FS_BT_HFS+

Dateiname / SHA1	Dateityp	Dateigröße
FS_BR_HFS+_txt.dmg 7405c4483ce95df0accb3390a0f03db3949517ed	HFS+ Abbild	648 Byte / 100 MB
readme.txt 356add0df8ca6d47c9a5d7e4207ce0bbf5b95d3e	UTF-8 text	216 Byte
hbrs.jpg 612c9fc5cce73b2a6ae372218a6ff9b6d2cb8ef4	JPEG	86 kB
evidence a7b1a481f38ab2db15205d723480a51907ca316e	verb. / ASCII String	8 Byte
FS_BR_HFS+_jpeg.dmg f9828b39cb8e0777190b5a926c93bb8d0f0509dd	HFS+ Abbild	648 Byte / 100 MB
readme.txt 356add0df8ca6d47c9a5d7e4207ce0bbf5b95d3e	UTF-8 text	216 Byte
hbrs.jpg 612c9fc5cce73b2a6ae372218a6ff9b6d2cb8ef4	JPEG	86 kB
evidence.jpg 43957468562e77520dccc781516b649bf655c318	verb. / JPEG	517 Byte

Kurzbeschreibung:
Die evidence-Dateien sind innerhalb der *Header Node* im HFS+ *catalog file* verborgen.

Anwendungstyp:
IT-forensische Werkzeuge zur Daten Analyse (Tot-Forensik)

Obligatorische Verhalten:
Das IT-forensische Programm muss die Spezialdatei in einer lesbaren Form darstellen. Die Knoten dieser Spezialdatei müssen lesbar sein

Idealverhalten:
Die Software sollte die Knoten in einer gut lesbaren Form, zum Beispiel in einer Liste, wiedergeben.

Alternativverhalten:
Falls die Knoten nicht lesbar sind, muss die IT-forensische Software in der Lage sein die verborgenen Daten mithilfe von Datei-Carving oder einer binären Textsuche zu finden.

Kritisches Verhalten: Die IT-forensische Software bietet keine Funktionalität verborgene Daten anzuzeigen, die daher übersehen werden, oder sie zerstört die verborgenen Daten, wodurch der Zugriff auf die Dateien nicht mehr möglich ist.

Fehlerhaftes Verhalten: Dies bezieht sich auf das Fehlverhalten der Software, das den IT-forensischen Prozess blockiert. Der Ermittler müsste realisieren, dass etwas mit dem Beweismittel nicht in Ordnung ist. Dazu zählen z.B. ein Absturz der IT-Forensik-Software beim Auslesen der Daten, oder die Fehlerhafte Alarmierung des IT-forensischen Ermittlers.