Morgan Stanley

Tag, you're it!
Streamlining Privilege Review Using Open Source Tools

Emily Wicki

Digital Forensics Investigator

Insider Threat Investigations

Legal Privilege & The Review Process in a Nutshell

Attorney-Client Privilege:

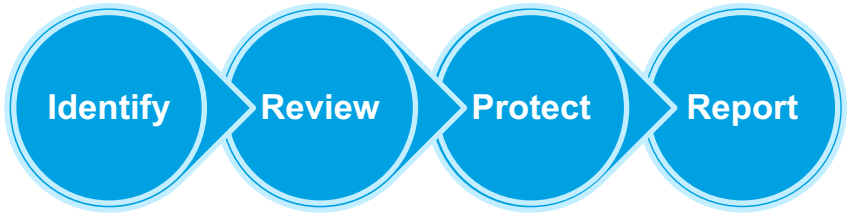
Preserves the confidentiality of communications between lawyers and their clients.

Work-Product Doctrine:

Protects certain prepared materials and information from discovery.

Legal Privilege Reviews:

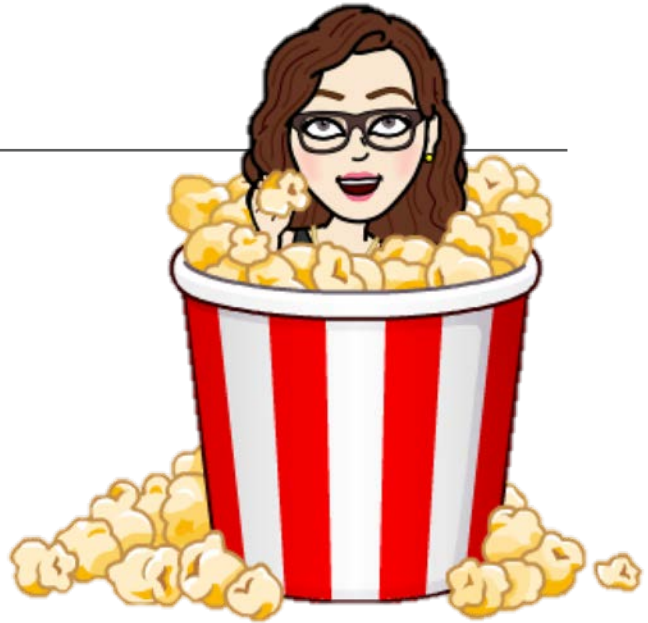
The exercise of identifying privileged, confidential, and protected information and materials to withhold from discovery.



The nature of digital evidence requires a partnership between legal and technical experts.

Morgan Stanley

Setting the Scene



Morgan Stanley

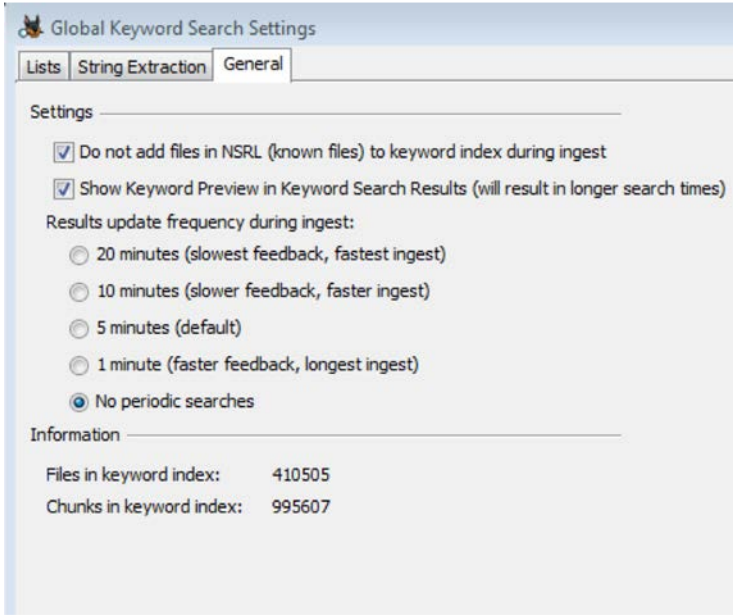
Identifying Potentially Privileged Material

Identifying Potentially Privileged Material

Apply a "Privilege Filter"

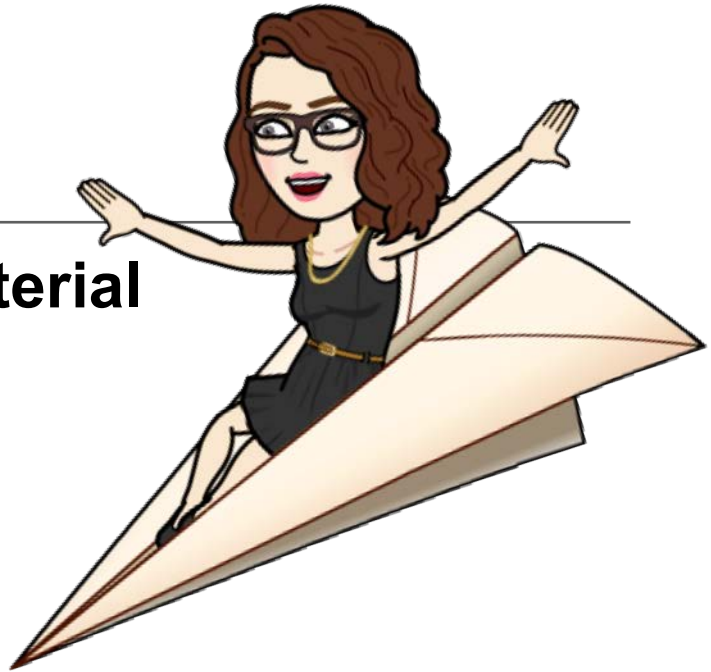
Autopsy keyword search:

- Extracts text and strings from more than a thousand file types
- Provides options to
  - Exclude or include "knowns"
  - Search by regex and/or exact match



Morgan Stanley

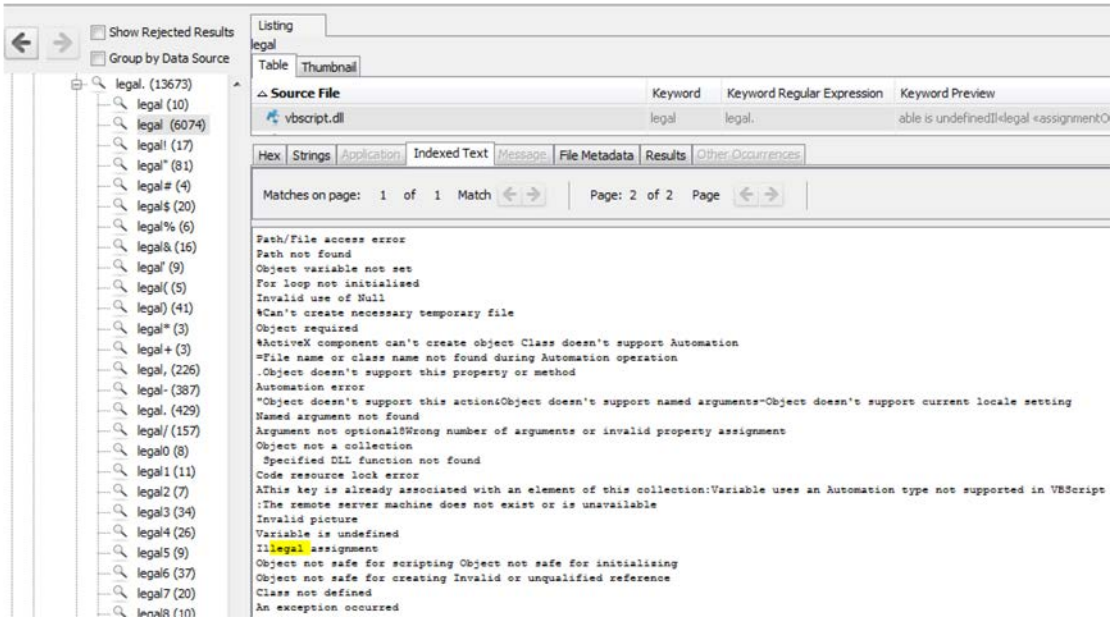
Reviewing Potentially Privileged Material



Reviewing Potentially Privileged Material

Keyword Search Results

- Organized by search parameters
- Appear in the directory tree on the left panel
- Can be reviewed by the forensics examiner
  - For obvious false-positives
  - For hits within technical artifacts



Reviewing Potentially Privileged Material

Tag & Export

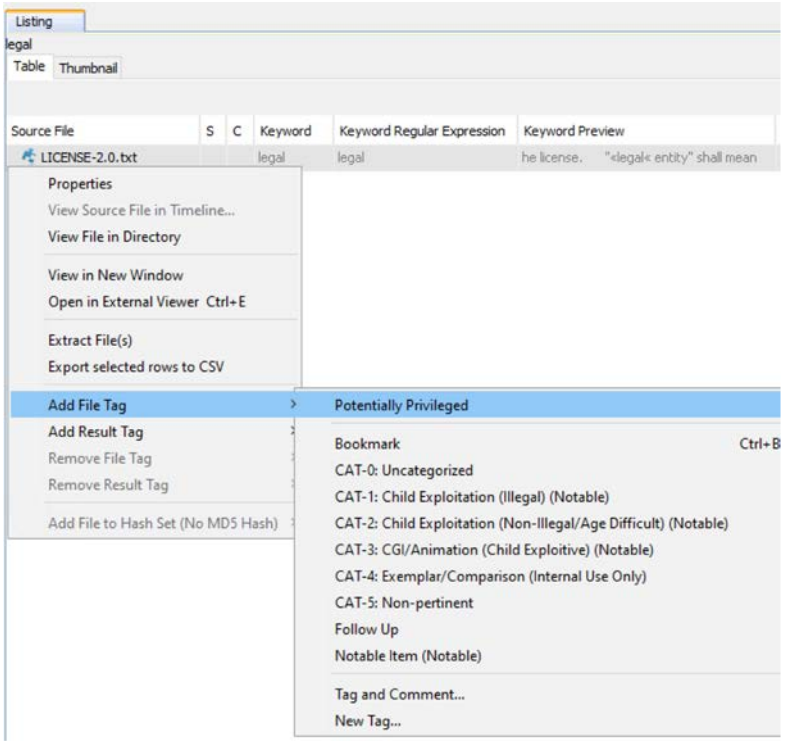
Tag items responsive to the privilege filter

- Take care to “Tag File”
  - (not “Tag Result”)

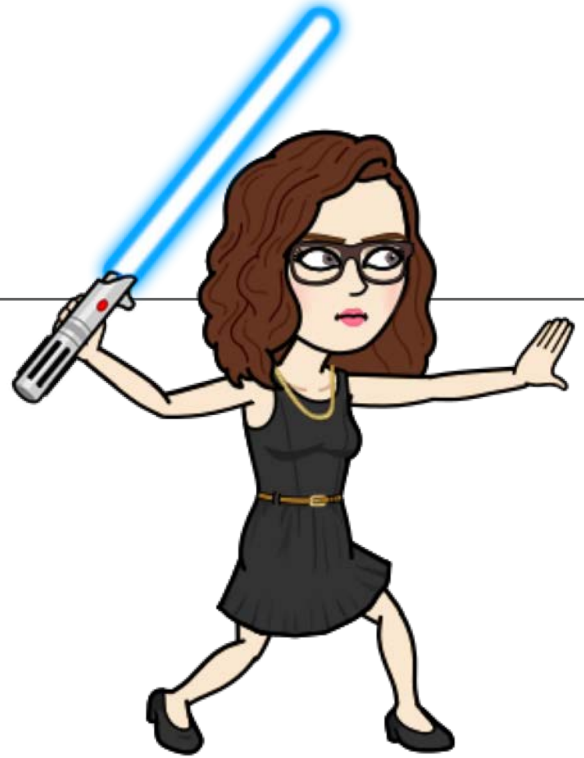
Generate a report

- A “Portable Case” exports the tagged items along with an Autopsy case file

The tagged items can be reviewed by counsel within Autopsy and tagged to flag actually privileged material



Morgan Stanley



Protecting Privileged Material

Protecting Privileged Material

Use Autopsy & dd

- Open the portable case in Autopsy
  - Identify each privileged item
    - Note its size and location
- Use dd on a copy of the image
  - Overwrite the privileged data with zeros
  - The output is a redacted copy of the image

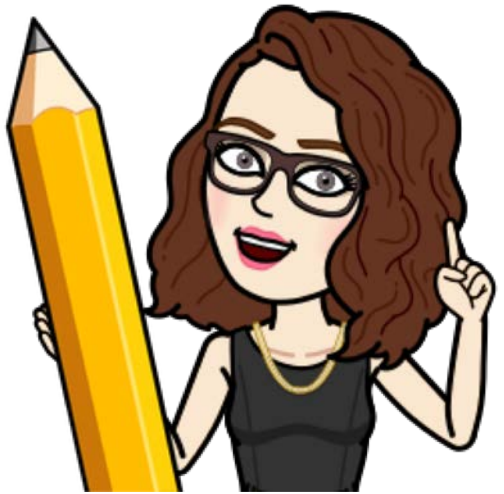
The redacted image can be reviewed in Autopsy to verify the results are as intended

Morgan Stanley

Reporting

Generating a Privilege Log & Documenting Actions

- Built-in logging functionality helps document the examiner's actions
- The Report Generator provides the appropriate options for building your privilege log
  - Select the results tagged as privileged
  - Use the Results Pane to preview information about each file
  - Export the information that's most appropriate for your report



Morgan Stanley

Questions?