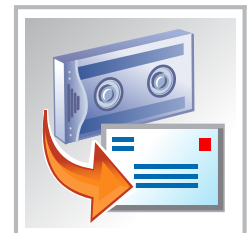


E-Discovery with Quest Recovery Manager for Exchange

Technical Brief

Version 2.2



written by
Dung Hoang Khac, HP and
David Sengupta, Quest Software, Inc

© Copyright Quest® Software, Inc. 2005. All rights reserved.

This guide contains proprietary information, which is protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software, Inc.

WARRANTY

The information contained in this document is subject to change without notice. Quest Software makes no warranty of any kind with respect to this information. QUEST SOFTWARE SPECIFICALLY DISCLAIMS THE IMPLIED WARRANTY OF THE MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Quest Software shall not be liable for any direct, indirect, incidental, consequential, or other damage alleged in connection with the furnishing or use of this information.

TRADEMARKS

All trademarks and registered trademarks used in this guide are property of their respective owners.

World Headquarters
8001 Irvine Center Drive
Irvine, CA 92618
www.quest.com
e-mail: info@quest.com
U.S. and Canada: 949.754.8000

Please refer to our Web site for regional and international office information.

Quest Recovery Manager for Exchange
Updated—March 7, 2005
Software version—2.2

CONTENTS

ABOUT HP	III
ABOUT QUEST WINDOWS MANAGEMENT	IV
ABOUT QUEST SOFTWARE, INC.	IV
CONTACTING QUEST SOFTWARE.....	IV
CONTACTING CUSTOMER SUPPORT.....	IV
PREFACE	5
INTRODUCTION TO E-DISCOVERY.....	6
ESTABLISHING AN E-DISCOVERY PLAN	7
<i>Example Scenario.....</i>	7
E-DISCOVERY CHALLENGES	10
<i>Compliance Regimes.....</i>	10
<i>Record Retention Policies</i>	10
<i>Staggering Volumes of Data</i>	11
<i>Potentially Staggering Costs</i>	11
<i>Technical Challenges</i>	11
OPTIONS FOR E-DISCOVERY	12
E-DISCOVERY AND MICROSOFT EXCHANGE	13
EXCHANGE 5.5 AND EXCHANGE 2000 NATIVE TOOLS	13
EXCHANGE 2003 AND RECOVERY STORAGE GROUPS	14
SOLUTION REQUIREMENTS FOR E-DISCOVERY.....	14
INTRODUCTION TO QUEST RECOVERY MANAGER FOR EXCHANGE	15
INSTALLATION.....	16
DEFINING THE SOURCE FOR E-DISCOVERY.....	17
E-DISCOVERY OPTIONS	19
RESTORING DISCOVERED ITEMS	20
A NOTE ABOUT ARCHIVAL.....	21
SUMMARY	22
FOR MORE INFORMATION.....	23
ABOUT DUNG HOANG-KHAC	23
ABOUT DAVID SENGUPTA.....	23
CALL TO ACTION	24

ABOUT HP

HP is a technology solutions provider to consumers, businesses and institutions globally. The company's offerings span IT infrastructure, personal computing and access devices, global services and imaging and printing. For the fiscal year ending on October 31, 2003, HP revenue totaled \$73.1 billion and is ranked No. 14 among the Fortune 500. HP serves more than one billion customers in more than 160 countries on five continents, dedicates \$4 billion (U.S.) annually to R&D of products, solutions and new technologies and employs 142,000 persons worldwide. HP and Microsoft have a 20-year relationship, the Frontline Partnership (FLP) that is dedicated to developing and delivering high value industry-standard computing solutions with data center reliability while offering unmatched ownership satisfaction and value. More details are available at the FLP web site: <http://www.hp.com/microsoft>.

For more information on HP Storage Solutions for Exchange 2003 go to www.hp.com/solutions/microsoft/exchange/storage.

ABOUT QUEST WINDOWS MANAGEMENT

Quest Software, Microsoft's 2004 Global Independent Software Vendor Partner of the Year, provides solutions that simplify, automate and secure Active Directory, Exchange and Windows environments. The Quest Windows Management group delivers comprehensive capabilities for secure Windows management and migration. For more information on Quest Software's Windows Management group, please visit www.quest.com/microsoft.

ABOUT QUEST SOFTWARE, INC.

Quest Software, Inc. delivers innovative products that help organizations get more performance and productivity from their applications, databases and infrastructure. Through a deep expertise in IT operations and a continued focus on what works best, Quest helps more than 18,000 customers worldwide meet higher expectations for enterprise IT. Quest Software, headquartered in Irvine, Calif., can be found in offices around the globe and at www.quest.com.

Contacting Quest Software

Phone: 949.754.8000 (United States and Canada)

Email: info@quest.com

Mail: Quest Software, Inc.
World Headquarters
8001 Irvine Center Drive
Irvine, CA 92618
USA

Web site www.quest.com

Please refer to our Web site for regional and international office information.

Contacting Customer Support

Quest Software's world-class support team is dedicated to ensuring successful product installation and use for all Quest Software solutions.

SupportLink www.quest.com/support

Email at support@quest.com.

You can use SupportLink to do the following:

- Create, update, or view support requests
- Search the knowledge base
- Access FAQs
- Download patches

PREFACE

With a critical dependency on e-mail communications set against the backdrop of obstinate and often elusory e-mail retention by end users, companies performing e-Discovery for operational or investigational purposes can find themselves facing monumental effort and costs. Whether responding to a legal challenge under the umbrella of any number of compliance regimes, or simply recovering lost messages for a VIP, organizations need to have both business continuity and e-Discovery preparedness technologies and processes in place.

About this document

This white paper will provide a comprehensive overview of what organizations need to consider when thinking of e-Discovery and retrieving message-level data from their Microsoft Exchange environment. It is intended to demonstrate how compliance managers, legal investigation teams, Exchange administrators, and outsourced recovery solution vendors can use Quest® Recovery Manager for Exchange to overcome the many complexities associated with mailbox recovery and e-mail investigations.

The authors wish to thank the following contributors and reviewers for their invaluable insights and assistance in producing this white paper: Aric Bernard (HP), Donald Livengood (HP), Liz Carpenter (Quest), Dave Champine (Quest), Keri Farrell (Quest), Vladimir Gusarov (Quest) and Peter terSteege (Quest).

INTRODUCTION TO E-DISCOVERY

Electronic Discovery—or “e-Discovery” as it is generally called—simply refers to discovering any information created, stored, or best utilized with computer technology of any sort¹. There are an ever-increasing range of scenarios coming to the attention of CIOs, Human Resources departments and IT managers alike in which e-Discovery is required to respond to one business requirement or another. Yet with its history entrenched in the legal technology realm, e-Discovery and its associated technologies remain largely misunderstood within most enterprise IT organizations today.

A requirement for e-Discovery can arise in any organization. Criminal and civil law define what is legal and illegal when it comes to the creation, storage, and distribution of certain content which includes electronic documents. Most corporate environments are affected by government legislation, including labor laws, privacy legislation or freedom-of-information requests, to mention a few. All publicly traded companies—notably those traded on U.S. stock exchanges, but increasingly others—are affected by industry regulations such as the Sarbanes-Oxley act, Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Gramm-Leach Bliley Act of 1999 and countless other regulations of various breadth and reach. And finally many organizations implement written IT policies that employees must consent to affecting everything from personal use of corporate resources, to distribution of e-mail jokes, to use of racially-sensitive or politically-correct language and even to careless stewardship of network and e-mail quotas. In every case listed—and many others—e-Discovery technologies become the means for periodic samplings and ongoing assessments of data stored, and become foundational when related crises arise and a need for deep investigation or legal defense arise.

Reacting to an e-Discovery crisis can be as simple as finding a lost e-mail, or as complex as finding every mention of a certain keyword in all documents on all daily, weekly, monthly and yearly backup tapes for all file and e-mail servers globally for the past seven years. Given the nature of distributed computing, the obstinate and often elusory retention of documents by end users, the broad span of technologies entailed, the massive volumes of data involved and the urgency with which e-Discovery demands often present themselves, organizations need to perform due diligence in managing the risks entailed and to ensure organizational readiness.

Establishing an e-Discovery Plan

Having a documented e-Discovery plan with all necessary technology, processes and contact information is a must. Ideally this service should be included as part of an overall Business Continuity Plan—if one exists—but as a minimum an e-Discovery plan should consist of a set of procedures to search for, discover and recover e-mail and file content for a given term—typically several years—should the need arise. Creation of the e-Discovery plan should involve representatives from IT Management along with corporate legal counsel. Often the process of establishing an e-Discovery plan leads organizations to evaluate document retention and destruction policies; obviously reducing the overall volume of data has a direct relationship on the ability to search this corpus. With e-mail representing approximately 83% of all corporate communication todayⁱⁱ, and in light of the distributed and volatile nature of e-mail, e-mail e-Discovery preparedness is generally a good place to start. If your e-Discovery plan necessitates readiness for possible legal defense having a watertight e-Discovery plan for e-mail is a must.

If you are still not convinced that you need an e-Discovery plan, consider the following example scenario.



Disclaimer: All companies and individuals named, together with the events, are completely fictional. Any resemblance to any person living or dead is purely coincidental. No similarity to any person either living or dead is intended or should be inferred.

Example Scenario

Joe is the network administrator for ACME Software, a small supplier of medical supplies. As a vendor to both governmental agencies and to a large publicly-traded pharmaceutical company, ACME Software must comply with several industry regulations concerning the confidentiality of patient records. Field trials of some of ACME Software's products are frequently discussed via e-mail, though specific mention of patient records for the approximately 90 patients involved must remain confidential.

One of the patients in the field trials—Sarah—has recently brought suit against ACME Software claiming her personal records were shared with a third party over the past 5 years and is suing for damages. Sarah's legal counsel has requested through the courts that ACME Software produce all e-mails and documents in their possession which mention Sarah. The deadline for production of this evidence is 90 days from original court order. The court has defined five categories of electronic data which must be assessed, namelyⁱⁱⁱ:

- *Active, online data, including hard drives*
- *Near-line data, including optical disks*
- *Offline storage/archives (optical disk or magnetic tape media)*
- *Backup tapes*
- *Erased, fragmented or damaged data*

Microsoft Exchange e-Discovery with Quest Recovery Manager for Exchange

In this particular case the e-Discovery costs associated with the first two data types—considered 'accessible' by the court, are to be borne exclusively by ACME Software. The costs for e-Discovery of the last three types of data—considered 'inaccessible data' by the court, will be tabled for consideration of cost-sharing between the two parties.

In defense of their claim, ACME Software has decided to comply with the request and find all documents containing Sarah's name. Joe is tasked with leading the investigation, working closely with a legal technology consultant from ABC LLC, who has been retained as ACME's legal counsel. For the purposes of this example, ACME Software has chosen to comply with all five components, though in any large-scale real scenario the first two are generally begun prior to the latter three. Here is the process that Joe must go through to produce the documents required for all five scenarios:

Initial Preparatory Phase

1. Identify all servers from which he must retrieve data:
 - i.e., ACMEFILE01, ACMEFILE2, ACMEMAIL1, ACMEDC1, etc. where ACMEFILE01 and ACMEFILE02 are file servers, ACMEMAIL1 is an Exchange Server, and ACMEDC1 is a domain controller and global catalog server.
2. Identify, locate, and retrieve all backup tapes for these servers spanning the last five years. For each server he has a maximum of:
 - i.e., 7 daily tapes + 5 weekly tapes + 12 monthly tapes + 4 yearly tapes = 28 tapes per server
 - Specifics will depend on whether tapes are zeroed out as part of tape migration, etc.
3. Identify all backup software that has been used on these servers over the past five years. Joe needs to identify for each tape:
 - Software media
 - License keys
4. Identify all domain controller versions and service packs that have been used by ACMEDC1 and its predecessors in the past five years
 - Windows NT 4.0, Windows NT 4.0 Service Pack 3.0, Windows 2000 Server, Windows 2000 Advanced Server, Windows 2000 SP2, Windows 2000 SP4
5. Identify all Exchange Server versions and all service packs that have been used on ACMEMAIL1 and its predecessors over the past five years
 - Exchange 5.5 Server, Exchange 5.5 SP3, Exchange 2000 Server, Exchange 2000 Server SP1, Exchange 2000 Server SP2, Exchange 2000 Server SP3, Exchange Server 2003
6. Identify all other computers from which he must retrieve data:
 - i.e., LAPTOP1, LAPTOP3, LAPTOP4, LAPTOP5, DESKTOP1, DESKTOP2, SPAREPC1, etc.

e-Discovery Phase—File System

1. Systematically search every server that is currently in production (ACMEFILE01 and ACMEFILE02) for:
 - file containing <Sarah's name>
 - filename containing <Sarah's name>



Note: This can be achieved using Microsoft native tools i.e., Windows Explorer "Search" facility

2. Repeat Step 1 for every backup tape in existence. Either use built-in search capabilities in backup software (where it exists) or recover each server from backup step-by-step and then search the content restored.
3. Systematically search all production Exchange Server mailboxes for:
 - Messages containing <Sarah's name> in the message body
 - Messages containing <Sarah's name> in the message subject
 - Messages containing <Sarah's name> in the attachment name
 - Messages containing <Sarah's name> in the attachment body



Native Microsoft tools (i.e., Exchange Mailbox Merge Wizard (ExMerge)) permit some of this; namely searches for keywords in message subject or in attachment name. Yet the vast majority of critical data is in the message body and especially in attachment bodies. These can NOT be searched using native Microsoft tools. A third party solution is required.

****CHECK LATEST ExMerge FEATURESET****

4. Repeat Step 3 for every backup tape in existence.
5. Systematically search the content from each personal folder (.PST) file in the environment.



The only native Microsoft mechanism for achieving this would be to set up a Messaging Application Programming Interface (MAPI) profile for each .PST using Microsoft Outlook and then using Outlook search capabilities to locate messages of interest.

6. If .PSTs are stored on network shares, then find all instances of .PSTs and repeat step 5 for each .PST. If a solution such as Quest Archive Manager for Exchange (<http://wm.quest.com/products/ArchiveManagerExchange/>) is in use, it can be used to identify all active .PSTs, control .PST usage, and pull all .PST content into a central location to simplify overall storage management and facilitate e-Discovery from a central location.
7. Identify any alternate storage locations for e-mail (i.e., Blackberry, iPAQ) and search any relevant message stores for e-mail relating to Sarah.
8. Perform de-duplication of all e-mail content discovered, preserving only unique message instances.

9. Maintain all discovered content and related search queries in a secure location.
10. Present all resultant e-mails in .PST format for review by ACME legal team.
11. Prepare select subset of resultant e-mails for review of opposing party in the format instructed by the courts, such as .PST format, TIFF, or even hard copy printouts.

Effort

It is important to note that as the size of the environment increases (file servers, workstations, mailboxes, public folders, etc.) that the cost and effort will increase in a linear fashion at the very least.

So hopefully you have seen that e-Discovery can be far from trivial, especially when set against the backdrop of a formal investigation. The ramifications of ignoring e-Discovery can be equally complex. You should make every effort to add an e-Discovery plan to your list of projects for the current fiscal year rather than waiting until a subpoena arrives.

e-Discovery Challenges

As you have seen in our example, numerous challenges come with e-Discovery.

Compliance Regimes

In the wake of corporate scandals and the resulting legal regulations (such as HIPAA and The Sarbanes-Oxley Act of 2002), organizations have gotten the message that they need to police their messaging systems and take a pro-active approach to compliance. The list of regulations is likely to increase and organizations need to take a pro-active approach to reducing risks. The financial penalties, and even jail time, associated with non-compliance have raised the stakes and forced many companies to create e-Discovery plans and related compliance procedures.

Record Retention Policies

Organizations typically establish record retention and destruction policies that align with relevant compliance regimes and dovetail with their e-Discovery plan. Organizations with retention policies stating that after an e-mail has been read, it should be deleted or moved to a personal folder (.PST) files as soon as possible does not remove the organization's responsibility to produce that e-mail. The courts do not "believe that a records retention policy which is inconsistent with a party's obligations to a potential or actual adversary in litigation operates to excuse the party's failure to respond to discovery."^{iv}

Staggering Volumes of Data

As stated earlier, there is not an enterprise-wide forensic investigation in this day and age that does not necessitate inspection of e-mail. In actual fact, e-mail accounts for nearly half the electronic information requested in litigation.^v In 2004, e-mail usage grew a staggering 53% over the previous year. With organizations storing a hefty 14.7 MB of e-mail data per day per user^{vi}, an Exchange administrator conducting an e-Discovery search is looking for the proverbial needle in a haystack.



See Best Practice for Exchange Storage Management for more information at <http://wm.quest.com/questexchangestorageforediscovery>

Potentially Staggering Costs

Finding that needle—in even the most simple environment—is time-consuming and expensive, and typically organizations need to find that needle fast. Time is money in litigation. Legal fees, court fees, and penalties are all on the line when organizations are ordered to turnover evidence. “Bank of America, for example, was fined \$10 million [USD] in March 2004 when it failed to turn over e-mails to the SEC in a timely manner (currently interpreted as only 36 to 72 hours)”.^{vii} In the final settlement Bank of America agreed to pay a total of \$375 million, consisting of \$250 million in disgorgement and \$125 million in penalties.^{viii} That’s not a lot of time to search through millions of e-mails, especially if you’re caught without a plan of action.

Technical Challenges

Technical challenges abound in e-Discovery. Let’s take e-Discovery in an Exchange environment as an example:

- E-mail servers are often distributed, and .PSTs can be very hard to locate, so simply getting to the data for inspection can be difficult.
- Exchange databases (comprised partly of .EDB & .STM files) are based on proprietary Microsoft technologies and cannot be searched or opened by any native Microsoft technologies without first performing a MAPI-based logon to every mailbox, which is extremely time and resource intensive.
- Searching for content on backup media requires first building a recovery environment—which can consist of one or more servers depending on the scenario; this alone could eat up your allotted time for e-Discovery.
- Average success rates in the industry for Exchange data recovery are surprisingly low. Only 70% of companies have a tape recovery success rate greater than 80%.^{ix} This poses risk and challenges in ensuring that e-Discovery efforts yield the results required to achieve a watertight defense.

Options for e-Discovery

Whether determining a plan of action for e-Discovery or actually engaging in an investigation, there are four options organizations need to consider.

In-house Investigations

Depending on the type of investigation anticipated organizations can perform e-Discovery in-house. This is especially suitable for human resources investigations and periodic data samplings to assess implementation of compliance recommendations or policies. In-house investigations generally necessitate a cross-platform team with representatives of corporate IT and corporate law under the direction of a corporate security officer. Enterprises wishing to handle investigations internally will require e-Discovery software that supports e-mail based discovery operations, as an absolute minimum.

Legal Technology Consultants

To assist companies discover and process the massive amounts of data entailed and the short turnaround time required for legal purposes, a new brand of e-Discovery specialists has emerged, generally under the umbrella of multi-discipline legal technology consulting teams. These teams have the technical expertise and software toolkit to manage large-scale forensic investigations. These firms also provide the added benefit during legal suits as they can testify to the e-Discovery procedures used. The court may insist all parties correct any technical problems arising in the electronic document production process, to explain any evidence containing questionable or missing data, re-format data as required by the responding party, judges, juries, and agreed upon by both parties^x, as well as resolve other technical file related issues.^{xi}

Outsourced Data Recovery & Digital Archival Clearinghouses

Fuelled by the staggering growth of e-mail combined with the ever-increasing reach of compliance regimes, numerous outsourced data recovery clearinghouses have sprung up over the past two years. In many cases these companies provide simple tape-to-.PST recovery, either directly to enterprises or to law firms handling investigations on the behalf of their clients.

Several of the larger data recovery clearinghouses also provide outsourced digital archival solutions—in essence circumventing part of the requirement for data recovery by attempting to capture critical corporate records into massive secure clean-rooms from which they can be inspected should the need for legal review be required.

Law Enforcement & Data Forensics

Finally, should the need arise for a criminal investigation, law enforcement organizations at all levels employ data forensics experts who use specialized tools to discover purposely hidden or destroyed data under any variety of scenarios affecting file servers, personal computers and laptops, or e-mail systems.

E-DISCOVERY AND MICROSOFT EXCHANGE

We have already pointed out that every enterprise e-Discovery investigation today involves e-mail, and with Microsoft Exchange holding an impressive 31% share of the corporate messaging software market (74% of the corporate market use Microsoft Outlook client)^{xii}, e-Discovery solutions for Microsoft Exchange environments sit at the core of most e-Discovery toolkits. We will now turn our attention to selection of a tool for Exchange-based e-Discovery.

We will begin our discussion by reviewing what capabilities are available in native Microsoft technologies.

Exchange 5.5 and Exchange 2000 Native Tools

In Exchange 5.5 and Exchange 2000 native tools, e-Discovery hinges on the concept of recovery. Organizations typically maintain a "spare" Exchange recovery server in their production environment to be used as a target location for recovery operations. Administrators can mount an extra copy of the production database on the spare server and start retrieving items from the store using Outlook or ExMerge. Administrators can then store extracted items to a .PST file or restore them back into production mailboxes. With Exchange 5.5 and earlier versions of Exchange, the spare server can be any server (member server or domain controller) in the same domain as the original server being recovered. However, the recovery server must have a different name from the server being recovered. Administrators configure this recovery server by installing it within the same organization and using the same site naming conventions and hierarchy as the original server (but a different server name), but they don't join this server to the production organization.

With Exchange 2000, administrators need to deploy a separate Active Directory forest for recovery operations as Exchange depends completely on the Active Directory for directory services. A spare server needs to be installed in the forest with the same characteristics as the production environment. Administrators can then perform restore operations in the forest, using tools such as Mbconn and ExMerge to bring mailbox data back to user accounts in the production forest. Building such an infrastructure typically requires about two hours of setup time prior to the restore operation. Administrators have to rebuild the environment every time they change an Exchange organization, especially when they are providing restore services to various customers.

Exchange 2003 and Recovery Storage Groups

Exchange 2003 introduced a new feature called the Recovery Storage Group (RSG) for mailbox recovery. Administrators simply create a new type of storage group on an Exchange server in production and restore online backup sets to it. The database copy running in the RSG is logically isolated from the rest of the Exchange organization. Clients cannot log on to it and mail cannot be delivered to it. Administrators can safely extract messages from it using a new version of the ExMerge utility. Creating an RSG takes just a few mouse clicks in Exchange System Administrator and a total setup time of about two minutes, which is a big improvement from previous versions of Exchange. However, the most important limitation of using the RSG is that a copy of the database can only be mounted on a server in the same administrative group. Also, the RSG cannot be used to recover items stored in public folders.

For detailed information about the recovery server and RSG, please see Using Exchange Server 2003 Recovery Storage Groups (<http://www.microsoft.com/technet/prodtechnol/exchange/guides/UseE2k3RecStorGrps/1b10818d-c547-4195-92e8-2d1d4dcb2086.mspx>).

Solution Requirements for e-Discovery

In light of our review of native Microsoft tools, we can assemble a list of requirements for a comprehensive solution for e-Discovery. Regardless of why an organization needs to go through an e-Discovery exercise, finding a solution that meets the following requirements will reduce the financial and resource burden involved. The solution must be able to:

- Support multiple parallel e-Discovery operations to process backups of multiple servers and/or stores
- Support multiple backups for each server
- Accurately recover all message components including header, body, and attachments
- Search via keyword in all message components including header, body, and inside attachments
- Provide output that can be consumed by legal case management software or outsourcing workflow processes, including output to .PST
- Provide output to online mailboxes and public folders
- Provide output suitable for review by one or more teams
- Provide log of progress and errors
- Provide automation capabilities to facilitate large-scale e-Discovery
- Provide support for a wide range of backup vendors
- Provide support for Exchange 5.5, Exchange 2000 and Exchange 2003 Server
- Provide support for Exchange archival solutions

INTRODUCTION TO QUEST RECOVERY MANAGER FOR EXCHANGE

An ideal solution for e-Discovery in all of the scenarios that we have discussed, Quest Recovery Manager for Exchange, offers a comprehensive solution for e-Discovery and subsequent recovery of messages and mailboxes from backup tapes or offline Exchange databases. Recovery Manager works seamlessly across multiple versions of Exchange. It can use any computer that is running Windows XP or Windows 2000/2003 and has access to either an Exchange offline database or a backup copy of a database to search and retrieve existing mailboxes or selected messages, based on multiple criteria set by the user. Recovery Manager supports e-Discovery and restoration of data at information store-, mailbox-, and message-level including:

- Messages
- Attachments
- Notes
- Tasks
- Contacts
- Appointments
- Journal entries
- Public folders

Using the search feature, administrators can select items for retrieval based on criteria such as:

- A word in the subject or body of a message
- A word in the body of an attachment
- Sender of a message
- Recipient of a message
- A given date range for sent or received messages

Once selected, administrators can preview messages directly from the Recovery Manager interface as if they were in a Microsoft Outlook session connected to Exchange, as shown in the figure below.

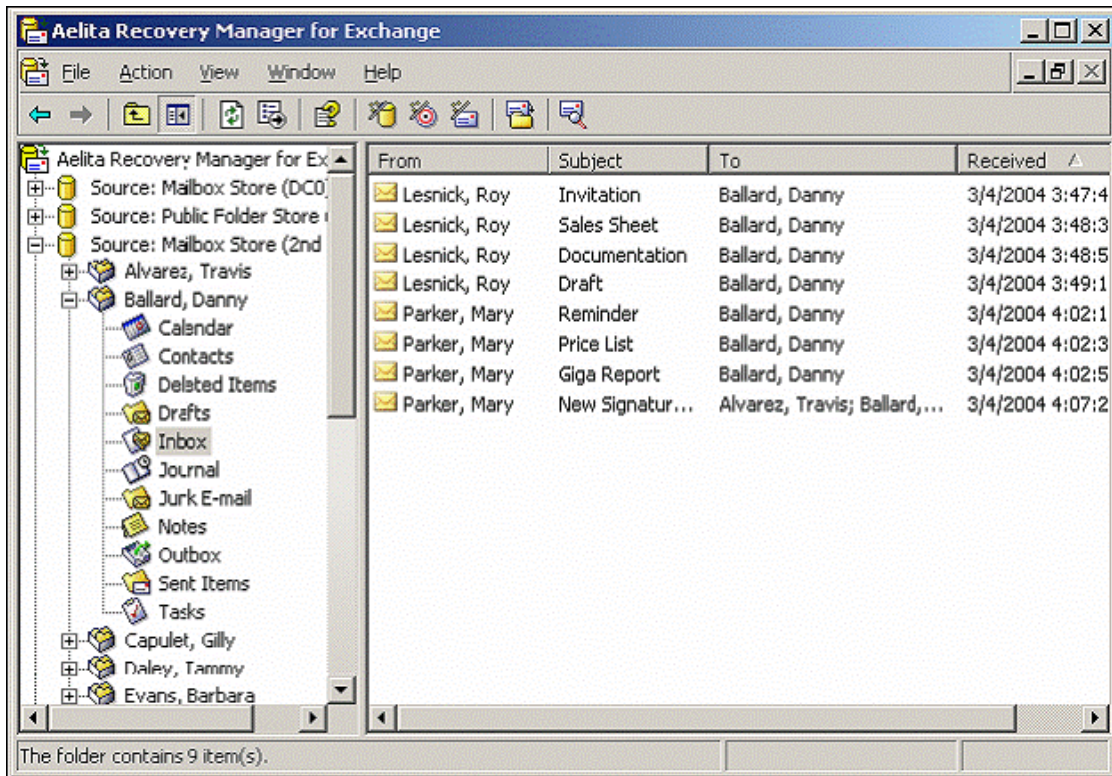


Figure 1: Previewing items of a mailbox directly from an .EDB file

Finally, administrators can restore selected items, either individual items or entire folders, to a .PST file or, by connecting to a production Exchange server, deposit restored items to a designated mailbox or folder directly.

Installation

As stated earlier, administrators can install Recovery Manager on any computer running Windows XP, Windows 2000 SP3 or later, and the Windows Server 2003 operating system. There is no requirement to have Recovery Manager running on an Exchange server or running on a system that is a member of a Windows 2000/2003 Active Directory forest. This flexibility greatly helps to reduce the preparation time needed for the restore operation. Prior to the installation, Recovery Manager only requires deploying Microsoft Outlook 2000/2003 on the computer and copying the following DLLs from an existing Exchange server:

- For Exchange 5.5: ESE.DLL—EXCHMEM.DLL
- For Exchange 2000/2003: ESE.DLL—EXCHMEM.DLL—EXOSAL.DLL—JCB.DLL

It is preferable that the DLLs are copied from the same Exchange server where the databases have been backed up, and mandatory that .DLLs match the Exchange Server version and service pack if transaction LogFiles will be rolled forward as part of bringing an Exchange database to a consistent state.

Outlook components allow Recovery Manager to create a MAPI session and display items of a given mailbox from the Recovery Manager interface. The other DLLs allow Recovery Manager to access offline Exchange databases.

Defining the Source for e-Discovery

Recovery Manager performs message-level restores from regular Exchange backups or offline .EDB files. .STM files are also supported. In the case of OWA-only deployments, it should be noted that while .STM files contain most of the binary data, .EDB files are still required as they contain all the associated pointers. A restore can be done from any type of backup—full, incremental, or differential, and with or without replaying database transaction logfiles. Recovery Manager also supports Volume Shadow Copy Service (VSS) Snapshot backups, Microsoft Tape Format (MTF)-compliant backups created by native tools such as Windows NT Backup, as well as most major third-party tools including:

VENDOR	SOFTWARE	VERSION
CommVault Systems	CommVault Galaxy	5.0
Computer Associates	BrightStor ARCserve	2000
Computer Associates	BrightStor ARCserve Backup	9.0, 11.0
Computer Associates	BrightStor ARCServeIT	6.6
Computer Associates	BrightStor Enterprise Backup	10.5
HP	OpenView Storage Data Protector	A.05.10
IBM	Tivoli Storage Manager	5.1 or later
Legato	Networker	6.0.1, 6.0.2, 7.0, 7.1
Microsoft	Windows Backup	Windows NT, Windows 2000, Windows Server 2003
Veritas	NetBackup DataCenter/Business Server	4.5 (MP6)
Veritas	NetBackup Server/Enterprise Server	5.0GA
Veritas	Backup Exec for Windows Servers	7.3, 8.6, 9.0, 9.1



This list is only current as of the date of publication. For an updated list, please refer to the Vendor List document at <http://wm.quest.com/products/recoverymanagerexchange/documentation.asp>.

Microsoft Exchange e-Discovery with Quest Recovery Manager for Exchange

.EDBs are accompanied by .STM files if the environment is running Exchange 2000/2003.

In the Recovery Manager interface, administrators simply register the different sources for the restore. For offline databases, .EDB and .STM files can be stored locally or on a network share accessible by the Recovery Manager computer.

When registering a source using backup (.BKF) files, administrators may specify multiple sources if you select differential or incremental backups. Recovery Manager will then extract databases and log files from the .BKF files. For Exchange 2000, since each storage group includes a set of log files that applies to all information stores within the storage group, administrators must specify the name of the storage group and information store when operating on those types of backups.

After the files are extracted, Recovery Manager replays the transaction log files to write all pending transactions to the database file. This operation is required in order to ensure that the databases are in a consistent state before commencing e-Discovery investigations. Otherwise, there is a chance administrators may miss some items that were in the transaction log files but not committed to the database at the time of the backup.

It is important to note that Recovery Manager is able to put EDB into consistent state while .STM or some logs are corrupted. This may be important if you are searching data archived a long time ago.

e-Discovery Options

Recovery Manager has a powerful search engine that can be used to search and browse items in an offline database. Administrators can perform a search against the entire database or in specified locations within the database. The engine offers a wide range of criteria based on message content, recipient, sender, and dates as shown in the figure below.

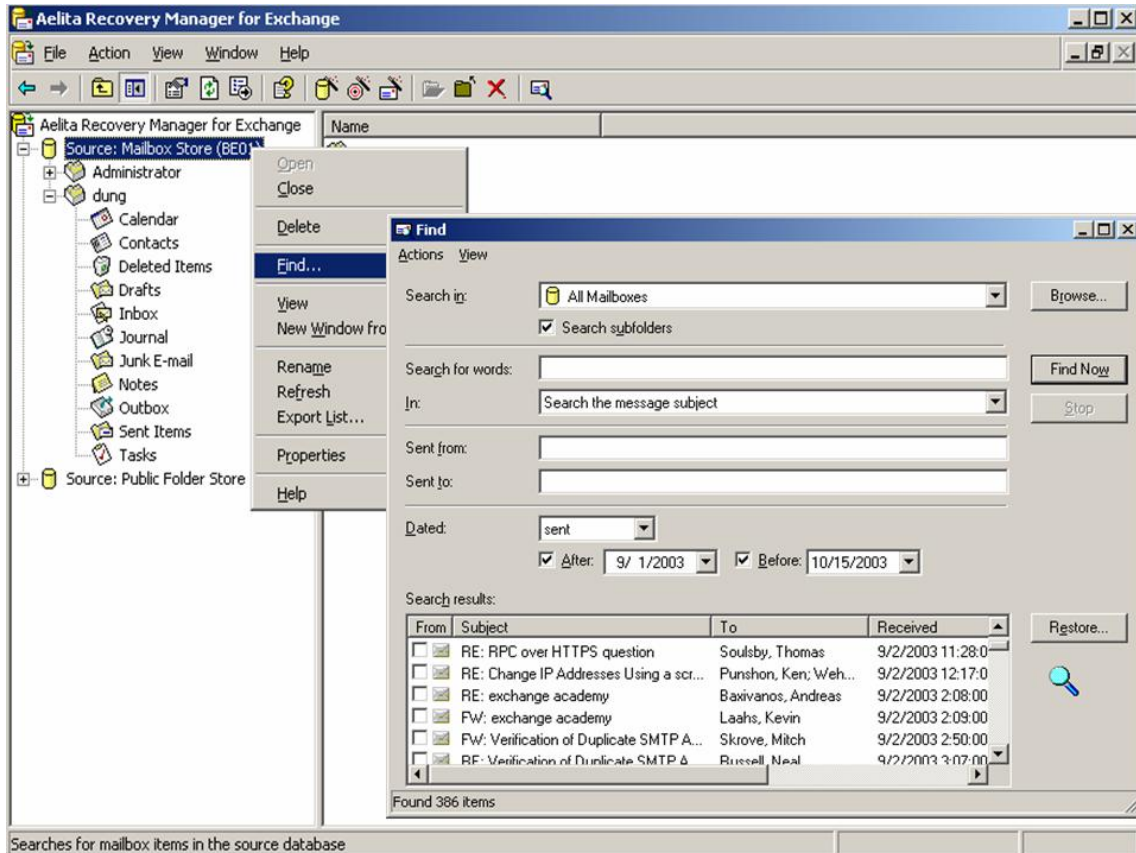


Figure 2: Search criteria using date range

Restoring Discovered Items

Once items of interest for e-Discovery or other recovery purposes are discovered in the database and selected for restore or .PST export, Recovery Manager retrieves them from the database and writes them to the specified mailbox, public folder or .PST file. Administrators can also connect directly to a production mailbox and restore items to it. Recovery Manager allows administrators to create a MAPI session to an Exchange server from its interface. Another possibility is to store retrieved items into a .PST file and send it to the appropriate legal teams or other investigators for review and further processing. The figure below shows some examples of targets for restore.

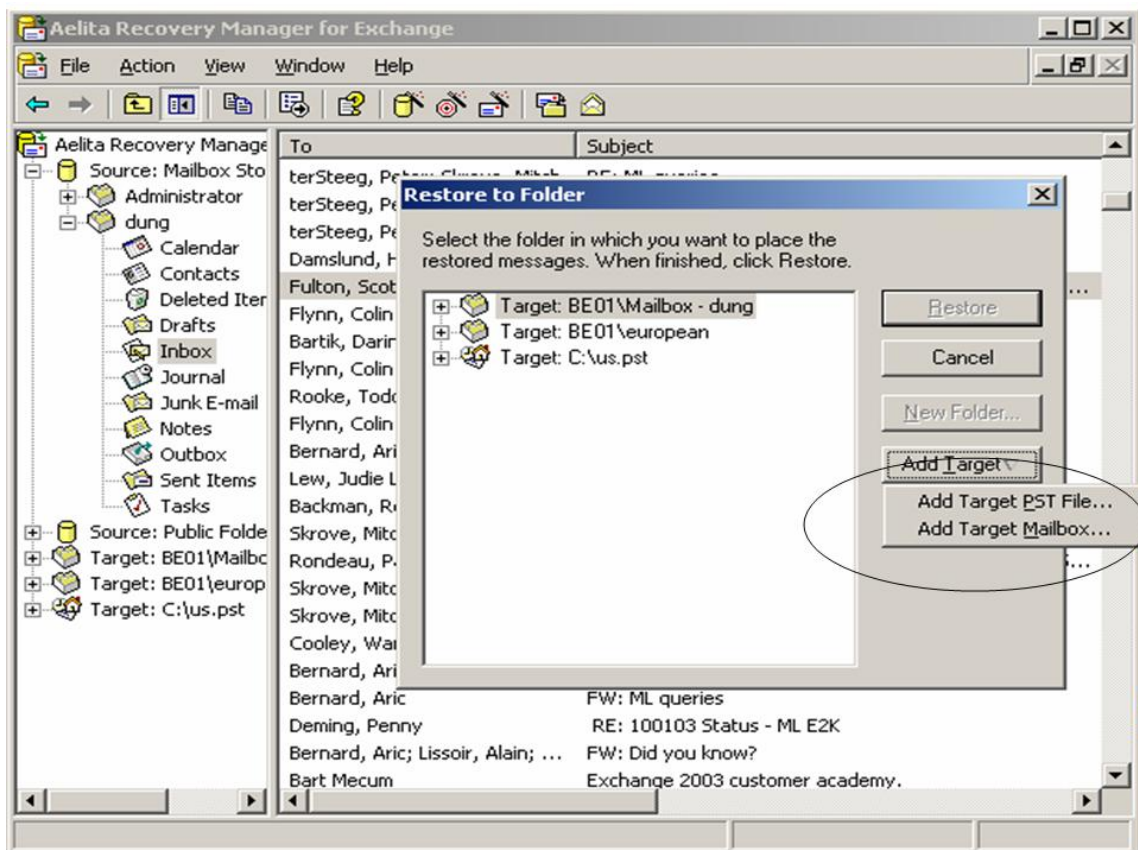


Figure 3: Adding a target for items restore

A NOTE ABOUT ARCHIVAL

It should become clear in the reading of this document that implementation of an archival solution can, at least from the point of implementation, greatly simplify e-Discovery of content by providing a central location from which to manage and analyze content. Whether this involves storage management archival solutions such as Quest Archive Manager for Exchange, or compliance management archival solutions, the centralized nature of associated storage combined with well-defined policies and procedures can minimize the overall impact of e-Discovery when the time comes. Depending on the scope of archive coverage, the date of cutover to the archive and whether a historical backup-to-archive migration was performed as part of or subsequent to the implementation will impact how much e-Discovery of backup content is required.

SUMMARY

Quest Recovery Manager for Exchange is an ideal e-Discovery solution for Exchange environments and should be part of any e-Discovery toolkit. For enterprises engaged in in-house investigations, Recovery Manager eliminates the need for a dedicated Exchange recovery server or the need to invest in message-level (“brick-level”) restore, while facilitating rapid and powerful e-Discovery of data spanning numerous backup formats created over the past years. Legal technology consultants will find Recovery Manager’s underlying technology and ability to perform keyword searches within attachment content—where most content of interest is kept—unique in the industry. Outsourced data recovery clearinghouses will realize substantial savings from replacing costly and labor-intensive Exchange recovery environments and virtual machines with powerful recovery capabilities from a software vendor with a proven track record of customer responsiveness and vendor partnership. Finally, law enforcement and data forensics specialists will find in Recovery Manager the ideal solution for investigation of offline Exchange databases circumventing a need to gain expertise in Microsoft Exchange and facilitating rapid and powerful search capabilities.

Recovery Manager is an expert-level e-Discovery solution focused on providing sophisticated Exchange discovery and recovery capabilities that are compelling to both the enterprise and to the e-Discovery community at large.

FOR MORE INFORMATION

About Dung Hoang-Khac

Dung Hoang Khac, is member of the Applied Microsoft Technologies Group of HP Services Corporate Worldwide practice. Dung provides architectural design, implementation and technical support to HP Services customers in the areas of Enterprise Windows and Messaging and supports other HP consultants in similar efforts. Dung is instrumental in designing and delivering the Exchange Server 2003 and Exchange 2000 Academies; an intensive 5-day combination of lecture and lab exercises on how to design and implement the new technology. These Academies are delivered to both HP consultants and HP's customers in North America, Europe and Asia Pacific. In addition to this white paper, Dung co-authored various Windows and Exchange Server 2003 migration publications, and is a contributor to the Exchange Administrator newsletter. Dung recently relocated from Europe to North America and is now based in Seattle, WA.



About David Sengupta

David Sengupta is a Product Manager in the Windows Management group at Quest Software, where he focuses on Quest's Exchange management solutions, notably Quest® MessageStats™ and future Exchange products. Microsoft has for six consecutive years granted David the "Most Valuable Professional (MVP)" Award in the Exchange Server category for significant technical contributions to the international Exchange community. David has worked with Exchange since the Exchange 4.0 beta, worked on various Joint Development Partner (JDP) initiatives and Partner Advisory Councils (PACs) with the Exchange Product Group, and played a lead role in introducing hosting Exchange 2000 to the ASP marketplace. He has contributed to various Exchange and Windows books, magazines and whitepapers from a number of publishers, and frequently represents Microsoft on staff at Ask the Experts, Microsoft Experts Area and Peer Talk in conferences such as MEC or TechEd. He also frequently speaks on Exchange management. David recently led development of a national training lab on Windows Server 2003 and XML Web Services for Microsoft and Intel Canada. David has an M.T.S. from Tyndale Seminary, Canada, and a B.Sc. from University of Ottawa, Canada, along with MCSE (Messaging) and CCA certifications.



CALL TO ACTION

For more information on Quest Recovery Manager for Exchange go to:
<http://wm.quest.com/products/recoverymanagerexchange/>

For more information on Quest Software Exchange Solutions go to:
wm.quest.com/products/Exchange/.

For more information on HP Storage Solutions for Exchange 2003 go to
www.hp.com/solutions/microsoft/exchange/storage

NOTES

- ⁱ [Electronic Discovery](http://www.fjc.gov/public/pdf.nsf/lookup/ElecDi07.pdf/$file/ElecDi07.pdf), presented at the National Workshop for U.S. Magistrate Judges, June 12, 2002:
[http://www.fjc.gov/public/pdf.nsf/lookup/ElecDi07.pdf/\\$file/ElecDi07.pdf](http://www.fjc.gov/public/pdf.nsf/lookup/ElecDi07.pdf/$file/ElecDi07.pdf)
- ⁱⁱ January 2005 The Radicati Group, Inc, "Radicati Market Stats,
<http://www.radicati.com/cgi-local/news.pl>
- ⁱⁱⁱ Zublake I: Court Orders Production of Deleted E-mail from Backup Tapes and Articulates Cost-shifting Analysis; December 15, 2004 Posted By PGE; Zubulake v. UBS Warburg LLC, 217 F.R.D. 309 (S.D.N.Y. 2003) ("Zubulake I"); <http://www.ediscoverylaw.com/case-summaries-43-zublake-i-court-orders-production-of-deleted-e-mail-from-backup-tapes-and-articulates-costshifting-analysis.html>
- ^{iv} Court Orders Production of Backup Tapes and Provides for Hard Drive Access Based on Failure to Preserve Evidence, December 15, 2004 Posted By PGE, Renda Marine, Inc. v. United States, 58 Fed.Cl. 57 (2003);
<http://www.ediscoverylaw.com/case-summaries-61-court-orders-production-of-backup-tapes-and-provides-for-hard-drive-access-based-on-failure-to-preserve-evidence.html>
- ^v [EDD Growth is Staggering; Experts: \\$500 million by year-end, \\$2 billion by '05](#), Albert Barsocchini, Law Technology News, August 23, 2003; pg 18
- ^{vi} July 2004 The Radicati Group, Inc., Messaging and Collaboration Corporate Survey, 2004-2005 – Executive Summary
- ^{vii} CIO Magazine; Jan 15, 2005; Message Therapy; by Ben Worthen;
<http://www.cio.com/archive/011505/compliance.html>
- ^{viii} Bank of America to pay monster fine in provisional settlement with SEC, SRI Media, 15 March 2005,
http://www.srimedia.com/artman/publish/article_780.shtml
- ^{ix} CIO Magazine; Jan 15, 2005; Message Therapy; by Ben Worthen;
<http://www.cio.com/archive/011505/compliance.html>
- ^x Court Directs Production of Electronic Material in Native Format, December 15, 2004 Posted By PGE; Jicarilla Apache Nation v. United States, 60 Fed.Cl. 413 (2004); <http://www.ediscoverylaw.com/case-summaries-84-court-directs-production-of-electronic-material-in-native-format.html>
- ^{xi} Court Orders Party to Correct Technical Problems with Electronic Production, Declines to Appoint Neutral Consultant; February 9, 2005 Posted By PGE; United States v. Merck-Medco Managed Care, L.L.C., 2005 WL 273030 (E.D.Pa. Feb. 2, 2005); <http://www.ediscoverylaw.com/case-summaries-84-court-directs-production-of-electronic-material-in-native-format.html>
- ^{xii} Microsoft Exchange and Outlook, Market Analysis, 2004 – 2008, March 2004, The Radicati Group, Inc.; <http://www.radicati.com/>