

MLROs.com

26th June 2009

**“Forensic Computing and
Technical Support for
Regulatory Investigations”**

- **PLT Overview & Project Types**
- **Forensic Computing**
 - Deleted Data
- **Deleting data**
- **Email and its many sources**
- **Conceptual searching**
 - Identifying code names
 - Don't know what to look for
- **Document review during an investigation**

- **Law Firms & General Counsel**
 - Litigation (Parts 31 & 35)
 - Regulatory & Compliance
 - Employment Disputes
 - Fraud Investigations
- **General Counsel**
 - ‘Disclosure Readiness’
 - Data Loss Prevention (DLP)
- **Accountants**
 - Insolvency & Asset Recovery
 - Fraud Investigations

- **Who did what and when?**
 - 'Data Theft'
 - Webmail & Instant Messenger
 - USB Media
 - Internet Access & Web History
 - Computer Access & Network Logs
 - Mobile Phones & Blackberries™

Forensic Computing

- **File Access**
 - Peak before an 'event'?
 - What files were accessed by whom?
- **Passwords**
 - 3 types – average
 - Weak & strong encryption
- **'Social Networks'**
 - Who emails whom?
- **Part 35 Expert Witness Reports**

- **Data isn't 'deleted' until it is overwritten**
 - Applies to system & User generated data
 - Data from the remainder of a partially overwritten, file is recoverable
- **Deleted data is often valuable evidence – Human Behaviour**
- **Data Wiping**

Saving a File

User 's
view

FILENAME.DOC

You choose a
filename for
your
document

Saving a File

User's
view

FILENAME.DOC

FAT

LINK

FILENAME.DOC

1

2

3

4

The File Allocation Table (FAT) is a map of where data is stored on the drive

Saving a File

User's
view

FILENAME.DOC

FAT

LINK

FILENAME.DOC

1

2

3

4

1							
		2					4
					3		

The file fragments are stored in various clusters on the hard drive of the computer

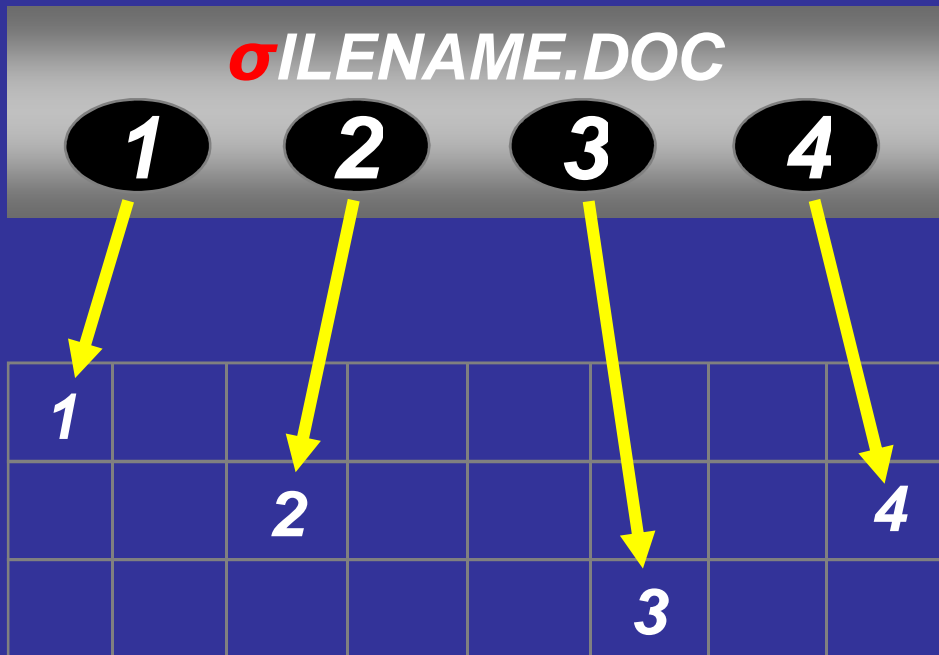
Deleting a File

User's view

DELETED

FAT

LINK



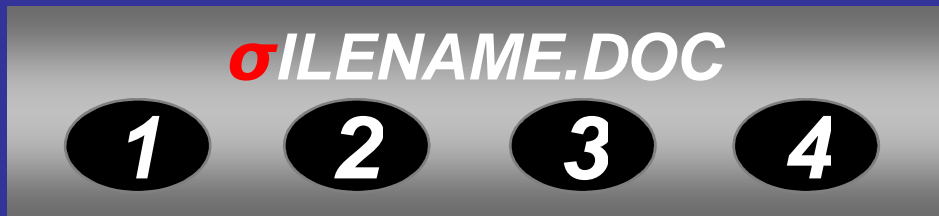
The first character of the filename is removed

Deleting a File

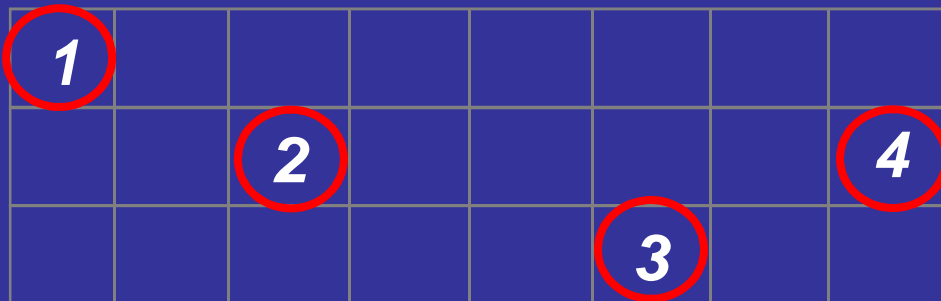
User's view

DELETED

FAT



This breaks the link between the filename and the data fragments



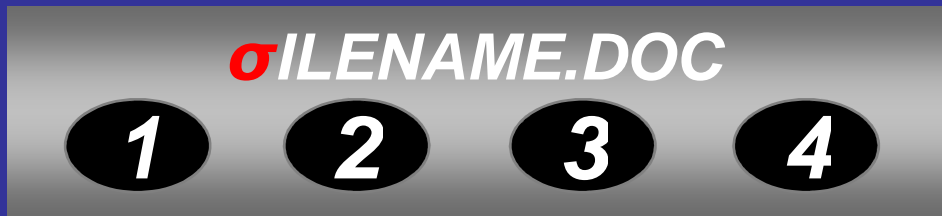
File fragments remain on the hard drive and can be forensically recovered

Data Wiping

User's
view

****DELETED****

FAT



1	0	1	0	1	0	1	0
1	0	1	0	1	0	1	0
1	0	1	0	1	0	1	0

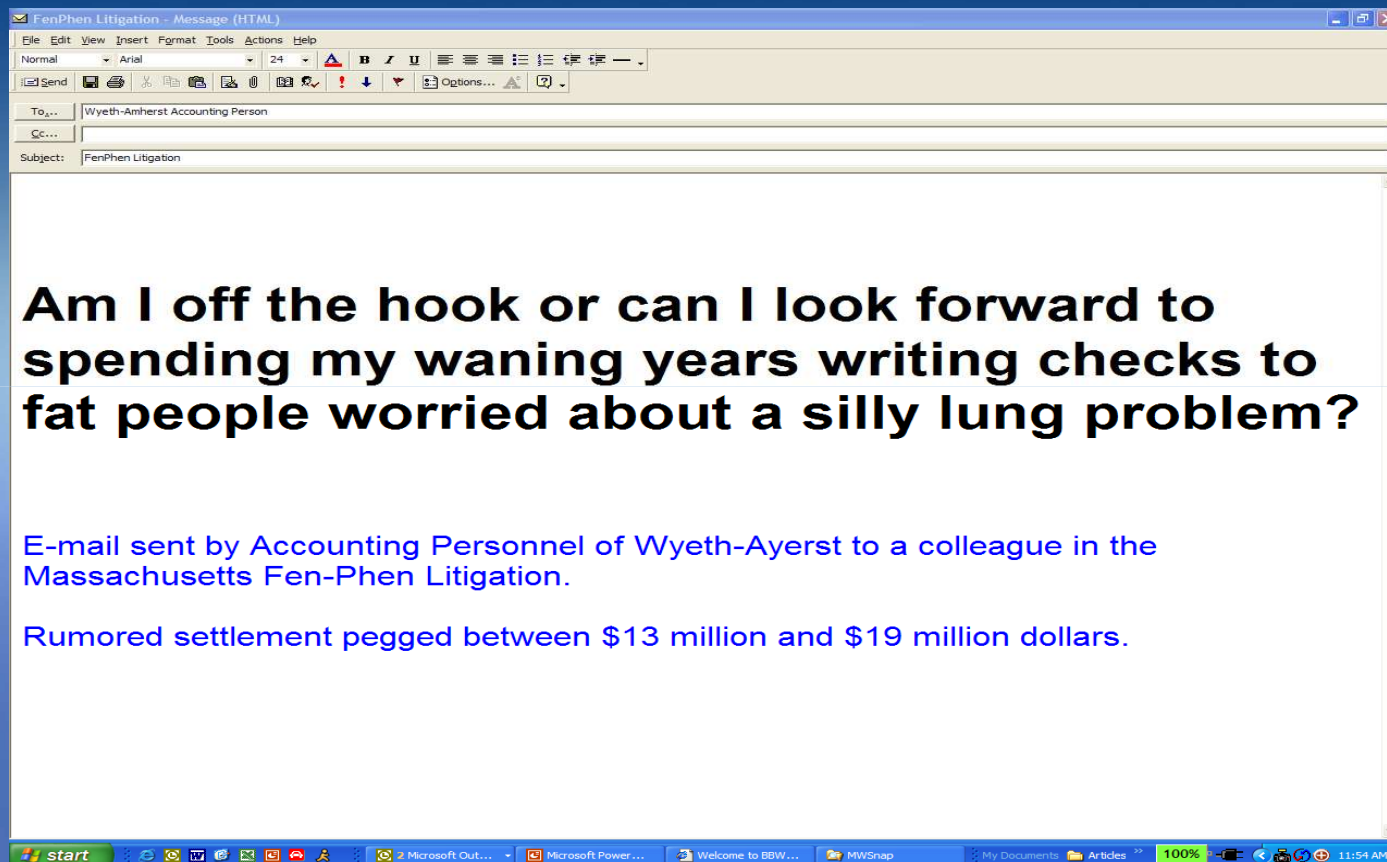
File fragments are
intentionally over-
written with 1s &
0s

Searching e-Documents

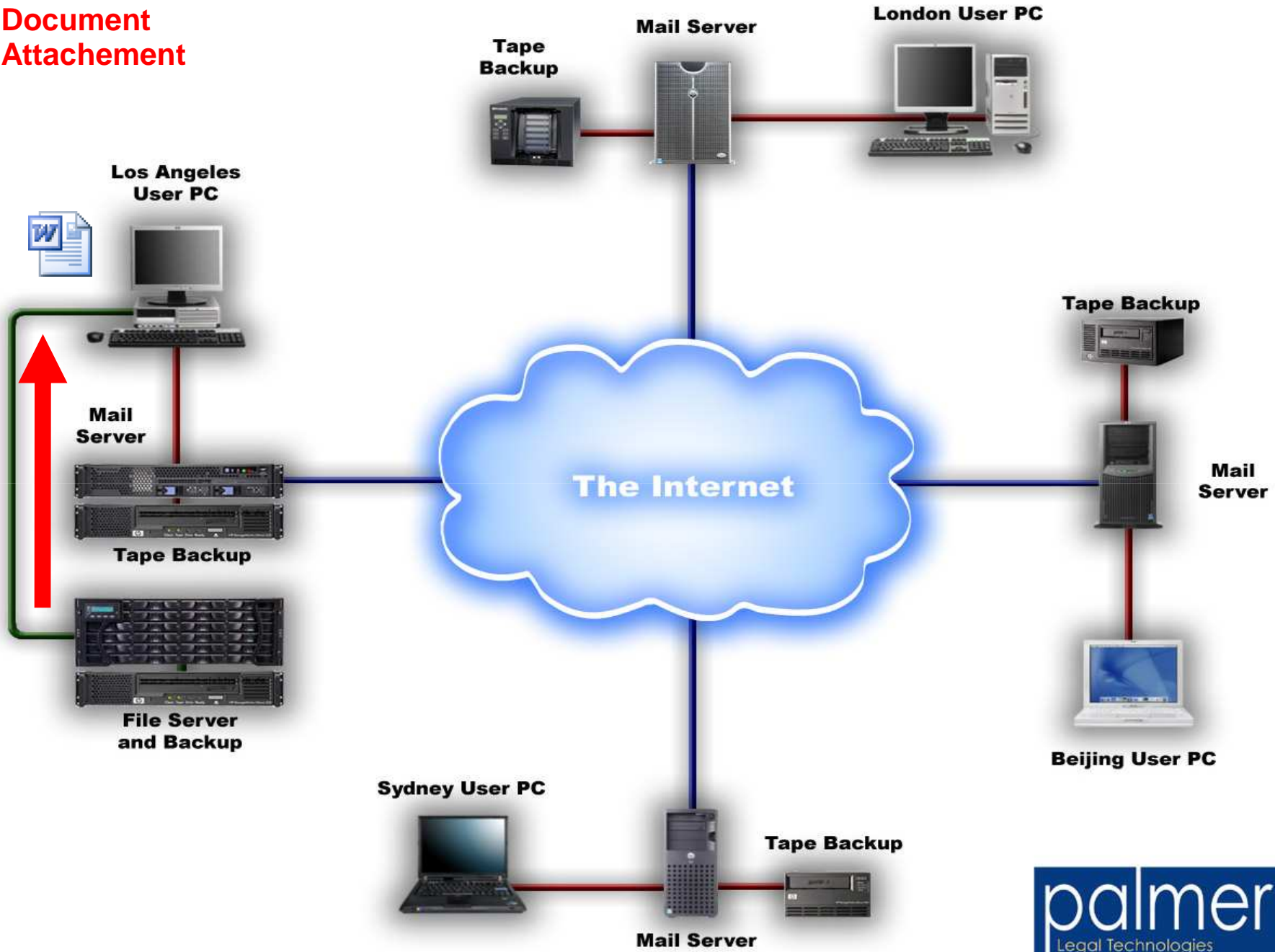
- **Key Words**
 - “Turkey”
 - Boolean Operators
- **Latent Semantic Indexing**
 - Relationship between characters
 - Language independent (incl. slang)
 - Concept - “*Large bird, Christmas, Thanksgiving, Edible (allegedly)*”
 - What about Goose ?? Relevant?
 - Code words
- **Document Review Platforms**
 - More Like This!

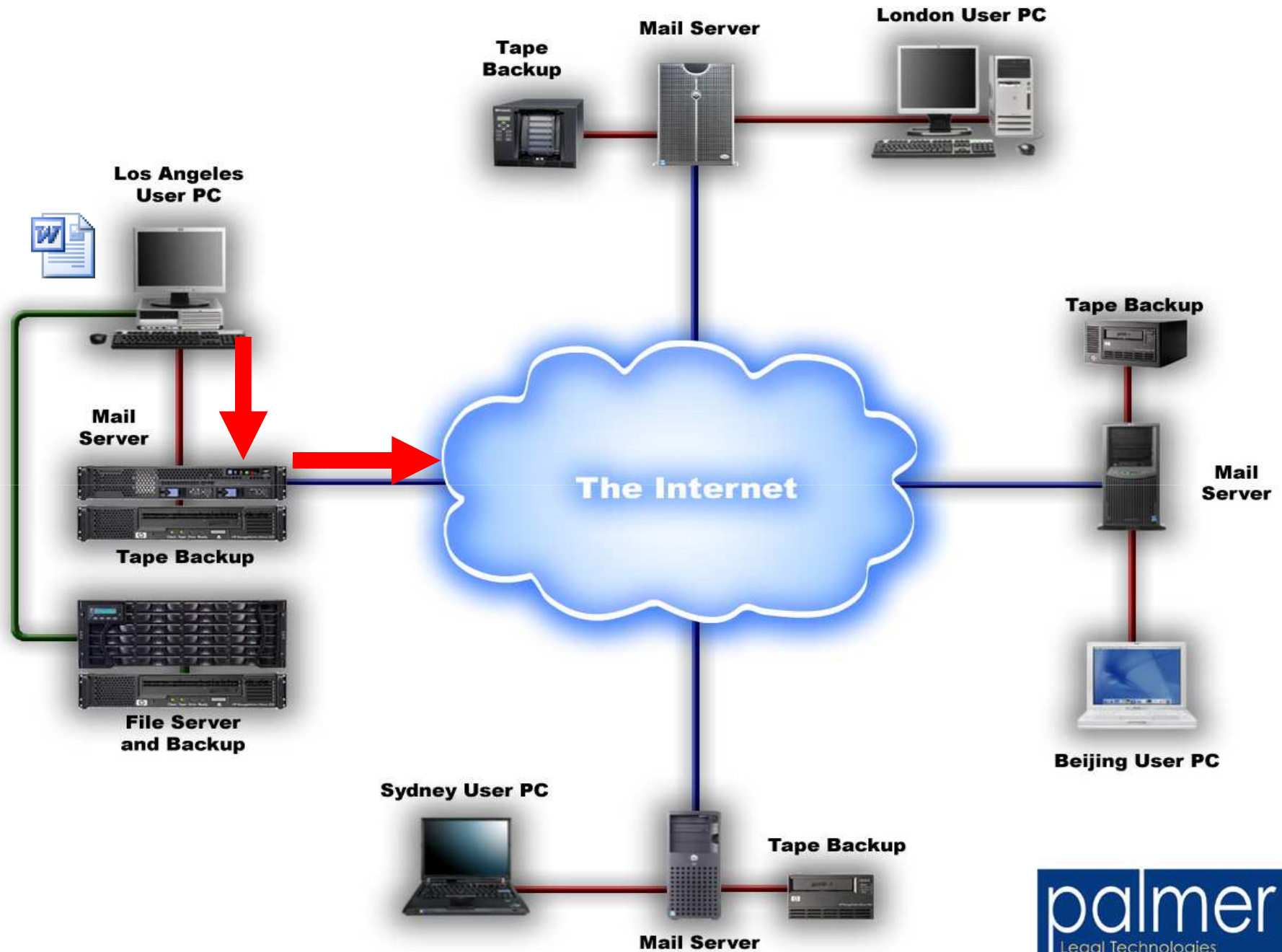
Dealing with the Volume

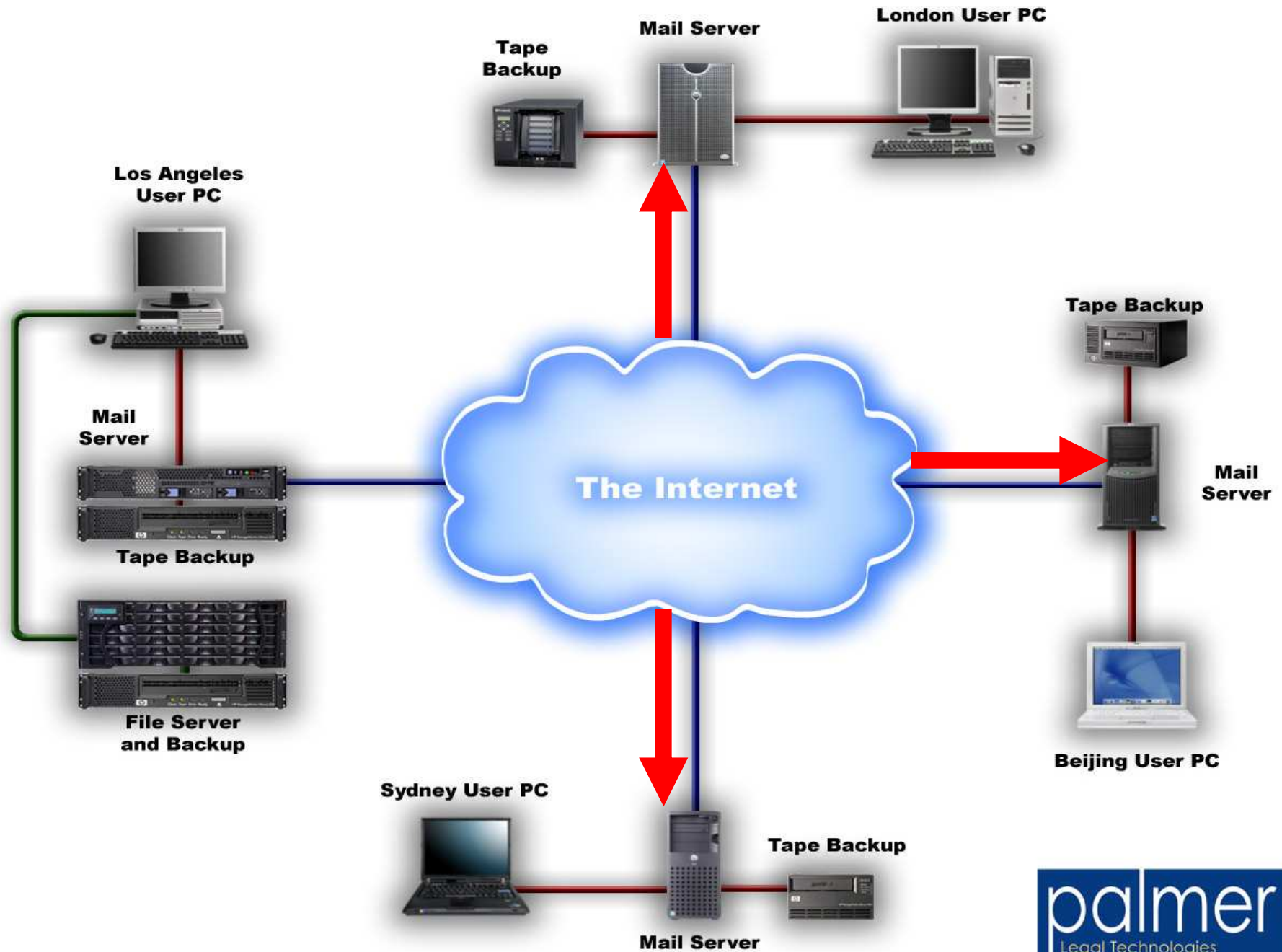
- **Volume**
 - 1Gb could be 100,000 pages of email
 - 1 Backup Tape could be 400Gb or 40m documents
 - 40m docs = 200 tonnes of paper!
- **Data, Relevancy Filtering**
 - Custodian
 - Dates
 - Key Words
 - File Types
 - Duplicates
- **Find the Important Documents Quickly**

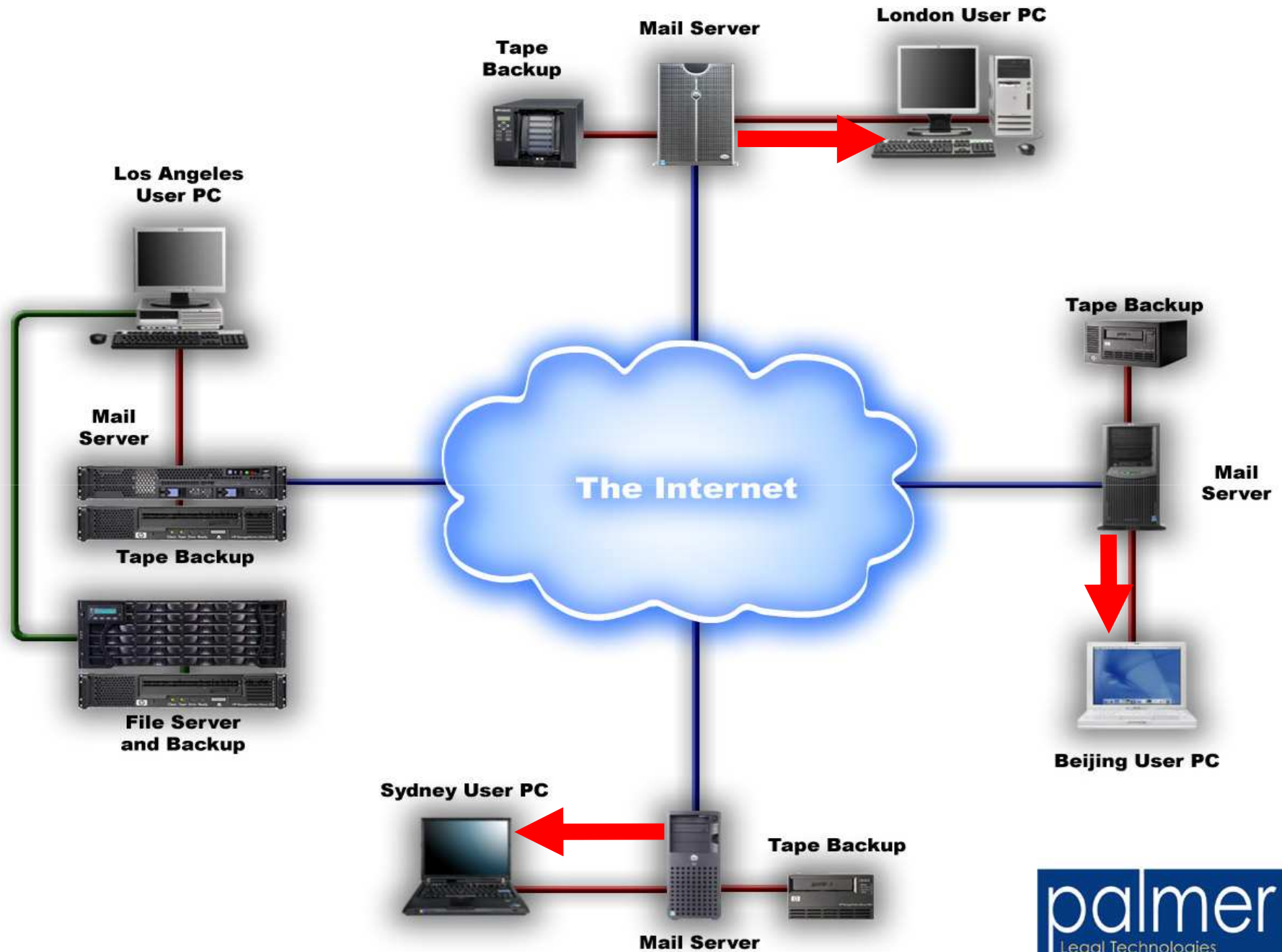


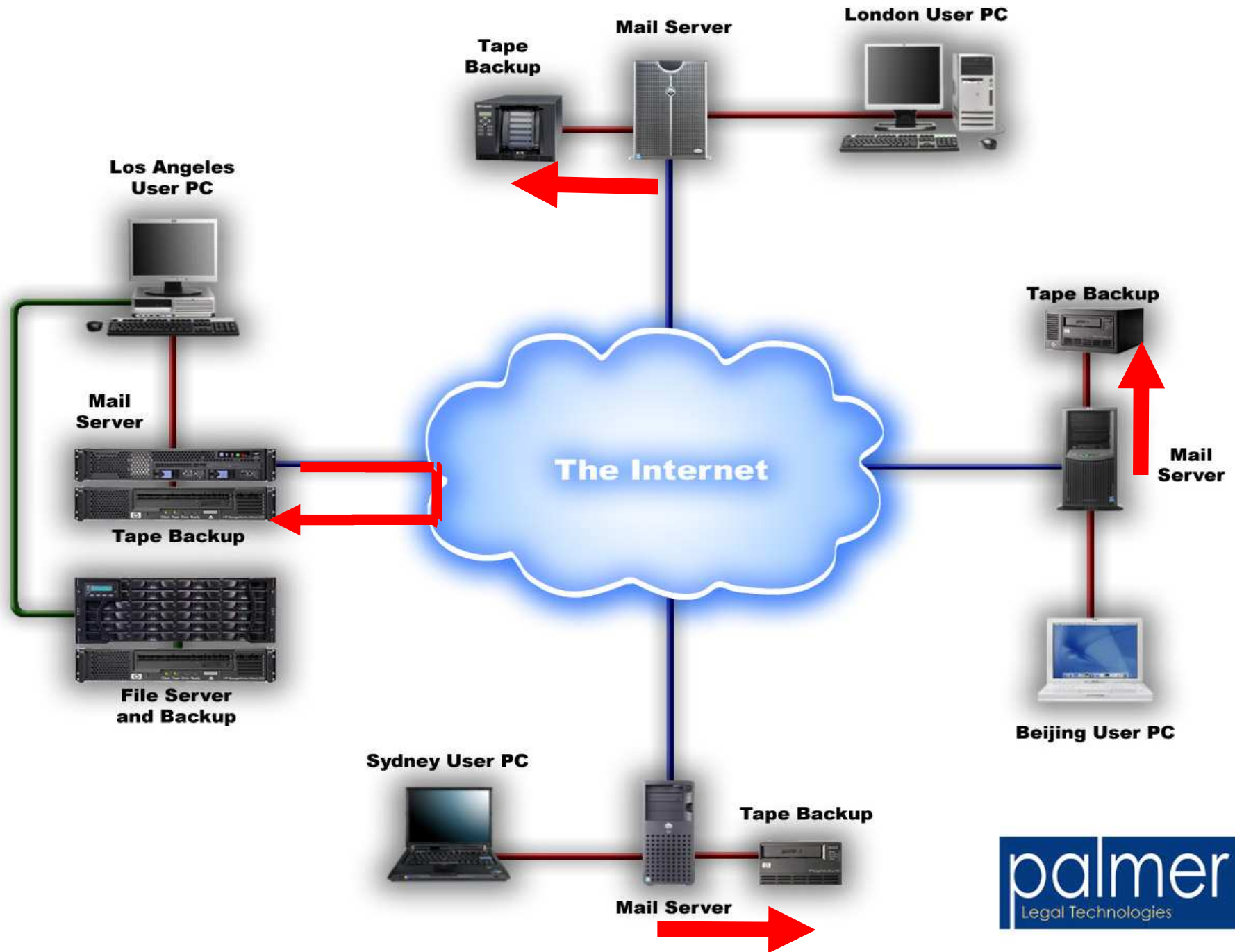
**Document
Attachement**







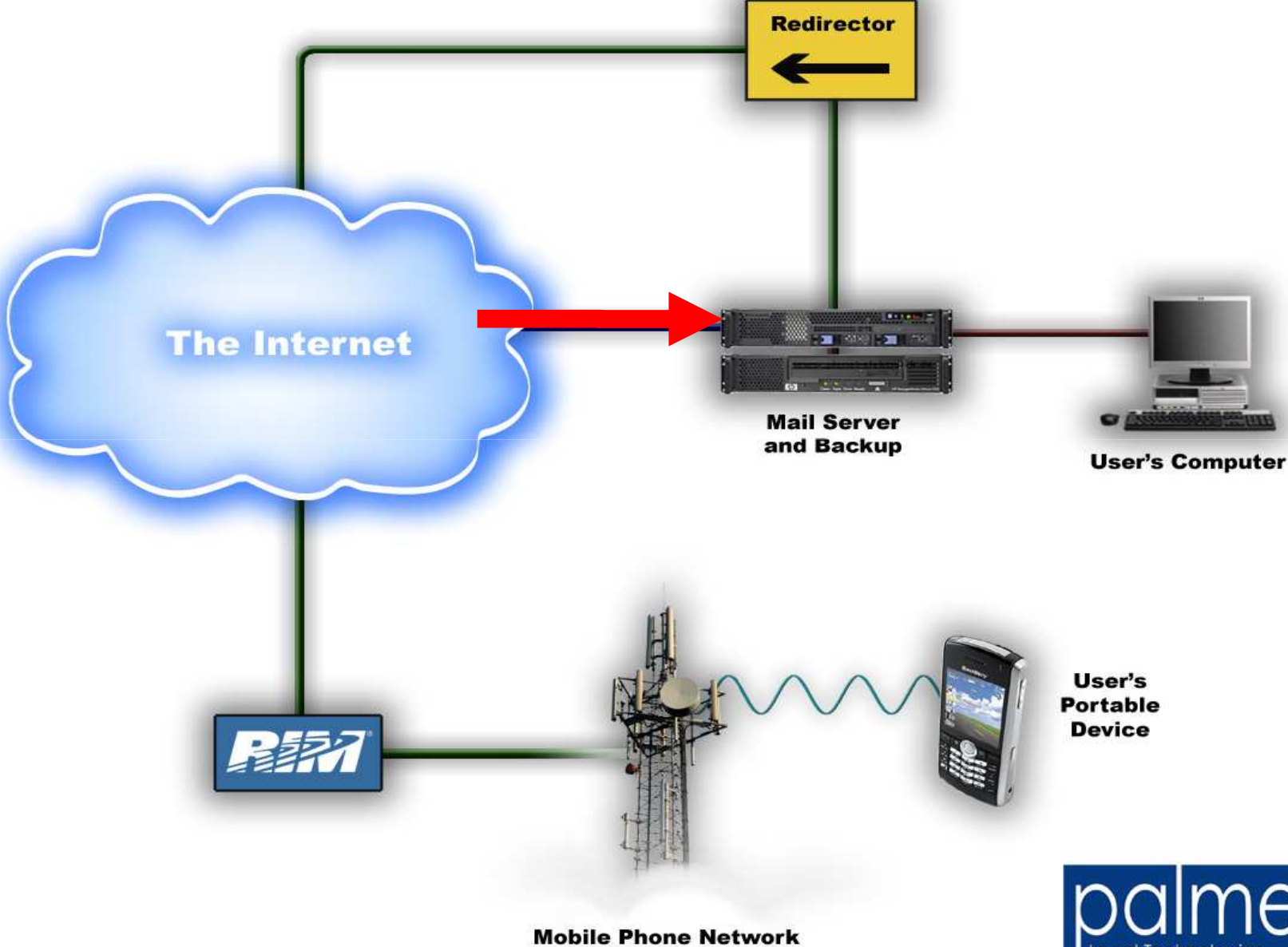


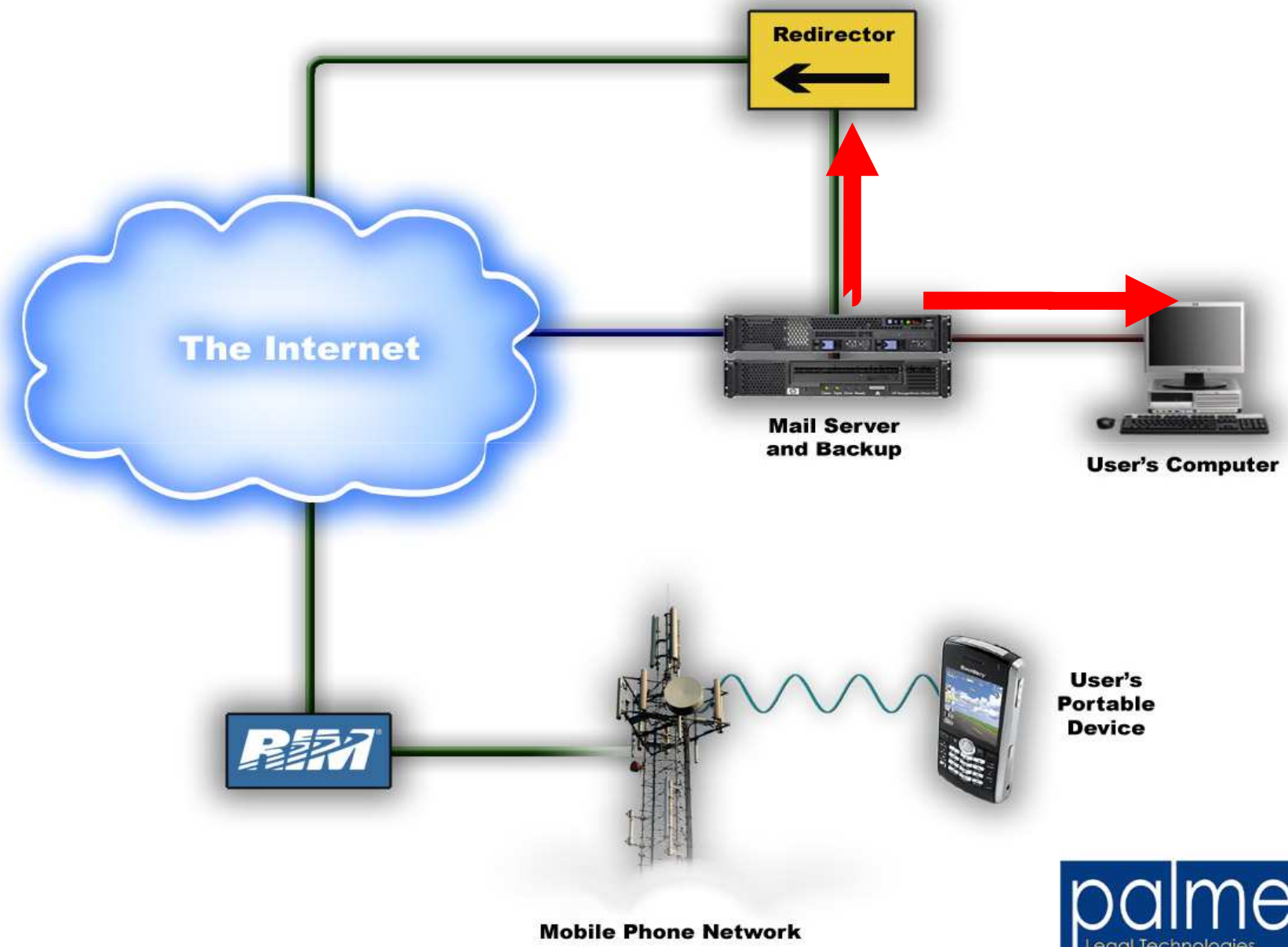


How Many Copies?

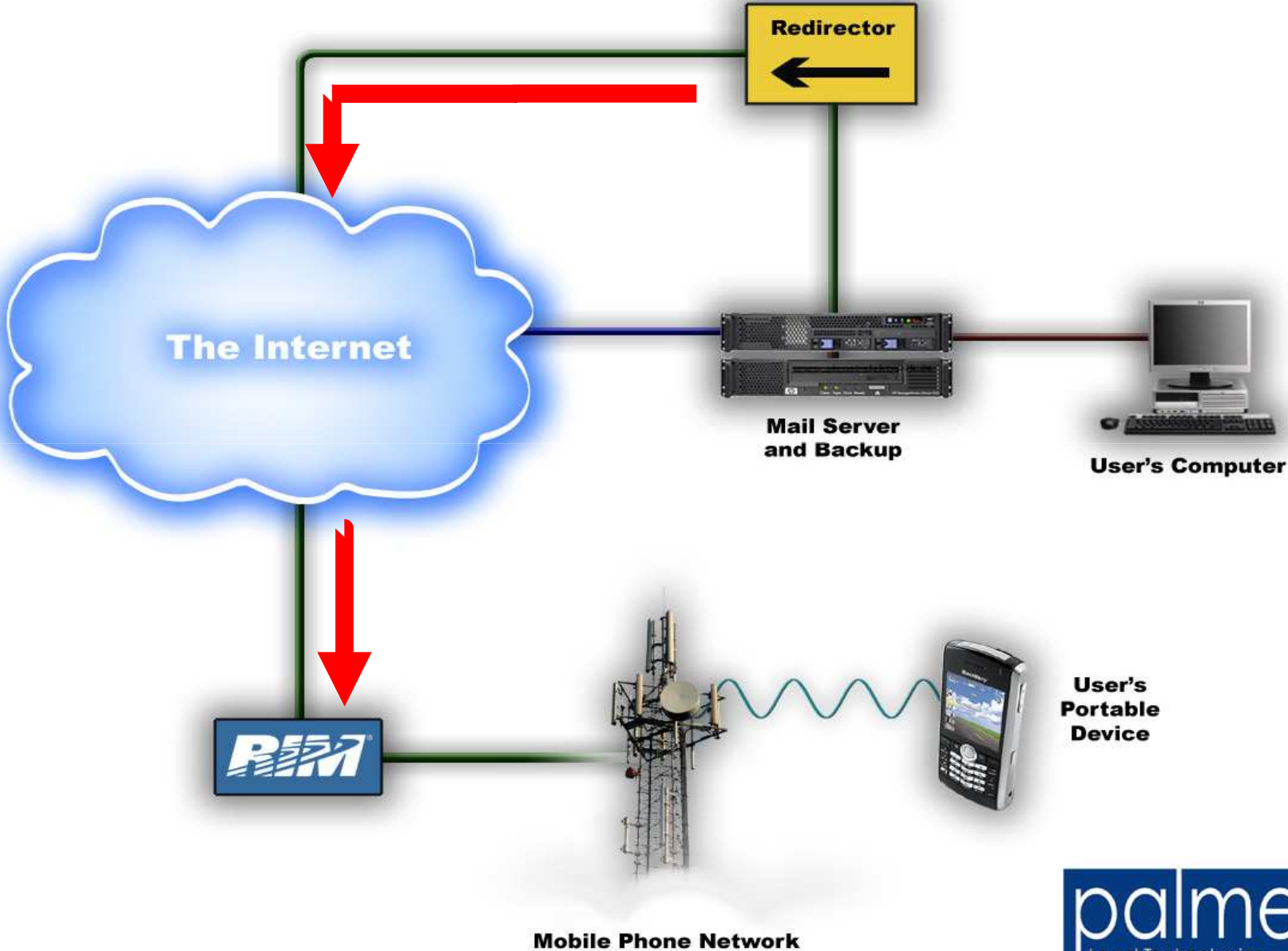
- **Los Angeles**
 - File Server & Backup (2 Copies)
 - Email Server & Backup (2 Copies)
 - User PC (1 Copy)
- **London, Beijing & Sydney**
 - Users' PCs (3 Copies)
 - Email Servers (3 Copies)
 - Email Backups (3 Copies)
- **Minimum - 14 Copies**

'Blackberry'

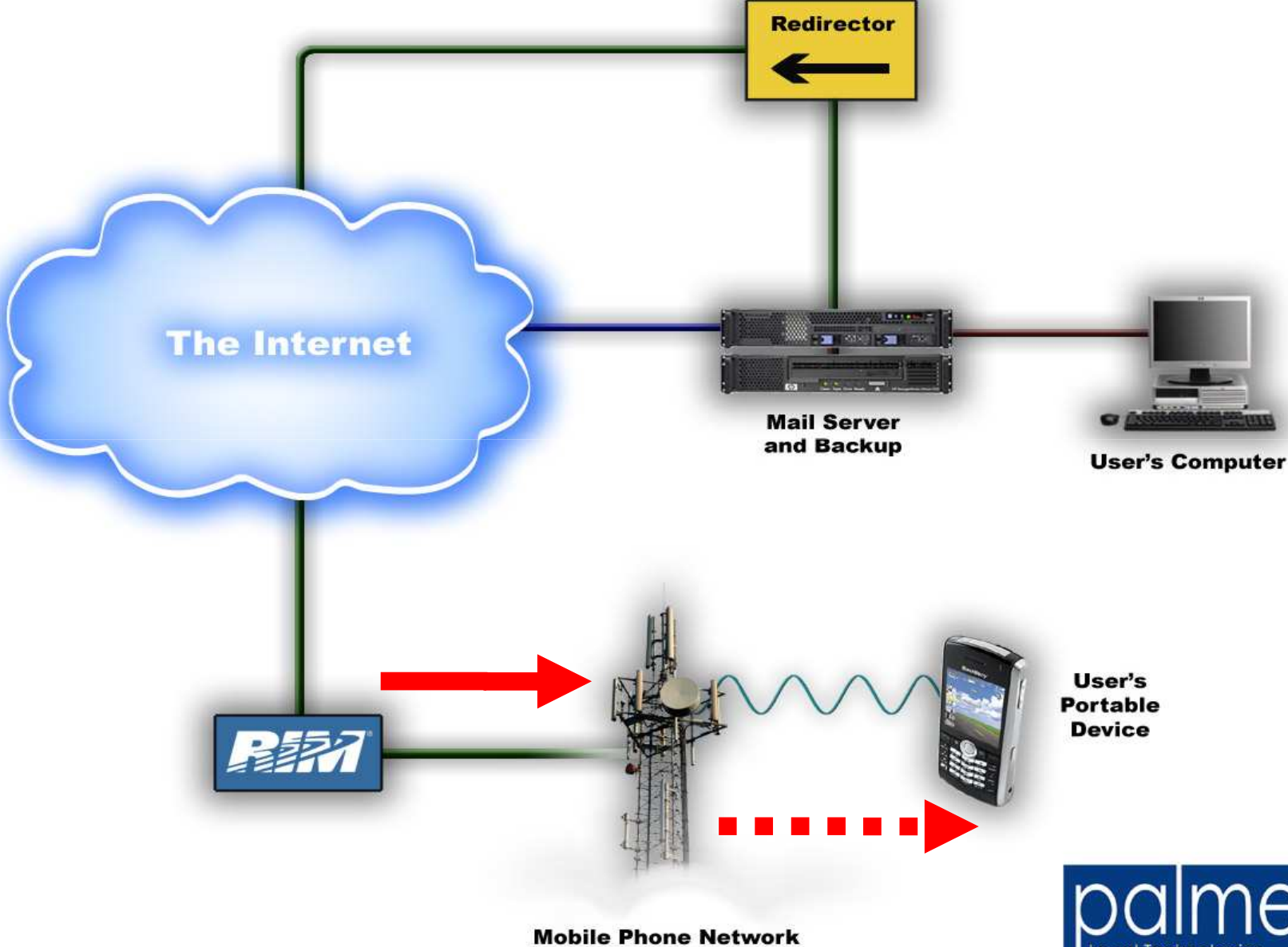




'Blackberry'



'Blackberry'



Document Review Platforms

- **Emails & All Other Documents**
- **Secure, Online Repositories**
 - Upload electronic & paper docs
- **Search Capability**
 - Boolean (“Adrian” + “Palmer”)
 - Conceptual
 - Languages (any)
- **Redact Privileged Docs**
- **Document Category Coding**
- **Produce Docs to Regulators**

- Folders
 - Salt vs Pepper - Migration
 - Admin Staging
 - Custodians
 - Allen, Paul
 - Arnold, John
 - Arora, Harry
 - Badeer, Rober
 - Bailey, Susan
 - Bass, Eric
 - Benson, Robert
 - Blair, Lynn
 - Brawner, Sandra F
 - Buy, Rick
 - Campbell, Larry
 - Carson, Mike
 - Maggi, Mike
 - Mann, Kay
 - Martin, Thomas
 - May, Larry
 - McCarty, Danny
 - McConnell, Mike
 - McKay, Brad
 - McKay, Johnathan
 - McLaughlin, Errol
 - Schurz, Taffi
 - Sieja, Andrew
 - Slinger, Ryan

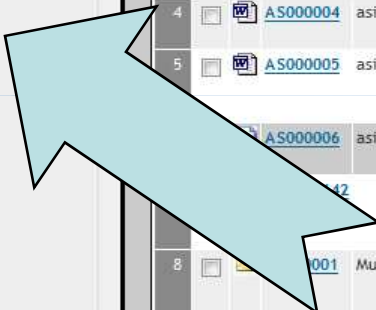
Salt vs Pepper - Migration

Searching 73,956 Admin In This Folder & Subfolders

0 Selected Item(s) Show Filters | Clear All | Items 1 - 100 (of 1,000)

	Control Number	Author	Folder Name	Recipients	Subject	Issues	Responsiveness	Privilege	
1	AS000001	asieja@kcura.com	Sent Items		kCura Relativity	Pam's Hot topic	Not Responsive	Not Privileged; Privileged; Attorney-Client	1
2	AS000002	asieja@kcura.com	Sent Items		Relativity Review Stats.xls	Pam's Hot topic	Responsive	Not Privileged; Privileged; Work Product; Not Sure	1
3	AS000003	asieja@kcura.com	Sent Items		client_presentation.ppt	Pam's Hot topic	Responsive	Privileged	1
4	AS000004	asieja@kcura.com	Sent Items		korean.doc	Pam's Hot topic	Responsive	Not Privileged	1
5	AS000005	asieja@kcura.com	Sent Items		relativity_pilot_agenda.doc	Pam's Hot topic	Responsive	Privileged; Attorney-Client	1
6	AS000006	asieja@kcura.com	Sent Items		big_video.wav	Pam's Hot topic	Responsive	Privileged; Attorney-Client	1
7	AS000007	asieja@kcura.com	Sent Items		December 14, 2000 - Bear Stearns' predictions for telecom in Latin America	Business Development; New Deals; Hot; Really Hot; Super Hot; en fuego; ouch	Responsive	Not Privileged	1
8	AS000008	asieja@kcura.com	Sent Items		Bloomberg Power Lines Report	Business Development; Personal	Not Responsive	Not Privileged; Privileged; Super Priv	1
9	EN000002	me...							
10	EN000003	philip.allen@enron.com	all_documents	keith.holst@enron.com	Consolidated positions: Issues & To Do list		Responsive	Not Privileged	0
11	EN000004	philip.allen@enron.com	all_documents	keith.holst@enron.com	Consolidated positions: Issues & To Do list		Responsive	Not Privileged	0
12	EN000005	philip.allen@enron.com	all_documents	david.detainey@enron.com		Business Development; New Deals	Responsive	Not Privileged	0

Checked Edit Go Viewing the First 1,000 items in sets of 100 per page



Folders containing the various documents for review

- Advanced & Saved Searches
- New Search
 - _DeDuplicated Concept Source
 - 3yr Confidential Author
 - 5yr Email Authored Distribution
 - 9yr Custodian Search
 - Batch First Half
 - Batch Second Half
 - Batch Source
 - Full File Export
 - Paul Allen Investing Documents - Date
 - PLT_Test**
 - Production QC
 - Redacted Document
 - Redacted Documents
 - Responsive Email
 - Robin 1
 - Saved Search 1
 - Saved Search 1

Search Save & Search

Information:

Name: PLT_Test

Includes: [Dropdown]

Scope: Entire Case Selected Folders
[Select Folders](#) - Currently searching entire case.

Search Conditions:

Search With: Keyword Search [Dropdown]

Search Text: football

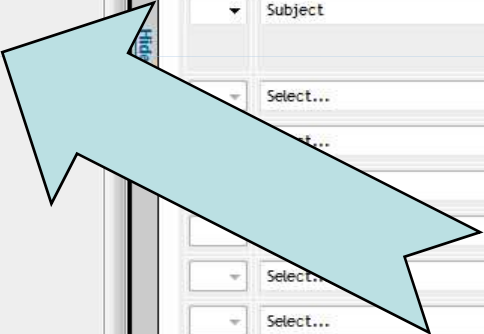
Sort By Rank:

Conditions:

Field	Operator	Value		
Subject	is like	football	[Dropdown]	[Dropdown]
Select...	is like		[Dropdown]	[Dropdown]
Select...	is like		[Dropdown]	[Dropdown]
Select...	is like		[Dropdown]	[Dropdown]
Select...	is like		[Dropdown]	[Dropdown]
Select...	is like		[Dropdown]	[Dropdown]
Select...	is like		[Dropdown]	[Dropdown]
Select...	is like		[Dropdown]	[Dropdown]
Select...	is like		[Dropdown]	[Dropdown]

Fields (Required):

Alert Script	Edit
Artifact ID	File Icon
Assigned To	Control Number
Author	Full Title
Auto Category	Sent To
Auto Category Example	Sent CC



Advanced search results can be saved

Return to document list

AS000001 Document 1 of 1000

Viewer Native Image Extracted Text Delete Images Save Save & Next Cancel Coding

Email From, To, CC, BCC or Subject information may be truncated in Draft or Normal mode.
View email in Preview mode to see all information.

100%

To: Taffi Schurz[tschurz@kcura.com]
From: Andrew H. Sieja
Sent: Thur 1/10/2008 3:51:31 AM
Importance: Low
Sensitivity: None
Subject: kCura **Relativity**

Document coding fields

Relativity [Review Stats.xls](#)
[client_presentation.ppt](#)
[korean.doc](#)
[relativity_pilot_agenda.doc](#)
[big_video.wav](#)
[pilot_agenda.docx](#)

Hi Taffi -

I hope you are enjoying this demonstration of **Relativity**. During the demonstration we are going to cover a lot of material so please stay awake! If you have any questions, don't hesitate to stop me along the way, but if you sit tight, I'll probably cover it at some point during the demonstration.

We are about to go through some attachments that showcase how **Relativity** displays native documents inside our proprietary viewer. It will include an Excel spreadsheet, a Word document, a PowerPoint presentation, a Word document in Korean, a document with tracked changes, and finally a 10 MB video file.

I just want to note that we are accessing **Relativity** deployed at our datacenter clear across the internet. You will notice that the documents still come up pretty quickly.

Enjoy the rest of the demo...

Kind Regards,

Andrew H. Sieja
kCura Corporation
333 West Wacker Drive
Suite 1430
Chicago, IL 60606
telephone: (312) 263-1177 Ext.13
mobile: (312) 493-3728
<http://www.kcura.com>

Family (linked docs)

Reviewer Details
Control Number: AS000001
Custodian: Sieja, Andrew

Coding

Responsiveness: Not Responsive Not Sure
 Responsive
[Add](#)

Confidentiality: FYIO Confidential
 Not Confidential Not Sure
[Add](#)

Privilege: Not Privileged
 Privileged
 Attorney-Client
 Work Product
 Super Priv
 Not Sure
[Add](#)

Issues: Look at this later
 MAPP
 Pam's Hot topic
 V. Important
 Accounting
 Business Development
 New Deals
 Personal
 Suspended Email

Save Save & Next Cancel

Family

Control Number	Subject
AS000001	kCura Relativity
AS000002	Relativity Review Stats.xls
AS000003	client_presentation.ppt
AS000004	korean.doc
AS000005	relativity_pilot_agenda.doc

Items 1 - 6 (of 6)

Checked Items Edit Go

Attorney 246.15 kb/s

Trusted sites | Protected Mode: Off 100%



Redactions and highlighting with comments and log

To: Taffi Schurz[tschurz@kcure.com]
From: Andrew H. Sieja
Sent: Thur 1/10/2008 3:51:31 AM
Importance: Low
Sensitivity: None
Subject: kCura Relativity

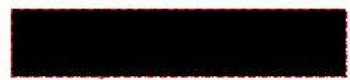
- Relativity_Review_Stats.xls
- client_presentation.ppt
- korean.doc
- relativity_pilot_agenda.doc
- big_video.wmv
- pilot_agenda.docx

Hi Taffi-

I hope you are enjoying this demonstration of Relativity. During the demonstration we are going to cover a lot of material so please stay awake! If you have any questions, don't hesitate to stop me along the way, but if you sit tight, I'll probably cover it at some point during the demonstration.

REDACTED

I just want to note that we are accessing Relativity deployed at our datacenter clear across the internet. You will notice that the documents still come up pretty quickly.



kCura Corporation
333 West Wacker Drive
Suite 1400
Chicago, IL 60606
Telephone: (312) 263-1177 Ext.13
Mobile: (312) 493-3728
http://www.kcure.com

Reviewer Details

Control Number: AS000001
Custodian: Sieja, Andrew

Coding

Responsiveness: Not Responsive
Confidentiality: Not Confidential
Privilege: Not Privileged; Privileged; Attorney-Client;
Issues: Pam's Hot topic;

Reviewer Comments

some important stuff - please read chapter 5

Redaction Log Comments

JCR made change

Edit

Family

	Control Number	Subject
	AS000001	kCura Relativity
	AS000002	Relativity Review Stats.xls
	AS000003	client_presentation.ppt
	AS000004	korean.doc
	AS000005	relativity_pilot_agenda.doc

Items 1 - 6 (of 6)

Edit Delete Back Edit Permissions

Report Information

Name: Demo Report

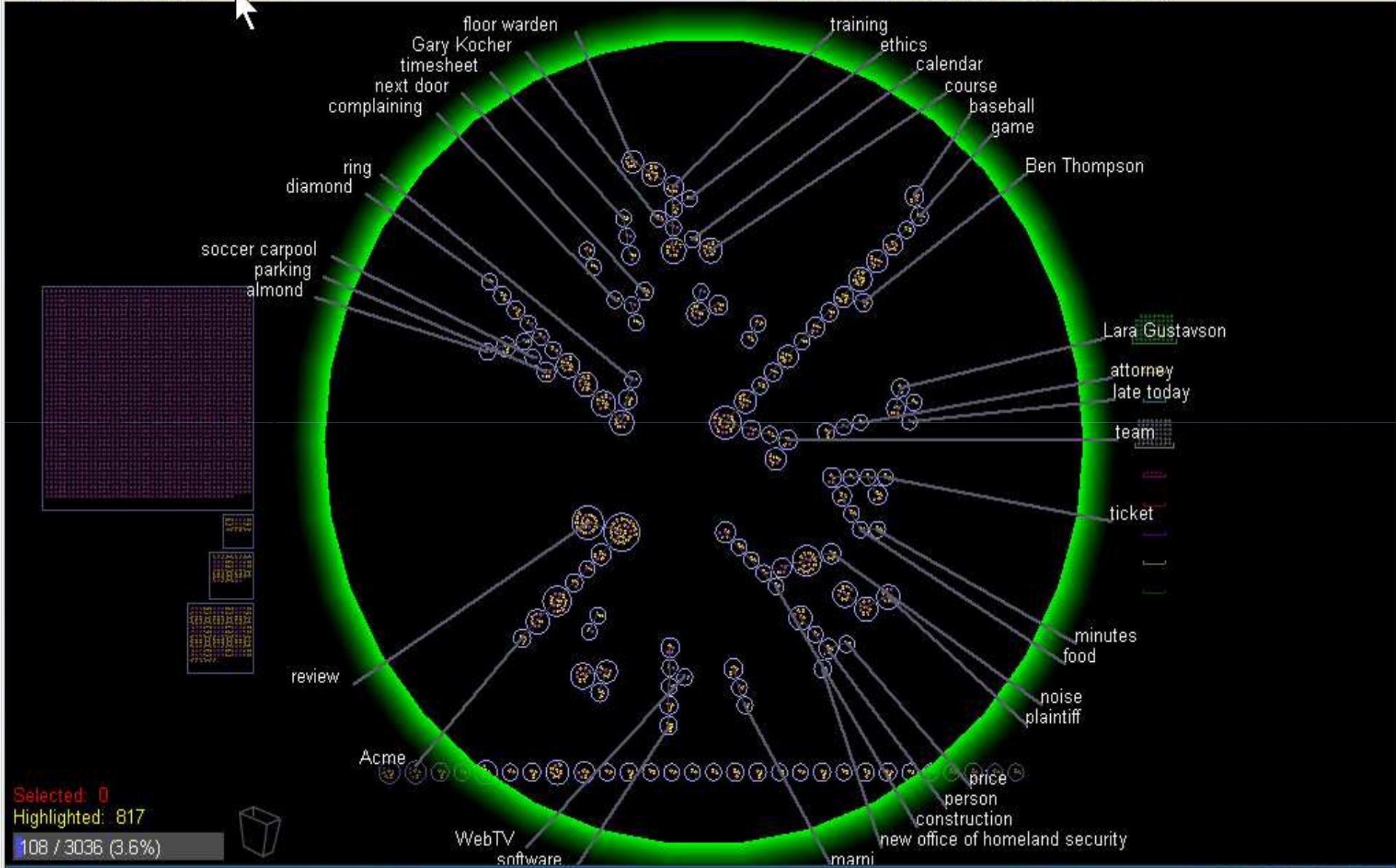
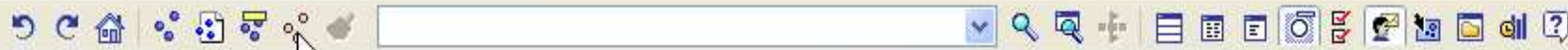
Export to Excel | Show Filters | Clear All | Items 1 - 25 (of 25) << < > >>

Custodian	Responsiveness: (t set)	Confidentiality: Confidential	Issues: Business Development	Privilege: Privileged	Record Count
Allen, Paul	3,002	10	10	13	3,040
Arnold, Johnny	4,884		0	12	4,897
Arora, Harry	653		0	0	654
Badeer, Robert	877		0	0	877
Bailey, Susan	478		0	0	478
Bass, Eric	7,335		0	1	7,823
Baughman, Don	2,760		0	0	2,760
Benson, Robert	767	0	0	0	767
Blair, Lynn	3,415	0	0	0	3,415
Brawner, Sandra F.	1,026	0	0	0	1,026
Buy, Rick	2,429	0	0	0	2,429
Campbell, Larry	6,487	3	0	3	6,490
Carson, Mike	1,358	0	0	0	1,400
Maggi, Mike	1,991	0	0	0	1,991
Mann, Kay	23,381	0	0	0	23,381
Martin, Thomas	1,112	0	0	0	1,112
May, Larry	1,600	0	0	0	1,600
McCarty, Danny	691	0	0	0	691
McConnell, Mike	4,542	0	0	0	4,542
McKay, Brad	676	0	0	0	681
McKay, Johnathan	998	0	0	0	998
McLaughlin, Errol	2,760	0	0	0	2,760
Schurz, Taffi	6	0	1	0	6
Sieja, Andrew	0	3	0	4	6
Stinger, Ryan	132	0	0	0	132
Totals:	73,360	27	11	33	73,956

Reporting on reviewer progress

Select Page Size: 100

Edit Delete Back Edit Permissions



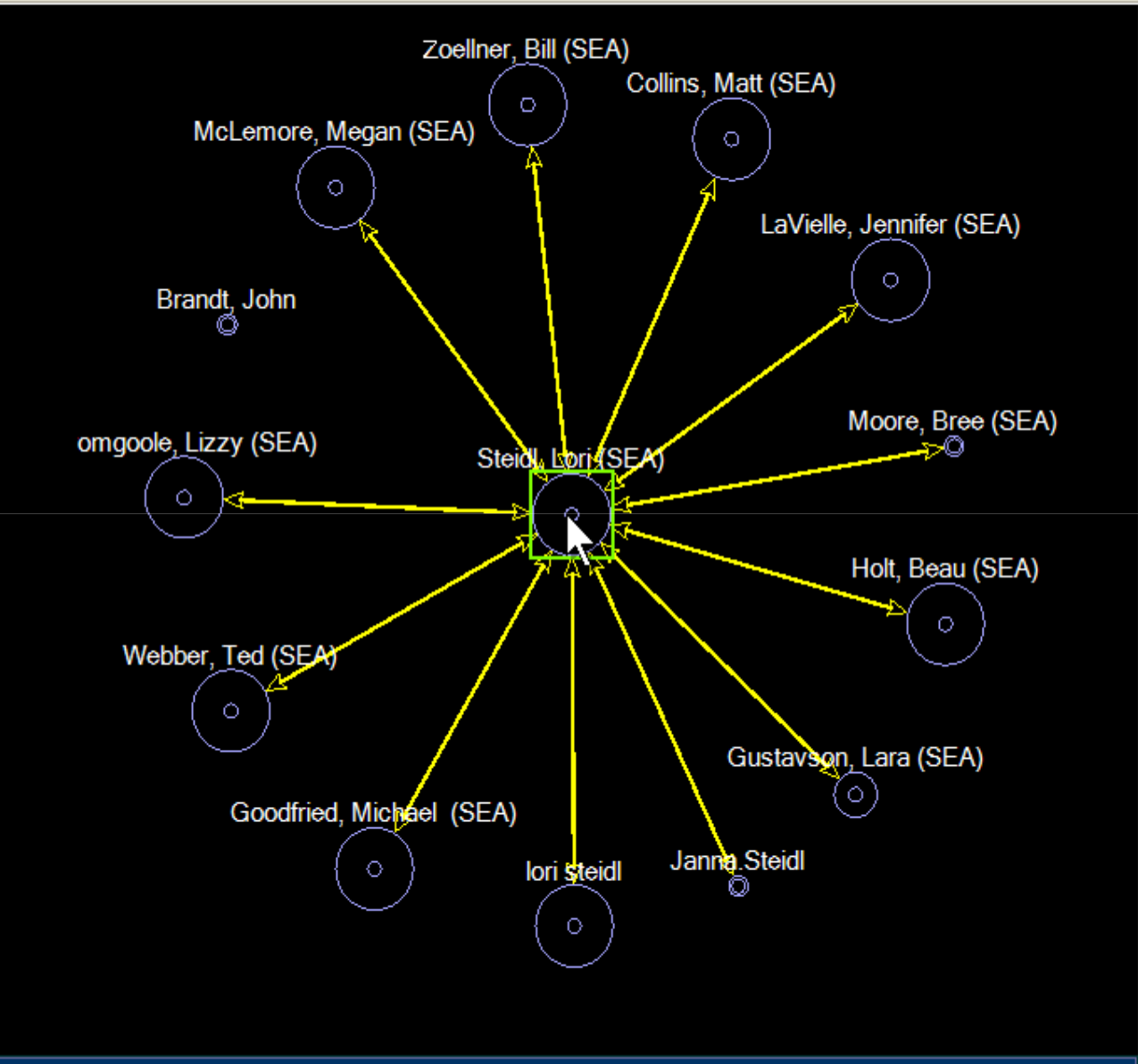
Selected: 0
Highlighted: 817
108 / 3036 (3.6%)



Participant	Domain	Sent	R...
Larry Fennel	aol.com	39	40
Brandt, John	PRESTON	42	12
Collins, Matt (SEA)	PRESTON	123	316
Dromgoole, Lizzy (SEA)	PRESTON	49	185
Goodfried, Michael (SEA)	PRESTON	94	170
Gustavson, Lara (SEA)	PRESTON	30	130
Holt, Beau (SEA)	PRESTON	70	105
LaVielle, Jennifer (SEA)	PRESTON	274	199
McLemore, Megan (SEA)	PRESTON	56	116
Moore, Bree (SEA)	PRESTON	47	10
Steidl, Lori (SEA)	PRESTON	253	941
Webber, Ted (SEA)	PRESTON	150	278
Zoellner, Bill (SEA)	PRESTON	134	382
Janna Steidl	target.com	29	2
lori steidl	yahoo.com	192	96

Hidden Participants (1114)

Participant	Domain	Sent	R...
'connie.zener@ace-ina.com'	ace-ina.com	0	2
'h.maurice.booth@ace-ina.c...	ace-ina.com	0	2
'sheri.kristiansen@ace-ina.c...	ace-ina.com	0	2
Mike Conardo (E-mail)	ADCO-W/W...	0	4
'lisa.lindquist@adecco.com'	adecco.com	0	2
'srebmann@adolphlaw.com'	adolphlaw.c...	0	2
'kory.balls@am.joneslangla...	am.joneslan...	0	2
'terry.dallas@am.joneslangla...	am.joneslan...	0	2
'Lara G 123"@aol.com	aol.com	0	1
'gmflaw@aol.com, kellstea...	aol.com,	0	1
Alkitnuu@aol.com	aol.com	0	1



Questions

Thank you For Listening