University of South Wales
Prifysgol De Cymru

ADISA
ASSET DISPOSAL & INFORMATION SECURITY ALLIANCE

Products Claims Testing
Claims Test ADPC0033
Extreme Protocol

Author: Professor Andrew Blyth,
University of South Wales

Revision 1.0
Date: February 21, 2018
Distribution: Confidential

DISCLAIMER

The Product Claims Test is presented as the outcome of a specific test ran in laboratory environment under controlled conditions. Use of this certified product for the purpose of sanitizing data from devices tested needs to be done so after a risk assessment process. ADISA reserves the right to review the validity of this award upon changes in threat landscape.

LIABILITY

ADISA accepts no liability for any claims resulting from the use of the product tested.

REVISION HISTORY

16/02/2018 Revision 1.0 issued to Steve Mellings

ADISA ASSET DISPOSAL & INFORMATION SECURITY ALLIANCE

Asset Disposal and Information Security Alliance Limited

Phone: 0044 845 557 7726

Web: www.adisa.global

Registration Number: 07390092
Registered Office: 50 Brook Street, London, W1K 5DR, United Kingdom

University of South Wales Prifysgol De Cymru

University of South Wales

Phone: 0044 845 576 0101

Web: www.southwales.ac.uk

Contents

1.0 Executive Summary

This is a preliminary report detailing the findings in relation to the execution of the ADISA Testing Methodology on Claims Test ADPC0033 submitted by Extreme Protocol in January 2018.

The claims test was carried out in accordance with ADISA Claims Testing (ACT) v1.0 and supporting document ADISA Testing Methodology v1.0, both of which are available from ADISA.

The claim made for the drive was:

> *"Extreme Protocol Solutions Inc. software/ product called XErase Enterprise Data Erasure, when used in accordance with User Manual V12.0 will overwrite data / destroy data carrying media on the hardware sample within this test to protect from a forensic attack equivalent to test level 2 of the ADISA threat matrix.*
>
> *Specifically, the NIST 800-88 Rev1 Purge Erasure Method will perform the functions supported by each individual drive. These include Block Erase, Block Overwrite and Cryptographic Erasure.*
>
> *Additionally, the 3x Wrt/Vfy – DoD Sanitize performed on a hard drive will apply a pattern, it's compliment and finally a repeating random block of data to all accessible blocks of the media making any previous data unrecoverable.*
>
> *Erasure methods can be selected by using the Wrench/Screwdriver Button in XErase and selecting the appropriate method prior to the start of each test.- Claim Number ADPC0033."*

Four devices were submitted as part of this test and these are listed below:

Device	***Test Level***
Micron 2.5 SSD / Model: MTFDDAK256TBN	1 and 2
SanDisk Lightening Enterprise Class SSD / Model: LB406M	1 and 2
Dell Enterprise 1Tb SAS / Model: ST91000642SS	1 and 2
WD Scorpio Blue 500GB SATA / Model: WD5000BPVT	1 and 2

After testing it is confirmed that the Extreme Protocol **claim is true** for the devices tested up to Test Level 1 results. Those devices are:

- Micron 2.5 SSD Model: MTFDDAK256TBN
- SanDisk Lightening Enterprise Class SSD Model: LB406M
- Dell Enterprise 1Tb SAS Model: ST91000642SS
- WD Scorpio Blue 500GB SATA Model: WD5000BPVT

After testing it is confirmed that the Extreme Protocol **claim is true** for the devices tested up to Test Level 2 results. Those devices are:

- Micron 2.5 SSD Model: MTFDDAK256TBN
- SanDisk Lightening Enterprise Class SSD Model: LB406M
- Dell Enterprise 1Tb SAS Model: ST91000642SS
- WD Scorpio Blue 500GB SATA Model: WD5000BPVT

2.0 Test Level 1 Testing Solid State and Electromagnetic Drives

2.1 Methodology.

This test phase is designed to evaluate the claim made by recreating an attack by a threat adversary utilising standard COTS forensic tools and techniques.

For each computer hard drive device, the following methodology is performed:

1. Structured data, the string "ISRG", was written to every logical block address on the hard drive.
2. The device was then imaged using Access Data / FTK to create a base-line forensic image.
3. The device was then erased using the XErase – Enterprise Data Erasure V12 in accordance with the manufacturer's instructions.
4. The device was then analysed use using the following tools to create a second forensic image:
    a. Standard commercial tools and techniques such as Access Data/FTK and Encase.
5. The two forensic images (Stage 3 and Stage5) were then compared and contrasted to ensure that all structured data had been removed.
    a. For this test, there is no tolerance for remnant structured data and the result is a straight Pass or Fail.

2.2 Test Results.

Test Level 1 Summary Results

Test Level 1 replicated an attack on these devices being made by an aggressor with capabilities outlined below.

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

The Results of Test Level 1.

Hard Drive/Model	***Result***
Micron 2.5 SSD / Model: MTFDDAK256TBN	PASS
SanDisk Lightening Enterprise Class SSD /Model: LB406M	PASS
Dell Enterprise 1Tb SAS / Model: ST91000642SS	PASS
WD Scorpio Blue 500GB SATA / Model: WD5000BPVT	PASS

Pass means that the Extreme Protocol XErase – Enterprise Data Erasure V12 mitigates the threat posed by the Threat Actors holding the capabilities outlined by Test Level 1 on the tested devices and the claim made can be confirmed. A key element to the claims test is that the software has to be used in accordance with the manufacturers user manual.

3.0 Test Level 2 Testing Solid State Drive

3.1 Methodology.

This test phase is designed to evaluate the claim made by recreating an attack by a threat adversary utilising standard intrusive/destructive testing tools designed to read data directly off the device at the platter/chip level.

For each computer hard drive device, the following methodology is performed:

1. The device is connected to a target PC and place in a stable state.
2. Structured data, the string "ISRG", was written to every logical block address on the hard drive.
3. The device was then imaged using Access Data/FTK to create a base-line forensic image.
4. The device was then erased using the XErase – Enterprise Data Erasure V12 in accordance with the manufacturer's instructions.
5. The device was then analysed use the following tools and techniques to create a series of forensic images that are compared and contrasted with the base-line forensic image to ensure that all structured data has been removed. For this test, there is no tolerance for remnant structured data and the result is a straight Pass or Fail.
    a. Software based forensic tools/techniques such as:
        i. Standard commercial tools and techniques such as Access Data/FTK and ENCase;
        ii. State of the art data recovery tools such as PC3000 SSD;
        iii. Customer designed data recovery software.
    b. Hardware/Chip based forensic tools/techniques such as:
        i. Flash/NAND TSOP/BGA chip readers;
        ii. State of the art data recovery tools such as PC3000 FLASH and Rusolut;
        iii. Customer designed data recovery software/hardware.

3.2 Test Results.

Test Level 2 Summary Results

Test Level 2 replicated an attack on these devices being made by an aggressor with capabilities outlined below.

Risk Level	Threat Actor and Compromise Methods	Test Level
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

The Results of Test Level 2.

Hard Drive/Model	*Result*
Micron 2.5 SSD / Model: MTFDDAK256TBN	PASS
SanDisk Lightening Enterprise Class SSD / Model: LB406M	PASS

Pass means that the Extreme Protocol XErase – Enterprise Data Erasure V12 mitigates the threat posed by the Threat Actors holding the capabilities outlined by Test Level 2 on the tested devices and the claim made can be confirmed. A key element to the claims test is that the software has to be used in accordance with the manufacturers user manual.

4.0 Test Level 2 Testing Electromechanical Drive

4.1 Methodology.

This test phase is designed to evaluate the claim made by recreating an attack by a threat adversary utilising standard intrusive/destructive testing tools designed to read data directly off the device at the platter/chip level.

For each computer hard drive device, the following methodology is performed:

1. The device is connected to a target PC and place in a stable state.
2. Structured data, the string "ISRG", was written to every logical block address on the hard drive.
3. The device was then imaged using Access Data/FTK to create a base-line forensic image.
4. The device was then erased using the XErase – Enterprise Data Erasure V12 in accordance with the manufacturer's instructions.
5. The device was then analysed use the following tools and techniques to create a series of forensic images that are compared and contrasted with the base-line forensic image to ensure that all structured data has been removed. For this test, there is no tolerance for remnant structured data and the result is a straight Pass or Fail.
    a. Software based forensic tools/techniques such as:
        i. Standard commercial tools and techniques such as Access Data/FTK and Encase;
        ii. State of the art data recovery tools such as PC3000 UDMA/SAS;
        iii. Customer designed data recovery software.

4.2 Test Results.

Test Level 2 Summary Results

Test Level 2 replicated an attack on these devices being made by an aggressor with capabilities outlined below.

Risk Level	Threat Actor and Compromise Methods	Test Level
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

The Results of Test Level 2.

Hard Drive/Model	*Result*
Dell Enterprise 1Tb SAS Model: ST91000642SS	PASS
WD Scorpio Blue 500GB SATA Model: WD5000BPVT	PASS

Pass means that the Extreme Protocol XErase – Enterprise Data Erasure V12 mitigates the threat posed by the Threat Actors holding the capabilities outlined by Test Level 2 on the tested devices and the claim made can be confirmed. A key element to the claims test is that the software has to be used in accordance with the manufacturers user manual.

5.0 Summary and Conclusions.

Claims Test Result: Pass on all devices tested.

The two devices passed the claims test as all-forensic data recovery techniques up to and including ADISA Test Level 1 and 2 failed to recover any data. The software tested was the Extreme Protocol XErase – Enterprise Data Erasure V12.

Claims Test Carried Out By: Professor Andrew Blyth, PhD.

Test Facility: University of South Wales

Signature: 

Date: 15th February 2018

Appendix A Claims Test Application Form (copy)

ASSET DISPOSAL & INFORMATION SECURITY ALLIANCE

Claims Testing Application Form

Form Number ADPC0033

Section 1 – Applicant Information

Company Name: Extreme Protocol Solutions
Address: 10 River Road, Suite 101, Uxbridge, MA 01569 (USA)

General Contact
Name: Brian Therrien, ITAD Sales Director
Phone: 508-278-3600 Ext.115
Mobile: 508-422-6916
E-Mail: btherrien@extremeprotocol.com

Section 2 – Applicant Software Information

Manufacturer Extreme Protocol Solutions
Version of software XErase – Enterprise Data Erasure V12

Background (Explanation of the company and software)

Based in the United States, Extreme Protocol Solutions is an industry leader in software solutions for overwriting of both magnetic and solid-state media. This product has been in use by corporate and industrial clients. Extreme Protocol (EPS) has been in business since 1999 and its engineering team have over twenty years of expertise in storage and hard drive engineering.

Technical / physical architecture of claims test applicant software.

Extreme Protocol Solutions Inc. software/ product called XErase Enterprise Data Erasure, when used in accordance with User Manual V12.0 will overwrite/destroy data on both Magnetic Media (Hard Disk Drives) and Solid-State Media (SSD) to protect from a forensic attack equivalent to test level 2 of the ADISA threat matrix.

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

XErase Enterprise Data Erasure V12 Manual provides concise and detailed guidance for software operation across all deployment platforms.

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

EPS has varied solutions for direct connected erasure. At time of testing EPS will provide hardware and software to facilitate erasures using the various deployment methods indicated in the physical architecture claim section.

Section 3 – Test Hardware Information

EPS will provide 2 media samples for each of the following media types; magnetic media, and SSD media. These are:

1. Micron 2.5 SSD Model: MTFDDAK256TBN
2. SanDisk Lightening Enterprise Class SSD Model No: LB406M
3. Dell Enterprise Model number ST91000642SS
4. WD Scorpio Blue / 500GB / WD5000BPVT / SATA / Electromechanical Drive

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

Section 4 – The Claim

Extreme Protocol Solutions Inc. software/ product called XErase Enterprise Data Erasure, when used in accordance with User Manual V12.0 will overwrite data / destroy data carrying media on the hardware sample within this test to protect from a forensic attack equivalent to test level 2 of the ADISA threat matrix.

Specifically, the NIST 800-88 Rev1 Purge Erasure Method will perform the functions supported by each individual drive. These include Block Erase, Block Overwrite and Cryptographic Erasure.

Additionally, the 3x Wrt/Vfy – DoD Sanitize performed on a hard drive will apply a pattern, it's compliment and finally a repeating random block of data to all accessible blocks of the media making any previous data unrecoverable.

Erasure methods can be selected by using the Wrench/Screwdriver Button in XErase and selecting the appropriate method prior to the start of each test.

Claim Technical Contact at applicant.

Name: Brent Burkholder, VP of Engineering
Phone: 508-278-3600, Ext. 113
Mobile: 774-287-6257
E-Mail: bburk@extremeprotocol.com

Acceptance

I, Roger D. Gagnon of Extreme Protocol Solutions Inc. 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 Extreme Protocol Solutions Inc.

SIGNED:

NAME: Roger D. Gagnon

TITLE: President and CEO

DATE: 01/28/2018

Claim Accepted by:

Signed on behalf of University of South Wales

SIGNED:

NAME: Andrew Blyth

TITLE: Professor

DATE: 30.01.2018

Signed on behalf of ADISA

SIGNED:

NAME: Steve Mellings

TITLE: Director

DATE: 30.01.2018