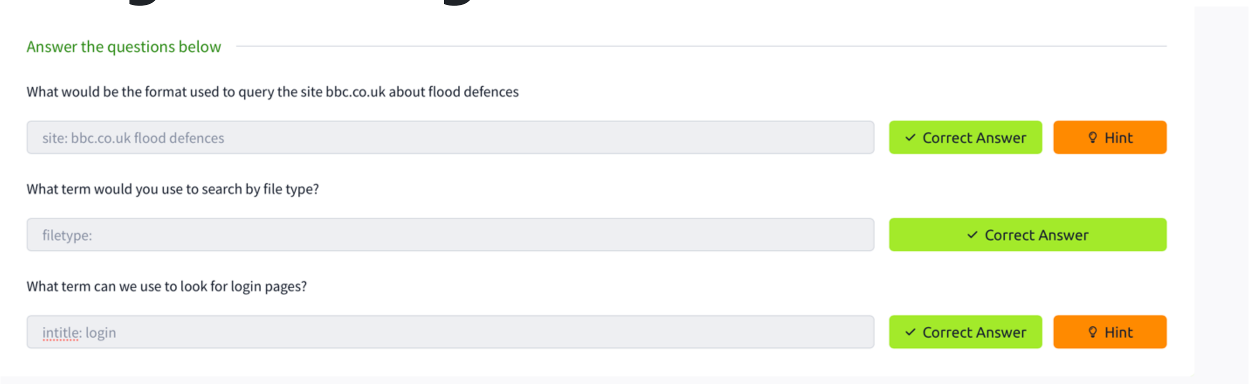
Google Dorking



Answer the questions below

What would be the format used to query the site bbc.co.uk about flood defences

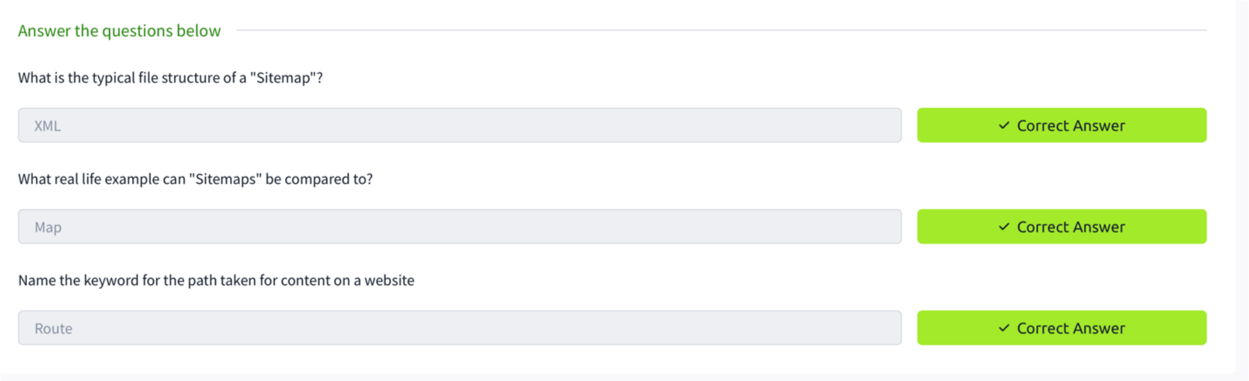
site: bbc.co.uk flood defences

What term would you use to search by file type?

filetype:

What term can we use to look for login pages?

intitle: login



Answer the questions below

What is the typical file structure of a "Sitemap"?

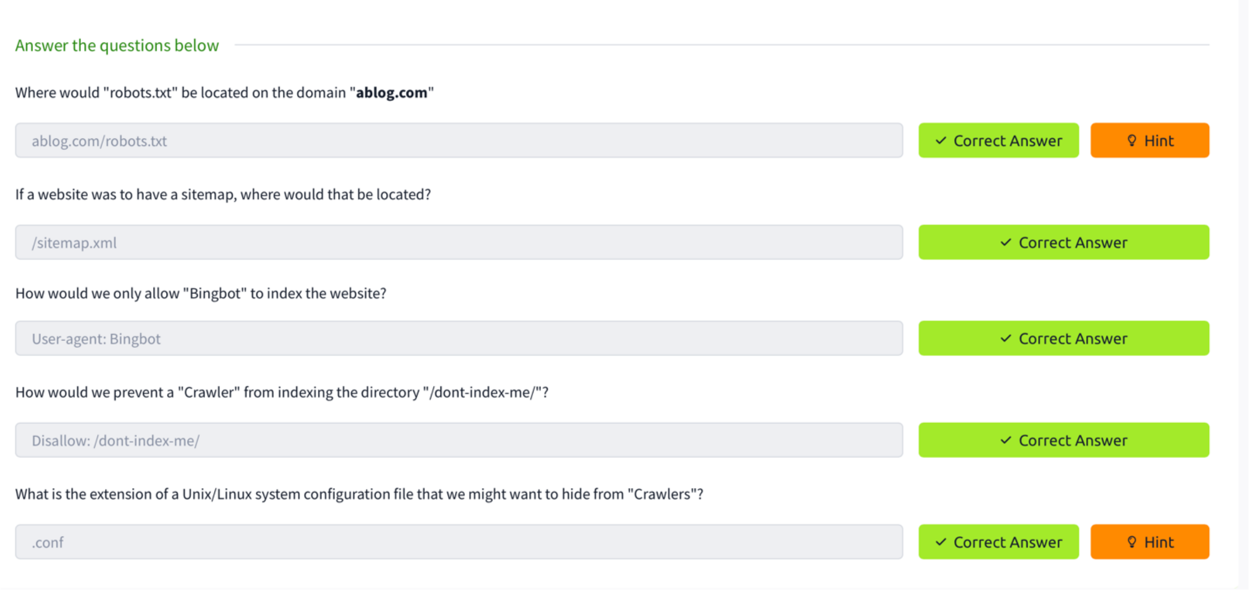
XML

What real life example can "Sitemaps" be compared to?

Map

Name the keyword for the path taken for content on a website

Route



Answer the questions below

Where would "robots.txt" be located on the domain "**ablog.com**"

ablog.com/robots.txt

If a website was to have a sitemap, where would that be located?

/sitemap.xml

How would we only allow "Bingbot" to index the website?

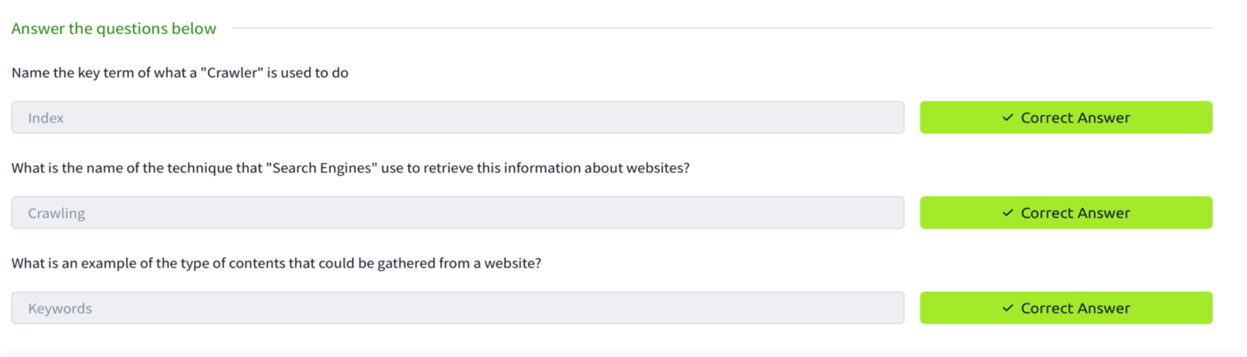
User-agent: Bingbot

How would we prevent a "Crawler" from indexing the directory "/dont-index-me/"?

Disallow: /dont-index-me/

What is the extension of a Unix/Linux system configuration file that we might want to hide from "Crawlers"?

.conf



Answer the questions below

Name the key term of what a "Crawler" is used to do

Index

What is the name of the technique that "Search Engines" use to retrieve this information about websites?

Crawling

What is an example of the type of contents that could be gathered from a website?

Keywords

Browsing Internet resources

1.What is the registrant postal code for facebook.com?

Your response: Postal Code: 94025

2. When was the becode.org domain first registered (Format: DD/MM/YYYY)?

Your response: 04/10/2016

3. Which city is the registrant based for microsoft.com ?

your response: Redmond

4. What is the name of the golf course that is near the registrant address for microsoft.com?

Your response: Bellevue Golf Course

5. What is the registered Tech Email for microsoft.com?

Your response: mnshst@microsoft.com

6. Which subdomain of becode.org starts with `d` and ends with `n`?

Your response:

7. Among the BeCode team, who is a fan of Oscar Wilde ?

Your response: **Pierre-Yves Dehon, David Thewissen**

8. Which of the BeCode partners begins with the letter `p` and ends with the letter `t`?

Your response:Phitrust

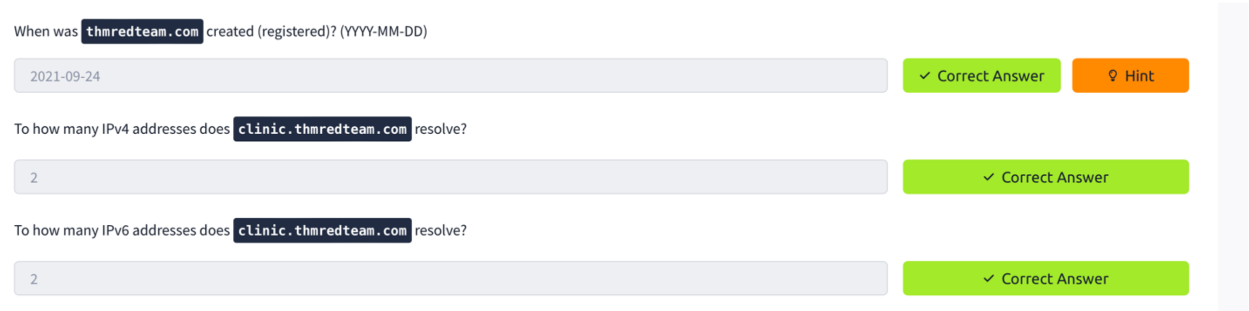
9. Who are the founders of BeCode?

Your response: Karen Boers, Laurent Hublet, and Rodolphe Verhaegen.

Shodan

Maltego

Recon-ng and Maltego



When was `thmredteam.com` created (registered)? (YYYY-MM-DD)

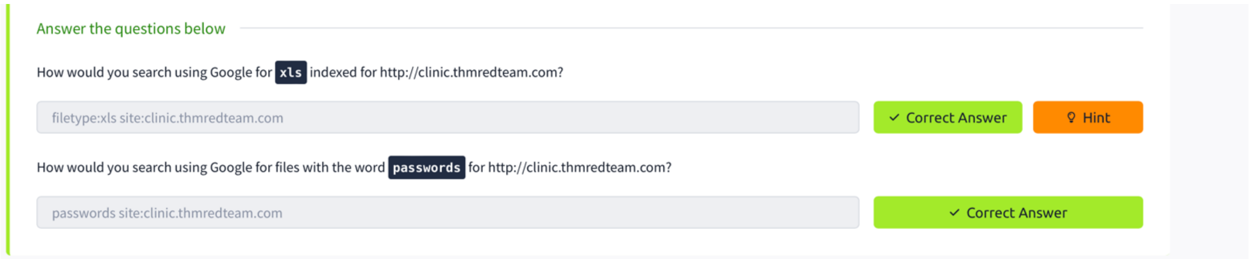
2021-09-24

To how many IPv4 addresses does `clinic.thmredteam.com` resolve?

2

To how many IPv6 addresses does `clinic.thmredteam.com` resolve?

2



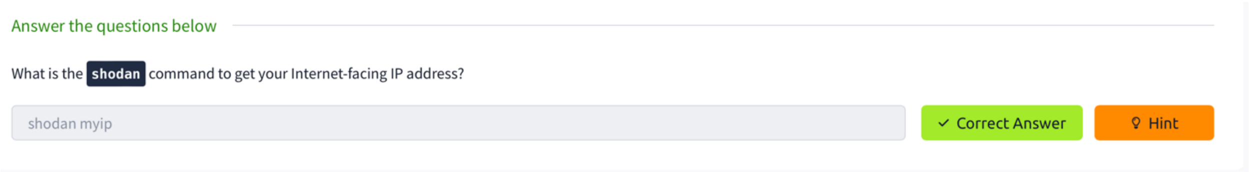
Answer the questions below

How would you search using Google for `xls` indexed for http://clinic.thmredteam.com?

filetype:xls site:clinic.thmredteam.com

How would you search using Google for files with the word `passwords` for http://clinic.thmredteam.com?

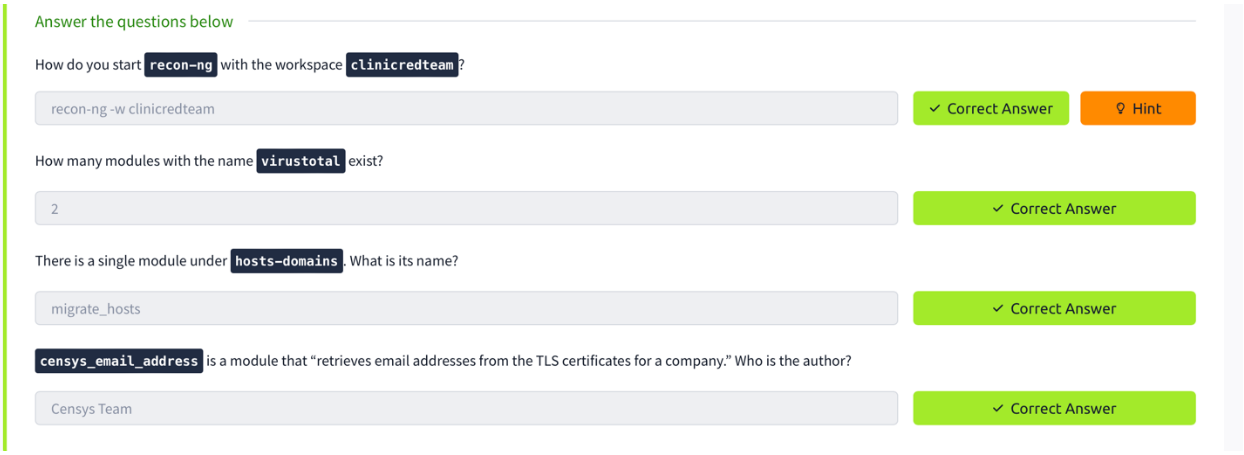
passwords site:clinic.thmredteam.com



Answer the questions below

What is the `shodan` command to get your Internet-facing IP address?

shodan myip



Answer the questions below

How do you start `recon-ng` with the workspace `clinicredteam`?

recon-ng -w clinicredteam

How many modules with the name `virustotal` exist?

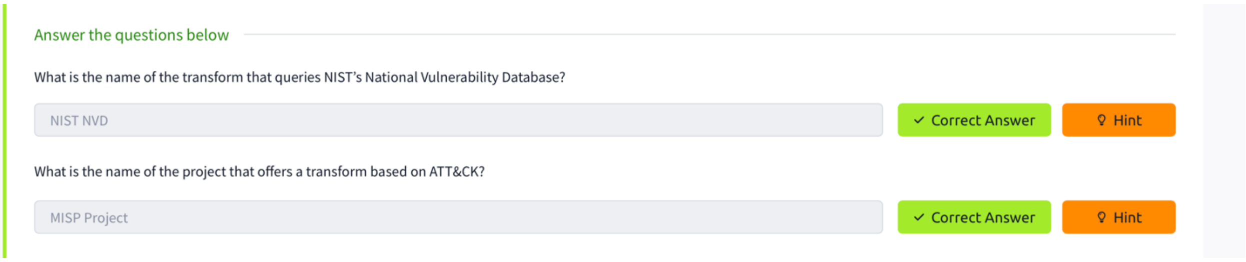
2

There is a single module under `hosts-domains`. What is its name?

migrate_hosts

`censys_email_address` is a module that "retrieves email addresses from the TLS certificates for a company." Who is the author?

Censys Team



Answer the questions below

What is the name of the transform that queries NIST's National Vulnerability Database?

NIST NVD

What is the name of the project that offers a transform based on ATT&CK?

MISP Project

Maltego Becode.org

The provided Maltego graph visualizes a network of entities related to BeCode.org, a Belgian non-profit organization focused on digital skills training. The graph, created using open-source intelligence (OSINT) techniques with the free version of Maltego, offers a limited view of the organization's online presence and potential connections.

Entities include:

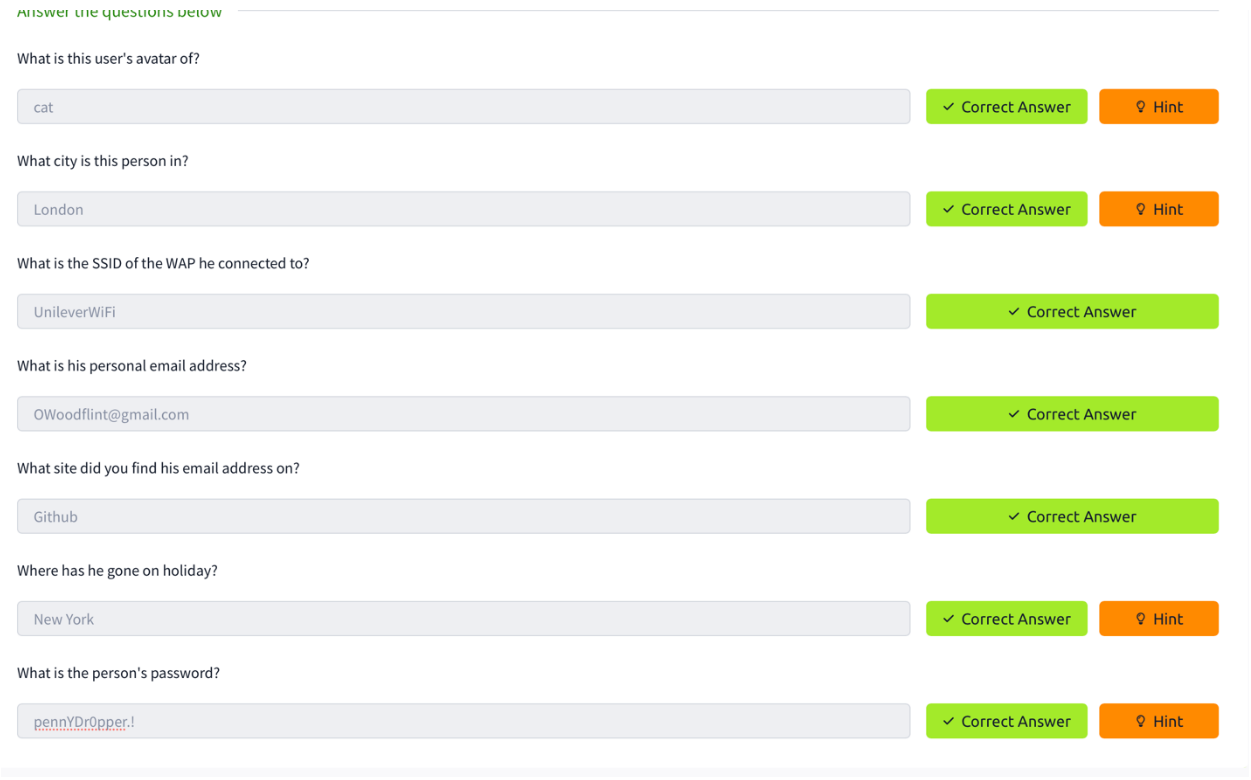
- **Hash:** Unique identifiers for files or data, useful for tracking and identifying specific content.
- **Email Address:** Used for communication, can be linked to individuals or organizations.
- **Domain:** Internet addresses associated with websites or organizations.
- **STIX2 Domain Name:** Standardized format for threat intelligence information related to domain names.
- **maltego.STIX2.x-opencti-hostname:** A custom entity type specific to Maltego, a tool used for investigations.
- **Location:** Geographical coordinates associated with entities.
- **MX Record:** Mail exchange records indicating servers responsible for email delivery for a domain.
- **Snapshot:** Likely a saved image or data capture of a website or system.
- **Website:** Collection of web pages under a specific domain.

- **DNS Name:** Domain Name System entry, translating domain names to IP addresses.
- **Phrase:** Specific text strings relevant to the investigation.
- **Person:** Individuals identified in the analysis.
- **Organization:** Groups or companies involved.
- **Netblock:** Range of IP addresses associated with an organization or network.
- **BuiltWith Technology:** Information about technologies used to build websites.
- **Image:** Visual content found during the investigation.
- **URL:** Uniform Resource Locators, addresses of web pages.
- **Port:** Network ports used for communication between systems.
- **AS:** Autonomous Systems, networks under a single administrative control.
- **Date Time:** Timestamps indicating when events or data were recorded.
- **IPv4 Address:** Internet Protocol version 4 addresses, identifiers for devices on the internet.
- **Document:** Files relevant to the investigation.
- **Shodan Tag:** Labels from Shodan, a search engine for internet-connected devices.
- **File Snapshot:** Saved version of a file.
- **IPv6 Address:** Internet Protocol version 6 addresses.

Connections: Lines connecting entities indicate relationships. The specific nature of these relationships would depend on the context of the investigation. For example, a connection between an email address and a domain could indicate the email was sent from that domain.

Review challenges

- CTF OhSint



Answer the questions below

What is this user's avatar of?

cat

What city is this person in?

London

What is the SSID of the WAP he connected to?

UnileverWiFi

What is his personal email address?

OWoodflint@gmail.com

What site did you find his email address on?

Github

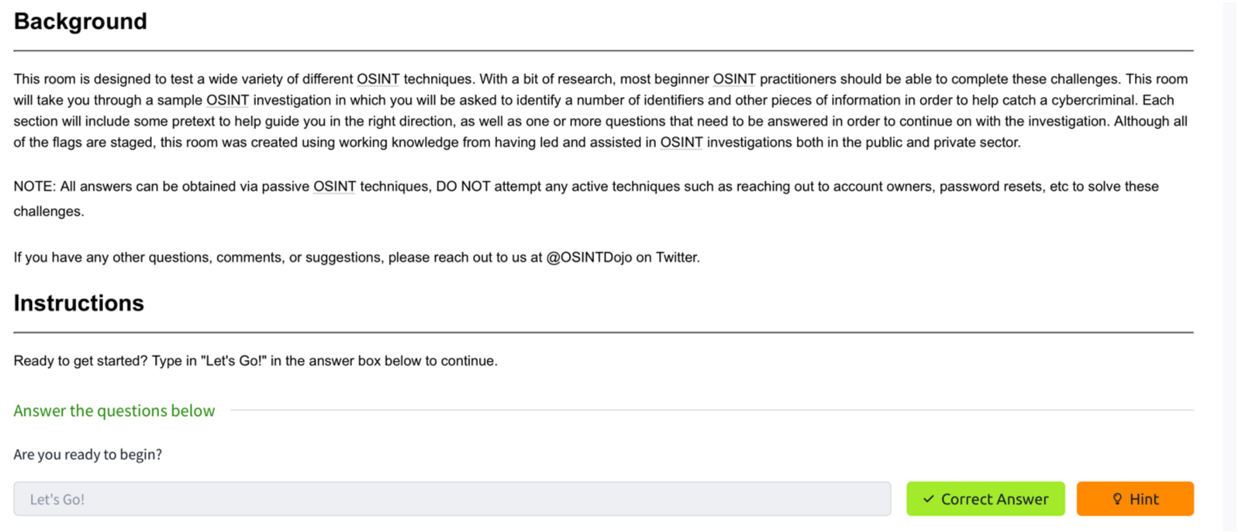
Where has he gone on holiday?

New York

What is the person's password?

pennYDr0pper.!

Sakura



Background

This room is designed to test a wide variety of different OSINT techniques. With a bit of research, most beginner OSINT practitioners should be able to complete these challenges. This room will take you through a sample OSINT investigation in which you will be asked to identify a number of identifiers and other pieces of information in order to help catch a cybercriminal. Each section will include some pretext to help guide you in the right direction, as well as one or more questions that need to be answered in order to continue on with the investigation. Although all of the flags are staged, this room was created using working knowledge from having led and assisted in OSINT investigations both in the public and private sector.

NOTE: All answers can be obtained via passive OSINT techniques, DO NOT attempt any active techniques such as reaching out to account owners, password resets, etc to solve these challenges.

If you have any other questions, comments, or suggestions, please reach out to us at @OSINTDojo on Twitter.

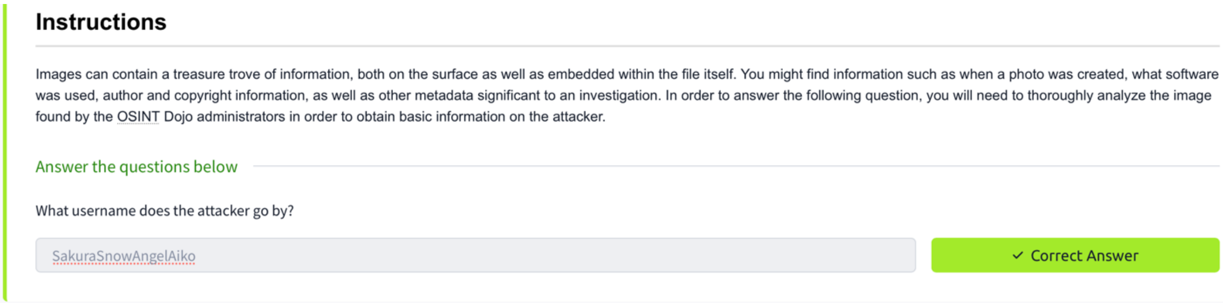
Instructions

Ready to get started? Type in "Let's Go!" in the answer box below to continue.

Answer the questions below

Are you ready to begin?

Let's Go!



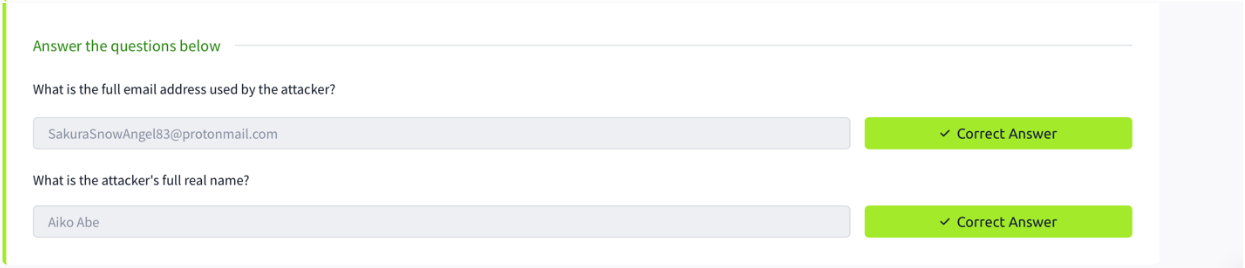
Instructions

Images can contain a treasure trove of information, both on the surface as well as embedded within the file itself. You might find information such as when a photo was created, what software was used, author and copyright information, as well as other metadata significant to an investigation. In order to answer the following question, you will need to thoroughly analyze the image found by the OSINT Dojo administrators in order to obtain basic information on the attacker.

Answer the questions below

What username does the attacker go by?

SakuraSnowAngelAiko



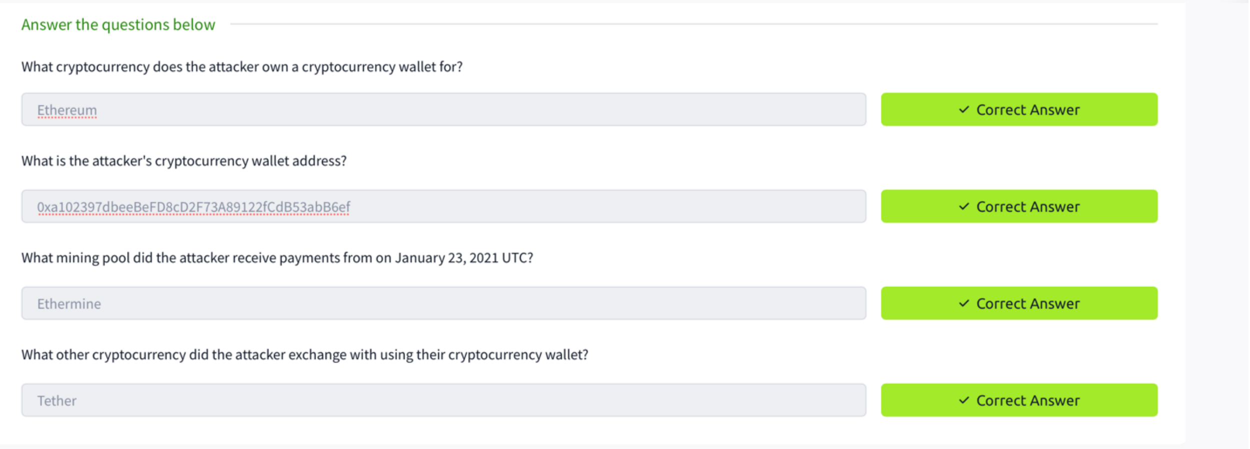
Answer the questions below

What is the full email address used by the attacker?

SakuraSnowAngel83@protonmail.com

What is the attacker's full real name?

Aiko Abe



Answer the questions below

What cryptocurrency does the attacker own a cryptocurrency wallet for?

Ethereum

What is the attacker's cryptocurrency wallet address?

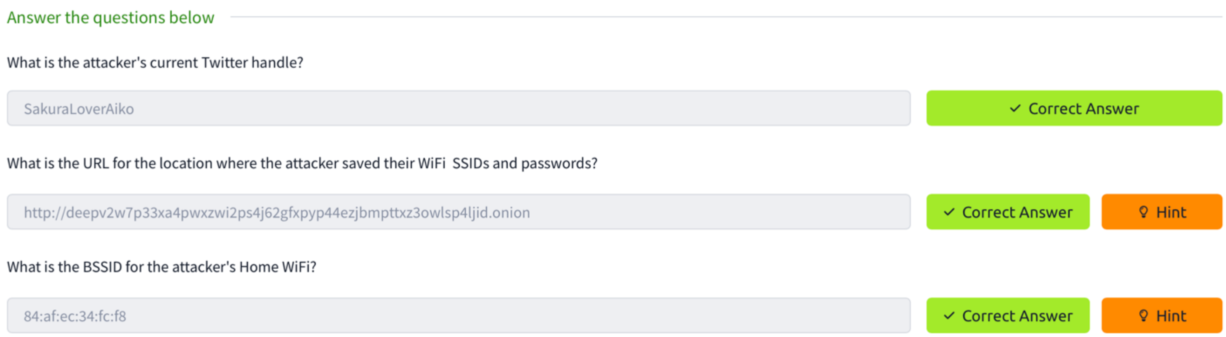
0xa102397dbeeBeFD8cD2F73A89122fCdB53abB6ef

What mining pool did the attacker receive payments from on January 23, 2021 UTC?

Ethermine

What other cryptocurrency did the attacker exchange with using their cryptocurrency wallet?

Tether



Answer the questions below

What is the attacker's current Twitter handle?

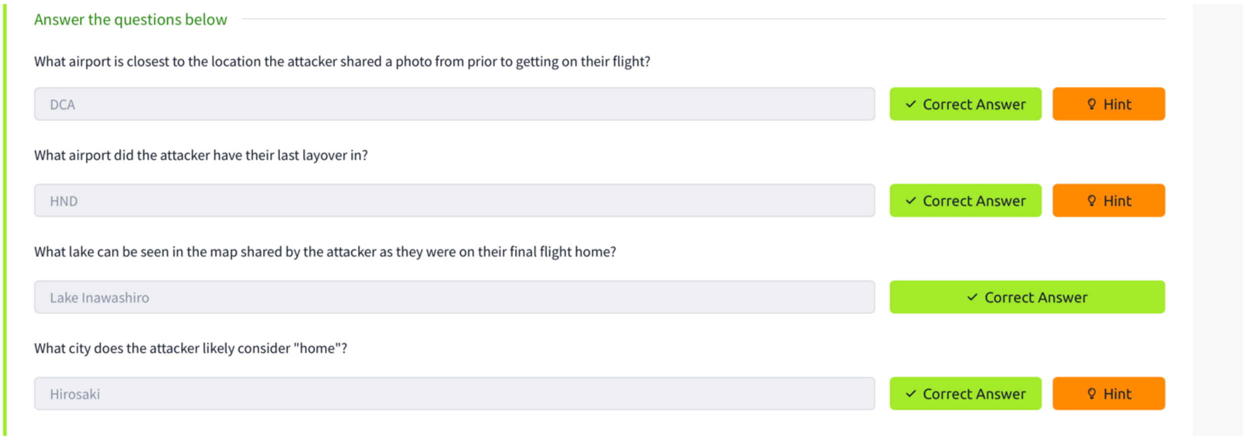
SakuraLoverAiko

What is the URL for the location where the attacker saved their WiFi SSIDs and passwords?

http://deepv2w7p33xa4pwxzwi2ps4j62gfxpyp44ezjbmpttxz3owlsp4ljid.onion

What is the BSSID for the attacker's Home WiFi?

84:af:ec:34:fc:f8



Answer the questions below

What airport is closest to the location the attacker shared a photo from prior to getting on their flight?

DCA

What airport did the attacker have their last layover in?

HND

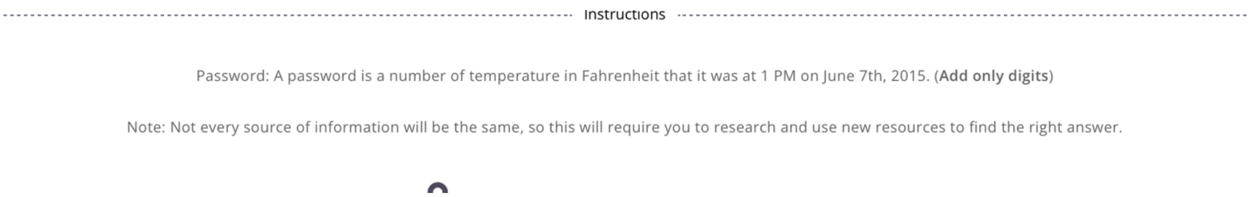
What lake can be seen in the map shared by the attacker as they were on their final flight home?

Lake Inawashiro

What city does the attacker likely consider "home"?

Hirosaki

- OSINT sourcing

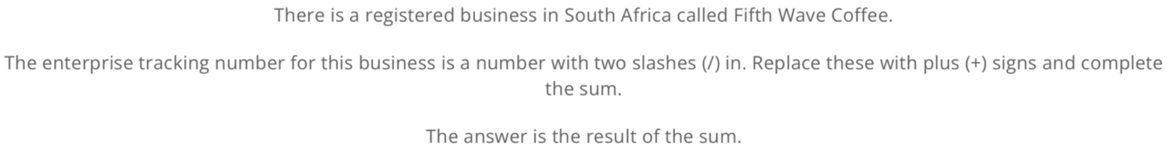


Instructions

Password: A password is a number of temperature in Fahrenheit that it was at 1 PM on June 7th, 2015. (**Add only digits**)

Note: Not every source of information will be the same, so this will require you to research and use new resources to find the right answer.

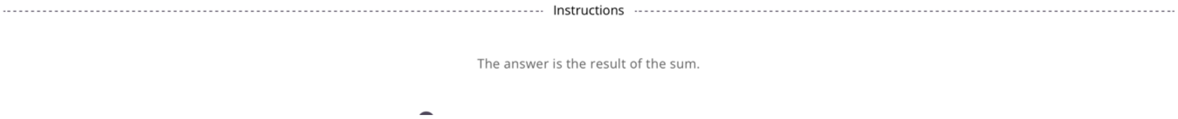
85



There is a registered business in South Africa called Fifth Wave Coffee.

The enterprise tracking number for this business is a number with two slashes (/) in. Replace these with plus (+) signs and complete the sum.

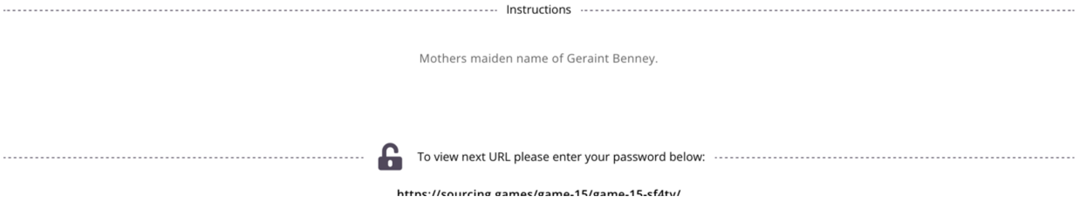
The answer is the result of the sum.



Instructions

The answer is the result of the sum.

2018+463990+07=466.015



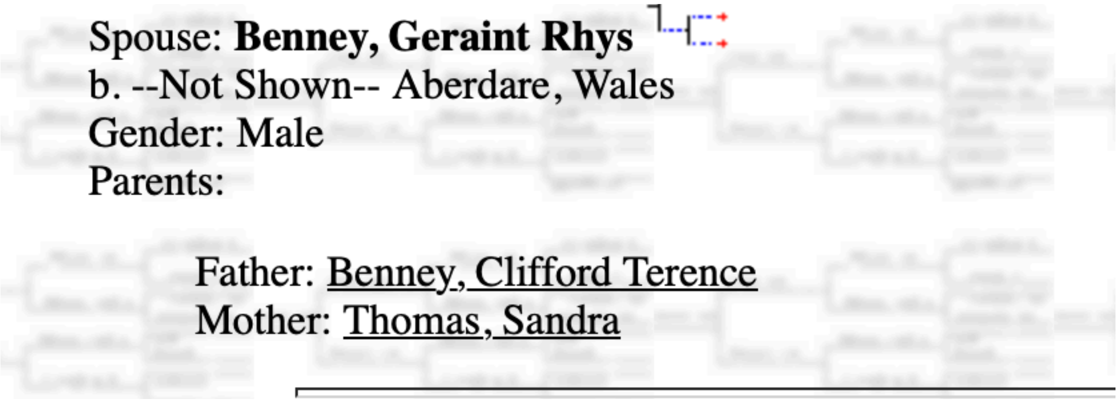
Instructions

Mothers maiden name of Geraint Benney.

To view next URL please enter your password below:

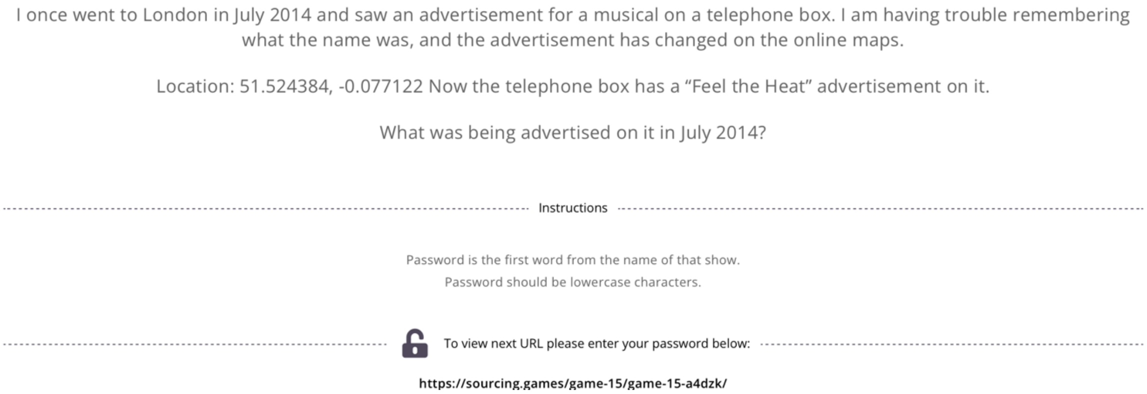
https://sourcing.games/game-15/game-15-sf4tv/

Thomas



Spouse: **Benney, Geraint Rhys**
b. --Not Shown-- Aberdare, Wales
Gender: Male
Parents:

Father: Benney, Clifford Terence
Mother: Thomas, Sandra



I once went to London in July 2014 and saw an advertisement for a musical on a telephone box. I am having trouble remembering what the name was, and the advertisement has changed on the online maps.

Location: 51.524384, -0.077122 Now the telephone box has a "Feel the Heat" advertisement on it.

What was being advertised on it in July 2014?

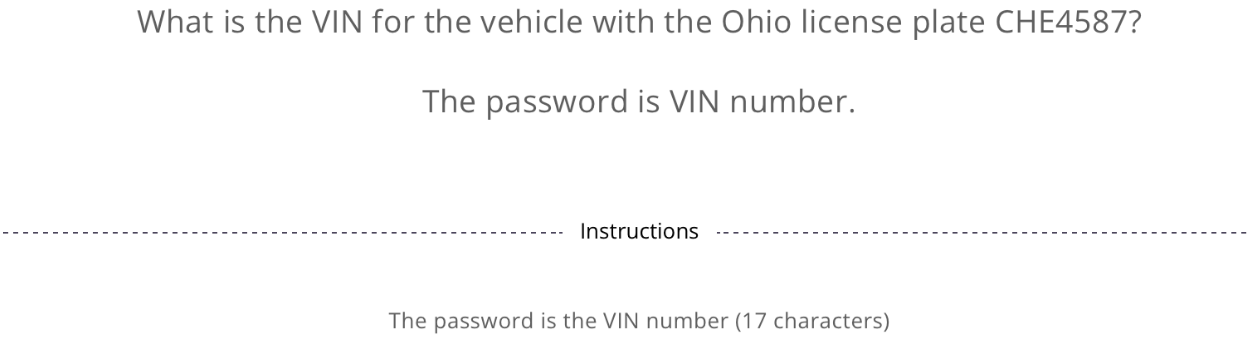
Instructions

Password is the first word from the name of that show.
Password should be lowercase characters.

To view next URL please enter your password below:

https://sourcing.games/game-15/game-15-a4dzk/

- **wicked**



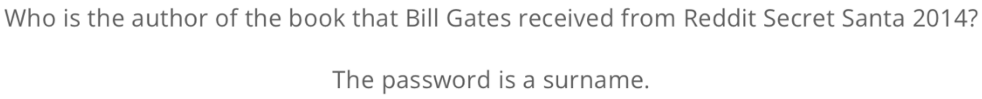
What is the VIN for the vehicle with the Ohio license plate CHE4587?

The password is VIN number.

Instructions

The password is the VIN number (17 characters)

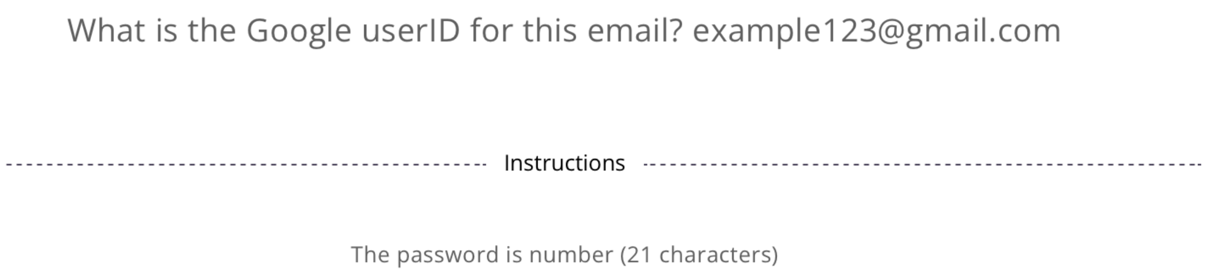
WP0AC2A89GK191430



Who is the author of the book that Bill Gates received from Reddit Secret Santa 2014?

The password is a surname.

Braun



What is the Google userID for this email? example123@gmail.com

Instructions

The password is number (21 characters)

108403360061219275275

ADLP

A combination of manual inspection and automated tools was used to uncover hidden flags on the ADLP website. The following methods proved successful:

1. **HTML Comments:** By inspecting the HTML source code, a flag was found within a comment section:ADLP{HTML_COMMENT_FL4G_G456688}.
2. **CSS Files:** Examining the website's CSS files revealed another flag: ADLP{CSS_HSBUSGYIG569816}.
3. **Robots.txt:** Checking the robots.txt file, which instructs search engine crawlers, exposed a flag:ADLP{ROBOTS_TXT_G569816}.
4. **Sitemap.xml:** The sitemap, a file that lists web pages, contained a flag: ADLP{SITM4PAS_XML_G569816}.
5. **DNSDumpster:** Using the DNSDumpster tool to analyze DNS records associated with the website's domain uncovered a flag: BC{DESCRIPTIVE-DOMAIN-TXT}.
6. **JavaScript Console:** Investigating the JavaScript console within the browser's developer tools revealed a flag:ADLP{JS_CONSOLE_G7894419816}.
7. **Cookies:** Inspecting the cookies stored by the website in the browser led to the discovery of a flag:ADLP{JS_COOKIES_G7894546569816}.