



PRIFYSGOL CYMRU
Y Drindod Dewi Sant
UNIVERSITY OF WALES
Trinity Saint David
SWANSEA - ABERTAWE



Network Security (NS)

Lab -

Introduction to Digital Forensics

Faculty of Architecture, Computing & Engineering

School of Applied Computing

Mount Pleasant Campus

Swansea

SA1 6ED

1. Background

During Introduction lab exercise titled “Introduction to Digital Forensics”, you learnt how digital forensics is used to retrieve and chronicle evidence located on a computer's hard drives and other sources of Electronically Stored Information (ESI) such as floppies, CDs and DVDs, external drives, thumb drives and voice mail servers, so that it can be presented as evidence in a court of law.

In this exercise, you will learn how to use the Win-UFO v6 tool that is stacked in the CAINE DVD, to conduct a real life digital forensics investigation on your PC in the computer lab. This real life forensics investigation can also be conducted on your personal computer or any other computer that has been exposed to abuse on the Internet.

2. The scenario

The scenario of this digital forensics investigation is that a group of unscrupulous students in the university have been using the PCs in the computer lab to download and share inappropriate images and videos from the Internet. The students also save some of these images and videos on their USB devices to take home.

Downloading pornography on university computers is a disciplinary matter. It is disruptive to learning and also exposes the university computers and network to outside hackers.

As a digital forensics student, you have been commissioned by your module leader to investigate this abuse of university facility and report your findings. To accomplish this task, you have been given the CAINE DVD. You have also been given tips on how to conduct your investigation as follows:

- a. Use image recovery tool called “Recuva” to recover downloaded and deleted images and emails on the computer.
- b. Use browser history applications like “BrowsingHistoryView”, “Favourites View”, and “Historian” to establish the offensive websites visited, the number of times visited, and the users who visited the offensive websites.
- c. Use Log Viewers like “LastActivityView”, “RecentFilesView”, “USBDeview” and “VideoCacheView” to corroborate your findings in (a) and (b) above.
- d. Use Reporting applications like “OutlookAddressView”, “OutlookAttacheView”, “OutlookStatView” and “UserProfilesView” to establish the names and email addresses of users and the inappropriate files and videos they shared as suggested by your findings in (a), (b) and (c).

3. The Lab Exercise

Switch on your PC in the lab to boot from Windows 7 without the CAINE DVD in the drive. After a successful boot-up, insert the DVD and run it as described in the “Introduction to Digital Forensics” document. This time use a USB drive for your report folder.

3.1 Running the Recuva Tool to recover images and emails

From the Win-UFO v6 main window, click on the “Recovery” button and select “Recuva” as shown below in figure 1 below.

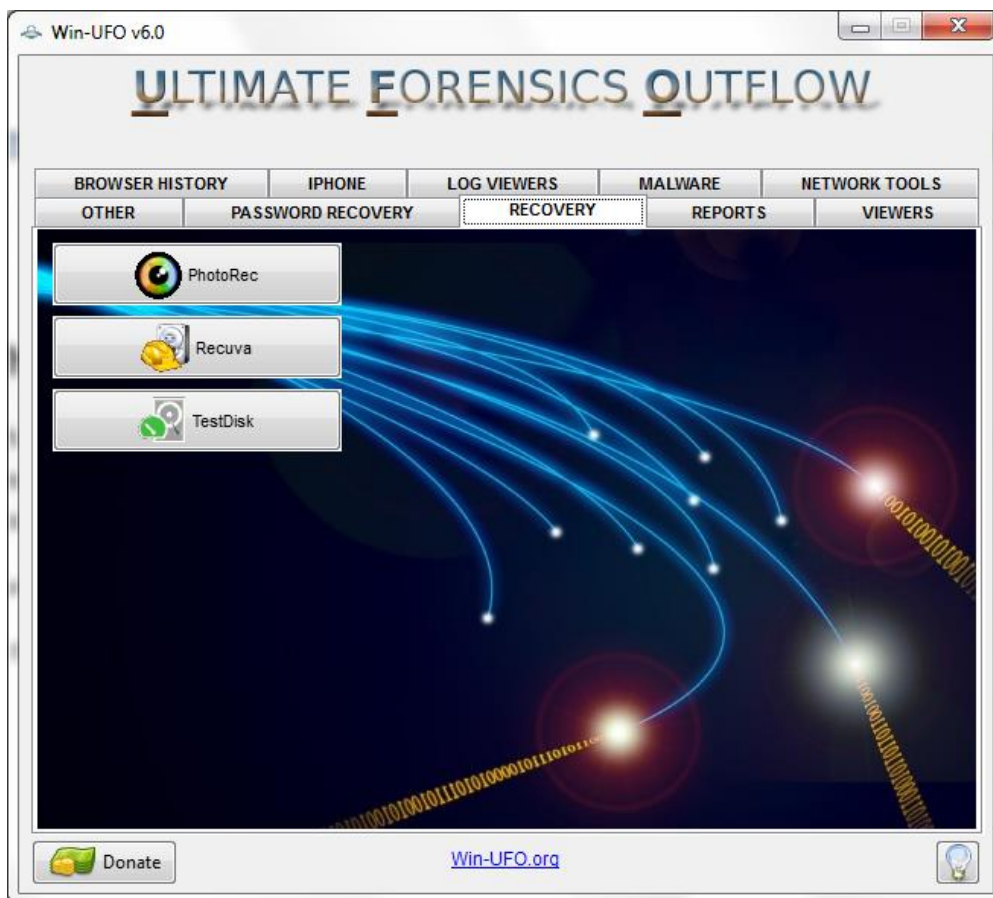


Figure 1: Running the Recuva tool.

The Recuva tool is one of the best free to download file recovery tools available for both Windows and Linux operating system platforms. The application has the capacity to recover deleted files and files kept in hidden folders.

For the purpose of this digital forensics exercise, we are only concerned with emails, and images and video, which are inappropriately downloaded on university computers. You will conduct forensics analysis involving other file types of files in subsequent exercises.

Once the “Recuva Wizard” application is loaded as in figure 2 below, select “Pictures” radio button and then click on the “Next” button.

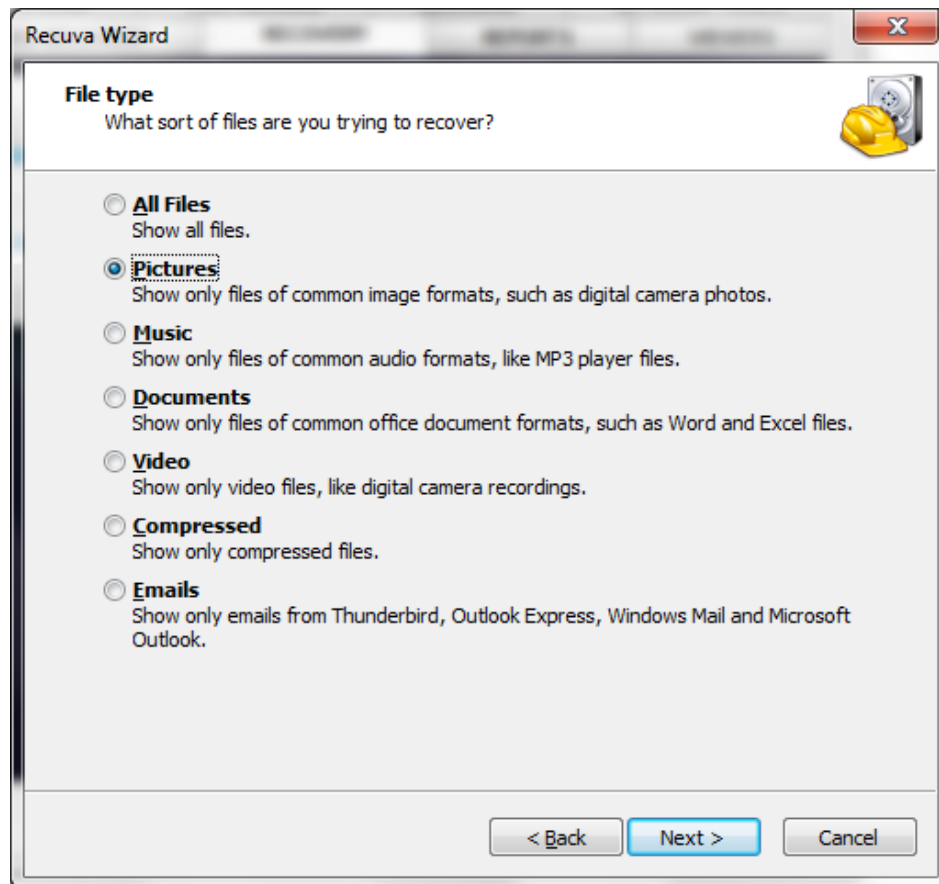


Figure 2: Selecting “Pictures” from Recuva Wizard.

At the file location window as shown in figure 3 below, select the default drive for the Windows 7 operating system, which is usually drive “C”. If you are not sure, use the “Browse” button to browse your computer and select the drive where Windows 7 is installed.

Note that we are selecting drive “C” not because it is where all the images and video are necessarily saved. We are selecting the drive because that is where browsing history, USB usage history, and user profiles etc are saved. The Recuva tool can recover files from any drives with or without operating system installed in it, including DVDs and USB sticks.

After selecting the drive location, click on the “Next” button. The “Thank You” window appears as shown in figure 4 below.

If you have more than two hours time allowance in the lab, you may click on the “Enable Deep Scan” check button, otherwise leave it blank. By clicking this button, you are telling the Recuva tool to conduct indepth forensics analysis of the target drive. This may take more than one hour to accomplish, depending on the size of the HDD , the processing power of your computer and of course available memory.

Now, click on the “Start” button to start forensics scan of your HDD for images.

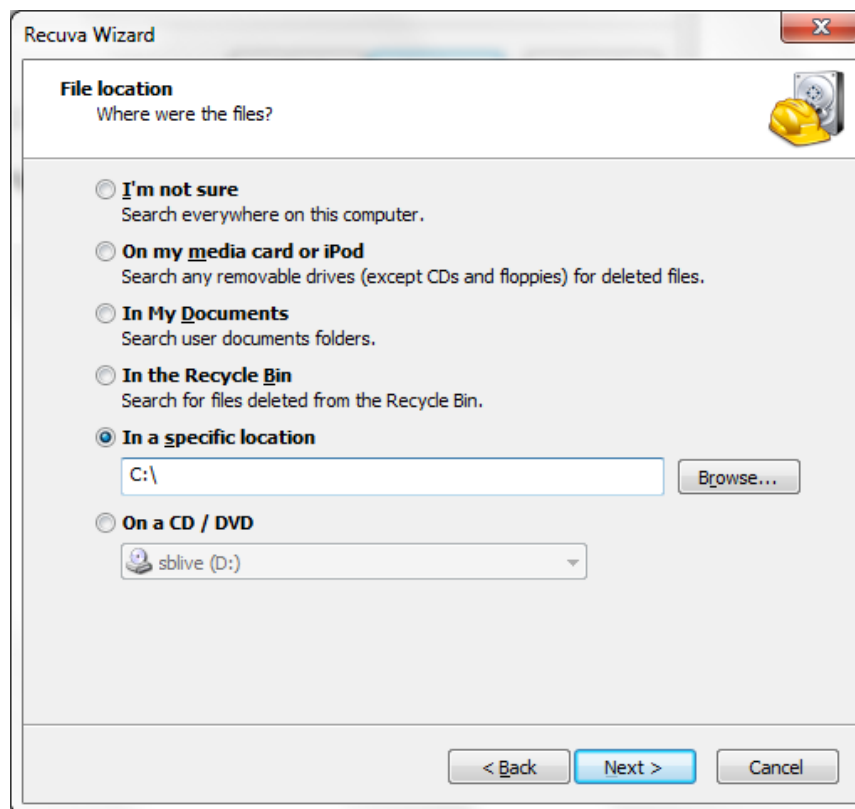


Figure 3: Selecting file location in Recuva Wizard.

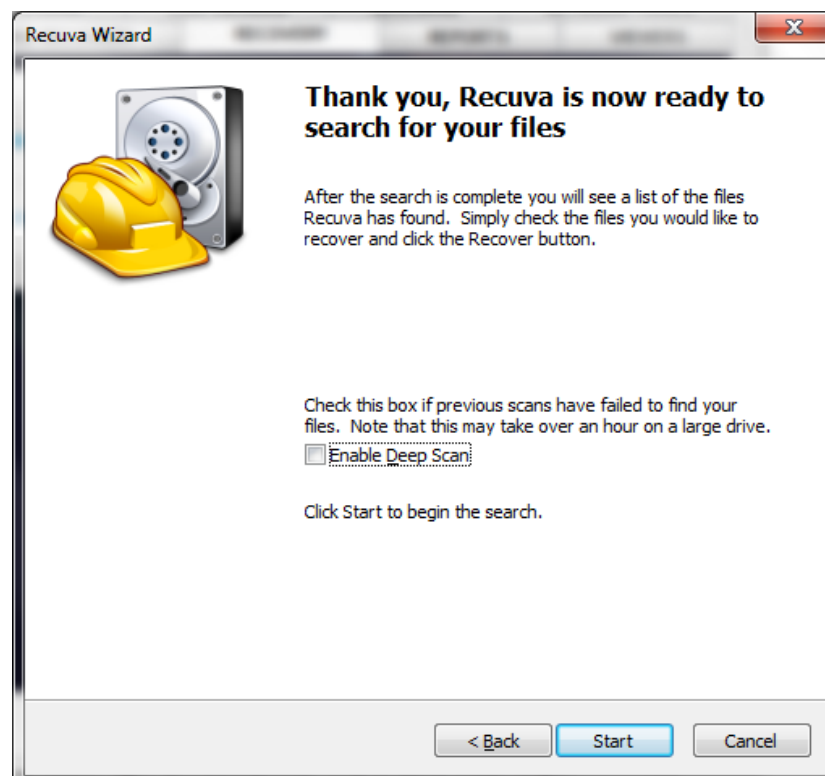


Figure 4: Thank You Window.

The forensics scan is a three stage process as shown in figure 5 below.

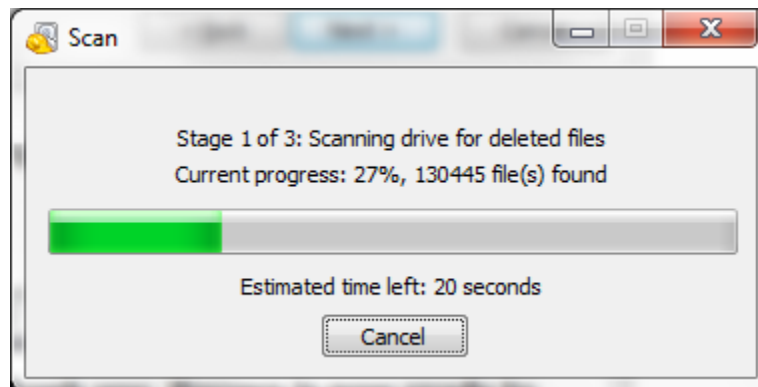


Figure 5: HDD scan.

The scan process (without deep scan) is usually fast. Upon completing a scan, Recuva shows a window complete with a grid of image files. Click on the “Switch To Advanced Mode”. Browse through the files shown in the main window as in figure 6 below. Note that the file names are colour coded in orange, red and green. Orange means the file quality is poor. The chances of recovery are low. Red means the file is simply irrecoverable. Green means the file is in excellent condition and is fully recoverable.

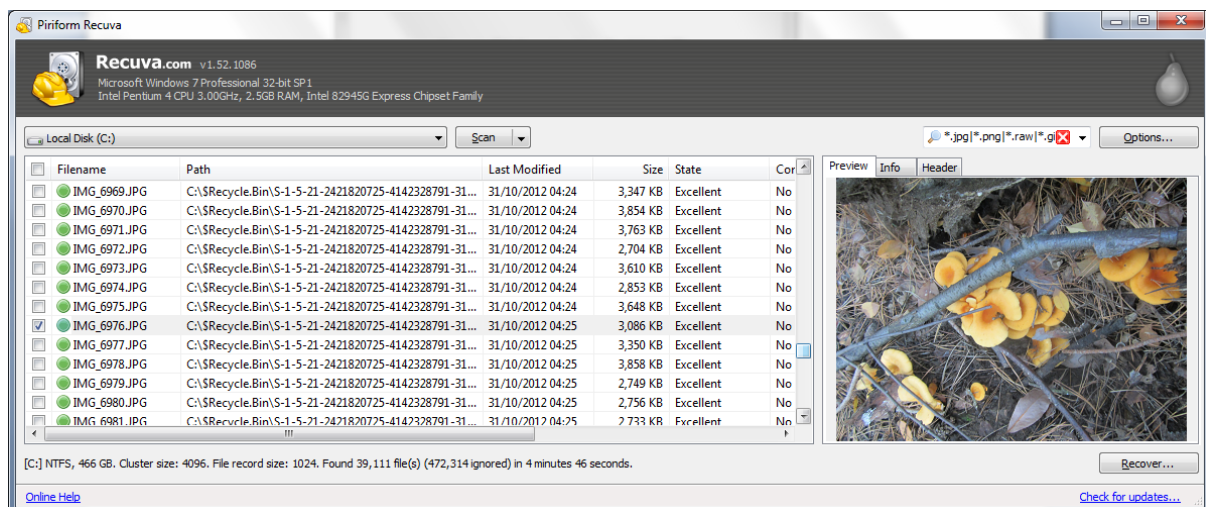


Figure 6: Recuva in Advanced Mode.

Note that by selecting a file name with green colour tag, the file can be viewed in the “Preview” pane. Useful information such as the creation date and time, last modified date and time, and last accessed date and time can all be easily retrieved from the “Info” pane.

Take your time to browse the list of all the files that are green coded. You are almost certainly likely to discover some images that are useful for further investigation. Take note of the information available for each image of interest. Click on the “Recover” button to recover the

selected file and save it in your digital forensics report folder, preferably in a different drive such as a USB drive.

Repeat this scanning process for emails by selecting “Emails” as shown in figure 2 above.

After a successful scan, all emails such as outlook, thunderbird and webmail which are saved or hidden on the “C” drive are recovered as shown in figure 7 below.

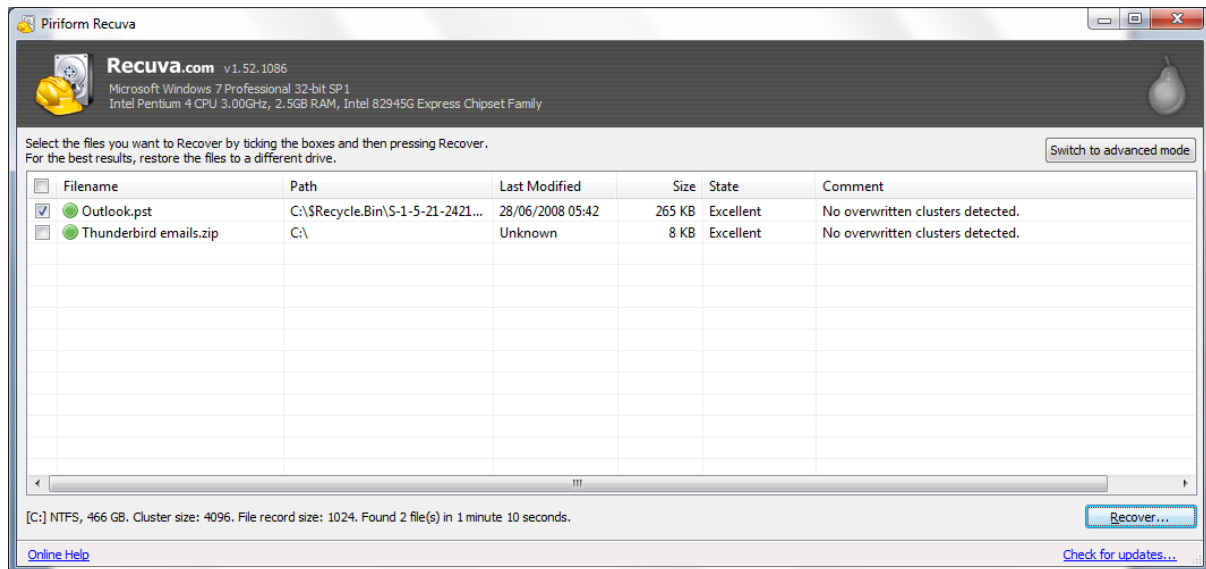


Figure 7: Recovered emails.

Click on the “Recover” button and save your recovered emails in your forensics report folder in a USB drive.

3.2 Running Browser History

The browsing history of a computer user is powerful digital forensics evidence. Many cyber criminals are not aware of this fact. From the Win-UFO main menu, click on “Browser History” and select “BrowsingHistoryView”. A window like figure 8 below appears.

At the “Filter by visit date/time” drop down menu, select “Load history items from any time”. At “Web browsers” click on all available browsers shown on the list. At “Load history from” drop down menu, select “Load history from current running system (all users).” Then click on the “OK” button.

After scanning the HDD for browsing history, the Recuva application shows a window similar to figure 8 below.

Figure 8 shows the URL, the time and date visited, the number of times visited, what browser was used, the name of the user, and the URL length.

Using the date and time associated with any images that you have found in section 3.1 of this exercise, try to browse through the browser history and see if you can link an image with a browsing history. Select URLs of interest and save them in your digital forensics report folder. Note that you can visit a site by simply double clicking on the URL.

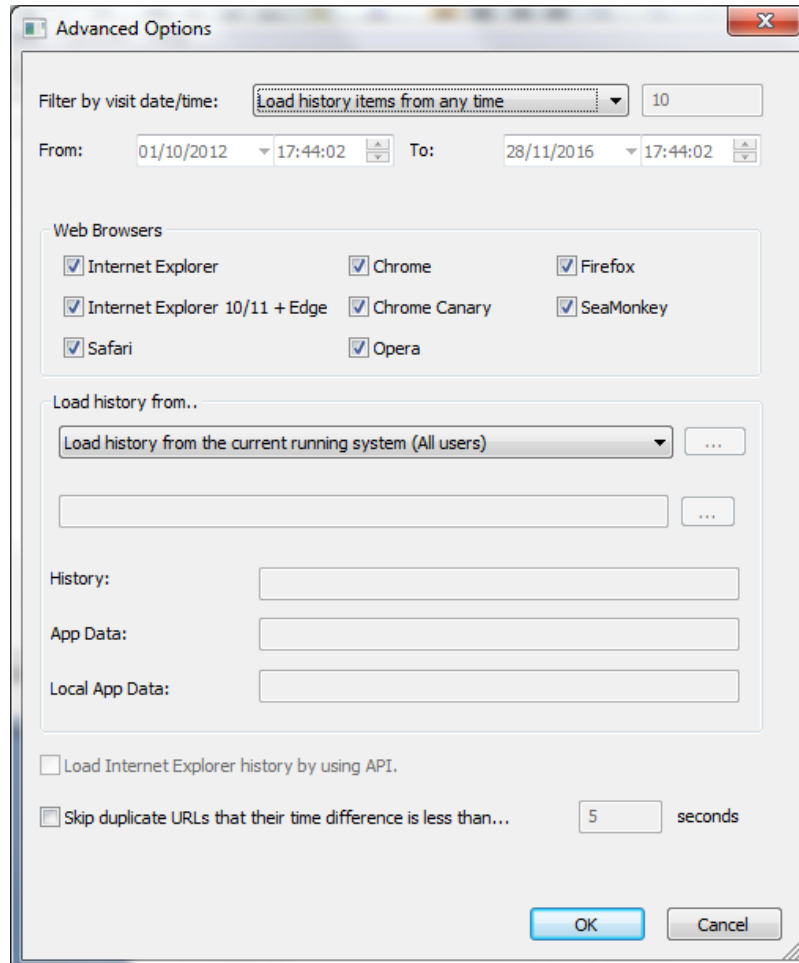


Figure 8: Selecting browser options.

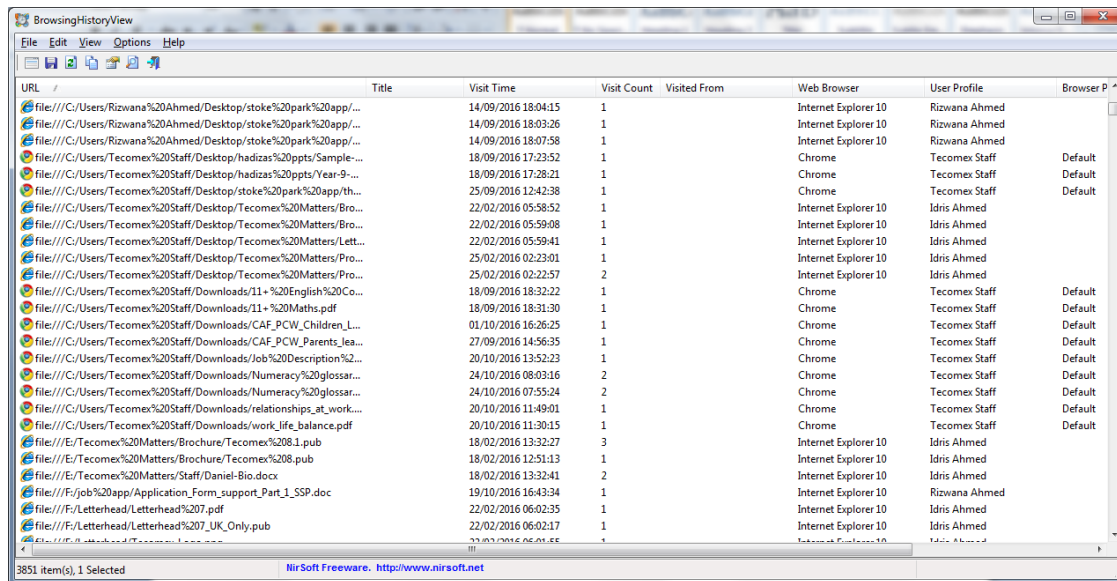


Figure 9: Browser history.

3.3 Running Log Viewers

At the main Recuva menu, click on it and then click on the “Log Viewers”. Then select the “LatestActivityView”. This is another useful application in the Win-UFO tool. It gives a list of file names that are recently viewed on the computer. It also gives the date and time the files were created, the last time they were modified and the last time they were viewed. Refer to figure 10 below.

Browse through your list of recently viewed files and see if you can associate any file in the list with your saved browsing history. Save any files of interest in your report folder.

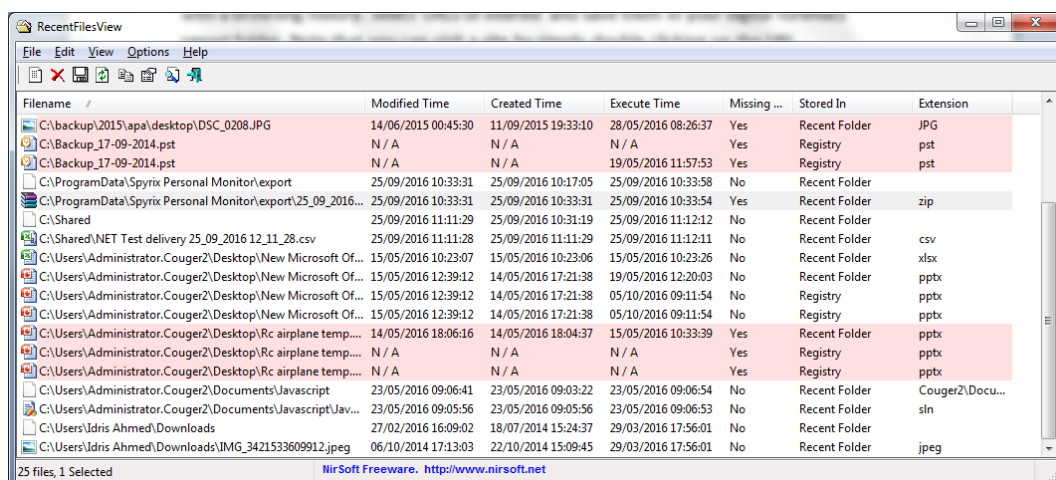
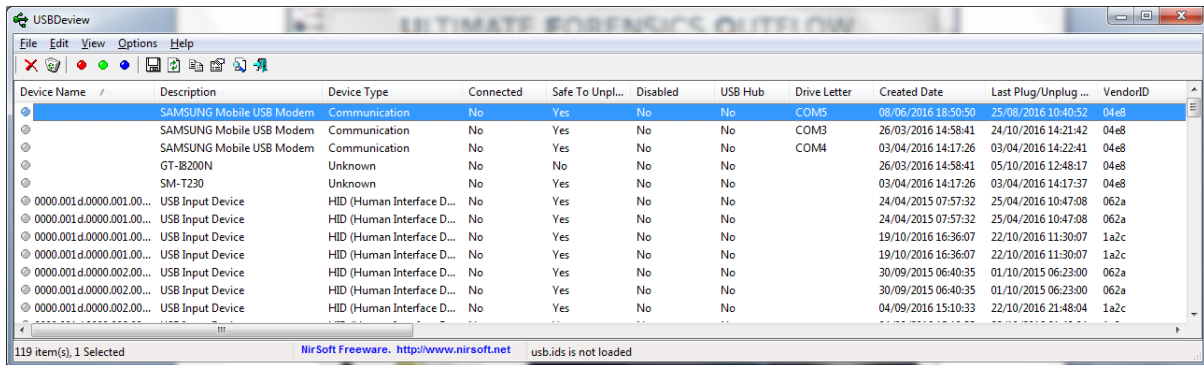


Figure 10: Recent File View.

From the scenario description in section 2.0 above, we are informed that images are shared through email and also saved on USB drives and taken home. From the “Log Viewers” window, click on “USBDevView”. This will load the USB usage window as shown in figure 11 below. The information provided is quite revealing. Try to compare the “Created Date”, “Last Plug/Unplug Date” with any dates of interest that you have identified in the previous sections.



Device Name	Description	Device Type	Connected	Safe To Unpl...	Disabled	USB Hub	Drive Letter	Created Date	Last Plug/Unplug ...	VendorID
SAMSUNG Mobile USB Modem	SAMSUNG Mobile USB Modem	Communication	No	Yes	No	No	COM5	08/06/2016 18:50:50	25/08/2016 10:40:52	04e8
SAMSUNG Mobile USB Modem	SAMSUNG Mobile USB Modem	Communication	No	Yes	No	No	COM3	26/03/2016 14:58:41	24/10/2016 14:21:42	04e8
SAMSUNG Mobile USB Modem	SAMSUNG Mobile USB Modem	Communication	No	Yes	No	No	COM4	03/04/2016 14:17:26	03/04/2016 14:22:41	04e8
GT-B200N	GT-B200N	Unknown	No	No	No	No		26/03/2016 14:58:41	05/10/2016 12:48:17	04e8
SM-T230	SM-T230	Unknown	No	Yes	No	No		03/04/2016 14:17:26	03/04/2016 14:17:37	04e8
0000.001d.0000.001.00...	USB Input Device	HID (Human Interface D...	No	Yes	No	No		24/04/2015 07:57:32	25/04/2016 10:47:08	062a
0000.001d.0000.001.00...	USB Input Device	HID (Human Interface D...	No	Yes	No	No		24/04/2015 07:57:32	25/04/2016 10:47:08	062a
0000.001d.0000.001.00...	USB Input Device	HID (Human Interface D...	No	Yes	No	No		19/10/2016 16:36:07	22/10/2016 11:30:07	1a2c
0000.001d.0000.001.00...	USB Input Device	HID (Human Interface D...	No	Yes	No	No		19/10/2016 16:36:07	22/10/2016 11:30:07	1a2c
0000.001d.0000.002.00...	USB Input Device	HID (Human Interface D...	No	Yes	No	No		30/09/2015 06:40:35	01/10/2015 06:23:00	062a
0000.001d.0000.002.00...	USB Input Device	HID (Human Interface D...	No	Yes	No	No		30/09/2015 06:40:35	01/10/2015 06:23:00	062a
0000.001d.0000.002.00...	USB Input Device	HID (Human Interface D...	No	Yes	No	No		04/09/2016 15:10:33	22/10/2016 21:48:04	1a2c

Figure 11: USB Usage View.

3.4 Running Reports

From the Win-UFO main menu, click on “Reports” and then run “OutlookAddressBookView”, “OutlookAttachView”, and “OutlookStatView”.

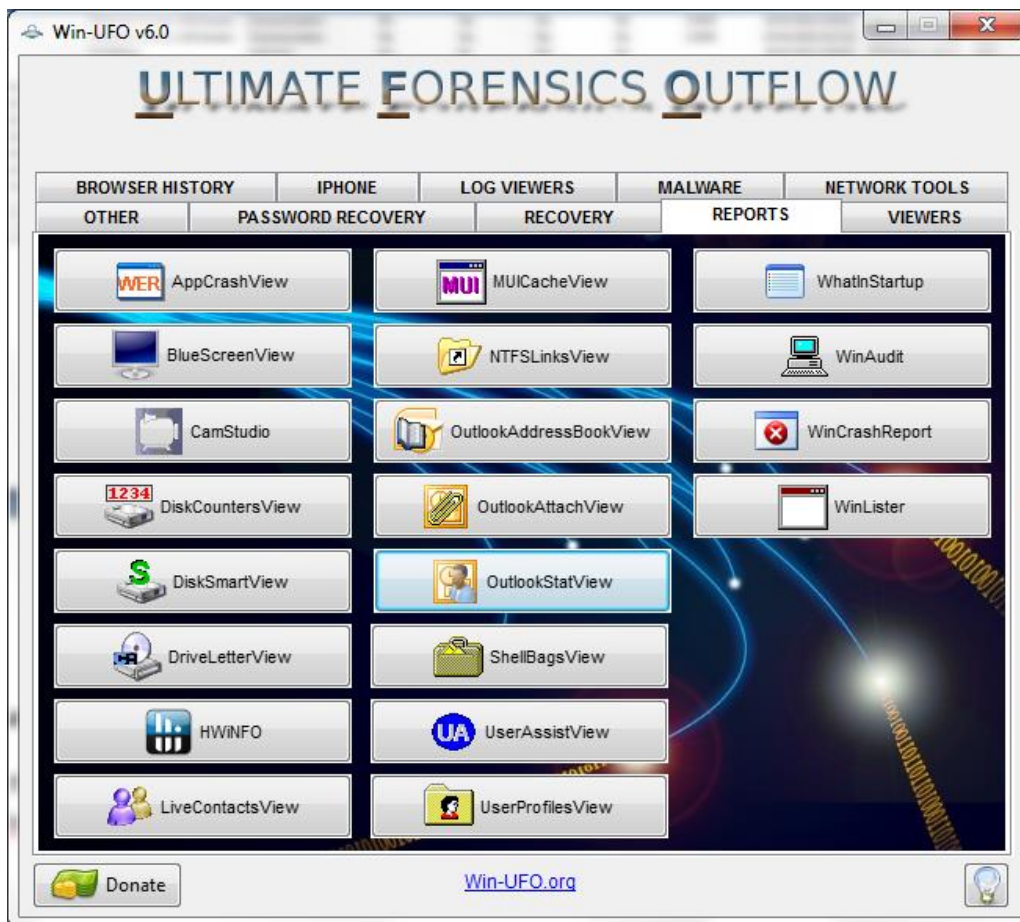


Figure 12: Running Reports.

Save your findings in your report folder. Compare user profiles, files, dates, and emails of interest. You will discover with almost certainty that you have identified at least one computer user who accessed the Internet at a particular date, downloaded an image disapproved by the university IT policy and very likely emailed it or saved it in a USB device.

Conclusion

Digital forensics is a very interesting area of cyber security. Equipped with the right tools and methodical approach, it is possible to recover most evidence of criminality committed by hackers. In this exercise, you have learnt that the computer has a way of recording almost every event that took place while it is switched on. It is just a matter for the digital forensics expert like you to uncover the evidence. Doing forensics exercise of any description requires concentration and patience. The outcome is however almost always rewarding.