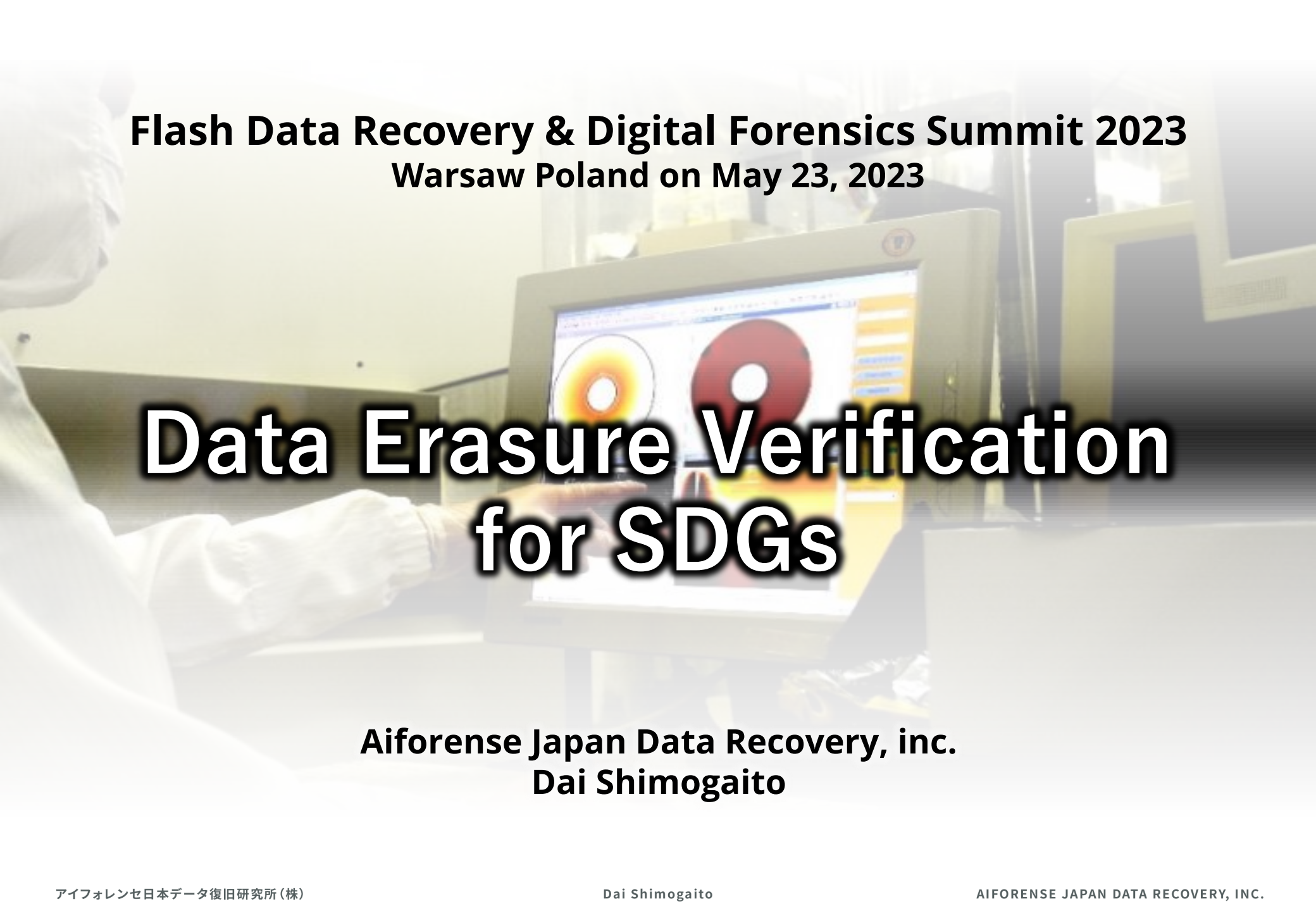


Flash Data Recovery & Digital Forensics Summit 2023
Warsaw Poland on May 23, 2023

Data Erasure Verification for SDGs

Aiforense Japan Data Recovery, inc.
Dai Shimogaito

Speaker : Dai Shimogaito

Aiforense Japan Data Recovery, inc. Founder CEO

- Established : 1998
- Locations : Osaka, Japan & New York, U.S.A.

- **Patent**

  New firmware of HDDs for controlling allocation of data (Patent #6398023)

- **Award**

  "Research & Development Award" by Institute of Digital Forensics (2018)

  - The most authoritative award for DF technology in Japan. Only one in every 5 years.

- **Research Presentations at International Conferences**

  - **High Technology Crime Investigation Association International Conference** (USA, 2016)

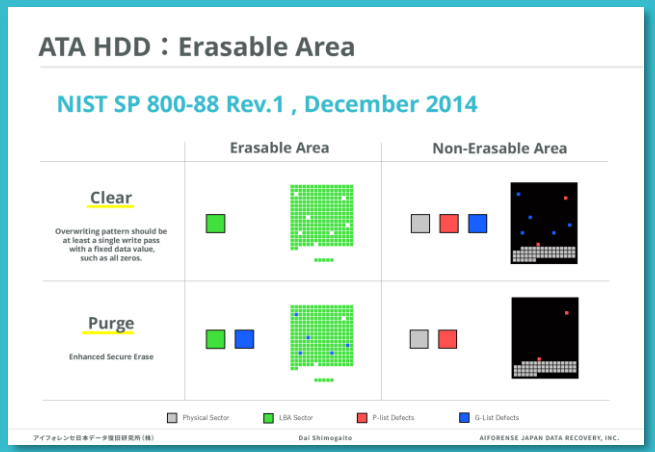
    - The oldest and the most respected high-technology investigation conferences in the world.

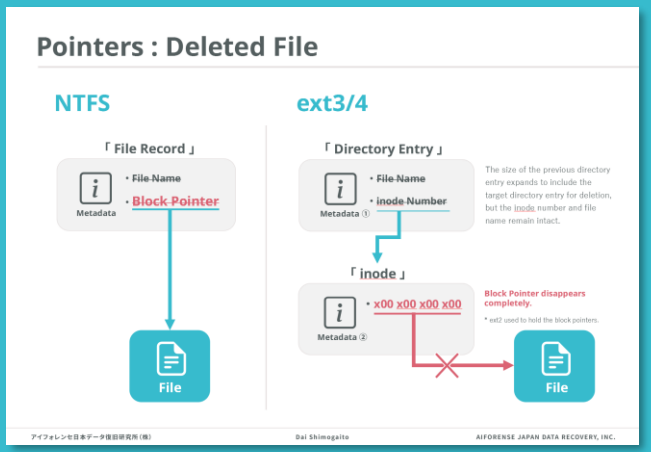
  - **Code Blue** (Japan, 2014 & 2016)

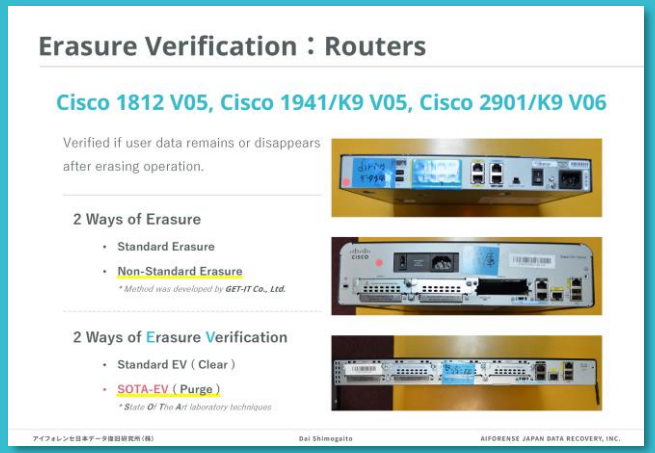
    - An international gathering of world-class computer security experts. Japan's "Black Hat"

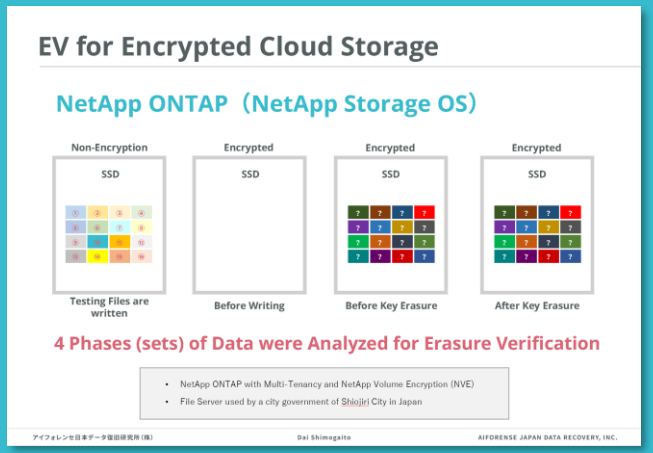
Contents of Today's Lecture

Data Erasure Verification (EV)

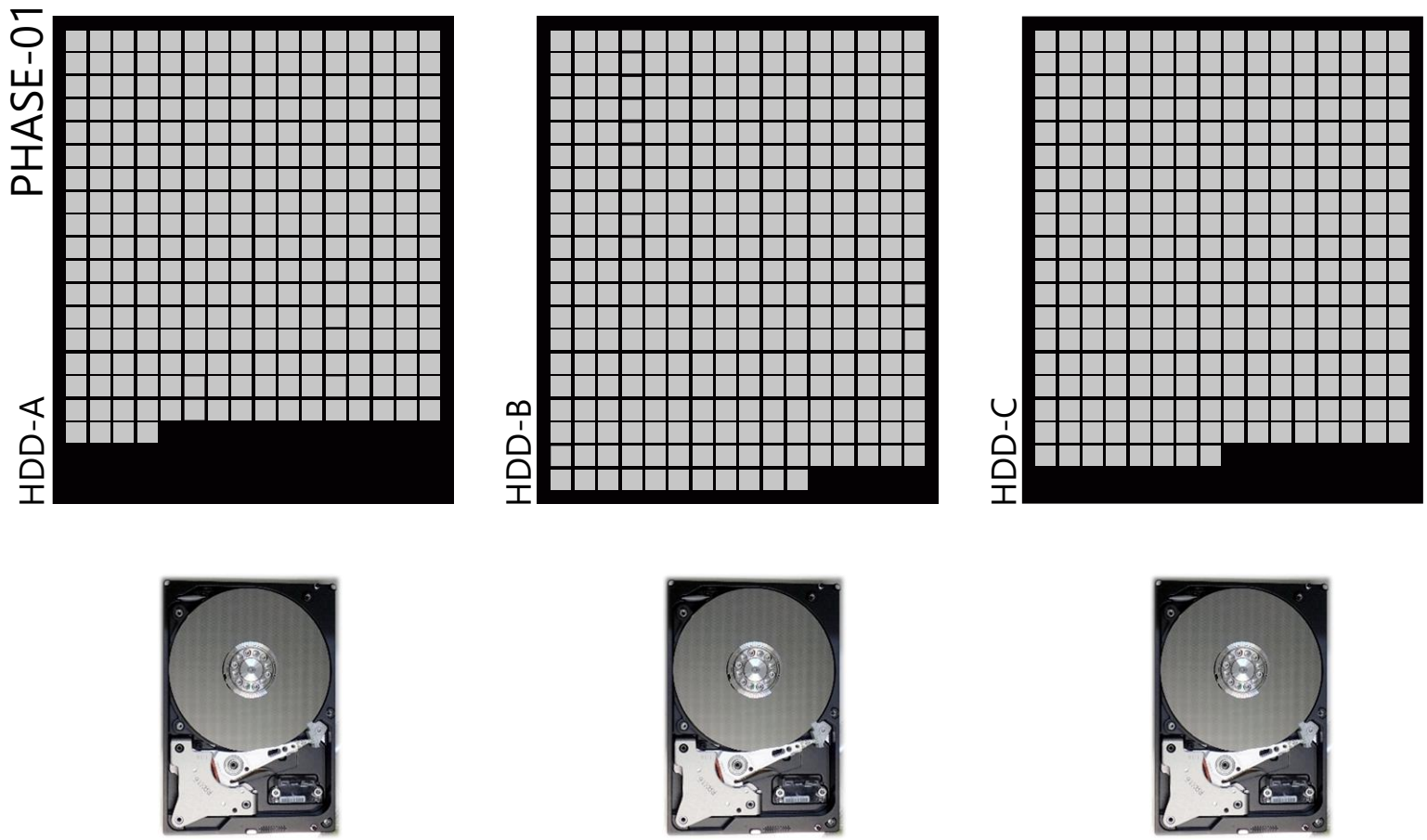






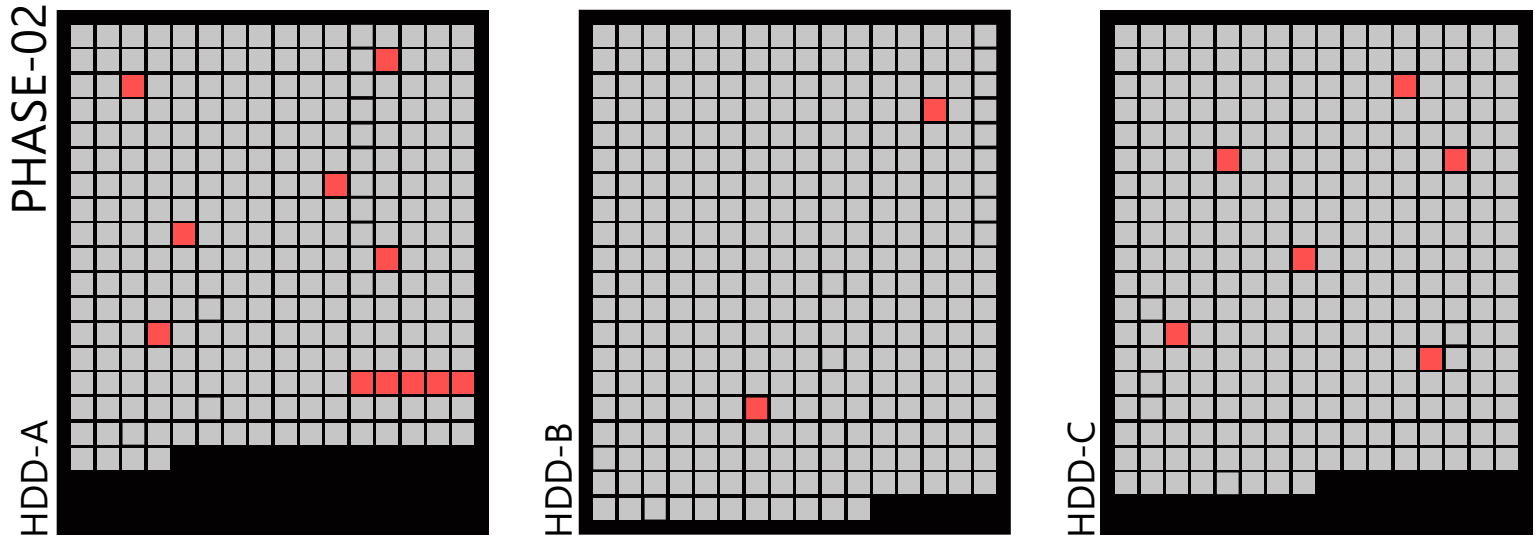


HDD : Physical Sectors

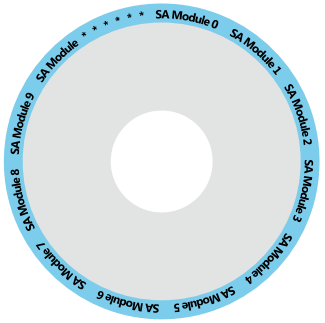


Physical Sector　LBA Sector　P-list Defects　G-List Defects

HDD：Primary Defects on Disk (P-List)

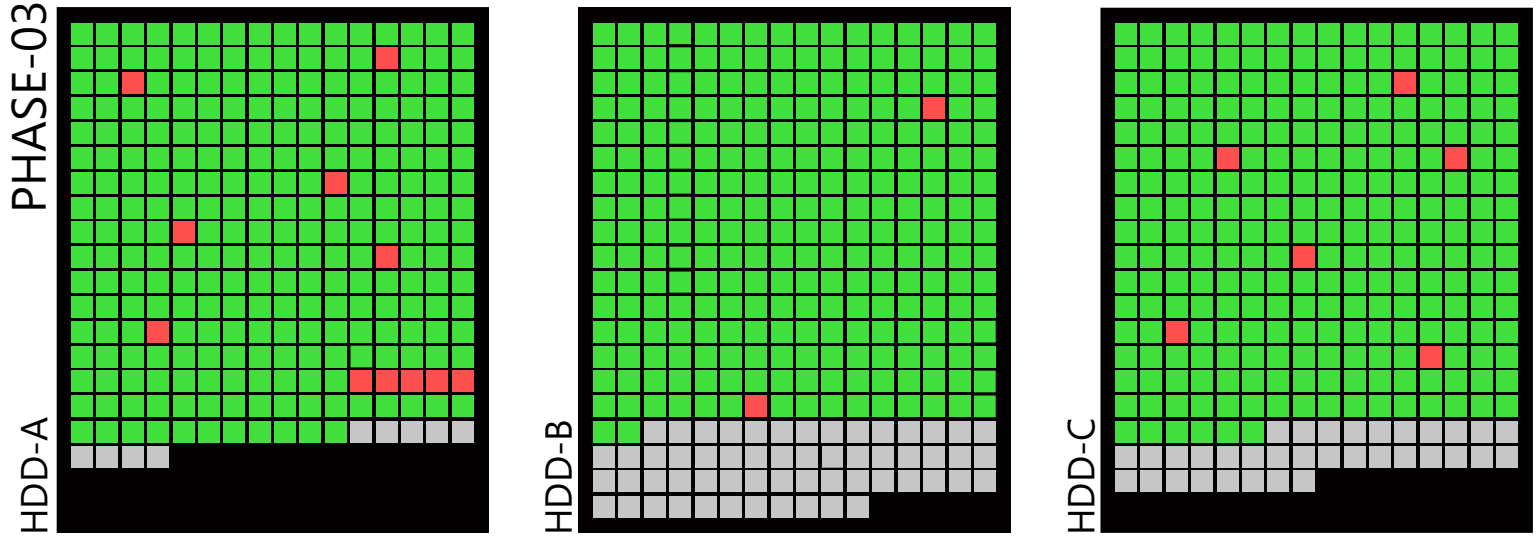


- indicates a Primary Defect
- P-List is an abbreviation of Primary Defects List
- P-List is a part of Firmware
- P-List is unique for each individual product



Physical Sector　LBA Sector　P-list Defects　G-List Defects

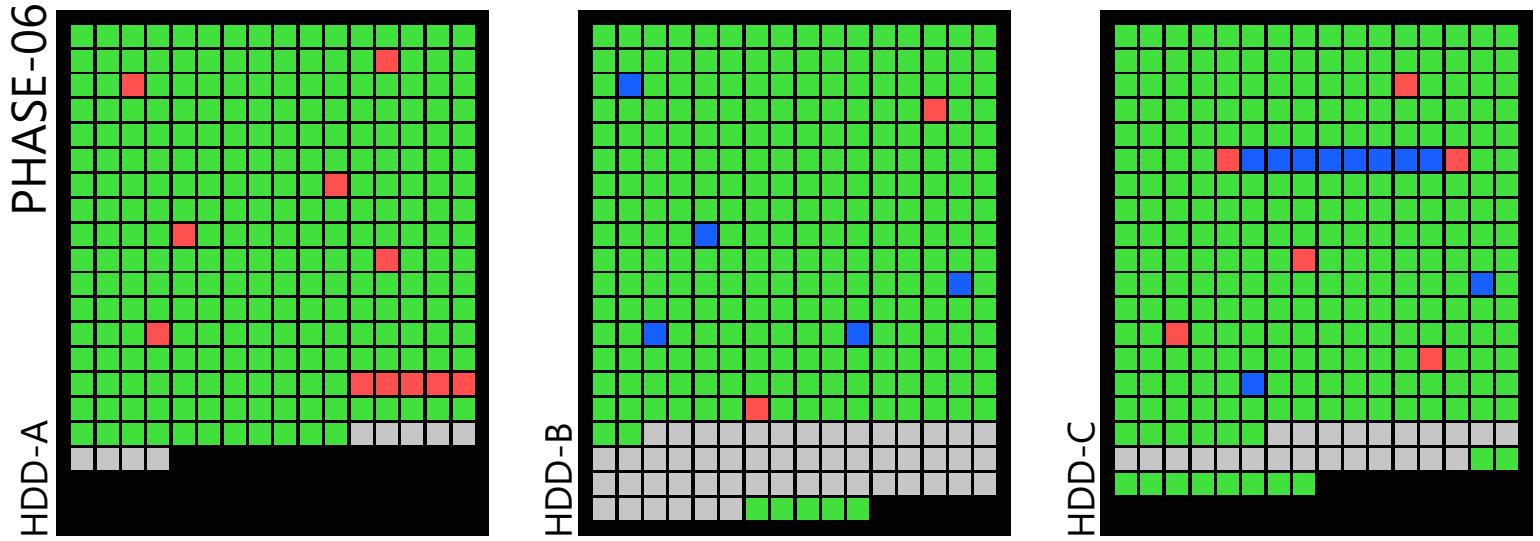
HDD：Default State (Before Use)



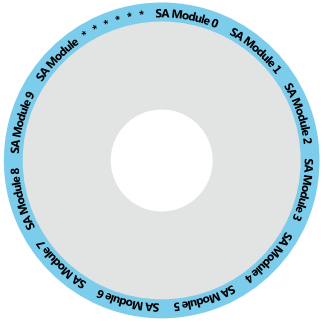
Same Capacity with equal number of LBAs.
But the number of total physical sectors are different.

Physical Sector　LBA Sector　P-list Defects　G-List Defects

HDD：After Use with Additional Defects ■

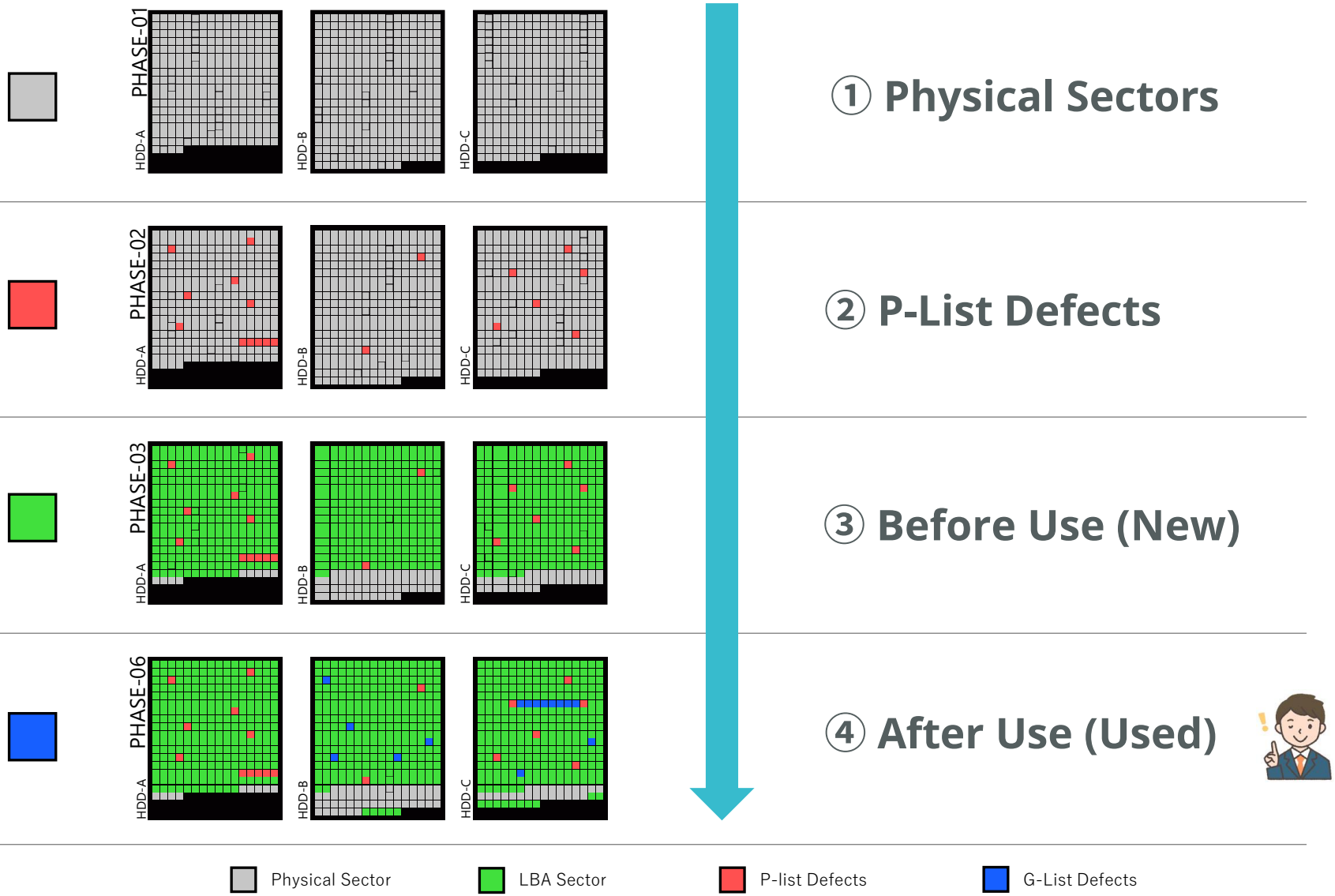


- ■ indicates a Growth Defect
- G-List is an abbreviation of Growth Defects List
- G-List is a part of Firmware
- G-List is unique for each individual product
- ■ **may hold past data**



Physical Sector　LBA Sector　P-list Defects　G-List Defects

HDD：Physical Sectors and Logical Sectors



NIST SP 800-88 Rev.1

Guidelines for Media Sanitization

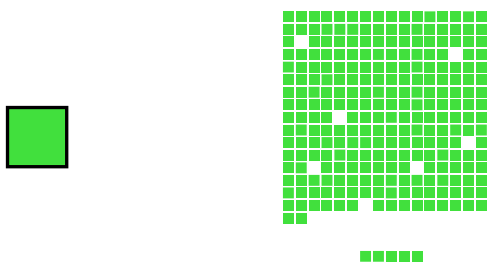
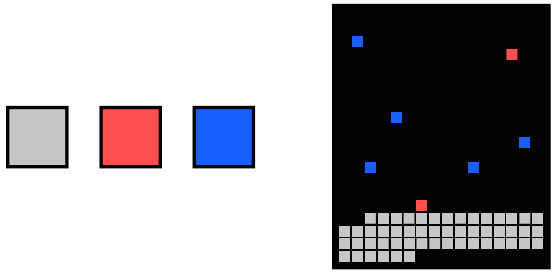
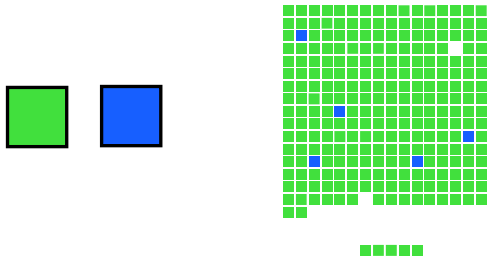
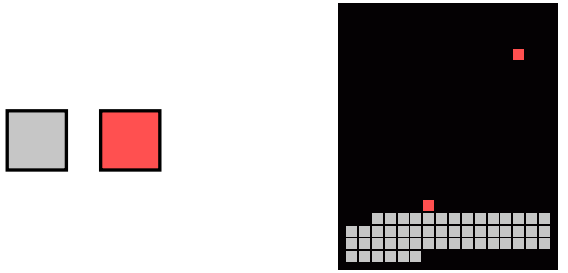
Clear, Purge, and Destroy are actions that can be taken to sanitize media. The categories of sanitization are defined as follows:

- **Clear** applies logical techniques to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques; typically applied through the standard Read and Write commands to the storage device, such as by rewriting with a new value or using a menu option to reset the device to the factory state (where rewriting is not supported).
- **Purge** applies physical or logical techniques that render Target Data recovery infeasible using state of the art laboratory techniques.
- **Destroy** renders Target Data recovery infeasible using state of the art laboratory techniques and results in the subsequent inability to use the media for storage of data.

Source of Reference：NIST.「NIST Special Publication 800-88 Revision 1」. December 2014. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-88r1.pdf, p.9,（Accessed : Jan 28 2023）.

ATA HDD：Erasable Area

NIST SP 800-88 Rev.1 , December 2014

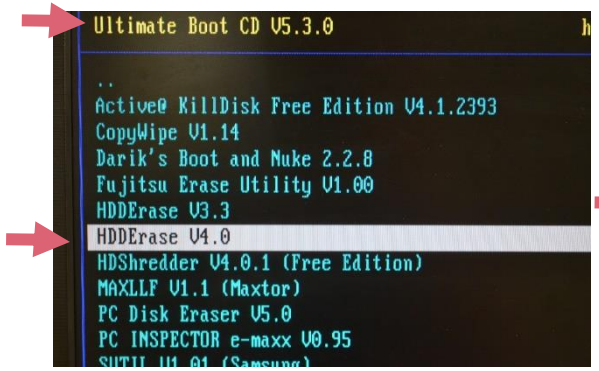
	Erasable Area	Non-Erasable Area
Clear Overwriting pattern should be at least a single write pass with a fixed data value, such as all zeros.		
Purge Enhanced Secure Erase		

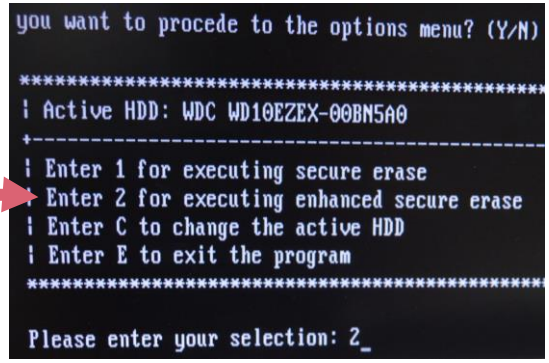
Physical Sector　LBA Sector　P-list Defects　G-List Defects

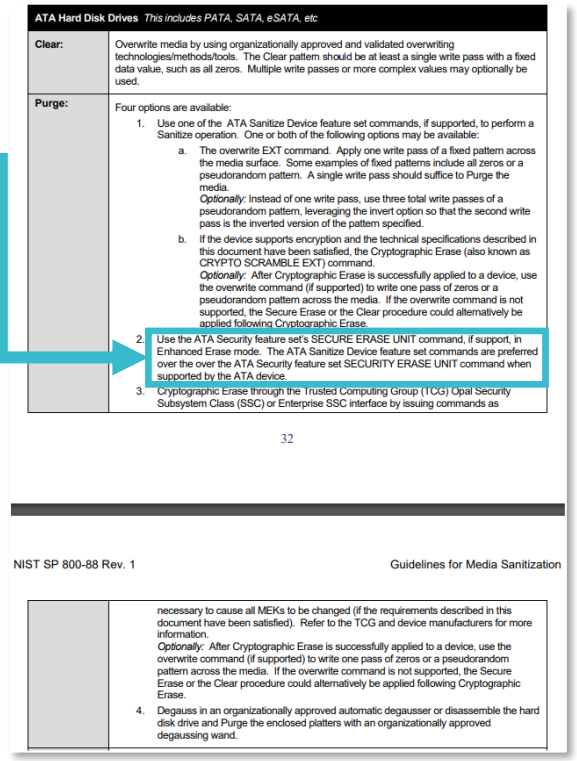
Purge : NIST SP 800-88 Rev.1 (ATA HDDs)

“Enhanced SECURE ERASE” to Purge

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.







ATA Hard Disk Drives *This includes PATA, SATA, eSATA, etc*	
Clear:	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.
Purge:	Four options are available: 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

32

NIST SP 800-88 Rev. 1 Guidelines for Media Sanitization

	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.

NIST SP 800-88 Rev.1

Source of Reference：NIST.「NIST Special Publication 800-88 Revision 1」. December 2014. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-88r1.pdf, p.32-33,（Accessed : May 13 2023）.

Question 1 from the Speaker

Has anyone read data from G-List Sectors ?

Question 2 from the Speaker

Has anyone ever found data from HDD which had been wiped by Enhanced Secure Erase ?

After Enhanced Secure Erase

Click the screen shot to watch on Youtube

https://www.youtube.com/watch?v=Bvv8AjyEzy8

InfoSec by Data Recovery Specialists

Who has *"state of the art laboratory techniques"*?

NIST SP 800-88 Rev. 1 Guidelines for Media Sanitization

Clear, Purge, and Destroy are actions that can be taken to sanitize media. The categories of sanitization are defined as follows:

- **Clear** applies logical techniques to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques; typically applied through the standard Read and Write commands to the storage device, such as by rewriting with a new value or using a menu option to reset the device to the factory state (where rewriting is not supported).
- **Purge** applies physical or logical techniques that render Target Data recovery infeasible using state of the art laboratory techniques.
- **Destroy** renders Target Data recovery infeasible using state of the art laboratory techniques and results in the subsequent inability to use the media for storage of data.

Source of Reference：NIST.「NIST Special Publication 800-88 Revision 1」. December 2014. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-88r1.pdf, p.9,（Accessed : Jan 28 2023）.

My Proposal for SDGs

It is essential for us, as Data Recovery Experts, to have a clear understanding of the data that could remain after a 'Clear' or 'Purge'.

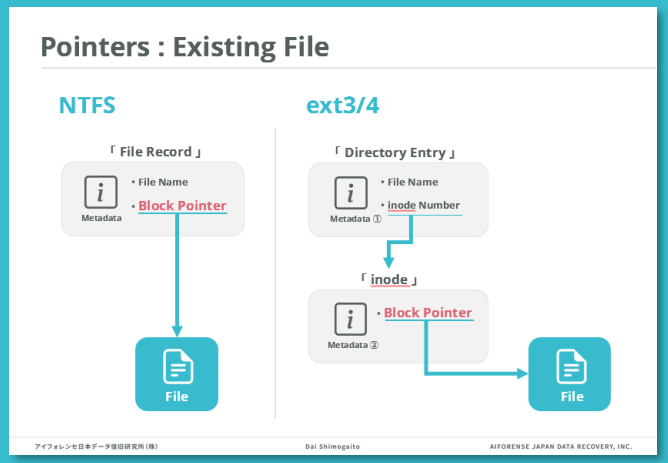
In spite of my demo at Code Blue 2016, I think the chances of data being found after "Enhanced Secure Erase" are close to zero.

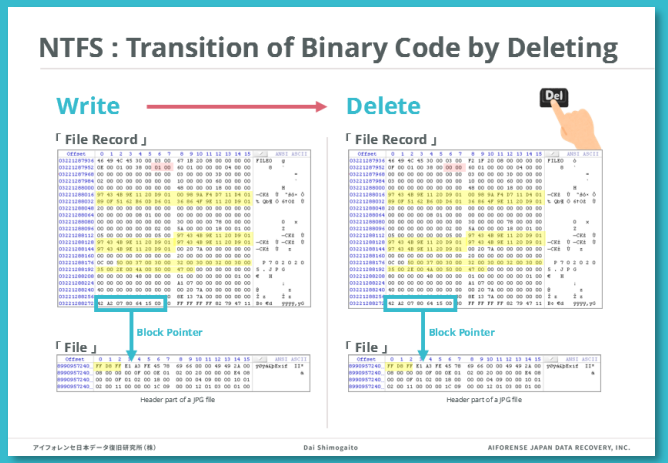
Why don't we prevent unnecessary destruction ?

Mechanism of Deleting Files

Contents

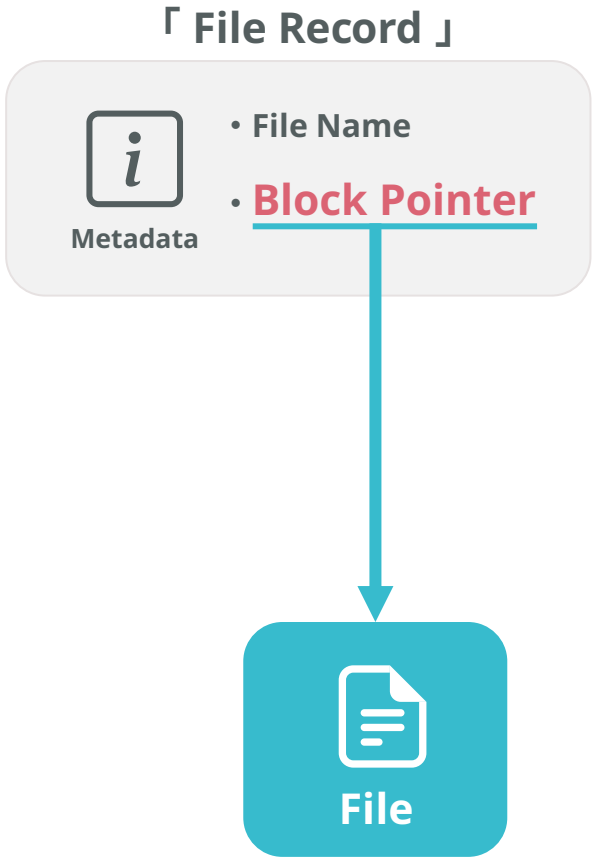
- How Pointers work
- Transition of Binary Code by Deleting Files



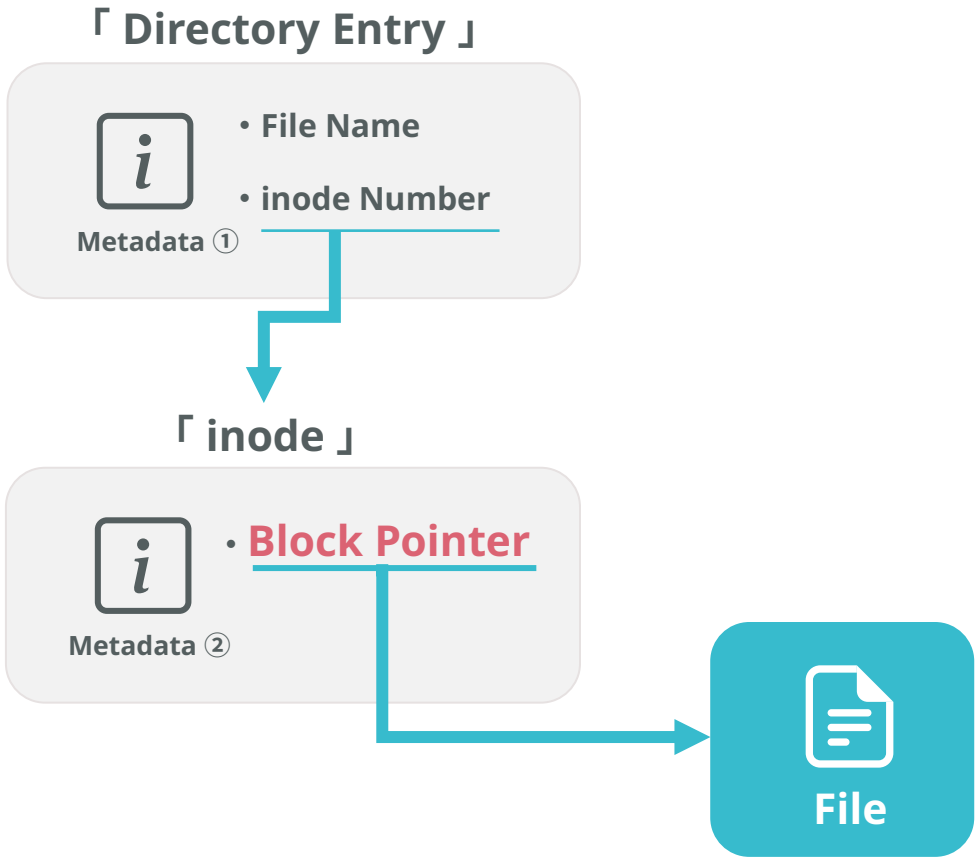


Pointers : Existing File

NTFS

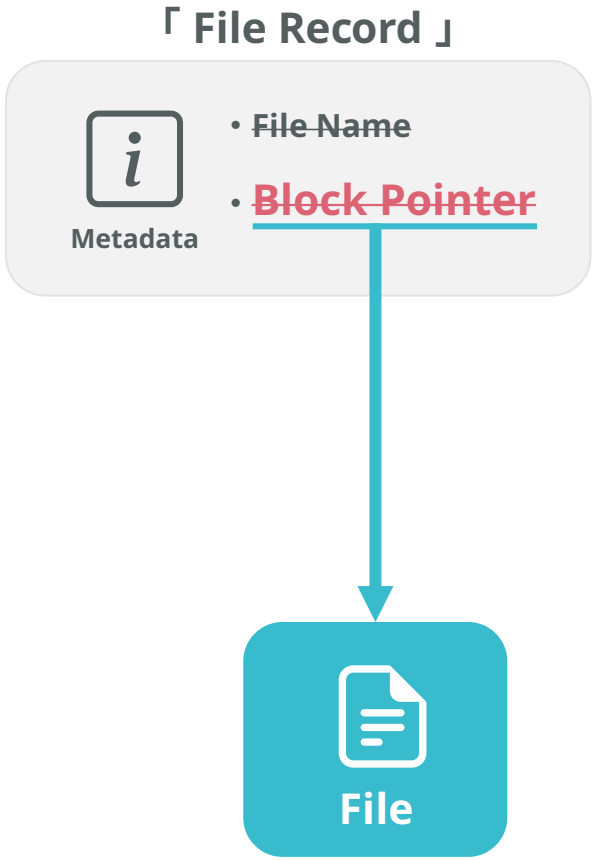


ext3/4

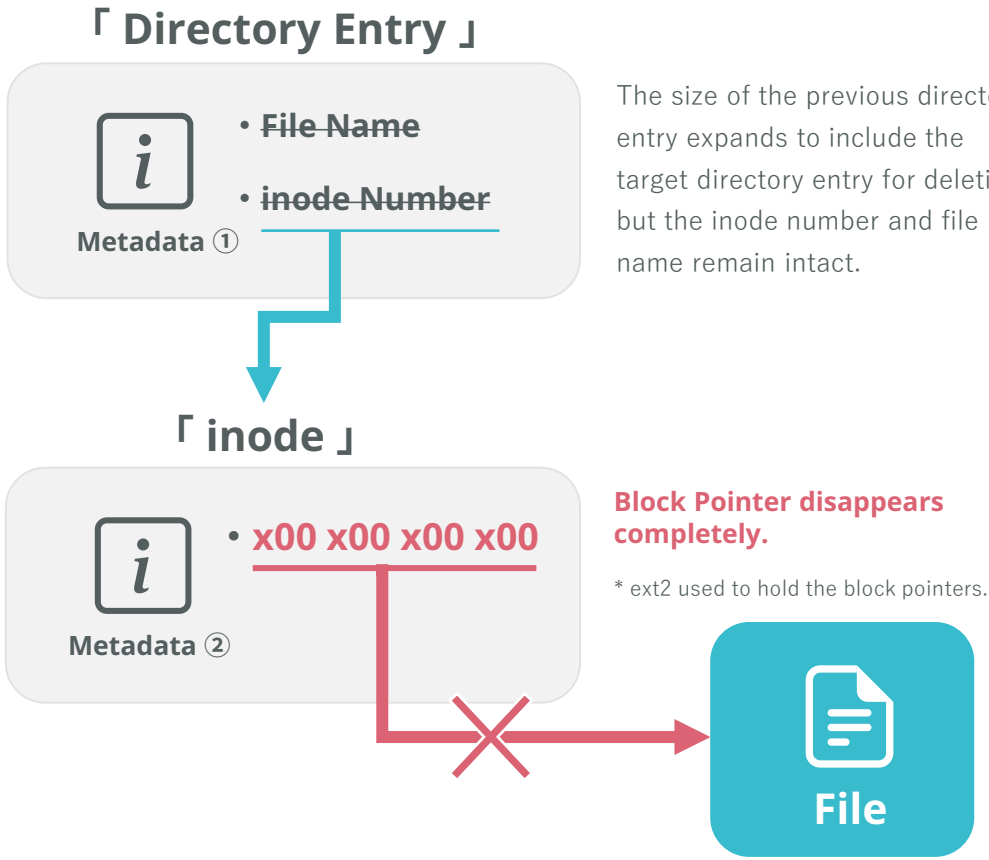


Pointers : Deleted File

NTFS



ext3/4



The size of the previous directory entry expands to include the target directory entry for deletion, but the inode number and file name remain intact.

Block Pointer disappears completely.

* ext2 used to hold the block pointers.

NTFS : Transition of Binary Code by Deleting

Write

「 File Record 」

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
03221287936	46	49	4C	45	30	00	03	00	67	1B	20	08	00	00	00	00	FILE0 g
03221287952	0E	00	01	00	38	00	01	00	60	01	00	00	00	04	00	00	8 `
03221287968	00	00	00	00	00	00	00	00	03	00	00	00	3D	00	00	00	=
03221287984	02	00	00	00	00	00	00	00	10	00	00	00	60	00	00	00	`
03221288000	00	00	00	00	00	00	00	00	48	00	00	00	18	00	00	00	H
03221288016	97	43	4B	9E	11	20	D9	01	00	98	9A	F4	D7	11	D4	01	—CKž Ù ˜šô× Ô
03221288032	89	0F	51	62	B6	0D	D6	01	36	86	4F	9E	11	20	D9	01	‰ Qb¶ Ö 6†Ož Ù
03221288048	20	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
03221288064	00	00	00	00	08	01	00	00	00	00	00	00	00	00	00	00	
03221288080	00	00	00	00	00	00	00	00	30	00	00	00	78	00	00	00	0 x
03221288096	00	00	00	00	00	00	02	00	5A	00	00	00	18	00	01	00	Z
03221288112	05	00	00	00	00	00	05	00	97	43	4B	9E	11	20	D9	01	—CKž Ù
03221288128	97	43	4B	9E	11	20	D9	01	97	43	4B	9E	11	20	D9	01	—CKž Ù —CKž Ù
03221288144	97	43	4B	9E	11	20	D9	01	00	20	7A	00	00	00	00	00	—CKž Ù z
03221288160	00	00	00	00	00	00	00	00	20	00	00	00	00	00	00	00	
03221288176	0C	00	50	00	37	00	30	00	32	00	30	00	32	00	30	00	P 7 0 2 0 2 0
03221288192	35	00	2E	00	4A	00	50	00	47	00	00	00	00	00	00	00	5 . J P G
03221288208	80	00	00	00	48	00	00	00	01	00	00	00	00	00	01	00	€ H
03221288224	00	00	00	00	00	00	00	00	A1	07	00	00	00	00	00	00	¡
03221288240	40	00	00	00	00	00	00	00	00	20	7A	00	00	00	00	00	@ z
03221288256									0	8E	13	7A	00	00	00	00	Ž z
03221288272	42	A2	07	80	64	15	0D		0	FF	FF	FF	FF	82	79	47	11	B¢ €d ÿÿÿÿ‚yG

Block Pointer

「 File 」

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
8990957240...	FF	D8	FF	E1	A3	FE	45	78	69	66	00	00	49	49	2A	00	ÿØÿá£þExif II*
8990957240...	08	00	00	00	0F	00	0E	01	02	00	20	00	00	00	E4	08	ä
8990957240...	00	00	0F	01	02	00	18	00	00	00	04	09	00	00	10	01	
8990957240...	02	00	11	00	00	00	1C	09	00	00	12	01	03	00	01	00	

Header part of a JPG file

Delete

「 File Record 」

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
03221287936	46	49	4C	45	30	00	03	00	F2	1F	20	08	00	00	00	00	FILE0 ò
03221287952	0F	00	01	00	38	00	00	00	60	01	00	00	00	04	00	00	8 `
03221287968	00	00	00	00	00	00	00	00	03	00	00	00	3D	00	00	00	=
03221287984	03	00	00	00	00	00	00	00	10	00	00	00	60	00	00	00	`
03221288000	00	00	00	00	00	00	00	00	48	00	00	00	18	00	00	00	H
03221288016	97	43	4B	9E	11	20	D9	01	00	98	9A	F4	D7	11	D4	01	—CKž Ù ˜šô× Ô
03221288032	89	0F	51	62	B6	0D	D6	01	36	86	4F	9E	11	20	D9	01	‰ Qb¶ Ö 6†Ož Ù
03221288048	20	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
03221288064	00	00	00	00	08	01	00	00	00	00	00	00	00	00	00	00	
03221288080	00	00	00	00	00	00	00	00	30	00	00	00	78	00	00	00	0 x
03221288096	00	00	00	00	00	00	02	00	5A	00	00	00	18	00	01	00	Z
03221288112	05	00	00	00	00	00	05	00	97	43	4B	9E	11	20	D9	01	—CKž Ù
03221288128	97	43	4B	9E	11	20	D9	01	97	43	4B	9E	11	20	D9	01	—CKž Ù —CKž Ù
03221288144	97	43	4B	9E	11	20	D9	01	00	20	7A	00	00	00	00	00	—CKž Ù z
03221288160	00	00	00	00	00	00	00	00	20	00	00	00	00	00	00	00	
03221288176	0C	00	50	00	37	00	30	00	32	00	30	00	32	00	30	00	P 7 0 2 0 2 0
03221288192	35	00	2E	00	4A	00	50	00	47	00	00	00	00	00	00	00	5 . J P G
03221288208	80	00	00	00	48	00	00	00	01	00	00	00	00	00	01	00	€ H
03221288224	00	00	00	00	00	00	00	00	A1	07	00	00	00	00	00	00	¡
03221288240	40	00	00	00	00	00	00	00	00	20	7A	00	00	00	00	00	@ z
03221288256									00	8E	13	7A	00	00	00	00	Ž z
03221288272	42	A2	07	80	64	15	0D		00	FF	FF	FF	FF	82	79	47	11	B¢ €d ÿÿÿÿ‚yG

Block Pointer

「 File 」

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
8990957240...	FF	D8	FF	E1	A3	FE	45	78	69	66	00	00	49	49	2A	00	ÿØÿá£þExif II*
8990957240...	08	00	00	00	0F	00	0E	01	02	00	20	00	00	00	E4	08	ä
8990957240...	00	00	0F	01	02	00	18	00	00	00	04	09	00	00	10	01	
8990957240...	02	00	11	00	00	00	1C	09	00	00	12	01	03	00	01	00	

Header part of a JPG file

ext4 : Transition of Binary Code by Deleting

※Verified on Kali 2021.1 (OS:ext4)

Write

「 Directory Entry 」

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
0C	00	00	00	0C	00	01	02	2E	00	00	00	02	00	00	00	.
0C	00	02	02	2E	2E	00	00	0D	00	00	00	1C	00	14	01	..
2E	63	72	65	64	65	6E	74	69	61	6C	73	2E	74	78	74	.credentials.txt
2E	73	77	70	0E	00	00	00	18	00	0F	01	63	72	65	64	.swp cred
65	6E	74	69	61	6C	73	2E	74	78	74	00	0F	00	00	00	entials.txt
20	00	18	01	41	72	74	69	66	61	63	74	73	2D	52	65	Artifacts-Re
66	65	72	65	6E	63	65	2E	78	6C	73	78	10	00	00	00	ference.xlsx
88	0F	16	01	42	61	6E	6B	69	6E	67	20	4F	70	65	72	^ Banking Oper
61	74	69	6F	6E	73	2E	70	64	66	00	00	00	00	00	00	ations.pdf

①inode番号 (0x00,4) ②エントリ長 (0x04,2) ③ファイル名長 (0x06,1) ④ファイルタイプ (0x07,1) ⑤ファイル名 (0x08,③)

「 inode 」

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
A4	81	E8	03	56	99	00	00	97	FC	2B	61	97	FC	2B	61	¤ è V™ —ü+a—ü+a
A5	F9	2B	61	00	00	00	00	E8	03	01	00	50	00	00	00	¥ù+a è P
00	00	08	00	01	00	00	00	0A	F3	01	00	04	00	00	00	ó
00	00	00	00	00	00	00	00	0A	00	00	00	44	80	00	00	D€
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	31	31	DB	34	00	00	00	00	00	00	00	00	?1Û4

Block Pointer

①パミッション＆ファイルタイプ (0x00,2) ②ファイルサイズ下位 (0x04,4) ③アクセス日時 (0x08,4) ④inode変更日時 (0x0C,4) ⑤ファイル更新日時 (0x10,4) ⑥ファイル削除日時 (0x14,4) ⑦ハードリンク数 (0x1A,2) ⑧Extent Header (0x28,12) **⑨Extent ※上図では(0x34,12)**

検証ファイル：Kali_1-02-After-Files-are-written.vmdk

Delete

「 Directory Entry 」

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
0C	00	00	00	0C	00	01	02	2E	00	00	00	02	00	00	00	.
0C	00	02	02	2E	2E	00	00	0D	00	00	00	1C	00	14	01	..
2E	63	72	65	64	65	6E	74	69	61	6C	73	2E	74	78	74	.credentials.txt
2E	73	77	70	0E	00	00	00	38	00	0F	01	63	72	65	64	.swp 8 cred
65	6E	74	69	61	6C	73	2E	74	78	74	00	0F	00	00	00	entials.txt
20	00	18	01	41	72	74	69	66	61	63	74	73	2D	52	65	Artifacts-Re
66	65	72	65	6E	63	65	2E	78	6C	73	78	10	00	00	00	ference.xlsx
88	0F	16	01	42	61	6E	6B	69	6E	67	20	4F	70	65	72	^ Banking Oper
61	74	69	6F	6E	73	2E	70	64	66	00	00	00	00	00	00	ations.pdf

削除対象エントリのひとつ前のエントリ長が、削除対象エントリの分だけ増加している。これにより削除対象エントリは、認識されない状態となる。inode番号は残存。

「 inode 」

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
A4	81	E8	03	00	00	00	00	97	FC	2B	61	81	FD	2B	61	¤ è —ü+a ý+a
81	FD	2B	61	81	FD	2B	61	E8	03	00	00	00	00	00	00	ý+a ý+aè
00	00	08	00	01	00	00	00	0A	F3	00	00	04	00	00	00	ó
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	31	31	DB	34	00	00	00	00	00	00	00	00	?1Û4

x00 x00
x00 x00

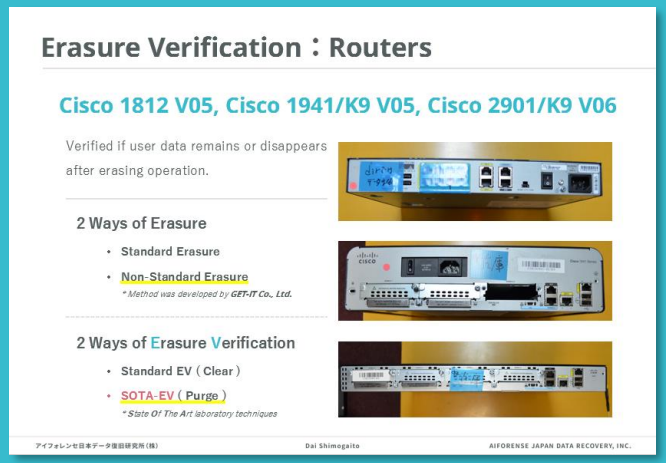
ブロックポインタ（エクステント）はゼロフィルされるため、データ本体の追跡は不可能。ファイルサイズ情報が消滅し、ファイル削除日時が記録される。

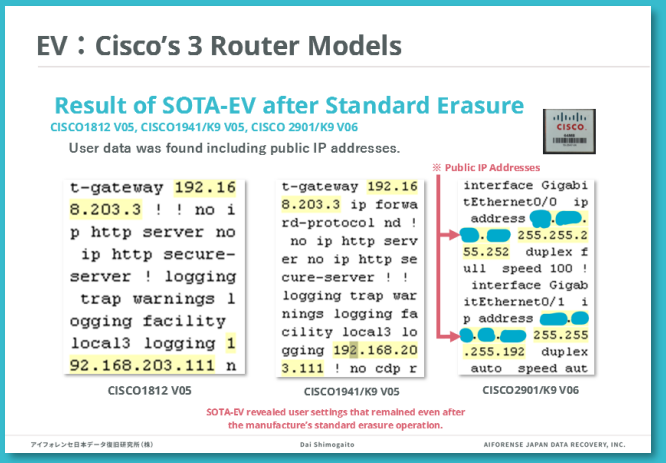
検証ファイル：Kali_1-03-After-excel-file-is-deleted.vmdk

EV for Network Devices

Contents

- Cisco’s network switch & router
- The devices can be reused after purge-level erasure





Erasure Verification : Network Switch

Network Switch : Cisco WS-C3560V2-24TS-E V05

Verified if user data remains or disappears after erasing operation.

2 Ways of Erasure

- Standard Erasure
- Non-Standard Erasure

** Method was developed by **GET-IT Co., Ltd.***

2 Ways of Erasure Verification

- Standard EV (Clear)
- SOTA-EV (Purge)

** **S**tate **O**f **T**he **A**rt laboratory techniques*

EV：Cisco WS-C3560V2-24TS-E V05

Result of SOTA-EV after Standard Erasure

IPv4 addresses were found at 1,696 locations by SOTA-EV.

```
21 0A 69 6E 74 65 72 66  61 63 65 20 56 6C 61 6E | ! interface Vlan
31 32 30 32 0A 20 69 70  20 61 64 64 72 65 73 73 | 1202  ip address
20 31 39 32 2E 31 36 38  2E 32 30 32 2E 32 32 20 |  192.168.202.22
32 35 35 2E 32 35 35 2E  32 35 35 2E 30 0A 20 6E | 255.255.255.0  n
```

```
6C 6F 63 61 6C 33 0A 6C  6F 67 67 69 6E 67 20 31 | local3 logging 1
39 32 2E 31 36 38 2E 32  30 33 2E 31 31 31 0A 6E | 92.168.203.111 n
6F 20 63 64 70 20 72 75  6E 0A 21 0A 21 0A 21 0A | o cdp run ! ! !
```

```
65 0A 21 0A 69 70 20 64  65 66 61 75 6C 74 2D 67 | e ! ip default-g
61 74 65 77 61 79 20 31  39 32 2E 31 36 38 2E 32 | ateway 192.168.2
30 33 2E 33 0A 69 70 20  63 6C 61 73 73 6C 65 73 | 03.3 ip classles
```

SOTA-EV revealed user settings that remained even after the manufacture's standard erasure operation.

Erasure Verification：Routers

Cisco 1812 V05, Cisco 1941/K9 V05, Cisco 2901/K9 V06

Verified if user data remains or disappears after erasing operation.

2 Ways of Erasure

- Standard Erasure
- Non-Standard Erasure

** Method was developed by **GET-IT Co., Ltd.***

2 Ways of Erasure Verification

- Standard EV (Clear)
- SOTA-EV (Purge)

** **S**tate **O**f **T**he **A**rt laboratory techniques*

EV：Cisco’s 3 Router Models

Result of SOTA-EV after Standard Erasure

CISCO1812 V05, CISCO1941/K9 V05, CISCO 2901/K9 V06

User data was found including public IP addresses.

※ Public IP Addresses

```
t-gateway 192.16
8.203.3 ! ! no i
p http server no
 ip http secure-
server ! logging
 trap warnings l
ogging facility
local3 logging 1
92.168.203.111 n
```

CISCO1812 V05

```
t-gateway 192.16
8.203.3 ip forwa
rd-protocol nd !
 no ip http serv
er no ip http se
cure-server ! !
logging trap war
nings logging fa
cility local3 lo
gging 192.168.20
3.111 ! no cdp r
```

CISCO1941/K9 V05

```
interface Gigabi
tEthernet0/0  ip
 address [redacted]
[redacted] 255.255.2
55.252  duplex f
ull  speed 100 !
 interface Gigab
itEthernet0/1  i
p address [redacted]
[redacted] 255.255
.255.192  duplex
 auto  speed aut
```

CISCO2901/K9 V06

SOTA-EV revealed user settings that remained even after the manufacture’s standard erasure operation.

EV for Cisco’s Network Devices

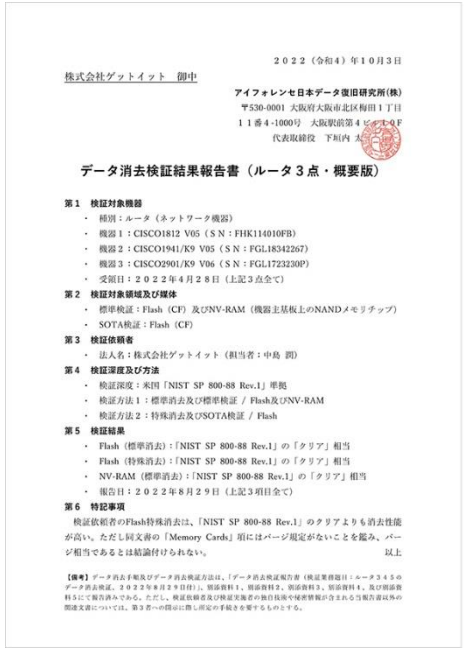
First Successful “Purge-Level” EV in Japan

GET-IT Co., Ltd. newly developed the purge level data erasure technology which meets “NIST SP800-88 Rev.1”

Those verified Cisco’s network devices can be reused.

GET IT

News Release : https://www.get-it.ne.jp/news_230203/



2022（令和4）年10月3日

株式会社ゲットイット　御中

アイフォレンセ日本データ復旧研究所(株)
〒530-0001 大阪府大阪市北区梅田1丁目
11番4-1000号 大阪駅前第4ビル7-9F
代表取締役 下垣内 太

データ消去検証結果報告書（ルータ３点・概要版）

第１ 検証対象機器
- 種別：ルータ（ネットワーク機器）
- 機器１：CISCO1812 V05（ＳＮ：FHK114010FB）
- 機器２：CISCO1941/K9 V05（ＳＮ：FGL18342267）
- 機器３：CISCO2901/K9 V06（ＳＮ：FGL1723230P）
- 受領日：２０２２年４月２８日（上記３点全て）

第２ 検証対象領域及び媒体
- 標準検証：Flash（CF）及びNV-RAM（機器主基板上のNANDメモリチップ）
- SOTA検証：Flash（CF）

第３ 検証依頼者
- 法人名：株式会社ゲットイット（担当者：中島 潤）

第４ 検証深度及び方法
- 検証深度：米国「NIST SP 800-88 Rev.1」準拠
- 検証方法１：標準消去及び標準検証 / Flash及びNV-RAM
- 検証方法２：特殊消去及びSOTA検証 / Flash

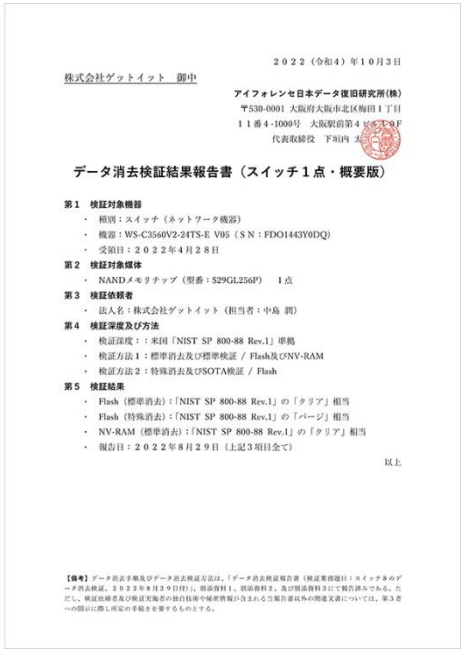
第５ 検証結果
- Flash（標準消去）：「NIST SP 800-88 Rev.1」の「クリア」相当
- Flash（特殊消去）：「NIST SP 800-88 Rev.1」の「クリア」相当
- NV-RAM（標準消去）：「NIST SP 800-88 Rev.1」の「クリア」相当
- 報告日：２０２２年８月２９日（上記３項目全て）

第６ 特記事項

検証依頼者のFlash特殊消去は、「NIST SP 800-88 Rev.1」のクリアよりも消去性能が高い。ただし同文書の「Memory Cards」項にはパージ規定がないことを鑑み、パージ相当であるとは結論付けられない。

以上

【備考】データ消去手順及びデータ消去検証方法は、「データ消去検証報告書（検証業務題目：ルータ３４５のデータ消去検証。２０２２年８月２９日付）」、別添資料１、別添資料２、別添資料３、別添資料４、及び別添資料５にて報告済みである。ただし、検証依頼者及び検証実施者の独自技術や秘密情報が含まれる当報告書以外の関連文書については、第３者への開示に際し所定の手続きを要するものとする。



2022（令和4）年10月3日

株式会社ゲットイット　御中

アイフォレンセ日本データ復旧研究所(株)
〒530-0001 大阪府大阪市北区梅田1丁目
11番4-1000号 大阪駅前第4ビル7-9F
代表取締役 下垣内 太

データ消去検証結果報告書（スイッチ１点・概要版）

第１ 検証対象機器
- 種別：スイッチ（ネットワーク機器）
- 機器：WS-C3560V2-24TS-E V05（ＳＮ：FDO1443Y0DQ）
- 受領日：２０２２年４月２８日

第２ 検証対象媒体
- NANDメモリチップ（型番：S29GL256P） １点

第３ 検証依頼者
- 法人名：株式会社ゲットイット（担当者：中島 潤）

第４ 検証深度及び方法
- 検証深度：：米国「NIST SP 800-88 Rev.1」準拠
- 検証方法１：標準消去及び標準検証 / Flash及びNV-RAM
- 検証方法２：特殊消去及びSOTA検証 / Flash

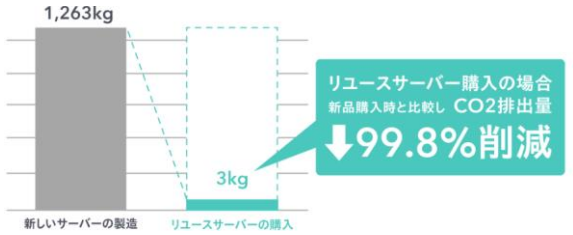
第５ 検証結果
- Flash（標準消去）：「NIST SP 800-88 Rev.1」の「クリア」相当
- Flash（特殊消去）：「NIST SP 800-88 Rev.1」の「パージ」相当
- NV-RAM（標準消去）：「NIST SP 800-88 Rev.1」の「クリア」相当
- 報告日：２０２２年８月２９日（上記３項目全て）

以上

【備考】データ消去手順及びデータ消去検証方法は、「データ消去検証報告書（検証業務題目：スイッチ１のデータ消去検証。２０２２年８月２９日付）」、別添資料１、別添資料２、及び別添資料３にて報告済みである。ただし、検証依頼者及び検証実施者の独自技術や秘密情報が含まれる当報告書以外の関連文書については、第３者への開示に際し所定の手続きを要するものとする。

物理破壊以外の方法が、IT機器の循環型経済の鍵

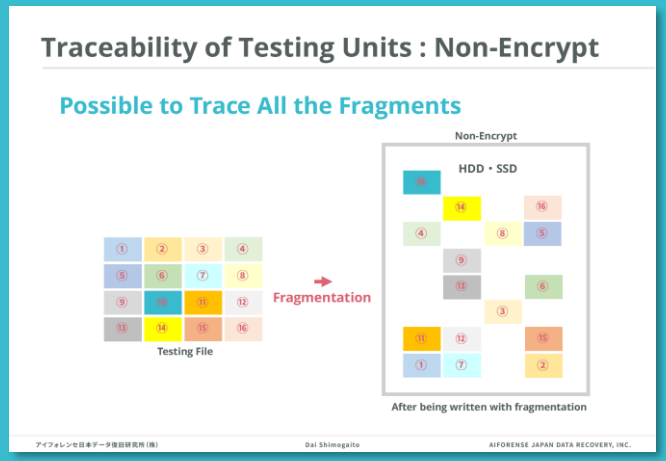
ゲットイットは「Sustainable Computing®」を掲げ、IT機器のリユース・リサイクルを推進しています。「物理破壊」では機器をリユースすることはできません。「磁気破壊」を選んだ際もリユースはできません。それに対し、適切なソフトウェア消去を選択した場合は撤去費、消去費を上回る買い取り額を提示できる場合があり、企業側は従来の「コスト」を「投資」に転換することが可能になります。

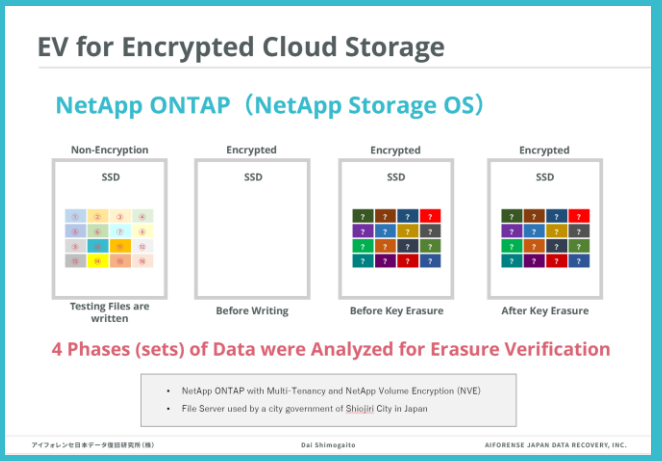


EV for Encrypted Cloud Storage

Contents

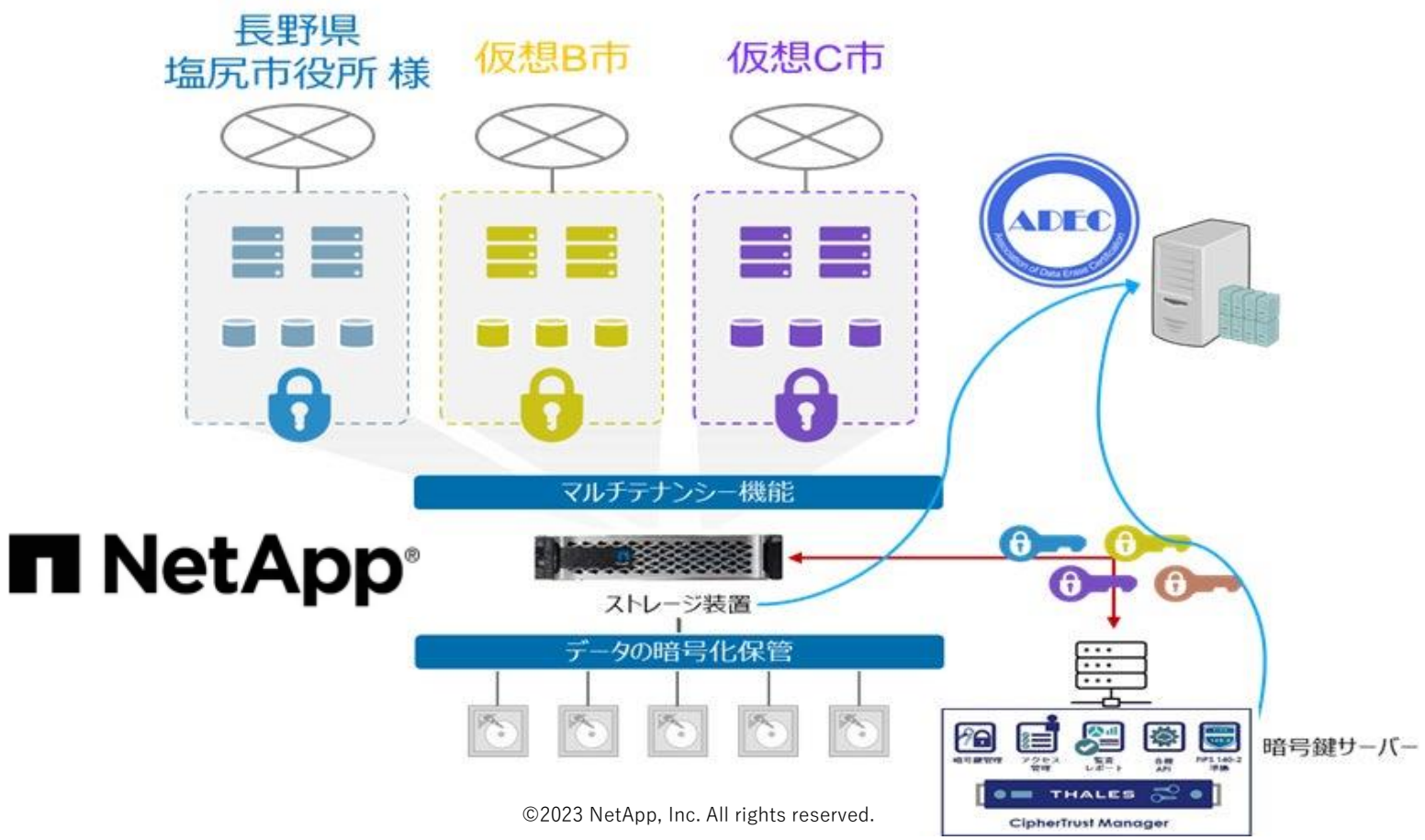
- Basics of EV Procesures
- EV for Encrypted Cloud Storage





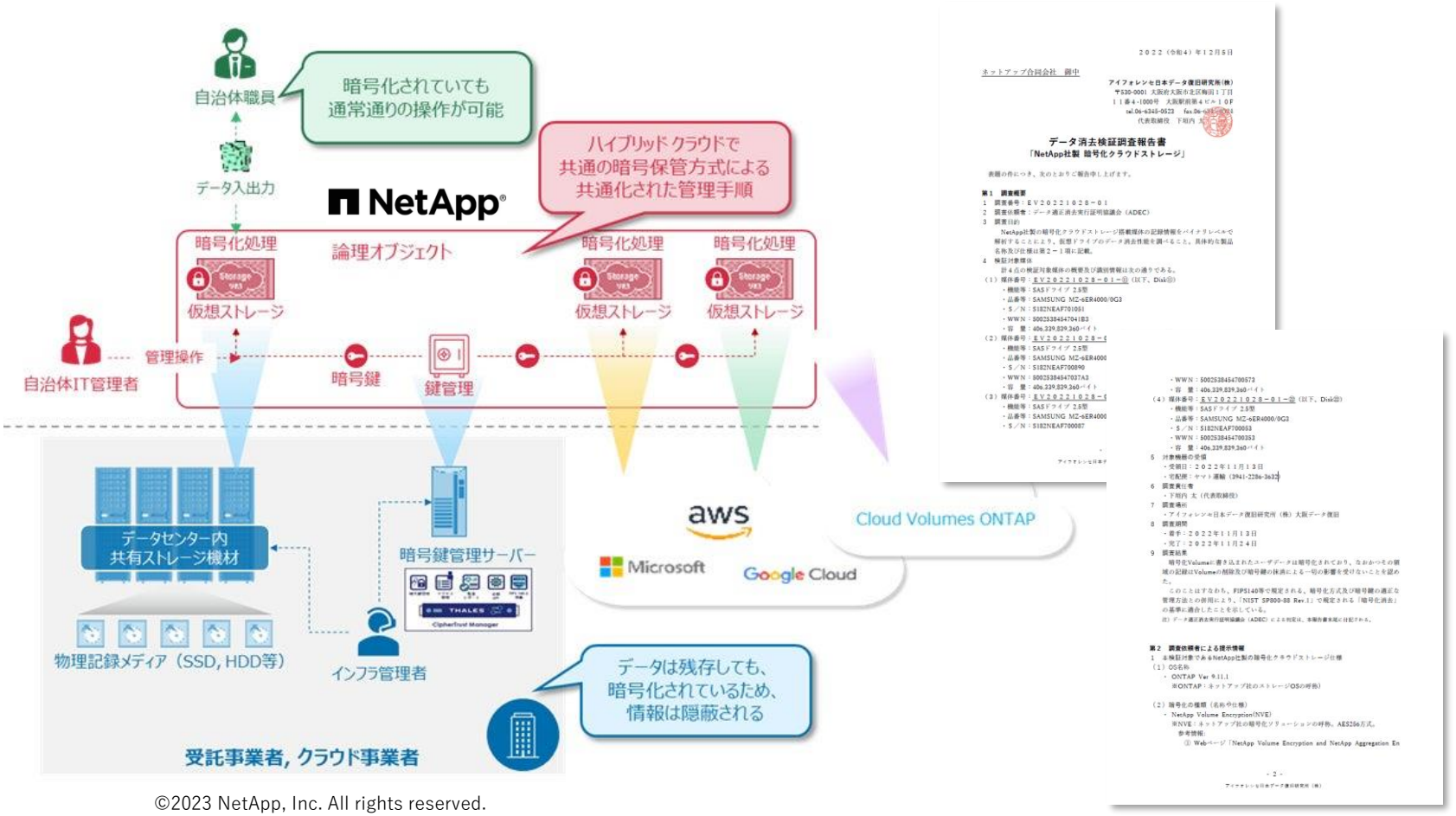
EV for NetApp's Encrypted Cloud Storage

First PoC-EV in Japan with a City Government



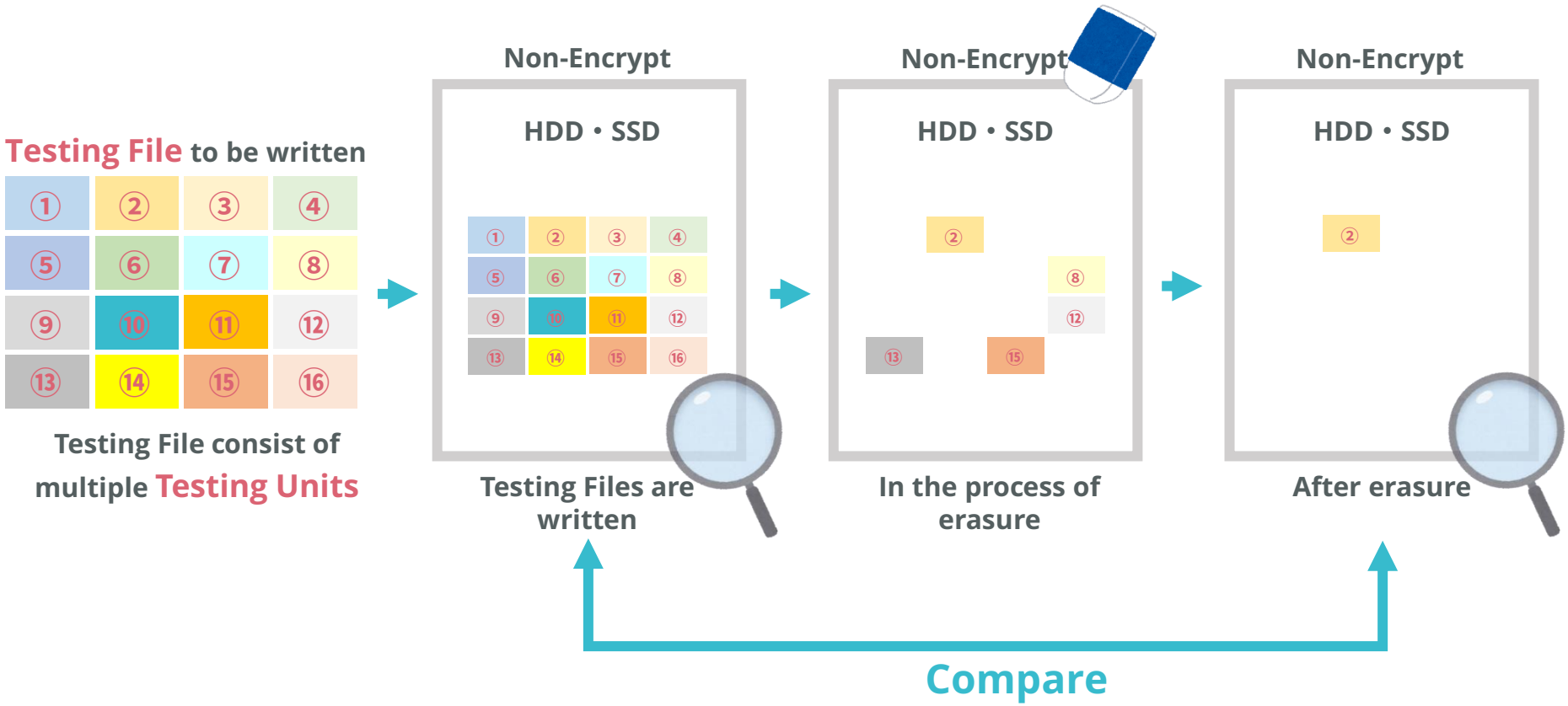
EV for NetApp's Encrypted Cloud Storage

First PoC-EV in Japan with a City Government



EV Procedure : Non-Encryption

Compare Binary Code Before and After Erasure

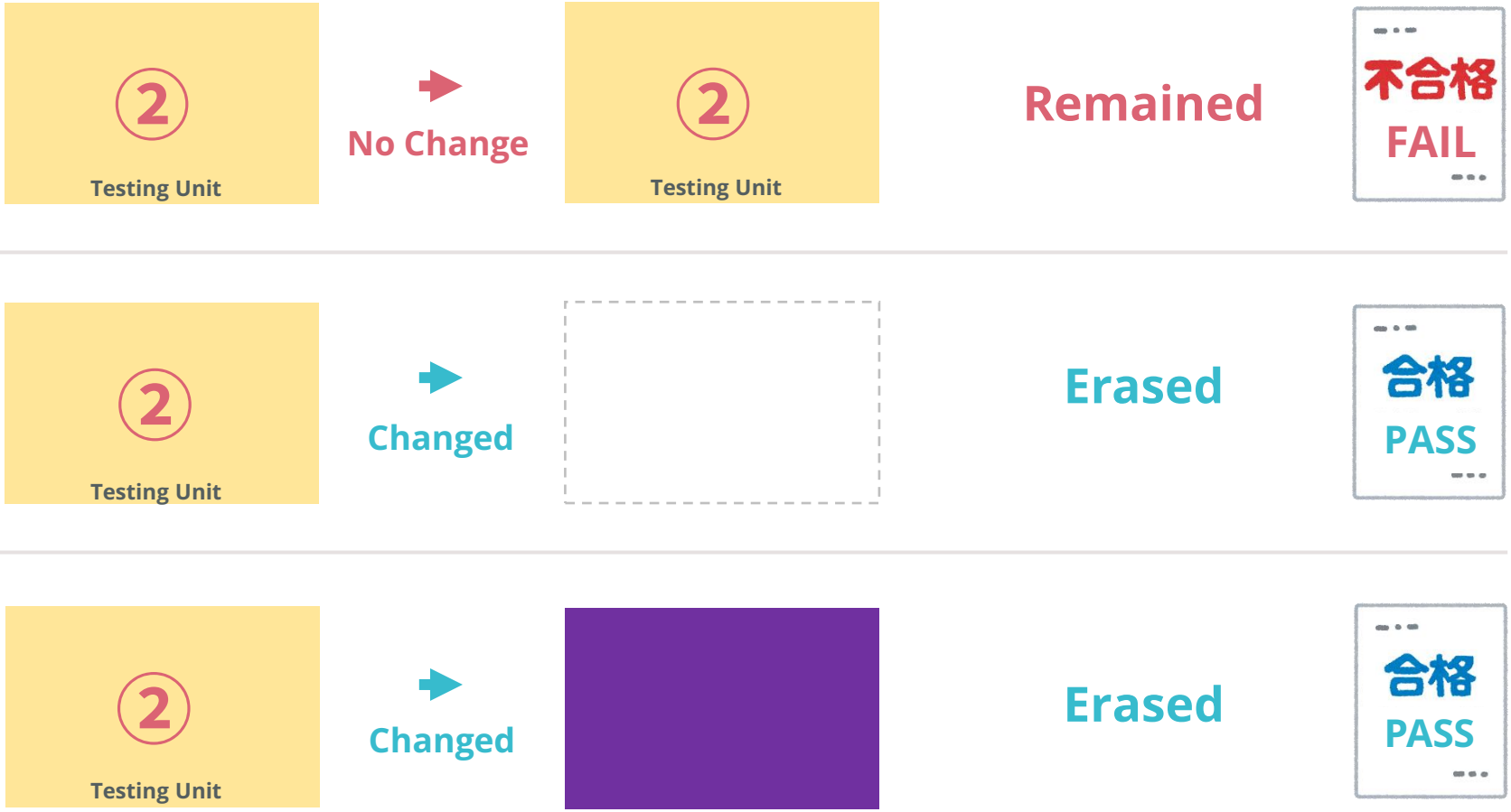


EV Procedure : Non-Encryption

Comparing data at the same position : Overwrite

Before Erasure

After Erasure



EV Procedure : Non-Encryption

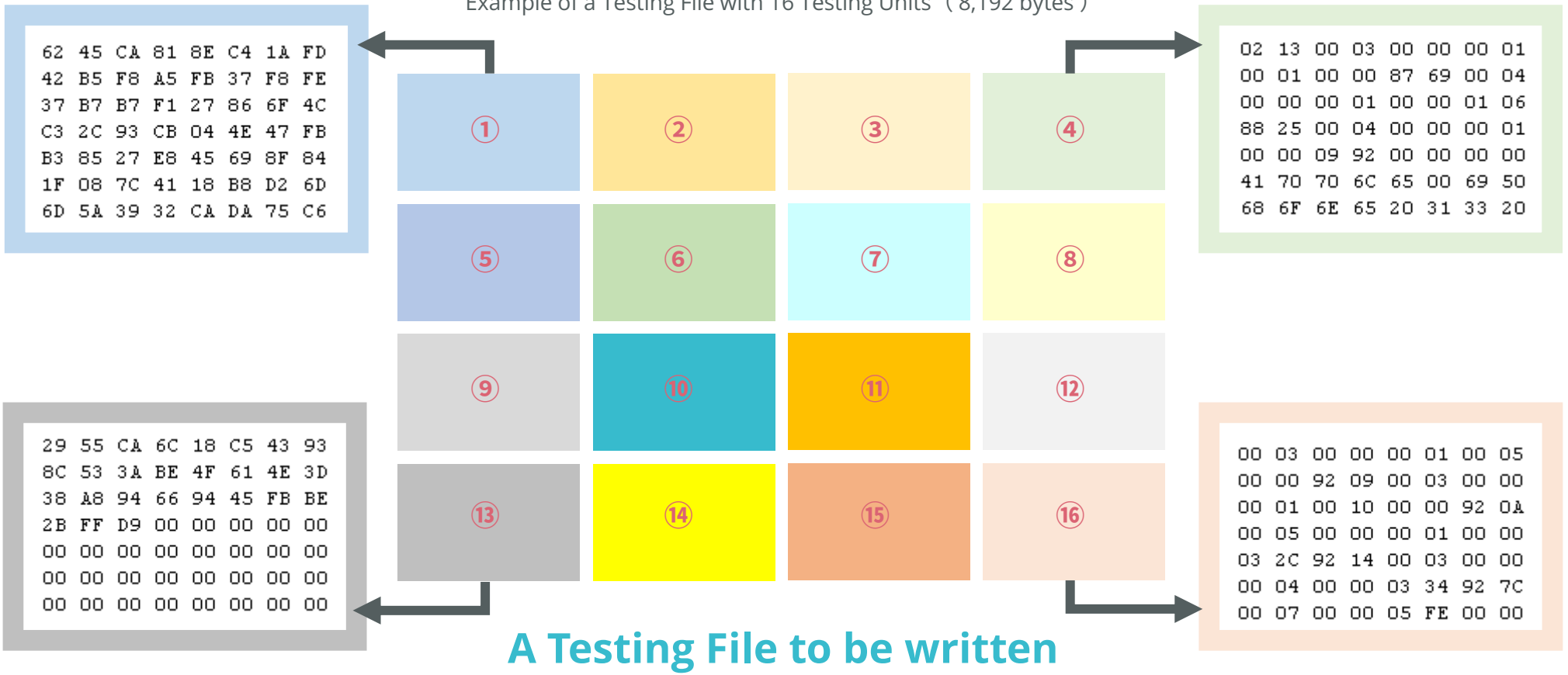
Comparing data at the same position : Overwrite

Before Erasure		After Erasure		
3E CE 46 95 17 B4 A4 E3 48 1C F5 AC FB 8D 3A F2 OF E7 5B BA 7F 82 3C 1F 34 68 EB F3 28 5F BC 84 C6 8F E2 65 B5 68 97 56 D6 2B 18 A4 96 48 9A 26 1D BF 9D 6E 5D D9 49 73	→ No Change	3E CE 46 95 17 B4 A4 E3 48 1C F5 AC FB 8D 3A F2 OF E7 5B BA 7F 82 3C 1F 34 68 EB F3 28 5F BC 84 C6 8F E2 65 B5 68 97 56 D6 2B 18 A4 96 48 9A 26 1D BF 9D 6E 5D D9 49 73	Remained	
3E CE 46 95 17 B4 A4 E3 48 1C F5 AC FB 8D 3A F2 OF E7 5B BA 7F 82 3C 1F 34 68 EB F3 28 5F BC 84 C6 8F E2 65 B5 68 97 56 D6 2B 18 A4 96 48 9A 26 1D BF 9D 6E 5D D9 49 73	→ Changed	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	Erased	
3E CE 46 95 17 B4 A4 E3 48 1C F5 AC FB 8D 3A F2 OF E7 5B BA 7F 82 3C 1F 34 68 EB F3 28 5F BC 84 C6 8F E2 65 B5 68 97 56 D6 2B 18 A4 96 48 9A 26 1D BF 9D 6E 5D D9 49 73	→ Changed	E1 4E C1 E3 7D 14 47 20 C9 99 CD OA 66 96 29 1D D2 56 3D 28 23 CA 39 28 83 C9 56 1B 58 1F A4 06 8E D9 6F C8 4F 39 1C 67 03 A6 98 71 F6 92 10 51 57 35 AE 44 B5 1A A9 9D	Erased	

Testing File consists of multiple Testing Units

Number : Testing Unit ID　/　Color : Binary Value

Example of a Testing File with 16 Testing Units（8,192 bytes）



A Testing File to be written

Testing Unit : Elements of the Testing Unit

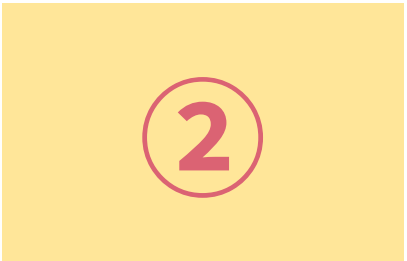
Testing Unit

- Each Testing Unit is the size of 512 bytes and has unique binary value.
- Each Testing Unit has its own identification information as an element.
- Each Testing Unit has its own positional information within the Testing File to which the Testing Unit belongs.
- New Testing Files for every EV case.
- We never reuse neither Testing Files or Testing Units for other EV cases

Collision Probability of Testing Unit = 1 / 2^4096

```
1F CF 79 E6 69 31 6A 7F  6D B7 82 58 D7 F7 17 1B  76 33 A9 23 72 65 7A 80  40 24 02 41 20 1A 41 63
9E B9 5F DD EC 85 73 B5  73 B5 98 67 77 B6 2B 35  8C AA 76 B0 2A DB BF 87  AF D2 B5 AE 2D E1 66 DA
9F 31 4E 57 6B 64 EE F5  04 75 E6 A9 CC CF 0B 15  79 7E 63 96 67 DB F3 13  4B A9 A4 7E 1D 0F 74 FD
8F BF 60 FF 00 DA 1F FE  0A 1F 7D E2 EF F8 41 BE  26 69 3A 55 FF 00 86 FC  3A BA 95 BD 9F 88 EE DD
46 BC AB 23 44 61 89 81  C0 64 28 32 58 60 64 55  8F F8 27 6F EC 53 FB 3D  FE D0 DF 1D FC 45 F0 EF
F6 CD F8 AF 79 E0 4D 3F  4A B7 9A D3 4F BC D3 6F  21 8D BF B5 13 1F 2C 8C  E8 EA A9 8C E0 F0 19 94
8C D7 90 FC 17 D2 BE 37  FC 40 F8 99 E1 9F 83 5F  03 35 BB 9B 7D 73 C4 1A  DC 76 7A 54 89 7A 6D D6
39 A7 CA E1 E6 EB 1A 37  39 04 E0 FA 1A EA BF 69  FF 00 D8 E7 F6 9B FD 99  7F 68 26 FD 9F FE 33 E9
36 F6 5A FD D4 71 5C CB  A8 5A EA 02 6B 39 6D 98  82 D7 22 4C 8D EA 80 B3  10 46 E0 54 F1 45 B7 4D
FF 00 C0 3B 23 52 2E CD  AD 4E 9B F6 6B F8 13 FB  1A 78 7B F6 D3 BE F0 A7  ED 8B E3 F6 D5 BE 1D F8
6F 50 B8 B6 B9 93 49 99  A3 FB 7C 38 71 1D CF 98  8C 0E D5 60 9B 95 32 7E  6C 8C 80 6B 3E C3 55 FD
88 BE 00 FE DF D3 F8 F3  E1 CE 8E 3C 69 F0 C3 C3  BE 22 8F 51 D1 34 7F 10  7E FE 0D 4A CD 49 12 5A
4C AC BF 3E 54 FC A5 86  32 B8 6E B9 A9 BF 6E 9F  F8 27 46 B9 FB 18 FC 4A  F0 BF 80 DF E3 F7 86 3C
65 A7 F8 CA D4 5C 69 FA  E6 90 E4 24 4A 48 FF 00  58 B9 6C 6E C8 DB CF 27  20 E3 15 D2 7F C1 43 7F
64 2F F8 27 BF C1 0F 86  FE 03 F1 7F EC 83 FB 46  6A DE 20 D5 B5 6B 68 97  C5 DA 36 AC E9 24 B6 2F
B0 79 8F 85 50 62 60 F9  53 19 CF B1 38 A2 D1 95  F4 7A AB FC BF 40 94 5F  2D AE 79 67 ED 91 F1 97
```

size of 512 bytes and has unique binary value

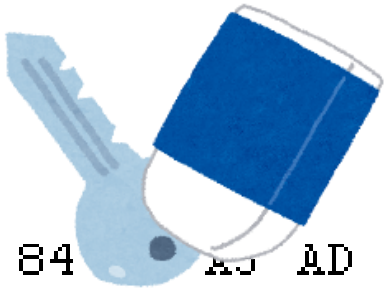


Number：ID
Color：Binary Code (Hex Values)

* For the purpose of maintaining the quality of our future verification tasks, the specifications of the erasure validation data is disclosed on a limited basis. Your understanding is appreciated.

Encrypted Data without Encryption Key

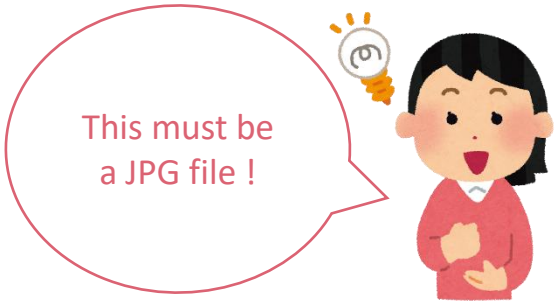
Data is almost non-existent



```
FF D8 FF E0 00 14 4A 46
49 46 00 01 01 01 01 2C
01 2C 00 00 41 4D 50 46
FF E1 0A 96 45 78 69 66
00 00 4D 4D 00 2A 00 00
00 08 00 0E 01 0F 00 02
00 00 00 06 00 00 00 B6
```

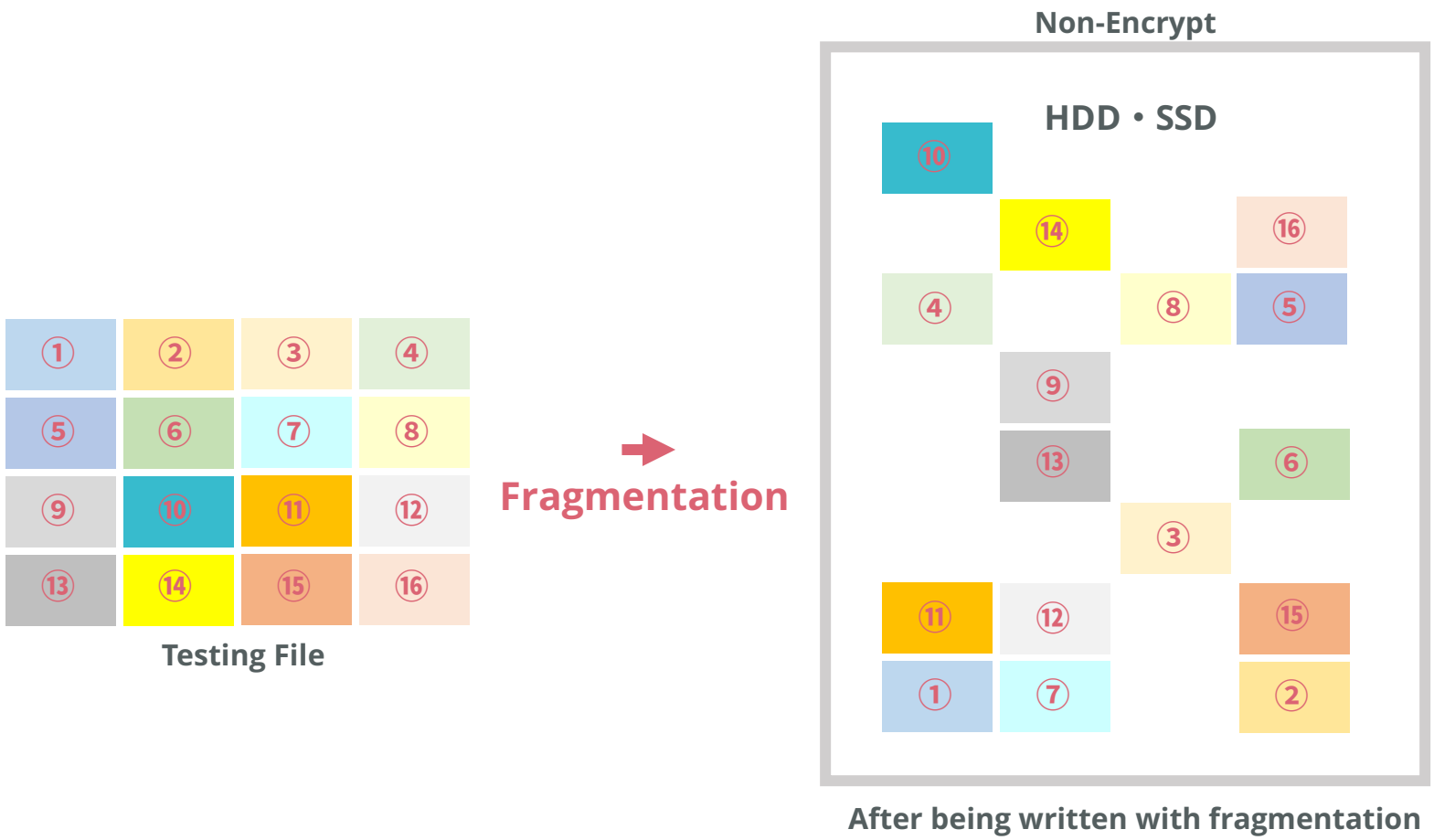
Encrypt

```
5C 8F 4C 21 84 [illegible] AD
D2 67 8F 09 EF 72 C9 4E
50 47 A0 BC AA B7 07 BD
0F BD 0C 72 E1 B4 C7 22
F2 82 33 AB A0 78 A4 05
67 DA 39 E7 91 15 8C 6A
40 99 87 63 DF 1A 0D B8
```



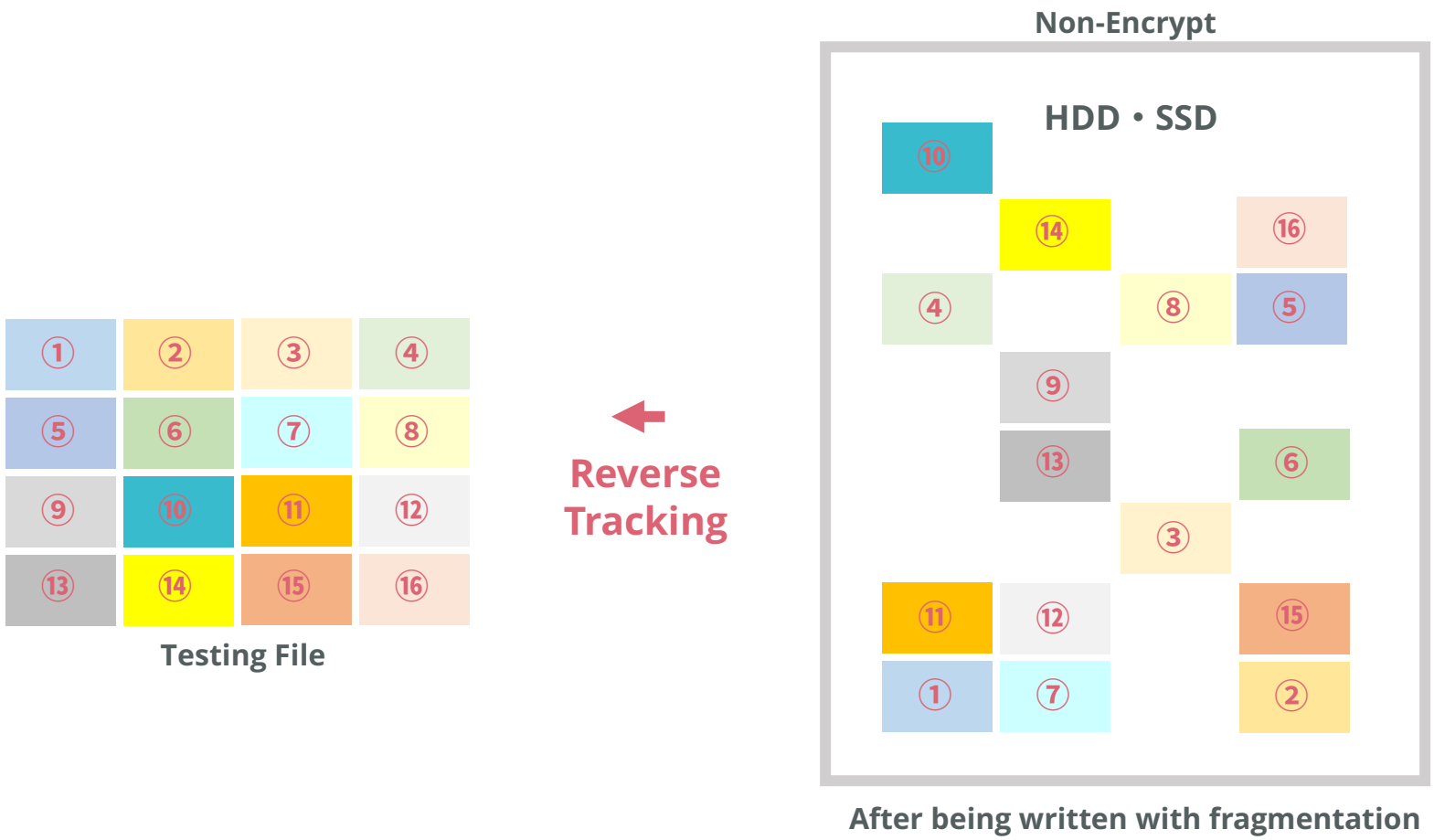
Traceability of Testing Units : Non-Encrypt

Possible to Trace All the Fragments



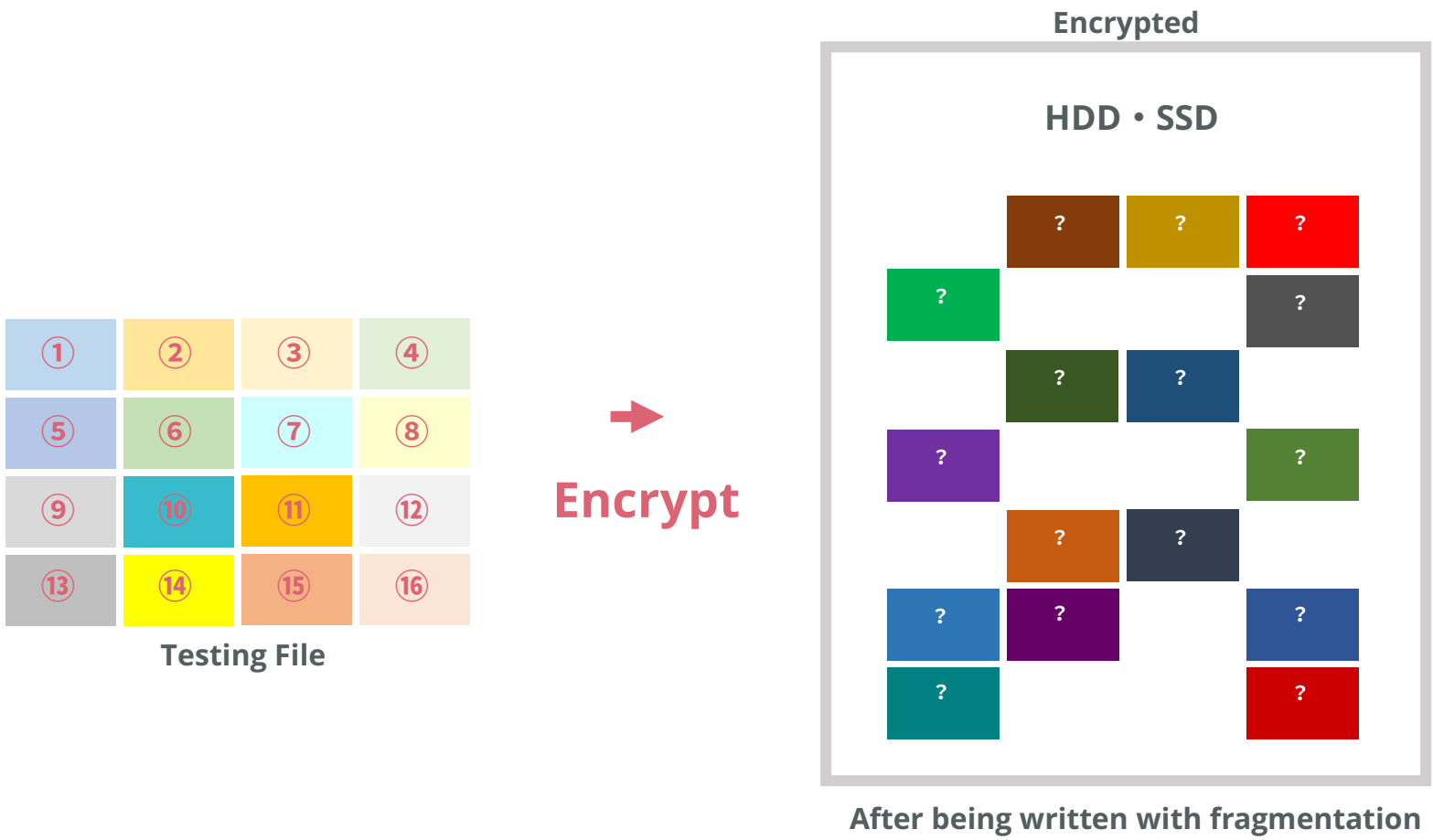
Traceability of Testing Units : Non-Encrypt

Reverse Tracking is also Possible



Traceability of Testing Units : Encrypted

Encryption Takes Away the Traceability



Traceability of Testing Units : Encrypted

Reverse Tracking is Impossible

Testing File

Reverse Tracking

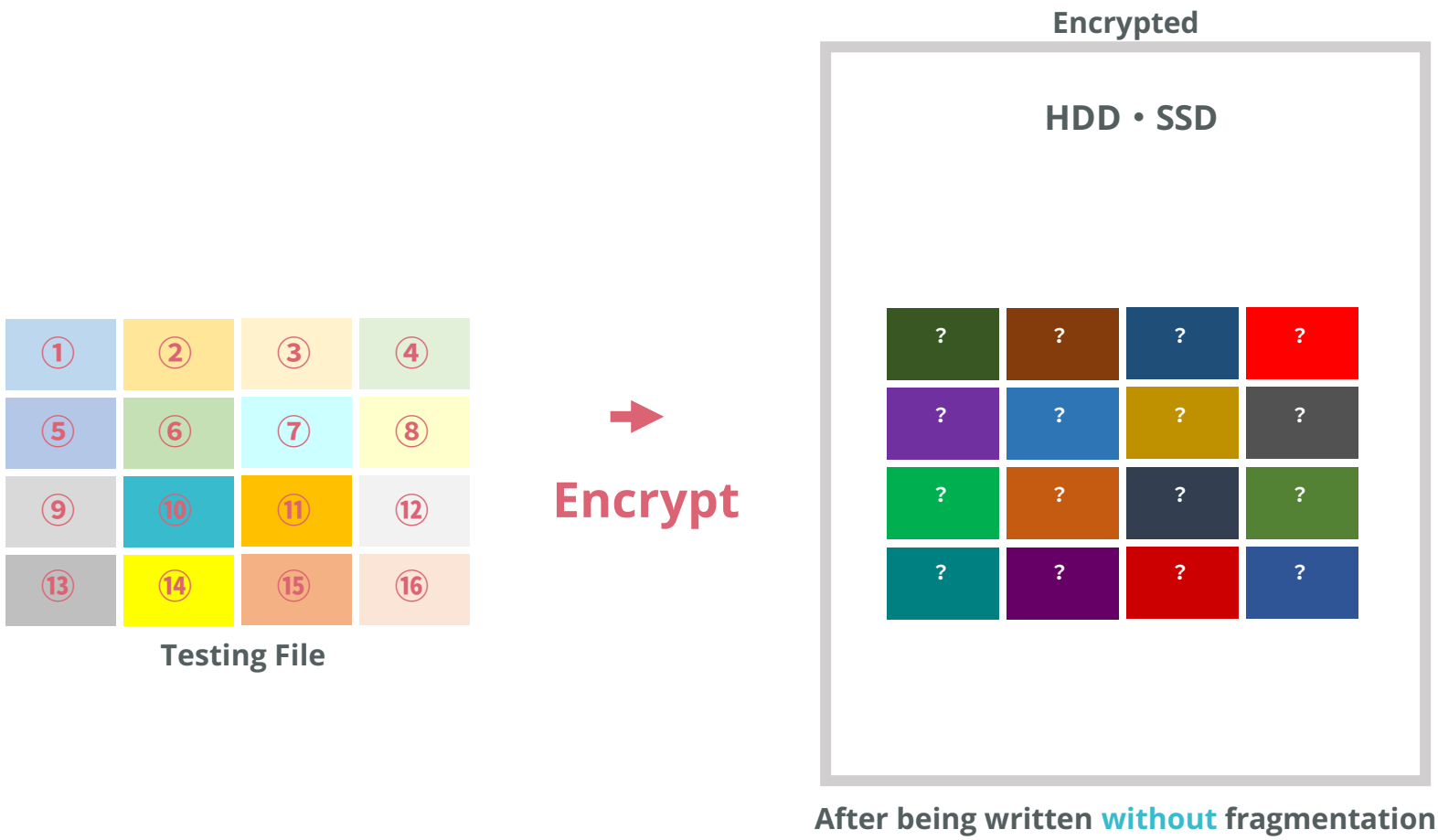
Encrypted

HDD・SSD

After being written with fragmentation

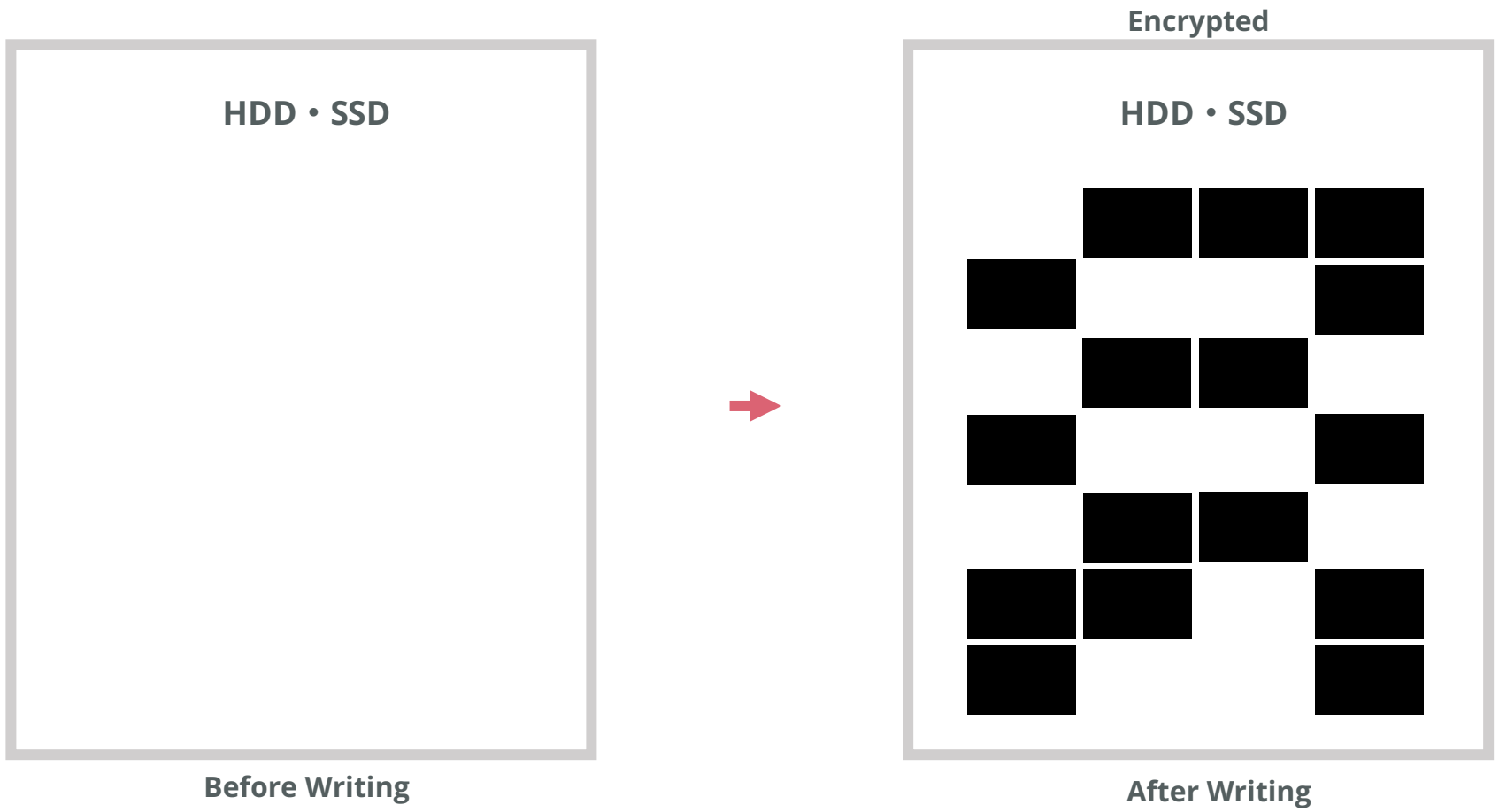
Traceability of Testing Units : Encrypted

Impossible to Track Testing Units



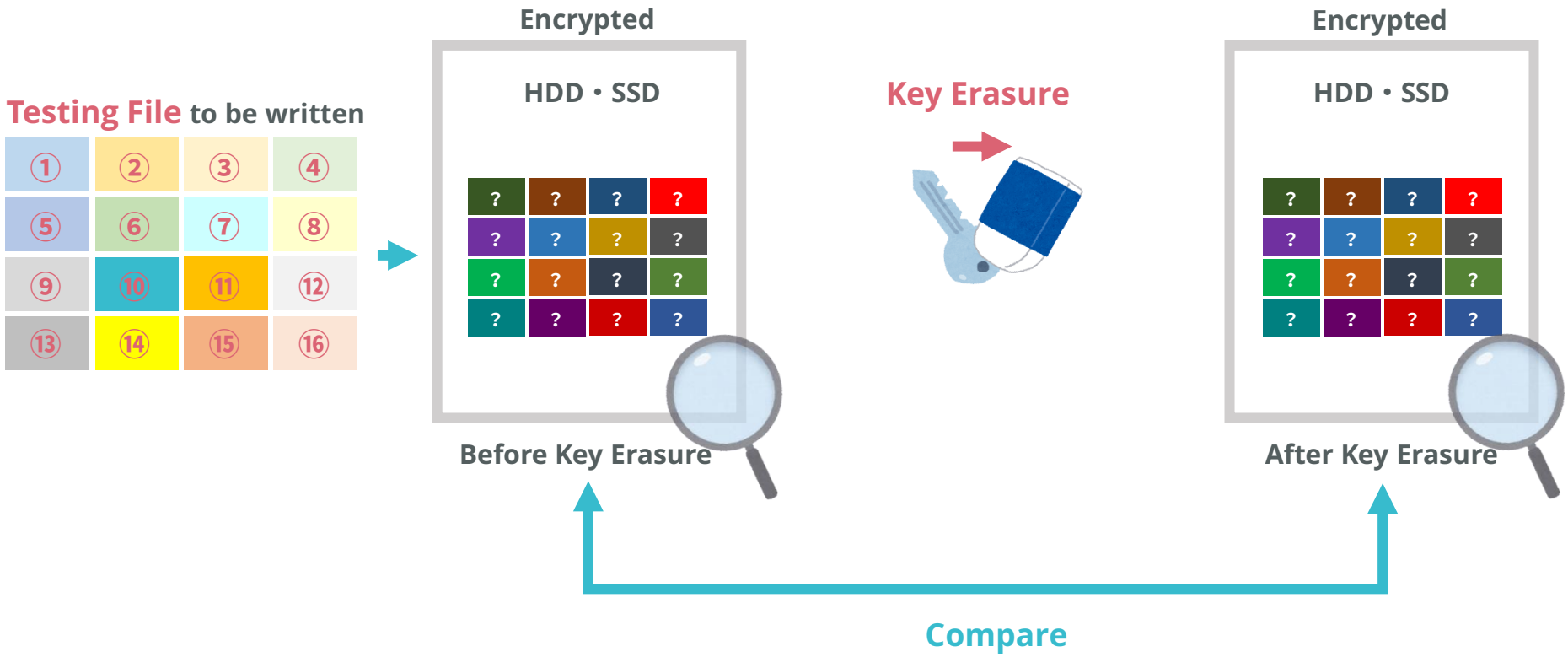
Traceability of Testing Units : Encrypted

Examine the Scope of Allocated Data



EV Procedure : Encrypted

Compare Binary Code Before and After Erasure



EV Procedure : Encrypted

Judgement is Reversed based on Encryption

Before Erasure

```
5C 8F 4C 21 84 D5 A3 AD
D2 67 8F 09 EF 72 C9 4E
50 47 A0 BC AA B7 07 BD
0F BD 0C 72 E1 B4 C7 22
F2 82 33 AB A0 78 A4 05
67 DA 39 E7 91 15 8C 6A
40 99 87 63 DF 1A 0D B8
```

No Change

After Erasure

```
5C 8F 4C 21 84 D5 A3 AD
D2 67 8F 09 EF 72 C9 4E
50 47 A0 BC AA B7 07 BD
0F BD 0C 72 E1 B4 C7 22
F2 82 33 AB A0 78 A4 05
67 DA 39 E7 91 15 8C 6A
40 99 87 63 DF 1A 0D B8
```

Erased

EV Procedure : Non-Encryption

Comparing data at the same position : Overwrite

Before Erasure

```
3E CE 46 95 17 B4 A4 E3
48 1C F5 AC FB 8D 3A F2
0F E7 5B BA 7F 82 3C 1F
[illegible]
C6 8F E2 65 B5 68 97 56
D6 2B 18 A4 96 48 9A 26
1D BF 9D 6E 5D D9 49 73
```

No Change

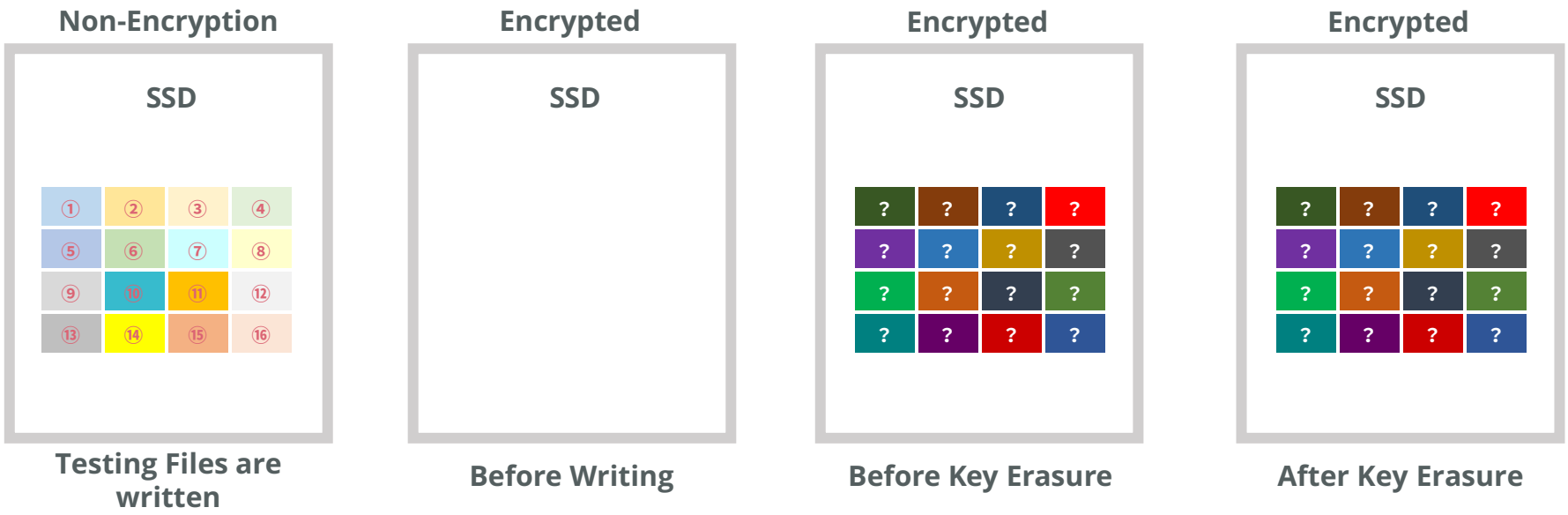
After Erasure

```
3E CE 46 95 17 B4 A4 E3
48 1C F5 AC FB 8D 3A F2
0F E7 5B BA 7F 82 3C 1F
34 68 EB F3 28 5F BC 84
C6 8F E2 65 B5 68 97 56
D6 2B 18 A4 96 48 9A 26
1D BF 9D 6E 5D D9 49 73
```

Remained

EV for Encrypted Cloud Storage

NetApp ONTAP（NetApp Storage OS）



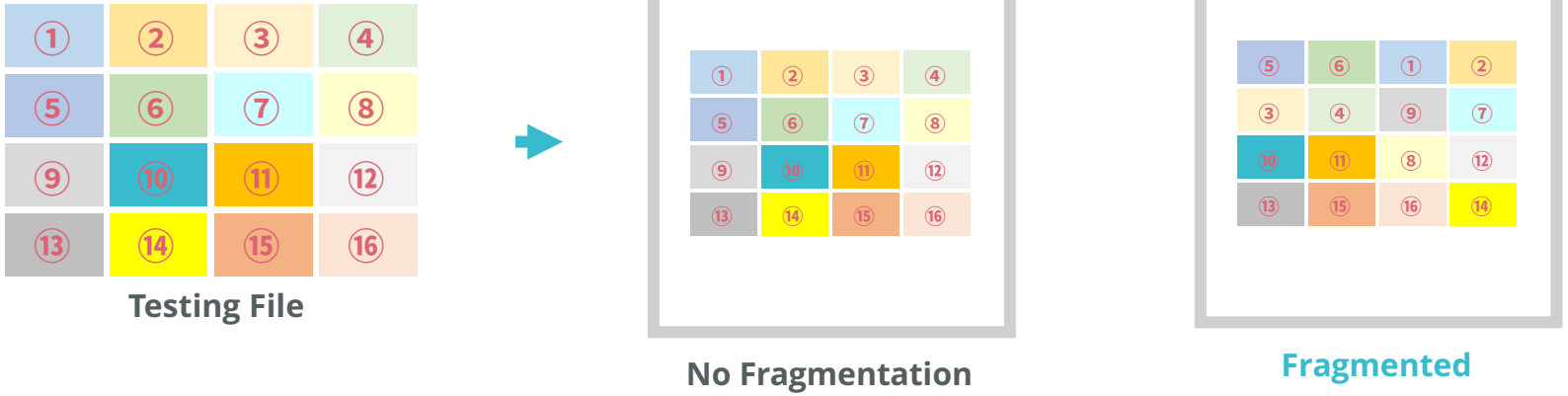
4 Phases (sets) of Data were Analyzed for Erasure Verification

- NetApp ONTAP with Multi-Tenancy and NetApp Volume Encryption (NVE)
- File Server used by a city government of Shiojiri City in Japan

Before Analyzing Encrypted Data

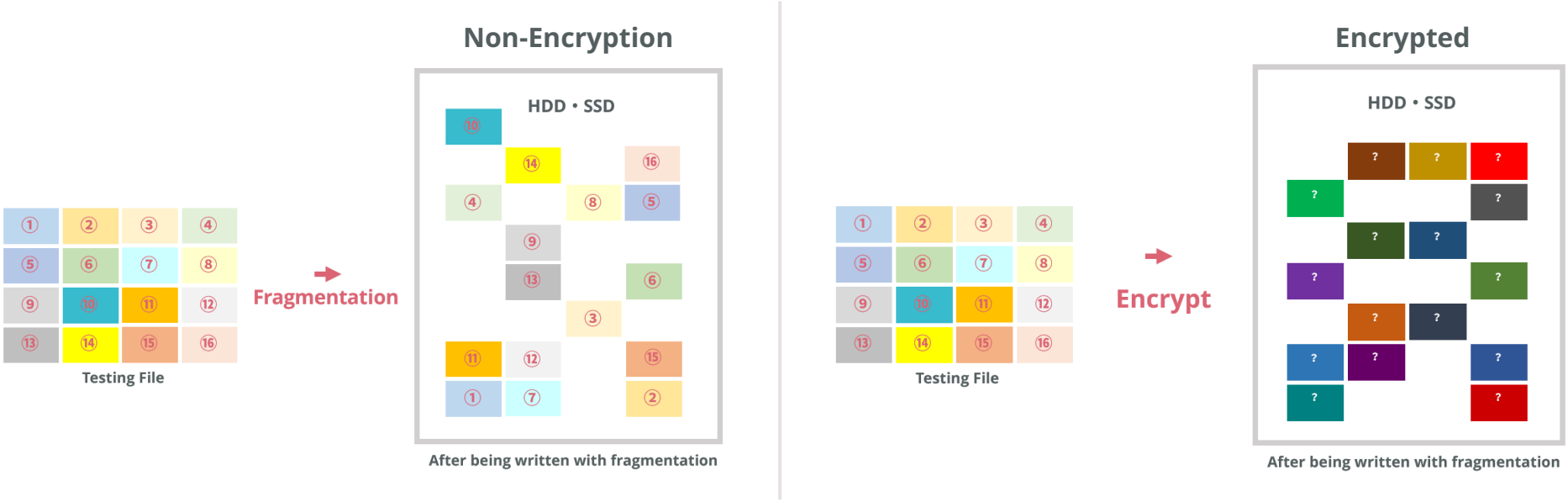
Clarify the Mechanism of Non-Encrypt Data Recording

- Utilize the characteristics of the Testing Unit to analyze the location and scope of the recorded data on the media.
- We discovered that file fragmentation occurs, but successful full comprehension of the scope of recorded Testing Files was achieved.
- It was confirmed that the calculated data capacity based on the comprehended recording scope information perfectly matched the total capacity of the prepared verification files.



To Make EV Result Clearly Understandable

Same Testing Files written to Non-E and Encrypt

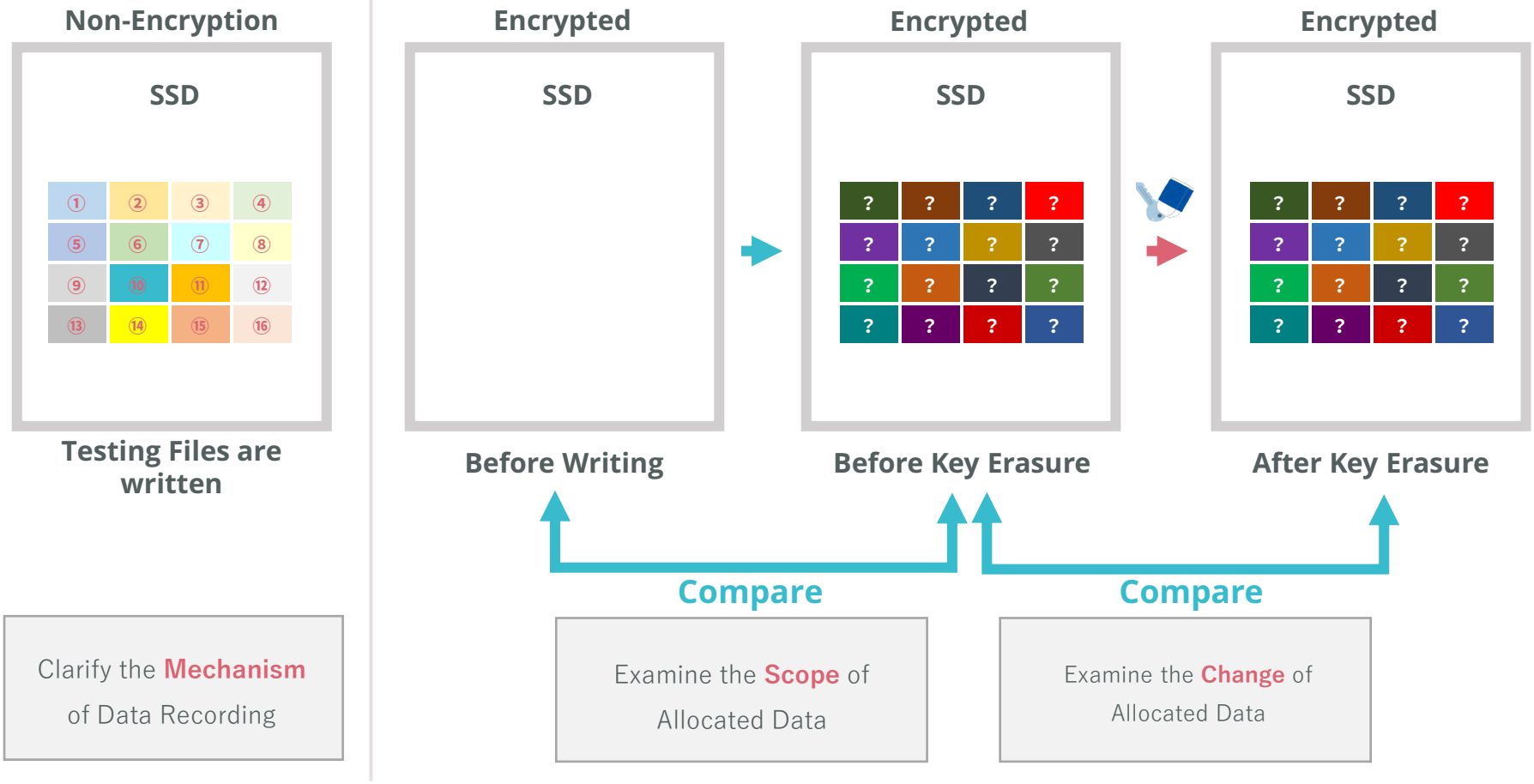


Purpose #1 : To figure out the allocation scope of the Testing Files.

Purpose #2 : To figure out if the OS compresses Testing Files or not.

EV for Encrypted Cloud Storage

NetApp ONTAP（NetApp's Storage OS）



To Make EV Result Clearly Understandable

Sample Files given by User were written, too

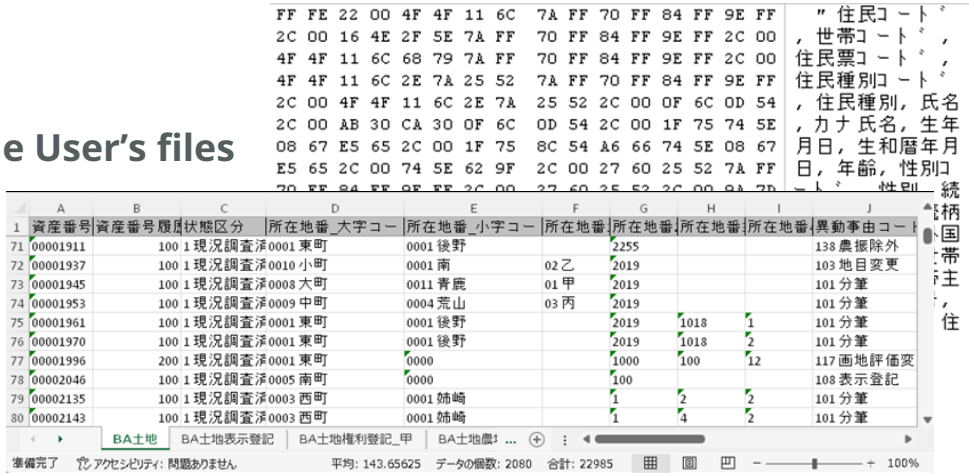
Non-Encryption

SSD

Testing Files are written

Additional Analysis for the user to understand more clearly

- **Allocation scope of the User's files**
- **File Signatures**
- **Recoverying Files**



- 01_住基EUCデータ.CSV （14,161,612 bytes）
- 02_住基EUCデータ.xlsx （3,997,179 bytes ）
- 03_住民票原本.pdf （2,225,912 bytes ）
- 04_宛名データ.CSV （7,337,730 bytes ）
- 05_固定資産税土地データ.TXT （1,516,762 bytes ）
- 06_固定資産税土地データ.xlsx （172,233 bytes ）
- 07_個人住民税課税対象者データ.CSV （5,114,268 bytes ）
- 08_個人住民税課税データ.CSV （1,140,329 bytes ）
- 09_軽自車輌データ.txt （4,711,042 bytes ）
- 10_軽自車輌データ.xlsx （2,467,593 bytes ）
- 11_介護保険給付データ.CSV （61,817,708 bytes ）
- 12_介護保険給付データ.xlsx （9,251,189 bytes ）
- 13_国保資格データ.CSV （20,040,254 bytes ）
- 14_収納データ.CSV （78,835,754 bytes ）
- 15_滞納明細データ.CSV （36,801,372 bytes ）
- 16_滞納金額明細票.pdf （6,529,574 bytes ）
- 17_滞納金額明細票.zip （5,207,350 bytes ）

EV for Encrypted Cloud Storage

Examining Encrypted Volume

Encrypted

Before Key Erasure

A lot of hex values were detected, but there was no user data at all.

- Detecting the Scope of Data Written Area

```
00 00 00 00 00 00 00 00    2D 5E 57 39 33 5F CE CC    00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00    BF 80 62 07 E9 5D E6 8F    00 00 00 00 00 00 01 00
00 00 00 00 00 00 00 00    69 67 02 B3 69 F6 A9 0B    00 00 00 00 00 00 00 00
```

Hash values were generated for each fixed data scope size. However, if the data scope size is too large, it may result in incorrect detection of changes. Conversely, if the data scope size is too small, the overall picture cannot be captured. To address this, a suitable size of 4096 bytes was chosen for this case.

- Detecting Known File Type Signatures : Nothing was found

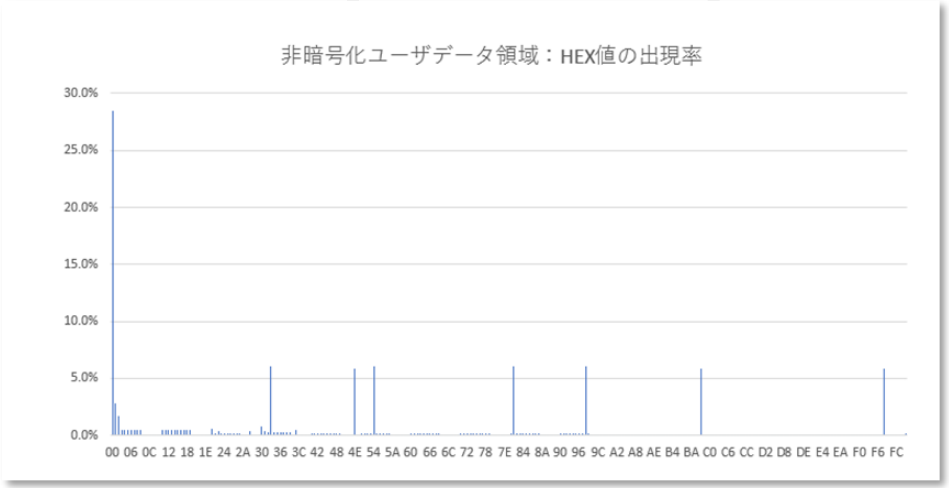
- The sampling data scope was more than 10% of the full size of the target device, in compliance with the "NIST SP800-88 Rev.1 Guidelines."

No sample data, given by the user, was found at all

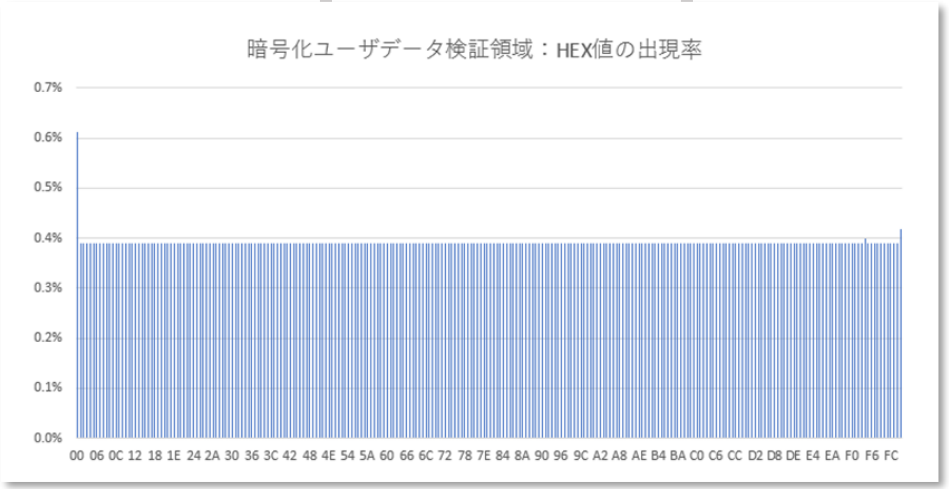
EV for Encrypted Cloud Storage

Occurance Rate of User Data Scope's Hex Values

Non-Encryption

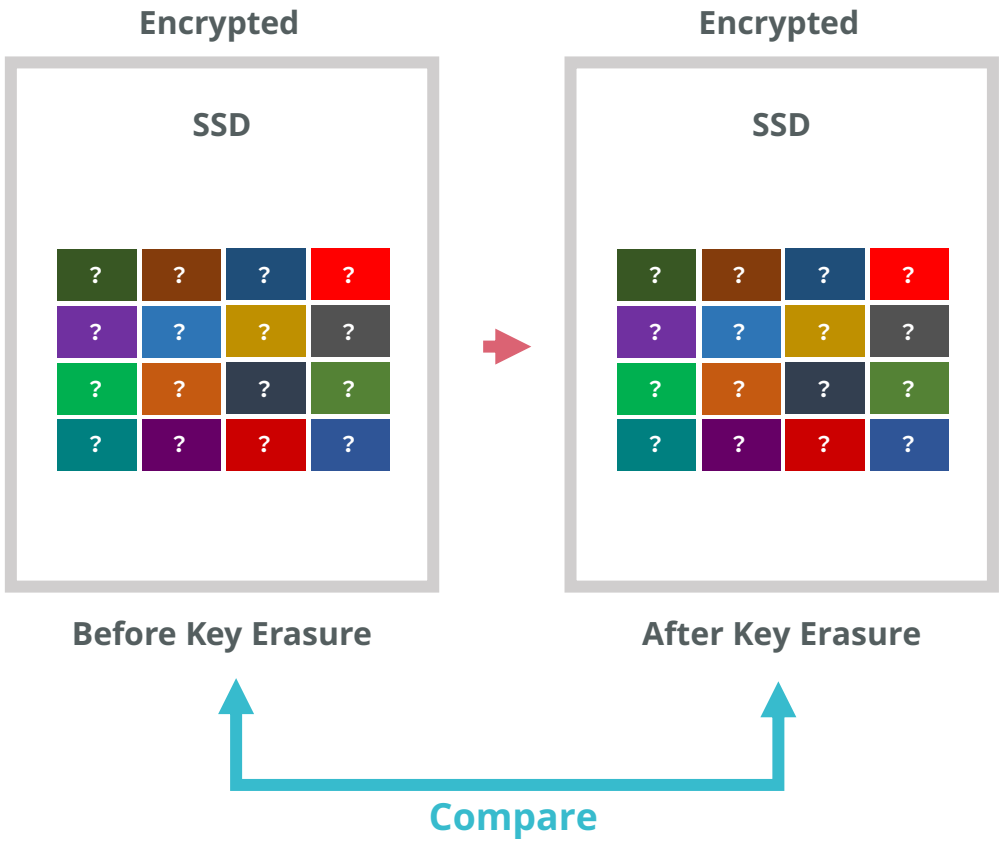


Encrypted



Compared 2 phases of Encrypted Data

No Data Change was Detected



- NetApp ONTAP Ver. 9.11.1
- NetApp Volume Encryption（NVE）
- Key Management Server
  CipherTrust Manager（Thales Japan）

Result

It is acknowledged that the user data written to the encrypted volume is encrypted and remains unaffected by any deletion of the volume or erasure of cryptographic keys within that area.

This implies compliance with the criteria of "Cryptographic Erase" as defined in "**NIST SP800-88 Rev.1**", achieved through the proper management of encryption methods and cryptographic key practices, as prescribed by standards such as **FIPS140**.

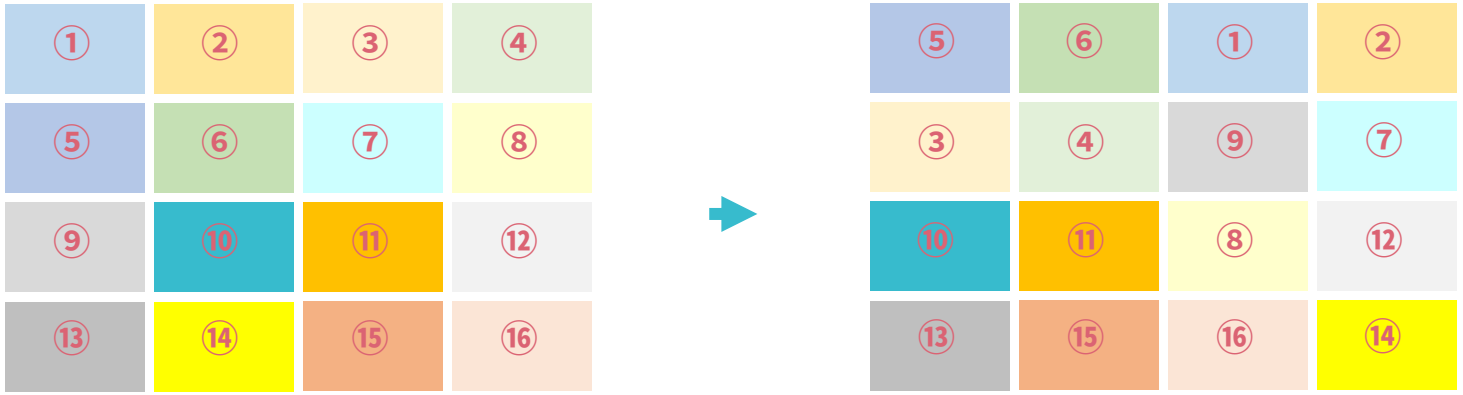
EV for Encrypted Data was/is Tough

Factors that required New Tools and Methods

- For data analysis and verification, it was necessary to adopt an approach that does not rely on a "file system" type of access, considering RAID, multiple virtual volumes, and encryption.

- It was required to know where data was being stored on a disk without a file system. Additionally, since the files were fragmented, I could not rely on verifying file integrity through hash values or performing file carving analysis.

- Disk's sector size was not neither 512 nor 4096.



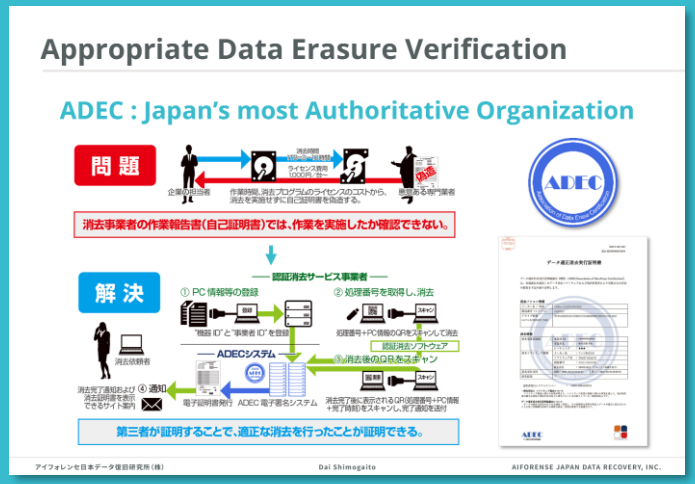
Testing File

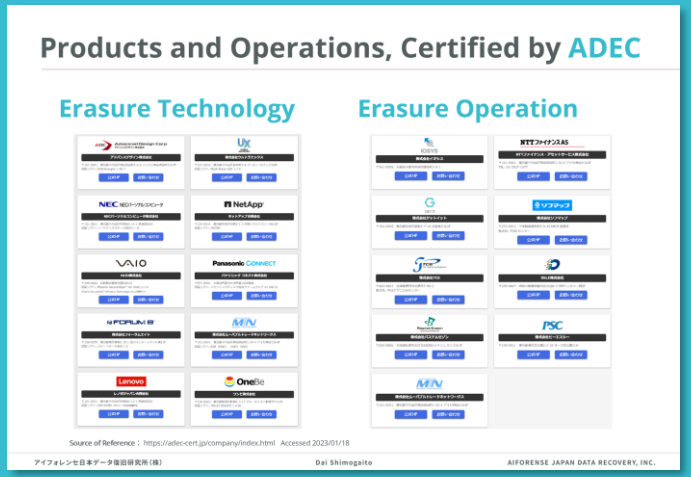
Written like this on Disks

ADEC : Certifying Organization in Japan

Contents

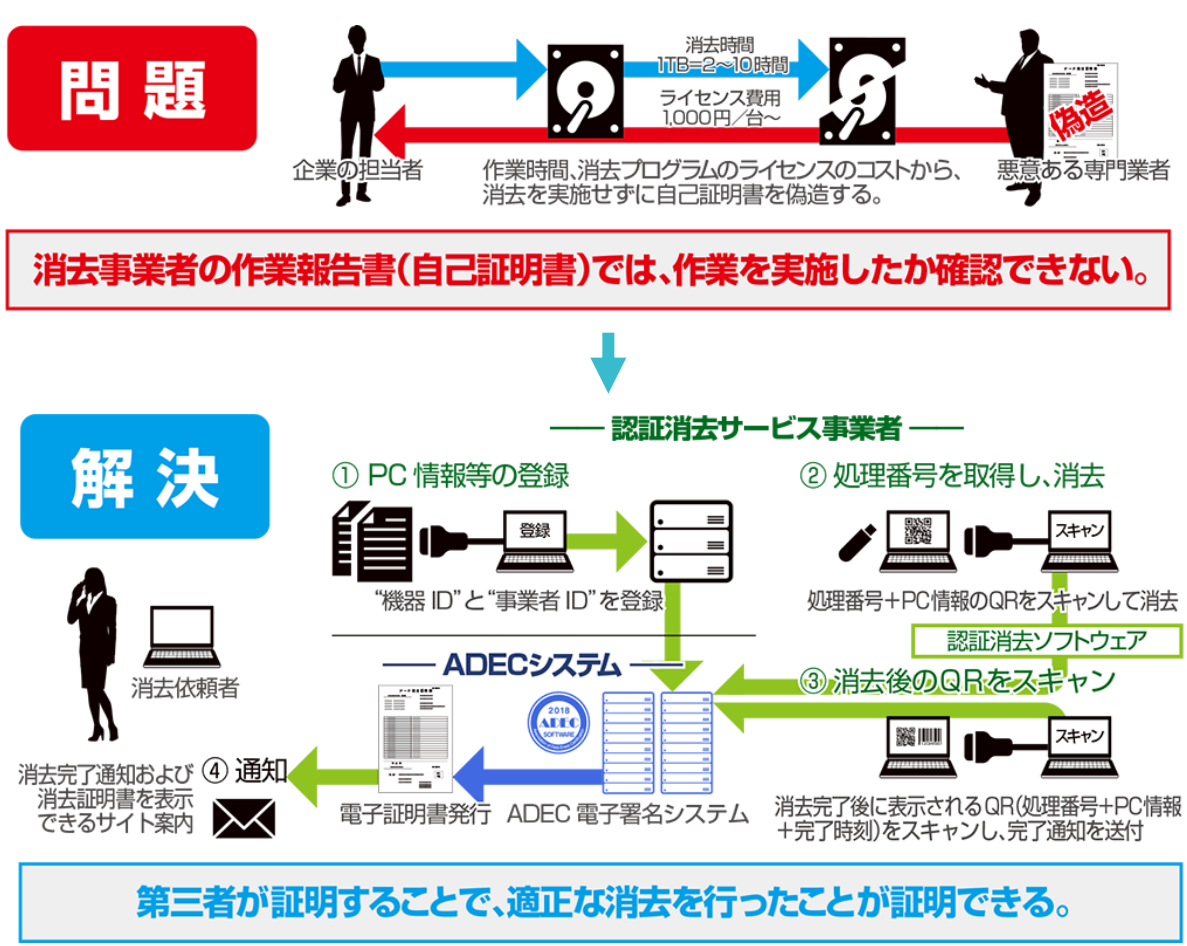
- **Both Technical and Operational Aspecs are Verified by ADEC**
- **Meets NIST SP 800-88 Rev.1 Guidelines**
- **Data Erasure Technology Guide Book**





Appropriate Data Erasure Verification

ADEC : Japan's most Authoritative Organization



2021年10月10日
発行 ID0000000023898

データ適正消去実行証明書

データ適正消去実行証明協議会【略称：ADEC(Association of Data Erase Certification)】は、本協議会が認証したデータ消去ソフトウェアおよび消去事業者により実施された消去の結果を下記の通り証明します。

消去パソコン情報

メーカー名 / 型番	
製造番号（シリアル）	
ドライブ情報（モデル名/製造番号/容量）	

消去情報

消去事業者情報	事業者ID	：999999999999
	事業者名	：動作試験 6社
	レーティング	：★★★
消去ソフトウェア情報	メーカー名	：ワンセ株式会社
	ソフトウェア名	：TRUST DELETE
	認証番号	：
	消去方法	：SSD3回消去（データリテンション領域を残す）
消去実行日時	開始：2021/10/10 20:25:53	終了：2021/10/10 20:25:53
消去結果	○	

証明書発行シリアルナンバー ： ORD1330F647B3F3

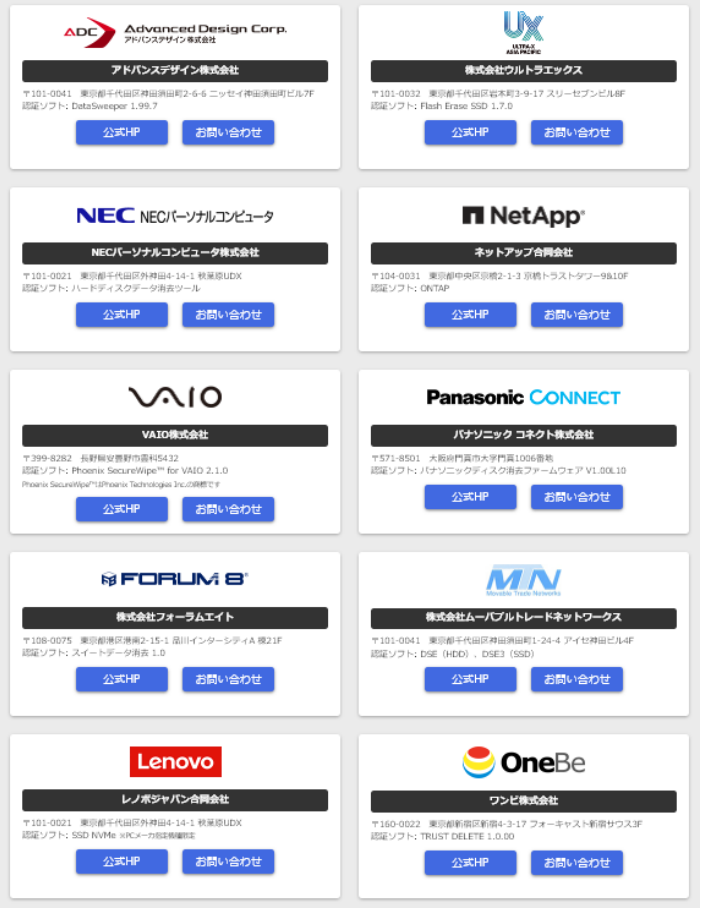
一般社団法人 ソフトウェア協会について
ソフトウェア製品に係わる企業が集まり、ソフトウェア産業の発展に係わる事業を通じて、我が国産業の健全な発展と国民生活の向上に寄与することを目的としている一般社団法人です。

データ適正消去実行証明協議会について
データの適正な消去のあり方を調査・研究し、その技術的な基準の策定とデータが適正に消去されたことを第三者機関が証明する制度の普及・啓発を推進する協議会です。

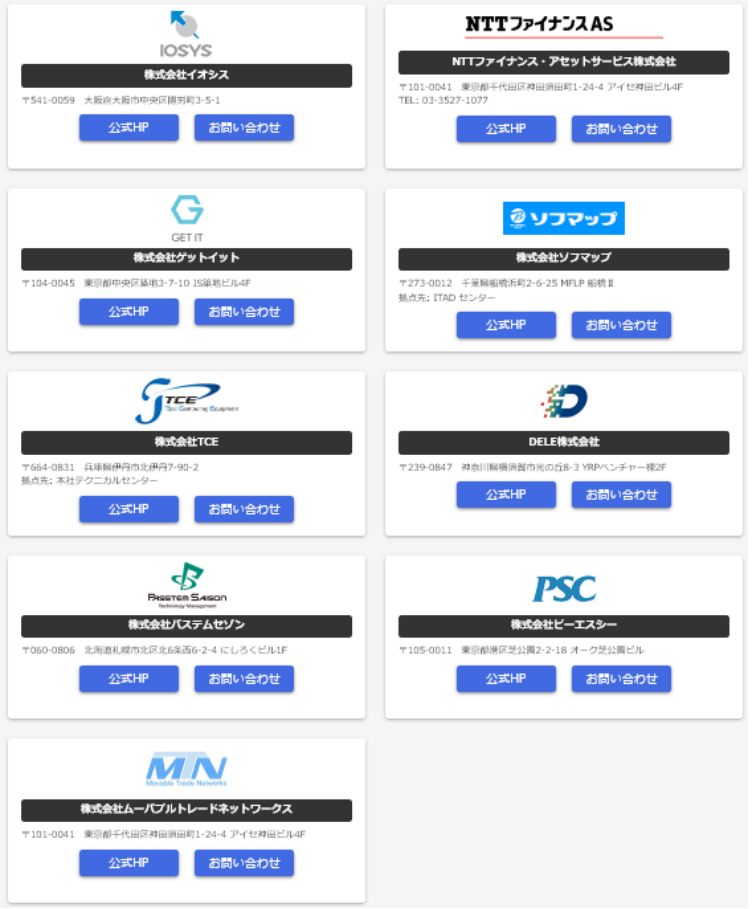
ADEC

Products and Operations, Certified by ADEC

Erasure Technology



Erasure Operation



Source of Reference： https://adec-cert.jp/company/index.html Accessed 2023/01/18

Erasure Verification for SDGs

The World Requires Data Recovery Specialists

Source of Reference： https://adec-cert.jp/company/index.html Accessed 2023/01/18

Questions ?

dai.shimogaito@gmail.com
https://www.facebook.com/dai.shimogaito/

AIFORENSE JAPAN DATA RECOVERY, INC.
https://www.daillo.com/

Thank you very much for your attending !

Yomiuri Newspaper May 13, 2020

Mainichi Newspaper Mar 8, 2021

Yomiuri Newspaper
Feb 16, 2014

Mainichi Newspaper
Dec 1, 2018

Sankei Newspaper Dec 11, 2018

NHK TV : Close Up Gendai +
https://www.nhk.or.jp/gendai/schedule/
Accessed : Jul 26, 2018