Visualdrives Forensic Tool

Mustafa Anil Tuncel[1], Hulya Francis[1], Mark Taylor[1], David Llewellyn Jones[1]
[1]School of Computing and Mathematical Sciences
Liverpool John Moores University
Liverpool L3 3AF, UK
tuncel.manil@gmail.com, h.francis@ljmu.ac.uk, M.J.Taylor@ljmu.ac.uk,
D.Llewellyn-Jones@ljmu.ac.uk

***Abstract*— Visualdrives is a tool for visualising files stored on a hard drive. The application combines a 3D interactive game-style visualisation combined with a LeapMotion input device providing gesture control over the interface.**

The purpose of the tool is to understand the potential for abstract digital forensics data to be visualised in a richer, more interactive environment than has traditionally been the case.

Keywords—Computer Forensics; Digital Investigation; Information Visualisation, LeapMotion, Forensic data.

I. INTRODUCTION

This research study use of a novel 3D visualisation, combined with LeapMotion gesture control, and it is intended to support rapid transition between macro-level and detailed data visualisation across multiple dimensions of data. It is envisaged that the tool would be useful as a forensic software tool which would help forensic scientists in their investigations. The purpose of the tool is to understand the potential for abstract digital forensics data to be visualised in a richer and more meaningful display.

There is a large pool of existing research in the area of visualising file hierarchies and mapping file characteristics to visual representations. Wiss and Carr considered the use of 3D interfaces and the importance of the relationship between global overview and local focus [2]. The scope to focus on particular areas of interest within an abstract data visualisation has also been developed by Cignoni, Montani and Scopigno [3].

Given the nature of file hierarchies as tree structures, there has also been a variety of work developing practical ways to achieve good visualisation of tree data [4, 5]. Although more general, there is also a large body of work considering graph visualisation, which is a recurring topic in the area of visual analytics [6]. This also introduces the issue of presenting multiple characteristics of data in an effective way, for example with Beamtrees attempting to clearly show both filesize and hierarchy in a single presentation [5].

While the application to digital forensics is less well explored, Teelink and Erbacher considered the importance of visualisation for representing file information in a forensic context. The work considers the move from text-based investigation to a 2D graphical representation, and inspired us to take this further to consider a move from 2D to 3D [7]. The question of visualisation of forensic data has other facets as well, for example clarity is a key issue, especially where visualisations may be used to present to a jury in court [8]. For survey work in this area see Schrenk and Poisel [9], Osborne and Turnbull [10]

Digital forensics involves the collection of evidence or intelligence for the purposes of investigating historical – alleged criminal – activity. Crimes being investigated are often partitioned into traditional crimes that happen to have involved the use of a computer (e.g. where a suspect has sent emails describing a robbery), and crimes which are digital in nature (e.g. computer hacking). In both cases, investigators will invariably want to collect digital evidence. This can take many forms, but one of the most common involves analysis of the files on a computer. So much data is now stored digitally that investigating the files on a suspect's computer is an essential part of most investigations.

The reminder of this paper is organized as follows. Section II will outline the design considerations for the proposed tool. Section III will discuss the test results from the research study and finally an effective conclusion will be drawn.

With the huge growth in digital storage sizes and data retention, finding relevant files, for example from a hard disk image, can be extremely challenging. Developing practical ways for an investigator to move from an overview of the contents of a hard drive to the specific areas of interest (the relevant individual files) is especially important and challenging.

Existing digital forensics tools tend to provide traditional 2D WIMP (Windows Icons Mouse Pointer) style interfaces that combine text and layout with limited graphics. Two of the most widely used digital forensics tools for hard drive analysis are EnCase and FTK. The screenshots below show elements of the FTK user interface: on the left a hierarchical representation of the files, on the right the graphics file explorer.

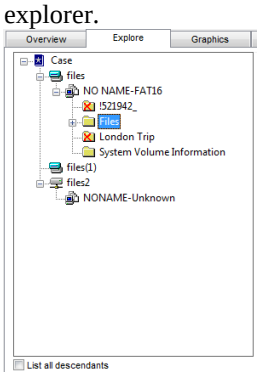

Figure 1: FTK file hierarchy

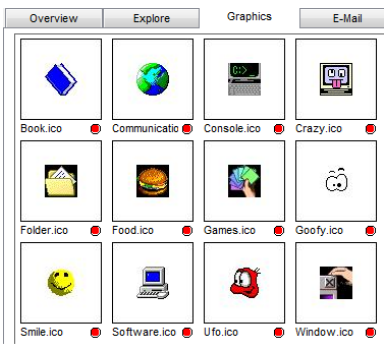

Figure 2: FTK graphics viewer

Both EnCase and FTK provide industry-leading forensic tools. However, their traditional interfaces are limited by the windows paradigm that they work within. Visualdrives takes a very different approach, displaying file information within a 3D virtual environment with a perspective controllable using gestures. Individual files are represented as objects within the virtual environment, with different dimensions of information mapped to different characteristics of the object. For example, the height of the object might represent the size of the file, the colour the filetype, and so on.

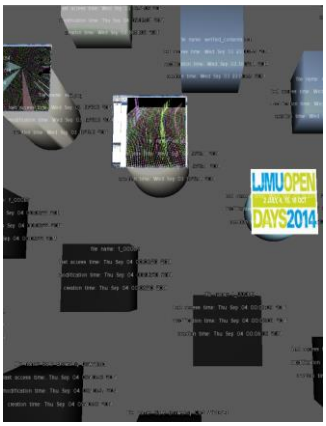

Figure 3: File name and dates are written over the object.

The following summarises the standard mapping between file characteristics and object properties.

- Each object in the visualisation represents a file. Files are **ordered** on the disc by date as selected at the start.
- Zoom in close to see **text** showing the name, last access date, last modification date and creation date of a file.
- The shape represents the access permission of a file: **pyramid** (execute permission), **truncated pyramid** (write and execute permissions), **cube** (write permission), **cylinder** (no permissions).
- In the case of **images files**, the image is shown above the shape.
- Different **colours** represent different file extensions.

The 3D approach allows the user to switch between a broad overview containing all of the files accessed within a given time period, to a close-up view of individual files, quickly and easily using gesture controls. The ease of switching, which we feel is an important characteristic of the system, is made possible by the ability to scale the representation using simple gestures. However, we believe the situated 3D representation is also important for allowing users to perform these actions intuitively, since they are easily relatable to real-world actions. However, this has yet to be determined empirically. The actions used to control the visualisation are as follows.

Figure 4:
1. Translation

Figure 5:
2. No movement

Figure 6:
3. Rotation

1. Translation: **Hand flat, fingers apart:** move the camera in the direction of your hand movement.
2. No movement: **Hand flat, fingers together:** ignore hand movement.
3. Rotation: **Fist:** rotate the camera in the direction of your movement.

Gestures are detected using a commercial LeapMotion device [1], which requires the use to hold their hand around 20cm above the sensor.

II. DESIGN

Control of the developed system has been streamlined. In addition to the mouse and keyboard inputs to control the GUI, the natural gestures of human hand can be used to control the system. To capture the gestures of hand, a Leap Motion controller is used.

Fig. 7: Using hand gestures to control the system

In order to improve ease of use, the system recognizes three states of the human hand. Fig. 8 shows the system controlled by hand gestures. The first state is a move state. In this state a user can change the viewpoint position via her/his hand while the fingers are open. This state allows users to move the viewpoint of the camera in 3 dimensions. Users can zoom in/ zoom out on the Y-axis or can move around on the X and Z axis. In Fig. 8 the user is examining objects from a distance and by using hand gestures the user can zoom in to see the objects from a particular viewpoint.

Second state is rotation, which permits a user to rotate the camera to see objects from different perspectives while the user is making a fist shape with the hand.
The third state is an idle state. In this state the system controller does not detect gestures from a user's hand. The fingers are closed in order to achieve this state. Despite the third state's not detecting any gestures, it is the most important of all three states because it overcomes the instability and unsteadiness problems of human hand. By combining an open fingers state and closed fingers state, users achieve successive movement to permit movement around objects contained on the storage media.
Unified Modelling Language (UML) has been used for the gestural control of the system. Fig. 8 shows a state transition diagram of the gestural control of the system.

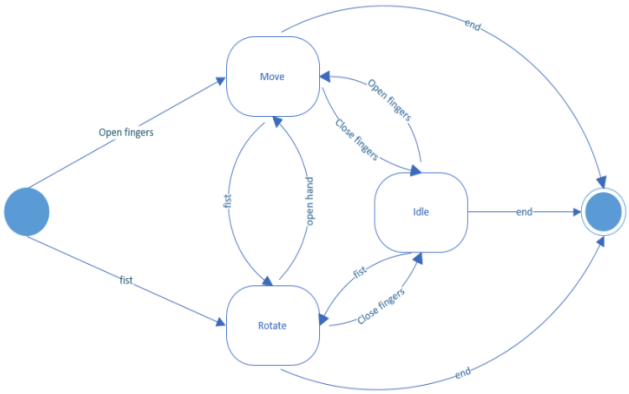

Fig. 8 State transition diagram of the system

In the system developed, information about files stored on the hard drive is represented using various 3D attributes. The height attribute of an object represents the size of a file whereas the colour attribute displayed represents the file type. Employing these two attributes assist greatly in the interpretation of stored files on the storage media. In addition, employment of these two attributes allows investigators to understand the relationship between file properties. Fig. 9 displays a screen shot of the system. It can be seen (Fig.10) the type and size of each file is readily apparent.

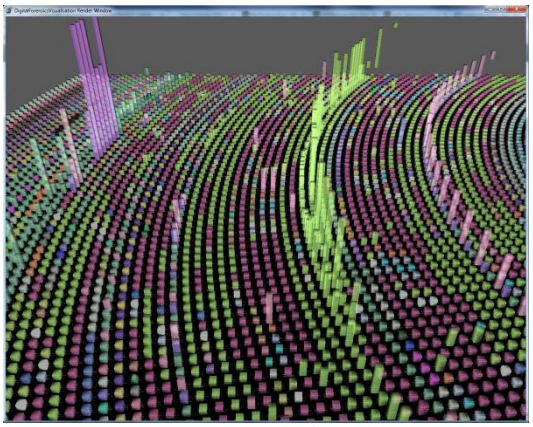

Fig. 9: Colour and height represent file type and size.

The attribute shape displayed for a file represents the permissions of a file. There are four different shapes used in the developed system. The shapes employed are: cube, frustum, cylinder and triangular pyramid. Frustum shapes represent files that have both write and execute permission granted. Whereas the cube shapes represent files with only write permission assigned. Pyramid shapes, on the other hand, represent files with only execute permission granted and finally, cylinder shapes represent files with no permission to write or execute granted. The file name, file last access time, file creation time and file modification time information are displayed attached to the attribute shapes described. The four shapes are illustrated (Fig. 10) below.

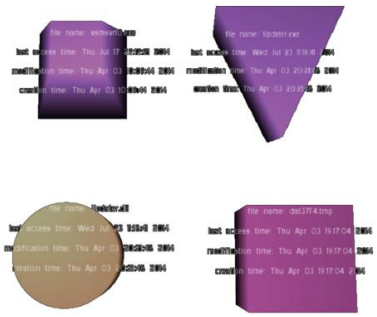

Fig. 10: Representation of different file permissions

The position of a file in the system is represented by the creation time or last accessed time of the file, or the last modification time of the file depending on the choice of the investigator. Therefore, all of the objects in the system are sorted in chronological order. This feature allows users to trace the time relationship between stored files.

A GUI (graphical user interface) is provided for forensics investigators to filter stored files according to chosen criteria. Forensics investigators can select files that have been created, accessed, or modified between chosen time intervals. To accomplish this, investigators first enter date intervals, and then they choose their criteria for sorting the results of the given search. Files may be sorted in reverse order since recently accessed files are more likely to become evidence.

Figure 11 illustrates the circular shape in which the time of the file changes diverging from the centre of the shape.

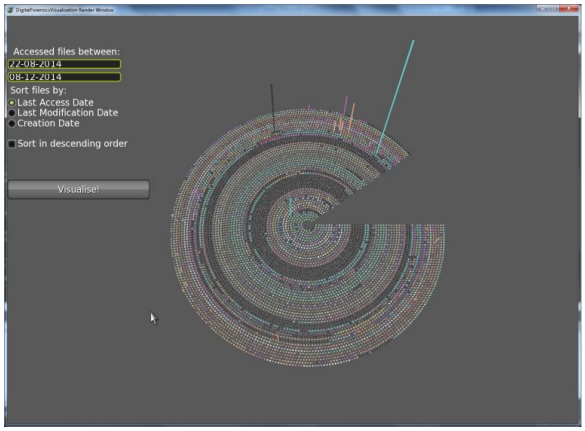

Fig. 11 Files are sorted in chronological order

All of the objects displayed are rendered transparent in order to avoid one object covering others. This feature also helps users to control the complexity of the displayed information.
Fig.12 shows the transparency of the 3D objects.

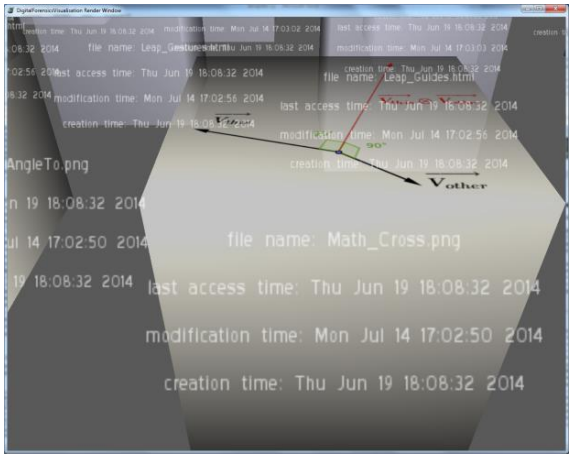

Fig. 12 Slightly transparent objects

Image files have a crucial impact in forensics investigations. Considering this impact, the system is designed to show a preview of the image on the top of the object using a

Table 1: Keystrokes and Gestures

#of hand gestures	#of key strokes	#of mouse clicks	#of key strokes + mouse clicks
1991	983	1604	2587

UV mapping technique in order to help forensics investigators easily and quickly detect suspicious image files.

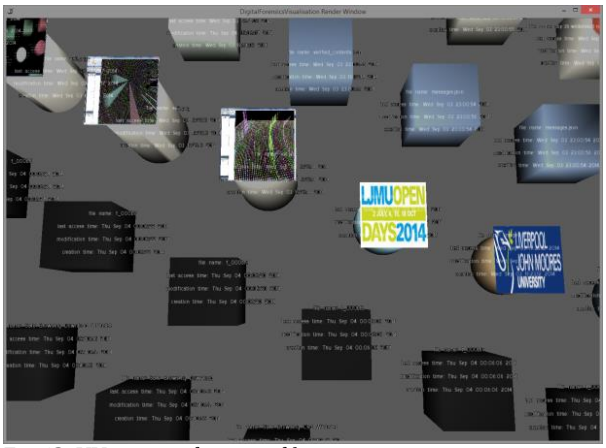

Fig. 13: UV mapping for image files

III. TEST RESULTS

During the FTK tasks, the users completed a total of 983 key strokes and 1604 mouse clicks and performed the same tasks, using 1991 hand gestures with the Visualdrives tool.

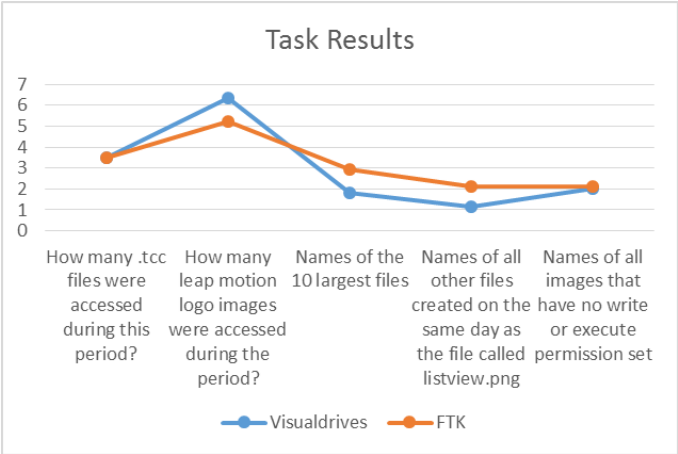

Figure 14: Graph illustrating the results of tasks using FTK and Visualdrives

Figure 14 shows the results of tasks performed using FTK and Visualdrives software. The Y-Axis of the graph depicts the results of tasks performed that have been divided by the duration of the performance of each task. Further, the results indicate that the approach adopted by FTK improves the performance of the third, fourth, and fifth tasks. Visualdrives on the other hand, produce superior results in the second task, which is related with identifying visual data. In the first task, the results are the same for both tools.

IV. CONCLUSION

The use of a novel 3D visualisation, combined with LeapMotion gesture control, is intended to support rapid transition between macro-level and detailed data visualisation across multiple dimensions of the data. Ultimately, this will allow forensic investigators to better identify and hone in on the most fruitful areas for further study.

REFERENCES

[1] [1] Leap Motion Inc., "LeapMotion," 2014. [Online]. Available: https://www.leapmotion.com/. [Accessed: 02-Oct-2014].

[2] [2] U. Wiss and D. A. Carr, "An empirical study of task support in 3D information visualizations," in 1999 IEEE International Conference on Information Visualization (Cat. No. PR00210), 1999, pp. 392–399.

[3] [3] P. Cignoni, C. Montani, and R. Scopigno, "Magicsphere: an insight tool for 3D data visualization," Computer Graphics Forum, vol. 13, no. 3, pp. 317–328, Aug. 1994.

[4] [4] A. Kobsa, "User Experiments with Tree Visualization Systems," in IEEE Symposium on Information Visualization, 2004, pp. 9–16.

[5] [5] F. van Ham and J. J. van Wijk, "Beamtrees: compact visualization of large hierarchies," Information Visualization, vol. 2, no. 1, pp. 31–39, Mar. 2003.

[6] [6] I. Herman, G. Melancon, and M. S. Marshall, "Graph visualization and navigation in information visualization: A survey," IEEE Transactions on Visualization and Computer Graphics, vol. 6, no. 1, pp. 24–43, 2000.

[7] [7] S. Teelink and R. F. Erbacher, "Improving the computer forensic analysis process through visualization," Communications of the ACM, vol. 49, no. 2, p. 71, Feb. 2006.

[8] [8] D. Ellis, L. Pritchard, and J. C. Roberts, "Forensic Visual Analytics of User Computing Activities," in The Third International UKVAC Workshop on Visual Analytics (VAW2011), University College London, 2011, pp. 1–4.

[9] [9] G. Schrenk and R. Poisel, "A Discussion of Visualization Techniques for the Analysis of Digital Evidence," in 2011 Sixth International Conference on Availability, Reliability and Security, 2011, pp. 758–763.

[10] [10] G. Osborne and B. Turnbull, "Enhancing Computer Forensics Investigation through Visualisation and Data Exploitation," in 2009 International Conference on Availability, Reliability and Security, 2009, pp. 1012–1017.