

Intel[®] Management Engine

Braidwood Tools User Guide

April 2009

Revision 0.65

Intel Confidential



INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

This document contains information on products in the design phase of development.

All products, platforms, dates, and figures specified are preliminary based on current expectations, and are subject to change without notice. All dates specified are target dates, are provided for planning purposes only and are subject to change.

This document contains information on products in the design phase of development. Do not finalize a design with this information. Revised information will be published when the product is available. Verify with your local sales office that you have the latest datasheet before finalizing a design.

Code names featured are used internally within Intel to identify products that are in development and not yet publicly announced for release. Customers, licensees and other third parties are not authorized by Intel to use code names in advertising, promotion or marketing of any product or services and any such use of Intel's internal code names is at the sole risk of the user.

Intel and the Intel logo are trademarks of Intel Corporation in the U.S. and other countries.

*Other names and brands may be claimed as the property of others.

Copyright © 2009, Intel Corporation. All rights reserved.



Intel Software License Agreement

IMPORTANT—READ BEFORE COPYING, INSTALLING OR USING.

Do not use or load this software or any associated materials (collectively, the "Software") until you have carefully read the following terms and conditions. By loading or using the Software, you agree to the terms of this Agreement. If you do not wish to so agree, do not install or use the Software.

LICENSE—Subject to the restrictions below, Intel Corporation ("Intel") grants you the following limited, revocable, non-exclusive, non-assignable, royalty-free copyright licenses in the Software.

The Software may contain the software and other property of third party suppliers, some of which may be identified in, and licensed in accordance with, the "license.txt" file or other text or file in the Software:

DEVELOPER TOOLS—including developer documentation, installation or development utilities, and other materials, including documentation. You may use, modify and copy them internally for the purposes of using the Software as herein licensed, but you may not distribute all or any portion of them.

RESTRICTIONS—You will make reasonable efforts to discontinue use of the Software licensed hereunder upon Intel's release of an update, upgrade or new version of the Software.

You shall not reverse-assemble, reverse-compile, or otherwise reverse-engineer all or any portion of the Software.

Use of the Software is also subject to the following limitations:

You,

(i) are solely responsible to your customers for any update or support obligation or other liability which may arise from the distribution of your product(s)

(ii) shall not make any statement that your product is "certified," or that its performance is guaranteed in any way by Intel

(iii) shall not use Intel's name or trademarks to market your product without written permission

(iv) shall prohibit disassembly and reverse engineering, and

(v) shall indemnify, hold harmless, and defend Intel and its suppliers from and against any claims or lawsuits, including attorney's fees, that arise or result from your distribution of any product.

OWNERSHIP OF SOFTWARE AND COPYRIGHTS—Title to all copies of the Software remains with Intel or its suppliers. The Software is copyrighted and protected by the laws of the United States and other countries, and international treaty provisions. You will not remove, alter, deface or obscure any copyright notices in the Software. Intel may make changes to the Software or to items referenced therein at any time without notice, but is not obligated to support or update the Software. Except as otherwise expressly provided, Intel grants no express or implied right under Intel patents, copyrights, trademarks, or other intellectual property rights. You may transfer the Software only if the recipient agrees to be fully bound by these terms and if you retain no copies of the Software.

LIMITED MEDIA WARRANTY—If the Software has been delivered by Intel on physical media, Intel warrants the media to be free from material physical defects for a period of ninety (90) days after delivery by Intel. If such a defect is found, return the media to Intel for replacement or alternate delivery of the Software as Intel may select.

EXCLUSION OF OTHER WARRANTIES—EXCEPT AS PROVIDED ABOVE, THE SOFTWARE IS PROVIDED "AS IS" WITHOUT ANY EXPRESS OR IMPLIED WARRANTY OF ANY KIND INCLUDING WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, OR FITNESS FOR A PARTICULAR PURPOSE. Intel or its suppliers do not warrant or assume responsibility for the accuracy or completeness of any information, text, graphics, links or other items contained in the Software.

LIMITATION OF LIABILITY—IN NO EVENT SHALL INTEL OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, LOST PROFITS, BUSINESS INTERRUPTION, OR LOST INFORMATION) ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE, EVEN IF INTEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME JURISDICTIONS PROHIBIT EXCLUSION OR LIMITATION OF LIABILITY FOR IMPLIED WARRANTIES OR CONSEQUENTIAL OR INCIDENTAL DAMAGES, SO THE ABOVE LIMITATION MAY NOT APPLY TO YOU. YOU MAY ALSO HAVE OTHER LEGAL RIGHTS THAT VARY FROM JURISDICTION TO JURISDICTION.



Contents

1	Introduction	6
1.1	About This User Guide.....	6
1.2	Terminology	6
2	Braidwood Tools	7
2.1	NANDUtil.exe.....	7
2.1.1	System Requirements	8
2.1.2	Query Command	8
2.1.3	Create Command	9
2.1.4	Destroy Command.....	11
2.1.5	Erase Command.....	12
2.1.6	Test Command	13
2.1.7	Status Command	14
2.1.8	Compliance Command	14
2.1.9	Help Command	15
2.1.10	NANDUtil Tool Usage	15

Figures

Figure 1. VECI Interface.....	7
-------------------------------	---



Revision History

Revision Number	Description	Revision Date
0.5	Initial release	March 2009
0.6	<ul style="list-style-type: none">• All sample outputs updated to NANDUtil v0.23• For 'destroy' command, added WARNING about synchronizing cache and/or backup SSD contents prior to destroying regions• For 'erase' command, added note of its destructive nature and regions are destroyed with '-total' option, also added WARNING about synchronizing cache and/or backup SSD contents prior to using 'erase' command• For 'test' command, added comment about regions are destroyed as well, also added WARNING about synchronizing cache and/or backup SSD contents prior to using 'test' command	April 2009
0.65	<ul style="list-style-type: none">• All sample outputs updated to NANDUtil v0.24	April 2009

§



1 Introduction

1.1 About This User Guide

This document is intended for Original Equipment Manufacturers (OEM), Original Design Manufacturers (ODM) and System Integrators. The document introduces and provides details on how to use the tools for Braidwood technology.

1.2 Terminology

Acronym or Term	Definition
EB	Erase Block
FW	Firmware
HDD	Hard Disk Drive
Intel® ME	Intel® Management Engine
NVMHCI	Non-Volatile Memory Host Controller Interface
PCH	Platform Controller Hub
SPI Flash	Serial Peripheral Interface Flash
VE	Virtualization Engine
VECI	Virtualization Engine Control Interface

2 Braidwood Tools

The tool(s) provided for the Braidwood technology include:

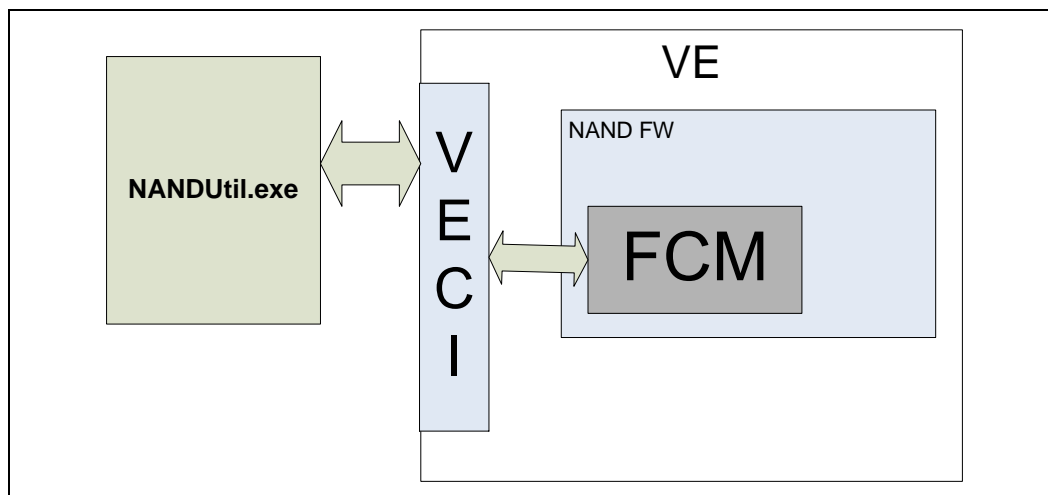
1. **NANDUtil.exe:**

- DOS based command line tool
- Provides support for following commands:
 - NAND configuration commands such as create, destroy and erase for NVMHCI (cache) and/or SSD regions
 - NAND quality check using test command
 - Compliance command to check platform, BIOS and NAND subsystem compliancy
 - Firmware status and NAND region query command

2.1 NANDUtil.exe

The NANDUtil.exe tool is a DOS based application which is used for configuring, testing and checking platform compliance of a Braidwood NAND module. It communicates with the NAND FW (running on the VE) via the VECI interface. NAND configuration is handled by the Firmware Configuration Module (FCM) in the NAND FW.

Figure 1. VECI Interface





2.1.1 System Requirements

NANDUtil.exe will run on MS DOS* version 6.22 and above.

Braidwood NAND modules are available in 3 different sizes – 4 GB, 8 GB and 16 GB. In addition, they come in two form factors - desktop version and mobile version. To use the NANDUtil tool, a NAND module must be installed on the ONFI 2.0 connector or exist based on motherboard down option.

On system power up, the Intel® ME loads the VE image from SPI Flash. It uses the soft straps which are also stored in SPI Flash to initialize and configure the VE. Therefore the soft straps must be set appropriately to select and enable the Braidwood technology (ie. NAND FW). For more information on soft straps requirements for Braidwood, please refer to the PCH_SPI_Programming_Guide document which can be found in the Intel® ME Kit on VIP.

2.1.2 Query Command

This command is used for fetching the firmware revision, details of Flash and region(s) from NAND Flash devices on the NAND module.

Note that the NAND FW may take several seconds after system power on to initialize the NAND device(s). It is recommended that users issue this “query” command first and check that it executes successfully with no error codes returned. See sample output below to determine successful output messages. After this command finishes successfully, users may then issue other NANDUtil commands.

Usage and Options:

NANDUtil.exe -query

NANDUtil.exe -query flash

NANDUtil.exe -query region ssd|nvme

Sample Output:

(successful command)

```
> NANDUtil.exe -query
NANDUtil 0.24 started.
Proceeding with query command...
  NAND firmware revision: 00.04.00.107
  SSD support: fuse - no, soft strap - no
  NVMe support: fuse - yes, soft strap - yes
  NAND Device Model: JS29H32G08FANC1
  NAND Device Manufacturer: INTEL
  Number of Logical Devices (Chip Enables): 2
  Number of Logical Units per Logical Device: 2
  Number of Erase Blocks per Logical Unit: 2048
  Number of Logical Pages per Erase Block: 128
  Logical Page size: 8192 B, Spare Bytes per Logical Page: 436 B
```




```
Sector size: 512 B
Total NAND Capacity: 1048576 Pages, User NAND Capacity: 838380 Pages
Region size: SSD - not present, NVMHCI - not present
ONFI revisions supported: 1.0 - yes, 2.0 - yes
NAND Health: read only - no, should be backed up - no
BIOS Allocated Memory: 16 MB
NAND utility execution normally terminated.
```

2.1.3 Create Command

This command creates a NVMHCI (cache) and/or SSD region(s).

Note that if a region already exists, it must first be destroyed before it can be re-created. Individual region resizing is not supported. Therefore, to change a region's size, the region must first be destroyed and then re-created with the new size. Both the SSD and NVMHC regions can be created with a single "create" command. The "-aligned" option may only be used during SSD region creation. When the "-aligned" option is used, the SSD region with logical LBA0 will be aligned to the beginning of the first physical sector of the region created. Otherwise logical LBA0 will offset from the start of the first physical sector of the SSD region by 512 bytes (1 sector), which is recommended for Microsoft OSs.

When creating a region, the NAND FW performs the following checks:

- Check the soft strap settings; NAND FW will not allow the SSD and/or NVMHCI region(s) to be created if they are not enabled via soft straps.
- Check if the requested amount of NAND is available. If the requested amount is not available, an error is returned.

Usage and Options:

NANDUtil.exe -create ssd -lpages|percents [size] {-aligned}

NANDUtil.exe -create nvmehci -lpages|percents [size]

**NANDUtil.exe -create nvmehci ssd -lpages|percents [size nvmehci]
[size ssd] {-aligned}**

NOTE: Creating both the SSD and NVMHCI regions in one single command is **not supported** in this version of the tool. As a workaround, separate create commands may be issued as shown below in the examples. Also, the system will need to be **rebooted** after a "create" command is issued. These workarounds and requirements will be fixed in subsequent releases.

For the "-lpages" option, the valid values for 'size' are from 1 to the maximum number of lpages of the NAND module. For the "-percents" option, valid values for 'size' are from 1-100. Use 100 to create only one region of maximum size. When creating both SSD and NVMHCI regions, the size parameters added up cannot be greater than 100. If they add up to less than 100, then some of the total memory space will be left unused.



Examples:

(size in lpages)

NANDUtil.exe -create nvmehci -lpages 1250

(create 90% NVMEHCI cache region)

NANDUtil.exe -create nvmehci -percents 90

(create 10% SSD region)

NANDUtil.exe -create ssd -percents 10

(size in percentage)

NANDUtil.exe -create nvmehci ssd -percents 50 50

(with -aligned option, affects only SSD region)

NANDUtil.exe -create nvmehci ssd -percents 50 50 -aligned

Sample Output:

(successful command)

```
> NANDUtil.exe -create nvmehci -percents 100

NANDUtil 0.24 started.
Proceeding with create command...
Size of NVMEHCI that shall be created: 100%
Request ok, proceeding.
Regions successfully created.
Platform reboot may be necessary.
NAND utility execution normally terminated.
```

(unsuccessful command and error messages)

```
> NANDUtil.exe -create nvmehci -percents 100

NANDUtil 0.24 started.
Proceeding with create command...
Size of NVMEHCI that shall be created: 100%
Create error: NVMEHCI region already exists, please issue 'destroy'
command
first to delete all regions and then reboot platform.
Bad request.
Invalid request error.
```



2.1.4 Destroy Command

This command destroys all SSD and/or NVMHCI region(s) on the NAND Flash.

Individual regions cannot be destroyed; this command destroys all regions present on the NAND. Once destroyed, regions must be re-created before they may be accessed and any data that was present on the region prior to its destruction will not be accessible. **WARNING: If data on NAND is important, users should synchronize the NAND cache with the HDD and/or backup SSD contents prior to destroying regions.** This command does not erase the contents of NAND.

Usage and Options:

NANDUtil.exe -destroy {-force}

NOTE: The system will need to be **rebooted** after a “destroy” command is issued. This will be fixed in subsequent releases.

Use the “-force” option to skip warning messages, this may be useful for scripting

Sample Output:

(successful command)

```
> NANDUtil.exe -destroy -force

NANDUtil 0.24 started.
Proceeding with destroy command.
Force : yes
Request ok, proceeding.
Destroy message sending ok.
Regions successfully destroyed.
Platform reboot may be necessary.
NAND utility execution normally terminated.
```

(unsuccessful command and error message)

```
> NANDUtil.exe -destroy -force

NANDUtil 0.24 started.
Proceeding with destroy command.
Force : yes
Destroy error: NVMHCI/SSD region(s) do not exist, please use 'create'
command first and then reboot platform.
No region found error.
```



2.1.5 Erase Command

This command erases all data on the NAND module.

This “erase” command is destructive which means that it will change data values on NAND. Individual regions cannot be erased; this feature physically erases all data present on the NAND module. The “-total” option erases the entire NAND Flash except for any bad erase blocks (EB). This is a lower level erase operation which clears the data structures and also destroys all cache/SSD region(s) stored on NAND. This may be needed when NANDUtil commands are always getting errors. Note that the “-total” option may not be used with the “-force” option. **WARNING: If data on NAND is important, users should synchronize the NAND cache with the HDD and/or backup SSD contents prior to using the “erase” command.**

Usage and Options:

NANDUtil.exe -erase {-force}

NANDUtil.exe -erase -total

Use the “-force” option to skip warning messages, this may be useful for scripting

Sample Output:

```
> NANDUtil.exe -erase -force

NANDUtil 0.24 started.
Proceeding with erase command.
Force : yes
Request ok, proceeding.
Erase message sending ok.
Successfully erased.
NAND utility execution normally terminated.
```

```
> NANDUtil.exe -erase -total

NANDUtil 0.24 started.
Proceeding with erase command.
Please, press 'y' to accept or 'n' to cancel.
User accepted.
Request ok, proceeding.
Erase message sending ok.
Successfully erased.
Platform reboot may be necessary.
NAND utility execution normally terminated.
```



2.1.6 Test Command

This command initiates a memory test of the NAND module.

This “test” command is destructive which means that it will change data values on NAND. In addition, this command will destroy all cache/SSD region(s) stored on NAND. This command will not cleanup (ie. erase) the data after running through the memory test operations. **WARNING: If data on NAND is important, users should synchronize the NAND cache with the HDD and/or backup SSD contents prior to using the “test” command.**

Usage and Options:

NANDUtil.exe -test [scope] {-force}

scope: percentage of NAND to test; valid values are 10, 20, 30, 50 and 100

Examples:

(test 100% of NAND memory)

NANDUtil.exe -test 100 -force

Sample Output:

```
> NANDUtil.exe -test 10 -force

NANDUtil 0.24 started.
Proceeding with test command...
  The percentage of NAND that shall be tested: 10%
  Force : yes
Test init successfully done.
  Progress: 100%
No more EBs, result:
Test statistics:
  Total number of erase blocks tested: 819
  Total ECC corrections: 0
  Total program errors: 0
  Total uncorrectable ECC errors: 0
  Total erase errors: 0
NAND utility execution normally terminated.
```

```
> NANDUtil.exe -test 100 -force

NANDUtil 0.24 started.
Proceeding with test command...
  The percentage of NAND that shall be tested: 100%
  Force : yes
Test init successfully done.
  Progress: 100%
No more EBs, result:
Test statistics:
  Total number of erase blocks tested: 8181
  Total ECC corrections: 4
  Total program errors: 0
  Total uncorrectable ECC errors: 0
  Total erase errors: 0
NAND utility execution normally terminated.
```



2.1.7 Status Command

Report the status of the NAND FW.

Usage and Options:

NANDUtil.exe -status

Sample Output:

```
> NANDUtil.exe -status

NANDUtil 0.24 started.
Proceeding with status command.
    Current status: NAND success.
NAND utility execution normally terminated.
```

2.1.8 Compliance Command

This command checks the platform to ensure it meets Ibex Peak PCH requirements and will operate with the Braidwood NAND modules.

This “compliance” test is non-destructive (ie. does not change data values on NAND) and may be run prior to NAND configuration.

Usage and Options:

NANDUtil.exe -compliance

Sample Output:

```
> NANDUtil.exe -compliance

NANDUtil 0.24 started.
Proceeding with compliance command...
    PCH vendor ID: 0x8086 (compliant) MCH vendor ID: 0x8086 (compliant)
    SATA controller device ID: 0x2822 (compliant)
    SATA controller mode: RAID mode (compliant)
    SATA chipset revision: 0x03
    VE enabled: yes (compliant)
    SSD support: fuse - no, soft strap - no
    NVMHCI support: fuse - yes, soft strap - yes
    At least one region SKU enabled. (compliant)
    NAND Device Model: JS29H32G08FANC1
    NAND Device Manufacturer: INTEL
    Number of Logical Devices (Chip Enables): 2
    Number of Logical Units per Logical Device: 2
    Number of Erase Blocks per Logical Unit: 2048
    Number of Logical Pages per Erase Block: 128
    Logical Page size: 8192 B, Spare Bytes per Logical Page: 436 B
    Sector size: 512 B
    Total NAND Capacity: 1048576 Pages, User NAND Capacity: 838380 Pages
    BIOS Allocated Memory: 16 MB
    Compliancy test passed: yes
NAND utility execution normally terminated.
```



2.1.9 Help Command

Display help information on tool usage.

Usage and Options:

NANDUtil.exe -help

Sample Output:

```
> NANDUtil.exe -help

NANDUtil 0.24 started.
nandutil -query
nandutil -query flash
nandutil -query region ssd|nvme
nandutil -create nvme -lpages|-percents [size in logical pages]
eg. nandutil -create nvme -lpages 2000 - creates nvme region of
size
2000 logical pages
nandutil -create ssd -lpages|-percents [size in logical pages] {-
aligned}
nandutil -create nvme ssd -lpages|-percents [size nvme in logical
pages]
[size ssd in logical pages] {-aligned}
eg. nandutil -create nvme ssd -percents 40 60 -aligned - creates
NVMHCI
region of size 40% of total user memory and SSD region of size 60% of
total user memory
nandutil -destroy {-force}
nandutil -erase {-force}
nandutil -erase -total
nandutil -test [scope of test 10,20,30,50,100] {-force}
eg. nandutil -test 50 -force - tests flash using 50% of logical
pages
without user confirmation
nandutil -status
nandutil -compliance
nandutil -help
NAND utility execution normally terminated.
```

2.1.10 NANDUtil Tool Usage

A NAND Flash module must be configured before it can be used by the host. Configuration of the NAND module involves creation of NVMHCI (ie. cache) and/or SSD region(s). NANDUtil tool can be used to configure the NAND Flash module.

Use the following procedures to create a NVMHCI and/or SSD region:

1. Copy NANDUtil.exe from "\Tools\Braidwood Tools\" folder to the root directory of a bootable USB drive.
2. Boot the target system to DOS, change directory to the root directory of the bootable USB drive. Note that NANDUtil will run on MS DOS version 6.22 and above.



3. Braidwood NAND FW may take several seconds after system power on to initialize the NAND module. It is recommended to use the "query" command first and check that it executes successfully with no error codes returned. This command is used for fetching the details of NAND Flash/region from NAND FW. Type the following command at DOS prompt:

```
> NANDUtil.exe -query
```

In case of an error, perform the whole NAND Flash erase using the following command, then power off the target system after successful completion of erase command and go to step 2:

```
> NANDUtil.exe -erase -total
```

If "erase" command fails then perform complete NAND Flash memory test using the following command at DOS prompt, then power off the target system after successful completion of test command and go to step 2:

```
> NANDUtil.exe -test 100
```

If "test" command fails or repeated failures occur with query command then please power off the target system, replace the NAND Flash module and go to step 2.

4. Use the "create" command to create NVMHCI and/or SSD region(s). For example, to create a 100% NVMCHI region on the NAND module, type the following command at the DOS prompt:

```
> NANDUtil.exe -create nvnhci -percents 100
```

Note: If region(s) already exist on the NAND Flash module and you wish to re-create the region(s) then you will need to destroy the region(s) first using the following command at the DOS prompt, then power off the target system after completion of "destroy" command and go to step 2:

```
> NANDUtil.exe -destroy
```

5. Power off the target system.
6. Boot the target system to DOS, change directory to the root directory of the bootable USB drive.
7. Use the "query" command to confirm the NVMHCI/SSD region(s) have been setup correctly:

```
> NANDUtil.exe -query
```

For 100% NVMHCI (ie. cache) region on an 8 GB NAND module, the "query" command's output will show a line similar to,

Region size: SSD - not present, NVMHCI - 838383 1. pages