KÜRT had been asked to process a detailed analysis of YouWipe edition v4.1.93.2010221419-945f40cc data erasure tool capabilities on hard disk drives with data recovery tools.

1. ASSIGNMENT

In response to YouWipe engagement KÜRT Data Recovery Lab have performed the test of the erasure capabilities of YouWipe tool on the following HDD devices:

1.	Model :	Seagate Barracuda ST1000DM003
	Serial number:	Z1D6GVFS
2.	Model:	Western Digital WD20EZRX-00D8PB0
	Serial number:	WCC4M5LSR3A0

2. ACTIVITIES

KÜRT test was performed in accordance with data recovery current technological standards and included the procedures considered necessary in the circumstances to obtain a reasonable basis for rendering the last opinion.

3. TEST LEVELS

Examination can include different Test Levels in the context of a desired defense against a certain Risk Level (ADISA) or Effort Level (NIST).

1. Test Level 1: NIST Clear, ADISA Risk level 1 (Low)
2. Test Level 2: NIST Purge, ADISA Risk Level 2 (Medium)

KÜRT Data Recovery performed the tests on Test Level 1 and Test Level 2.

4. EXAMINATION PROCESS

The examination was performed during the period 5 - 21. October 2020 and included the following steps:

1. A special - KÜRT specific - data pattern was written on the HDD's, filling the full available capacity of the HDD's.
2. Using YouWipe v4.1.93 software with "EXT HMG Infosec High" HDD Erasure Method, the HDD's were wiped following the instructions given with YouWipe software.
3. The HDD's were analyzed on low level (sector by sector) with several KÜRT Data Recovery software tools.
4. After the automatic analyze process a data recovery engineer verified the wiped HDD content (cross check of step 3).
5. Repeat step 1 to 4 with a different data pattern.

Based on KÜRT Data Recovery Lab experience it can be stated that this process is sufficient and appropriate to provide a good evidence for the conclusion. The result of the test process is this assurance report.

5. ASSURANCE TEST RESULT

Based on the outcome of the repeated test processes KÜRT Data Recovery can declare that after wiping the above-mentioned Hard Disk Drives with YouWipe v4.1.93.2010221419-945f40cc it is not possible to recover any recognizable data physically or logically. In addition, no trace of the prewritten pattern fragments could be determined at the logical or physical level.

6. APPENDICES

1. Appendix A: NIST SP 800-88 Rev.1 Media Sanitization Guide
2. Appendix B: ADISA Threat Matrix

7. DISCLOSURE

This report is intended only for customers who use YouWipe software or services. KÜRT Data Recovery gives the permission to YouWipe to place this Assurance Test Report on their website or within other related documentation.

October 27, 2020, Budapest

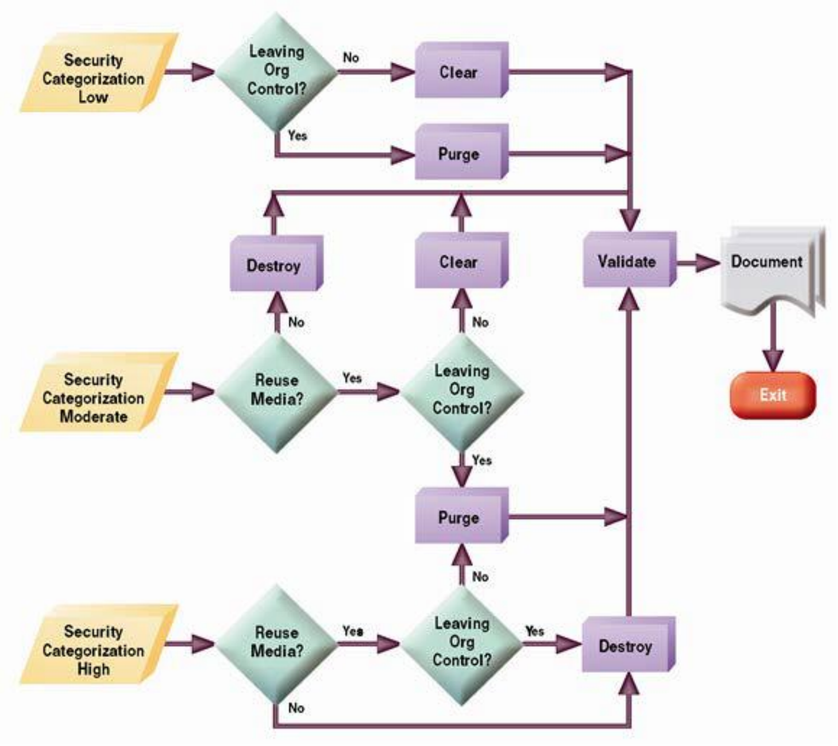
....

Zoltán Kertész

Head of KÜRT Data Recovery Division

Appendix A NIST Special Publication 800-88 Revision 1

Media sanitization refers to a process that renders access to target data on the media infeasible for a given level of effort. This guide will assist organizations and system owners in making practical sanitization decisions based on the categorization of confidentiality of their information.



In case of HDD Clear means:

Overwrite media by using organizationally approved and validated overwriting technologies/methods/tools. The Clear pattern should be at least a single write pass with a fixed data value, such as all zeros. Multiple write passes or more complex values may optionally be used.

In case of HDD Purge means:

1. Use one of the ATA Sanitize Device feature set commands, if supported, to perform a Sanitize operation. One or both of the following options may be available:
   a. The overwrite EXT command. Apply one write pass of a fixed pattern across the media surface. Some examples of fixed patterns include all zeros or a pseudorandom pattern. A single write pass should suffice to Purge the media. Optionally: Instead of one write pass, use three total write passes of a pseudorandom pattern, leveraging the invert option so that the second write pass is the inverted version of the pattern specified.
   b. If the device supports encryption and the technical specifications described in this document have been satisfied, the Cryptographic Erase (also known as CRYPTO SCRAMBLE EXT) command. Optionally: After Cryptographic Erase is successfully applied to a device, use the overwrite command (if supported) to write one pass of zeros or a pseudorandom pattern across the media. If the overwrite command is not supported, the Secure Erase or the Clear procedure could alternatively be applied following Cryptographic Erase.
2. Use the ATA Security feature set's SECURE ERASE UNIT command, if support, in Enhanced Erase mode. The ATA Sanitize Device feature set commands are preferred over the over the ATA Security feature set SECURITY ERASE UNIT command when supported by the ATA device.
3. Cryptographic Erase through the Trusted Computing Group (TCG) Opal Security Subsystem Class (SSC) or Enterprise SSC interface by issuing commands as necessary to cause all MEKs to be changed (if the requirements described in this document have been satisfied). Refer to the TCG and device manufacturers for more information. Optionally: After Cryptographic Erase is successfully applied to a device, use the overwrite command (if supported) to write one pass of zeros or a pseudorandom pattern across the media. If the overwrite command is not supported, the Secure Erase or the Clear procedure could alternatively be applied following Cryptographic Erase.
4. Degauss in an organizationally approved automatic degausser or disassemble the hard disk drive and Purge the enclosed platters with an organizationally approved degaussing wand.

Source: NIST Special Publication 800-88 Revision 1

Appendix B ADISA THREAT MATRIX

The threat matrix defines a series of capabilities and risks that various threat agents can pose on the security of a device.

THREAT CAPABILITY LEVEL	THREAT ACTOR AND COMPROMISE METHODS	TYPE OF ATTACK	COMPARISON
1 (Low)	Casual or opportunistic threat actor only able to mount high-level non-invasive and non-destructive software attacks utilizing freeware, COTS and OS tools,	Keyboard attacks from a motivated individual or professional organization. Typical attack could be using open-source forensic tools or commercial tools	Clear NIST 800–88 Rev 1 ISO 27040
2 (Medium)	Commercial data recovery and computer forensics organization able to mount invasive/destructive software and hardware attack, utilizing both COTS and bespoke software and software.	Laboratory attacks from commercial data recovery experts or specialist forensic scientists. Typical attack could be: Advanced data recover software, Chip Readers and protocol decoders. Typical attack would involve analysis of individual hardware components as well as protocol structures.	Purge NIST 800–88 Rev 1 ISO 27040
3 (High)	Government-sponsored organizations using advanced techniques to mount all types of software and hardware attacks with unlimited time and resources to recover sanitized data.	An attack agent of unknown capability and unlimited resource. Typical attacks: Taking theoretical forensic possibilities and making them an actual capability.	Destroy NIST 800–88 Rev 1 ISO 27040

Source: ADISA