The other document contains screenshots of both volatility and Redline working. Also, screenshots of the hash values for the memory dump evidence files and when they are compressed are there as well,

The computers that were analysed is this project that contains information were a Windows 7 and Ubuntu version 14.0.4.1.

Windows
Starting with Windows. The tools used was Redline and command line.

Procesure for Installing Redline.
Redline was provided in a .zip folder from web courses. The file was downloaded and stored on the C drive. Once the application downloaded and installed. I opened the application. Redline provides the functionality to collect data about a machine as well. An empty folder was created and selected to store were the memory dump will be created.

Following these steps, we go into the file explorer and go to the new folder that we created. In this case the folder was named “Forensic”.
Within the forensic folder, there is a batch file called RunRedlineAudit. This collects the information and creates a new folder within forensic called “Sessions”. This is whee the memory dump is placed.

Once the dump has been created, we go back into the Redline application and select “Analyse data”. The option I chose was “From aSaved Memory file” and selected the memory dump file. The file selected was “AnalysisSession1.mans” file. From here we can now analyse the information on this file using Redline. Information such as volatility and non volatility information can be retrieved.

Any information that couldn't be retrieved using Redline such IIS flags, this information was retrieved using the command line on the targeted machine.

Linux
The tools used for creating a memory dump of the Ubuntu machine was called LiME. The analyser tool was called “Volatility”. On the Ubuntu machine, git was installed. Once Git was installed, Lime was cloned to the targeted machine from the URL https://github.com/504ensicsLabs/LiME.

Once Lime was cloned, Within the command line, I went to to the following path LiME/src. I used the linux command “make” to compile the files. As a result of this, a .ko file is created.

```
jonathan@jonathan-VirtualBox:/$ sudo insmod LiME/src/lime-4.4.0-31-generic.ko "p
ath=/home/jonathan/documents/linux1.lime format=lime"
```

The above command will create a dump of the linux machine called linux1.lime.

When the memory dump of the Ubuntu machine was collected, I was able to run plugins against the memory dump to return me information. The command was
python vol.py -f /home/jonathan/Desktop/dump.lime --profile=Linuxforensicx64 linux_banner.

The linux_banner in the command above is the plugin. This command can be used to retrieve the date and time from the Linux machine. Also, other information such as the Operating system which is been used and the version can be retrieved.

The plugin can be replaced with any of the following linux commands from the following link.
https://github.com/volatilityfoundation/volatility

For getting the hash value on Windows, a tool was downloaded from the Microsoft website called File Checksum Integrity Verifier (FCIV). This was used to get the hash value of the .mans file and the hash value of the .mans file when it was compressed.

AnalysisSession1.mans Hash value: edf379bc66e22315f473c384ae8

AnalysisSession1.zip Hash value: 60cd33a00ec3f0d15c40e6a9eb1ce68c

For Linux, Linux comes with a built in tool that was used. It was called the md5Sum. The hash value for the .lime file and the compressed file was used using this tool.

dump.lime hash: 2b22d8af7efa758b42943cb0dd1b99bb

dump.lime.zip hash value: 231fe6da59b312bbabec9064ad46248

Report Compare g the Evidence

From Testing both volatility on Linux and RedLine on Windows 7, the evidence obtained from both the operating systems are similar enough. Redline provides the user with a GUI which makes it easier for an investigator to read the information compared to volatility, to get results, the investigator must type the correct command and plugin in the command line.

From testing both these softwares, I found it difficult to run volatility, even though there is plenty of resources online, it was difficult to install. Volatility was very time consuming and to use volatility, another tool had to be used to gather the information about the system. This tool was used create a memory dump and in my case I used Lime. Comparing this to Redline, the installation and the using of Redline had the edge over volatility. For me, it was easier to use, there was no need to use the command line and the GUI provided was simple and clear. the information provided to me was easier to read compared to the information that would be returned to me using volatility on the command line.

Both tools provide the evidence for the date and time. They also both provide information about the current system, such as what Operating system is been used and the patch level. Where the evidence differs between these tools is that in volatility, there is no command to get information about the user who was currently logged in. Also from examine the evidence gathered by the tools, I noticed that for the system information, Redline provides greater detail to the investigator. Evidence such as install date, Bios information is available, even though this might not be that significant to an investigator, redline provides more information about the current targeted machine.

Another area where redline is better to volatility in my opinion is in the running process. While volatility provides the process name and the start time, Redline goes the extra step and provides information to the path of the process and which user was logged in when the process was running. This can be vital information for an investigation in order to determine who ran a process if multiple users were on a computer. Other information that is present in Redline would be scheduled processes, the start time, end time and the date of the process to be be executed is recorded. From my experience of using Redline, it can be useful in tracking and locating suspicious files on a machine. When a process is been executed, the information will be stored into a file. If malware is present, there is no signing of the process to the file. Redline can allow a user or investigator to see the untrusted processes on the system. This can be used to detect malware on a system.

A similarity between the two different tools was the network evidence. Both were able to provide me with the interfaces of the system. This could provide information such as the MAC addresses for the adaptors on the machine. Also information such as what executables where opening either UDP or TCP ports where shown to me in both Redline and in volatility. Information provided back to me by both tools where the process name that was opening the the ports, the path to where the processes was been executed and the state of the port such as “Listening” or “Established” could be viewed. the only difference between the evidence returned in this section would be that Redline sometimes returned information such as the time when a process was created when opening a port. Redline provides just a little bit of extra information which overall could be very useful to an investigation as this information could provide a timeline of the network tasks to an investigator.

Also in volatility, the internal routing table plugin was removed so I was unable to access this information within volatility. As a result of this, the investigator would have to run the command on the linux machine and no to be using a plugin to retrieve this information. The disadvantage of this would be that this data isn't stored in the memory dump, therefore analysis on a different date, for example a week later, this information will be lost if the targeted machine is ever turned off.

Other areas I believe Redline out did volatility was in the collecting of non volatile data. Redline could provide me with registry entry data. Also for redline, the user is able to change the script. this allows the user to select and deselect which data the investigator would like to analyse. This can be beneficial as if the investigator only wants certain amount of data. Redline would produce this faster as the investigator can select what data can be returned to be analysed.

Comparing the evidence collected by both machine, in my option, I believe Redline is better in the section about users on system. Redline provides clear information about system users, such as how many users exist, does the user require a password to log in, when the last time that user logged into the machine and what group that specific user belongs too. There is huge amount of information that gets retrieved and that can be analysed using the Redline software compared to volatility. I was unable to retrieve information about users using volatility on a Linux machine. This could be a result that maybe there was no plugin to display this information. This is where volatility and Redline differ, Volatility was unable to display the similar information such as what Redline was able to provide. I couldn't find information about users on the linux machine or when that user was last logged in.

Evidence that I was unable to retrieve while using Reline would be the Cached netbios table and the IIS logs. Even though Redline was able to retrieve the event logs, i was unable to view the IIS logs. Other evidence that I couldn't retrieve was the auditing policy on redline. This information though can be retrieved using the command line commands but as mentioned before, this information could be come lost if its not saved on the system or any information in RAM.

Volatility is crossed platform compared to Redline that only runs on Windows. Volatility will run on Mac OS, Windows and Linux.

Volatility is open source, this allows people to create their own plugins in areas where Redline overcomes volatility in areas such as information about the user. This in turn will make volatility more useful but is limited by the person who is using the tool as if the person doesn't create their own plugins, they are limited by the number of plugins.

Other area where Redline and volatility are similar as mentored above previously is evidence related to the IIS flags and adding poles, both tools were unable to retrieve this information.

References:

[1]. https://github.com/volatilityfoundation/volatility/wiki/Linux%20Command%20Reference#linux_netstat

[2]. https://code.google.com/archive/p/volatility/wikis/LinuxMemoryForensics.wiki

[3]. https://github.com/volatilityfoundation/volatility

[4]. https://github.com/504ensicsLabs/LiME

[5]. https://support.microsoft.com/en-ie/kb/841290