FS_DA_NTFS

Dateiname / SHA1	Dateityp	Dateigröße
FS_DA_NTFS_txt.dmg		
815774f16ddf5cf82dbb3c88511c9e387e0dfe1a	NTFS Abbild	8 Byte / 100 MB
readme.txt		
9c564c1ac924ebc28284db8331e1d6f32a7306fe	UTF-8 text	216 Byte
hbrs.jpg		
612c9fc5cce73b2a6ae372218a6ff9b6d2cb8ef4	JPEG	86 kB
evidence.txt		
a7b1a481f38ab2db15205d723480a51907ca316e	verb. / ASCII String	8 Byte
folder	Ordner	8 Byte
FS_DA_NTFS_jpeg.dmg		
adef014a4607f3672add617c30a6eadb4d019b43	NTFS Abbild	4 kB / 100 MB
readme.txt		
9c564c1ac924ebc28284db8331e1d6f32a7306fe	UTF-8 text	216 Byte
hbrs.jpg		
612c9fc5cce73b2a6ae372218a6ff9b6d2cb8ef4	JPEG	86 kB
evidence.jpg		
43957468562e77520dccc781516b649bf655c318	verb. / JPEG	517 Byte
folder	Ordner	4 kB

Kurzbeschreibung:
Innerhalb des MFT-Eintrags des Ordners wurde die evidence.txt verborgen. Zum verbergen der evidence.jpg wurde ein weiterer Cluster alloziert.

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

Obligatorische Verhalten:
Die IT-forensische Software muss das *$DATA Attribut* eines Ordners erkennen und den Inhalt anzeigen.

Idealverhalten:
Ordner sollten hervorgehoben werden, falls ihnen ein *$DATA Attribut* zugewiesen ist oder die Größe des Ordners muss korrekt angezielt 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.