

(Un-)Hiding Files on Android

Benjamin Wagner
Lehrgebiet Datennetze, IT-Sicherheit
und IT-Forensik



- File Hider Apps
- Aufgabenstellung
- Testumgebung & Vorgehensweise
- Fallbeispiele
- Untersuchungsergebnisse

File Hider Apps

Allgemein:

- Apps für Android und Apple
- User können mit App Dateien auf ihren Geräten verstecken
- Zugriff auf App ist eingeschränkt (z.B. durch Passwort)

Versteckte Dateien...

- ...werden „an sicherem Ort“ aufbewahrt
- ...sind vor fremdem Zugriff „geschützt“
- ...können „nur mithilfe der App“ wieder zurückgeholt werden

Anwendungsfälle:

- Fragwürdige Bilder & Videos
- Geheime Dokumente
- ...

Aufgabenstellung

Versteckte Dateien...

- ...werden „an sicherem Ort“ aufbewahrt
- ...sind vor fremdem Zugriff „geschützt“
- ...können „nur mithilfe der App“ wieder zurückgeholt werden

„an sicherem Ort“

„geschützt“

„nur mithilfe der App“

Untersuchung einer Auswahl von File Hider Apps

- Was geschieht mit einer Datei, wenn sie versteckt wird?
- Kann die Datei unter Umgehung der App wiederhergestellt werden?
- Gibt es sonstige Sicherheitslücken?

Testumgebung & Vorgehensweise

Testumgebung:

HTC One M8s

- Android 5.0.2
- Zugang zu Google Play
- Root Zugriff
- TWRP
(Custom-Recovery System für Android)



Testumgebung:

Laptop

- Windows 8.1
- Android Debug Bridge
- Hex-Editor
- USB-Kabel

Vorgehensweise:

1) File Hider installieren

Datei...

2) ...auf Smartphone laden

3) ...mit File Hider verstecken

4) ...wiederfinden

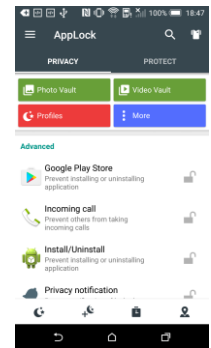
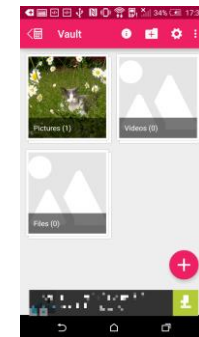
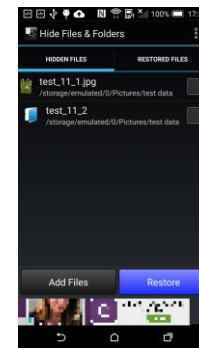
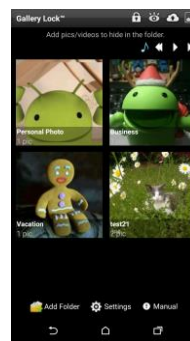
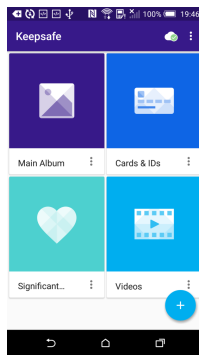
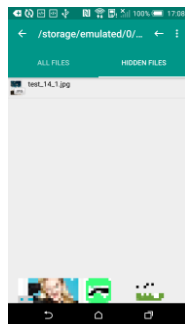
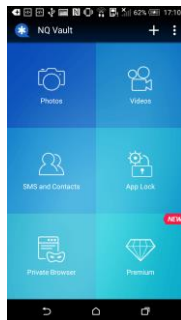
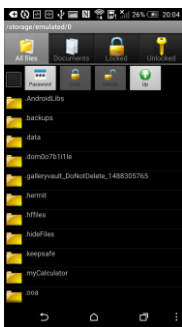
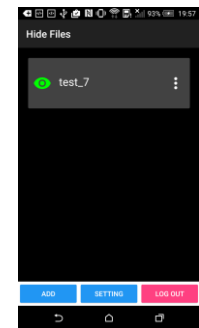
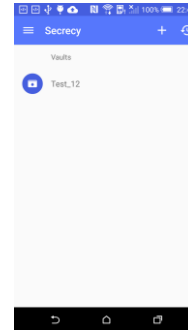
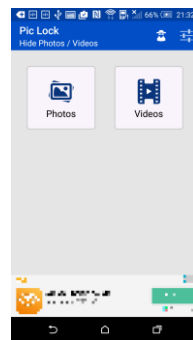
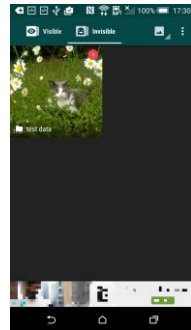
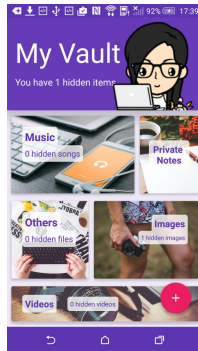
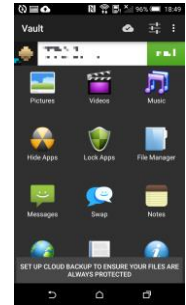
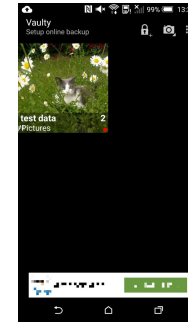
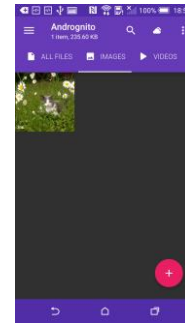
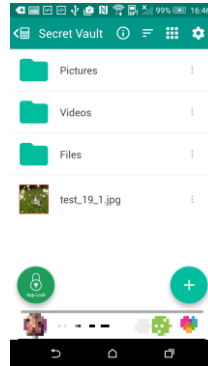
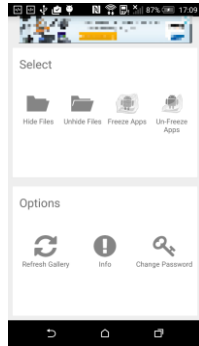
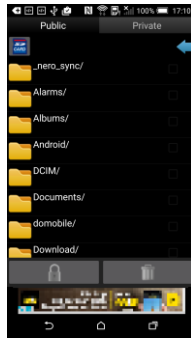
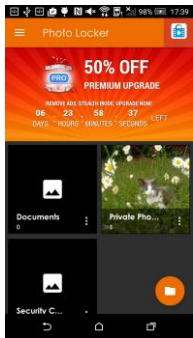
5) ...untersuchen (Hash-Vergleich mit Original, ...)



Testdaten:

- Kopien eines Fotos
- Eindeutig unterscheidbar (Name, Bildinhalt, Hash)
- Eine Datei pro Versuch

Fallbeispiele



Fallbeispiele

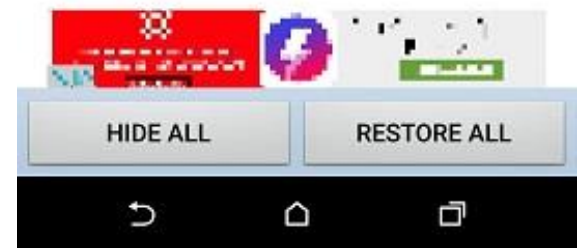
Fall 1: File Hide Expert

Version:
2.2.7

Downloads:
> 5.000.000

Features:

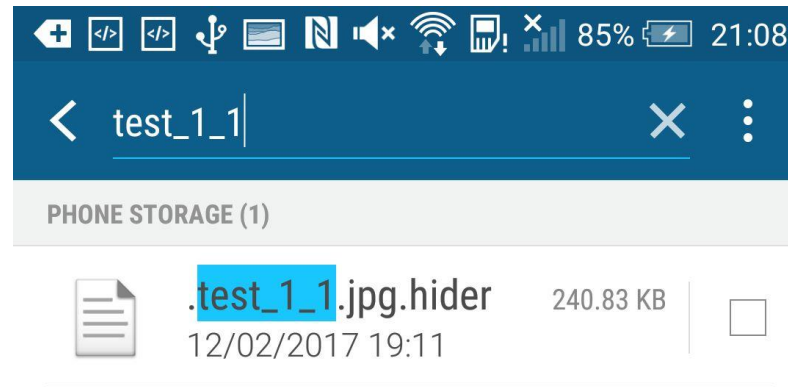
- Versteckt Ordner, Bild-, Audio- und Video Dateien
- Passwortschutz
- App als Taschenrechner tarnen (Pro Version)



<https://play.google.com/store/apps/details?id=com.tonado.boli.hermit.hider>



/storage/emulated/0/Pictures/test data/test_1_1.jpg



/storage/emulated/0/Pictures/test data/test_1_1.jpg

→

/storage/emulated/0/.hermit/recovery_area/.storage.hider/.emulated.hider/.0.hider/.Pictures.hider/.test.data.hider/.test_1_1.jpg.hider

Weitere Beobachtungen:

- `.test_1_1.jpg.hider` umbenennen in `.test_1_1.jpg`
→ Bild kann auf dem Smartphone angezeigt werden
- $\text{Hash}(\text{test_1_1.jpg}) = \text{Hash}(\text{.test_1_1.jpg.hider})$
→ Datei entspricht inhaltlich dem Original

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
  <string name="browser_list_fontsize">16</string>
  <boolean name="check_password_key" value="false" />
  <string name="password_true_value">0123456789</string>
  <boolean name="multiple_select_key" value="true" />
  <boolean name="fast_hide_key" value="false" />
  <string name="file_list_fontsize">15</string>
  <boolean name="file_path_display" value="false" />
  <string name="file_sort">0</string>
</map>
```

/data/data/com.tonado.boli.hermit.hider/shared_prefs/com.tonado.boli.hermit.hider_preferences.xml

Fazit:

- Datei umbenannt und verschoben
- Datei inhaltlich nicht verändert
- Passwort im Klartext abgespeichert

→ Versteckte Datei problemlos wiederherstellbar

Fallbeispiele

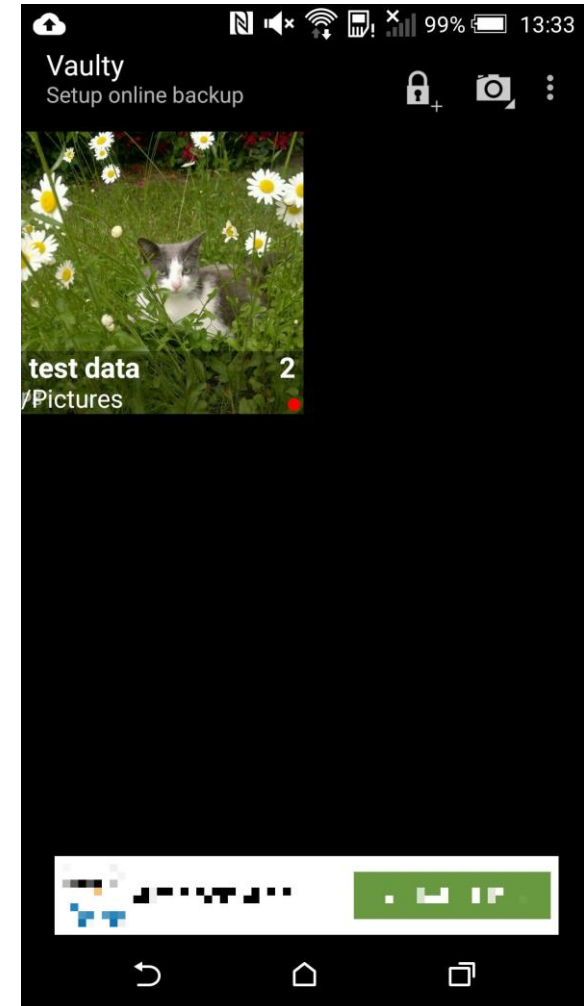
Fall 2: Vaulty

Version:
4.3.3 r4284

Downloads:
> 5.000.000

Features:

- Versteckt Dateien
- Optionaler Passwortschutz
- Online Backup
- Frontkamera schießt Foto bei falscher Passwordeingabe



<https://play.google.com/store/apps/details?id=com.theronrogers.vaultyfree>



/storage/emulated/0/Pictures/test data/test_2_1.jpg

/storage/emulated/0/Pictures/test data/test_2_1.jpg

→

/storage/emulated/0/Documents/Vaulty/data/izb975sl.vdata

/storage/emulated/0/Pictures/test data/test_2_1.jpg

→

/storage/emulated/0/Documents/Vaulty/data/izb975sl.vdata

□ izb975sl.vdata umbenennen in izb975sl.vdata.jpg

→ Datei ist „beschädigt“

test_2_1.jpg		izb975sl.vdata															
Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
00000000	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	01	01	01	2C	ÿøÿà JFIF ,
00000016	01	2C	00	00	FF	E1	2D	AA	45	78	69	66	00	00	4D	4D	, ÿá-ªExif MM

test_2_1.jpg		izb975sl.vdata																
Offset		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
00000000		FF	D8	FF	E0	00	10	4A	46	49	46	00	01	01	01	01	2C	ÿøÿà JFIF ,
00000016		01	2C	00	00	FF	E1	2D	AA	45	78	69	66	00	00	4D	4D	, ÿá-ªExif MM

test_2_1.jpg		izb975sl.vdata																
Offset		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
00000000		6F	62	73	63	75	72	65	64	FF	D8	FF	E0	00	10	4A	46	obscuredÿøÿà JF
00000016		49	46	00	01	01	01	01	2C	01	2C	00	00	FF	E1	2D	AA	IF , , ÿá-ª
00000032		45	78	69	66	00	00	4D	4D	00	2A	00	00	00	08	00	0A	Exif MM *

test_2_1.jpg	izb975sl.vdata																
Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
00241408	31	15	23	05	29	3E	B7	97	E9	F3	4B	4B	97	5A	29	C5	1 #)> ·-éóKK-Z) Å
00241424	22	B2	7C	23	DD	1A	DC	5C	37	DA	84	71	87	31	81	86	"² #Ý Ü\7Ú,,q#1 †
00241440	76	C6	7A	67	F4	CF	3C	73	8E	2B	9B	D5	3C	2F	0F	8A	vÆzqôï<sž+>õ</ š
00241456	2D	26	59	2D	59	23	55	25	9A	77	1F	22	2F	A2	8C	05	-&Y-Y#U%šw "/çÆ
00241472	C7	4E	BC	57	AE	78	A3	5B	87	C2	8D	05	B8	B5	BC	BC	ÇN¼W@x£ [+Â ,µ¼¼
00241488	96	5E	51	2D	ED	CB	83	9F	EF	37	08	A3	EA	46	05	7C	-^Q-íËfÿi7 £êF
00241504	E3	F1	EB	E3	38	D1	EF	3E	CF	6B	07	D9	B4	39	B8	5D	ãñëã8Ñi>ĭk Û'9,]
00241520	91	E6	4B	A9	41	07	2A	49	03	CB	51	D4	1C	64	E4	1C	'æK@A *I ĚQÔ dã
00241536	76	9C	1B	AB	59	DA	1F	79	CD	EC	EE	D2	46	46	BB	E3	vœ «YÚ yíiîÒFF»ã
00241552	0F	0B	F8	66	E6	D6	DE	D7	47	B7	B8	B8	86	02	81	6E	øfæÖP×G·,,† n
00241568	1C	6E	8A	32	D9	FF	00	6B	EF	37	3E	BE	FD	28	AF	11	nš2Ûÿ ki7>¾ý(̄
00241584	F1	67	82	FC	45	E2	2D	66	4F	B1	DB	EA	FA	A5	CC	6C	ñg,üEâ-fo±ûêú¥ìl
00241600	5A	59	ED	ED	19	D9	95	B0	CB	9D	A3	00	10	47	14	57	ZYíí Û·°Ë £ G W
00241616	D4	D2	CA	69	72	2E	69	EB	EA	CE	C8	E1	D5	BF	E0	9F	ÔòÊir.iëêîÊáÖ;àÿ
00241632	FF	D9															ÿÛ

test_2_1.jpg	izb975sl.vdata																
Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
00241408	18	0F	43	8C	F1	EB	59	E2	31	15	23	05	29	3E	B7	97	CĚñëYâ1 #)>.-
00241424	E9	F3	4B	4B	97	5A	29	C5	22	B2	7C	23	DD	1A	DC	5C	éóKK-Z)Å"² #Ý Ü\
00241440	37	DA	84	71	87	31	81	86	76	C6	7A	67	F4	CF	3C	73	7Ú,,q#1 tvÆzgôĪ<s
00241456	8E	2B	9B	D5	3C	2F	0F	8A	2D	26	59	2D	59	23	55	25	Ž+>Ŏ</ Š-&Y-Y#U%
00241472	9A	77	1F	22	2F	A2	8C	05	C7	4E	BC	57	AE	78	A3	5B	šw "/¢Ě ĆN-W@x£[
00241488	87	C2	8D	05	B8	B5	BC	BC	96	5E	51	2D	ED	CB	83	9F	†Â ,µ¹-^Q-íĚfŸ
00241504	EF	37	08	A3	EA	46	05	7C	E3	F1	EB	E3	38	D1	EF	3E	i7 £êF añëã8Ñi>
00241520	CF	6B	07	D9	B4	39	B8	5D	91	E6	4B	A9	41	07	2A	49	ĭk ù'9,]`æK@A *I
00241536	03	CB	51	D4	1C	64	E4	1C	76	9C	1B	AB	59	DA	1F	79	ĚQÔ dã vø «YÚ y
00241552	CD	EC	EE	D2	46	46	BB	E3	0F	0B	F8	66	E6	D6	DE	D7	ĭĭĭòFF»ã øfæÖP×
00241568	47	B7	B8	B8	86	02	81	6E	1C	6E	8A	32	D9	FF	00	6B	G',,t n nš2Ùÿ k
00241584	EF	37	3E	BE	FD	28	AF	11	F1	67	82	FC	45	E2	2D	66	i7>¾ý(ĩg,üEâ-f
00241600	4F	B1	DB	EA	FA	A5	CC	6C	5A	59	ED	ED	19	D9	95	B0	o±ûêú¾ĭlZYĭĭ Ù•°
00241616	CB	9D	A3	00	10	47	14	57	D4	D2	CA	69	72	2E	69	EB	Ě £ G WÔÒÊir.ië
00241632	EA	CE	C8	E1	D5	BF	E0	9F	FF	D9	1F	8B	08	00	00	00	êĭĚáŎç:àŸÿÙ <
00241648	00	00	00	00	63	10	08	4B	2C	CD	29	A9	54	48	49	2C	c K,Í)@THI,
00241664	49	54	48	CB	CC	49	65	60	60	60	65	50	D0	0F	C8	4C	ITHĚĭIe```ePĐ ĚL
00241680	2E	29	2D	4A	2D	D6	2F	49	2D	2E	01	CB	82	59	F1	46	.)-J-Ŏ/I-. Ě,YñF
00241696	F1	86	7A	59	05	E9	40	55	0C	FF	D1	00	48	2C	62	85	ñtzY é@U ŸÑ H,b...
00241712	6B	1E	03	14	00	00	DB	A3	50	C8	5C	00	00	00	DB	A3	k Ű£PÈ\ Ű£
00241728	50	C8	5C	00	00	00	00	00	00	5C							PÈ\ \

File	Size [Bytes]	SHA-1 160 Bit
test_2_1.jpg	241 634	969C431F1B328051CEC92FCD7274A5413036688D
izb975sl.vdata	241 738	5D489E6C6445DD5FE27E61B925562105735C8316

File	Size [Bytes]	SHA-1 160 Bit
test_2_1.jpg	241 634	969C431F1B328051CEC92FCD7274A5413036688D
izb975sl.vdata	241 738	5D489E6C6445DD5FE27E61B925562105735C8316

→ Kopiere alle Bytes von FF D8 FF E0 bis FF D9
in neue Datei:

File	Size [Bytes]	SHA-1 160 Bit
test_2_1.jpg	241 634	969C431F1B328051CEC92FCD7274A5413036688D
restored.vdata	241 634	969C431F1B328051CEC92FCD7274A5413036688D

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
  <string name="security_answer">test answer!</string>
  <string name="device">HTC One M8s 5.0.2</string>
  <int name="synced_settings_version" value="3" />
  <string name="security_question">test question?</string>
  <boolean name="use_default_media_player" value="true" />
  <boolean name="show_all_items_album" value="true" />
  <boolean name="is_backup_authorized" value="true" />
  <boolean name="fullscan_required" value="false" />
  <string name="password_hash">kAFQmDzST7DWlj99KOF/cg==</string>
  <long name="help_select" value="1487429962986" />
  <boolean name="sync_require_wifi" value="true" />
  <int name="version" value="4284" />
  <boolean name="show_old_user_backup_setup_screen" value="false" />
  <long name="last_interstitial_time" value="1495727914016" />
  <string name="password"></string>
  <string name="timeout">5000</string>
```

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
  <string name="security_answer">test answer!</string>
  <string name="device">HTC One M8s 5.0.2</string>
  <int name="synced_settings_version" value="3" />
  <string name="security_question">test question?</string>
  <boolean name="use_default_media_player" value="true" />
  <boolean name="show_all_items_album" value="true" />
  <boolean name="is_backup_authorized" value="true" />
  <boolean name="fullscan_required" value="false" />
  <string name="password_hash">kAFQmDzST7DWlj99KOF/cg==</string>
  <long name="help_select" value="1487429962986" />
  <boolean name="sync_require_wifi" value="true" />
  <int name="version" value="4284" />
  <boolean name="show_old_user_backup_setup_screen" value="false" />
  <long name="last_interstitial_time" value="1495727914016" />
  <string name="password"></string>
  <string name="timeout">5000</string>
```

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
  <string name="security_answer">test answer!</string>
  <string name="device">HTC One M8s 5.0.2</string>
  <int name="synced_settings_version" value="3" />
  <string name="security_question">test question?</string>
  <boolean name="use_default_media_player" value="true" />
  <boolean name="show_all_items_album" value="true" />
  <boolean name="is_backup_authorized" value="true" />
  <boolean name="fullscan_required" value="false" />
  <string name="password_hash">kAFQmDzST7DWlj99KOF/cg==</string>
  <long name="help_select" value="1487429962986" />
  <boolean name="sync_require_wifi" value="true" />
  <int name="version" value="4284" />
  <boolean name="show_old_user_backup_setup_screen" value="false" />
  <long name="last_interstitial_time" value="1495727914016" />
  <string name="password"></string>
  <string name="timeout">5000</string>
```

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
  <string name="security_answer">test answer!</string>
  <string name="device">HTC One M8s 5.0.2</string>
  <int name="synced_settings_version" value="3" />
  <string name="security_question">test question?</string>
  <boolean name="use_default_media_player" value="true" />
  <boolean name="show_all_items_album" value="true" />
  <boolean name="is_backup_authorized" value="true" />
  <boolean name="fullscan_required" value="false" />
  <string name="password_hash">kAFQmDzST7DWlj99KOF/cg==</string>
  <long name="help_select" value="1487429962986" />
  <boolean name="sync_require_wifi" value="true" />
  <int name="version" value="4284" />
  <boolean name="show_old_user_backup_setup_screen" value="false" />
  <long name="last_interstitial_time" value="1495727914016" />
  <string name="password"></string>
  <string name="timeout">5000</string>
```

Fazit:

- Datei umbenannt und verschoben
- Datei durch triviale Änderung unlesbar gemacht
- Sicherheitsfrage und -antwort im Klartext abgespeichert

→ Versteckte Datei problemlos wiederherstellbar

Fallbeispiele

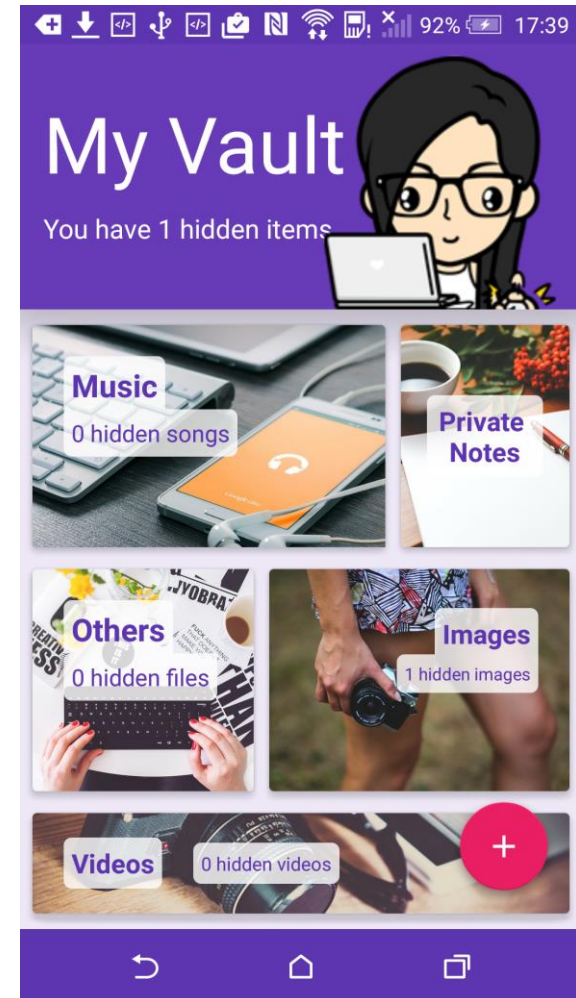
Fall 3: Disguised Encrypter

Version:
1.3

Downloads:
1.000 – 5.000

Features:

- Versteckt Dateien
- Passwortschutz
- AES-256 Verschlüsselung
- App als Taschenrechner getarnt



<https://play.google.com/store/apps/details?id=com.kay.june.disguisedfilehider>

Fall 3: Disguised Encrypter



/storage/emulated/0/Pictures/test data/test_15_1.jpg

/storage/emulated/0/Pictures/test data/test_15_1.jpg

→

/storage/emulated/0/.myCalculator/.Picz/test_15_1.jpg

/storage/emulated/0/Pictures/test data/test_15_1.jpg

→

/storage/emulated/0/.myCalculator/.Picz/test_15_1.jpg

□ Verstecktes Bild öffnen

→ Datei ist „beschädigt“

Fall 3: Disguised Encrypter

test_15_1.jpg																	
Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
00000000	55	CE	B7	27	2F	DD	52	FD	8F	CF	4E	32	47	A9	B7	3D	Uî··/ÝRý ïN2G@·=
00000016	37	10	64	E3	BE	B3	CB	A9	C9	FF	66	26	1B	C5	4D	8A	7 dã¾°È@Éýf& ÅŠ
00000032	CE	77	B1	F1	66	A1	C1	77	F3	26	56	72	22	E4	5C	2B	Îwîñf;Áwó&Vr"ä\+
00000048	97	3D	04	5B	0D	06	C9	93	93	79	2C	EF	77	CE	B2	E1	-= [É""y,iwî²á
00000064	95	EB	3B	1F	CC	CA	9A	F4	FE	81	C2	EA	D3	43	34	DC	•ë; îÊšôp ÂêÓC4Ü
00000080	39	64	71	DA	A6	5A	BE	AC	DE	F4	2C	27	B7	42	7E	B8	9dqÚ!Z¾-Ðó,'·B~,
00000096	34	1A	78	B0	EF	A7	E1	E9	EA	83	99	D4	36	EC	D7	31	4 x°i\$áééf™Ô6ì×1
00000112	6F	11	FC	BC	35	18	04	96	2B	65	5D	1F	3D	A7	06	BB	o ü¾5 -+e] =§ »
00000128	98	23	31	6F	32	A4	15	4D	AC	1D	A6	BE	0F	7F	29	BE	#1o2¾ M- ¾)¾
00000144	5B	CB	58	DB	74	5C	A9	D0	D2	30	8F	10	16	64	45	9F	[ÈXÛt\@ÐÒ0 dEÿ
00000160	AC	68	89	F8	92	64	6E	D0	42	ED	72	F6	D9	DD	25	A3	-h%ø'dnÐBíróÛÝ%£
00000176	BD	D5	4F	12	06	28	13	49	50	7D	56	C9	85	92	A0	9D	¾ÕO (IP}VÉ...'
00000192	96	6F	CE	36	42	9C	8A	43	D0	9A	95	D6	96	D2	55	6A	-oî6BœŠÇÐš•Ö-ÒUj
00000208	E4	57	B4	67	E0	BE	62	ED	BF	32	33	4D	F0	86	09	14	äW'gà¾bí;23Mø†
00000224	FD	08	68	B5	A4	84	7C	8B	3C	B7	A2	E3	55	64	95	A8	ý hu¾,, <<·çäUd·"
00000240	EC	A8	EA	8D	ED	DC	1A	8D	BB	C2	2E	6D	9B	88	4A	D7	ì"ê íÛ »Â.m>^Jx
00000256	39	47	7C	CA	F7	68	E6	1E	1B	24	B6	1C	56	4E	F4	EF	9G Ê÷hæ \$¶ VNôì

/storage/emulated/0/.myCalculator/.Picz/.myImageThumbs/

→ test_15_1.jpg

/storage/emulated/0/.myCalculator/.Picz/.myImageThumbs/

→ test_15_1.jpg



Fazit:

- Datei verschoben
- Datei verschlüsselt
- Unverschlüsselter Thumbnail in Unterordner

→ Versteckte Datei teilweise wiederherstellbar

Fallbeispiele

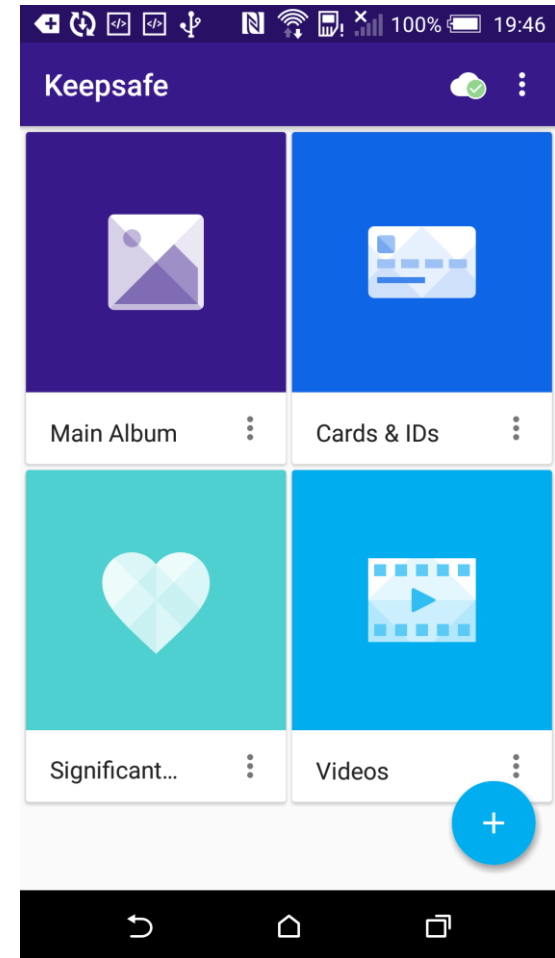
Fall 4: Keepsafe

Version:
8.1.1

Downloads:
> 10 000 000

Features:

- Versteckt Dateien
- Passwortschutz
- AES-256 Verschlüsselung
- Unauffällige Tarnung
- Sync & Backup



<https://play.google.com/store/apps/details?id=com.kii.safe>



/storage/emulated/0/Pictures/test data/test_4_1.jpg

/storage/emulated/0/.keepsafemanifests/primary/fe/
fe05a2344ac5ffd7f17ab71782fff4eec18f883e/

→ ORIGINAL	244 987	Bytes
→ PREVIEW	124 580	Bytes
→ THUMBNAIL	46 110	Bytes

```
/storage/emulated/0/.keepsafemanifests/primary/fe/  
fe05a2344ac5ffd7f17ab71782fff4eec18f883e/
```

→ ORIGINAL	244 987	Bytes
→ PREVIEW	124 580	Bytes
→ THUMBNAIL	46 110	Bytes



- Lesbare PNG Dateien (ohne Endung)
- 100 * 100 Pixel Auflösung
- Größe von ORIGINAL ähnelt test_4_1.jpg (241 265 Bytes)

Fall 4: Keepsafe

ORIGINAL	PREVIEW	THUMBNAIL															
Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
00000000	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	%PNG IHDR
00000016	00	00	00	64	00	00	00	64	08	03	00	00	00	47	3C	65	d d G<e
00000032	66	00	00	03	00	50	4C	54	45	9C	E3	E2	31	C9	C5	2D	f PLTEœãâ1ÉÅ-
00000048	94	DA	1A	5D	E4	DA	F4	F3	17	6B	E6	B5	E8	F9	35	BC	"Ú]äÚóó kæµèù5*

Fall 4: Keepsafe

ORIGINAL	PREVIEW	THUMBNAIL															
Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
00000000	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	%PNG IHDR
00000016	00	00	00	64	00	00	00	64	08	03	00	00	00	47	3C	65	d d G<e
00000032	66	00	00	03	00	50	4C	54	45	9C	E3	E2	31	C9	C5	2D	f PLTEœãâ1ÉÅ-
00000048	94	DA	1A	5D	E4	DA	F4	F3	17	6B	E6	B5	E8	F9	35	BC	"Ú]äÚóó kæµèù5*

ORIGINAL	PREVIEW	THUMBNAIL															
Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
00003024	0A	DD	00	00	00	00	49	45	4E	44	AE	42	60	82	4B	65	Ý IEND@B`,Ke
00003040	65	70	53	61	66	65	4B	65	65	70	53	61	66	65	4B	65	epSafeKeepSafeKe
00003056	65	70	53	61	66	65	4B	65	65	70	53	61	66	65	4B	65	epSafeKeepSafeKe
00003072	65	70	53	61	66	65	4B	65	65	70	53	61	66	65	4B	65	epSafeKeepSafeKe

ORIGINAL	PREVIEW	THUMBNAIL															
Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
00000000	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	%PNG IHDR
00000016	00	00	00	64	00	00	00	64	08	03	00	00	00	47	3C	65	d d G<e
00000032	66	00	00	03	00	50	4C	54	45	9C	E3	E2	31	C9	C5	2D	f PLTEœãâ1ÉÅ-
00000048	94	DA	1A	5D	E4	DA	F4	F3	17	6B	E6	B5	E8	F9	35	BC	"Ú]äúÓó kæµèù5*

ORIGINAL	PREVIEW	THUMBNAIL															
Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
00003024	0A	DD	00	00	00	00	49	45	4E	44	AE	42	60	82	4B	65	Ý IEND@B`,Ke
00003040	65	70	53	61	66	65	4B	65	65	70	53	61	66	65	4B	65	epSafeKeepSafeKe
00003056	65	70	53	61	66	65	4B	65	65	70	53	61	66	65	4B	65	epSafeKeepSafeKe
00003072	65	70	53	61	66	65	4B	65	65	70	53	61	66	65	4B	65	epSafeKeepSafeKe

ORIGINAL	PREVIEW	THUMBNAIL															
Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
00003680	65	70	53	61	66	65	4B	65	65	70	53	61	66	65	4B	65	epSafeKeepSafeKe
00003696	65	70	53	61	66	65	4B	65	65	BF	A6	16	2C	3F	AB	6C	epSafeKee¿! ,?«1
00003712	9B	B8	80	8E	47	ED	AC	7A	20	01	10	12	91	54	A0	4E	>,€ŽGí~z `T N
00003728	05	3E	40	A1	F8	41	C0	90	E6	CB	A2	78	B2	EA	83	3A	>@;øAÀ æËçx²êf:
00003744	A0	00	9E	44	FD	6E	83	61	CC	18	21	AD	8A	30	B9	11	žDýnfai !-Š0¹
00003760	F2	0E	D3	CD	63	E6	B9	DC	98	6C	A7	36	54	C0	A8	55	ò ÓÍcæ¹ÜIŞ6TÀ`U
00003776	F2	19	7C	F3	38	49	10	4F	CD	AC	99	9B	D4	1F	44	A4	ò ó8I OÍ~»>Ô D»
00003792	0B	46	C3	B6	D8	E7	B1	B7	04	91	C9	51	54	D4	86	60	FĂŦøç±· `ÉQTôT`
00003808	82	24	96	E9	E7	9A	98	F8	CC	3C	95	6A	2A	35	6B	05	,\$-éçššÏ<·j*5k `

Fazit:

- Datei in Trägermedium versteckt
- Datei verschlüsselt

→ Versteckte Datei nicht wiederherstellbar

Untersuchungsergebnisse

- 23 File Hider Apps untersucht, davon waren bei
- 19: versteckte Daten rekonstruierbar
- 13: dazu keine externen Hilfsmittel nötig
- 14: Originaldaten unverändert
- 10: Passwort im Klartext gespeichert

- 23 File Hider Apps untersucht, davon waren bei
- 19: versteckte Daten rekonstruierbar
- 13: dazu keine externen Hilfsmittel nötig
- 14: Originaldaten unverändert
- 10: Passwort im Klartext gespeichert

→ 4 Apps vertrauenswürdig



<http://atxcatholic.com/wp-content/uploads/2013/06/thatsallfolks.jpg>