

CLAIMS TESTING APPLICATION FORM

FORM NUMBER: ADPC 0046



SECTION 1 – APPLICANT INFORMATION

Company Name: Horizon Technology, LLC

Address: 1 Rancho Circle, Lake Forest CA 92630 USA

General Contact

Name: Stephen Buckler

Phone: 781-544-4036

Mobile: 617-784-5946

E-Mail: stephen.buckler@horizontechnology.com

SECTION 2 – APPLICANT SOFTWARE INFORMATION

Manufacturer: Prosoft Engineering Inc.

Version of software: Media Tools Wipe 1.2.1 (v160218)

Background (Explanation of the company and software)

Horizon is a US based company supporting storage products and services including sales of both HDD and SSD, value added services including testing and flashing of HDD/SSD and storage asset recovery services including data sanitization, destruction and sales of storage assets.

Technical / physical architecture of claims test applicant software.

Installed and executed through Microsoft Windows 10 Operating System utilizing x64-based PC.

Best practice usage guide for usage of software being tested. (Please enclose any manuals)

To be provided.

Host information for claims test applicant software to run on. To be shipped by test claimant.

A flash drive with pre-loaded software. SATA Solid State and Spinning disk

SECTION 3 – TEST HARDWARE INFORMATION

1 spinning media drives and 1 solid state drives with data in them.

ADISA Threat Matrix

RISK LEVEL	THREAT ACTOR AND COMPROMISE METHODS	TEST LEVEL
1 (Very Low)	Casual or opportunistic threat actor only able to mount high-level non-invasive and non-destructive software attacks utilising freeware, OS tools and COTS products.	1
2 (Low)	Commercial data recovery organisation able to mount non-invasive and non-destructive software attacks and hardware attacks.	1
3 (Medium)	Commercial computer forensics organisation able to mount both non-invasive/non-destructive and invasive/ non-destructive software and hardware attack, utilising COTS products.	2
4 (High)	Commercial data recovery and computer forensics organisation able to mount both non-invasive/non-destructive and invasive/ non-destructive software and hardware attack, utilising both COTS and bespoke utilities.	2
5 (Very High)	Government-sponsored organisations or an organisation with unlimited resources and unlimited time capable of using advanced techniques to mount all types of software and hardware attacks to recover sanitised data.	3

CLAIMS TESTING APPLICATION FORM



SECTION 4 – THE CLAIM

"Prosoft Engineering Inc.'s product called "Media Tools Wipe version 1.2.1" when used in accordance with User Manual "Media Tools 1.2.1 Wipe Guide" will overwrite all user data on the hardware sample within this test to protect from a forensic attack equivalent to test level 2 of the ADISA threat matrix. Upon successful sanitization, it produces a Certificate of Sanitization to validate the media serial number has been processed

I, Stephen Buckler of Horizon Technology confirm that the information outlined in this document is an accurate and true reflection of the claims made by our product wishing to undergo the ADISA testing method.

Signed on behalf of _____

SIGNED:

NAME: Stephen Buckler

TITLE: Chief Operating Officer

DATE: 5/1/2018

ACCEPTANCE

Claim Accepted by:

SIGNED:

NAME: A. Blyth, PhD.

TITLE: Professor

DATE: 23rd May 2018

SIGNED:

NAME: STEVE MELLINGS

TITLE: DIRECTOR

DATE: 25-5-2018