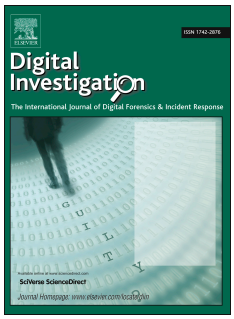
Accepted Manuscript



Navigating the Windows Mail database

Howard Chivers

PII: S1742-2876(17)30354-7

DOI: 10.1016/j.diin.2018.02.001

Reference: DIIN 742

To appear in: *Digital Investigation*

Received Date: 10 November 2017

Accepted Date: 4 February 2018

Please cite this article as: Chivers H, Navigating the Windows Mail database, *Digital Investigation* (2018), doi: 10.1016/j.diin.2018.02.001.

Navigating the Windows Mail Database

Howard Chivers[1]

Department of Computer Science, The University of York

Abstract

The Windows Mail application in Windows 10 uses an ESE database to store messages, appointments and related data; however, field (column) names used to identify these records are hexadecimal property tags, many of which are un- documented. To support forensic analysis a series of experiments were carried out to diagnose the function of these tags, and this work resulted in a body of related information about the Mail application. This paper documents prop- erty tags that have been diagnosed, and presents how Windows Mail artifacts recovered from the ESE *store.vol* database can be interpreted, including how the paths of file recorded by the Mail system are derived from database records. We also present example emails and appointment records that illustrate forensic issues in the interpretation of message and appointment records, and show how additional information can be obtained by associating these records with other information in the ESE database.

Keywords: Windows Mail, email, message, appointment, calendar, ESE, Database, store.vol, unistore, ESECarve

1. Introduction

The Microsoft Extensible Storage Engine (ESE[1]) is important to foren- sic practitioners because of the growing number of applications that use this

*Corresponding author

Email address: hrchivers@iet.org (Howard Chivers)

[1]We acknowledge Microsoft copyright in terms used in this paper to describe Microsoft products, including: Windows, Windows 10, unistore and ESE