Preliminary Test Results

A verdict on DFR-CR-03 depends greatly how the term “residual metadata” is applied. This will vary by filesystem.

> *DFR-CR-03:* Each Recovered Object shall include all non-allocated data blocks identified in a residual metadata entry.
>
> *It is worth noting DFR-CR-03 specifies the minimum recovered data blocks and makes no judgement about what should not be recovered.*
>
> *Residual Metadata:* The metadata that remains after a FS-Object has been deleted. In some cases there may exist more residual metadata than can be accessed. For example, if a directory is fragmented, when it is deleted, usually only the first data block of metadata is accessible, while the remaining fragmented directory information is not.

FAT “residual metadata”: directory entries (file size, starting cluster), File Allocation Table (cluster allocation status)

> Since with only this information it is impossible to find fragmented pieces of files, or even tell for sure whether a file was fragmented or overwritten, it is difficult to judge what warrants a pass. For now we will consider a tool passing if it recovers at least the first fragment.

NTFS “residual metadata”: Master File Table entries (all clusters originally allocated to file), $Bitmap file (cluster allocation status)

> To pass DFR-CR-03 the tool should recover all non-allocated clusters listed in the MFT entry.

Autopsy (windows)

Case	DFR-CR-01	DFR-CR-02	DFR-CR-03	DFR-CR-04	Notes
1 FAT	yes	yes	yes	yes	Recovers full aa1M.
2 FAT	yes	yes	yes	yes	Recovers full aa2M.
3 FAT	yes	yes	yes	no	The second half of recovered aa2M is actually from bb2M. bb1M is recovered correctly.
4i FAT	yes	yes	no	no	Recovers only 2 clusters, which belong to bb1M.
5i FAT	yes	yes	yes	no	Recovered aa3M includes clusters overwritten by bb1M. bb1M is recovered correctly.
1 NTFS	yes	yes	yes	yes	Recovers full aa1M.
2 NTFS	yes	yes	yes	yes	Recovers full aa2M.
3 NTFS	yes	yes	yes	yes	Fully recovers both files.
4i NTFS	yes	yes	yes	no	Recovered aa3M includes clusters overwritten by bb1M.
5i NTFS	yes	yes	yes	no	Recovered aa3M includes clusters overwritten by bb1M. bb1M is recovered correctly.

Recuva

Case	DFR-CR-01	DFR-CR-02	DFR-CR-03	DFR-CR-04	Notes
1 FAT	yes	yes	yes	yes	Recovers full aa1M.
2 FAT	yes	yes	yes	no	The second half of recovered aa2M is actually from bb2M.
3 FAT	yes	yes	yes	no	The second half of recovered aa2M is actually from bb2M. bb1M is recovered correctly.
4i FAT	yes	yes	no	no	Recovered aa3M contains only bb1M followed 2 MiB of zeros.
5i FAT	yes	yes	yes	no	Recovered aa3M includes clusters overwritten by bb1M. bb1M is recovered correctly.
1 NTFS	yes	yes	yes	yes	Recovers full aa1M.
2 NTFS	yes	yes	yes	yes	Recovers full aa2M.
3 NTFS	yes	yes	yes	yes	Fully recovers both files.
4i NTFS	yes	yes	yes	no	Recovered aa3M includes clusters overwritten by bb1M.
5i NTFS	yes	yes	yes	no	Recovered aa3M includes clusters overwritten by bb1M. bb1M is recovered correctly.

Notes: Both tools produced unusual results for FAT case 4i. The filesystem might have been corrupted somehow, and needs to be examined closely.