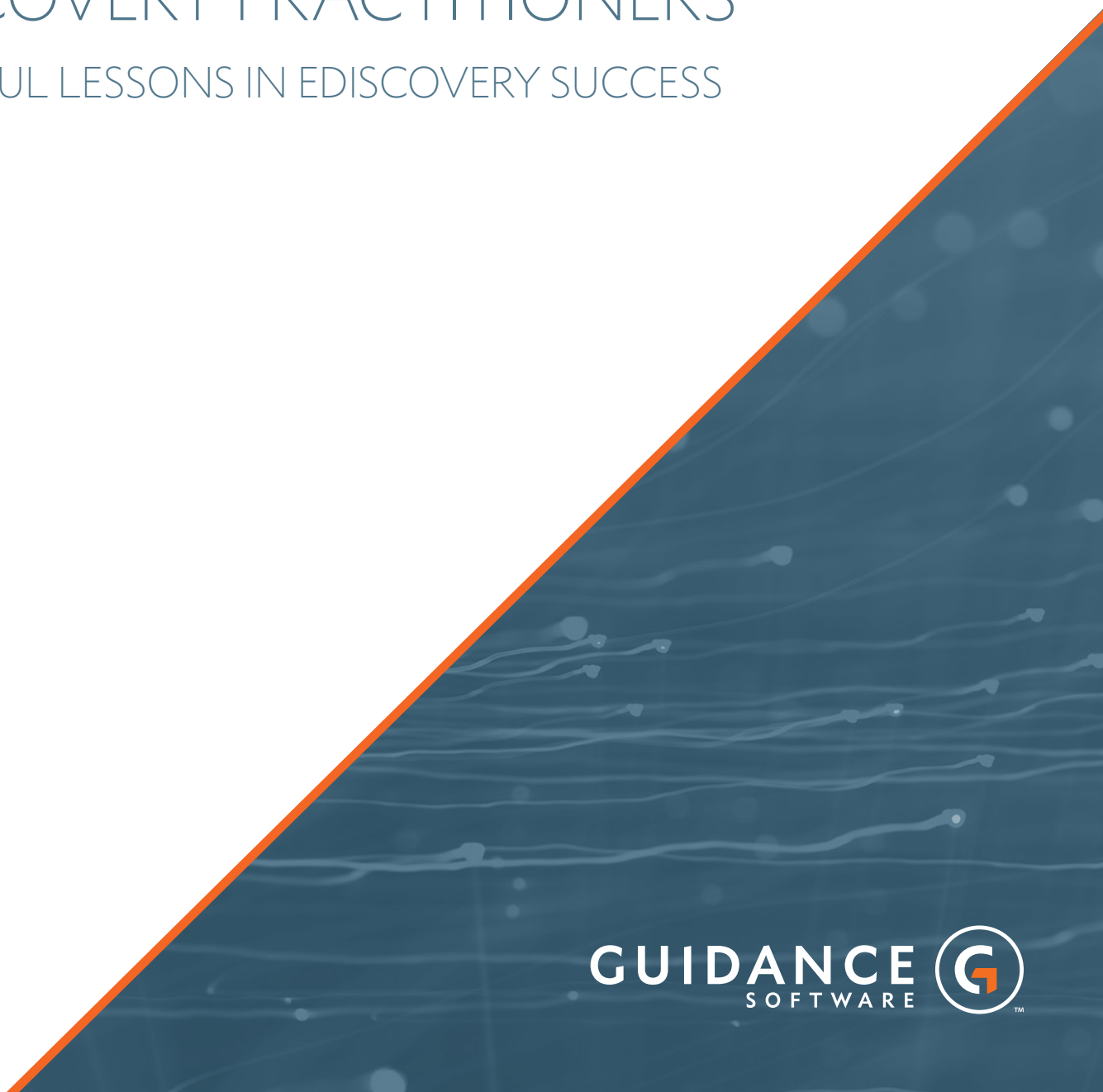
Whitepaper

THE SEVEN BEST PRACTICES OF HIGHLY EFFECTIVE EDISCOVERY PRACTITIONERS

POWERFUL LESSONS IN EDISCOVERY SUCCESS



GUIDANCE SOFTWARE™

POWERFUL LESSONS IN EDISCOVERY SUCCESS

More than six years have passed since the initial Zubulake opinion addressing the preservation duties for ESI and more than three years since the changes to the Federal Rules of Civil Procedure addressing e-discovery. However, corporations and organizations continue to suffer spoliation sanctions and make missteps in the search and preservation of relevant ESI.

Many organizations have focused effort on established processes and implementing records management solutions to address e-discovery. While such initiatives are important to the overall goal of establishing a defensible, repeatable process for addressing e-discovery, such efforts are not enough in and of themselves to avoid the pitfalls of e-discovery preservation.

This document identifies seven key best practice considerations that will assist in establishing a complete e-discovery process for the defensible, systematic, repeatable preservation of ESI for litigations and investigations.

1 ESI OTHER THAN EMAIL

BEST PRACTICE	LEGAL STANDARD	ENCASE eDISCOVERY SOLUTION
Preserve Relevant ESI from all potential data sources – not just email.	Attention to the duty to preserve ESI involves more than just preserving emails; the duty requires the preservation of ALL relevant ESI, including Word docs, Excel files, .pdfs, e-mail archives, etc. stored locally on laptops, desktops, servers, etc. There are hundreds of cases where the critical evidence was ESI other than email. See, e.g., Beard Research v. Kates, CA No. 1316, (Del. Chanc. May 29, 2009) (PowerPoint presentations); Digene Corp. v. Third Wave Technologies, Inc., 2008 U.S. Dist. LEXIS 10816 (W.D. Wisc. Feb. 8, 2008) (PowerPoint presentations); Sprint v. United Management Co., 2007 U.S. Dist. LEXIS 5477 (D. Kan. Jan. 23, 2007) (spreadsheets); United States v. Woody, 2008 U.S. Dist. LEXIS 16734 (W.D.N.C. Feb. 20, 2008) (spreadsheets); Convolve, Inc. v. Compaq Computer Corp., 2004 U.S. Dist. LEXIS 16164 (S.D.N.Y. Aug. 17, 2004) (party wanted direct access to databases, hard drives, and servers); Sklar v. Clough, 2007 U.S. Dist. LEXIS 49248 (N.D. Ga. Jul. 6, 2007 (article from online newspaper, PowerPoint presentation); General Medicine, PC v. Morning View Care Centers, 2006 U.S. Dist. LEXIS 49598 (S.D. Ohio Jul. 20, 2006) (billing data); W.E. Aubuchon Co., Inc. v. BeneFirst, LLC, 245 F.R.D. 38 (D.Mass.,2007) (electronic images of claim forms); In re eBay Seller Antitrust Litigation, 2007 U.S. Dist. LEXIS 75498 (N.D. Cal. Oct. 2, 2007) (document retention notices).	EnCase eDiscovery can search and collect from all potentially relevant data sources, including computer hard drives, servers, and shared drives. EnCase eDiscovery allows processing of all potentially relevant file types --- including Word, Excel, PowerPoint, .pdf, etc. --- as well as emails from ALL email sources (archives, Exchange and Domino servers, locally stored PST and NSF files). EnCase eDiscovery can also collect content from various content management and email archive systems such as Microsoft SharePoint, EMC Documentum ECM, Open Text ECM and Symantec Enterprise Vault through its Connectors.

2 AUTHENTICATION AND CHAIN OF CUSTODY

BEST PRACTICE	LEGAL STANDARD	ENCASE eDISCOVERY SOLUTION
Create a defensible, repeatable process that establishes authentication and preserves chain of custody of ESI.	Authentication requires specific tracking of when and how ESI is acquired, as well as how ESI is maintained from collection through trial. United States v. O'Keefe, 2008 WL 449729 (DC February 18, 2008) ("A piece of electronically stored information, without any indication of its creator, source, or custodian may not be authenticated under Federal Rule of Evidence 901."); Williams v. Great-West Healthcare, 2007 WL 4564176 (N.D.Ga. June 8, 2007) ("The requirement that there be something more than the appearance of the item is particularly important with respect to documents that can be easily altered, such as those generated by computer").	EnCase eDiscovery's CRC checking, MD5-hashing, and proprietary LEF storage file with GUID identifier ensure proof that ESI is not altered from collection through trial. EnCase eDiscovery's database automatically tracks sources of ESI searched and files collected. The GUID identifies what search criteria was used to identify the preserved ESI. The database also keeps a full audit trail of all user activities, such as processing and document tagging. Complete chain of custody is kept from collection, through processing, and load file creation.

3 LEGAL RISK

BEST PRACTICE	LEGAL STANDARD	ENCASE eDISCOVERY SOLUTION
Preserve and collect ESI for EVERY potential case as early as reasonably practical.	80-90% of the legal risk in e-discovery occurs at the preservation stage. If you fail to preserve ESI properly at the beginning of a case, it is difficult and sometimes impossible to reliably retrieve relevant ESI and metadata months or years later, and the effort can be costly. This legal exposure is increasing. According to a recent Gibson Dunn survey, the number of cases considering and awarding sanctions in the first 5 months of 2009 for preservation failures increased two-fold compared to cases during the first 10 months of 2008. Sanctions were awarded in 36% of 2009 cases considering challenges to eDiscovery collections. The amount of sanctions can be substantial. See Qualcomm, Inc. v. Broadcom Corp., 2008 WL 66932 (S.D.Cal. 2008) ($8.5 million in sanctions); United States v. Philip Morris USA, 327 F. Supp.2d 21 (D.D.C 2004) ($2.75 million in sanctions); MOSAID Techs. Inc. v. Samsung Elec. Co., 348 F. Supp. 2d 334 (D.N.Y. 2004) ($500+ million in sanctions). Other severe sanctions can also result. Micron Tech v. Rambus, 225 F.R.D. 135 (D. Del 2009) (Rambus DRAM patents held unenforceable because of destruction of ESI prior to litigation); Kvitka v. Puffin Co., 2009 WL 385582 (M.D. Pa. Feb. 13, 2009) (dismissal of claims and adverse inference on counter-claim).	EnCase eDiscovery squarely addresses the area of highest risk in eDiscovery -- collection and preservation of ESI. EnCase eDiscovery enables an organization to search, assess, and collect data without involvement or disruption of potential witnesses. Data sources such as computers, shared drives, email, and structured data sources are searched and collected in a systematic, repeatable, and defensible manner at the onset of litigation. EnCase eDiscovery automates the collection of ESI using the same technology and same criteria to search all relevant data sources.

4 LEGAL HOLD

BEST PRACTICE	LEGAL STANDARD	ENCASE eDISCOVERY SOLUTION
Implement an automated legal hold solution.	It is important to have a defensible process for giving notice of an ESI legal hold to potentially relevant witnesses. Green v. McClendon, 2009 WL 2496275 (S.D.N.Y. Aug. 13, 2009) (finding defendant failed to meet discovery obligations by neglecting to issue a litigation hold and properly search for responsive documents). Courts have imposed sanctions for failure to issue a legal hold. KCH Servs., Inc. v. Vanaire, Inc., 2009 WL 2216601 (W.D.Ky. July 22, 2009) (issuing adverse inference instruction for defendant's failure to issue a legal hold notice).	EnCase eDiscovery Legal Hold automates the issuance of hold notices and provides high level reporting on the status of responses. EnCase eDiscovery Legal Hold is an integrated part of EnCase eDiscovery so that Legal and IT are working off the same list of potential witnesses for issuing hold notices and executing ESI collections. EnCase eDiscovery Legal Hold can be used by corporate legal departments through a simple webbased interface to automate and track custodian email notification workflows. They can receive, compile and analyze custodian acknowledgments and create customizable, open-ended or multiple choice caserelated interview style questions.

5 TARGETED SEARCH AND COLLECTION

BEST PRACTICE	LEGAL STANDARD	ENCASE eDISCOVERY SOLUTION
Employ technology enabling targeted surgical search capability for pre-collection testing, collection of relevant data, and post-collection analysis.	Courts consider the concept of sampling to test cost and potential volume of searches part of the mainstream approach to eDiscovery. SEC v. Collins & Aikman Corp., 2009 WL 94311 (S.D.N.Y. Jan. 13, 2009). In re Genetically Modified Rice Litigation, 2007 WL 1655757 (June 5, 2007 E.D.Mo.) ("Preservation efforts can become unduly burdensome and unreasonably costly unless those efforts are targeted to those documents reasonably likely to be relevant or lead to the discovery of relevant evidence related to the issues in this matter.") "Acceptable sampling techniques, in lieu of discovery and presentation of voluminous data from the entire population, can save substantial time and expense, and in some cases provide the only practicable means to collect and present relevant data." Manual for Complex Litigation, 4th. Most cases do not require full-disk collections. Standard for ESI is to collect potentially relevant information. Zubulake v. UBS Warburg LLC, 220 F.R.D. 212, 217 (S.D.N.Y. 2004) ("Zubulake IV"); Diepenhorst v. City Of Battle Creek, 2006 WL 1851243 (W.D.Mich. June 30, 2006): (Full Disk Imaging not required as a matter of course in eDiscovery context). Also, for FRE 502, organizations are encouraged to use search technology to assist in identifying potentially privileged ESI. A party that uses advanced analytical software applications in screening for privilege and work product may be found to have taken "reasonable steps" to prevent inadvertent disclosure. Explanatory Note on Evidence Rule 502, Judicial Conference Advisory Committee.	EnCase eDiscovery's Pre-Collection Testing and Analytics provides initial metrics on the amount and types of potentially relevant ESI by testing environments for specific types of files, ESI types, date ranges, etc. EnCase eDiscovery provides assessment of collected data through advanced search, email threading, and tagging capabilities. EnCase eDiscovery allows for targeted search and collection of ESI, using filtering criteria on the front-end such as file types, keywords, and date ranges. Front-end filtering reduces volume of data collections by over 90% by excluding non-relevant file types. At either the pre- or post-collection stage, ESI can be analyzed for confidential or privileged ESI with search criteria through the ability to search for keywords, file types, metadata, timestamps, hashing and other fields.

6 TRAINING AND CERTIFICATION

BEST PRACTICE	LEGAL STANDARD	ENCASE eDISCOVERY SOLUTION
Designate testifying experts as to the organization's defensible, repeatable eDiscovery processes, and provide them with appropriate training and certifications.	Training and certification are essential for 30(b)(6) and expert testimony. Education and certification provides foundation for testimony addressing collection and preservation of ESI. U.S. Gypsum Co. v. Lafarge North America Inc., 2009 WL 3598422 (N.D. Ill., Oct. 27, 2009) (Testifying expert with EnCase certification determined to be a competent expert in computer forensics, motion in limine to exclude testimony denied as to evaluation of evidence and opposing expert).	Guidance Software provides world-class training and certifications in forensics (EnCE) and eDiscovery (EnCEP) for established industry standards to qualify witnesses for expert testimony relating to ESI collections. With 12 training classes offered in over 30 countries worldwide, along with online and OnDemand training, Guidance Software is an industry leader in training and certification. http://www.guidancesoftware.com/computer-forensics-training.htm

7 METADATA

BEST PRACTICE	LEGAL STANDARD	ENCASE eDISCOVERY SOLUTION
Preserve metadata in a forensically-sound manner at the point of collection.	The volatile nature of metadata makes preserving it at the point of collection critical to future requirements and to avoid adverse inferences or sanctions. Production of ESI should be made in a form in which information is ordinarily maintained or reasonably usable, taking into account the need to produce reasonably accessible metadata that gives the receiving party the same ability to access, search, and display information as the producing party. Sedona Conference Principle 12. Common metadata fields for electronic files include author, subject, file name, date and time created, and date and time last saved. For e-mail, common fields include author, recipient, CC, subject, BCC, date sent, and file name. Preserving these basic fields in a forensically-sound manner is important for authentication of ESI at trial as well as giving context to files and searchability for review. Courts generally order production of metadata when requested in the initial discovery request. Aguilar v. ICE / DHS, 2008 WL 5062700 (S.D.N.Y. Nov. 21, 2008). The challenge with metadata is that at the time of preservation and collection of ESI, it is unknown if the metadata is, or will become, relevant. If the metadata is altered at the outset, it can be impossible to reset it to its original state. Thus, best practice is to lock down the metadata in a forensically sound manner for every case. Preserving original metadata assists in the document review stage of litigation, in creating timelines, and in establishing authorship of ESI. Failure to preserve metadata has significant adverse consequences. Bray & Gillespie Management LLC, v. Lexington Ins. Co., 2009 WL 546429 (M.D. Fla. Mar. 4, 2009) (Sanctions imposed on plaintiff's counsel and plaintiffs required to cover costs and allow access to their data sources for failure to produce ESI with metadata included).	EnCase eDiscovery automatically maintains ALL original metadata, including created and last accessed dates, with the source file in a Logical Evidence File ("LEF") container, which cannot be altered. Metadata is kept in its original state with the file, not stored separately. Collected files are exact duplicates in every manner of the original source file, and are kept in its original state throughout processing and load file creation within EnCase eDiscovery.

ENCASE EDISCOVERY SOLUTION

For legal counsel and Information Security/IT Directors within large organizations that need a more cost-effective and efficient business process to conduct electronic discovery in-house for internal, legal, or regulatory investigations --- EnCase eDiscovery is the market-leading electronic discovery software that delivers a more efficient in-house business process and significantly reduces legal risk and cost to organizations with a judicially accepted solution that provides legal hold to first-pass review and is scalable, defensible, and repeatable.

EnCase eDiscovery is a single integrated, in-house e-discovery solution that includes everything organizations want to do in-house:

- Legal Hold
- Pre-Collection Analytics
- Collection and Preservation
- Processing
- Analysis and First-pass Review

In order to ensure in-house success, EnCase eDiscovery is bolstered by expert resources, services, training and certification.

EnCase eDiscovery uniquely enables legal teams to conduct early case assessment with its pre-collection analytics, powerful search analytics, and first-pass review features that enable customers to conduct analysis at any point in the process. Through this optimized process, customers obtain the necessary facts – early – to understand and assess case merits, risk, and cost.

CONCLUSION

When enterprises need to respond to time-sensitive requests for ESI – for litigation, internal investigations, or regulatory requests – they know the proven track record of EnCase makes it the market-leading, go-to solution to get the job done and defend their corporate reputation. Guidance Software is the gold standard for digital investigations and a proven leader with more than 800 enterprise customers and nearly 250 EnCase eDiscovery customers, which include more than 20% of the Fortune 100.

GUIDANCE SOFTWARE

ABOUT GUIDANCE

Guidance exists to turn chaos and the unknown into order and the known-so that companies and their customers can go about their daily lives as usual without worry or disruption, knowing their most valuable information is safe and secure. The makers of EnCase®, the gold standard in forensic security, Guidance provides a mission-critical foundation of market-leading applications that offer deep 360-degree visibility across all endpoints, devices and networks, allowing proactive identification and remediation of threats. From retail to financial institutions, our field-tested and court-proven solutions are deployed on an estimated 33 million endpoints at more than 70 of the Fortune 100 and hundreds of agencies worldwide, from beginning to endpoint.