

Referentie/Documentnummer: 004

Betreft: onderzoek laptopdata ten behoeve van digitaal onderzoek

Datum: 19-5-2024

Rapporteur: [REDACTED] Ivan, [REDACTED]

Bevindingen

In het kader van het onderzoek privé laptop Anton de Bok hebben wij op 19 mei 2024 op verzoek van Dennis een onderzoek ingesteld in het kader van de privé laptop van Anton de Bok naar de data die was veiliggesteld. Dit betrof de data van een zwarte privé laptop van vermoedelijk het merk Fujitsu, type Livebook E-series met 256GB opslag met een extra SD-kaart van vermoedelijk het merk Kingston, type micro SD-adapter met een opslagcapaciteit van 16GB, opgeslagen in de imagebestanden met de namen HardschijfImageA1Sc3.E01 en BitlockImageA1Sc3.E01. De HardschijfImageA1Sc3.E01 bevat de data van de 256GB opslag en de BitlockImageA1Sc3.E01 bevat de data van de SD-kaart 16GB.

Tijdens het onderzoek in de data van het imagebestand HardschijfImageA1Sc3.E01, de kopie van de data van de hardeschip in de privé laptop, zagen wij het volgende:

De hardeschip bevat twee partities die zijn gemaakt dit is waargenomen met behulp van FTK Imager 4.7.1.2. De eerste partitie bevat FAT32 en een map die EFI is genoemd met een BOOT en ubuntu map. In de ubuntu map is een grub.cfg file aangetroffen en drie .efi files. Dit zijn files om ubuntu te kunnen gebruiken.

Op de tweede partitie zijn meer mappen gevonden met behulp van FTK-imager. Wij hebben waargenomen dat op deze partitie veel verschillende licenties zijn voor software, waarvan veel verschillende talen zijn geïmplementeerd. Hieruit valt op dat talen zoals morse en braille zijn toegevoegd.

Er is waargenomen dat er .mod files ontstaan. De .mod files zijn geëncrypt, echter hebben twee van de .mod files de tekst "password" erin staan.

Er is een blacklist lijst waargenomen waarin verdere configuraties staan.

In het waargenomen mapje mythes dat gevonden is door het pad te volgen [root] > usr > share > mythes, staan twee bestanden. Deze bestanden bevatten verschillende plaatsnamen en staan er termen in zoals .22 caliber en firearm.

Er is een mail gevonden dat vermoedelijk werk gerelateerd is. Verder zijn er meerdere afbeeldingen gevonden van vermoedelijk kinderknuffels die bewerkt zijn. Er zijn 59661 afbeeldingen gevonden met behulp van autopsy 4.21.0, één video en 135 audio bestanden.

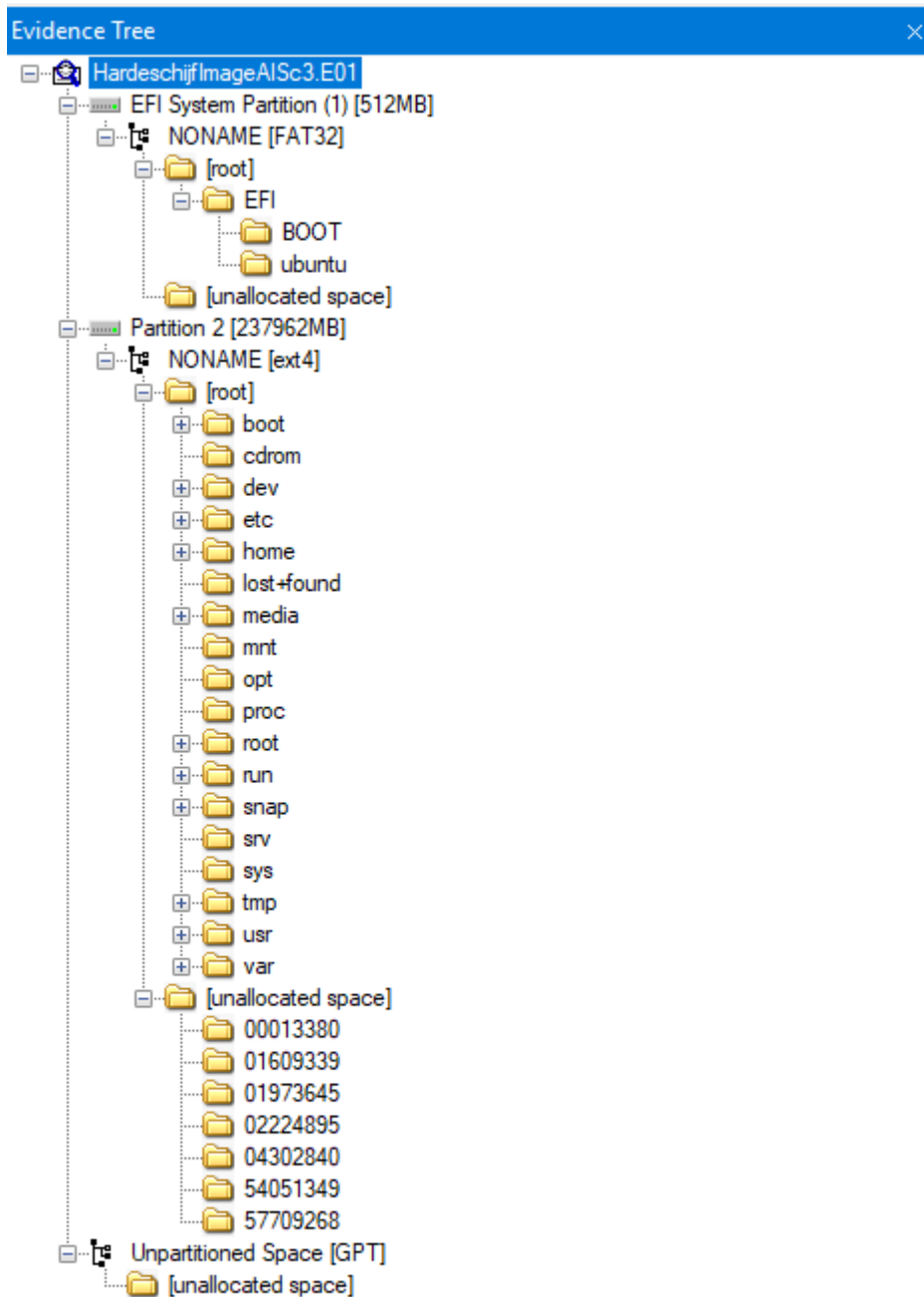
De analyse van het programma autopsy 4.21.0 heeft 18 interessante items aangegeven. De interessante items duiden op encryptie programma's waardoor de bestanden zijn versleuteld.

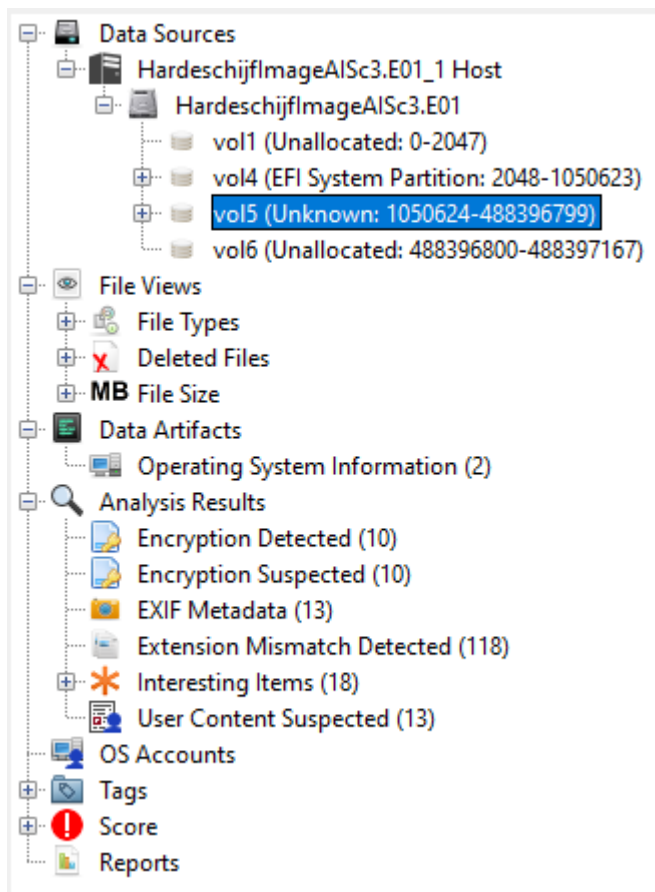
De shadow bestanden zijn verwijderd van de hardeschip waar vermoedelijk wachtwoorden op hebben gestaan. Deze vermoedelijke wachtwoorden hebben wij niet terug kunnen vinden.

Er is een database waargenomen die wij hebben geopend door middel van DB Browser for SQLite version 3.12.2 met SQLite Version 3.35.5. In deze database hebben wij geen gegevens waargenomen.

Tijdens het onderzoek van de data van het imagebestand BitlockImageAISc3.E01, de kopie van de data van de SD-kaart, zagen wij het volgende:














De SD-kaart bevat één partitie die encrypt is met FAT32 Bitlock. Hierdoor is er door ons niet verder in te zien wat de SD-kaart voor informatie bevat. Hieruit is niet op te maken of dit opslagmedium heeft kunnen zorgen voor het TOR verkeer dat is opgetreden.

Foto's (indien van toepassing)



Evidence Tree		File List			
HardschijfImageAISC3.E01		Name	Size	Type	Date Modified
EFI System Partition (1) [512MB]		BOOTX64.CSV	1	Regular File	01/12/2021 12:31:42
NONAME [FAT32]		grub.cfg	1	Regular File	01/12/2021 12:31:42
[root]		grubx64.efi	1,694	Regular File	01/12/2021 12:31:42
EFI		mmx64.efi	837	Regular File	01/12/2021 12:31:42
BOOT		shimx64.efi	934	Regular File	01/12/2021 12:31:42
ubuntu					
[unallocated space]					
Partition 2 [237962MB]					
NONAME [ext4]					

File List

Name	Size	Type	Date Modified
 01609339	8	Unallocated Sp...	
 01609355	8	Unallocated Sp...	
 01609468	68	Unallocated Sp...	
 01609690	4	Unallocated Sp...	
 01609693	16	Unallocated Sp...	
 01609700	24	Unallocated Sp...	
 01609727	120	Unallocated Sp...	
 01609832	4	Unallocated Sp...	
 01610016	4	Unallocated Sp...	
 01610037	48	Unallocated Sp...	
 01610085	112	Unallocated Sp...	
 01610208	4	Unallocated Sp...	
 01610235	24	Unallocated Sp...	

```

src/glx/eval.c
src/glx/glxclient.h
src/glx/glxcmds.c
src/glx/glxcurrent.c
src/glx/glxext.cGreg
src/glx/packrender.h
src/glx/packsingle.h
src/glx/pixel.c
src/glx/pixelstore.c
src/glx/render2.c
src/glx/renderpix.c
src/glx/single2.c
src/glx/singlepix.c
src/glx/vertarr.c

```

Copyright: 1991-2000 Silicon Graphics, Inc.
License: SGI

Files: src/getopt
Copyright: 2000 The NetBSD Foundation, Inc.
License: BSD-2-clause














Files: src/gtest/include src/gtest/src
Copyright: 2008-2015 Google, Inc.
License: BSD-3-google

Files: debian
Copyright: 2006, Thierry Reding <thierry@gilfi.de>
License: GPL

License: MIT

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

File List

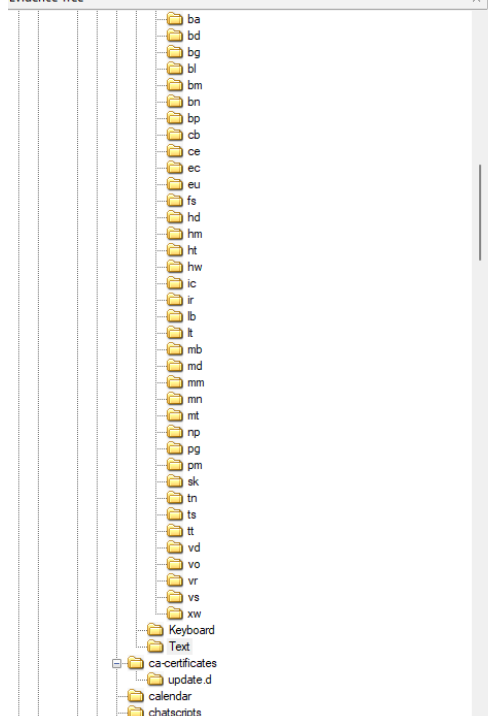
Name	Size	Type	Date Modified
 test_blockarg.mod	3	Regular File	01/12/2021 12:31:42
 testspeed.mod	4	Regular File	01/12/2021 12:31:41
 testload.mod	4	Regular File	01/12/2021 12:31:41
 test.mod	8	Regular File	01/12/2021 12:31:42
 terminfo.mod	19	Regular File	01/12/2021 12:31:41
 terminal.mod	7	Regular File	01/12/2021 12:31:42
 terminal.lst	1	Regular File	01/12/2021 12:31:42
 tar.mod	5	Regular File	01/12/2021 12:31:42
 syslinuxcfg.mod	30	Regular File	01/12/2021 12:31:42
 strtoull_test.mod	4	Regular File	01/12/2021 12:31:42
 squash4.mod	10	Regular File	01/12/2021 12:31:42
 spkmodem.mod	4	Regular File	01/12/2021 12:31:42
 smbios.mod	9	Regular File	01/12/2021 12:31:42

```














iat_keyboard: at_keyboard
iserial: serial
iserial_*: serial
oaudio: morse
ocbmemc: cbmemc
ogfxterm: gfxterm
oserial: serial
oserial_*: serial
ospkmodem: spkmodem

```

Evidence Tree



File List

Name	Size	Type	Date Modified
 alias.tti	3	Regular File	03/03/2020 20:32:07
 ar.ttb	9	Regular File	03/03/2020 20:32:07
 as.ttb	1	Regular File	03/03/2020 20:32:07
 ascii-basic.tti	1	Regular File	03/03/2020 20:32:07
 awa.ttb	1	Regular File	03/03/2020 20:32:07
 bengali.tti	5	Regular File	03/03/2020 20:32:07
 bg.ttb	2	Regular File	03/03/2020 20:32:07
 bh.ttb	1	Regular File	03/03/2020 20:32:07
 blocks.tti	2	Regular File	03/03/2020 20:32:07
 bn.ttb	1	Regular File	03/03/2020 20:32:07
 bo.ttb	1	Regular File	03/03/2020 20:32:07
 boxes.tti	12	Regular File	03/03/2020 20:32:07
 bra.ttb	1	Regular File	03/03/2020 20:32:07

```

#####
# BRLTTY - A background process providing access to the console screen (when in
#      text mode) for a blind person using a refreshable braille display.
#
# Copyright (C) 2008-2019 by The BRLTTY Developers.
#
# BRLTTY comes with ABSOLUTELY NO WARRANTY.
#
# This is free software, placed under the terms of the
# GNU Lesser General Public License, as published by the Free Software
# Foundation; either version 2.1 of the License, or (at your option) any
# later version. Please see the file LICENSE-LGPL for details.
#
# Web Page: http://brlTTY.app/
#
# This software is maintained by Dave Mielke <dave@mielke.cc>.
#####














# BRLTTY Text Table - Assamese

include bengali.tti
include ascii-basic.tti

include common.tti

```

File List

Name	Size	Type	Date Modified
 part_sun.mod	3	Regular File	01/12/2021 12:31:42
 part_sunpc.mod	3	Regular File	01/12/2021 12:31:42
 password.mod	4	Regular File	01/12/2021 12:31:42
 password_pbkdf2.mod	5	Regular File	01/12/2021 12:31:42
 pata.mod	8	Regular File	01/12/2021 12:31:42
 pbkdf2.mod	3	Regular File	01/12/2021 12:31:42
 pbkdf2_test.mod	4	Regular File	01/12/2021 12:31:42
 pcidump.mod	4	Regular File	01/12/2021 12:31:42
 pgp.mod	19	Regular File	01/12/2021 12:31:42
 play.mod	5	Regular File	01/12/2021 12:31:42
 png.mod	11	Regular File	01/12/2021 12:31:42
 priority_queue.mod	3	Regular File	01/12/2021 12:31:42
 probe.mod	5	Regular File	01/12/2021 12:31:42

```

0c0 00 00 41 54 49 89 FC BF-00 04 00 00 55 48 89 F5  ··ATI·û· ···UH·õ
0d0 53 FF D0 48 85 C0 75 11-48 B8 00 00 00 00 00 00  SÿDH·Àu·H, ·····
0e0 00 00 8B 28 E9 80 00 00-00 48 89 C3 48 89 EF 48  ···(é· ···H·ÃH·iH
0f0 B8 00 00 00 00 00 00 00-00 FF D0 BA FF 03 00 00  , ······ÿD°ÿ· ···
100 48 89 EE 48 89 DF 3D FF-03 00 00 0F 4F C2 48 63  H·iH·B=ÿ· ···OÃHc
110 D0 48 B8 00 00 00 00 00-00 00 00 FF D0 48 89 DA  DH, ······ÿDH·Ú
120 4C 89 E7 48 BE 00 00 00-00 00 00 00 00 48 B8 00  L·çH% ······H, ·
130 00 00 00 00 00 00 00 FF-D0 89 C5 85 C0 74 11 48  ······ÿD·Ã·Àt·H
140 B8 00 00 00 00 00 00 00 00-00 48 89 DF FF D0 EB 19  , ······H·BÿDë·
150 48 B8 00 00 00 00 00 00 00-00 00 48 8B 38 48 B8 00  H, ······H·8H, ·
160 00 00 00 00 00 00 00 FF-D0 89 E8 5B 5D 41 5C C3  ······ÿD·è·]A\Ã
170 F3 0F 1E FA 83 FE 02 74-1D 48 BE 00 00 00 00 00 00  ó·ú·p·t·H% ·····
180 00 00 00 BF 12 00 00 00-31 C0 48 BA 00 00 00 00 00  ···· ···lÃH° ····
190 00 00 00 00 FF E2 48 8B-72 08 48 8B 3A 48 B8 00  ····ÿâH·r·H·:H, ·
1a0 00 00 00 00 00 00 00 FF-E0 F3 0F 1E FA 50 48 89  ······ÿâó·úPH·
1b0 F8 45 31 C0 48 BA 00 00-00 00 00 00 00 00 48 A3  øE1ÃH° ······Hè
1c0 00 00 00 00 00 00 00 00-48 B9 00 00 00 00 00 00  ······H¹ ·····
1d0 00 00 48 BE 00 00 00 00-00 00 00 00 48 BF 00 00  ··H% ······H· ··
1e0 00 00 00 00 00 00 48 B8-00 00 00 00 00 00 00 00  ······H, ······
1f0 FF D0 48 A3 00 00 00 00-00 00 00 00 5A C3 F3 0F  ÿDHè ······ZÃó·
200 1E FA 48 B8 00 00 00 00-00 00 00 00 48 8B 38 48  ·úH, ······H·8H
210 B8 00 00 00 00 00 00 00 00-00 FF E0 61 63 63 65 73  , ······ÿâacces
220 73 20 64 65 6E 69 65 64-00 74 77 6F 20 61 72 67  s denied two arg
230 75 6D 65 6E 74 73 20 65-78 70 65 63 74 65 64 00  uments expected·
240 53 65 74 20 75 73 65 72-20 70 61 73 73 77 6F 72  Set user passwor
250 64 20 28 70 6C 61 69 6E-74 65 78 74 29 2E 20 55  d (plaintext). U
260 6E 72 65 63 6F 6D 6D 65-6E 64 65 64 20 61 6E 64  nrecommended and
270 20 69 6E 73 65 63 75 72-65 2E 00 55 53 45 52 20  insecure·USER
280 50 41 53 53 57 4F 52 44-00 70 61 73 73 77 6F 72  PASSWORD·passwor
290 64 00 00 00 00 00 00 00 00-4C 49 43 45 4E 53 45 3D  d· ······LICENSE=
2a0 47 50 4C 76 33 2B 00 00-63 72 79 70 74 6F 00 6E  GPLv3+· ·crypto·n
2b0 6F 72 6D 61 6C 00 70 61-73 73 77 6F 72 64 00 00  ormal·password·

```

Evidence Tree

- np
- pg
- pm
- sk
- tn
- ts
- tt
- vd
- vo
- vr
- vs
- xw
- Keyboard
- Text
- ca-certificates
- update.d
- calendar
- chatscripts
- console-setup
- cached_ISO-8859-1.acm.gz
- cached_ISO-8859-1_del.kmap.gz
- cached_Uni2-Fixed16.psf.gz
- cached_UTF-8_del.kmap.gz
- Uni2-Fixed16.psf.gz
- cracklib
- cron.d
- cron.daily
- cron.hourly
- cron.monthly
- cron.weekly
- cups
- interfaces
- ppd
- ssl
- cupshelpers
- dbus-1
- session.d
- system.d
- dconf
- db
- ibus.d
- profile
- default

Custom Content Sources

Evidence:File System|Path|File

Options

New

Edit

Remove

Remove All

Create Image

File List

Name	Size	Type	Date Modified
.placeholder	1	Regular File	13/02/2020 20:44:42
0anacron	1	Regular File	16/07/2019 18:19:13
apport	1	Regular File	04/12/2019 20:25:28
apt-compat	2	Regular File	09/04/2020 10:21:07
bsdmainutils	1	Regular File	29/12/2017 09:02:08
cracklib-runtime	1	Regular File	19/11/2019 15:14:51
dpkg	2	Regular File	05/09/2019 21:05:14
logrotate	1	Regular File	21/01/2019 10:11:39
man-db	2	Regular File	25/02/2020 17:13:45
popularity-contest	5	Regular File	18/07/2019 15:45:22
update-notifier-common	1	Regular File	14/05/2021 19:02:18

```

# regenerate man database
if [ -x /usr/bin/mandb ]; then
    # --pidfile /dev/null so it always starts; mandb isn't really a daemon,
    # but we want to start it like one.
    start-stop-daemon --start --pidfile /dev/null \
        --oknodo --chuid man $iosched_idle -- -c \
        "find /var/cache/man -type f -name '*.gz' -atime +6 -print0 | \
        xargs -r0 xm -f"
fi

# regenerate man database
if [ -x /usr/bin/mandb ]; then
    # --pidfile /dev/null so it always starts; mandb isn't really a daemon,
    # but we want to start it like one.
    start-stop-daemon --start --pidfile /dev/null \
        --oknodo --chuid man $iosched_idle -- -c \
        "find /var/cache/man -type f -name '*.gz' -atime +6 -print0 | \
        xargs -r0 xm -f"
fi

exit 0

```

Evidence Tree

- nfs-top
- panic
- inserv.conf.d
- iproute2
- rt_protos.d
- rt_tables.d
- kernel
- header_postinst.d
- install.d
- postinst.d
- posttm.d
- preinst.d
- premd
- ld.so.conf.d
- ldap
- libblockdev
- conf.d
- libn1-3
- libpaper.d
- libreoffice
- lighttpd
- conf-available
- conf-enabled
- logcheck
- ignore.d.paranoid
- ignore.d.server
- logrotate.d
- modprobe.d
- modules-load.d

File List

Name	Size	Type	Date Modified
alsa-base.conf	3	Regular File	31/07/2015 03:42:17
amd64-microcode-blacklist.conf	1	Regular File	16/02/2020 07:43:50
blacklist-ath_pci.conf	1	Regular File	12/03/2020 13:15:28
blacklist-firewire.conf	1	Regular File	12/03/2020 13:15:28
blacklist-framebuffer.conf	1	Regular File	12/03/2020 13:15:28
blacklist-modem.conf	1	Regular File	31/07/2015 03:42:17
blacklist-oss.conf	1	Symbolic Link	01/12/2021 12:26:03
blacklist-rare-network.conf	1	Regular File	12/03/2020 13:15:28
blacklist.conf	2	Regular File	12/03/2020 13:15:28
dkms.conf	1	Regular File	22/01/2020 15:43:24
intel-microcode-blacklist.conf	1	Regular File	26/05/2021 04:14:00
iwwifi.conf	1	Regular File	12/03/2020 13:15:28

```

# Select the legacy firewire stack over the new CONFIG_FIREWIRE one.

blacklist ohci1394
blacklist sbp2
blacklist dv1394
blacklist raw1394
blacklist video1394

#blacklist firewire-ohci
#blacklist firewire-sbp2

```


Evidence Tree

- menu
- metainfo
- mime
- mime-info
- misc
- mobile-broadband-provider-info
- ModemManager
- mousetweaks
- mozilla
- mysql-common
- mythes
- nano
- nautilus-share
- netplan
- openvpn
- orca
- org.gnome.Characters
- os-prober
- p11-kit
- package-data-downloads
- PackageKit
- pam
- pam-configs
- perl
- perl5
- perl-openssl-defaults
- pixmap
- pkgconfig
- plymouth
- prnm2ppa
- polkit-1
- poppler
- popularity-contest
- ppd
- ppp
- publicsuffix
- pulseaudio
- pyshared
- python3
- python-apt
- qt5
- readline
- remmina

File List

Name	Size	Type	Date Modified
th_en_US_v2.dat	18,119	Regular File	07/04/2020 15:26:48
th_en_US_v2.idx	2,974	Regular File	14/04/2020 14:22:54

Custom Content Sources

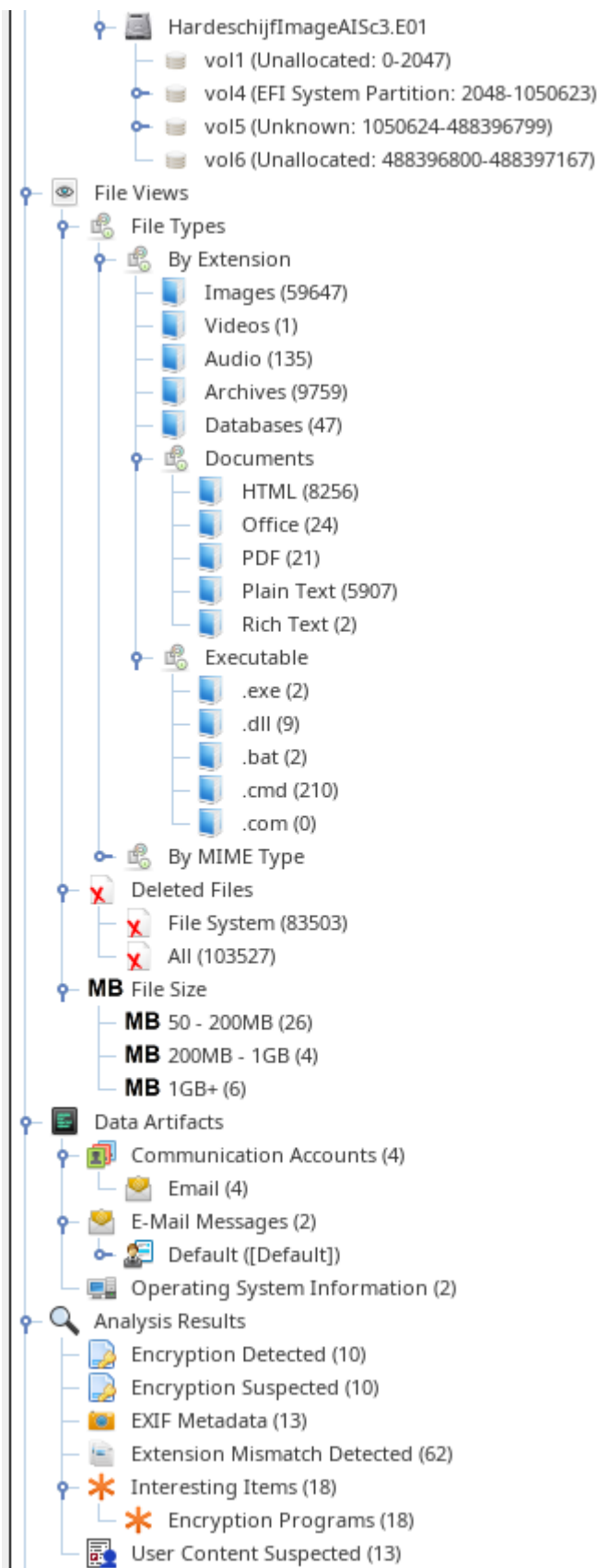
Evidence:File System Path File	Options

New Edit Remove Remove All Create Image

```

0000150 65 6C 61 74 65 64 20 74-65 72 6D 29 0A 2E 32 32 elated term)..22
0000160 20 63 61 6C 69 62 65 72-7C 31 0A 28 61 64 6A 29 caliber|l-(adj)
0000170 7C 2E 32 32 2D 63 61 6C-69 62 65 72 7C 2E 32 32 |.22-caliber|.22
0000180 20 63 61 6C 69 62 72 65-7C 2E 32 32 2D 63 61 6C calibre|.22-cal
0000190 69 62 72 65 7C 64 69 61-6D 65 74 65 72 7C 64 69ibre|diameter|di
00001a0 61 6D 20 28 72 65 6C 61-74 65 64 20 74 65 72 6D am (related term
00001b0 29 0A 2E 32 32 2D 63 61-6C 69 62 72 65 7C 31 0A )..22 calibre|l-
00001c0 28 61 64 6A 29 7C 2E 32-32 2D 63 61 6C 69 62 65 (adj)|.22 calibe
00001d0 72 7C 2E 32 32 2D 63 61-6C 69 62 65 72 7C 2E 32 r|.22-caliber|.2
00001e0 32 2D 63 61 6C 69 62 72-65 7C 64 69 61 6D 65 74 2-calibre|diamet
00001f0 65 72 7C 64 69 61 6D 20-28 72 65 6C 61 74 65 64 er|diam (related
0000200 20 74 65 72 6D 29 0A 2E-33 38 2D 63 61 6C 69 62 term)..38-calib
0000210 65 72 7C 31 0A 28 61 64-6A 29 7C 2E 33 38 2D 63 er|l-(adj)|.38 c
0000220 61 6C 69 62 65 72 7C 2E-33 38 2D 63 61 6C 69 62 aliber|.38 calib
0000230 72 65 7C 2E 33 38 2D 63-61 6C 69 62 72 65 7C 64 rel|.38-calibre|d
0000240 69 61 6D 65 74 65 72 7C-64 69 61 6D 20 28 72 65 iameter|diam (re
0000250 6C 61 74 65 64 20 74 65-72 6D 29 0A 2E 33 38 2D lated term)..38-
0000260 63 61 6C 69 62 72 65 7C-31 0A 28 61 64 6A 29 7C calibre|l-(adj)|
0000270 2E 33 38 2D 63 61 6C 69-62 65 72 7C 2E 33 38 2D .38 calibre|.38-
0000280 63 61 6C 69 62 65 72 7C-2E 33 38 2D 63 61 6C 69 calibre|.38 cali
0000290 62 72 65 7C 64 69 61 6D-65 74 65 72 7C 64 69 61 bre|diameter|dia
00002a0 6D 20 28 72 65 6C 61 74-65 64 20 74 65 72 6D 29 m (related term)
00002b0 0A 2E 33 38 2D 63 61 6C-69 62 65 72 7C 31 0A 28 ..38 calibre|l-(
00002c0 61 64 6A 29 7C 2E 33 38-2D 63 61 6C 69 62 65 72 adj)|.38-caliber
00002d0 7C 2E 33 38 2D 63 61 6C-69 62 72 65 7C 2E 33 38 |.38 calibre|.38
00002e0 2D 63 61 6C 69 62 72 65-7C 64 69 61 6D 65 74 65 -calibre|diameter
00002f0 72 7C 64 69 61 6D 20 28-72 65 6C 61 74 65 64 20 r|diam (related
0000300 74 65 72 6D 29 0A 2E 33-38 2D 63 61 6C 69 62 72 term)..38 calibr
0000310 65 7C 31 0A 28 61 64 6A-29 7C 2E 33 38 2D 63 61 e|l-(adj)|.38 ca
0000320 6C 69 62 65 72 7C 2E 33-38 2D 63 61 6C 69 62 65 liber|.38-calibe
0000330 72 7C 2E 33 38 2D 63 61-6C 69 62 72 65 7C 64 69 r|.38-calibre|di
0000340 61 6D 65 74 65 72 7C 64-69 61 6D 20 28 72 65 6C ameter|diam (rel
0000350 61 74 65 64 20 74 65 72-6D 29 0A 2E 34 35 2D 63 ated term)..45-c
0000360 61 6C 69 62 65 72 7C 31-0A 28 61 64 6A 29 7C 2E aliber|l-(adj)|.
0000370 34 35 2D 63 61 6C 69 62-65 72 7C 2E 34 35 2D 63 45 calibre|.45 c
0000380 61 6C 69 62 72 65 7C 2E-34 35 2D 63 61 6C 69 62 alibre|.45-calib
0000390 72 65 7C 64 69 61 6D 65-74 65 72 7C 64 69 61 6D re|diameter|diam
00003a0 20 28 72 65 6C 61 74 65-64 20 74 65 72 6D 29 0A (related term)
00003b0 2E 34 35 2D 63 61 6C 69-62 72 65 7C 31 0A 28 61 .45-calibre|l-(a
00003c0 64 6A 29 7C 2E 34 35 2D-63 61 6C 69 62 65 72 7C dj)|.45 calibre|
00003d0 2E 34 35 2D 63 61 6C 69-62 65 72 7C 2E 34 35 2D .45-caliber|.45

```



RAPPORTAGE INZAKE IT FORENSISCH ONDERZOEK

Listing											
Encryption Programs											
Table Thumbnail Summary											
Save Table as CSV											
Source Name	S	C	O	Source Type	Score	Conclusion	Configuration	Justification	Category	File Path	Modifie
luks.mod				File	Likely Notable		Encryption Programs		LUKS(Linux)	/img_HardeschijfImageAISC3.E01/vol_vo15/usr/lib/gru...	2021-08
luks.mod				File	Likely Notable		Encryption Programs		LUKS(Linux)	/img_HardeschijfImageAISC3.E01/vol_vo15/usr/lib/gru...	2021-09
ecryptfs-utils.mo				File	Likely Notable		Encryption Programs		Ecrypt(Linux)	/img_HardeschijfImageAISC3.E01/vol_vo15/usr/share/l...	2021-08
luksformat.mo				File	Likely Notable		Encryption Programs		LUKS(Linux)	/img_HardeschijfImageAISC3.E01/vol_vo15/boot/share/l...	2021-08
luks.mod				File	Likely Notable		Encryption Programs		LUKS(Linux)	/img_HardeschijfImageAISC3.E01/vol_vo15/boot/grub/...	2021-12
luksformat.mo				File	Likely Notable		Encryption Programs		LUKS(Linux)	/img_HardeschijfImageAISC3.E01/vol_vo15/usr/share/l...	0000-00
ecryptfs-migrate-home				File	Likely Notable		Encryption Programs		Ecrypt(Linux)	/img_HardeschijfImageAISC3.E01/vol_vo15/usr/share/...	2020-02
cryptsetup-luks.mo				File	Likely Notable		Encryption Programs		LUKS(Linux)	/img_HardeschijfImageAISC3.E01/vol_vo15/usr/share/l...	2021-08
ecryptfs-utils.mo				File	Likely Notable		Encryption Programs		Ecrypt(Linux)	/img_HardeschijfImageAISC3.E01/vol_vo15/usr/share/l...	2021-08
luksformat				File	Likely Notable		Encryption Programs		LUKS(Linux)	/img_HardeschijfImageAISC3.E01/vol_vo15/usr/sbin/lu...	2021-10
ecryptfs				File	Likely Notable		Encryption Programs		Ecrypt(Linux)	/img_HardeschijfImageAISC3.E01/vol_vo15/usr/src/lin...	2021-08
ecryptfs.h				File	Likely Notable		Encryption Programs		Ecrypt(Linux)	/img_HardeschijfImageAISC3.E01/vol_vo15/src/lin...	2021-02
luksformat.mo				File	Likely Notable		Encryption Programs		LUKS(Linux)	/img_HardeschijfImageAISC3.E01/vol_vo15/usr/share/l...	0000-00
ecryptfs-utils.mo				File	Likely Notable		Encryption Programs		Ecrypt(Linux)	/img_HardeschijfImageAISC3.E01/vol_vo15/usr/share/l...	2021-08
cryptsetup-luks.mo				File	Likely Notable		Encryption Programs		LUKS(Linux)	/img_HardeschijfImageAISC3.E01/vol_vo15/usr/share/l...	2021-08
ecryptfs				File	Likely Notable		Encryption Programs		Ecrypt(Linux)	/img_HardeschijfImageAISC3.E01/vol_vo15/usr/src/lin...	2021-12
luksformat.mo				File	Likely Notable		Encryption Programs		LUKS(Linux)	/img_HardeschijfImageAISC3.E01/vol_vo15/usr/share/l...	2021-08
ecryptfs.h				File	Likely Notable		Encryption Programs		Ecrypt(Linux)	/img_HardeschijfImageAISC3.E01/vol_vo15/usr/src/lin...	2021-02

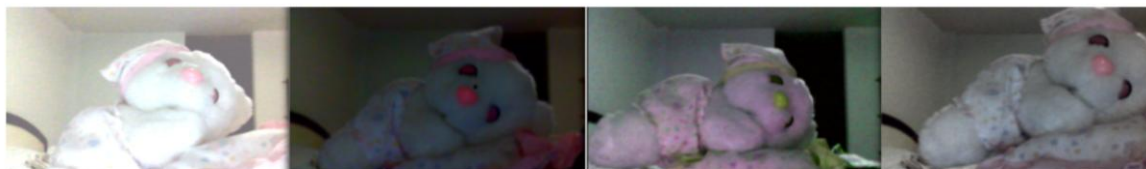
From: rms@gnu.org;
To: chet@nike.ins.cwru.edu;
CC:
Subject: Use of Readline

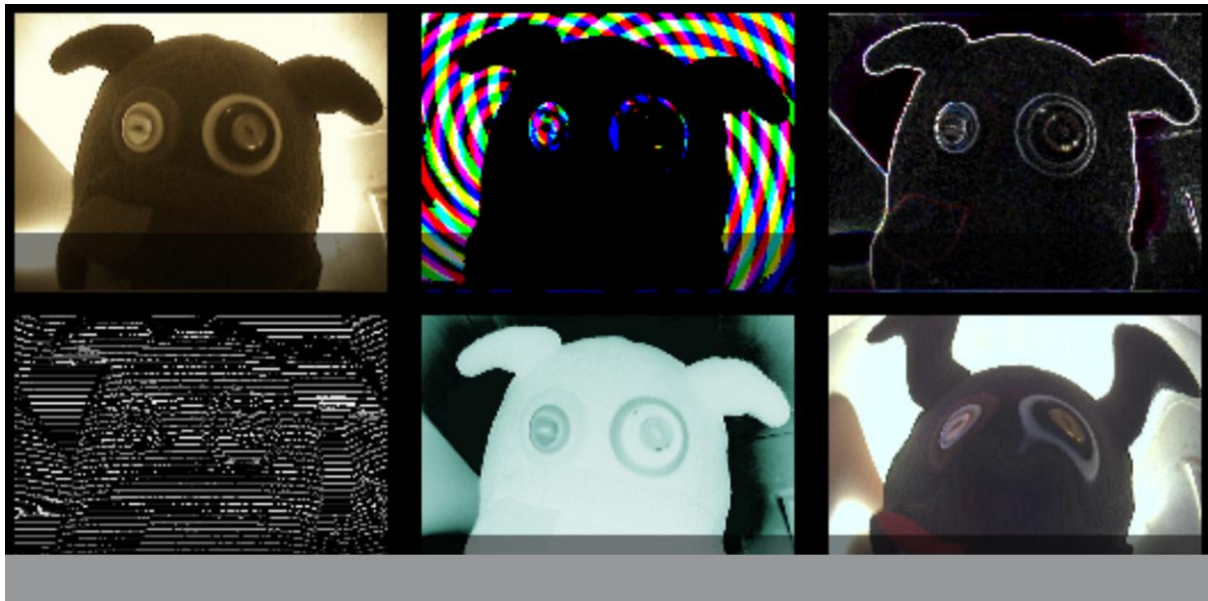
Headers Text HTML RTF Attachments (0) Accounts

I think Allbery's suggestion is a good one. So please add this text in a suitable place. Please don't put it in the GPL itself; that should be the same as the GPL everywhere else. Putting it in the README and/or the documentation would be a good idea.

Our position on the use of Readline through a shared-library linking mechanism is that there is no legal difference between shared-library linking and static linking--either kind of linking combines various modules into a single larger work. The conditions for using Readline in a larger work are stated in section 3 of the GNU GPL.

gdm:*:18858:0:99999:7:::
sssd:*:18858:0:99999:7:::
adb:\$6\$X5o1m1jQtxL.ajmi\$01y0vp3L6X/REGuokY4fQT5MA5a7D6UCr6UHR58fZokfospixRXnjcEBV7Q3ccN.ZQYNCmkVeQcXPjEgd6nD50:18962:0:99999:7:::
systemd-coredump:!:18962:.....





- openvpn (5)
- opt (2)
- PackageKit (4)
- pam.d (30)
- pcmcia (3)
- perl (3)
- pki (4)
- pm (3)
- polkit-1 (4)
- ppp (15)
- profile.d (11)
- pulse (11)
- python3 (3)
- python3.8 (4)
- rc0.d (27)
- rc1.d (25)
- rc2.d (32)
- rc3.d (32)
- rc4.d (32)
- rc5.d (32)
- rc6.d (27)
- rcS.d (16)
- rsyslog.d (5)
- sane.d (83)
- security (25)
- selinux (3)
- sensors.d (3)
- sgml (7)
- shadow (0)
- skel (5)
- snmp (3)
- speech-dispatcher (5)

RAPPORTAGE INZAKE IT FORENSISCH ONDERZOEK

to Sources

HardeschijfImageAISC3.E01_1 Host

HardeschijfImageAISC3.E01

- var (Unallocated) 9.2047
- vol4 (EFI System Partition: 2048-1050623)
- vol5 (Unknown: 1050624-488396799)
- var (Unallocated) 111
- var (Unallocated) 110
- boot (20)
- cdrom (2)
- dev (16)
- etc (395)
- home (3)
- lost+found (2)
- media (4)
- adt (3)
- New Volume (2)
- BitLockerMount (2)

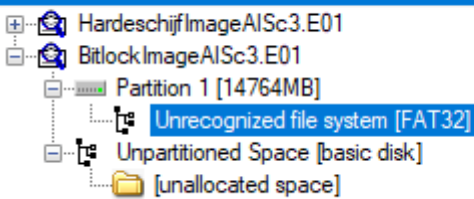
2 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	FlagsDir	FlagsMeta	Known	Location	MDS Hash	SHA-256 Hash
[current folder]				2021-12-01 13:38:51 CET	2021-12-01 13:38:51 CET	2021-12-01 13:40:04 CET	2021-12-01 13:38:51 CET	4096	Allocated	Allocated	unknown	img_HardeschijfImageAISC3.E01\vol_vo5\media\bitloc...		
[parent folder]				2021-12-01 13:38:51 CET	2021-12-01 13:38:51 CET	2021-12-01 13:40:02 CET	2021-12-01 13:25:10 CET	4096	Allocated	Allocated	unknown	img_HardeschijfImageAISC3.E01\vol_vo5\media\bitloc...		

8 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	FlagsDir	FlagsMeta	Known	Location
user-1000@e36c7a50164d52b97546263991e111	B			2021-12-01 11:57:09 CET	2021-12-01 11:57:09 CET	2021-12-02 16:25:42 CET	2021-12-01 14:02:22 CET	8388608	Allocated	Allocated	unknown	img_HardeschijfImageAISC3.E01\vol_vo5\var\...
user-1000@9005c2146c7e02a-08E5e18958674	B			2021-12-01 13:00:44 CET	2021-12-01 13:00:44 CET	2021-12-02 16:25:44 CET	2021-12-01 11:57:09 CET	8388608	Allocated	Allocated	unknown	img_HardeschijfImageAISC3.E01\vol_vo5\var\...
user-1000.journal	B			2021-12-02 11:29:12 CET	2021-12-02 11:29:12 CET	2021-12-02 16:25:42 CET	2021-12-01 13:00:44 CET	8388608	Allocated	Allocated	unknown	img_HardeschijfImageAISC3.E01\vol_vo5\var\...
system@0512b76c746c8b17c402058c148-00002	B			2021-12-01 11:57:09 CET	2021-12-01 11:57:09 CET	2021-12-02 16:25:42 CET	2021-12-01 13:34:27 CET	8388608	Allocated	Allocated	unknown	img_HardeschijfImageAISC3.E01\vol_vo5\var\...
system@0512b76c746c8b17c402058c148-00002	B			2021-12-01 13:00:20 CET	2021-12-01 13:00:20 CET	2021-12-02 16:25:42 CET	2021-12-01 11:57:09 CET	8388608	Allocated	Allocated	unknown	img_HardeschijfImageAISC3.E01\vol_vo5\var\...
system.journal	B			2021-12-02 16:44:18 CET	2021-12-02 16:44:18 CET	2021-12-02 16:25:42 CET	2021-12-01 13:00:20 CET	16777216	Allocated	Allocated	unknown	img_HardeschijfImageAISC3.E01\vol_vo5\var\...
[parent folder]				2021-12-01 13:34:27 CET	2021-12-01 13:34:31 CET	2021-12-02 16:25:42 CET	2021-12-01 13:27:51 CET	4096	Allocated	Allocated	unknown	img_HardeschijfImageAISC3.E01\vol_vo5\var\...
[current folder]				2021-12-01 13:00:44 CET	2021-12-01 13:00:44 CET	2021-12-02 16:25:34 CET	2021-12-01 13:34:27 CET	4096	Allocated	Allocated	unknown	img_HardeschijfImageAISC3.E01\vol_vo5\var\...

Evidence Tree



Database Structure

Browse Data

Edit Pragma

Execute SQL

Create Table

Create Index

Print

Schema

```
CREATE TABLE 'folder_id' (uid TEXT PRIMARY KEY, Rev TEXT, file_as TEXT, file_as_localized TEXT, nickname TEXT, full_name TEXT, given_name TEXT, given_name_localized TEXT, family_name TEXT, family_name_localized TEXT, is_list INTEGER, list...  
CREATE TABLE 'folder_id_email_list' (uid TEXT NOT NULL REFERENCES 'folder_id' (uid), value TEXT)  
CREATE TABLE 'folder_id_phone_list' (uid TEXT NOT NULL REFERENCES 'folder_id' (uid), value TEXT)  
CREATE TABLE folders (folder_id TEXT PRIMARY KEY, version INTEGER, multivalues TEXT, lc_collate TEXT, countrycode VARCHAR(2))  
CREATE TABLE keys (key TEXT PRIMARY KEY, value TEXT, folder_id TEXT REFERENCES folders)  
  
CREATE INDEX 'INDEX_email_folder_id' ON 'folder_id_email_list' (value)  
CREATE INDEX 'INDEX_family_name_folder_id' ON 'folder_id' (family_name)  
CREATE INDEX 'INDEX_file_as_folder_id' ON 'folder_id' (file_as)  
CREATE INDEX 'INDEX_full_name_folder_id' ON 'folder_id' (full_name)  
CREATE INDEX 'INDEX_given_name_folder_id' ON 'folder_id' (given_name)  
CREATE INDEX 'INDEX_nickname_folder_id' ON 'folder_id' (nickname)  
CREATE INDEX 'SINDEX_family_name_folder_id' ON 'folder_id' (family_name_localized)  
CREATE INDEX 'SINDEX_file_as_folder_id' ON 'folder_id' (file_as_localized)  
CREATE INDEX 'SINDEX_given_name_folder_id' ON 'folder_id' (given_name_localized)  
CREATE INDEX 'UID_INDEX_email_folder_id' ON 'folder_id_email_list' (uid)  
CREATE INDEX 'UID_INDEX_phone_folder_id' ON 'folder_id_phone_list' (uid)  
CREATE INDEX keyindex ON keys (folder_id)
```

Logging Analyse

Datum/tijd	Handeling/Observatie/Resultaat
19-5-2024 10:03	Evidence tree uitgevouwen, alle mappen in kaart gebracht
19-5-2024 10:06	Image hardeschijf verkennen
19-5-2024 10:08	Licenses gevonden in unallocated space
19-5-2024 10:27	Alle software is maintained door Dave Mielke (dave@mielke.cc)
19-5-2024 10:30	Mogelijke mandb erin
19-5-2024 10:40	Contactsdb downloaden
19-5-2024 11:34	Klaar met verkennen
19-5-2024 11:38	Openen Contactsdb
19-5-2024 14:00	Op Linux met Autopsy automatische scans uitgevoerd.
19-5-2024 14:30	Alle gearvde images gesorteerd van groot naar klein en deze vervolgens kort gescand.
20-5-2024 11:00	Verder door de bestanden heen gegaan in Autopsy.
20-5-2024 11:20	Opgemerkt dat “/etc/shadow” verwijderd is en /etc/passwd niet op standaard plek staat.
20-5-2024 12:00	Alle audiobestanden en video langsgedaan en geluisterd. Geluid bestanden klinken als standaard “stock-audio” terug te vinden in geluid libraries. De video wou niet openen en is vermoedelijk geencrypt.
20-5-2024 12:20	Enige mail geopend en screenshot van gemaakt.
20-5-2024 12:30	Gekeken naar tools/mogelijkheden om toegang te krijgen tot de bitlocked image, geen succes.
20-5-2024 13:40	Journal logging geëxporteerd en bestudeerd in Linux, geen interessante dingen tegengekomen.
20-5-2024 14:05	In timeline plug-in van autopsy gezocht naar ‘bitlock’, niks interessants gevonden
20-5-2024 14:15	In timeline plugin van autopsy gezocht naar ‘shadow’, oude /etc/shadow file teruggevonden en screenshot van gemaakt.
20-5-2024 14:20	In timeline plugin van autopsy gezocht naar ‘passwd’, oude /etc/passwd file teruggevonden en screenshot van gemaakt.
20-5-2024 14:30	Met John the Ripper de /etc/shadow en /etc/passwd hashes geprobeerd te kraken voor 2 uur, geen resultaat.