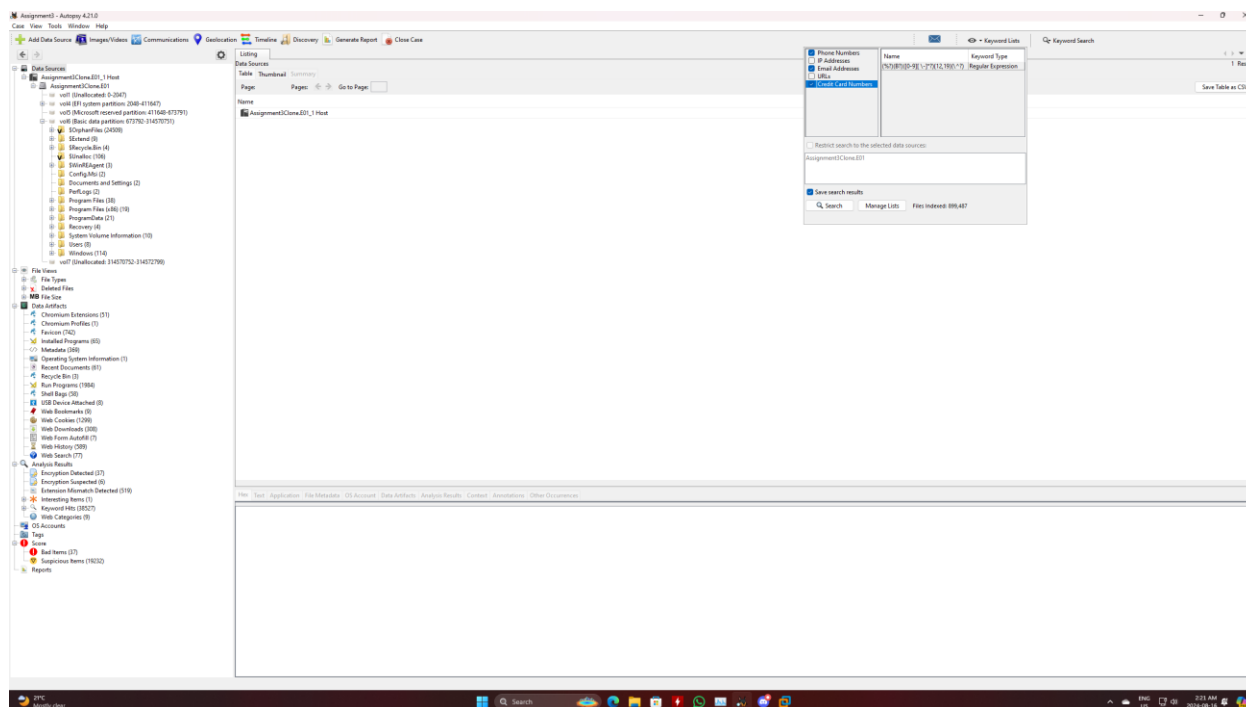


IDENTIFYING PERSONALLY IDENTIFIABLE INFORMATION IN A DISK IMAGE FILE USING AUTOPSY

Jordan Patterson

This document demonstrates an example of finding PII in a disk
image using Autopsy.

In Autopsy, I ran a “Keyword Lists” search for phone numbers, email addresses, and credit card numbers. While the search for phone numbers and email addresses finished successfully, the credit card numbers search failed and froze Autopsy at every attempt, so for this exercise we will continue just with email addresses and phone numbers.



Upon inspecting the Email address results, of which there were 5093, I could classify the results into 2 groups. Legitimate emails and false positives. The false positives all contained an @ symbol. Example: D39D97E@6EH4FP2FY0Fc.Gn.

The screenshot displays the Autopsy 4.21.0 interface. The left sidebar shows the 'Data Sources' tree with categories like File Views, File Types, File Size, Data Artifacts, and Analysis Results. The main window is titled 'Keyword search' and shows a table of results for the keyword 'D39D97E@6EH4FP2FY0Fc.Gn'. The table has columns for Name, Keyword, Preview, Location, Modified Time, and Change Time. The results list various files and their associated email addresses, including 'Training.pots', 'microsoft.data.sapclient.resources.dll', 'AuthWSnapIn.Resources.dll', 'maintenance.service.exe', 'wab32.dll', 'and64_microsoft-windows-crypt32-dll_31b3856a...', 'cryptdlg.dll', 'JapanColor2001Coated.icc', 'JapanColor2003WebCoated.icc', 'main.zee', 'TailMeOutlookMeetingReqSend.exe', 'conct140.dll', 'ANTQUA1.TTF', and 'TCUI.App.dll'. The bottom status bar shows the system clock at 3:24 PM on 2024-08-16.

Name	Keyword	Preview	Location	Modified Time	Change Time
Training.pots	im@company.com	dee	.../Assignment3Clone/E01/vol_yol6/Program Files L...	2024-08-14 13:50:02 EDT	2024-08-14 13:50:1...
microsoft.data.sapclient.resources.dll	d software gmbh19@info@theobald-software.com@...		.../Assignment3Clone/E01/vol_yol6/\$OphanFiles/...	2024-06-01 09:31:44 EDT	2024-08-14 13:50:2...
AuthWSnapIn.Resources.dll	all - eg. contoso@contoso.com-the online id...		.../Assignment3Clone/E01/vol_yol6/Windows/Syst...	2024-07-05 16:46:48 EDT	2024-08-14 13:50:5...
maintenance.service.exe	la corporation1D - release+certificate@mozilla.com...		.../Assignment3Clone/E01/vol_yol6/Program Files L...	2024-07-04 15:14:56 EST	2024-08-14 13:51:5...
wab32.dll	gincard19@bim@compuserve.com@aol.com@tm...		.../Assignment3Clone/E01/vol_yol6/Program Files L...	2024-07-05 16:46:17 EDT	2024-08-14 13:55:5...
and64_microsoft-windows-crypt32-dll_31b3856a...	ocsp.d-trust.net03@info@d-trust.net-http://www.d-tr...		.../Assignment3Clone/E01/vol_yol6/Windows/Win...	2024-07-05 16:49:24 EDT	2024-07-05 17:42:5...
cryptdlg.dll	gn.com by e-mail at <cs-requests@verisign.com> or...		.../Assignment3Clone/E01/vol_yol6/Windows/Win...	2019-12-07 04:09:41 EST	2024-08-14 13:55:5...
JapanColor2001Coated.icc	6e4f42b2b-0b-c5-c-c-d39d97e@6eh4fp2fy0fc.gn-g...		.../Assignment3Clone/E01/vol_yol6/Program Files L...	2021-02-01 20:49:24 EST	2023-09-10 03:38:4...
JapanColor2003WebCoated.icc	6e4f42b2b1y1f7q 5r-e4v2b2b1@9ag.bm-tv\10k\y\y#y		.../Assignment3Clone/E01/vol_yol6/Program Files L...	2021-02-01 20:49:24 EST	2023-09-10 03:38:4...
main.zee	thms = set("all"; "cdl@openssh.com") ## if tru...		.../Assignment3Clone/E01/vol_yol6/ProgramData/...	2023-10-01 13:58:04 EDT	2024-05-25 09:22:5...
TailMeOutlookMeetingReqSend.exe	eol sonia chuig an <synchot@service.microsoft.com>...		.../Assignment3Clone/E01/vol_yol6/\$OphanFiles/...	2024-06-01 09:31:42 EDT	2024-08-14 13:50:2...
conct140.dll	(mof one drive, <synchot@service.microsoft.com> &...		.../Assignment3Clone/E01/vol_yol6/\$OphanFiles/c...	2019-09-02 07:25:08 EDT	2024-08-14 13:50:1...
ANTQUA1.TTF	n.com by e-mail at <cs-requests@verisign.com> orb...		.../Assignment3Clone/E01/vol_yol6/Program Files L...	2024-08-14 13:48:23 EDT	2024-08-14 13:59:1...
TCUI.App.dll	r/readcontentaschar&readcontentasingle&readelem...		.../Assignment3Clone/E01/vol_yol6/Program Files L...	2023-09-11 10:21:52 EDT	2023-09-11 10:21:5...

As for the legitimate emails, most were contact addresses found in readme and text files associated with the applications installed on the PC. One such example was: CPS-requests@verisign.com

The screenshot displays the Autopsy 4.21.0 interface. The left sidebar shows the 'Data Sources' tree with 'Data Artifacts' expanded, listing various file types like 'Chromium Extensions', 'Favicon', 'Installed Programs', etc. The main window is titled 'Keyword search' and shows a table of search results for the keyword 'CPS-requests@verisign.com'. The table has columns for Name, Keyword Preview, Location, and Modified Time. The results list several files, including 'JapanColor2003WebCoated.icc', 'main.zeek', 'TellMeOutlookMeetingReqSend.nrr', 'concr140.dll', 'ANTQUAB.TTF', 'TCUI-App.dll', 'ANTQUAB.TTF', 'mozilla-ca-list.zeek', 'OfficeC2RCom.dll', 'BASVILL.TTF', 'ARLRDBD.TTF', 'BELL.TTF', 'XandrVastPlayer_eb09440ee890ca44e6455c70967e9.js', and 'BELL.TTF'. The 'BASVILL.TTF' file is highlighted. Below the table, the 'Strings' tab is selected, showing the extracted text from the selected file. The text includes a URL 'https://www.verisign.com', a copyright notice for VeriSign, Inc., and a warning about the use of the certificate. The bottom status bar shows the system clock as 3:33 PM on 2024-08-16.

Name	Keyword Preview	Location	Modified Time
JapanColor2003WebCoated.icc	.../Assignment3Clone.E01/vol_0/Program Files/...	/Assignment3Clone.E01/vol_0/Program Files/...	2021-02-01 20:49:24 EST
main.zeek	thms = set("dlb", "cdlb@openssh.com");	/Assignment3Clone.E01/vol_0/Program Data/...	2023-10-01 13:58:04 EDT
TellMeOutlookMeetingReqSend.nrr	.../Assignment3Clone.E01/vol_0/Orphan Files/...	/Assignment3Clone.E01/vol_0/Orphan Files/...	2024-06-01 09:31:42 EDT
concr140.dll	(mft onedrive, <synchot@service.microsoft.com> &...)	/Assignment3Clone.E01/vol_0/Orphan Files/...	2018-09-02 07:25:08 EDT
ANTQUAB.TTF	n.com; by e-mail at <cps-requests@verisign.com> or b...	/Assignment3Clone.E01/vol_0/Program Files/...	2024-08-14 13:48:23 EDT
TCUI-App.dll	"readcontentaschar&readcontentassingle&readelem...	/Assignment3Clone.E01/vol_0/Program Files/...	2023-09-11 10:21:52 EDT
ANTQUAB.TTF	n.com; by e-mail at <cps-requests@verisign.com> or b...	/Assignment3Clone.E01/vol_0/Program Files/...	2024-08-14 13:48:23 EDT
mozilla-ca-list.zeek	2", ["emailaddress=<info@e-szigno.hu>@microsof...	/Assignment3Clone.E01/vol_0/Program Data/...	2023-10-01 13:58:04 EDT
OfficeC2RCom.dll	missionsource"; <someone@example.com>"; errorsin...	/Assignment3Clone.E01/vol_0/Orphan Files/...	2018-09-08 04:30:04 EDT
BASVILL.TTF	n.com; by e-mail at <cps-requests@verisign.com> or b...	/Assignment3Clone.E01/vol_0/Program Files/...	2024-08-14 13:48:23 EDT
ARLRDBD.TTF	n.com; by e-mail at <cps-requests@verisign.com> or b...	/Assignment3Clone.E01/vol_0/Program Files/...	2024-08-14 13:48:23 EDT
BELL.TTF	n.com; by e-mail at <cps-requests@verisign.com> or b...	/Assignment3Clone.E01/vol_0/Program Files/...	2024-08-14 13:48:23 EDT
XandrVastPlayer_eb09440ee890ca44e6455c70967e9.js	2016 falsat salman <<fyzlman@gmail.com>> which a...	/Assignment3Clone.E01/vol_0/Users/MjohierT...	2024-08-14 14:16:30 EDT
BELL.TTF	n.com; by e-mail at <cps-requests@verisign.com> or b...	/Assignment3Clone.E01/vol_0/Program Files/...	2024-08-14 13:48:23 EDT

Strings: Extracted Text Translation

Page: 1 of 1 Page 1 Matches on page: 1 of 1 Match 100% Reset

Text Source: Search Results

https://www.verisign.com; by e-mail at <CPS-requests@verisign.com> or by mail at VeriSign, Inc., 2593 Coast Ave., Mountain View, CA 94043 USA Copyright (c)1996 VeriSign, Inc. All Rights Reserved. CERTAIN WARRANTIES DISCLAIMED AND LIABILITY LIMITED. WARNING: THE USE OF THIS CERTIFICATE IS STRICTLY SUBJECT TO THE VERISIGN CERTIFICATION PRACTICE STATEMENT. THE ISSUING AUTHORITY DISCLAIMS CERTAIN IMPLIED AND EXPRESS WARRANTIES, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, AND WILL NOT BE LIABLE FOR CONSEQUENTIAL, PUNITIVE, AND CERTAIN OTHER DAMAGES. SEE THE CPS FOR DETAILS. Contents of the VeriSign registered nonverifiedSubjectAttributes extension value shall not be considered as accurate information validated by the IA. https://www.verisign.com/repository/verisignlogo.gil06 /D-0- %http://status.verisign.com/class1.o10 mra4f IQ^7 0u0a1 Internet1 VeriSign, Inc.1301

Legitimate emails directing to an individual were found as well, an example of this was a readme file containing the names and direct email addresses of the applications contributors.

Andreas Gohr <andi@splitbrain.org>
Michael Klier <chi@chimeric.de>
Andreas Barton <andreas.barton@web.de>
Hubert Chathi <hubert@uhoreg.ca>
Johan Koehne <johankohne@gmail.com>
Rudi von Staden <rudivs@iafrica.com>
Daniel Darvish <ddarvish@hibm.org>
Andy Pascall <apascall@engineering.ucsb.edu>
Seth <seth.holcomb@gmail.com>
David Carella <david.carella@gmail.com>
Tom N. Harris <telliamed@fastmail.us>
Brandon Carmon Colvin <b.carmon.colvin@gmail.com>

The screenshot displays the Autopsy 4.21.0 interface. On the left, the 'Data Sources' pane shows a tree view of file types and artifacts. The 'Data Artifacts' section is expanded, showing various file types like 'Chromium Extensions', 'Chromium Profiles', 'Firefox', 'Installed Programs', 'Metadata', 'Operating System Information', 'Recent Documents', 'Recycle Bin', 'Run Programs', 'Shell Bags', 'USB Device Attached', 'Web Bookmarks', 'Web Cookies', 'Web Downloads', 'Web Form Autofill', 'Web History', and 'Web Search'. The 'File Views' section is also visible, showing 'Deleted Files' and 'File Size'. The main pane shows a 'Keyword search' results table with columns: Name, Keyword Preview, Location, Modified Time, and Chk. The table lists various files, including 'MSOUTL.OLB', 'CENSCBK.TTF', 'p0fa.fp', 'CASTELAR.TTF', 'ThirdPartyNotices.txt', 'CINTAUR.TTF', 'README', 'COOPBL.TTF', 'COLONNA.TTF', 'COPRGLT.TTF', 'COPRGLT.TTF', 'SOCALCONNECTOR.DLL', 'Unalloc_1147074_40137474048_41808506880', 'Unalloc_1147074_39123435520_40137424896', and 'Unalloc_1147074_4333571104_46779043840'. The 'README' file is selected, and its contents are displayed in the 'Strings' pane. The README text includes a release notice, a note about the majority of icons being created by the creators listed below, and a list of creators with their email addresses: Andreas Gohr, Michael Klier, Andreas Barton, Hubert Chathi, Johan Koehne, Rudi von Staden, Daniel Darvish, Andy Pascall, Seth, David Carella, Tom N. Harris, and Brandon Carmon Colvin.

Name	Keyword Preview	Location	Modified Time	Chk
MSOUTL.OLB	0 { g g 2 ? ,+synd /Amg_Assignment3Clone.E01/vol6/\$OrphanFiles/...	/Amg_Assignment3Clone.E01/vol6/\$OrphanFiles/...	2024-06-01 09:31:34 EDT	202
CENSCBK.TTF	n.com; by e-mail at <cps-requests@verisign.com>; orb...	/Amg_Assignment3Clone.E01/vol6/Program Files L...	2024-08-14 13:48:30 EDT	202
p0fa.fp	uted by ryan kruse <+kruse@alterpoint.com> - trial t...	/Amg_Assignment3Clone.E01/vol6/Users/MjohiL...	2023-05-03 11:51:58 EDT	202
CASTELAR.TTF	n.com; by e-mail at <cps-requests@verisign.com>; orb...	/Amg_Assignment3Clone.E01/vol6/Windows/Win...	2024-08-14 13:48:30 EDT	202
ThirdPartyNotices.txt	mark adler <loup@grip.org> madler@alu	/Amg_Assignment3Clone.E01/vol6/Windows/Win...	2019-12-07 04:10:48 EST	202
CINTAUR.TTF	n.com; by e-mail at <cps-requests@verisign.com>; orb...	/Amg_Assignment3Clone.E01/vol6/Program Files L...	2024-08-14 13:48:30 EDT	202
README	g.ucsb.edu> seth <seth.holcomb@gmail.com>; dav...	/Amg_Assignment3Clone.E01/vol6/Program Files L...	2023-08-29 14:26:54 EDT	202
COOPBL.TTF	n.com; by e-mail at <cps-requests@verisign.com>; orb...	/Amg_Assignment3Clone.E01/vol6/Program Files L...	2024-08-14 13:48:30 EDT	202
COLONNA.TTF	n.com; by e-mail at <cps-requests@verisign.com>; orb...	/Amg_Assignment3Clone.E01/vol6/Program Files L...	2024-08-14 13:48:30 EDT	202
COPRGLT.TTF	n.com; by e-mail at <cps-requests@verisign.com>; orb...	/Amg_Assignment3Clone.E01/vol6/Program Files L...	2024-08-14 13:48:30 EDT	202
COPRGLT.TTF	n.com; by e-mail at <cps-requests@verisign.com>; orb...	/Amg_Assignment3Clone.E01/vol6/Program Files L...	2024-08-14 13:48:30 EDT	202
SOCALCONNECTOR.DLL	brosti poajite na <grinchot@service.microsoft.com>wop...	/Amg_Assignment3Clone.E01/vol6/\$OrphanFiles/...	2024-06-01 09:31:34 EDT	202
Unalloc_1147074_40137474048_41808506880	ange box (example: "someone@example.com") sepa...	/Amg_Assignment3Clone.E01/vol6/\$Unalloc/Unal...	0000-00-00 00:00:00	000
Unalloc_1147074_39123435520_40137424896	.f4, cryptograms by <agpro@openstl.org>+vssuatau...	/Amg_Assignment3Clone.E01/vol6/\$Unalloc/Unal...	0000-00-00 00:00:00	000
Unalloc_1147074_4333571104_46779043840	/ole 97ec?page=8+@gg-lyzv/tvdlfo @tla)+*	/Amg_Assignment3Clone.E01/vol6/\$Unalloc/Unal...	0000-00-00 00:00:00	000

Strings: Extracted Text Translation

Page: 1 of 1 Page Matches on page: 1 of 12 Match 100% Reset Text Source: Search Results

[readme: http://www.splitbrain.org/projects/file_icons

Released to the Public Domain
Free to use. Provided as is. No warranties.

Note: The big majority of icons were created by the creators listed below. Only a few ones where found on the net. They were too widespread to determine the original author and thus were considered public domain.
If you are the author of one of those icons just send a short mail to either be included in the list below or have the icon removed from the package.

Creators:

- Andreas Gohr <andi@splitbrain.org>
- Michael Klier <chi@chimeric.de>
- Andreas Barton <andreas.barton@web.de>
- Hubert Chathi <hubert@uhoreg.ca>
- Johan Koehne <johankohne@gmail.com>
- Rudi von Staden <rudivs@iafrica.com>
- Daniel Darvish <ddarvish@hibm.org>
- Andy Pascall <apascall@engineering.ucsb.edu>
- Seth <seth.holcomb@gmail.com>
- David Carella <david.carella@gmail.com>
- Tom N. Harris <telliamed@fastmail.us>
- Brandon Carmon Colvin <b.carmon.colvin@gmail.com>

There were 892 phone numbers identified in the search. Like the Email addresses, the phone number results came with its own share of legitimate numbers and false positives. What was interesting about the phone number results is that they were often accompanied by even more PII such as names, titles, addresses, and email addresses. One such example is a text file containing all of the PII that I just mentioned.

Example:

Chair: Mike Sneed
Sand Channel Systems
Postal: P.O. Box 37324
Raleigh NC 27627-732
Email: sneedmike@hotmail.com
Phone: +1 206 600 7022

Co-Chair/Co-editor:
Bob Ray
PESA Switching Systems, Inc.
Postal: 330-A Wynn Drive
Huntsville, AL 35805 USA
Email: r-ray@pesa.com
Phone: +1 256 726 9200 ext. 142

The screenshot displays the Autopsy 4.21.0 interface. The left sidebar shows the file tree with categories like Data Sources, File Views, and Analysis Results. The main window shows search results for the keyword 'phone'. The results table lists files with columns for Name, Keyword Preview, Location, Modified Time, and Change Time. A detailed view of a text file is shown below the table, containing contact information for Mike Sneed and Bob Ray.

Name	Keyword Preview	Location	Modified Time	Change Time
TRIP-MIB	phone: +1-905 886-7818-x2515	/img_Assignment3CloneE01/vol_yol6/Program Files/...	2011-06-27 15:50:30 EDT	2023-09-10 03:34:0
ACWIDAT.DLL	iskenelmodestdip1-824.460.10474elddivertype0000	/img_Assignment3CloneE01/vol_yol6/OrphanFiles/...	2024-06-01 09:31:54 EDT	2024-08-14 13:50:3
UMTS-PIB	phone: +1-613 768 3409+	/img_Assignment3CloneE01/vol_yol6/Program Files/...	2011-06-27 15:50:32 EDT	2023-09-10 03:34:0
TUBS-IBR-AGENT-CAPABILITIES	391 3283 fac: +49-531 391 5936+ e-mail: sc...	/img_Assignment3CloneE01/vol_yol6/Program Files/...	2011-06-27 15:50:30 EDT	2023-09-10 03:34:0
UPS-MIB	fax: +1-615 573 9197+ e-mail	/img_Assignment3CloneE01/vol_yol6/Program Files/...	2011-06-27 15:50:30 EDT	2023-09-10 03:34:0
UMTS-PIB-orig	phone: +1-613 768 3409+	/img_Assignment3CloneE01/vol_yol6/Program Files/...	2011-06-27 15:50:32 EDT	2023-09-10 03:34:0
VDSL-LINE-EXT-MCM-MIB	phone: +1-206 600 7022+ co-chair/c	/img_Assignment3CloneE01/vol_yol6/Program Files/...	2011-06-27 15:50:30 EDT	2023-09-10 03:34:0
VDSL-LINE-MIB	phone: +1-919 850 6194+ "descriptio	/img_Assignment3CloneE01/vol_yol6/Program Files/...	2011-06-27 15:50:30 EDT	2023-09-10 03:34:0
runtime-20.win32.bundle	ivate organization+603 389 0681=washingtontred...	/img_Assignment3CloneE01/vol_yol6/OrphanFiles/...	2024-06-01 09:31:51 EDT	2024-08-14 13:50:2
VDSL-LINE-EXT-SCM-MIB	phone: +1-206 600 7022+ co-chair/c	/img_Assignment3CloneE01/vol_yol6/Program Files/...	2011-06-27 15:50:30 EDT	2023-09-10 03:34:0
VDSL2-LINE-TC-MIB	phone: +1-206 600 7022+ co-cha	/img_Assignment3CloneE01/vol_yol6/Program Files/...	2011-06-27 15:50:30 EDT	2023-09-10 03:34:0
zh-CN.pak	k \$1 \$3 \$1\$1+1-@840 552 7621-5352535254 (\$5+	/img_Assignment3CloneE01/vol_yol6/Program Files L...	2024-08-07 04:43:13 EDT	2024-08-14 14:00:0
runtime-20.win32.bundle-slack	2+*04us washington-603 389 0680+@http://crl3.di...	/img_Assignment3CloneE01/vol_yol6/OrphanFiles/...	2024-06-01 09:31:51 EDT	2024-08-14 13:50:2
VDSL2-LINE-MIB	phone: +1-206 600 7022+ co-cha	/img_Assignment3CloneE01/vol_yol6/Program Files/...	2011-06-27 15:50:30 EDT	2023-09-10 03:34:0
and54_microsoft-windows-p-ormancebasecounte	"value":230 232 786-740 816 1408-1500 1548 17...	/img_Assignment3CloneE01/vol_yol6/Windows/serv...	2024-08-10 20:32:14 EDT	2024-08-14 13:51:4
VRBP-MIB	4303 tab: +1-650 687 3367+ a-mail: hnsuall	/img_Assignment3CloneE01/vol_yol6/Program Files/...	2011-06-27 15:50:30 EDT	2023-09-10 03:34:0

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Strings: Extracted Text Translation

Page: 1 of 1 Page 100% Matches on page: 1 of 2 Match Reset Text Source: Search Results

ORGANIZATION "ADSLMIB Working Group"

CONTACT-INFO "WG-email: adslmib@ietf.org"

Info: <https://www1.ietf.org/mailman/listinfo/adslmib>

Chair: Mike Sneed
Sand Channel Systems
Postal: P.O. Box 37324
Raleigh NC 27627-732
Email: sneedmike@hotmail.com
Phone: +1 206 600 7022

Co-Chair/Co-editor:
Bob Ray
PESA Switching Systems, Inc.
Postal: 330-A Wynn Drive
Huntsville, AL 35805
USA
Email: r-ray@pesa.com
Phone: +1 256 726 9200 ext. 142