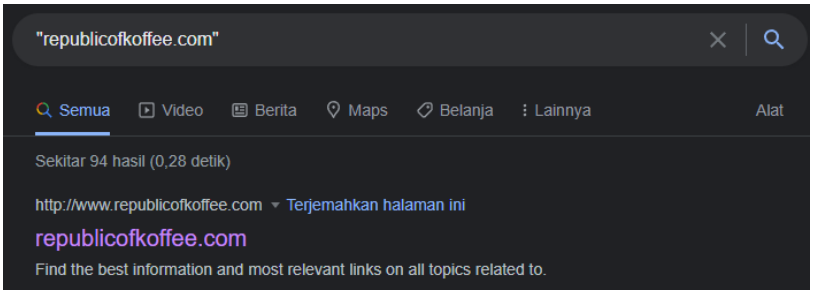
TRYHACKME – WEBOSINT

https://tryhackme.com/room/webosint

Task 1 – When A Website Does Not Exist

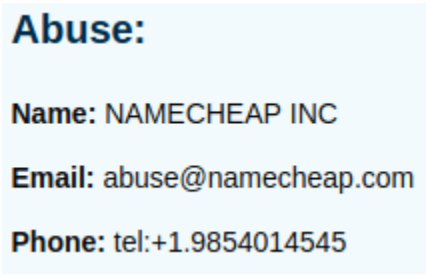


Task 2 - Whois Registration

Pencarian “Whois” adalah bentuk paling dasar dalam melakukan reconnaissance. Whois merupakan layanan internet yang memberikan informasi tentang sebuah domain. Ada banyak sekali tools yang dapat digunakan dalam recon whois, di antaranya https://lookup.icann.org/ , https://who.is/, atau whois (command line di kali linux) dan lainnya.

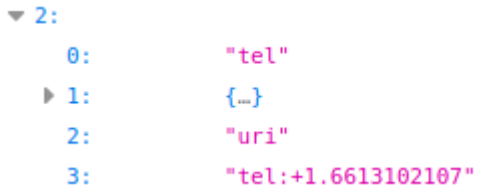
1. **What is the name of the company the domain was registered with?**

   Pada task 2.1 ini, saya menggunakan https://lookup.icann.org/ dalam mencari nama perusahaan dari RepublicofKoffee.com dan jawabannya ialah **Namecheap Inc.**



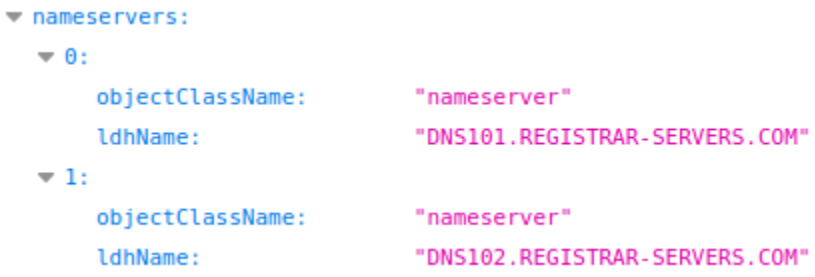
2. **What phone number is listed for the registration company? (do not include country code or special characters/spaces)**

   Pada task 2.2, saya mencari nomor yang digunakan perusahaan dalam melakukan pendaftaran website RepublicofKoffee.com dan ditemukan pada https://rdap.namecheap.com/domain/REPUBLICOFKOFFEE.COM dan jawabannya ialah **tel:+1.6613102107**



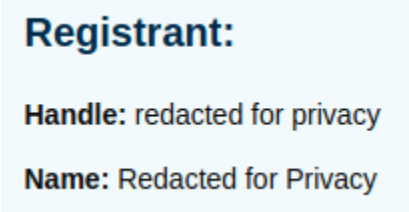
3. **What is the first nameserver listed for the site?**

   Pada task 2.3, saya melakukan pencarian nameserver-1 yang digunakan website RepublicOfKoffee.com. Nameserver merupakan nama dari sebuah web server yang digunakan untuk mengarahkan domain ke server tertentu dan biasanya ditulis dengan format ns1.namasever dan lain-lain. Penamaan tersebut berbeda-beda setiap layanan dan tergantung dengan konfigurasi yang dilakukan. Nameserver-1 yang digunakan adalah **DNS101.REGISTRAR-SERVERS.COM**



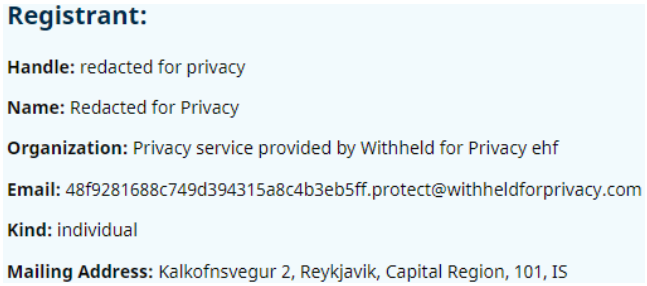
4. **What is listed for the name of the registrant?**

Pada task 2.4 dengan menggunakan hasil pencarian yang sama, saya menemukan bahwa nama yang digunakan untuk mendaftar sebenarnya ialah **"Redacted for Privacy".**

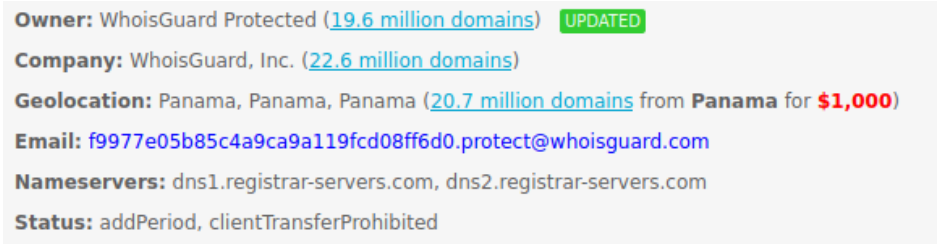


5. **What country is listed for the registrant?**

   Pada task 2.5, saya sedikit kebingunan dikarenakan terkecoh dengan hasil pencarian di https://lookup.icann.org/lookup, dimana hasil pencarian ini menunjukan bahwasanya di Kalkofnsvegur 2, Reykjavik, Capital Region, 101, IS. IS adalah kode negara untuk Iceland.



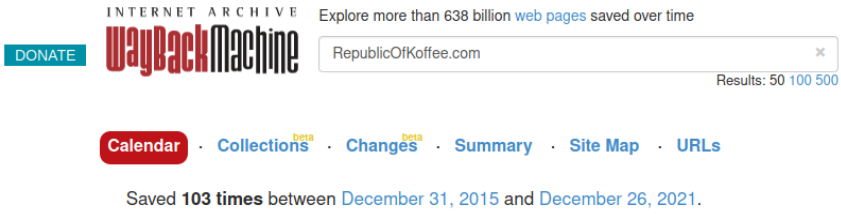
   Namun, saya mencoba melakukan tracking whois history dengan menggunakan https://www.whoxy.com/republicofkoffee.com#history dan didapatkan bahwasanya negara yang terdaftar ialah **Panama.**



Task 3 - Ghost of Websites Past

1. **What is the first name of the blog's author?**

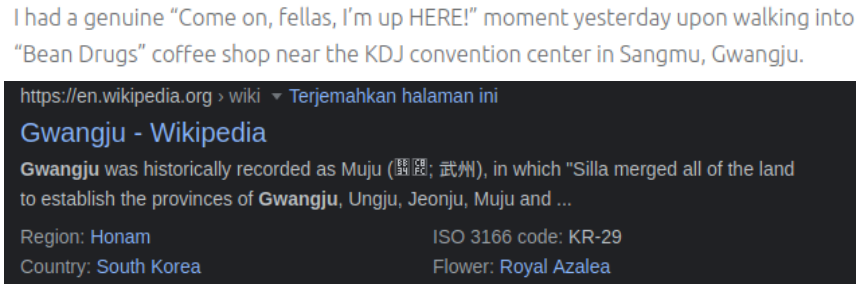
   Pada task 3.1, saya menggunakan Wayback Machine untuk melihat artefak masa lalu dan ditemukan bahwa RepublicOfKoffee.com menunjukan 103 tangkapan dari rentang 31 Desember 2015 – 26 Desember 2021.



Berdasarkan data tersebut, saya mencoba mencari penulis pertama blog tersebut dan jawabannya ialah **Steve.**

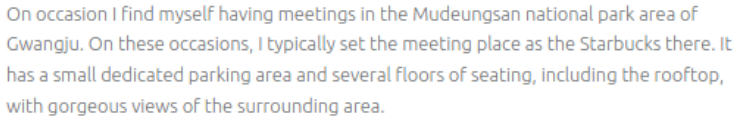
2. **What city and country was the author writing from?**

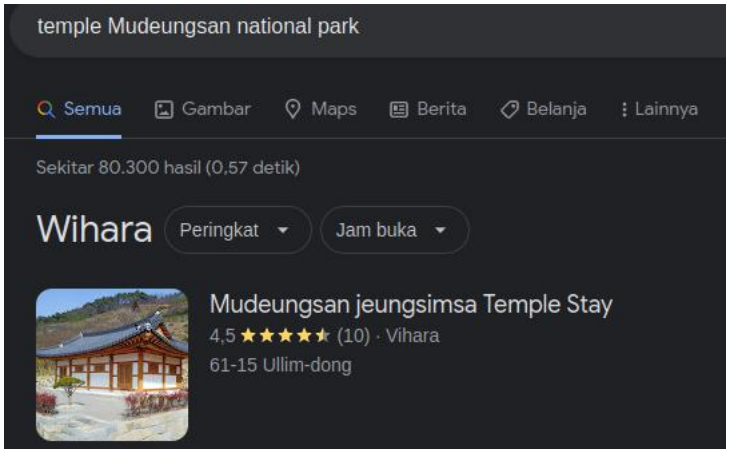
   Pada task 3.2, saya menemukan bahwa kota dan negara mana penulis menulis ialah di **Gwangju, South Korea.**



3. **[Research] What is the name (in English) of the temple inside the National Park the author frequently visits?**

   Pada task 3.3, saya mencari candi yang berada di dalam Taman Nasional Mudeungsan yang sering penulis kunjungi dan jawabannya ialah **Jeungsimsa Temple.**





Task 4 - Digging Into DNS

1. **What was RepublicOfKoffee.com's IP address as of October 2016?**

   Pada task 4.1, saya menggunakan tools https://viewdns.info https://viewdns.info/iphistory/?domain=republicofkoffee.com untuk menemukan history IP Address pada Oktober 2016 dan jawabannya ialah **173.248.188.152**

ViewDNS.info > Tools > **IP History**

Shows a historical list of IP addresses a given domain name has been hosted on as well as where that IP address is geographically located, and the owner of that IP address.

Domain (e.g. *domain.com*):

RepublicOfKoffee.com GO

IP history results for RepublicOfKoffee.com.

IP Address	Location	IP Address Owner	Last seen on this IP
99.83.154.118	Seattle - United States	Amazon.com	2022-01-09
192.64.119.238	Los Angeles - United States	Namecheap	2022-01-01
69.64.147.10	Seattle - United States	Rightside Group LTD	2017-07-30
173.248.188.152	Denver - United States	MDDHosting LLC	2016-10-03
173.248.187.2	Denver - United States	MDDHosting LLC	2016-02-01

2. **Based on the other domains hosted on the same IP address, what kind of hosting service can we safely assume our target uses?**

   Pada task 4.2, saya mengacu dari hasil IP History dan jawabannya ialah **Shared.** Shared hosting adalah layanan hosting dimana sebuah account hosting diletakan bersama-sama beberapa account hosting lain dalam satu server yang sama, dan memakai services bersama-sama.

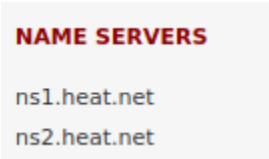
3. **How many times has the IP address changed in the history of the domain?**

   Pada task 4.3, saya semula menjawab 5 dan ternyata salah. Kemudian iseng jawab **4** ternyata benar dan sampai sekarang juga masih bingung ☺ kenapa bisa 4.

Task 5 - Taking of The Training Wheels

1. **What is the second nameserver listed for the domain?**

Pada task 5.1 jawabannya ialah **ns2.heat.net** https://www.whoxy.com/heat.net



2. **What IP address was the domain listed on as of December 2011?**

   Pada task 5.2 dengan menggunakan https://viewdns.info/iphistory/?domain=heat.net, saya menemukan IP Address pada Desember 2011 ialah **72.52.192.240**.

3. **Based on domains that share the same IP, what kind of hosting service is the domain owner using?**

   Pada task 5.3 dengan menggunakan Reverse IP Lookup untuk menemukan layanan yang digunakan dan jawabanya ialah **Shared.**

Reverse IP results for heat.net (208.117.87.195)

There are 49 domains hosted on this server.
The complete listing of these is below:

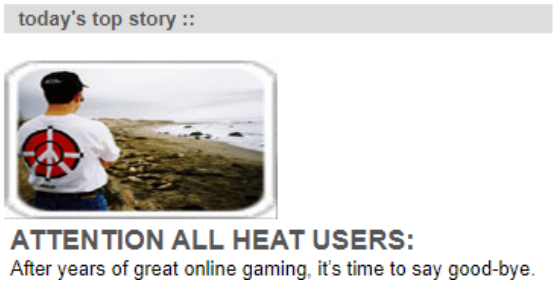
Domain	Last Resolved Date
acefest.com	2022-01-08
addonplanet.com	2022-01-08
astronomy-pictures.net	2022-01-08
blackberryfaq.com	2022-01-08
blackberryforums.com	2022-01-08
canon-30d.com	2021-12-04
ccmostwanted.com	2022-01-08
collectorcarsforsale.com	2022-01-08
creativenoise.net	2022-01-08
dragcars.com	2022-01-08
egyptartsite.com	2022-01-08
electronic-circuits-diagrams.com	2022-01-08
fast-autos.net	2022-01-08

4. **On what date did was the site first captured by the internet archive? (MM/DD/YY format)**

   Pada task 5.4, saya menggunakn wayback machine untuk menemukan captute pertama pada website heat.net dan jawabannya ialah **06/01/97** (https://web.archive.org/web/2021*/heat.net).

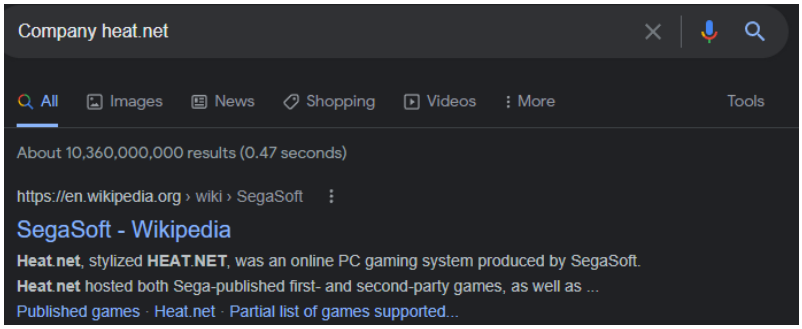
5. **What is the first sentence of the first body paragraph from the final capture of 2001?**

   Pada task 5.5, saya mencari kalimat pertama pada paragraf yang di tulis pada tahun 2001 dan jawabannya ialah **After years of great online gaming, it's time to say good-bye** (https://web.archive.org/web/20010706211455/http://www.heat.net/)



6. **Using your search engine skills, what was the name of the company that was responsible for the original version of the site?**

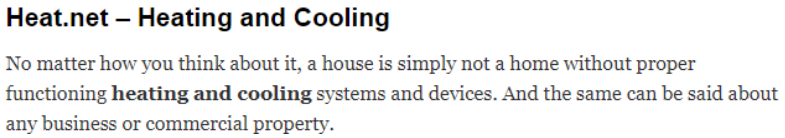
   Pada task 5.6, saya menemukan bahwasanya perusahaan yang bertanggung jawab terhadap original versi situs heat.net ialah **SegaSoft.**



7. **What does the first header on the site on the last capture of 2010 say?**

   Pada task 5.7, saya mencari header pertama yang terdapat pada tangkapan tahun 2010 dan jawabannya ialah **Heat.net – Heating and Cooling**

   https://web.archive.org/web/20101230184331/http://www.heat.net/



Task 6 - Taking A Peek Under The Hood Of A Website

1. **How many internal links are in the text of the article?**

   Pada task 6.1, saya menemukan bahwa ada **5 internal links** yang terdapat pada artikel http://www.heat.net/36/need-to-hire-a-commercial-heating-contractor/ sebagai berikut:

- http://www.heat.net/39/save-money-on-your-commercial-heating-bill/
- http://www.heat.net/32/how-do-heating-and-cooling-systems-work/
- http://www.heat.net/36/need-to-hire-a-commercial-heating-contractor/
- http://www.heat.net/
- http://www.heat.net/15/cutting-your-heating-costs-without-emptying-your-wallet/

2. **How many external links are in the text of the article?**

   Pada task 6.2, saya menemukan bahwa ada **1 External links** yang terdapat pada artikel http://www.heat.net/36/need-to-hire-a-commercial-heating-contractor/ ialah https://purchase.org/ .

3. **Website in the article's only external link (that isn't an ad)**

   Pada task 6.3 jawabannya ialah **purchase.org**

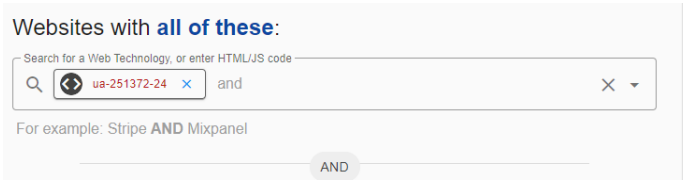
4. **Try to find the Google Analytics code linked to the site**

   Pada task 6.4, saya mencoba menemukan Google Analytics dengan cara klik kanan lalu view page source (ctrl+u) dan menemukan bahwa GA-nya ialah **UA-251372-24.** view-source:http://www.heat.net/36/need-to-hire-a-commercial-heating-contractor/

```
<script type="text/javascript">
window.google_analytics_uacct = "UA-251372-24";
</script>
```

5. **Is the the Google Analytics code in use on another website? Yay or nay**

   Pada task 6.5, saya mencoba mencari apakah GA UA-251372-24 sudah digunakan oleh website lain dengan menggunakan https://www.nerdydata.com/ dan jawabannya ialah **nay (tidak).**



6. **Does the link to this website have any obvious affiliate codes embedded with it? Yay or Nay**

   Pada task 6.6, saya mencari apakah tautan situs web http://www.heat.net/36/need-to-hire-a-commercial-heating-contractor/ memiliki kode aflisiasi yang tertanam di dalamnya dan jawabannya ialah **nay (tidak).**

Task 7 - Final Exam: Connect the Dots

1. **Use the tools in Task 4 to confirm the link between the two sites. Try hard to figure it out without the hint**

   Pada task 7.1 (Final Exam), saya menggunakan tools viewdns.info untuk mengkonfimasi link antara dua situs yaitu heat.net dan purchase.org dan ditemukan jawabannya **yaitu Liquid Web, L.L.C**

IP history results for heat.net.
==========

IP Address	Location	IP Address Owner	Last seen on this IP
208.117.87.195	Reston - United States	Atlantic.Net - Ashburn	2022-01-09
74.116.2.147	United States	Express Web Systems	2019-06-19
72.52.192.240	Lansing - United States	Liquid Web	2011-12-19

IP history results for purchase.org.
==========

IP Address	Location	IP Address Owner	Last seen on this IP
172.67.197.177	United States	Cloudflare, Inc.	2022-01-08
104.21.92.201	United States	Cloudflare, Inc.	2022-01-08
104.27.185.115	United States	Cloudflare, Inc.	2021-01-14
104.27.184.115	United States	Cloudflare, Inc.	2021-01-14
206.196.110.108	St Louis - United States	Rose Web Services LLC	2017-11-03
67.43.1.187	Lansing - United States	Liquid Web	2013-04-19
72.52.193.127	Lansing - United States	Liquid Web	2012-11-16

Terima kasih telah membaca Writeup TryHackMe Room Webosint, Semoga bermanfaat bagi semuanya. See you next time, Happy Learning ☺