



# ruSolut VNR Chip-Off Data Recovery Forensics

ruSolut's Visual NAND Reconstructor (VNR) Chip-Off Data Recovery Forensics training teaches students how to access data from broken or damaged flash storage devices. In this course you will learn how to perform chip-off data recovery using digital forensics methodologies used in cases when data access through the standard interface is not possible. Students will learn how to access data on USB, SD, Smartphones and NAND devices. This course will use, and cover tools in the *H-11 and ruSolut Standard, Professional, and/or Ultimate Chip-Off Lab Kits*.

## DAY 1

### Module 1: FLASH MEMORY USAGE OVERVIEW

- Overview
- Diversity of devices
- Structure, components and functionality
- Standard and monolithic devices
- Controller and Flash memory functions
- Pros and cons of flash memory
- Data recovery workflow
- *LAB: Overview of different flash storage devices and flash memory localization*

### Module 2: NAND FLASH MEMORY

- Raw NAND vs managed NAND
- Flash memory chip types
- Flash memory packages
- *LAB: Overview of flash memory packages*
- NAND interface
- Internal structure
- Crystals, Planes, Blocks, Pages
- Data allocation within memory
- Multi/Single page allocation
- NAND parameters
- Direct memory access mode
- Bit errors in NAND memory
- Voltage tuning for better reading
- Physical image extraction
- *LAB: Direct access to NAND and Physical image extraction to file*

### Module 3: PHYSICAL IMAGE OF NAND MEMORY

- Internal structure
- Blocks, Pages, Data, Spare and ECC areas
- Page layout
- Spare area structure



## DAY 2

### Module 4: FLASH CONTROLLERS

- Data flow from input to NAND
- Reverse operations
- Error Correction Codes
- Data optimization in channel
- Page allocation
- Block management, wear leveling and translation (FTL)
- *LAB: ECC detection on 2-3 cases*

### Module 5: VISUAL NAND RECONSTRUCTOR

- Software overview
- Databases, settings and components
- Workspace overview
- Elements, Parameters, Toolbars and functions
- Dump viewers
- Hex, Bitmap, Structure viewers
- Bitmap concept
- Work in Bitmap and Structure viewer
- *LAB: Page structure analysis on 2-4 dumps*

### Module 6: PHYSICAL IMAGE ANALYSIS BASED ON PATTERNS

- Page layout analysis
- Data, Spare and ECC area patterns
- Inverted data patterns
- *LAB: Analysis of inversion on 1-2 cases*
- Scrambled/Non-scrambled data patterns
- *LAB: Analysis of scrambler and XOR key on 2-3 cases*
- Page allocation patterns
- *LAB: Page allocation analysis on 2-3 cases*

### Module 7: BLOCK TRANSLATION ALGORITHM

- Concept of block management and translation
- Block size determination
- Spare area pattern analysis
- Logical Block Number parameters
- Header parameters
- Translator creation in software
- Missing and duplicated blocks
- Data cache
- Logical image creation
- *LAB: Logical image reconstruction on 1-3 cases*

## DAY 3

### Module 8: LOGICAL IMAGE RECONSTRUCTION PROCESS

- Three phases of the data recovery process
- Physical images
- Virtual images
- Logical image
- Translator adjustment
- Analysis of conflicts within block sequence
- *LAB: Complete data recovery process*

### Module 9: PRACTICAL DATA RECOVERY ON DUMPS

- LAB: Low complexity 2-3 cases
- LAB: Medium complexity 2-3 cases
- LAB: High complexity 1-2 cases

## DAY 4

### Module 10: REVERSE ENGINEERING OF UNSUPPORTED DEVICES. ECC CODES

- ECC (BCH) code analysis and reverse engineering
- Code structure
- Codewords, Payload, Parity
- Polynomials, tweaks
- BCH brute force
- *LAB: Reverse engineering of ECC code on 2-3 dumps*

### Module 11: REVERSE ENGINEERING OF UNSUPPORTED DEVICES. SCRAMBLING (XOR) KEYS

- XOR key patterns
- Search of XOR key
- XOR key extraction
- XOR key cleaning
- XOR key check and application
- *LAB: XOR key extraction from dump on 1-2 cases*

## DAY 4 – continued

### Module 12: REVERSE ENGINEERING OF UNSUPPORTED DEVICES. NAND MEMORY CONFIG ANALYSIS

- NAND protocol parameters
- Physical parameters: crystals, planes, blocks, pages
- Async vs WL protocols
- Reverse engineering of all parameters
- Configuration test
- *LAB: NAND memory config analysis on 1 case*

## DAY 5

### Module 13: PRACTICE ON NON-STANDARD AND COMPLICATED CASES

- Bad columns
- Analysis and removal
- *LAB: Data recovery with bad columns on 1 case*
- Multiple chips
- *LAB: Data recovery from multiple dumps on 1-2 cases*

### Module 14: EMMC CHIPS

- Overview
- eMMC application in multimedia devices
- Logical image extraction
- Smartphones, tablets
- Operating systems, file systems
- Data categories
- VNR capabilities
- Android data extractor
- Data extraction vs Data carving
- Carvers for deleted data recovery
- *LAB: Data carving from Android dump*

### Module 15: EMMC CHIPS. NAND ACCESS

- New technology overview
- eMMC-NAND access for un-erased data extraction
- eMMC-NAND access on faulty chip
- *LAB: Data recovery from eMMC-NAND dump*

