Forensics and Electronic Documents:

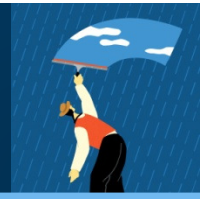
Critical Activities, Considerations, and Steps for Success

SCCE's How to Conduct Effective
Internal Investigations Workshop

November 11, 2010

NAVIGANT
CONSULTING

Agenda



- Electronically Stored Information
- Preliminary Investigative Considerations
- Collections: Scope and Capture
- Interrogation of Electronic Data
- Forensics and Data Analysis

NAVIGANT CONSULTING

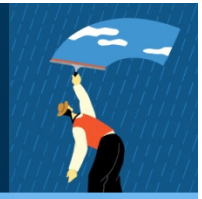
Electronically Stored Information

NAVIGANT CONSULTING

Common Sources of Electronic Evidence: Where to Look

NAVIGANT
CONSULTING

Boxes of Bytes: Putting It All in Perspective

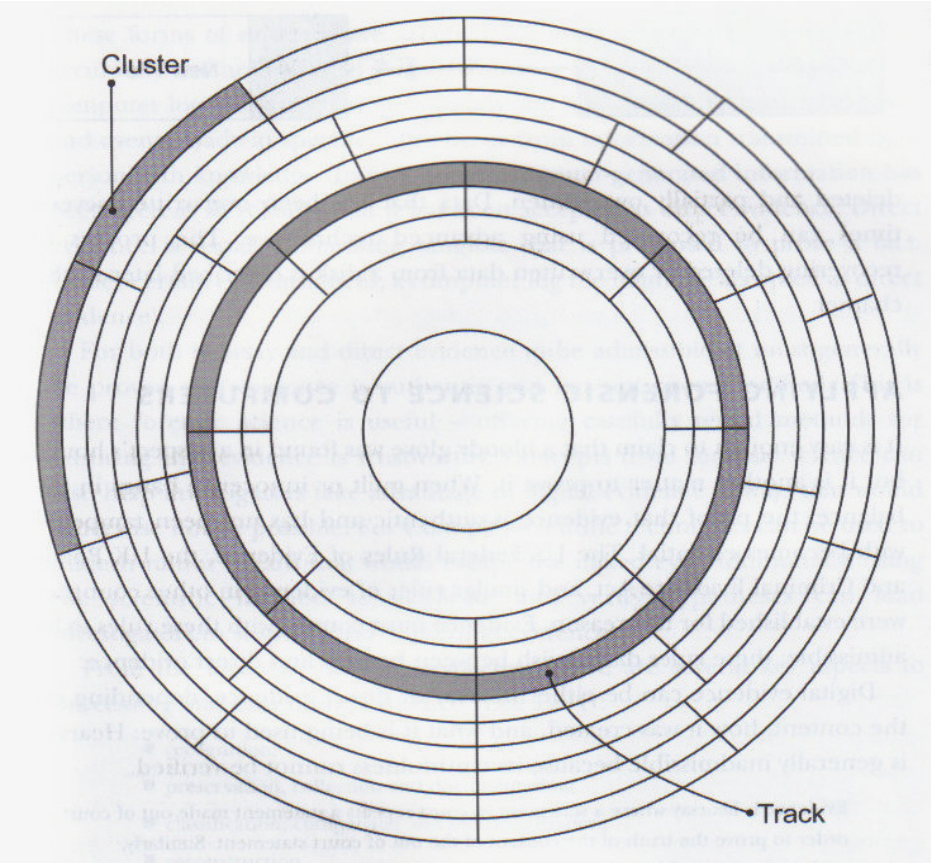


Assumptions:

1	**2,500**	**50**	**Megabytes**
10	25,000	500	
20	50,000	1	
100	250,000	5	
200	500,000	10	
300	750,000	15	
400	1,000,000	20	**Gigabytes**
500	1,250,000	25	
1,000	2,500,000	50	
2,000	5,000,000	100	
5,000	12,500,000	250	
10,000	25,000,000	500	
20,000	50,000,000	1	
40,000	100,00,000	2	**Terabytes**
60,000	150,000,000	3	

NAVIGANT CONSULTING

Forms of Digital Data



- **Active**

  Files that "actively" reside on the user's hard drive and/or the network server

- **Archival**

  Data and files compiled in back-up tapes

- **Replicant**

  Temporary files created by programs, also called “ghost” files

- **Residual**

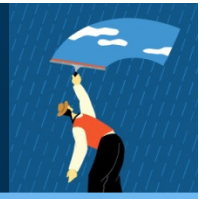
  Deleted files and e-mails, are not actually deleted until the medium has been destroyed or completely overwritten

- **Metadata**

  Embedded information surrounding the content or “data about the data”

NAVIGANT CONSULTING

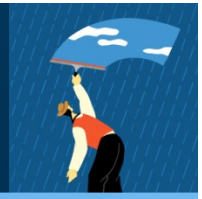
Metadata - Definitions



- "Metadata" means (i) information embedded in a Native File that is not ordinarily viewable or printable from the application that generated, edited, or modified such Native file; and (ii) information generated automatically by the operation of a computer or other information technology system when a Native File is created, modified, transmitted, deleted or otherwise manipulated by a user of such system.
- "Native File" means ESI in the electronic format of the application which such ESI is normally created, viewed, and/or modified.
- "Static Image" means a representation of ESI produced by converting a Native File into a standard image format capable of being viewed and printed on a standard computer system.

NAVIGANT CONSULTING

Metadata - Types



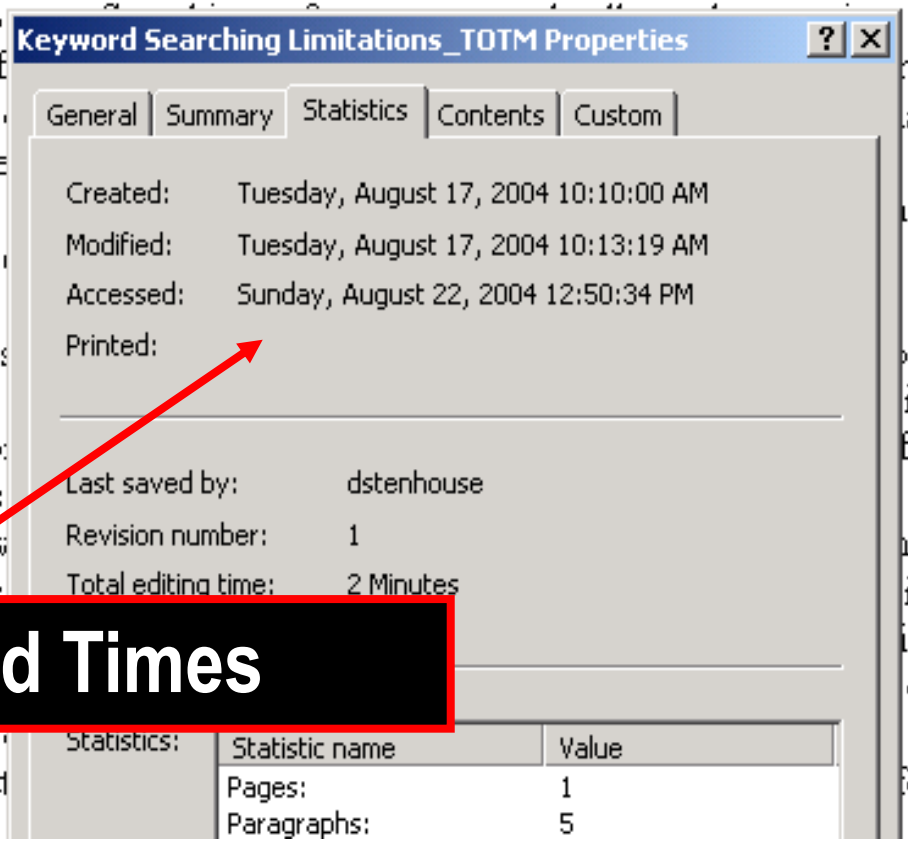
- "System Metadata" is data that is automatically generated by a computer system.
  - Examples: author, date and time of creation, and the date the document was modified.
- "Substantive Metadata" is data that reflects the substantive changes made to the document by the user created as a function of the application software used to create the document or file. It remains with the document when it is moved or copied.
  - Examples: prior edits, editorial comments, instructions how to display fonts and spacing text of actual changes to a document.
- "Embedded Metadata" means the text, numbers, content, data or other information that is directly or indirectly inputted into a Native File by a user and which is not typically visible to the user viewing the output display of the Native File on a screen or print out.
  - Examples: spreadsheet formulas, hidden columns, linked files (such as sound files), hyperlinks, and certain database information.

NAVIGANT CONSULTING

Metadata - Types

those strings to search through a computer's hard drive and/or individual documents for at least one occurrence. For instance, a search for the word "gadget" will force the software to look over the hard drive and find the characters "g-a-d-g-e-t" in that precise order without sp to adjust the search terms to f rms. The search can be performe allocated space[1], where de that are relevant to a spe at keyword searching only s

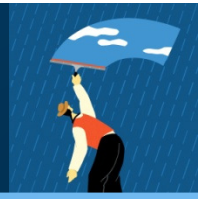
A good forensics mputer system as an initial part ion. For example, keywo f "hits" in active and deleted files hard drive. Upon further rev iner may see the email addres idea the user of system for comm il or Yahoo address to the att orporate email search through of the email for them to

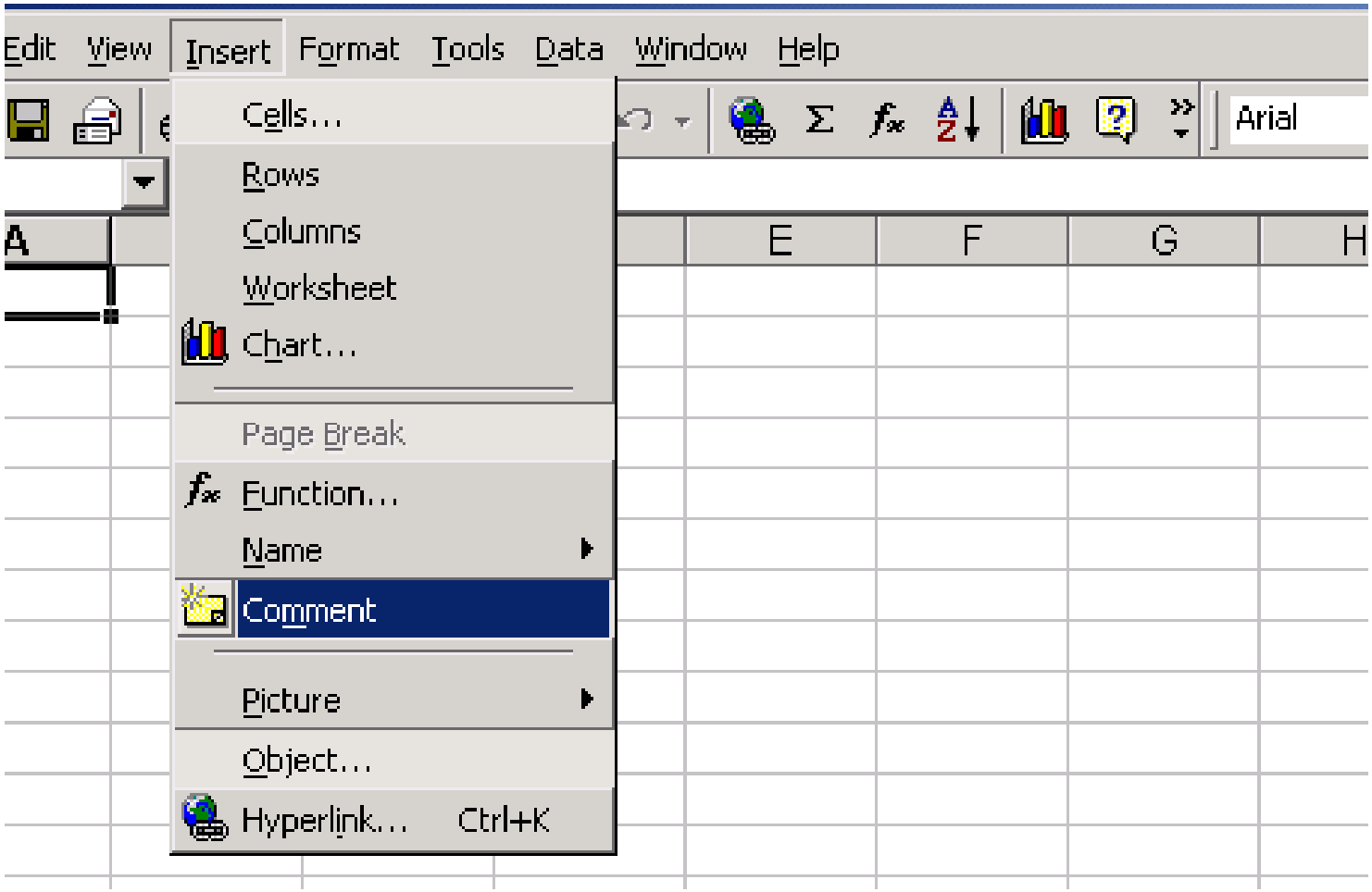


Vital Dates and Times

NAVIGANT CONSULTING

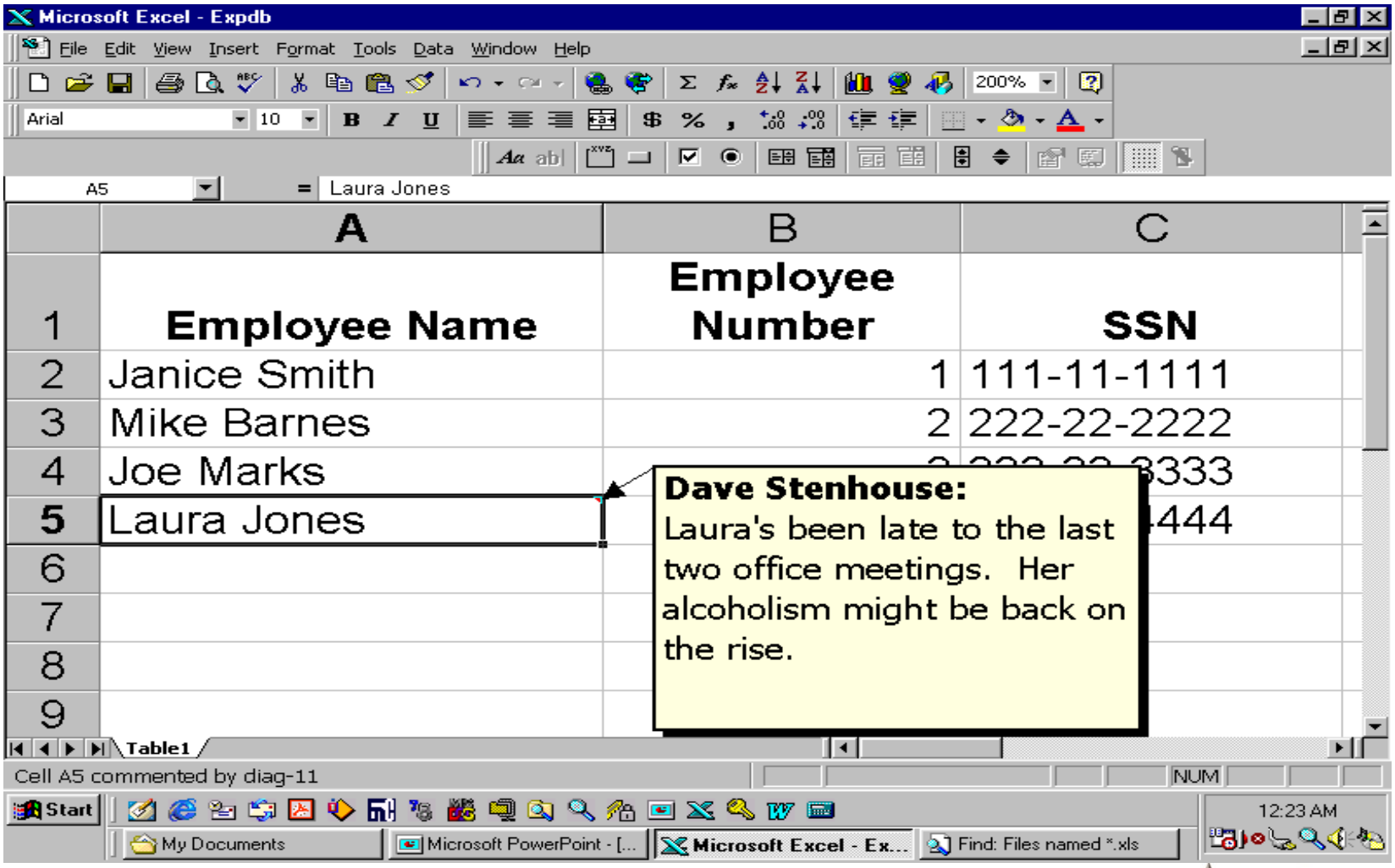
MS Excel “Comments”





NAVIGANT CONSULTING

Embedded Data

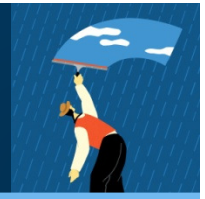


NAVIGANT CONSULTING

Preliminary Investigative Considerations

NAVIGANT CONSULTING

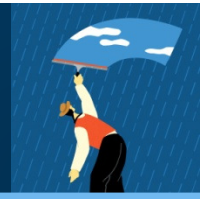
Initial Preliminary Considerations



- Information gathering during kickoff
  - Understand history of players
  - Allegations/issues
  - Information already developed
- Geographic locations
  - Data privacy and protection laws
  - Data export
  - Travel requirements

NAVIGANT CONSULTING

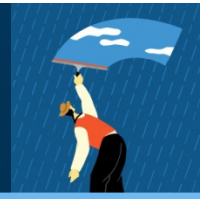
Initial Preliminary Considerations (cont'd)



- Covert or overt investigation and cover story if necessary
  - Collections vs. notification (conducted as part of audit, annual reviews, risk assessments)
- Internal resources available to work with independent investigators
  - Role of IT department
  - Appropriate information gathering process

NAVIGANT CONSULTING

Initial Preliminary Considerations: Working as a Team



- Teaming Strategies: Close alignment with Compliance, Investigators, and Forensic Accountants
  - Communication on IT policies and procedures/environment
  - Aid in activation of logging mechanisms
    - Telephones/mobile devices (if company or government owned)
    - Fax machines
    - Security logs (pass cards, security codes)
  - Active cross-communication re: data and systems/sources of interest

NAVIGANT CONSULTING

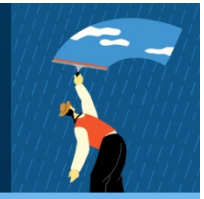
Collections:
Scope and Capture

NAVIGANT
CONSULTING

Collection Planning

NAVIGANT CONSULTING

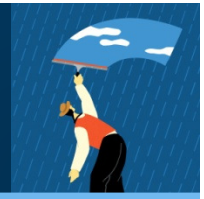
Collection Planning: Ask the Right Questions First



- Develop an understanding of the relevant information systems
  - Physical inspection
  - Interview
  - Get an organizational chart
  - Obtain a schematic overview of the computer systems
  - Identify business owners
  - Understand retention policies

NAVIGANT CONSULTING

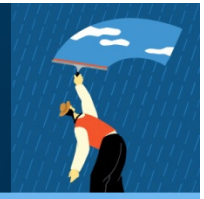
Collection Planning: Ask the Right Questions First (cont'd)



- Determine what evidence exists and where it's likely to reside
  - Who's got what, where, in what form?
  - Who keeps what and for how long?
  - Reporting features
- Custodian focused inquiries and capture
  - Inventory listings
  - AD listings
  - Interview Custodians
    - Assistants

NAVIGANT CONSULTING

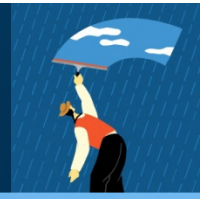
Appropriately Scope, but Cast a Wide Net



- Secure computers and data
- Create forensic images of computer hard drives and complete appropriate documentation
- Retrieve or isolate backup tapes
- Retrieve loose media
- Mobile devices
- Retrieve logs

NAVIGANT CONSULTING

We now have copies of the initial evidence. Now what?



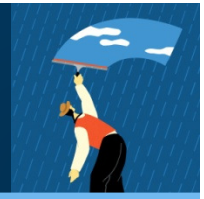
- Identify critical dates, keywords, custodians, documents type
- What does the “smoking gun” look like?
- Extract files from local drives
- Recover deleted files
- Prepare data for review

NAVIGANT CONSULTING

Interrogation of Electronic Data

NAVIGANT CONSULTING

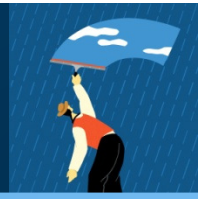
Key Decisions for Document Review (Custodian Material)



- Review Platform considerations:
  - Getting arms around data quickly
  - Pre-defined set of terms vs. refining and targeting data
  - Foreign language identification capabilities
  - Large-scale review by large teams
  - Review methodology: custodian vs. issue review
  - Tagging and coding functionality
  - Production and reporting capabilities
  - Pre-processing steps: Single vs. Multi-step
  - Cost models (processing and hosting)

NAVIGANT
CONSULTING

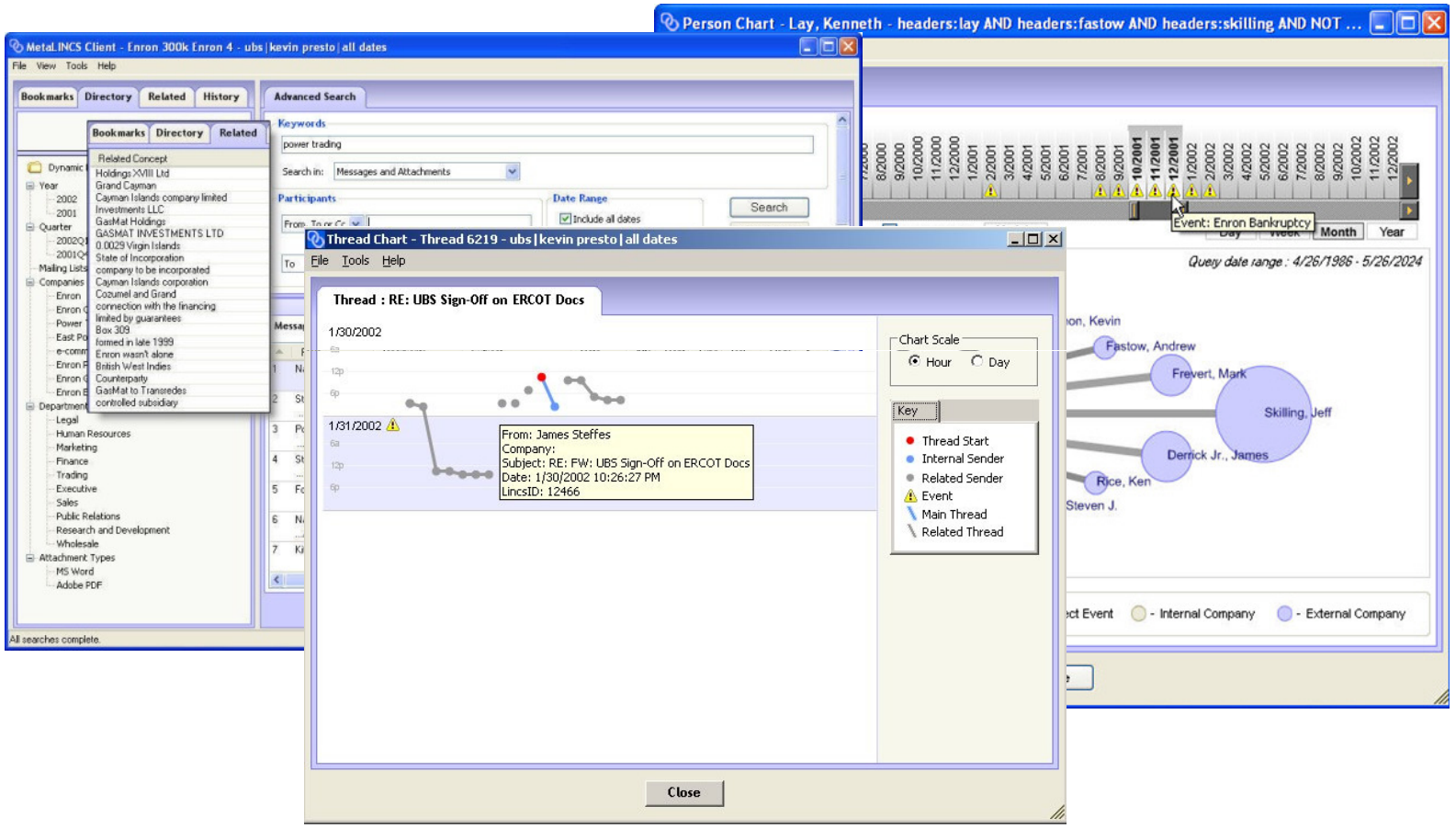
Early Case Assessment Tools



- Concept/contextual analysis
  - Determines what themes/concepts are being discussed and in what context
  - Unbiased, system-based view of what the documents are about
- Email threads/social networking analysis
  - Determine time period and recipients of an email
  - Frequency with which someone receives email from another person and patterns
    - Gaps in email correspondence
    - Unusual times for sending messages
  - Manner in which email was sent/received to specific people (To, From, CC, BCC)

NAVIGANT CONSULTING

User Experience

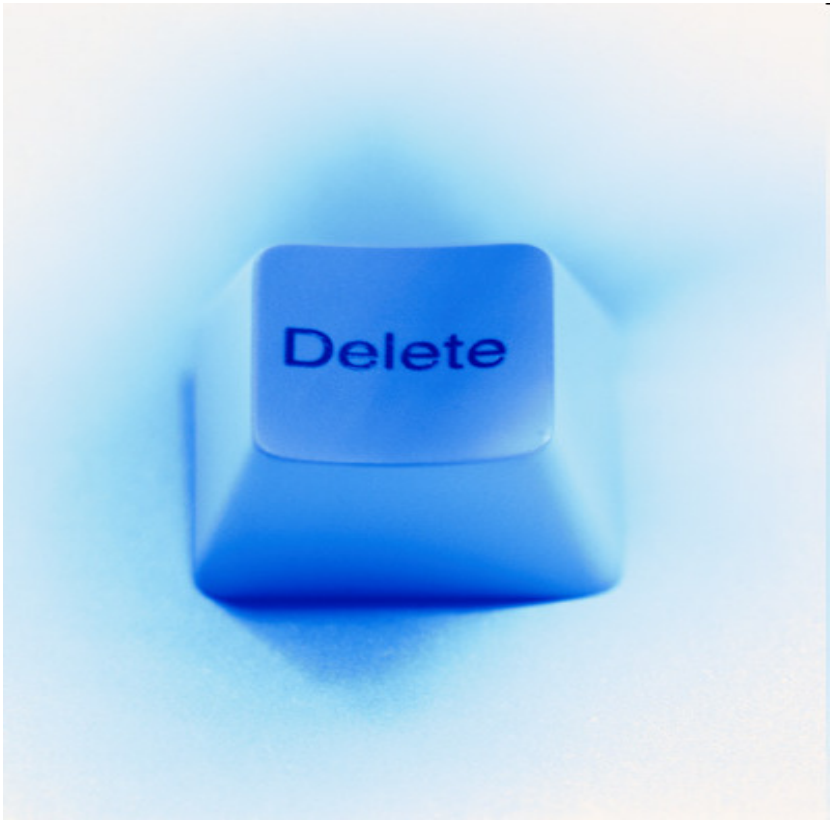


NAVIGANT CONSULTING

Forensics and Data Analysis

NAVIGANT CONSULTING

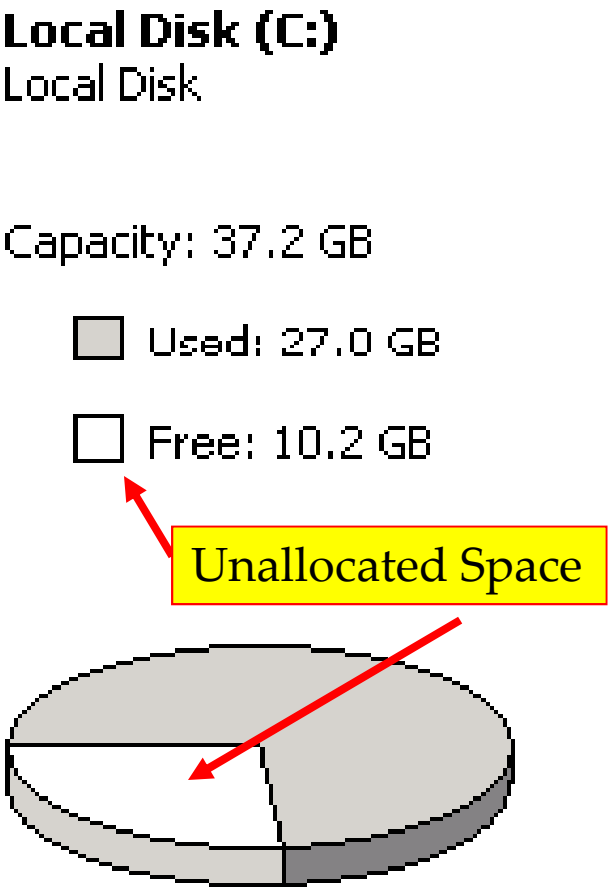
What Happens to Deleted Files?



- Operating system just marks space as available
- True text of file still viewable with forensic software
- Text may stay on computer's hard drive for years

NAVIGANT CONSULTING

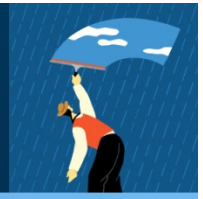
Unallocated Space



- Remainder of space on the hard drive
- Is constantly used by the computer's operating system
- May hold vast amounts of old information
- Exists on most electronic media

NAVIGANT CONSULTING

Data Forensics and Further Targeted Data Inquiries



- Email
  - Did the custodian have suspect communications with others not identified as custodians
  - Was anything deleted? Wiped?
  - Run keyword searches against fragments, partially overwritten data
- Files on images
  - Was anything deleted? Wiped?
  - What websites were accessed and when?
- Webmail & IM
  - Identify if Custodians used a webmail accounts or IM
  - Identify if other custodians of interest used webmail account

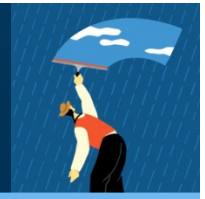
NAVIGANT CONSULTING

Web-Based Email: Spotlight

- Hotmail and Yahoo are widely used
- Mostly used for personal mail
- Messages are read while on the internet
- Pages are in “HTML” format
- Data may exist with some frequency in unallocated space of hard drive

NAVIGANT CONSULTING

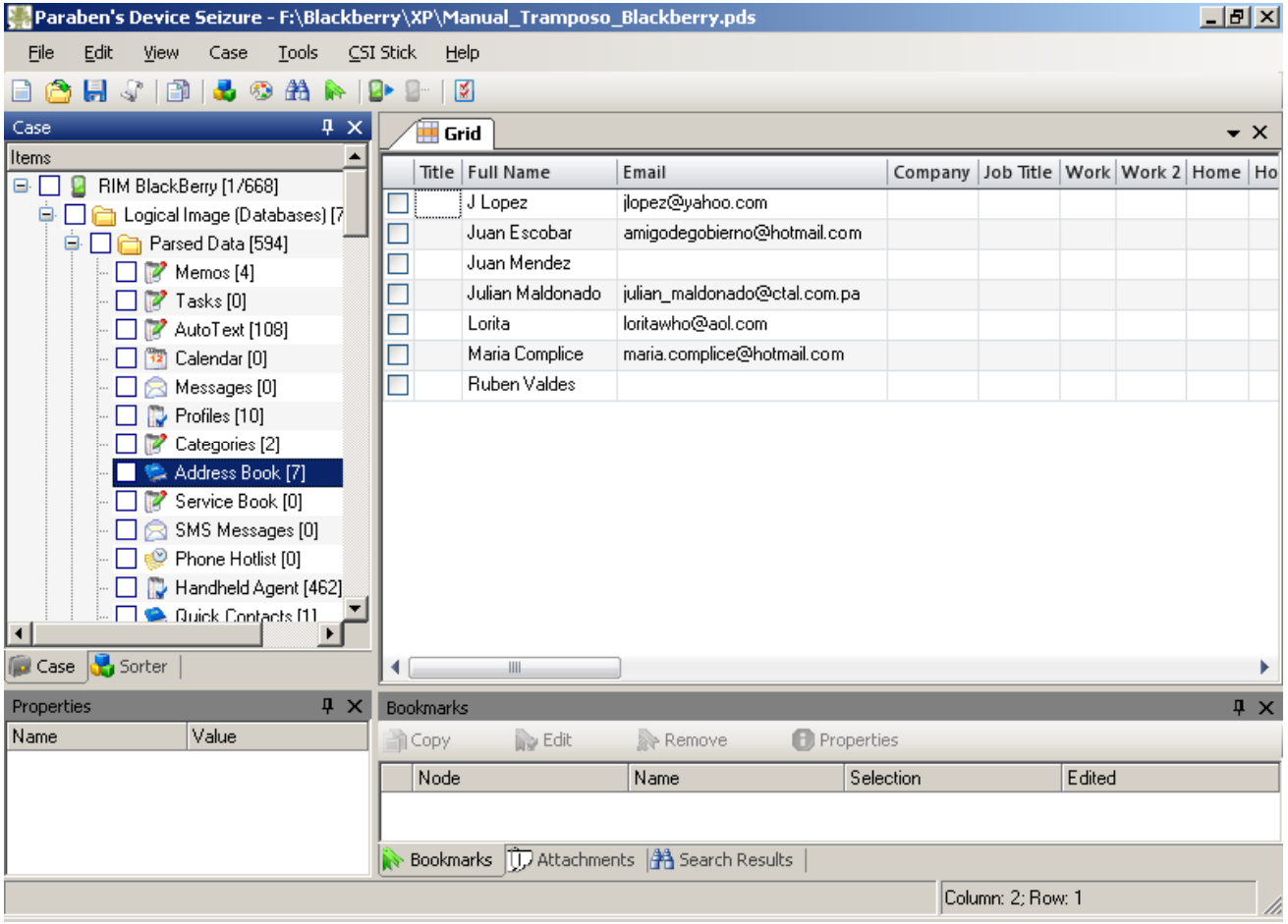
Data Forensics and Further Targeted Data Inquiries (cont'd)



- Consider review of non-email based blackberry data
  - Identify SMS messages
  - Identify call logs and address books
- Consider other mobile devices
- Collect additional data based on the above findings
  - Image custodians additional computers
  - Image additional media and server locations identified
  - Image additional custodian computers, email, and media that have been identified

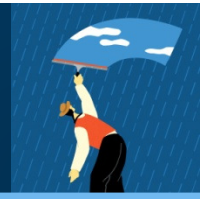
NAVIGANT CONSULTING

Forensics: Mobile Device – Non-Email Data



NAVIGANT CONSULTING

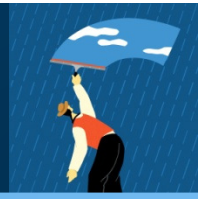
Ongoing Drill Down Efforts

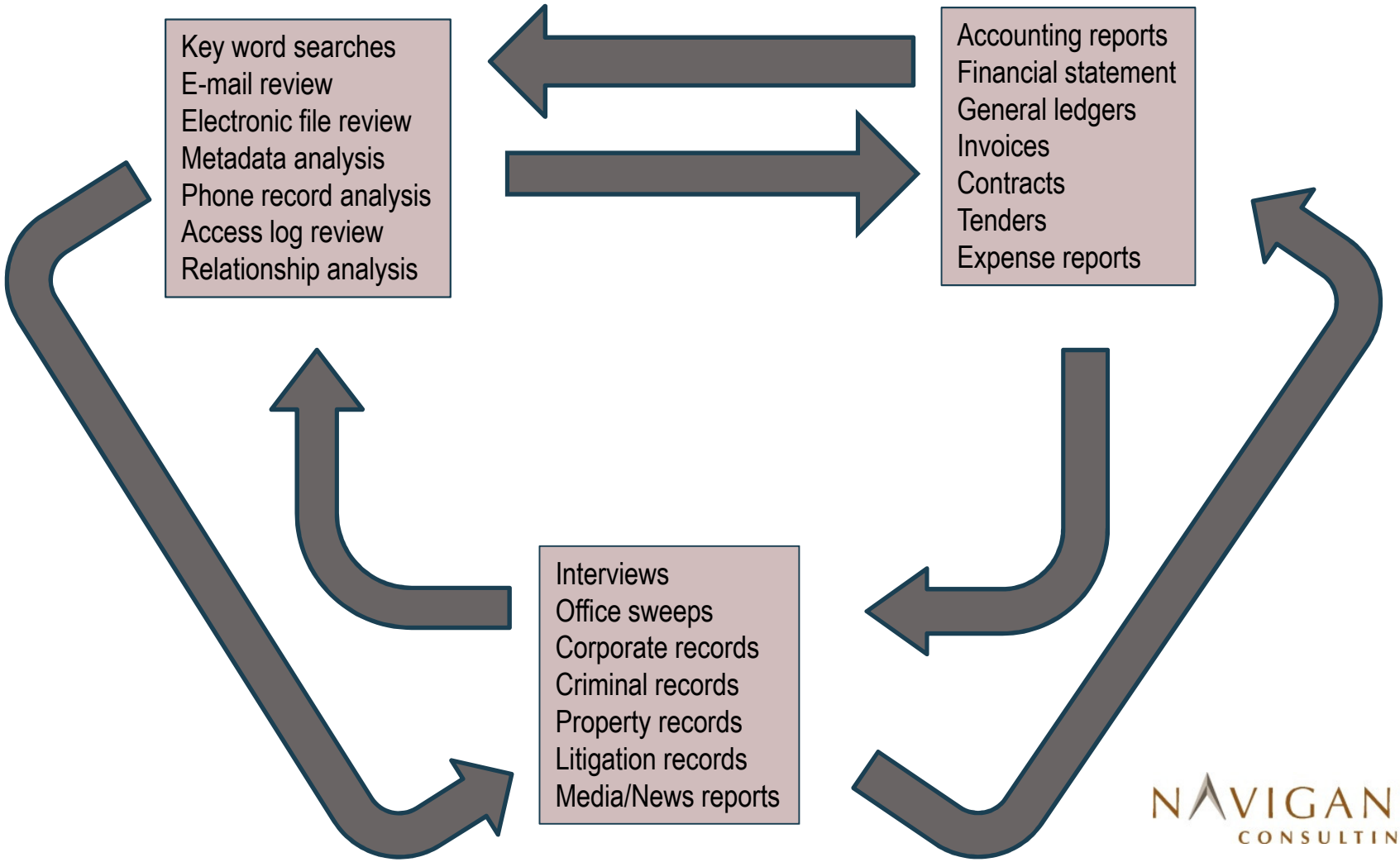


- Identify additional custodians
- Data sources
- Revise keywords
- Extract relevant emails and files
- Recover web pages
- Additional documents for review

NAVIGANT
CONSULTING

Ideal Investigative Workflow and Methodology



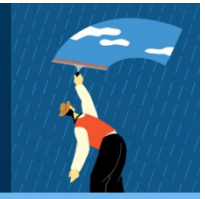


NAVIGANT CONSULTING

Q & A

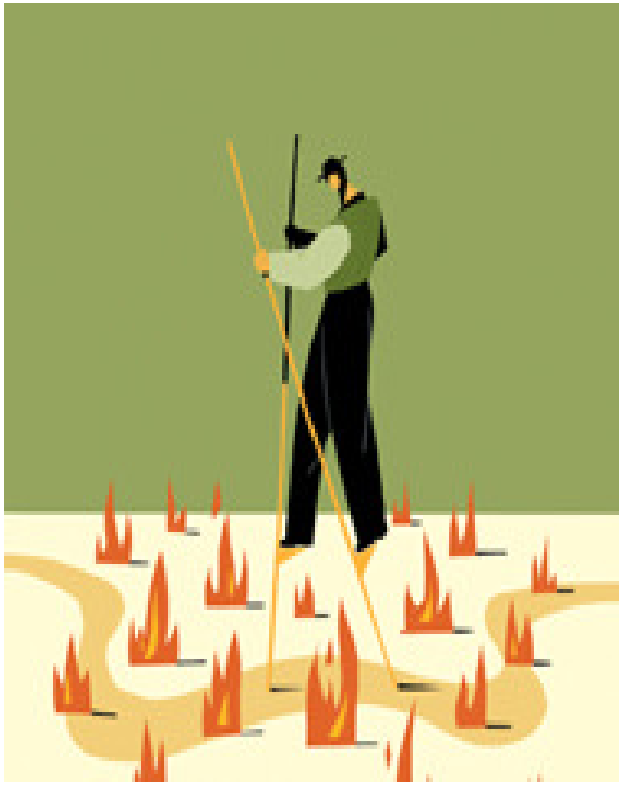
NAVIGANT CONSULTING

Contact Information



NAVIGANT CONSULTING

Andy Teichholz, JD
Director
Disputes & Investigations
ateichholz@navigantconsulting.com
646.227.4241 direct



NAVIGANT CONSULTING