

Product Scope and Categorisation

Record for CRA

Document No. : CRA- CLASS- 001
Version : V1.0
Date of Compilation : 24 August 2026
Prepared by : Jin Cancan
Reviewed by : Zhou Yang
Applicable Product : Nand Flash Tracer (NFT)

1. Basic Product Information

Item	Content
Product Name	Nand Flash Tracer (abbreviation: NFT)
Product Type	Pure software (data- recovery and data- reorganisation software)
Current Version	Ver 2.26.0617 (and all subsequent versions)
Official Website	https://www.flash-tracer.com/
Manufacturer	Dalian ByteSmart Technology Co.,Ltd.
Manufacturer Address	No.32,1st Floor, No.555 Huanghe Road, Shahekou District, Dalian City, Liaoning Province, China.
Contact Information	Tel: +86 15524692190 Email: nandflashttracer@gmail.com

1.1 Economic Operator Role Confirmation

Item	Content
Role Confirmation	This company acts as the Manufacturer of this product and assumes all core manufacturer- obligations under

Item	Content
	the CRA.
Manufacturer Registered Location	Dalian City, Liaoning Province, China.
Authorised Representative	[To-be-filled: Full legal entity name & full EU physical address; Mandate reference: Doc-AR-001, mandate stored as separate archived document]

1.2 Product Boundary Statement

This assessment covers ****only the locally-installed software body of Nand Flash Tracer****. It excludes third-party hardware reading devices used by end- users, third-party storage media, and contents displayed on the official website.

If cloud-based services or additional online functions are added in future product releases, product boundary re-assessment shall be performed.

2. Product Functional Description

2.1 Core Functions

NFT is a professional software tool focused on data-recovery for memory-chip devices. Its core capabilities include:

- Parse raw NAND- Flash dump images obtained from chip read-out, perform virtual-page re-assembly and data reconstruction to realise data- recovery for storage media.
- Process chip-dump data originating from NAND-Flash-based storage devices including USB-drives, SD-cards, TF-cards, eMMC and consumer-grade SSDs.
- Provide bad-block identification, filtering and correction; compatible with SLC / MLC / TLC / QLC NAND flash memory particles.
- Support XOR- key detection, data-offset calibration and Read-Retry; handle complex fault scenarios including encrypted data, out-of-order pages, weak-blocks and incomplete dump images.
- Provide ECC error-correction verification and batch ECC processing; parse ECC status within raw dump images to assist media- fault diagnosis.
- Offer pre-processing utilities including sector cutting, bad-byte trimming and

formula-based conversion for business-oriented processing of dump-image data.

- Be compatible with third-party flash-reading hardware; able to import dump-images generated by external hardware tools for subsequent recovery workflows.
- Implement device-binding licence validation for software permission management.

2.2 Key Features

- Preview ECC error status and perform batch ECC processing; visualise ECC-error distribution within raw dump-images.
- Automatic and manual bad-byte trimming modes; processing results can be validated against ECC-check outcomes.
- Formula-driven conversion within the sector-cutting module to adapt to page-layout differences across controller types.
- Optimised processing for weak-blocks, corrupted and incomplete dump-images to improve recovery success-rate for faulty media.
- Automatic identification and handling of out-of-order and XOR-scrambled pages generated by mainstream flash-controllers.
- Device-binding licence validation to control software permission scope.

2.3 Intended Purpose

Deliver NAND-Flash chip data-recovery solutions for professional data-recovery laboratories and technical specialists.

2.4 Target Users

- Professional data-recovery laboratories
- Data-recovery technical specialists
- Digital-forensics organisations

2.5 Operating Environment

Item	Content
Operating System	Windows 7 / 10 / 11
Deployment Model	Local standalone installation
Data Handling	Does not store personal or sensitive

Item	Content
	user-recovered data
Network Usage	Licence activation only
Third-party Dependencies	No third-party dependencies

3. CRA Jurisdiction- Scope Confirmation

3.1 Confirmation Conclusion

NFT software qualifies as a product with digital elements falling within scope of EU Cyber Resilience Act (CRA), Regulation (EU) 2024/2847.

3.2 Justification

- NFT is a standalone software product implemented via digital code.
 - Its core business is processing digital data originating from storage chips (data-recovery and data-reorganisation).
 - The product will be made available on the EU market.
- Reference: Regulation (EU) 2024/2847 Article 2(1).

3.3 Jurisdiction- Scope Check- List

Check Item	Yes / No	Legal Reference
Does the product contain digital elements?	Yes	CRA Article 2(1)
Will the product be placed / made available on the EU market?	Yes	CRA Article 2(1)
Does the product fall within statutory exclusion categories?	No	CRA Article 3 (see Section 3.4 for full comparison)

3.4 Full Comparison against CRA Article 3

Exclusion- Criteria

This product does not satisfy any Article 3 exclusion condition:

Exclusion Scenario	Applicable?	Remarks
Medical devices and in-vitro diagnostic products	No	This is data-recovery software, outside medical-device scope
Motor vehicles and components	No	Not applicable
Civil-aviation products	No	Not applicable
Products covered by separate EU cybersecurity- specific legislation	No	No other dedicated EU sector- legislation applies
Products intended exclusively for research- and- development purposes	No	Commercial product for market release, not limited to R&D only
Bespoke products manufactured for a single end- user	No	Standard off-the- shelf software for multiple end- users
Second- hand products or spare replacement- parts	No	New original software product
Non- commercial open- source software	No	Commercially- distributed software; this exclusion does not apply

Jurisdiction conclusion: This product falls within CRA scope.

4. Product Categorisation Confirmation

4.1 Confirmation Conclusion

Based on NFT's core- functionality, it is categorised as a ****Default / Standard product****.

4.2 Categorisation Legal Basis

Per CRA Articles 6- 8, categorisation is determined by product core- functionality and risk profile:

- ****Critical products****: listed in Annex IV, including Hardware Security Modules (HSM), Secure Elements (SE), smart- cards, etc.
- ****Important products****: listed in Annex III, subdivided into Class I and Class II; including identity- management systems, password- managers, anti- malware, VPN- products, network- management- systems, virtual- machine monitors, firewalls, operating- systems, etc.
- ****Default / Standard products****: all other products- with- digital- elements not listed in Annex III or Annex IV.

4.3 Categorisation Comparison Table

Product Category	Outcome	Remarks
Critical product (Annex IV)	No	Does not implement core-functions of Annex IV items (HSM, SE, smart-cards etc.)
Important product Class II (Annex III)	No	Does not implement Class II functions (virtual-machine monitors, firewalls, operating-systems etc.)
Important product Class I (Annex III)	No	Does not implement Class I functions (identity-management, password-managers, anti-malware, VPN, network-management-systems etc.)
Default / Standard product	Yes	Product-with-digital-elements not listed within Annex III or Annex IV

4.4 Categorisation Argumentation

Full review against Annex III and Annex IV:

- Annex III (Important Products) covers operating- systems, network- security- products, industrial- automation- software, identity- authentication- software and network- equipment. NFT is a

local- running data- recovery utility and does not implement core- functions of those categories.

- Annex IV (Critical Products) governs high- security hardware- /software components relied- upon by critical- infrastructure (HSM, smart- cards etc.). NFT does not operate within those scenarios.

Therefore the product is classified as a **Default / Standard product**.

4.5 Conformity- Assessment Route

Given the Default- product classification, **Module A (Internal Production Control)** self- assessment procedure applies.

As manufacturer, we shall perform self- assessment against CRA requirements based on the complete technical documentation and issue the EU Declaration of Conformity (DoC). No Notified- Body third- party intervention is required.

5. Support- Period Information

Per CRA Article 13(8), manufacturers shall define a support- period of minimum five years.

Item	Content
Support-Period Start Date	10 February 2024 (date of first placing-on-the-market within the EU; sales-order / transactional evidence archived within technical-documentation package)
Support-Period End Date	10 February 2029
Support-Period Rationale	This is a professional flash-chip data-recovery tool. The support-period is defined with reference to expected service-life of comparable software-tools, flash-chip hardware-iteration cadence and reasonable end-user expectations; minimum 5-year support-period is guaranteed.

Reference: Regulation (EU) 2024/2847 Article 13(8).

Note: The support- period commences from the date the product is **first placed- on- the- market within the EU**, not from domestic- release or development- completion date.

6. Applicable Standards & Approaches

As of August 2026, no harmonised standards under the CRA have been published within the Official Journal of the European Union.

The relevant CRA harmonised- standard series is ****EN 40000****.
(EN 18031 series relates to the older RED directive and is irrelevant to CRA).

Standard / Specification	Status	Remarks
EN 40000-series (CRA harmonised standards)	Draft status	Not yet published in Official Journal of EU
Oter harmonised standards	To-be-identified	Will be updated upon official EU publication

7. Technical- Document Retention Rules

Item	Content
Technical-documentation retention period	Minimum 10 years from the date of last placing-on-the-market within the EU
EU Declaration-of-Conformity (DoC) retention period	Minimum 10 years from the date of last placing-on-the-market within the EU
Retention-period rule	If the product support-period exceeds 10 years, documents shall be retained until end-of-support
Legal Reference	Regulation (EU) 2024/2847

8. Re- assessment Requirement for Substantial Modifications

Per CRA Article 3(30): A ****substantial modification**** means any change after placing- on- the- market that affects compliance with Part I essential cybersecurity- requirements of Annex I or alters the product’s intended purpose.

This categorisation conclusion applies only to the current product- version.

If future product changes constitute substantial- modifications as defined above, full scope- and- categorisation re- assessment shall be triggered.

> Illustrative internal guidance (non- binding legal judgement):

> - Examples of potential substantial- modification: adding cloud service modules, built- in identity- authentication capabilities, VPN / encryption- gateway core- components; or changes altering intended- purpose or materially modifying security- risk- profile.

> - Examples not constituting substantial- modification: pure security- vulnerability fixes, performance- optimisation, UI adjustments.

> Note: These examples serve internal reference only. Final judgement shall be based on material impact on product security- risks and intended- purpose.

> Additional transition- clause remark for this product:

> This assessment document covers Nand Flash Tracer Ver 2.26.0617 and subsequent new- releases. Historical product- versions were first placed- on- the- market in the EU on 10 February 2024. Pursuant to CRA Article 69 transition- provisions, legacy versions placed- on- the- market before 11 December 2027 without substantial- modification benefit from transitional- rules. **Article 14 vulnerability- and- incident- reporting obligations apply to all released product- versions effective 11 September 2026**.

9. Conclusion

Following above assessment:

1. NFT software is within CRA scope as a **product with digital elements**.
2. NFT is classified as a **Default / Standard product**, with Module A self- assessment conformity- route applicable.
3. Subsequent compliance activities shall follow Default- product obligations: compile full Annex VII technical- documentation package, complete manufacturer self- assessment and issue the EU Declaration of Conformity (DoC).

10. Sign- off Record

Role	Name	Signature	Date
Prepared by	Jin Cancan		27 August 2026
Reviewed by	Zhou Yang		27 August 2026
Approved by	Zhou Yang		27 August 2026