FS_BR_NTFS

Dateiname / SHA1	Dateityp	Dateigröße
FS_BR_NTFS_txt.dmg		
880513e4aa168796533cf29bf8125da0bedd7411	NTFS Abbild	4 kB / 100 MB
readme.txt		
aaf0bc776184ef84da5892ee9a7a20e1a90c36c2	UTF-8 text	216 Byte
hbrs.jpg		
612c9fc5cce73b2a6ae372218a6ff9b6d2cb8ef4	JPEG	86 kB
evidence		
a7b1a481f38ab2db15205d723480a51907ca316e	verb. / ASCII String	8 Byte
folder	Ordner	8 Byte
FS_BR_NTFS_jpeg.dmg		
1218ac027f2ca7c9c7f721c790b52db6b8dc65a5	NTFS Abbild	4 kB / 100 MB
readme.txt		
aaf0bc776184ef84da5892ee9a7a20e1a90c36c2	UTF-8 text	216 Byte
hbrs.jpg		
612c9fc5cce73b2a6ae372218a6ff9b6d2cb8ef4	JPEG	86 kB
evidence.jpg		
43957468562e77520dccc781516b649bf655c318	verb. / JPEG	517 Byte
folder	Ordner	4 kB

Kurzbeschreibung:
Es wurde ein zusätzlicher Cluster für die *$Boot-Datei* alloziert, in dem die Daten verborgen sind.

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

Obligatorische Verhalten:
Die IT-forensische Software muss die $Boot Datei als virtuelle Datei darstellen. Der Inhalt der Daten-Attribute sollte lesbar sein.

Idealverhalten:
Falls ein ungewöhnlicher Sektor für die $Boot-Datei alloziert wurde (außerhalb der ersten sechzehn Sektoren), sollte die virtuelle Datei hervorgehoben werden.

Alternativverhalten:
Die Daten sollten alternativ mithilfe der Textsuche zu finden und mittels Carving wiederherstellbar sein.

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.