

Industry In The Classroom

Virtual Engagement Lesson Guide How To Solve A Murder

Version 1.0

January 2021

Introduction

The web is filled with educational resources that can be used to bring cyber security to life. But it can be difficult to know which ones will work well for young learners, and which are suitable to be delivered virtually in classrooms.

This lesson plan is an example of a high quality cyber security activity suitable for highschool age students. Cyber Skills Live activities are tried-and-tested and are great for industry volunteers to use remotely with a class.

In *How To Solve A Murder* pupils solve the case of a murder in Bishopbriggs by sifting through the evidence. This introduces some of the basics of *digital forensics*.

Each is designed to last around 30 minutes, and learners only need a web browser to use them. These activities may be used to support the teaching and delivery of learning outcomes for the NPA Cyber Security qualification.


Daniel Devine
Digital Skills Education
January 2021

How to use this lesson plan

- ❑ Play through the “How To Solve A Murder” activity:
<https://cyberskillslesson.com/activity/how-to-solve-a-murder/>
- ❑ Watch the playthrough video:
<https://drive.google.com/file/d/1zZRRMr83unbvYBgKU9AibBbev-Yk6DAs/view?usp=sharing>
- ❑ Read through the lesson plan, this suggests timings and talking points. Where possible use these notes but you should also add in your own knowledge and experience
- ❑ Read the sample slides and adapt them to suit you:
https://docs.google.com/presentation/d/1ai51ZzO-xhds00qMz90J5jyOENSNKcVeKW_eZGWUJaY/edit?usp=sharing
- ❑ Practice running through the activity using the lesson plan

Remember, for advice on organising and running this virtual engagement session you should refer to the Virtual Engagement Best Practice Guide.

Factsheet

- Topics:** Cyber Security, Digital Forensics
- Target Audience:** S1-S4 (ages 11-16) secondary school students.
- Target Volunteers:** Anyone working in technology with a familiarity with the basics of cyber security. Background knowledge in forensics is useful but not required.
- Skills Level:**  Suitable for Beginners.
- Need to know:** These are really popular with learners and a fun activity to do in the classroom. They're a great way to introduce digital forensics topics in a way that feels like a game.
- Preparatory work:**
- 1) Read the Virtual Engagement Best Practice Guide
 - 2) Play the activity yourself
 - 3) Build and customise your session
- Required equipment:** Pupils each need access to a modern web browser.
- Websites required:** <https://cyberskillslesson.com/>
<https://scotiarail.co.uk/>
<https://nationalrail.co.uk/>
- The context:** *"Become a digital detective and see how you can use your digital skills to solve a crime. Start the investigation by collecting, identifying and validating the digital evidence and see if you catch the criminal."*
- Hints for on the day:** Play along with the young people, it'll keep your pace right and will mean you can give hints or directly talk about what they are doing.

Lesson Plan

<p>Time</p>	<p>Cyber Skills Live - How To Solve A Murder Volunteer: Teacher:</p> <p>Sample Slides: https://docs.google.com/presentation/d/1ai51ZzO-xhds00qMz90J5jyOENSNKcVeKWeZGWUJaY/edit?usp=sharing</p>
<p>Hook</p>	
<p>2</p>	<p>Make sure to include:</p> <ul style="list-style-type: none"> ● Your name and how you'd like to be addressed ● Where you are calling from ● What your role is (a brief description of what you do) ● Who you work for and what the company does <p>"Hello, I'm Andrew McLeish. Today you can call me Andy. I'm joining you today from our office in Linlithgow. I am a digital forensics analyst at Fair Isle Forensics, we're a company that helps people recover deleted files from smartphones, tablets, and computers. Sometimes we work with businesses who need to recover documents they've accidentally deleted, and other times we work with the Police to help them gather evidence for cases."</p> <p>"Today you're going to become a digital detective and see how you can use your digital skills to solve a crime. Our activity is based on a real-life job role, digital forensics for the police."</p> <p>"You're also going to get the chance to ask me any questions about my role as Digital Forensics Officer working at Fair Isle Forensics."</p>
<p>Engage</p>	
<p>5</p>	<p>Give a short, 2-3 slide, presentation on the area and what you do. Think about what context the learners might need for the activity - in this case linking it to the need to work digital evidence.</p> <p>Use the question in the slide to prompt discussion: "Are deleted files gone forever?"</p> <p>As part you this section you could:</p> <ul style="list-style-type: none"> ● Talk about a task you do at work ● Ask the pupils a question ● Discuss a relevant recent news story
<p>Explore</p>	
<p>2</p>	<p>Starting the activity: "Go to cyberskillslesson.com and select How To Solve A Murder. It'll work in any modern web browser like Google Chrome or Firefox.</p>

	<p>You'll be asked what school you are joining from, select " ____ "</p> <p>Enter your first name, and choose an avatar"</p>
5	<p>Log the evidence: A series of questions where you have to collect information on the evidence found.</p> <p>Data to collect:</p> <ul style="list-style-type: none"> ● type ● manufacturer ● serial ● date of seizure ● location of seizure <p>Things to talk about:</p> <ul style="list-style-type: none"> ● Logging the evidence ● Chain of custody/forensic link/paper trail <ul style="list-style-type: none"> ○ Documentation of the collection, transfer and analysis of evidence ● Contamination/tampering could lead to evidence being challenged or ruled inadmissible
5	<p>Preparing The Drive For Examination Steps:</p> <ul style="list-style-type: none"> ● Take a digital copy ● Calculate the hash ● Mount the image <p>Things to talk about:</p> <ul style="list-style-type: none"> ● Why it's important to take a forensic clone -> may accidentally destroy or tamper with the evidence if working on original ● A hash is like a digital fingerprint, if the clone is a bit for bit copy the hash of the copy and the original will be the same ● Mounting let's you open a clone/image as if it was a real drive, allowing you to look at the files and folders within <p>Ask the students to pause playing after mounting the image to keep everyone working at a similar pace.</p>
5	<p>Examining Chat Logs Steps:</p> <ul style="list-style-type: none"> ● Find the chat logs ● Sift through the chat logs <p>Things to talk about:</p> <ul style="list-style-type: none"> ● We've heard that our suspect has been speaking to a known criminal called Neville. It would be great to know what they've been talking about. ● Terminal commands to list files (ls), move into folders (cd), output files (cat), and search (grep).

	<ul style="list-style-type: none"> • Too many texts to work through manually, can search for keywords. <p>Key messages:</p> <ul style="list-style-type: none"> • Our suspect, Chris: <ul style="list-style-type: none"> ○ "I've planned my escape, I've just booked my ticket to the secret hideout" • Known criminal, Neville: <ul style="list-style-type: none"> ○ "Good. I'll meet you there - make sure you're not followed" <p>"Well done, this is very interesting. We know that Neville really is helping Chris run away, and he's getting a ticket. Suggests to me that it could be for public transport so a bus, train, or boat."</p> <p>Ask the students to pause playing after the successful search for 'hideout' to keep everyone working at a similar pace.</p>
5	<p>Examining Browsing History</p> <p>Steps:</p> <ul style="list-style-type: none"> • Find the web browsing history • Search the web history <p>Things to talk about:</p> <ul style="list-style-type: none"> • Needing to know where the hideout is. We know he bought a ticket. Online? • Amount of data browsing history tells you about a person • Using search (by date) to cut down the number of entries to look at
5	<p>Find The Hideout</p> <p>Steps:</p> <ul style="list-style-type: none"> • Learners to look at each of the URLs • One is for ScotiaRail, they should look at this (let them work it out) • Look at the destination (they'll need to click the link to National Rail website) • Answer is Dunrobin Castle
Involve	
10	<p>Q&A with the class. The teacher will relay questions to you.</p> <p>Common Questions and sample answers:</p> <p><i>"How much do you get paid?"</i></p> <p><i>"People working in Digital Forensics on average get paid around £25,000 a year when they start. With experience, you can earn £30,000 to £45,000 a year. Analysts can earn up to £80,000 in more senior roles."</i></p>

	<p><i>"Do you only work with the police?"</i> <i>"No, usually I work with businesses who have accidentally deleted files or think they have suffered from a cyber crime. I only sometimes work with the police. The police also employ a lot of digital forensics workers."</i></p> <p><i>"Where can I study digital forensics?"</i> <i>"There are different options, some universities have degrees in digital forensics, but there are also modern and graduate apprenticeships. Studying cyber security is a good start. I went to Abertay University and studied computer science, then changed job roles after a few years at my previous company."</i></p> <p><i>"What school subjects should I pick?"</i> <i>"People in cyber security have a wide range of backgrounds. Computing is probably the most important subject. Maths and Physics are useful too."</i></p> <p>Link what you say to everyday life, make it relatable to the learners. Share <i>your</i> experience, you can give so much more than generic career information.</p>
Sustain	
2	<ul style="list-style-type: none"> ● Visit the Digital World website (https://www.digitalworld.net/cyber-security-careers) ● Play more Cyber Skills Live activities ● Does your company have any outreach planned? ● Teachers: register for next event


Activity Screenshots

CYBER SKILLS LIVE

What is your first name?

What is your first name, detective?

Submit intelligence



Report a bug

CYBER SKILLS LIVE



What type of device was found?

The first step is to log the evidence into our secure computer system. It's important we create these records so we can prove the evidence collected at the crime scene is the same evidence that is being presented in a court of law.

The device collected is an external hard drive.




Report a bug

Report a bug

CYBER SKILLS LIVE

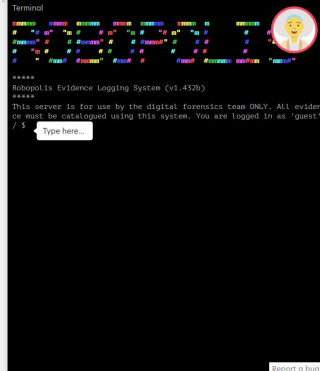
Take a digital copy

It's important we never perform analysis on the original USB drive - we might accidentally destroy or tamper with the evidence. The first thing we need to do is create an exact copy of the drive. A forensic clone is an exact, bit for bit copy of the USB drive.

To do this let's use the `dd` command. This will create an exact copy of the USB drive and save it to our computer.

Copy this command into the terminal and press enter to run it.

```
dd input=/dev/usb/lcd output=/evidence.img
```



Report a bug

CYBER SKILLS LIVE

Find the chat logs

Now we're ready to start analysing the digital evidence. Let's start by reading through the text message conversations that have been stored in the computer.

The `ls` command is short for list and will list all the files in the current directory (another name for a folder). Try it now. Type this command and press enter.

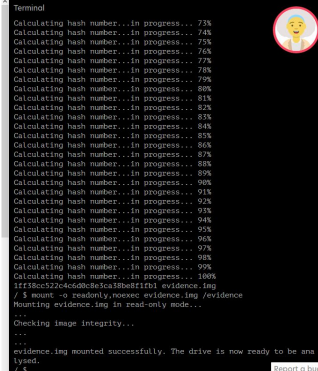
```
ls
```

On a normal computer you can move into a directory by double clicking on the folder icon. But in a terminal you can use the `cd` command followed by the name of the directory.


Try that now to move into the chats directory.

```
cd chats
```

Now you can list all the files that are in this directory.



Report a bug




Report a bug

CYBER SKILLS LIVE

Search the web history

This is a massive list of all the URLs (website addresses) the suspect has visited. Scroll up the list to see how many there are. We'll never be able to check them all in time.

Let's use the `grep` command again to find only URLs accessed on the day the text message to Neville was sent.


```
grep "26-10-2020" website_history.log
```

There are several URLs left, can you spot which one might be most relevant?

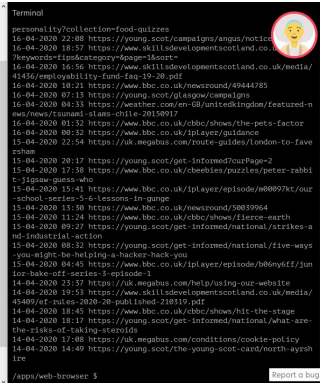
- Open a new tab in your web browser.
- Copy and paste the URL into that new tab.
- Can you tell where the suspect is heading?

Where is the suspect heading? Type the place name of the secret location.


Submit intelligence



Report a bug



Report a bug



Your booking confirmation.

Booking reference: 14471
 Ticket Booked for: Thu 29 October 2020
 Single Ticket

Time	Origin Station		Time	Destination Station
10:10	[GLQ]	→	16:12	[DNO]

Terms and conditions

Travel is subject to availability and requested journeys cannot be guaranteed. Tickets are non-