**Forensic Assignment 2**

Student Name: Jonathan Riordan

Student ID: C13432152

**Part 1. Ad-Hoc**

Ad-hoc is a network sharing abilities on operating system such as Linux, Windows and Mac OS. It allows the host machine to share its internet connection to other devices and doesn't require an extra router.

An ad hoc network can be created on most Operating systems such as Mac OS, Windows and Linux. Once a network is created, other devices can connect to it if they select the network name. Tools used to analyse a network or local network are advanced IP scanner, IP scanner and Angry IP scanner. The tool IP Scanner allows an investigator to scan a local network and information such as discovered user devices can be retrieved. For each device, the IP address, the MAC address, the manufacturer, the DNS and the last seen on the local network can be retrieved. This can be valuable information to an investigator for scanning a network to identify all the devices connected. This tool allows has the function for each device on the network to scan open ports that I believe that device is using. The tool also has the functionality to ping a device and an investigator can check to see whether or not that ping was successful or not. This can be used to see if the device is still connected to the network.

As seen below in the image, here is an IOS device connected to the network.



The information returned to an investigator is important because it allows them to identify all the devices connected to the internet and the last time a device was connected. If someone was trying to hide a device, these types of tools will inform the investigator that there is a device a person has used that has been connected to the remote network.

From using this tool, I was able to monitor my local network and identify the devices. I was able to test to see if these devices were still on the network as this application allowed me to ping them. The only disadvantage an investigator will find with using this tool is that they are unable to see files or pieces of data that is been transferred between devices. The investigator will be able to see the devices but the actual activity of those devices will be unknown.

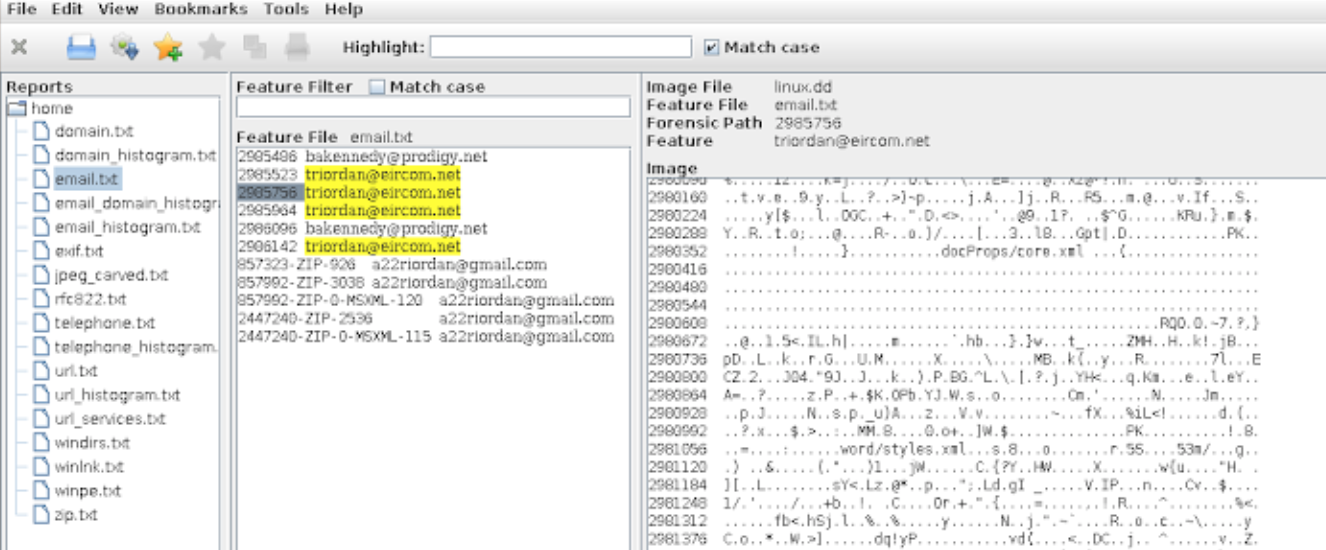
**Part 2. Caine**

Caine is a forensic operating system that allows investigators to use multiple tools that are provided on the OS to inspect peripheral drives, local and remote devices. Caine comes with Network tools such as Wireshark and Zenmap. It also has the ability to provide images of devices such as USB with the use of Guymage. Once an image has been created, they can be analysed using Autopsy, XALL or Bulk Extractor.

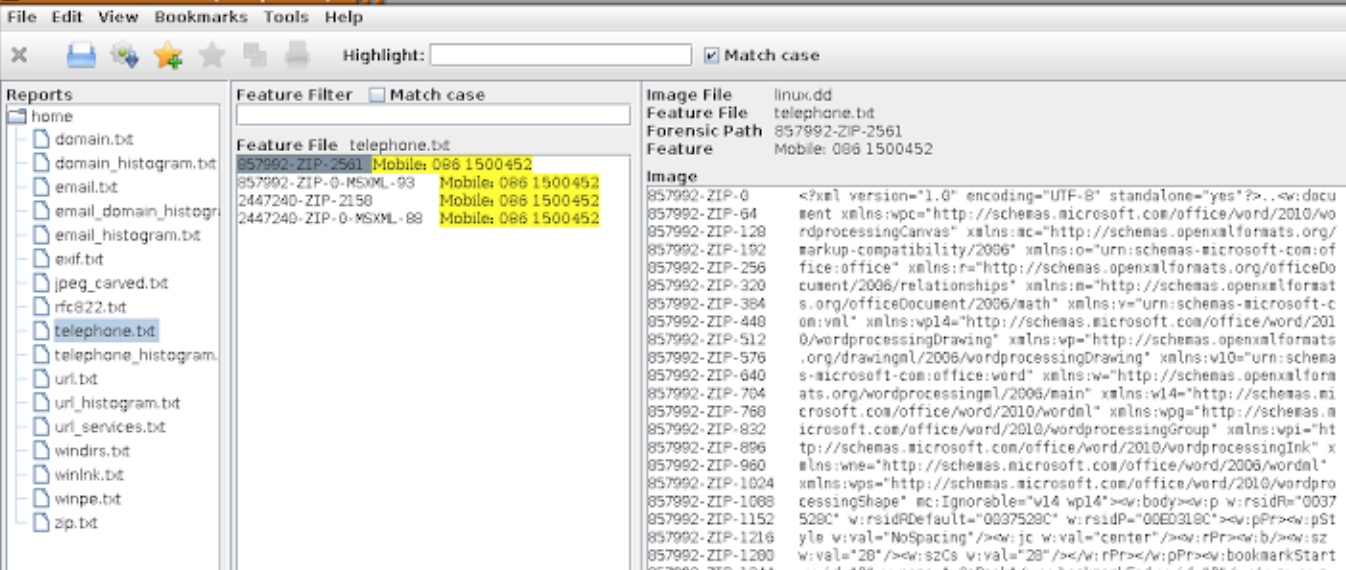
Guymager is a forensic image tool that I used to create images of devices such as a USB. It can also be used to create an image of a hard disk.

Once these images have been created, I was able to analyse the the data using a tool called Bulk Extractor. Using the forensic image created from Guymager, I was able to run bulk\_extractor against the image. The finding to an investigator are amazing. This tool retrieved information such as phone numbers, emails.

As seen from the image below, all the emails that were contained in the image file from the USB stick were retrieved. The investigator can also use this tool to retrieve all the website URL’s and jpeg within the image file. Selecting on an email as seen in the image bellow will also display where that email came from, such as the name of the file.



The below image also displays information about telephones been returned to an investigator.



This is a powerful tool, it can be used on hard drives as well. It can be useful in returning vast amounts of information or information that people might try to hide from an investigator. The filtering mechanisms is great and is simple to use. The tool also provides the ability to export the results as well.

**Part 3. Sleuthkit + Autopsy**

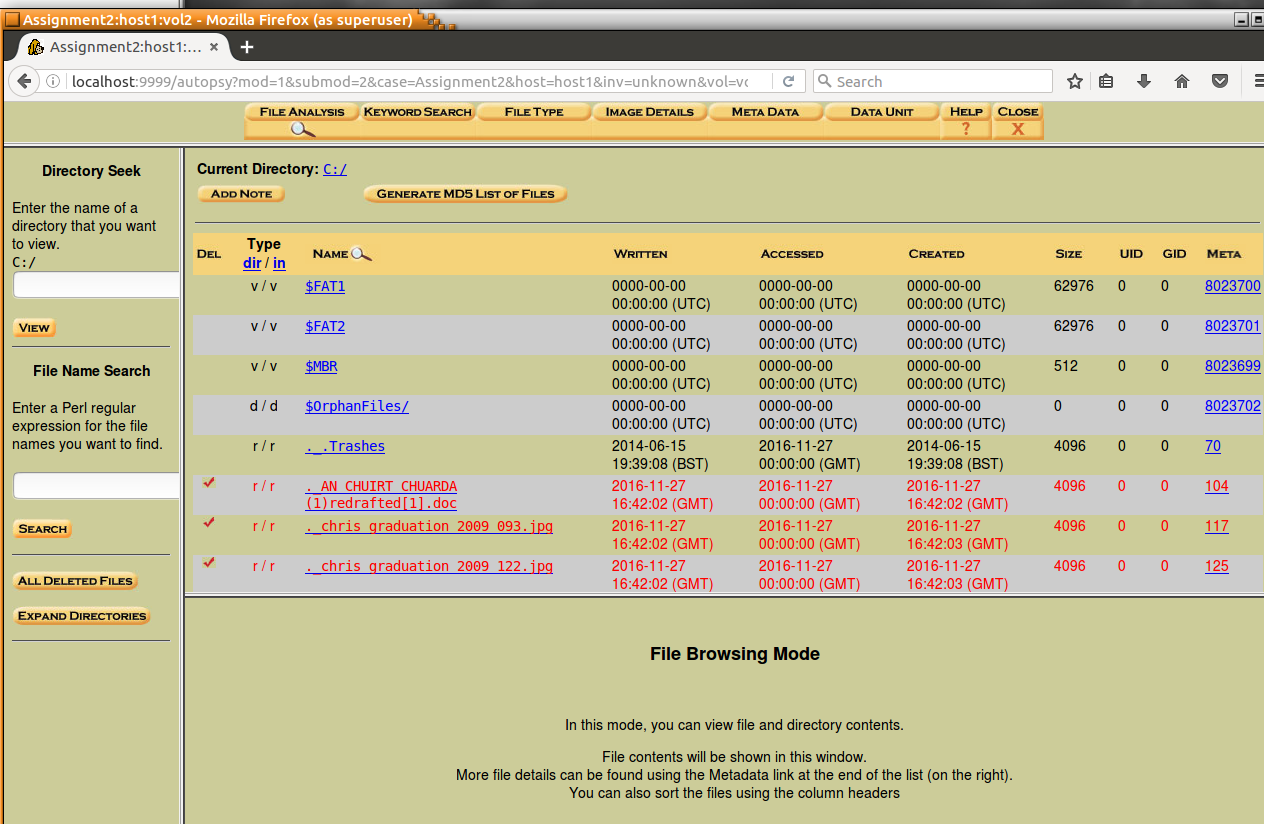
Sleuthkit and Autopsy are tools that can recover information from peripheral devices and hard drive but it is limited due to space. What ever image you acquire using GuyMager, a storage device must be equal or the same length to hold the image to hold.

These tools are digital forensic tool that with the use of Autopsy. can provide the investigator with a GUI for a better user experience. For peripheral devices, I used a tool called ‘GuyMager’ in a linux machine. This created a media image with an extension of .dd. This file was then analysed using Autopsy. I used autopsy on a Linux machine. Autopsy is sleuth kit except with a GUI. It is designed for Windows operating system but can work on a Linux machine through local host on the browser.

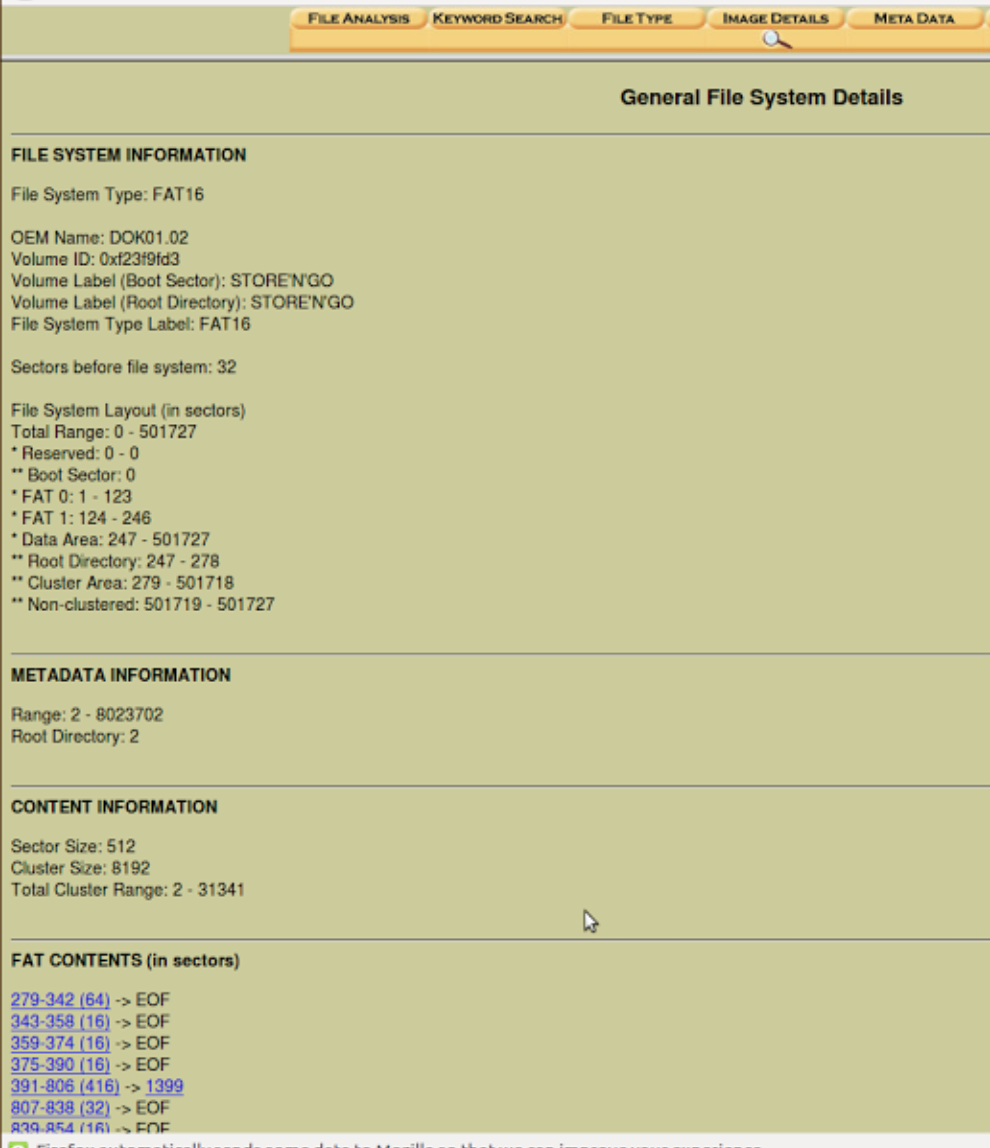
The information autopsy can return to a user is information such as the files on the USB device. Valuable information such as when a file was created, last accessed and very importantly, Autopsy has the functionality to return information about files that have been deleted. This is very important as deleted files can be retrieved and reviewed by an investigator.

Autopsy has the ability to filter data by GPS location, date added, ip addresses, email addresses. Autopsy also allows the investigator to categories the files on the device. Information about the number of files on the device can be retrieved. Investigators can also get information about the file system and the metadata on the disk.

In the following image below demonstrates the use of Autopsy. All the files are returned to the investigator, even files that have been deleted can be retrieved. Information such as when a file was written, last accessed, date of creation and size can be returned to the investigator providing sufficient amount of information. Metadata for each file can also be retrieved as seen in the image below.



Other information that autopsy can provide to an investigator is information relating to the file system. From the USB stick that this evidence was retrieved, an investigator can retrieve file system volume ID and content information.



Sleuth Kit can also be ran in the command line on a operating system such as Windows. Sleuth kit has multiple command line tools that can return information back to an investigator. The following command line tools were ran on a Windows 7 machine. Similar to Autopsy, an image must be provided, I used the image retrieved from Guymager. The first command tool I ran was fls. This tool returned a list of deleted file names.

From using autopsy on the Linux machine, I found it very useful and the information that can be returned to an investigator is plenty. Even if a person does try to hide information on a peripheral device, this information can be retrieved. The face that Autopsy can also return when the file was last accessed in significant amount of information.

**Part 4. Own choice of tool.**

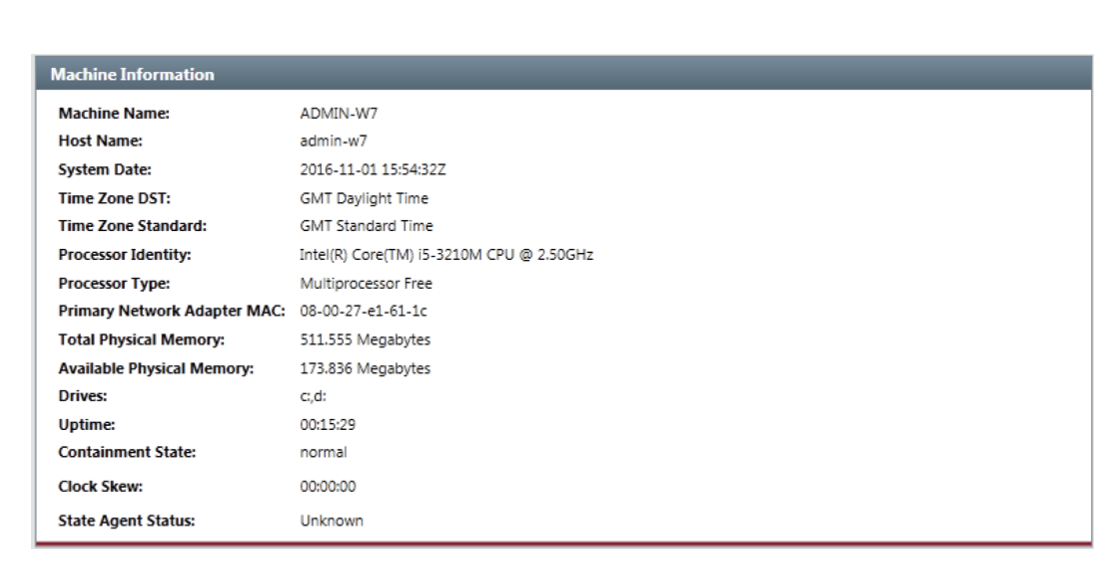
The tool I chose to use to analyse data locally was Redline. Redline is a forensic analyser that can create a memory dump of a system, and it also has the ability to analyse that data. For the system we want to analyse, we run the RunRedlineAudit executable. This executable can be put onto a usb stick then inserted into a targeted machine. Redlins creates a .mans file and can store this information back onto the USB stick. The purpose of this is that no information is added to the target machine, only a scan is performed and very little data is modified. Once the scan is complete, we can analyse this data back on the investigator machine. The information retrieved from Redline is huge. Information such about the system, what operating system is been used can be retrieved.

Redline can return information about the registry, what processes are currently been run at the time of the scan. Other information such as timed processes and information relating to files can be retrieved. User information is also collected and can be viewed within this tool. Overall, this tool is very powerful. Comparing this tool to others such as volatility, Redline provides the ability to create a live memory dump, the GUI provided as well makes it easier for an investigator to use and observe the data.

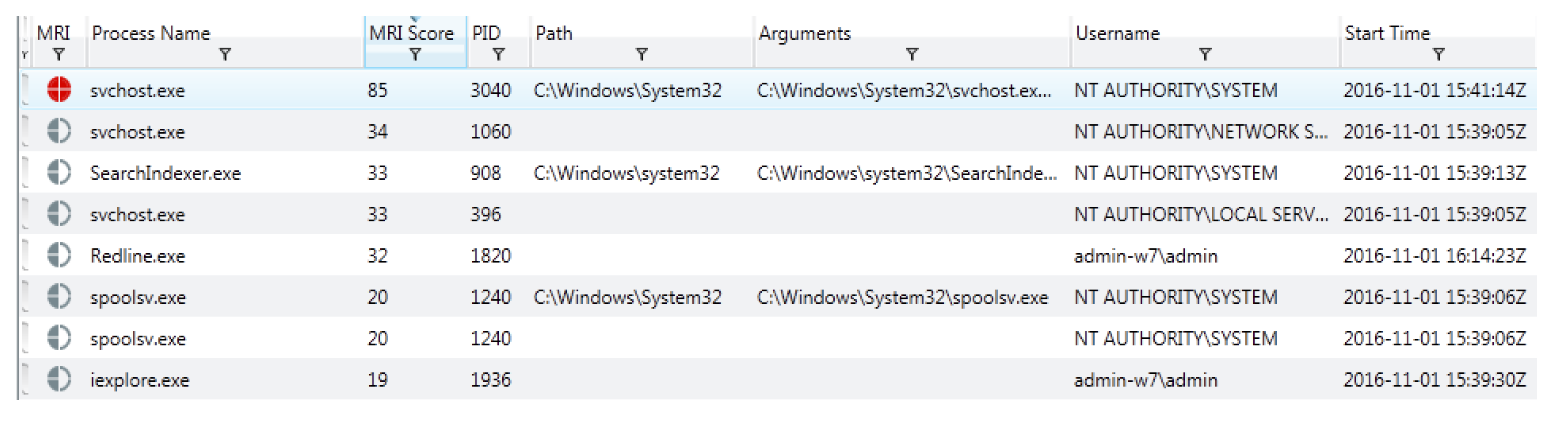
Redline has the functionality as well of identify network information. What ports are been opened by what processes. What user has authenticated this as well. This evidence is a lot to an investigator and it can inform the investigator on what a specific user was doing on the internet. Also relating to the processes been executed, the user that executed them and the time the process was executed is recorded. It provides a timeline for an investigator.

Redline also has the ability to identify all the suspicious files on the system. If user was going to hide information in a file and it is not properly signed, Redline Will return this information back to the investigator. The files that might contain malware or seem out of place in s system will be displayed and can be further analysed.

I used Redline and was able to return information back about my Window 7 machine. Information such as the system name and user information was retrieved. As mentioned before, I was able to return the information about processes and scheduled processes. All this information is locally and can be further analysed at any time.



The below image will also display all the running processes when the scan has been performed

on the system As seen from the image below, the process running, the process ID, the username that was logged in and the start time is returned to the investigator.

Another important piece of information retrieved using Redline was relating to user accounts on the Operating System. Redline was able to analyse the data of the users on the system. Information such as the usernames, the last time a specific user was logged in, does the user require a password in order to log in and which group the user belongs to such as Administrator or Guest.

There was numerous tools used throughout this assignment. The tool that I used to retrieve forensic evidence about a network was IP Scanner. If I wanted to analyse the packets on a network, wireshark could have been used. It is a packet analyser but the application would have to be installed on the targeted machine and therefore will be manipulating data on the evidence machine. This is not what an investigator would want to do as data can be overwritten or become encrypted.

The tool I used for analysing peripheral devices such as a USB stick was autopsy. Autopsy was ran in a Linux machine. The image I ran the file against was created using Guymager in Caine. This tool can also be used on a Linux machine.

The final tool that I used to collect and analyse local data was Redline. This can create a live image of a system and provides the functionality as well to analyse the information it collected.