Random Cookie Names

As forensic examiners will be aware, Microsoft Internet Explorer stores cached data within randomly assigned folders. This behaviour was designed to prevent Internet data being stored in predictable locations on the local system in order to foil a number of attack types. Prior to the release of Internet Explorer v9.0.2, cookies were an exception to this behaviour and their location was insufficiently random in many cases.

Cookie Files

Generally, for Vista and Windows 7, cookie files are stored in the location shown below:

Microsoft Windows Internet Explorer Cookie Location
`\AppData\Roaming\Microsoft\Windows\Cookies\`

The cookie filename format was the user's login name, the @ symbol and then a partial Hostname for the domain of the cookie.

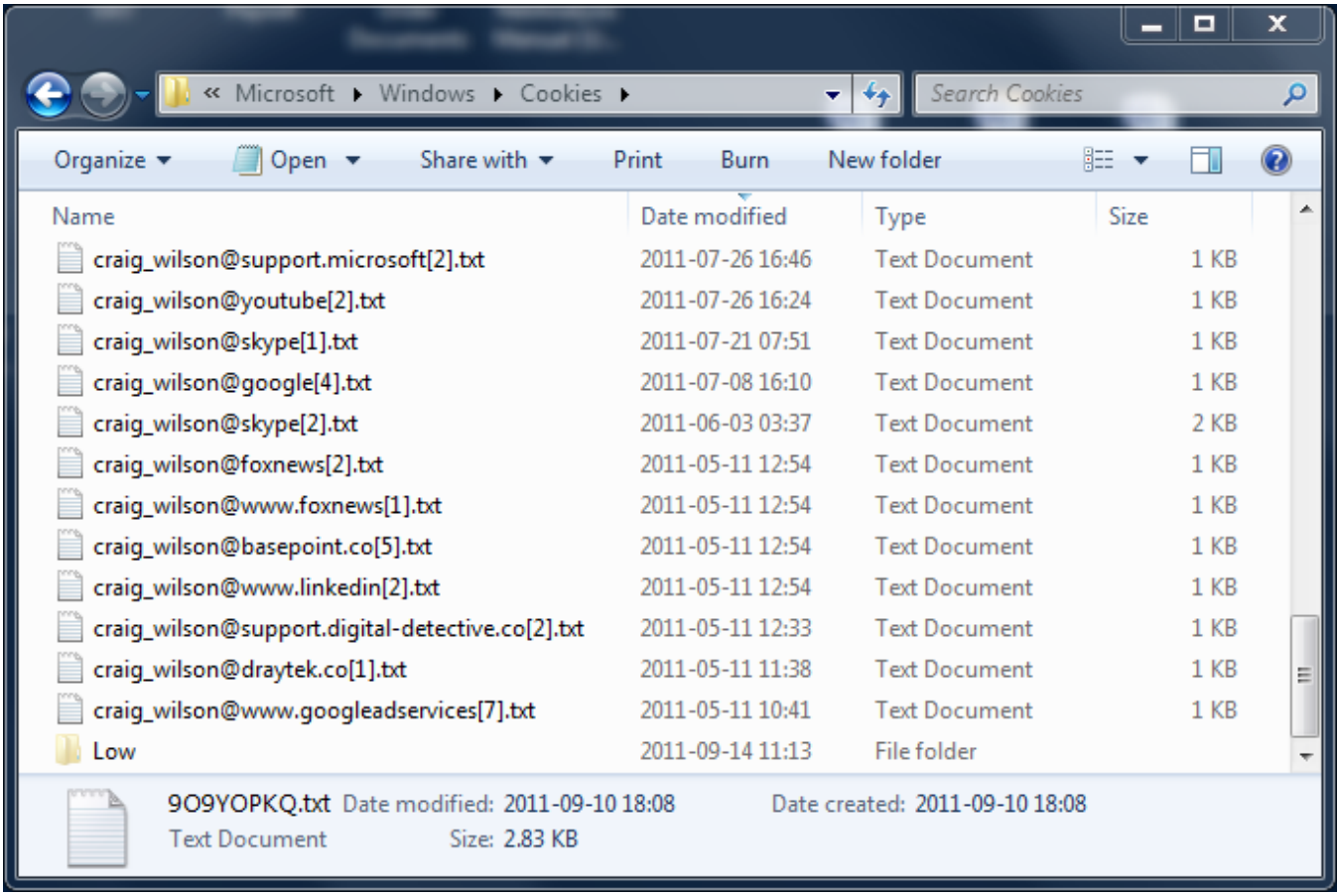

Figure 1

With sufficient information about a user's environment, an attacker might have been able to establish the location of any given cookie and use this information in an attack. To mitigate the threat, Internet Explorer 9.0.2 now names the cookie files using a randomly-generated alphanumeric string. Older cookies are not renamed during the upgrade, but are instead renamed as soon as any update to the cookie data occurs. Figure 2 shows an updated cookie folder containing the new files.

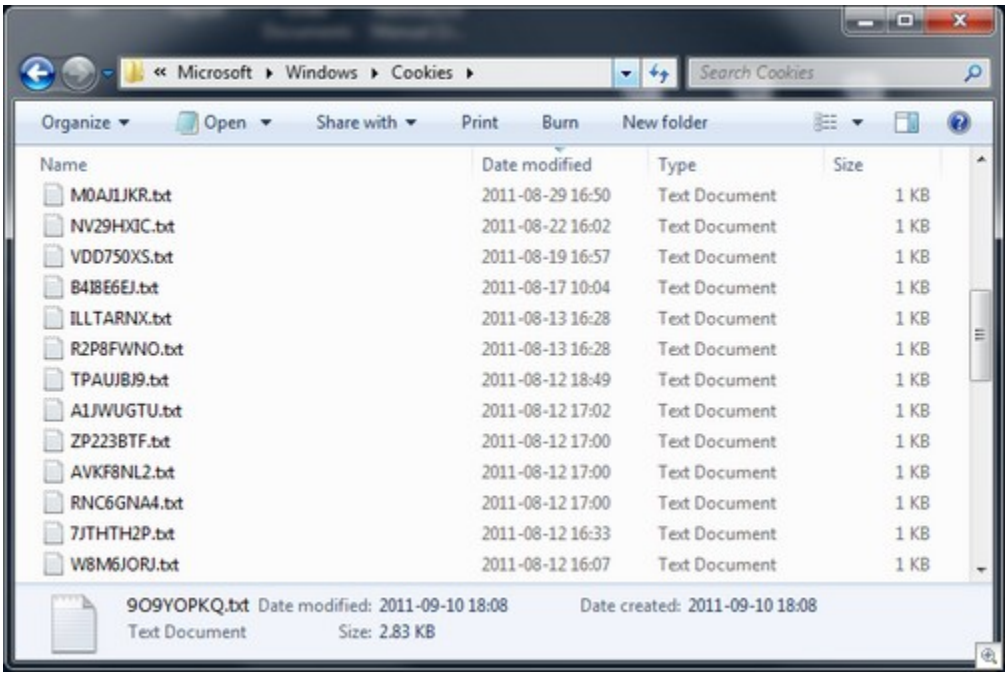

Figure 2

This change will have no impact on dealing with the examination of cookie data. It will obviously no longer be possible to identify which domain a cookie belongs to from just the file name.

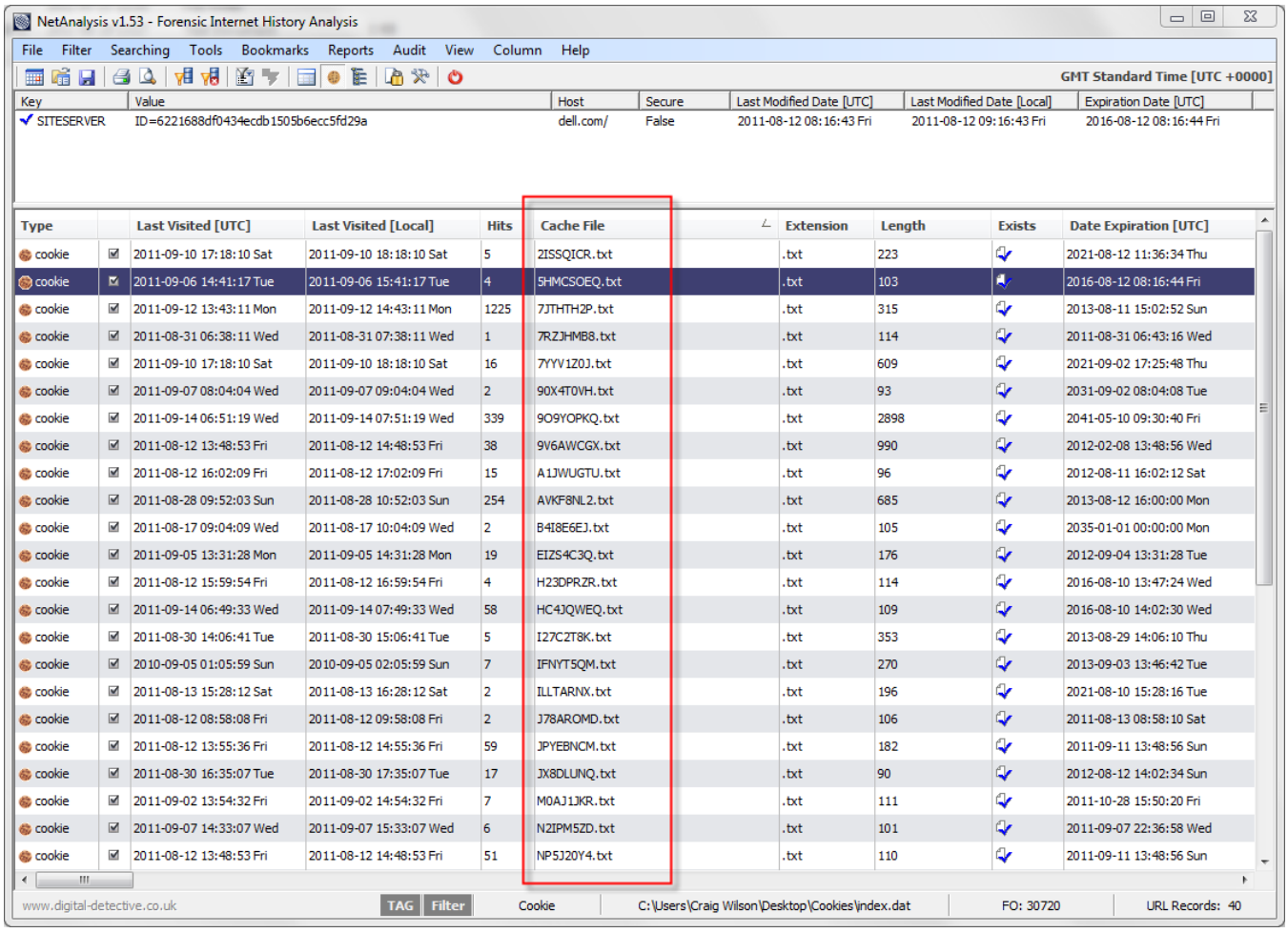

Figure 3

Figure 3 shows NetAnalysis displaying the new format cookies.