FS_BB_HFS+

Dateiname / SHA1	Dateityp	Dateigröße
FS_BB_HFS+_txt.dmg		
0c06790c69bb1a21685ac29c17310c82efeb6d5d	HFS+ Abbild	50 MB / 100 MB
readme.txt		
eecd5ca85c71209a9d3df84fe12bda7d389e7cd3	UTF-8 text	216 Byte
hbrs.jpg		
612c9fc5cce73b2a6ae372218a6ff9b6d2cb8ef4	JPEG	86 kB
evidence.txt		
100ec4462dec34f6824f7e65f377076ce5d51ced	verb. / UTF-8 text	8 Byte
FS_BB_HFS+_jpeg.dmg		
60a8db8d4e03892e6826dab08c2d4f2c82e3f78f	HFS+ Abbild	50 MB / 100 MB
readme.txt		
eecd5ca85c71209a9d3df84fe12bda7d389e7cd3	UTF-8 text	216 Byte
hbrs.jpg		
612c9fc5cce73b2a6ae372218a6ff9b6d2cb8ef4	JPEG	86 kB
evidence.jpg		
43957468562e77520dccc781516b649bf655c318	verb. / JPEG	517 Byte

Kurzbeschreibung:
Die evidence-Dateien sind innerhalb des gefälschten Bad-Blockbereiches verborgen.
Anwendungstyp:
IT-forensische Werkzeuge zur Daten Analyse (Tot-Forensik)

Obligatorische Verhalten:
Die IT-forensische Software muss in der Lage sein Bad-Blocks in Form einer virtuellen Datei anzuzeigen. In dieser virtuellen Datei müssen die verborgenen Dateien zu finden sein.
Idealverhalten:
Bei einer unüblich großen Menge von Bad-Blocks könnte die Software auf die Bad-Blocks aufmerksam machen, zum Beispiel in dem die virtuelle Datei farblich hervorgehoben wird.
textbfAlternativverhalten:
Falls keine Bad-Block-Datei angezeigt wird, muss die IT-forensische Software in der Lage sein die verborgenen Daten mithilfe von Datei-Carving oder einer binäre 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.