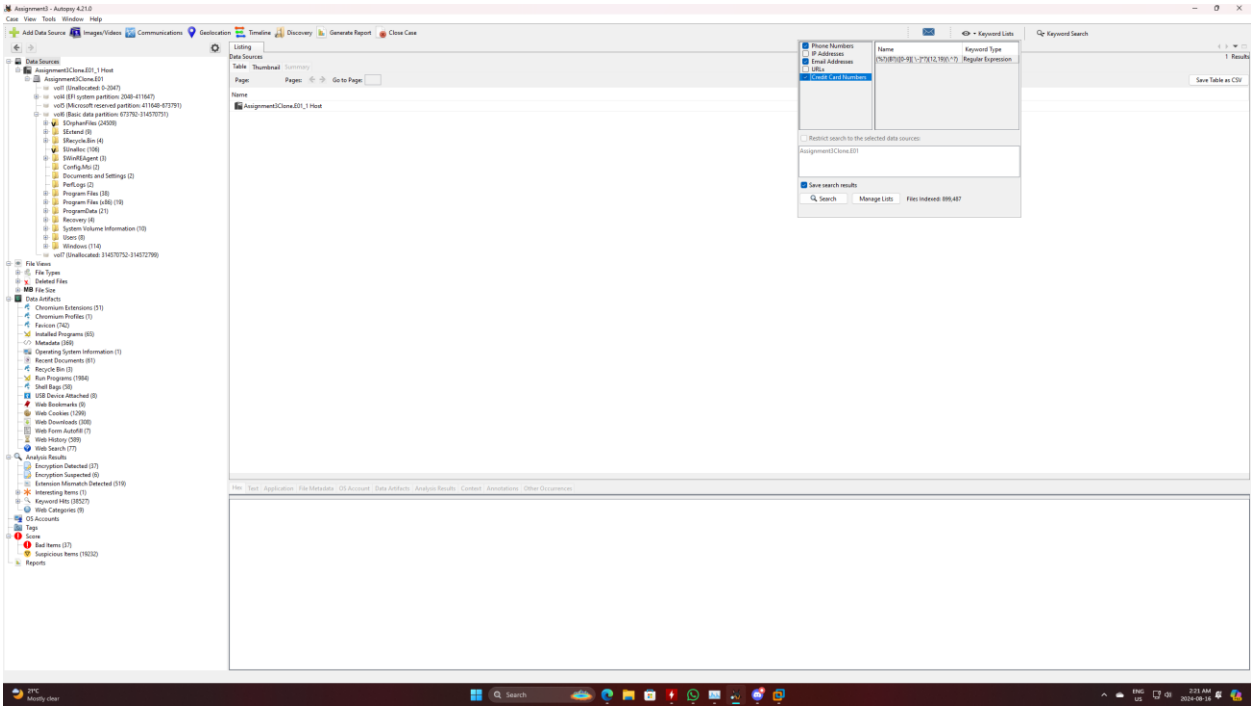
IDENTIFYING PERSONALLY IDENTIFIABLE INFORMATION IN A DISK IMAGE FILE USING AUTOPSY

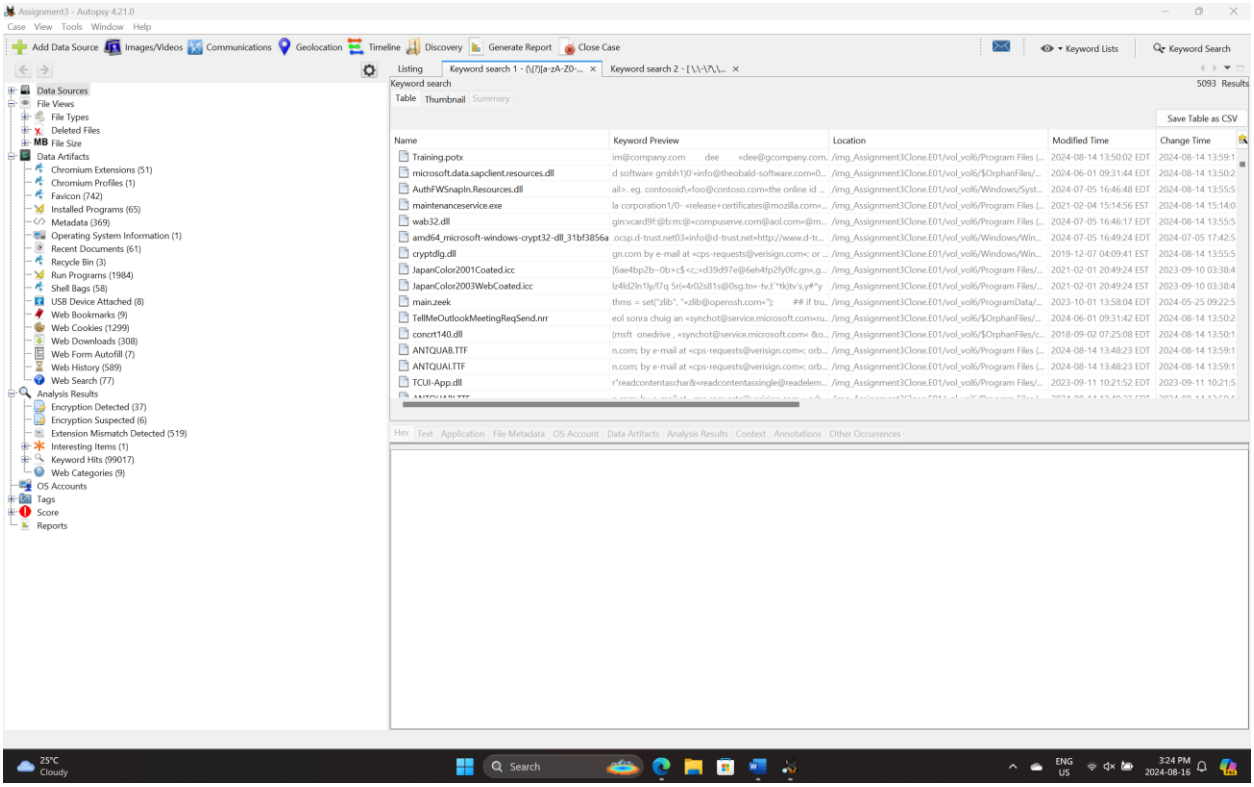
Jordan Patterson

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

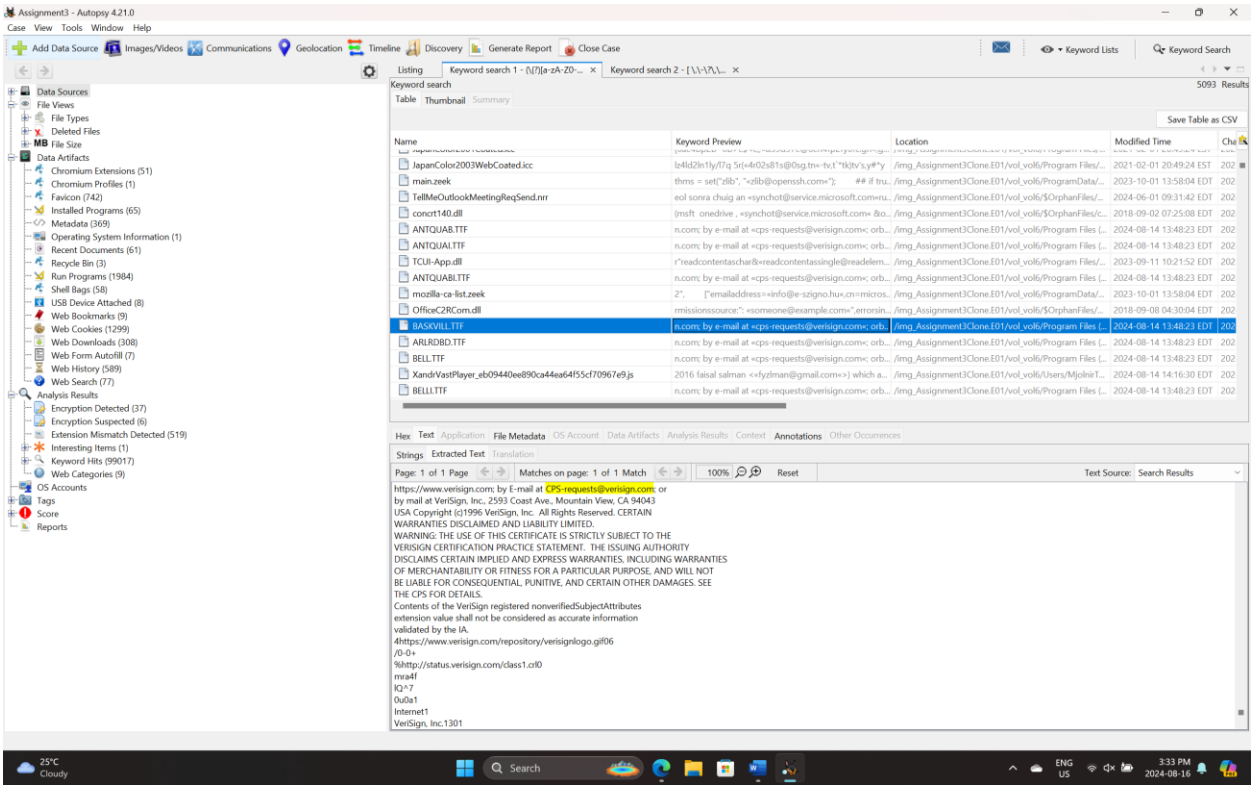
In Autopsy, I ran a “Keyword Lists” search for phone numbers, email addresses, and credit card numbers. While the search for phone numbers and email addresses finished successfully, the credit card numbers search failed and froze Autopsy at every attempt, so for this exercise we will continue just with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

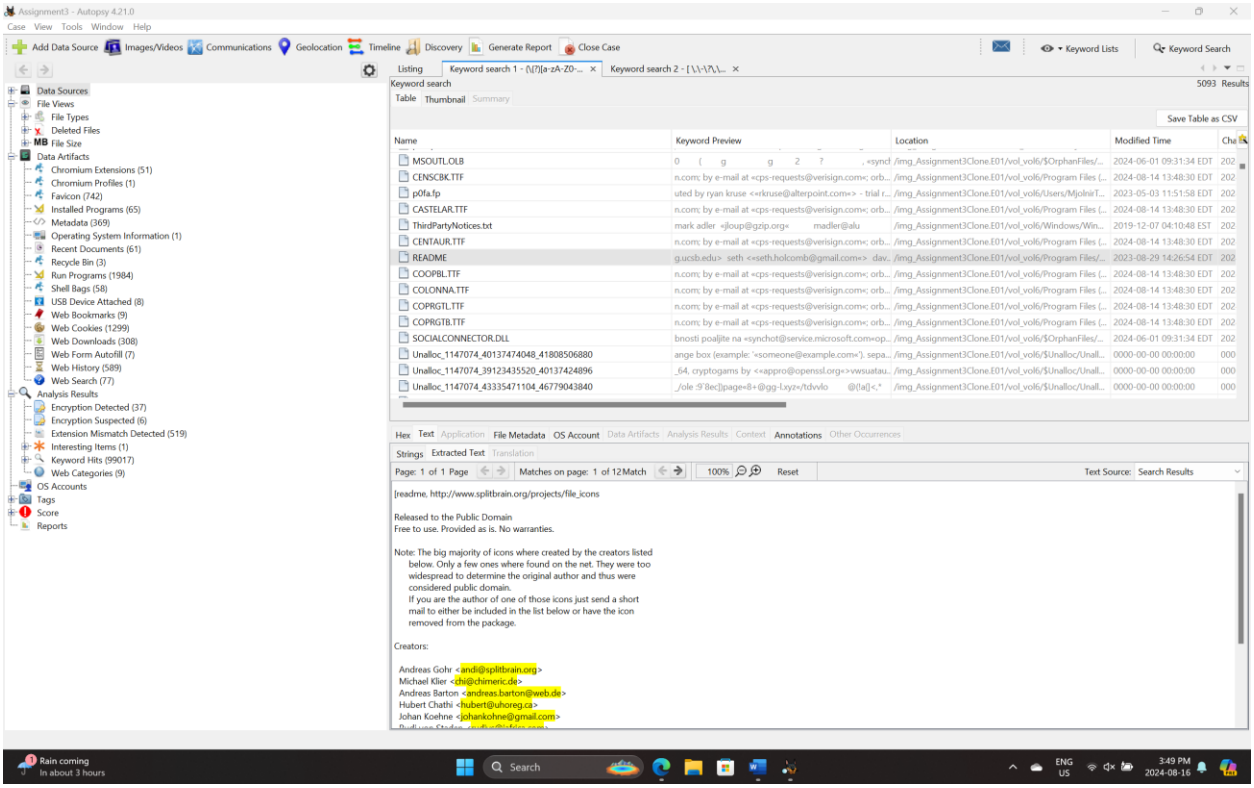


As for the legitimate emails, most were contact addresses found in readme and text files associated with the applications installed on the PC. One such example was: CPS-requests@verisign.com



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>



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: rray@pesa.com
Phone: +1 256 726 9200 ext. 142