

Defining Digital Forensic Examination and Analysis Tools

Brian Carrier
carrier@atstake.com

August 7, 2002

2 Definitions

The Digital Forensics Research Workshop in 2001 defined Digital Forensic Science as [6

appropriate data structures are displayed. The data that represents the directory contents exist in the acquired file system image file, but in a format that is too low to identify. The directory is a layer of abstraction in the file system. Examples of non-file system layers of abstraction include:

ASCII

HTML Files

Windows Registry

To help identify the risk of unknown bugs in a given tool, each tool could have a margin of Tool Implementation Error

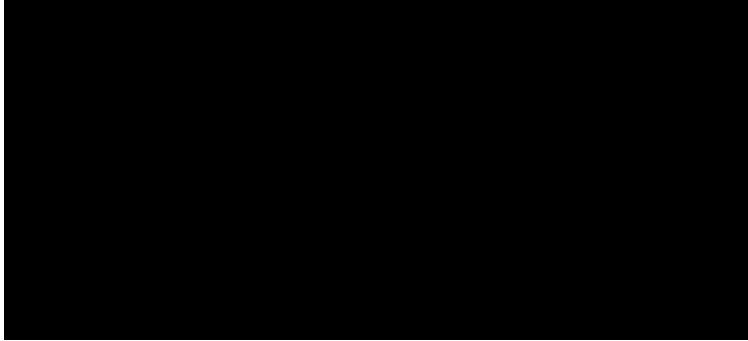


Figure 2: Levels and layers of abstraction of an HTML document

the needs of an application. The last layer in a level of abstraction is called the Boundary

the results can be interpreted appropriately.

Deterministic To ensure the accuracy of a tool, it must always produce the same output when given a translation rule set and input.

Verifiable To ensure the accuracy of a tool, one needs to be able to verify the results. This can be done manually or by using a second and independent toolset. Therefore, one needs access

the acquisition was done of the raw partition using a tool such as the **UNIX dd tool**. This layer uses the defined **Boot Sector structure** and extracts out the size and location values. Examples of extracted values

	Input	Output
--	--------------	---------------

