



cutting through complexity™

Denetim ve Adli Bilişim

II. Bilgi Teknolojileri Yönetişim ve Denetim
Konferansı

Ankara

10 Haziran 2011

Göktürk Tamay



1. Adli Bilişim

1.1 Temel tanımlar

1.2 Adli bilişimin uygulama alanları

2. Adli Bilişimin Temel Bölümleri

2.1 Veri Analizi

2.2 Veri Kurtarma

2.3 Elektronik Kanıt Yönetimi

3. Özet

4. Sorular



1. Adli Bilişim

1.1 Temel Tanımlar

1.2 Adli Bilişim Uygulama Alanları

1.1 Temel Tanımlar

Adli Bilişim

Adli bilişim, elektronik ortamlardan elde edilen bulguların, çeşitli teknik donanım ve yazılımlar kullanılarak denetim, soruşturma, inceleme veya dava süreçlerinde kullanılacak delillere dönüştürülme bilimidir.

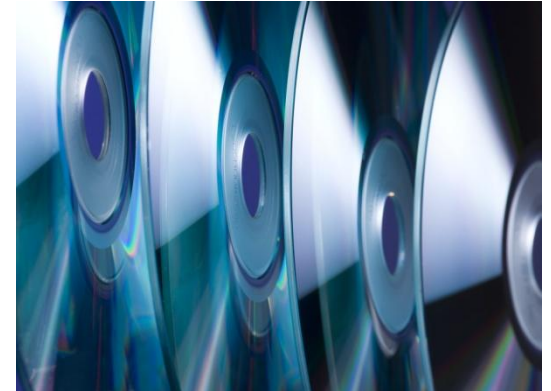


Delil

Bir şeyin doğruluğu, gerçekliği konusunda kanaat verici belge, iz veya argümandır.

Elektronik Ortam

Bilginin dijital olarak iletilebildiği veya depolanabildiği yöntem ve aygıtlara verilen isim.



1.2 Adli Bilişim Uygulama Alanları

Adli Bilişim Uygulama Alanları (Finansal)

- Suistimal önleme, tespit ve inceleme çalışmaları
- Soruşturmalar (Yasal / Şirket içi)
- Finansal denetimler
- İç Denetim Çalışmaları
- İç Kontrol Çalışmaları
- Kontrol testleri
- Kara para Aklamanın Önlenmesi ve Tespiti
- Yasal mevzuata uyum çalışmaları
- Sözleşme maddelerine uyum kontrolleri
- Ticari anlaşmazlıkların incelenmesi ve analizi
- Performans ölçümleri
- Veri kalitesinin kontrolü
- Fikri haklar ile ilgili uyuşmazlıklar (İnternet)
-

Veri Analizi

Veri Kurtarma

E-Kanıt Yönetimi



2. Adli Bilişimin Temel Bölümleri

2.1 Veri Analizi

2.2 Veri Kurtarma

2.3 Elektronik Kanıt Yönetimi

2.1 Veri Analizi

Potansiyel Suistimal Risklerinin Analizi (Ktrace)

- 106 farklı risk senaryosu
- Risk rating
- Kısıtlı denetim kaynaklarının riskli alanlara yönlendirilmesi
- Uluslararası standartlara uygun denetim faaliyetlerinin gerçekleştirilmesi (SEC vb.)
- Denetim çalışmasının kayıtların %100'ü üzerinde gerçekleştirilebilmesi
- Kontrol eksikliklerinin ve zayıflıklarının tespit edilebilmesi
- İstenilen formatta raporların çıktı olarak alınabilmesi
- Zaman tasarrufu sağlanması
- Denetim maliyetlerinin düşürülmesi
-

Veri Analizi Uygulamaları

- Ktrace
- Web Focus
- SQL
- Idea
- ACL
- Picalo

2.1 Veri Analizi

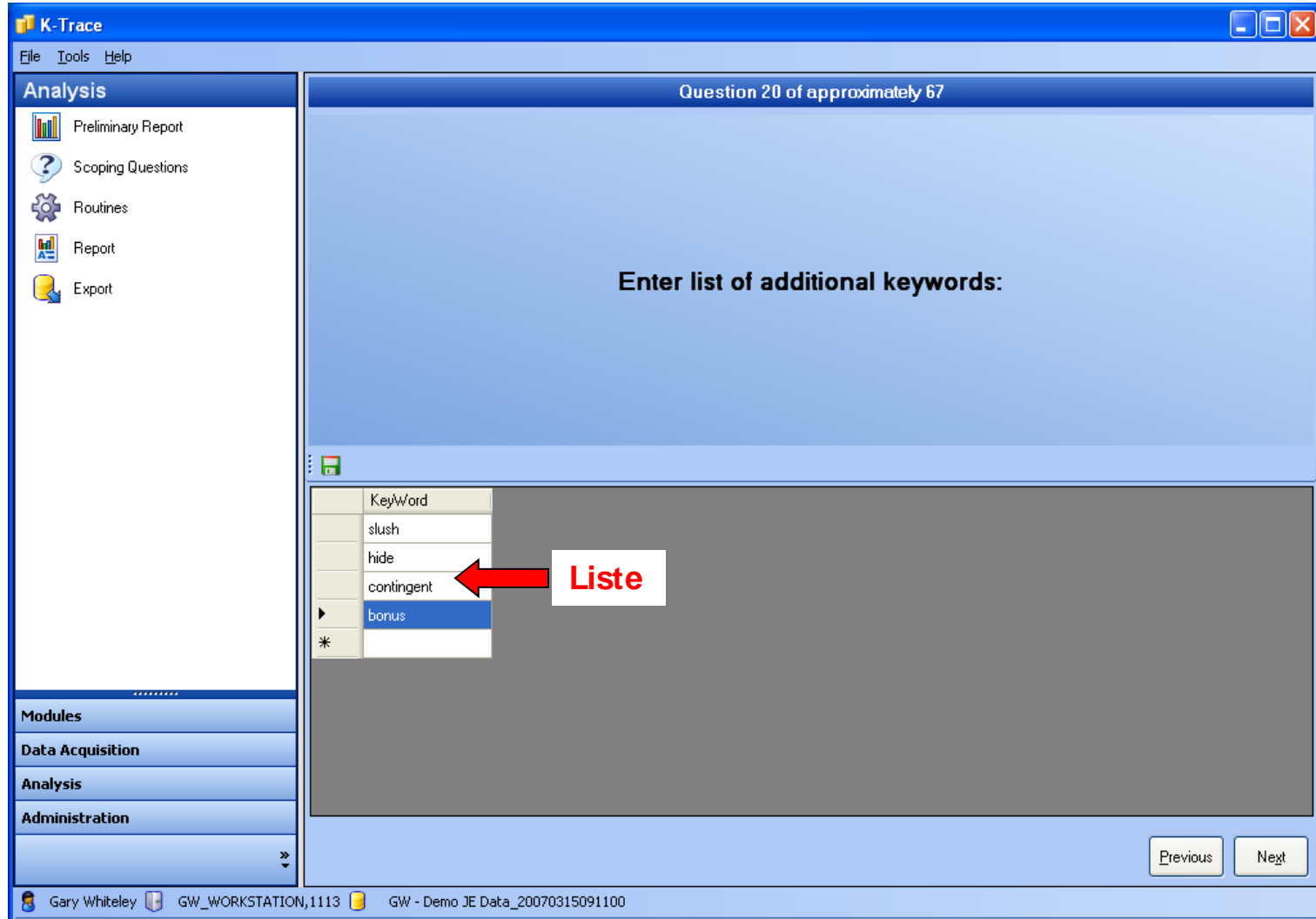
The screenshot displays the K-Trace software interface. The window title is "K-Trace" and the menu bar includes "File", "Tools", and "Help". The left sidebar contains an "Analysis" section with options: "Preliminary Report", "Scoping Questions", "Routines", "Report", and "Export". Below this is a "Modules" section with "Data Acquisition", "Analysis", and "Administration".

The main area is titled "Question 1 of approximately 67" and contains the question: "Would it be unexpected if a journal line has an account number that is not in the current chart of accounts?". A red arrow points to this question text with the label "Kriter".

Below the question, there are radio buttons for "No" and "Yes", with "Yes" selected. To the right is a "Weight" slider set to 3, with a red arrow pointing to the number 3 and the label "Ağırlık".

At the bottom right of the main area are "Previous" and "Next" buttons. The status bar at the bottom shows the user "Gary Whiteley" and the workstation "GW_WORKSTATION,1113".

2.1 Veri Analizi



The screenshot displays the K-Trace software interface. The main window is titled "Question 20 of approximately 67" and contains the text "Enter list of additional keywords:". Below this text is a list of keywords in a table format. A red arrow points to the word "contingent" in the list, with a white box containing the word "Liste" next to it.

KeyWord
slush
hide
contingent
bonus
*

At the bottom of the interface, there are "Previous" and "Next" buttons. The status bar at the very bottom shows the user "Gary Whiteley" and the file path "GW - Demo JE Data_20070315091100".

2.1 Veri Analizi

The screenshot displays the K-Trace software interface. The window title is "K-Trace" and it has a menu bar with "File", "Tools", and "Help". On the left side, there is a sidebar with the following options: "Analysis", "Preliminary Report", "Scoping Questions", "Routines", "Report", and "Export". Below the sidebar, there are sections for "Modules", "Data Acquisition", "Analysis", and "Administration". The main area of the window shows "Question 30 of approximately 67". The question text is: "How many zero digits need to occur to be considered a rounded dollar entry? Example - \$10,000 = 4 digits." Below the question, there is a Turkish translation: "Kaydın yuvarlanmış bir kayıt olduğuna karar verilmesi için kaç basamağın sıfır ile bitmesi gerekir?". A text input field contains the number "4", with a red arrow pointing to it and the text "Eşik Değer" (Threshold Value) next to it. At the bottom right of the main area, there are "Previous" and "Next" buttons. The status bar at the bottom shows the user "Gary Whiteley", the workstation "GW_WORKSTATION,1113", and the demo file "GW - Demo JE Data_20070315091100".

2.1 Veri Analizi

Score by Lines

Top 30 Journal Entries Based on JE Lines with the Highest Scores

The table below represents the top 30 journal entries based on

JE Identifier	Max Line Score	Average Line Score	Total JE Score	One Sided Entries	Same Side Corrections	Zero-Monetary Amount	Account Not In COA	No Account Number	Blank JE Description	DR Asset CR Expense	DR & CR Inventory-Reserve	DR & CR Reserve	DR & CR Suspense	DR Inventory CR COS	DR Inv-Res CR Non-COGs E	DR Liability CR Expense	DR Liability CR Revenue	DR Retained-Earnings CR Re	DR Sus-Asset CR Non-Asset	DR Sus-Liab CR Non-Liab	Invalid Effective Dates	Invalid Post Dates	Large Journal Entries	Missing User ID	Additional Keywords 1	Additional Keywords 2	Additional Keywords 3	Additional Keywords 4	Additional Keywords 5	Additional Keywords 6	Reclassification	Restatements	Reversals	Standard Deviation	Late Hours	Weekends	Holidays	Rounded Amounts	Manual Period Monetary Volt	Manual Period Transaction Y	Seldom Used Account	Back-Posted	Unauthorized Users	Manual User ID	Manual Revenue Trending							
GM00115590	25	25.00	25	0	0	0	0	0	0	0	3	0	0	0	0	3	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	2	3	2	0	0	0	0	0	0	0	0	0	0	0	0					
GM00115590	20	20.00	20	0	0	0	0	0	0	0	3	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	2	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0			
GM00115590	20	20.00	20	0	0	0	0	0	0	0	3	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		
GM00115590	20	20.00	20	0	0	0	0	0	0	0	3	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	3	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
GM00115590	20	20.00	20	0	0	0	0	0	0	0	3	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

2.1 Veri Analizi

Finansal Sektörden Bir Örnek

Kullanılan veriler

- 4 farklı veri seti:

Muhasebe fişleri – Hesap planı – İnsan kaynakları – Kullanıcı listesi

-10 milyon satır muhasebe fişleri verisi

- 100 sütun muhasebe fişleri verisi

Bankanın İzmir şubesinde görev yapan A müşteri temsilcisinin işten ayrılmadan 2 gün önce kendi yetkisi üzerinde olan **350.000 TL**'lik bir ödeme işlemi gerçekleştirdiği ve bu işlem için ilgili ana bankacılık modülünde ek bir onaylama yapılmadığı tespit edildi. Ayrıca işlem detayları olarak işlem tarihi, işlem saati, para cinsi, işlem tutarı, işlemi gerçekleştiren müşteri temsilcisinin adı ve ilgili müşterinin adı ortaya çıkarıldı.

2.2 Veri Kurtarma

The screenshot displays the EnCase Forensic software interface. The main window shows a list of files with columns for Name, Filter, In Report, File Ext, File Type, File Category, Signature, Description, Is Deleted, and Last Accessed. The file explorer tree on the left is circled in red, showing a directory structure under 'C:\'. A large graphic of a bunch of grapes is also circled in red at the bottom of the interface.

Name	Filter	In Report	File Ext	File Type	File Category	Signature	Description	Is Deleted	Last Accessed
22195	PE00049_		WMF	Windows Metafile	Picture		File, Archive		05/03/11 11:14:4
22196	PE06049_		WMF	Windows Metafile	Picture		File, Archive		05/03/11 12:20:0
22197	NA01149_		WMF	Windows Metafile	Picture		File, Archive		05/03/11 11:14:3
22198	DD00449_		WMF	Windows Metafile	Picture		File, Archive		05/03/11 12:20:0
22199	NA01849_		WMF	Windows Metafile	Picture		File, Archive		05/03/11 11:14:3
22200	SO00159_		WMF	Windows Metafile	Picture		File, Archive		05/03/11 11:14:4
22201	FD00459_		WMF	Windows Metafile	Picture		File, Archive		05/03/11 11:14:1
22202	PE03459_		WMF	Windows Metafile	Picture		File, Archive		05/03/11 11:14:4
22203	PE00559_		WMF	Windows Metafile	Picture		File, Archive		05/03/11 11:14:4
22204	AN02559_		WMF	Windows Metafile	Picture		File, Archive		05/03/11 11:14:0
22205	FD01659_		WMF	Windows Metafile	Picture		File, Archive		05/03/11 11:14:1
22206	HH01759_		WMF	Windows Metafile	Picture		File, Archive		05/03/11 11:14:1
22207	NA01069_		WMF	Windows Metafile	Picture		File, Archive		05/03/11 11:14:3
22208	DD01169_		WMF	Windows Metafile	Picture		File, Archive		05/03/11 11:14:1
22209	PE02169_		WMF	Windows Metafile	Picture		File, Archive		05/03/11 11:14:4
22210	BL00269_		WMF	Windows Metafile	Picture		File, Archive		05/03/11 11:14:0
22211	SO02269_		WMF	Windows Metafile	Picture		File, Archive		05/03/11 11:14:4
22212	AN04269_		WMF	Windows Metafile	Picture		File, Archive		05/03/11 11:14:0
22213	FD00369_		WMF	Windows Metafile	Picture		File, Archive		05/03/11 11:14:1
22214	PE02369_		WMF	Windows Metafile	Picture		File, Archive		05/03/11 11:14:4
22215	AN04369_		WMF	Windows Metafile	Picture		File, Archive		05/03/11 11:14:0
22216	SO01569_		WMF	Windows Metafile	Picture		File, Archive		05/03/11 11:14:4
22217	HH00669_		WMF	Windows Metafile	Picture		File, Archive		05/03/11 11:14:1
22218	PE05869_		WMF	Windows Metafile	Picture		File, Archive		05/03/11 11:14:4
22219	DD01179_		WMF	Windows Metafile	Picture		File, Archive		05/03/11 11:14:1
22220	SO00479_		WMF	Windows Metafile	Picture		File, Archive		05/03/11 11:14:4
22221	FD00779_		WMF	Windows Metafile	Picture		File, Archive		05/03/11 11:14:1
22222	SO00289_		WMF	Windows Metafile	Picture		File, Archive		05/03/11 11:14:4
22223	NA00389_		WMF	Windows Metafile	Picture		File, Archive		05/03/11 11:14:3
22224	NA02389_		WMF	Windows Metafile	Picture		File, Archive		05/03/11 11:14:3
22225	PF00489_		WMF	Windows Metafile	Picture		File, Archive		05/03/11 11:14:4

2.2 Veri Kurtarma

The screenshot displays the EnCase Forensic application window. The interface is divided into several sections:

- Left Panel:** A file system tree showing various folders and files, including Intel, Internet Explorer, Java, McAfee, Microsoft Office, and others.
- Top Panel:** A menu bar (File, Edit, View, Tools, Help) and a toolbar with options like New, Open, Save, Add Device, Search, and Refresh.
- Main Area:** A large grid displaying data entries. The grid has columns for file names and numerical values. A red circle highlights a specific entry in the grid.
- Bottom Panel:** A toolbar with tabs for Text, Hex, Doc, Transcript, Picture, Report, Console, and Details. The 'Details' tab is highlighted with a red circle.
- Bottom Right Panel:** A sidebar with a tree view showing folders like EnScript, Examples, Forensic, Include, Main, and Source Processor.

2.2 Veri Kurtarma

The screenshot displays the EnCase Forensic interface. The top menu bar includes File, Edit, View, Tools, and Help. Below it are icons for New, Open, Save, Print, Add Device, Search, Refresh, and Query. The main window is divided into several panes:

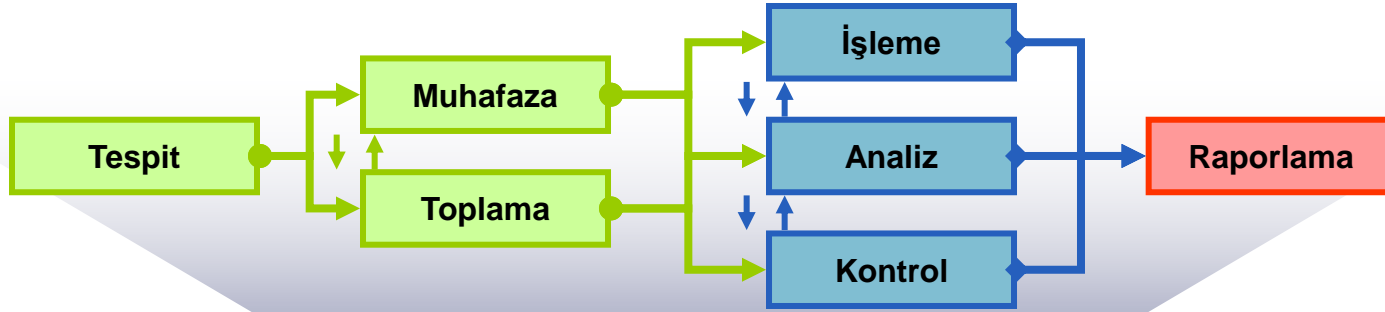
- Left Pane:** A tree view showing the file system structure, including folders like Intel, Internet Explorer, Java, McAfee, and Microsoft Office.
- Center Pane:** A table listing files. Two files are highlighted with a red circle:

Name	Filter	In Report	File Ext	File Type	File Category	Signature	Description	Is Deleted	Last Accessed	File Created	Last Written
Outlook.pst	MS Outlook		pst	Outlook Personal ...	Mail		File, Archive		05/06/11 03:55:48	11/25/10 12:06:22	05/06/11 03:55:48
archive.pst	MS Outlook		pst	Outlook Personal ...	Mail		File, Archive		05/09/11 11:57:51	02/17/11 10:08:18	05/09/11 11:57:51

- Bottom Pane:** A hex view of a file, showing a grid of hexadecimal values and their corresponding ASCII characters. A red circle highlights the right side of this pane, which contains a sidebar with a tree view of file types, including Files Groups, File Details, Printer Spool Files, and Microsoft Office (MS Word, MS Powerpoint, MS Access, MS Excel).

2.3 Elektronik Kanıt Yönetimi

Elektronik Kanıt Yönetimi Süreci



100 GB Veri Üzerinde
Çalışılmak Üzere
Hazırlanıyor

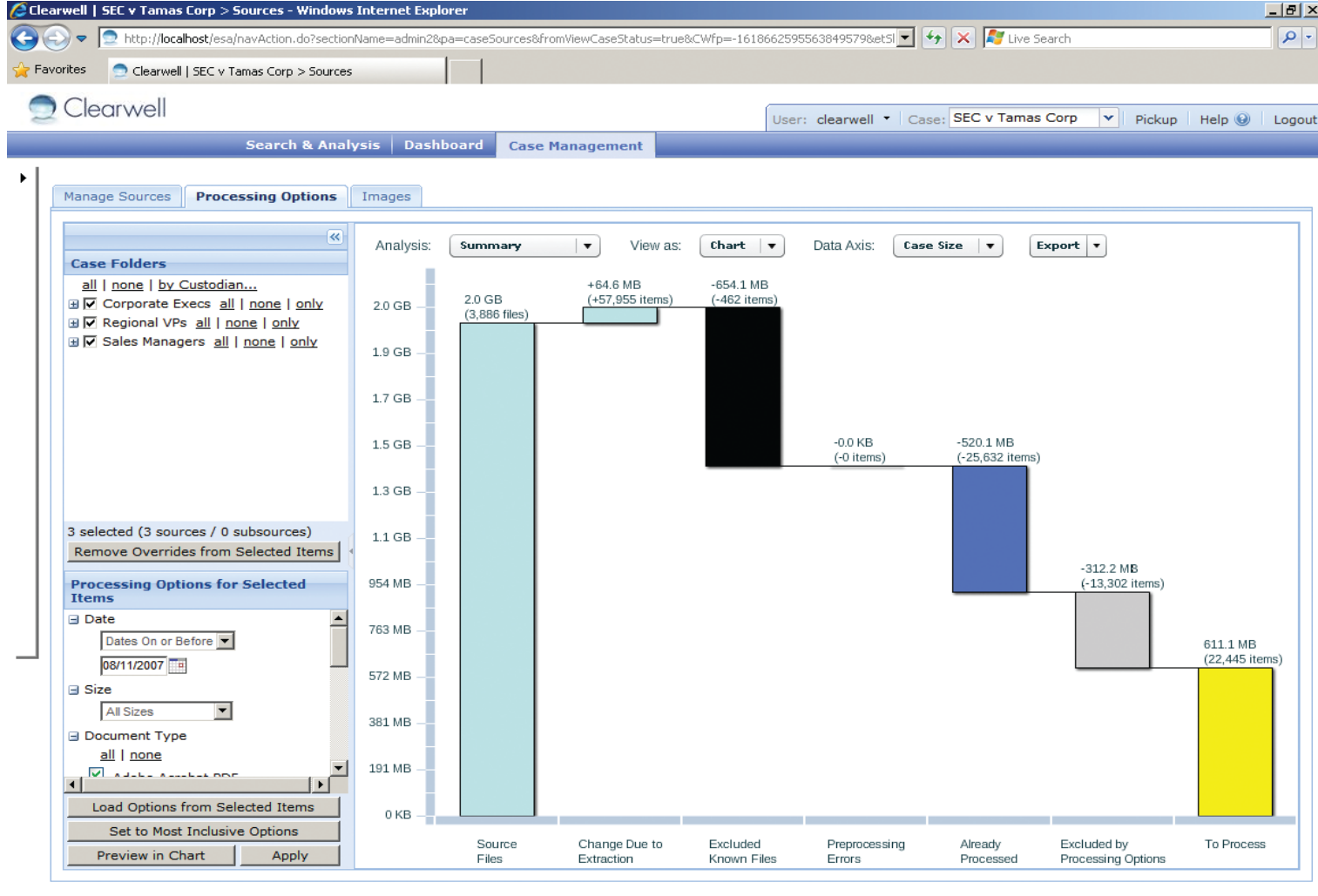
~80+% seçilme süreci sonucu



Asıl incelenmesi
gerekten veri
20GB 'a düşüyor

- Tarih ve dosya tipine göre filtreleme
- Mükerrer kayıtların tespiti
- Arama yapılacak başlık, konu ve isme göre filtreleme
- İnteraktif analiz yöntemleri
- Üstün arama teknikleri

2.3 Elektronik Kanıt Yönetimi



©2004-2010, Clearwell Systems, Inc. All Rights Reserved. [Feedback](#) | [Support](#) | [Documentation](#) v6.0.7.0 x86

2.3 Elektronik Kanıt Yönetimi

Select Variations

Select variations for: fals* Show: All

<input type="checkbox"/>	Variation	Matching Emails	Matching Unique Files
<input type="checkbox"/>	falsestart	274	4
<input type="checkbox"/>	falsetto	74	5
<input type="checkbox"/>	falsie	0	5
<input type="checkbox"/>	falsification	1	6
<input type="checkbox"/>	falsifications	15	4
<input checked="" type="checkbox"/>	falsified	68	8
<input checked="" type="checkbox"/>	falsify	27	0
<input checked="" type="checkbox"/>	falsifying	29	8
<input type="checkbox"/>	falsity	148	5
<input type="checkbox"/>	falsom	43	2
<input type="checkbox"/>	falstaff	70	2
<input type="checkbox"/>	falstore	25	4

Displaying 10 - 21 of 21

OK Copy Shown Variations Cancel

3. Özet

4. Sorular

Teşekkürler

Göktürk Tamay tarafından sunulmuştur

gtamay@kpmg.com





cutting through complexity™

© 2011 Akis Bağımsız Denetim ve Serbest Muhasebeci Mali Müşavirlik A.Ş., KPMG International Cooperative'in üyesi bir Türk şirkettir. Tüm hakları saklıdır.

KPMG adı, KPMG logosu ve "cutting through complexity"
KPMG International Cooperative'in tescilli ticari markalarıdır.