ADISA Claims Test Report

Professor Andrew Blyth, Ph.D - andrew.blyth@southwales.ac.uk

17th June 2013

1 Introduction

This report documents the findings of a forensic test that was conduction on behalf of ADISA on the 17th Jun 2013. The target of the test was the eDR Hard Disk Crusher. The test was conducted in accordance with the ADISA Physical Destruction Claims Test Methodology v1.3. The claim made by eDR EUROPE / EDR SOLUTIONS LLC, is that

"An electromechanical hard disk drive will be destroyed in less that 15 seconds to the extent that any data contained on it is unrecoverable (Risk Level 4 on the ADISA Threat Matrix)."

Claim Number ADPC0007.

Reference: The ADISA Physical Destruction Claims Test Methodology Document
http://www.adisa.org.uk/wp-content/uploads/2013/06/ADISA-Physical-Destruction-Claims-Test-Methodology-v1.3.pdf

2 Methodology

The basic test methodology is outlined below.

- Data is placed on the drive in a forensically sound manner.
- The eDR Hard Disk Crusher is then applied to the drive
- Forensic tools in accordance to the ADISA threat levels 1, 2, 3 and 4 are applied to the drive in an attempt to recover data.

Five IDE/SATA 3.5" computer hard drives where selected at random and each drive was forensically wiped (0x00 written to every LBA on the hard drive), in accordance with the ACPO forensic guidelines. The makes and models of the five drives are listed below:

- Seagate 3.5" ST33232A - 3,2GB
- Western Digital 3.5" WD200 Protege - 20GB
- Samsung 3.5" SP0411N - 40GB
- Maxtor 3.5" Diamond Plus - 80GB
- Hitachi 3.5" Diskstar - 160GB

Each drive was then placed into the eDR Hard Disk Crusher and the time taken to crush the hard drive noted. The eDR Hard Disk Crusher was operated in accordance with the operators manual. Each hard drive was then connected to a forensic analysis workstation and in accordance with the ADISA Threat Matrix, forensic analysis techniques where applied to recover data from the hard-drive. The following are the results related to the ADISA threat matrix.

Threat level	Threat Description	Results
1	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.	Unable to Recover Data
2	Commercial data recovery organisation able to mount non-invasive and non-destructive software attacks and hardware attacks.	Unable to Recover Data
3	Commercial computer forensics organisation able to mount both non-invasive/non-destructive and invasive/ non-destructive software and hardware attack, utilising COTS products.	Unable to Recover Data
4	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.	Unable to Recover Data

3 Summary and Conclusions

All forensic data recovery techniques up to, and including, ADISA Threat Level 4 failed to recover any data from an electromechanical hard disk drive once it had been crushed by the eDR Hard Disk Crusher. The eDR Hard Disk Crusher never took longer that 15 seconds to crush an electromechanical hard disk drive.

4 Sign and Date

Name: Prof. A Blyth

Signature: 

Date: 17th June 2013

Appendix 1. The 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