**C16406984**

**Arthur Coll**

Q1.

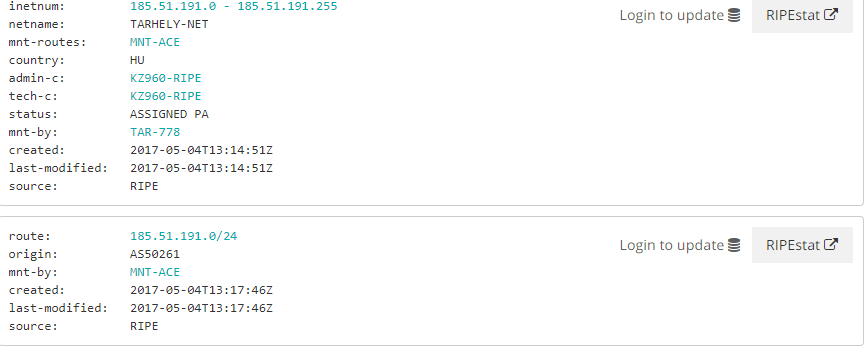
In my Inbox I received an email purporting to be from Bill Gates offering me the chance to get rich quick.  
Using Gmail, I then opened the raw contents of the Email and examined the headers below, I identified the Client IP of the sending mail server 185.53.191.58



To identify the ISP of this client IP I preformed a whois search on the ip address, using who.is

This reported that the IP range in question was managed by the RIPE NCC, the European registar meaning the IP range was probably based within Europe.

I then visited RIPE’s website and used their who.is tool to get the following output, which indicates the range was registered to Tarherly a Hungarian ISP.

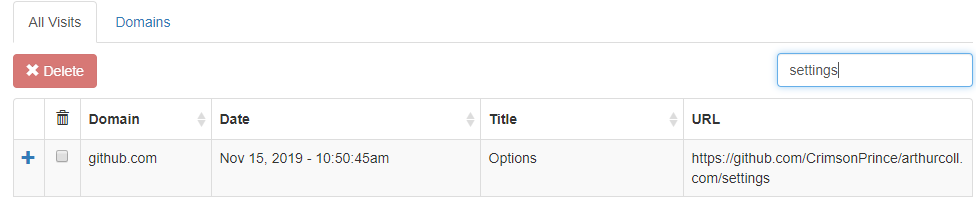


Q2.

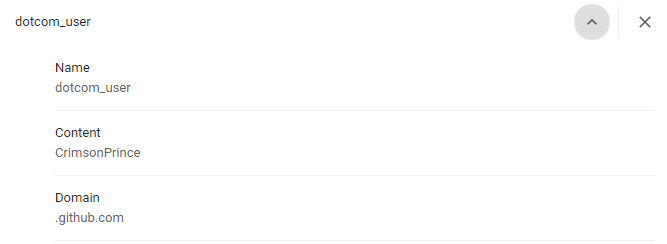
Using WebHistorian I determined that Github.com was one of my most visited sites.

Running the website profiler, I determined that in the period of Sep 22, 2019 to: Nov 15, 2019, I visited github.com 359 times.

To Determine a specific user that visited the site, I filtered the URL’s for those with “settings” within then. I then looked for repositories and I identified the user from the user who is the repository owner as seen in the image below. In this case it was “CrimsonPrince” and this will be further validated with cookies later.



Following this I then used Chrome Settings to view the cookies registered to Github.com, there was 10 cookies registered and by looking into the user cookie, I confirmed that the user CrimsonPrince had been logged in as seen below.



To identify the temporary files stored by chrome, I used the chrome cache view tool provided by nirsoft because chrome has removed native viewing of the cache.

This produced over 259 temporary files, a mixture of images, javascript files, css files and regularly visited pages.

