

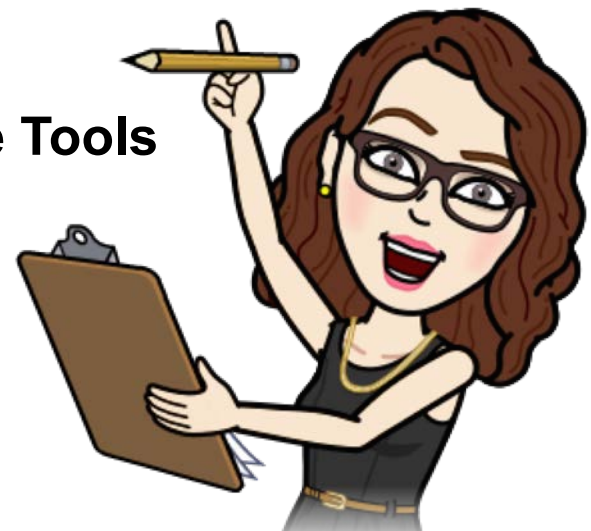
Morgan Stanley

# 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:

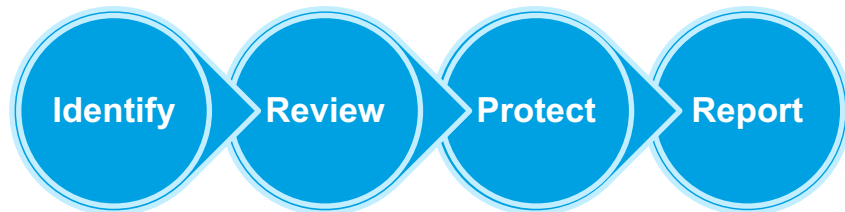
Preserves the confidentiality of communications between lawyers and their clients.

## 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.

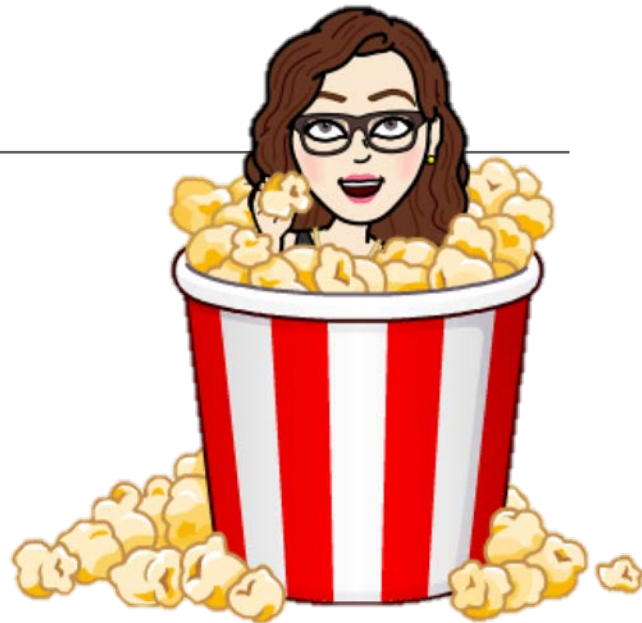


The nature of digital evidence requires a partnership between legal and technical experts.

Morgan Stanley

---

## Setting the Scene



Morgan Stanley



---

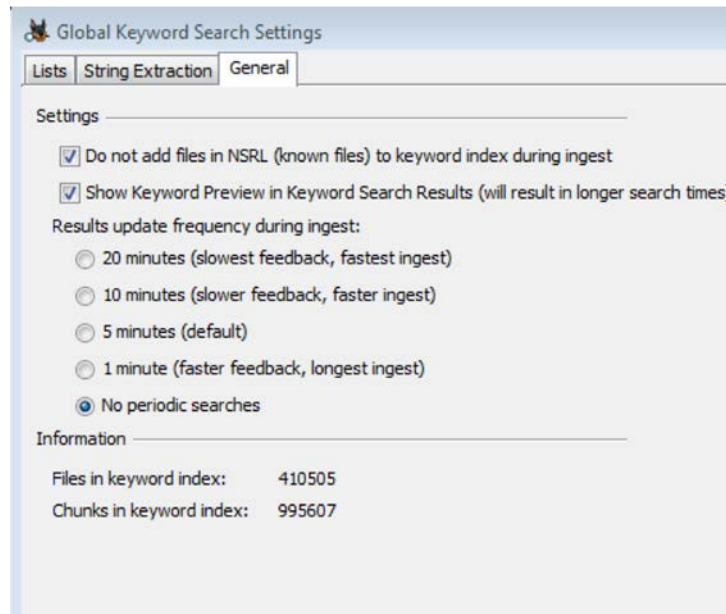
## Identifying Potentially Privileged Material

# 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

The screenshot displays a search interface with a directory tree on the left and a results pane on the right. The directory tree shows a search for 'legal' with various results counts. The results pane shows a table with columns for 'Source File', 'Keyword', 'Keyword Regular Expression', and 'Keyword Preview'. Below the table, there are tabs for 'Hex', 'Strings', 'Application', 'Indexed Text', 'Message', 'File Metadata', 'Results', and 'Other Occurrences'. The 'Results' tab is active, showing a list of matches on page 1 of 1. The matches include various error messages and warnings, such as 'Path/File access error', 'Object variable not set', and 'Illegal assignment'.

Source File	Keyword	Keyword Regular Expression	Keyword Preview
vbscript.dll	legal	legal.	able is undefined  legal <assignmentO

Matches on page: 1 of 1 Match

Path/File access error  
Path not found  
Object variable not set  
For loop not initialised  
Invalid use of Null  
\*Can't create necessary temporary file  
Object required  
\*ActiveX component can't create object Class doesn't support Automation  
\*File name or class name not found during Automation operation  
\*Object doesn't support this property or method  
Automation error  
\*Object doesn't support this action|Object doesn't support named arguments-Object doesn't support current locale setting  
Named argument not found  
Argument not optional|Wrong number of arguments or invalid property assignment  
Object not a collection  
Specified DLL function not found  
Code resource lock error  
!This key is already associated with an element of this collection:Variable uses an Automation type not supported in VBScript  
:The remote server machine does not exist or is unavailable  
Invalid picture  
Variable is undefined  
Illegal assignment  
Object not safe for scripting Object not safe for initialising  
Object not safe for creating Invalid or unqualified reference  
Class not defined  
An exception occurred

# Reviewing Potentially Privileged Material

## Tag & Export

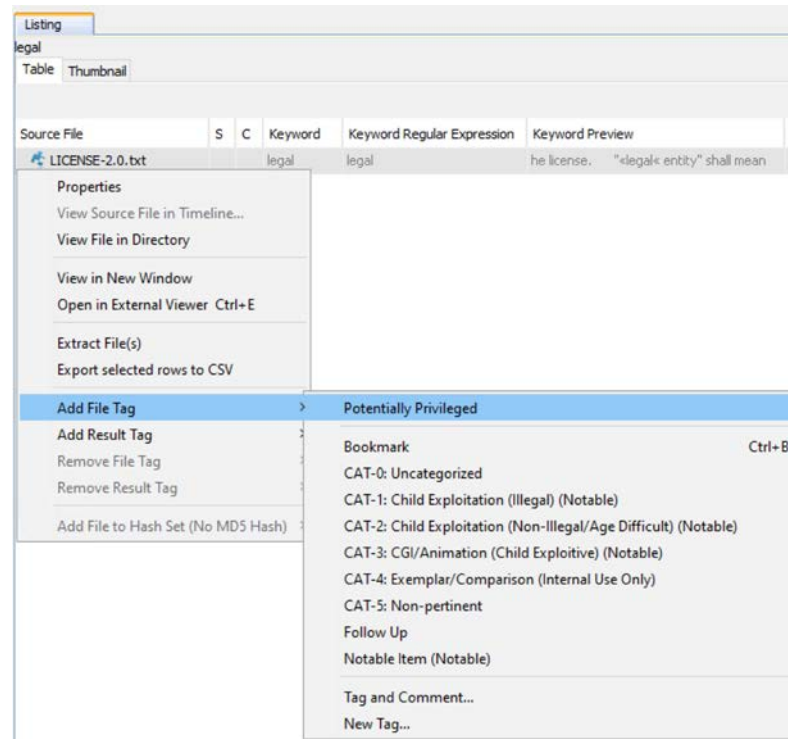
Tag items responsive to the privilege filter

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

Generate a report

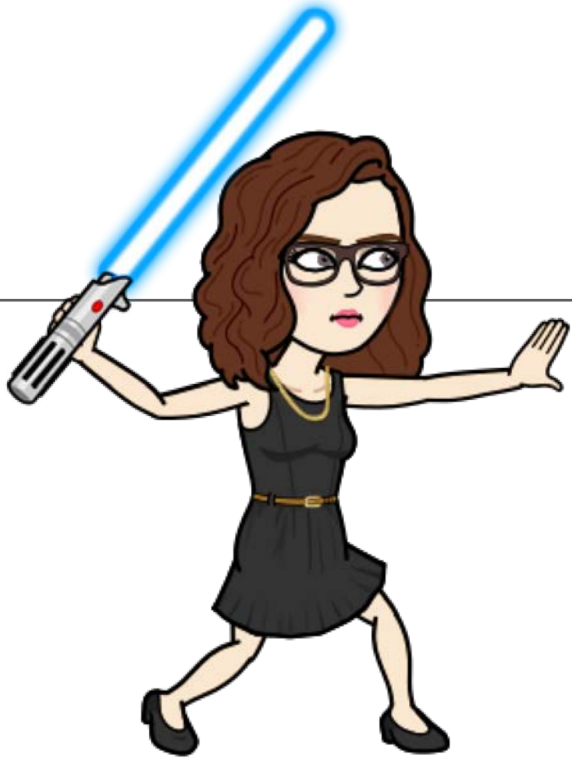
- A “Portable Case” exports the tagged items along with an Autopsy case file

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?**