EtwDump User Guide

User Guide of EtwDump for Windows 10 Mobile

Version: 3.0.1.0

Date: 06/24/2016

Table of Contents

[Table of Contents 2](#_Toc454536298)

[1 Notices 3](#_Toc454536299)

[2 Introduction 3](#_Toc454536300)

[3 Installation Instruction 3](#_Toc454536301)

[4 Update Instruction 3](#_Toc454536302)

[5 Uninstallation Instruction 3](#_Toc454536303)

[6 Runtime Dependencies 3](#_Toc454536304)

[7 Usage 3](#_Toc454536305)

[7.1 Help 3](#_Toc454536306)

[7.2 Example of Execution 4](#_Toc454536307)

[8 Known Issues and Workarounds 5](#_Toc454536308)

# Notices

None.

# Introduction

EtwDump is a desktop tool which converts ETW files into text/csv/html formats.

EtwDump has the following contents:-

|  |  |
| --- | --- |
| Filename | Description |
| EtwDump.exe | Desktop binary |
| EtwDump\_UserGuide.docx | This user guide document |

# Installation Instruction

EtwDump is installed as part of Windows 10 Mobile CPTT installation.

# Update Instruction

EtwDump is updated as part of Windows 10 Mobile CPTT update.

# Uninstallation Instruction

EtwDump is uninstalled as part of Windows 10 Mobile CPTT uninstallation.

# Runtime Dependencies

EtwDump requires .NET 4.5 to be installed.

EtwDump uses manifests from Windows 10 Mobile kit.

# Usage

## Help

Microsoft (R) ETWDUMP Version 3.0.1.0

Copyright (C) Microsoft Corporation 2013-2016. All rights reserved.

ETWDUMP <ETL path> -import <manifest path> -o <output filename>

[-of <TEXT|CSV|HTML|ALL>] [-y] [-missing] [-filter]

[-utc] [-tz <offset>] [-debug]

Parameters:

<ETL path> : ETL files or folder to be decoded.

-import <manifest path>: Path to the manifest files.

Semicolon can be used for multiple paths.

-o <output filename> : Output filename.

Note that any given file extension is ignored.

Options:

-of [TEXT/CSV/HTML/ALL]: Output file format.

Optional, default is TEXT.

-y : Overwriting output files without confirmation.

Optional, default is prompt for overwrite.

-missing : Report missing provider GUIDs from manifests.

Optional, default is do not report.

-filter : Filter undecoded messages.

Optional, default uses the provider GUID as name.

-utc : Convert timestamps to UTC time.

Optional, default is use raw tracert timestamps.

-tz <offset> : Convert timestamps to a specific offset from UTC.

Optional, offset in minutes and can be negative.

E.g. PST -480, PDT -420, CET 60, CEST 120,

EET 120, EEST 180, CST 480

-debug : Show tracerpt command lines.

Optional, default is to not show them.

Example:

1) ETWDUMP logs\w\*.etl\* -import D:\Manifests -o decoded -of text

: logs\w\*.etl\* files are decoded with D:\Manifests files,

and the file decoded.txt is created as output.

2) ETWDUMP \*.etl -import D:\Manifests -o decoded.txt -of all

: \*.etl files in current folder are decoded with D:\Manifests files,

and the files decoded.txt/decoded.csv/decoded.htm are created as output.

## Example of Execution

D:\EtwTest> **etwdump.exe \*.etl\* -import "C:\Program Files (x86)\Windows Kits\10\Manifests";D:\MoreManifests -o Decoded.dat -of ALL -y -utc**

Microsoft (R) ETWDUMP Version 3.0.1.0

Copyright (C) Microsoft Corporation 2013-2016. All rights reserved.

Options:

Manifest Path = C:\Program Files (x86)\Windows Kits\10\Manifests;D:\MoreManifests

ETL Path = \*.etl\*

Output Path = Decoded.dat

Output Format = ALL

Output Overwrite = yes

Report Missing = no

Filter Undecoded = no

UTC timestamps = yes

UTC offset = n/a

tracerpt debug = no

Creating temp folder ...

Copying all manifest files from C:\Program Files (x86)\Windows Kits\10\Manifests to temp folder ...

Copying all manifest files from D:\MoreManifests to temp folder ...

Preprocessing manifest files ...

WARNING: Duplicated provider c72d385e-3a63-4e6d-8393-9399a36bd6e4

Microsoft-WindowsPhone-PhoneAudioSrv.mc

Microsoft-WindowsPhone-AudioRouting.mc

Parsing ETL files ...

Decoding WinPhoneCircular.etl ...

Decoding WinPhoneCritical.etl ...

Merging decoded results ...

Parsing WinPhoneCircular.xml ...

Parsing WinPhoneCritical.xml ...

Sorting decoded results ...

Writing final results in format TEXT ...

WARNING: Unknown provider {dd4ac270-4867-49a1-b6cc-fa2e39325865} encountered.

WARNING: Unknown provider {3e542731-dbcf-47b3-aed9-c2bee11a5497} encountered.

=> Decoded.txt has been created successfully.

Writing final results in format CSV ...

=> Decoded.csv has been created successfully.

Writing final results in format HTML ...

=> Decoded.htm has been created successfully.

Deleting temp folder ...

# Known Issues and Workarounds

None.