POLIZEIDIREKTION
SÜDWESTSACHSEN

POLIZEI
Sachsen

Vorläufiger Untersuchungsbericht

der DV Ermittlungsunterstützung zum Vorgang-Nr.: 2135/11/173440

Auftraggeber:
Kriminalpolizeiinspektion Südwestsachsen
Dezernat 1
EKHK Müller
Lessingstrasse 17-21
08058 Zwickau

Auswertung:
Kriminalpolizeiinspektion Südwestsachsen
Kommissariat 41
Digitale Medienstelle
DV Ermittlungsunterstützung
Lessingstrasse 17-21
08058 Zwickau

Auswerter:
Dipl.-Ing. (BA) Ronny Bodach
Kriminalkommissar

Datum:
6. November 2011

Seiten insgesamt:
14 Seiten

Aktenzeichen:
Staatsanwalt:
Telefon:

PD Südwestsachsen
Kriminalpolizeiinspektion
Kommissariat 41/DMS
Lessingstraße 17 – 21
08058 Zwickau

Tgb.-Nr.: *2135/11/173440*
Sachbearbeiter *Bodach, KK*
öffentlich *0375 428*
LIK *791*
Telefon *4422*
Telefax *2299*

Ermittlungsverfahren der Staatsanwaltschaft
Az.:
gegen
wegen

Anordnung zur Vernichtung von gespeicherten Daten

Die in diesem Verfahren gespeicherten Datenbestände werden in der Digitalen Medienstelle auf dem Datenarchivierungsserver unter DMS Nummer 110423 gesichert.

Diese werden nicht mehr benötigt und können vernichtet werden.

Löschungsgrund: ☐ **Verfahren rechtskräftig abgeschlossen**
☐ **Verfahren eingestellt**

Datum:

_____
Name des Anordnenden

Inhalt

Auftrag

Sachverhalt

Laut Anzeige.

Auftragsstellung

Unterzeichner wurde mit der Auswertung der sichergestellten Asservate vom Brandort Zwickau Frühlingstrasse 26 bezüglich relevanter Daten für das Ermittlungsverfahren beauftragt.

Sicherung des Datenträgers

Die Sicherung des Datenträgers erfolgte am 06.11.2011 in der Dienststelle durch KK Bodach.

Dazu wurde die Festplatte Maxtor Model STM3250318AS Serial number 5VY0RA1Qausgebaut und mit Hilfe eines TABLEAU Forensic SATA/IDE Bridge Schreibblockers an den Sicherungsrechner angeschlossen. Danach wurde mit der Software AccessData® FTK® Imager 3.0.0.1442 101005 ein forensisches Datenträger Image im Evidential Format erstellt (siehe Sicherungsprotokoll im Anhang A). Dieses Datenträger Image stellt eine exakte Kopie der Festplatte dar und kann nach der Erstellung nicht mehr verändert werden. Alle weiteren Arbeiten werden nur noch an dem Datenträger Image durchgeführt, so dass der originale Datenträger nicht mehr benutzt wird. (gemäß BSI Leitfaden IT-Forensik 09/2010)

Durch die Nutzung des Schreibblockers kann sichergestellt werden, dass keine Daten auf dem originalen Datenträger geändert, gelöscht oder überschrieben werden.

Nach dem Erstellen des Datenträger Images wurde die gesicherte Festplatte wieder eingebaut. Ein Funktionstest wurde auf Grund der physikalischen Eigenschaften des Asservates nicht durchgeführt.

Auswertung

Die weitere Auswertung der Daten erfolgte an der gesicherten Image Datei mit dem Programm X-Ways Forensics Version 16.1 der Firma X-Ways Software Technology AG. Der gesicherte Datenbestand wurde in die Auswertesoftware eingelesen und eine erweiterte Analyse des Datenbestandes nach gelöschten Dateien durchgeführt. Im Anschluss daran wurde der Datenbestand nach sachverhaltsrelevanten Dateien durchsucht. Die aufgefundenen Dateien wurden entsprechend extrahiert und mit geeigneten Programmen in ein verständliches Format überführt. (gemäß BSI Leitfaden IT-Forensik 09/2010)

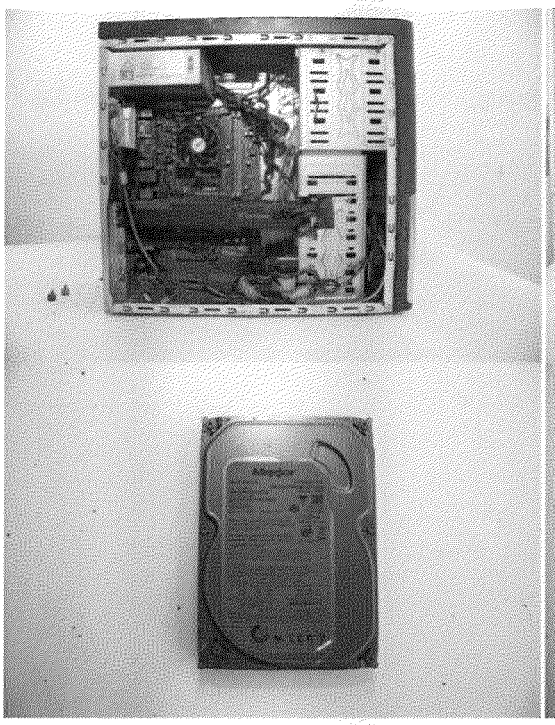
Zur Auswertung wurde eine Windows 7 basiertes Untersuchungssystem mit einem Intel Core Duo Prozessor und Windows 7 Ultimate 64 Bit mit Service Pack 1 und installiertem Internet Explorer 9 genutzt.

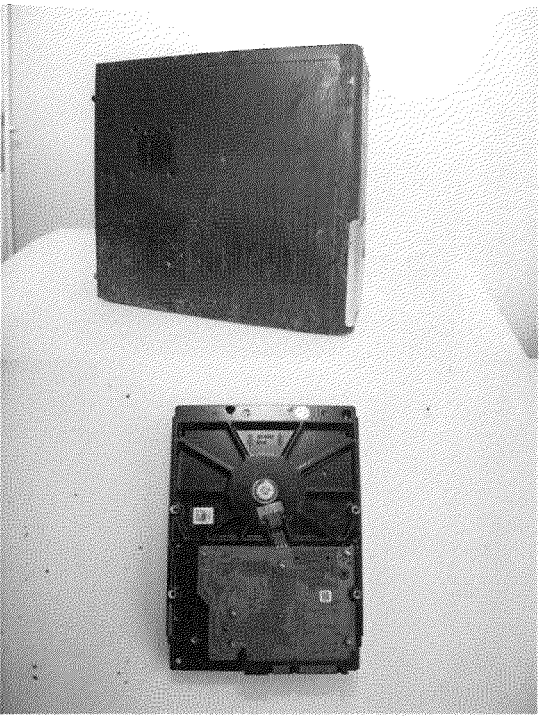
Ergebnis

Hardwarekonfiguration

Asservat EDV01

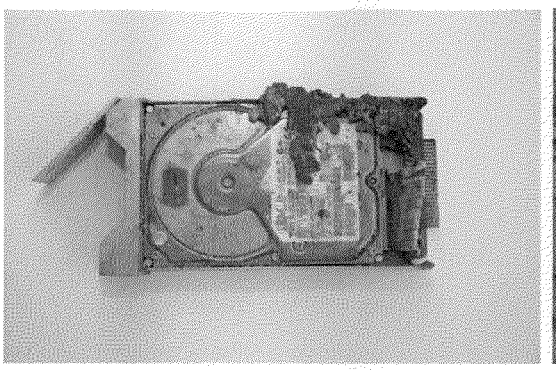
Bei Asservat EDV01 handelt es sich um ein PC AMD der Marke ASUS Serial Number 649081203942 mit einer eingebauten Festplatte mit 250 GB, aufgeteilt in 1 Partition mit NFTS formatiert. Der PC weist äußerlich Brandspuren auf und auch die interne Festplatte ist mit einem Brandbelag überzogen. Ein Auslesen der Daten der Festplatte ist jedoch möglich.

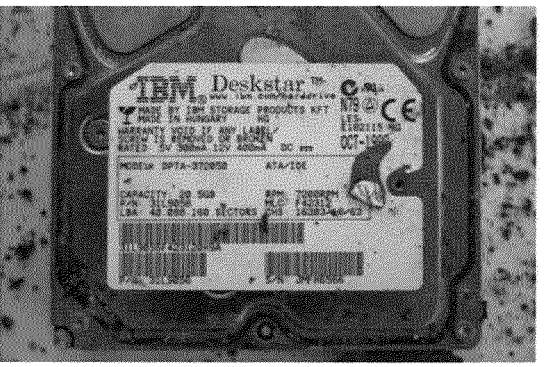


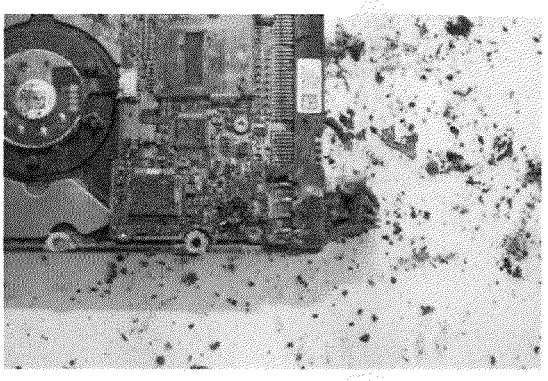


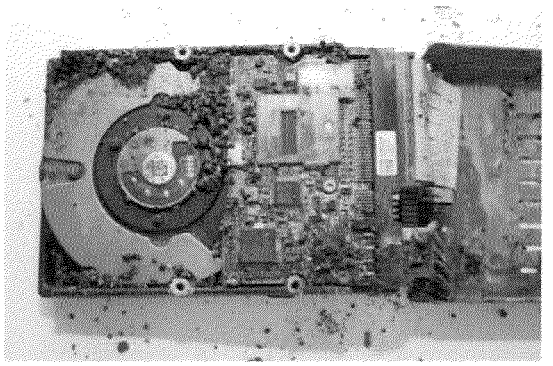
Asservat EDV02

Bei Asservat EDV02 handelt es sich um eine USB interne Wechselfestplatte IDM/Hitachi Deskstar DPTA-372050 mit 20GB Speicherplatz. Die Festplatte weist äußerlich starke Brandspuren auf und die Festplattenelektronik wurde durch Brandeinwirkung beschädigt. Ein Auslesen der Daten dieser Festplatte kann erst nach einem Austausch dieser Elektronik durchgeführt werden.









Daten von Asservat EDV01

Betriebssystem

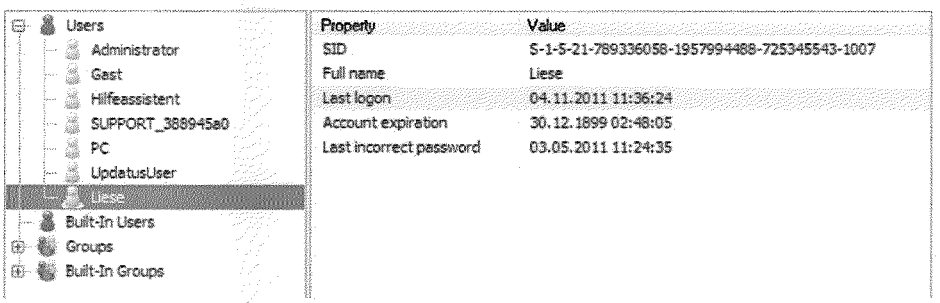
Im Folgenden werden die Registrierungsinformationen zum benutzten Betriebssystem sowie die Betriebssystem Version inklusive Updates aufgelistet:

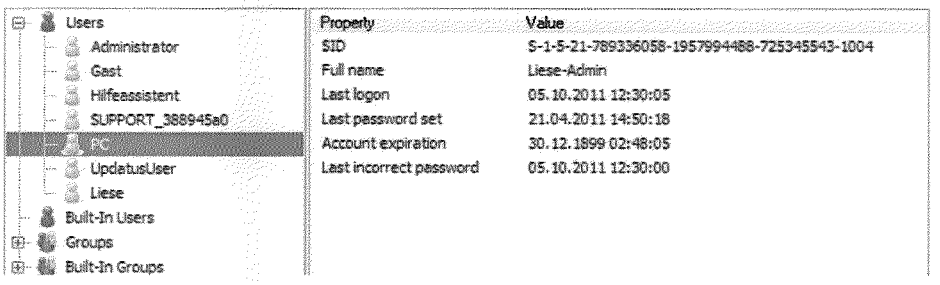
Product Name:	Microsoft Windows XP
Owner:	PC
Organization:	
Product ID:	76416-OEM-0058663-73083
Product Key:	KXKDB-7CG33-XY2B4-MTQTK-M8868
Product Version:	Multiprocessor Free 5.1.2600.xpsp_sp3_gdr.101209-1647
Install Date:	14.04.2011 15:33:35
Service Pack:	Service Pack 3
System Root:	C:\WINDOWS

[Eintragungen aus dem Registry Schlüssel HKLM\Software\\Microsoft\Windows NT\CurrentVersion der SOFTWARE Registrierungsdatei]

Benutzer

Folgende Benutzer waren am Rechner eingetragen:





[Eintragungen aus dem Registry Schlüssel SAM\SAM\SAM\Domains\Account\ der SAM Registrierungsdatei]

Als Hauptnutzer waren die Nutzer **Liese** und **PC** eingetragen. Die restlichen Benutzereinträge sind Benutzereinträge die vom Betriebssystem oder von bestimmten Softwareinstallationen als Standard eingetragen werden.

Die letzte Benutzeranmeldung von **Liese** erfolgte am **04.11.2011 um 12:36 MEZ**.

Die letzte Benutzeranmeldung von **PC** erfolgte am **05.10.2011 um 13:30 MEZ**.

Rechnerbenutzung

Laut Eintragungen des Systemlog-Protokolls[1] des Betriebssystems war der Rechner zu folgenden Zeiten im Zeitraum 21.10.2001 - 05.11.2011 in Betrieb:

Datum (MEZ)	Protokoll	ID	Details	Benutzername
24.10.2011 11:06	System	6005	Der Ereignisprotokolldienst wurde gestartet.	
24.10.2011 11:06	System	6009	Microsoft (R) Windows (R) 5.01. 2600 Service Pack 3	
24.10.2011 11:06	Security	528	An-/Abmeldung	PC
24.10.2011 11:07	Security	528	An-/Abmeldung	Liese
24.10.2011 11:07	Security	528	An-/Abmeldung	Liese
24.10.2011 12:13	System	6006	Der Ereignisprotokolldienst wurde beendet.	
24.10.2011 15:37	System	6005	Der Ereignisprotokolldienst wurde gestartet.	
24.10.2011 15:37	System	6009	Microsoft (R) Windows (R) 5.01. 2600 Service Pack 3	
24.10.2011 15:37	Security	528	An-/Abmeldung	PC
24.10.2011 15:37	Security	528	An-/Abmeldung	Liese
24.10.2011 15:37	Security	528	An-/Abmeldung	Liese
24.10.2011 16:03	Security	528	An-/Abmeldung	Liese
24.10.2011 16:03	Security	528	An-/Abmeldung	Liese
24.10.2011 16:34	Security	528	An-/Abmeldung	Liese
24.10.2011 16:34	Security	528	An-/Abmeldung	Liese
24.10.2011 16:35	System	6006	Der Ereignisprotokolldienst wurde beendet.	
29.10.2011 11:00	System	6005	Der Ereignisprotokolldienst wurde gestartet.	
29.10.2011 11:00	System	6009	Microsoft (R) Windows (R) 5.01. 2600 Service Pack 3	
29.10.2011 11:00	Security	528	An-/Abmeldung	Liese
29.10.2011 11:00	Security	528	An-/Abmeldung	Liese
29.10.2011 11:00	Security	528	An-/Abmeldung	PC
29.10.2011 11:04	System	6005	Der Ereignisprotokolldienst wurde gestartet.	
29.10.2011 11:04	System	6009	Microsoft (R) Windows (R) 5.01. 2600 Service Pack 3	
29.10.2011 11:04	Security	528	An-/Abmeldung	Liese
29.10.2011 11:04	Security	528	An-/Abmeldung	Liese
29.10.2011 11:04	Security	528	An-/Abmeldung	PC
29.10.2011 11:50	System	6006	Der Ereignisprotokolldienst wurde beendet.	
30.10.2011 16:22	System	6005	Der Ereignisprotokolldienst wurde gestartet.	
30.10.2011 16:22	System	6009	Microsoft (R) Windows (R) 5.01. 2600 Service Pack 3	
30.10.2011 16:23	Security	528	An-/Abmeldung	PC
30.10.2011 16:26	Security	528	An-/Abmeldung	Liese

[1] Pfad: C:\ \WINDOWS\system32\config\SysEvent.Evt

30.10.2011 16:26	Security	528	An-/Abmeldung	Liese
30.10.2011 16:53	System	6006	Der Ereignisprotokolldienst wurde beendet.	
31.10.2011 17:24	System	6005	Der Ereignisprotokolldienst wurde gestartet.	
31.10.2011 17:24	System	6009	Microsoft (R) Windows (R) 5.01. 2600 Service Pack 3	
31.10.2011 17:24	Security	528	An-/Abmeldung	PC
31.10.2011 17:25	Security	528	An-/Abmeldung	Liese
31.10.2011 17:25	Security	528	An-/Abmeldung	Liese
31.10.2011 17:34	System	6006	Der Ereignisprotokolldienst wurde beendet.	
03.11.2011 21:35	System	6005	Der Ereignisprotokolldienst wurde gestartet.	
03.11.2011 21:35	System	6009	Microsoft (R) Windows (R) 5.01. 2600 Service Pack 3	
03.11.2011 21:36	Security	528	An-/Abmeldung	PC
03.11.2011 21:36	Security	528	An-/Abmeldung	Liese
03.11.2011 21:36	Security	528	An-/Abmeldung	Liese
03.11.2011 23:16	System	6006	Der Ereignisprotokolldienst wurde beendet.	
04.11.2011 11:33	System	6005	Der Ereignisprotokolldienst wurde gestartet.	
04.11.2011 11:33	System	6009	Microsoft (R) Windows (R) 5.01. 2600 Service Pack 3	
04.11.2011 11:33	Security	528	An-/Abmeldung	PC
04.11.2011 11:33	Security	528	An-/Abmeldung	Liese
04.11.2011 11:33	Security	528	An-/Abmeldung	Liese
04.11.2011 12:12	System	6006	Der Ereignisprotokolldienst wurde beendet.	
04.11.2011 12:35	System	6005	Der Ereignisprotokolldienst wurde gestartet.	
04.11.2011 12:35	System	6009	Microsoft (R) Windows (R) 5.01. 2600 Service Pack 3	
04.11.2011 12:35	Security	528	An-/Abmeldung	PC
04.11.2011 12:36	Security	528	An-/Abmeldung	Liese
04.11.2011 12:36	Security	528	An-/Abmeldung	Liese
04.11.2011 14:30	System	6006	Der Ereignisprotokolldienst wurde beendet.	

Externe Laufwerke

Folgende USB Massenspeicher Geräte waren am Rechner angeschlossen:

Gerätname	Beschreibung	Gerät-Typ	LW	Serie-Nr.	Erstellungsdatum
Intenso Rainbow Line	Intenso Rainbow USB Device	Massenspeicher	E:	10090400010040	21.04.2011 15:12
USB to ATA/ATAPI bridge	SAMSUNG HD502HI USB Device	Massenspeicher		19AA04700FFF	27.04.2011 09:53

[Eintragungen aus dem Registry Schlüssel HKLM\system\ControlSet001\Enum\USBSTOR\ der SYSTEM Registrierungsdatei]

Diese Geräte waren nicht als Asservate verfügbar und sind somit auch nicht im Umfang der Auswertung.

Internetaktivität

Für die Nutzung des Internet konnte ein installierter Mozilla Firefox Version 7.0.0 gefunden werden. Dieser loggt seine Internet Aktivität im entsprechenden Benutzer Verzeichnis in einem Profilverzeichnis zum Mozilla Firefox in **.sqlite* Datenbankdateien mit.

Folgende Eintragungen zum Benutzer Liese konnten ermittelt werden:

Es wurde ein Internetverlauf mit Eintragungen vom 2011-04-21 19:02:42 (MEZ) bis 2011-11-04 14:28:52 (MEZ) ermittelt dieser befindet sich inklusiver aller Eintragungen in Anlage zu diesem Untersuchungsbericht auf DVD Datenträger.

In der Formularhistorie[2] des Mozilla Firefox konnten folgende Eintragungen ermittelt werden.

Feldname	Eintrag	Esrtmals (UTC)	Zuletzt (UTC)
q	gamestar	21.04.2011 17:04	01.06.2011 10:18
q	you tube	24.04.2011 10:36	14.09.2011 18:26
query	sexy cora	24.04.2011 17:34	19.10.2011 18:40
userQuery	sexy cora	24.04.2011 17:38	03.11.2011 20:56
q	bb newes	06.05.2011 08:45	02.06.2011 19:18
q	pentagramm	08.05.2011 15:50	09.05.2011 13:47
q	tropical island	09.05.2011 09:19	09.05.2011 09:19
q	tropical island mit übernachtung	09.05.2011 09:29	09.05.2011 09:29
SD	05.08.2011	09.05.2011 09:32	09.05.2011 09:33
ED	07.08.2011	09.05.2011 09:32	09.05.2011 09:33
q	audio one	09.05.2011 13:33	09.05.2011 13:33
q	db	09.05.2011 19:19	14.06.2011 08:39
REQ0JourneyTime	12	09.05.2011 19:21	09.05.2011 19:21
REQ1JourneyDate	Di, 10.05.11	09.05.2011 19:21	09.05.2011 19:21
REQ1JourneyTime	17:00	09.05.2011 19:21	09.05.2011 19:21
q	Natürliche Mittel gegen Übelkeit	10.05.2011 12:19	04.11.2011 13:05
q	sparkasse zwickau öffnungszeiten	11.05.2011 09:30	11.05.2011 09:30
q	premiere	11.05.2011 10:10	11.05.2011 10:10
q	eintrittspreis von disneyland paris	11.05.2011 11:03	11.05.2011 11:03
q	neckermannnreisen paris disneyland paris	11.05.2011 20:16	11.05.2011 20:16
q	argentinisches essen	12.05.2011 08:40	12.05.2011 08:40
q	rio band	12.05.2011 08:58	12.05.2011 08:58
q	neckermannreisen	12.05.2011 18:31	12.05.2011 18:31
oKalHin_input	Do, 18.08.11	12.05.2011 18:35	12.05.2011 18:35
oKalRueck_input	Fr, 21.10.11	12.05.2011 18:35	12.05.2011 18:35
destination	disneyland patis	12.05.2011 18:42	12.05.2011 18:42

[2] Firefox merkt sich, was Sie in Formularfelder (auch als einzeilige Textfelder bekannt) auf Webseiten eingegeben haben. Nachdem Sie etwas in ein Formularfeld (z.B. in ein Suchfeld [Google Suche]) auf einer Webseite eingegeben haben, wird Ihre Eingabe bei Ihrem nächsten Besuch der Webseite wieder verfügbar sein. [Quelle: support.mozilla.org]

startdate	20 8 2011	12.05.2011 18:42	12.05.2011 18:42
enddate	28beliebig	12.05.2011 18:42	12.05.2011 18:42
oKalHin_input	Mo, 01.08.11	12.05.2011 18:44	12.05.2011 18:44
oKalRueck_input	Fr, 23.09.11	12.05.2011 18:44	12.05.2011 18:44
q	ravenpath	12.05.2011 19:11	12.05.2011 19:11
q	claudia mehner	12.05.2011 19:23	12.05.2011 19:23
q	campingplatz mecklenburg vp surfen	17.05.2011 09:24	17.05.2011 09:24
REQ0JourneyDate	do 19 05	17.05.2011 10:00	17.05.2011 10:00
REQ0JourneyTime	16:00	17.05.2011 10:00	28.05.2011 09:10
REQ0JourneyDate	Do, 19.05.11	18.05.2011 20:41	18.05.2011 20:42
REQ0JourneyTime	15:00	18.05.2011 20:41	18.05.2011 20:42
q	argentienisches restaurant zwickau	21.05.2011 07:34	21.05.2011 07:34
q	prerow zelten	22.05.2011 10:40	22.05.2011 10:40
q	göhren mietwohnwagen	22.05.2011 10:53	22.05.2011 10:53
q	ebay	27.05.2011 18:01	07.10.2011 12:41
q	yappi	27.05.2011 19:15	27.05.2011 19:15
q	zwigge	27.05.2011 19:16	27.05.2011 19:16
q	bahnauskunft	28.05.2011 09:09	28.05.2011 09:09
q	niedersachsen ferien 2012	29.05.2011 09:48	29.05.2011 09:48
q	wohnzelt	29.05.2011 14:38	29.05.2011 14:38
q	Brand Steilwandzelt Chiemsee Plus 400	29.05.2011 14:50	29.05.2011 14:54
q	steilwandzelt	29.05.2011 14:53	29.05.2011 14:53
q	steilwandzelt für 8 personen	29.05.2011 14:58	29.05.2011 14:58
q	wohnzelt 8personen	29.05.2011 15:00	29.05.2011 15:00
q	wulfener hals	29.05.2011 15:03	29.05.2011 15:26
q	preisliste camping wulfenerhals	29.05.2011 15:07	29.05.2011 15:07
q	adobe reader	29.05.2011 15:11	29.05.2011 15:11
q	simon ordnung ist das lösung	29.05.2011 19:24	01.06.2011 22:03
q	better pr	31.05.2011 15:31	31.05.2011 15:31
q	better privacy	31.05.2011 15:31	31.05.2011 15:31
q	saturn	31.05.2011 16:07	31.05.2011 16:07
lmcrit	pink floyd	31.05.2011 16:09	31.05.2011 16:09
lmcrit	bob dylan	31.05.2011 16:15	31.05.2011 16:15
q	deutsche bank zwickau öffnungszeiten	31.05.2011 18:12	31.05.2011 18:12
q	zev	01.06.2011 09:55	01.06.2011 09:55
searchword	22	01.06.2011 09:56	01.06.2011 10:01
q	zwickauer nahverkehr	01.06.2011 09:57	01.06.2011 09:58
q	billy talent tour 20112	04.06.2011 21:22	04.06.2011 21:22
q	fitnessvideo bauch	05.06.2011 18:24	05.06.2011 18:24
REQ0JourneyDate	Do, 16.06.11	14.06.2011 08:40	14.06.2011 08:44
REQ0JourneyTime	06:00	14.06.2011 08:40	14.06.2011 08:44
REQ1JourneyDate	Do, 16.06.11	14.06.2011 08:40	14.06.2011 08:44

REQ1JourneyTime	15:00	14.06.2011 08:40	14.06.2011 08:40
REQ1JourneyTime	16:00	14.06.2011 08:44	14.06.2011 08:44
q	metalkonzrte 2011 sachsen	19.06.2011 18:48	19.06.2011 18:48
q	eluveitie	21.06.2011 16:19	21.06.2011 16:19
q	olaf busch	21.06.2011 16:24	21.06.2011 16:24
q	ursula schiffner	21.06.2011 16:29	21.06.2011 16:29
q	nofx	25.06.2011 15:44	25.06.2011 15:44
q	offspring	25.06.2011 15:47	25.06.2011 15:47
q	katharina mork	25.06.2011 16:26	25.06.2011 16:26
q	hamburger mopo	20.08.2011 10:17	30.10.2011 15:43
q	bungalow eisennach	21.08.2011 12:28	21.08.2011 12:28
q	campingplätze eisenach	21.08.2011 12:45	21.08.2011 12:45
q	bild	21.08.2011 13:01	03.11.2011 20:38
q	gina lisa sexfilm	23.08.2011 08:36	23.08.2011 08:36
q	sexy coras schwester	23.08.2011 09:33	30.08.2011 20:50
q	anne marie ebert	23.08.2011 09:56	23.08.2011 09:56
q	sexy cora	23.08.2011 10:13	14.09.2011 19:12
q	die alm	24.08.2011 10:14	06.09.2011 07:37
q	jasmin geil im keller	24.08.2011 10:53	24.08.2011 10:53
q	bb 11 jasmin porno	24.08.2011 11:28	24.08.2011 11:28
query	rtl computergames	27.08.2011 19:24	27.08.2011 19:24
q	zdf	27.08.2011 19:24	27.08.2011 19:24
query	gina lisa	30.08.2011 19:15	30.08.2011 19:15
q	frankfurter mopo	30.08.2011 19:24	30.08.2011 19:24
q	dirty tracy	30.08.2011 20:51	06.10.2011 17:31
q	neues von rhcp	30.08.2011 20:59	30.08.2011 20:59
q	bushido	30.08.2011 21:14	30.08.2011 21:14
q	jump	06.09.2011 07:46	06.09.2011 07:46
q	sexy barbie	06.09.2011 15:28	06.09.2011 15:28
q	sexy cora news	06.09.2011 15:35	06.10.2011 17:26
q	mdr	06.09.2011 19:08	06.10.2011 17:16
q	big brother	06.09.2011 19:10	14.09.2011 18:54
q	bushido über bb bewohner	06.09.2011 19:18	06.09.2011 19:18
q	ingrid pavic	06.09.2011 19:25	06.09.2011 19:25
q	fabienne bb11	06.09.2011 19:35	06.09.2011 19:35
q	carolin wosnitza	07.09.2011 10:53	07.09.2011 10:53
q	amazon	08.09.2011 12:39	12.09.2011 09:30
q	bild sachsen	08.09.2011 13:44	30.10.2011 15:27
q	bb news	11.09.2011 16:25	03.11.2011 20:52
field-title	vater unser in der hölle	11.09.2011 16:56	11.09.2011 16:56
q	v serie	12.09.2011 09:12	12.09.2011 09:12
q	Sci-Fi-Serien	12.09.2011 09:40	12.09.2011 09:40
q	Sci-Fi-Serien Starhunter 2300	12.09.2011 09:48	12.09.2011 09:48
q	Büromöbel Zwickau	13.09.2011 08:57	13.09.2011 09:06
q	Büromöbel Chemnitz	13.09.2011 09:05	13.09.2011 09:05
search	undercover boss	14.09.2011 18:23	14.09.2011 18:23

search	sexy cora	14.09.2011 18:25	03.11.2011 21:01
search	bb news	14.09.2011 18:26	14.09.2011 18:26
q	cosimo bb	14.09.2011 19:08	14.09.2011 19:08
q	bb barry	16.09.2011 09:32	16.09.2011 09:32
q	neue lied von evance	17.09.2011 10:46	17.09.2011 10:46
q	promiklatsch	17.09.2011 11:17	17.09.2011 11:17
q	vox	20.09.2011 12:39	20.09.2011 12:39
q	sixx	22.09.2011 10:09	22.09.2011 10:09
search	big brother	22.09.2011 10:29	29.10.2011 09:43
q	steam	24.09.2011 13:56	24.09.2011 13:56
query	frauentausch	26.09.2011 16:29	26.09.2011 16:29
q	zwckauer nachrichten	26.09.2011 16:38	07.10.2011 12:35
userQuery	gina lisa	26.09.2011 16:51	26.09.2011 16:51
q	zitrone in kühlschrank	27.09.2011 10:08	27.09.2011 10:08
q	big brother franzi	27.09.2011 10:17	27.09.2011 10:17
q	lebensmittelklarheit	28.09.2011 11:02	28.09.2011 11:02
q	zysten	29.09.2011 09:45	29.09.2011 09:45
q	gestagen	29.09.2011 10:02	29.09.2011 10:02
q	ovaria comp	29.09.2011 10:14	29.09.2011 10:14
q	agnolyt	29.09.2011 10:20	29.09.2011 10:20
q	eierstockzysten hoomophatisch	29.09.2011 10:22	29.09.2011 10:22
q	promiflash	02.10.2011 15:51	03.11.2011 20:59
q	gina lisa news	02.10.2011 15:54	02.10.2011 15:54
q	philip roth	06.10.2011 16:57	06.10.2011 16:57
q	welche daten sind auf der neuen gesundheitskarte	13.10.2011 12:40	13.10.2011 12:40
q	hartz 4	19.10.2011 18:13	19.10.2011 18:13
q	beckenbruch	19.10.2011 18:30	19.10.2011 18:30
q	deichmann werbelied	19.10.2011 18:47	19.10.2011 18:47
q	deichmann	19.10.2011 18:53	19.10.2011 18:53
q	the tamper trap	19.10.2011 18:57	19.10.2011 18:57
q	grimma zeitung	19.10.2011 19:09	19.10.2011 19:09
q	sturz vom dach	19.10.2011 19:26	19.10.2011 19:33
q	sturz vom dach 17 10 2011	19.10.2011 19:31	29.10.2011 09:40
s	sturz vom dach	19.10.2011 20:04	19.10.2011 20:04
q	arbeitslosengeld	24.10.2011 09:09	24.10.2011 09:09
Entgelt	2500	24.10.2011 09:12	24.10.2011 09:12
Entgelt	4000	24.10.2011 09:13	24.10.2011 09:13
q	erst selbstständig dann arbeitslos	24.10.2011 09:29	24.10.2011 09:29
q	atu zwickau	24.10.2011 10:08	24.10.2011 10:08
q	zwickau news	29.10.2011 09:15	04.11.2011 11:09
q	mdr jump	03.11.2011 20:43	03.11.2011 20:43
search	gina lisa	03.11.2011 21:01	03.11.2011 21:01
q	juliane schiffner peine	03.11.2011 21:38	03.11.2011 21:46
q	sexy cora co	03.11.2011 22:09	03.11.2011 22:09
q	bid	04.11.2011 10:34	04.11.2011 10:34

q	sachsennachrichten	04.11.2011 10:40	04.11.2011 10:40
q	sachsen news	04.11.2011 10:57	04.11.2011 10:57
q	promi news	04.11.2011 11:11	04.11.2011 11:11
q	autounfall sachsen 31 10	04.11.2011 11:39	04.11.2011 11:39
q	auto unfall mitteldeutschland	04.11.2011 11:50	04.11.2011 11:50
q	autounfall,1 11	04.11.2011 12:10	04.11.2011 12:10
q	zwickauer news	04.11.2011 12:11	04.11.2011 12:11
q	blldl	04.11.2011 12:15	04.11.2011 12:15
query	bild 3 11	04.11.2011 12:24	04.11.2011 12:24
q	sachsen radio	04.11.2011 12:43	04.11.2011 12:43
q	greenpeace	04.11.2011 13:07	04.11.2011 13:07
q	gegen pelze	04.11.2011 13:13	04.11.2011 13:13
q	biobauern zwickau	04.11.2011 13:26	04.11.2011 13:26

Folgende Eintragungen zum Benutzer PC konnten ermittelt werden:

Es wurde ein internetverlauf mit Eintragungen vom 2011-04-21 18:47:04 (MEZ) bis 2011-09-29 10:54:02 (MEZ) ermittelt dieser befindet sich inklusiver aller Eintragungen in Anlage zu diesem Untersuchungsbericht auf DVD Datenträger.

In der Formularhistorie[3] des Mozilla Firefox konnten folgende Eintragungen ermittelt werden.

Feldname	Eintrag	Esrtmals (UTC)	Zuletzt
q	gamestar	21.04.2011 17:20	21.04.2011 17:20
q	direct x	23.04.2011 15:59	23.04.2011 15:59
q	heroes v patch	23.04.2011 16:01	23.04.2011 16:01
searchstring	heroes v	23.04.2011 16:03	23.04.2011 16:04
q	7zip	23.04.2011 16:32	23.04.2011 16:32
q	win xp automatische benutzerabmeldung ausschalten	03.05.2011 10:49	03.05.2011 10:49
q	batman kamera probleme	06.05.2011 14:04	06.05.2011 14:04
q	patch spider man 2	09.05.2011 12:40	09.05.2011 12:40
q	Thrustmaster	09.05.2011 12:48	09.05.2011 12:48
q	thrustmapper	09.05.2011 13:01	09.05.2011 13:01
q	Thrustmapper download	09.05.2011 13:14	09.05.2011 13:14
keywords	Thrustmapper	09.05.2011 13:14	09.05.2011 13:14
q	bild	29.09.2011 08:33	29.09.2011 08:33

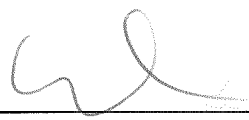
Emails

Emails konnten keine festgestellt werden.

[3] Firefox merkt sich, was Sie in Formularfelder (auch als einzeilige Textfelder bekannt) auf Webseiten eingegeben haben. Nachdem Sie etwas in ein Formularfeld (z.B. in ein Suchfeld [Google Suche]) auf einer Webseite eingegeben haben, wird Ihre Eingabe bei Ihrem nächsten Besuch der Webseite wieder verfügbar sein. [Quelle: support.mozilla.org]

Bild und Videodateien

Es wurden keinerlei existierenden oder gelöschten privaten Foto oder Videoaufnahmen auf dem Asservat ermittelt. Eine Tiefen-Untersuchung auf ehemals existierende Bilddateien steht noch aus und wird nachgereicht.



Diplom-Ingenieur (BA) für Informationstechnik
Ronny Bodach
Kriminalkommissar

Anhang A

Sicherungsprotokolle

Asservat EDV01

Created By AccessData® FTK® Imager 3.0.0.1442 101005

Case Information:
Acquired using: ADI3.0.0.1442
Case Number: 2135/11/173440
Evidence Number: Asservat EDV01
Unique description: PC AMD ASUS Serial 649081203942
Examiner: Bodach, KK
Notes: interne HDD 250 GB mit Brandbelag auf Oberfläche, Maxtor Model STM3250318AS Serial number 5VY0RA1Q

Information for D:\2135-11-173440\Asservat EDV01 - PC AMD aus Brandwohnung\2135-11-173440-AssEDV01-250GB:

Physical Evidentiary Item (Source) Information:
[Drive Geometry]
Cylinders: 30.401
Tracks per Cylinder: 255
Sectors per Track: 63
Bytes per Sector: 512
Sector Count: 488.397.168
[Physical Drive Information]
Drive Model: Seagate STM3250318AS SCSI Disk Device
Drive Serial Number: 5VY0RA1Q
Drive Interface Type: SCSI
Source data size: 238475 MB
Sector count: 488397168
[Computed Hashes]
MD5 checksum: b7f58234110527cf2f3bf68ff736eb5e
SHA1 checksum: ced30ab8cba031a24bede7e47a777d247cd7cda8

Image Information:
Acquisition started: Sun Nov 06 09:42:57 2011
Acquisition finished: Sun Nov 06 10:48:52 2011
Segment list:
D:\2135-11-173440\Asservat EDV01 - PC AMD aus Brandwohnung\2135-11-173440-AssEDV01-250GB.E01
D:\2135-11-173440\Asservat EDV01 - PC AMD aus Brandwohnung\2135-11-173440-AssEDV01-250GB.E02
D:\2135-11-173440\Asservat EDV01 - PC AMD aus Brandwohnung\2135-11-173440-AssEDV01-250GB.E03
D:\2135-11-173440\Asservat EDV01 - PC AMD aus Brandwohnung\2135-11-173440-AssEDV01-250GB.E04
D:\2135-11-173440\Asservat EDV01 - PC AMD aus Brandwohnung\2135-11-173440-AssEDV01-250GB.E05
D:\2135-11-173440\Asservat EDV01 - PC AMD aus Brandwohnung\2135-11-173440-AssEDV01-250GB.E06
D:\2135-11-173440\Asservat EDV01 - PC AMD aus Brandwohnung\2135-11-173440-AssEDV01-250GB.E07
D:\2135-11-173440\Asservat EDV01 - PC AMD aus Brandwohnung\2135-11-173440-AssEDV01-250GB.E08
D:\2135-11-173440\Asservat EDV01 - PC AMD aus Brandwohnung\2135-11-173440-AssEDV01-250GB.E09
D:\2135-11-173440\Asservat EDV01 - PC AMD aus Brandwohnung\2135-11-173440-AssEDV01-250GB.E10
D:\2135-11-173440\Asservat EDV01 - PC AMD aus Brandwohnung\2135-11-173440-AssEDV01-250GB.E11
D:\2135-11-173440\Asservat EDV01 - PC AMD aus Brandwohnung\2135-11-173440-AssEDV01-250GB.E12
D:\2135-11-173440\Asservat EDV01 - PC AMD aus Brandwohnung\2135-11-173440-AssEDV01-250GB.E13
D:\2135-11-173440\Asservat EDV01 - PC AMD aus Brandwohnung\2135-11-173440-AssEDV01-250GB.E14
D:\2135-11-173440\Asservat EDV01 - PC AMD aus Brandwohnung\2135-11-173440-AssEDV01-250GB.E15
D:\2135-11-173440\Asservat EDV01 - PC AMD aus Brandwohnung\2135-11-173440-AssEDV01-250GB.E16
D:\2135-11-173440\Asservat EDV01 - PC AMD aus Brandwohnung\2135-11-173440-AssEDV01-250GB.E17
D:\2135-11-173440\Asservat EDV01 - PC AMD aus Brandwohnung\2135-11-173440-AssEDV01-250GB.E18
D:\2135-11-173440\Asservat EDV01 - PC AMD aus Brandwohnung\2135-11-173440-AssEDV01-250GB.E19
D:\2135-11-173440\Asservat EDV01 - PC AMD aus Brandwohnung\2135-11-173440-AssEDV01-250GB.E20
D:\2135-11-173440\Asservat EDV01 - PC AMD aus Brandwohnung\2135-11-173440-AssEDV01-250GB.E21
D:\2135-11-173440\Asservat EDV01 - PC AMD aus Brandwohnung\2135-11-173440-AssEDV01-250GB.E22
D:\2135-11-173440\Asservat EDV01 - PC AMD aus Brandwohnung\2135-11-173440-AssEDV01-250GB.E23
D:\2135-11-173440\Asservat EDV01 - PC AMD aus Brandwohnung\2135-11-173440-AssEDV01-250GB.E24
D:\2135-11-173440\Asservat EDV01 - PC AMD aus Brandwohnung\2135-11-173440-AssEDV01-250GB.E25
D:\2135-11-173440\Asservat EDV01 - PC AMD aus Brandwohnung\2135-11-173440-AssEDV01-250GB.E26
D:\2135-11-173440\Asservat EDV01 - PC AMD aus Brandwohnung\2135-11-173440-AssEDV01-250GB.E27
D:\2135-11-173440\Asservat EDV01 - PC AMD aus Brandwohnung\2135-11-173440-AssEDV01-250GB.E28
D:\2135-11-173440\Asservat EDV01 - PC AMD aus Brandwohnung\2135-11-173440-AssEDV01-250GB.E29
D:\2135-11-173440\Asservat EDV01 - PC AMD aus Brandwohnung\2135-11-173440-AssEDV01-250GB.E30
D:\2135-11-173440\Asservat EDV01 - PC AMD aus Brandwohnung\2135-11-173440-AssEDV01-250GB.E31
D:\2135-11-173440\Asservat EDV01 - PC AMD aus Brandwohnung\2135-11-173440-AssEDV01-250GB.E32

Image Verification Results:
Verification started: Sun Nov 06 10:48:54 2011
Verification finished: Sun Nov 06 11:21:25 2011
MD5 checksum: b7f58234110527cf2f3bf68ff736eb5e : verified
SHA1 checksum: ced30ab8cba031a24bede7e47a777d247cd7cda8 : verified