

DIGITAL FORENSIC TECHNOLOGY

SEE BEYOND THE NUMBERS

Key Terms and Definitions

- **Forensic Technology**
- **e-Discovery**
- **Computer Forensics**
- **Data Analysis / Data Mining**
- **FRCP - Revised**

SEE BEYOND THE NUMBERS

Key Terms and Definitions

- **Forensic Technology** - The application of scientific knowledge and methodology to legal problems and criminal investigations. It's a very broad field with subdivisions such as criminalistics, anthropology, archeology, biology, entomology, geology, etc. More recently, with the increasing role of electronic devices and media (computers, recordable CDs / DVDs, cell phones, and more) in our lives, a new branch of forensic technology now concentrates in the investigation of electronic evidence, in a variety of forms.

SEE BEYOND THE NUMBERS

Key Terms and Definitions

- **e-Discovery** - Short for electronic discovery, is the process by which litigants find and produce documents stored in electronic form in response to internal investigations, litigation or regulatory requirement.

SEE BEYOND THE NUMBERS

Key Terms and Definitions

- **Computer Forensics** - There are a number of slightly varying definitions for computer forensics. Generally speaking, computer forensics is the use of analytical and investigative techniques to identify, collect, examine and preserve electronic evidence, which is magnetically stored or encoded.

SEE BEYOND THE NUMBERS

Key Terms and Definitions

- **Data Analysis / Data Mining** - the process of systematically applying statistical and logical techniques to describe, summarize, and compare data. The process of discovering meaningful correlations, patterns, and trends by sifting through large amounts of data stored in repositories, using pattern recognition technologies as well as statistical and mathematical techniques.

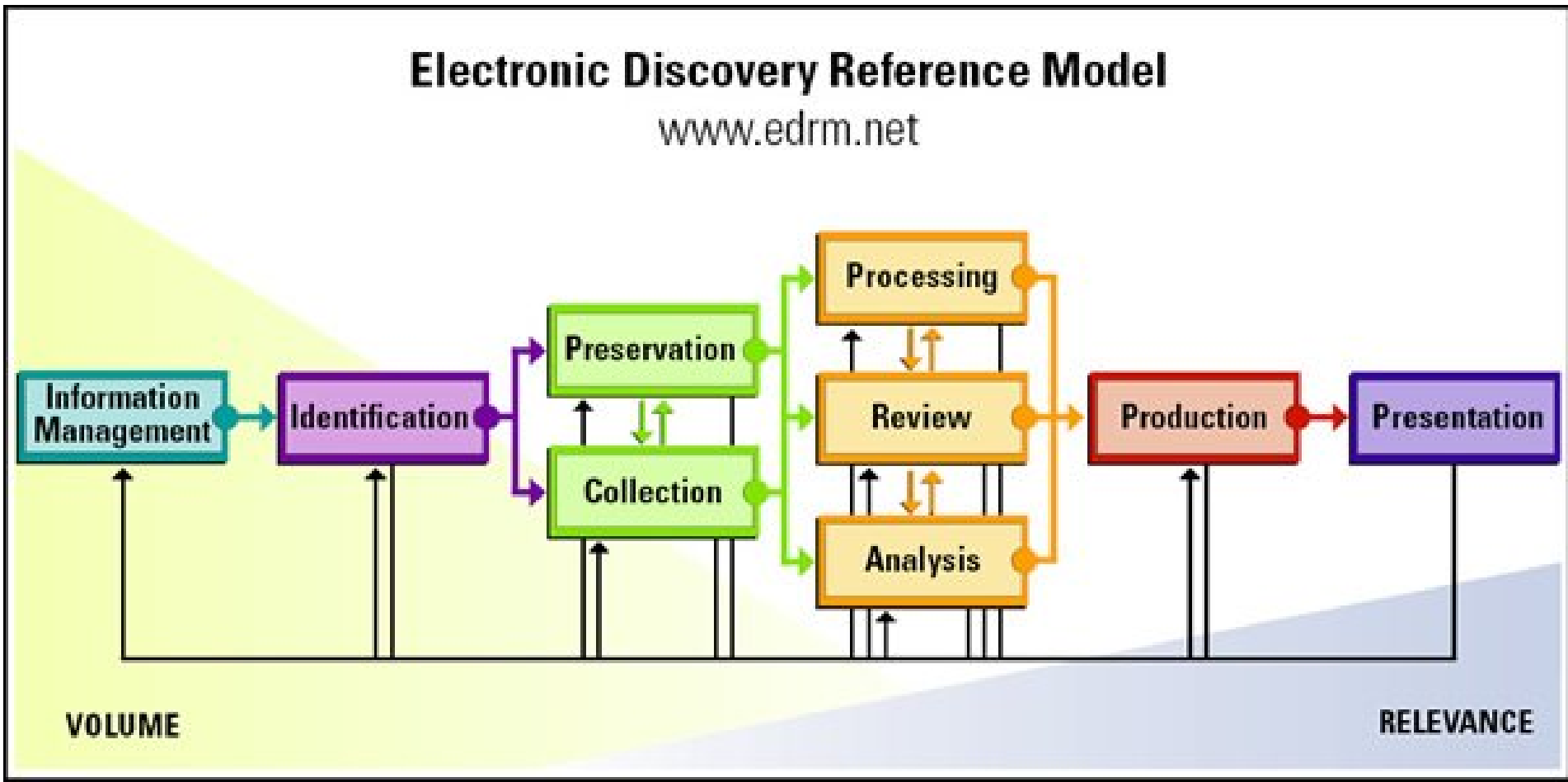
SEE BEYOND THE NUMBERS

Key Terms and Definitions

- Federal Rules of Civil Procedure - Revised
 - December 1st 2006
- Revision aimed at a particular area of discovery: Electronic Stored Information – ESI
- Main rules concerning ESI
 - Rule 16(b) 5 & 6: Pretrial Conferences; Scheduling management
 - Rule 26: General provisions for discovery; duty to disclosure
 - Rule 33(d): Interrogatories to parties
 - Rule 34(a) & (b): Production of docs, ESI, “Entry Upon Land”
 - Rule 37(f): Good faith (“Safe Harbor”), Failure to disclose
 - Rule 45: Subpoena rules affecting ESI

SEE BEYOND THE NUMBERS

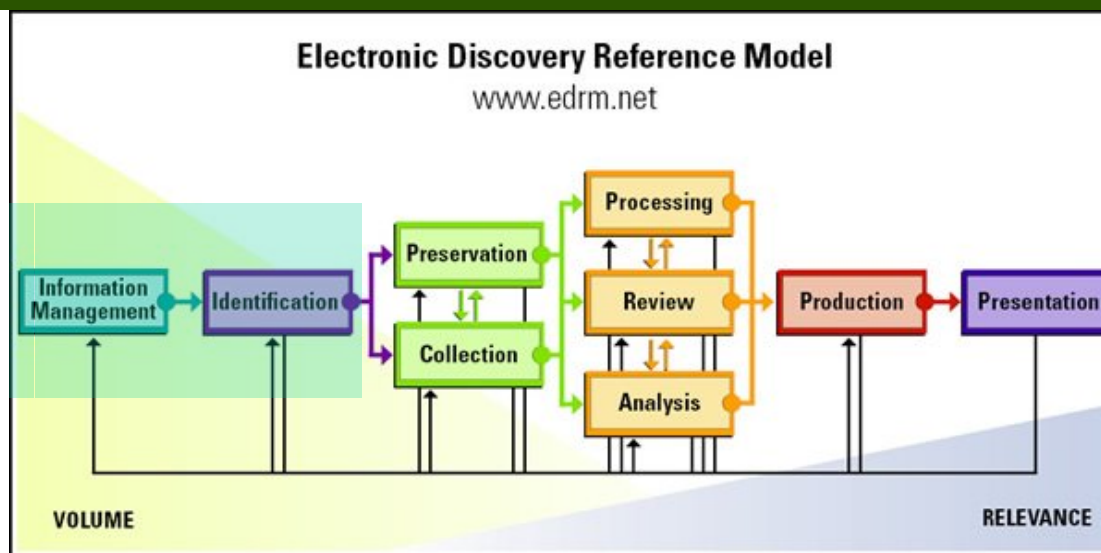
E-Discovery Reference Model



Note: EDRM (www.edrm.net) is a widely-recognized organization that since 2005 focus its efforts in creating resources, standards and best practices for e-Discovery.

SEE BEYOND THE NUMBERS

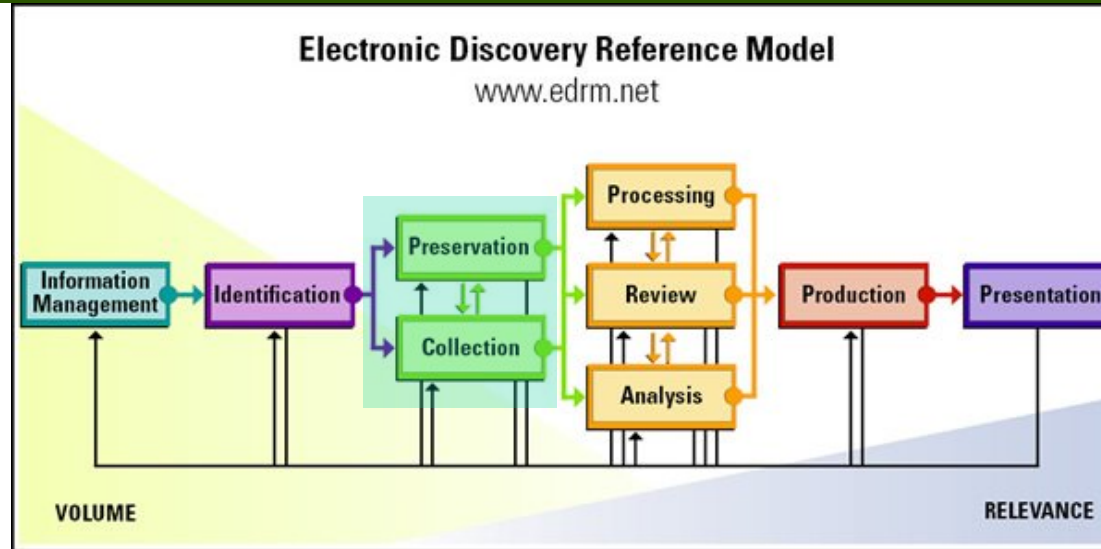
Pre-Acquisition



- During the information management and identification phases (highlighted above):
 1. Identify custodians and location of electronically stored information and estimating the magnitude of data,
 2. Map of network in advance of litigation,
 3. Respond to production request, or
 4. Craft a production request.
- All with the objective of developing a strategy to identify the potential evidence items pertinent to the case.

SEE BEYOND THE NUMBERS

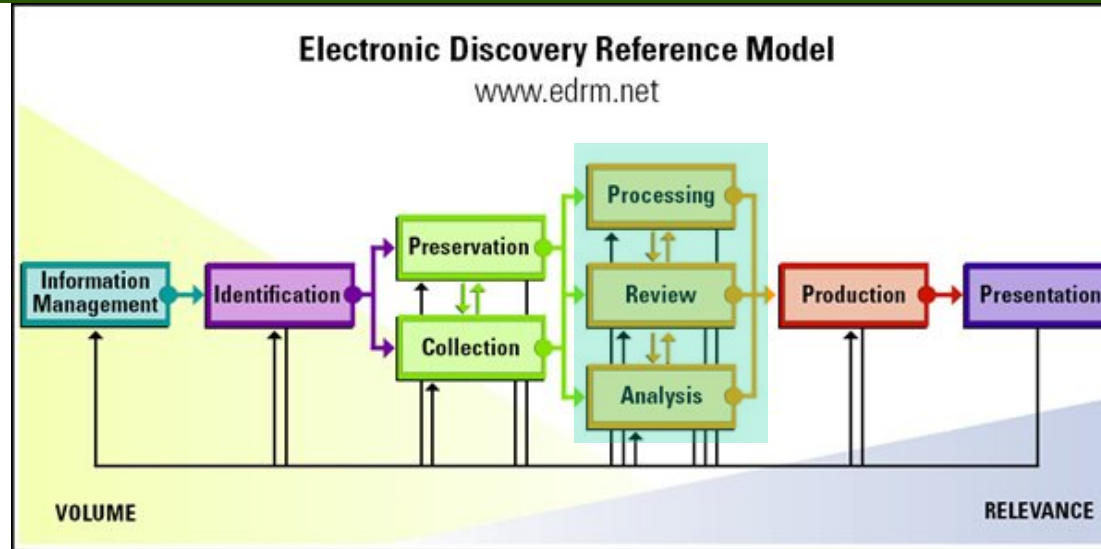
Preservation & Collection



- In the preservation and collection phases, evidence items are acquired and preserved to avoid spoliation.
- All pertinent documentation (chain of custody, evidence intake, evidence inventory, investigator notes, etc) is prepared to ensure admissibility in court.

SEE BEYOND THE NUMBERS

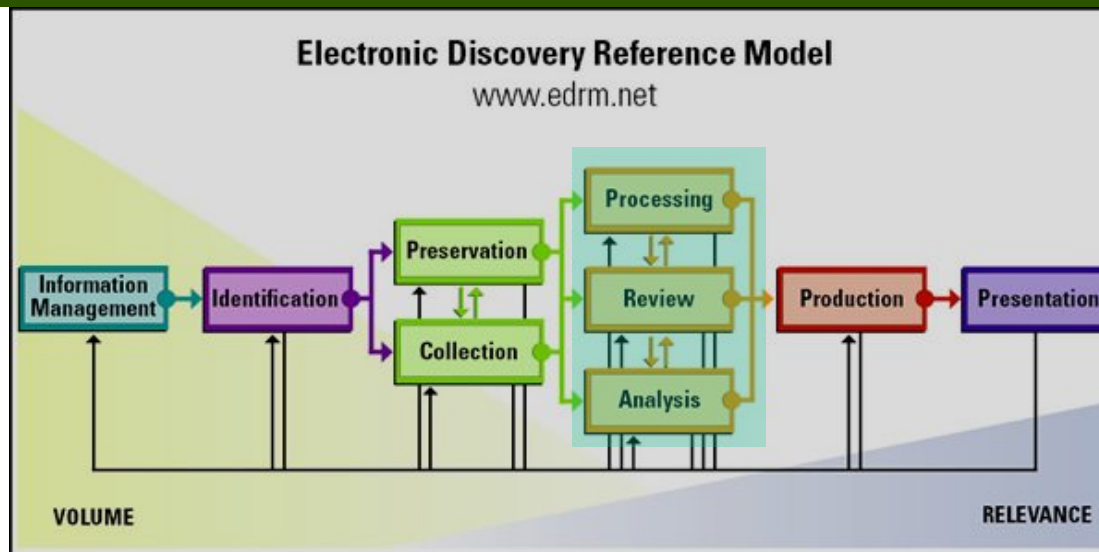
Processing



- At this point, evidence items are processed and prepared for analysis and review.
- The specifics of each phase will depend on the situation and can be computer forensics, e-Discovery or data mining.

SEE BEYOND THE NUMBERS

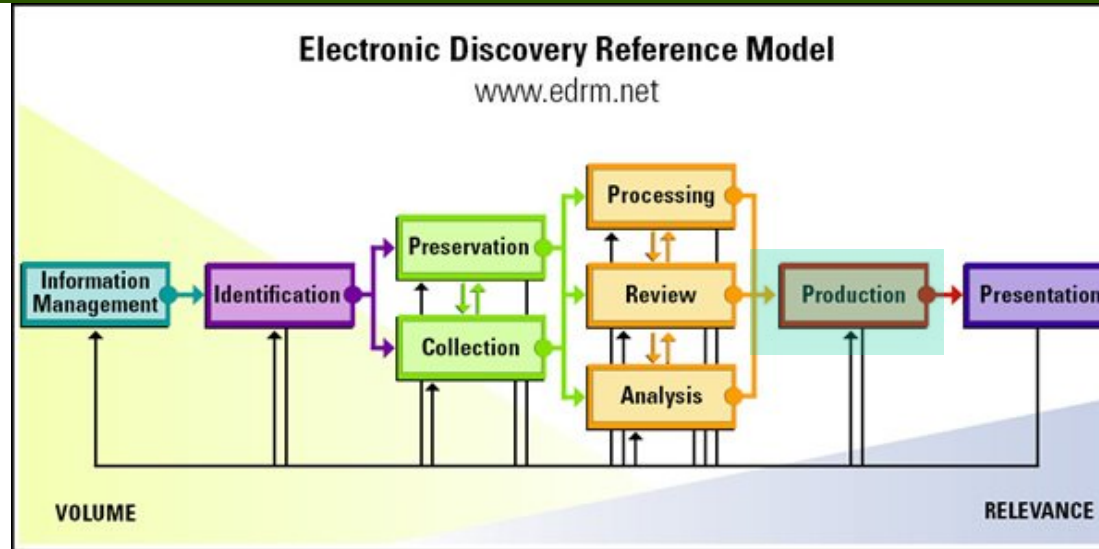
Processing



- Computer Forensics – Interpret how the computer was used by conducting a detailed analysis of hard drive(s), such as deleted files, registry entries, etc.
- e-Discovery – Conduct initial search, data culling and production of documents for legal review.
- Data Mining – Manipulating large volumes of data to identify anomalies, suspicious transactions, links between suspects, key emails and attempts to manipulate financial records.

SEE BEYOND THE NUMBERS

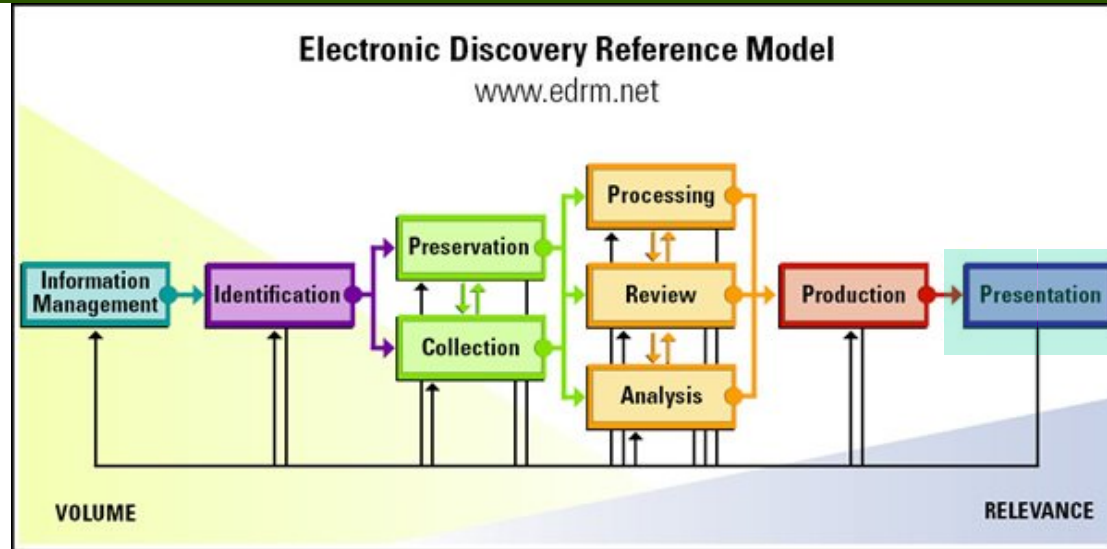
Production



- Preparation of deliverables typically depend on the situation and can range from production on electronic media (CD's and DVD's) to complex analysis, timeline reports, etc.

SEE BEYOND THE NUMBERS

Presentation



- The culmination of the entire process. Help counsel determine the best suitable way to demonstrate the results of the investigation to prove or disprove a case.

SEE BEYOND THE NUMBERS

Digital Forensics Technology

	Digital Investigations	e-Discovery	ESI Consulting	Computer Forensics
Information Management		<ul style="list-style-type: none"> Regulatory Compliance Data Security e-Disc. Preparedness 	<ul style="list-style-type: none"> Regulatory Compliance Data Security e-Disc. Preparedness 	
Data Identification	<ul style="list-style-type: none"> Data mapping Collection plan develop. Custodians Repositories 	<ul style="list-style-type: none"> Data mapping Collection plan develop. Custodians Repositories 	<ul style="list-style-type: none"> Data mapping Collection plan develop. Custodians Repositories 	<ul style="list-style-type: none"> Collection plan develop. Custodians Repositories
Acquisition & Preservation	<ul style="list-style-type: none"> Hard drives Network & data files E-mail Other media 	<ul style="list-style-type: none"> Hard drives Network & data files E-mail Other media 		<ul style="list-style-type: none"> Hard drives Network & data files E-mail Other media
Processing, Analysis & Review	<ul style="list-style-type: none"> Data mining Anomaly identification Search terms e-mail & document review 	<ul style="list-style-type: none"> Data culling <ul style="list-style-type: none"> De-duping Search terms Date filtering 		<ul style="list-style-type: none"> Use analysis Deleted files analysis Link files analysis
Production		<ul style="list-style-type: none"> Request for production Response to request for production Responsive documents 		<ul style="list-style-type: none"> Findings
Presentation	<ul style="list-style-type: none"> Investigative report Fact testimony 	<ul style="list-style-type: none"> Affidavits Expert report Expert testimony 	<ul style="list-style-type: none"> Consulting report 	<ul style="list-style-type: none"> Affidavits Expert report Expert testimony

SEE BEYOND THE NUMBERS