

Anti-Forensik

Sascha Preuth
Lehrgebiet Datennetze

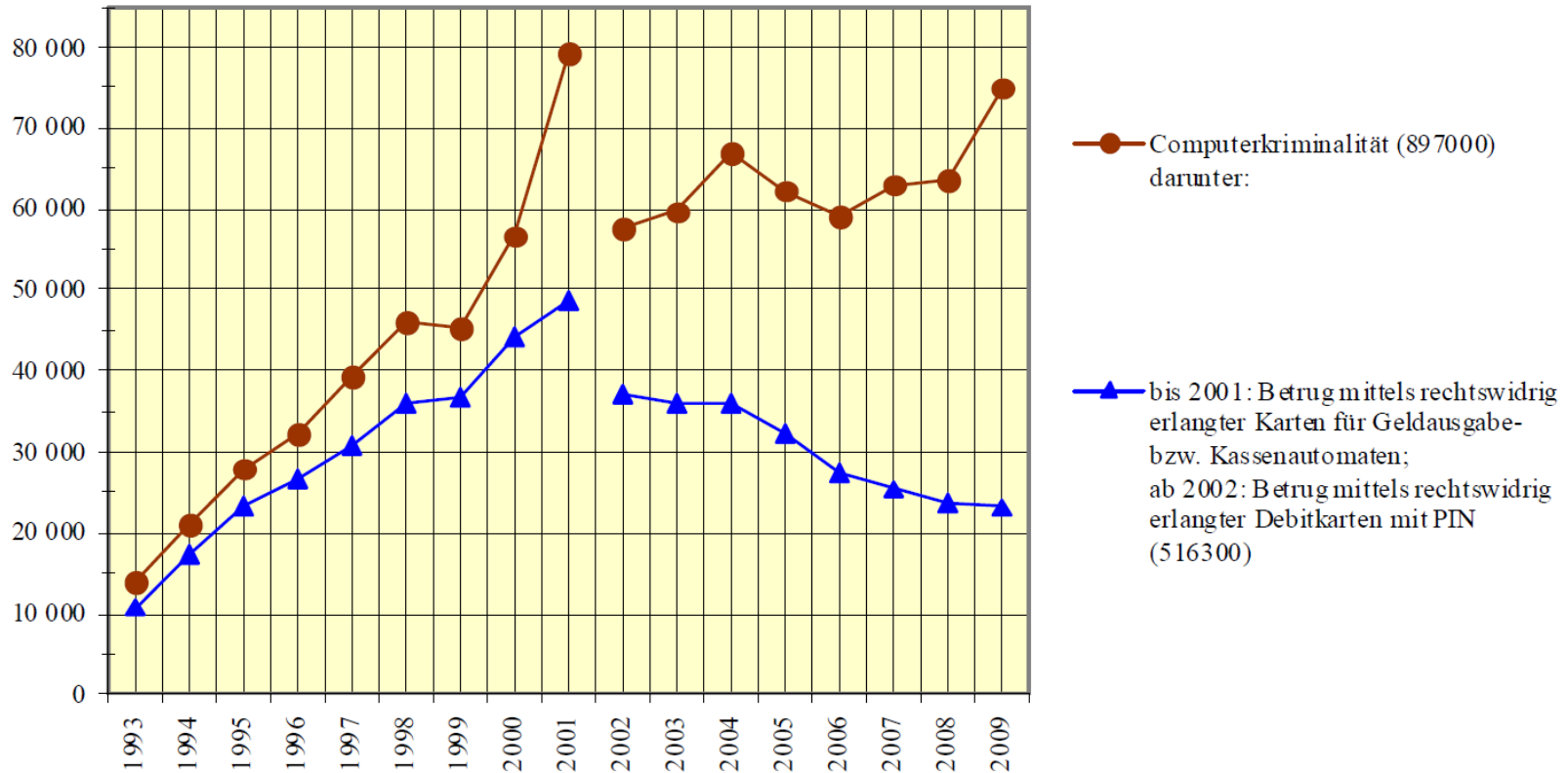


- Definition und Klassifizierung der Anti-Forensik
- Computerkriminalität
- Aufbau Praxisprojekt
- Kryptographie
- Steganographie
- Sichere Lösungsverfahren
- Manipulation von Zeitstempeln
- Fazit

- Negative Beeinflussung der Existenz oder Qualität von digitalen Beweisen.
- Erschwerung der Analyse von Beweismitteln bei forensischen Untersuchungen.
 - Löschen/Verbergen von Daten
 - (durch Rootkits, **Kryptographie**, **Steganographie**)
 - Vernichten von (nebenläufigen) Informationen/Artefakten
 - (mittels **sicherer Lösungsverfahren**)
 - Verwischen von Spuren
 - (durch Spoofing, Desinformation anhand **Dateimodifikation**)

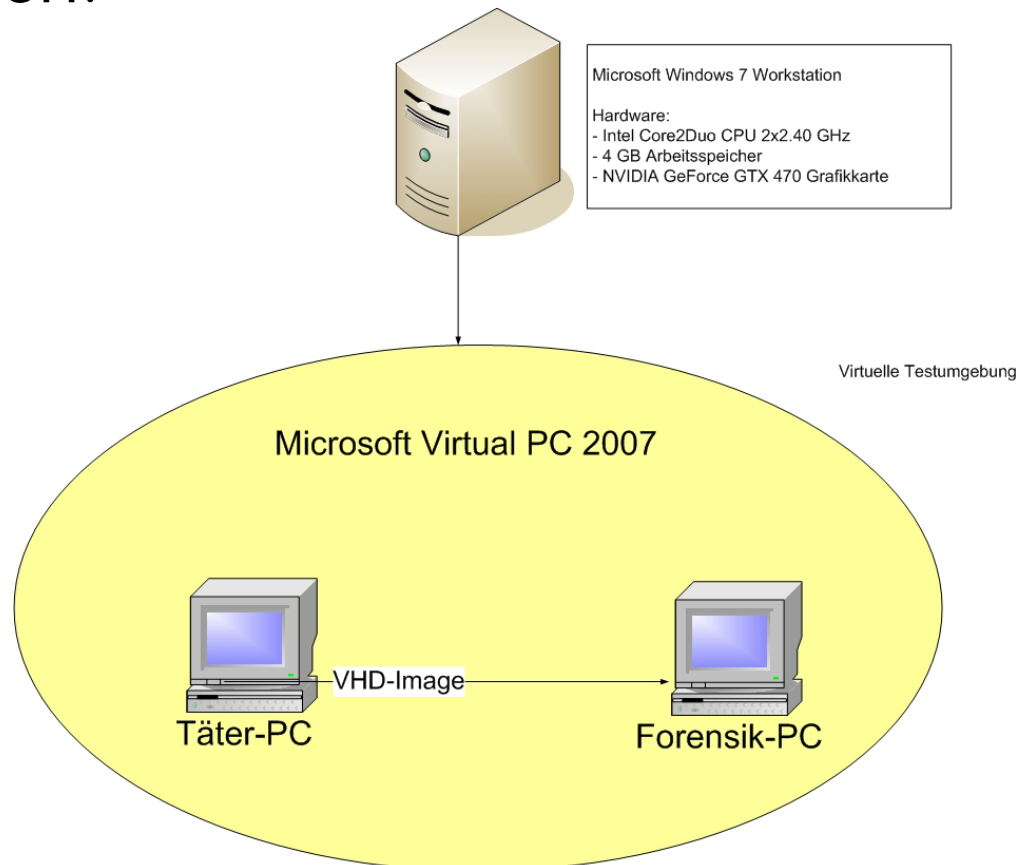
- Was versteht man unter Computerkriminalität?
 - Computersabotage
 - Computerbetrug
 - Ausspähen, Abfangen von Daten
 - Softwarepiraterie
 - Fälschung beweiserheblicher Daten

- IT-forensische Untersuchungen von Datenträgern finden dort statt, wo der PC als Tatmittel genutzt wurde.



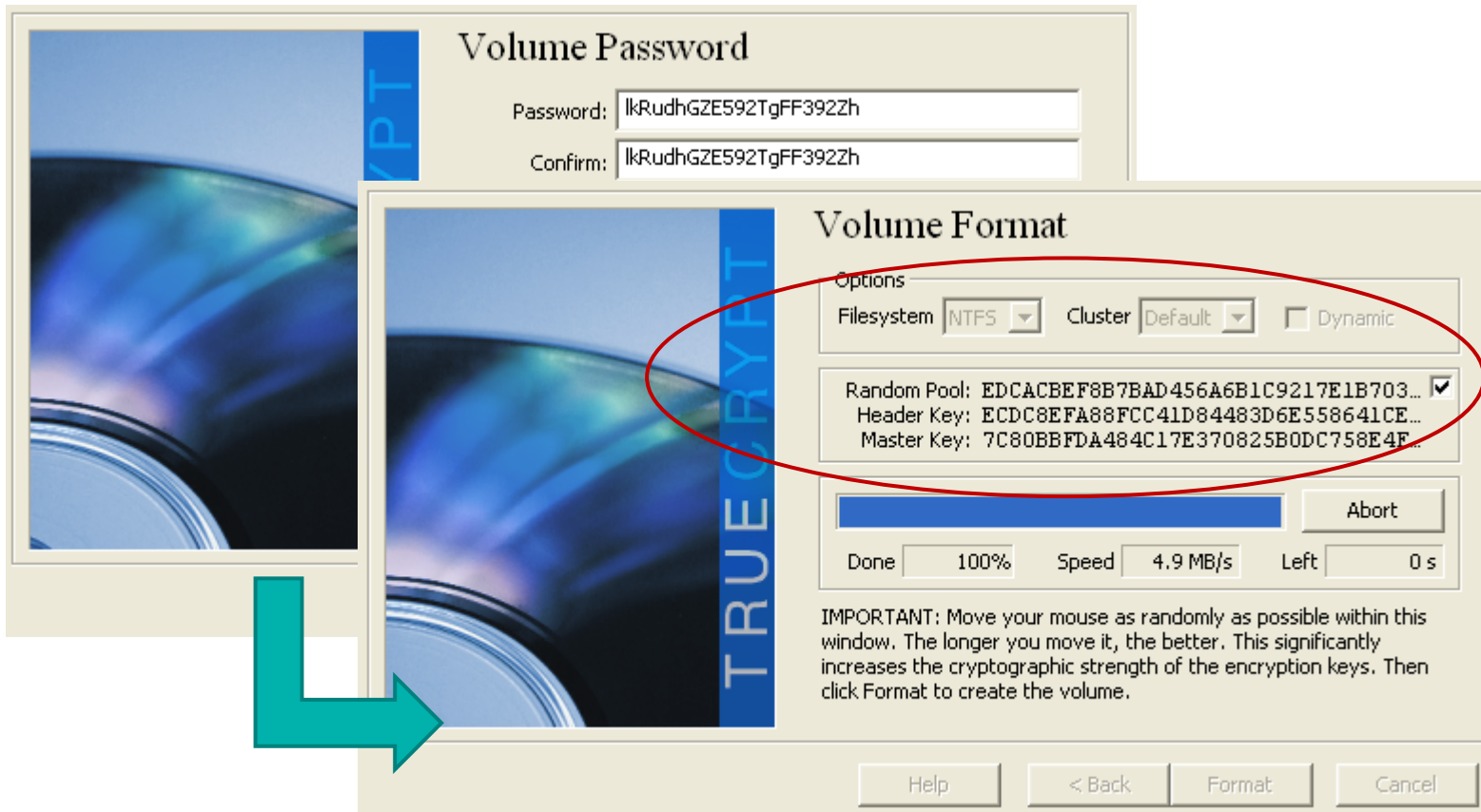
- Computerkriminalität ist ein Kontrolldelikt !

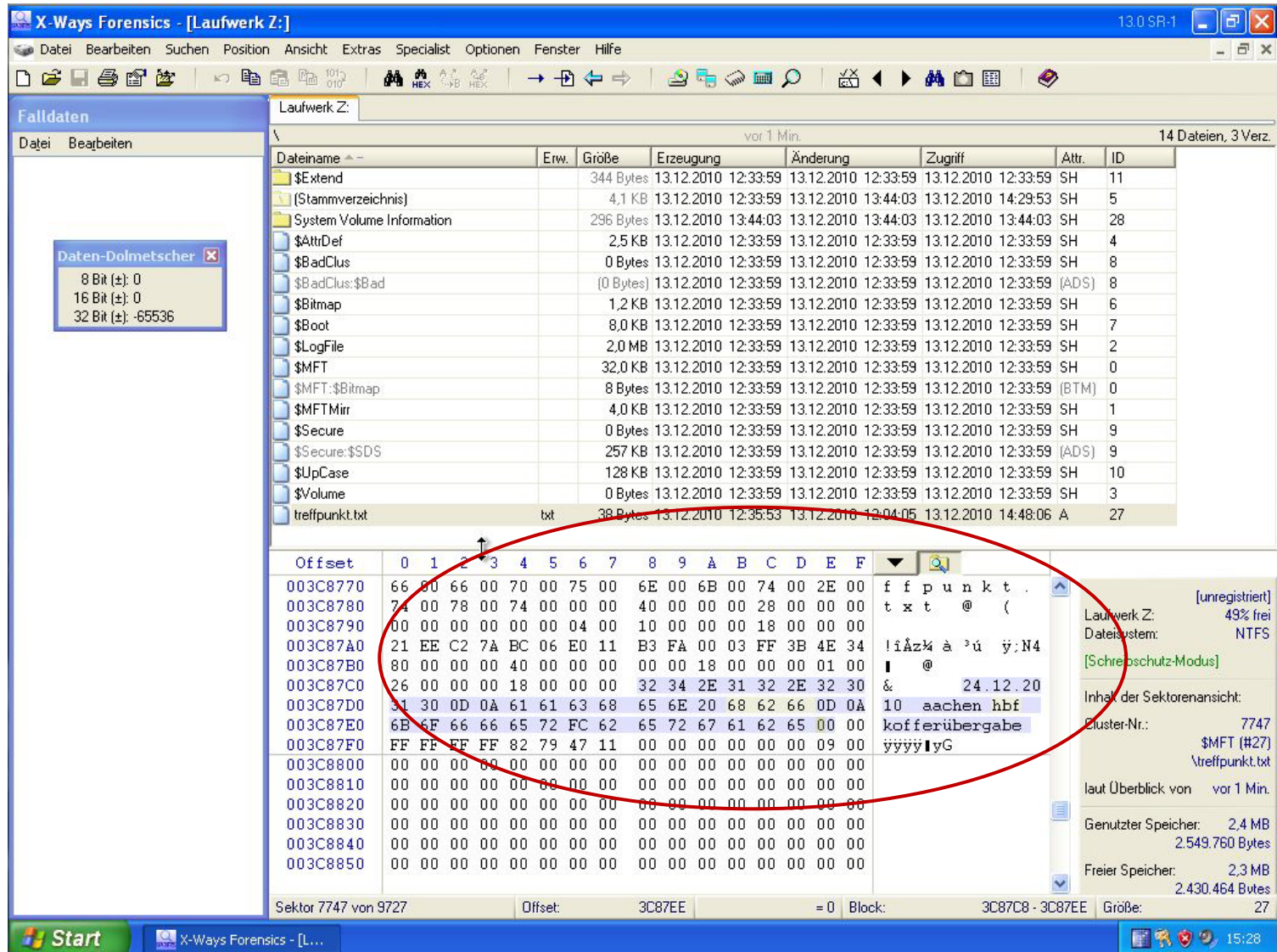
- Ziel: Daten auf Datenträgern anti-forensisch vorbereiten und im Anschluss IT-forensisch untersuchen.



- Vorbereitung der Systeme:
 - Täter-PC:
 - Deaktivierung „Windows System Restore Points“
 - Installation:
 - TrueCrypt
 - JPHS
 - Steganos Privacy Suite
 - Eraser
 - TimeStomp
 - Forensik-PC:
 - Installation:
 - X-Ways Forensics
 - StegDetect
 - WinMerge
 - Ntfsinfo

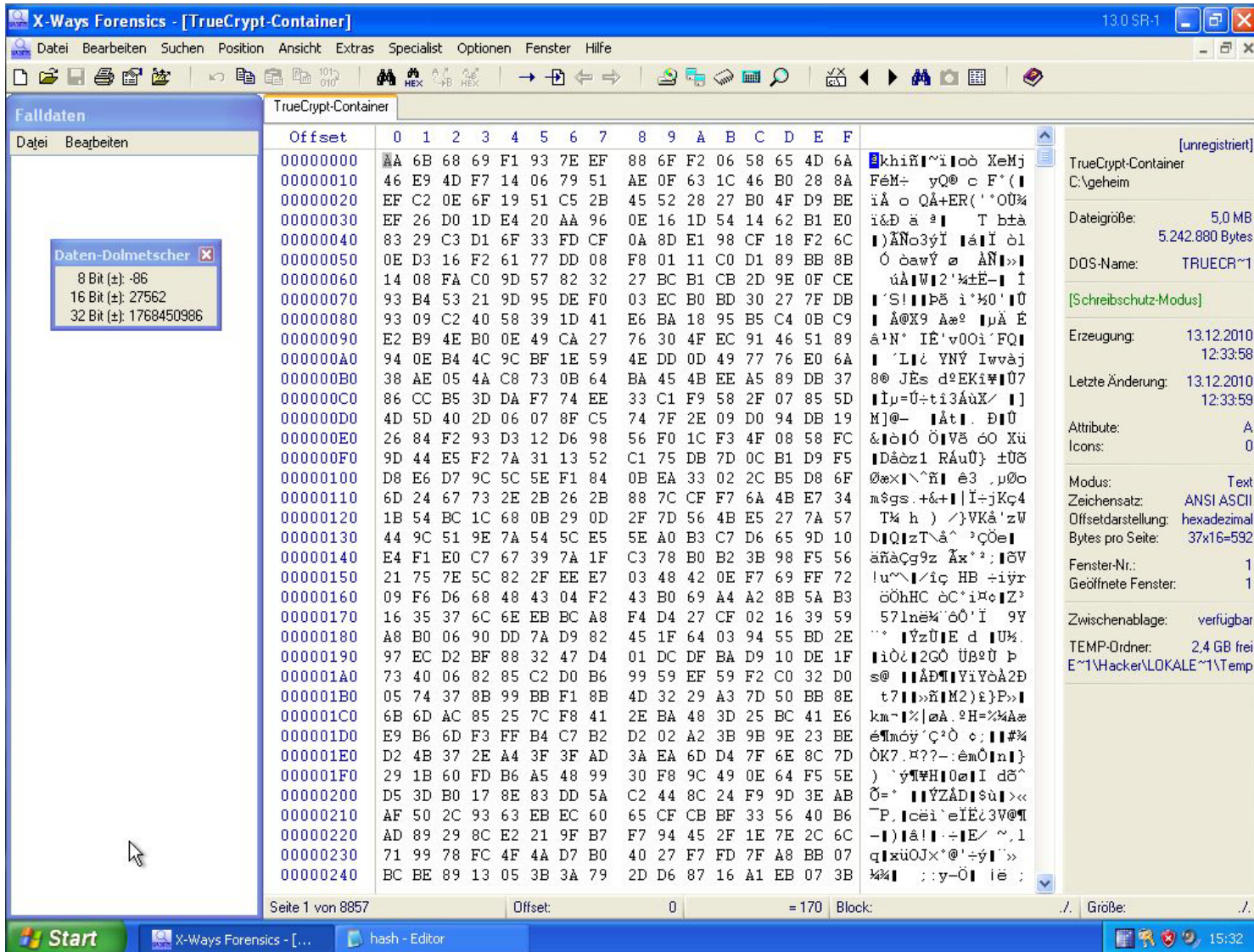
- Verschlüsselung mit TrueCrypt:
 - AES-Algorithmus, 256-Bit Schlüssel, 128-Bit Blockgröße
 - Test-Szenario anhand eines verschlüsselten Containers:
 - Datei wird innerhalb eines erstellten TrueCrypt Containers erzeugt
 - ! Sichere Passwortwahl !
 - Notieren der erzeugten Schlüssel: Header & Master Key
 - Überprüfung des Datenträgers und Arbeitsspeichers auf Spuren der Schlüssel (Vor, während und nach dem „Mounten“ des Containers)
 - Analyse des verschlüsselten Inhaltes
 - Zusatz-Szenario: „Hidden Volume“





The screenshot shows the X-Ways Forensics interface. The main window displays a file system view of drive Z: with a list of files and folders. A file named 'treffpunkt.txt' is selected. Below the file list, a hex dump of the file's content is shown, with a red circle highlighting the first few lines of the dump. The hex dump shows the ASCII characters 'treffpunkt.txt' followed by some special characters and a date '24.12.2010'.

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Hex	ASCII
003C8770	66	00	66	00	70	00	75	00	6E	00	6B	00	74	00	2E	00	f	t
003C8780	74	00	78	00	74	00	00	00	40	00	00	00	28	00	00	00	t	.
003C8790	00	00	00	00	00	00	04	00	10	00	00	00	18	00	00	00		
003C87A0	21	EE	C2	7A	BC	06	E0	11	B3	FA	00	03	FF	3B	4E	34	!	ä
003C87B0	80	00	00	00	40	00	00	00	00	00	18	00	00	00	01	00	@	
003C87C0	26	00	00	00	18	00	00	00	32	34	2E	31	32	2E	32	30	&	
003C87D0	31	30	0D	0A	61	61	63	68	65	6E	20	68	62	66	0D	0A	10	a
003C87E0	6B	6F	66	66	65	72	FC	62	65	72	67	61	62	65	00	00	k	o
003C87F0	FF	FF	FF	FF	82	79	47	11	00	00	00	00	00	00	09	00	ü	ü
003C8800	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
003C8810	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
003C8820	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
003C8830	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
003C8840	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
003C8850	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		



X-Ways Forensics - [TrueCrypt-Container] 13.0 SR-1

File Edit Search Position View Extras Specialist Options Window Help

Falldaten

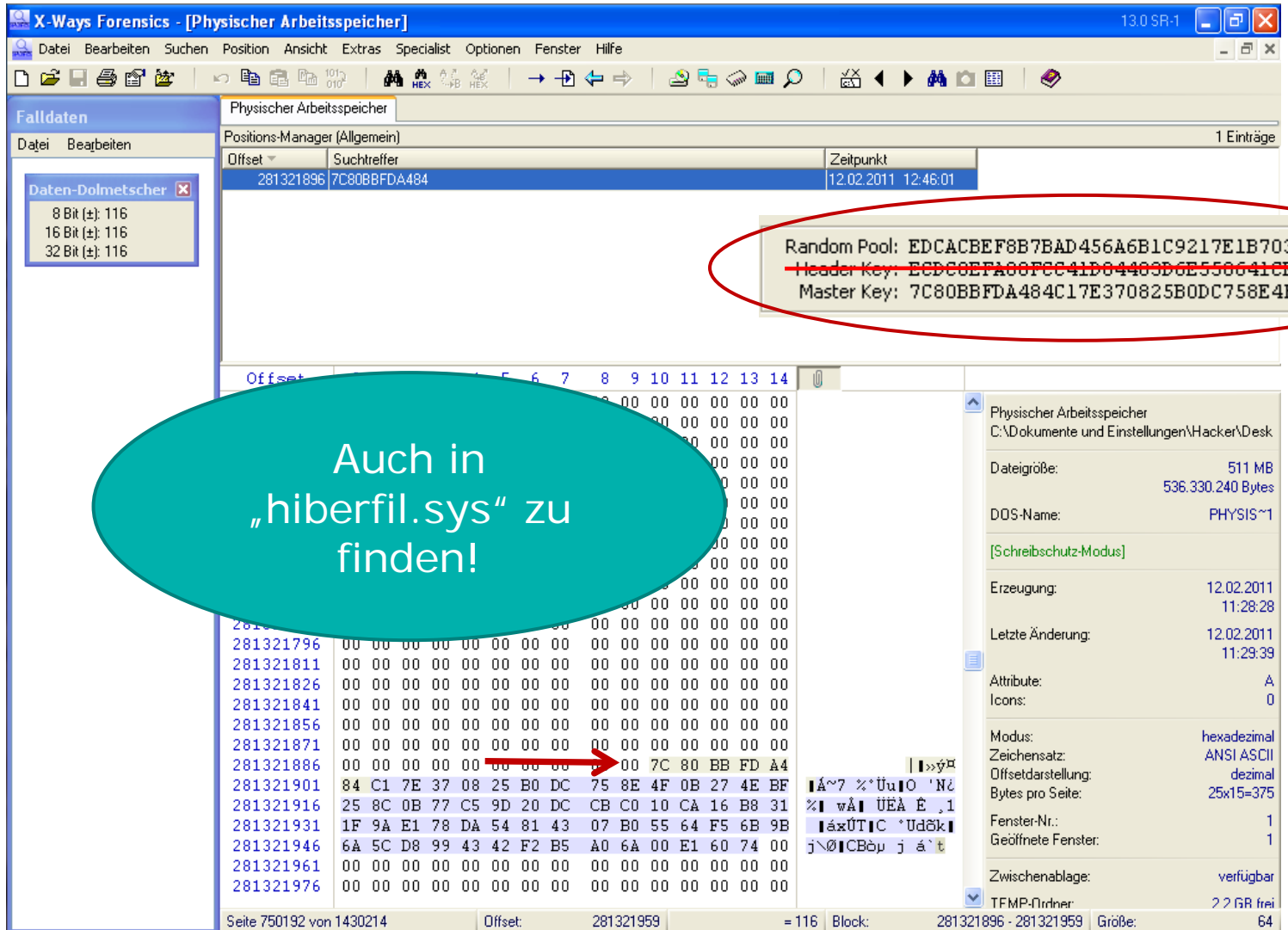
TrueCrypt-Container

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	AA	6B	68	69	F1	93	7E	EF	88	6F	F2	06	58	65	4D	6A	khifñ~iioò XeMj
00000010	46	E9	4D	F7	14	06	79	51	AE	0F	63	1C	46	B0	28	8A	FéM+ yQ0 c F*(
00000020	EF	C2	0E	6F	19	51	C5	2B	45	52	28	27	B0	4F	D9	BE	iÁ o QÁ+ER('`00%
00000030	EF	26	D0	1D	E4	20	AA	96	0E	16	1D	54	14	62	B1	E0	i&D ä ß T btà
00000040	83	29	C3	D1	6F	33	FD	CF	0A	8D	E1	98	CF	18	F2	6C)Ñ03ýÍ íáÍ òl
00000050	0E	D3	16	F2	61	77	DD	08	F8	01	11	C0	D1	89	BB	8B	Ó òawÿ ø ÆÑI>>
00000060	14	08	FA	C0	9D	57	82	32	27	BC	B1	CB	2D	9E	0F	CE	úÀW 2'¼±E- í
00000070	93	B4	53	21	9D	95	DE	F0	03	EC	B0	BD	30	27	7F	DB	'S I B8 i'¼0'Í0
00000080	93	09	C2	40	58	39	1D	41	E6	BA	18	95	B5	C4	0B	C9	Á0X9 Aæ° ÍµÁ É
00000090	E2	B9	4E	B0	0E	49	CA	27	76	30	4F	EC	91	46	51	89	á'N' IE'v00i'FQ
000000A0	94	0E	B4	4C	9C	BF	1E	59	4E	DD	0D	49	77	76	E0	6A	'L ¿ YNÝ Iwváj
000000B0	38	AE	05	4A	C8	73	0B	64	BA	45	4B	EE	A5	89	DB	37	80 JÉS d°EKi#Í07
000000C0	86	CC	B5	3D	DA	F7	74	EE	33	C1	F9	58	2F	07	85	5D	Íµ=Û+ti3ÁúX/
000000D0	4D	5D	40	2D	06	07	8F	C5	74	7F	2E	09	D0	94	DB	19	M]@- Át . DÍ0
000000E0	26	84	F2	93	D3	12	D6	98	56	F0	1C	F3	4F	08	58	FC	& ò Ó Ö V8 ó0 Xu
000000F0	9D	44	E5	F2	7A	31	13	52	C1	75	DB	7D	0C	B1	D9	F5	Dáòz1 RÁU0} ±Ü8
00000100	D8	E6	D7	9C	5C	5E	F1	84	0B	EA	33	02	C8	B5	D8	6F	0æx '^ñ é3 .µ0o
00000110	6D	24	67	73	2E	2B	26	2B	88	7C	CF	F7	6A	4B	E7	34	m\$gs.+&+ Í+jKç4
00000120	1B	54	BC	1C	68	0B	29	0D	2F	7D	56	4B	E5	27	7A	57	T¼ h) /}VKÁ'zW
00000130	44	9C	51	9E	7A	54	5C	E5	5E	A0	B3	C7	D6	65	9D	10	D Q zT\^` ³ç0e
00000140	E4	F1	E0	C7	67	39	7A	1F	C3	78	B0	B2	3B	98	F5	56	ãñàçg9z Áx'²: 8V
00000150	21	75	7E	5C	82	2F	EE	E7	03	48	42	0E	F7	69	FF	72	!u~\ iç HB ÷iyr
00000160	09	F6	D6	68	48	43	04	F2	43	B0	69	A4	A2	8B	5A	B3	òÖhHC óC'iµo Z³
00000170	16	35	37	6C	6E	EB	BC	A8	F4	D4	27	0F	02	16	39	59	57lnè'ò'0'Í 9Y
00000180	A8	B0	06	90	DD	7A	D9	82	45	1F	64	03	94	55	BD	2E	"" ÿzÜ E d U¼.
00000190	97	EC	D2	BF	88	32	47	D4	01	DC	DF	BA	D9	10	DE	1F	iÖ¿ 2G0 ÜßÜ0 þ
000001A0	73	40	06	82	85	C2	D0	B6	99	59	EF	59	F2	C0	32	D0	s@ IÁD¶ YiYòÁ2D
000001B0	05	74	37	8B	99	BB	F1	8B	4D	32	29	A3	7D	50	BB	8E	t7 I>>ñ M2)£ P>
000001C0	6B	6D	AC	85	25	7C	F8	41	2E	BA	48	3D	25	BC	41	E6	km~ ¼ øÁ.²H=¼¼Aæ
000001D0	E9	B6	6D	F3	FF	B4	C7	B2	D2	02	A2	3B	9B	9E	23	BE	éµmóý'c²0 c; I#¼
000001E0	D2	4B	37	2E	A4	3F	3F	AD	3A	EA	6D	D4	7F	6E	8C	7D	ÖK7.µ??-:ém0 n }
000001F0	29	1B	60	FD	B6	A5	48	99	30	F8	9C	49	0E	64	F5	5E)'ýµ¶H 0e I d8^
00000200	D5	3D	B0	17	8E	83	DD	5A	C2	44	8C	24	F9	9D	3E	AB	Ö=° IÿZÁD sù >>>
00000210	AF	50	2C	93	63	EB	EC	60	65	CF	CB	BF	33	56	40	B6	°P. cèi'eIE¿3V0¶
00000220	AD	89	29	8C	E2	21	9F	B7	F7	94	45	2F	1E	7E	2C	6C	-)Iá I+ E/ ~.l
00000230	71	99	78	FC	4F	4A	D7	B0	40	27	F7	FD	7F	A8	BB	07	q zü0Jx'@'+ý I>>
00000240	BC	BE	89	13	05	3B	3A	79	2D	D6	87	16	A1	EB	07	3B	¼¼ :;y-Ö iè ;

Seite 1 von 8857 Offset: 0 = 170 Block: ./ Größe: ./

Properties Panel:

- [unregistriert]
- TrueCrypt-Container
- C:\Geheim
- Dateigröße: 5,0 MB
- 5.242.880 Bytes
- DOS-Name: TRUECR~1
- [Schreibschutz-Modus]
- Erzeugung: 13.12.2010 12:33:58
- Letzte Änderung: 13.12.2010 12:33:59
- Attribute: A
- Icons: 0
- Modus: Text
- Zeichensatz: ANSI ASCII
- Offsetdarstellung: hexadezimal
- Bytes pro Seite: 37x16=592
- Fenster-Nr.: 1
- Geöffnete Fenster: 1
- Zwischenablage: verfügbar
- TEMP-Ordner: 2,4 GB frei
- E:\1\Hacker\LOKALE\1\Temp



X-Ways Forensics - [Physischer Arbeitsspeicher]

Physischer Arbeitsspeicher

Positions-Manager (Allgemein)

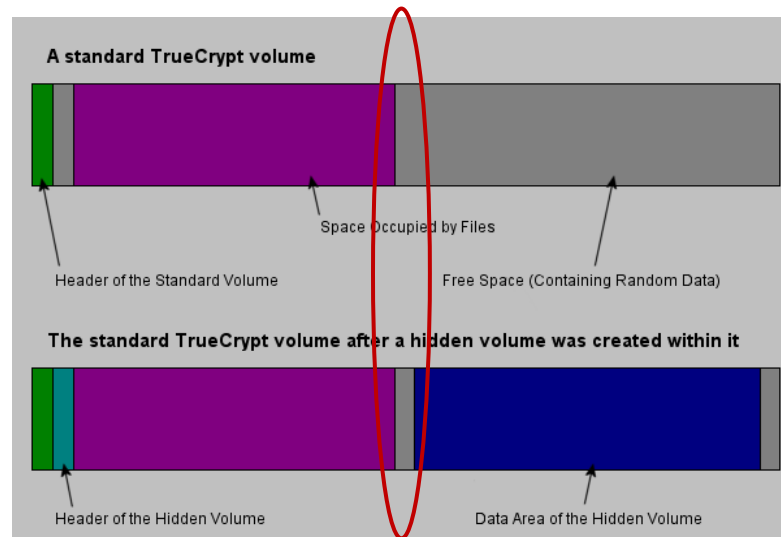
Offset	Suchtreffer	Zeitpunkt
281321896	7C80BBFDA484	12.02.2011 12:46:01

Random Pool: EDCACBEF8B7BAD456A6B1C9217E1B703...
~~Header Key: ECDC0EFA00FCC41D04403D6E550641CE...~~
 Master Key: 7C80BBFDA484C17E370825B0DC758E4F...

Auch in „hiberfil.sys“ zu finden!

Offset: 281321959 = 116 Block: 281321896 - 281321959 Größe: 64

- Zweck: Bei Erzwingung der Herausgabe eines Passwortes. -> „Fake-Container“
- Untersuchung der „Hidden Volumes“ zeigt Hinweise auf versteckten Container.
 - Abweichung bei den zufälligen Bit-Bereichen des „freien Speichers“ innerhalb des TrueCrypt Containers



...0000... bei den ersten 64 KB!

Zufalls-Bits von Beginn an!

- Verborgene Speicherung oder Übermittlung von Informationen in Bild-, Video- und Tondateien.
 - Primärziel: Existenz darf nicht erkannt werden!
- Eingesetzte Software:
 - JPEG Hide and Seek
 - Steganos Crypt and Hide
- Beide Tools das LSB-Verfahren (JPG) um Inhalte in Bilddateien einzubetten.
 - Test-Szenario: 8 KB Test-Nachricht -> 82 KB Trägerdatei



Original

JPHS



Original



Crypt and Hide

- Optisch in beiden Fällen unauffällig, wobei „Crypt and Hide“ deutlich besser arbeitet.
 - JPHS zerstört JPEG-Header -> zu auffällig!

- Detektions-Tools meist machtlos.

- Kriterien für Sicherheit:
 - Originalbild darf nicht bekannt sein.
 - Originalbild sollte detailreich sein.
 - Das Trägerbild sollte, den Vorgaben der Software entsprechend, groß gewählt sein.
 - Sicheres Passwort.

- Hauptziel: Daten unwiderruflich löschen!
- Die besten Verfahren:
 - U.S. Standard, DoD 5220.22-M (3- bis 7-fach)
 - Gutmann-Methode (35-fach)
- In der Praxis reicht einmaliges Überschreiben der Bits!
- Wahrscheinlichkeiten der Bit-Widerherstellung:
 - 1 Bit = 56 Prozent
 - 1 Byte = 0,97 Prozent

X-Ways Forensics - [Laufwerk C:] 13.0 SR-1

Datei Bearbeiten Suchen Position Ansicht Extras Specialist Optionen Fenster Hilfe

Laufwerk C: vor 0 Min. 3 Dateien, 0 Verz.

Dateiname	Erw.	Größe	Erzeugung	Änderung	Zugriff	Attr.	ID
Testbild.jpg	jpg	42,8 KB	13.01.2011 11:02:20	13.01.2011 11:02:09	12.02.2011 12:40:47	A	11167
Testnachricht.txt	txt	17 Bytes	12.02.2011 12:41:00	12.02.2011 12:41:18	12.02.2011 12:41:18	A	11812
TrueCrypt-Container		5,0 MB	13.12.2010 11:33:58	12.02.2011 09:49:05	12.02.2011 09:49:05	A	10834

Daten-Dolmetscher

- 8 Bit (±): 70
- 16 Bit (±): 18758
- 32 Bit (±): 1162627398

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	Hex	ASCII
1085837522	56	1A	B2	CA	CB	01	00	00	00	00	00	00	00	00	00	56 1A B2 CA CB 01 00 00 00 00 00 00 00 00 00	v *ËË
1085837537	00	00	00	00	00	00	00	20	00	00	00	00	00	00	00	00 00 00 00 20 00 00 00 00 00 00 00 00 00	
1085837552	0C	02	54	00	45	00	53	00	54	00	4E	00	41	00	7E	0C 02 54 00 45 00 53 00 54 00 4E 00 41 00 7E	T E S T N A ~
1085837567	00	31	00	2E	00	54	00	58	00	54	00	74	00	2E	00	00 31 00 2E 00 54 00 58 00 54 00 74 00 2E 00	l . T X T t .
1085837582	74	00	30	00	00	00	80	00	00	00	00	00	00	00	00	74 00 30 00 00 00 80 00 00 00 00 00 00 00 00	t 0
1085837597	00	04	00	64	00	00	00	18	00	01	00	F2	18	00	00	00 04 00 64 00 00 00 18 00 01 00 F2 18 00 00	d ò
1085837612	00	00	0A	00	80	E4	56	1A	B2	CA	CB	01	80	E4	56	00 00 0A 00 80 E4 56 1A B2 CA CB 01 80 E4 56	äV *ËË äV
1085837627	1A	B2	CA	CB	01	80	E4	56	1A	B2	CA	CB	01	80	E4	1A B2 CA CB 01 80 E4 56 1A B2 CA CB 01 80 E4	*ËË äV *ËË ä
1085837642	56	1A	B2	CA	CB	01	00	00	00	00	00	00	00	00	00	56 1A B2 CA CB 01 00 00 00 00 00 00 00 00	v *ËË
1085837657	00	00	00	00	00	00	00	20	00	00	00	00	00	00	00	00 00 00 00 00 00 20 00 00 00 00 00 00 00	
1085837672	11	01	54	00	65	00	73	00	74	00	6E	00	61	00	63	11 01 54 00 65 00 73 00 74 00 6E 00 61 00 63	T e s t n a c
1085837687	00	68	00	72	00	69	00	63	00	68	00	74	00	2E	00	00 68 00 72 00 69 00 63 00 68 00 74 00 2E 00	h r i c h t .
1085837702	74	00	78	00	74	00	18	00	00	00	40	00	00	00	28	74 00 78 00 74 00 18 00 00 40 00 00 00 28	t x t @ (
1085837717	00	00	00	00	00	00	00	00	00	06	00	10	00	00	00	00 00 00 00 00 00 06 00 10 00 00 00 00	
1085837732	18	00	00	00	1A	95	59	38	8D	36	E0	11	B4	13	00	18 00 00 00 1A 95 59 38 8D 36 E0 11 B4 13 00	!Y8!6ä
1085837747	03	FF	3B	4E	34	80	00	00	00	30	00	00	00	00	00	03 FF 3B 4E 34 80 00 00 00 30 00 00 00 00 00	ÿ:N4 0
1085837762	18	00	00	00	01	00	11	00	00	00	18	00	00	00	44	18 00 00 00 01 00 11 00 00 00 18 00 00 00 44	D
1085837777	61	73	20	69	73	74	20	65	69	6E	20	54	65	73	74	61 73 20 69 73 74 20 65 69 6E 20 54 65 73 74	a s i s t e i n T e s t
1085837792	21	00	00	00	00	00	00	00	FF	FF	FF	FF	82	73	47	21 00 00 00 00 00 00 FF FF FF FF 82 73 47	! ÿÿÿÿ!yG
1085837807	11	00	00	00	00	00	00	00	00	00	00	00	00	00	00	11 00 00 00 00 00 00 00 00 00 00 00 00 00	
1085837822	03	00	00	00	00	00	00	00	00	00	00	00	00	00	00	03 00 00 00 00 00 00 00 00 00 00 00 00 00	
1085837837	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00 00 00 00 00 00 00 00 00 00 00 00 00	
1085837852	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00 00 00 00 00 00 00 00 00 00 00 00 00	
1085837867	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00 00 00 00 00 00 00 00 00 00 00 00 00	
1085837882	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00 00 00 00 00 00 00 00 00 00 00 00 00	

Sektor 2120776 von 14683344 Offset: 1085837312 = 70 Block: ./ Größe: ./

Laufwerk C: 31% frei
Dateisystem: NTFS
[Schreibschutz-Modus]
Inhalt der Sektorenansicht:
Cluster-Nr.: 265097
\$MFT (#11812)
\\geheim\Testnachricht.txt
laut Überblick von vor 1 Min.
Physische Sektor-Nr.: 2120839
Logische Sektor-Nr.: 2120776
Genutzter Speicher: 4,8 GB
5.154.353.152 Bytes
Freier Speicher: 2,2 GB
2.363.518.976 Bytes
Gesamtkapazität: 7,0 GB
7.517.872.128 Bytes
Bytes pro Cluster: 4.096
Freie Cluster: 577.031
Cluster insgesamt: 1.835.418
Bytes pro Sektor: 512
Sektoren insgesamt: 14.683.344

X-Ways Forensics - [Laufwerk C:] 13.0 SR-1

Datei Bearbeiten Suchen Position Ansicht Extras Specialist Optionen Fenster Hilfe

Laufwerk C: vor 0 Min. 2 Dateien, 0 Verz.

Dateiname	Erw.	Größe	Erzeugung	Änderung	Zugriff	Attr.	ID
Testbild.jpg	jpg	42,8 KB	13.01.2011 11:02:20	13.01.2011 11:02:09	12.02.2011 12:40:47	A	11167
TrueCrypt-Container		5,0 MB	13.12.2010 11:33:58	12.02.2011 09:49:05	12.02.2011 09:49:05	A	10834

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1085837312	46	49	4C	45	30	00	03	00	98	10	3C	03	00	00	00
1085837327	00	05	00	01	00	38	00	00	00	60	01	00	00	00	04
1085837342	00	00	00	00	00	00	00	00	00	00	08	00	00	00	24
1085837357	2E	00	00	04	00	00	00	00	00	00	00	10	00	00	00
1085837372	60	00	00	00	00	00	00	00	00	00	00	00	48	00	00
1085837387	00	18	00	00	00	80	E4	56	1A	B2	CA	CB	01	40	6B
1085837402	DE	24	B2	CA	CB	01	30	AC	DB	AF	B2	CA	CB	01	E0
1085837417	3C	62	AE	B2	CA	CB	01	20	00	00	00	00	00	00	00
1085837432	00	00	00	00	00	00	00	00	00	00	00	00	76	01	00
1085837447	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
1085837462	00	00	30	00	00	00	68	00	00	00	00	00	00	00	00
1085837477	00	07	00	50	00	00	00	18	00	01	00	82	0F	00	00
1085837492	00	00	02	00	80	E4	56	1A	B2	CA	CB	01	40	6B	DE
1085837507	24	B2	CA	CB	01	40	6B	DE	24	B2	CA	CB	01	40	6B
1085837522	DE	24	B2	CA	CB	01	18	00	00	00	00	00	00	00	11
1085837537	00	00	00	00	00	00	20	00	00	00	00	80	00	00	00
1085837552	07	03	44	00	63	00	32	00	2E	00	74	00	78	00	74
1085837567	00	40	00	00	00	28	00	00	00	00	00	00	00	00	00
1085837582	06	00	10	00	00	00	18	00	00	00	1A	95	59	38	8D
1085837597	36	E0	11	B4	13	00	03	FF	3B	4E	34	80	00	00	00
1085837612	30	00	00	00	00	00	18	00	00	00	00	00	11	00	00
1085837627	00	18	00	00	00	44	61	73	20	69	73	74	20	65	69
1085837642	6E	20	54	65	73	74	21	00	00	00	00	00	00	FF	FF
1085837657	FF	FF	FF	FF	82	79	47	11	21	00	00	00	00	00	00
1085837672	FF	FF	FF	FF	82	79	47	11	74	00	6E	00	61	00	63

Sektor 2120776 von 14683344 Offset: 1085837357 = 46 Block: ./ Größe: ./

Daten-Dolmetscher

8 Bit (±): 46
16 Bit (±): 46
32 Bit (±): 67108910

Laufwerk C: 31% frei
Dateisystem: NTFS
[Schreibschutz-Modus]

Inhalt der Sektorensicht:

Cluster-Nr.: 265097
\$MFT (#11812)
\\RECYCLER\1-5-21-823...\Dc2.txt (gelöscht)

Physische Sektor-Nr.: 2120839
Logische Sektor-Nr.: 2120776

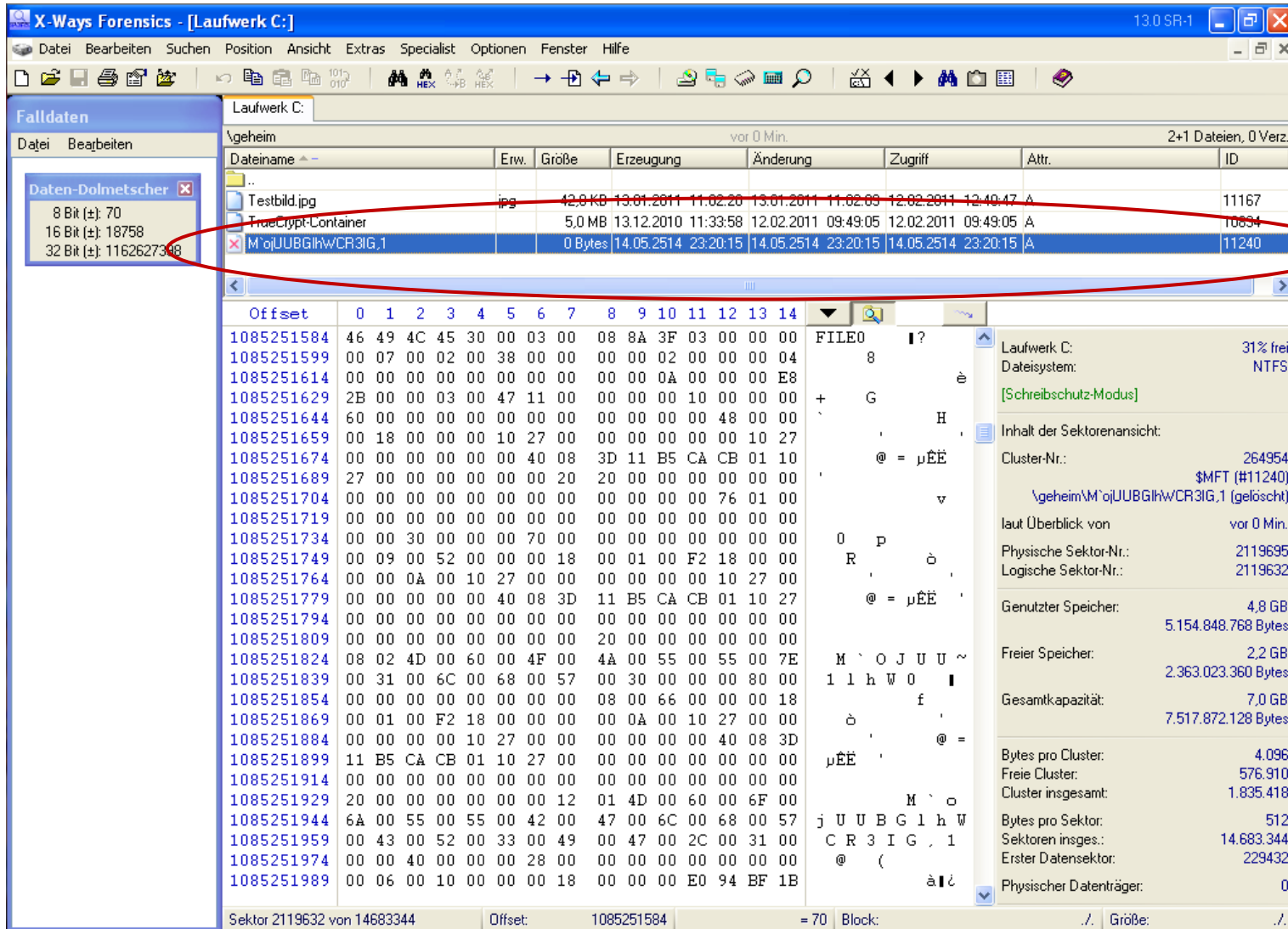
Genutzter Speicher: 4,8 GB
5.154.349.056 Bytes

Freier Speicher: 2,2 GB
2.363.523.072 Bytes

Gesamtkapazität: 7,0 GB
7.517.872.128 Bytes

Bytes pro Cluster: 4.096
Freie Cluster: 577.032
Cluster insgesamt: 1.835.418

Bytes pro Sektor: 512
Sektoren insgesamt: 14.683.344

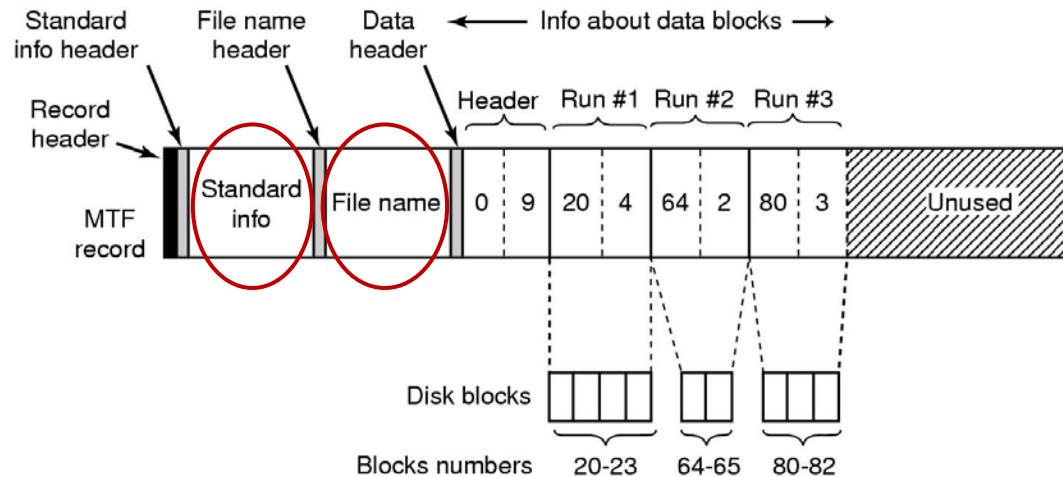


The screenshot shows the X-Ways Forensics interface. On the left, the 'Falldaten' pane shows the file 'M\ojUUBGih\WCR3IG.1' selected. The main window displays a file list for drive C: with columns for Dateiname, Erw., Größe, Erzeugung, Änderung, Zugriff, Attr., and ID. The file 'M\ojUUBGih\WCR3IG.1' is highlighted in red. Below the file list, a hex view shows the file's content, with the text 'M \ O J U U ~' and '1 1 h W 0 |' visible. The right pane shows the file's properties, including its location, size, and deletion status.

Dateiname	Erw.	Größe	Erzeugung	Änderung	Zugriff	Attr.	ID
Testbild.jpg	jpg	42,9 KB	13.01.2011 11:02:20	13.01.2011 11:02:09	12.02.2011 13:40:47	A	11167
TrueCrypt-Container		5,0 MB	13.12.2010 11:33:58	12.02.2011 09:49:05	12.02.2011 09:49:05	A	10834
M\ojUUBGih\WCR3IG.1		0 Bytes	14.05.2514 23:20:15	14.05.2514 23:20:15	14.05.2514 23:20:15	A	11240

- Veränderung der Dateizugriffe oder Erstellungsdaten
 - Z.B.: Manipulierte Beweise für zeitliche Abläufe

- Zeitstempel in MFT-Datei gespeichert

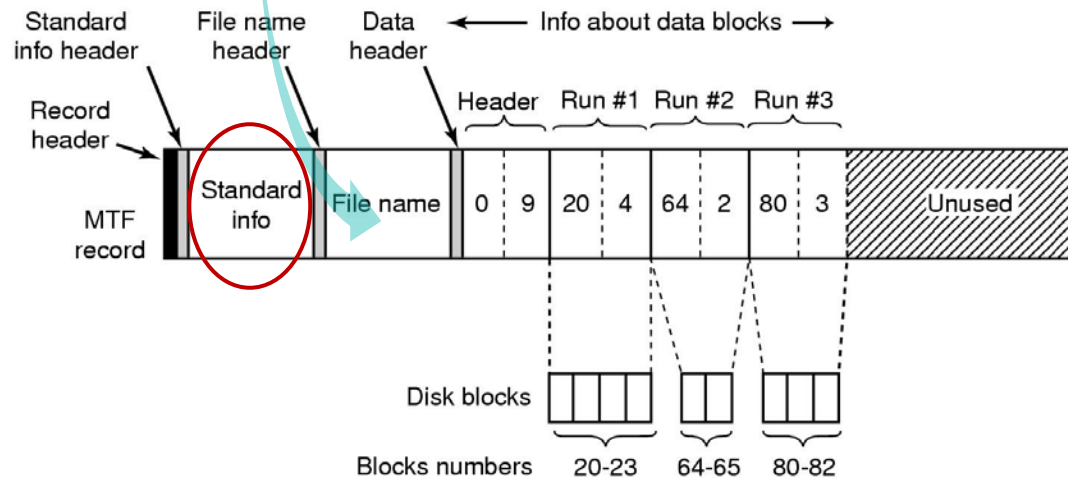


- Jede Datei im NTFS-Dateisystem besitzt folgende zeitlichen Eigenschaften:
 - Letzte Dateiänderung (file altered time)
 - Letzter Dateizugriff (last accessed time)
 - Erstelldatum (file creation time)
 - Eintrag der Datei in Master File Table (MFT changed time)

```
C:\>timestomp c:\zeittest.txt -v
Modified:      Friday 2/25/2011 15:41:29
Accessed:     Friday 2/25/2011 15:41:29
Created:      Friday 2/25/2011 15:41:29
Entry Modified: Friday 2/25/2011 15:41:33
```



```
C:\>timestomp c:\zeittest.txt -z "Saturday 12/11/2010 08:03:11 PM"
C:\>timestomp c:\zeittest.txt -v
Modified:      Saturday 12/11/2010 20:3:11
Accessed:     Saturday 12/11/2010 20:3:11
Created:      Saturday 12/11/2010 20:3:11
Entry Modified: Saturday 12/11/2010 20:3:11
```



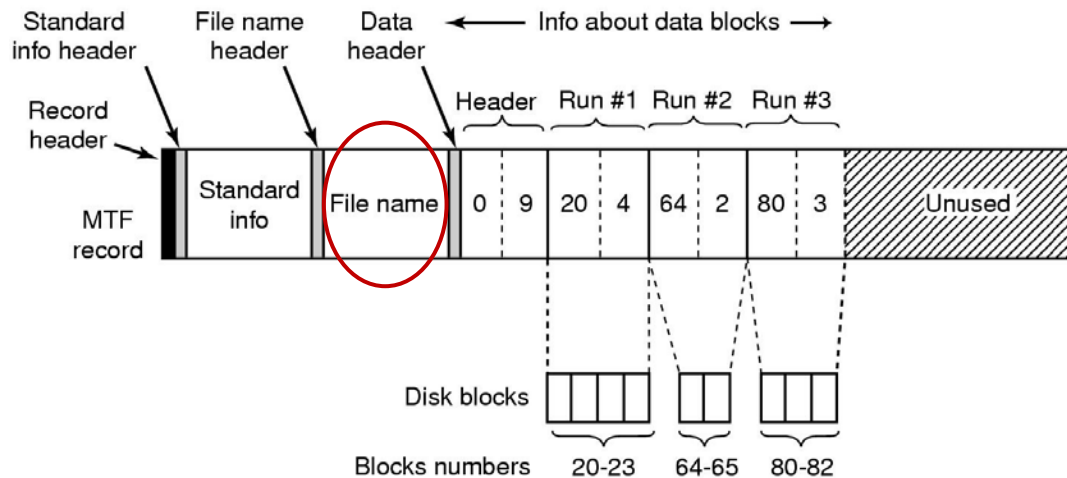
- Originalzeiten

- Modifizierte Zeit

- Änderung nur im „Standard Information“-Eintrag

- X-Ways und Windows zeigen die veränderten Zeiten richtig an, ntfsinfo zeigt Originalzeit:

```
C:\GnuWin32\bin>ntfsinfo -d /dev/hda1 -i 16790
Failed to set locale, using default '(null)'.
Dumping $STANDARD_INFORMATION <0x10>
  Size of STANDARD_INFORMATION is 76. It should be either 72 or 48, something is wrong...
Dumping $FILE_NAME <0x30>
File Name:                zeittest.txt
File Name Length:         12
Allocated File Size:      0
Real File Size:           0
File Creation Time:       Fri Feb 25 15:41:29 2011
File Altered Time:        Fri Feb 25 15:41:29 2011
MFT Changed Time:         Fri Feb 25 15:41:29 2011
Last Accessed Time:       Fri Feb 25 15:41:29 2011
```

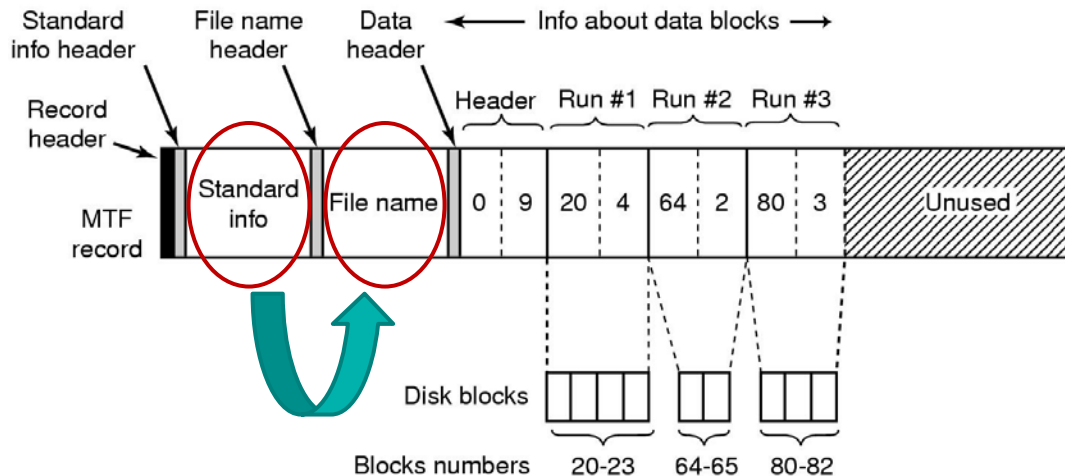


- Problem umgehen, indem man Datei verschiebt:

```
C:\>timestomp c:\zeittest.txt -v
Modified:      Saturday 12/11/2010 20:3:11
Accessed:     Saturday 12/11/2010 20:3:11
Created:      Saturday 12/11/2010 20:3:11
Entry Modified: Saturday 12/11/2010 20:3:11
```

```
C:\GnuWin32\bin>ntfsinfo -d /dev/hda1 -i 16790
Failed to set locale, using default '<null>'.
Dumping $STANDARD_INFORMATION (0x10)
  Size of STANDARD_INFORMATION is 76. It should be e
ing is wrong...
Dumping $FILE_NAME (0x30)
  File Name:          zeittest.txt
  File Name Length:  12
  Allocated File Size: 0
  Real File Size:    0
  File Creation Time: Sat Dec 11 20:03:11 2010
  File Altered Time:  Sat Dec 11 20:03:11 2010
  MFT Changed Time:   Sat Dec 11 20:03:11 2010
  Last Accessed Time: Sat Dec 11 20:03:11 2010
```

```
C:\>timestomp c:\geheim\zeittest.txt -v
Modified:      Saturday 12/11/2010 20:3:11
Accessed:     Saturday 12/11/2010 20:3:11
Created:      Saturday 12/11/2010 20:3:11
Entry Modified: Friday 2/25/2011 15:50:7
```



- Alle Methoden sind bei richtigem Einsatz sehr effektiv um forensische Ermittlungen zu behindern:
 - Kryptographie für die Verschleierung von großen Datenmengen.
 - Steganographie für sichere Nachrichtenübermittlung.
 - Sichere Löschverfahren sollten grundsätzlich auf jedem System zur sicheren Datenvernichtung eingesetzt werden.
 - Dateimodifikationen müssen sehr bedacht angewendet werden.

Vielen Dank für
Ihre Aufmerksamkeit!