

Digital Evidence

Week 7 – Creating Productions & Types of Experts

Shawn Davis
ITMS X83 – Spring 2026

Slides contain original content from Davis, S. and
E-discovery: An Introduction to Digital Evidence



Last Week - Review

- Kahoot Review – 22 questions
 - 20 seconds for multiple choice
 - 10 seconds for true and false

Overview

1. Everlaw: Uploading Native Docs for a Production
2. Everlaw: Finding Responsive Docs for a Production
3. Everlaw: Creating a Production
4. Managing E-discovery
5. Digital Forensics Consultants and Examiners
6. E-discovery Consultants
7. Special Masters and Forensics Mediators

Objectives

- Demonstrate using Everlaw to create a production
- Summarize the developments in managing discovery
- Explain the roles of digital forensics consultants and examiners in civil and criminal cases
- Describe when to use e-discovery consultants, including outsourcing factors
- Explain when to use special masters and forensics mediators
- Summarize best practices in e-discovery team management

Everlaw

- This week we cover how to create a production and find responsive documents
- Next week we will cover:
 - How to load an existing production with load files
 - Troubleshoot load file errors
 - Search for potential evidence and tag it

Part I

Everlaw: Uploading Native Documents for a Production

Note

- Everlaw can be used to create as well as review productions
- Therefore, you would use similar steps to:
 - Be the producing party and upload documents that will eventually become a production that you will send to the receiving party
 - We are covering this example now.
 - Be the receiving party and upload a production that you have received from a producing party
 - We will cover this next week

Everlaw: Creating Your Account

- Open your IIT email that says:
 - [Everlaw] Shawn Davis invited you to “Illinois Institute of Technology”
- Click “Create account”

Everlaw: Creating Your Account

- Fill out the form
- Job title: Student
- Create Account
- Scroll down, accept terms and “Continue”
- Check your email again for the auth code
- Logon with creds you created

Create your Everlaw account

First name

Last name

Email address

Job title

Create password

Confirm password

Passwords must:

- Be a minimum of 8 characters
- Not contain repeating digits
- Not contain sequential digits (e.g. 1234)

Create account

Everlaw: Home Screen

- X out of the yellow banner and purple release note if shown

The screenshot displays the Everlaw home screen. At the top, a yellow banner contains the text: "Production Mastery Webinar Series Part II: Quality Control and Modifications on Feb. 24th! Part I now available on-demand. [Register for both sessions today.](#)". To the right of this banner is a red rectangular box containing two 'X' icons, indicating where to click to close the banner. Below the banner is a large purple section titled "WHAT'S NEW ON EVERLAW". It features the text: "Overlay Metadata Using a Custom Unique Identifier, a New OCR Option That is Optimized for Handwriting, and More!". To the right of this text is a screenshot of the Everlaw document review interface. This interface shows a table of documents with columns for Type, Row #, Bates/Contr..., Document Sec, Num P..., Rat..., Coded, Notes, and Name. A modal dialog titled "Confirm reprocessing" is open in the center of the interface, asking the user to confirm that documents with highlights or image redactions will not be reprocessed. To the right of the document review interface is a green vertical button labeled "Walk Me Through" with a downward arrow and an 'X' icon in the top right corner.

Production Mastery Webinar Series Part II: Quality Control and Modifications on Feb. 24th! Part I now available on-demand. [Register for both sessions today.](#)

WHAT'S NEW ON EVERLAW

Overlay Metadata Using a Custom Unique Identifier, a New OCR Option That is Optimized for Handwriting, and More!

Everlaw BlockVault

Binder Documents to Review grouped by a... Created 1:38 PM PST

5 selected / 5 total • 4 Attachment groups • Default grouping

Type	Row #	Bates/Contr...	Document Sec	Num P...	Rat...	Coded	Notes	Name
Email	1	497						Marcus Th...
Email	2	49740.1						Gabrie Hu...
Email	3	49.1						Patrick An...

Confirm reprocessing

Please confirm the following:

- Docs with highlights or image redactions will not be reprocessed

Cancel Process

Walk Me Through

Everlaw: Home Screen

The screenshot displays the Everlaw Home Screen. At the top, the Everlaw logo is on the left, and the text "Illinois Institute of Tec" is followed by a home icon, a refresh icon, a search icon, a bar chart icon, a document icon, an envelope icon, a user icon, and a help icon. Below the header, the left sidebar contains a "Filter cards" input field, a list of navigation items: "All" (selected), "Favorites", "Mine", "Shared with me", and "Document overview" (with a bar chart icon). At the bottom of the sidebar is a "Folders" section with a folder icon, a plus icon, and a "Filter folders" input field. The main content area is titled "All" and includes a "View all documents" button. Below the title, there are two sections: "Assignments" with a "Learn more" link and a dashed box containing the text "+ Create a new Assignment Group", and "Searches" with a plus icon and a refresh icon. The "Searches" section lists two items: "SEARCH All Documents" with 10,679 documents and a star icon, and "SEARCH TERM REPORT Untitled" with 652 documents, a red "NG" badge, and a star icon.

Everlaw

Illinois Institute of Tec

Filter cards

All

Favorites

Mine

Shared with me

Document overview

Folders

Filter folders

All

Assignments [Learn more](#)

+ Create a new Assignment Group

Searches

SEARCH All Documents 10,679

SEARCH TERM REPORT Untitled 652 NG

View all documents

EDRM Free Micro Datasets

- I have uploaded the EDRM Public Micro Dataset from:

- <https://www.edrm.net/resources/data-sets/edrm-micro-datasets/>

- Contents:

- A variety of.csv files
- Websites and web pages
- Adobe Acrobat files
- Graphic files and photographs
- Public census data
- Microsoft Office files
- Audio files
- 4 email boxes with shared correspondence, threads and attachments
- Multiple Encase .e01 files containing data from a phone and another data source

Everlaw: Upload

- You can upload single files or multiple files at once
- Multiple files need to be placed into a single zip file
- We'll go over the upload process as a lab in a moment

Everlaw: Database vs Project

- Database:
 - Holds clean copy of all data uploaded
- Projects:
 - Where documents are organized, annotated, and coded by reviewer team

Everlaw: Upload

- We are going to pretend we are the producing party and are gathering evidence to upload into Everlaw to:
- Review and find responsive documents
- Export into an imaged production for the receiving party
- Just watch for the next four slides

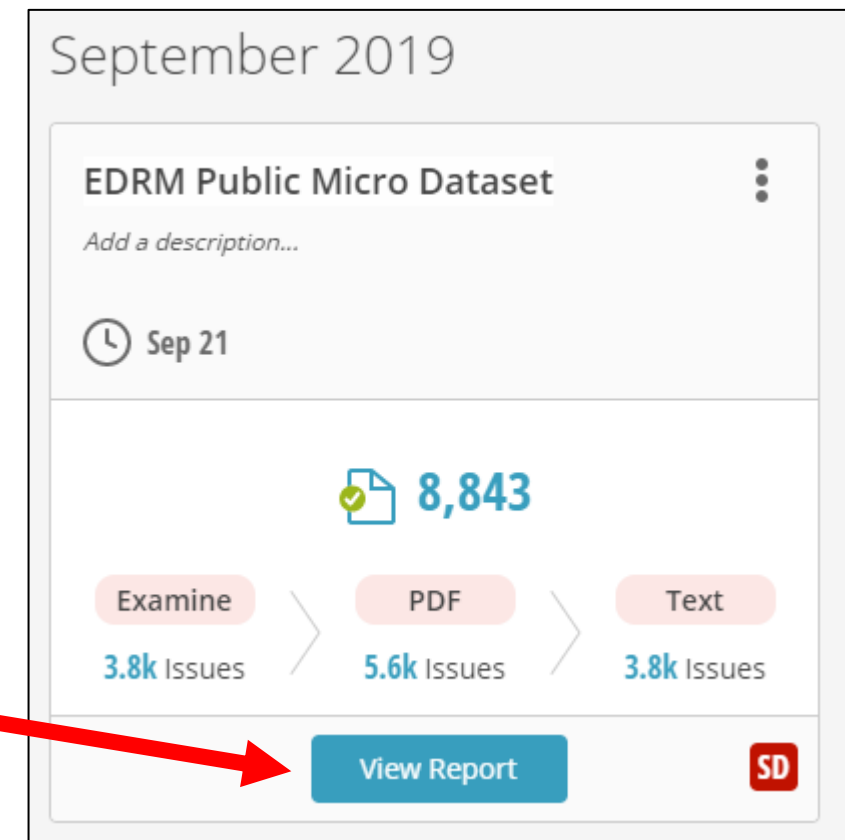
Everlaw: Upload

- Once I uploaded the Public Micro dataset, processing starts:

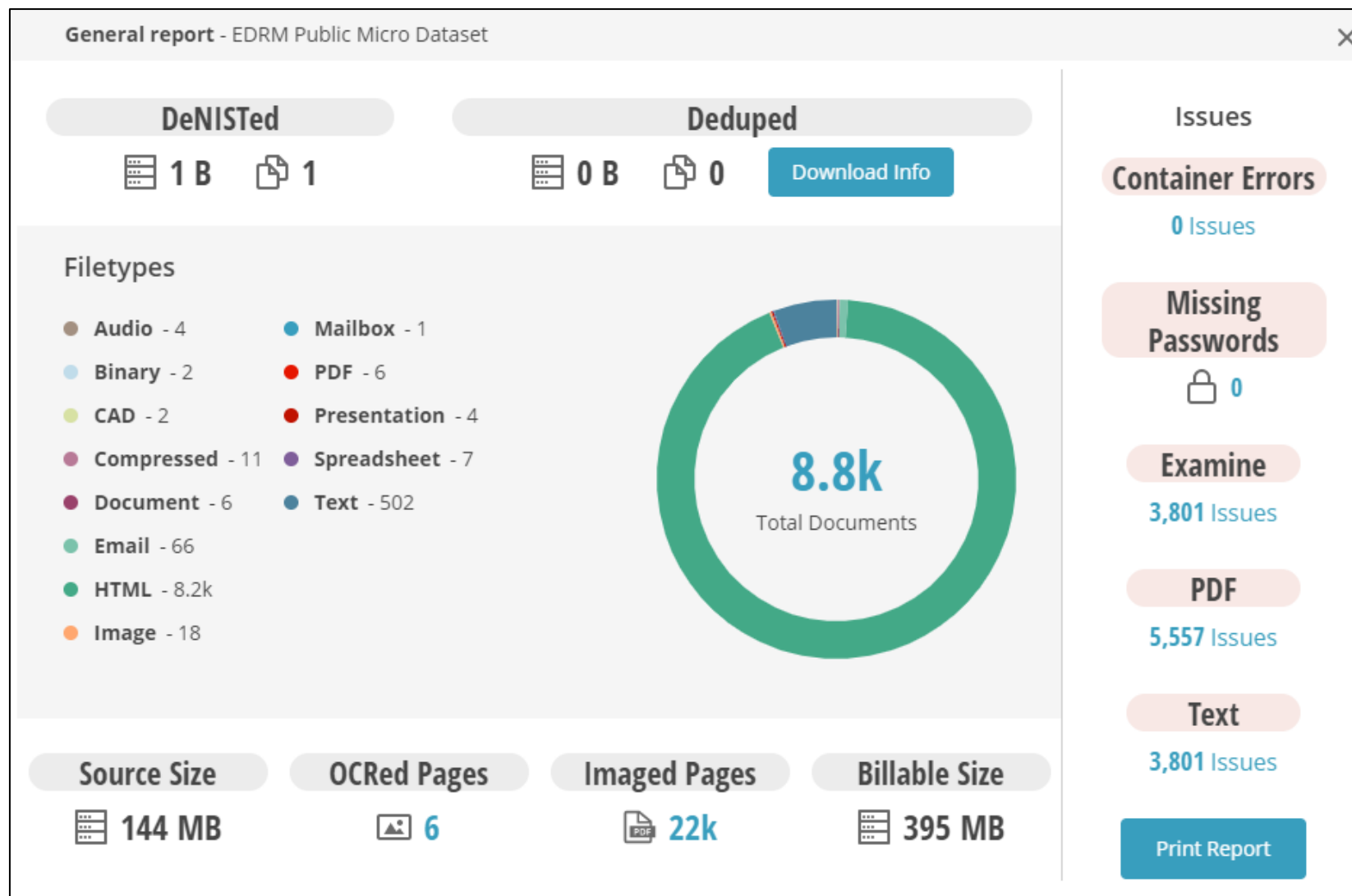
The screenshot displays the 'Native Data' interface in Everlaw. At the top, there is a search bar labeled 'Filter cards' and a 'Filter By Date' dropdown menu set to 'Any'. Below this, the date 'September 2019' is shown. The main content area features a card for the 'EDRM Public Micro Dataset'. The card includes a three-dot menu icon, a description field with the placeholder 'Add a description...', and a clock icon next to the date 'Sep 21', with a 'Cancel' button to its right. A progress bar indicates the status 'PROCESSING' with the text '471 / 7,795 docs, 0h 12m'. Below the progress bar, a document icon with a checkmark is followed by the number '7,412'. At the bottom of the card, there are three tabs: 'Examine' (with 'No Issues' below it), 'PDF' (with 'No Issues' below it), and 'Text' (with 'No Issues' below it). A blue 'View Report' button is located at the bottom center of the card, and a red 'SD' icon is in the bottom right corner.

Everlaw: Upload

- Once processing is finished, you can view a full report:

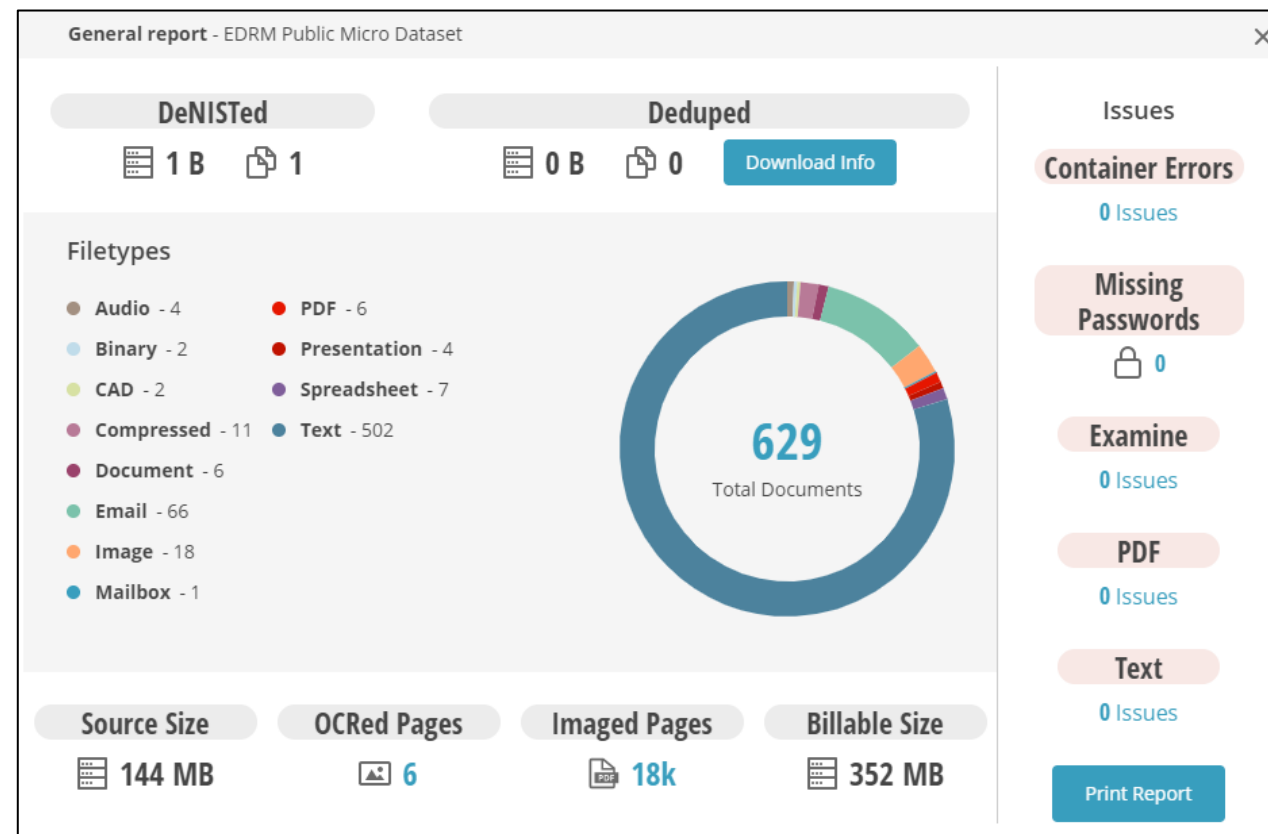


Everlaw: Public Micro Report



Everlaw: Public Micro Report

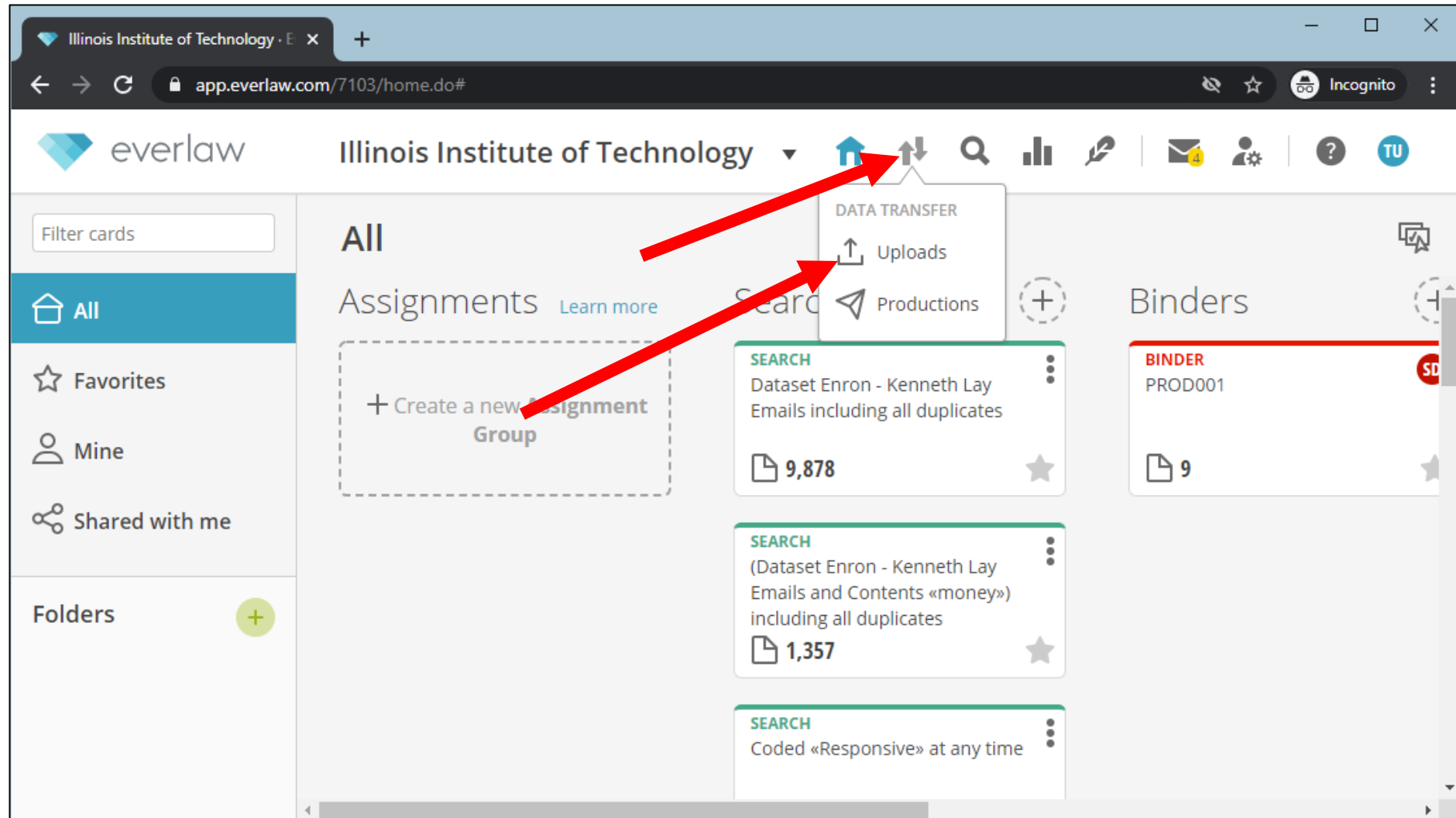
- I removed the 8k html files just to make things a little easier to go through later



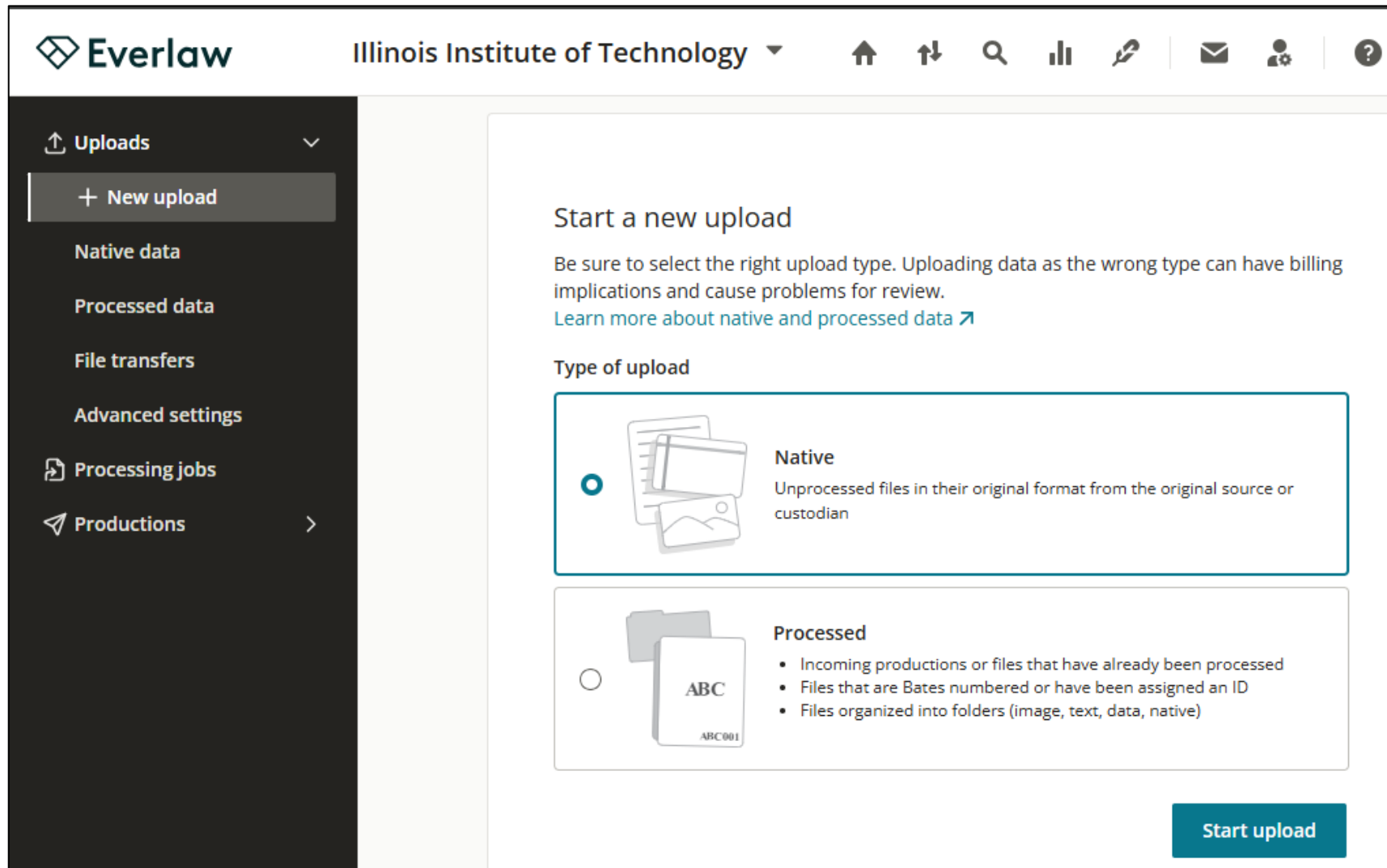
Lab 1: Uploading a Document

- I will walk you through how to upload a document
- Pay close attention on where the menu options are located as you will upload a second document on your own without the step by step directions after this walk through

Lab 1: Uploading a Document



Lab 1: Uploading a Document



The screenshot displays the Everlaw web application interface. The top navigation bar includes the Everlaw logo, the text "Illinois Institute of Technology" with a dropdown arrow, and several utility icons (home, upload, search, bar chart, pencil, envelope, user, and help). A dark sidebar on the left contains a menu with "Uploads" (expanded), "New upload", "Native data", "Processed data", "File transfers", "Advanced settings", "Processing jobs", and "Productions". The main content area is titled "Start a new upload" and includes a warning about selecting the correct upload type. Below this, the "Type of upload" section offers two options: "Native" (selected with a radio button) and "Processed" (unselected). The "Native" option is described as "Unprocessed files in their original format from the original source or custodian". The "Processed" option is described with a list of criteria: "Incoming productions or files that have already been processed", "Files that are Bates numbered or have been assigned an ID", and "Files organized into folders (image, text, data, native)". An illustration of a folder labeled "ABC" with a sub-label "ABC001" is shown next to the "Processed" option. A teal "Start upload" button is located at the bottom right of the main content area.

Everlaw Illinois Institute of Technology

Uploads

- + New upload
- Native data
- Processed data
- File transfers
- Advanced settings
- Processing jobs
- Productions

Start a new upload

Be sure to select the right upload type. Uploading data as the wrong type can have billing implications and cause problems for review.
[Learn more about native and processed data](#)

Type of upload

☒  **Native**
Unprocessed files in their original format from the original source or custodian

☐  **Processed**

- Incoming productions or files that have already been processed
- Files that are Bates numbered or have been assigned an ID
- Files organized into folders (image, text, data, native)

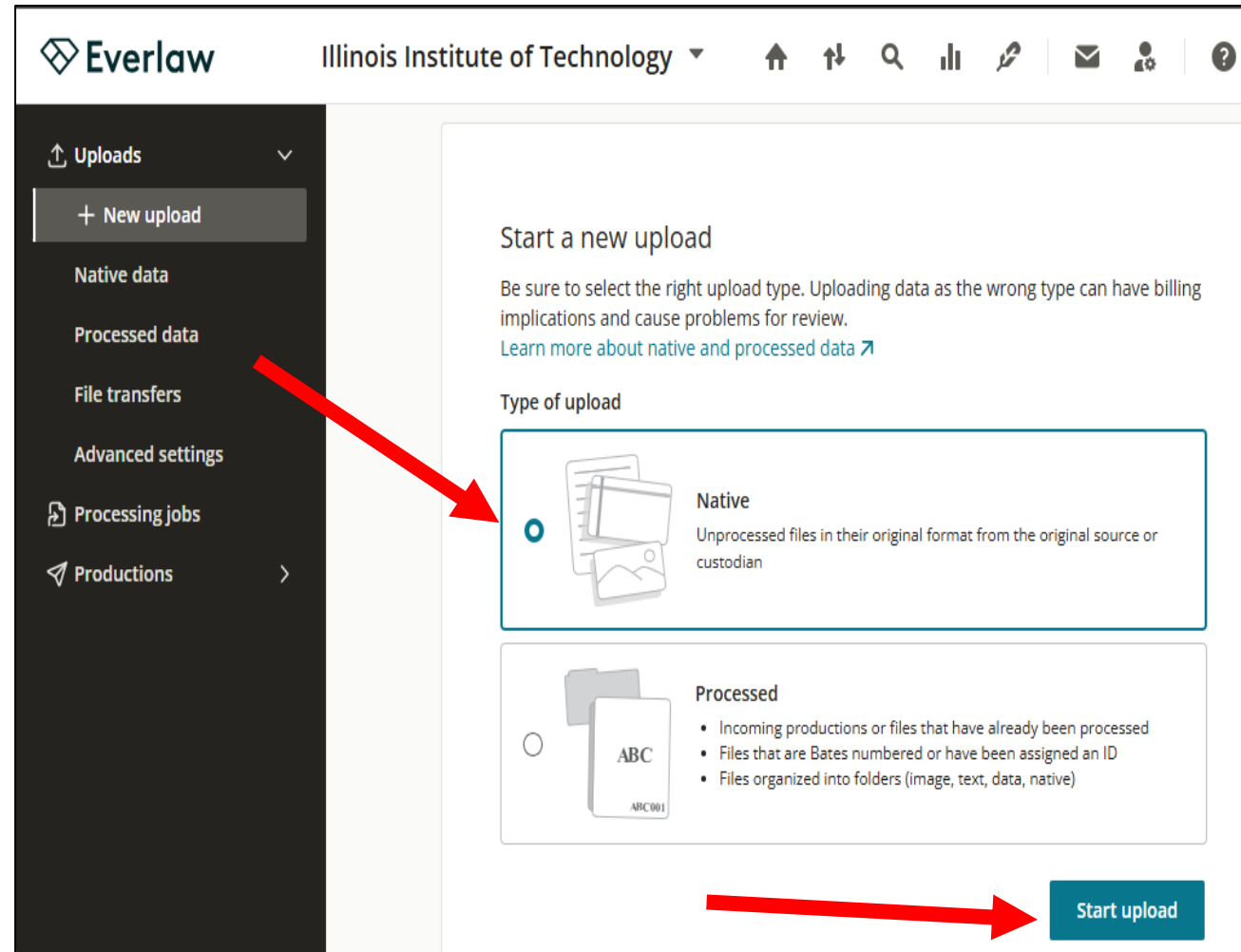
Start upload

Lab 1: Uploading a Document

- Create a word doc on your computer and name it as your lastname.docx
- Put a sentence or two in the document and save it

Lab 1: Uploading a Document

- Select “Native” and “Start upload”
- The next screen you will drag/drop or browse to your word doc



Lab 1: Uploading a Document

- Under “Name”
put your last
name
- Select “None”
for dedupe

Everlaw Illinois Institute of Technology

Upload Natives

Details Custodians Additional options Summary

Details

Custom settings

Name

Native data deduplication

Deduplication against native data always respects document families. [Learn more](#)

☐ Global
Deduplication on a family level across all custodians in the database. If two or more custodians contain the same documents, only one set will be uploaded.

☐ By custodian
Deduplication on a family level within individual custodians in the database. If two or more custodians contain the same document, both sets will be uploaded.

☒ None
No documents will be deduplicated

Cancel Next

Walk Me Through

Lab 1: Uploading a Document

- Scroll down
- Hit “Next”

Everlaw Illinois Institute of Technology

Upload Natives

Details Custodians Additional options Summary

Advanced settings

- ▶ **Language and location**
OCR language: Autodetect, Default timezone: America/Chicago
- ▶ **Image details**
PDFs: All documents, excluding file types (e.g. Excel) that do not convert well to PDF, Page size: Letter, Inline images in attachments: Smart inline images found in emails, Hyperlinked images: Do not fetch hyperlinked images, PowerPoint speaker notes: Include speaker notes with original formatting
- ▶ **Chat documents**
Segmentation: Split chat conversations by number of messages: Medium segments, Slack attachments: Fetch attachments referenced in Slack messages
- ▶ **Decryption**
- ▶ **DeNIST settings**
DeNIST: Exclude files from the NIST list

Cancel **Next**

Walk Me Through

Lab 1: Uploading a Document

- Put Test Corp as default custodian
- Hit “Next” / “Next” / “Upload”

The screenshot shows the Everlaw 'Upload Natives' workflow. The 'Custodians' step is active, indicated by a green checkmark. A red arrow points to the 'Default custodian' dropdown menu, which currently shows 'Select or enter custom value'. The interface includes a sidebar with navigation options like 'Uploads', 'Native data', and 'Processing jobs'. At the bottom are 'Cancel', 'Previous', and 'Next' buttons. A 'Walk Me Through' tooltip is visible on the right.

Lab 1: Uploading a Document

- Hit the X to close the window

Upload details for Davis

Transferring

Processing

Upload report

Transfer completed successfully

Add files

Source file	Documents	Transfer status	Actions
▼ Local upload (1)			
davis.docx 12 KB		Processing...	
Show custodian assignment			

Total:
1 source file

Lab 1: Uploading a Document

- Once processing is complete and “1” appears, hit “View Report” for your new upload named by your last name

The screenshot displays the ITMSX83 interface. On the left is a dark sidebar with navigation options: 'Uploads' (with an upward arrow icon), 'New upload' (with a plus icon), 'Native data' (highlighted), 'Processed data', 'File transfers', 'Advanced settings', 'Processing jobs' (with a document icon), and 'Productions' (with a paper plane icon). The main panel on the right has a header with 'Filter by custodian' and a dropdown menu. Below this is the date 'February 2026'. The central area shows a card for 'Davis' with a user icon 'JS' and a menu icon. It includes a link '+ Add description' and a clock icon with the date '2026/02/22'. A green checkmark and the text 'Upload complete' are displayed. Below this, a document icon with the number '1' is highlighted by a red rectangle. At the bottom, a table lists document types and their status:

EXAMINE	No issues
ARTIFACTS	No issues
PDF	No issues
TEXT	No issues

A red arrow points to a 'View report' button at the bottom of the card.

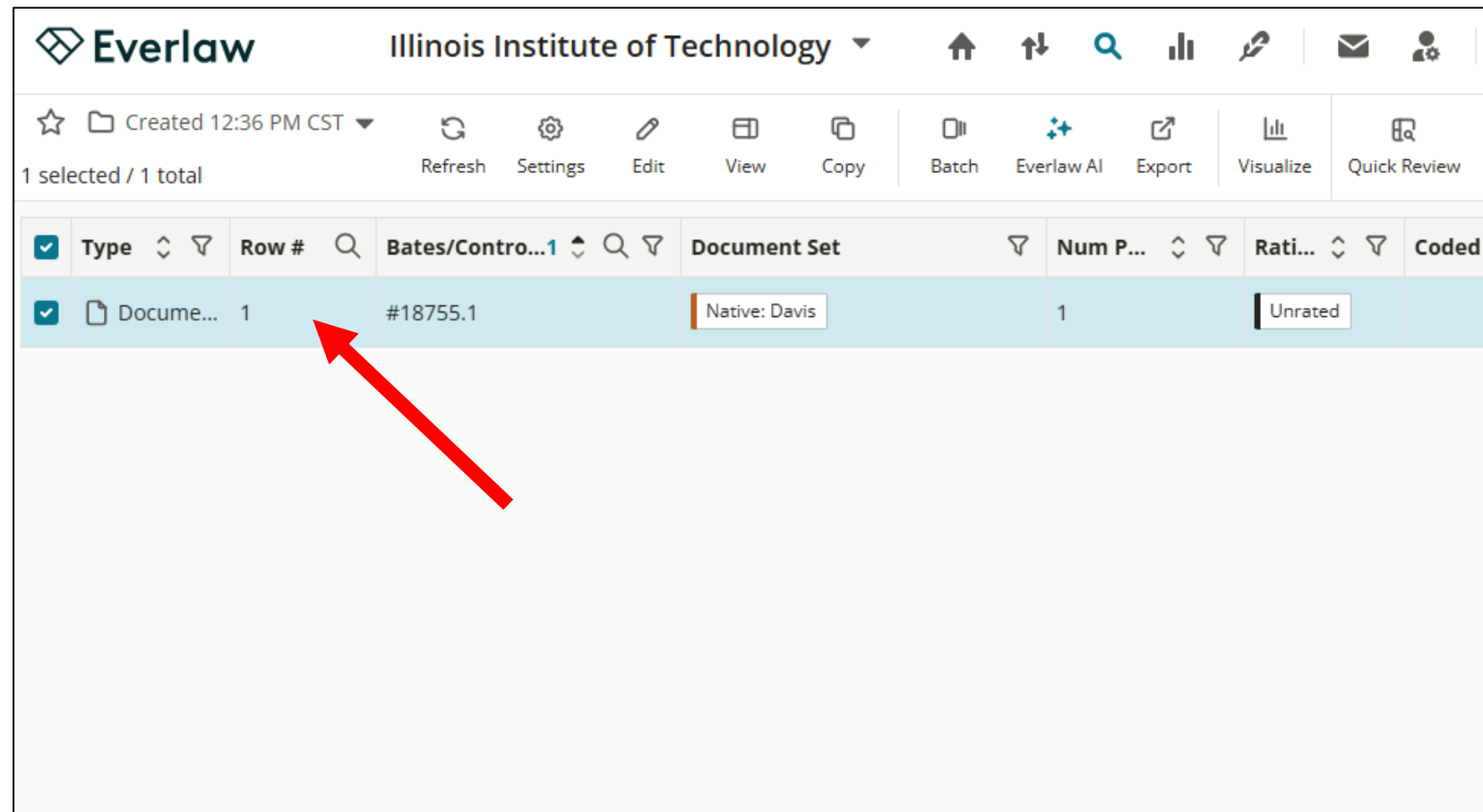
Lab 1: Uploading a Document

- Scroll down and click on the “1” after “Imaged Pages”

Upload details for Davis			
● Text	0	● Meeting	0
● Binary	0	● Profile	0
● Chat	0	● CRM ⓘ	0
● Presentation	0	● Other	0
● Audio	0		
Documents with issues			
✓ Examine errors	0	✓ Container errors	0
✓ Artifacts errors	0	✓ Missing passwords	0
✓ PDF errors	0		
✓ Text errors	0		
Flags			
✓ Flagged malicious	0		
OCRed and imaged			
🖼️ OCRed pages	0	📄 Imaged pages	1

Lab 1: Uploading a Document

- Click the top line to get to the Review window

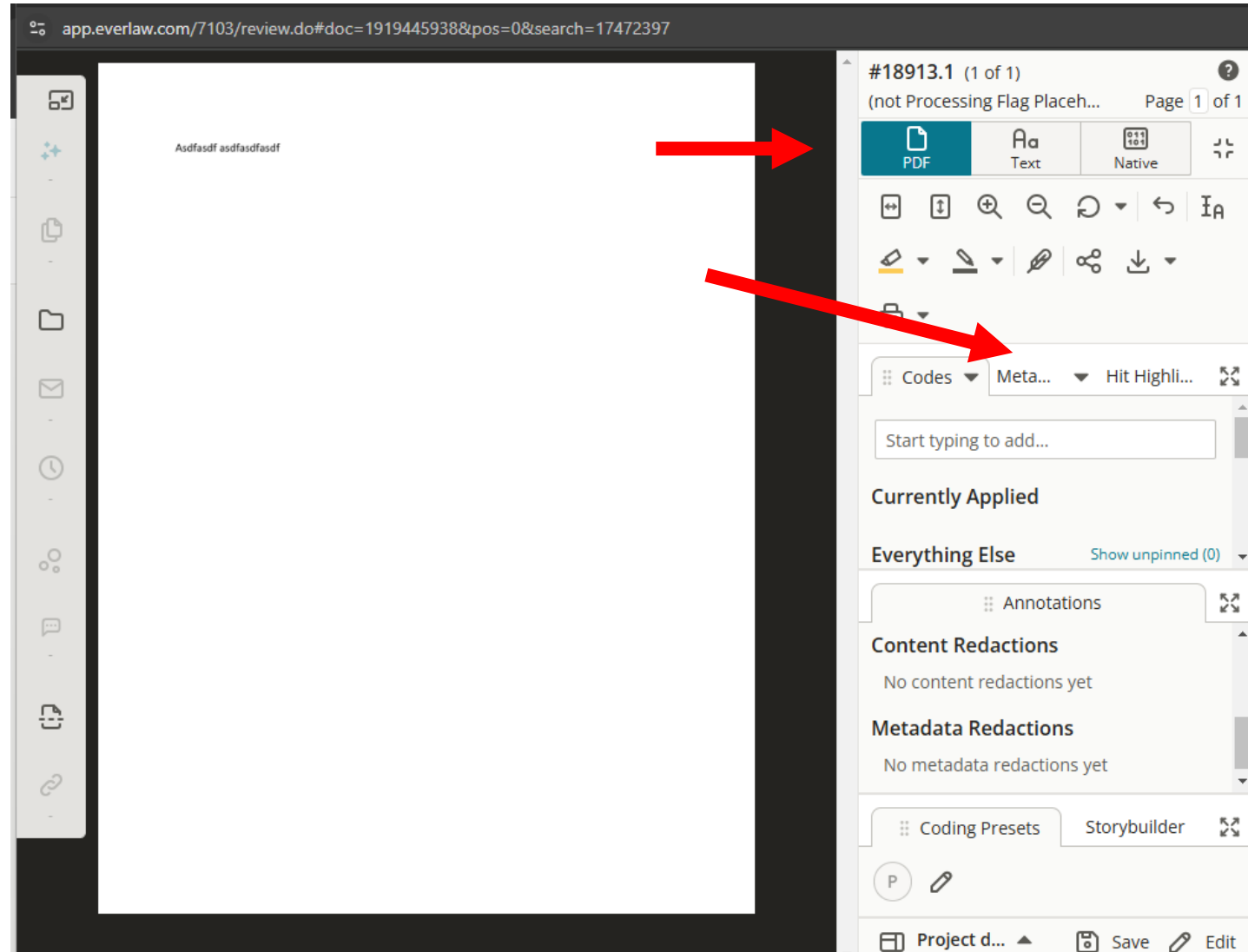


The screenshot shows the Everlaw interface for the Illinois Institute of Technology. The top navigation bar includes the Everlaw logo, the institution name, and various icons for home, upload, search, and user settings. Below this is a toolbar with icons for star, folder, refresh, settings, edit, view, copy, batch, Everlaw AI, export, visualize, and quick review. The main content area displays a table with 1 selected / 1 total document. The table has columns for Type, Row #, Bates/Contro..., Document Set, Num P..., Rati..., and Coded. The first row is highlighted in blue and contains the following data: Type: Document..., Row #: 1, Bates/Contro...: #18755.1, Document Set: Native: Davis, Num P...: 1, Rati...: Unrated, and Coded: (empty). A red arrow points to the first row of the table.

Type	Row #	Bates/Contro...	Document Set	Num P...	Rati...	Coded
Document...	1	#18755.1	Native: Davis	1	Unrated	

Lab 1: Uploading a Document

- View the doc in the PDF, Text, and Native views
- Click on “Meta..” to view the meta-data properties



Lab 1: Practice

- Close the review window
- Please create another file and upload it using the same process as before on your own
- Name this file as your lastname appended with a 2

Part II

Everlaw: Finding Responsive Documents for a Production

Flow to Add Documents to Production Binder

- I already created a “Binder” called “PROD001”
 - Close any review windows and go back to the main screen
 - Click your home button in Everlaw to see it 
- Ultimately, we can search and review documents and code the responsive ones as “Responsive”
- Then, we can search all documents with the “Responsive” code and batch add them to the “PROD001” binder

- Scroll to the right to “Document Sets” and find and click on the “EDRM Public Micro Dataset”
- You should now see all 626 documents

Illinois Institute of Technology

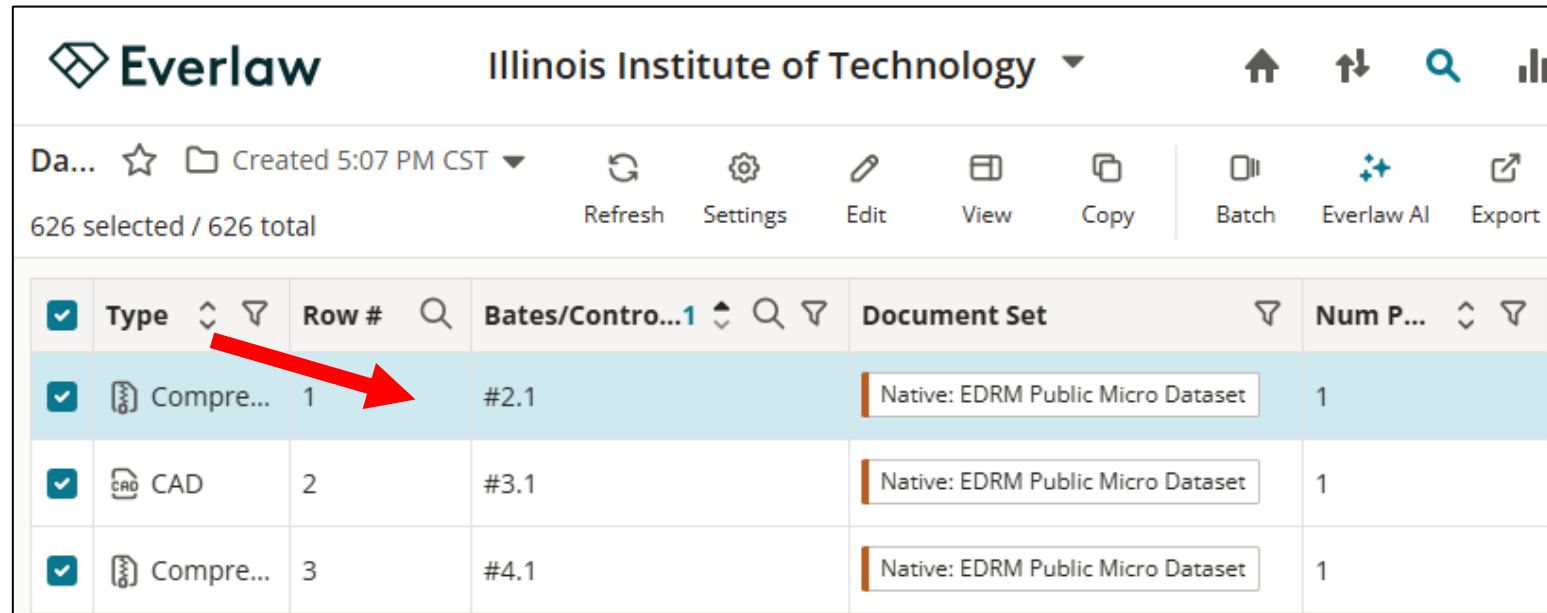
Created 5:07 PM CST

626 selected / 626 total

☒	Type	Row #	Bates/Contro...1	Document Set	Num P...	Rati...	Code
☒	Text	1	#33.1	Native: EDRM Public Micro Dataset	1	Unrated	
☒	Text	2	#36.1	Native: EDRM Public Micro Dataset	1	Unrated	
☒	Text	3	#5752.1	Native: EDRM Public Micro Dataset	1	Unrated	

Manual Review

- Click on #2.1 to open the reviewer pane
- If you don't see it, click on the Bates/Control header twice to sort small to large so that #2.1 appears on top



The screenshot shows the Everlaw interface for the Illinois Institute of Technology. The table displays document sets, with the first row highlighted in light blue. A red arrow points to the first row, which is highlighted in light blue. The table has columns for Type, Row #, Bates/Control, Document Set, and Num P....

Type	Row #	Bates/Control	Document Set	Num P...
Compre...	1	#2.1	Native: EDRM Public Micro Dataset	1
CAD	2	#3.1	Native: EDRM Public Micro Dataset	1
Compre...	3	#4.1	Native: EDRM Public Micro Dataset	1

Manual Review

- Why is it blank in PDF View?
 - It is a zip file (look at the document list filename under the Metadata tab)
- Close the reviewer window

Manual Review

- Click “Home” and select the “Enron – Kenneth Lay Emails” Document Set
- Select the #8880.1 email to open the reviewer pane

☒	Email	4	#8880.1	Native: Enron - Kenneth Lay Emails	1	Unrated
-------------------------------------	-------	---	---------	------------------------------------	---	---------

Manual Review

- Maximize the Reviewer Pane
- Drag the right gray panel to the left a little to expand it a bit

Manual Review

- How do you search for any phone numbers in the email?
 - Select Hit Highlights
 - Click on “Search document”
 - Select “Phone Numbers (US)”
 - The number is highlighted

From: <Lay>, "Kenneth" </O=ENRON/OU=NA/CN=RECIPIENTS/CN=KLAY>
To: "Lhjamail@aol.com" <Lhjamail@aol.com>
Subject: FW: Soul food dinner
Date: 2001-08-29 18:31:10 -0500

Hi Mrs. Jamail -

Ken and Linda Lay would very much like to attend the dinner on September 12. Will you please send me the details or phone me at 713-853-6773?

Thanks.

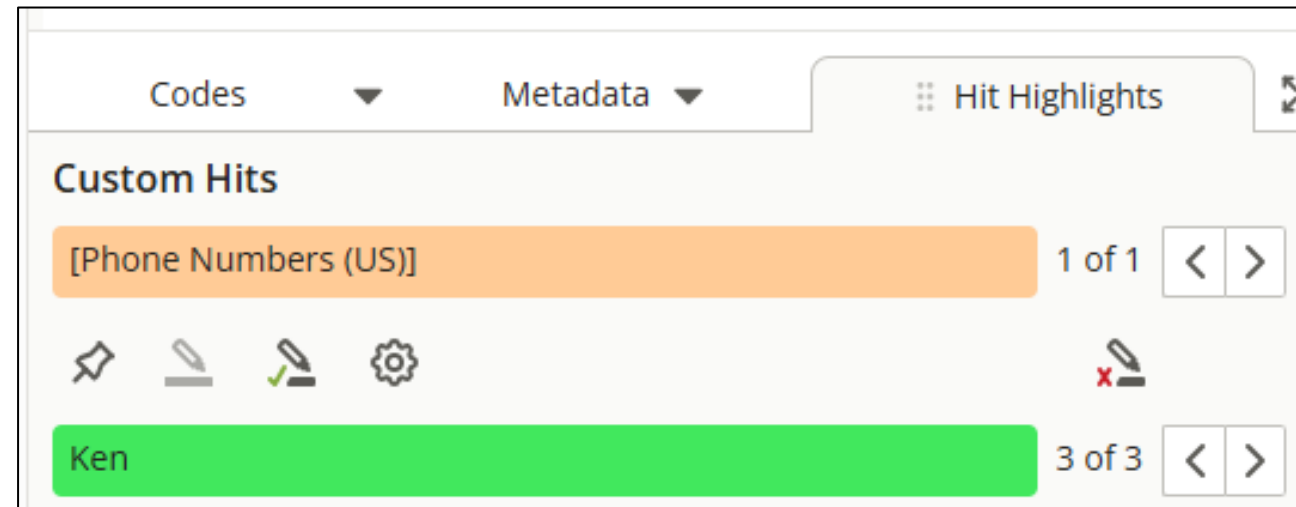
Rosalee Fleming
Assistant to Ken Lay

-----Original Message-----

From: "Linda P. Lay" <mrlinda@lplpi.com>@ENRON [mailto:IMCEANOTES-+22Linda+20P+2E+20Lay+22+20+3Cmrlinda+40lplpi+2Ecom+3E+40ENRON@ENRON.com]
Sent: Monday, August 27, 2001 6:01 PM
To: Kenneth L. Lay (E-mail)
Cc: Sally A. Keepers (E-mail); jessica
Subject: FW: Soul food dinner

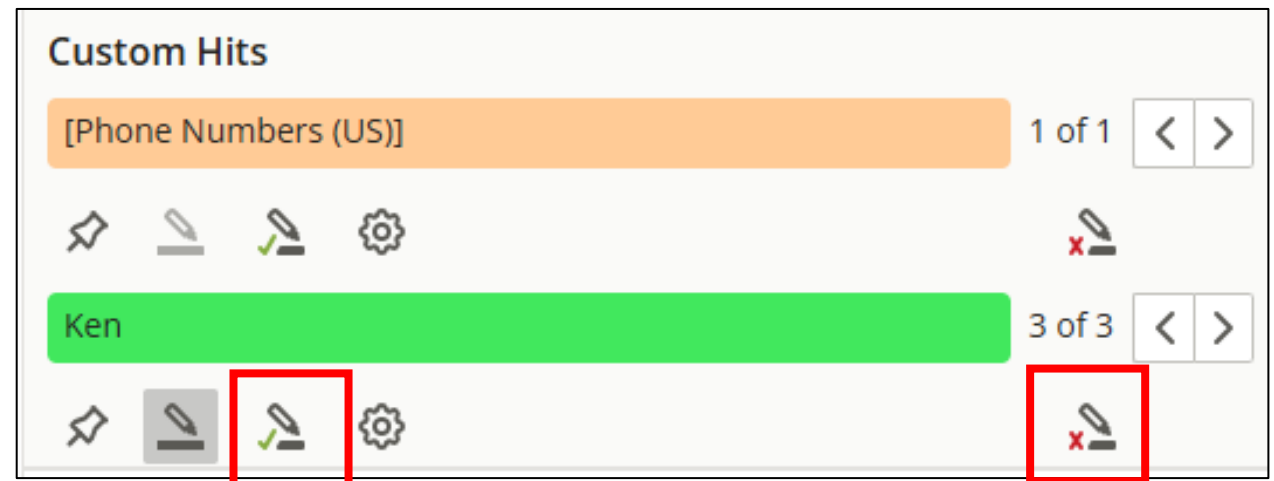
Manual Review

- Let's search for all of the times "Ken" appears
- Type "Ken" under "Search document..." and hit Enter
- Use the arrow keys to see all entries



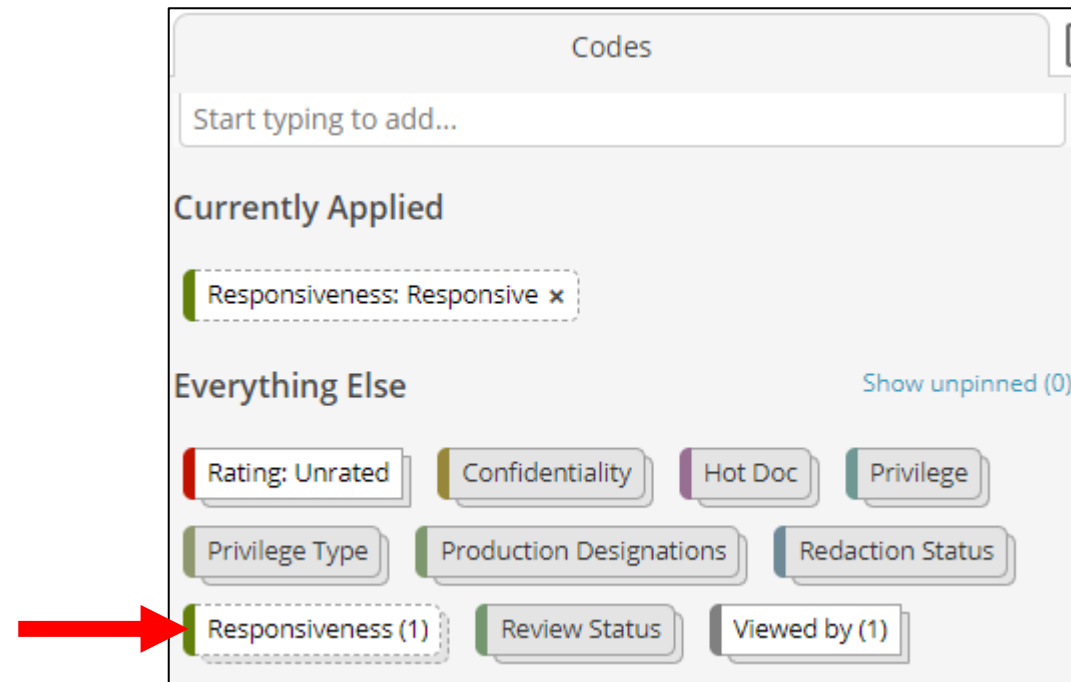
Manual Review

- Let's say we want to redact all instance of "Ken" in this document
- Click the icon for "Redact all instances"
- Notice the left pane. Click the "Remove all redact.."
- Hit "Delete"



Manual Review

- Select the “Codes” tab, click on “Responsiveness” and notice this has already been marked as “Responsive” by the original reviewer selecting that code.



Note

- We are all reviewing the same document set
- Normally, a review team would each take different bates ranges to look through and determine if responsive or not
- I won't have you mark things as responsive for simplicity's sake but make sure you understand how to do it

Manual Review – Annotations/Notes

- Let's each add a note to this document under "Annotations"
- For the note, put your last name and test and hit "Save"
- Annotations/Notes are a good way to remember why a document might be responsive and to let other reviewers know as well

Manual Review – Annotations/Notes

- Turn on “highlight mode”  
- Drag across some text to highlight it
- Put your last name and test 2 and the note and hit “Save”
- Click into the black space and notice your highlight on the right
- Click on the highlighted section to see your note
- Hit the trash can and delete your note

Manual Review – Redactions

- Select the redaction highlighter   |
- Drag it across a random place in the document
- Notice the new redaction entry in the “Annotations” section if you scroll down
- Toggle off the redaction highlighter

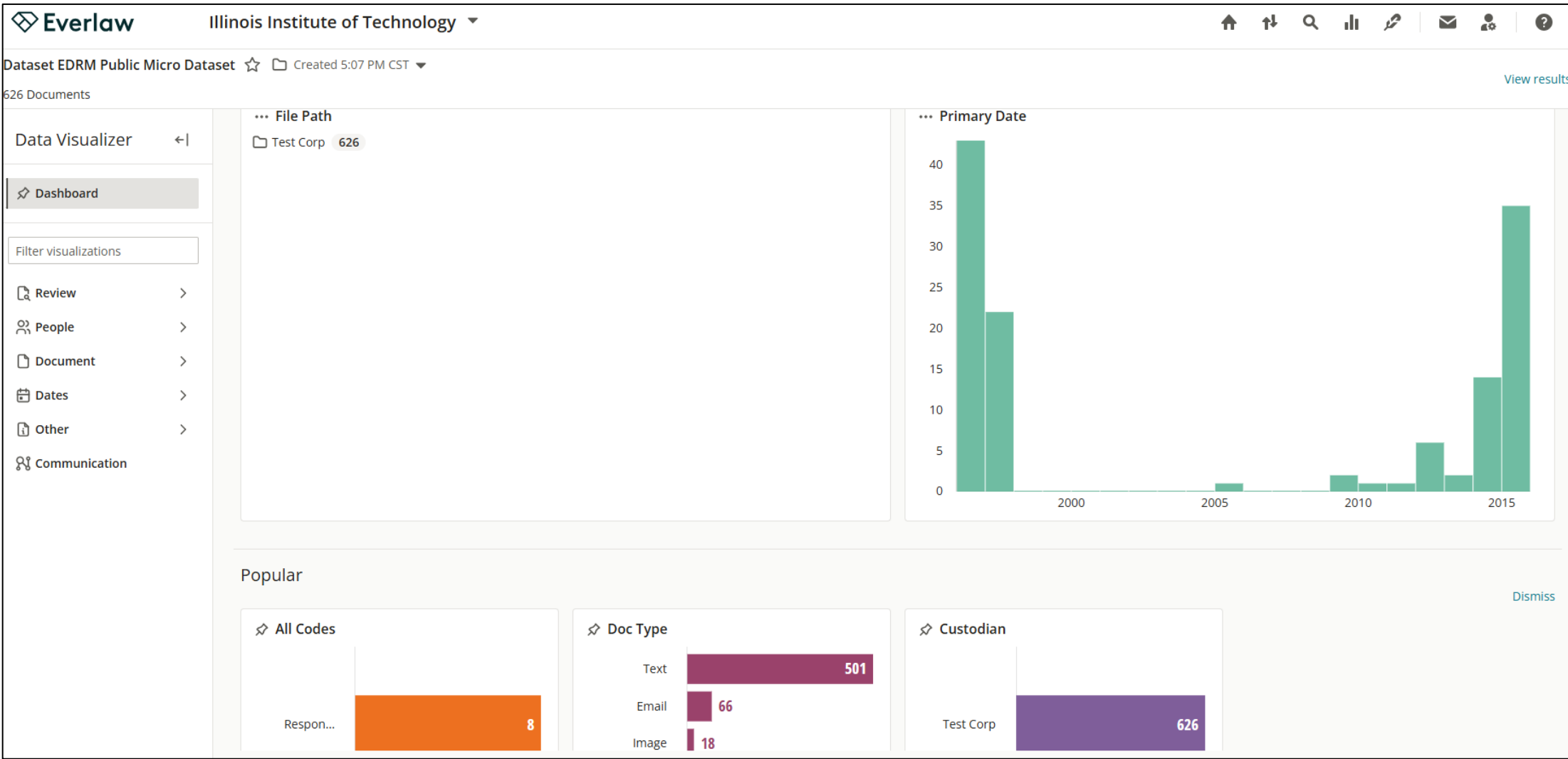
Manual Review

- Close the review pane and hit the Home button
- Select the EDRM Public Micro Dataset under Document Sets
- Select the top document
- Take some time to use the double arrows and look at some of the other documents in the different views (PDF, Text, Native, etc.)

Visualizing Data in Everlaw

- Close the review Pane and Go back to the main Everlaw window
- Click the Home button in Everlaw
- Scroll to the right to “Document Sets” and click on the “EDRM Public Micro Dataset”
- Click on “Visualize” on the upper right
- Maximize the window

Visualizing Data in Everlaw



Visualizing Data in Everlaw

- Expand “People” on the left
- Select “From”
- Select “Tyson Dimetrio”
- Select “Add filter”
- Select “Apply filters to search”
- Now you will see the six emails that meet the filter criteria

Visualizing Data in Everlaw

- Select the first item to open the Review Pane

Everlaw Illinois Institute of Technology

Dataset EDM Public Micro Dataset ☆ Last edited 8:15 PM CST

6 selected / 6 filtered of 626 total

From: Tyson Dimetrio X

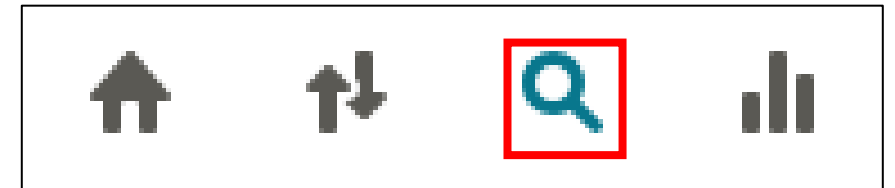
☒	Type	Row #	Bates/Contro...1	Document Set	Num P...	Rati...	Coded	Notes
☒	Email	1	#161.1	Native: EDM Public Micro Dataset	1	Unrated	Responsiveness: Responsive	
☒	Email	2	#168.1	Native: EDM Public Micro Dataset	1	Unrated	Responsiveness: Responsive	
☒	Email	3	#172.1	Native: EDM Public Micro Dataset	1	Unrated	Responsiveness: Responsive	
☒	Email	4	#178.1	Native: EDM Public Micro Dataset	1	Unrated	Responsiveness: Responsive	
☒	Email	5	#185.1	Native: EDM Public Micro Dataset	1	Unrated	Responsiveness: Responsive	
☒	Email	6	#186.1	Native: EDM Public Micro Dataset	1	Unrated	Responsiveness: Responsive	

Question

- Manual review is a lengthy process to go through each document
- What is a quicker option to find responsive documents?
 - Use the search feature to look for specific terms!

Using the Search Feature

- Close the review window
- Select the Home Button
- Select the magnifying glass for “Project Search”
- You can search by:
 - Booleans
 - Document info
 - Review Codes
 - Metadata
 - Etc.



Using the Search Feature

- Let's run some searches on the Enron emails only
- Select "Custodian" under "Metadata"
- Select "Enron" which shows how many docs?
- Under "Contents" above "Custodian," enter "Fraud" and hit the blue "Search" button
- How many docs now?
- Click on the first email below
- Click the "Open for Review" button

Using the Search Feature

- Select the “Hit Highlights” tab
- Hit the arrow next to “Fraud” to find it in the doc
- Use the double arrow buttons at the bottom to go through more of the docs and look for “Fraud” in each one with “Hit Highlights”
- Read the interesting #16206.1 email
- Next week we will go into more advanced searches

Adding to Binder

- Now we have performed our review and found all of our responsive documents
 - We just performed a quick example
 - A real review will take a lot more work and time
- Close Reviewer Pane
- Hit the Home button in Everlaw
- Hit the search magnifying glass

Adding to Binder

- Select “Coded”
- Select “Responsiveness: Responsive, Anyone, Any time”
 - How many documents do you have?
 - 9
- Select “Search”
- Select “Batch” and “Modify”
- ****Don’t do anything else****

Adding to Binder

- **Don't perform the following steps!**
 - If you wanted to add these to the binder, you would normally scroll down on bottom window and select "Prod001", "Apply", and "Apply"
 - I have already done this and I don't want us to duplicate things but that is how you add documents to a binder for production

Adding to Binder

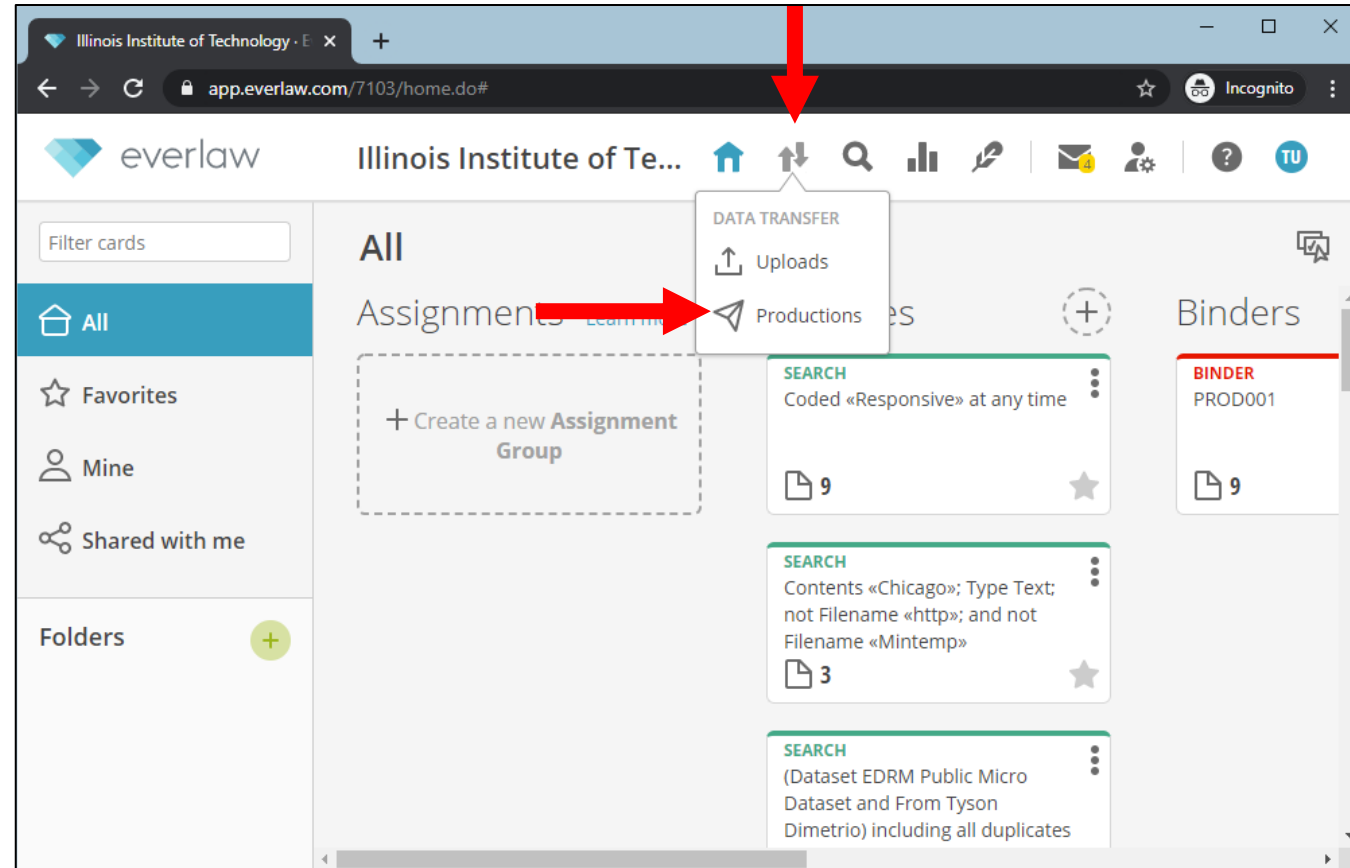
- Select Home button in Everlaw
- Select PROD001 and you should see the 9 documents inside

Part III

Everlaw: Creating a Production

Creating a Production

- Select “Data Transfer”
- Select “Productions”

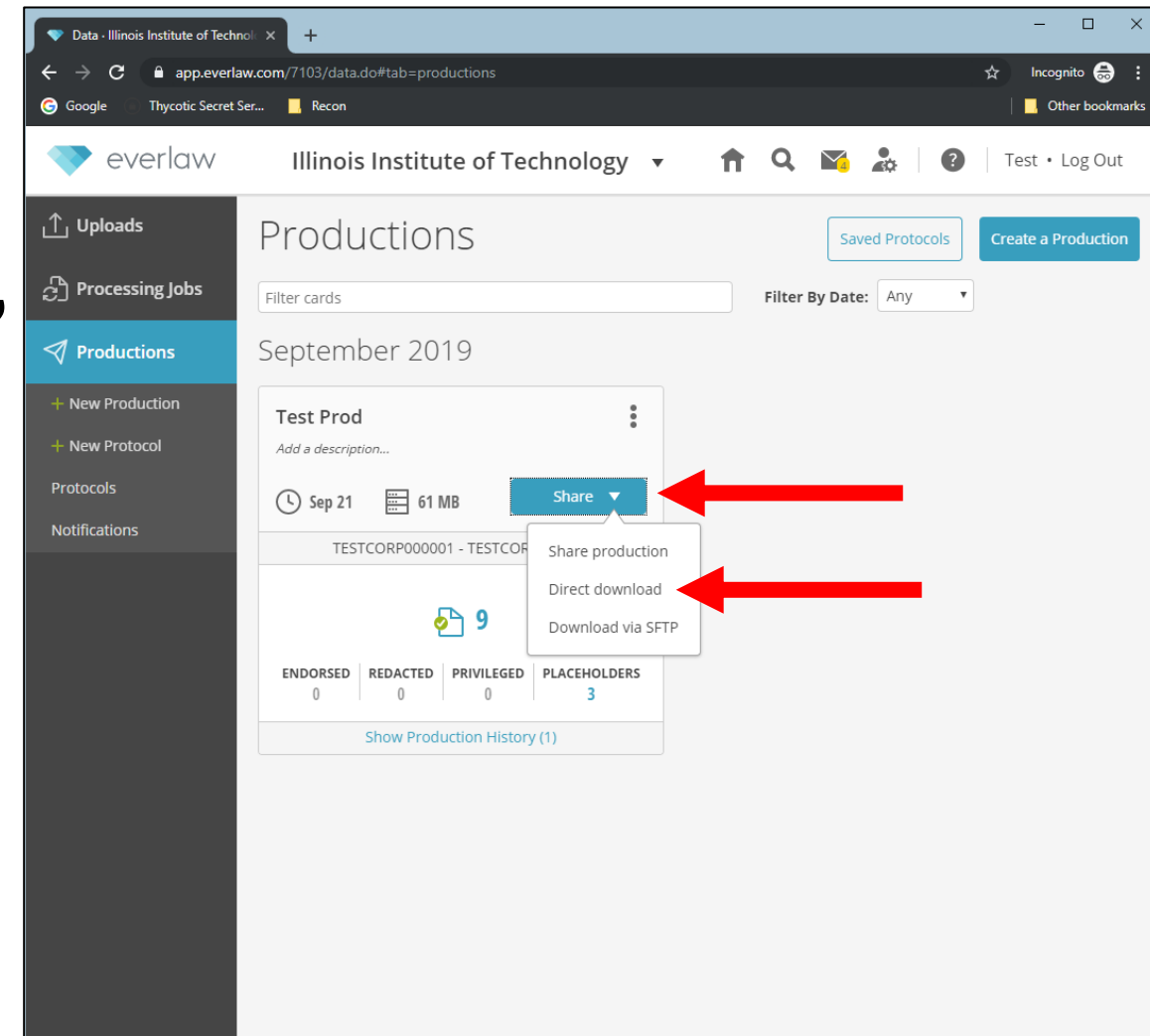


Creating a Production

- I already have a production in here, so we don't need each of you to create duplicate ones

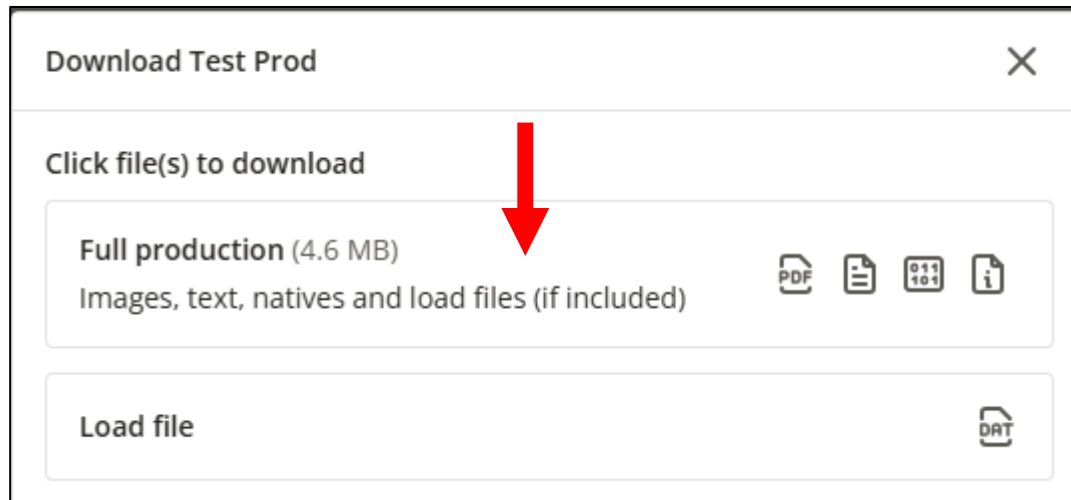
Downloading the Production

- For “Test Prod”
- Select “Share”
- Select “Direct download”



Downloading the Production

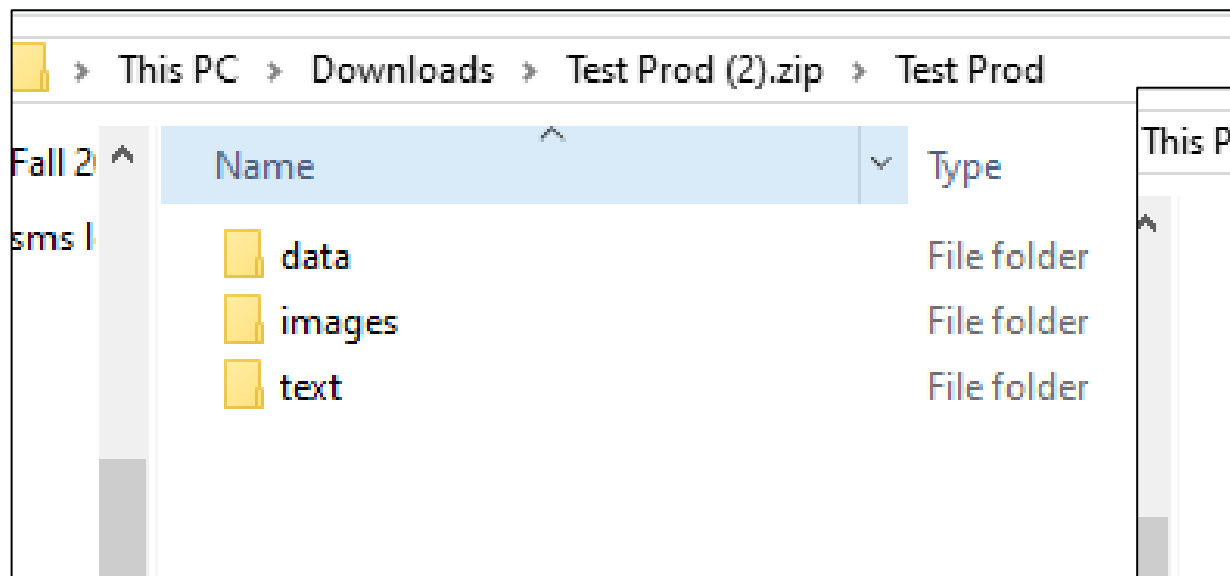
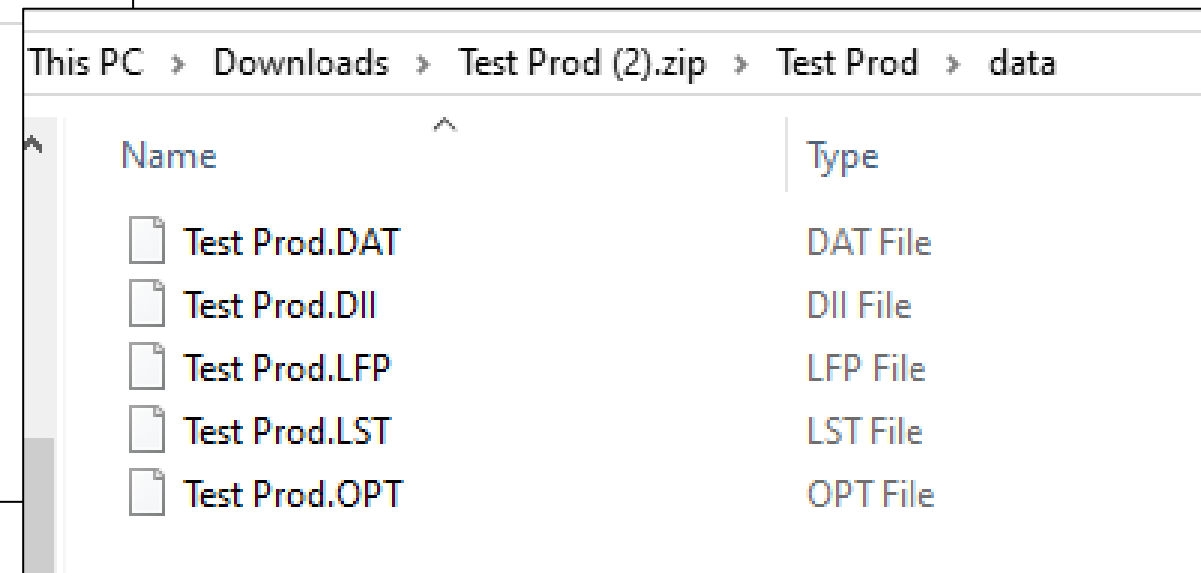
- Select “Full production”



- Save it somewhere accessible on your computer

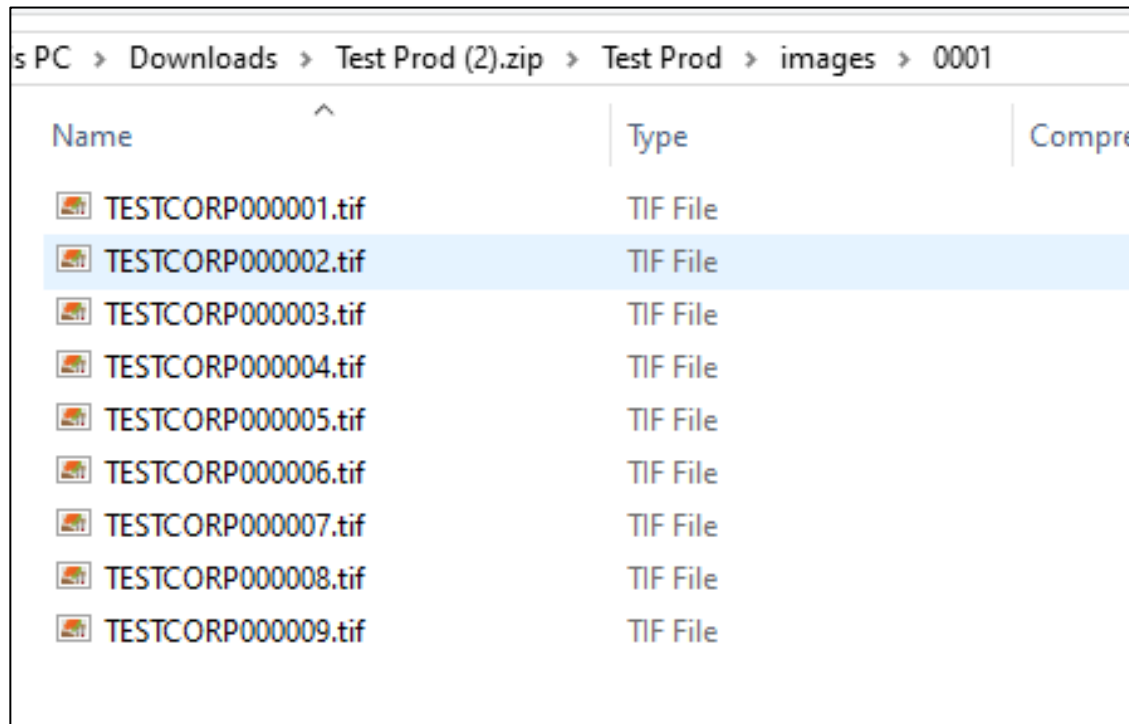
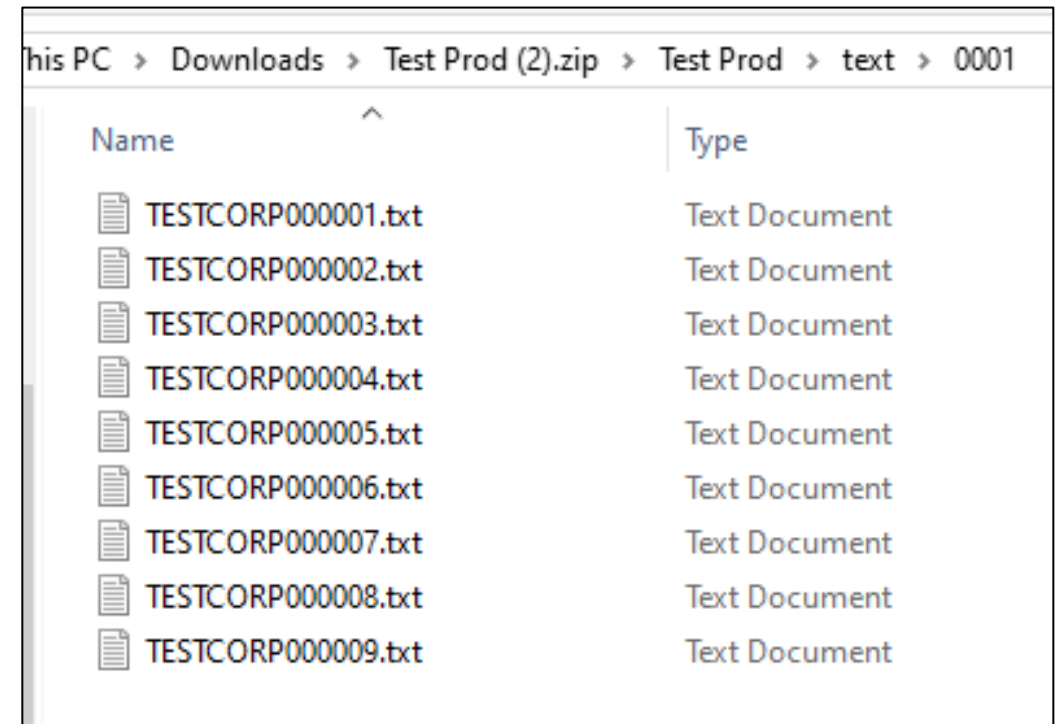
Viewing the Production

- Open up Test Prod.zip
- Look through the folders and open the files
 - Open the load files in a text editor on your computer



Viewing the Production

- Open up Test Prod.zip
- Look through the folders and open the files



Question

- Why did some of the TIFF images show “No Images Produced”
 - CSVs are not produced as an image and instead as a text file

Everlaw

- You can now close out of Everlaw
 - Remember your credentials though for next week
- Feel free to play around in Everlaw with searches and things
- Please don't make any big any changes to documents as I want our online students to be able to perform the same lab

Part IV

Managing E-discovery

Managing E-discovery

- Managing e-discovery involves understanding:
 - The process and tools
 - Skills needed to do the job
 - When to bring in the “experts”
 - How to select the right expert
- Also involves merging the knowledge of two fields: law and information technology (IT)
 - Problems can often be avoided if the IT staff has a reasonable grasp of litigation concepts and procedures

Experts vs. Consultants

- **Expert:** those having special knowledge of a subject who can provide testimony
 - Expertise can come from “study or education or from experience and observation”
 - To testify in court or at depositions, expert witnesses “must be qualified by the court”
- **Consultants:** those who give professional advice or services
 - Generally don’t give a testimony
 - May occasionally be asked to testify (then become an expert witness)

Discovery vs. Evidence

- **Discovery:** the process of identifying, locating, securing, and producing information and materials for the purpose of obtaining evidence for utilization in the legal process
- **Evidence:** the testimony of witnesses, introduction of records, documents, exhibits, objects, or any other matter

Discovery for Civil Cases Review:

- In a civil case, discovery is generally done through what processes?
 - Interrogatories
 - Written questions
 - Requests for admission
 - Requesting party to admit or deny the truth of a statement under oath
 - Requests for production
 - Requesting documents
 - Depositions after a complaint is filed
 - Interviews under oath

Privacy Obligations for Electronic Filings

- What do the Federal Rules of Civil Procedure require for privacy protection for clients?
 - <https://www.pacer.gov/privacy/cv.html>
 - Redaction (or partial redaction with only last four digits showing) of
 - SSN/TIN
 - DOB
 - Minor's name
 - Financial account number

Redaction and Filing Under Seal

- If you would like to redact anything else or file under seal the attorney must file a motion for protective order
- What would be some reasons to file under seal/redact??
 - Trade secrets
 - Vulnerability disclosure
 - Danger to the public
 - Required by statute (sexual assault victim, minors)

Protective Orders

- Protective order: limits access to information or evidence
 - Used in both civil and criminal cases
 - Documents filed with the court are public record unless they're sealed from public access or protected
- In criminal cases, protective orders are usually applied to witness or informant identities
 - To protect them from harm or intimidation

Part V

Digital Forensics Consultants and Examiners

A Digital Forensics Consultant's Role in Civil Cases

- Use of digital forensics consultants in the civil sector is growing
 - Attorneys are becoming more knowledgeable about gathering and analyzing digital evidence
- Digital forensics consultants might be involved in
 - Prelitigation corporate policymaking
 - Postlitigation expert witness services
 - To identify what digital material should be subject to a hold notice or how to comply with a hold notice
 - Sarbanes-Oxley Act compliance
 - Family law cases

A Digital Forensics Consultant's Role in Civil Cases

- After litigation has started, the active process of discovery begins
 - An interrogatory is often the first formal discovery request
- Digital forensics consultants can advise on the interrogatory's technical aspects for specific case issues
 - Such as questions on server backup frequency and storage, where Web sites are hosted, frequency of required password changes, etc.

A Digital Forensics Examiner's Role in Criminal Cases

- In most criminal cases, commissioned law enforcement officers or agents perform digital forensics examinations
- Initial law enforcement investigations rarely use consultants
- Examiners are limited in an examination's scope
 - Based on search warrant criteria

A Digital Forensics Examiner's Role in Criminal Cases

- In some criminal cases, a search warrant might not be required to seize a digital device
 - Example: when evidence is in plain view, immediate seizure is allowed
 - What are “exigent circumstances?”
 - Might exist when law enforcement believes evidence could be destroyed or a safety risk to the public or officer is believed possible

A Digital Forensics Examiner's Role in Criminal Cases

- A consultant is used because defense attorneys rarely have forensic examiners as employed staff
- In corporations, a digital forensics examiner or consultant might be asked to:
 - Determine whether espionage has occurred or trade secrets were stolen
 - Participate in network security policymaking or incident response

Testimony by Digital Forensics Consultants and Examiners

- In pretrial declarations, a digital forensics consultant might be asked to provide a written statement under oath about a specific aspect of the examination
 - Accompany a summary judgment or other motion
- **Summary judgment:** a formal request to the judge to determine facts of a case before trial
 - An attempt to erode a case bit by bit, until no core issues are left for trial
 - Digital forensics consultants function as expert witnesses

Motion for Summary Judgement Example

- Glauser vs. Groupme

- My declaration was cited to in motion

at GM_0000176-0000188.)² Together, GroupMe's and Twilio's hardware and software equipment dialed numbers from a stored list without human intervention through a straightforward process:

1. GroupMe collected and stored all group member information (e.g., group member names and telephone numbers) provided by the group creators in databases maintained on its servers, (*see, e.g.*, Declaration of Shawn Davis ¶¶ 3-8, attached as Exhibit 1; Dkt. 107-3 ¶ 7; Dkt. 120-1, Ex. I at GM_000134; Dkt. 120-1, Ex. J at GM_0000230; Dkt. 120-1, Ex. K at GM_0000365);
2. Upon storing that information, GroupMe's software automatically checked to see if the user was already a member, and if not, automatically generated the pre-programmed GroupMe Mobile App Text (*see, e.g.*, Davis Decl. ¶ 13; Dkt. 107-2 ¶ 17; Dkt. 107-3 ¶ 3; Dkt. 120-1, Ex. E at GM_0000117-0000123; Dkt. 120-1, Ex. F at GM_0000398; Dkt. 120-1, Ex. C at GM_0000088 and
3. GroupMe sent the pre-programmed text messages along with the telephone numbers to Twilio's API, which transmitted the text messages to the group members. (*See* Davis Decl. ¶¶ 19-30; Dkt. 107-2 ¶ 19; Dkt. 107-3 ¶ 5; Dkt. 120-1, Ex. L at GM_00000228; Dkt. 120-1, Ex. J at GM_0000230; Dkt. 120-1, Ex. M at GM_0000356-0000357; Dkt. 120-1, Ex. N at GM_0000366).

Testimony by Digital Forensics Consultants and Examiners

- A digital forensics examiner can be deposed or testify before a grand jury
 - In order to get an indictment in criminal cases
- Grand jury hearings are normally held in secret
 - The opposing side isn't usually present or aware of the hearing until the indictment is issued
 - The opposing side usually gets the digital forensics examiner's testimony transcript under the Jencks Act
 - Jencks Act: defendants in federal criminal cases can use this act to discovery witness statements

Testimony by Digital Forensics Consultants and Examiners

- Digital forensics examiners are asked for their qualifications when testifying as expert witnesses
- Expert testimony is usually permitted when it comes from a reasonably reliable source and is done in a way that can assist the jury (or judge)

Daubert Hearing

- Opposing side can challenge an expert and ask for a Daubert hearing to consider the Expert's:
 - Qualifications
 - Methods
 - Science relied upon

Training and Experience for Digital Forensics Consultants

- Digital forensics and e-discovery professionals rely on tool-centered and academic training
 - Actual case experience helps to gain a thorough knowledge of their specialties
- Tool-centered training covers a wide variety of technology topics ranging from:
 - Hexadecimal (bit-level) analysis to user activity analysis

Training and Experience for Digital Forensics Consultants

- Aside from Encase, FTK, X-Ways, mobile is popular

 <p>CAFF Cellebrite Apple Forensic Fundamentals GMT-6</p> <p>Apr 07-10 Virtual</p>	 <p>CCPA Inseyets CCPA Inseyets Wheaton, IL GMT-6</p> <p>Apr 08-10 In-Person</p>	 <p>CCPA Inseyets CCPA Inseyets Tempe, AZ GMT-7</p> <p>Apr 08-10 In-Person</p>
 <p>CCPA Inseyets CCPA Inseyets Burlington, WA GMT-8</p> <p>Apr 08-10 In-Person</p>	 <p>CASA Cellebrite Advanced Smartphone Analysis for Inseyets GMT-6</p> <p>Apr 13-17 Virtual</p>	 <p>CCO Inseyets CCO Inseyets GMT0</p> <p>Apr 13-14 Virtual</p>

SANS Forensic Training Roadmap

FORENSICS ESSENTIALS

Every Forensics and IR Professional Should Know

FORENSICS ESSENTIALS

FOR308 Digital Forensics Essentials

BATTLEFIELD FORENSICS
& DATA ACQUISITION

FOR498 Battlefield Forensics & Data Acquisition | GBFA

INCIDENT RESPONSE & THREAT HUNTING | HOST & NETWORK FORENSICS

Every Forensics and IR Professional Should Know

ENDPOINT
FORENSICS

FOR500 Windows Forensic Analysis | GCFE
FOR508 Advanced Incident Response, Threat Hunting,
and Digital Forensics | GCFA
FOR608 Enterprise-Class Incident Response & Threat Hunting

NETWORK
FORENSICS

FOR572 Advanced Network Forensics: Threat Hunting,
Analysis, and Incident Response | GNFA

Whether you're seeking to maintain a trail of evidence on host or network systems, or hunting for threats using similar techniques, larger organizations need specialized professionals who can move beyond first-response incident handling in order to analyze an attack and develop an appropriate remediation and recovery plan.

DIGITAL FORENSICS, MALWARE ANALYSIS, & THREAT INTELLIGENCE | SPECIALIZED INVESTIGATIVE SKILLS

Specialization

CLOUD FORENSICS

FOR509 Enterprise Cloud Forensics and Incident Response

MALWARE ANALYSIS

FOR610 Reverse-Engineering Malware:
Malware Analysis Tools and Techniques | GREM
FOR710 Reverse-Engineering Malware: Advanced Code Analysis

Threat Intelligence

CYBER THREAT INTELLIGENCE

FOR578 Cyber Threat Intelligence | GCTI

Digital Forensics & Media Exploitation

SMARTPHONES

FOR585 Smartphone Forensic Analysis In-Depth | GASF

MAC FORENSICS

FOR518 Mac and iOS Forensic Analysis and Incident Response

Training and Experience for Digital Forensics Consultants

- The Association of Certified Fraud Examiners has both beginning and advanced training in digital forensics
- CFEs are well trained in investigative techniques for fraud prevention and detection
 - Some specialize in digital forensics investigations
 - Should not be viewed as a substitute for digital forensics certification

Training and Experience for Digital Forensics Consultants

- Licensed private investigators might be former law enforcement officers who have:
 - IACIS training
 - Certifications
 - Training with a forensics software vendor
 - No digital forensics training at all
- Each state has different private investigator licensing requirements
 - No consistency in background or training requirements

Part VI

E-discovery Consultants

E-discovery Consultants

- Some law firms have established litigation support departments specializing in e-discovery
 - Many staff hold varying degrees of certifications and training
- Ultimately, the American Bar Association or another credible association will likely identify bona fide certifications in this area

Consultant Categories

- IT professionals who began their careers as in-house support at law firms
 - Often move on to litigation support service providers or independent consultants
- Litigation support houses and Web-based service providers are often extremely knowledgeable and experienced
 - Devote substantial resources to improving products and services
 - Seek out IT professionals with law firm experience
 - Usually have e-discovery attorneys in management

Tool-Centered Training

- Litigation software vendors usually offer two types of training:
 - End-user training - prepares people to use the software's basic features
 - Administrator training - covers more complex end-user features as well as how to create a database and how to populate it with documents and data

Academic Training

- Academic institutions with law school, computer engineering, and other IT based programs are establishing courses to train law students, paralegals, and IT professionals

ACEDS Training & Certification

- Association of Certified E-Discovery Specialists
 - <https://aceds.org/>

CEDS Certification

The Certified E-Discovery Specialist (CEDS) Certification responds to the need for professionals with diverse skills and knowledge across the e-discovery spectrum. It facilitates sound hiring practices, advances careers and gives a competitive advantage to individuals who earn it and their employers.

The exam is constructed with the help of 40 experts under the strict auspices of a psychometric firm and a worldwide survey. This produces a neutral, legally defensible professional certification examination and program.

Testimony by E-discovery Consultants

- E-discovery consultants are sometimes asked to testify in court
 - Not as commonly as digital forensics consultants
 - Usually their testimony is limited to methods they used to collect or process discovery

Outsourcing E-discovery Consultants

- Many law firms outsource e-discovery to vendors until they gain experience or have access to in-house resources
- Ensuring quality assurance is very important
 - Failure to ensure QA could result in higher case costs or adverse case outcomes

Outsourcing E-discovery Consultants

- August 5, 2008 - American Bar Association issued “Formal Opinion 08-451: Lawyer’s Obligations When Outsourcing Legal and Nonlegal Support Services”
 - Places responsibility for outsourcing results on the attorney
- Outsourcing is also used in criminal cases
 - Although less often because of security, chain of custody, and other concerns

Part VII

Special Masters and Forensics Mediators

Special Masters and Forensics Mediators

- **Special master:** a person the court appoints to assist in performing specific functions in a pending action
 - Perform a neutral role between parties
 - May often be a lawyer or former judge
- E-discovery and computer forensics special masters can:
 - Conduct on-site inspections of computer equipment and files
 - Review sensitive data collections for relevance and privilege

Special Masters and Forensics Mediators

- An article in April 2010 issue of *Federal Courts Law Review* proposed the term **forensics mediator** for a new type of consultant
- Forensics mediator: a person who would perform the actual discovery investigation, instead of the plaintiff or defendant
 - Would also facilitate agreements on production between both parties
 - Possible solution to achieving full and fair discovery

Summary

- The organizational concepts of discovery are the same today as in the past
- Index cards have been replaced with litigation databases
- As technology continues to develop, e-discovery becomes more complex
- The industry has many consultants and experts; some with certifications and training and some without
- Tool-centered training is available in both e-discovery and digital forensics

Summary

- Digital forensics training for law enforcement officers can be obtained from a variety of sources, including IACIS and independent agencies
- Non-law enforcement training is available from IACIS, the International Society of Forensic Computer Examiners, The SANS Institute, and the Association of Certified Fraud Examiners
- Digital forensics examiners and consultants often testify in court or in pretrial proceedings
- Law firms sometimes outsource legal and nonlegal support services but remain responsible for the case

Summary

- The use of special masters, neutrals, and forensics mediators is becoming important in complex civil and criminal cases to minimize disputes
- UTBMS task-based billing can be used instead of narrative billing to establish case cost and efficiency benchmarks

Text References

- Phillips, A., Godfrey, R., Steuart, C., & Brown, C. (2014). E-discovery: An Introduction to Digital Evidence. Boston, MA: Cengage Learning.

Homework

- Review and understand this slide deck on Canvas
 - Read Chapter 5 before next class
- Feel free to play around with Everlaw on your own
 - Just don't upload extremely large datasets as we have a class 10GB limit before getting charged
- Research paper bibliography due next Monday,
3/2

Homework

- Research paper due in 6 weeks on 4/6
 - Can start on paper once outlines are graded and I post the paper assignment and rubric
- No in-person class in two weeks on 3/9 as I will be attending Legal Week in NYC
 - I will post a video lecture

Questions???

