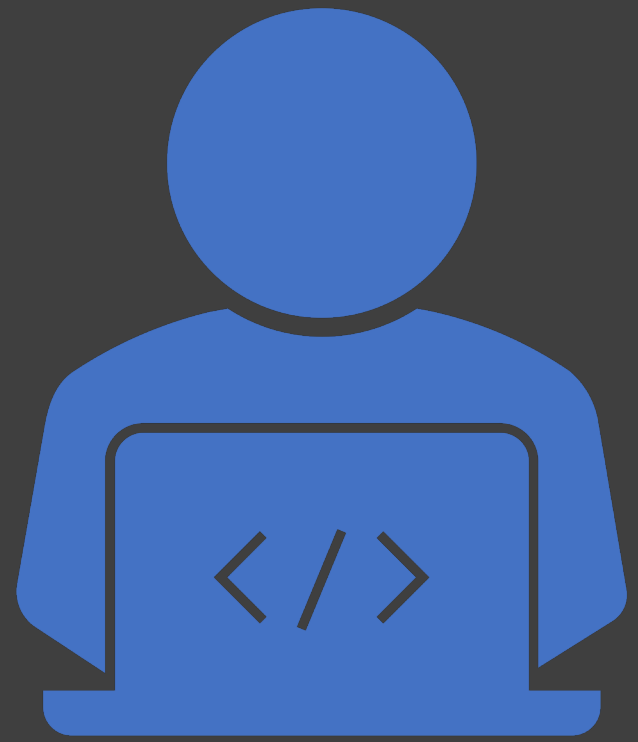
Autopsy Plugins

Mark McKinnon

Davenport University



Plugin Types

- Two (2) types of plugins available
  - Netbean plugins which use the Netbean framework that Autopsy is built on.
  - Python plugins
- Autopsy addon module repository
  - https://github.com/sleuthkit/autopsy_addon_modules

Netbeans Plugins

Image Fingerprint

- You can get the source here https://github.com/LoWang123/ImageFingerprintModulePackage

- A module package containing a File Ingest Module and its corresponding Data Content Viewers. Allows the user to create different perceptual hashes as fingerprints from images in the datasource. This also creates an additional database, which is managed from the expanded options menu of the ingest module. Images can be compared to images in the database.
- Autopsy Version 4.1+
- Author Tobias Maushammer

Windows Registry Content Viewer

- You can get the source here https://github.com/LoWang123/ImageFingerprintModulePackage
- Content viewer that analyzes a registry hive and allows you to navigate the tree and its key and value pairs. Functions something like Regedit.exe.
- Autopsy Version 4.1+
- Author Willi Ballenthin
- Now part of Autopsy Core as of 4.12

Windows Registry Ingest Module

- You can get the source here https://github.com/sleuthkit/Autopsy-WindowsRegistryIngestModule
- An ingest module that extracts Registry keys and values into derived directories and files so that they show up as nodes in the directory tree.
- Autopsy Version 4.1+
- Author Willi Ballenthin

AuthentiCodeVerification

- Source code can be found here https://github.com/mvetsch/Autopsy-AuthentiCodeVerification

- The module verifies code signing certificates of Windows executables. It creates Content Tags with the Signer Name of the binary. This module helps to quickly eliminate known-good files from the OS vendor. You can also list the files from any unknown publisher, that signed software on the system you are investigating on.
- Author: Mathias Vetsch and Luca Taennler

TagFilter

- Source code can be found here https://github.com/colapse/Autopsy-TagFilter
- In Autopsy there are several tags of various modules which have the same or a similar meaning (For example tags to mark files as “known-good”). In Autopsy there is a listing of files per tag, but you might want to have a list containing all files that were tagged with “known-good”-a-like tags. The TagFilter module. This module enables you to create a list of files by applying several filters (for tags). You can add an unlimited amount of filters and connect them by AND-OR operators. Further on you can also specify f you want the filter to be true or false (File contains or doesn’t contain tag). Besides that, you can also create so called “Filter Groups” in which you can combine filters. The filters are applied top-down and they are built up similar to the SQL WHERE clause. You can also select if you want to search for files on all data sources within your case or just a specific one. In the end you will get a list with all the files that match your filter.
- Authors Mathias Vetsch and Luca Taennler

VirusTotal Online Checker

- Source code can be found here https://github.com/mvetsch/VirusTotalOnlineChecker
- Minimum Version of Autopsy 4.1
- Autopsy File Ingest Module to check file hashes against online VirusTotal Database
- Requirements: API Key which can obtained on https://www.virustotal.com/en/documentation/public-api/
- Authors : Mathias Vetsch, Luca Tannler

Golden Image

- Source code can be found here https://github.com/colapse/Autopsy-GoldenImage
- The Golden Image module uses two data sources – a “dirty image” and a “golden image” – and compares them with each other. The main task is, to find the difference between these two data sources – newly added files, deleted files and changed files
- Authors: Mathias Vetsch and Luca Taennler

Cortana Edge

- Source code can be found here https://github.com/Tattieness/Cortana_Edge_Autopsy

- The basis of the module is that it extracts the browsing history for I.E 11/Edge and also a set of artifacts that relate to the use of Cortana. These include the speech files, html files and other files generated when talking to Cortana. The module also extracts reminders and attachments. This will include notifications such a missed calls and texts from a mobile phone, running Cortana which is associated with Microsoft Account in use.
- Author: Clare Taylor

Reversing Labs Hash Query Plugin

- Source code can be found here https://github.com/PolitoInc/autopsy-reversinglabs-plugin
- The ReversingLabs hash query plugin assists digital investigators with faster analysis results and makes the process more efficient when trying to find malicious activity. The goal is to filter out the known good and known bad, and focus on the unknowns. This speeds up the analysis process and results when looking for malicious activity using forensics tools. More information can be found here https://www.politoinc.com/single-post/2018/03/05/Enhancing-Digital-Forensics-with-ReversingLabs-Hash-Query-Plugin-for-Autopsy
- Version of Autopsy tested with 4.5 and 4.6
- Authors: Polito Inc and Reversing Labs

Tika Language Detector

- Code can be found here https://github.com/benreillyss/TikaLanguageDetector
- Ingest Module that uses Tika to detect the language of common file documents.
- Author: benreillyss

Browser History Histogram

- Code can be found here https://github.com/labcif/BHH
- Extract all webactivity of a user to a local database and then generate a report to display this information.
- Author: Kevin Baptista and Tomás Honório

Python Plugins

Tom Van der Mussele Plugins.

- You can get the modules from https://github.com/tomvandermussele/autopsy-plugins
- Version of Autopsy > 4.3

- Skype Analyzer
  - investigate Skype databases within a Windows environment and extract information such as:
    - Call data
    - IP Addresses
    - Chats
    - Names

Tom Van der Mussele Plugins

- Chrome Passwords Identifier
  - Identified Chrome Password Databases and extract certain artifacts
- Connected iPhone Analyzer
  - Investigate .plist files related to iTunes backups within a Windows environment
- GoogleDrive
  - Investigate Google Drive snapshot databases and list filenames with full path.
- IE Tiles
  - Will enumerate Internet Explorer Tiles.
- Windows Communication App
  - Extract the services and contacts from the Windows Communication Application

Microsoft Office Telemetry Parser for Autopsy

- Source code can be found here https://github.com/MadScientistAssociation/Autopsy-MSOT

- In Office 2013, Microsoft introduced telemetry collection in Office. This created a gold mine of data for digital forensics examiners.
  - Included in Office telemetry collection are:
    - File name
    - User name
    - File open/close date/times
    - File size
    - Document title
    - Document author
    - Office version
    - Last loaded date/times
- This ingest module searches for folders containing all three of the files sln.tbl, user.tbl, and evt.tbl. It then combines the data from these 3 files and outputs artifacts to the blackboard as type TSK_RECENT_OBJECT.
- Author : Sam Koffman

Log Forensics

- Source code can be found here https://github.com/L-Andrade/LFA

- Minimum Autopsy Version 4.6
- Log Forensics for Autopsy is a 2-part Jython module for Autopsy. It consists of a file ingest and report. The file ingest tags certain log files, specific to Windows, such as: .wer, .etl, .evtx, .dmp, .log, and specific .xml. Extracts information from .wer, .log and .xml: Windows Error Reporting events, startup processes, and RegEx patterns from .log (IPs by default).
- Authors: Luís Andrade, João Silva, Patrício Domingues, Miguel Frade.

Copy Move

- The source code can be found here https://github.com/LoWang123/CopyMoveModulePackage
- Minimum Autopsy version: 4.1.0
- A module package containing a File Ingest Module and its corresponding Data Content Viewer. Allows the user to identify Copy-Move forgeries within images in the datasource. Please read the readme before using the package.
- Author: Tobias Maushammer

P2PForensic

- Source code can be found here https://github.com/CarlosLannister/P2PForensic

- The main purpose of this plugin is try to get usage information of P2P Windows programs in a forensics environment.
- The current version has been developed using the following P2P programs:
  - Emule v0.50a
  - uTorrent 3.4.8
  - bitTorrent 7.9.9
- Author Carlos Cilleruelo Rodríguez

Payment Card Scanner

- Source code can be found here
- Search for possible payment card numbers, and will then check the Luhn checksum of each possible payment card number, which will provide a greater degree of confidence regarding if a numeric sequence is a payment card number or not.
- Version 4.1+
- Author Shea Nangle

digiSignedOrProtectedPDF

- Source code can be found here https://github.com/PatricioDomingues/digiSignedOrProtectedPDF

- Autopsy 4.4.1+.
- The digiSigned|ProtectedPDF module is a file ingest jython-based module for the Autopsy software. It provides two main services for PDF files:
- Identifies the PDF files that are digitally signed (digital signature refers to the cryptographically-based signature of documents. It does **not** refer to have images of physical signatures in a document.)
- Identifies the PDF files which some kind of user-level protection. Specifically, the module flags as interesting files PDF files that forbids the "document assembly" and "document modify".
- The digiSigned|ProtectedPDF module depends on two excellent external tools (not included in this repository):
  - JSignPDF (http://jsignpdf.sourceforge.net)
  - ExifTool (https://sno.phy.queensu.ca/~phil/exiftool/)
- Author Patricio Domingues

FEA - Forensics Enhanced Analysis

- Source can be found here https://bitbucket.org/psychodeath/fea-forensics-enhanced-analysis/overview

- FEA comprises three separate tools: i) for email filtering and validation, ii) for credit card number validation and iii) for Bitcoin wallet addresses and private key search and validation
- Authors: João Mota, Miguel Frade, Patrício Domingues

Face Detection

- Source code can be found here https://github.com/AlexXandreE/Autopsy-Plugin-2017-FaceDetection

- This is a face detection and face recognition module,
  it will find the files to use using the filemanager and copy them to the /temp folder.
  Will mark files with faces as interesting file hit, and the recognition face as Wanted.
- Authors: Alexandre Frazao, Patricio Domingues

Amcache Scan

- Source code can be found here https://github.com/0xbecca/Amcache_Scan

- The module will parses the following key: - Amcache.hve\Root\File*?*? - Amcache.hve\Root\Programs*? - Amcache.hve\Root\InventoryApplicationFile*? - Amcache.hve\Root\InventoryDeviceContainer*? - Amcache.hve\Root\InventoryDevicePnp*? - Amcache.hve\Root\InventoryDriverBinary*? - Amcache.hve\Root\InventoryDriverPackage*? - Amcache.hve\Root\InventoryApplicationShortcut*?
- After the keys are parsed, the results are added to Autopsy, then the VirusTotal scanning begins using the SHA1 hashes from Amcache.hve\Root\File*?*? and Amcache.hve\Root\InventoryApplicationFile*?.
- Author Rebecca Anderson

FDRI - Facial Detection and Recognition in Images module

- Source code can be found here https://github.com/FDRI/FDRI-Autopsy

- FDRI is a image analysis module that focus in finding human faces in images, as well finding images that contain a specific person. It provides this functionality's appealing to AI Convolutional Neural Networks. The executable is a implementation of facial detection and recognition with Dlib DNN(http://dlib.net/).
- The facial recognition element is activated when selecting a folder with images from the person that the program should look for, it will look for the person and if it finds, marks it as interesting file hit.
- All the detectors used can be found at: https://github.com/davisking/dlib-models
- Authors: Alexandre Frazão, Patrício Domingues

Image Classification

- Source code can be found here https://github.com/freakstatic/image-classification-server and https://github.com/freakstatic/image-classification

- The module performs automatic classification of objects that it find in images. It can detect a wide variety of objects (cars, guns, etc.—the user can select the type of objects he/she wants to detect) in the images (.png, jpg, etc.) of a digital forensic image loaded within Autopsy. The module relies on Yolo and has a distributed architecture: the server parts run on top of node.js and requires, for proper performance, an NVIDIA GPU. It makes use of the open source YOLO image classifier. The client runs on the Autopsy side. The module was designed this way, so that a single server (possibly fitted with a powerful NVIDIA GPU—Titan XP) in a digital forensic lab can be shared with multiple workstations running Autopsy. Note that although “Image Classification for Autopsy” runs on a node without an NVIDIA GPU, the performance is significantly impacted.
- Authors: Ricardo Maltez, Rúben Caceiro, Patrício Domingues

Hyun Yi

- Source code can be found here https://github.com/hy00un/Autopsy_Plugins
- Plugins
  - HWP Parser
  - HWP Report
  - Yara
- Author: Hyun Yi

Autopsy Volatility Plugin

- Source code can be found here https://github.com/CharlMeyers/AutopsyVolatilityPlugin
- This is a plugin for Autopsy Framework that will create a memory image of a computer and then use Volatility to process this memory image. The results can then be passed off to AUtopsy so that a visual timeline can be created for investigators.
- Author Charl Meyers

Tagged Files Report Module

- Source code can be found here https://github.com/grzesiug/autopsy_plugins
- Reporting module for Tagged files
- Author: grzesiug

Massive Extraction Filtering By Mime-Type

- Code can be found here https://github.com/cube0x8/autopsy-massive_extraction
- Designed to automatically extracts files from a device image, filtering them by (Apache Tika) mime-type.
- Author: cube0x8

Email Slicer

- Code can be found here https://github.com/labcif/EmailSlicer
- Split individual email messages from large files (e.g. PST files) within the scope of final project from the Computer Science Degree fromn ESTG "Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Leiria", Portugal.
- Author: André Agostinho Nogueira

YourPhoneAnalyzer

- Code can be found here https://github.com/labcif/YPA
- Extract information from the 'Your Phone' Windows 10 App
- Author: Luís Miguel Andrade, João Victor Silva, Patrício Domingues, and Miguel Frade.

Windows10 Facebook App Data Parser

- Code can be found here https://github.com/group305/windows10-facebook-app-data-parser
- Parse SQLite Databases generated by the Facebook App on Windows 10 platforms.
- Author: mcoates1

Proton Mail

- Source code can be found here https://github.com/dkarpo/autopsy-plugins
- Performs basic parsing of the ProtonMail database and attempts to extract as much clear text data as possible.
- Note: Much of the data within ProtonMail is encrypted so you may want to analyze the 'proton.db' manually. Also, this module, like most things I write, is not 100% complete!
- Author Derrick Karpo

Mark McKinnon's Plugins

- You can get the source code here https://github.com/markmckinnon/Autopsy-Plugins

- Installer module available that will install plugins for you
- Version 1.1 of Plugin installer works for version 4.6 and below
- Version 1.2 of plugin installer works for Autopsy version 4.7+
- Version 1.2 has Linux support for most of the plugins.
- 53 total plugins, 3 for developers, 50 for production use.

Developer Plugins

- GUI Test
- Gui Test with Settings
- Remove

Forensic Examiner Plugins

- Amazon Echosystem Parser
- Atomic Wallet
- BAM Key
- ClamAV Hashets
- CCM Recently Used Apps
- Create Datasource Hashset
- Create Preview Data Container
- Cuckoo
- EML_Parser
- File History
- Jump List AD
- Mac FS Events
- Mac OSX Recent
- Mac OSX Safari

Forensic Examiner Plugins

- Mac Mail
- Parse Plists
- Parse SAM
- Parse SQLite Databases
- Parse SQLite Deleted Records
- Parse Shellbags
- Parse USNJ
- Plaso (2 separate plugins)
- Process ActivitiesCache
- Process Amcache
- Process APPX Programs
- Process APPX Reg Programs
- Process EVTX

Forensic Examiner Plugins

- Process EVTX by Eventid
- Process Extract VSS
- Process Facebook Chats
- Process Prefetch Files
- Process SRUdb
- Process TeraCopy
- Process Windows Mail
- Recycle Bin
- Shimcache Parser
- Spotlight Parser
- Thumbcache Parser

Forensic Examiner Plugins

- Thumbs Parser
- Timesketch
- Volatility (3 separate plugins)
- Webcache
- Windows Internals
- Hash Images
- iTunes Backup
- DJI Phantom Drone Parser

Custom Report Module Created for The DGPTC - Technical Police.

- Source code can be found here https://github.com/markmckinnon/Custom_Autopsy_Plugins/tree/master/Report_Modules/SPAI_Model_Report_Module

- Custom Report Module Created for The DGPTC - Technical Police.
- Author: Mark McKinnon

What's Next

What are your needs?

What do you want to see?

Help us help you.

Contact Info

- Mark.McKinnon@Davenport.edu