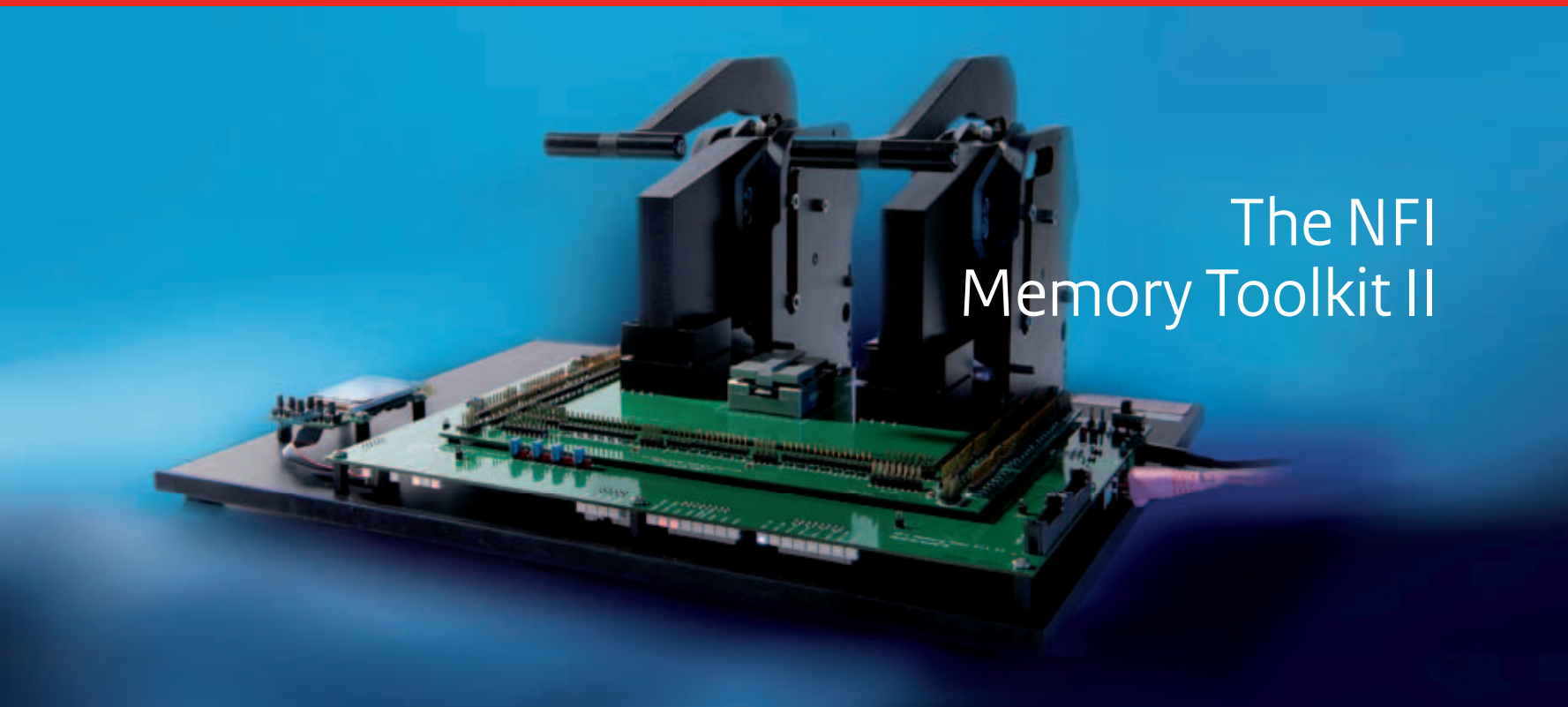
Netherlands Forensic Institute
Ministry of Security and Justice

A universal forensic solution to read memory chips developed by the **Netherlands Forensic Institute**



The NFI Memory Toolkit II

The NFI Memory Toolkit II

The NFI Memory Toolkit II is a universal forensic solution to read memory chips that store user data in devices such as mobile phones, satellite navigation devices, car electronics and USB flash drives. With the Memory Toolkit, erased data such as text messages, phone numbers, pictures and browser history may potentially be recovered. It can also be used to recover data from damaged or password-protected devices.

Reading memory chips

The NFI Memory Toolkit II can extract all data from a memory chip (1-on-1 copy), including information from spare area, bad blocks et cetera. The toolkit is intended for memory chips which are desoldered from the target device. Its exact possibilities depend on the target device's type, version and manufacturer.

The system can handle various types of chip families, for example:

- Micro BGA (Ball Grid Array) without the replacement of BGA balls (reballing),
- Thin Small-Outline Packages (TSOP),
- Small-Outline Integrated Circuit (SOIC),
- Nor, Nand, I2C, OneNand et cetera.

Reading desoldered memory chips has the advantage over other acquisition methods that no data is changed and even memory chips from non-functional target devices (for instance those damaged by heat, water or force) can be read, if the memory chip itself is still intact. Memory chips from password-protected devices can also be read.

The toolkit is a combination of hardware and software. The hardware makes a physical connection, generates signals and supplies power to a memory chip. The software takes care of the command sets to access data in the various types of memory chips.

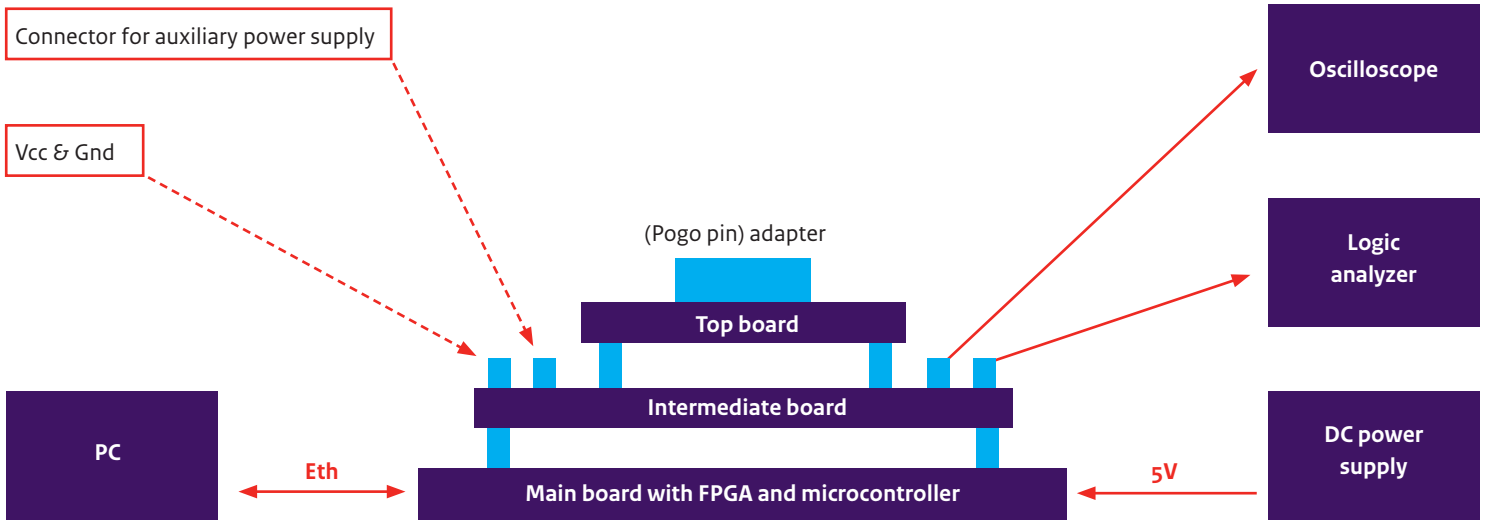


Figure 1: Schematic of the NFI Memory Toolkit II

Hardware

A hardware schematic is drawn in Figure 1. The system has three layers of printed circuit boards: a top board, intermediate board and main board. The top and intermediate board can be swapped by the user to configure the system for different types of memory chip packages. The main board is fixed and has the main hardware components like a Field Programmable Gate Array (FPGA), microcontroller and programmable power supply.

A DC power supply and a PC are necessary for system operation (not included). A logic analyzer and an oscilloscope are recommended for debugging purposes (not included). The electrical connection between the three boards is made with connector arrays and two mechanical pressure units. Figure 2 shows a picture of the complete system including the two mechanical pressure units.

Top boards

A desoldered memory chip is placed in an adapter which is mounted on a top board. The user can choose between five top boards (future expandable) with different types of adapters depending on memory chip package and pitch. Pogo pin adapters are used for micro BGA packages. These pogo pin adapters contain an array of small contacts in the same pitch as a memory chip package, to make an electrical contact.

Differences in height of the desoldered micro BGA balls are compensated with small springs in the contacts. The pogo pin adapters eliminate the need for reballing. A locator is used to place and hold a memory chip precisely located on the pogo pin array. The locator is a small plastic plate made from polyetheretherketone or 'peek' material, a high performance engineering thermo-plastic. Different locators can be milled for different package dimensions.

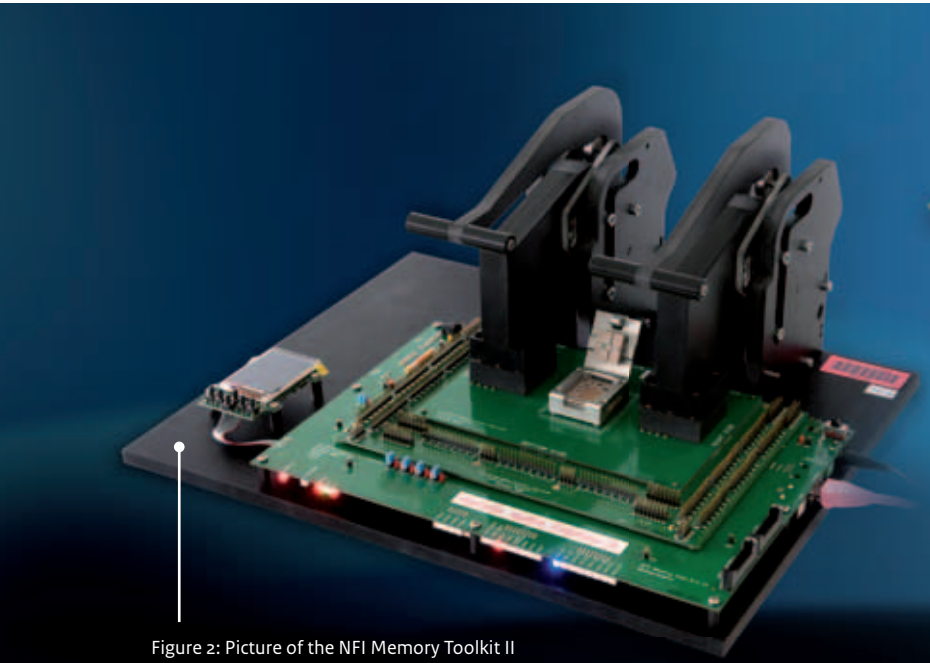


Figure 2: Picture of the NFI Memory Toolkit II

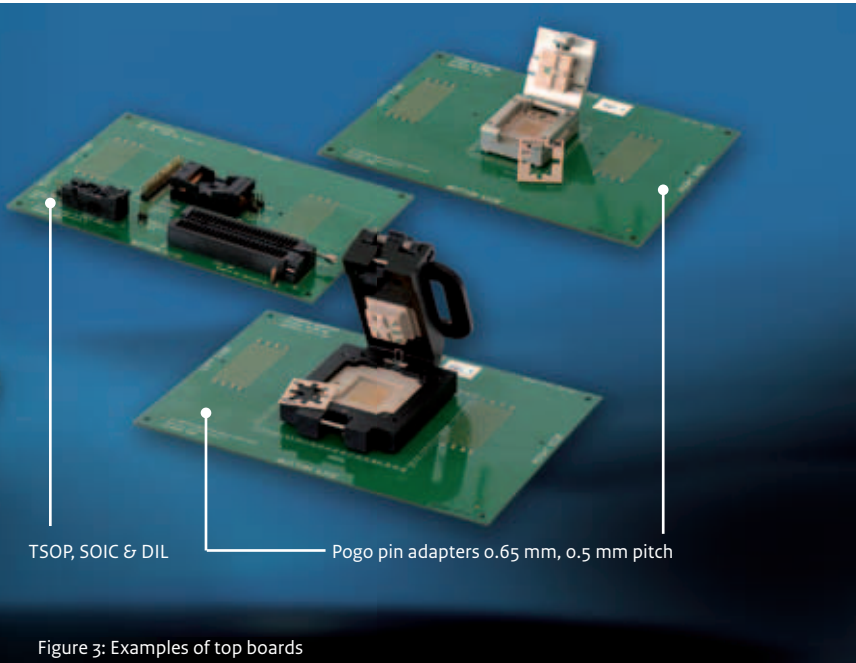


Figure 3: Examples of top boards

Currently available top boards:

- Top board for pogo pin adapter with 0.5 mm pitch (array of 15x15 pins)
- Top board for pogo pin adapter with 0.65 mm pitch (array of 24x24 pins)
- Top board for pogo pin adapter with 0.75 mm pitch (array of 15x15 pins)
- Top board for pogo pin adapter with 0.8 mm pitch (array of 15x15 pins)
- Top board with TSOP, SOIC and DIL zero insertion force adapters

Intermediate boards

An intermediate board selects a subset of pins when the pogo pin array is too large for the main board. The intermediate board also brings all signals to a connector for measuring purposes (with an oscilloscope for example) or for supplying extra power to a memory chip.

Currently available intermediate boards (future expandable):

- Board for an array of 15x15 pins
- Board selecting an inner block of 19x19 out of an array of 24x24 pins
- Board selecting an outer ring of 7 rows out of an array of 24x24 pins

Main board

The main board contains the key components of the system:

- FPGA with 384 user-programmable IO (input-output) pins. These IO pins are connected to the pogo pin array via the intermediate board. Because the IO pins are programmable, the system can easily be adapted for each memory chip signal layout. The FPGA is also used to execute a continuity test to detect if all pogo pins are connected to a memory chip.
- Microcontroller to control the power supply, power supply monitor, status LEDs and to communicate over Ethernet (100Mbit/sec) with a host PC.
- System power supply with over and reverse input protection.
- Two user-programmable power supplies for supplying power to a memory chip (can be programmed between 1.2 and 3.3 Volt).
- Power supply monitor for monitoring voltage level and current consumption (not yet supported by the software).
- Universal connectors for a logic analyzer.

Software

The software consists of:

- FPGA configurations
- Embedded software running on the microcontroller
- Host PC software

FPGA configurations are written in Very High Speed Integrated Circuit Hardware Description Language (VHDL). Different configurations are available for hardware protocols and can be expanded in the future for other protocols. The microcontroller is running uClinux, a version of Linux designed for microcontrollers. Communication software communicates with the FPGA. Written in C++, it is using a Linux TCP/IP stack for host PC communication and programs the power supply and power supply monitor, and status LEDs. A command-line program running on a host PC generates the command sets to access data in different types of memory chips. Each command set is implemented in a separate C++ class and can also be expanded in the future when new protocols are implemented.

Currently supported flash families:

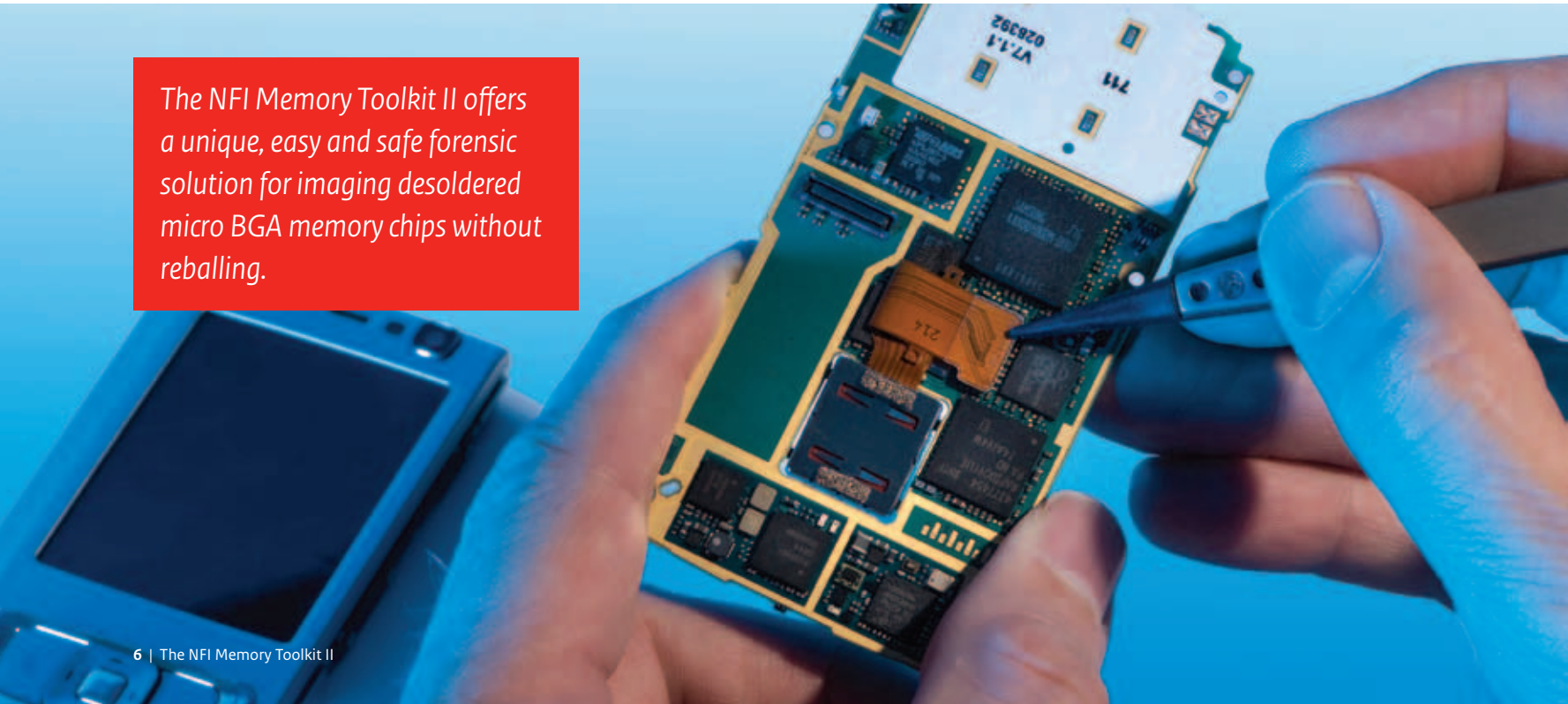
- NorFlash
- NandFlash
- OneNand
- DiskOnChip (not all types)
- I2C and SPI EEPROM (work currently in progress)
- MoviNand

A graphical user interface (GUI), written in C++ and Qt, is used to configure FPGA IO pins for memory chip signal layouts. This GUI also calls the previously mentioned command-line program for reading a memory chip and storing data in a file. All settings to access a memory chip are stored in an XML file. This file contains information such as signal layout, memory type, power supply, size. This file is user-editable.

Figure 4 shows a screenshot of primary memory chip properties.
Figure 5 shows a screenshot while editing a memory chip signal layout.
Figure 6 shows a screenshot of a continuity test. This test can be executed to detect if all pogo pins are connected to a memory chip.
When the continuity test is passed, a memory chip can be read, this is shown in Figure 7.

A hash sum is calculated over the data during a read cycle and stored in a separate log file. This log file also contains all meta-information read from the memory chip, software version numbers et cetera. All host PC software is platform-independent (tested on Ubuntu Linux 9.04 and 10.04 LTS and Microsoft Windows XP SP3).

The NFI Memory Toolkit II offers a unique, easy and safe forensic solution for imaging desoldered micro BGA memory chips without reballing.



Screenshots

Figure 4: Screenshot of primary memory chip properties

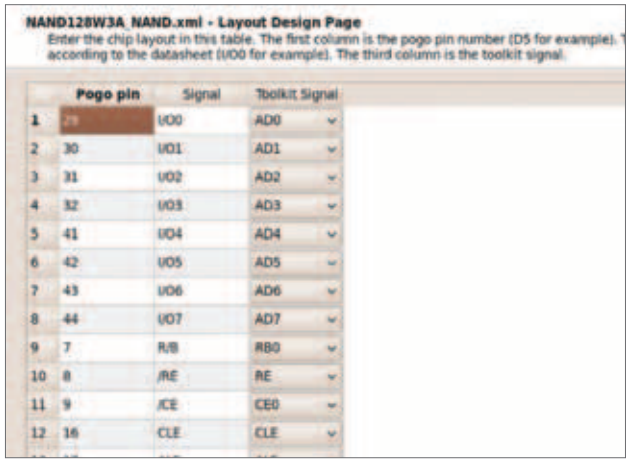


Figure 5: Screenshot while editing a memory chip signal layout

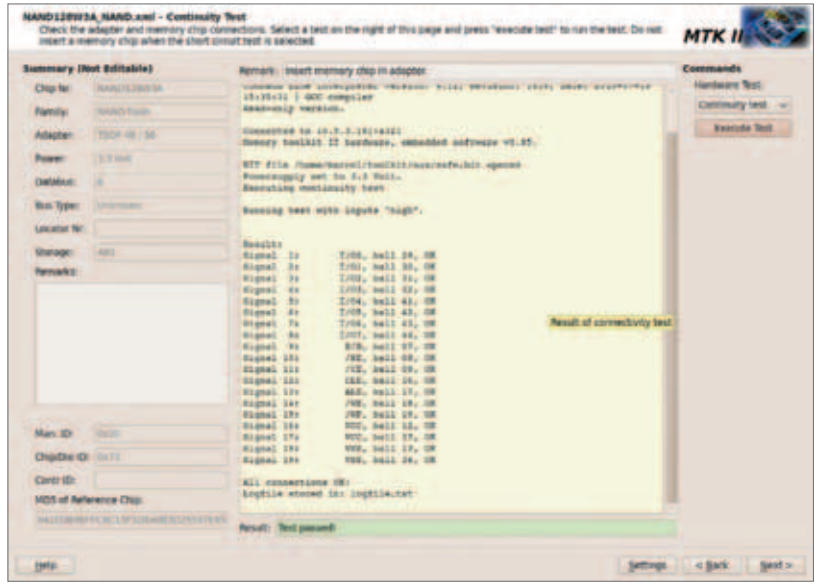


Figure 6: Screenshot of a continuity test

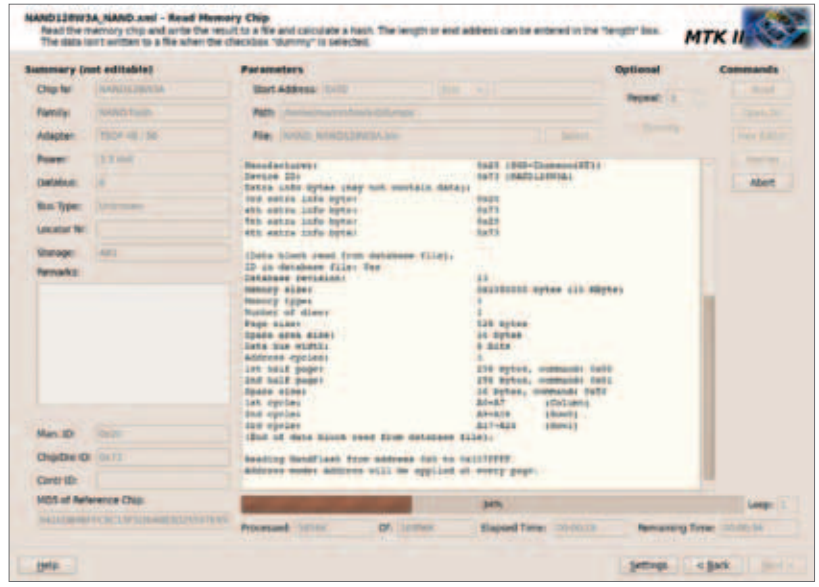


Figure 7: Screenshot while reading a memory chip

Additional information

- To be able to use a NFI Memory Toolkit II a user must also have (access to):
  - A rework station with a collection of nozzles for desoldering micro BGA chips
  - An electronic temperature-controlled miniature soldering iron with multiple fine pitch tips
  - Tools for desoldering TSOP, SOIC chips et cetera (for example a Digital Programmable Hot Air Reflow System)
  - An inspection microscope
  - Cleaning tools
  - Flux remover
  - An ESD-safe working place
  - A precision milling machine to make locators
  - A DC power supply (5 to 6 Volt, 1 Amp) and a PC are necessary for system operation
  - A logic analyzer (at least 100M samples/sec, 2M samples wide, 64 channels) and a Digital Storage Oscilloscope (at least 1GHz bandwidth 4GS/s, 2-4 channels)*
  - Storage equipment for a reference collection, printed circuit boards, locators et cetera

- It is also recommended to collect reference target devices and reference memory chips.

* *recommended for debugging purposes*

- Some memory technologies might not be supported due to the universal concept of the toolkit (for example, strong peak currents can cause problems due to the relatively long wires to the adapters).

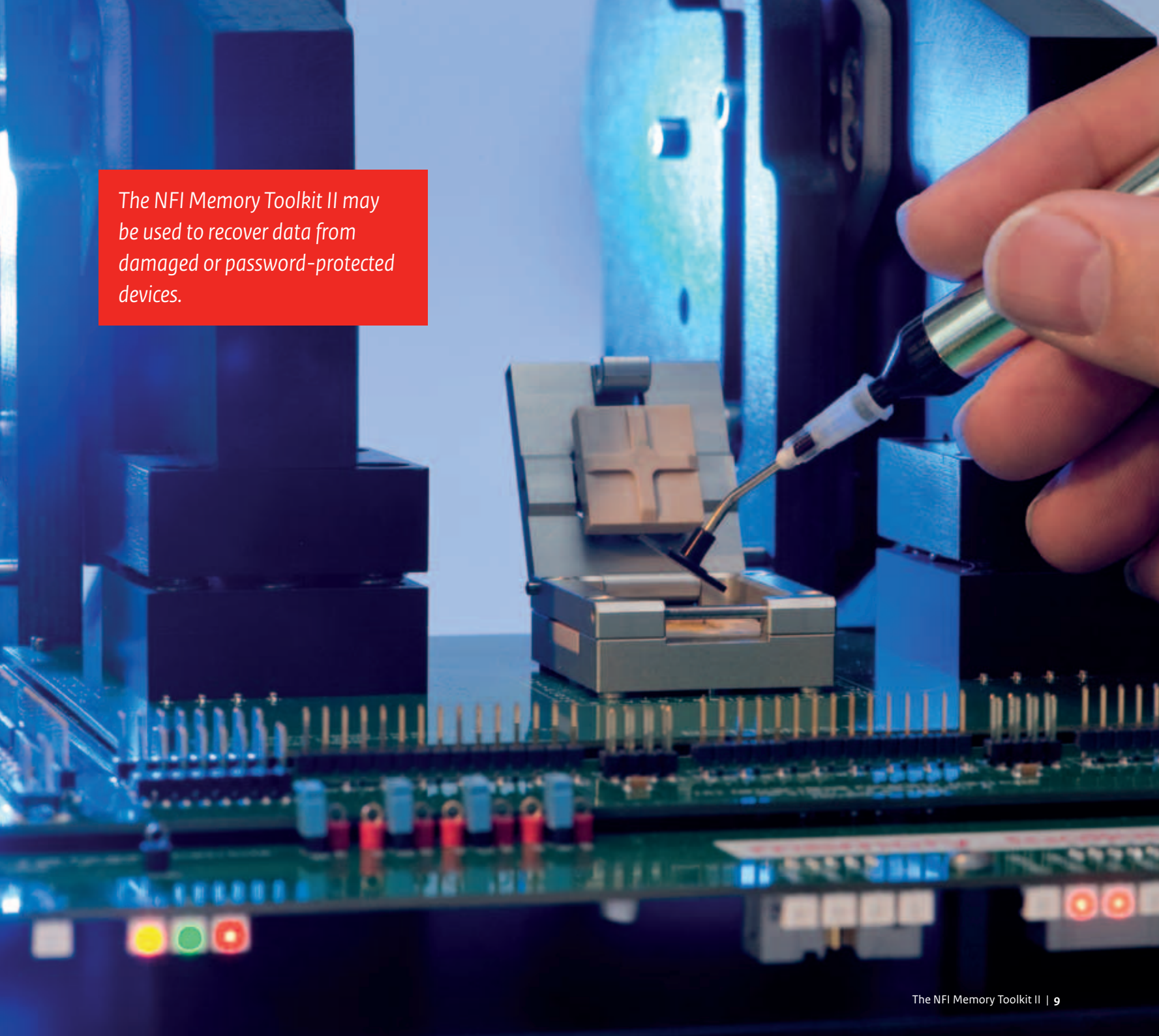
- The user must gain experience in removing micro BGA chips from target devices. Desoldering memory chips from target devices is a critical step in the process. Especially underfilled micro BGA chips are more difficult to remove (underfilling is a method used to glue a chip to the printed circuit board to improve mechanical reliability). Inexperienced operators may damage the chip beyond repair.

- Removed micro BGA chips can not easily be mounted back on the target device.

- Chips added by the NFI are available as free updates. It is also possible to request support for specific memory chips for a fee.

- The user can also create new configuration XML files. For that the user will need to have access to the data sheets of the memory chips and it is necessary to understand the communication signals for these memory chips (like NandFlash, NorFlash et cetera).

- A toolkit operator needs to have professional electronics skills.



The NFI Memory Toolkit II may be used to recover data from damaged or password-protected devices.

NFI Memory Toolkit II part list

Hardware

- ☐ 1 Base board with mechanical pressure units
- ☐ 1 NFI Memory Toolkit II main board
- ☐ 1 Intermediate board for 15x15 adapter
- ☐ 1 Intermediate board for 19x19 adapter
- ☐ 1 Intermediate board for 24x24 adapter
- ☐ 1 Top board for 15x15 adapter 0.5 mm pitch
- ☐ 1 Top board for 15x15 adapter 0.75 mm pitch
- ☐ 1 Top board for 15x15 adapter 0.8 mm pitch
- ☐ 1 Top board for 24x24 adapter 0.65 mm pitch
- ☐ 1 Top board with TSOP, SOIC and DIL sockets
- ☐ 4 Samtec board-to-board connectors and 2 spare connectors
- ☐ Connector cleaning tissues
- ☐ 1 Reference memory chip
- ☐ 1 Reference locator
- ☐ 10 Spare locators (for milling new locators)
- ☐ 1 Adapter for connector continuity test

PC software

Optional

- ☐ 1 Pogo pin adapter 15x15 0.5 mm pitch
- ☐ 1 Pogo pin adapter 15x15 0.75 mm pitch
- ☐ 1 Pogo pin adapter 15x15 0.8 mm pitch
- ☐ 1 Pogo pin adapter 24x24 0.65 mm pitch with stiffener

For shipping

- ☐ Peli transport case

The NFI Memory Toolkit II is exclusively available at the Netherlands Forensic Institute.

Information and availability

The NFI Memory Toolkit II is available from the Netherlands Forensic Institute exclusively. For more information about the toolkit, prices and the terms and conditions of sale, please contact:

NFI Front Office
Account Management, Marketing & Sales
Email accountmanagement@nfi.minjus.nl
Phone +31 70 888 66 40

The NFI Memory Toolkit II

A universal forensic solution to read memory chips developed by the **Netherlands Forensic Institute**

Netherlands Forensic Institute
Ministry of Security and Justice

PO Box 24044 | 2490 AA The Hague
The Netherlands

www.forensicinstitute.nl

May 2011