ……

Your friend hasn't told you their password (as you should never share this information), but to login to their Instagram it needs you to enter a password or answer the following security questions instead. See if you can answer the questions with the information you can gather from the video and close-up images:

1. **What is your favourite song?**

A: ……

2. **What is your pet's name?**

A: ……

3. **What is the name of your best friend?**

A: ……

This goes to show that the information they have shared by recording a video in their living room can help criminals log into their online accounts. They weren't even aware this information was all on show!

In the next part of the activity, link up the typical security questions on the left with the information shared in the pictures/video (hint: it might not link to just one crime scene marker number).

Question	Crime Scene Marker Number	Answer
What is your mother's maiden name?	1	Johnson
	2	
	3	
What is your favourite food?	4	White
	5	
What is your favourite colour?	6	Cornflakes
	7	

Oh no… they also haven't realised that their Amazon password can be seen in the video. What is it?

A: ……

Every piece of information adds up and can provide people a detailed insight into your personal life. To protect yourselves you should consider what people can see about you online. Remember you can setup privacy settings to only allow certain trusted people to see your data. You can also set your security question answers to be fake, you just need to remember what they are! Consider setting up password management software and use two-factor authentication.

Check the answer booklet to see if you were able to get all of the answers correct, and then try the next activity which is another digital forensics investigation, but a little more difficult…

Activity 2
Forensics

Follow the clues in this digital treasure hunt activity to find out if a crime has been committed. Use your digital forensic investigation skills to identify some evidence, preserve it, analyse it and document it so that you can report back if there has been any wrongdoing.

Task 1 - Identify

Find the first clue by using the grid cypher below:

F3 D1 A1 F1 A4 D1 E4 E3 A4 B2 F1 D3 A4 A2 B2 F6 C2 D2 F6 E3 D3 F6 B4 E3 C5 B2 F1 C2 A1 E5 E3 E5 B2 E4 B2.

E6 A1 D1 A1 E4 B1 C1 C1 B5 C5 D3 E1 F1 A5 F5 F2 F5 D5 D2 D3 F1 B4 A1 F1 E3, E4 D3 D1 E3 C5 F3 A2 E3 D1 D3 C3 E3 E3 E6 A1 E5 E3 F1 C5 E3 A6 D3 A2 E4 C2 E3 F1 E3 B6 E4 E4 B2 D1 C6 D1.

	A	B	C	D	E	F
1	I	i	B	S	/	N
2	R	A	H	Y	f	4
3	9	Z	M	O	E	U
4	G	L	s	1	T	z
5	W	.	C	J	D	5
6	F	X	K	c	V	P

Task 2 - Preservation (Exploring the Metadata)

In a digital forensics investigation, you need to be careful not to change any of the data. Opening a file might change the ‘last opened date’ of a file, so a copy should be taken. This will leave the original file unchanged or preserved.

Metadata is ‘data about data’. When you create a file, the date it was created or modified is stored with the file. In fact, lots of data can be stored such as the name of the computer used, the file name, comments, the owner and so much more. You just need to know where to look to find the metadata!

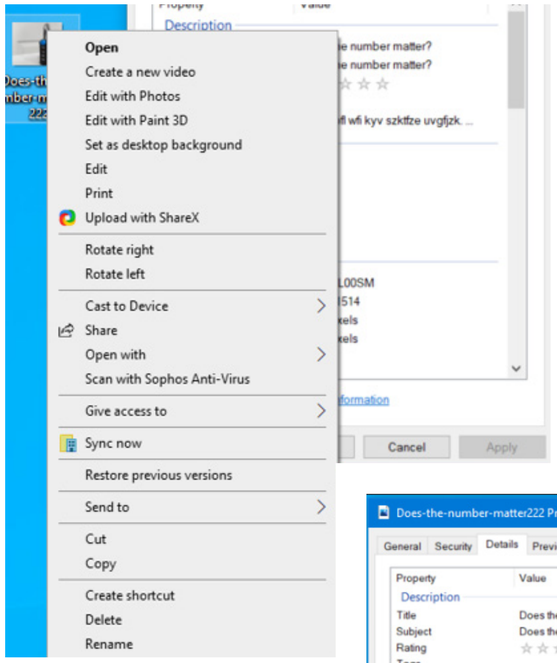
Metadata can offer clues during a digital forensics investigation. People can also easily add in their own metadata to files if they want to secretly exchange messages with others!

Upload the file you downloaded from Task 1 into this online tool (_____) to explore the metadata. See if you can find the next clue!

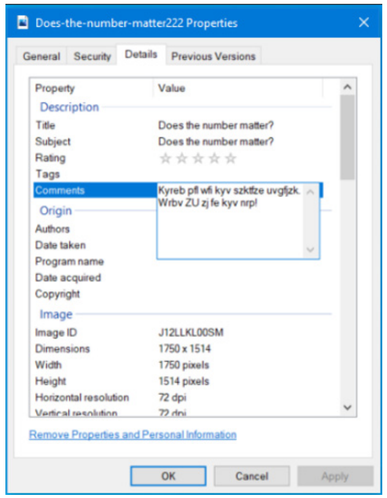
Alternatively, you can do the following to look into the metadata yourself:

- Once the image of the lock is downloaded, the metadata can be viewed by ‘Right Clicking’ on the file and going to ‘Properties’ and then ‘Details’.

Activity 2
Forensics



Extension: What might be some of the dangers of metadata when you take pictures?



Task 3 - Analysis (Decrypt the evidence)

Even though you may find (and preserve) some digital evidence, it might by encrypted and therefore you can't read or understand it.

To decrypt the data found in Task 2, use this online tool which uses a Caesar Cipher: https://tinyurl.com/yc2vzstw

Task 4 - Documentation

Using the evidence you've collected, and the online decryption tool - decrypt the message, using the correct key, to reveal the contents. Has a crime been committed?

In a real digital forensic investigation, you would then produce a report about the evidence that you have found and present the report to the police for them to use in court.

Key outcomes:

During this activity, you should have identified evidence that needed to be investigated further. Digital evidence can be stored in a range of places including hard disks, mobile phones and cloud storage. You have preserved some digital evidence and then analysed this to produce more evidence.

The final stage was to document the evidence you gathered and present this as part of your investigation.

In the process of this activity, you have:

- Seen how data can be hidden in plain sight using steganography.
- Used a cipher to decrypt data.
- Explored the use of metadata and considered the implications of this.