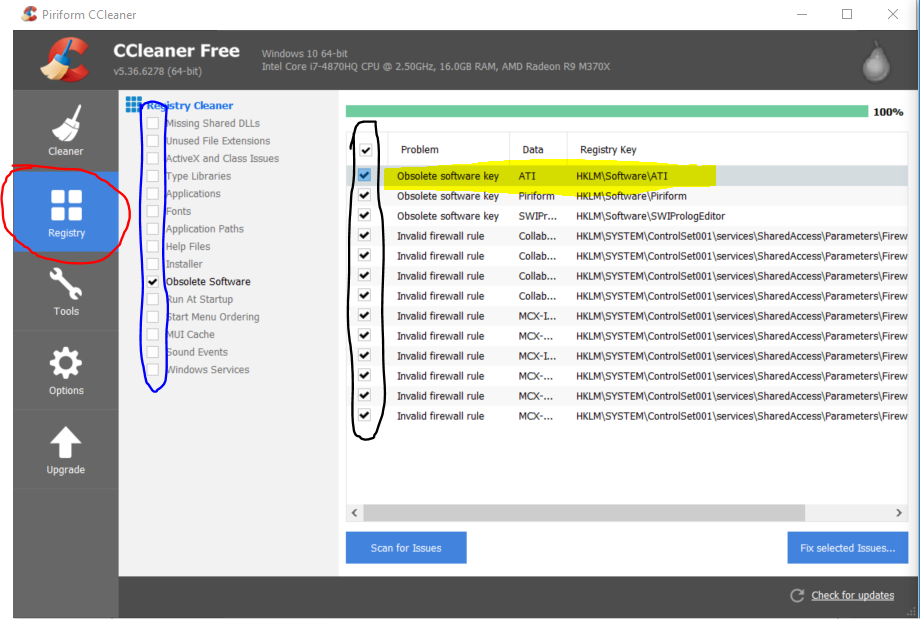
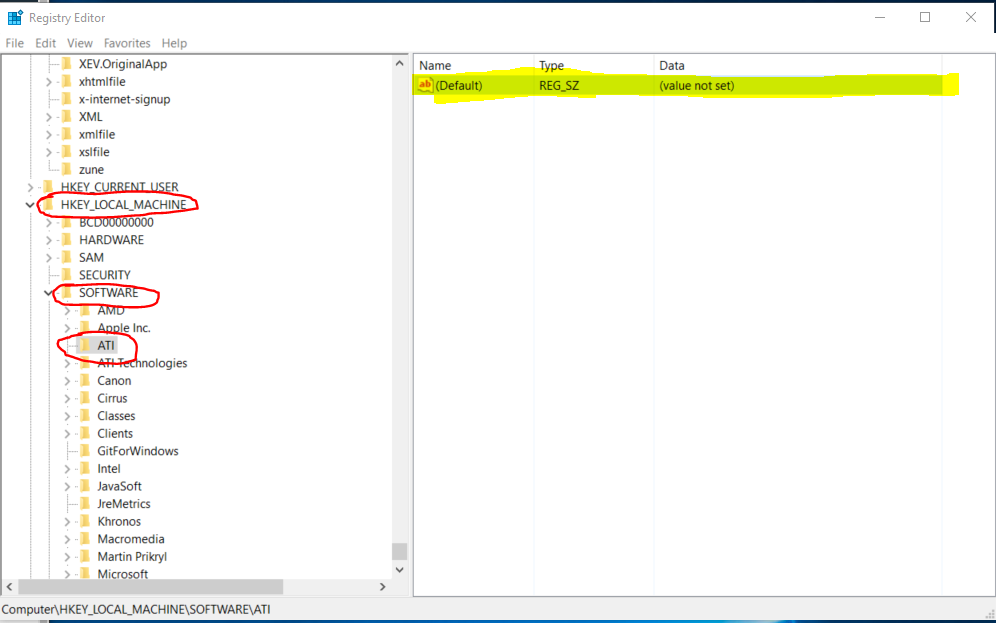
**C14337041 – Daniel Tilley - Assignment**

**Question 1:** CCleaner offers use the ability to delete a lot of things from are pc’s. One of the features it provides is the option to scan the registry for entries which present a problem. Once it has scanned the registry, the user is free to do as they please with the results. They may wish to delete and entry, update it or do nothing with it at all. In the image below, we can see CCleaner has scanned my registry for obsolete software.



Once the scan had finished, it returned a few results. Several of the entries related to invalid firewall rules, whilst the others related to obsolete software keys. The user can simple check the boxes (in black) to deal with and then can click the “fix selected items” to allow to software to “work its magic”. However, if you would rather have more control over what happens to the entry, you can simply right click on it and click “open in regedit”. See the highlighted result opened in the image below.



One regedit is opened, you can edit or delete the file highlighted above by right clicking on it and selecting either “Modify..” or “Delete”. Alternatively, you can leave it as is.

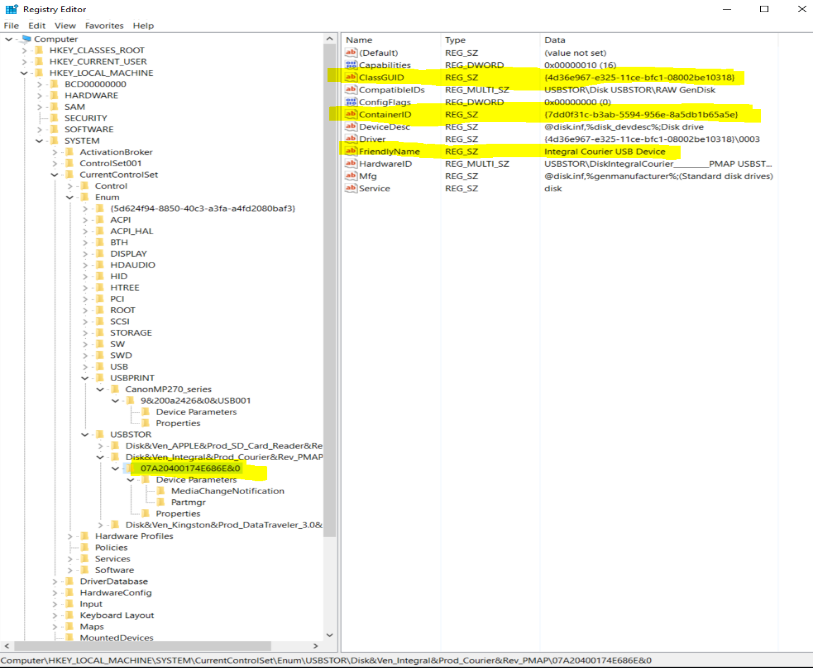
**Question 2:** By using the following pages:

<https://www.magnetforensics.com/computer-forensics/how-to-analyze-usb-device-history-in-windows/>

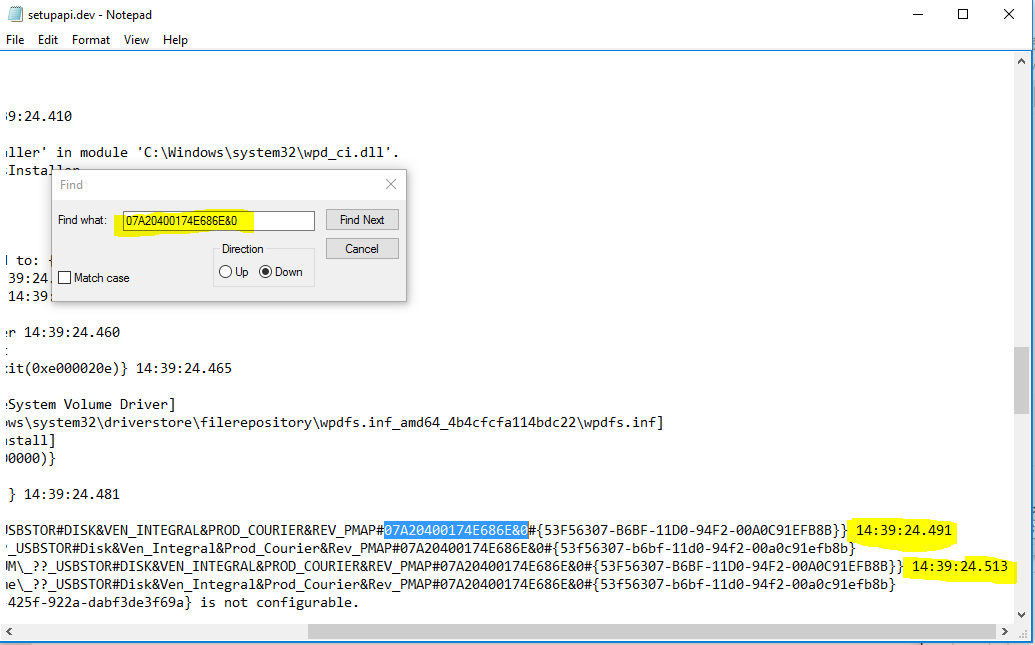
<https://www.forensicmag.com/article/2012/08/windows-7-registry-forensics-part-6>

I was able to locate several pieces of information about a usb storage device I had plugged into my mac (running windows via bootcamp). All the info acquired is shown in the image below and was found in the following hive:

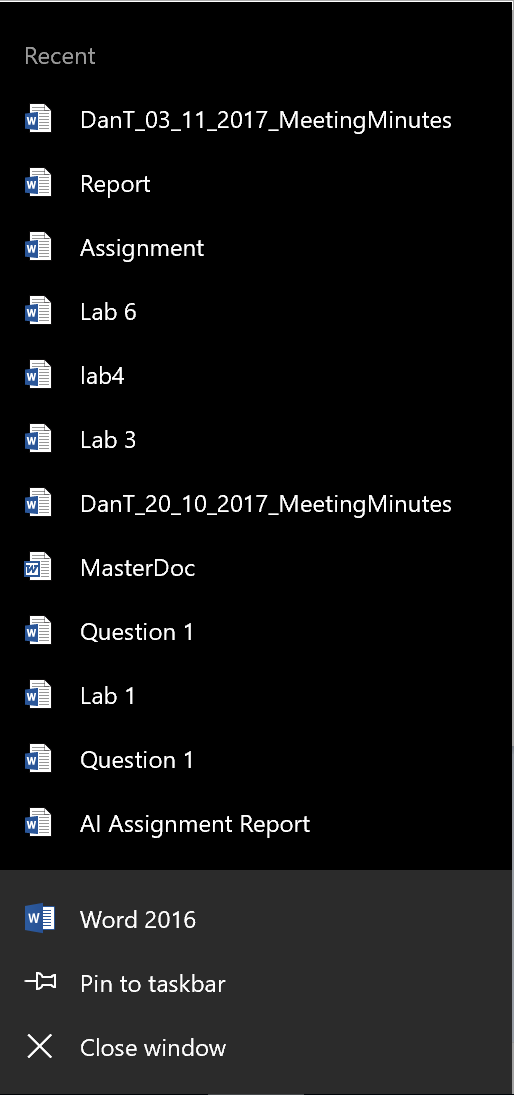
HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR



I was unable to locate dates in the registry however, using the serial key of the usb device, I was able to find dates in the following setup file: C:\Windows\INF\setupapi.dev



**Question 3:** Windows jump lists can be very helpful when it comes to forensics. They can tell us as investigators many things about a person’s behaviour on a pc. For example, see below the ui equivalent of a jump list used in Microsoft word. From this list I am able to determine what documents were worked on last from my pc. This can be helpful as we may need to know if a user was working on specific files which may aid in a forensic investigation. It also allows the investigator to build a trail of what documents the user has accessed and when the accessed them.

****

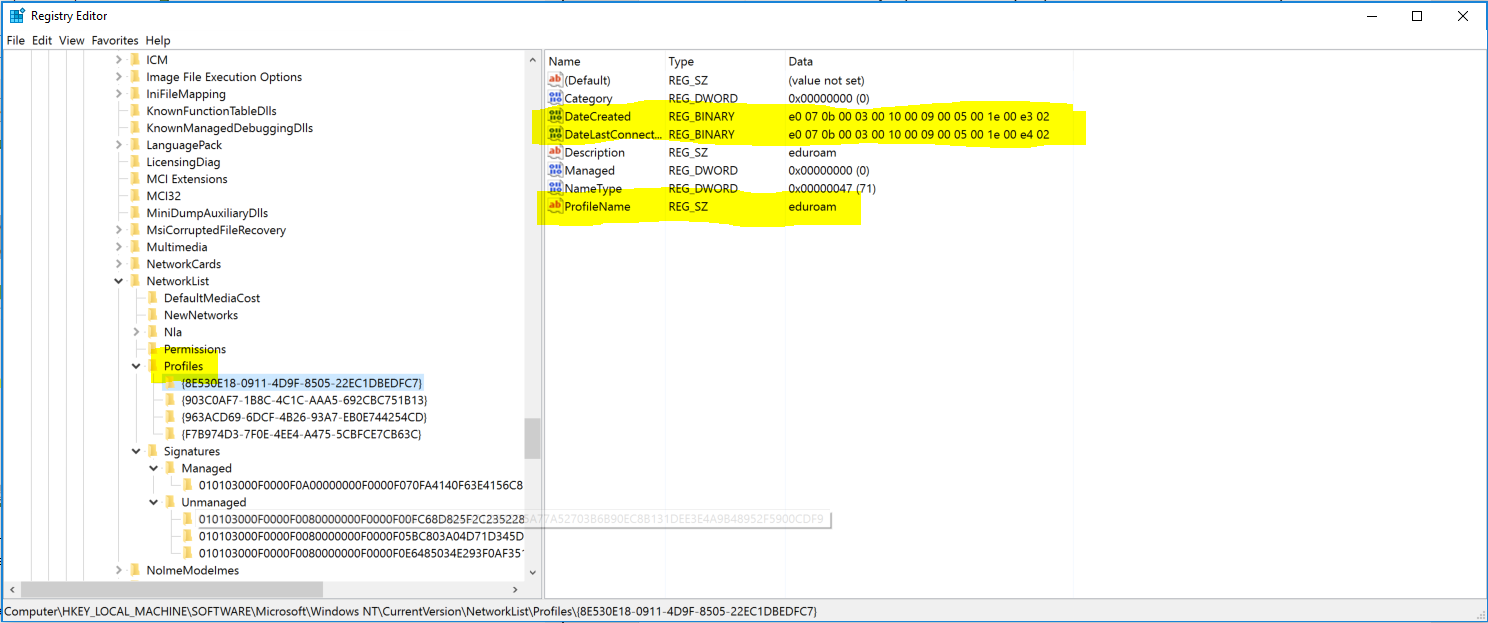
**Question 4:**

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles

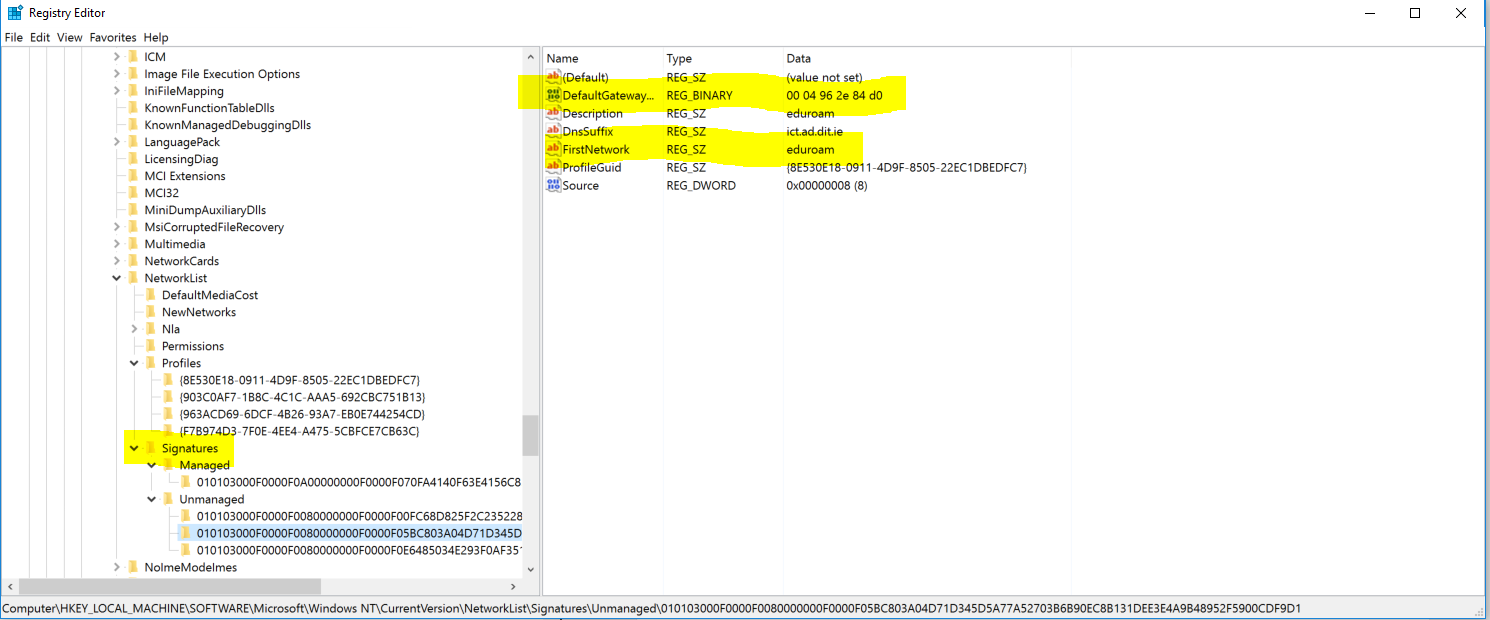
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures

By searching in the two hives listed above I was able to locate client side data (such as connection dates, ssid which the user connected to and so on) and also server side data (router mac address, ssid, dns suffix etc) for the eduroam wifi in college.

Client Data:

****

Server Data:

****

**Question 5:** It is possible to hide data in the registry. A very basic example would be if you wished to hide a mobile phone number or address of “an associate” so that you wouldn’t forget it.

For my example I created a fake phone number (made it up), reversed it so it was back to front and changed it into a hex format. 0860294532 -> 2354920680 -> 32333534393230363830

Next, I picked a random folder in the software hive (any folder was as good as the other), created a new string and put the reversed hex number into it. I think it’s as good a place to hide something as any just for the simple reason that why would anyone put anything in a registry entry for printer software? For that reason also, it could be considered “hidden” unless you knew you were looking for it or you already knew it was there.

