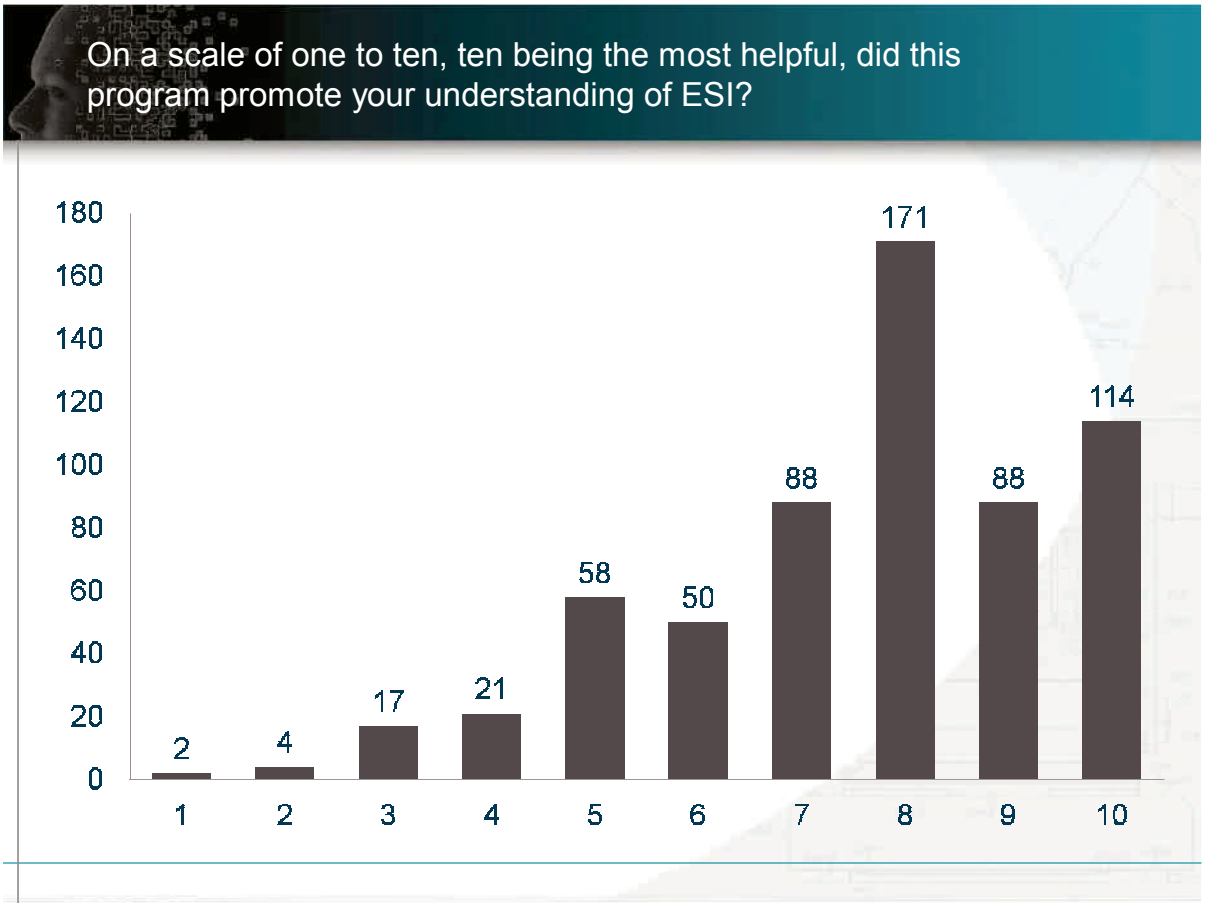
ESI 101 Frequently Asked Questions, Poll and Survey Results

Disclaimers: All of the disclaimers recited in the live event, also apply to the FAQ list. These responses reflect the opinion of the author alone and are not to be taken as legal advice on any specific situation.

1. Is it worth my time to watch this program?

This is a good technical overview if you have no prior experience or technical background on ESI issues. Participants in the live event were asked to rate this program on a scale of 1-10 in terms of whether or not it helped their understanding of ESI:



2. How do I get CLE credit?

CLE credit is only available for participation in the live event. CLE credit is not available for viewing the recorded event on the discoverypilot.com site. Certificates of attendance will be sent to all participants from Wisconsin and Illinois, for whom we can verify participation using all technical means available to us, in about two weeks. You will need to submit the appropriate paperwork to your state to perfect your claim for CLE credit. We use a combination of responses to Polls, IP address connection logging, survey responses, and live dialogue to confirm attendance. The event was fully subscribed in advance. Unfortunately, with such a large event there are always individual instances where participants are unable, for technical reasons, to connect to the live event; we regret that we cannot certify attendance for unsuccessful participation.

3. Could I get a copy of the slides please?

The webinar is available for review on the discoverypilot.com web site, and the slides can be downloaded as a .pdf file from the site. If you are interested in editable copy, please contact the author privately at GSchodde@mcandrews-ip.com.

4. What preservation obligations do I have with respect to ESI?

Generally, the obligation to preserve ESI is no different than the obligation to preserve any other evidence. Principles 2.03 and 2.04 of the 7th Circuit Electronic Discovery Committee further discuss ESI preservation issues.

See http://www.discoverypilot.com/sites/default/files/Principles8_10.pdf. A summary of a number of cases and a Seventh Circuit Analysis is contained in the previously broadcast webinar, "The Four Ps of E-Discovery", under the "Preservation" section, also on the discoverypilot.com web site. See http://www.discoverypilot.com/sites/default/files/the_4_p_of_ediscovery.pdf.

5. If information is on paper and opponent asks for it to be produced electronically, am I required to convert it for them or can I deliver it in paper, charge for the copies, and tell them to convert it themselves?

If the original documents are in paper, it requires no translation to make it reasonably useable and is not ESI. If ESI is printed, note that Rule 34 allows your opponent to seek ESI in "native form" or "other useable form." The process of conversion from electronic, to paper, back to electronic in this fashion, eliminates all metadata and degrades the use of electronic text retrieval tools, as well as causing unnecessary costs. See Kershaw & Howie, Judge's Guide to Cost-Effective E-Discovery, Electronic Discovery Institute, October 1, 2010 at section 13, pages 17-18 (describing print-scan as a "worst practice").

6. What are the security measures for ESI in clouds? How do the cloud providers back-up the data in case something happens in their facility?

The security and disaster recovery measures taken by cloud storage providers is beyond the scope of this event, however note that the attraction of using cloud services is that the cloud provider can leverage their scale and specialization in storage to provide services that may be more robust and/or more secure than what a small scale enterprise can execute internally. Note also, that if cloud storage is being used for backup, there is geographic diversity since the cloud provider's server location(s) are probably distant from the user's location.

7. Can the reviewer be "tricked" by changing the file extension, so that for example, a ".doc" file is renamed a ".exe" file and isn't selected for review?

Visually, this is possible, any file can be renamed. However, software tools are available that will ignore the label and inspect the actual file to determine whether it is in fact, an executable application. These tools can be used to filter applications out of a collection and eliminate this concern.

8. What are "forensically sound copying tools"

A tool that makes an accurate copy of the file without altering it, such that at least the application and system level metadata is preserved. In some cases, such as cases where deleted files are in issue, it may be necessary to make copies that are true "mirrors" or "bit level" copies of media, which will include the information in things like disk slack space and sectors that have been released but not written over at all.

9. Does getting a "read only" copy of the file solve the problem of changing the metadata?

Setting a file to "read only" keeps the file's contents from being changed, but it doesn't address how the read only copy was made. A copy from one drive to another, may still reflect the file modification/created dates and user information associated with the new drive, even if the copy is set to "read only." The "read only" copy will of course contain all the application level metadata, that the original file contained.

10. Is metadata copied when the information in a word doc is copied & pasted into a new document as opposed to making a copy of the .doc file?

The system level metadata, that is the information tracked by the operating system about the first and original file, is not affected other than it may show that the file was accessed. The new document will have its own system metadata reflecting its own creation date, last modified date, file name, and so on. Any application level metadata in the copied text, will also be embedded in the new document.

11. So my best bet might be to sit down with my retrieval specialist, someone from the company who knows the systems used, *and* opposing counsel, to define the search or preservation criteria?

Generally, resolving issues early is highly recommended. Principles 1.02, 2.01, and 2.02 suggest that an informed, transparent, early and cooperative process for resolving electronic discovery issues is the best approach.

12. Will the Hash value search tool distinguish identical files with different metadata?

Hash de-duplication works by identifying files that have different system level metadata, for example, different file names, but identical content. If the file contents differ, even slightly, the hash values will be different.

13. Will the algorithms assign a nearly identical hash to the same data in different form, e.g., a Word document and its pdf copy?

No. The value produced by a hashing algorithm does not measure "closeness"; in this particular case, the values produced by a hash algorithm for these two files will bear no relationship to each other at all – hashing algorithms are designed to generate differing values even for files that contain similar, but not identical content. Different tools are used to measure "near duplication", which is the process of identifying groups of closely related files that have the same or nearly identical content, which requires comparing text files looking for degrees of similarity.

14. Would the use of a thumb drive on a desktop computer leave any information on the desk top hard drive that a thumb drive was used?

Yes. Most desktop computers will register the ID of any drive connected including a thumb drive, which typically includes the serial number of the drive, and log when it was last connected. See e.g., http://www.forensicswiki.org/wiki/USB_History_Viewing; see also http://www.appleexaminer.com/MacsAndOS/Analysis/USBOSX/USBOSX.html. Some organizations install DLP (Data Loss Prevention) tools that log more detail regarding what devices are connected and disconnected as well as track file transfers. These log files are important evidence sources in data theft cases.

15. Are there any established standards in the courts for maintenance of metadata during discovery?

The standard for maintenance of metadata is still evolving. Absent agreement, the author's recommendation is to collect files in native

format while preserving system and application metadata, since even if it is ultimately not produced for one reason or another, software and search tools for working with ESI collections are more effective if the original metadata is intact.

16. Understanding that each case is probably different, as a general rule do the costs for securing and disclosing ESI information run in the thousands of dollars or tens of thousands?

The cost for a given ESI project is highly variable. The committee has endorsed the concept of proportionality, suggesting that the cost of the discovery should be proportional to the issues at stake. Principle 1.03; see also Fed. R. Civ. P. 26(b)(2)(B) and (C).

17. Any basis or authority to insist on translations from a foreign language to English?

Foreign language translations are beyond the scope of this program; there are no special rules when the original foreign document is in electronic form. Note however, that as automated translation software continues to improve, there are possibilities for low cost, uncertified electronic language translation as a discovery tool that are not available or less effective for paper documents.

18. Are natural language searches on Westlaw "statistical ranked" searches?

Yes. See e.g., http://nlp.stanford.edu/IR-book/html/htmledition/the-extended-boolean-model-versus-ranked-retrieval-1.html

19. What does it mean to produce ESI "in its native form"? Does that just mean any type of TIFF file?

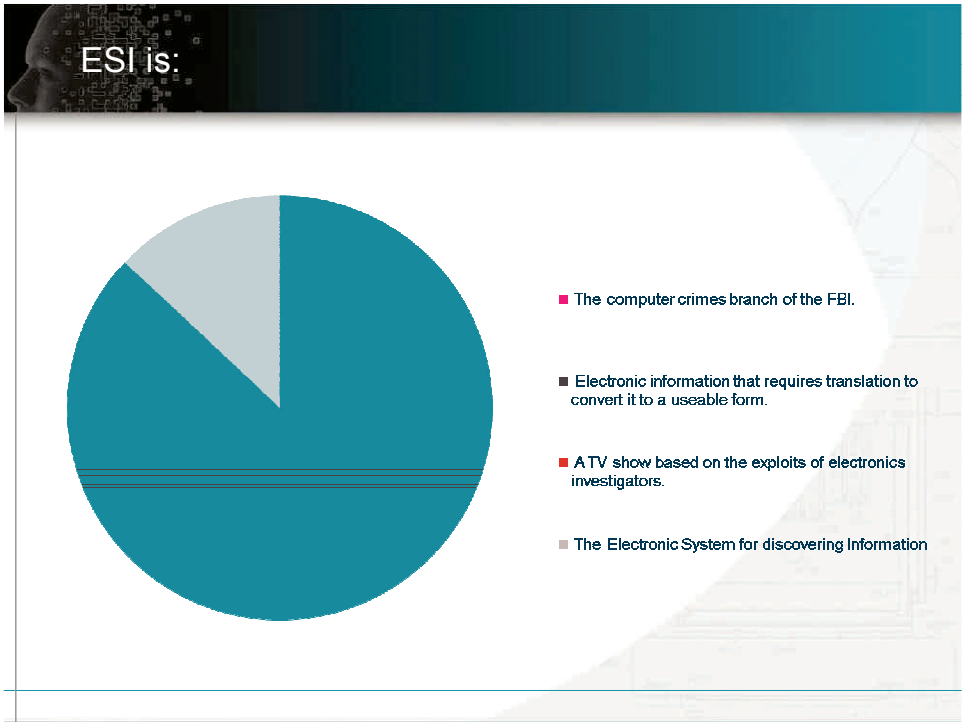
A "native" ESI production means to produce the file as it exists in the client's system. To review it, the original application that created it or a "viewer" that emulates the original application is used to open and view

the file. "TIFF" files are not "native" in this sense unless that was the format the client held the file in.

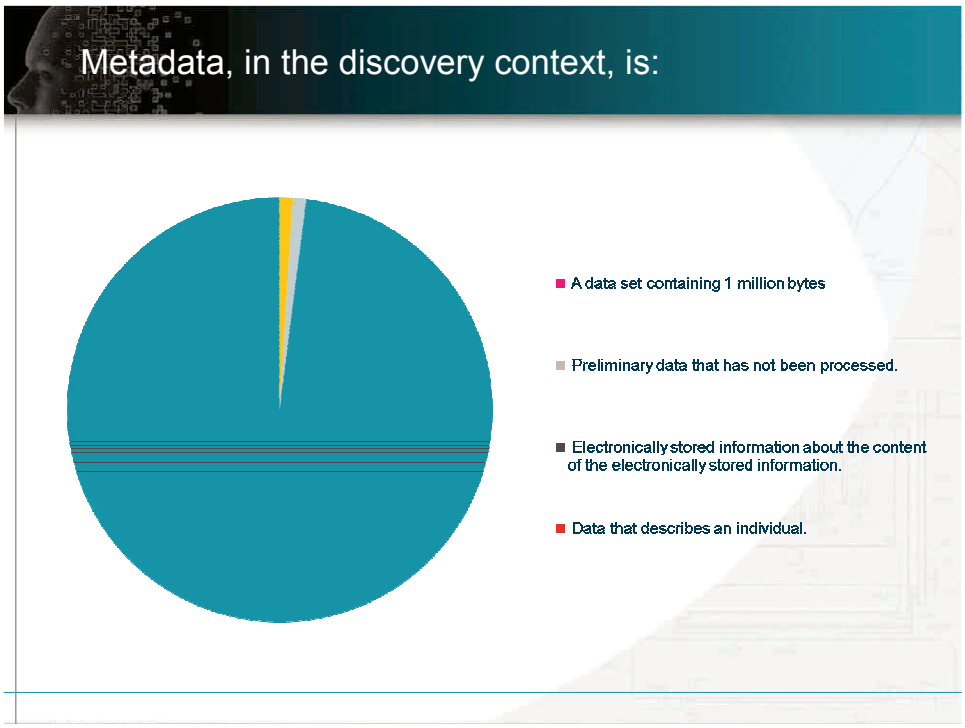
20. In Windows Explorer, does moving a file save the metadata? What about copying a file? Does it make a difference if I transfer to the same drive versus a different drive?

The application level metadata will be preserved by moves and copies made this way. However, system timestamp and file location information will or may be affected. The file location information is particularly vulnerable. For example, suppose responsive files are selected and moved or copied to a single new folder for production. All of the subfolder and original drive location information is lost in this operation, which can make it difficult to later determine the original custodian of the file. To accurately protect system and application level metadata, a file copy tool designed to copy files for ESI production that preserves metadata is the safest practice.

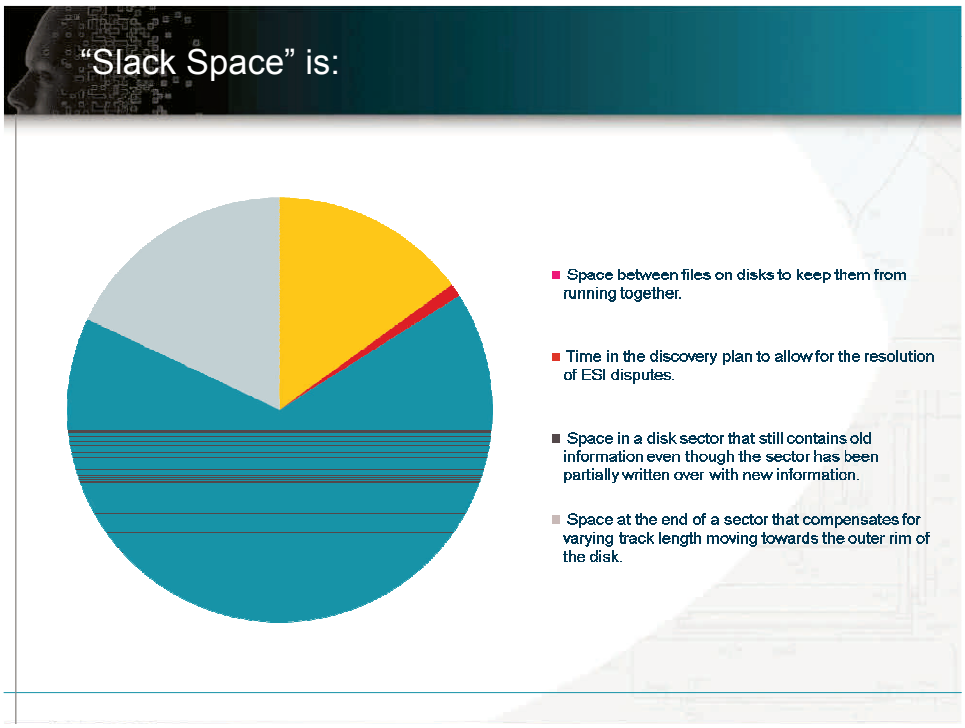
Other Survey and Poll Responses
Poll No. 1



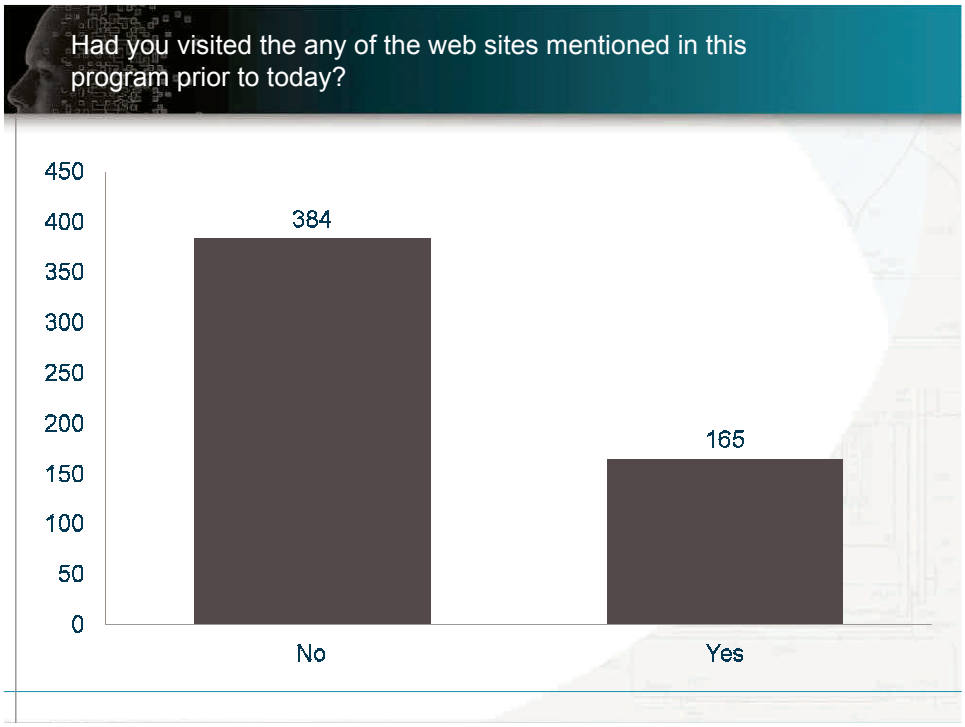
Poll No. 2

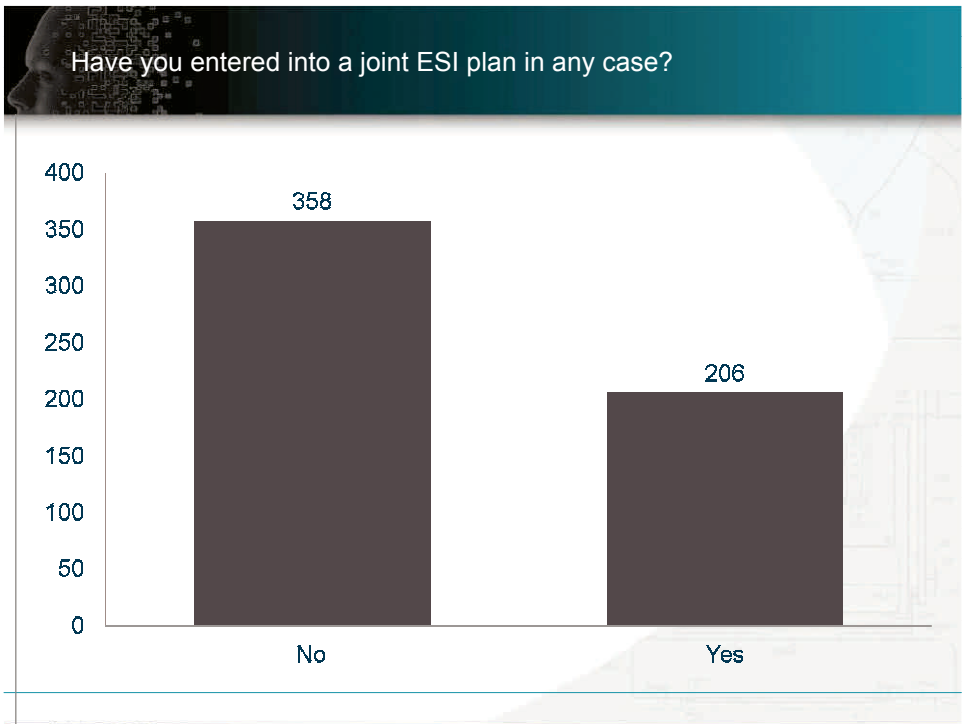


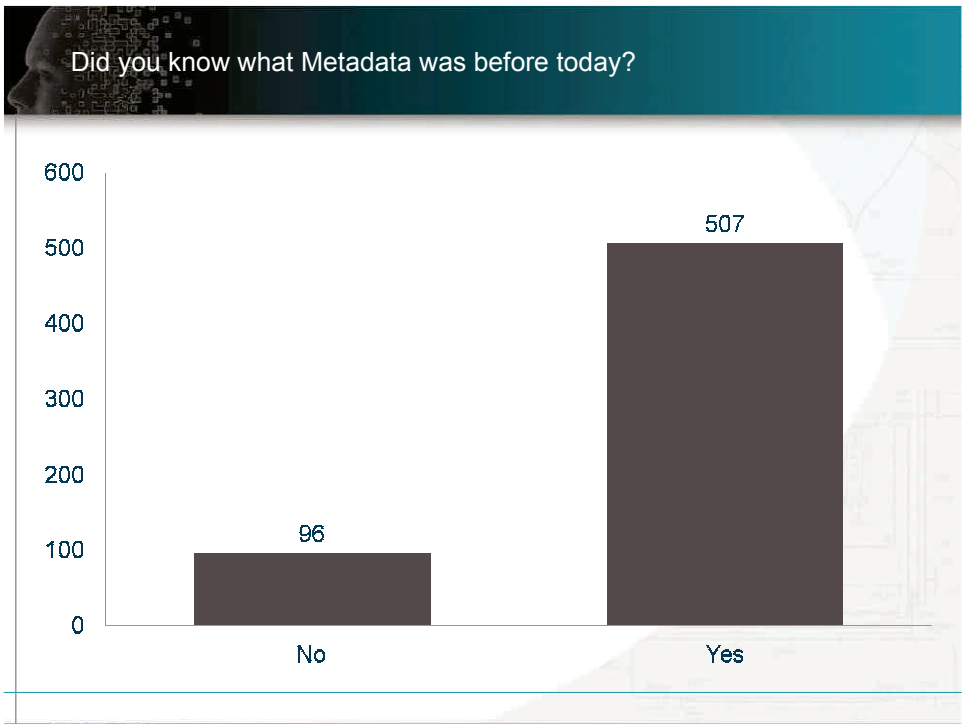
Poll No. 3



Survey Questions




Have you entered into a joint ESI plan in any case?
400
350
300
250
200
150
100
50
0
358
206
No
Yes


Did you know what Metadata was before today?
600
500
400
300
200
100
0
96
507
No
Yes