**ACTIVITY FROM UNIT 1**

**Question 1**

### The idea behind our technique is simple. You basically give your victim a link: they can open it with their mobile, PC, or any sort of device. On that link, they will see an image of your choice (we recommend using a fun one). However, your system will also track automatically their IP address and more information, like the browser they are using and their operating system.

### While this happens, they will see the fun image and have a laugh about it. They have no way of knowing that you are tracking their IP address.

### 

### 

### Step #1 – Register a website (for free!)

### Step #2 – Creating the website itself

### Step #3 – Download the IPFinder script

### Step #4 – Upload the IPFinder Script

### Step #5 – Extract the IPFinder

### Step #6 – Adding images

### Step 7# – Using IPFinder

**Question 2**

Man-in-the-middle attacks (MITM) are a [common type of cybersecurity attack](https://www.rapid7.com/fundamentals/types-of-attacks/) that allows attackers to eavesdrop on the communication between two targets. The attack takes place in between two legitimately communicating hosts, allowing the attacker to “listen” to a conversation they should normally not be able to listen to, hence the name “man-in-the-middle.”

**Types of man-in-the-middle attacks**

* Rogue Access Point
* ARP Spoofing
* DNS Spoofing
* mDNS Spoofing

**Man-in-the-middle attack techniques**

* Sniffing
* Packet Injection
* Session Hijacking
* SSL Stripping