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

```
Delivered-To: arthur1coll@gmail.com
Received: by 2002:a92:1586:0:0:0:0:0 with SMTP id 6csp2726993ilv;
        Sun, 27 Oct 2019 17:57:25 -0700 (PDT)
X-Google-Smtp-Source: APXvYqxf8KtBGIs2Son9Hm9s+FOYjwo58+UObD33Vev9G7FfeVtct99uTfx0wgCEec9BMCAVdFm3
X-Received: by 2002:a17:90a:9293:: with SMTP id n19mr2257381pjo.67.1572224245122;
        Sun, 27 Oct 2019 17:57:25 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1572224245; cv=none;
        d=google.com; s=arc-20160816;
        b=zmY7zzDbR3q73Mncjb8ol5Sh1yiUQb6iPsFPYgjcMhHT2njwekMQj5o6r1rB2XS/j1
         ioH/TpotD9MaATfSNsipIM8sJ28/bMNKmoIe5xqCj46b5j8CgC8XBzaIyWzuaTK8vYtq
         ppL08Tu4oXodSAz1ZqFERPfdppVJQV57YAnqSOcNEePIYZllpdAyiHsdtFd4VMY1nNXX
         eU+b6u7Ah1YqaBp7F+yxUaCURz3y4MqavUPJyOYKas+ldhkt/BlVVOMN2748kM92oGpK
         EX8AykchvF7LlZu7bqRqDr3Ve8HQSvtPid9vrgHKdNCL6KRWxv/jTbBfYfcdQI0p8RA0
         FXMg==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
        h=content-transfer-encoding:message-id
         :planetoid-birefringent-waveform:to:strayed-betterments-berkelium
         :from:date:subsidy-fragmenting:playful-masochists-mayor:subject
         :whatever-pandemonium:mime-version;
        bh=SZgVci57NgFvHjN4PLhH6er2sk12UWcajPyPbFZHlSg=;
        b=hySrJ0Q8v5dz9z9OvSza9w6EOgSQxYwmLRHPcYryEA/S2Q4p6RtROIfFIZ89q+CqM9
         c/4psZpGKwllNL5amA+vpUqnMh6i1Fkg8ZXCSl/Y1xblfX8kS9sFArUsFf5L1xDtPUvs
         jpqKyHtB7W+QO10j6KRElgVArhXkVoluzA8DEb5q/61WCDI9phjbBeeuGFzp5Vri0Q3a
         BbUQlkCjw0oOY2ejxKpv70zRyoiwR6+wnuNkS8qgO7dM3+Olgf9S/D8Vkk6iQM5g8jfA
         dQS9TSa5MKovaipcrLquSIPHzpSxxODon7c/Tl/FjMjpsGybBWr1XruFqmTAetEaqMjk
         xqfg==
ARC-Authentication-Results: i=1; mx.google.com;
       spf=neutral (google.com: 185.51.191.58 is neither permitted nor denied by best guess record for domain of cellule.marches@ch-pierrefeu.com) smtp.mailfrom=cellule.marches@ch-
pierrefeu.com
Return-Path: <cellule.marches@ch-pierrefeu.com>
Received: from thfiftyeight.tarhely.eu (thfiftyeight.tarhely.eu. [185.51.191.58])
        by mx.google.com with ESMTP id s24si10476019pgn.18.2019.10.27.17.57.23
        for <arthur1coll@gmail.com>;
        Sun, 27 Oct 2019 17:57:25 -0700 (PDT)
Received-SPF: neutral (google.com: 185.51.191.58 is neither permitted nor denied by best guess record for domain of cellule.marches@ch-pierrefeu.com) client-ip=185.51.191.58;
Authentication-Results: mx.google.com;
       spf=neutral (google.com: 185.51.191.58 is neither permitted nor denied by best guess record for domain of cellule.marches@ch-pierrefeu.com) smtp.mailfrom=cellule.marches@ch-
pierrefeu.com
MIME-Version: 1.0
Whatever-Pandemonium: c11354429586
Subject: Notification
Playful-Masochists-Mayor: collecting
Subsidy-Fragmenting: D79FE1F54869919
Date: Mon, 28 Oct 2019 01:57:24 +0000
From: Gabriel Mixon Support <cellule.marches@ch-pierrefeu.com>
Strayed-Betterments-Berkelium: 3278FD19F86C9E
To: "arthur1coll@gmail.com" <arthur1coll@gmail.com>
Planetoid-Birefringent-Waveform: 4288
Message-ID: <12143fcb.2feba.68e715@ch-pierrefeu.com>
Content-Type: text/html; charset="UTF-8"
Content-Transfer-Encoding: 7bit
```

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.

Login to update RIPEstat

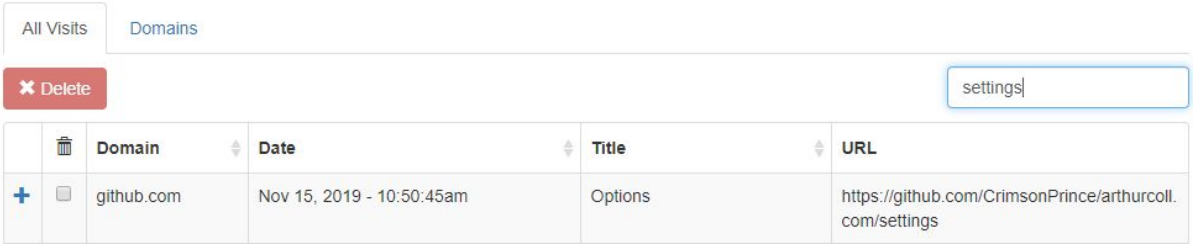
```
inetnum:        185.51.191.0 - 185.51.191.255
netname:        TARHELY-NET
mnt-routes:     MNT-ACE
country:        HU
admin-c:        KZ960-RIPE
tech-c:         KZ960-RIPE
status:         ASSIGNED PA
mnt-by:         TAR-778
created:        2017-05-04T13:14:51Z
last-modified:  2017-05-04T13:14:51Z
source:         RIPE
```

Login to update RIPEstat

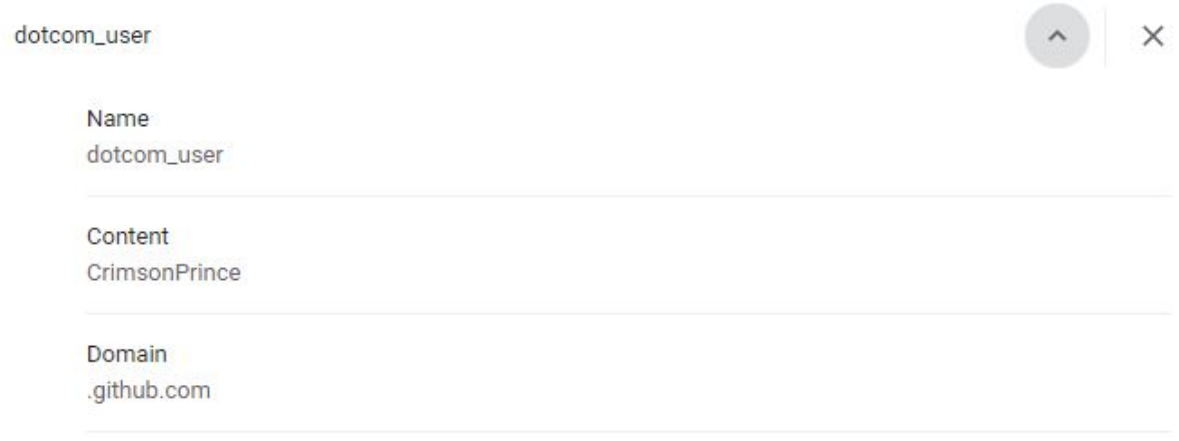
```
route:          185.51.191.0/24
origin:         AS50261
mnt-by:         MNT-ACE
created:        2017-05-04T13:17:46Z
last-modified:  2017-05-04T13:17:46Z
source:         RIPE
```

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.