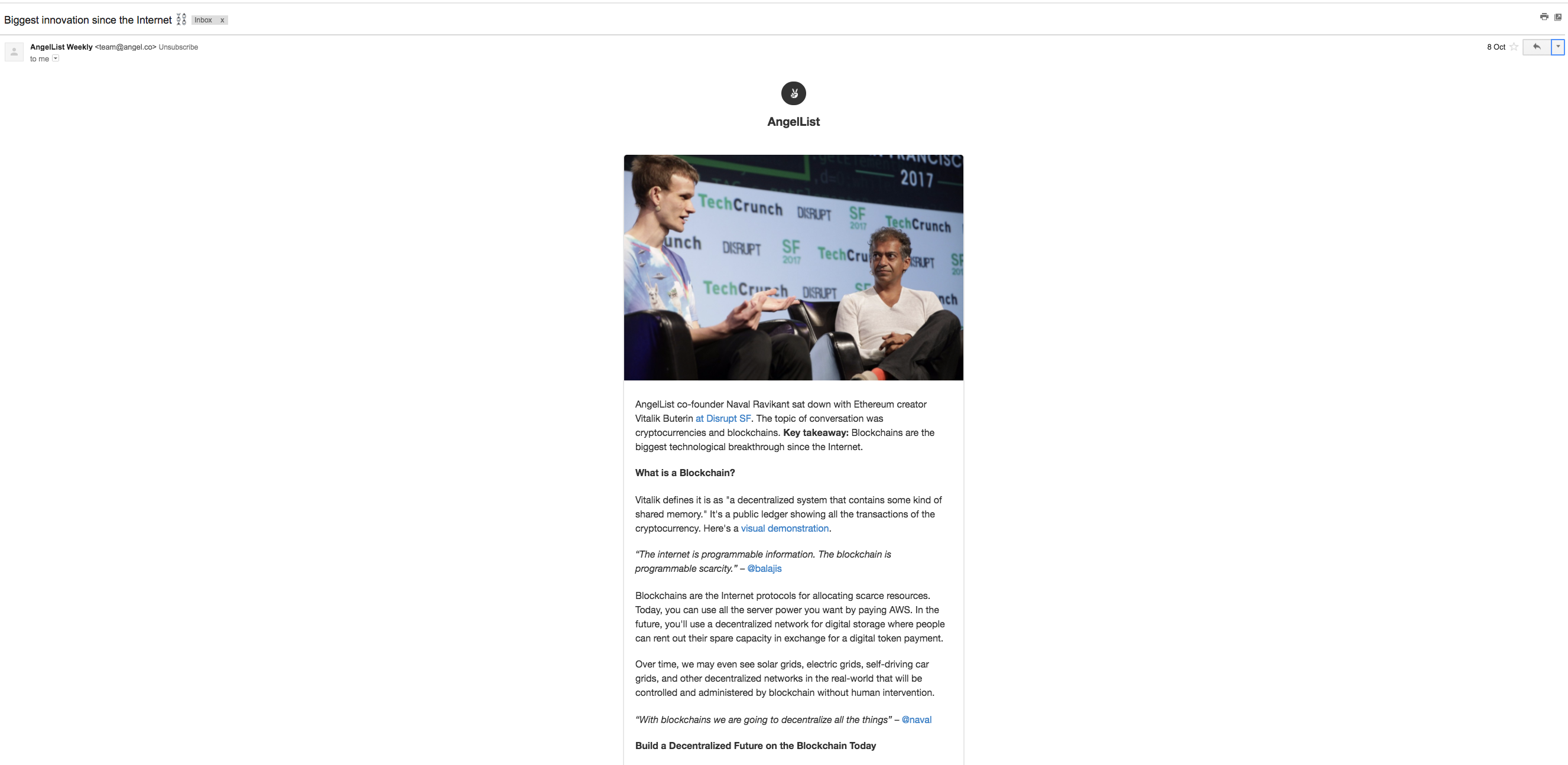
**Question 1:** Find an example of spam on one of your machines. Extract copies of the headers and analyse the message. See if you can figure out the originating server and if possible the ISP that initially forwarded the message.

**Answer:** I had no spam e-mails because I delete them all, so I picked one from AngelList.com. The e-mail was about one of the talks given by entrepreneurs about block chains.



By viewing the e-mail headers, I was able to find two separate headers containing IP addresses. They were as follows:

Received-SP: ……… designates 167.89.15.5 as permitted sender …… (E-mail sending SaaS)

Received: from angel.co …… [54.176.222.40] ……. (Website IP address)

Using the site <https://www.iplocation.net/> I was able to determine the location and ISP’s of both the IP addresses.

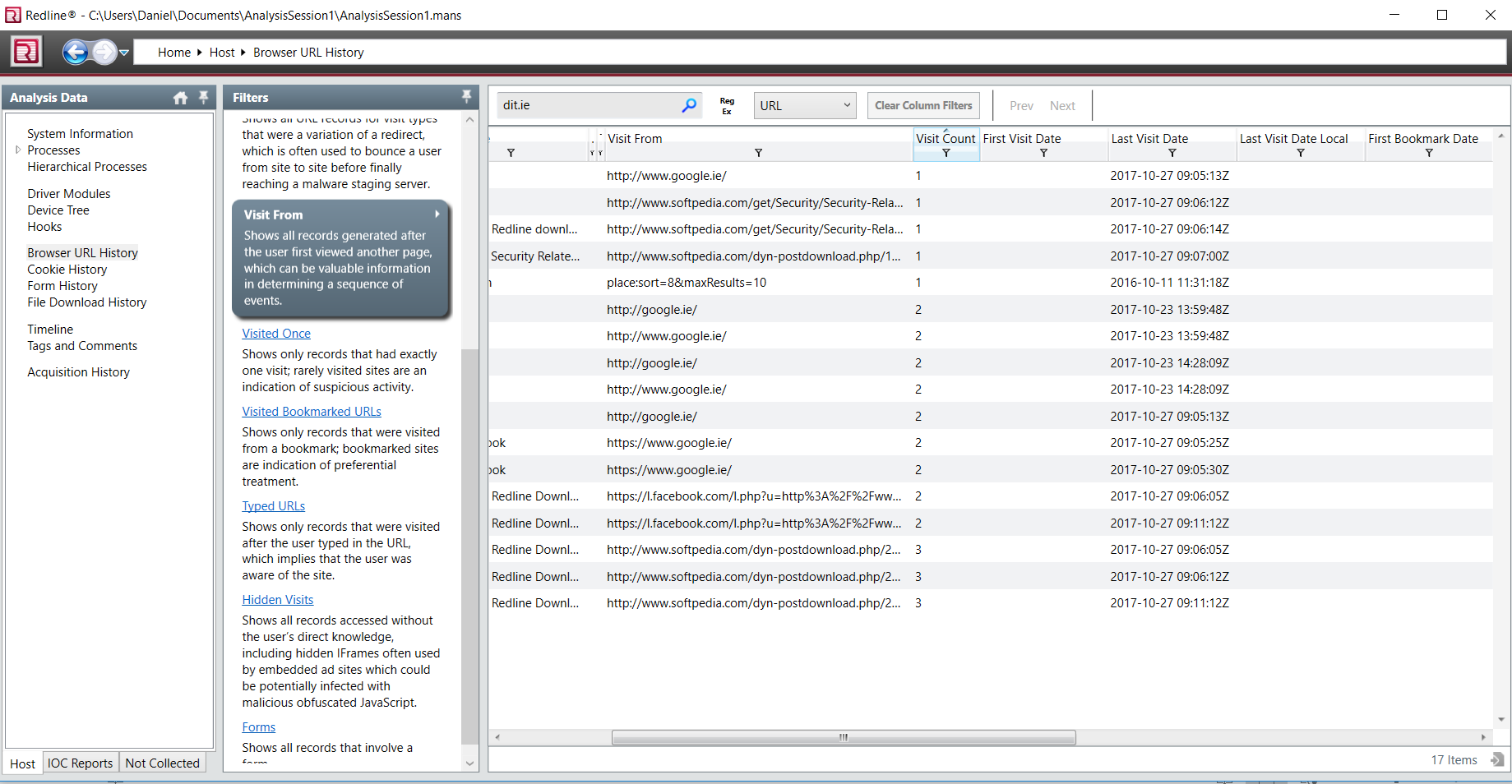
|  |  |
| --- | --- |
| 167.89.15.5: | 54.176.222.40: |
| ../../../../../Desktop/download.png | ../../../../../Desktop/download%20(1).png |

**Question 2:** Download a copy of Web Historian, and run it against the Web History on a machine that has had internet access for some time. Locate a Website that seems to get a lot of traffic, and run the website profiler report against it. See if you can identify a specific user who has accessed the site. How many cookies were stored on a system by the site? How many temporary internet files were stored by the site?

Web Historian was merged into Redline a few years ago, so we can still run an analysis on the pc. It can be downloaded at:

<http://www.softpedia.com/get/Security/Security-Related/Mandiant-Redline.shtml>

By using redline, we can scan the whole pc and include browser history in the scan. (As I am using bootcamp on my mac to run windows, it will only show the history from the current session – see image below). It will show things like the visit date and time, the url and number of visits on the site.



Redline can also show cookies associated with different websites and a whole host of info about them.

