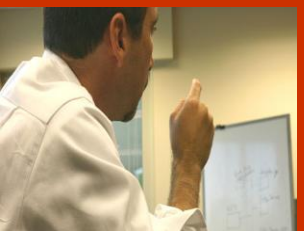


SENSAGE

The Devil's in the Detail

A Real World Problem

Taliban using Skype phones to dodge MI6

By **Glen Owen**

TALIBAN fighters targeting British troops in Afghanistan are using the latest 'internet phones' to evade detection by MI6, security sources said last night.

Skype, a popular piece of consumer software that allows free calls to be made over the web, has been adopted by insurgents to communicate with cells strung out across the country.

Unlike traditional mobile calls, which can be monitored by RAF Nimrod spy planes, Skype calls – the commercial application of a technology called Voice Over Internet Protocol (VOIP) – are heavily encrypted.

Voice calls are broken into millions of pieces of data before being sent down the line and reassembled by the other caller's computer.

The British and American governments are investing considerable resources to crack the codes, and in the UK the Government is introducing legislation to force internet service providers to log all web activity by subscribers, which could then be turned over to the security services on demand. The disclosure comes as the 8,000 British troops in Afghanistan are facing attacks almost daily from an increasingly well co-ordinated Taliban.

'The trouble with this technology is that it is easily available but devilishly hard to crack,' the source said. 'The technology can now be accessed on mobile internet devices and the country's mobile phone network is expanding rapidly.'

Skype was created in 2003 and three years ago was bought by eBay for £1.4 billion. It has 300 million accounts and at any one time, more than 12 million people are using the service.

Sir David Pepper, the head of GCHQ, the British Government's top-secret listening post, has told MPs that internet calls are 'seriously undermining' his organisation's ability to intercept communications.

Skype said last night it did not want to comment.

WEB OF DECEIT: Taliban internet calls are hard to monitor

SenSage

Principals of Data Retention

- Collect
  - All Records must be collected in a timely & secure manner
  - Records should not be modified
- Retain
  - Data must be held in a secure & tamperproof environment
  - Minimal operational overheads to maintain availability of data
  - Data must be available as and when needed with minimum delay
- Analyse
  - Records must be queried in both pre defined reports and in a ad-hoc manner
  - Queries should return “Without Undue Delay”
  - Reports should be made availble in many formats
  - Authentication should be used to safeguard data access
- Dispose
  - Once retention has expired records should be deleted in an irretrievable manner
  - Legal Hold should be available on records under investigation

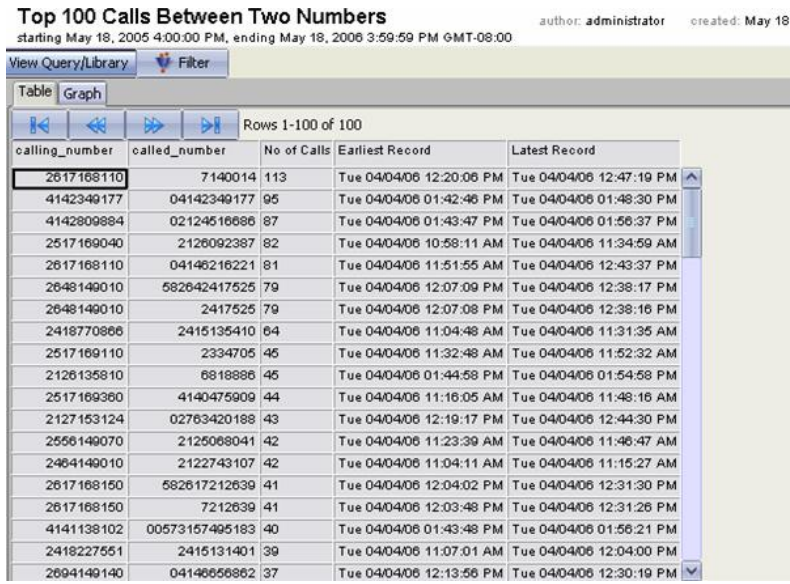
SENSAGE

Data Created

- 100's of Billions of Records
- Records typically short but Structured
- Huge Growth on a periodic basis
- Example:
  - 1 department of a European Telco = 13.6Tb / Qtr
  - Storage up to 24 Months (may be extended)
  - Therefore total required: 108.8 Tb
- Rapid access / querying required so "Off-Line" not an option

Reporting

- Complex correlations
  - Who called who, when, from where, how long
  - Who called who but didn't get answered
  - Repeating patterns of call behaviour
  - Interconnections with calls and other communication activity (SMS)
  - Who owned this IP address
  - Who accessed these websites & When?
- Historical Access
  - Up to 24 months
  - (Option for longer Periods)



Top 100 Calls Between Two Numbers

author: administrator created: May 18

starting May 18, 2005 4:00:00 PM, ending May 18, 2006 3:59:59 PM GMT-08:00

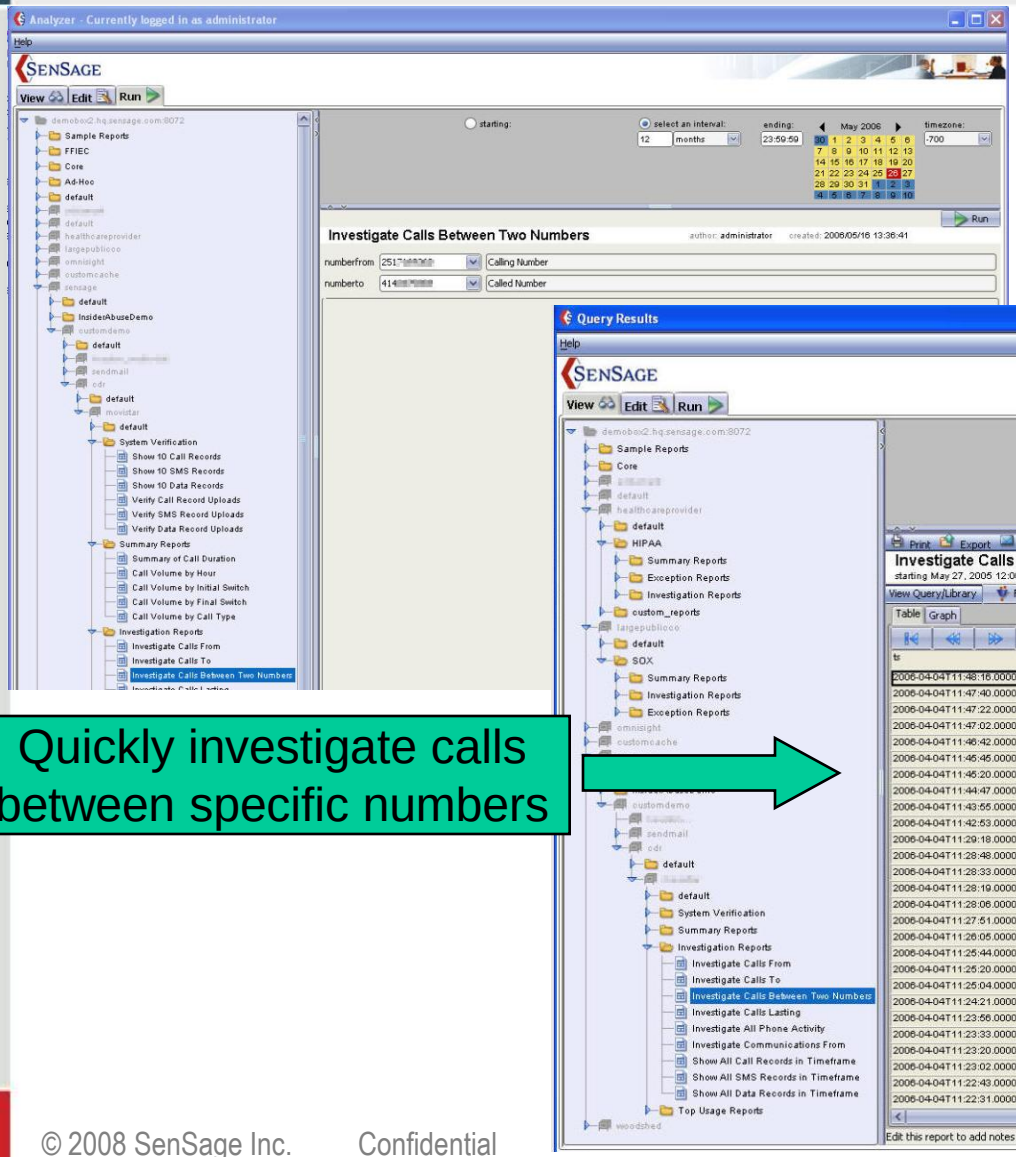
View Query/Library | Filter

Table | Graph

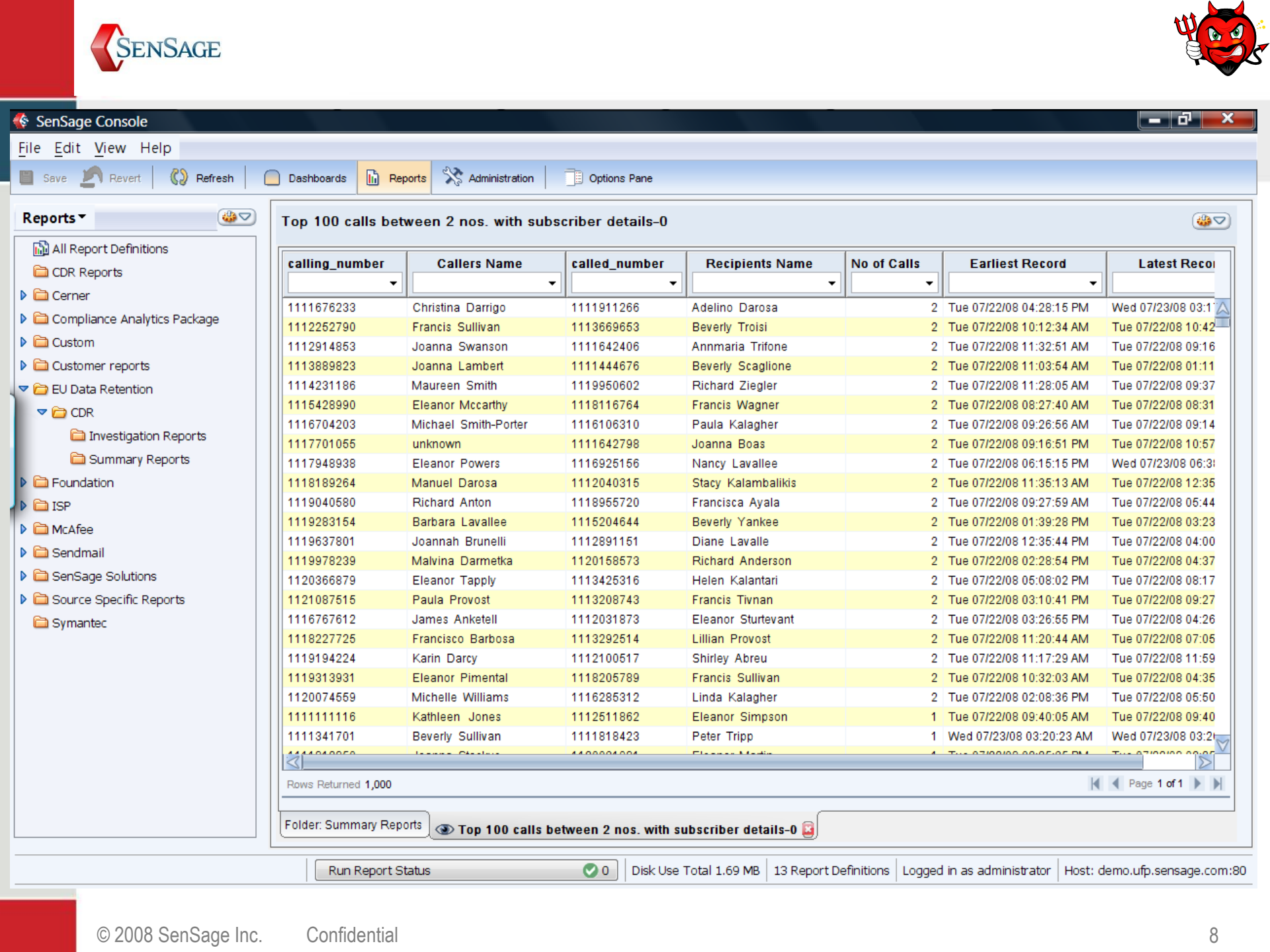
Rows 1-100 of 100

calling_number	called_number	No of Calls	Earliest Record	Latest Record
2617168110	7140014	113	Tue 04/04/06 12:20:06 PM	Tue 04/04/06 12:47:19 PM
4142349177	04142349177	95	Tue 04/04/06 01:42:46 PM	Tue 04/04/06 01:48:30 PM
4142809884	02124516686	87	Tue 04/04/06 01:43:47 PM	Tue 04/04/06 01:56:37 PM
2517169040	2126092387	82	Tue 04/04/06 10:58:11 AM	Tue 04/04/06 11:34:59 AM
2617168110	04146216221	81	Tue 04/04/06 11:51:55 AM	Tue 04/04/06 12:43:37 PM
2648149010	582642417525	79	Tue 04/04/06 12:07:09 PM	Tue 04/04/06 12:38:17 PM
2648149010	2417525	79	Tue 04/04/06 12:07:08 PM	Tue 04/04/06 12:38:16 PM
2418770866	2415135410	64	Tue 04/04/06 11:04:48 AM	Tue 04/04/06 11:31:35 AM
2517169110	2334705	45	Tue 04/04/06 11:32:48 AM	Tue 04/04/06 11:52:32 AM
2126135810	6818886	45	Tue 04/04/06 01:44:58 PM	Tue 04/04/06 01:54:58 PM
2517169360	4140475909	44	Tue 04/04/06 11:16:05 AM	Tue 04/04/06 11:48:16 AM
2127153124	02763420188	43	Tue 04/04/06 12:19:17 PM	Tue 04/04/06 12:44:30 PM
2556149070	2125068041	42	Tue 04/04/06 11:23:39 AM	Tue 04/04/06 11:46:47 AM
2464149010	2122743107	42	Tue 04/04/06 11:04:11 AM	Tue 04/04/06 11:15:27 AM
2617168150	582617212639	41	Tue 04/04/06 12:04:02 PM	Tue 04/04/06 12:31:30 PM
2617168150	7212639	41	Tue 04/04/06 12:03:48 PM	Tue 04/04/06 12:31:26 PM
4141138102	00573157495183	40	Tue 04/04/06 01:43:48 PM	Tue 04/04/06 01:56:21 PM
2418227551	2415131401	39	Tue 04/04/06 11:07:01 AM	Tue 04/04/06 12:04:00 PM
2694149140	04146656862	37	Tue 04/04/06 12:13:56 PM	Tue 04/04/06 12:30:19 PM

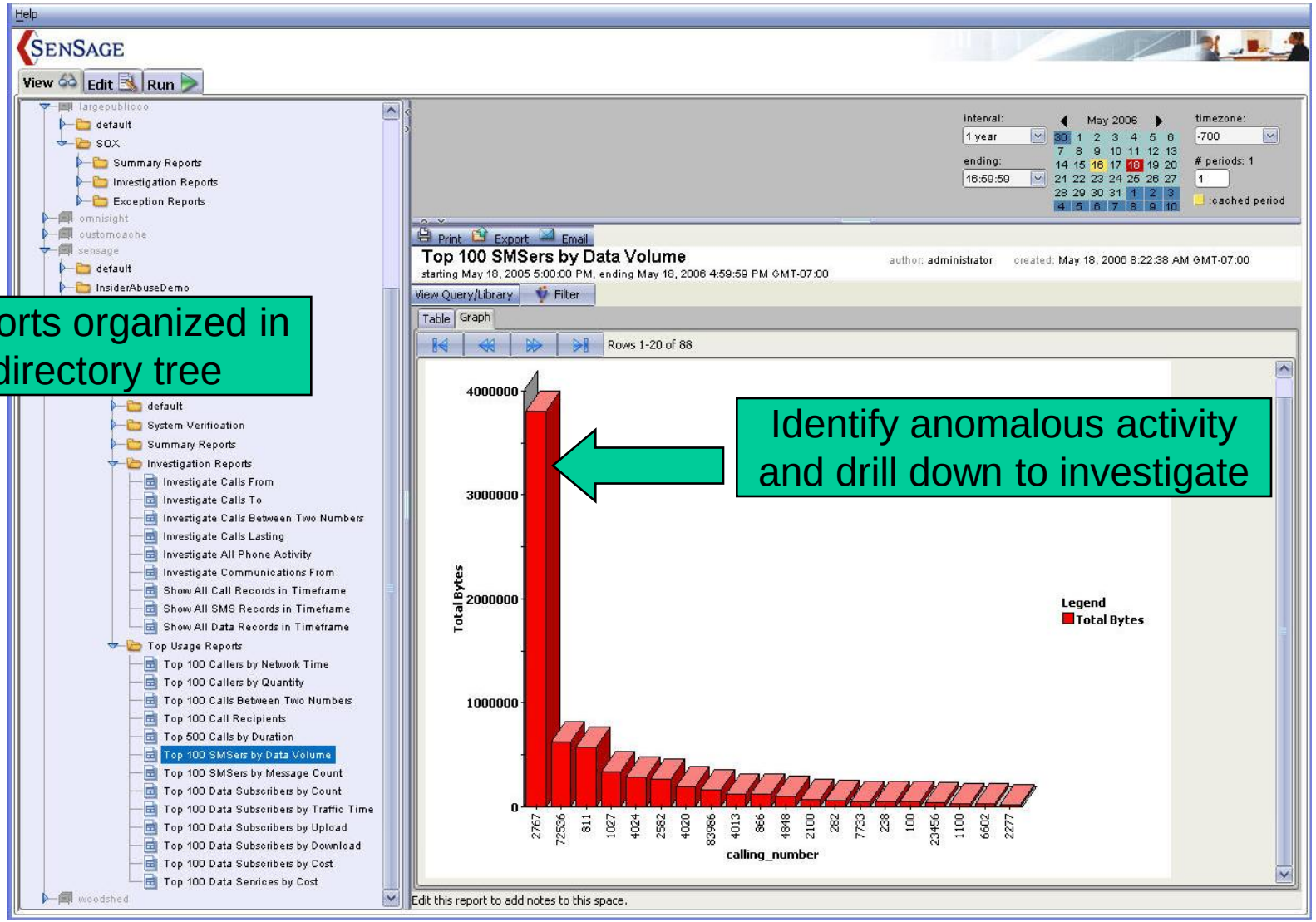
Flexible Investigation Interface



Quickly investigate calls between specific numbers


SenSage Console
File Edit View Help
Save Revert Refresh Dashboards Reports Administration Options Pane
Reports
All Report Definitions
CDR Reports
Cerner
Compliance Analytics Package
Custom
Customer reports
EU Data Retention
CDR
Investigation Reports
Summary Reports
Foundation
ISP
McAfee
Sendmail
SenSage Solutions
Source Specific Reports
Symantec
Top 100 calls between 2 nos. with subscriber details-0
calling_number
Callers Name
called_number
Recipients Name
No of Calls
Earliest Record
Latest Reco
1111676233 Christina Darrigo 1111911266 Adelino Darosa 2 Tue 07/22/08 04:28:15 PM Wed 07/23/08 03:1
1112252790 Francis Sullivan 1113669653 Beverly Troisi 2 Tue 07/22/08 10:12:34 AM Tue 07/22/08 10:42
1112914853 Joanna Swanson 1111642406 Annmaria Trifone 2 Tue 07/22/08 11:32:51 AM Tue 07/22/08 09:16
1113889823 Joanna Lambert 1111444676 Beverly Scaglione 2 Tue 07/22/08 11:03:54 AM Tue 07/22/08 01:11
1114231186 Maureen Smith 1119950602 Richard Ziegler 2 Tue 07/22/08 11:28:05 AM Tue 07/22/08 09:37
1115428990 Eleanor Mccarthy 1118116764 Francis Wagner 2 Tue 07/22/08 08:27:40 AM Tue 07/22/08 08:31
1116704203 Michael Smith-Porter 1116106310 Paula Kalagher 2 Tue 07/22/08 09:26:56 AM Tue 07/22/08 09:14
1117701055 unknown 1111642798 Joanna Boas 2 Tue 07/22/08 09:16:51 PM Tue 07/22/08 10:57
1117948938 Eleanor Powers 1116925156 Nancy Lavallee 2 Tue 07/22/08 06:15:15 PM Wed 07/23/08 06:3
1118189264 Manuel Darosa 1112040315 Stacy Kalambalikis 2 Tue 07/22/08 11:35:13 AM Tue 07/22/08 12:35
1119040580 Richard Anton 1118955720 Francisca Ayala 2 Tue 07/22/08 09:27:59 AM Tue 07/22/08 05:44
1119283154 Barbara Lavallee 1115204644 Beverly Yankee 2 Tue 07/22/08 01:39:28 PM Tue 07/22/08 03:23
1119637801 Joannah Brunelli 1112891151 Diane Lavalle 2 Tue 07/22/08 12:35:44 PM Tue 07/22/08 04:00
1119978239 Malvina Darmetka 1120158573 Richard Anderson 2 Tue 07/22/08 02:28:54 PM Tue 07/22/08 04:37
1120366879 Eleanor Tapply 1113425316 Helen Kalantari 2 Tue 07/22/08 05:08:02 PM Tue 07/22/08 08:17
1121087515 Paula Provost 1113208743 Francis Tivnan 2 Tue 07/22/08 03:10:41 PM Tue 07/22/08 09:27
1116767612 James Anketell 1112031873 Eleanor Sturtevant 2 Tue 07/22/08 03:26:55 PM Tue 07/22/08 04:26
1118227725 Francisco Barbosa 1113292514 Lillian Provost 2 Tue 07/22/08 11:20:44 AM Tue 07/22/08 07:05
1119194224 Karin Darcy 1112100517 Shirley Abreu 2 Tue 07/22/08 11:17:29 AM Tue 07/22/08 11:59
1119313931 Eleanor Pimental 1118205789 Francis Sullivan 2 Tue 07/22/08 10:32:03 AM Tue 07/22/08 04:35
1120074559 Michelle Williams 1116285312 Linda Kalagher 2 Tue 07/22/08 02:08:36 PM Tue 07/22/08 05:50
1111111116 Kathleen Jones 1112511862 Eleanor Simpson 1 Tue 07/22/08 09:40:05 AM Tue 07/22/08 09:40
1111341701 Beverly Sullivan 1111818423 Peter Tripp 1 Wed 07/23/08 03:20:23 AM Wed 07/23/08 03:2
Rows Returned 1,000
Page 1 of 1
Folder: Summary Reports
Top 100 calls between 2 nos. with subscriber details-0
Run Report Status 0
Disk Use Total 1.69 MB
13 Report Definitions
Logged in as administrator
Host: demo.ufp.sensage.com:80

Comprehensive Analytics



SenSage Console

File Edit View Help

Save | Revert | Refresh | Dashboards | Reports | Administration | Options Pane

Dashboards

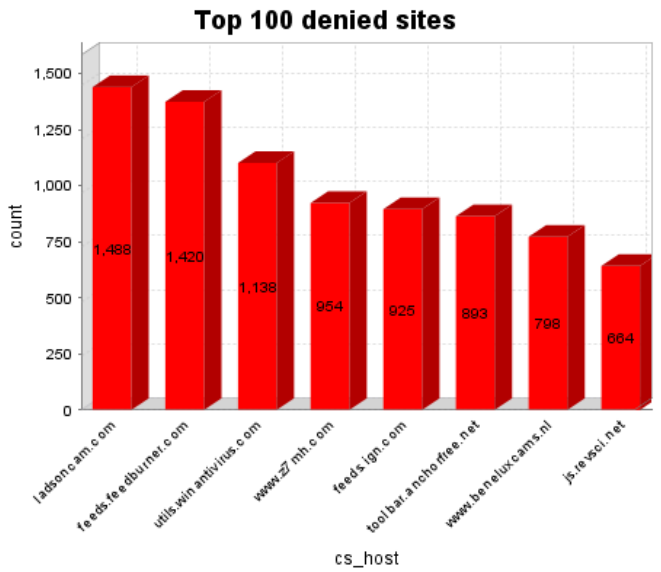
- Compliance Dashboards
- Custom Dashboards
  - SE
    - Danny
    - Elia
    - Pete
    - Peter
    - Richard
      - ISP
    - Tim
    - Wes
  - SenSage Solutions

Search

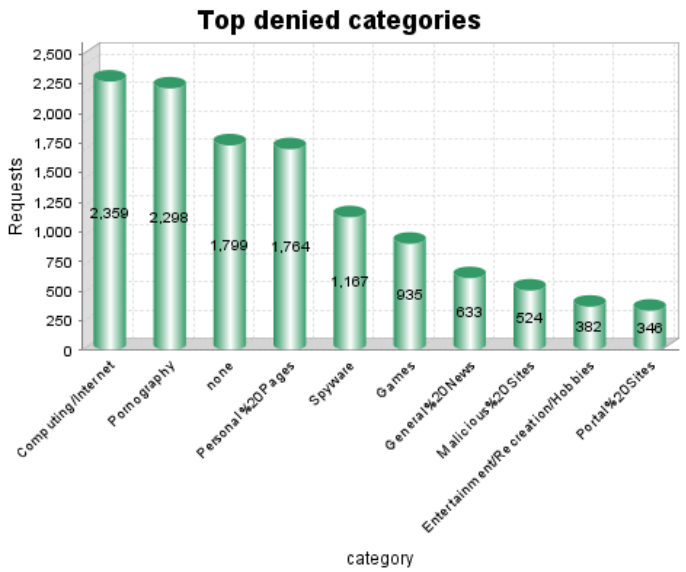
Widgets

- System Alerts
- Security Alerts
- Exception Alerts
- Text
- Image
- McAfee Intrushield Top 20 Most C...
- McAfee Intrushield Systems At Risk
- McAfee MWS Virus Summary By ...
- McAfee MWS Virus Email Summary
- McAfee Intrushield Attacks Summ...
- McAfee Intrushield Top 10 Source...
- McAfee MWS Virus Summary
- McAfee MWS Virus Web Details
- McAfee MWS Virus Web Summary
- McAfee Intrushield Top 10 Target...

ISP



Rows Returned 100 | Page 1 of 13



Rows Returned 47 | Page 1 of 5

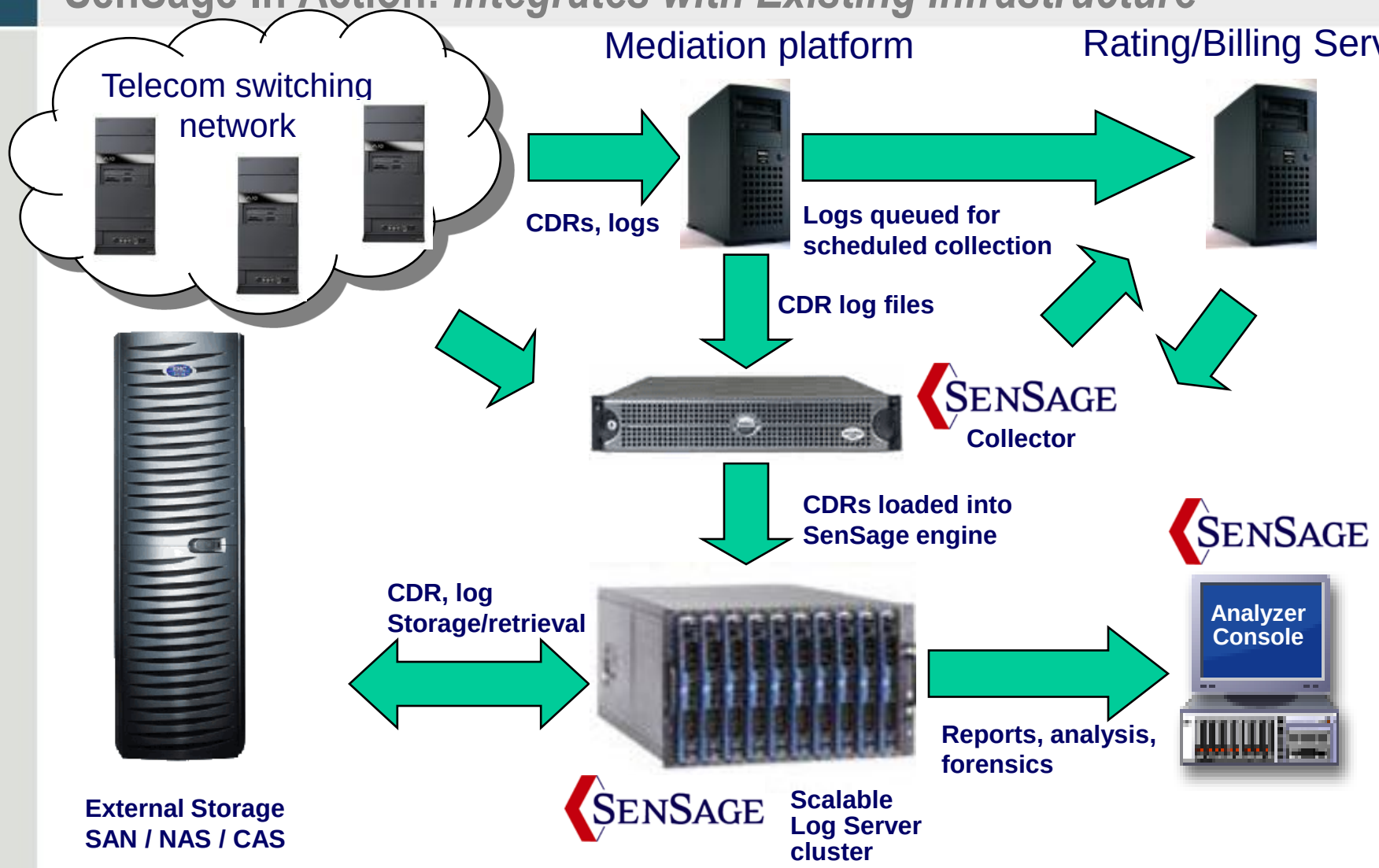
Listing of the top denied sites and categories.

Qtel Let's Connect

Denieds

Run Report Status 0 | Logged in as administrator | Host: demo.ufp.sensage.com:80

SenSage In Action: *Integrates with Existing Infrastructure*



SENSAGE

Example: Recent EMC/SenSage "100 billion" POC Results

- Off-the-shelf software and hardware
- Load & Query performance test
  - Simulate Telco Events; 10M subscribers, 135M calls/day, 2 years retained data
  - Search all events from a source / between sources within 3 month range
- Event load & retention rate
  - 100B records; approximately 26TB of raw data
  - Loaded 300,000 records/sec. on a sustained basis
  - No filtering or summarization required
  - Net result was 13 TB of online storage (2 copies stored for D/R)
- Response time on typical law enforcement requests
  - Who has "Charlie McAlister" called over any 3 mos.

    – results with detail in 6 minutes
  - List calls between "Charlie McAlister" & "Mauro Bonfanti"

    - results with detail in 6.8 minutes

IP Use Case Middle East Operator

- Requirement to identify specific individuals accessing a defined list of "Interesting" websites (5000 initial list)on specific dates

  Mandate from Ministry of Interior

Anonymizers	Government/Military	Provocative%20Attire
Art/Culture/Heritage	Health	Religion%20and%20Ideology
Business	Humor	Search%20Engines
Chat	Instant%20Messaging	Sexual%20Materials
Computing/Internet	Internet%20Radio/TV	Shareware/Freeware
Consumer%20Information	Job%20Search	Shopping/Merchandizing
Criminal%20Skills	Malicious%20Sites	Spam%20Email%20URLs
Dating/Social	Mobile%20Phone	Sports
Education/Reference	Non-Profit%20Organizations/Advocacy%20Groups	Spyware
Entertainment/Recreation/Hobbies	Nudity	Stock%20Trading
Extreme	P2P/File%20Sharing	Streaming%20Media

SENSAGE

Data Sources & Volumes

- **Bluecoat ProxySG**
- **RADIUS – Session/Authentication Logs**
  - DSLUsers , WiFi , PrePaid
- 50 – 60 Gb / Day
- Oracle Subscriber Database

- Solution: SenSage system (~ $300k project) providing correlated queries with look-ups to databases of Subscriber information
- Operational within 8 weeks from project start
- Answers with 60 seconds

SENSAGE

Secondary Usage

- Checking and Investigating for revenue assurance purposes
- Determine
  - double-billing
  - missed billing
  - use of prepaid service cards

Penetration - EMEA

- Germany
  - Cable Provider
- Greece
  - National Carrier
  - Mobile Operators
- Ireland
  - Major Mobile Operator
- Italy
  - National Carrier
  - Multiple Mobile Operators
- Poland
  - Major Mobile Operator
- Slovenia
  - Cable Provider
  - Multiple Mobile Operators

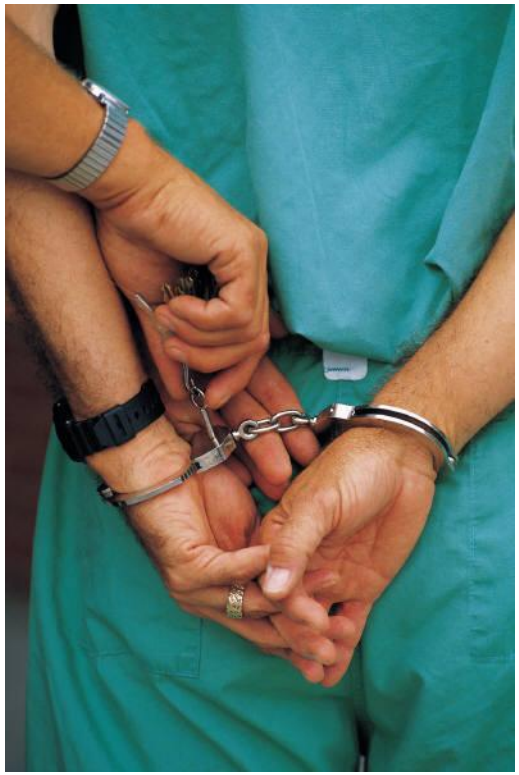
Many more projects in pipeline

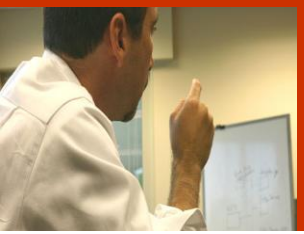
Penetration - Non EU

- Middle East
  - National Carrier
  - Major Mobile Operators
- Brazil
  - Major Mobile Operator
- Japan
  - Major Mobile Operator
- US
  - National Operator
  - Cable Operators

SenSage Summary

- 100's Million Subscribers
- Multiple LEAs served Daily
- Cost Effective Solutions
- Rapid Deployments
- Satisfied Customers
- Finding the Devils





Case Study: Telecom Italia

agora
Living the Information Age

TELECOM ITALIA